

Administrative Guide

FORTANIX DATA SECURITY
MANAGER – OKTA INTEGRATION
WITH EXISTING SENSU SERVER

VERSION 1.0

TABLE OF CONTENTS

1.0	INTRODUCTION	2
1.1	Purpose	2
1.2	Intended Audience	2
2.0	INTEGRATION STEPS	2
2.1	Configuration in Okta	2
2.2	Configuration in Sensu.....	5
2.3	Test the Integration.....	7
3.0	DOCUMENT INFORMATION	9
3.1	Document Location.....	9
3.2	Document Updates	9

1.0 INTRODUCTION

1.1 PURPOSE

Welcome to the Fortanix Data Security Manager (DSM) Administration guide. The purpose of this guide is to describe steps to integrate Sensu server with Okta for Open ID Connect (OIDC) based authentication.

1.2 INTENDED AUDIENCE

This setup guide is intended to be used by technical stakeholders of Fortanix DSM who will be responsible for planning, performing, or setting up the monitoring and alerting solution, such as the Systems Administrator, Chief Information Officer (CIO), Analysts, or Developers.

2.0 INTEGRATION STEPS

2.1 CONFIGURATION IN OKTA

1. Log in to the Okta admin console and go to **Applications**.
2. Click the **App Integration** option.
 - a. Select the **OIDC** option as the **Sign-in method**.
 - b. Select **Web Application** as the **Application type**.

The screenshot shows a dialog box titled "Create a new app integration" with a close button (X) in the top right corner. It is divided into two main sections: "Sign-in method" and "Application type".

Sign-in method: This section includes a "Learn More" link with an external icon. There are four radio button options:

- OIDC - OpenID Connect**: Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**: XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**: Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**: Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type: This section includes a question: "What kind of application are you trying to integrate with Okta?" and a note: "Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations." There are three radio button options:

- Web Application**: Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**: Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**: Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

At the bottom right of the dialog, there are "Cancel" and "Next" buttons.

FIGURE 1: APP INTEGRATION OPTIONS

- c. Click **Next**.
3. On the New Web App Integration page, fill in the following information:
 - a. **App integration name**- Type *sensu* as the value.
 - b. **Grant type**- Select the **Refresh Token** option.
 - c. **Sign-in redirect URIs**- **http://<api-url>/authorization-code/callback**
Where, the **<api url>** for sensu is **<<serverip>:8080** generally.
 - d. **Assignments**- Select the **Skip group assignment for now** option.
4. Click **Save**.

New Web App Integration

General Settings

App integration name:

Logo (Optional):

Grant type:

- Client acting on behalf of itself
 - Client Credentials
- Client acting on behalf of a user
 - Authorization Code
 - Interaction Code
 - Refresh Token
 - Implicit (hybrid)

Sign-in redirect URIs:

- Allow wildcard * in sign-in URI redirect.

Trusted Origins:

Base URIs (Optional):

FIGURE 2: WEB APP INTEGRATION OPTIONS

5. A new Web App Integration is now created. Click the app, and copy the **Client ID**, **Client secret**, and **Okta domain** to the notepad.

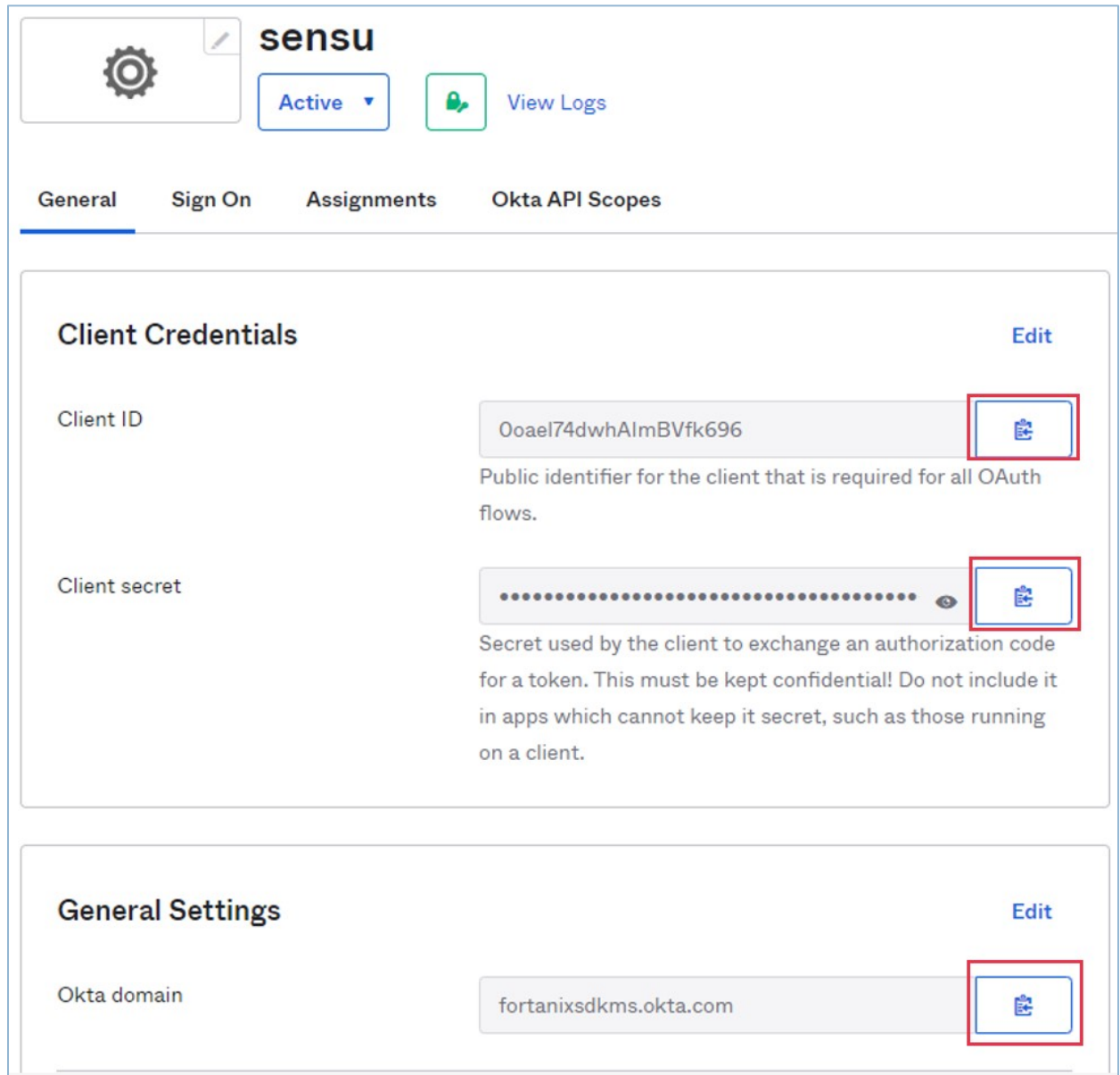


FIGURE 3: COPY CLIENT CREDENTIALS

- Next, click the **Assignments** tab and add people/group assignments as required.

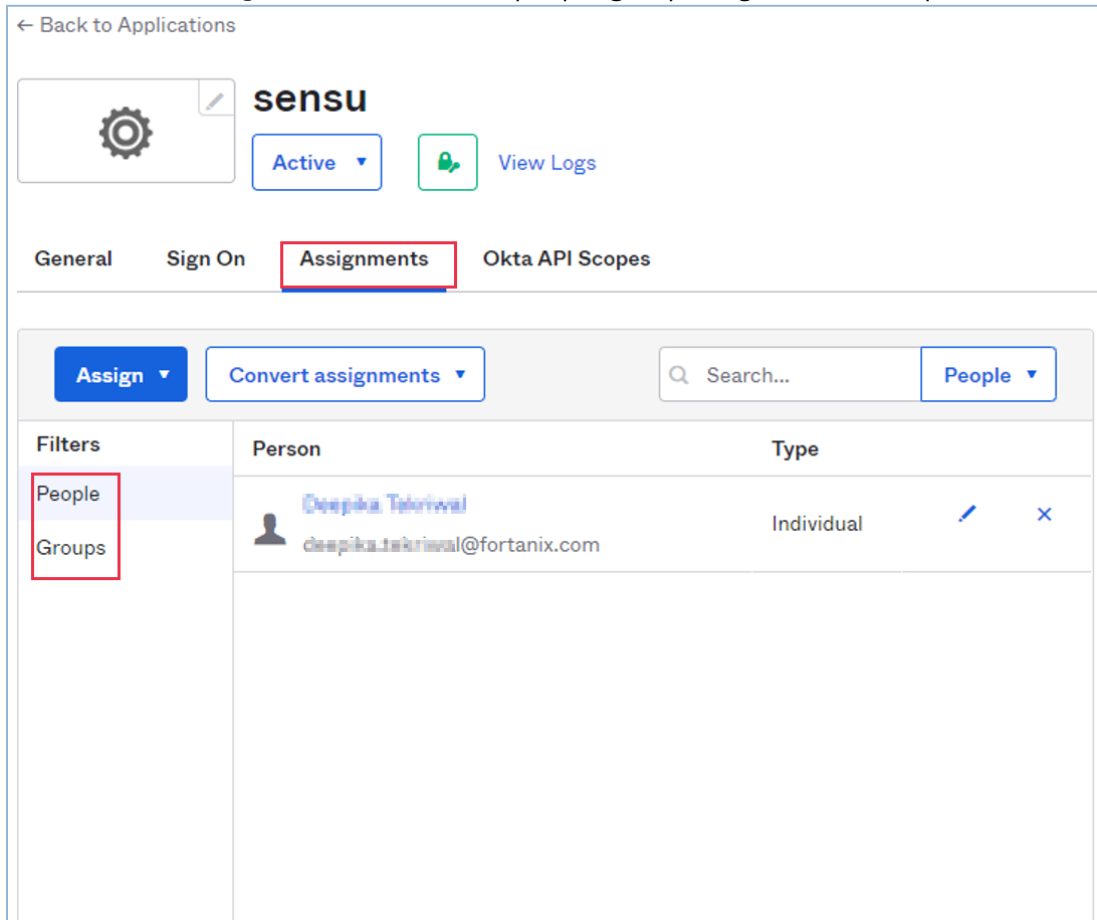


FIGURE 4: ADD PEOPLE AND GROUP ASSIGNMENTS

2.2 CONFIGURATION IN SENSU

- Create an `oidc.yml` file with all the information.

Here is a sample `oidc.yml` file:

```
type: oidc
api_version: authentication/v2
metadata:
  name: okta
spec:
  additional_scopes:
    - email
    - groups
```

```
client_id: 0oael74dwhAImBVfk696
client_secret: tfbocOodGFnxefgydm4yFSjDSLvpw_mv41vI1QLM
redirect_uri:
http://54.151.121.234:8080/api/enterprise/authentication/v2/oidc/call
back
server: https://fortanixsdkms.okta.com
disable_offline_access: false
username_claim: email
group_claim: groups
username_prefix: 'oidc:'
group_prefix: 'oidc:'
```

Where,

- `client_id`, `client_secret` and `server` are from Okta. *Refer to Step 5 in the Section: Configuration in Okta.*
- `Redirect_uri` is the value provided in *Step 3c in Section: Configuration in Okta.*

2. Next, create OIDC authentication using the following command:

```
sensuctl create --file oidc.yml
```

Check if the OIDC authentication is created using the following command:

```
sensuctl auth list
```

3. Now create a role and do role-binding for the user/group:

For example, if you are creating a read-only role for a user- rose.bush@fortanix.com

Create a read-only role:

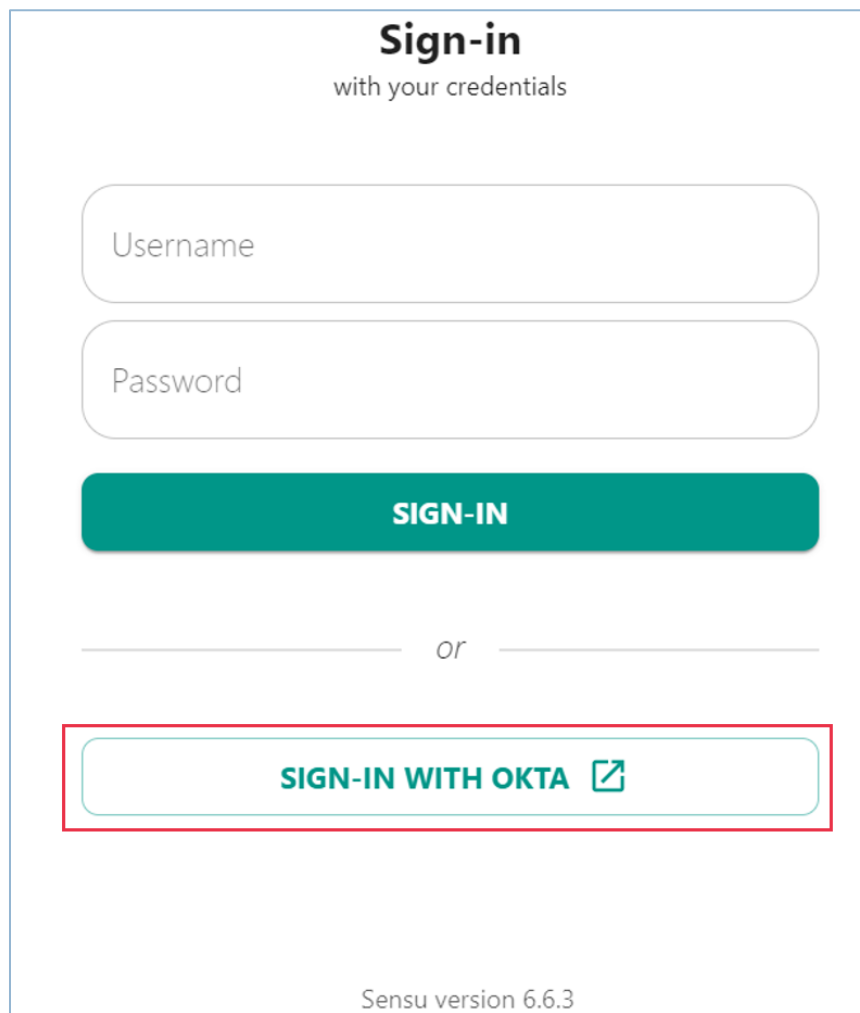
```
sensuctl role create readonlyuser --namespace default --
resource=checks,entities,events --verb=get,list
```

Create a role binding on the user:

```
sensuctl role-binding create rbokta --user oidc:rose.bush@fortanix.com  
--role readonlyuser --namespace default
```

2.3 TEST THE INTEGRATION

1. Log in to the Sensu app and click **SIGN-IN WITH OKTA** button.



The screenshot shows the Sensu Sign-in page. At the top, it says "Sign-in with your credentials". Below this are two input fields: "Username" and "Password". A green "SIGN-IN" button is positioned below the password field. Below the button is the word "or" flanked by horizontal lines. At the bottom of the form, a button labeled "SIGN-IN WITH OKTA" with an external link icon is highlighted with a red rectangular border. The footer of the page indicates "Sensu version 6.6.3".

FIGURE 5: SIGN IN WITH OKTA

2. After you are logged in as an Okta user, you should be able to view the Sensu dashboard with the required “view” privileges.

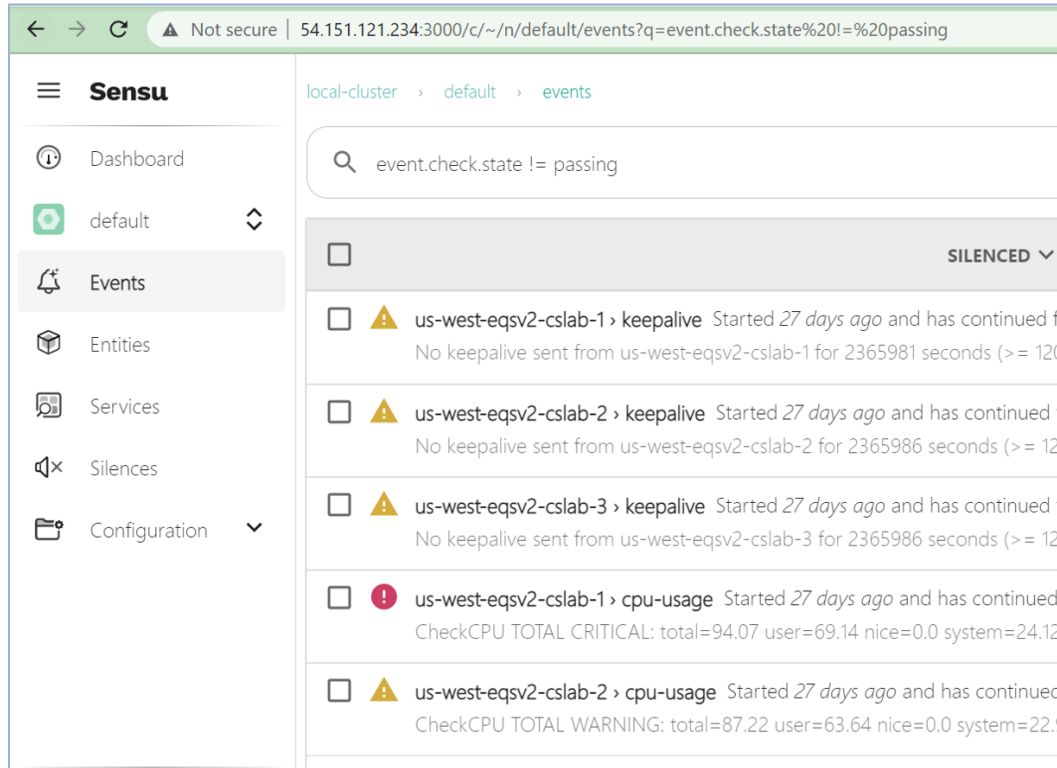


FIGURE 6: SENSU DASHBOARD

3.0 DOCUMENT INFORMATION

3.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

<https://support.fortanix.com/hc/en-us/articles/4403030801812-Splunk-Integration-with-Sensu-Server>

3.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com

© 2016 – 2022 Fortanix, Inc. All Rights Reserved.

Fortanix® and the Fortanix logo are registered trademarks or trade names of Fortanix, Inc.

All other trademarks are the property of their respective owners.

NOTICE: This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform info@fortanix.com immediately.