

All about
**Azure Cross -
Tenant Setup**
by

TEMS SECURITY SERVICES





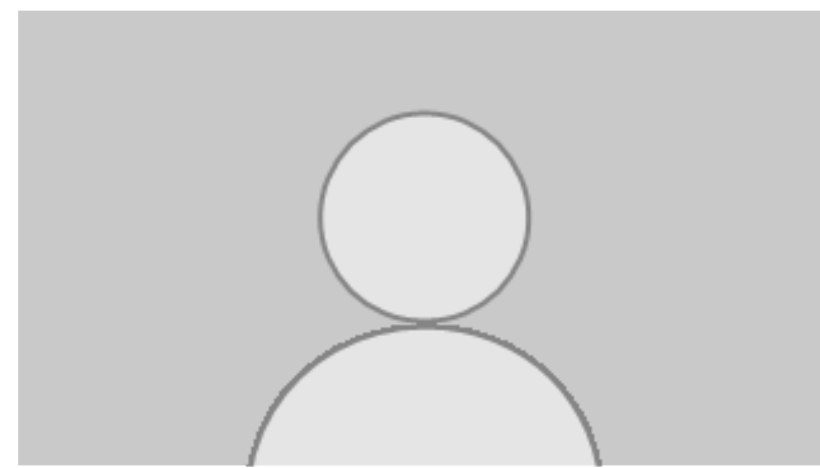
PHILIP BERGER

MICHAEL MEIXNER

Agenda

Azure Cross tenant setup

- Preparation
- Setup
- Sync
- Lesson learned




In-house advertising



Book your expert for a 30-minute Slot

<https://tems-security.at>



IT-SECURITY

CYBER-SECURITY

IT-FORENSIC

ONLINE-TERMINBUCHUNG



Philip Berger

IT-Security Specialist, Endpoint Specialist

[Hier gehts zur BUCHUNG »](#)



Michael Meixner, CISSP

DFIR, Incident Response Manager, Forensik Experte

[Hier gehts zur BUCHUNG »](#)

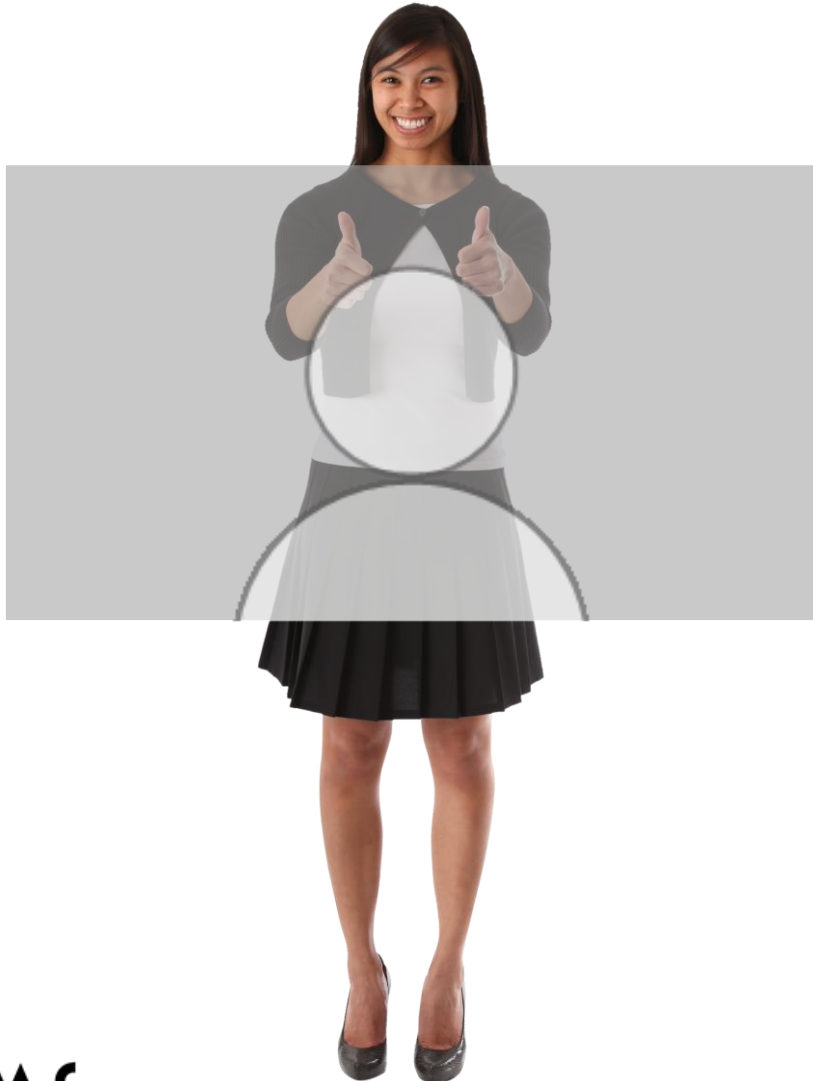



Ing. Alexander Kuchelbacher

IT-Security Specialist, Datacenter Specialist


[Hier gehts zur BUCHUNG »](#)

How easy is that?





Michael Meixner 

Grab some time with us for an appointme... [Read more](#)


\$195/hour · 4 hours 


Booking for **Michael Meixner**

 **SELECT STAFF (OPTIONAL)**

Michael Meixner 

August 10 with Michael Meixner



 **DATE**

 **TIME**

< > August 2023

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

This person isn't available on this date. Please choose another date or person.

 All times are in (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna 

Cross Tenant Setup

Preparation & Setup

- Own MS-Tenant ID
- Partner MS-Tenant ID
- New O365 Security Group *(optional)*
- Step1 : External Identity Setup
 - Inbound access
 - Outbound access
- Step 2: Cross-tenant synchronisation
 - Adjust – Mapping for cross sync
 - Define User or Group for sync *(push)*

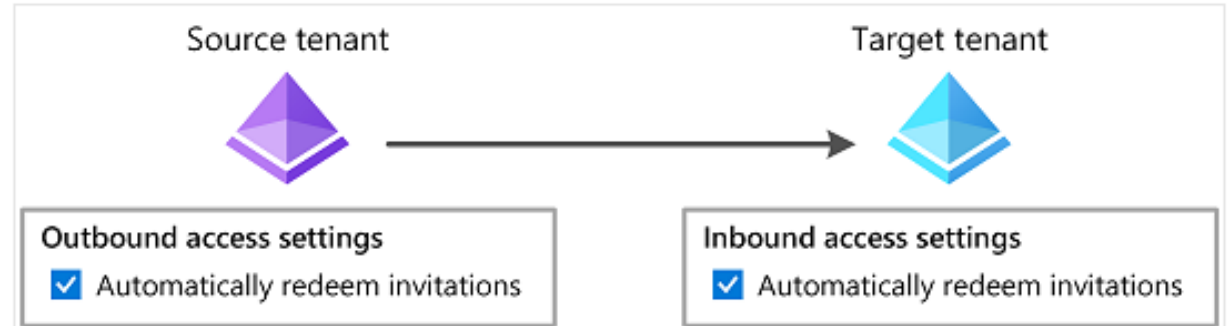


What we can see as an advantage with cross tenant



- Easier to apply and compliance with your zero trust model and IT-Security policies
- You can trust your partners MFA settings within azure.
- You can trust your partners Intune settings for compliant machine.
- Automatic notification for mass delete / add / change by your partner.
- No individual invite by users.
- All partner's email will automatically be shown in your global address book.
- Admins can set up a defined and documented workflow on both sites.
- Automatic with granted access to Azure resources without optical.
- Easy to set up, monitor and revoke if needed from a single central point of view.
- Simple audit for compliance and audit purpose on both partners.

Redemption setting



Item	Cross-tenant synchronization	B2B collaboration	B2B direct connect
Automatic redemption setting	Required	Optional	Optional
Users receive a B2B collaboration invitation email	No	No	N/A
Users must accept a consent prompt	No	No	No
Users receive a B2B collaboration notification email	No	Yes	N/A

Source: Microsoft

External Identities | Cross-tenant access settings

Tems Security Services GmbH - Azure Active Directory



Got feedback?

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes

All API connectors

Custom authentication extensions (Preview)

User flows

Subscriptions

Linked subscriptions

Lifecycle management

Terms of use

Access reviews

Troubleshooting + Support

New support request

Organizational settings

Default settings

Microsoft cloud settings

+ Add organization Refresh Columns

Use cross-tenant access settings to manage collaboration with external Azure AD organizations. For non-Azure AD organizations, use collaboration settings.

[Edit or view collaboration restrictions](#)

Organizational settings are cross-tenant access settings you've configured for specific Azure AD organizations. Any Azure AD organizations not listed here will use the default settings.

[Learn more](#)

2 organizations found

Name	Inbound access	Outbound access	Tenant
Computerforensic & more GmbH	Configured	Configured	Inheri
TEMS GmbH	Configured	Configured	Inheri

[Home](#) > [Tems Security Services GmbH | Cross-tenant synchronization](#) > [Cross-tenant synchronization | Configurations](#) >

New cross-tenant synchronization configuration ...

Azure Active Directory

Create a cross-tenant synchronization configuration by providing a name. You will be able to define your settings and start provisioning later in the setup.

[Learn more](#) 


Provide a name for your configuration (e.g. Contoso Production)

Next steps:

After creating your configuration with default parameters, you will be taken to the configuration details page to manage advanced settings.

Inbound access settings - TEMS GmbH ...

B2B collaboration B2B direct connect Trust settings Cross-tenant sync

B2B collaboration inbound access settings determine whether users from TEMS GmbH can be invited to your organization and added to your tenant as guests. B want to make available for B2B collaboration.
[Learn more](#) 

- Default settings
- Customize settings

External users and groups Applications

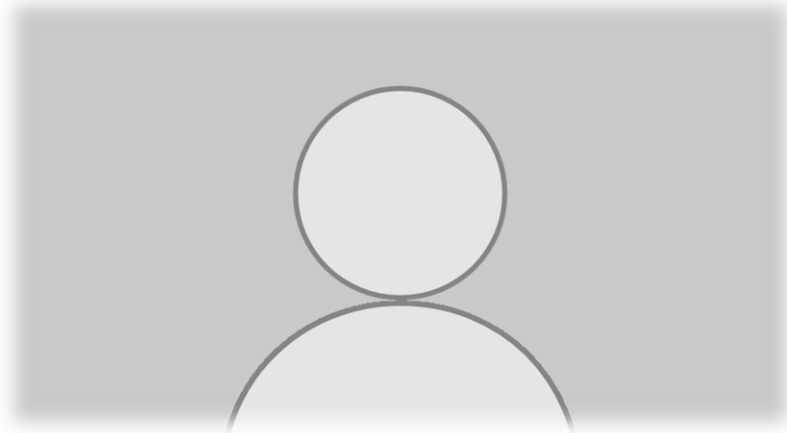
Access status

- Allow access
- Block access

Applies to

- All TEMS GmbH users and groups
- Select TEMS GmbH users and groups


Simple setup
Keep standard here 



Inbound access settings - TEMS GmbH ...


B2B collaboration B2B direct connect Trust settings Cross-tenant sync

B2B direct connect inbound access settings determine whether users from external Azure AD organizations can access your resources with connect with you. To establish a connection, an admin from the other organization must also enable B2B direct connect.

[Learn more](#) 

- Default settings
- Customize settings

External users and groups Applications

 Blocking all users also blocks all external applications

Access status

- Allow access
- Block access

Applies to

- All TEMS GmbH users and groups
- Select TEMS GmbH users and groups

Simple setup
Keep standard here



Inbound access settings - TEMS GmbH ...

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

Configure whether your Conditional Access policies will accept claims from other Azure AD organizations when external users access your resources. The default settings apply to all external Azure AD organizations.

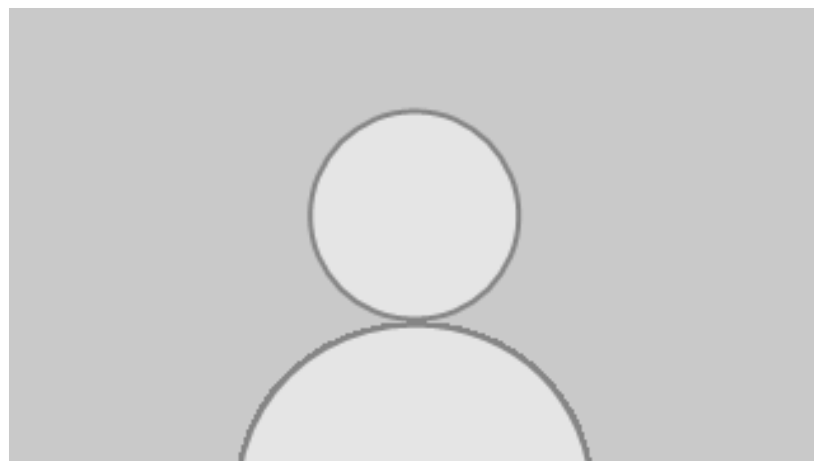
You'll first need to configure Conditional Access for guest users on all cloud apps if you want to require multifactor authentication or require a device to be compliant or hybrid Azure AD joined. [Learn more](#)

- Default settings
- Customize settings
- Trust multifactor authentication from Azure AD tenants
- Trust compliant devices
- Trust hybrid Azure AD joined devices

Automatic redemption

i 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 user resources. 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 TEMS GmbH.



[Home](#) > [Tems Security Services GmbH | External Identities](#) > [External Identities | Cross-tenant access settings](#) >

Inbound access settings - TEMS GmbH ...

[B2B collaboration](#)

[B2B direct connect](#)

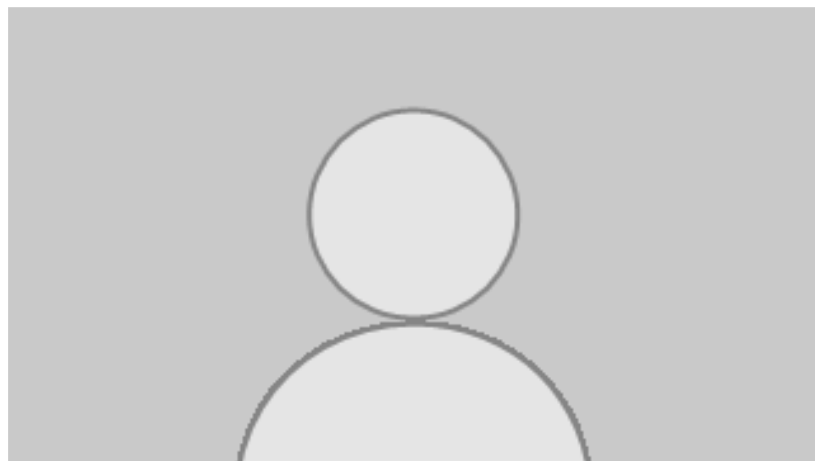
[Trust settings](#)

[Cross-tenant sync](#)

Enabling this will allow the admin of the specified (source) tenant to sync objects into this (target) tenant.

Disabling this will block admins of the source tenant from syncing objects into the target tenant but will not remove currently synced objects. We recommend that this setting should only be used between


Allow users sync into this tenant



Outbound access settings - TEMS GmbH ...

B2B collaboration B2B direct connect Trust settings

B2B collaboration outbound access settings determine whether your users can be invited to TEMS GmbH for B2B collaboration a access.

[Learn more](#) 

- Default settings
- Customize settings

Users and groups External applications

Access status

- Allow access
- Block access

Applies to


- All Tems Security Services GmbH users
- Select Tems Security Services GmbH users and groups

Simple setup 
Keep standard here


Outbound access settings - TEMS GmbH ...

B2B collaboration **B2B direct connect** Trust settings

Outbound access settings determine how your users and groups can interact with apps and resources in external organizations. The default settings can be modified but not deleted.


[Learn more](#) 

B2B direct connect lets your users and groups access apps and resources that are hosted by an external organization. To establish a connection with an external organization, limited data about your users is shared with the external organization, so that they can perform actions such as searching for resources.

[Learn more](#) 

- Default settings
- Customize settings

Users and groups External applications

 Blocking all users also blocks all external applications

Access status

- Allow access
- Block access

Applies to

- All Tems Security Services GmbH users
- Select Tems Security Services GmbH users and groups

Simple setup
Keep standard here

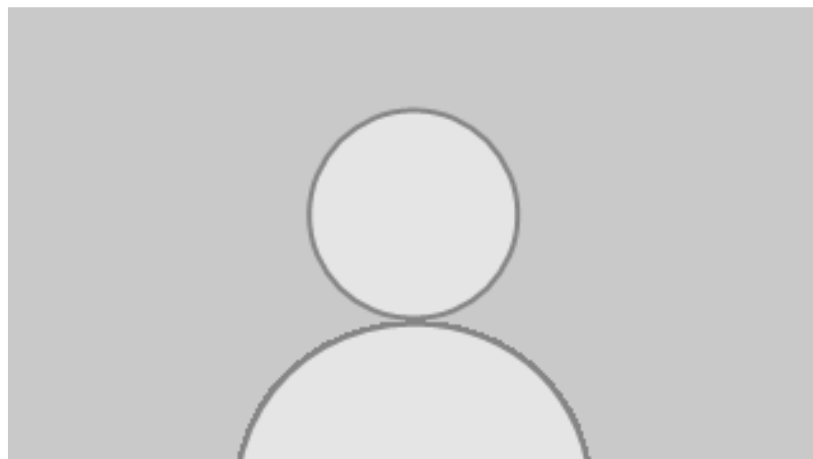


Outbound access settings - TEMS GmbH ...

B2B collaboration


B2B direct connect

Trust settings



Automatic redemption

i Check this setting if you want to automatically redeem invitations. If so, users from this tenant don't have to accept the consent prompt the first time only suppress the consent prompt if the specified tenant checks this setting for inbound access as well.

[Learn more](#) 

Automatically redeem invitations with the tenant TEMS GmbH.

- Overview
- Preview features
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Delegated admin partners
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Custom security attributes
- Licenses
- Cross-tenant synchronization
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding

<< + Add ▾ ⚙

ⓘ Azure Active Directory

Overview Mo

🔍 Search your tenant

Basic information

Name

Tenant ID

Primary domain

License

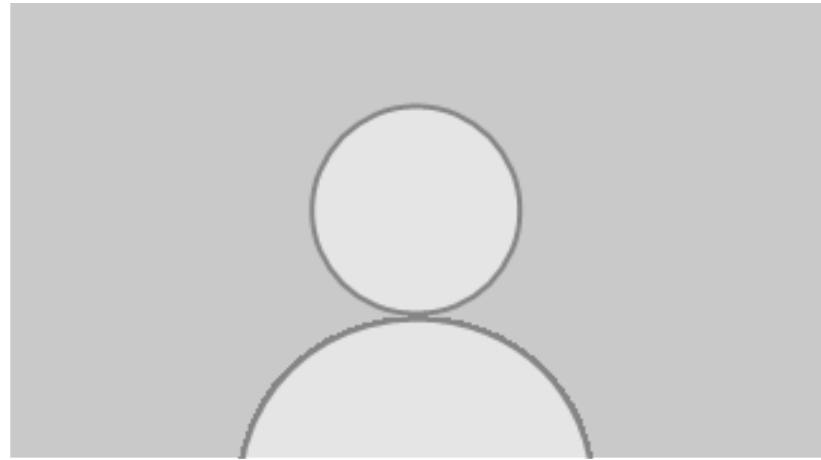
Workload License

Alerts

Upcoming
Microsoft
Director

My feed

Try Microsoft
Secure permissions



2

Cross-tenant synchronization | Configurations

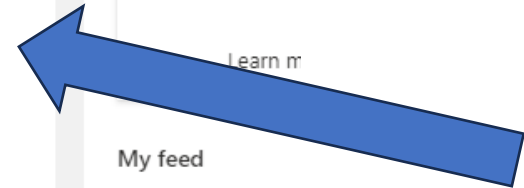
ⓘ Overview

⚙ Configurations

+ New configuration Refresh Delete Got feedback?

Sync identities between Azure AD tenants. [Learn more](#)


<input type="checkbox"/>	Name	Tenant Name
<input type="checkbox"/>	TEMS-CFM	Computerforensic & more GmbH
<input type="checkbox"/>	Tems Sec with Tems GmbH	TEMS GmbH




Tems Sec with Tems GmbH | Provisioning


Tems Security Services GmbH - Azure Active Directory


«  Save  Discard


 Overview

 Provision on demand


Manage


 Users and groups

 Provisioning


 Expression builder

Activity

 Audit logs

 Provisioning logs

Troubleshooting + Support

 New support request

Provisioning Mode


Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Tems Sec with Tems GmbH based on user and group assignment.

∨ Admin Credentials

∨ Mappings

∨ Settings

Provisioning Status 

On

Off

Attribute Mapping

 Save  Discard

Name

Provision Azure Active Directory Users

Enabled

Yes

No

Source Object

User

Source Object Scope

[All records](#)

Source Object

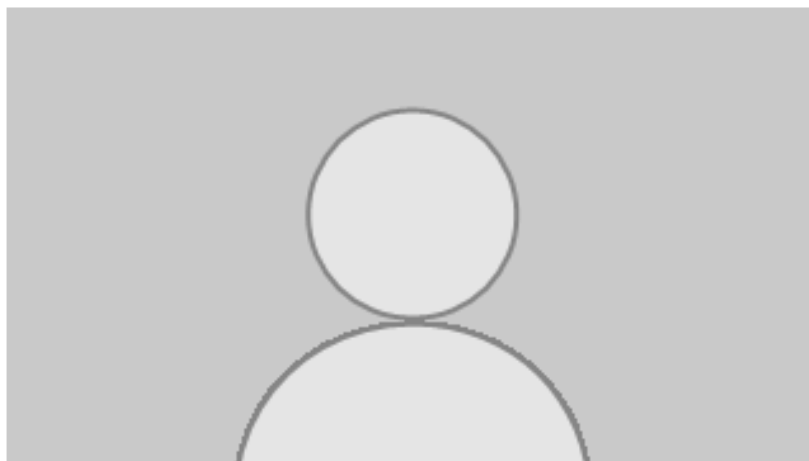
User

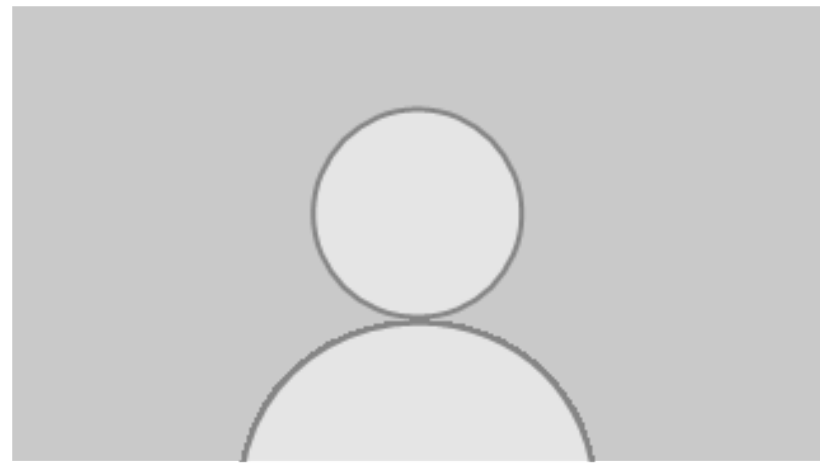
Target Object Actions

Create

Update

Delete





^ Mappings

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and Azure Active Directory (target tenant).

Name	Enabled
Provision Azure Active Directory Users	Yes

Restore default mappings

Missing Mapping overview

Edit Attribute ...

2

A mapping lets you define how the attributes in one class of Azure AD object (e.g. Users) should flow to and from this application.

Mapping type ⓘ

Expression

Expression ⓘ

Append("EXT-TEMS-SECURITY-", [displayName])

Append("EXT-TEMS-SEC-",[displayName])

The expression was correctly parsed.

Default value if null (optional) ⓘ

[Use the expression builder](#)

Target attribute * ⓘ

displayName

Match objects using this attribute

No

Matching precedence ⓘ

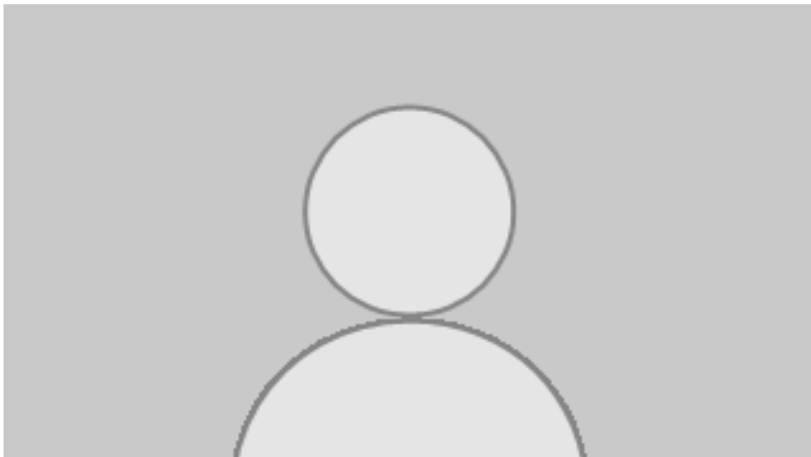
0

Apply this mapping ⓘ

Always

Tems Sec with Tems GmbH | Overview

Tems Security Services GmbH - Azure Active Directory



Start provisioning Stop provisioning Restart provisioning Edit provisioning Provision on demand Refresh Got feedback?

Overview

Provision on demand

Manage

Users and groups

Provisioning

Expression builder

Activity

Audit logs

Provisioning logs

Troubleshooting + Support

New support request

Current cycle status

Incremental cycle completed.

100% complete

Users
21

[View provisioning logs](#)

Manage provisioning

- [Update credentials](#)
- [Edit attribute mappings](#)
- [Add scoping filters](#)
- [Provision on demand](#)

Statistics to date

- [View provisioning details](#)
- [View technical information](#)

Settings

Send an email notification when a failure occurs

Notification Email ⓘ

michael.meixner@tems-security.at ✓

Prevent accidental deletion ⓘ

Accidental deletion threshold

5 ✓

Scope ⓘ

Sync only assigned users and groups ✓

Provisioning Status ⓘ

On

Off



+ New user ▾ | ↓ Download users | 📄 Bulk operations ▾ | 🔄 Refresh | ⚙️ Manage view ▾ | 🗑️ Delete | 📄 Per-user MFA | 🛠️ Preview features | 🗨️ Got feedback?

📄 [Azure Active Directory is becoming Microsoft Entra ID.](#)

🔍 Want to switch back to the legacy users list experience? [Click here to leave the preview.](#)

✕ 🔍 Add filter

1 user found

<input type="checkbox"/>	Display name ↕	User principal name ↕	User type	On-premises sy...	Identities	Company name	Creation type
<input type="checkbox"/>	EE EXT-TEMS-SECStephan Emich	Stephan.Emich_tems.at#E...	📄 Member	No	ExternalAzureAD		Invitation

Tems Sec with Tems GmbH | Provisioning

Tems Security Services GmbH - Azure Active Directory



Overview

Provision on demand

Manage

Users and groups

Provisioning

Expression builder

Activity

Audit logs

Provisioning logs

Troubleshooting + Support

New support request

Save Discard

Provisioning Mode

Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Tems Sec with Tems GmbH based on user and group assignment.

Admin Credentials

Mappings

Settings

Send an email notification when a failure occurs

Notification Email ⓘ

michael.meixner@tems-security.at

Prevent accidental deletion ⓘ

Accidental deletion threshold

5

Scope ⓘ

Sync only assigned users and groups



Provisioning Status ⓘ

On

Off

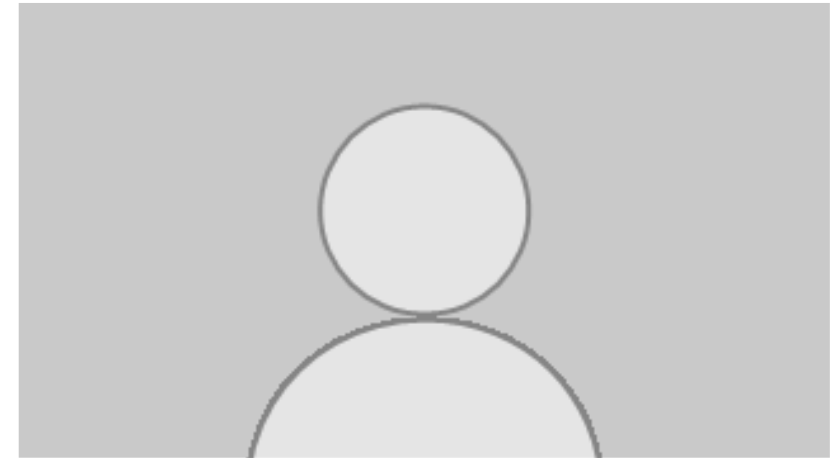


Lessons learned

- It's possible to convert User Type from Member to Guest and vice-versa by editing the user's profile in the Azure portal or by using PowerShell
- Set up tenant restrictions V2 (Preview per June 30th 2023)
 - OneDrive
 - Teams
 - non-Windows platforms.
 - Tenant, user, group, and application granularity.
- Can be used for inbound, outbound or both directions
- Setup within 2 – 3 hours from scratch with porter Azure Admin



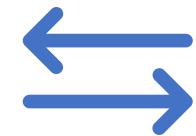
Next Webinar



August 30th
2023 09:00am



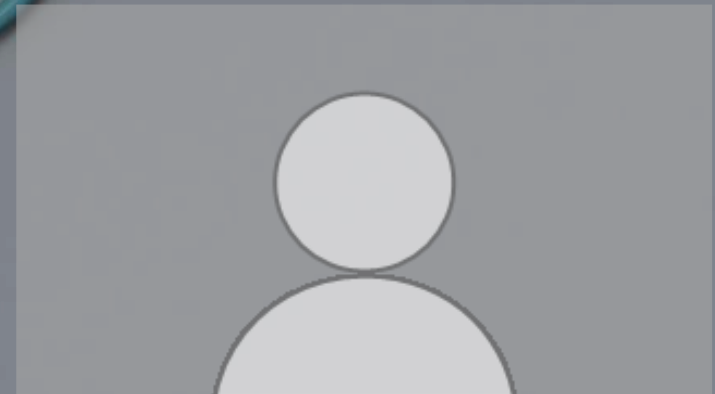
??



??

Poll 3

1. IT-Security Monitoring my Azure Tenant
2. Good practice Discussion about Conditionals Access Rules
3. IT-Security outlook by Tems Security
4. How to deal with BYOI



Q&A


tems
security



Get in contact with us


Book your expert

Philip Berger
Managing Director

 +43(664) 343 8644

 Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director

 +43(664) 1453328

 Michael.meixner@tems-security.at