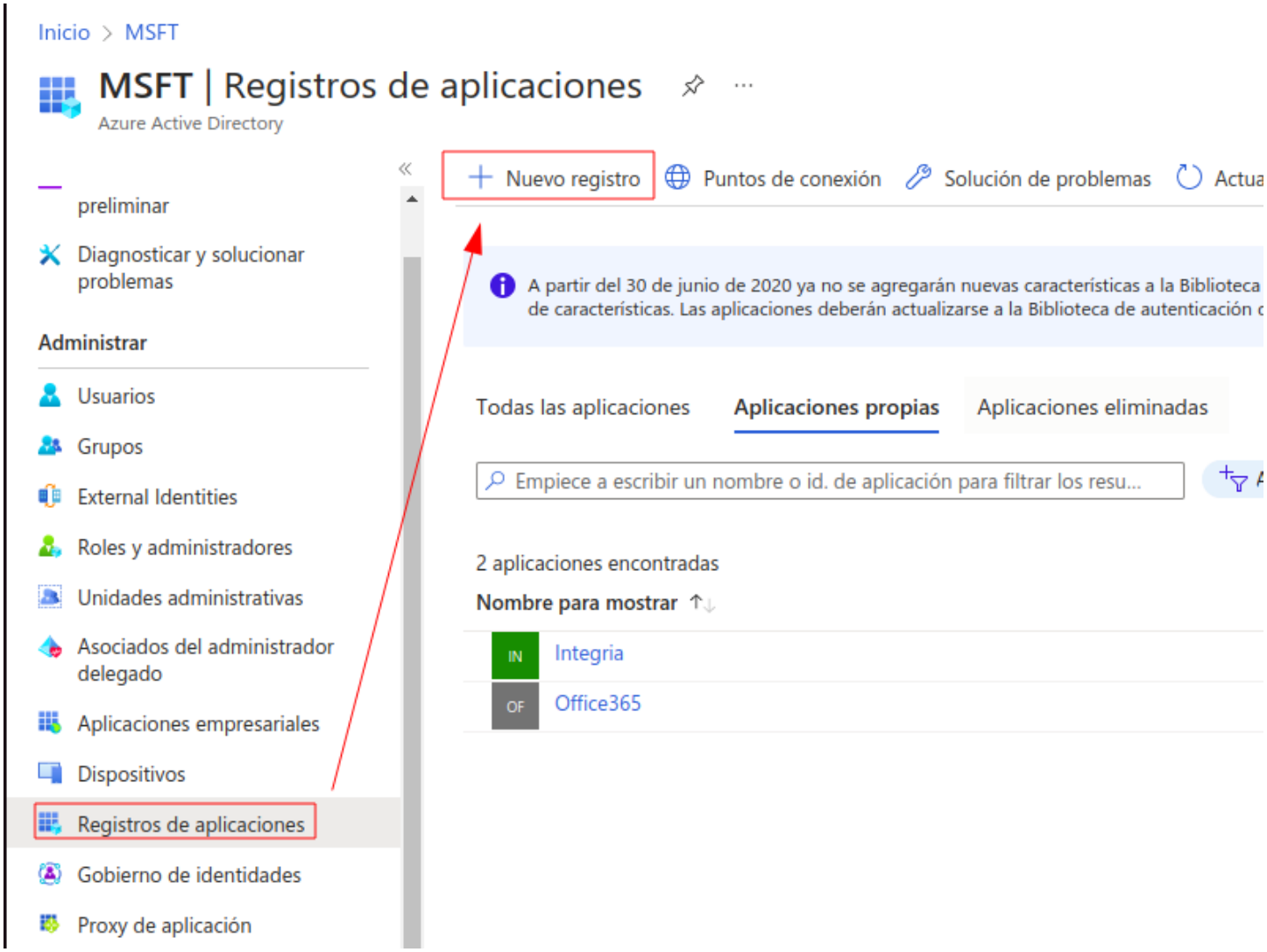
Integration with Microsoft Office 365 mail server protocols

Integration with Microsoft Office 365 mail server protocols

Creating application and obtaining identifiers

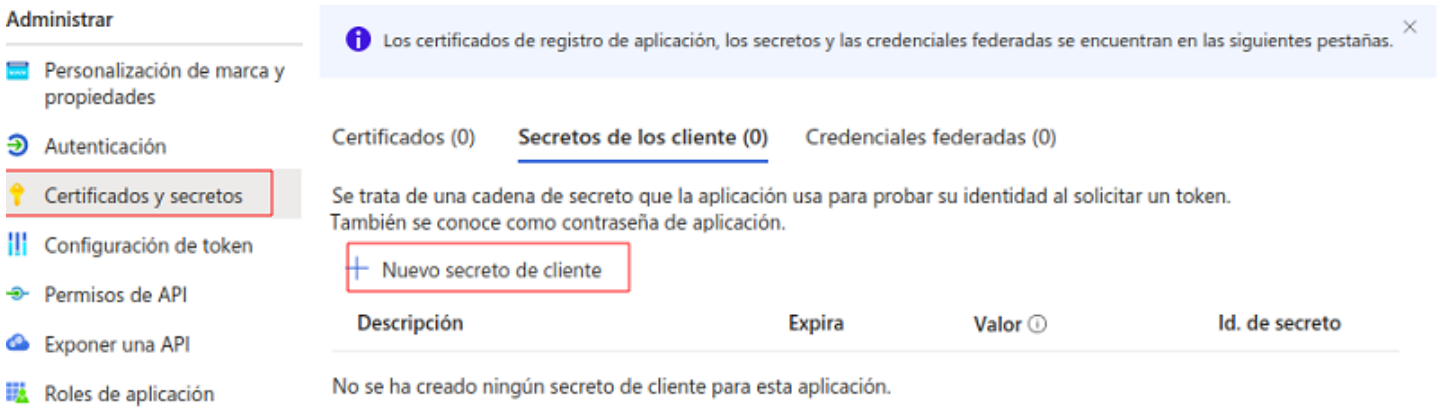
First, log into the https://portal.azure.com/ portal and search for Azure Active Directory®. It is recommended to implement double authentication in Azure® to increase access security.

Click Application Record → New Record.

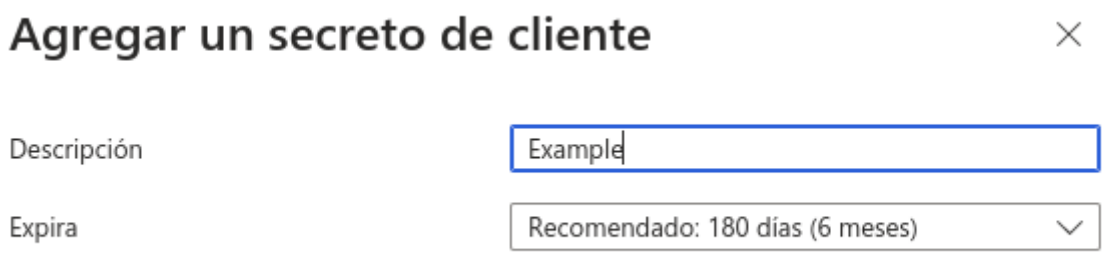


The information is filled in as needed. In this example MSFT (single tenant) is used.

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.



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



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?

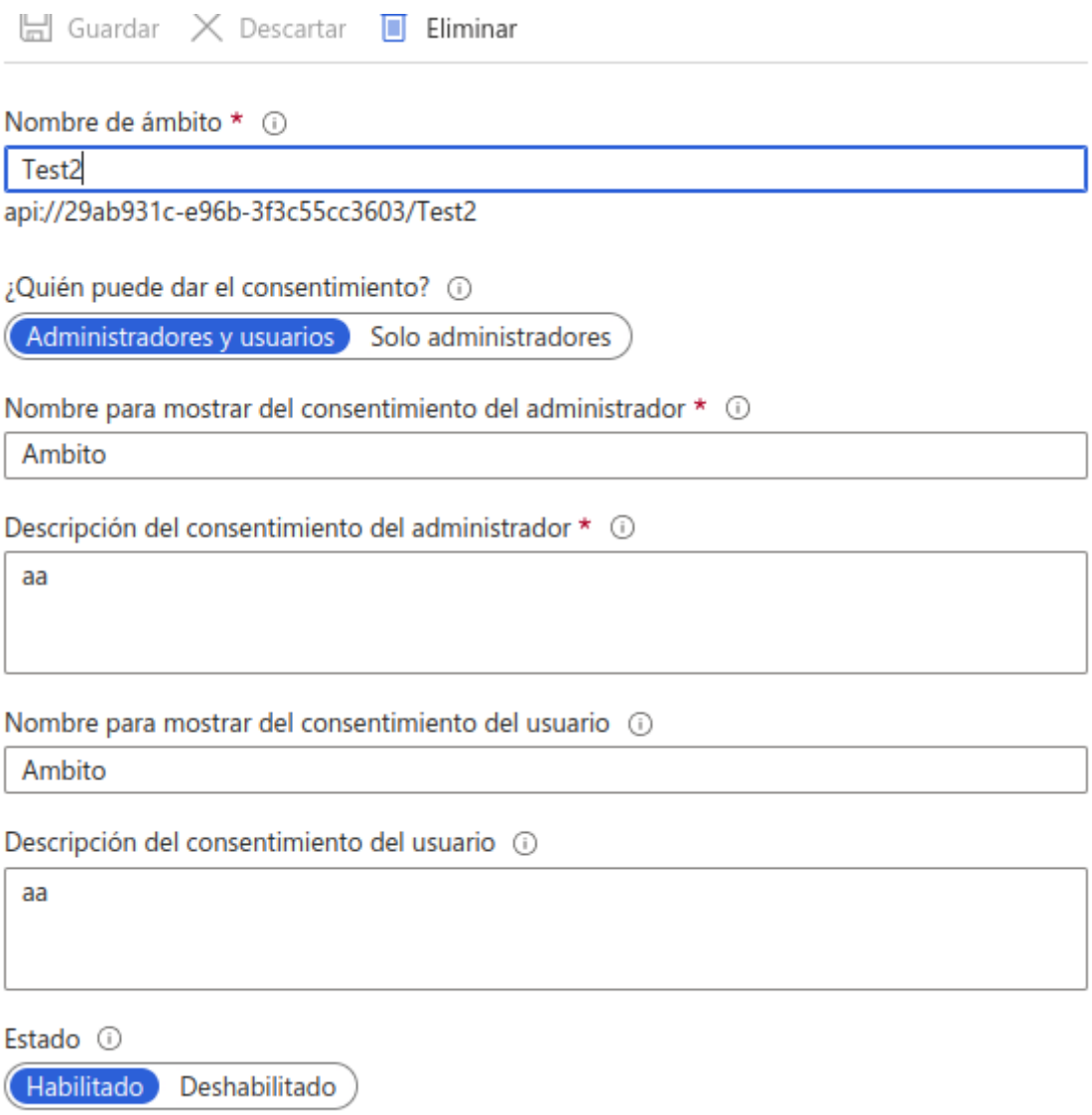
Agregar un permiso | Conceder consentimiento de administrador para MSFT

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:



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.

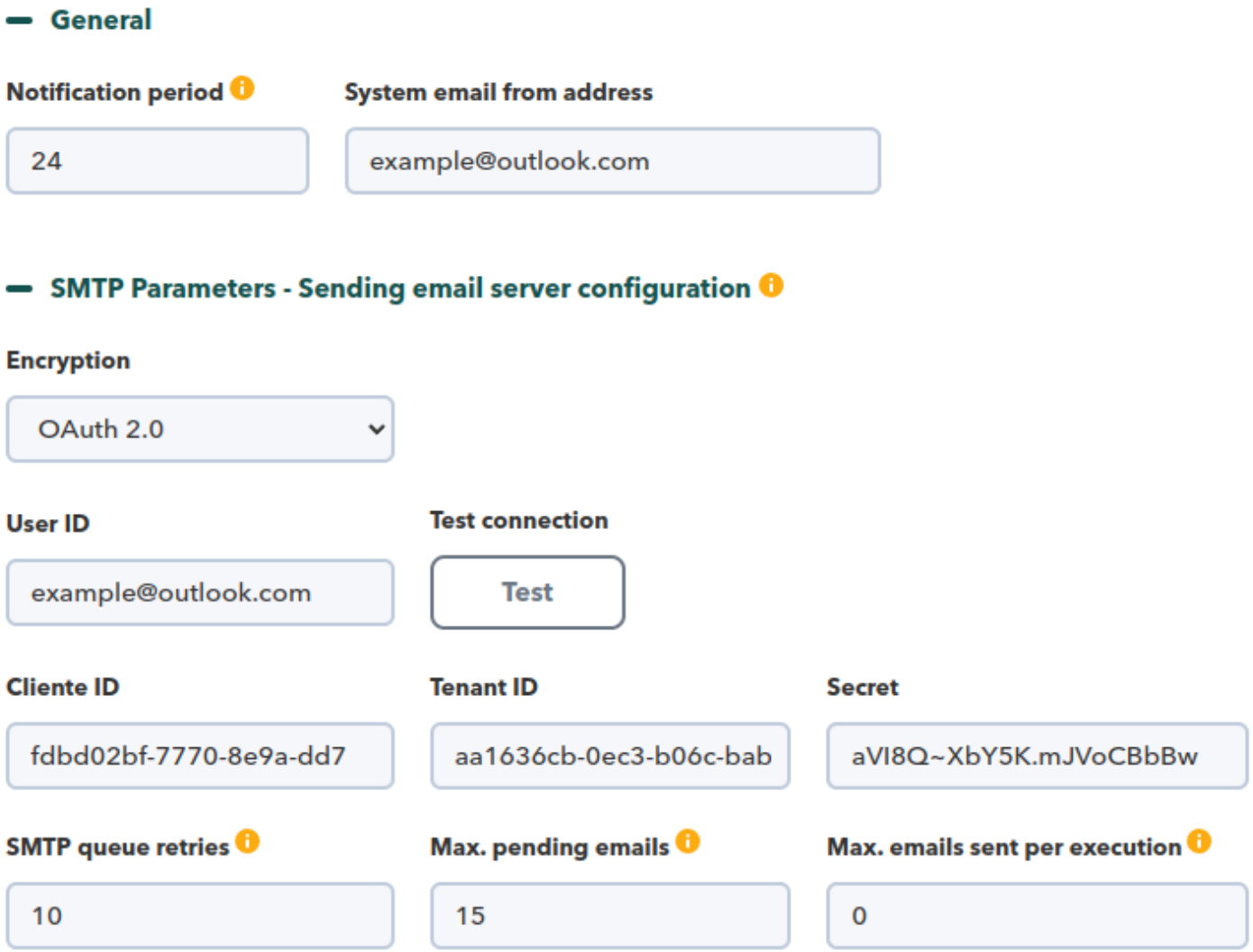
1. At Cloud apps or actions go to Select what this policy applies to and check Cloud apps is selected.
2. At Include choose Select apps.
3. Browse the list and search for Microsoft Azure Management and check yourself as selected.
4. Now the MFA access controls must be configured, go to Access controls → 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:



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