Microsoft Exchange Online Functions for IBM Resilient

Release Notes

v1.1.0

The 1.1.0 release addresses performance issues when querying messages of all Exchange Online users of a tenant.

- Added batching of multiple message query requests into a single Microsoft Graph API request call using the /$batch endpoint. The maximum number of requests that Microsoft Graph currently supports in the batch endpoint is 20 requests. Should Microsoft change this value, the `max_batch_requests` parameter should be updated in the app.config file.
- Added "max retries" capability to Microsoft Graph API requests. When making many Microsoft Graph API calls, the Microsoft Graph server may throttle the client and return 503 (server unavailable) or 429 (too many requests) status codes. When this happens, the server may send back a "Retry-After" response header indicating to the client how long to wait and retry sending the request. If this header is not sent to the client, parameters can be set to indicate how long to wait and retry sending the request again. These parameters are settable in the app.config file:
  - max_retries_total
  - max_retries_backoff_factor
- Added capability to specify a subset of email addresses to search. When querying messages of `all` tenant email addresses, the user can specify a subset of all user mailboxes to search. For example, enter `all:r` in the `Email Address` select field of the `Example: Exchange Online Query Messages` activity popup menu to specify searching all users with PrincipalUserName starting with the letter "r". Enter `all:mc` to search all users starting with "mc".
- The `Example: Exchange Online Query Messages` and `Example: Exchange Online Delete Messages from Query Results` menu item rules and workflows allow the user to multi-select where query results are displayed:
  - Exchange Online data table
  - Incident note
  - Incident attachment
- Fixed bug in query messages function which resulted in the search not completing when the queried message subject or message body contained single quote, hashtag or ampersand characters.
- Removed Exchange Online Web Link to Outlook message from the Exchange Online Message Query Results data table when the message is deleted or not found.

NOTE Existing users running Exchange Online functions on an integration server, should save the [fn_exchange_online] section of their app.config file to another file and delete that section from the app.config file before installing the new version, as this section has changed. After installation, run the following command to obtain the new configuration:

```
$ resilient-circuits config -u -l fn-microsoft-exchange-online
```

Edit the required configuration setting as described in the Integration Server section.

v1.0.0

- Initial Release

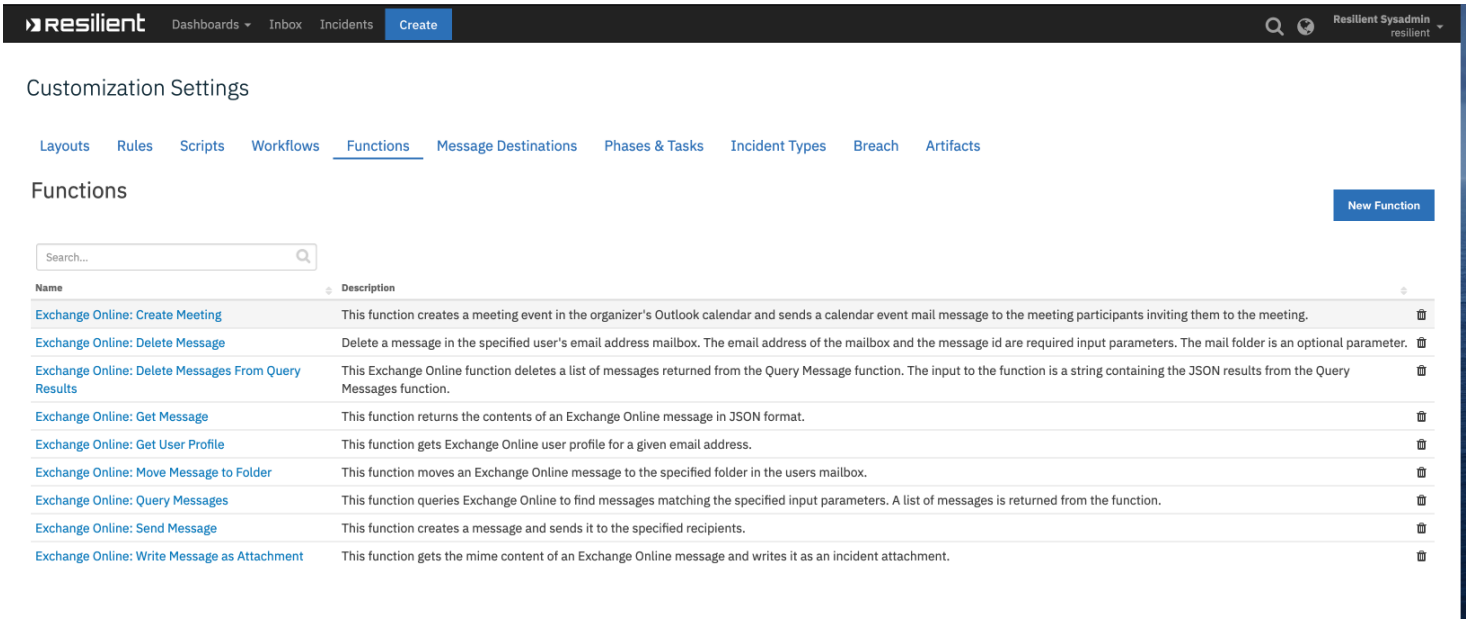
Overview

Microsoft Exchange Online Functions for IBM Resilient provides the capability to access and manipulate Microsoft Exchange Online messages from the IBM Resilient SOAR Platform. The integration uses Microsoft Graph API to access the data in Microsoft 365. Included in the integration are the following capabilities:

- Get the user profile of the specified email address in JSON format.
- Get a specified message 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 a 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
  - message received date
  - text contained in the message subject or the message body
  - whether the message has attachments.

  Detailed results are returned in the Exchange Online Query Message Results data table. Total messages found in each mailbox and the total query time are written to an incident note or attachment.
- 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 >= `v35.0.0`
- If not using an App Host, 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:

        - Org Data.Edit
        - Incidents.Read
        - Incidents.Edit.Fields
        - Incidents.Edit.Notes
        - 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" for this integration:
    - Calendars.ReadWrite
    - Mail.ReadWrite
    - Mail.Send
    - MailboxSettings.Read
    - User.Read.All

  NOTE: Not all permissions are needed for each function, as explained in the Exchange Online Integration User Guide.
  To set up Microsoft Azure permissions see section, Microsoft Azure App Configuration.

Installation

App Format

The app .zip file is in a container format and requires a Resilient platform configured with an App Host.

The app tar.gz file is an extension format and requires a Resilient platform configured with an integration server.

App Host

For a complete guide on how to configure App Host and install apps in the Resilient platform, please reference the Resilient Apps topic in the Knowledge Center. Knowledge Center.

All the components for running this integration in a container already exist when using the App Host app.

To install,

- Navigate to Administrative Settings and then the Apps tab.
- Click the Install button and select the downloaded file: app-fn_echange_online-x.x.x.zip.
- Go to the Configuration tab and edit the app.config file, editing the tenant_id, client_id and client_secret and making any additional setting changes.

Config	Required	Example	Description
microsoft_graph_token_url	Yes	`https://login.microsoftonline.com/{tenant}/oauth2/v2.0/token`	*Microsoft Graph URL endpoint for acquiring access token*

Config	Required	Example	Description
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_batched_requests	Yes	`20`	*Maximum number of requests to send MS Graph API $batch endpoint in single call*
max_messages	Yes	`100`	*Maximum number of messages that a query returns*
max_users	Yes	`2000`	*Maximum number of users searched in a query*
max_retries_total	Yes	`10`	*Maximum number of retries for MS Graph API request*
max_retries_backoff_factor	Yes	`5`	*Backoff factor used to determine time to sleep between requests*

Integration Server

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

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

- **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 -l fn-exchange-online
```

- 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
```

- 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 -l fn-exchange-online
```

- 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 acquiring access token*
microsoft_graph_url	Yes	`https://graph.microsoft.com/v1.0`	*Microsoft Graph base URL*

Config	Required	Example	Description
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_batched_requests	Yes	`20`	*Maximum number of requests to send MS Graph API $batch endpoint in single call*
max_messages	Yes	`100`	*Maximum number of messages that a query returns*
max_users	Yes	`2000`	*Maximum number of users searched in a query*
max_retries_total	Yes	`10`	*Maximum number of retries for MS Graph API request*
max_retries_backoff_factor	Yes	`5`	*Backoff factor used to determine time to sleep between requests*

- **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
```

Uninstall

If using an integration server, you can uninstall your app as follows:

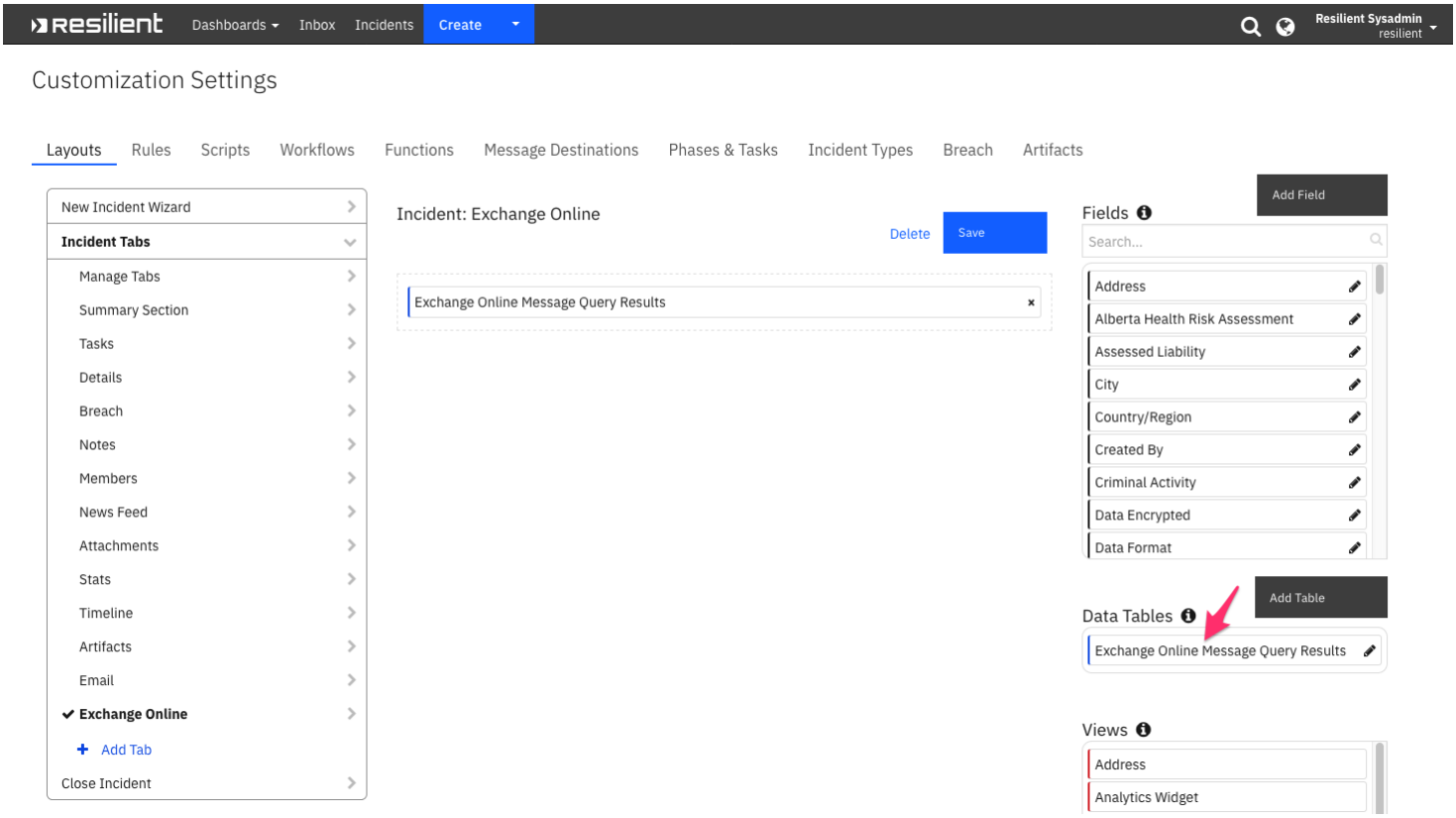
- SSH into your Integration Server.
- **Uninstall** the package:

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

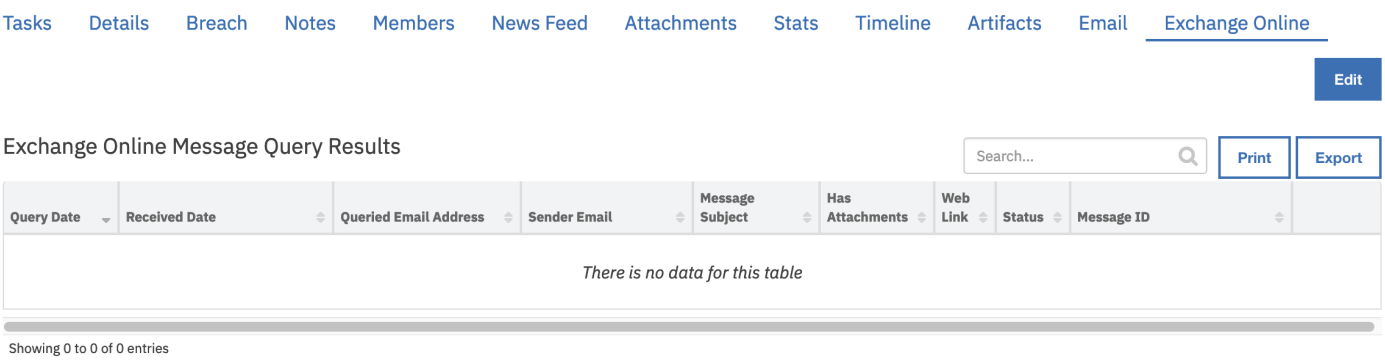
- Open the config file, scroll to the [fn_exchange_online] section and remove the section or prefix `#` to comment out the section.
- **Save** and **Close** the app.config file.

Custom Layouts

Create an Exchange Online custom incident tab and drag the Exchange Online Message Query Results data table on to the layout as shown in the following screenshot. When done, click Save.



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

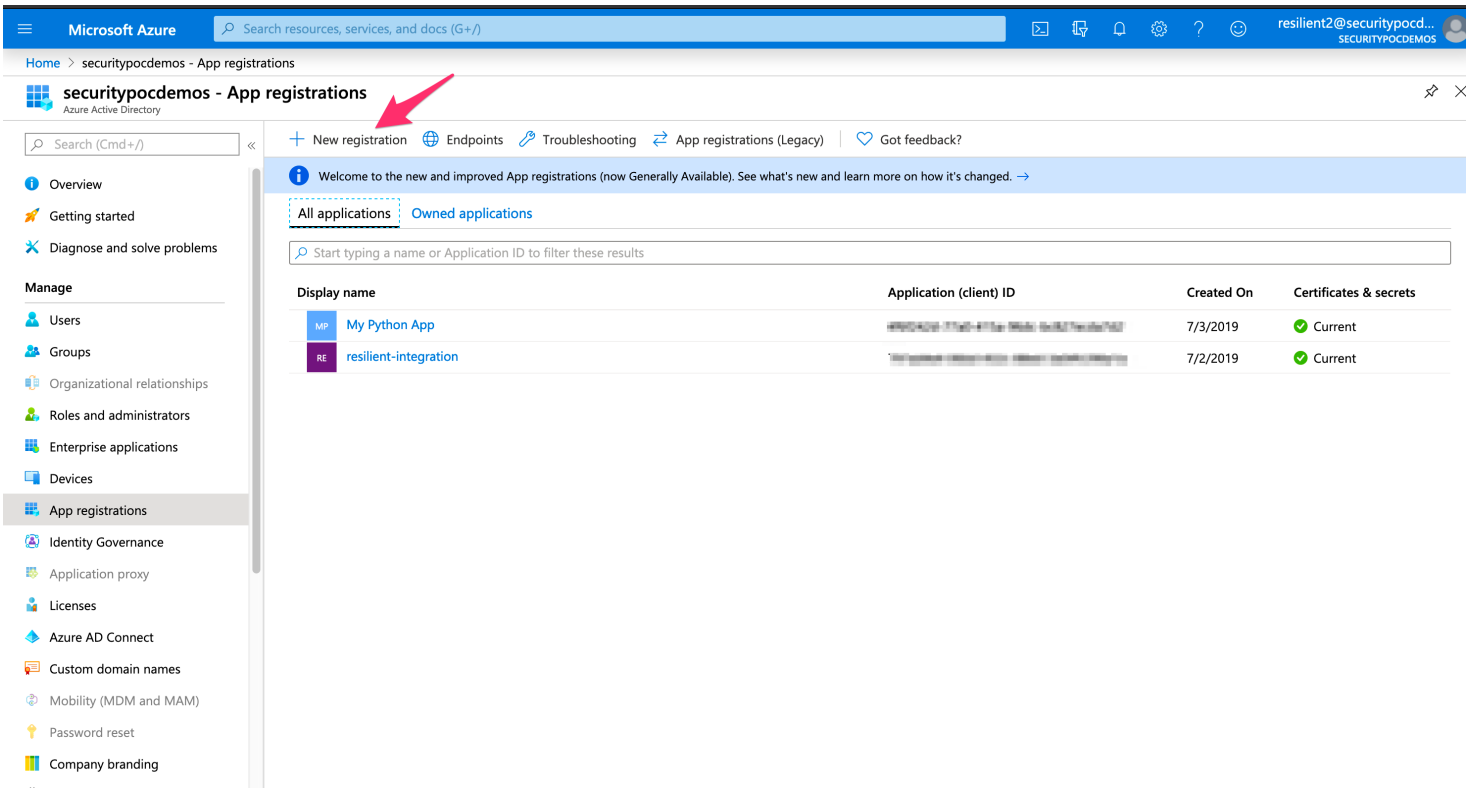


Microsoft Azure App Configuration

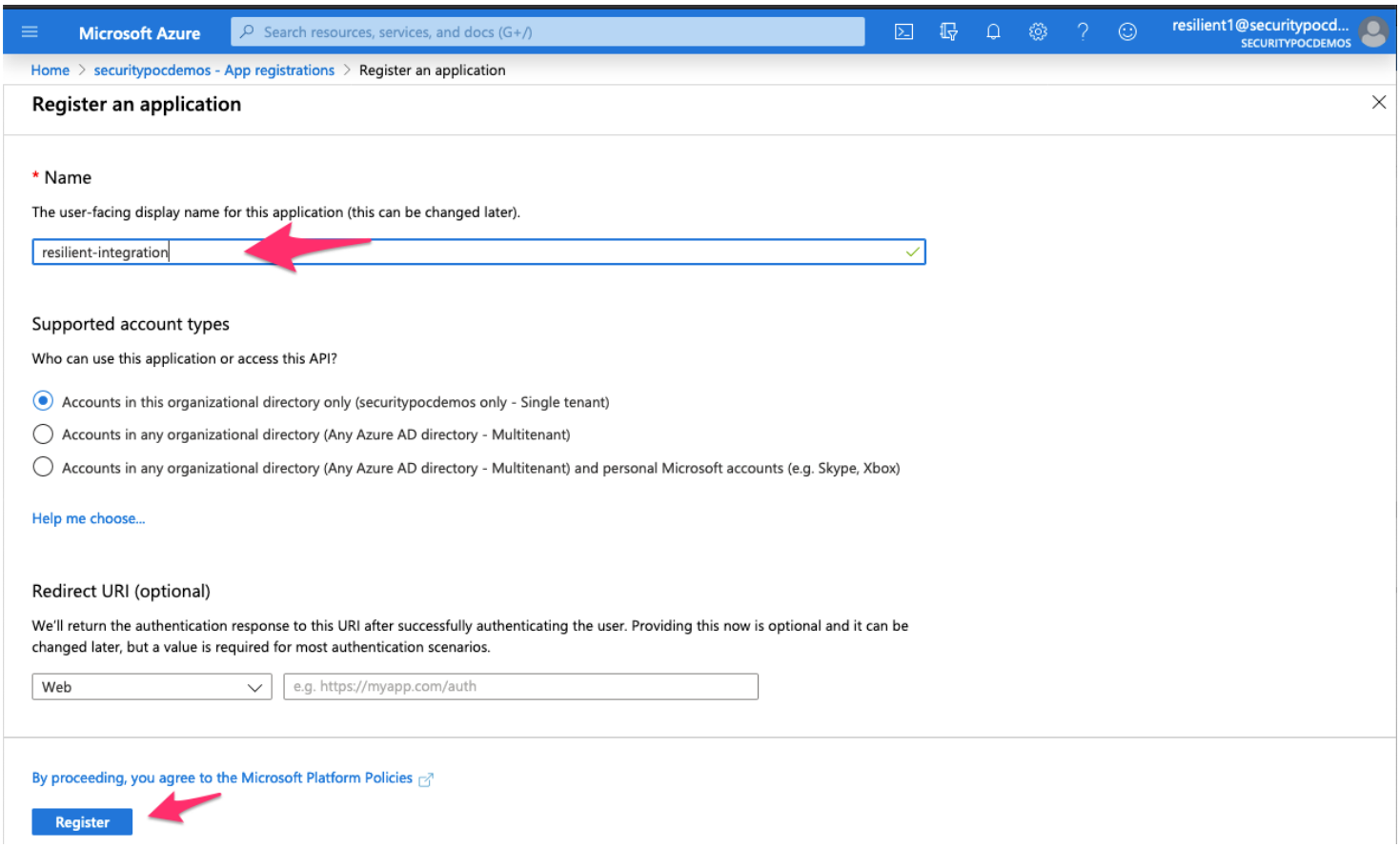
To run the Resilient Exchange Online integration, you must first register the application on Microsoft Azure portal. The tenant ID, client ID and the client secret that are defined in the fn_exchange_online section of the app.config are assigned by Azure when the application is registered.

App Registration

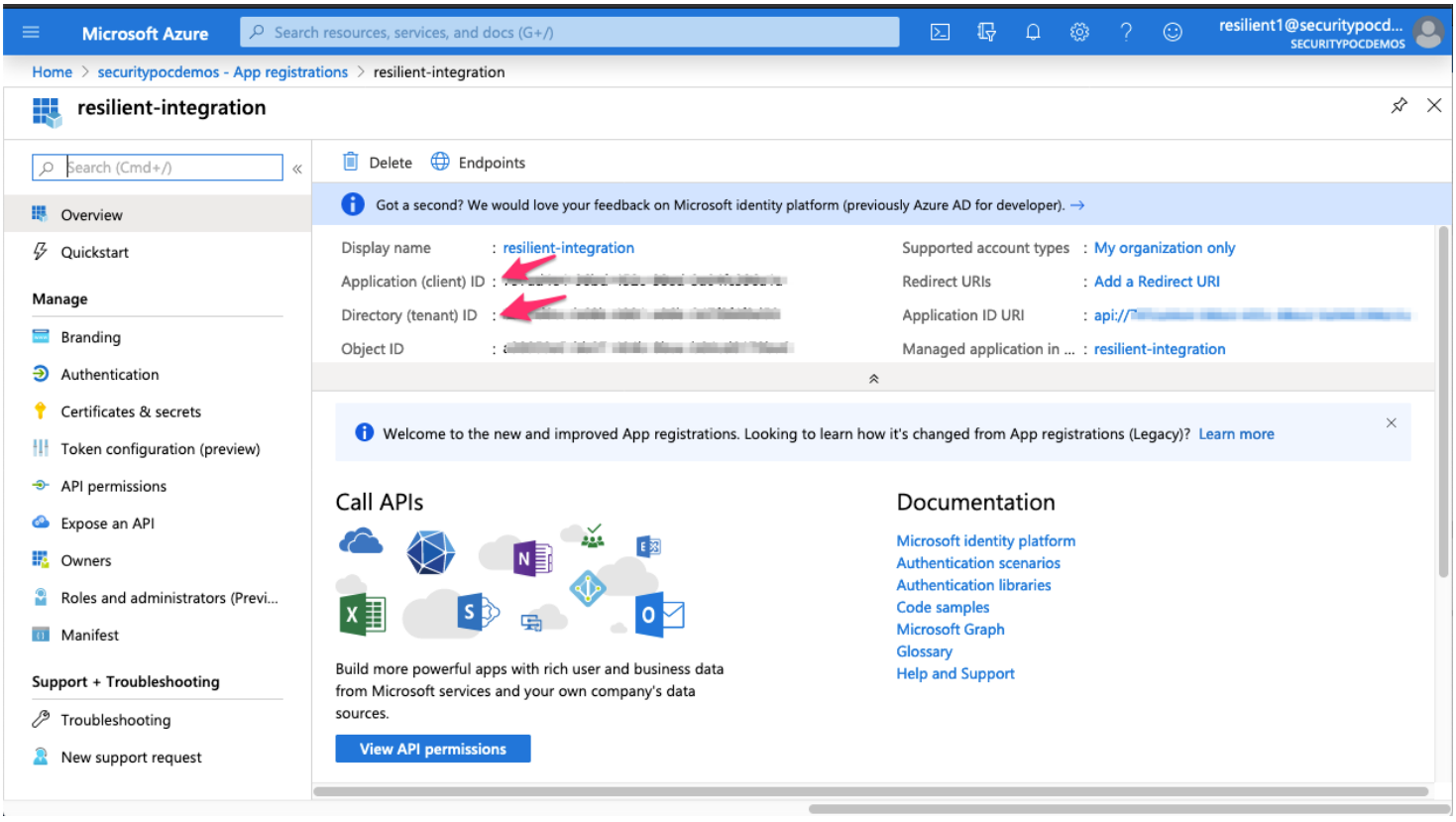
To register the Resilient integration, click "App registrations" in Manage section of your Azure Active Directory domain account. Then click the "New Registration" button as depicted in the image below.



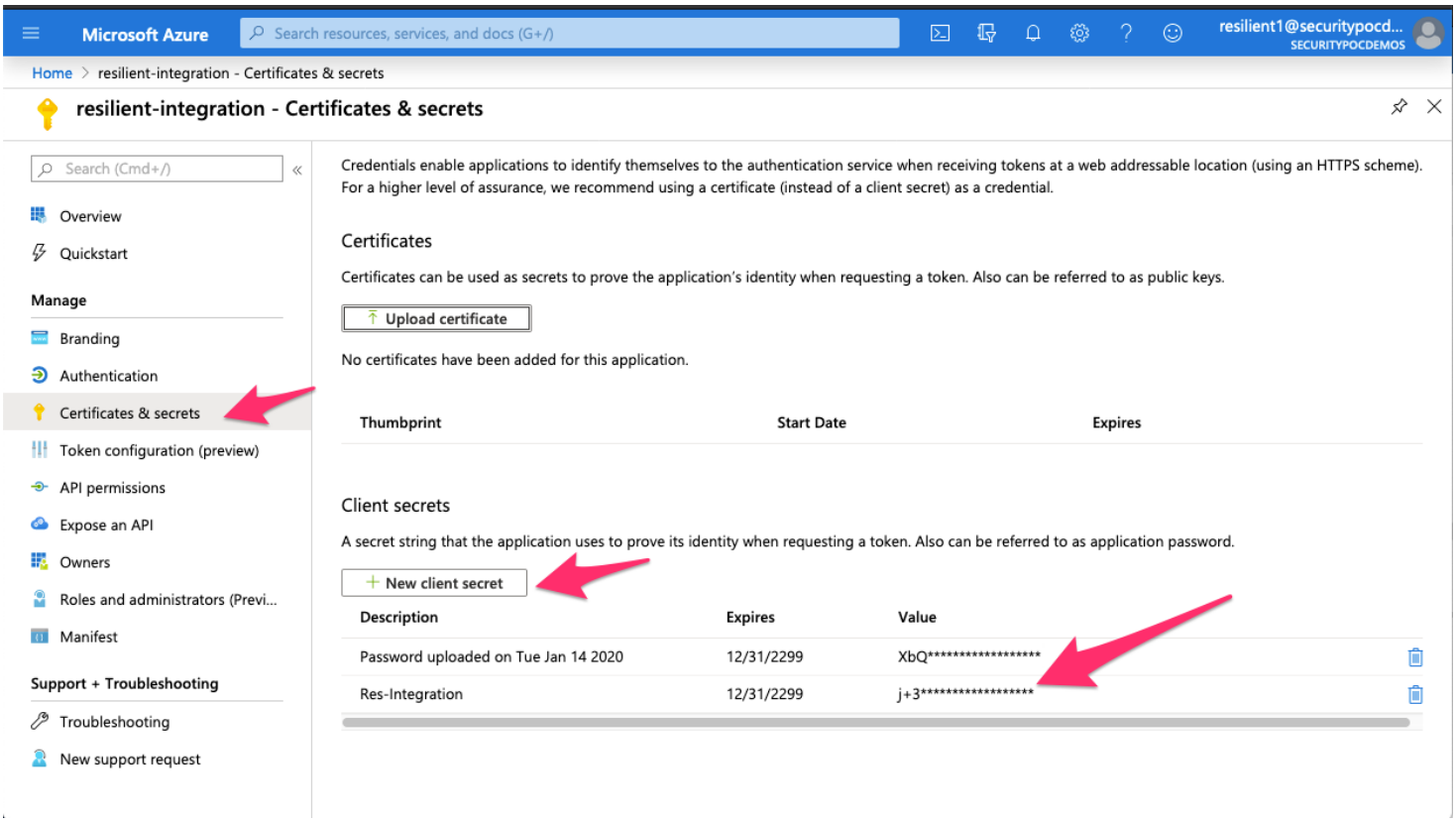
Enter a name for the integration. In this example, the name is "resilient-integration". Then press the "Register" button.



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:

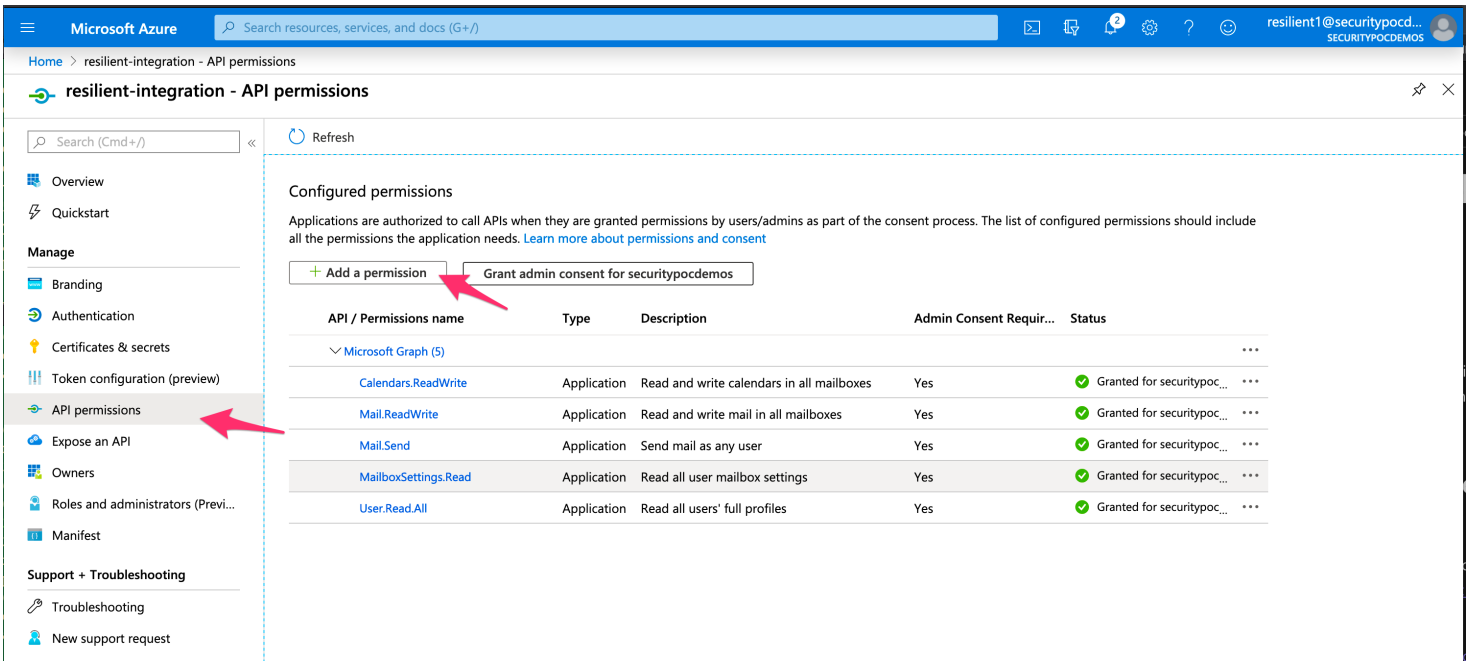


Next, click on the left menu item, "Certificates & secrets" and create a secret, which is another application credential in the app.config.

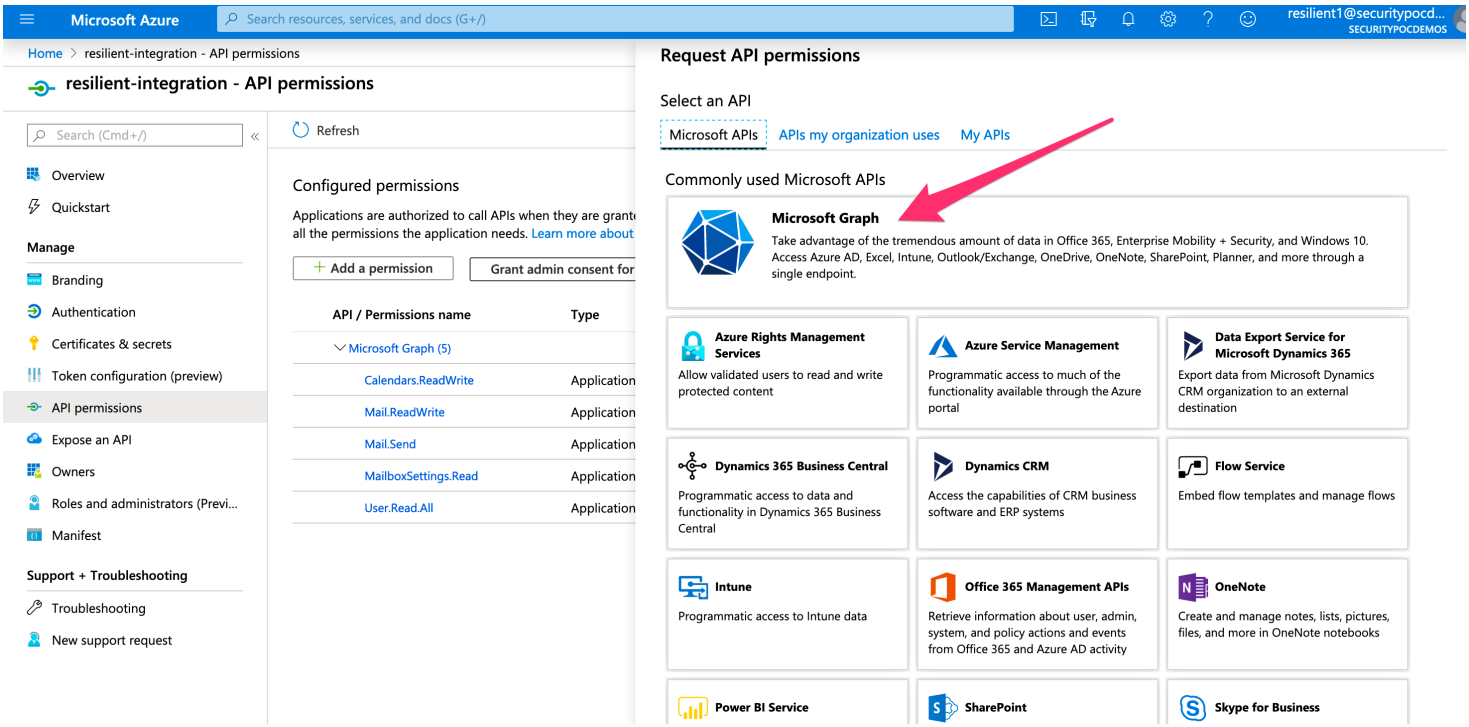


API Permissions

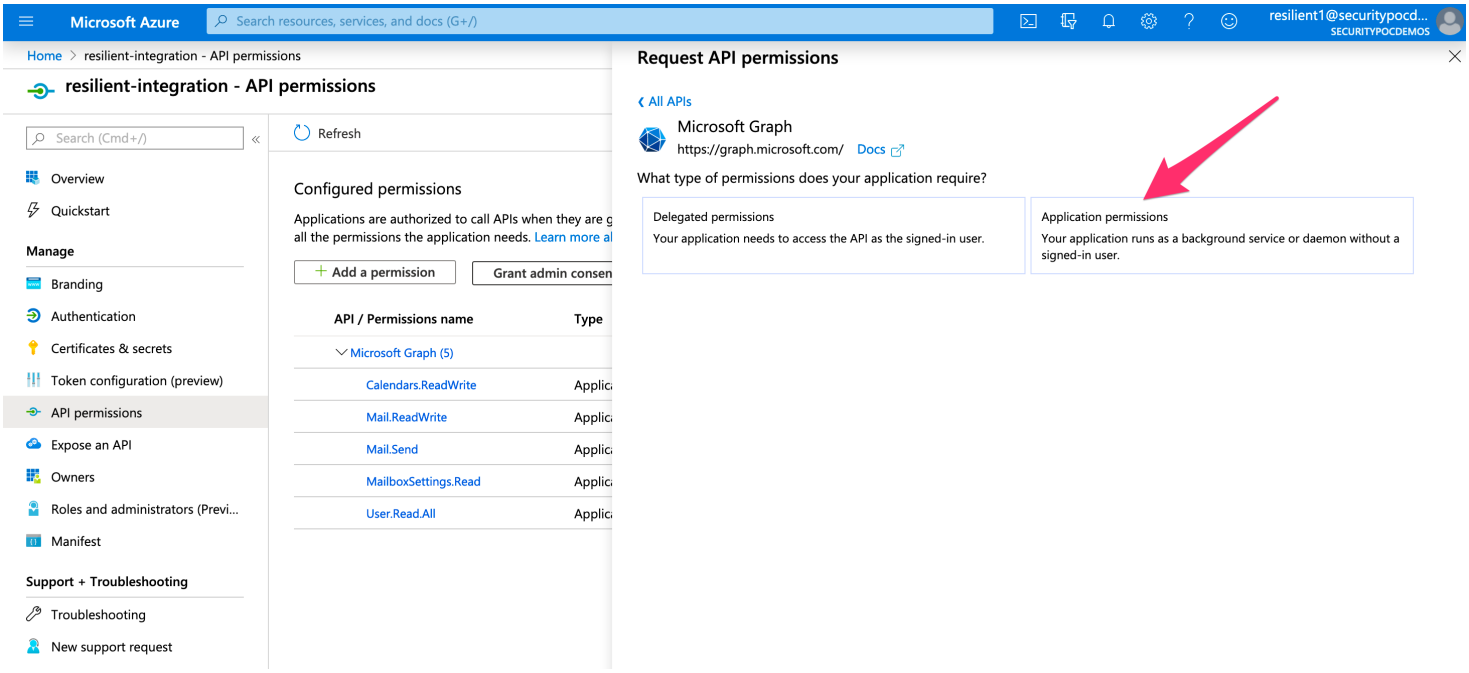
For the Resilient integration app to access data in Microsoft Graph, an administrator must grant it the correct permissions via a consent process. Click on "API permissions" on the left menu and then "+ Add a Permission".



Click on Microsoft Graph:

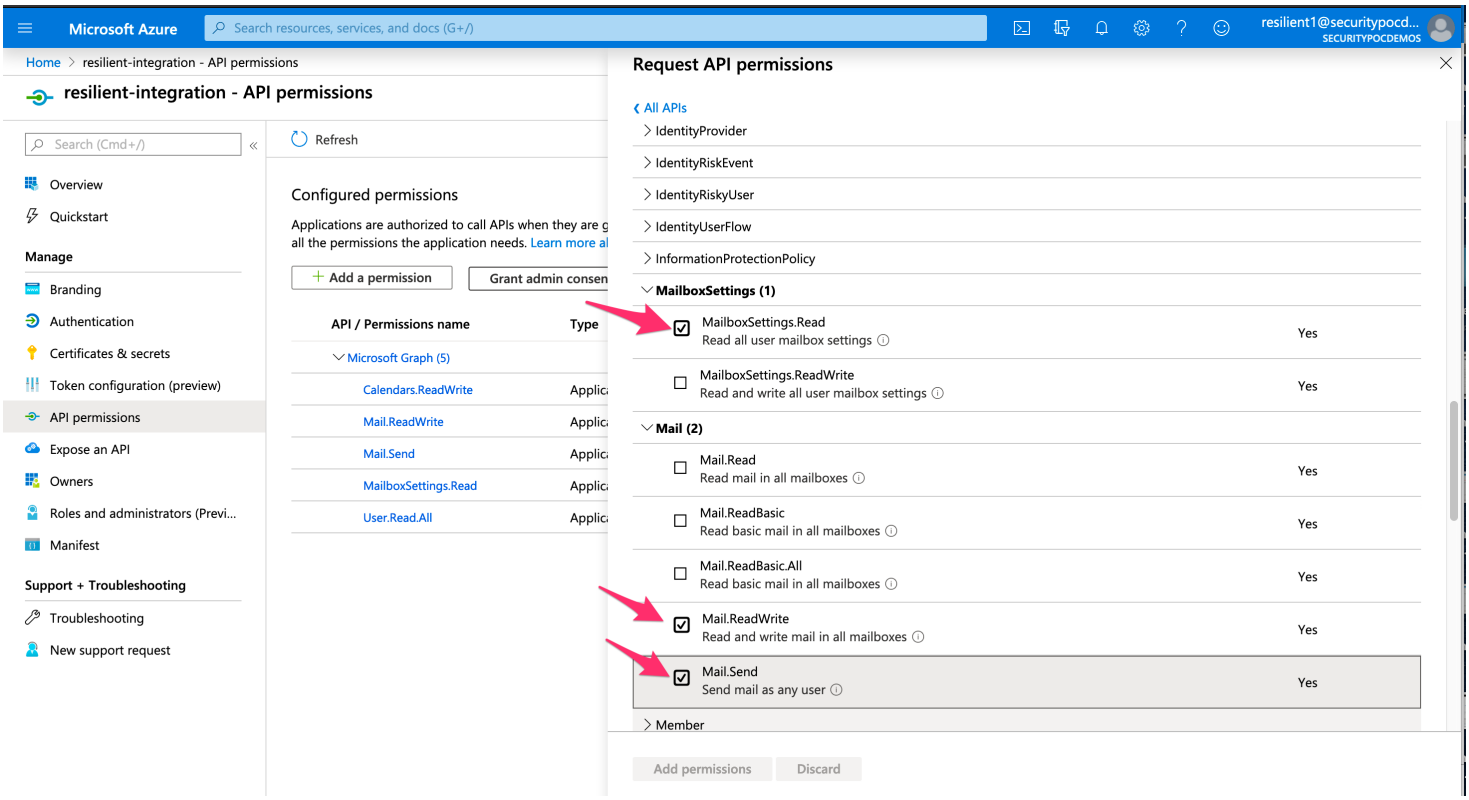


Select Application permissions (not Delegated permissions):

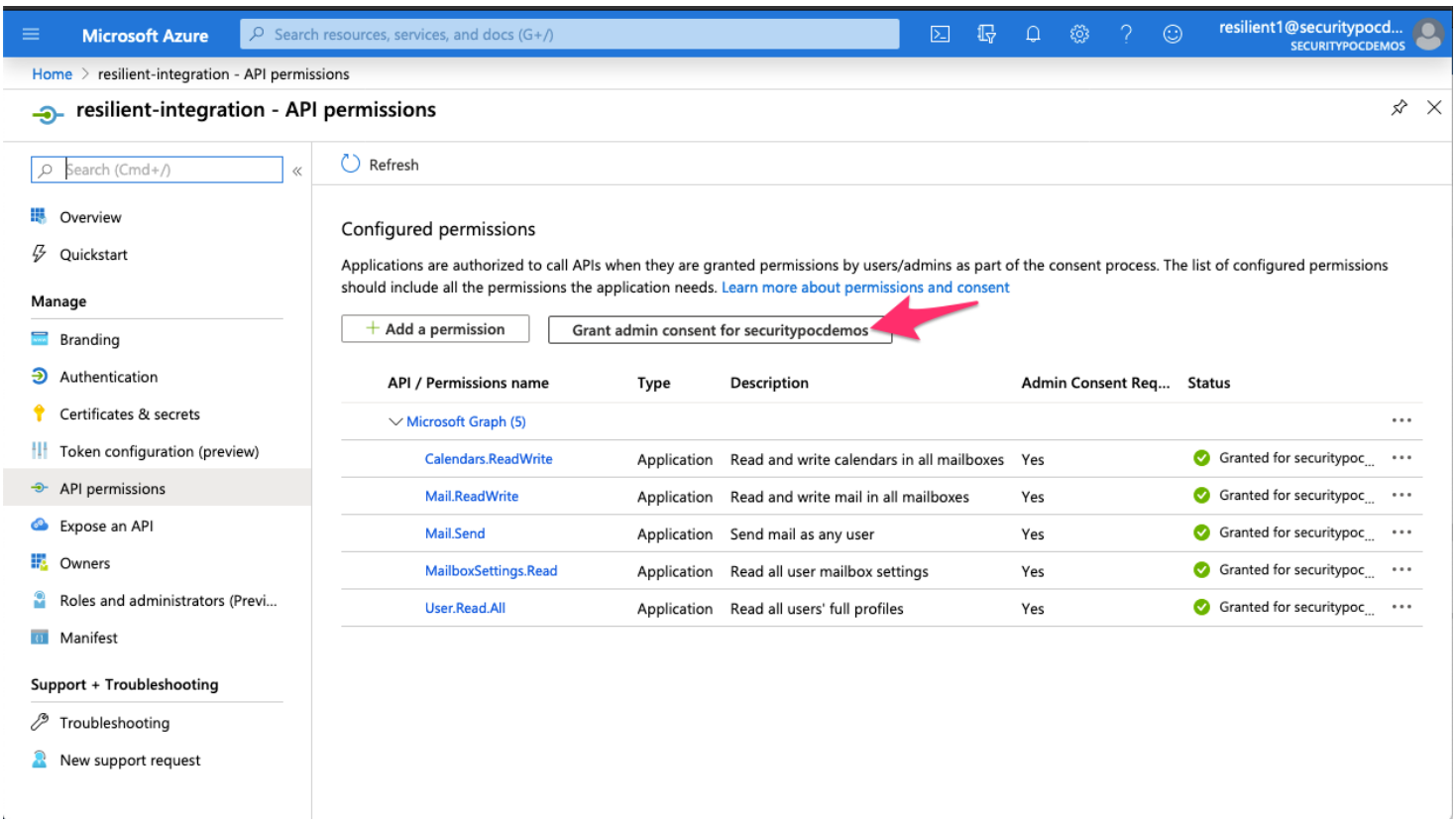


Check each of the following Microsoft Graph API "Application permissions":

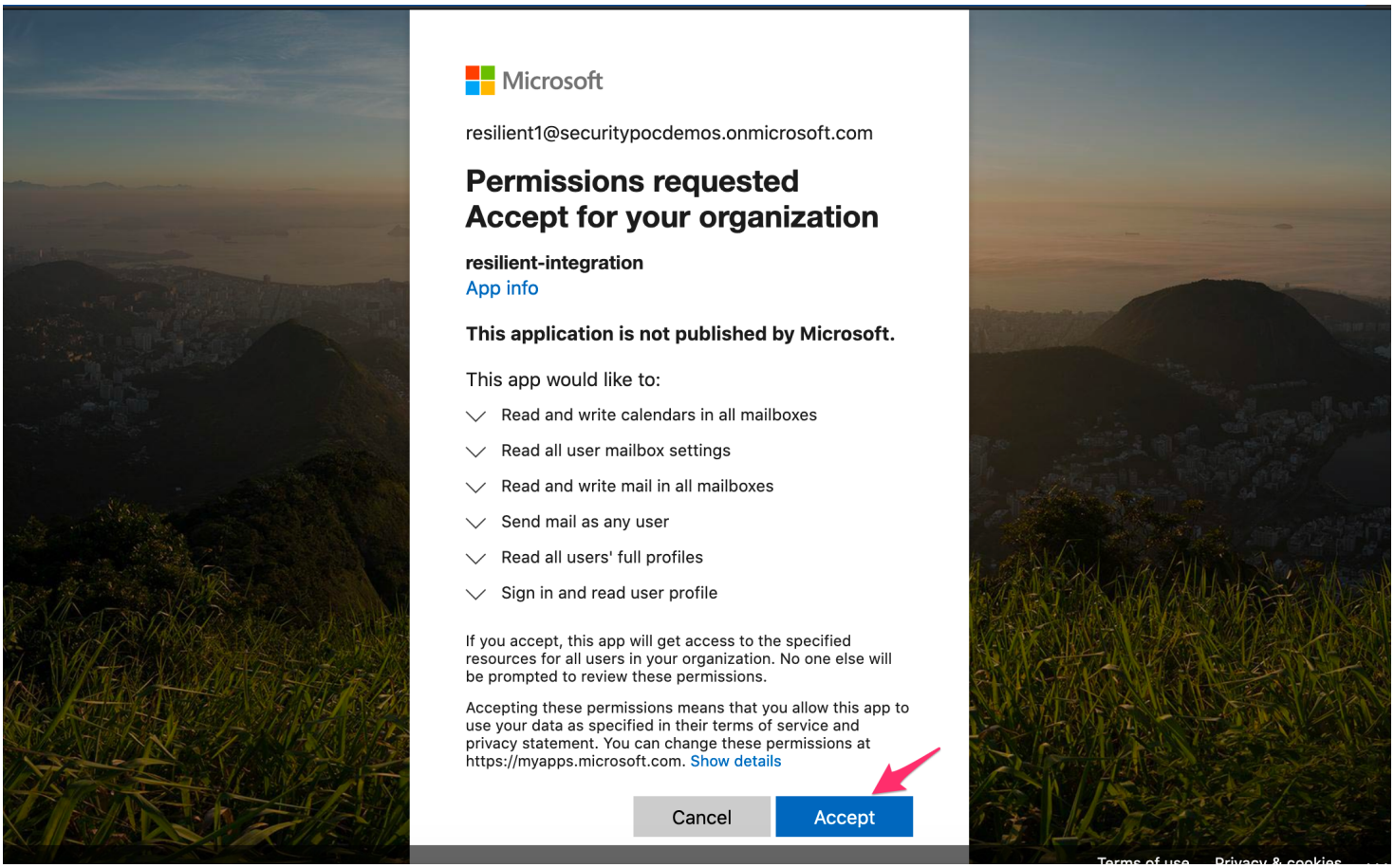
- Calendar.ReadWrite
- Mail.ReadWrite
- Mail.Send
- MailboxSetting.Read
- User.Read.All



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:



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	1.1.0	IBM Resilient	https://ibm.com/mysupport