3rd Party Access via Azure B2B

Guide for Sponsors

Cognizant Oil and Gas Consulting Services Norway AS
Snarøyveien 36, PO Box 222, 1326 Lysaker, Norway
Tel: +47 67 59 50 00
Registered in Norway, registration no. NO 984 755 384 VAT

1. General information

1.1 What is 3PA?

3PA stands for Third Party Access. The 3PA service provides external parties with access to internal applications. External Users will be invited to join Aker Solution Azure AD Tenant and then they can gain access to the on-premise 3PA applications using their Shadow Accounts

1.2 What will the invitation email look like?

Hello
You have been invited to the Aker Solutions Partner Service Portal to allow you to access some of our Applications as a Third Party (3PA) user.
To register for access, please have your registered mobile device ready and then follow the invitation process that will be emailed to you from Microsoft Invitations invites@microsoft.com

NB: You will be using your current business Office 365 subscription details for this registration and not the 3PA credentials supplied by us.

Need Help?
If you require support when accessing the network remotely you can contact the global IT Service Desk.

The Global IT Service Desk covers all regions. You can call the Service Desk 24 hours per day, seven days per week, all year round using any of the regional contact numbers and speak to an agent.

Norway	+47 51 85 22 00
Malaysia	+603 2300 5200
UK	+44 (0) 1224 287 287
US	+1 713 596 4357
US (Toll free)	866 401 8847
Brazil	+55 41 2102 4370

You can also contact IT: service.desk@cognizantog.com

Aker Solutions Partner Services Team

1.3 What are Shadow Accounts?

Shadow account of the same Guest User gets created at on-premise active directory, via a B2B powershell script, automatically. This shadow account is basically a footprint of the invited guest at on-premise domain. The B2B powershell script is maintained by the Cloud Ops & Directory Services Team.

The "shadow account" will be created in the below format:
User Principal Name (UPN): firstname.lastname_guestdomain.com#EXT#@tenantname.onmicrosoft.com

Example:
User Principal Name (UPN): john.doe_contoso.com#EXT#@tenantname.onmicrosoft.com
SAM Account Name: 1st 20 characters of the UPN above (john.doe_contoso.com)
Display Name: Last Name, First name
Email : john.doe_contoso.com#EXT#@tenantname.onmicrosoft.com

After the shadow account has been created & the cost code has been updated by security team in ARCA, you will need to request access to the specific 3PA application/SPS. See list in Self Service Catalogue -> Place an order.

Note: You will have to use the SAM Account Name of the Shadow account to raise an application access request for the Guest User.

1.4 Roles and responsibilities

Sponsor – you as a requester

The sponsor responsibility is to:

- Request a new 3PA service.
- Request a Risk Assessment if the application is not already hosted on the 3PA platform (only for application. - Participate in the start-up meeting with the Service Provider (SDM and Solution Architect).
- Request new end user accounts.
- Ensure Guest Users configure Muti-Factor Authentication as soon as possible and agree to Terms of Use.
- Failing to configure Multi-Factor Authentication within 15 days of requesting access to an application may end up in deletion of the guest account. Access request needs to be initiated all over again.
- Request access for end user (after account has been created) to specific application.
- Request demobilization of the user accounts, or remove end user access to specific applications if the end user subscribes to more than one 3PA service.

In addition to above requests (all available via IT Self Service Portal), the sponsor is required to take the coordination role between Cognizant and the 3rd party/end user, by collecting all data in order to create the end user accounts.

If end users are facing problems with the login, they can call the Service Desk directly. See point 3 for more information:

SDM 3PA services

The SDM responsibility is to:

- Coordinate order requests for new services (application), organize required start-up meetings and follow up from start till delivery.
- SDM can assist the sponsor on how to order, what needs to be ordered, time and cost estimate.
- Handle any queries regarding cost or the service.
- License management.

Solution Architect

The Architect responsibility is to:

- Participates on sponsors -, SDM/TSM- and Security-team meetings after a new 3PA service (application) is requested,
- Create the required design document for the new 3PA service.
- Help with troubleshooting and testing of the new 3PA Service.

3PA Support

The 3PA support team responsibility is to:

- Create the Change for the new services, coordinate tasks with other involved teams and test before release.
- End user communication.
- Establish and maintain User Manuals and email templates that are being sent out to customer.
- Create end user accounts.
- Token provisioning.
- Reset passwords.
- Grant 3PA access to end users via Arca (additional access to the specific application must be granted by application team responsible).
- Coordinate distribution of hard tokens if required (only for end user without mobile network).
- Support and troubleshoot incidents raised by sponsor or 3PA end user.
- Lifecycle management.

By calling Service Desk (see contact in point 3), they can support on following:

- 3PA: RFI - How do I log in?
- 3PA: user phone number change request
- 3PA: unable to access login page
- 3PA: user account password reset
- 3PA user email change

End user from 3rd parties

The end user responsibility is to:

- Provide required end user information to sponsor in order to create a 3PA account, access and provisioning token.
- Accept the Terms and Conditions send in email in order to share the 3PA password, (Three strike rule before the request is closed from our end).
- If any problems with log-in, or questions about the access or token types, end user can contact the 3PA Services support team by sending an email to 3PA.Support@cognizantog.com or service.desk@cognizantog.com
- Report back to sponsor when the 3PA access is no longer required.
- Return hard token to the sponsor.

SDM for Application

The application SDM responsibility is to:

- Participates on SDM/TSM- and Security-team meetings after a new 3PA service (application) is requested.
- Participate on testing before a new 3PA Service is released.
- Grant end users access to the application.

1.5 Response time from Cognizant

Delivery time of 3PA for an application depends on the complexity. The time estimate will be provided at the same time a quote for setting up the new service is provided.
Delivery of a new user account: maximum 3 days, however dependent on when end user is accepting the disclaimer provided in the welcome email.
Delivery of access to end user: maximum 3 days
Demobilizing a user account: maximum 3 days
Incidents: maximum 3 days

2. Sponsors action items in details

2.1 How do I invite a new Azure B2B Guest User?

Use this option to request a new user account for an external party to be set up within 3PA.
A separate request must be raised for each end user. After the user account has been created, you will need to request access to the specific 3PA application/SPS. See list in Self Service Catalogue -> Place an order.

Go to IT Self Service Portal -> Place an order

Search for "**Request for a new Azure B2B Guest Account - 3rd Party (3PA)**"

Fill in the mandatory answers before you submit the request in the Portal. Sample questions are provided below for your ease of reference.

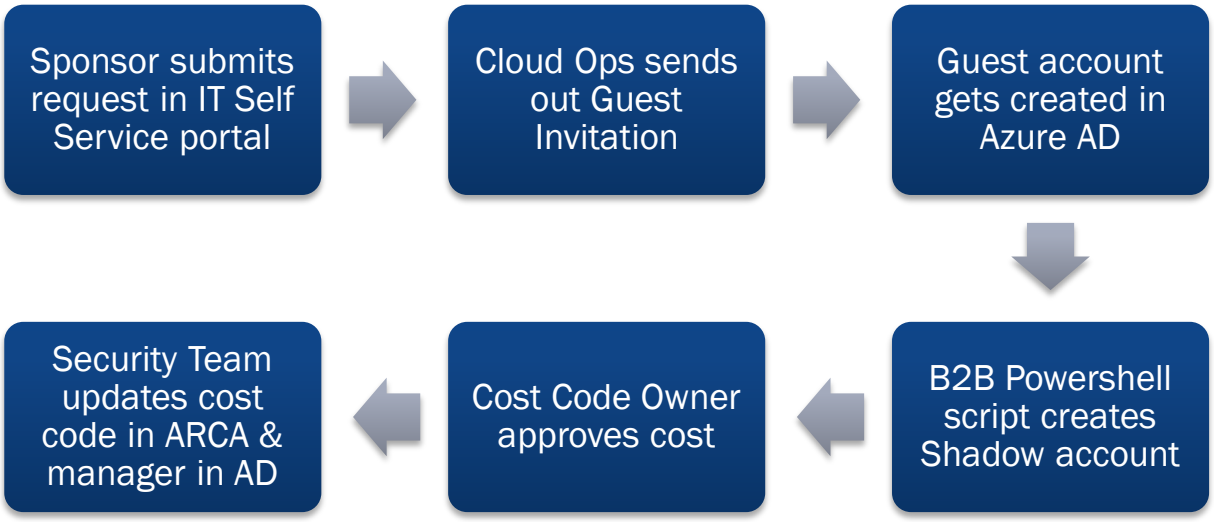
Sponsor information
Please provide your details as a sponsor
- Company:
- First name:
- Last name:
- Email address:
- Phone number:

Guest User information
- External Company:
- First name (***mandatory***):
- Last name (***mandatory***):
- External email address (***mandatory***):
- Phone number:
- Cost code to charge end users costs to (***mandatory***):

The guest user will receive an email invitation to join Akersolutions tenant in Azure AD.

Note: After the user account has been created & the cost code has been updated by security team in ARCA, you will need to request access to the specific 3PA application/SPS. See list in Self Service Catalogue -> Place an order.

2.2 What happens when I request for a new Azure B2B Guest Account?



Step1: You (the sponsor) should submit this request with all the necessary details.

Step2: Guest User invitation is sent out by Cloud Ops team.

- *Work Order will be created and assigned to "**IS Azure Managed Service**"*
- *Cloud Ops team will invite the Guest*
- *Cloud Ops team will add the Guest to Azure AD Group "**SG-TA-B2B-GUEST**"*

Step3: Guest account gets created in Azure AD with email as user name (for example: john.doe@contoso.com)

Step4: Shadow account of the same Guest User gets created at on-premise active directory, via a B2B powershell script, automatically. This shadow account is basically a footprint of the invited guest at on-premise. The B2B powershell script is maintained by the Directory Services Team.

Step5: Cost Code Approver approves the cost code assignment (needs to be specified in "Place an Order form")

Step6: The Cost code as provided by You (the sponsor) is updated for the Shadow Account by Security Team, in ARCA.

- *Cloud Ops will wait for the creation of the Shadow Account*
- *Once it's there, Cloud Ops will transfer the same Work Order to "**IS Information Security**" mentioning the Shadow Account for the invited Guest user*
- *Security team will update the Cost code* & Manager attribute

A separate request must be raised for each end user. If the request contains more than one user, it will be rejected.

Note: After the user account has been created & the cost code has been updated by security team in ARCA, you will need to request access to the specific 3PA application/SPS. See list in Self Service Catalogue -> Place an order.

2.3 How do I request access to an application, for a 3PA guest user?

A user account for the 3PA guest user must have been ordered first. See point 2.1 to know more on the guest invitation process based on Azure B2B.

To request for access to an application for an existing 3PA guest user (already invited through Azure B2B),
Go to IT Self Service Portal -> Place an order
Search for 3PA and choose the specific application.
Example "**Access to CCS (AKSO) via Azure B2B - 3rd Party (3PA)**".

Fill in the mandatory answers before you submit the order.

Note: You will have to use the SAM Account Name of the Shadow account to raise an application access request for the Guest User. For details on how the SAM account name will look like see below.

The "shadow account" will be created for all Azure B2B invited Guest users (as part of point 2.1) in the below format:
User Principal Name (UPN): firstname.lastname_guestdomain.com#EXT#@tenantname.onmicrosoft.com

Example:
User Principal Name (UPN): john.doe_contoso.com#EXT#@tenantname.onmicrosoft.com
SAM Account Name: 1st 20 characters of the UPN above (john.doe_contoso.com)
Display Name: Last Name, First name
Email : john.doe_contoso.com#EXT#@tenantname.onmicrosoft.com

Tenant name for Aker Solutions is: akersolutions.onmicrosoft.com

2.4 How do I remove a user from a service?

Go to IT Self Service Portal -> Place an order
Search for 3PA and choose "**Demobilize an Azure B2B Guest Account - 3rd Party (3PA)"**

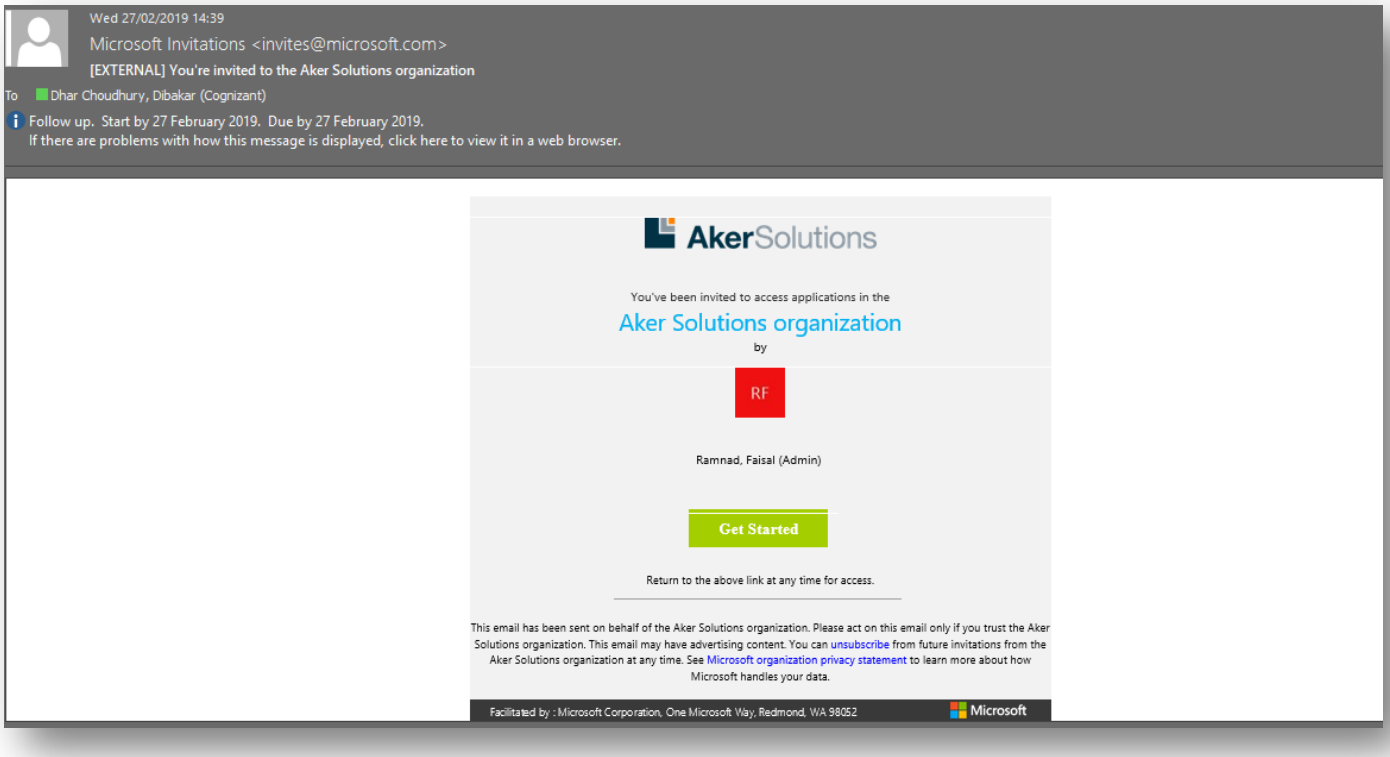
Fill in the mandatory answers before you submit.

You will have to answer the questions concerning which 3PA access you wish to demobilize, as it could be that end user has access to multiple 3PA accesses, and this will be checked before demobilizing the account.

2.5 How can the 3PA Guest Users access the User Guide?

a. Redeem Invitation

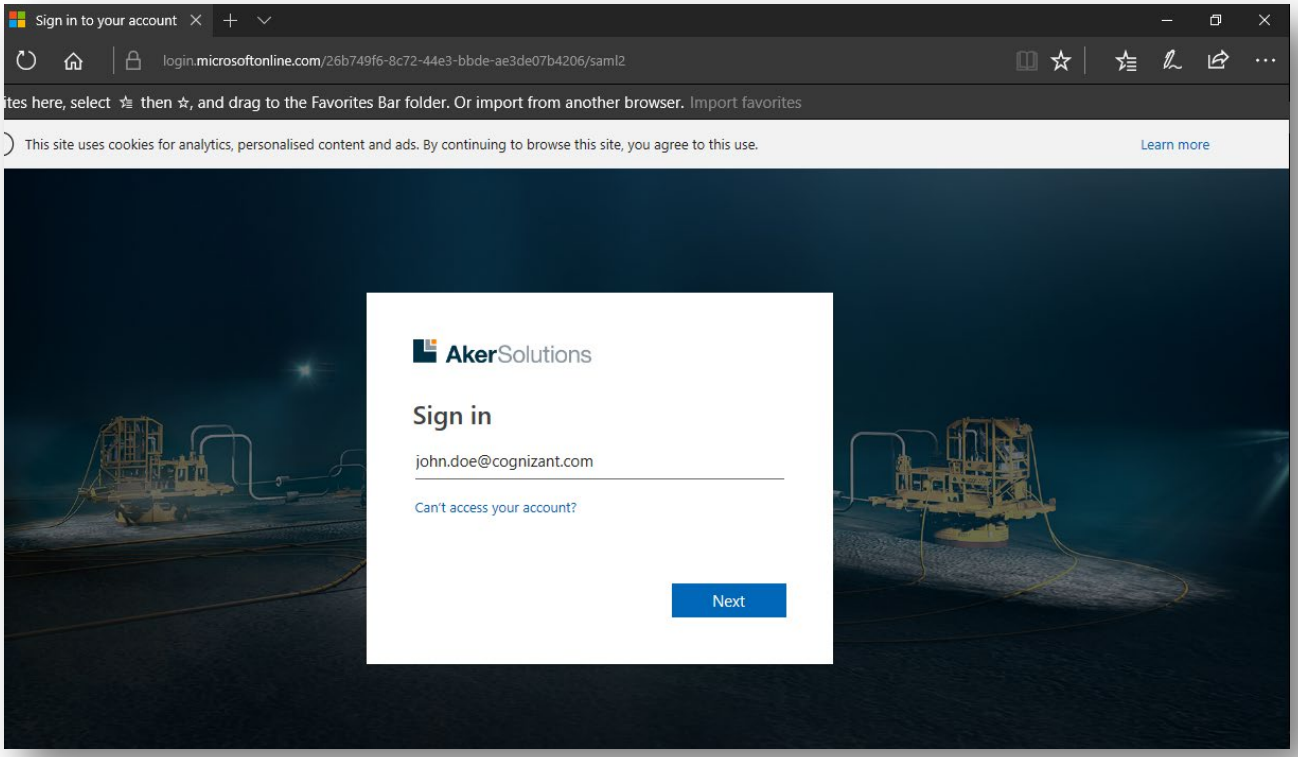
An invitation email (similar to the screenshot below) will be sent from invites@microsoft.com & the guest will have to click on the green “Get Started” button to redeem the invitation.



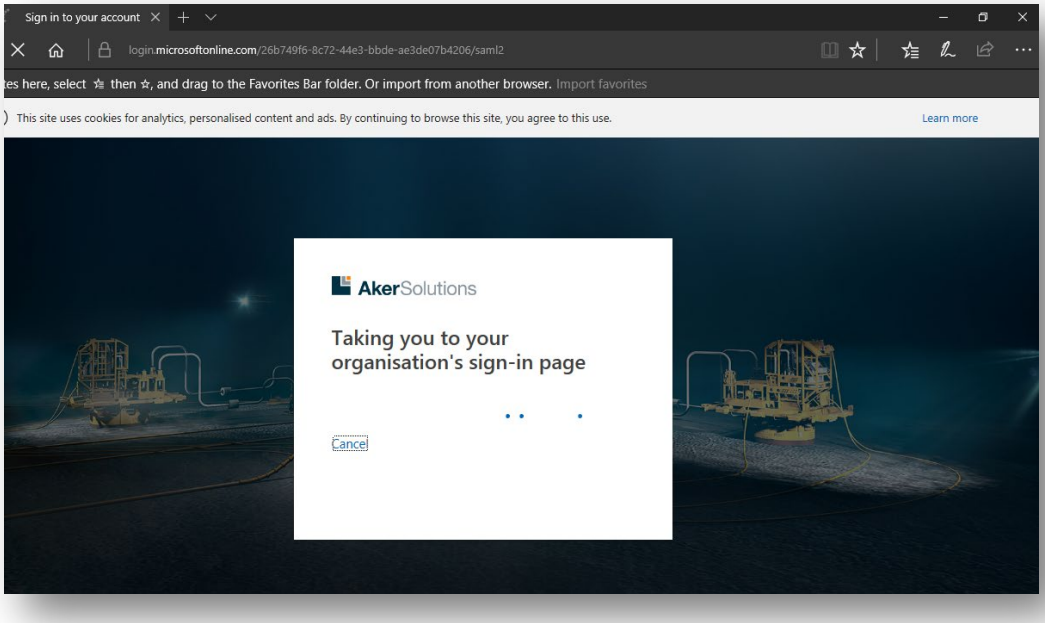
b. Provide the guest’s own business Office 365 credentials to Log on

You will have to use your current business Office 365 subscription details for this registration and not the 3PA credentials supplied by us.

You will now be presented with a login window similar to the below:

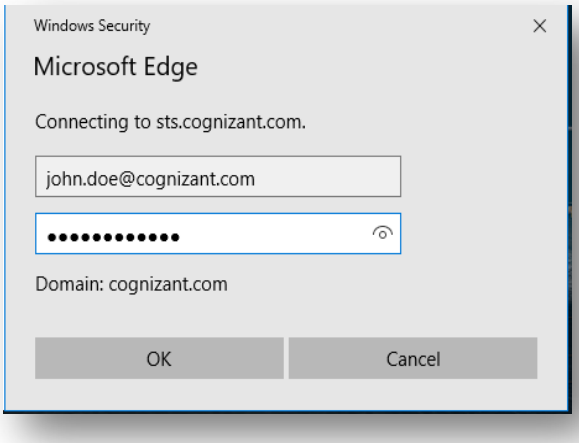


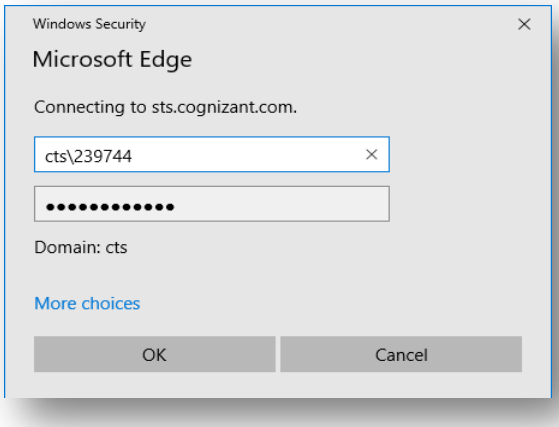
You will be taken to your Organization's page to enter the credentials. These are the credentials that you use to sign in to your own organization.



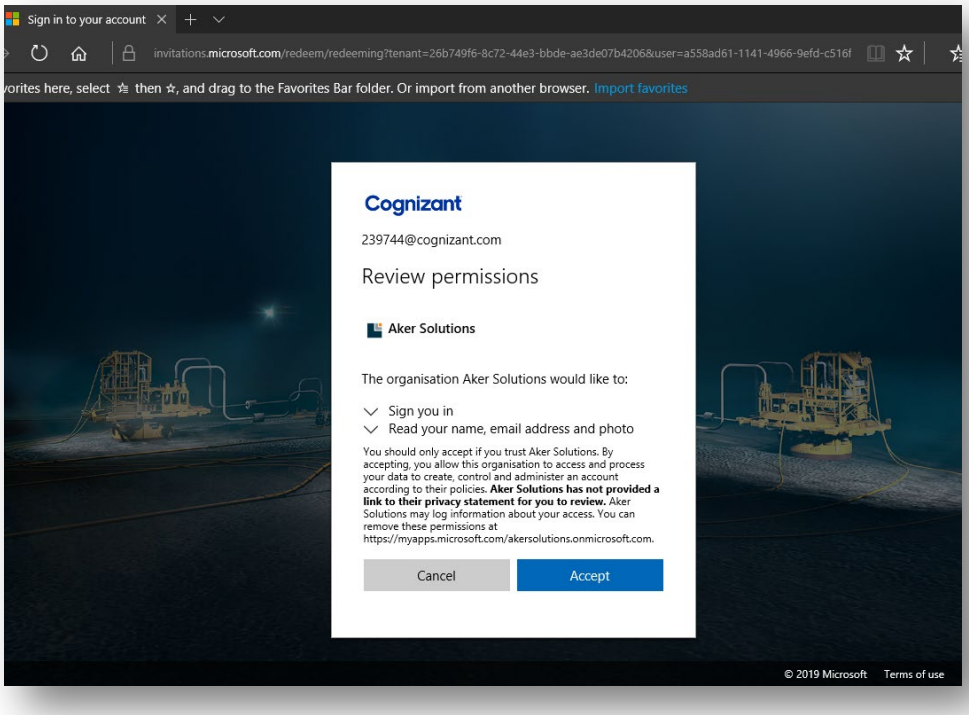
Please note that you may not see the below login page at all if you are already logged into your business Office 365 account.

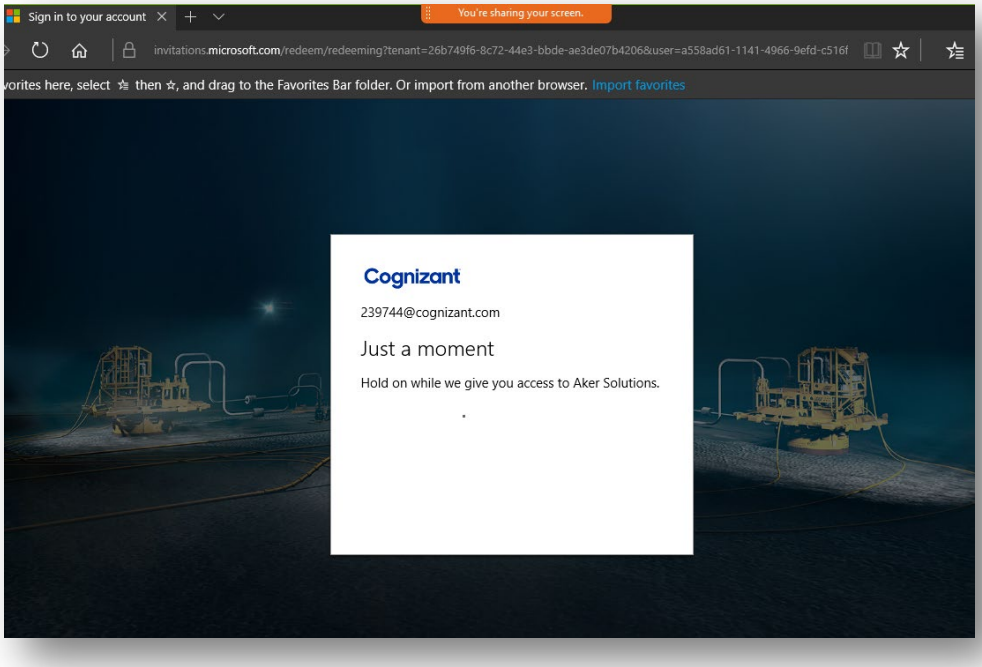
In case you do see the below prompts, provide your email address or your domain credentials whichever is applicable to sign in to your own Organization's Office 365 or Azure AD tenant. The below login prompt may differ based on your organization's subscription and the browser that you are using.





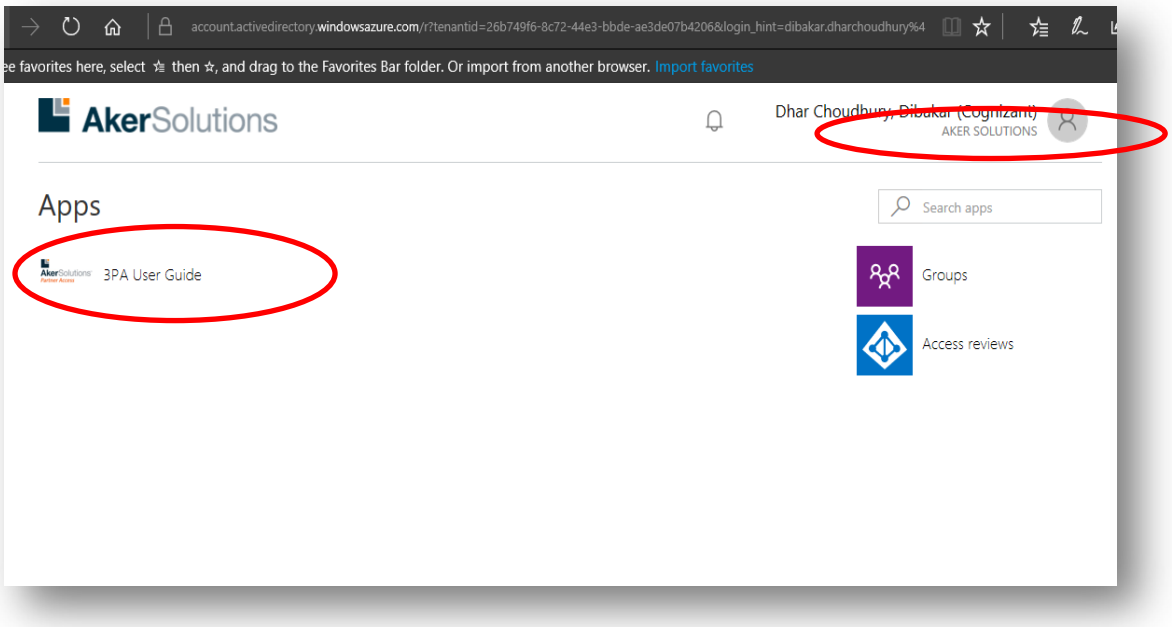
c. Review the Permissions and click on Accept



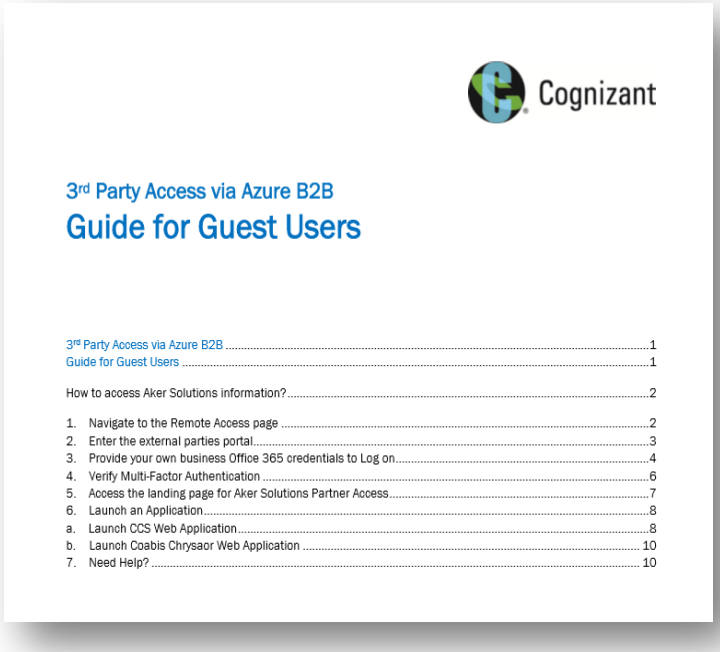


d. Reach the Myapps landing page in Aker Solutions Azure AD Tenant

Ensure that you are logged into “Aker Solutions” tenant or directory on the Top Right Hand Corner (below your name). If not, change it to “Aker Solutions” directory.
Now, you should be able to see “3PA User Guide” Application. Click on it to view the User Guide



The User guide will open in a new browser window. In case you are not able to open the user guide, please reach out to you Sponsor or to service desk.


Cognizant

3rd Party Access via Azure B2B

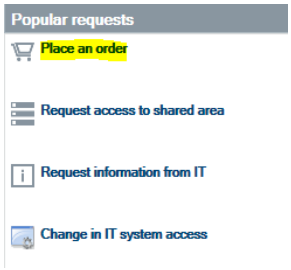
Guide for Guest Users

e. For ready reference, the User Guide for 3PA Guest Users is attached here

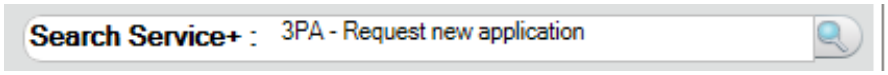
3PA via Azure B2B - Guide for Guest Use

2.6 How do I request the 3PA tram for a new application?

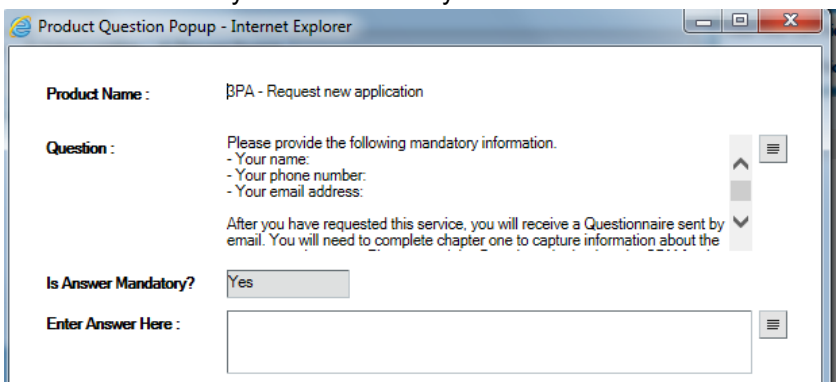
Go to IT Self Service Portal -> Place an order



Search for 3PA and choose “3PA – Request new application”

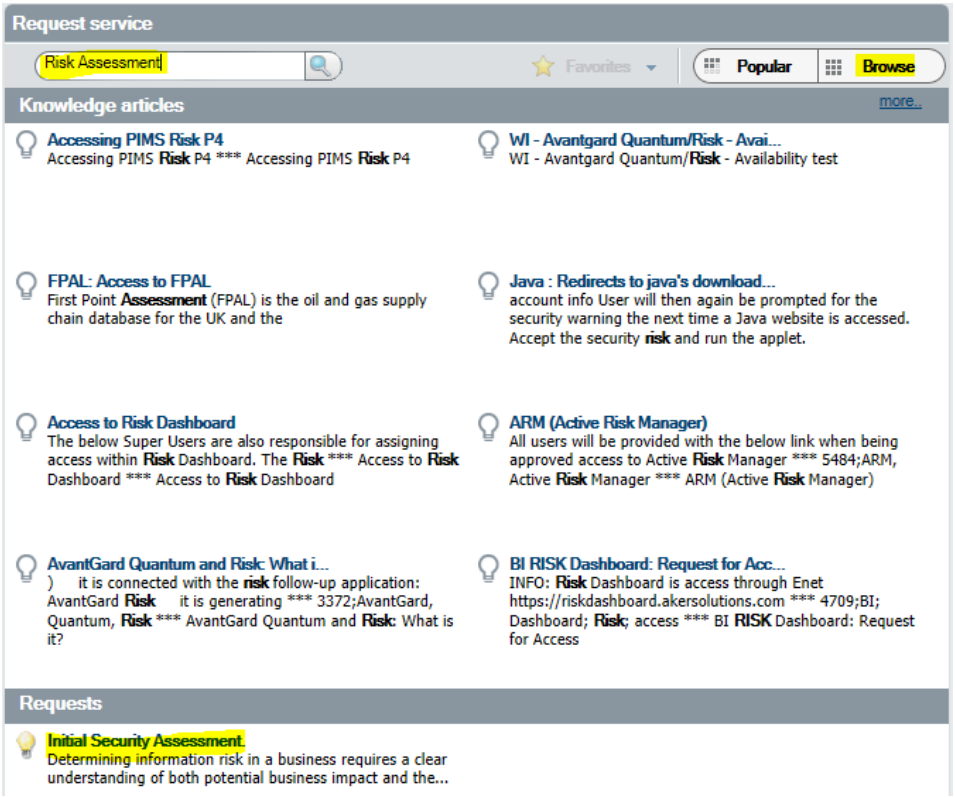


Fill in the mandatory answers before you submit the order.



After you have requested this service, you will receive a Questionnaire document sent by email. You will need to complete chapter one to capture information about the access requirements. Please send the Questionnaire document back to the SDM for the 3PA Service and he/she will initiate meetings with you and the SDM/TSM for the application.

Also, a Risk assessment request is required in parallel. Go to IT Self Service Portal -> Browse
Search for Risk assessment and choose “Initial Security Assessment”



3. Frequently asked questions

3.1 If I want to re-send end user the user manual, where can I find it?

The 3PA end users can get access to the end user manual once they click on ‘Get Started’ link on the Microsoft invitation page. There will be an application in Azure ‘End User Manual’ which they can access online in Azure. However, if they would like it to be re-sent, please contact Service Desk

3.2 How do I or the end user report a problem?

Report a problem via IT Self Service Portal -> Report a problem.

NB! It is important that you inform the Service Desk that you are a "3PA user" to identify your shadow account quickly in our Service Desk system.

The "shadow account" will be created in the below format:
User Principal Name (UPN): firstname.lastname_guestdomain.com#EXT#@tenantname.onmicrosoft.com

Example:
User Principal Name (UPN): john.doe_contoso.com#EXT#@tenantname.onmicrosoft.com
SAM Account Name: 1st 20 characters of the UPN above
Display Name: Last Name, First name
Email : john.doe_contoso.com#EXT#@tenantname.onmicrosoft.com

Requests Service Desk will cover are:
3PA: RFI - How do I log in?
3PA: unable to access login page

All regions:
70000 (internal)
Norway: +47 518 52200 or 35 52200
Malaysia: +603 2300 5200
United Kingdom: +44 1224 287287
United States:+1 713 596 4357 (Toll free 866 401 8847)
Brazil: (+55) 41-2102-4370
India: +47 518 52200

*Local language support is provided during local working hours.
You can also send an email, but call if urgent.
E-mail: Service.Desk@Cognizantog.com

For any other issues, the Service Desk will raise a ticket and forward it to the dedicated technical 3PA support team.