

FTK SCIM 2.0

USER PROVISIONING & CONFIGURATION GUIDE

JULY 2026

Table of Contents

About Exterro.....	3
1 Configuration Overview.....	3
1.1 Key Capabilities.....	3
2 Configuration Prerequisites.....	4
3 Configuring SCIM in Exterro FTKC	4
3.1 Step-by-Step UI Activation.....	5
3.2 Core Attribute Mapping Rules	8
3.3 Identity Provider Integration: Okta	9
3.3.1 Creating the App Integration	9
3.4 Configuring Connection & Credentials	12
3.5 Directory Groups & User Management.....	15
3.5.1 Creating a Group	15
3.6 To Push Groups to the created app.....	17
3.6.1 Adding People	19
4 Azure - SCIM Configuration	21
4.1 Microsoft Entra ID – Configurations	21
4.1.1 Setting up an App Integration.....	21
4.1.2 Creating a Group	27
4.1.3 Adding People	29
4.2 SCIM Token Lifecycle & Notifications	34
4.2.1 Token Expiry Alerts	34
4.3 SAML Configuration and Single Sign-On (SSO)	35
Contact Exterro	36

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*

The screenshot shows the 'Administration' section of the Exterro FTKC interface. The 'Configuration' tab is selected, and the 'SCIM Configuration' option is highlighted in the left sidebar. The main content area displays the 'SCIM Configuration' settings, which include:

- Identity Provider:** A dropdown menu with 'Okta' selected.
- Authentication Type:** A dropdown menu with 'HTTP Header' selected.
- SCIM Token Expiry in days:** A text input field with '1' entered.
- SCIM Connector Base URL:** A text input field with a placeholder URL.
- Token Generated On:** A date and time field showing 'Jun 13, 2026 01:23 PM'.
- Current Token Expires On:** A date and time field showing 'Jun 14, 2026 01:23 PM'.
- Select Recipients:** A text input field with a placeholder email address and a search icon.
- Send API Key:** A button to generate and send the API key.

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

The screenshot displays the 'SCIM Configuration' page with the following elements:

- SCIM Configuration** header with a sub-header **SCIM Settings**.
- Identity Provider *** section: A dropdown menu currently showing 'Okta'. Below it is a search bar with a magnifying glass icon and a 'Select Field' label. Two options are listed: 'Azure' and 'Okta' (which is highlighted with a dark blue background).
- SCIM Connector Base URL** section: A text input field containing a masked URL.
- Token Generated On** section: A text input field showing the date and time 'Jun 17, 2026 01:35 PM'.
- Current Token Expires On** section: A text input field showing the date and time 'Jun 18, 2026 01:35 PM'.
- Select Recipients *** section: A text input field.
- A **Send API Key** button located at the bottom right of the form.

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

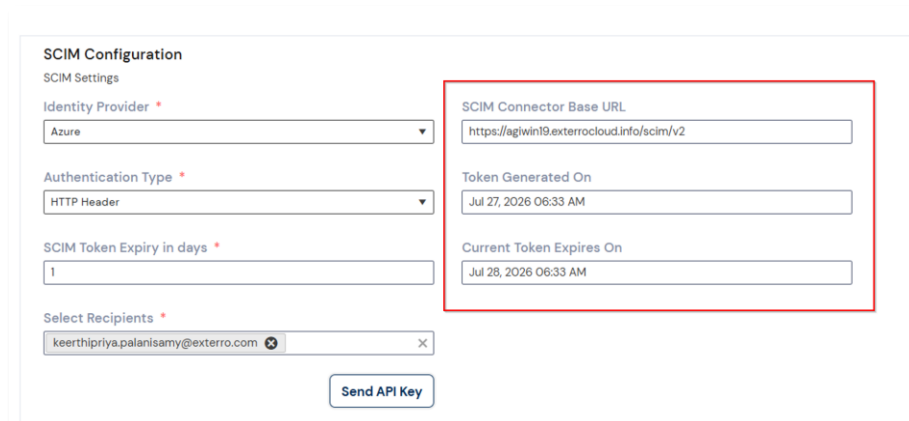
The screenshot displays the 'Administration' section of the Exterro interface. Under the 'Configuration' tab, the 'SCIM Configuration' option is selected in the left-hand menu. The main content area shows the 'SCIM Configuration' settings. The 'Identity Provider' is set to 'Okta'. The 'Authentication Type' is set to 'HTTP Header', and a dropdown menu is open showing 'HTTP Header' as the selected option. The 'Select Recipients' field is currently empty. A 'Send API Key' button is located at the bottom right of the configuration panel.

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.

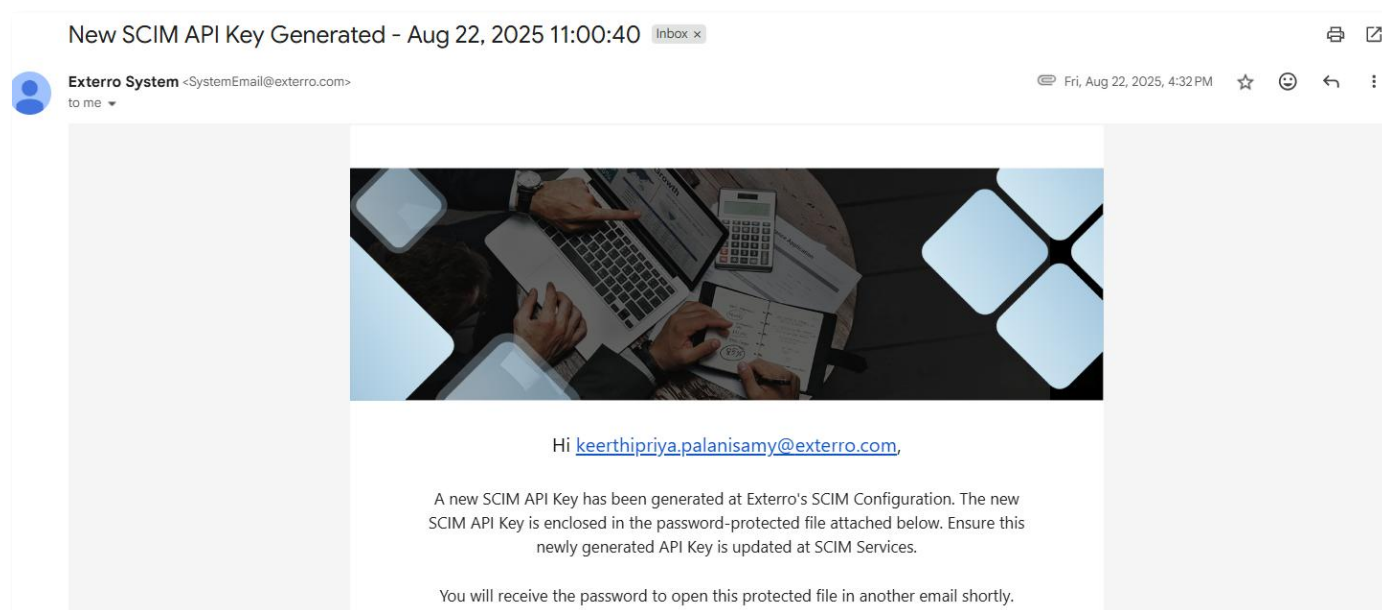
Note: Ensure to keep a copy of the **SCIM Connector Base URL** for your reference. You will need to provide this value when configuring the newly created app integration in the corresponding SCIM-enabled Identity Provider application.



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.

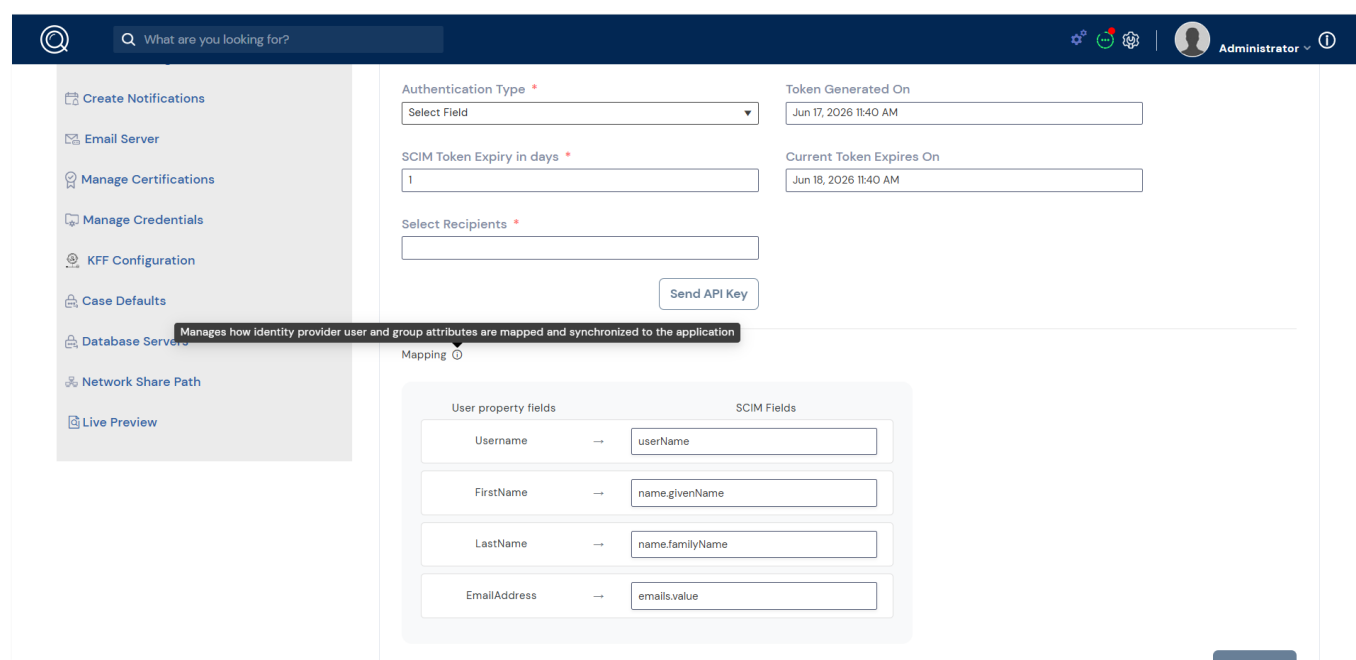
Note: It is required to update the generated token in the SCIM-configured Identity Provider application for the successful integration of SCIM Services with the Exterro FTK.



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.



Manages how identity provider user and group attributes are mapped and synchronized to the application

User property fields	SCIM Fields
Username	userName
FirstName	name.givenName
LastName	name.familyName
EmailAddress	emails.value

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**.

The screenshot shows the Okta Admin Console dashboard. On the left is a navigation sidebar with items: Dashboard, Tasks, Notifications, Getting Started, Directory, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area is titled 'Overview' and 'Updated at October 30, 10:24 PM'. It features three summary cards: 'Users' with a count of 13 and an 8% increase, 'Groups' with a count of 21 and an 11% increase, and 'SSO Apps' with a count of 8. To the right is a 'Status' section showing 'Okta service' as 'Operational' and 'Agents' as 'No agents added'. Below these is a 'Tasks' table with columns 'Type', 'Items', and 'Description'. The table lists four tasks: 'To-do' (50 items), 'Info' (1 item), 'Error' (1 item), and 'Error' (6 items). At the bottom of the main area are 'Org changes' and 'Security Monitoring' sections.

Type	Items	Description
To-do	50	Application accounts need deprovisioning
Info	1	Applications can be updated to use provisioning
Error	1	Profile push updates encountered errors
Error	6	Application assignments encountered errors

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

The screenshot shows the 'Applications' page in the Okta Admin Console. The left sidebar has 'Applications' selected. The main content area is titled 'Applications' and includes a 'Developer Edition provides a limited number of apps.' message. Below this message are four buttons: 'Create App Integration' (highlighted with a red box), 'Browse App Catalog', 'Assign Users to App', and 'More'.

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

Create a new app integration

Sign-in method

[Learn More](#)

☐ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

☒ **SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

☐ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

☐ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel Next

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

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name

App logo (optional)

App visibility

☐ Do not display application icon to users

Cancel Next

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**.

App Settings Cancel

Application label
This label displays under the app on your home page

Application visibility ☐ Do not display application icon to users

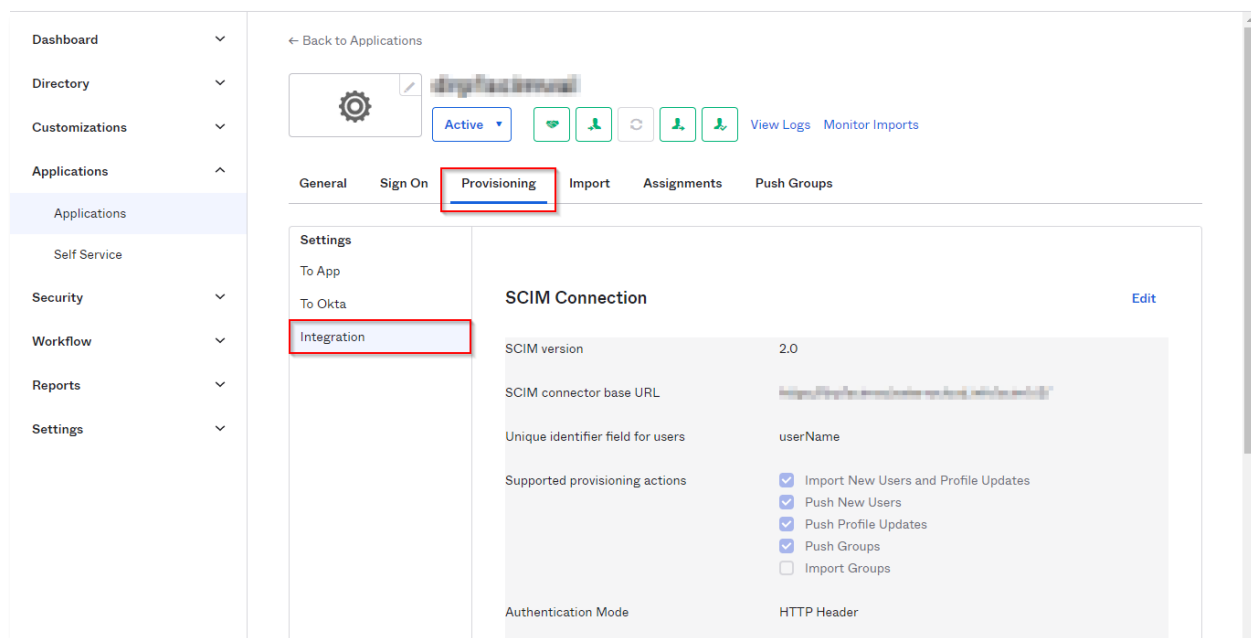
Provisioning ☒ Enable SCIM provisioning

Auto-launch ☐ Auto-launch the app when user signs into Okta.

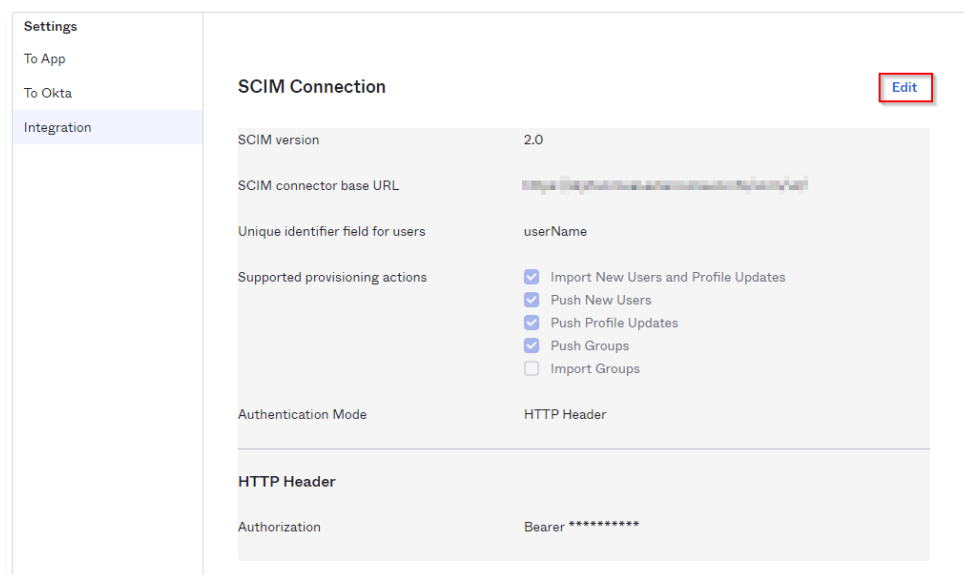
General Settings
All fields are required unless marked optional. Some fields may no longer be editable.

3.4 Configuring Connection & Credentials

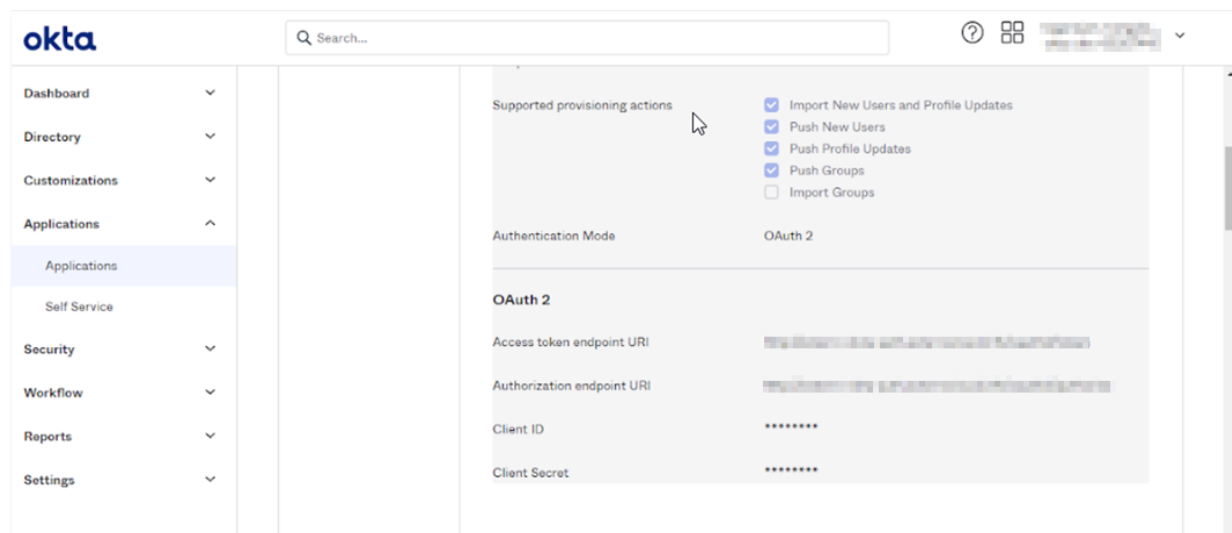
1. From within your newly saved Okta app, select the freshly visible **Provisioning** tab menu element.



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'.
 - o 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.



The screenshot shows the 'SCIM Connection' configuration window. On the left is a sidebar with 'Settings' expanded, containing 'To App', 'To Okta', and 'Integration' (which is selected). The main panel is titled 'SCIM Connection' and includes a 'Cancel' button in the top right. The configuration fields are as follows:

- SCIM version: 2.0
- SCIM connector base URL: [Redacted]
- Unique identifier field for users: userName
- Supported provisioning actions:
 - ☒ Import New Users and Profile Updates
 - ☒ Push New Users
 - ☒ Push Profile Updates
 - ☒ Push Groups
 - ☐ Import Groups
- Authentication Mode: HTTP Header

Below these is the 'HTTP Header' section with an 'Authorization' field set to 'Bearer' and a masked token '*****'. At the bottom right of the main panel is a button labeled 'Test Connector Configuration'. Below the main panel, there are 'Save' and 'Cancel' buttons; the 'Save' button is highlighted with a red rectangle.

- 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

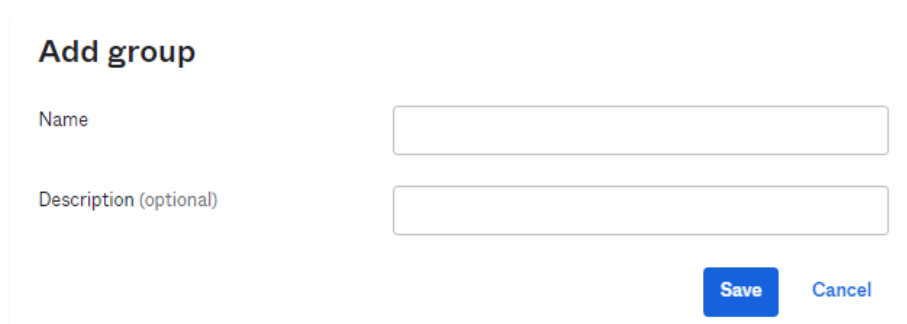
Steps:

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

The screenshot displays the Okta Groups management interface. On the left, a sidebar contains navigation links: Dashboard, Directory, People, Groups (highlighted), Devices, Profile Editor, Directory Integrations, Profile Sources, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area is titled 'Groups' and includes tabs for 'All' and 'Rules'. A search bar with the placeholder 'Search by group name' and a magnifying glass icon is present, along with an 'Add group' button. Below the search bar is an 'Advanced search' dropdown and a 'Group source type' dropdown set to 'All'. A table lists existing groups with columns for 'Group name', 'People', and 'Applications'. The table shows 15 groups, with the first six visible.

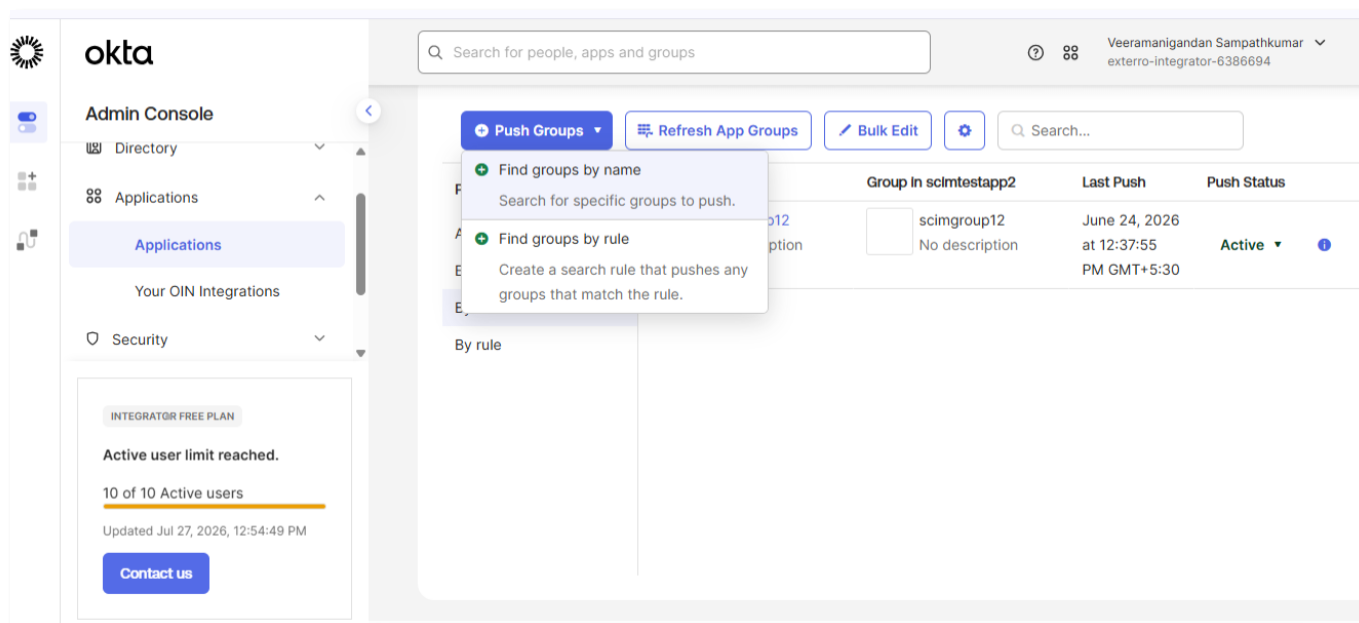
Group name	People	Applications
SCIM_Release	0	1
SCIM_Release Group		
Exterro Admin	5	0
Admin		
SCIM_Group	5	2
No description		
Everyone	15	2
all users in your organization		
EXT-Admin	6	0
No description		
EXT-User	6	1
No description		

- Click **Add group**.



The 'Add group' form is a simple interface with two text input fields. The first field is labeled 'Name' and the second is labeled 'Description (optional)'. At the bottom right of the form are two buttons: 'Save' and 'Cancel'.

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



The screenshot shows the Okta Admin Console interface. On the left is a sidebar with navigation links: Admin Console, Directory, Applications, Your OIN Integrations, and Security. The 'Applications' link is selected. The main content area has a search bar at the top and a 'Push Groups' button. A dropdown menu is open from the 'Push Groups' button, showing two options: 'Find groups by name' (with a subtext 'Search for specific groups to push.') and 'Find groups by rule' (with a subtext 'Create a search rule that pushes any groups that match the rule.'). Below the dropdown is a table with columns: 'Group in scimtestapp2', 'Last Push', and 'Push Status'. The table contains one row with the group 'scimgroup12', a last push date of 'June 24, 2026 at 12:37:55 PM GMT+5:30', and a status of 'Active'. At the bottom left, there is a notification box for the 'INTEGRATOR FREE PLAN' stating 'Active user limit reached. 10 of 10 Active users' and a 'Contact us' button.

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.

← Back to Applications

drp1scimval

Active View Logs Monitor Imports

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

Push Groups to drp1scimval

Push Groups Refresh App Groups Bulk Edit Search...

Pushed Groups	Group in Okta	Group in drp1scimval	Last Push	Push Status
All	1 group has an error. Click Retry All Groups to re-push all groups that have an error. Retry All Groups			
Errors	Show Errors			
By name	☒ Exterro Admin Admin	☐ Exterro Admin Admin	Oct 31, 2022 4:38:31 AM	Active ●
By rule	☒ All Users with Rights R...	☐ All Users with Rights R...	Oct 31, 2022 4:45:32 AM	Error ●
	☒ All Users with Rights R...	☐ All Users with Rights R...	Oct 31, 2022 4:06:17 AM	Active ●

4. Search for the required groups and push them.

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

Push Groups to **drp1scimval**

[Close](#)

Pushed Groups

All

Errors

By name

By rule

Push groups by name

To sync group memberships from Okta to drp1scimval, choose a group in Okta and a group in the app.

☒ Push group memberships immediately

Group	Match result & push action
☐ Admin	No Match found Create Group
	SDI Admin

[Save](#) [Save & Add Another](#)

5. Click **Save**.

Push Groups [Refresh App Groups](#) [Bulk Edit](#) [Settings](#)

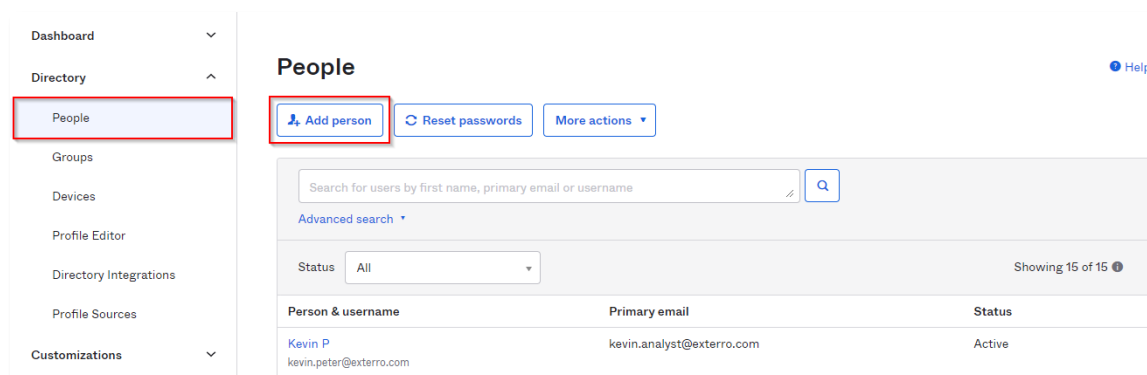
Pushed Groups	Group in Okta	Group in drp1scimval	Last Push	Push Status
All	☒ Exterro Admin Admin	☐ Exterro Admin Admin	Oct 31, 2022 4:38:31 AM	Active Info
Errors	☒ LIA Admin	☐ LIA Admin	Oct 31, 2022 5:04:50 AM	Error Info
By name	☒ BOM test	☐ BOM test	Oct 31, 2022 4:06:17 AM	Active Info
By rule	☒ BOM test	☐ BOM test	Oct 31, 2022 4:34:51 AM	Active Info
	☒ BOM test	☐ BOM test	Oct 31, 2022 5:04:50 AM	Error Info
	☒ BOM test	☐ BOM test	Oct 31, 2022 4:41:23 AM	Active Info

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**.

The 'Add Person' form contains the following fields and options:

- User type:** A dropdown menu currently set to 'User'.
- First name:** A text input field.
- Last name:** A text input field.
- Username:** A text input field with a placeholder 'Must be an email'.
- Primary email:** A text input field.
- Groups (optional):** A text input field.
- Activation:** A dropdown menu currently set to 'Activate now'.
- Checkbox:** An unchecked checkbox labeled 'I will set password'.
- Buttons:** 'Save', 'Save and Add Another', and 'Cancel'.

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.

Home > Administration

What are you looking for?

Administrator

User Management System Management

Configuration Site Server Console Hash Sets KFF Groups System Log **Activity Log** Jobs AWS S3 Management

Activity Logs 7

Activity Date	User Name	Activity	Category	Machine IP
17/06/2026 12:19:49 PM	Boopathy	Admin roles for Group: scimgroup12 have been updated	UpdateGroup	192.168.1.101
17/06/2026 12:19:49 PM	Boopathy	Project associations have been updated for Group: scimgroup12	UpdateGroup	192.168.1.101
17/06/2026 12:19:49 PM	Boopathy	User associations have been updated for Group: scimgroup12	UpdateGroup	192.168.1.101
17/06/2026 12:19:48 PM	Boopathy	User Group: scimgroup12 updated	UpdateGroup	192.168.1.101
17/06/2026 12:17:00 PM	Boopathy	User associations have been updated for Group: scimgroup12	UpdateGroup	192.168.1.101
17/06/2026 12:17:00 PM	Boopathy	User Group: scimgroup12 updated	UpdateGroup	192.168.1.101
17/06/2026 12:17:00 PM	Boopathy	User Group: scimgroup12 created	CreateGroup	192.168.1.101

Page 1 Of 1 10 Items per page 1 - 7 Of 7

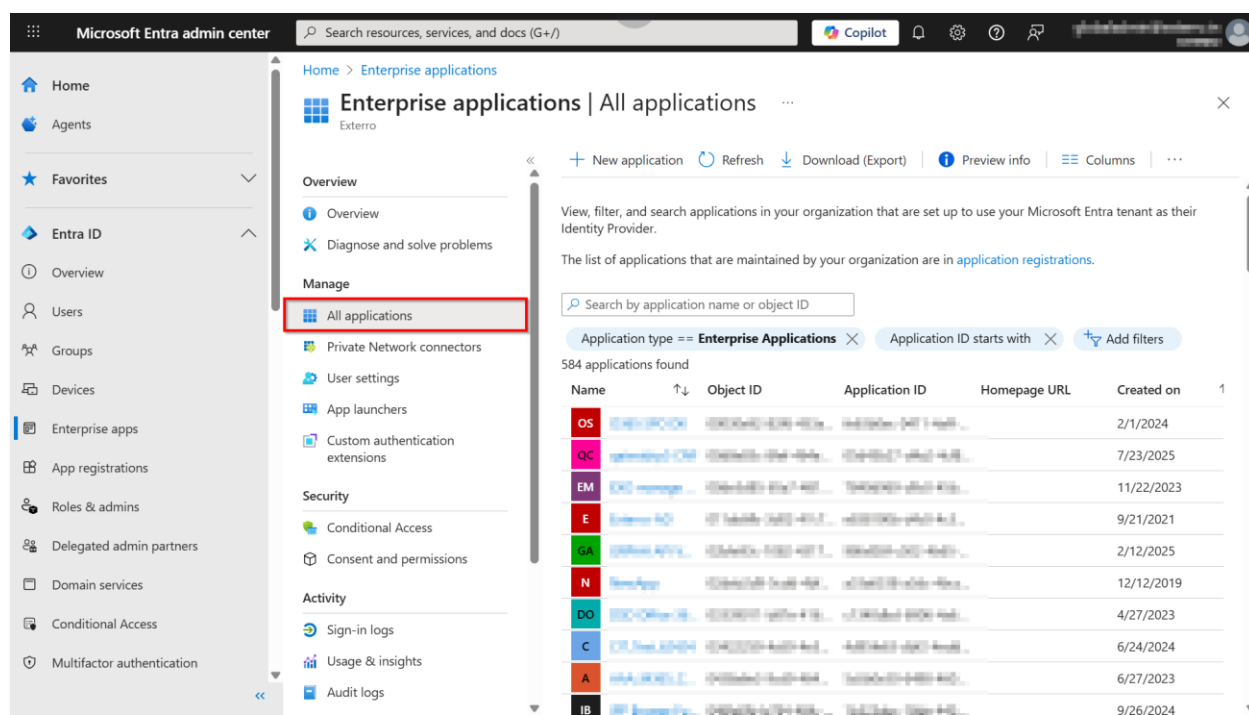
4 Azure - SCIM Configuration

4.1 Microsoft Entra ID – Configurations

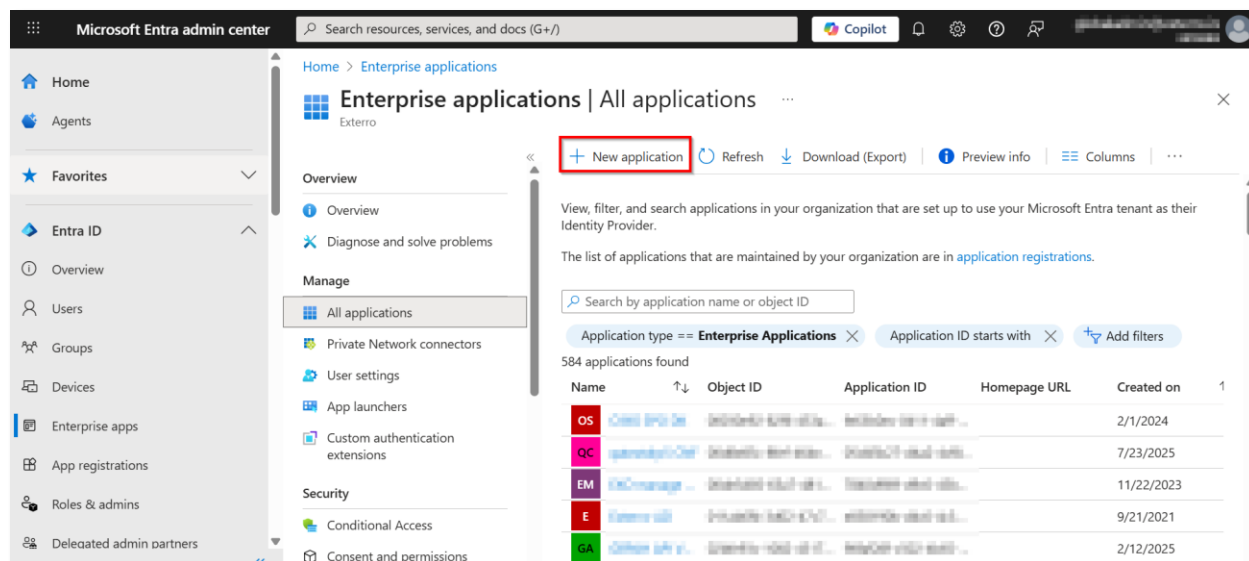
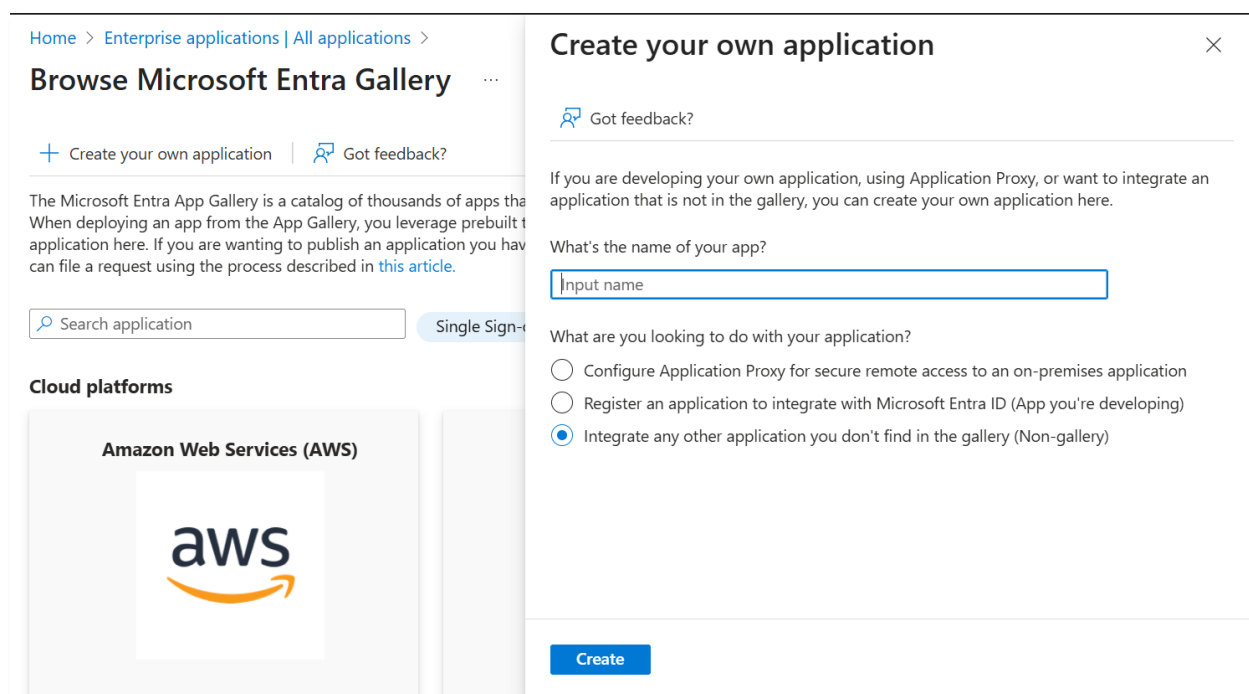
4.1.1 Setting up an App Integration

Steps:

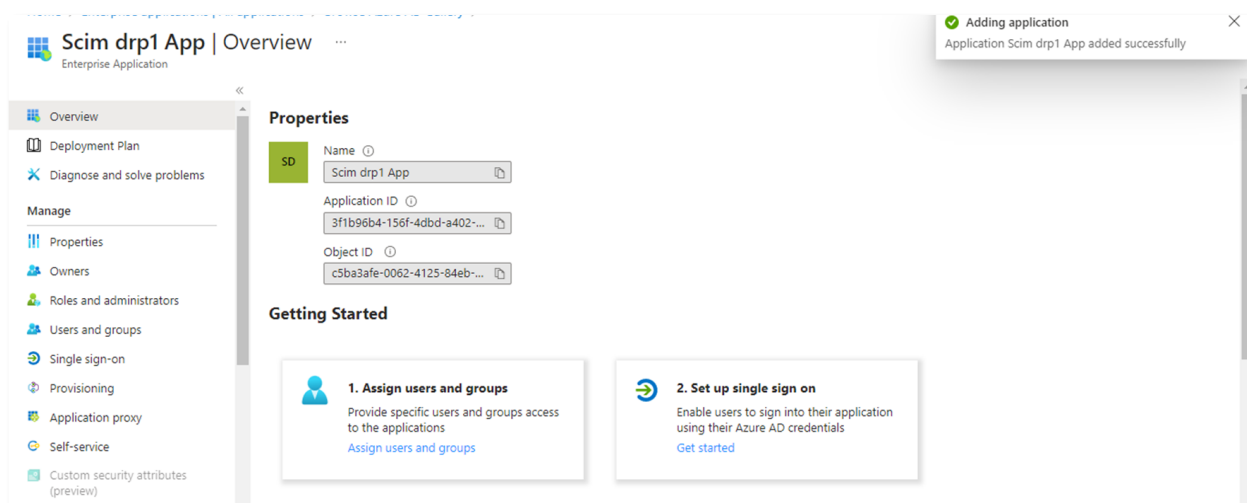
1. Log in to the Microsoft Entra ID application.
2. Navigate to the **Enterprise applications** page.



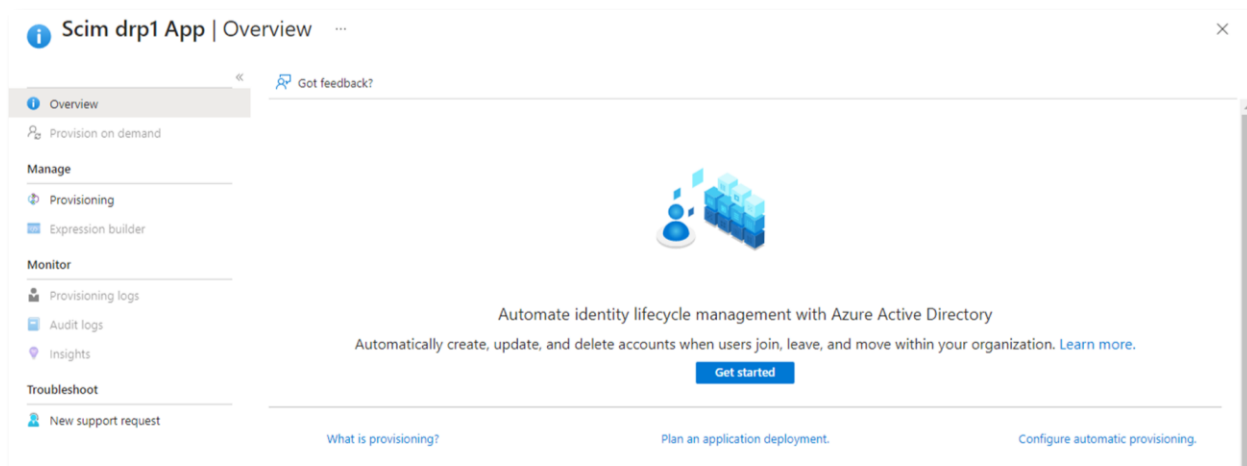
3. Select **All applications** from the left pane.

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

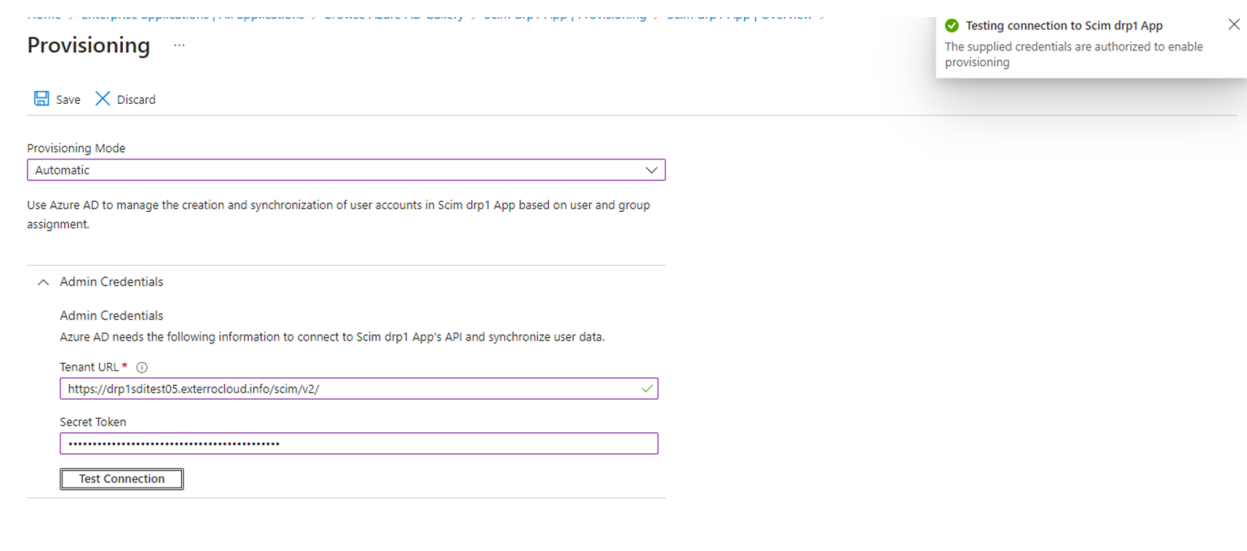
6. Enter the following details to set up the new application in the right pane,
 - a. What's the name of your app?
 - b. What are you looking to do with your application?
 - o It is recommended to select 'Integrate any other application you don't find in the gallery (non-gallery)'.
7. Click **Create**.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

- o **Application URL:** Provide the **SCIM Connector Base URL** of Exterro.
- o **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**.

Overview

Provision on demand

Manage

Connectivity

Provisioning

Attribute mapping

Scoping filters

Users and groups

Expression builder

Discover identities

Monitor

Troubleshoot

Save Discard

^ Mappings

A new version of this experience is available. [Click here to switch to the new attribute mapping experience.](#)

Mappings

Mappings allow you to define how data should flow between Microsoft Entra ID and customappsso.

Name	Enabled
Provision Microsoft Entra ID Groups	Yes
Provision Microsoft Entra ID Users	Yes

☐ Restore default mappings

Settings

Attribute Mapping

Save Discard

customappsso Attribute	Microsoft Entra ID Attribute	Matching precedence	Edit	Remove
userName	userPrincipalName	1	Edit	Delete
active	Switch([IsSoftDeleted], "False", "True", "True", "False")		Edit	Delete
displayName	displayName		Edit	Delete
title	jobTitle		Edit	Delete
emails[type eq "work"].value	mail		Edit	Delete
preferredLanguage	preferredLanguage		Edit	Delete
name.givenName	givenName		Edit	Delete
name.familyName	surname		Edit	Delete
name.formatted	Join(" ", [givenName], [surname])		Edit	Delete
addresses[type eq "work"].formatted	physicalDeliveryOfficeName		Edit	Delete
addresses[type eq "work"].streetAddress	streetAddress		Edit	Delete
addresses[type eq "work"].locality	city		Edit	Delete

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

Home > [Attribute mapping](#)

Edit Attribute Mapping

A mapping lets you define how the attributes in one class of Microsoft Entra object (e.g. Users) should flow to and from this application. [Learn more](#)

Users

Mapping type * ⓘ Direct

Source attribute (Microsoft Entra ID) * ⓘ objectId

Default value (if null) ⓘ

Target attribute (customappsso) * ⓘ externalId

Apply this mapping ⓘ Always

Match objects using this attribute ⓘ ☐ Yes

[Apply](#) [Discard](#)

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.

Provisioning

[Save](#) [Discard](#)

[Provision Azure Active Directory Users](#) Yes

☐ Restore default mappings

Settings

☒ Send an email notification when a failure occurs ⓘ
Notification Email ⓘ nagarajan.manganathan@exterro.com ✓

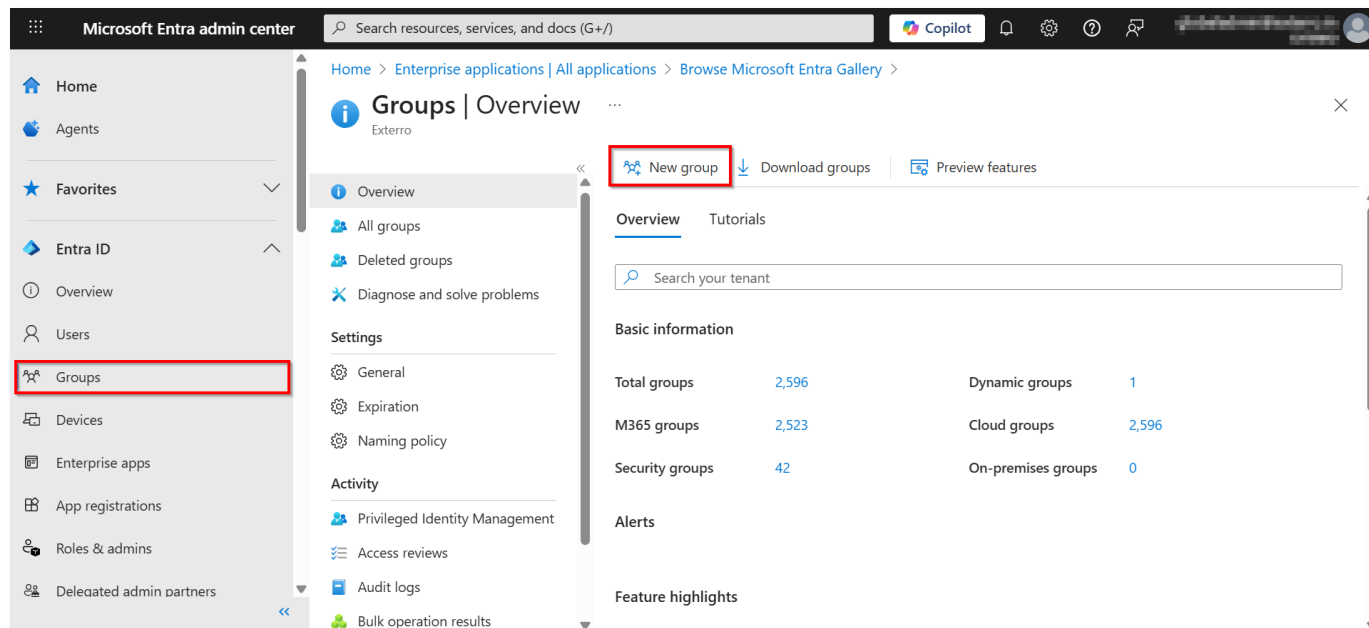
☒ Prevent accidental deletion ⓘ
Accidental deletion threshold ⓘ 5000 ✓
Scope ⓘ Sync only assigned users and groups

Provisioning Status ⓘ
☒ On ☐ Off

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.

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Groups | Overview >

New Group

[Got feedback?](#)

Group type * ⓘ
Security

Group name * ⓘ
Enter the name of the group

Group description ⓘ
Enter a description for the group

Microsoft Entra roles can be assigned to the group ⓘ
☐ Yes ☒ No

Membership type * ⓘ
Assigned

Owners

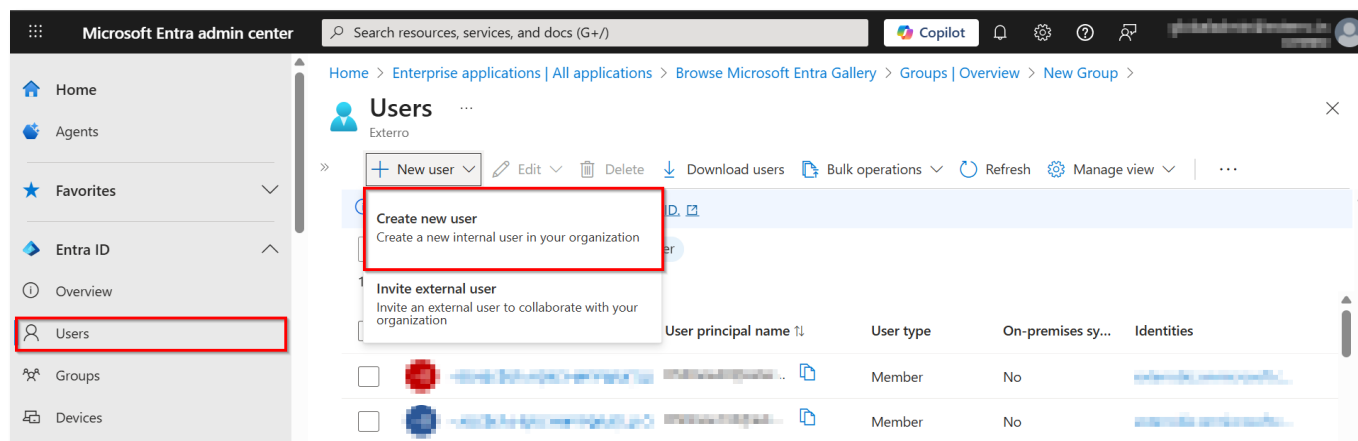
Create

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**.

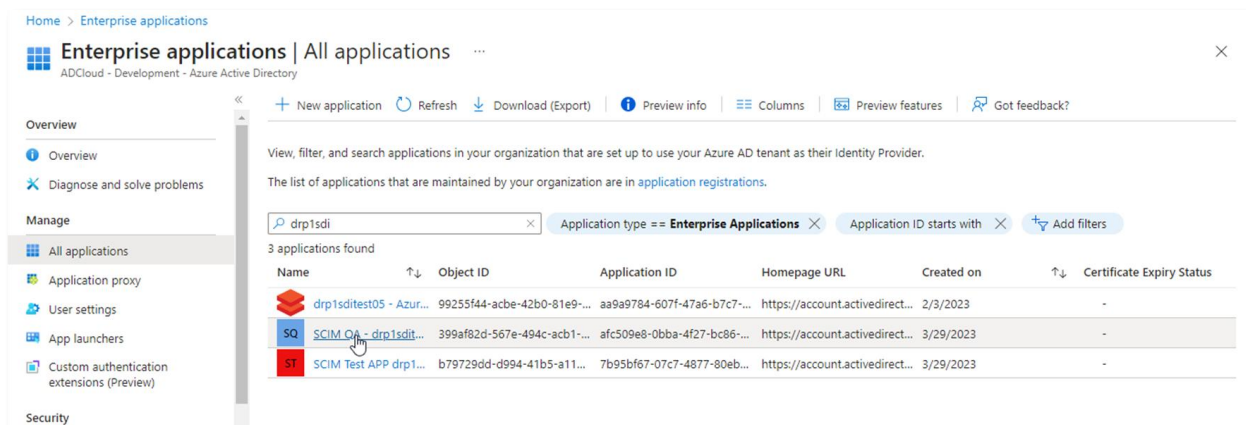
Notes:

- 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.

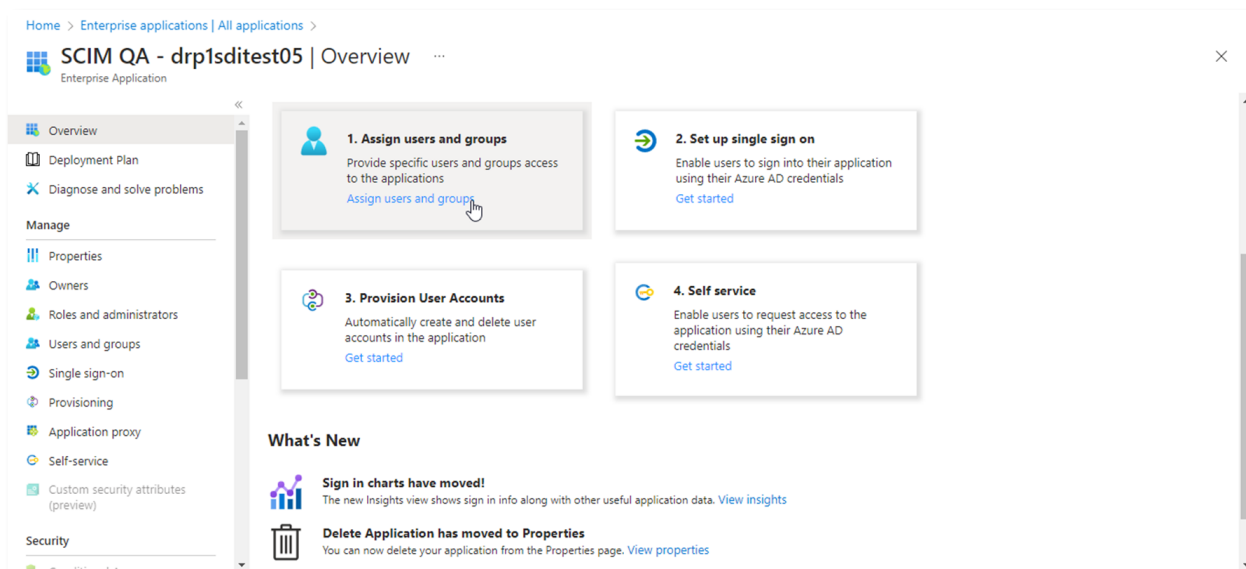
Assigning Users / Groups to an Application

Steps:

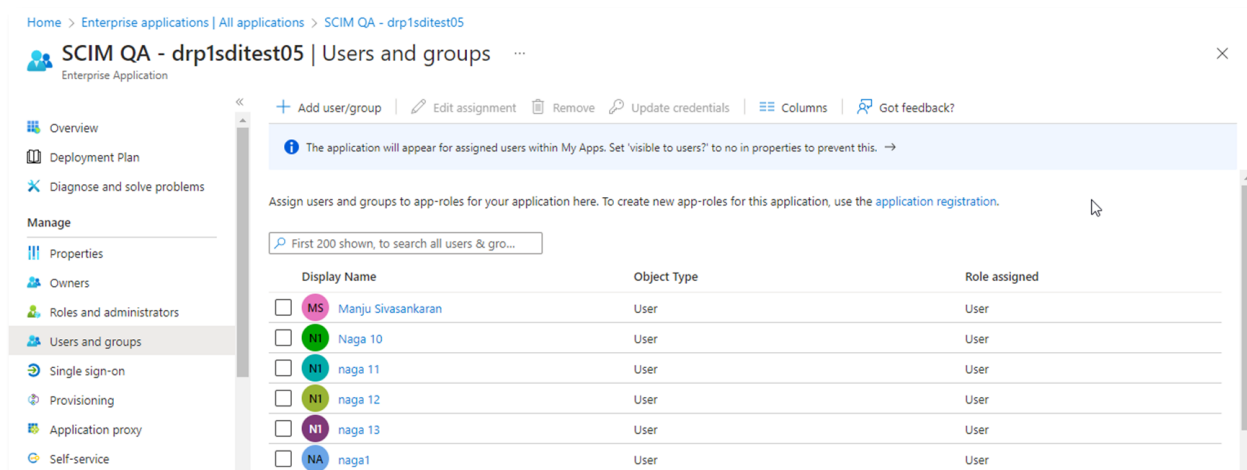
1. Log in to the **Microsoft Entra ID** application.
2. Navigate to the **Enterprise applications** page.
3. From the **All applications** page, click on the 'Microsoft Entra ID' app connected via Exterro.



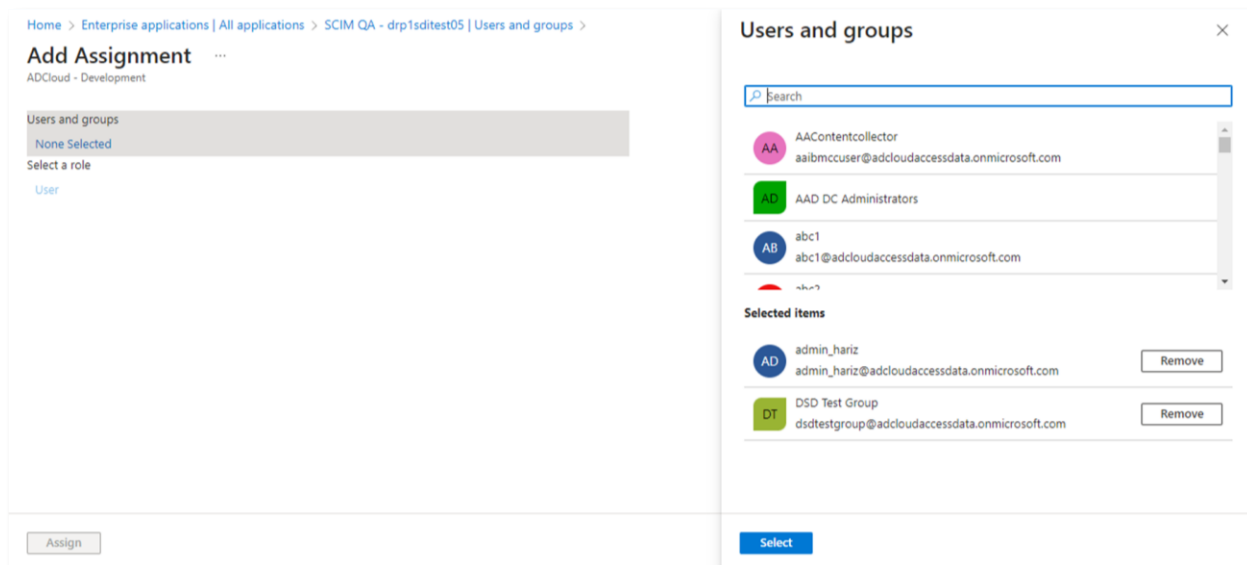
4. Select **Assign users and groups**.



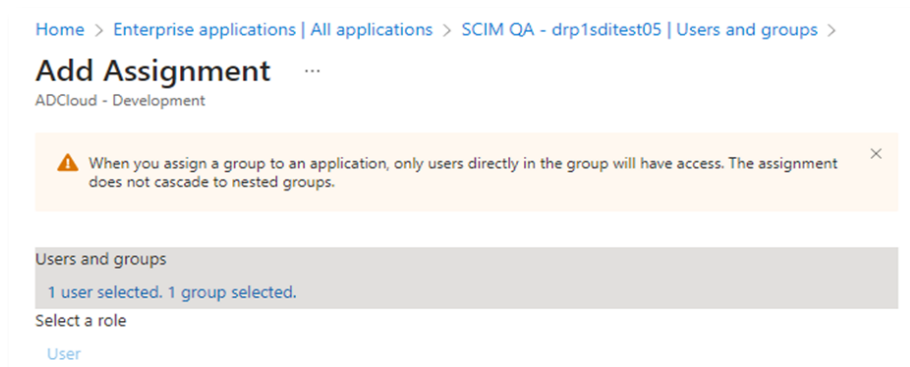
- From the **Users and groups** page, click **Add user/group**.



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



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

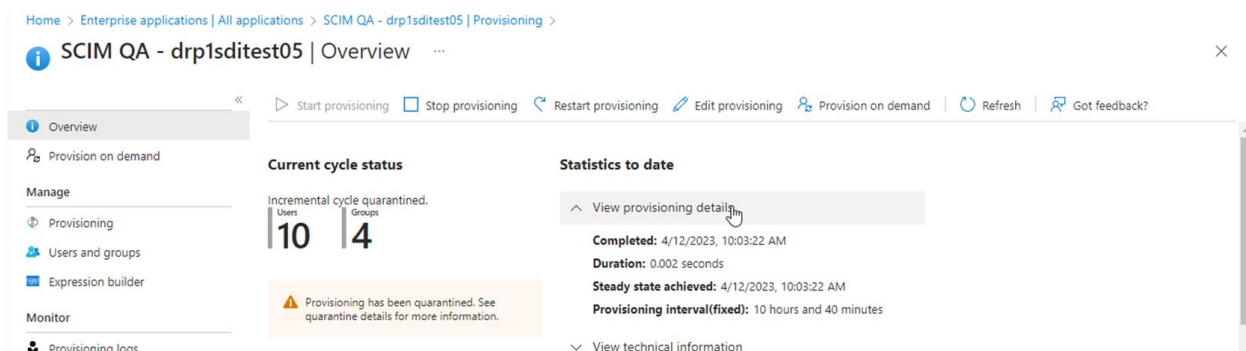


Note: The selected users and the assigned users and groups are listed under the 'Users and groups' page.

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:
- o Start
 - o Stop
 - o Restart
 - o Edit
 - o 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.

The screenshot displays the 'SCIM Configuration' window. At the top left, there is a status badge that reads 'SCIM token expired'. Below this, the 'SCIM Settings' section is visible. It includes several fields: 'Identity Provider' (a dropdown menu currently showing 'Azure'), 'Authentication Type' (a dropdown menu currently showing 'HTTP Header'), and 'SCIM Token Expiry in days' (a text input field containing the number '1'). To the right of these, there are two more fields: 'SCIM Connector Base URL' (a text input field containing a long URL) and 'Current Token Expires On' (a text input field showing 'Jun 22, 2026 07:54 AM'). Below the 'SCIM Token Expiry in days' field is a 'Select Recipients' dropdown menu. At the bottom right of the configuration area is a button labeled 'Send API Key'.

- **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

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Exterro, Inc. The trademarks, service marks, logos or other intellectual property rights of Exterro, Inc and others used in this documentation ("Trademarks") are the property of Exterro, Inc and their respective owners. The furnishing of this document does not give you license to these patents, trademarks, copyrights or other intellectual property except as expressly provided in any written agreement from Exterro, Inc.

The United States export control laws and regulations, including the Export Administration Regulations of the U.S. Department of Commerce, and other applicable laws and regulations apply to this documentation which prohibits the export or re-export of content, products, services, and technology to certain countries and persons. You agree to comply with all export laws, regulations and restrictions of the United States and any foreign agency or authority and assume sole responsibility for any such unauthorized exportation.

You may not use this documentation if you are a competitor of Exterro, Inc, except with Exterro Inc's prior written consent. In addition, you may not use the documentation for purposes of evaluating its functionality, or for any other competitive purposes.

If you have any questions, please contact Customer Support by email at support@exterro.com.