

Technical manual

Configure LoopBooking Azure AD user authentication.

Please note, this guide is for Administrators.

1. Introduction

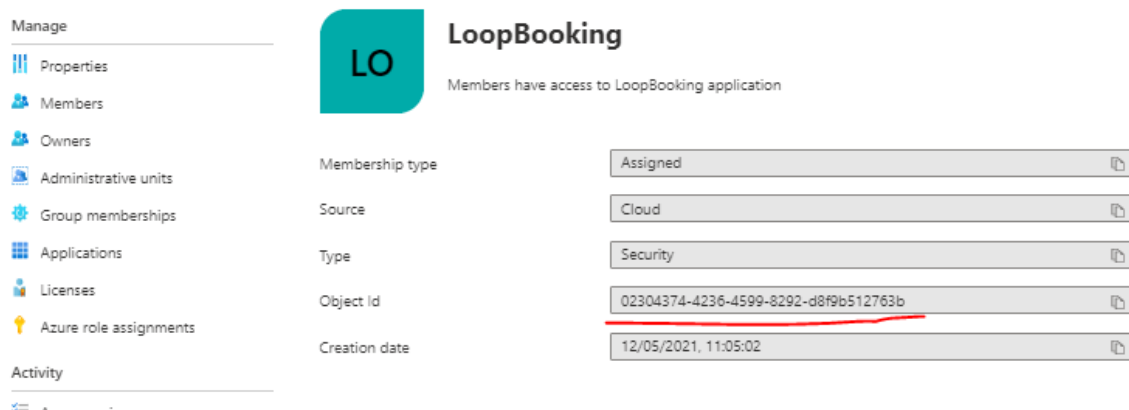
Traditionally LoopBooking (LB) uses its own user database for authentication of users. This guide will show you how to integrate with Azure AD. With this integration users can use their Azure AD (Office365) account to login to LoopBooking, enabling Single-Sign-On and MFA for their user accounts.

For this to work full name and mobile phone number must be registered on each user in Azure AD, cause the user will be created in LoopBooking the first time they log on with their Azure AD account, and these details are mandatory.

1.1 Prerequisites

Before you begin, make sure you have a security group in Azure AD with the name “LoopBooking” where all the users that will have access to the LB are members.

Make a note of the Object ID for this group, it will be needed for configuration in LoopBooking. **(Do a copy/paste into for example notepad)**



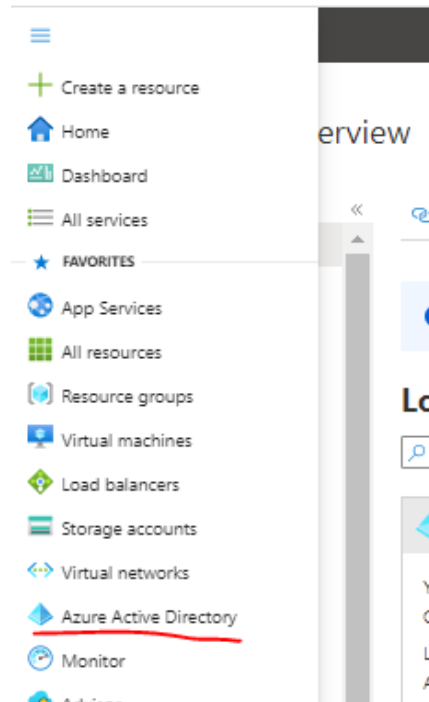
The screenshot shows the configuration page for the LoopBooking application in Azure AD. The left sidebar contains navigation options: Manage (Properties, Members, Owners, Administrative units, Group memberships, Applications, Licenses, Azure role assignments) and Activity. The main content area shows the application details for LoopBooking, including a list of members and their properties.

Property	Value
Membership type	Assigned
Source	Cloud
Type	Security
Object Id	02304374-4236-4599-8292-d8f9b512763b
Creation date	12/05/2021, 11:05:02

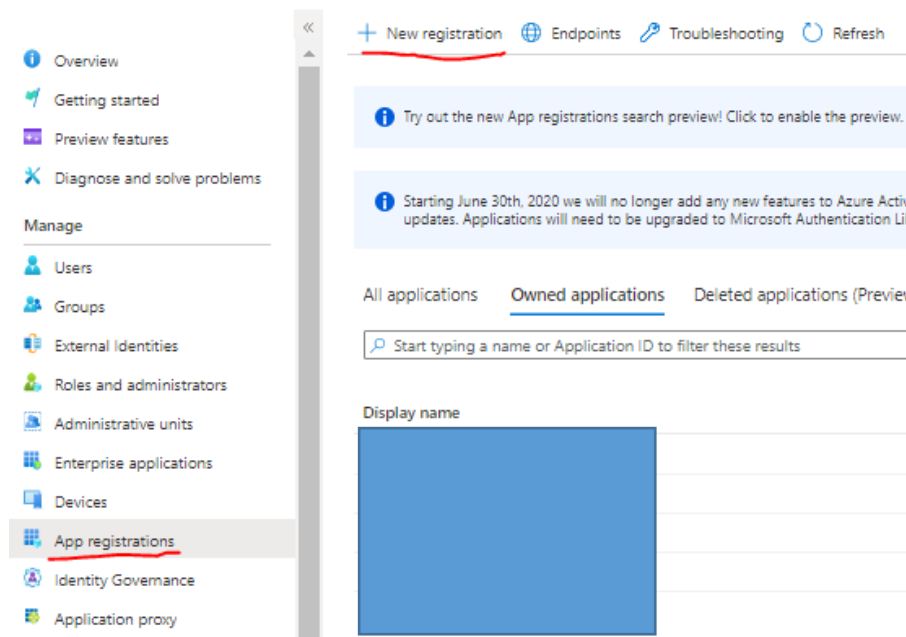
2. Register Azure Application

Open your Azure portal - <https://portal.azure.com/> and make sure you log in as a Global Administrator account.

Go to “Azure Active Directory” in you left menu.



Select “App Registrations” in the left menu and click “New Registration” in top menu.



Give the application a name, for example “LoopBooking Azure AD”

Set correct Redirect URI – <https://yoururl.loopbooking.no/login>

Then click “Register”

Register an application

*** Name**

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Loop24 AS only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI 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.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

In the left menu, select “API permissions”
 Select “Add a permission”

LoopBooking Azure AD | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview
 Quickstart
 Integration assistant

Manage

Branding
 Authentication
 Certificates & secrets
 Token configuration
API permissions
 Expose an API
 App roles
 Owners
 Roles and administrators | Preview
 Manifest

Support + Troubleshooting

Troubleshooting
 New support request

The “Admin consent required” column shows the default value for an organization. However, user consent can be used. [Learn more](#)

Configured permissions

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

+ Add a permission ✓ Grant admin consent for Loop24 AS

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

To view and manage permissions and user consent, try [Enterprise applications](#).

Select “Microsoft Graph”

Microsoft Azure Dashboard > Loop24 AS > LoopBooking Azure AD

LoopBooking Azure AD | API permissions

Search (Ctrl+/) Refresh Got feedback?

The “Admin consent required” column shows the default value for an organization. However, user consent can be used. [Learn more](#)

Configured permissions

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

+ Add a permission ✓ Grant admin consent for Loop24 AS

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

To view and manage permissions and user consent, try [Enterprise applications](#).

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
 Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
 Schedule large-scale parallel and HPC applications in the cloud.

Azure DevOps
 Integrate with Azure DevOps and Azure DevOps server.

Azure Key Vault
 Manage your key vaults as well as the keys, secrets and certificates within your Key Vaults.

Azure Rights Management Services
 Allow validated users to read and write protected content.

Azure Service Management
 Programmatic access to much of the functionality available through the Azure portal.

Azure Storage
 Secure, massively scalable object and data lake storage for unstructured and semi-structured data.

Data Export Service for Microsoft Dynamics 365
 Export data from Microsoft Dynamics CRM organization to an external destination.

Dynamics 365 Business Central
 Programmatic access to data and functionality in Dynamics 365 Business Central.

Dynamics CRM
 Access the capabilities of CRM business software and ERP systems.

Select “Delegated permissions”

The screenshot shows the 'Request API permissions' dialog in the Azure portal. Under 'What type of permissions does your application require?', the 'Delegated permissions' option is selected. A note below it states: 'Your application needs to access the API as the signed-in user.' The 'Application permissions' option is also visible but not selected.

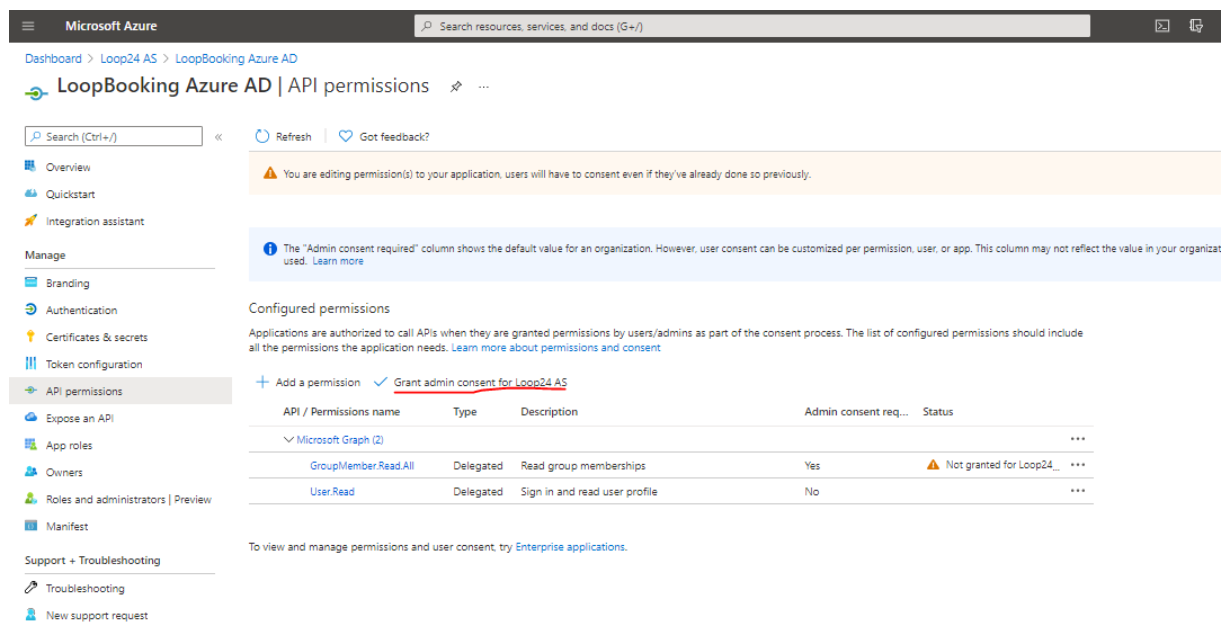
In the “select permissions” field, type “groupmember”.

Expand the GroupMember menu and select “GroupMember.Read.All”, then click “Add permissions”

This screenshot shows the 'Request API permissions' dialog with the search field containing 'groupmember'. The 'GroupMember' menu is expanded, and the 'GroupMember.Read.All' permission is selected. The 'Admin consent required' column for this permission is set to 'Yes'. The 'Add permissions' button is highlighted at the bottom of the dialog.

Permission	Admin consent required
<input checked="" type="checkbox"/> GroupMember.Read.All Read group memberships	Yes
<input type="checkbox"/> GroupMember.ReadWrite.All Read and write group memberships	Yes
> UnifiedGroupMember	

Click “Grant Admin Consent for (your tenant name)”



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

Dashboard > Loop24 AS > LoopBooking Azure AD

LoopBooking Azure AD | API permissions

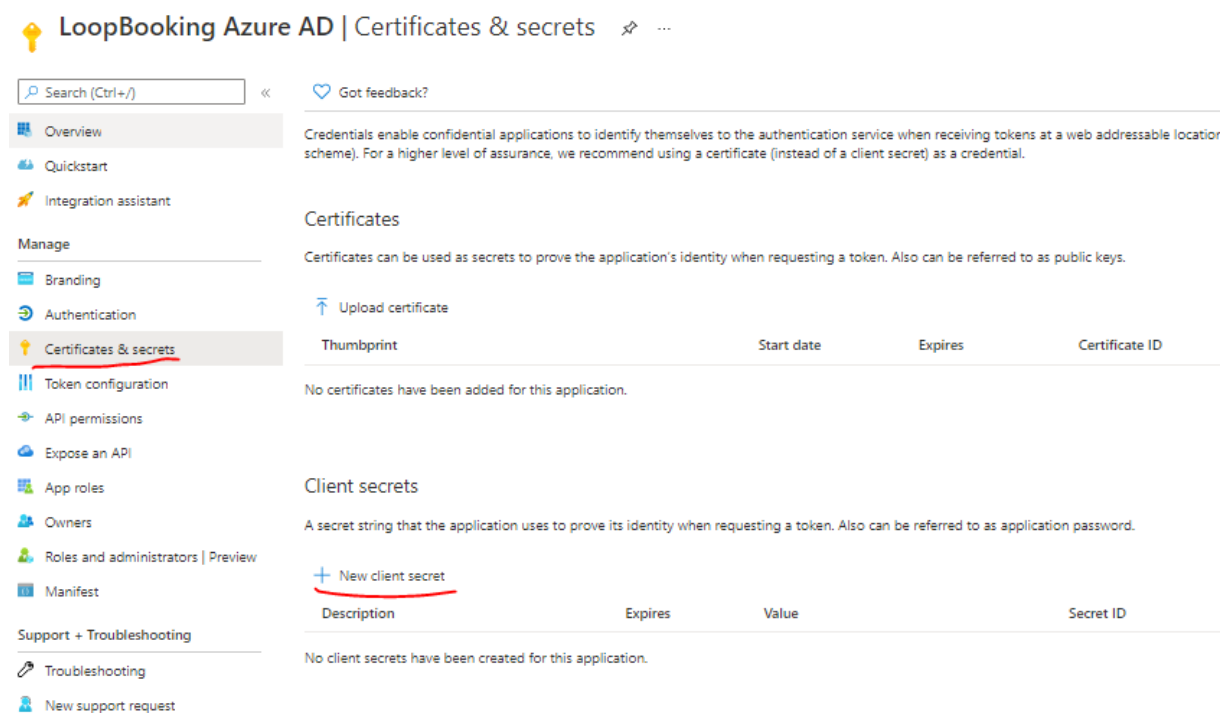
Search (Ctrl+/) | Refresh | Got feedback?

Overview, Quickstart, Integration assistant, Manage (Branding, Authentication, Certificates & secrets, Token configuration, **API permissions**, Expose an API, App roles, Owners, Roles and administrators | Preview, Manifest), Support + Troubleshooting (Troubleshooting, New support request)

Grant admin consent for Loop24 AS

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
GroupMember.Read.All	Delegated	Read group memberships	Yes	⚠ Not granted for Loop24...
User.Read	Delegated	Sign in and read user profile	No	...

Select “Certificates & Secrets” in the left menu
Press “+ New client secret”.



LoopBooking Azure AD | Certificates & secrets

Search (Ctrl+/) | Got feedback?

Overview, Quickstart, Integration assistant, Manage (Branding, Authentication, **Certificates & secrets**, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators | Preview, Manifest), Support + Troubleshooting (Troubleshooting, New support request)

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates
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	Certificate ID
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	Secret ID
No client secrets have been created for this application.			

Give it a description and select how long it is to be valid.

Remember after it expires it needs to be created again and LoopBooking integration must be reconfigured.

Make a note of the Value, this is needed later in LoopBooking configuration.
(Paste value into notepad)

LoopBooking Azure AD | Certificates & secrets

Search (Ctrl+/) | Got feedback?

Overview | Quickstart | Integration assistant | Manage | Branding | Authentication | **Certificates & secrets** | Token configuration | API permissions | Expose an API | App roles | Owners | Roles and administrators | Preview | Manifest | Support + Troubleshooting | Troubleshooting | New support request

Certificates
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.
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	Certificate ID
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	Secret ID
LB Secret	03/06/2023	<u>6qm-X-x5Vf3aXjEC27WB-Ox0byc-05t0</u>	ce836be4-8651-47a7-9263-37dc097ad584

Select "Overview" in the left hand side menu
Make a note of Application (client) ID and Directory (tenant) ID
(Paste value into notepad)

LoopBooking Azure AD

Search (Ctrl+/) | Delete | Endpoints | Preview features

Overview | Quickstart | Integration assistant | Manage | Branding | Authentication | Certificates & secrets | Token configuration | API permissions | Expose an API | App roles | Owners | Roles and administrators | Preview | Manifest | Support + Troubleshooting | Troubleshooting | New support request

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : LoopBooking Azure AD
Application (client) ID : ef135452-bddb-4555-aa24-e5172d6faa51
Object ID : 35c79790-f011-4b62-9dab-726dcb4687ad
Directory (tenant) ID : a46e1d7a-8792-487e-b21d-99e2a179d49a
Supported account types : My organization only

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Get Started | Documentation

Build your application with t
The Microsoft identity platform is an authentication service, open-source libra authentication solutions, access and protect APIs, and

3. Register Application in LoopBooking

In LoopBooking Admin Console, select the tenant that wants to use Azure AD authentication. Edit the tenant and add all the data from section 2.

Business Name*

Specify customer*

Customer ID Number*

Default Tenant Admin

Azure

Use Azure AD

Azure Domain*

Application "client" ID*

Group Object ID*

Azure Client Secret*

Directory "tenant" ID*

Business contact

Phone number*

Email*

Org. Number

Business Address

Building No, Street*

City*

State, Province

Country*

Zip Code*

*Azure Domain = your domain name (company.com)

*Group Object ID - for the security group that will have access to LoopBooking as described in section 1.1.

* Azure Client Secret is the "value" from the Certificates & Secrets.

Then save tenant settings.