

 README.md

# User Guide: Microsoft Exchange Online Functions for IBM Resilient v1.0.0

## Table of Contents

- [Key Features](#)
- [Function - Exchange Online: Create Meeting](#)
- [Function - Exchange Online: Delete Message](#)
- [Function - Exchange Online: Delete Messages From Query Results](#)
- [Function - Exchange Online: Get Message](#)
- [Function - Exchange Online: Get User Profile](#)
- [Function - Exchange Online: Move Message to Folder](#)
- [Function - Exchange Online: Query Messages](#)
- [Function - Exchange Online: Send Message](#)
- [Function - Exchange Online: Write Message as Attachment](#)
- [Data Table - Exchange Online Message Query Results](#)
- [Rules](#)

## Key Features

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.

## Integration Flow for Phishing Investigation Use Case

---

The Exchange Online integration primary use case is to monitor and control email activities in Exchange Online (Office 365 Outlook in the cloud) and protect against inbound malicious emails.

To use the integration, run the Query Messages rule from the Action menu of an incident. From the rule, you can search a single email address, a list of email addresses or the entire tenant. Results of the query are returned in the Exchange Online Message Query Results data table on the Exchange Online incident tab. Each row in the data table contains information from one message and the following actions can be performed on each message when its state is Active in the Status column:

- Create artifacts: Email Recipient, Email Sender, Email Subject.
- Delete the message.
- Move the message to a Well-known folder.
- Write the message .eml as an incident.
- Write the message JSON returned from MS Graph to an incident note.

The data table Status column is set to Active when the message is entered in the table. Any time after that, a user can delete the message; however, this could update the Status field to Not Found or Deleted if the message is deleted when running one of the above data table rules or workflows.

The first column of the data table displays the time the query occurred. You can use this value to sort through data if multiple queries are run and entered into the data table. You may want to empty the data table after each query.

Because a large number of messages can be returned from a query, the integration has following parameters in the app.config to limit the number of messages returned:

- max\_messages
- max\_users

Considering using these parameters to improve performance when running queries.

You can perform additional investigation, including using other email analysis scripts and integrations, on messages after writing the message to a note or attachment.

Once you complete the investigation of the messages and there are problematic messages that you want to delete, use the Example: Exchange Online Delete Messages for Query Results rule from the incident's Actions menu. The rule starts a workflow that performs a query of messages and sends the matching results to a function that deletes a list of messages. The results are written to the Exchange Online Message Query Results data table with a Status column of "Deleted" in red. An incident note is also written that indicates the number of messages deleted.

Use this rule with caution as you can delete many user messages.

At anytime the user can send a message or schedule a meeting using the Exchange Online: Send Message and Exchange Online: Create meeting rules and workflows.

## Function - Exchange Online: Create Meeting

---

Exchange Online: Create Meeting function requires the following Microsoft Graph API Application permissions:

- Calendars.ReadWrite
- MailboxSettings.Read

The Exchange Online: Create Meeting function creates a meeting event in the organizer's Outlook calendar and sends a calendar event invitation message to the meeting participants.

The meeting start and end times are set in the time zone of the meeting organizer's Outlook mailbox preferred time zone setting. If no mailbox time zone setting is set, the meeting time is calculated using UTC time zone.

The screenshot shows the Resilient platform's 'Customization Settings' page for a function named 'exchange\_online\_create\_meeting'. The top navigation bar includes 'Dashboards', 'Inbox', 'Incidents', 'Create', and a search bar. The current page is 'Functions' under 'exchange\_online\_create\_meeting'. The right side of the screen displays metadata: Creator (Resilient Sysadmin), Last Modified (01/21/2020 10:21), Last Modified By (Resilient Sysadmin), and Associated Workflows (Example: Exchange Online Create Meeting). Below the metadata, there are two sections: 'Inputs' and 'Input Fields'.

**Inputs:**

Name	Type	Required	Example	Tooltip
exo_meeting_email_address	text	Yes	meeting message body	Meeting message body
exo_meeting_start_time	text	Yes	user@example.com	Email address of meeting coordinator
exo_meeting_end_time	datetimepicker	Yes	-	End date and time for meeting
exo_meeting_location	text	No	-	-
exo_meeting_optional_attendees	text	No	user1@example.com, user2@example.com	Comma separated list of optional attendee email addresses
exo_meeting_required_attendees	text	No	user1@example.com, user2@example.com	Comma separated list of required attendee email addresses
exo_meeting_start_time	datetimepicker	Yes	-	Meeting start date and time
exo_meeting_subject	text	Yes	-	Meeting Subject

**Input Fields:**

Field
exo_attachment_name
exo_destination_mailfolder_id
exo_email_address
exo_email_address_sender
exo_end_date
exo_has_attachments
exo_mail_folders
exo_mailfolders_id

#### ▼ Inputs:

Name	Type	Required	Example	Tooltip
exo_meeting_body	text	Yes	meeting message body	Meeting message body
exo_meeting_email_address	text	Yes	user@example.com	Email address of meeting coordinator
exo_meeting_end_time	datetimepicker	Yes	-	End date and time for meeting
exo_meeting_location	text	No	-	-
exo_meeting_optional_attendees	text	No	user1@example.com, user2@example.com	Comma separated list of optional attendee email addresses
exo_meeting_required_attendees	text	No	user1@example.com, user2@example.com	Comma separated list of required attendee email addresses
exo_meeting_start_time	datetimepicker	Yes	-	Meeting start date and time
exo_meeting_subject	text	Yes	-	Meeting Subject

#### ▼ Outputs:

```
results = {
```

```
'inputs': {
    u'exo_meeting_end_time': 1581022800000,
    u'exo_meeting_optional_attendees': None,
    u'exo_meeting_subject': u'phishing meeting',
    u'exo_meeting_body': u'<div class="rte"><div>We need to talk about this!</div></div>', u'exo_meeting_require
    u'exo_meeting_start_time': 1581004800000,
    u'exo_meeting_email_address': u'reslient2@securitypocdemos.onmicrosoft.com', u'exo_meeting_location': None}
'metrics': {'package': 'fn-exchange-online',
    'timestamp': '2020-02-04 13:30:45',
    'package_version': '1.0.0',
    'host': 'MacBook-Pro.local',
    'version': '1.0',
    'execution_time_ms': 1728},
'success': True,
'content': {u'body': {u'content': u'', u'contentType': u'html'}, u'sensitivity': u'normal', u'locations': []},
'reason': None,
'version': '1.0',
'pretty_string': u'{\n    "body": {\n        "content": "",\n        "contentType": "html"\n    },\n    "sensitivity": "normal",\n    "locations": []\n}'}]
```

#### ▼ Workflows:

The Example: Exchange Online Create Meeting workflow calls the create meeting function and then write the results to an incident note.

Customization Settings

Workflows / Example: Exchange Online Create Meeting

Name *	Example: Exchange Online Create Meeting	Creator	Resilient Sysadmin
API Name *	example_exchange_online_create_meeting	Last Modified	01/28/2020 13:59
Description	This workflow will create a meeting event in the meeting organizer's calendar and send email to the required and optional attendees informing them of the event. An incident note is added containing the status of creating the meeting.	Last Modified By	Resilient Sysadmin
Object Type *	Incident	Associated Rules	Example: Exchange Online Create Meeting

Start your workflow here → Exchange Online: Create Meeting → End

email, meeting: start and date and time, location, message, subject and body, required and optional attendee email list

Incident note added indicating the results of creating the meeting.

#### ▼ Example Pre-Process Script:

```
inputs.exo_meeting_email_address = inputs.exo_meeting_email_address if rule.properties.exo_meeting_email_address is N
inputs.exo_meeting_start_time = inputs.exo_meeting_start_time if rule.properties.exo_meeting_start_time is None else r
inputs.exo_meeting_end_time = inputs.exo_meeting_end_time if rule.properties.exo_meeting_end_time is None else rule.pr
inputs.exo_meeting_subject = inputs.exo_meeting_subject if rule.properties.exo_meeting_subject is None else rule.prope
inputs.exo_meeting_body = inputs.exo_meeting_body if rule.properties.exo_meeting_body.content is None else rule.proper
inputs.exo_meeting_required_attendees = inputs.exo_meeting_required_attendees if rule.properties.exo_meeting_required_
```

```
inputs.exo_meeting_optional_attendees = inputs.exo_meeting_optional_attendees if rule.properties.exo_meeting_optional_
inputs.exo_meeting_location = inputs.exo_meeting_location if rule.properties.exo_meeting_location is None else rule.pr
```

▼ Example Post-Process Script:

```
if results.success:
    noteText = u"Exchange Online created meeting\n  From: {0}\n{1}".format(results.inputs["exo_meeting_email_address"],
else:
    noteText = u"Exchange Online meeting was NOT created\n  From: {0}\n{1}".format(results.inputs["exo_meeting_email_ad
incident.addNote(noteText)
```

▼ Example Rule:

The following Example: Exchange Online Create Meeting incident menu item rule is included to create a meeting via Exchange Online:

Customization Settings

Rules / Example: Exchange Online Create Meeting

Display Name \* Example: Exchange Online Create M

Object Type Incident

Conditions Add conditions in which to invoke the rule. [Add New](#)

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include: *Add Tasks, Run Script, and Set Field.* [Add New](#)

Workflows Workflow Activities are started after all Ordered Activities complete.

Destinations Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

[Show Activity Fields](#)

© Copyright IBM Corporation 2020

When the Example: Exchange Online Create Meeting rule is activated the following rule activity popup dialog appears prompting for input for creating the meeting and sending a message to the invitees:

## Example: Exchange Online Create Meeting

The screenshot shows the 'Create Meeting' dialog box for Exchange Online. It includes fields for Meeting Organizer Email Address (user@example.com), Meeting Start Time and End Time (both set to MM/DD/YYYY HH:mm:ss Z), Meeting Subject (empty), and a rich text editor toolbar. Below the toolbar is a large empty text area. At the bottom, there are fields for Meeting Location (empty), Required Attendees (user1@example.com, user2@example.com), and Optional Attendees (user1@example.com, user2@example.com). A footer bar at the bottom right contains 'Cancel' and 'Execute' buttons.

Meeting Organizer Email Address \*

user@example.com

Meeting Start Time \*

MM/DD/YYYY HH:mm:ss Z

Meeting End Time \*

MM/DD/YYYY HH:mm:ss Z

Meeting Subject \*

Meeting Body \*

Sans Serif ▾ Normal ▾ B I U S E E

≡ A A 🔗 🖼 W ▾

Meeting Location

Required Attendees

user1@example.com, user2@example.com

Optional Attendees

user1@example.com, user2@example.com

Cancel Execute

### Function - Exchange Online: Delete Message

Exchange Online: Delete Message function requires the following Microsoft Graph API Application permission:

- Mail.ReadWrite

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.

The screenshot shows the Resilient platform's 'Customization Settings' interface for a function named 'exchange\_online\_delete\_email'. The top navigation bar includes links for Dashboards, Inbox, Incidents, Create, and a search bar. The main content area shows the function details:

- Name \***: Exchange Online: Delete Message
- API Name \***: exchange\_online\_delete\_email
- Message Destination \***: fn\_exchange\_online
- Description**: 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.

**Inputs** section (left):
 

- exo\_email\_address
- exo\_mailfolders\_id
- exo\_messages\_id

**Input Fields** section (right):
 

- exo\_attachment\_name
- exo\_destination\_mailfolder\_id
- exo\_email\_address
- exo\_email\_address\_sender
- exo\_end\_date
- exo\_has\_attachments
- exo\_mail\_folders
- exo\_mailfolders\_id
- exo\_meeting\_body

**Associated Workflows** section (top right):
 

- Creator: Resilient Sysadmin
- Last Modified: 01/02/2020 16:22
- Last Modified By: Resilient Sysadmin
- Example: Exchange Online Delete Message

#### ▼ Inputs:

Name	Type	Required	Example	Tooltip
exo_email_address	text	Yes	user@example.com	Get information on this user email account
exo_mailfolders_id	text	No	inbox	MailFolders ID
exo_messages_id	text	Yes	-	The message ID of the message to be deleted

#### ▼ Outputs:

```

results = {
    'inputs': {u'exo_mailfolders_id': None,
               u'exo_messages_id': u'AAMkAGFmNDE0ZDA1LTfM0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABAAAAAAD45IEka4IVS4DBeEtMPu
    'metrics': {'package': 'fn-exchange-online',
                'timestamp': '2020-02-04 09:08:13',
                'package_version': '1.0.0',
                'host': 'MacBook-Pro.local',
                'version': '1.0',
                'execution_time_ms': 1300},
    'success': True,
    'content': {'value': True},
    'raw': '{"value": true}',
    'reason': None,
    'version': '1.0'
}
    
```

#### ▼ Workflows:

The example Delete Message workflow uses the information in the Query Results data table. After the message is deleted using the Example: Exchange Online Delete Message workflow, the "Status" column in the data table is updated from Active to Deleted in red text. Any data table rules accessing the deleted message become inactive.

**Customization Settings**

Workflow Details:

- Name: Example: Exchange Online Delete Message
- API Name: example\_exchange\_online\_delete\_email
- Description: Delete an message that is entered as a row in the Exchange Online Message Query Results data table.
- Object Type: Data Table
- Data table: Exchange Online Message Query Results

Associated Rules: Example: Exchange Online Delete Message

Workflow Logic:

```

graph LR
    Start((Start your workflow here)) --> Task{Exchange Online: Delete Message}
    Task -- "Input: email address, mailbox folder id and message id of email to be deleted." --> Output((Output: message is deleted if found. "Status" column is updated to indicate the result of the delete operation.))
    
```

The screenshot shows a detailed view of a workflow configuration in Grip. It includes a form for entering metadata like name and API name, and a visual editor for defining the workflow logic. The logic consists of a single task node labeled 'Exchange Online: Delete Message' with associated input and output descriptions. A sidebar on the left contains various workflow element icons.

▼ Example Pre-Process Script:

```
inputs.exo_email_address = row.exo_dt_email_address
inputs.exo_messages_id = row.exo_dt_message_id
inputs.exo_mailfolders_id = None
```

▼ Example Post-Process Script:

```
if results.success:
    # The message was deleted, so update "status" column in data table.
    text = u"""<p style="color:{color}">{status} </p>""".format(color="red", status="Deleted")
    row['exo_dt_status'] = helper.createRichText(text)
elif results.content["error"] is not None:
    # There is an "item not found" error mostly likely here
    row['exo_dt_status'] = helper.createRichText(results.content["error"]["code"])
```

▼ Example Workflow Output:

## SecurityPOCdemos

### Description

No description.

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

Edit

### 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	
02/03/2020 14:37:48	2020-02-04 T20:44:03Z	resilient2@securitypocdemos.onmicrosoft.com	resilient2@securitypocdemos.onmicrosoft.com	lunch	No	Link	Deleted	AAMkAGFmNDE0ZDA1LTfM0GMtNGU2MS04Y2IwLTjhMmViNWU3Y2VhMABGAAA AAAD45IEka4IVS4DBeEtMPuSEBwBJf-ANAwqcRJF4hFv_x44UAAAAAEJAABJf-ANAwqcRJF4hFv_x44UAAAAlbtF2AAA=	...
02/03/2020 14:37:48	2020-02-04 T20:44:03Z	resilient3@securitypocdemos.onmicrosoft.com	resilient2@securitypocdemos.onmicrosoft.com	lunch	No	Link	Deleted	AAMkADZkZDY2NTRILWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhmcZQBGA AAAAA CPU6DCGuV7Sa2kl4jNbcmuBwCU6ehSHWGRTqkx2knKE-6AAAAAAEMA ACU6ehSHWGRTqkx2knKEQ-6AAALRtgQAAA=	...

Displaying 1 - 2 of 2

### ▼ Example Rule:

The Example: Exchange Online Delete Message rule works off the Query Results data table. The Delete Message rule is available when the "Status" column of the message row-entry is set to Active.

### Customization Settings

Layouts   Rules   Scripts   Workflows   Functions   Message Destinations   Phases & Tasks   Incident Types   Breach   Artifacts

Rules / Example: Exchange Online Delete Message

Cancel   Save & Close   Save

Display Name \*

Example: Exchange Online Delete M

Object Type

Data Table: Exchange Online Message Query Results

Conditions

Add conditions in which to invoke the rule. [Clear All](#)

Status is equal to Active



### Activities

Ordered   Ordered Activities will be invoked in the order specified below. They include: Add Tasks, Run Script, and Set Field. [Add New](#)

Workflows   Workflow Activities are started after all Ordered Activities complete.

Example: Exchange Online Delete Message

Destinations

Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

[Show Activity Fields](#)

© Copyright IBM Corporation 2020

## Function - Exchange Online: Delete Messages From Query Results

Exchange Online: Delete Messages From Query Results function requires the following Microsoft Graph API Application permissions:

- Mail.ReadWrite
- User.Read.All (if querying the whole tenant)

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.

The screenshot shows the Resilient platform's 'Functions' page. A new function is being created with the following details:

- Name:** Exchange Online: Delete Messages From Query Results
- API Name:** exchange\_online\_delete\_messages\_from\_query\_results
- Message Destination:** fn\_exchange\_online
- Description:** This Exchange Online function will delete 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.
- Inputs:** exo\_query\_messages\_results
- Input Fields:** exo\_attachment\_name, exo\_destination\_mailfolder\_id, exo\_email\_address, exo\_email\_address\_sender, exo\_end\_date, exo\_has\_attachments

### ▼ Inputs:

Name	Type	Required	Example	Tooltip
exo_query_messages_results	text	Yes	-	String containing JSON data results from Query Messages function

### ▼ Outputs:

```
results = {'inputs': {u'exo_query_messages_results': u'[{"status_code": 200, "email_address": "resilient3@securitypocd.onmicrosoft.com", "attachment_name": "Attachment 1", "attachment_content": "Attachment content", "attachment_type": "Image", "attachment_size": 1024, "attachment_id": "1234567890"}, {"status_code": 200, "email_address": "resilient3@securitypocd.onmicrosoft.com", "attachment_name": "Attachment 2", "attachment_content": "Attachment content", "attachment_type": "Image", "attachment_size": 1024, "attachment_id": "987654321"}]', 'metrics': {'package': 'fn-exchange-online', 'timestamp': '2020-02-05 15:06:25', 'package_version': '1.0.0', 'host': 'MacBook-Pro.local', 'version': '1.0', 'execution_time_ms': 4869}, 'success': True, 'content': [{"not_deleted_list": [], "deleted_list": [{"sentDateTime": "2020-02-05T20:03:21Z", "webLink": "https://outlook.office.com/mail/1234567890?view=normal&id=1234567890"}]}], 'reason': None, 'version': '1.0'}}
```

### ▼ Workflows:

**Customization Settings**

**Workflow Details:**

- Name \***: Example: Exchange Online Delete Messages From Query Results
- API Name \***: example\_exchange\_online\_delete\_messages\_from\_query\_results
- Description**: This workflow calls the Query Messages function to find messages that meet user input search criteria. The results of the query are passed to the Delete Messages From Query Function. The list of messages is deleted and placed in the Querv data table. An incident note is written indicating the number of messages deleted.
- Object Type \***: Incident

**Associated Rules**: Example: Exchange Online Delete Message from Query Results

**Workflow Diagram:**

```

graph LR
    Start((Start your workflow here)) --> Query[Exchange Online: Query Messages]
    subgraph "Input"
        direction TB
        A["An email address, a comma separated list of email addresses or a list of \"ALL\" to search all mailboxes to search"]
        B["List of message IDs matching the search criteria"]
        C["JSON object in string format of the list of messages matching the search criteria"]
    end
    Query --> Delete[Exchange Online: Delete Messages ...]
    subgraph "Output"
        D["messages are deleted and placed in the query data table. An incident note is written indicating the number of messages deleted"]
    end
    Delete --> End(( ))
    
```

The diagram shows a workflow starting with a 'Start your workflow here' node, followed by an 'Exchange Online: Query Messages' node. This node receives input from three sources: 'An email address, a comma separated list of email addresses or a list of "ALL" to search all mailboxes to search', 'List of message IDs matching the search criteria', and 'JSON object in string format of the list of messages matching the search criteria'. The output of this node is passed to an 'Exchange Online: Delete Messages ...' node, which then leads to a final 'End' node. The output of the delete node is described as 'messages are deleted and placed in the query data table. An incident note is written indicating the number of messages deleted'.

▼ Example Pre-Process Script:

```
inputs.exo_query_messages_results = workflow.properties.exo_query_results['raw']
```

▼ Example Post-Process Script:

```
from java.util import Date

deleted_count = 0
not_deleted_count = 0

# Add each email as a row in the query results data table
for user in results["content"]:

    not_deleted_count = not_deleted_count + len(user["not_deleted_list"])
    for email in user["deleted_list"]:
        deleted_count = deleted_count + 1
        message_row = incident.addRow("exo_message_query_results_dt")
        message_row.exo_dt_query_date = Date()
        message_row.exo_dt_message_id = email.id
        message_row.exo_dt_received_date = email.receivedDateTime
        message_row.exo_dt_email_address = user["email_address"]
        if email.sender:
            message_row.exo_dt_sender_email = email.sender.emailAddress.address
        else:
            message_row.exo_dt_sender_email = ""
        message_row.exo_dt_message_subject = email.subject
        message_row.exo_dt_has_attachments = email.hasAttachments
        if email.webLink:
            ref_html = u"""<a href='{0}'>Link</a>""".format(email.webLink)
            message_row.exo_dt_web_link = helper.createRichText(ref_html)
        else:
            message_row.exo_dt_web_link = ""
```

```

text = u"""\n<p style= "color:{color}">{status} </p>""".format(color="red", status="Deleted")
message_row.exo_dt_status = helper.createRichText(text)

# Post a note containing the number of emails deleted
note = u"Exchange Online Delete Messages From Query Results:\n {0} messages deleted".format(deleted_count)

# Add to the note if any messages from the query were not deleted.
if not_deleted_count > 0:
    note2 = u" {0} messages NOT deleted".format(not_deleted_count)
    note = u"{0}\n{1}".format(note, note2)
incident.addNote(note)

```

▼ Example Workflow Output:

The messages deleted will appear in the data table with red "Deleted" text in the Status column:

Query Date	Received Date	Queried Email Address	Sender Email	Message Subject	Has Attachments	Web Link	Status	Message ID	
02/03/2020 14:37:48	2020-02-04 T20:44:03Z	resilient2@securitypocdemos.onmicrosoft.com	resilient2@securitypocdemos.onmicrosoft.com	lunch	No	<a href="#">Link</a>	Deleted	AAMkAGFmNDE0ZDA1LTfmOGMtNGU2M... ANAwqcRJF4hFv_x44UAAAAAAEJAABJf-ANAwqcRJF4hFv_x44UAAAAlbtF2AAA=	<a href="#">...</a>
02/03/2020 14:37:48	2020-02-04 T20:44:03Z	resilient3@securitypocdemos.onmicrosoft.com	resilient2@securitypocdemos.onmicrosoft.com	lunch	No	<a href="#">Link</a>	Deleted	AAMkADZkZDY2NTRILWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjh... Q-6AAALRtgQAAA=	<a href="#">...</a>

Displaying 1 - 2 of 2

▼ Example Rule:

The screenshot shows the Resilient platform's 'Customization Settings' page for 'Rules'. At the top, there are navigation links for Dashboards, Inbox, Incidents, Create, and a search bar. The main content area is titled 'Customization Settings' and shows a 'Rules' section with the path 'Rules / Example: Exchange Online Delete Message from Query Results'. Below this, there are fields for 'Display Name' (with a placeholder 'Example: Exchange Online Delete M'), 'Object Type' (set to 'Incident'), and 'Conditions' (with a link to 'Add New'). The 'Activities' section is expanded, showing 'Ordered' activities, 'Workflows', and 'Destinations'. Under 'Ordered', it says 'Ordered Activities will be invoked in the order specified below. They include: Add Tasks, Run Script, and Set Field.' with a 'Add New' link. Under 'Workflows', it says 'Workflow Activities are started after all Ordered Activities complete.' with a text input field containing 'Example: Exchange Online Delete Messages From Query Results'. Under 'Destinations', it says 'Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.' with a 'Select Destinations' button. At the bottom right are 'Cancel', 'Save & Close', and 'Save' buttons.

The Example: Exchange Online Delete Message From Query Results incident menu item rule will bring up the rule activity popup dialog pictured below to prompt for input querying message to be deleted. See the Query function section for a description of querying.

## Example: Exchange Online Delete Message from Query Results

Email Address \* 

Mail Folder 

 

Choose from at least one of the search criteria below:

Sender email address 

 user@example.com

Start date/time 

 MM/DD/YYYY HH:mm:ss Z 

End date/time 

 MM/DD/YYYY HH:mm:ss Z 

Message Subject 

Message Body

Has attachments 

 Unknown 

[Cancel](#)

[Execute](#)

### Function - Exchange Online: Get Message

Exchange Online: Get Message function requires the following Microsoft Graph API Application permission:

- Mail.Read

This function returns the contents of an Exchange Online message in JSON format.

Customization Settings

Functions / exchange\_online\_get\_message

Name *	Exchange Online: Get Message
API Name * ⓘ	exchange_online_get_message
Message Destination *	fn_exchange_online
Description	This function returns the contents of an Exchange Online message in json format.

**Inputs**

exo_email_address
exo_messages_id

**Input Fields ⓘ**

Search...
exo_attachment_name
exo_destination_mailfolder_id

▼ Inputs:

Name	Type	Required	Example	Tooltip
exo_email_address	text	Yes	user@example.com	Get information on this user email account
exo_messages_id	text	Yes	-	The message ID of the message to get

▼ Outputs:

```

results = {'inputs': {u'exo_messages_id': u'AAMkAGFmNDE0ZDA1LTf0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEka4IVS4',
                     u'exo_email_address': u'resilient2@securitypocdemos.onmicrosoft.com'},
          'metrics': {'package': 'fn-exchange-online',
                      'timestamp': '2020-02-03 15:39:31',
                      'package_version': '1.0.0',
                      'host': 'cambridge.ibm.com',
                      'version': '1.0',
                      'execution_time_ms': 654},
          'success': True,
          'pretty_string': u'\n      "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users(\'resilient2%40resilient.com\')/messages(id)"\n    }',
          'content': {u'sentDateTime': u'2020-01-29T16:17:23Z',
                      'conversationId': u'AAQkAGFmNDE0ZDA1LTf0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMAAQAGjzfC_8ndR0s7000o-q',
                      'isDraft': False,
                      'internetMessageId': u'<MMMMprod.outlook.com>',
                      'id': u'AAMkAGFmNDE0ZDA1LTf0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEka4IVS4DBeEtMPuSEBwB',
                      'isReadReceiptRequested': False,
                      'subject': u'test text area body',
                      'lastModifiedDateTime': u'2020-02-03T16:46:41Z',
                      'bodyPreview': u'test text area body',
                      'from': {u'emailAddress': {u'name': u'Resilient User 3', u'address': u'resilient2@securitypocdemos.onmicrosoft.com'}},
                      'flag': {u'flagStatus': u'notFlagged'},
                      'reason': None,
                      'version': '1.0'}
        }
    }
}
```
```

▼ Workflows:

The workflow Write Message JSON as Note calls the Get Message function and writes the JSON contents returned from MS Graph API to an incident note. The JSON returned from MS Graph API contains information that is different from the .eml file, so both formats are provided in this package For information on writing EML to attachment see:

[Write Message as Attachment.](#)

Customization Settings

Workflows / Example: Exchange Online Write Message JSON as Note

Name \* Example: Exchange Online Write Message JSON as Note

API Name \* example\_exchange\_online\_get\_message

Description Get an Exchange Online message and write the JSON content to an incident note.

Object Type \* Data Table

Data table \* Exchange Online Message Query Results

Creator Resilient Sysadmin  
Last Modified 01/05/2020 13:39  
Last Modified By Resilient Sysadmin  
Associated Rules Example: Exchange Online Write Message JSON as Note

Cancel Save & Close Save

▼ Example Pre-Process Script:

```
inputs.exo_email_address = row.exo_dt_email_address
inputs.exo_messages_id = row.exo_dt_message_id
```

▼ Example Post-Process Script:

```
# Print the message to an incident note if it is found, otherwise update the status as Not Found in the datatable.
if results.content["error"] is not None:
    noteText = u"Exchange Online message NOT FOUND: \n email address: {0}\n message ID: {1}\n{2}".format(results.inputs[
        row.exo_dt_status = "Not Found"
else:
    noteText = u"Exchange Online email address: {0} message:{\n{1}}".format(results.inputs["exo_email_address"], results.p
incident.addNote(noteText)
```

▼ Example Rule:

Customization Settings

Layouts    Rules    Scripts    Workflows    Functions    Message Destinations    Phases & Tasks    Incident Types    Breach    Artifacts

Rules / Example: Exchange Online Write Message JSON as Note

Display Name \*

Object Type Data Table: Exchange Online Message Query Results

Conditions Add conditions in which to invoke the rule. [Clear All](#)

Status is equal to Active

Cancel    Save & Close    Save

---

**Activities**

Ordered Ordered Activities will be invoked in the order specified below. They include: *Add Tasks, Run Script, and Set Field*. [Add New](#)

Workflows Workflow Activities are started after all Ordered Activities complete.

Destinations Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

[Show Activity Fields](#)

© Copyright IBM Corporation 2020

## Function - Exchange Online: Get User Profile

Exchange Online: Get User Profile function requires the following Microsoft Graph API Application permission:

- **User.Read.All**

The Get User Profile function returns Exchange Online user profile for a given email address.

Customization Settings

Functions / exchange\_online\_get\_email\_user\_profile

Name \* Exchange Online: Get User Profile

API Name \* exchange\_online\_get\_email\_user\_profile

Message Destination \* fn\_exchange\_online

Description This function will get Exchange Online user profile for a given email address.

Creator Resilient Sysadmin  
Last Modified 01/02/2020 16:22  
Last Modified By Resilient Sysadmin  
Associated Workflows Example: Exchange Online Get User Profile

**Inputs**

exo\_email\_address

**Input Fields**

Add Field

Search...

- exo\_attachment\_name
- exo\_destination\_mailfolder\_id
- exo\_email\_address
- exo\_email\_address\_sender
- exo\_end\_date
- exo\_has\_attachments
- exo\_mail\_folders
- exo\_mailfolders\_id
- exo\_meeting\_body

▼ Inputs:

| Name              | Type | Required | Example          | Tooltip                                    |
|-------------------|------|----------|------------------|--------------------------------------------|
| exo_email_address | text | Yes      | user@example.com | Get information on this user email account |

▼ Outputs:

```

results = {
    'inputs': {'exo_email_address': u'resilient2@securitypocdemos.onmicrosoft.com'},
    'metrics': {'package': 'fn-exchange-online',
                'timestamp': '2020-01-31 11:14:42',
                'package_version': '1.0.0',
                'host': 'MacBook-Pro.local',
                'version': '1.0',
                'execution_time_ms': 599},
    'success': True,
    'pretty_string': u'{\n      "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",\n      "busi
    'content': {
        'displayName': u'Resilient User 2',
        'mobilePhone': None,
        'preferredLanguage': u'en-US',
        'jobTitle': None,
        'userPrincipalName': u'resilient2@securitypocdemos.onmicrosoft.com',
        '@odata.context': u'https://graph.microsoft.com/v1.0/$metadata#users/$entity',
        'officeLocation': None,
        'businessPhones': [],
        'mail': u'resilient2@securitypocdemos.onmicrosoft.com',
        'surname': u'Resilient User 2',
    }
}

```

```

    u'givenName': u'Resilient User 2',
    u'id': u'393c1ebb-8222-4ba1-8665-f54eaf7f024f'},
    'raw': {'displayName": "Resilient User 2", "mobilePhone": null, "preferredLanguage": "en-US", "jobTitle": null,
    'reason': None,
    'version': '1.0'
}
}

```

▼ Workflows:

The example Get User Profile workflow accesses the artifact whose value contains the email address of the user whose profile is to be queried. The user profile is returned in JSON format as an incident note.

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

Workflows / Example: Exchange Online Get User Profile

Name \* Example: Exchange Online Get User Profile

API Name \* example\_exchange\_online\_get\_user\_profile

Description This example workflow gets the Exchange Online user profile that matches the input email address and writes the information to a note.

Object Type \* Artifact

Creator Resilient Sysadmin  
Last Modified 01/02/2020 16:22  
Last Modified By Resilient Sysadmin  
Associated Rules Example: Exchange Online Get User Profile

Start your workflow here

Input: email address of Exchange Online user

Output: Incident Note contain the email user information

Exchange Online: Get User Profile

▼ Example Pre-Process Script:

```
inputs.exo_email_address = artifact.value
```

▼ Example Post-Process Script:

```

if results.content["error"] is not None:
    noteText = u"Exchange Online user profile NOT FOUND: {0}\n{1}".format(results.inputs["exo_email_address"], results.p
else:
    noteText = u"Exchange Online user profile: {0}\n{1}".format(results.inputs["exo_email_address"], results.pretty_stri
incident.addNote(noteText)

```

▼ Example Workflow Output:

The Get User Profile workflow writes the user profile in JSON format to an incident note. Sample output of the note is pictured below:

## SecurityPOCdemos

[Actions ▾](#)**Description**

No description.

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

Sans Serif  Normal  B  I  U  S  E  E  A  A    W

[Post](#)[Cancel](#)Search...  Show Task Notes  Oldest Notes FirstCreated By: 0 selected Date Created: All     **Resilient Sysadmin** added a note to the *Incident 01/31/2020 09:22 edited*

Exchange Online user profile: resilient2@securitypocdemos.onmicrosoft.com

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
  "businessPhones": [],
  "displayName": "Resilient User 2",
  "givenName": "Resilient User 2",
  "id": "393c1ebb-8222-4ba1-8665-f54eaf7f024f",
  "jobTitle": null,
  "mail": "resilient2@securitypocdemos.onmicrosoft.com",
  "mobilePhone": null,
  "officeLocation": null,
  "preferredLanguage": "en-US",
  "surname": "Up",
  "userPrincipalName": "resilient2@securitypocdemos.onmicrosoft.com"
}
```

**Summary**

|                                                     |            |
|-----------------------------------------------------|------------|
| ID                                                  | 2099       |
| Phase                                               | Engage     |
| Severity                                            | Low        |
| Date Created                                        | 01/13/2020 |
| Date Occurred                                       | —          |
| Date Discovered                                     | 01/14/2020 |
| Date Determined                                     | 01/14/2020 |
| Was personal information or personal data involved? | Unknown    |

Incident Type

[Phishing](#)**People**

|            |                              |
|------------|------------------------------|
| Created By | <b>Resilient Sysadmin</b>    |
| Owner      | <b>Resilient Sysadmin</b>    |
| Members    | <i>There are no members.</i> |

**Related Incidents**

#2101 Exchange Online demo

**Attachments***There are no attachments.*

## ▼ Example Rule:

The example Get User Profile rule invokes the Get User Profile workflow if the artifact type is one of the following:

- Email Recipient
- Email Sender
- Email Sender Name
- User Account

Customization Settings

Rules / Example: Exchange Online Get User Profile

Display Name \* Example: Exchange Online Get User

Object Type Artifact

Conditions Add conditions in which to invoke the rule. [Clear All](#)

All  Any  Advanced example: 1 OR (2 AND 3)

Type is equal to Email Recipient +   
 Type is equal to Email Sender Name +   
 Type is equal to Email Sender +   
 Type is equal to User Account +

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include: [Add Tasks](#), [Run Script](#), and [Set Field](#). [Add New](#)

Workflows Workflow Activities are started after all Ordered Activities complete.

Destinations Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

[Show Activity Fields](#)

## Function - Exchange Online: Move Message to Folder

Exchange Online: Move Message to Folder function requires the following Microsoft Graph API Application permission:

- **Mail.ReadWrite**

This function moves an Exchange Online message to the specified folder in the users mailbox.

The screenshot shows the Resilient platform's 'Customization Settings' page for a function. The function is named 'Exchange Online: Move Message to Folder' with an API name 'exchange\_online\_move\_message\_to\_folder'. It is associated with a message destination 'fn\_exchange\_online' and a description stating it moves an Exchange Online message to a specified folder. The 'Inputs' section lists several variables: exo\_email\_address, exo\_mailfolders\_id, exo\_messages\_id, and exo\_destination\_mailfolder\_id. To the right, there is a list of 'Input Fields' including exo\_attachment\_name, exo\_destination\_mailfolder\_id, exo\_email\_address, exo\_email\_address\_sender, exo\_end\_date, exo\_has\_attachments, exo\_mail\_folders, exo\_mailfolders\_id, and exo\_meeting\_body. The 'Associated Workflows' section shows an example workflow named 'Example: Exchange Online Move Message to Folder'.

#### ▼ Inputs:

| Name                          | Type   | Required | Example                   | Tooltip                                      |
|-------------------------------|--------|----------|---------------------------|----------------------------------------------|
| exo_email_address             | text   | Yes      | user@example.com          | Get information on this user email account   |
| exo_mailfolders_id            | text   | No       | -                         | MailFolders ID                               |
| exo_messages_id               | text   | Yes      | -                         | The message ID of the message to be deleted  |
| exo_destination_mailfolder_id | select | Yes      | recoverableitemsdeletions | Destination folder to which message is moved |

#### ▼ Outputs:

```
Result: {
  'inputs': {'exo_destination_mailfolder_id': {'id': 126,
  'name': 'recoverableitemsdeletions'},
             'exo_mailfolders_id': None,
             'exo_messages_id': 'AAMKAGFmNDE0ZDA1LTfM0GmtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAAD45IEka4IVS4DBeEtMPuSE'},
  'metrics': {'package': 'fn-exchange-online',
              'timestamp': '2020-01-31 13:23:41',
              'package_version': '1.0.0',
              'host': 'MacBook-Pro.local',
              'version': '1.0',
              'execution_time_ms': 1706},
  'success': True,
  'content': {'value': True},
  'raw': '{"value": true}',
  'reason': None,
  'version': '1.0'}
```

▼ Workflows:

The example Move Message to Folder workflow accesses the Exchange Online Message Query Results data table. Messages can be moved to a "Well known" Outlook folder, such as:

- archive
- clutter
- conflicts
- conversationhistory
- deleteditems
- drafts
- inbox
- junkemail
- localfailures
- msgfolderroot
- outbox
- recoverableitemsdeletions
- scheduled
- searchfolders
- sentitems

**Customization Settings**

Workflow / Example: Exchange Online Move Message to Folder

|               |                                                                                                                                        |                  |                                                 |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|------------------|-------------------------------------------------|
| Name *        | Example: Exchange Online Move Message to Folder                                                                                        | Creator          | Resilient Sysadmin                              |
| API Name *    | example_exchange_online_move_message_to_folder                                                                                         | Last Modified    | 01/14/2020 10:07                                |
| Description   | This workflow will move a row-entry message in the Exchange Online Message Query Results data table to the specified user mail folder. | Last Modified By | Resilient Sysadmin                              |
| Object Type * | Data Table                                                                                                                             | Associated Rules | Example: Exchange Online Move Message to Folder |
| Data table *  | Exchange Online Message Query Results                                                                                                  |                  |                                                 |

**Workflow Diagram:**

```

graph LR
    Start((Start your workflow here)) --> Activity[Exchange Online: Move Message to ...]
    Activity --> End(( ))
    
```

**Input:** The email address and the message ID of the message to move and the mail folder ID where to move the message.

**Output:** An incident note is written indicating whether the move operation was successful.

▼ Example Workflow Output:

The Move Message to Folder workflow calls the MS Graph API to move a message in the data table row to the Well-known Outlook folder specified in the exo\_destination\_mailfolder\_id input parameter. When a message is moved, its message ID is changed, the status field column of the Exchange Online Message Query Results data table is updated to "Moved" in Red, and any rules to be run on the data table row are changed.

Below is a screen shot of an example Note after a message is moved to a folder:

The screenshot shows the Resilient platform interface. At the top, there is a navigation bar with links for Dashboards, Inbox, Incidents, and Create. Below the navigation bar, the title "SecurityPOCdemos" is displayed. Under the title, there is a section titled "Description" with the subtext "No description." Below this, there is a toolbar with various tabs: Tasks, Details, Breach, Notes (which is currently selected), Members, News Feed, Attachments, Stats, Timeline, Artifacts, Email, and Exchange Online. A rich text editor window is open, showing a toolbar with font styles (Sans Serif, Normal, B, I, U, S), alignment (Left, Center, Right, Justify), and other options like bold, italic, underline, etc. Below the toolbar is a large text area for the note content. At the bottom of the editor are two buttons: "Post" and "Cancel". Below the editor, there is a search bar with placeholder text "Search..." and a magnifying glass icon. To the right of the search bar are two checkboxes: "Show Task Notes" (checked) and "Oldest Notes First" (unchecked). On the far right, there are filters for "Created By: 0 selected" and "Date Created: All". The main content area displays a note from a user named "Resilient Sysadmin" added on "02/02/2020 22:42". The note content is: "Exchange Online email address: resilient2@securitypocdemos.onmicrosoft.com". Below the note are several small icons for editing, deleting, and more. The note also includes a message about being moved to a clutter folder and some old and new message IDs.

#### ▼ Example Pre-Process Script:

```
inputs.exo_email_address = row.exo_dt_email_address
inputs.exo_mailfolders_id = None
inputs.exo_messages_id = row.exo_dt_message_id
inputs.exo_destination_mailfolder_id = rule.properties.exo_destination_mailfolder_id
```

#### ▼ Example Post-Process Script:

```
if results.content["error"] is not None:
    # Print the message to an incident note if it is found, otherwise update the status as Not Found in the datatable.
    noteText = u"Exchange Online message NOT FOUND: \n email address: {0}\n message ID: {1}".format(results.inputs["exo_status_text"] = u"""\<p style= "color:{color}">{status} </p>""".format(color="red", status="Not Found"))
    row['exo_dt_status'] = helper.createRichText(status_text)
else:
    # When a message is moved it's ID changes, so update the new message ID into the data table
    noteText = u"Exchange Online email address: {0}\n\n Message has been moved to folder: {1}\n\n Old message ID: {2}"
    row['exo_dt_message_id'] = results.content["new_message_id"]
incident.addNote(noteText)
```

#### ▼ Example Rule:

The example Move Message to Folder rule accesses the Exchange Online Message Query Results data table. When the status column of the row is Active the Move Message To Folder rule is available to initiate the corresponding workflow. The status column may be non-Active if the message is Deleted or Not Found, in which case the message cannot be moved.

Customization Settings

Rules / Example: Exchange Online Move Message to Folder

Display Name \* Example: Exchange Online Move Me

Object Type Data Table: Exchange Online Message Query Results

Conditions Add conditions in which to invoke the rule. [Clear All](#)

Status is equal to Active

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include: *Add Task, Run Script, and Set Field.* [Add New](#)

Workflows Workflow Activities are started after all Ordered Activities complete.

Destinations Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

[Show Activity Fields](#)

© Copyright IBM Corporation 2020

## Function - Exchange Online: Query Messages

Exchange Online: Query Messages function requires the following Microsoft Graph API Application permissions:

- **Mail.Read**
- **User.Read.All** (if querying the whole tenant)

The Exchange Online: Query Message function queries the Exchange Online to find messages matching the specified input parameters. The function returns a list of messages matching the search criteria.

The function will search over the following email accounts:

- all mailboxes of a tenant (specify "all", "ALL", "all users")
- single email address
- comma separated list of email addresses

If no mail folder is specified, all folders and subdirectories are queried. The mail folder to be searched can be one of the list of Outlook "Well-known" folders:

- archive
- clutter
- conflicts
- conversationhistory
- deleteditems
- drafts
- inbox
- junkemail
- localfailures

- msgfolderroot
- outbox
- recoverableitemsdeletions
- scheduled
- searchfolders
- sentitems

At least one of the following search criteria must be passed to the query messages function:

- Sender email address
- Message received date/time start/end
- Message subject "contains" text
- Message body "contains" text
- Boolean flag indicating whether the message has an attachment

NOTE: There can be a large number of results of the Query Message function. If needed, use the max\_user and max\_messages parameters in the app.config file to limit the number of users searched and the number of messages returned from a query.

**Customization Settings**

**Functions** / exchange\_online\_query\_emails

**Name \***: Exchange Online: Query Messages  
**API Name \***: exchange\_online\_query\_emails  
**Message Destination \***: fn\_exchange\_online  
**Description**: This function will query Exchange Online to find messages matching the specified input parameters. A list of messages is returned from the function.

**Creator**: Resilient Sysadmin  
**Last Modified**: 01/05/2020 13:36  
**Last Modified By**: Resilient Sysadmin

**Associated Workflows**:

- Example: Exchange Online Delete Messages From Query Results
- Example: Exchange Online Query Messages
- Example: Exchange Online Query Messages on Artifact

**Inputs**

|                          |
|--------------------------|
| exo_email_address        |
| exo_mail_folders         |
| exo_email_address_sender |
| exo_start_date           |
| exo_end_date             |
| exo_message_subject      |
| exo_message_body         |
| exo_has_attachments      |

**Input Fields**

|                               |
|-------------------------------|
| exo_attachment_name           |
| exo_destination_mailfolder_id |
| exo_email_address             |
| exo_email_address_sender      |
| exo_end_date                  |
| exo_has_attachments           |
| exo_mail_folders              |
| exo_mailfolders_id            |
| exo_meeting_body              |

▼ Inputs:

| Name                     | Type           | Required | Example          | Tooltip                                                                              |
|--------------------------|----------------|----------|------------------|--------------------------------------------------------------------------------------|
| exo_email_address        | text           | Yes      | user@example.com | Get information on this user email account                                           |
| exo_email_address_sender | text           | No       | user@example.com | Search messages sent from this email address; leave blank to ignore sender attribute |
| exo_end_date             | datetimepicker | No       | -                | Query messages received ending at this date/time                                     |

| Name                | Type           | Required | Example           | Tooltip                                                                       |
|---------------------|----------------|----------|-------------------|-------------------------------------------------------------------------------|
| exo_has_attachments | boolean        | No       | -                 | True to include attachments, False to exclude attachments, Unknown to get all |
| exo_mail_folders    | text           | No       | Inbox             | The folder to search in the users mailbox                                     |
| exo_message_body    | text           | No       | message body text | message body                                                                  |
| exo_message_subject | text           | No       | message subject   | message subject                                                               |
| exo_start_date      | datetimepicker | No       | -                 | Query messages received starting at this date/time                            |

▼ Outputs:

```
results = {
    'inputs': {u'exo_start_date': None,
               u'exo_email_address_sender': None,
               u'exo_end_date': None,
               u'exo_message_subject': u'lunch',
               u'exo_has_attachments': None,
               u'exo_email_address': u'all',
               u'exo_mail_folders': None,
               u'exo_message_body': None},
    'metrics': {'package': 'fn-exchange-online',
                'timestamp': '2020-02-04 15:36:12',
                'package_version': '1.0.0',
                'host': 'MacBook-Pro.local',
                'version': '1.0',
                'execution_time_ms': 9492},
    'success': True,
    'content': [{u'status_code': 200,
                 'email_address': u'resilient2@securitypocdemos.onmicrosoft.com',
                 'email_list': [{u'sentDateTime': u'2020-02-04T20:44:02Z',
                               u'conversationId': u'AAQkAGFmNDE0ZDA1LTfM0GmtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMAAQANIXI-VmHPNIslAVFC4yWrI='},
                               u'internetMessageId': u'<MWPR2201MB11359DA0C07AF09AB319DD9FB1030@MWPR2201MB1135.namprd22.prod.outloo
                               u'id': u'AAMkAGFmNDE0ZDA1LTfM0GmtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAAD45IEka4IVS4DBeEtMPuSEBwBJf-ANA
                               u'subject': u'lunch',
                               u'lastModifiedDateTime': u'2020-02-04T20:44:04Z',
                               u'bodyPreview': u'"Let's have lunch at 12!"',
                               u'from': {u'emailAddress': {u'name': u'Resilient User 2',
                               u'address': u'resilient2@securitypocdemos.onmicrosoft.com'}},
                               u'flag': {u'flagStatus': u'notFlagged'},
                               u'isDraft': False,
                               u'replyTo': [],
                               u'changeKey': u'CQAAABYAAABJf/ANAwqcRJF4hFv+x44UAAAac/G', u'receivedDateTime': u'2020-02-04T20:44:03Z
                               u'parentFolderId': u'AQMkAGFmNDE0ZDA1LTfM0GmtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMAAuAAAD_0SBJGuCFUuAwXhLTD7kh
                               u'body': {u'content': u'<html>\r\n<head>\r\n<meta http-equiv="Content-Type" content="text/html; charset
                               u'isDeliveryReceiptRequested': False,
                               u'importance': u'normal',
                               u'toRecipients': [{u'emailAddress': {u'name': u'Resilient User 3',
                               u'address': u'resilient3@securitypocdemos.onmicrosoft.com'}}],
                               u'ccRecipients': [],
                               u'isRead': True,
                               u'categories': [],
                               u'sender': {u'emailAddress': {u'name': u'Resilient User 2',
                               u'address': u'resilient2@securitypocdemos.onmicrosoft.com'}},
                               u'createdDateTime': u'2020-02-04T20:44:02Z',

```

```

    u'webLink': u'https://outlook.office365.com/owa/?ItemID=AAMkAGFmNDE0ZDA1LTfmoGMtNGU2MS04Y2IwLTJhMmViNW
    u'conversationIndex': u'AQHV25vV0jEj9WYc80iyUBUULjJasg==',
    u'hasAttachments': False,
    u'bccRecipients': [],
    u'inferenceClassification': u'focused',
    u'@odata.etag': u'W/"CQAAABYAAABJf/ANAwqcRJF4hFv+x44UAAAlac/G"!'}]}},
    'reason': None,
    'version': '1.0'
}

```

▼ Workflows:

The Example: Exchange Online Query Messages workflow places results into the Exchange Online Query Results data table, which appears on the Exchange Online custom incident tab. (See the Installation Guide to configure the custom tab.)

**Customization Settings**

Workflow Details:

- Name: Example: Exchange Online Query Messages
- API Name: example\_exchange\_online\_query\_messages\_of\_a\_group
- Description: This workflow will query the Exchange Online messages for a list of email address and write a row entry into the Exchange Message Query Results data table for each email that matches the search criteria. If the string "ALL" or "all" is specified, all user mailboxes of the tenant are queried for the
- Object Type: Incident

Metadata:

- Creator: Resilient Sysadmin
- Last Modified: 01/28/2020 07:25
- Last Modified By: Resilient Sysadmin
- Associated Rules: Example: Exchange Online Query Messages

Workflow Diagram:

```

graph LR
    Start((Start your workflow here)) --> Task{Exchange Online: Query Messages}
    Task --> End(( ))
    
```

Annotations for the workflow diagram:

- An email address, a comma separated list of email addresses or a string "ALL" or "all" specify what email mailboxes to search.
- Each message matching the search criteria is added as a row to the results data table.

▼ Example Pre-Process Script:

```

# Get the email address of the user whose mailbox will be queried.
inputs.exo_email_address = inputs.exo_email_address if rule.properties.exo_email_address_list is None else rule.proper

# Get the search criteria from the activity rules if available.
inputs.exo_mail_folders = inputs.exo_mail_folders if rule.properties.exo_mailfolder_id is None
inputs.exo_email_address_sender = inputs.exo_email_address_sender if rule.properties.exo_email_address_sender is None
inputs.exo_message_subject = inputs.exo_message_subject if rule.properties.exo_message_subject is None
inputs.exo_message_body = inputs.exo_message_body if rule.properties.exo_message_body is None
inputs.exo_start_date = inputs.exo_start_date if rule.properties.exo_start_date is None
inputs.exo_end_date = inputs.exo_end_date if rule.properties.exo_end_date is None
inputs.exo_has_attachments = inputs.exo_has_attachments if rule.properties.exo_has_attachments is None

```

▼ Example Post-Process Script:

```

from java.util import Date

note = u"Exchange Online Query Multiple users:\n"

```

```

note_len = len(note)

# Add each email as a row in the query results data table
for user in results["content"]:
    # If an email address is not found post to a note.
    if user["status_code"] == 404:
        line = u"email address not found: {}\\n".format(user["email_address"])
        note = note + line

    for email in user["email_list"]:
        message_row = incident.addRow("exo_message_query_results_dt")
        message_row.exo_dt_query_date = Date()
        message_row.exo_dt_message_id = email.id
        message_row.exo_dt_received_date = email.receivedDateTime
        message_row.exo_dt_email_address = user["email_address"]
        if email.sender:
            message_row.exo_dt_sender_email = email.sender.emailAddress.address
        else:
            message_row.exo_dt_sender_email = ""
        message_row.exo_dt_message_subject = email.subject
        message_row.exo_dt_has_attachments = email.hasAttachments
        if email.webLink:
            ref_html = u"""

```

▼ Example Rule:

Customization Settings

Display Name \* Example: Exchange Online Query Mes

Object Type Incident

Conditions Add conditions in which to invoke the rule. [Add New](#)

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include: [Add Tasks](#), [Run Script](#), and [Set Field](#). [Add New](#)

Workflows Workflow Activities are started after all Ordered Activities complete.

Destinations Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

[Show Activity Fields](#)

© Copyright IBM Corporation 2020

When the Example: Exchange Online Delete Messages from Query Results rule is activated, the following rule activity popup dialog prompts for input to create the meeting and send a message to the invitees:

## Example: Exchange Online Query Messages

Email Address \*

Mail Folder

Choose from a least one of the search criteria below:

Sender email address

Start date/time

End date/time

Message Subject

Message Body

Has attachments

### Function - Exchange Online: Send Message

Exchange Online: Send Message function requires the following Microsoft Graph API Application permission:

- Mail.Send

This function creates a message and sends it to the specified recipients.

The screenshot shows the Resilient platform's 'Customization Settings' page for a function. The function is named 'Exchange Online: Send Message' with the API name 'exchange\_online\_send\_message'. The message destination is set to 'fn\_exchange\_online'. The description states: 'This function will create a message and send to the specified recipients.' The 'Inputs' section lists four variables: 'exo\_email\_address', 'exo\_recipients', 'exo\_message\_subject', and 'exo\_message\_body'. To the right, there is a list of 'Input Fields' such as 'exo\_attachment\_name', 'exo\_destination\_mailfolder\_id', etc. The top right corner shows the creator ('Resilient Sysadmin') and last modified date ('01/14/2020 12:47').

#### ▼ Inputs:

| Name                | Type | Required | Example           | Tooltip                                    |
|---------------------|------|----------|-------------------|--------------------------------------------|
| exo_email_address   | text | Yes      | user@example.com  | Get information on this user email account |
| exo_message_body    | text | No       | message body text | Message body                               |
| exo_message_subject | text | No       | message subject   | Message subject                            |
| exo_recipients      | text | Yes      | -                 | Comma separated list of message recipients |

#### ▼ Outputs:

```
results = {
    'inputs': {'exo_recipients': 'resilient2@securitypocdemos.onmicrosoft.com', 'exo_email_address': 'resilient3@securitypocdemos.onmicrosoft.com', 'exo_message_subject': 'Please investigate', 'exo_message_body': '<div class="rte"><div>Can you look into this?</div><div><br /></div><div>Thanks!</div>'},

    'metrics': {'package': 'fn-exchange-online', 'timestamp': '2020-02-04 11:18:16', 'package_version': '1.0.0', 'host': 'MacBook-Pro.local', 'version': '1.0', 'execution_time_ms': 796},
    'success': True,
    'content': {'value': True},
    'raw': {'value': true},
    'reason': None,
    'version': '1.0'}
}
```

#### ▼ Workflows:

The Example: Exchange Online Send Message workflow calls the Exchange Online Send Message function and writes an incident note containing the results of the function.

Customization Settings

**Workflow Details:**

- Name \***: Example: Exchange Online Send Message
- API Name \***: example\_exchange\_online\_send\_message
- Description**: This workflow will send a message from a specified email address with specified message subject and body to the specified recipients.
- Object Type \***: Incident

**Creator**: Resilient Sysadmin  
**Last Modified**: 01/28/2020 09:20  
**Last Modified By**: Resilient Sysadmin  
**Associated Rules**: Example: Exchange Online Send Message

**Buttons:** Cancel, Save & Close, Save

▼ Example Pre-Process Script:

```
inputs.exo_email_address = inputs.exo_email_address if rule.properties.exo_message_sender_address is None else rule.properties.exo_message_sender_address
inputs.exo_recipients = inputs.exo_recipients if rule.properties.exo_message_recipients is None else rule.properties.exo_message_recipients
inputs.exo_message_subject = inputs.exo_message_subject if rule.properties.exo_message_subject is None else rule.properties.exo_message_subject
inputs.exo_message_body = inputs.exo_message_body if rule.properties.exo_message_send_body.content is None else rule.properties.exo_message_send_body.content
```

▼ Example Post-Process Script:

```
if results.success:
    noteText = "Exchange Online message sent\n  From: {0}\n  To: {1}\n  Subject: {2}\n  Body: {3}.".format(results.inputs["exo_email_address"], results.inputs["exo_recipients"], results.inputs["exo_message_subject"], results.inputs["exo_message_body"])
else:
    noteText = "Exchange Online message NOT sent\n  From: {0}\n  To: {1}.".format(results.inputs["exo_email_address"], results.inputs["exo_recipients"])
incident.addNote(noteText)
```

▼ Example Workflow Output:

The following is a sample incident note that is created from Example: Exchange Online Send Message workflow:

**Description**

No description.

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

Sans Serif   Normal   B   I   U   S   E   E   E   A   M   G   I   W   •

Post   Cancel

Search...    Show Task Notes    Oldest Notes First   Created By: 0 selected   Date Created: All ▾

• Resilient Sysadmin added a note to the *Incident* 02/03/2020 08:01  
Exchange Online message sent  
From: resilient2@securitypocdemos.onmicrosoft.com  
To: resilient2@securitypocdemos.onmicrosoft.com, resilient3@securitypocdemos.onmicrosoft.com  
Subject: Please investigate  
Body: <div class="rte"><div>Can you take a look at this?</div></div>

▼ Example Rule:

The following Example: Exchange Online Send Message incident menu item rule is included to send a message via Exchange Online:

Customization Settings

Layouts   **Rules**   Scripts   Workflows   Functions   Message Destinations   Phases & Tasks   Incident Types   Breach   Artifacts

Rules / Example: Exchange Online Send Message  

Display Name \*   Example: Exchange Online Send Me.

Object Type   Incident

Conditions   Add conditions in which to invoke the rule. [Add New](#)

Activities

Ordered   Ordered Activities will be invoked in the order specified below. They include: *Add Tasks, Run Script, and Set Field*. [Add New](#)

Workflows   Workflow Activities are started after all Ordered Activities complete.

Destinations   Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

▶ Show Activity Fields

© Copyright IBM Corporation 2020

When the Example Send Message rule is initiated the following rule activity popup dialog will appear prompting for input on the message to send:

## Function - Exchange Online: Write Message as Attachment

Exchange Online: Write Message as Attachment function requires the following Microsoft Graph API Application permission:

- Mail.Read

This function gets the mime content of an Exchange Online message and writes it as an incident attachment. The attachment file name is an optional parameter. The function uses a default message-{email-address}-{message-ID}.eml filename if none is specified.

Customization Settings

Resilient Dashboards ▾ Inbox Incidents Create

Search Resilient Sysadmin resilient

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

Functions / exchange\_online\_write\_message\_as\_attachment

Name \* Exchange Online: Write Message as Attachment

API Name \* exchange\_online\_write\_message\_as\_attachment

Message Destination \* fn\_exchange\_online

Description This function will get the mime content of an Exchange Online message and write it as an incident attachment.

Creator Resilient Sysadmin Last Modified 01/21/2020 10:22 Last Modified By Resilient Sysadmin Associated Workflows Example: Exchange Online Write Message as A

Cancel Save & Close Save

Inputs

incident\_id  
task\_id  
exo\_email\_address  
exo\_messages\_id  
exo\_attachment\_name

Input Fields Add Field

Search... exo\_attachment\_name exo\_destination\_mailfolder\_id exo\_email\_address exo\_email\_address\_sender exo\_end\_date exo\_has\_attachments exo\_mail\_folders exo\_mailfolders\_id exo\_meeting\_body

▼ Inputs:

| Name                | Type   | Required | Example          | Tooltip                                         |
|---------------------|--------|----------|------------------|-------------------------------------------------|
| incident_id         | number | Yes      | -                | -                                               |
| task_id             | number | No       | -                | -                                               |
| exo_email_address   | text   | Yes      | user@example.com | Get information on this user email account      |
| exo_messages_id     | text   | Yes      | -                | The message ID of the message to be deleted     |
| exo_attachment_name | text   | No       | my-message.eml   | The attachment file to which message is written |

▼ Outputs:

```
results = {'inputs': {u'incident_id': 2099,
                     u'exo_attachment_name': u'my-message.eml',
                     u'exo_messages_id': u'AAMkAGFmNDE0ZDA1LTNmOGMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEka4IVS4
                     u'exo_email_address': u'resilient2@securitypocdemos.onmicrosoft.com'},
           'metrics': {'package': 'fn-exchange-online',
                       'timestamp': '2020-02-03 14:54:13',
                       'package_version': '1.0.0',
                       'host': 'annmarie-mbp.cambridge.ibm.com',
                       'version': '1.0', 'execution_time_ms': 5929},
           'success': True, 'content': {'attachment_name': u'my-message.eml'},
           'raw': '{"attachment_name": "my-message.eml"}',
           'reason': None,
           'version': '1.0'}
}
```

▼ Workflows:

▼ Example Pre-Process Script:

```
inputs.incident_id = incident.id
#inputs.task_id = task.id
inputs.exo_attachment_name = rule.properties.exo_attachment_name
inputs.exo_email_address = row.exo_dt_email_address
inputs.exo_messages_id = row.exo_dt_message_id
```

▼ Example Post-Process Script:

None

▼ Example Rule:

The example Write Message EML as Attachment rule accesses the Exchange Online Message Query Results data table. When the status column of the row is Active, the Write Message as Attachment rule is available to initiate the corresponding workflow. If the status is non-Active, which includes Deleted or Not Found, the message content cannot be retrieved or written.

Customization Settings

Layouts    Rules    Scripts    Workflows    Functions    Message Destinations    Phases & Tasks    Incident Types    Breach    Artifacts

Rules / Example: Exchange Online Write Message EML as Attachment

Display Name \*

Object Type Data Table: Exchange Online Message Query Results

Conditions Add conditions in which to invoke the rule. [Clear All](#)

Status is equal to Active

**Activities**

Ordered Ordered Activities will be invoked in the order specified below. They include: *Add Task, Run Script, and Set Field.* [Add New](#)

Workflows Workflow Activities are started after all Ordered Activities complete.

Destinations Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

[Show Activity Fields](#)

## Data Table - Exchange Online Message Query Results

The following is an example of message query results that are populated in the Exchange Online Message Query Results data table:

NOTE: The Web Link column contains a link to the message, but you must be logged in as the message owner user to view the message in the link.

The screenshot shows the Resilient platform interface. At the top, there is a navigation bar with the Resilient logo, Dashboards, Inbox, Incidents, Create, and other tabs. Below the navigation bar, the title "SecurityPOCdemos" is displayed. Under the title, there is a section titled "Description" with the note "No description." Below this, there is a horizontal menu bar with links: Tasks, Details, Breach, Notes, Members, News Feed, Attachments, Stats, Timeline, Artifacts, Email, Exchange Online (which is underlined, indicating it is the active tab), and Edit. The main content area is titled "Exchange Online Message Query Results". It features a search bar with placeholder "Search...", a magnifying glass icon, and buttons for Print and Export. A table displays two rows of query results. The columns are: Query Date, Received Date, Queried Email Address, Sender Email, Message Subject, Has Attachments, Web Link, Status, and Message ID. The first row shows a query from 02/03/2020 at 14:37:48, received on 2020-02-04 at 20:44:03Z, with the message "lunch" from "resilient2@securitypocdemos.onmicrosoft.com" to "resilient2@securitypocdemos.onmicrosoft.com". The status is Deleted, and the message ID is AAMkAGFmNDE0ZDA1LTFmOGMtNGU2M... The second row shows a similar query from 02/03/2020 at 14:37:48, received on 2020-02-04 at 20:44:03Z, with the message "lunch" from "resilient3@securitypocdemos.onmicrosoft.com" to "resilient2@securitypocdemos.onmicrosoft.com". The status is Active, and the message ID is AAMkADZkZDY2NTRILWQwNjgtNDMxZi1i... Both rows have a "..." button in the last column.

| Query Date          | Received Date         | Queried Email Address                       | Sender Email                                | Message Subject | Has Attachments | Web Link             | Status  | Message ID                                                                                                                                                                       |                     |
|---------------------|-----------------------|---------------------------------------------|---------------------------------------------|-----------------|-----------------|----------------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 02/03/2020 14:37:48 | 2020-02-04 T20:44:03Z | resilient2@securitypocdemos.onmicrosoft.com | resilient2@securitypocdemos.onmicrosoft.com | lunch           | No              | <a href="#">Link</a> | Deleted | AAMkAGFmNDE0ZDA1LTFmOGMtNGU2M...<br>S04Y2IwlTJhMmViNWU3Y2vhMABGAAA<br>AAAD45IEka4IVS4DBeEtMPuSEBwBJf-<br>ANAwqcRJF4hFv_x44UAAAAAEJAABJf-<br>ANAwqcRJF4hFv_x44UAAAAbtF2AAA=       | <a href="#">...</a> |
| 02/03/2020 14:37:48 | 2020-02-04 T20:44:03Z | resilient3@securitypocdemos.onmicrosoft.com | resilient2@securitypocdemos.onmicrosoft.com | lunch           | No              | <a href="#">Link</a> | Active  | AAMkADZkZDY2NTRILWQwNjgtNDMxZi1i...<br>YTA2LTQ0ZmYxN2UwMjhmmZQBGA.....<br>CPU6DCGuV7Sa2k4jNbcmuBwCU6ehSH<br>WGRTqkx2knKEQ-<br>6AAAAAAEMAACU6ehSHWGRTqkx2knKE<br>Q-6AAAALRtgQAAA= | <a href="#">...</a> |

API Name:

exo\_message\_query\_results\_dt

Columns:

| Column Name           | API Access Name        | Type           | Tooltip |
|-----------------------|------------------------|----------------|---------|
| Queried Email Address | exo_dt_email_address   | text           | -       |
| Has Attachments       | exo_dt_has_attachments | boolean        | -       |
| Message ID            | exo_dt_message_id      | text           | -       |
| Message Subject       | exo_dt_message_subject | text           | -       |
| Query Date            | exo_dt_query_date      | datetimepicker | -       |
| Received Date         | exo_dt_received_date   | text           | -       |
| Sender Email          | exo_dt_sender_email    | text           | -       |
| Status                | exo_dt_status          | textarea       | -       |
| Web Link              | exo_dt_web_link        | textarea       | -       |

## Rules

| Rule Name                                                  | Object                       | Workflow Triggered                                         |
|------------------------------------------------------------|------------------------------|------------------------------------------------------------|
| Example: Exchange Online Write Message JSON as Note        | exo_message_query_results_dt | example_exchange_online_get_message                        |
| Example: Exchange Online Send Message                      | incident                     | example_exchange_online_send_message                       |
| Example: Exchange Online Get User Profile                  | artifact                     | example_exchange_online_get_user_profile                   |
| Example: Exchange Online Delete Message from Query Results | incident                     | example_exchange_online_delete_messages_from_query_results |
| Example: Exchange Online Move Message to Folder            | exo_message_query_results_dt | example_exchange_online_move_message_to_folder             |
| Example: Exchange Online Query Messages on Artifact        | artifact                     | example_exchange_online_query_emails                       |
| Example: Exchange Online Write Message EML as Attachment   | exo_message_query_results_dt | example_exchange_online_write_message_as_attachment        |
| Example: Exchange Online Query Messages                    | incident                     | example_exchange_online_query_messages_of_a_group          |
| Example: Exchange Online Create Meeting                    | incident                     | example_exchange_online_create_meeting                     |
| Example: Exchange Online Create Artifacts                  | exo_message_query_results_dt | -                                                          |
| Example: Exchange Online Delete Message                    | exo_message_query_results_dt | example_exchange_online_delete_email                       |