Integration Manual

Microsoft Sentinel

Document Information

Code: **IM-Sentinel**
Version: **2.2**
Date: **14 February 2025**

Admin By Request
ZERO TRUST PLATFORM

Copyright © 2025 Admin By Request

Contact Admin By Request

+64 21 023 57020
marketing@adminbyrequest.com
adminbyrequest.com
Unit C, 21-23 Elliot St, Papakura, NZ

Table of Contents

Overview

Introduction

Microsoft Sentinel offers various ways to consume data from different sources. As Admin By Request provides public REST APIs for pulling Auditlog and Events data (see the API documentation here), it's an easy task to leverage the power of Azure Logic Apps to consume the APIs 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 and Events data in your Microsoft Sentinel setup. This manual provides a step-by-step guide on how to configure the integration.

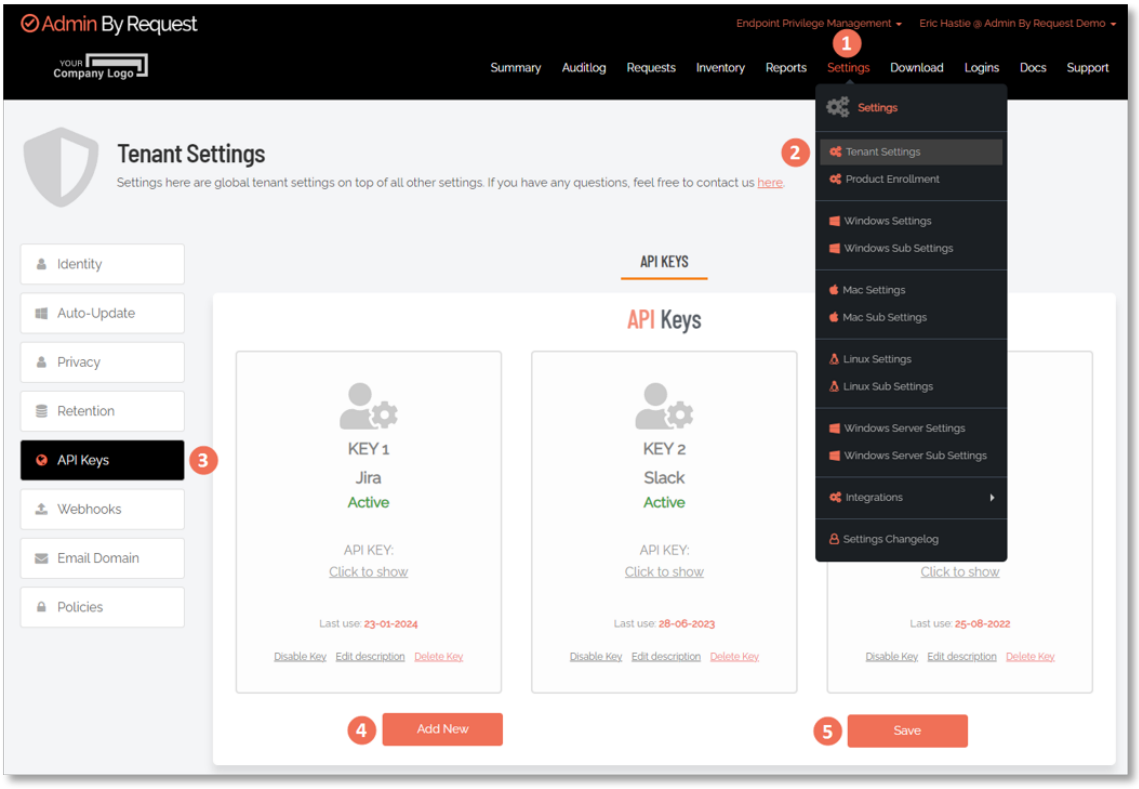
Assumptions

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

Prerequisites

To enable this integration, you must first:

1. Obtain your Admin By Request API Key. This key can be self-generated through your Admin By Request Portal via **Settings > Tenant Settings > API Keys > API KEYS**:



> **NOTE**
> Remember to 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 appears next to the **Save** button when the action is complete.

2. Make sure you have access to a Microsoft Sentinel Log Analytics Workspace to store your audit log entries.

Integration JSON Code

You will also need some JSON code to configure the API. Find the JSON code for this integration at the following links:

- Auditlog JSON Code
- Events JSON Code

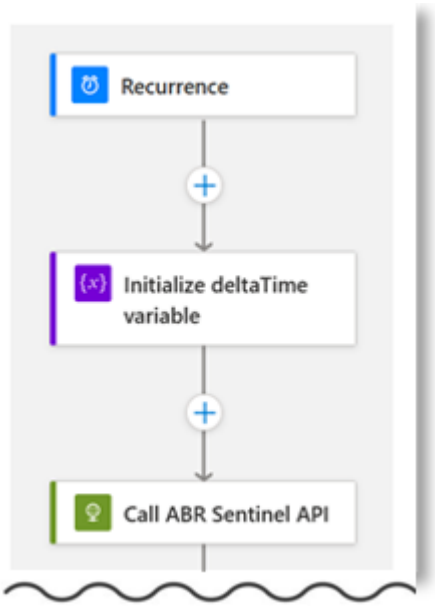
Why Integrate Microsoft Sentinel?

Microsoft Sentinel is Microsoft's scalable, cloud-native, SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) solution.

Many customers use Microsoft Sentinel for SIEM tasks and so we offer a public REST API to our customers as part of their Admin By Request license, providing the ability to pull data into their own SIEM systems for further analysis.

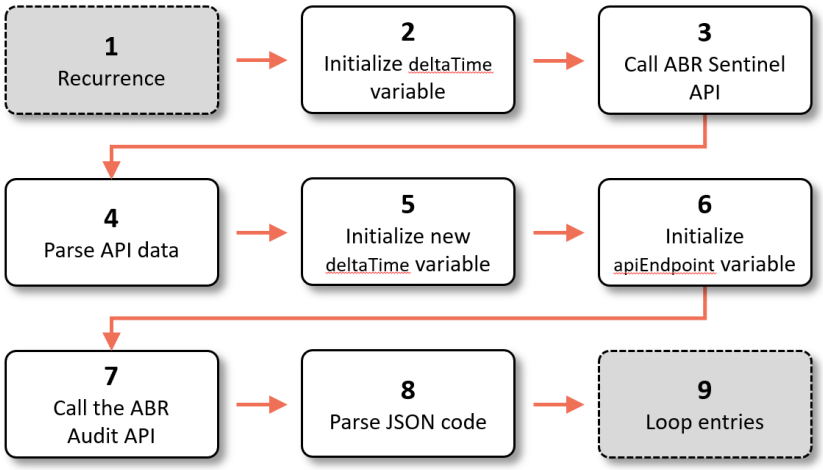
What the Integration Offers

With this integration, we've set up a hassle-free way to send Auditlog and Events data from your User Portal to Microsoft Sentinel using *Azure Logic Apps*. It's quick, painless, and ensures you get the best of both worlds: comprehensive user data combined with Sentinel's intelligent security analysis and threat detection capabilities:



How it Works

Microsoft Sentinel offers various ways to consume data from different sources. For this integration, we leverage the power of Azure Logic Apps to consume the Admin By Request Auditlog and Events APIs and forward each new entry to an Azure Log Analytics Workspace for further Sentinel consumption:



Refer to "Auditlog Data" on page 4 for full details on each of these Azure Logic App steps.

The Azure Logic App requires only a few simple changes before having you up and running with the appropriate data in your Sentinel setup. You can then point your Sentinel setup to use the configured workspace as a data source.

Something Missing?

If you've identified a bug or have a suggestion for this integration, or another SIEM integration you'd like us to add, contact us here and we'll see what we can do.

NOTE
The task descriptions in this document (and screenshots in particular) cover the state of Microsoft Sentinel at the time of writing. While every effort is made to ensure currency, the screens you see during setup may look a little different, especially color schemes and the placement of buttons and links.

Integration Tasks

The remainder of this document describes two groups of tasks; one group for "Auditlog Data" on page 4 and the other for "Events Data" on page 19.

Auditlog Data

Introduction

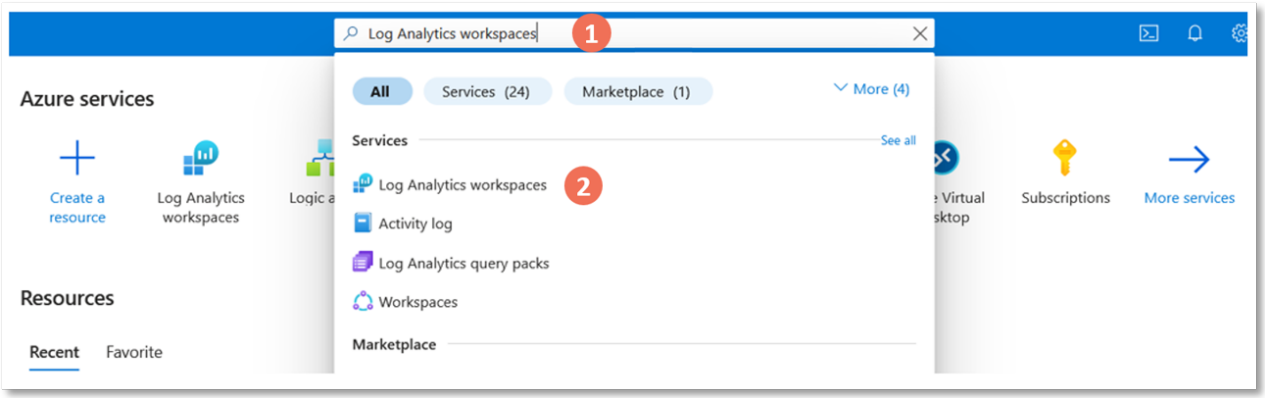
The following tasks are covered in this section:

NOTE
As mentioned in the Overview (under *Something Missing?*), due to regular Sentinel updates by Microsoft, some screens may look slightly different from those depicted in this document.

A. Set up Log Analytics Workspace

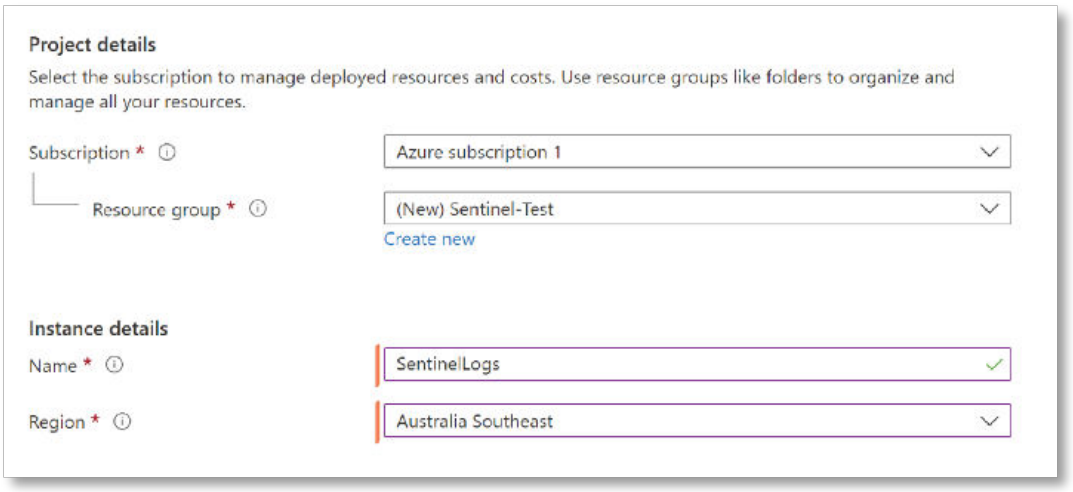
A Log Analytics Workspace is the management unit which allows you to store, query, and retain data pulled in from other tools – in this case, Auditlog data pulled from your Admin By Request User Portal. Task A involves setting up this storage unit for use in subsequent tasks.

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 Workspaces** from the *Services* list:



3. Click **Create** and fill out the Project details.

In the *Instance Details* section, give the workspace a Name and select the appropriate Region from the drop-down menu:



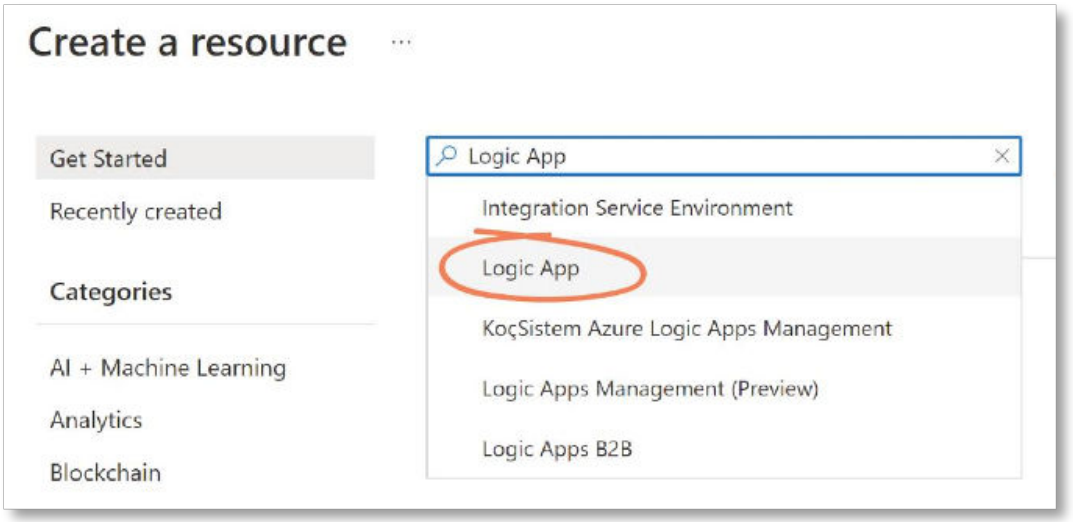
In the above screenshot, we have created a new *Resource group* called **Sentinel-Test** for the purpose of this demonstration.

4. Click **Review + Create** at the bottom of the page.
5. When validation has passed, click **Create**, and wait for deployment to complete.

B. Create new Azure Logic App

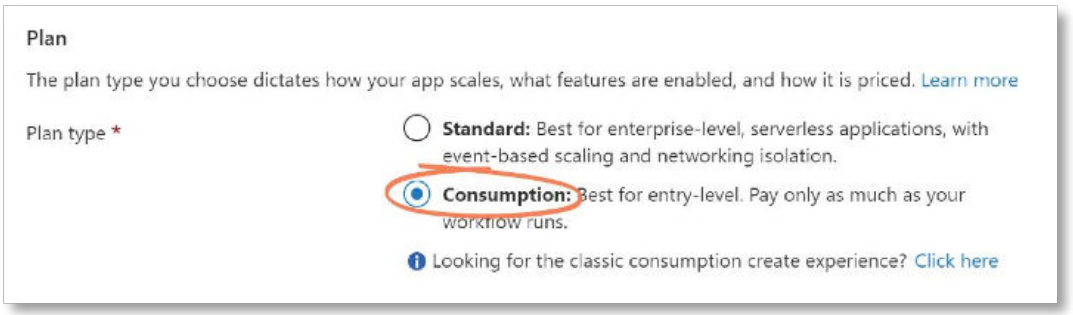
An Azure Logic App is needed to consume the Admin By Request Auditlog API and forward each new entry to the Azure Log Analytics Workspace created in Task A.

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, click the **Create** button.
3. Use the Search box to search for and select **Logic App** from the drop-down menu:

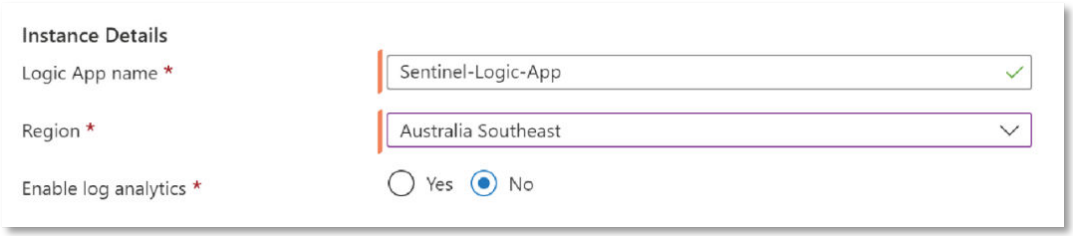


4. Click **Create**.

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



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



6. Select the **Review + Create** button, followed by **Create**.
7. Once deployment is complete, click **Go to resource**.

C. Paste in JSON Code

To get the app behaving correctly for this integration, replace the default code in the Logic app code view with the JSON code we have written – access it here.

1. Confirm which data center you are connected to. This is important because the data center domain (also known as *API prefix*) is embedded during creation of the API key (see "Prerequisites" on page 1) and is also specified in the JSON code around line 27 and the two must match:

To determine your data center, go to page Tenant Settings > API Keys in the portal and check which API prefix is shown under **About API Keys**. The API prefix will be one of the following:

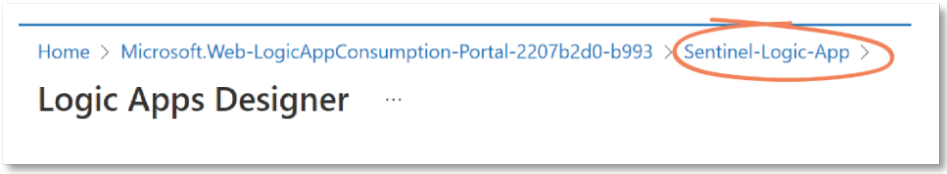
- **https://dc1api.adminbyrequest.com** (Europe)
- **https://dc2api.adminbyrequest.com** (USA)

Make a note of your prefix - among other things, this is the domain used when an API Key is created.

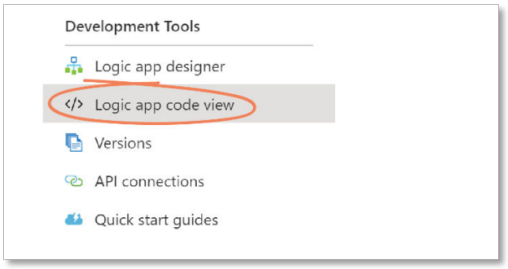
> You can also see your API prefix on the API web pages (e.g. Public API > Auditlog API). However, a small script runs in the background that determines to which data center you are attached, so JavaScript must be enabled in your browser for this to work.

If the data center is incorrect, you must edit the JSON code after copying and pasting it (step 4 in this procedure).

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



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



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

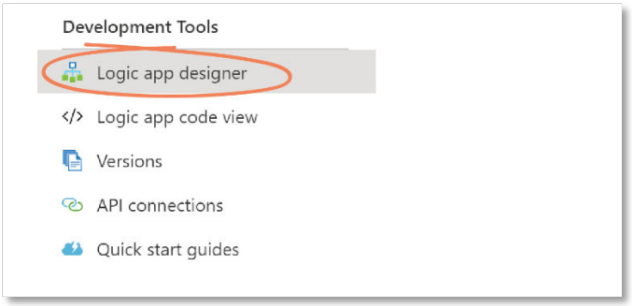
> **IMPORTANT**
> As mentioned in step 1, if you need to change the data center (~line 27), do so now.

5. Click **Save**.

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.

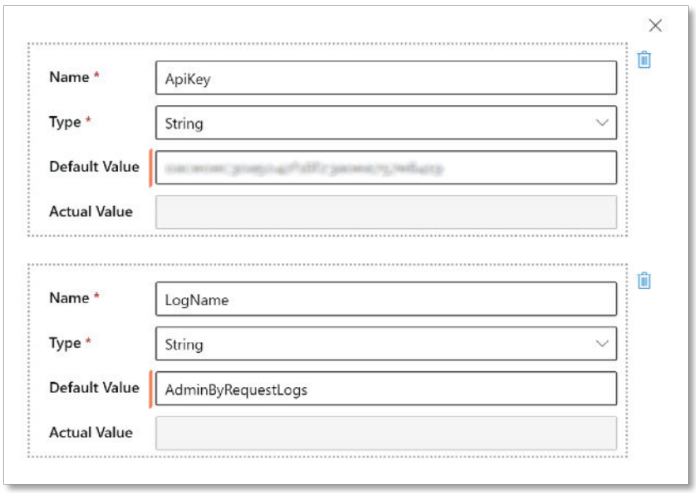
1. From the left-hand menu, under *Development Tools*, select **Logic app designer**:



2. From the top menu, select **Parameters**:

3. 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:



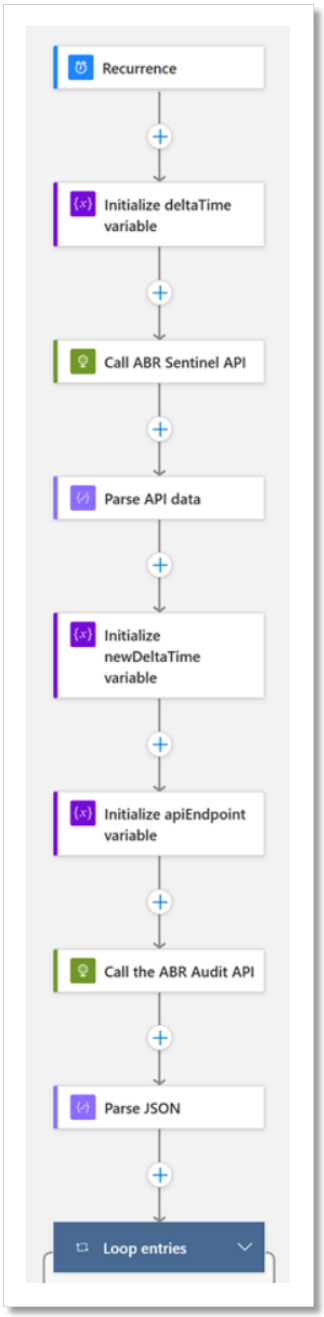
In the above screenshot, the API Key is blurred out, and we have used **AdminByRequestLogs** as the *LogName*.

4. Click **Save** in the Logic app designer and close the Parameter window.

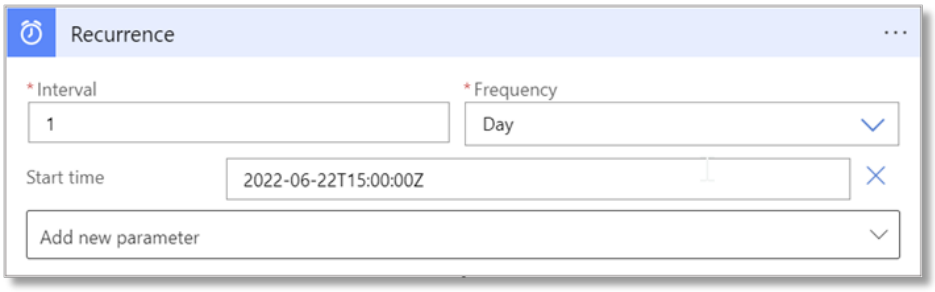
E. Understand the App Flow

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:

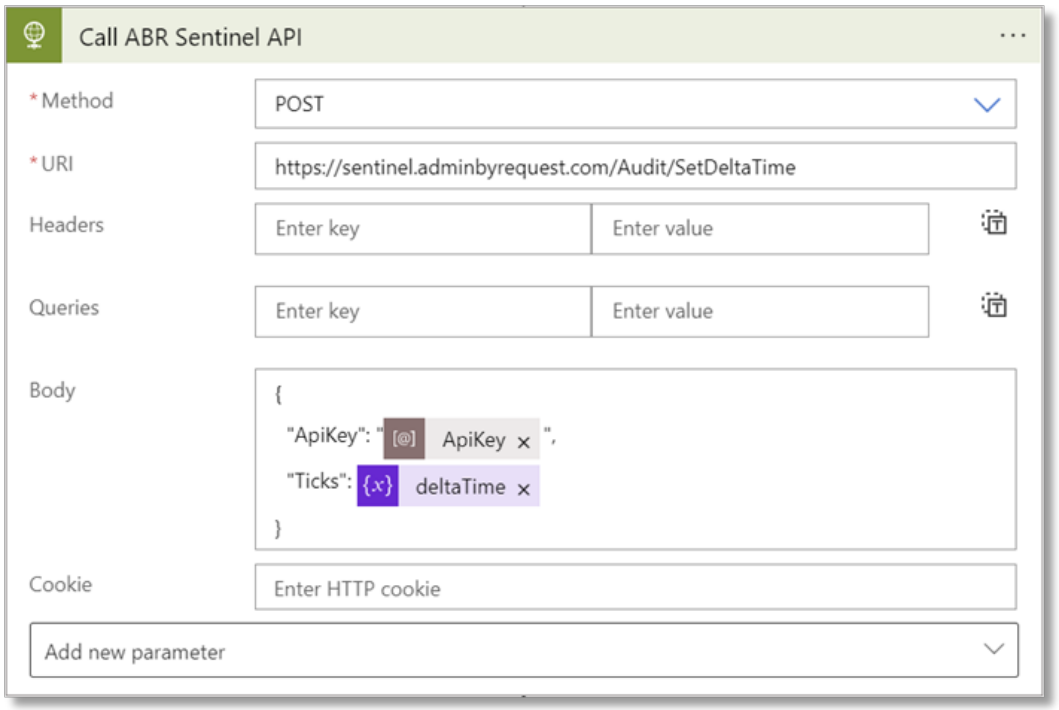


- **Recurrence** – This tells the app when it should run. In our example we've set up a recurring trigger that runs once every day. You can replace this trigger with whatever works best for your setup.

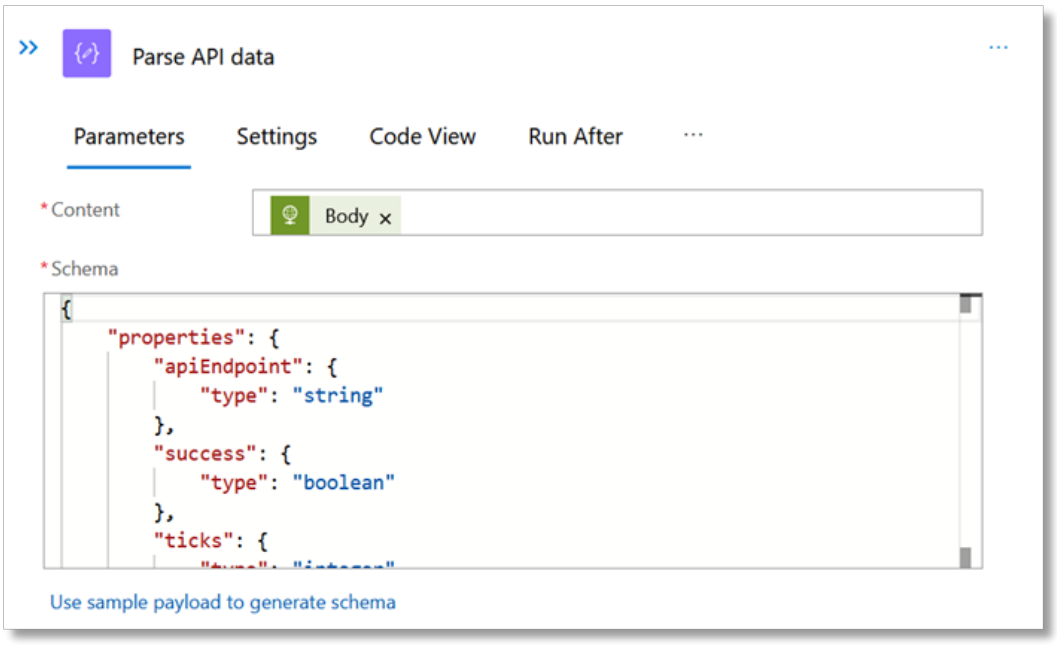


- **Initialize deltaTime variable** – In order to call the Admin By Request Audit API, we need a variable containing the 'from' ticks. Basically, telling the Audit API to 'give me all audit logs since this time'. This is defaulted to the number of ticks representing DateTime.Now.

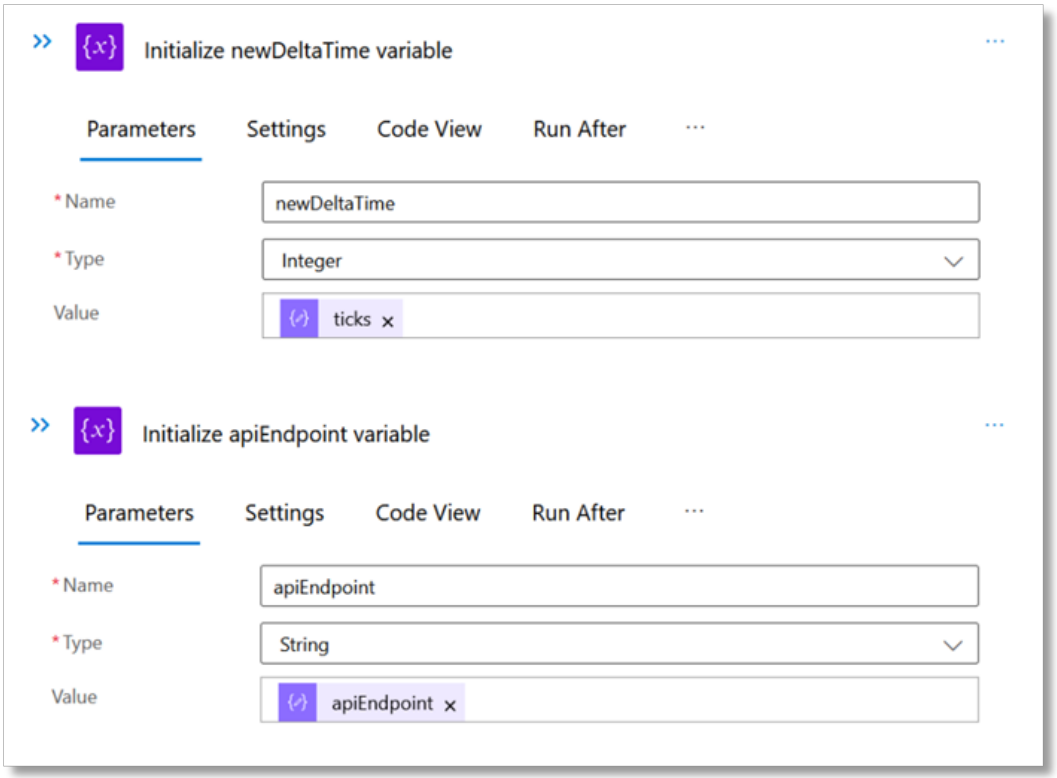
- **Call ABR Sentinel API** – Since Logic Apps don't hold any state, we need some way of storing the last time the Audit API was called for a given API-key.
  We've created an API endpoint that allows you to do just this. We simply call the SetDeltaTime endpoint with your API Key and the deltaTime variable, 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.



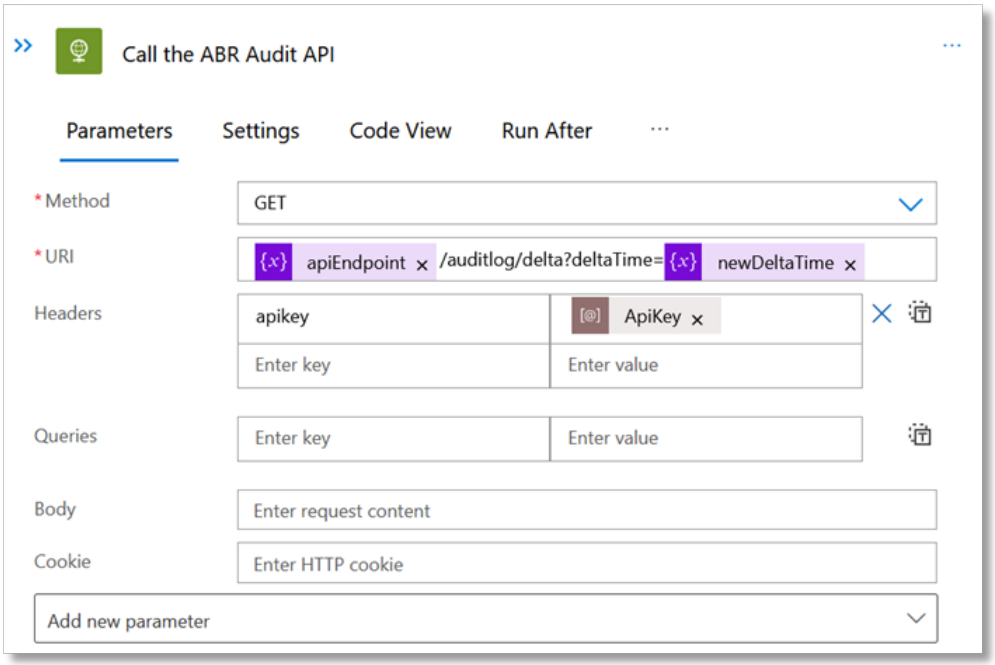
- **Parse API Data** – The result from the API needs to be parsed in order to use the resulting variables.



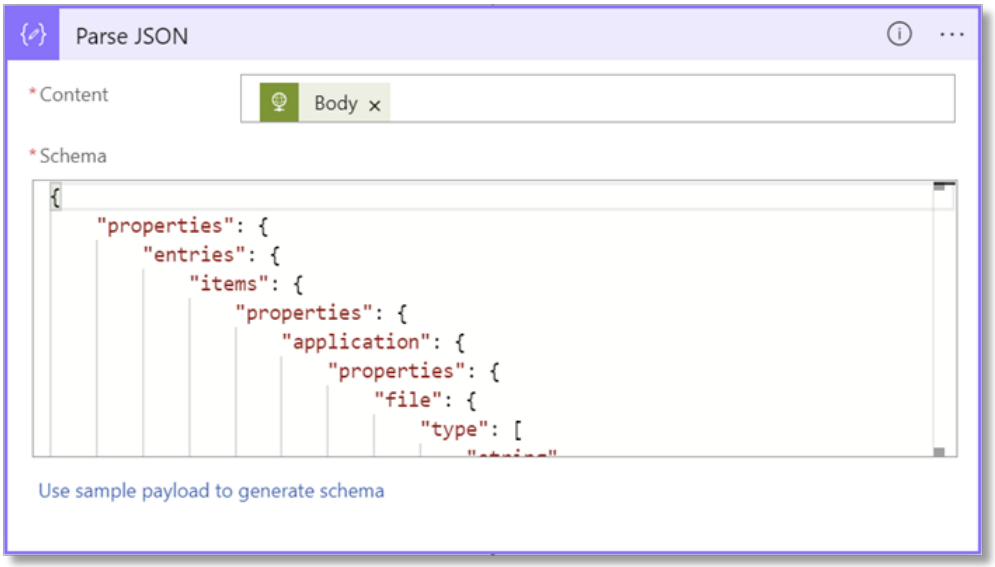
- **Initialize newDeltaTime and apiEndpoint variable** – With the values from the SetDeltaTime endpoint, we need to store two variables: newDeltaTime and apiEndpoint.
  These variables hold the tick-value for when the Audit API was last called, as well as the Admin By Request endpoint to call for Audit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



- **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.



- **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).

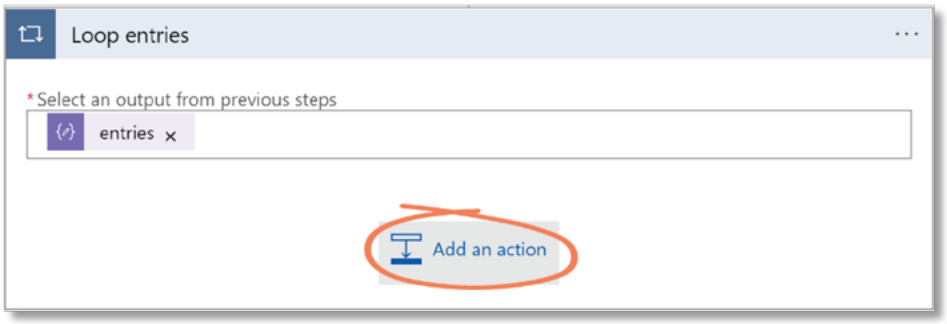


- **Loop entries** – The final step in the app flow simply loops through every entry from the Audit call. Here you decide what to do with the data (see Task F).

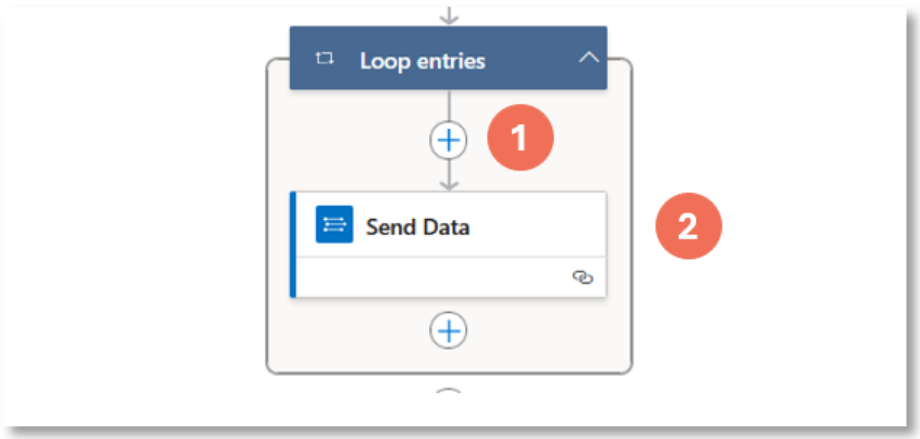
F. Configure Loop Entries

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:



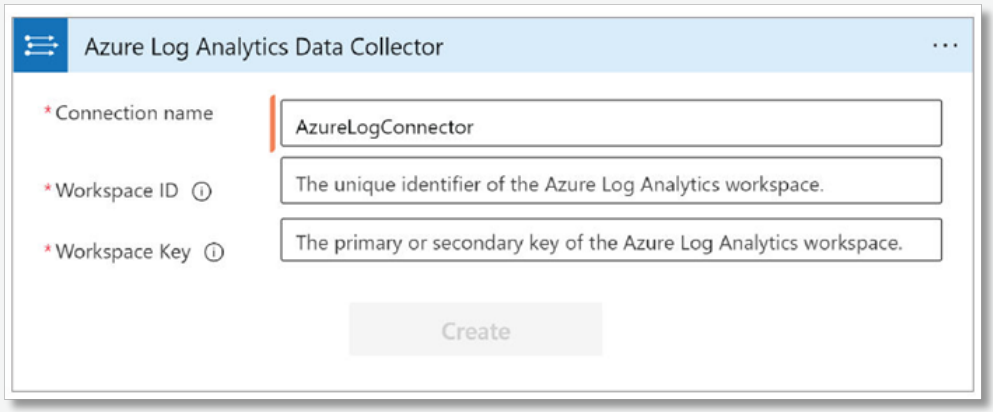
2. Click the **+** sign to add a **Send Data** action:



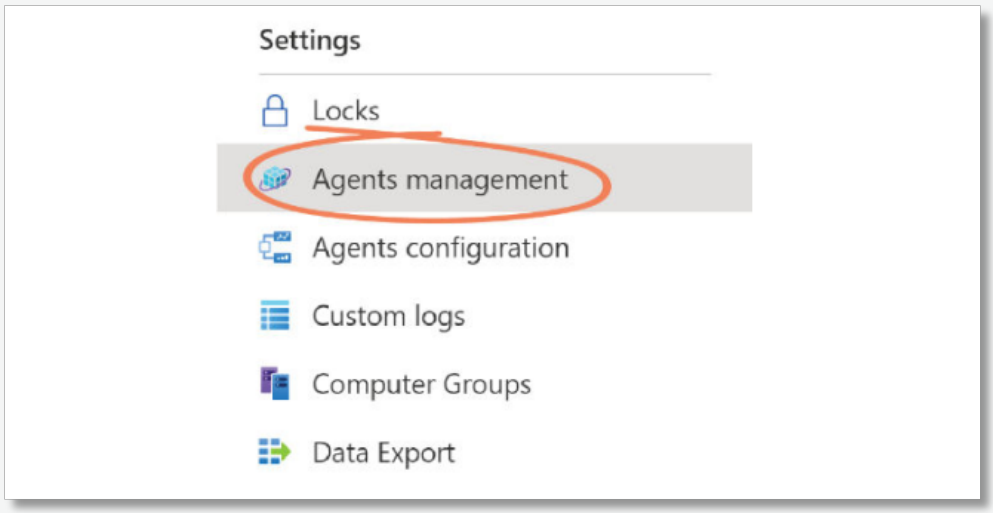
> **NOTE**
> Earlier versions of MS Sentinel might require selection of a Data Collector first. If so, make sure you select **Azure Log Analytics Data Collector**.

After clicking **Send Data**, you may be prompted to create a connection. If so, follow the steps below.

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

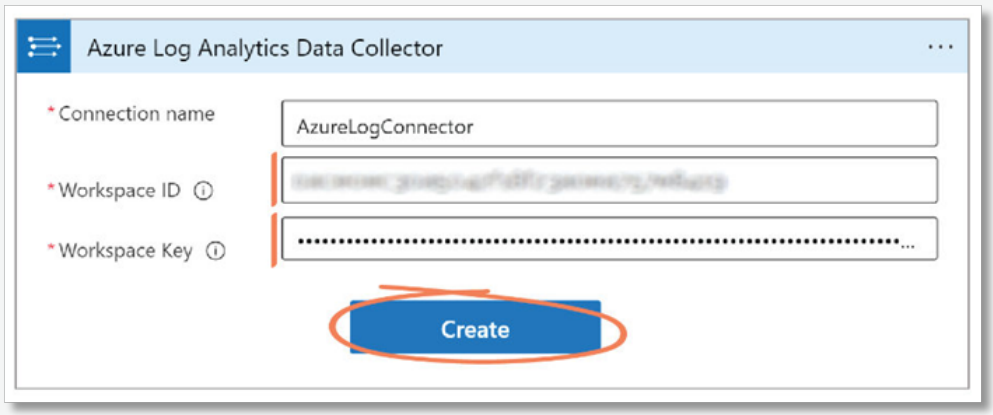


2. To locate the *Workspace ID* and *Workspace Key*, open your Log Analytics Workspace (i.e., *SentinelLog*) in a new tab and select **Agents Management** under *Settings* from the left-hand menu:

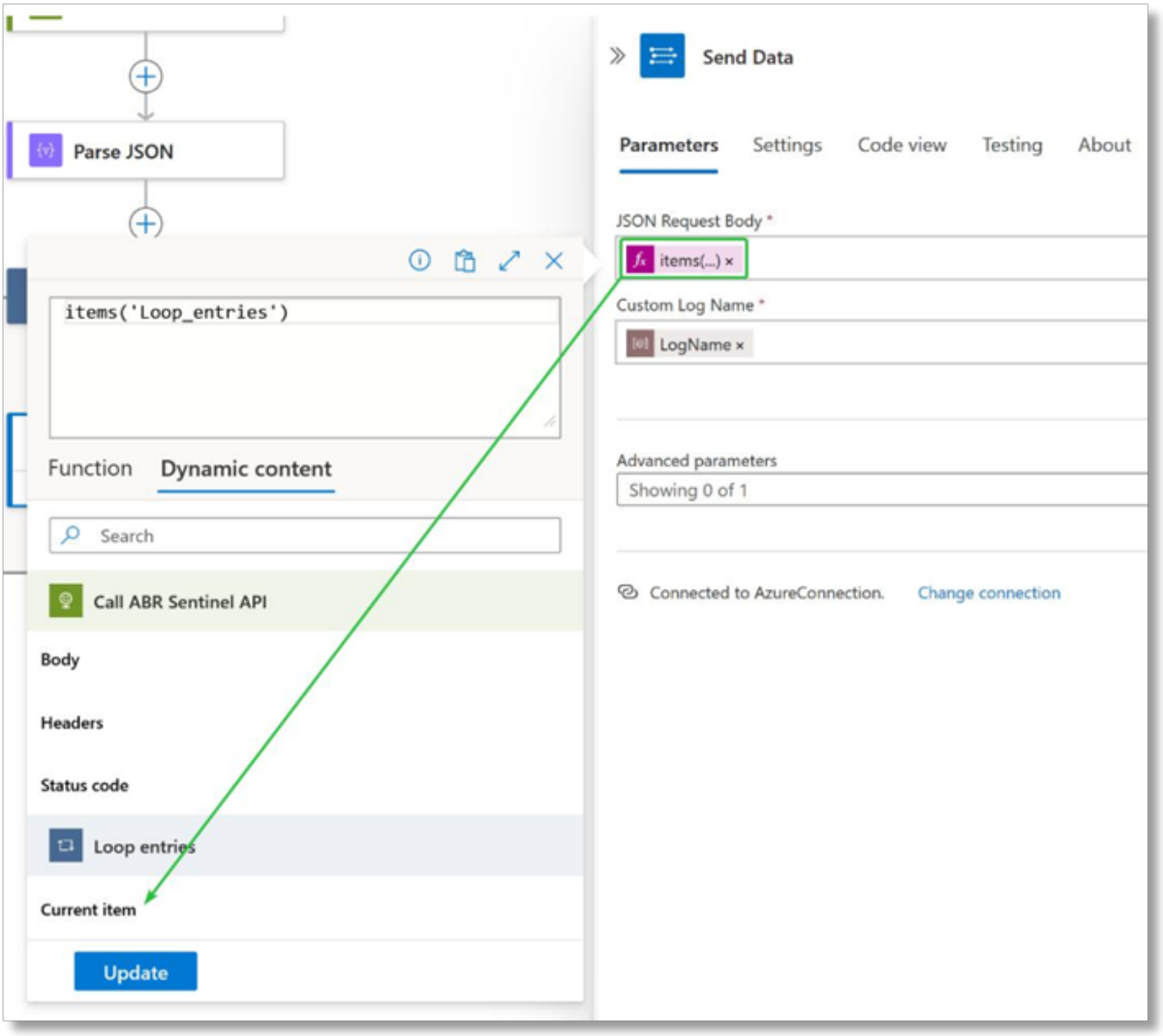


3. Copy the *Workspace ID* and *Primary key* values from this page:

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

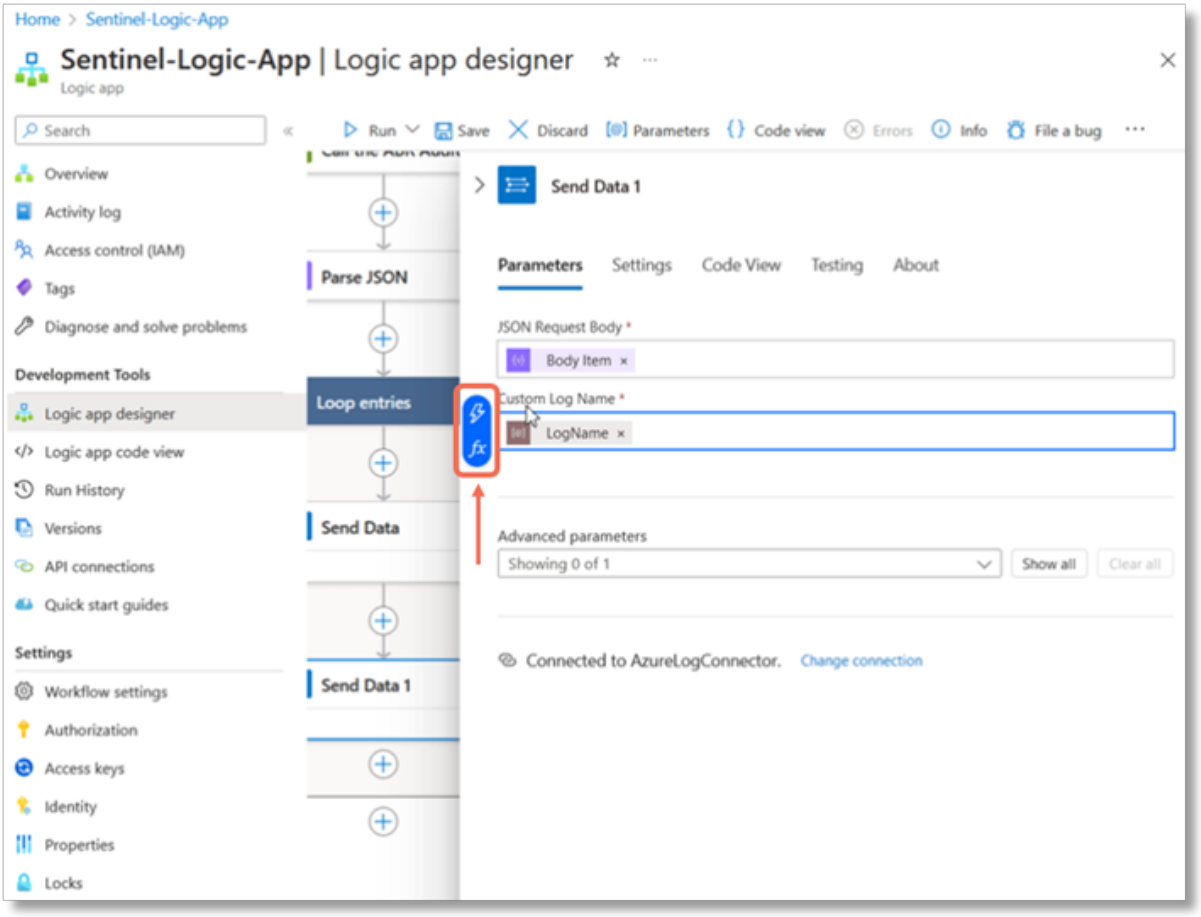


3. For **Send Data**, add the following two items:
   - In the *JSON Request Body* field, select **Add dynamic content** via the blue and white function icon (***fx***), and in the *Dynamic content* tab, select **Loop entries** > **Current item**:



   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.

The screenshot shows where to find the function icon (***fx***), which enables adding dynamic content:

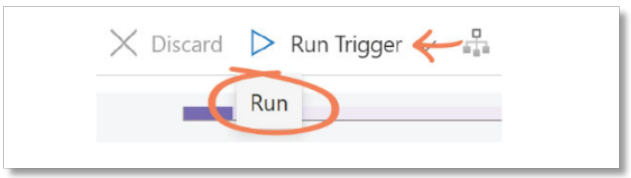


An animated GIF in our Documentation Center provides further detail on the steps required to add dynamic content.

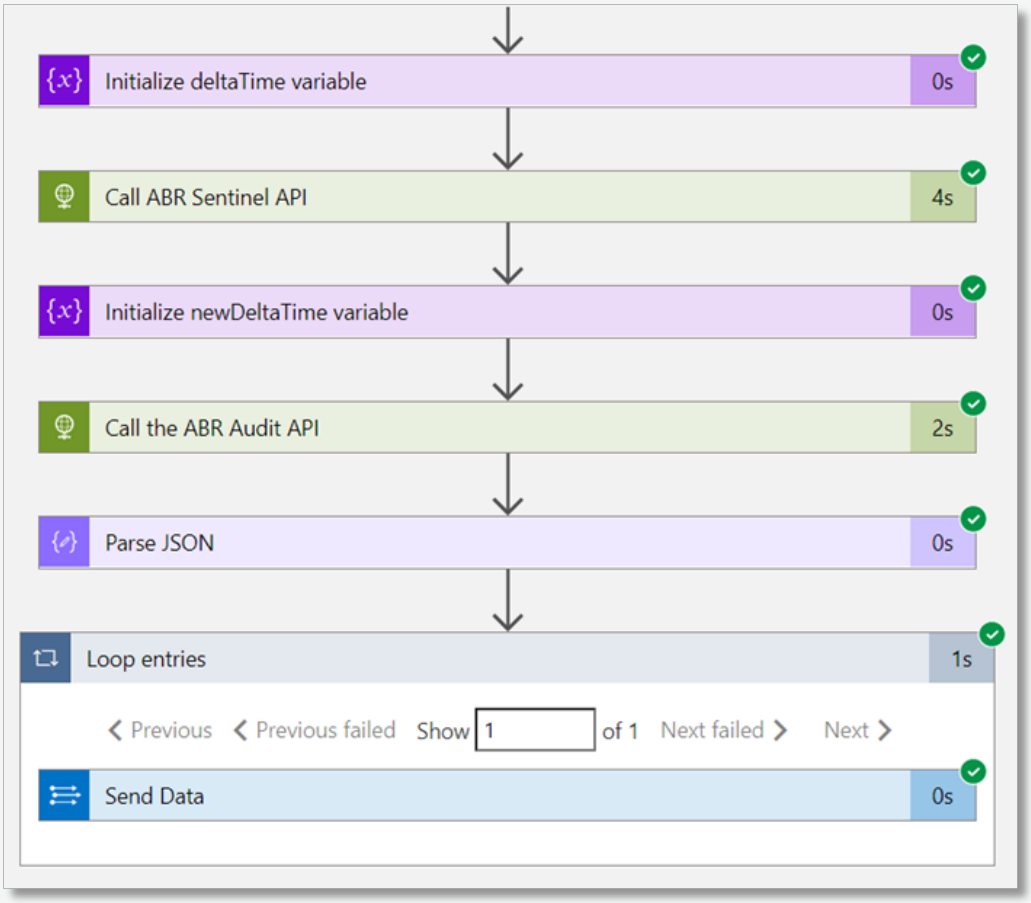
4. Select the **Save** button to save your app.

G. Test the Integration

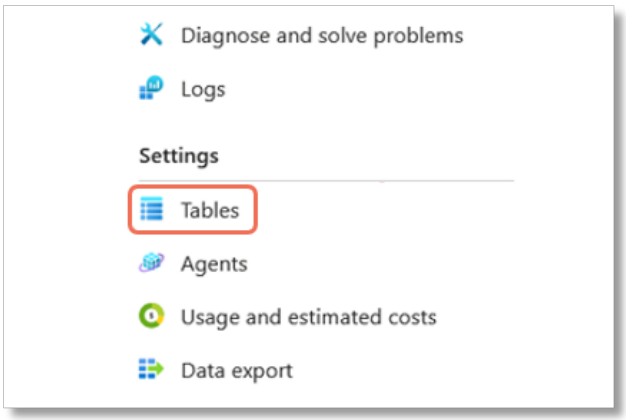
1. Select **Run Trigger > Run** from the top menu:



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

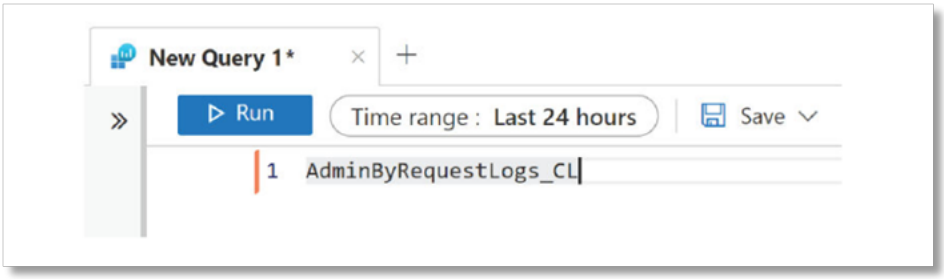


2. Navigate to your Log Analytics Workspace (i.e., *SentinelLog*), and select **Tables** under *Settings* from the left-hand menu:

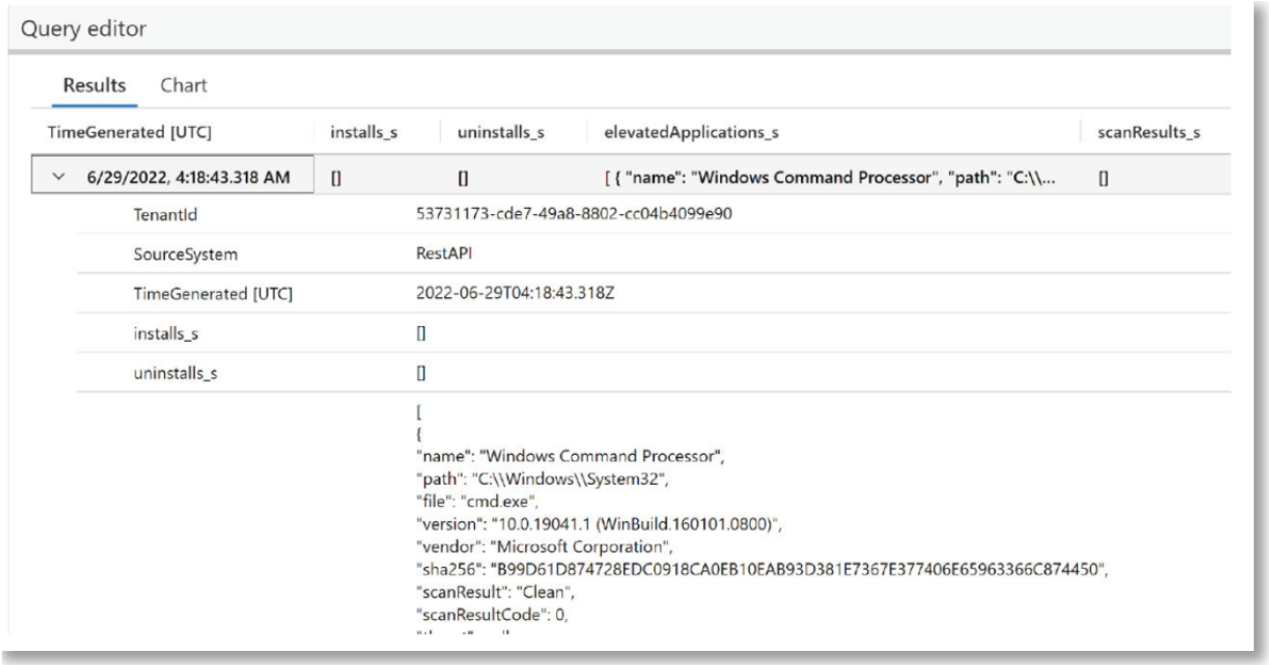


3. Highlight and copy the *Name* of the log listed – in this case, *AdminByRequestLogs_CL*:

4. Select **Logs** from the left-hand menu (if a *Queries* window pops-up, close it).
5. Paste the copied log name into the *New Query* field and select **Run**:



6. 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:



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

7. 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.

Events Data

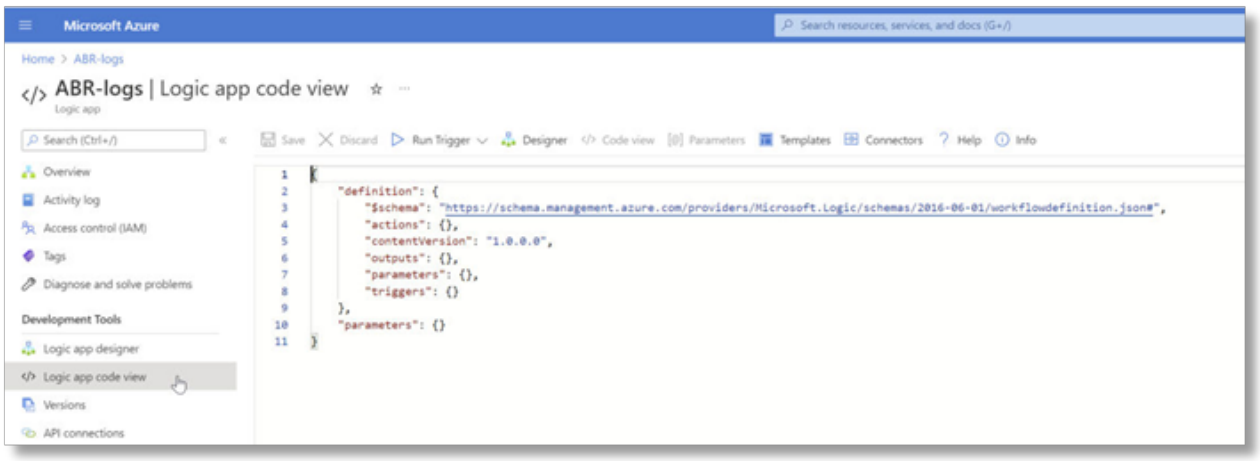
Introduction

The following tasks are covered in this section:

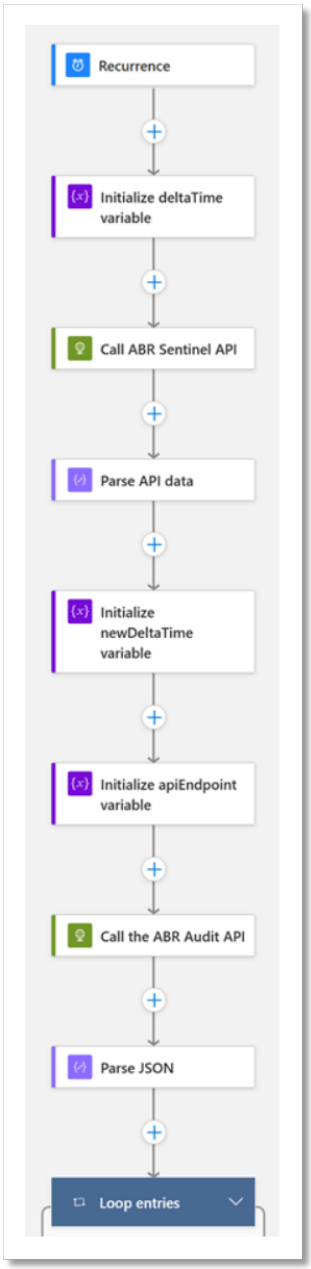
NOTE
As mentioned in the Overview (under *Something Missing?*), due to regular Sentinel updates by Microsoft, some screens may look slightly different from those depicted in this document.

A. Set up Azure Logic App

1. In order to get started, first set up an Azure Logic App within Azure Portal. You can choose to either setup the app from scratch, or you can choose to use the Admin By Request template. If you choose to use the Admin By Request template, jump into the Code View of your Logic App and paste in this logic app code (refer to "JSON Code – Events Data" on page 40 for a full code listing):



2. Now that we have the structure for the Logic App, navigate to the Logic App Designer to view the different steps.
   The app flow has nine segments arranged as follows:



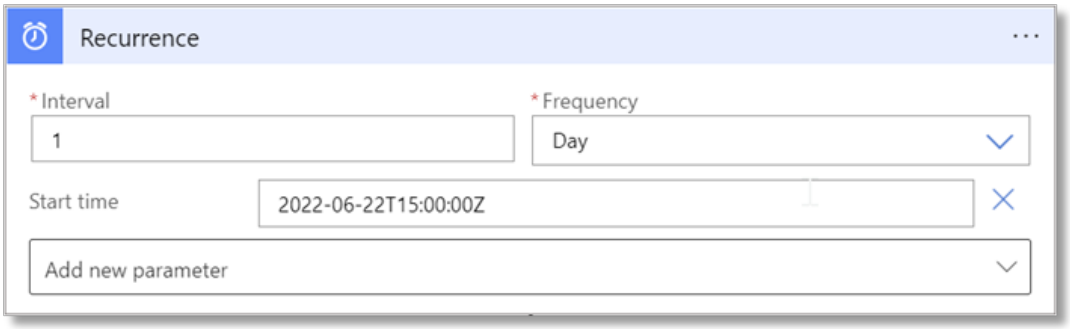
B. Enter Parameters

1. The app has two configurable parameters. Replace these with your own API-key and the name you'd like for the custom log in your Log Analytics Workspace. This is similar to the earlier task "Auditlog Data" on page 4

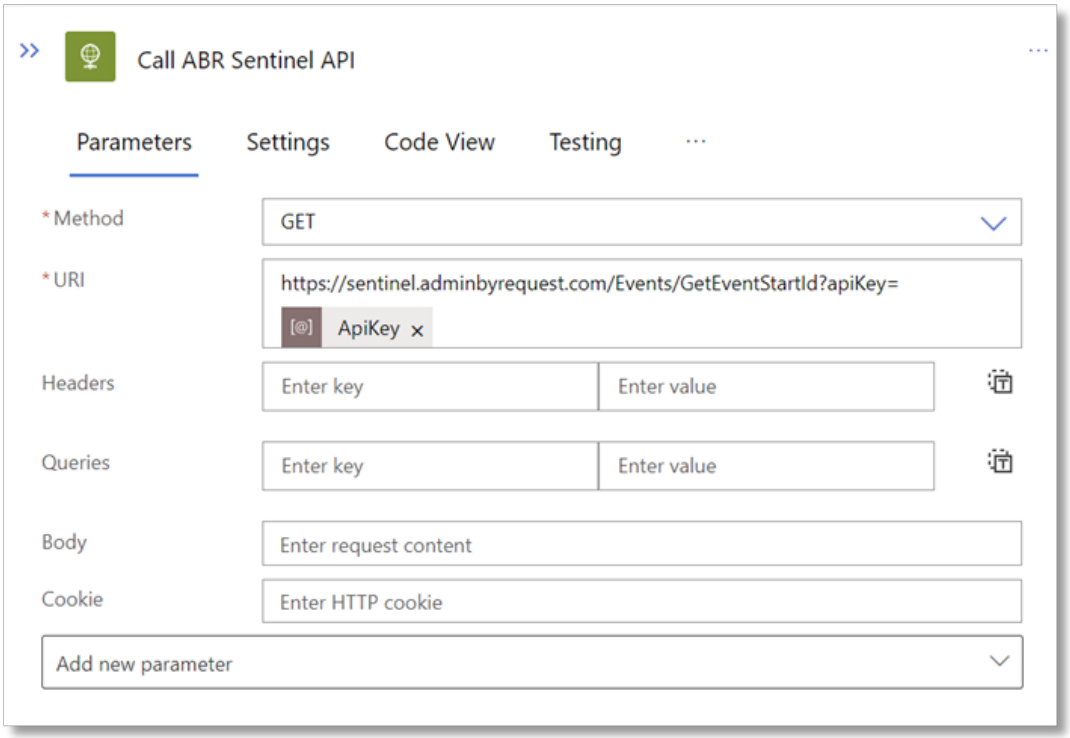
C. Understand the App Flow

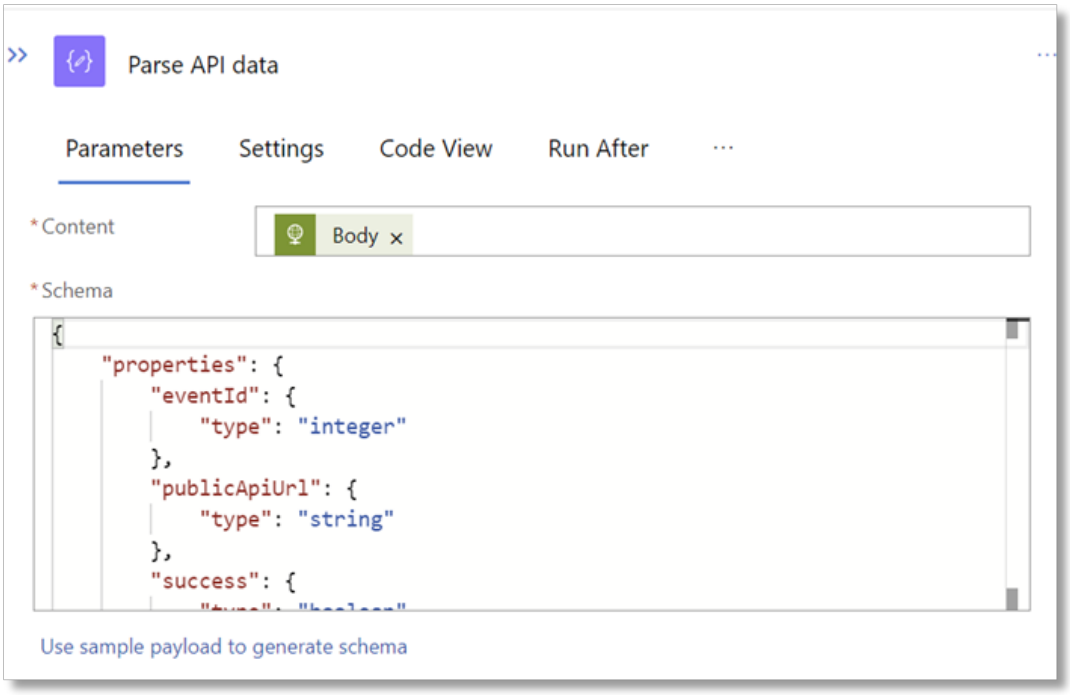
The flow of the app is simple – let's go through the different bits:

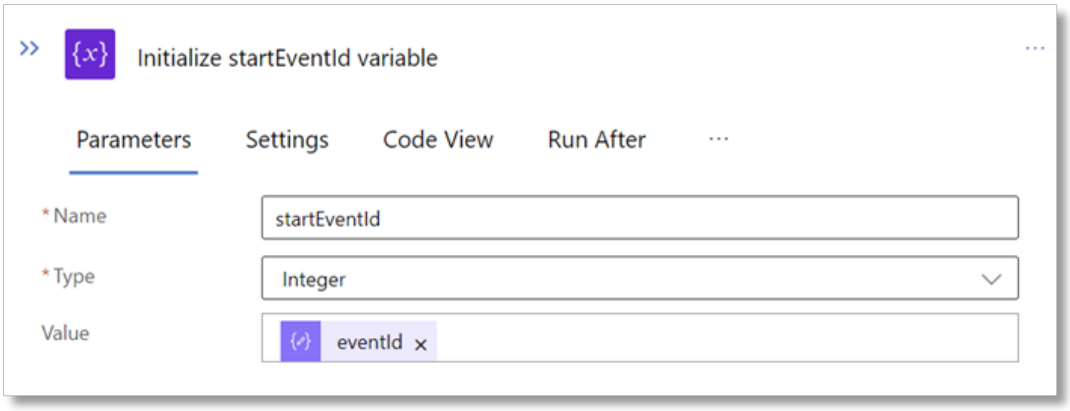
1. Recurrence tells the app when it should run. In our example we've set up a recurring trigger that runs once every day. You can replace this trigger with whatever works best for your setup:

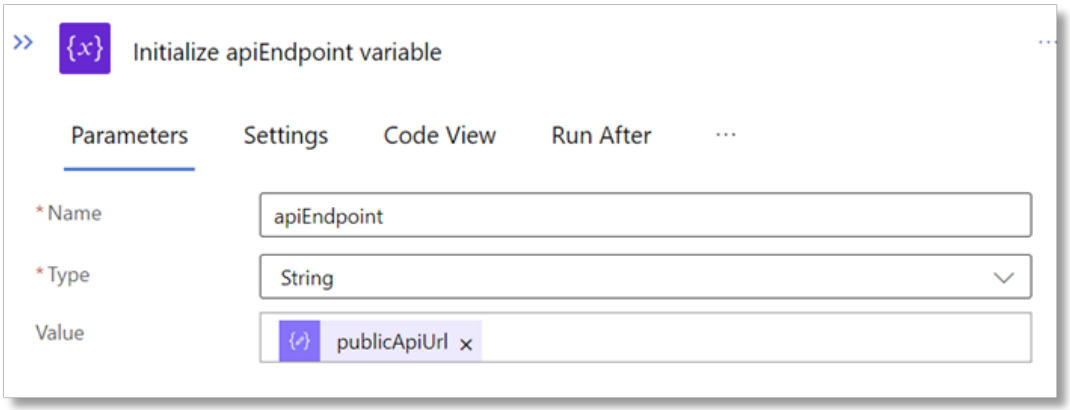


2. In order to call the Admin By Request Events API, we'll need to fetch the EventID to serve as the starting point for the query. Furthermore, we need to determine which API endpoint to use.
   This is done by calling the Admin By Request Sentinel API and storing this information (four screenshots in this step):

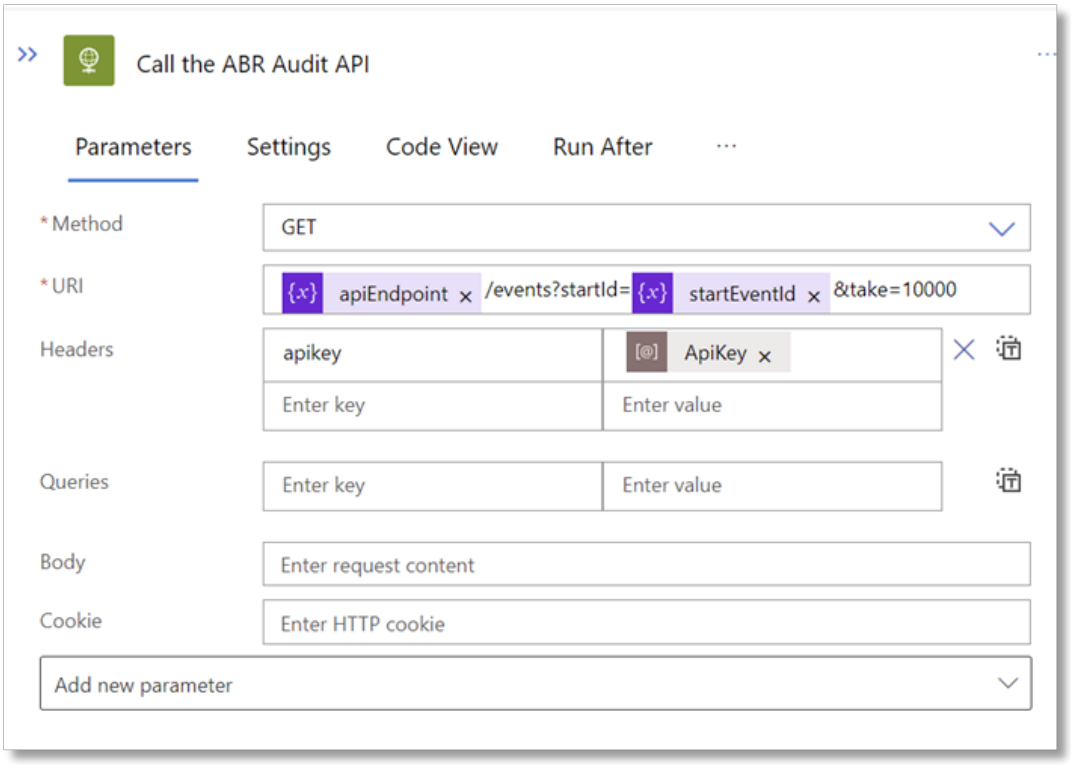



Parse API data
Parameters
Settings
Code View
Run After
*Content
Body
*Schema
{
"properties": {
"eventId": {
"type": "integer"
},
"publicApiUrl": {
"type": "string"
},
"success": {
Use sample payload to generate schema

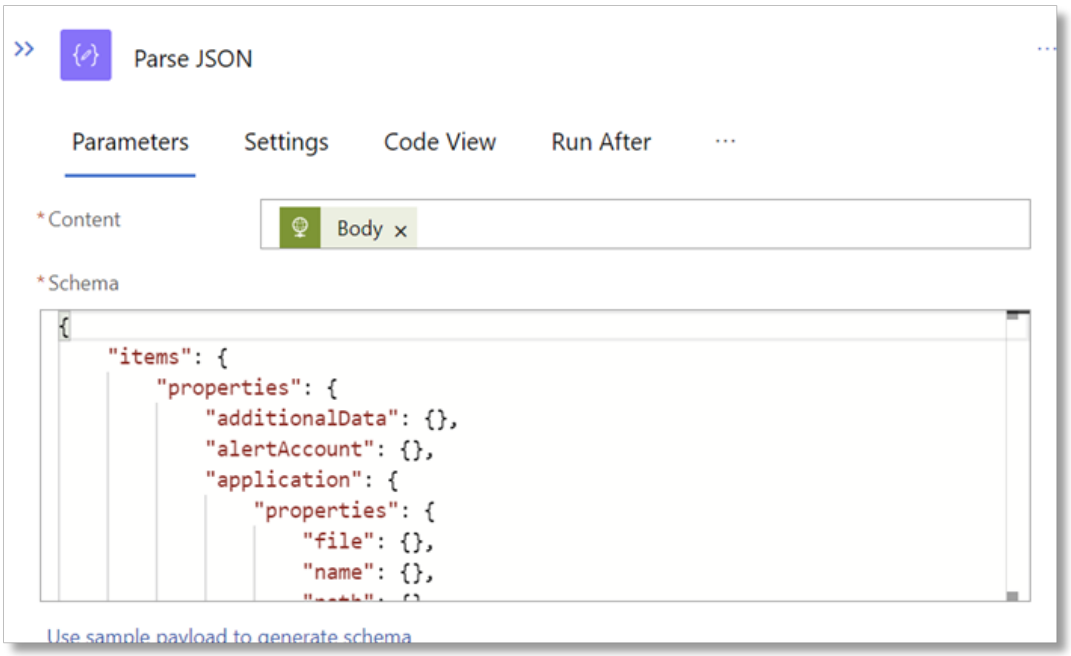

Initialize startEventId variable
Parameters
Settings
Code View
Run After
*Name
startEventId
*Type
Integer
Value
eventId


Initialize apiEndpoint variable
Parameters
Settings
Code View
Run After
*Name
apiEndpoint
*Type
String
Value
publicApiUrl

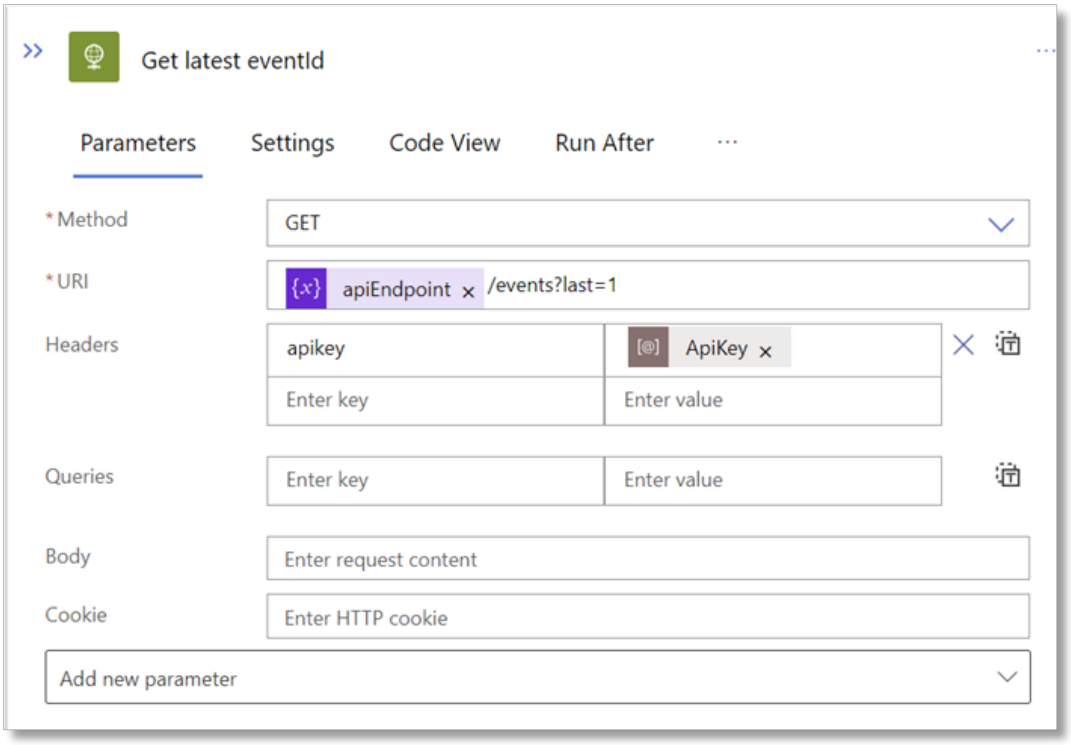
3. Once we have the startEventId and the apiEndpoint parameters in place, we can use these to call the Admin By Request Events API to fetch the events that have been created since the query last ran:

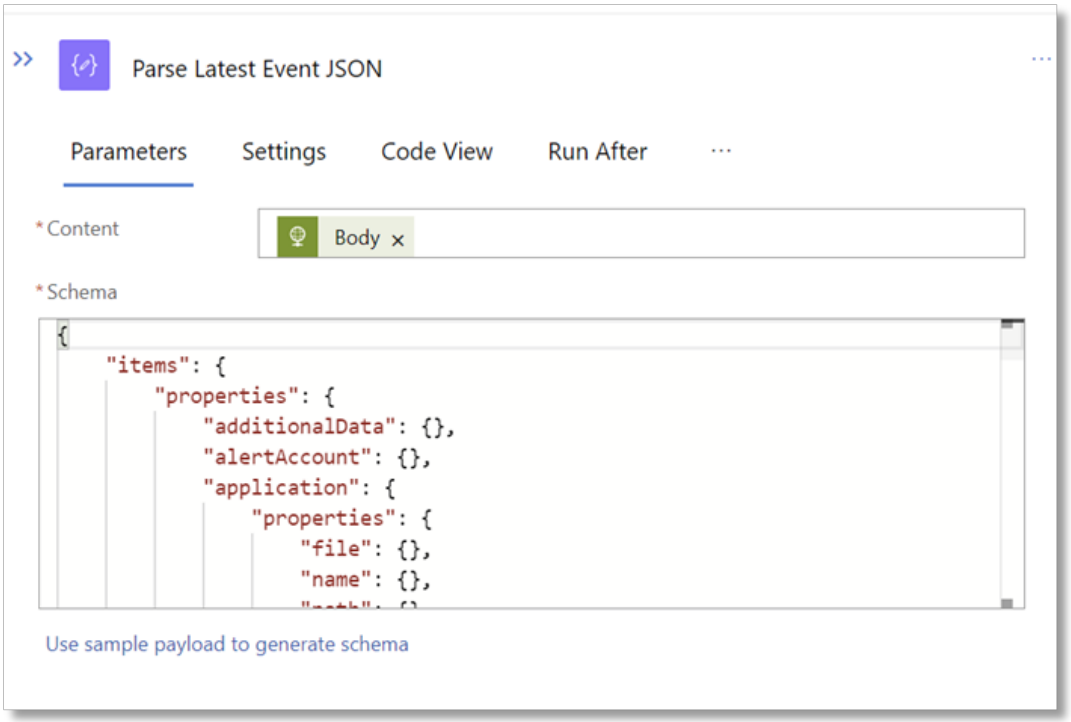


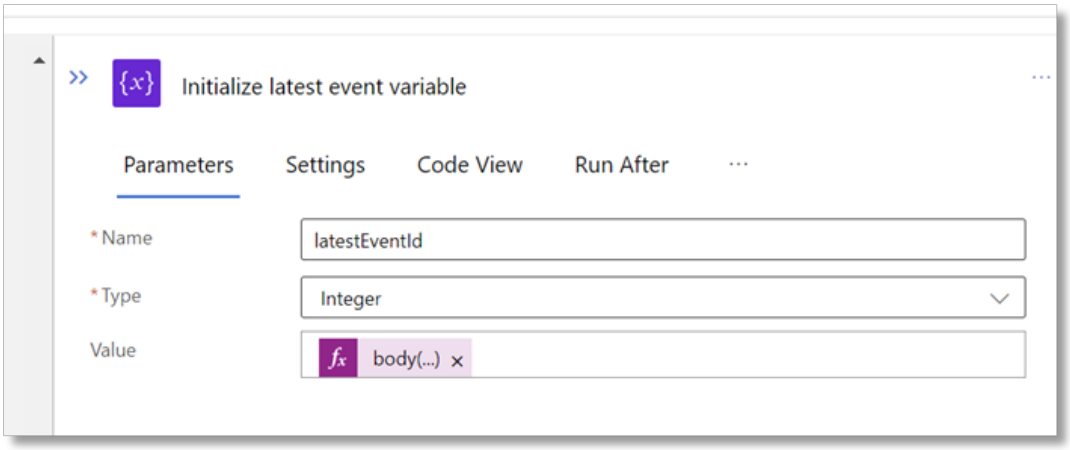
4. We can then parse the result of this API call to be used when looping through the data later on.

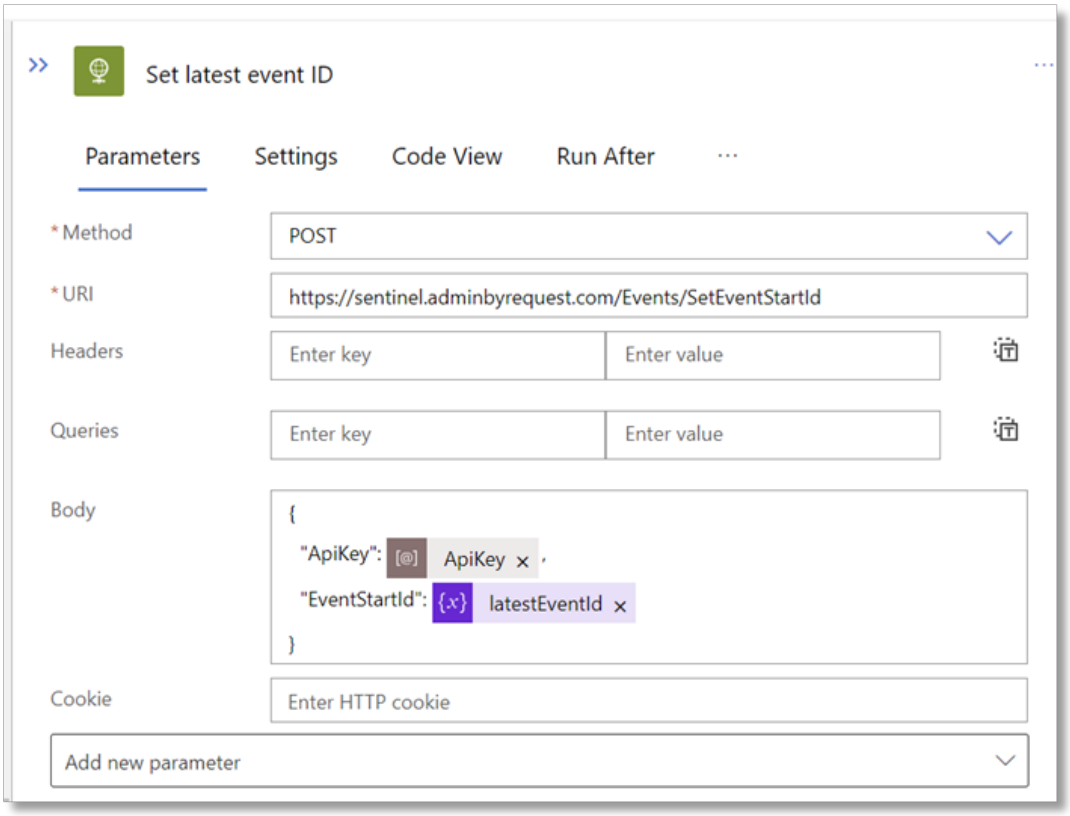


5. Because Logic Apps can't hold state, we'll need to save the latest EventID to the Admin By Request Sentinel API in order to have the starting point for the next time the Logic App runs (four screenshots in this step):

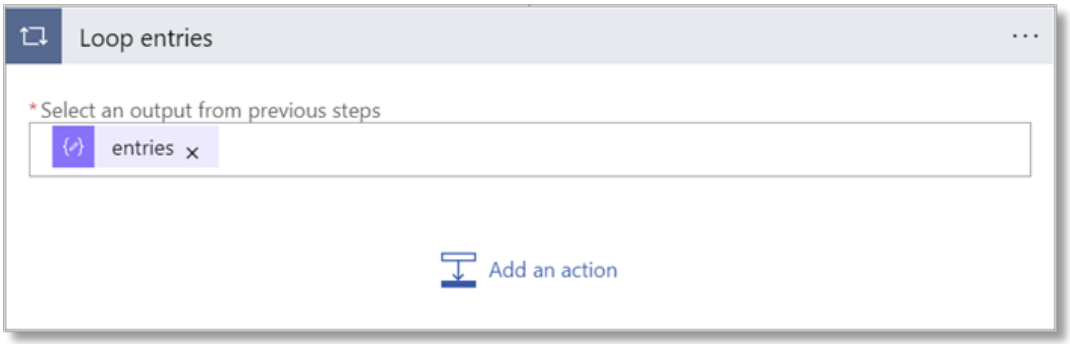








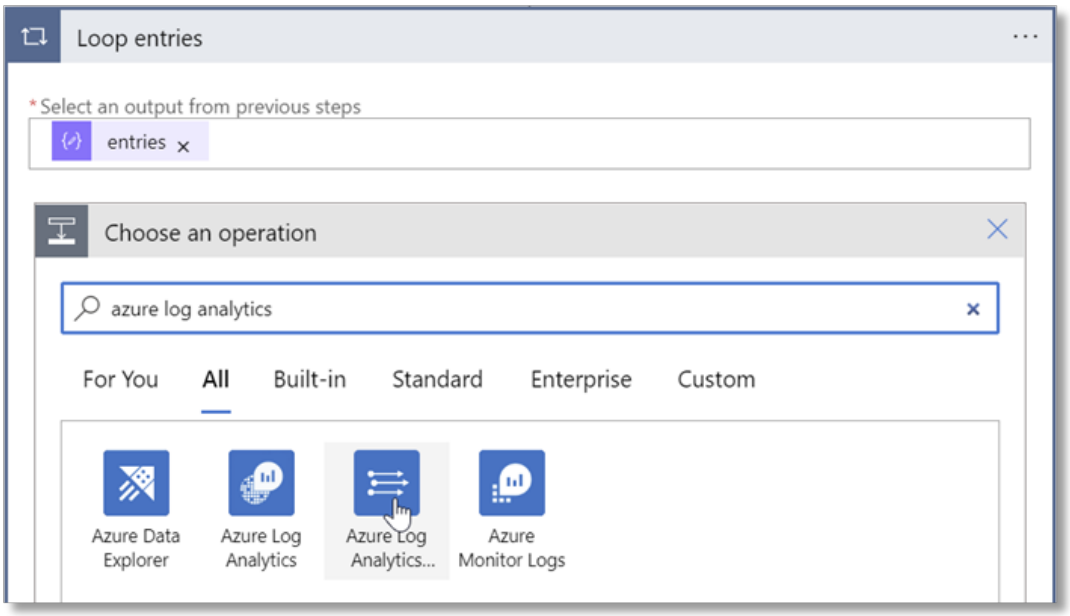
6. Next up we parse the response from the Events API as JSON using a schema based on the response type from the Events API (view this page for more information).



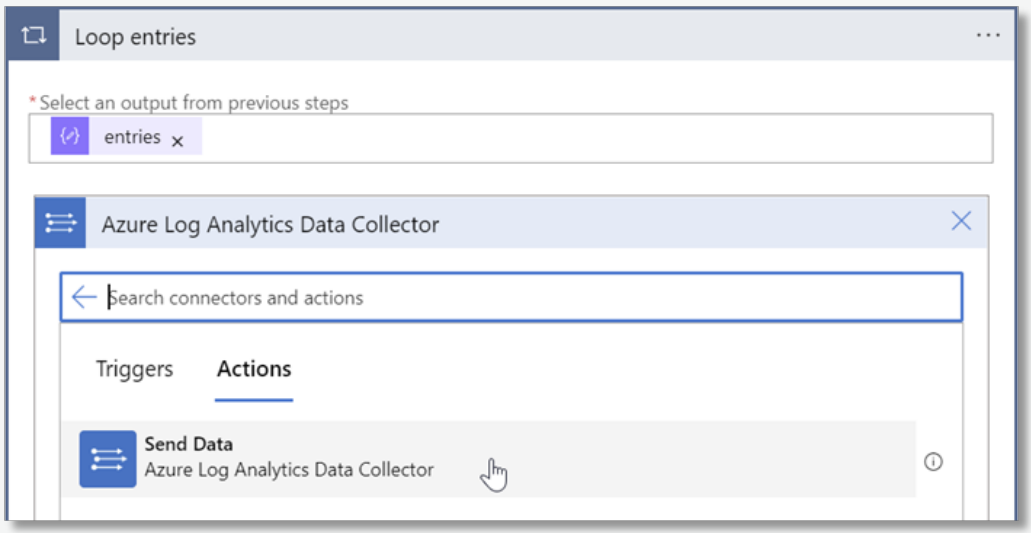
7. The last step simply loops through every entry from the Events call. Here you decide what to do with the data.

D. Configure Loop Entries

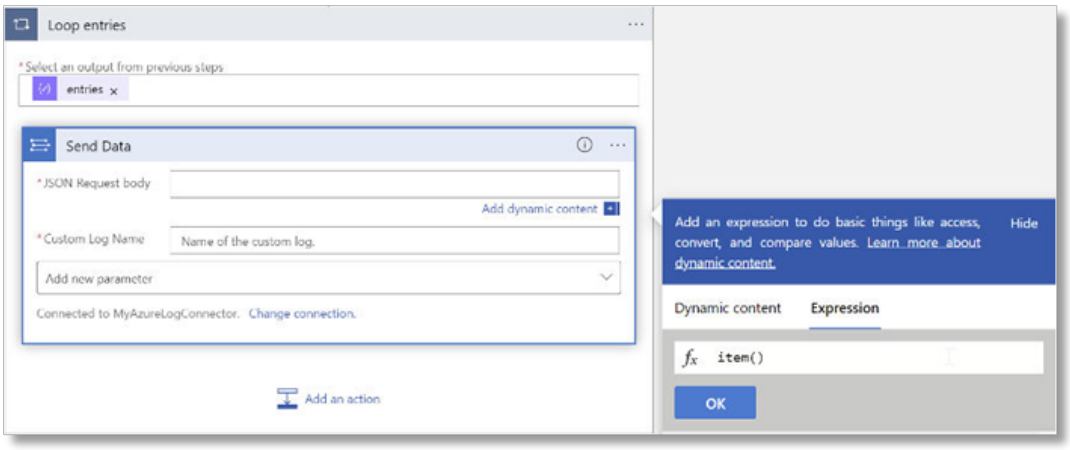
1. In order to send these to your Azure Log Analytics Workspace, do the following. Click on "Add an action" within the Loop entries action and search for "Azure Log Analytics". Click the Azure Log Analytics result.



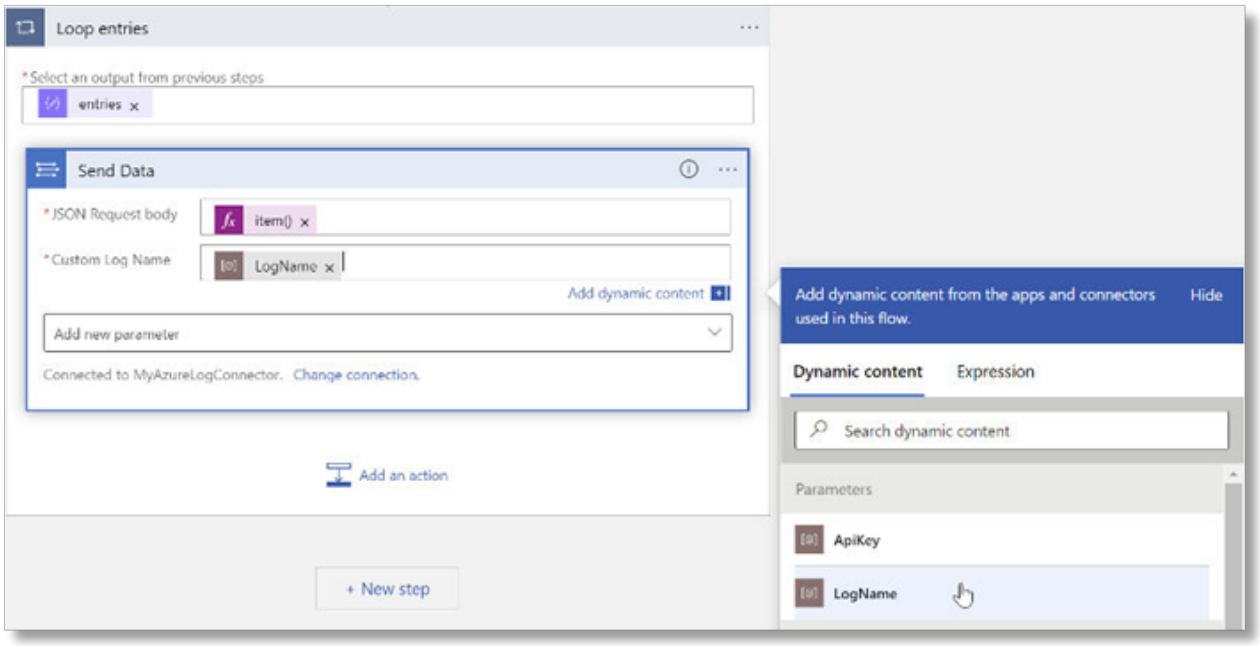
As in Configure Loop Entries in chapter Auditlog Data, you may also need to configure a data collector:



2. Select the 'Send Data' action



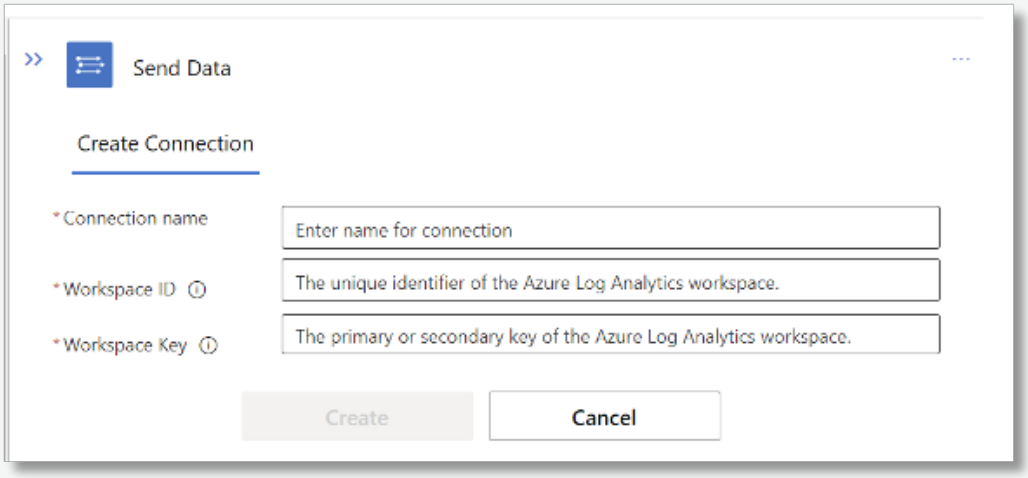
3. In the "JSON Request body", select the "Dynamic content" tab and select **Loop entries > Current item** (similar to Configure Loop Entries (step 3) in chapter Auditlog Data). This selects the current item in the JSON loop and adds it as the request body.



4. For the Custom Log Name, select the "LogName" parameter. This tells the Logic App to send the audit entries to a custom log with the name supplied in the parameter.

NOTE

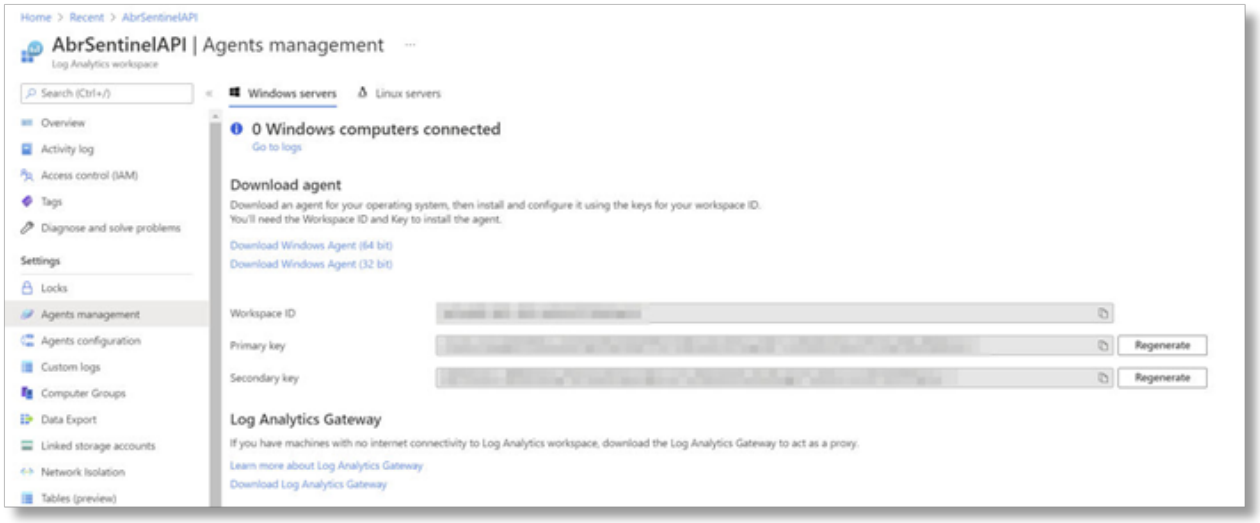
The previous steps assume that you already have an API Connection for your Azure Log Analytics Workspace set up. If this is not the case, you'll be met with the option to create a new connection:



5. Simply fill out the three fields and click "Create".

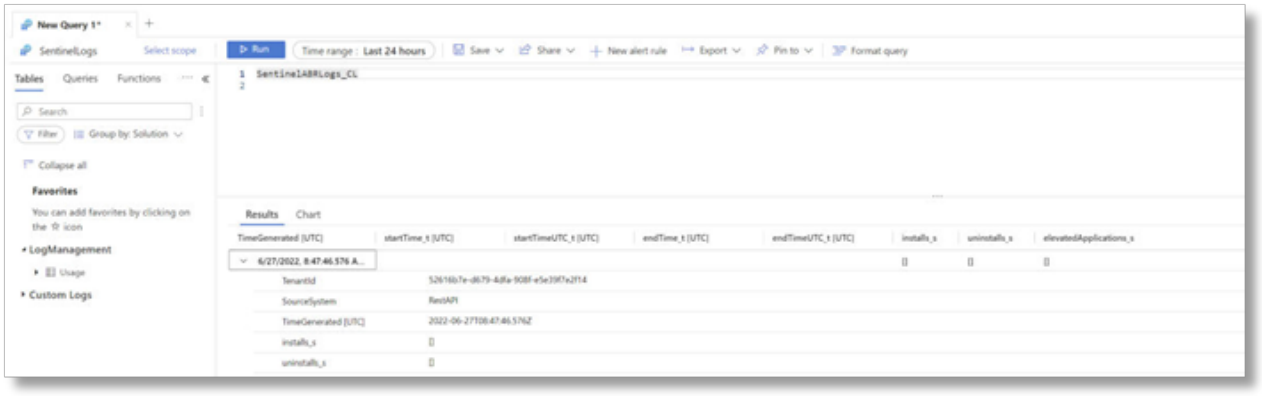
E. Locate Workspace & Run App

1. To find the Workspace ID and the Workspace Key, navigate to the Log Analytics workspace and select "Agents management":



2. Copy the workspace ID and Primary Key and paste these into the connection properties in your Logic App.

3. Now, save your app – and you're done. If you run the app now, you'll see your new entries showing up in your Log Analytics Workspace:



JSON Code – Auditlog Data

```
{
    "definition": {
        "$schema":
"https://schema.management.azure.com/providers/Microsoft.Logic/schemas/2016-06-
01/workflowdefinition.json#",
        "actions": {
            "Call_ABR_Sentinel_API": {
                "inputs": {
                    "body": {
                        "ApiKey": "@{parameters('ApiKey')}",
                        "Ticks": "@variables('deltaTime')"
                    },
                    "method": "POST",
                    "uri": "https://sentinel.adminbyrequest.com/Audit/SetDeltaTime"
                },
                "runAfter": {
                    "Initialize_deltaTime_variable": [
                        "Succeeded"
                    ]
                },
                "type": "Http"
            },
            "Call_the_ABR_Audit_API": {
                "inputs": {
                    "headers": {
                        "apikey": "@parameters('ApiKey')"
                    },
                    "method": "GET",
                    "uri":
"https://dc1api.adminbyrequest.com/auditlog/delta?deltaTime=@{variables
('newDeltaTime')}"
                },
                "runAfter": {
                    "Initialize_newDeltaTime_variable": [
                        "Succeeded"
                    ]
                },
                "type": "Http"
            },
            "Initialize_deltaTime_variable": {
                "inputs": {
                    "variables": [
                        {
                            "name": "deltaTime",
                            "type": "integer",
                            "value": "@ticks(utcNow())"
                        }
                    ]
                },
                "runAfter": {},
                "type": "InitializeVariable"
            },
            "Initialize_newDeltaTime_variable": {
                "inputs": {
```

```
                    "variables": [
                        {
                            "name": "newDeltaTime",
                            "type": "integer",
                            "value": "@body('Call_ABR_Sentinel_API')"
                        }
                    ]
                },
                "runAfter": {
                    "Call_ABR_Sentinel_API": [
                        "Succeeded"
                    ]
                },
                "type": "InitializeVariable"
            },
            "Loop_entries": {
                "actions": {},
                "foreach": "@body('Parse_JSON')?['entries']",
                "runAfter": {
                    "Parse_JSON": [
                        "Succeeded"
                    ]
                },
                "type": "Foreach"
            },
            "Parse_JSON": {
                "inputs": {
                    "content": "@body('Call_the_ABR_Audit_API')",
                    "schema": {
                        "properties": {
                            "entries": {
                                "items": {
                                    "properties": {
                                        "application": {
                                            "properties": {
                                                "file": {
                                                    "type": [
                                                        "string",
                                                        "null"
                                                    ]
                                                },
                                                "name": {
                                                    "type": [
                                                        "string",
                                                        "null"
                                                    ]
                                                },
                                                "path": {
                                                    "type": [
                                                        "string",
                                                        "null"
                                                    ]
                                                },
                                                "preapproved": {
                                                    "type": "boolean"
                                                },
                                                "scanResult": {
                                                    "type": [
```

```
                                        "string",
                                        "null"
                                    ]
                                },
                                "scanResultCode": {
                                    "type": "integer"
                                },
                                "sha256": {
                                    "type": [
                                        "string",
                                        "null"
                                    ]
                                },
                                "threat": {},
                                "vendor": {
                                    "type": [
                                        "string",
                                        "null"
                                    ]
                                },
                                "version": {
                                    "type": [
                                        "string",
                                        "null"
                                    ]
                                },
                                "virustotalLink": {
                                    "type": [
                                        "string",
                                        "null"
                                    ]
                                }
                            },
                            "type": "object"
                        },
                        "approvedBy": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "auditlogLink": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "computer": {
                            "properties": {
                                "make": {
                                    "type": [
                                        "string",
                                        "null"
                                    ]
                                },
                                "model": {
                                    "type": [
                                        "string",
```

```
                                        "null"
                                    ]
                                },
                                "name": {
                                    "type": [
                                        "string",
                                        "null"
                                    ]
                                },
                                "platform": {
                                    "type": [
                                        "string",
                                        "null"
                                    ]
                                },
                                "platformCode": {
                                    "type": "integer"
                                }
                            },
                            "type": "object"
                        },
                        "deniedBy": {},
                        "deniedReason": {},
                        "elevatedApplications": {
                            "items": {
                                "properties": {
                                    "file": {
                                        "type": [
                                            "string",
                                            "null"
                                        ]
                                    },
                                    "name": {
                                        "type": [
                                            "string",
                                            "null"
                                        ]
                                    },
                                    "path": {
                                        "type": [
                                            "string",
                                            "null"
                                        ]
                                    },
                                    "scanResult": {
                                        "type": [
                                            "string",
                                            "null"
                                        ]
                                    },
                                    "scanResultCode": {
                                        "type": "integer"
                                    },
                                    "sha256": {
                                        "type": [
                                            "string",
                                            "null"
                                        ]
```

```
                                    },
                                    "threat": {},
                                    "vendor": {
                                        "type": [
                                            "string",
                                            "null"
                                        ]
                                    },
                                    "version": {
                                        "type": [
                                            "string",
                                            "null"
                                        ]
                                    },
                                    "virustotalLink": {
                                        "type": [
                                            "string",
                                            "null"
                                        ]
                                    }
                                },
                                "required": [
                                    "name",
                                    "path",
                                    "file",
                                    "version",
                                    "vendor",
                                    "sha256",
                                    "scanResult",
                                    "scanResultCode",
                                    "threat",
                                    "virustotalLink"
                                ],
                                "type": "object"
                            },
                            "type": "array"
                        },
                        "endTime": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "endTimeUTC": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "id": {
                            "type": "integer"
                        },
                        "installs": {
                            "items": {
                                "properties": {
                                    "application": {
                                        "type": [
                                            "string",
```

```
                                        "null"
                                    ]
                                },
                                "vendor": {
                                    "type": [
                                        "string",
                                        "null"
                                    ]
                                },
                                "version": {
                                    "type": [
                                        "string",
                                        "null"
                                    ]
                                }
                            },
                            "required": [
                                "application",
                                "version",
                                "vendor"
                            ],
                            "type": "object"
                        },
                        "type": "array"
                    },
                    "reason": {
                        "type": [
                            "string",
                            "null"
                        ]
                    },
                    "requestTime": {
                        "type": [
                            "string",
                            "null"
                        ]
                    },
                    "requestTimeUTC": {
                        "type": [
                            "string",
                            "null"
                        ]
                    },
                    "responseTime": {
                        "type": [
                            "string",
                            "null"
                        ]
                    },
                    "scanResults": {
                        "items": {
                            "properties": {
                                "engine": {
                                    "type": [
                                        "string",
                                        "null"
                                    ]
                                },
```

```
                                    "scanResult": {
                                        "type": [
                                            "string",
                                            "null"
                                        ]
                                    },
                                    "scanResultCode": {
                                        "type": "integer"
                                    },
                                    "threat": {}
                                },
                                "required": [
                                    "scanResult",
                                    "scanResultCode",
                                    "engine",
                                    "threat"
                                ],
                                "type": "object"
                            },
                            "type": "array"
                        },
                        "settingsName": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "startTime": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "startTimeUTC": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "status": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "statusCode": {
                            "type": "integer"
                        },
                        "traceNo": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "type": {
                            "type": [
                                "string",
                                "null"
```

```
                    ]
                },
                "typeCode": {
                    "type": "integer"
                },
                "uninstalls": {
                    "items": {
                        "properties": {
                            "application": {
                                "type": [
                                    "string",
                                    "null"
                                ]
                            },
                            "vendor": {
                                "type": [
                                    "string",
                                    "null"
                                ]
                            },
                            "version": {
                                "type": [
                                    "string",
                                    "null"
                                ]
                            }
                        },
                        "required": [
                            "application",
                            "version",
                            "vendor"
                        ],
                        "type": "object"
                    },
                    "type": "array"
                },
                "user": {
                    "properties": {
                        "account": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "email": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "fullName": {
                            "type": [
                                "string",
                                "null"
                            ]
                        },
                        "phone": {
                            "type": [
```

```
                                                    "string",
                                                    "null"
                                                ]
                                            }
                                        },
                                        "type": "object"
                                    }
                                },
                                "required": [
                                    "id",
                                    "traceNo",
                                    "settingsName",
                                    "type",
                                    "typeCode",
                                    "status",
                                    "statusCode",
                                    "reason",
                                    "approvedBy",
                                    "deniedReason",
                                    "deniedBy",
                                    "requestTime",
                                    "requestTimeUTC",
                                    "startTime",
                                    "startTimeUTC",
                                    "endTime",
                                    "endTimeUTC",
                                    "responseTime",
                                    "auditlogLink",
                                    "user",
                                    "computer",
                                    "application",
                                    "installs",
                                    "uninstalls",
                                    "elevatedApplications",
                                    "scanResults"
                                ],
                                "type": "object"
                            },
                            "type": "array"
                        },
                        "timeNow": {
                            "type": "integer"
                        }
                    },
                    "type": "object"
                }
            },
            "runAfter": {
                "Call_the_ABR_Audit_API": [
                    "Succeeded"
                ]
            },
            "type": "ParseJson"
        }
    },
    "contentVersion": "1.0.0.0",
    "outputs": {},
    "parameters": {
```

```
            "ApiKey": {
                "defaultValue": "xxxxxx",
                "type": "String"
            },
            "LogName": {
                "defaultValue": "AdminByRequestLogs",
                "type": "String"
            }
        },
        "triggers": {
            "Recurrence": {
                "evaluatedRecurrence": {
                    "frequency": "Day",
                    "interval": 1,
                    "startTime": "2022-06-22T15:00:00Z"
                },
                "recurrence": {
                    "frequency": "Day",
                    "interval": 1,
                    "startTime": "2022-06-22T15:00:00Z"
                },
                "type": "Recurrence"
            }
        }
    },
    "parameters": {}
}
```

JSON Code – Events Data

```
{
    "definition": {
        "$schema":
"https://schema.management.azure.com/providers/Microsoft.Logic/schemas/2016-06-
01/workflowdefinition.json#",
        "actions": {
            "Call_ABR_Sentinel_API": {
                "inputs": {
                    "method": "GET",
                    "uri":
"https://sentinel.adminbyrequest.com/Events/GetEventStartId?apiKey=@{parameters
('ApiKey')}"
                },
                "runAfter": {},
                "type": "Http"
            },
            "Call_the_ABR_Audit_API": {
                "inputs": {
                    "headers": {
                        "apikey": "@parameters('ApiKey')"
                    },
                    "method": "GET",
                    "uri": "@{variables('apiEndpoint')}/events?startId=@{variables
('startEventId')}&take=10000"
                },
                "runAfter": {
                    "Initialize_apiEndpoint_variable": [
                        "Succeeded"
                    ]
                },
                "type": "Http"
            },
            "Get_latest_eventId": {
                "inputs": {
                    "headers": {
                        "apikey": "@parameters('ApiKey')"
                    },
                    "method": "GET",
                    "uri": "@{variables('apiEndpoint')}/events?last=1"
                },
                "runAfter": {
                    "Parse_JSON": [
                        "Succeeded"
                    ]
                },
                "type": "Http"
            },
            "Initialize_apiEndpoint_variable": {
                "inputs": {
                    "variables": [
                        {
                            "name": "apiEndpoint",
                            "type": "string",
                            "value": "@body('Parse_API_data')?['publicApiUrl']"
```

```
                        }
                    ]
                },
                "runAfter": {
                    "Initialize_startEventId_variable": [
                        "Succeeded"
                    ]
                },
                "type": "InitializeVariable"
            },
            "Initialize_latest_event_variable": {
                "inputs": {
                    "variables": [
                        {
                            "name": "latestEventId",
                            "type": "integer",
                            "value": "@body('Parse_Latest_Event_JSON')[0]['id']"
                        }
                    ]
                },
                "runAfter": {
                    "Parse_Latest_Event_JSON": [
                        "Succeeded"
                    ]
                },
                "type": "InitializeVariable"
            },
            "Initialize_startEventId_variable": {
                "inputs": {
                    "variables": [
                        {
                            "name": "startEventId",
                            "type": "integer",
                            "value": "@body('Parse_API_data')?['eventId']"
                        }
                    ]
                },
                "runAfter": {
                    "Parse_API_data": [
                        "Succeeded"
                    ]
                },
                "type": "InitializeVariable"
            },
            "Loop_entries": {
                "actions": {},
                "foreach": "@body('Parse_JSON')",
                "runAfter": {
                    "Set_latest_event_ID": [
                        "Succeeded"
                    ]
                },
                "type": "Foreach"
            },
            "Parse_API_data": {
                "inputs": {
                    "content": "@body('Call_ABR_Sentinel_API')",
                    "schema": {
```

```
                        "properties": {
                            "eventId": {
                                "type": "integer"
                            },
                            "publicApiUrl": {
                                "type": "string"
                            },
                            "success": {
                                "type": "boolean"
                            }
                        },
                        "type": "object"
                    }
                },
                "runAfter": {
                    "Call_ABR_Sentinel_API": [
                        "Succeeded"
                    ]
                },
                "type": "ParseJson"
            },
            "Parse_JSON": {
                "inputs": {
                    "content": "@body('Call_the_ABR_Audit_API')",
                    "schema": {
                        "items": {
                            "properties": {
                                "additionalData": {},
                                "alertAccount": {},
                                "application": {
                                    "properties": {
                                        "file": {},
                                        "name": {},
                                        "path": {},
                                        "sha256": {},
                                        "vendor": {},
                                        "version": {}
                                    },
                                    "type": "object"
                                },
                                "auditLogURL": {},
                                "computerName": {
                                    "type": "string"
                                },
                                "eventCode": {
                                    "type": "integer"
                                },
                                "eventLevel": {
                                    "type": "integer"
                                },
                                "eventText": {
                                    "type": "string"
                                },
                                "eventTime": {
                                    "type": "string"
                                },
                                "eventTimeUTC": {
                                    "type": "string"
```

```
                                },
                                "id": {
                                    "type": "integer"
                                },
                                "rollback": {
                                    "type": "boolean"
                                },
                                "userAccount": {},
                                "userName": {}
                            },
                            "required": [
                                "id",
                                "eventCode",
                                "eventLevel",
                                "eventText",
                                "eventTime",
                                "eventTimeUTC",
                                "computerName",
                                "userAccount",
                                "userName",
                                "alertAccount",
                                "auditLogURL",
                                "rollback",
                                "additionalData",
                                "application"
                            ],
                            "type": "object"
                        },
                        "type": "array"
                    }
                },
                "runAfter": {
                    "Call_the_ABR_Audit_API": [
                        "Succeeded"
                    ]
                },
                "type": "ParseJson"
            },
            "Parse_Latest_Event_JSON": {
                "inputs": {
                    "content": "@body('Get_latest_eventId')",
                    "schema": {
                        "items": {
                            "properties": {
                                "additionalData": {},
                                "alertAccount": {},
                                "application": {
                                    "properties": {
                                        "file": {},
                                        "name": {},
                                        "path": {},
                                        "sha256": {},
                                        "vendor": {},
                                        "version": {}
                                    },
                                    "type": "object"
                                },
                                "auditLogURL": {},
```

```
                                "computerName": {
                                    "type": "string"
                                },
                                "eventCode": {
                                    "type": "integer"
                                },
                                "eventLevel": {
                                    "type": "integer"
                                },
                                "eventText": {
                                    "type": "string"
                                },
                                "eventTime": {
                                    "type": "string"
                                },
                                "eventTimeUTC": {
                                    "type": "string"
                                },
                                "id": {
                                    "type": "integer"
                                },
                                "rollback": {
                                    "type": "boolean"
                                },
                                "userAccount": {
                                    "type": "string"
                                },
                                "userName": {}
                            },
                            "required": [
                                "id",
                                "eventCode",
                                "eventLevel",
                                "eventText",
                                "eventTime",
                                "eventTimeUTC",
                                "computerName",
                                "userAccount",
                                "userName",
                                "alertAccount",
                                "auditLogURL",
                                "rollback",
                                "additionalData",
                                "application"
                            ],
                            "type": "object"
                        },
                        "type": "array"
                    }
                },
                "runAfter": {
                    "Get_latest_eventId": [
                        "Succeeded"
                    ]
                },
                "type": "ParseJson"
            },
            "Set_latest_event_ID": {
```

```
                "inputs": {
                    "body": {
                        "ApiKey": "@parameters('ApiKey')",
                        "EventStartId": "@variables('latestEventId')"
                    },
                    "method": "POST",
                    "uri":
"https://sentinel.adminbyrequest.com/Events/SetEventStartId"
                },
                "runAfter": {
                    "Initialize_latest_event_variable": [
                        "Succeeded"
                    ]
                },
                "type": "Http"
            }
        },
        "contentVersion": "1.0.0.0",
        "outputs": {},
        "parameters": {
            "ApiKey": {
                "defaultValue": "xxx",
                "type": "String"
            },
            "LogName": {
                "defaultValue": "SentinelTest",
                "type": "String"
            }
        },
        "triggers": {
            "Recurrence": {
                "evaluatedRecurrence": {
                    "frequency": "Day",
                    "interval": 1,
                    "startTime": "2022-06-22T15:00:00Z"
                },
                "recurrence": {
                    "frequency": "Day",
                    "interval": 1,
                    "startTime": "2022-06-22T15:00:00Z"
                },
                "type": "Recurrence"
            }
        }
    },
    "parameters": {}
}
```

Document History

Version	Author	Changes
1.0 9 February 2023	Sophie Alice Dodson	Initial document release.
2.0 6 January 2025	Steve Dodson	Updated manual structure and layout. Updated procedures to improve clarity and reflect changes to Sentinel look and feel by Microsoft.
2.1 13 January 2025	Steve Dodson	Updated links. Added a second method for determining data center domain/API prefix in chapter "Auditlog Data".
2.2 14 February 2025	Steve Dodson	Corrected typos and a missing link. Clarified step 3 of *Task F. Configure Loop Entries* in chapter "Auditlog Data", including adding a new screenshot.

Index