

Quick Setup Guide - Single Sign-On (SSO)

Last modified on 03 December, 2024

This Quick Setup Guide helps you to understand:

- Getting access to Single Sign-On (SSO) through an access package.
- Setting up a Multi Factor Authentication (MFA).
- Logging into various applications and navigate them through UI.

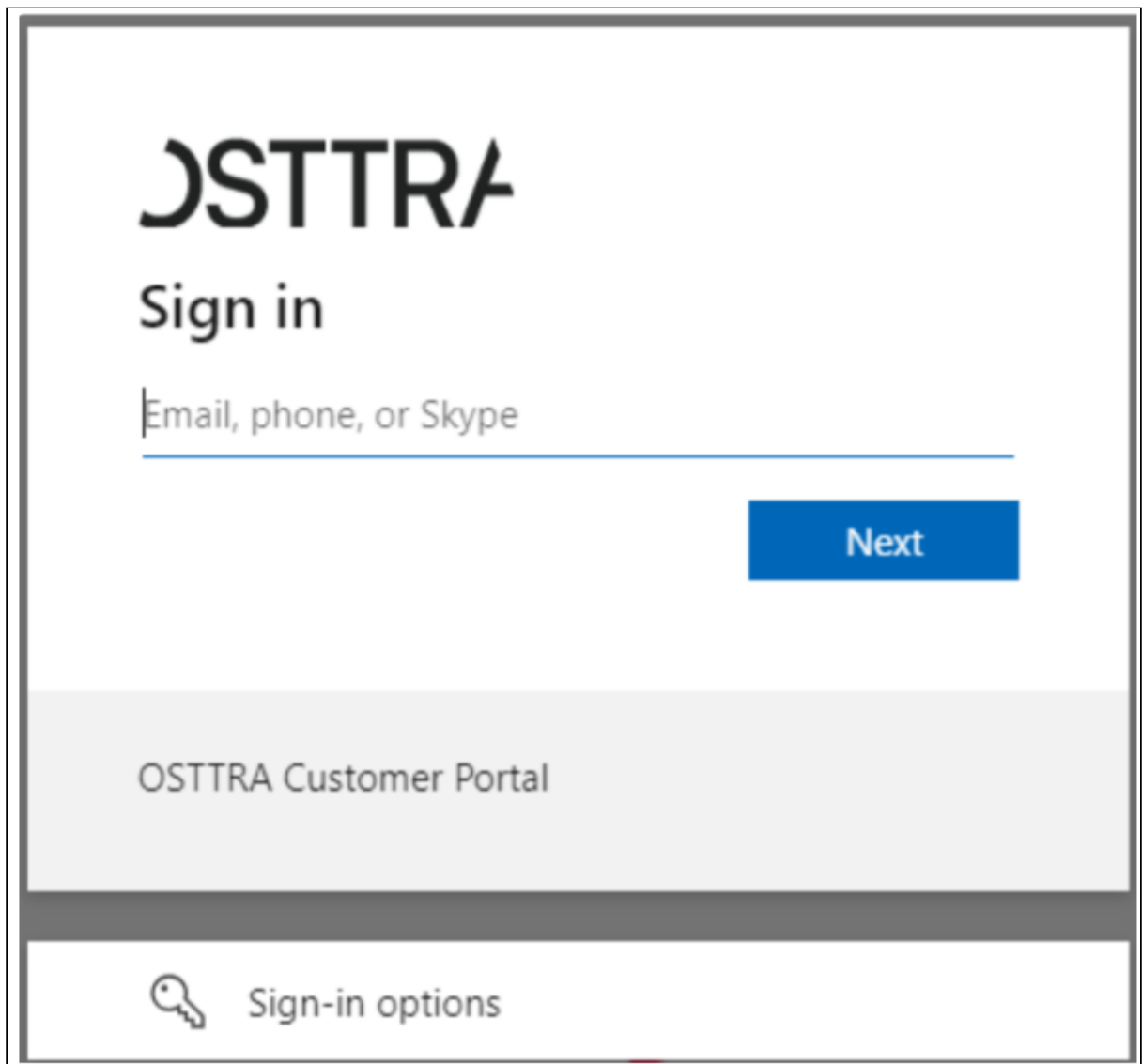
Getting access to Single Sign-On (SSO) through an access package:

This section applies only if you have been provided with a link to an access package, which is applicable to certain applications. Note that the access packages are only available for a limited set of applications, and Operations will not necessarily send you an access package for all applications. Alternatively, you may be self-onboarding to SSO.



Prior to performing the following steps, make sure that you have an existing account created by OSTTRA Operations in an underlying platform (CFD, for example).

1. OSTTRA support representative will provide you a link to an **access package** that is specific to an application. By accessing the link to that **access package**, you will be able to complete your setup. The link to an access package looks as follows:
<https://myaccess.microsoft.com/@sso.osttra.com#/access-packages/d7436c94-0e53-436b-a5da-3216fa3xxxxx>
2. Enter your email address and click **Sign In**.



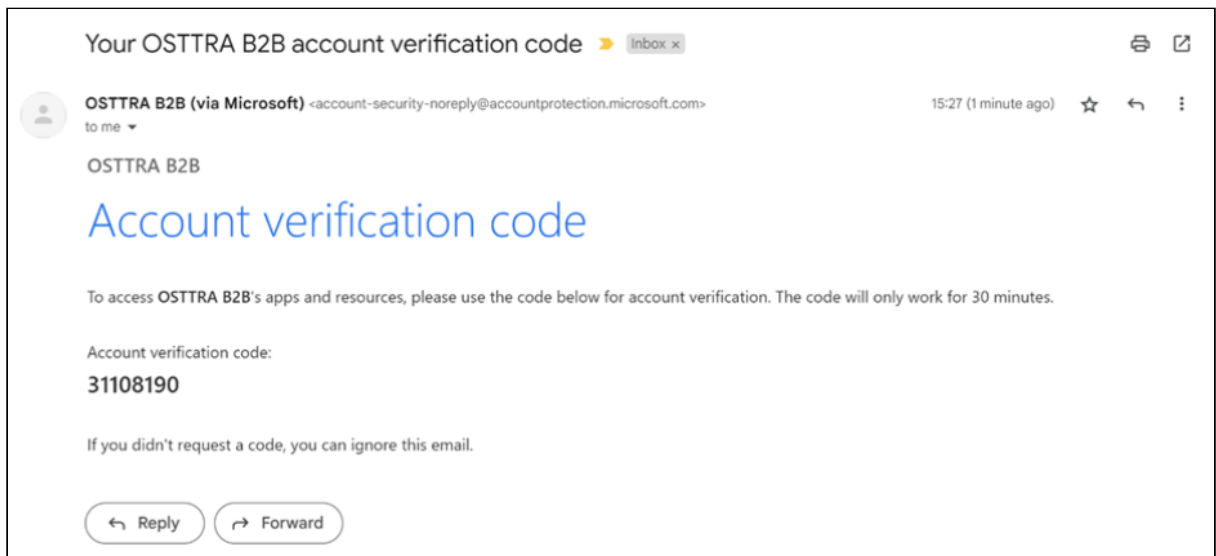
If your setup is federation (using your own identity provider - not managed by OSTTRA), then follow the prompts on the screen. However, if you are leveraging OSTTRA for user management, the following screen appears.



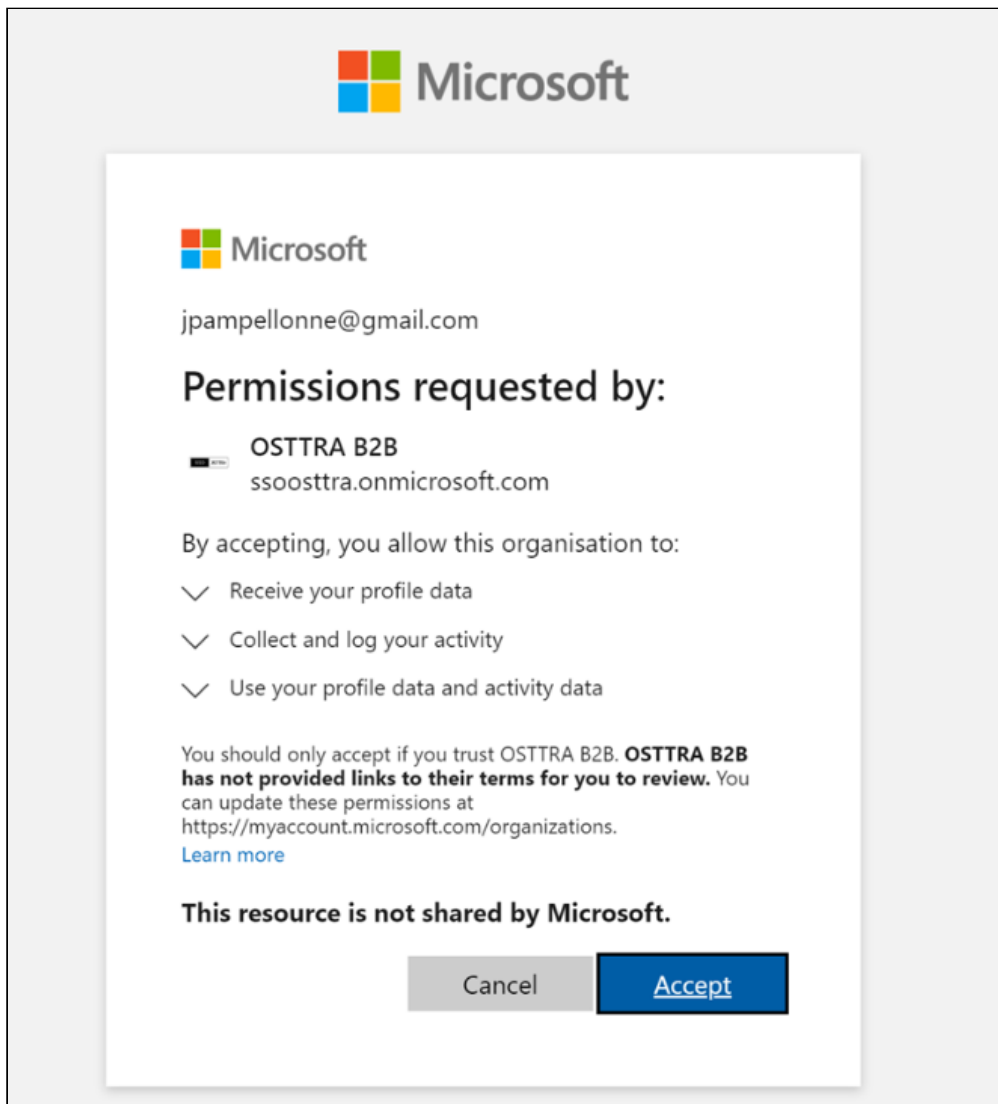
OSTTRA uses One Time Passcode (OTP) to validate users, this is a more secure way of accessing the services than the traditional username and password.

3. After providing your email, a One Time Passcode (OTP) is sent to your email that you will need to enter.

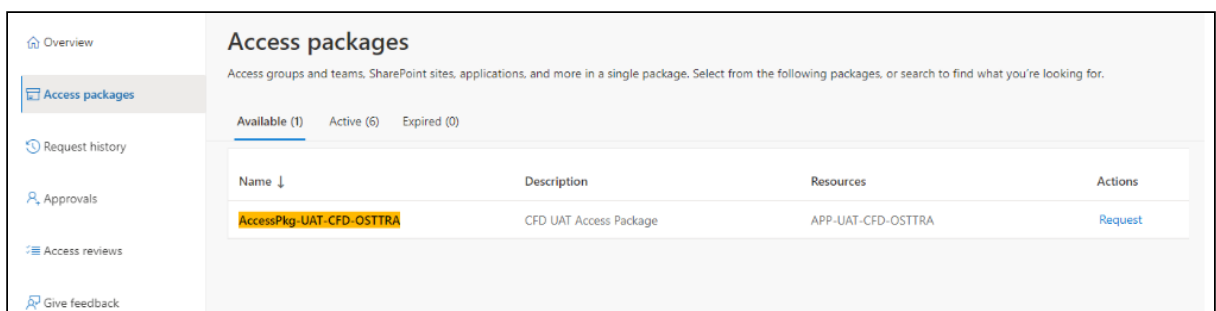
The example of the email you receive:




4. After you have entered the OTP, you will be prompted to accept the following permissions:



- OSTTRA requires a Multi-Factor Authentication (MFA) to access applications or resources. You will be guided to provide more information and to complete MFA using the tool of your choice.
- Once you have successfully authenticated the setup, the Access packages screen appears asking which packages you want to access; the packages available will be determined by what your organisation has been set up for. Choose the appropriate package, for example, to gain access to CFD UAT, select the AccessPkg UAT-CFD-OSTTRA package encircled below:



7. Once your request is completed, a message appears saying your request has been successful.

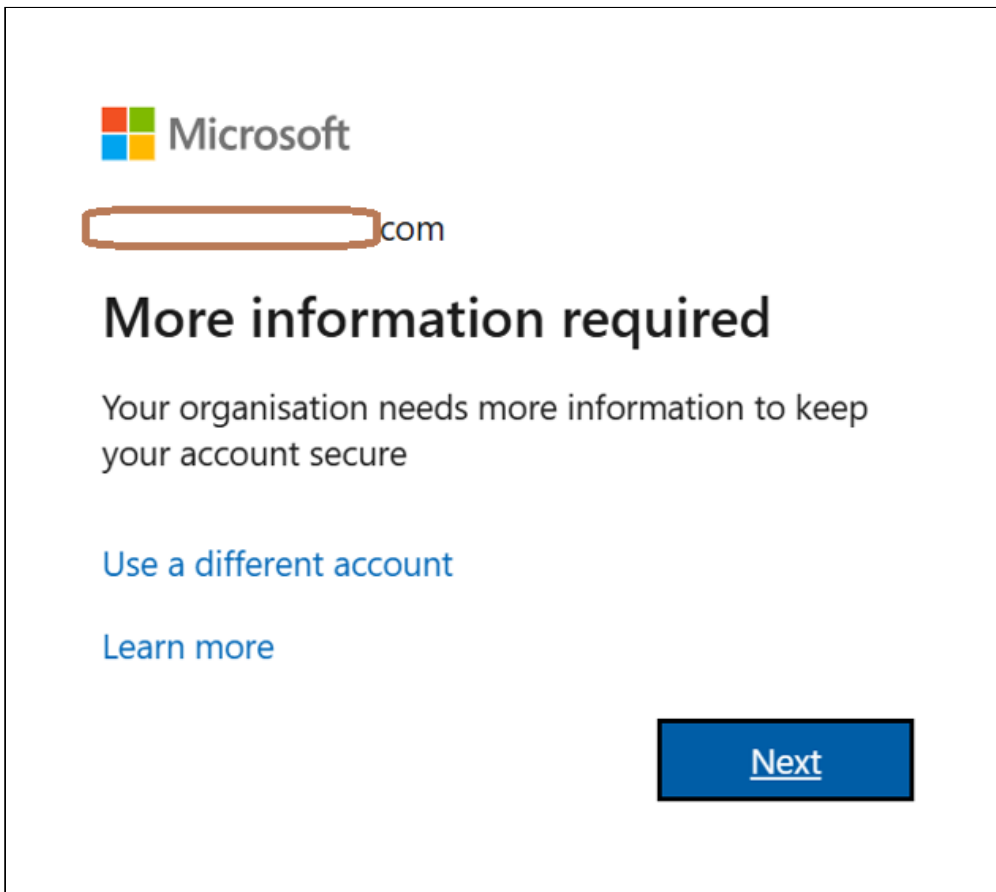
 From the point of requesting the application access to its availability, there could be a delay of several minutes.

Setting up a Multi Factor Authentication (MFA):

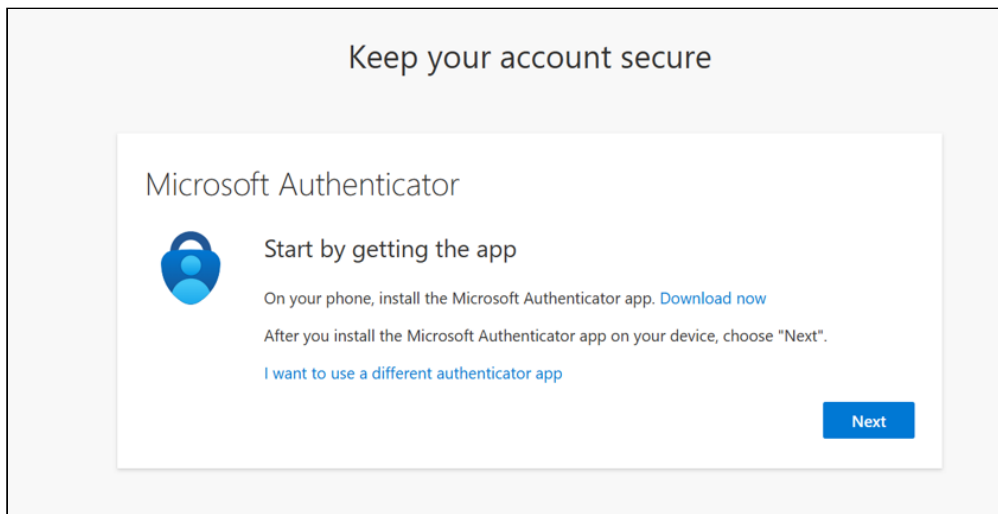
When a user is set up with federation, a customer’s IDP will manage the Multi Factor Authentication (MFA) setup. In case a customer’s IDP is not set up for MFA or the MFA setting is off in the IDP, the OSTTRA Azure tenant will enforce the MFA setup the first time that user logs in.

When a user first logs into an application through SSO, the user will be prompted to set up MFA. Users can follow on screen instructions to set up the MFA of their choice.

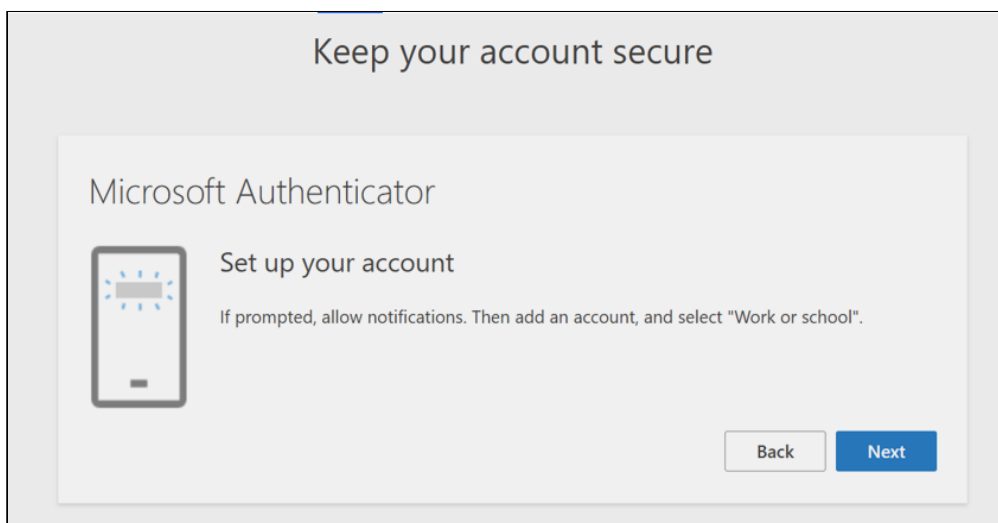
1. On first time login, the system will prompt to set up MFA.



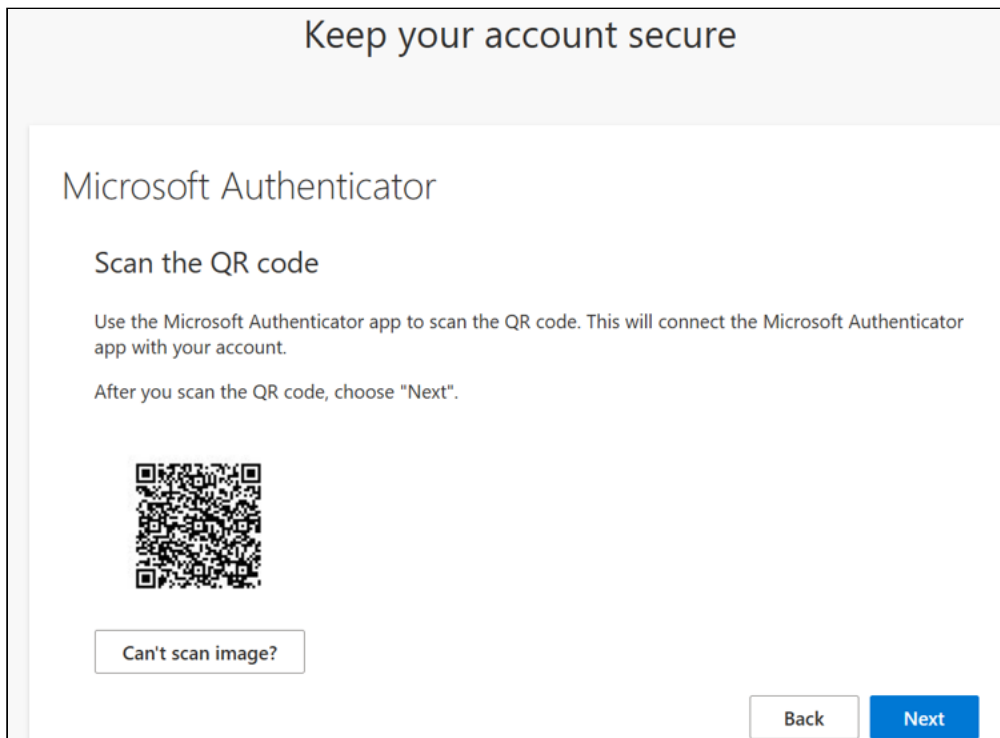
2. Users will be asked to choose the authenticator app. By default, the system tries to set up Microsoft Authenticator, however, the user can choose a different authenticator app as well.



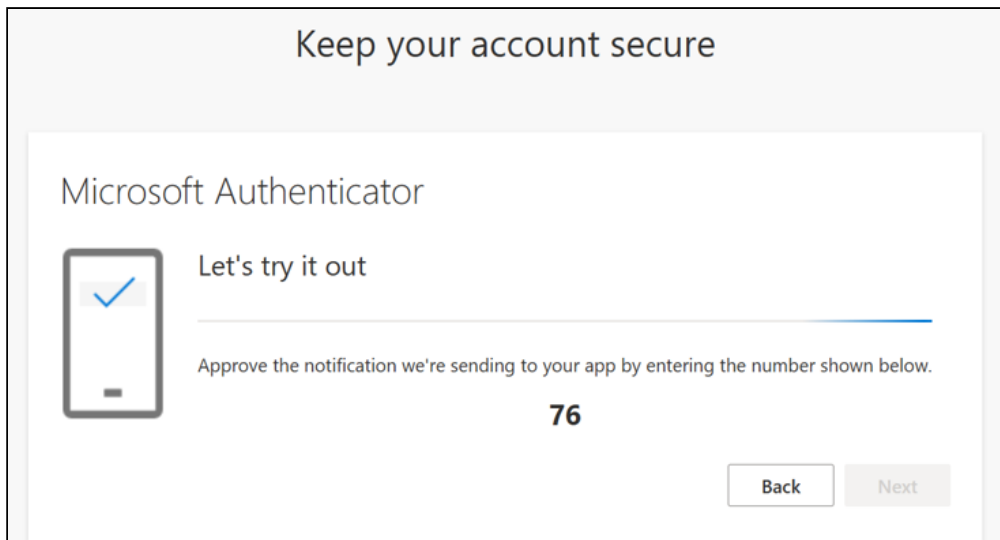
3. Assuming a user selected the Microsoft Authenticator app and clicked **Next**, the system will prompt to set up the account. Click **Next**.



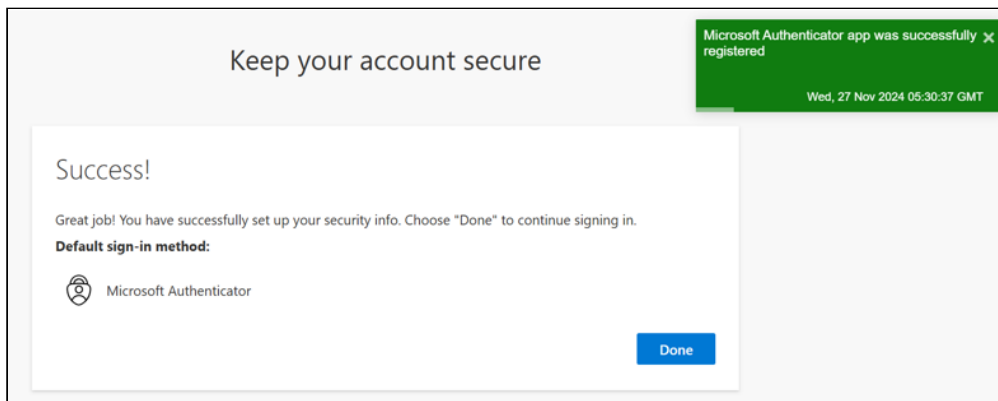
4. For any other authenticator app - follow the steps on the screen.
5. Users will be asked to scan the QR code or can set up the account manually by clicking **Can't Scan image?**.



6. Click **Next**, the user will be asked to verify the code in the authenticator app.



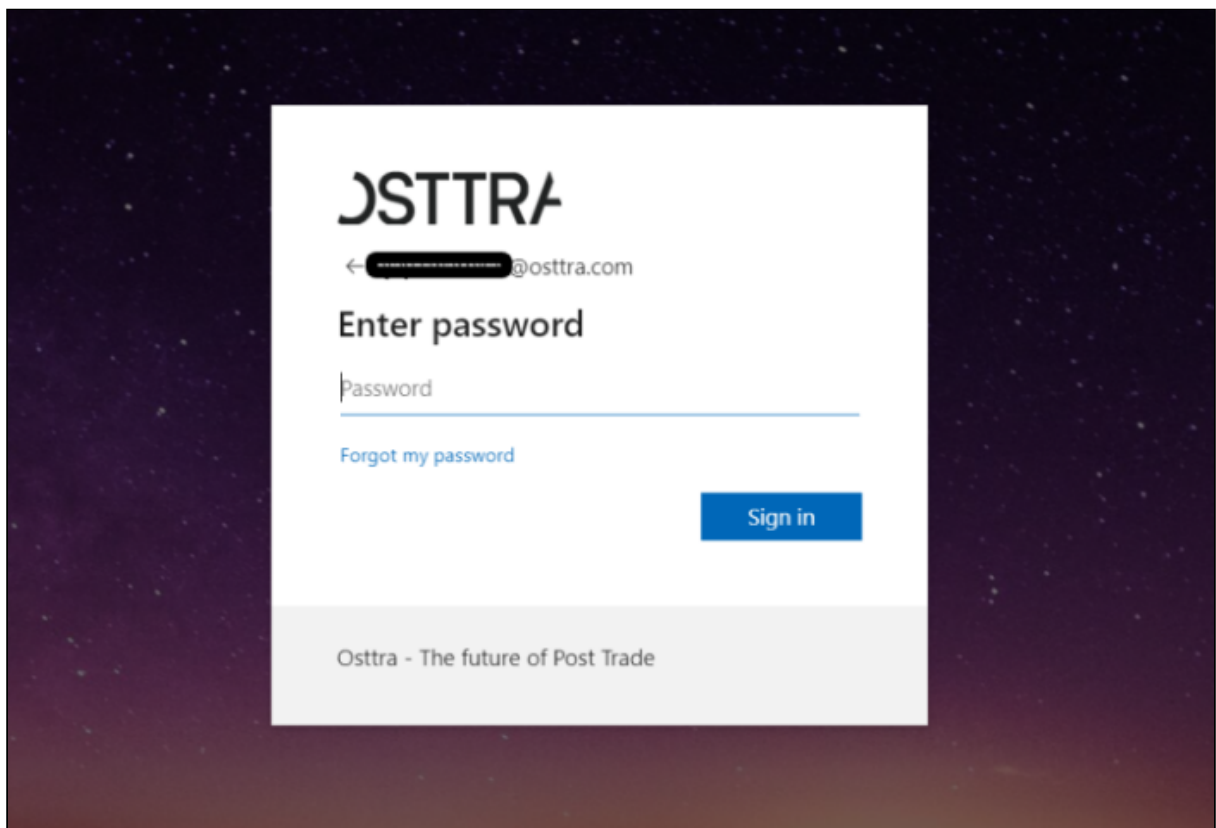
7. After verification, the **notification approved** message appears. Click **Done**.



The user is successfully setup for MFA.

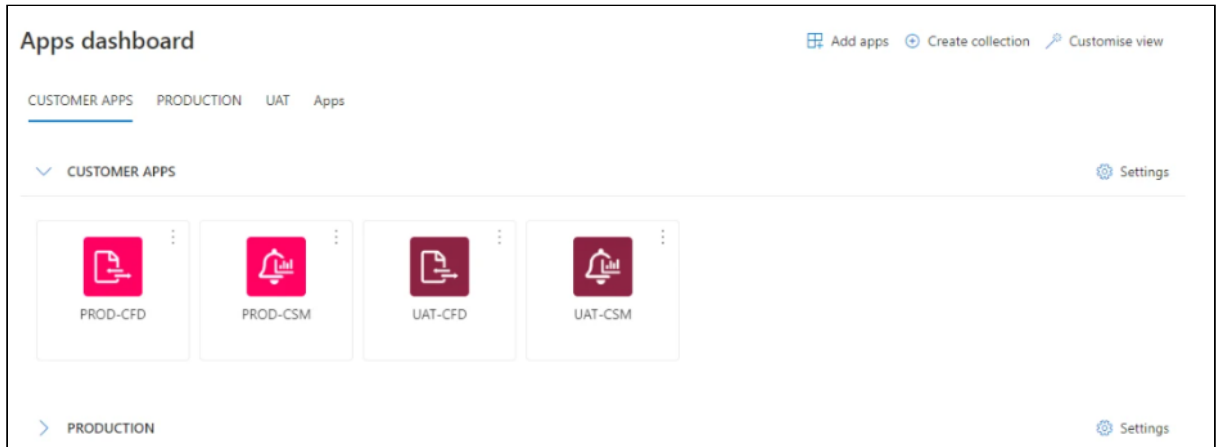
Logging into various applications through SSO and navigate them through UI:

1. Users can continue to access the application login URL directly and an option will be available to login via SSO. Alternatively, user can follow the <https://sso.osttra.com> link and select the account you are logging into - it will be the email address associated with the main account, which is set up by OSTTRA Operations. Enter your login credentials. If you do not have the federated setup, a One Time Passcode will be sent to your email address. Use that passcode to login followed by MFA authentication.



2. If the user directly logs in to the application via the application URL then the user will be logged in to the application. If the user logged in via sso.osttra.com then user will be directed to OSTTRA applications

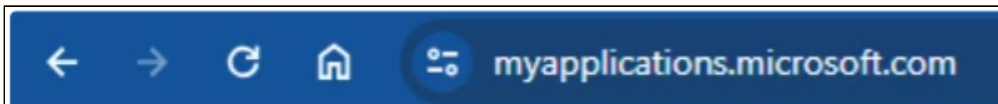
page, where you can select the application, you would like to access:



- 3. In this screen, you can create your own groups of applications by clicking **Create Collection** at the top-right corner. For example, here a group called “CUSTOMER APPS” has been created.

⚠ OSTTRA utilises Microsoft Azure technologies, which are commonly used within customer organisations. To do this, OSTTRA has created a specific OSTTRA B2B tenant in which it hosts all its customer facing applications and users. A tenant is a way of storing records and authorisation information of users.

You may notice that the URL you originally entered sso.osttra.com has changed to <http://myapplications.microsoft.com>. This is an expected behaviour.



If your organisation uses <http://myapplications.microsoft.com>, then it may be necessary to switch between your organisation’s tenant and the OSTTRA tenant. This can be achieved by selecting the organisation icon at the top-right corner of the window:

