DEGEA
WE'VE GOT YOU COVERED

Degea SOC Guest Access

Description of steps the script performs

Enterprise application (Service principal)

The first step of the script will ask you to consent to the **Degea Customer Guest Access Sync** application (Application ID: 2fb9874d-773d-4b74-bc24-282f4c0e7816).

The service principal is granted the following API permissions:

- User.Invite.All
  Allows the application to invite guest users. This is used to sync Degea users as B2B guests to the local directory.
- Directory.Read.All
  Allows the application to read directory data (e.g. groups, users, apps). This is also used as part of the sync process.

The service principal is also added to the Degea Security Reader group which allows it to add members to the group.

External Identities (Cross-tenant access)

Degea's tenant (Tenant ID: e832fb77-95d5-4bff-8f4e-09d1d922582e) is added to external identities. The settings that are explicitly set are:

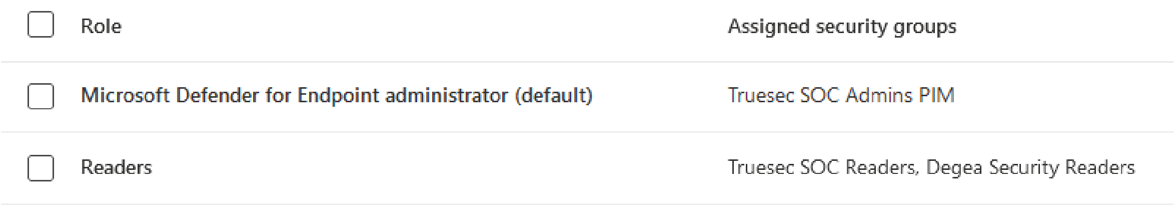
- B2B Collaboration:
  - Allow access (External users and groups)
  - Applies to: All users and groups
- Trust settings:
  - Trust MFA from Azure AD tenants
  - Trust compliant devices

Groups

A role-assignable group is created (Degea Security Readers).
The groups is assigned the Security Reader directory role. The service principal **Degea Customer Guest Access Sync** is added as owner to this group.

Manual step: https://security.microsoft.com -> Settings -> Endpoints -> Permissions -> Roles

Add the group **Degea Security Readers** to the role "Readers" in the same way as the steps in part 4.



□	Role	Assigned security groups
□	Microsoft Defender for Endpoint administrator (default)	Truesec SOC Admins PIM
□	Readers	Truesec SOC Readers, Degea Security Readers