exterro®
Data Risk Management

FTK SCIM 2.0

USER PROVISIONING & CONFIGURATION GUIDE

JULY 2026

Table of Contents

About Exterro

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today. We deliver a fully integrated Data Risk Management platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world's largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.

1 Configuration Overview

The System for Cross-domain Identity Management (SCIM 2.0) specification provides a powerful mechanism for automated provisioning and user identity management across cloud enterprise applications. Exterro recommends using SCIM 2.0 Services to significantly reduce the operational complexity and long-term costs of User Management by establishing a common schema and a robust extension model.

Through this feature, Exterro FTK users and groups can be seamlessly assigned, provisioned, updated, and managed directly from enterprise Identity Providers (IdPs) that adhere to the SCIM 2.0 protocols.

1.1 Key Capabilities

- **Automated Provisioning:** Instantly create, assign, and provision users to the Exterro FTKC application directly from your central directory.
- **Continuous Identity Management:** Dynamically update and maintain user attributes and information through synchronous SCIM services.

2 Configuration Prerequisites

Before proceeding with your SCIM integration, ensure that the following baseline system prerequisites are met:

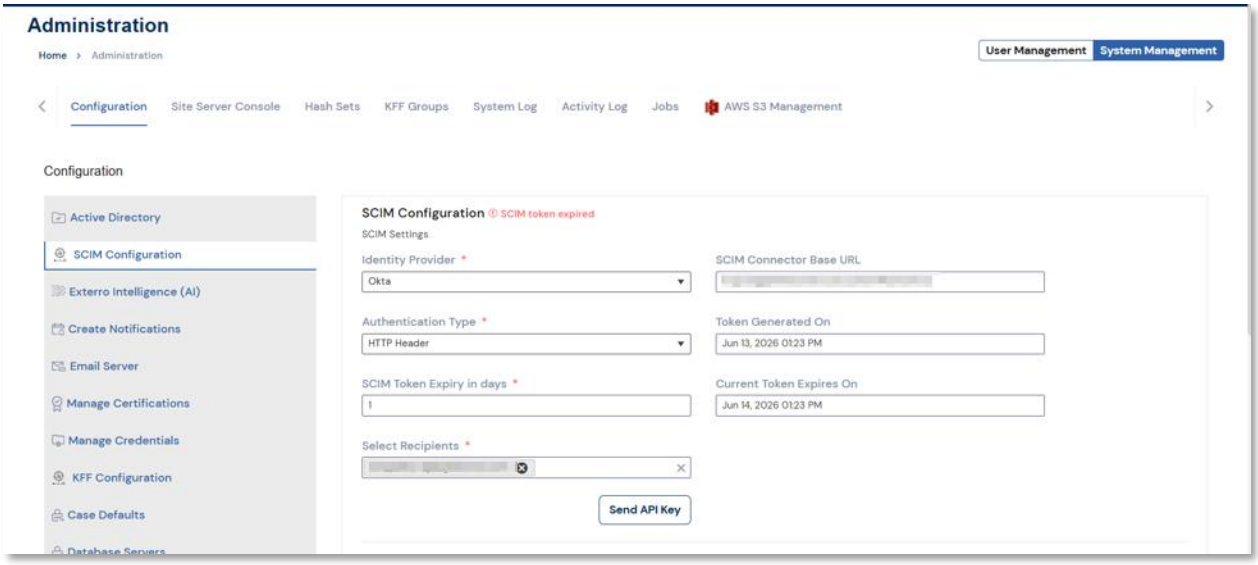
- **Feature Access:** Your deployment must have explicit access to the SCIM - SAML SSO Authentication Type, and SCIM Services must be fully enabled within your specific Exterro application bundle.
- **SMTP Configuration:** A properly configured SMTP server must be active within FTKC. This is mandatory to securely email newly generated API keys and file passwords to designated administrators.

3 Configuring SCIM in Exterro FTKC

The SCIM Configuration feature is enabled by default within the FTK application environment. Administrators can view, update, and manage the configuration.

***Navigation**: From the home page of **FTK Central > Settings > System Management > SCIM Configuration**.*

- *View SCIM Configuration and Edit SCIM Configuration*

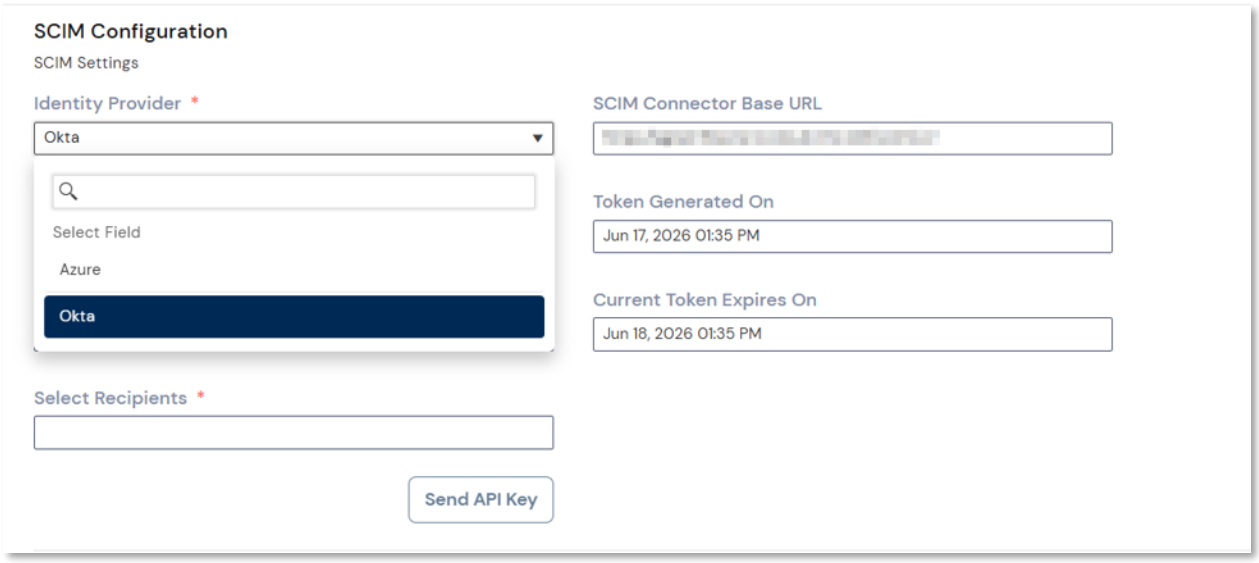


3.1 Step-by-Step UI Activation

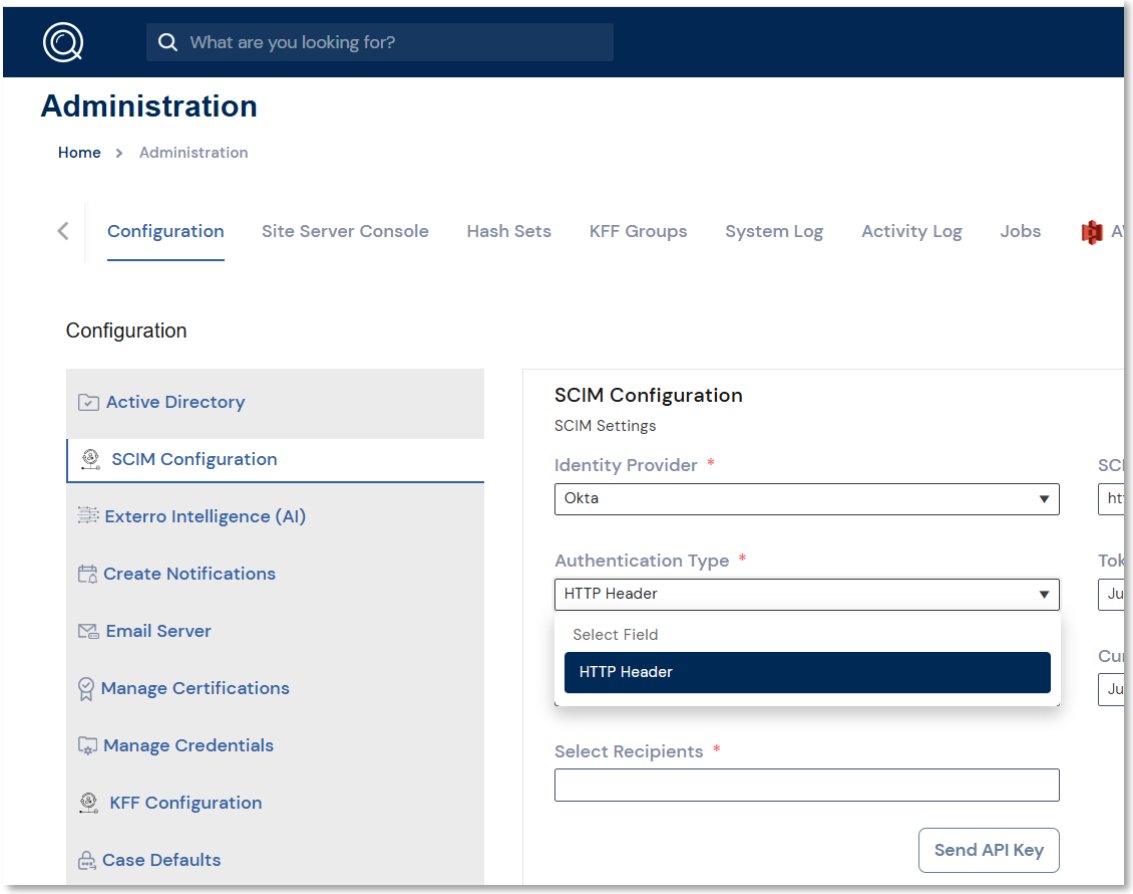
1. Log into the Exterro FTKC application using regular administrative credentials.
2. Navigate to the upper-right configuration gear icon and click **Settings**.
3. From the administration menu layout, click **System Management** and select the **SCIM Configuration** side tab.
4. Provide the values for the following fields:

- **Identity Provider:** Choose your Identity Provider from the dropdown list. Exterro natively supports **Okta** and **Azure (Microsoft Entra ID)** frameworks.

  Examples: *For Azure AD or Okta*



- **Authentication Type:** Set this option to **HTTP Header** (or OAuth 2.0 depending on your operational architecture).



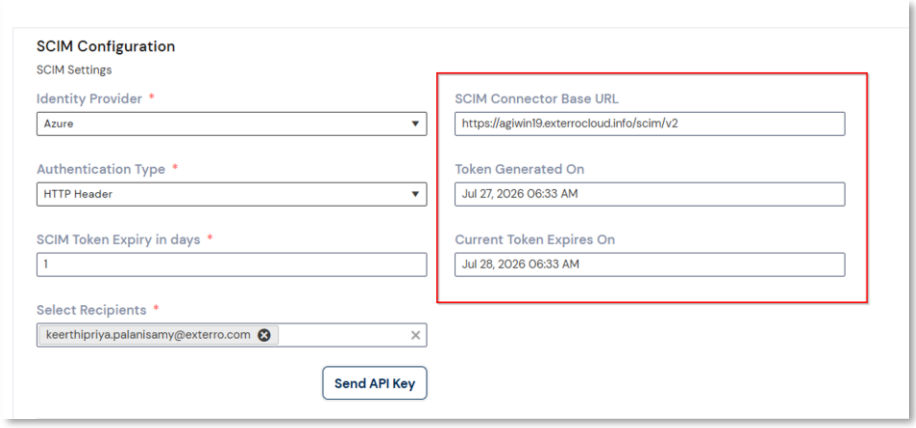
***Note:** The 'Expiry in Days' and 'Select Recipients' fields will be available only when the 'Authentication Type' is set as **HTTP Header**.*

- **SCIM Token Expiry in Days:** Define the lifetime duration of the integration token. Enter an integer value strictly between 1 and 999 days.
- **Select Recipients:** Specify the designated email accounts from the dropdown scheduled to receive integration credentials. Additionally, even if the desired email address is not present in the dropdown menu, you can manually enter a valid email address and click the use <Email> which is populated to send the API key.

5. Click the **Send API Key** action button. When you click the send API key button, the values in the right side will get auto populated according to the values provided by the users.

6. View the token generated date and expiry token time.

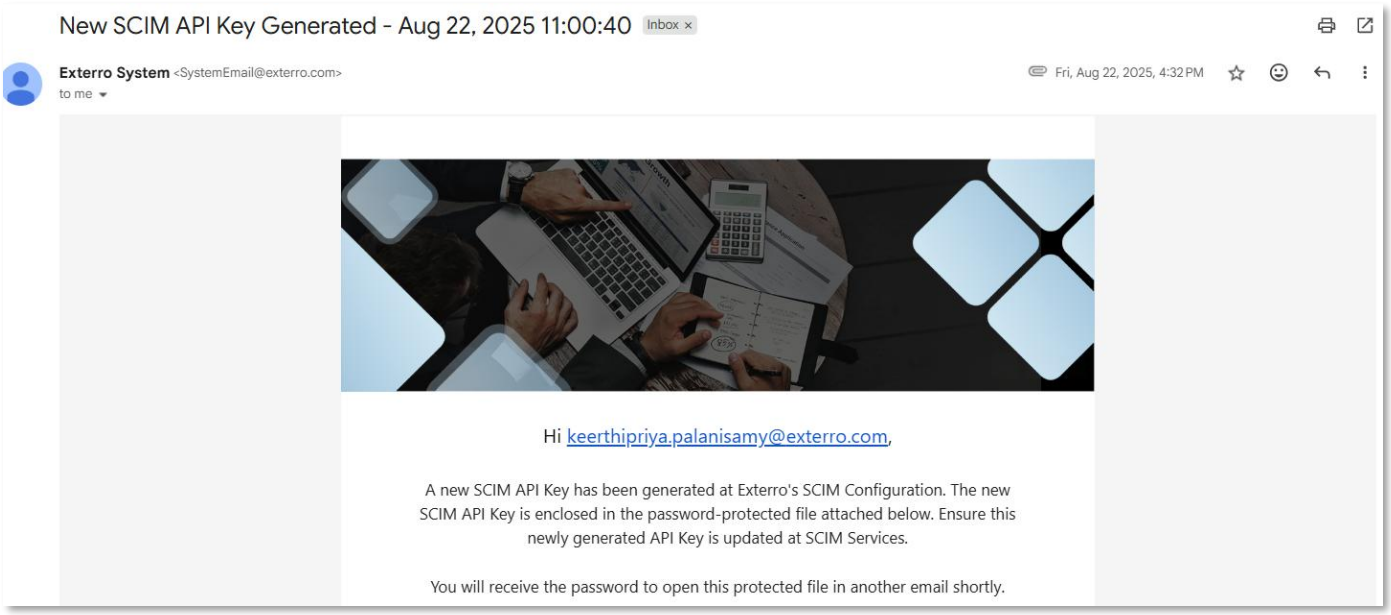
   Note: *Ensure to keep a copy of the* ***SCIM Connector Base URL*** *for your reference. You will need to provide this value when configuring the newly created app integration in the corresponding SCIM-enabled Identity Provider application.*



Also, this routine triggers two distinct, automated emails to ensure secure, split knowledge delivery:

- **Email 1:** Contains an encrypted, password-protected attachment containing the fresh system **API Key**.
- **Email 2:** Delivers the separate unique **Password** required to open and decrypt the API Key attachment file.

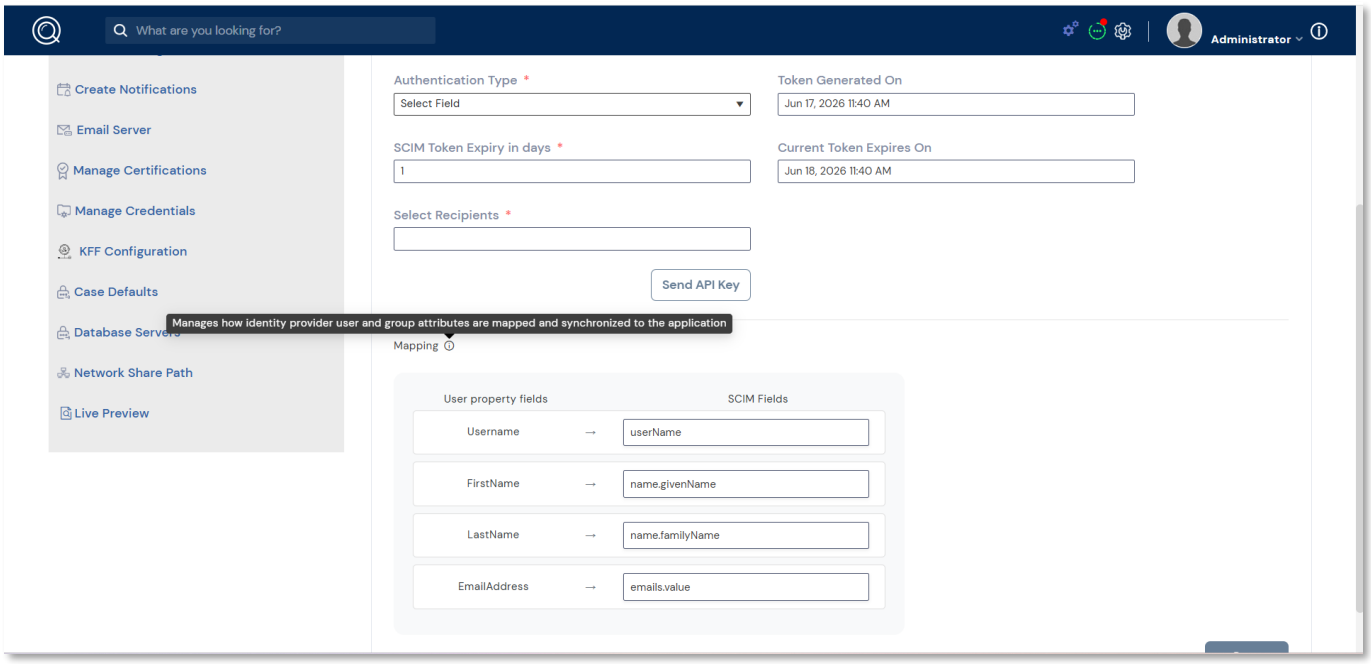
Note*: It is required to update the generated token in the SCIM-configured Identity Provider application for the successful integration of SCIM Services with the Exterro FTK.*



3.2 Core Attribute Mapping Rules

Exterro automatically enforces standard attribute mapping metrics across the identity providers. Ensure your IdP configuration correctly reflects the properties outlined in the mapping matrix below:

User property Fields	SCIM Fields	Description
Username	userName	Denotes the unique login identifier of the enterprise user.
First Name	name.givenName	Denotes the verified given name of the user resource.
Last Name	name.familyName	Denotes the verified family name of the user resource.
EmailAddress	emails.value	Denotes the primary operational communication email address.



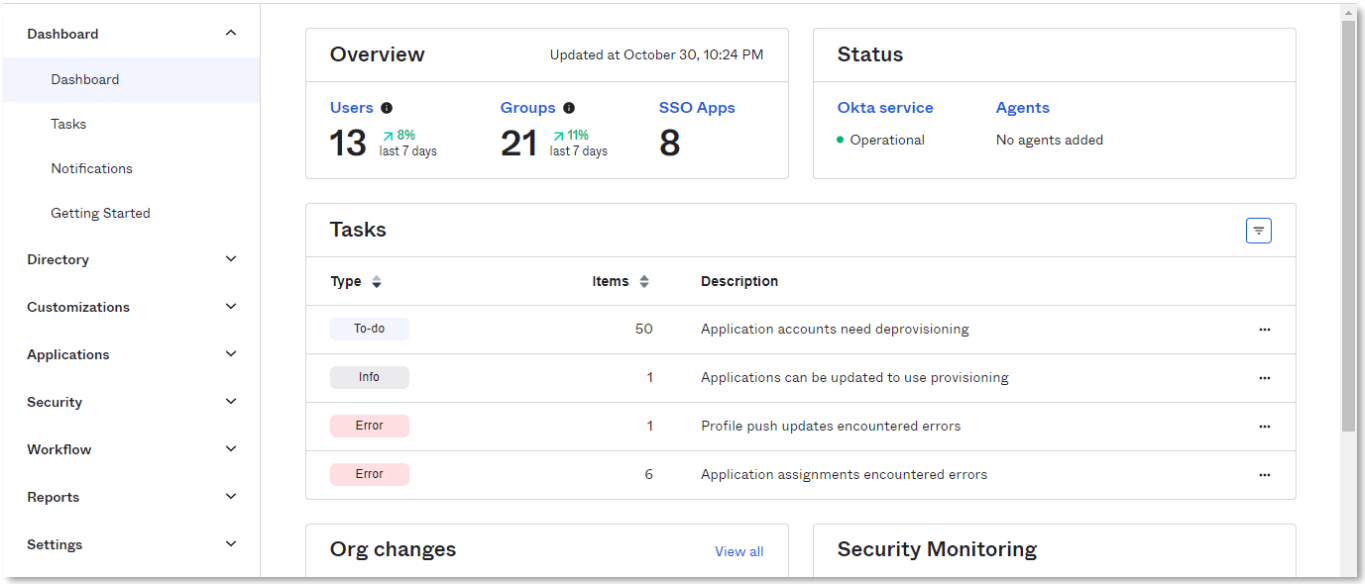
Configure all the mandatory fields. These fields are common to both Okta and Azure IdP.

3.3 Identity Provider Integration: Okta

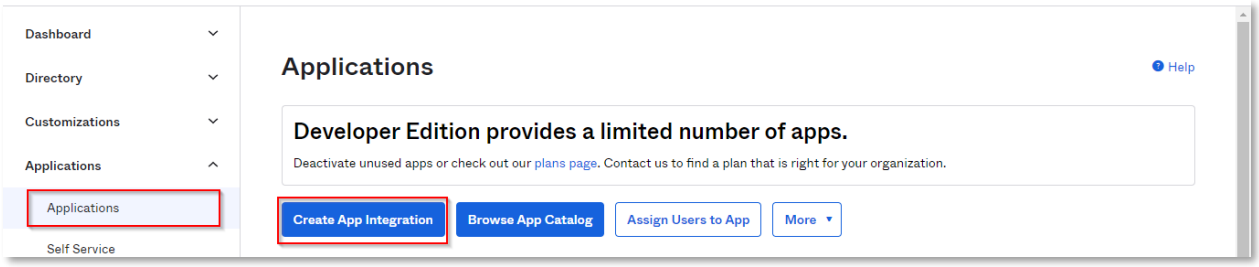
3.3.1 Creating the App Integration

Steps:

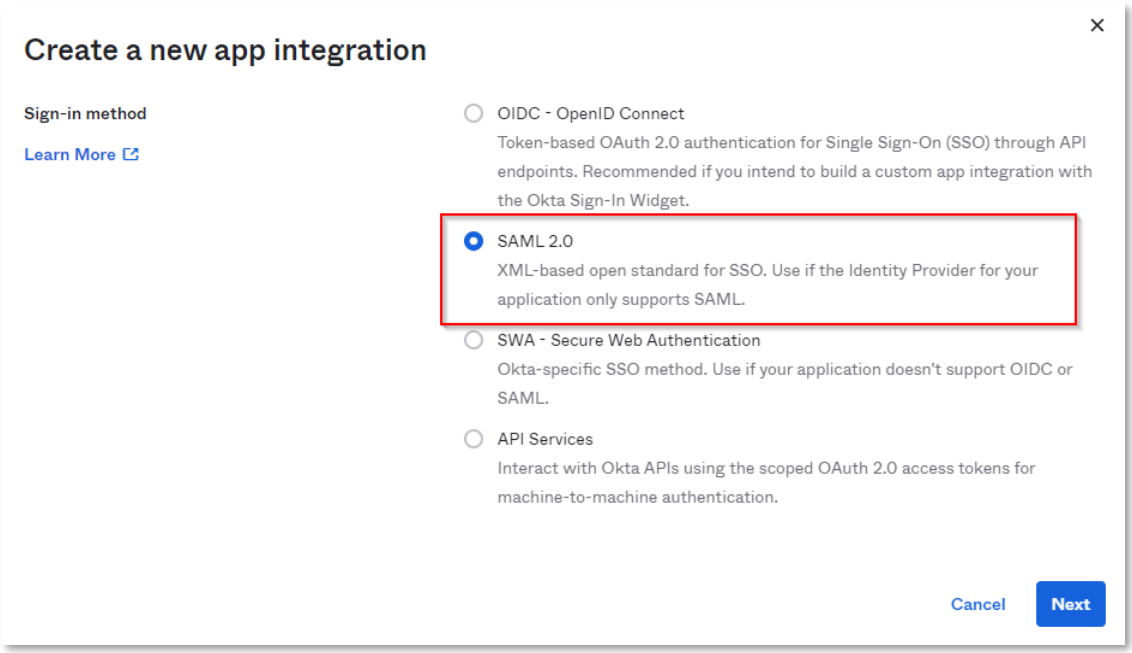
1. Log into your enterprise **Okta Admin Console**.



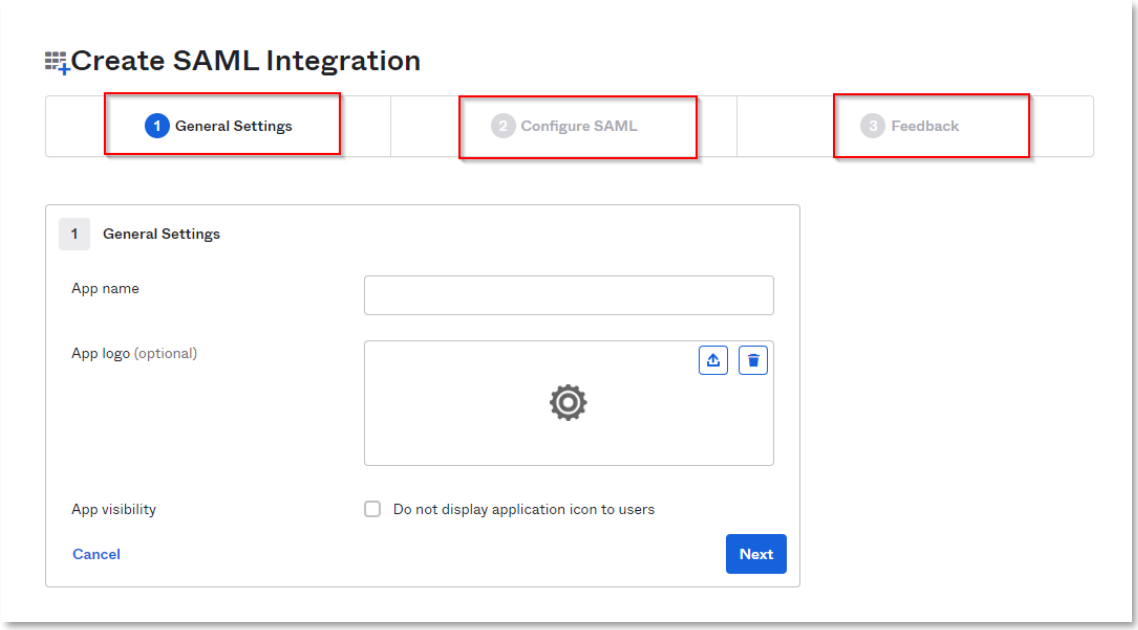
2. Using the left navigation sidebar pane, select **Applications** and click the nested **Applications** item.
3. Click the blue **Create App Integration** button.



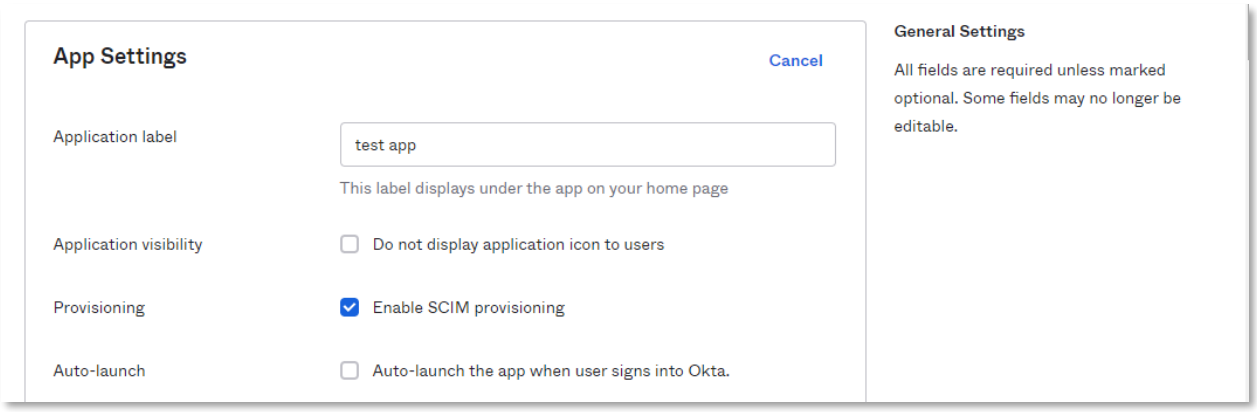
4. From the pop-up panel, select the sign-in method option button labeled **SAML 2.0** and click **Next**.



5. Provide appropriate workspace identities inside the **General Settings**, **Configure SAML**, and **Feedback** fields, then finalize the wizard by clicking **Finish**.

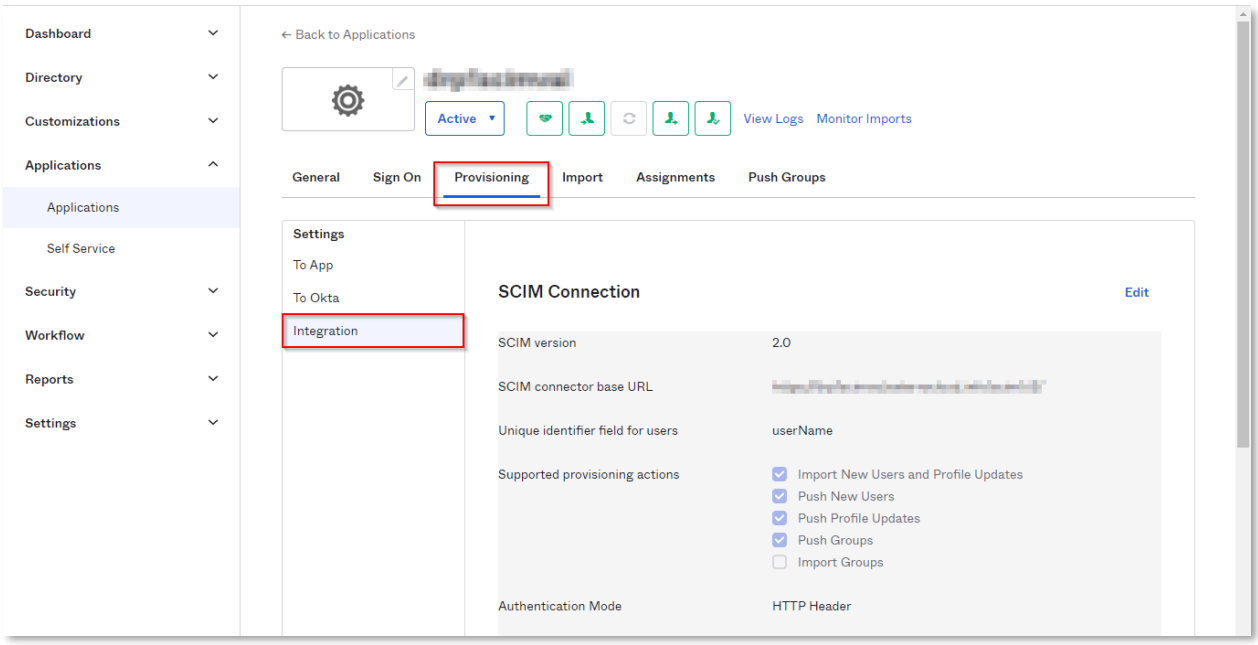


6. Once the base application details screen populates, navigate to its **General Settings** header block and choose **Edit**.
7. Locate the **Provisioning** row checkbox labeled **Enable SCIM provisioning**, check it, and click **Save**.

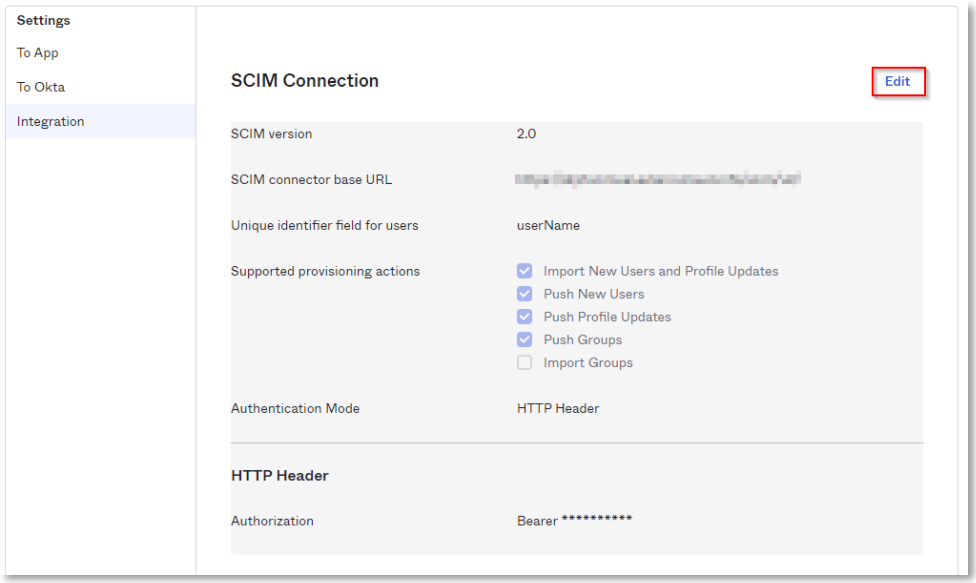


3.4 Configuring Connection & Credentials

1. From within your newly saved Okta app, select the freshly visible **Provisioning** tab menu element.



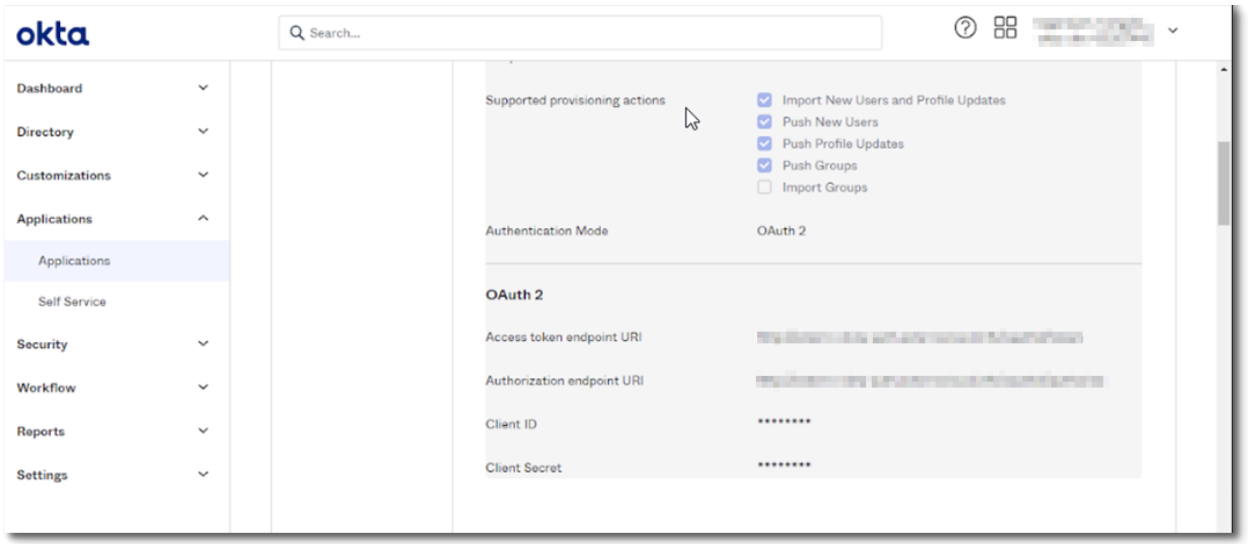
2. Under the left-hand settings pane, click on the **Integration** subsection line item and click **Edit**.

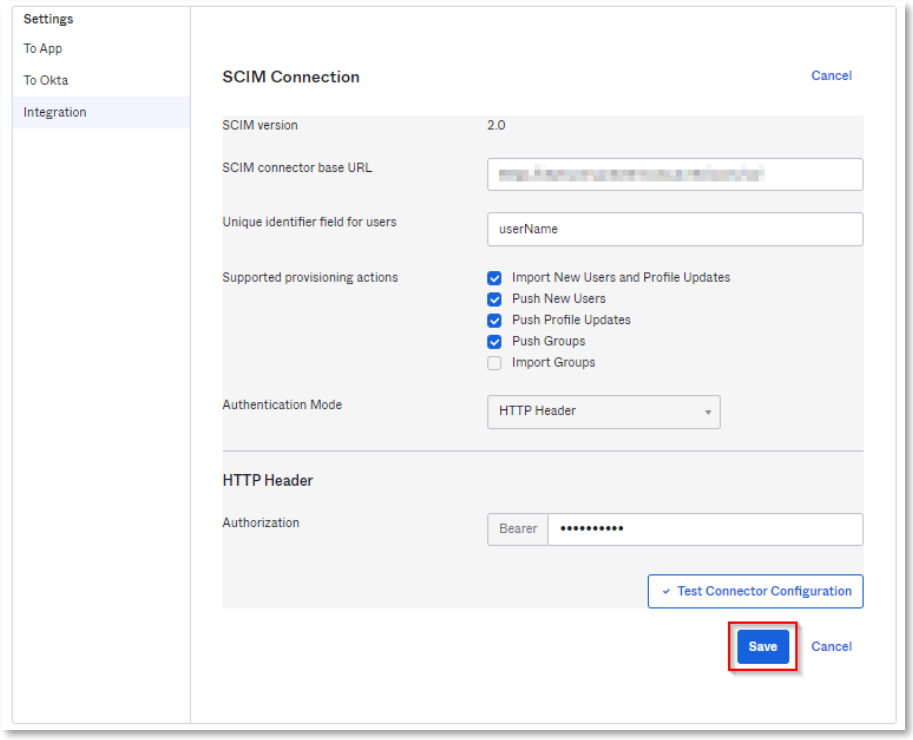


3. In the **SCIM connector base URL** input, insert the exact endpoint string value copied earlier from the Exterro SCIM Configuration panel.
4. For the **Unique identifier field for users** parameter, type userName.
5. Under **Supported provisioning actions**, check the following capabilities:
   - Import New Users and Profile Updates
   - Push New Users
   - Push Profile Updates
   - Push Groups
6. Set the **Authentication Mode** given below:

   - **Authentication Mode:** Select the authentication as 'HTTP Header'.
     - If HTTP Header is selected, provide the API Key generated in the above section for Authorization.
   - Configuring the requested fields in the SCIM application:

     A sample image is provided for your reference.





7. Click **Test Connector Configuration** to run a sandbox diagnostic validation. Once the connection indicates success, click **Save**.

***Note**: Due to downstream Okta schema rules, the Import Groups checkbox option is not applicable. Group records must originate in Okta and push downward into Exterro security frameworks.*

Follow the steps provided in the Creating a Group section for more information on creating Groups in Okta.

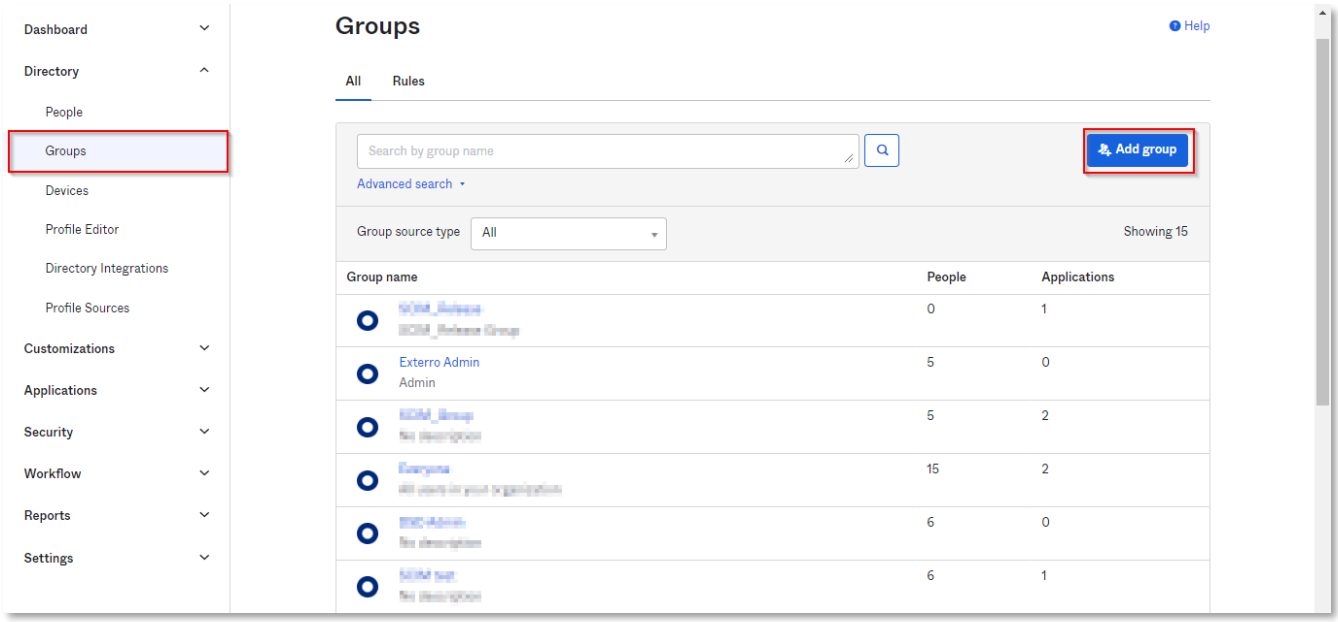
3.5 Directory Groups & User Management

- **Group Assignment:** To sync security profiles, navigate to **Directory > Groups** inside Okta, create a new structural group, Pushing this group via the **Push Groups** tab maps memberships seamlessly.

3.5.1 Creating a Group

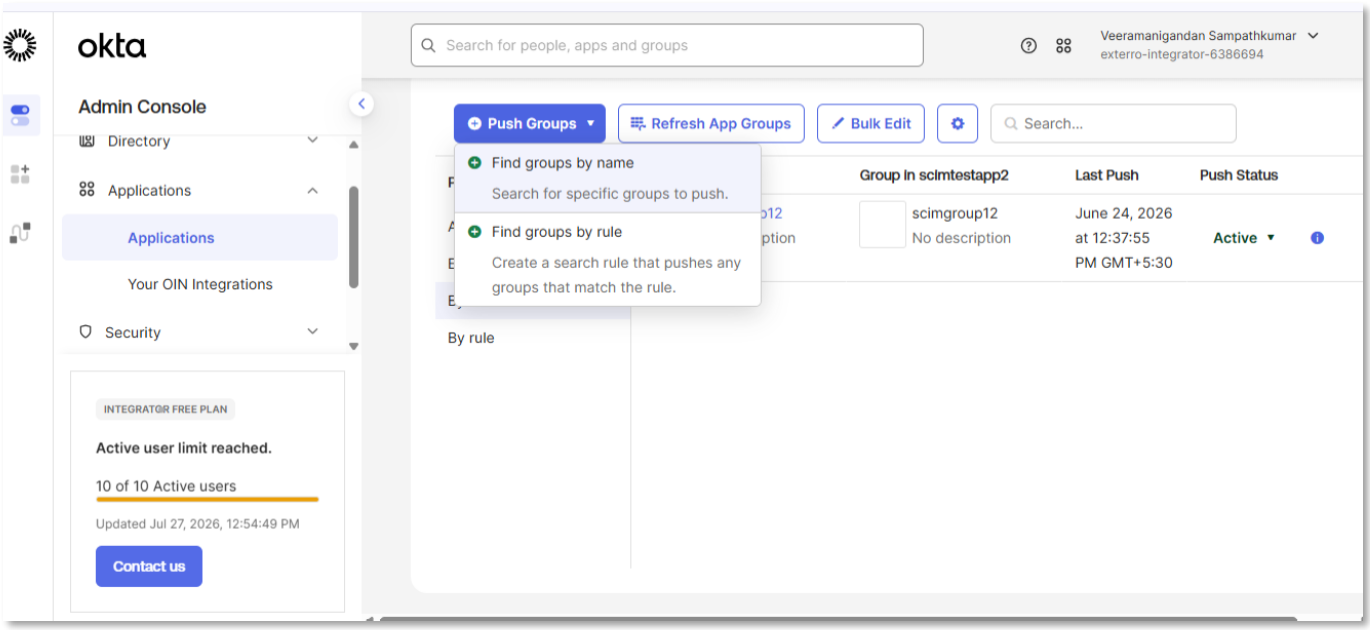
Steps:

1. Log in to the Okta application.
2. Navigate to the **Directory** from the left pane.
3. Click **Groups**.



4. Click **Add group**.

5. Click **Save**.
6. You can push the groups to application using the below options.



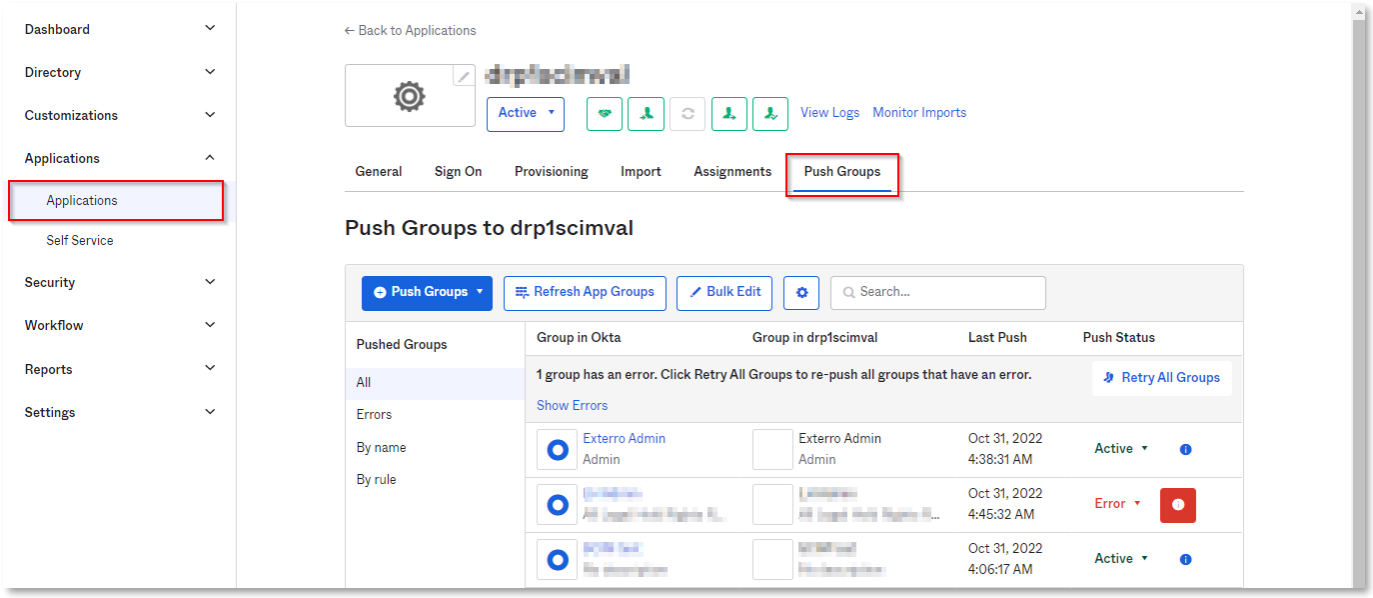
***Note**: You can add the desired users to the designated group in Idp; they will automatically synchronize with the FTK application.*

3.6 To Push Groups to the created app

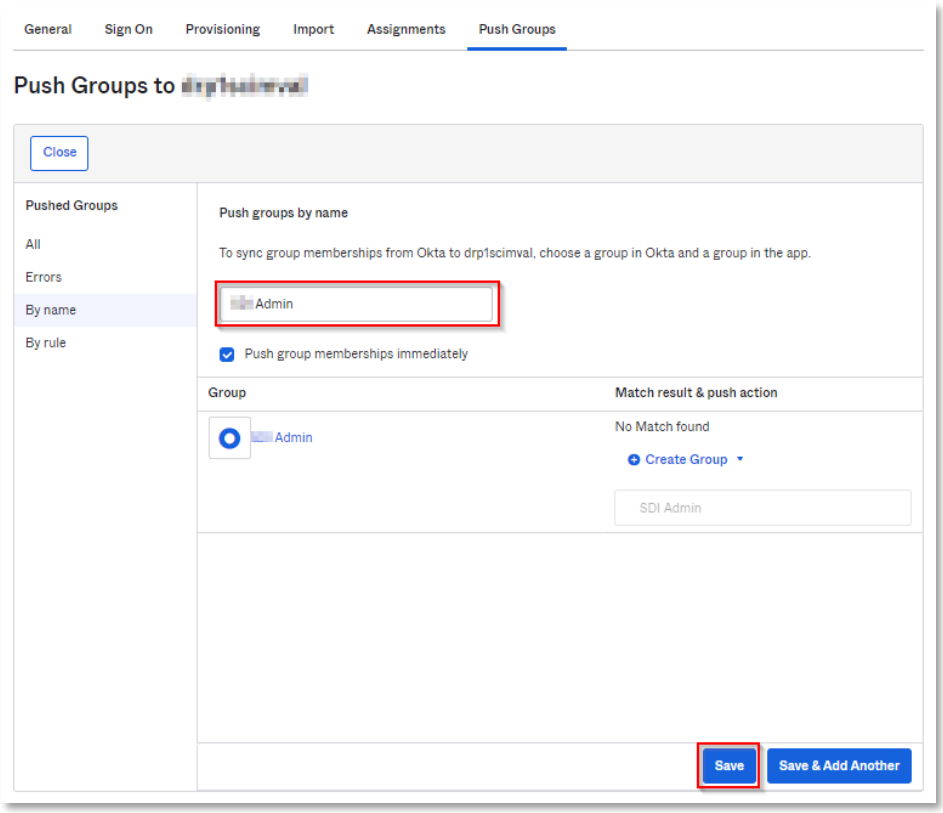
Follow the steps provided below to sync the groups created in Okta with the groups present in the Exterro application.

Steps:

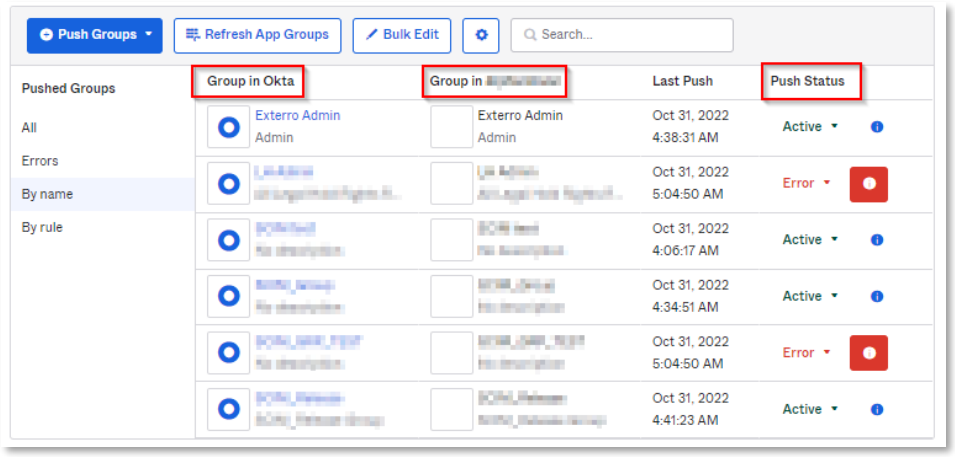
1. From the Manage Page of Applications.
2. Click on the created app.
3. Navigate to the **Push Groups** tab.



4. Search for the required groups and push them.



5. Click **Save**.

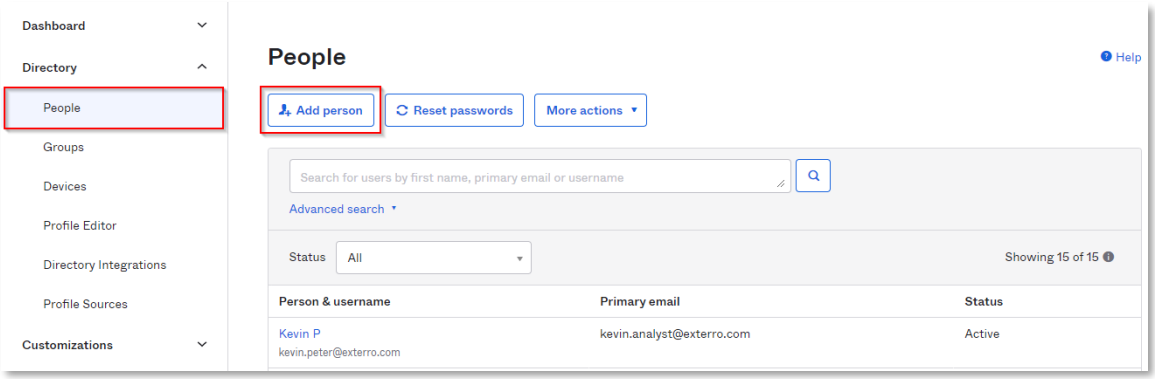


Here you can view the group name synced between the Okta and Exterro applications and its successful connection indicated in the 'Push Status' column.

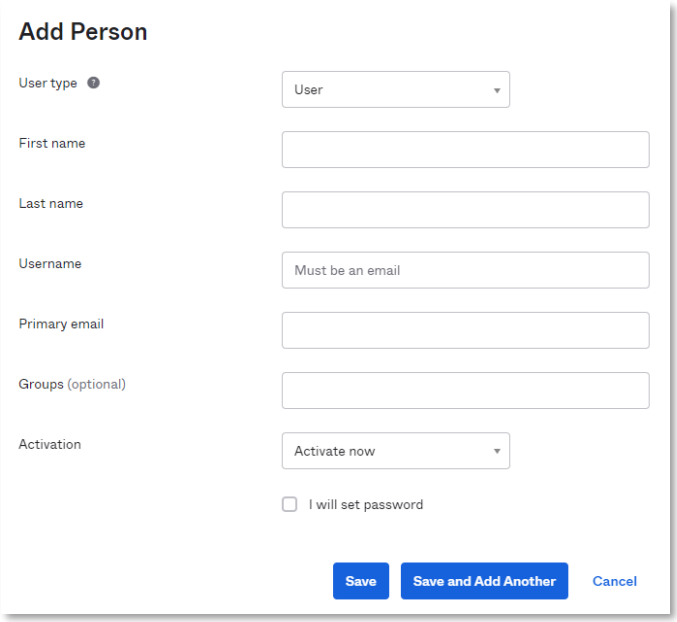
3.6.1 Adding People

Steps:

1. From the Okta application.
2. Navigate to the **People** section from the left pane.
3. Click **Add person**.



4. Provide the user details and click **Save**.



Notes:

- *The details provided for the People in the Okta application will be synced with the respective Users in the Exterro application.*
- *By default, the UTC TimeZone will be set in case an incorrect/empty value is entered for the 'TimeZone' field.*

To view the Logs:

FTK system administrators can accurately track, monitor, and troubleshoot user sync pipelines via two core telemetry options:

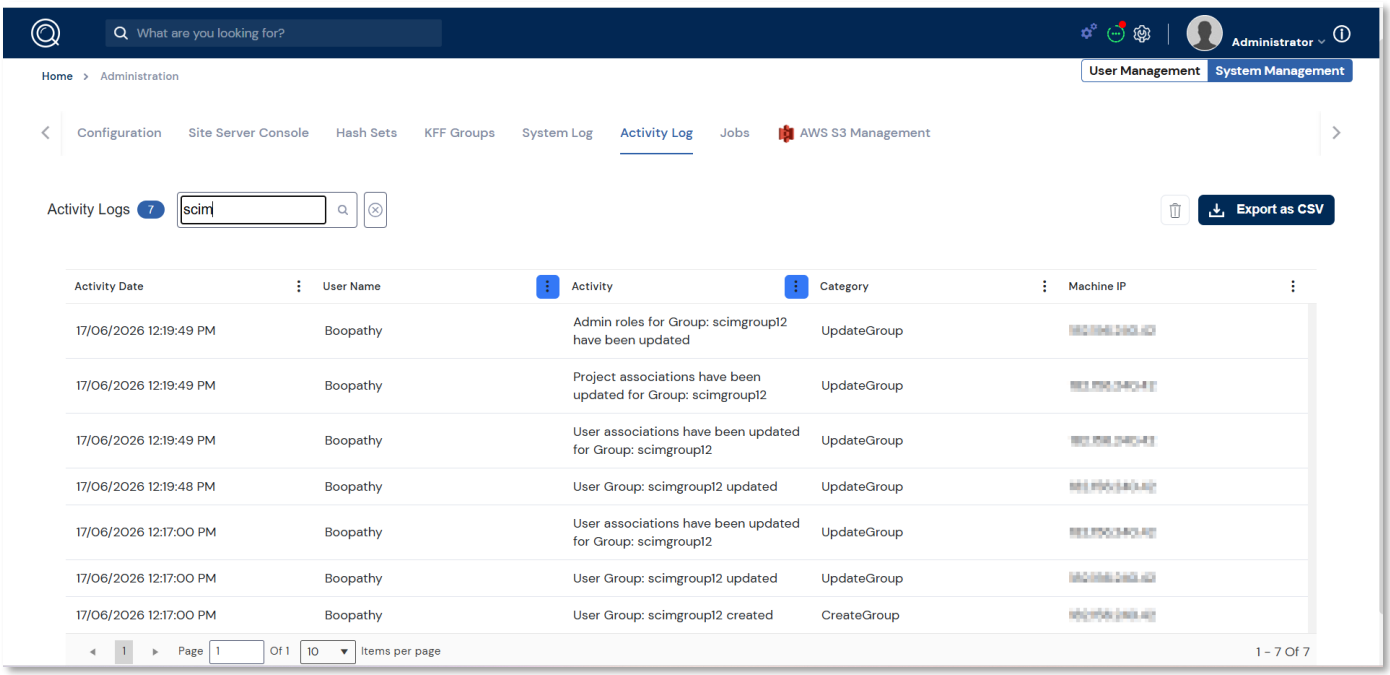
a. **Self-Host System File Logs:** Granular integration telemetry, raw data sync records, execution errors, and connection events are written directly onto the host server machine system file path: ***%PUBLIC%\Documents\AccessData\AccessDataLogs\adgselfhost.txt***

b. **UI Activity Log Dashboards:**

i. From the primary Exterro FTKC administrator panel dashboard interface layout, click the **Activity Log** view tab item.

ii. Locate the contextual text filter bar field element and search for the identifier token string: **scim**.

iii. The workspace will display an audit trail history logging action records (such as CreateGroup, UpdateGroup,etc,.), including precise timestamps, execution status metrics, and the executing administrative IP footprint.



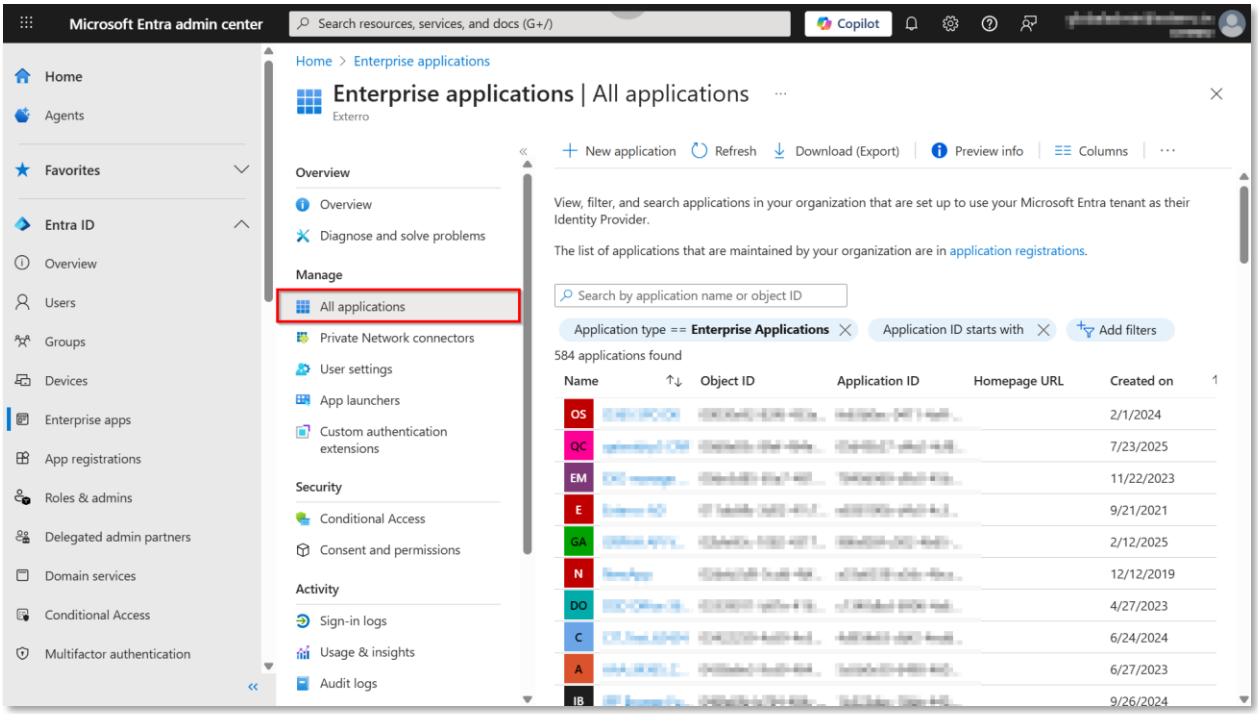
4 Azure - SCIM Configuration

4.1 Microsoft Entra ID – Configurations

4.1.1 Setting up an App Integration

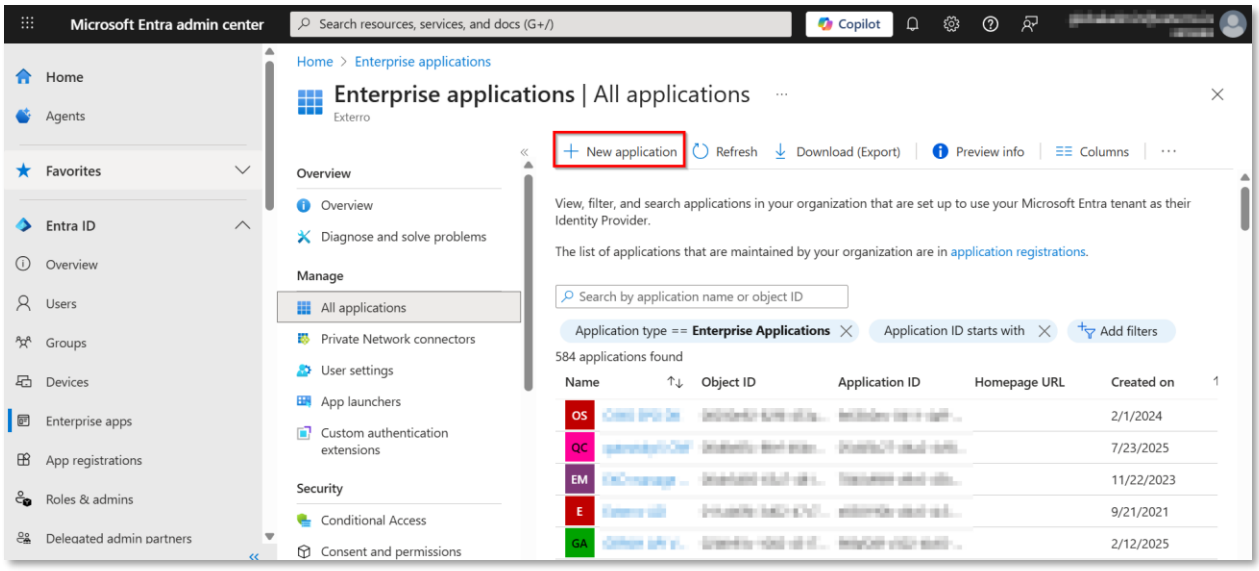
Steps:

1. Log in to the Microsoft Entra ID application.
2. Navigate to the **Enterprise applications** page.

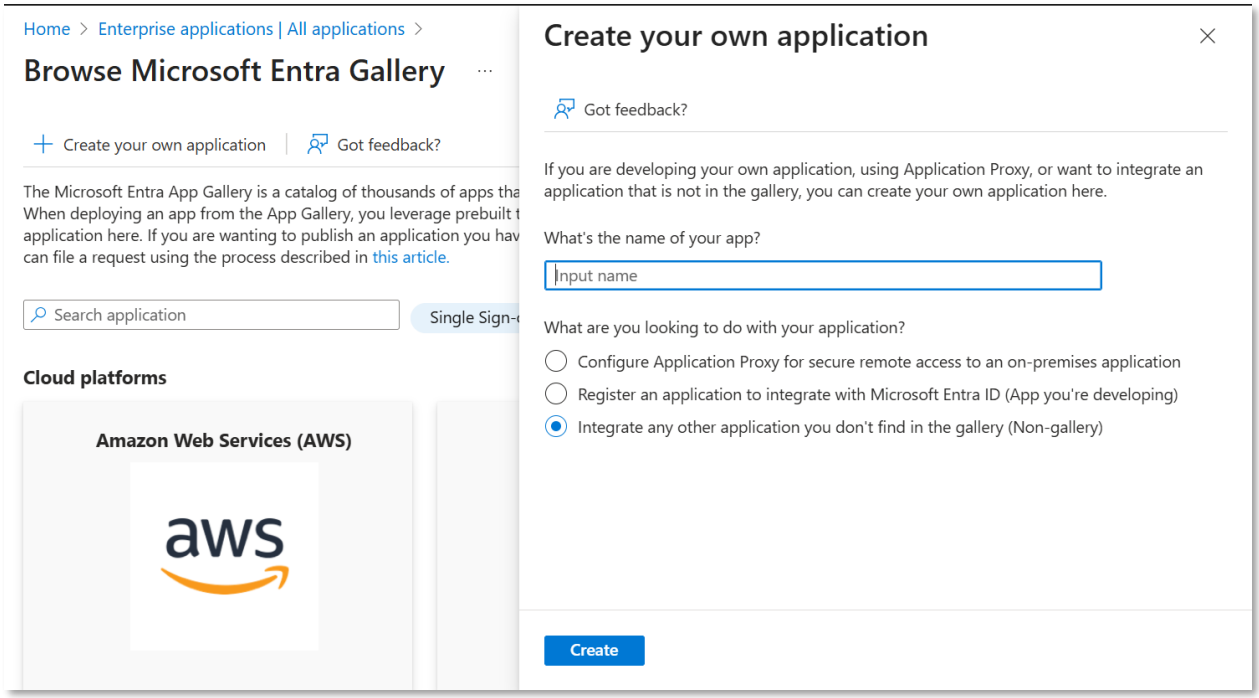


3. Select **All applications** from the left pane.

4. Click **New application** tab.

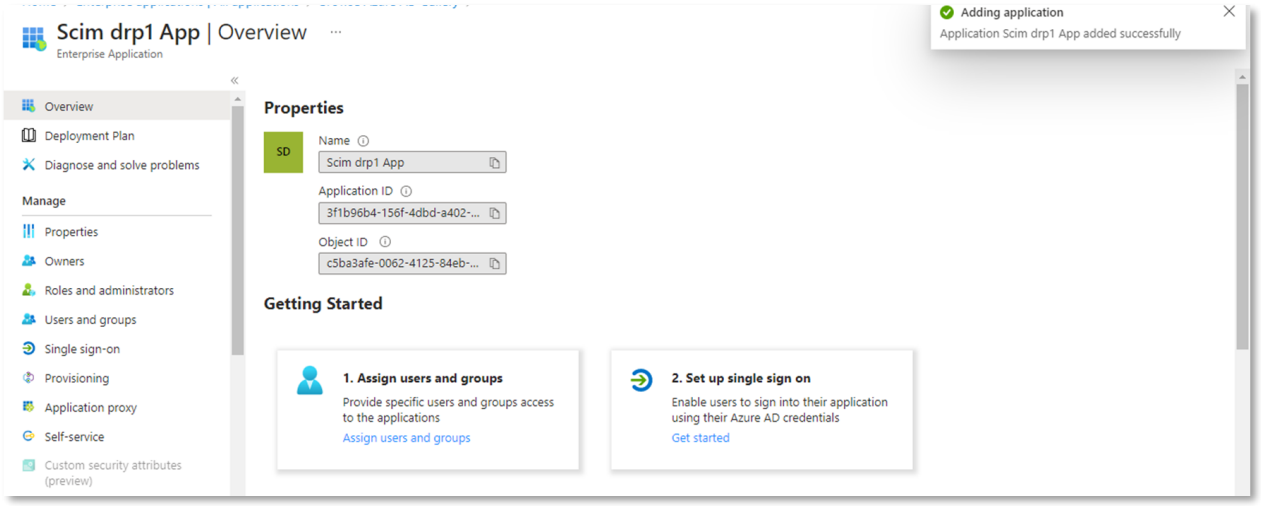


5. From the **Browse Microsoft Entra Gallery** page, click **Create your own application**.



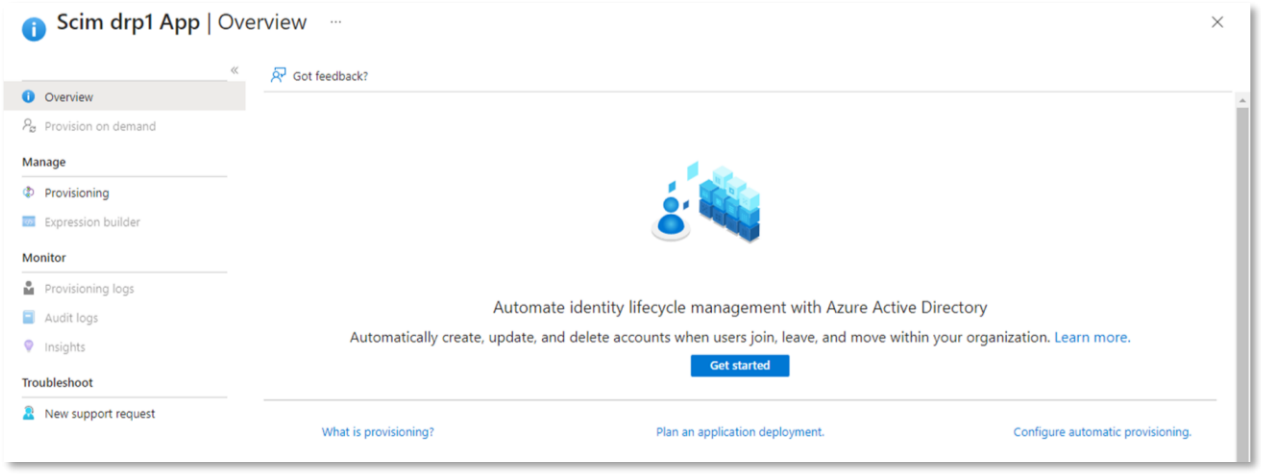
6. Enter the following details to set up the new application in the right pane,
   a. What's the name of your app?
   b. What are you looking to do with your application?
      o It is recommended to select 'Integrate any other application you don't find in the gallery (non-gallery)'.

7. Click **Create.**
   - A new application is created successfully.

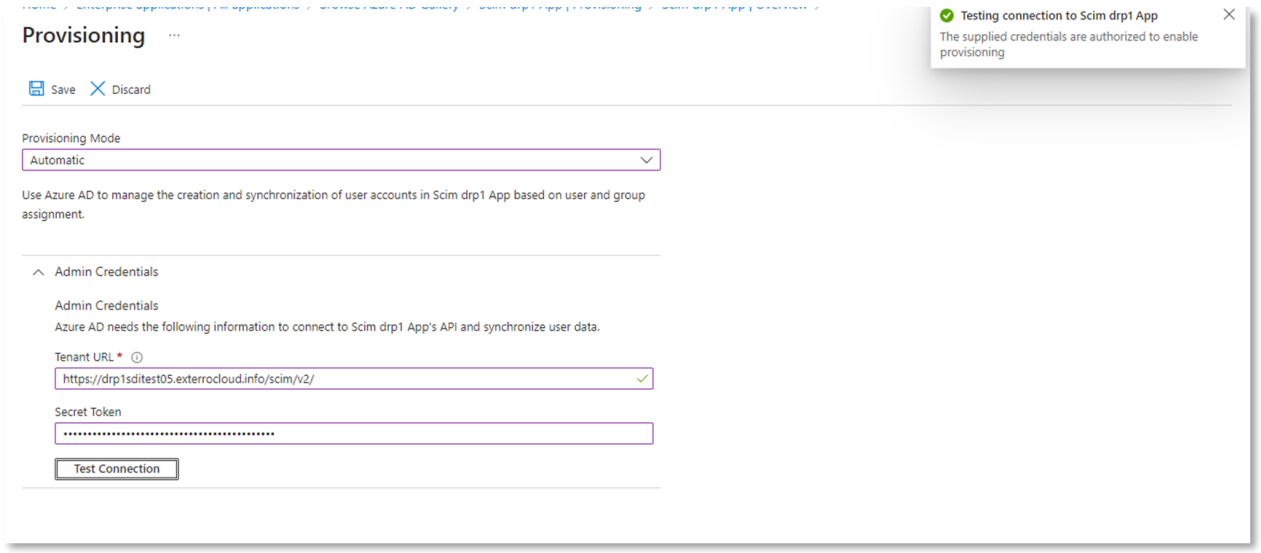


8. From the newly created application page,
   i. In the **Getting Started** section, select **Provision User Accounts** or navigate to the **Provisioning** section from the left pane.

9. Click **Get started.**



10. From the **Provisioning** page, select the **Provisioning Mode** as **Automatic**.
11. Enter the following details in the **Admin Credentials** section:
    - **Application URL:** Provide the **SCIM Connector Base URL** of Exterro.
    - **Secret Token:** Provide the **Generated API Key** via Exterro.



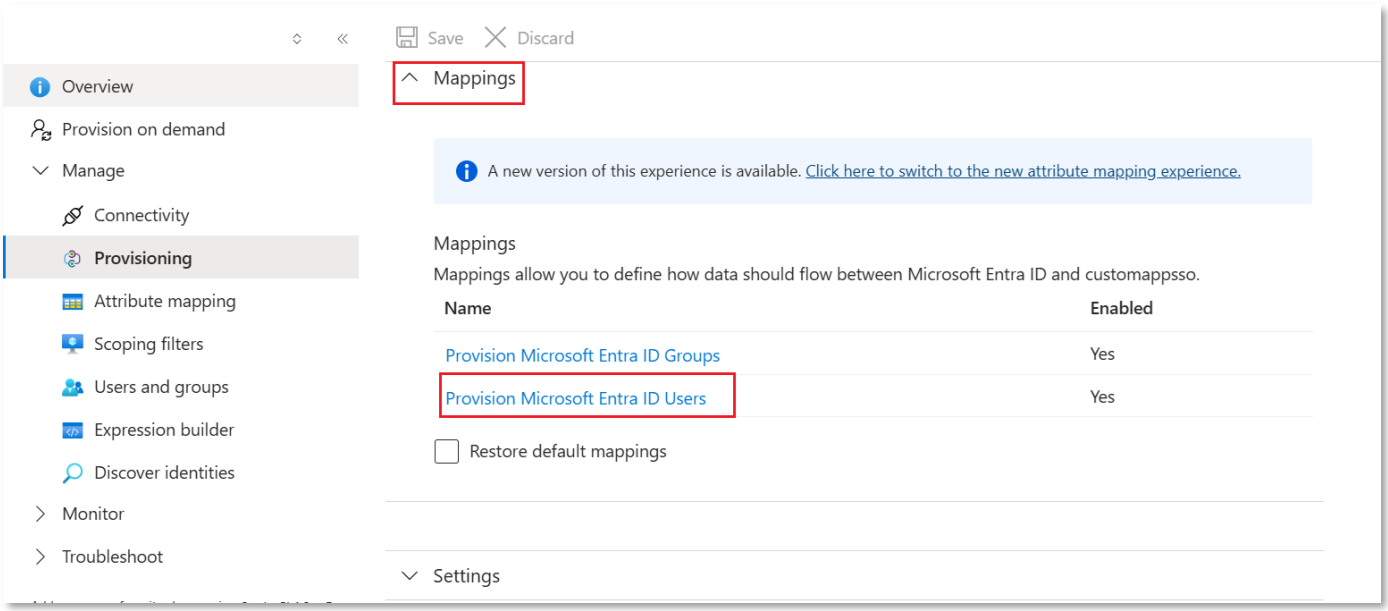
***Note**: Test Connections can be performed to validate the connection establishment between the Exterro FTK and the Microsoft Entra ID application.*

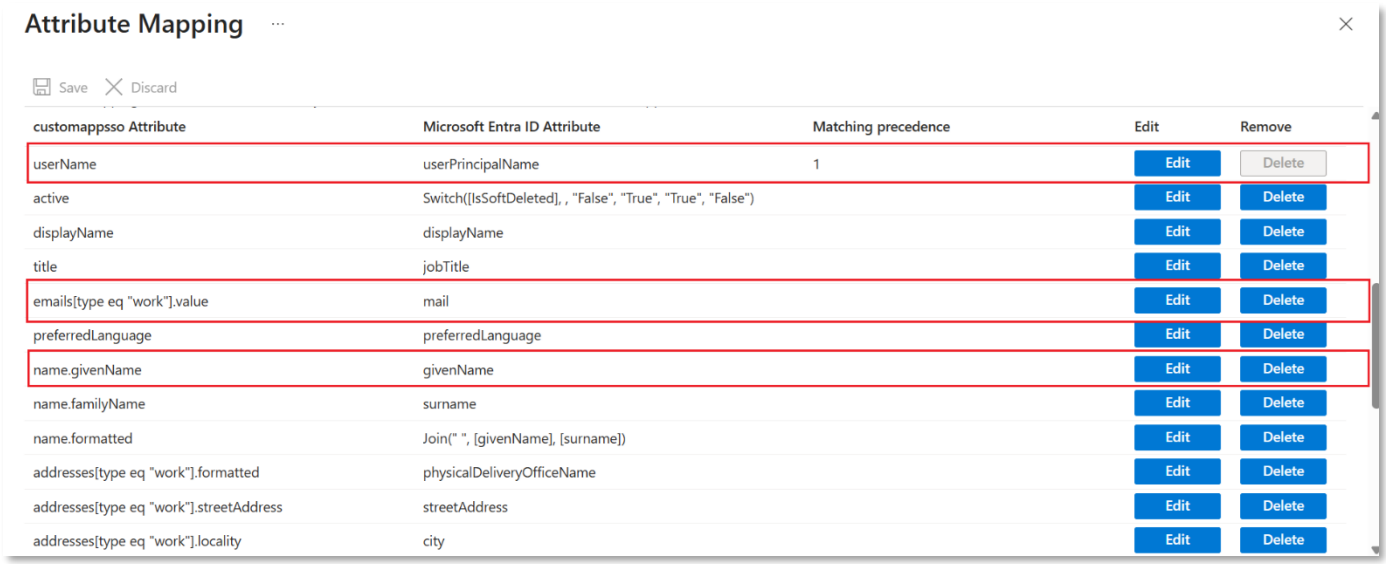
12. Click **Save.**

13. Upon saving the **Admin Credentials** from the **Mappings** section:

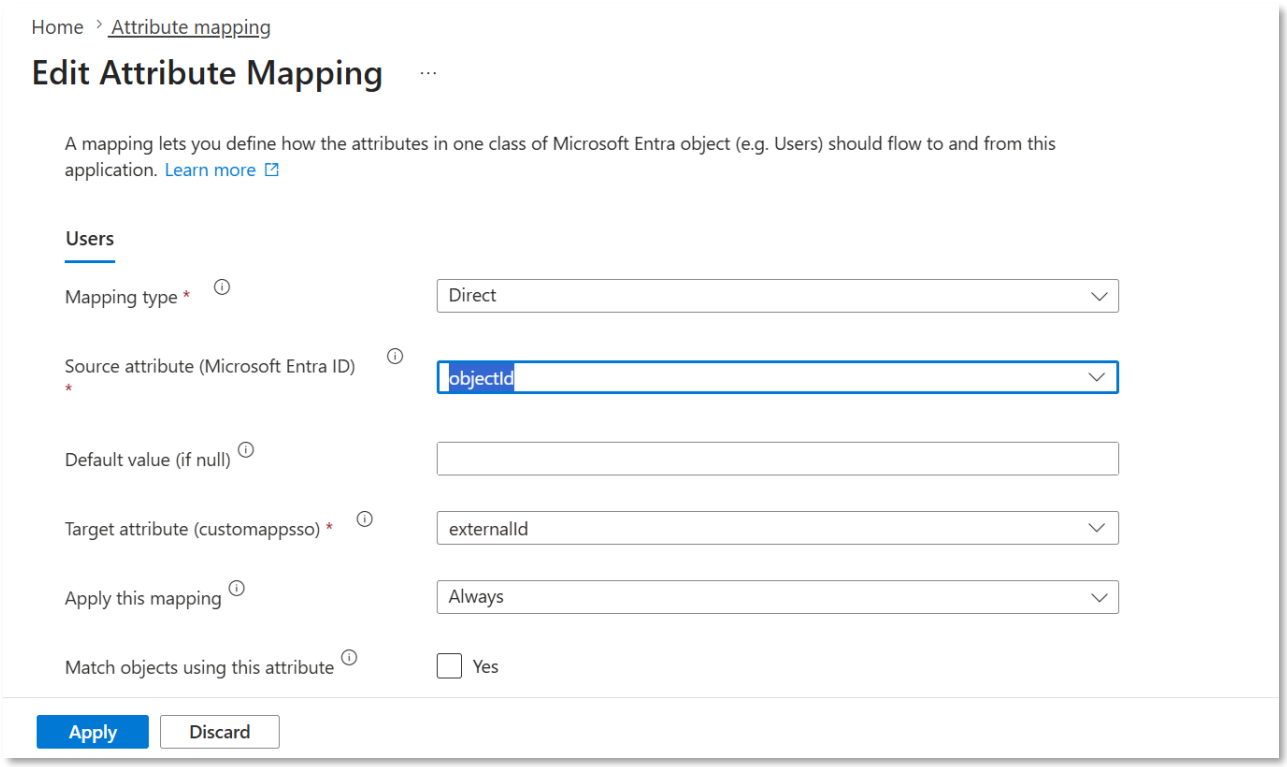
i. Click **Provision Azure Active Directory Users** to configure the Attribute Mapping.

ii. Click **Save**.

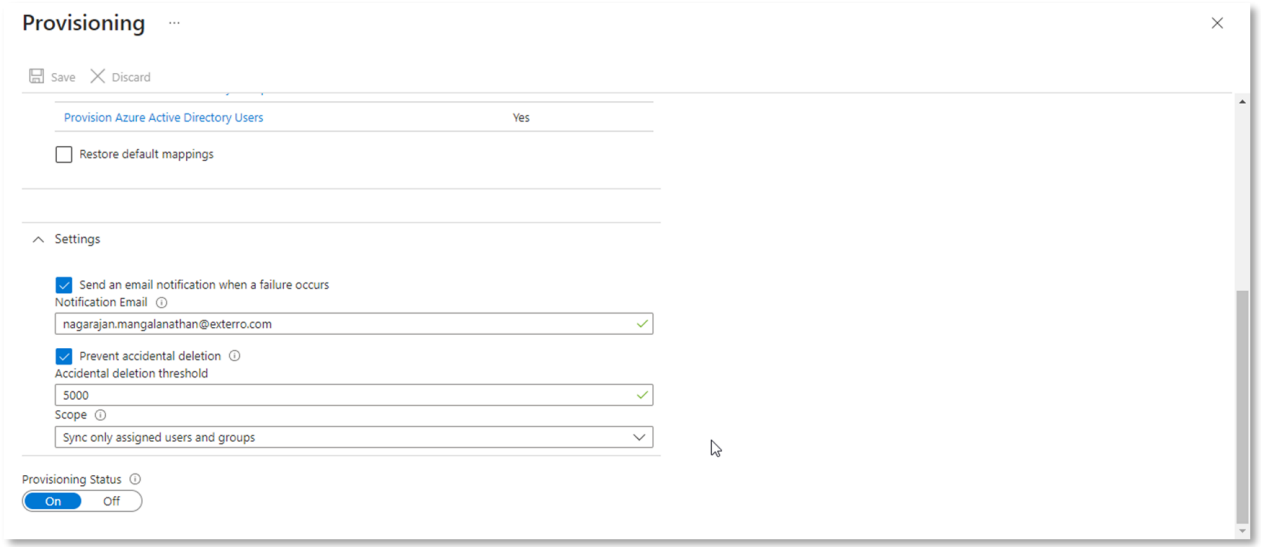




14. Locate the **Target attribute (customappsso)** with the value **externalId**, then edit it.



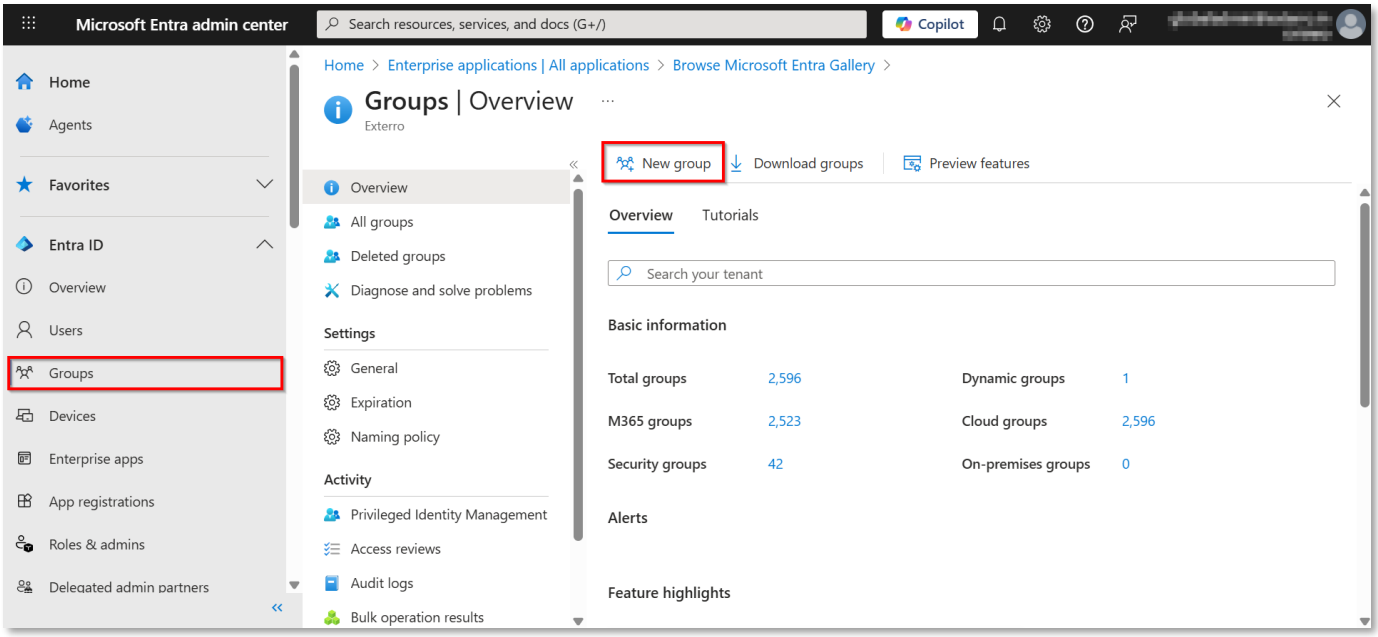
15. Update its **Source attribute (Microsoft EntraID)** as **objectId**.
16. Upon saving the **Mappings** on the **Settings** section, the required configuration on the user notifications and scopes can be configured here.



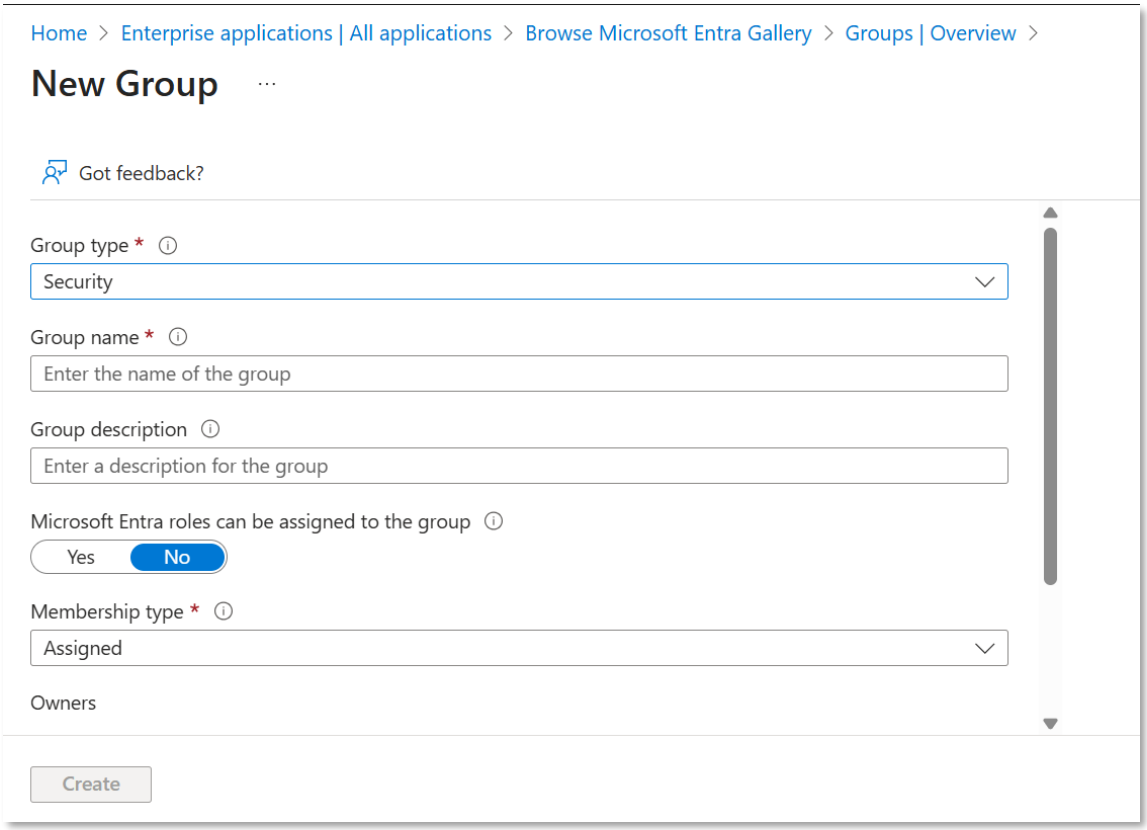
4.1.2 Creating a Group

Steps:

1. Log in to the **Microsoft Entra ID** application.
2. Navigate to the **Groups** from the left pane.
3. Click **New group**.



4. Provide the values for required fields on the **New Group** page.

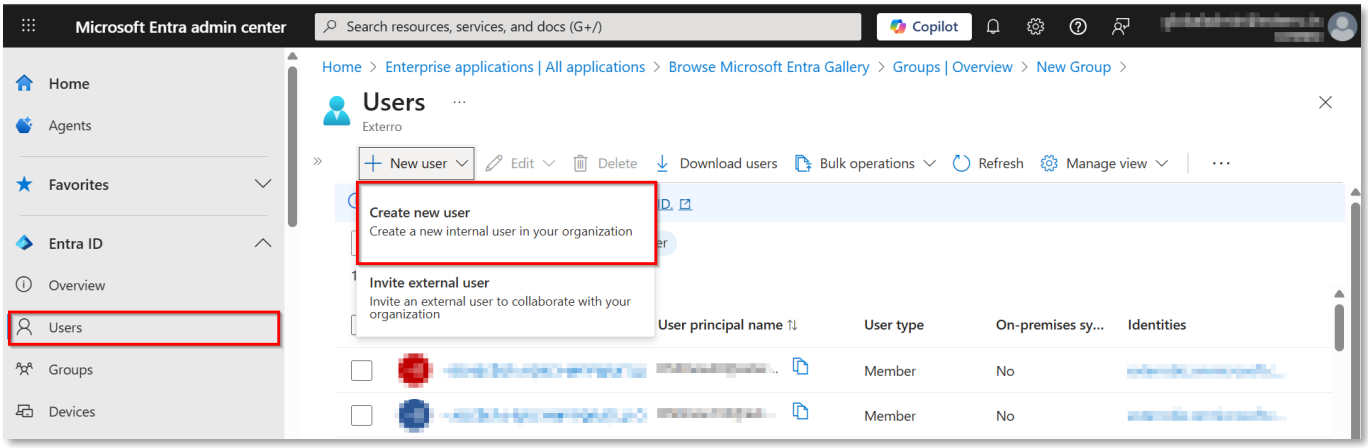


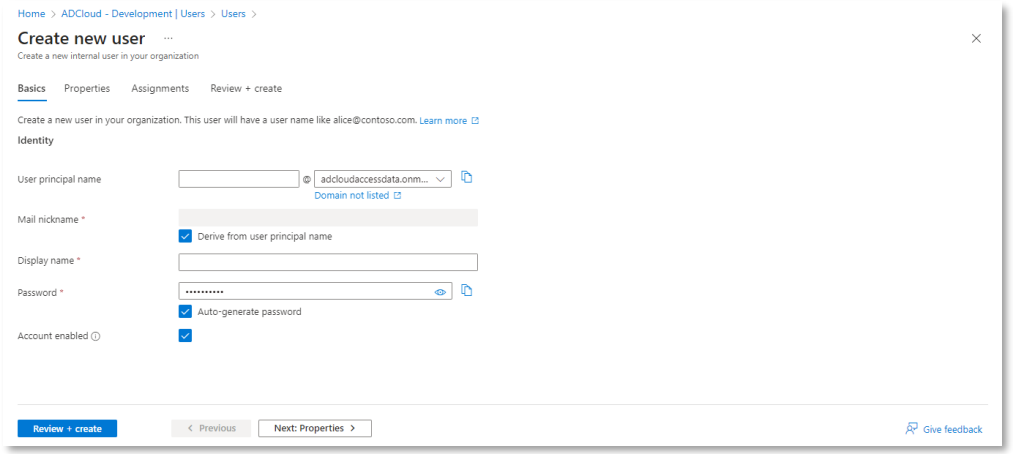
5. Click **Create.**

4.1.3 Adding People

Steps:

1. From the **Microsoft Entra ID** application.
2. Navigate to the **Users** section from the left pane.
3. Click **Create New User.**





4. Provide the user details and click **Create**.

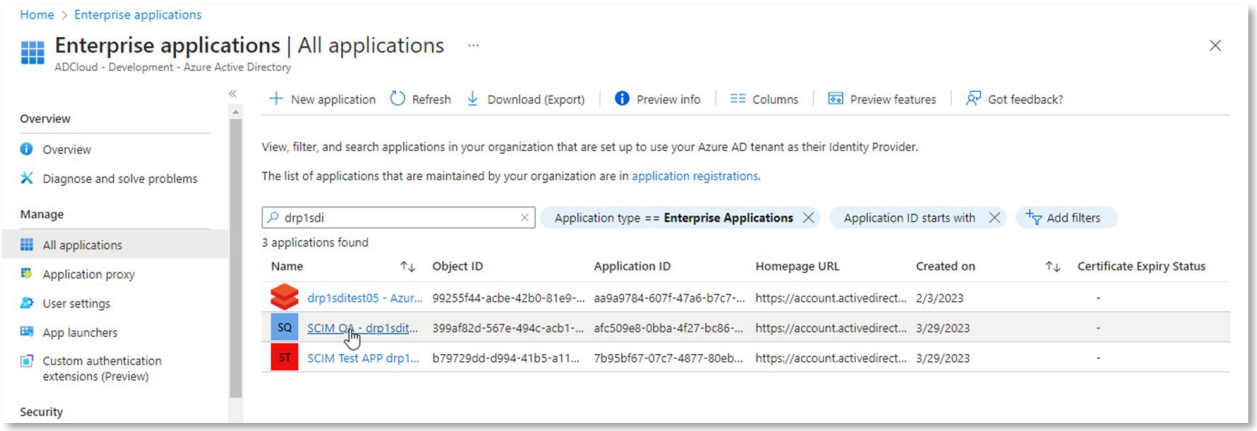
Notes:

- *The details provided for the People in the Microsoft Entra ID application will be synced with the respective Users in the Exterro FTK.*
- *UTC TimeZone will be set by default in case of providing an incorrect/empty value for the 'TimeZone' field.*

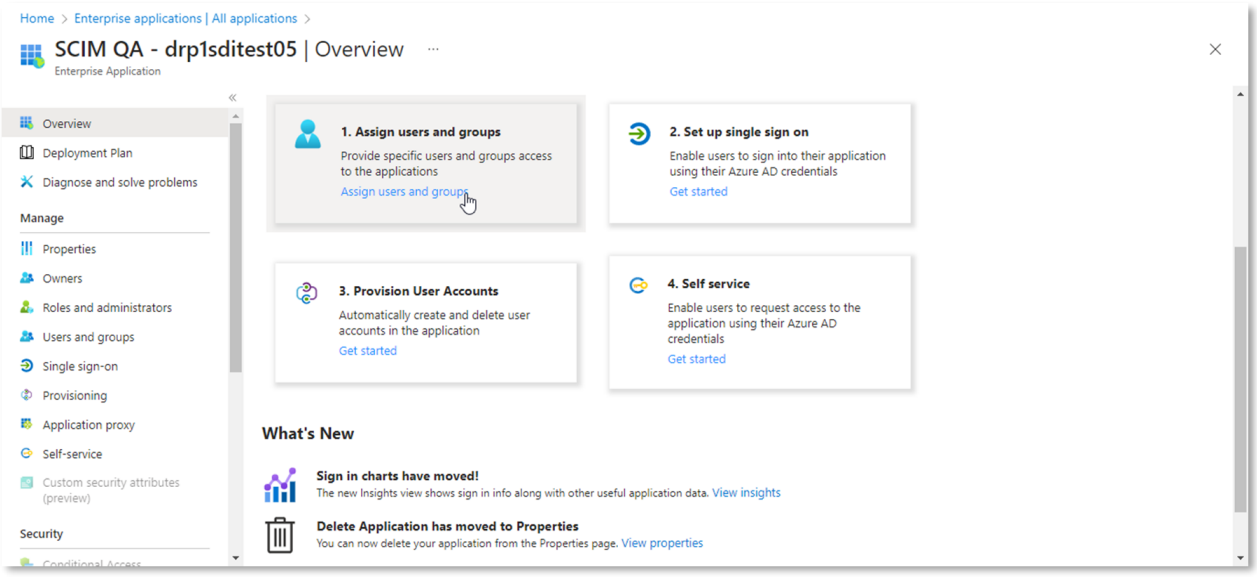
Assigning Users / Groups to an Application

Steps:

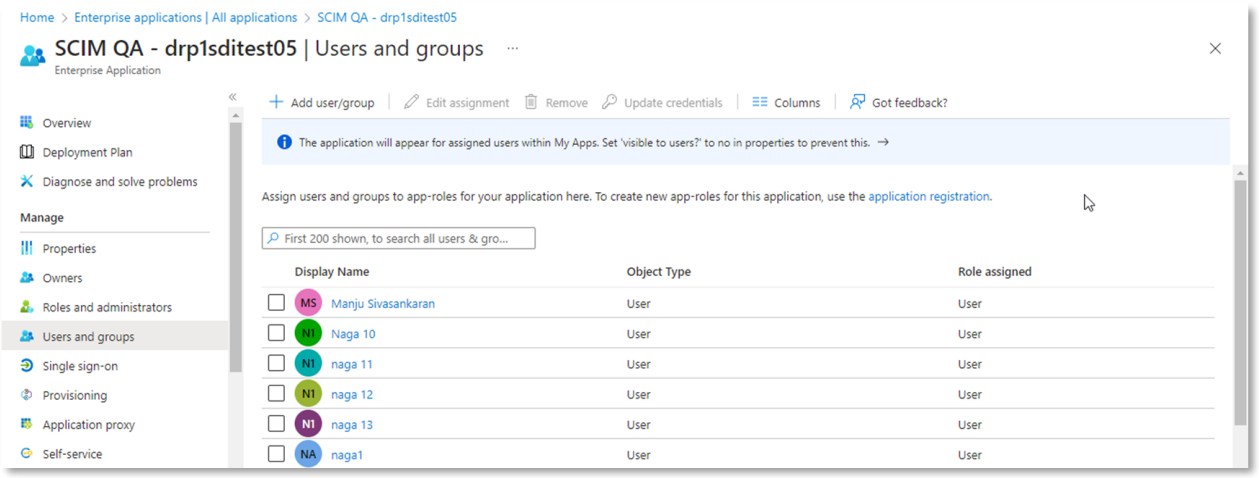
1. Log in to the **Microsoft Entra ID** application.
2. Navigate to the **Enterprise applications** page.
3. From the **All applications** page, click on the 'Microsoft Entra ID' app connected via Exterro.



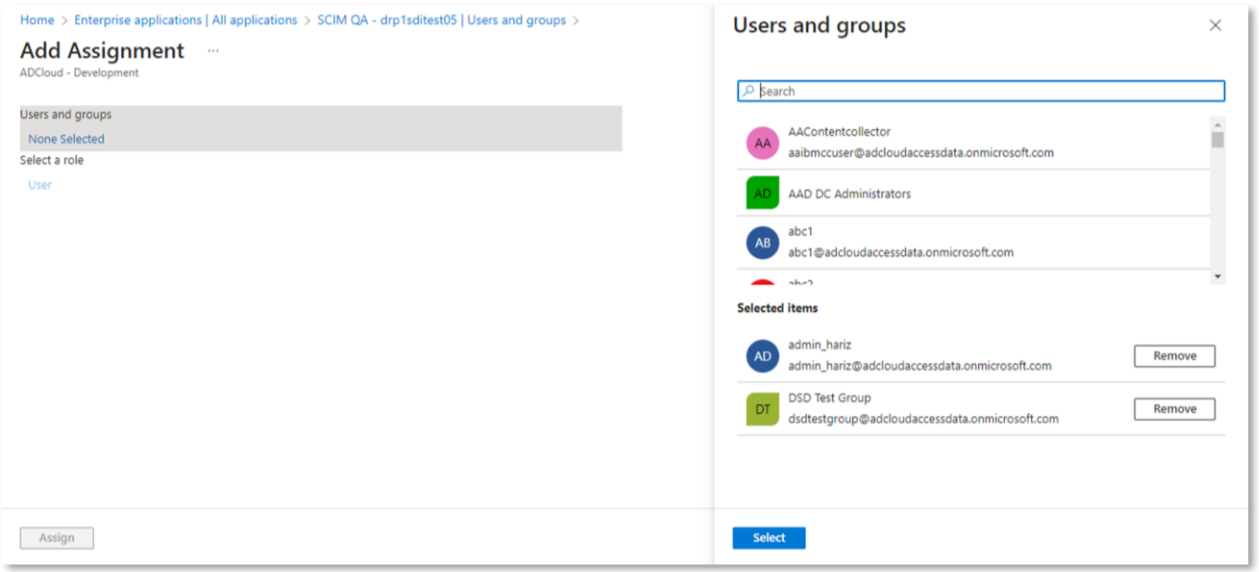
4. Select **Assign users and groups**.



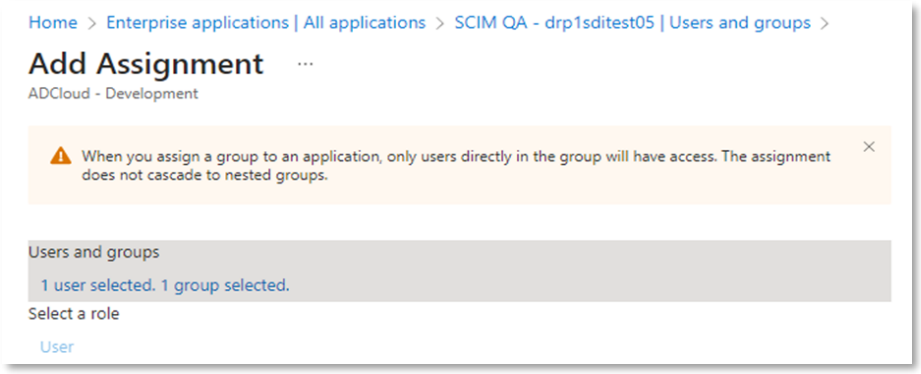
5. From the **Users and groups** page, click **Add user/group**.



6. On the **Add Assignment** page, click **None Selected** in **Users and groups**.
7. Search and select the users and groups under **Users and groups section** from the right pane.
8. Click **Select**.



9. From the **Add Assignment** page, click **Assign**.

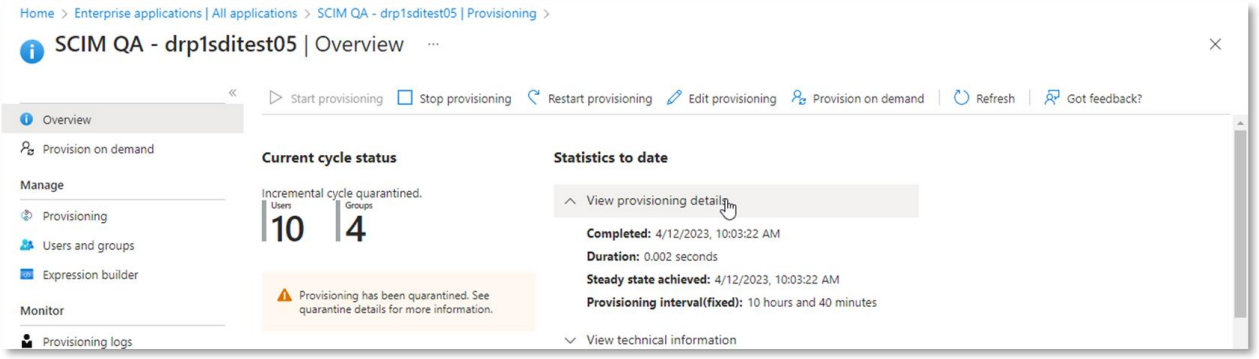


***Note**: The selected users and the assigned users and groups are listed under the 'Users and groups' page.*

10. Click the **Provisioning** option from the left pane. The following actions available on the 'Provisioning' page can be used for provisioning users and groups to the Exterro FTK from Microsoft Entra ID:
    - Start
    - Stop
    - Restart
    - Edit
    - Provision on demand action

***Notes**:*

- *The automatic provisioning occurs once every 40 minutes. If you need to sync users immediately, use the **Provision on demand** option.*
- *The **Provision on demand** action allows you to manually select and provision a single user into the Exterro FTK immediately.*



- *You can navigate to the **Monitor** section in the left pane and select **Provisioning logs** to monitor the users and groups with their provisioning status and details.*
- *While synchronizing users from the Microsoft Entra ID application to the Exterro FTK,*
  - *Only the users in 'Active' status will be created in the Exterro FTK.*
- *When the status of a user is changed in Microsoft Entra ID after the synchronization with the Exterro FTK, the updated status will not be reflected in the Exterro FTK.*
- *Since the users are authenticated via Microsoft Entra ID, only the users updated as 'Active' in Microsoft Entra ID will be able to access the Exterro application regardless of the status displayed for the corresponding user in the Exterro FTK.*

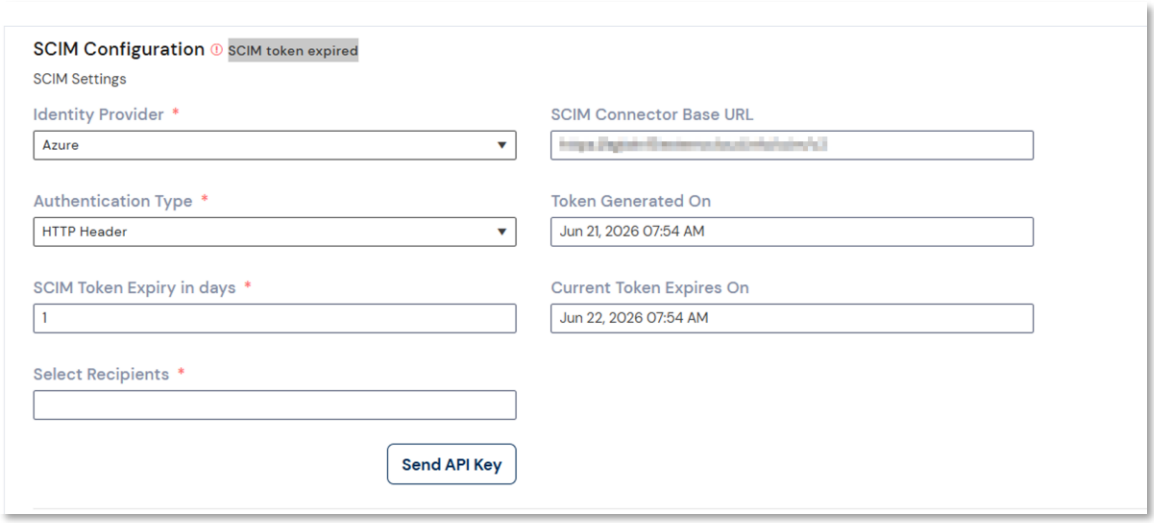
4.2 SCIM Token Lifecycle & Notifications

When configuring user synchronization via SCIM, managing token expiry is critical to ensuring uninterrupted user provisioning.

***Note**: When a user or group is removed from the Identity Provider (IdP), the corresponding user within the Exterro application will automatically be deactivated.*

4.2.1 Token Expiry Alerts

- **In-App Notifications:** If a token expires, a prominent **"SCIM token expired"** status badge will display inside the System Management configuration window.



- **Email Notifications:** In addition to the UI status indicator, an automated notification email will be sent immediately to the designated recipients when a token officially expires.

***Note**: To help you prevent sync interruptions, the system sends a warning notification 2 days before the SCIM token expires. This alert is visible both in the application interface and sent directly to your configured email recipients.*

4.3 SAML Configuration and Single Sign-On (SSO)

Customers must install and configure the SAML service to authenticate and log into their Exterro application using standard Single Sign-On credentials.

- Detailed setup instructions, metadata configurations, and mapping requirements can be found in the **Exterro - SAML Integration with FTK Applications**.

Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro. For usage questions, please check with your organization's internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:

Exterro, Inc.

2175 NW Raleigh St., Suite 110

Portland, OR 97210.

Telephone: 503-501-5100

Toll Free: 1-877-EXTERRO (1-877-398-3776)

Fax: 1-866-408-7310

General E-mail:info@exterro.com

Website: www.exterro.com