

User Guide: Microsoft Exchange Online Functions for IBM Resilient v1.3.0

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](#)
-

History

Date	Version	Note
2/2021	1.3.0	Added attachments to send message
12/2020	1.2.0	Performance improvement when querying a large tenant using the "all" query parameter
9/2020	1.1.0	Numerous performance and functional improvements around querying mailboxes
2/2020	1.0.0	Initial publication

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.

Customization Settings

Functions / exchange_online_create_meeting

Name * Exchange Online: Create Meeting

API Name * exchange_online_create_meeting

Message Destination * fn_exchange_online

Description This function will create a meeting event in the organizer's Outlook calendar and send a calendar event mail message to the meeting participants inviting them to the meeting.

Creator Resilient Sysadmin

Last Modified 01/21/2020 10:21

Last Modified By Resilient Sysadmin

Associated Workflows Example: Exchange Online Create Meeting

Inputs

- exo_meeting_email_address
- exo_meeting_start_time
- exo_meeting_end_time
- exo_meeting_subject
- exo_meeting_body
- exo_meeting_required_attendees
- exo_meeting_optional_attendees
- exo_meeting_location

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

► 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_required_attendees':
u'resilient3@securitypocdemos.onmicrosoft.com,
resilient2@securitypocdemos.onmicrosoft.com',
u'exo_meeting_start_time': 1581004800000,
u'exo_meeting_email_address': u'resilient2@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        "040000008200E00074C5B7101A82E0080000000096E4493689DBD501000000000000000010000000ADDA5C\n7497FB60469CE3850456D898C5",\n        "seriesMasterId": null,\n        "responseStatus": {\n            "response": "organizer",\n            "time": "0001-01-01T00:00:00Z"\n        },\n        "@odata.etag": "W/\\"SX/wDQMKnESReIRb/se0FAAAJWnN6Q==\\\""\n    }\n},\n    'content': {u'body': {u'content': u'', u'contentType': u'html'}, u'sensitivity':
u'normal', u'locations': [],.....}'
}

```

► 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
API Name *	example_exchange_online_create_meeting
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.
Object Type *	Incident
Creator	Resilient Sysadmin
Last Modified	01/28/2020 13:59
Last Modified By	Resilient Sysadmin
Associated Rules	Example: Exchange Online Create Meeting

Start your workflow here → Exchange Online: Create Meeting → 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 None else

```

```

rule.properties.exo_meeting_email_address
inputs.exo_meeting_start_time = inputs.exo_meeting_start_time if
rule.properties.exo_meeting_start_time is None else
rule.properties.exo_meeting_start_time
inputs.exo_meeting_end_time = inputs.exo_meeting_end_time if
rule.properties.exo_meeting_end_time is None else rule.properties.exo_meeting_end_time
inputs.exo_meeting_subject = inputs.exo_meeting_subject if
rule.properties.exo_meeting_subject is None else rule.properties.exo_meeting_subject
inputs.exo_meeting_body = inputs.exo_meeting_body if
rule.properties.exo_meeting_body.content is None else
rule.properties.exo_meeting_body.content
inputs.exo_meeting_required_attendees = inputs.exo_meeting_required_attendees if
rule.properties.exo_meeting_required_attendees is None else
rule.properties.exo_meeting_required_attendees
inputs.exo_meeting_optional_attendees = inputs.exo_meeting_optional_attendees if
rule.properties.exo_meeting_optional_attendees is None else
rule.properties.exo_meeting_optional_attendees
inputs.exo_meeting_location = inputs.exo_meeting_location if
rule.properties.exo_meeting_location is None else rule.properties.exo_meeting_location

```

► 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"],results.pretty_string)
else:
    noteText = u"Exchange Online meeting was NOT created\n  From:
{0}\n{1}".format(results.inputs["exo_meeting_email_address"], results.pretty_string)

incident.addNote(noteText)

```

► Example Rule:

The screenshot shows the Resilient platform's 'Customization Settings' page for a rule. The rule is titled 'Example: Exchange Online Create Meeting'. It is configured to run on 'Incident' objects. Under the 'Activities' section, there is one ordered activity: 'Example: Exchange Online Create Meeting'. This activity is a workflow step. The 'Conditions' field is empty. At the bottom, there are buttons for 'Cancel', 'Save & Close', and 'Save'.

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

X

Meeting Organizer Email Address *	<input type="text" value="user@example.com"/>
Meeting Start Time *	<input type="text" value="MM/DD/YYYY HH:mm:ss Z"/> 
Meeting End Time *	<input type="text" value="MM/DD/YYYY HH:mm:ss Z"/> 
Meeting Subject *	<input type="text"/>
Meeting Body *	<div style="border: 1px solid #ccc; padding: 5px;"><p>Sans Serif ▾ Normal ▾ B I U S E E</p><p>≡ A A S I W ▾</p><hr/><div style="height: 150px;"></div></div>
Meeting Location	<input type="text"/>
Required Attendees	<input type="text" value="user1@example.com, user2@example.com"/>
Optional Attendees	<input type="text" value="user1@example.com, user2@example.com"/>

CancelExecute

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.

Customization Settings

Functions / exchange_online_delete_email

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

- exo_email_address
- exo_mailfolders_id
- exo_messages_id

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_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'AAMkAGFmNDE0ZDA1LTfM0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEka4IVS4DBeEtMPuSEBwBJf-ANAwqcRJF4hFv_x44UAAAinByvAABJf-ANAwqcRJF4hFv_x44UAAAinIROAAA='},
    '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 screenshot shows the 'Customization Settings' page for a workflow named 'Example: Exchange Online Delete Message'. The page includes fields for Name, API Name, Description, Object Type, and Data table, along with a status bar showing creator, last modified, last modified by, and associated rules.

Workflow Diagram:

```

graph LR
    Start((Start your workflow here)) --> Function{f(x)}
    Function --> End(( ))
    subgraph Inputs [Input: email address, mailbox folder id and message id of email to be deleted.]
        direction TB
        I1[Input: email address, mailbox folder id and message id of email to be deleted.]
        I2[Output: message is deleted if found.]
        I3[status column is updated to indicate the result of the delete operation.]
    end
    I1 -.-> Function
    I2 -.-> Function
    I3 -.-> Function

```

The diagram illustrates a workflow starting from a 'Start your workflow here' node, leading to a central function node labeled 'Exchange Online: Delete Message'. This function node has three outgoing arrows pointing to three separate nodes representing input and output data flow.

► 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)
    row['exo_dt_web_link'] = ""
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"])
    row['exo_dt_web_link'] = ""
```

► Example Workflow Output:

The screenshot shows the Resilient interface with the 'Exchange Online' tab selected. At the top, there's a navigation bar with links for Dashboards, Inbox, Incidents, and Create. Below the navigation is a search bar with placeholder 'Search...' and icons for Print and Export.

Exchange Online Message Query Results

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	AAMkAGFmNDE0ZDA1LTfmOGMtNGU2M... S04Y2IwLTJhMmViNWU3Y2VhMABGAA... AAAD45IEka4IVS4DBeEtMPuSEBwBJf-... ANAwqcRJF4hFv_x44UAaaaaEJAABJf-... ANAwqcRJF4hFv_x44UAAlbtF2AAA=
02/03/2020 14:37:48	2020-02-04 T20:44:03Z	resilient3@securitypocdemos.onmicrosoft.com	resilient2@securitypocdemos.onmicrosoft.com	lunch	No	Link	Deleted	AAMkADZkZDY2NTRILWQwNjgtNDMxZi1i... YTA2LTQ0ZmYxN2UwMjhmnZQBGAaaaa... CPU6DCGuV7Sa2kl4jNbcmuBwCU6ehSH... WGRTqkx2knKEQ-... 6AAAAAAEACU6ehSHWGRTqkx2knKEQ-6AAALRtgQAAA=

Displaying 1 - 2 of 2

► Example Rule:

The screenshot shows the Resilient Rule configuration page. At the top, there's a navigation bar with links for Dashboards, Inbox, Incidents, and Create. To the right is a user dropdown for 'Resilient Sysadmin'.

Customization Settings

Rules / Example: Exchange Online Delete Message

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](#)

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.

© 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.

Customization Settings

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

Functions / exchange_online_delete_messages_from_query_results

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

Creator Resilient Sysadmin Last Modified 01/21/2020 21:48 Last Modified By Resilient Sysadmin Associated Workflows Example: Exchange Online Delete Messages From Query R

Input Fields Add Field

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@securitypocdemos.onmicrosoft.com", "email_list": [{"sentDateTime": "2020-02-05T20:03:21Z", "conversationId": "AAQkADZkZDY2NTRllWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhZQBGAAAAACPU6DCGuV7Sa2kl4jNbcmuBwCU6ehSHWGRTqkx2knKEQ-6AAAAAAEMAACU6ehSHWGRTqkx2knKEQ-6AAALRtgSAAA=", "internetMessageId": "<MWHP2201MB11357FA62DE5F7C1B1EBCF53B1020@MWHP2201MB1135.namprd22.prod.outlook.com>", "id": "AAMkADZkZDY2NTRllWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhZQBGAAAAACPU6DCGuV7Sa2kl4jNbcmuBwCU6ehSHWGRTqkx2knKEQ-6AAAAAAEMAACU6ehSHWGRTqkx2knKEQ-6AAALRtgSAAA=", "isReadReceiptRequested": false, "subject": "lunch", "lastModifiedDateTime": "2020-02-05T20:05:13Z", "bodyPreview": "Do you want to meet for lunch?", "from": {"emailAddress": {"name": "Resilient User 2", "address": "resilient2@securitypocdemos.onmicrosoft.com"}}, "flag": {"flagStatus": "notFlagged"}, "isDraft": false, "replyTo": [], "changeKey": "CQAAABYAAACU6ehSHWGRTqkx2knKEQ/6AAALRVqT", "receivedDateTime": "2020-02-05T20:03:24Z", "parentFolderId": "AAMkADZkZDY2NTRllWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhZQAUAAAAACPU6DCGuV7Sa2kl4jNbcmuAQCU6ehSHWGRTqkx2knKEQ-6AAAAAAEMAACU6ehSHWGRTqkx2knKEQ-6AAALRtgSAAA=", "body": {"content": "<html>\\r\\n<head>\\r\\n<meta http-equiv=\\\"Content-Type\\\" content=\\\"text/html; charset=utf-8\\\">\\r\\n<meta content=\\\"text/html; charset=iso-8859-1\\\">\\r\\n<style type=\\\"text/css\\\" style=\\\"display:none\\\">\\r\\n!--\\r\\n<np\\r\\n\\t{margin-top:0;\\r\\n\\tmargin-bottom:0}\\r\\n--\\r\\n</style>\\r\\n</head>\\r\\n<body dir=\\\"ltr\\\">\\r\\n<div style=\\\"font-family:Calibri,Arial,Helvetica,sans-serif; font-size:12pt; color:rgb(0,0,0)\\\">\\r\\nDo you want to meet for lunch?  
<br>\\r\\n</div>\\r\\n</body>\\r\\n</html>\\r\\n", "contentType": "html"}, "isDeliveryReceiptRequested": false, "importance": "normal", "toRecipients": [{"emailAddress": {"name": "Resilient User 3", "address": "resilient3@securitypocdemos.onmicrosoft.com"}]}, "ccRecipients": [], "isRead": false, "categories": [], "sender": {"emailAddress": {"name": "Resilient User 2", "address": "resilient2@securitypocdemos.onmicrosoft.com"}}, "createdDateTime": "2020-02-05T20:03:23Z", "webLink": "https://outlook.office365.com/owa/?ItemID=AAMkADZkZDY2NTRllWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhZQBGAAAAACPU6DCGuV7Sa2kl4jNbcmuBwCU6ehSHWGRTqkx2knKEQ%2F6AAAAAAEMAACU6ehSHWGRTqkx2knKEQ%2F6AAALRtgSAAA%3D&exvsurl=1&iewmodel=ReadMessageItem", "conversationIndex": "AOHV3F90TGJJcpCC200b79aiMCXkCw==".
```

```
"hasAttachments": false, "bccRecipients": [], "inferenceClassification": "focused", "@odata.etag": "W\\\"CQAAABYAAACU6ehSHWGRTqkx2knKEQ/6AAALRVqT\\\""}]}},  
  
'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': u'2020-02-05T20:03:21Z',  
        'webLink': u'https://outlook.office365.com/owa/?  
ItemID=AAMkADZkZDY2NTR1LLWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhmZQBGAAAAACPU6DCGuV7Sa2kl4jNb  
muBwCU6ehSHWGRTqkx2knKEQ%2F6AAAAAAEMAACU6ehSHWGRTqkx2knKEQ%2F6AAALRtgSAAA%3D&exvsurl=1&vi  
ewmodel=ReadMessageItem',  
        'conversationId':  
u'AAQkADZkZDY2NTR1LLWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhmZQAQAExiSXKQggttDm_-WozA15As=',  
        'internetMessageId':  
u'<MWHPR2201MB11357FA62DE5F7C1B1EBCF53B1020@MWHPR2201MB1135.namprd22.prod.outlook.com>',  
        'id':  
u'AAMkADZkZDY2NTR1LLWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhmZQBGAAAAACPU6DCGuV7Sa2kl4jNbcmuBwC  
U6ehSHWGRTqkx2knKEQ-6AAAAAAEMAACU6ehSHWGRTqkx2knKEQ-6AAALRtgSAAA=',  
        'isReadReceiptRequested': False, 'subject': 'lunch', 'lastModifiedDateTime': u'2020-02-05T20:05:13Z',  
        'bodyPreview': 'Do you want to meet for lunch?', 'from': {  
            'emailAddress': {  
                'name': 'Resilient User 2',  
                'address': 'resilient2@securitypocdemos.onmicrosoft.com'}},  
        'isDraft': False, 'importance': 'normal',  
        'changeKey': u'CQAAABYAAACU6ehSHWGRTqkx2knKEQ/6AAALRVqT',  
        'receivedDateTime': u'2020-02-05T20:03:24Z', 'parentFolderId':  
u'AAMkADZkZDY2NTR1LLWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhmZQAuAAAAACPU6DCGuV7Sa2kl4jNbcmuAQC  
U6ehSHWGRTqkx2knKEQ-6AAAAAAEMAACU6ehSHWGRTqkx2knKEQ-6AAALRtgSAAA=',  
        'body': {  
            'content': u'\r\n<head>\r\n<meta http-equiv="Content-Type" content="text/html; charset=utf-8">\r\n<meta content="text/html; charset=iso-8859-1">\r\n<style type="text/css" style="display:none">\r\n<!--\r\nnp\r\nn\t{margin-top:0;\r\nn\tmargin-bottom:0}\r\n-->\r\n</style>\r\n</head>\r\n<body dir="ltr">\r\n<div style="font-family:Calibri,Arial,Helvetica,sans-serif; font-size:12pt; color:rgb(0,0,0)">\r\nDo you want to meet for lunch?  
<br>\r\n</div>\r\n</body>\r\n</html>\r\n',  
            'contentType': 'html',  
            'isDeliveryReceiptRequested': False, 'replyTo': [],  
            'toRecipients': [  
                {  
                    'emailAddress': {  
                        'name': 'Resilient User 3',  
                        'address': 'resilient3@securitypocdemos.onmicrosoft.com'}},  
                {  
                    'ccRecipients': [],  
                    'flag': {  
                        'flagStatus': 'notFlagged'},  
                    'categories': [],  
                    'sender': {  
                        'emailAddress': {  
                            'name': 'Resilient User 2',  
                            'address': 'resilient2@securitypocdemos.onmicrosoft.com'}}},  
                    'createdDateTime': u'2020-02-05T20:03:23Z',  
                    'isRead': False, 'conversationIndex':  
u'AQHV3F9QTGJJcpCC200b79ajMCXkCw==',  
                    'hasAttachments': False, 'bccRecipients': [],  
                    'inferenceClassification': 'focused',  
                    '@odata.etag':  
u'W/"CQAAABYAAACU6ehSHWGRTqkx2knKEQ/6AAALRVqT"'},  
                    'email_address':  
u'resilient3@securitypocdemos.onmicrosoft.com'}],  
                    'raw': '[{"not_deleted_list": [],  
"deleted_list": [{"sentDateTime": "2020-02-05T20:03:21Z", "webLink":  
"https://outlook.office365.com/owa/?  
ItemID=AAMkADZkZDY2NTR1LLWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhmZQBGAAAAACPU6DCGuV7Sa2kl4jNb  
muBwCU6ehSHWGRTqkx2knKEQ%2F6AAAAAAEMAACU6ehSHWGRTqkx2knKEQ%2F6AAALRtgSAAA%3D&exvsurl=1&vi  
ewmodel=ReadMessageItem", "conversationId":  
"AAQkADZkZDY2NTR1LLWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhmZQAQAExiSXKQggttDm_-WozA15As=",  
"internetMessageId": "  
<MWHPR2201MB11357FA62DE5F7C1B1EBCF53B1020@MWHPR2201MB1135.namprd22.prod.outlook.com>","  
"id":  
u'AAMkADZkZDY2NTR1LLWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhmZQBGAAAAACPU6DCGuV7Sa2kl4jNbcmuBwC  
U6ehSHWGRTqkx2knKEQ-6AAAAAAEMAACU6ehSHWGRTqkx2knKEQ-6AAALRtgSAAA=",  
"isReadReceiptRequested": false, "subject": "lunch", "lastModifiedDateTime": "2020-02-05T20:05:13Z",  
"bodyPreview": "Do you want to meet for lunch?", "from": {"emailAddress": {  
"name": "Resilient User 2",  
"address": "resilient2@securitypocdemos.onmicrosoft.com"}},  
"isDraft": false, "importance": "normal", "changeKey":  
"CQAAABYAAACU6ehSHWGRTqkx2knKEQ/6AAALRVqT", "receivedDateTime": "2020-02-05T20:03:24Z",  
"parentFolderId":
```

```
"AAMkADZkZDY2NTRlLWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhmZQAUAAAAACPU6DCGuV7Sa2k14jNbcmuAQCUn6ehSHWGRTqkx2knKEQ-6AAAAAAEAAA=", "body": {"content": "<html>\r\n<head>\r\n<meta http-equiv=\"Content-Type\" content=\"text/html; charset=utf-8\">\r\n<meta content=\"text/html; charset=iso-8859-1\">\r\n<style type=\"text/css\" style=\"display:none\">\r\n<!--\r\n<np>\r\n<t margin-top:0; margin-bottom:0>\r\n-->\r\n</style>\r\n</head>\r\n<body dir=\"ltr\">\r\n<div style=\"font-family:Calibri,Arial,Helvetica,sans-serif; font-size:12pt; color:rgb(0,0,0)\">\r\nDo you want to meet for lunch?\r\n<br>\r\n</div>\r\n</body>\r\n</html>\r\n", "contentType": "html"}, "isDeliveryReceiptRequested": false, "replyTo": [], "toRecipients": [{"emailAddress": {"name": "Resilient User 3", "address": "resilient3@securitypocdemos.onmicrosoft.com"}}, {"ccRecipients": [], "flag": {"flagStatus": "notFlagged"}, "categories": [], "sender": {"emailAddress": {"name": "Resilient USer 2", "address": "resilient2@securitypocdemos.onmicrosoft.com"}}, "createdDateTime": "2020-02-05T20:03:23Z", "isRead": false, "conversationIndex": "AQHV3F9QTGJJcpCC200b79ajMCXkCw==", "hasAttachments": false, "bccRecipients": [], "inferenceClassification": "focused", "@odata.etag": "W/\\"CQAAABYAAACU6ehSHWGRTqkx2knKEQ/6AAALRVqT\\\""}, {"email_address": "resilient3@securitypocdemos.onmicrosoft.com"}]}, "reason": "None", "version": "1.0"}]
```

► Workflows:

Customization Settings

Workflows / Example: Exchange Online Delete Messages From Query Results

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
Object Type *	Incident
Creator	Resilient Sysadmin
Last Modified	01/24/2020 07:42
Last Modified By	Resilient Sysadmin
Associated Rules	Example: Exchange Online Delete Message from Query Re

Start your workflow here

```

graph LR
    Start(( )) --> Query[Exchange Online: Query Messages]
    subgraph Inputs [Input]
        direction TB
        A["An email address, a comma separated list of email addresses or a string \"ALL\" or \"all\" specifying which email 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
    Inputs --> Query
    Query --> Delete[Exchange Online: Delete Messages ...]
    Delete --> End(( ))
    subgraph Outputs [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 --> Outputs

```

► Example Pre-Process Script:

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

► Example Post-Process Script:

```
from java.util import Date

content = results.get("content")
output_format = content.get("exo_query_output_format")
```

```
# Write to the data table if the user requested it.
if "Exchange Online data table" in output_format:

    user_list = content.get("delete_results")
    # Add each email as a row in the query results data table
    for user in user_list:

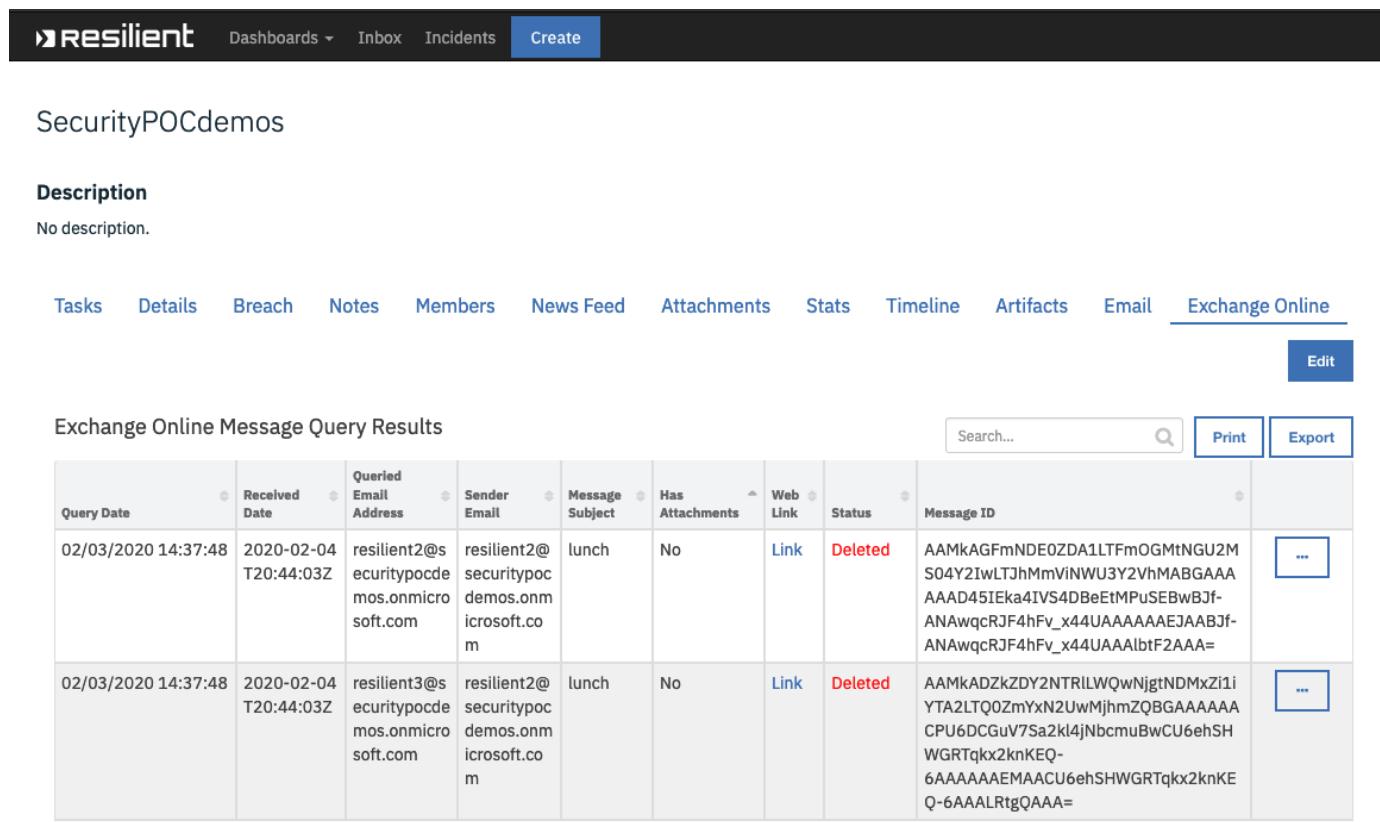
        for email in user.get("deleted_list"):
            message_row = incident.addRow("exo_message_query_results_dt")
            message_row.exo_dt_query_date = Date()
            message_row.exo_dt_message_id = email.id
            message_row.exo_dt_received_date = email.receivedDateTime
            message_row.exo_dt_email_address = user.get("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"""Link".format(email.webLink)
                message_row.exo_dt_web_link = helper.createRichText(ref_html)
            else:
                message_row.exo_dt_web_link = ""

            text = u"""

{status}

".format(color="red",
            status="Deleted")
            message_row.exo_dt_status = helper.createRichText(text)
```

► Example Workflow Output:



The screenshot shows the Resilient platform interface. At the top, there is a navigation bar with the Resilient logo, Dashboards, Inbox, Incidents, and a Create button. Below the navigation bar, the title 'SecurityPOCdemos' is displayed. Underneath the title, there is a 'Description' section with the text 'No description.' and a 'Details' tab. The main content area features a table titled 'Exchange Online Message Query Results'. The table has columns for Query Date, Received Date, Queried Email Address, Sender Email, Message Subject, Has Attachments, Web Link, Status, and Message ID. There are two rows of data in the table. Each row includes a 'More' button (three dots) and an 'Edit' button. The first row's 'Status' column is red and displays 'Deleted'. The second row's 'Status' column is red and displays 'Deleted'. The 'Message ID' column contains long, encoded strings.

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	AAMkAGFmNDE0ZDA1LTNmOGMtNGU2M... ANAwqcRJF4hFv_x44UAAAAAAEJAABJf-ANAwqcRJF4hFv_x44UAAAAbtF2AAA=	...
02/03/2020 14:37:48	2020-02-04 T20:44:03Z	resilient3@securitypocdemos.onmicrosoft.com	resilient2@securitypocdemos.onmicrosoft.com	lunch	No	Link	Deleted	AAMkADZkZDY2NTRILWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjh... Q-6AAAAAEMAACU6ehSHWGRTqkx2knKEQ-6AAALRtgQAAA=	...

► Example Rule:

Customization Settings

Rules / Example: Exchange Online Delete Message from Query Results

Display Name * Example: Exchange Online Delete 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

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 X

Email Address * * i

Mail Folder i

—

Choose from a least one of the search criteria below:

Sender email address i

Start date/time i



End date/time i



Message Subject i

Message Body

Has attachments i

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

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

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'AAMkAGFmNDE0ZDA1LTf0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAAAD45IEka4IVS4DBeEtMPuSEBwBJf-ANAwqcRJF4hFv_x44UAAAinByvAABJf-ANAwqcRJF4hFv_x44UAAAinIROAAA=',
                     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":\n"https://graph.microsoft.com/v1.0/$metadata#users(''\\resilient2@securitypocdemos.onmicrosoft.com'')/messages/$entity",\n    "@odata.etag":\n"W/\"CQAAABYAAJF/ANAwqcRJF4hFv+x44UAAAil53\"",\n    "bccRecipients": [],\n    "body": {\n        "content": "<html>\r\n<head>\r\n<meta http-equiv=\"Content-Type\" content=\"text/html; charset=utf-8\">\r\n<meta content=\"text/html; charset=us-ascii\">\r\n</head>\r\n<body>\r\n<div class=\"rte\">\r\n<div>test text area body</div>\r\n</div>\r\n</body>\r\n</html>\r\n",\n        "contentType": "html",\n        "bodyPreview": "test text area body",\n        "categories": [],\n        "ccRecipients": []},\n    "content": {"sentDateTime": "2020-01-29T16:17:23Z"}\n}'}
```

```

u'conversationId': u'AAQkAGFmNDE0ZDA1LTfM0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMAAQAGjzfC_8ndR0s
7000o-q8ys=',
        u'isDraft': False,
        u'internetMessageId': u'<MMMMprod.outlook.com>',
        u'id':
u'AAMkAGFmNDE0ZDA1LTfM0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEka4IVS4DBeEtMPuSEBwB
Jf-ANAwqcRJF4hFv_x44UAAAinByvAABJf-ANAwqcRJF4hFv_x44UAAAinIROAAA=',
        u'isReadReceiptRequested': False,
        u'subject': u'test text area body',
        u'lastModifiedDateTime': u'2020-02-03T16:46:41Z',
        u'bodyPreview': u'test text area body',
        u'from': {u'emailAddress': {u'name': u'Resilient User 3'}},
        u'address': u'resilient2@securitypocdemos.onmicrosoft.com'},
        u'flag': {u'flagStatus': u'notFlagged'},
        .
        .
        .
    },
    'reason': None,
    'version': '1.0'}

```

► Workflows:

[Write Message as Attachment.](#)

The screenshot shows the Resilient platform's 'Customization Settings' interface for a workflow. The workflow is titled "Example: Exchange Online Write Message JSON as Note". It has the following configuration:

- 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

On the right side, there are details about the creator and last modified date, and a link to the associated rule. Below the form is a visual workflow diagram:

```

graph LR
    Start((Start your workflow here)) --> Task{Exchange Online: Get Message}
    Task -- "Input: email address and message id of message to get" --> Task
    Task -- "Output: the message is written to an incident note." --> End(( ))

```

The diagram shows a start node connected to a task node labeled "Exchange Online: Get Message". The task node has two outgoing arrows: one labeled "Input: email address and message id of message to get" and another labeled "Output: the message is written to an incident note.". Both arrows point to an end node.

► 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["exo_email_address"], results.inputs["exo_messages_id"], results.pretty_string)
row.exo_dt_status = "Not Found"
row..exo_dt_web_link = ""
else:
    noteText = u"Exchange Online email address: {0} message:\n{1}" .format(results.inputs["exo_email_address"], results.pretty_string)

incident.addNote(noteText)

```

► Example Rule:

The screenshot shows the Resilient platform's 'Rules' configuration screen. At the top, there is a navigation bar with links for Dashboards, Inbox, Incidents, Create, and a user profile for 'Resilient Sysadmin'. Below the navigation is a section titled 'Customization Settings' with tabs for Layouts, Rules, Scripts, Workflows, Functions, Message Destinations, Phases & Tasks, Incident Types, Breach, and Artifacts. The 'Rules' tab is selected. A breadcrumb trail indicates the current path: Rules / Example: Exchange Online Write Message JSON as Note. On the right side of the screen are three buttons: Cancel, Save & Close, and Save.

Display Name *: Example: Exchange Online Write Me

Object Type: Data Table: Exchange Online Message Query Results

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

Status: 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.
- 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.

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': {u'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":\n        "https://graph.microsoft.com/v1.0/$metadata#users/$entity",\n        "businessPhones": [],\n        "displayName": "Resilient User 2",\n        "givenName": "Resilient User 2",\n        "id": "393c1ebb-8222-4ba1-8665-f54eaf7f024f",\n        "jobTitle": null,\n        "mail": "resilient2@securitypocdemos.onmicrosoft.com",\n        "mobilePhone": null,\n        "officeLocation": null,\n        "preferredLanguage": "en-US",\n        "surname": "Resilient User 2",\n        "userPrincipalName": "resilient2@securitypocdemos.onmicrosoft.com"\n    },\n    'content': {\n        u'displayName': u'Resilient User 2',\n        u'mobilePhone': None,\n        u'preferredLanguage': u'en-US',\n        u'jobTitle': None,\n        u'userPrincipalName': u'resilient2@securitypocdemos.onmicrosoft.com',\n        u'@odata.context': u'https://graph.microsoft.com/v1.0/$metadata#users/$entity',\n        u'officeLocation': None,\n        u'businessPhones': [],\n        u'mail': u'resilient2@securitypocdemos.onmicrosoft.com',\n        u'surname': u'Resilient User 2',\n    }
}

```

```

        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, "userPrincipalName": "resilient2@securitypocdemos.onmicrosoft.com", "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity", "officeLocation": null, "businessPhones": [], "mail": "resilient2@securitypocdemos.onmicrosoft.com", "surname": "Resilient User 2", "givenName": "Resilient User 2", "id": "393c1ebb-8222-4ba1-8665-f54eaf7f024f"}},
        'reason': None,
        'version': '1.0'
}

```

► Workflows:

Customization Settings

Workflows / Example: Exchange Online Get User Profile

Name *	Example: Exchange Online Get User Profile	Creator	Resilient Sysadmin
API Name *	example_exchange_online_get_user_profile	Last Modified	01/02/2020 16:22
Description	This example workflow gets the Exchange Online user profile that matches the input email address and writes the information to a note.	Last Modified By	Resilient Sysadmin
Object Type *	Artifact	Associated Rules	Example: Exchange Online Get User Profile

Start your workflow here

```

graph LR
    Start(( )) --> Action{Exchange Online: Get User Profile}
    Action --> End(( ))
    
```

► 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.pretty_string)
else:
    noteText = u"Exchange Online user profile:
{0}\n{1}".format(results.inputs["exo_email_address"], results.pretty_string)

incident.addNote(noteText)

```

► Example Workflow Output:

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 ≡ ≡ ≡ A ⌘ ✖ ↶ ↷ 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* 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	👤 Resilient Sysadmin
Owner	👤 Resilient Sysadmin
Members	<i>There are no members.</i>

Related Incidents

#2101 Exchange Online demo

Attachments

There are no attachments.

► Example Rule:

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

The screenshot shows the Resilient platform's customization settings for a rule. The top navigation bar includes links for Dashboards, Inbox, Incidents, Create, and a user account for 'Resilient Sysadmin'. The main menu has tabs for Layouts, Rules, Scripts, Workflows, Functions, Message Destinations, Phases & Tasks, Incident Types, Breach, and Artifacts. The 'Rules' tab is selected, and the sub-page title is 'Example: Exchange Online Get User Profile'. On the right, there are buttons for Cancel, Save & Close, and Save.

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)

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 for a function. The top navigation bar includes links for Dashboards, Inbox, Incidents, Create, and a user account for 'Resilient Sysadmin'. The main menu has tabs for Layouts, Rules, Scripts, Workflows, Functions, Message Destinations, Phases & Tasks, Incident Types, Breach, and Artifacts. The 'Functions' tab is selected, and the sub-page title is 'exchange_online_move_message_to_folder'. On the right, there are buttons for Cancel, Save & Close, and Save.

Name *: Exchange Online: Move Message to Folder

API Name *: exchange_online_move_message_to_folder

Message Destination *: fn_exchange_online

Description: This function will move an Exchange Online message to the specified folder in the users mailbox.

Inputs

- exo_email_address
- exo_mailfolders_id
- exo_messages_id
- exo_destination_mailfolder_id

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_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': {u'exo_destination_mailfolder_id': {u'id': 126,
                                              u'name': u'recoverableitemsdeletions'},
             u'exo_mailfolders_id': None,
             u'exo_messages_id': u'AAMkAGFmNDE0ZDA1LTf0GMrNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEk
a4IVS4DBeEtMPuSEBwBJf-ANAwqcRJF4hFv_x44UAAAAAEMAABJf-ANAwqcRJF4hFv_x44UAAAxaS2qAAA=',
             u'exo_email_address': u'resilient2@securitypocdemos.onmicrosoft.com'},
  '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:

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

Customization Settings

Workflows / Example: Exchange Online Move Message to Folder

Name * Example: Exchange Online Move Message to Folder
API Name * example_exchange_online_move_message_to_folder
Description This workflow will move a row-entry message in the Exchange Online Message Query Results data table to the specified user mail folder.
Object Type * Data Table
Data table * Exchange Online Message Query Results

Creator Resilient Sysadmin
Last Modified 01/14/2020 10:07
Last Modified By Resilient Sysadmin
Associated Rules Example: Exchange Online Move Message to Folder

► Example Workflow Output:

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

SecurityPOCdemos

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 First Created By: 0 selected Date Created: All

Resilient Sysadmin added a note to the Incident 02/02/2020 22:42
 Exchange Online email address: resilient2@securitypocdemos.onmicrosoft.com

Message has been moved to folder: clutter

Old message ID: AAMkAGFmNDE0ZDA1LTfM0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEka4IVS4DBeEtMPuSEBwBJf-ANAwqcRJF4hFv_x44UAAAAAETAABJf-ANAwqcRJF4hFv_x44UAAinHiKAAA=

New message ID: AAMkAGFmNDE0ZDA1LTfM0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEka4IVS4DBeEtMPuSEBwBJf-ANAwqcRJF4hFv_x44UAAinByvAABJf-ANAwqcRJF4hFv_x44UAAinIROAAA=

► 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_email_address"], results.inputs["exo_messages_id"])
    status_text = u"""

{status}

".format(color="red",
    status="Not Found")
    row['exo_dt_status'] = helper.createRichText(status_text)
    row['exo_dt_web_link'] = ""

else:
    # When a message is moved it's ID changes, so update the new message ID into the data
    # table
    # The message status is still "Active" but the weblink is no longer valid, so make is
    # empty string.
    noteText = u"Exchange Online email address: {0}\n\n Message has been moved to folder:
    {1}\n\n Old message ID: {2} \n\n New message ID:
    {3}.".format(results.inputs["exo_email_address"],
    results.inputs["exo_destination_mailfolder_id"]["name"],
    results.inputs["exo_messages_id"], results.content["new_message_id"])
    row['exo_dt_message_id'] = results.content["new_message_id"]
    row['exo_dt_web_link'] = ref_html = u"""".format\(results.content\["new\_web\_link"\]\)
incident.addNote\(noteText\)

```

► Example Rule:

The screenshot shows the Resilient platform's 'Customization Settings' page for a rule. The rule is titled 'Example: Exchange Online Move Message to Folder'. The 'Rules' tab is selected. The 'Conditions' section contains a condition: 'Status' is 'is equal to' 'Active'. The 'Activities' section shows 'Ordered' and 'Workflows' activities, and the 'Destinations' section shows a 'Select Destinations' field.

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.

The screenshot shows the Resilient platform's 'Customization Settings' interface for a function. The function is named 'exchange_online_query_emails' and has an API name of 'exchange_online_query_emails'. It is associated with the 'fn_exchange_online' message destination. The description states: 'This function will query Exchange Online to find messages matching the specified input parameters. A list of messages is returned from the function.' The creator is 'Resilient Sysadmin' and it was last modified on 01/05/2020 at 13:36. Associated workflows include 'Example: Exchange Online Delete Messages From Query R', 'Example: Exchange Online Query Messages', and 'Example: Exchange Online Query Messages on Artifact'. The 'Inputs' section lists various parameters like exo_email_address, exo_email_folders, etc. The 'Input Fields' section lists fields such as exo_attachment_name, exo_destination_mailfolder_id, etc.

► 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
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': [{status_code': 200,
        'email_address': 'resilient2@securitypocdemos.onmicrosoft.com',
        'email_list': [{u'sentDateTime': '2020-02-04T20:44:02Z',
            'u'conversationId': 'AAQkAGFmNDE0ZDA1LTFmOGMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMAAQANIXI-VmHPNIslAVFC4yWrI=',
            'u'internetMessageId': '<MWHPR2201MB11359DA0C07AF09AB319DD9FB1030@MWHPR2201MB1135.namprd22.prod.outlook.com>',
            'u'id': 'AAMkAGFmNDE0ZDA1LTFmOGMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEka4IVS4DBeEtMPuSEBwBJf-ANAwqcRJF4hFv_x44UAAAAEJAABJf-ANAwqcRJF4hFv_x44UAAAAbtF2AAA=',
            'u'isReadReceiptRequested': False,
            'u'subject': 'lunch',
            'u'lastModifiedDateTime': '2020-02-04T20:44:04Z',
            'u'bodyPreview': "Let's have lunch at 12!",
            'u'from': {u'emailAddress': {u'name': 'Resilient User 2',
                'u'address': 'resilient2@securitypocdemos.onmicrosoft.com'}},
            'u'flag': {u'flagStatus': 'notFlagged'},
            'u'isDraft': False,
            'u'replyTo': [],
            'u'changeKey': 'CQAAABYAAABJf/ANAwqcRJF4hFv+x44UAAAAlac/G',
            'u'receivedDateTime': '2020-02-04T20:44:03Z',
            'u'parentFolderId': 'AQMKAGFmNDE0ZDA1LTFmOGMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMAAuAAAD_OSBJGuCFUuAwXhLTD7khAEASX-wDQMKnESReIRb-se0FAAAAgEJAAA',
            'u'body': {u'content': u'<html>\r\n<head>\r\n<meta http-equiv="Content-Type" content="text/html; charset=utf-8">\r\n<meta content="text/html; charset=iso-8859-1">\r\n<style type="text/css" style="display:none">\r\n<!--\r\nnp\r\n\t{margin-top:0;\r\n\tmargin-bottom:0}\r\n-->\r\n</style>\r\n</head>\r\n<body dir="ltr">\r\n<div style="font-family:Calibri,Arial,Helvetica,sans-serif; font-size:12pt; color:rgb(0,0,0)">\r\nLet's have lunch at 12!<br>\r\n</div>\r\n</body>\r\n</html>\r\n',
            'u'contentType': 'html',
            'u'isDeliveryReceiptRequested': False,
            'u'importance': 'normal',
            'u'toRecipients': [{u'emailAddress': {u'name': 'Resilient User 3',
                'u'address': 'resilient3@securitypocdemos.onmicrosoft.com'}}],
            'u'ccRecipients': [],
            'u'isRead': True,
            'u'categories': [],
            'u'sender': {u'emailAddress': {u'name': 'Resilient User 2',
                'u'address': 'resilient2@securitypocdemos.onmicrosoft.com'}},
            'u'createdDateTime': '2020-02-04T20:44:02Z',
            'u'webLink': 'https://outlook.office365.com/owa/?ItemID=AAMkAGFmNDE0ZDA1LTFmOGMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEka4IVS4DBeEtMPuSEBwBJf%2FANAwqcRJF4hFv%2Bx44UAAAAEJAABJf%2FANAwqcRJF4hFv%2Bx44UAAAAbtF2AAA%3D&exvsurl=1&viewmodel=ReadMessageItem',
            'u'conversationIndex': 'AQHV25vV0jEj9WYc80iyUBUULjJasg==',
            'u'hasAttachments': False,
            'u'bccRecipients': [],
            'u'inferenceClassification': 'focused',
            'u'odata.etag': 'W/"CQAAABYAAABJf/ANAwqcRJF4hFv+x44UAAAAlac/G"',
            'u'reason': None,
            'u'version': '1.0'
        }]}]
```

► Workflows:

Customization Settings

Workflows / Example: Exchange Online Query Messages

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

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

Cancel Save & Close Save

► 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.properties.exo_email_address_list

# 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 else rule.properties.exo_mailfolder_id
inputs.exo_email_address_sender = inputs.exo_email_address_sender if
rule.properties.exo_email_address_sender is None else
rule.properties.exo_email_address_sender
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_body is None else rule.properties.exo_message_body
inputs.exo_start_date = inputs.exo_start_date if
rule.properties.exo_start_date is None else rule.properties.exo_start_date
inputs.exo_end_date = inputs.exo_end_date if
rule.properties.exo_end_date is None else rule.properties.exo_end_date
inputs.exo_has_attachments = inputs.exo_has_attachments if
rule.properties.exo_has_attachments is None else rule.properties.exo_has_attachments
```

► Example Post-Process Script:

```
from java.util import Date

note = u"Exchange Online Query user:\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"""Link".format(email.webLink)
        message_row.exo_dt_web_link = helper.createRichText(ref_html)
    else:
        message_row.exo_dt_web_link = ""

    message_row.exo_dt_status = helper.createRichText("Active")

# If any email addresses where not found post a note
if len(note) > note_len:
    incident.addNote(note)

```

► Example Rule:

The screenshot shows the Resilient platform's 'Customization Settings' page for a rule. The rule is titled 'Example: Exchange Online Query Messages'. The 'Activities' section contains three items: 'Ordered' (described as 'Ordered Activities will be invoked in the order specified below. They include: Add Tasks, Run Script, and Set Field.'), 'Workflows' (described as 'Workflow Activities are started after all Ordered Activities complete.'), and 'Destinations' (described as 'Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.'). There is also a 'Select Destinations' button. At the bottom of the page, there is a copyright notice: '© 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 X

Email Address *

Mail Folder

Choose from at least one of the search criteria below:

Sender email address i

Start date/time i calendar icon

End date/time i calendar icon

Message Subject

Message Body

Has attachments i

Cancel Execute

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.

Customization Settings

Functions / exchange_online_send_message

Name * Exchange Online: Send Message

API Name * exchange_online_send_message

Message Destination * fn_exchange_online

Description This function will create a message and send to the specified recipients.

Creator Resilient Sysadmin

Last Modified 01/14/2020 12:47

Last Modified By Resilient Sysadmin

Associated Workflows Example: Exchange Online Send Message

Inputs

- exo_email_address
- exo_recipients
- exo_message_subject
- exo_message_body

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

    '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:

Customization Settings

Workflows / Example: Exchange Online Send Message

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

Cancel Save & Close Save

Start your Workflow here

Input: sender address, comma separated recipient addresses, message body and subject

Output: Incident Note indicating status of message sent.

f(w) Exchange Online: Send Message

► 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 = u"Exchange Online message sent\n  From: {0}\n  To: {1}\n  Subject: {2}\nBody: {3}".format(results.inputs["exo_email_address"], results.inputs["exo_recipients"], results.inputs["exo_message_subject"], results.inputs["exo_message_body"])
else:
    noteText = u"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:

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 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:

Resilient Dashboards ▾ Inbox Incidents **Create** Resilient Sysadmin ▾

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.

[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:

Example: Exchange Online Send Message

Message Sender Address *

Message Recipient Addresses * ⓘ

Message Subject ⓘ

Message Body ⓘ

Sans Serif ▾ Normal ▾ B I U S E E = A A ⌂ W ▾

Cancel Execute

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

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.

Inputs

incident_id
task_id
exo_email_address
exo_messages_id
exo_attachment_name

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

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

► Inputs:

Name	Type	Required	Example	Tooltip
------	------	----------	---------	---------

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'AAMkAGFmNDE0ZDA1LTf0GMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAAAAD45IEka4IVS4DBeEtMPuSEBwB
Jf-ANAwqcRJF4hFv_x44UAAAinByvAABJf-ANAwqcRJF4hFv_x44UAAAinIROAAA=',
                     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:

```

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:

Customization Settings

Display Name * Example: Exchange Online Write 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](#)

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.

SecurityPOCdemos

Description

No description.

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

Edit

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	AAMkAGFmNDE0ZDA1LTNmOGMtNGU2MS04Y2IwLTJhMmViNWU3Y2VhMABGAAA AAAD45IEka4IVS4DBeEtMPuSEBwBjf-ANAwqcRJF4hFv_x44UAaaaaaaEJAABJf-ANAwqcRJF4hFv_x44UAAlbtF2AAA=
02/03/2020 14:37:48	2020-02-04 T20:44:03Z	resilient3@securitypocdemos.onmicrosoft.com	resilient2@securitypocdemos.onmicrosoft.com	lunch	No	Link	Active	AAMkADZkZDY2NTRILWQwNjgtNDMxZi1iYTA2LTQ0ZmYxN2UwMjhzmZQBGAaaaaCPU6DCGu7Sa2kl4jnbcnuBwCU6ehSHWGRTqkx2knKE-6AAAAAAEMAACU6ehSHWGRTqkx2knKEQ-6AAALRtgQAAA=

API Name:

`exo_message_query_results_dt`

Columns:

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

Rules

Rule Name	Object	Workflow Triggered
Example: Exchange Online Write Message JSON as Note	<code>exo_message_query_results_dt</code>	<code>example_exchange_online_get_message</code>
Example: Exchange Online Send Message	<code>incident</code>	<code>example_exchange_online_send_message</code>
Example: Exchange Online Get User Profile	<code>artifact</code>	<code>example_exchange_online_get_user_profile</code>
Example: Exchange Online Delete Messages from Query Results	<code>incident</code>	<code>example_exchange_online_delete_messages_from_query_results</code>

Rule Name	Object	Workflow Triggered
Example:		
Exchange		
Online Move	exo_message_query_results_dt	example_exchange_online_move_message_to_folder
Message to Folder		
Example:		
Exchange		
Online Query	artifact	example_exchange_online_query_emails
Messages on Artifact		
Example:		
Exchange		
Online Write	exo_message_query_results_dt	example_exchange_online_write_message_as_attachment
Message EML as		
Attachment		
Example:		
Exchange		
Online Query	incident	example_exchange_online_query_messages_of_a_group
Messages		
Example:		
Exchange		
Online Create	incident	example_exchange_online_create_meeting
Meeting		
Example:		
Exchange		
Online Create	exo_message_query_results_dt	-
Artifacts		
Example:		
Exchange		
Online Delete	exo_message_query_results_dt	example_exchange_online_delete_email
Message		