

MS Teams Integration

**LMS Teams Integration Prerequisites
imc Learning Suite**

MS Teams Integration

LMS Teams Integration Prerequisites imc Learning Suite

Author(s): Andreas Pohl

Date: 2023-02-16

Document	Description
Version	ILS 14.15
Status (Draft / Review / Finalisation)	Finalisation
Contact Person(s)	Andreas Pohl

History	Status	Who
2020-07-02	Draft	Andreas Pohl
2022-03-30	Review	Nadine Gohr
2022-06-30	Review	Lia Ghiță
2022-06-30	Finalisation Version 14.13	Dr. Peter Zönnchen
2023-02-13	Finalisation Version 14.15	Bettina Stiehl/ Karlo Susac

Contents

MS Teams Integration	2
Contents	3
1 Description / Purpose	4
2 Getting Started	4
2.1 Prerequisite	4
3 Functional Summary	4
4 Configuration	5
4.1 Creation of the technical user / app	5
4.1.1 System Requirements	5
4.1.2 Technology Stack	5
4.1.3 Integration Steps	5
4.1.4 Adding Permissions on Registered Application	8
4.1.5 MS Teams application configuration	10
4.1.6 Online Meeting application access policy	12
4.1.7 REST API Documentation	12
4.2 Validation of the Active Directory settings	13
4.3 Group naming policy	14
4.4 Known Issues	16

1 Description / Purpose

The purpose of this document is to provide information on integration steps for MS Teams APIs and is divided among three sections as:

- Creation of new account on Azure portal along with steps to register a new application.
- Adding permissions to the registered application.

2 Getting Started

2.1 Prerequisite

The following pre-conditions needs to be followed for the integration of MS Teams APIs:

- The service (social-integration-backend) needs to be configured to be part of the delivery package.
- A MS Teams tenant is needed (usually included in an Office 365 subscription / tenant).
- A technical user / app needs to be created to access the Microsoft Graph API with specific permissions.
- The frontend URL need to be configured in the client properties.
- Only internal users belonging to the company's tenant can be added to the teams - no guests.
- The following MS Teams administration rights are required:

`Group.Read.All, Group.ReadWrite.All, TeamsTab.ReadWrite`

(see <https://docs.microsoft.com/en-us/graph/permissions>-reference for more details).

3 Functional Summary

- Sharing of visual representation of courses into Teams and Channels.
- Creation of an individual Teams Team per Course from within Course's Creation.
- Representation of the Course Content (Syllabus) inside the Course 's Team.
- Creation/Editing/Deletion of Online Meeting in Media/ Course Manager
- Creation of Online Meeting for Tutors in Tutor center

4 Configuration

4.1 Creation of the technical user / app

4.1.1 System Requirements

Application / Web Server

Product	Version	Fix Level
Tomcat	9	

4.1.2 Technology Stack

The following table provides a list of the technologies used for the implementation of MS Teams API's.

Name	Version	Comments
Java	1.8	
Spring boot	2.1.8	
Gradle	4.10	
Microsoft Graph SDK	1.0	
Junit	4.12	
lombok	1.18.12	

4.1.3 Integration Steps

Register New Application on Azure

To register a new application using the [Azure Portal](#) follow these steps:

- Sign into the Azure portal using either a work or school account or a personal Microsoft account.
- If your account gives you access to more than one tenant, select your account in the top right corner, and set your portal session to the Azure AD tenant that you want.
- In the left-hand navigation pane, select the **Azure Active Directory** service, and then select **App registrations > New registration**.

1. When the **Register an application** page appears, enter your application's registration information:

- **Name** - Enter a meaningful application name that will be displayed to users of the app.
- **Supported account types** - Select which accounts you would like your application to support.

Supported Account Types	Description
Accounts in this organizational directory only	<p>Select this option if you're building a line-of-business (LOB) application. This option is not available if you're not registering the application in a directory. This option maps to Azure AD only single tenant.</p> <p>This is the default option unless you're registering the app outside of a directory. In cases where the app is registered outside of a directory, the default is Azure AD multi-tenant and personal Microsoft accounts.</p>
Accounts in any organizational directory	<p>Select this option if you would like to target all business and educational customers. This option maps to an Azure AD only multi-tenant.</p> <p>If you registered the app as Azure AD only single-tenant, you could update it to be Azure AD multi-tenant and back to single-tenant through the Authentication blade.</p>
Accounts in any organizational directory and personal Microsoft accounts	<p>Select this option to target the widest set of customers. This option maps to Azure AD multi-tenant and personal Microsoft accounts.</p> <p>If you registered the app as Azure AD multi-tenant and personal Microsoft accounts, you cannot change this in the UI. Instead, you must use the application manifest editor to change the supported account types</p>

- **Redirect URI** (optional) - Select the type of app you're building, **Web** or **Public client** (mobile & desktop), and then enter the redirect URI (or reply to URL) for your application. This Option is optional and can be skipped.

2. When Finish, select **Register**.

The screenshot shows the Microsoft Azure portal interface for registering an application. The left sidebar contains navigation links for various Azure services. The main content area is titled 'Register an application' and includes the following fields and options:

- Name:** A text input field containing 'ContosoApp_1' with a green checkmark indicating it is valid.
- Supported account types:** A section titled 'Who can use this application or access this API?' with three radio button options:
 - ☒ Accounts in this organizational directory only (Contoso Enterprises)
 - ☐ Accounts in any organizational directory
 - ☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)A link 'Help me choose...' is provided below the options.
- Redirect URI (optional):** A section with a description: 'We'll return the authentication response to this URL after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.' It includes a dropdown menu set to 'Web' and a text input field containing 'https://contosoapp1/auth' with a green checkmark.
- Register:** A blue button at the bottom of the form.

Fig. 4.1: Register an application.

Azure AD assigns a unique application (client) ID to your app, and you're taken to your application's Overview page. To add additional capabilities to your application, you can select other configuration options including branding, certificates and secrets, API permissions, and more.

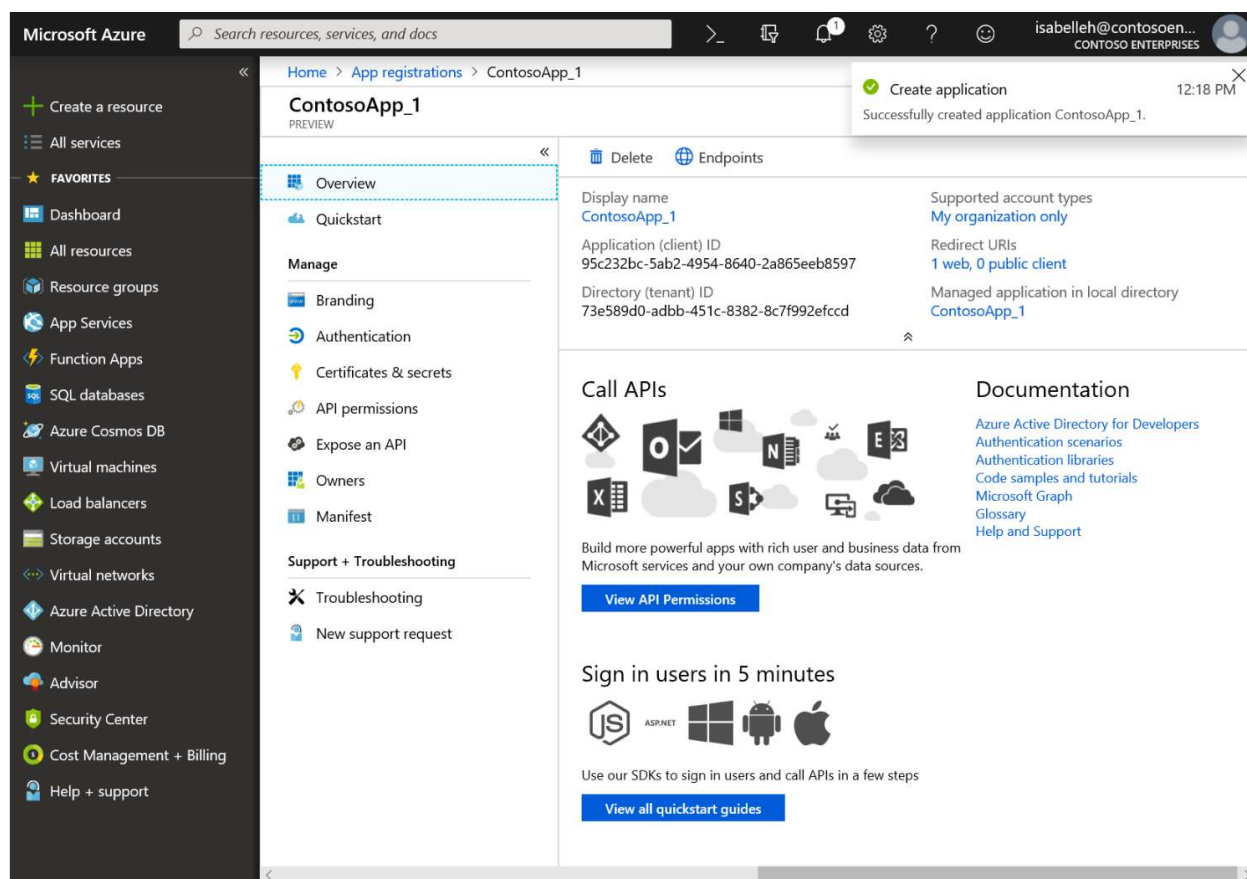


Fig. 4.2: New registered application – Overview.

4.1.4 Adding Permissions on Registered Application

Permissions are required to the registered application so as to create a new group, add and remove members from a group and adding tabs to channels. To add permissions, perform below steps:

- In the left-hand navigation pane, select the Azure Active Directory service, and then select App registrations. This will list all the registered applications. Now select the newly registered application. This will redirect to the overview page of application.
- In left-hand navigation pane select API Permissions.
- Click on Add a permission button and assign below permissions to your app at Application level and Grant admin consent:

1. Group Create/Edit
 - Group.Create
 - Group.ReadWrite.All,
 - Directory.ReadWrite.All

Group Members Add/Remove
 - GroupMember.ReadWrite.All,

Online Meeting Create/Edit/Delete
 - OnlineMeetings.ReadWrite.All

Online Meeting Attendance Tracking
- OnlineMeetingArtifact.Read.All

Invite
- User.Invite.All

Guests

To get further information about the required permissions you can follow these links:

Update groups (<https://learn.microsoft.com/en-us/graph/api/group-update?view=graph-rest-1.0&tabs=http>):

Delete groups (<https://learn.microsoft.com/en-us/graph/api/group-delete?view=graph-rest-1.0&tabs=http>):

Add group members (<https://learn.microsoft.com/en-us/graph/api/group-post-members?view=graph-rest-1.0&tabs=http>):

Remove group members (<https://learn.microsoft.com/en-us/graph/api/group-delete-members?view=graph-rest-1.0&tabs=http>):

Add group owners (<https://learn.microsoft.com/en-us/graph/api/group-post-owners?view=graph-rest-1.0&tabs=http>):

Remove group owners (<https://learn.microsoft.com/en-us/graph/api/group-delete-owners?view=graph-rest-1.0&tabs=http>):

Create an online meeting (<https://learn.microsoft.com/en-us/graph/api/application-post-online-meetings?view=graph-rest-1.0&tabs=http>):

Update online meeting (<https://learn.microsoft.com/en-us/graph/api/onlineMeeting-update?view=graph-rest-1.0&tabs=http>):

Delete online meeting (<https://learn.microsoft.com/en-us/graph/api/onlineMeeting-delete?view=graph-rest-1.0&tabs=http>):

List attendance (<https://learn.microsoft.com/en-us/graph/api/meetingattendancereport-list?view=graph-rest-1.0&tabs=http>):

Get attendance (<https://learn.microsoft.com/en-us/graph/api/meetingattendancereport-get?view=graph-rest-1.0&tabs=http>):

Invite Guest members (<https://learn.microsoft.com/en-us/graph/api/invitation-post?view=graph-rest-1.0&tabs=http>):

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Contoso

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (11) ***				
Directory.ReadWrite.All	Application	Read and write directory data	Yes	✓ Granted for Contoso ***
Group.Create	Application	Create groups	Yes	✓ Granted for Contoso ***
Group.ReadWrite.All	Application	Read and write all groups	Yes	✓ Granted for Contoso ***
GroupMember.ReadWrite.All	Application	Read and write all group memberships	Yes	✓ Granted for Contoso ***
OnlineMeetingArtifact.Read.All	Application	Read online meeting artifacts	Yes	✓ Granted for Contoso ***
OnlineMeetings.ReadWrite.All	Application	Read and create online meetings	Yes	✓ Granted for Contoso ***
TeamsTab.Create	Application	Create tabs in Microsoft Teams.	Yes	✓ Granted for Contoso ***
TeamsTab.ReadWrite.All	Application	Read and write tabs in Microsoft Teams.	Yes	✓ Granted for Contoso ***
TeamsTab.ReadWriteForTeam.All	Application	Allow the Teams app to manage all tabs for all teams	Yes	✓ Granted for Contoso ***
TeamsTab.ReadWriteSelfForTeam.All	Application	Allow the Teams app to manage only its own tabs for all t...	Yes	✓ Granted for Contoso ***
User.Invite.All	Application	Invite guest users to the organization	Yes	✓ Granted for Contoso ***

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Fig. 4.3: API permissions.

4.1.5 MS Teams application configuration

To configure the Microsoft Teams Services, we have to create a new external service provider of the type MS Teams in ILS.

In that MS Teams service provider, we pass in the values.

- Client ID
- Tenant ID
- Client secret

taken from the Azure Active Directory. These values are taken to authenticate requests from ILS to Microsoft Graph.

Created	Last update	Object ID
18-Oct-2022 14:46 (imc Admin)	06-Jan-2023 12:32 (TL_User Change_I	894

Note: Mandatory fields are marked with an asterisk (*).

☐ Relevant to validation ⓘ

Name* (50 characters max.)

MS teams provider|

Description (2000 characters max.)

MS Teams Client ID* (255 characters max.) ⓘ

CLIENT_ID

MS Teams Client Secret ID* (255 characters max.) ⓘ

.....

Tenant ID* (255 characters max.) ⓘ

TENANT_ID

Fig. 4.4: Creation External Service Provider

In the following screens you can see how to get above mentioned values.

Microsoft Azure | Search resources, services, and docs (G+/I)

Home > localenv | App registrations >

TestRegistration | Certificates & secrets

Search (Ctrl+/)

Overview

Quickstart

Integration assistant (preview)

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Roles and administrators (Pre...

Manifest

Support + Troubleshooting

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires
No certificates have been added for this application.		

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value
Password uploaded on Thu Jul 02 2020	7/2/2021	z_ED0G9dL-9UjP.z806f-tbN.4HxVGWCW

Client secret key

Fig. 4.5: Certificates & secrets.

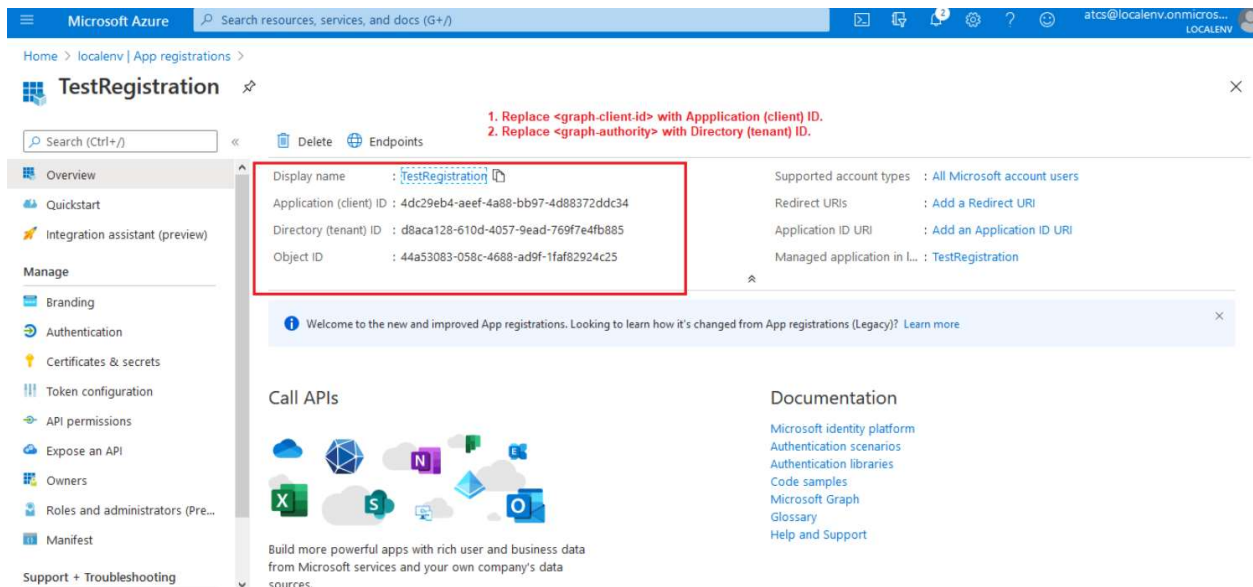


Fig. 4.6: New client secret.

4.1.6 Online Meeting application access policy

To use application permission for online meeting APIs, tenant administrators must create an **application access policy** and grant it to a user to authorize the app configured in the policy to create online meetings on behalf of that user (with user ID specified in the request path). This is a mandatory setting for the creation of online meetings.

<https://learn.microsoft.com/en-us/graph/cloud-communication-online-meeting-application-access-policy>

4.1.7 REST API Documentation

Documentation of APIs for teams can be found in Back-end project structure under `doc` folder in root directory.

- For Postman collection refer file: `IMC_Teams_Postman_Collection.json`.
- For Swagger documentation refer file: `swagger-document.json`.

4.2 Validation of the Active Directory settings

To make sure that organizations can invite guest members to online meetings in the AD under the external collaboration settings we mustn't have "No one in the organization can invite guest users including admins (most restrictive)" setting enabled.

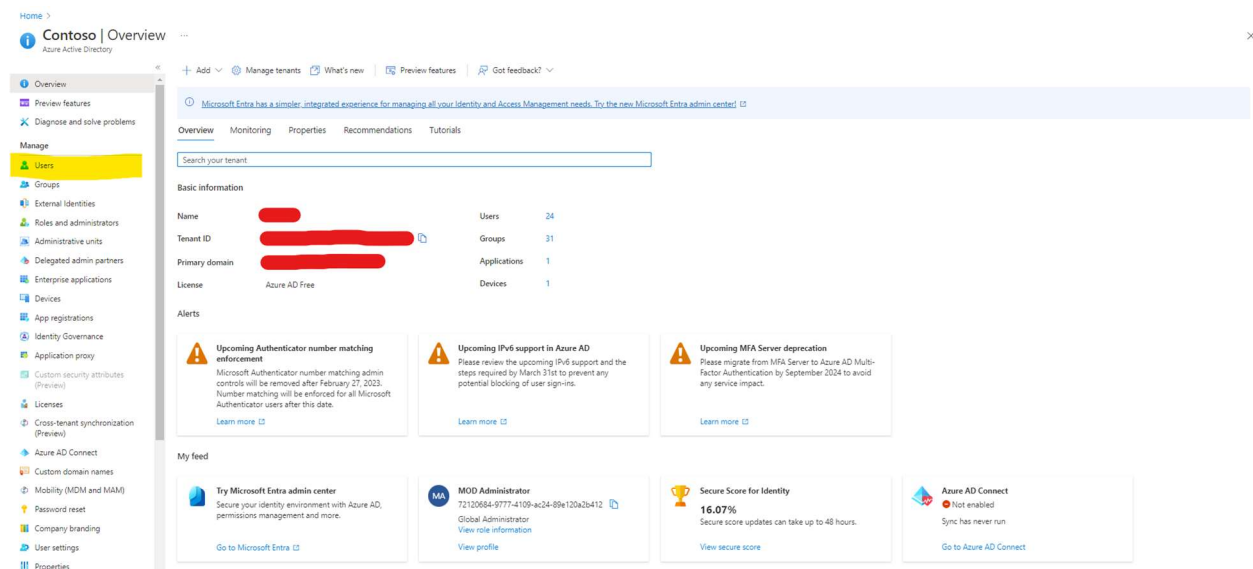


Fig. 4.7: User Settings

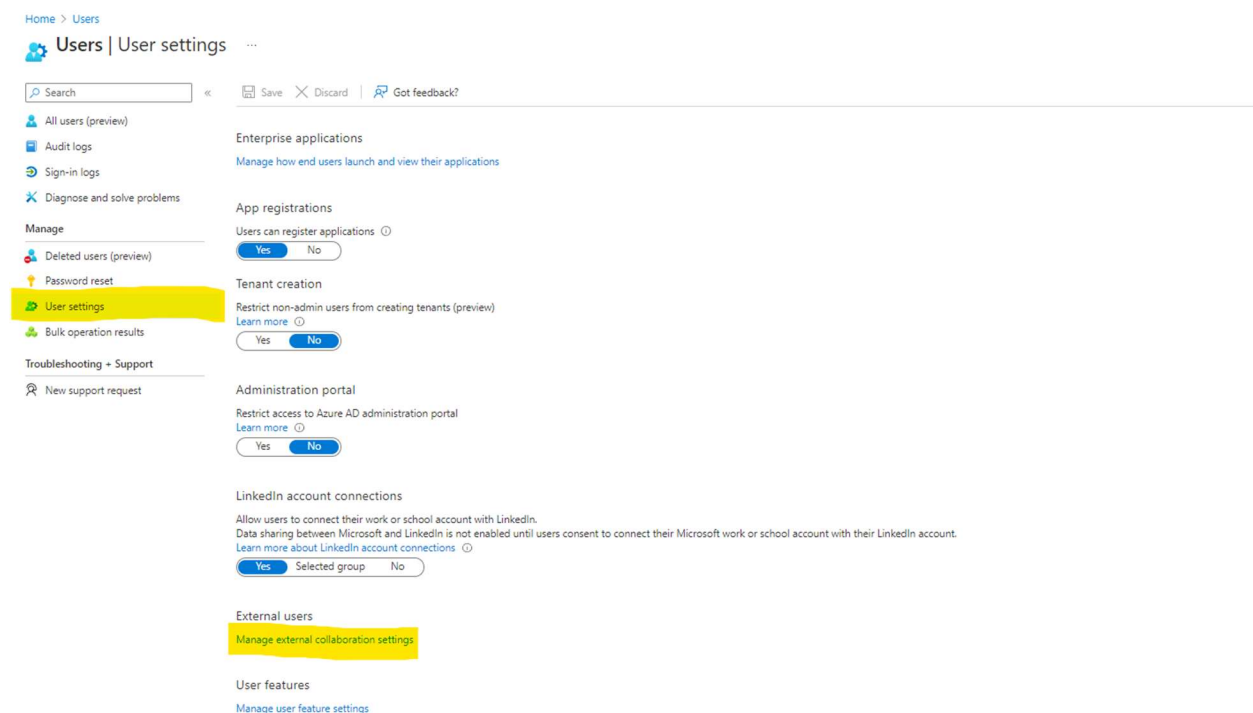



Fig. 4.8: External collaboration settings

[Home](#) > [Users | User settings](#) >

External collaboration settings

Save Discard

 Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☒ Guest users have limited access to properties and memberships of directory objects
- ☐ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- ☒ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- ☐ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- ☐ Only users assigned to specific admin roles can invite guest users
- ☐ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

Yes No

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

[Learn more](#)

Yes No

Collaboration restrictions

- ☒ Allow invitations to be sent to any domain (most inclusive)
- ☐ Deny invitations to the specified domains
- ☐ Allow invitations only to the specified domains (most restrictive)

Fig. 4.9: Guest invite settings

4.3 Group naming policy

Organizations can have a group naming policy. A group naming policy requires all organization groups to have a specific Prefix and/ or Suffix in their names. This can cause issues in the LMS group creation for MS Teams. In the External Service Provider Manager of the LMS there is a possibility to enter group Prefix/Suffix which should fit to the one defined in the AD.

Home > Contoso | Overview

Azure Active Directory

Overview | Manage tenants | What's new | Preview features | Got feedback?

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Overview | Monitoring | Properties | Recommendations | Tutorials

Search your tenant

Basic information

Name	[Redacted]	Users	24
Tenant ID	[Redacted]	Groups	31
Primary domain	[Redacted]	Applications	1
License	Azure AD Free	Devices	1

Alerts

- Upcoming Authenticator number matching enforcement**
Microsoft Authenticator number matching admin controls will be removed after February 27, 2023. Number matching will be enforced for all Microsoft Authenticator users after this date.
[Learn more](#)
- Upcoming IPv6 support in Azure AD**
Please review the upcoming IPv6 support and the steps required by March 31st to prevent any potential blocking of user sign-ins.
[Learn more](#)
- Upcoming MFA Server deprecation**
Please migrate from MFA Server to Azure AD Multi-Factor Authentication by September 2024 to avoid any service impact.
[Learn more](#)

My feed

- Try Microsoft Entra admin center**
Secure your identity environment with Azure AD, permissions management and more.
[Go to Microsoft Entra](#)
- MOD Administrator**
72120684-9777-4109-ac24-89e120a2b412
Global Administrator
[View role information](#)
[View profile](#)
- Secure Score for Identity**
16.07%
Secure score updates can take up to 48 hours.
[View secure score](#)

Feature highlights

Fig. 4.10: Group settings

Home > Contoso | Groups > Groups

Groups | Naming policy

Contoso - Azure Active Directory

Save | Discard | Delete policy

Blocked words **Group naming policy**

Group naming policy

The Microsoft 365 groups naming policy allows you to add a specific prefix and/or suffix to the group name and alias of any Microsoft 365 group created by users. For example: <Finance> <group> <Seattle>

Current policy

<Group name>

Delete

☐ Add prefix

Select the type of prefix

Delete

☐ Add suffix

Select the type of suffix

Fig. 4.11: Groups – Naming policy

4.4 Known Issues

- MS Teams owners are created from Administrator and Tutors on the first saving, they are currently not updated later.
- Tab name only in one language; will be moved to a bundle.
- Teams are not removed when course is deleted / archived - Teams can be deleted by owners inside Teams.