SCIM Integration

Okta

FastTrack Software

Admin By Request

Table of Contents

Introduction

Admin By Request provides the ability to automatically synchronize data from your Identity Provider (IDP) to your Admin By Request User Portal according to the System for Cross-Domain Identity Management (SCIM) protocol, eliminating the need for manual entering and managing individual users on the Admin By Request side. This process manual provides a step-by-step guide on how to enable and configure the integration and provision users and groups in your User Portal with Okta.

Assumptions and Limitations

This implementation is targeted towards Admin By Request Portal users (i.e., company administrators who have access to the User Portal). It does not integrate with endpoint users.

The tasks described in this manual assume that the user has access to and is familiar with Okta, the Admin By Request User Portal, and features of the software (e.g., Inventory, Requests, etc.).

Breakdown of Tasks

Eight tasks are covered in this manual:

1. Task A: Enable SCIM
2. Task B: Define Group-Based Roles
3. Task C: Create Okta Application
4. Task D: Set up Single Sign-On
5. Task E: Set up Provisioning
6. Task F: Assign Users and Groups
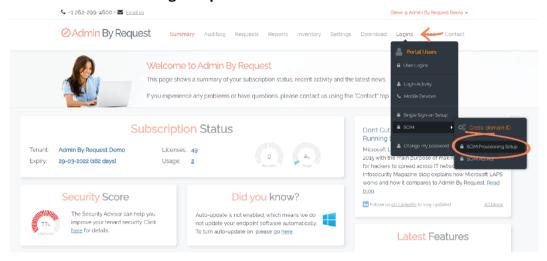7. Task G: Start Provisioning
8. Task H: View Data in User Portal

📝 **NOTE:** Before you begin, we recommend you have a tab open in your Admin By Request User Portal and a second tab open in your Okta portal, as the tasks listed above switch back and forward frequently between the two.
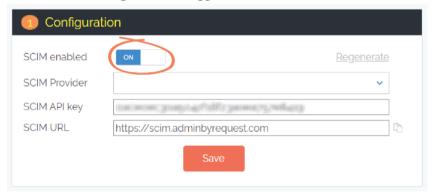
Integration Tasks

Task A: Enable SCIM

The first task of this process involves enabling the integration in the Admin By Request User Portal.
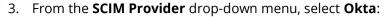
1. In your Admin By Request User Portal, locate **Logins** in the top menu and navigate to **SCIM** > **SCIM Provisioning Setup**:
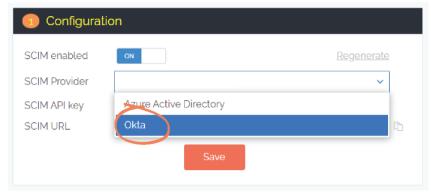

2. In section **1. Configuration**, toggle **SCIM enabled** to **ON**:

> 📝 **NOTE:** This action generates an API key (blurred out in this document), which appears in the **SCIM API key** field. Using the API key is covered in Task D.

3. From the **SCIM Provider** drop-down menu, select **Okta**:
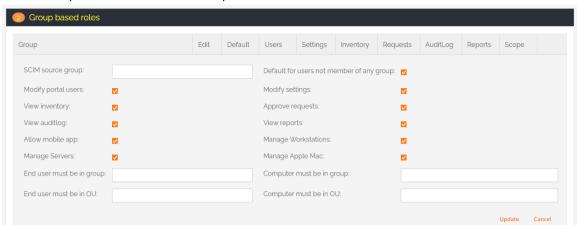

4. Click **Save**:

📝 **NOTE:** Whenever the **Save** button is selected in the Admin By Request User Portal, a green icon appears next to the button when the action is successfully completed.

Task B: Define Group-Based Roles

Admin By Request's SCIM implementation provides the ability to define rules about what synchronized users have access to within the User Portal, based on their SCIM source group (i.e., their group in the IDP).

This means that if you don't want all imported users having access to everything within the User Portal, you can create a Group-Based Role for each Okta group specifying exactly what the users in that group do and do not have access to. As soon as users are synchronized to Admin By Request, their designated permissions are applied.

If you do not create any Group-Based Roles, all synchronized users will have complete access to the User Portal.

The filter options available for Group-Based Roles are as follows:

- **SCIM source group** – This refers to the source group in the IDP (i.e., Okta). Whatever group is typed here needs to match the name of a group in Okta.

- **Default for users not member of any group** – When checked, the permissions defined for this Role become the 'default' permissions, applying to all users who aren't assigned any of the other Group-Based Roles defined for other groups. This checkbox can only be applied to one Group-Based Role.

The checkbox properties such as **Modify Settings**, **View Auditlog**, and **Manage workstations** refer to the various features in Admin By Request. If checked, users assigned the Role have access to the respective feature / can do the specified action.

The four textboxes (**End user** and **Computer** etc.) are used to filter out end point data. Here you can specify IDP groups or OUs (Organizational Units) of end users and / or computers, so that Admin By Request Portal users assigned this Group-Based Role only have access to end users and / or computers that fall into those groups / OUs.

📝 **NOTE:** You can specify multiple groups or OUs in these textboxes, separated by commas.

Before creating Group-Based Roles for specific groups, we recommend that you create a Default Role specifying permissions for the 'general' user; these are all synchronized users who are not members of any of the other groups that you have defined Group-Based Roles for. When synchronized, they get assigned the Default permissions in the User Portal (demonstrated in the example below).

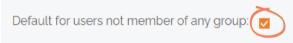## Create Default Group-Based Role

1. In the Admin By Request **SCIM Provisioning Setup** page, section **2. Group based roles**, select the **New entry** button:
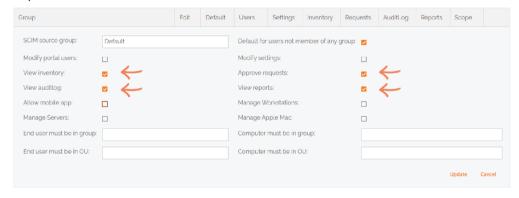

2. In the **SCIM source group** textbox, type the desired name for this group – this example uses *Default*:

3. Ensure the **Default for users not member of any group** checkbox is checked:

> ⚠️ **IMPORTANT:** Only one Group-Based Role can have this property checked, i.e., there can only be one set of default permissions that users without any other Group-Based Role are assigned.

4. Use the filters to define default permissions. In this example, permissions for default users include viewing the Inventory, Auditlog, and Reports, and Approving requests:
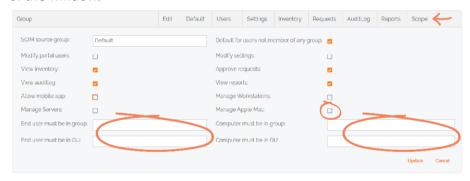

5. Click the **Update** button to save the Role:

6. To **Edit** or **Delete** the rule, use the respective buttons to the left and right of the eight filter columns:

> 📝 **NOTE:** The first seven filter columns correspond to their matching checkbox in the Edit window (i.e., **Default** to **Reports**), however, the **Scope** checkbox corresponds to multiple properties: the **Manage Apple Mac** checkbox and the **End user** and **Computer** textboxes at the bottom of the window:
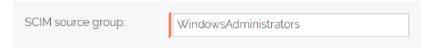

The process for assigning Roles with specific permissions to actual IDP groups follows a similar set of steps to those described above. The section below uses a common example to illustrate how Group-Based Roles could be applied.

Create Group-Based Role for Windows Admins

You have a group in Okta called 'WindowsAdministrators' whose members only require access to Windows-related data. You therefore want to prevent all users in this group from accessing Mac data in the Admin By Request User Portal (e.g., Inventory, Requests and Auditlogs from Mac devices / users, etc.). The solution is to create a Group-Based Role which filters out Mac access for members of the WindowsAdministrators source group.

1. After creating a **New entry** in the **SCIM source group** textbox, type the name of the IDP source group you want to define specific permissions for – in this example, *WindowsAdministrators*:
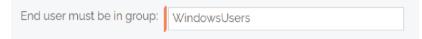

> 📝 **NOTE:** If you have created a Default group as described above, the **Default for users not member of any group** checkbox will automatically be unchecked when you come to create another Group-Based Role, as this property can only be applied once.

2. Use the checkboxes to filter out the source group's access to the appropriate features. For this example, uncheck the **Manage Apple Mac** checkbox to remove Mac access for the *WindowsAdministrators* source group:

> 📝 **NOTE:** You could also use any of the other Scope textboxes to ensure the *WindowsAdministrators* group has the correct permissions. For example:
>
> - If you have a group in Okta for Windows end users called *WindowsUsers*, you could type this group name into the **End user must be in group** textbox, which would prevent the *WindowsAdministrators* source group from seeing any data other than that of end users in the *WindowsUsers* Okta group:

3. Click the **Update** button to save the Role. When users in the *WindowsAdministrators* Okta group are synchronized, they will only have the permissions defined in this Role within the Admin By Request User Portal.
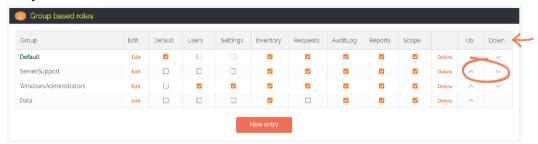

The Group-Based Roles appear in the list according to the order they were created: the first appearing at the top of the list, and the most recent getting added to the bottom. If a user belongs to multiple groups – all of which have Group-Based Roles defined – the first Role in the list will apply for that user.

> 📝 **NOTE:** Four Roles have been created in the example below with the following properties checked:
>
> - **Default** – *Default, Inventory, Requests, Auditlog, Reports, Scope*.
> - **ServerSupport** – *Inventory, Requests, Auditlog, Reports, Scope*.
> - **WindowsAdministrators** – *Users, Settings, Inventory, Requests, Auditlog, Reports, Scope*.
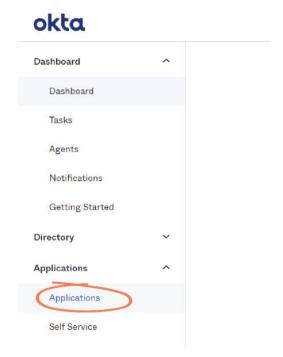> - **Data** – *Inventory, Auditlog, Reports, Scope*.

To change the order of Roles in the list, use the up and down arrows to the right of each entry:
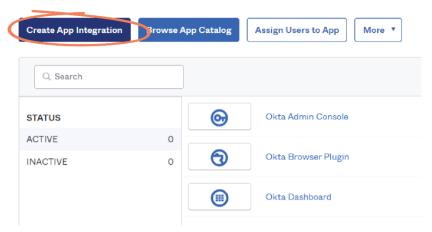

Task C: Create Okta Application

Task C in the integration process involves creating an Admin By Request application on the IDP side (i.e., Okta) which acts as the SCIM connector.

1. Log in to your Okta portal, select the **Applications** drop-down from the left-hand menu and click **Applications**:
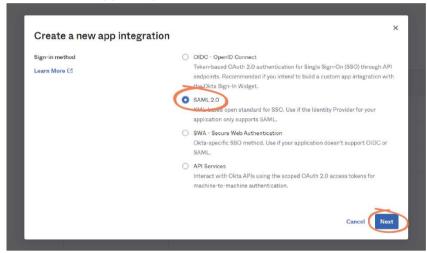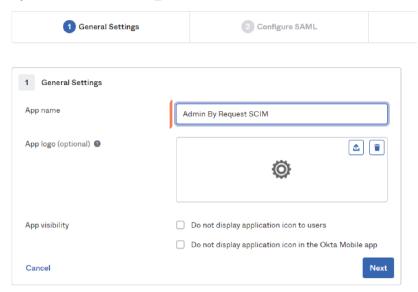
2. Click the **Create App Integration** button:

3. In the **Create App Integration** window, select the **SAML 2.0** radio button and click **Next**:

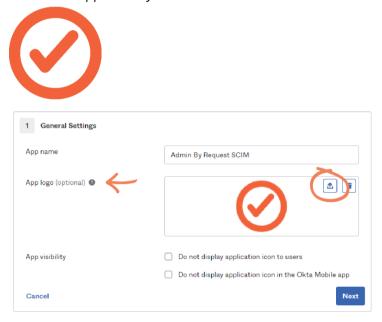4. In the **General Settings** tab of the **Create SAML Integration** page, type *Admin By Request SCIM* in the **App Name** textbox:

> 📋 **NOTE:** The two **App Visibility** checkboxes are optional, as is adding an **App logo**. However, we recommend using the Admin By Request logo image below to ensure the app is easily identifiable:
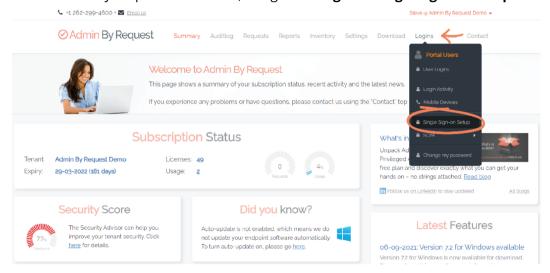

5. Click **Next** to proceed to SAML configuration, covered in the next task (i.e., Task D):

Task D: Set up Single Sign-On

The Okta SCIM integration requires Single Sign-On (SSO) to be configured for Admin By Request before provisioning can occur. Task D covers setting up SSO.

1. In the Admin By Request User Portal, navigate to **Logins** > **Single Sign-On Setup**:
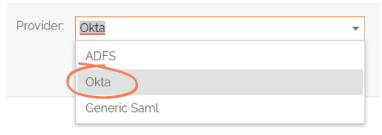

2. In section **1. Create SAML Single sign-on** section, select the **New entry** button:

> 📝 **NOTE:** If this is your first SAML Single sign-on entry, there will be no sections on the page other than **1. Create SAML Single Sign-on**. Further sections appear after you create at least one entry here.

3. Type your desired name in the **Name (e.g., domain)** textbox – this example uses *hotsmudge.com*:

4. From the **Provider** drop-down menu, select **Okta**:
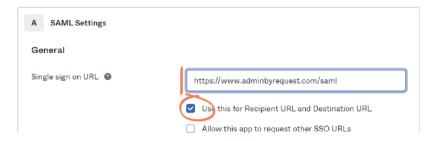
5. Click **Update**:

6. In section **2. Add Identity Provider (IDP) Metadata**, select the SAML Single sign-on entry you have just created from the **Name** drop-down menu – in this example, *hotsmudge.com*:
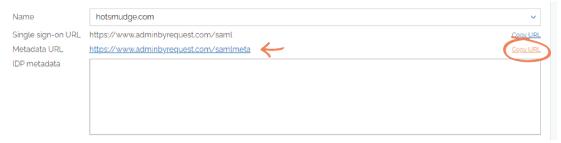

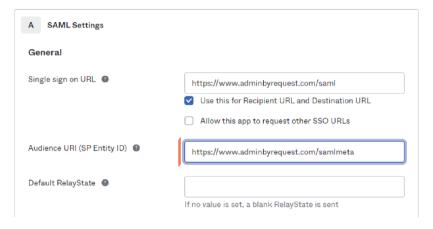7. Use the **Copy URL** button to copy the **Single sign-on URL**: [Copy buttons aren't working]

📝 **NOTE:** Click **OK** to dismiss the confirmation pop-up that appears.

8. In the **SAML Settings** page in Okta, paste the URL in the first textbox: **Single sign-on URL**, and ensure the **Use this for Recipient URL and Destination URL** checkbox is checked:

9. Go back to your Admin By Request User Portal, copy the **Metadata URL**:
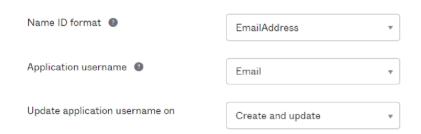

10. In Okta, paste the URL in the **Audience URI (SP Entity ID)** textbox:

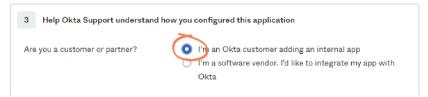📝 **NOTE:** Leave the **Default Relay State** field blank.

11. Use the drop-down menus to select the following for each field:

- **Name ID format** = *EmailAddress*
- **Application username** = *Email*
- **Update application username on** = *Create and update*

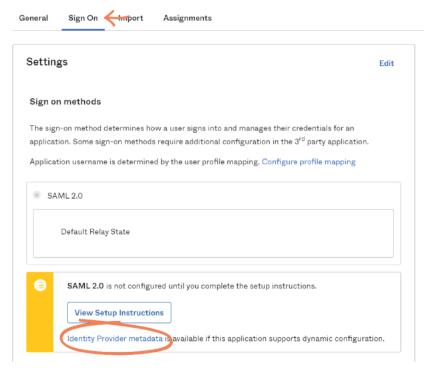12. Scroll to the bottom of the page and click **Next**:

13. Next to **Are you a customer or partner** select **I'm an Okta customer adding an internal app**:

📝 **NOTE:** This action displays a new section of questions. These are optional, and not required for the Admin By Request integration.

14. Scroll to the bottom of the page and click **Finish**. This action opens the application page in the next step:
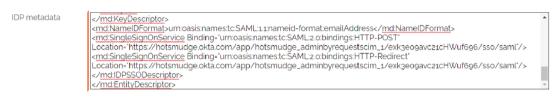

15. In the application page, ensure you are in the **Sign On** tab in the top menu. Scroll down and select the **Identity Provider metadata** button:

16. The metadata opens in a new window. Highlight and copy it:

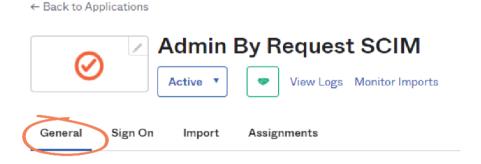17. In your Admin By Request User Portal, paste the metadata in the **IDP metadata** textbox:
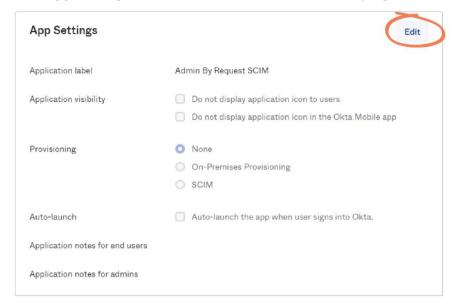

18. Click **Save**:

Task E: Set up Provisioning

This task involves connecting the newly created SCIM app to the Admin By Request SCIM endpoint.

1. In your Okta portal, click into the **General** tab in the top menu of the **Admin By Request SCIM** application page:
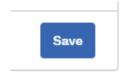
2. In the **App Settings** screen, click the **Edit** button in the top right-hand corner:

3. Next to **Provisioning**, select the **SCIM** radio button:

📋 **NOTE:** The other fields in this section can be left blank.
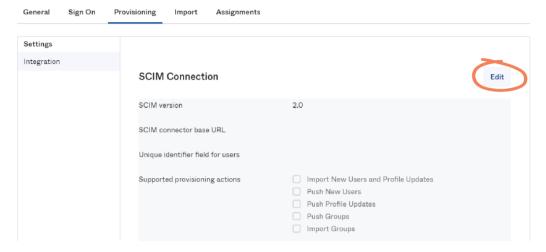
4. Click **Save**:

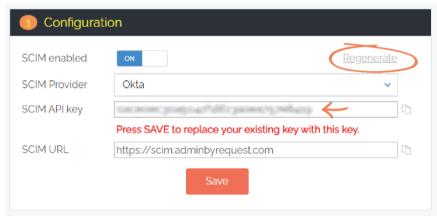📋 **NOTE:** This action creates a new **Provisioning** tab in the top menu.
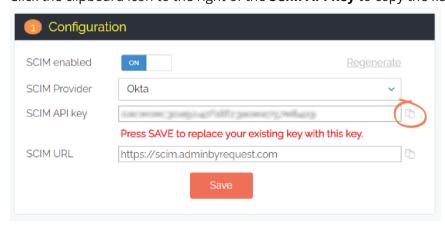
5. Click into the **Provisioning** tab:

📝 **NOTE:** A **Testing Connector Configuration** window appears. This window could remain for up to 30 seconds.

6. In the **SCIM Connection** screen, select the **Edit** button from the top right-hand corner:

7. In your Admin By Request User Portal, navigate to the **SCIM Provisioning Setup** page and select the **Regenerate** button in section **1. Configuration**, to generate a new API key:

8. Click the clipboard icon to the right of the **SCIM API key** to copy the key:
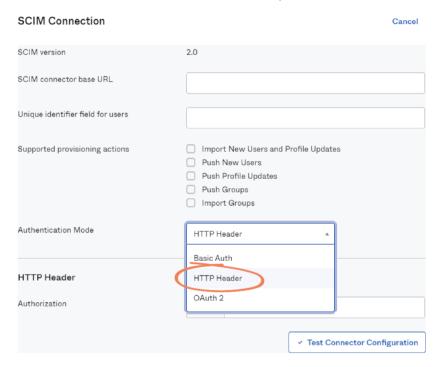
NOTE: Click **OK** to dismiss the confirmation pop-up.

9. Click **Save** to ensure the new API key is used:

> Save ✓

IMPORTANT: Do not click the **Save** button until you have copied the API key. Doing so will hide the key and it will then need to be regenerated before it can be copied. However, it is imperative that you save *after* copying the API key, to ensure this key is used in the SCIM integration:

10. In Okta, from the **Authentication Mode** drop-down menu, select **HTTP Header**

SCIM Connection   Cancel

SCIM version	2.0
SCIM connector base URL	
Unique identifier field for users	
Supported provisioning actions	☐ Import New Users and Profile Updates
	☐ Push New Users
	☐ Push Profile Updates
	☐ Push Groups
	☐ Import Groups
Authentication Mode	HTTP Header ▲

Basic Auth
HTTP Header
OAuth 2

HTTP Header

Authorization

✓ Test Connector Configuration

11. Paste the API key copied from your Admin By Request User Portal into the **Token** textbox next to **Authorization | Bearer**:

HTTP Header

Authorization   Bearer ••••••••••••••••••••••••••••••

✓ Test Connector Configuration

12. In your Admin By Request User Portal, copy the **SCIM URL**:

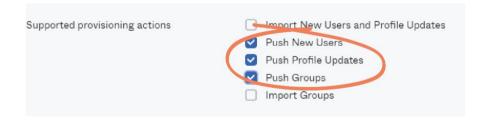13. In Okta, paste the URL into the **SCIM connector base URL** textbox:

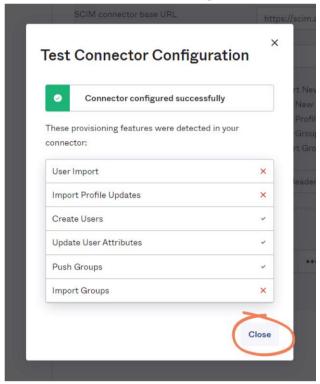14. In the **Unique identifier field for users** textbox, type *email*:

15. Under **Supported provisioning actions**, enable all of the Push actions by checking the following three checkboxes:

- **Push New Users**
- **Push Profile Updates**
- **Push Groups**

16. Click the **Test Connector Configuration** button:

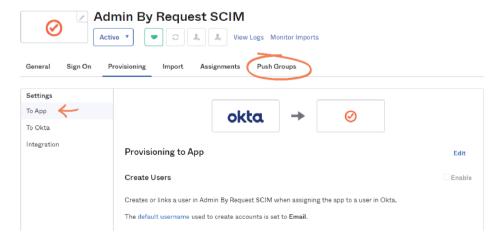17. **Close** the **Test Connector Configuration** window:
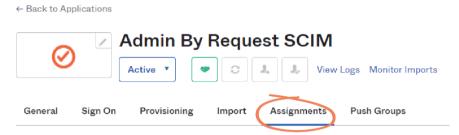

18. Click **Save**:

📋 **NOTE:** Clicking the **Save** button opens a new menu item, **To App** in the left-hand menu of the **Provisioning** tab. It also creates a new tab in the top menu: **Push Groups**. This tab is used in Task G: Start Provisioning:
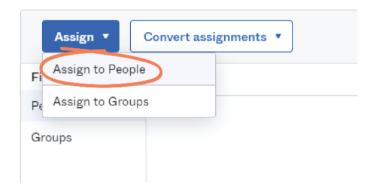
Task F: Assign Users and Groups

Assigning users and groups determines what data will be synchronized to the Admin By Request User Portal when the provisioning cycle runs.
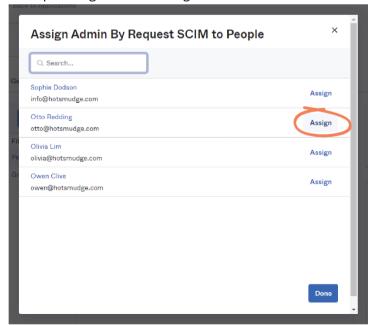
1. From In your Okta portal, click into the **Assignments** tab in the top menu of the application page:

2. Click **Assign** and select one of the two options from the drop-down menu – this example demonstrates both, beginning with **Assign to People**:

3. Locate the desired user and click the **Assign** button to the right of their name. This example assigns *Otto Redding*:
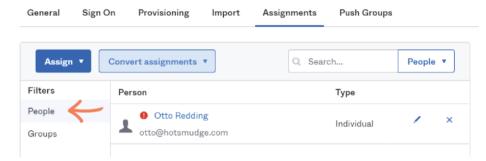
4. This action opens an **Assign Admin By Request SCIM to People** window displaying the properties for that user. Scroll to the bottom of the window and select **Save and Go Back**:

Save and Go Back   Cancel

📝 **NOTE:** You are able to edit the **User Name** property, but the other values are read-only.

❗ **IMPORTANT:** All assigned users must have an email address listed or provisioning will fail.
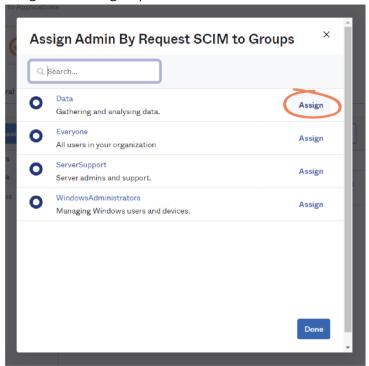
5. When the desired users are assigned, click **Done**:

Done

6. The assigned user now appears in the **People** tab (left-hand menu) of the **Assignments** screen:

| General | Sign On | Provisioning | Import | Assignments | Push Groups |

Assign ▼   Convert assignments ▼   🔍 Search...   People ▼

Filters	Person	Type		
People	❗ Otto Redding otto@hotsmudge.com	Individual	✏️	✕
Groups				

7. To assign a group of users, repeat step 2, but **Assign to Groups** from the **Assign** drop-down menu:

Assign ▼   Convert assignments ▼

Assign to People

Assign to Groups
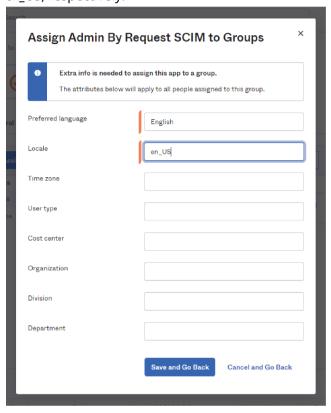
tto Redding
otto@hotsmudge.com

8. Click the **Assign** button to the right of a group to assign to that group – this example assigns the *Data* group:

9. As with **Assign to People**, this action opens a properties window (**Assign Admin By Request SCIM to Groups**). If no other information is required (i.e., you already have the property fields adequately filled), click **Save and Go Back**:

⚠ **IMPORTANT:** You may have to enter the **Preferred Language** and **Locale** before the window will allow you to **Save and Go Back**. This example uses *English* and *en_US*, respectively:
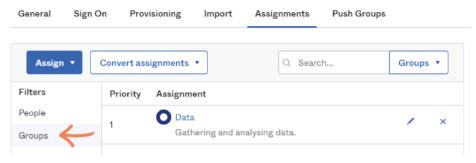

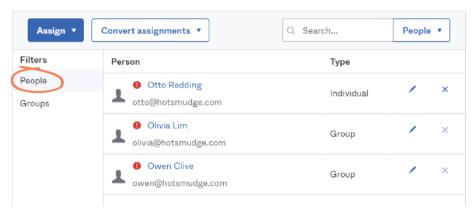10. When the desired groups have been assigned, click **Done**:

📝 **NOTE:** Multiple groups can be assigned at a time (i.e., in the **Assign Admin By Request SCIM to Groups** window, before clicking **Done**).

⚠ **IMPORTANT:** Assigning Groups will assign all of the users in that group to the application, and those users will be synchronized to Admin By Request when provisioning occurs. However, the group data for the assigned group will not be pushed during provisioning. Pushing group data is a manual process that is covered in the following task (i.e., Task G).

11. The assigned group now appears in the **Groups** tab (left-hand menu) of the **Assignments** screen:
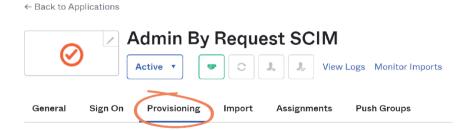

12. Click into the **People** tab in the left-hand menu, which displays all of the users that have been assigned either individually (*Otto Redding* – **Assign to People**) or as part of a group (*Olivia Lim* and *Owen Clive*, from the *Data* group – **Assign to Group**). These are the users that will be synchronized during Task G:
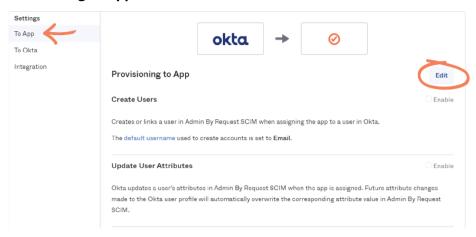

Task G: Start Provisioning

Task F initiates the provisioning cycle, in which requests are made to create, update, and delete users within Admin By Request.

1. In your Okta portal, click into the **Provisioning** tab in the top menu:
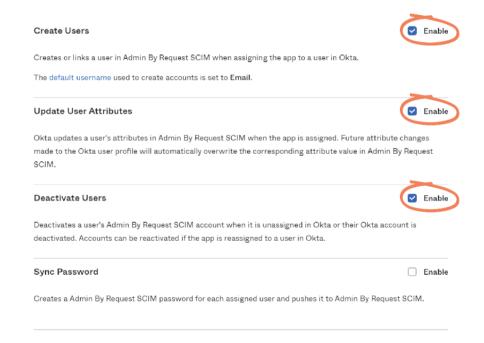
2. Ensure you are in the **To App** tab (left-hand menu) and click the **Edit** button in the **Provisioning to App** section:

3. Check **Enable** for the following three properties:

- **Create Users**
- **Update User Attributes**
- **Deactivate Users**

4. Click **Save**:

5. Scroll down to the **Admin By Request SCIM Attribute Mappings** section and select the **Force Sync** button, which will synchronize data to Admin By Request (i.e., push all users assigned in Task F to the User Portal):

Admin By Request SCIM Attribute Mappings

Select a(n) Admin By Request SCIM attribute to set its value based on values stored in Okta.

[✎ Go to Profile Editor]   [C Force Sync]

> 📝 **NOTE:** A success message appears at the top of the screen on completion (this is the location of all similar success messages in the Okta portal):
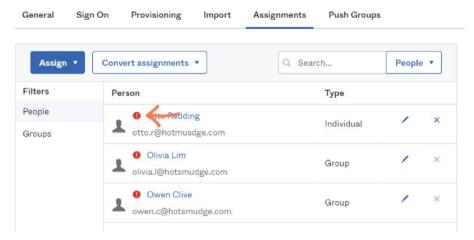
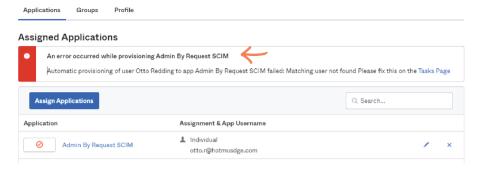✅ Job created to update values in app to match Okta

Synchronization Errors

Force Sync should immediately push assigned individual users and users assigned from groups to the Admin By Request User Portal. However, synchronization is not always immediately successful (even if the success message above was displayed).

Failed synchronization is indicated by a red exclamation mark to the left of the user name and can be accompanied by the error: **Matching user not found**. The following subset of steps resolve this issue.
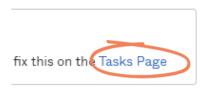
    i.   Click into the **Assignments** tab. The red exclamation mark indicates an error with synchronization:

General	Sign On	Provisioning	Import	Assignments	Push Groups

Person	Type		
❗ otto Redding otto.r@hotmusdge.com	Individual	✎	✕
❗ Olivia Lim olivia.l@hotsmudge.com	Group	✎	✕
❗ Owen Clive owen.c@hotsmudge.com	Group	✎	✕

Filters: People, Groups

[Assign ▾] [Convert assignments ▾] [🔍 Search...] [People ▾]
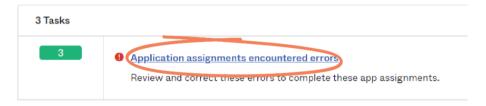
ii.   Click one of the users that have a red exclamation mark next to their name (in this example, *Otto Redding*) and view the error message that appears in the new page:
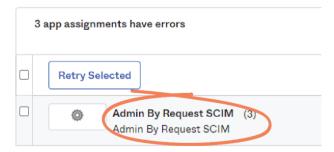

iii.   If the error reads **Matching user not found**, select the **Tasks Page** button:

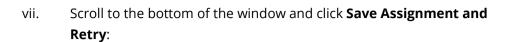iv.   Click into the task header, **Application assignments encountered errors**:

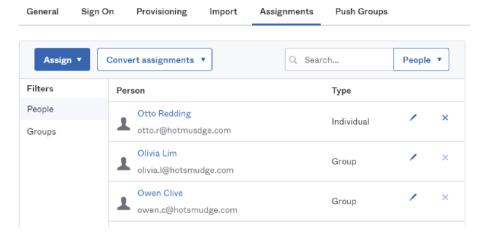v.   Select the **Admin By Request SCIM** task:

vi.   Click the **Edit Assignment** button for the first user:

vii.   Scroll to the bottom of the window and click **Save Assignment and Retry**:

viii.   Repeat steps v to vii for the other users in the list, then navigate back to the application **Assignments** tab (from the left-hand menu: **Applications** > **Applications** > **Admin By Request SCIM** > **Assignments**) and in the **People** tab, confirm that the red exclamation mark is gone for all users:

> ⚠ **IMPORTANT:** As mentioned, this is confirmation of synchronization within Okta; not with the Admin By Request User Portal. Viewing that the data has been pushed through as expected to your User Portal is covered in detail in Task H.

ix.   Navigate to the **Provisioning** tab, scroll down to the **Admin By Request SCIM Attribute Mappings** section, and select **Force Sync**:
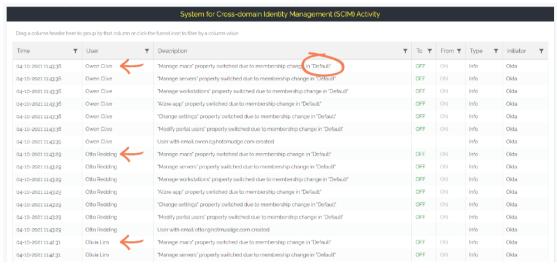

Pushing Groups

If synchronization is successful (**Force Sync**), the assigned users are pushed to your Admin By Request User Portal. However, as mentioned, assigning and synching groups of users does not push their group data to Admin By Request.
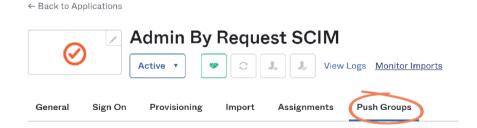
This means that the group of users will be in the User Portal, but they will all be assigned the Default Group-Based Role (and thus, have default permissions) until their group data is manually pushed from Okta

See the images below of the Admin By Request User Portal demonstrating this for the three users pushed earlier on in this task: *Otto Redding*, *Owen Clive*, and *Olivia Lim* have all been assigned *Default* permissions:
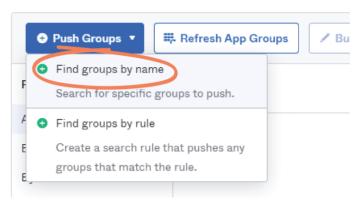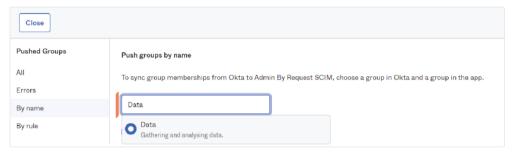

📝 **NOTE:** Viewing the above data in the Admin By Request User Portal is covered in detail in Task H.

1. To manually push assigned groups to the User Portal, select the **Push Groups** tab from the top menu:
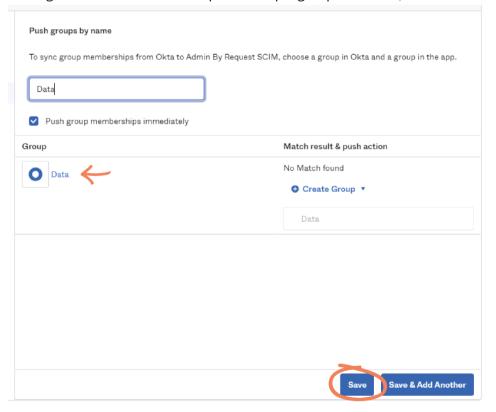
2. Click **Push Groups** and select one of the two options from the drop-down menu – this example uses **Find groups by name**:
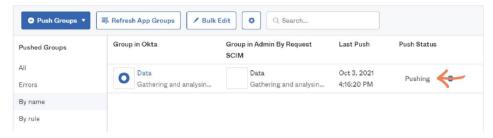

3. Type the group you want to push into the search bar – this example pushes the *Data* group (the only group assigned to the application in Task F):
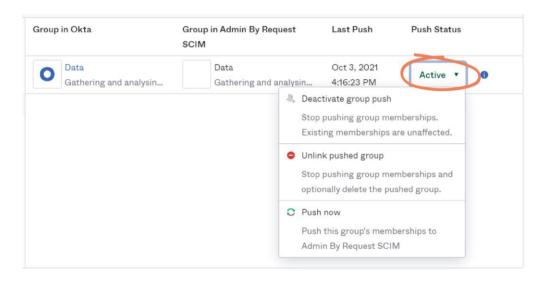

4. Select the appropriate group name and click **Save** (you also have the option of clicking **Save & Add Another** to push multiple groups at a time):
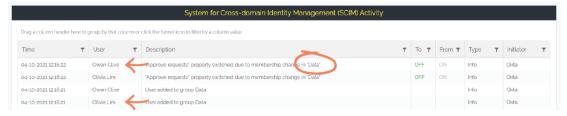
📝 **NOTE:** The **Push Status** initially displays *Pushing*, and changes to **Active** when pushing is complete (i.e., the group data is successfully sent to Admin By Request):

5. Click the **Active** drop-down menu for more options for groups:

- **Deactivate group push** – Stop pushing group memberships. Existing memberships are unaffected.
- **Unlink pushed group** – Stop pushing group memberships and optionally delete the pushed group.
- **Push now** – Push this group's membership to Admin BY Request SCIM.

Now that group data has been manually pushed to the Admin By Request User Portal, the provisioned users are assigned their correct Group-Based Role and corresponding permissions (i.e., *Olivia Lim* and *Owen Clive* are assigned the *Data* Group-Based Role):
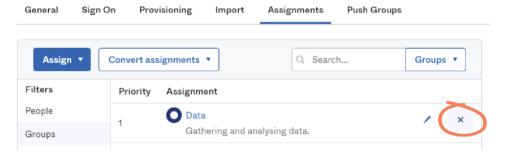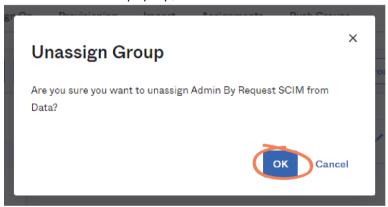
Deprovisioning

Deprovisioning users and groups in Okta occurs as soon as you unassign a user / group from the app.

1. In the **Assignments** tab, select either **People** or **Groups** from the left-hand menu, and click the **x** icon to the right of the user or group name. This example unassigns the *Data* group:
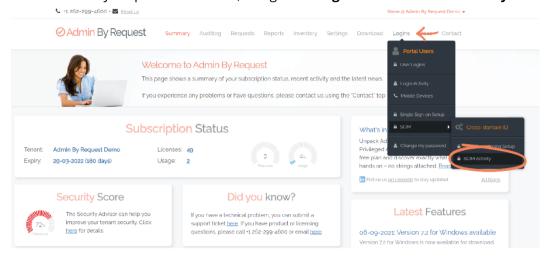

2. In the confirmation pop-up, click **OK**:

⚠️ **IMPORTANT:** The Admin By Request SCIM implementation with Okta does not provide functionality to remove users from Groups. I.e., once a group is assigned to the Admin By Request SCIM app in Okta, removing users from that group within Okta does not remove the user from the corresponding group in the Admin By Request User Portal.
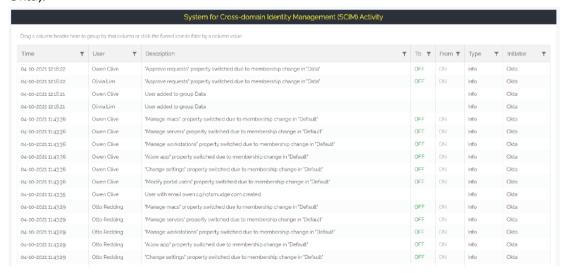
Task H: View Data in User Portal

Provisioned users and groups are now available in the Admin By Request User Portal.
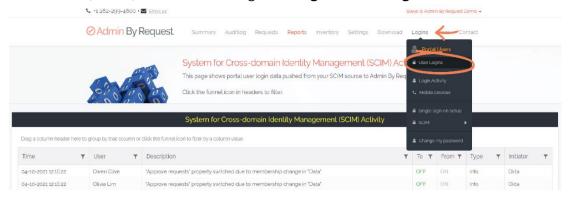
1. In the Admin By Request User Portal, navigate to **Logins** > **SCIM** > **SCIM Activity**:

2. The table displays all synchronized user and group data, including the **Time** synchronization occurred, the name of the **User**, a **Description** of the activity, **To** and **From** columns (which only display content if a permission has changed – i.e., a property has 'switched' from checked to unchecked, such as when a user has been added to a group or their Group-Based Role has been edited, etc.), and the **Initiator** (the IDP – i.e., Okta):

3. All provisioned users should have the appropriate permissions as defined in Group-Based Roles (Task B). To view this, navigate to **Logins** > **User Logins**:

4. As mentioned in Task G, the correct checkboxes should be ticked next to each user depending on their group and the Group-Based Role defined for that group:

- *Otto Redding* has the *Default* permissions assigned as he is not a member of any group.
- *Olivia Lim* and *Owen Clive* have the permissions defined for the *Data* Group-Based Role.
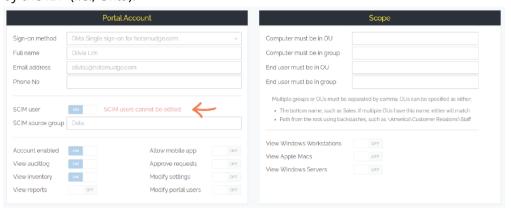

⚠ **IMPORTANT:** As soon as a user is synchronized, they get the permission defined for their group in Group-Based Roles (either Default or specific IDP group). If Group-Based Roles are edited, the users assigned that Role get the updated permissions as soon as the provisioning cycle runs again.

5. Click the **Edit** button next to a user in **Portal User Logins** to view more information on their permissions in the User Portal. This example uses *Olivia Lim*:
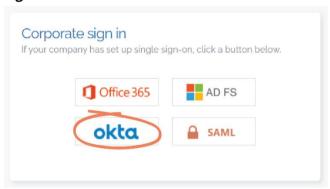
> ⚠️ **IMPORTANT:** Users that have been synchronized with SCIM cannot be edited within the Admin By Request User Portal. You can view their data in the Portal Account section, but are not able to make changes because the data is controlled by the IDP (i.e., Okta):

User Login

Now that users are provisioned, they can sign into the Admin By Request User Portal through Okta.
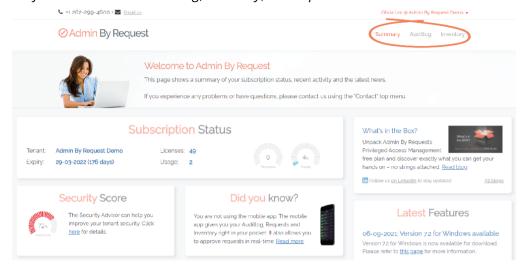
1. Go to the Admin By Request Sign in page and select **Okta** from the **Corporate Sign-in** section:

2. Provisioned users can use their Okta user name to sign in. This example uses *Olivia Lim*:

3. Once signed in, the user only has access to User Portal features according to the permissions defined in their Group-Based Role. *Olivia Lim* is in the *Data* group, so only has access to the *Auditlog*, *Inventory*, and *Reports* data:

📝 **NOTE:** As mentioned, making changes to the *Data* Group-Based Role will affect what *Olivia Lim* can access in her User Portal.