ThreatQuotient

ThreatQ CDF for Microsoft Exchange

Version 1.0.0

August 19, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.29.0
Compatible with Microsoft Deployments	• Cloud • On-Prem with Hybrid Authentication
Support Tier	ThreatQ Supported

Introduction

The Microsoft Exchange CDF for ThreatQ is an integration that enables the ingestion of emails and attachments from an Exchange Mailbox, into ThreatQ.

The integration provides the following feed:

- **Microsoft Exchange Intel Mailbox** - ingests emails from Microsoft Exchange/Outlook mailbox as ThreatQ Email.

The integration ingests the following system objects:

- Events
- Files (attachments)
- Indicators

Prerequisites

The following is required to run the integration:

- A Microsoft Azure-Cloud Office365 Exchange License/Account
- Microsoft Azure App Credentials and Permissions

Generating Azure OAuth Credentials

In order to use this integration, you *must* be using Microsoft Azure-Cloud Office365 Exchange. This integration *does not work* with any on-premise deployments of Office365 Exchange. This means, your Microsoft account needs to be within an Azure-Cloud Tenant that has access to Office365 Exchange.

Below are the steps for creating an App Registration with the correct permissions for this integration:

1. Login to `https://portal.azure.com` as an Administrator.
2. Navigate to the `App registrations` Azure service.
3. Click on the `New registration` button to register a new App.
4. For the **Name**, enter `ThreatQ Mail Integration`.
5. For the **Supported account types**, select the first option, `Accounts in this organizational directory only`.
6. Skip the **Redirect URI** field and click `Register`.
7. On the `Overview` page for your App, copy your `Directory (tenant) ID` and your `Application (client) ID` to a secure location.
8. Click on the `API permissions` tab on the left sidebar.
9. Click on the `Add a permission` button and add the following permissions under the `Microsoft Graph` API (Type: Application): - Mail.Read - Mail.ReadBasic - MailBasic.All
10. Make sure to `Grant admin consent` for your Organization
11. Click on the `Certificates & secrets` tab on the left sidebar.
12. Click on the `New client secret` button and create a new secret with any name and expiration
    - Note: When the token expires, the integration will not work until a new token is applied.
13. Copy the new client secret `value` (not the Secret ID) to a secure location (with the other credentials you saved).

You will now use the `Tenant ID`, `Client ID`, and `Client Secret` with this integration.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the file on your local machine

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. The feed will be added to the integrations page. You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

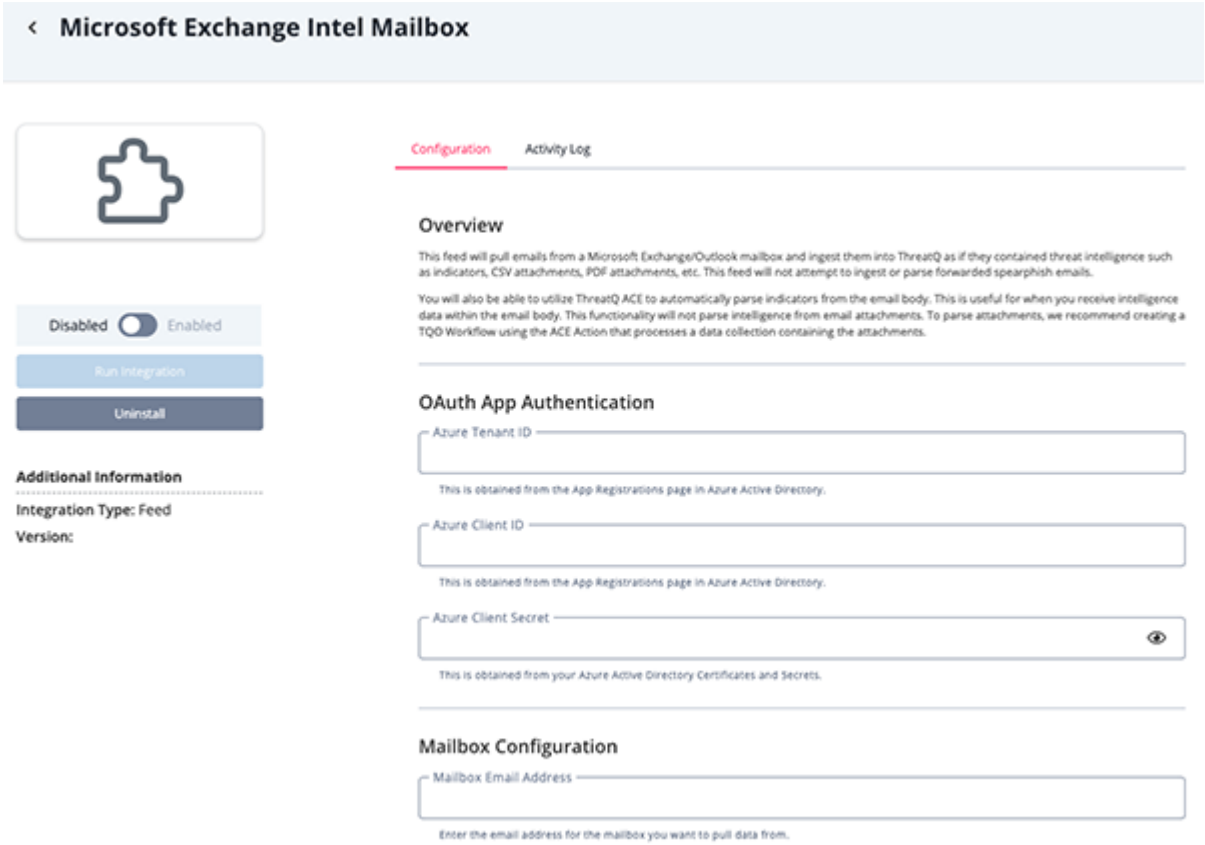
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Tenant ID	Enter your Tenant ID found under the App Registrations page in Azure Active Directory. See the Generating Azure OAuth Credentials section for more details.
Client ID	Enter your Client ID found under the App Registrations page in Azure Active Directory. See the Generating Azure OAuth Credentials section for more details.
Client Secret	Enter your Client Secret found under the **Azure Active Directory Certificates and Secrets**. See the Generating Azure OAuth Credentials section for more details.
Mailbox Email Address	Enter the email address for the mailbox you want to pull data from.
Folder Name	Enter the name of the folder you want to pull data from.
Strip HTML from Email Body	Enable this option to strip any HTML formatting from the email body.

PARAMETER	DESCRIPTION
Ingest Attachments	Enable this option to ingest email attachments into ThreatQ. This option is enabled by default.
Require Attachments	Enable this option to only ingest emails that include at least one attachment. This option is disabled by default.
Malware Lock Attachments	Enable this option to protect attachments with a malware lock once ingested into ThreatQ. This option is enabled by default.
Ignored Attachment MIME Types	Enter a comma-separated list of MIME types to ignore when ingesting attachments. The default value is: `image/png,image/jpeg,image/jpg,image/gif,image/bmp,image/tiff`.
Parse Indicators from Email Body	Enable this option to use ThreatQ ACE to parse IOCs from the email body. **Caution, since this will be parsing unstructured data, it may not always be accurate, and may result in false positives. Always ingest IOCs into the Review state.**
Parsed Indicator Types	Select which indicator types to parse the email body for. This field will only display if the **Parse Indicators from Email Body** option is enabled. Options include: ◦ MD5 (default) ◦ SHA-1 (default) ◦ SHA-256 (default) ◦ SHA-384 ◦ SHA-512 (default) ◦ IP Address (default) ◦ CIDR Block ◦ FQDN ◦ URL ◦ CVE (default) ◦ Email Address ◦ Filename ◦ File Path



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Microsoft Exchange Intel Mailbox

The Microsoft Exchange Intel Mailbox feed pulls emails from a Microsoft Exchange/Outlook mailbox and ingest them into ThreatQ as if they contained threat intelligence such as indicators, CSV attachments, PDF attachments, etc. This feed will not attempt to ingest or parse forwarded spearphish emails.

You will also be able to utilize ThreatQ ACE to automatically parse indicators from the email body. This is useful for when you receive intelligence data within the email body. This functionality will not parse intelligence from email attachments. To parse attachments, we recommend creating a TQO Workflow using the ACE Action that processes a data collection containing the attachments.

`GET https://graph.microsoft.com/v1.0/users/{{ mailbox_address }}/mailFolders/{{ folder_id }}/messages`

Sample Response:


```
{
  "@odata.context": "https://graph.microsoft.com/
v1.0/$metadata#users('threatq%40threatq.onmicrosoft.com')/mailFolders/Inbox/
messages",
  "value": [
    {
      "@odata.etag": "W/\"CQAAABYAAABlpCmrska5TqIMPpjD6wUjAAGCPCps\"",
      "id":
"AAMkADAwMzYwMmI0LTAyMjAtNGRmOS05OTAyLTM4ODEzODdmMDY3MgBGAAAAAAAwQJ--
D9f2QZgyDjTFwH1rBwBlpCmrska5TqIMPpjD6wUjAAAAAAEMAABlpCmrska5TqIMPpjD6wUjAAGCK85
yAAA=",
      "createdDateTime": "2022-09-06T16:15:36Z",
      "lastModifiedDateTime": "2022-09-06T16:20:38Z",
      "changeKey": "CQAAABYAAABlpCmrska5TqIMPpjD6wUjAAGCPCps",
      "categories": [],
      "receivedDateTime": "2022-09-06T16:15:37Z",
      "sentDateTime": "2022-09-06T16:15:23Z",
      "hasAttachments": true,
      "internetMessageId": "fe7f78eb-9799-4358-8689-728c5f17a10f@Spark>",
      "subject": "Microsoft unusual account activity",
      "bodyPreview": "We've detected some unusual activity on your Microsoft
account!\r\n\r\n\r\n\r\n\r\nAccount:\r\nacme@roadrunner.com",
      "importance": "normal",
      "parentFolderId":
"AAMkADAwMzYwMmI0LTAyMjAtNGRmOS05OTAyLTM4ODEzODdmMDY3MgAuAAAAAAAwQJ--
D9f2QZgyDjTFwH1rAQBlpCmrska5TqIMPpjD6wUjAAAAAAEMAAA=",
      "conversationId":
"AAQkADAwMzYwMmI0LTAyMjAtNGRmOS05OTAyLTM4ODEzODdmMDY3MgAQAI6FEMPhN1lFhPdM6oLfsBU=",
      "conversationIndex": "AQHYwgvljoUQw+E3WUWE90zqgt+wFQ==",
```

```
      "isDeliveryReceiptRequested": null,
      "isReadReceiptRequested": false,
      "isRead": false,
      "isDraft": false,
      "webLink": "https://outlook.office365.com/owa/?
ItemID=AAMkADAwMzYwMmI0LTAyMjAtNGRmOS05OTAyLTM4ODEzODdmMDY3MgBGAAAAAAAwQJ%2F%2F
D9f2QZgyDjTFwH1rBwBlpCmrska5TqIMPpjD6wUjAAAAAAEMAABlpCmrska5TqIMPpjD6wUjAAGCK85
yAAA%3Dexvsurl=1viewmodel=ReadMessageItem",
      "inferenceClassification": "focused",
      "body": {
        "contentType": "html",
        "content": "[redacted]"
      },
      "sender": {
        "emailAddress": {
          "name": "ThreatQ User",
          "address": "threatq@threatq.com"
        }
      },
      "from": {
        "emailAddress": {
          "name": "ThreatQ User",
          "address": "threatq@threatq.com"
        }
      },
      "toRecipients": [
        {
          "emailAddress": {
            "name": "ThreatQ User",
            "address": "threatq@threatq.onmicrosoft.com"
          }
        }
      ],
      "ccRecipients": [],
      "bccRecipients": [],
      "replyTo": [],
      "flag": {
        "flagStatus": "notFlagged"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.subject`	Event Title	Email	`.receivedDateTime`	Microsoft unusual account activity	N/A
`.receivedDateTime`	Event Happened At	N/A	N/A	2022-09-06T16:15:37Z	N/A
`.categories`	Event Tags	N/A	N/A	N/A	N/A
`.body.content`	Event Description	N/A	N/A	N/A	HTML tags are removed if `Strip HTML from Email Body` is enabled.
`.body.content`	Event Related Indicators	N/A	N/A	N/A	Indicators are parsed from the email body.
`.importance`	Event Attribute	Importance	`.receivedDateTime`	Normal	Title cased. Updated at ingestion.
`.hasAttachments`	Event Attribute	Has Attachments	`.receivedDateTime`	True	N/A
`.flag.flagStatus`	Event Attribute	Flag Status	`.receivedDateTime`	N/A	If value does not equal `notFlagged`. Updated at ingestion.
`.flag.dueDateTime.dateTime`, `.flag.dueDateTime.timeZone`	Event Attribute	Due Date	`.receivedDateTime`	N/A	Values are concatenated. Updated at ingestion.
`.sender[].emailAddress.name`, `.sender[].emailAddress.address`	Event Attribute	Sender	`.receivedDateTime`	ThreatQ User threatq@threatq.com	It can be a list or a mapping. Values are concatenated.
`.toRecipients[].emailAddress.name`, `.toRecipients[].emailAddress.address`	Event Attribute	Recipient	`.receivedDateTime`	ThreatQ User threatq@threatq.onmicrosoft.com	It can be a list or a mapping. Values are concatenated.
`.ccRecipients[].emailAddress.name`, `.ccRecipients[].emailAddress.address`	Event Attribute	CC Recipient	`.receivedDateTime`	N/A	It can be a list or a mapping. Values are concatenated.
`.bccRecipients[].emailAddress.name`, `.bccRecipients[].emailAddress.address`	Event Attribute	BCC Recipient	`.receivedDateTime`	N/A	It can be a list or a mapping. Values are concatenated.
`.replyTo[].emailAddress.name`, `.replyTo[].emailAddress.address`	Event Attribute	Reply To	`.receivedDateTime`	N/A	It can be a list or a mapping. Values are concatenated.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.from.emailAddress.name`, `.from.emailAddress.address`	Event Attribute	From	`.receivedDateTime`	ThreatQ User threatq@threatq.com	Values are concatenated.

Microsoft Graph - List Message Attachments (Supplemental)

The Microsoft Graph - List Message Attachments Supplemental feed fetches the attachments associated with a given email message.

`GET https://graph.microsoft.com/v1.0/users/{{ mailbox_address }}/messages/{{ message_id }}/attachments`

Sample Response:


```
{
  "@odata.context": "https://graph.microsoft.com/
v1.0/$metadata#users('threatq%40threatq.onmicrosoft.com')/
messages('AAMkADAwMzYwMmI0LTAyMjAtNGRmOS05OTAyLTM4ODEzODdmMDY3MgBGAAAAAAAwQJ--
D9f2QZgyDjTFwH1rBwBlpCmrska5TqIMPpjD6wUjAAAAAAEMAABlpCmrska5TqIMPpjD6wUjAAGCK85
1AAA%3D')/attachments",
  "value": [
    {
      "@odata.type": "#microsoft.graph.fileAttachment",
      "@odata.mediaContentType": "image/png",
      "id":
"AAMkADAwMzYwMmI0LTAyMjAtNGRmOS05OTAyLTM4ODEzODdmMDY3MgBGAAAAAAAwQJ--
D9f2QZgyDjTFwH1rBwBlpCmrska5TqIMPpjD6wUjAAAAAAEMAABlpCmrska5TqIMPpjD6wUjAAGCK85
1AAABEgAQAJL_haQBRm9CqUy8CLwnv_A=",
      "lastModifiedDateTime": "2022-09-07T15:15:35Z",
      "name": "899A338D9CB24C1EBA6C2A45762C8222.png",
      "contentType": "image/png",
      "size": 10665,
      "isInline": true,
      "contentId": "899A338D9CB24C1EBA6C2A45762C8222",
      "contentLocation": null
    },
    {
      "@odata.type": "#microsoft.graph.fileAttachment",
      "@odata.mediaContentType": "application/octet-stream",
      "id":
"AAMkADAwMzYwMmI0LTAyMjAtNGRmOS05OTAyLTM4ODEzODdmMDY3MgBGAAAAAAAwQJ--
D9f2QZgyDjTFwH1rBwBlpCmrska5TqIMPpjD6wUjAAAAAAEMAABlpCmrska5TqIMPpjD6wUjAAGCK85
1AAABEgAQAGvKvdg3sj9Htr1-cXU271k=",
      "lastModifiedDateTime": "2022-09-07T15:15:35Z",
      "name": "Test.eml",
      "contentType": "application/octet-stream",
      "size": 27409,
      "isInline": false,
```

```
      "contentId":
"D3A9DCB82C56334F8C4F507EC8B2C438@namprd06.prod.outlook.com",
      "contentLocation": null
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

> The mapping for this feed is based on each item within the `.value[]` list of items from the API response

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.name`	Attachment Title	Email Attachment	`.lastModifiedDateTime`	N/A	N/A
`.parent_values[].id, .name`	Attachment Name	N/A	N/A	N/A	Message ID & Attachment name are concatenated
`.user_fields.malware_lock`	Attachment Malware Lock	N/A	N/A	N/A	User config field
`.contentType`	Attachment MIME Type	N/A	N/A	`application/octet-stream`	N/A

Microsoft Graph - Get Raw Attachment (Supplemental)

The Microsoft Graph - Get Raw Attachment Supplemental feed fetches the raw attachment content/bytes for attachments in an email. This supplemental feed allows us to upload attachments to the ThreatQ platform.

```
GET https://graph.microsoft.com/v1.0/users/{{ mailbox_address }}/messages/{{ message_id }}/$value
```

Average Feed Run

Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Microsoft Exchange Intel Mailbox

METRIC	RESULT
Run Time	1 minute
Events	2
Event Attributes	40

Known Issues / Limitations

- When parsing IOCs from the intelligence imported from the Intel Mailbox feed, attachments will not be parsed for IOCs. Only the main email body will be parsed.
- To parse IOCs from attachments, create a TQO Workflow using the ThreatQ ACE Action that will process a data collection containing the attachments.

Change Log

- **Version 1.0.0**
  - Initial release