

# Setup Azure cross-tenant access settings

## 1. Prerequisites

- Representative with Global Administrator role access.
- Minimum Microsoft Entra ID Premium P1

## 2. Background

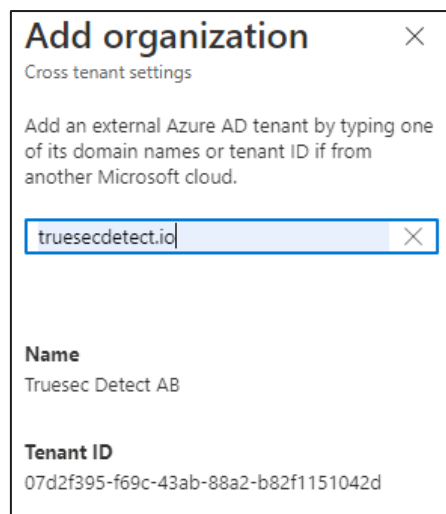
This guide describes how an organizations Azure tenant can be setup to trust MFA authentication performed in the Truesec Detect Azure tenant. It also configures the guest tenant to treat devices, verified to be compliant by the Truesec Detect Azure tenant, as compliant.

These settings will reduce the number of MFA authentications that operators in the Truesec SOC must perform, to reduce the risk of MFA fatigue, without reducing the security.

The configuration will also make it possible to restrict access to compliant devices using Conditional Access Policies, without disrupting the SOC service delivery.

## 3. Tasks

- Visit <https://portal.azure.com>
- Go to “Entra ID” → “External Identities” → “Cross-tenant access settings”
- Under “Organizational settings”, click “+ Add organization”.
  - Enter “truesecdetect.io”
  - Verify that the tenant ID match Figure 1 below and click “Add”.



**Add organization** ✕

Cross tenant settings

Add an external Azure AD tenant by typing one of its domain names or tenant ID if from another Microsoft cloud.

✕

**Name**  
Truesec Detect AB

**Tenant ID**  
07d2f395-f69c-43ab-88a2-b82f1151042d

Figure 1 Verify tenant ID

- Under “Inbound access”, click “Inherited from default”
  - Select the “B2B collaboration” tab and select “Customize settings”
  - Select “Allow access” under “Access status”.
  - Select “All Truesec Detect AB users and groups” under “Applies to”
  - Make sure the configuration looks like Figure 2 below.
  - Click “Save”

**Inbound access settings - Truesec Detect AB** ... X

**B2B collaboration** B2B direct connect Trust settings

B2B collaboration inbound access settings determine whether users from Truesec Detect AB can be invited to your organization and added to your tenant as guests. Below, specify whether Truesec Detect AB users and groups can be invited to your organization and select the applications you want to make available for B2B collaboration.  
[Learn more](#)

☐ Default settings  
☒ Customize settings

**External users and groups** Applications

**Access status**

☒ Allow access  
☐ Block access

**Applies to**

☒ All Truesec Detect AB users and groups  
☐ Select Truesec Detect AB users and groups

Figure 2 B2B collaboration settings

- Select the “Trust settings” tab and select “Customize settings”
- Enable “Trust multifactor authentication from Entra tenants”
- Enable “Trust compliant devices”
- Make sure the configuration looks like Figure 3 below.
- Click “Save”

**Inbound access settings - Truesec Detect AB** ...

B2B collaboration   B2B direct connect   **Trust settings**   Cross-tenant sync

Configure whether your Conditional Access policies will accept claims from other Microsoft Entra tenants when external users access your resources. The default settings apply to all external Microsoft Entra tenants except those with organization-specific settings.

You'll first need to configure Conditional Access for guest users on all cloud apps if you want to require multifactor authentication or require a device to be compliant or Microsoft Entra hybrid joined.  
[Learn more](#)

☐ Default settings  
☒ **Customize settings**

☒ Trust multifactor authentication from Microsoft Entra tenants  
☒ Trust compliant devices  
☐ Trust Microsoft Entra hybrid joined devices

**Automatic redemption**

☐ Check this setting if you want to automatically redeem invitations. If so, users from the specified tenant won't have to accept the consent prompt the first time they access this tenant using cross-tenant synchronization, B2B collaboration, or B2B direct connect. This setting will only suppress the consent prompt if the specified tenant checks this setting for outbound access as well.  
[Learn more](#)

☐ Automatically redeem invitations with the tenant Truesec Detect AB.

Figure 3 Trust settings

## 4. Verify

- Visit <https://portal.azure.com>
- Go to “Entra ID” → “External Identities” → “Cross-tenant access settings”
- Make sure “Truesec Detect AB” exists in the list according to the figure below (Figure 4).

Name	Inbound access	Outbound access	Tenant restrictions	Remove
Truesec Detect AB	Configured	Inherited from default	Inherited from default	

Figure 4 List after configuration has been performed.