



Exium Intelligent Cyber Security Mesh

- User Guides

08th February 2021

Integration with OKTA SCIM

Overview

Exium's Intelligent Cybersecurity Mesh™ provides secure access to distributed workforce and IoT devices, protecting businesses from malware, ransomware, phishing, denial of service, and botnet infections in one easy to use cloud service.

From single sign-on to enhanced user provisioning Okta's Exium integration handles users and groups seamless access to Exium. Administrators can easily attach Exium security policy groups to Okta user groups.

The remainder of this guide is focused on enabling you to configure both Exium and Okta to get provisioning up and running for your organization.

1. Supported Features
2. Requirements
3. Configuration Steps
4. Known Issues/Troubleshooting

Features

The following provisioning features are supported by Exium at present:

- Push New Users:
 - Users in Okta that are assigned to the Exium application in Okta are automatically added as members to your workspace in Exium.
- Push Profile Updates:
 - Updates made to the user's profile through OKTA will be pushed to the Exium application.
- Push Groups:
 - Groups and their members in Okta can be pushed to Exium (as Exium user groups and users).
- Push User Deactivation
 - Deactivating the user or disabling the user's access to the application through OKTA will deactivate the user in Exium. In this case, Exium will remove access to service for user, but maintains user's information as inactive user.
- Reactivate Users
 - User accounts can be reactivated in the application.

Presently, Exium does not support the following Okta provisioning features, but may in the future:

- Remove users* (This is supported in Exium, but not by Okta)
- Enhanced group push

Requirements

- SCIM-based user provisioning is available to Exium administrators.
- Administrator has to create a workspace on Exium to get Okta SCIM2.0 Bearer token. In workspace is not created on Exium, please refer <https://exium.net/help-center/> for workspace creation.
- SAML should be provisioned before SCIM provisioning. Please refer https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-Exium.html for SAML provisioning.

Configuration From Exium

On Exium workspace Profile page, Expand “SSO Settings” and Click on ”copy” for “SCIM 2.0 Bearer Token”, as shown below.

The screenshot displays the Exium workspace Profile page. On the left is a navigation sidebar with categories: Dashboards, User Management (Users, Groups), Gateway Management, Policy, Events, Location Policy, and Web Categories. The main content area is titled 'Profile' and contains two columns of settings. The left column is 'Profile Settings' and the right is 'Primary Address'. Below these is the 'SCIM Configuration' section. In this section, the 'SCIM 2.0 Bearer Token' field is highlighted with a red box, and a red arrow points to its 'copy' button. The 'copy' button for the 'SCIM 2.0 Base URL' is also visible. At the bottom left, there is a user profile for 'vuppala' with a 'Settings & Subscriptions' dropdown.

Profile Settings

- Workspace: vuppala
- Workspace ID: de91c7b9-7665-11eb-8332-c674f83e42c9 [copy](#)
- Primary User: chandrashekar.vuppala@vuppala.exium.net
- Default Qos Name: DefaultOrgQoS
- Policy Groups: Select... | v
- Location Policies *: DefaultLocationPolicy x | v

[Edit](#)

Primary Address

- Name*
- Phone*
- Address line 1*
- Address line 2
- Country* | State*
- City* | Postal Code*

[Edit](#)

SCIM Configuration

- SCIM 2.0 Base URL: https://subapi.exium.net/scim [copy](#)
- SCIM 2.0 Bearer Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRuYWV1IjoianVwcGFsYSIsIlNTNT1R5cGUuIjoiPa3RhlwiZXhwIjoxNzQ1NzgzMjUuNDk4LCJpYXQiOiJlMjMTQyNDkyNTEuNTU0OTg [copy](#)

Profile

- Manage Subscription
- vuppala Settings & Subscriptions

Configuration on Okta – Step 1

- Add Exium application to your Okta account
 - Go to **Applications/Applications** tab
 - Click **Add Application**, this will take you to Okta application portal

The screenshot displays the Okta management console. On the left, the navigation menu includes Dashboard, Directory, Applications (highlighted with a red box), Security, Workflow, Reports, and Settings. The main area is titled 'Applications' and features a search bar, three buttons ('Add Application', 'Assign Applications', 'More'), and a table of applications. A red arrow points to the 'Add Application' button.

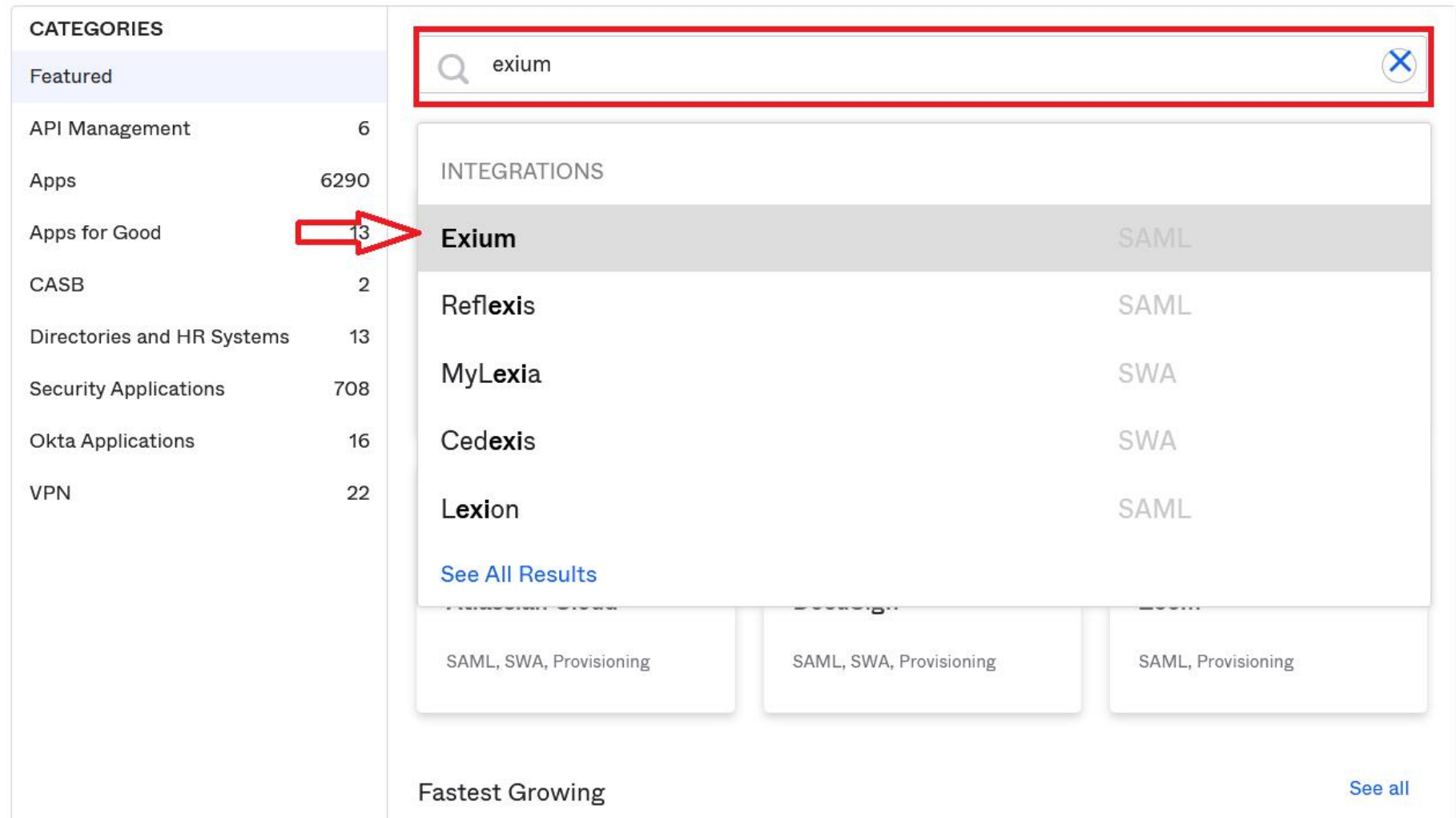
| STATUS | | | |
|----------|---|--|-------------------|
| ACTIVE | 4 | | Exium Sample |
| INACTIVE | 0 | | Exium SASE (SAML) |
| | | | Exium SASE (SCIM) |
| | | | vuppala |

Configuration on Okta – Step2

- Add Exium application to your Okta account
 - In Search bar type “**Exium**”
 - Select **Exium**

Add Application

Create New App



The screenshot shows the 'Add Application' interface in Okta. On the left, there is a 'CATEGORIES' sidebar with a list of categories and their counts. The 'Apps' category has 6290 items. The 'Apps for Good' category has 13 items, which is highlighted with a red arrow. The main area shows a search bar with 'exium' entered. Below the search bar, there is a list of search results under the heading 'INTEGRATIONS'. The first result is 'Exium' with 'SAML' listed next to it. Other results include 'Reflexis' (SAML), 'MyLexia' (SWA), 'Cedexis' (SWA), and 'Lexion' (SAML). At the bottom, there are three filter buttons: 'SAML, SWA, Provisioning', 'SAML, SWA, Provisioning', and 'SAML, Provisioning'. The page also features a 'Fastest Growing' section with a 'See all' link.

| CATEGORIES | Count |
|----------------------------|-------|
| Featured | |
| API Management | 6 |
| Apps | 6290 |
| Apps for Good | 13 |
| CASB | 2 |
| Directories and HR Systems | 13 |
| Security Applications | 708 |
| Okta Applications | 16 |
| VPN | 22 |

Search: exium

| INTEGRATIONS | Protocol |
|--------------|----------|
| Exium | SAML |
| Reflexis | SAML |
| MyLexia | SWA |
| Cedexis | SWA |
| Lexion | SAML |

[See All Results](#)

SAML, SWA, Provisioning | SAML, SWA, Provisioning | SAML, Provisioning

Fastest Growing [See all](#)

Configuration on Okta – Step3

- Add Exium application to your Okta account
 - Click **Add**, the **Exium** app will be added to your Okta account

[← Back to Add Application](#)



Exium

Overview

Add

CATEGORIES

[Security Applications](#)

LAST UPDATE

2021-02-08T09:32:20

Exium's Intelligent Cybersecurity Mesh provides secure access to distributed workforce and IoT devices, protecting businesses from malware, ransomware, phishing, denial of service, and botnet infections in one easy to use cloud service. From single sign-on to enhanced user provisioning Okta's Exium integration handles users and groups seamless access to Exium. Administrators can easily attach Exium security policy groups to Okta user groups.

Capabilities

Access

✓ SAML

OIDC

WS-Federation

SWA

Provisioning

Create

Update

Deactivate

Sync Password

Configuration on Okta – Step4

- After adding app, now configure “**Application Username format**”
 - Go to Exium app “**Sign On**” tab
 - Click Edit
 - Select “**Email**” as “Application username format”
 - Click “**Save**” as shown in image

General Sign On Mobile Provisioning Import Assignments Push Groups

Settings

[Cancel](#)

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0 is the only sign-on option currently supported for this application.

SAML 2.0

Default Relay State
All IDP-initiated requests will include this RelayState.

Attributes (Optional) [Learn More](#)

Disable Force Authentication
Never prompt user to re-authenticate.

[Preview SAML](#)

SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic configuration.

Advanced Sign-on Settings

These fields may be required for a Exium proprietary sign-on option or general setting.

Workspace ID
Enter your Workspace ID. Refer to the Setup Instructions above to obtain this value.

Credentials Details

Application username format

Password reveal Allow users to securely see their password (Recommended)

Password reveal is disabled, since this app is using SAML with no password.

[Save](#)

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Configuration on Okta – Step5

- Configure SCIM Provisioning
 - Go to Exium app “**Provisioning**” tab
 - Click on “**Configure API Integration**” as shown below

General Sign On Mobile **Provisioning** Import Assignments Push Groups

Settings
Integration

i Help text
[Exium: Configuration Guide](#)
Provisioning Certification: Okta Verified
This provisioning integration is partner-built by Exium
Contact partner support: service@exium.net

Provisioning is not enabled
Enable provisioning to automate Exium user account creation, deactivation, and updates.

[Configure API Integration](#)

Configuration on Okta – Step6

- Configure SCIM Provisioning
 - Select “**Enable API integration**”
 - Paste (from Configuration from Exium section) “**API Token**”
 - Click **Save** as shown

General Sign On Mobile Provisioning Import Assignments Push Groups

Settings
Integration

Help text
[Exium: Configuration Guide](#)
Provisioning Certification: Okta Verified
This provisioning integration is partner-built by Exium
Contact partner support: service@exium.net

Cancel

Enable API integration

Enter your Exium credentials to enable user import and provisioning features.

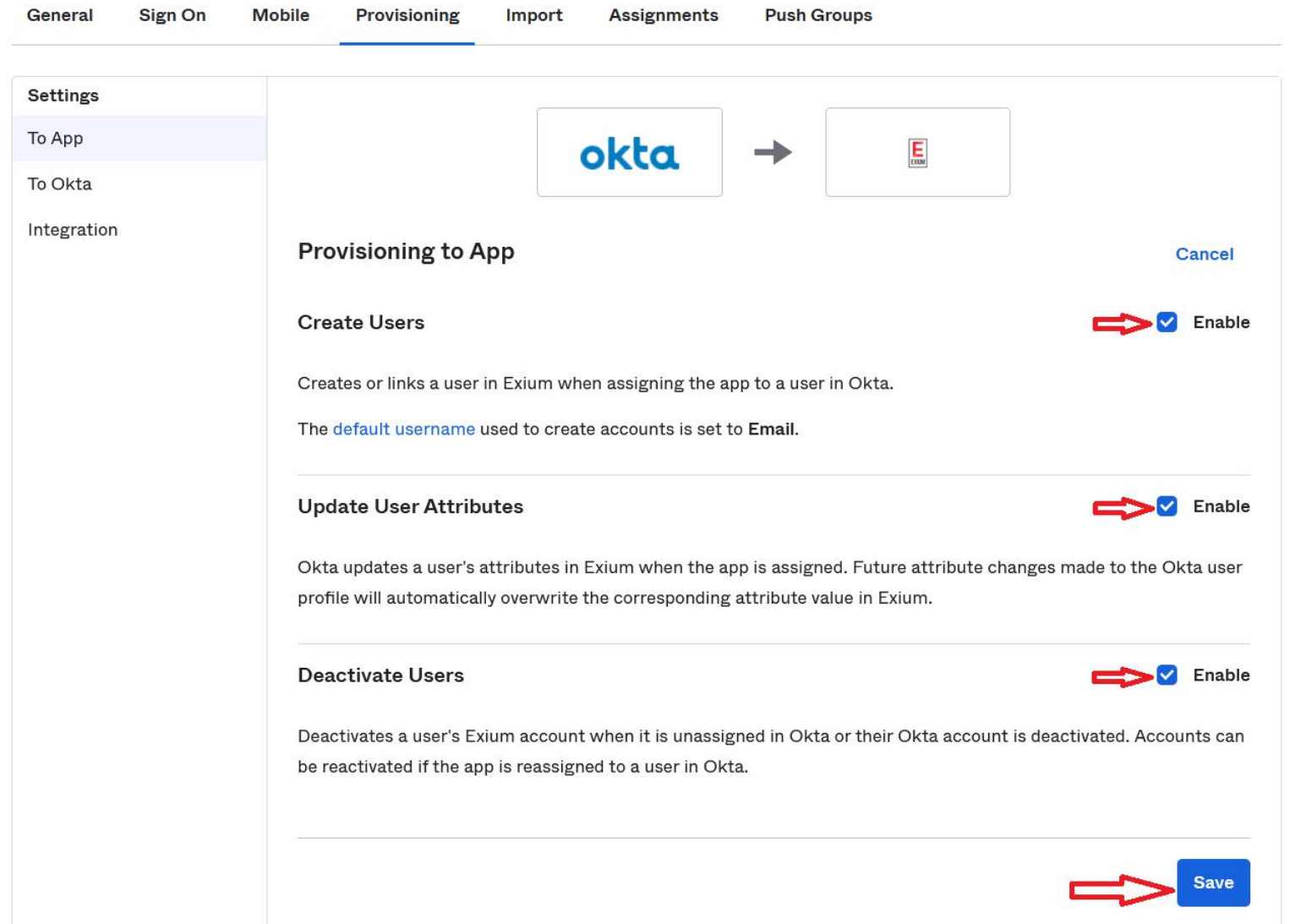
API Token

Test API Credentials

Save

Configuration on Okta – Step7

- After configuration of “API Token”, configure “To APP” Provisioning allowed operations
 - Click on **Edit**
 - Enable **Create Users, Update User Attributes, Deactivate Users** operations
 - Click **Save** as shown



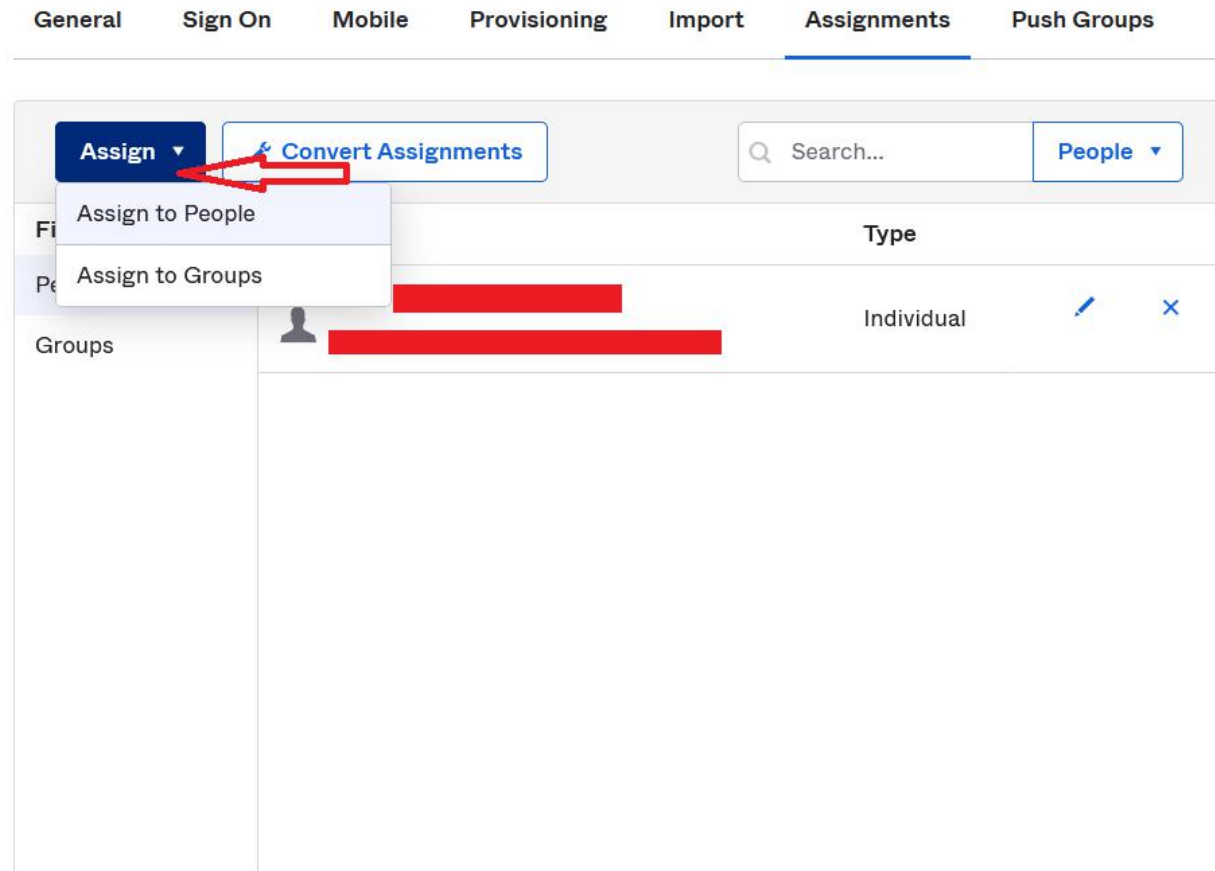
The screenshot shows the Okta Provisioning configuration page for an application. The navigation tabs at the top are General, Sign On, Mobile, Provisioning (selected), Import, Assignments, and Push Groups. On the left, the Settings menu includes To App (selected), To Okta, and Integration. The main content area is titled 'Provisioning to App' and features a diagram showing the 'Okta' logo pointing to the 'Exium' logo. Below this, three provisioning operations are listed, each with a red arrow pointing to its status:

- Create Users**: Enabled (checkbox checked). Description: Creates or links a user in Exium when assigning the app to a user in Okta. The default username used to create accounts is set to **Email**.
- Update User Attributes**: Enabled (checkbox checked).
- Deactivate Users**: Enabled (checkbox checked).

At the bottom right, a red arrow points to the **Save** button. A **Cancel** link is also visible in the top right corner of the main content area.

Configuration on Okta – Step8

- Provisioning/Assigning users/groups to **Exium** service
 - Go to “**Assignments**” tab
 - Click on **Assign**
 - Choose one of the options



Configuration on Okta – Step9

- If you select either Assign Users/ Assign Group, it will open popup
- Click assign corresponding to user
- That will open another popup, to modify user attributes
- Click **“Save and Go Back”**, then click **Done**

Assign Exium Sample to People ×

User Name

Given name

Family name

Middle name

Primary email

Primary email type

Display name

Primary phone

Primary phone type

Address type

Street address

Locality

Region

Postal Code


Country code

Formatted Postal Address

Time zone








User type

Department

 **Save and Go Back** Cancel

Assign Exium Sample to People ×

Q Search...

| | |
|---|---|
|  |  Assign |
|  | Assign |
|  | Assign |
|  | Assign |
|  | Assign |
|  | Assign |

Done

Known Issues/Troubleshooting

- Exium does not support modifications to the username or email address.
- When users are deactivated in Okta, they will be deactivated in Exium. Users will not be able to login and use Exium, but their data will remain available as an 'inactive user'. To permanently delete user data, administrator can do so by logging into Exium workspace.
- When users are added from Exium portal and associate these users to the group created from Okta, Okta will not overwrite of the overall membership and does not makes Okta complete owner of the group.
- The user/group which is created from Exium Admin Portal can be linked to the same user/group added from Okta Portal, but entity(Okta/Exium Portal) which is creating the user/group in the Exium Portal can only delete the user/group. eg. suppose from Okta one group is created and associated to the Exium app in the Okta portal, deleting this group from Exium Portal will not delete the group, only from Okta can be deleted this group.