

P R O C E S S M A N U A L

Document Code: PM-MSI

Microsoft Sentinel Integration

Send Auditlog data from your User Portal to your Microsoft Sentinel setup.

 **FastTrack** Software

 **Admin** By Request

Table of Contents

Introduction	3
Assumptions	3
Prerequisites	3
Breakdown of Tasks.....	4
Integration Tasks	5
Task A: Set up Log Analytics Workspace	5
Task B: Create new Azure Logic App.....	7
Task C: Paste in JSON Code	9
Task D: Enter Parameters.....	10
Task E: Understand the App Flow	12
Task F: Configure Loop Entries	16
Task G: Test the Integration	19

Introduction

Microsoft Sentinel offers various ways to consume data from different sources. As Admin By Request provides a public REST API for pulling Auditlog data (see the documentation [here](#)), it's an easy task to leverage the power of Azure Logic Apps to consume the Auditlog API and forward each new entry to an Azure Log Analytics Workspace for further Sentinel consumption.

We've created an Azure Logic App that requires very few changes before having you up and running with Admin By Request Auditlog data in your Microsoft Sentinel setup. This manual provides a step-by-step guide on how to configure the integration.

Assumptions

The tasks described in this manual assume that the user has access to their Azure Portal, Admin By Request User Portal, and some familiarity with both environments.

Prerequisites

To enable this integration, you must first obtain your Admin By Request API Key. This key can be self-generated through your Admin By Request User Portal via **Settings > [OS] Settings > Data > API**:

The screenshot shows the Admin By Request user portal interface. At the top, there is a navigation bar with the following items: Summary, Auditlog, Requests, Reports, Inventory, Settings (highlighted with a red arrow), Download, Logins, Docs, and Contact. Below the navigation bar, the main content area is titled 'Windows Workstation Global Settings'. Underneath, there are tabs for PRIVACY, RETENTION, WEBHOOKS, and API (highlighted with a red arrow). The 'API Access' section is active, showing a toggle for 'API access' set to 'ON' (circled in red) and a 'Regenerate' button. Below this is the 'API Key' field, which is blurred. A red arrow points to the 'Save' button. To the right, there is an 'About API Access' section with explanatory text. On the left side of the page, there is a sidebar menu with items: Authorization, Endpoint, Lockdown, Malware, Applications, Data (highlighted with a red arrow), and Emails.

IMPORTANT: Click the **Save** button after Regenerating an API Key, to ensure this is the key used to establish the connection to Azure. A green tick icon will appear next to the **Save** button when the action is complete:



NOTE: The API Key has been blurred out in the above example.

Breakdown of Tasks

Seven tasks are covered in this manual:

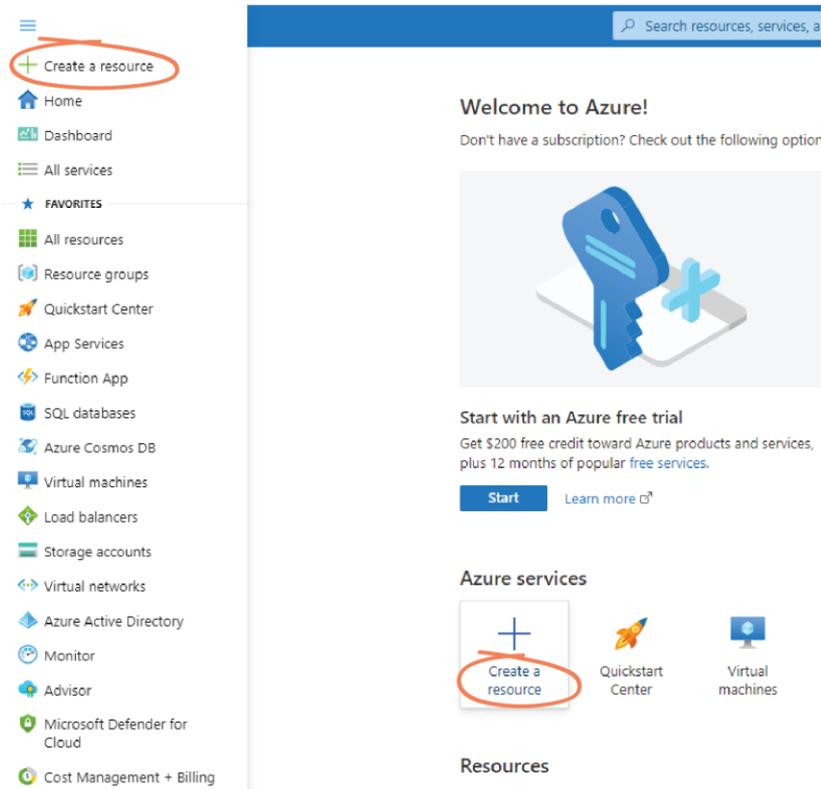
1. Task A: Set up Log Analytics Workspace
2. Task B: Create new Azure Logic App
3. Task C: Paste in JSON Code
4. Task D: Enter Parameters
5. Task E: Understand the App Flow
6. Task F: Configure Loop Entries
7. Task G: Test the Integration

Integration Tasks

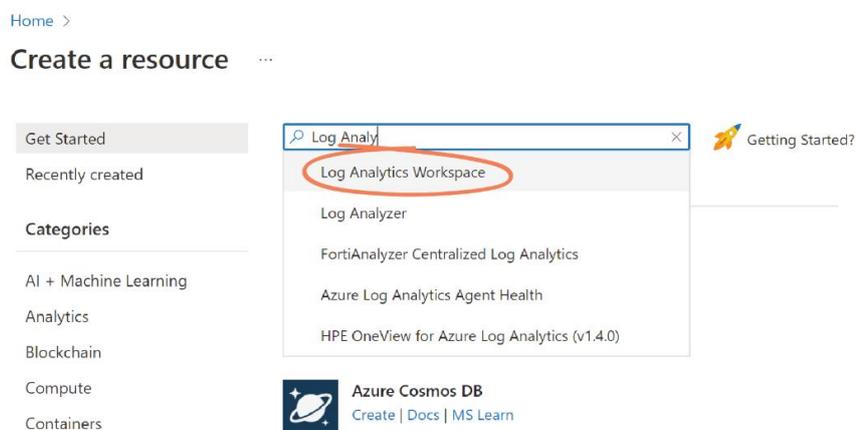
Task A: Set up Log Analytics Workspace

A Log Analytics Workspace is the management unit which allows you to store, query, and retain data pulled in from other tools – in this case, Auditlog data pulled from your Admin By Request User Portal. Task A involves setting up this storage unit for use in subsequent tasks.

1. Log in to your Microsoft Azure Portal, and select **Create a resource** from the Home page or the side menu:



2. Use the search box to search for and select **Log Analytics Workspace** from the drop-down menu:



3. Select **Create**:4. Fill out the Project details, and in the *Instance Details* section, give the Workspace a *Name* and select the appropriate *Region* from the drop-down menu:

Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Azure subscription 1

Resource group * ⓘ (New) Sentinel-Test
[Create new](#)

Instance details

Name * ⓘ SentinelLogs ✓

Region * ⓘ Australia Southeast

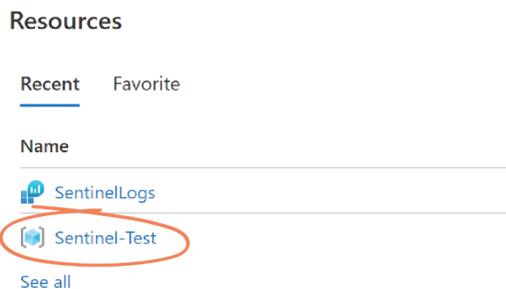
 **NOTE:** In the above screenshot, we have created a new Resource group called *Sentinel-Test* for the purpose of this demonstration.

5. Select the **Review + Create** button at the bottom of the page:6. When validation has passed, select **Create**, and wait for deployment to complete:

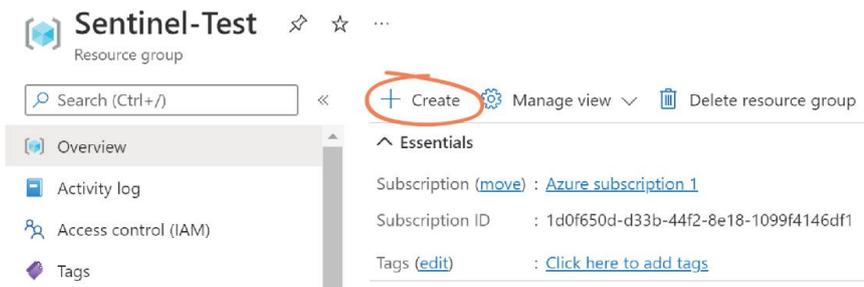
Task B: Create new Azure Logic App

An Azure Logic App is needed to consume the Admin By Request Auditlog API and forward each new entry to the Azure Log Analytics Workspace created in Task A.

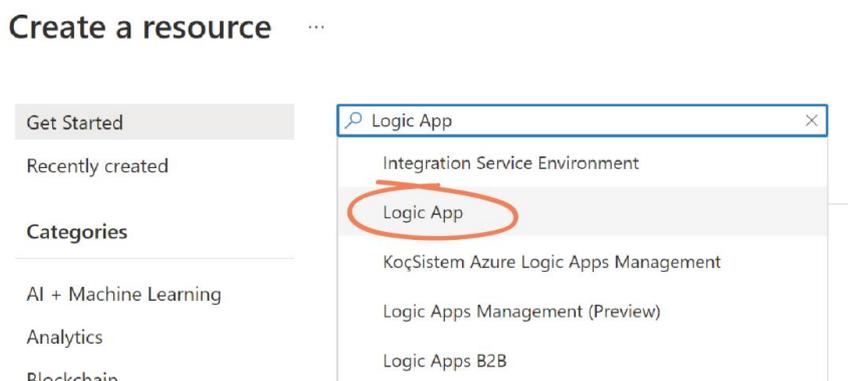
1. Navigate to *Resource groups* and select the Resource Group used in Task A from the *Recent* list under *Resources* – in this example, **Sentinel-Test**:



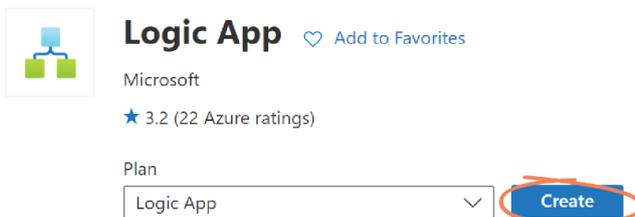
2. Once in Sentinel-Test, select the **Create** button:



3. Use the Search bar to locate and select **Logic App** from the drop-down menu:



4. Click **Create**:



5. In the *Plan* section, select your *Plan type*. In this example, we use **Consumption**:

Plan

The plan type you choose dictates how your app scales, what features are enabled, and how it is priced. [Learn more](#)

Plan type *

Standard: Best for enterprise-level, serverless applications, with event-based scaling and networking isolation.

Consumption: Best for entry-level. Pay only as much as your workflow runs.

[Looking for the classic consumption create experience? Click here](#)

6. In the *Instance Details* section, enter a *Logic App name* (in this case, **Sentinel-Logic-App**) and select the appropriate *Region*:

Instance Details

Logic App name *

Sentinel-Logic-App ✓

Region *

Australia Southeast ✓

Enable log analytics *

Yes No

7. Select the **Review + Create** button, followed by **Create**.

8. Once deployment is complete, click **Go to resource**:



Your deployment is complete



Deployment name: Microsoft.Web-LogicAppConsumption-Portal-2...

Subscription: [Azure subscription 1](#)

Resource group: [Sentinel-Test](#)

∨ **Deployment details** ([Download](#))

∧ **Next steps**

[Setup log analytics for your app.](#) Recommended

Go to resource

Task C: Paste in JSON Code

To get the app behaving how we need it to for this integration, you need to replace the default code in the Logic app code view with the JSON code we have written – download it [here](#).

1. In the *Logic Apps Designer* page, select the app you created in Task B from the top menu (in this case, **Sentinel-Logic-App**):

Home > Microsoft.Web-LogicAppConsumption-Portal-2207b2d0-b993 > **Sentinel-Logic-App** >
Logic Apps Designer ...

2. From the left-hand menu, under *Development Tools*, select **Logic app code view**:

Development Tools

 Logic app designer

 **Logic app code view**

 Versions

 API connections

 Quick start guides

3. Open the Admin By Request JSON file (found [here](#)) and select and copy all code. Navigate back to the *Logic app code view* in Azure, and replace the existing code with the code copied from the JSON file:

Save X Discard Run Trigger Designer </> Code view Parameters

```

511     },
512     "contentVersion": "1.0.0.0",
513     "outputs": {},
514     "parameters": {
515       "apiKey": {
516         "defaultValue": "xxxxxx",
517         "type": "String"
518       },
519       "LogName": {
520         "defaultValue": "AdminByRequestLogs",
521         "type": "String"
522       }
523     },
524     "triggers": {
525       "Recurrence": {
526         "evaluatedRecurrence": {
527           "frequency": "Day",
528           "interval": 1,
529           "startTime": "2022-06-22T15:00:00Z"
530         },
531         "recurrence": {
532           "frequency": "Day",
533           "interval": 1,
534           "startTime": "2022-06-22T15:00:00Z"
535         },
536         "type": "Recurrence"
537       }
538     },
539     "parameters": {}
540   },
541 }

```

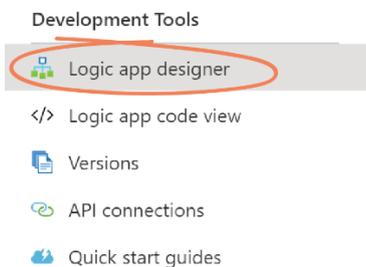
4. Click **Save**:

 **Save** X Discard

Task D: Enter Parameters

The Admin By Request API Key (found in the [Prerequisite](#) section of this document) is used to establish a connection between the Azure Logic App and your Admin By Request User Portal.

- From the left-hand menu, under *Development Tools*, select **Logic app designer**:



- From the top menu, select **Parameters**:



- The two parameters required for the integration are:

- Apikey - String*: The API Key obtained from your Admin By Request User Portal (see [Prerequisite](#)).
- LogName - String*: The name you would like for the custom log in your Log Analytics Workspace.

In the *Default Value* field for each of these parameters, replace the placeholder text with the appropriate / desired value:

×
🗑️

Name *	<input type="text" value="ApiKey"/>
Type *	<input type="text" value="String"/>
Default Value	<input type="text" value="Placeholder text"/>
Actual Value	<input type="text"/>

×
🗑️

Name *	<input type="text" value="LogName"/>
Type *	<input type="text" value="String"/>
Default Value	<input type="text" value="AdminByRequestLogs"/>
Actual Value	<input type="text"/>

NOTE: In the above screenshot, the API Key is blurred out, and we have used *AdminByRequestLogs* as the *LogName*.

4. Select the **Save** button in the Logic app designer:

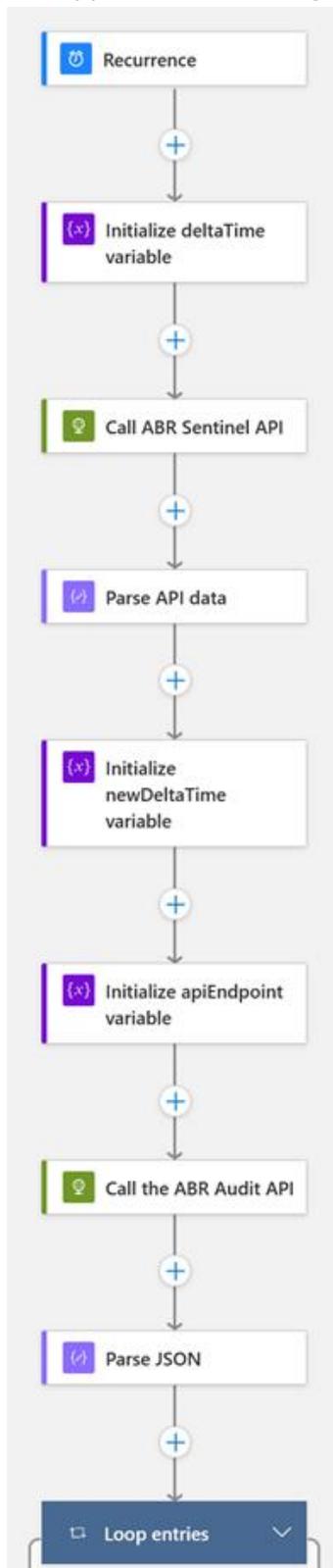


5. Close the Parameter window by selecting the **X** in the top right-hand corner.

Task E: Understand the App Flow

In this Task, we take a look at what's going on 'behind the scenes' – at API calls, variables, and loops involved in the preconfigured app flow.

The app flow has nine segments arranged as follows:



- **Recurrence** – This tells the app when it should run. In our example we've set up a recurring trigger that runs once every day. You can replace this trigger with whatever works best for your setup.

The screenshot shows the 'Recurrence' configuration panel. It includes a title bar with a refresh icon and a three-dot menu. Below are three main sections:

- * Interval**: A text input field containing the number '1'.
- * Frequency**: A dropdown menu currently set to 'Day'.
- Start time**: A text input field containing the ISO 8601 timestamp '2022-06-22T15:00:00Z'.

 At the bottom, there is a text input field labeled 'Add new parameter' with a dropdown arrow.

- **Initialize deltaTime variable** – In order to call the Admin By Request Audit API, we need a variable containing the 'from' ticks. Basically, telling the Audit API to 'give me all audit logs since this time'. This is defaulted to the number of ticks representing DateTime.Now.

The screenshot shows the 'Initialize deltaTime variable' configuration panel. It includes a title bar with a refresh icon and a three-dot menu. Below are three main sections:

- * Name**: A text input field containing 'deltaTime'.
- * Type**: A dropdown menu currently set to 'Integer'.
- Value**: A text input field containing a function call 'ticks(...)' with a small 'x' icon to its right.

 At the bottom, there is a text input field labeled 'Add new parameter' with a dropdown arrow.

- **Call ABR Sentinel API** – Since Logic Apps don't hold any state, we need some way of storing the last time the Audit API was called for a given API-key. We've created an API endpoint that allows you to do just this. We simply call the SetDeltaTime endpoint with your API Key and the deltaTime variable, and the API returns that value for when the Audit endpoint was last called – and it stores the new value, so that the next time the Logic App runs, it has the correct tick-values to ensure that you don't get any duplicate entries.

The screenshot shows the 'Call ABR Sentinel API' configuration panel. It includes a title bar with a globe icon and a three-dot menu. Below are several sections:

- * Method**: A dropdown menu set to 'POST'.
- * URI**: A text input field containing the URL 'https://sentinel.adminbyrequest.com/Audit/SetDeltaTime'.
- Headers**: A table with two columns: 'Enter key' and 'Enter value'.
- Queries**: A table with two columns: 'Enter key' and 'Enter value'.
- Body**: A text input field containing a JSON object:


```
{
  "ApiKey": "@ ApiKey x",
  "Ticks": "{x} deltaTime x"
}
```
- Cookie**: A text input field labeled 'Enter HTTP cookie'.

 At the bottom, there is a text input field labeled 'Add new parameter' with a dropdown arrow.

- Parse API Data** – The result from the API needs to be parsed in order to use the resulting variables.

>>  Parse API data ...

Parameters Settings Code View Run After ...

*Content

*Schema

```

{
  "properties": {
    "apiEndpoint": {
      "type": "string"
    },
    "success": {
      "type": "boolean"
    },
    "ticks": {
      "type": "integer"
    }
  }
}

```

[Use sample payload to generate schema](#)

- Initialize newDeltaTime and apiEndpoint variable** – With the values from the SetDeltaTime endpoint, we need to store two variables: newDeltaTime and apiEndpoint. These variables hold the tick-value for when the Audit API was last called, as well as the Admin By Request endpoint to call for Audit logs.

>>  Initialize newDeltaTime variable ...

Parameters Settings Code View Run After ...

*Name

*Type

Value

>>  Initialize apiEndpoint variable ...

Parameters Settings Code View Run After ...

*Name

*Type

Value

- **Call the ABR Audit API** – Now it's a matter of calling the Admin By Request Audit endpoint with your API Key, as well as the newDeltaTime variable.

>>  Call the ABR Audit API ...

Parameters Settings Code View Run After ...

* Method

* URI

Headers

apikey	 ApiKey x	✕ 📄
Enter key	Enter value	

Queries

Enter key	Enter value	📄
-----------	-------------	----------------

Body

Cookie

- **Parse JSON** – The next step parses the response from the Audit API as JSON using a schema based on the response type from the Audit API (view the [Auditlog API documentation](#) for more information on this).

 Parse JSON (i) ...

* Content

* Schema

```

{
  "properties": {
    "entries": {
      "items": {
        "properties": {
          "application": {
            "properties": {
              "file": {
                "type": [
                  "string"
                ]
              }
            }
          }
        }
      }
    }
  }
}

```

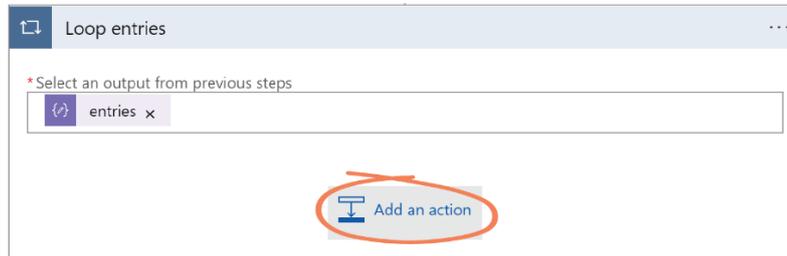
[Use sample payload to generate schema](#)

- **Loop entries** – The final step in the app flow simply loops through every entry from the Audit call. Here you decide what to do with the data. (See Task F, below.)

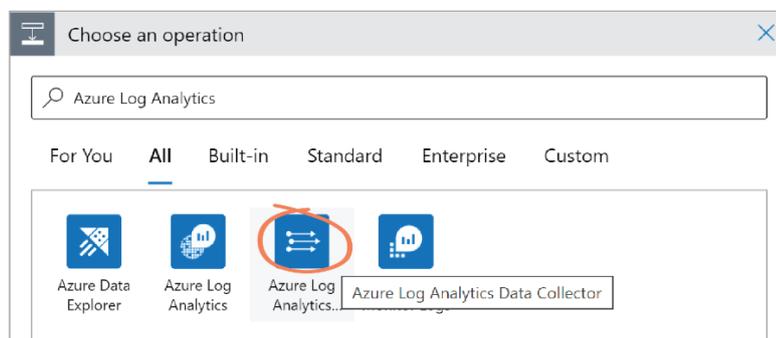
Task F: Configure Loop Entries

In order to send data to your Azure Log Analytics Workspace, you must add an action for each entry in the dataset.

1. Select the *Loop entries* segment of the app flow and click the **Add an Action** button:

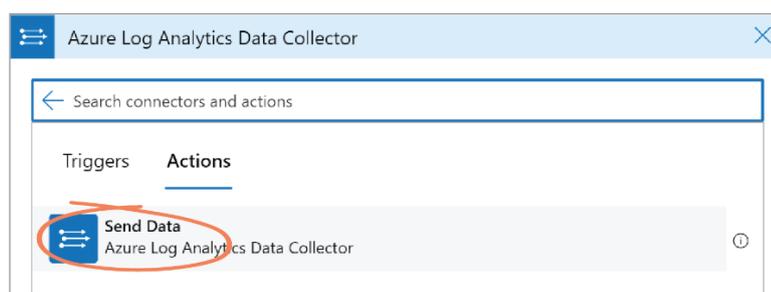


2. In the *Choose an operation* section, use the search box to locate and select **Azure Log Analytics Data Collector**:



IMPORTANT: Be sure to select **Azure Log Analytics Data Collector**, rather than *Azure Log Analytics* (to the left in the screenshot above).

3. Select **Send Data** under the *Actions* tab:



IMPORTANT: After clicking Send Data, you may be prompted to create a connection. If so, follow the steps below (steps 4-7). Otherwise, skip to step 8.

- If prompted to create a connection, in the *Connection name* field, choose your desired name – in this case, we've used *AzureLogConnector*:

Azure Log Analytics Data Collector

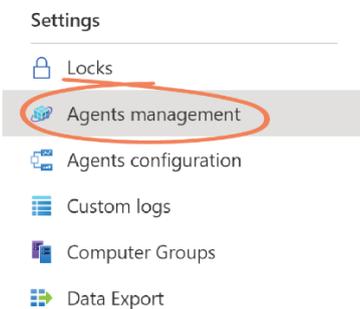
* Connection name: AzureLogConnector

* Workspace ID ⓘ: The unique identifier of the Azure Log Analytics workspace.

* Workspace Key ⓘ: The primary or secondary key of the Azure Log Analytics workspace.

Create

- To locate the *Workspace ID* and *Workspace Key*, open your Log Analytics Workspace (i.e., *SentinelLog*) in a new tab and select **Agents Management** under *Settings* from the left-hand menu:



- Copy the *Workspace ID* and *Primary key* values from this page:

Workspace ID ←

Primary key ←

Regenerate

- Navigate back to the Logic App, paste the keys into their corresponding fields in the *Azure Log Analytics Data Collector* window, and select **Create**:

Azure Log Analytics Data Collector

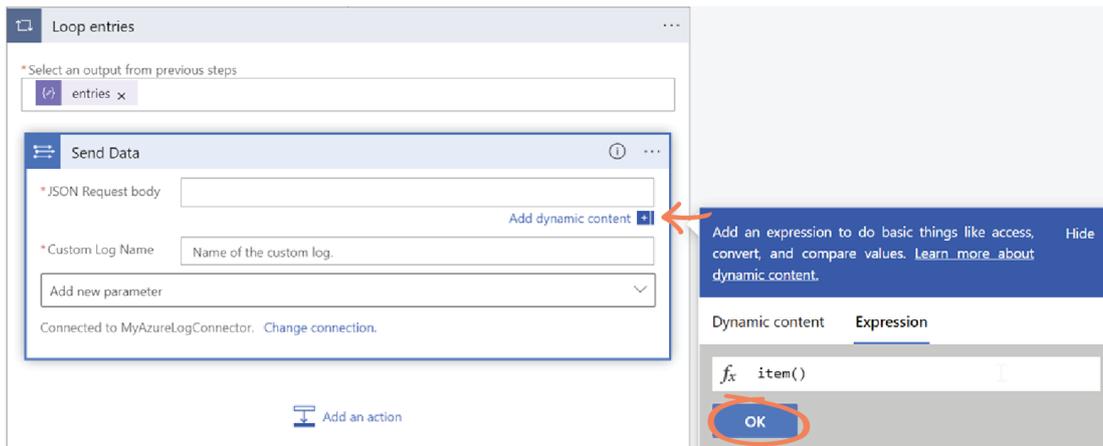
* Connection name: AzureLogConnector

* Workspace ID ⓘ: [Copied Workspace ID]

* Workspace Key ⓘ: [Copied Primary Key]

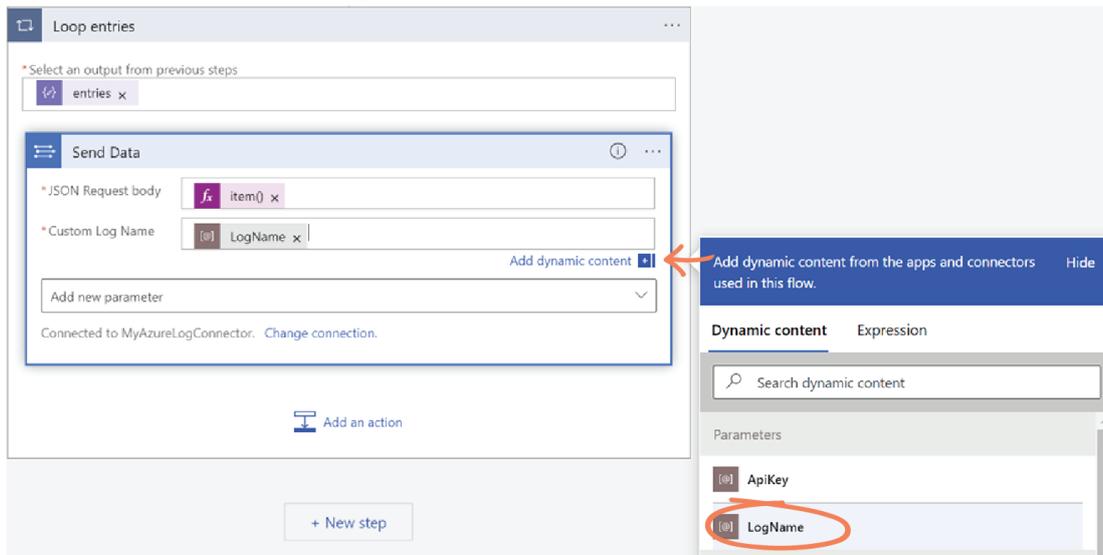
Create

- In the *JSON Request body* field, select **Add dynamic content**, and in the *Expression* tab, enter *item()* and click **OK**:



NOTE: This selects the current item in the JSON loop and adds it as the request body.

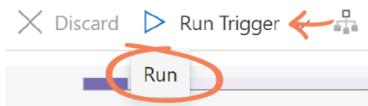
- In the *Custom Log Name* field, select **Add dynamic content**, and in the *Dynamic content* tab, locate and select the **LogName** parameter:



- Select the **Save** button to save your app.

Task G: Test the Integration

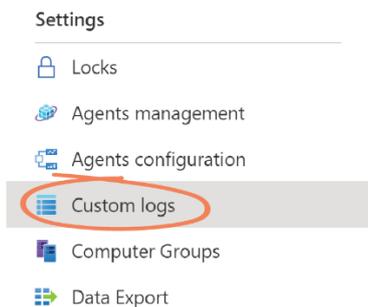
1. Select **Run Trigger > Run** from the top menu:



NOTE: You may need to wait a few minutes for the flow to complete. When successful, it should look something like the following:



2. Navigate to your Log Analytics Workspace (i.e., *SentinelLog*), and select **Custom logs** under *Settings* from the right-hand menu:

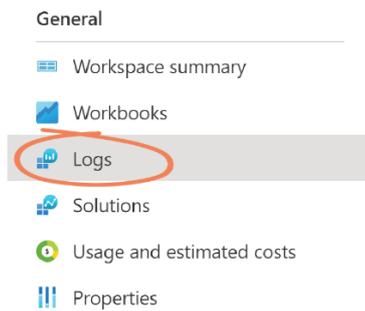


3. Highlight and copy the *Name* of the Custom log listed – in this case, *AdminByRequestLogs_CL*:

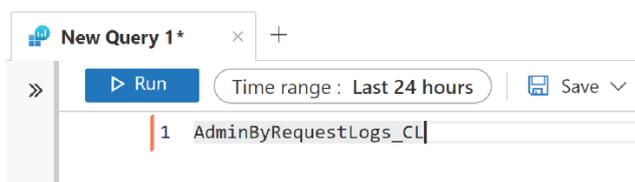
Showing 1 results

Name ↑↓	Type ↑↓
AdminByRequestLogs_CL	Ingestion API

- Select **Logs** under *General* from the left-hand menu:



- Close the *Queries* window that pops up. Paste the copied Custom log in the *New Query* field and select **Run**:



- New entries will begin to display in your Log Analytics Workspace as they are pushed through. Click the drop-down arrow to display details for each entry:

Query editor

Results Chart

TimeGenerated [UTC]	installs_s	uninstalls_s	elevatedApplications_s	scanResults_s
6/29/2022, 4:18:43.318 AM	[]	[]	[{"name": "Windows Command Processor", "path": "C:\\..."}]	[]
TenantId	53731173-cde7-49a8-8802-cc04b4099e90			
SourceSystem	RestAPI			
TimeGenerated [UTC]	2022-06-29T04:18:43.318Z			
installs_s	[]			
uninstalls_s	[]			
	[{"name": "Windows Command Processor", "path": "C:\\Windows\\System32", "file": "cmd.exe", "version": "10.0.19041.1 (WinBuild.160101.0800)", "vendor": "Microsoft Corporation", "sha256": "B99D61D874728EDC0918CA0EB10EAB93D381E7367E377406E65963366C874450", "scanResult": "Clean", "scanResultCode": 0,			

 **NOTE:** It may take several minutes for log entries to show up in the Log Analytics Workflow.

- Click **Save** to save the query for later use.
- With the Azure Log Analytics Workspace set up, you can now point your Sentinel setup to use this workspace as a data source.