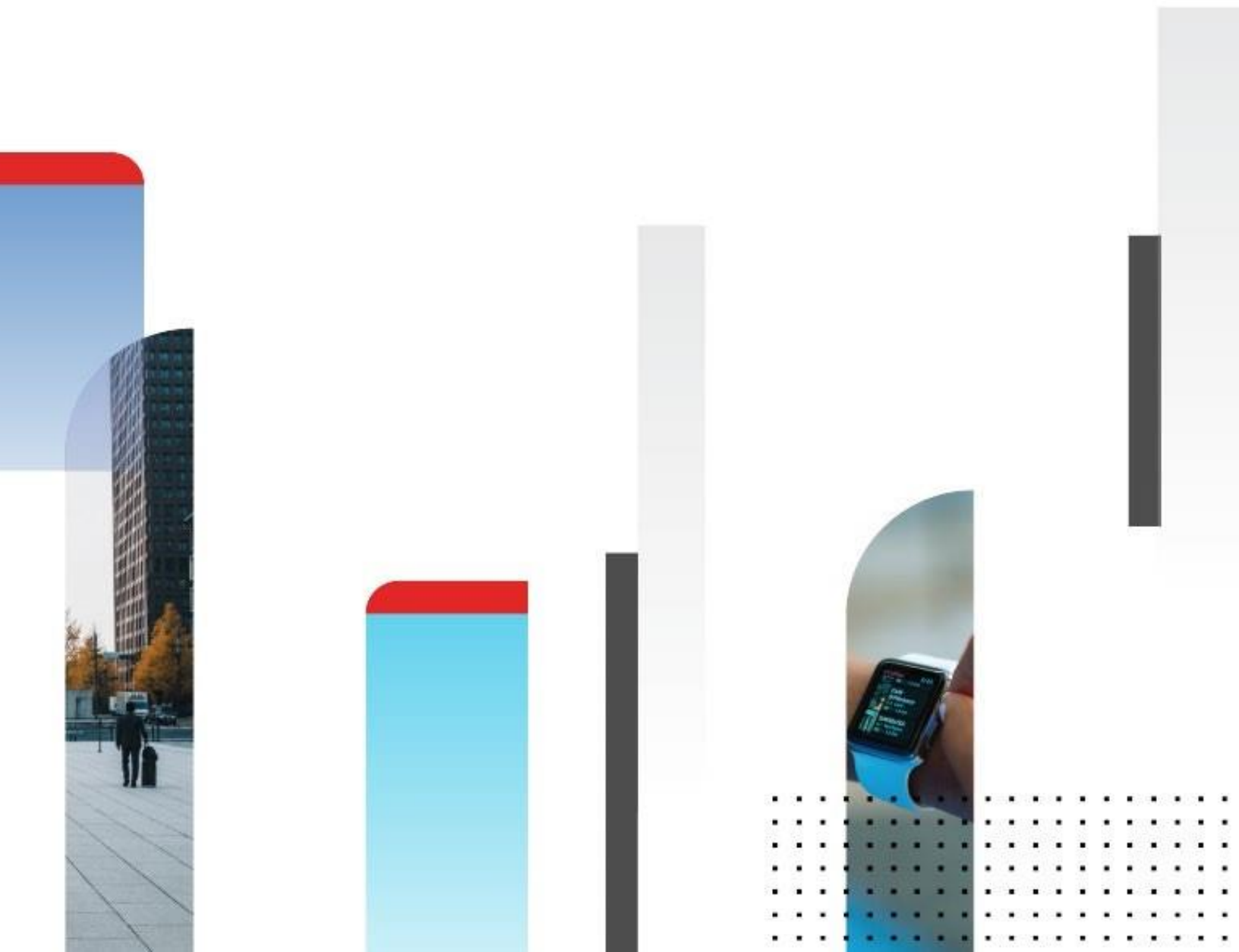


FortiMail Cloud: User Import from Microsoft 365 Deployment Guide

Version 7.4



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<https://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<https://www.fortinet.com/training>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



March 01, 2024

TABLE OF CONTENTS

Change Log..... 4

Introduction 5

Configuring MS365 accounts 5

Configuring FortiMail Cloud with Tenant ID, Application ID, and Application Secret11

Change Log

Date	Change Description
2024-03-01	Initial release

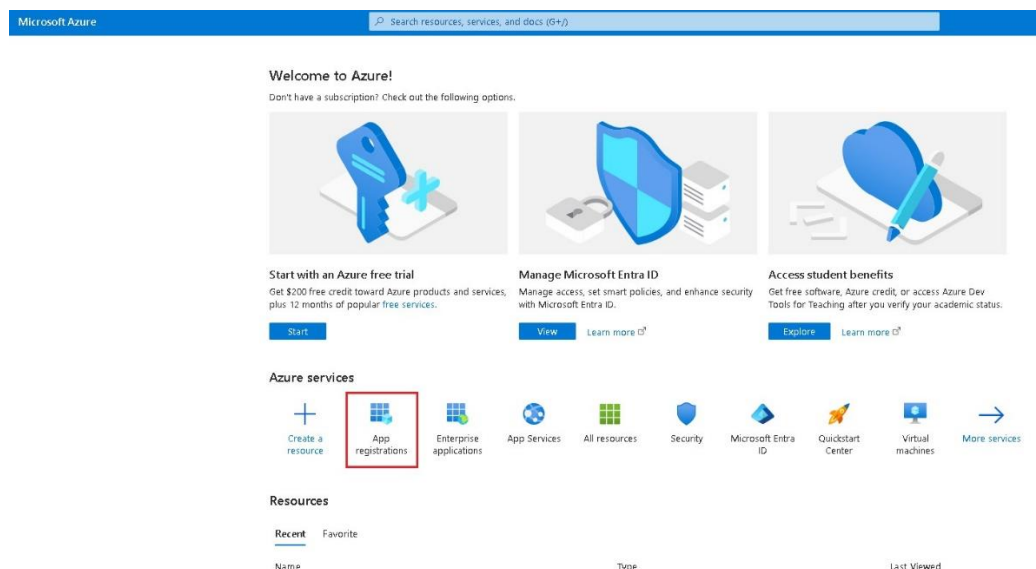
Introduction

This document describes how to import users from Microsoft 365 to FortiMail.

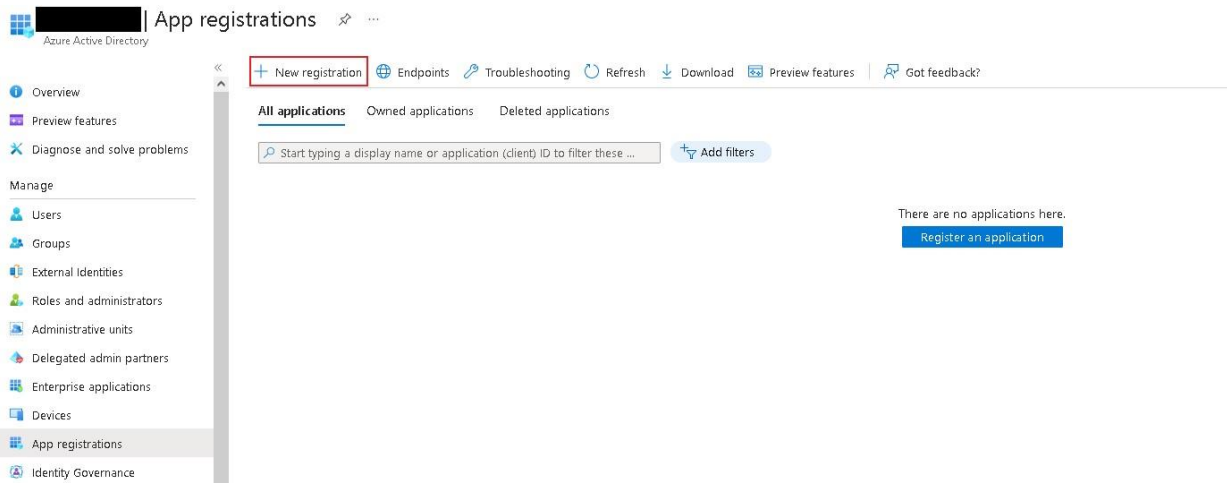
Configuring MS365 Accounts

To register the application in Azure admin center

1. Log in to <https://portal.azure.com> and Select *App registrations*. (You may also search it in the search bar).



2. Select *New registration*.



3. Register an application, you may select the supported account type based on your requirements.

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 (██████████ - 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

Once completed, you will find your *Application ID* and *Tenant ID* here.

The screenshot shows the 'Overview' page for a newly registered application in the Microsoft Entra ID portal. The left sidebar contains navigation links: Overview, Quickstart, Integration assistant, Manage, Branding & properties, Authentication, Certificates & secrets, and Token configuration. The main content area is titled 'Essentials' and displays the following information:

- Display name: ██████████
- Application (client) ID: ██████████ (highlighted with a red box)
- Object ID: ██████████
- Directory (tenant) ID: ██████████ (highlighted with a red box)
- Supported account types: [My organization only](#)

On the right side, there are links for client credentials and other settings:

- Client credentials: [Add a certificate or secret](#)
- Redirect URIs: [Add a Redirect URI](#)
- Application ID URI: [Add an Application ID URI](#)
- Managed application in I...: [fml-test](#)

At the bottom, there are links for 'Get Started' and 'Documentation'.

4. Go to *Certificates & secrets* > *New client secret* to create a secret for your application.

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

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.			

Warning: Once the secret has been created, you must copy and save your secret value. It will not be shown again after you close the page.

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
		[Redacted Value]	

5. Go to *API permissions* > *Add a permission* to set up API permissions for the application.

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

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 FMLddqa

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

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

Add the following permissions for the admin in MS365:

- User.Read
- User.Read.All


Note that *User.Read* is added by default. You may find the other three permissions under *Microsoft Graph* > *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 Communication Services

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




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




Intune

Programmatic access to Intune data




Office 365 Management APIs

Retrieve information about user, admin, system, and policy actions and events



Power BI Service

Programmatic access to Dashboard resources such



SharePoint

Interact remotely with SharePoint data

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.

Search for *User.Read* to find the required 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](#)

Permission

Admin consent required

> IdentityRiskyUser

▼ User (1)

<input checked="" type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes
<input type="checkbox"/>	User.ReadBasic.All ⓘ Read all users' basic profiles	Yes
<input type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

Once you have added all the permissions, click *Grant admin consent for (your application)*. The permission status will change to *Granted for (your application)*.

| API permissions [✎](#) [...](#)

[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

Successfully granted admin consent for the requested permissions.

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

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 \[App\]](#)

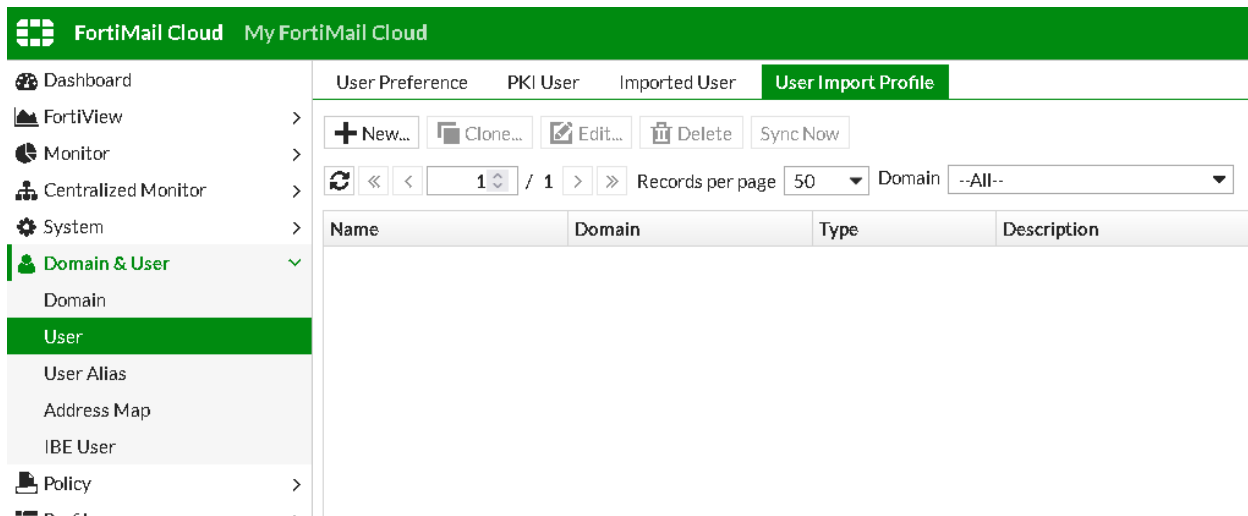
API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (2)				
User.Read	Delegated	Sign in and read user profile	No	✔ Granted for [App] ...
User.Read.All	Application	Read all users' full profiles	Yes	✔ Granted for [App] ...

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

Configuring FortiMail Cloud with Tenant ID, Application ID, and Application Secret

Note: This feature requires MSSP license.

1. Go to your FortiMail Cloud instance, then go to *Domain & Users > User > User Import Profile*.



2. Fill in your Azure AD application info: *Tenant ID*, *Application ID*, and *Application Secret* value.

The screenshot shows the 'User Import Profile' configuration form. It contains the following fields and options: 'Profile name' (text input), 'Domain' (dropdown menu), 'Search timeout' (60 seconds, with a spinner and '(Seconds)' label), 'Type' (radio buttons for 'LDAP' and 'Microsoft 365', with 'Microsoft 365' selected), 'Tenant ID' (text input), 'Application ID' (text input), 'Application secret' (password input), 'Service endpoint' (dropdown menu set to 'Global'), 'Custom attributes' (text input with '+' and '-' icons), and 'Comment' (text area). At the bottom left is a 'Schedule' button with a calendar icon. At the bottom right are 'Create' and 'Cancel' buttons.

Once created, you can either configure the schedule to synchronize or manually synchronize the user list by clicking on *Sync Now*. It will take some time to synchronize and the status will change to *syncing*.

User Preference	PKI User	Imported User	User Import Profile
-----------------	----------	---------------	---------------------

+ New...	Clone...	Edit...	Delete	Sync Now	
----------	----------	---------	--------	----------	--

Records per page	50	Domain	--All--	Selected: 1 / 1
------------------	----	--------	---------	-----------------

Name	Domain	Type	Description	Schedule	Sync Status	Last Sync
test		Microsoft 365		Not Scheduled		

After synchronized, the status will change to succeeded. And you will be able to check and manage the user list from *Domain & Users > User > Imported User* under corresponding domain.

FortiMail Cloud	MyFortiMail Cloud
-----------------	-------------------

Dashboard	User Preference	PKI User	Imported User	User Import Profile
-----------	-----------------	----------	---------------	---------------------

+ New...	Edit...	Delete	Import	Export	Type	--All--	Search
----------	---------	--------	--------	--------	------	---------	--------

Records per page	50	Domain		Profile	--All--
------------------	----	--------	--	---------	---------

Stat...	Display Name	Email	Type	Profile
On				test
On				test
On				test
On				test
On				test
On				test
On				test

