CLARITY STREET

HOW TO SET UP A NEW EMPLOYEE

A STEP-BY-STEP GUIDE ON HOW TO SET UP A NEW EMPLOYEE ON XERO, XPM & PRACTICE PROTECT

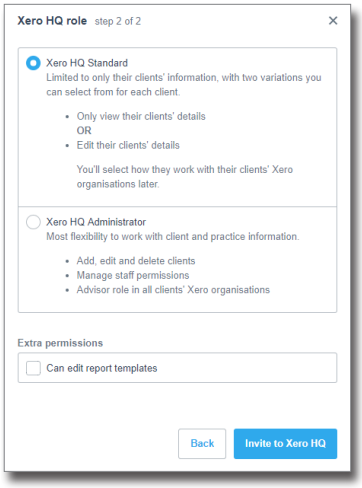
You want your new employee's first day to be as seamless as possible so they can hit the ground running. You need to get their computer set up, their phone configured, payroll elements and office access sorted. You also definitely need them set up on all the software applications you use. Where do you begin though? There's so many applications, and it's really important that they are set up in a specific order.

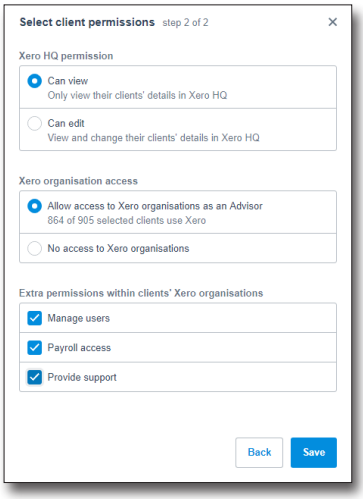
We've developed this guide to take you through each process step-by-step.

We'll walk you through the setting up of a new team member through all the Xero ecosystem applications as well as Practice Protect.

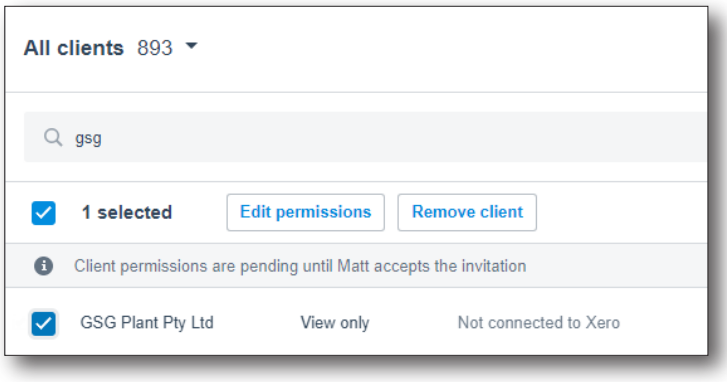
1 SETTING UP USER ON XERO

1. Log into Xero HQ as an administrator.
2. Go to the staff tab.
3. Click on invite staff in the top right.
4. Type in the staff members details.
5. Select the type of role that they can fulfil. Most of the time unless they are a director this will be Xero HQ Standard.
6. Tick if they will have the ability to edit practice report templates.
7. Invite to Xero HQ.
8. Give the user access to all organisations by clicking on Add Clients then Select All (you will then deselect after step 8 any clients that they should not have access to).
9. If your firms policy is to only give access to clients that they will be working on you will need to select those client individually rather than selecting all. Using a job/staff report in XPM will help you to identify those that they will be accessing, if this allocation in XPM has been done already.





- If selecting all the clients then DE-SELECT the following as its easier to do when giving initial access. Search for names below, tick and select Remove Client.
- If not selecting all the clients and adding them one by one, you will not need to do this step.



Insert private clients Xero files below. Eg. Directors files or files that are not to be shared with anyone.

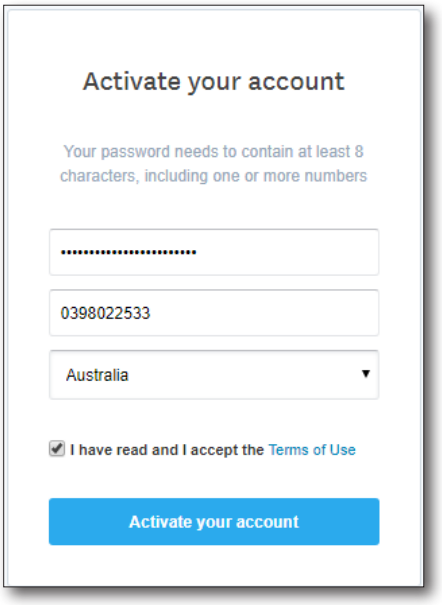
- The user that receives the password redirects will receive the employee's invitation. Forward this to the employee to be set up on their first day.

1 SETTING UP USER ON XERO

Users First Day

Please ensure that the user accepts the Xero HQ invitation first and not the Xero Practice Manager invitation.

1. Click on accept invitation from the Xero HQ email.
2. Have the employee set up their password and log in.
3. Have the employee now accept their Xero Practice Manager Invitation from their emails and use the password that was just set up for Xero HQ.
4. The user will be prompted to set up their dual factor authentication, security questions and alternative email.
5. This will now link Xero HQ & Xero Practice Manager.



Resetting the new employees password and adding to Practice Protect

You will now need to reset the employee Xero password, once they have set up both Xero HQ and Xero Practice manager.

1. Go to www.login.xero.com and click on forgot password and enter the employees email you are wanting to reset.
2. The staff member who is receiving Practice Protect password redirects will now receive a password reset email.
3. Click on reset password and reset the password. Use the Practice Protect Password Generator to generate a random password.
4. Go to your Practice Protect admin portal and click on users and the appropriate user.
5. Click on application settings and click add (top right) and add the Xero app.
6. Enter the users email and password that you generated in step 3.

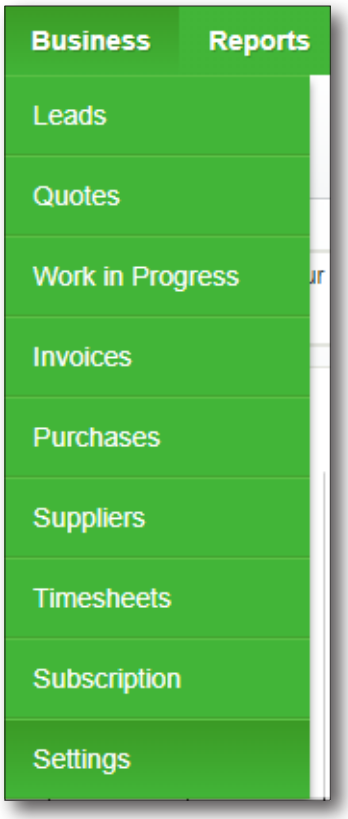
The employees Xero password is now reset and they can access Xero via their Practice Protect Portal.

2 SETTING UP XERO PRACTICE MANAGER USER

1. Log into Xero Practice Manager as an administrator.
2. Click on Business then Settings.
3. Click on Staff on the right hand side.
4. Invite Staff (left-hand side toolbar).
5. Enter the relevant information of the new staff member (no payroll code) (Ask a Director for the base and billable rate if not already known).
6. Tick Fee Earner so that their KPI's work in the reports. Leave full-time equivalent at 100% unless they are part-time. This will be used in the productivity reports.
7. Depending on the employee you will need to decide on what permissions to assign to them.

   (Insert below standard permissions as agreed by Directors)

8. At the bottom click Save.
9. The staff member who is receiving Practice Protect password redirects will now receive an email login to their email address.
10. Forward email to new employee's email address as they will need to login and set up their user on their first day due to Multifactor Authentication setup.



Employees first day

Please ensure this step is completed after the Xero HQ invitation has been accepted and their password has been set.

1. Click on the link from the XPM email to accept the new user.
2. Use the Username and Password that the employee set up in the Xero HQ set up to accept the invitation.
3. This will associate XPM with the users Xero File.
4. The employee will now be prompted to activate their dual-factor authentication. This cannot be done any earlier as the authentication must be on their phone and not yours!

2 SETTING UP XERO PRACTICE MANAGER USER

Resetting the new employees' password and adding to Practice Protect

You will now need to reset the employee Xero password, once they have set up both Xero HQ and Xero Practice Manager.

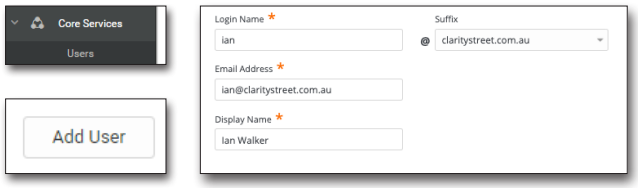
1. Go to www.login.xero.com and click on forgot password and enter the employee's email you are wanting to reset.
2. The staff member who is receiving Practice Protect password redirects will now receive a password reset email.
3. Click on reset password and reset the password. Use the Practice Protect Password Generator to generate a random password.
4. Go to your Practice Protect admin portal and click on users and the appropriate user.
5. Click on application settings and click add (top right) and add the Xero app.
6. Enter the user's email and password that you generated in step 3.

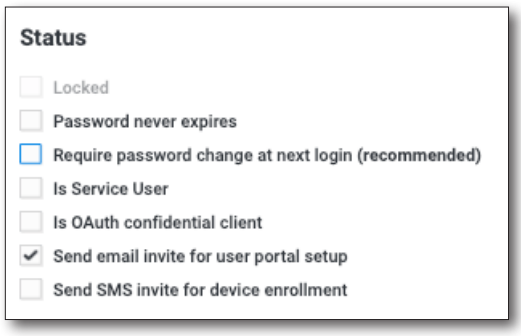
The employees Xero password is now reset, and they can access Xero via their Practice Protect Portal.

3 SETTING UP AN EMPLOYEE ON PRACTICE PROTECT

Adding a new user

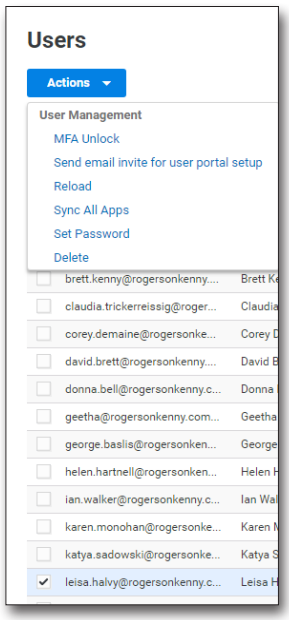
1. Log into Practice Protect as an administrator.
2. Add the employee as a new user under Core Services Users.





3. Keep the password type as manual as and make the password ChangeMe123 as the user will need to change this the first time they log into Practice Protect.
4. Keep the status's as seen above.
5. Select Create User. The user will now be created and a confirmation email sent to their inbox. When the employee starts you will need to help them through the setup stage (i.e. they will need to put in their unique chosen password (8 characters), dual factor authentication and security question.

Inviting User

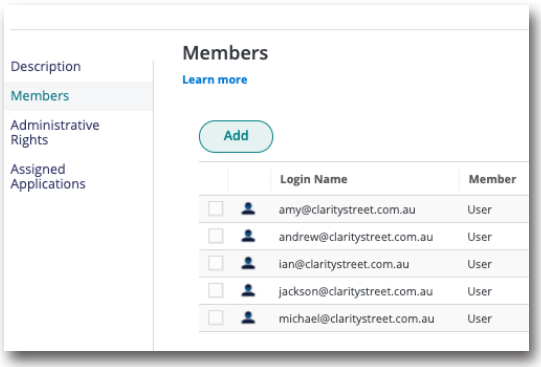


1. Click on the user under core services and then go to Screen Clipping and invite user to portal.
2. Select Yes to send.

Setting up new users applications

Setting up roles

1. Click on Core Services.
2. Click on Roles.
3. Click into the relevant role and assign the user eg if they are an accountant please tick accountants, if they are admin please click admin. All staff are automatically assigned to Everybody.
4. Click on Members when in Roles.
5. Select Add.
6. Search by using first name and select and Add.



3 SETTING UP AN EMPLOYEE ON PRACTICE PROTECT

Setting up user applications

1. Click on Users under Core Services.
2. Click into the relevant employee.
3. Click on assigned applications to view what the user should have access to – These are all the applications that the user will have access too. Some will have generic usernames and passwords while others will have to be user specific. Refer to below to see what needs to be set up on an individual user basis.
4. Click on application settings and add the following applications following their application specific user guide steps.

Shared User Logins

Some applications only have one user and the login credentials are shared between multiple users. If this is the case then make sure that the user is assigned to a role that has the application within it. They will then be able to access the application WITHOUT you having to set a password at the user level as this has been setup from the application itself as a shared login.

Testing Applications from Employee's Portal

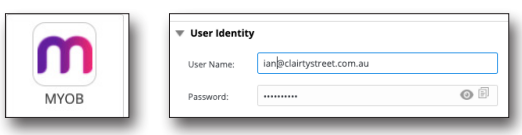
1. Log into the employees emails.
2. Accept the invitation to join Practice Protect.
3. Enter the created password – ChangeMe123.
4. You will be prompted to enter in MultiFactor Authentication (MFA) sometimes referred to as OATH.
5. Enter this authenticator on your phone. This needs to be done so you can access the applications as it is mandatory to set up the MFA.
6. Set up the secret question if prompted.

You are now logged in as the employee in their user portal

Click on the applications that you have set up for them from the Admin portal to test that they login correctly. If they do not login correctly, check that the username is correct and or reset the password and update in the Admin portal for that particular users application.

You can also set up passwords to applications that the user is required to know at this point. Eg MYOB is a hybrid cloud application where the user is required to know their password. You would enter this password by doing the following:

1. Hover over the appropriate application eg MYOB.
2. Click on the gear icon of the appropriate app in the user portal.
3. Click on "user identity".
4. Enter the username and password for that application.



3 SETTING UP AN EMPLOYEE ON PRACTICE PROTECT

The user is now able to see the password that has been set by clicking on the eye symbol from within the user identity.

It is important that this function is only performed for applications where the user is REQUIRED to know their password. For all other applications the user's password should be stored at the user application level within the admin portal.

When you are happy that all the applications have been assigned and are working correctly, logout of the users portal.

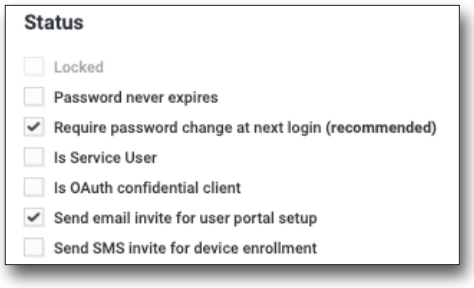
Finalising User Creation

When you are happy that you have allocated all the applications and to the user and they are working appropriately, follow the steps below to finalise the setup.

Re-enable password change at next login

You need to re-enable "require password change at next login" from the users account in the Admin Portal.

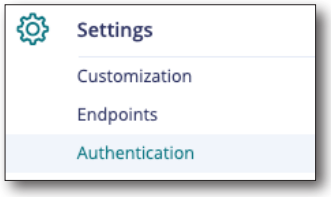
1. Log into the admin portal.
2. Click on users.
3. Click on the user.
4. Scroll down to the status section.
5. Tick the box "require password change at next login".
6. Save.



Disable MFA

You will need to disable MFA to allow the employee to login on their first day without being prompted to enter the MFA code that you set up on your phone.

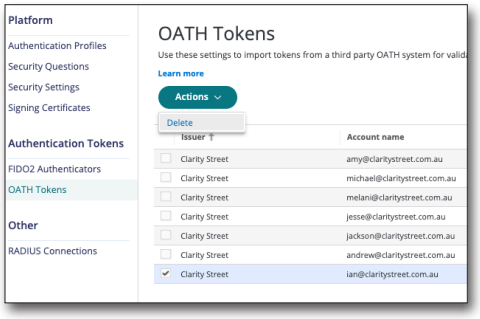
1. Login to Admin Portal.
2. Click on Settings and then Authentication.
3. Select under Authentication Tokens OATH Tokens.



3 SETTING UP AN EMPLOYEE ON PRACTICE PROTECT

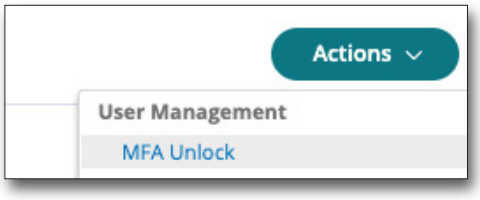
Disable MFA

4. Select the new employee.
5. Click on Actions up the top left of the screen. and delete the Multifactor Authentication that you had set up initially.
6. Re invite the user to the user portal so that they can set up their Multifactor Authentication on their first login via the email.



If the user cannot access their Practice Protect Portal on the next login you will need to disable their MFA from the admin portal.

1. Login to Admin Portal.
2. Click on users.
3. Select the new employee.
4. Click on actions in the top right and click on MFA unlock.
5. This will enable the user to login to their portal without entering their MFA. This is a single use process and is valid for 15 minutes.



Logging in for the first time

On the user's first day they will need to login using the email for the portal invitation.

When the user logs into their portal for the first time with the password ChangeMe123 they will be required to change this to an appropriate unique password.

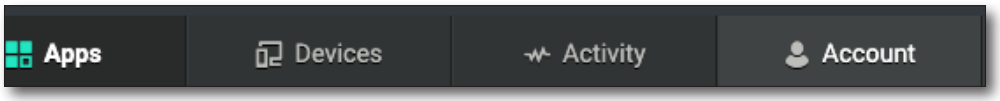
They should NOT be prompted to enter their MFA as per the steps above re Disabling MFA. If they are prompted to login you will need to follow the steps to disable MFA.

The user is now in their user portal and should be prompted with the setup guide if using the link from the email or if directly logging in they will need to follow the steps below.

Changing Default Password

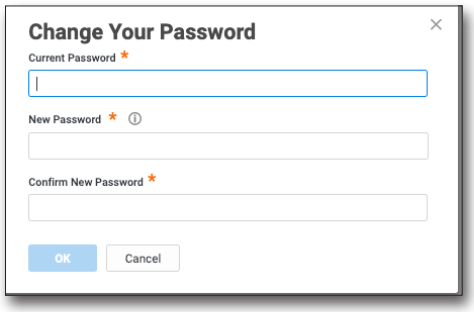
The user will now have to change their password from the default of ChangeMe123.

1. Go to account.



3 SETTING UP AN EMPLOYEE ON PRACTICE PROTECT

2. Click on edit next to password.
3. Change to a password that is unique to the user and that no one else knows. A phrase is suggested here like 1LikeDogs as this is harder than a word to break.
4. The user's password has now been changed.



Security Question

The user will now need to set up their security question for when they are not able to use their Authentication app.

1. From the security section where they changed their password – see above.
2. Click on edit next to the security question.
3. Enter a security question that no-one else knows and that is not able to be found on social media. A good example is what was my birth weight or who was my first boyfriend/girlfriend.

Multifactor Authentication / OATH OTP Client

The user will now need to update the MFA onto their phone using Google Authenticator. If the user does not have Google Authentication, have them download this from the appropriate app store on their phone.

1. Click on Show QR Code next to OATH OTP Client.
2. A unique QR code will be displayed on the screen.
3. Have the user open Google Authenticator and add a new authentication.
4. Scan the barcode – Tip if it is not scanning try zooming in the screen by pressing Control and the + symbol.
5. The user will now have a code on their phone.
6. Enter this into the box in Practice Protect.
7. The phone is now linked to the users Practice Protect Portal.

Deleting users MFA on initial setup phone

Now that the user has successfully been set up on Practice Protect you are able to delete the MFA that you set up originally to login to their portal. Open your Google Authenticator and delete the appropriate users MFA.

At Clarity Street, we help accounting firms transform their frustrations into best practice.

Want to know more about how we can help?

Book a meeting with us here.