Quick Setup Guide - Single Sign-On (SSO)

Last modified on 18 September, 2026

Copyright © 2026 OSTTRA Group

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, **if you chose Federated access to OSTTRA applications,** your B2B/ SAML collaboration setup must be completed. If you have not done that, contact the OSTTRA Support team.

You will be migrated to OSTTRA SSO, and no additional steps are required from your end, if:

1. You're an existing user of one or more OSTTRA applications,
2. If opting for federation, the required setup along with MFA configuration is complete,
3. If opting for non-federation, MFA setup (if requested) is complete.

For the new users, yours 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 (ENTRA B2B or SAML), 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 facilitate MFA for ENTRA B2B to ensure a secure login, however OSTTRA trust client IDP for the MFA for SAML collaboration, and OSTTRA provided Authenticator is not supported for SAML onboarding. For ENTRA B2B, users will be required to set up the Microsoft Authenticator application the first time they log in if OSTTRA provided authenticator is chosen.

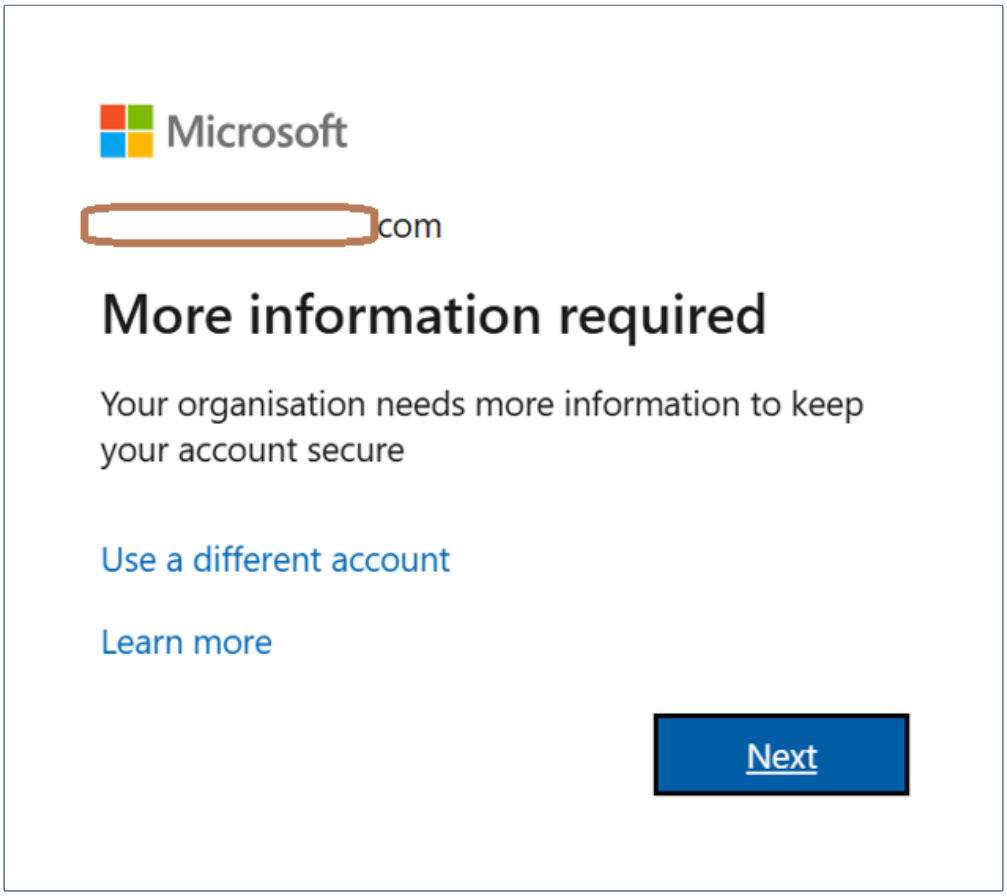
When a user is setup as non-federated, by default OSTTRA offers OTP based authentication for non-fed setup which currently do not support MFA, however if client want MFA to be enabled for non-fed setup , OSTTRA offers password based authentication supported by MFA. To enable the MFA for non-fed (password based) 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 (password based) user, follow the Microsoft Authenticator's steps for MFA setup. Below steps are applicable to setup the MFA.

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

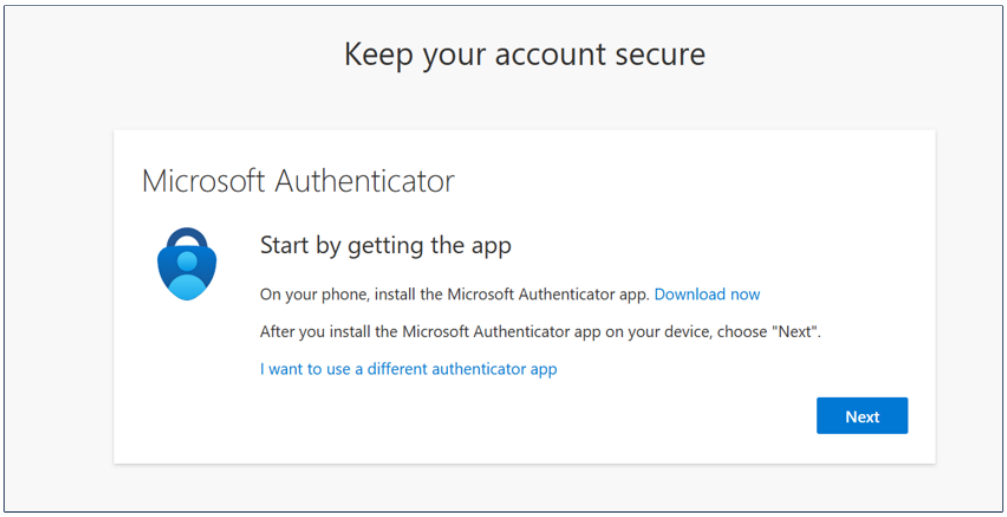
When a user first logs into an application through SSO, the user will be prompted to set up MFA. Users can follow on screen instructions to set up the MFA of their choice.

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

Confidential | Copyright © 2026 OSTTRA Group

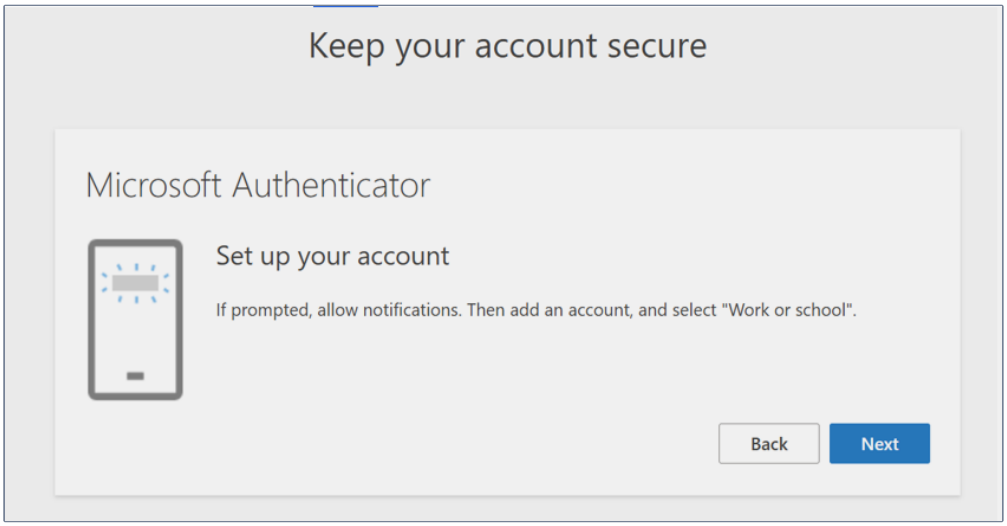


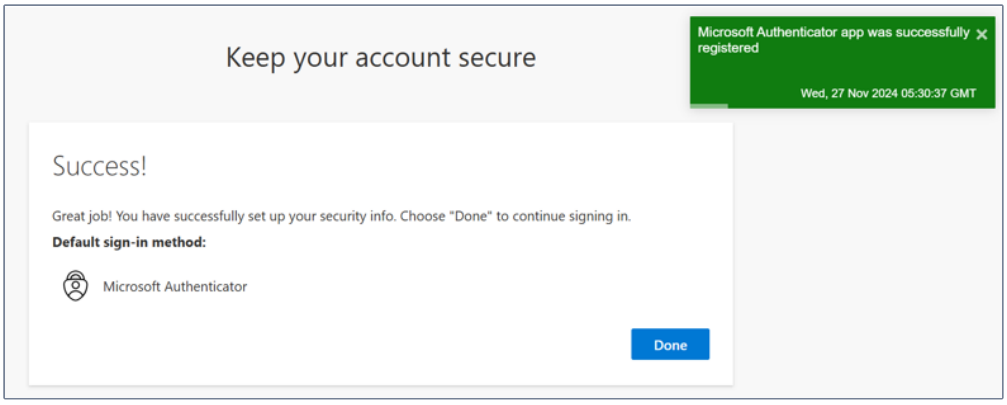
2. Users will be asked to choose the Authenticator application. The system will enforce to set up the Microsoft Authenticator application.



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

Confidential | Copyright © 2026 OSTTRA Group



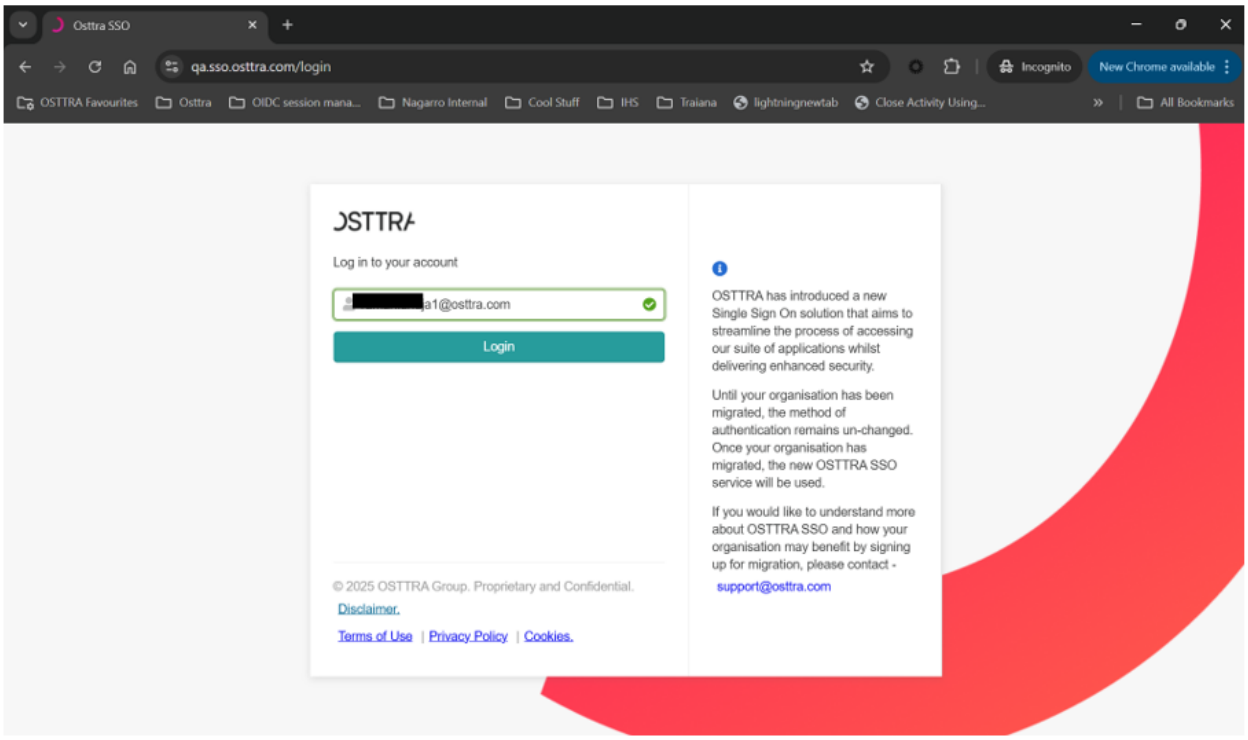


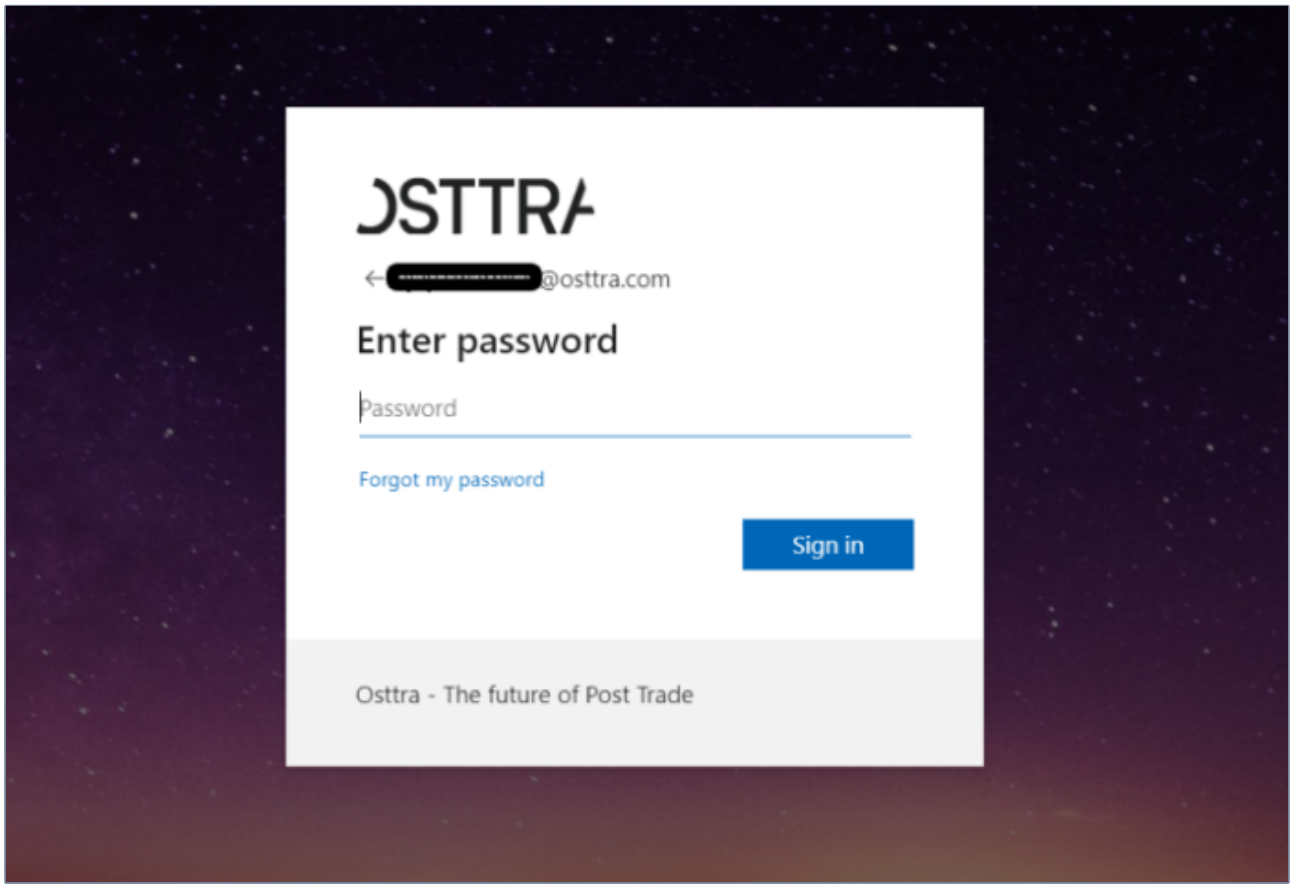
The user is successfully setup for MFA.

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 are setup as non-fed based on OTP authentication, a One Time Passcode (OTP) will be sent to your email address. Use that passcode to log in.

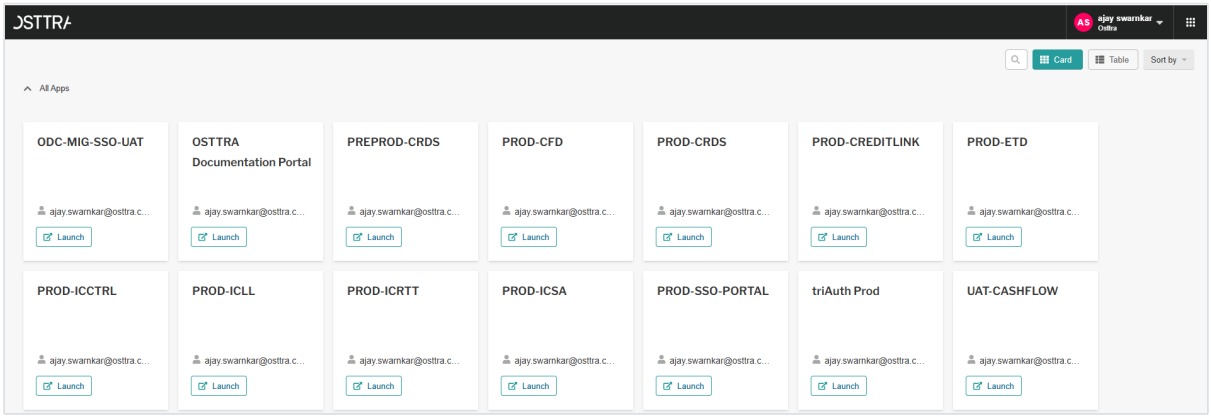
Confidential | Copyright © 2026 OSTTRA Group





Confidential | Copyright © 2026 OSTTRA Group

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.



Confidential | Copyright © 2026 OSTTRA Group