



ArcSight SmartConnector

Software Version: CE 24.4.1

Configuration Guide for Microsoft Azure Event Hub 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 Azure Event Hub SmartConnector	7
Product Overview	8
Azure Event Logs	8
Related Azure Services	9
Azure Event Log Categories	9
Understanding Data Collection	13
Prerequisites	15
Supported Event Hub Tiers	15
Setting User Permissions in Azure	15
Permission Requirements	15
Configuration	16
Creating a Resource Group	16
Creating an Event Hub Namespace	17
Creating an Event Hub	18
Registering the Application in Azure AD	19
For registration of the App, the following steps must be implemented:	20
For authenticating the App, the following steps must be implemented:	20
Assigning IAM Role	21
Streaming Logs	22
Installing the SmartConnector	27
Preparing to Install the SmartConnector	27
Installing and Configuring the SmartConnector by Using the Wizard	28
Adding Support for New Log Sources	31
Supported Log Sources	31
Adding Support for New Log Sources	33
Configuring Advanced Parameters	35
Accessing Advanced Parameters	35
Additional Connector Configuration for Defender for Endpoint Data Source	37
Connector limits the character length of the rawEvent field	37
Migrating the SmartConnector	39
Prevention of Data Loss	40
Hardware Consideration	42
Device Event Mapping to ArcSight Fields	43
Event Mappings for Active Directory	43
Common Event Mapping	43

Sign-in Logs Event Mapping	43
Audit Logs Event Mapping	44
Event Mappings for Microsoft Defender for Cloud	45
Common Event Mapping	45
Security Alerts Event Mapping	45
Security Recommendations Event Mapping	47
Event Mappings for Activity	47
Common Event Mapping	47
Action Event Mapping	47
Administrative Event Mapping	48
Alert Event Mapping	49
Delete Event Mapping	50
Recommendation Event Mapping	50
Security Event Mapping	51
Service Health Event Mapping	51
Write Event Mapping	52
Event Mappings for Resource Log	53
Common Event Mapping	53
Activity Runs Event Mapping	54
Application Gateway Access Log Event Mapping	55
Archive Logs Event Mapping	55
Audit Event Mapping	56
Authoring Event Mapping	56
Automatic Tuning Event Mapping	57
Azure Firewall Application Rule Event Mapping	57
Azure Firewall Network Rule Event Mapping	57
Azure Site Recovery Jobs Event Mapping	58
Blocks Event Mapping	58
C2D Command , C2D Twin Operations, and D2C Twin Operations Event Mapping	59
Database Wait Statistics Event Mapping	59
Deadlocks Event Mapping	60
Engine Event Mapping	60
Errors Event Mapping	61
Gateway Logs Event Mapping	61
Job Logs Event Mapping	62
Jobs Operations Event Mapping	62
Load Balancer Alert Event Mapping	63
Network Security Group Event Mapping	63
Operational Logs Event Mapping	63

P2S Diagnostic Logs Event Mapping	64
Postgre SQL Logs Event Mapping	64
Query Store Wait Statistics Event Mapping	65
Requests Event Mapping	65
Routes Event Mapping	66
Service Log Event Mapping	66
Timeouts Event Mapping	66
Trigger Runs Event Mapping	67
Twin Queries Event Mapping	67
Workflow Runtime Event Mapping	68
Event Mappings for Windows AD	68
Event 4624	68
Event 4625	69
Event 4648	70
Event 4768	73
Event 4769	74
Event 4770	75
Event 4771	75
Event 4772	75
Event 4773	76
Event 4776	76
Event 4777	76
Event 5137	77
Event 5139	77
Event 5140	77
Event 5141	78
Event 5145	78
Event 6272	79
Event 6273	79
Event 6274	80
Event 6275	80
Event 6276	80
Event 6277	81
Event 6278	81
Event Mappings for Defender for Endpoint	82
Troubleshooting	82
Reconfiguring the expired Client Secret or Client Certificate	82

Send Documentation Feedback	85
-----------------------------------	----

Configuration Guide for Microsoft Azure Event Hub SmartConnector

The Microsoft Azure Event Hub SmartConnector helps you monitor the activities on Microsoft Azure Cloud services.

This SmartConnector collects events and logs from the following Microsoft Azure log sources:

- Azure Active Directory
- Azure Monitor
- Microsoft Defender for Endpoint

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

Microsoft Azure is a set of cloud services to help organizations build, manage, and deploy applications on a massive, global network using their favorite tools and frameworks.

Azure Event Logs

The Microsoft Azure Event Hub connector collects the following event logs from Active Directory, Azure Monitor, and Microsoft Defender for Cloud in Azure:

- **Active Directory Logs**

- **Audit logs:** Provides records of system activities for compliance.
- **Sign-in logs:** Provides information related to user logins.



Note: To export Active Directory sign-in logs, you must have one of P1 or P2 premium editions of Azure Active Directory.

- **Activity Logs:** Provides data related to write operations, such as CREATE, UPDATE, and DELETE that were performed on resources in your subscription. For more information, see [Azure Activity log](#).
- **Resource Log (formerly known as Diagnostic Log):** Provides data related to operations performed within an Azure resource (the data plane).

Getting a secret from a key vault or making a request to a database. The content of resource log varies by the Azure service and resource type.

- **Microsoft Defender for Cloud**

- **Security alerts:** Provides data related to security actions performed on Microsoft Defender for Cloud in your subscription.
- **Recommendation logs:** Provides data related to prevention recommendations provided for the resources in your subscription.
- **Windows AD Logs:** Records details related to the system, security, and application stored on a Windows operating system. It contains information regarding hardware and software events occurring on a Windows operating system. It can be monitored to track system and application issues or forecast any potential issues.
- **Defender for Endpoint Logs:** Provides visibility into what is happening on a computer or other endpoint device. These logs include information about user activity, system activity, network connections, and more. These logs are also used to track suspicious activity, identify malware infections, and detect signs of data exfiltration or other malicious behavior. It can also be used to provide forensic evidence during the event of a security breach.

Related Azure Services

The following services are used when working with Microsoft Azure Event Hub SmartConnector:

- **Azure Resource Manager:** Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure subscription. You use management features, such as access control, locks, and tags, to secure and organize your resources after deployment. For more information, see [Azure Resource Manager](#).
- **Azure Event Hubs:** Azure Event Hubs is a big data streaming platform and event ingestion service. It can receive and process millions of events per second. Data sent to an event hub can be transformed and stored by using any real-time analytics provider or batching/storage adapters. For more information, see [Azure Event Hubs — A big data streaming platform and event ingestion service](#).

Azure Event Log Categories

Following tables list the categories for mappings supported by the Microsoft Azure Event Hub SmartConnector. The mappings are done using the schemas provided in the Azure documents.

Active Directory Log Categories

Categories	Certified
Signin	Yes
Audit	Yes

Activity Log Categories

Categories	Certified	Comments
Administrative	Yes	These are the sub-categories: <ol style="list-style-type: none">1. Action2. Write3. Delete For more information, see Azure Activity Log event schema .
Alert	Yes	Azure alerts.

Categories	Certified	Comments
Recommendation	Yes	Recommendation events from Azure Advisor.
Security	No	Same as Microsoft Defender for Cloud log events for Security Alert activity without remediation steps.
ServiceHealth	Yes	Service Health incidents occurred in Azure.

Resource Log Categories

Categories	Resource Type
AppServiceHTTPLogs	Microsoft.Web/sites
AppServiceIPSecAuditLogs	Microsoft.Web/sites
GatewayLogs	Microsoft.ApiManagement/service
JobLogs	Microsoft.Automation/automationAccounts JobStreams
JobStreams	Microsoft.Automation/automationAccount
CoreAnalytics	Microsoft.Cdn/profiles/endpoints
PipelineRuns	Microsoft.DataFactory/factories
TriggerRuns	Microsoft.DataFactory/factories
Audit	Microsoft.DataLakeAnalytics/accounts
Requests	Microsoft.DataLakeAnalytics/accounts
Audit	Microsoft.DataLakeStore/accounts
Requests	Microsoft.DataLakeStore/accounts
Connections	Microsoft.Devices/IotHubs
DeviceTelemetry	Microsoft.Devices/IotHubs
C2DCommands	Microsoft.Devices/IotHubs
DeviceIdentityOperations	Microsoft.Devices/IotHubs
FileUploadOperations	Microsoft.Devices/IotHubs
Routes	Microsoft.Devices/IotHubs
D2CTwinOperations	Microsoft.Devices/IotHubs
C2DTwinOperations	Microsoft.Devices/IotHubs
TwinQueries	Microsoft.Devices/IotHubs
JobsOperations	Microsoft.Devices/IotHubs
DirectMethods	Microsoft.Devices/IotHubs

Categories	Resource Type
DataPlaneRequests	Microsoft.DocumentDB/databaseAccounts
ArchiveLogs	Microsoft.EventHub/namespaces
OperationalLogs	Microsoft.EventHub/namespaces
AuditEvent	Microsoft.KeyVault/vaults
WorkflowRuntime	Microsoft.Logic/workflows
NetworkSecurityGroupEvent	Microsoft.Network/networksecuritygroups
NetworkSecurityGroupRuleCounter	Microsoft.Network/networksecuritygroups
LoadBalancerAlertEvent	Microsoft.Network/loadBalancers
LoadBalancerProbeHealthStatus	Microsoft.Network/loadBalancers
ApplicationGatewayAccessLog	Microsoft.Network/applicationGateways
ApplicationGatewayPerformanceLog	Microsoft.Network/applicationGateways
ApplicationGatewayFirewallLog	Microsoft.Network/applicationGateways
OperationalLogs	Microsoft.ServiceBus/namespaces
QueryStoreRuntimeStatistics	Microsoft.Sql/servers/databases
QueryStoreWaitStatistics	Microsoft.Sql/servers/databases
Errors	Microsoft.Sql/servers/databases
DatabaseWaitStatistics	Microsoft.Sql/servers/databases
Timeouts	Microsoft.Sql/servers/databases
Blocks	Microsoft.Sql/servers/databases
Audit	Microsoft.Sql/servers/databases
Execution	Microsoft.StreamAnalytics/streamingjobs
Authoring	Microsoft.StreamAnalytics/streamingjobs
AzureFirewallApplicationRule	Microsoft.Network/AzureFirewalls
AzureFirewallNetworkRule	Microsoft.Network/AzureFirewalls
ServiceLog	Microsoft.Batch/batchAccounts
SQLSecurityAuditEvents	Microsoft.Sql/servers/databases
SQLSecurityAuditEvents	Microsoft.Synapse/workspaces
AutomaticTuning	Microsoft.Sql/servers/databases
Deadlocks	Microsoft.Sql/servers/databases
ActivityRuns	Microsoft.DataFactory/factories
AzureBackupReport	Microsoft.RecoveryServices/Vaults

Categories	Resource Type
AzureSiteRecoveryEvents	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryJobs	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryProtectedDiskDataChurn	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryRecoveryPoints	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicatedItems	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicationDataUploadRate	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicationStats	Microsoft.RecoveryServices/Vaults
DscNodeStatus	Microsoft.Automation/automationAccounts
Engine	Microsoft.PowerBI
Engine	Microsoft.AnalysisServices/servers
GatewayDiagnosticLog	microsoft.network/p2svpngateways
GatewayDiagnosticLog	microsoft.network/virtualnetworkgateways
GatewayDiagnosticLog	microsoft.network/vpngateways
IkeDiagnosticLog	microsoft.network/p2svpngateways
IkeDiagnosticLog	microsoft.network/virtualnetworkgateways
IkeDiagnosticLog	microsoft.network/vpngateways
Operationlogs	microsoft.loadtestservice/loadtests
Operationlogs	Microsoft.Search/searchServices
P2Sdiagnosticlog	microsoft.network/virtualnetworkgateways
P2Sdiagnosticlog	microsoft.network/p2svpngateways
Routediagnosticlog	microsoft.network/virtualnetworkgateways
Routediagnosticlog	microsoft.network/vpngateways
OperationalLogs	Microsoft.NotificationHubs/namespaces
OperationalLogs	Microsoft.ServiceBus/Namespaces
PostgreSQLLogs	Microsoft.DBforPostgreSQL

Microsoft Defender for Cloud Log Categories

Categories	Resource Type	Certified
Securityalerts	All resources	Yes
SecurityRecommendations	All resources	Yes

Windows AD Log Categories

Categories	Resource Type	Certified
Security	All resources	Yes

Defender for Endpoint Log Categories



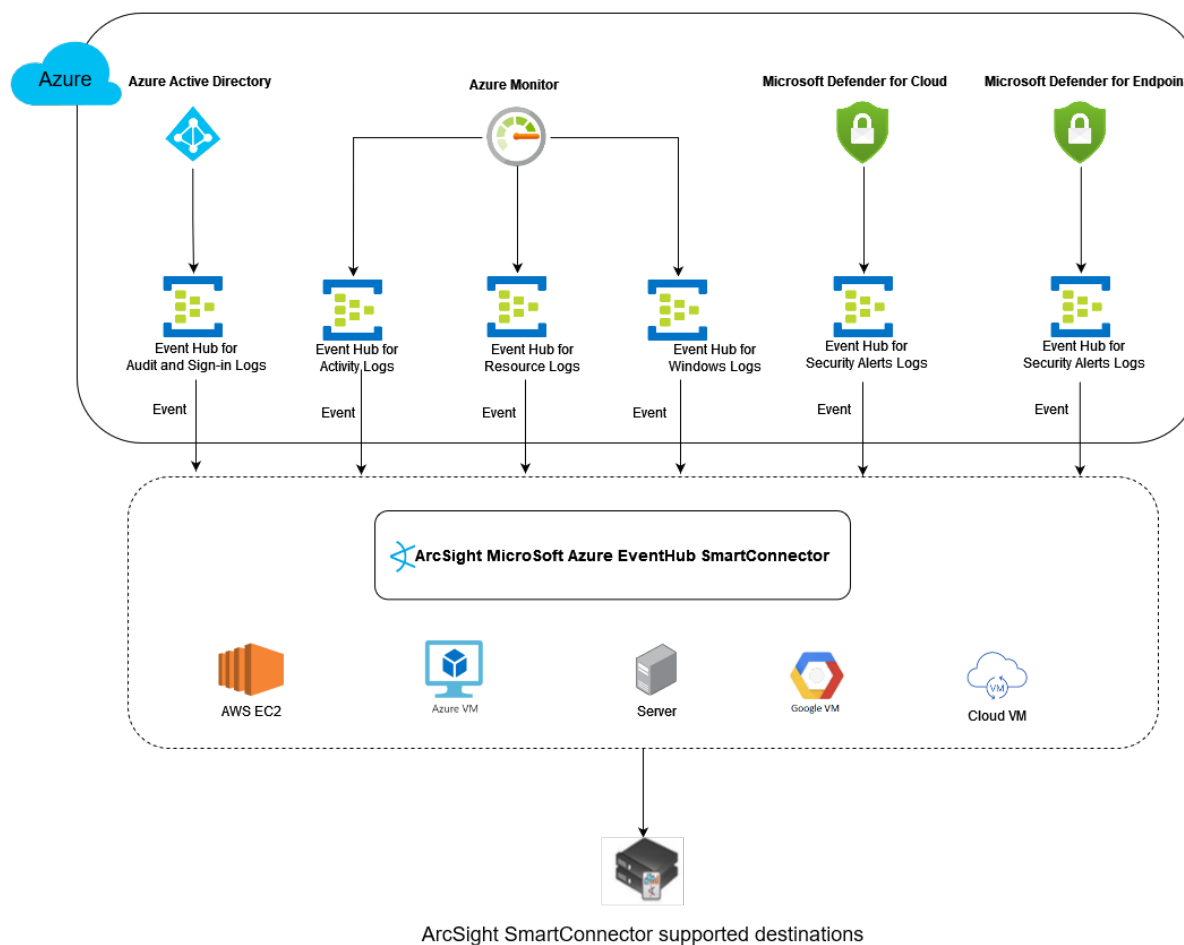
Important: The Defender for Endpoint Log Categories is supported only for **ArcSight Intelligence** deployments. In this case, the Microsoft Azure Event Hub SmartConnector acts as a carrier and sends events to the ArcSight supported destinations without normalizing the events. You can install the Microsoft 365 Defender SmartConnector to process the Microsoft 365 defender events. For more information, see [Configuration Guide for Microsoft 365 Defender SmartConnector](#).

Categories	Certified
Device Alert Events	Yes
Device Info	Yes
Device Network Info	Yes
Device Process Events	Yes
Device Network Events	Yes
Dynamic Event Collection	Yes
Device Registry Events	Yes
Device Logon Events	Yes
Device Image Load Events	Yes
Device Events	Yes

The Microsoft Azure Event Hub SmartConnector currently includes mapping files for several log categories of activity, audit, sign-in, resource, and windows Active Directory log categories. If schemas are not available for any category in Azure documents, then, the mappings for these categories are not available in the connector. Such events are sent unparsed to the ArcSight destination.

Understanding Data Collection

The following diagram provides a high-level overview of how the Microsoft Azure Event Hub SmartConnector collects and sends data to ArcSight's destinations.



Understanding the process flow of data collection

1. Before installing the Microsoft Azure Event Hub SmartConnector, configure the required Event Hubs to stream the raw data. See [Streaming Logs](#).
2. After installing, ArcSight Microsoft Azure Event Hub SmartConnector collects logs in JSON format and then sends the events to the ArcSight SmartConnector supported destination.

Prerequisites

- [Supported Event Hub Tiers](#)
- [Setting User Permissions in Azure](#)

Supported Event Hub Tiers

Azure Event Hubs is a fully-managed, real-time data ingestion service that is simple, secure and scalable. Event Hubs lets you stream millions of events per second from any source so you can build dynamic data pipelines and respond to business challenges immediately. Keep data ingestion secure with geo-disaster recovery and geo-replication options.

With Azure Event Hubs for Apache Kafka, you can enable existing Kafka clients and applications to talk to Event Hubs without any code changes, giving you a managed Kafka experience without having to manage your own clusters.

The following tiers are supported: Standard, Premium, and Dedicated. For more information, refer to this [Microsoft Documentation](#).

Next Step: [Setting User Permissions in Azure](#)

Setting User Permissions in Azure

In Azure, users must be associated with a subscription to provide them with access to resources such as Resource group, Event Hub namespace, and Event hubs. Therefore, you must determine the subscription you want to use for Microsoft Azure Event Hub SmartConnector and add users to the required subscription. You must also assign users to a role to define their permission to perform tasks.

Permission Requirements

Scope	Description
Azure Subscription	The users must have the Security Administrator IAM role on the subscription.
Resource group	The users must create a resource group. The users must ensure that they are assigned the Application Administrator role and Owner role on the resource group before deploying the connector.

Configuration

The following configuration steps must be implemented before installing the connector:

Creating a Resource Group

1. Log in to the Azure portal and navigate to the **Resource Group** service.
2. Click **+Create**.
3. Select the **Subscription** and enter a name for the group in the **Resource group** field.
4. Navigate to **Resource details** and select the region.
5. (Optional) Click **Next:Tags** to create a tag for the group.

6. Click **Next:Review > +Create**.

The screenshot shows the 'Create a resource group' page in the Microsoft Azure portal. The page has a blue header with the 'Microsoft Azure' logo and a search bar. Below the header, there's a breadcrumb trail: 'Home > Resource groups >'. The main heading is 'Create a resource group'. There are three tabs: 'Basics' (selected), 'Tags', and 'Review + create'. A description of a 'Resource group' is provided. Under 'Project details', there are two fields: 'Subscription' (a dropdown menu) and 'Resource group' (a text input field). Under 'Resource details', there is a 'Region' dropdown menu set to '(US) East US'. At the bottom, there are three buttons: 'Review + create', '< Previous', and 'Next : Tags >'.

Creating an Event Hub Namespace

1. Log in to the Azure portal and navigate to the **Event Hubs** service.
2. Click **+Create**.
3. Select the **Subscription** and the **Resource group** that is created above.
4. Navigate to **Instance Details** and enter a name in the **Namespace name** field.

5. Select the same **Location** that is selected while creating the **Resource Group**.
6. Select the pricing tier according your requirement. Ensure the selected pricing tier supports Apache Kafka. Refer to this [Microsoft documentation](#) for more plans.
7. Click **Review + Create**.

The screenshot shows the 'Create Namespace' page for Event Hubs in the Microsoft Azure portal. The page is divided into two main sections: 'Project Details' and 'Instance Details'. In the 'Project Details' section, there are dropdown menus for 'Subscription' and 'Resource group', with a 'Create new' link below the 'Resource group' dropdown. In the 'Instance Details' section, there are fields for 'Namespace name', 'Location', 'Pricing tier', and 'Throughput Units'. The 'Namespace name' field has a placeholder '.servicebus.windows.net'. The 'Location' dropdown is set to 'East US', with a note indicating that the region supports Availability zones. The 'Pricing tier' dropdown is empty, with a link to 'Browse the available plans and their features'. The 'Throughput Units' field is a slider set to 1. At the bottom of the page, there are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next: Advanced >'.

Creating an Event Hub

1. Click the **Namespace** that is created above.
2. Navigate to **Event Hubs > +Event Hub**.

3. Enter a **Name** for the hub and select the **Partition count**. For more information regarding Partition count, refer to this [Microsoft Documentation](#).
4. Navigate to **Retention**. Select the **Cleanup policy** and choose the required **Retention time**.
5. Click **Review + create**.

Create Event Hub ...

Event Hubs

Basics Capture Review + create

Event Hub Details

Enter required settings for this event hub, including partition count and message retention.

Name * ⓘ

Partition count ⓘ 2

Retention

Configure retention settings for this Event Hub. [Learn more](#)

Cleanup policy ⓘ

Retention time (hrs) ⓘ min. 1 hour, max. 24 hours (1day)

Review + create < Previous Next: Capture >

**Note:**

- Ensure to select the same **Subscription** and **Region** while creating the **Resource Group** and **Event Hub Namespace**.
- Creating a Resource Group and Event Hub Namespace is a one-time activity. For each data source, all the Event Hubs must be created under the same Event Hub Namespace.

Registering the Application in Azure AD

Azure Active Directory applications streamline secure access and authentication for Azure cloud resources, enabling centralized identity management and seamless integration with a

wide range of applications and services.

Azure AD applications provide robust security measures such as multi-factor authentication, conditional access policies, and role-based access control, ensuring authorized access and protecting against unauthorized entry.

For registration of the App, the following steps must be implemented:

1. Log in to Azure Portal.
2. Navigate to **Azure Active Directory** and select **App registrations**.
3. Click **+New registration** to create a new application registration.
4. Enter a name for the application, select the appropriate account type and click **Register**.

For authenticating the App, the following steps must be implemented:

The connector supports two methods of authentication: **Client Certificate** and **Client Secret**. You can choose either of them.



Note: From a security standpoint, **Client Certificates** are often considered to be more secure than **Client Secrets**.

1. If **Client Certificate** method is opted.

To generate the self-signed certificate implement the following steps:

- a. Open the command prompt and run the below command by replacing the certificate filename, password and validity days.

```
keytool -genkey -keystore <filename.pfx> -storetype PKCS12 -keyalg RSA -storepass <password> -validity <days> -keysize 2048
```

This will generate the .pfx certificate file. This certificate will be provided while installing the connector when **Client Certificate** mechanism is used for authentication.

- b. Run the below command to generate .cer certificate file by replacing the same filename and password as mentioned in the above step.

```
keytool -export -keystore <filename.pfx> -file <client.cer> -storetype PKCS12 -storepass <password>
```

This will generate the .cer certificate file. This must be uploaded in the Azure portal to authenticate the connector to access the Azure AD application. Implement the following steps to upload this certificate to the Azure portal:

- i. Navigate to the Application that is registered in step 3 and click **Certificates & secrets**.
- ii. Under **Certificates > Upload Certificate**.
- iii. Select the public key file of the certificate **.cer** file. Enter a meaningful description to it. Then click **Add**.

Certificate will be listed in **Certificates** section.

2. If **Client Secret** is opted then implement the following steps to configure the Client Secret in Azure:
 - a. Navigate to the application that is registered in step 3 and click **Certificates & secrets**.
 - b. Under **Client Secret > +New Client Secret**.
 - c. Enter a **Description** to the secret. Set the value for expiry and click **Add**. This will generate the **Client Secret**.



Important: Note the generated Secret Key Value to provide the same while installing and configuring the connector. If you do not note down the Secret Value, you will not be able to retrieve it later.



Note: Ensure to note the expiry date of the **Client Secret** and **Client Certificate**. After the Client Secret/ Certificate expires, the connector will fail to authenticate the application and it will stop working. To reconfigure the new Client Secret or Client Certificate, see the [Troubleshooting](#) section.

Assigning IAM Role

IAM role must be assigned to this application in Event Hubs Namespace to allow the application to read data from Azure Event Hub.

To assign IAM role:

1. Navigate to **Event Hubs Namespace** created [here](#) and select **Access Control (IAM)**.
2. Click **Role Assignments > +Add** and select **Add role assignment**.
3. Assign **Azure Event Hubs Data Receiver** role and click **Next**.



Note: If you want to configure the SmartConnector to use **Microsoft Azure Event Hub** as a destination, an additional role as **Azure Event Hubs Data Sender** is required to send events to Microsoft Azure Event Hub.

4. Click **+Select members** and select the registered application.
5. Click **Next > Review + Assign**.

Streaming Logs

Azure Active Directory Logs

To send Azure Active Directory events to Event Hub, follow these steps:

1. Log in to the Azure portal.
2. Navigate to **Azure Active Directory** and select **Diagnostic settings**.
3. Click **+Add Diagnostic Setting** and then enter a name for **Diagnostic setting name**.
4. Navigate to **Categories** and select **AuditLogs and SignInLogs**.
5. (Optional) For Intelligence, only **SignInLogs** must be enabled.
6. Navigate to **Destination details** and select **Stream to an event hub** as the destination.
7. Select the required **Subscription, Event Hub Namespace, Event Hub Name** and ensure to save the settings.

Activity Logs

To send Activity events to Event Hub, follow these steps:

1. Log in to the Azure portal.
2. Select the **Resource Group** from which you want to stream the **Activity Logs**.
3. Click **Activity Log > Export Activity Logs Settings**.
4. Click **+ Add Diagnostic Setting** and enter a name for **Diagnostic setting name**.
5. Navigate to **Categories**. Select the log categories that are required to be enabled.
6. Navigate to **Destination details** and select **Stream to an event hub** as the destination.
7. Select the required **Subscription, Event hub namespace, Event hub name** and ensure to save the settings.

Microsoft Defender for Cloud Event Logs

To send Microsoft Defender for Cloud events to Event Hub, follow these steps:

1. From the left sidebar, select **Microsoft Defender for Cloud**, and then click **Environment Setting**.
2. Select the specific subscription to be used when configuring data export.
3. On the **Subscription** settings, go to the sidebar and select **Continuous Export**.
4. Select the data type to be exported and choose from the filters on each type.
5. From **Export target**, choose the required **Subscription, Event Hub namespace, Event Hub name**, and **Event hub policy name**.

For the Event hub policy name:

- a. Navigate to the required Event Hub to which you want to stream the logs.
 - b. Click **Shared access policy** tab > **+Add** to create a new policy and enter a name for it.
 - c. Select the required permissions and click **Create**.
6. Save your changes.

Resource Logs

You must manually add diagnostic settings to configure streaming of these logs. The following procedure provides a brief overview of settings required for streaming Diagnostic Logs. For information, see [Azure documentation](#).

1. Select **Azure Home > Monitor > Diagnostic Settings**.
2. Select the required **Subscription**, **Resource group**, **Resource type**, and **Resource** from the drop-down.
3. Click **+Add diagnostic setting** and add a name for it.
4. Select the required log categories under **Logs** section.
5. Navigate to **Destination details** and select **Stream to an event hub** as the destination.
6. Select the required **Subscription**, **Event hub namespace**, **Event hub name** and ensure to save the settings.

Windows AD Logs

Azure Monitor Agent (AMA) collects the monitoring data from the guest operating system of Azure and hybrid virtual machines and delivers it to the Azure Monitor for use by features, insights, and other services.

Azure Monitor Agent uses data collection rules, where you define which data you want each agent to collect. Data collection rules let you manage data collection settings at scale and define unique, scoped configurations for subsets of machines. You can define a rule to send data from multiple machines to multiple destinations across regions and tenants. For more information refer to this [Microsoft Documentation](#).

Azure Monitor Agent must be installed on the resource to collect the Windows AD data. The resource can be either Azure or Non-Azure resource.

- **Azure Resources:** Azure Resources includes Azure VM.
- **Non-Azure Resources:** Non-Azure Resources includes the physical servers and virtual machines hosted outside of Azure (that is on-premises) or in other clouds.

To collect the Windows AD data from Non-Azure Resources, implement the following steps:

1. Establish connection between Non-Azure Resources and Azure.

Different methods can be used or connecting the machines in your hybrid environment directly with Azure. For connecting machines using a deployment script, implement the steps mentioned in the [Microsoft Documentation](#).

Generate the installation script from the Azure portal. This will download and install the **Microsoft Monitoring Agent** and establish the connection with Azure Arc.



Note: For authentication, log in using the pop-up browser while running the script.

Ensure the machine is registered in the Azure portal under **Servers-Azure Arc** after the successful execution of the script. This will confirm the connection establishment.

2. Register the Server extension for Azure Monitor Agent.

Azure Monitor Agent for Windows is an extension that can be installed on servers registered with Azure Arc to collect and send data to Azure Monitor.

- a. Navigate to **Servers-Azure Arc** and select the registered server.
- b. Navigate to **Settings** and click **Extension > +Add**.
- c. Select **Azure Monitor Agent for Windows** extension and click **Next**.
- d. Click **Review + Create**.

This will only install the agent. You must use Data Collection Rule to configure Azure Monitor Agent's data collection settings for it to start working.

3. Create a Log Analytics workspace in Azure.

- a. Log in to Azure portal.
- b. Navigate to **Log Analytics workspaces** and click **+ Create**.
- c. Specify the Resource group created [here](#).
- d. Enter a name for the workspace and select the same region that was selected while creating the Resource group.
- e. Click **Review+Create**.

4. Configure the **Azure Monitoring Agent** to send the logs to the Log Analytical workspace.

- a. Creating a Data Collection Rule in Azure Monitor (For more information regarding this, see this [Microsoft Documentation](#)):
 - i. Log in to Azure portal.
 - ii. Navigate to **Monitor** and select **Data Collection Rules**.
 - iii. Click **+Create** to create a new data collection rule and associations.

- On the Basics tab:
 - A. Enter a **Rule** name and specify the **Subscription, Resource Group, Region,** and **Platform Type**. Region specifies where the DCR will be created. The virtual machines and their associations can be in any subscription or resource group in the tenant.
 - B. Select the same region as your [Log Analytics workspace](#). Platform Type specifies the type of resources in which the rule can be applied. The Custom is for both Windows and Linux.
- On the Resources tab:
 - A. Click **+ Add resources** to add associated resources to the data collection rule. These resources can be Virtual Machines, Virtual Machine Scale Sets, and Azure Arc for servers. The Azure portal installs Azure Monitor Agent on those resources where it is not installed.
 - B. Select the resource group that is created [here](#) and specify the required resources. Click **Apply**.
- On the Collect and Deliver tab:
 - A. Click **+Add data source** to add a data source and select a destination.
 - B. Select the data source type and the data to collect for the resources. Select **Windows Event Logs**.
 - C. Select **Basic** to enable collection of event logs. **Select** Custom if you want control over the collected event logs.
 - D. Navigate to **Security** and enable both **Audit Success** and **Audit Failure** to configure the security event logs.
 - E. Click **Next:Destination>** to configure the destination to the data sources.
 - F. Click **+Add** to select destination and for sending Windows event data sources to Azure Monitor Logs only.
 - G. Select **Destination type** as **Azure Monitor Logs** and select the required Subscription.
 - H. Select the Log Analytics workspace that is created [here](#).
 - I. Click **Add data source > Review + Create** to review the details of the data collection rule associated with the set of virtual machines.
 - J. Select **+Create** to create the data collection rule.
- b. Creating a Data Export Rule in Azure Monitor:

- i. Log in to the Azure portal and Navigate to **Log Analytics workspace** created [here](#).
- ii. Navigate to **Settings** and select **Data Export > New export rule**.
 - On the Basics tab:
 - A. Enter a name For the Export rule.
 - B. Check the **Enable upon creation** check box and click **Next**.
 - On the Source tab:
 - A. Select the **Event table** and click **Next**.
 - On the Destination tab:
 - A. Select **EventHub** as **Destination**.
 - B. In **Destination details** and select the required **Subscription** and the **Event Hub Namespace** created [here](#).
 - C. Enter the **Event hub Name** for configuring the windows logs.
 - D. Click **Next** to create the Export rule.

Defender for Endpoint Logs

1. Log in to Microsoft Defender Security Center.
2. Click **Partners & APIs > Data export settings**.
3. Click **+Add data export settings** to add the export rule.
4. Provide a name to the export rule and select **Forward events to Azure Event Hub**.
5. Provide the **Event-hub Resource Id** of the Event Hub namespace that is created [here](#).
Navigate to Properties > Settings and copy the **Id** under **Essentials** Section.
6. Enter the Event Hub name to stream the Defender for Endpoint logs.
7. Select the types of events that the raw data streaming API senses and click **Save**.

Microsoft Azure

Search resources, services, and docs (G+/I)

Home > jb-emitter-arc-sight

NamespaceDemo | Properties

Event Hubs Namespace

Search Refresh

Essentials

Id /subscriptions/... Copy to clipboard

Name jb-emitter-arc-sight

Type Microsoft.EventHub/Namespaces

Location East US

Tags View value as JSON

SKU View value as JSON

Identity ---

System data ---

Encryption

Key vault properties ---

Key source ---

Require infrastructure enc... ---

Properties

Provisioning state Succeeded

Status Active

Created at 12/23/2022, 1:10:43 PM

Updated at 3/9/2023, 10:06:26 AM

Service bus endpoint https://.../

Cluster arm id ---

Metric id ---

Is auto inflate enabled false

Maximum throughput units 0

Kafka enabled true

Zone redundant false

Private endpoint connecti... ---

Disable local auth false

Note: This data source is for ArcSight Intelligence only and is specific to the current release.

Installing the SmartConnector

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText 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:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector by Using the Wizard

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

To install and configure the Azure Event Hub 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 Azure Event Hub** as the type of connector, then click **Next**.
5. Enter the following SmartConnector parameter values, then click **Next**:

Connector Setup

opentext™ ArcSight

Configure

Enter the parameter details

Host:Port

Directory (tenant) ID

Application (client) ID

Credential Type: Client Secret

Client Secret

Client Certificate

Client Certificate Password

Event Hub for 'Azure AD': insights-activedirectory-logs

Event Hub for 'Activity': insights-operational-logs

Event Hub for 'Defender for Cloud': insights-defender-logs

Event Hub for 'Resource': insights-resource-logs

Event Hub for 'Windows AD': insights-monitorwindows-logs

Event Hub for 'Defender for Endpoint': insights-defender-endpoint-logs

Read Events From: latest

< Previous **Next >** Cancel

Parameters	Description
Host:Port	Enter the host and port of Event Hubs Namespace. Select the Event Hub from the Event Hub Namespace list and copy the host value from the Overview section. The recommended port value is 9093.
Directory (tenant) ID	Enter the Directory (tenant) ID of your registered application. For this value, refer to the Overview section of the application.
Application (Client) ID	Enter the Client ID generated for your registered application. For this value, refer to the Overview section of the application.
Credential Type	If Client secret is selected, then client secret will be used to authenticate the app. If Client certificate is selected, then client certificate will be used to authenticate the app

Parameters	Description
Client Secret	Enter the client secret value generated as mentioned in step 2 . This value is obfuscated. This field is mandatory if the Credential Type is Client secret. For detailed information, see Troubleshooting .
Client Certificate	Specify the client certificate path. This field is mandatory if the Credential Type is Client certificate. For detailed information, see Troubleshooting .
Client Certificate Password	Enter the password of client certificate.
Event Hub for 'Azure AD'	Enter the event hub name for Azure AD.
Event Hub for 'Activity'	Enter the event hub name for Activity.
Event Hub for 'Defender for Cloud'	Enter the event hub name for Defender for Cloud.
Event Hub for 'Resource'	Enter the event hub name for Resource.
Event Hub for 'Windows AD'	Enter the event hub name for Windows AD.
Event Hub for 'Defender for Endpoint'	Enter the event hub name for Defender for Endpoint.
Read Events From	Specify the value from where the connector will read the events.

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 install 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 [Installation and User Guide for SmartConnector](#).



Note: For the Defender for Endpoint events, ensure to enable the **Preserve Raw Event** option while configuring the destination. Refer the steps mentioned here under [Configuring Processing in Configuring Destination Settings](#).

Adding Support for New Log Sources

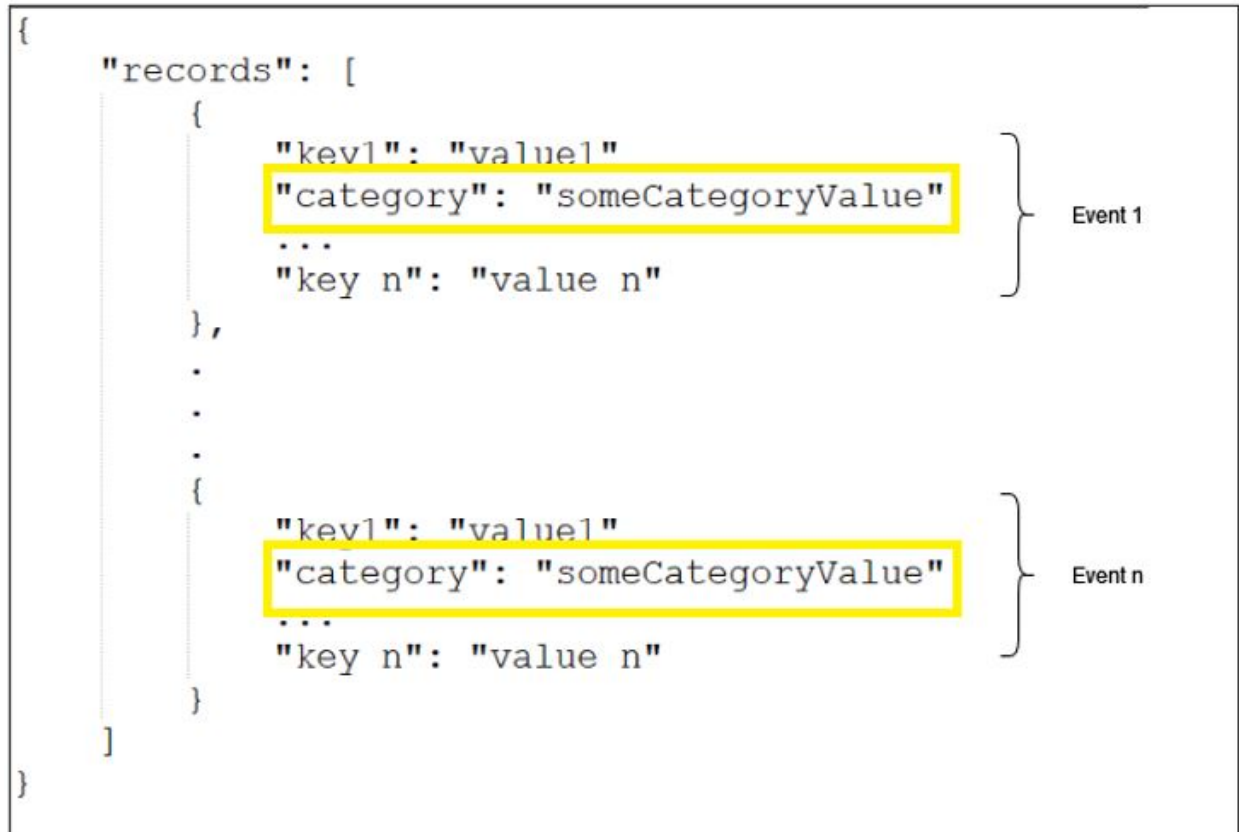
The Microsoft Azure Event Hub SmartConnector supports new log sources because it is flexible in the parser loading technique without needing any code changes.. Most of the Azure activities go through the Microsoft Azure Monitor Event Hub by following the standard schema and reach Event Hub.

Supported Log Sources

The Microsoft Azure Event Hub SmartConnector supports logs with the following conditions without having any framework changes:

All events that are sent to Event Hub must be specified within the "records" key containing the "category" key. The events must be in the Json format.

```
{  
  "records": [  
    {  
      "key1": "Value1",  
      "key2": "Value2",  
      ...  
      "Key n": "Value n"    } Event 1  
    },  
    {  
      "key1": "Value1",  
      "key2": "Value2",  
      ...  
      "Key n": "Value n"    } Event 2  
    },  
    .  
    .  
    .  
    {  
      "key1": "Value1",  
      "key2": "Value2",  
      ...  
      "Key n": "Value n"    } Event n  
    }  
  ]  
}
```

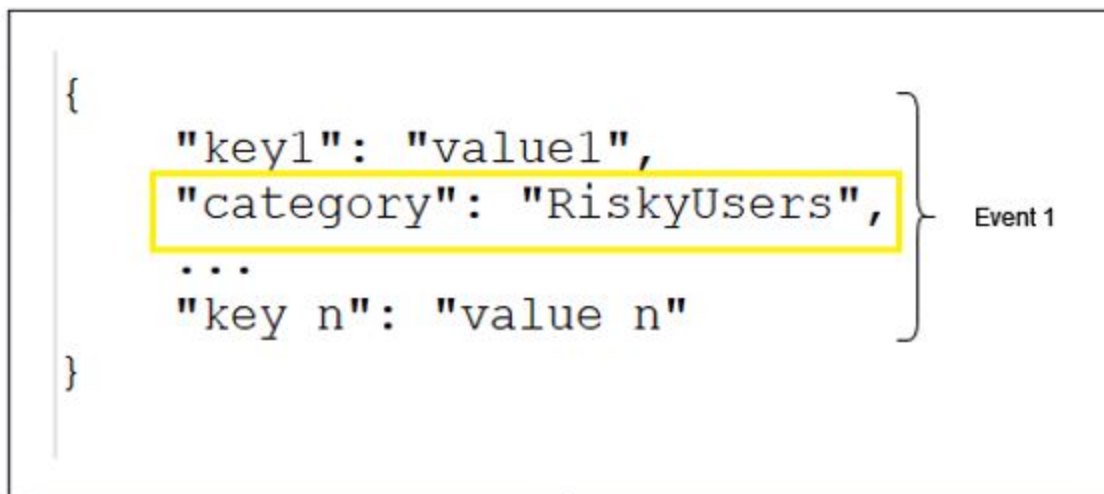




Adding Support for New Log Sources

Perform the following steps to add support for the new log sources:

1. Create a Json parser and then create the mappings. The value specified for the **"category"** field is considered as a name of the parser file.

For example, if the raw event appears as follows, then the parser file name will be `riskyusers.jsonparser.properties`.



 **Note:** Ensure that the parser file name is in lower case.

2. Perform the following steps to override a parser file:
 - a. Download ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-X.X.X.XXXX.X.zip file.
 - b. Unzip the downloaded file to a temporary location.
 - c. Locate and copy the **azureeventhub** folder to <ARCSIGHT_HOME>/current/user/agent/fcp/.
 - d. Delete the unzipped directory from a temporary location.

The directory structure appears as follows:

Name	Date modified	Type	Size
 activedirectory		File folder	
 activity		File folder	
 defendercloud		File folder	
 defenderendpoint		File folder	
 resource		File folder	
 windowsad		File folder	

3. The Event Hubs are created at this step. Choose the Event Hub you want to send the data to and create your data collection rules as required.
4. Event Hubs and directories mentioned in [Step 1](#) are directly related. Copy the parser file in the directory that is related to the event hub to which you are sending the data.

The following table describes the relation between the parser folder and event hubs:

If data is sent to	Folder to copy a Parser file
Event Hub for 'Azure AD'	activedirectory
Event Hub for 'Resource'	resource
Event Hub for 'Activity'	activity
Event Hub for 'Defender for Cloud'	defendercloud



Note: Do not send the data to Event Hubs that are created for **Windows AD** or **Defender for Endpoint**.

5. Restart the connector.

The connector will start processing the events.

Configuring Advanced Parameters

Accessing Advanced Parameters

After installing the SmartConnector, you can edit the `agent.properties` file to modify the parameters. This file is located at `$ARCSIGHT_HOME\current\user\agent` directory.

1. Advanced Kafka Configuration Parameters

Parameter	Default	Specify
consumerthreadcount	1	Number of Kafka consumer threads that will be spawned to read data from Azure Event Hub.
offset.async.commit	true	Offset commit mechanism used by the Kafka Consumer.
groupid	kafkabusgroupid	Parameter that is used to identify the consumer group to which a consumer belongs.
polltimeout	50 ms	Maximum amount of time a Kafka consumer will wait for new messages to arrive from a Azure Event Hub before returning the control to the calling application.
maxpollrecords	500	Maximum number of records a consumer can fetch in a single poll request.
maxpartitionfetchbytes	1048576 Bytes	Maximum number of bytes that a consumer can fetch from a single partition in a single request.
reconnectbackoffms	50 ms	Amount of time that a Kafka client should wait before attempting to reconnect to a broker after a connection failure.
retrybackoffms	100 ms	Amount of time a Kafka client should wait before retrying a failed operation.
requesttimeoutms	40,000 ms	Maximum amount of time Kafka client will wait for a response from the Azure Event Hub before considering the request as failed.
heartbeatintervalms	3000 ms	Interval at which Kafka consumer will send heartbeats to the broker to indicate that it is still alive and processing messages.
connectionsmaxidlems	540,000 ms	Specifies the maximum amount of time a connection can remain idle before it is closed by the broker.

2. Advanced Performance Tuning Parameters

Parameter	Default	Specify
consumerthreadcount	1	The number of Kafka consumer threads that will be spawned to read data from Azure Event Hub. This number of threads must be kept equal to number of partitions you have in Event Hub for optimal performance.
offset.async.commit	true	Offset commit mechanism used by the Kafka Consumer. The default is Asynchronous commit which gives a better performance. If changed to Synchronous commit by setting the parameter value as false, the performance will decrease.

For more performance scaling options for Azure Event Hub, refer to this [Microsoft documentation](#).

Additional Connector Configuration for Defender for Endpoint Data Source

Connector limits the character length of the rawEvent field

The Microsoft Azure Event Hub connector currently limits the character length of the rawEvent field to 4000 for Microsoft Defender for Endpoint Data Source. The rawEvent field was getting truncated in the following scenarios:

- If the value exceeds 4000 characters from the connector side.
- If the value exceeds 16384 characters from the Avro output side with Amazon S3 as destination.

Workaround:

To increase the size of the raw event field to hold a larger data size, implement the following procedure:

1. Search for the following properties in agent.default.properties file under the \$ARCSIGHT_HOME\current\config\agent folder:
 - size.validation.fields = field1, field2, field3...
 - size.validation.sizes = size1, size2, size3...

Change the size of the corresponding value of the `rawEvent` field to 1048576 in `size.validation.sizes`

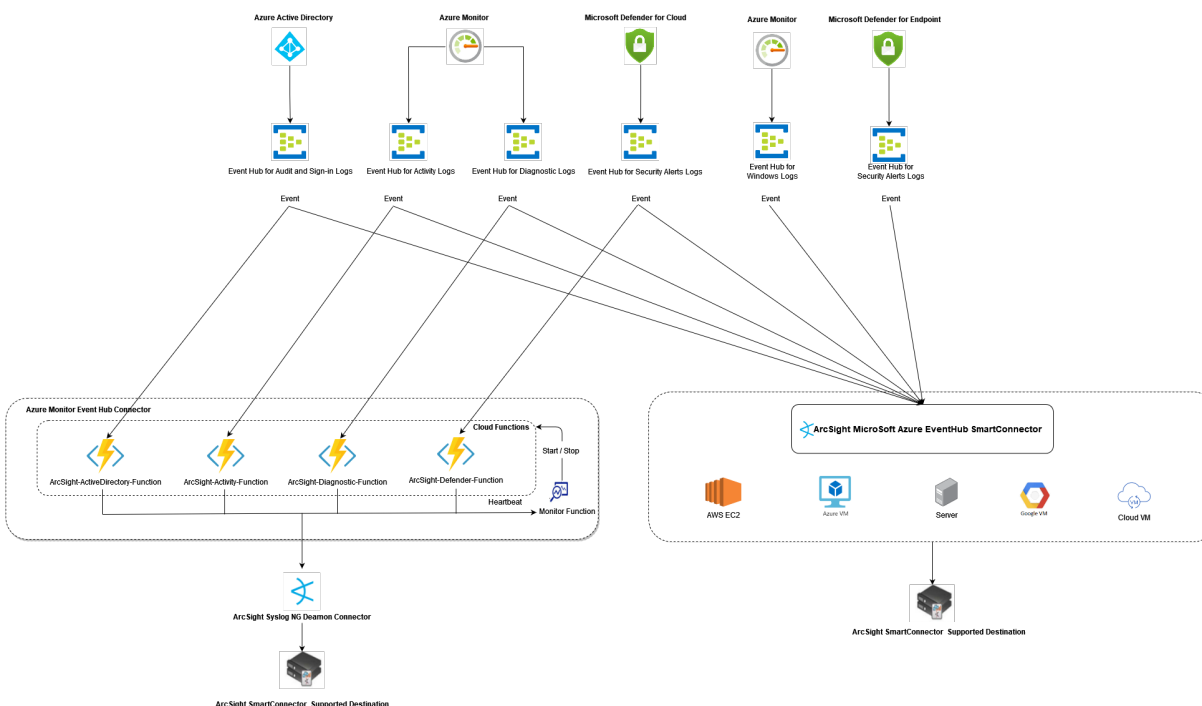
2. Browse the directory to find the `$ARCSIGHT_HOME\current\user\agent\avroschema\avro_schema_202111_1.2.0.avsc` file and update the `rawEvent maxLength` to 1048576.
3. Restart the connector.



Note: `$ARCSIGHT_HOME` in the file name is a placeholder and the value will depend on the standard reference for path.

Migrating the SmartConnector

The following diagram provides a high-level overview of the migration from the Azure Monitor Event Hub Connector to the Microsoft Azure Event Hub SmartConnector:



The following steps must be implemented for migrating from the Azure Monitor Event Hub Connector to Microsoft Azure Event Hub SmartConnector:


1. Stop the Azure Monitor Event Hub connector instance.
2. In the Azure portal, reuse the existing Resource group, Event Hub Namespace and Event hubs that were created for Azure AD logs, Activity logs, Resource logs and Defender for Cloud logs as part of the existing deployment. Delete all other resources that were created manually. Do not run the undeployment script as it will delete all the resources.
3. Windows AD logs and Defender for Endpoint logs are supported as part of the Microsoft Azure Event Hub SmartConnector.

Refer to this [section](#) for creating the Event Hubs. Also, see [here](#) for streaming the logs to the respective Event Hubs.

4. For creating Event Hubs and streaming logs refer to the following table for the Supported Logs:

Microsoft Azure Monitor Event Hub Connector	Microsoft Azure Event Hub Connector
Azure AD	Azure AD For more information, refer Product Overview .
Activity	Activity
Resource	Resource
Defender for Cloud	Defender for Cloud
	Windows AD For more information, refer Product Overview .
	Defender for Endpoint

- In the Azure portal, register an application and assign IAM role to the application with these [steps](#).
- Install the Microsoft Azure Event Hub SmartConnector and configure the Event Hubs based on the required Event Types as mentioned [here](#).

 **Note:** The destination must be the same that was selected initially while configuring the Syslog NG SmartConnector with the same parameters for reusing the destination.

- The Microsoft Azure Event Hub SmartConnector outputs the Avro files in S3 bucket and formats it in a similar way to the Microsoft Azure Monitor Event Hub Connector (This is done using a Syslog connector). When configuring the destination, select the same S3 bucket while collecting the data.
- Start the SmartConnector. It will start processing the events and send it to the configured ArcSight destination.

Prevention of Data Loss

The ArcSight Microsoft Azure Event Hub SmartConnector reads the data from latest offset from event hubs. After the connector starts, all the events that reach the Event hub will be received.

By the time the installation of the Microsoft Azure Event Hub SmartConnector completes, the Microsoft Azure Monitor Event Hub Connector stops. Henceforth, to avoid the data loss, the following steps must be implemented:

1. Stop the streaming of data to existing Event Hubs.
2. All the events must be read which means you must wait till the Syslog NG connector's EPS becomes zero.
3. Run the Undeployment Script and remove the Syslog NG SmartConnector. Only the Resource Group will remain after running the Undeployment script, which can be reused in the next step.
4. Create new Event Hubs and Event Hubs Namespace.
Configure the data sources to stream to the new Event Hubs.
5. Install and configure the ArcSight Microsoft Azure Event Hub SmartConnector to use new Event Hubs created in step 3 based on the Event Types.
While Installing, ensure to set the offset to **Earliest** and to read all the events that reach the Event Hubs.
6. Start the SmartConnector.

Hardware Consideration

The following table provides insights on resources consumed during the testing environment that was done on 8 core 16 GB RHEL box:

Event Size	EPS Processed	Tested Hardware	CPU Utilization	Memory Utilization (approx.)
1 K	10 K	8 core 16 GB	8%	500 MB
1 K	25 K	8 core 16 GB	34%	700 MB
2.2 K	5 K	8 core 16 GB	8%	600 MB
2.2 K	10 K	8 core 16 GB	25%	700 MB

The hardware resources consumed by the connector are based on the size of event and the number of EPS being processed by the connector.

When the event size is increased for the same EPS, both CPU and memory consumption increase. If the EPS is increased with a constant event size, both CPU and memory consumption increase. The resource consumption increases for higher event size and higher EPS.



Note: During production you must ensure that the connector is not consuming more than 75% of host resources.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the ArcSight Console User's Guide for more information about the ArcSight data fields.

Event Mappings for Active Directory

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Class ID	operationName
Device Product	Azure Active Directory
Device Vendor	Microsoft
Name	operationName
Severity	Level

Sign-in Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Application Protocol	properties/clientAppUsed
Destination Process Name	properties/appDisplayName
Destination User ID	properties/userId
Destination User Name	properties/userDisplayName
Device Custom Date 1	properties/createdDateTime
Device Custom Floating Point 1	properties/location/geoCoordinates/latitude
Device Custom Floating Point 2	properties/location/geoCoordinates/longitude
Device Custom String 1	properties/deviceDetail/operatingSystem
Device Custom String 2	properties/isRisky
Device Custom String 3	properties/location
Device Custom String 4	location
Device Custom String 5	correlationId

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	properties/userPrincipalName
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
External ID	properties/id
Reason	resultDescription
Request Client Application	properties/deviceDetail/browser
Source Address	callerIpAddress

Audit Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	properties/targetResources/userPrincipalName
Device Event Category	properties/category
Device Custom String 1	properties/identityType
Device Custom String 2	properties/operationType
Device Custom String 3	properties/targetResources/modifiedProperties(Role.DisplayName)/displayName (Role.DisplayName)
Device Custom String 5	correlationId
Device Custom String 6	properties/targetResources
Device Receipt Time	time
Event Outcome	resultType
External ID	properties/id
File Hash	properties/targetResources/modifiedProperties(Role.DisplayName)/newValue (Role.DisplayName)
File Name	properties/targetResources/modifiedProperties(Group.DisplayName)/newValue (Group.DisplayName)
File Path	properties/targetResourceName

ArcSight ESM Field	Device-Specific Field
File Type	properties/targetResourceType
Old File Hash	properties/targetResources/modifiedProperties(Role.DisplayName)/oldValue (Role.DisplayName)
Old File Name	properties/targetResources/modifiedProperties(Group.DisplayName)/oldValue (Group.DisplayName),
Reason	resultDescription
Source Address	callerIpAddress
Source User ID	properties/initiatedBy/user/id,
Source User Name	properties/initiatedBy/user/userPrincipalName

Event Mappings for Microsoft Defender for Cloud

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Name	AlertDisplayName
Device Event Class ID	AlertType
Severity	Severity

Security Alerts Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	AlertType
Destination Host Name	CompromisedEntity, Entities/HostName
Device Custom Date 1	ProcessingEndTime
Device Custom Number 1	Entities/\$id

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	ExtendedProperties
Device Custom String 2	IsIncident
Device Custom String 3	ResourceIdentifiers
Device Custom String 4	AlertUri
Device Custom String 5	Entities/Location/Asn & Entities/Location/CountryCode & Entities/Location/CountryName & Entities/Location/State & Entities/Location/City & Entities/Location/Longitude & Entities/Location/Latitude
Device Receipt Time	TimeGenerated
Device Severity	Severity
End Time	EndTimeUtc
Event Outcome	Status
External ID	SystemAlertId
File Path	AzureResourceId, Entities/AzureID, Entities/ResourceId
File Type	Entities/Type
Message	Description & RemediationSteps
Reason	Intent
Start Time	StartTimeUtc
Source Address	Entities/Address

Security Recommendations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	type
Device Action	assessmentEventDataEnrichment/action
Device Custom String 1	properties/metadata/policyDefinitionId
Device Custom String 2	properties/metadata/threats
Device Custom String 4	properties/links/azurePortal
Device Severity	properties/metadata/severity
File Name	file
File Path	ID
Message	properties/metadata/description & properties/metadata/remediationDescription
Name	properties/displayName
Event Outcome	properties/status/code
Reason	properties/status/cause

Event Mappings for Activity

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Name	operationName
Device Event Class ID	operationName
Severity	level

Action Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Port	properties/eventProperties/destinationPort
Destination Host Name	resourceId, properties/eventProperties/machineName
Destination User Name	identity/claims/name

ArcSight ESM Field	Device-Specific Field
Destination User Privileges	identity/authorization/evidence/role
Device Custom Date 1 Label	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/eventProperties, properties/policies
Device Custom String 3	properties/eventProperties/title
Device Custom String 4	location
Device Custom String 5	correlationId
Device Custom String 6	properties/isComplianceCheck
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
External ID	eventDataId
File Hash	properties/eventProperties/fileSha256
File Path	resourceId, properties/eventProperties/filePath
File Name	properties/eventProperties/fileName
File Type	resourceType, properties/eventProperties/type
Message	description
Old File Type	properties/eventProperties/resourceType
Reason	properties/eventProperties/cause
Request Client Application	properties/eventProperties/compromisedEntity
Source Address	callerIpAddress
Source Service Name	properties/eventProperties/attackedResourceType
Transport Protocol	properties/eventProperties/protocol

Administrative Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Action	identity/authorization/action
Device Custom Number 1	durationMs

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	resultSignature
Device Custom String 4	location
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
File Path	resourceId
Message	identity/claims
Request Client Application	identity/claims/iss
Request URL	identity/claims/aud
Source Address	callerIpAddress

Alert Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom Number 1	properties/Threshold
Device Custom Number 2	properties/WindowSizeInMinutes
Device Custom String 1	properties/RuleUri, subStatus
Device Custom String 2	properties/RuleName
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
Event Outcome	status
External ID	eventDataId
File Path	resourceId
File Type	resourceType
Message	description

Delete Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Privileges	identity/authorization/evidence/role
Destination User Name	identity/claims/name
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	correlationId
Device Custom String 4	location
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
File Type	resourceType
Event Outcome	resultType
External ID	eventDataId
Message	description
Source Address	callerIpAddress

Recommendation Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/recommendationCategory
Device Custom String 3	properties/recommendationImpact
Device Custom String 4	properties/recommendationRisk
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
Event Outcome	status
External ID	eventDataId

ArcSight ESM Field	Device-Specific Field
File Path	resourceId
File Type	resourceType
Message	description

Security Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Process ID	properties/processId
Destination Process Name	properties/processName
Destination NT Domain	properties/domainName
Destination User ID	properties/accountLogonId
Destination User Name	caller, properties/userName
Device Action	properties/ActionTaken
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/UserSID
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
External ID	eventDataId
Event Outcome	status
File Path	resourceId
File Type	resourceType
Message	description

Service Health Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Service Name	properties/impactedServices
Destination User Name	caller
Device Custom Date 1	submissionTimestamp

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	properties/trackingId
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
External ID	eventDataId
Event Outcome	status
File Path	resourceId
File Type	resourceType
Message	description
Start Time	properties/impactStartTime
Reason	properties/communication

Write Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 4	location
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	time
External ID	eventDataId,
Event Outcome	properties/statusCode
File Path	resourceId
File Type	resourceType
Source Address	callerIpAddress

Event Mappings for Resource Log

Common Event Mapping

Device Event Mapping	ArcSight Fields
Name	operationName
Device Event Class ID	operationName
Severity	Level

App Service HTTP Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Additional Data Event Primary Stamp Name	EventPrimaryStampName
Additional Data Event Stamp Name	EventStampName
Additional Data Event Stamp Type	EventStampType
Bytes In	Properties/csbytes
Bytes Out	Properties/scbytes
Destination Address	Properties/CIP
Destination Hostname	Properties/cshost
Destination User Name	Properties/csusername
Device Custom Floating Point 1	Properties/timetaken
Device Custom Floating Point 1 Label	Time Taken
Device Custom Number 2	Properties/scstatus
Device Custom Number 2 Label	Status code
Device Event Category	Category
Device Event Class ID	Category
Device Hostname	Properties/computername
Device Product	Azure
Device Receipt Time	Time
Device Vendor	Microsoft
Event Outcome	Properties/result
File Path	Resourceid

Name	Category
Request Client Application	Properties/useragent
Request Method	Properties/Csmethod
Source Hostname	Host
Source Port	Properties/sport
Application Protocol	Properties/protocol

App Service IP Sec Audit Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Ad.serviceendpoint	Service endpoint
Destination Address	CIP
Destination Hostname	CsHost
Device Event Category	Category
Device Event Class ID	Operation Name
Device Product	Azure
Device Receipt Time	Time
Device Vendor	Microsoft
Event Outcome	Result
File Path	ResourceId
Message	Details
Name	OperationName
Source Address	XForwardedFor
Source Hostname	XForwardedHost

Activity Runs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 2	Error
Device Custom String 5	correlationId
Device Receipt Time	time

ArcSight ESM Field	Device-Specific Field
External ID	activityRunId
File ID	pipelineRunId
File Path	resourceId
File Name	pipelineName
Destination Process Name	activityName
Start Time	start
End Time	end
Message	Output

Application Gateway Access Log Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
Device External ID	instanceId
Source Address	properties/clientIP
Source Port	properties/clientPort
Request URL	properties/requestUri
Request Client Application	properties/userAgent
Event Outcome	properties/httpStatus
Bytes In	properties/receivedBytes
Bytes Out	properties/sentBytes
Device Custom Floating Point 1	properties/timeTaken
Device Custom String 1	properties/sslEnabled

Archive Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
External ID	ActivityId
Device Custom String 1	trackingId

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	archiveStep
File Path	resourceId
File Name	eventHub
Start Time	startTime
Device Custom Number 1	failures
Device Custom Number 2	durationInSeconds
Message	message

Audit Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Event Outcome	resultType
Source Address	callerIpAddress
Destination User ID	identity
Device Custom String 1	properties/JobId
Device Custom String 2	properties/JobRunTime
Device Custom String 5	correlationId
Destination Process Name	properties/JobName
Start Time	properties/StartTime
End Time	properties/EndTime

Authoring Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Event Outcome	status
Device Receipt Time	time
Device Custom String 1	properties/Error

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	properties/correlationId
Message	properties/Message
Reason	properties/Type

Automatic Tuning Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
File Path	ResourceId

Azure Firewall Application Rule Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceid
Message	properties/smg

Azure Firewall Network Rule Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceid
Message	properties/smg

Azure Site Recovery Jobs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Event Outcome	properties/resultType
Message	properties/resultDescription
Start Time	properties/startTime
End Time	properties/endTime
Device Custom String 2	properties/affectedResourceType
Device Custom String 3	properties/affectedResourceId
Device Custom String 5	properties/correlationId

Blocks Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	duration_d
File Path	ResourceId
Destination User Name	resource_owner_type_s

C2D Command , C2D Twin Operations, and D2C Twin Operations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Database Wait Statistics Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	delta_wait_time_ms_d
Device Custom Number 2	delta_waiting_tasks_count_d
File Path	ResourceId

Deadlocks Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	duration_d
File Path	ResourceId
Destination User Name	resource_owner_type_s

Engine Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
File Path	resourceId
Device Event Category	category
Start Time	properties/StartTime
Device Custom String 1	properties/ObjectID
Device Custom String 2	properties/ObjectType
Device Custom String 3	properties/ObjectName
Device Custom String 4	properties/ObjectPath
Device Custom String 5	properties/ObjectReference
End Time	properties/EndTime
Event Outcome	properties/Success
Device Custom Number 1	properties/ConnectionID
Device Custom Number 2	properties/SPID
Source NT Domain	properties/NTDomainName

ArcSight ESM Field	Device-Specific Field
Source Host Name	properties/ClientHostName
Source Process ID	properties/ClientProcessID
Device Custom String 6	properties/ApplicationName
Destination User Name	properties/User
Destination Service Name	properties/ServerName

Errors Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
File Path	ResourceId
Message	Message
Event Outcome	state_d
Reason	error_number_d

Gateway Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
Device Custom Number 1	durationMs
Device Custom String 2	location
Source Address	callerIpAddress

ArcSight ESM Field	Device-Specific Field
Request URL Method	properties/method
Request URL	properties/url
Event Outcome	properties/responseCode

Job Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	TimeGenerated
File Name	RunbookName_s
Destination User Name	Caller_s
Device Custom String 1	resourceId
Device Custom String 2	resourceGroup
Device Custom String 3	Tenant_g
Device Custom String 5	correlationId
File ID	JobId_g
Event Outcome	ResultType
Device Event Category	category

Jobs Operations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Load Balancer Alert Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Device Custom String 1	systemId
File Path	resourceId
Reason	properties/eventDescription
Destination Address	properties/eventProperties/public ip address

Network Security Group Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Destination MAC Address	properties/macAddress
Destination Address	properties/primaryIPv4Address
Device Custom String 1	properties/subnetPrefix
Device Custom String 2	properties/ruleName
Device Custom String 3	properties/direction
Device Custom String 4	properties/priority
Device Custom String 5	properties/type
Message	properties/conditions
Transport Protocol	properties/conditions/protocols

Operational Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
File Path	resourceId

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	subscriptionId
Device Custom String 4	Region
Device Receipt Time	EventTimeString
Message	EventProperties
Event Outcome	Status
Source Process Name	Caller
External ID	ActivityId

P2S Diagnostic Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Message	properties/message
Device External ID	properties/instance

Postgre SQL Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Device Custom String 3	ResourceGroup
Device Custom String 2	SubscriptionId
Source Service Name	LogicalServerName
Message	properties/message

Query Store Wait Statistics Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 1	TenantId
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	total_query_wait_time_ms_d
File Path	ResourceId

Requests Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Event Outcome	resultType
Source Address	callerIpAddress
Destination Use ID	identity
Request Method	properties/HttpMethod
Request URL	properties/Path
Bytes In	properties/RequestContentLength
External ID	properties/ClientRequestId
Start Time	properties/StartTime
End Time	properties/EndTime

Routes Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Service Log Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Tenant
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
External ID	properties/id
File Type	properties/imageType

Timeouts Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Receipt Time	TimeGenerated
File Name	Resource

ArcSight ESM Field	Device-Specific Field
File Type	ResourceType
Azure Logical Server Name_s	LogicalServerName_s
Azure Elastic Pool Name_s	ElasticPoolName_s
CS 4 Label	DatabaseName_s
File Path	ResourceId

Trigger Runs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 2	triggerEvent
Device Custom String 5	correlationId
Device Receipt Time	time
External ID	activityRunId
File Path	resourceId
File Name	pipelineName
Destination Process Name	activityName
Start Time	start
End Time	end
File ID	triggerId
File Type	triggerType

Twin Queries Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Device Custom Number 1	durationMs
Device Custom String 1	properties
Device Custom String 2	location

ArcSight ESM Field	Device-Specific Field
Event Outcome	resultType
File Path	resourceId
Message	resultDescription

Workflow Runtime Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Reason	code
Event Outcome	properties/status
Start Time	properties/startTime
End Time	properties/endTime
Device Custom String 1	properties/resource/subscriptionIdEndpoint
Device Custom String 2	properties/resource/resourceGroupName
Device Custom String 4	properties/resource/location
Device Action	properties/resource/actionName
File Name	properties/resource/workflowName

Event Mappings for Windows AD

Event 4624

OpenText ArcSight ESM Field	Device-Specific Field
Additional data	TargetOutboundUserName
Additional data	TargetOutboundDomainName
Destination NT Domain	TargetDomainName
Destination Process Name	ProcessName
Destination User ID	TargetLogonId
Destination User Name	TargetUserName

OpenText ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom Number 1	LogonType
Device Custom String 1	ImpersonationLevel
Device Custom String 3	ProcessId
Device Custom String 4	RestrictedAdminMode
Device Custom String 5	AuthenticationPackageName
Device Custom String 6	LogonGuid
Device NT Domain	SubjectDomainName
Device Process Name	LogonProcessName
File ID	TargetLinkedLogonId
File Name	ElevatedToken
File Type	VirtualAccount
Message	'This event is generated when a logon session is created. It is generated on the computer that was accessed.'
Name	'An account was successfully logged on.'
Source Address	IpAddress
Source Host Name	One of (IpAddress, 'localhost')
Source Port	IpPort
Source User ID	SubjectLogonId

Event 4625

OpenText ArcSight ESM Field	Device-Specific Field
Destination NT Domain	TargetDomainName
Destination Process Name	ProcessName
Destination User ID	' '
Destination UserName	TargetUserName
Device Custom Number 1	LogonType
Device Custom String 1	SubStatus
Device Custom String 3	ProcessId
Device Custom String 4	FailureReason
Device Custom String 5	AuthenticationPackageName

OpenText ArcSight ESM Field	Device-Specific Field
Device NT Domain	SubjectDomainName
Device Process Name	LogonProcessName
Message	<p>'This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request.</p> <ul style="list-style-type: none"> - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.'
Name	'An account failed to log on.'
Reason	FailureReason
Source Address	IpAddress
Source Host Name	WorkstationName
Source Port	IpPort
Source Process Name	ProcessId

Event 4648

OpenText ArcSight ESM Field	Device-Specific Field
Destination NT Domain	TargetDomainName
Destination Process Name	ProcessName
Destination User ID	SubjectLogonId
Destination User Name	TargetUserName
Device Custom String 3	ProcessId (Process ID)
Device Custom String 5	TargetServerName
Device Custom String 6	TargetLogonGuid (Logon GUID)

OpenText ArcSight ESM Field	Device-Specific Field
Device NT Domain	SubjectDomainName
Message	'This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.'
Name	'A logon was attempted using explicit credentials.'
Source Address	IpAddress
Source Port	IpPort
Source User Name	One of (SubjectUserName, SubjectUserSid)

Event 4656

OpenText ArcSight ESM Field	Device-Specific Field
Name	'A handle to an object was requested.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom String 3	ProcessId
Device Custom String 1	AccessList
Device NT Domain	SubjectDomainName
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Privileges	PrivilegeList
File ID	HandleId
File Name	ObjectName
File Type	ObjectType

Event 4663

OpenText ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to access an object.'
Device Custom String 1	AccessList
Device Custom String 3	ProcessId

OpenText ArcSight ESM Field	Device-Specific Field
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File ID	HandleId
File Name	ObjectName
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Name	One of (SubjectUserName, SubjectUserSid)

Event 4664

OpenText ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to create a hard link.'
Destination User ID	SubjectLogonId
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event 4674

OpenText ArcSight ESM Field	Device-Specific Field
Name	'An operation was attempted on a privileged object.'
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList
Device Custom String 3	ProcessId
File ID	HandleId

Event 4688

OpenText ArcSight ESM Field	Device-Specific Field
Name	'A new process has been created.'
Destination User Name	One of (SubjectUserName, SubjectUserSid, TargetUserName, TargetUserSid)
Destination NT Domain	One of (SubjectDomainName, destinationNtDomain)
Destination User ID	One of (SubjectLogonId, TargetLogonId)
Device Custom String 1	MandatoryLabel
Device Custom String 3	NewProcessId
Device Custom String 6	TokenElevationType
Device Custom String 5	ProcessId
Device Custom String 4	CommandLine
Destination Process Name	NewProcessName
Device NT Domain	SubjectDomainName
File Path	ParentProcessName
Message	'Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. Type 2 is an elevated token with no privileges removed or groups disabled. Type 3 is a limited token with administrative privileges removed and administrative groups disabled.'

Event 4768

OpenText ArcSight ESM Field	Device-Specific Field
Destination Nt Domain	TargetDomainName
Destination Service Name	ServiceName
Destination User Name	TargetUserName
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device custom String 3	IpAddress, SourceAddress
Device Custom String 4	Status
Device Custom String 5	PreAuthType

OpenText ArcSight ESM Field	Device-Specific Field
Message	Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.
Name	A Kerberos authentication ticket (TGT) was requested.
Source Address	IpAddress
Source Port	IpPort

Event 4769

OpenText ArcSight ESM Field	Device-Specific Field
Destination Nt Domain	TargetDomainName
Destination Service Name	ServiceName
Destination User Name	TargetUserName
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device custom String 1	TicketOptions
Device custom String 1 Label	Ticket Options
Device custom String 3	IpAddress
Device Custom String 4	Status
Device Custom String 5	TicketEncryptionType
Device Custom String 6	LogonGuid
File Name	ServiceSid
Message	This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.
Name	A Kerberos service ticket was requested.
Source Address	IpAddress
Source Port	IpPort

Event 4770

OpenText ArcSight ESM Field	Device-Specific Field
Destination Nt Domain	TargetDomainName
Destination Service Name	ServiceName
Destination User Name	TargetUserName
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device custom String 3	IpAddress
Message	Ticket options and encryption types are defined in RFC 4120.
Name	A Kerberos service ticket was renewed.
Source Address	IpAddress
Source Port	IpPort

Event 4771

OpenText ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device custom String 3	IpAddress
Source Address	IpAddress

Event 4772

OpenText ArcSight ESM Field	Device-Specific Field
Destination Service Name	ServiceName
Device custom String 3	IpAddress
Device Custom String 4	FailureCode
Message	Ticket options and failure codes are defined in RFC 4120.
Name	A Kerberos authentication ticket request failed.
Source Address	IpAddress
Source Port	IpPort

Event 4773

OpenText ArcSight ESM Field	Device-Specific Field
Destination Service Name	ServiceName
Device custom String 3	IpAddress
Device Custom String 4	FailureCode
Message	Ticket options and failure codes are defined in RFC 4120.
Name	A Kerberos service ticket request failed.
Source Address	IpAddress
Source Port	IpPort

Event 4776

OpenText ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Device Custom String 4	Status
Device Custom String 5	PackageName
Name	The domain controller attempted to validate the credentials for an account.
Reason	Status
Source Host Name	Workstation

Event 4777

OpenText ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Device Custom String 4	Status
Device Custom String 5	ClientUserName
Name	The domain controller failed to validate the credentials for an account.
Source Host Name	Workstation

Event 5137

OpenText ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom String 5	ObjectClass
Device Custom String 6	ObjectDN
Device NT Domain	SubjectDomainName
Name	'A directory service object was created.'

Event 5139

OpenText ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom String 5	ObjectClass
Device Custom String 6	NewObjectDN
Device NT Domain	SubjectDomainName
Name	'A directory service object was moved.'

Event 5140

OpenText ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom String 1	AccessList
Device Custom String 6	ShareName

OpenText ArcSight ESM Field	Device-Specific Field
Device NT Domain	SubjectDomainName
File Path	ShareName
File Type	ObjectType
Name	'A network share object was accessed.'
Source Address	IpAddress
Source Port	IpPort

Event 5141

OpenText ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom String 5	ObjectClass
Device Custom String 6	ObjectDN
Device NT Domain	SubjectDomainName
Name	'A directory service object was deleted.'

Event 5145

OpenText ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom String 1	AccessList
Device Custom String 6	ShareName
Device NT Domain	SubjectDomainName
File Name	RelativeTargetName
File Path	ShareLocalPath

OpenText ArcSight ESM Field	Device-Specific Field
Name	'A network share object was checked to see whether client can be granted desired access.'
Source Address	IpAddress
Source NT Domain	SubjectDomainName
Source Port	IpPort
Source User ID	SubjectLogonId

Event 6272

OpenText ArcSight ESM Field	Device-Specific Field
Destination Address	NASIPv4Address
Destination NT Domain	SubjectDomainName
Destination Port	NASPort
Destination User ID	FullyQualifiedSubjectUserName
Destination User Name	SubjectUserName
Destination User Privileges	QuarantineState
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIpAddress
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier
Name	'Network Policy Server granted access to a user.'
Source Address	CallingStationID
Source User ID	FullyQualifiedSubjectMachineName
Source User Name	SubjectMachineName

Event 6273

OpenText ArcSight ESM Field	Device-Specific Field
Destination Address	NASIPv4Address
Destination NT Domain	SubjectDomainName
Destination Port	NASPort

OpenText ArcSight ESM Field	Device-Specific Field
Destination User ID	FullyQualifiedSubjectUserName
Destination User Name	SubjectUserName
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIPAddress
Device Custom String 4	Reason
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier
Name	'Network Policy Server denied access to a user. Contact the Network Policy Server administrator for more information.'
Source Address	CallingStationID
Source User ID	FullyQualifiedSubjectMachineName
Source User Name	SubjectMachineName

Event 6274

OpenText ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server discarded the request for a user. . Contact the Network Policy Server administrator for more information.'

Event 6275

OpenText ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server discarded the accounting request for a user. . Contact the Network Policy Server administrator for more information.'

Event 6276

OpenText ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server quarantined a user. . Contact the Network Policy Server administrator for more information.'

Event 6277

OpenText ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy . Contact the Network Policy Server administrator for more information.'

Event 6278

OpenText ArcSight ESM Field	Device-Specific Field
Destination Address	NASIPv4Address
Destination NT Domain	SubjectDomainName
Destination Port	NASPort
Destination User ID	FullyQualifiedSubjectUserName
Destination User Name	SubjectUserName
Destination User Privileges	QuarantineState
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIPAddress
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier
Name	'Network Policy Server granted full access to a user because the host met the defined health policy.'
Source Address	CallingStationID
Source User ID	FullyQualifiedSubjectMachineName
Source User Name	SubjectMachineName

For information regarding the Common Event Mappings, refer to the [Windows Common Security Mappings](#) section of the *SmartConnector for Microsoft Windows Event Log - Native Configuration Guide*.

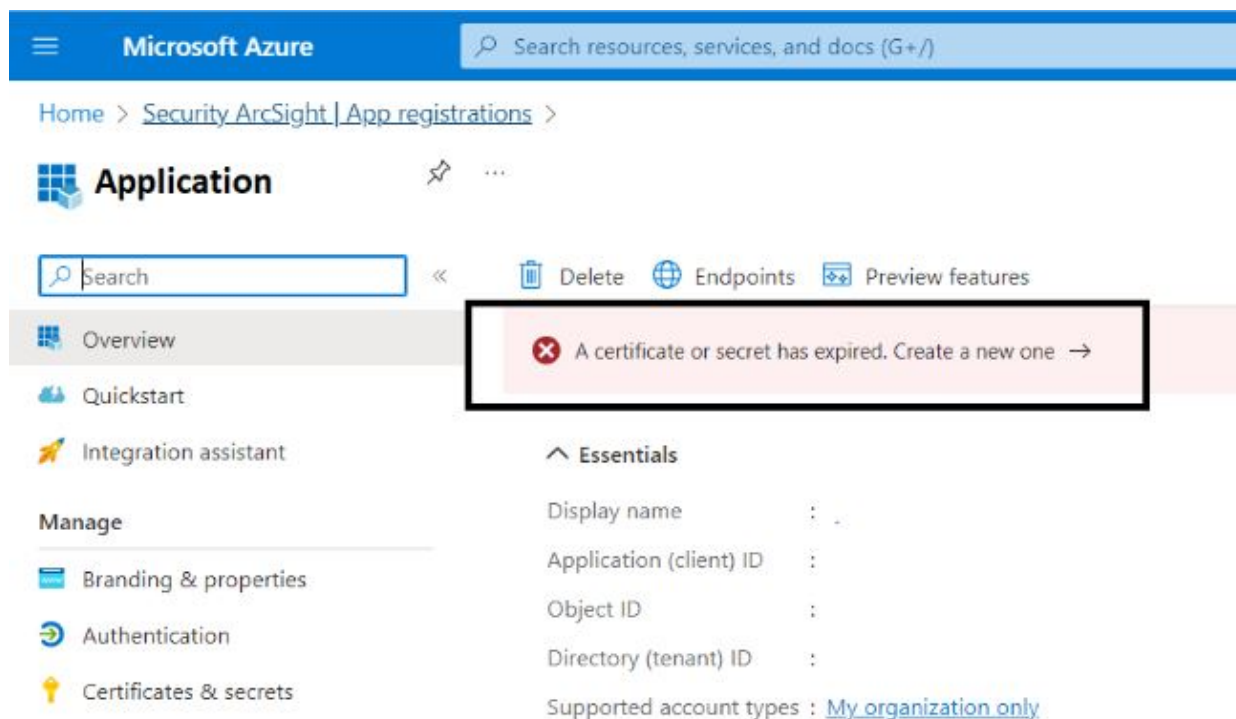
Event Mappings for Defender for Endpoint

ArcSight ESM Field	Device-Specific Value
Device Vendor	Microsoft
Device Product	Microsoft Defender for Endpoint
Raw Event	rawevent

Troubleshooting

Reconfiguring the expired Client Secret or Client Certificate

The following warning will be displayed in the Azure Portal after the expiry of the **Client Secret** or **Client Certificate**:



1. Create a new **Client Secret** or **Client Certificate** with the steps mentioned [here](#).
2. Stop the connector.

3. Start the connector setup again to reconfigure the new **Client Secret** or **Client Certificate**.
4. Restart the connector.

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 Azure Event Hub SmartConnector
(SmartConnector CE 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!