

Microsoft Exchange Online Functions for IBM Resilient

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

Release Notes

v1.3.0

- Support attaching incident attachments to a message.

v1.2.0

- Minor performance improvement when query "all" user mailboxes.
- Continue querying "all" users if there is an error returned from a single call to the \$batch endpoint.

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-exchange-online
```

Edit the required configuration setting as described in the [Integration Server](#) section.

v1.0.0

- Initial Release

Overview

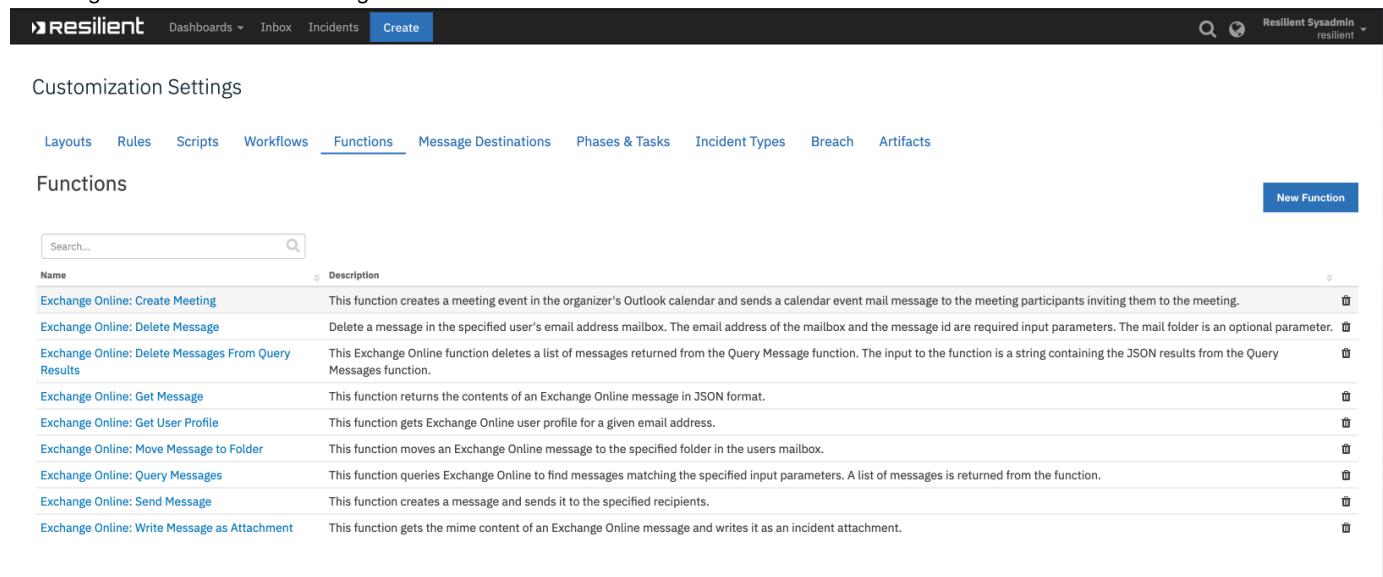
Microsoft Exchange Online Functions for IBM Resilient provides the capability to access and manipulate Microsoft Exchange Online messages from the IBM Resilient SOAR Platform. The integration uses Microsoft Graph API to access the data in Microsoft 365. Included in the integration are the following capabilities:

- 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:



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 Results 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

This app supports the IBM Resilient SOAR Platform and the IBM Cloud Pak for Security.

Resilient platform

The Resilient platform supports two app deployment mechanisms, App Host and integration server.

If deploying to a Resilient platform with an App Host, the requirements are:

- Resilient platform >= [37.1](#).
- The app is in a container-based format (available from the AppExchange as a [zip](#) file).

If deploying to a Resilient platform with an integration server, the requirements are:

- 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

The following Resilient platform guides provide additional information:

- *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *Integration Server Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *System Administrator Guide*: provides the procedure to install, configure and deploy apps.

The above guides are available on the IBM Knowledge Center at [ibm.biz/resilient-docs](#). On this web page, select your Resilient platform version. On the follow-on page, you can find the *App Host Deployment Guide* or *Integration Server Guide* by expanding **Resilient Apps** in the Table of Contents pane. The System Administrator Guide is available by expanding **System Administrator**.

Cloud Pak for Security

If you are deploying to IBM Cloud Pak for Security, the requirements are:

- IBM Cloud Pak for Security >= 1.4.
- Cloud Pak is configured with an App Host.
- The app is in a container-based format (available from the AppExchange as a [zip](#) file).

The following Cloud Pak guides provide additional information:

- *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings. From the Table of Contents, select Case Management and Orchestration & Automation > **Orchestration and Automation Apps**.
- *System Administrator Guide*: provides information to install, configure, and deploy apps. From the IBM Cloud Pak for Security Knowledge Center table of contents, select Case Management and Orchestration & Automation > **System administrator**.

These guides are available on the IBM Knowledge Center at [ibm.biz/cp4s-docs](#). From this web page, select your IBM Cloud Pak for Security version. From the version-specific Knowledge Center page, select Case Management and Orchestration & Automation.

Proxy Server

The app supports a proxy server.

-
- 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

Install

- To install or uninstall an App or Integration on the *Resilient platform*, see the documentation at [ibm.biz/resilient-docs](#).
- To install or uninstall an App on *IBM Cloud Pak for Security*, see the documentation at [ibm.biz/cp4s-docs](#) and follow the instructions above to navigate to Orchestration and Automation.

App Configuration

The following table describes the settings you need to configure in the app.config file. If using App Host, see the Resilient System Administrator Guide. If using the integration server, see the Integration Server Guide.

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
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

Config	Required	Example	Description
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

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.

Tasks Details Breach Notes Members News Feed Attachments Stats Timeline Artifacts Email Exchange Online

Edit

Exchange Online Message Query Results

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 left sidebar is titled 'Microsoft Azure' and includes sections for Home, securitypocdemos - App registrations, Overview, Getting started, Diagnose and solve problems, Manage (Users, Groups, Organizational relationships, Roles and administrators, Enterprise applications, Devices), App registrations (selected), Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, and Company branding. The main content area is titled 'securitypocdemos - App registrations' under 'Azure Active Directory'. It features a search bar and navigation links for Endpoints, Troubleshooting, App registrations (Legacy), and Got feedback? Below these are tabs for All applications (selected) and Owned applications, with a search bar for filtering results. A table lists two applications: 'My Python App' (client ID: redacted, created 7/3/2019, certificates & secrets current) and 'resilient-integration' (client ID: redacted, created 7/2/2019, certificates & secrets current). A red arrow points to the '+ New registration' button at the top of the page.

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

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

✓

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 [\[link\]](#)

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:

resilient-integration

Search (Cmd+)

Delete Endpoints

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

Display name : resilient-integration	Supported account types : My organization only
Application (client) ID : [REDACTED]	Redirect URLs : Add a Redirect URI
Directory (tenant) ID : [REDACTED]	Application ID URI : api://[REDACTED]
Object ID : [REDACTED]	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

Microsoft identity platform
Authentication scenarios
Authentication libraries
Code samples
Microsoft Graph
Glossary
[Help and Support](#)

Documentation

Overview

Quickstart

Manage

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

Support + Troubleshooting

Troubleshooting

New support request

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

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.

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".

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](#)

API / Permissions name	Type	Description	Admin Consent Requir...	Status
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:

The screenshot shows the Microsoft Azure portal interface. On the left, a sidebar menu includes options like Overview, Quickstart, Manage, API permissions (which is currently selected), Expose an API, Owners, Roles and administrators, and Manifest. The main content area is titled "resilient-integration - API permissions". It shows a list of "Configured permissions" for the Microsoft Graph API, including Calendars.ReadWrite, Mail.ReadWrite, Mail.Send, MailboxSettings.Read, and User.Read.All. To the right, a "Request API permissions" section lists "Commonly used Microsoft APIs". A red arrow points to the "Microsoft Graph" entry, which is highlighted with a blue border. Below it, other APIs listed include Azure Rights Management Services, Azure Service Management, Data Export Service for Microsoft Dynamics 365, Dynamics 365 Business Central, Dynamics CRM, Flow Service, Intune, Office 365 Management APIs, OneNote, Power BI Service, SharePoint, and Skype for Business.

Select Application permissions (not Delegated permissions):

This screenshot shows the same Microsoft Azure portal interface as the previous one, but with a different focus. The "Request API permissions" section is now visible, showing a list of APIs under "All APIs". The "Microsoft Graph" API is selected, indicated by a blue border around its icon and name. A red arrow points to the "Application permissions" section, which is highlighted with a blue border. This section contains the text: "Your application runs as a background service or daemon without a signed-in user." Below this, there is a table comparing "Delegated permissions" (which your application needs to access the API as the signed-in user) and "Application permissions" (which 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

The screenshot shows the 'Request API permissions' section of the Microsoft Azure portal. It lists several permissions under 'MailboxSettings (1)', 'Mail (2)', and 'Mail.Send'. Three specific permissions are highlighted with red arrows:

- MailboxSettings.Read**: Read all user mailbox settings. Status: Yes.
- Mail.ReadWrite**: Read and write all user mailbox settings. Status: Yes.
- Mail.Send**: Send mail as any user. Status: Yes.

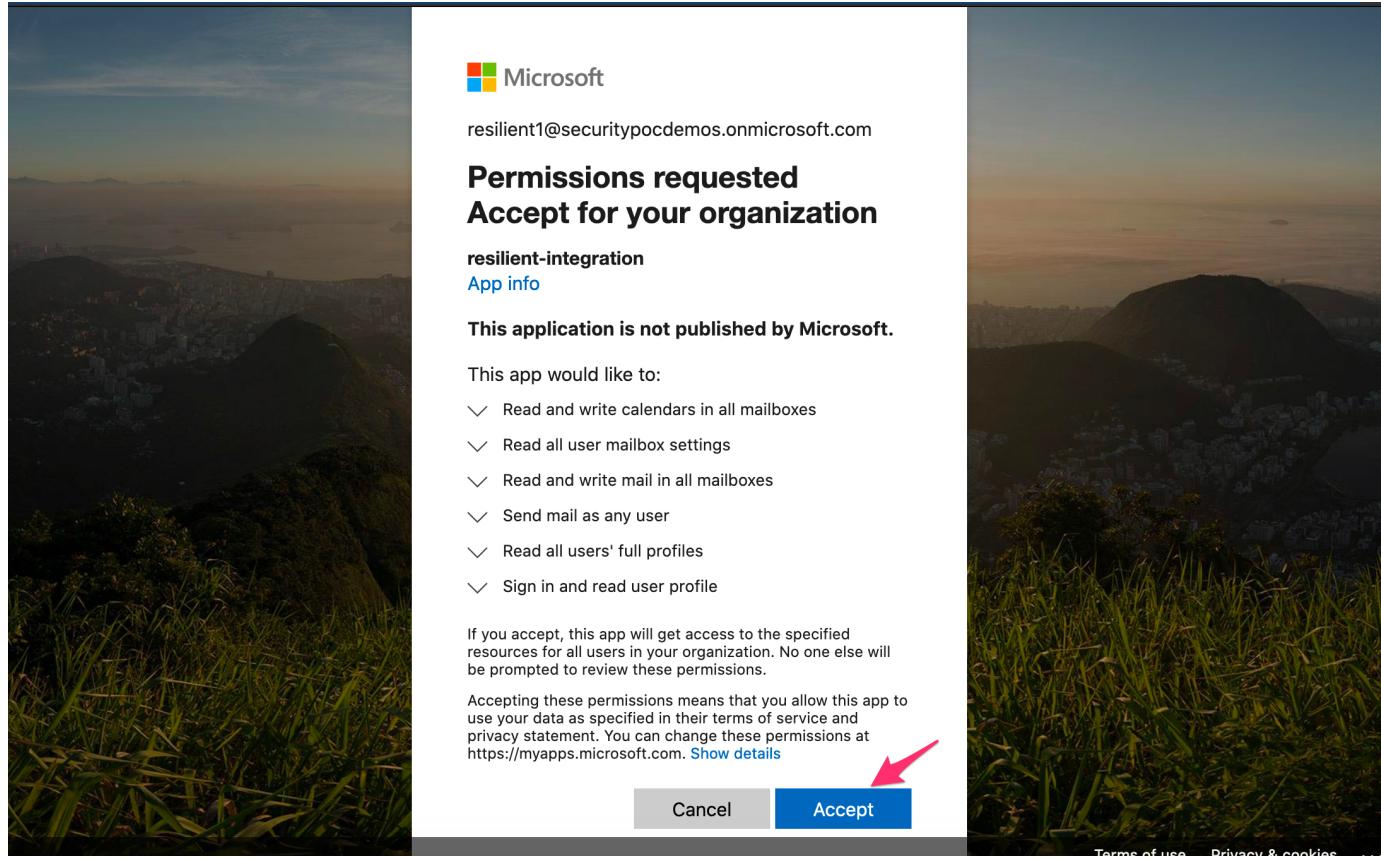
At the bottom, there are 'Add permissions' and 'Discard' buttons.

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

The screenshot shows the 'Configured permissions' section of the Microsoft Azure portal. It lists the same set of permissions as the previous screen, but now all have green checkmarks in the 'Admin Consent Req...' column, indicating they are granted. A large red arrow points to the 'Grant admin consent for securitypocdemos' button at the top right of the table.

API / Permissions name	Type	Description	Admin Consent Req...	Status
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 & Support

Refer to the documentation listed in the Requirements section for troubleshooting information.

For Support

This is an IBM supported app. Please search <https://ibm.com/mysupport> for assistance.