Single Sign-On (SSO) Technical FAQs

Last modified on 19 July, 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.