

 README.md

Microsoft Exchange Online Functions for IBM Resilient

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

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 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:

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 >= 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" 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

- 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
<code>microsoft_graph_token_url</code>	Yes	<code>https://login.microsoftonline.com/{tenant}/oauth2/v2.0/token</code>	<i>Microsoft Graph URL endpoint for acquiring access token</i>
<code>microsoft_graph_url</code>	Yes	<code>https://graph.microsoft.com/v1.0</code>	*Microsoft Graph base URL *
<code>tenant_id</code>	Yes	xxx	<i>Microsoft Azure Tenant ID</i>
<code>client_id</code>	Yes	xxx	<i>Microsoft Azure Client ID (Application ID)</i>
<code>client_secret</code>	Yes	xxx	<i>Microsoft Azure Client Secret</i>

Config	Required	Example	Description
max_messages	Yes	100	<i>Maximum number of messages that a query will return</i>
max_users	Yes	2000	<i>Maximum number of users searched in a query</i>

- 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 screenshot shows the Resilient platform's customization settings interface. On the left, there's a sidebar with various tabs like 'New Incident Wizard', 'Incident Tabs', and 'Exchange Online'. The main area displays an 'Incident: Exchange Online' page with a 'Save' button. To the right, there are sections for 'Fields', 'Data Tables', and 'Views'. A red arrow points to the 'Exchange Online Message Query Results' table under 'Data Tables'.

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

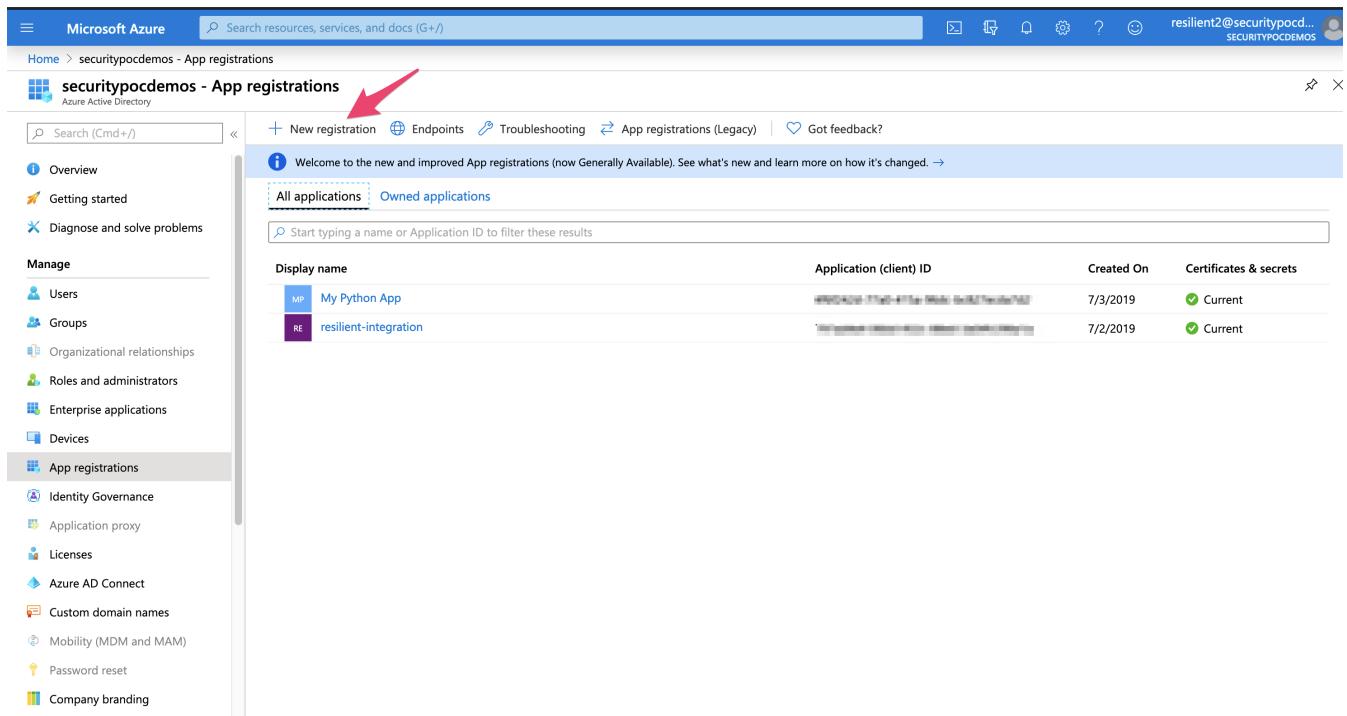
This screenshot shows the 'Exchange Online' tab selected on the incident page. It features a table titled 'Exchange Online Message Query Results' with columns for 'Query Date', 'Received Date', 'Queried Email Address', 'Sender Email', 'Message Subject', 'Has Attachments', 'Web Link', 'Status', and 'Message ID'. A red arrow points to this table. Below the table, it says '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.

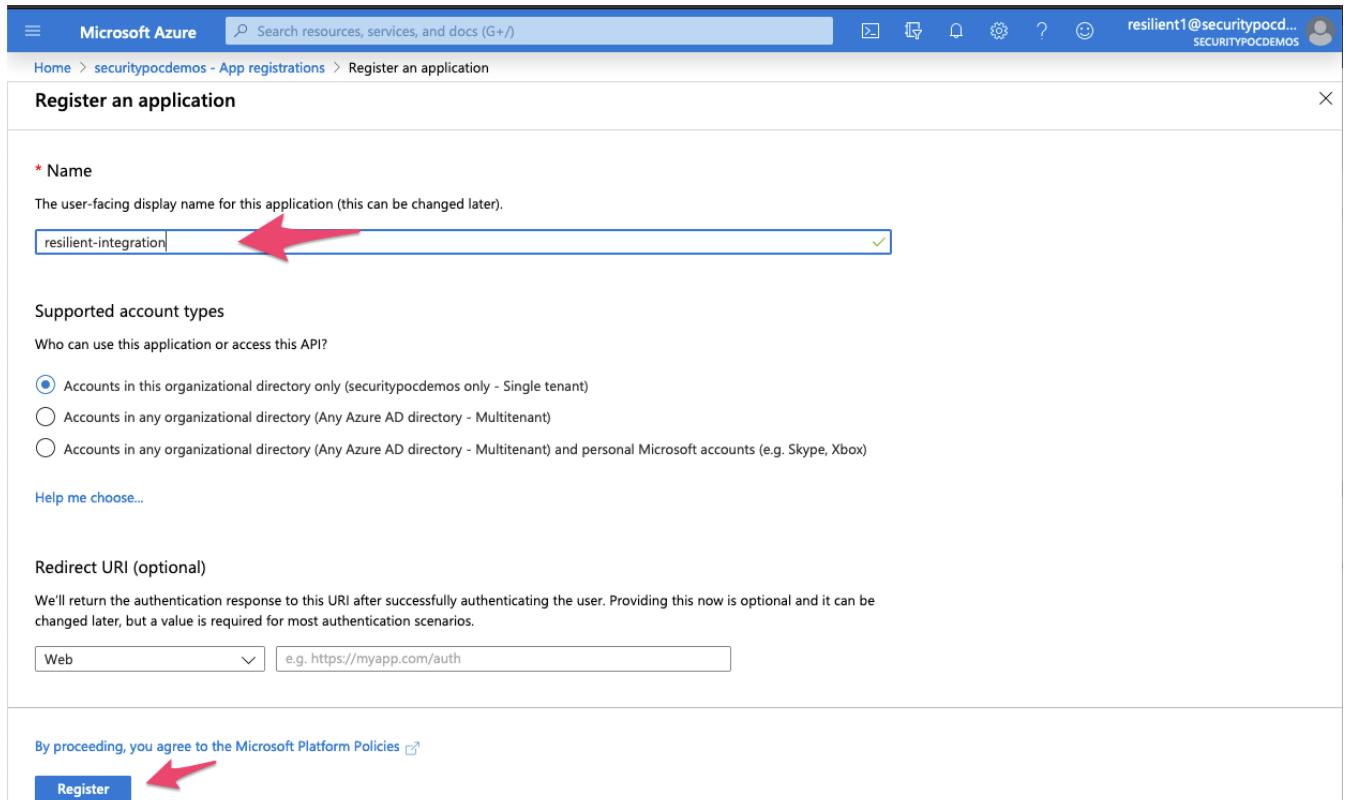
App Registration

To register the Resilient integration 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.



The screenshot shows the Microsoft Azure portal's App registrations page. The left sidebar is open, showing various Azure services like Users, Groups, and App registrations. The 'App registrations' option is selected. The main area shows a table of existing applications, with one named 'My Python App' and another named 'resilient-integration'. At the top of the main area, there is a blue bar with the text 'Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed.' Below this, there are tabs for 'All applications' and 'Owned applications', with 'All applications' selected. A search bar allows filtering by application ID. A red arrow points to the '+ New registration' button at the top left of the main content area.

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



The screenshot shows the 'Register an application' form. The 'Name' field is filled with 'resilient-integration' and has a red arrow pointing to it. Below the name field, there is a section for 'Supported account types' with three radio button options: 'Accounts in this organizational directory only (securitypocdemos only - Single tenant)' (which is selected), 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)', and 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)'. There is also a 'Help me choose...' link. The 'Redirect URI (optional)' section is present with a note about returning the authentication response and a dropdown menu set to 'Web' with a corresponding input field. At the bottom, there is a link 'By proceeding, you agree to the Microsoft Platform Policies' and a large blue 'Register' button with a red arrow pointing to it.

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

Home > securitypocdemos - App registrations > resilient-integration

resilient-integration

Search (Cmd+ /)

Delete Endpoints

Overview

Quickstart

Manage

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

Support + Troubleshooting

- Troubleshooting
- New support request

Display name : **resilient-integration**

Application (client) ID : **[REDACTED]**

Directory (tenant) ID : **[REDACTED]**

Object ID : **[REDACTED]**

Supported account types : **My organization only**

Redirect URIs : **Add a Redirect URI**

Application ID URI : **api://[REDACTED]**

Managed application in ... : **resilient-integration**

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

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

Call APIs

Documentation

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

View API permissions

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

Microsoft Azure

Home > resilient-integration - Certificates & secrets

resilient-integration - Certificates & secrets

Search (Cmd+ /)

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".

The screenshot shows the Microsoft Azure portal interface. In the left sidebar under the 'Manage' section, the 'API permissions' link is highlighted with a red arrow. In the main content area, there is a table titled 'Configured permissions' showing five permissions for 'Microsoft Graph'. At the top right of this table, there is a button labeled '+ Add a permission' with a red arrow pointing to it. The top right corner of the screen shows the user's email address: 'resilient1@securitypocd... SECURITYPOCDEMOS'.

Click on Microsoft Graph:

The screenshot shows the 'Request API permissions' page for Microsoft Graph. The left sidebar shows the 'API permissions' link is selected. The main content area has a heading 'Request API permissions' and a sub-section 'Select an API' with tabs for 'Microsoft APIs', 'APIs my organization uses', and 'My APIs'. Below this, there is a section titled 'Commonly used Microsoft APIs' with several cards. One card for 'Microsoft Graph' is highlighted with a red arrow. Other cards 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'. The top right corner shows the user's email address: 'resilient1@securitypocd... SECURITYPOCDEMOS'.

Select Application permissions (not Delegated permissions):

The screenshot shows the Microsoft Azure portal with the URL https://portal.azure.com/#blade/Microsoft_Azure门户/ResourceManagementBlade/resourceType=Microsoft%2fGraph%2fpermissions. The left sidebar shows the 'resilient-integration - API permissions' blade. The main area displays 'Configured permissions' for Microsoft Graph, listing several application permissions like 'Calendars.ReadWrite', 'Mail.ReadWrite', etc. To the right, a 'Request API permissions' dialog is open. It has two sections: 'Delegated permissions' (disabled) and 'Application permissions' (selected). A red arrow points from the 'Application permissions' section to the 'Grant admin consent' button at the bottom of the dialog.

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 Microsoft Azure portal with the URL https://portal.azure.com/#blade/Microsoft_Azure门户/ResourceManagementBlade/resourceType=Microsoft%2fGraph%2fpermissions. The left sidebar shows the 'resilient-integration - API permissions' blade. The main area displays 'Configured permissions' for Microsoft Graph, listing several application permissions. To the right, a 'Request API permissions' dialog is open. Under the 'MailboxSettings' section, the 'MailboxSettings.Read' checkbox is checked. Under the 'Mail' section, the 'Mail.ReadWrite' and 'Mail.Send' checkboxes are checked. Red arrows point to these three checked checkboxes. At the bottom of the dialog, there are 'Add permissions' and 'Discard' buttons.

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

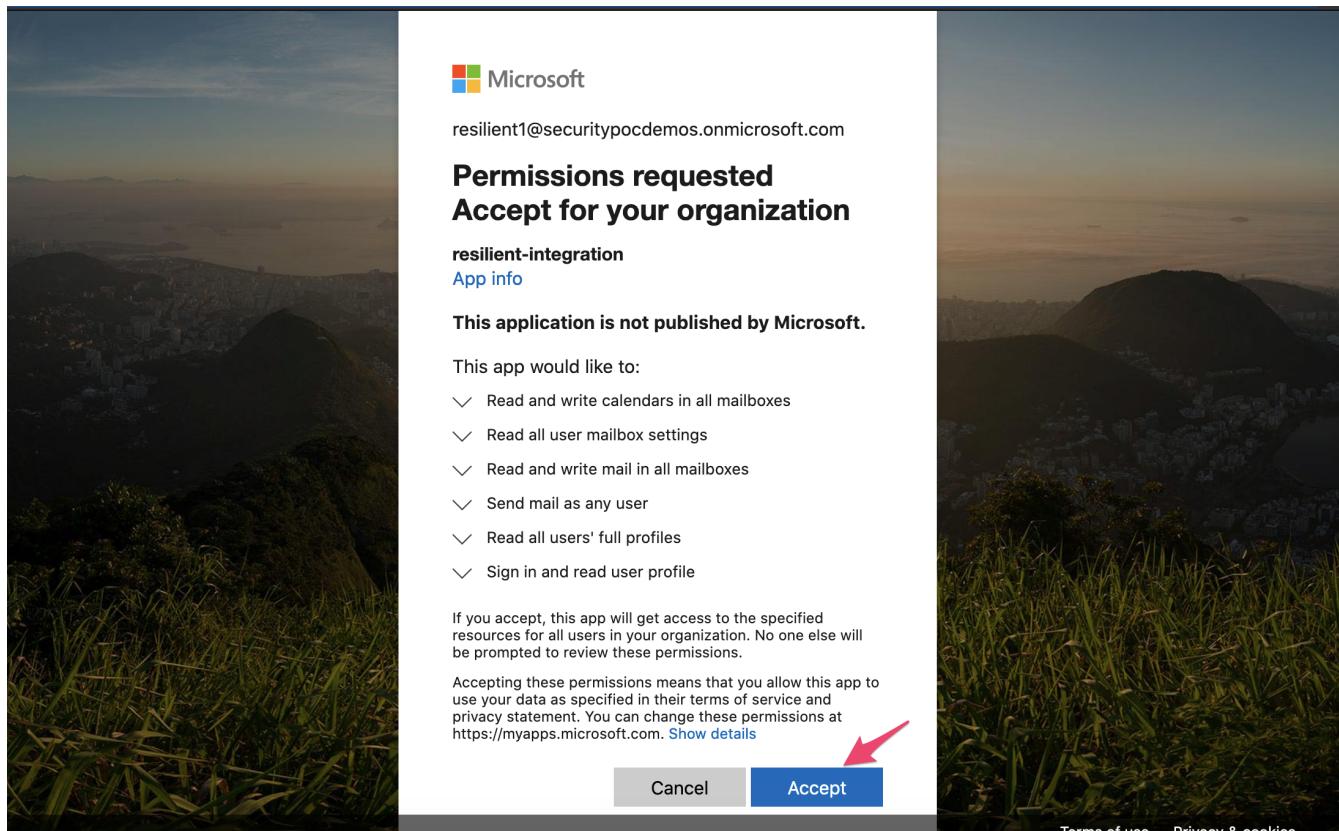
resilient-integration - API permissions

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 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:



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