

---

# Micro Focus Security ArcSight SmartConnectors

## SmartConnector for Microsoft 365 Defender Configuration Guide

Document Release Date: February 2022

Software Release Date: February 2022



## Legal Notices

Micro Focus  
The Lawn  
22-30 Old Bath Road  
Newbury, Berkshire RG14 1QN  
UK

<https://www.microfocus.com>

## Copyright Notice

© Copyright 2022 Micro Focus or one of its affiliates

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.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

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

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
<b>ArcSight Product Documentation</b>	<a href="https://www.microfocus.com/documentation/arcsight/">https://www.microfocus.com/documentation/arcsight/</a>

# Contents

Configuration Guide for SmartConnector for Microsoft 365 Defender .....	5
Product Overview .....	5
Understanding Event Collection .....	5
Preparing to Install the SmartConnector .....	6
Installing and Configuring the SmartConnector by Using the Wizard .....	6
Device Event Mapping to ArcSight Fields .....	8
Incident .....	8
Alerts .....	9
Devices .....	10
Entities .....	10
Send Documentation Feedback .....	12

# Configuration Guide for SmartConnector for Microsoft 365 Defender

The Arcsight Microsoft 365 Defender configuration guide provides information to install the SmartConnector for Microsoft 365 Defender and configuring the connector for event collection.

## Product Overview

The SmartConnector for Microsoft 365 Defender retrieves incidents from Microsoft 365 Defender, normalizes and sends these events to the configured destinations.

For more information about Microsoft 365 Defender and its services, see the [Microsoft 365 Defender documentation](#).

## Understanding Event Collection

The SmartConnector for Microsoft 365 Defender uses access tokens to authenticate and allow an application to access an API. The access token will be retrieved by using the client credentials - client ID and client secret.

The following call details are used:

**Request type:** Post

**Token URL:** https://login.windows.net/<tenant\_id provided in setup>/oauth2/token

**Parameters:**

```
grant_type = client_credentials
```

```
client_id=<client_id provided in setup>
```

```
client_secret = <client_secret provided in setup>
```

```
resource=https://api.security.microsoft.com
```

The retrieved access token will be valid for one hour by default. A new access token will be retrieved after the old access token expires.

Microsoft 365 Defender incidents are retrieved by using the following Event URL:

```
https://api.security.microsoft.com/api/incidents?$filter=lastUpdateTime+ge+<START_AT_TIME>
```

<START\_AT\_TIME> is replaced with the current time in the following format:

```
yyyy-MM-dd'T'HH:mm:ss.SSSSSS'Z'
```

## Limitations

- Maximum page size is 100 incidents
- Maximum rate of requests is 50 calls per minute and 1500 calls per hour

## Preparing to Install the SmartConnector

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

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

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

Before installing the SmartConnector, ensure that you have the following:

- Register Azure Active Directory application with Microsoft threat protection - **Incident.Read.All** permission.
  - To register an Azure Active Directory application with appropriate permissions for Microsoft Defender for Endpoint, see the [Microsoft documentation](#).
  - To register an Azure Active Directory application with the appropriate permissions for Microsoft 365 Defender Incidents, see the [Microsoft documentation](#).
- Application (Client) ID, Directory (Tenant) ID, and Client Secret.

## Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the Microsoft 365 Defender Connector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the Microsoft 365 Defender Connector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. From the **Type** drop-down list, select **Microsoft 365 Defender** as the type of connector, then click **Next**.

5. Enter the following parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Proxy Host	If proxy is enabled for your machine, the IP address or host name of the proxy server for HTTPS connection.  Specify this value only if proxy needs access to internet.
Proxy Port	If proxy is enabled for your machine, the port number of the proxy server for HTTPS connection.  Specify this value only if proxy needs access to internet.
Proxy User Name	If proxy is enabled for your machine, the user name for the proxy server. This value is optional for additional proxy authentication. If you enter the proxy user name, you must provide the proxy password.  Specify this value only if proxy needs access to internet.
Proxy Password	If proxy is enabled for your machine, the password for the proxy server user.  Specify this value only if proxy needs access to internet.
Client Secret	The client secret key generated for your app in the registration portal.
Application (Client) ID	The client application ID assigned to your application.
Directory (Tenant) ID	The directory tenant ID, which the application plans to operate against, in GUID or domain-name format.

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. 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.
9. Select whether you want to run the connector as a service or in the standalone mode.
10. Complete the installation.
11. Run the SmartConnector.

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

## Device Event Mapping to ArcSight Fields

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



Each incident retrieved from Microsoft 365 defender is processed, split, and sent to the configured destinations in the following structure:

- **Incidents**

One top level incident event is sent per incident.

- **Alerts**

- One Alert event is sent for each device present in the alert
- One Alert event is sent for each entity present in the alert

Alert events can be correlated using the alertId (Device Custom String 2) and the incidentId (External ID) fields.

## Incident

ArcSight ESM Field	Device-Specific Field
Additional Data	redirectIncidentId
Additional Data	assignedTo
Additional Data	determination
Device Custom String 4	tags
Device Event Class ID	"365DefenderIncident"
Device Product	"365 Defender"
Device Receipt Time	lastUpdateTime
Device Severity	severity
Device Vendor	"Microsoft"
Event Outcome	status
External ID	incidentId
Name	incidentName
Reason	classification
Start Time	createdTime



## Alerts

ArcSight ESM Field	Device-Specific Field
Additional Data	actorName
Additional Data	assignedTo
Additional Data	detectorId
Additional Data	investigationId
Additional Data	serviceSource
Additional Data	determination
Additional Data	classification
Device Action	investigationState
Device Custom Date 1	firstActivity
Device Custom Date 2	lastActivity
Device Custom String 1	threatFamilyName
Device Custom String 2	alertId
Device Custom String 5	mitreTechniques
Device Event Category	category
Device Event Class ID	category
Device Process Name	detectionSource
Device Receipt Time	lastUpdatedTime
Device Severity	severity
End Time	resolvedTime
Event Outcome	status
External ID	incidentId
Message	description
Name	title
Start Time	creationTime

## Devices

ArcSight ESM Field	Device-Specific Field
Additional Data	firstSeen
Additional Data	rbacGroupName
Additional Data	aadDeviceId
Additional Data	healthStatus
Destination Host Name	deviceDnsName
Device Custom String 3	riskScore
Device Custom String 4	tags
Device Custom String 6	__concatenate(osPlatform," ",version," ",osProcessor," ",osBuild)
Device External ID	mdatpDeviceId

## Entities

ArcSight ESM Field	Device-Specific Field
Additional Data	registryValueType
Additional Data	evidenceCreationTime
Additional Data	sha1
Additional Data	deliveryAction
Additional Data	mailboxDisplayName
Destination Address	ipAddress
Destination Nt Domain	domainName
Destination Process ID	processId
Destination User ID	userSid
Destination User Name	__oneOf(accountName,recipient)
Device Custom String 3	__oneOf(registryKey,mailboxAddress)
Device Custom String 4	__oneOf(processCommandLine,subject)
Device Custom String 6	__oneOf(registryValue,userPrincipalName)
Device External ID	deviceId
File Create Time	processCreationTime

ArcSight ESM Field	Device-Specific Field
File Hash	sha256
File Name	fileName
File Path	filePath
File Type	entityType
Old File Create Time	parentProcessCreationTime
Old File ID	parentProcessId
Old File Name	parentProcessFileName
Request Url	url
Source User Name	sender

# 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 (SmartConnectors 8.3.0)**

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 [Documentation-Feedback@microfocus.com](mailto:Documentation-Feedback@microfocus.com).

We appreciate your feedback!