



Integration with Microsoft Office 365 mail server protocols



pm:
<https://pandorafms.com/manual/!779/>
Permanent link:
https://pandorafms.com/manual/!779/en/documentation/10_pandora_itsm/24_pandora_itsm_email_mso365
25/01/22 19:13





Integration with Microsoft Office 365 mail server protocols

Creating application and obtaining identifiers

First, log into the <https://portal.azure.com/> portal and search for Azure Active Directory®. It is recommended to implement **double authentication** in Azure® to increase access security.

Click Application Record → New Record.

The screenshot shows the Azure Active Directory portal interface. The breadcrumb navigation is 'Inicio > MSFT'. The main heading is 'MSFT | Registros de aplicaciones' with 'Azure Active Directory' below it. On the left, a navigation pane lists various administrative tasks, with 'Registros de aplicaciones' highlighted and circled in red. At the top of the main content area, there is a '+ Nuevo registro' button, also circled in red, with a red arrow pointing to it. To the right of this button are links for 'Puntos de conexión', 'Solución de problemas', and 'Actua...'. Below these is a blue information banner with a warning icon and text: 'A partir del 30 de junio de 2020 ya no se agregarán nuevas características a la Biblioteca de características. Las aplicaciones deberán actualizarse a la Biblioteca de autenticación...'. Underneath, there are tabs for 'Todas las aplicaciones', 'Aplicaciones propias' (selected), and 'Aplicaciones eliminadas'. A search bar contains the text 'Empiece a escribir un nombre o id. de aplicación para filtrar los resu...'. Below the search bar, it says '2 aplicaciones encontradas' and 'Nombre para mostrar ↑↓'. The list of applications includes 'Integria' (with a green 'IN' icon) and 'Office365' (with a grey 'OF' icon).

The information is filled in as needed. In this example MSFT (single tenant) is used.

[Inicio](#) > [MSFT | Registros de aplicaciones](#) >

Registrar una aplicación ...

* Nombre

Nombre para mostrar accesible por los usuarios de esta aplicación. Se puede cambiar posteriormente.

Tipos de cuenta compatibles

¿Quién puede usar esta aplicación o acceder a esta API?

- Solo cuentas de este directorio organizativo (solo de MSFT: inquilino único)
- Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino)
- Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: multiinquilino) y cuentas de Microsoft personales (como Skype o Xbox)
- Solo cuentas personales de Microsoft

[Ayudarme a elegir...](#)

Once the application is created, both the `tenantId` (client application identifier) and the `clientID` (tenant directory identifier) may be found in the general information of the application.

Administrar

- [Personalización de marca y propiedades](#)
- [Autenticación](#)
- [Certificados y secretos](#)
- [Configuración de token](#)
- [Permisos de API](#)
- [Exponer una API](#)
- [Roles de aplicación](#)

i Los certificados de registro de aplicación, los secretos y las credenciales federadas se encuentran en las siguientes pestañas. ×

Certificados (0)
Secretos de los cliente (0)
Credenciales federadas (0)

Se trata de una cadena de secreto que la aplicación usa para probar su identidad al solicitar un token. También se conoce como contraseña de aplicación.

+ Nuevo secreto de cliente

| Descripción | Expira | Valor ⓘ | Id. de secreto |
|---|--------|--|----------------|
| No se ha creado ningún secreto de cliente para esta aplicación. | | | |

To obtain the value of the secret, go to Certificates and Secrets → New Customer Secret.

Agregar un secreto de cliente ×

Descripción

Expira ▼

Follow the instructions shown and create the secret.

| Descripción | Expira | Valor ⓘ | Id. de secreto |
|-------------|------------|-----------------------------|---------------------------------|
| Example | 30/12/2023 | y-o8Q~KUEP1Fzm2cr8JPWg4Y... | 59c35a3b-d231-4aab-785f16342527 |

For the next step, copy the value of the secret, do so immediately when creating the secret, since the value will be hidden and will not be shown again.

Actualizar | ¿Tiene algún comentario?

+ Agregar un permiso Conceder consentimiento de administrador para MSFT


| Nombre de permisos/API | Tipo | Descripción | Se necesita el conse... | Estado |
|---|------------|--|-------------------------|--|
| ▼ Microsoft Graph (19) ... | | | | |
| Directory.Read.All | Aplicación | Read directory data | Sí | Concedido para MSFT ... |
| Directory.ReadWrite.All | Aplicación | Read and write directory data | Sí | Concedido para MSFT ... |
| email | Delegada | Ver la dirección de correo electrónico de los usuarios | No | Concedido para MSFT ... |
| IMAP.AccessAsUser.All | Delegada | Read and write access to mailboxes via IMAP. | No | Concedido para MSFT ... |
| Mail.Read | Delegada | Leer correo de usuario | No | Concedido para MSFT ... |
| Mail.Read.Shared | Delegada | Leer correo compartido y del usuario | No | Concedido para MSFT ... |
| Mail.ReadWrite.Shared | Delegada | Leer y escribir correo compartido y del usuario | No | Concedido para MSFT ... |
| Mail.Send | Aplicación | Send mail as any user | Sí | Concedido para MSFT ... |
| Mail.Send.Shared | Delegada | Enviar correo en nombre de otros usuarios | No | Concedido para MSFT ... |
| offline_access | Delegada | Mantener el acceso a los datos a los que se le ha concedi... | No | Concedido para MSFT ... |
| openid | Delegada | Iniciar la sesión de usuarios | No | Concedido para MSFT ... |
| POP.AccessAsUser.All | Delegada | Read and write access to mailboxes via POP. | No | Concedido para MSFT ... |
| profile | Delegada | Ver el perfil básico de los usuarios | No | Concedido para MSFT ... |
| SMTP.Send | Delegada | Send emails from mailboxes using SMTP AUTH. | No | Concedido para MSFT ... |
| User.Read | Delegada | Iniciar sesión y leer el perfil del usuario | No | Concedido para MSFT ... |
| User.Read.All | Aplicación | Read all users' full profiles | Sí | Concedido para MSFT ... |
| User.ReadBasic.All | Delegada | Leer los perfiles básicos de todos los usuarios | No | Concedido para MSFT ... |
| User.ReadWrite | Delegada | Acceso de lectura y escritura al perfil de usuario | No | Concedido para MSFT ... |
| User.ReadWrite.All | Aplicación | Read and write all users' full profiles | Sí | Concedido para MSFT ... |

If the page is refreshed, the only ID retained is the one checked in the image and that the 'Value' will only show a part and without being able to display the rest.

API Permissions


Now the necessary permissions must be added to the application. To do this, go to API Permissions → Add Permission → Microsoft Graphy and add the following permissions:

 Guardar  Descartar  Eliminar


Nombre de ámbito * 

Test2

api://29ab931c-e96b-3f3c55cc3603/Test2

¿Quién puede dar el consentimiento? 

Administradores y usuarios Solo administradores

Nombre para mostrar del consentimiento del administrador * 


Ambito

Descripción del consentimiento del administrador * 


aa

Nombre para mostrar del consentimiento del usuario 

Ambito

Descripción del consentimiento del usuario 

aa

Estado 

Habilitado Deshabilitado

Finally, go to Expose an API → Add a scope in order to add the scope to the application just created in the previous section. In case it says that you do not have a URL added, click next and then configure the scope.

Once all the steps have been completed and the information gathered, the application can be registered in Pandora ITSM.

Dual authentication in Azure

Rather than double authentication, Microsoft Azure® uses multi-factor authentication, *Azure AD*

Multi-Factor Authentication® (MFA) which includes SMS with verification code, an application such as Microsoft Authenticator App® or Google Authenticator®, a fingerprint scan, and so on.

The following is a very simplified summary of the process, for full details see “[Tutorial: Secure user sign-in events with Azure AD Multi-Factor Authentication](#)”.

- It is recommended to use a Conditional Access Policy, which can be assigned to users, groups and applications and which will be responsible for responding to login requests.
- It is therefore necessary to have non-administrator users already created and assigned to work groups created for this purpose. Such work is beyond the scope of this tutorial.
- To create a Conditional Access Policy, log in to the Azure portal with the required rights (*global administrator*).
- In the left side menu, go to Azure Active Directory → Security.
- Select Conditional Access → New policy → Create new policy.
- Enter a name, e.g. MFA Pilot.
- At Assignments, select Users or workload identities.
- At What does this policy apply to? verify that users and groups are selected.
- Now at Include choose Select users and groups and check Users and groups.
- Since it will be empty, a dialog box will automatically open. Select your Azure AD group, suppose it was created with the name MFA-Test-Group, select this group.
- Now assign the applications that will use this Conditional Access Policy. The example below assumes that it will be applied only to the Azure portal.
 1. At Cloud apps or actions go to Select what this policy applies to and check Cloud apps is selected.
 2. At Include choose Select apps.
 3. Browse the list and search for Microsoft Azure Management and check yourself as selected.
 4. Now the MFA access controls must be configured, go to Access controls → Grant → Grant access.
 5. Select Require multi-factor authentication, check it as selected and click Select.


Now just activate the policy, go to Enable policy, select the On value and click Create.

From this point on, users and groups created accessing the Azure portal should select the Mobile app method in step one and check Use verification code and click the Setup button to start configuring the personal Microsoft Authenticator app or Google Authenticator.

Pandora ITSM mail configuration

Access, [with the necessary permissions](#), the menu Setup → Setup → Email setup and fill in the fields with the information obtained:

— General

Notification period 

System email from address

— SMTP Parameters - Sending email server configuration

Encryption

User ID

Test connection


Cliente ID

Tenant ID

Secret

SMTP queue retries 

Max. pending emails 

Max. emails sent per execution 

See [“Advanced PITSM configuration”](#) for more details.

Double authentication in Pandora ITSM

It is recommended to implement the second authentication factor in Pandora ITSM to increase application access security. See [“Dual authentication”](#) for more details.

[Back to Pandora ITSM Documentation Index](#)