Integration with Microsoft Office 365 mail server protocols

Integration with Microsoft Office 365 mail server protocols

Back to Pandora FMS documentation index

Page under construction, sorry for the inconvenience.

Creation of application and obtaining of identifiers

You must first sign in to the portal at https://portal.azure.com/ and search for Azure Active Directory. It is recommended to implement double authentication in Azure to increase access security.

Click on Application Registration → New Registration.

Information is filled in as needed. This example uses MSFT (Single Tenant).

Once the application is created, it will be possible to locate both the `tenantId` (client application identifier) and the `clientID` (tenant directory identifier) in the general information of the application.

To obtain the value of the secret, go to Certificates and secrets → New client secret.

Follow the instructions shown and create the secret.

In the next step we must copy the value of the secret, this must be done immediately when creating it since the value will be hidden and will not be shown again.

If the page is updated, the only ID that is kept is the one marked in the image and that the 'Value' will only be shown in part and without being able to view 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 to be able to add said scope to the application just created in the previous section. In case it says that you do not have a URI address added, you must click next and then configure the scope in a similar way as indicated below:

Once all the steps have been completed and with the information collected, the application can be registered in Integria IMS.

Double authentication in Azure

More than double authentication, Microsoft Azure® uses multi-factor authentication, Azure AD Multi-Factor Authentication (MFA) that includes SMS with verification code, an application such as Microsoft Authenticator app or Google Authenticator , a fingerprint scan, etc.

Below 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 in charge of 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 necessary 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, for example `MFA Pilot`.
- Under Assignments select Users or workload identities.
- In What does this policy apply to? verify that users and groups is selected.
- Now in 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, let's say it was created with the name `MFA-Test-Group`, select that group.
- Now the applications that will use said Conditional Access Policy must be assigned. The example below assumes that it will be applied to the Azure portal only.

1. Under Cloud apps or actions go to Select what this policy applies to and verify that Cloud apps is selected.
2. In Include choose Select apps.

3. Browse the list and find Microsoft Azure Management and mark it as selected.
4. MFA access controls should now be configured, go to Access controls → Grant → Grant access.
5. Select Require multi-factor authentication mark it as selected and press the Select button.

Now all that remains is to activate the policy, go to Enable policy select the value On and press the Create button.

From now on, users and groups created that access the Azure portal must select the Mobile app method in step number one and check Use verification code and press the Setup button to start to configure the personal application Microsoft Authenticator app or Google Authenticator.

Email configuration in Integria IMS

You must access, with the necessary permissions, to the Setup menu → Setup → Email setup and fill in the fields with the information obtained, for example:

See "IIMS Advanced Configuration" for more details.

Double authentication in IIMS

It is recommended to implement the second authentication factor in Integria IMS to increase security in accessing applications. See "Double authentication" for more details.

Back to Pandora FMS documentation index