Single Sign-On (SSO) Technical FAQs

Last modified on 08 November, 2024

Q1: 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.

Q2: 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.

Q3: 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.

Q4: 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

Q5: 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.

Q6. 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.

Q7. 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.

Q8. 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.

Q9. Can we configure your application using SAML metadata on our Identity Provider (IDP)?

Yes, Azure AD B2B (Microsoft Entra Workforce) supports integration via SAML.

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, the SAML integration is possible in the standard way.

Q10. 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.

Q11. 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).

Q12. 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.

Q13. 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 inbound authentication requests from our B2B tenant (sso.osttra.com).). We can do this explicitly with SAML as well, however, Microsoft requires that B2B collaboration feature must be enabled to allow SAML between two Azure AD tenants. Default B2B collaboration also uses SAML under the hood, but Microsoft takes care of the integration.

Q14. 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.

Q15. What type of cross-tenant 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.

Q16. 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.

Q17. 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.

Q18. 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"
}
```

Q19. 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.

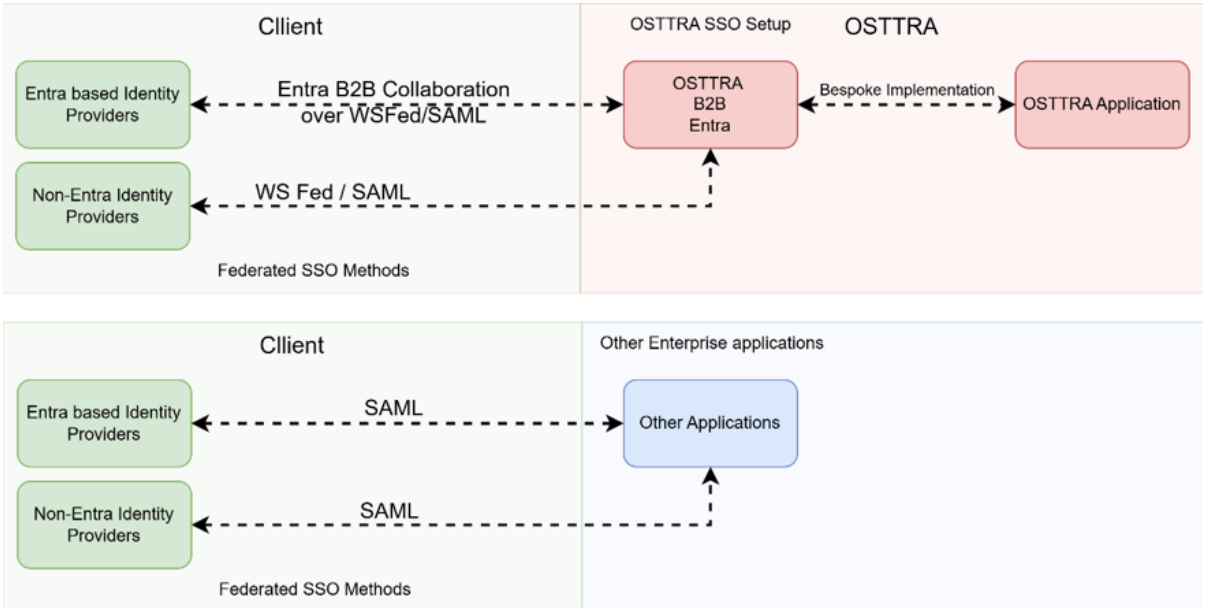
In your Azure AD tenant for the users who need access to our sso.osttra.com tenant, you can use either of the following options to enable:

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

Q20. We have never done this before. We have other enterprise applications that integrates fine with SAML without cross tenant whitelisting.

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.



Q 21: 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.