Ciphr HR Sign-In Update actions

May 2025 | V1.4

Ciphr Limited
3rd Floor, 33 Blagrave Street, Reading, RG1 1PW | +44 (0)1628 814000 | info@ciphr.com | ciphr.com

Index

Ciphr Sign-In update actions

Introduction

Get ready to experience the latest update from Ciphr!

We're excited that you will soon have access to our newest release and all the benefits that come along with it:

- **A modernised user interface** with a fresh, intuitive look
- **Standardised navigation** for a consistent, smoother platform experience
- **A version switcher** lets you toggle between old and new interfaces for a seamless transition, minimising disruption
- **Action-oriented menus** improve efficiency, helping users get more done faster
- **Self-serve branding** lets you control your software's appearance without our support
- **Improved two-factor authentication (2FA)** setup and user experience
- **New sign-in** and email-based login for a streamlined, user-friendly experience
- **Self-service single sign-on (SSO) configuration** with third-party providers like Microsoft and Google
- **In-app guidance** provides real-time support to end users and admins, improving efficiency for all

Note: the new version will only be visible to end users when you choose to enable it: you're in complete control of when and how it's introduced.

Click here for a preview of the new features in action.

Ciphr Sign-In update actions

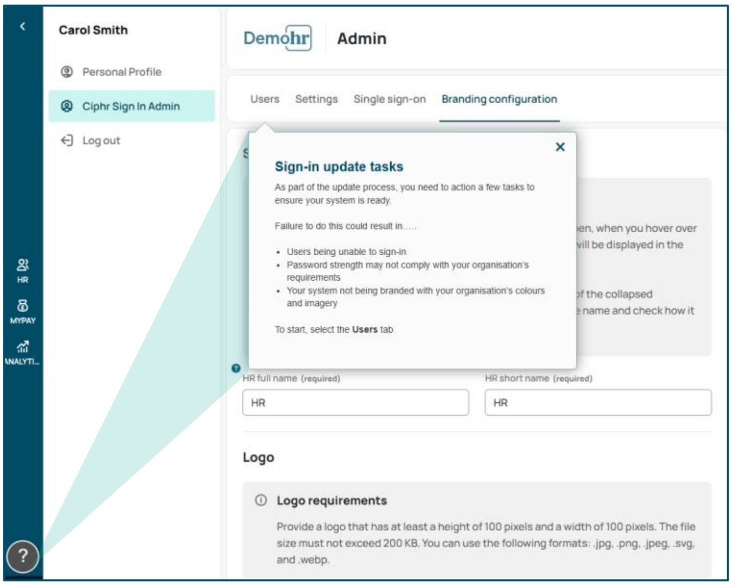
Preparation

You'll soon gain access to our new Sign-In app; our new centralised user management area where you will be able to easily control and manage user access in one place. While it's *not yet linked* to your live system, there are **five** important steps you'll need to complete before we update your HR system to the latest version:

1. **Settings configuration**: review and adjust settings such as password policies, two-factor authentication, and system timeouts
2. **SSO setup** (if applicable): configure and test SSO to ensure seamless access for your users after the update
3. **Branding**: customise the branding of your system to align with your organisation's identity, such as sign-in image, logo and colour scheme
4. **User email review**: check in your HR system to ensure all users who need to access the system have a unique email address
5. **IP Address** (if applicable): add new IP address to your Allow-list

This guide walks you through the steps you need to complete to ensure you're ready.

Once you have access, our new in-app guidance will also walk you through the necessary actions step-by-step and is always available by clicking the help icon whenever you need it:



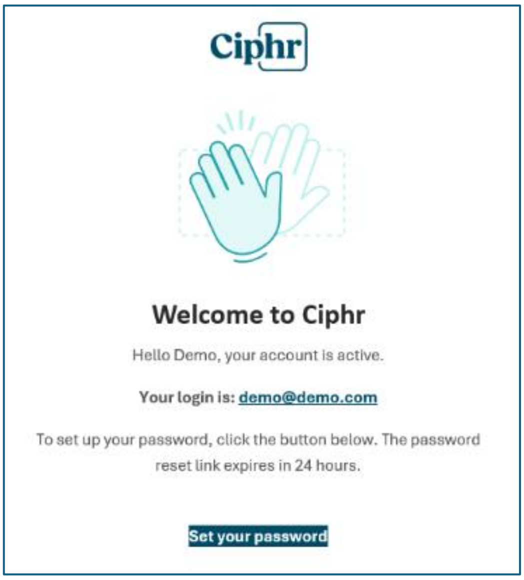
We anticipate the tasks will take two hours on average, to be completed by an HR system administrator, with support from an IT technical colleague to review the SSO and Marketing colleague for Branding configuration. You may wish to allow more time depending on the amount of email data you need to check.

Click here for an overview video of what to expect when completing your tasks in Sign-In.

Ciphr Sign-In update actions

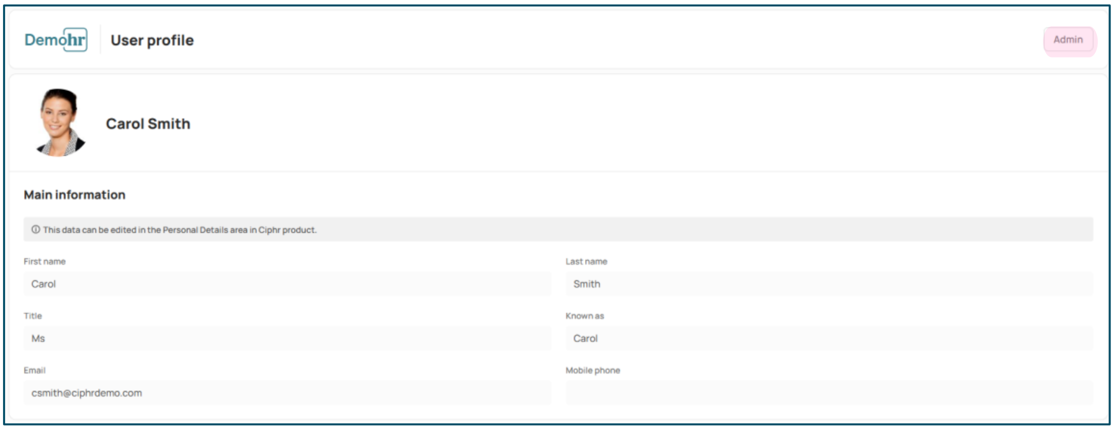
Getting started

1. Firstly, HR system admins will receive a system generated email notifying them that their account has been activated. Simply click the "**Set your password**" link in the email, follow the steps to set up your password, and configure your 2FA settings to gain access to the system.



2. Once logged in, you'll have access to your new Sign-In application.

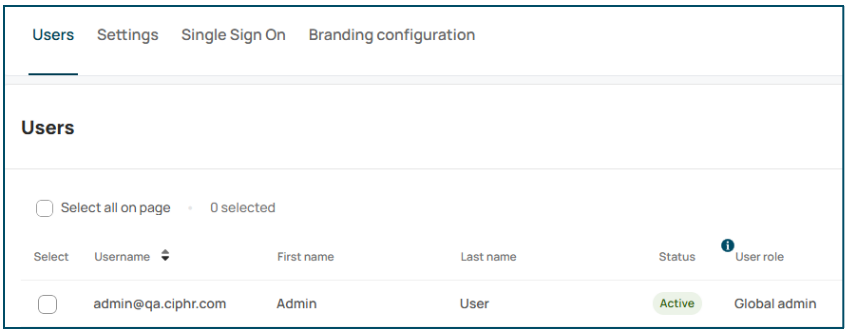
3. Start by clicking **"Admin"** in the top-right corner of your profile page, or open the left-hand burger menu and select **Ciphr Sign-In Admin**.



Ciphr Sign-In update actions

Users

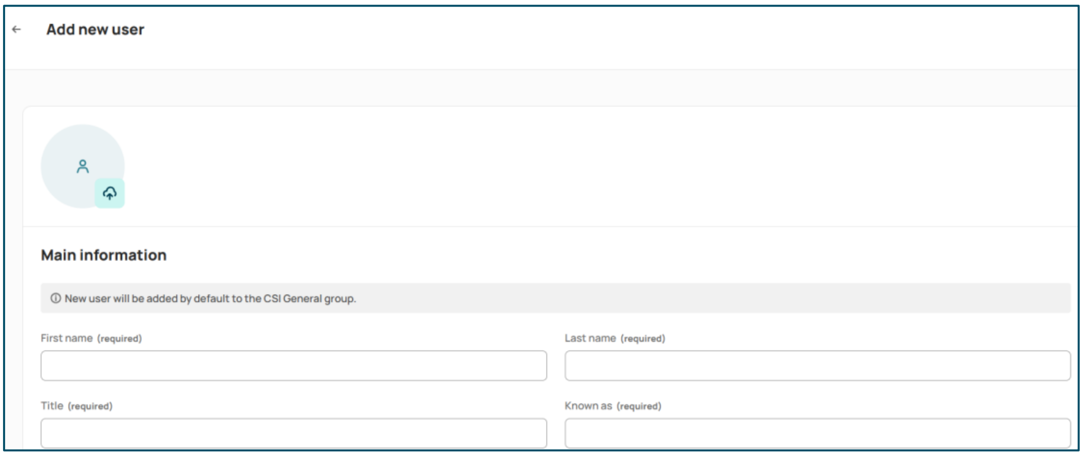
The **Users** tab displays all individuals who have access and can sign in to the system. HR system admins have been synced to Sign-In and granted admin access to complete the pre-update tasks.



Adding a new user

If you need to add other users to assist with your actions, such as an IT colleague, follow these steps:

1. Select **Add New User**, complete the required information, and click **Create User**.



2. Within a few minutes, the user will receive an account activation email with a link to set their password and access the system.

   Once the user is created, you'll need to change their sign-in user role:

   1. Select **Actions** > **Change User Role**.
   2. Change the role from **Employee** to **Global Admin**.

They will now have admin access to the sign-in admin panel and can assist with pre-update tasks.

Ciphr Sign-In update actions

Deleting a user

If there are system administrators in the user list who won't be involved in the update actions and you wish to remove them, you can delete in two ways:

- **Individually** by selecting **Actions > Delete** to the right of the record
- **In bulk** using the multi-select tick boxes in the left hand column. Ticking boxes will enable the bulk ⋮ Actions button at the top of the right column, then select **Delete User** to remove all selected users

Settings

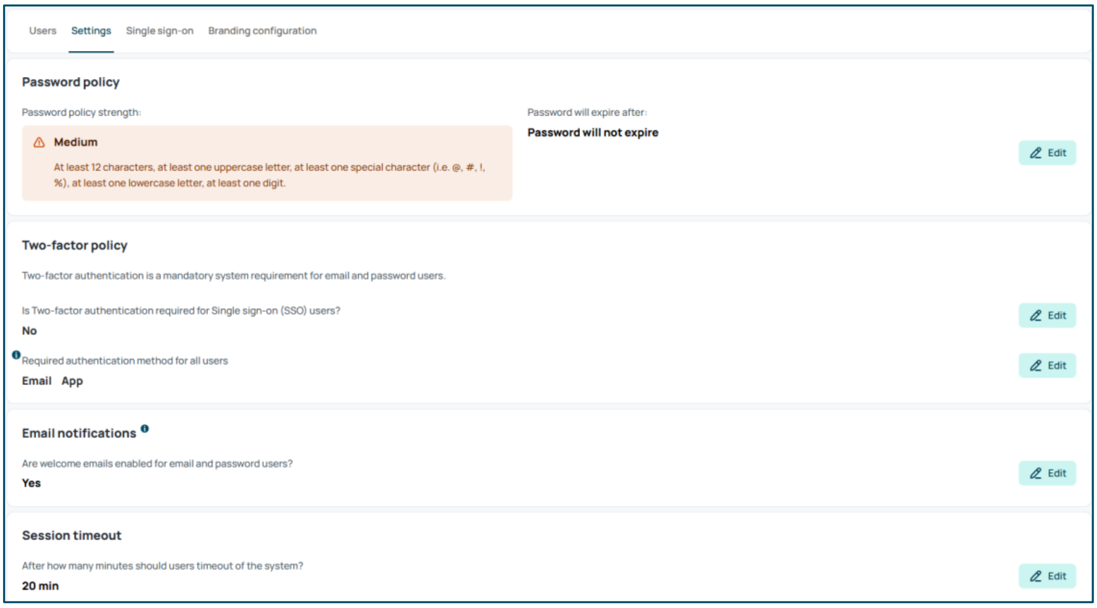
1. Click **Settings** to review and update your preferences as needed by selecting the **Edit** button to the right of each section.

   On this screen, you can configure:

   - Password policy strength
   - Password expiration period
   - 2FA settings – select which 2FA method(s) from email, authentication app or SMS you want your users to be able to use.
   - Whether to send an account activation email to users when they are set up
   - System timeout period – defaulted to 20 minutes but can be changed to a maximum of 480 minutes (8 hours)

Note: If **welcome emails** are enabled, users who need to sign in with a password will receive an account activation email when we sync your users. They will follow the same activation process you did to access the system.

Users who sign in with SSO will **not** receive a welcome email.



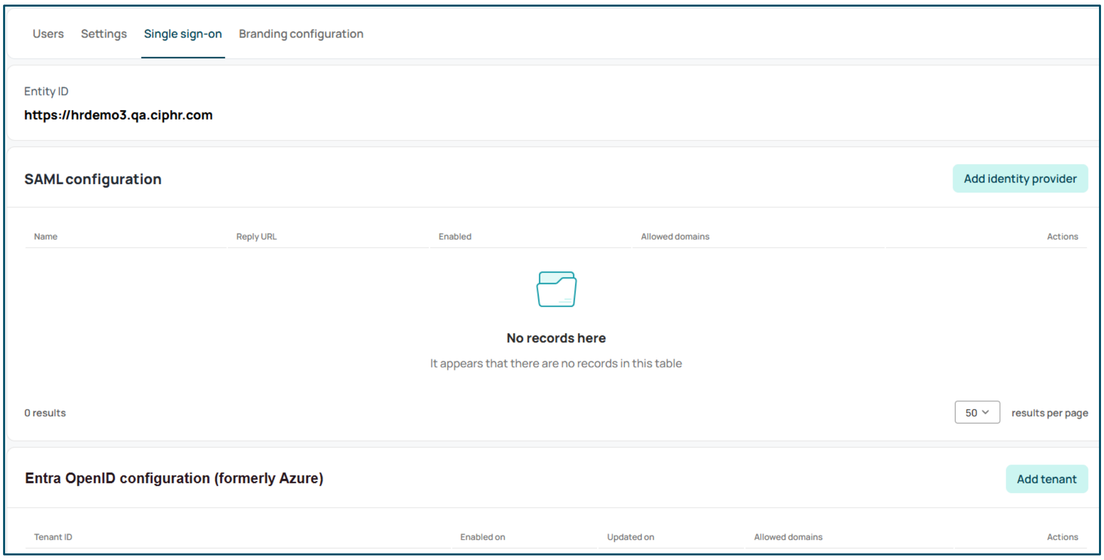
Once you're satisfied with your settings, proceed to the **Single Sign-On** tab.

Ciphr Sign-In update actions

Single sign-on

Important! If SSO is enabled in your live system, it's *essential* to complete this step to ensure your users can successfully sign in after the update.

1. If you don't use SSO, you can skip this step, alternatively, now that it is easy to configure SSO you may wish to choose to do so, if so follow the below steps otherwise, select your identity provider on the screen.



2. If you use Security Assertion Markup Language (**SAML)**, go to the **SAML Configuration** section and click **Add Identity Provider** to complete the details. If you use **Entra OpenID (formerly Azure)**, you can skip this step.

   For full guidance on SAML Configuration view our guide.

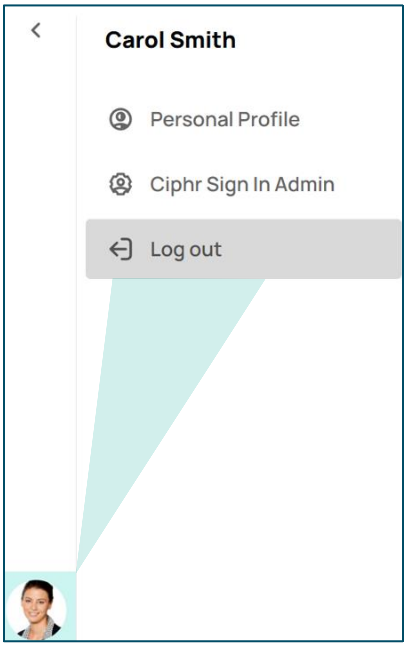
3. If you use **Entra OpenID (formerly Azure)**, go to the **Entra OpenID configuration** section.

   For full guidance on Entra OpenID (Azure) Configuration view our guide.

Ciphr Sign-In update actions

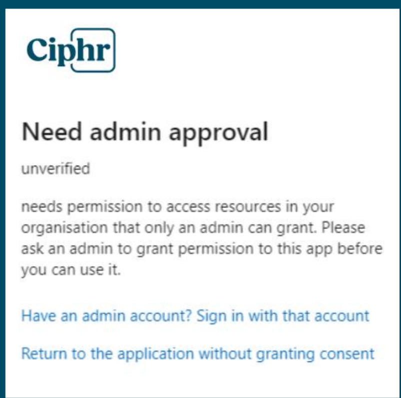
4. Once you’ve configured your Single sign-on (SSO) settings, you're ready to test:

    1. Sign out by clicking your **profile** in the bottom left and selecting **Log out**.



    2. Sign back in using **SSO**. The system will identify that you are signing in with a domain requiring SSO and will prompt you to follow your organisation’s authentication process.

Note: Depending on your Azure setup, an Azure system administrator may need to sign in and approve before you can sign in with SSO.

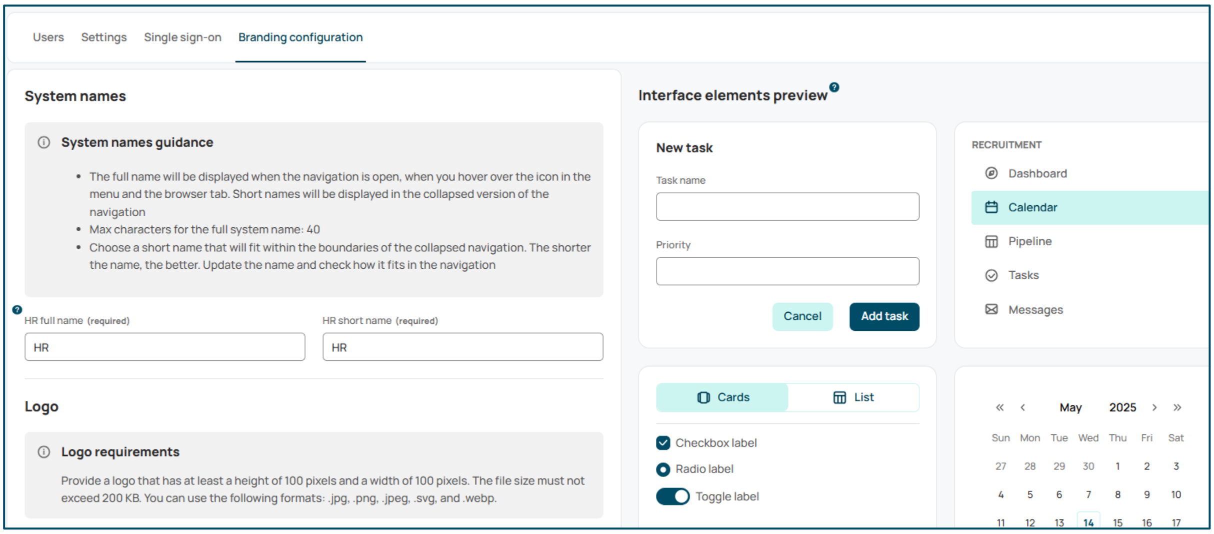


Once you have successfully signed in using SSO, this step is complete.

Ciphr Sign-In update actions

Branding configuration

1. The final task in this area is to set up your branding. Click on the **Branding configuration** tab and follow the steps listed on the left-hand side of the page to:
    - Assign a name to your system (this will appear in the new interface navigation after your update)
    - Upload your company logo
    - Upload a favicon (the small icon that represents your system in the browser tab)
    - Select a colour scheme that aligns with your company branding
    - Choose a font
    - Add a sign-in screen image



Note: Completing the **Branding** step is *essential*. While users won't immediately see the new user interface after your update (as you will need to grant them access to view the version switcher when you're ready), they will see the new customised sign-in screen.

Additionally, emails generated from the new sign-in application, such as 'Account Activated', 'Email Two-Factor Code', and 'Reset Password' emails will feature your logo and company colour from the Branding Configuration, reinforcing your brand identity.

If you have **Multi Entity** configured then you'll be able to apply branding per Entity in the HR system after the update.

Ciphr Sign-In update actions

Active users check

1. Ciphr Sign-In has been designed to enhance security and simplify user access, and once connected to your HR system, it will sync all 'active' users so they can access your system. The criteria for an active account is:

    - A **unique contact/work email address** - this will serve as the user's sign-in credential, replacing the traditional username. Emails can be either a work or personal email address
    - Their **Enabled From** date is populated (this corresponds to the **Account Enabled From** field in Account Settings). Where dates are in the future, the account will be accessible from this date
    - Their **Enabled To** date is either blank or set for the future (this corresponds to the **Account Expiry** field in Account Settings)

    Note: Past leavers will *not* be included in the sync and we'll provide guidance at the appropriate time, on how you'll be able to sync them if they need access to the updated version.

2. To prepare for the update, the next step takes place in your *current* HR system, where you need to ensure that all users who currently sign in with a username and password, have a *unique* email address populated on their **Personal Details** record in HR.

    An email must be populated against either the **Contact Email Address** or **Work Email Address** field, depending on which email field your system uses as the default.

    Important! Ensuring this step is completed is *essential* for a smooth transition to the latest version. **Without an email address users will not be able to sign in to the system after the update**.

    Note: If you have **onboarders** accessing the system before their start date, please make sure the default email field (Contact/Work Email) contains a *personal* email address they can access. They'll need it to log in after the update.

> **Note:** Records with *duplicate* emails will not be able to be synced when the update is applied, so the user will not be able to sign in.
>
> Secondary (multi-post) records will not be affected.
>
> This could also apply if you have used your email address for any test records so please check and remove any duplicate emails before the update which can be replaced with a work or personal email address.
>
> Alternatively you could use plus addressing (also known as sub addressing) to create a unique email variation of your email for your test users, but it's recommended to check with your IT team if this is supported. Please click on the link below to learn more:
>
> https://learn.microsoft.com/en-us/exchange/recipients-in-exchange-online/plus-addressing-in-exchange-online

You can use the **Specialist Report > Data Validation Export** to check for blank or duplicate email addresses, and which accounts are active. Please see this guide for full details.

Ciphr Sign-In update actions

IP address filtering

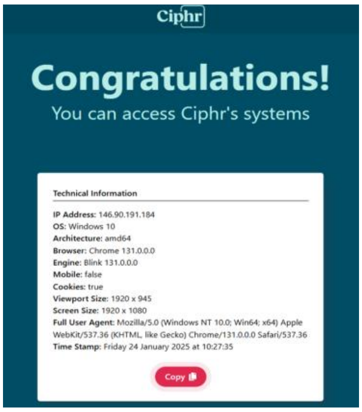
1. If your organisation uses IP address filtering, then your IT team will need to add some new IP addresses to your **Allow-list**.
2. **Why you need to make this change**

   Your organisation may restrict access to websites and as such will have previously allowed Ciphr IP addresses so that your users can access the system from within the company network.
3. **How you can check if your organisation uses IP filtering**

   If you are not sure if this is applicable to your organisation, please follow the link below to a webpage which resides under our new IP addresses:

   https://ipcheck.app.ciphr.com/

   If you can access this webpage, you'll see this message:



   If you can't access this webpage (it will not look like the image above), it's likely that your organisation uses IP filtering, and your IT team will need to add the new IP addresses.
4. **Adding IP addresses to your Allow-list**

   Add our new IP addresses listed below that we use to host our service, to your organisation's Allow-list:

   - 172.187.217.224
   - 20.77.3.86
5. After your IT team have added the new IP addresses, you should visit the above link again to check that you can access the webpage. This will confirm that once updated, you will be able to access your system.

Note: If you find that in-app guidance is not displaying properly then you may need to add some extra entries to the **Allow-list**. Click here for further guidance.

Next steps

Once all the actions are complete, you're ready to be updated to the latest version of Ciphr HR. You will soon receive an email from us confirming the date your update has been scheduled. We will provide you with at least two weeks' notice to complete your required actions.

After the update, the only change users will notice is the new and improved sign-in screen and process. Once signed in, they will continue to see and access your current version of Ciphr.

Rest assured, access to the new user interface switch is within your control and will not be available to your users until you choose to grant access.

Further details about the new user interface and how you can enable it will be shared with you closer to your update.

Further help

If you need any support or if you have any questions, please check out our [FAQ guide] for common queries, or our [customer care team] are on hand to help you via the support portal.