



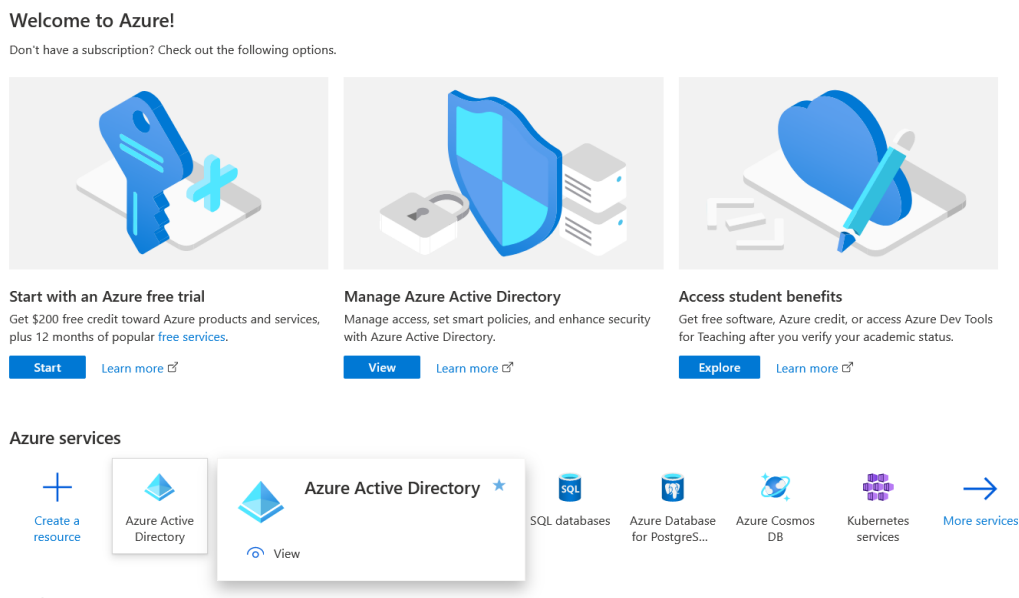
Integration with Azure ActiveDirectory

Date: 25/04/2023



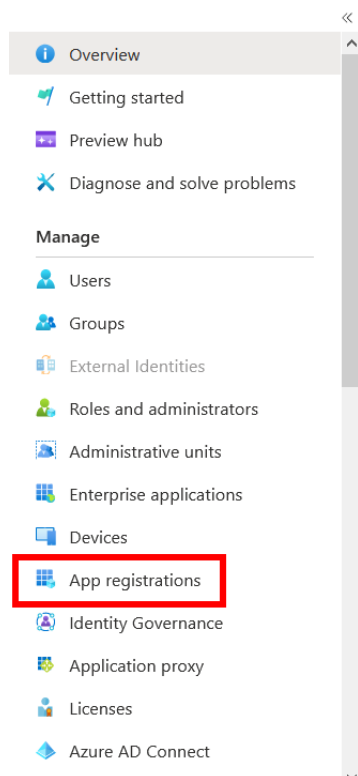
Getting started

The first step to integrate Essentials MDM manage with Azure Active Directory is to register the application in our Azure account. To do this, log in to the portal <https://portal.azure.com/> and then from the Azure services we choose Azure Active Directory.

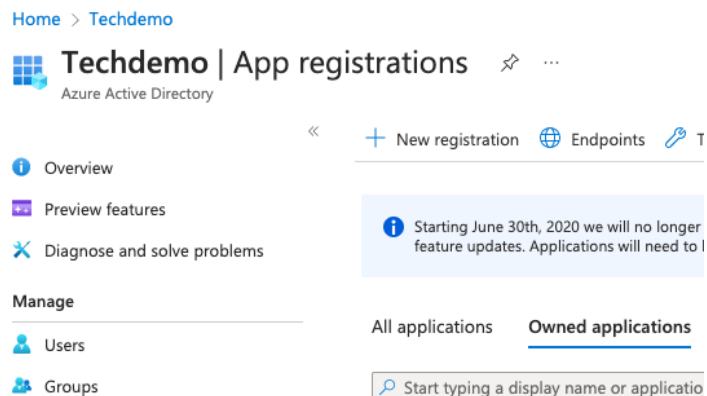


Registering Essentials MDM in Azure

After going to the Azure AD tab, select Application registration from the menu on the left.



Then select the **New registration** option



In the next step, enter the name of the Application and specify whether accounts from one domain or more domains should have access to it – select single- or multi-tenant. We can also provide the URI to which the user is to be redirected after successful authentication (this is optional and can be done later). Press “Register”.

Home >

Register an application

* Name

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

Techstep Essentials ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Techdemo 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

Then configure its permissions. Go to the API permissions tab.

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles | Preview

We can remove the default User delegated permissions by clicking the three dots icon, and then Remove permissions.

API / Permissions name	Type	Description	Admin consent req...	Status	
▼ Microsoft Graph (1)					
User.Read	Delegated	Sign in and read user profile	No		⋮
					Remove permission

Then, we click Add a permission. We select Microsoft Graph and then Application 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 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

◀ 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.

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

In the Directory section, select directory.read.all and confirm by clicking Add permissions.

▼ Directory (1)

<input checked="" type="checkbox"/>	Directory.Read.All ⓘ Read directory data	Yes
<input type="checkbox"/>	Directory.ReadWrite.All ⓘ Read and write directory data	Yes

In the API permissions section it is also required to Grant Admin consent for created app.

+ Add a permission ✓ Grant admin consent for Techdemo

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (1)				...
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Techdemo ...

Then go to the **Certificates & secrets** tab to add a new client secret. Click New client secret, enter its description and specify an expiration time.

Home > Techstep Essentials

Techstep Essentials | Certificates & secrets

Search Got feedback?

Overview
Quickstart
Integration assistant

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners

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

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

Certificates (0) Client secrets (0) 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
No client secrets have been created for this application.			

Add a client secret

Description: Password uploaded 25 April 2023

Expires: 365 days (12 months)

Then you **MUST** copy its value (it will not be displayed again).

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	ID
Password uploaded on Thu Feb 25 2021	2/25/2022	2_Sln83vanF0_hC5gW04wGlae5ee_8d	...

Then log in to the Essentials console. Go to your organization's settings, Users & Authorization section and then find the Azure Active Directory integration section. Click Activate.

TO

Managed devices
2
Device limit
5
Valid to
2021-07-15

Details
Users & authentication
Apple
Android
Notifications
Groups

Two-factor authentication
Two-factor authentication helps keep your user accounts safe by adding an extra security layer to your FAMOC login process.
Activate

Azure Active Directory Integration
Integrate FAMOC with Azure Active Directory and synchronize users and groups.
Activate

SAML integration
Activate

In the next step, enter the following data downloaded from the Azure portal:

- **Display name** (can be any)
- **Application (client) ID**
- **Directory (tenant) ID**
- **Application secret**

The screenshot shows a 'Details' window with a progress bar at the top. The first step, 'Provide credentials', is active. Below the progress bar, there is instructional text: 'In Azure portal go to "Azure Active Directory" > "App registrations" > "New registration". Then go to "API permissions", add permission and in "Directory" section select "directory.read.all". Go to "Certificates & secrets" tab to add a new client secret.' Below this text are four input fields: 'Display name *', 'Application (client) ID *', 'Directory (tenant) ID *', and 'Application secret *'. A 'Next' button is located at the bottom right of the window.

Once you click next your integration will be verified.

The screenshot shows the 'Details' window at the 'Verify integration' step. The progress bar indicates that the first step is complete. The main content area displays the following information: 'Users created by Azure: 15', 'Groups created by Azure: 6', and 'Users:'. Below the 'Users:' label is a scrollable list of user email addresses, including 'dimitris.dimitris@company.com.gr', 'haris@company.com.gr', and 'jane.doe@company.com.gr'. At the bottom right, there are 'Back' and 'Next' buttons.

In the last step you can define the integration settings. First, you can assign attributes from Azure AD to automatically match them with the corresponding values in Essentials MDM (e.g. e-mail address, first name, last name, phone number or job title).

The screenshot shows the 'Details' configuration page for 'User fields mapping'. At the top, a progress bar indicates the steps: 'Provide credentials' (completed), 'Verify integration' (completed), 'User fields mapping' (active), 'Group fields mapping', and 'Settings'. Below the progress bar, there is a table for mapping MDM Essentials attributes to Azure attributes. The table has four columns: 'MDM Essentials attribute', 'Azure attribute', 'Transform RegEx', and 'Transform value'. The first row is pre-filled with 'MDM Essentials login *' mapped to 'userPrincipalName'. The subsequent three rows are empty, with 'Name' mapped to 'givenName', 'Surname' mapped to 'surname', and 'Job title' mapped to 'jobTitle'. Each row has a 'Transform RegEx' input field and a 'Transform value' input field. There are 'X' buttons to delete each row. An 'Add new field' button is at the bottom of the table.

MDM Essentials attribute	Azure attribute	Transform RegEx	Transform value
MDM Essentials login *	userPrincipalName	Transform RegEx	Transform value
Name	givenName	Transform RegEx	Transform value
Surname	surname	Transform RegEx	Transform value
Job title	jobTitle	Transform RegEx	Transform value

In the next step you can do the same with group attributes.

The screenshot shows the 'Details' configuration page for 'Group fields mapping'. The progress bar at the top shows 'Provide credentials' (completed), 'Verify integration' (completed), 'User fields mapping' (completed), 'Group fields mapping' (active), and 'Settings'. Below the progress bar, there is a table for mapping MDM Essentials attributes to Azure attributes. The table has four columns: 'MDM Essentials attribute', 'Azure attribute', 'Transform RegEx', and 'Transform value'. The first row is pre-filled with 'Group name *' mapped to 'displayName'. The second row is empty, with 'Group description' mapped to 'description'. Each row has a 'Transform RegEx' input field and a 'Transform value' input field. There are 'X' buttons to delete each row. An 'Add new field' button is at the bottom of the table. At the bottom right of the page, there are 'Back' and 'Next' buttons.

MDM Essentials attribute	Azure attribute	Transform RegEx	Transform value
Group name *	displayName	Transform RegEx	Transform value
Group description	description	Transform RegEx	Transform value

In the last step, you can also define filters to limit the imported data according to specific parameters for Users and/or Groups. You can also define the synchronization interval (by default 60 minutes, the maximum is 24 hours) and the desired "Alert on synchronization failure".

The screenshot shows the 'Details' configuration page for 'Settings'. The progress bar at the top shows 'Provide credentials' (completed), 'Verify integration' (completed), 'User fields mapping' (completed), 'Group fields mapping' (completed), and 'Settings' (active). Below the progress bar, there are three main configuration sections: 1. A text input field for 'Import users only from filtered groups (leave empty to import all users)'. 2. A 'Synchronization interval' section with a dropdown menu currently set to '60 minutes'. 3. An 'Alert on synchronization failure' section with a dropdown menu currently set to 'On every synchronization error'. At the bottom right of the page, there are 'Back' and 'Save and run synchronization' buttons.

A detailed description of the filter syntax can be found in the Microsoft documentation:

<https://docs.microsoft.com/en-us/graph/query-parameters#filter-parameter>

Additionally, it is also possible to use advanced queries:

<https://docs.microsoft.com/en-us/graph/aad-advanced-queries>

Microsoft provides a tool to validate the entered filters:

<https://developer.microsoft.com/en-us/graph/graph-explorer>

To finish the process, click Save and run synchronization.

If everything went ok you will see a short summary of imported users as shown in the image below. You can make changes to the integration by clicking "Edit".

The screenshot displays the Techstep MDM Essentials web interface. At the top left is the 'TE' logo and 'Techstep' brand name. A sidebar on the left contains navigation links: 'Details', 'Users & authentication' (highlighted), 'Apple', 'Android', 'Notifications', and 'Groups'. The main content area is titled 'Two-factor authentication' with an 'Activate' button. Below this, a section for 'Azure Active Directory Integration' shows a green checkmark and three buttons: 'Synchronize now', 'Remove integration', and 'Edit'. The integration details include: 'Integrate MDM Essentials with Azure Active Directory and synchronize users and groups.', 'Name: Tehcstep Essentials', 'Synchronization status: successful', 'Last synchronization: 3 minutes ago', 'Next synchronization: in an hour', 'Users created by Azure: 0', and 'Groups created by Azure: 1'. A top-right panel shows 'Managed devices: 17', 'Device limit: No limit', and 'Valid to: No limit'.