Log In With Single Sign-On (SSO) and Multi-Factor Authentication (MFA)

Last Modified on 04/02/2025 1:23 pm GMT

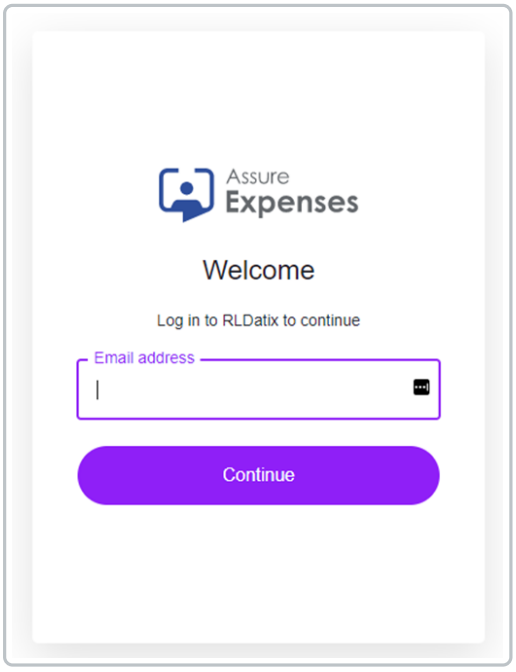
The Single Sign-On (SSO) and Multi-Factor Authentication (MFA) increase the security of your account and simplify the login process.

> **Note:** Your customer account needs to be enabled in the system before you can use the Single Sign-On (SSO) and Multi-Factor Authentication (MFA) features. If your system has not been enabled for **Login with SSO**, you can still log in and authenticate by entering the**Company ID**, **Username**, and **Password**.

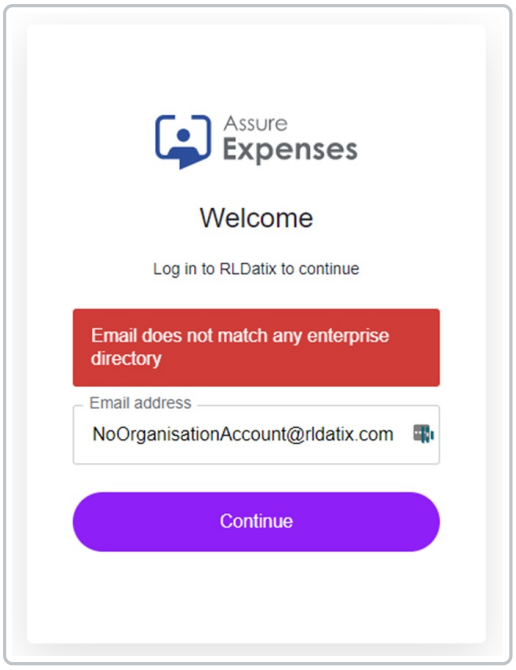
For more information on SSO and how it works, seeSingle Sing-On (SSO) - Feature Overview.

When your Expenses system is not enabled for **Login with SSO**

If you attempt to use **Login with SSO** when it has not been configured for your organisation, you will be redirected to your organisation's SSO logon page.



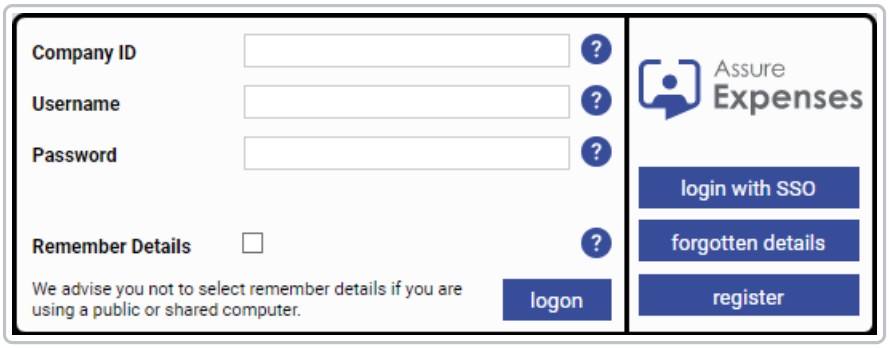
If you try to enter your corporate e-mail address and click**Continue**, you will get the following message:



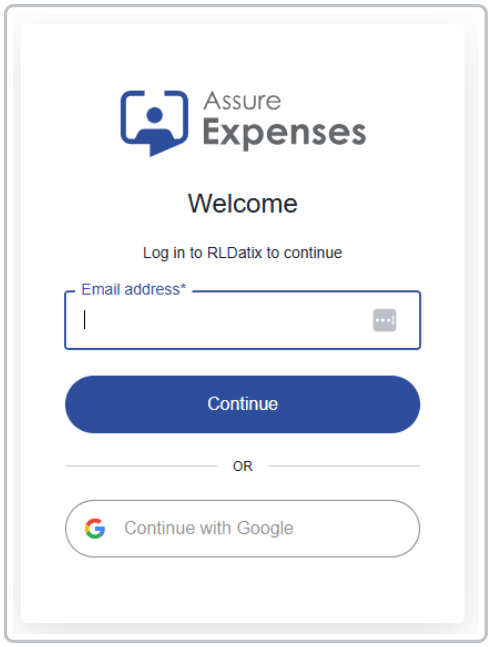
When this happens, use the **Back** button on your browser to go back to the previous page and log in as usual with the **Company ID**, **Username**, and **Password**.

When your Expenses system is enabled for **Login with SSO**

1. Click **Login with SSO**.



You will be redirected to your organisation's logon page.

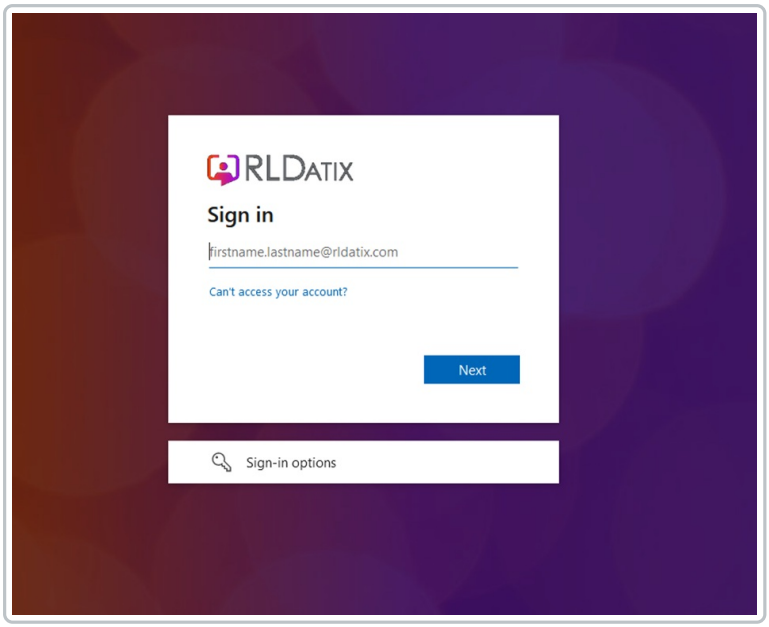


2. Enter your organisation e-mail address, then click **Continue**.

Note: When Single Sign-On (SSO) is enabled for your Expenses system, you will log in to Expenses using your organisation's SSO with your organisation's e-mail address for authentication. Where your organisation's SSO is configured for Multi-Factor Authentication (MFA), you will need to provide additional information to be authenticated to log in to Expenses.

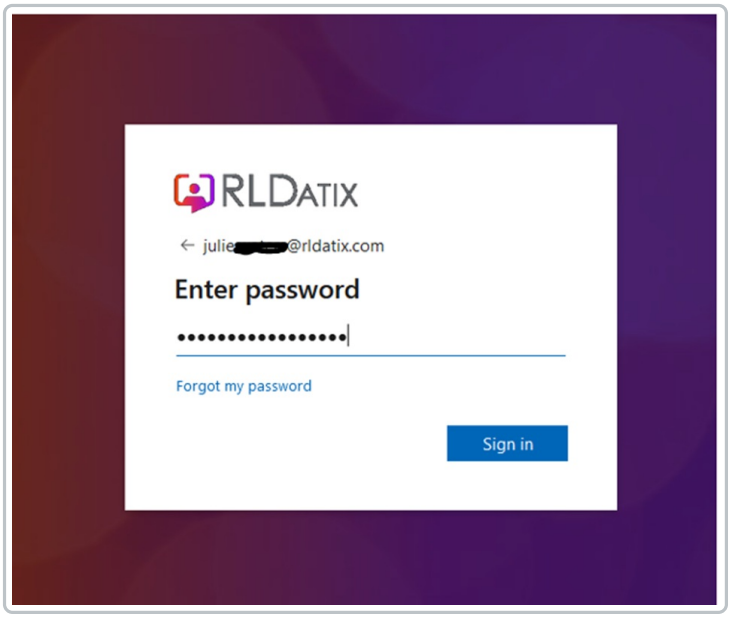
Authenticate with Multi-Factor Authentication (MFA)

After you enter your organisation e-mail address, you will be required to further authenticate through your organisation's Multi-Factor Authentication (MFA), as in the following example.



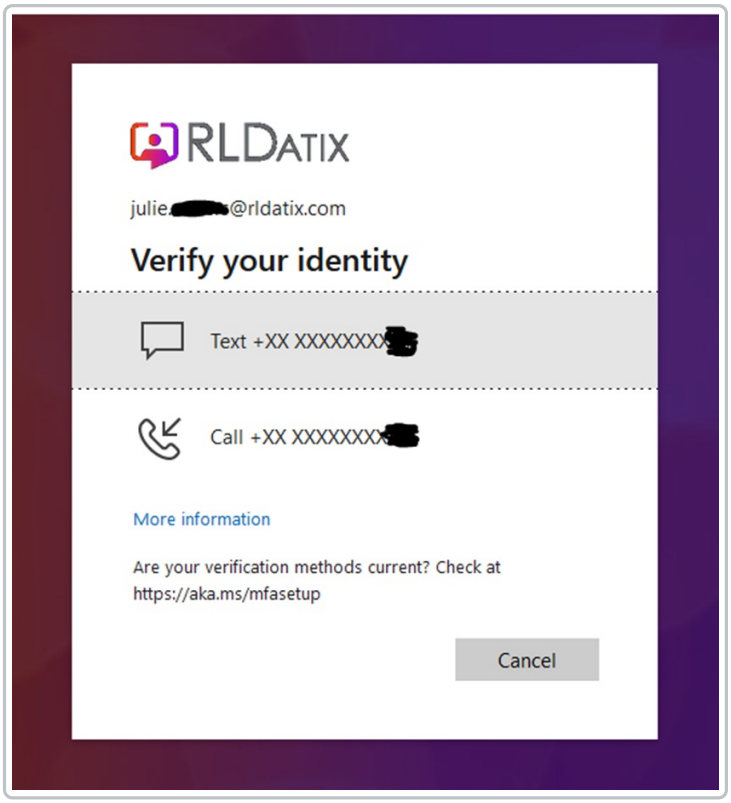
1. Enter your corporate e-mail address, then click**Next**.

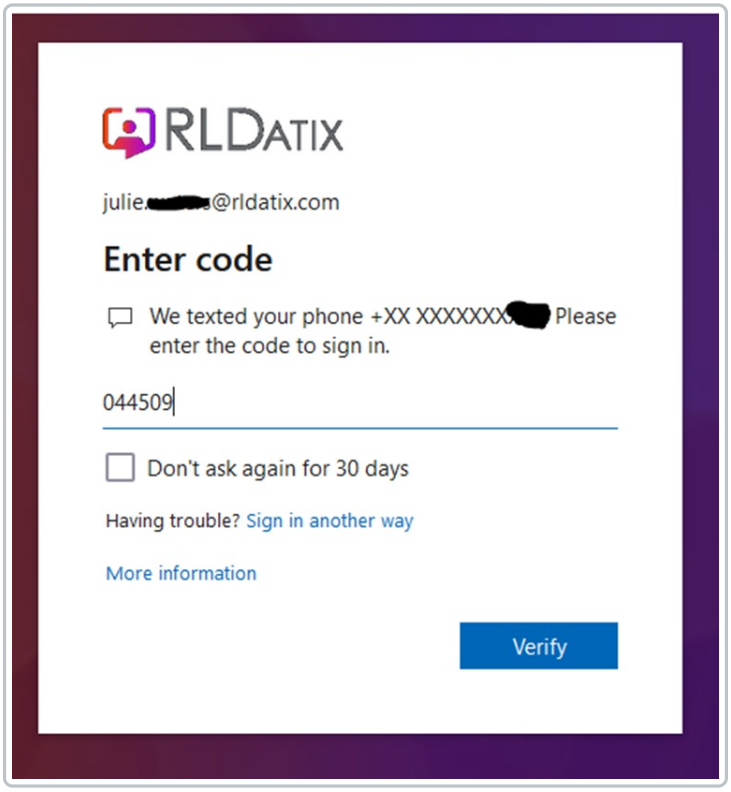
2. Enter your password.



3. Click **Sign in**.

4. Choose one of the options to**Verify your identity**. The options for verification depend on your organisation's IDP provider requirements.


RLDATIX
julie[redacted]@rldatix.com
Verify your identity
Text +XX XXXXXXX[redacted]
Call +XX XXXXXXX[redacted]
More information
Are your verification methods current? Check at https://aka.ms/mfasetup
Cancel


RLDATIX
julie[redacted]@rldatix.com
Enter code
We texted your phone +XX XXXXXXX[redacted] Please enter the code to sign in.
044509
Don't ask again for 30 days
Having trouble? Sign in another way
More information
Verify



After you have been authenticated, the Expenses**Home** page opens.

> **Note:** Once you have authenticated using Multi-Factor Authentication (MFA), you will be able to log in with your SSO account without MFA until such time as your organisation MFA configuration requires you to provide the additional details again.

Log In with SSO when your user account exists in Expenses but is not yet active

When you have an account in the Expenses system, but it has not yet been activated for you to claim your expenses, after the SSO authentication is completed, you will not be able to log in to the system. The 'Active' column in the **Company Select** page will not be ticked and the option to log in to the system in the 'Logon' column will not be available.



This can occur in two cases:

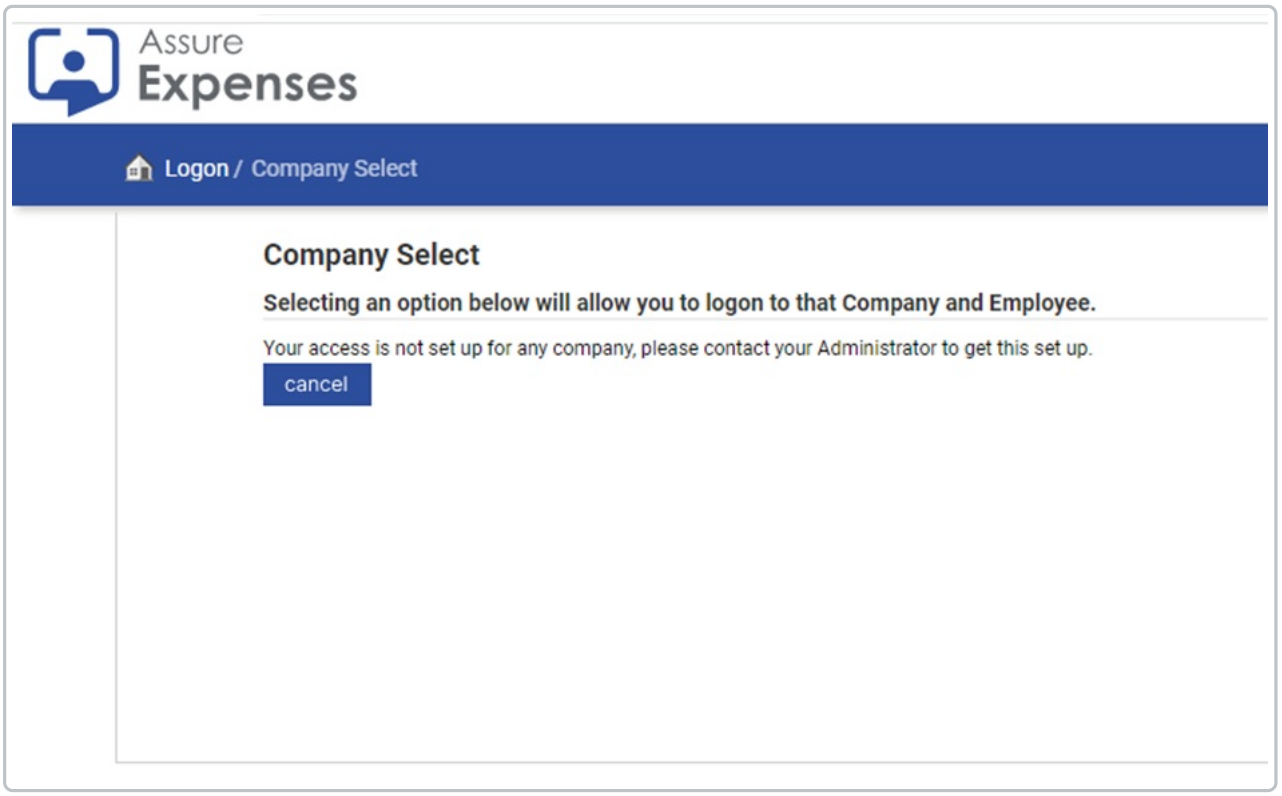
- If your account was created or imported by the administrator but hasn't been activated for use.
- If you have used **Self Registration** to create your Expenses account.

You will need to contact your system administrator to have your account activated in the Expenses

system.

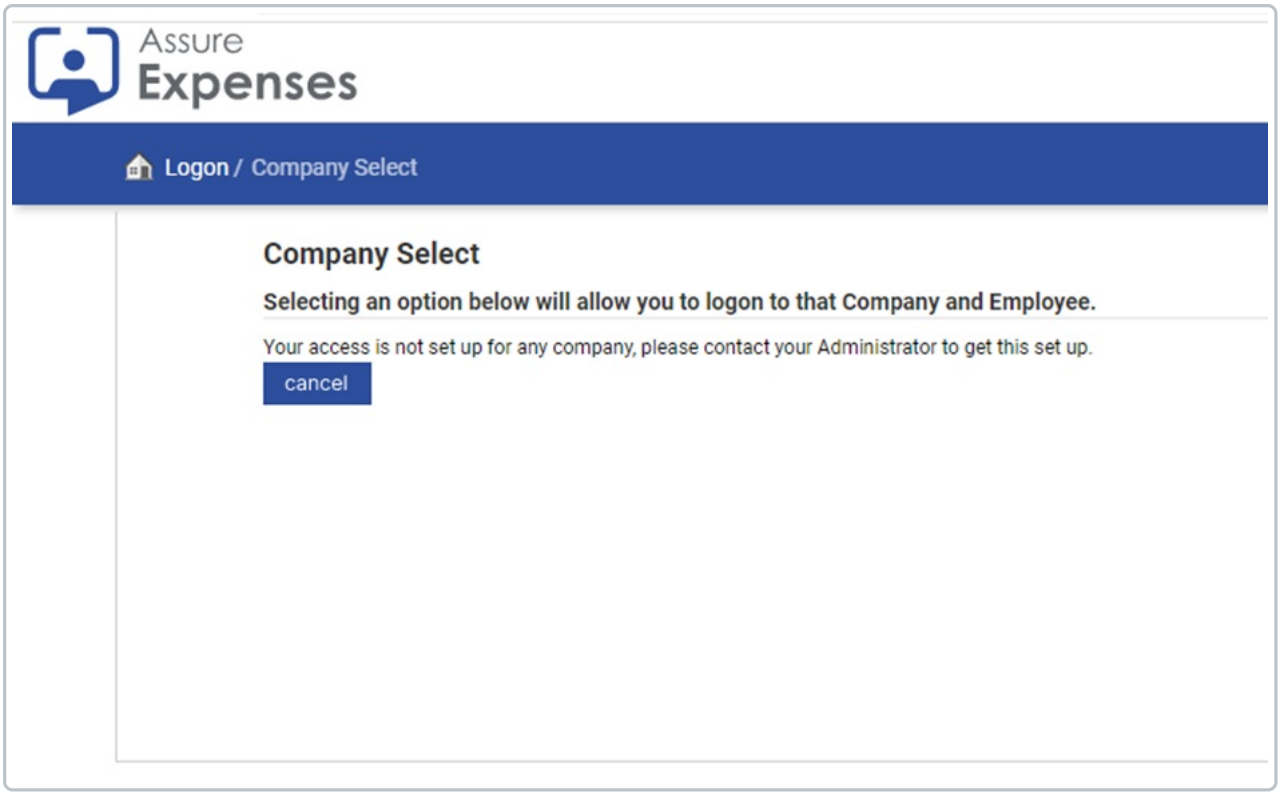
Log In with SSO when you do not have a user account in Expenses

When you have not been set up with access to the Expenses system, but have a valid account for your organisation's login system, after the SSO and MFA authentication to your organisation's system, your Expenses access will be prevented.



Log In with SSO when your user account in Expenses has been archived

When your user account for Expenses has been archived, your Expenses login access will be prevented, even if your company email is still active and your account is authenticated through SSO.



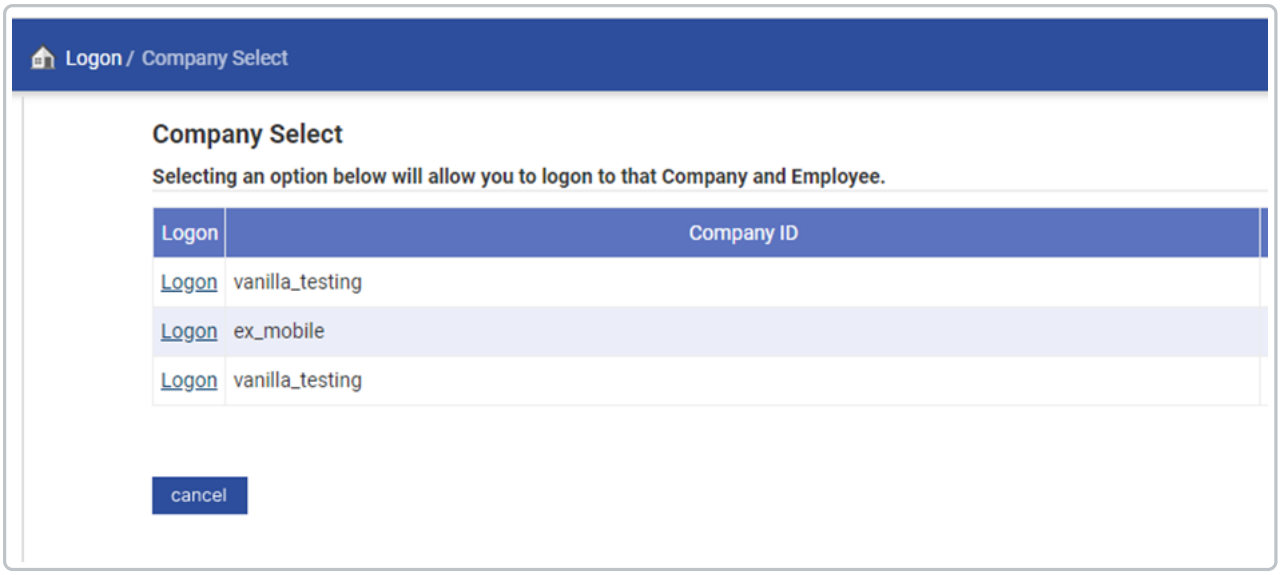
Log In with SSO when your user account exists in more than one Expenses system

It is possible for an Expenses user to have an active account in more than one Expenses database. This may occur in three cases:

- If the organisation has both a live and a separate test system.
- If there are individual Expenses systems across the organisation for separate countries or entities.
- Where the user runs a payroll service for several related organisations.

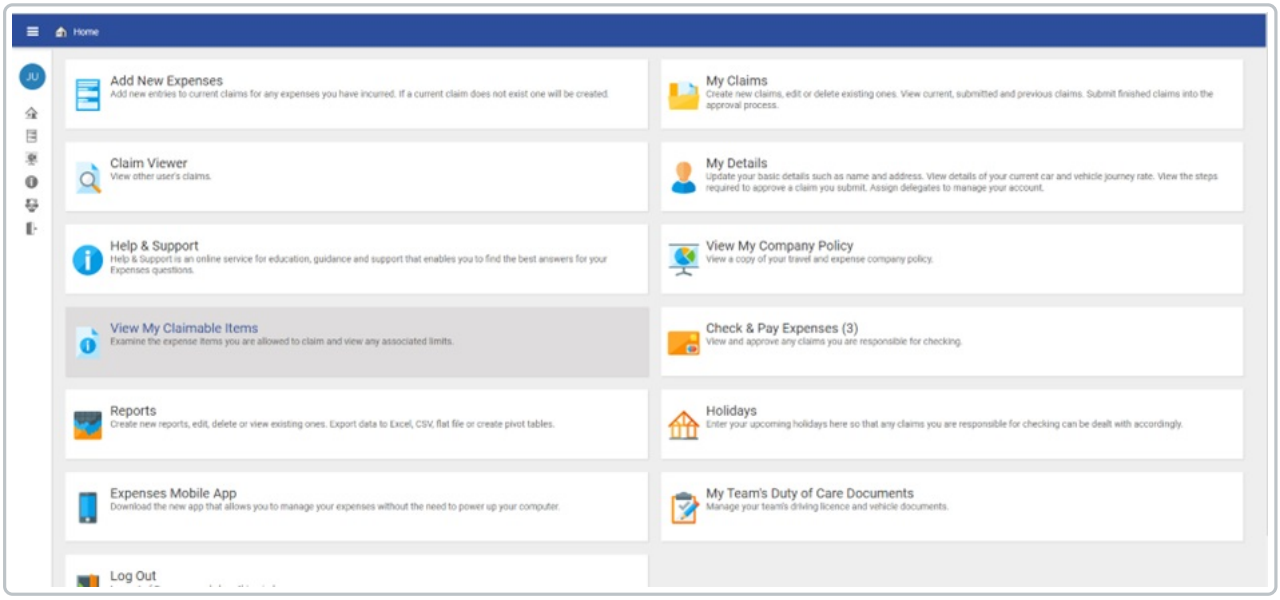
If you log in with SSO, once you're authenticated, you'll be able to choose the system you want to access.

In the 'Logon' column, click the**Logon** link that corresponds to the**Company ID** you want.



The Expenses **Home** page opens for the company selected.

You can verify this through the organisation's logo visible on the page, if this has been set up in the system.



Note: The icon that appears is from your organisation's Single Sign-On (SSO) system.

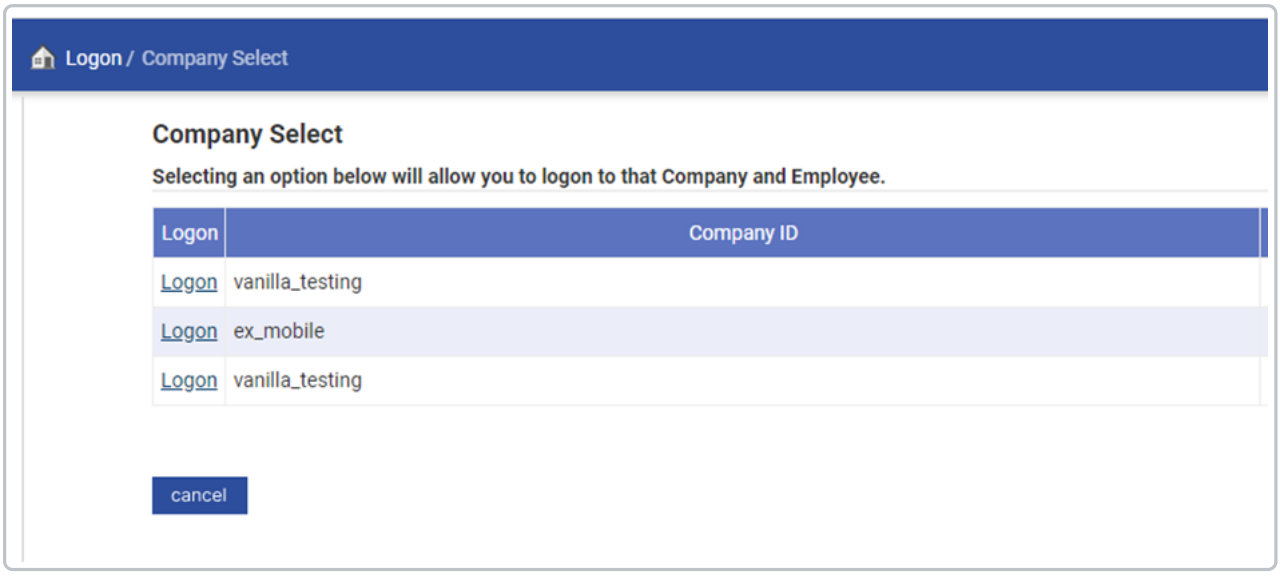


If you have access to more than one Expenses system, your menu option allows you to switch between the systems.



If you only have access to one system, this option is not available.

When you click this option, the**Company Select** page opens.



Log In with SSO for users with API access permissions

Users with API access are provided with additional options when logging in with SSO in order to use the API.

1. Log in to Expenses.
2. From the **Home** page, select **My Details**.
3. Select **Change my Details**.



API users need to generate a Personal Access Token (PAT) by using the **New PAT** option in **Page Options**. This generates a new token that you can use to access the publicly available APIs.

When the token is generated, copy the token and use it in the corresponding header **Auth Token** in the API request.

You'll be able to select how long the token will be valid for or you can revoke the token at any time by using the **Revoke** option.

Once the token is expired or revoked, in order to use the API, you will be required to generate a new personal access token via **New PAT**.