SSO Non-Fed FAQs

Last modified on 04 February, 2026

Q1. What does a non-federated setup mean?

In a non-federated setup, OSTTRA will manage and govern your authentication.

For **non-Entra** clients, we facilitate password-less authentication via a One Time Passcode (OTP) sent to your business email. Once you enter your username (your email address), you will receive a single-use passcode to log in. This will be followed by Multi-Factor Authentication (MFA) via an Authenticator such as Microsoft, Google, or OKTA, if you opted for this during user setup.

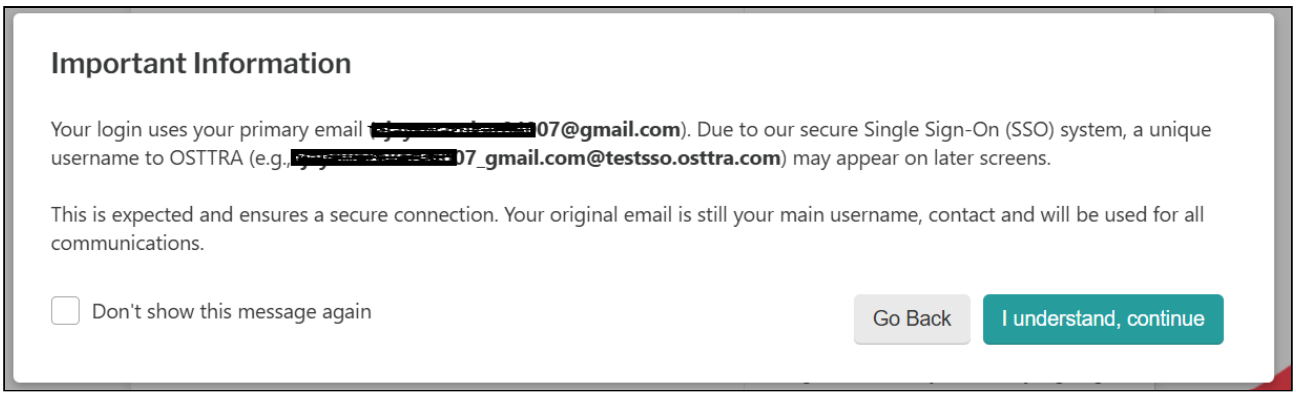
For **Entra** clients who do not wish to federate with OSTTRA B2B, we facilitate a password-based authentication using their email ID as the login ID. An OSTTRA member user ID mapped to your business email ID will be maintained within OSTTRA SSO to facilitate access.

> ⚠ In case your organization uses Azure AD (Entra) for authentication, Azure offers a straightforward method to federate by whitelisting the vendor's domain. This approach helps avoid the need for a non-federated setup.

Q2. Can non-fed users use their business email id to login?

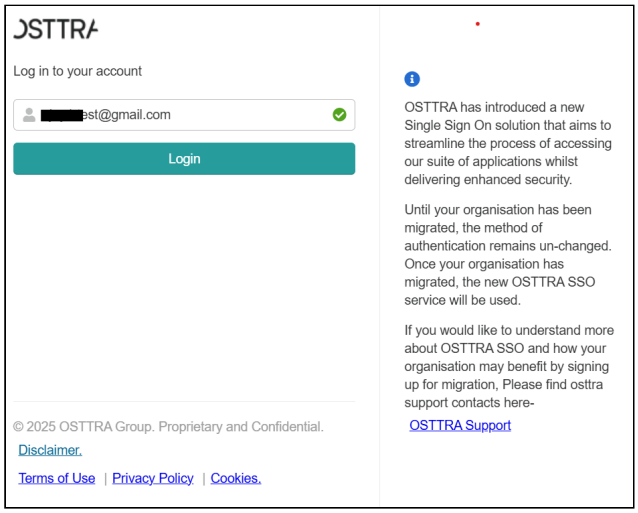
While non-federated users are member users on the OSTTRA B2B tenant and are onboarded via the sso.osttra.com domain, we do allow them to log in using their business email ID.

Since the mapping between the user's business email ID and login ID is maintained within OSTTRA SSO, users will receive the following information message:

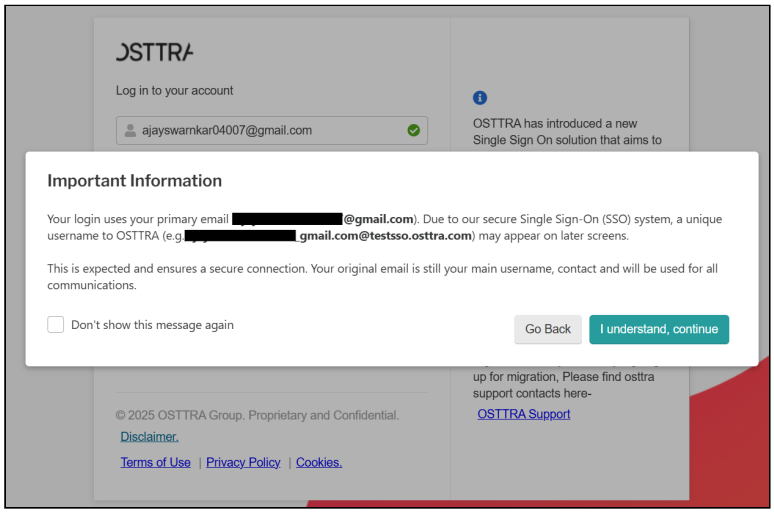


Q3. What is the non-fed user login journey?

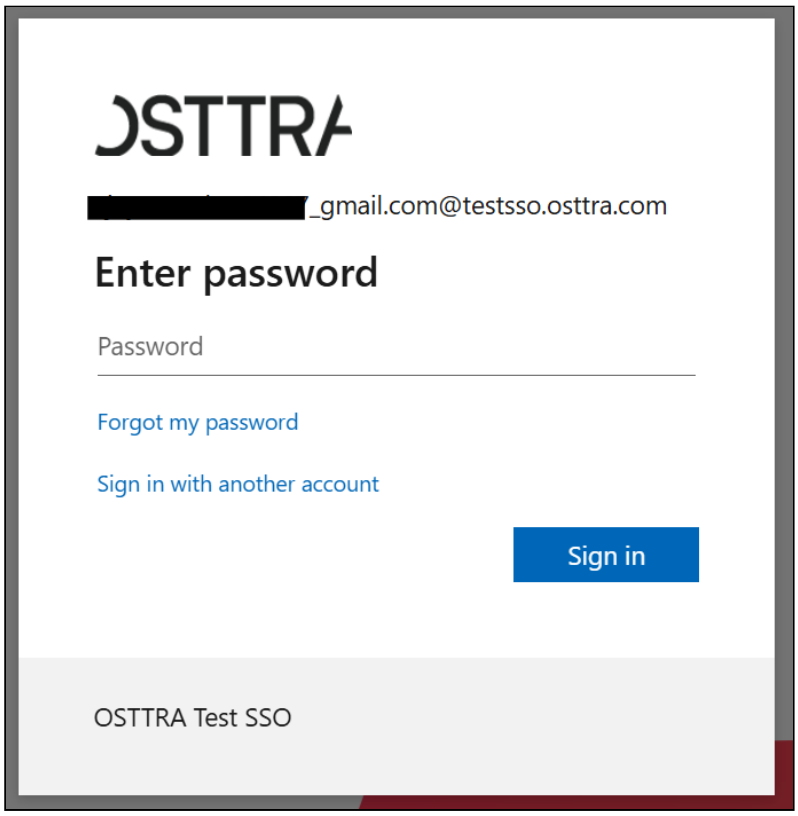
- Users can log in to the application directly by using the application login URL or via sso.osttra.com.
- Upon logging in, the user will be prompted to enter their email ID.



- Once the user click "Login," a prompt appears containing an important information regarding the login ID and user ID. Read this information and then continue to log in. Additionally, the user has the option to click "Don't show this message again" to prevent this pop-up from appearing on future logins.

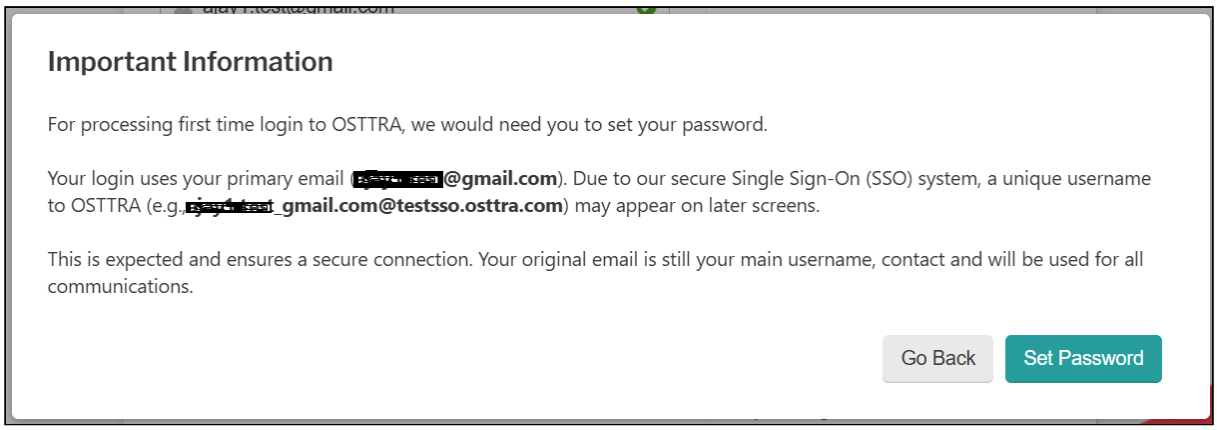


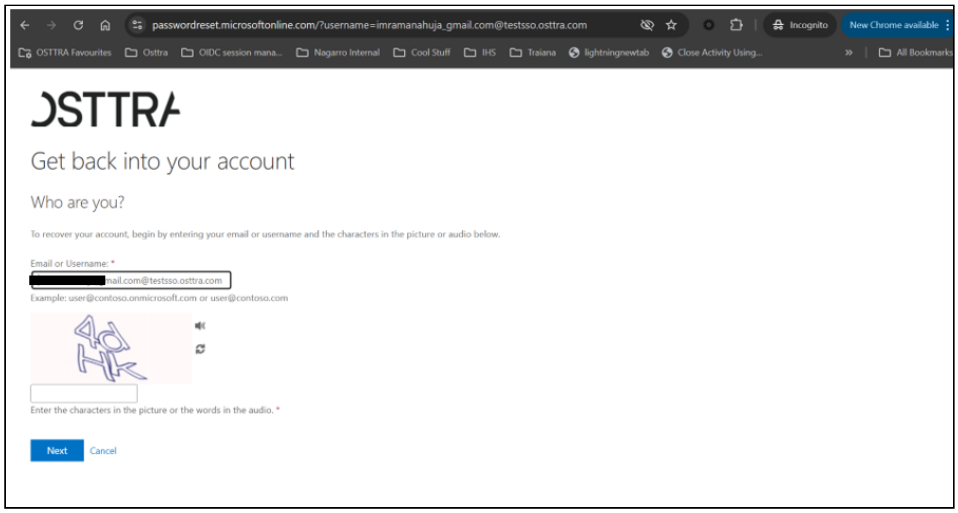
- User is required to enter the password and sign in to the application.

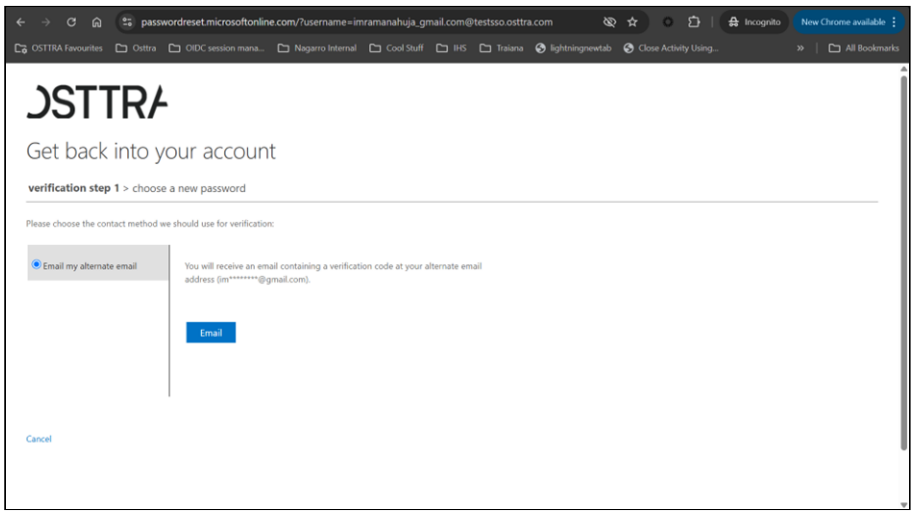


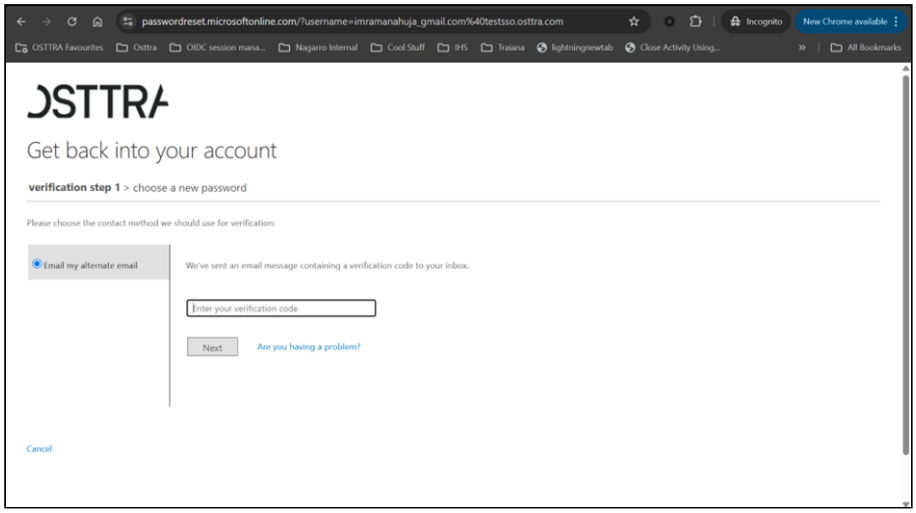
Q4. How user will get the password for first time login?

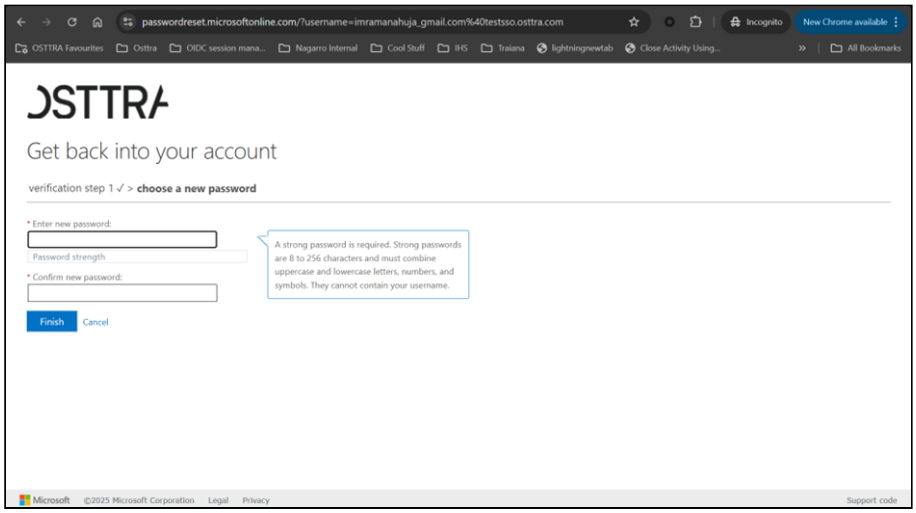
- For the first-time login, user will be asked to set up the password via Microsoft self-serve.
- Upon logging in, user will be prompted for password setup. User will then be asked to enter a One-Time Password (OTP) received on the business email.
- Once the password is set, relaunch the login URL.

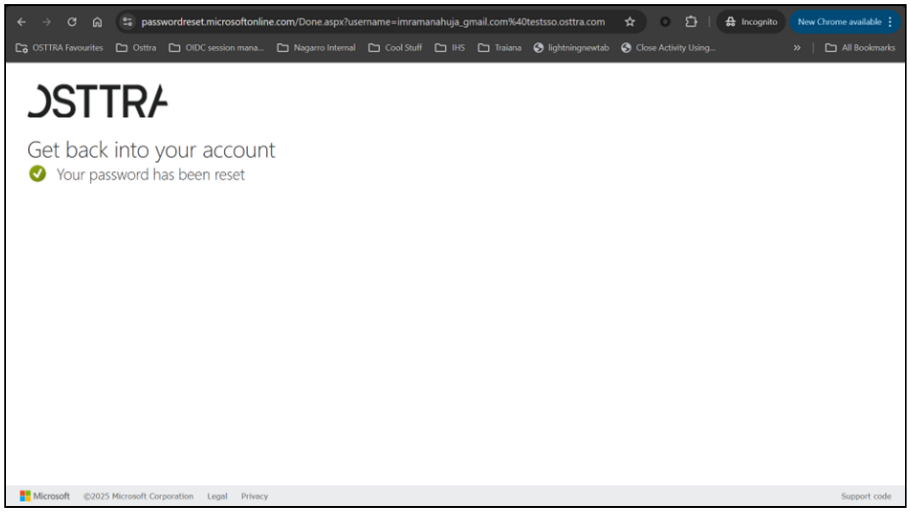












Q5. What is the password policy?

A non-federated user's password is managed in Microsoft Entra, and therefore the Entra password policy applies. Refer to the password policy of Azure Entra here.

Q6. Can I enable MFA for my non-fed account?

By default, Multi-Factor Authentication (MFA) is disabled for non-federated accounts. Users can opt for MFA (second-factor authentication) by raising a request with the OSTTRA support team. The only available option for MFA is the Microsoft Authenticator application on a mobile device, and control of MFA will remain with the OSTTRA team.

A customer-owned authenticator cannot be supported for non-federated users.

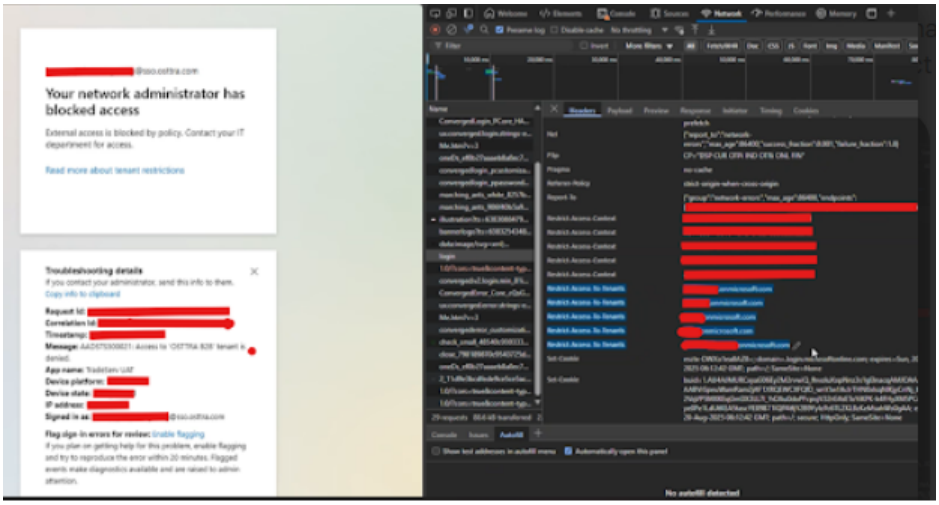
For Internal Usages: The support team needs to raise an SSOOB ticket with Entra team to enable the MFA.

Q7: Why some users are encountering any of the following access denial issues?

- AADSTS500021: Access to '<tenant>' tenant is denied.
- AADSTS500022: Access to '<tenant>' tenant is denied.

- Access to 'OSTTRA B2B' tenant is denied.

These errors occur due to traffic filtration at the network/firewall level on the client's end, which is implemented via Tenant Restriction version 1 [TRv1]. Refer to the screenshot of browser network logs for such an issue.



TRv1 is a network proxy-based solution that requires specific behavior: injecting HTTP headers such as "Restrict-Access-To-Tenants" and/or "Restrict-Access-Context" into Microsoft authentication traffic. It intercepts outbound HTTPS traffic. For example, traffic coming to the OSTTRA tenant from user's network. When users attempt to log into an Entra tenant not listed in their network allow-list via these headers, the Entra tenant (in this case, the OSTTRA tenant) refuses access. This can be verified by referring to the Microsoft documentation for tenant restrictions v1 at Use tenant restrictions to manage access to SaaS apps - Microsoft Entra ID.

To clarify, Tenant Restrictions TRv1 helps control user access to external tenants on the network, and as a result, it blocks access to the identity provider tenant, which is the OSTTRA tenant in this instance.

To resolve this issue, the network administrator needs to allow the OSTTRA tenant by adding it to the allowed tenant list using "Restrict-Access-To-Tenants" and/or "Restrict-Access-Context" headers. Please contact the network or IT team and request them to add the following details:

- Name: OSTTRA B2B
- Tenant ID: c0f79cf2-eac6-4f89-81a9-510a5688b4f0
- Primary Domains:
  - sso.osttra.com
  - ssoosttra.onmicrosoft.com

To further explain, OSTTRA applications leverage MS Azure Entra as an authentication solution. While a federation setup always requires outbound whitelisting in the Entra tenant (to federate as B2B guest collaboration), it also requires network-level whitelisting of the tenant in the network/proxy/firewall if the user has an active TRv1 network or proxy setup. This is equivalent to whitelisting a designated product URL.

> ⚠ Whitelisting the SSO domain on proxy/VPN to resolve TrV1 issue will not lead to our tenant getting the inbound access to customer resources.