B2B DIRECT CONNECT

Connection from BECU1 AAD to Greenfield

Production AAD tenant

October 2022

Contents

BECU B2B Direct Connect Overview ..........................................................................................2

Prerequisite Requirements.........................................................................................................2

Configuration Process Steps .......................................................................................................2

BECU1 – BECU Greenfield Production Cross Tenant Access Settings ............................................4

BECU1 – BECU Greenfield Production Inbound Settings ....................................................4

BECU1 – BECU Greenfield Production Outbound Settings .................................................7

BECU Greenfield Production – BECU1 Cross-Tenant Settings ........................................... 10

BECU Greenfield Production – BECU1 Outbound Settings................................................. 13

Testing Users Access After Cross Tenant Access Settings............................................................ 16

Test Microsoft Teams Shared Channels....................................................................................... 18

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

Production Tenant) collaborate with BECU1 Tenant (inbound access) and how BECU1

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 BECU1 and Greenfield Production

Configuration Process Steps

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

Connect

**Step Description**

1. Cross Tenant Access Settings

2. BECU1 – BECU Greenfield Production Inbound Settings

3. BECU1 – BECU Greenfield Production Outbound Settings

4. BECU Greenfield Production – BECU1 Cross-Tenant Setting

5. BECU Greenfield Production – BECU1 inbound Settings

6 BECU Greenfield Production – BECU1 Outbound Settings

7. Access Testing for test Users/Groups

- To set up a trust from the BECU1 Tenant to BECU Greenfield Production tenant, we need

the following from BECU Greenfield Production

1. Tenant ID Of BECU Greenfield Production 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 BECU1 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 Production tenant, and the name should be resolved. To add BECU Greenfield Production 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

BECU1 – BECU Greenfield Production 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.

BECU1 – BECU Greenfield Production Inbound Settings

- When BECU Greenfield Production 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

Production 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

Production 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 Production. 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 Production 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 Production external applications

-

BECU1 – BECU Greenfield Production Outbound Settings

- Outbound settings let you select users, groups and application that can access external

Greenfield Production 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

Production 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

Production 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 Production. 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 Production 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 Production 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 Production – BECU1 Cross-Tenant Setting

- Now, over at BECU Greenfield Production Tenant, we do the exact same thing, but now we enter the

tenant ID from BECU1 Tenant instead to add the organization.

- After BECU1 Tenant is added, we configure the **inbound** and **outbound** settings for

the cross-tenant access.

BECU Greenfield Production – BECU1 Inbound settings

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

Production 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 BECU1 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 Production. 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 BECU1 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 BECU1 external applications

BECU GREENFIELD SANDBOX - BECU Tech OUTBOUND SETTINGS

- Outbound settings let you select users, groups and application that can access external

Greenfield Production 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 BECU1 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 BECU1 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 BECU1. 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 Production users from accessing BECU1.

- 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 BECU1 external applications

- **B2B Direct Connect Trust Settings:** Configure weather to trust and accept claims from the

BECU1 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 BECU1 Tenant was able to access the domain of the BECU

Greenfield Production tenant. This is since we allowed outbound access from BECU1 to

BECU Greenfield Production and allow inbound access from BECU Greenfield Production to

BECU1 tenant (<https://myapps.microsoft.com/BECUGreenfieldProductiondomain>)

**Scenerio2:** A User from BECU Greenfield Production tenant was not able to access the

domain of the BECU1 Tenant. This is since we disallowed outbound access from

BECU Greenfield Production to BECU1 and disallowed inbound access from BECU

Greenfield Production to BECU1 tenant (<https://myapps.microsoft.com/becu1domain>)

**Scenerio3:** A test from a guest user from the BECU1 tenant to try and access the

BECU Greenfield Production tenant. Access to BECU Greenfield Production was denied for

guest users as seen from below screenshot

(<https://myapps.microsoft.com/BECUGreenfieldProductiondomain>)

**Sceenerio4:** A test from a guest user from BECU Greenfield Production tenant to try and

access the BECU1 tenant. Access to BECU1 tenant was denied for guest users as

seen from below screenshot (https://myapps.microsoft.com/becu.org)

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