



# Microsoft Entra ID SSO & SCIM Guide

Getting Started . . . . .	1
Accessing your user-based license . . . . .	1
Preparing SnapGene . . . . .	1
Microsoft Entra ID Configuration . . . . .	1
Creating an Application in Microsoft Entra ID . . . . .	2
Single sign-on (SSO) Configuration . . . . .	3
SCIM Identity Management Configuration . . . . .	9
Revoke User . . . . .	12

## Getting Started

### Accessing your user-based license

You can find your new SSO/SCIM User Licensing subscription in My Account:

- Navigate to [www.snapgene.com/account](http://www.snapgene.com/account)
- Log in with your existing credentials
- From the header drop down, select your user based subscription

### Preparing SnapGene

In order to follow the below steps to enable your SSO/SCIM configuration, you will need to be using at least version 8.0 (or 8.1 for Ubuntu) of SnapGene, and have deactivated your existing SnapGene activation.

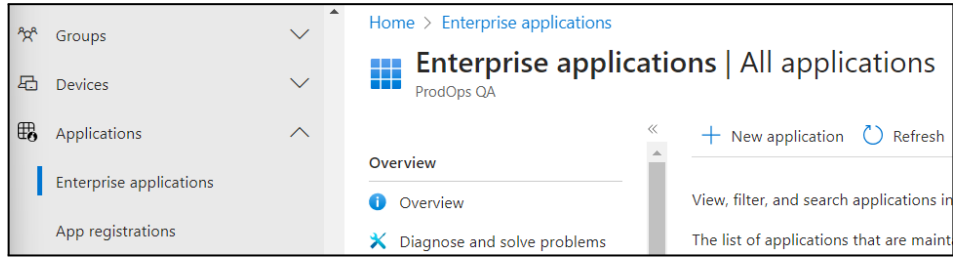
- To download the latest version, visit our [Updates](#) page, or update via the in-app updates feature
- Deactivate your current license by following **Help -> Manage License...**
- Let the SnapGene team know if your deactivation limit needs to be extended
- After deactivation, SnapGene should display the activation screen, or reopen in Viewer mode.  
You are now ready to apply your SSO and/or SCIM configuration following the steps below.

### Microsoft Entra ID Configuration

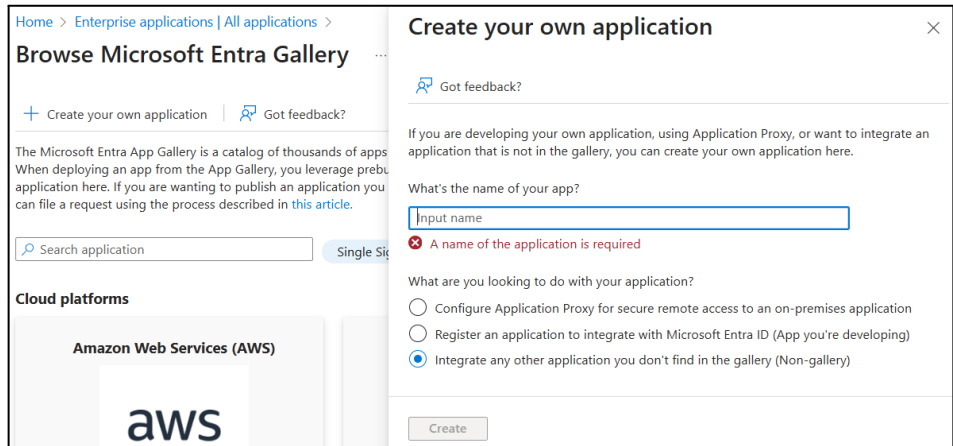
To use Microsoft Entra ID as your vendor, please follow the steps below to configure your application. The first two sections detail instructions for setting up SnapGene as an SSO application in Entra ID, while the third configures SCIM for identity management.

## Creating an Application in Microsoft Entra ID

1. From the **Applications** side menu, select **Enterprise applications**. From here, select **New application**:

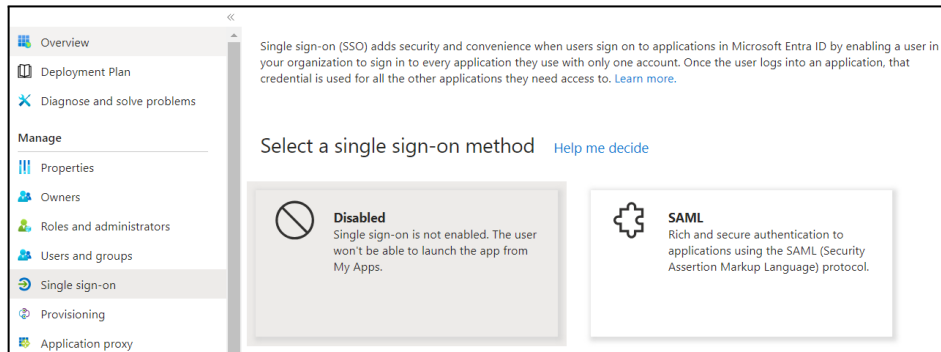


2. Select **Create your own application**. Enter your application name e.g. "SnapGene", select the **Non-gallery** application option, and click **Create**:

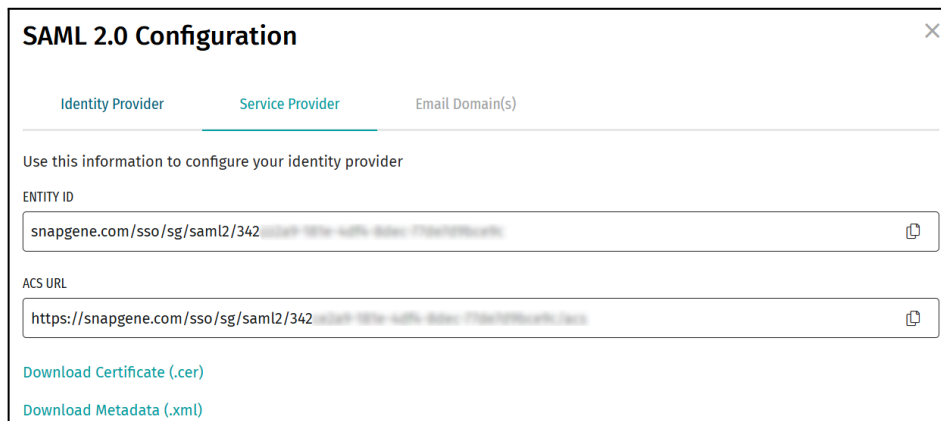


## Single sign-on (SSO) Configuration

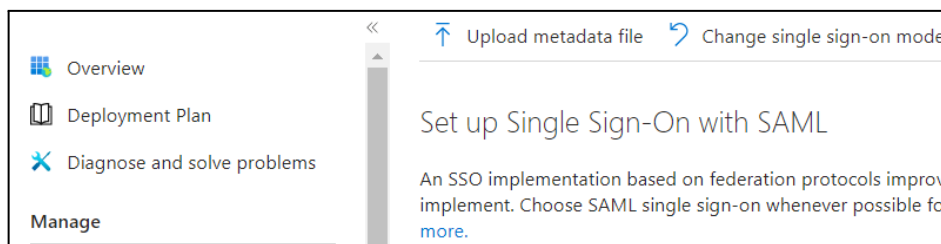
Once created, follow the **Manage -> Single sign-on** menu, then select **SAML** as your single sign-on method. Before continuing here, you will need to configure SnapGene's [My Account](#), and use information from here to configure Entra ID.



1. From My Account, select **Manage Seats**, then **Authentication**
2. Add a **SAML2 ID Provider**
3. Switch to the **Service Provider** tab and download the **Metadata** XML file. If the file opens in your browser rather than downloading, copy the XML data to a new file and save this as "metadata.xml"



4. Returning to Entra ID, select **Upload metadata file** and provide the above file. This will load the Entity ID and ACS URL seen in the above screenshot of My Account. Click Save:



## Basic SAML Configuration

Save | Got feedback?

**Identifier (Entity ID) \*** ⓘ

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

isapi.   ⓘ

[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.

https://isapi.   ⓘ

[Add reply URL](#)

5. Edit the **(2) Attributes & Claims** section. Verify that the claims are configured as below and update as necessary.

**Note:** the Identifier Claim must use the email address. This can be done by either specifying a Value of "user.mail", or as per below if email is your default identifier.

It is necessary that the email address used is consistent with the unique identifier. If aliasing between the email address and another identifier, please update the identifier claim here as necessary to use the email address of the invited user:

Required claim			
Claim name	Type	Value	
Unique User Identifier (Name ID)	SAML	user.userprincipalname [nameid-format:emailAddress]	***

Additional claims			
Claim name	Type	Value	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	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	***

6. Edit the **(3) SAML Certificates** section to use **Sign SAML response and assertion** as the **Signing Option**. Click **Save**:

**3** SAML Certificates

Token signing certificate Edit

Status: Active

Thumbprint: 2C960AB3F4DCD2FBB705E78097B487DB5CFF41FE

Expiration: 5/20/2027, 3:04:16 PM

Notification Email: demo@prodopsqa.onmicrosoft.com

App Federation Metadata Url: <https://login.microsoftonline.com/995bdd11-9512...>

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

### SAML Signing Certificate

Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

Save + New Certificate ↑ Import Certificate | Got feedback?

Status	Expiration Date	Thumbprint
Active	5/20/2027, 3:04:16 PM	2C960AB3F4DCD2FBB705E78097B487DB5CFF41FE

Signing Option: Sign SAML response and assertion

Signing Algorithm: SHA-256

- From the same **(3) SAML Certificates** section shown above, copy the **App Federation Metadata URL**
- Return to My Account and switch to the **Identity Provider** tab. Enter a name e.g. "Entra ID", and paste in the Metadata URL from Entra ID. Click **Save**:

### SAML 2.0 Configuration

Identity Provider    Service Provider    Email Domain(s)

NAME \*  STATUS: Enabled

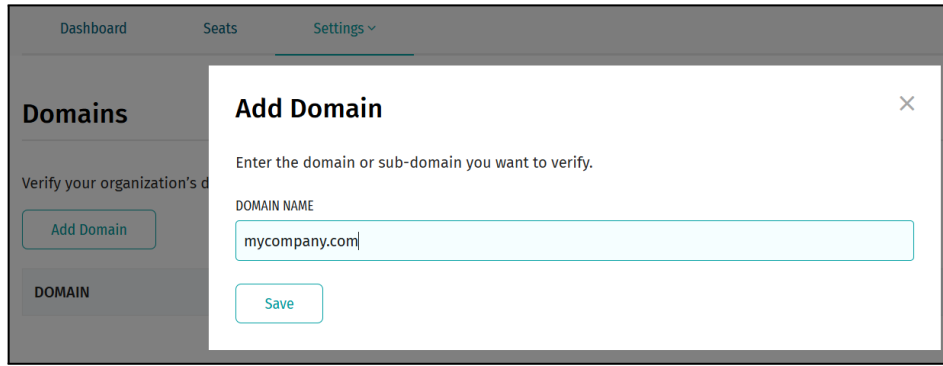
METADATA URL

METADATA XML

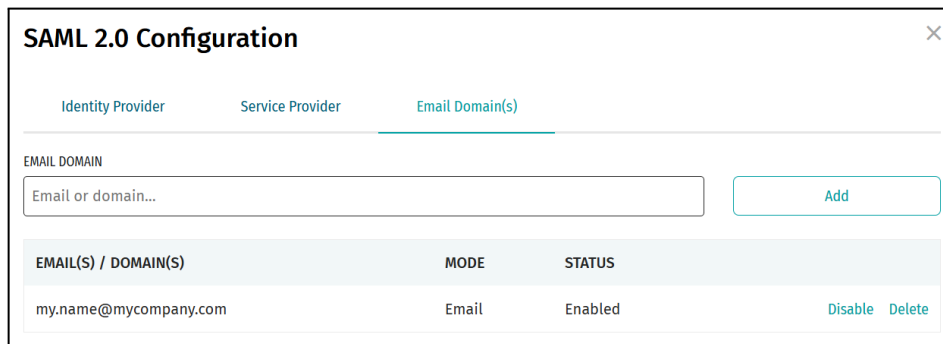
CONFIGURE MANUALLY

Save

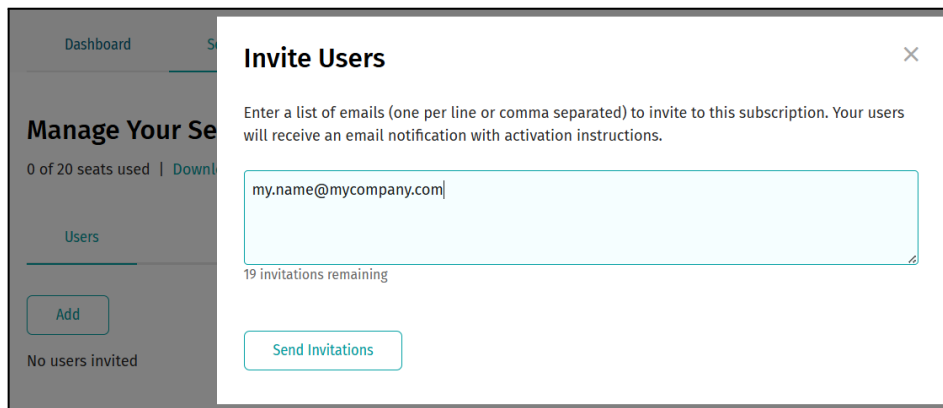
- Navigate to the **Domains** tab and add the email domain(s) that you wish to be able to use with SSO. Click **Save**:



10. You will need to verify ownership of this domain. Click **View** and follow the on-screen instructions to verify this, either by HTML file or DNS TXT record.
11. Once verified, return to the **Authentication** tab, and use the **Email Domain(s)** SAML tab to provide email addresses and/or email domains SSO access to SnapGene. **First, test SSO access with a single email address by adding that email address in full:**




12. If you are using Entra ID only for SSO, and not SCIM, you will need to invite these user(s) under the **Users** tab in My Account. Otherwise, SCIM users will be provisioned from Entra ID in the SCIM configuration section later in this guide.



13. If this user does not yet exist in Entra ID, create them in Entra ID now. From Entra ID, assign this user to your application from the Applications menu. If you are also configuring SCIM, then this process will instead be done later after provisioning has been configured (see the SCIM section of this guide for provisioning users).


14. In the SnapGene application, activate your software, selecting the **Email Sign In** option. Continue through the screens, selecting **Log In with SSO** as your authentication method:



## Choose an Activation Method

Your license type determines your activation method.  
[Need help?](#)

[Email Sign In](#) >  
Sign in with your SnapGene account used for your subscription.




## Choose Authentication Method

**my.name@mycompany.com**

Your email supports SSO through your organization or SnapGene login.

[Log In with SSO](#) >  
Connects to your organization's single sign-on portal.



## You're All Set

You're now ready to use all of the benefits included with your SnapGene subscription.

[Start Using SnapGene](#)

15. Once you have verified that SnapGene activates with this method, and are ready to enable SSO for your entire domain, add the email domain(s) that you wish to use with SSO. Also add the other users in both the **Users** tab of My Account, and in Entra ID as you have above:

### SAML 2.0 Configuration

Identity Provider    Service Provider    **Email Domain(s)**

EMAIL DOMAIN

Email or domain... [Add](#)

EMAIL(S) / DOMAIN(S)	MODE	STATUS	
mycompany.com	Domain	Enabled	<a href="#">Disable</a> <a href="#">Delete</a>

## SCIM Identity Management Configuration

1. To configure SCIM, you will first need to retrieve your SnapGene connection details from [My Account](#)
  1. From My Account, select **Manage Seats**, then **User Provisioning**
  2. Enable SCIM 2.0 and keep your **SCIM Base URL** and **API Token** handy for the next step:

Dashboard Seats Settings ▾

### User Provisioning

Configure automatic provisioning, updating and de-provisioning of users through SCIM. [Learn more](#)

**SCIM 2.0 STATUS**

ENABLED ▾

**Configuration Details**  
Use this information to set up the SCIM connection from IdP.

**SCIM BASE URL**

https://directory.snapgene.com/directories/

**API TOKEN**

\*\*\*\*\* [Regenerate Token](#)

**Provisioning Errors** ▾

2. Then in the **Provisioning** menu of your Entra ID **Enterprise** application:
  1. Select **Get started**
  2. Select **Automatic** as your **Provisioning Mode**
  3. Add your **SCIM Base URL** and **API Token Key**, copied from My Account, as the **Tenant URL** and **Secret Token**, respectively
  4. Click **Test Connection**
  5. Click **Save**

Overview Got feedback?

Provision on demand

**Manage**

Provisioning

**Monitor**

Provisioning logs

Audit logs

Insights

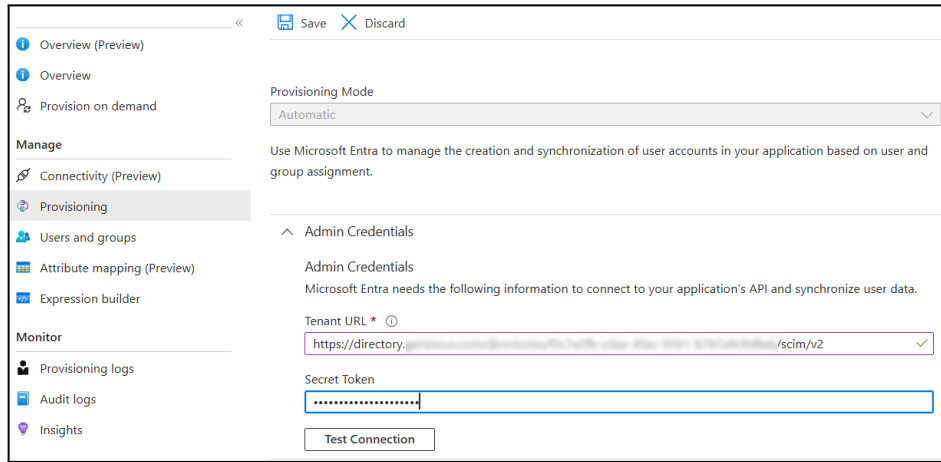
**Troubleshoot**

New support request

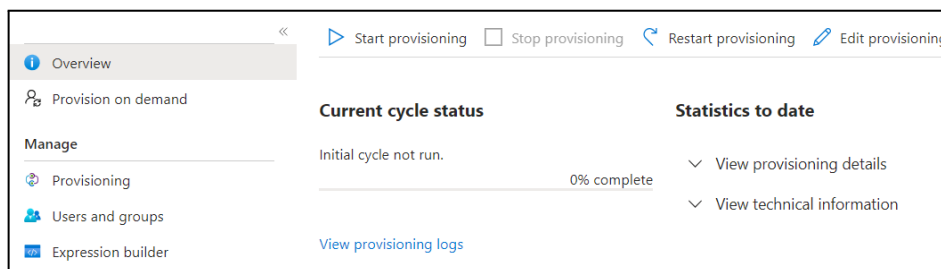
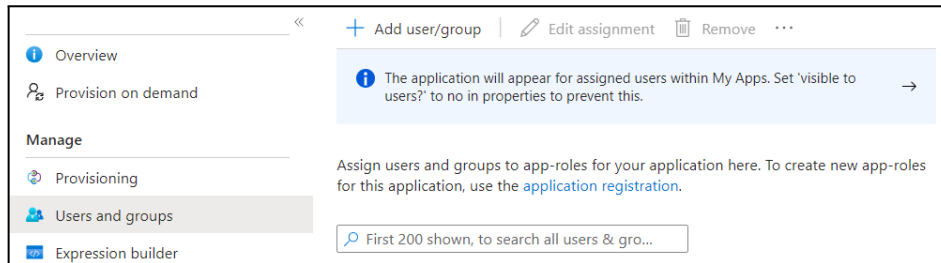
Automate identity lifecycle management with Microsoft Entra

Automatically create, update, and delete accounts when users join, leave, and move within your organization. [Learn more.](#)

[Get started](#)



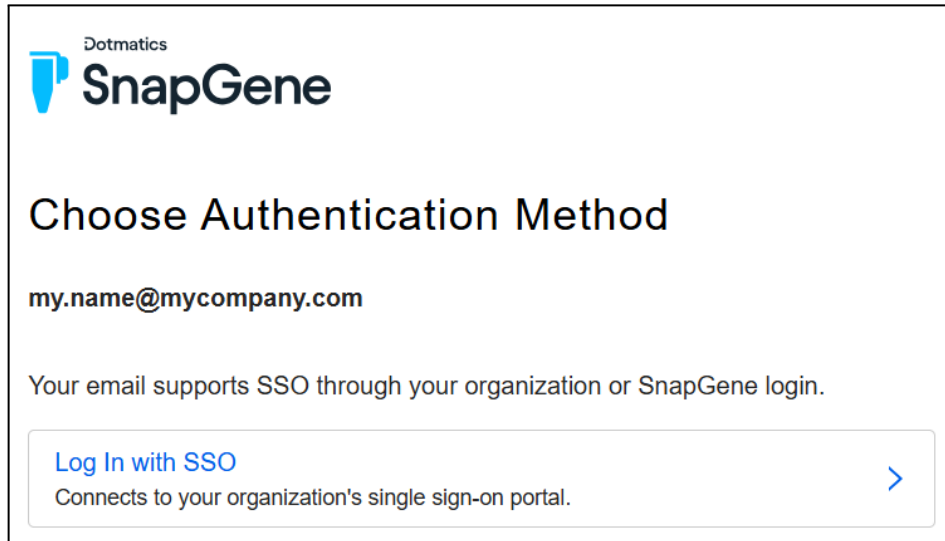
3. You have now successfully configured your user provisioning connection between Entra ID and SnapGene. You can now provision users from Entra ID into SnapGene by
  1. Returning to the **Provisioning** menu
  2. Select **User and groups**
  3. Click **Add user/group**
  4. **Select** and **Assign** those users/groups
  5. Return to the **Overview** of the **Provisioning** menu and click **Start provisioning**
  6. Click **Refresh** in the top right to see the provisioning complete



- Returning to My Account after provisioning is complete will show the end user(s) ready to activate SnapGene in the **Seats** tab - please reload the page:

EMAIL	NAME	ACTIVATED ON	DEVICES USED	STATUS
my.name@mycompany.com			0 / 2	PENDING

- In the SnapGene application, activate your software, selecting the **Email Sign In** option. Continue through the screens, selecting **Log In with SSO** as your authentication method:



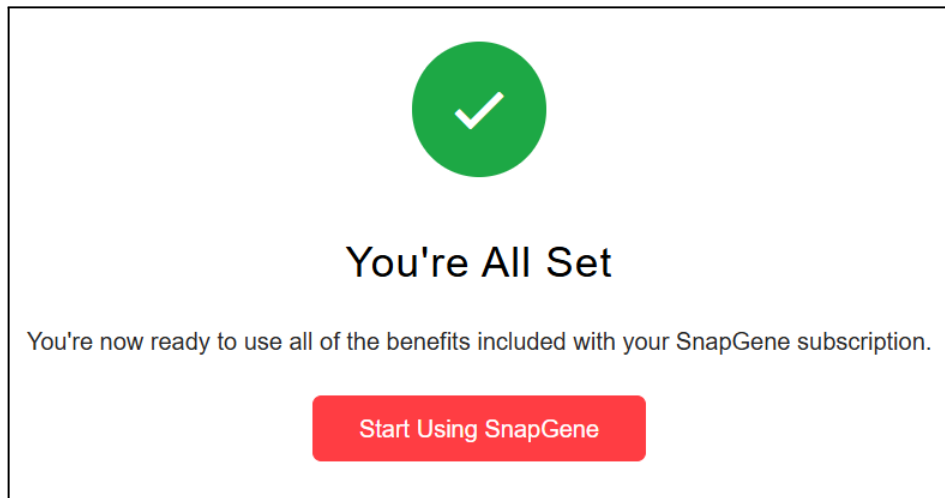
Dotmatics  
**SnapGene**


## Choose Authentication Method

my.name@mycompany.com

Your email supports SSO through your organization or SnapGene login.

[Log In with SSO](#) >  
Connects to your organization's single sign-on portal.





## You're All Set

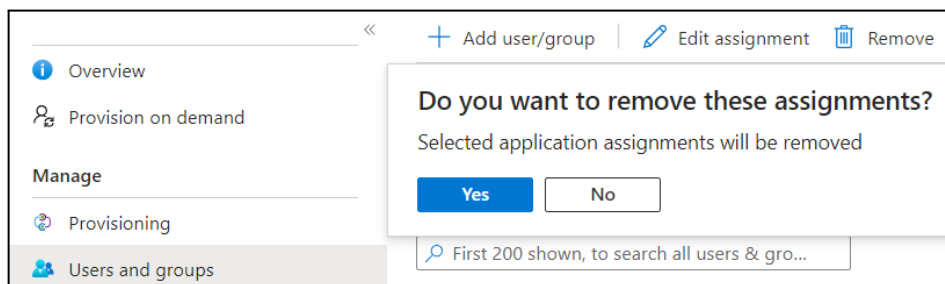
You're now ready to use all of the benefits included with your SnapGene subscription.

[Start Using SnapGene](#)

### Revoke User

To revoke a user via Entra ID:

1. In the **Users and groups** menu within your **Enterprise application**, select the user and click **Remove** and **Yes** to remove the assignment. Alternatively, remove the group, or the user from the group, if you have assigned a group to the application instead:



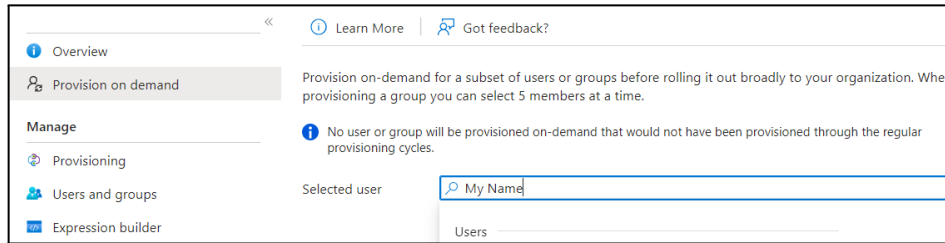
Navigation: Overview, Provision on demand, Manage, Provisioning, Users and groups

Actions: + Add user/group | Edit assignment | Remove

**Do you want to remove these assignments?**  
Selected application assignments will be removed

Search: First 200 shown, to search all users & gro...

2. Then from the **Provision on demand** menu, search for and select that same user, and click **Provision**:



3. Return to My Account and refresh the page. That user will now be removed from the **Users** list
4. Finally, in SnapGene, follow the **Help -> About SnapGene** menu. Here you will be notified that the activation has been revoked.