CREDAS
A SmartSearch Company

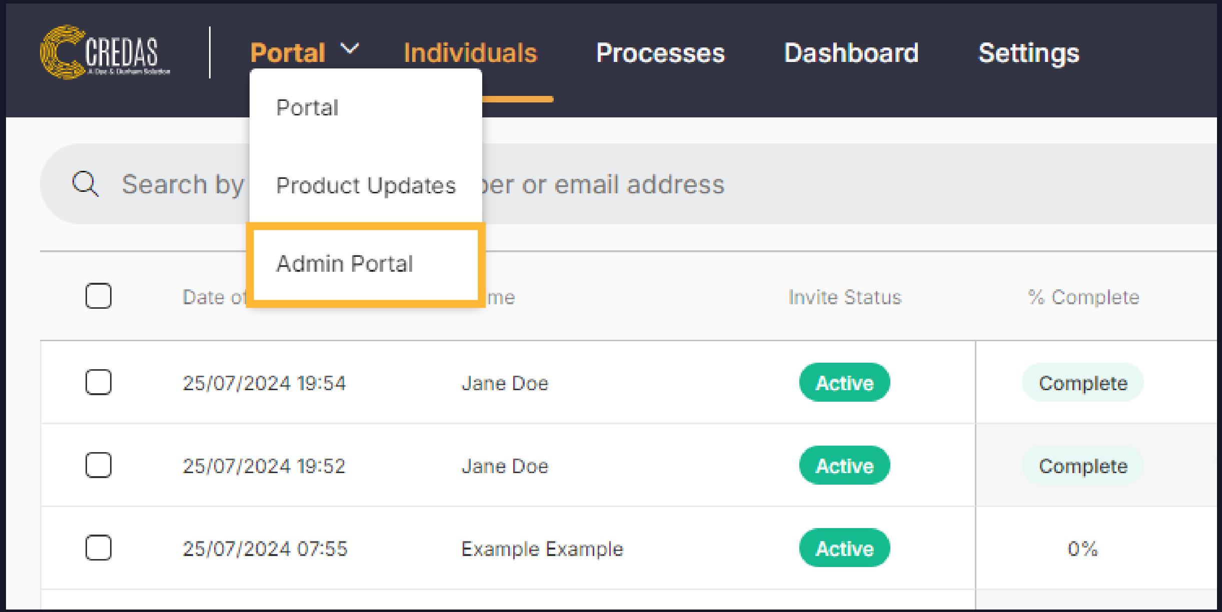
MANAGING USERS

How to manage your users on Credas via the Admin Portal

INTRODUCTION

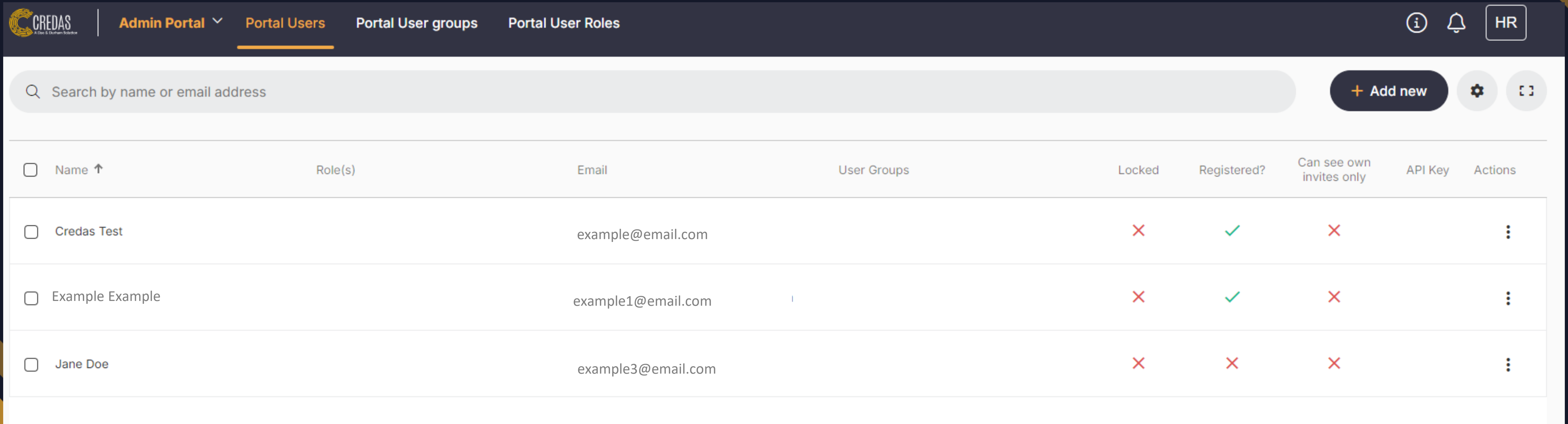
You can manage your users directly within your Credas portal via the Admin Portal. This includes adding new users, managing notifications, and assigning permissions. This guide covers:

ACCESSING THE ADMIN PORTAL



- To access the Admin Portal, click ‘Portal’ on the left-hand side of the header within your portal.
- Click ‘Admin Portal’ to then be taken to the admin portal.
- If you do not have access to the Admin Portal, please reach out to your portal admin or manager who can review your permissions.

THE ADMIN PORTAL



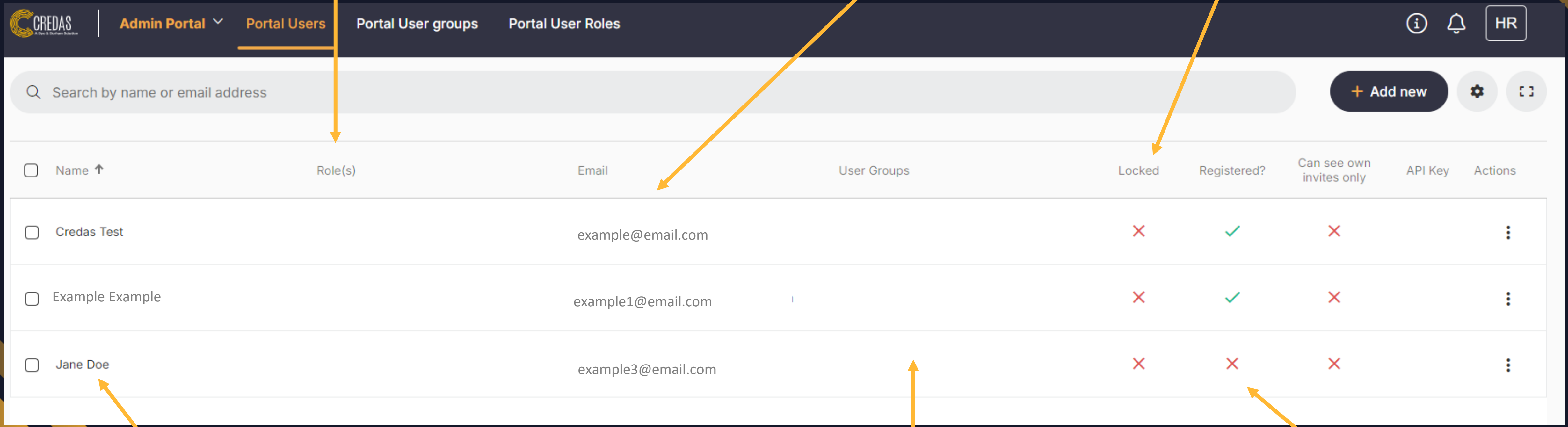
- The Admin Portal will list out any users who currently have access to your portal.

THE ADMIN PORTAL

If a *user role* has been assigned, it will appear here.

The email associated with the user will appear here.

If a user has been locked (suspended) from the portal, a tick will appear here.

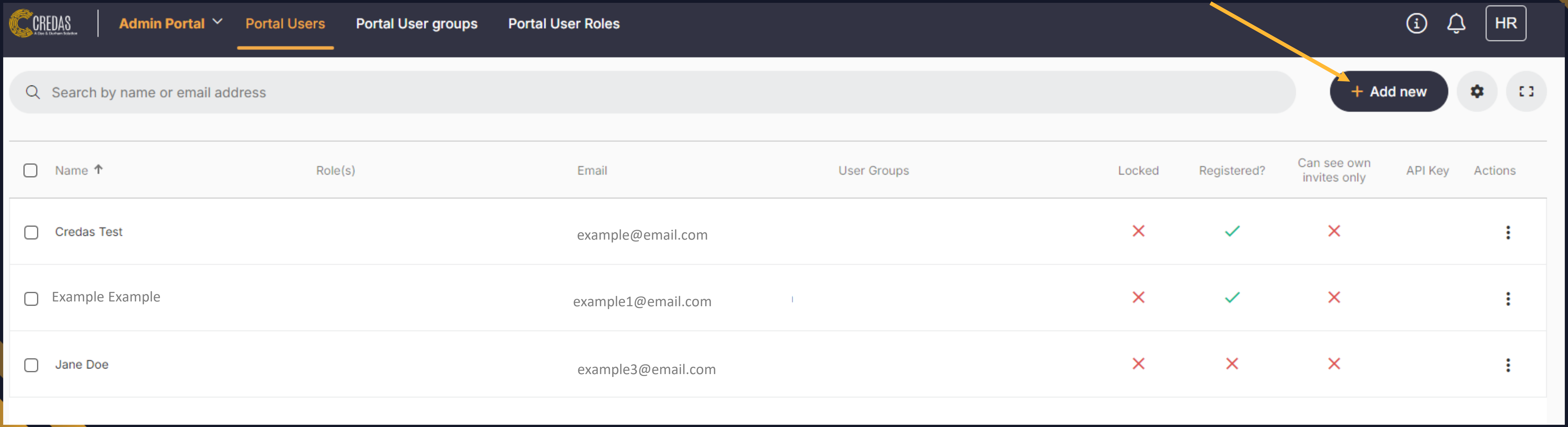


Their name will appear here.

If *user groups* have been assigned, they will appear here.

You can see if a user has registered on the portal here. If the user is unregistered, this means that they have not logged into the portal.

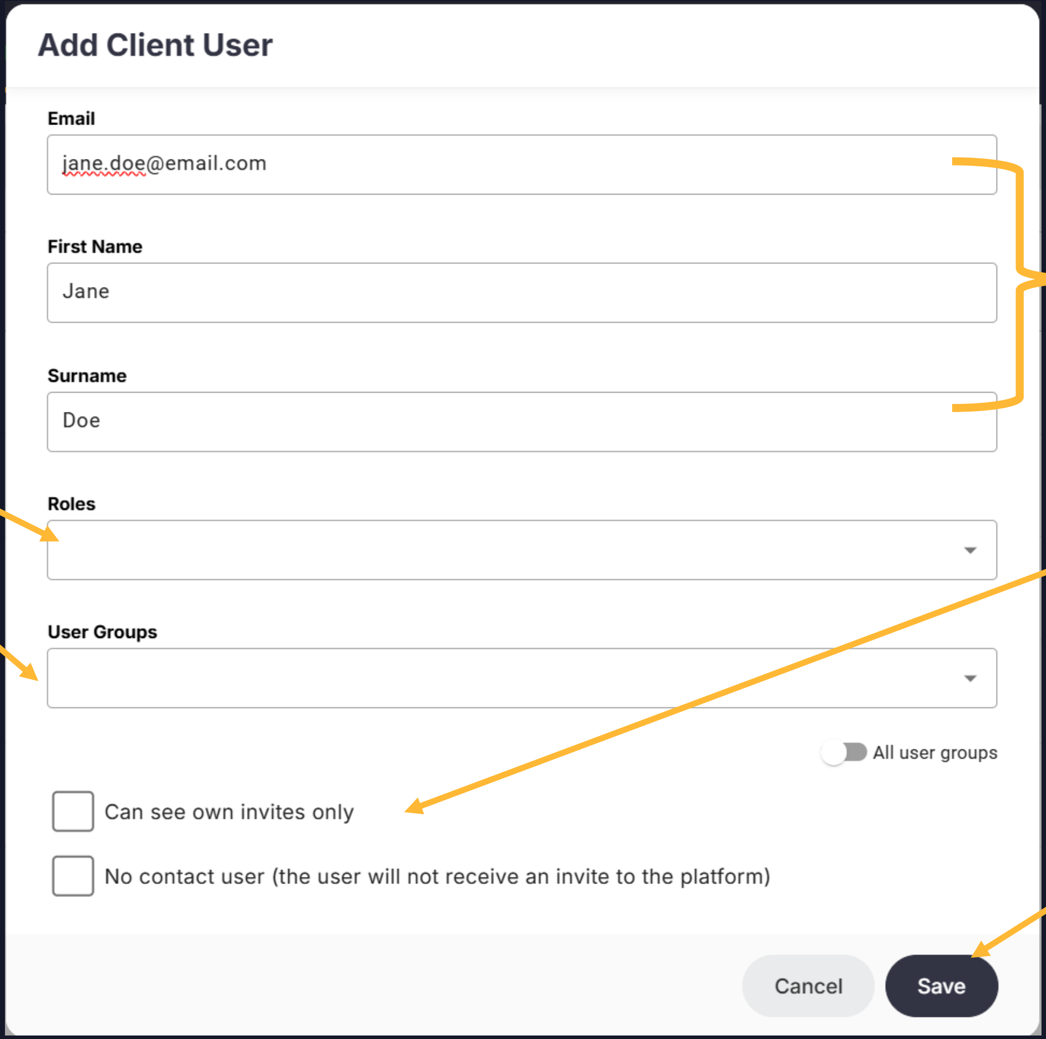
ADDING A NEW USER



- You can add new users to your portal by clicking ‘Add new’ within the Admin Portal.
- Please note, once a new user has been added, they will have 24 hours to register to your Credas portal. If they do not register within 24 hours, you will have to resend their invitation.

ADDING A NEW USER

If *user roles & groups* have been set up, you can assign them here.



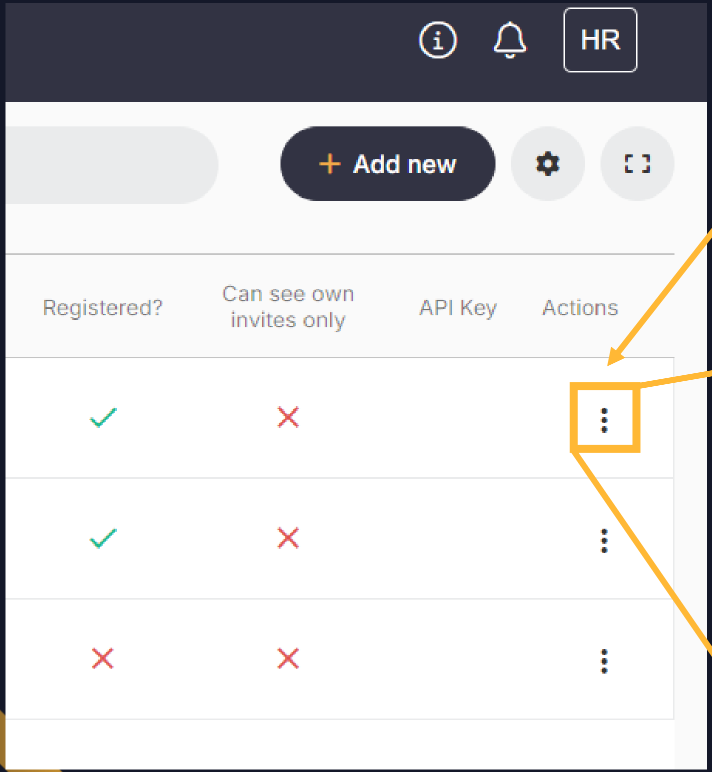
You will need to input the email, first and last name of the new user.

If you would like the user to only see the invitations they have created, you can tick the box here.

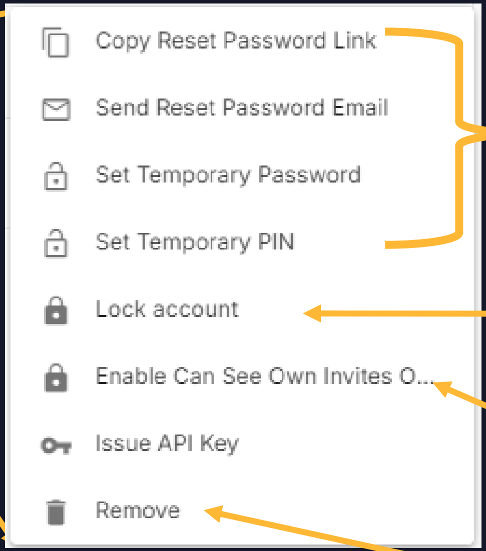
Don't forget to click 'Save'!

MANAGING EXISTING USERS

MANAGING EXISTING USERS



You can manage a user by clicking the actions button here. It will bring up the below menu.



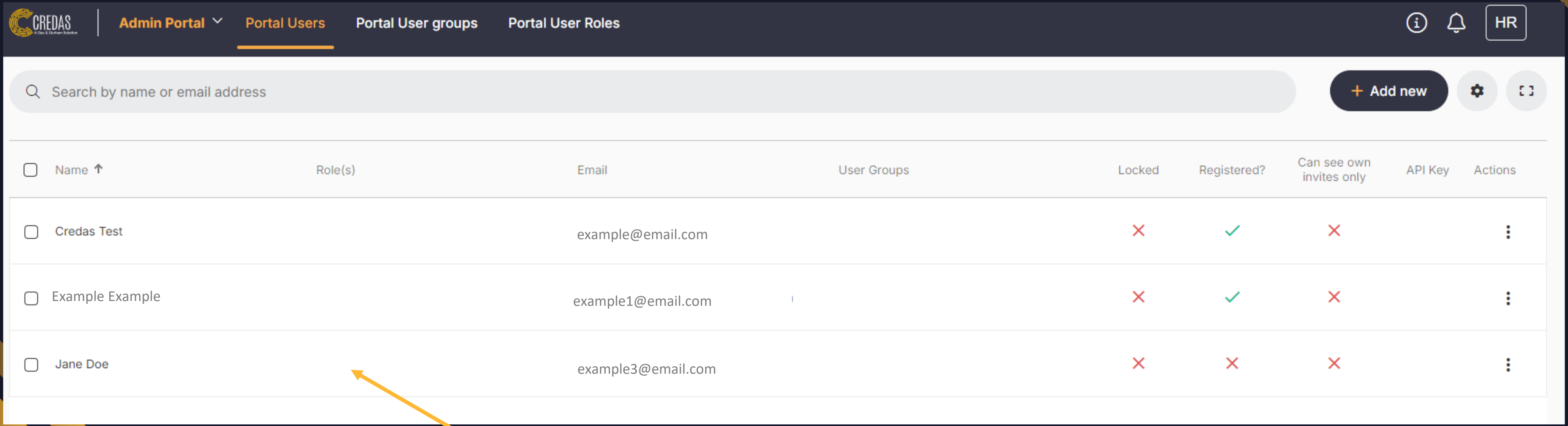
You can reset an account by either sending a password reset email/link or setting up temporary credentials for them.

You can lock/unlock (suspend) access to the portal here.

You can choose for a user to only see the invitations they have created on the portal here.

You can delete a user from your portal here.

MANAGING EXISTING USERS

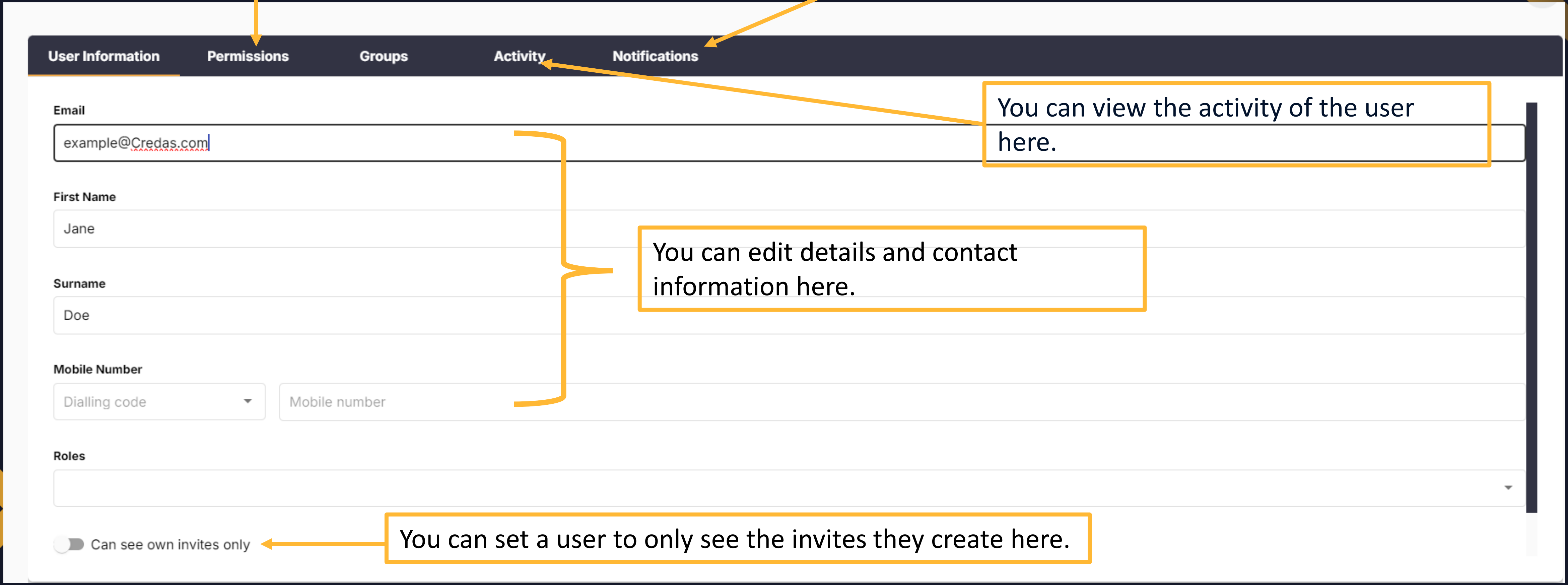


You can also manage permissions, information and notifications for a user by clicking into them.

MANAGING EXISTING USERS

You can manage *permissions* here.

You can access and set up *notifications* here.



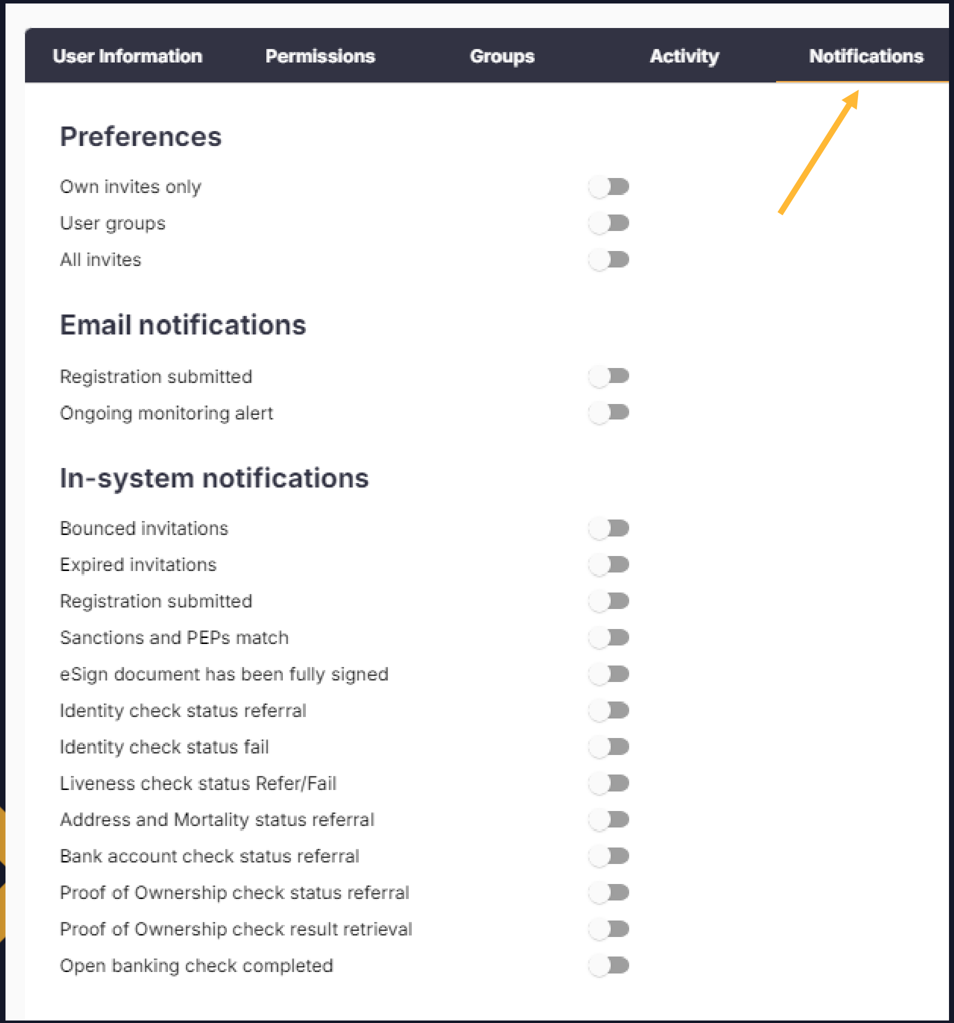
You can view the activity of the user here.

You can edit details and contact information here.

You can set a user to only see the invites they create here.

- Once you have clicked into a user profile, you will see the above screen. This is an overview of the user.

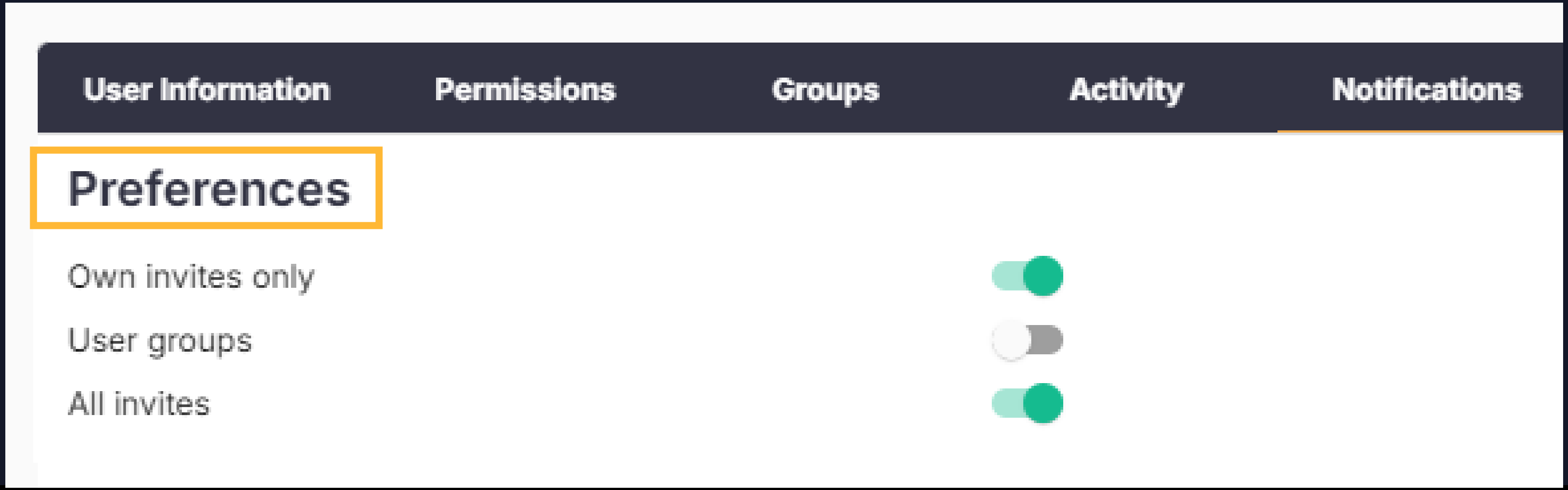
NOTIFICATIONS



- If you click into the notifications tab of a user, you will see we have a range of notifications that can be turned on.
- There are 3 main areas:
    - **Preferences** – These set the conditions for the notifications you will receive.
    - **Email Notifications** – These are notifications you can receive via email.
    - **In-system Notifications** – These are notifications you can receive via the notifications pane within the portal.

NOTIFICATIONS

- You will need to turn on notification preferences to receive the notifications.
- To receive notifications for your own invites, you will need to turn on ‘own invites only’.
- To receive notifications for all checks sent out via the portal, not including your own, you will need to also turn on ‘all invites’.
- To receive notifications for certain user groups, toggle on user groups and select the groups you wish to receive notifications for.
- The example preferences set below will see the user receive notifications for both their own checks **AND** notifications for all checks sent out within the portal.



CREDAS
A SmartSearch Company

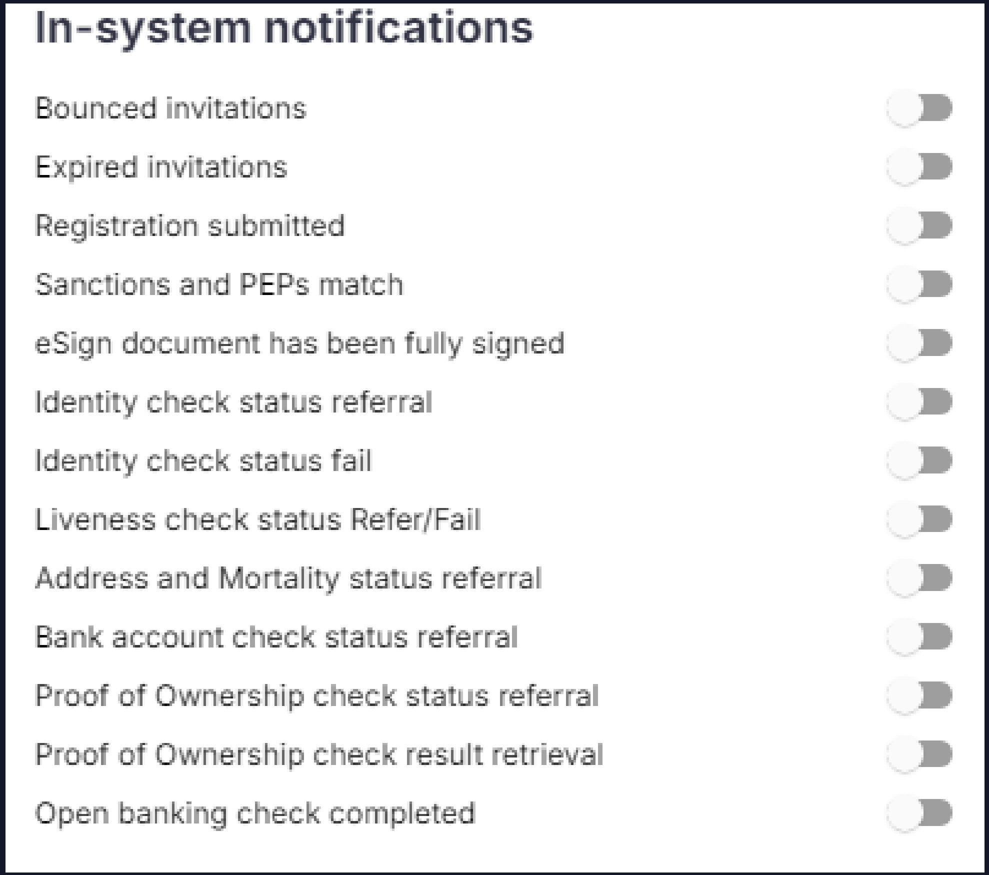
NOTIFICATIONS

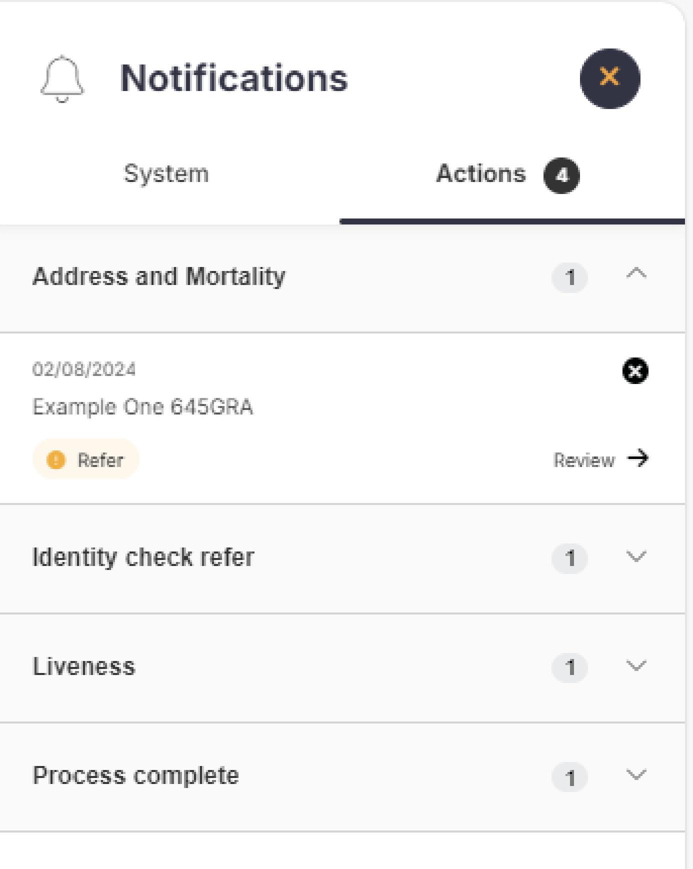
You have two email notifications you can turn on:

- **Registration Submitted** – This email alert will let you know when an individual has completed a journey.
- **Ongoing Monitoring alert** – This email alert will let you know if there has been any changes to an individuals Peps & Sanctions results during the period you have set up for ongoing monitoring. We highly recommend, if you are using ongoing monitoring, having this notification turned on for at least one person in your organisation. For more information on ongoing monitoring, please click *here*.

NOTIFICATIONS

- We have a range of in-system notifications that you can turn on.
- They will appear in your notification panel as below:





USER GROUPS, PERMISSONS & ROLES

USER GROUPS, ROLES & PERMISSONS

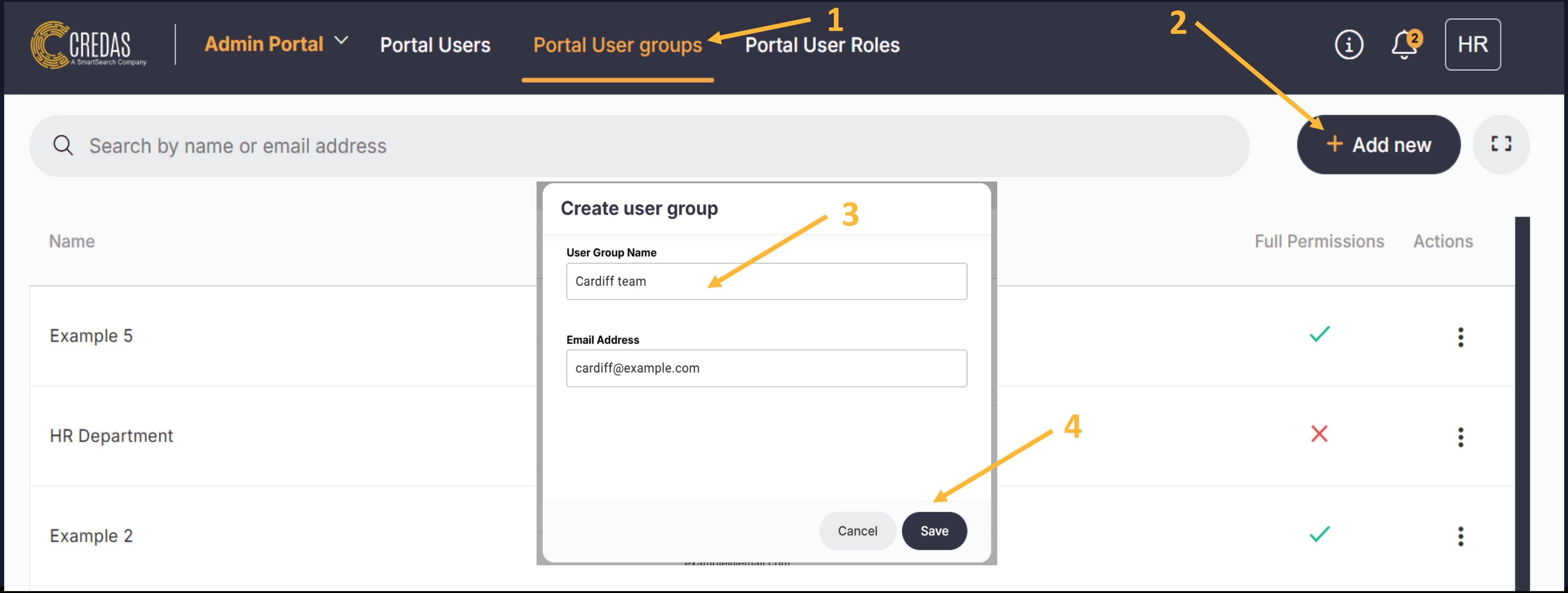
User Groups	User Roles	User Permissions
• User groups can be used to group a set of individuals, for example a set of users from the same branch or team. • Users in a user group will only be able to see invitations and checks sent from that user group.	• User roles can be used to set up permissions for different users depending on their ‘role’, and the level of access you wish for them to have.	• We have a selection of permissions that you can assign to users. • Permissions can be set at an individual, user group or user role level. • We recommend setting up permissions via user roles.

USER GROUPS

- User groups can be used to group a set of users where you wish to limit visibility of checks between groups, for example a set of users from the same branch or team.
- Users in a user group will only be able to see invitations and checks sent from that user group.
- Users not set up in a user group will be able to see all invitations and checks sent within the portal, including those sent from within a user group.
- If you are setting up multiple user groups, we advise to leave at least one person outside of a user group who can view all checks for emergency cases.
- Users can be assigned to multiple user groups.
- Once an invitation has been sent outside of a user group, it will not follow any subsequent changes to that user's group membership. Therefore, if the user who issued the check is later moved into a user group, the original invitation may no longer be visible to them.
- If you have any concerns regarding user visibility or access, please contact our Support team who will be happy to assist.

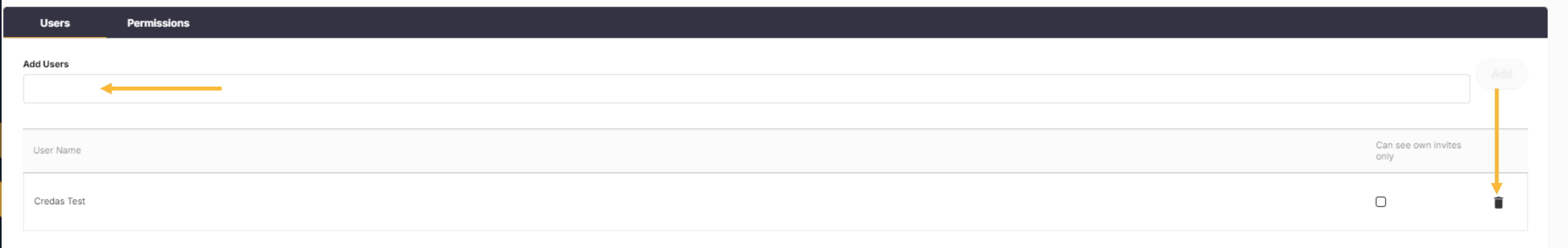
USER GROUPS

- To set up a user group, click on ‘Portal User groups’ within the Admin Portal header.
- After this, select ‘Add new’ on the right-hand side of the portal.
- A new screen will open called ‘Create user group’. Simply enter the ‘User Group Name’ and an email address.
- If you are happy with the information entered, click ‘Save’.



USER GROUPS

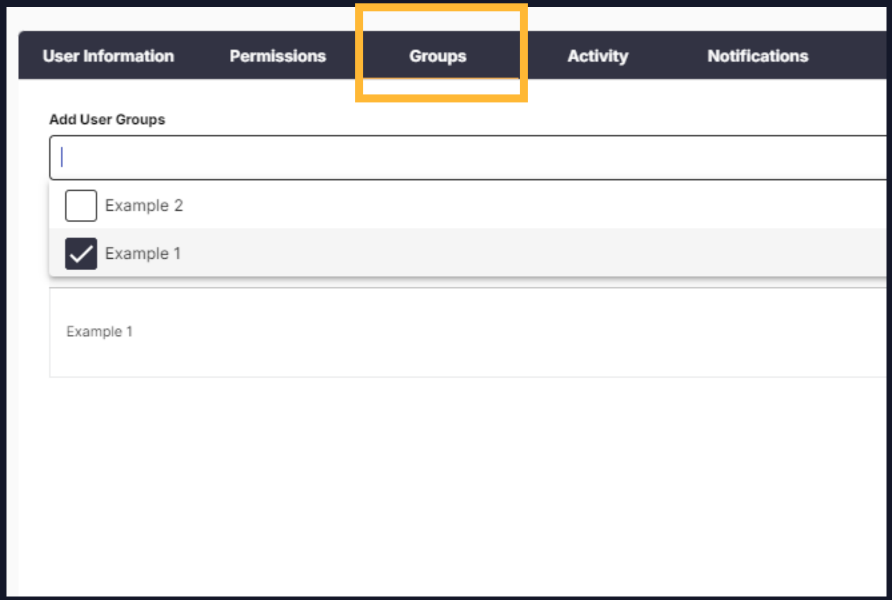
- Once the user groups have been created, these will be visible within the 'Portal User groups' tab.
- To add a new user to a group, click into the user group in question.
- Search for the user(s) you wish to add within the 'Add Users' search bar.
- You can also delete users here by clicking the bin icon.



USER GROUPS

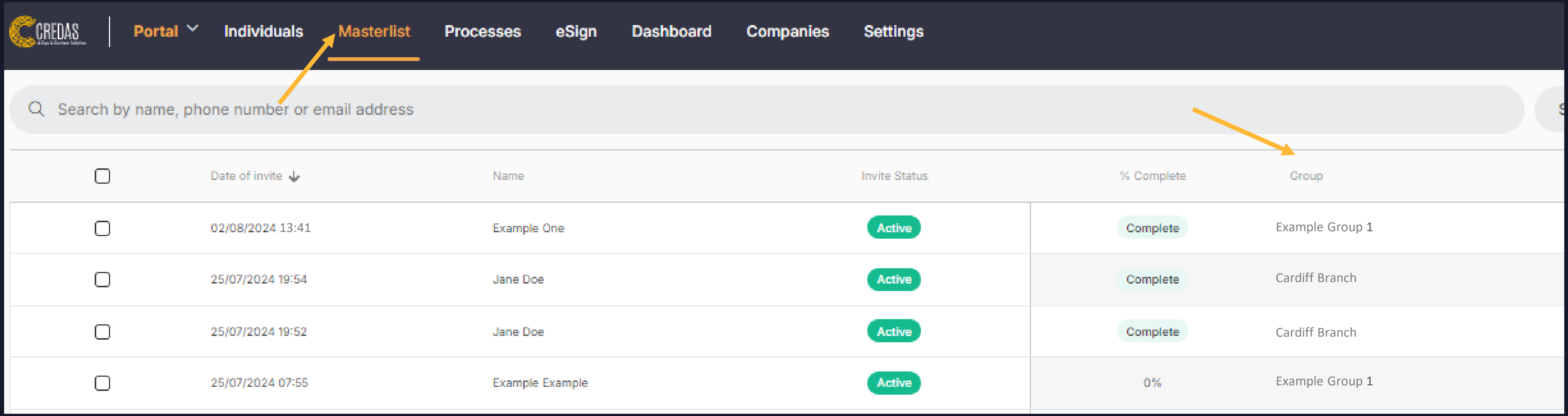
- Search for the user(s) you wish to add within the ‘Add Users’ tab.
- You can also remove users from a group by clicking the bin icon.

USER GROUPS



- Alternatively, you can add user groups to an individual user by going into the user *profile*.
- Click into the ‘Groups’ tab where you can add the user into user groups and view which groups they are currently assigned too.

MASTERLIST FOR USER GROUPS



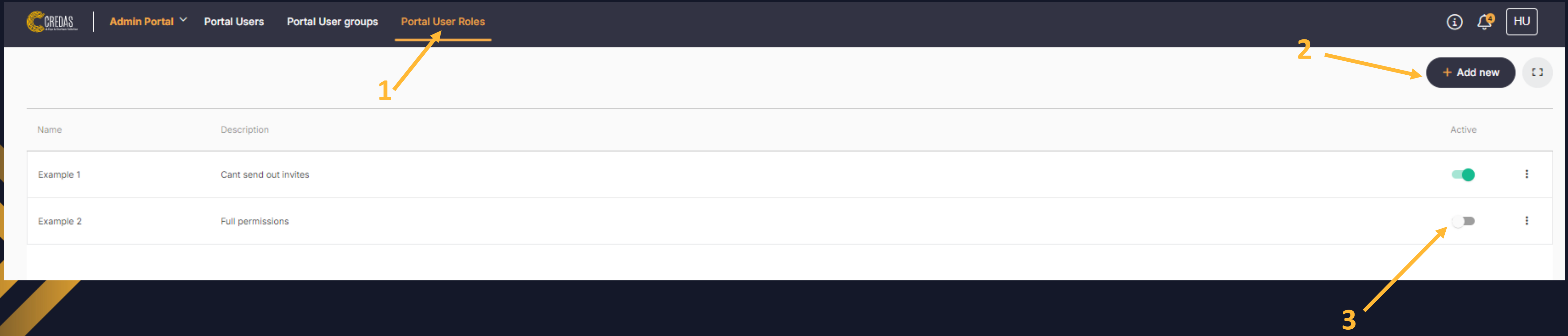
- If you or your users are set up in multiple user groups, we have a *masterlist* feature that allows you to view individuals that have been created from all the user groups assigned to the user.
- The user group the individual was created in will also appear in the table, as can be seen above.
- Please contact our support team if you wish to enable the masterlist function.

USER ROLES

- User roles can be used to set up permissions for different users depending on their ‘role’ and the level of access you wish for them to have.
- Instead of assigning these permissions manually for every individual user, you can create a user role to change the permissions of a group of people.
- For example, you may want your standard users to be able to send out invites and download PDFs but not be able to remediate checks.
- A user should only be assigned one user role, if a user is assigned to multiple user roles, the permissions will conflict with each other, and the user will have the lowest user role permissions.
- User roles can be used in conjunction with user groups. For example, you may have multiple user groups, and within those user groups you have users with different user roles applied.

USER ROLES

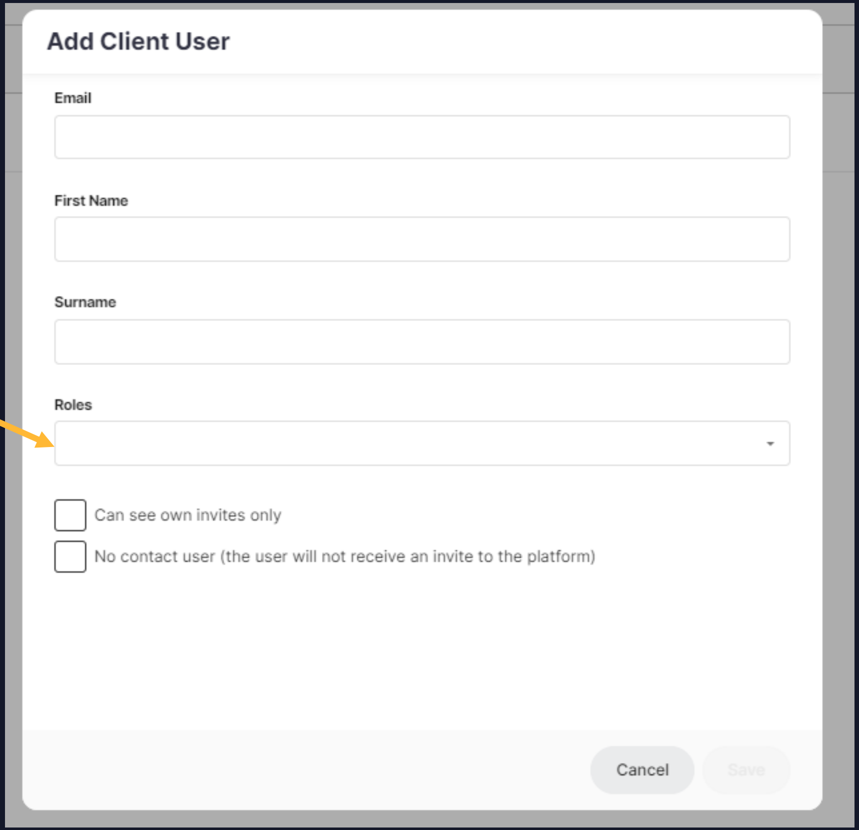
- To set up a user role, click on ‘Portal User Roles’, found within the Admin Portal header.
- Click the ‘Add new’ button.
- You will be asked to give a name and description to the user role as well as assigning *permissions*. We recommend detailing within the description the permissions assigned.
- Once set up, you will need to turn the user role active.



USER ROLES

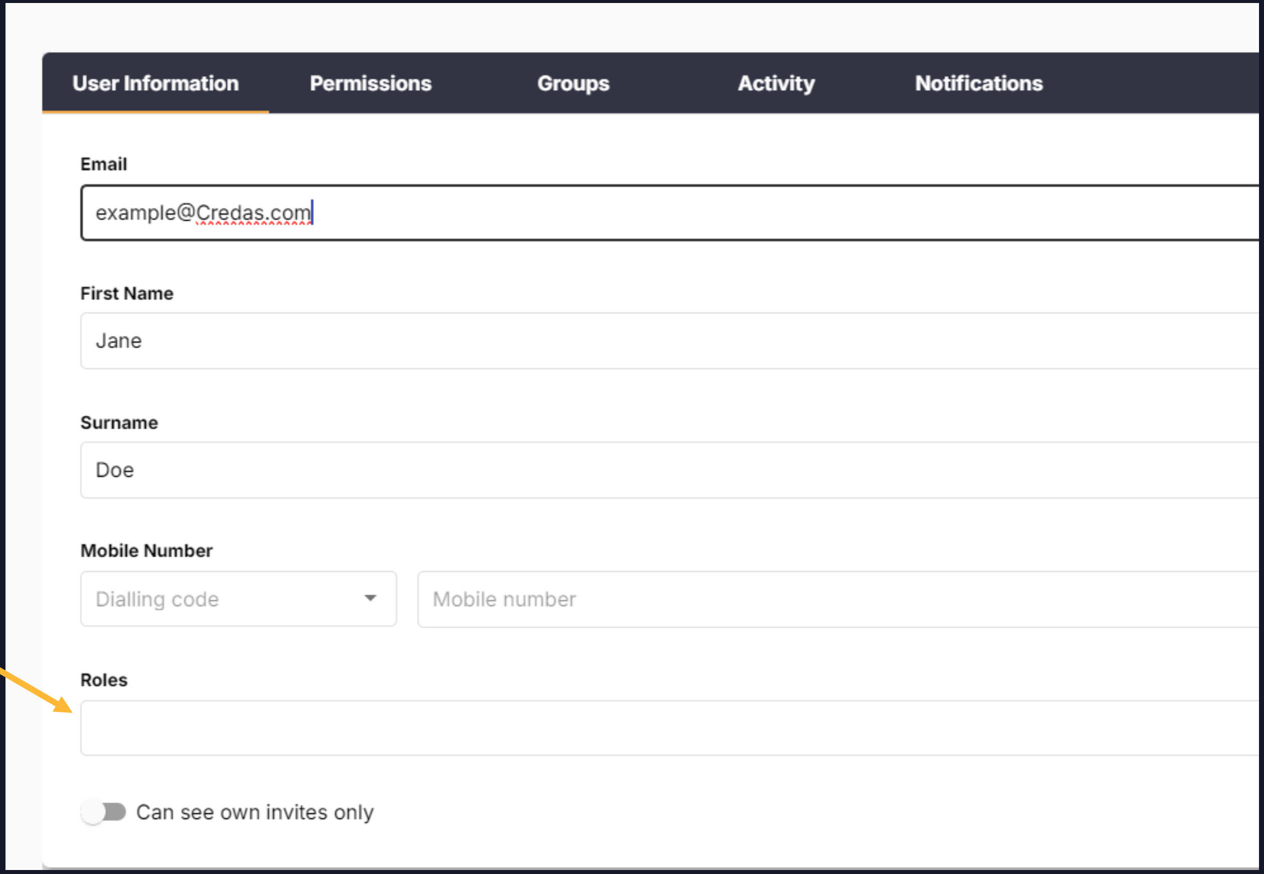
- You can assign a user role when you are creating a new user as can be seen below.

You can assign a user role here



USER ROLES

- Alternatively, you can apply user roles to existing users by going into the user *profile* and adding a role.



You can assign a user role here

USER PERMISSONS

- We have a selection of permissions that you can use to alter the level of access for a user within Credas.
- Permissions can be set at an individual, *user group* or *user role* level.
- You should only configure permissions at one of these levels. If permissions are applied across multiple levels, the user will inherit the most restrictive permission set.
- We recommend setting up user permissions via user roles.
- The next few pages will walk you through the main permissions that can be altered.
- For a full list of up-to-date permissions, please click *here*.

USER PERMISSONS

Allows a user to add new individuals.

Portal	Connect Portal
Individuals	Allows the user to see the list of Processes for the Client
Entities Admin	Allows the user to create Entities
Invite entities to processes	Allows the user to invite entities to a process
Create Entity Folders	Allows the user to create folders for entities
Add Entities to Folders	Allows the user to add entities to folders
Allow Auto-refresh on Entity List	Allows the user to turn on auto-refresh on the Entities list
Allow Export to CSV	Allows the user to export Entities to CSV
Edit entity user details	Allows the user to edit entity user's details
Delete Entities	Allows the user to delete entities
Add Data Checks for Entities	Allows the user to add data checks to entities
Add Entity Notes	Allows the user to add notes to entities

Allows a user to issue a journey to an individual.

Allows a user to manage *folders*.

Allows a user to edit an individual's details, such as their name.

Allows a user to *delete* individuals.

Allows a user to add *notes* to an individual's profile.

Allows a user to run *data checks* such as Proof of Ownership or one-off manual Address checks.

USER PERMISSONS

Allows a user to manage *tags.*

Add Entity Tags	Allows the user to create tags for entities
Add Tags to Entities	Allows the user to add tags to entities
Entity Milestones	Allows the user to view entity milestones
View Entity Processes	Allows the user to view entity processes
View Entity Identity Checks	Allows the user to view entity identity checks
View Entity Documents	Allows the user to view entity documents
View Entity Notes	Allows the user to view entity notes
View Entity PDF Exports	Allows the user to view entity PDF exports
Entity Evidence	Allows the user to view and add entity evidence
Entity PDF Export	Allows the user to export an entity to a PDF document
Processes	Allows the user to see the list of Processes for the Client
Create Processes	Allows the user to create Processes

Allows a user to view the relevant areas on an individuals profile.

Allows a user to view and add *evidence* to an individual's profile.

Allows a user to export PDFs.

Allows a user *to issue a journey* to an individual.

USER PERMISSONS

Dashboard	Allows the user to view the Dashboard
Update status of a check	Allows the user to update the status of a check
Liveness	Allows the user to update the status of a Liveness check
ID Document	Allows the user to update the status of an ID Document check
Standard check	Allows the user to update the status of a Standard check
International Sanctions and PEPs	Allows the user to update the status of a Sanctions and PEPs check
Credas AML Protection Pack	Users can update the status of the Credas AML Protection Pack report and its sections.
Companies	Allows the user to create and manage companies
Settings	Allows users to manage portal settings

- *Dashboard* – Allows a user to access the dashboard tab.
- *Companies* – Allows a user to access our KYB solution.
- *Update status of a check* – Allows a user to manually update the status of a check.
- *Settings* – Allows a user to access the portal settings tab.

USER PERMISSONS

Permission	Description
☑ Admin Portal	Connect system administration (super user)
☑ Portal Users	User can administer users
☑ Create Users	Allows the user to create users
☑ Copy reset password links	Allows the user to copy reset password links
☑ Send reset password emails	Allows the user to send reset password emails
☑ Allow setting tempory passwords	Allows the user to set temporary passwords
☑ Remove Users	Allows the user to remove users
☑ Edit users	Allows the user to edit users
☑ Portal User groups	User can administer user groups within a client
☑ Remove user groups	Allows the user to remove user groups
☑ Create user groups	Allows the user to create user groups
☑ Portal User Roles	

- These permissions relate to the admin portal.
- If you do not want a user to access any parts of the admin portal, turn off the top ‘Admin Portal’ permission.
- The portal user groups permissions are linked to creating and managing user groups.
- The portal user role permissions are linked to creating and managing user roles.

USER PERMISSONS

Legislation	Allows users to administer legislations
Digital Identity Trust Framework	Allows users to activate DITF profiles
Right to Work (RTW)	Allows users to activate the Right to Work card on the Identity checks table cards
Right to Rent (RTR)	Allows users to activate the Right to Rent card on the Identity checks table cards
Safe Harbour	Allows users to activate the Safe Harbour card on the Identity checks table cards
Proof of Ownership	Allows users to activate the Proof of Ownership card on the Identity checks table cards

- The legislation permissions allow a user to administer Digital Identity Trust Framework, Right to Work, Right to Rent, Safe Harbour and Proof of Ownerships checks
- You will only see the relevant legislations to your portal, for example if you do not have safe harbour journeys, you will not be able to see the Safe Harbour permission.

SUPPORT

Log a Support Ticket here

Call us on 029 2010 2555

View our Knowledge Base here