B2B DIRECT CONNECT

Connection from BECU TECH AAD to Greenfield Sandbox AAD tenant

October 2022

Contents

BECU B2B Direct Connect Overview

Azure B2B direct connect is part of the cross-tenant access settings in Azure AD. These settings will give you granular control over how external Azure AD organizations (BECU Greenfield sandbox Tenant) collaborate with BECU Tech Tenant (inbound access) and how BECU Tech users collaborate with external Azure AD organizations (outbound access).

With B2B direct connect, administrators can set up mutual trusts between external Azure AD tenants. Trust claims from external Azure AD tenants like MFA or device claims can be configured to prevent double prompt issue for external Azure AD users.

Prerequisite Requirements

The following items were identified prior to configuration:

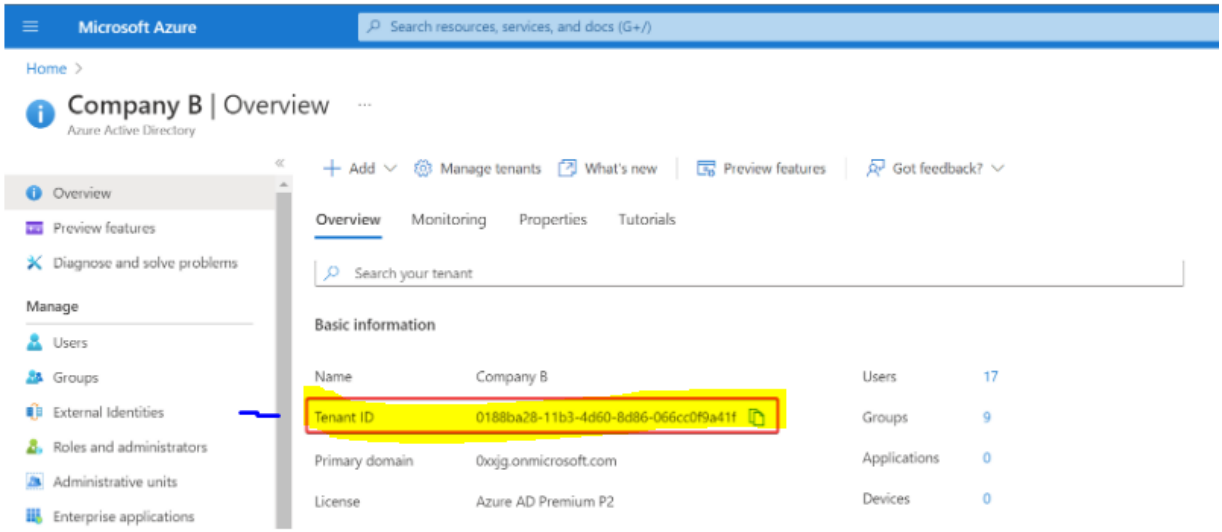
- Someone with **Global Administrator** or **Security Administrator** role access was required to make configuration changes
- An **Azure AD Premium P1 License** is required
- **Tenant IDs** for BECU.TECH and Greenfield Sandbox

Configuration Process Steps

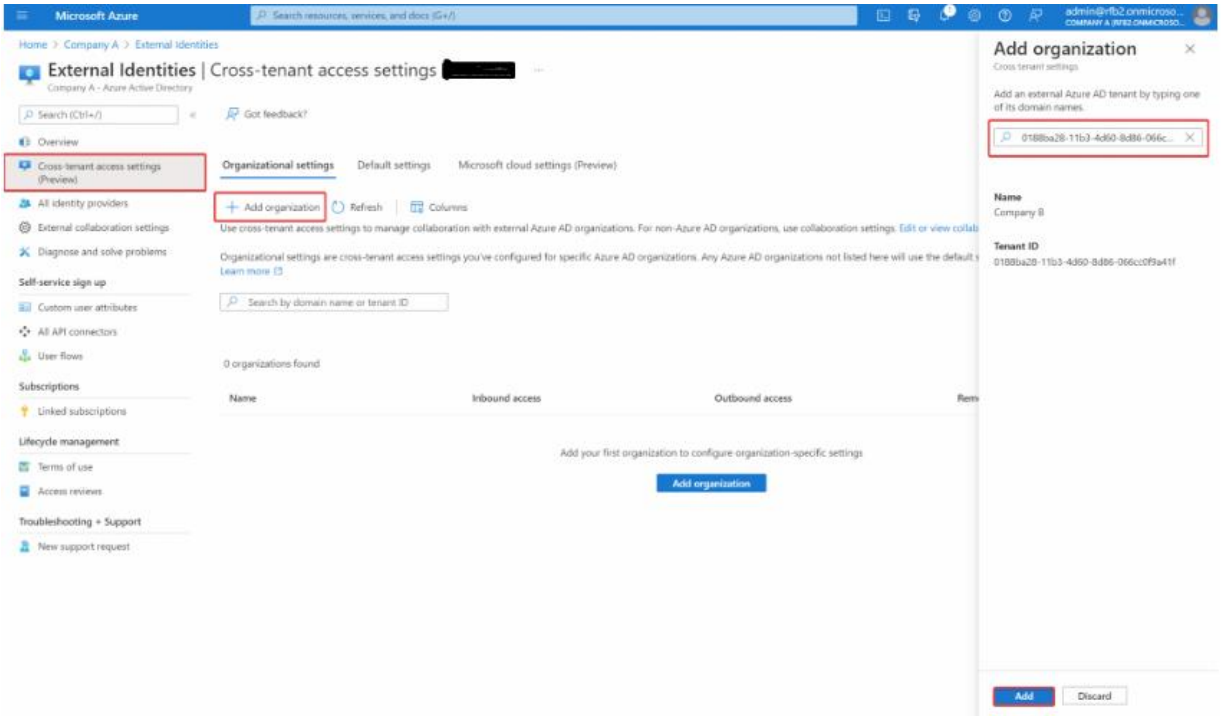
The steps in table below showcase, at a high-level, the configuration process necessary for B2B Direct Connect

Step No.	Description
1.	Cross Tenant Access Settings
2.	BECU TECH – BECU GREENFIELD SANDBOX INBOUND SETTINGS
3.	BECU TECH – BECU GREENFIELD SANDBOX OUTBOUND SETTINGS
4.	BECU GREENFIELD SANDBOX - BECU TECH CROSS TENANT SETTINGS
5.	BECU GREENFIELD SANDBOX - BECU Tech INBOUND SETTINGS
6.	BECU GREENFIELD SANDBOX - BECU Tech OUTBOUND SETTINGS
7.	Access Testing for test Users/Groups

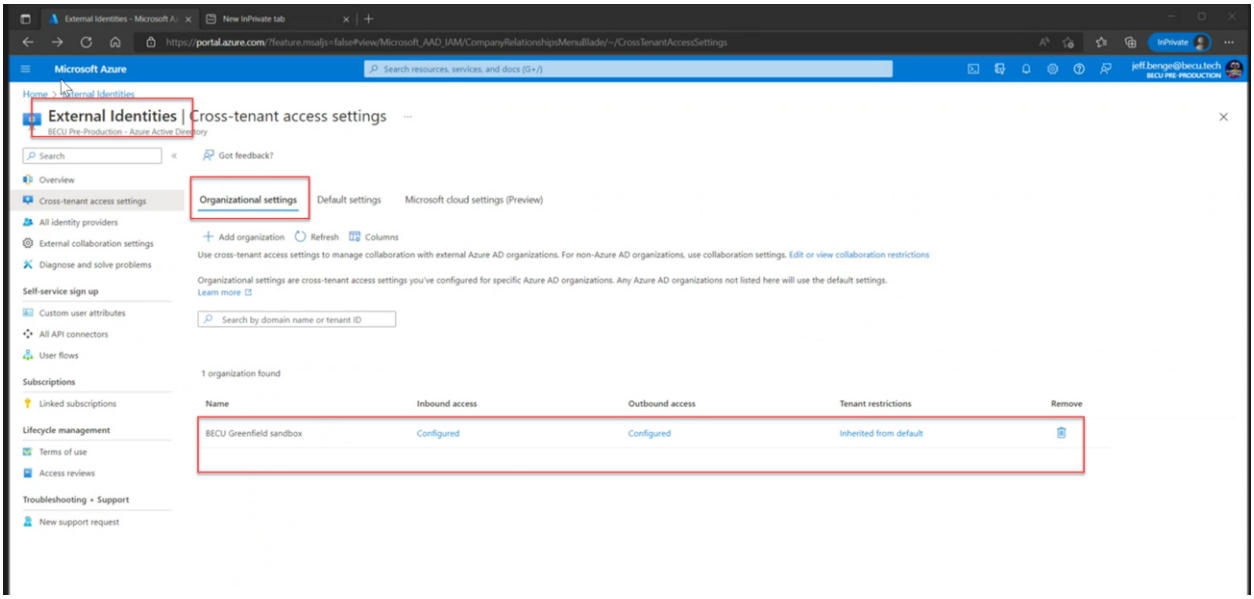
- To set up a trust from the BECU Tenant to BECU Greenfield sandbox tenant, we need the following from BECU Greenfield sandbox
  1. Tenant ID Of BECU Greenfield Sandbox Tenant
  2. The Group ID of the collaboration group (Optional) if we are only allowing group collaboration, else the whole tenant will have the access.
  3. The Tenant ID can be found by navigating to the AAD Portal as shown below



- On the BECU Tenant, navigate to ***Azure Active Directory -> External Identities***. Next, go to Cross-tenant access settings and **+ Add organization**. Then, enter the tenant ID from BECU Greenfield tenant, and the name should be resolved. To add BECU Greenfield tenant, click the **Add** button.
Below screenshot for sample cross tenant settings to add organization.



After the Organization is added, the organization should now be visible as below with the inbound, outbound and tenant restrictions pane for easy configuration

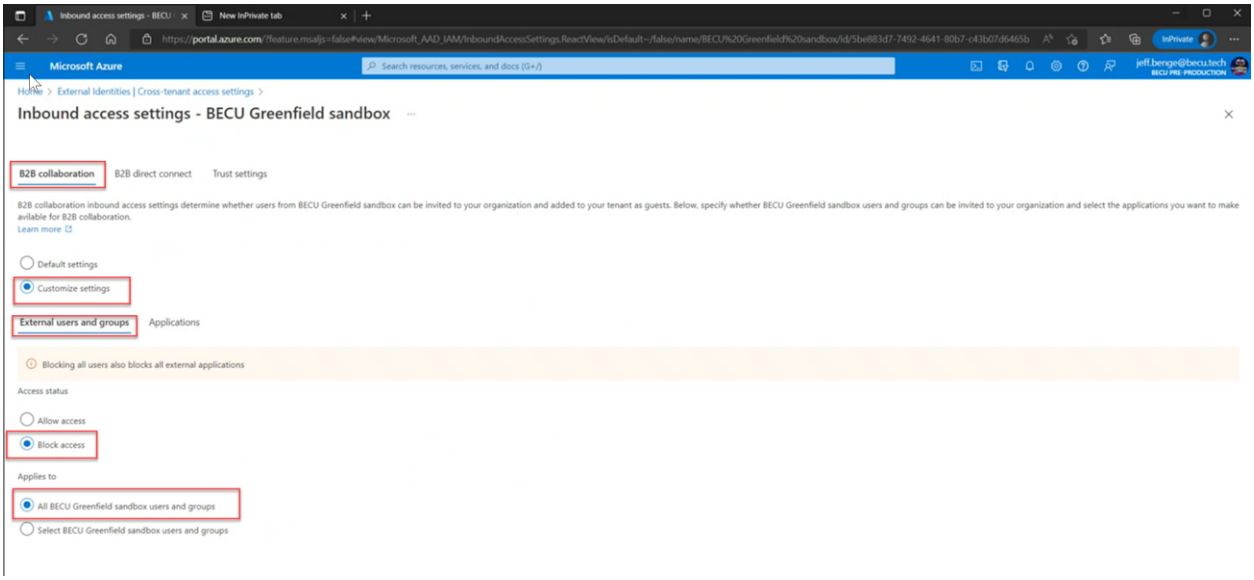


BECU Tech – BECU Greenfield Sandbox Cross Tenant Access Settings

For access configuration between the collaborating tenants, inbound and outbound settings will be configured, this will enable different inbound traffic or outbound traffic configuration to restrict visibility to users, groups, or external applications.

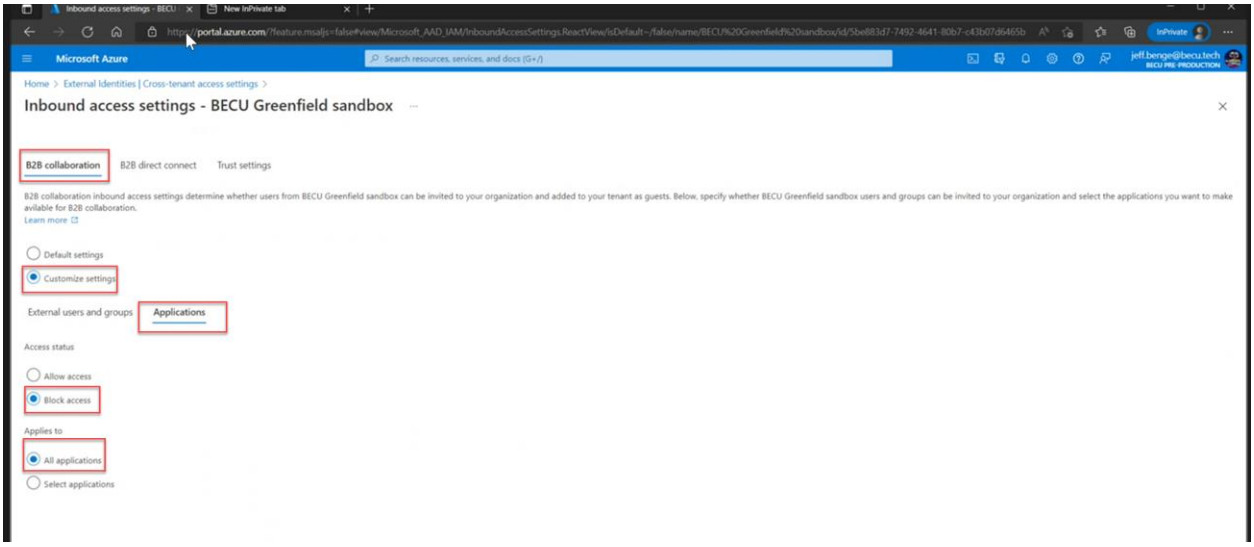
BECU TECH – BECU GREENFIELD SANDBOX INBOUND SETTINGS

- When BECU Greenfield tenant is added successfully, click on ***Inherited from default*** to edit the inbound access settings for this specific trust.
- **B2B Collaboration:** Default settings configured to allow access for All BECU Greenfield sandbox users



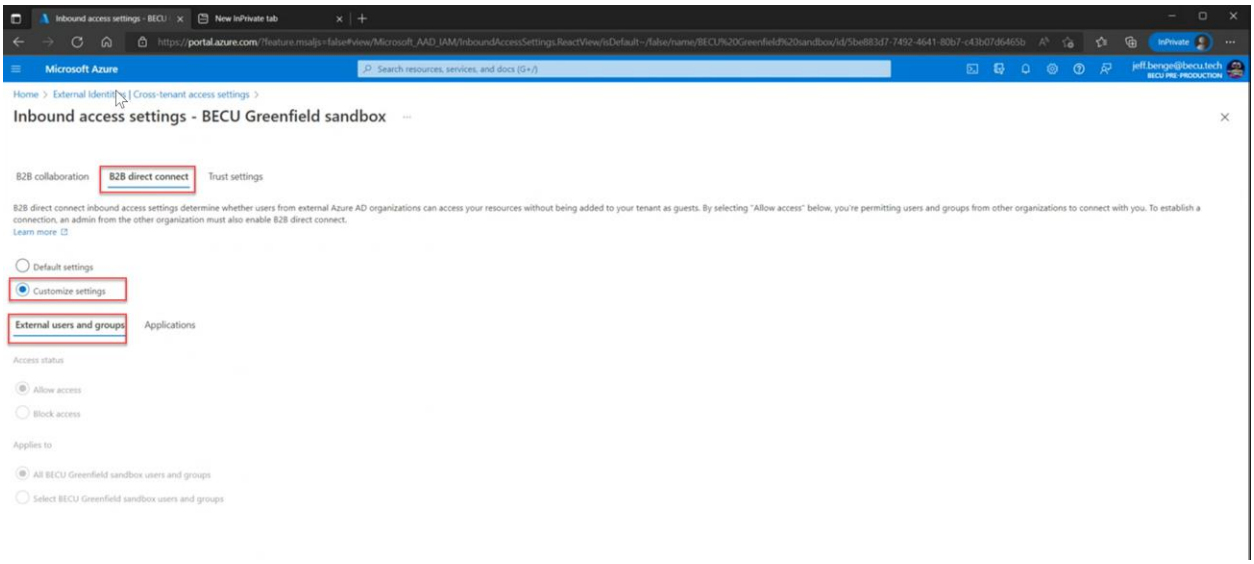
- Next, head over to the ***Applications*** tab and select Allow/Block access. Note that both users and groups and application types must match in order to save the configuration.

- **B2B Collaboration:** Default settings configured to allow access for All BECU Greenfield sandbox external applications



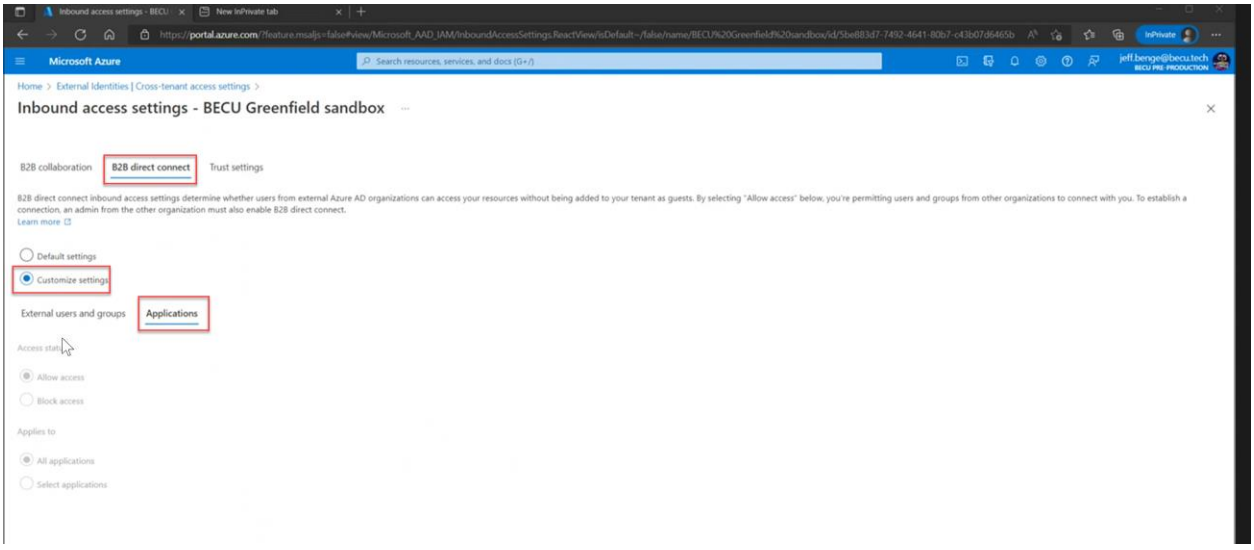
- Next, go to the **B2B direct connect** tab, and select ***Customize settings*** to overrule the default settings. In the access status section, choose **Allow access**. Then, select the ***Select external user and groups*** (Optional) if we are trying to restrict the access to a user or a specific group(s). Enter the group ID from BECU Greenfield sandbox. Also change the type from user to **group** and click **Add**.

- **B2B Direct Connect:** ***Customize settings*** to overrule the default settings configured to block access from All BECU Greenfield sandbox users

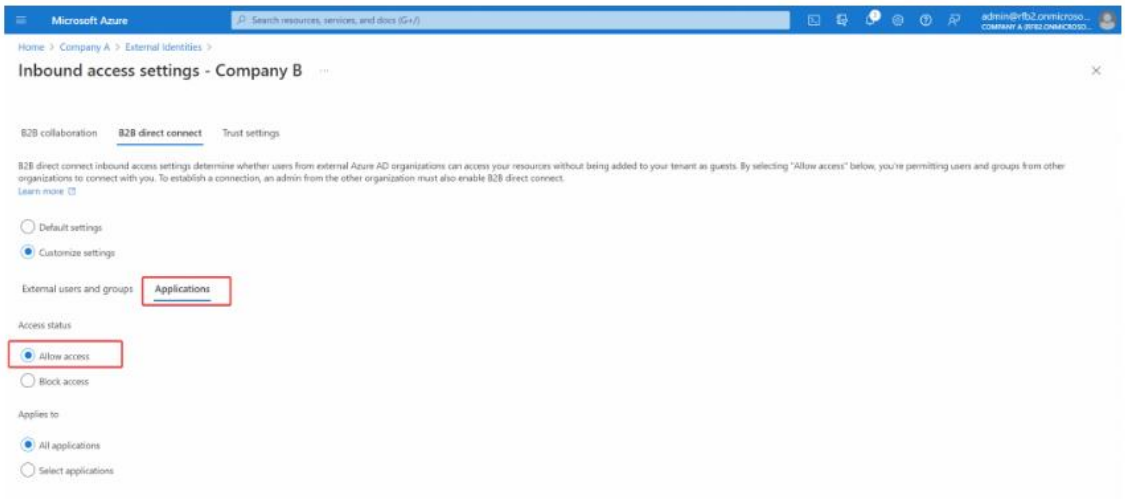


- Next, head over to the ***Applications*** tab and select Allow/Block access. Note that both users and groups and application types must match in order to save the configuration.

- **B2B Direct Connect:** ***Customize settings*** to overrule the default settings configured to block access from All BECU Greenfield sandbox external applications

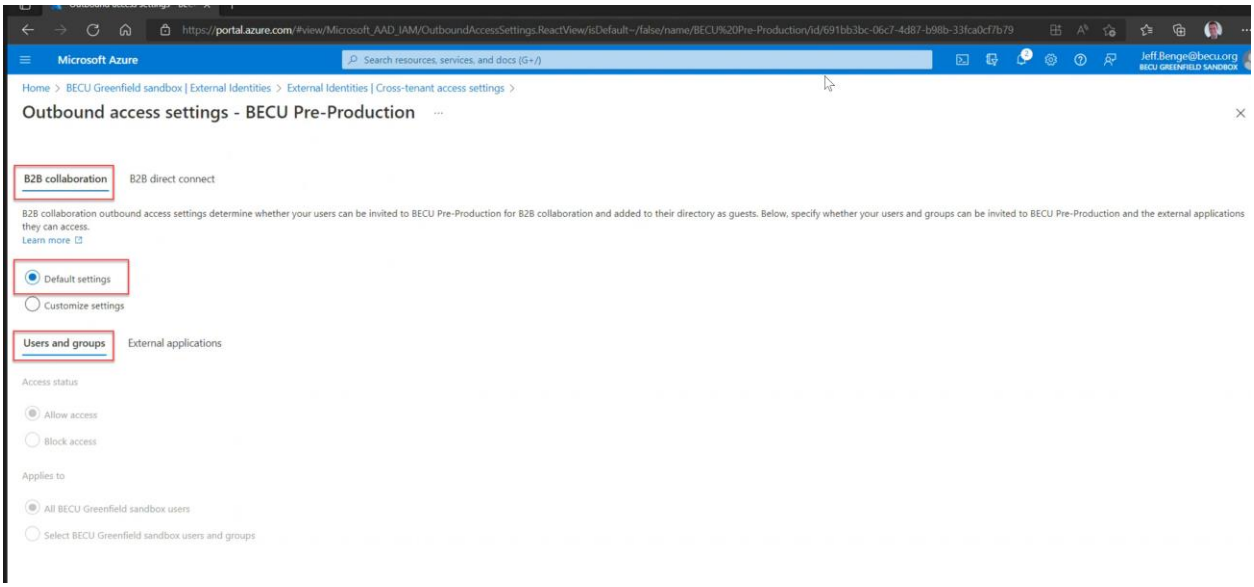


-



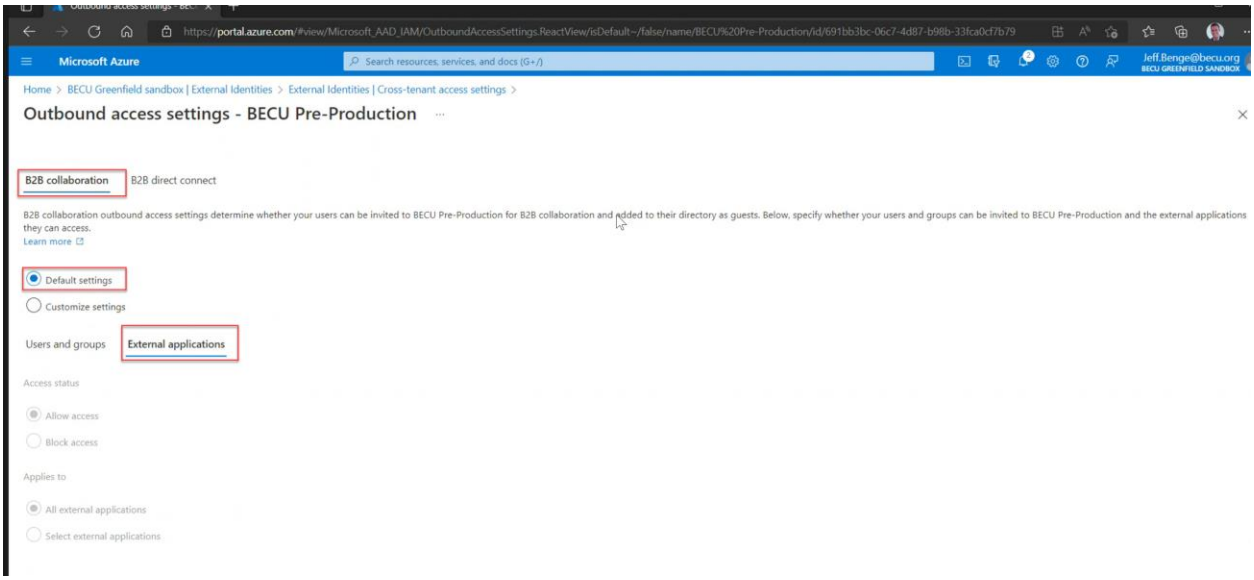
BECU TECH – BECU GREENFIELD SANDBOX OUTBOUND SETTINGS

- Outbound settings let you select users, groups and application that can access external Greenfield Sandbox tenant, navigate to the Default tab or an organization on the organizational settings, click on ***Inherited from default*** to edit the outbound access settings for this specific trust.
- **B2B Collaboration:** Default settings configured to allow access for All BECU Greenfield sandbox users



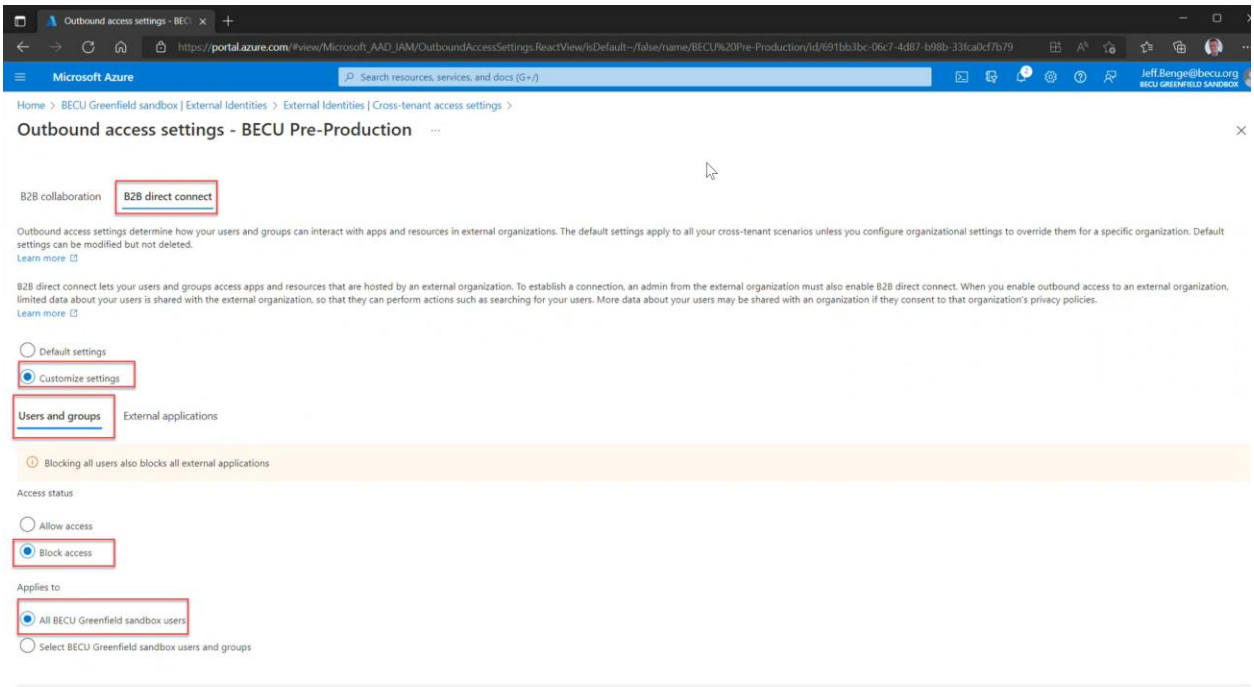
- Next, head over to the ***Applications*** tab and select Allow/Block access. Note that both users and groups and application types must match in order to save the configuration.

- **B2B Collaboration:** Default settings configured to allow access for All BECU Greenfield sandbox external applications



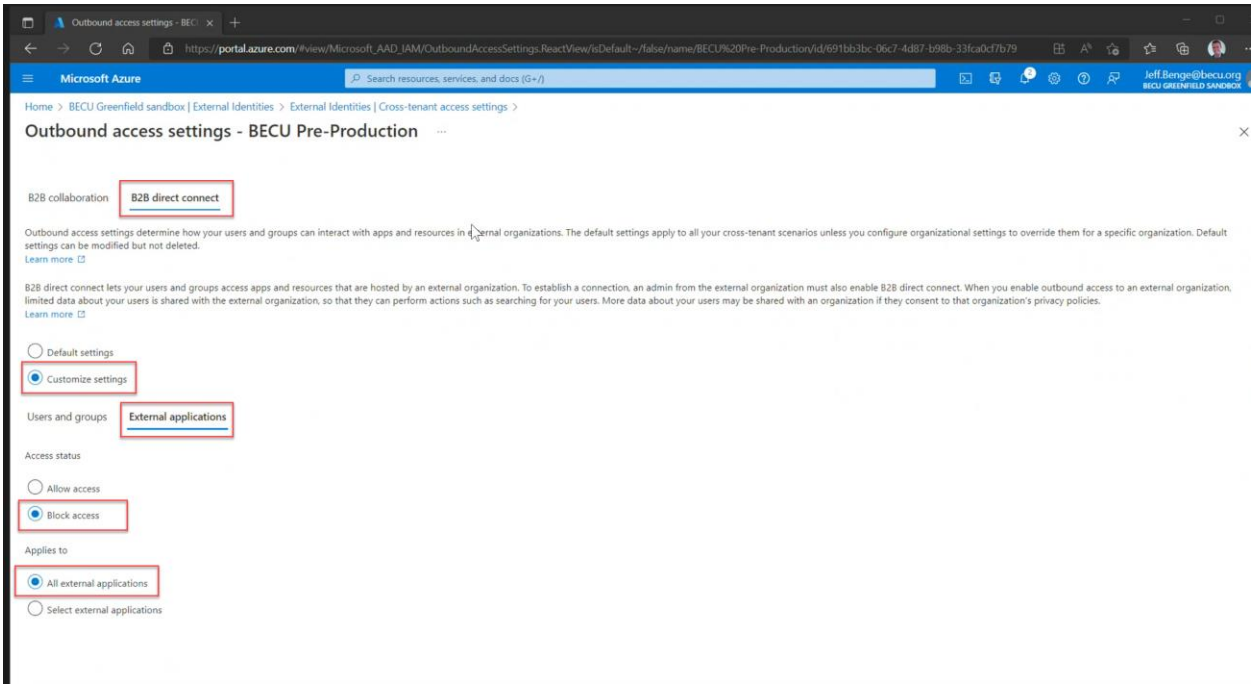
- Next, go to the **B2B direct connect** tab, and select ***Customize settings*** to overrule the default settings. In the access status section, choose **Allow access**. Then, select the ***Select external user and groups*** (Optional) if we are trying to restrict the access to a user or a specific group(s). Enter the group ID from BECU Greenfield sandbox. Also change the type from user to **group** and click **Add**.

- **B2B Direct Connect:** ***Customize settings*** to overrule the default settings configured to allow access to All BECU Greenfield sandbox users

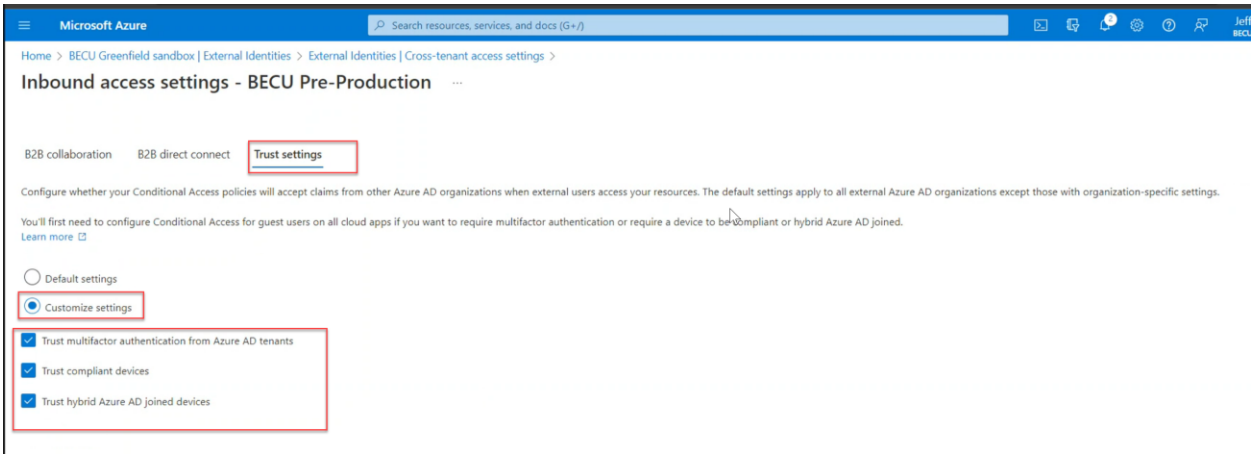


- Next, head over to the ***Applications*** tab and select Allow/Block access. Note that both users and groups and application types must match in order to save the configuration.

- **B2B Direct Connect:** ***Customize settings*** to overrule the default settings configured to allow access to All BECU Greenfield sandbox external applications

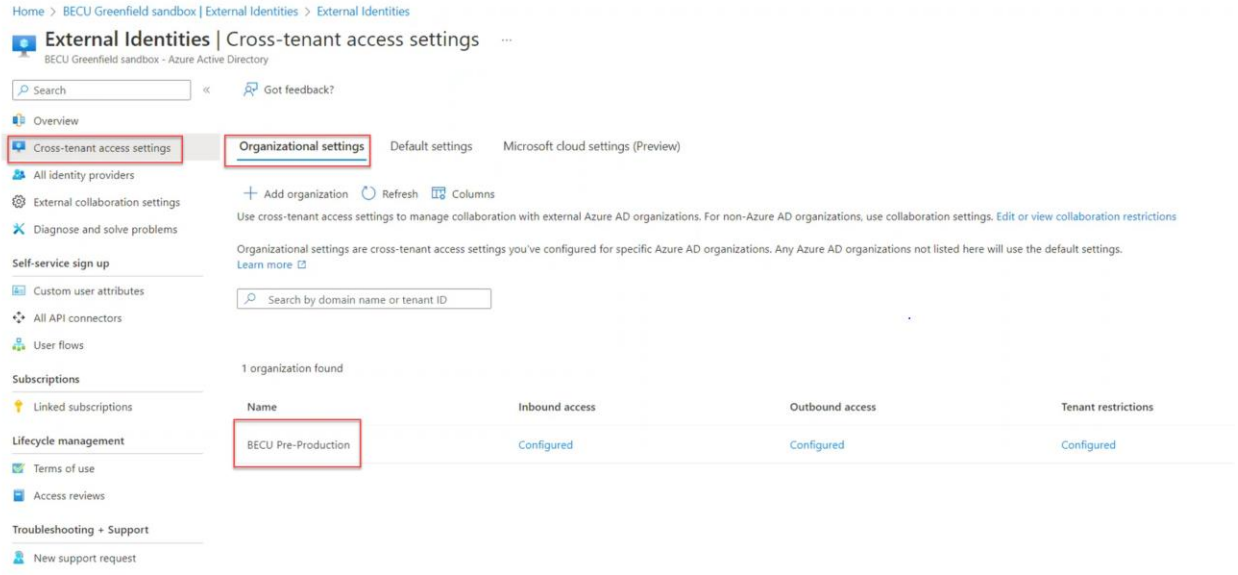


- **B2B Direct Connect Trust Settings:** Configure weather to trust and accept claims from the BECU Greenfield Tenant, conditional access policies will accept claims like MFA, Compliant devices.



BECU GREENFIELD SANDBOX - BECU TECH CROSS TENANT SETTINGS

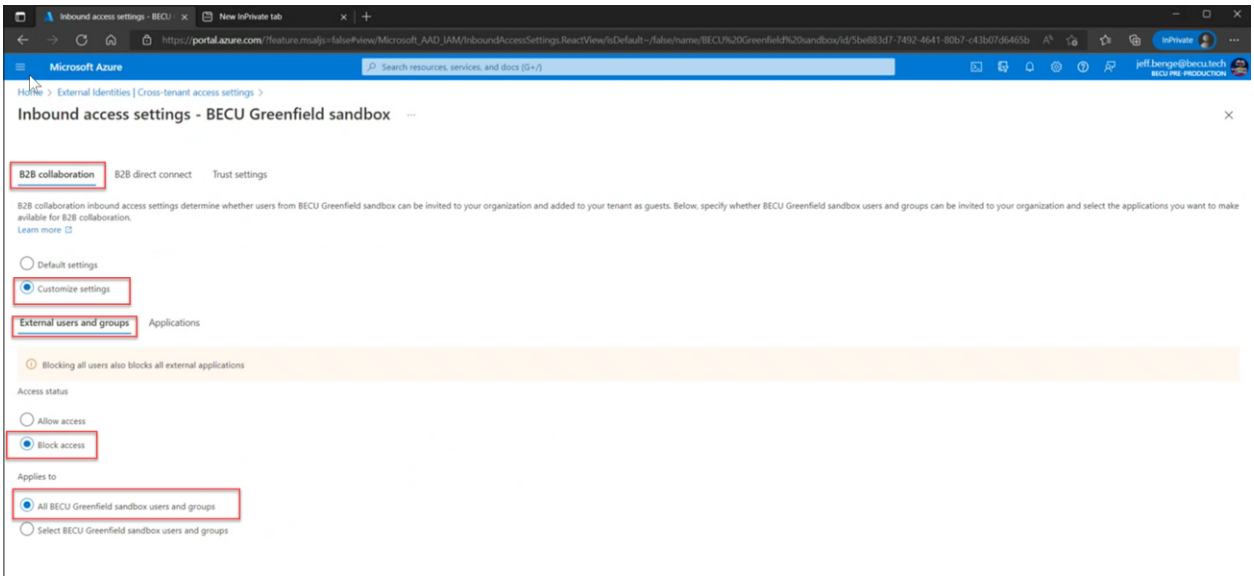
- Now, over at BECU Greenfield Sandbox, we do the exact same thing, but now we enter the tenant ID from BECU Tech Tenant instead to add the organization.



- After BECU Tech Tenant is added, we configure the **inbound** and **outbound** settings for the cross-tenant access.

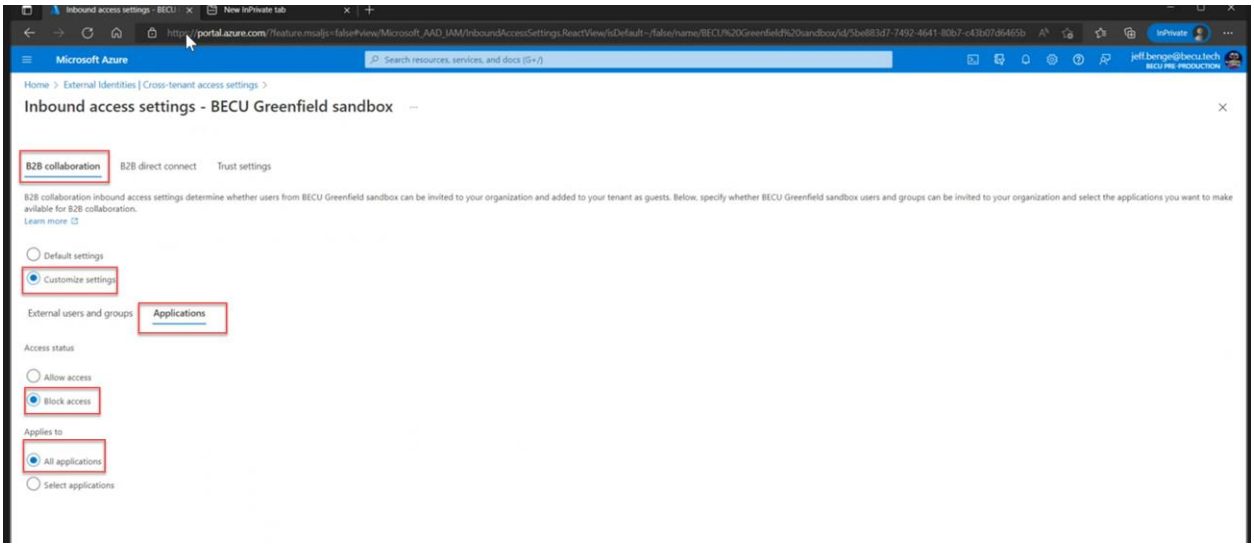
BECU GREENFIELD SANDBOX - BECU Tech INBOUND SETTINGS

- **B2B Collaboration:** Default settings configured to allow access for All BECU Greenfield sandbox users



- Next, head over to the ***Applications*** tab and select Allow/Block access. Note that both users and groups and application types must match in order to save the configuration.

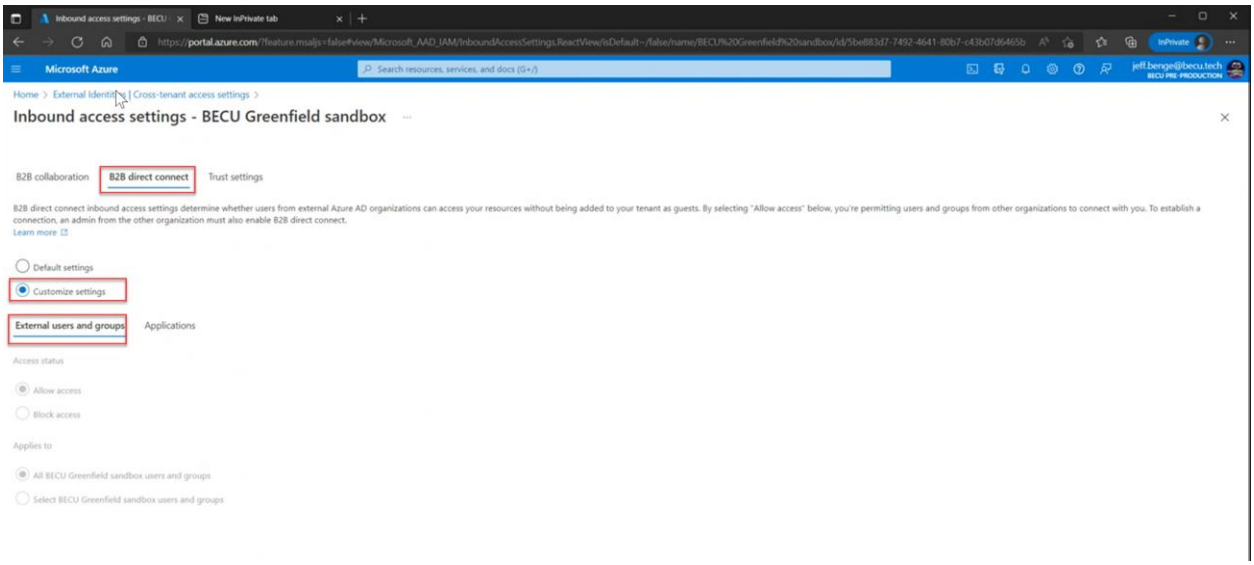
- **B2B Collaboration:** Default settings configured to allow access for All BECU Tech external applications



- Next, go to the **B2B direct connect** tab, and select ***Customize settings*** to overrule the default settings. In the access status section, choose **Allow access**. Then, select

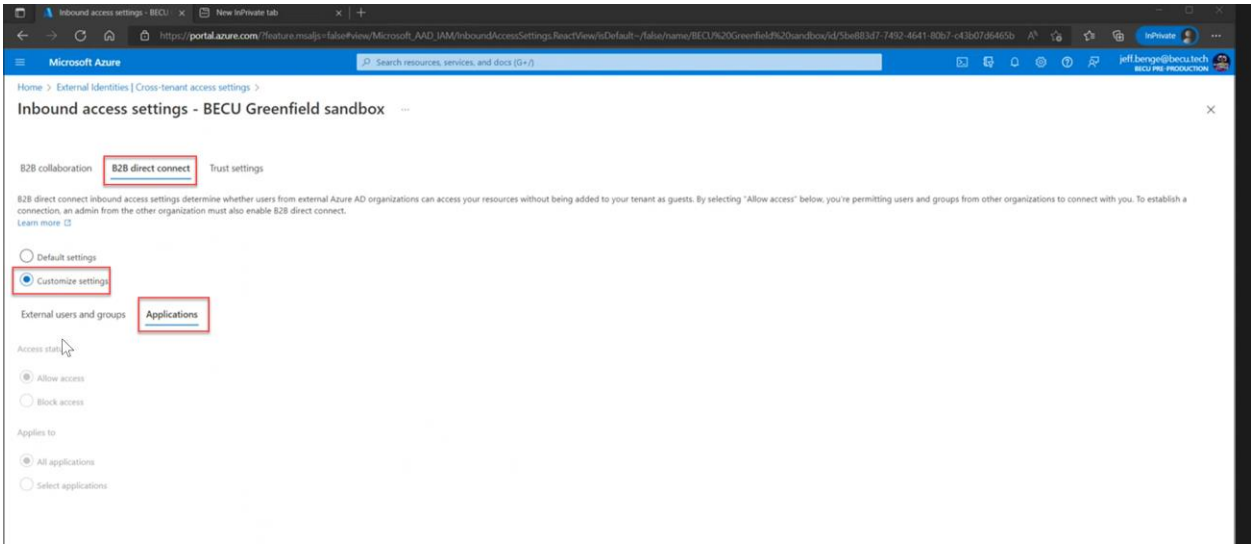
the ***Select external user and groups*** (Optional) if we are trying to restrict the access to a user or a specific group(s). Enter the group ID from BECU Greenfield sandbox. Also change the type from user to **group** and click **Add**.

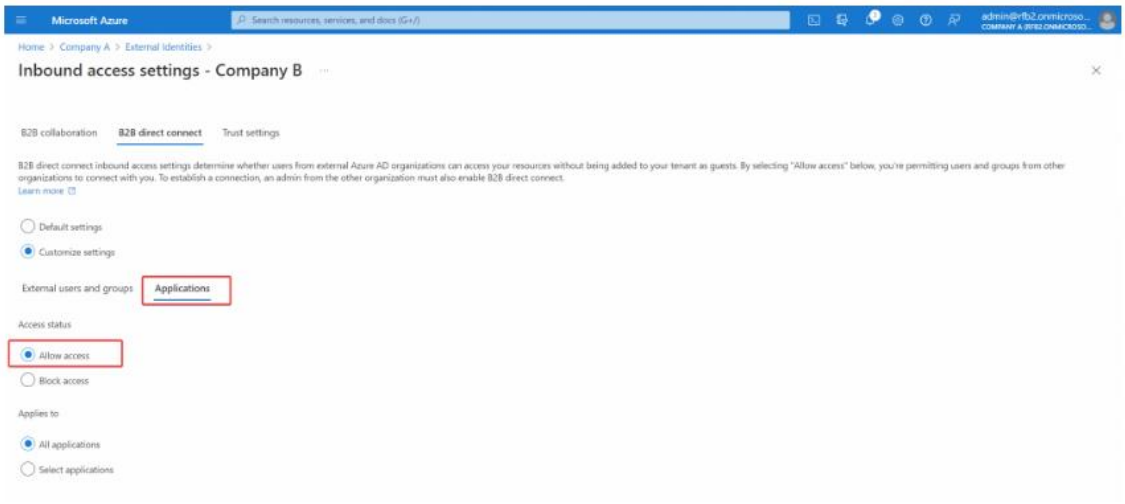
- **B2B Direct Connect:** ***Customize settings*** to overrule the default settings configured to allow access from All BECU Tech users and groups.



- Next, head over to the ***Applications*** tab and select Allow/Block access. Note that both users and groups and application types must match in order to save the configuration.

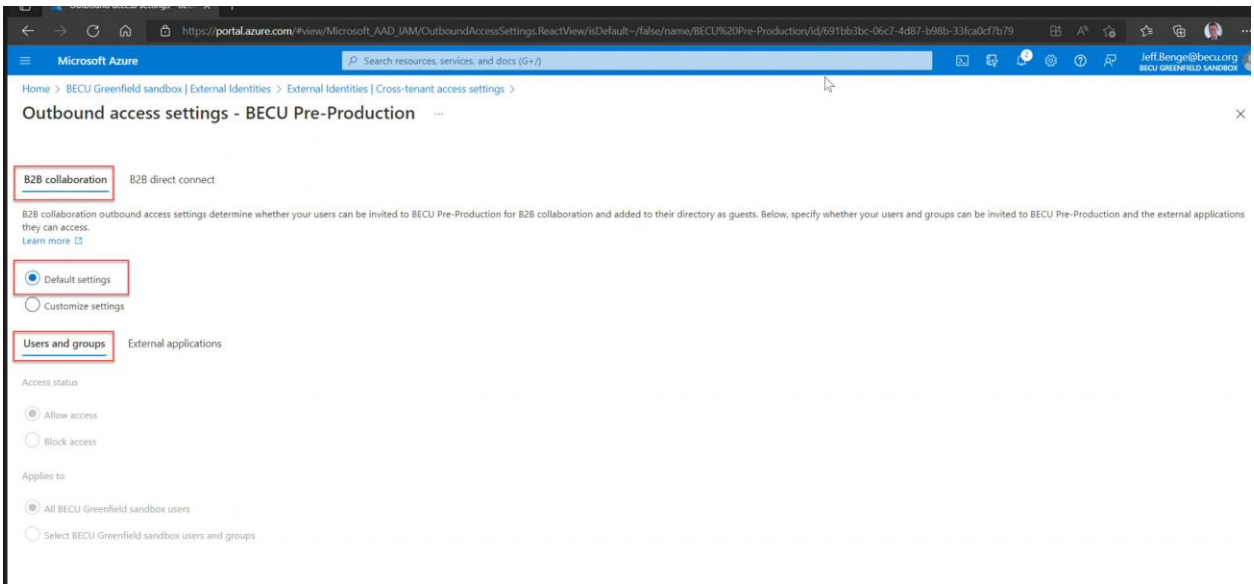
- **B2B Direct Connect:** ***Customize settings*** to overrule the default settings configured to allow access from All BECU Tech external applications





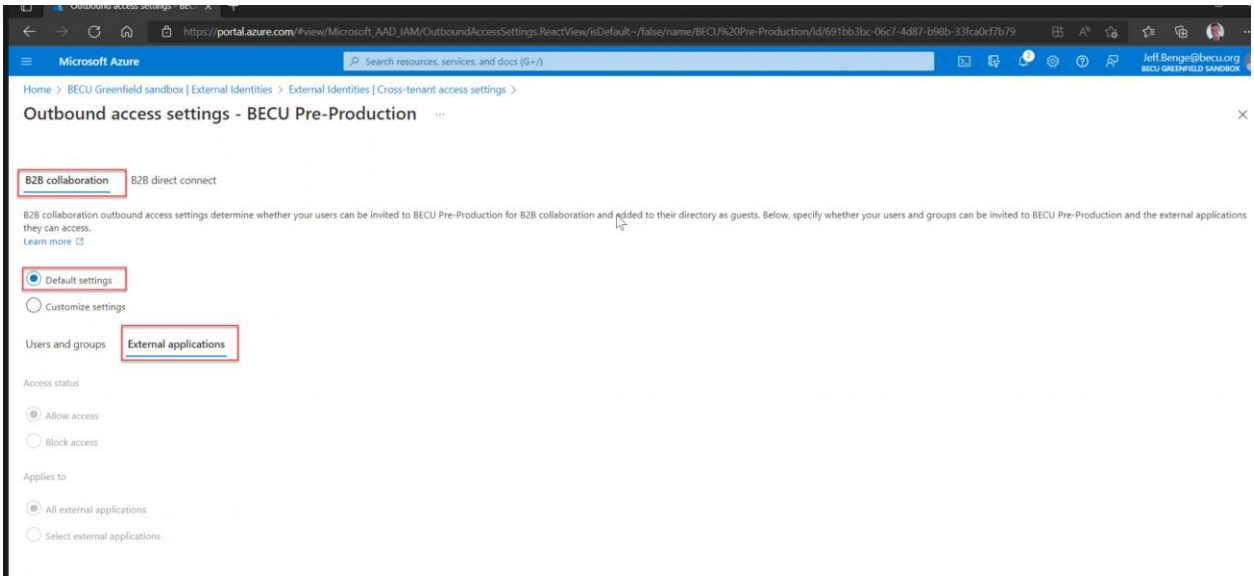
BECU GREENFIELD SANDBOX - BECU Tech OUTBOUND SETTINGS

- Outbound settings let you select users, groups and application that can access external Greenfield Sandbox tenant, navigate to the Default tab or an organization on the organizational settings, click on ***Inherited from default*** to edit the outbound access settings for this specific trust.
- **B2B Collaboration:** Default settings configured to allow access for All BECU Tech users



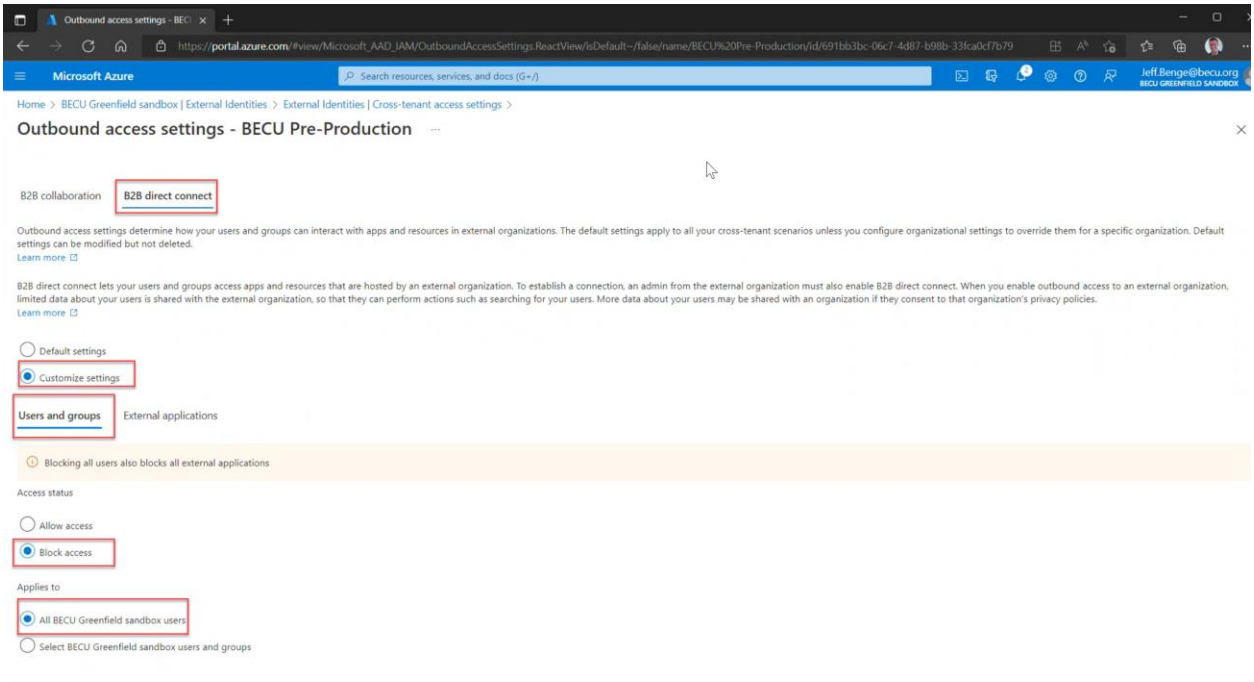
- Next, head over to the ***Applications*** tab and select Allow/Block access. Note that both users and groups and application types must match in order to save the configuration.

- **B2B Collaboration:** Default settings configured to allow access for All BECU Tech external applications



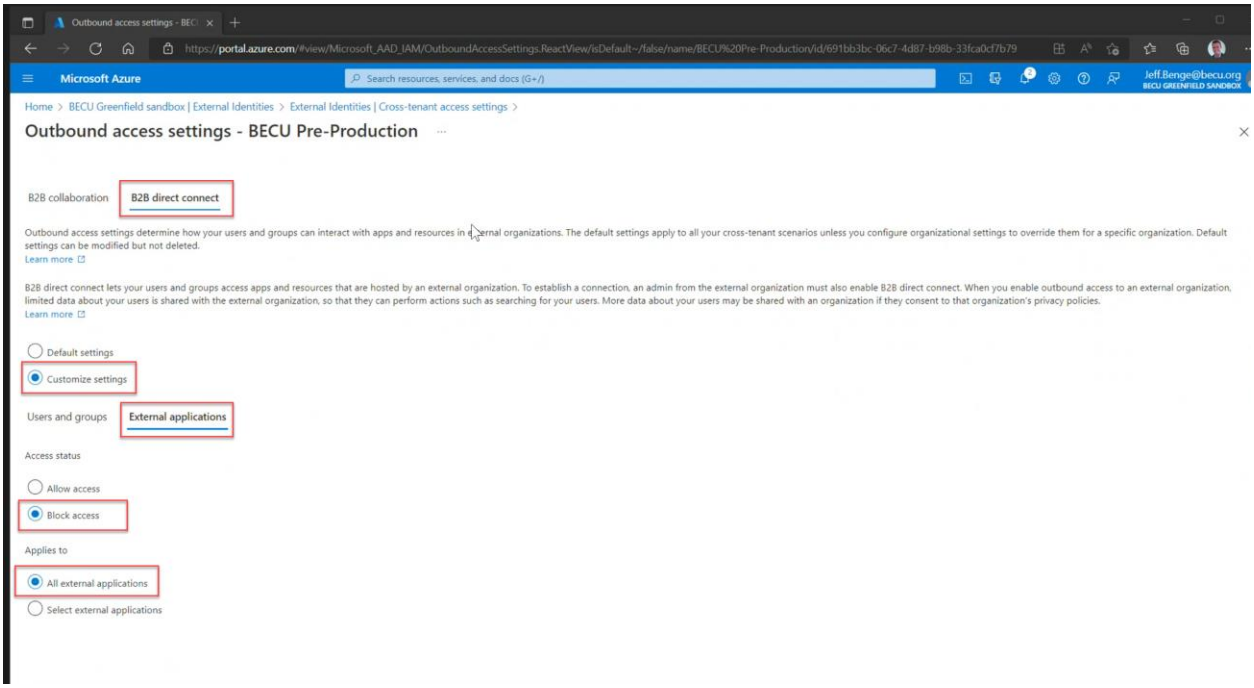
- Next, go to the **B2B direct connect** tab, and select ***Customize settings*** to overrule the default settings. In the access status section, choose **Allow access**. Then, select the ***Select external user and groups*** (Optional) if we are trying to restrict the access to a user or a specific group(s). Enter the group ID from BECU Tech. Also change the type from user to **group** and click **Add**.

- **B2B Direct Connect:** ***Customize settings*** to overrule the default settings configured to block access to All BECU Greenfield sandbox users from accessing BECU Tech.

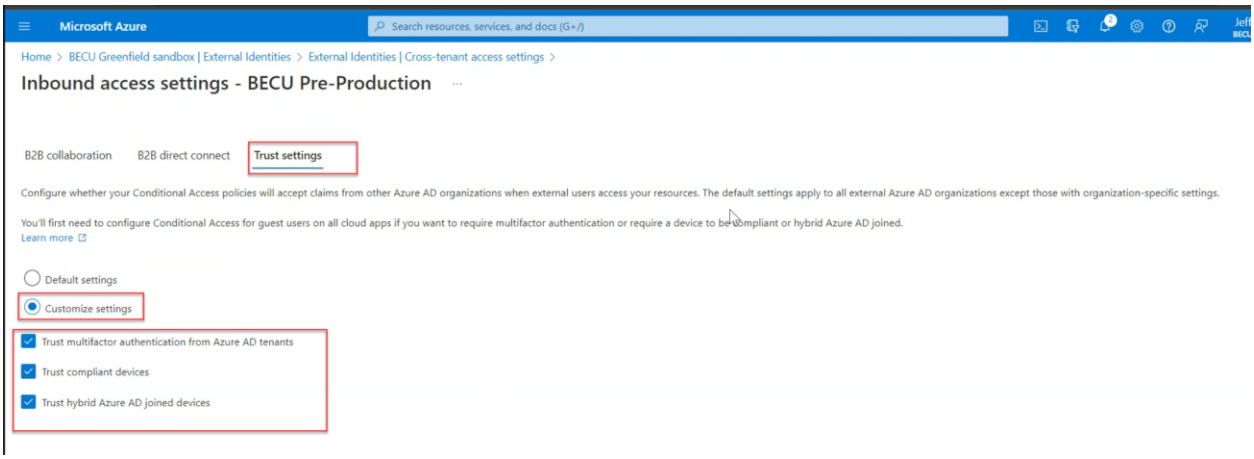


- Next, head over to the ***Applications*** tab and select Allow/Block access. Note that both users and groups and application types must match in order to save the configuration.

- **B2B Direct Connect:** ***Customize settings*** to overrule the default settings configured to block access to All BECU Tech external applications

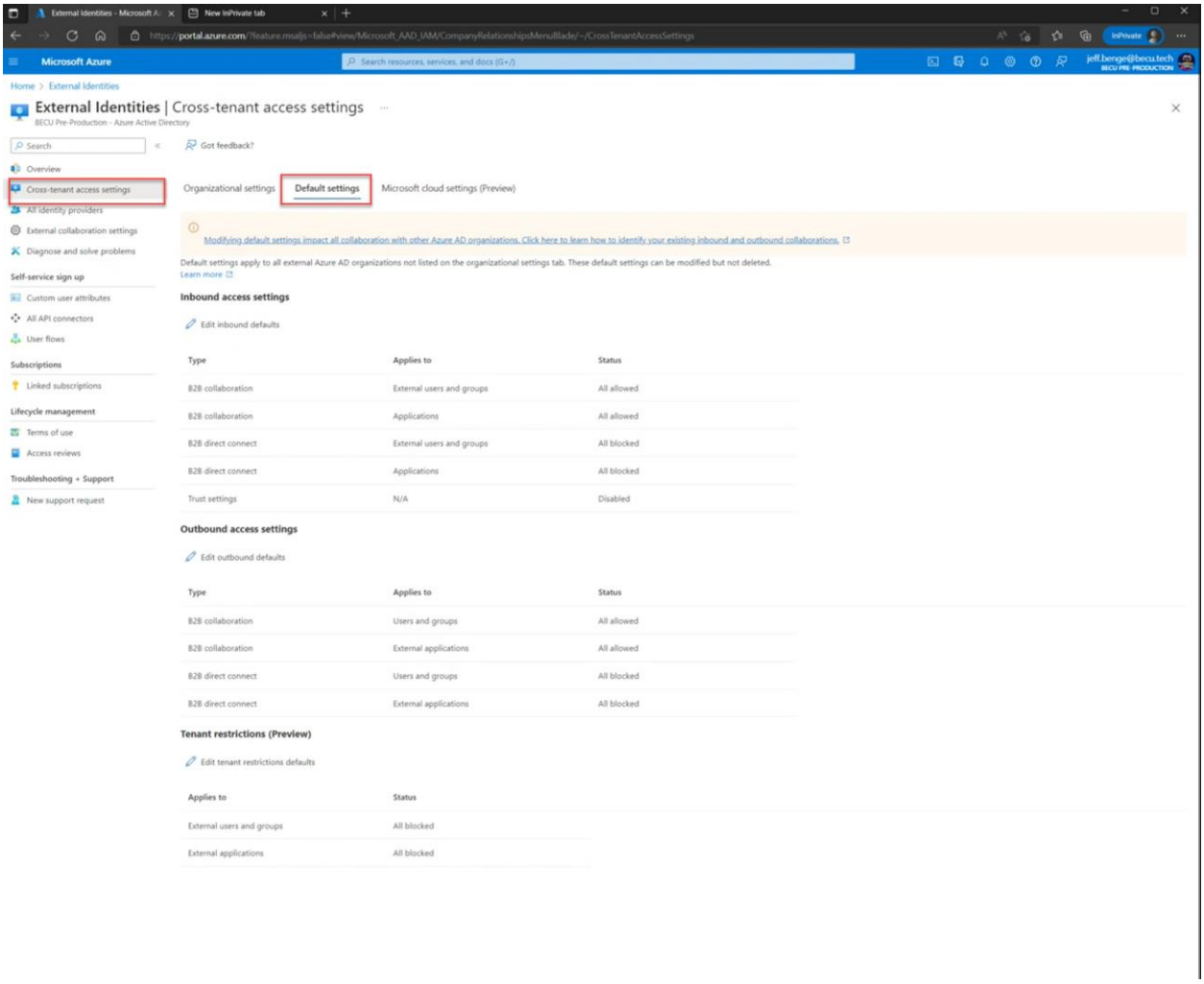


- **B2B Direct Connect Trust Settings:** Configure weather to trust and accept claims from the BECU Tech Tenant, conditional access policies will accept claims like MFA, Compliant devices.



- **Note:** By default, B2B Collaboration is allowed and B2B direct connect is blocked for all users, but by editing the settings for a specific trust, we can overrule the defaults. Note

that this only applies to this specific trust and that there are actions needed from both sides to set this up.

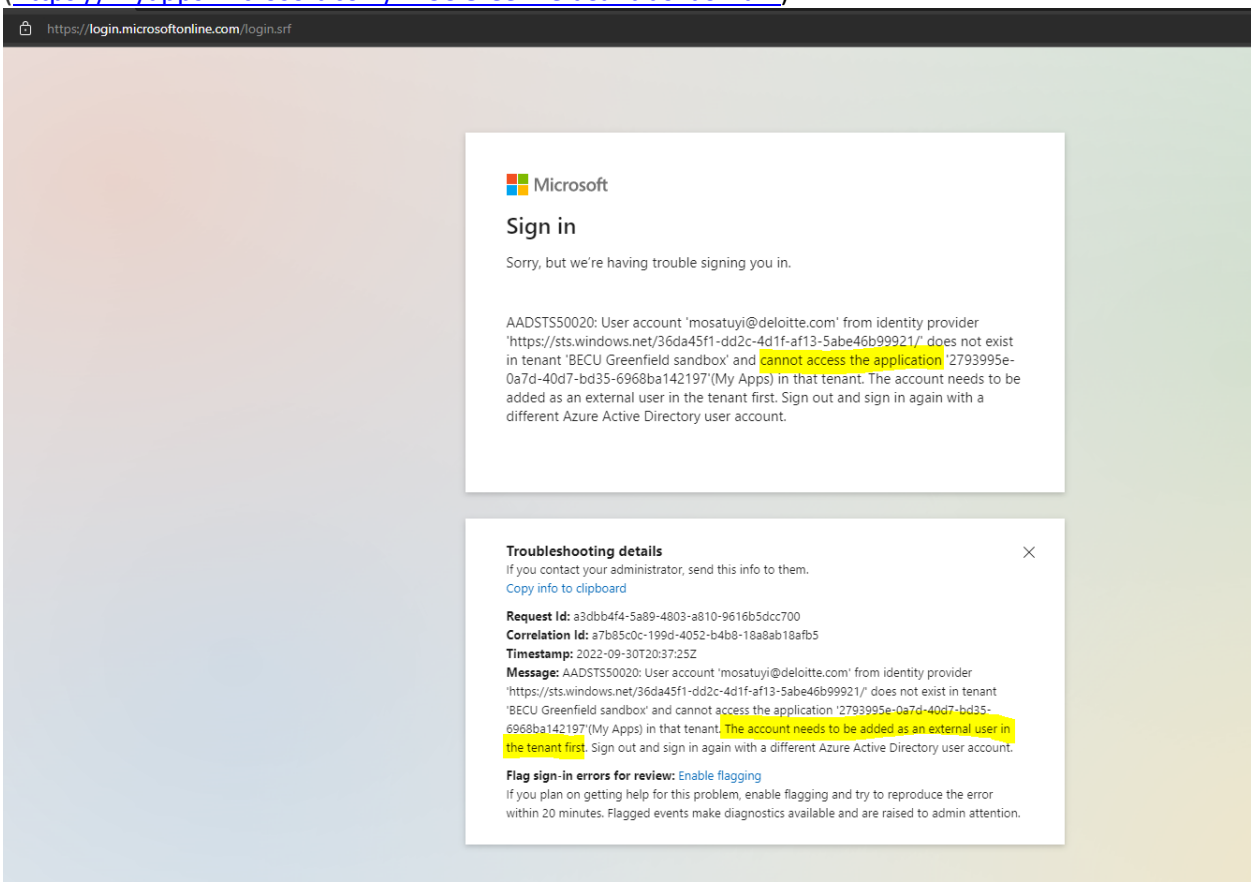


Testing Users Access After Cross Tenant Access Settings

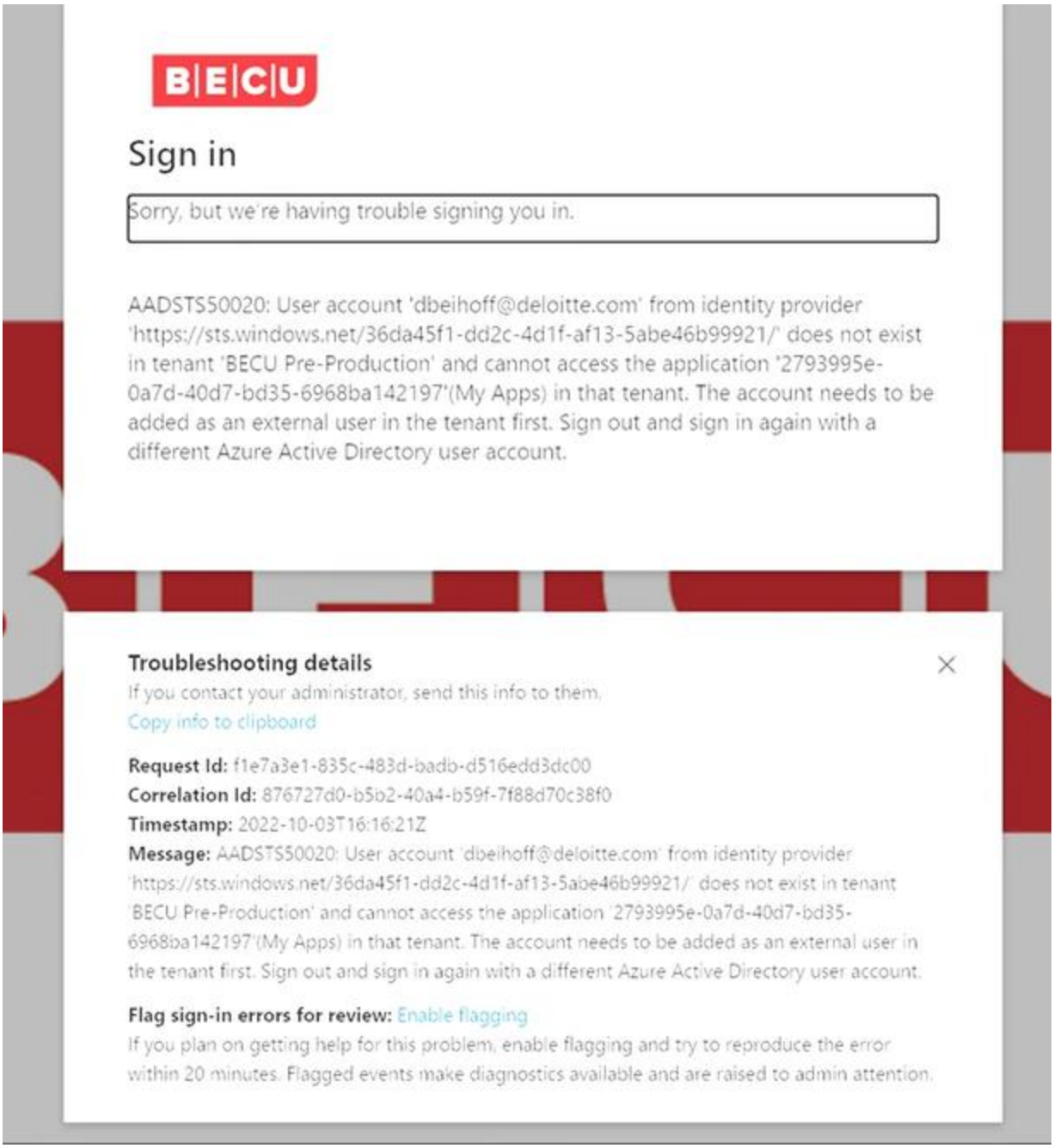
Scenerio1: A User from BECU Tech Tenant was able to access the domain of the BECU Greenfield sandbox tenant. This is since we allowed outbound access from BECU Tech to BECU Greenfield Sandbox and allow inbound access from BECU Greenfield sandbox to BECU Tech tenant (https://myapps.microsoft.com/BECUGreenfieldSandboxdomain)

Scenerio2: A User from BECU Greenfield sandbox tenant was not able to access the domain of the BECU Tech Tenant. This is since we disallowed outbound access from BECU Greenfield Sandbox to BECU Tech and disallowed inbound access from BECU Greenfield sandbox to BECU Tech tenant (https://myapps.microsoft.com/becuTechdomain)

Scenerio3: A test from a guest user from the BECU Tech tenant to try and access the BECU Greenfield sandbox tenant. Access to BECU Greenfield sandbox was denied for guest users as seen from below screenshot (https://myapps.microsoft.com/BECUGreenfieldSandboxdomain)



Sceenerio4: A test from a guest user from BECU Greenfield sandbox tenant to try and access the BECU Tech tenant. Access to BECU Tech tenant was denied for guest users as seen from below screenshot (https://myapps.microsoft.com/becu.tech)



Test Microsoft Teams Shared Channels

- Guest settings for Microsoft 365 groups must be enabled to use shared channels with external participant.
- The link below for guidance on setting up a shared channel

[Collaborate with external participants in a shared channel | Microsoft Learn]