Single Sign-On (SSO) FAQs

Last modified on 13 October, 2026

Copyright © 2026 OSTTRA Group

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?

In a non-federated setup, OSTTRA directly manages and governs your authentication. We support the following two authentication methods for non-federated users:

- **Password less Authentication (Email OTP) - Recommended:** Enter your business email address to receive a single-use One-Time Passcode (OTP) to log in.
- **Password-Based Authentication:** Log in using a permanent password, followed by Multi-Factor Authentication (MFA), if enabled during user setup.

***Note**: If your organization manages users through an Identity Provider (IdP), we recommend setting up identity federation with OSTTRA via SAML 2.0 or Microsoft Entra ID (formerly Azure AD) for a seamless Single Sign-On (SSO) experience*

Q4. What is the SAML Federation? Does OSTTRA support this?

SAML Federation, a protocol-based authentication mechanism recently introduced by OSTTRA.

Security Assertion Markup Language (SAML) is a standardized protocol used to communicate a user's identity to external applications and services. It primarily enables Single Sign-On (SSO) technology, allowing users to authenticate once and access multiple applications without logging into each one separately. As an interoperable standard, SAML works across different systems and devices, making it widely accepted for cloud service providers.

A typical SAML authentication process involves three main parties:

- Principal (Subject): The user attempting to access a cloud-hosted application.
- Identity Provider (IdP): The cloud software service that stores and confirms the user's identity through a login process.
- Service Provider (SP): The cloud-hosted application or service the user wants to access.

Confidential | Copyright © 2026 OSTTRA Group

The authentication workflow follows these steps:

1. The principal requests access from the service provider.
2. The service provider requests authentication from the identity provider.
3. The identity provider sends a SAML assertion to the service provider.
4. The service provider validates the assertion and grants access to the principal.

If your organization prefers not to establish a direct Microsoft Entra-to-Entra B2B Collaboration with OSTTRA, you can instead set up a secure federation using the SAML protocol by exchanging configuration metadata.

Q5. How is a client set up for SAML?

To set up a client via SAML, please follow these steps:

1. Metadata Exchange: The client must share their SAML configuration metadata details with the OSTTRA support team. Once provided, we will generate the necessary metadata for you to configure the handshake.
2. IdP Configuration: OSTTRA will share its SAML metadata, which the client's technical team must configure within their internal Identity Provider (IdP).
3. Login URL: The dedicated URL for SAML-based authentication is sso.osttra.com/saml/login.

Once your metadata is shared by the customer/client, we will generate metadata for you to configure for the handshake.

Q6. What is the user journey for SAML login?
There is no change to the overall user journey for SAML:

- Users can continue to access the application directly via the standard login URL or by navigating to sso.osttra.com/saml/login.
- After initiating the login, users will be prompted to enter their corporate credentials.
- The authentication request will be sent to the user's organization/IDP, and they will be granted access based on the response.

Q7. Can I set up MFA with SAML?
Yes, Multi-Factor Authentication (MFA) for the SAML setup is **entirely managed by the client/customer**. OSTTRA does not provide or enforce MFA options for SAML federations. Clients can implement any MFA solution required by their organization's security policies.

Q8. What additional setup is required for a user to use SAML?
OSTTRA does **not** support Just-In-Time (JIT) user provisioning.

Users must be created and provisioned in both the target OSTTRA application and your internal SSO system before they can log in via SAML.

Q9. What is OTP-based authentication and who uses it?

OTP (One-Time Passcode) authentication is the default method for non-federated setups managed directly by OSTTRA. It is designed for users whose organizations do not leverage a federated Identity Provider (IdP), allowing them to authenticate securely without managing a permanent password by receiving a single-use code at their registered corporate email address.

Q10. Can I receive my OTP on a personal email address or via SMS?

Confidential | Copyright © 2026 OSTTRA Group

No. OSTTRA strictly delivers OTP passcodes to your individual corporate email address to maintain security compliance. Additionally, group or distribution email addresses are not supported for OTP/SSO logins as individual identity verification is required.

Q11. How long is a One-Time Passcode valid before it expires?

Each OTP is valid for a single login attempt within a limited timeframe for 5 minutes. If the passcode expires before you enter it, return to the login screen, select the option to re-login, and request a new OTP.

Q12. What happens if I enter an incorrect OTP multiple times?
Repeatedly entering an incorrect OTP will temporarily lock your authentication attempt to safeguard your account. If your account becomes locked or you run out of attempts, wait a few minutes to request a fresh passcode or reach out to the OSTTRA support team for assistance.

Q13. Do I need to enter an OTP every time I sign in?
Yes. Under a non-federated setup, a unique, single-use passcode is generated for every new login session. Once logged in, your access will remain active according to standard application session timeouts.

Q14. Does OTP authentication support Multi-Factor Authentication (MFA)?
No, Multi-Factor Authentication (MFA) is currently not supported for OTP-based (non-federated) logins. Verification is completed solely via the single-use passcode sent to your registered corporate email address. If your organization requires MFA policies you can opt for the Federated setup or password based non-federated setup.

Q15. What should I do if my OTP expires or does not arrive?
Check your network connection or spam folder , if you still have not received the OTP try login again or contact to OSTTRA support

Q16. Is authorization under scope of the federation or non-federation authentication workflows?

Authorization and application roles and privilege management are out of scope for this change and will remain unaffected.

Q17. Which OSTTRA applications are in scope?

All OSTTRA applications will be in scope for onboarding via OSTTRA SSO. Some applications are yet to onboard, which are planned on or before EOY 2026. Please reach out to Client Services to enquire for specific applications.

Q18. Does enabling OSTTRA SSO through Microsoft Entra grant access to any other Microsoft services, for example, Ofiice365?
No, enabling SSO establishes the authentication workflow only (how users log in). It will not provision any other Microsoft services like Office365, SharePoint, or Mailbox. OSTTRA guarantees to never provision any other Microsoft services without prior intimation to the clients.

Q19. 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.

Confidential | Copyright © 2026 OSTTRA Group

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

Q20. 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.

Q21. 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.

Q22. 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.

Q23. What if I already have a bookmark to the application I use to login?

You can choose either of these options:

- 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.

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

Q24. 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 “noreply@osttra.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.

Q25. 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 login via OSTTRA SSO 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.

Confidential | Copyright © 2026 OSTTRA Group

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.

Q26. Will my session timeout change?

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

Q27. 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.

Q28. Whom do I reach out to for further information?

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

.

Confidential | Copyright © 2026 OSTTRA Group