# Log Forwarding Destinations / SIEMs

# AWS S3 Bucket

Multicloud Defense supports forwarding Security Events and Traffic Logs to an AWS S3 Bucket to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi- structured JSON format where the attribute-value pairs can be accessed and processed.

### Requirements

In order to forward Events/Logs to the AWS S3 Bucket, the following is required:

1. Create a new or use an existing AWS S3 Bucket.

2. Apply the following policy to the AWS S3 Bucket to permit the Multicloud Defense Controller to access and write to the bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "<controller-role-arn>"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::<s3bucketname>/*",
        "arn:aws:s3:::<s3bucketname>"
      ]
    }
```

```
        ]
    }
```

**Profile Parameters**

| Parameter | Requirement | Default | Description |
|---|---|---|---|
| Profile Name | Required | | A unique name to use to reference the Profile. |
| Description | Optional | | A description for the Profile. |
| Destination | Required | AWS S3 | AWS S3 Bucket. |
| CSP Account | Required | | The CSP Account where the AWS S3 Bucket resides. |
| S3 Bucket | Required | | The AWS S3 Bucket name where Events/Logs will be forwarded. |

# Datadog

Datadog is a very common and powerful SIEM that is used by many companies. Multicloud Defense supports Log Forwarding to Datadog to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi-structured JSON format where the attribute-value pairs can be accessed and processed.

### Requirements

In order to forward logs to Datadog, the following information is required:

- Datadog account

- Endpoint URL

- API Key

**Tip**
- To Sign up for a Datadog account, refer to **Datadog Account** (https://www.datadoghq.com/).

- To create a Datadog API Key, refer to **Datadog API Key** (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api).

**Profile Parameters**

| Parameter | Requirement | Default | Description |
|---|---|---|---|
| Profile Name | Required | | A unique name to use to reference the Profile. |
| Description | Optional | | A description for the Profile. |
| Destination | Required | Datadog | The SIEM used for the Profile. |
| Skip Verify Certificate | Optional | Unchecked | Whether to skip verifying the authenticity of the certificate. |
| API Key | Required | | The Datadog API Key to authenticate the communication. |
| Endpoint | Required | https://http-intake.logs.datadoghq.com/ | The URL endpoint used to receive the forwarded Events/Logs. |

# GCP Logging

GCP Stackdriver Logging is a service offer by Google Cloud Provider (GCP) for collecting and storing logs from applications and services. Multicloud Defense supports Log Forwarding to GCP Stackdriver Logging to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi- structured JSON format where the attribute-value pairs can be accessed and processed.

### Requirements

The GCP *multicloud defense-firewall* Service Account must be assigned **Logs Writer** role in order for the Gateway to write events to the GCP Stackdriver Log.

### Profile Parameters

| Parameter | Requirement | Default | Description |
|---|---|---|---|
| Profile Name | Required | | A unique name to use to reference the Profile. |
| Description | Optional | | A description for the Profile. |
| Destination | Required | GCP Logging (From Gateway) | The SIEM used for the Profile. |

| Parameter | Requirement | Default | Description |
|---|---|---|---|
| Log Name | Required | ciscomcd -gateway-logs | The name of the Stackdriver Log used to store events. |

### Field Integer to String Mappings

When events are forwarded from the Controller, the Controller introduces mappings of event field values to friendly names. When events are forwarded directly from the Gateway (e.g., GCP Logging), the Controller is not involved and thus the event field values are not mapped to friendly names. In order to interpret these fields, the user is responsible for performing the field value to friendly name mapping.

The fields, sub-fields and their value to friendly mapping are provided below:

| Field | Integer | String |
|---|---|---|
| **action** | 0 | DUMMY_ACTION |
| | 1 | ALLOW |
| | 2 | DENY |
| | 3 | DROP |
| | 4 | REDIRECT |
| | 5 | PROXY |
| | 6 | LOG |
| | 7 | OTHER |
| | 8 | DELAY |
| | 9 | DETECT_SIG |

| Field | Integer | String |
|---|---|---|
| **gatewaySecurityType** | 1 | INGRESS_FIREWALL |
| | 2 | EAST_WEST_AND_EGRESS_FIREWALL |

| Field | Integer | String |
|---|---|---|
| **level** | 1 | DEBUG |
| | 2 | INFO |
| | 3 | NOTICE |
| | 4 | WARNING |
| | 5 | ERROR |
| | 6 | CRITICAL |
| | 7 | ALERT |
| | 8 | EMERGENCY |

| Field | Integer | String |
|---|---|---|
| **policyMatchInfo.serviceType** | 0 | UNKNOWN |
| | 1 | PROXY |
| | 2 | FORWARDING |
| | 3 | REVERSE_PROXY |
| | 4 | FORWARD_PROXY |

| Field | Integer | String |
|---|---|---|
| **protocol** | 0 | DUMMY |
| **sessionSummaryInfo.egressConnection.protocol** | 1 | ICMP |
| **sessionSummaryInfo.ingressConnect.protocol** | 6 | TCP |
| | 17 | UDP |
| | 252 | HTTP |

| Field | Integer | String |
|---|---|---|
| **rule.type** | 0 | DUMMY_RULE_TYPE |
| | 1 | THIRD_PARTY |
| | 2 | USER_DEFINED |

| Field | Integer | String |
|---|---|---|
| **statusText** <br> **ingressConnectionStates.state** | 0 | CLOSED |
| | 1 | SYN_SENT |
| | 2 | SYN_RECV |
| | 3 | ESTABLISHED |
| | 4 | FIN_WAIT |
| | 5 | CLOSE_WAIT |
| | 6 | LAST_ACK |
| | 7 | TIME_WAIT |
| | 8 | CLOSE |

| Field | Integer | String |
|---|---|---|
| **type** | 1 | WAF |
| | 2 | DPI |
| | 3 | HTTP_REQUEST |
| | 4 | L4_FW |
| | 5 | FLOW_LOG |
| | 6 | MALICIOUS_IP |
| | 7 | TLS_ERROR |
| | 8 | TLS_LOG |
| | 9 | L7DOS |
| | 10 | SNI |
| | 11 | APPID |
| | 12 | URLFILTER |
| | 13 | SESSION_SUMMARY |
| | 14 | DLP |
| | 15 | FQDNFILTER |
| | 16 | AV |

# Microsoft Sentinel

Microsoft Sentinel is a powerful SIEM that is used by many companies. Multicloud Defense supports Log Forwarding to Microsoft Sentinel to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi-structured JSON format where the attribute-value pairs can be accessed and processed.

### Requirements

In order to forward logs to Microsoft Sentinel, the following information is required:

- Create an Azure Log Analytics Workspace.

- Define an Azure Log Table.

### Profile Parameters

| Parameter | Requirement | Default | Description |
|---|---|---|---|
| Profile Name | Required | | A unique name to use to reference the Profile. |
| Description | Optional | | A description for the Profile. |
| Destination | Required | Microsoft Sentinel | The SIEM used for the Profile. |
| Azure Log Analytics Workspace ID | Required | | The ID of the Azure Log Analytics Workspace. |
| Shared Key | Required | | The Shared Key used to authenticate the communication. |
| Azure Log Table Name | Required | | Name of the Azure Log Table where the logs/events will be stored. |

# Splunk

Splunk is a very common and powerful SIEM that is used by many companies. Multicloud Defense supports Log Forwarding to Splunk to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi-structured JSON format where the attribute-value pairs can be accessed and processed.

### Requirements

In order to forward logs to Splunk, the following information is required:

- Splunk account

- Splunk Collector URL

- Event Collector Key

- Index Name

🔍

**Tip** For information on the Splunk Event Collector, refer to **Splunk HTTP Event Collector** (https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/UsetheHTTPEventCollector).

**Profile Parameters**

| Parameter | Requirement | Default | Description |
|---|---|---|---|
| Profile Name | Required | | A unique name to use to reference the Profile. |
| Description | Optional | | A description for the Profile. |
| Destination | Required | Datadog | The SIEM used for the Profile. |
| Skip Verify Certificate | Optional | Unchecked | Whether to skip verifying the authenticity of the certificate. |
| Endpoint | Required | | The URL used to access the HTTP Event Collector. |
| Token | Required | | The Splunk Token to allow Multicloud Defense to communicate with Splunk. |
| Index | Required | main | The name of the Splunk index used to store events. |

# Sumo Logic

Sumo Logic is a very common and powerful SIEM that is used by many companies. Multicloud Defense supports Log Forwarding to Sumo Logic to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi-structured JSON format where the attribute-value pairs can be accessed and processed.

**Requirements**

In order to forward logs to Sumo Logic, the following information is required:

- Sumo Logic account

- Sumo Logic collector endpoint

**Tip** For information on how to setup Sumo Logic Collector, refer to **Sumo Logic Setup Guide** (https://help.sumologic.com/docs/send-data/setup-wizard/).

**Profile Parameters**

| Parameter | Requirement | Default | Description |
| --- | --- | --- | --- |
| Profile Name | Required | | A unique name to use to reference the Profile |
| Description | Optional | | A description for the Profile |
| Destination | Required | Sumo Logic | The SIEM used for the Profile |
| Endpoint | Required | | The URL endpoint used to receive the forwarded Events/Logs |

# Syslogs

A syslog server is a common log collector that accepts a standard formatted syslog message. Each syslog message contains fields for facility, severity and message. Almost any SIEM can accept syslog formatted messages, although most SIEMs support other message formats. Multicloud Defense supports sending security events and traffic logs to a syslog server. The following are a list of events and logs that are forwarded:

- Flow Logs (Traffic Summary)

- Firewall Events (AppID, L4FW, GeoIP, MaliciousIP, SNI)

- HTTPS Logs (HTTP, TLS)

- Network Threats (AV, DLP, IDS/IPS)

- Web Protection (WAF, L7 DoS)

At this time this list of included events and logs is mandatory and cannot be altered. If you configure syslogs to be forwarded then **all** of these logs are included in the report.

**Note** Flow logs are deprecated in gateway version 2.10 and later releases. The information contained within each flow log is made available as part of the session information available in **Traffic Summary** > **Logs**.

Events can be forwarded to a syslog server using a log forwarding profile. Once created, the profile needs to be associated with a new or existing gateway in order for the events to be sent to the syslog Server. To create, modify or change the gateway association of a log forwarding profile, refer to Log Forwarding - Security Events and Traffic Logs.

**Profile Parameters**

| Parameter | Requirement | Default | Description |
|---|---|---|---|
| Profile Name | Required | | A unique name to use to reference the Profile. |
| Description | Optional | | A description for the Profile. |
| SIEM Vendor | Required | Syslog | The SIEM used for the profile. |
| Server IP | Required | | The IP address of the syslog server. |
| Protocol | Required | UDP | The protocol to use when sending messages (TCP / UDP). |
| Port | Required | | The port to use when sending messages. |
| Format | Required | IETF | The format of the messages (only IETF is supported). |
| Flow Logs | Required | No | Whether to send flow logs (Yes / No). |
| Firewall Events | Required | No | Whether to send firewall events (Yes / No). |
| HTTPS Logs | Required | No | Whether to send HTTPS logs (Yes / No). |
| Network Threats | Required | Emergency | The lowest severity level to send network threats. |
| Web Attacks | Required | Emergency | The lowest severity level to send web attacks. |

**Note** The following levels of severity (highest to lowest) are available:

- Emergency

- Alert

- Criticial

- Error

- Warning

- Notice

- Info

- Debug

All events for the category that contain the severity level specified or higher will be sent to the syslog server.

# Webhook

Logging forward with a webhook can be a useful practice in various scenarios, particularly when you need to integrate different systems or services in real-time. Webhooks can enable real-time data transfer, are ideal for an event-driven architecture or centralized logging, as well as support automation and integration with other third-party services. Customize the log forwarding profile to support your specific environment.

### Requirements

If you are forwarding logs to a service that requires an authetnication token or password, have that configured and readily available when creating this profile.

### Profile Parameters

| Parameter | Requirement | Default | Description |
|---|---|---|---|
| Profile Name | Required | | A unique name to use to reference the Profile. |
| Description | Optional | | A description for the Profile. |
| Type | Required | | Select **Standalone**. |
| Destination | Required | Webhook | |
| Endpoint | Required | | Enter the URL for the webhook. |
| Message Field Name | Required | | This value is defines the structure and meaning of the data being transmitted. |
| Batch size | Required | 100 | This value determines the number of log entries that are grouped together and sent in a single transmission. |

| Parameter | Requirement | Default | Description |
|---|---|---|---|
| Authentication Type | Required | | Select **Basic** for username and password or **Bearer token**. |