Single Sign-On (SSO) Technical FAQs

Last modified on 30 July, 2026

Q1. How do I refresh my SAML certificates for an existing setup?

Refreshing your SAML certificates can be completed in one of two ways, depending on your configuration:

- **Self-Serve Refresh (Dynamic Metadata URL):** If you provided a SAML Metadata URL during setup, the process is fully automated. Simply update the certificate in your Identity Provider (IdP). OSTTRA's configuration will automatically fetch the updated certificate from your URL with no further action required.
- **Manual Refresh (via OSTTRA Support):** If you do not use a dynamic Metadata URL, send your updated SAML metadata file or certificate details directly to **OSTTRA Support**. The support team will coordinate with the backend team to update your setup.

Q2. I am currently a non-federated OSTTRA SSO user. What are the steps to migrate to SAML federation? Is there an environment to experience it before migration?

Migration Process: To migrate from your current non-federated setup to SAML, share your SAML metadata with OSTTRA support. We will then convert your domain configuration to SAML and migrate the underlying domain users to the Federated model.

We can schedule a downtime window to execute this change. During this time, a test user will be migrated to verify the authentication flow, after which we can proceed with the bulk user migration upon your approval.

Q3. I am currently an Entra federated OSTTRA SSO user. What are the steps to migrate to the SAML federation? Is there an environment to experience it before migration?

Migration Process: Similar to the non-federated to SAML migration, moving from Entra Federation to SAML requires you to provide your SAML metadata details to OSTTRA. You will also need to configure the corresponding OSTTRA-provided metadata within your Identity Provider environment.

Testing Environment: Once this is ready, we can schedule a downtime window to migrate a test user. After the test user verifies and approves the authentication flow, we can proceed with the bulk user migration.

Q4. How does OSTTRA handle users with multiple email domain aliases (for example, @domain.com Vs. @domain.co.uk) federated to the same IdP?

OSTTRA identifies users strictly by the exact email address attribute returned in the SAML assertion from your IdP.

Even if both domain aliases route to the same IdP, OSTTRA cannot automatically reconcile or alias two different email addresses. The email address returned by your IdP **must exactly match** the primary email address provisioned for that user account in OSTTRA.

Q5. Do I need to set up SAML configurations separately for each service and environment?

No, separate configurations are not required. OSTTRA uses a single SAML Service Provider (SP) setup across all client-facing environments, including both UAT and Production. Once integrated, this single SAML setup is valid for all environments and OSTTRA services.

Q6. What do I need to do to set up a federation?

First you need to confirm the Identity Provider (IDP) / Identity Access Management (IAM) solution you use. Your internal Access Management team or helpdesk should be able to help with this. The OSTTRA support teams will be able to provide details of the information that you need to capture. Once you have the correct

information / contacts within your organisation, the OSTTRA support team will be able to guide through the next steps.

In the instance your organisation is using Microsoft Entra (Azure), then the federated setup can be very simple. In many cases, a few simple configuration changes within the Entra platform allow you to federate with OSTTRA. OSTTRA support teams can provide documentation covering the exact steps needed for federation.

Q7. Why does OSTTRA require "Outbound Collaboration" to be enabled in our Microsoft Entra ID (formerly Azure AD) tenant?

Enabling **Outbound Collaboration** allows users to securely authenticate with OSTTRA applications using their existing corporate credentials. This configuration is strictly a **one-way trust relationship** initiated by your network.
Key security points include:

- **One-Way Traffic:** Communication is strictly outbound from the client system to OSTTRA.
- **No Inbound Access:** OSTTRA cannot access your internal resources, browse your directory, or enter your private network.
- **No Data Syncing:** OSTTRA does not synchronise or store your tenant's metadata.
- **User Control:** Retain full control over which specific users or groups are permitted to authenticate with OSTTRA services.

Q8. Does the OSTTRA SSO integration handle both Authentication and Authorization?

No. The SSO integration is used exclusively for **Authentication**.
Enabling SSO at the organizational level does not automatically grant your users access to OSTTRA services. We maintain a strict separation between verifying identity and granting permissions:

- **Authentication (Handled by Client):** Your Entra ID tenant confirms the user's identity. OSTTRA trusts this "digital handshake" to ensure the person logging in is who they say they are.
- **Authorization (Unchanged):** Access to specific OSTTRA applications, data, or functions will **remain unchanged** and will be managed as usual at the **application level**. You will keep on following the same process for user authorization, the one you are following today.
- **No Automated Provisioning:** OSTTRA does not use Entra ID to automatically provision roles or permissions. Even after a successful SSO login, a user will only see the services they have been specifically authorized to use by an OSTTRA administrator.

> ⚠ Since we are not provisioning authorization from Entra, there will be existing means to control access to specific applications. Therefore, there is no need to do specific application-based integration. The Entra application ids may change over time since Entra always assigns a new application id if it will be unregistered and re-registered.

Q9. What is the alternative if our organization does not allow Entra-to-Entra (B2B) Outbound Collaboration? Do we have an option to federate over SAML via Entra?

If your security policy restricts B2B Guest Collaboration, OSTTRA supports **SAML-based Federation via Entra** (often referred to as **Passive Authentication**). This allows for a secure SSO connection without requiring a direct B2B trust relationship between Entra tenants.
How it Works:
To prevent Entra ID from automatically triggering a B2B guest flow, we use a "Domain Masking" technique:

- **Custom Identifier:** Both organizations define a Conditional Access policy or use a specific sub-domain alias (for example, auth.yourdomain.com).

- **Bypassing Auto-Discovery:** Because this alias is not a primary verified domain in Entra, it prevents the systems from forcing a B2B collaboration flow, allowing them to communicate through standard SAML tokens instead.
- **Seamless User Experience:** Users continue to log in using their standard business email address. The technical routing happens in the background.

Benefits of this Approach:

- **Enhanced Isolation:** No guest user objects are created in the directory.
- **Standardized Security:** Fully supports your existing Multi-Factor Authentication (MFA) and Conditional Access policies.
- **Compliance:** Meets the requirements of organizations with "No External Collaboration" mandates while still providing the convenience of SSO.

Q10. How OSTTRA Entra (Azure) determines if a client is federated or not?

In the instance where your organisation is using Microsoft Entra (Azure), the OSTTRA Entra (Azure) tenant tries to federate **automatically** with your organisation's Entra, once your domain has been added to the OSTTRA Entra instance. This leverages inbuilt functionality within Microsoft Entra (Azure), and this is how Microsoft envisaged the service operating.

In the instance where your organisation is **not** using Entra (Azure) for access management, the integration has to be configured manually. In these cases, a One Time Password (OTP) becomes the default mechanism for logging in. Alternatively, your organisation's Access Management Team can work with our OSTTRA teams to set up federation.

Q11. How can I switch off the federation and instead opt for One Time Password (OTP)?

At present this option is only available for customers not using Microsoft Entra (Azure) as their IDP/ IAM. Read more about Tenant restriction here - https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/tenant-restrictions

In the case where you are **not** using Microsoft Entra (Azure), you may opt for OTP using your business email.

Q12. Can I connect Entra (Azure) to Active Directory (AD) over Security Assertion Markup Language (SAML)?

Microsoft Entra (Azure) does support connecting to Active Directory (AD) over SAML 2.0 directly with on-prem. Read more about connecting Entra (Azure) to AD over SAML here:

- https://learn.microsoft.com/en-us/entra/external-id/hybrid-cloud-to-on-premises
- https://learn.microsoft.com/en-us/entra/identity-platform/saml-protocol-reference

Q13. Can I integrate SSO into my internal applications portal?

Yes, this is possible, you can use the sso.osttra.com as a redirect URL while configuring the applications, which will authenticate the user in the background.

Q14. Does Entra (Azure) support audit of admin activities and how those audit logs can be accessed?

Yes, Entra (Azure) admin portal captures the audit activities as well as user sign-in logs. Only OSTTRA Azure admin can access them and can be provided on request. The default limit of retention of Audit and sign-in logs is 30 days. However, if required, these logs can be routed to Azure storage for a longer retention period.

Q15. Can I configure OSTTRA application in my (clients) IDP dashboard?

Yes, it is possible to configure the OSTTRA application URL in clients IDP dashboard. You need to create the application link in your IDP dashboard, which will be provided by OSTTRA. You can create an application icon/tile that will point to OSTTRA application URL. Alternatively, you can bookmark the application URL and launch it directly.

Q16. Are your applications SaaS offerings?

No, OSTTRA applications are not typical SaaS offerings. They are designed to integrate exclusively with OSTTRA **Azure AD B2B (or Microsoft Entra Workforce) tenant** for Single Sign-On (SSO) capabilities.

OSTTRA Azure AD B2B can be linked with your organization's corporate identity provider to streamline access.

Q17. Can we configure your application using SAML metadata on our Identity Provider (IDP)?

No, OSTTRA applications are not traditional SAML offerings. OSTTRA application can only integrate with OSTTRA IDP, which is Azure AD B2B (Microsoft Entra Workforce).

External Azure IDPs can only federate through B2B guest collaboration.

However, if your corporate identity provider is also Azure AD (Microsoft Entra Workforce), Microsoft requires that B2B cross-tenant collaboration be enabled for the two Azure AD B2B instances to integrate, regardless of whether you are using B2B collaboration, SAML, or WS-Fed.

If your corporate identity provider is not Azure AD, then B2B SAML integration between OSTTRA and external IDP is possible in the standard way.

Q18. How B2B guest collaboration is different than B2B direct connect?

B2B direct connect i.e. full cross tenant whitelisting provides you an option to synchronize user metadata, directories, and security groups across two Azure Entra tenants. **OSTTRA is not asking for B2B direct connect**.

OSTTRA requires to have a very limited cross-tenant access i.e. **B2B collaboration** enabled from clients IDP (to access sso.osttra.com) so that client users can login into OSTTRA SSO through their business email ids. By default, Microsoft Entra keeps it enabled. Enabling this is really safe and secure as only traffic towards OSTTRA tenant has to be enabled. OSTTRA tenant would not be accessing any data from customer tenant except the session token to validate user/ login. OSTTRA would not be fetching or keeping user metadata, except keeping the users as guest i.e. aliases of users.

Q19. How can we enable SSO with your application?

SSO can be enabled by integrating your IDP with our Azure AD B2B tenant. Depending on your IDP setup, there are different ways Azure AD B2B can establish this connection.

Q20. In what ways can Azure AD B2B integrate with our IDP?

Azure AD B2B can integrate with your IDP in two ways:

- **If your IDP is not on Azure AD**: integration will only work with SAML or WS-Fed compatible IDPs.

- **If your IDP is on Azure AD**: you can use the Azure AD B2B Collaboration feature to allow inbound authentication requests from our tenant (sso.osttra.com).

Q21. What should we do if our employee IDP is not on Azure AD?

If your employee IDP is not on Azure AD, Azure AD B2B can only integrate with any SAML or WS-Fed compatible IDPs to enable SSO.

Q22. What if our employee IDP is already on Azure AD?

If your IDP is on Azure AD, you can enable SSO using the Azure AD B2B Collaboration feature. This just requires you to allow outbound collaboration from your tenant to share your authenticated session details inbound to OSTTRA B2B tenant. Your site will remain secure since you are only opening outbound access and keeping the inbound access disabled for OSTTRA. We are not enabling any M365/O365 suites or services for your users at OSTTRA B2B tenant.

Q23. What is the difference between Azure AD B2B Collaboration and B2B Direct Connect?

- **B2B Collaboration**: This is the feature you need to enable SSO. It allows scoped access for specific users, groups, and applications. You can set a default configuration for all external organizations or create organization-specific settings.
- **B2B Direct Connect**: This feature establishes a mutual trust relationship between Microsoft Entra organizations, but OSTTRA is not supporting this.

Q24. What type of IDP settings should we enable for SSO?

You should enable **B2B Collaboration**, which will allow scoped access for specific users, groups, and applications. This is the configuration needed to enable SSO between your IDP and our Azure AD B2B tenant.

In this setup, OSTTRA will enable inbound settings for your Azure AD domain, while you will need to enable outbound settings for sso.osttra.com domain.

Q25. Are there any risks in enabling B2B collaboration feature on your Azure AD?

Enabling B2B collaboration allows two Azure AD B2B (Entra Workforce) instances to establish trust and enable SSO federation.

This collaboration is designed to be secure on your end, with several benefits:

- Establishes a trust relationship between the two Azure AD instances.
- Avoids user duplication, as no new user accounts are created. Users do not need to go through an account activation process.
- Users can log in using their existing credentials, so there is no need to remember additional credentials.
- You maintain control over MFA, conditional access policies, and corporate device policies according to your cybersecurity standards.
- Allows you to create user groups to manage which employees can access our instance. You can also regularly review, and revoke access as needed.
- Provides control over which verified Entra domains you choose to federate with.
- When an employee leaves your organization, they are disabled in your Azure AD, and their access to our applications is automatically revoked.

Q26. What controls OSTTRA have at your end for such B2B Collaboration?

OSTTRA have several features to manage and control access:

- We can specify which B2B tenants we collaborate with.
- We can control access to our applications by assigning permissions through AD groups and roles.
- We could verify if the user authenticated with MFA and deny access if MFA was not used.
- We can periodically review access and confirm if external users should still have access to resources. We can also remind users to renew their access.
- Control who can invite guests to the tenant by limiting invitation rights to specific users or admins, ensuring that only authorized personnel can onboard new guests.
- Control which guest user attributes are visible to the organization and limit unnecessary data exposure.
- Require guests to adhere to privacy policies that govern the use of organizational data. This helps ensure compliance with data protection regulations, such as GDPR or CCPA.
- Azure AD provides audit logs that capture guest user activity, such as sign-ins, role assignments, and access requests. This enables admins to monitor and investigate suspicious or unusual guest activities.

Q27. We are concerned that our employee information will the exposed to you if we enable B2B collaboration.

OSTTRA only receive a limited set of basic user information for the guest user:

- Display Name
- Email Address
- User Principal Name
- Identity Provider (your corporate Identity Provider domain)
- User State (indicating if the invitation has been accepted or is pending)
- Timestamp of User State changes
- Last sign-in date, created date, and last modified date
- Whether the user signed in with MFA

You may choose to include additional information using custom claims, but this information will not be used in any way on our end.

```
{
  "id": "federated-user-id",
  "displayName": "John Doe",
  "userPrincipalName": "john.doe#EXT#@tenant.onmicrosoft.com",
  "mail": "john.doe@partnerdomain.com",
  "userType": "Guest",
  "externalUserSource": "Federated",
  "identityProvider": "partnerdomain.com",
  "userState": "Accepted",
  "userStateChangedOn": "2023-08-21T12:34:56Z",
  "conditionalAccess": {
    "mfaRequired": true
  },
  "lastSignInDateTime": "2023-08-21T12:34:56Z",
  "createdDateTime": "2023-01-01T10:00:00Z",
  "lastModifiedDateTime": "2023-08-01T10:00:00Z"
}
```

Q28. How can you control which users and groups have access through B2B Collaboration?

Azure AD B2B Collaboration allows you to scope access to specific users, groups, and applications.

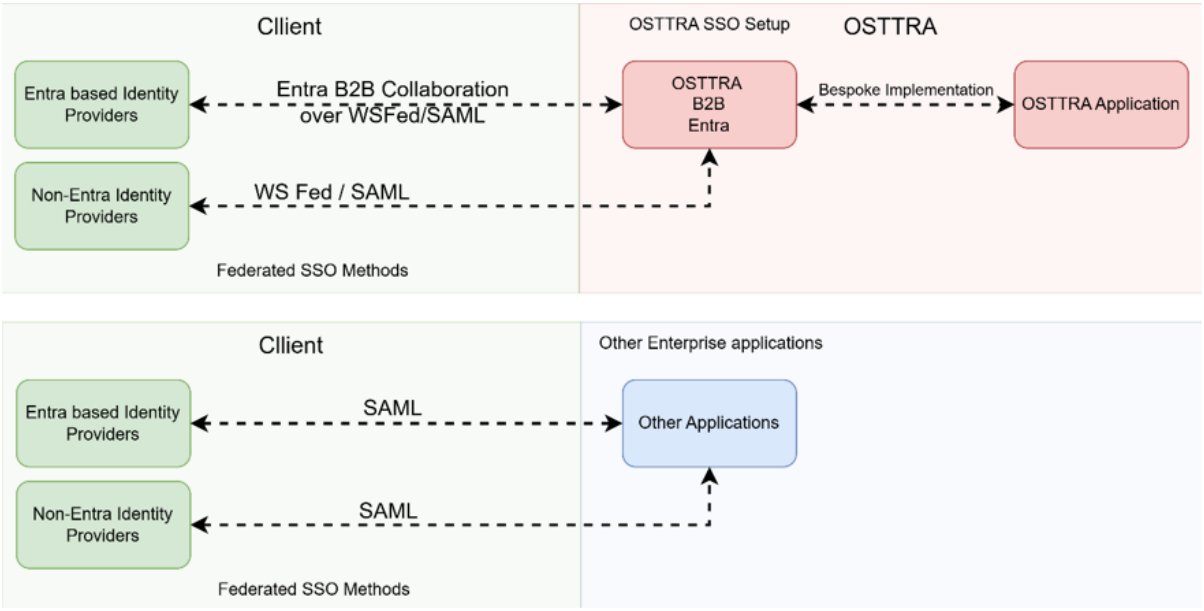
In your Azure AD tenant for the users who need access to our sso.osttra.com tenant, you can use either of the following options to enable:

- all users,
- *or* individual users,
- *or* user groups

Q29. We have never done this before. We have other enterprise applications that integrates fine with SAML solution.

As mentioned, OSTTRA applications differ from traditional enterprise or SaaS applications that can directly integrate with your Azure AD instance. These are designed to work specifically with our Azure AD B2B instance, which then requires setting up an identity federation with your identity provider for secure access.

This setup is distinct from typical Azure AD Marketplace applications, which function as SaaS services, or from B2C applications that utilize social media credentials or Microsoft Entra External tenants as the identity provider.



Q30. How OSTTRA support MFA setup for federated and non-federated clients?

OSTTRA strongly recommends and supports MFA setup for both federated and non-federated clients.

Mostly federated clients manage the MFA setup at their IDP, but OSTTRA ENTRA ID can also define policy to support MFA on clients' behalf.

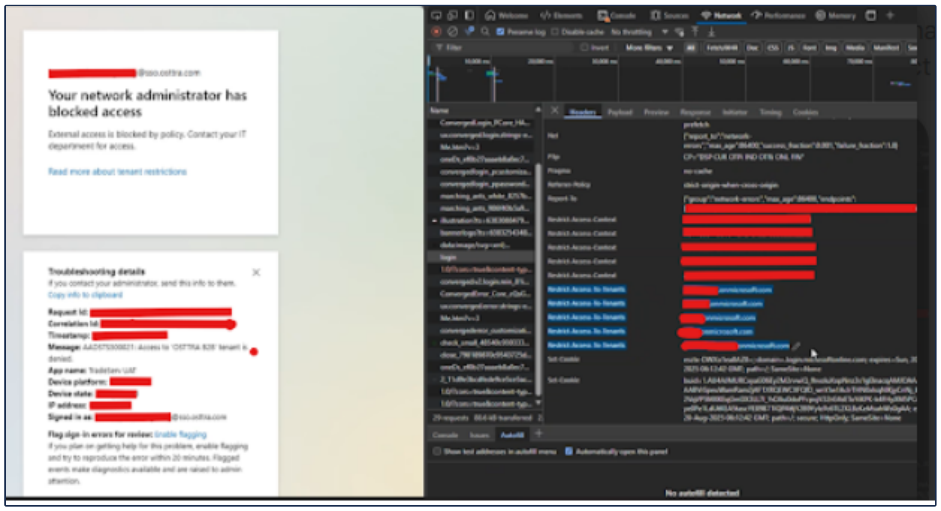
For non-federated clients, OSTTRA offers the MFA setup to client on first time login. This ensure a secure and hassle-free login experience to the user.

In addition, user can choose number of options to setup the MFA including text message, authenticator app, and so forth. However, OSTTRA recommends to choose Microsoft Authenticator as a default MFA authenticator application.

Q 31. Why a few users face any of the following issues?

- AADSTS500021: Access to '<tenant>' tenant is denied.
  or
- AADSTS500022: Access to '<tenant>' tenant is denied.
  or
- Access to 'OSTTRA B2B' tenant is denied.

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



TRv1 is a network proxy-based solution that requires very specific behaviour: injecting HTTP headers such as "Restrict-Access-To-Tenants" and/or "Restrict-Access-Context" into Microsoft authentication traffic. It intercepts outbound HTTPS traffic only, for example, in given case, the traffic coming to OSTTRA tenant from the user's network. When the users attempt to log into an Entra tenant not listed in their network allow-list via said header/s, the given Entra tenant (in this case, OSTTRA tenant) refuses access. The same can be verified by referring Microsoft documentation for tenant restrictions v1 @ https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/tenant-restrictions

To clearly explain, Tenant restrictions TRv1 helps to control users access to external tenants on their network. Therefore, blocks access to identity provider tenant i.e. in this case the OSTTRA tenant.

To resolve this, user's network admin has to allow OSTTRA tenant by adding the same in allowed tenant list as "Restrict-Access-To-Tenants" and/or "Restrict-Access-Context" headers. Please contact your network or IT team and request them to add the following:
Name: OSTTRA B2B
Tenant ID: c0f79cf2-eac6-4f89-81a9-510a5688b4f0
Primary Domains:
sso.osttra.com
ssoosttra.onmicrosoft.com

To understand this more, OSTTRA applications are leveraging MS Azure Entra as authentication solution. While federation setup ALWAYS needs an outbound whitelisting in customer's Entra tenant (to federate as B2B guest collaboration), it also requires network level whitelisting of tenant in customer's network/proxy/firewall if customer 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 does not require our tenant getting the inbound access to customer resources.