



Micro Focus Security ArcSight Connectors

SmartConnector for Microsoft Office 365 Management Activity

Configuration Guide

December 3, 2020

Configuration Guide

SmartConnector for Microsoft Office 365 Management Activity

December 3, 2020

Copyright © 2016 – 2020 Micro Focus or one of its affiliates.

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

<https://www.microfocus.com>.

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202- 3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR,

DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs>

Revision History

Date	Description
12/03/2020	Updated the troubleshooting section.
09/17/2020	Added support for SecurityComplianceCenterEOPCmdlet Record Type. Added support for Security and Compliance Center EOP Cmdlets events.
06/18/2020	Added support for Data Insights REST API and Compliance Exchange events. Added new mappings for Exchange Online Mailbox Item.
04/30/2020	Added suport for Sway events, PowerBIAudit events, CRM events, Yammer events, SkypeForBusiness events, Discovery events, Microsoft Teams events, Advanced Threat Protection events, Advanced eDiscovery events, Project events, Security and Compliance Center events and Power Apps events.
02/21/2020	Added mappings for SharePoint Online Sharing Mappings to ArcSight Fields.
01/16/2020	Added Supported Audit Log Record Types.
01/16/2020	Updated mappings for SharePoint Online and OneDrive for Business to ArcSight Fields.
01/16/2020	Added mappings for SharePoint Online DLP Mappings to ArcSight Fields. Updated mappings for SharePoint Online (List).
01/16/2020	Added mappings for SharePoint Online and One Drive for Business List Mappings to ArcSight Fields and SharePoint Online and One Drive for Business File Mappings to ArcSight Fields.
01/16/2020	Added mappings for Exchange Online Mailbox Item Group Mappings to ArcSight Fields and Exchange Online Mailbox Item Mappings to ArcSight Fields.
01/16/2020	Added mappings for Azure AD Common Mappings to ArcSight Fields.
01/16/2020	Replaced "Enter the parameter details" image with the latest and added the respective parameters in the table.
09/19/2019	Added mapping for Azure AD Account Logon Mappings to ArcSight Fields.

Date	Description
09/19/2019	Updated mapping for Azure AD Other Mappings to ArcSight Fields.
09/19/2019	Updated mapping for SharePoint Online File Operations Mappings to ArcSight Fields.
05/17/2019	Added Azure AD Common Mappings.
12/17/2018	Updated mappings for Exchange Online Admin mappings.
11/19/2018	Added mappings for Microsoft Office 365 Common Mappings to ArcSight Fields. Updated mappings for SharePoint Online (List). Updated mappings for Exchange Online (Mailbox Item Group).
07/16/2018	Added support for ComplianceDLPExchange Record Type. Updated mapping for Exchange Online (DLP).
10/17/2017	Added encryption parameters to Global Parameters.
07/15/2017	Added support for OneDrive.
04/17/2017	Updated mappings for Exchange Online (Admin, Mailbox, Mailbox Item, and Mailbox Item Group) and SharePoint Online File Operations.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/16/2016	GA release of this connector.

SmartConnector for Microsoft Office 365 Management Activity

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, Azure Active Directory (AD) and OneDrive.

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 Azure AD activity logs. You can use the actions and events from the Office 365 and Microsoft Azure Active Directory 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.
14	SharePoint Sharing Operation	SharePoint Online sharing events.
15	AzureActiveDirectoryStsLogon	Secure Token Service (STS) logon events in Azure Active Directory.

Value	Member Name	Description
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.
56	SharePointFieldOperation	SharePoint list field 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 Azure AD and the OAuth2 protocol for authentication and authorization. To allow the connector to access the API, you must first register it in Azure AD and configure it with appropriate permissions.

SmartConnector Application Registration in Azure AD

The following configuration procedures allows you to establish an identity for the connector and specify the permission levels it needs in order to access the Management Activity API. Before registering the connector application with Azure AD, the following prerequisites must exist:

- An Office 365 subscription account must be enabled and configured.
- The Office 365 subscription must be associated with an Azure AD Tenant Domain account.

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

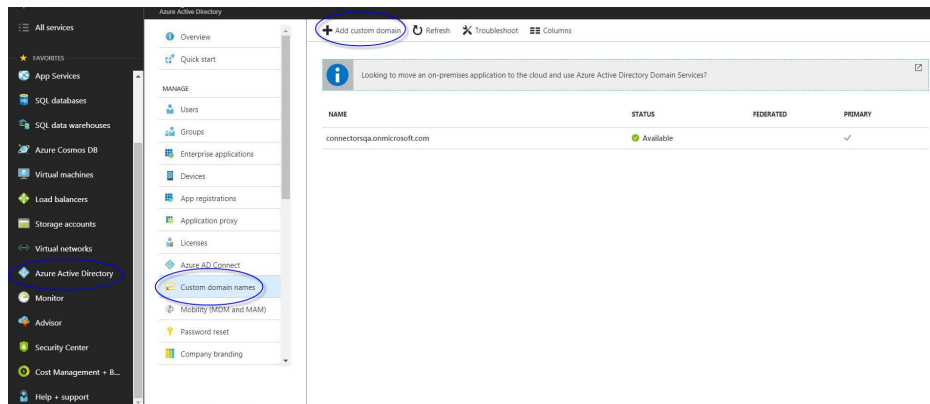
To register your connector application in Azure AD:

Once you have a Microsoft tenant with the proper subscriptions, you can register your connector application in Azure AD.

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



- 2 In the left navigation panel, select **Azure Active Directory** (1). Select custom domain names (2) and add custom domain (3).



3 Add the custom domain name (1). Click on add domain (2) and verify (3).

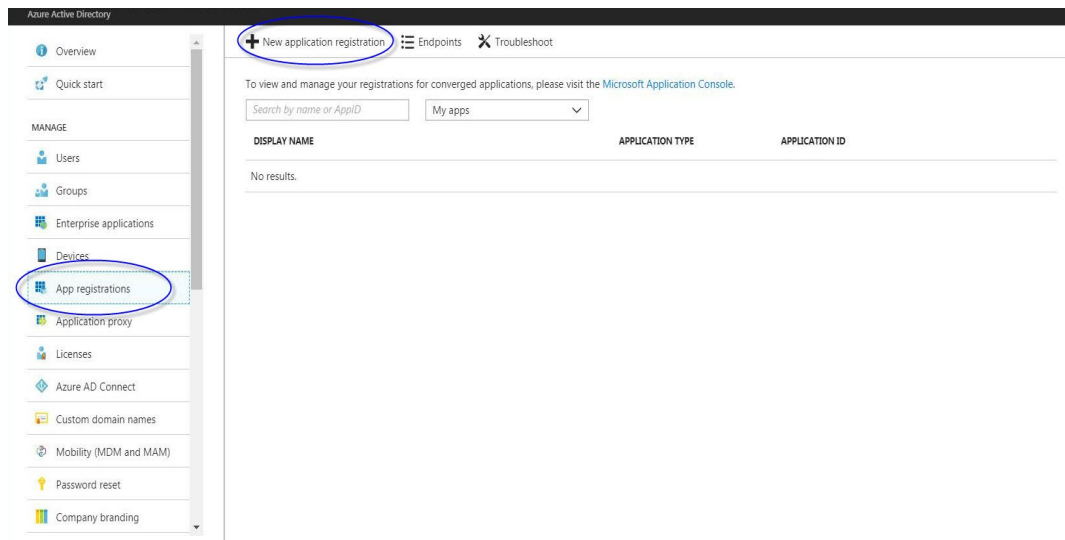
The first part of the image shows the 'Add Domain' form. It has a text input field for 'Custom domain name' containing 'qaconn.onmicrosoft.com' with a green checkmark. Below the field is a blue 'Add Domain' button. The second part shows the 'Verify' page for the domain 'qaconn.onmicrosoft.com'. It instructs the user to create a new TXT record with the following details:

RECORD TYPE	ALIAS OR HOST NAME	DESTINATION OR POINTS TO ADDRESS	TTL
TXT	@	MS=ms89951200	3600

Below the table, there is a 'Verify' button and a note: 'Verification will not succeed until you have configured your domain with your registrar as described above.'

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 Azure Active Directory to register the connector as a client application.

4 In the left navigation panel, select App registrations, then click on new application registration.



5 Enter a logical name, supported account types and redirect URI. Click register.

Home > Micro Focus - App registrations > Register an application

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

SmartConnector ✓

Supported account types
Who can use this application or access this API?

☐ Accounts in this organizational directory only (Micro Focus only - Single tenant)
☒ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ✓

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

SIGN-ON URL: This parameter is not required by the connector, but it is required by Azure Active Directory in order to register the connector 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.

- 6 The "registered app" screen pops.** Your connector app is now registered with Azure AD and has been assigned a client ID. However, there are several aspects of your connector app left to configure.

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? →

Display name SmartConnector	Supported account types Multiple organizations
Application (client) ID	Redirect URIs 1 web, 0 public client
Directory (tenant) ID	Application ID URI Add an Application ID URI
Object ID	Managed application in local directory SmartConnector

Generate Keys and Configure the Application Properties

Now that your connector application is registered, there are several important properties you must specify that determine how your connector application functions within Azure AD.

- 1 Click Certificates and secrets.**

Home > Micro Focus > App registrations > SmartConnector - Certificates & secrets

SmartConnector - Certificates & secrets

Search (Ctrl+/)

Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

No certificates have been added for this application.

THUMBPRINT	START DATE	EXPIRES
------------	------------	---------

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

DESCRIPTION	EXPIRES	VALUE
-------------	---------	-------

No client secrets have been created for this application.

- 2 Click New client secret. Enter a description and select never expires. Click Add.**

Add a client secret

Description

Expires
☐ In 1 year
☐ In 2 years
☒ Never

- 3 Scroll up to view the **Client ID** value. This value is automatically generated by Azure AD. Your connector application will use this value.
- 4 Use the highlighted Clipboard icon to copy the **Client ID** value and paste it somewhere it can be saved, such as a text document. This value will be used to configure the connector during the connector installation.

The screenshot shows the 'Keys' blade in the Azure AD portal. On the left is a 'Settings' sidebar with options like Filter settings, GENERAL, Properties, Reply URLs, Owners, API ACCESS, Required permissions, and Keys (highlighted). The main pane shows a table of keys. The first key, 'Any Description', has an expiration date of 12/31/2299 and a value that has been truncated. A yellow banner at the top of the keys table says 'Copy the key value. You won't be able to retrieve after you leave this blade.' A clipboard icon is highlighted next to the key value.

DESCRIPTION	EXPIRES	VALUE
Any Description	12/31/2299	Value will be displayed on save

- 5 Scroll down to view the **Reply URL**. This parameter is not required by the connector, but it is required by Azure Active Directory in order to register the connector 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. Sample value: `https://localhost:8081/oauth2callback`
- 6 Click **Save** if you make any changes to these values. Example value:
- 7 Remain on the **Configuration** page for the next procedure.

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

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

Limitations of the Microsoft Management Activity API

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

When the connector 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 Azure Management Portal, click **App registrations**, select your connector application and click **API permissions**, click **Add a permission**.

Home > Micro Focus > App registrations > SmartConnector - API permissions

SmartConnector - API permissions

Search (Ctrl+/)

Overview
Quickstart

Manage

Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest

Support + Troubleshooting
Troubleshooting
New support request

API permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs.

+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT...	STATUS
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	

These are the permissions that this application requests statically. You may also request user consentable permissions dynamically through code. [See best practices for requesting permissions](#)

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

Grant admin consent for Micro Focus

- 2 Select the Office 365 Management APIs.

Request API permissions

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

OneNote
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

Power BI Service
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

PowerApps Runtime Service
Powerful data storage, modeling, security and integration capabilities

- 3 Click **Delegated permissions** and check the **ActivityFeed.Read**, **ActivityFeed.ReadDlp** and **ServiceHealth.Read**. Click **add permissions**.
- 4 Click **Save** to save the configuration. Select **API Office 365** and click **done**.

← All APIs

Delegated permissions
 Your application needs to access the API as the signed-in user.

Application permissions
 Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
▼ ActivityFeed (2)	
<input checked="" type="checkbox"/> ActivityFeed.Read Read activity data for your organization ⓘ	Yes
<input checked="" type="checkbox"/> ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data ⓘ	Yes
▼ ActivityReports	
<input type="checkbox"/> ActivityReports.Read Read activity reports for your organization ⓘ	Yes
<input type="checkbox"/> ActivityReports.Read Read activity reports for your organization ⓘ	Yes
▼ ServiceHealth (1)	
<input checked="" type="checkbox"/> ServiceHealth.Read Read service health information for your organization ⓘ	Yes
▼ ThreatIntelligence	
<input type="checkbox"/> ThreatIntelligence.Read Read threat intelligence data for your organization ⓘ	Yes
<input type="checkbox"/> ThreatIntelligence.Read Read threat intelligence data for your organization ⓘ	Yes

[Add permissions](#) [Discard](#)

5 Click Grant admin consent.



This step must be performed by an admin account. Ask your administrator to go to the **Azure portal > App registrations** and click on the application that you registered. Then click **API permissions > Grant admin consent**.

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

[Grant admin consent for Micro Focus](#)

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

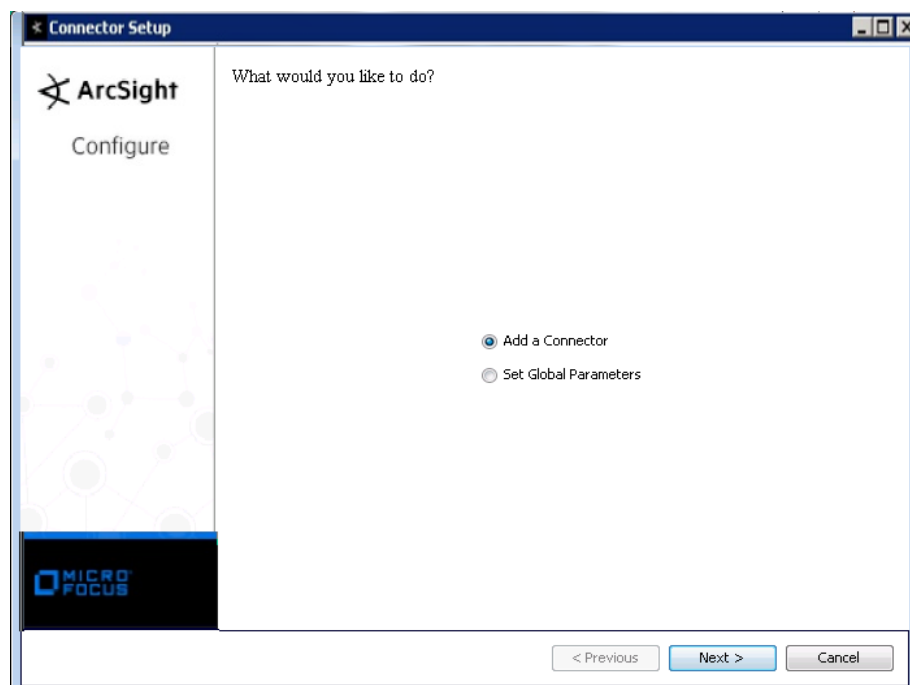
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the Micro Focus 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'.
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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus 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 Micro Focus 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 Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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

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 Azure Active Directory. See step 3 in the "Generate Keys and Configure the Application Properties" section.
Management API	The Office 365 Management API URL. Default value: https://manage.office.com/api
Client Secret	The Client Secret of the application registered in Azure Active Directory. See step 2 in the "Generate Keys and Configure the Application Properties" section.
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
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, targetPUIID, 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
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	CasId
File Name	Case
File Path	SharepointLocations

ArcSight ESM Field	Device-Specific Field
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
--------------------	-----------------------

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	InternetMessageld
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)
Old File Hash	Path in AffectedItems (overloading field)

ArcSight ESM Field	Device-Specific 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 3	TeamName
File Hash	TeamGuid
File Id	ChannelGuid
File Name	ChannelName
File Permission	Members
File Type	ChannelType
Old File Id	MessageId
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
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
Source User Id	P2Sender
Source User Name	P1Sender

Microsoft Flow Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
--------------------	-----------------------

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	Caseld

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
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
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, 13=ComplianceDLPEExchange)
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)
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

ArcSight ESM Field	Device-Specific Field
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

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

ArcSight ESM Field	Device-Specific Field
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.