Instructions for SSO with Microsoft Entra ID via SAML 2.0 Set Up for LeapXpert Integration

Introduction: This document provides step-by-step instructions on how to set up Single-Sign-On in LeapXpert with a SAML 2.0 identity provider (IdP).

Note: Some of the parameters are just for informational purposes, the customer is expected to use the right parameters as provided in the design document.

Prerequisite: Must have Azure subscription and necessary permission to create a new application in Microsoft Entra ID.

Procedure

Step 1. LXP provides Service Provider Entity ID and Reply URL.

LeapXpert will provide the information for Entity ID and Reply URL.

Identifier (Entity ID)
https://web.hk.leapxloud.com/auth/realms/nortonrosefulbright
Reply URL
https://web.hk.leapxloud.com/auth/realms/nortonrosefulbright/broker/saml/endpoint

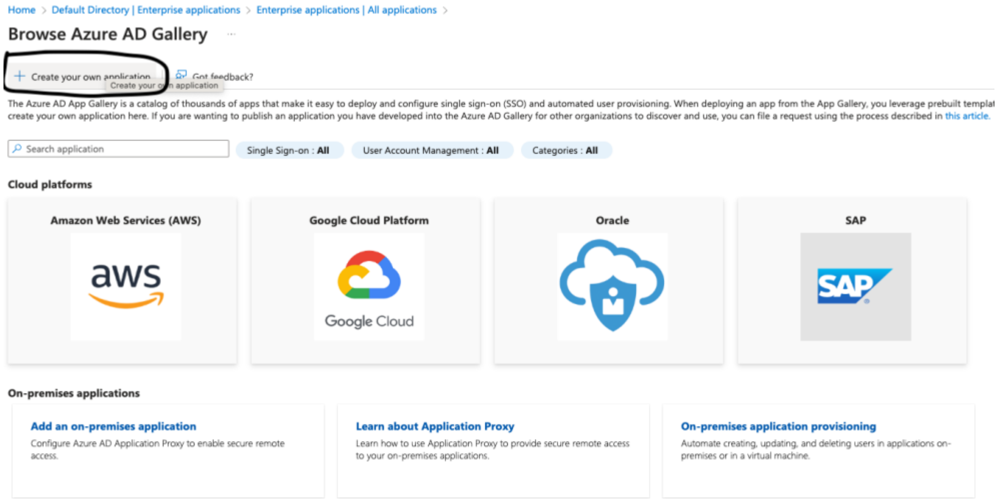
Step 2. Navigate to Azure Entra page.

On the Azure Entra page, Select "**Enterprise applications.**"

- Click on the New application button.

Step 3. On Browse Azure Entra Gallery page

a. Click on Create your own application.



Home > Default Directory | Enterprise applications > Enterprise applications | All applications >
Browse Azure AD Gallery
+ Create your own application
Create your own application
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
aws
Google Cloud Platform
Google Cloud
Oracle
SAP
SAP
On-premises applications
Add an on-premises application
Learn about Application Proxy
On-premises application provisioning

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templat create your own application here. If you are wanting to publish an application you have developed into the Azure AD Gallery for other organizations to discover and use, you can file a request using the process described in this article.

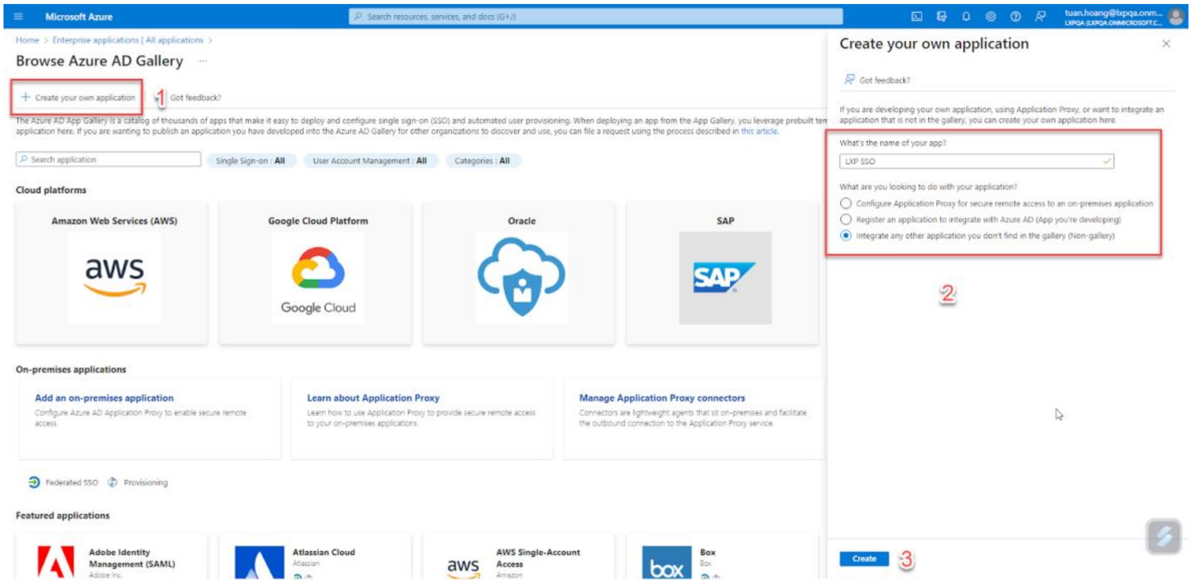
Configure Azure AD Application Proxy to enable secure remote access.

Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

Automate creating, updating, and deleting users in applications on-premises or in a virtual machine.

b. Input application name – recommended application name – LXP-<ENV>-SSO

c. Select the option “Integrate any other application you don't find in the gallery (non-gallery)”.
d. Click the “Create button”.


Microsoft Azure
Search resources, services, and docs (G+/)
tuan.hoang@lxpqa.onm...
LXPQA (LXPQA.ONMICROSOFT.C...
Home > Enterprise applications | All applications >
Browse Azure AD Gallery
+ Create your own application
1
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
Google Cloud Platform
Oracle
SAP
On-premises applications
Add an on-premises application
Learn about Application Proxy
Manage Application Proxy connectors
Federated SSO
Provisioning
Featured applications
Adobe Identity Management (SAML)
Adobe Inc.
Atlassian Cloud
Atlassian
AWS Single-Account Access
Amazon
Box
Box
Create your own application
Got feedback?
2
Create
3

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt tem application here. If you are wanting to publish an application you have developed into the Azure AD Gallery for other organizations to discover and use, you can file a request using the process described in this article.

Configure Azure AD Application Proxy to enable secure remote access.

Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

Connectors are lightweight agents that sit on-premises and facilitate the outbound connection to the Application Proxy service.

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

LXP SSO ✓

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application to integrate with Azure AD (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

Step 4. Enable Single Sign-on method SAML.

a. Open the created application.

b. Select Single sign-on in the left menu.

c. Select single sign-on method SAML.

Step 5. Set up Single Sign-On with SAML

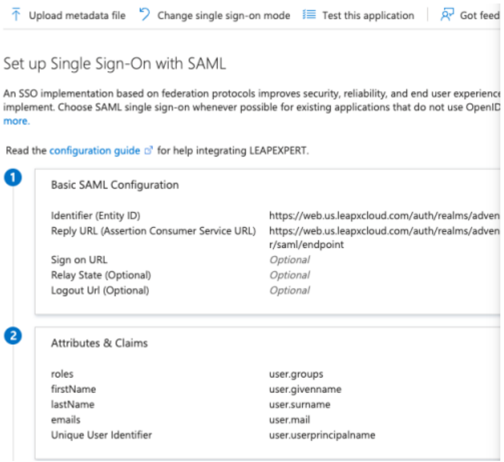
a. Edit the Basic SAML Configuration section.

b. Add identifier (Entity ID) links:

https://web.hk.leapxloud.com/auth/realms/nortonrosefulbright

c. Add Reply URL links:

https://web.hk.leapxloud.com/auth/realms/nortonrosefulbright/broker/saml/endpoint



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experienc
implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID
more.

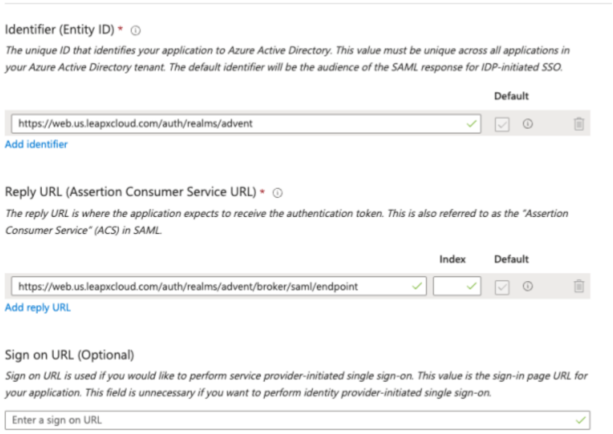
Read the configuration guide for help integrating LEAPEXPERT.

1 Basic SAML Configuration

Identifier (Entity ID)	https://web.us.leapxcloud.com/auth/realms/adven
Reply URL (Assertion Consumer Service URL)	https://web.us.leapxcloud.com/auth/realms/adven r/saml/endpoint
Sign on URL	*Optional*
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

2 Attributes & Claims

roles	user.groups
firstName	user.givenname
lastName	user.surname
emails	user.mail
Unique User Identifier	user.userprincipalname



Identifier (Entity ID) *

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://web.us.leapxcloud.com/auth/realms/advent ✓	☐

Add identifier

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://web.us.leapxcloud.com/auth/realms/advent/broker/saml/endpoint ✓	✓	☐

Add reply URL

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL ✓

d. Click Save

Note: **Service Provider Entity ID** and **Reply URL** are provided by LeapXpert in step 1.

Step 6. Create new groups in the Azure Entra – Take screenshots to send to LXP

Note: This step is only required if group claims mapping to LeapXpert roles is applicable.

The roles you see below are the Azure entra roles that will be mapped to respective LeapXpert equivalent roles with the Single Sign on. This mapping can be done by either LeapXpert or your company's LeapXpert platform admin once they have access to the Org admin Portal.

Recommended Groups:

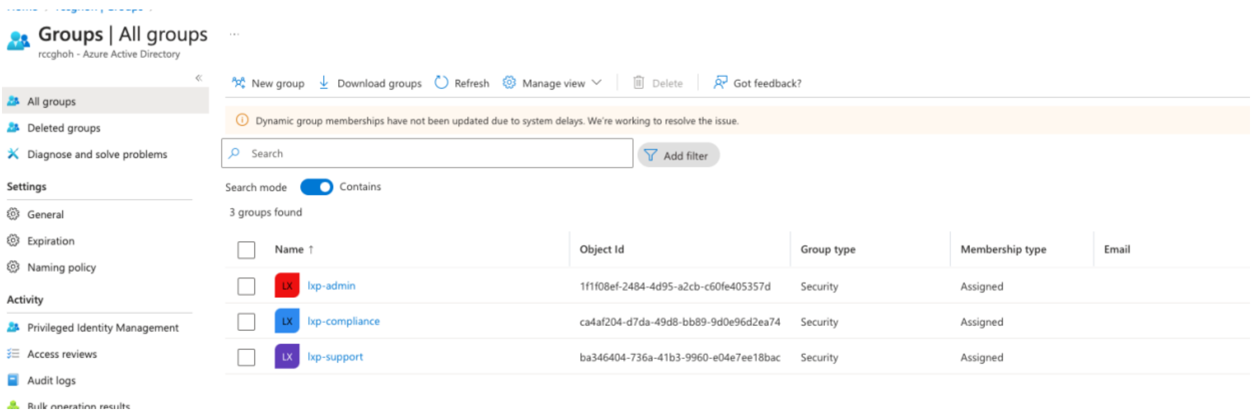
a. **lxp-admin**
   Permissions for the users within this group will be related to administrative tasks. This should be assigned to the Company's LeapXpert admin(s).

b. **lxp-compliance**
   Permissions for the users within this group will be related to management and compliance related tasks on the LeapXpert platform. This is subjective and changes from customer to customer depending on their scope and usage of the LeapXpert solution.

c. **lxp-support**

   Permissions for the users within this group will be related to support tasks, troubleshooting and operations specific.

   Note: Please refer to sample screenshots towards the end of this document & Roles and Permissions support portal link for better understanding of the permission model in the LeapXpert platform.



Dynamic group memberships have not been updated due to system delays. We're working to resolve the issue.

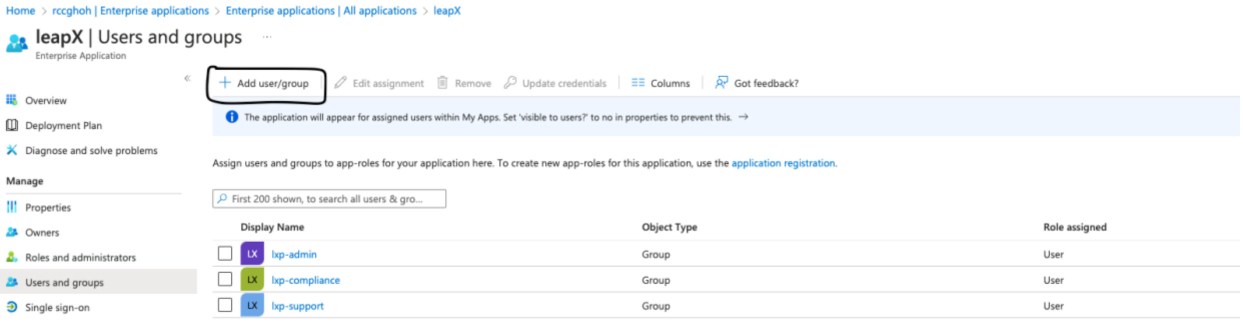
3 groups found

Name ↑	Object Id	Group type	Membership type	Email
LX lxp-admin	1f1f08ef-2484-4d95-a2cb-c60fe405357d	Security	Assigned	
LX lxp-compliance	ca4af204-d7da-49d8-bb89-9d0e96d2ea74	Security	Assigned	
LX lxp-support	ba346404-736a-41b3-9960-e04e7ee18bac	Security	Assigned	

Step 7. Add groups to Single Sign-on application.

Go to the homepage.

- Click Enterprise Application
- Select the created Single Sign-on application.
- Click Assign users and groups.
- Click Add user/group.
- Click None Selected under Groups
- Select the groups created for LeapXpert SSO setup.
- Click the Assign button.



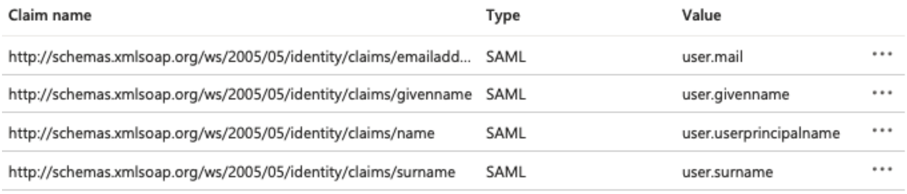
The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

Display Name	Object Type	Role assigned
LX lxp-admin	Group	User
LX lxp-compliance	Group	User
LX lxp-support	Group	User

Step 8. Edit Attributes and Claims- take screenshots to send to LXP

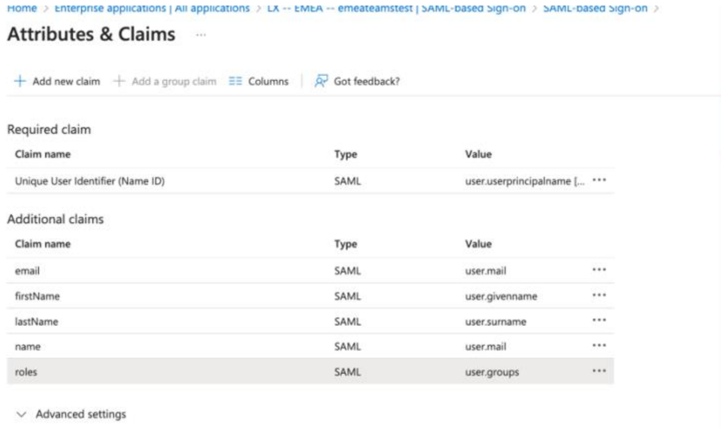
- Go back to the enterprise application on Azure Entra → select the application→ Single Sign on → Click on Edit the Attributes & Claims section. It should look like below:



Claim name	Type	Value	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail	···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname	···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname	···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname	···

- LeapXpert attributes in column 2 should be added to your Azure Entra exactly as shown below.

LeapXpert Profile	LeapXpert Attribute Name	Source Attributes	Description
User Name	userName	user.userprincipalname	Principal identifier of a federated user on the LeapXpert platform.
First Name	firstName	user.givenname	User’s first name
Last Name	lastName	user.surname	User’s last name
Email	emails	user.email	User’s unique email
Roles	roles	user.groups	Group claims to map to groups


Home > Enterprise applications | All applications > LX -- EMEA -- emeateamstest | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

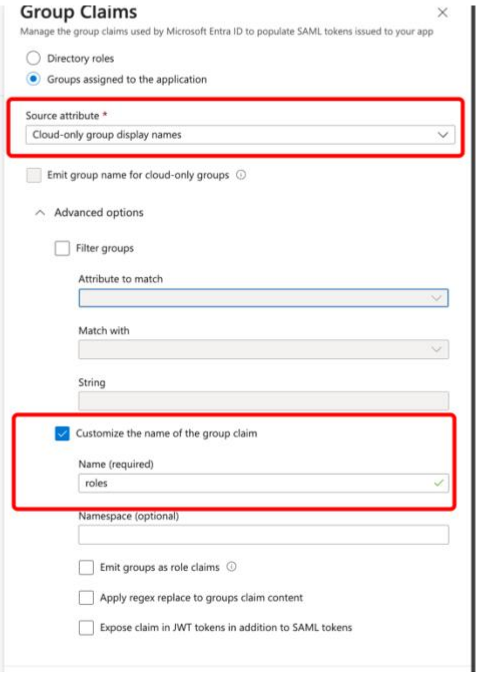
+ Add new claim
+ Add a group claim
Columns
Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...

Additional claims

Claim name	Type	Value
email	SAML	user.mail
firstName	SAML	user.givenname
lastName	SAML	user.surname
name	SAML	user.mail
roles	SAML	user.groups


Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

○ Directory roles
● Groups assigned to the application

Source attribute *: Cloud-only group display names

□ Emit group name for cloud-only groups

Advanced options

□ Filter groups

Attribute to match:

Match with:

String:

☑ Customize the name of the group claim

Name (required): roles

Namespace (optional):

□ Emit groups as role claims

□ Apply regex replace to groups claim content

□ Expose claim in JWT tokens in addition to SAML tokens

Note:

- If an email address is used for Unique User Identifier, our application will remove “@” from the email addresses in the username.
- Additional attributes can be added based on customer requirements.
- Download a copy of SAML federation metadata XML File & Certificate in Base64 Format.
- Take screenshots of the Step 6,7,8 pages.

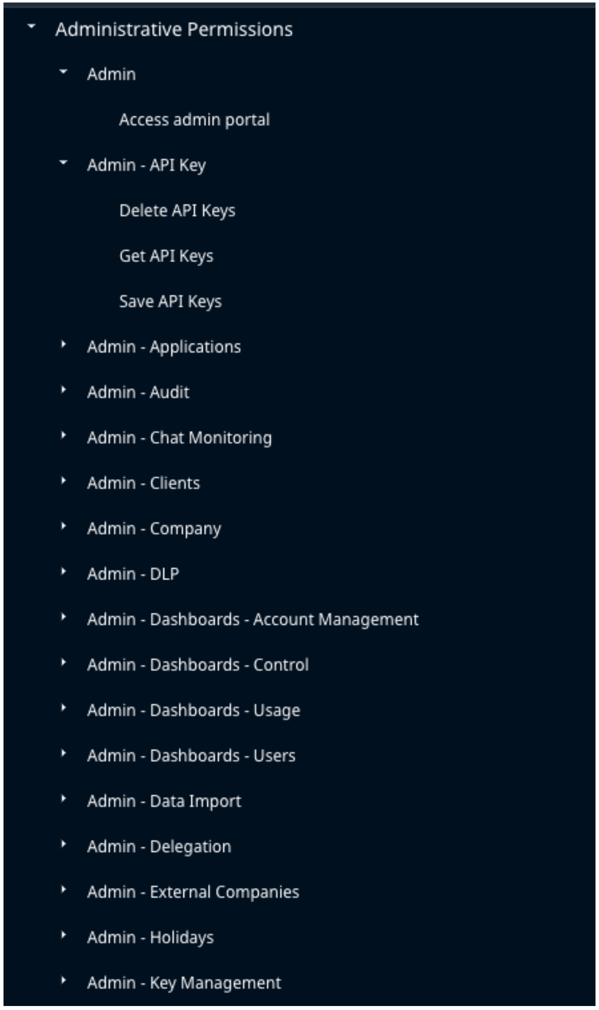
Step 9: Please email LeapXpert the following information:

1. Downloaded SAML federation metadata XML File & Certificate in Base64 Format
2. Screenshots of the Step 6,7,8 (Groups, Groups added to enterprise application & Final Attributes & Claims Page)

Step 10: Final Step - Logging In (Please wait for request)

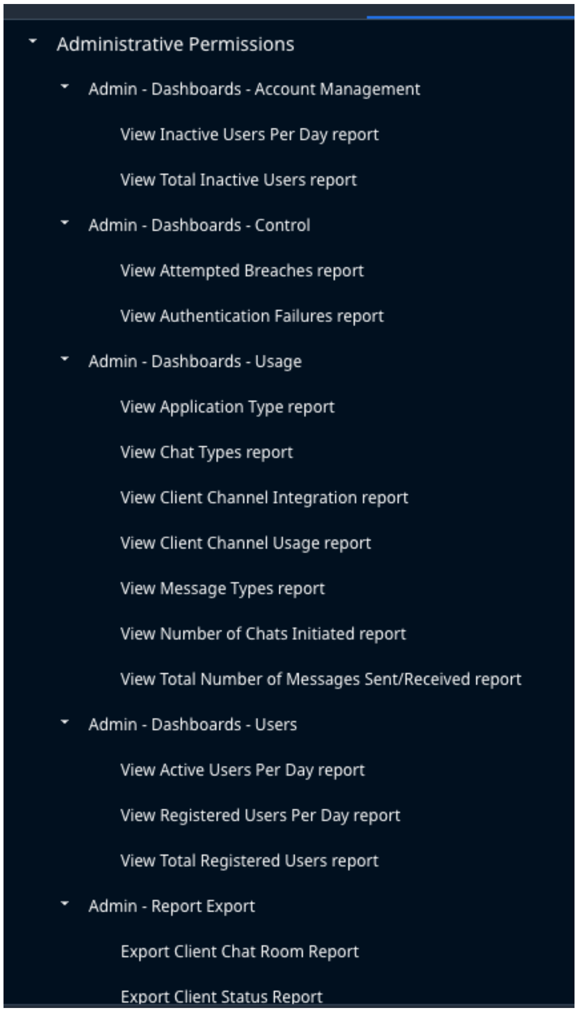
Once the above information in Step 9 is received, LXP will perform additional configuration on the LeapXpert platform to complete the SSO setup. We will then reach out and request you to login to test the SSO integration.

Admin role standard permissions sample

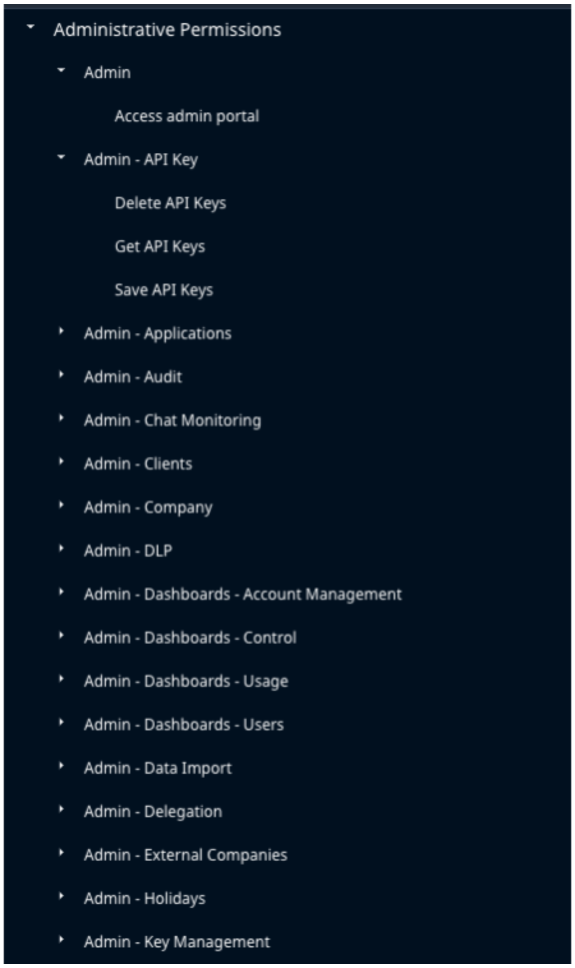


- Administrative Permissions
  - Admin
    - Access admin portal
  - Admin - API Key
    - Delete API Keys
    - Get API Keys
    - Save API Keys
  - Admin - Applications
  - Admin - Audit
  - Admin - Chat Monitoring
  - Admin - Clients
  - Admin - Company
  - Admin - DLP
  - Admin - Dashboards - Account Management
  - Admin - Dashboards - Control
  - Admin - Dashboards - Usage
  - Admin - Dashboards - Users
  - Admin - Data Import
  - Admin - Delegation
  - Admin - External Companies
  - Admin - Holidays
  - Admin - Key Management

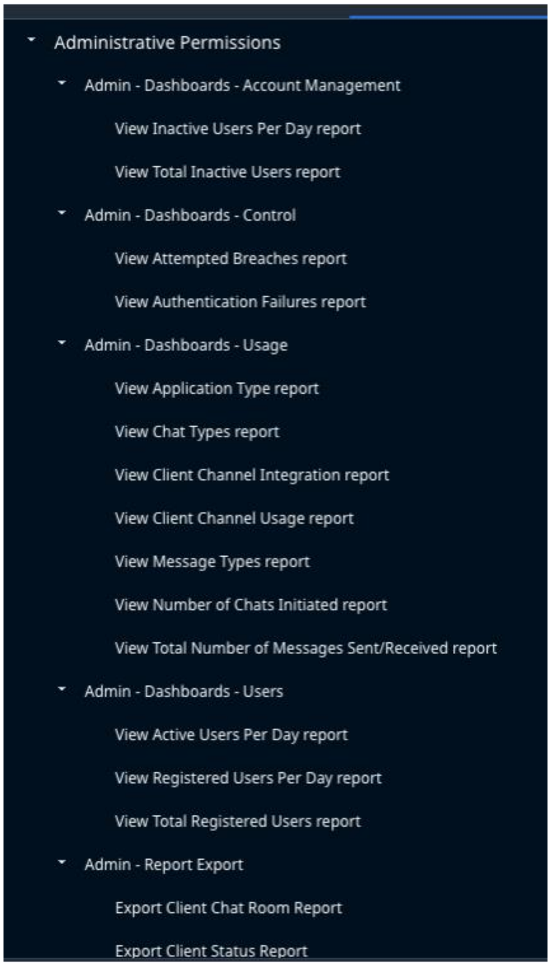
Compliance role – Standard Permissions sample



- Administrative Permissions
  - Admin - Dashboards - Account Management
    - View Inactive Users Per Day report
    - View Total Inactive Users report
  - Admin - Dashboards - Control
    - View Attempted Breaches report
    - View Authentication Failures report
  - Admin - Dashboards - Usage
    - View Application Type report
    - View Chat Types report
    - View Client Channel Integration report
    - View Client Channel Usage report
    - View Message Types report
    - View Number of Chats Initiated report
    - View Total Number of Messages Sent/Received report
  - Admin - Dashboards - Users
    - View Active Users Per Day report
    - View Registered Users Per Day report
    - View Total Registered Users report
  - Admin - Report Export
    - Export Client Chat Room Report
    - Export Client Status Report



- Administrative Permissions
  - Admin
    - Access admin portal
  - Admin - API Key
    - Delete API Keys
    - Get API Keys
    - Save API Keys
  - Admin - Applications
  - Admin - Audit
  - Admin - Chat Monitoring
  - Admin - Clients
  - Admin - Company
  - Admin - DLP
  - Admin - Dashboards - Account Management
  - Admin - Dashboards - Control
  - Admin - Dashboards - Usage
  - Admin - Dashboards - Users
  - Admin - Data Import
  - Admin - Delegation
  - Admin - External Companies
  - Admin - Holidays
  - Admin - Key Management



- Administrative Permissions
  - Admin - Dashboards - Account Management
    - View Inactive Users Per Day report
    - View Total Inactive Users report
  - Admin - Dashboards - Control
    - View Attempted Breaches report
    - View Authentication Failures report
  - Admin - Dashboards - Usage
    - View Application Type report
    - View Chat Types report
    - View Client Channel Integration report
    - View Client Channel Usage report
    - View Message Types report
    - View Number of Chats Initiated report
    - View Total Number of Messages Sent/Received report
  - Admin - Dashboards - Users
    - View Active Users Per Day report
    - View Registered Users Per Day report
    - View Total Registered Users report
  - Admin - Report Export
    - Export Client Chat Room Report
    - Export Client Status Report