

McKesson – Org2Org Runbook

**Version**: 1.0

**Last Updated**: June 24, 2022

Table of Contents

[1. Background 3](#_Toc107244679)

[2. Prerequisites 4](#_Toc107244680)

[3. Dashboard 5](#_Toc107244681)

[4. Directory 6](#_Toc107244682)

[4.1 People 6](#_Toc107244683)

[4.2 Groups 6](#_Toc107244684)

[4.3 Devices 7](#_Toc107244685)

[4.4 Profile Editor 7](#_Toc107244686)

[4.5 Directory Integrations 21](#_Toc107244687)

[4.6 Profile Sources 21](#_Toc107244688)

[5. Customization 22](#_Toc107244689)

[6. Applications 23](#_Toc107244690)

[6.1 Applications 23](#_Toc107244691)

[6.2 Self Service 27](#_Toc107244692)

[7. Security 28](#_Toc107244693)

[7.1 General 28](#_Toc107244694)

[7.2 HealthInsight 28](#_Toc107244695)

[7.3 Authenticators 28](#_Toc107244696)

[7.4 Authentication policies 31](#_Toc107244697)

[7.5 Global Session Policy 32](#_Toc107244698)

[7.6 Profile Enrollment 34](#_Toc107244699)

[7.7 Identity Provider 35](#_Toc107244700)

[7.8 Delegated Authentication 45](#_Toc107244701)

[7.9 Networks 45](#_Toc107244702)

[7.10 Behavior Detection 45](#_Toc107244703)

[7.11 Device Integrations 45](#_Toc107244704)

[7.12 Administrators 45](#_Toc107244705)

[7.13 API 46](#_Toc107244706)

[8. Workflow 53](#_Toc107244707)

[9. Reports 54](#_Toc107244708)

[10. Settings 55](#_Toc107244709)

[11. Org2Org Setup 56](#_Toc107244710)

[11.1 B2E Admin Access 56](#_Toc107244711)

[11.2 B2E End User Access 56](#_Toc107244712)

# Background

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

This document captures the inbound SAML configuration that provides federation between the McKesson B2E Okta Tenant and B2B Okta tenants.

# 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** |
| Okta B2B Super Admin  credentials | On the Okta B2B tenant, super admin user requires to perform:   1. Configure Org2Org related setup 2. Create service account for generating API token |
| Okta B2B API Token | API tokens are generated with the permissions of the user that created the token. On the Okta B2B tenant, service account (super admin) required to create API token to use for Org2Org provisioning |
| Okta B2E Admin Credentials | Super admin or combination of Organization admin and Application admin role should be given to perform Org2Org setup in Okta B2E tenant |
| AD Groups availability | Separate AD groups for admin users and end users should be available in Okta B2E tenant |

# Integration Overview

Org2Org integration is required for below types of access:

1. **B2E admin access:** McKesson internal user who requires to work as Okta administrators in Okta B2B tenant.
2. **B2E end user access:** McKesson internal users who requires access in application integrated with Okta B2B tenant.

*Note: Separate setup is required for B2E admin access and end user access.*

## Okta Tenant

Below table captures the details of Okta tenants integrated through Org2Org connect.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Role** | **Okta Tenant** | **Application Name** | **Dev** | **UAT** | **Prod** |
| Source (Spoke) | Okta B2E | McKesson Okta B2E | https://mckesson-uat.okta.com | | https://mckesson.okta.com |
| Destination (Hub) | Okta B2B | Data Insights | https://rxservices-admin.oktapreview.com/ | https://rxservices-uat.okta.com/ | https://rxservices.okta.com/ |
| New Ipsen Portal | https://mckb2bipsen-qa.oktapreview.com/ | https://mckb2bipsen-qa.oktapreview.com | https://mckb2bipsen.okta.com |
| Biologics Portal | https://mckb2bbiologics-qa.oktapreview.com/ | https://mckb2bbiologics-qa.oktapreview.com | https:// mckb2bbiologics.okta.com |
| Hub Connect | https://hubconnect.oktapreview.com/ | [https://hubconnectqa.oktapreview.com](https://urldefense.com/v3/__https:/hubconnectqa.oktapreview.com__;!!KMayzP4JbQ!caycFk45dBUpsr34aIg0bqKf92eHHCC5VJp2_0DLVtXXQEK5ZNL8qhHXR3vcQd1WV7lYNRty-LyqdMe-NHY$) | https://hubconnect.okta.com |

**NOTE:** Please do NOT change/modify any default policy over any tenant. If any policy (like authentication policy, password policy or MFA policy) required as per application requirement, need to create separately without changing/modifying any default or existing policy.

## AD Groups

Below table captures the AD group name pushed from Okta B2E to Okta B2B through Org2Org connect.

|  |  |  |  |
| --- | --- | --- | --- |
| **Access Type** | **Application Name** | **UAT** | **Prod** |
| Administrator Access | All Application | EAMOKTADEVONLY |  |
| End user access | Data Insights | NA | NA |
| New Ipsen Portal |  |  |
| Biologics Portal |  |  |
| Hub Connect2 |  |  |
|  |  |  |

## Service Account

Below table captures the service account name used to create provisioning API token in Okta B2B tenants

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **UAT** | | | | | **Prod** |
| **Admin Role** | **Userlogin** | **First Name** | **Last Name** | **Email** |  |
| Super Administrator | b2eadmin@mckesson.com | b2e | org2orgadmin | iam@mckesson.com |  |

## Custom Attributes

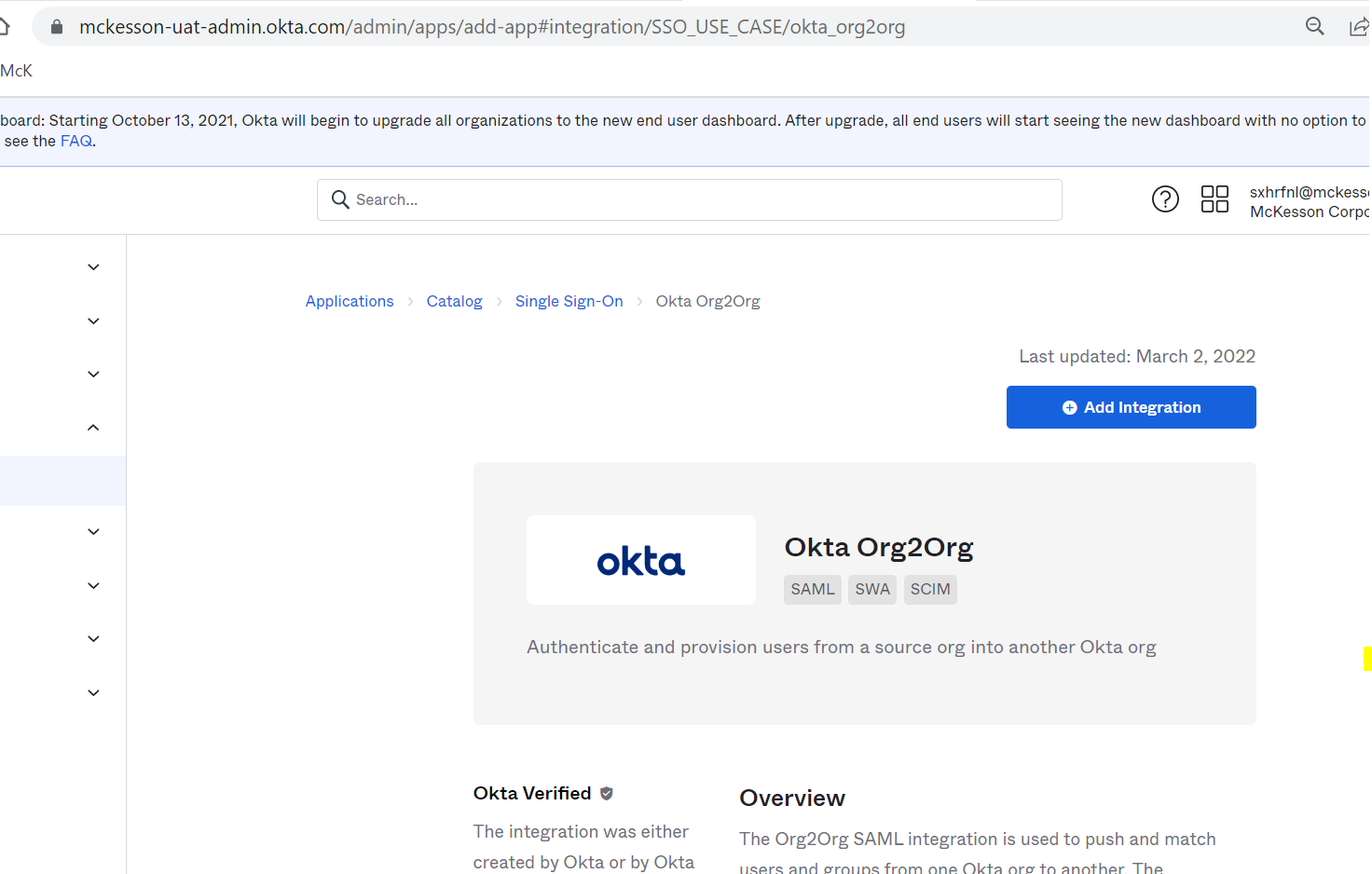
Below table captures the custom attribute required in Okta B2B tenants

|  |  |  |
| --- | --- | --- |
| **Profile** | **Custom Attributes** | **Attribute Type** |
| [User (default)](https://rxservices-admin.oktapreview.com/admin/universaldirectory) | uid | string |
| eid | string |

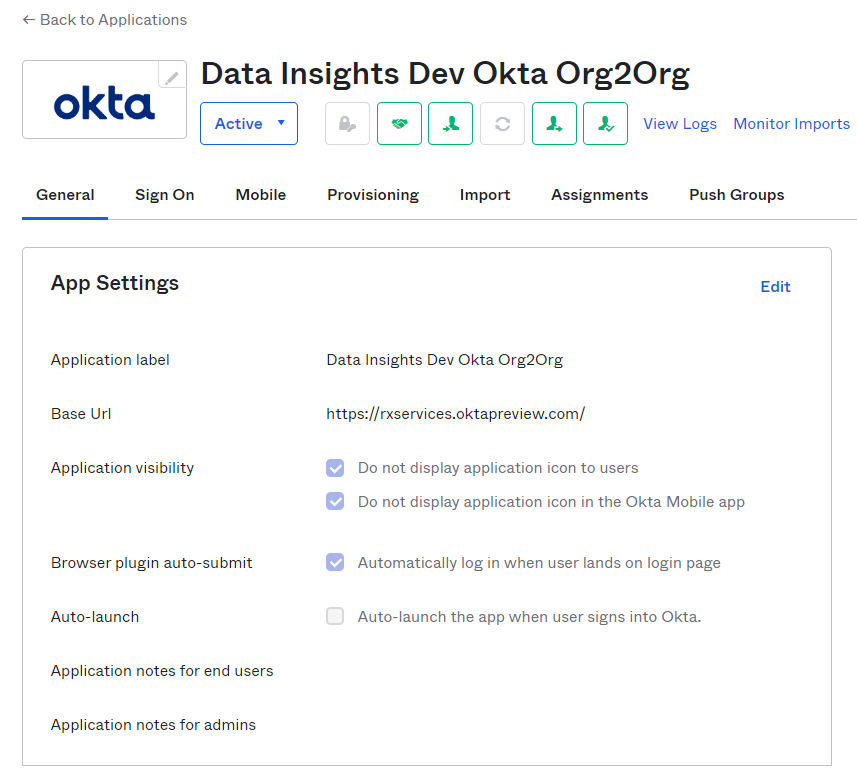
# Okta B2E Tenant Configuration

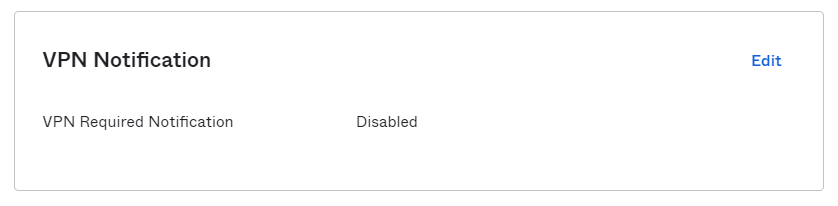
*Note: Configuration screenshots are taken from Data Insights application setup, change the URLs as per application details.*

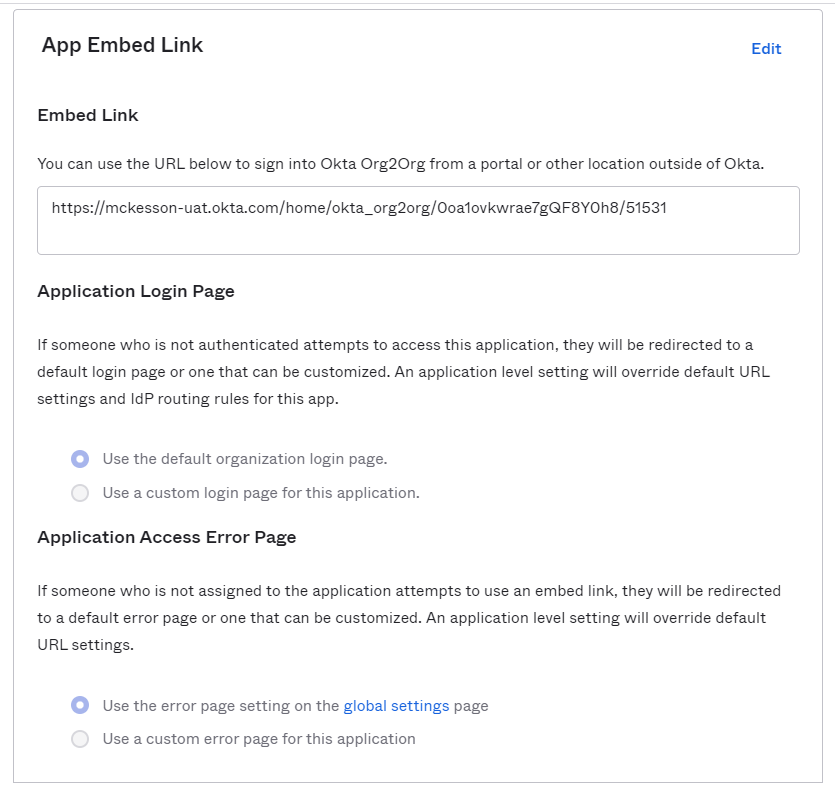
## Register Org2Org Application



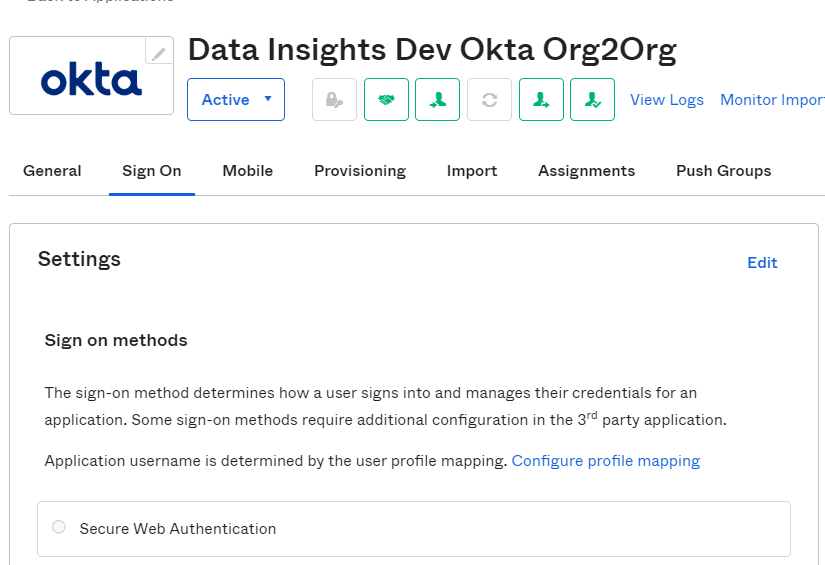
### General

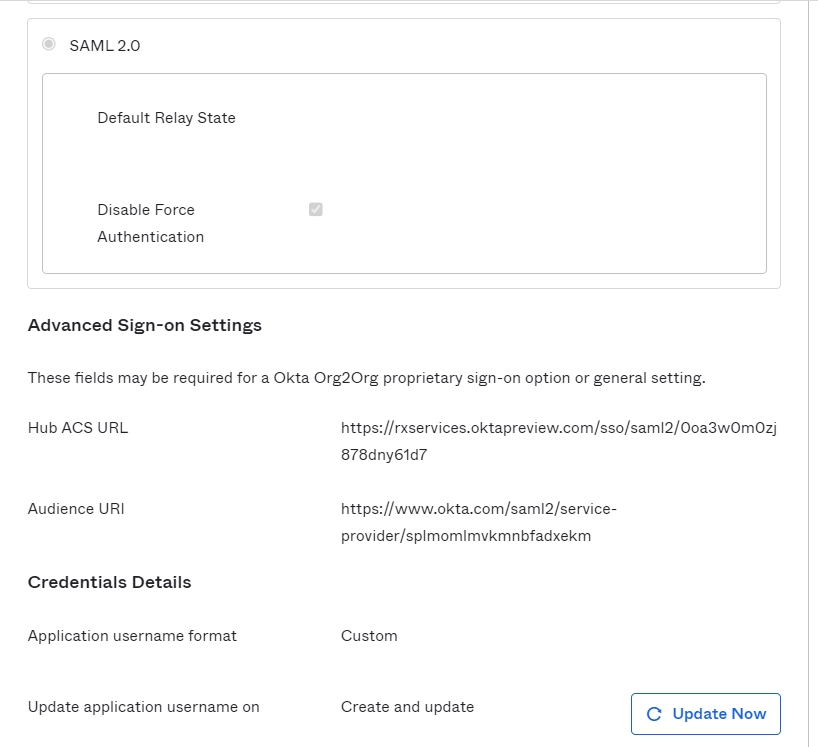


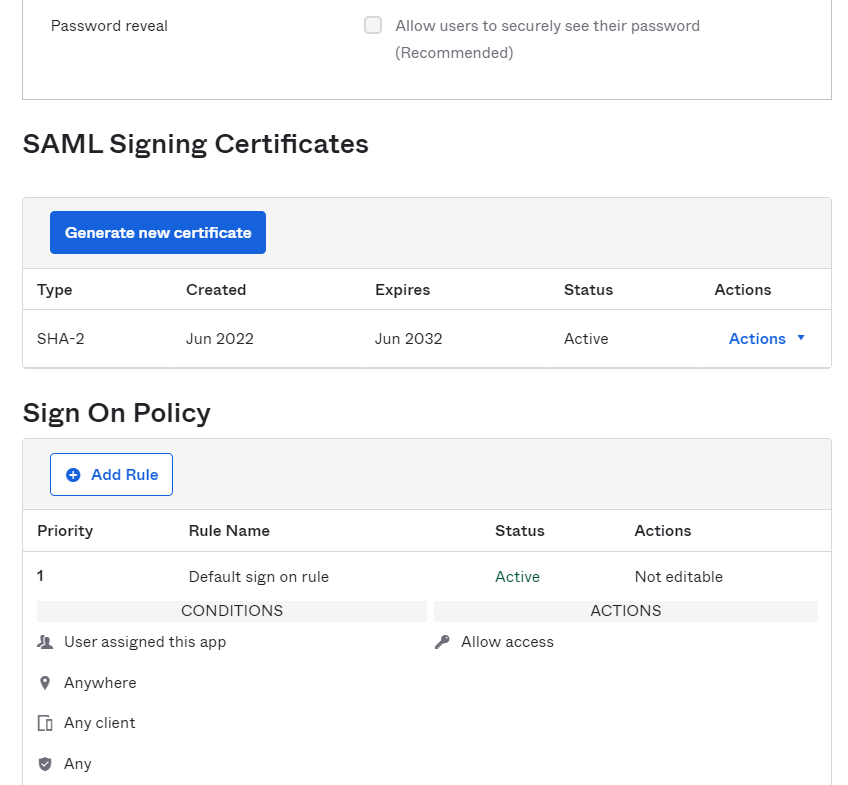




### SignOn





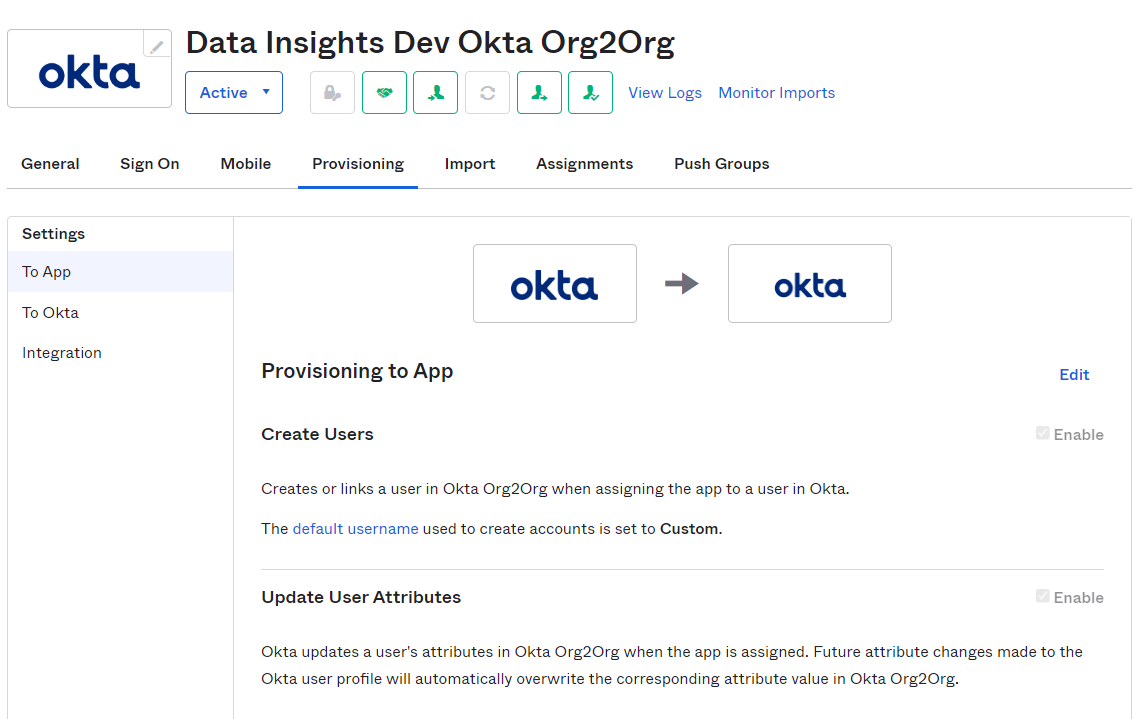


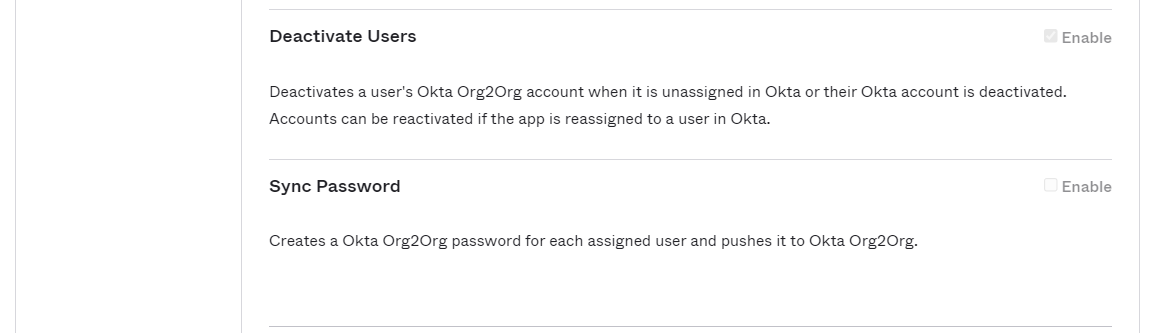
### Provisioning

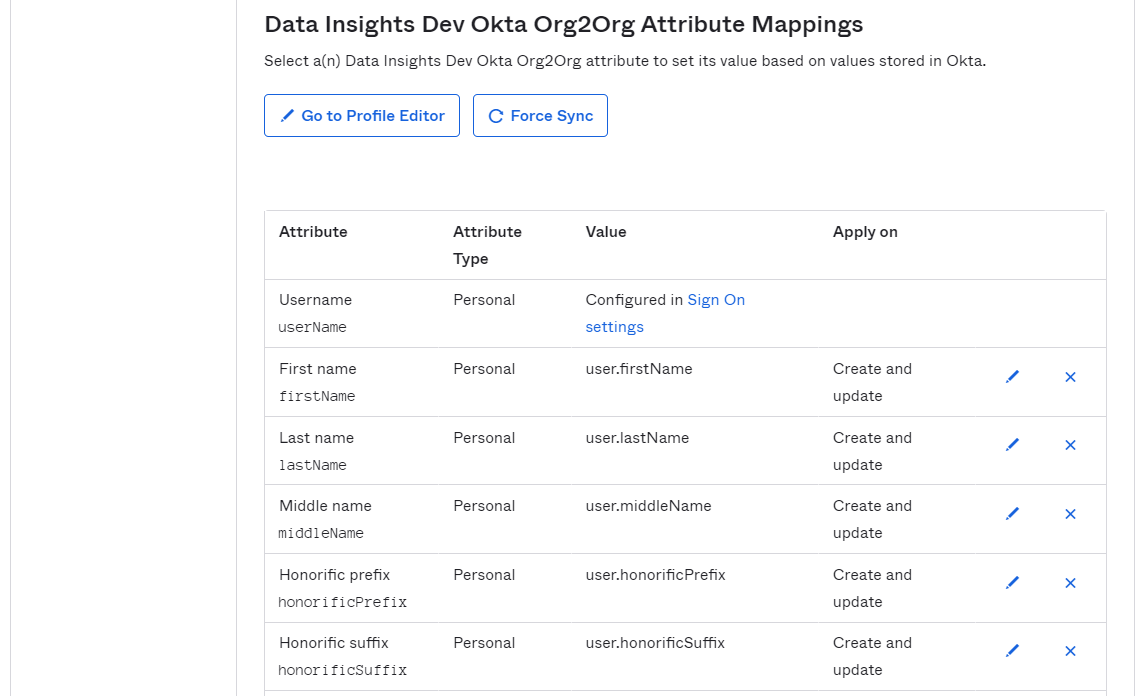
#### To App

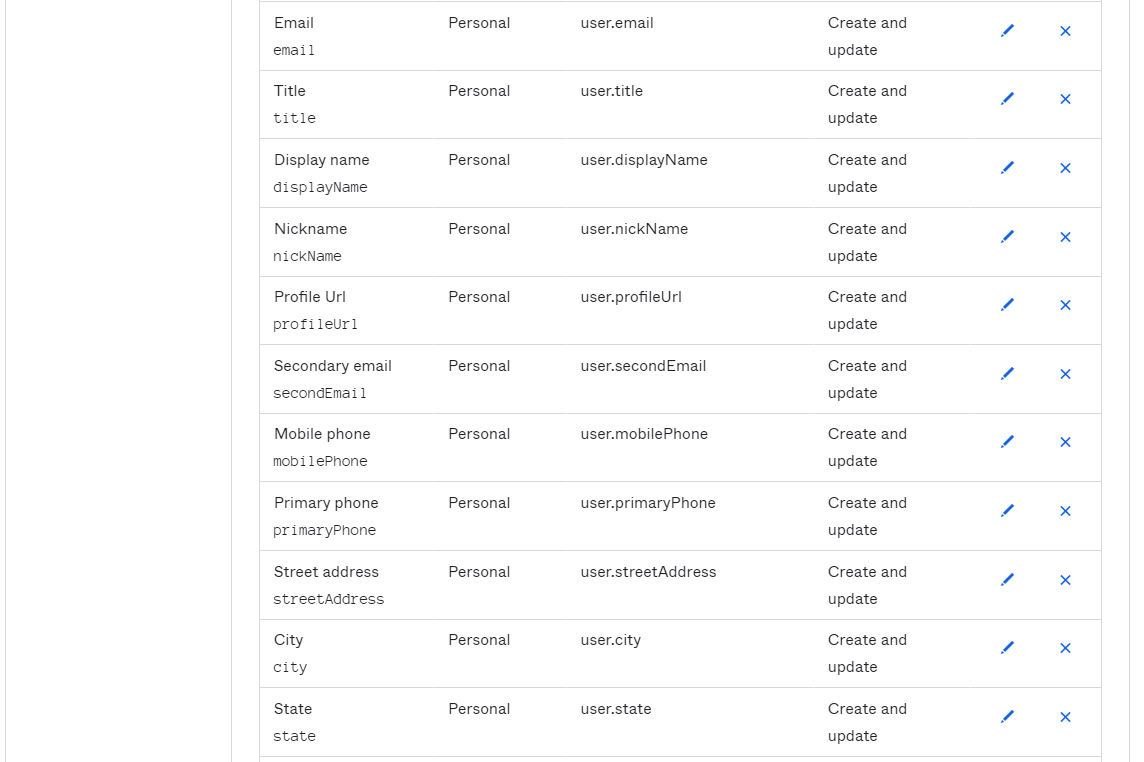
Follow below mappings for access types:

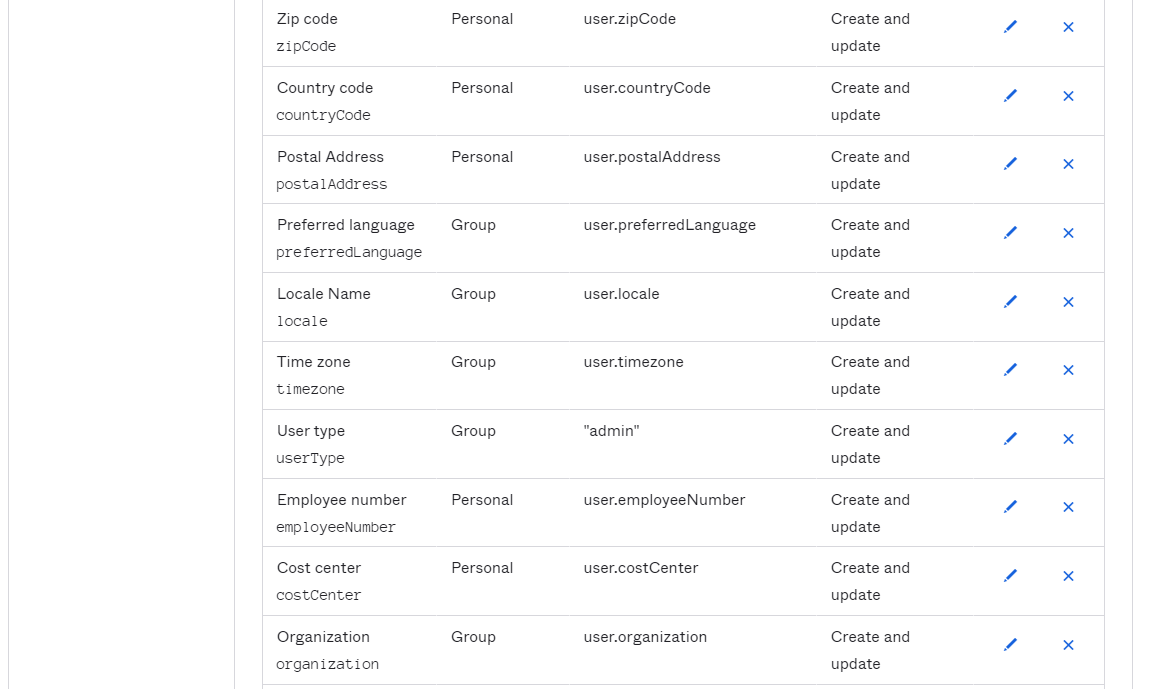
|  |  |
| --- | --- |
| **Access Type** | **Mapping** |
| B2E Admin Access | userType: “Admin” |
| B2E End User Access | userType: “Internal” |

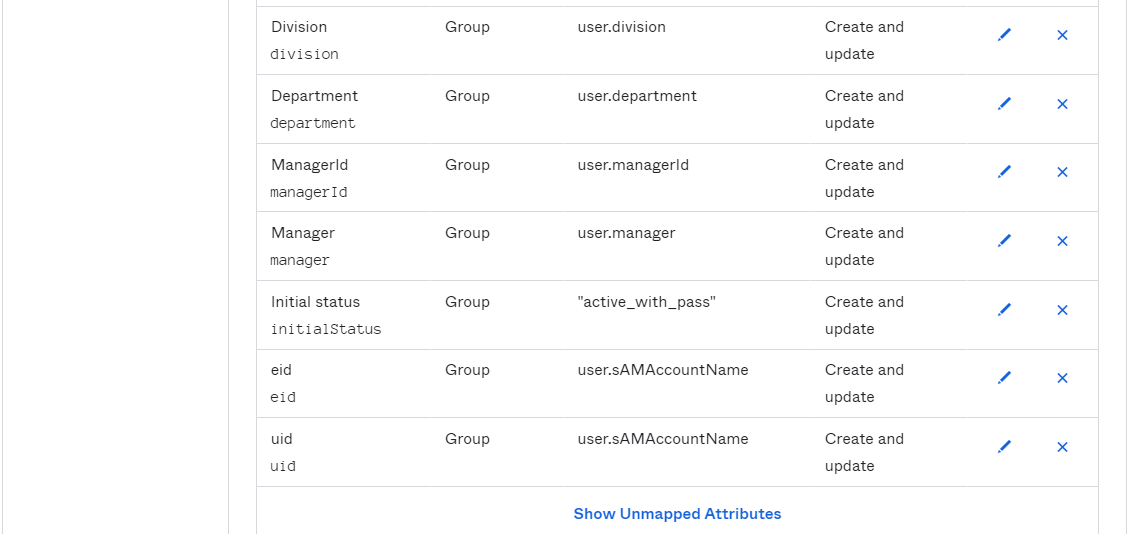








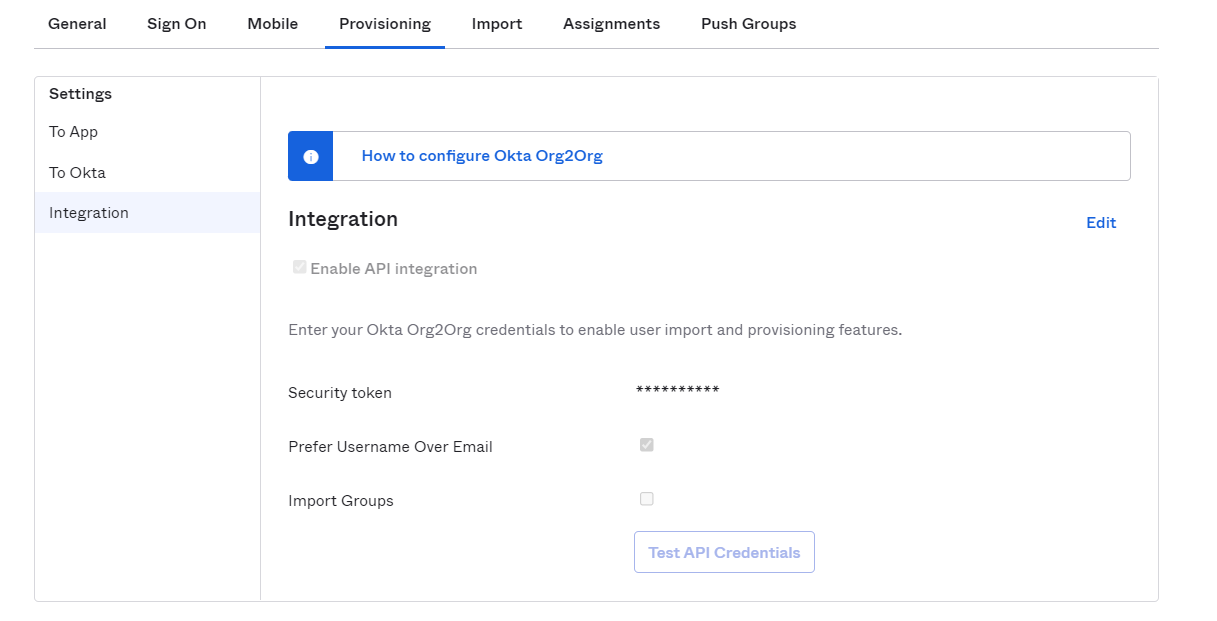




#### To Okta

NA

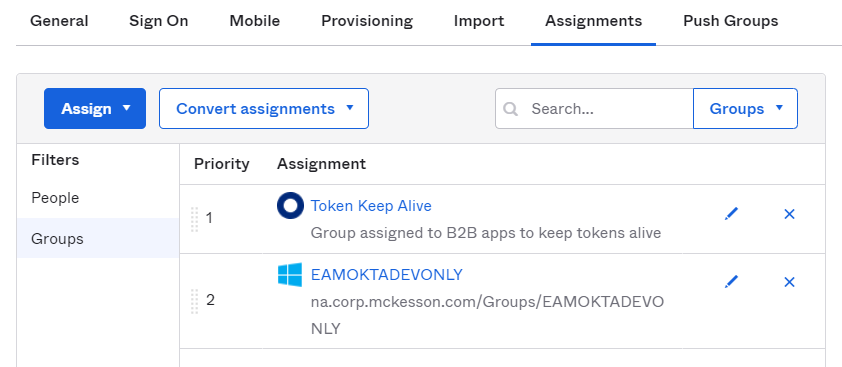
#### Integration



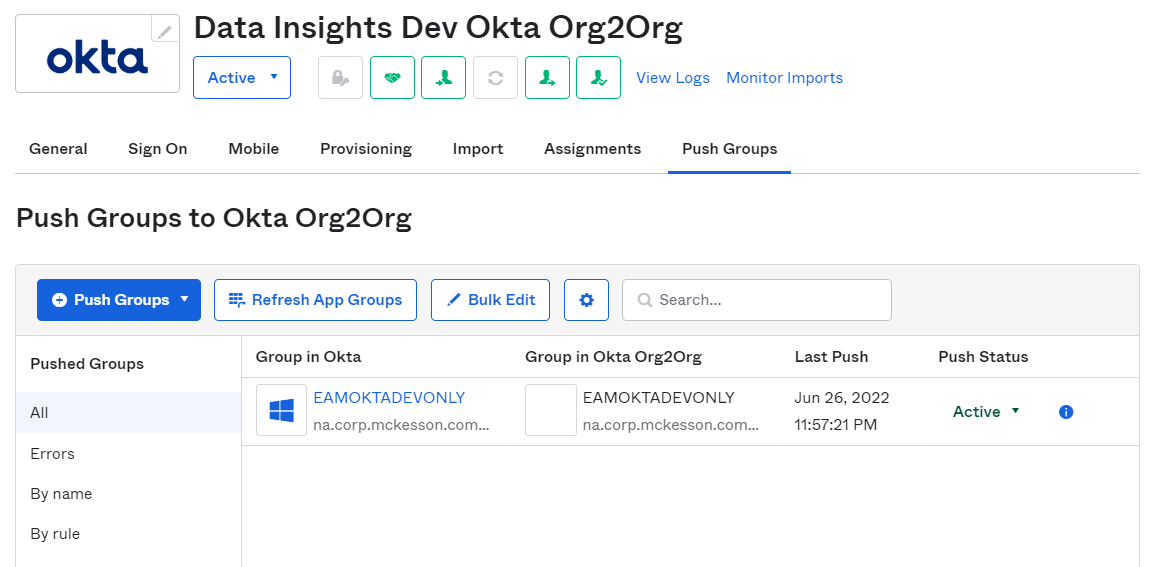
### Import

NA

### Assignments

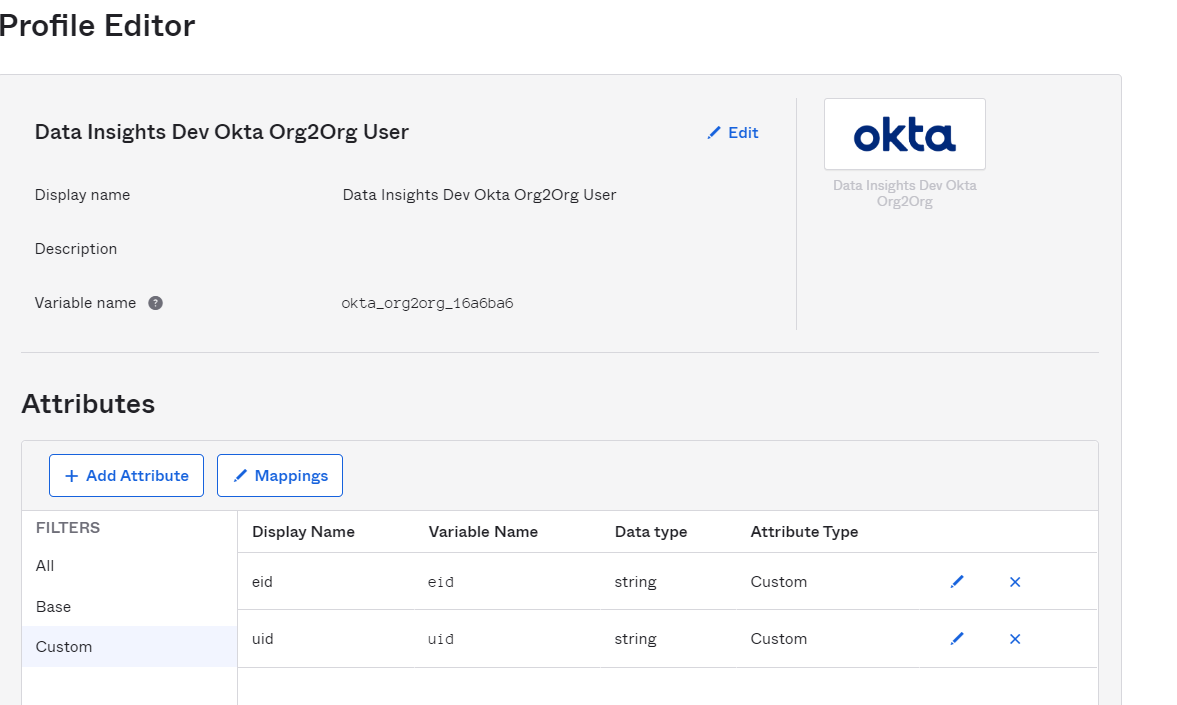


### Push Groups

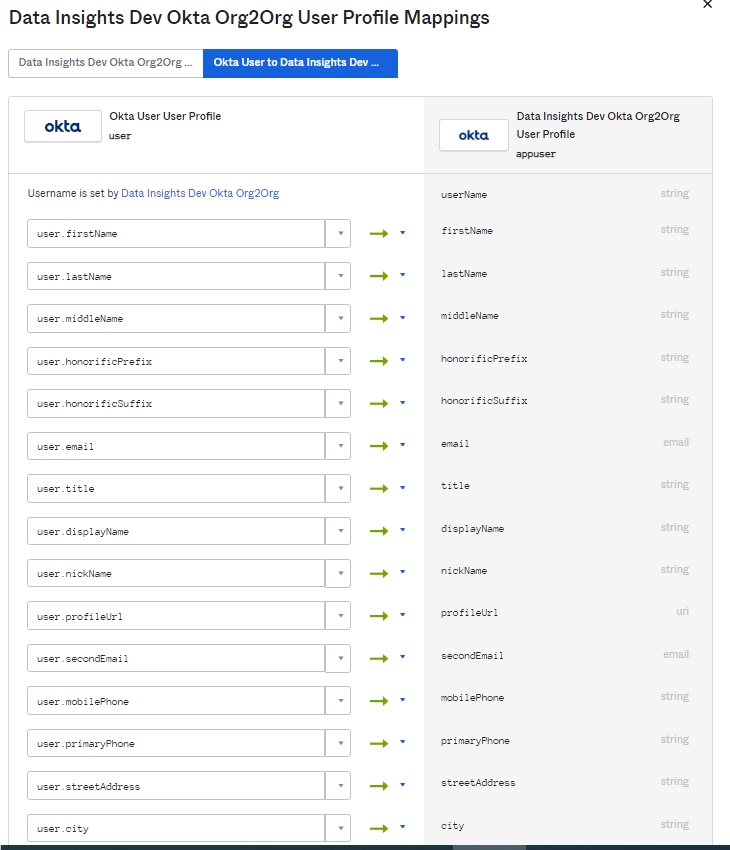


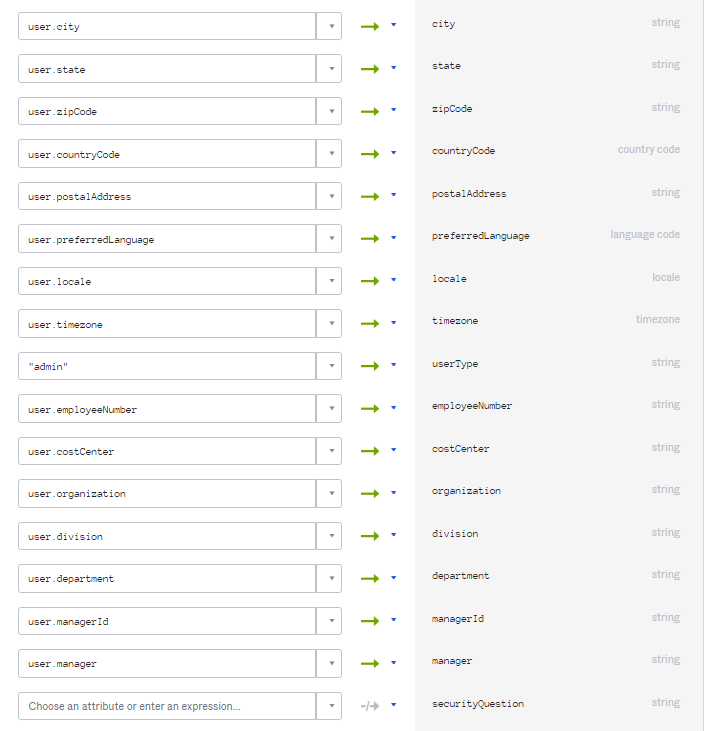
## Profile Editor

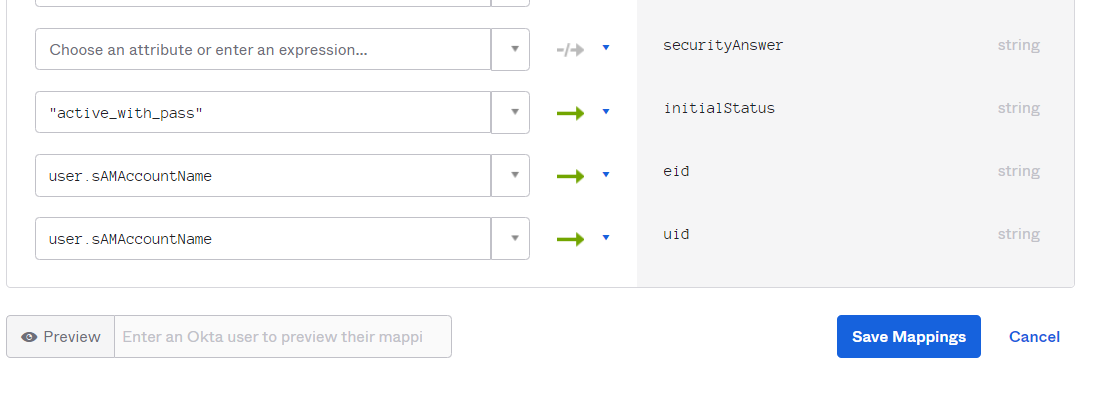
### Add Attribute



### Mappings





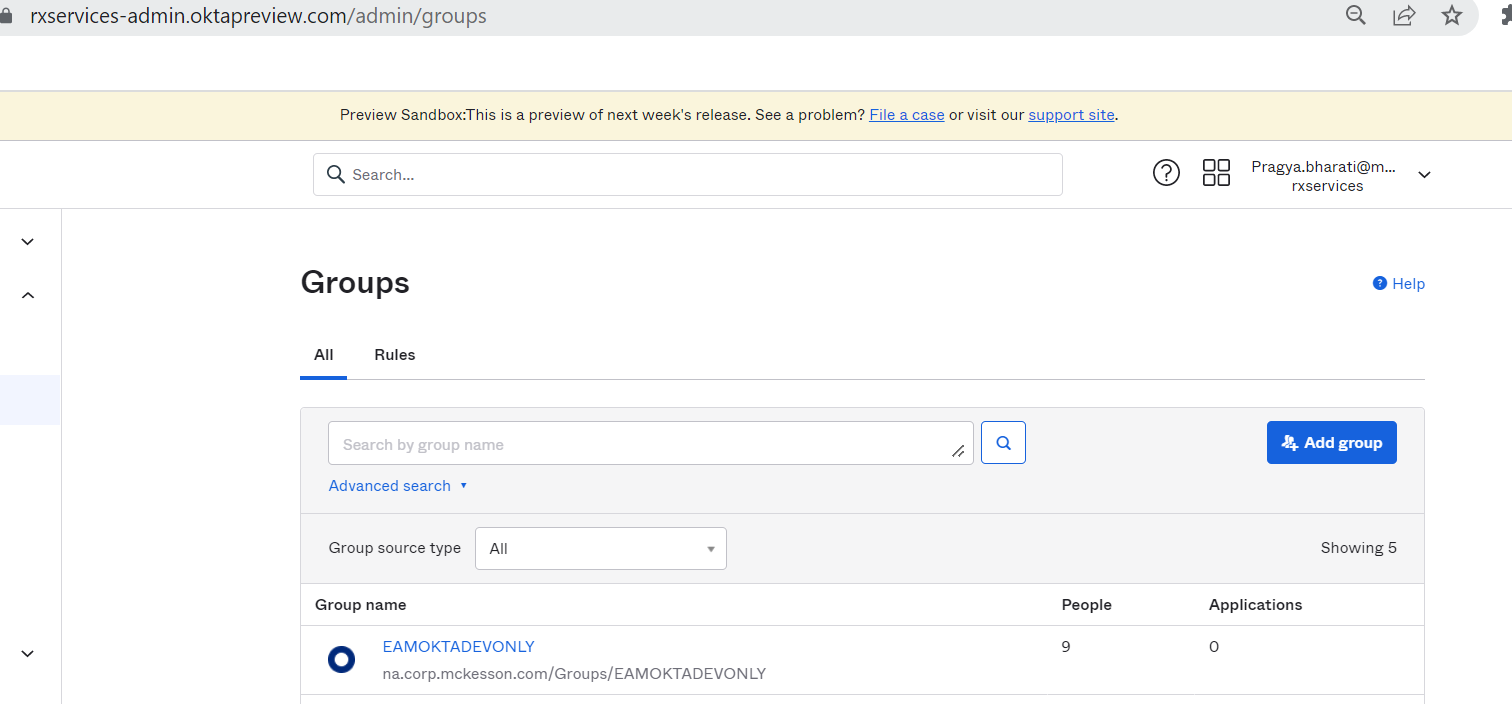


# Okta B2B Tenant Configuration

## Directory

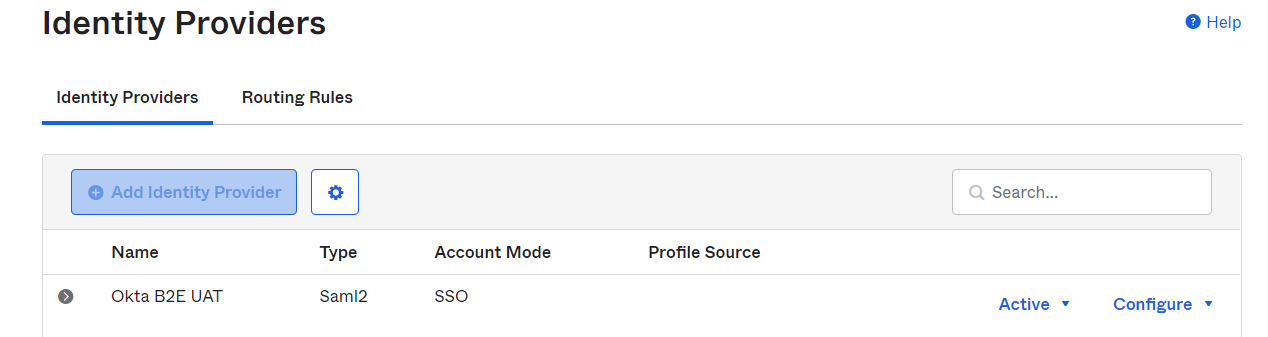
### Groups

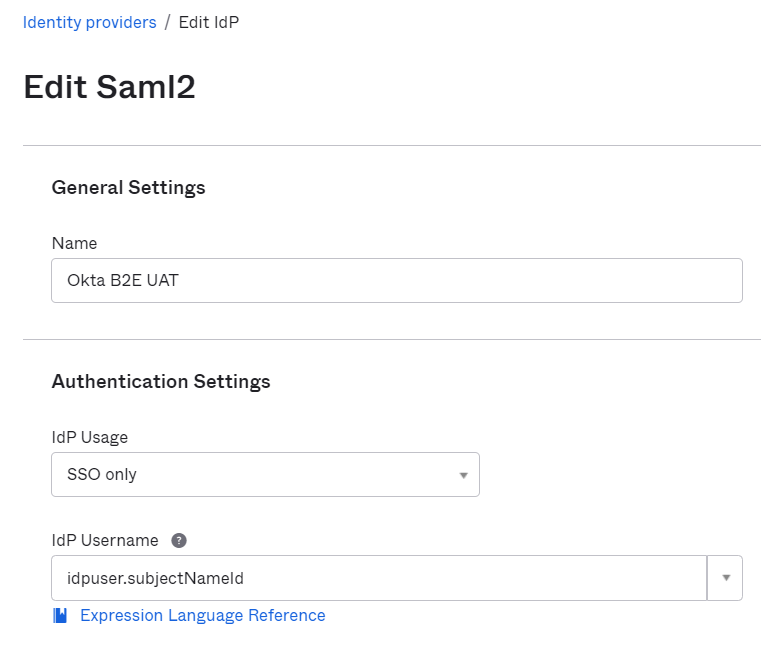
Group and its members are provisioned-

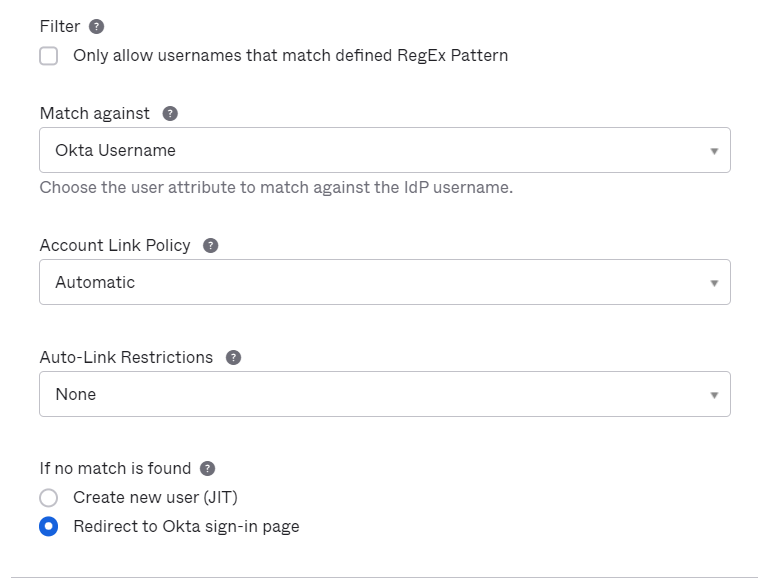


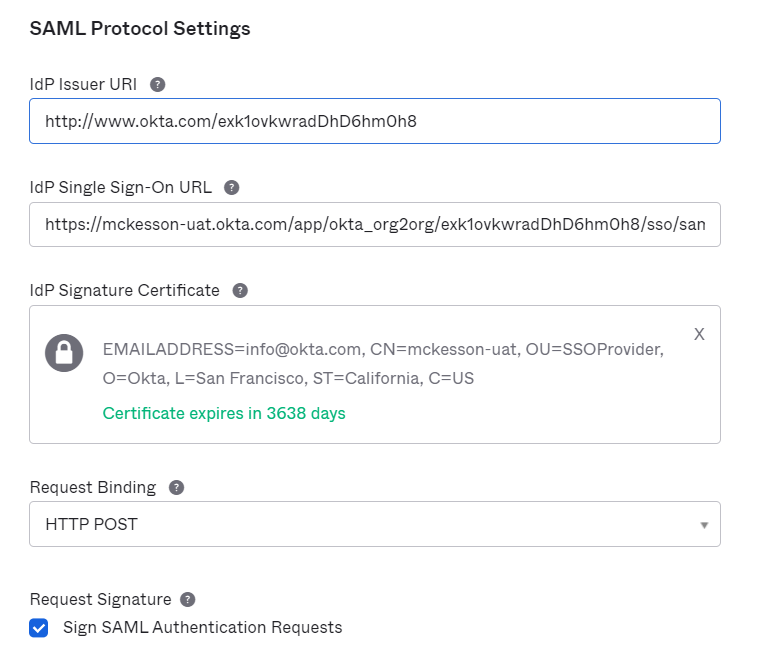
## Identity Providers

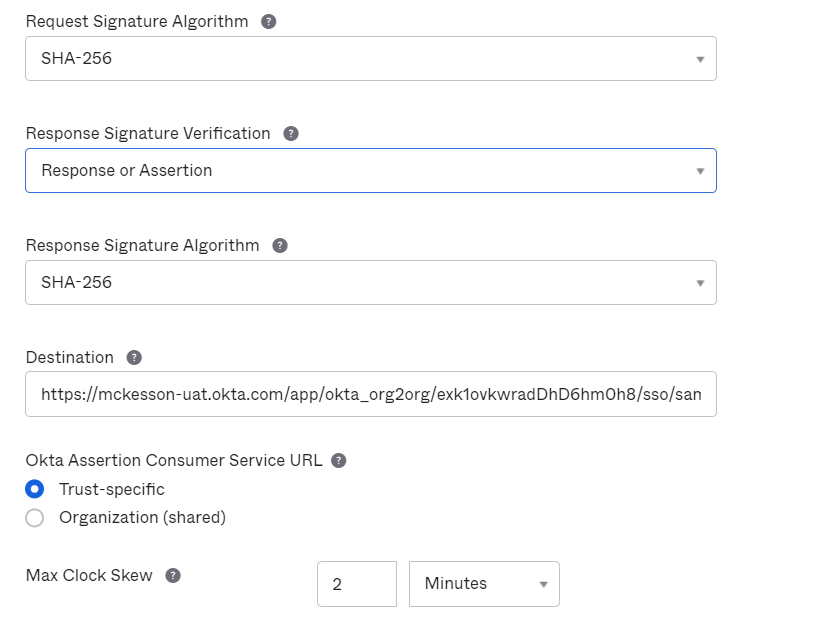
### Identity Providers







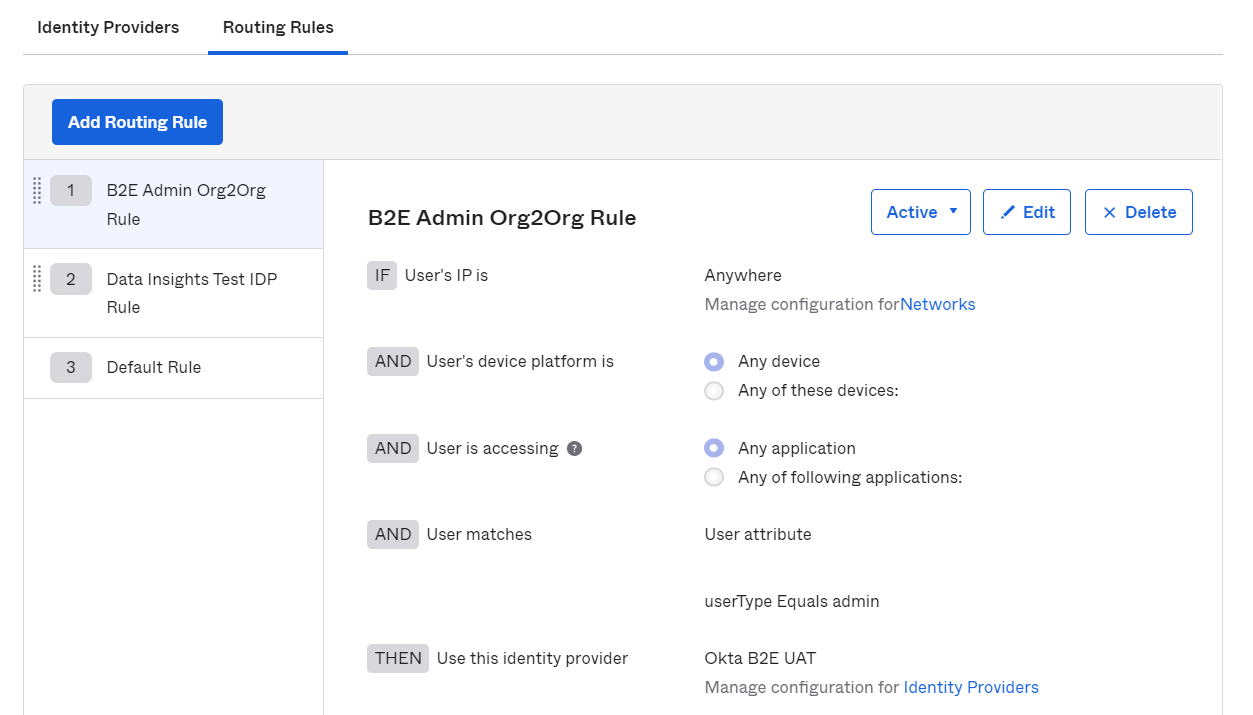




### Routing rules

Follow below filters for access types:

|  |  |
| --- | --- |
| **Access Type** | **Mapping** |
| B2E Admin Access | userType: “Admin” |
| B2E End User Access | userType: “Internal” |

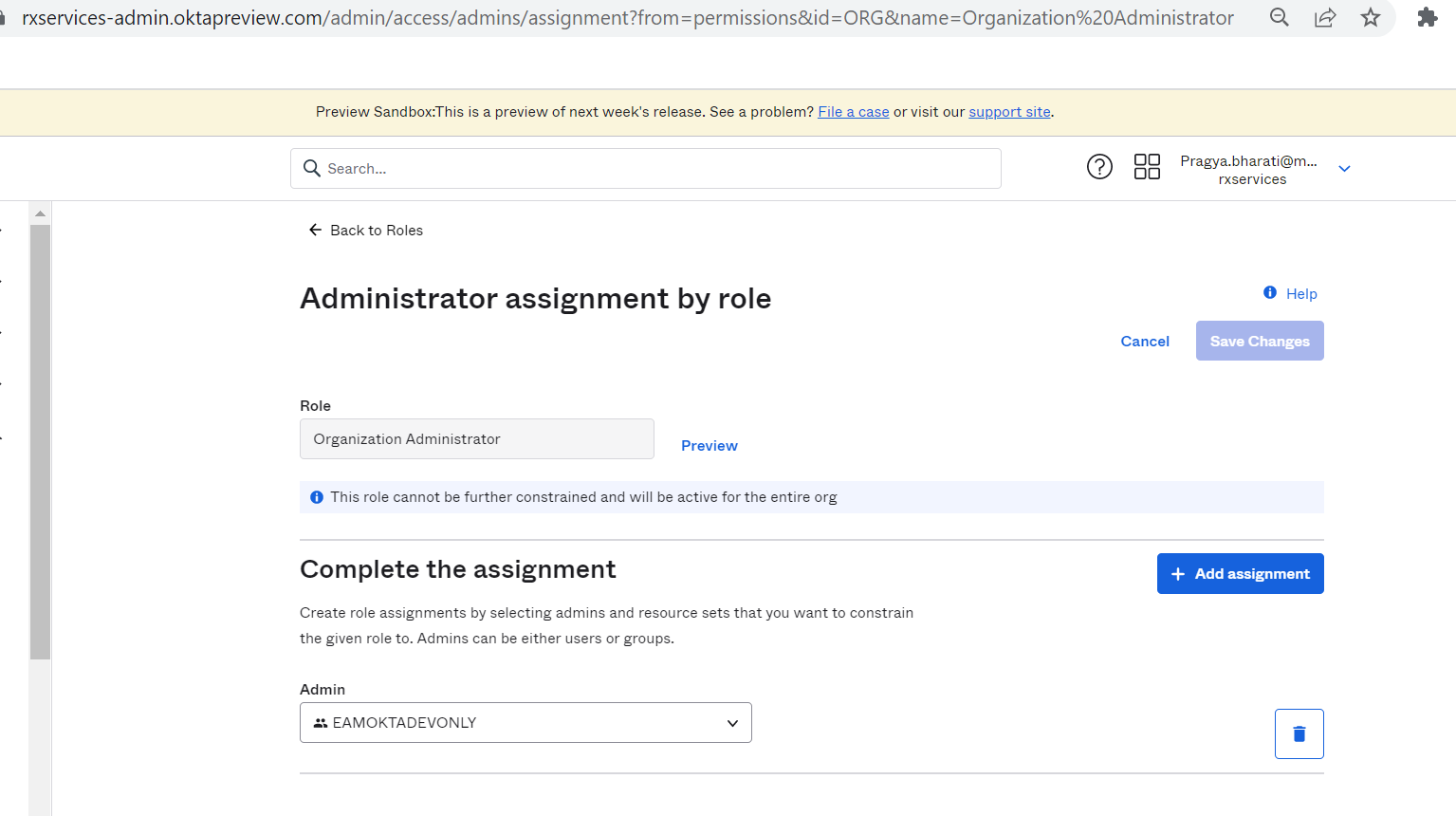


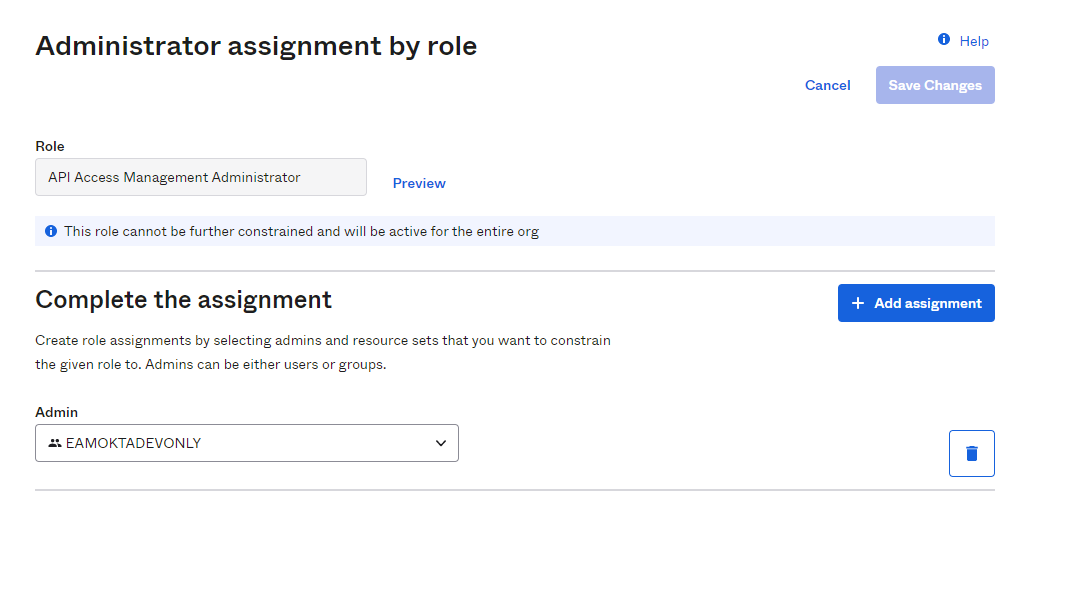
## Administrators

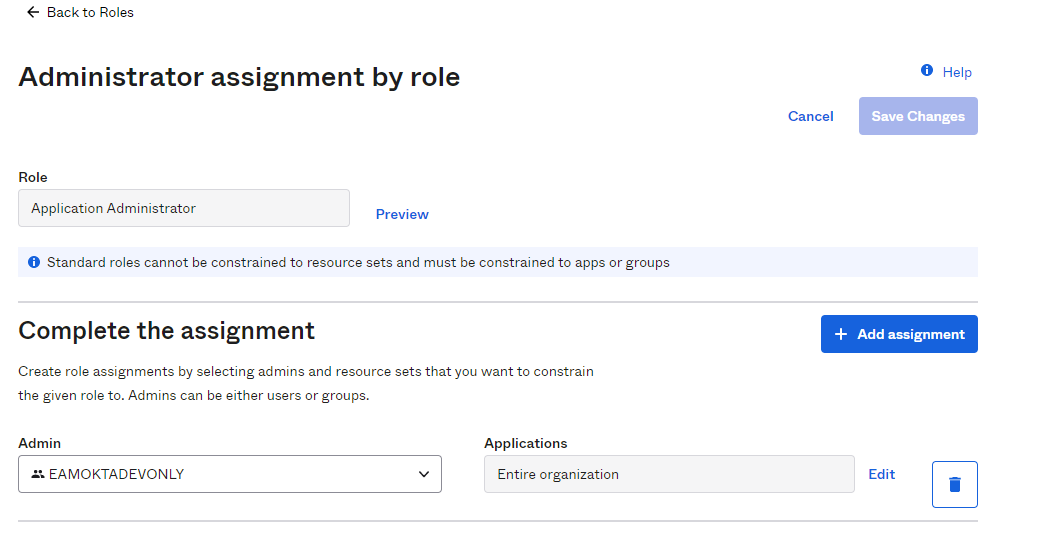
Admin role assignment is only required for admin access Org2Org setup.

### Roles

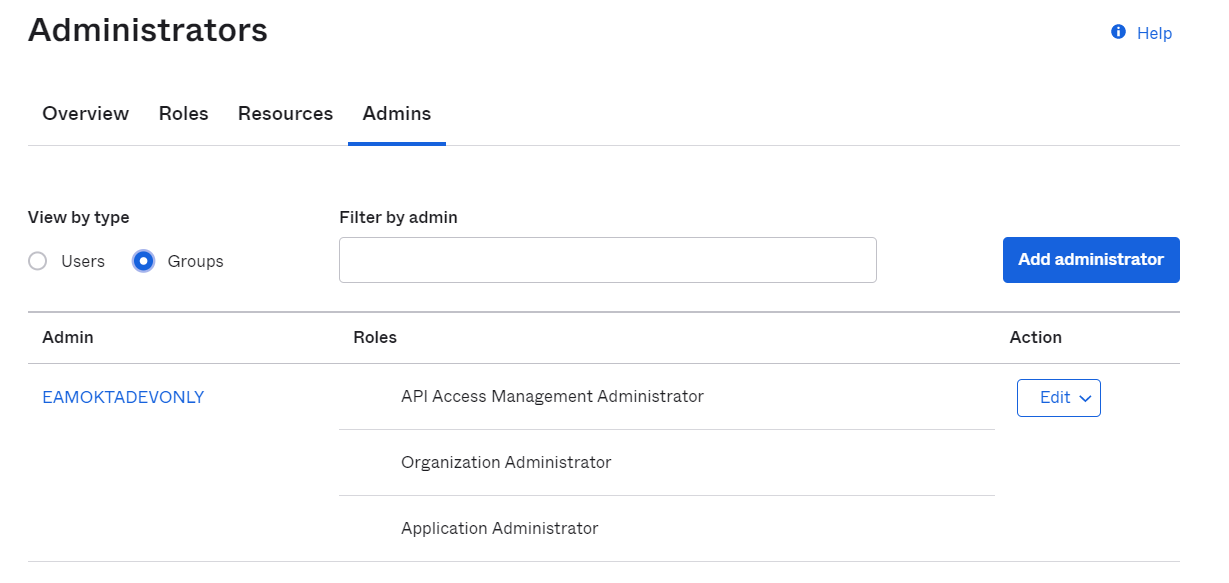
Assign *Organization Admin, Application Admin and API Access Management Administrator* role to EAMOKTADEVONLY group







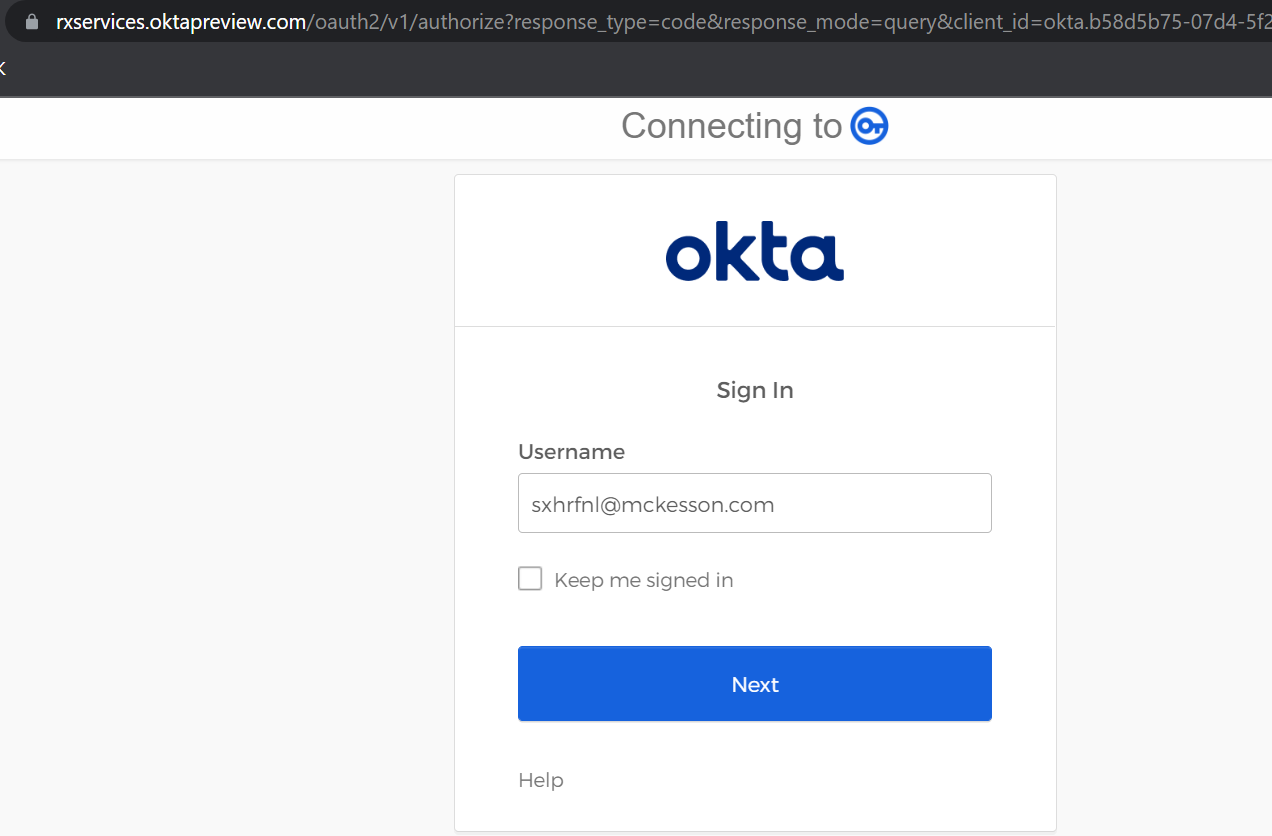
### Admins



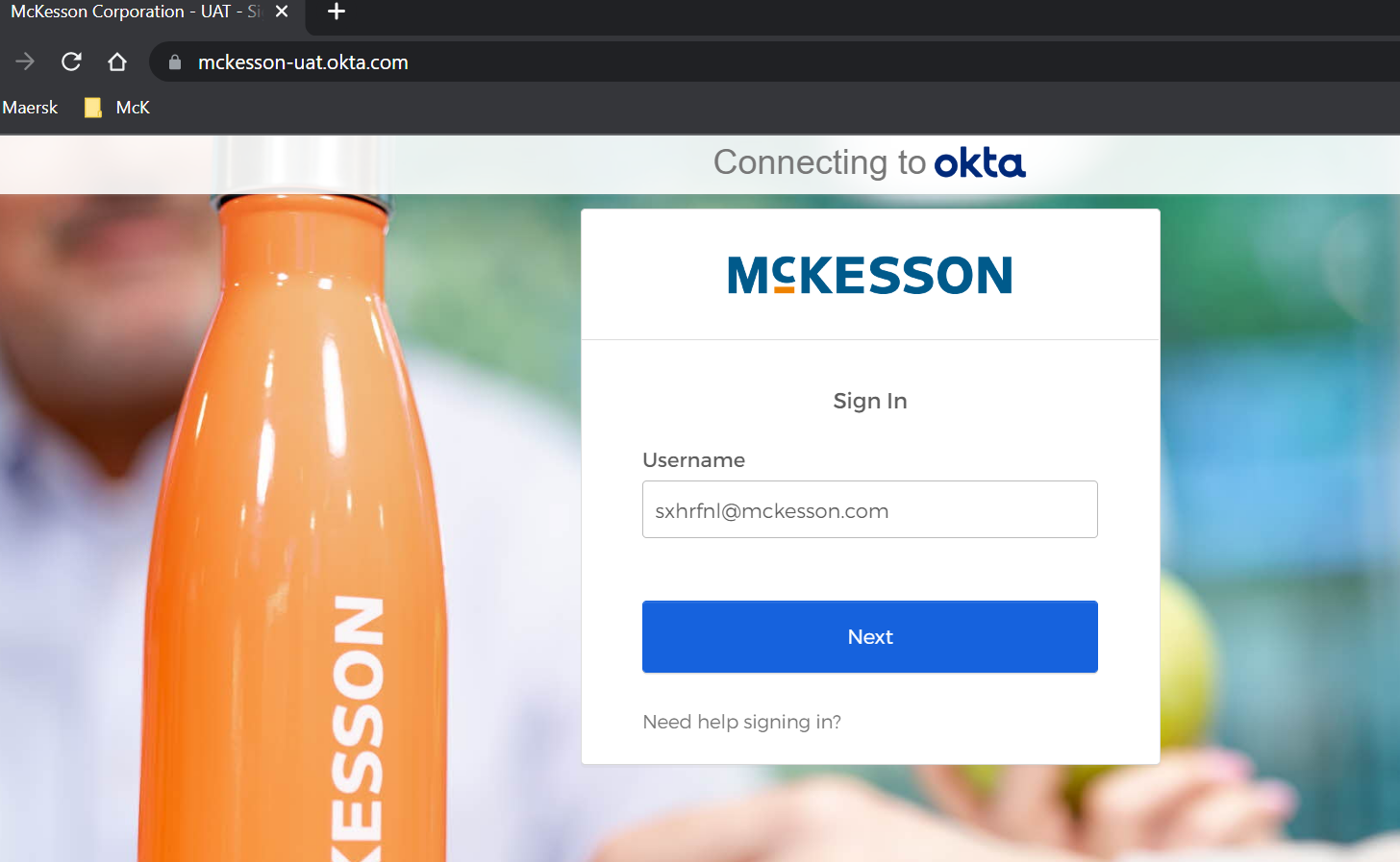
# Test login

## B2E Admin Access

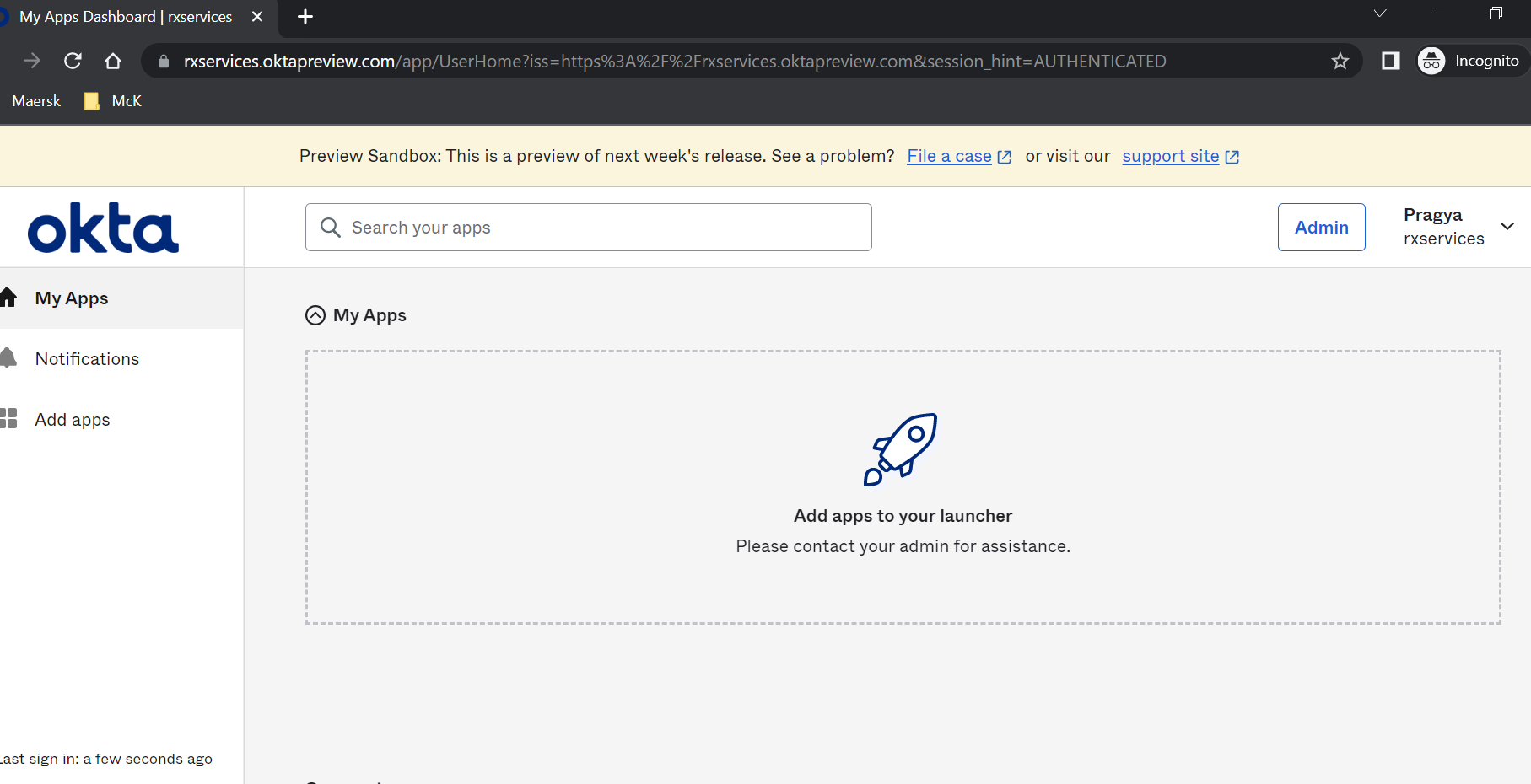
1. Access Okta B2B URL <https://rxservices.oktapreview.com/> and enter sid@mckesson.com



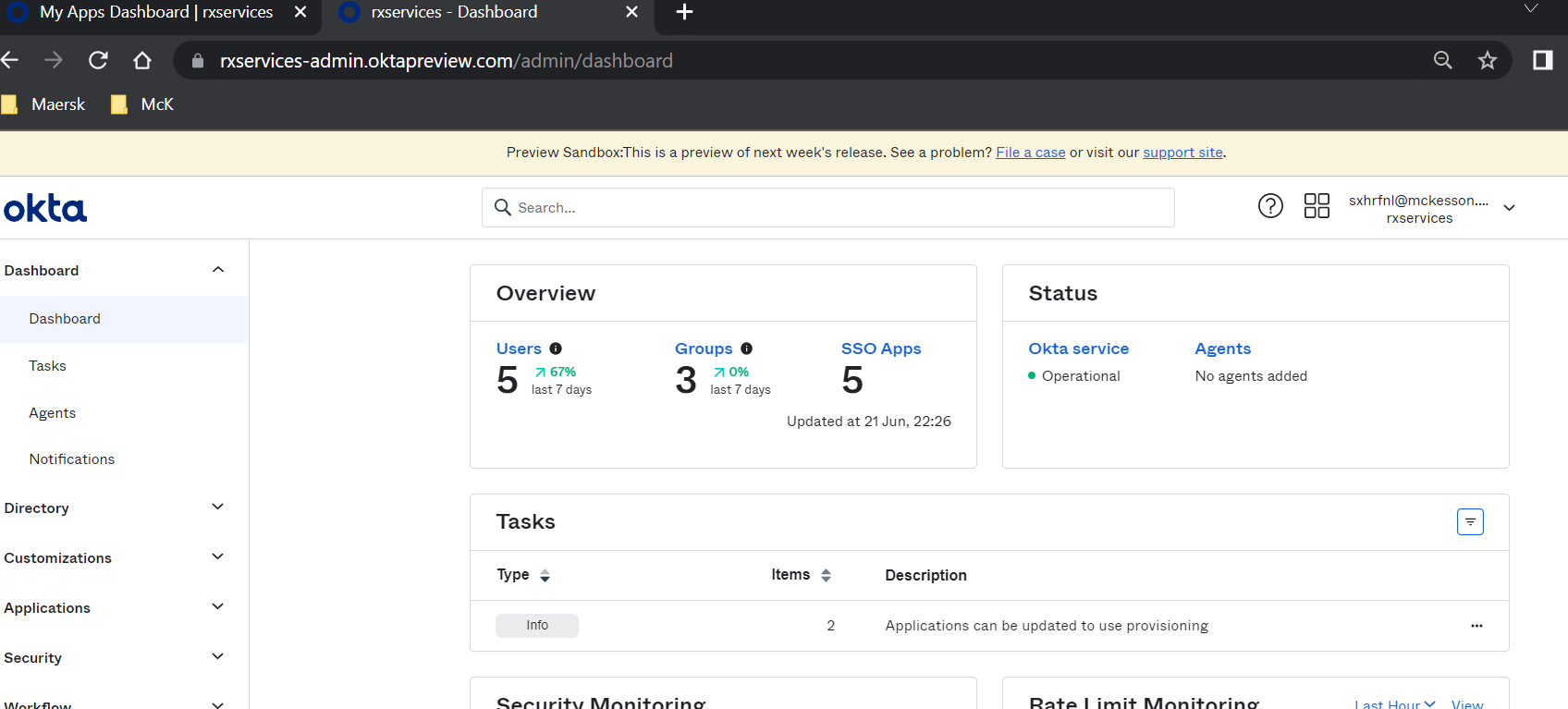
1. Request redirected to B2E UAT login page with auto filled username



1. Login with CyberArk password
2. Verify B2E tenant prompted MFA
3. Verify Okta B2B prompted MFA
4. Login successful in Okta B2B-



1. Test admin access



## B2E End User Access

**NOTE:** Please do NOT change/modify any default policy over any tenant. If any policy (like authentication policy, password policy or MFA policy) required as per application requirement, need to create separately without changing/modifying any default or existing policy.