README.md

Microsoft Exchange Online Functions for IBM Resilient

Release Notes

v1.0.0

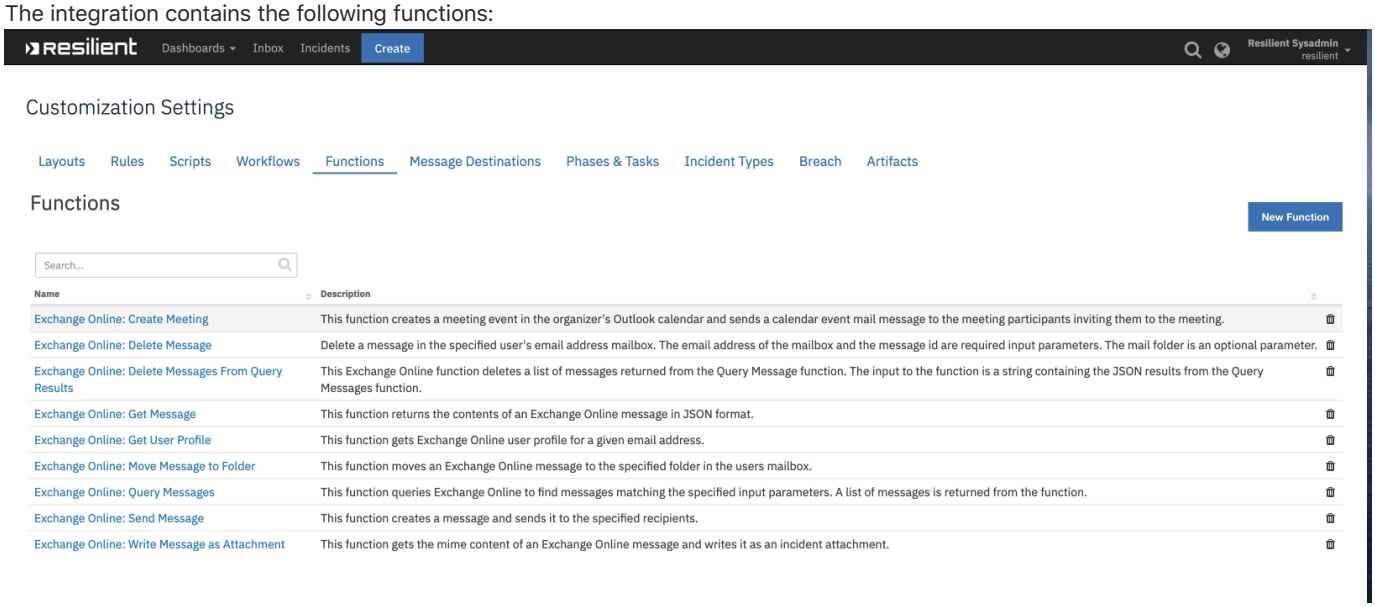
- Initial Release

Overview

Resilient Integration with Exchange Online provides the capability to access and manipulate Microsoft Exchange Online (Office 365 in the cloud) messages from the IBM Resilient Soar Platform. The integration uses Microsoft Graph API to access the data in Office 365. Included in the integrations are the following capabilities:

- Get the user profile of the specified email address in JSON format.
- Get a specified message and and return the results in JSON format.
- Get a specified message in .eml format and write as an incident attachment.
- Move a message to a specified "Well-known" Outlook folder.
- Send an message: from the specified email address to the specified recipients with specified message subject and body text.
- Query messages of a single user, a list of users, or the whole tenant and return a list of messages matching the criteria: message sender, messages from a specific Well-known folder, a time frame for when the message was received, text contained in the message subject or the message body, whether the message has attachments. Results are returned in the Exchange Online Query Message Results data table.
- Delete a single specified message from a specified email address.
- Delete a list of messages that are the results of a message query. The messages deleted are written to the Exchange Online Query Messages data table.
- Create a meeting event in the organizer's Outlook calendar and send a calendar event message to meeting participants inviting them to the meeting.

The integration contains the following functions:



Requirements

- Resilient platform >= `v34.2.47`
- An Integration Server running:
  - `resilient_circuits>=31.0.0`
  - `resilient_lib>=35.0.0`
  - The minimum set of Resilient API permissions for this integration if using an API key account:
    - Edit Org Data
    - Incidents.Edit.Fields
    - Functions.Read
    - Functions.Edit
    - Layouts.Read
    - Other.ReadIncidentsActionInvocations
    - Scripts.Create
    - Scripts.Edit
    - Workflows.Create
    - Workflow.Edit
  - To set up an Integration Server see: ibm.biz/res-int-server-guide
- The following Microsoft Graph API "Application permissions" (See Microsoft Azure App Configuration section below to configure):
  - Calendar.ReadWrite
  - Mail.ReadWrite
  - Mail.Send
  - MailboxSetting.Read
  - User.Read.All

Installation

- Download the `fn_exchange_online.zip` .
- Copy the `.zip` to your Integration Server and SSH into it.
- **Unzip** the package:

```
$ unzip fn_exchange_online-x.x.x.zip
```

- **Change Directory** into the unzipped directory:

```
$ cd fn_exchange_online-x.x.x
```

- **Install** the package:

```
$ pip install fn_exchange_online-x.x.x.tar.gz
```

- Import the **configurations** into your app.config file:

```
$ resilient-circuits config -u
```

- Import the fn_exchange_online **customizations** into the Resilient platform:

```
$ resilient-circuits customize -y -l fn-exchange-online
```

- Open the config file, scroll to the bottom and edit your fn_exchange_online configurations:

```
$ nano ~/.resilient/app.config
```

Config	Required	Example	Description
microsoft_graph_token_url	Yes	`https://login.microsoftonline.com/{tenant}/oauth2/v2.0/token`	*Microsoft Graph URL endpoint for acquring access token*
microsoft_graph_url	Yes	`https://graph.microsoft.com/v1.0`	*Microsoft Graph base URL *
tenant_id	Yes	`xxx`	*Microsoft Azure Tenant ID*
client_id	Yes	`xxx`	*Microsoft Azure Client ID (Application ID)*
client_secret	Yes	`xxx`	*Microsoft Azure Client Secret*
max_messages	Yes	`100`	*Maximum number of messages that a query will return*
max_users	Yes	`2000`	*Maximum number of users searched in a query*

- **Save** and **Close** the app.config file.

- [Optional]: Run selftest to test the Integration you configured:

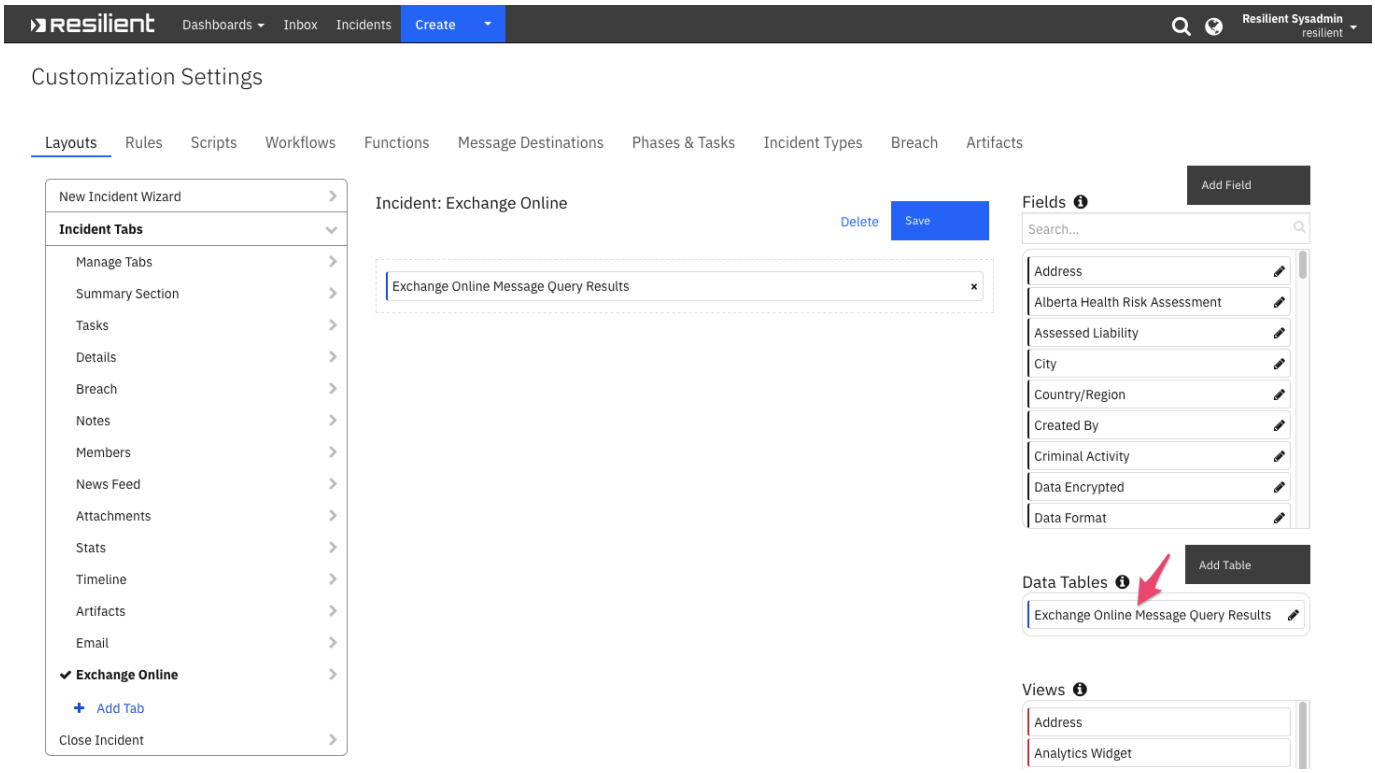
```
$ resilient-circuits selftest -l fn-exchange-online
```

- **Run** resilient-circuits or restart the Service on Windows/Linux:

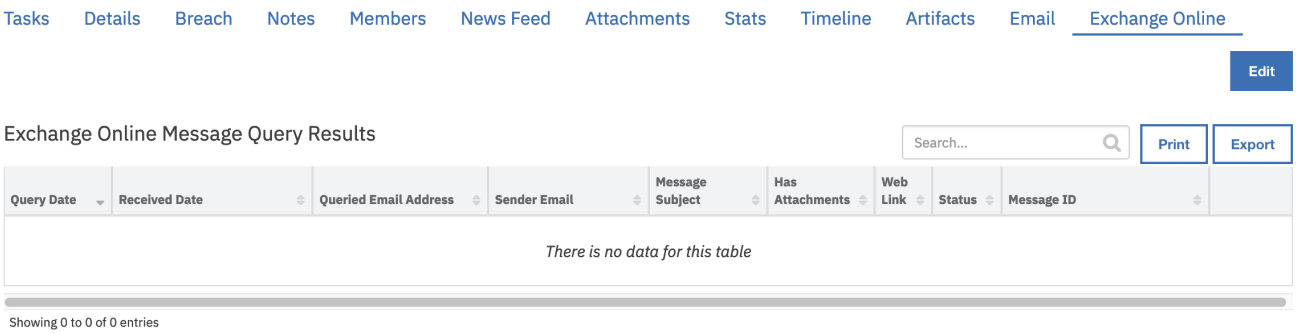
```
$ resilient-circuits run
```

Custom Layouts

Create an Exchange Online custom incident tab and drag the Exchange Online Message Query Results data table on to the layout and click Save as shown in the screenshot below:



The results of any Exchange Online message query are displayed in this data table on the Exchange Online custom incident tab.

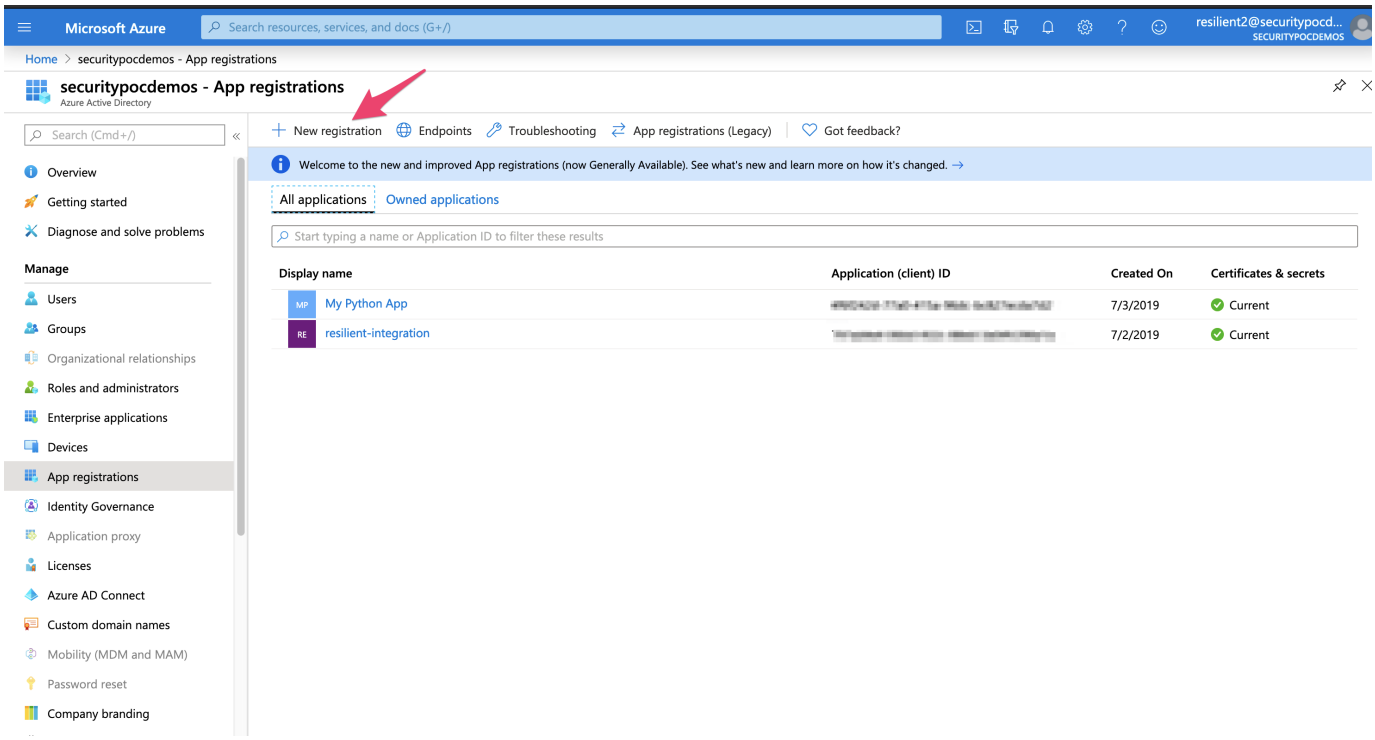


Microsoft Azure App Configuration

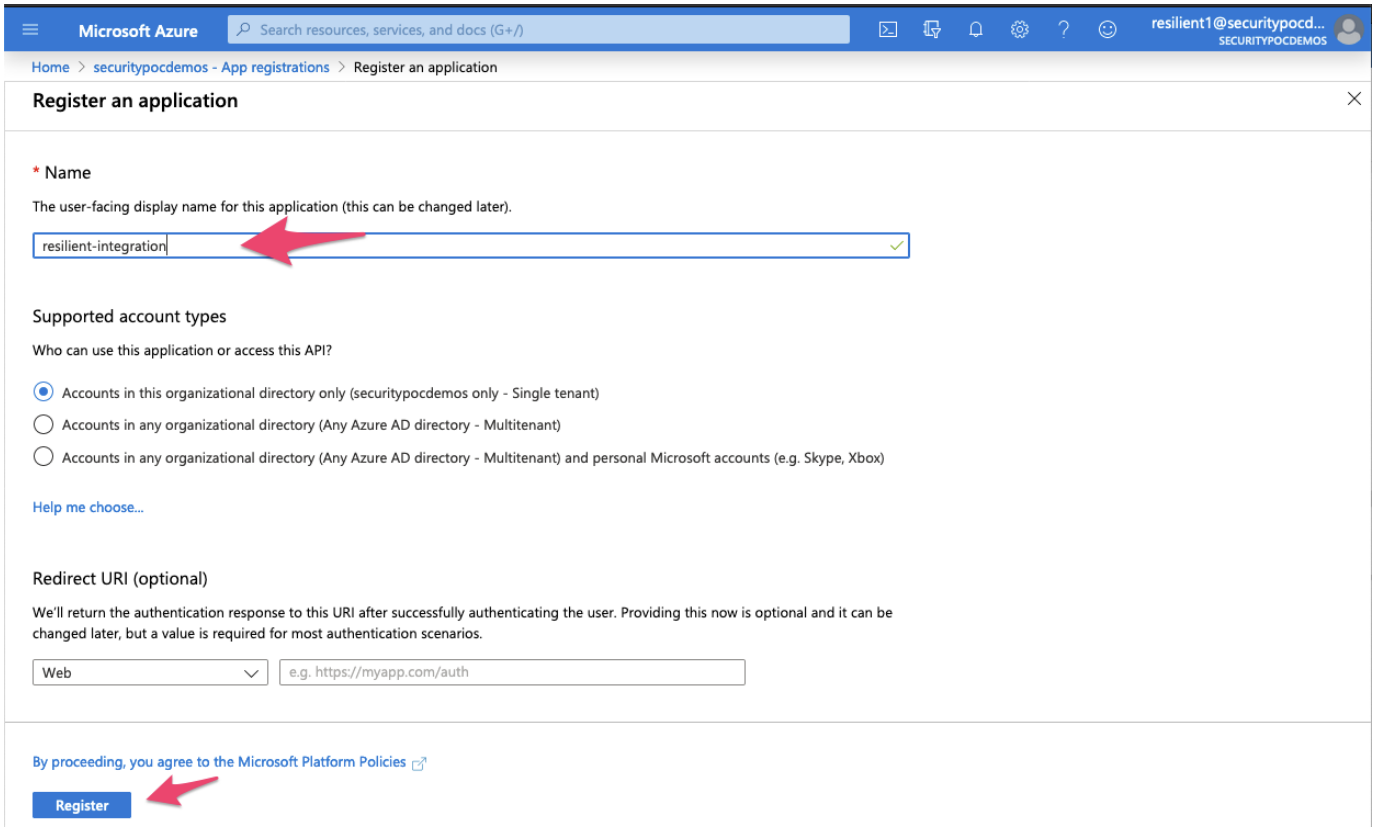
To run the Resilient Exchange Online integration, you must first register the application on Microsoft Azure portal. The tenant ID, client ID and the client secret that are defined in the fn_exchange_online section of the app.config are assigned by Azure when the application is registered.

App Registration

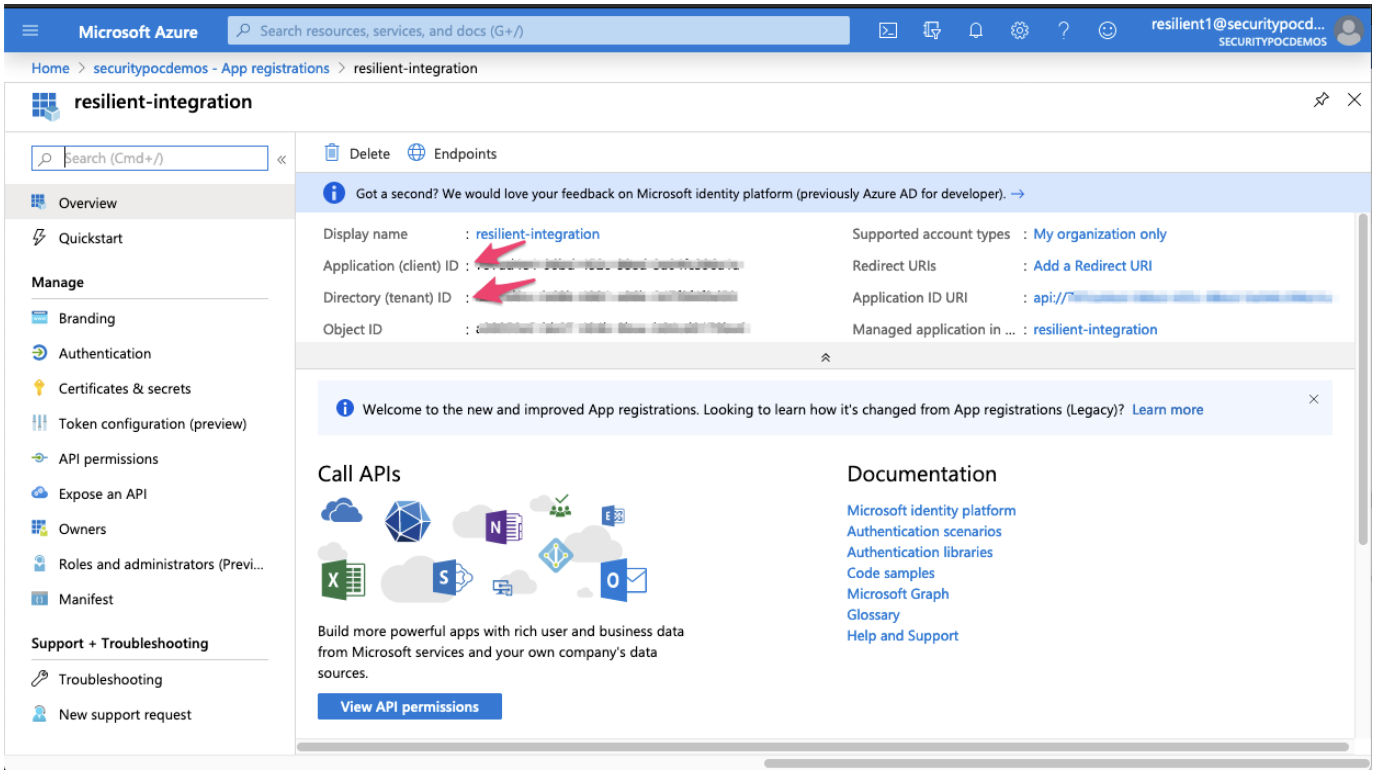
To register the Resilient integration application click "App registrations" in Manage section of your Azure Active Directory domain account. Then click the "New Registration" button as depicted in the image below.



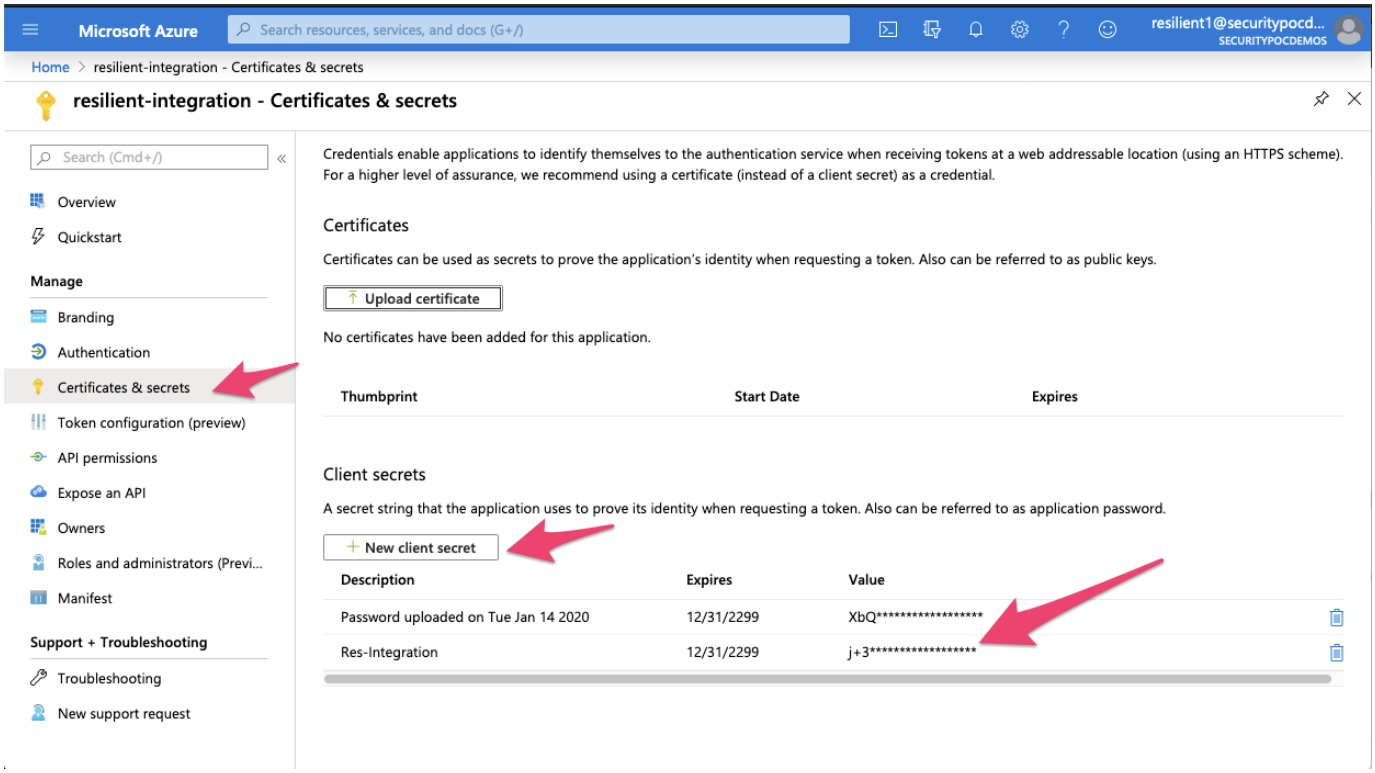
Enter a name for the integration. In this example, the name is "resilient-integration". Then press the "Register" button.



Click on the newly created application. A page appears that is similar to the screenshot below. Get the tenant and client IDs for the application, which are parameters in the app.config file:

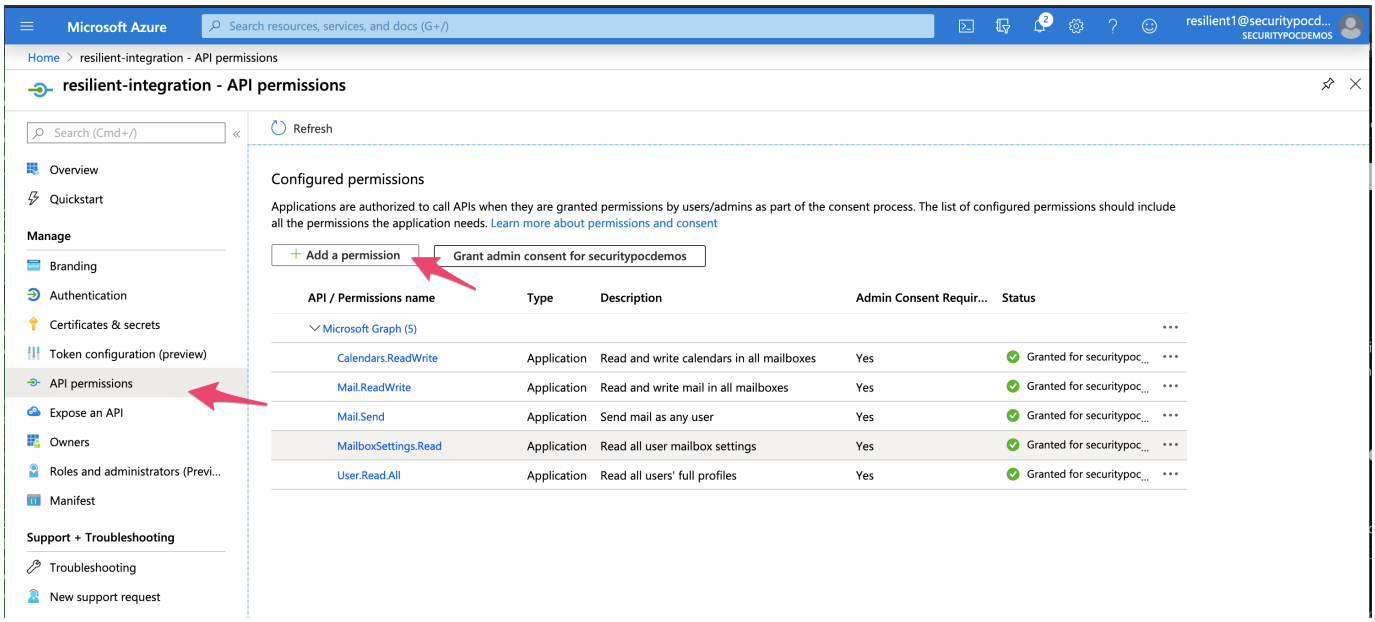


Next, click on the left menu item, "Certificates & secrets" and create a secret, which is another application credential in the app.config.

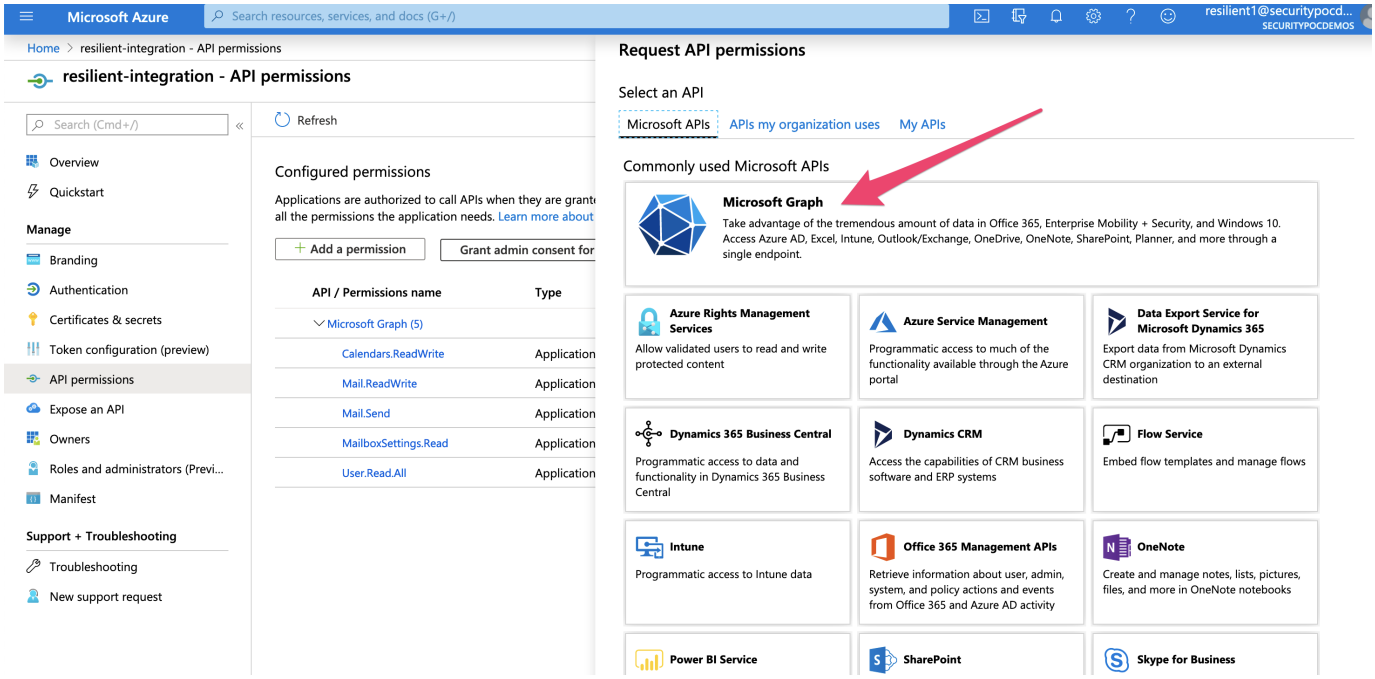


API Permissions

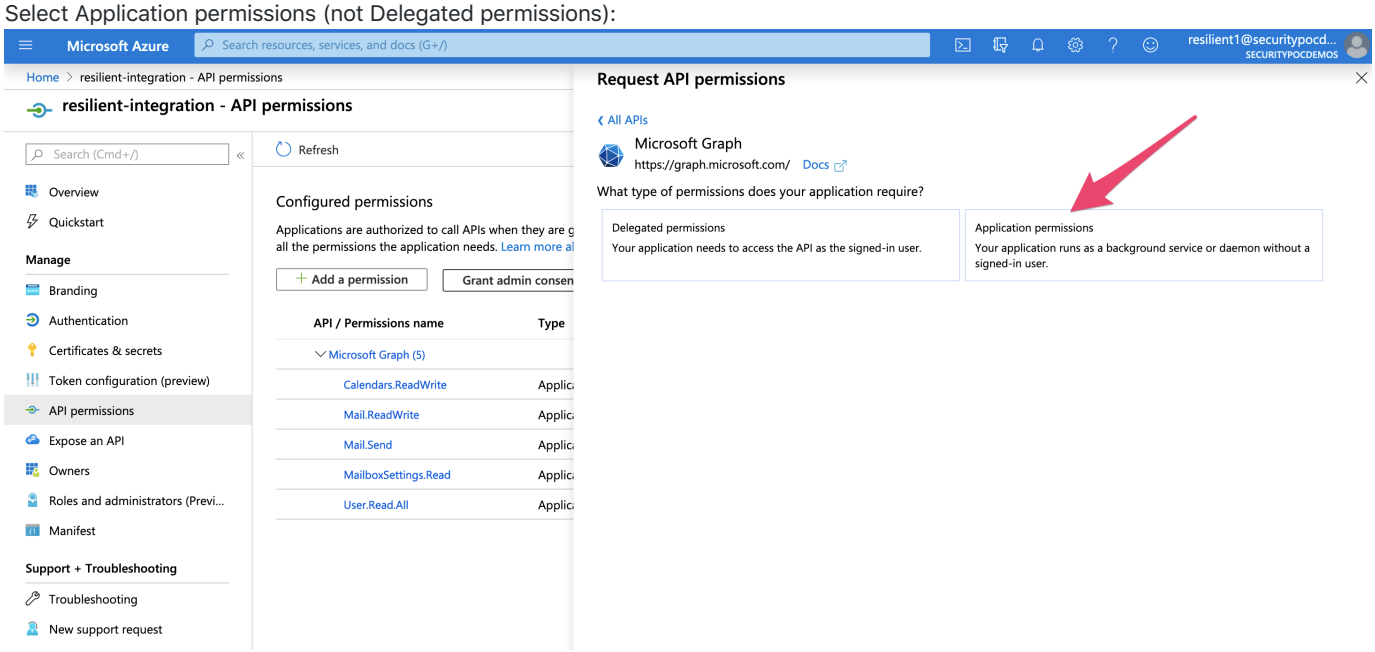
For the Resilient integration app to access data in Microsoft Graph, an administrator must grant it the correct permissions via a consent process. Click on "API permissions" on the left menu and then "+ Add a Permission".



Click on Microsoft Graph:

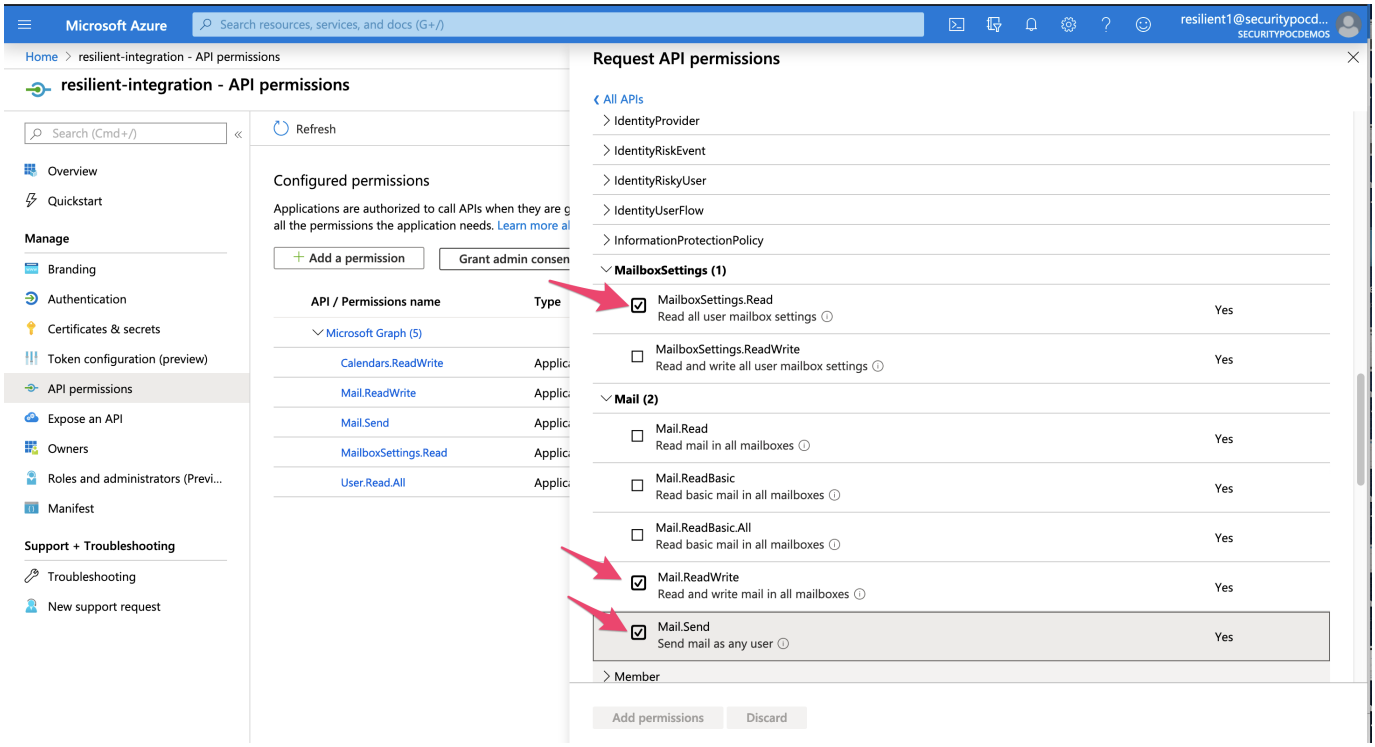


Select Application permissions (not Delegated permissions):

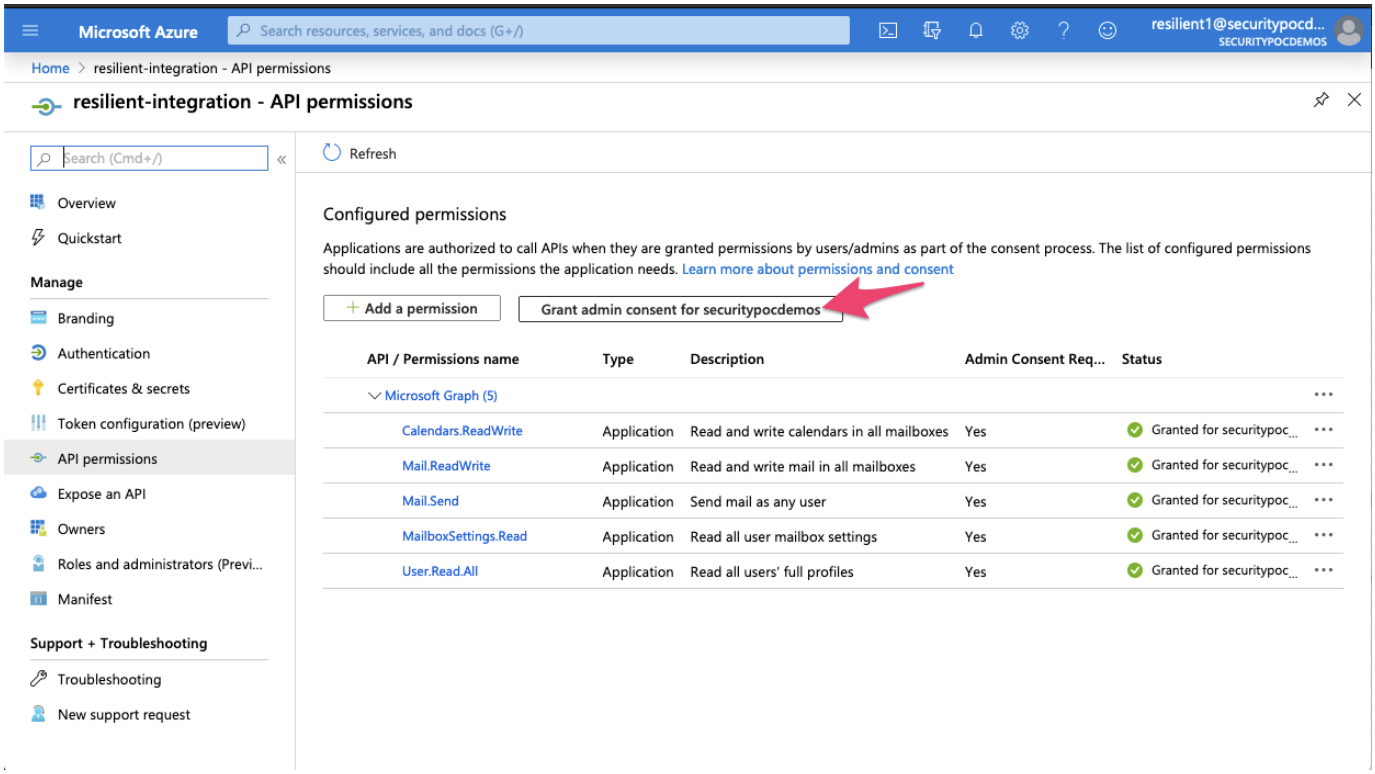


Check each of the following Microsoft Graph API "Application permissions":

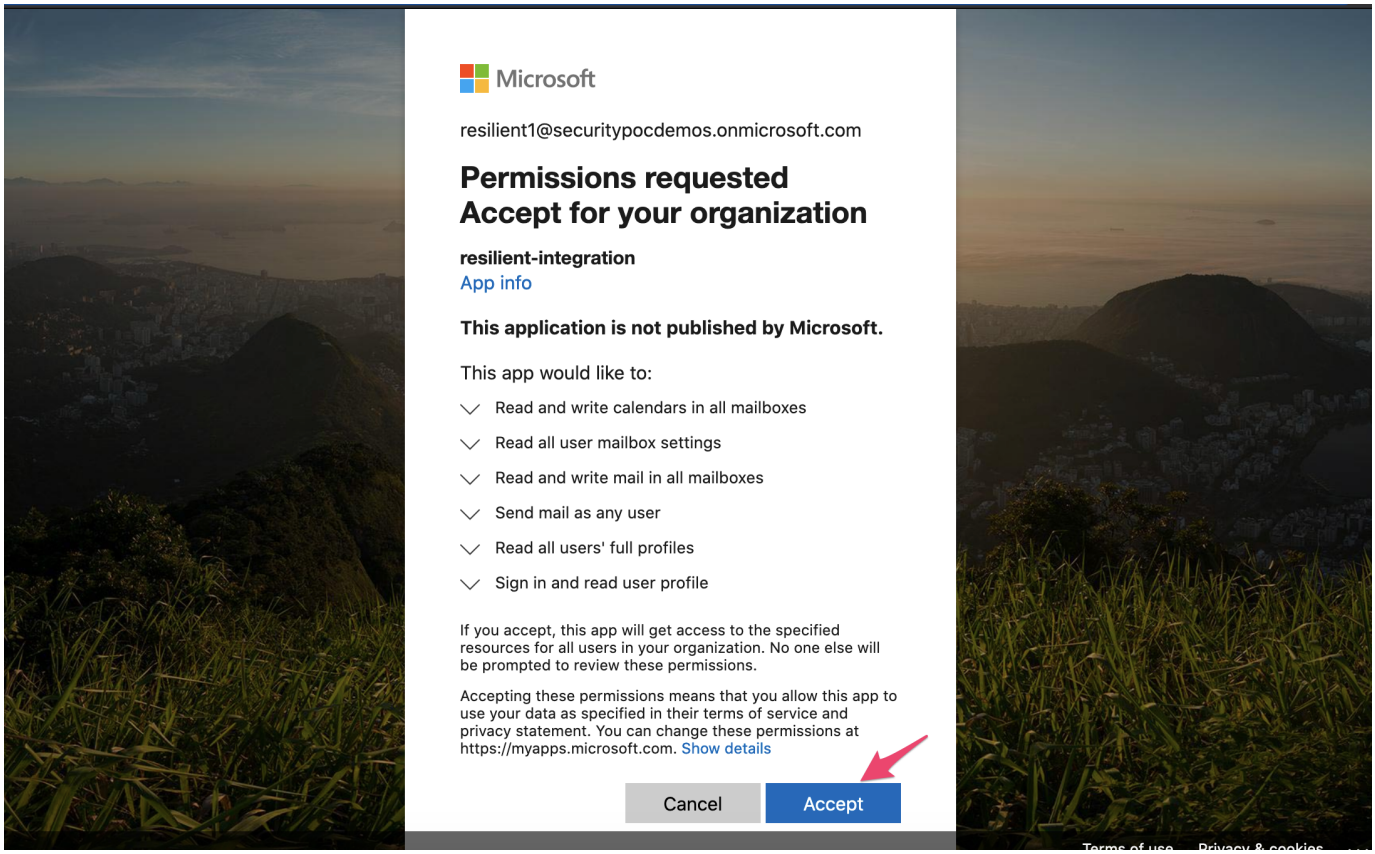
- Calendar.ReadWrite
- Mail.ReadWrite
- Mail.Send
- MailboxSetting.Read
- User.Read.All



Once the API Application permissions are added, click the "Grant admin consent" button for your domain:



You may need to log in to an admin account to accept the permissions requested on behalf of your organization:



Uninstall

- SSH into your Integration Server.
- **Uninstall** the package:

```
$ pip uninstall fn-exchange-online
```

- Open the config file, scroll to the [fn_exchange_online] section and remove the section or prefix `#` to comment out the section.
- **Save** and **Close** the app.config file.

Troubleshooting

There are several ways to verify the successful operation of a function.

Resilient Action Status

- When viewing an incident, use the Actions menu to view **Action Status**.
- By default, pending and errors are displayed.
- Modify the filter for actions to also show Completed actions.
- Clicking on an action displays additional information on the progress made or what error occurred.

Resilient Scripting Log

- A separate log file is available to review scripting errors.
- This is useful when issues occur in the pre-processing or post-processing scripts.

- The default location for this log file is: `/var/log/resilient-scripting/resilient-scripting.log` .

Resilient Logs

- By default, Resilient logs are retained at `/usr/share/co3/logs` .
- The `client.log` may contain additional information regarding the execution of functions.

Resilient-Circuits

- The log is controlled in the `.resilient/app.config` file under the section [resilient] and the property `logdir` .
- The default file name is `app.log` .
- Each function will create progress information.
- Failures will show up as errors and may contain python trace statements.

Support

Name	Version	Author	Support URL
fn_exchange_online	1.0.0	IBM Resilient	https://ibm.com/mysupport