



Configuring Okta for nShift.IdentityServer

nShift

February, 2022

The following document contains details for Single Sign-On configuration of nShift.IdentityServer with Okta Identity Provider, using OpenID Connect or OIDC. Okta is a customizable, secure, and drop-in solution that can be also used to add authentication and authorization services to your applications.

Okta will be used as the centralizer for your user access to other applications.

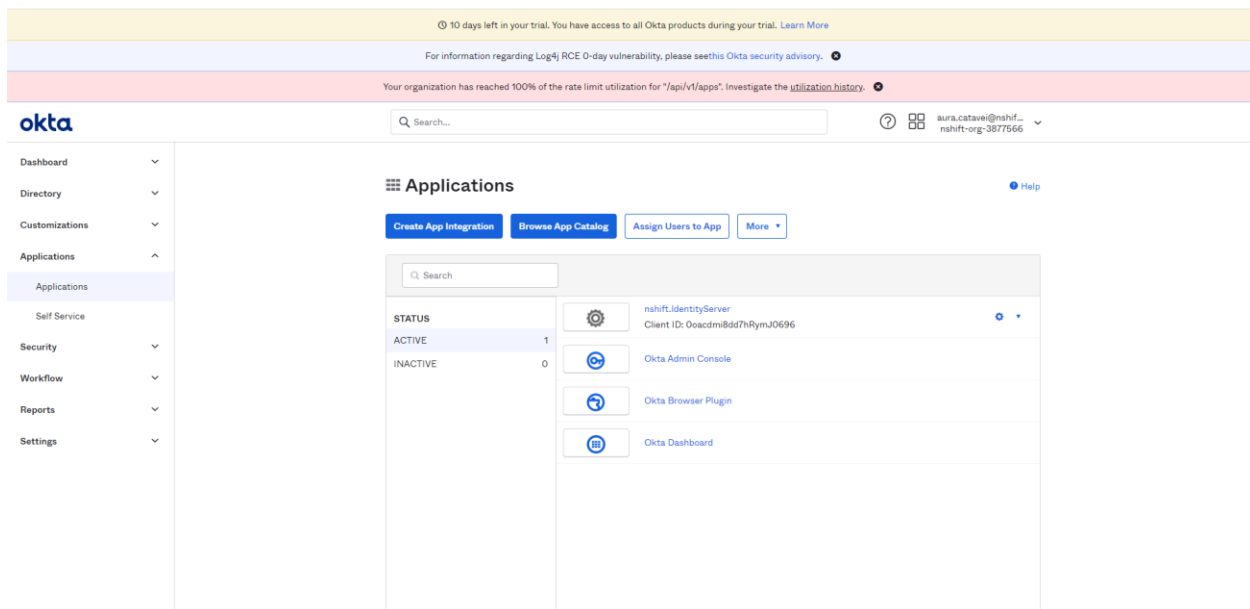
Requirements

To configure you will require a user with administrator rights in Okta. To access nShift applications the users configured in Okta for the new application will need to have the same username configured in nShift.

Step by Step Procedure

From your Okta account access the Admin area and Applications menu.

Step 1) Use Create App Integration. You will be required to setup a new oidc application as it follows



The screenshot shows the Okta Admin Console interface. At the top, there are three notification banners: a yellow one for a 10-day trial, a blue one for a Log4j RCE vulnerability advisory, and a red one for a 100% rate limit utilization warning. The main header includes the Okta logo, a search bar, and user information for 'aura.catawei@nshf...' with the organization 'nshift-org-3877566'. The left sidebar contains navigation options: Dashboard, Directory, Customizations, Applications (expanded), Self Service, Security, Workflow, Reports, and Settings. The main content area is titled 'Applications' and features buttons for 'Create App Integration', 'Browse App Catalog', 'Assign Users to App', and 'More'. Below these buttons is a search bar and a table of applications. The table has columns for 'STATUS' and a count. The 'ACTIVE' status has a count of 1, and 'INACTIVE' has a count of 0. The application list includes 'nshft.IdentityServer' (Client ID: Ooacdm8dd7hRymJO696), 'Okta Admin Console', 'Okta Browser Plugin', and 'Okta Dashboard'.

STATUS	Count
ACTIVE	1
INACTIVE	0

Application Name	Client ID
nshft.IdentityServer	Ooacdm8dd7hRymJO696
Okta Admin Console	
Okta Browser Plugin	
Okta Dashboard	

Create a new app integration



Sign-in method

[Learn More](#)

- 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

What kind of application are you trying to integrate with Okta?




Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- 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)

For the following setup the URLs for Sign-in redirect and Sign-out redirect will be provided by nShift.

General Settings

App integration name

Logo (Optional)   


Grant type [Learn More](#)

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.


Okta sends the authentication response and ID token for the user's sign-in request to these URIs



[Learn More](#) [+ Add URI](#)

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs



[+ Add URI](#)

Proceed to save the new application.

You should be able to view and edit it afterwards

Step 1)

In the General tab: Client Id and Client Secret for the application will be autogenerated. Please note down this information as it will be shared with nShift.

The screenshot shows the Okta Admin Console interface. On the left is a navigation menu with options like Dashboard, Directory, Customizations, Applications, Self Service, Security, Workflow, Reports, and Settings. The main content area is titled "nshift.IdentityServer" and has tabs for "General", "Sign On", "Assignments", and "Okta API Scopes". The "Client Credentials" tab is active, showing fields for "Client ID" (Ooacdmj8dd7hRymJO696) and "Client secret" (a masked field). There are "Edit" and "View Logs" buttons. On the right, there is a "Ready to code" section with a "Download sample app" button and a link to the "Okta Developer's guide".

Step 2)

Please make sure you have selected Authorization Code

The screenshot shows the Okta Admin Console interface, specifically the "General Settings" tab for the application "nshift.IdentityServer". The "Okta domain" is set to "nshift.okta.com". Under the "APPLICATION" section, the "App integration name" is "nshift.IdentityServer" and the "Application type" is "Web". The "Grant type" section shows "Client acting on behalf of a user" selected, with "Authorization Code" checked. Other options like "Interaction Code", "Refresh Token", and "Implicit (hybrid)" are unchecked. Under the "USER CONSENT" section, "Require consent" is checked. There are "Edit" and "View Logs" buttons.

Step 3)

The URLs for Sign-in redirect and Sign-out redirect will be provided by nShift.

The screenshot shows the Okta Admin Console interface. On the left is a navigation menu with categories like Dashboard, Directory, Customizations, Applications, Self Service, Security, Workflow, Reports, and Settings. The 'Applications' section is expanded, and the 'Applications' sub-item is selected. The main content area displays configuration for a specific application, divided into two sections: 'USER CONSENT' and 'LOGIN'. Under 'USER CONSENT', there is a 'Require consent' checkbox which is checked. Below it are fields for 'Terms of Service URI', 'Policy URI', and 'Logo URI'. The 'LOGIN' section includes 'Sign-in redirect URIs' with a checkbox for 'Allow wildcard * in login URI redirect' (unchecked) and a text field containing 'https://localhost:7000/okta-callback'. Below that is 'Sign-out redirect URIs' with a text field containing 'https://localhost:7000/okta-signout'. At the bottom, 'Login initiated by' is set to 'App Only' and 'Initiate login URI' is also present. The footer contains copyright information for Okta, Inc. and various links like Privacy, Version 2022.01.1 E, OK14 US Cell, Status site, Download Okta Plugin, and Feedback.

Step 4) Sign In method should be OpenID Connect

The screenshot shows the Okta Admin Console interface for configuring the 'Sign On' method for an application named 'nshift.IdentityServer'. The left navigation menu is the same as in the previous screenshot. The main content area shows the application's status as 'Active' and provides a 'View Logs' link. Below this, there are tabs for 'General', 'Sign On', 'Assignments', and 'Okta API Scopes', with 'Sign On' being the active tab. The 'Settings' section is expanded, showing 'Sign on methods'. A text box contains 'OpenID Connect'. Below this, the 'Token Credentials' section is visible, showing 'Signing credential rotation' set to 'Automatic'. An 'About' section on the right explains that 'OpenID Connect allows users to sign-on to applications using the OpenID Connect protocol.' The footer is consistent with the previous screenshot.

okta

Q Search...

aura.catavei@nshif... nshif-org-3877566

- Dashboard
- Directory
- Customizations
- Applications
 - Applications
 - Self Service
- Security
- Workflow
- Reports
- Settings

Token Credentials

Signing credential rotation: Automatic

OpenID Connect ID Token

Issuer: Dynamic (based on request domain)

Audience: Ooacdm8dd7hRymJO696

Claims: Claims for this token include all user attributes on the app profile.

Groups claim type: Filter

Groups claim filter: None [Using Groups Claim](#)

Sign On Policy

[Add Rule](#)

A sign on policy is a set of rules that determine how users access this application. For example, you can deny access when a specific group of users is off network.

1	Catch-all Rule	ENABLED
---	----------------	---------

Step 5) Catch-all Rule will be setup as in the image below.

okta

Q Search...

aura.catavei@nshif... nshif-org-3877566

- Dashboard
- Directory
- Customizations
- Applications
 - Applications
 - Self Service
- Security
- Workflow
- Reports
- Settings

Sign On Policy

[Add Rule](#)

A sign on policy is a set of rules that determine how users access this application. For example, you can deny access when a specific group of users is off network.

1	Catch-all Rule	ENABLED
---	----------------	---------

IF

- User type: Any
- Group: Any
- User is: Any
- Zone: Any
- Device: Any
- Platform: Any

THEN

Access: Allowed after successful authentication

User must authenticate with: Password

Available Authenticators: Password

© 2022 Okta, Inc. Privacy Version 2022.01.1 E OK14 US Call Status site Download Okta Plugin Feedback


Step 6) Next you will be required to configure the okta users who will be able to access nShift through the okta identity provider.

Important Note: We keep as a standard that the okta configured user name(ex: from image aura@nshift.com) will also be the user name configured in nShift

The screenshot shows the Okta Admin Console interface. On the left is a navigation menu with options like Dashboard, Directory, Customizations, Applications, Self Service, Security, Workflow, Reports, and Settings. The main content area is titled 'nshift.IdentityServer' and has tabs for General, Sign On, Assignments, and Okta API Scopes. The 'Assignments' tab is selected, showing a table with columns for Filters, Person, and Type. The table lists two groups: 'aura@nshift.com' and 'Aura TUdor', both of type 'Group'. There are also buttons for 'Assign', 'Convert assignments', and 'People'. On the right side, there are sections for 'REPORTS' (Current Assignments, Recent Unassignments) and 'SELF SERVICE' (Requests: Disabled, Approval: -).

Please note that nShift also requires configuration for communicating with the Okta provider.

After a successful configuration on the Okta as well as on nShift IdentityServer, accessing the nShift application will redirect you to the Okta login page.

Connecting to 
Sign-in with your nshift-org-3877566 account to access
nshift.IdentityServer

okta

Sign In

Username

Password

Keep me signed in

[Forgot password?](#)
[Help](#)