Single Sign-On (SSO) Technical FAQs

Last modified on 25 October, 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, our applications are not typical SaaS offerings. They integrate exclusively with our Azure Active Directory (Azure AD) B2B tenant (Microsoft Entra ID), which is necessary for Single Sign-On (SSO) functionality.

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

No, we do not provide SAML metadata for clients to configure on their IDP. Instead, we enable SSO by integrating our Azure AD B2B tenant with your IDP.

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). 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 we are 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.

Q16. 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