

McKesson – Data Insights Runbook

**Version**: 1.0

**Last Updated**: July 19, 2022

Table of Contents

[1. Background 3](#_Toc109315127)

[1.1 Application Overview 3](#_Toc109315128)

[1.2 Application Team Details 3](#_Toc109315129)

[2. Prerequisites 4](#_Toc109315130)

[3. Directory 5](#_Toc109315131)

[3.1 Groups 5](#_Toc109315132)

[3.2 Profile Editor 6](#_Toc109315133)

[3.3 Profile Sources 18](#_Toc109315134)

[4. Applications 19](#_Toc109315135)

[4.1 Applications 19](#_Toc109315136)

[5. Security 24](#_Toc109315137)

[5.1 Authenticators 24](#_Toc109315138)

[5.2 Authentication policies 27](#_Toc109315139)

[5.3 Global Session Policy 28](#_Toc109315140)

[5.4 Identity Provider 30](#_Toc109315141)

[5.5 API 38](#_Toc109315142)

[6. Functional Diagram & Flow 45](#_Toc109315143)

[6.1 Flow Diagram 45](#_Toc109315144)

[6.2 Process Flow 45](#_Toc109315145)

[7. Logging 47](#_Toc109315146)

[7.1 System Logs 47](#_Toc109315147)

[8. Test Login 48](#_Toc109315148)

[9. Common Error/Issues: 50](#_Toc109315149)

# Background

This runbook has been created to use as a reference guide to complete the application integration in higher environment.

## Application Overview

DataInsight application is reporting and analytic tool for EnterpriseRX application. It has two components front-end and back-end. Front-end part takes care of user login while back-end contains all application functionality related to reports and analytics.

## Application Team Details

|  |  |  |
| --- | --- | --- |
| **Role** | **Name** | **Email** |
| BU Owner | MPS | NA |
| Business Owner | Amber Miner | amber.miner@mckesson.com |
| Product/Application Owner | Brad Miller | brad.miller@mckesson.com |
| Technical POC | Pat Stromberg Katie Koslosky | pat.stromberg@mckesson.com katie.koslosky@mckesson.com |
| Application DL | NA | NA |
| 3rd Party technical Contact | NA | NA |

# Prerequisites

In order to proceed through this runbook, the following activities need to be completed and information/access acquired in order to have a successful implementation through the runbook.

|  |  |
| --- | --- |
| **Activity** | **Reason** |
| Super Admin  credentials | Org2Org Admin group push should be enabled and integrated to B2E for a centralized access control of tenant administration. Super admin requires to do all Org2Org setup. |
| Okta API Token | API tokens are generated with the permissions of the user that created the token. On the Okta B2B tenant, super admin required to create API token to use for Org2Org provisioning |
| Data Insights Application Endpoints | Callback/Redirect URL and signout URL is required to integrate with Okta |
| External (Customer’s) IDP SAML Metadata | External IDP details required to integrated with Okta for external user’s federated login |

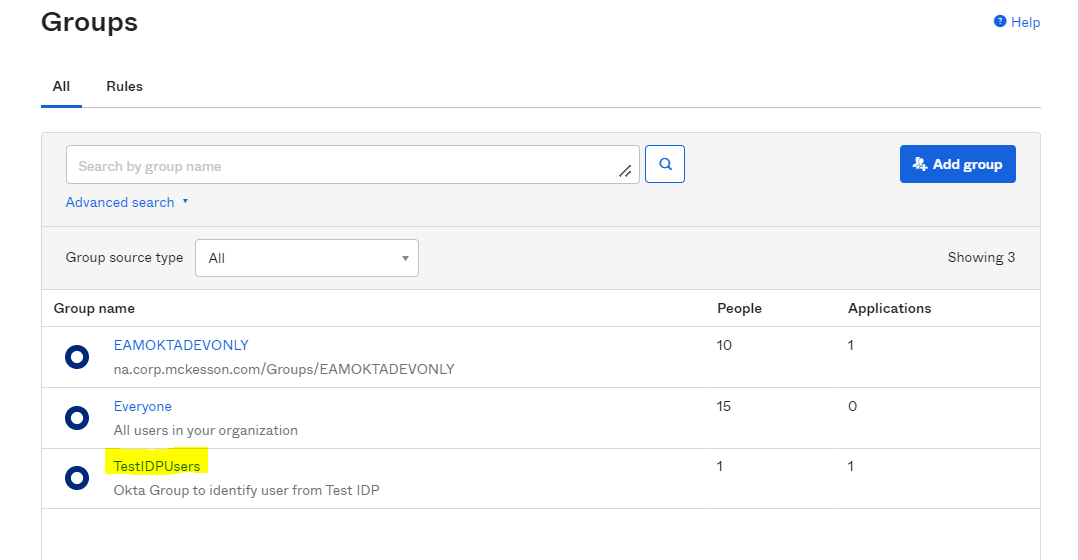
Fill out the following based on environment deployment:

|  |  |  |  |
| --- | --- | --- | --- |
| **Application** | **Dev** | **UAT** | **Prod** |
| Okta | https://rxservices.oktapreview.com | https://rxservices-uat.okta.com/ | https://rxservices.okta.com/ |
| Data Insights | https://dev-reporting.rxservices.mckesson.com | https://uat-reporting.rxservices.mckesson.com | https://reporting.rxservices.mckesson.com |

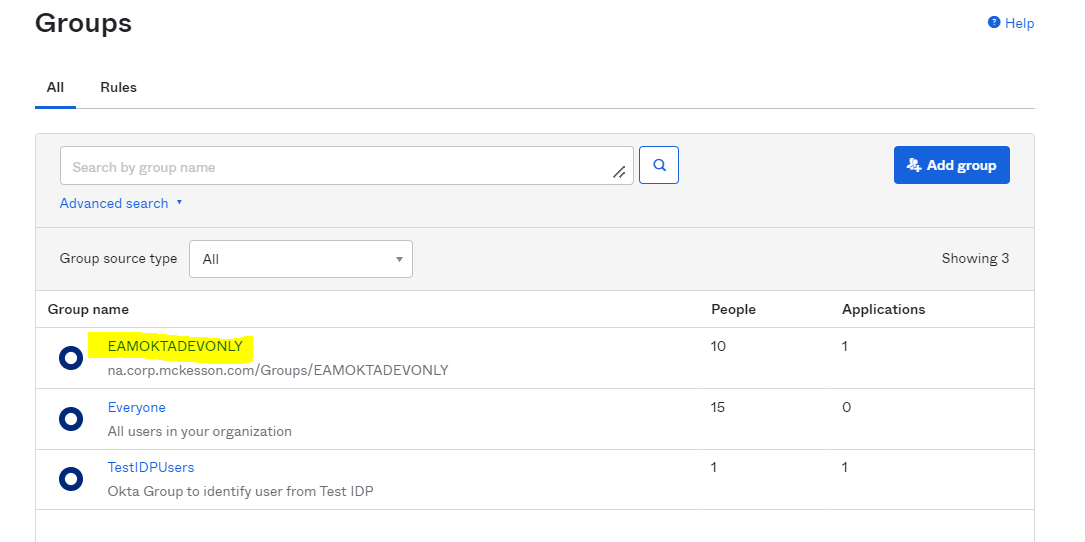
# Directory

## Groups

1. Create groups (relevant to external IDP name) to store users form different IDP sources. These groups will be assigned for application access.



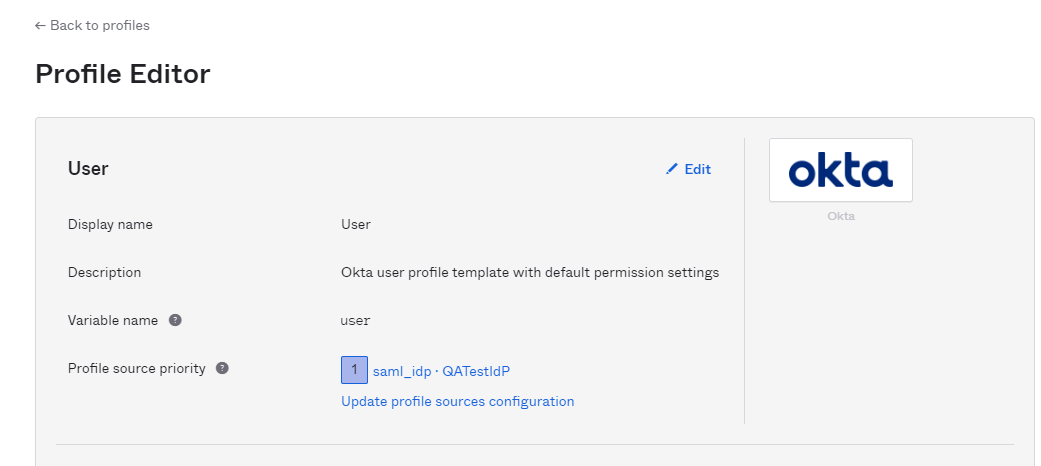
2. Admin group pushed from Okta B2E tenant

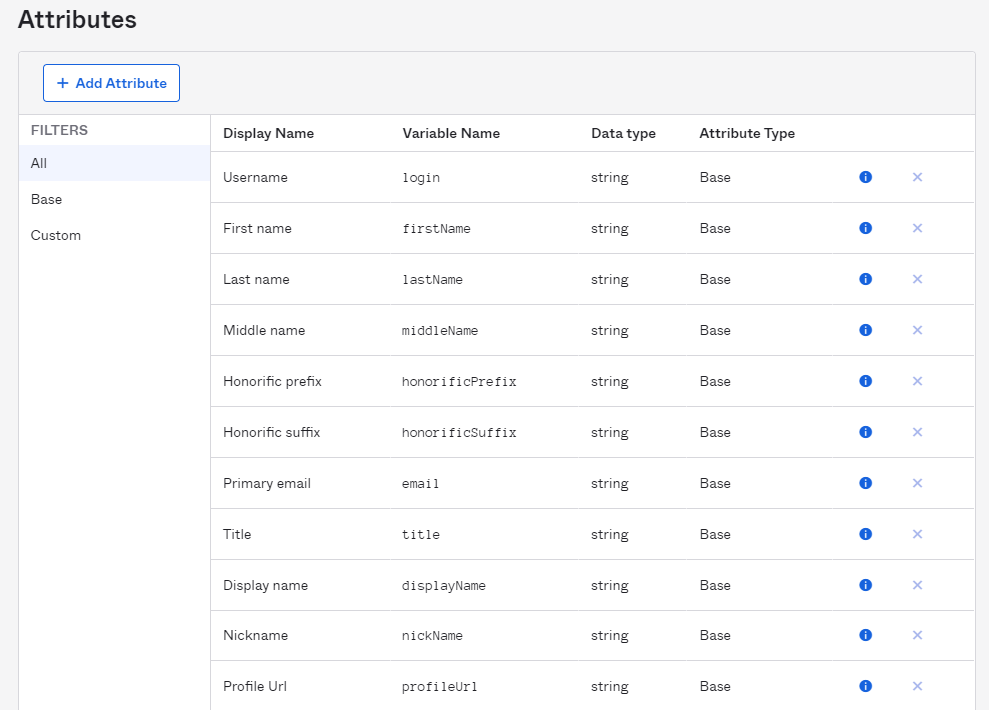


## Profile Editor

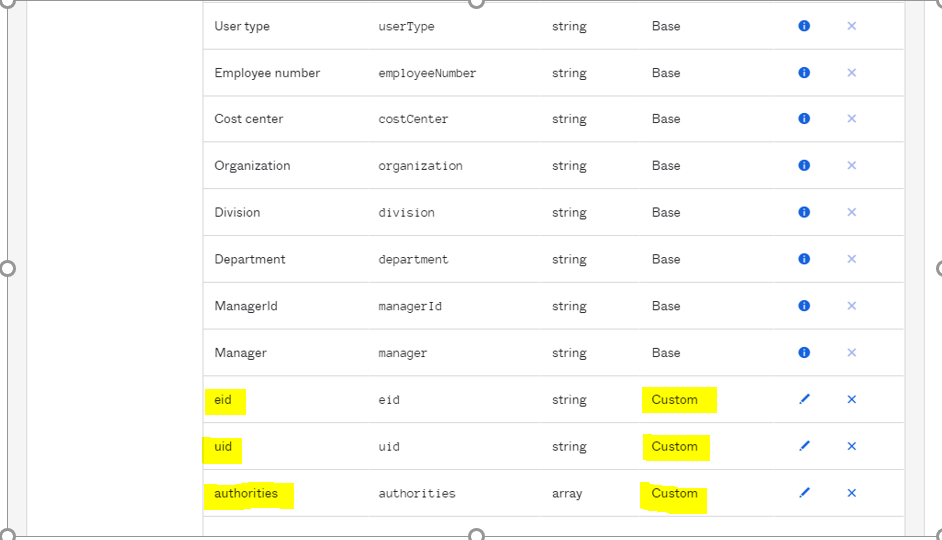
### User (Default)

Three custom attributes (eid, uid, authorities) have been added.

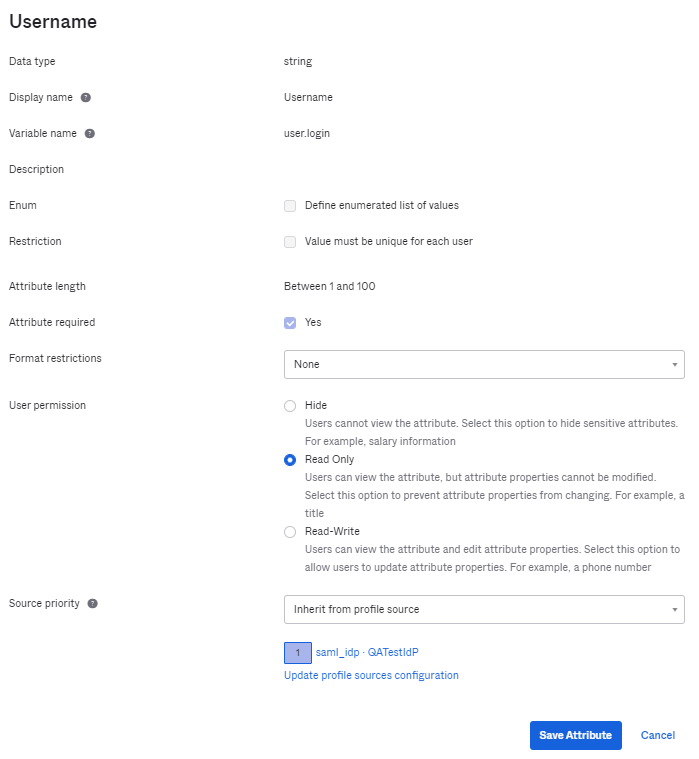




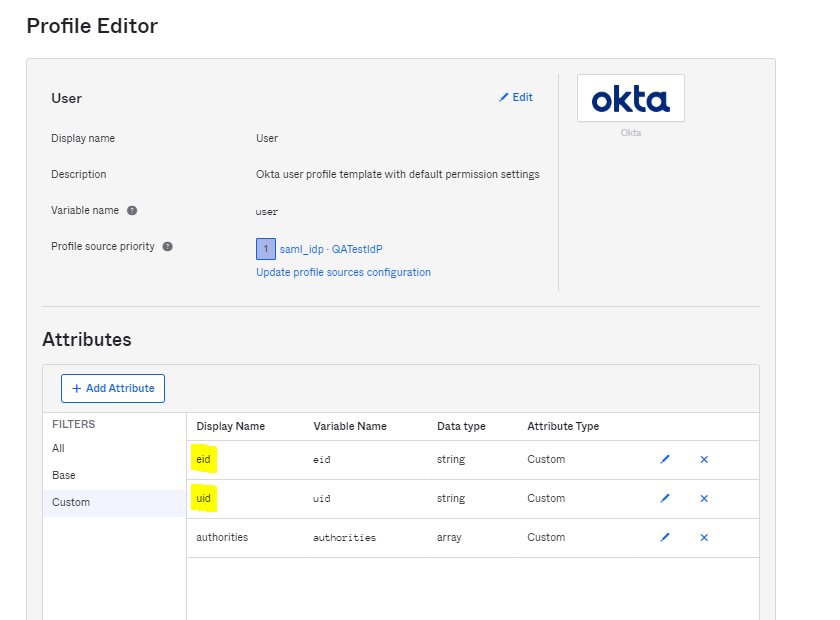


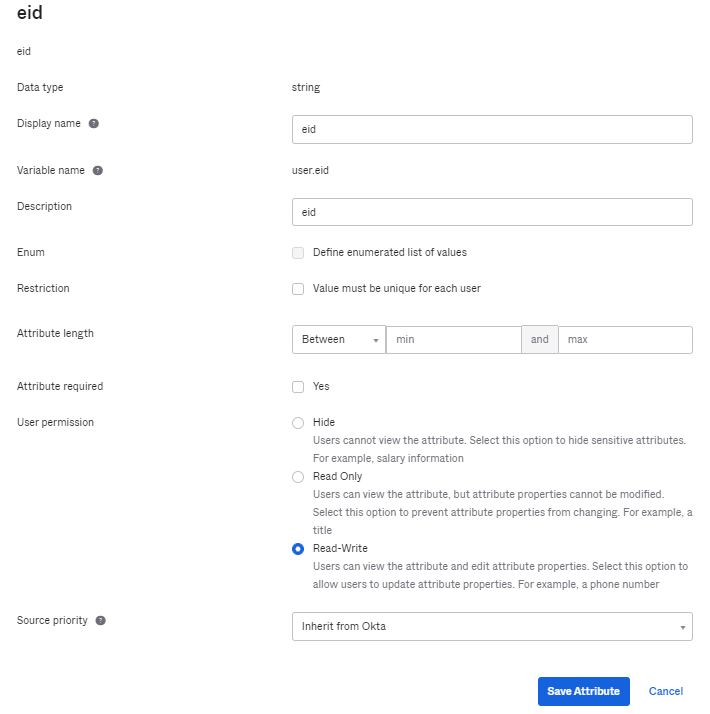


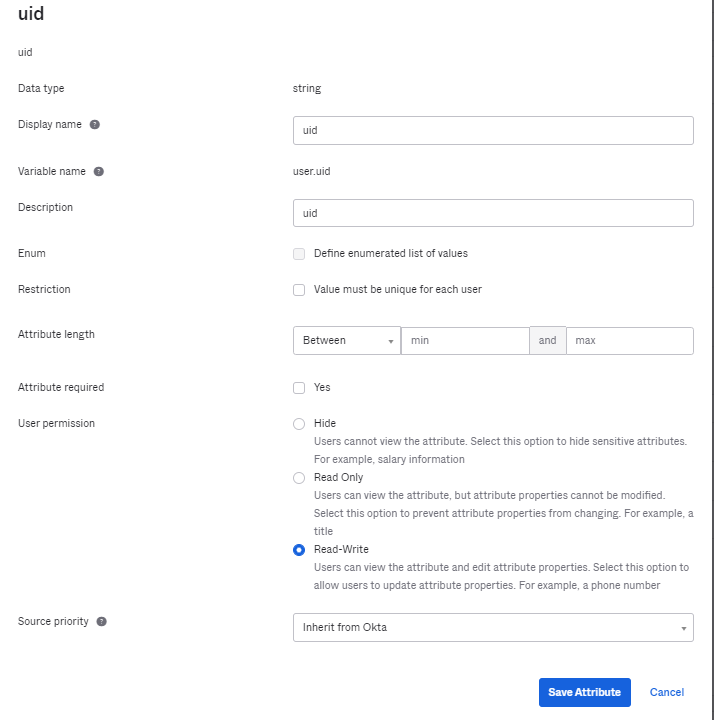
Update user login format from email format- since users from external IDP can have either email format or user login format



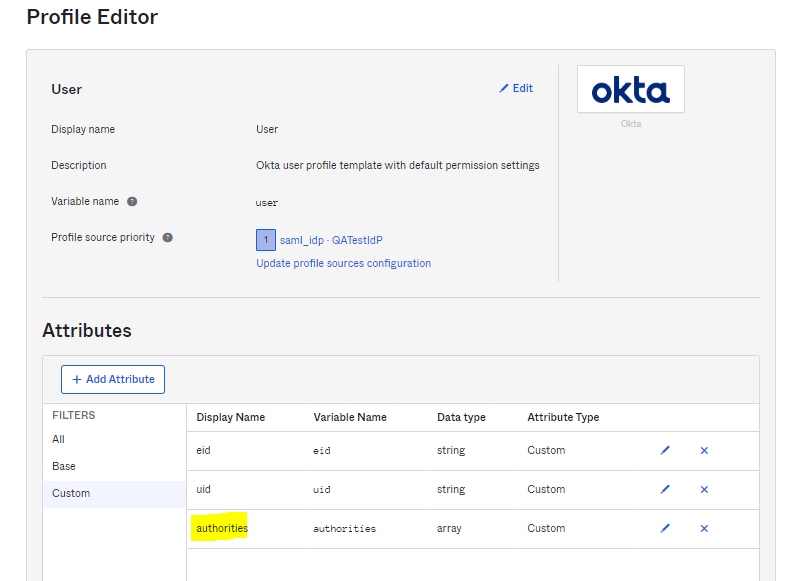
Create custom attribute in Okta User (default) profile for Org2Org admin setup- eid and uid

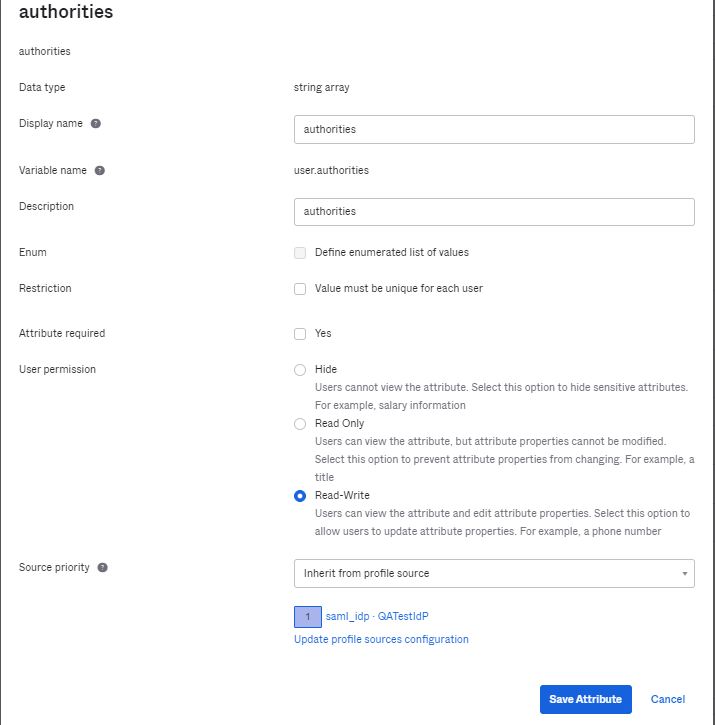






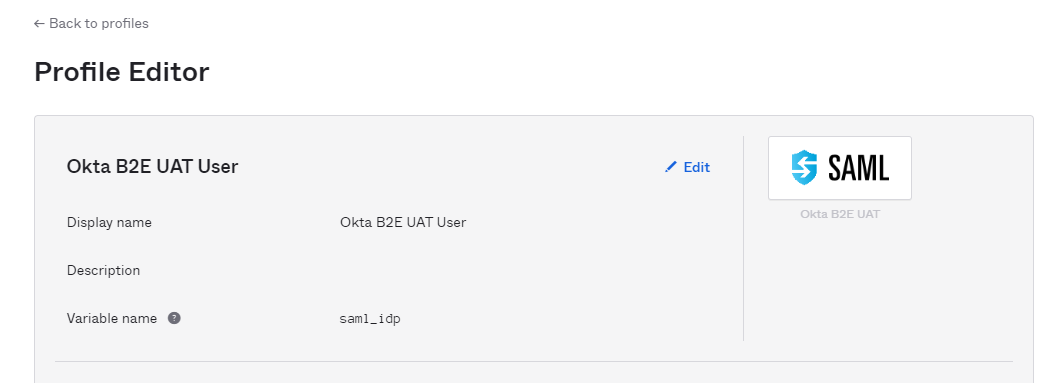
Create custom attribute (authorities) in Okta User (default) profile to store user’s roles coming from external IDP

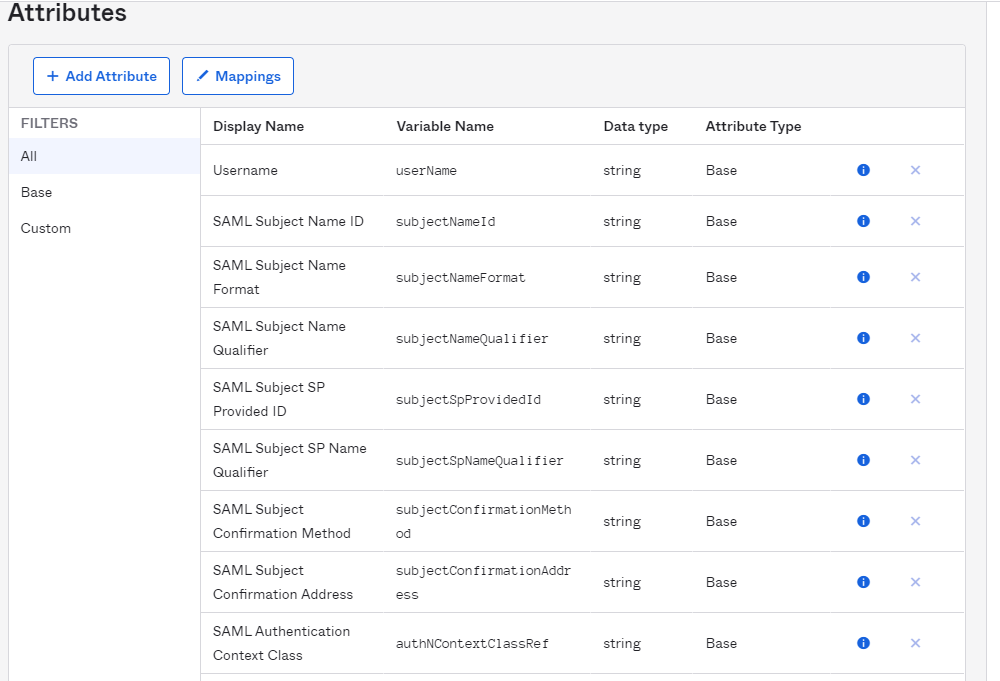


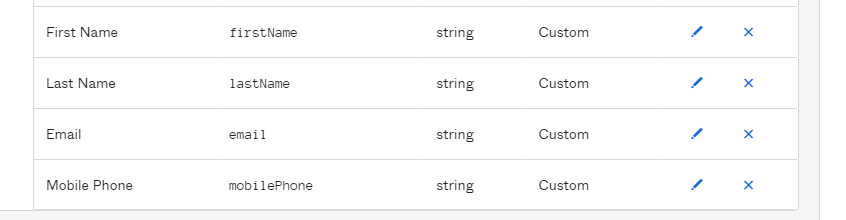


### [Okta B2E UAT User](https://rxservices-admin.oktapreview.com/admin/universaldirectory)

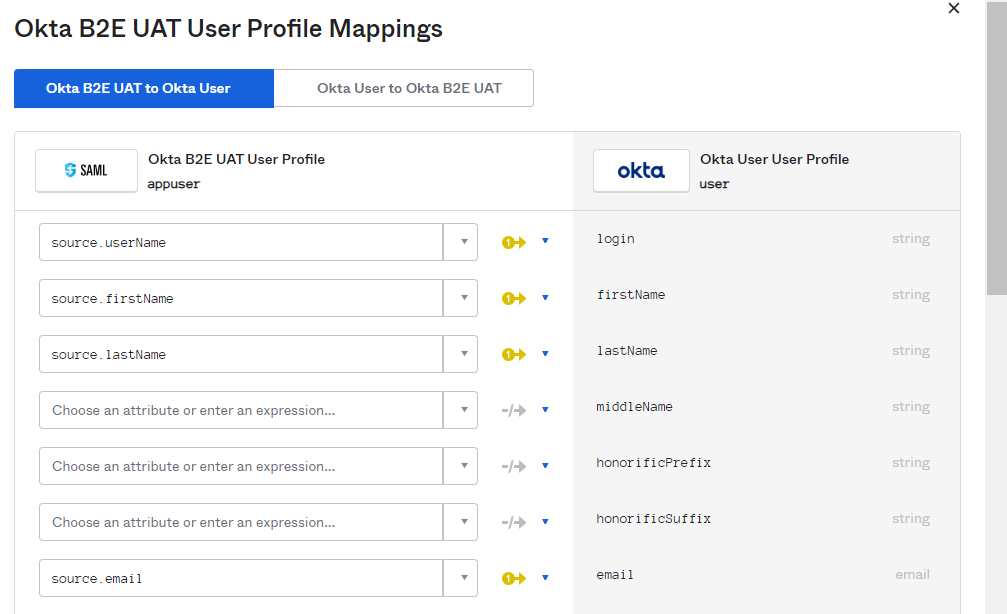
#### Profile

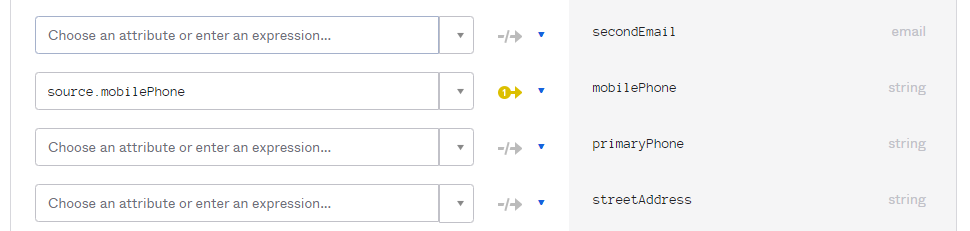






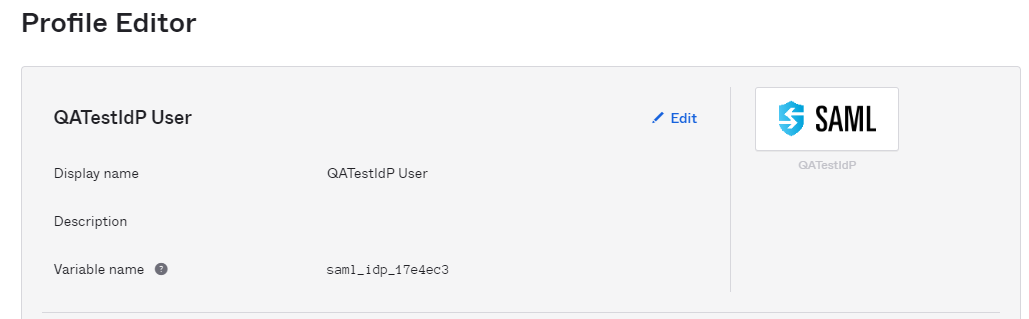
#### Mapping

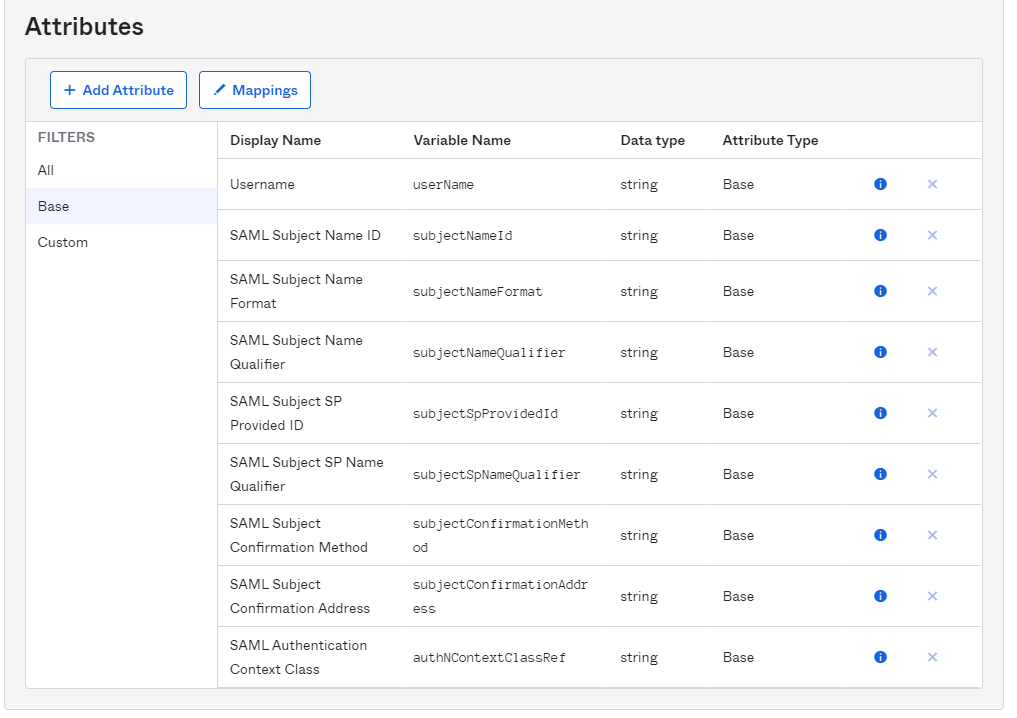


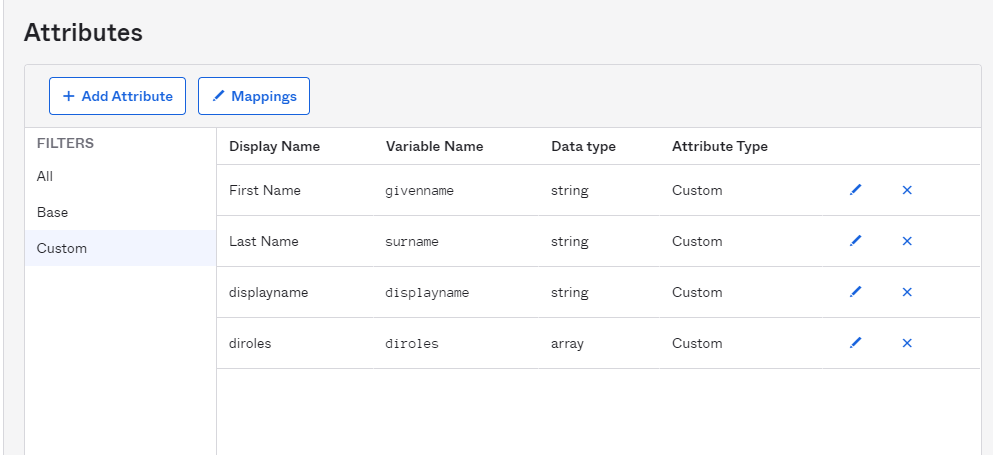


### [QATestIdP User](https://rxservices-admin.oktapreview.com/admin/universaldirectory)

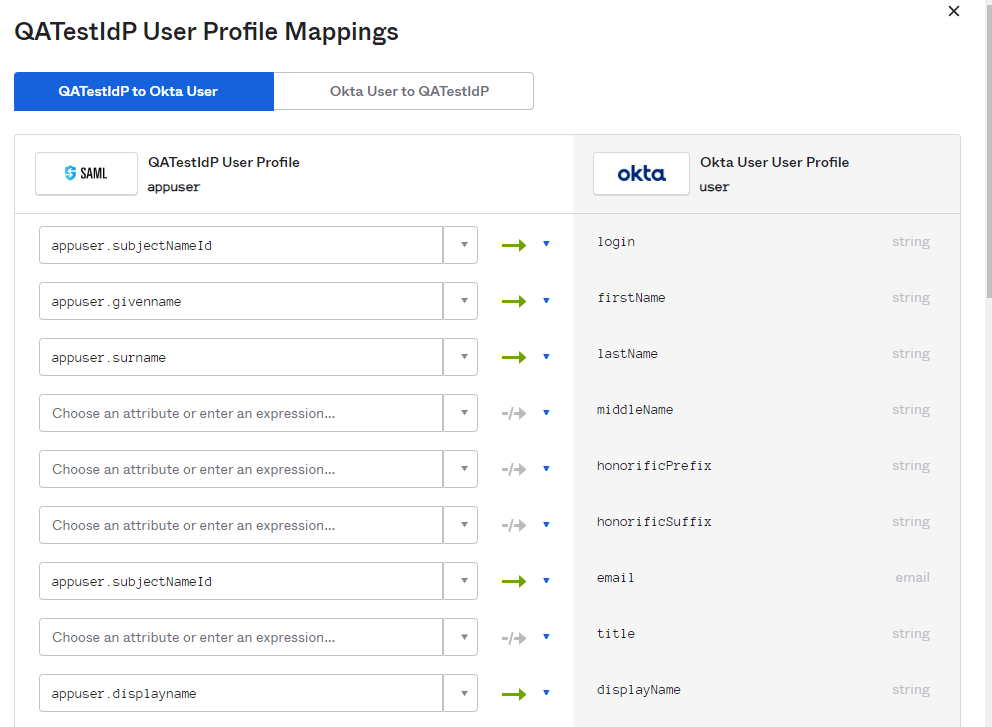
#### Profile







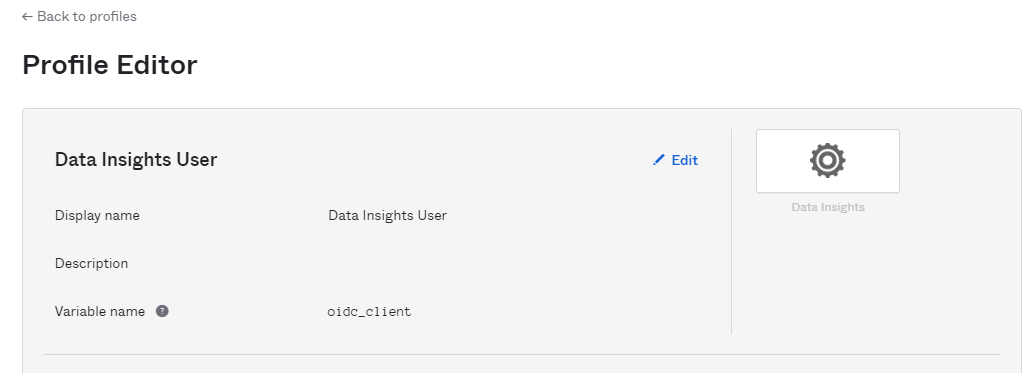
#### Mapping

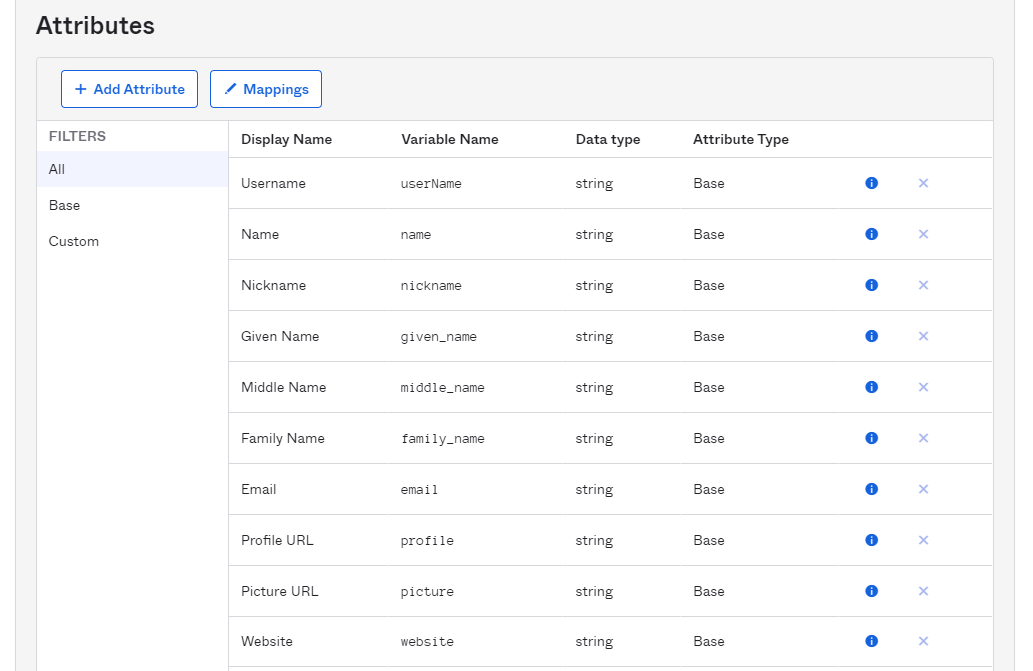


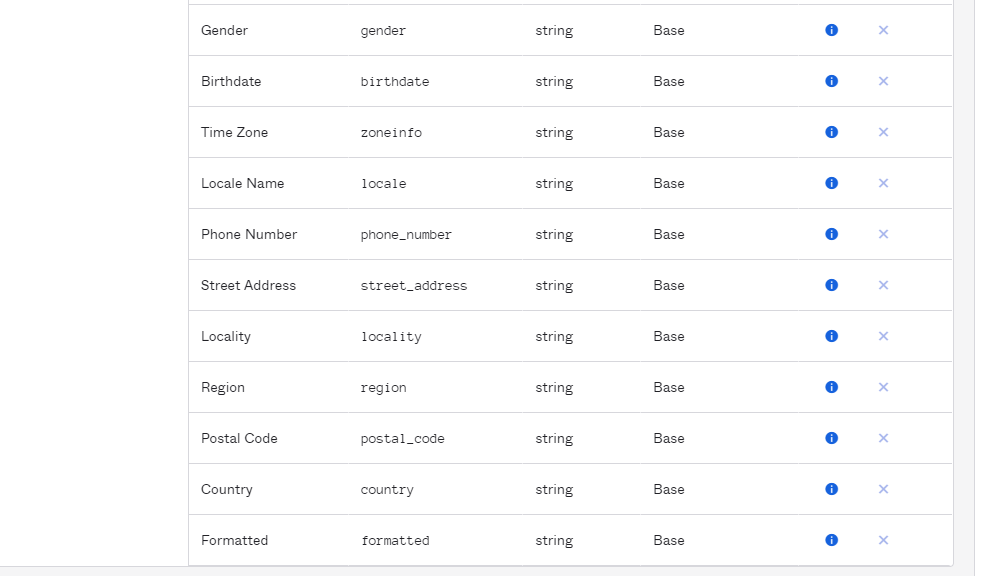


### [Data Insights User](https://rxservices-admin.oktapreview.com/admin/universaldirectory)

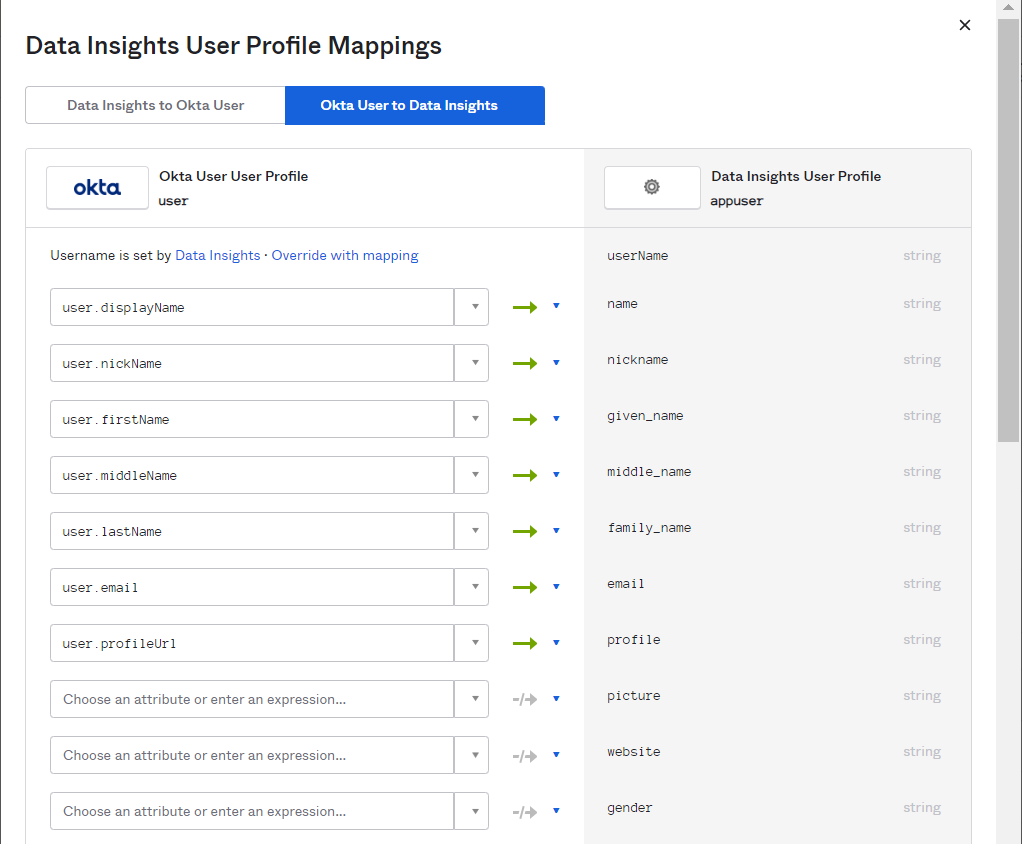
#### Profile

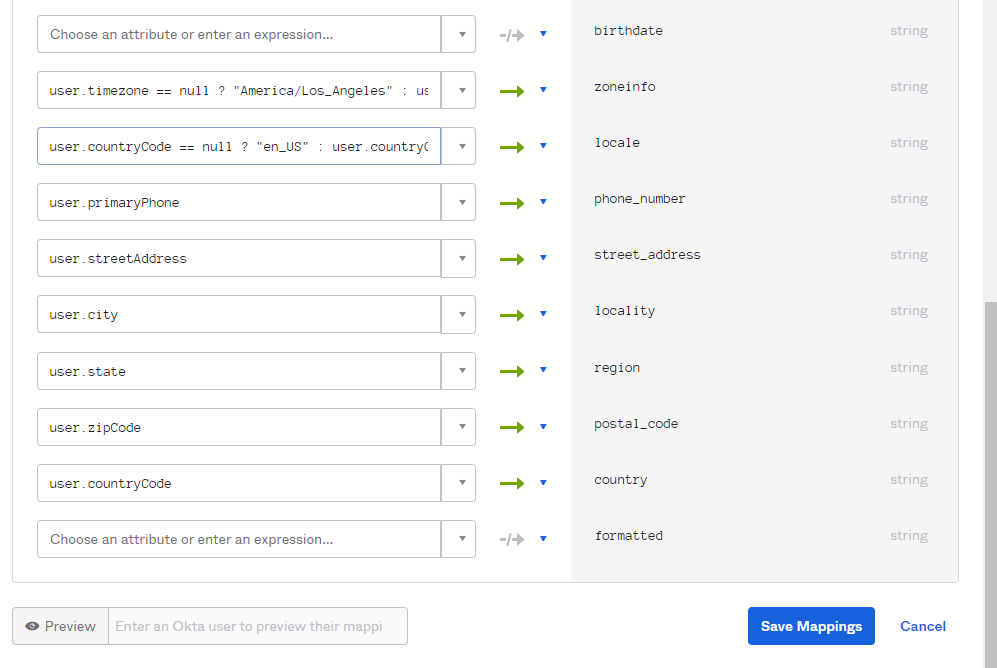




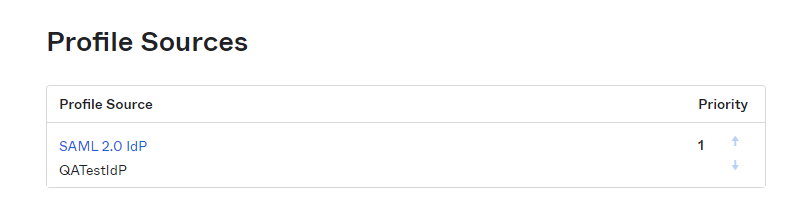


#### Mapping



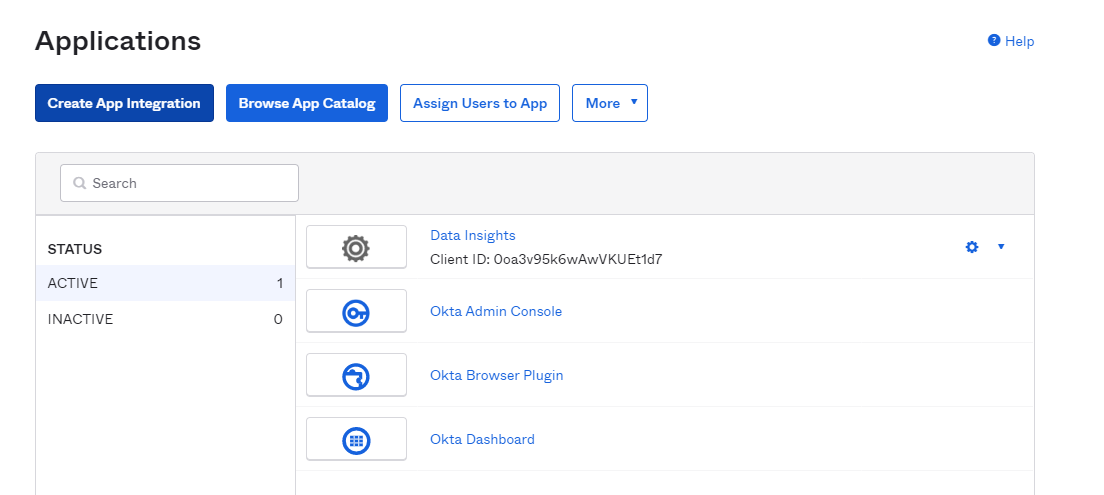


## Profile Sources

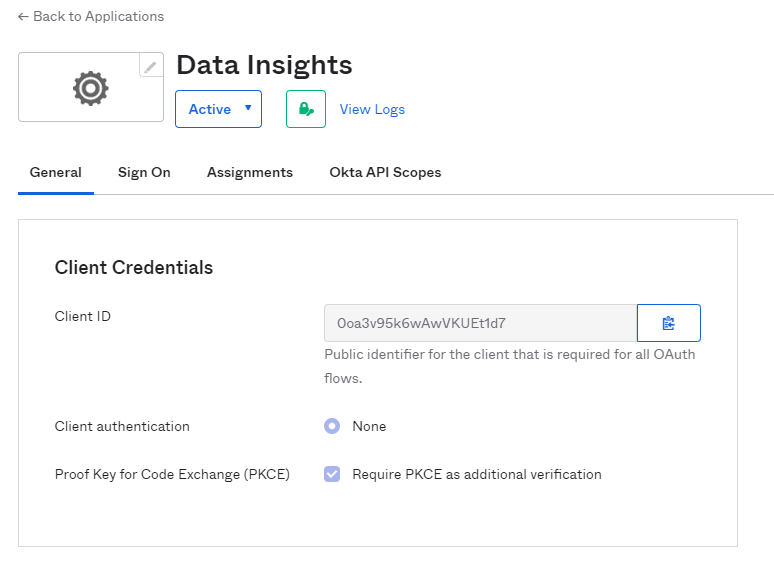


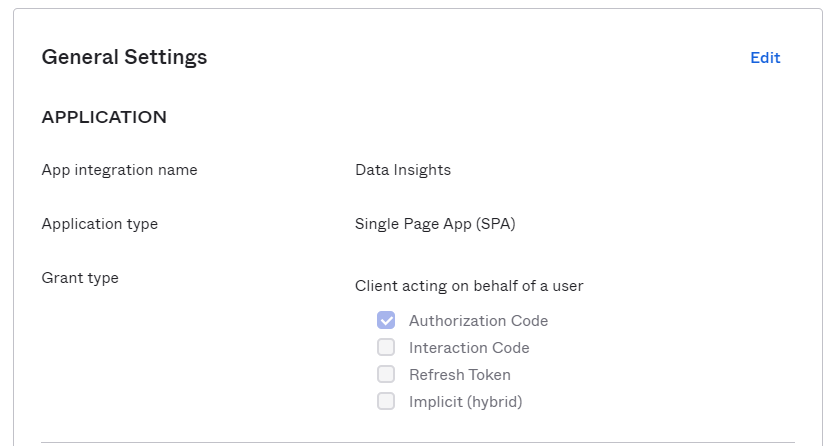
# Applications

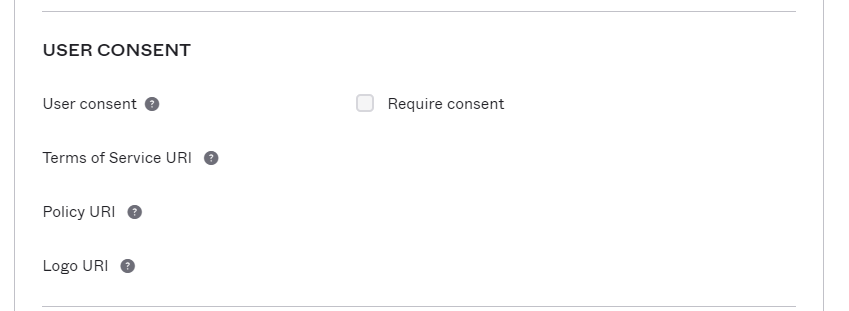
## Applications

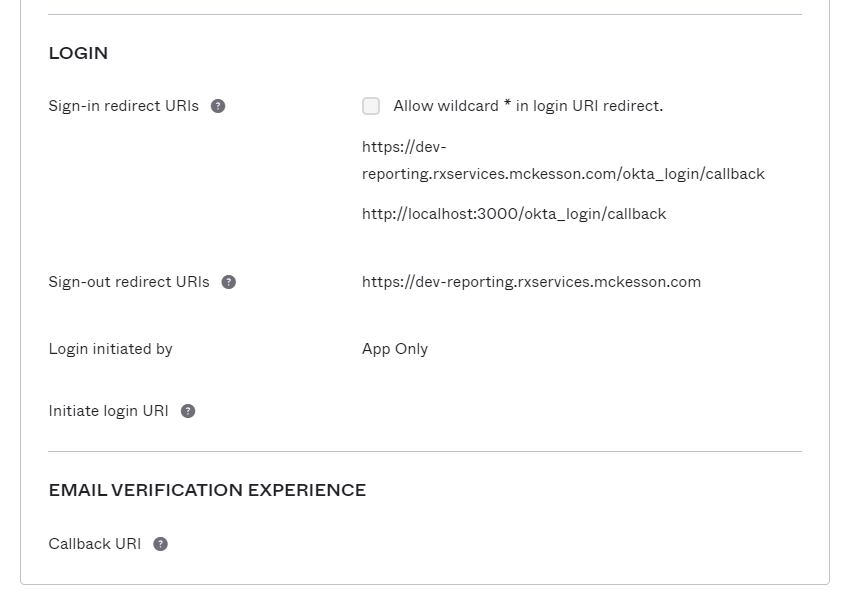


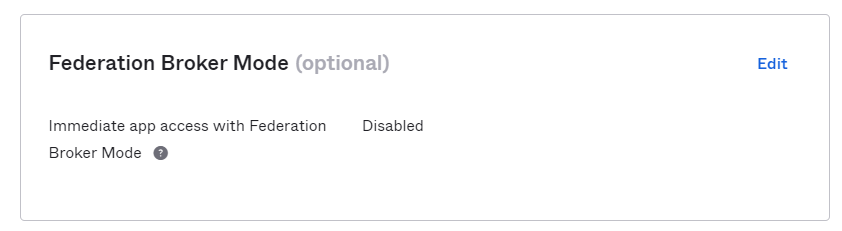
### General



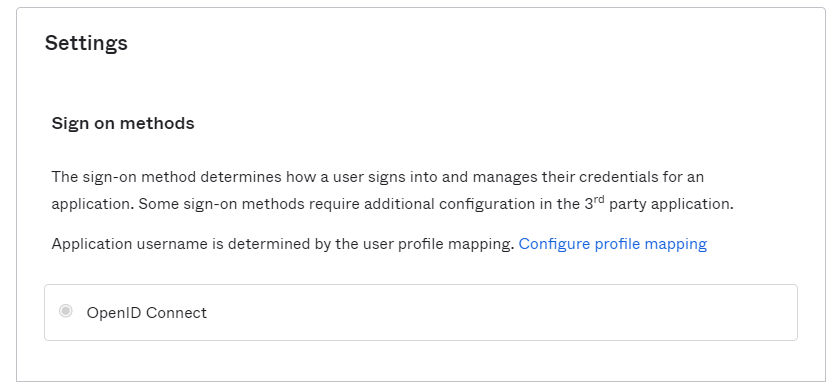


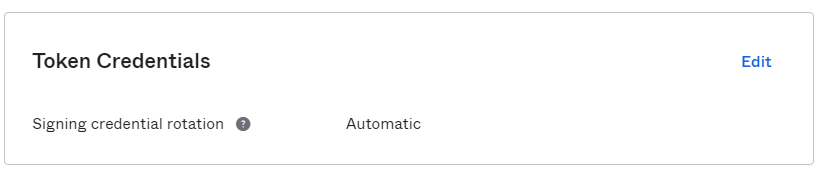


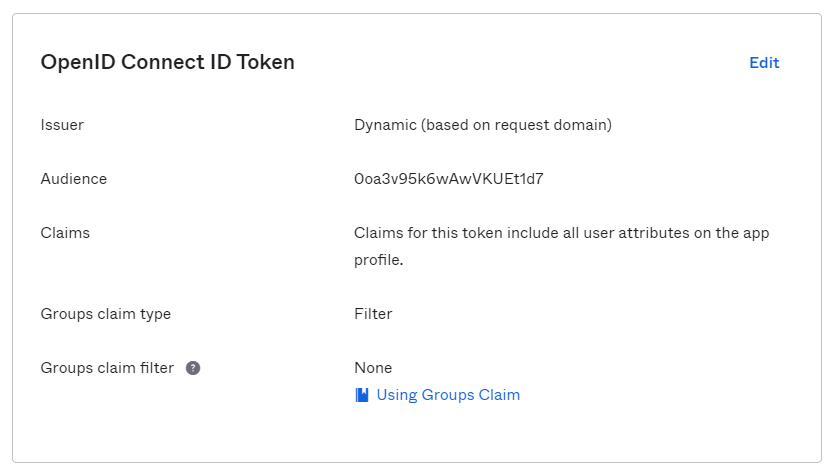


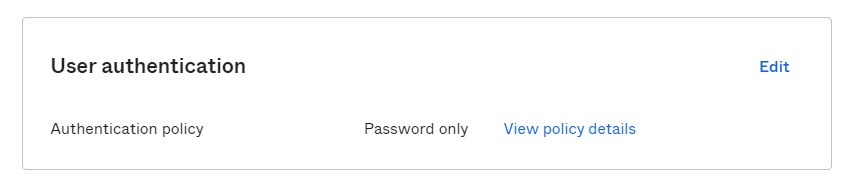


### SignOn

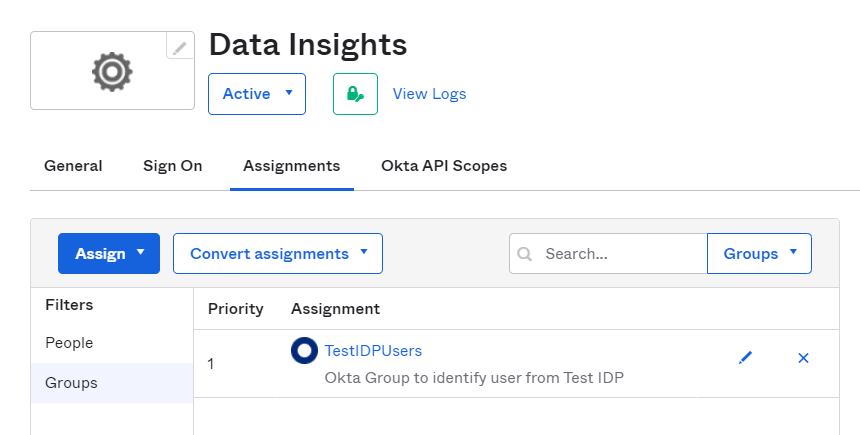








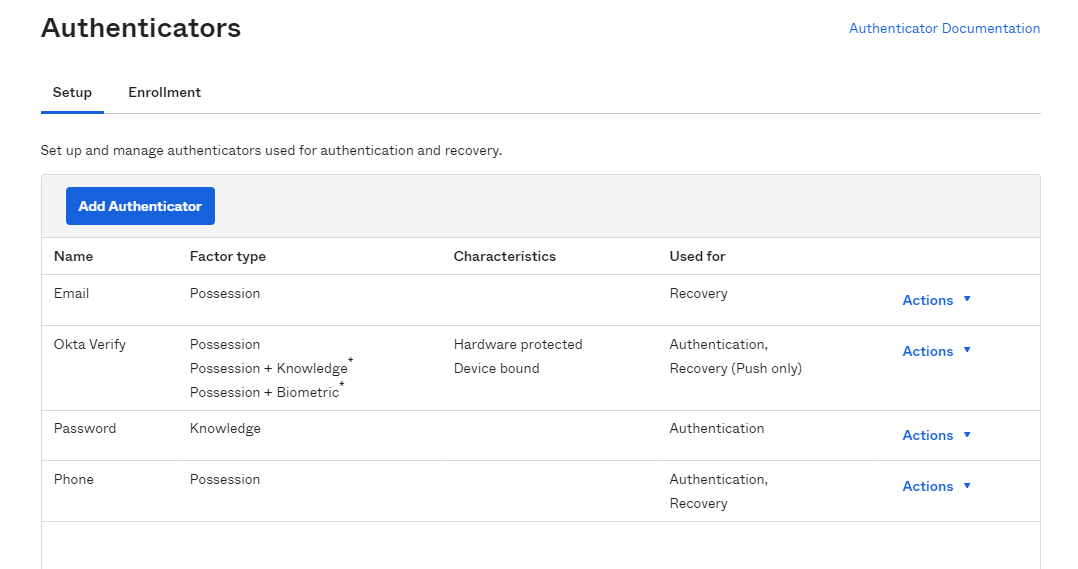
### Assignments



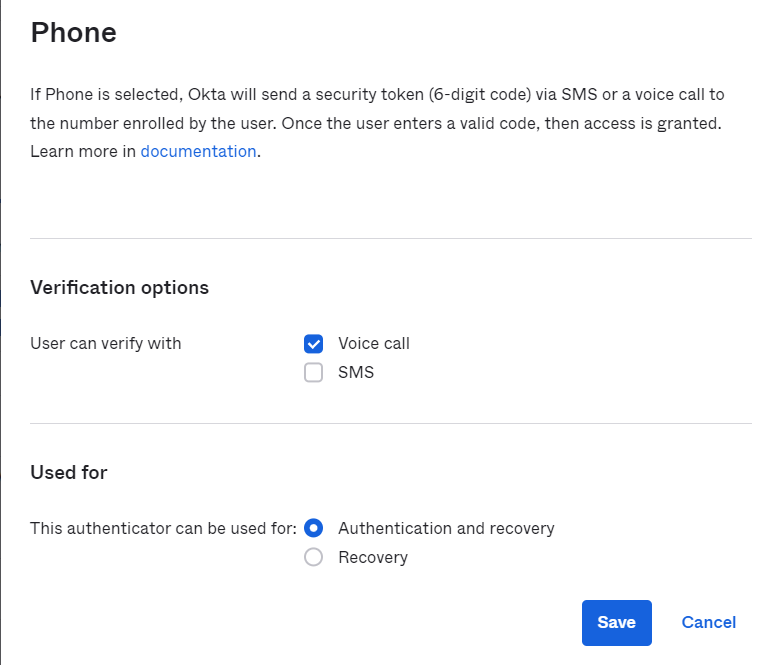
# Security

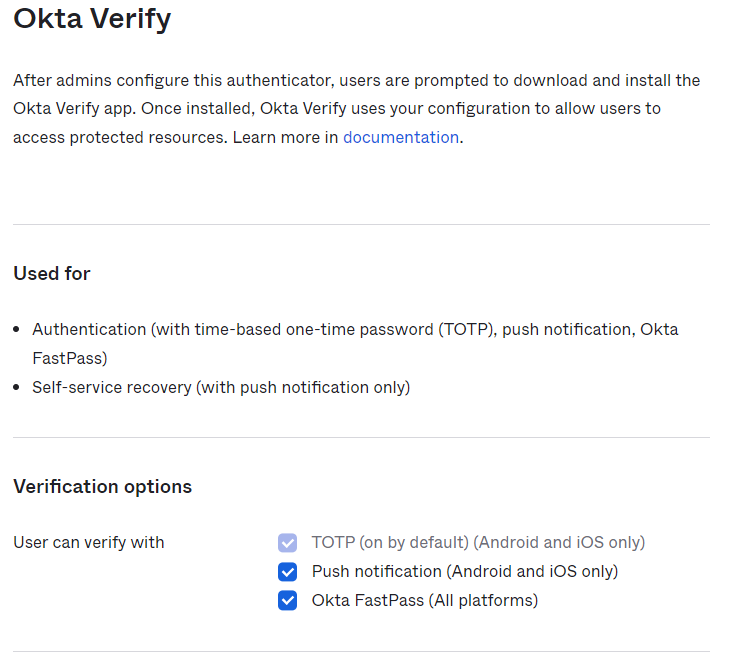
Please refer the McKesson Password & MFA Policy here: [McKesson Password & MFA Policy Data Insights .docx](https://mckessoncorp.sharepoint.com/:w:/r/sites/GRPMcKIAM-OktaIntegration/Shared%20Documents/Jira%20High%20Priority%20Tickets/02%20Erx%20DataInsight/03%20Implementation%20and%20Unit%20Test%20Phase/Okta%20Runbook/McKesson%20Password%20%26%20MFA%20Policy%20Data%20Insights%20.docx?d=w5d6087af4fc64a799cf7564374b18cad&csf=1&web=1&e=ztRFOX)

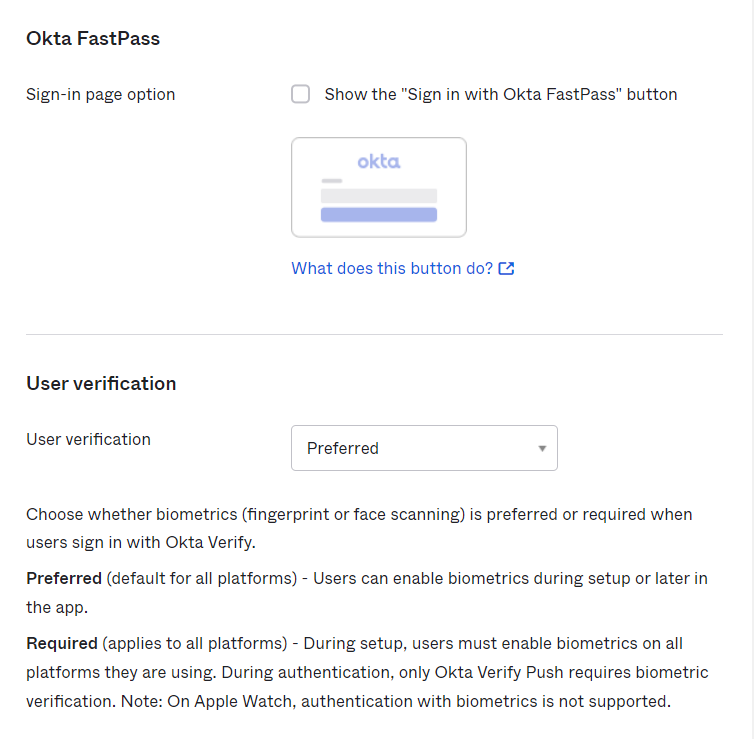
## Authenticators

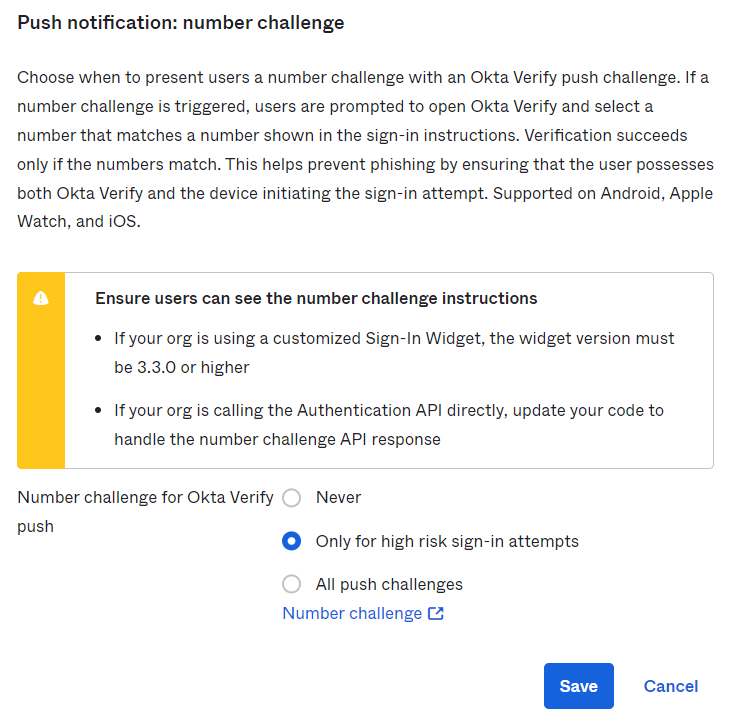


### Setup

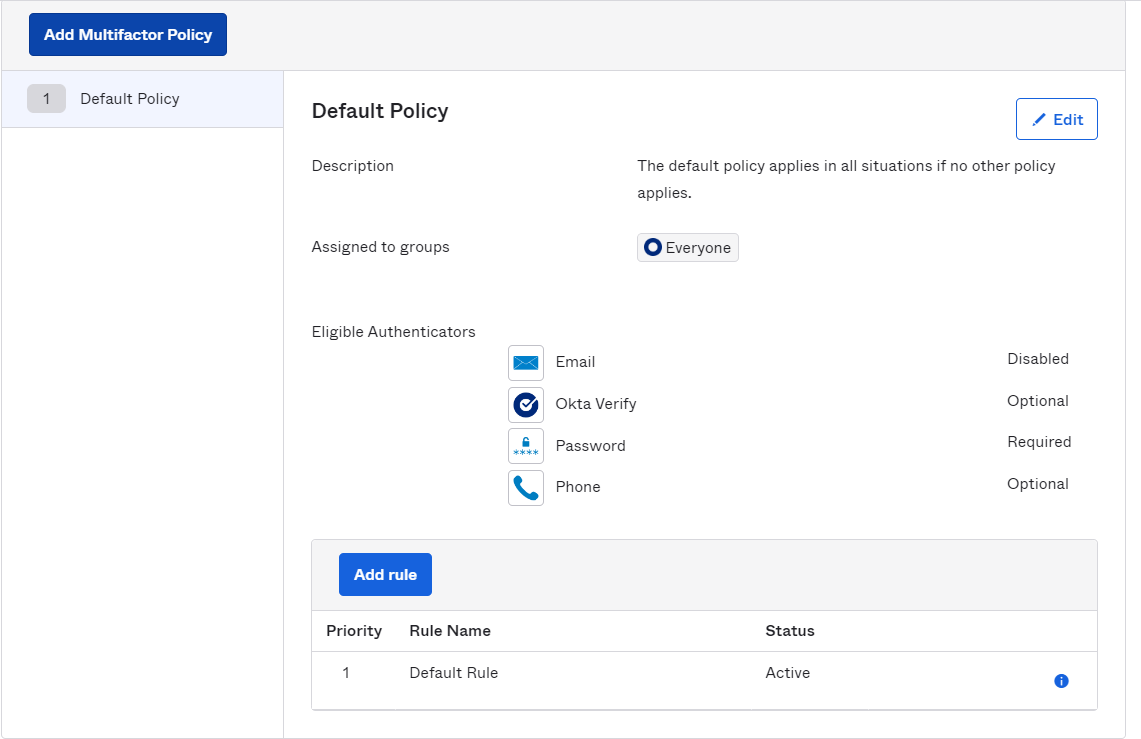




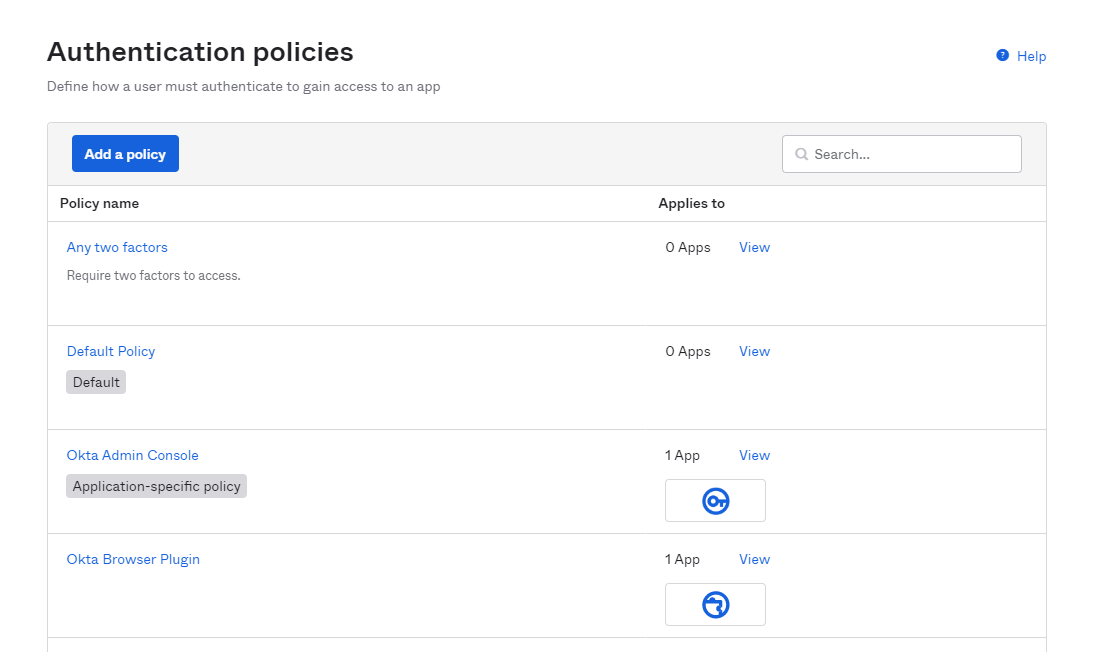


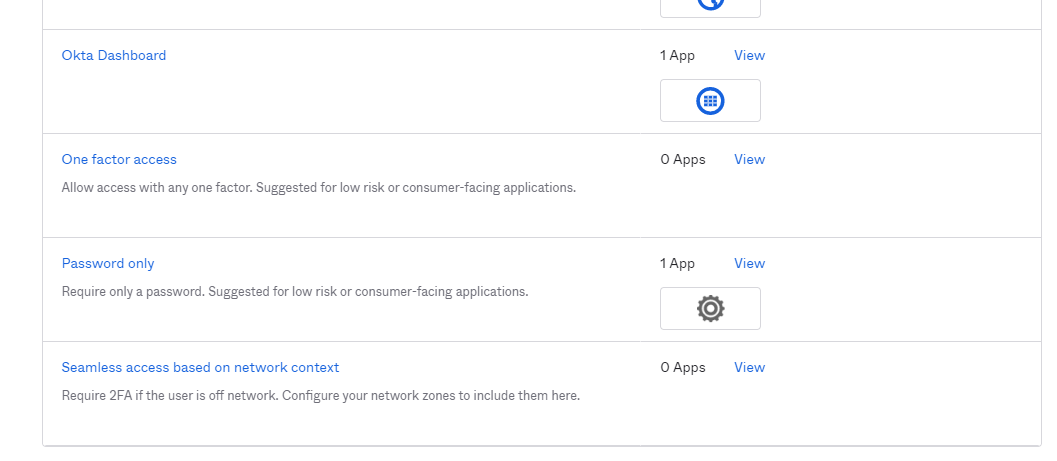


### Enrollment

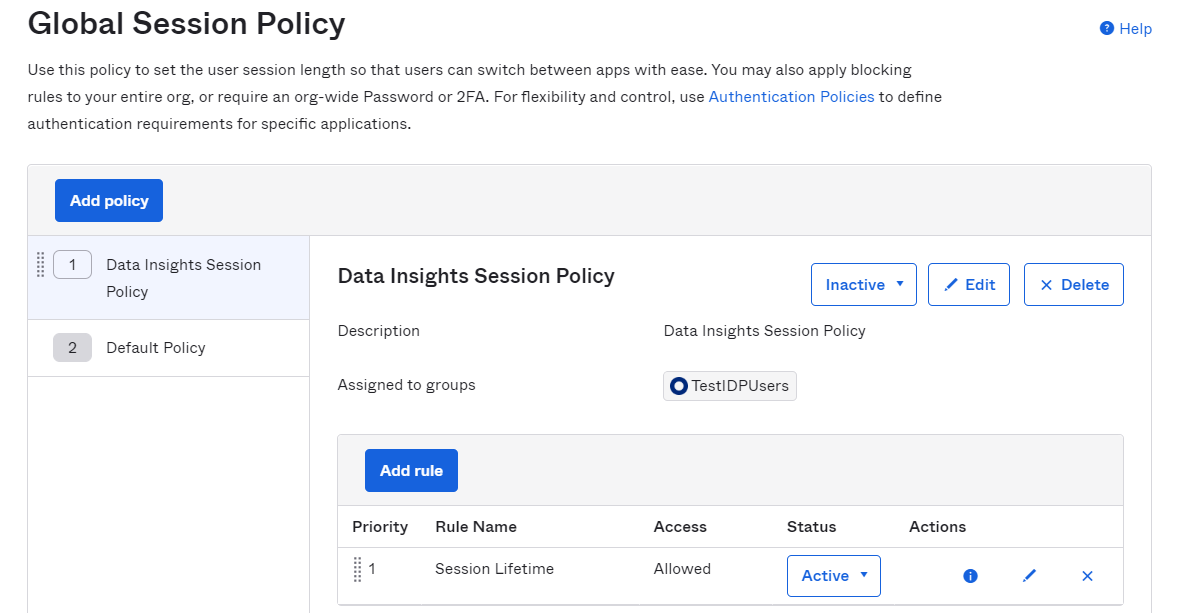


## Authentication policies

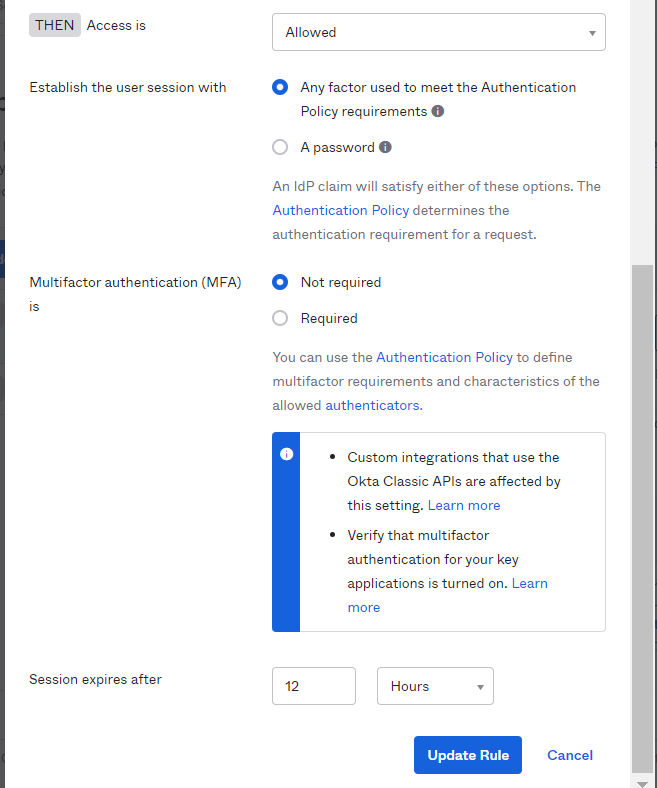




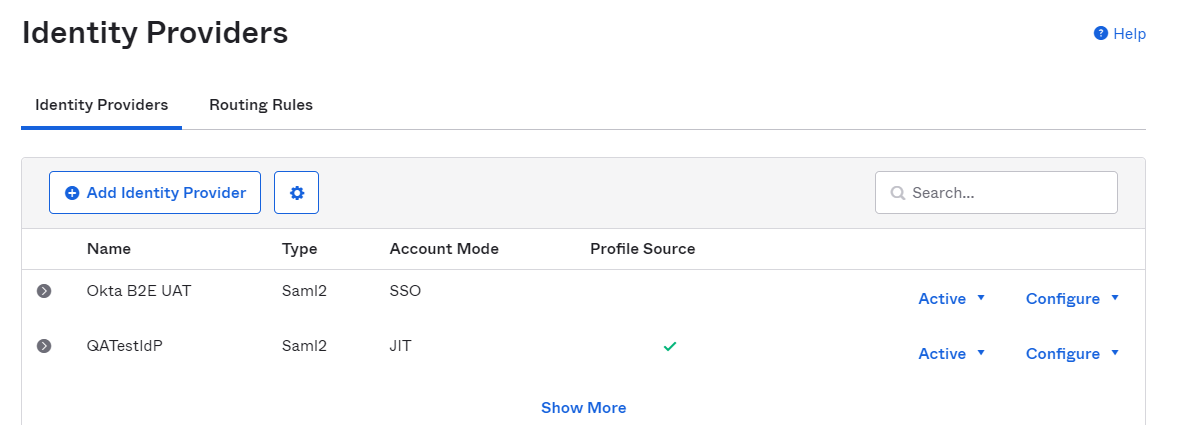
## Global Session Policy

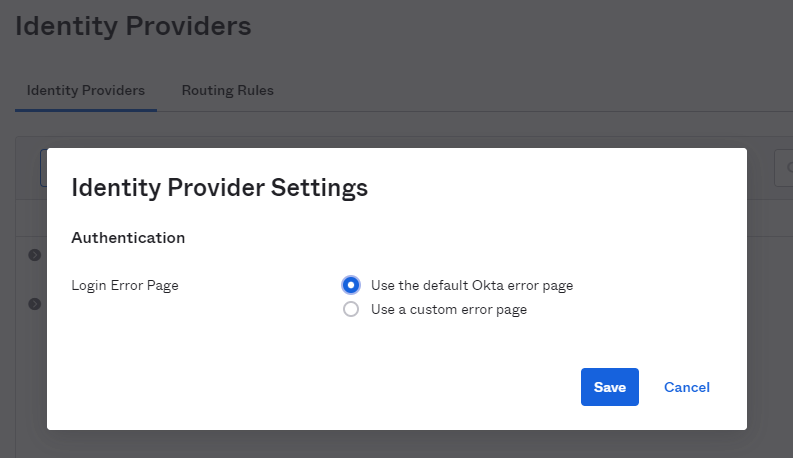




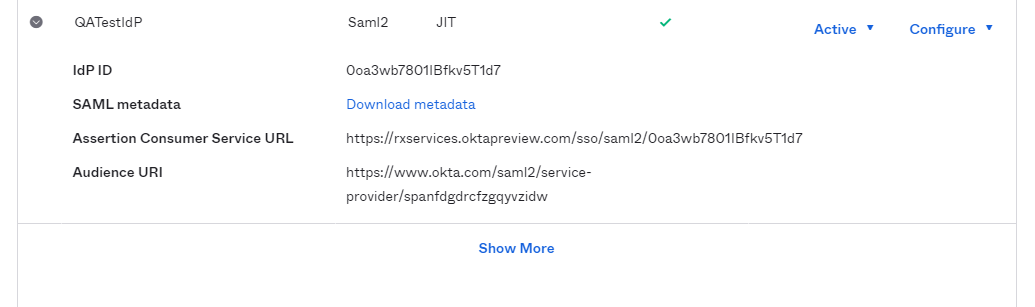


## Identity Provider

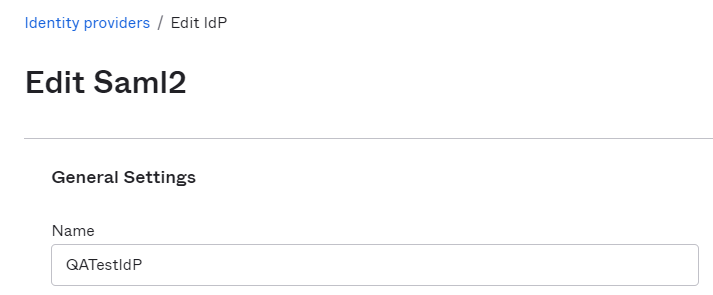


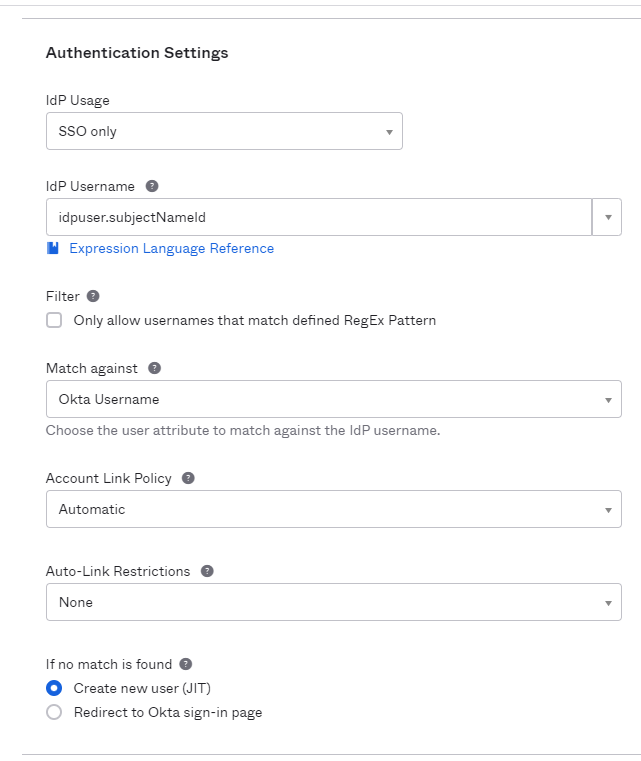


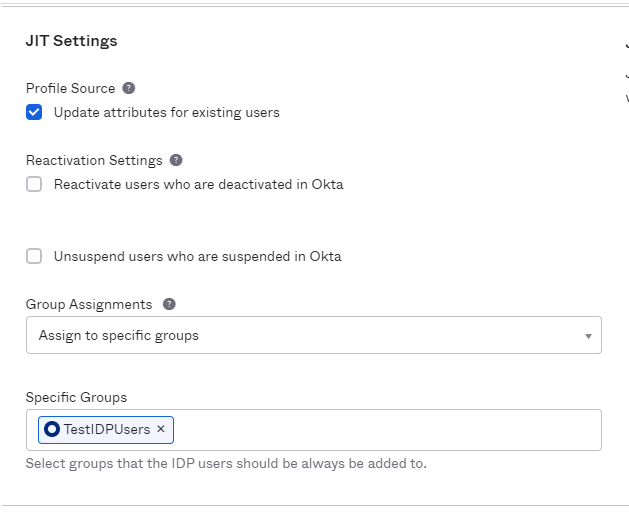
### External IDP Integration

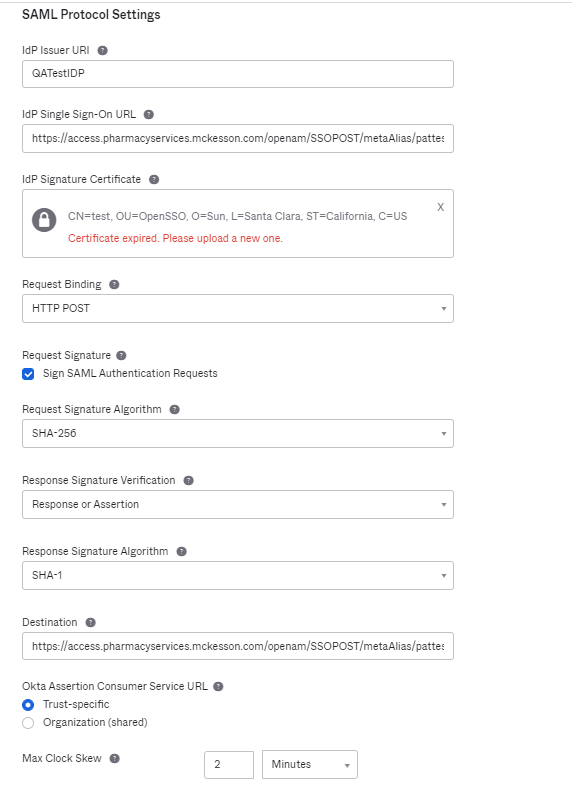


#### Configuration





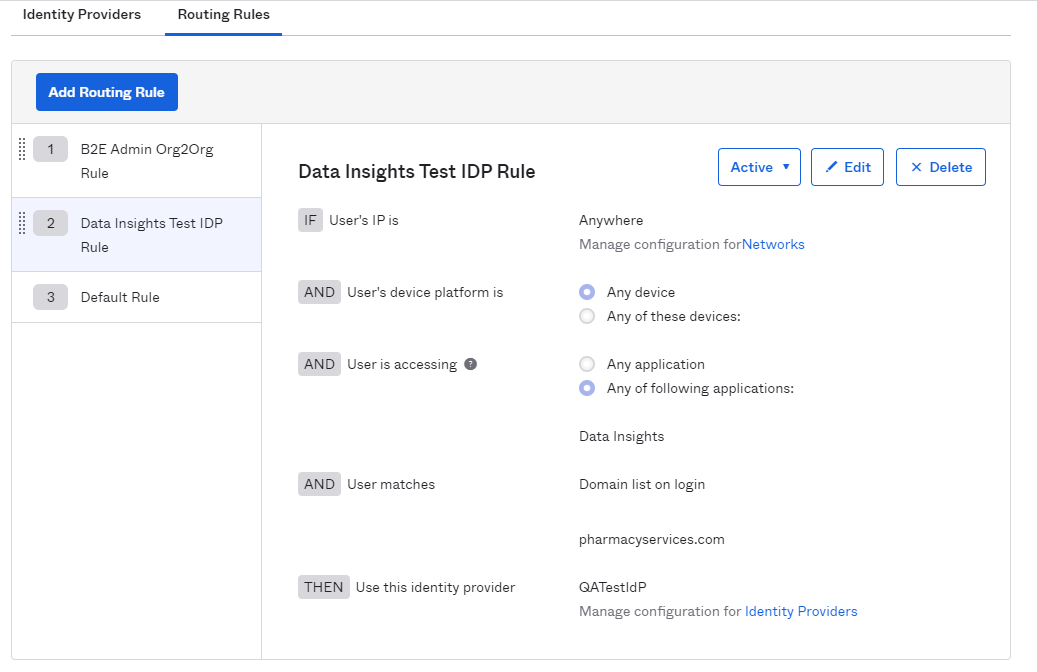




#### Edit Profile and Mappings

Refer to section [3.2.3. QATestIDP User](#_QATestIdP_User)

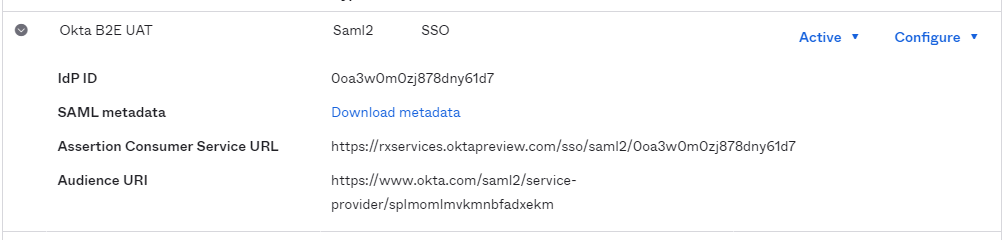
#### Routing Rules



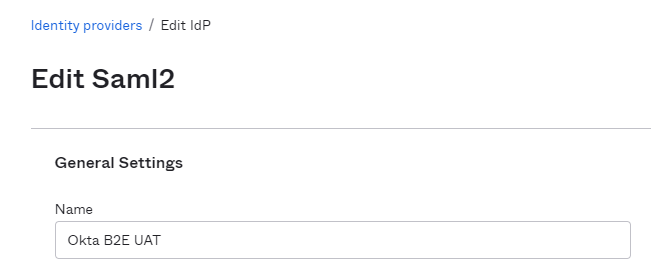
### Okta B2E IDP Integration

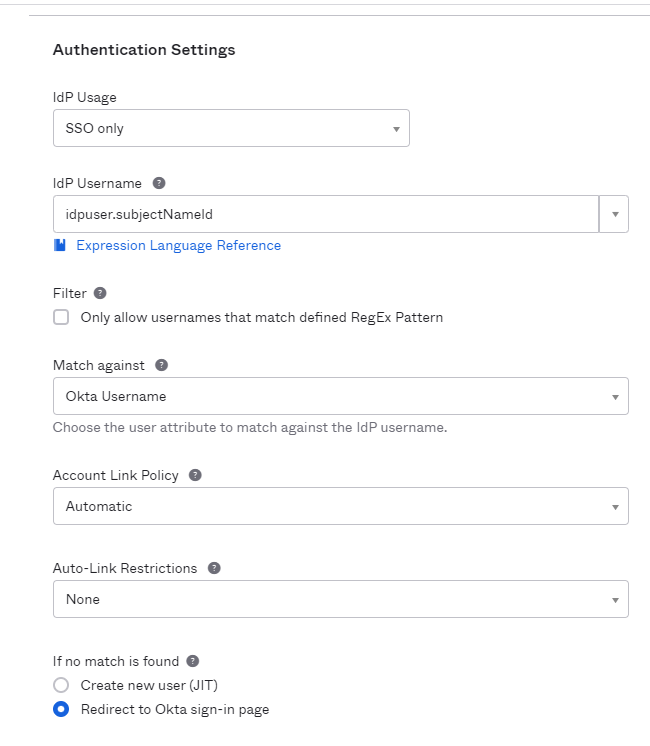
*B2E IDP setup is done as part of Org2Org integration with Okta B2E tenant. Please refer to document*

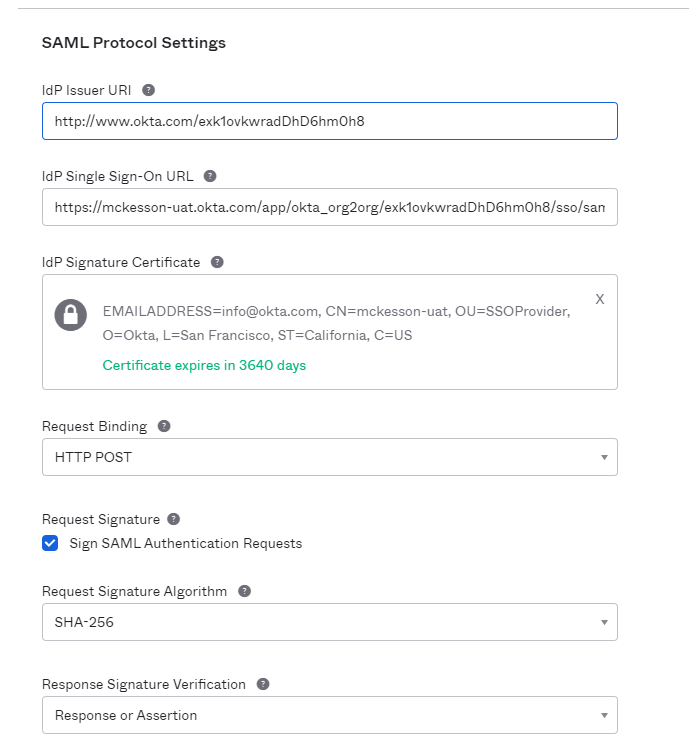
[McKessonB2B Okta\_B2B Org2Org\_Runbook v1.0.docx](https://mckessoncorp.sharepoint.com/:w:/r/sites/GRPMcKIAM-OktaIntegration/Shared%20Documents/Jira%20High%20Priority%20Tickets/02%20Erx%20DataInsight/03%20Implementation%20and%20Unit%20Test%20Phase/Okta%20Runbook/McKessonB2B%20Okta_B2B%20Org2Org_Runbook%20v1.0.docx?d=w406c070f535b4456af11046d42262fde&csf=1&web=1&e=OoGdLu) *for detail steps.*

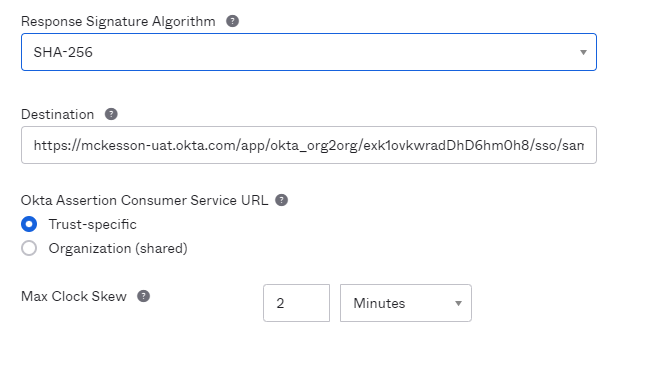


#### Configuration





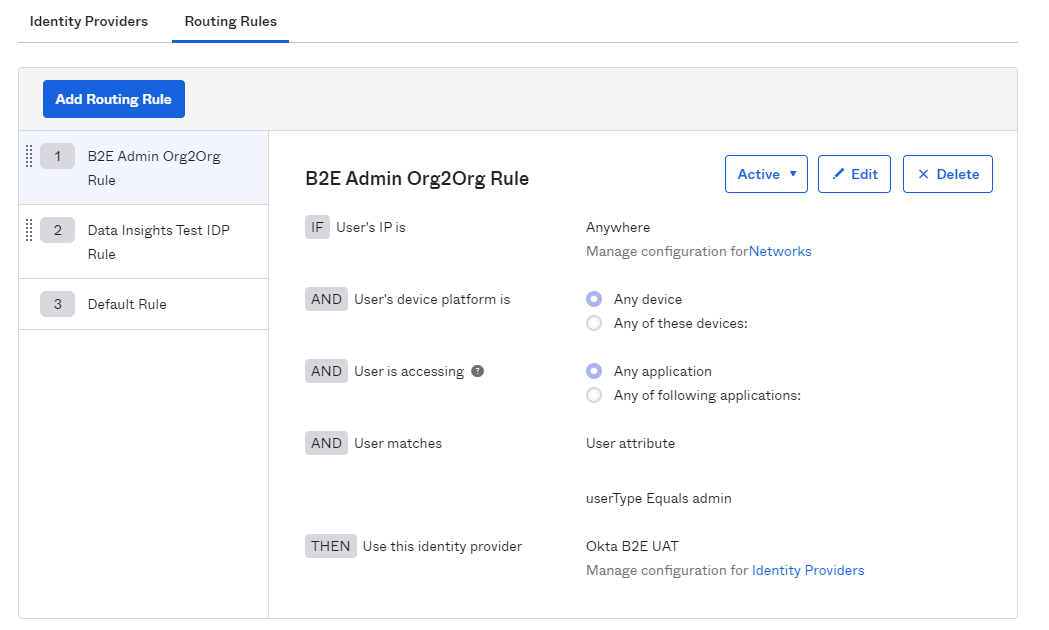




#### Edit Profile and Mappings

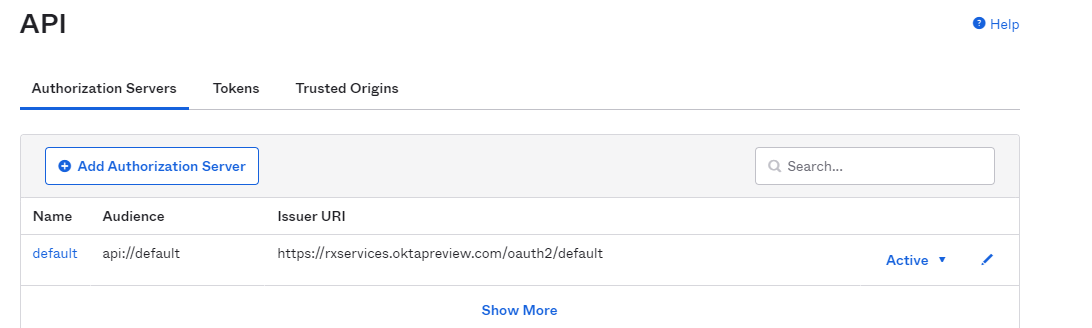
Refer to section [3.2.2. Okta B2E UAT User](#_Okta_B2E_UAT)

#### Routing Rules



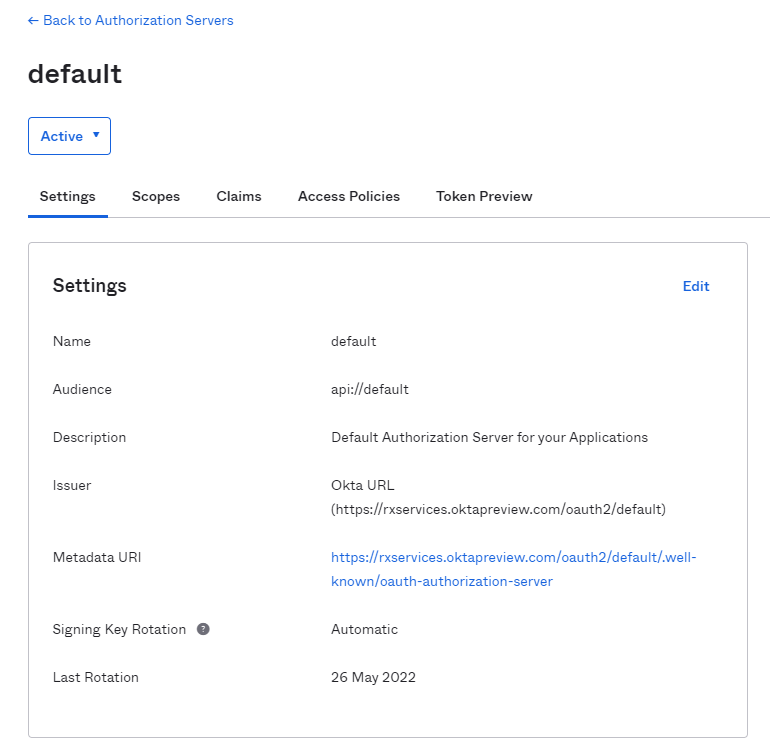
## API

### Authorization Servers

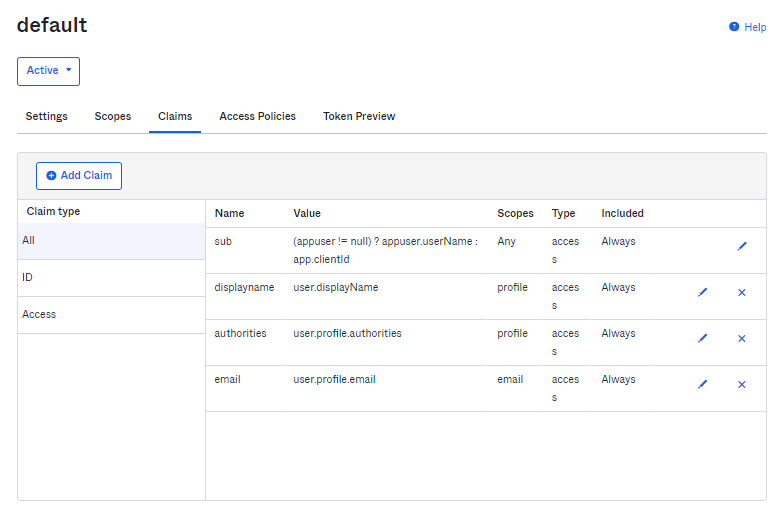


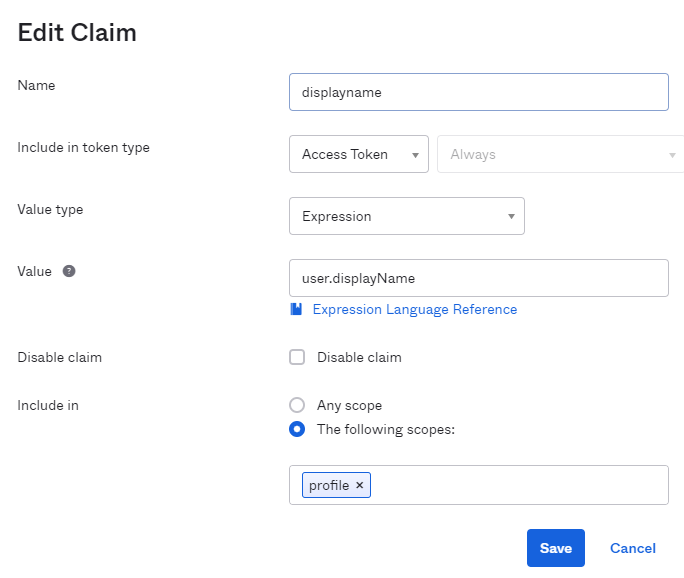
#### Default

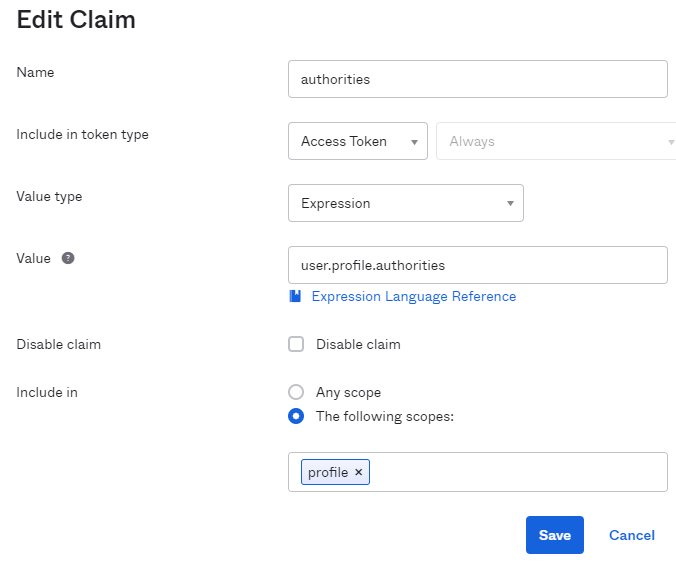
##### Settings



##### Claims

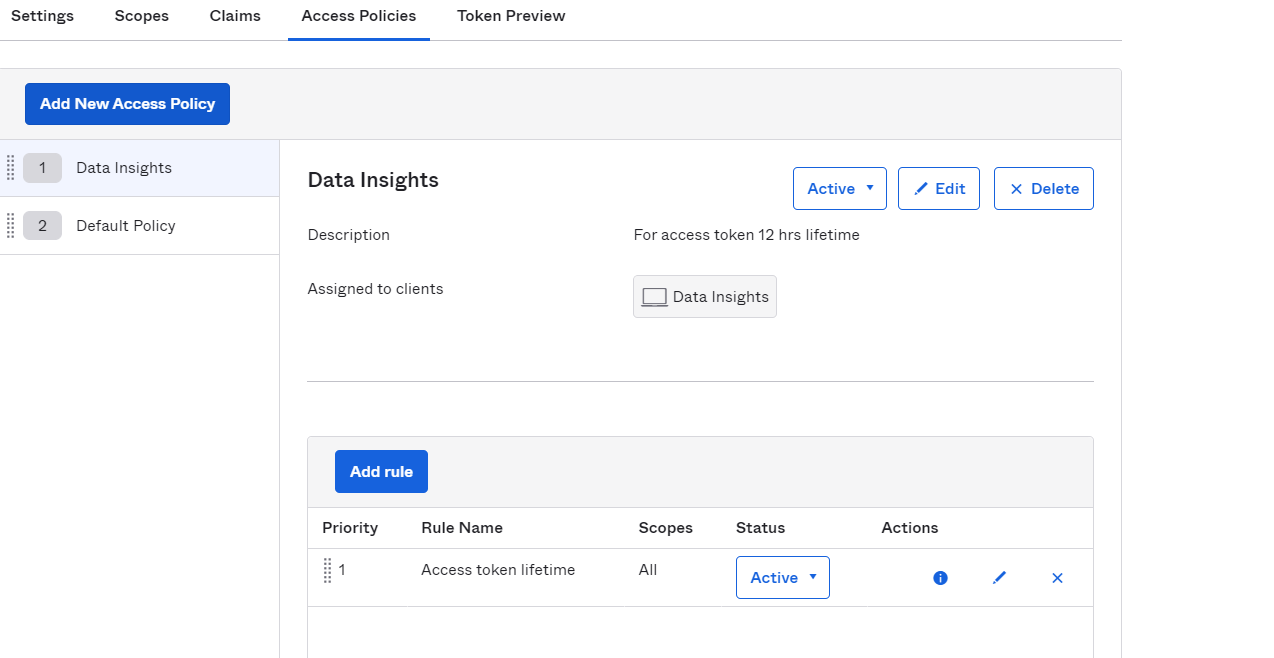


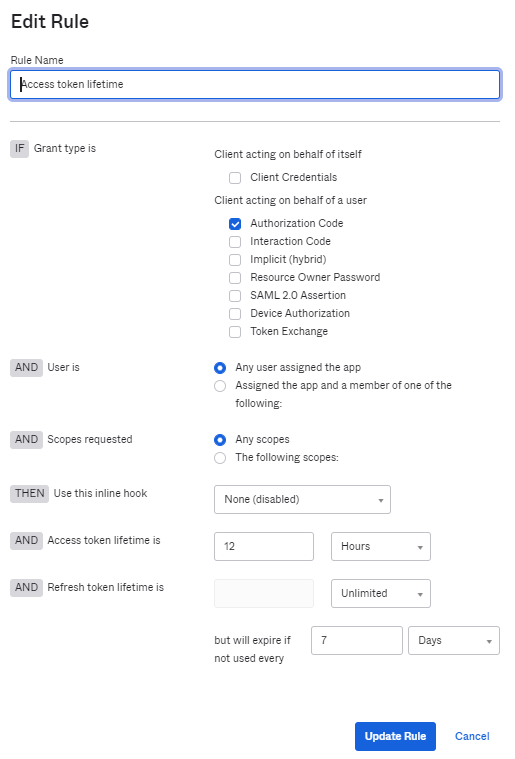






##### Access Policies





##### Token Preview

To test the token generated with a test user. Below is the token, generated for a test user:

**Grant type:** Authorization code

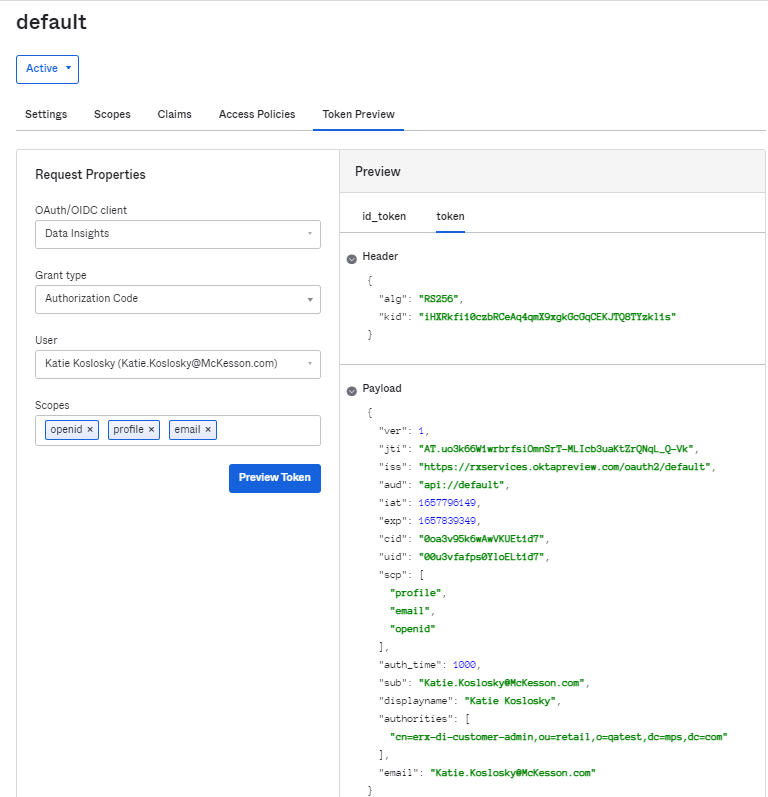
**Scope:** openid, profile, email

OIDC claims:

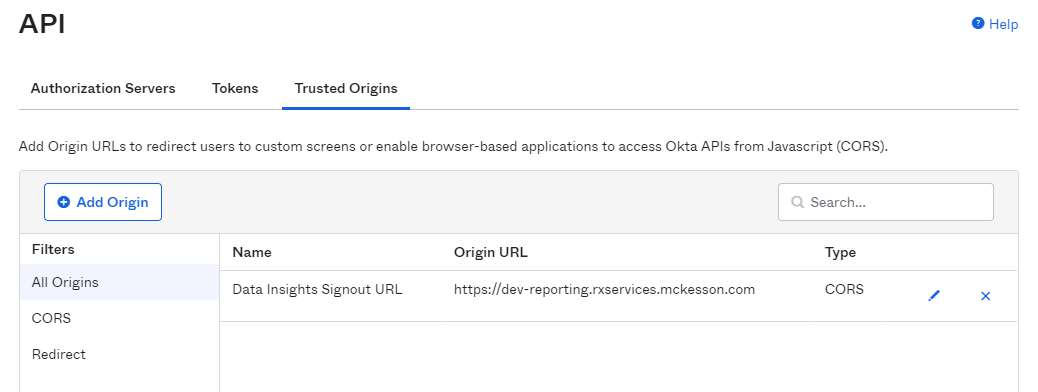
* 1. sub – userlogin in email address format
  2. displayname – First Name + Last Name
  3. authorities – Role name starts with “erx-di-“

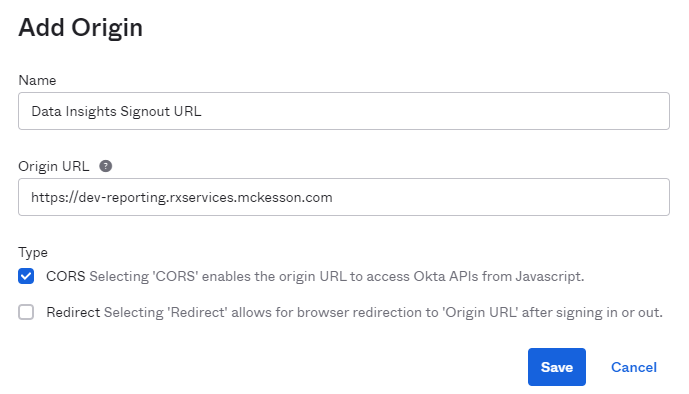
Sample claims in access token:





#### Trusted Origins





# Functional Diagram & Flow

## Flow Diagram

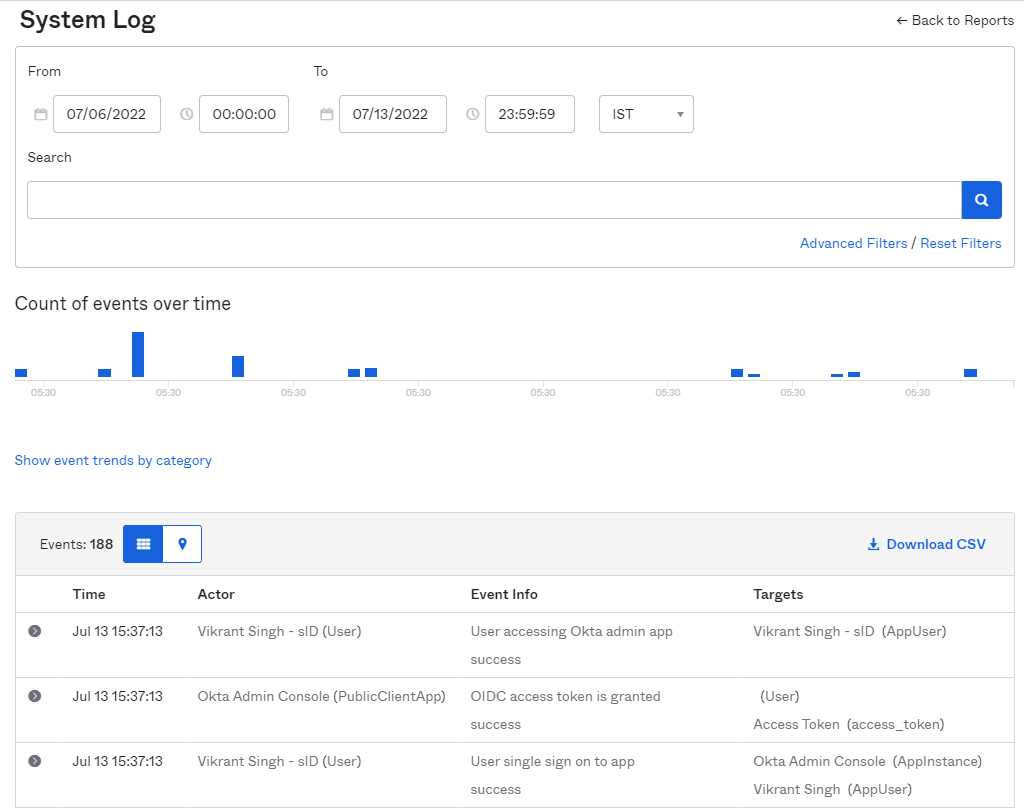


## Process Flow

|  |  |
| --- | --- |
| **Steps#** | **Description** |
| 1 | External users try to access Data Insights application URL in browser through internet. |
| 2 | Data Insights is SPA and integrated with Okta using OIDC PKCE integration pattern. Data Insights sends authentication request to Okta OIDC endpoint. |
| 3 | Routing rules are configured in Okta for IDP discovery which redirect user authentication request to appropriate customer’s IDP. Okta prompts user to enter user login. |
| 4 | User enters his/her user login in email address format on Okta login page. |
| 5 | Okta is integrated with Customer’s IDP using SAML 2.0 integration pattern. Okta identifies userlogin and redirect user to respective customer’s IDP for authentication as per routing rule. |
| 6 | Customer’s IDP prompt login page to user and user enters userlogin and password. If customer IDP has enabled MFA, user will be prompted for MFA. |
| 7 | Customer IDP validates user login credential and MFA (if applicable) and sends back SAML assertion back to Okta. |
| 8 | Okta will enable JITP for basic details of user coming into SAML assertion into Okta Directory. Following attributes will be JIT provisioned to Okta through Customer’s IDP.   1. username – login id of user i.e., email address 2. display name (typically first name last name) 3. authorities – Roles (erx-di-view, erx-di-explore, erx-di-customer-admin) |
| 9 | Okta will create access token with required claims and send back to Data Insights application. |
| 10 | Data Insights receives user’s access token, it will fetch OIDC claims. Data Insights will also derive user realm based on their userlogin domain. User authorization will be performed based on received OIDC claims and derived user realm. |

# Logging

## System Logs





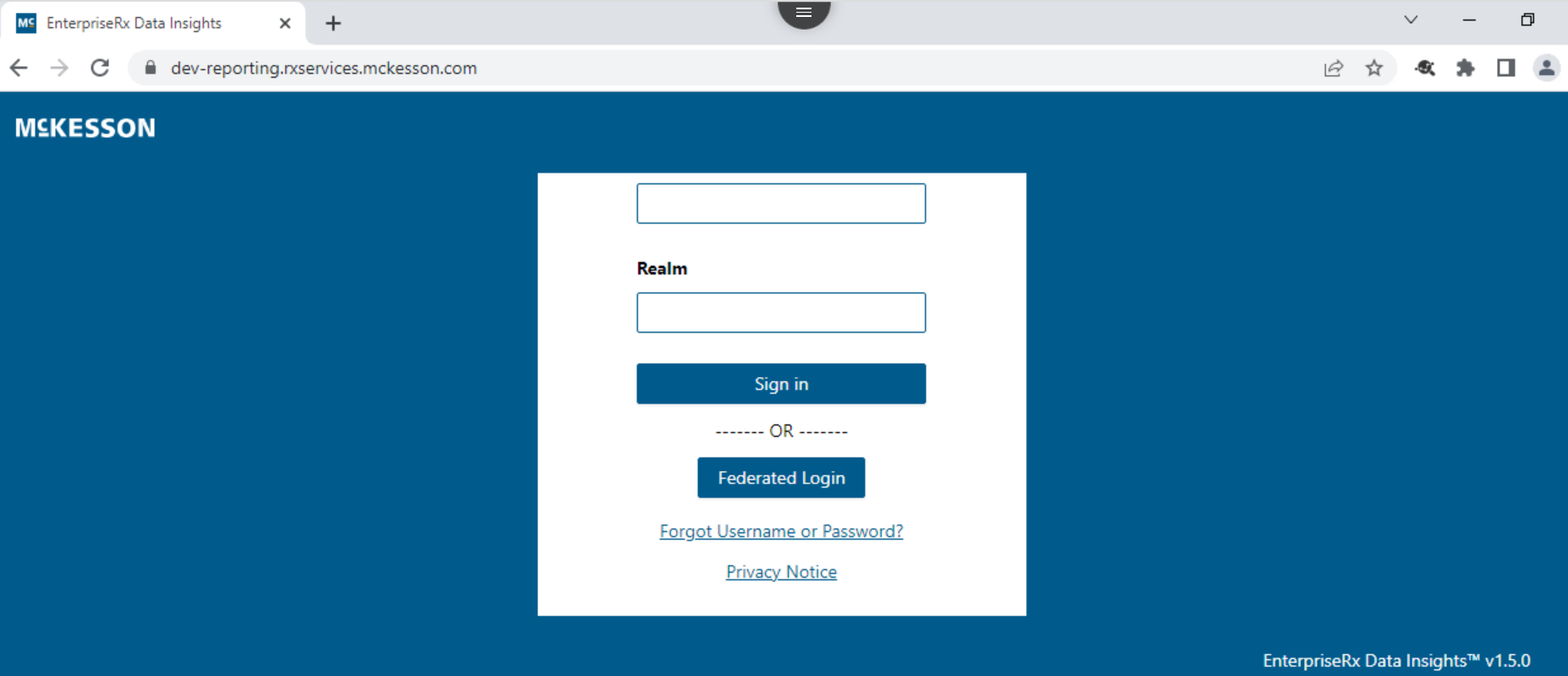
# Test Login

**Test user credetails:**

Username - test.user@pharmacyservices.com

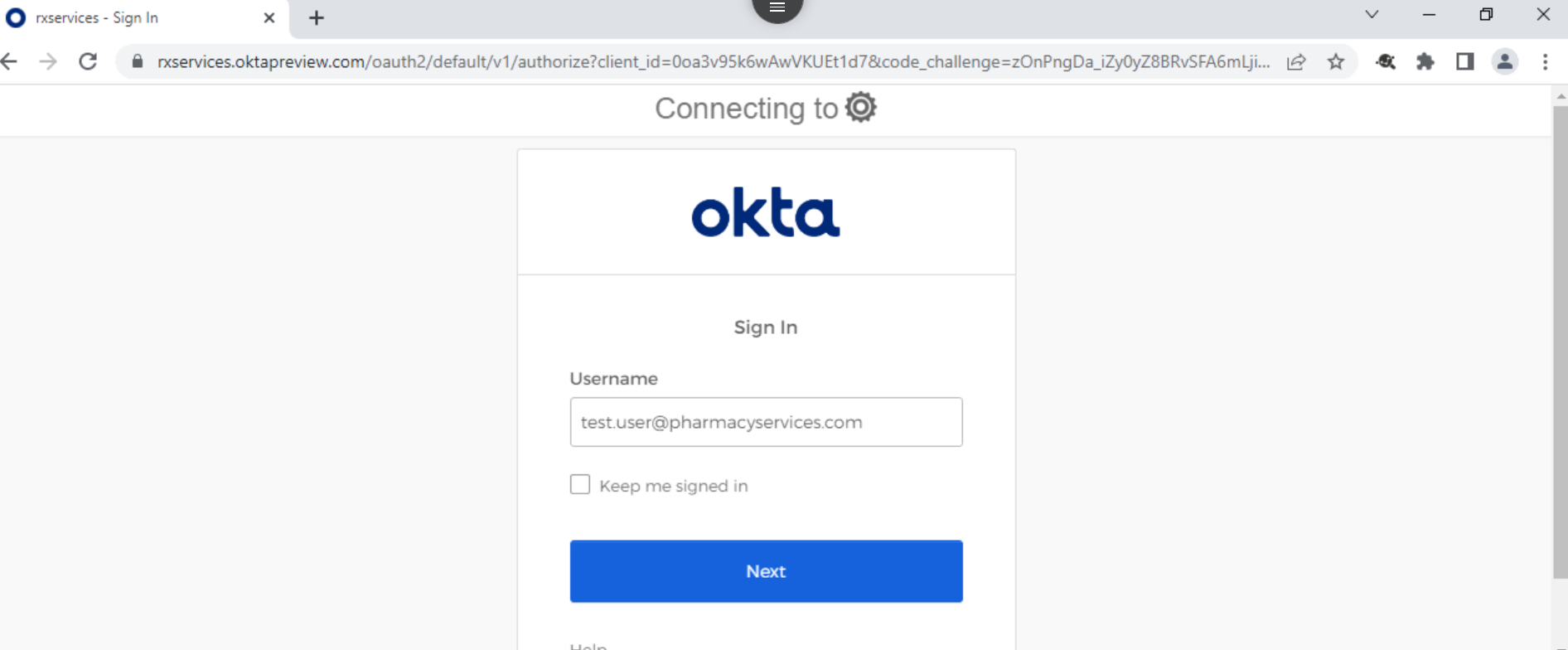
Password - TestTest1234

1. Access Data Insights Dev URL

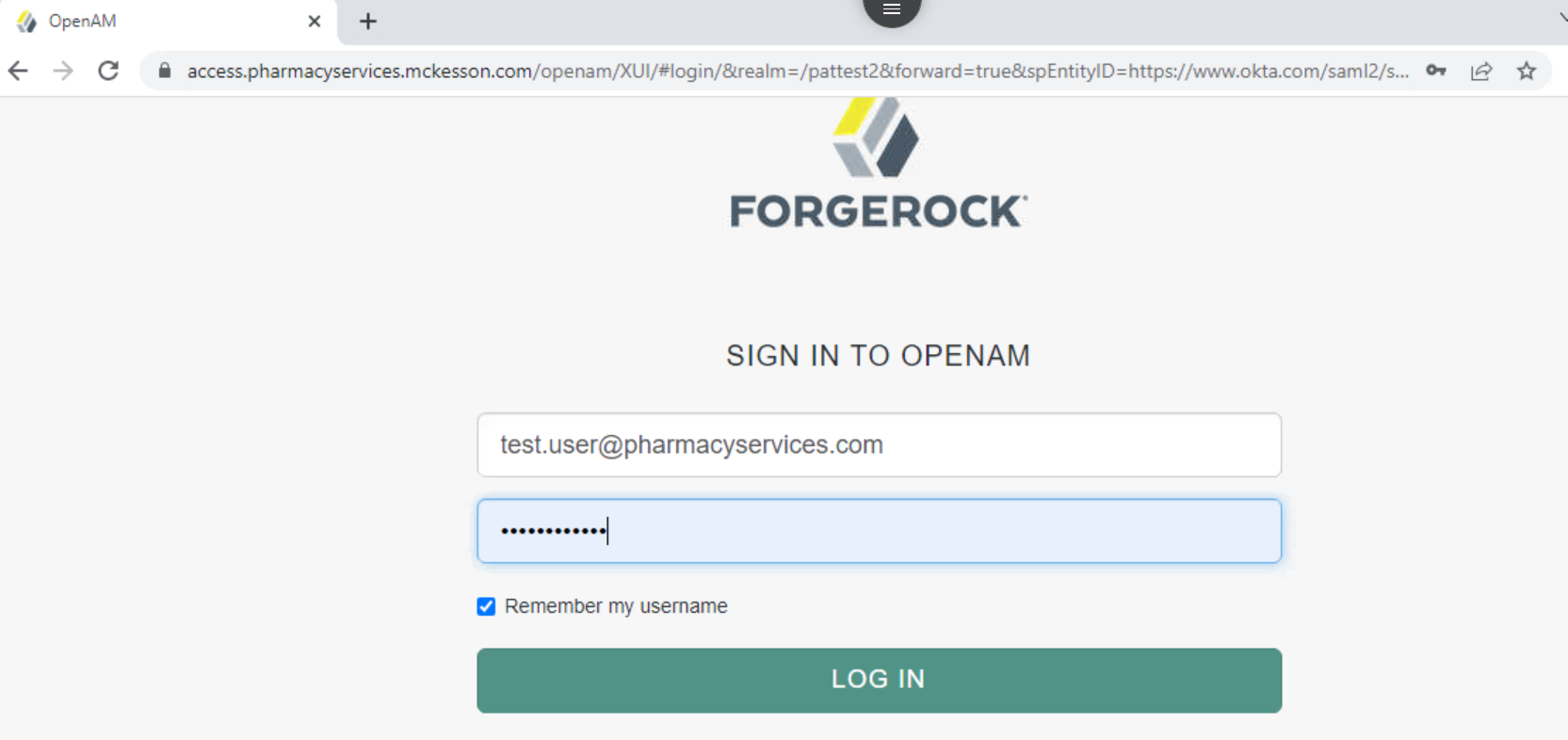


1. Click on Federated Login

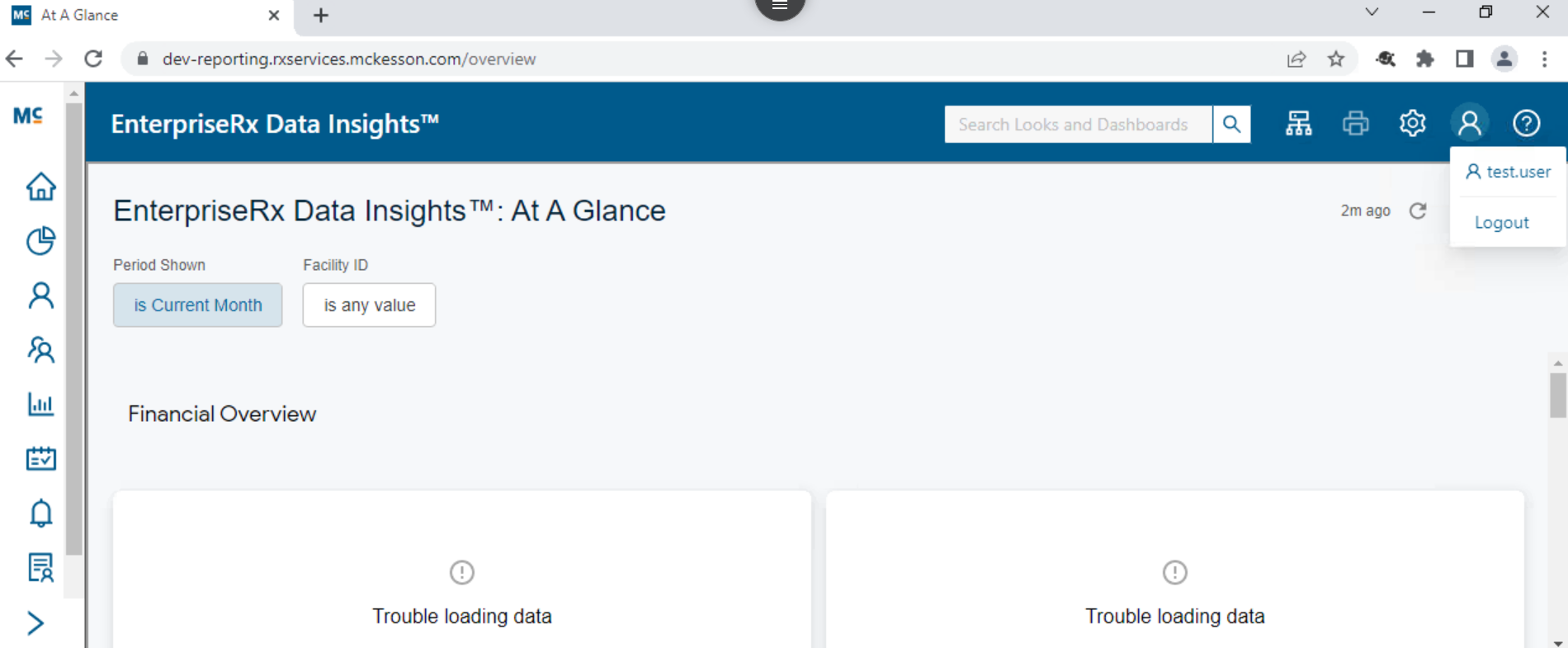
Login redirect to Okta B2B login page, enter test userlogin



1. Login redirected to Test IDP as per routing rule (test user login domain). Enter test user login and password.

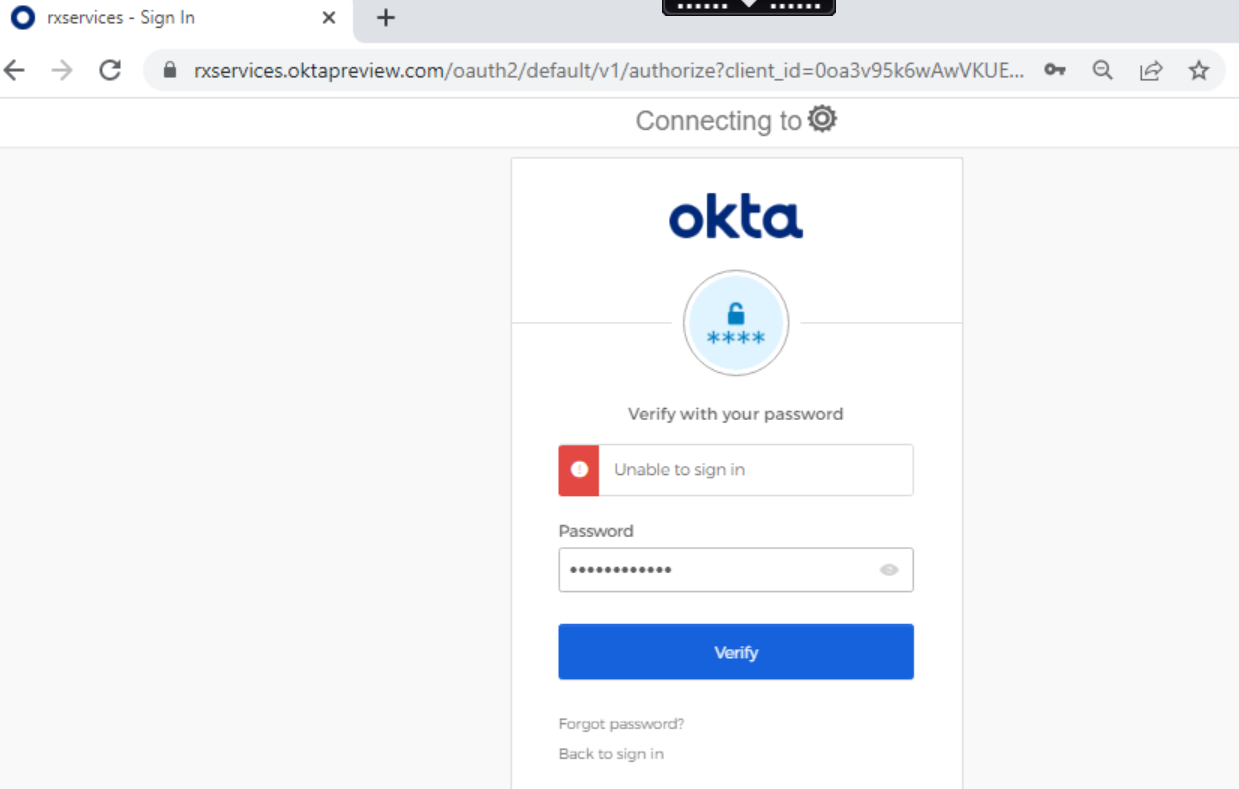


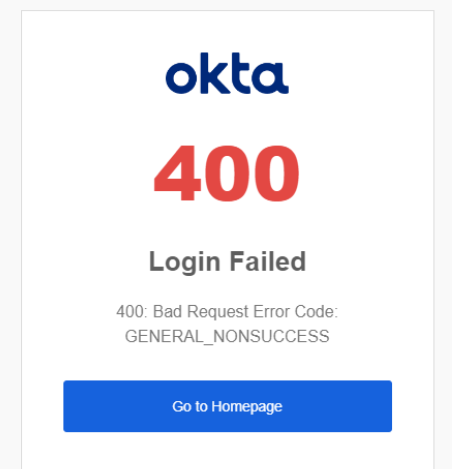
1. Test IDP validates user credential and send back response to Okta B2B.
2. Okta B2B sends access token to Data Insights.
3. Data Insights authorize user based on claims and present authorized page to user.



# Common Error/Issues:

**1 -** If user don’t have access to the appropriate IDP/application, the below okta error page appears.



**2 –** Due to the old cache or cookies below error page appears sometime. In this case, usr need to try in a new browser session or bu clearing the cache/cookies.  
  


**3 –** If the user’s account password has expired or not reset, the below error screen could occur.

In this case, user need to reset the password.

