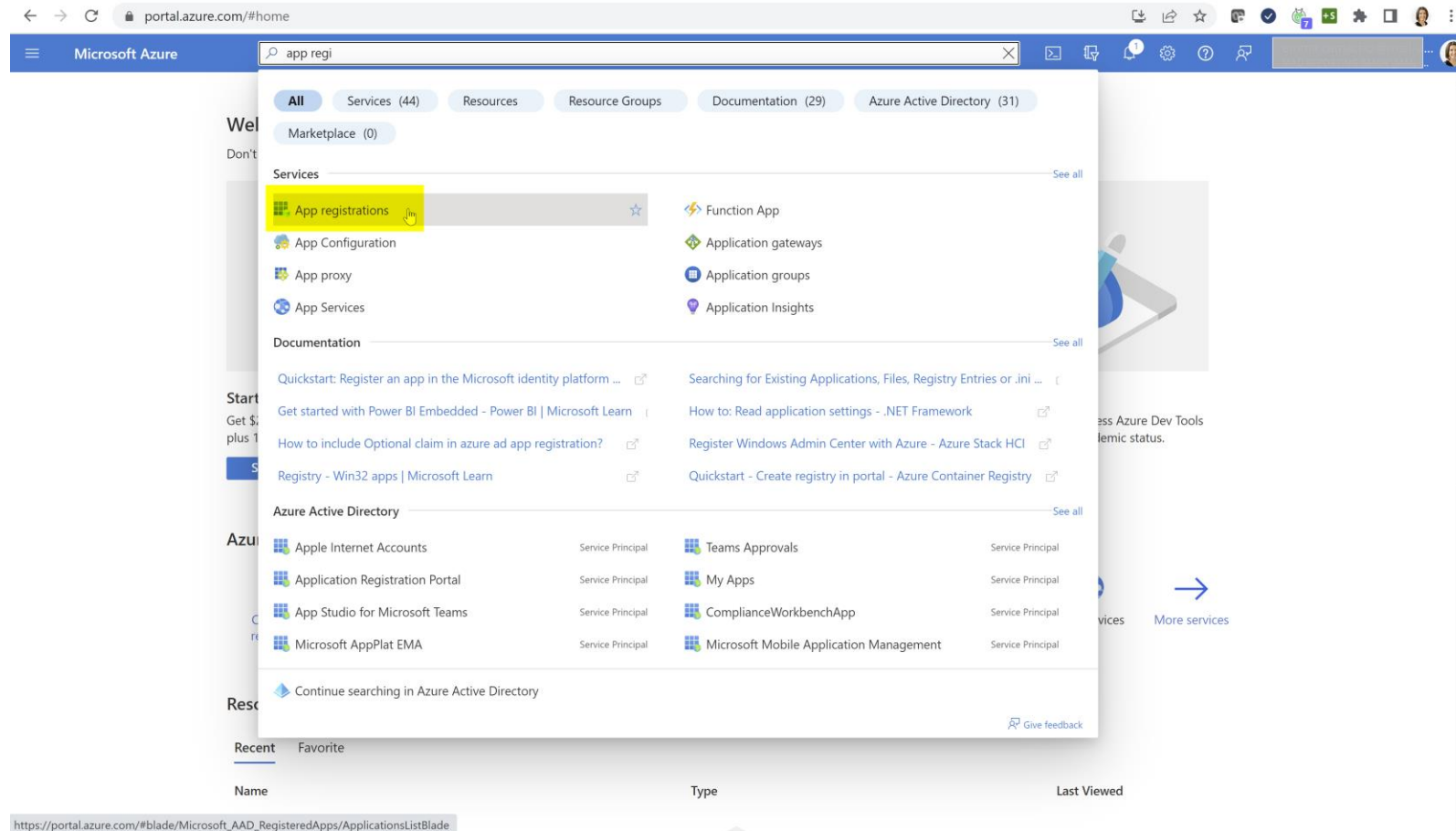




Configure Azure AD

Open portal.azure.com



Register an application

portal.azure.com/#view/Microsoft_AAD_RegisteredApps/CreateApplicationBlade/quickStartType~/null/isMSAApp~/false

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

Home > App registrations >

Register an application

* Name

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

MaD Tutorial ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory 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.

Select a platform e.g. https://example.com/auth

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](#)

Register

In Token configuration, add optional claims

portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade~/TokenConfiguration/appld/4bb621ee-64a4-40e6-8156-e9df9716327b/isMS...

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

Home > App registrations > MaD Tutorial

MaD Tutorial | Token configuration

Search Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration**
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim + Add groups claim

Claim ↑↓	Description
email	The addressable email for this user, if the user has one
upn	An identifier for the user that can be used with the username_hint parameter; no
verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail
xms_pl	User-preferred language

https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade~/Ap...

Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

*Token type

Access and ID tokens are used by applications for authentication. [Learn more](#)

- ☒ ID
☐ Access
☐ SAML

Claim ↑↓	Description
<input type="checkbox"/> acct	User's account status in tenant
<input type="checkbox"/> auth_time	Time when the user last authenticated; See OpenID Con...
<input type="checkbox"/> ctry	User's country/region
<input checked="" type="checkbox"/> email	The addressable email for this user, if the user has one
<input type="checkbox"/> family_name	Provides the last name, surname, or family name of the ...
<input type="checkbox"/> fwd	IP address
<input type="checkbox"/> given_name	Provides the first or "given" name of the user, as set on ...
<input type="checkbox"/> in_corp	Signals if the client is logging in from the corporate net...
<input type="checkbox"/> ipaddr	The IP address the client logged in from
<input type="checkbox"/> login_hint	Login hint
<input type="checkbox"/> onprem_sid	On-premises security identifier
<input type="checkbox"/> preferred_username	Provides the preferred username claim, making it easier...
<input type="checkbox"/> pwd_exp	The datetime at which the password expires

Add Cancel

Add optional claim

Some of these claims (email, upn) require OpenID Connect scopes to be configured through the API permissions page or by checking the box below. [Learn more](#)

☒ Turn on the Microsoft Graph email, profile permission (required for claims to appear in token).

Add Cancel

Get the FQDN and Callback URL Folder from M&D

Settings -> Server

Server Configuration

GENERAL SERVICE ENDPOINTS ADDITIONAL SETTINGS

Authentication

TYPE: Windows

USERNAME: SERVER\md_service

PASSWORD:

Network

FQDN: SERVER

Enable HTTP: ☒

HTTP PORT: 14999

Enable HTTPS: ☒

HTTPS PORT: 14998

THUMBPRINT: D2C26F2364A1D60801CF81A43C38CA2F995F122F

Debugging

Enable Debug Mode: ☐

Settings -> User Directories -> Create User Directory -> Azure AD

Create: Azure AD User Directory

GENERAL USER GROUP QUERIES

NAME:

TENANT ID:

CLIENT ID:

CLIENT SECRET:

CALLBACK URL FOLDER: AuthenticationCallback/AzureAd

TEST CONNECTION

Keep this window open!

In Authentication, Add a platform

Microsoft Azure

Home > App registrations > MaD Tutorial

MaD Tutorial | Authentication

Search resources, services, and docs (G+/)

Search

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required, such as redirect URIs, specific authentication settings, or fields specific to the platform.

Add a platform

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

Yes No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

App instance property lock

Configure the application instance modification lock. [Learn more](#)

Configure

Configure single-page application

All platforms Quickstart Docs

The latest version of MSAL.js uses the authorization code flow with PKCE and CORS. [Learn more](#)

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

Grant types

MSAL.js 2.0 does not support implicit grant. Enable implicit grant settings only if your app is using MSAL.js 1.0. [Learn more about auth code flow](#)

☒ Your Redirect URI is eligible for the Authorization Code Flow with PKCE.

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens](#)

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows)

Configure Cancel

In Certificates & secrets add a New client secret

The screenshot displays the Microsoft Azure portal interface. On the left, the navigation pane shows the 'Certificates & secrets' section under 'MaD Tutorial'. The main content area shows the 'Client secrets (1)' tab. A dialog box titled 'Add a client secret' is open on the right. The dialog contains two fields: 'Description' with the value 'AzureAD' and 'Expires' set to '730 days (24 months)'. At the bottom of the dialog are 'Add' and 'Cancel' buttons. The background page shows a table with columns 'Description', 'Expires', 'Value', and 'Secret ID', and a '+ New client secret' button.

Microsoft Azure

Home > App registrations > MaD Tutorial

MaD Tutorial | Certificates & secrets

Search resources, services, and docs (G+)

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

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

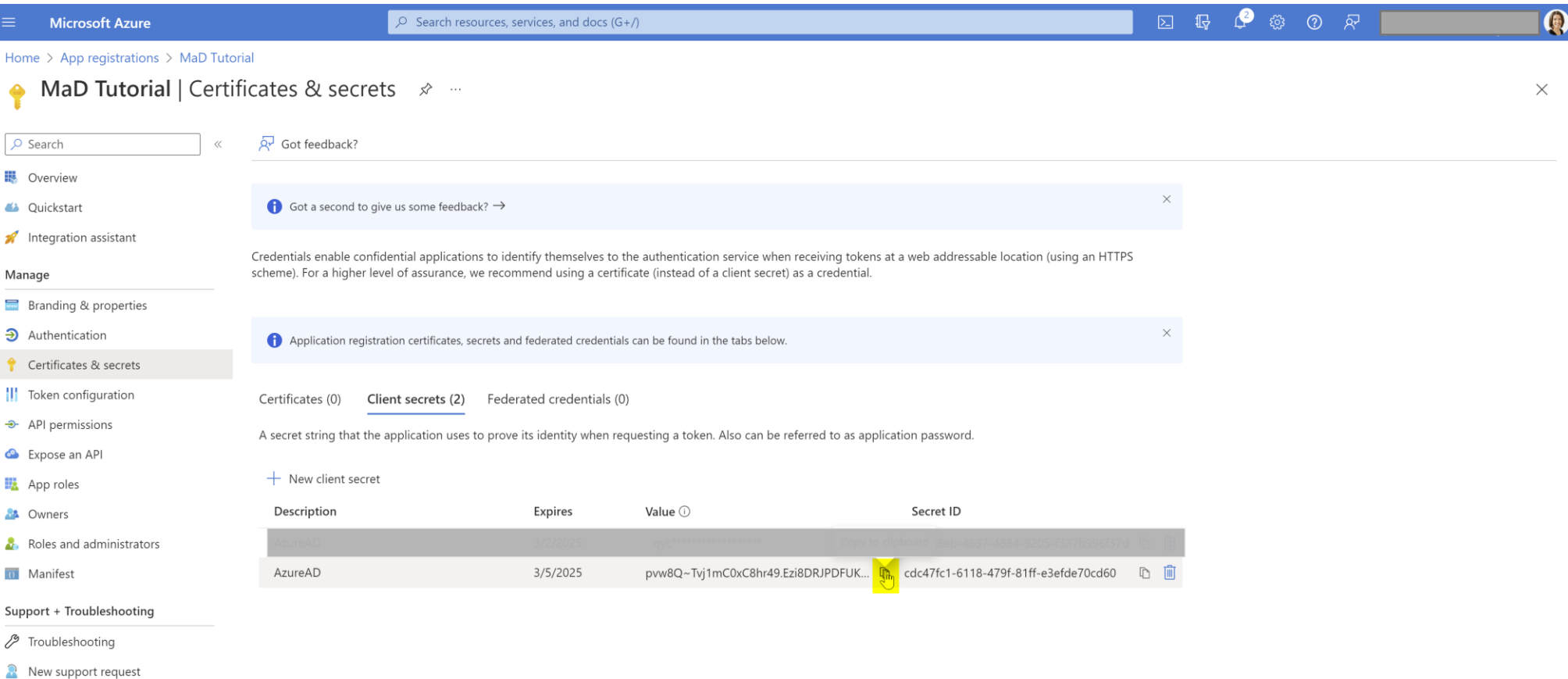
Add a client secret

Description AzureAD





Expires 730 days (24 months)

Add Cancel

100



Paste the value in the Client Secret property

 Create: Azure AD User Directory   

GENERAL

USER GROUP QUERIES

NAME

TENANT ID


CLIENT ID

CLIENT SECRET

.....

CALLBACK URL FOLDER

AuthenticationCallback/AzureAd

 TEST CONNECTION

In API permissions, Add Microsoft Graph permissions

Microsoft Azure

Home > App registrations > MaD Tutorial

MaD Tutorial | API permissions

Search

Refresh | Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

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

Configured permissions

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

+ Add a permission

Grant admin consent for MaD Reporting GmbH

API / Permissions name	Type	Description
Microsoft Graph		
email	Delegated	View users' email addresses
groups.read.all	Application	Read all groups
openid	Delegated	Sign users in
profile	Delegated	View users' basic profile
users.read.all	Application	Read all users' full profiles

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

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 Communication Services

Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

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

Flow Service

Embed flow templates and manage flows

Add Delegated permissions

Request API permissions

< All APIs



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Start typing a permission to filter these results



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission

Admin consent required

OpenId permissions (3)

<input checked="" type="checkbox"/>	email ⓘ View users' email address	No
<input type="checkbox"/>	offline_access ⓘ Maintain access to data you have given it access to	No
<input checked="" type="checkbox"/>	openid ⓘ Sign users in	No
<input checked="" type="checkbox"/>	profile ⓘ View users' basic profile	No
<input checked="" type="checkbox"/>	User.Read ⓘ Sign in and read user profile	No

Add permissions

Discard

Delegated permissions

- email
- openid
- profile
- User.Read

Add Application permissions

Request API permissions ×

[All APIs](#)

Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

group.read.all

Permission	Admin consent required
Group (1)	
<input checked="" type="checkbox"/> Group.Read.All ⓘ Read all groups	Yes
<input checked="" type="checkbox"/> User.Read.All ⓘ Read all users' full profiles	Yes

Add permissions Discard

Application permissions

- Group.Read.All
- User.Read.All

Grant the permissions, if needed

Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations > MaD Tutorial

MaD Tutorial | API permissions

Search

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the

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 MaD Reporting GmbH

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (5)				
email	Delegated	View users' email address	No	Granted for MaD Report...
Group.Read.All	Application	Read all groups	Yes	Granted for MaD Report...
openid	Delegated	Sign users in	No	Granted for MaD Report...
profile	Delegated	View users' basic profile	No	Granted for MaD Report...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for MaD Report...

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

In Enterprise applications, disable Assignment required

The screenshot displays the Microsoft Azure portal interface for managing an Enterprise Application named 'MaD Tutorial'. The left-hand navigation pane includes sections for Overview, Deployment Plan, Diagnose and solve problems, Manage (with Properties highlighted), Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, Custom security attributes (preview), Security (with Conditional Access, Permissions, and Token encryption), and Activity (with Sign-in logs, Usage & insights, and Audit logs). The main content area shows the 'Properties' tab for the application. It includes a header with 'Save', 'Discard', 'Delete', and 'Got feedback?' options. Below this, there is a description of the application and a link to 'Learn more'. The 'Assignment required?' toggle is currently set to 'No', which is highlighted with a yellow box. Other visible fields include 'Name' (MaD Tutorial), 'Homepage URL', 'Logo' (MT), 'Application ID' (4bb621ee-64a4-40e6-8156-e9df9716327b), 'Object ID' (34f957ae-2e0a-4046-bbc2-347d9322a9e7), and 'Visible to users?' (set to 'No').

Microsoft Azure

Home > Enterprise applications | All applications > MaD Tutorial

MaD Tutorial | Properties

Enterprise Application

« Save Discard Delete Got feedback?

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

If this application resides in your tenant, you can manage additional properties on the [application registration](#).

Enabled for users to sign-in? ☒ Yes ☐ No

Name *

Homepage URL

Logo

Application ID

Object ID

Assignment required? ☐ Yes ☒ No

Visible to users? ☐ Yes ☒ No

Notes

Copy the client ID and tenant ID to M&D

Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations > MaD Tutorial

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Essentials

Display name : MaD Tutorial

Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : My organization only

Client credentials : 0 certificate, 1 secret

Redirect URIs : 0 web, 3 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in ... : MaD Tutorial

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)





Get Started Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

Icons representing various Microsoft services: X, S, N, E, O, and a clock icon.

Copy the client ID and tenant ID to M&D, and test connection

 Create: Azure AD User Directory   

GENERAL

USER GROUP QUERIES

NAME

AzureAD

TENANT ID


CLIENT ID


CLIENT SECRET

.....


CALLBACK URL FOLDER

AuthenticationCallback/AzureAd

 TEST CONNECTION

 CONNECTION SUCCESSFUL

The connection to the Azure AD could successfully be established.



Create a User Group

Edit: Azure AD User Directory

GENERALUSER GROUP QUERIES

Name

Development

CREATE USER GROUP QUERY


Click this button to create a new user group query.

Create: User Directory User Group Query





















GENERAL

NAME	
MATCHING METHOD	Exact Match
MEMBERS TYPE	Standard User
DEFAULT LANGUAGE	English
TIME ZONE	(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
CULTURE	Deutsch (Österreich)

And press sync

 User Directories

LIST

Name	Type	
Azure AD	Azure AD	    
Executive Dashboard OLD format	CSV File	    
Workshop	CSV File	    
Workshop Toare	CSV File	    

CREATE USER DIRECTORY

Click this button to sync

Add an Azure AD Service Endpoint

M&D Management Console -> Settings -> SERVER -> SERVICE ENDPOINTS -> CREATE ENDPOINT

The screenshot displays the 'Server Configuration' window with the 'SERVICE ENDPOINTS' tab selected. A modal dialog titled 'Edit: Service Endpoint' is open, showing the 'GENERAL' tab. The dialog contains four fields: 'URL FOLDER' with the value 'Management/AzureAD', 'SERVICE' with the value 'Management Service', 'AUTHENTICATION METH...' with the value 'Azure AD', and 'USER DIRECTORY' with the value 'Azure AD'. The background shows a table of existing service endpoints.

URL Folder	Service	Authentication Method
Api	API Service	Access Key
Heartbeat	Heartbeat Service	None
Hub	Hub Service	Windows
Hub/Custom	Hub Service	Custom
Management	Management Service	Windows

Edit: Service Endpoint

GENERAL

URL FOLDER: Management/AzureAD

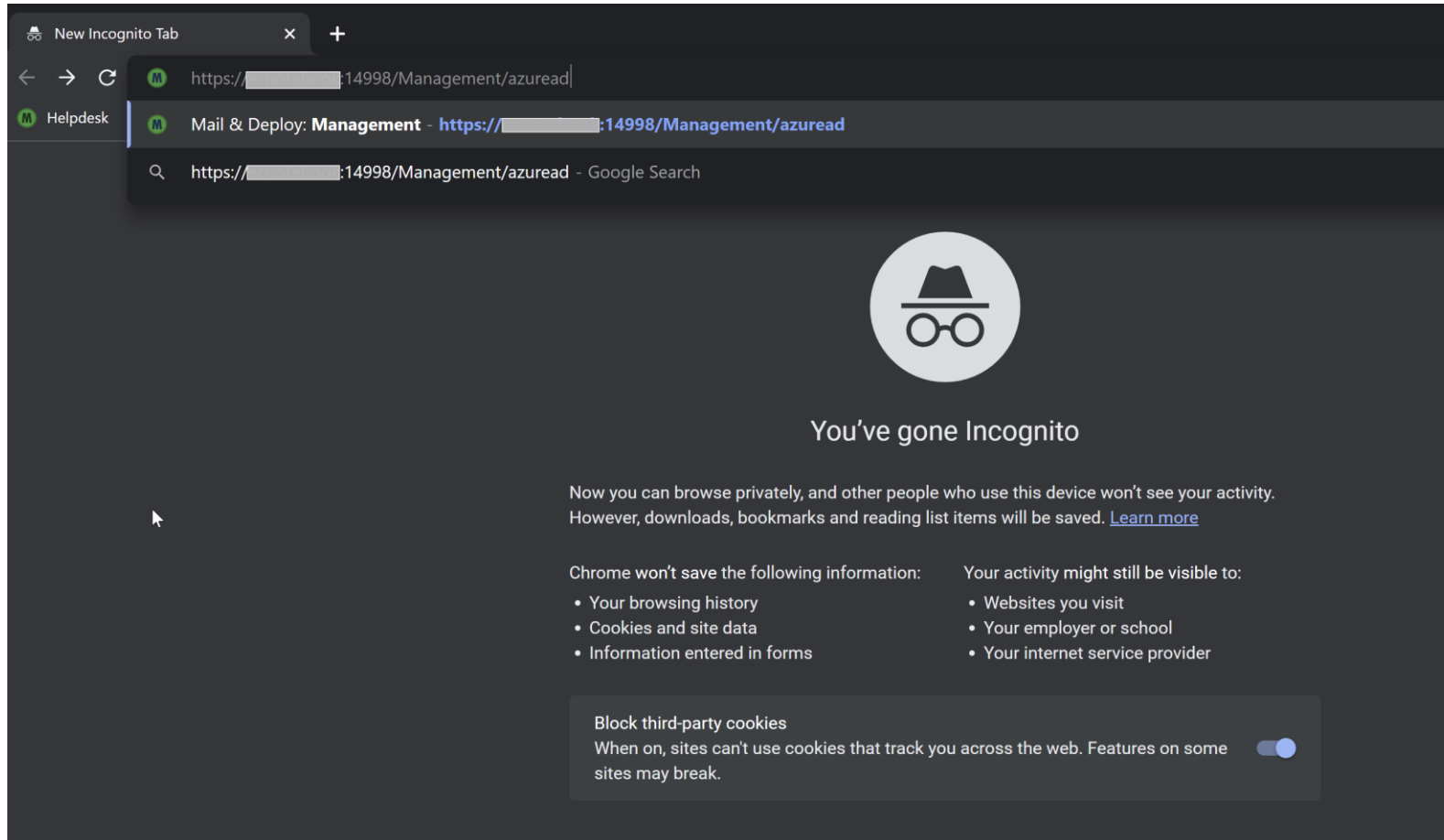
SERVICE: Management Service

AUTHENTICATION METH...: Azure AD

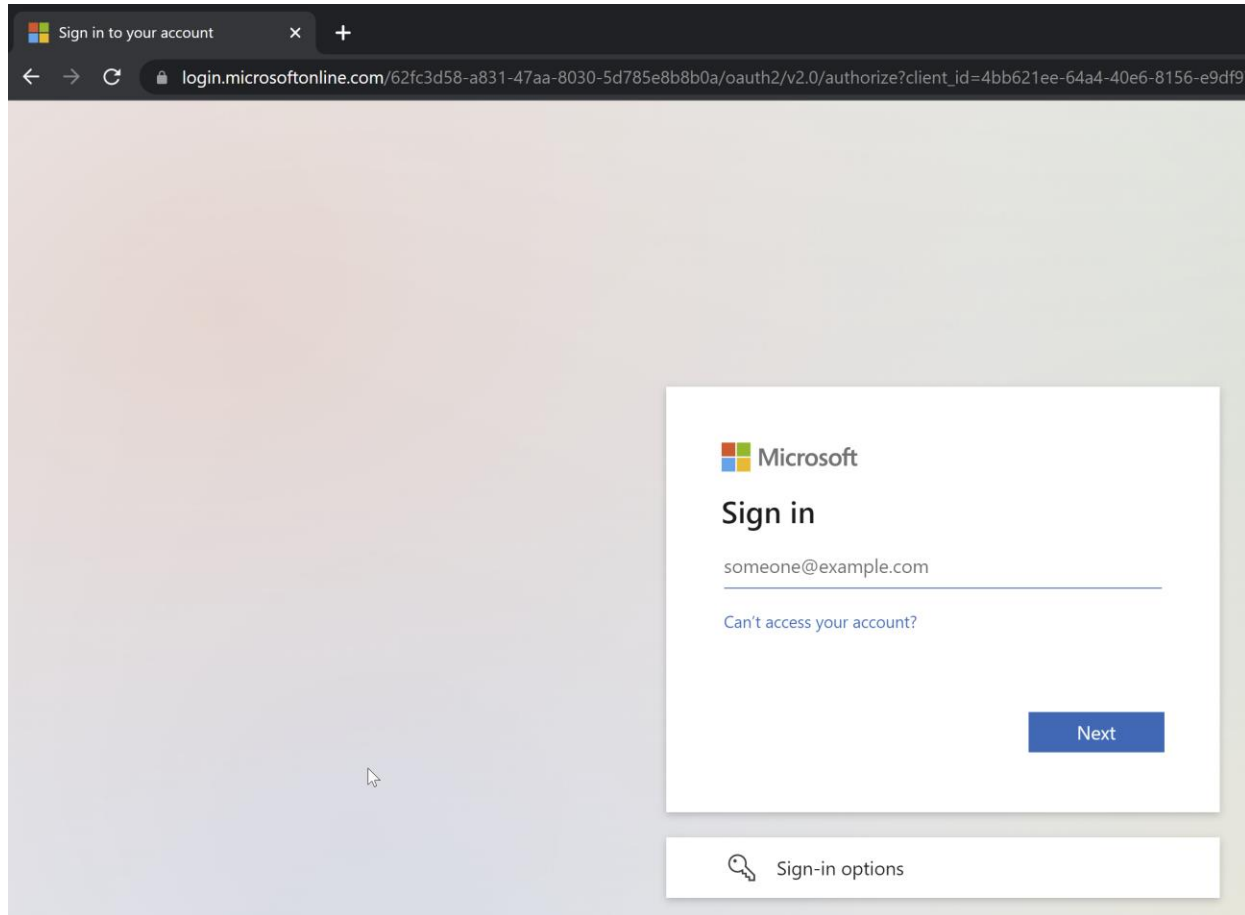
USER DIRECTORY: Azure AD

In an incognito browser, test the new Service Endpoint

Type in the URL https://your_server_name:your_port/Management/azuread in your browser



Sign in



A screenshot of a web browser showing the Microsoft sign-in page. The browser's address bar displays the URL: `login.microsoftonline.com/62fc3d58-a831-47aa-8030-5d785e8b8b0a/oauth2/v2.0/authorize?client_id=4bb621ee-64a4-40e6-8156-e9df97`. The page features the Microsoft logo at the top left of the sign-in card, followed by the text "Sign in". Below this, there is a text input field containing the email address "someone@example.com". Underneath the input field is a link that reads "Can't access your account?". A blue "Next" button is positioned at the bottom right of the sign-in card. At the very bottom of the page, there is a section titled "Sign-in options" with a key icon.

Sign in to your account

login.microsoftonline.com/62fc3d58-a831-47aa-8030-5d785e8b8b0a/oauth2/v2.0/authorize?client_id=4bb621ee-64a4-40e6-8156-e9df97

Microsoft

Sign in

someone@example.com

Can't access your account?


Next

Sign-in options

You are logged in!


Mail & Deploy: Management


← → ↺ 🔒 14998/Management/azuread





Emma Camacho


GENERAL CONTENT

 Users


 User Groups


 Variables

 Modules


 Workspaces


TOOLS

 Execution Status


 Execution Calendar


CONFIGURATION

 Settings

 Preferences


HELP

 Documentation

 Users

LIST

Name ^	User Directory / Identity Provider	Type	E-Mail Address	Language
Amelia Craig	Workshop	Administrator	email@company.com	German
Amanda Honda	Workshop	Standard User	email@company.com	English
Amelia Fields	Workshop	Standard User	email@company.com	English
Angelen Carter	Workshop	Standard User	email@company.com	English
API User	-	API User		English
Bernd Podhradsky	Azure AD	Administrator	bernd.podhradsky@mail-and-d...	English
Bima Malek	Workshop	Standard User	email@company.com	English
Brad Taylor	Workshop	Standard User	email@company.com	English
Brenda Gibson	Workshop	Standard User	email@company.com	English
Brenda Kegler	Workshop	Standard User	email@company.com	English
Carolyn Halmon	Workshop	Standard User	email@company.com	English
Cert Lynch	Workshop	Standard User	email@company.com	English
Emma Camacho	-	Standard User	emma.camacho@mail-and-de...	English
Emma Camacho	Azure AD	Administrator	emma.camacho@mail-and-de...	English
ExtensionAPI	-	API User		English
Root Admin	-	Administrator	emma.camacho@mail-and-de...	English
Service Account	-	Administrator		English
StandardUser	-	Standard User	emma.camacho@hpartner.at	English
TITANDBernd	-	Standard User		English
User	-	Standard User		English

 Mail & Deploy