



ArcSight SmartConnectors

Software Version: 24.4.1

Configuration Guide for Microsoft 365 Defender SmartConnector

Document Release Date: December 2024

Software Release Date: December 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2024 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 365 Defender SmartConnector	4
Product Overview	5
Understanding Event Collection	5
Preparing to Install the SmartConnector	6
Microsoft 365 Defender API in Microsoft Threat Protection (Security API)	6
Registering an Azure Active Directory Application with appropriate Permissions for Microsoft 365 Defender	6
Adding Permissions for Microsoft 365 Defender Incidents	7
Generating Client Secret for the Application	7
Microsoft 365 Defender API in Microsoft Graph	7
Registering an Azure Active Directory Application with appropriate Permissions for Microsoft 365 Defender	7
Adding Permissions for Microsoft 365 Defender Incidents	8
Generating Client Secret for the Application	8
Microsoft 365 Defender API in Certificate-based Authentication	8
Creating Self-Signed Certificate	9
Installing and Configuring the SmartConnector	10
Device Event Mapping to ArcSight Fields	13
Event Mapping for Alerts via Security API	15
Incident	15
Alerts	15
Devices	16
Entities	17
Event Mapping for Alert V2 via Graph API - alert V2	18
Alerts	18
Device Evidence	18
Process Evidence	19
File Evidence	20
IP Evidence	20
Url Evidence	20
Registry Value Evidence	21
Cloud Application Evidence	21
Oauth Application Evidence	21
Analyzed Message Evidence	22
Send Documentation Feedback	23

Configuration Guide for Microsoft 365 Defender SmartConnector

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

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.

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

Product Overview

The SmartConnector for Microsoft 365 Defender retrieves incidents from Microsoft 365 Defender, normalizes and sends these incidents 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 to access the retrieved tokens:

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

The SmartConnector for Microsoft 365 Defender uses certificate-based authentication method to authenticate applications and services that need to access the Graph API. To authenticate

using certificate, an Application must be registered with Azure AD and certificate needs to be uploaded in the Azure AD portal to obtain the Application ID and Client Secret.

The following call details are used to access the retrieved tokens:

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_assertion_type = The value must be set to urn:ietf:params:oauth:client-assertion-type:jwt-bearer
```

```
client_assertion= An assertion (a JSON web token) is created. Log in with the certificate that you registered as credentials for your application.
```

```
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.

Preparing to Install the SmartConnector

Before Installing the SmartConnector, complete the following procedures:

1. [Microsoft 365 Defender API in Microsoft Threat Protection \(Security API\)](#)
2. [Microsoft 365 Defender API in Microsoft Graph](#)
3. [Microsoft 365 Defender API in Certificate-based Authentication](#)

Microsoft 365 Defender API in Microsoft Threat Protection (Security API)

Registering an Azure Active Directory Application with appropriate Permissions for Microsoft 365 Defender

1. Log in to **Azure** as a **Global Administrator User**.
2. Navigate to **Azure Active Directory > App Registrations > New Registration**.

3. In the registration form, select your application.
4. Click **Register**.

Adding Permissions for Microsoft 365 Defender Incidents

1. On the **Application Page**, select **API Permissions > Add a Permission > APIs my Organization uses**.
2. Type **Microsoft Threat Protection** on the search panel, and select **Microsoft Threat Protection**. Your application can now access **Microsoft 365 Defender**.
3. Choose **Application Permissions > Incident.Read.All** and select **Add Permissions**.

For more information regarding Azure Active Directory application with the appropriate permissions for Microsoft 365 Defender Incidents, see <https://docs.microsoft.com/en-us/microsoft-365/security/defender/api-hello-world?view=o365-worldwide>

Generating Client Secret for the Application

1. Click **Certificates and Secrets**.
2. Click **New Client Secret**.
3. Add **Description** to the secret and click **Add**.
4. Note the generated **Secret Value**.



Important: If you do not note down the **Secret Value**, you will not be able to retrieve it later.

5. On the application page, go to **Overview** and **Copy** the following:
 - Application (Client) ID
 - Directory (Tenant) ID

Microsoft 365 Defender API in Microsoft Graph

Registering an Azure Active Directory Application with appropriate Permissions for Microsoft 365 Defender

1. Log in to **Azure** as a **Global Administrator User**.
2. Navigate to **Azure Active Directory > App Registrations > New Registration**.

3. In the registration form, select your application.
4. Click **Register**.

Adding Permissions for Microsoft 365 Defender Incidents

1. Navigate to the application page and select **API Permissions > Microsoft Graph**.
2. Select **Delegated permissions**, and type **security** in the search bar. Then select **SecurityAlert.Read.All** and click **Add permission**.
3. Click **admin consent** for your tenant. Multiple permissions can be selected. You can then grant admin consent for all.

For more information regarding Azure Active Directory application with the appropriate permissions for Microsoft 365 Defender Incidents, see <https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/the-new-microsoft-365-defender-apis-in-microsoft-graph-are-now/ba-p/3603099>

Generating Client Secret for the Application

1. Click **Certificates and Secrets**.
2. Click **New Client Secret**.
3. Add **Description** to the secret and click **Add**.
4. Note the generated **Secret Value**.



Important: If you do not note down the **Secret Value**, you will not be able to retrieve it later.

5. On the application page, go to **Overview** and **Copy** the following:
 - Application (Client) ID
 - Directory (Tenant) ID

Microsoft 365 Defender API in Certificate-based Authentication

Certificate-based authentication is used to authenticate applications and services that need to access the Graph API. To authenticate using certificate, an Application must be registered with Azure AD to obtain the Application ID and Client Secret. The Application must also generate a self-signed certificate or obtain a certificate from a Trusted Certificate Authority (CA). The

Certificate is then uploaded to the Azure AD Application Registration and is used to authenticate the application when it requests access to the Graph API.

When an Application requests access to the Graph API using certificate-based authentication, Azure AD verifies the Certificate to ensure that it is valid and issued by a trusted CA. If the certificate is valid, Azure AD grants the Application an Access Token, which the Application can use to access the Graph API.

Creating Self-Signed Certificate

1. Create the self-signed certificate. Refer to the [Microsoft documentation](#) for more information regarding the self-signed certificate and authenticating the Application.
2. Register an Azure Active Directory Application with appropriate permissions for Microsoft 365 Defender as per the following steps:
 - a. Log in to **Azure** as a **Global Administrator User**.
 - b. Navigate to **Azure Active Directory > App Registrations > New Registration**.
 - c. In the registration form, select your application.
 - d. Click **Register**.
3. Add the required permissions for Microsoft 365 Defender Incidents as per the following steps:
 - a. On the **Application Page**, select **API Permissions > Add a Permission > APIs my Organization uses**.
 - b. Type **Microsoft Threat Protection** on the search panel, and select **Microsoft Threat Protection**. Your application can now access **Microsoft 365 Defender**.
 - c. Choose **Application Permissions > Incident.Read.All** and select **Add Permissions**.
 - d. For more information regarding Azure Active Directory application with the appropriate permissions for Microsoft 365 Defender Incidents, see <https://docs.microsoft.com/en-us/microsoft-365/security/defender/api-hello-world?view=o365-worldwide>
4. Generate the Client Secret for the Application as per the following steps:
 - a. Click **Certificates and Secrets**.
 - b. Click **New Client Secret**.
 - c. Add **Description** to the secret and click **Add**.
 - d. Note the generated **Secret Value**.



Important: If you do not note down the **Secret Value**, you will not be able to retrieve it later.

- e. On the application page, go to **Overview** and **Copy** the following:
 - Application (Client) ID
 - Directory (Tenant) ID
 5. Select **Certificates & Secrets > Certificates**.
 6. Click **Upload Certificate** and select the required certificate file to be uploaded.
 7. Click **Add**.
- After the certificate is uploaded, the **Thumbprint**, **Start Date**, and **Expiration Values** are displayed.

Installing and Configuring the SmartConnector


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:

Start the installation wizard.

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 and then click **Next**.

Parameter	Description
Proxy Host (https)	(Optional) If proxy is enabled for your machine, the IP address or host name of the proxy server required for proxy configuration to access the internet.
Proxy Port	(Optional) If proxy is enabled for your machine, the port number of the proxy server required for proxy configuration.
Proxy User Name	(Optional) If proxy is enabled for your machine, the user name for the proxy server. Specify this value only if proxy needs access to the Internet. If you enter the proxy user name, you must provide the proxy password.
Proxy Password	(Optional) If proxy is enabled for your machine, the password for the proxy server user. Specify this value only if proxy needs access to internet and you have specified a user name for the proxy server.

Parameter	Description
Event URL	<p>This is a mandatory field.</p> <p>The URL from where you need to fetch events.</p> <p>The default value is: <code>https://graph.microsoft.com/beta/security/alerts_v2?\$filter=lastUpdateDateTime+ge+\$START_AT_TIME</code></p> <p>Sample URL for Graph API - alert V2 - <code>https://graph.microsoft.com/beta/security/alerts_v2?\$filter=lastUpdateDateTime+ge+\$START_AT_TIME</code></p> <p>Sample URL for Security API - <code>https://api.security.microsoft.com/api/incidents?\$filter=lastUpdateTime+gt+\$START_AT_TIME</code></p> <div>  <p>Note: If you want to fetch events of a specific period, use the startatime parameter in <code>agent.properties</code>. Do not remove "<code>\$START_AT_TIME</code>" in the URL.</p> </div> <p>Event URL will depend on the selected Alert Type.</p>
Authentication Method	<p>This is a mandatory field.</p> <p>An authentication method for authenticating using Certificate. You can select either Shared Secret or Certificate for the authentication method in Microsoft 365 defender.</p> <p>The default value is: Shared Secret</p>
Application (Client) ID	<p>The client application ID assigned to your application.</p> <p>This is a mandatory field when you select the Authentication Method parameter value as Shared Secret or Certificate both.</p>
Client Secret	<p>The client secret key generated for your application in the registration portal.</p> <p>This is a mandatory field when you select the Authentication Method parameter value as Shared Secret.</p>
Certificate Path	<p>The certificate file path(.pfx) that you will provide.</p> <p>This is a mandatory field when you select the Authentication Method parameter value as Certificate.</p>
Certificate Password	<p>The certificate password that you will provide.</p> <p>This is a mandatory field when you select the Authentication Method parameter value as Certificate.</p>

Parameter	Description
Token URL	The URL to get the access token. The default value is: <code>https://login.windows.net/{tenant_id}/oauth2/token</code> . It is mandatory that you must replace the {tenant_id} in the URL with <your Tenant ID>.
Resource URL	The URL to locate the resources. The default value is: <code>https://graph.microsoft.com</code> Sample URL for Security API - <code>https://api.security.microsoft.com</code> Sample URL for Graph API - alert V2 - <code>https://graph.microsoft.com</code> Resource URL will depend on the selected Alert Type .
Alert Type	The type of alert through which you want to fetch events. You can select any of the following alert types: <ul style="list-style-type: none"> Security API (For further information, visit this website). Graph API - alert V2 (For further information, visit this website).

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



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

9. Select whether you want to run the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).
12. For instructions about upgrading the connector or modifying 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](#).

Security API

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.

Graph API - alert V2

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

Alerts

- One alert event is sent for each evidence present in the alert.
- One top-level alert event is sent per alert.

Sample alert:

```
Alert1
{
  Evidence1
  Evidence2
}
```

ArcSight security event format expected by the connector:

1. Alert1 + Evidence1 (+ device evidence if applicable)
2. Alert1 + Evidence2 (+ device evidence if applicable)
3. Alert1 (top level alert event)

Event Mapping for Alerts via Security API

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

ArcSight ESM Field	Device-Specific Field
Device Custom Date 2	lastActivity
Device Custom String 1	threatFamilyName
Device Custom String 2	alertId
Device Custom String 6	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 5	__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 5	__oneOf (registryValue,userPrincipalName)
Device External ID	deviceId
File Create Time	processCreationTime
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

Event Mapping for Alert V2 via Graph API - alert V2

Alerts

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Event Class ID	category
Device Process Name	detectionSource
Device Receipt Time	lastUpdateDateTime
Device Severity	category
End Time	resolvedDateTime
Event Outcome	status
External ID	incidentid
flex Number1	evidenceCount
flex Number1Label	evidenceCount
flex String2	parentEvent
flex String2Label	parentEvent
Message	description
Name	title
Request URL	alertWebUrl
Start Time	createdDateTime

Device Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole
File Modification Time	firstSeenDateTime
Device External Id	mdeDeviceId
Destination Host Name	deviceDnsName
Device Custom String 3	osPlatform version osBuild
Additional Data	healthStatus

ArcSight ESM Field	Device-Specific Field
Old File Permission	riskScore
Source Translated Address	lastExternalIpAddress
Source Address	lastIpAddress
Device Inbound Interface	ipInterfaces
Source User Name	loggedOnUsers (accountName)
Source NT Domain	loggedOnUsers (domainName)

Process Evidence

ArcSight ESM Field	Device-Specific Field
Destination Process Id	processId
Old File Id	parentProcessId
Device Custom Date 1	processCreationDateTime
Device Custom Date 2	parentProcessCreationDateTime
Device Custom String 4	processCommandLine
Device Custom String 5	remediationStatus & remediationStatusDetails
Additional Data.Sha1	sha1
File Hash	sha256
File Name	fileName
File Path	filePath
File Size	fileSize
Old File Hash	parentProcessImageFile/sha256
Old File Name	parentProcessImageFile/fileName
Old File Path	parentProcessImageFile/filePath
Old File Size	parentProcessImageFile/fileSize
Destination User Name	__oneOf (userAccount/accountName,userAccount/userPrincipalName)
Destination NT Domain	userAccount/domainName
Destination User ID	userAccount/userSid

File Evidence

ArcSight ESM Field	Device-Specific Field
Additional Data	fileDetails/sha1
File Hash	fileDetails/sha256
File Name	fileDetails/fileName
File Path	fileDetails/filePath
File Size	fileDetails/fileName
Device Custom String 5	remediationStatus & remediationStatusDetails
User Evidence	
File Create Time	createdDateTime
Old File Type	evidenceRole
Destination User Name	__oneOf(userAccount_accountName,userAccount_userPrincipalName)
Destination NT Domain	userAccount/domainName
Destination User ID	userAccount/userSid

IP Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole
Device Custom String 5	remediationStatus & remediationStatusDetails
Source Address	ipAddress

Url Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	remediationStatus & remediationStatusDetails
Source DNS Domain	url

Registry Value Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole
Device Custom String 3	registryKey
Device Custom String 5	remediationStatus & remediationStatusDetails
Old File Permission	registryHive
Old File Path	registryValue
Old File Name	registryValueName
Additional Data	registryValueType

Cloud Application Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole
Device Custom String 5	remediationStatus & remediationStatusDetails
Old File ID	appId
Additional Data	displayName
File ID	instanceId
Old File Name	instanceName

Oauth Application Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	remediationStatus & remediationStatusDetails
Old File ID	appld
Additional Data	displayName
Old File Permission	objectId
Destination NT Domain	publisher

Analyzed Message Evidence

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	threats
Device Custom String 3 Label	Threats
Device Custom String 4	networkmessageid
Device Custom String 4 Label	Networkmessageid
Source Address	senderIp
Old File Type	evidenceRole
Device Custom String 5	remediationStatus & remediationStatusDetails
Device Custom String 5 Label	Remediation Status
Destination User Name	recipientEmailAddress
Source User Name	p1Sender/emailAddress
Source NT Domain	p1Sender/domain
Additional Data p2 Sender Domain	p2Sender/domain
Device Custom Number 1	urlCount
Device Custom Number 1 Label	urlCount
Device Custom Number 2	attachmentsCount
Device Custom Number 2 Label	attachmentsCount
Additional Data p2 Sender Email	p2Sender/emailAddress
Additional Data URLs	urls
Additional Data Delivery Action	deliveryAction
Destination Geo Location Info	deliveryLocation

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 365 Defender SmartConnector
(SmartConnectors 24.4.1)**

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 .

We appreciate your feedback!