



Micro Focus Security ArcSight Connectors

SmartConnector for Microsoft Office 365

Configuration Guide

November 19, 2018

Configuration Guide

SmartConnector for Microsoft Office 365

November 19, 2018

Copyright © 2016 – 2018 Micro Focus and its affiliates and licensors.

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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.

Revision History

Date	Description
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

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).
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	SharePointSharingOperation	SharePoint Online sharing events.

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.](#)

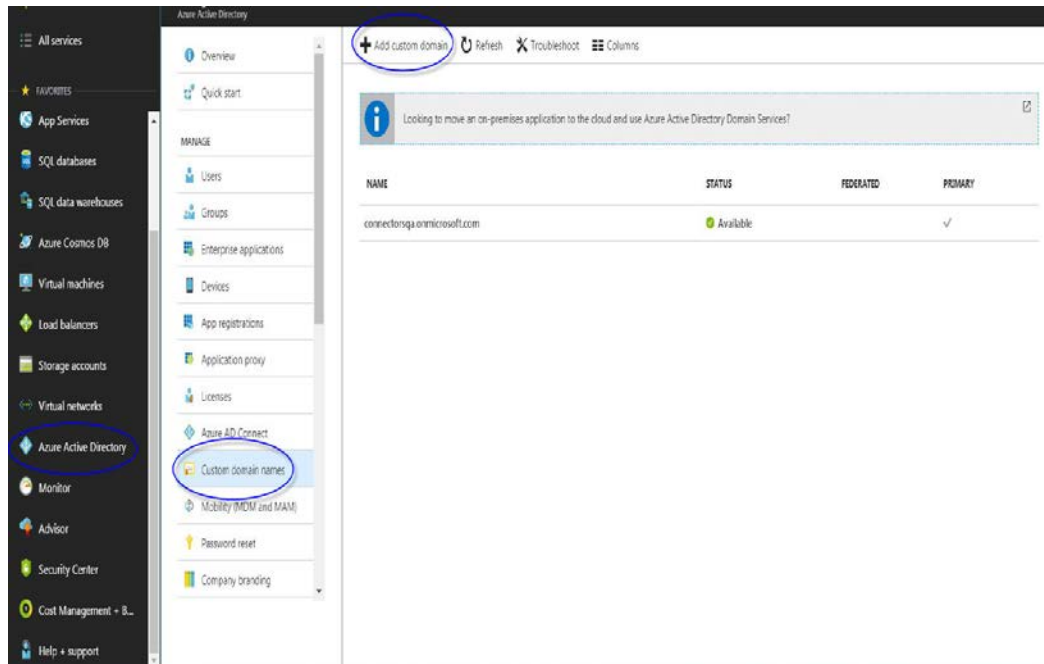
To register your connector application in Azure AD:

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 'Add Domain' dialog box shows a text input field for the 'Custom domain name' containing 'qaconn.onmicrosoft.com' with a green checkmark. Below the input field is a blue 'Add Domain' button.

The domain verification page for 'qaconn.onmicrosoft.com' shows instructions to create a new TXT record. The form includes the following fields:

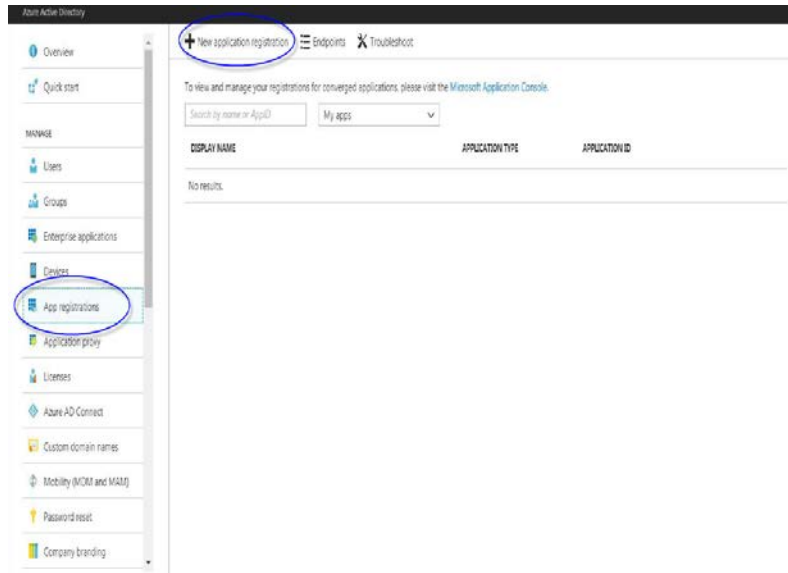
- RECORD TYPE: ☒ TXT ☐ MX
- ALIAS OR HOST NAME: @
- DESTINATION OR POINTS TO ADDRESS: NS=ms6961300
- TTL: 3600

Below the form, there is a 'Verify domain' section with a 'Verify' button.

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.

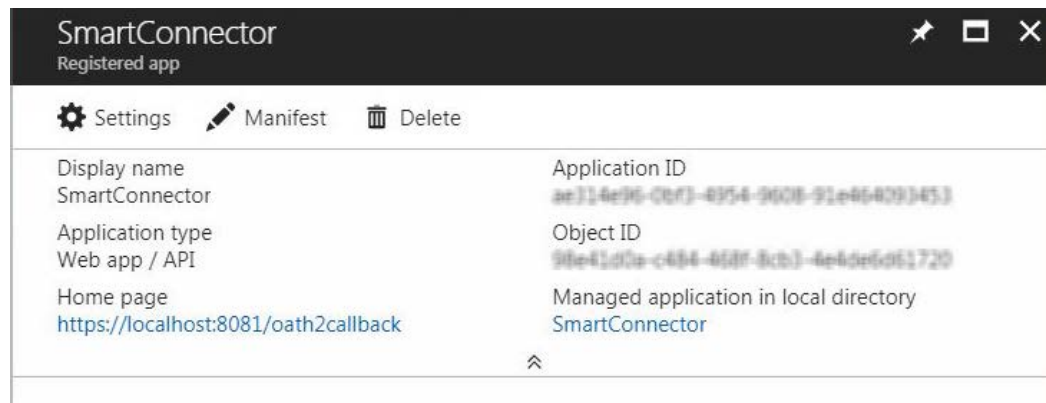


- 5 Enter a logical name and specify the Type as Web Application and/or Web API. Click create.

The screenshot shows the 'Create' dialog box in the Azure AD portal. It contains three fields: 'Name' with the value 'SmartConnector', 'Application type' set to 'Web app / API', and 'Sign-on URL' with the value 'https://localhost:8081/oath2callback'. Each field has a green checkmark indicating it is valid. A 'Create' button is at the bottom.

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.

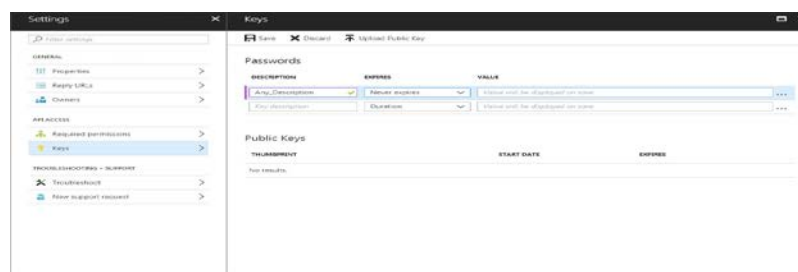
- The "registered app" screen pops. Click Configuration. Remain on the Configuration page. Your connector app is now registered with Azure AD and has been assigned a client ID. However, there are several aspects of your connector app left to configure.



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.

- After selecting the **Settings** tab in the previous procedure, scroll down to the **Keys** section and select **Description**: any description (1) and expires: never expires (2) from the drop-down list.



- Click **Save** to display the app (or client) secret.
- Scroll up to view the **Client ID** value. This value is automatically generated by Azure AD. Your connector application will use this value.
- 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.



- 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>

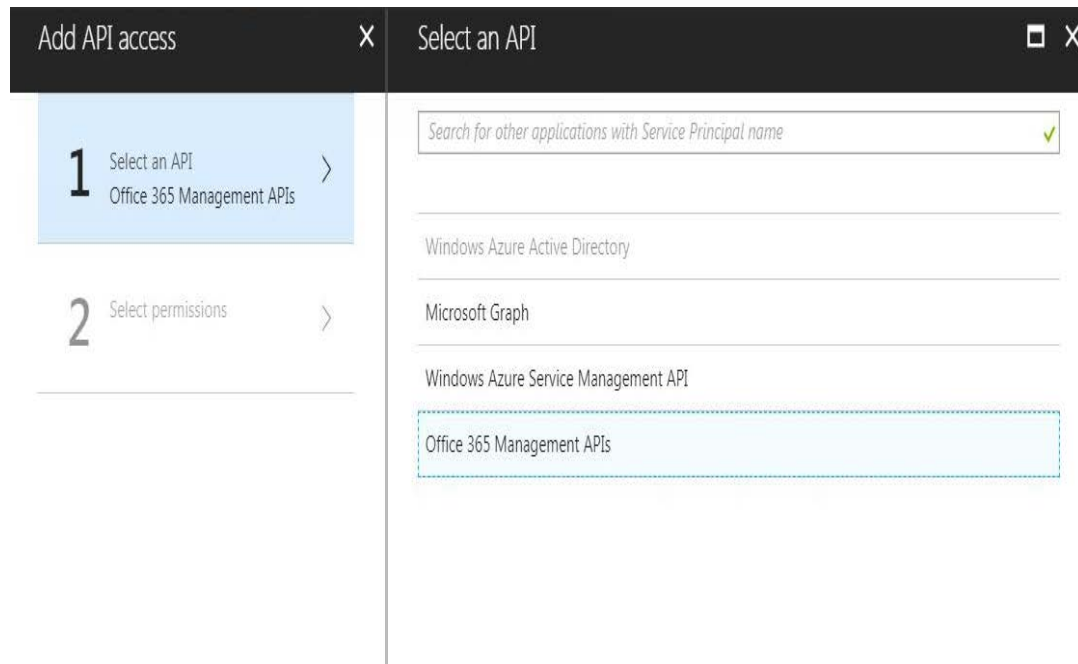
Specifying Permissions in Microsoft Management Activity API

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

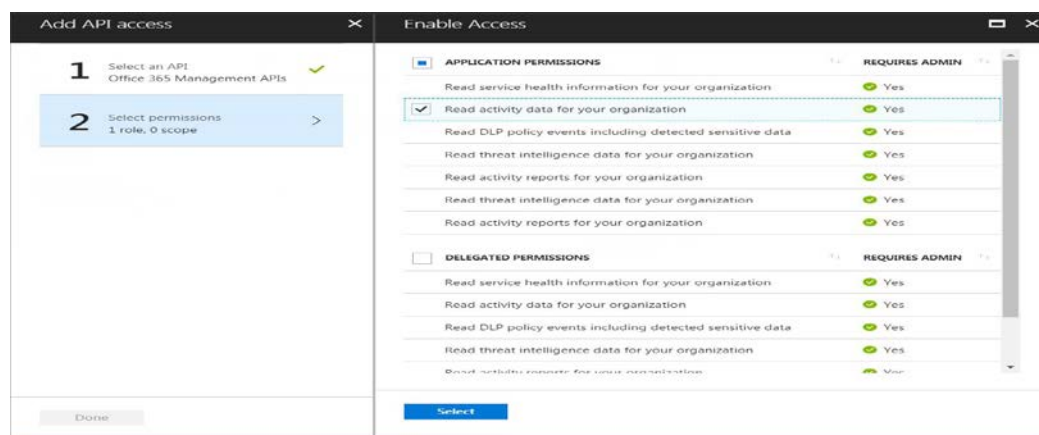
- 1 From the Azure Management Portal, click **settings**, select your connector application and scroll down to required permissions (1), click **Add API access** (2), and select an API.
Configure tab, select your connector application and scroll down to **permissions to other applications**, and click **Add application**.



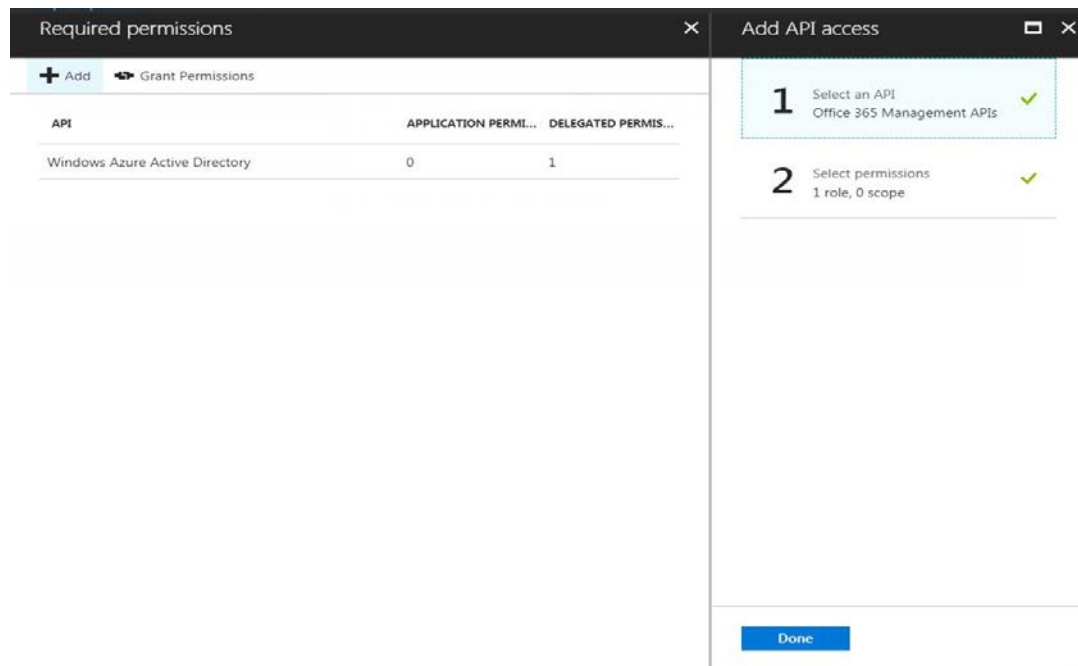
- 2 Select the Office 365 Management APIs (1) so that it appears in the Selected column (2), then click select and return to the main configuration page for your application.



- 3 The Office Management APIs will now appear in the list of applications to which your application requires permissions. Under Application Permissions, select **Read activity data for an organization**.



- 4 Click **Save** to save the configuration. Select API Office 365 and click done.



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

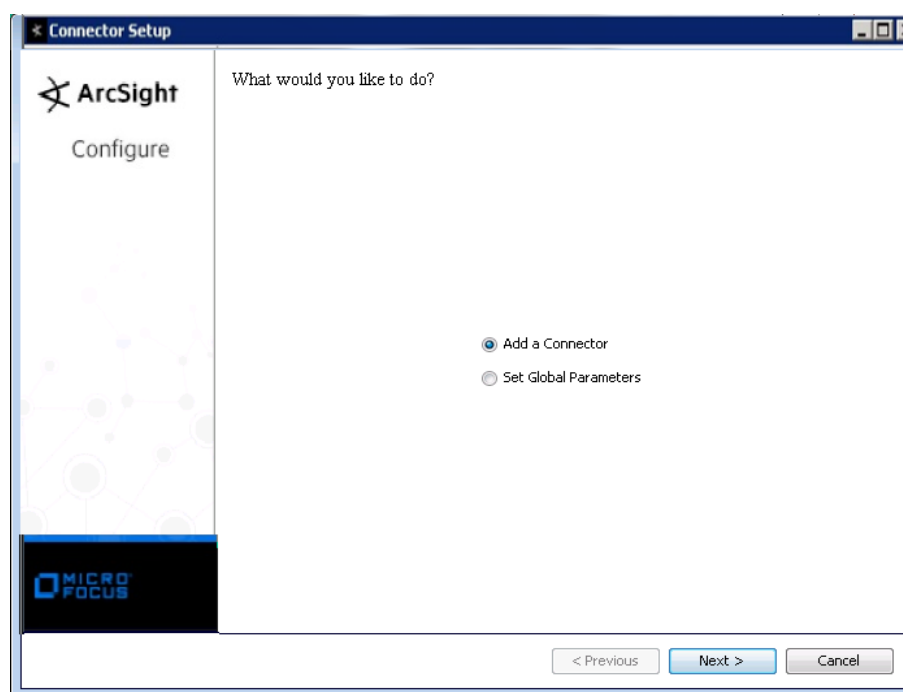
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 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'.

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 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**.

Parameter	Description
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.
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.

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=ComplianceDLPEXchange)
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

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 List Mappings to ArcSight Fields

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

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	ListTitle
Old File Type	ListBaseType

SharePoint Online File Operations Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User ID	EventData.<Shared by>
Destination User Name	One of (UserSharedWith, EventData.<Shared by>)
Destination User Privileges	SharingType
File Name	DestinationFileName
File Path	DestinationRelativeUrl
File Type	DestinationFileExtension
Old File Name	SourceFileName
Old File Path	SourceRelativeUrl
Old File Type	SourceFileExtension
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

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 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)
Device Custom String 3	Subject
File Name	Item.Attachments
File Path	Item.Path
File Size	Item.Attachments

Exchange Online Mailbox Item Group Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User ID	DestMailboxOwnerSid
Destination User Name	DestMailboxOwnerUPN

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Subject
File Id	DestFolder (Id)
File Path	DestFolder (Path)
Old File Id	Folder (Id)
Old File Path	Folder (Path)

Azure AD Common Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	ModifiedProperties
Device Custom String 6	ExtendedProperties
File Type	AzureActiveDirectoryEventType, 0=AccountLogon, 1=AzureApplicationAuditEvent

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)
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
Device Custom Number 3	Actor
Device Custom Number 5	Target