



# ArcSight SmartConnectors

Software Version: 25.1.1

## Configuration Guide for Microsoft Office 365 Management Activity SmartConnector

Document Release Date: April 2025

Software Release Date: April 2025

## Legal Notices

Open Text Corporation

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

## Copyright Notice

Copyright 2025 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>

# Contents

Configuration Guide for Microsoft Office 365 Management Activity SmartConnector .....	5
Product Overview .....	6
Supported Audit Log Record Types .....	6
Microsoft Office 365 Event Retrieval Configuration .....	8
Register the SmartConnector Application with Microsoft Entra ID .....	8
Generate Keys and Configure the Application Properties .....	9
Specify the Permissions the Connector Application Requires to Access the Office 365 Management Activity API .....	10
Limitations of the Microsoft Management Activity API .....	10
Specify Permissions in Microsoft Management Activity API .....	10
Install the SmartConnector .....	11
Prepare to Install Connector .....	11
Install Core Software .....	12
Set Global Parameters (optional) .....	12
Select Connector and Add Parameter Information .....	13
Select a Destination .....	15
Complete Installation and Configuration .....	15
Run the SmartConnector .....	16
Device Event Mapping to ArcSight Fields .....	16
Azure AD Common Mappings to ArcSight Fields .....	16
Azure AD Account Logon Mappings to ArcSight Fields .....	17
Azure AD Other Mappings to ArcSight Fields .....	17
Compliance Exchange Mappings to ArcSight Fields .....	18
CRM Mappings to ArcSight Fields .....	18
Data Insights REST API Mappings to ArcSight Fields .....	18
Discovery Mappings to ArcSight Fields .....	19
Exchange Online Admin Mappings to ArcSight Fields .....	19
Exchange Online DPL Mappings to ArcSight Fields .....	20
Exchange Online Mailbox Mappings to ArcSight Fields .....	20
Exchange Online Mailbox Item Mappings to ArcSight Fields .....	21
Exchange Online Mailbox Item Group Mappings to ArcSight Fields .....	21
Microsoft Teams Mappings to ArcSight Fields .....	22
(Office 365 Advanced Threat Protection) Threat Intelligence Mappings to ArcSight Fields .....	22
Microsoft Flow Mappings to ArcSight Fields .....	23
Advanced eDiscovery Mappings to ArcSight Fields .....	23

Project Mappings to ArcSight Fields .....	24
Security and Compliance Center to ArcSight Fields .....	24
Security and Compliance Center EOP Cmdlet Mappings to ArcSight Fields .....	24
Security and Compliance Alert Signals to ArcSight Fields .....	25
(Office 365 Advanced Threat Protection) Threat Intelligence Url to ArcSight Fields .....	25
Power Apps to ArcSight Fields .....	26
(Office 365 Advanced Threat Protection) Threat Intelligence Atp Content to ArcSight Fields .....	26
Microsoft Office 365 Common Mappings to ArcSight Fields .....	27
Power BI Audit Mappings to ArcSight Fields .....	28
SharePoint Online Common Mappings to ArcSight Fields .....	28
SharePoint Online and One Drive for Business List Mappings to ArcSight Fields ....	28
SharePoint Online and One Drive for Business File Mappings to ArcSight Fields ...	29
SharePoint Online Other Mappings to ArcSight Fields .....	29
SharePoint Online DLP Mappings to ArcSight Fields .....	30
SharePoint Online Sharing Mappings to ArcSight Fields .....	30
Sway Mappings to ArcSight Fields .....	31
Skype For Business Mappings to ArcSight Fields .....	31
Yammer Mappings to ArcSight Fields .....	31
Troubleshooting .....	32
Send Documentation Feedback .....	33

# Configuration Guide for Microsoft Office 365 Management Activity SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Office 365 and configuring the connector for event collection. Event collection is supported for Microsoft SharePoint Online, Exchange Online, Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) and OneDrive.

This guide provides a high level overview of ArcSight SmartConnectors for the Cloud.

## 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](#).

## 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](mailto:MFI-Documentation-Feedback@opentext.com).

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

## Product Overview

Microsoft Office 365 refers to subscription plans that include access to Office 365 applications that are enabled over the Internet (cloud services). Use the Microsoft Office 365 connector to retrieve information about user, admin, system, and policy actions and events from Microsoft Office 365 and Microsoft Entra ID activity logs. You can use the actions and events from the Office 365 and Microsoft Entra ID audit and activity logs to create solutions that provide monitoring, analysis, and data visualization. These solutions give organizations greater visibility into actions taken on their content.

For complete information about Microsoft Office 365, see the Microsoft website for Microsoft Office 365 documentation.

## Supported Audit Log Record Types

The SmartConnector for Microsoft Office 365 supports the following Audit Log Record Types:

Value	Member Name	Description
1	ExchangeAdmin	Events from the Exchange Online admin audit log.
2	ExchangeItem	Events from an Exchange Online mailbox audit log for actions that are performed on a single item, such as creating or receiving an email message.
3	ExchangeItemGroup	Events from an Exchange Online mailbox audit log for actions that can be performed on multiple items, such as moving or deleting one or more email messages.
4	SharePoint	Sharepoint Online events.
6	SharePointFileOperation	Sharepoint Online file operation events.
8	AzureActiveDirectory	Azure Active Directory events.
9	AzureActiveDirectoryAccountLogon	Azure Active Directory OrgId logon events (deprecating).
10	DataCenterSecurityCmdlet	Data Center security cmdlet events.
11	ComplianceDLPSharePoint	Data loss protection (DLP) events in SharePoint and OneDrive for Business.
12	Sway	Events from the Sway service and clients.
13	ComplianceDLPEXchange	Data loss protection (DLP) events in Exchange, when configured via Unified DLP Policy. DLP events based on Exchange Transport Rules are not supported.

Value	Member Name	Description
14	SharePoint Sharing Operation	SharePoint Online sharing events.
15	AzureActiveDirectoryStsLogon	Secure Token Service (STS) logon events in Azure Active Directory.
18	SecurityComplianceCenterEOPCmdlet	Admin actions from the Security and Compliance Center.
20	PowerBIAudit	Power BI events.
21	CRM	Microsoft CRM events.
22	Yammer	Yammer events.
23	Skype for Business CMDlets	Skype for Business events.
24	Discovery	Events for eDiscovery activities performed by running content searches and managing eDiscovery cases in the Security and Compliance Center.
25	Microsoft Teams	Events for Microsoft Teams.
28	ThreatIntelligence	Phishing and malware events from Exchange Online Protection and Office 365 Advanced Threat Protection.
30	MicrosoftFlow	Microsoft Power Automate (formerly called Microsoft Flow) events.
31	AeD	Advanced eDiscovery events.
33	Compliance DLP SharePoint Classification	Events related to DLP classification in SharePoint.
35	Project	Microsoft Project events.
36	SharePointListOperation	SharePoint List events.
38	DataGovernance	Events related to retention policies and retention labels in the Security and Compliance Center.
40	SecurityComplianceAlerts	Security and compliance alert signals.
41	ThreatIntelligenceUrl	Safe links time-of-block and block override events from Office 365 Advanced Threat Protection.
45	PowerAppsApp	Power Apps events
47	ThreatIntelligenceAtpContent	Phishing and malware events for files in SharePoint, OneDrive for Business, and Microsoft Teams from Office 365 Advanced Threat Protection.
52	DataInsightsRestApiAudit	Data Insights REST API events.
55	SharePointContentTypeOperation	SharePoint list content type events.

Value	Member Name	Description
56	SharePointFieldOperation	SharePoint list field events.
57	MicrosoftTeamsAdmin	Teams admin events.
68	ComplianceSupervisionExchange	Events tracked by the Communication compliance offensive language model.

See Microsoft documentation about Audit Log Record Types at:

<https://msdn.microsoft.com/en-us/library/office/mt607130.aspx#AuditLogRecordType>

## Microsoft Office 365 Event Retrieval Configuration

The Office 365 connector uses the Office 365 Management Activity API which is a RESTful web service. The API relies on Microsoft Entra ID (formerly known as Azure Active Directory or Azure AD) and the OAuth2 protocol for authentication and authorization. To allow the connector to access the API, you must first register it in Microsoft Entra ID and configure it with appropriate permissions.

### Register the SmartConnector Application with Microsoft Entra ID

The following configuration procedures allow you to establish an identity for the SmartConnector and specify the permission levels it needs to access the Management Activity API. Before registering the SmartConnector application with Microsoft Entra ID, the following prerequisites must exist:

- An Office 365 account must be enabled and configured.
- The Office 365 subscription must be associated with Microsoft Entra ID tenant domain account.

For more details, see [Associate your Office 365 account with Azure AD to create and manage apps](#).

#### To register your SmartConnector application in Microsoft Entra ID:

After you have a Microsoft tenant with the proper subscriptions, you can register your SmartConnector application in Microsoft Entra ID.

1. Log in to the [Microsoft Azure portal](#) using the credentials of your Microsoft tenant that has the subscription to Office 365 you wish to use.



2. From the Azure portal menu, select **Microsoft Entra ID**.
3. In the left pane, click **Manage > Custom domain names**, and then click **Add custom domain** to add your custom domain name.
4. Enter **Custom domain name** in the box and click **Add Domain**. Verify domain details and click **Verify**.

**APP ID URI:** The URI is used as a unique logical identifier for your app. It must be a verified custom domain name used for external user to grant app access to their data in Windows Azure AD. This parameter is not required by the connector but it is required by Microsoft Entra ID to register the SmartConnector as a client application.

5. In the left pane, click **Manage > App registrations**, and then click **New registration**.
6. Enter a logical **Name**, **Supported account types**, and **Redirect URI (Optional)**.
7. Click **Register**.

The **Application (client) ID** is generated automatically. You may copy this ID somewhere to use the same while configuring the SmartConnector.

**SIGN-ON URL:** This parameter is not required by the SmartConnector, but it is required by Microsoft Entra ID to register the SmartConnector as a client application. This value must be configured. You may want to configure this with any URL path that is not in use by any of your other applications. You can change this later as needed.

Your SmartConnector application is now registered with Microsoft Entra ID and has been assigned with a client ID. However, there are several aspects of your SmartConnector application left to configure.

For more information about registering an app, see [Register an app by using the Azure portal](#) section in Microsoft documentation.

## Generate Keys and Configure the Application Properties

After the SmartConnector application is registered, there are several important properties you must specify that determine how your SmartConnector application functions within Microsoft Entra ID.

### To generate keys and configure the application properties:

1. On the App registration page, in the **Display name** column, select your application for which you want to create the certificate and secret.
2. On the app details page, do any of the following:
  - Look for the **Client credentials** field and click **<x> certificate, <y> secret** where -  
 <x> = the number of certificates and  
 <y> = the number of secrets

For example: 0 certificate, 1 secret or 2 certificates, 2 secrets.

- In the left pane, click **Manage > Certificate & secrets**.
3. In the **Certificate & secrets** page, on the **Client secrets** tab, click **New client secret**.
  4. In the Add a client secret window, enter the description for the client secret.
  5. In the **Expires** list, select an expiration for the secret or select **Custom** for lifetime.
  6. Enter start date and end date, and then click **Add**.

The client secret value is automatically generated by Microsoft Entra ID and is displayed in the **Value** column

7. Click the highlighted **Clipboard** icon to copy the client secret value and save it somewhere so that it can be used to configure the SmartConnector during the SmartConnector installation.



**Important:** You must copy the client secret value because you will not be able to retrieve it after you leave this page.

## Specify the Permissions the Connector Application Requires to Access the Office 365 Management Activity API

You need to specify the appropriate permissions your SmartConnector application requires of the Office 365 Management Activity API. To do so, you must add access to the Office 365 Management APIs to your SmartConnector application, and then you specify the required permission(s).

### Limitations of the Microsoft Management Activity API

The maximum lifespan of events available from the Microsoft Management Activity API is seven days.

When the SmartConnector is first started, it can take up to 12 hours for the first events to become available from the Management Activity API. The events may also appear out of order. This is due to the limitation of the Management Activity API, as mentioned by Microsoft at: <https://msdn.microsoft.com/library/office/mt227394.aspx>

## Specify Permissions in Microsoft Management Activity API

**To specify permission for the connector application to access the Microsoft Management Activity API**

1. From the [Microsoft Azure portal](#) menu, select **Microsoft Entra ID**.
2. In the left pane, click **Manage > App registrations**, and then select the app name for which you want to specify permissions.
3. In the left pane, click **Manage > API permissions**.
4. On the **API permissions** page, click **Add a permission**.
5. On the **Request API permissions** page, on the **Microsoft APIs** tab, select **Office 365 Management APIs**.
6. Click **Application permissions**.
7. Select the **ActivityFeed.Read**, **ActivityFeed.ReadDlp**, and **ServiceHealth.Read** check boxes, and then click **Add permissions** to complete the process.

After adding permissions to your API, the list of configured permissions is displayed under **Configured permissions**.

8. Click **Grant admin consent for <your tenant>**. The Grant admin consent confirmation window is displayed.
9. Click **Yes**.

After granting consent, the state of the permissions can be viewed in the **Status** column.



**Important:** This step must be performed by an admin. The **Grant admin consent** option is disabled if you are not an admin or if no permissions have been configured for the application.

For more information about API permissions and admin consent, refer to the [Microsoft documentation](#).

## Install the SmartConnector

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

### Prepare to Install Connector

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

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight*

*Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

## Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the OpenText SSO site.

**1** Download the SmartConnector executable for your operating system from the OpenText SSO site.

**2** Start the SmartConnector installation and configuration wizard by running the executable.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction  
Choose Install Folder  
Choose Shortcut Folder  
Pre-Installation Summary  
Installing...

**3** When the installation of SmartConnector core component software is finished, the following window is displayed:

## Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.

Parameter	Setting
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using OpenText SecureData solutions to provide encryption. See the *OpenText SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the OpenText SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The OpenText SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for OpenText SecureData.
Format Preserving Secret	Enter the secret configured for OpenText SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

## Select Connector and Add Parameter Information

- 1 Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
- 2 Select **Microsoft Office 365** and click **Next**.

**3** Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

**Connector Setup**

opentext  
ArcSight

Configure

Enter the parameter details

Resource URL:

Azure Tenant Domain:

Client ID:

Client Secret:

Management API:

SharePoint Online:

Exchange Online:

Azure Active Directory:

Other Workloads:

Proxy Server (Optional):

Proxy Port (Optional):

Proxy User (Optional):

Proxy Password (Optional):

< Previous   **Next >**   Cancel

Parameter	Description
Resource URL	The Office 365 Management URL. Default value: https://manage.office.com
Azure Tenant Domain	The domain name of the Office 365 Azure tenant. Sample value: mycompany.onmicrosoft.com
Client ID	The Client ID of the application registered in Microsoft Entra ID. You can retrieve the Application (client) ID from the App registrations page. For more information, see <a href="#">SmartConnector Application Registration in Microsoft Entra ID</a> .
Management API	The Office 365 Management API URL. Default value: https://manage.office.com/api

Parameter	Description
Client Secret	The Client Secret of the application registered in Microsoft Entra ID. For more information, see <a href="#">Generate Keys and Configure the Application Properties</a> .
SharePoint Online	To collect events from SharePoint Online, select 'true'.
Exchange Online	To collect events from Exchange Online, select 'true'.
Azure Active Directory	To collect events from Azure AD, select 'true'.
Proxy Server (Optional)	(Optional) The proxy server used to access the Internet.
Proxy Port (Optional)	(Optional) The proxy port used to access the Internet.
Proxy User (Optional)	(Optional) The proxy user used to access the Internet.
Proxy Password (Optional)	(Optional) The proxy password used to access the Internet.

## Select a Destination

- 1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.
- 2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.
- 3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
- 4 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 click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

## Complete Installation and Configuration

- 1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
- 2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

**3** If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

**4** Click **Next** on the summary window.

**5** To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

## Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

## Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

### Azure AD Common Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
DestinationUserName	targetUPN
DestinationUserPrivileges	Role.DisplayName NewValue



ArcSight ESM Field	Device-Specific Field
Device Custom String 2	ModifiedProperties
Device Custom String 6	ExtendedProperties
File Type	AzureActiveDirectoryEventType, 0=AccountLogon, 1=AzureApplicationAuditEvent
Old File Hash	RequestType in ExtendedProperties (overloading field)
Old File Id	ResultStatusDetail in ExtendedProperties (overloading field)
Old File Name	UserAgent in ExtendedProperties (overloading field)
Old File Path	resultDescription in ExtendedProperties (overloading field)
Request Context	__concatenate(targetContextId, targetName, targetObjectId, targetPUID, targetSPN) in ExtendedProperties (overloading field)
Request Method	UserAuthenticationMethod in ExtendedProperties (overloading field)
SourceUserName	actorUPN
SourceUserPrivileges	Role.DisplayName OldValue

## Azure AD Account Logon Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	LoginStatus
Device Custom String 5	Client (Client Details)
Old File Name	SupportTicketId (if its value is String)
Request Client Application	Application
Source NT Domain	UserDomain

## Azure AD Other Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Source Username	Actor
Destination Username	Target
Device Custom Number 2	SupportTicketId (if its value is Long)
Device Custom String 3	Actor
Device Custom String 5	Target

## Compliance Exchange Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	IsPolicyHit
Device Custom String 2 Label	Is Policy Hit
File Id	ObjectId
Old File Hash	SRPolicyMatchDetails/SRPolicyMatchDetails
Old File Id	SRPolicyMatchDetails/SRPolicyId
Old File Name	SRPolicyMatchDetails/SRPolicyName

## CRM Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination Service Name	ServiceName
Destination User Id	SystemUserId
Destination User Name	UserUpn
Device Custom String 3	CrmOrganizationUniqueName
File Id	ObjectId
File Type	ItemType
Old File Hash	CorrelationId
Old File Id	EntityId
Old File Name	EntityName
Request Client Application	UserAgent
Request Context	__concatenate(ServiceContextId,ServiceContextIdType)
Request URL	__oneOf(InstanceUrl,ItemUrl)

## Data Insights REST API Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
File Type	DataType

## Discovery Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
File Hash	Cmdlet
File Id	Caseld
File Name	Case
File Path	SharepointLocations
File Permission	PublicFolderLocations
File Type	ObjectType
Old File Hash	CmdletOptions
Old File Path	ExchangeLocations

## Exchange Online Admin Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	Parameters, Organization
Destination User Name	One of (StatusMailRecipients, User, Name, Identity)
DestinationUserPrivileges	Parameters, AccessRights
Device Custom Number 1	Public Folder Hierarchy Mailbox Count Quota
Device Custom String 5	Identity
Device Custom String 6	Organization Name
End Time	Parameters, EndDate, UTC, MM/dd/yyyy hh:mm:ss a z
File ID	ObjectId
File Name	ModifiedObjectResolvedName
File Type	Parameters, FileTypes
Request Method	ExternalAccess
Request Parameters	Parameters
Request URL	Parameters, PrivacyStatementURL
Source Host Name	OriginatingServer
Start Time	Parameters, StartDate, UTC, MM/dd/yyyy hh:mm:ss a z

## Exchange Online DPL Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	ExchangeMetaData
Device Custom Date 1	Sent Time
Device Custom Number 1	Unique Count
Device Custom String 2	Subject
Device Custom String 3	Policy Name
Device Custom String 5	Actions
Device Custom String 6	Recipients
Device Severity	PolicyDetails
File Id	Incident Id
File Name	Message ID
Old File Id	Policy Id
Old File Name	PolicyDetails
Source User Name	ExchangeMetaData

## Exchange Online Mailbox Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom Number 1	LogonType
Device Custom String 2	ClientInfoString
Device Custom String 5	ExternalAccess
Device Custom String 6	OrganizationName
Device Version	ClientVersion
Source Address	ClientIPAddress
Source Host Name	OriginatingServer
Source Process Name	ClientProcessName
Source User Name	One of (LogonUserDisplayName, MailboxOwnerUPN)

## Exchange Online Mailbox Item Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SendAsUserSmtp,SendOnBehalfOfUserSmtp)
Destination User Privileges	MailboxOwnerSid
Device Custom Number 2 Label	Internal Logon Type
Device Custom Number2	InternalLogonType
Device Custom String 3	Subject
File Hash	MailboxGuid (overloading field)
File Id	InternetMessageId
File Name	Item.Attachments
File Path	Item.Path
File Permission	SessionId (overloading field)
File Size	Item.Attachments
Old File Name	Item (overloading field)
Old File Path	Item/ParentFolder
Source User Privileges	LogonUserSid

## Exchange Online Mailbox Item Group Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User ID	DestMailboxOwnerSid
Destination User Name	DestMailboxOwnerUPN
Destination User Privileges	MailboxOwnerSid
Device Custom Number 2	InternalLogonType
Device Custom Number 2 Label	Internal Logon TypeA
Device Custom String 3	Subject
File Hash	MailboxGuid (overloading field)
File Id	DestFolder (Id)
File Path	DestFolder (Path)
File Permission	SessionId (overloading field)
File Type	Attachments in AffectedItems (overloading field)

ArcSight ESM Field	Device-Specific Field
Old File Hash	Path in AffectedItems (overloading field)
Old File Id	Folder (Id)
Old File Name	Item (overloading field)
Old File Path	Folder (Path)
Old File Type	Id in AffectedItems (overloading field)
Request Cookies	AffectedItems
Source User Privileges	LogonUserSid

## Microsoft Teams Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	AdminActionDetail
Device Custom String 3	TeamName
File Hash	TeamGuid
File Id	ChannelGuid
File Name	__oneOf(ChannelName, ItemName)
File Permission	Members
File Type	ChannelType
Old File Id	__oneOf(MessageId, ObjectId)
Request Client Application	ClientApplication
Source User Name	UPN

## (Office 365 Advanced Threat Protection) Threat Intelligence Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	Recipients
Device Custom Date 1	MessageTime
Device Custom Number 3	Subject
File Hash	SHA256
File Id	NetworkMessageId

ArcSight ESM Field	Device-Specific Field
File Name	FileName
File Permission	FileVerdict
Old File Hash	MalwareFamily
Old File Id	InternetMessageId
Old File Permission	Verdict
Old File Type	DetectionType
Request Context	AttachmentData
Request Method	DetectionMethod
Request URI	EventDeepLink
Source Address	SenderIp
Device Custom String 2	P2Sender
Source User Name	P1Sender

## Microsoft Flow Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
File Name	FlowConnectorNames
File Permission	SharingPermission
File Type	UserTypeInitiated
Request Context	LicenseDisplayName
Request URI	FlowDetailsUrl
Source User Name	UserUPN

## Advanced eDiscovery Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	StartTime
Device Custom Date 2	EndTime
File Name	CaseName
File Type	WorkingSetId
Old File Id	CaseId

## Project Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Action	Action
Device Custom String 5	EventSource
File Name	Entity
File Type	ItemType
Old File Hash	CorrelationId
Request Client Application	UserAgent

## Security and Compliance Center to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	ModifiedBy
Device Action	RetentionAction
Device Custom Date 1	CreatedDateUTC
Device Custom Date 2	LastModifiedDateUTC
Device Custom String 3	PolicyName
Device Custom String 6	Workload
File Hash	Cmdlet
File Name	LabelName
File Type	ObjectType
Old File Hash	CmdletOptions
Old File Type	RetentionType
Source User Name	AlertEntityId

## Security and Compliance Center EOP Cmdlet Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	ClientApplication
Device Custom String 2	CmdletVersion
Device Custom String 2 Label	CMD Let Version



ArcSight ESM Field	Device-Specific Field
File Hash	Parameters
File Type	SecurityComplianceCenterEventType
Old File Hash	NonPIIParameters
Old File Id	EffectiveOrganization

## Security and Compliance Alert Signals to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Data
Device Custom String 3 Label	Data
Device Custom String 6	Source
Device Custom String 6 Label	Source
Device Severity	Severity
Event Outcome	Status
File Id	AlertId
File Name	Name
File Permission	Category
File Type	AlertType
Old File Id	PolicyId
Old File Permission	Comments
Old File Type	EntityType
Source User Name	CreatedBy

## (Office 365 Advanced Threat Protection) Threat Intelligence Url to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	TimeOfClick
Device Custom String 2	EventDeepLink
Device Custom String 5	UrlClickAction
Device Custom String 6	SourceWorkload

ArcSight ESM Field	Device-Specific Field
File Id	SourceId
Request Client Application	AppName
Request URI	Url
Source Address	UserIp

## Power Apps to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	AdditionalInfo
Request Client Application	AppName

## (Office 365 Advanced Threat Protection) Threat Intelligence Atp Content to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	DetectionDate
Device Custom Date 2	LastModifiedDate
Device Custom String 2	EventDeepLink
Device Custom String 3	LastModifiedBy
Device Custom String 6	SourceWorkload
File Hash	FileData\SHA256
File Id	FileData\DocumentId
File Name	FileData\FileName
File Path	FileData\FilePath
File Permission	FileData\FileVerdict
File Size	FileData\FileSize
File Type	FileData\MalwareFamily
Request Method	DetectionMethod

## Microsoft Office 365 Common Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Action	Operation
Device Custom IPv6 Address2	Source IPv6 Address
Device Custom Number 3	UserType
Device Custom String 1	OrganizationId
Device Custom String 4	UserKey
Device Event Category	(RecordType, 1=ExchangeAdmin, 2=ExchangeItem, 3=ExchangeItemGroup, 4=SharePoint, 6=SharePointFileOperation, 8=AzureActiveDirectory, 9=AzureActiveDirectoryAccountLogon, 10=DataCenterSecurityCmdlet, 11=ComplianceDLPSharePoint, 12=Sway, 13=ComplianceDLPEXchange), 14=SharePointSharingOperation, 15=AzureActiveDirectoryStsLogon, 18=SecurityComplianceCenterEOPCmdlet, 20=PowerBI, 21=CRM, 22=Yammer, 23=SkypeForBusinessCmdlets, 24=Discovery, 25=MicrosoftTeams, 28=ThreatIntelligence, 30=MicrosoftFlow, 31=AeD, 33=ComplianceDLPSharePointClassification, 35=Project, 36=SharepointListOperation, 38=DataGovernance, 40=SecurityComplianceAlerts, 41=ThreatIntelligenceUrl, 45=PowerAppsApp, 47=ThreatIntelligenceAtpContent, 52=DataInsightRESTAPI, 55=SharePointContentTypeOperation, 57=MicrosoftTeamsAdmin, 68=ExchangeCommunicationCompliance
Device Event Class ID	Operation
Device Product	Workload, AzureActiveDirectory=Azure Active Directory, Exchange=Exchange Online, SharePoint=SharePoint Online, OneDrive=OneDrive
Device Receipt Time	CreationTime, UTC, yyyy-MM-dd'T'HH:mm:ss z
Device Vendor	"Microsoft"
Event Outcome	ResultStatus
External ID	Id
Message	Operation
Name	Operation
Source Address	ClientIP
Source Port	ClientIP
Source User ID	UserId

## Power BI Audit Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	DeviceType
File Hash	ReportName
File Name	DashboardName
Old File Name	DatasetName
Request Context	Endpoint
Source User Privileges	WorkSpaceName

## SharePoint Online Common Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Site
Device Custom String 5	One of ((EventSource, 0=SharePoint, 1=ObjectModel) EventSource)
File Path	ObjectId
File Type	One of ((ItemType, 0=Invalid, 1=File, 5=Folder, 6=Web, 7=Site, 8=Tenant, 9=DocumentLibrary) ItemType)
Request Client Application	UserAgent
Source Process Name	SourceName

## SharePoint Online and One Drive for Business List Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	ListBaseTemplateType
Device Custom String 6	ListTitle
File Id	ListId (overloading field)
File Name	FileName
File Path	FilePathUrl
Old File Hash	CorrelationId (overloading field)
Old File Id	ListItemUniqueId (overloading field)

ArcSight ESM Field	Device-Specific Field
Old File Type	ListBaseType
Request Context	ApplicationDisplayName
Request Cookies	WebId (overloading field)

## SharePoint Online and One Drive for Business File Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Bytes In	FileSyncBytesCommitted
Destination User ID	EventData.<Shared by>
Destination User Name	One of (UserSharedWith, EventData.<Shared by>, TargetUserOrGroupName)
Destination User Privileges	SharingType
Device Custom String 6	PolicyDetails
Device CustomString 6 Label	PolicyDetails
File Name	DestinationFileName
File Path	DestinationRelativeUrl
File Type	DestinationFileExtension
Old File Hash	CorrelationId (overloading field)
Old File Id	ApplicationId (overloading field)
Old File Name	SourceFileName
Old File Path	SourceRelativeUrl
Old File Type	SourceFileExtension
Request Context	ApplicationDisplayName
Request URL	SiteUrl
Source User Name	EventData,<Invited account>

## SharePoint Online Other Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	ModifiedProperties

## SharePoint Online DLP Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	DocumentLastModifier
Device Custom String 6 Label	Document Last Modifier
File Id	UniqueID
File Name	FileName
File Path	FilePathUrl
File Size	FileSize
Old File Permission	FileOwner (overloading field)
Request Cookies	SiteCollectionGuid (overloading field)
Request Method	SharePointMetaData
Request Url	SiteCollectionUrl
Source Process Name	From

## SharePoint Online Sharing Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserOrGroupName
Destination User Privileges	TargetUserOrGroupType
Device Custom Number 1	Version
Device Custom Number 1 Label	Version
Device Custom String 2	ModifiedProperties\NewValue
Device Custom String 2 Label	Old Value
Device Custom String 6	ModifiedProperties\OldValue
Device Custom String 6 Label	New Value
File ID	UniqueSharingId
File Name	ModifiedProperties\Name
File Type	__oneOf (__simpleMap(ItemType,"0=Invalid","1=File","5=Folder","6=Web","7=Site","8=Tenant","9=DocumentLibrary"),ItemType)
Old File ID	ApplicationId
Old File Name	SourceFileName

ArcSight ESM Field	Device-Specific Field
Old File Path	SourceRelativeUrl
Old File Type	SourceFileExtension
Request Context	ApplicationDisplayName
Request Cookies	WebId
Request Method	EventData
Request Url	SiteUrl

## Sway Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	DeviceType
File ID	SwayLookupId
File Type	ObjectType
Request Client Application	BrowserName
Request Context	Endpoint
Request Url	SiteUrl

## Skype For Business Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	DomainController
Destination User Name	Destination
Device Custom String 6	CmdletVersion
Event Outcome	Status
File Hash	EnableCustomTrunking
File Name	ObjectName
Source User Name	Organization

## Yammer Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Id	TargetYammerUserId
Destination User Name	TargetUserId

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	VersionId
Device Custom Number 2	YammerNetworkId
File Id	FileId
File Name	FileName
Old File Id	MessageId
Source User Name	ActorUserId
Source User Privileges	ActorYammerUserId

## Troubleshooting

What to do if the SmartConnector stops receiving new events after running for a few days?

By default, the connector sends a query to the Management API and gets new events every 30 seconds, this process can be interrupted by a proxy or a firewall.

Workaround: Increase the execution time between queries. Go to the `agent.properties` file and change the `content.uri.queue.producer.thread.sleepTime` value from 30000 to 300000.



# 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 Microsoft Office 365 Management Activity  
SmartConnector (SmartConnectors 25.1.1)**

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](mailto:MFI-Documentation-Feedback@opentext.com).

We appreciate your feedback!