SSO - Azure/Entra Enable External Client

Last modified on 15 January, 2026

OSTTRA

1 Introduction: B2B guest collaboration v/s 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 won't be accessing any data from customer tenant except the session token to validate user/login. OSTTRA won't be fetching or keeping user metadata, except keeping the users as guest i.e. aliases of users.

2 Guide: External collaboration setup

When OSTTRA Azure tenant tries to collaborate with external client's Azure tenant, it may be external tenant's B2B collaboration settings blocks the collaboration and federation. This guide is to show how to verify and switch on the required settings in Azure to allow external collaboration.

> Prerequisite: The external clients must whitelist ***.osttra.com** at their network and firewall level to ensure osttra.com and its subdomains are allowed on the client network.

1. Open https://entra.microsoft.com
   Go To Identity → External Identities → Cross-tenant access Settings
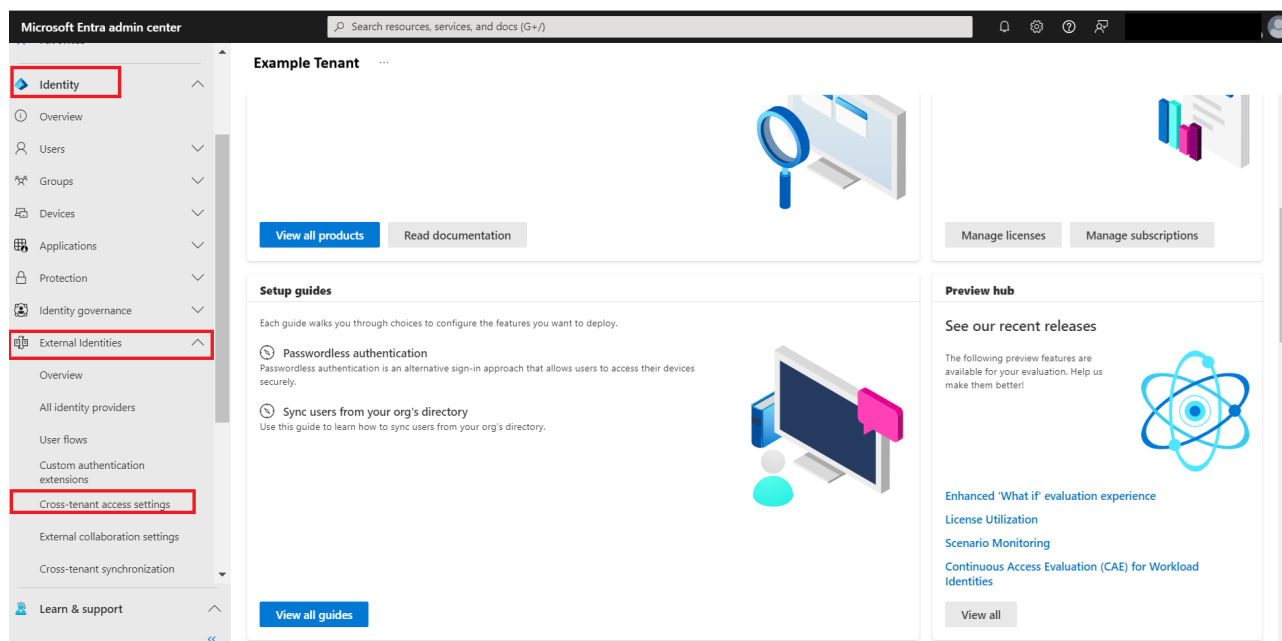
2. Check the Outbound access setting if status is "**All allowed**" then you are good to federate, no further action is required. Liaise with OSTTRA support to test the user setup. If its "*All blocked*" or "*limited access*" then follow the guide to enable the collaboration.
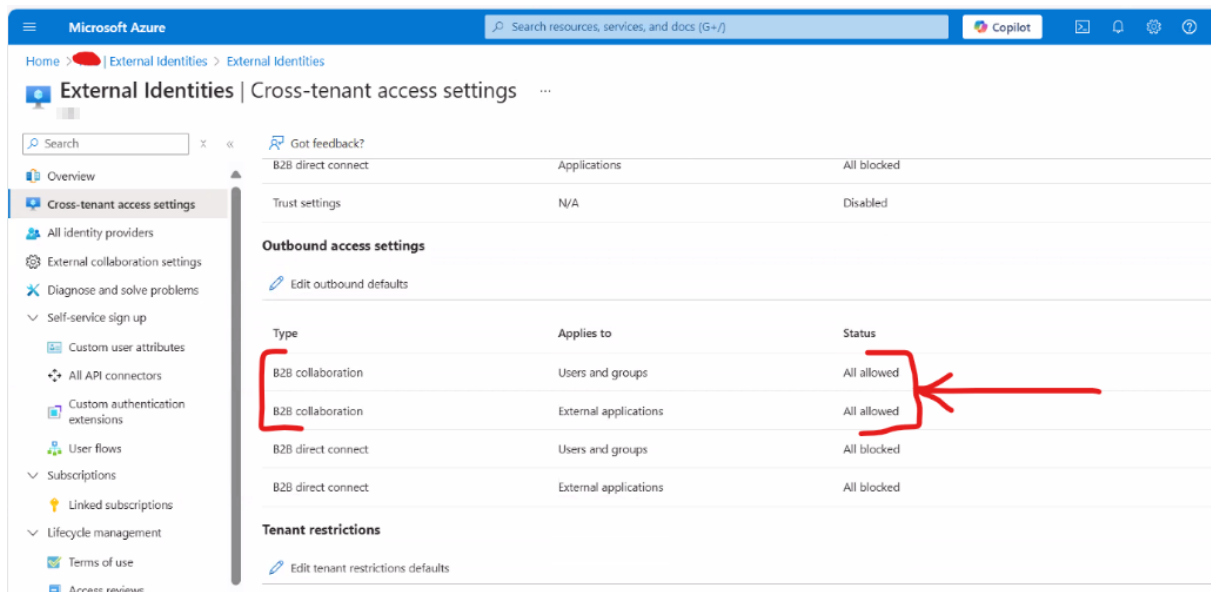
OSTTRA

3. Click Organizational Setting and Add Organization.

Where you see 'Example Tenant' , you will see name of your own tenant

4. Enter sso.osttra.com in the field that asks for "Tenant ID or domain name" and Click Add.
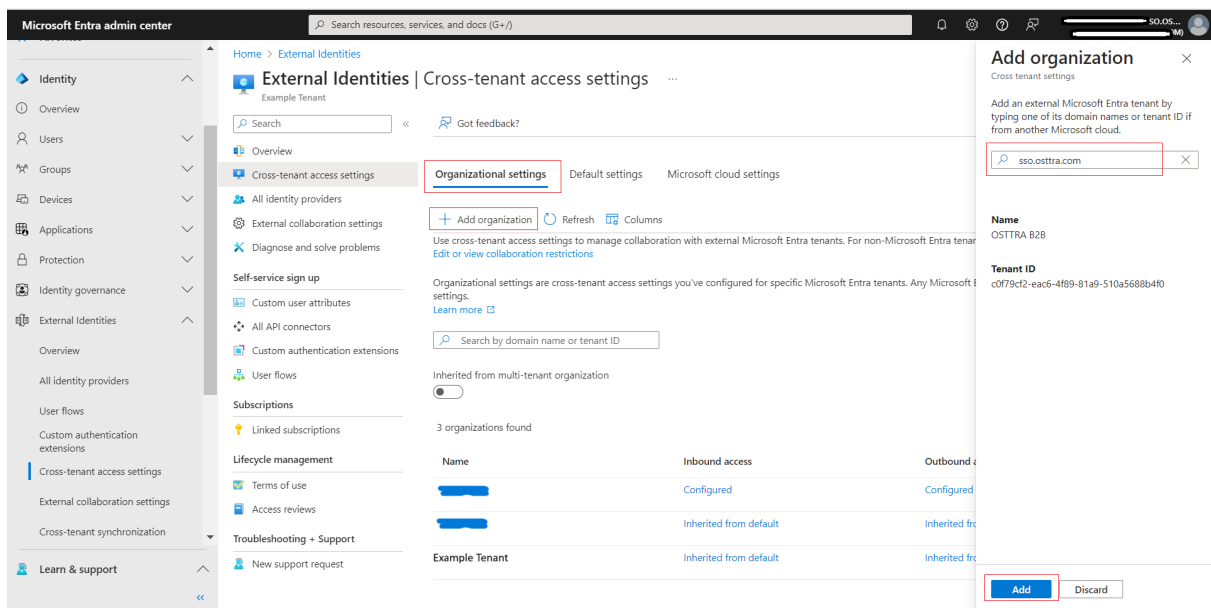
5. Click the link "Inherited by default", in the column Outbound access on the line that says OSTTRA B2B in the Name column.

6. On the B2B Collaboration tab, click Customize settings under Users & Groups and choose Allow access (this can be scoped to a specific group on the tenant.)

you can specify your AD groups that will be able to use this outbound setup , or you can allow the setup for your whole tenant , this would depend on your company security policies.

7. On the same page, click External applications tab and select Allow access.

8. By default, B2B Direct Connect is blocked and We don't support B2B Direct connect so make sure it's blocked. Select Trust and check 'Automatically redeem invitations with Osttra B2B Tenant'.