IBM Resilient

Incident Response Platform Integrations

Microsoft Exchange Function V1.0.1

Release Date: November 2020

Version	Publication	Notes
1.0.1	December 2020	Added App Host support, Added proxy support.
1.0.0	August 2018	Initial publication.

Resilient Functions simplify development of integrations by wrapping each activity into an individual workflow component. These components can be easily installed, then used and combined in Resilient workflows. The Resilient platform sends data to the function component that performs an activity then returns the results to the workflow. The results can be acted upon by scripts, rules, and workflow decision points to dynamically orchestrate the security incident response activities.

This guide describes the Microsoft Exchange Function.

Overview

This Resilient Function package provides seven functions that work with Microsoft Exchange:

1) Exchange Create Meeting – Creates a meeting in Microsoft Exchange and send out invites
2) Exchange Delete Emails – Deletes queried emails from a user's mailbox
3) Exchange Find Emails – Queries emails from a user's mailbox
4) Exchange Get Mailbox Info – Gets mailbox info for a sender
5) Exchange Move Folder Contents and Delete Folder – Moves the contents of one folder to another folder and deletes the original
6) Exchange Move Emails – Moves queried emails from one folder to another folder
7) Exchange Send Email – Sends email to a list of recipients

The package also includes corresponding menu item rules and workflows that create Notes and Artifacts from the function results.

Installation

Requirements

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 >= 31.0.4035.
- The app is in the older integration format (available from the AppExchange as a `zip` file which contains a `tar.gz` file).
- Integration server is running `resilient_circuits>=30.0.0`.
- If using an API key account, make sure the account provides the following minimum permissions:

Name	Permission
Org Data	Read, Edit

If 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.Integration server is running `resilient_circuits>=30.0.0`.
- The app is in a container-based format (available from the AppExchange as a zip file).

Installation

The Resilient platform and Cloud Pak guides providing installation, configuration, and troubleshooting information are available on the Knowledge Center.

Configuration

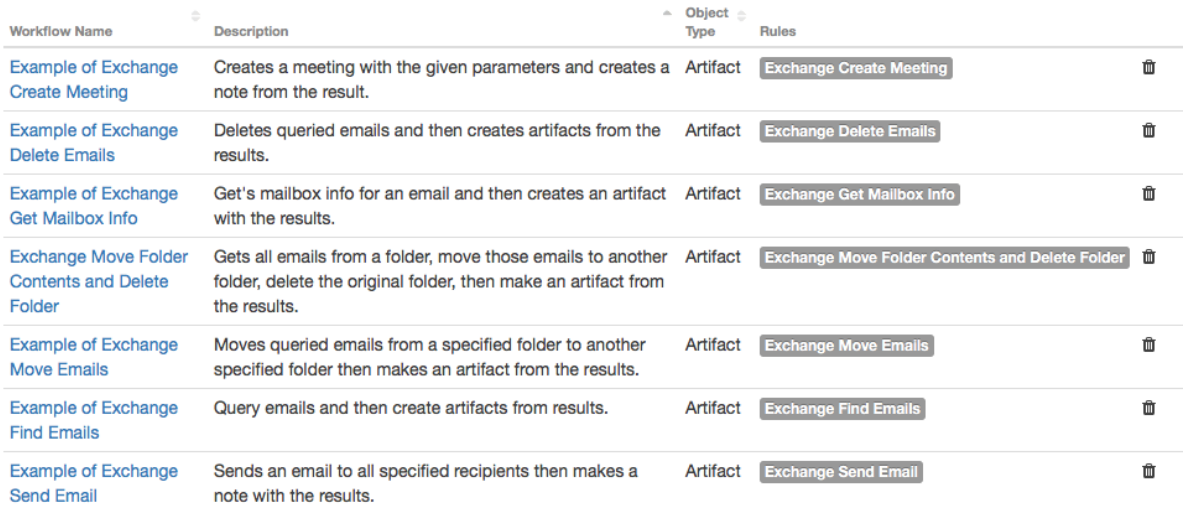
After installing the app or package, a new section, *fn_exchange*, is created in the app.config file. You need to edit the following settings in that section. If using App Host, see the Resilient System Administrator Guide on the Knowledge Center. If using the integration server, see the Integration Server Guide.

Complete the following steps to configure and run the integration:

```
[fn_exchange]
verify_cert=[True|False]
server=example.com
username=domain\\username  - to use this package, this must be an admin account
with mailbox access to other accounts
email=admin@example.com - this is the default account to send emails and create
meetings if one was not specified. Specifying an account that is not this one
will require impersonation access.
password=password
default_folder_path=Some folder path after root i.e. Top of Information
Store/Inbox. Multiple folderpaths must be separated by commas.
# Uncomment to specify proxy settings
```

```
#https_proxy=https://your.proxy.com
#http_proxy=http://your.proxy.com
```

Once the function package deploys the function(s), you can view them in the Resilient platform Functions tab, as shown below.



Workflow Name	Description	Object Type	Rules
Example of Exchange Create Meeting	Creates a meeting with the given parameters and creates a note from the result.	Artifact	Exchange Create Meeting
Example of Exchange Delete Emails	Deletes queried emails and then creates artifacts from the results.	Artifact	Exchange Delete Emails
Example of Exchange Get Mailbox Info	Get's mailbox info for an email and then creates an artifact with the results.	Artifact	Exchange Get Mailbox Info
Exchange Move Folder Contents and Delete Folder	Gets all emails from a folder, move those emails to another folder, delete the original folder, then make an artifact from the results.	Artifact	Exchange Move Folder Contents and Delete Folder
Example of Exchange Move Emails	Moves queried emails from a specified folder to another specified folder then makes an artifact from the results.	Artifact	Exchange Move Emails
Example of Exchange Find Emails	Query emails and then create artifacts from results.	Artifact	Exchange Find Emails
Example of Exchange Send Email	Sends an email to all specified recipients then makes a note with the results.	Artifact	Exchange Send Email

The package includes example workflows and rules that show how you can use the functions, as shown in the following table. Resilient users can view the rules in the Rules tab and the workflows in the Workflows tab, and modify them as needed. The object type for the workflows is Artifact. The provided sample workflows create notes and artifacts from the function results.

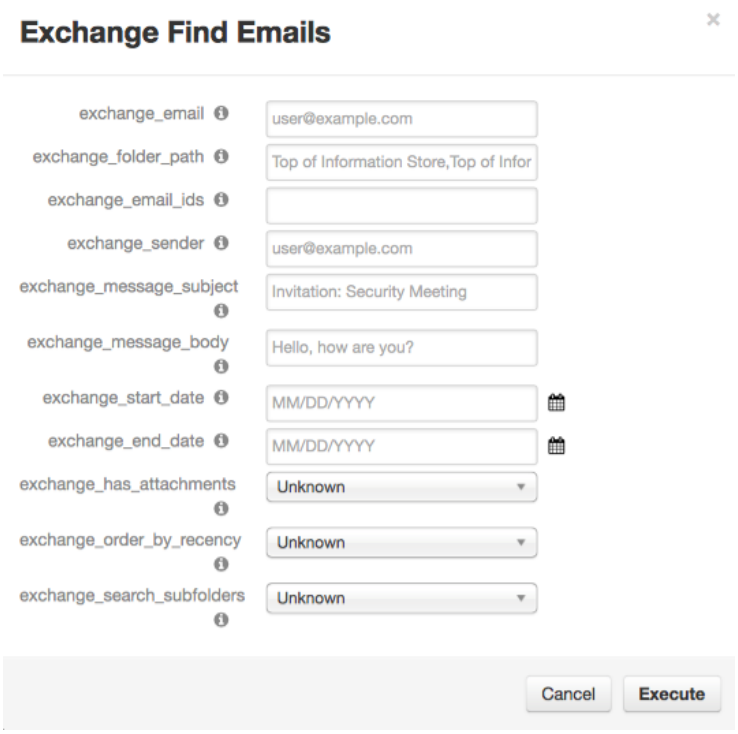
Function	Rule	Workflow
exchange_create_meeting	Exchange Create Meeting	Example of Exchange Create Meeting
exchange_delete_emails	Exchange Delete Emails	Example of Exchange Delete Emails
exchange_find_emails	Exchange Find Emails	Example of Exchange Find Emails
exchange_get_mailbox_info	Exchange Get Mailbox Info	Example of Exchange Get Mailbox Info
exchange_move_emails	Exchange Move Emails	Example of Exchange Move Emails
exchange_move_folder_contents_and_delete_folder	Exchange Move Folder Contents and Delete Folder	Example of Exchange Move Folder Contents and Delete Folder
exchange_send_email	Exchange Send Email	Example of Exchange Send Email

Inputs

Each function has a set of inputs, which you can view by clicking the function name in the Functions tab of the Resilient platform.

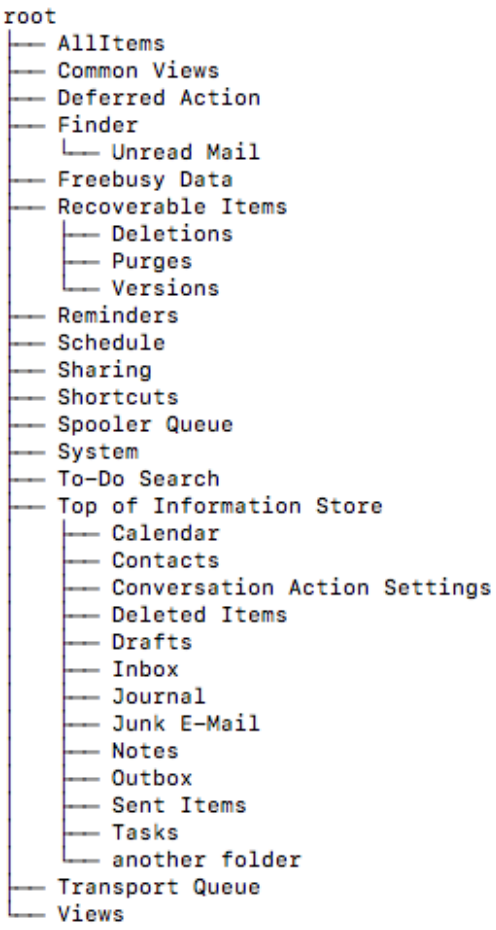
The Resilient functions use input parameters starting with `exchange_`, examples include `exchange_email`, `exchange_subject` and `exchange_body`

The function inputs can also be set by the user when clicking a menu item. For example:



The example preprocessing script uses the inputs from the popup menu when executing a function, if no fields are provided, then it uses the value from the workflow input/artifact.

The `exchange_folder_path` or `exchange_destination_folder_path` fields may be difficult to configure and are dependent on the Exchange environment. Upon entering an invalid folder path, a tree structure of the folder hierarchy will be printed. Here is an example:



Example folder paths given this folder structure could be any path following the root path:

```
-    Top of Information Store/Inbox
-    Top of Information Store/Deleted Items
-    Finder/Unread Mail
-    Finder
```

Additionally, if the `exchange_search_subfolders` path is set to `true`, every folder in its branch will be included in the query. For example if the specified folder is `Recoverable Items`, then the searched folders would be:

```
-   Recoverable Items
-   Recoverable Items/Deletions
-   Recoverable Items/Purges
-   Recoverable Items/Versions
```

To search folder paths, the specified account in config file must have access to the searched folders.

Folders that contain `/` or `,` must be wrapped in quotes.

```
-   Example/”One/With/Quotes”/Folder
-   Example/”One, with, commas”/Folder
-   Example/”One/with, both”/Folder
```

Multiple folder paths can be specified by separating them with commas and following the above rules.

For more information on specific function inputs, check the tooltips.

The Resilient functions use input parameters starting with Resilient Platform Configuration

The configuration file must specify credentials that have access to mailboxes that are being queried otherwise the functions can only query the account that is specified.

The package only currently supports on-premise Exchange servers. Functionality for Ofifce365 is not guaranteed.

Knowledge Center

App Host or integration server

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.

These guides are available on the IBM Knowledge Center at Knowledge Center. 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

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. 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.

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

For additional support, contact support@resilientsystems.com.

Including relevant information from the log files will help us resolve your issue.