Quick Setup Guide - Single Sign-On (SSO)

Last modified on 15 October, 2025

This Quick Setup Guide helps you to understand:

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

Getting access to Single Sign-On (SSO):

> ⚠ Before you can get started, your B2B collaboration setup must be completed. If you have not done that, contact the OSTTRA Support team.

If you are an existing user of OSTTRA services, you will be migrated to OSTTRA SSO, and no additional steps are required by the user.

For the new users, existing onboarding process will take care of users SSO onboarding through automated workflows, user can continue to leverage the existing user onboarding process to OSTTRA services, and no additional steps are required for the SSO access.

Setting up a Multi Factor Authentication (MFA):

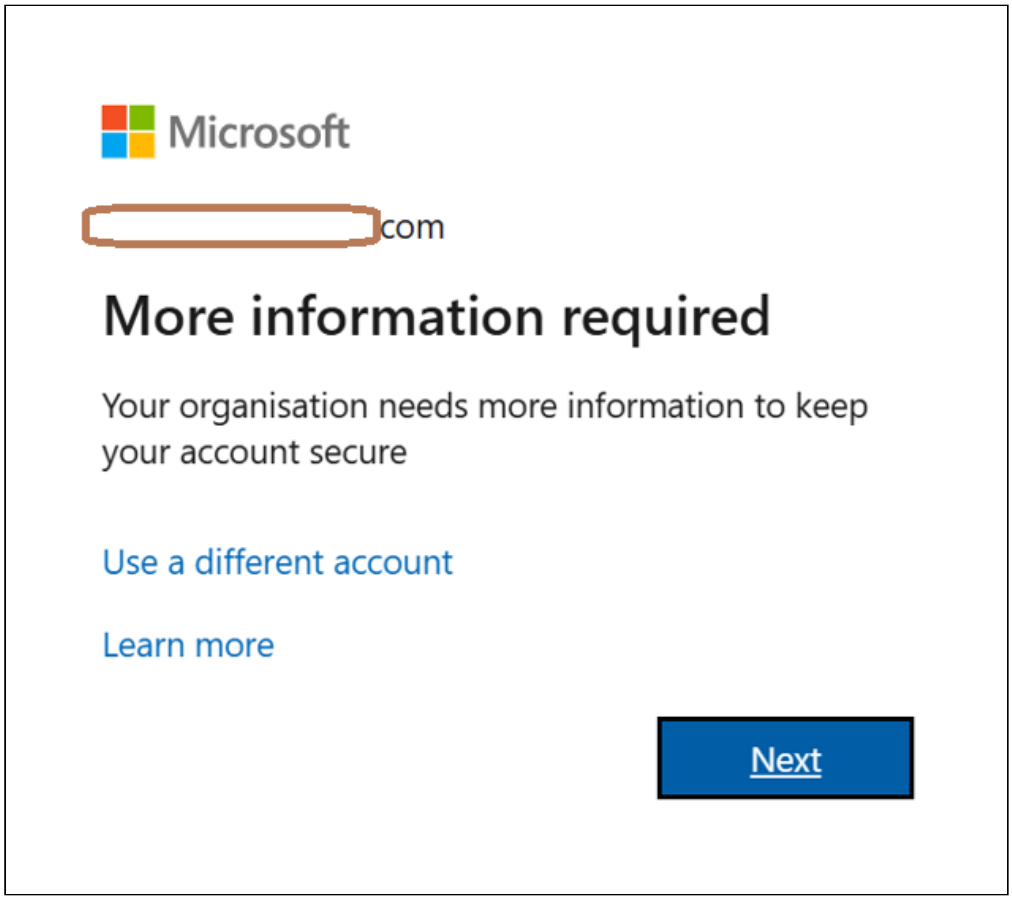
When a user is set up with federation, when an account is set up with federation, the responsibility for MFA lies with the user's organization's Identity Provider (IdP). This allows the customer to use any MFA method that their IdP supports. However, if a customer's IdP is not configured to enforce MFA, or if the MFA setting is turned off, the OSTTRA Azure tenant will take over to ensure a secure login. In this scenario, users will be required to set up the Microsoft Authenticator application the first time they log in.

When a user is setup as non-federated, by default MFA is disabled for non-fed accounts. To enable the MFA for non-fed on domain level, it requires additional setup, therefore, raise a request to OSTTRA support team. Once OSTTRA team enables the MFA setup for non-fed user, follow the Microsoft Authenticator's steps for MFA setup. Below steps are applicable for both fed and non-fed users.

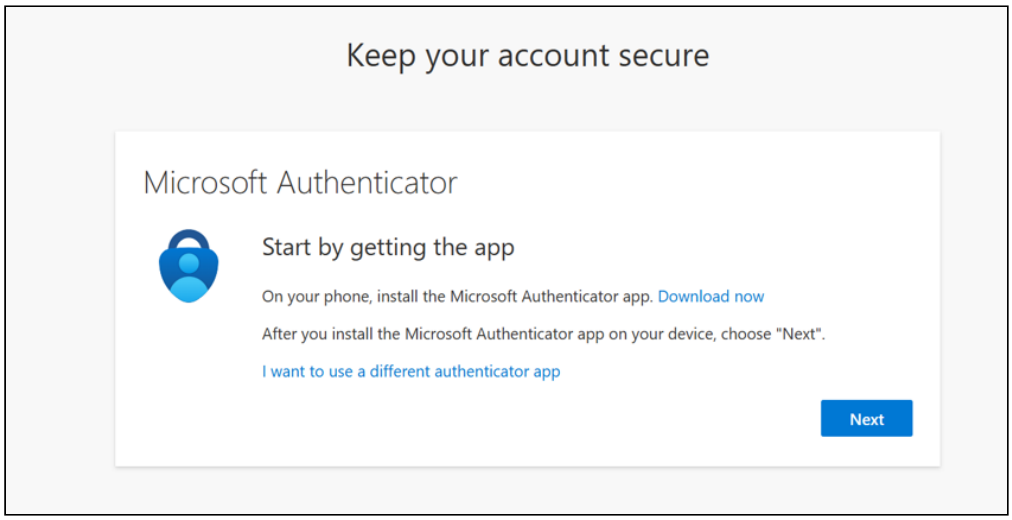
> ⚠ The OSTTRA Azure tenant only supports the Microsoft Authenticator app for MFA enforcement for both Fed and Non-Fed users.

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.

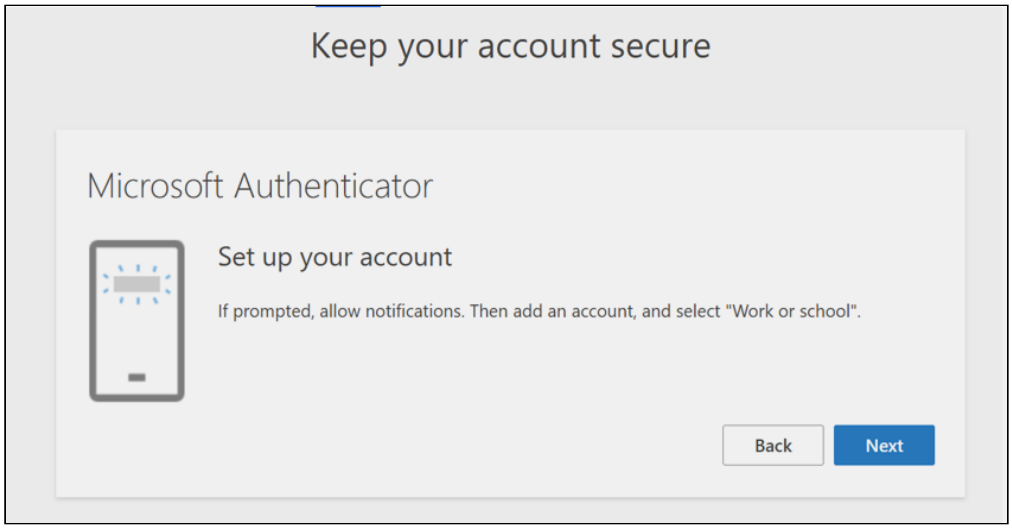
1. On first time login, the system will prompt to set up MFA.

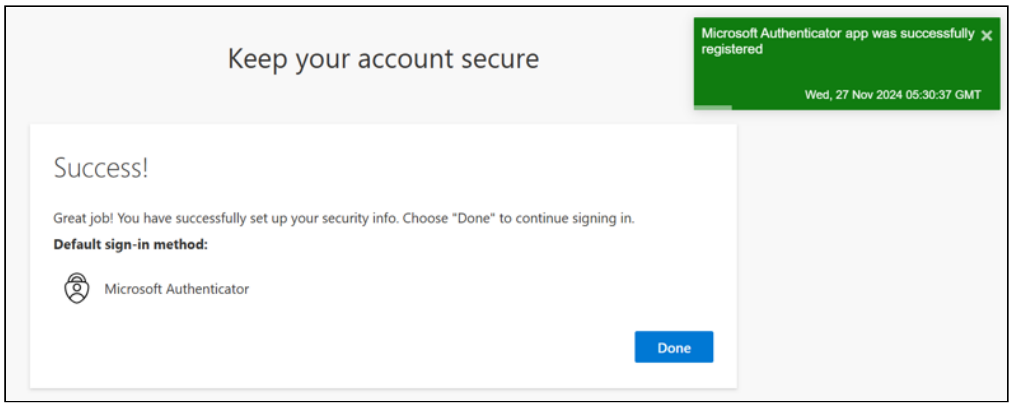


2. Users will be asked to choose the Authenticator application. The system will enforce to set up the Microsoft Authenticator application.



3. Click **Next** to setup the Microsoft Authenticator application and follow the instructions on the screen.

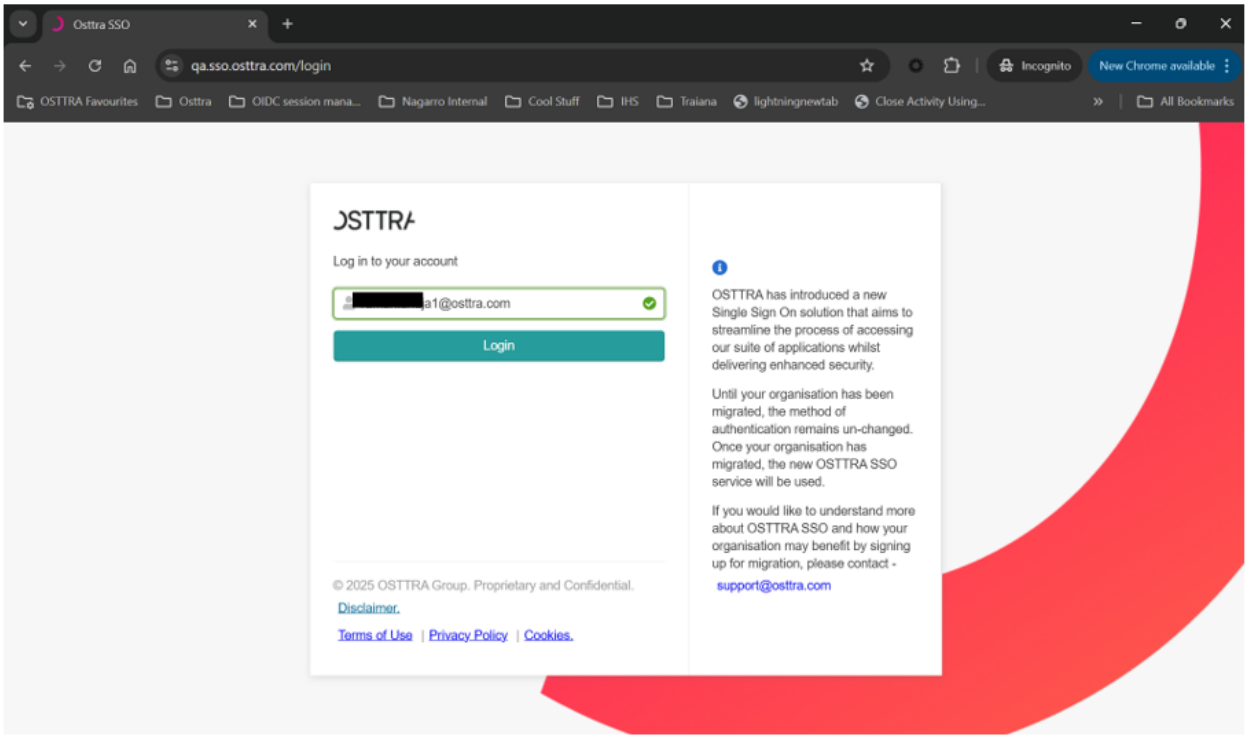


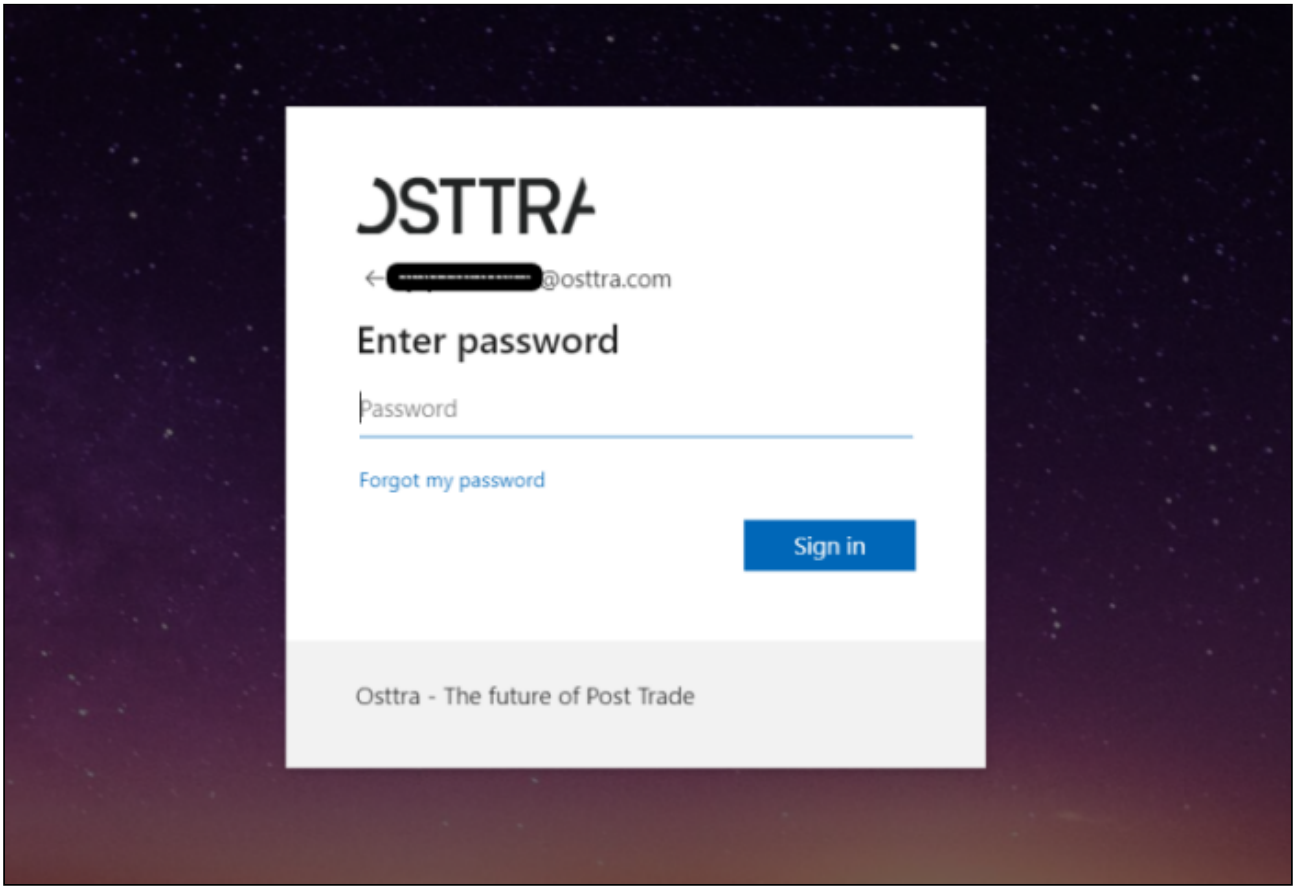


The user is successfully setup for MFA.

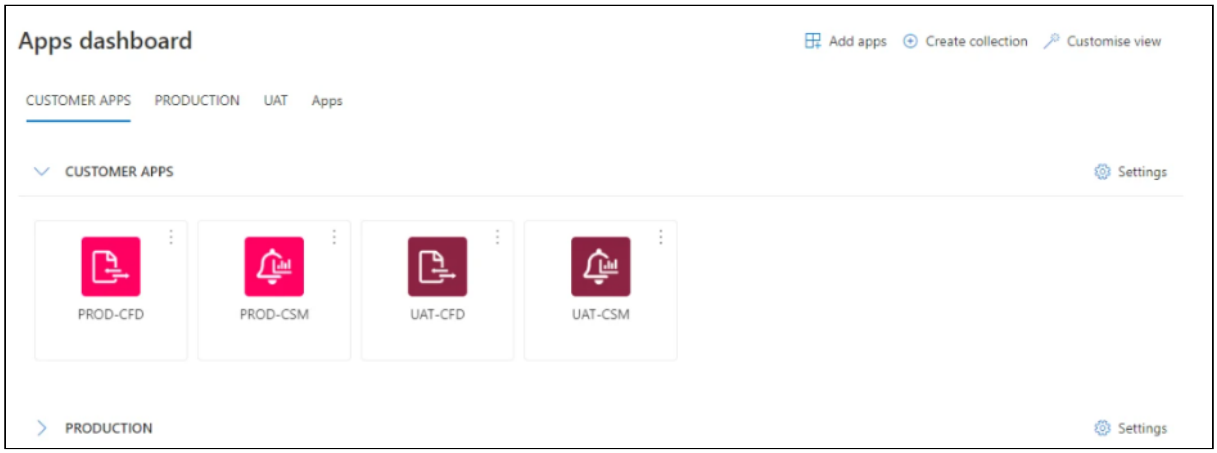
Logging into various applications through SSO and navigate them through UI:

You can continue to access the application login URL directly. An option will be available to log in via SSO. Alternatively, you can follow the link: https://sso.osttra.com. Select the account you are logging into, which will be the email address associated with your main account set up by OSTTRA Operations. Enter your login credentials. If you do not have a federated setup and your Identity Provider (IDP) is not Azure Entra, a One Time Passcode (OTP) will be sent to your email address. Use that passcode to log in, followed by MFA (Multi-Factor Authentication) authentication..





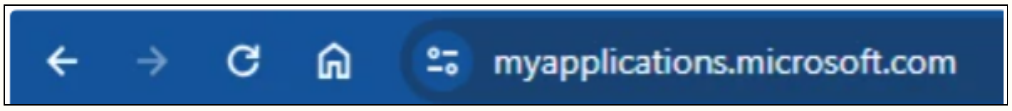
1. If you log in directly using the application URL, you will be directed straight into the application.
2. If you log in via sso.osttra.com, you will be redirected to the OSTTRA applications page, where you can select the application, you wish to access.



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

⚠ OSTTRA utilises Microsoft Azure technologies, which are commonly used within customer organisations. To facilitate this, OSTTRA has established a dedicated OSTTRA B2B tenant to host all its customer-facing applications and users. A tenant serves as a method for storing user records and authorization information.

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: