Dotmatics
Prism

OneLogin SSO & SCIM Guide

Getting Started

Accessing your user-based license

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

- Navigate to https://www.graphpad.com/myaccount/
- Log in with your existing credentials
- From the header drop down, select your user based subscription

Preparing Prism

In order to follow the below steps to enable your SSO/SCIM configuration, you will need to be using at least version 10.0.0 of Prism, and have deactivated your existing Prism activation.

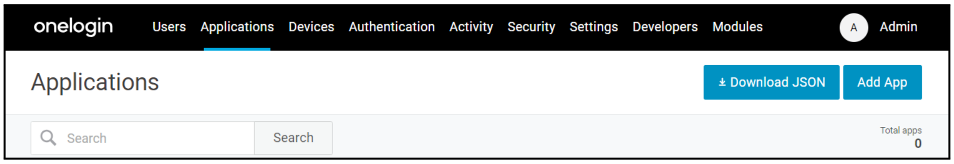
- To download the latest version, visit our Updates page, or update via the in-app updates feature
- Deactivate your current license by following **Help -> Manage License. . .**
- Let the Prism team know if your deactivation limit needs to be extended
- After deactivation, Prism should display the activation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

OneLogin Configuration

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

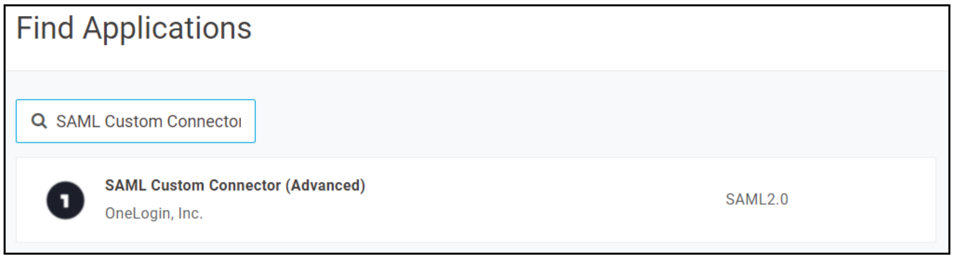
Creating an Application in OneLogin

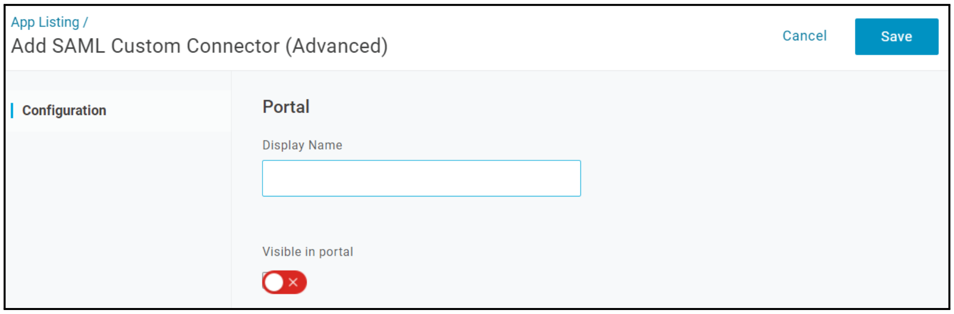
1. In the top menu of the Administration portal, navigate to **Applications** → **Applications**, and then select **Add App**:



2. **If using OneLogin only for SSO, and not SCIM provisioning**, search for **SAML Custom Connector (Advanced)**. Select this, enter a **Display Name** such as "GraphPad Prism", disable the **Visible in portal** option, and click **Save**.

   Otherwise, if using OneLogin for both SSO and SCIM (or planning to in the future), then use the **SCIM Provisioner with SAML (SCIM v2 Enterprise, full SAML)** application instead. The following screenshots correspond to the SSO case, but also apply to the SCIM application type.



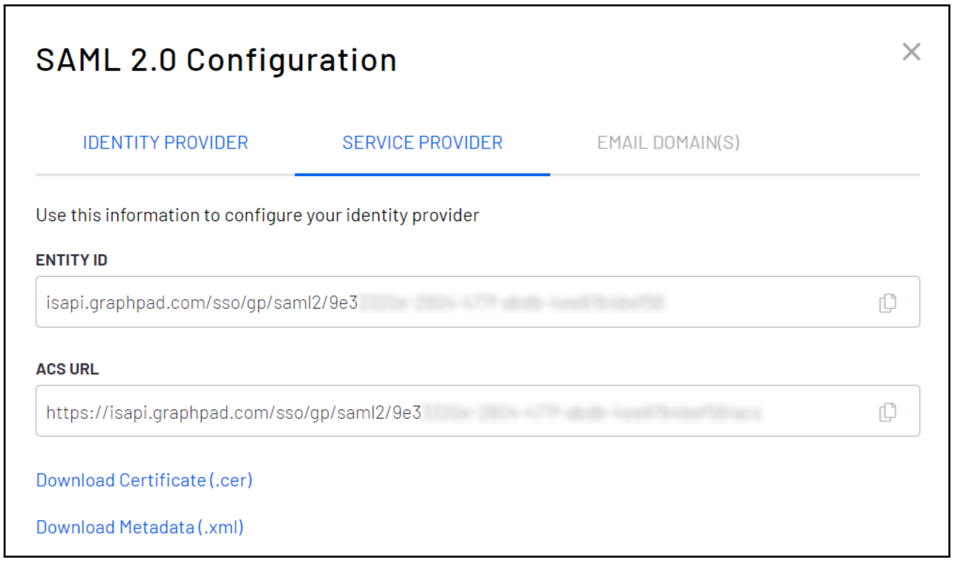


Single sign-on (SSO) Configuration

Once created, switch to the **Configuration** tab. Before continuing here, you will need to configure GraphPad Prism's My Account, and use information from here to configure OneLogin.

1. From My Account, select **Manage Seats**, then **Authentication**
2. Add a SAML2 **ID Provider**
3. Switch to the **Service Provider** tab and copy the **Entity ID** and **ACS URL**. Paste these into the **Configuration** tab in your OneLogin application.

   The **Entity ID** corresponds to the **Audience (Entity ID)** (this is called **SAML Audience URL** in SCIM), and the **ACS URL** corresponds to both the **ACS (Consumer) URL Validator** and **ACS (Consumer) URL** fields:



SAML 2.0 Configuration

Use this information to configure your identity provider

ENTITY ID

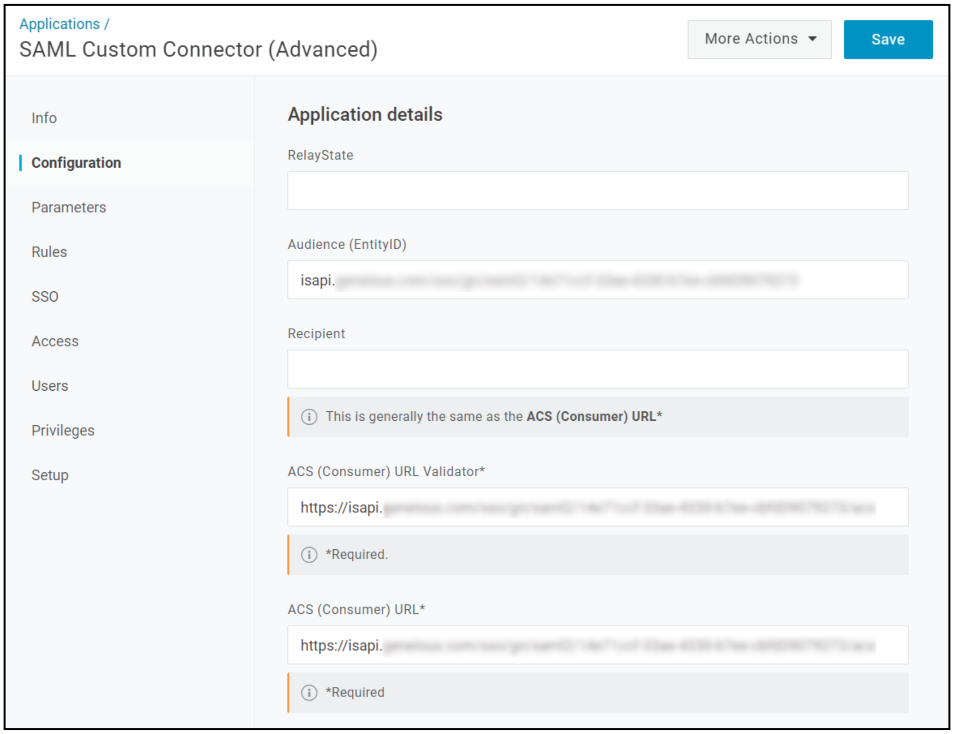
isapi.graphpad.com/sso/gp/saml2/9e3[redacted]

ACS URL

https://isapi.graphpad.com/sso/gp/saml2/9e3[redacted]

Download Certificate (.cer)

Download Metadata (.xml)



Applications /

SAML Custom Connector (Advanced)

Application details

RelayState

Audience (EntityID)

isapi.[redacted]

Recipient

This is generally the same as the **ACS (Consumer) URL***

ACS (Consumer) URL Validator*

https://isapi.[redacted]

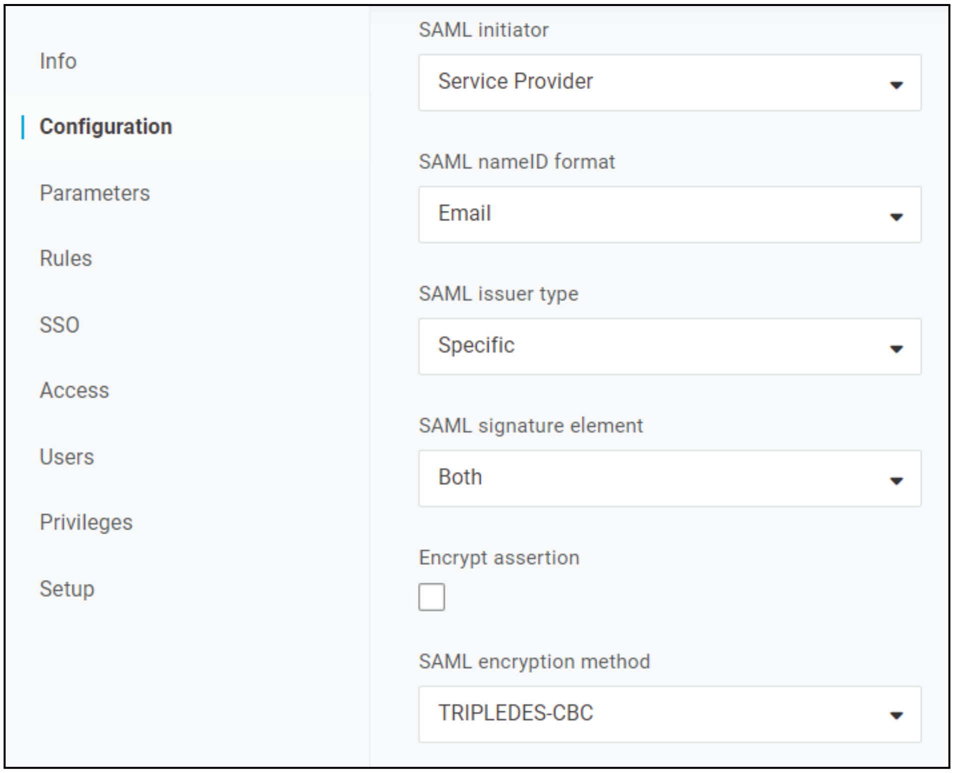
*Required.

ACS (Consumer) URL*

https://isapi.[redacted]

*Required

4. Set the **SAML Initiator** to **Service Provider** and the **SAML signature element** to **Both**. Check that the other fields match the below screenshot. Click **Save**:



SAML initiator: Service Provider

SAML nameID format: Email

SAML issuer type: Specific

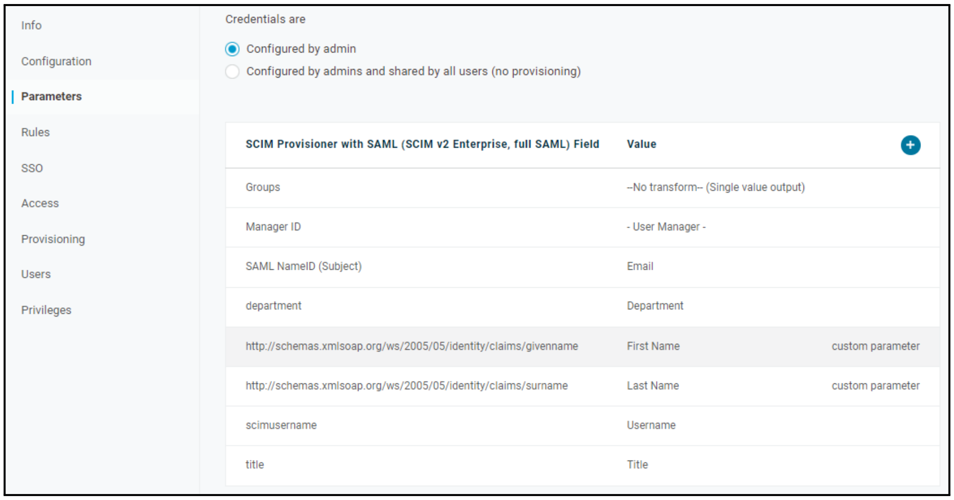
SAML signature element: Both

Encrypt assertion: □

SAML encryption method: TRIPLEDES-CBC

5. In the **Parameters** menu, add the following two fields:
   - **Field name**: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`
     Value: First Name
   - **Field name**: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`
     Value: Last Name

   Select the **Include in SAML assertion** flag (and **Include in User Provisioning** for SCIM)



Credentials are

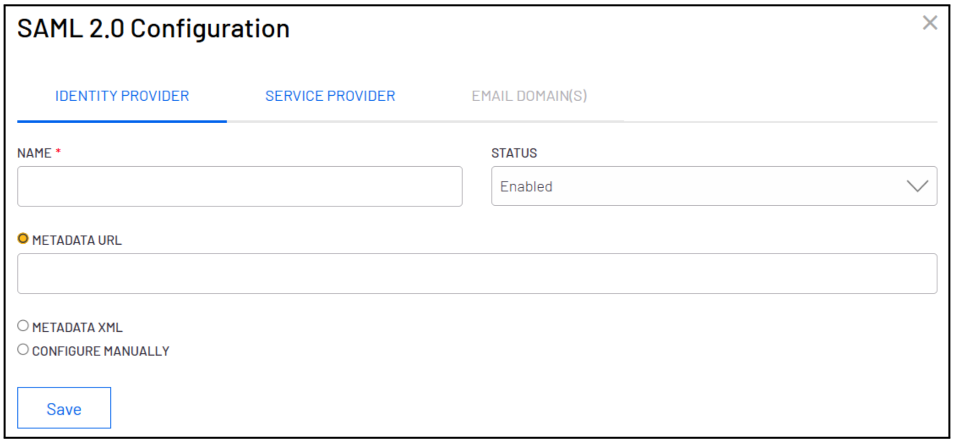
● Configured by admin

○ Configured by admins and shared by all users (no provisioning)

SCIM Provisioner with SAML (SCIM v2 Enterprise, full SAML) Field	Value	
Groups	--No transform-- (Single value output)	
Manager ID	- User Manager -	
SAML NameID (Subject)	Email	
department	Department	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	First Name	custom parameter
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Last Name	custom parameter
scimusername	Username	
title	Title	

6. In the SSO menu, set the **SAML Signature Algorithm** to **SHA-256**:
7. From the **More Actions** menu in the top right, download the **SAML Metadata** file
8. Return to My Account and switch to the **Identity Provider** tab. Enter a name e.g. “OneLogin”,

and copy the content of the downloaded file from OneLogin into the **Metadata XML** field. Click **Save**:


SAML 2.0 Configuration

NAME *

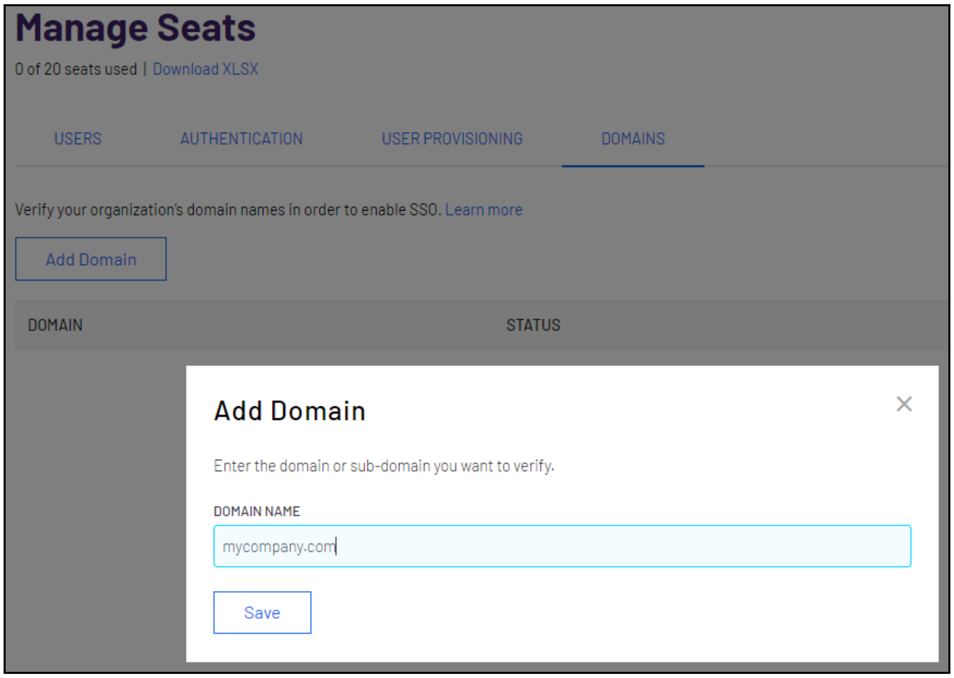
STATUS: Enabled

● METADATA URL

○ METADATA XML

○ CONFIGURE MANUALLY

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


Manage Seats

0 of 20 seats used | Download XLSX

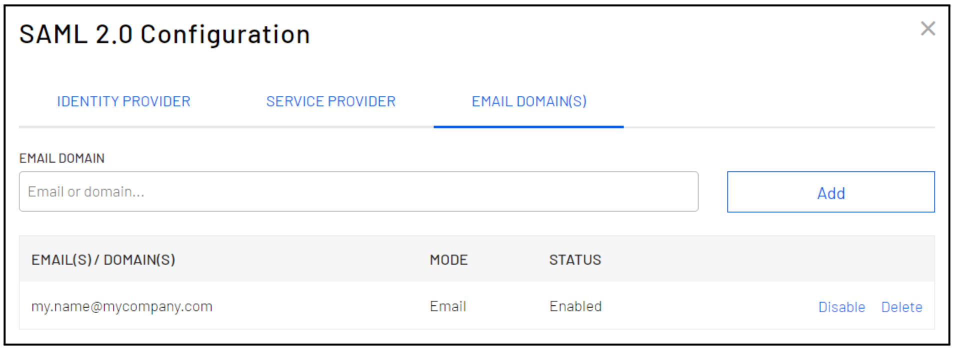
Verify your organization's domain names in order to enable SSO. Learn more

Add Domain

Enter the domain or sub-domain you want to verify.

DOMAIN NAME: mycompany.com

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 Prism. **First, test SSO access with a single email address by adding that email address in full:**



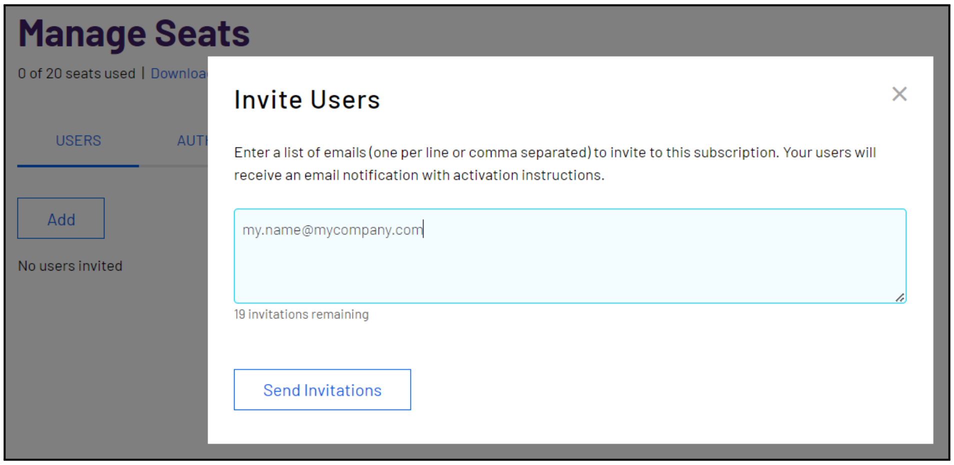
SAML 2.0 Configuration

EMAIL DOMAIN

Email or domain...

EMAIL(S) / DOMAIN(S)	MODE	STATUS
my.name@mycompany.com	Email	Enabled

12. If you are using OneLogin 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 OneLogin in the SCIM configuration section later in this guide.



0 of 20 seats used

No users invited

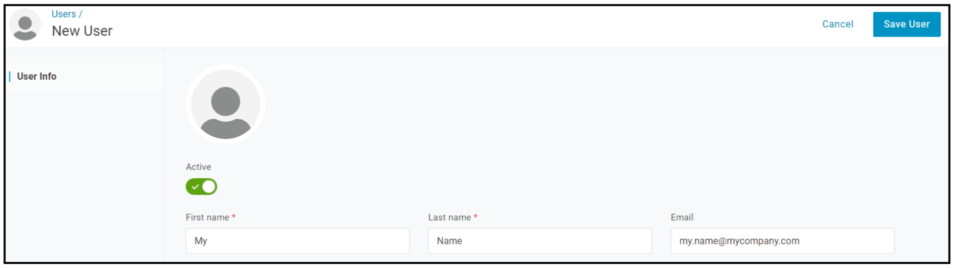
Invite Users

Enter a list of emails (one per line or comma separated) to invite to this subscription. Your users will receive an email notification with activation instructions.

my.name@mycompany.com

19 invitations remaining

13. If this user does not yet exist in OneLogin, create them in OneLogin now.
From OneLogin, 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).
Tick **Allow the user to sign in** and **Hide this app in Portal**:

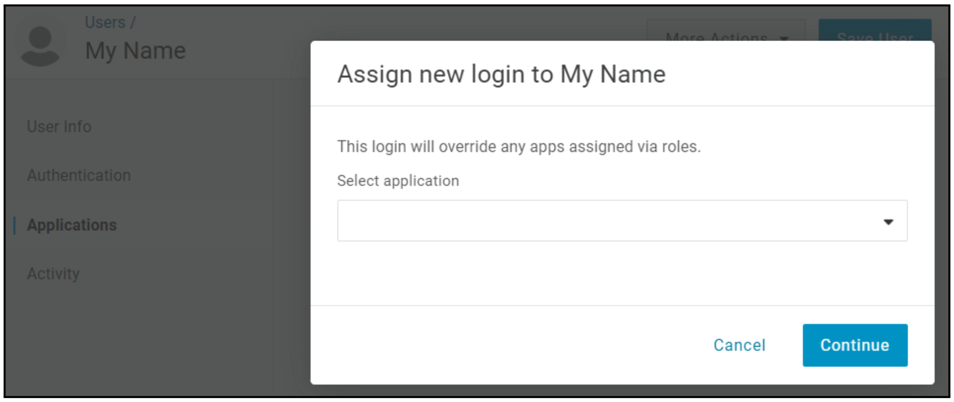


Active

First name * My

Last name * Name

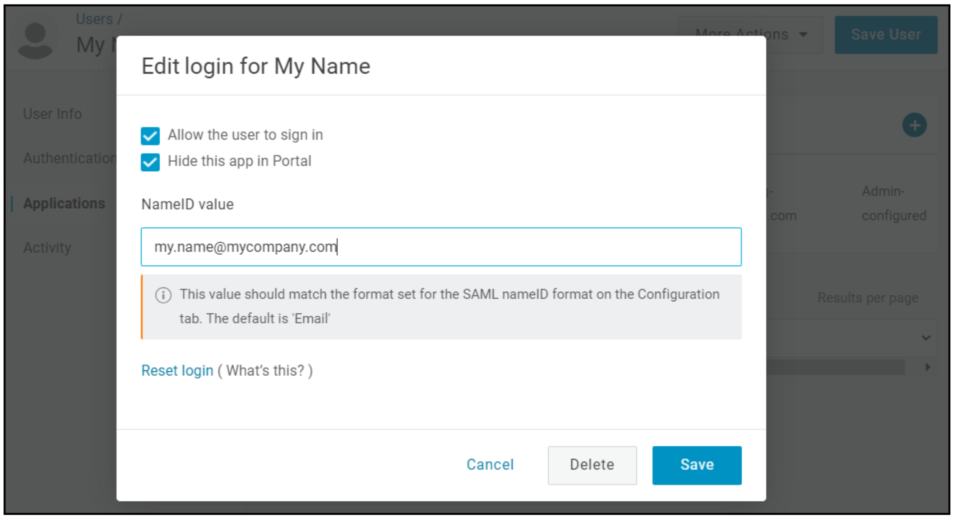
Email my.name@mycompany.com



Assign new login to My Name

This login will override any apps assigned via roles.

Select application



Edit login for My Name

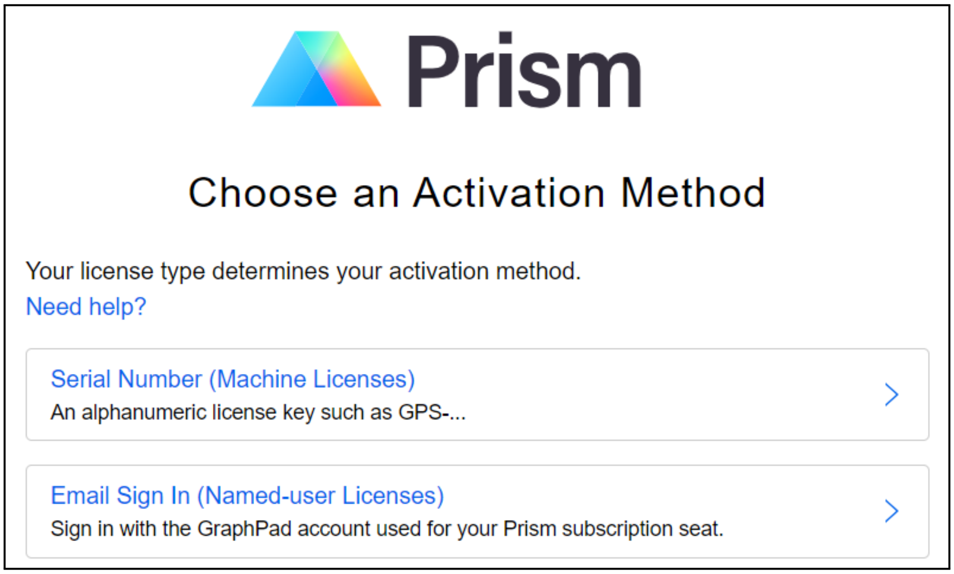
☑ Allow the user to sign in
☑ Hide this app in Portal

NameID value: my.name@mycompany.com

This value should match the format set for the SAML nameID format on the Configuration tab. The default is 'Email'

Reset login (What's this?)

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

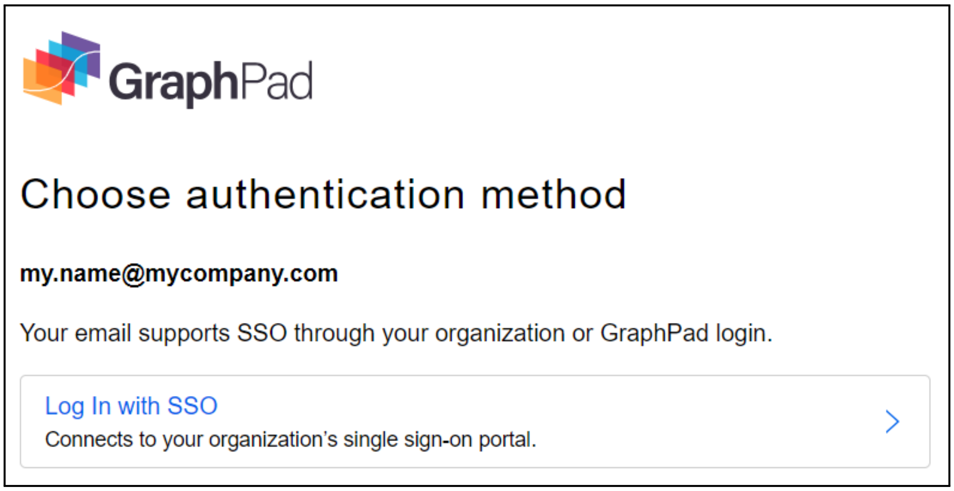


Choose an Activation Method

Your license type determines your activation method.
Need help?

Serial Number (Machine Licenses)
An alphanumeric license key such as GPS-...

Email Sign In (Named-user Licenses)
Sign in with the GraphPad account used for your Prism subscription seat.

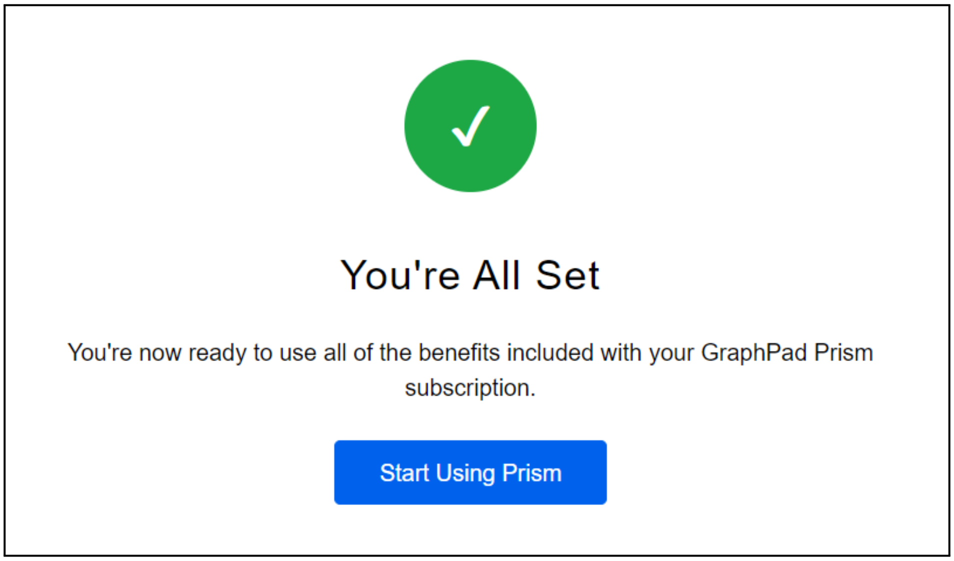


Choose authentication method

my.name@mycompany.com

Your email supports SSO through your organization or GraphPad login.

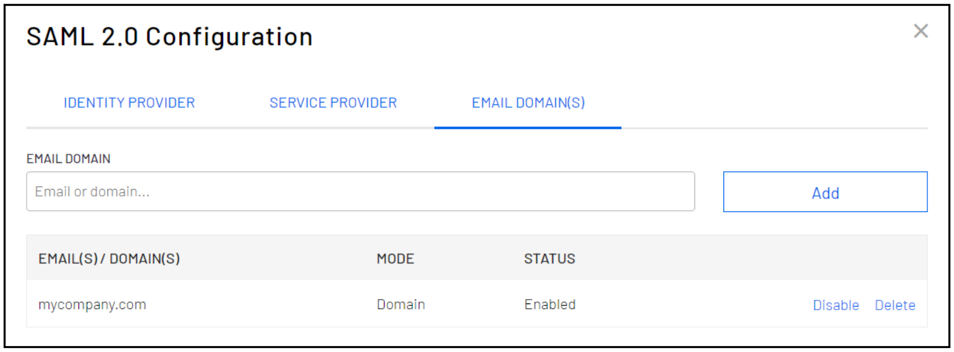
Connects to your organization's single sign-on portal.



You're All Set

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

15. Once you have verified that Prism 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 OneLogin as you have above:

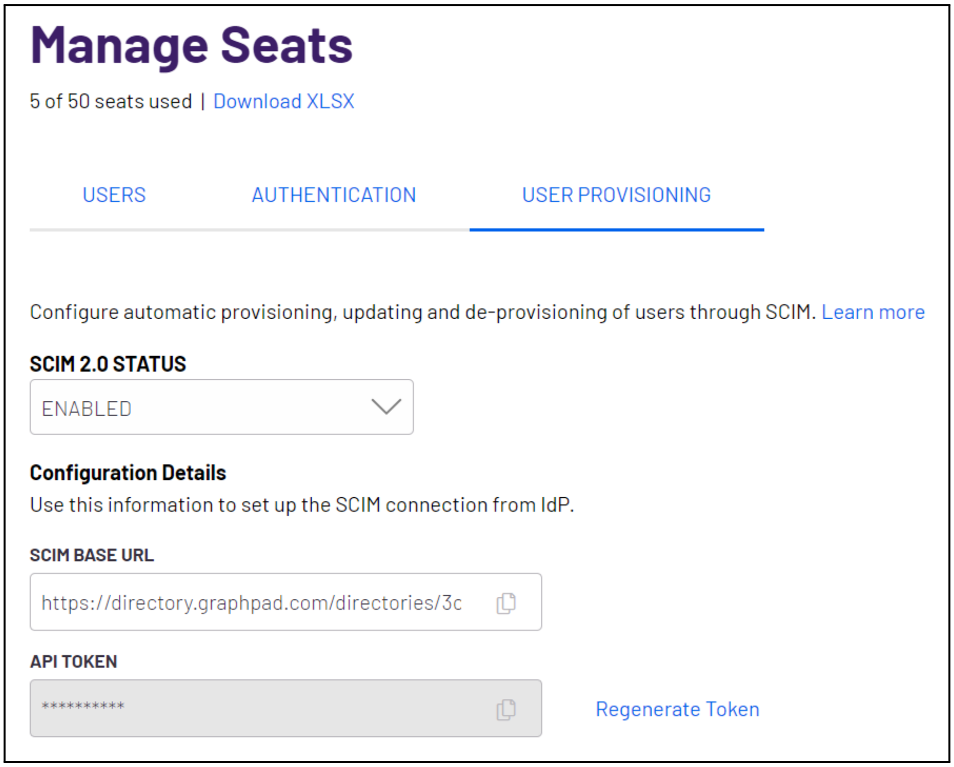


SAML 2.0 Configuration

EMAIL(S) / DOMAIN(S)	MODE	STATUS	
mycompany.com	Domain	Enabled	Disable Delete

SCIM Identity Management Configuration

1. To configure SCIM, you will first need to retrieve your Prism 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:



Manage Seats

5 of 50 seats used | Download XLSX

Configure automatic provisioning, updating and de-provisioning of users through SCIM. Learn more

SCIM 2.0 STATUS: ENABLED

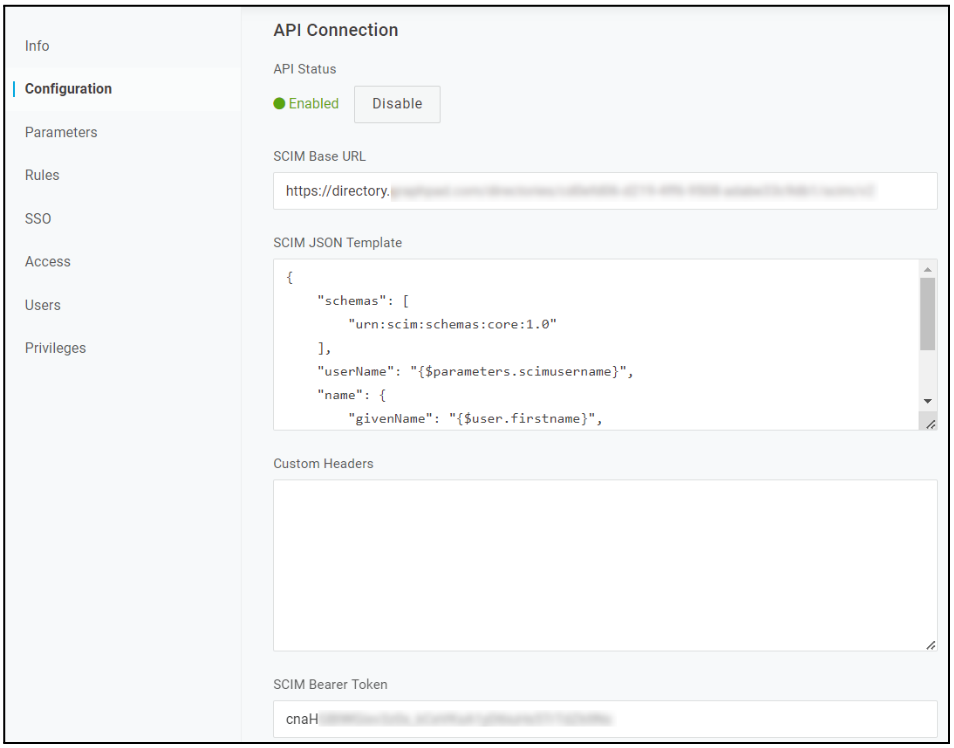
Configuration Details

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

SCIM BASE URL: https://directory.graphpad.com/directories/3c

API TOKEN: **********

2. Then in the **Configuration** menu of your OneLogin application:
    1. Add your **SCIM Base URL** and **API Token Key**, copied from My Account, as the **SCIM Base URL** and **SCIM Bearer Token**, respectively
    2. **Enable** the **API Connection**
    3. Click **Save**



API Connection

API Status

● Enabled

SCIM Base URL

https://directory.[redacted]

SCIM JSON Template

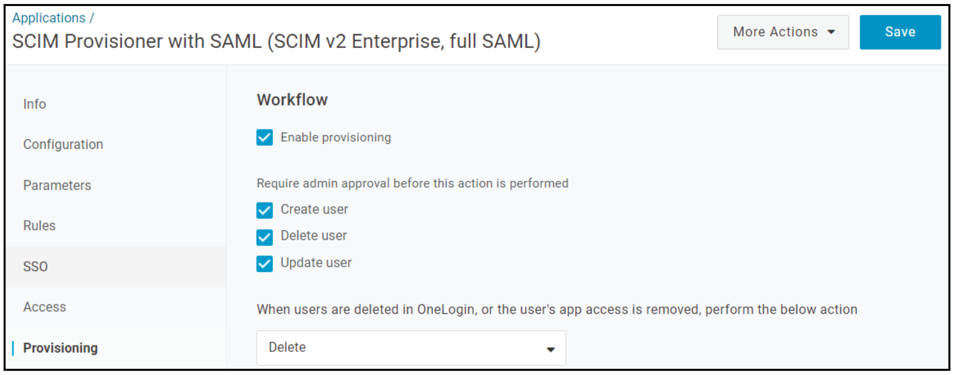
```
{
    "schemas": [
        "urn:scim:schemas:core:1.0"
    ],
    "userName": "{$parameters.scimusername}",
    "name": {
        "givenName": "{$user.firstname}",
```

Custom Headers

SCIM Bearer Token

cnaH[redacted]

3. From the **Provisioning** tab, enable provisioning:



SCIM Provisioner with SAML (SCIM v2 Enterprise, full SAML)

Workflow

☑ Enable provisioning

Require admin approval before this action is performed

☑ Create user

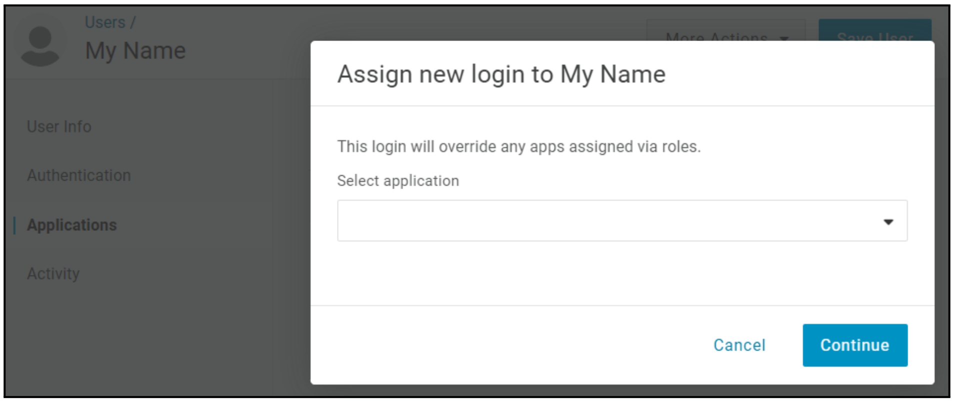
☑ Delete user

☑ Update user

When users are deleted in OneLogin, or the user's app access is removed, perform the below action

Delete

4. You have now successfully configured your user provisioning connection between OneLogin and GraphPad Prism. You can now provision users from OneLogin into Prism by
    1. Navigate to that user from the top level **Users** menu
    2. Using the **Applications** side menu of that user, add your application
    3. No changes should need to be made in the following screen. Scroll down to confirm that the first name and last name have been mapped correctly from their user account, and click **Save**
    4. If the status of the provisioning is showing as **Pending**, then click that status to complete the provisioning

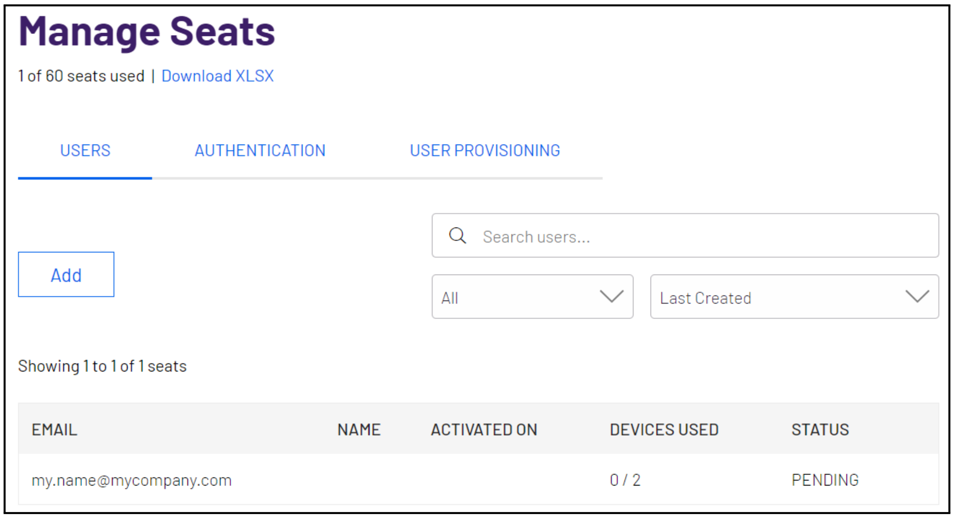


Assign new login to My Name

This login will override any apps assigned via roles.

Select application

5. Returning to My Account after provisioning is complete will show the end user(s) ready to activate GraphPad Prism in the **Users** tab - please reload the page:

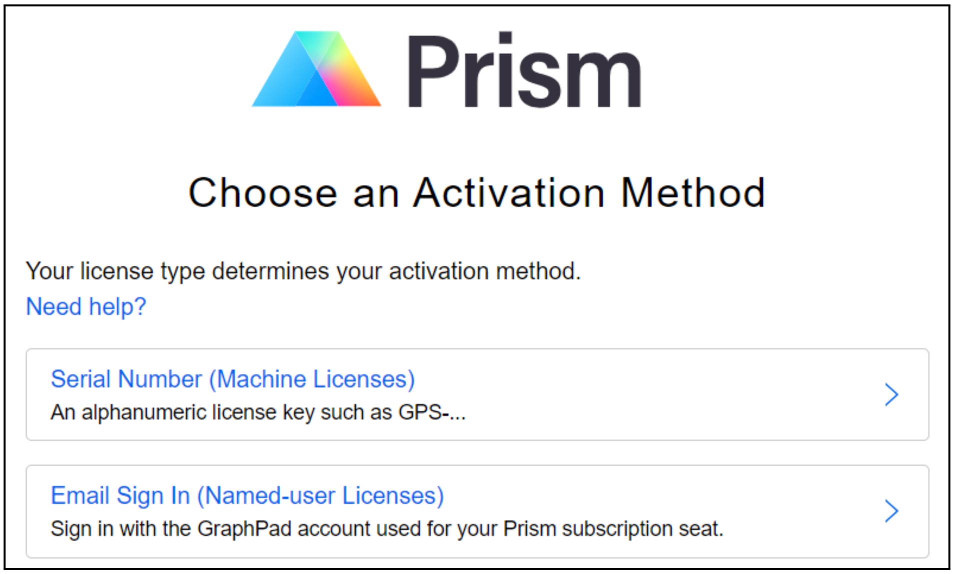

Manage Seats

1 of 60 seats used | Download XLSX

Showing 1 to 1 of 1 seats

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

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

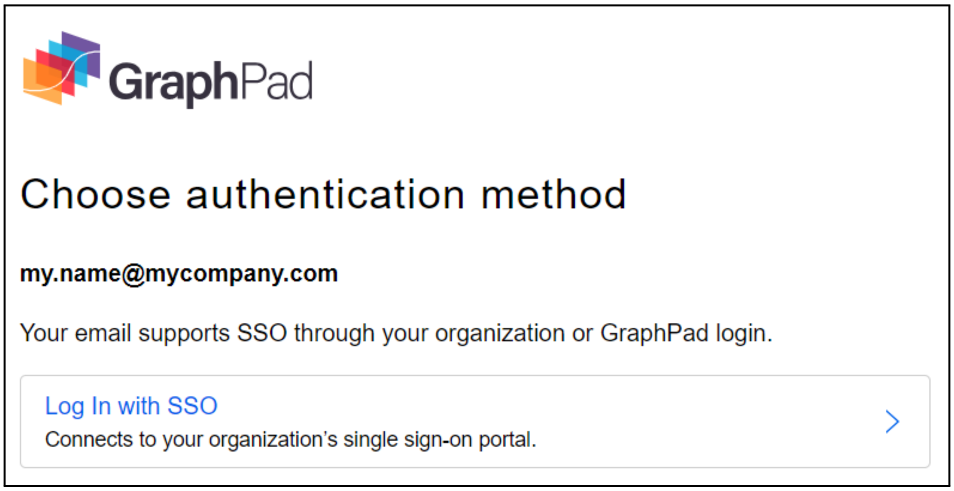


Choose an Activation Method

Your license type determines your activation method.
Need help?

Serial Number (Machine Licenses)
An alphanumeric license key such as GPS-...

Email Sign In (Named-user Licenses)
Sign in with the GraphPad account used for your Prism subscription seat.



GraphPad

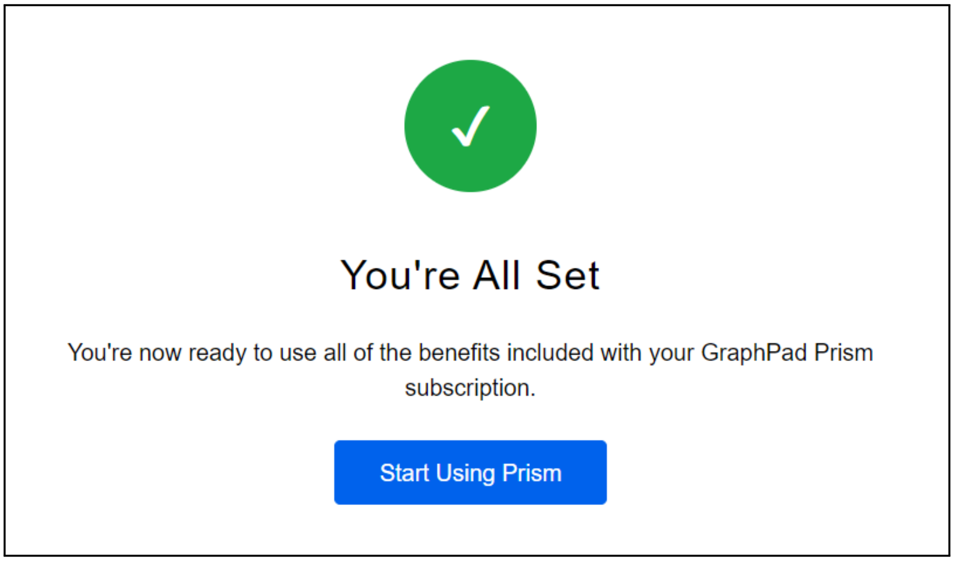
Choose authentication method

my.name@mycompany.com

Your email supports SSO through your organization or GraphPad 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 GraphPad Prism subscription.

Revoke User

To revoke a user via OneLogin:

1. Either from the **Applications** tab in the **User**, or the **User** tab in the **Application**, delete the association between the two. This may need to be approved in a second step if a status of **Pending** is shown - click the status to do so. Alternatively, remove the group, or the user from the group, if you have assigned a group to the application instead.
2. Return to My Account and refresh the page. That user will now be removed from the **Users** list
3. Finally, in Prism, follow the **Help -> About Prism** menu. Here you will be notified that the activation has been revoked.