

SSO Guide for Curation Health app via Okta

How to set up Okta Single Sign-on integration

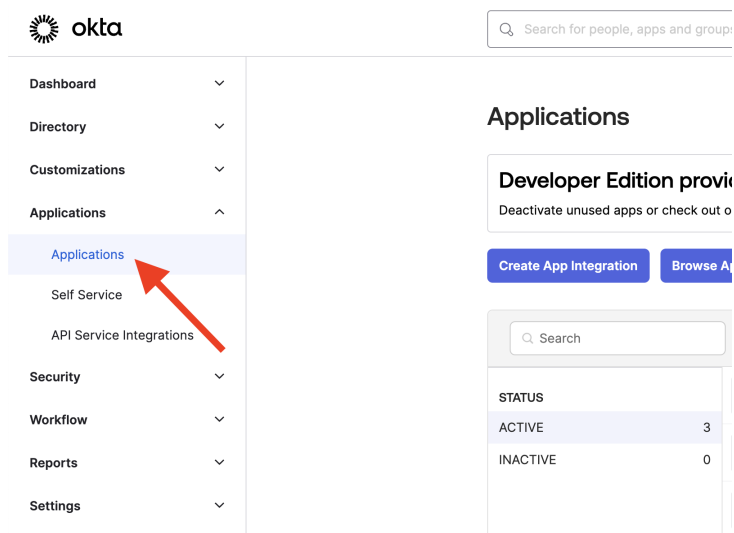
Prerequisites & Requirements:

- You must have access to an Okta organization on an Okta Business or Enterprise plan.
- You must be an Okta administrator for your organization.
- You must be an existing, or contractually bound, tenant of Curation Health.
- Install the Curation Health app for your organization on your Okta instance from the Okta Admin *Applications* page after clicking *Browse Applications* (see images below).

Supported features:

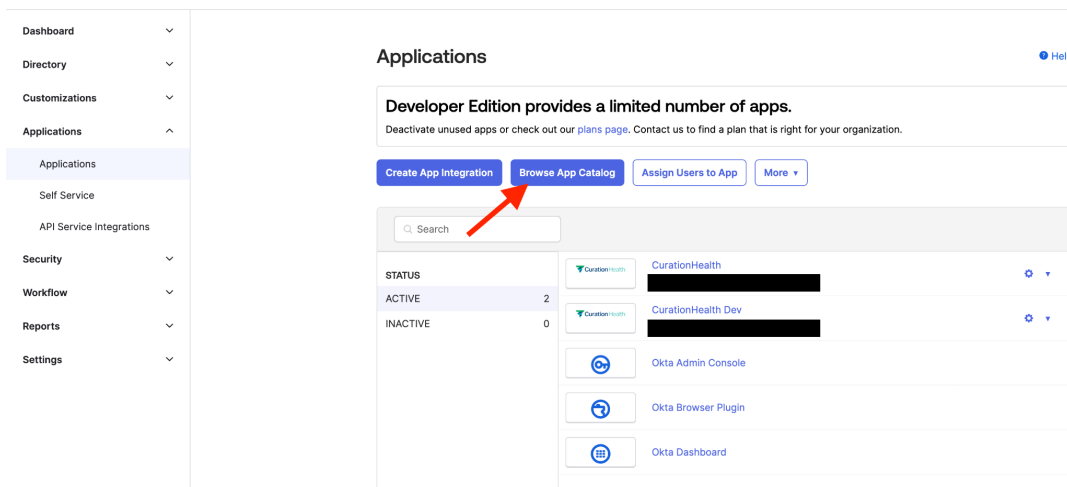
- Identity Provider (IdP)-initiated SSO (Single Sign-On via OIDC – OpenID Connect)
 - A single sign-on operation that was initiated from Okta (dashboard, plugin, etc.).
 - **Note:** We do not support JIT (just-in-time provisioning) creation of user accounts on first user login for HIPAA and protected health data reasons.

Installation:



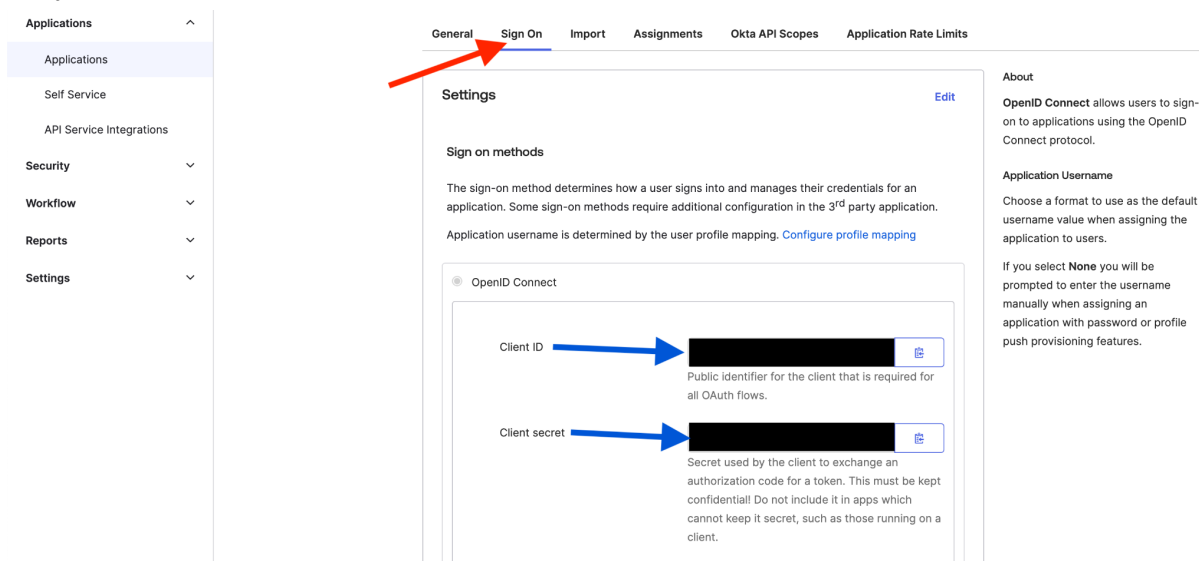
The screenshot shows the Okta Admin console interface. On the left is a sidebar with navigation links: Dashboard, Directory, Customizations, Applications, Self Service, API Service Integrations, Security, Workflow, Reports, and Settings. The 'Applications' link is highlighted in blue, and a red arrow points to it. The main content area is titled 'Applications' and includes a search bar, a 'Developer Edition provided' section, and buttons for 'Create App Integration' and 'Browse Applications'. Below these is a table showing the status of applications.

STATUS	
ACTIVE	3
INACTIVE	0

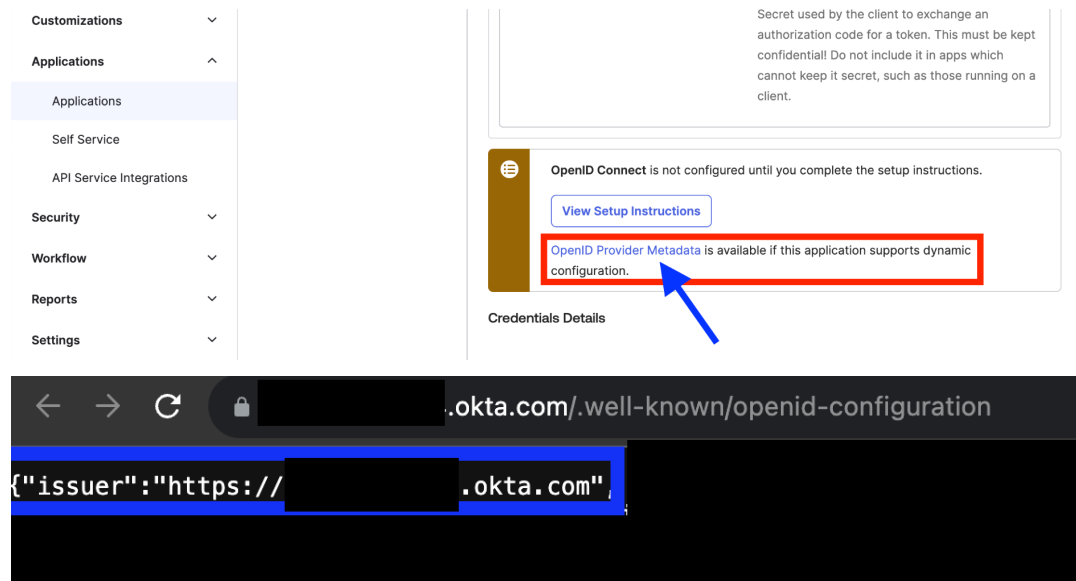


Configuration:

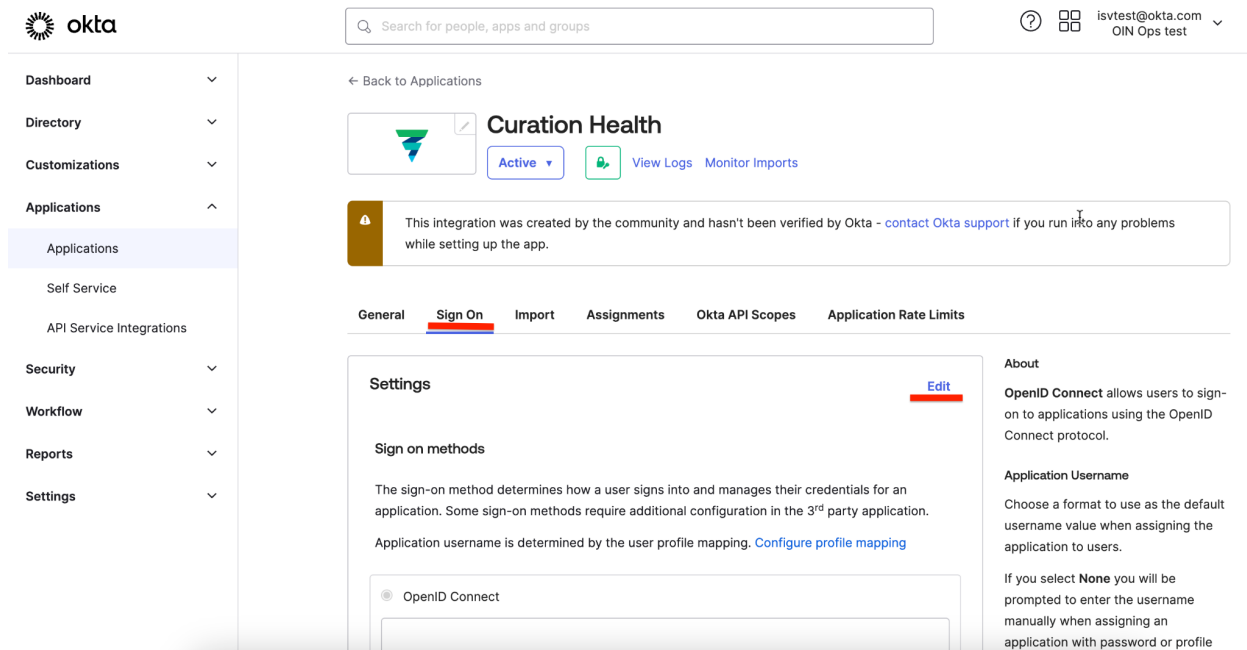
- Curation Health will need the following items from you to enable SSO:
 - *Client ID*
 - *Client Secret*
 - *Issuer base URL / Okta Domain (will look like: your_company.okta.com)*
 - *User list with Okta emails and the Curation Health application user type*
- Please gather this information and send it to your Curation Health Client Success Manager or Implementation Manager.
- Gather information from Okta:
 - In the Okta Admin Applications page, click the Curation Health application and then navigate to the *Sign On* tab.
 - Copy the values of *Client ID* and *Client Secret*.



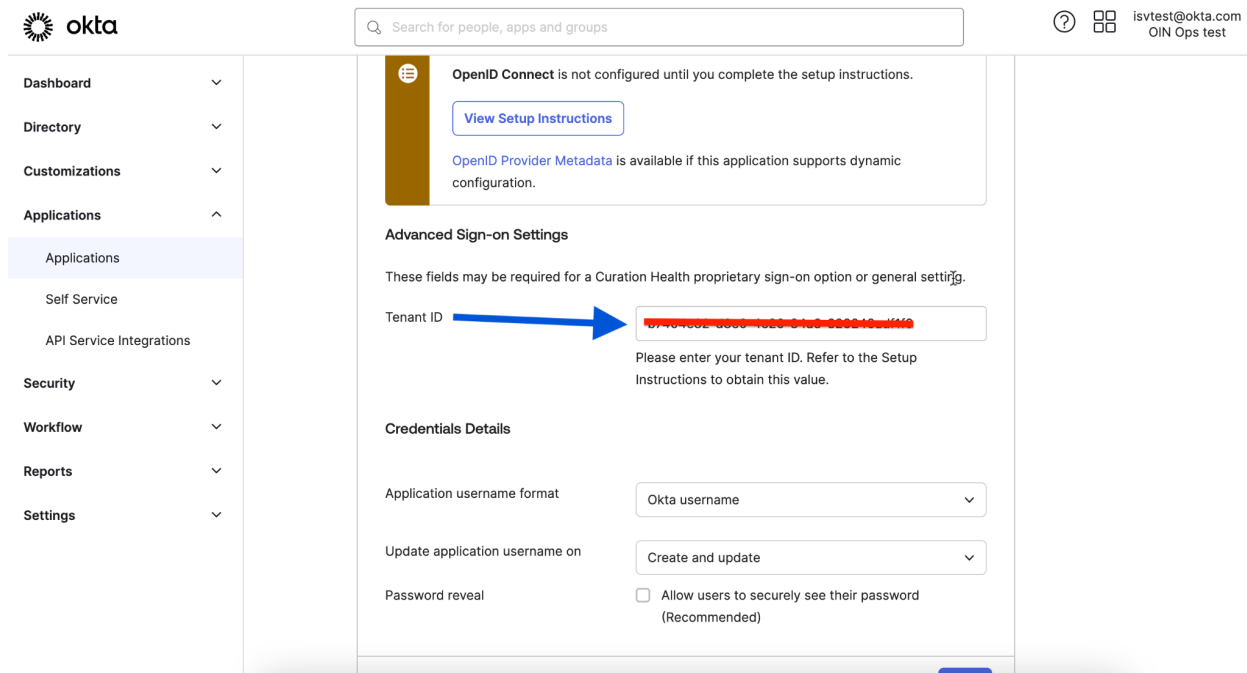
- There should be a section just below your *Client ID* and *Client Secret* that has a link titled *OpenID Provider Metadata* (the link may be in a different spot on the page than pictured below). Click this link. In the JSON document shown, look for a key titled “issuer” and copy the URL-value.



- Gather your internal user information:
 - Any users in your organization needing access to Curation Health must be sent as part of a user list containing their Okta login emails.
 - Each login email must exactly match that user's Okta email address.
 - For user registration in our application, we also need to know the type of the user whether they are a CDI, Physician, Coder, or Clinical Admin.
 - Please contact your Curation Health Client Success Manager or Implementation Manager if you need more guidance on information needed to onboard your users to our application.
- Gather information from Curation Health
 - Curation Health supports Okta SSO multi-tenancy, requiring a unique tenant variable in the Okta SSO initiation URI.
 - We will provide you with your unique tenant ID that you will need to set in the Initiate Login URI query parameter for the “tenant ID” variable.
 - Once you have obtained this tenant ID from our team at Curation Health, **you will be required to input your tenant ID** into your integration by:
 1. Going to your installed Curation Health app Integration.
 2. Under the **Sign On tab**, press **Edit**, and **Save** the changes as in the following photo examples:



Okta dashboard showing the configuration for the Curation Health application. The left sidebar lists navigation options: Dashboard, Directory, Customizations, Applications (selected), Self Service, API Service Integrations, Security, Workflow, Reports, and Settings. The main content area shows the application status as 'Active' with links for 'View Logs' and 'Monitor Imports'. A warning message states: 'This integration was created by the community and hasn't been verified by Okta - [contact Okta support](#) if you run into any problems while setting up the app.' Below this, the 'Sign On' tab is selected, showing 'Settings' for 'OpenID Connect'. The 'Sign on methods' section explains that the sign-on method determines how a user signs into and manages their credentials. The 'OpenID Connect' method is selected. On the right, the 'About' section describes OpenID Connect and provides instructions for 'Application Username'.



Okta dashboard showing the 'Advanced Sign-on Settings' for the Curation Health application. The left sidebar is the same as the previous screenshot. The main content area shows a message: 'OpenID Connect is not configured until you complete the setup instructions.' with a 'View Setup Instructions' button. Below this, the 'Advanced Sign-on Settings' section is displayed, noting that these fields may be required for a Curation Health proprietary sign-on option or general settings. The 'Tenant ID' field is highlighted with a blue arrow pointing to a redacted value. Below this, the 'Credentials Details' section includes fields for 'Application username format' (set to 'Okta username'), 'Update application username on' (set to 'Create and update'), and 'Password reveal' (unchecked, with a note 'Allow users to securely see their password (Recommended)').

- If you have questions at this stage of configuration, please contact your Curation Health Client Success Manager or Implementation Manager to provide assistance.

Service Provider (SP)-initiated SSO (Single Sign-On):

- **Caveat and restriction:** Curation Health does not support SP-initiated SSO via our UI/SPA login page. Your users must launch our app from Okta, or in a browser where they have already signed in with Okta. For example: a desktop icon or browser bookmark that is configured properly with the tenant ID URI parameter. We support the notion that a client via the tenant-configured URI can directly call our web app to initiate sign on and will then be redirected to Okta to login if they are not already logged in.