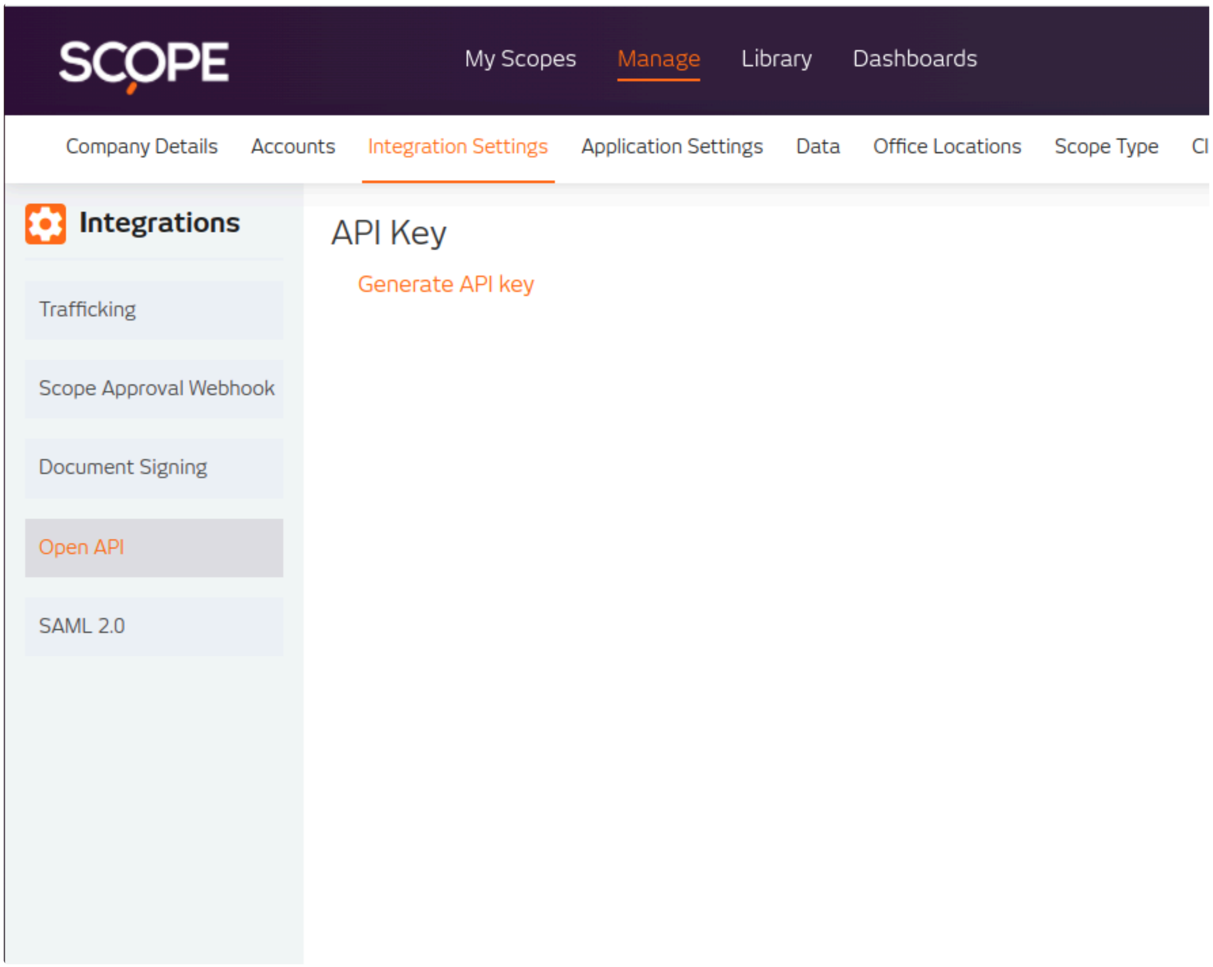
Azure SSO/SCIM Setup

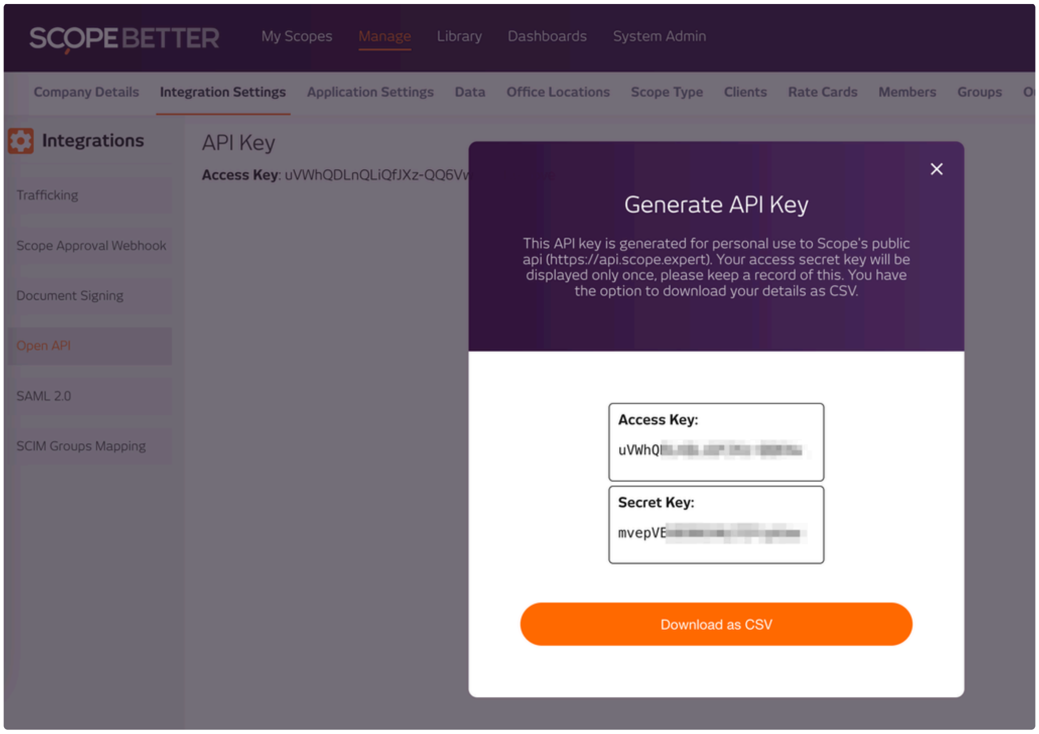
Requirements

To successfully integrate Azure SSO and SCIM with our application, ensure the following prerequisites are met:

1. **Active Directory**
   Your organization must use **Azure Active Directory** (Azure AD) for identity and access management. This will be used for Single Sign-On (SSO) and provisioning users via SCIM.
2. **Generate API Key**.

   How to Obtain OpenAPI Credentials:
   - Navigate to **Manage > Integration Settings > OpenAPI**.
   - Click on **Generate API Key**.
   - You will be shown the **username** and **password**.
   - **Important:** Copy the credentials and store them in a secure location, as they will be needed to configure SCIM in Azure AD.





API Key

Access Key: uVWhQDLnQLiQfJXz-QQ6Vv

Generate API Key

This API key is generated for personal use to Scope's public api (https://api.scope.expert). Your access secret key will be displayed only once, please keep a record of this. You have the option to download your details as CSV.

Access Key: uVWhQ[redacted]

Secret Key: mvepVE[redacted]

---

3. **How to Obtain OpenAPI Access Token:**

1. **Download Postman:** Download Postman | Get Started for Free

If you haven't already, download and install Postman from here.

2. **Create a New Request in Postman:**

Open Postman and create a new request.

Set the request method to **POST**.

In the request URL, enter the appropriate token endpoint (provided by our application).

3. **Add Authorization:**

In the Authorization tab, fill the username tab with this endpoint (scope-public-api_scim).

In the Body/ x-www-form-urlencoded fill the username and password with your credentials obtained from Scope Integration Settings:

Username: This is your Access Key.

Password: This is your Secret Key.

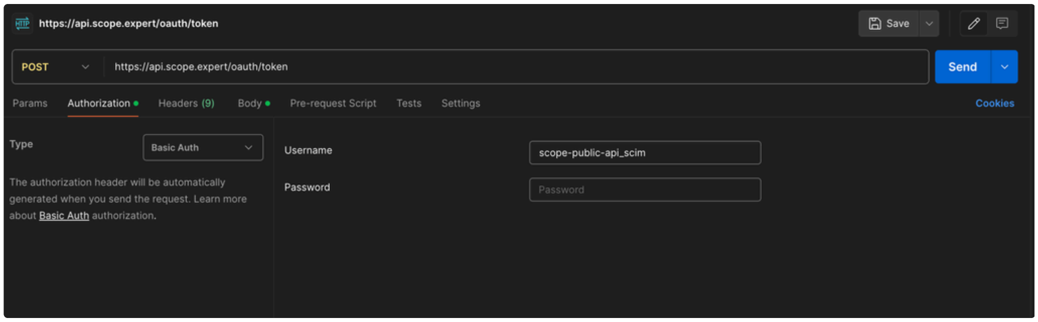
4. **Send the Request:**

Click Send to submit the request.

5. **Copy the Access Token:**

Once the request is successful, you will receive the access_token in the response. Copy the token and save it in a secure location.

ℹ Please use Production API url as your request's base url when making requests for your production instance https://api.scope.expert



https://api.scope.expert/oauth/token

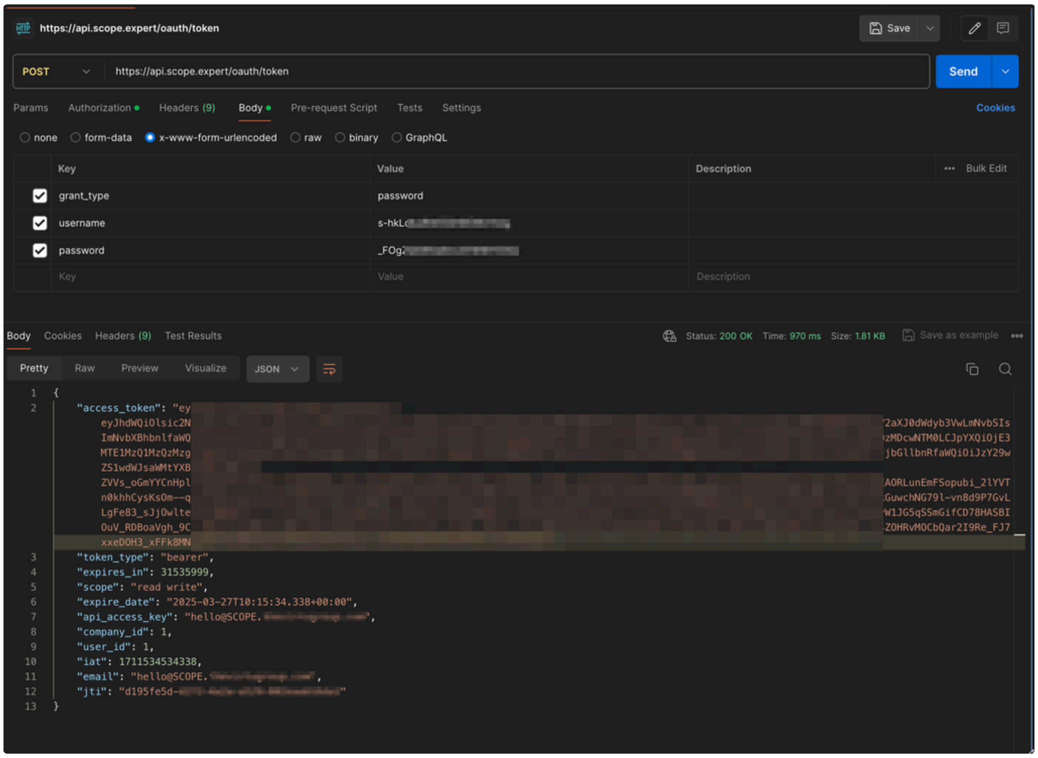
POST https://api.scope.expert/oauth/token

Type: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about Basic Auth authorization.

Username: scope-public-api_scim

Password: Password



https://api.scope.expert/oauth/token

POST https://api.scope.expert/oauth/token

○ none ○ form-data ● x-www-form-urlencoded ○ raw ○ binary ○ GraphQL

	Key	Value	Description
☑	grant_type	password	
☑	username	s-hkL[redacted]	
☑	password	_FOg[redacted]	
	Key	Value	Description

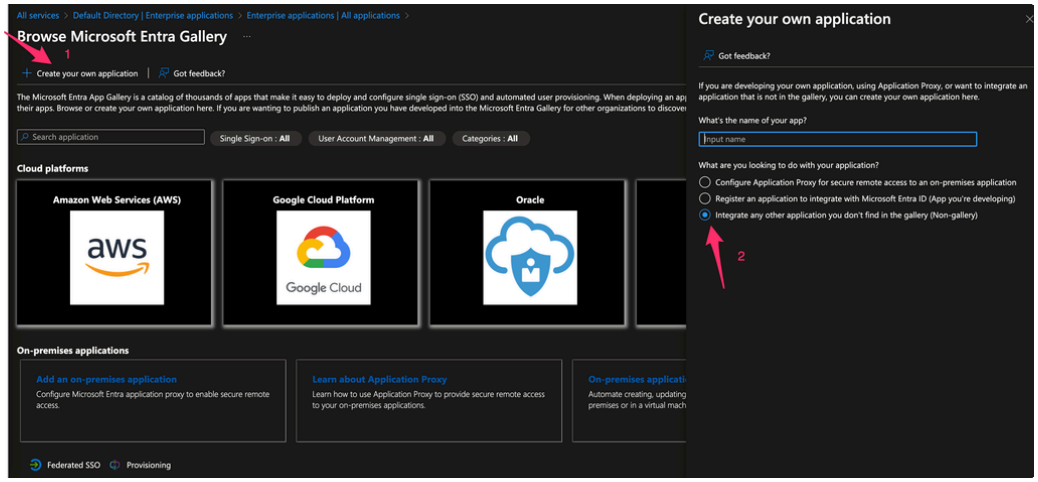
Status: 200 OK Time: 970 ms Size: 1.81 KB

```
{
    "access_token": "ey[redacted]
        eyJhdWQiOlsic2N[redacted]2aXJ0dWdyb3VwLmNvbSIs
        ImNvbXBhbnlfaWQ[redacted]zMDcwNTM0LCJpYXQiOjE3
        MTE1MzQ1MzQzMzg[redacted]jbGllbnRfaWQiOiJzY29w
        ZS1wdWJsaWMtYXB[redacted]
        ZVVs_oGmYYCnHpl[redacted]AORLunEmFSopubi_2lYVT
        n0khhCysKsOm--q[redacted]GuwchNG79l-vn8d9P7GvL
        LgFe83_sJjOwlte[redacted]W1JG5qSSmGifCD78HASBI
        OuV_RDBoaVgh_9C[redacted]ZOHRvMOCbQar2I9Re_FJ7
        xxeDOH3_xFFk8MN[redacted]
    "token_type": "bearer",
    "expires_in": 31535999,
    "scope": "read write",
    "expire_date": "2025-03-27T10:15:34.338+00:00",
    "api_access_key": "hello@SCOPE.[redacted]",
    "company_id": 1,
    "user_id": 1,
    "iat": 1711534534338,
    "email": "hello@SCOPE.[redacted]",
    "jti": "d195fe5d-[redacted]"
}
```

Configure SCIM app in Azure:

Before stating the setup you need to select a `userName` that is going to be inserted in Scope from Azure. Scope only supports email as username. Please make sure the correct username is being sent to Scope when provisioning and when login via SSO. Depends on your configuration you might need to map attributes in step 5.

1. In Your Active Directory Client on Enterprise applications tab.
2. Select “New application” > “Create your own application”. There you’ll be shown three options, select the last option “Non-gallery” app.


All services > Default Directory | Enterprise applications > Enterprise applications | All applications >
1
+ Create your own application
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All
Cloud platforms
Amazon Web Services (AWS)
Google Cloud Platform
Oracle
On-premises applications
Federated SSO
Provisioning
2

Browse Microsoft Entra Gallery

The Microsoft Entra 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 ap
their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discove

Add an on-premises application
Configure Microsoft Entra application proxy to enable secure remote access.

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

On-premises applicati
Automate creating, updating
premises or in a virtual mach

Create your own application

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.

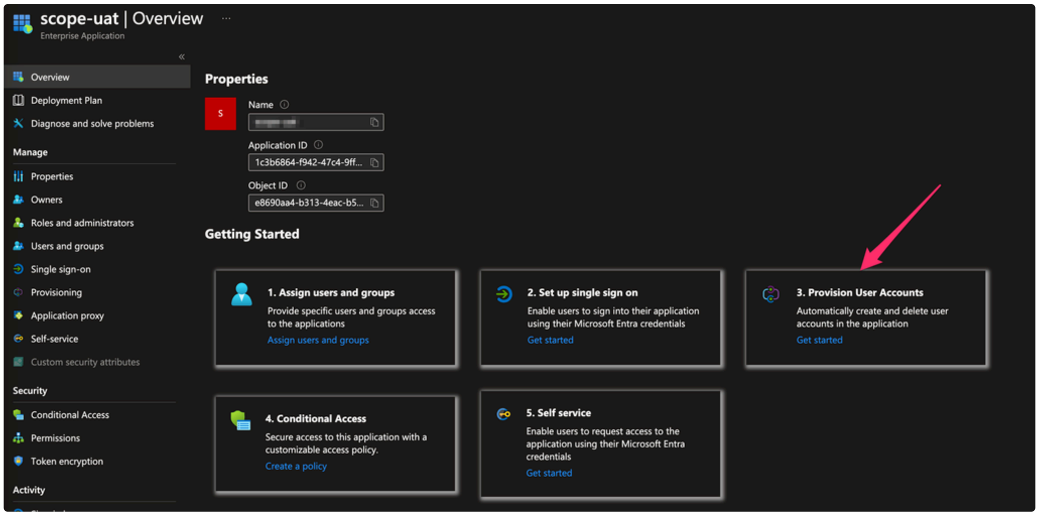
What's the name of your app?

Input name

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 Microsoft Entra ID (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

3. Once the app is created select “Provision User Accounts”.



scope-uat | Overview

Properties

Name [redacted]

Application ID 1c3b6864-f942-47c4-9ff...

Object ID e8690aa4-b313-4eac-b5...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
Get started

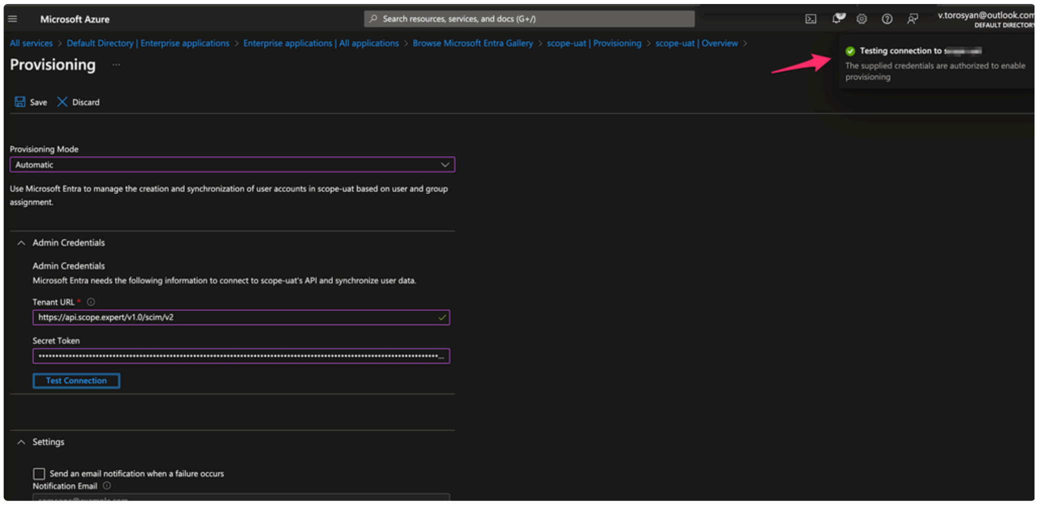
3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Microsoft Entra credentials
Get started

4. Enter appropriate values in given fields.

- Choose Provision Mode **Automatic**
- The value of the Tenant URL is **https://api.scope.expert/v1.0/scim/v2**
- The value of the Secret Token is `access_token` obtained from Scope OPEN API.
- Click Test Connection
- Click Save and wait until you get
- Once you save it, Azure will make a test request and confirm that the connection has been made.



Microsoft Azure
Search resources, services, and docs (G+/)
v.torosyan@outlook.com
DEFAULT DIRECTORY
All services > Default Directory | Enterprise applications > Enterprise applications | All applications > Browse Microsoft Entra Gallery > scope-uat | Provisioning > scope-uat | Overview >
Provisioning
Save
Discard

Testing connection to [redacted]

The supplied credentials are authorized to enable provisioning

Provisioning Mode: Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in scope-uat based on user and group assignment.

Admin Credentials

Admin Credentials

Microsoft Entra needs the following information to connect to scope-uat's API and synchronize user data.

Tenant URL *: https://api.scope.expert/v1.0/scim/v2

Secret Token: ••...

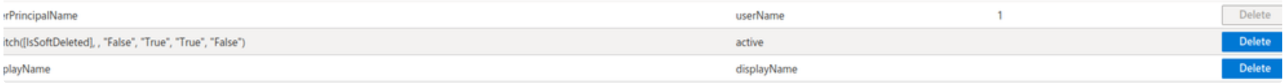
Settings

□ Send an email notification when a failure occurs

Notification Email: someone@example.com

5. After saving reload the form you will see toggle button at the end saying “Provisioning status”, toggle it to on and save it. The provision will start. The default interval is 40 mins.

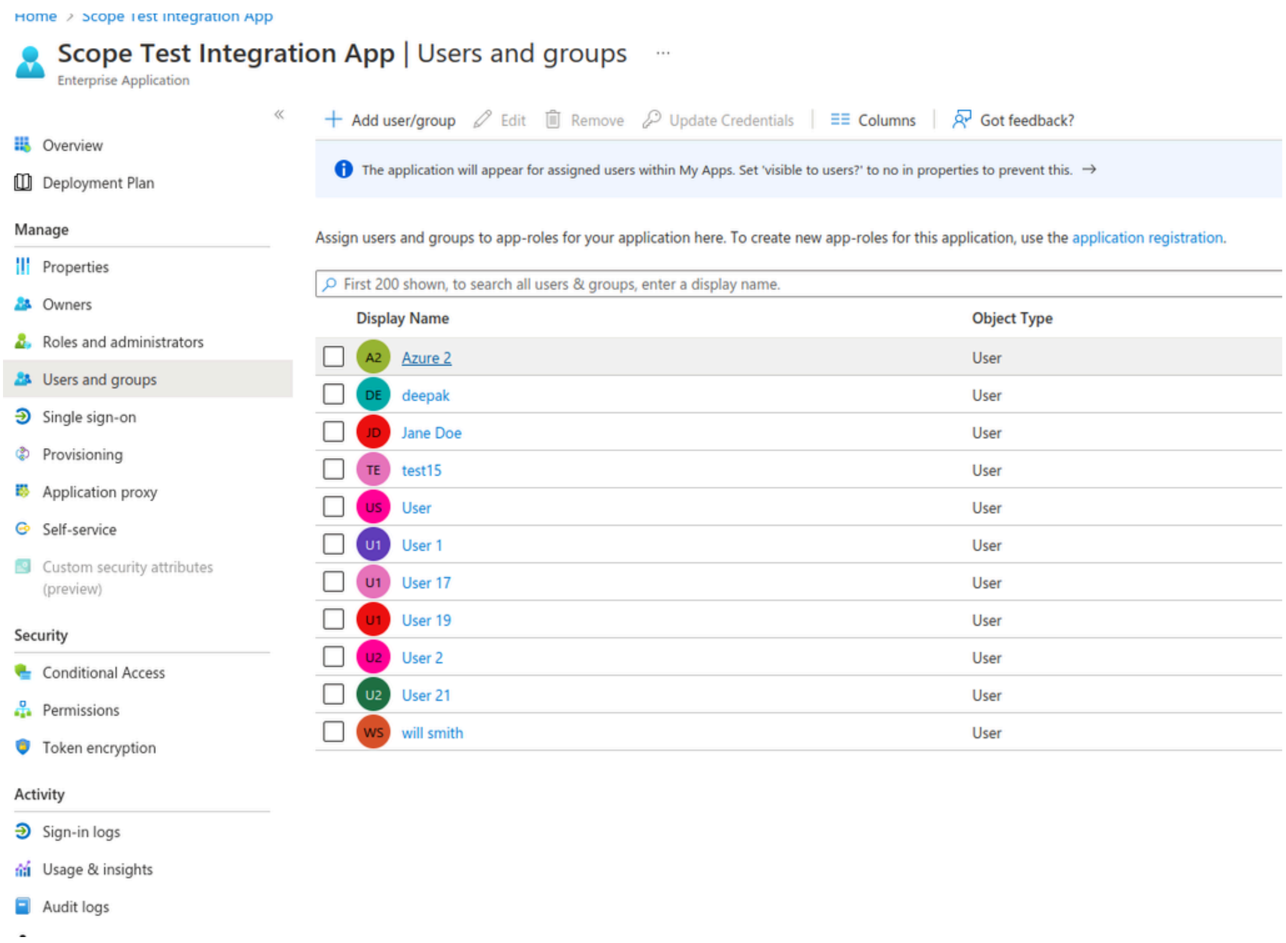
If you’re required to map email as attribute, you need to do that now by clicking, “Provision AZure Active Directory Users” link in Mappings and change following attribute.



rPrincipalName	userName	1	Delete
itch([IsSoftDeleted], , "False", "True", "True", "False")	active		Delete
playName	displayName		Delete

Note: The provisioning only happens when you assian a directory user the app you’ve created. It’s an straight forward process .

Active Director > Enterprise Applications > Your app



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.

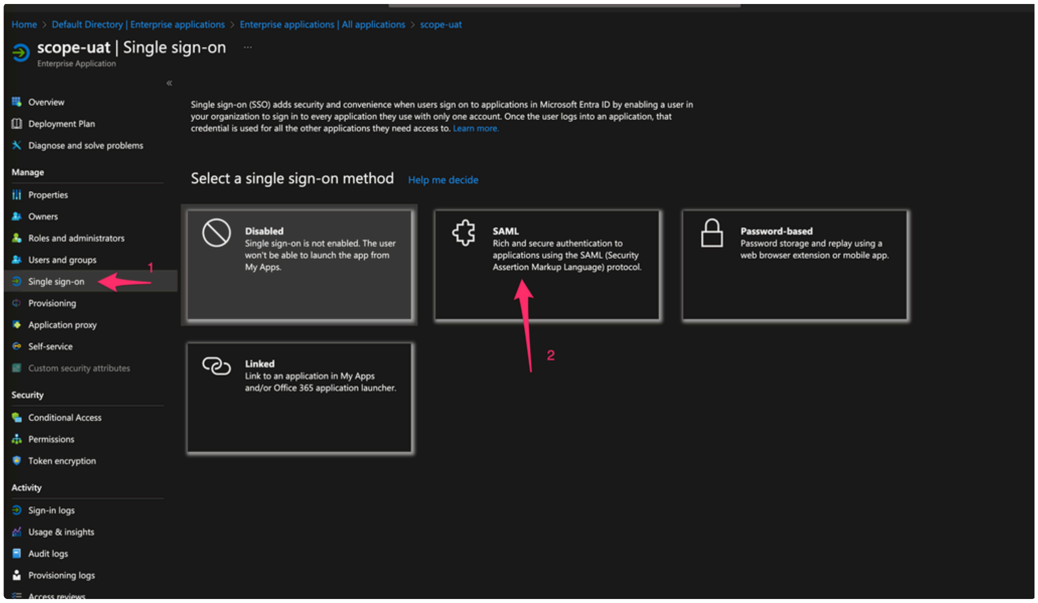
First 200 shown, to search all users & groups, enter a display name.

	Display Name	Object Type
□	A2 Azure 2	User
□	DE deepak	User
□	JD Jane Doe	User
□	TE test15	User
□	US User	User
□	U1 User 1	User
□	U1 User 17	User
□	U1 User 19	User
□	U2 User 2	User
□	U2 User 21	User
□	WS will smith	User

You'll be shown this screen. Select new users from "+Add user/group"

The next step is to configure SSO login in Scope.

1. On Azure Navigate your Enterprise Application and select Single sign-on and choose SAML.



Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

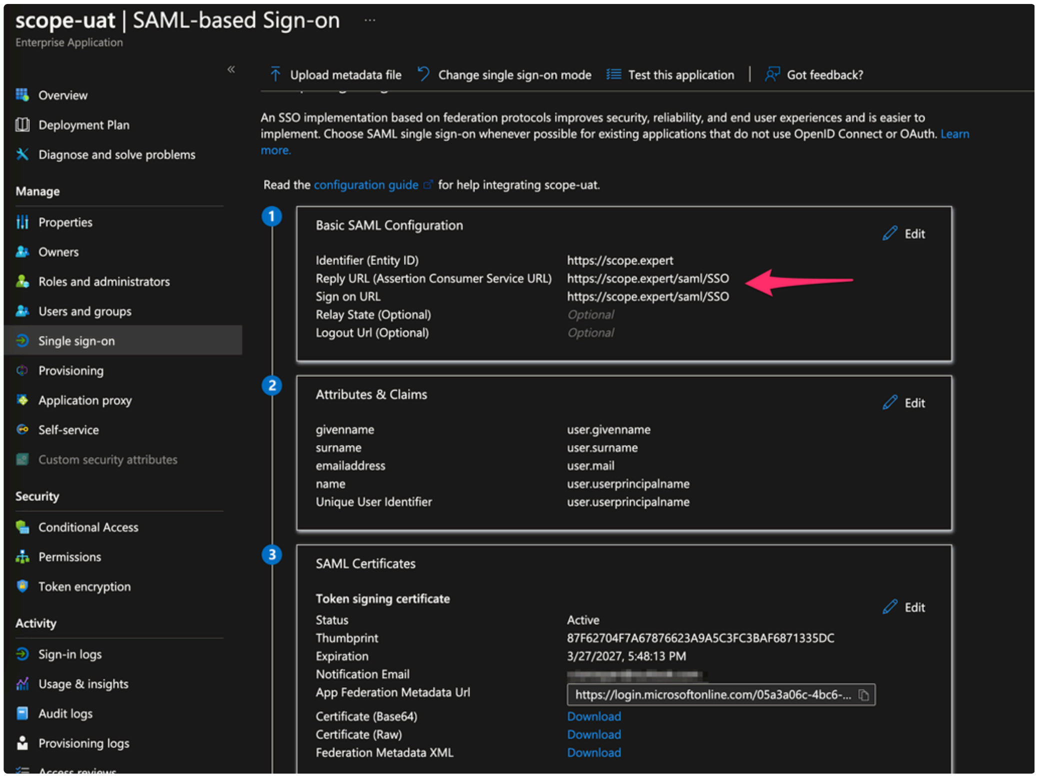
Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

2. Enter appropriate values in given fields.
   Identifier (Entity ID) - **https://scope.expert**

   Reply URL (Assertion Consumer Service URL) - **https://scope.expert/saml/SSO**

   Sign on URL - **https://scope.expert/saml/SSO**



An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating scope-uat.

1 Basic SAML Configuration

Identifier (Entity ID)	https://scope.expert
Reply URL (Assertion Consumer Service URL)	https://scope.expert/saml/SSO
Sign on URL	https://scope.expert/saml/SSO
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

2 Attributes & Claims

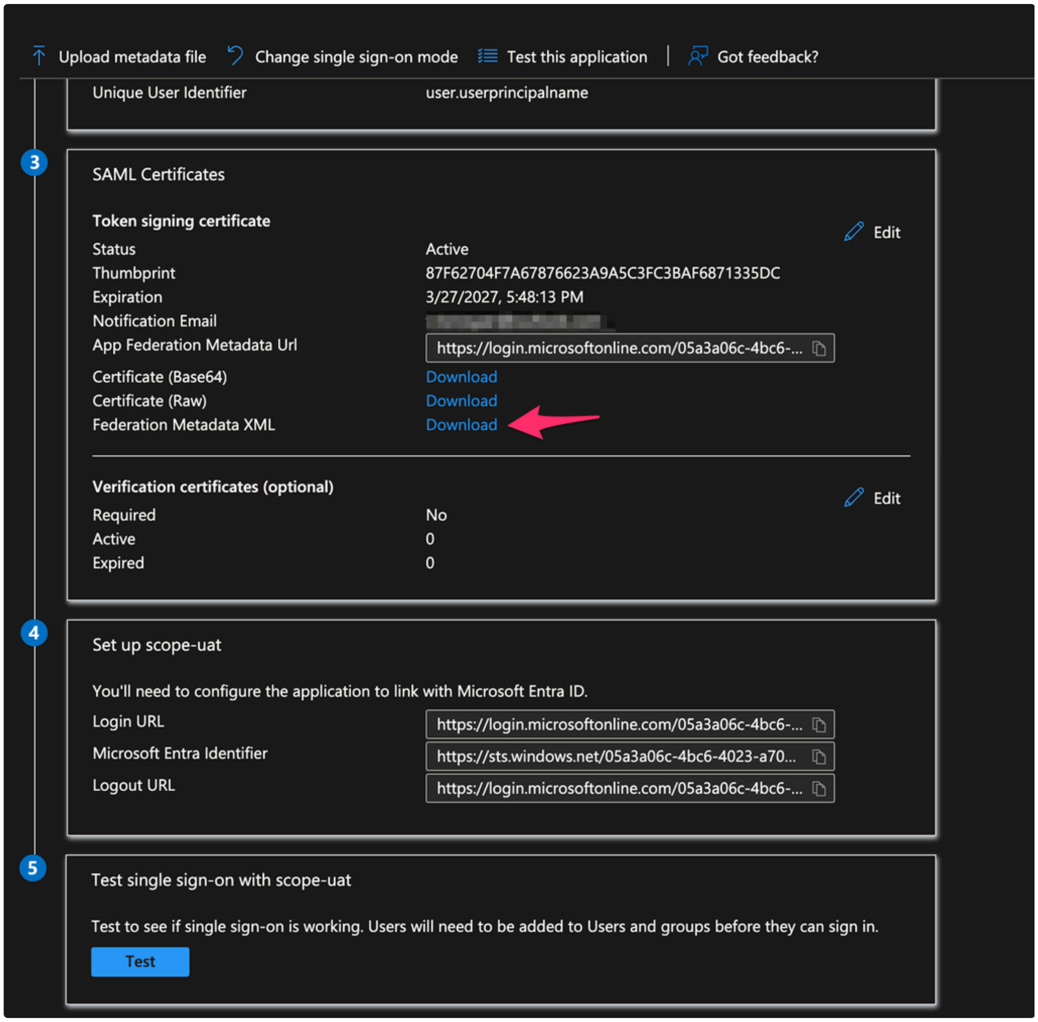
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate

Status	Active
Thumbprint	87F62704F7A67876623A9A5C3FC3BAF6871335DC
Expiration	3/27/2027, 5:48:13 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/05a3a06c-4bc6-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

3. Download Federation Metadata XML



Unique User Identifier	user.userprincipalname

3

SAML Certificates

Token signing certificate

Status	Active
Thumbprint	87F62704F7A67876623A9A5C3FC3BAF6871335DC
Expiration	3/27/2027, 5:48:13 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/05a3a06c-4bc6-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0
Expired	0

4

Set up scope-uat

You'll need to configure the application to link with Microsoft Entra ID.

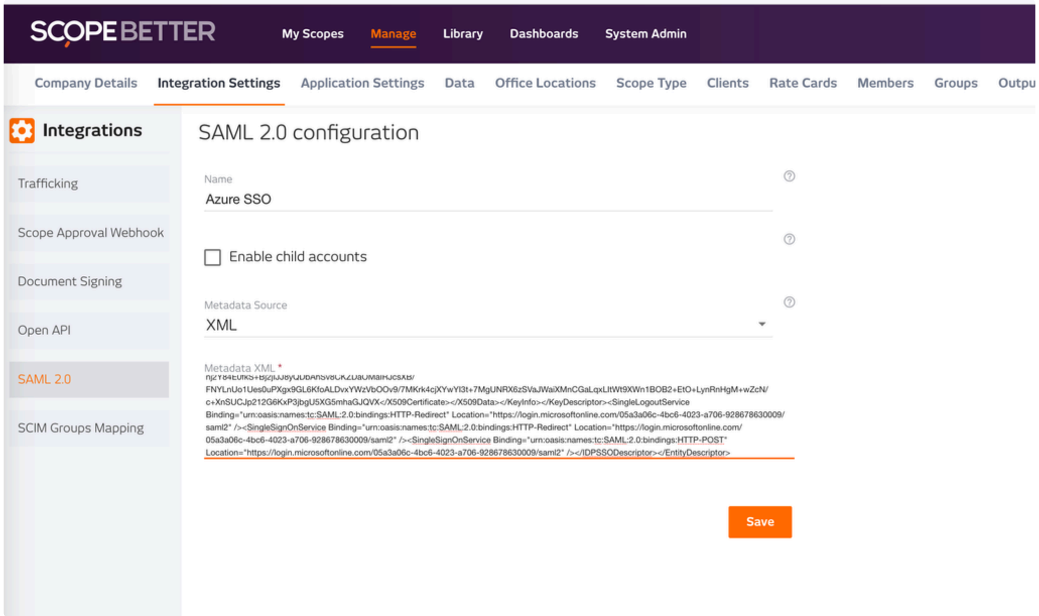
Login URL	https://login.microsoftonline.com/05a3a06c-4bc6-...
Microsoft Entra Identifier	https://sts.windows.net/05a3a06c-4bc6-4023-a70...
Logout URL	https://login.microsoftonline.com/05a3a06c-4bc6-...

5

Test single sign-on with scope-uat

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

4. Navigate Scope web app. Open Page “Integration Settings” → “SAML 2.0“.
   Type any name for SAML configuration.
   Metadata Source - choose XML
   Paste your XML content into the Metadata XML field and Save



SAML 2.0 configuration

Name
Azure SSO

□ Enable child accounts

Metadata Source
XML

Metadata XML *

```
nj2Y84EUfkS+Bj2jIJJ8yQDbAnSv8CKZDaUMalHJcsXB/
FNYLnUo1Ues0uPXgx9GL6KfoALDvxYWzVbOOv9/7MKrk4cjXYwYl3t+7MgUNRX6zSVaJWaiXMnCGaLqxLltWt9XWn1BOB2+EtO+LynRnHgM+wZcN/
c+XnSUCJp212G6KxP3jbgU5XG5mhaGJQVX</X509Certificate></X509Data></KeyInfo></KeyDescriptor><SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://login.microsoftonline.com/05a3a06c-4bc6-4023-a706-928678630009/
saml2" /><SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://login.microsoftonline.com/
05a3a06c-4bc6-4023-a706-928678630009/saml2" /><SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://login.microsoftonline.com/05a3a06c-4bc6-4023-a706-928678630009/saml2" /></IDPSSODescriptor></EntityDescriptor>
```

Known Limitations:

1. Only “Member” level of users can be created. Support for “Groups” and “Roles” are planned for future releases. If required once the user is created in Scope, an Scope Admin can elevate permissions from Scope Directly.

Optional

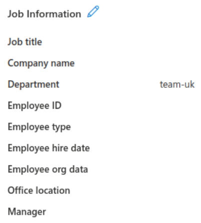
Setup Azure/OneLogin for Instance Selection

The SCIM implementation has been extended with a new feature that allows you to:

- Select any **child instance** directly from **Azure** or **OneLogin**.
- Assign users to these instances without additional configurations.

This enhancement streamlines the process of managing user assignments across multiple child instances directly from your identity provider.

This feature works with the value of “Department” field, available in both OneLogin and Azure and given in the screenshots below:



Job Information

Job title	
Company name	
Department	team-uk
Employee ID	
Employee type	
Employee hire date	
Employee org data	
Office location	
Manager	

Values:

The API is going to accept subdomain of instance in Department field. For an example if your child instance URL looks like this:

https://uk-team-demo.scope.expert

The acceptable value for Department field would be `uk-team-demo`. If no value is specified the user will go to parent instance.

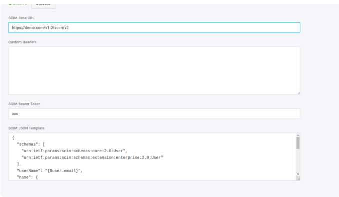
Setup:

OneLogin:

We need to update the SCIM schema to enable this feature and add 2 elements as given below.

```
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User" <--- Added
  ],
  "userName": "{$user.email}",
  "name": {
    "givenName": "{$user.firstname}",
    "familyName": "{$user.lastname}"
  },
  "emails": [
    {
      "value": "{$user.email}",
      "primary": true,
      "type": "work"
    }
  ],
"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User": { <--- Added
        "department": "{$user.department}"
    }
}
```

This config is available in Applications > Selected App > Configurations > SCIM Json Template



SCIM Base URL: https://demo.com/v1.0/scim/v2

Custom Headers:

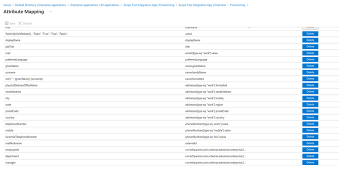
SCIM Bearer Token: xxx

SCIM JSON Template

```
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User",
    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"
  ],
  "userName": "{$user.email}",
  "name": {
```

Azure:

Azure takes care of schema, we just need to make sure the mapping is available here:

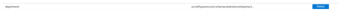


Home > Default Directory | Enterprise applications > Enterprise applications | All applications > Scope Test Integration App | Provisioning > Scope Test Integration App | Overview > Provisioning >

Attribute Mapping

mail	userName	Delete
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active	Delete
displayName	displayName	Delete
jobTitle	title	Delete
mail	emails[type eq "work"].value	Delete
preferredLanguage	preferredLanguage	Delete
givenName	name.givenName	Delete
surname	name.familyName	Delete
Join(" ", [givenName], [surname])	name.formatted	Delete
physicalDeliveryOfficeName	addresses[type eq "work"].formatted	Delete
streetAddress	addresses[type eq "work"].streetAddress	Delete
city	addresses[type eq "work"].locality	Delete
state	addresses[type eq "work"].region	Delete
postalCode	addresses[type eq "work"].postalCode	Delete
country	addresses[type eq "work"].country	Delete
telephoneNumber	phoneNumbers[type eq "work"].value	Delete
mobile	phoneNumbers[type eq "mobile"].value	Delete
facsimileTelephoneNumber	phoneNumbers[type eq "fax"].value	Delete
mailNickname	externalId	Delete
employeeId	urn:ietf:params:scim:schemas:extension:enterprise:2...	Delete
department	urn:ietf:params:scim:schemas:extension:enterprise:2...	Delete
manager	urn:ietf:params:scim:schemas:extension:enterprise:2...	Delete

This field should be available.



department	urn:ietf:params:scim:schemas:extension:enterprise:2...	Delete