



External Credentials

Used to store credentials for integrations with external systems. Different data items will need to be completed depending on the nature of the external system. These credentials are available to be used by built-in commands like <SendEmail> or directly in Jobs.

More sensitive items are stored in the database using AES256 encryption. Once saved, only the last four characters are shown, preceded by ****. The number of asterisks is unrelated to the length of the underlying data.

When you click on New, you will be asked for the Name, the Type and a Description of the credential record you want to create. The type and description can be edited later, but the name cannot be changed subsequently, and will be used to identify these credentials elsewhere in IQX. Once you have supplied these values and clicked OK, a new form will open where the details can be entered.

SMTP

As a minimum, a name, description and a host address are required. If specified, the Email Address will be used as the SMTP Sender email, otherwise it must be specified in the <SendEmail> command. If no port is specified, 25 is assumed. User Name and Password must be specified if authentication is required. TLS can be ticked if required.

If your email provider enforces two-factor authentication, or you find that you have issues with the valid credentials being rejected, you may need to set up and use an “App” password rather than using a standard password. These passwords are created for a single purpose and are used in conjunction with the normal user name. For more information see [GMail](#) or [Microsoft / Exchange / Azure / Outlook 365](#). Be aware that changing the “main” password on the email account can result in any “App” passwords for that account being silently invalidated, and requiring regeneration.

Microsoft Graph API

Registering IQX as an application in Azure

To use the Microsoft Graph API with IQX, you must first set up IQX as an Application in **your** Azure Active Directory using the Create Azure Active Directory application. To do this, log into **your** Microsoft Azure Portal as an **admin** user. Then select [Azure Active Directory](#) followed by [App registrations](#).

Next complete the Name field as, for example, *IQX*, set Supported account types to *Accounts in this organizational directory only* and set Redirect URI to *Web* with <http://localhost> as the URI.



Granting permissions to IQX

Now go back to App registrations and select All apps. Select the App record you have just created and then select API Permissions. Select + Add a permission and in Request API permissions select Microsoft Graph. Then configure Application permissions and grant Mail.Read and Mail.ReadWrite permission to the App. Finally ensure you choose Grant admin consent for <your company name>. Your settings should look something like this:

Microsoft Azure | Search resources, services, and docs (G+/I)

Home > IQX | API permissions

Search (Ctrl+/) | 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

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. [Add MPN ID to verify publisher](#)

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 organization, or in organizations where this app will be used. [Learn more](#)

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 LTD

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				
Mail.Read	Application	Read mail in all mailboxes	Yes	Granted for LTD
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	Granted for LTD

Setting up authentication for IQX

Choose Certificates and secrets from the right hand menu. Choose Add a client secret, give it a description and choose Never under Expires. Select Add and copy the displayed Secret into the **Client Secret** field in IQX and then click on **Save & Refresh**.

Then back in Azure, choose Authentication from the right hand menu. The screen should look something like this:



2024/05/24 07:13

3/3

External Credentials

Microsoft Azure Search resources, services, and docs (G+)

Home >

iqx

Search (Ctrl+/) << Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: iqx	Client credentials	: 0 certificates 1 secret
Application (client) ID	: ac34e4f1-1f22d	Redirect URIs	: Add a Redirect URI
Object ID	: 355238-b54f8e	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: a415e2-1de694	Managed application in l...	: iqx

Supported account types : All Microsoft account users

Now select and copy the Application (client) ID into **Client ID** in IQX, and Directory (tenant) ID into **Tenant ID** in IQX. Then click on **Save & Refresh**

From:

<https://iqxusers.co.uk/iqxhelp/> - iqx

Permanent link:

<https://iqxusers.co.uk/iqxhelp/doku.php?id=externalcredentials>

Last update: **2023/03/04 02:39**

