Micro Focus Security ArcSight SmartConnectors

SmartConnector for Microsoft 365 Defender

Configuration Guide

Document Release Date: May 2022
Software Release Date: May 2022

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Trademark Notices

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

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

Contents

Configuration Guide for SmartConnector for Microsoft 365 Defender 6
Product Overview 6
Understanding Event Collection 6
Preparing to Install the SmartConnector 7
Registering an Azure Active Directory Application with appropriate permissions for Microsoft 365 Defender 7
Adding appropriate permissions for Microsoft 365 Defender Incidents 7
Adding appropriate permissions for Microsoft Defender for Endpoint 8
Adding a secret to the application 8
Installing and Configuring the SmartConnector by Using the Wizard 9
Device Event Mapping to ArcSight Fields 10
Incident 10
Alerts 11
Devices 12
Entities 12
Configuration Guide for SmartConnector for Microsoft 365 Defender 13
Product Overview 13
Understanding Event Collection 14
Preparing to Install the SmartConnector 14
Registering an Azure Active Directory Application with appropriate permissions for Microsoft 365 Defender 15
Adding appropriate permissions for Microsoft 365 Defender Incidents 15
Adding appropriate permissions for Microsoft Defender for Endpoint 15
Adding a secret to the application 16
Installing and Configuring the SmartConnector by Using the Wizard 16
Device Event Mapping to ArcSight Fields 17
Incident 18
Alerts 18
Devices 19
Entities 20
Configuration Guide for SmartConnector for Microsoft 365 Defender 21
Product Overview 21
Understanding Event Collection 21
Preparing to Install the SmartConnector 22
Registering an Azure Active Directory Application with appropriate permissions for Microsoft 365 Defender 22
Adding appropriate permissions for Microsoft 365 Defender Incidents 22
Adding appropriate permissions for Microsoft Defender for Endpoint 23

Adding a secret to the application 23
Installing and Configuring the SmartConnector by Using the Wizard 24
Device Event Mapping to ArcSight Fields 25
Incident 25
Alerts 26
Devices 27
Entities 27
Configuration Guide for SmartConnector for Microsoft 365 Defender 28
Product Overview 28
Understanding Event Collection 28
Preparing to Install the SmartConnector 29
Registering an Azure Active Directory Application with appropriate permissions for Microsoft 365 Defender 30
Adding appropriate permissions for Microsoft 365 Defender Incidents 30
Adding appropriate permissions for Microsoft Defender for Endpoint 30
Adding a secret to the application 31
Installing and Configuring the SmartConnector by Using the Wizard 31
Device Event Mapping to ArcSight Fields 32
Incident 33
Alerts 33
Devices 34
Entities 35
Configuration Guide for SmartConnector for Microsoft 365 Defender 36
Product Overview 36
Understanding Event Collection 36
Preparing to Install the SmartConnector 37
Registering an Azure Active Directory Application with appropriate permissions for Microsoft 365 Defender 37
Adding appropriate permissions for Microsoft 365 Defender Incidents 37
Adding appropriate permissions for Microsoft Defender for Endpoint 38
Adding a secret to the application 38
Installing and Configuring the SmartConnector by Using the Wizard 38
Device Event Mapping to ArcSight Fields 40
Incident 40
Alerts 41
Devices 42
Entities 42

Send Documentation Feedback 44

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.SSSSSSS'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**, complete the following procedures:

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 appropriate 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 app 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

Adding appropriate permissions for Microsoft Defender for Endpoint

1. Allow the application to access **Defender for Endpoint** and assign **Read all Alerts** permission. The following steps are required to add **API**:
   - On the application page, click **API Permissions** > **Add Permission** > **APIs my Organization uses**. Type **WindowsDefenderATP**, then click **WindowsDefenderATP**.
   - Choose **Application Permissions** > **Alert.Read.All**, then click **Add Permissions**.
2. Select **Grant Admin Consent**.

Note: You must select **Grant Admin Consent**, every time you add a new permission.

For more information about Azure Active Directory application with appropriate permissions for Microsoft Defender for Endpoint, see

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/api-hello-world?view=o365-worldwide

Adding a secret to the application

1. Click **Certificates** and **Secrets**.
2. Click on **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. Note your **Application ID** and **Tenant ID**
6. On the application page, go to **Overview** and **Copy** the following:

- Application (Client) ID
- Directory (Tenant) ID

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"

ArcSight ESM Field	Device-Specific Field
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 6	mitreTechniques
Device Event Category	category
Device Event Class ID	category
Device Process Name	detectionSource
Device Receipt Time	lastUpdatedTime
Device Severity	severity

ArcSight ESM Field	Device-Specific Field
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

ArcSight ESM Field	Device-Specific Field
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

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.SSSSSSS'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**, complete the following procedures:

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 appropriate 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 app 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

Adding appropriate permissions for Microsoft Defender for Endpoint

1. Allow the application to access **Defender for Endpoint** and assign **Read all Alerts** permission. The following steps are required to add **API**:
   - On the application page, click **API Permissions** > **Add Permission** > **APIs my Organization uses**. Type **WindowsDefenderATP**, then click **WindowsDefenderATP**.
   - Choose **Application Permissions** > **Alert.Read.All**, then click **Add Permissions**.
2. Select **Grant Admin Consent**.

Note: You must select **Grant Admin Consent**, every time you add a new permission.

For more information about Azure Active Directory application with appropriate permissions for Microsoft Defender for Endpoint, see

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/api-hello-world?view=o365-worldwide

Adding a secret to the application

1. Click **Certificates** and **Secrets**.
2. Click on **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. Note your **Application ID** and **Tenant ID**
6. On the application page, go to **Overview** and **Copy** the following:

- Application (Client) ID
- Directory (Tenant) ID

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

ArcSight ESM Field	Device-Specific Field
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 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

ArcSight ESM Field	Device-Specific Field
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

ArcSight ESM Field	Device-Specific Field
Old File Name	parentProcessFileName
Request Url	url
Source User Name	sender

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.SSSSSSS'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**, complete the following procedures:

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 appropriate 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 app can now access **Microsoft 365 Defender**.

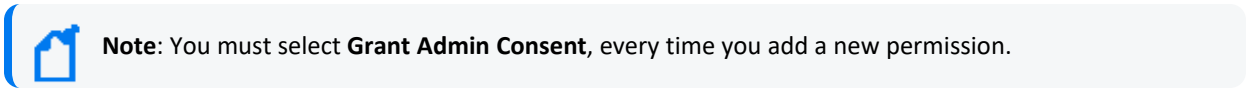
3. Choose **Application Permissions** > **Incident.Read.All** and select **Add Permissions**.

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

Adding appropriate permissions for Microsoft Defender for Endpoint

1. Allow the application to access **Defender for Endpoint** and assign **Read all Alerts** permission. The following steps are required to add **API**:
   - On the application page, click **API Permissions** > **Add Permission** > **APIs my Organization uses**. Type **WindowsDefenderATP**, then click **WindowsDefenderATP**.
   - Choose **Application Permissions** > **Alert.Read.All**, then click **Add Permissions**.
2. Select **Grant Admin Consent**.

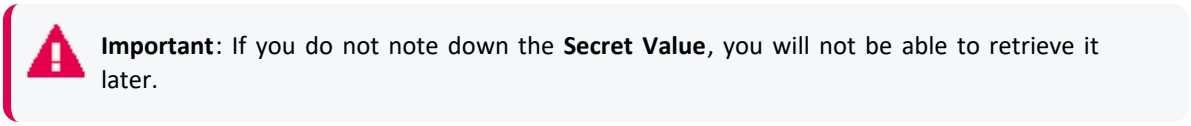


For more information about Azure Active Directory application with appropriate permissions for Microsoft Defender for Endpoint, see

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/api-hello-world?view=o365-worldwide

Adding a secret to the application

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



5. Note your **Application ID** and **Tenant ID**
6. On the application page, go to **Overview** and **Copy** the following:

- Application (Client) ID
- Directory (Tenant) ID

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

ArcSight ESM Field	Device-Specific Field
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 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

ArcSight ESM Field	Device-Specific Field
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)

ArcSight ESM Field	Device-Specific Field
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

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.SSSSSSS'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**, complete the following procedures:

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 appropriate permissions for Microsoft 365 Defender Incidents

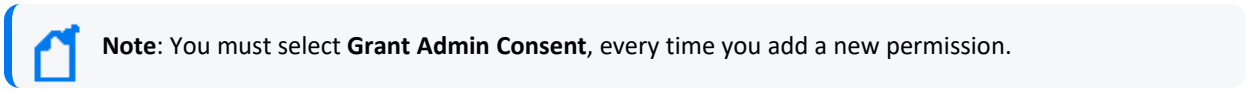
1. On the **Application Page**, select **API Permissions** > **Add a Permission** > **APIs my Organization uses**.
2. Type **Microsoft Threat Protection** on the search panel, and select **Microsoft Threat Protection**. Your app can now access **Microsoft 365 Defender**.
3. Choose **Application Permissions**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

Adding appropriate permissions for Microsoft Defender for Endpoint

1. Allow the application to access **Defender for Endpoint** and assign **Read all Alerts** permission. The following steps are required to add **API**:
   - On the application page, click **API Permissions** > **Add Permission** > **APIs my Organization uses**. Type **WindowsDefenderATP**, then click **WindowsDefenderATP**.
   - Choose **Application Permissions** > **Alert.Read.All**, then click **Add Permissions**.
2. Select **Grant Admin Consent**.



For more information about Azure Active Directory application with appropriate permissions for Microsoft Defender for Endpoint, see

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/api-hello-world?view=o365-worldwide

Adding a secret to the application

1. Click **Certificates** and **Secrets**.
2. Click on **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. Note your **Application ID** and **Tenant ID**
6. On the application page, go to **Overview** and **Copy** the following:

- Application (Client) ID
- Directory (Tenant) ID

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.

Parameter	Description
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

ArcSight ESM Field	Device-Specific Field
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 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

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.SSSSSSS'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**, complete the following procedures:

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 appropriate 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 app 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

Adding appropriate permissions for Microsoft Defender for Endpoint

1. Allow the application to access **Defender for Endpoint** and assign **Read all Alerts** permission. The following steps are required to add **API**:
   - On the application page, click **API Permissions** > **Add Permission** > **APIs my Organization uses**. Type **WindowsDefenderATP**, then click **WindowsDefenderATP**.
   - Choose **Application Permissions** > **Alert.Read.All**, then click **Add Permissions**.
2. Select **Grant Admin Consent**.

Note: You must select **Grant Admin Consent**, every time you add a new permission.

For more information about Azure Active Directory application with appropriate permissions for Microsoft Defender for Endpoint, see

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/api-hello-world?view=o365-worldwide

Adding a secret to the application

1. Click **Certificates** and **Secrets**.
2. Click on **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. Note your **Application ID** and **Tenant ID**
6. On the application page, go to **Overview** and **Copy** the following:

- Application (Client) ID
- Directory (Tenant) ID

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

ArcSight ESM Field	Device-Specific Field
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 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

ArcSight ESM Field	Device-Specific Field
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 8.3.1)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!