



# Configuration Guide

## Splunk Phantom

Version 1.0  
September 2019

Okta Inc.  
100 First Street  
San Francisco, CA 94105

[info@okta.com](mailto:info@okta.com)  
1-888-722-7871

## Table of Contents

<b>What Is This Document</b>	<b>2</b>
<b>What Is Okta</b>	<b>2</b>
<b>What Is Phantom</b>	<b>2</b>
<b>Solving Complex Business Problems</b>	<b>3</b>
Splunk Phantom Actions for Okta App	3
<b>Overview: Introduction to the Integration</b>	<b>4</b>
<b>Configuration Guides</b>	<b>4</b>
Generate an API Token in Okta	4
Configure Okta Actions in Phantom	5
Login to Splunk Phantom	5
<b>References</b>	<b>11</b>

## What Is This Document

This document is intended for Okta and Phantom customers. This document will provide an in-depth review of the involved components and how they can be paired. When combined, Okta and Phantom deliver advanced solutions for securing your enterprise.

## What Is Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 6,550 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers.

## What Is Phantom

The Phantom platform combines security infrastructure orchestration, playbook automation, and case management capabilities to integrate your team, processes, and tools together.

## Solving Complex Business Problems

In order to protect the enterprise, security teams must quickly resolve alerts as they arise, as well as proactively identify threats before they cause damage. Many of these threats involve weak or stolen credentials, demonstrating that hackers are increasingly targeting user identities. To better protect against these threat vectors and deliver identity-driven security, Okta integrates with Splunk Phantom to enable identity-centric response actions. When suspicious account activity is detected, like a login from a new device or location, security teams can mitigate the threat automatically by clearing active sessions or forcing multi-factor authentication (MFA) with Okta. If, after further investigation, the user does appear to be compromised, security teams can take additional remediation actions against the bad actor by suspending the compromised account and conducting a password reset. Together, Okta + Splunk Phantom orchestrate security using identity as the control point.

## Splunk Phantom Actions for Okta

Splunk Phantom and Okta have partnered to deliver the following Actions in the Okta app for Phantom. These actions can be used to automatically protect your sensitive assets in the cloud in the event of a detected breach or other anomaly.

Okta as the leading provider in Identity as a Service (IDaaS) sits at the center of your cloud and hybrid cloud authentication landscape, becoming a strategic point of control and enforcement.

This integration provides the following Actions for Okta:

- **list users** - Get the list of users
- **list user groups** - Get the groups that the user is a member of
- **add group** - Add a group
- **reset password** - Generate a one-time token that can be used to reset a user's password
- **set password** - Set the password of a user without validating existing credentials
- **disable user** - Disable the specified user
- **enable user** - Enable the specified user
- **get user** - Get information about a user
- **get group** - Get information about a group
- **list providers** - List identity providers (IdPs) in your organization
- **list roles** - Lists all roles assigned to a user
- **assign role** - Assign a role to a user
- **unassign role** - Unassign a role to a user

## Overview: Introduction to the Integration

When identity-centric alerts are encountered, Splunk Phantom can make use of Okta Responses to automatically protect your sensitive applications like Office 365, Box, AWS, and thousands of others available in the Okta Integration Network.

With the steady decay of traditional security perimeters, incorporating identity-centric controls to your security toolkit is a must have.

## Configuration Guides

Refer to the sections below for configuration steps.

### Generate an API Token in Okta

Login to Okta to produce an API Token. The API Token and your Okta domain name will be required in subsequent steps.

#### **Best practice guidance**

You should create a local Okta user account that will be dedicated to this integration, this account will be referred to as the Service Account.

- Assign an Okta admin role to this Service Account that provides just enough privilege to perform the actions that you desire.
- The Service Account needs to remain active to support this integration.
- The Password can be changed without affecting the API Token you generated.

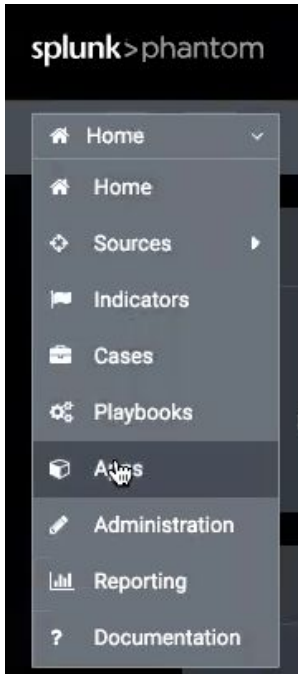
Refer to our [Administrators Guide](#) for more information about roles in Okta.

Refer to our [Getting a Token](#) guide for detailed steps to create an API Token.

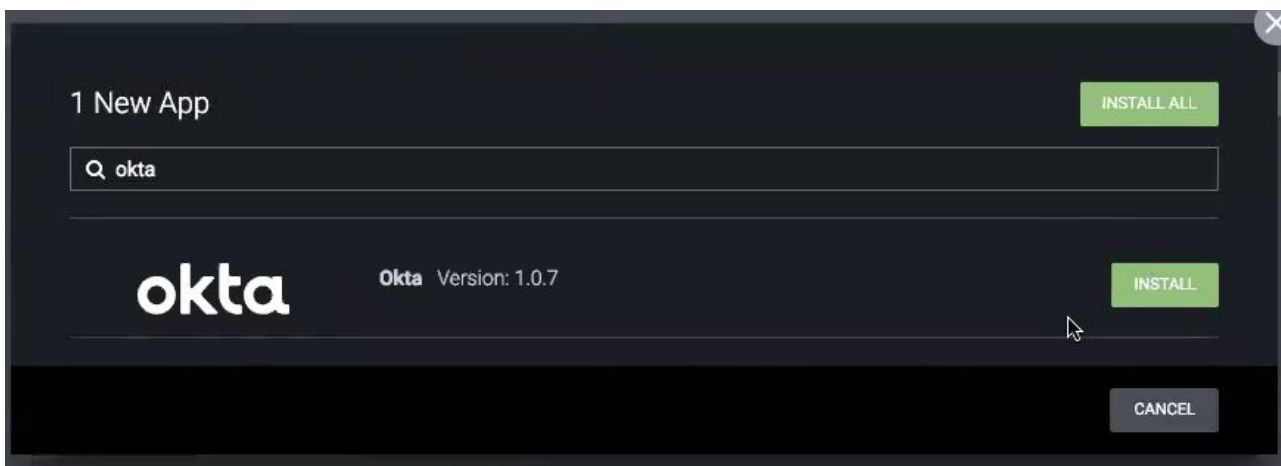
## Configure Okta Actions in Phantom

### Login to Splunk Phantom

1. Click on **Home** and select **Apps**



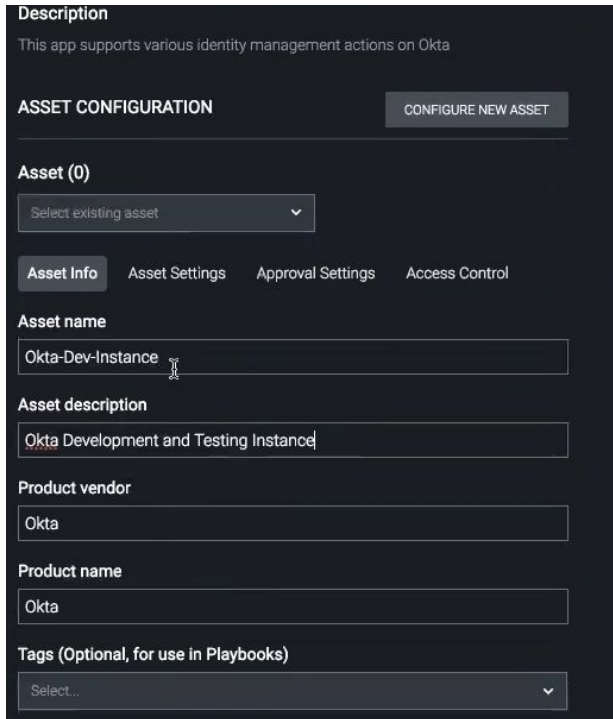
2. Search for and install the **Okta** app



3. Locate the newly installed Okta app from the list of **Unconfigured Apps** and click **Configure New Asset**

4. In the **Asset** info tab

a. Provide a name and description



The screenshot displays the 'Asset Configuration' interface for a new asset. At the top, there is a 'Description' section with the text 'This app supports various identity management actions on Okta'. Below this is the 'ASSET CONFIGURATION' header with a 'CONFIGURE NEW ASSET' button. The 'Asset (0)' section contains a dropdown menu for 'Select existing asset'. Below the dropdown are four tabs: 'Asset Info' (selected), 'Asset Settings', 'Approval Settings', and 'Access Control'. The 'Asset Info' tab contains several input fields: 'Asset name' with the value 'Okta-Dev-Instance', 'Asset description' with the value 'Okta Development and Testing Instance', 'Product vendor' with the value 'Okta', and 'Product name' with the value 'Okta'. At the bottom, there is a 'Tags (Optional, for use in Playbooks)' section with a dropdown menu for 'Select...'. The interface is dark-themed.

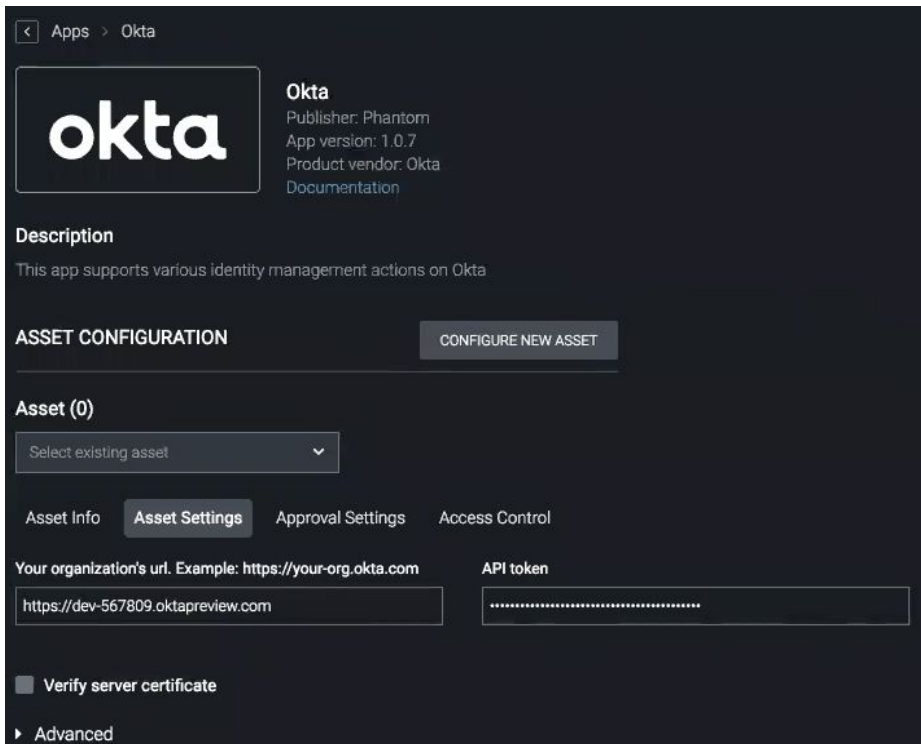
5. In the **Asset Settings** tab

a. Provide your **Okta Domain**:

i. YourOktaDomain.com

b. Provide your **API Token\***:

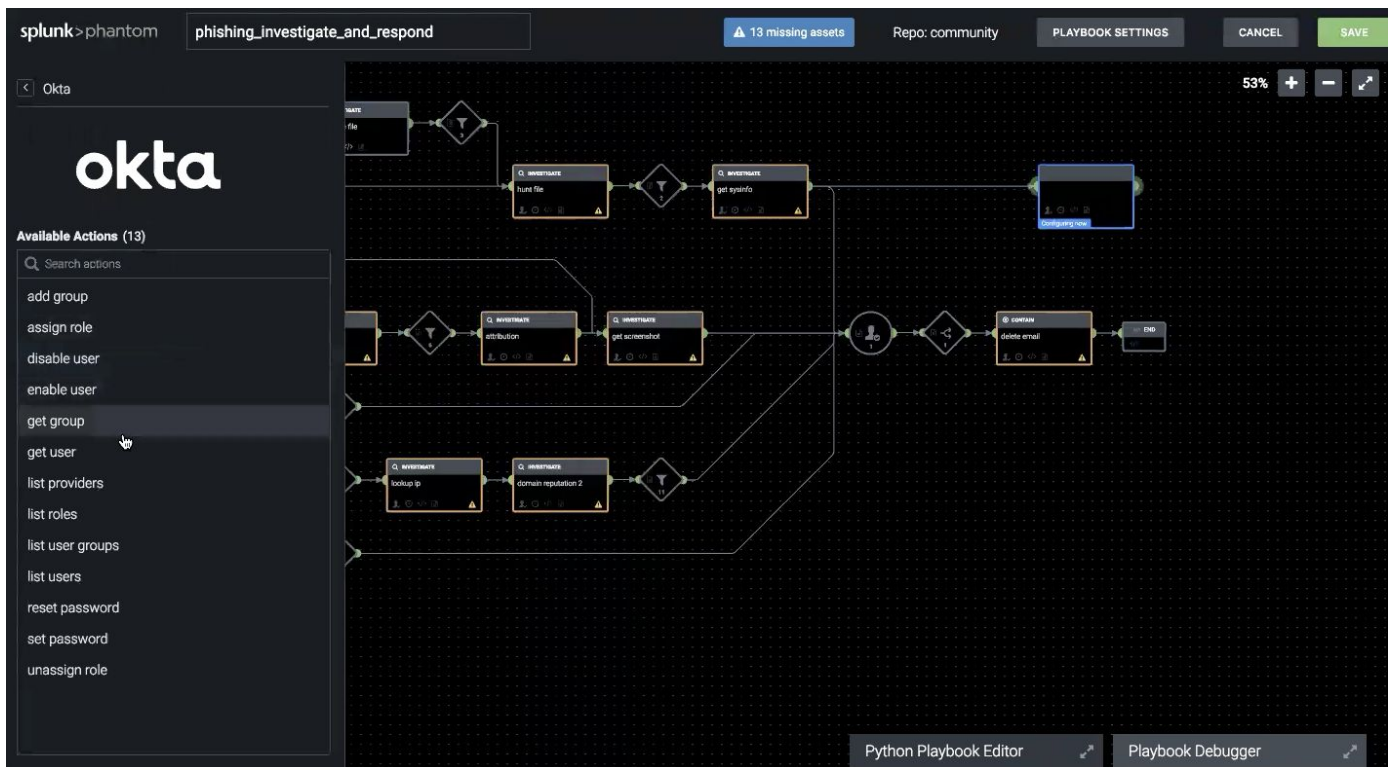
i. Created in previous section



6. Click **Save**

You are now ready to add Okta actions to your Playbooks or invoke the actions directly in an investigation.





**Run Action**    By Type    By App    Task

Action Name:    

Action Types:              Asset Types:  ▾

🔍     🔍

- add group
- approve user
- assign role
- create certificate
- create filter
- delete filter
- disable user
- enable user
- geolocate ip
- get certificate

The screenshot shows the Splunk Phantom interface for a 'Malicious URL Request Attempt' event. The event ID is 20, and it is categorized as 'LOW' severity. The interface includes a navigation bar with 'Activity' and 'Guidance' tabs, and a main content area with 'ARTIFACTS (1)' and a table of user data from the 'Okta' widget.

**Event Details:**

- events ID: 20
- Malicious URL Request Attempt
- Severity: LOW
- SLA: Exceeded by 19 days
- Owner: Select
- Set Status: New

**ARTIFACTS (1) Table:**

ID	LABEL	NAME	START TIME	CREATE TIME	SEVERITY	CREATED BY	TAGS
23	event	URL Artifact	Jan 24 at 04:34 AM	Jan 24 at 04:34 AM	LOW		

**Okta Widget: list users**

STATUS	FIRST NAME	LAST NAME	USER ID	LAST LOGIN
ACTIVE	Heena	Vaghela	00ugfn1pbqCsesAga0h7	None
ACTIVE	Heena	Vaghela	00ugfn2ea94teZbAD0h7	None
ACTIVE	Playbook	User	00uh3a0nyohmTniZJ0h7	None
PASSWORD_EXPIRED	TestUser	TestUser	00uh51fd7IP8UQXGJ0h7	None
PASSWORD_EXPIRED	SampleUser	SampleUser	00uh51hd9zXJcU0h20h7	None

## References

Links to relevant material from Okta and Splunk Phantom

Owner	Details	Link
Okta	Details about Okta	<a href="https://www.okta.com/">https://www.okta.com/</a>
Phantom	Okta app for Splunk Phantom	<a href="https://my.phantom.us/4.5/apps/">https://my.phantom.us/4.5/apps/</a> (requires Splunk Phantom login)
Okta	Getting an API Token in Okta	<a href="https://developer.okta.com/docs/api/getting_started/getting_a_token">https://developer.okta.com/docs/api/getting_started/getting_a_token</a>
Okta	Details about Okta Roles	<a href="https://support.okta.com/help/Documentation/Knowledge_Article/Administrators-793645444">https://support.okta.com/help/Documentation/Knowledge_Article/Administrators-793645444</a>