Single Sign-On (SSO) FAQs

Last modified on 19 July, 2024

Q1. What is OSTTRA Single Sign-On (SSO)?

OSTTRA SSO is a new secure authentication process taking away the complexity of managing multiple credentials for various OSTTRA platforms or for different roles into the same platform. Security will be assured via delegating authentication responsibility to the user's organisation (federated) or by leveraging a password-less mechanism (non-federated), one-time password (OTP) on the user's corporate email account and multi-factor authentication (MFA).

Together with this launch, we are offering customers an improved way to access OSTTRA applications from a single place and using a single set of credentials.

For example: If you currently use four OSTTRA platforms using four different credentials (one for each platform), you will only need to login once to gain access to each of these four platforms.

Q2. What does a federated setup mean?

A federated setup is when you as the client can leverage your organisation's own identity and authentication services to access OSTTRA's applications **without** needing to maintain separate credentials. You will gain access by signing on with your business credentials - no additional credentials are required. With this setup, the method of authentication is controlled by your own organisation's policies and processes. Going by industry trends, organisations are increasingly requiring federated access configuration in order to meet their security needs and to protect against threats.

Q3. What does a non-federated setup mean?

A non-federated setup is where OSTTRA will manage and govern your authentication. Under a non-federated setup, we will facilitate a password-less authentication via OTP (One Time Passcode) on your business email. Once you have entered your username (your email address), you will be emailed a single-use passcode to login, followed by MFA (via an authenticator like Microsoft or Google or OKTA) if you have opted for this during user setup.

Note: In case your organisation is on Azure AD (Entra) for authentication, Azure an easy way to federate by whitelisting the vendor's domain, avoiding the need of non-federated setup.

Q4. Which OSTTRA applications are in scope?

The plan is to rollout SSO across all OSTTRA applications. As of July the following applications will be supported in Production: CFD, ETD and CreditLink. We will notify you when other platforms are added to SSO. The move to SSO will be paced over time to minimise disruption and to ensure that users can experience the benefits as early as possible.

Additionally, all new OSTTRA applications will only support login via SSO.

Q5. How do I gain access to SSO?

Reach out to the OSTTRA support team and they will guide you through the process. It will first involve setting up your organisation for federation, then the underlying users can be mapped. In the majority of instances, configuration assistance will be required from your own internal technical teams who manage access control. Once complete, a link will be provided to you from which you can sign in to SSO.

Alternatively, you may navigate to the application(s) you use in the normal way and follow the 'login via SSO' option.

Q6. What will happen to my existing account?

Your user account profiles will remain the same under SSO. Your user permissions will also remain the same. Your old credentials will remain active in parallel with the SSO method for now. At some point, OSTTRA will remove direct access, but you will be kept informed of dates.

Q7. Can one SSO login be used to access a single platform for different entities?

Yes – if you have access to one platform on behalf of multiple entities, each of those representations will be available for access once you are logged in. You will continue to have access only to platforms that you currently have been permissioned for.

Q8. How will SSO impact me if I use a distribution email address to login?

Group email address credentialed accounts will not be eligible to benefit from SSO, because the functionality depends on the ability to authenticate individual user profile along with their email address. If you currently login to an OSTTRA application with a group email address, please contact us immediately to prevent any disruption in access.

Q9. What if I already have a bookmark to the application I use to login?

You can choose either of these options:

- Replace the existing bookmark(s) with a link to sso.osttra.com. This option works best if you if would like to bookmark a central (single) URL and dashboard to login to multiple OSTTRA applications or perspectives that you are permissioned to access.

  OR

- Proceed to the existing login page and select the option to 'login via SSO'. If you do not see it yet, it may be because the application has not yet been configured for OSTTRA SSO, but you can expect to see it soon.

Q10. I am signed up to login via One Time Password (OTP), but I have not received my passcode via my corporate email account?

Check your internet connection. If it is working, check your spam folders and add "account-security-noreply@accountprotection.microsoft.com" to your safe senders list. If the issue persists, try to re-login and generate a new OTP. If that fails, reach out to your existing OSTTRA support contacts.

Q11. When I try to login to OSTTRA SSO, I am receiving a message that it is blocked. What can I do?

First confirm if your organisation has been configured for SSO by OSTTRA, the OSTTRA support teams can help with this.

If you are accessing the OSTTRA B2B tenant for the first time and you are blocked from accessing SSO, then access may be restricted by your organisation. You will need to contact your IT or an IAM (Identify Access Management) team to check whether your firewalls or access management system is preventing federated setup with a third-party.

Finding an IT/IAM team in your organisation could be done by asking Service Desk or by going to CSO/CIO/CISO. If you are were able to login to SSO earlier and now you are blocked, then the following could be the probable reasons for this problem:

- User has been offboarded from the application; in this case, contact your local admin or OSTTRA support.
- User is disabled in the application; in this case contact OSTTRA Support.
- User is disabled/deleted in Entra (Azure); in this case contact OSTTRA Support.

Q12. Will my session timeout change?

Session timeouts for the underlying applications remain as they are today.

Q13. What do I do if I cannot access my MFA or reset my password?

If you are setup for Federated access, then this will be controlled by teams internal to your organisation. Raise a helpdesk ticket with them; OSTTRA will not be able to assist / help.

If you are logging in via a One Time Password (OTP) and you have exhausted all options, then reach out to the OSTTRA support team and they will be able to assist further.

Q14. Whom do I reach out to for further information?

You can email your queries to the usual OSTTRA support teams.

.