



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Message Trace Rest API SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Configuration Guide for Message Trace Rest API SmartConnector 8.4.3

This guide provides information to install the SmartConnector for Message Trace Rest API and configure the end point for event collection. For supported devices and versions, see [Technical Requirements for SmartConnector](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

Message tracking or message tracing, as it is called in Office 365, is one of the most basic tools used by administrators to monitor the email flow. As emails travel through Office 365, some information about them gets stored in logs and is available for administrative purposes. Even if users delete or purge messages, the administrator is able to view basic information about sent and received emails.

Message tracing does not allow you to view a message's content. However, it can provide a lot of important data about the message, such as the following:

- Sender and recipient
- Sent and received dates
- Subject and size
- Delivery status and details of events, which include:
 - Delivered
 - Failed
 - Pending
 - Expanded
 - Quarantined
 - Filtered as spam
 - Unknown
- IP address used to send the message
- Message ID, a unique number identifying a message. If a message has more than one recipient, the message tracing tool logs an entry for every recipient of the message. Each of these entries has the same Message-ID but a different Message Trace ID in the message trace search.

Installing the Connector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Preparing to Install the Connector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the Connector, do the followings:

- In the [Azure portal](#), create an Azure AD App Registration to receive the events from Office 365 message trace REST API.
- Assign your application the **Global Reader** role to enable an access to the Reporting Web Service.
- Add the **ReportingWebService.Read.All** permission to the application.
- Generate **Client ID** and **Client Secrets**.

Installing and Configuring the Connector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. From the **Type** drop-down menu, select **Message Trace REST API** as the type of connector, and then click **Next**.
5. Enter the following parameters to configure the connector, and then click **Next**:

Parameter	Description
Proxy Host (https)	(Optional) If proxy is enabled for your machine, the IP address or host name of the proxy server required for proxy configuration to access the internet.
Proxy Port	(Optional) If proxy is enabled for your machine, the port number of the proxy server required for proxy configuration.
Proxy User Name	(Optional) If proxy is enabled for your machine, the user name for the proxy server. Specify this value only if proxy needs access to the Internet. If you enter the proxy user name, you must provide the proxy password.
Proxy Password	(Optional) If proxy is enabled for your machine, the password for the proxy server user. Specify this value only if proxy needs access to internet and you have specified a user name for the proxy server.
Event URL	This is a mandatory field. The URL from where you need to fetch events. The default value is: https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MessageTrace

Authentication Type	<p>This is a mandatory field.</p> <p>An authentication method to secure REST APIs. You can select either Basic or OAuth2-Client Credentials for the authentication in message trace REST API.</p> <p>The default value is: Basic</p>
Application (Client) ID	<p>The client application ID assigned to your app.</p> <p>This is a mandatory field when you select the Authentication Type parameter value as OAuth2-Client Credentials.</p>
Client Secret	<p>The client secret key generated for your app in the registration portal.</p> <p>This is a mandatory field when you select the Authentication Type parameter value as OAuth2-Client Credentials.</p>
Token URL	<p>The URL to get access token.</p> <p>This is a mandatory field when you select the Authentication Type parameter value as OAuth2-Client Credentials.</p> <p>The default value is: https://login.microsoftonline.com/<tenant_id>/oauth2/v2.0/token In this URL, <tenant_id> is the directory tenant ID in the GUID or domain-name format, against which the application will operate.</p>
Scope	<p>This is a mandatory field when you select the Authentication Type parameter value as OAuth2-Client Credentials.</p> <p>The URL to identify scope. API users will be asked to consent to all of the configured permissions present on the Azure AD App Registration for the respective resource (for example: https://reports.office365.com).</p> <p>The default value is: https://outlook.office365.com/.default</p>
User Name	<p>The user name for the Office 365 server with administrative permissions.</p> <p>This is a mandatory field when you select the Authentication Type parameter value as Basic.</p>
Password	<p>The password for the Office 365 user.</p> <p>This is a mandatory field when you select the Authentication Type parameter value as Basic.</p>

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.

 **Note:** If you select **Do not import the certificate to connector from destination**, the connector installation will end.

9. Select whether you need to run the connector as a service or in the standalone mode.
10. Complete the installation.

11. [Run the SmartConnector.](#)
12. For instructions about upgrading the connector or modifying its parameters, see [Installation and User Guide for SmartConnector.](#)

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device-specific event definitions. For more information about the ArcSight data fields, refer to the [ArcSight Console User's Guide for ESM](#).

ArcSight ESM Field	Device-Specific Field
Destination Address	ToIP
Device Product	'Exchange Online'
External Id	MessageTraceId
Name	Both('Message ',Status)
Source Address	FromIP
Source User Name	SenderAddress
Destination User Name	RecipientAddress
Device Custom String 3	Subject
Device Custom String 6	Organization
Device Event Class Id	Both('Message ',Status)
Device Receipt Time	Received
Device Vendor	'Microsoft'
File Id	MessageId
File Size	Size

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Message Trace Rest API SmartConnector (SmartConnectors 8.4.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!