JSTTRA

Quick Setup Guide - Single Sign-On (SSO)

Last modified on 03 December, 2024

JSTTR

This Quick Setup Guide helps you to understand:

- Getting access to Single Sign-On (SSO) through an access package.
- Setting up a Multi Factor Authentication (MFA).
- Logging into various applications and navigate them through UI.

Getting access to Single Sign-On (SSO) through an access package:

This section applies only if you have been provided with a link to an access package, which is applicable to certain applications. Note that the access packages are only available for a limited set of applications, and Operations will not necessarily send you an access package for all applications. Alternatively, you may be self-onboarding to SSO.

- Prior to performing the following steps, make sure that you have an existing account created by OSTTRA Operations in an underlying platform (CFD, for example).
 - OSTTRA support representative will provide you a link to an access package that is specific to an application. By accessing the link to that access package, you will be able to complete your setup. The link to an access package looks as follows: https://myaccess.microsoft.com/@sso.osttra.com#/access-packages/d7436c94-0e53-436b-a5da-3216fa3xxxxx
 - 2. Enter your email address and click Sign In.



If your setup is federation (using your own identity provider - not managed by OSTTRA), then follow the prompts on the screen. However, if you are leveraging OSTTRA for user management, the following screen appears.

JSTTRA	
←e@gmail.com	
Enter code	
We just sent a code toe@gmail.com	
Enter code	la.

OSTTRA uses One Time Passcode (OTP) to validate users, this is a more secure way of accessing the services than the traditional username and password.

3. After providing your email, a One Time Passcode (OTP) is sent to your email that you will need to enter.

The example of the email you receive:

Your OSTTRA B2B account verification code 🔉 🔤			₽	ß
OSTTRA B2B (via Microsoft) <account-security-noreply@accountprotection.microsoft.com> to me -</account-security-noreply@accountprotection.microsoft.com>	15:27 (1 minute ago)	☆	¢	:
OSTTRA B2B				
Account verification code				
To access OSTTRA B2B's apps and resources, please use the code below for account verification. The code will only w	ork for 30 minutes.			
Account verification code:				
31108190				
If you didn't request a code, you can ignore this email.				
← Reply → Forward				

4. After you have entered the OTP, you will be prompted to accept the following permissions:

Microso	ft	
jpampellonne@	@gmail.com	
Permissio	ons requested	d by:
Ssoosttra	B2B a.onmicrosoft.com	
By accepting, y	ou allow this organis	sation to:
✓ Receive you	r profile data	
✓ Collect and	log your activity	
V Use your pro	ofile data and activity da	ata
You should only ac has not provided can update these p https://myaccount Learn more	ccept if you trust OSTTRA links to their terms for y permissions at .microsoft.com/organizati	B2B. OSTTRA B2B you to review. You ions.
This resource	is not shared by Mi	crosoft.
	Cancel	Accont

- 5. OSTTRA requires a Multi-Factor Authentication (MFA) to access applications or resources. You will be guided to provide more information and to complete MFA using the tool of your choice.
- 6. Once you have successfully authenticated the setup, the Access packages screen appears asking which packages you want to access; the packages available will be determined by what your organisation has been set up for. Choose the appropriate package, for example, to gain access to CFD UAT, select the AccessPkg UAT-CFD-OSTTRA package encircled below:

	Access packages	ons, and more in a single package. Select from the fo	llowing packages, or search to find what you're looking	1 for.	
Access packages	Available (1) Active (6) Evolved (0)				
Request history					
🞗 Approvals	Name ↓	Description	Resources	Actions	
	AccessPkg-UAT-CFD-OSTTRA	CFD UAT Access Package	APP-UAT-CFD-OSTTRA	Request	
I Access reviews					
R Give feedback					

JSTTR

7. Once your request is completed, a message appears saying your request has been successful.

From the point of requesting the application access to its availability, there could be a delay of several minutes.

Setting up a Multi Factor Authentication (MFA):

When a user is set up with federation, a customer's IDP will manage the Multi Factor Authentication (MFA) setup. In case a customer's IDP is not set up for MFA or the MFA setting is off in the IDP, the OSTTRA Azure tenant will enforce the MFA setup the first time that user logs in.

When a user first logs into an application through SSO, the user will be prompted to set up MFA. Users can follow on screen instructions to set up the MFA of their choice.

1. On first time login, the system will prompt to set up MFA.

	com
More inf	ormation required
Your organisat your account s	tion needs more information to keep secure
Use a differen	t account
Learn more	

2. Users will be asked to choose the authenticator app. By default, the system tries to set up Microsoft Authenticator, however, the user can choose a different authenticator app as well.

	Keep your account secure
Microso	oft Authenticator
•	Start by getting the app On your phone, install the Microsoft Authenticator app. Download now After you install the Microsoft Authenticator app on your device, choose "Next".
	Next

3. Assuming a user selected the Microsoft Authenticator app and clicked **Next**, the system will prompt to set up the account. Click **Next**.

	Keep your account secure
Microso	oft Authenticator Set up your account If prompted, allow notifications. Then add an account, and select "Work or school".
-	Back Next

- 4. For any other authenticator app follow the steps on the screen.
- 5. Users will be asked to scan the QR code or can set up the account manually by clicking **Can't Scan image?**.

Keep your account secure
Microsoft Authenticator
Scan the QR code
Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.
After you scan the QR code, choose "Next".
Can't scan image?
Back Next

6. Click **Next**, the user will be asked to verify the code in the authenticator app.

	Keep your account secure
Microso	oft Authenticator Let's try it out Approve the notification we're sending to your app by entering the number shown below. 76 Back Next

7. After verification, the notification approved message appears. Click Done.

Keep your account secure	Microsoft Authenticator app was successfully X registered Wed, 27 Nov 2024 05:30:37 GMT
SUCCESS! Great job! You have successfully set up your security info. Choose "Done" to continue signing in. Default sign-in method: Microsoft Authenticator	Done

The user is successfully setup for MFA.

Logging into various applications through SSO and navigate them through UI:

 Users can continue to access the application login URL directly and an option will be available to login via SSO. Alternatively, user can follow the https://sso.osttra.com link and select the account you are logging into - it will be the email address associated with the main account, which is set up by OSTTRA Operations. Enter your login credentials. If you do not have the federated setup, a One Time Passcode will be sent to your email address. Use that passcode to login followed by MFA authentication.

. · · · · · · · · · · · · · · · · · · ·	JSTTRA	
	←@osttra.com	
i gan in	Enter password	
	Password	
	Forgot my password	
	Sign in	1
	Osttra - The future of Post Trade	

2. If the user directly logs in to the application via the application URL then the user will logged in to the application. If the user logged in via sso.osttra.com then user will be directed to OSTTRA applications

page, where you can select the application, you would like to access:

Apps dashboard	I.			🕂 Add apps	ection 🎾 Customise view
CUSTOMER APPS PROD	UCTION UAT Apps				
✓ CUSTOMER APPS					Settings
	<u>f</u>				
PROD-CFD	PROD-CSM	UAT-CFD	UAT-CSM		
> PRODUCTION					Settings

3. In this screen, you can create your own groups of applications by clicking **Create Collection** at the topright corner. For example, here a group called "CUSTOMER APPS" has been created.

A	 OSTTRA utilises Microsoft Azure technologies, which are commonly used within customer organisations. To do this, OSTTRA has created a specific OSTTRA B2B tenant in which it hosts all its customer facing applications and users. A tenant is a way of storing records and authorisation information of users. You may notice that the URL you originally entered sso.osttra.com has changed to http://myapplications.microsoft.com C C C myapplications.microsoft.com If your organisation uses http://myapplications.microsoft.com, then it may be necessary to switch between your organisation's tenant and the OSTTRA tenant. This can be achieved be 			
	Selecting the organisation ic	Con at the top-rig	ht corner of the window	Øb ? Organisations Select an organisation below to sign in. You're signed in with:
	CUSTOMER APPS	UAT-CFD	: -csm	OSTTRA 828 Other organisations you belong to: Osttra