

# Microsoft Exchange Online Functions for IBM Resilient

- [Release Notes](#)
- [Overview](#)
- [Requirements](#)
- [Installation](#)
- [Troubleshooting](#)
- [Support](#)

## 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:

Resilient

Dashboards

Inbox

Incidents

Create

Q

Resilient Sysadmin resilient

Customization Settings

Layouts

Rules

Scripts

Workflows

Functions

Message Destinations

Phases & Tasks

Incident Types

Breach

Artifacts

Functions

New Function

Search...

Q

| Name                                                | Description                                                                                                                                                                                            |  |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Exchange Online: Create Meeting                     | This function creates a meeting event in the organizer's Outlook calendar and sends a calendar event mail message to the meeting participants inviting them to the meeting.                            |  |
| Exchange Online: Delete Message                     | Delete a message in the specified user's email address mailbox. The email address of the mailbox and the message id are required input parameters. The mail folder is an optional parameter.           |  |
| Exchange Online: Delete Messages From Query Results | This Exchange Online function deletes a list of messages returned from the Query Message function. The input to the function is a string containing the JSON results from the Query Messages function. |  |
| Exchange Online: Get Message                        | This function returns the contents of an Exchange Online message in JSON format.                                                                                                                       |  |
| Exchange Online: Get User Profile                   | This function gets Exchange Online user profile for a given email address.                                                                                                                             |  |
| Exchange Online: Move Message to Folder             | This function moves an Exchange Online message to the specified folder in the users mailbox.                                                                                                           |  |
| Exchange Online: Query Messages                     | This function queries Exchange Online to find messages matching the specified input parameters. A list of messages is returned from the function.                                                      |  |
| Exchange Online: Send Message                       | This function creates a message and sends it to the specified recipients.                                                                                                                              |  |
| Exchange Online: Write Message as Attachment        | This function gets the mime content of an Exchange Online message and writes it as an incident attachment.                                                                                             |  |

# 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](https://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\_exchange\_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                                                    |
|----------------------------------|----------|---------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>microsoft_graph_token_url</b> | Yes      | <code>https://login.microsoftonline.com/{tenant}/oauth2/v2.0/token</code> | <i>Microsoft Graph URL endpoint for acquiring access token</i> |

| Config                            | Required | Example                          | Description                                                                     |
|-----------------------------------|----------|----------------------------------|---------------------------------------------------------------------------------|
| <b>microsoft_graph_url</b>        | Yes      | https://graph.microsoft.com/v1.0 | Microsoft Graph base URL                                                        |
| <b>tenant_id</b>                  | Yes      | xxx                              | Microsoft Azure Tenant ID                                                       |
| <b>client_id</b>                  | Yes      | xxx                              | Microsoft Azure Client ID (Application ID)                                      |
| <b>client_secret</b>              | Yes      | xxx                              | Microsoft Azure Client Secret                                                   |
| <b>max_batched_requests</b>       | Yes      | 20                               | Maximum number of requests to send MS Graph API \$batch endpoint in single call |
| <b>max_messages</b>               | Yes      | 100                              | Maximum number of messages that a query returns                                 |
| <b>max_users</b>                  | Yes      | 2000                             | Maximum number of users searched in a query                                     |
| <b>max_retries_total</b>          | Yes      | 10                               | Maximum number of retries for MS Graph API request                              |
| <b>max_retries_backoff_factor</b> | 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                                                    |
|----------------------------------|----------|---------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>microsoft_graph_token_url</b> | Yes      | <code>https://login.microsoftonline.com/{tenant}/oauth2/v2.0/token</code> | <i>Microsoft Graph URL endpoint for acquiring access token</i> |
| <b>microsoft_graph_url</b>       | Yes      | <code>https://graph.microsoft.com/v1.0</code>                             | <i>Microsoft Graph base URL</i>                                |

| Config                            | Required | Example | Description                                                                     |
|-----------------------------------|----------|---------|---------------------------------------------------------------------------------|
| <b>tenant_id</b>                  | Yes      | xxx     | Microsoft Azure Tenant ID                                                       |
| <b>client_id</b>                  | Yes      | xxx     | Microsoft Azure Client ID (Application ID)                                      |
| <b>client_secret</b>              | Yes      | xxx     | Microsoft Azure Client Secret                                                   |
| <b>max_batched_requests</b>       | Yes      | 20      | Maximum number of requests to send MS Graph API \$batch endpoint in single call |
| <b>max_messages</b>               | Yes      | 100     | Maximum number of messages that a query returns                                 |
| <b>max_users</b>                  | Yes      | 2000    | Maximum number of users searched in a query                                     |
| <b>max_retries_total</b>          | Yes      | 10      | Maximum number of retries for MS Graph API request                              |
| <b>max_retries_backoff_factor</b> | 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 screenshot displays the Resilient Sysadmin interface for customizing an incident layout. The top navigation bar includes the Resilient logo and a 'Create' button. The left sidebar lists various customization options, with 'Layouts' selected. The main workspace shows the 'Incident: Exchange Online' configuration. A dashed box highlights the 'Exchange Online Message Query Results' data table being added to the layout. The right sidebar contains three sections: 'Fields' (with a search bar and a list of fields), 'Data Tables' (with a red arrow pointing to the 'Exchange Online Message Query Results' table), and 'Views' (with a list of views including 'Address' and 'Analytics Widget').

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

## Exchange Online Message Query Results

Search...

Print

Export

| Query Date                      | Received Date | Queried Email Address | Sender Email | Message Subject | Has Attachments | Web Link | Status | Message ID |
|---------------------------------|---------------|-----------------------|--------------|-----------------|-----------------|----------|--------|------------|
| There is no data for this table |               |                       |              |                 |                 |          |        |            |

Showing 0 to 0 of 0 entries

## 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.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information for 'resilient2@securitypocd...'. The left sidebar shows the 'Manage' section with 'App registrations' highlighted. The main content area displays the 'App registrations' page with a welcome message and a table of existing applications. A red arrow points to the 'New registration' button in the top navigation bar.

| Display name             | Application (client) ID | Created On | Certificates & secrets |
|--------------------------|-------------------------|------------|------------------------|
| MP My Python App         | ...                     | 7/3/2019   | Current                |
| RE resilient-integration | ...                     | 7/2/2019   | Current                |

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



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

Home > securitypocdemos - App registrations > Register an application

## Register an application

**\* Name**  
The user-facing display name for this application (this can be changed later).

resilient-integration ✓

**Supported account types**  
Who can use this application or access this API?

☒ Accounts in this organizational directory only (securitypocdemos only - Single tenant)  
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)  
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

**Redirect URI (optional)**  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

**Register**

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:

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

Home > securitypocdemos - App registrations > resilient-integration

## resilient-integration

Search (Cmd+/)

Overview

Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration (preview)
- API permissions
- Expose an API
- Owners
- Roles and administrators (Previous version)
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Delete Endpoints

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

Display name : resilient-integration

Application (client) ID : 11111111-1111-1111-1111-111111111111

Directory (tenant) ID : 11111111-1111-1111-1111-111111111111

Object ID : 11111111-1111-1111-1111-111111111111

Supported account types : My organization only

Redirect URIs : Add a Redirect URI

Application ID URI : api://11111111-1111-1111-1111-111111111111

Managed application in ... : resilient-integration

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

**Call APIs**

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API permissions](#)

**Documentation**

- Microsoft identity platform
- Authentication scenarios
- Authentication libraries
- Code samples
- Microsoft Graph
- Glossary
- Help and Support

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

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

Home > resilient-integration - Certificates & secrets

### resilient-integration - Certificates & secrets

Search (Cmd+)

- Overview
- Quickstart
- Manage
  - Branding
  - Authentication
  - Certificates & secrets**
  - Token configuration (preview)
  - API permissions
  - Expose an API
  - Owners
  - Roles and administrators (Previ...
  - Manifest
- Support + Troubleshooting
  - Troubleshooting
  - New support request

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

#### Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

No certificates have been added for this application.

| Thumbprint | Start Date | Expires |
|------------|------------|---------|
|------------|------------|---------|

#### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[New client secret](#)

| Description                          | Expires    | Value    |
|--------------------------------------|------------|----------|
| Password uploaded on Tue Jan 14 2020 | 12/31/2299 | XbQ***** |
| Res-Integration                      | 12/31/2299 | j+3***** |

## 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".

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

Home > resilient-integration - API permissions

### resilient-integration - API permissions

Search (Cmd+)

- Overview
- Quickstart
- Manage
  - Branding
  - Authentication
  - Certificates & secrets
  - API permissions**
  - Token configuration (preview)
  - Expose an API
  - Owners
  - Roles and administrators (Previ...
  - Manifest
- Support + Troubleshooting
  - Troubleshooting
  - New support request

Refresh

#### 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 securitypocdemos](#)

| API / Permissions name | Type        | Description                               | Admin Consent Requir... | Status                         |
|------------------------|-------------|-------------------------------------------|-------------------------|--------------------------------|
| Microsoft Graph (5)    |             |                                           |                         | ...                            |
| Calendars.ReadWrite    | Application | Read and write calendars in all mailboxes | Yes                     | Granted for securitypoc... ... |
| Mail.ReadWrite         | Application | Read and write mail in all mailboxes      | Yes                     | Granted for securitypoc... ... |
| Mail.Send              | Application | Send mail as any user                     | Yes                     | Granted for securitypoc... ... |
| MailboxSettings.Read   | Application | Read all user mailbox settings            | Yes                     | Granted for securitypoc... ... |
| User.Read.All          | Application | Read all users' full profiles             | Yes                     | Granted for securitypoc... ... |

Click on Microsoft Graph:

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

Home > resilient-integration - API permissions

### resilient-integration - API permissions

Search (Cmd+/) Refresh

Overview Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration (preview)
- API permissions**
- Expose an API
- Owners
- Roles and administrators (Previ...
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

#### Configured permissions

Applications are authorized to call APIs when they are granted all the permissions the application needs. [Learn more about](#)

+ Add a permission Grant admin consent for

| API / Permissions name | Type        |
|------------------------|-------------|
| Microsoft Graph (5)    |             |
| Calendars.ReadWrite    | Application |
| Mail.ReadWrite         | Application |
| Mail.Send              | Application |
| MailboxSettings.Read   | Application |
| User.Read.All          | Application |

#### Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

#### Commonly used Microsoft APIs

**Microsoft Graph**

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

**Azure Rights Management Services**

Allow validated users to read and write protected content

**Azure Service Management**

Programmatic access to much of the functionality available through the Azure portal

**Data Export Service for Microsoft Dynamics 365**

Export data from Microsoft Dynamics CRM organization to an external destination

**Dynamics 365 Business Central**

Programmatic access to data and functionality in Dynamics 365 Business Central

**Dynamics CRM**

Access the capabilities of CRM business software and ERP systems

**Flow Service**

Embed flow templates and manage flows

**Intune**

Programmatic access to Intune data

**Office 365 Management APIs**

Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

**OneNote**

Create and manage notes, lists, pictures, files, and more in OneNote notebooks

**Power BI Service**

**SharePoint**

**Skype for Business**

## Select Application permissions (not Delegated permissions):

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

Home > resilient-integration - API permissions

### resilient-integration - API permissions

Search (Cmd+/) Refresh

Overview Quickstart

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration (preview)
- API permissions**
- Expose an API
- Owners
- Roles and administrators (Previ...
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

#### Configured permissions

Applications are authorized to call APIs when they are granted all the permissions the application needs. [Learn more about](#)

+ Add a permission Grant admin consent for

| API / Permissions name | Type        |
|------------------------|-------------|
| Microsoft Graph (5)    |             |
| Calendars.ReadWrite    | Application |
| Mail.ReadWrite         | Application |
| Mail.Send              | Application |
| MailboxSettings.Read   | Application |
| User.Read.All          | Application |

#### Request API permissions

All APIs

**Microsoft Graph**

<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

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

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

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

Home > resilient-integration - API permissions

### resilient-integration - API permissions

Search (Cmd+/) << Refresh

Overview  
Quickstart  
Manage  
Branding  
Authentication  
Certificates & secrets  
Token configuration (preview)  
API permissions  
Expose an API  
Owners  
Roles and administrators (Previ...  
Manifest  
Support + Troubleshooting  
Troubleshooting  
New support request

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 securitypocdemos

| API / Permissions name | Type        |
|------------------------|-------------|
| Microsoft Graph (5)    |             |
| Calendars.ReadWrite    | Application |
| Mail.ReadWrite         | Application |
| Mail.Send              | Application |
| MailboxSettings.Read   | Application |
| User.Read.All          | Application |

### Request API permissions

< All APIs

- IdentityProvider
- IdentityRiskEvent
- IdentityRiskyUser
- IdentityUserFlow
- InformationProtectionPolicy
- MailboxSettings (1)
  - ☒ MailboxSettings.Read  
Read all user mailbox settings ⓘ Yes
  - ☐ MailboxSettings.ReadWrite  
Read and write all user mailbox settings ⓘ Yes
- Mail (2)
  - ☐ Mail.Read  
Read mail in all mailboxes ⓘ Yes
  - ☐ Mail.ReadBasic  
Read basic mail in all mailboxes ⓘ Yes
  - ☐ Mail.ReadBasic.All  
Read basic mail in all mailboxes ⓘ Yes
  - ☒ Mail.ReadWrite  
Read and write mail in all mailboxes ⓘ Yes
  - ☒ Mail.Send  
Send mail as any user ⓘ Yes
- Member

Add permissions Discard

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

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

Home > resilient-integration - API permissions

### resilient-integration - API permissions

Search (Cmd+/) << Refresh

Overview  
Quickstart  
Manage  
Branding  
Authentication  
Certificates & secrets  
Token configuration (preview)  
API permissions  
Expose an API  
Owners  
Roles and administrators (Previ...  
Manifest  
Support + Troubleshooting  
Troubleshooting  
New support request

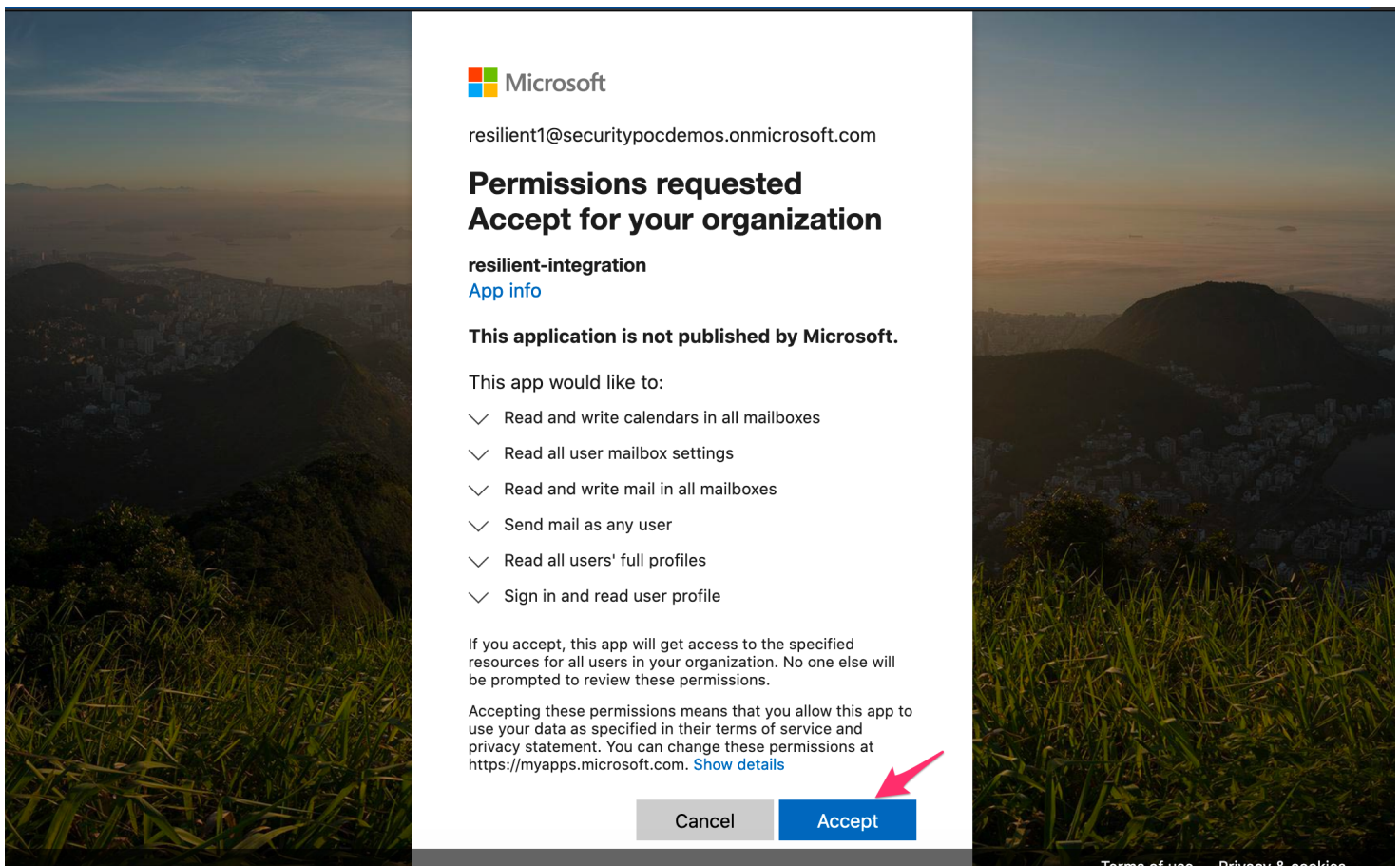
Configured permissions

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 securitypocdemos

| API / Permissions name | Type        | Description                               | Admin Consent Req... | Status                     |
|------------------------|-------------|-------------------------------------------|----------------------|----------------------------|
| Microsoft Graph (5)    |             |                                           |                      |                            |
| Calendars.ReadWrite    | Application | Read and write calendars in all mailboxes | Yes                  | Granted for securitypoc... |
| Mail.ReadWrite         | Application | Read and write mail in all mailboxes      | Yes                  | Granted for securitypoc... |
| Mail.Send              | Application | Send mail as any user                     | Yes                  | Granted for securitypoc... |
| MailboxSettings.Read   | Application | Read all user mailbox settings            | Yes                  | Granted for securitypoc... |
| User.Read.All          | Application | Read all users' full profiles             | Yes                  | Granted for securitypoc... |

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 | <a href="https://ibm.com/mysupport">https://ibm.com/mysupport</a> |