TECHNICAL
DOCUMENTATION

Illumio Sentinel Solution 3.4.0

Integration Guide

Table of Contents

Legal Notice

The content in this documentation is provided for informational purposes only and is provided "as is," without warranty of any kind, expressed or implied, of Illumio. The content in this documentation is subject to change without notice.

Resources

- Legal information
- Trademarks statements
- Patent statements
- License statements

Contact Information

- Contact Illumio
- Contact Illumio Legal
- Contact Illumio Documentation

What's New in the Illumio Sentinel Solution

Version	Release Date	Release Notes
3.4.0	February 4, 2025	Provides Illumio On-Premises PCE support for the Illumio Sentinel Solution and information about how to troubleshoot it.
3.3.0	December 17, 2024	Provides the Quarantine Workloads playbook and information about deploying the common function app.
3.2.3	December 3, 2024	Provides the following playbooks: • Containment Switch • Get VEN Details
3.2.2	October 31, 2024	• Provides three ASIM Parsers: Audit Parser, Network Session Parser, and Authentication Parser • Provides six Analytics Rules: Illumio VEN Deactivated Detection Rule, Illumio Firewall Tampering Analytic Rule, Illumio VEN Clone Detection Rule, Illumio Enforcement Change Analytic Rule, Illumio VEN Offline Detection Rule, and Illumio VEN Suspend Detection Rule • Enhancement to the function app: You can select the type of network traffic to be ingested. The types are blocked, allowed, potentially blocked, and unknown.
3.1.0	August 2, 2024	• Supports Core PCE SaaS • Azure Function Apps for data ingestion. Ingests audit events and traffic flow logs from Illumio PCE. • Provides three workbooks: Auditable Events, Traffic Flow, and Workload and Agent Status

Introduction to the Illumio Sentinel Solution

Microsoft Sentinel is a scalable, cloud-native security information and event management (SIEM) that delivers a comprehensive solution for SIEM and security orchestration, automation, and response (SOAR). Microsoft Sentinel provides cyberthreat detection, investigation, and response capabilities and also natively provides Azure services such as Log Analytics and Logic Apps.

The Illumio Sentinel Solution provides the integration between Microsoft Sentinel and Illumio's Zero Trust Segmentation platform and provides the following key benefits:

- Enhanced SecOps Security
- Greater visibility into workloads
- Faster response to incidents
- Strengthened compliance

Illumio Sentinel Solution includes a data connector that pulls audit events and traffic flow logs into Sentinel. Within Sentinel, the Illumio solution contains three new Sentinel workbooks: Auditable Events Workbook, Flow Data Workbook, and Workload Stats Workbook. These new workbooks allow network and security teams to centralize security, as well as work with enriched data for troubleshooting and use this data to meet their audit and compliance needs. This solution is now available on the Microsoft Azure Marketplace and Sentinel Content Hub.

Prerequisites for the Illumio Sentinel Solution

These are the prerequisites for installing and using the Illumio Sentinel Solution.

1. An AWS S3 Bucket and SQS
   - If Illumio provides an S3 bucket, contact Illumio for AWS credentials and the SQS URL.
   - Configure an AWS SQS for the S3 bucket, which is set up to receive events from PCE. If you provide the S3 bucket, you must deploy it with the following CloudFormation template: Use the AWS CloudFormation Template [7]. For more information about configuring S3 buckets, see Configuring a bucket for notifications.
   - Ensure that you have AWS credentials and an SQS URL.
2. Configure PCE Events to forward them to the S3 bucket.
   - For On-Premises PCE, configure using the UI: Syslog Forwarding.
   - For SaaS users, open a ticket with Illumio Support to configure Event forwarding.

   Contact Illumio to get the PCE API username and secret, PCE FQDN, and org ID or access the PCE UI and generate an API key.
3. Obtain the PCE FQDN, org ID, API username, and Client Secret.
4. A resource group to host all Azure objects. See Use the Azure portal and Azure Resource Manager to manage resource groups.
5. A Log Analytics workspace. See Create a Log Analytics workspace.

   Define a Log Analytics workspace in Azure and deploy Sentinel in that workspace.
6. A Microsoft Entra application

   Define an AAD application to authenticate the Logs Ingestion API. See Create a Microsoft Entra application for information about how to deploy an AAD application.
7. Privileges to create all the resources. See Microsoft Entra built-in roles. Users who deploy this solution in Azure either need to have owner rights or to be contributors with the Role-Based Access Control Administrator and Application Developer roles for Microsoft Entra.

Use the AWS CloudFormation Template

Use the following AWS CloudFormation template to set up the AWS S3 bucket objects.

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Flow log bucket",
  "Parameters": {
    "Bucketname": {
      "Type": "String"
    },
    "Externalid": {
      "Type": "String",
      "Default": "528298"
    }
  },
  "Resources": {
    "FlowbucketAwsS3Bucket": {
      "Type": "AWS::S3::Bucket",
      "Properties": {
        "BucketName": {
          "Ref": "Bucketname"
        }
      }
    },
    "IllumioFlowLogsAwsIamRole": {
      "Type": "AWS::IAM::Role",
      "Properties": {
        "RoleName": "illumio-flow-logs",
        "AssumeRolePolicyDocument": {
          "Version": "2012-10-17",
          "Statement": {
            "Effect": "Allow",
            "Principal": {
              "AWS": "857003445768"
            },
            "Action": [
              "sts:AssumeRole"
            ],
            "Condition": {
              "StringEquals": {
                "Sts:ExternalId": {
                  "Ref": "Externalid"
                }
              }
            }
          }
        },
        "Policies": [
          {
            "PolicyName": "can-see-bucket",
            "PolicyDocument": {
              "Version": "2012-10-17",
              "Statement": {
                "Effect": "Allow",
                "Sid": "illumioCanSeeBucket",
                "Action": [
                  "s3:ListBucket",
                  "s3:ListBucketVersions"
                ],
                "Resource": {
                  "Fn::Join": [
                    "",
                    [
                      "arn:aws:s3:::",
                      {
                        "Ref": "Bucketname"
                      }
                    ]
                  ]
                }
              }
            }
          },
          {
            "PolicyName": "can-use-bucket",
            "PolicyDocument": {
              "Version": "2012-10-17",
              "Statement": {
                "Effect": "Allow",
                "Sid": "illumioCanPutAndGet",
                "Action": [
                  "s3:PutObject",
                  "s3:GetObject"
                ],
                "Resource": {
                  "Fn::Join": [
                    "",
                    [
                      "arn:aws:s3:::",
                      {
                        "Ref": "Bucketname"
                      },
                      "/*"
                    ]
                  ]
                }
              }
            }
          }
        ]
      }
    }
  }
}
```

Use the following procedure:

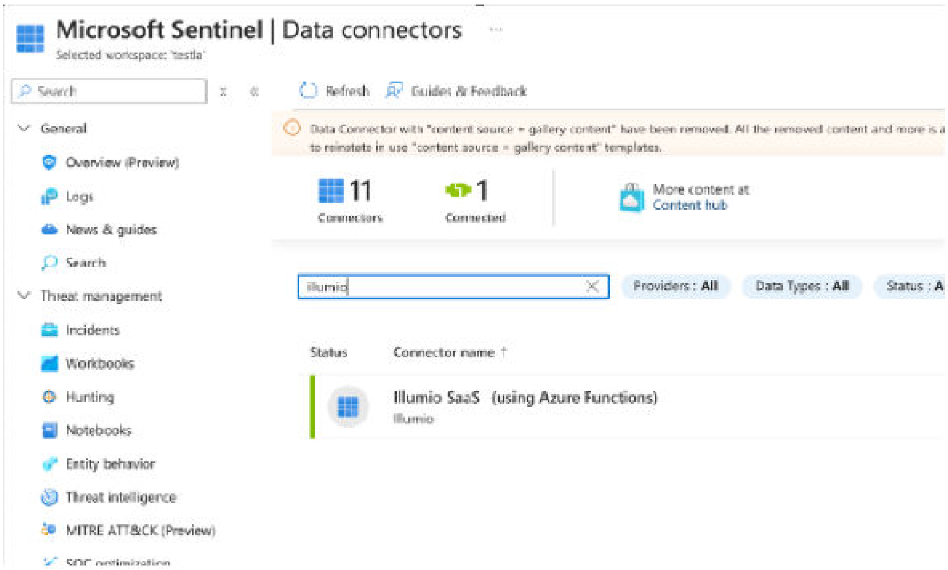
1. Save the template to a .JSON file, such as illumio-flow-logs-template.json
2. From the **AWS Console** > **CloudFormation Services** page, select **Stacks**, and note the current region because the AWS S3 bucket will be created in that region.
3. Select **Create Stack** and then select **With new resources (standard)**.
4. Select template is ready, upload the .JSON file that you created, and click **Next**.
5. Enter a name for the stack, such as illumio-flow-logs-s3-bucket-and-role.
6. Enter a bucket name. This name must be unique among all of the other S3 buckets in that region for all AWS customers. If it is not, the stack creation will fail with the "Bucketname already exists" error message.
7. Enter an external ID. See the following article for information about how and why to use an external ID: How to Use External ID When Granting Access to Your AWS Resources.
8. Keep the default options for **Configure stack options**, and click **Next**.
9. Review your configuration, check the acknowledgment, and click **Submit**.

   The bucket will be created along with a role called illumio-flow-logs with the appropriate permissions for the provided Illumio AWS account. You must also create a role for your SIEM to read objects from the bucket.

Install the Illumio Sentinel Solution

Here are the steps to install the solution from the content hub in Microsoft Sentinel.

1. Go to **MS Sentinel** > **Content Hub**, search for Illumio SaaS, and select **Install**.
2. On the **Create Illumio Sentinel Solution** screen, select the resource group and workspace where the solution will be deployed.
3. Select the **Data Connectors** or **Workbooks** tab to see a summary of this solution's features.
4. Click **Review+Create** and then click **Create** to deploy the resources.
5. Navigate to the **Data Connectors** tab.



Data Connector with "content source = gallery content" have been removed. All the removed content and more is a
to reinstate in use "content source = gallery content" templates.

illumio

Status	Connector name ↑
	Illumio SaaS (using Azure Functions) Illumio

Data Connectors

6. The Solutions Landing page displays what the solution provides:
   - Prerequisites
   - Deployment modes of data connectors
   - Information about specific tables that are created

Deploy the Illumio Sentinel Solution

The following topics describe how to deploy the Illumio Sentinel Solution:

- How to ARM to create objects to ingest the data
- The Custom tabs that you need to enter information in
- How to provide permissions to the data collection rule
- How to provision the Sentinel workbooks

Logs Ingestion API

You can create objects using the ARM templates to ingest the data into the Illumio Sentinel Solution.

Create the following objects:

1. Data Collection Rule
2. Data Collection Endpoint
3. Custom Tables
4. Function App
5. Storage account

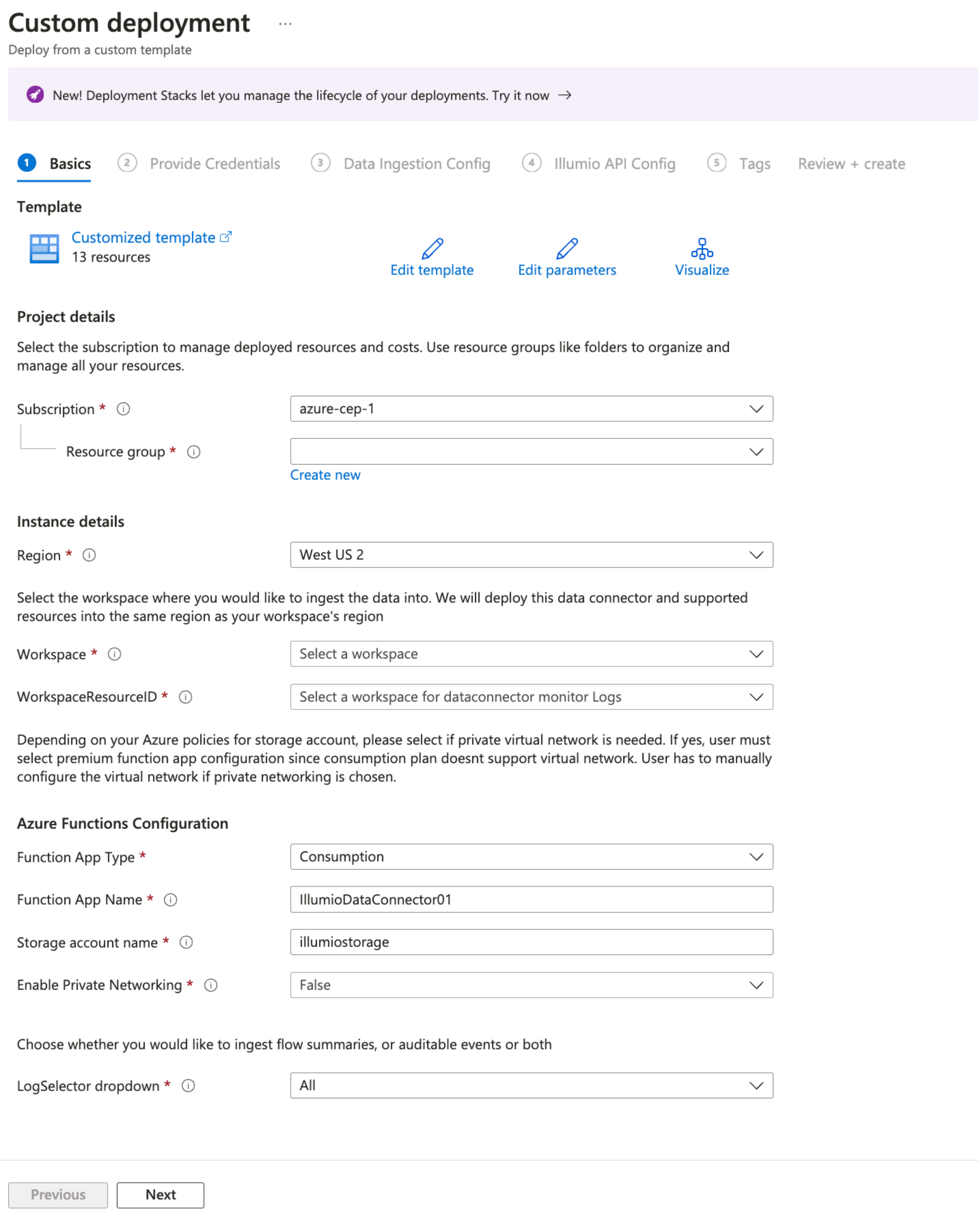
Here is a link to the template for creating DCR, DCE, custom tables, and function app definitions: Data Connectors.

Tabs for Custom Deployment

The following sections describe the tabs you will work with when creating a custom deployment.

Basics Tab

The **Basics** tab is the first tab within Custom deployment that you need to enter information into.



Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Template

Customized template
13 resources

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-cep-1
Resource group *	

Instance details

Region *	West US 2

Select the workspace where you would like to ingest the data into. We will deploy this data connector and supported resources into the same region as your workspace's region

Workspace *	Select a workspace
WorkspaceResourceID *	Select a workspace for dataconnector monitor Logs

Depending on your Azure policies for storage account, please select if private virtual network is needed. If yes, user must select premium function app configuration since consumption plan doesnt support virtual network. User has to manually configure the virtual network if private networking is chosen.

Azure Functions Configuration

Function App Type *	Consumption
Function App Name *	IllumioDataConnector01
Storage account name *	illumiostorage
Enable Private Networking *	False

Choose whether you would like to ingest flow summaries, or auditable events or both

LogSelector dropdown *	All

Basics Tab

Select or type in the following information:

1. Enter the Resource group.
2. Enter the Log Analytics Workspace.
3. Select the type of function app, which will be either "consumption" or "premium" depending upon event security and Azure policies.

4. Enter the name of the function app. By default, it is set to "IllumioDataConnector01".
5. Enter the name of the storage account. By default, it is set to "illumiostorage".

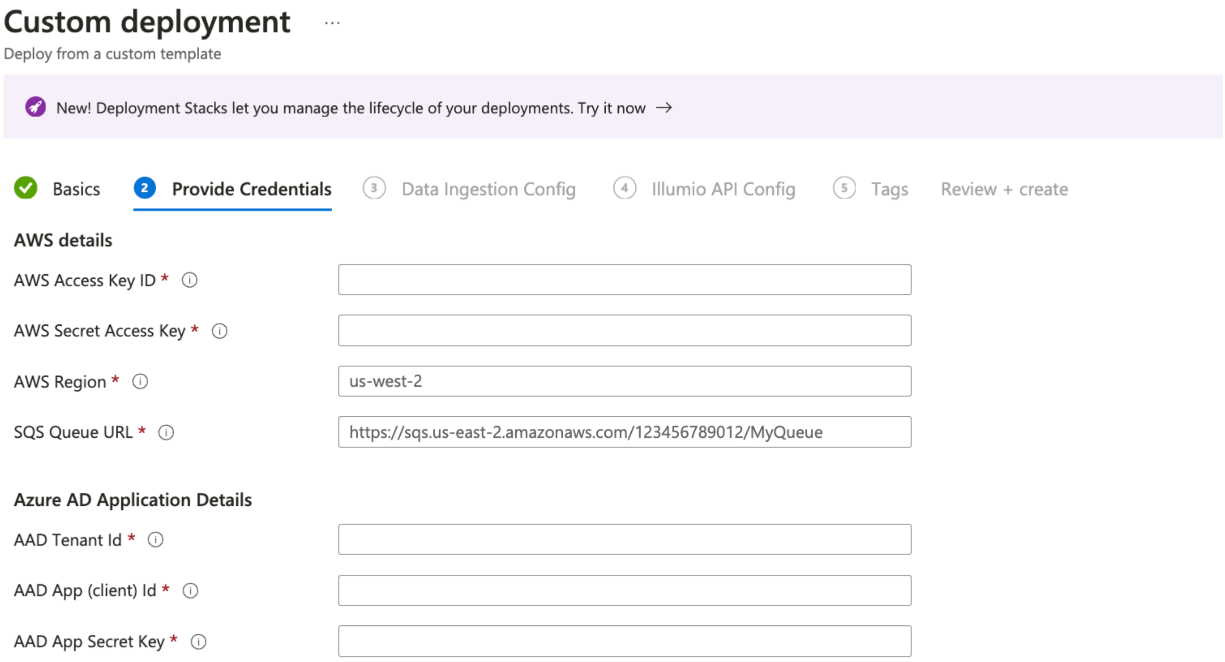
Private networking is set to `false` by default. See Configure a Private Network [24] for more information.

By default, all types of logs are ingested. This includes audit and flow events.

After you have provided the required information, click Next.

Provide Credentials Tab

The **Provide Credentials** tab is the second tab within Custom deployment that you need to add information into:



Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

AWS details

AWS Access Key ID *

AWS Secret Access Key *

AWS Region * us-west-2

SQS Queue URL * https://sqs.us-east-2.amazonaws.com/123456789012/MyQueue

Azure AD Application Details

AAD Tenant Id *

AAD App (client) Id *

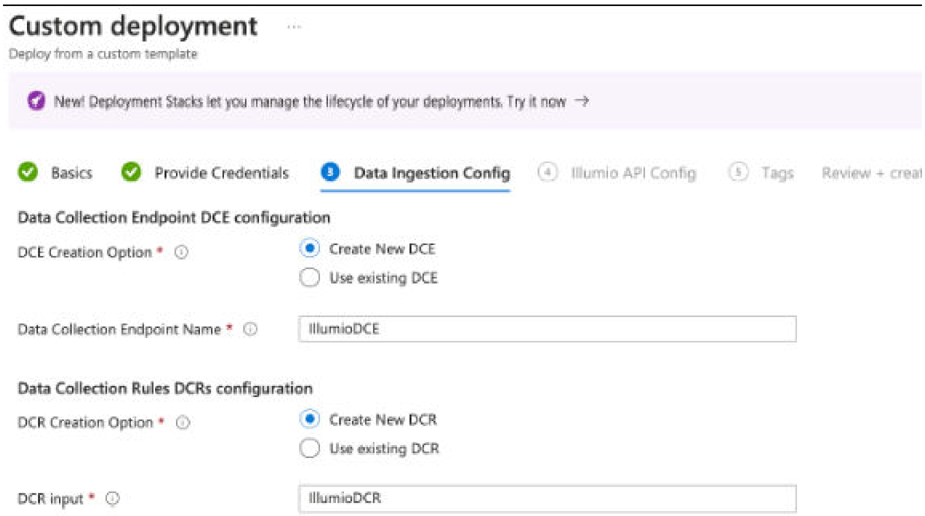
AAD App Secret Key *

Select or type in the following information:

1. Enter the AWS credentials, such as the access key, the secret, the region, and the SQS queue URL. If this is an Illumio-provided bucket, reach out to Illumio for details.
2. Provide the AAD Tenant Id, Client ID, and Secret Key. As mentioned in Prerequisites for the Illumio Sentinel Solution [7], this information must have been set up before you can complete these steps.

Data Ingestion Config Tab

The **Data Ingestion Config** tab is the third tab in Custom deployment that you need to enter information into:



Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Data Collection Endpoint DCE configuration

DCE Creation Option * ● Create New DCE ○ Use existing DCE

Data Collection Endpoint Name * IllumioDCE

Data Collection Rules DCRs configuration

DCR Creation Option * ● Create New DCR ○ Use existing DCR

DCR input * IllumioDCR

Data Ingestion Config tab

Select or type in the following information:

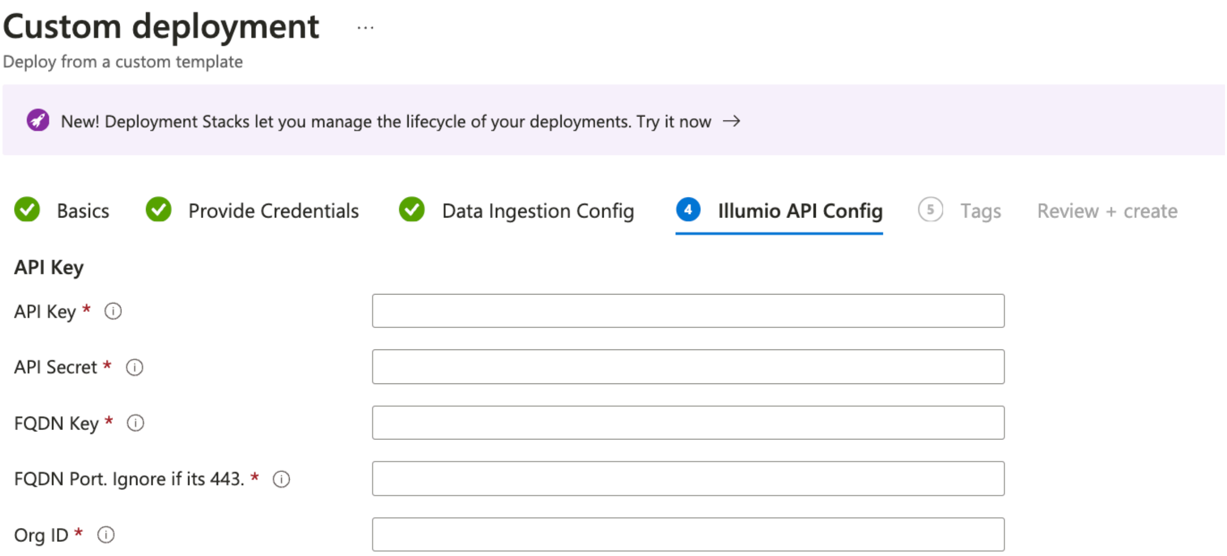
1. Enter a name for the data collection endpoint if you're creating it for the first time.
2. Enter a name for the data collection rule if you're creating it for the first time.
3. Select the preconfigured DCE and DCR only if you are deploying additional functional apps.

Illumio API Config Tab

NOTE

The Illumio PCE API key needs to have read-only permissions.

The **Illumio API Config** tab is the fourth tab within Custom deployment that you need to enter information into:



Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

API Key

API Key *

API Secret *

FQDN Key *

FQDN Port. Ignore if its 443. *

Org ID *

Select or type in the following information:

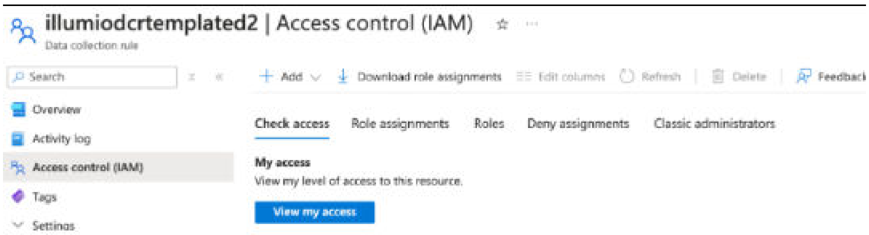
1. API Key
2. API Secret
3. FQDN of the PCE, in the scpx.illumio.com format. Do not enter "https".
4. FQDN Port
5. Org ID

Next, provide the necessary tags and proceed to the deployment. All of the resources that you specified will be deployed.

Provide Permissions for the Data Collection Rule

The data collection rule will not be able to ingest data into the Log Analytics workspace because it does not have the necessary permissions.

To address this, go to **Data Collection Rules**, select the DCR that you previously created, and go to **IAM**.



illumiodcrtemplated2 | Access control (IAM)

Data collection rule

My access

View my level of access to this resource.

Access Control (IAM)

Use Assign permissions to a DCR as a guide for assigning permissions to the data collection rule.

After you've assigned permissions, it takes approximately 45 minutes for the permissions to propagate and for the API calls to succeed.

Provision Workbooks

To view the available workbooks, select Sentinel > Workbooks > Templates.

Save the following workbooks:

- Illumio Auditable Events Workbook
- Illumio Flow Data Workbook
- Illumio Workload Stats Workbook

About the Data Connector

Keep these main points in mind about the Data Connector:

- The Data Connector contains four serverless functions.

- The Function app maintains two queues in the Azure storage queue: one is in the main queue and the other is a backlog queue. Notifications read from the AWS SQS are placed in the mainQueue until the max size queue count is reached. After that, events are placed in the backlog queue.

Consumption function app deployment: If events in the backlog queue are growing, it's an indication that additional function apps need to be deployed to handle the load.

Proceed with these steps:

1. Queue Trigger: Run it each time an item is added to the Azure storage queue.
2. Timer Trigger: Run it every 10 minutes. It is responsible for fetching the files from SQS/S3 and adding them to the Azure storage queue.
3. Timer Trigger: Run it every 10 minutes. It is responsible for managing the backlog and main queue. Each time there are items in the backlog queue, the Timer Trigger checks if there is space in the main queue and removes items from the queue.
4. Timed Api Trigger: Run it once every hour. It makes GET workloads requests to the PCE, summarizes the response, and stores it in log analytics.

If you are deploying additional function apps, use the same steps as above and follow these guidelines:

- For every new function app, ensure that it is deployed in a new app service plan.
- Select the same storage account for every new function app deployment.

For premium function app deployment, you can deploy a virtual network and configure the same for the storage account. This ensures that the storage account is not open to public access.

Monitor Data Ingestion

Use the following procedure to monitor data ingestion:

1. Select **Metrics**.
2. Create a new workbook.
3. Select the data collection rule that was deployed previously.
4. Add graphs that show the following:
   - API Requests/Min
   - Data Ingested in Bytes
   - Log Rows Ingested

Workbooks

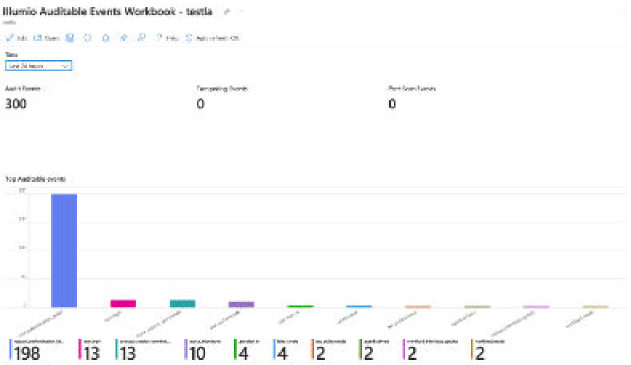
The following topics describe the Illumio Auditable Events Workbook, the Illumio Flow Data Workbook, and the Illumio APIs Workbook and provide detailed information about the widgets and graphs that are available in each workbooks.

Illumio Auditable Events Workbook

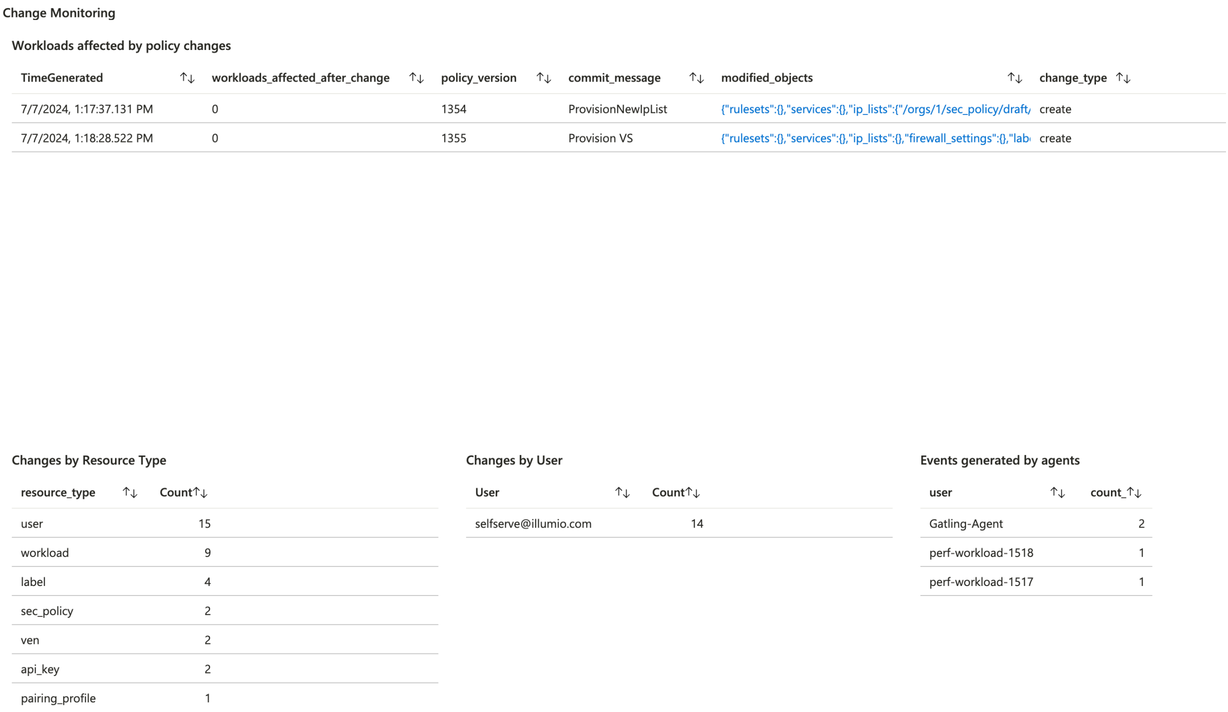
The **Illumio Auditable Events Workbook** shows a count of audit events, tampering events, and port scan events.

From the **Time** drop-down, select the time range for which you want to fetch flows.

- **Top Auditable Events**: This is a bar graph of all auditable events by event type.
- **Change Monitoring** contains the following widgets:
  - **Workloads affected by policy changes**: This depicts workloads that were affected by security policy changes, the list of modified objects per policy version, the commit message, and the time generated.
  - **Changes by Resource Type**: This displays the count of auditable events by resource types.
  - **Changes by User**: This displays the count of auditable events per user.
- **PCE events breakdown per hour**: This displays the trend of auditable events by event type per hour.
- **Authentication events**: This section presents all authentication events. You can include or exclude certain groups of events and can filter by severity and status.


Illumio Auditable Events Workbook - testla

Illumio Auditable Events Workbook



Change Monitoring

Workloads affected by policy changes

TimeGenerated	workloads_affected_after_change	policy_version	commit_message	modified_objects	change_type
7/7/2024, 1:17:37.131 PM	0	1354	ProvisionNewIpList	{"rulesets":{},"services":{},"ip_lists":{"/orgs/1/sec_policy/draft/	create
7/7/2024, 1:18:28.522 PM	0	1355	Provision VS	{"rulesets":{},"services":{},"ip_lists":{},"firewall_settings":{},"lab	create

Changes by Resource Type

resource_type	Count
user	15
workload	9
label	4
sec_policy	2
ven	2
api_key	2
pairing_profile	1

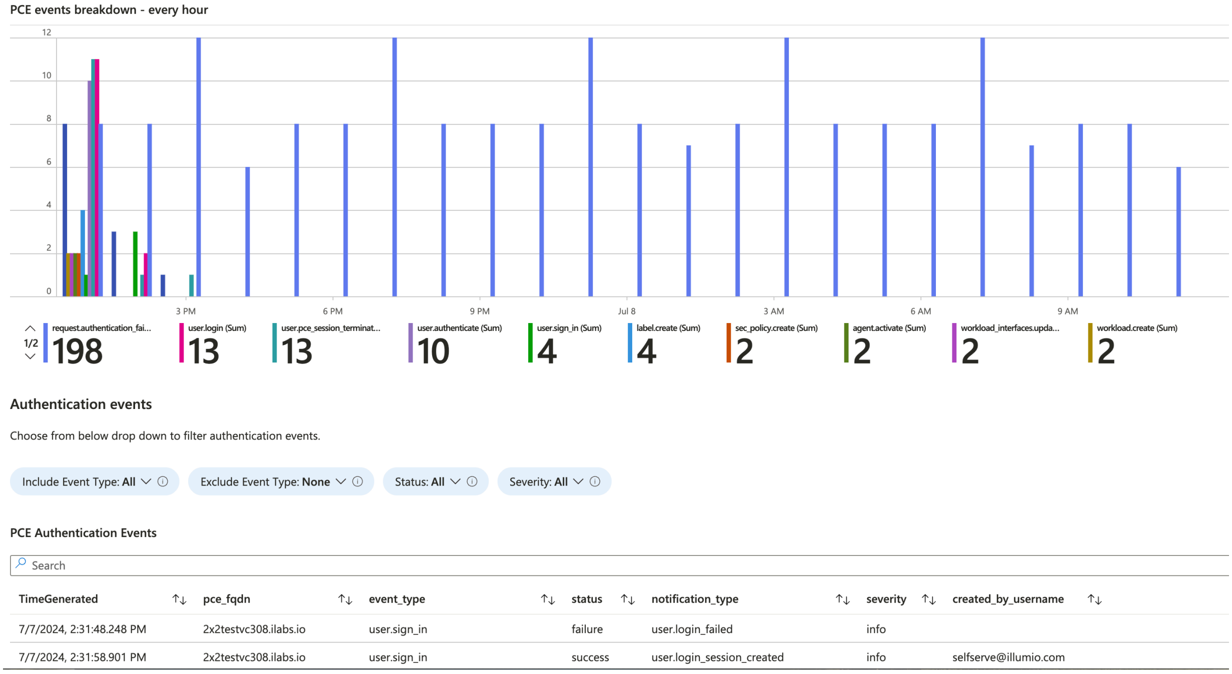
Changes by User

User	Count
selfserve@illumio.com	14

Events generated by agents

user	count_
Gatling-Agent	2
perf-workload-1518	1
perf-workload-1517	1

Workloads Affected by Policy Change



PCE events breakdown - every hour

Authentication events

Choose from below drop down to filter authentication events.

Include Event Type: All | Exclude Event Type: None | Status: All | Severity: All

PCE Authentication Events

Search

TimeGenerated	pce_fqdn	event_type	status	notification_type	severity	created_by_username
7/7/2024, 2:31:48.248 PM	2x2testvc308.ilabs.io	user.sign_in	failure	user.login_failed	info	
7/7/2024, 2:31:58.901 PM	2x2testvc308.ilabs.io	user.sign_in	success	user.login_session_created	info	selfserve@illumio.com

PCE Events Breakdown - Every Hour

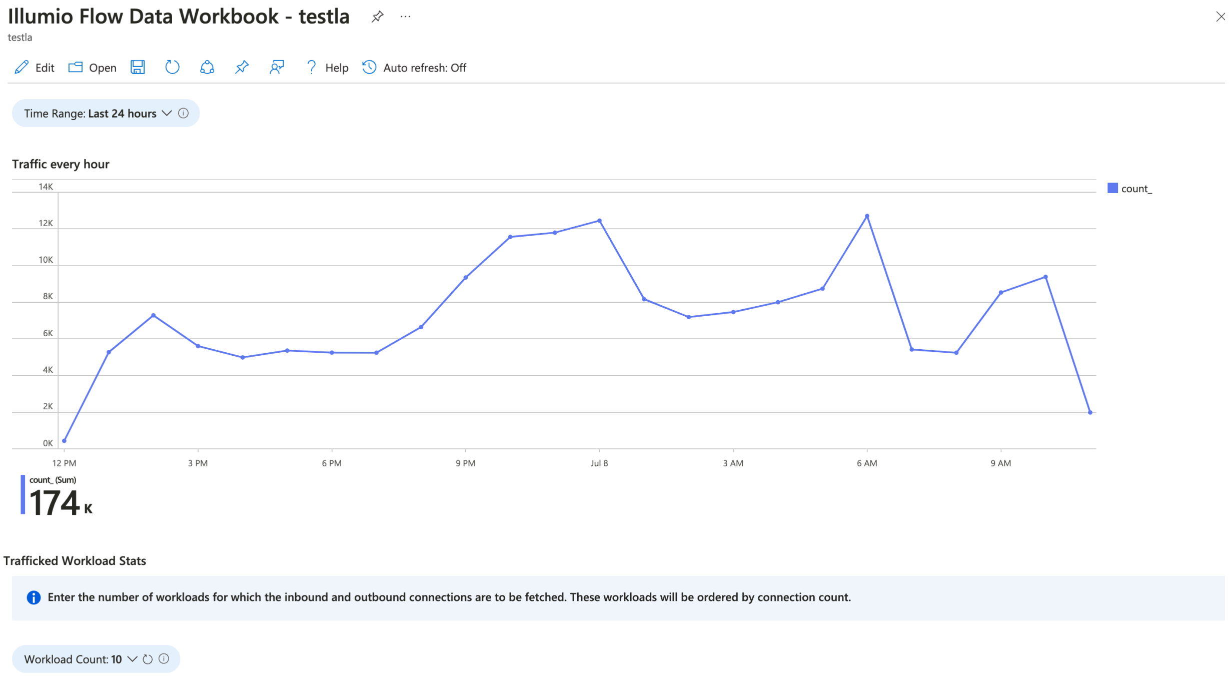
Illumio Flow Data Workbook

From the **Time Range** drop-down, select the time range for which you want to fetch the flows.

- The **Traffic every hour** widget shows the trend of the number of connections and traffic every hour.

- **Trafficked Workload Stats**: Enter the number of workloads for which the inbound and outbound connections are to be fetched. These workloads are ordered by the connection count.
- **Traffic Explorer**: This widget allows you to specify the Source IP, Destination IP, Destination Port, and Protocol. If you do not provide any inputs, by default all rows of traffic are fetched. However, if you do input values, the traffic that is fetched depends upon your input.
  - If you specify the Destination Port as 5353 and the protocol as 17, then the traffic rows that correspond to those values will be returned.
  - If you specify the Source IP as 10.6.0.2 and the Destination Port as 20000, then the traffic rows that correspond to this filter will be returned.

- **Flow Count by Policy Decision**: This widget specifies the flow count by policy decision.
- **Flows by Class**: This widget specifies the flow count by class, which is multicast, broadcast, or unicast.
- **Top 5 Ports by Flow Count**: This widget shows the top 5 ports by flow count.
- **Blocked Traffic**: This table presents blocked traffic.
- **Allowed Traffic**: This table presents allowed traffic.
- **Potentially Blocked Traffic**: This table presents potentially blocked traffic.



Illumio Flow Data Workbook - testla

testla

Time Range: Last 24 hours

Traffic every hour

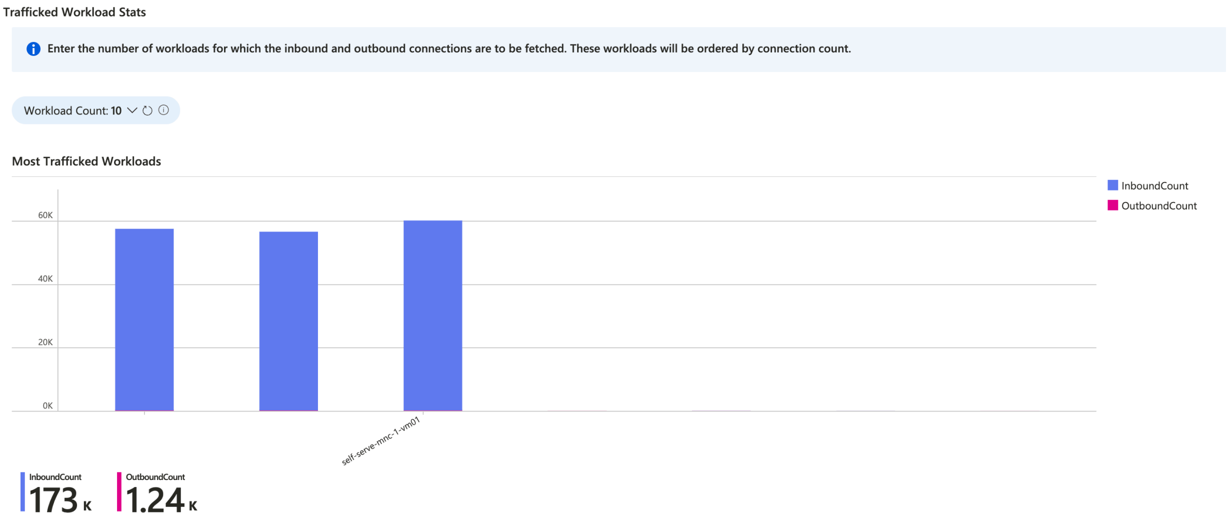
count_ (Sum)
174 K

Trafficked Workload Stats

Enter the number of workloads for which the inbound and outbound connections are to be fetched. These workloads will be ordered by connection count.

Workload Count: 10

Illumio Flow Data Workbook



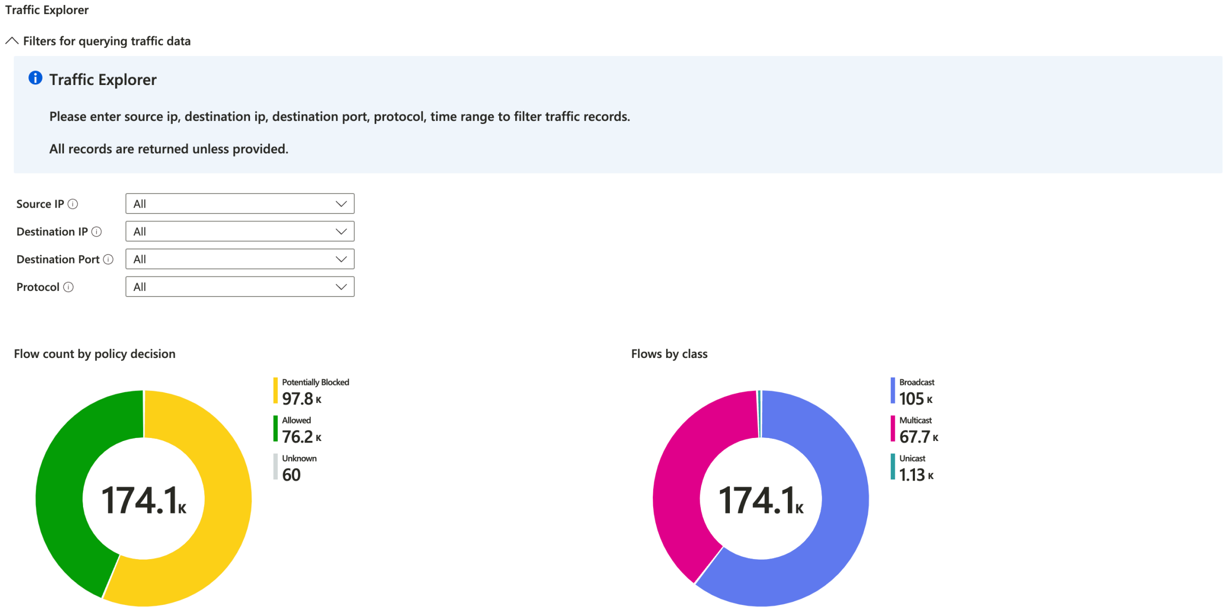
Trafficked Workload Stats

Enter the number of workloads for which the inbound and outbound connections are to be fetched. These workloads will be ordered by connection count.

Workload Count: 10

Most Trafficked Workloads

Trafficked Workload Stats



Traffic Explorer

Filters for querying traffic data

Traffic Explorer

Please enter source ip, destination ip, destination port, protocol, time range to filter traffic records.

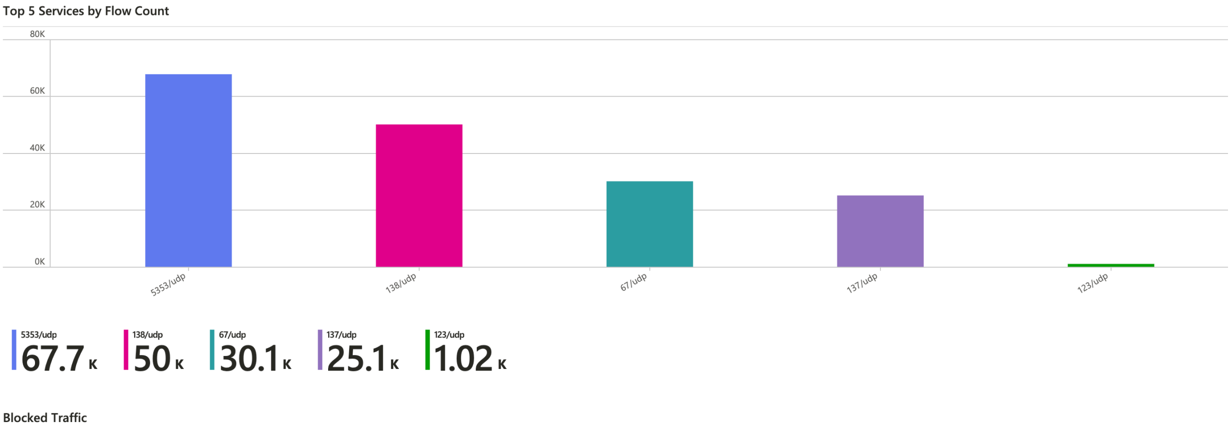
All records are returned unless provided.

Source IP	All
Destination IP	All
Destination Port	All
Protocol	All

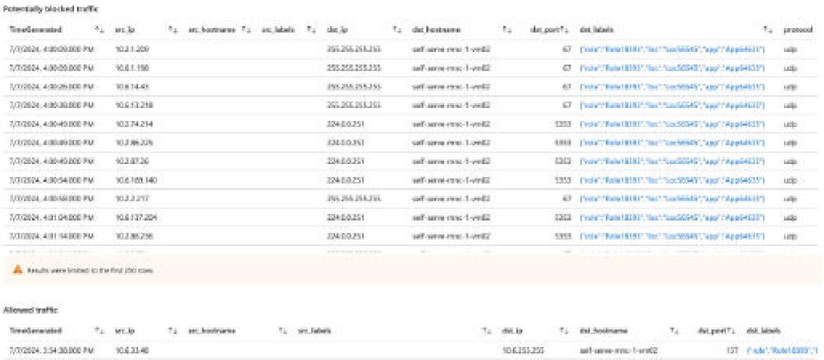
Flow count by policy decision

Flows by class

Traffic Explorer



Top 5 Services by Flow Count



Potentially blocked traffic

TimeGenerated	src_ip	src_hostname	src_labels	dst_ip	dst_hostname	dst_port	dst_labels	protocol
7/7/2024, 4:00:09.000 PM	10.2.1.209			255.255.255.255	self-serve-misc-1-vm02	67	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp
7/7/2024, 4:00:09.000 PM	10.6.1.198			255.255.255.255	self-serve-misc-1-vm02	67	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp
7/7/2024, 4:00:26.000 PM	10.8.14.43			255.255.255.255	self-serve-misc-1-vm02	67	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp
7/7/2024, 4:00:30.000 PM	10.6.13.218			255.255.255.255	self-serve-misc-1-vm02	67	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp
7/7/2024, 4:00:49.000 PM	10.2.74.214			224.0.0.251	self-serve-misc-1-vm02	5353	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp
7/7/2024, 4:00:49.000 PM	10.2.86.225			224.0.0.251	self-serve-misc-1-vm02	5353	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp
7/7/2024, 4:00:49.000 PM	10.2.87.26			224.0.0.251	self-serve-misc-1-vm02	5353	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp
7/7/2024, 4:00:54.000 PM	10.6.169.140			224.0.0.251	self-serve-misc-1-vm02	5353	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp
7/7/2024, 4:00:58.000 PM	10.2.2.217			255.255.255.255	self-serve-misc-1-vm02	67	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp
7/7/2024, 4:01:04.000 PM	10.6.137.224			224.0.0.251	self-serve-misc-1-vm02	5353	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp
7/7/2024, 4:01:14.000 PM	10.2.88.238			224.0.0.251	self-serve-misc-1-vm02	5353	{"role":"Role18181","loc":"Loc56545","app":"App64635"}	udp

⚠ Results were limited to the first 250 rows.

Allowed traffic

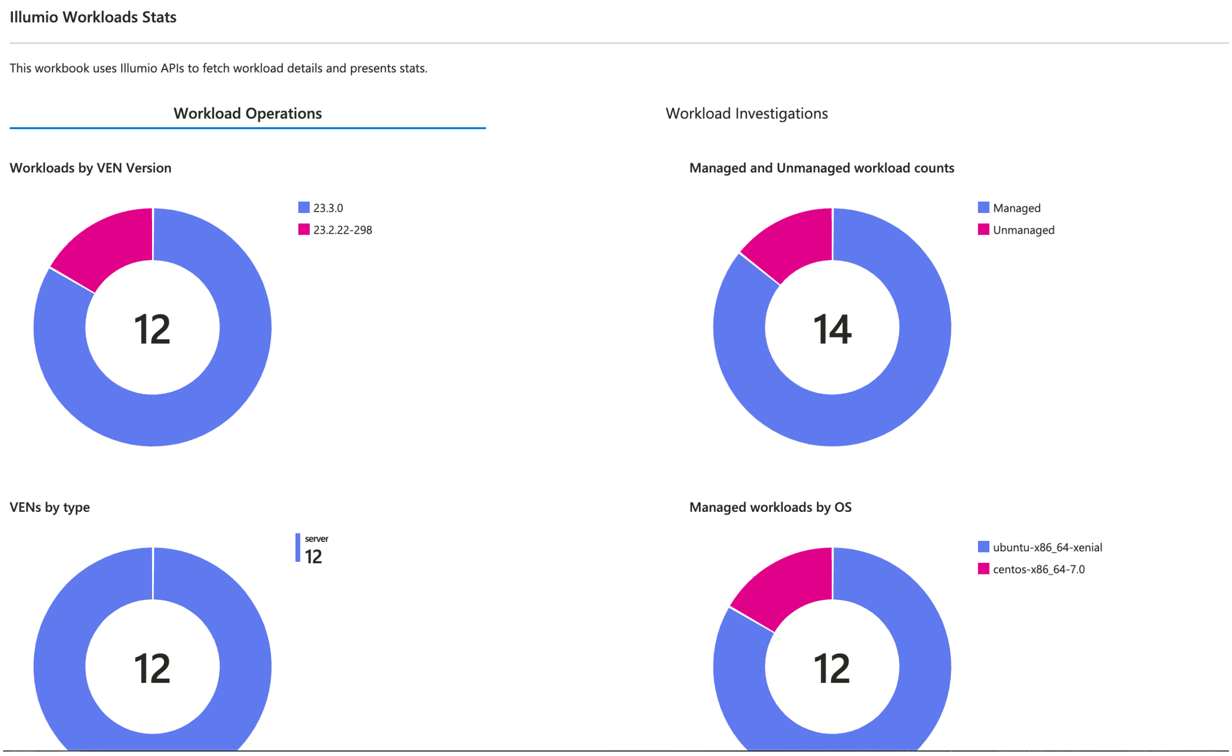
TimeGenerated	src_ip	src_hostname	src_labels	dst_ip	dst_hostname	dst_port	dst_labels
7/7/2024, 3:54:30.000 PM	10.6.33.40			10.6.255.255	self-serve-misc-1-vm02	137	{"role":"Role18181","l

Traffic Stats

Illumio Workload Stats Workbook

This workbook contains the following widgets:

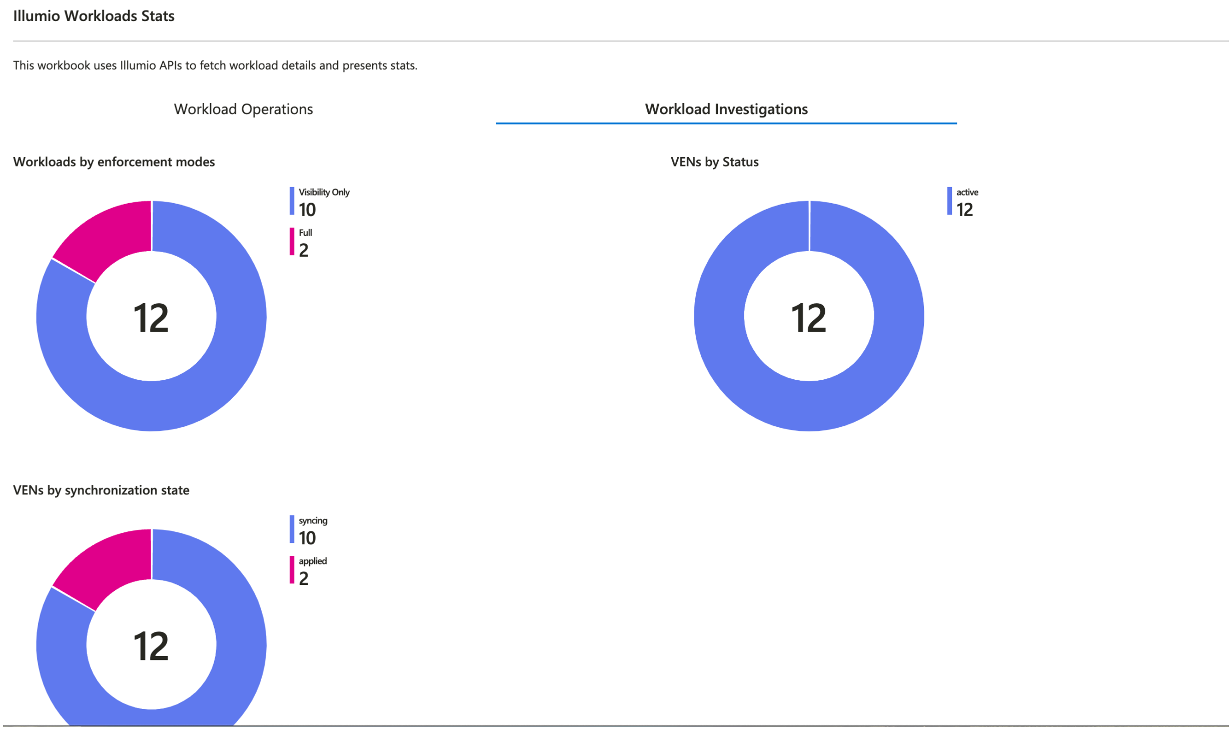
- **Workloads by VEN Version**
- **Managed and Unmanaged workload counts**
- **VENs by type**
- **Managed workloads by OS**
- **Workloads by enforcement modes**
- **VENs by Status**
- **VENs by synchronization state**



Illumio Workloads Stats

This workbook uses Illumio APIs to fetch workload details and presents stats.

Workload Operations



Illumio Workloads Stats

This workbook uses Illumio APIs to fetch workload details and presents stats.

Workload Investigations

Configure a Private Network

If Azure policies require storage accounts to use private networks, then follow these steps to configure a virtual network for function app and storage account communication. If additional functional apps are deployed, then use the same virtual network to configure the new function apps and configure the same in the storage account.

1. In the Search bar, enter "virtual networks".
2. Configure a virtual network in the same resource group as the function app, define an address space, and save. If you have already configured a virtual network, do not perform this step.
3. Go to function app, select **Networking**, and select **Configure outbound network access**.
4. Configure the function app to use the virtual network that you configured in Step 2 and save.
5. Navigate to the storage account that is linked to the function app.
6. Select **Networking** and then select **Enabled** from selected virtual networks and IP addresses.
7. Select the virtual network that you configured in Step 2 and save it. This ensures that the function app can talk to the storage account.
8. Select **Add your client IP address** so that accessing the storage browser from portal.azure.com does not cause permissions errors. This can be helpful to monitor the state of queues.

Deploy Additional Function Apps

Before a new function app is deployed, check the following:

1. Make sure that the messages on the AWS SQS are increasing compared to the messages that are being consumed from SQS. To do so, in the Monitoring section of AWS SQS, check the Message Received stats against the Sent stats.
2. Make sure that the function app's SQS_FILES_READ_LIMIT environment variable is set to 200 by default, which means that the function reads 200 messages every 5 minutes. This can be increased based on your requirements. However, increasing this value beyond 1000 can lead to performance issues because the Queue Trigger function resides in the same function app.
3. If the number of messages to be processed from the AWS SQS has to be beyond 1000, do the following:
   a. Disable the queue trigger app so that it doesn't starve the TimedSQS for resources.
   b. Deploy additional trigger queue apps separately to handle the load on the Azure queue.
4. If private networking is used, then deploying additional function apps requires manually configuring the virtual network on each new app and adjusting the network configuration on the storage account. After you do this, then you need to restart the new function app. See Configure a Private Network [24].

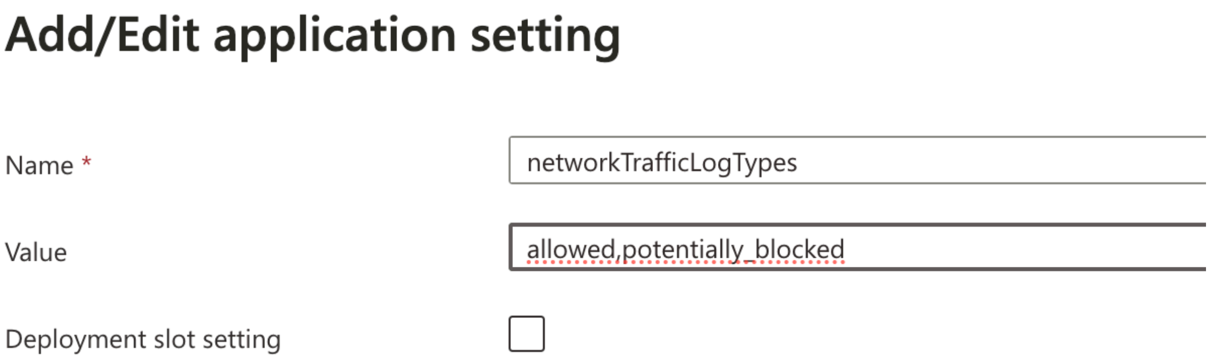
Additional function apps are required as a result of the incoming event rate. If the number of messages being ingested is less than the incoming rate, then it is essential to add additional queue triggers. Either use the landing page to deploy additional queue triggers or use https://github.com/Azure/Azure-Sentinel/tree/master/Solutions/IllumioSaaS/Data%20Connectors for deploying.

Ingest Specific Network Traffic Logs

You can select the type of network traffic to be ingested. After you deploy the function app, go to function app, select environment variables and modify the value of the `networkTrafficLogTypes` key to ingest only the type of network traffic that you want.

The supported values are allowed, blocked, potentially_blocked, All, and unknown.

You can add any combinations of the supported values, separated by commas. For example, if you only want blocked and potentially blocked traffic to be ingested by the data connector, set the value to blocked, potentially_blocked.

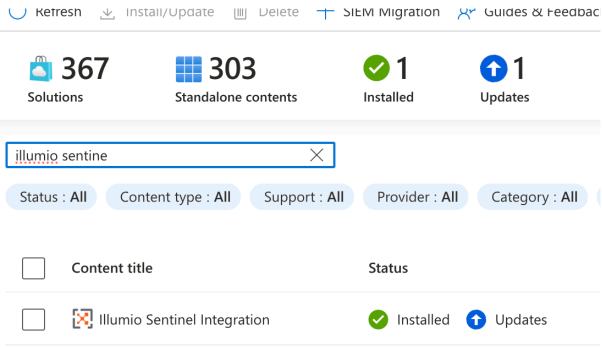


Add/Edit application setting

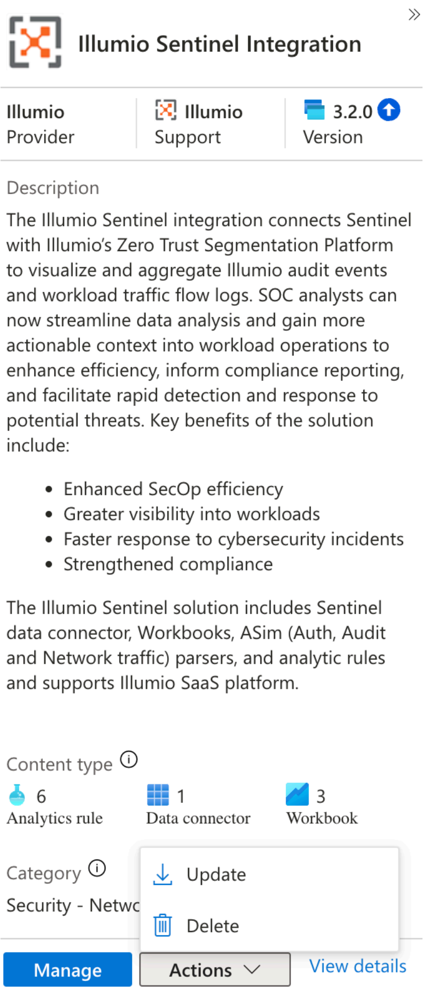
Name *	networkTrafficLogTypes
Value	allowed,potentially_blocked
Deployment slot setting	□

Upgrade to Illumio Sentinel Solution Version 3.4.0

To upgrade to version 3.4.0, select Illumio Sentinel Integration and then select **Actions > Update**.



□	Content title	Status
□	Illumio Sentinel Integration	✓ Installed Updates



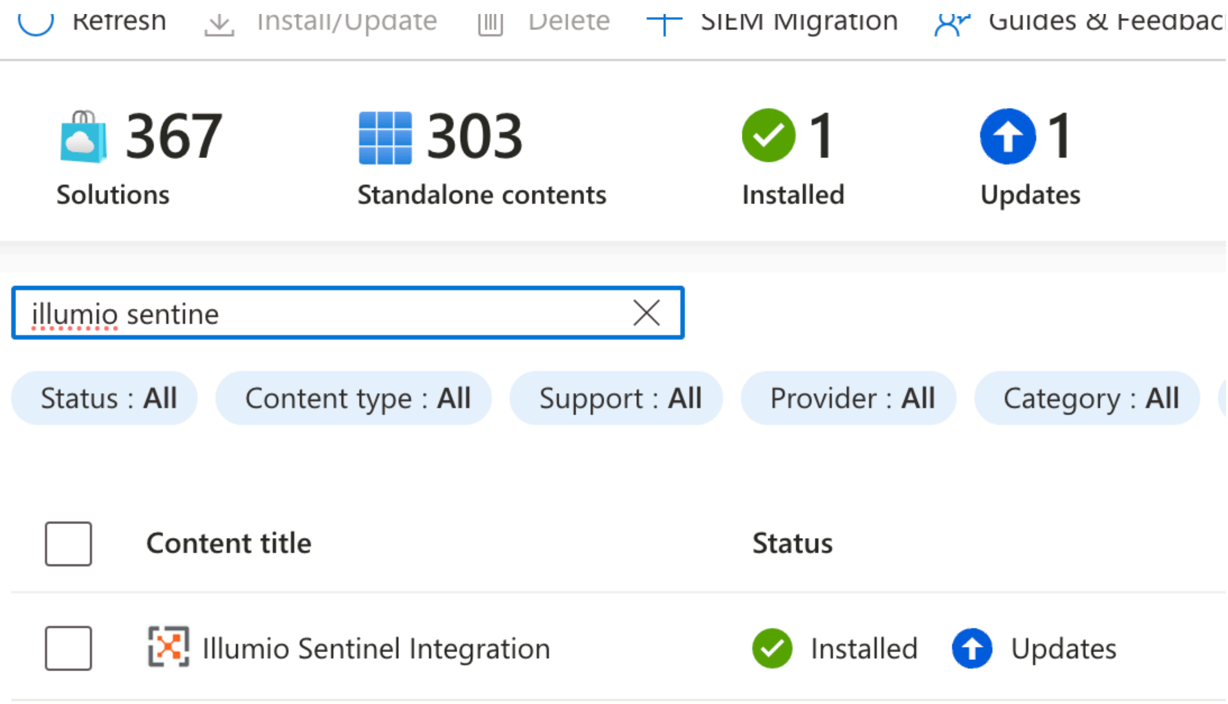
Illumio Sentinel Integration

Description

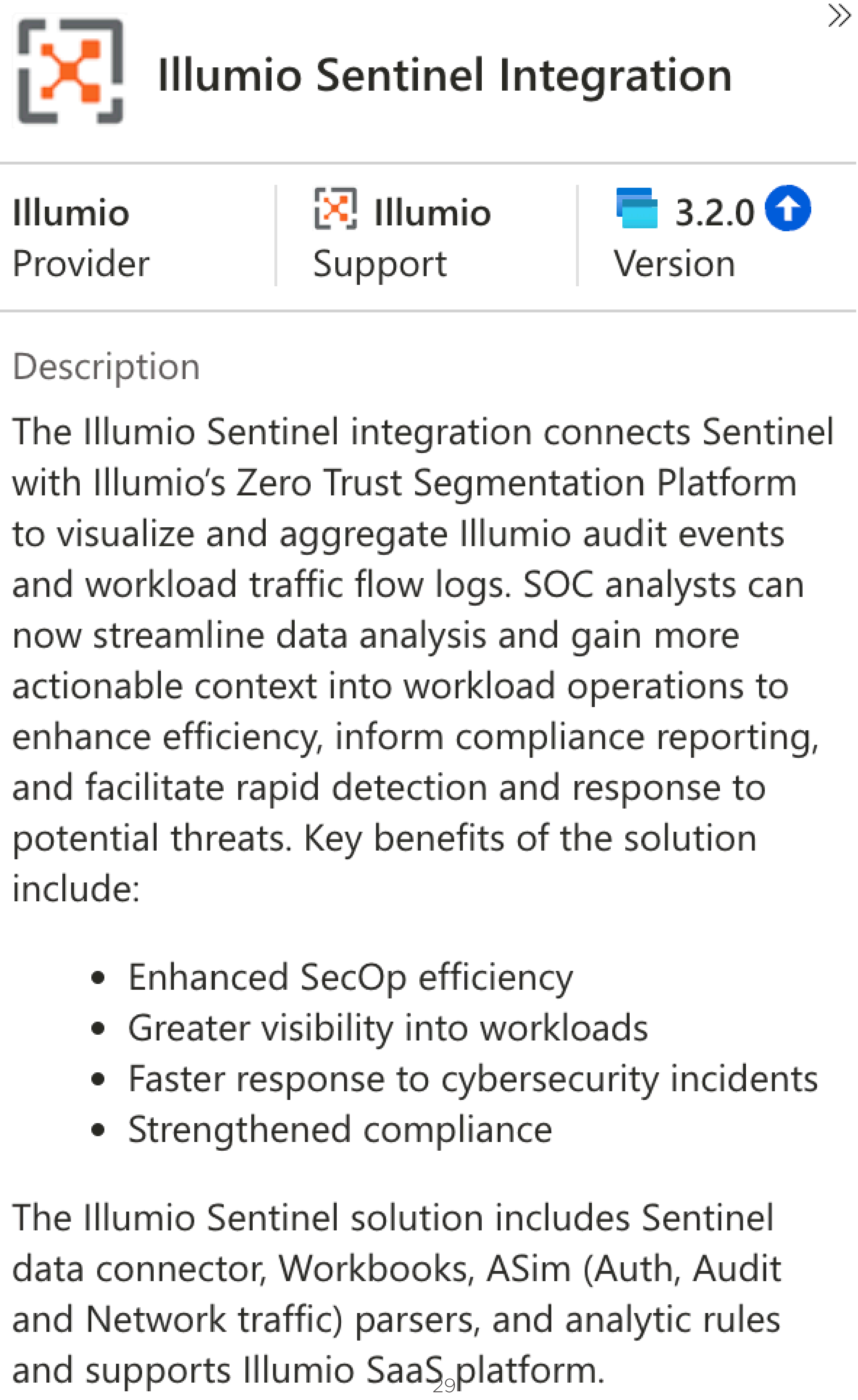
The Illumio Sentinel integration connects Sentinel with Illumio's Zero Trust Segmentation Platform to visualize and aggregate Illumio audit events and workload traffic flow logs. SOC analysts can now streamline data analysis and gain more actionable context into workload operations to enhance efficiency, inform compliance reporting, and facilitate rapid detection and response to potential threats. Key benefits of the solution include:

- Enhanced SecOp efficiency
- Greater visibility into workloads
- Faster response to cybersecurity incidents
- Strengthened compliance

The Illumio Sentinel solution includes Sentinel data connector, Workbooks, ASim (Auth, Audit and Network traffic) parsers, and analytic rules and supports Illumio SaaS platform.



□	Content title	Status
□	Illumio Sentinel Integration	✓ Installed ⬆ Updates



Illumio Sentinel Integration

Illumio Provider	**Illumio** Support	**3.2.0** Version

Description

The Illumio Sentinel integration connects Sentinel with Illumio's Zero Trust Segmentation Platform to visualize and aggregate Illumio audit events and workload traffic flow logs. SOC analysts can now streamline data analysis and gain more actionable context into workload operations to enhance efficiency, inform compliance reporting, and facilitate rapid detection and response to potential threats. Key benefits of the solution include:

- Enhanced SecOp efficiency
- Greater visibility into workloads
- Faster response to cybersecurity incidents
- Strengthened compliance

The Illumio Sentinel solution includes Sentinel data connector, Workbooks, ASim (Auth, Audit and Network traffic) parsers, and analytic rules and supports Illumio SaaS platform.

After you upgrade the solution, restart the function app.

About Analytics Rules

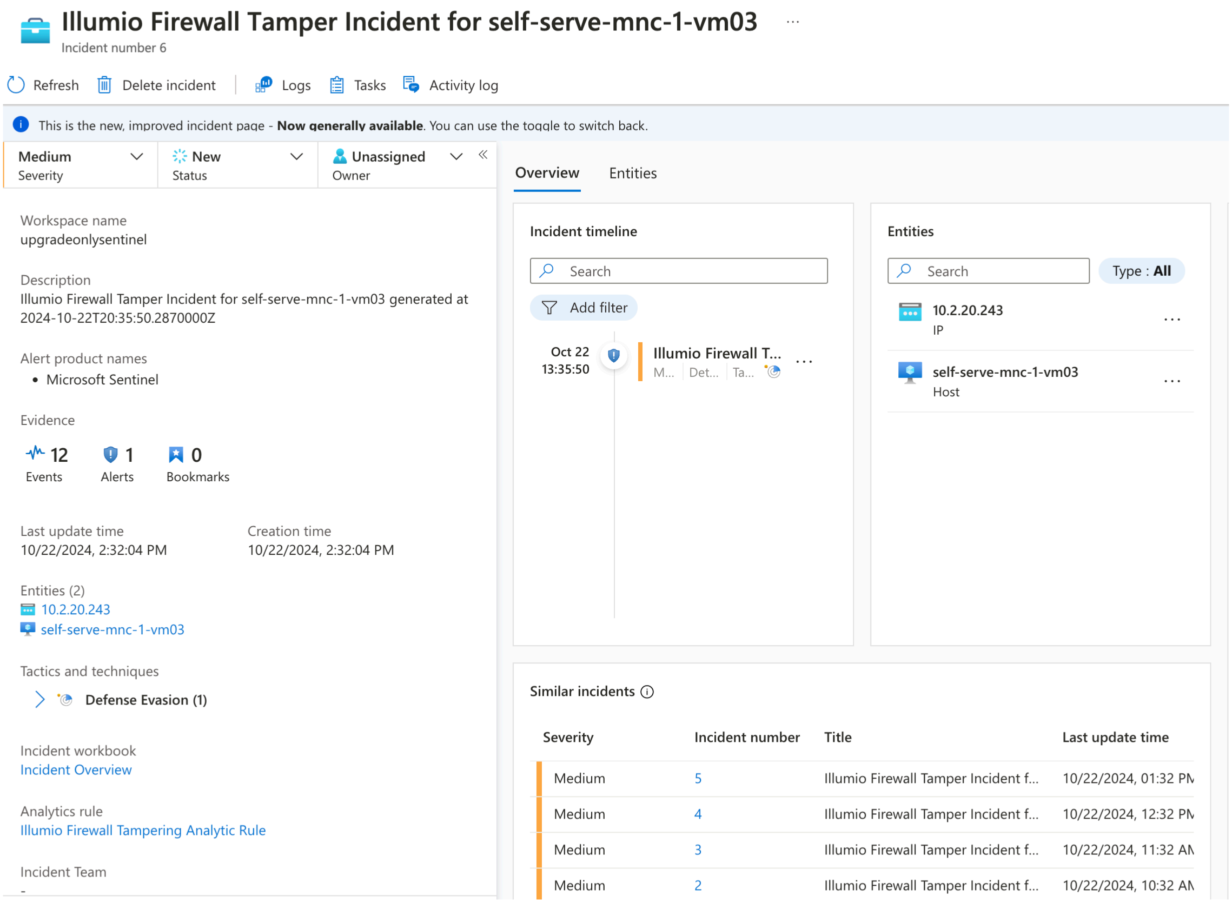
Sentinel Analytics rules are KQL queries on logs that you can either run upon request or schedule. When an Analytic rule finds a match in the log data, a Sentinel alert and incident are created.

The following rules are included in this release of Illumio Sentinel Solution:

- Illumio Firewall Tampering Analytic Rule
- Illumio Enforcement Change Analytic Rule
- Illumio VEN Offline Detection Rule
- Illumio VEN Deactivated Detection Rule
- Illumio VEN Suspend Detection Rule
- Illumio VEN Clone Detection Rule

Each of these rules will be triggered when there is a corresponding VEN event. The hostname and IP address will be collected so that the admin can troubleshoot.

The following screenshot shows an example of an incident from one of the Analytics rules:



Illumio Firewall Tamper Incident for self-serve-mnc-1-vm03

Incident number 6

This is the new, improved incident page - **Now generally available**. You can use the toggle to switch back.

Severity: Medium
Status: New
Owner: Unassigned

Workspace name
upgradeonlysentinel

Description
Illumio Firewall Tamper Incident for self-serve-mnc-1-vm03 generated at 2024-10-22T20:35:50.2870000Z

Alert product names
- Microsoft Sentinel

Evidence
12 Events
1 Alerts
0 Bookmarks

Last update time
10/22/2024, 2:32:04 PM

Creation time
10/22/2024, 2:32:04 PM

Entities (2)
10.2.20.243
self-serve-mnc-1-vm03

Tactics and techniques
Defense Evasion (1)

Incident workbook
Incident Overview

Analytics rule
Illumio Firewall Tampering Analytic Rule

Incident Team
-

Incident timeline

Search
Add filter

Oct 22
13:35:50
Illumio Firewall T...
M... Det... Ta...

Entities

Search
Type : **All**

10.2.20.243
IP

self-serve-mnc-1-vm03
Host

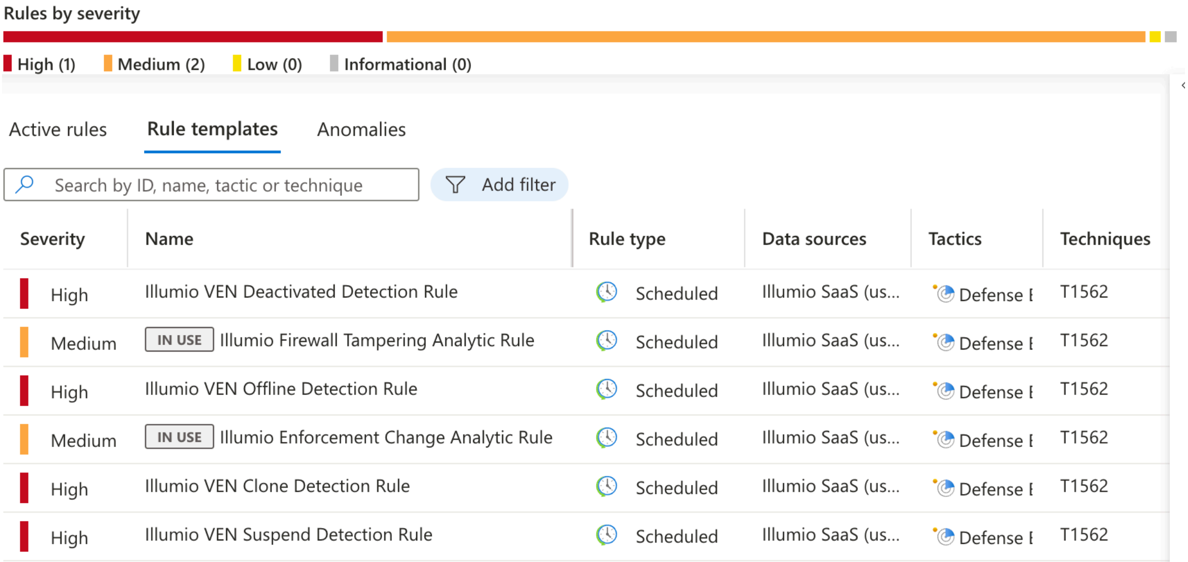
Similar incidents

Severity	Incident number	Title	Last update time
Medium	5	Illumio Firewall Tamper Incident f...	10/22/2024, 01:32 PM
Medium	4	Illumio Firewall Tamper Incident f...	10/22/2024, 12:32 PM
Medium	3	Illumio Firewall Tamper Incident f...	10/22/2024, 11:32 AM
Medium	2	Illumio Firewall Tamper Incident f...	10/22/2024, 10:32 AM

Deploy Analytics Rules

Follow these steps after you have deployed and installed the Illumio Sentinel Solution from the Content Hub.

1. Navigate to **Configuration > Analytics** and select **Rule templates**:



Rules by severity

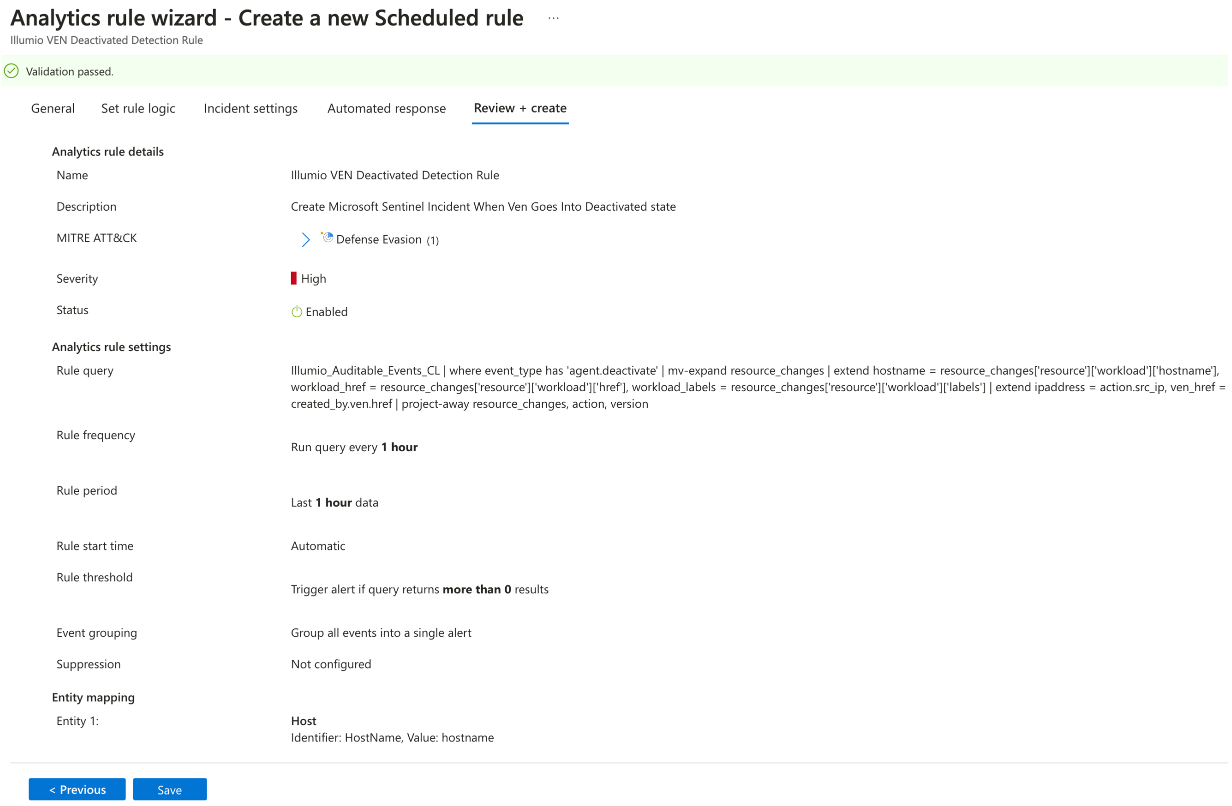
🟥 High (1) 🟧 Medium (2) 🟨 Low (0) ⬜ Informational (0)

Severity	Name	Rule type	Data sources	Tactics	Techniques
🟥 High	Illumio VEN Deactivated Detection Rule	Scheduled	Illumio SaaS (us...	Defense E	T1562
🟧 Medium	IN USE Illumio Firewall Tampering Analytic Rule	Scheduled	Illumio SaaS (us...	Defense E	T1562
🟥 High	Illumio VEN Offline Detection Rule	Scheduled	Illumio SaaS (us...	Defense E	T1562
🟧 Medium	IN USE Illumio Enforcement Change Analytic Rule	Scheduled	Illumio SaaS (us...	Defense E	T1562
🟥 High	Illumio VEN Clone Detection Rule	Scheduled	Illumio SaaS (us...	Defense E	T1562
🟥 High	Illumio VEN Suspend Detection Rule	Scheduled	Illumio SaaS (us...	Defense E	T1562

2. Create a rule from each of these templates. Note that most of the fields contain default values.

> **NOTE**
> For each rule, the query schedule is set to once and hour and it looks at the data from the past hour.

For example, the following figure shows the final step in the Analytics rule wizard before you create a rule:



Analytics rule wizard - Create a new Scheduled rule

Illumio VEN Deactivated Detection Rule

Validation passed.

Analytics rule details

Name	Illumio VEN Deactivated Detection Rule
Description	Create Microsoft Sentinel Incident When Ven Goes Into Deactivated state
MITRE ATT&CK	Defense Evasion (1)
Severity	🟥 High
Status	Enabled

Analytics rule settings

Rule query	Illumio_Auditable_Events_CL | where event_type has 'agent.deactivate' | mv-expand resource_changes | extend hostname = resource_changes['resource']['workload']['hostname'], workload_href = resource_changes['resource']['workload']['href'], workload_labels = resource_changes['resource']['workload']['labels'] | extend ipaddress = action.src_ip, ven_href = created_by.ven.href | project-away resource_changes, action, version
Rule frequency	Run query every **1 hour**
Rule period	Last **1 hour** data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns **more than 0** results
Event grouping	Group all events into a single alert
Suppression	Not configured

Entity mapping

Entity 1:	**Host** Identifier: HostName, Value: hostname

Advanced Security Information Model (ASIM) Parsers

ASIM parsers in general have two variants:

- A parameter variant
- A parameter-less variant

See List of Microsoft Sentinel Advanced Security Information Model (ASIM) parsers.

Audit Parser

This parser queries the Illumio_Auditable_Events_CL custom table. It supports the following parser arguments:

- starttime
- endtime
- srcipaddr_has_any_prefix
- actorusername_has_any
- eventtype_in
- eventresult
- operation_has_any
- object_has_any
- newvalue_has_any
- disabled

See The Advanced Security Information Model (ASIM) Audit Events normalization schema reference for the ASIM audit schema.

Network Session Parser

This parser queries the Illumio_Flow_Events_CL custom table. It supports the following parser arguments:

- starttime
- endtime
- srcipaddress_has_any_prefix
- dstipaddr_has_any_prefix
- ipaddr_has_any_prefix
- dstportnumber
- hostname_has_any
- dvcation
- eventresult
- disabled

See The Advanced Security Information Model (ASIM) Network Session normalization schema reference for the ASIM network session schema.

Authentication Parser

This parser queries the Illumio_Auditable_Events_CL custom table and looks for specific authentication-related events like:

- user.signin
- user.login
- user.sign_out
- user.logout
- user.authenticate
- user.use_expired_password

It supports the following parser arguments:

- starttime
- endtime
- username_has_any
- targetappname_has_any
- srchostname_has_any
- srcipaddr_has_any_prefix
- eventtype_in
- eventresultdetails_in
- eventresult
- disabled

See The Advanced Security Information Model (ASIM) Authentication normalization schema reference for the ASIM authentication schema.

About Microsoft Sentinel Playbooks

Microsoft Sentinel playbooks are collections of procedures that can be run from Microsoft Sentinel.

The Illumio Sentinel Solution contains three playbooks:

- Quarantine Workloads
- Containment Switch
- Get VEN Details

Deploy the Common Function App for Playbooks

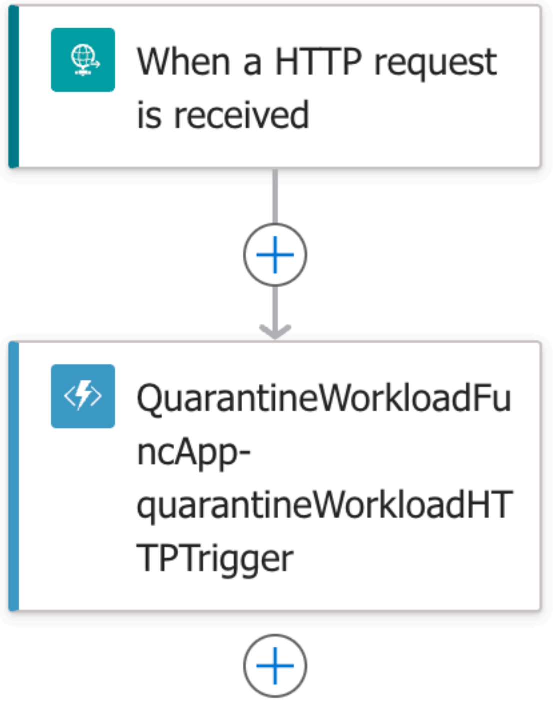
You need to deploy a function app to be able to use playbooks. Use the following link:

Microsoft Sentinel Function App for Playbooks

After you deploy the function app, make a note of its name and the region in which it is deployed. The playbooks need to reference the function app and you must deploy the playbooks in the same region as the function app.

About the Quarantine Workloads Playbook

This playbook has a collection of features that query the PCE and apply labels for a given list of workload names and labels.


When a HTTP request is received
QuarantineWorkloadFuncApp-quarantineWorkloadHTTPTrigger

When you run this playbook using an HTTP request, the payload should follow this example:

```
{  "workloads": [
     "Workload-1", "Workload-2"
 ],  "labels": [
       "quarantine_app",
       "quarantine_role"
 ]
}
```

Note that the labels should exist in the PCE before you run the playbook.

About the Containment Switch Playbook

This playbook has a collection of procedures that do the following:

1. Run an explorer query: This step runs an explorer query over the last week for a given port-protocol combination to find traffic to workloads that is marked as **potentially blocked** or **unknown**.
2. Get a list of **visibility-only** workloads: This step parses the response from Step 1 and identifies the **visibility-only** workloads.
3. Create a deny rule: This step creates a deny rule from all IPs to all workloads for given port-protocol combination and provisions the object.
4. Create a virtual service: This step creates a virtual service for given port-protocol combination and provisions the object.

5. Create workload bindings: This step binds workloads to the virtual service created in Step 4.
6. Create allow rule: This step creates an allow rule from workloads to the virtual service.
7. Change enforcement state: This step changes the enforcement state of **visibility-only** workloads to the selective state.

> **NOTE**
>
> The Containment Switch playbook will make changes on the PCE.

Each of the preceding steps are built into functions that are part of a function app.

During the deployment of a playbook, the function app needs specific context to execute properly. It uses the following environment variables:

```
....
,{
    "name": "PCE_FQDN",
    "value": "[variables('pceFQDN')]"
},
{
    "name": "PORT",
    "value": "[variables('port')]"
},
{
    "name": "ORG_ID",
    "value": "[variables('orgId')]"
},
{
    "name": "API_KEY",
    "value": "[variables('apiKey')]"
},
{
    "name": "API_SECRET",
    "value": "[variables('apiSecret')]"
},....
```

This playbook allows users to isolate a workload. It does the following:

1. Queries the Illumio PCE for potentially blocked or unknown traffic for a given port-protocol combination.

   The following is an example of input to a playbook:

   ```
   {
    "protocol": 17, "port": 5354, "applyChanges": true
   }
   ```

   Here, "applyChanges" can be used to control whether or not the playbook should create objects on the PCE.

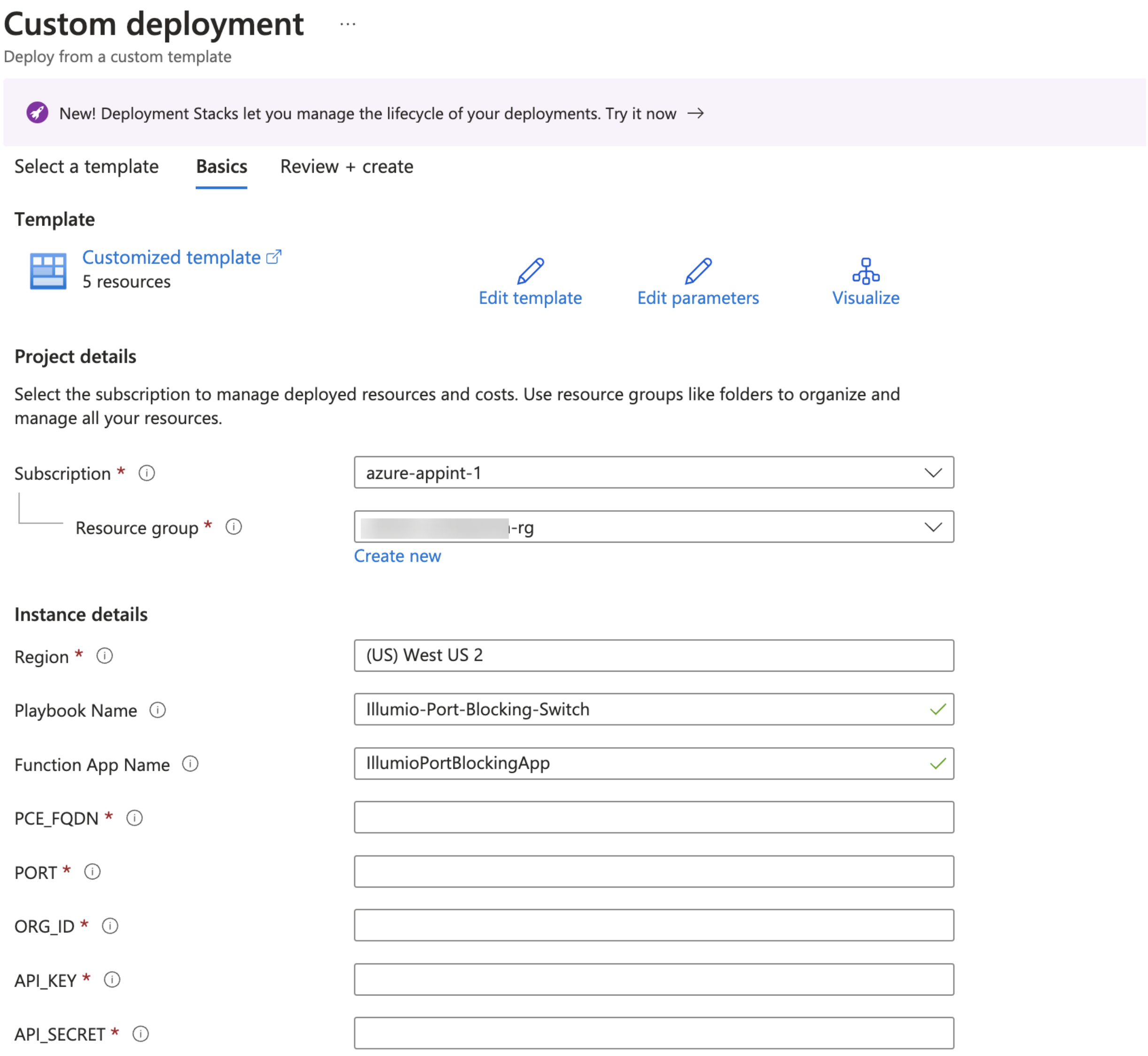
   - If this value is set to true, this playbook will create and provision changes, including workload enforcement changes.
   - If this value is set to false, the playbook will skip the create or modify object steps and will provide a summary of what will be done.

   Traffic Query results will still be available and visibility-only workloads will still be parsed from the response.

2. After the query has completed, visibility-only workloads are parsed from the response.
3. A deny rule is created where the source is "Any (0.0.0.0/0 and ::/0)" and the destination is **All** workloads.
4. The workloads parsed from the response to the query in Step 1 are converted to the **selective** enforcement state.
5. A virtual service is created for the port-protocol combination from Step 1 and the workloads identified in Step 1 are bound to the virtual service.
6. A ruleset is created in which an allow rule from "Any (0.0.0.0/0 and ::/0)" to the virtual service from Step 5 is created and provisioned.

Deploy the Containment Switch Playbook

You can deploy the playbook using this ARM template: Illumio Port Blocking Switch.



Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Select a template | **Basics** | Review + create

Template

Customized template ↗
5 resources

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-appint-1
Resource group * ⓘ	[redacted]-rg
	Create new

Instance details

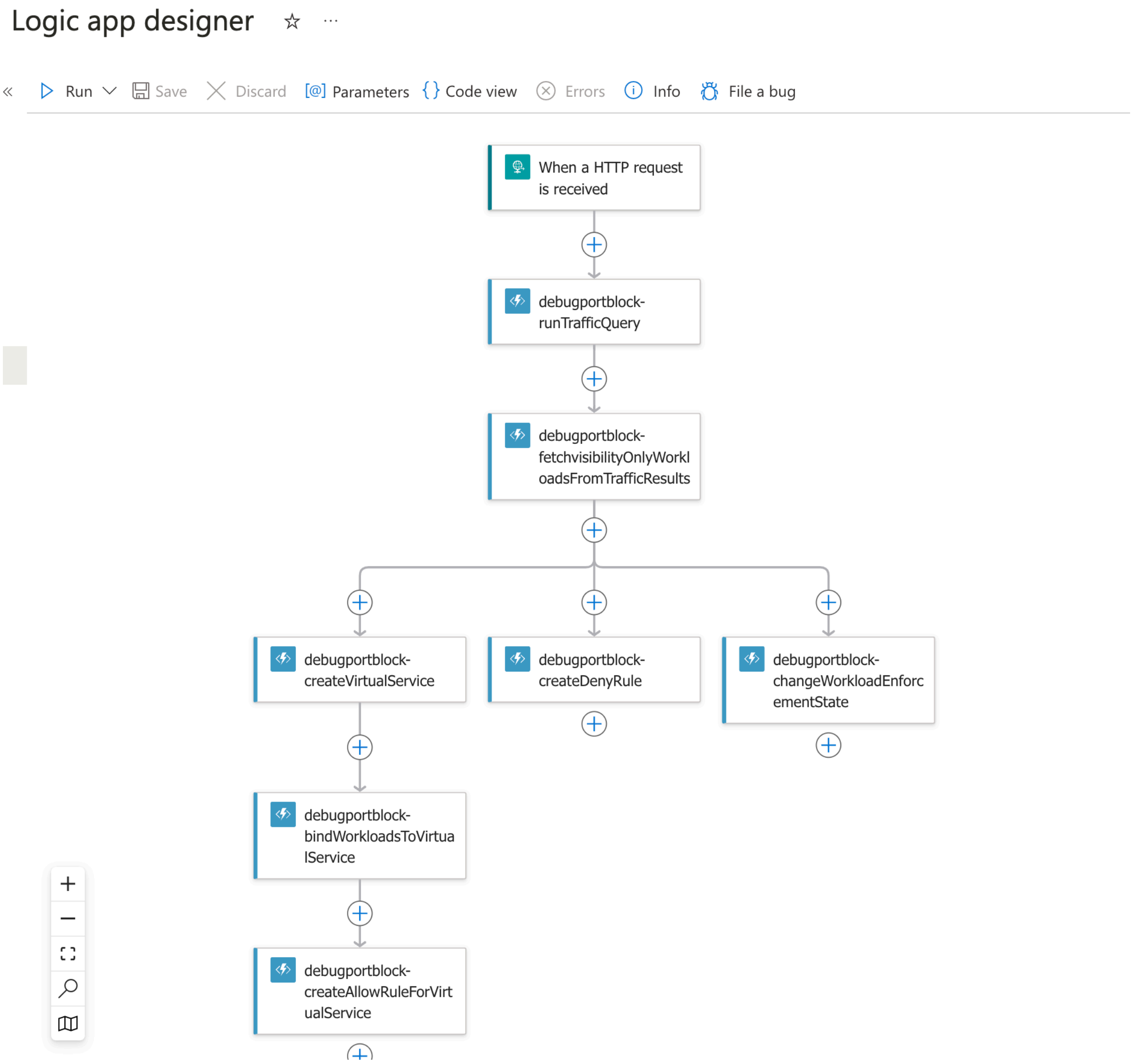
Region * ⓘ	(US) West US 2
Playbook Name ⓘ	Illumio-Port-Blocking-Switch ✓
Function App Name ⓘ	IllumioPortBlockingApp ✓
PCE_FQDN * ⓘ	
PORT * ⓘ	
ORG_ID * ⓘ	
API_KEY * ⓘ	
API_SECRET * ⓘ	

1. Enter the playbook name and function app. (You can modify the name of the playbook and function app to suit your organization.)

2. Enter the PCE FQDN, Org ID, API key, and API secret. These values are required to communicate with the PCE.
3. Click **Next** and follow the wizard steps to deploy the playbook.

After you have deployed the playbook, do the following:

1. Navigate to **Logic Apps** and select the name of the logic app that you set when you deployed the playbook.


Logic app designer
Run
Save
Discard
Parameters
Code view
Errors
Info
File a bug
When a HTTP request is received
debugportblock-runTrafficQuery
debugportblock-fetchvisibilityOnlyWorkloadsFromTrafficResults
debugportblock-createVirtualService
debugportblock-createDenyRule
debugportblock-changeWorkloadEnforcementState
debugportblock-bindWorkloadsToVirtualService
debugportblock-createAllowRuleForVirtualService

2. Execute the logic app in **one** of the following ways:
   - Generate a public URL for the logic app to use Postman to call the endpoint.
   - Within the logic app, select **Run > Run with payload**.

The payload is:

```
{
 "protocol": <   integer>, "port": <integer>, "applyChanges": <boolean>
}
```

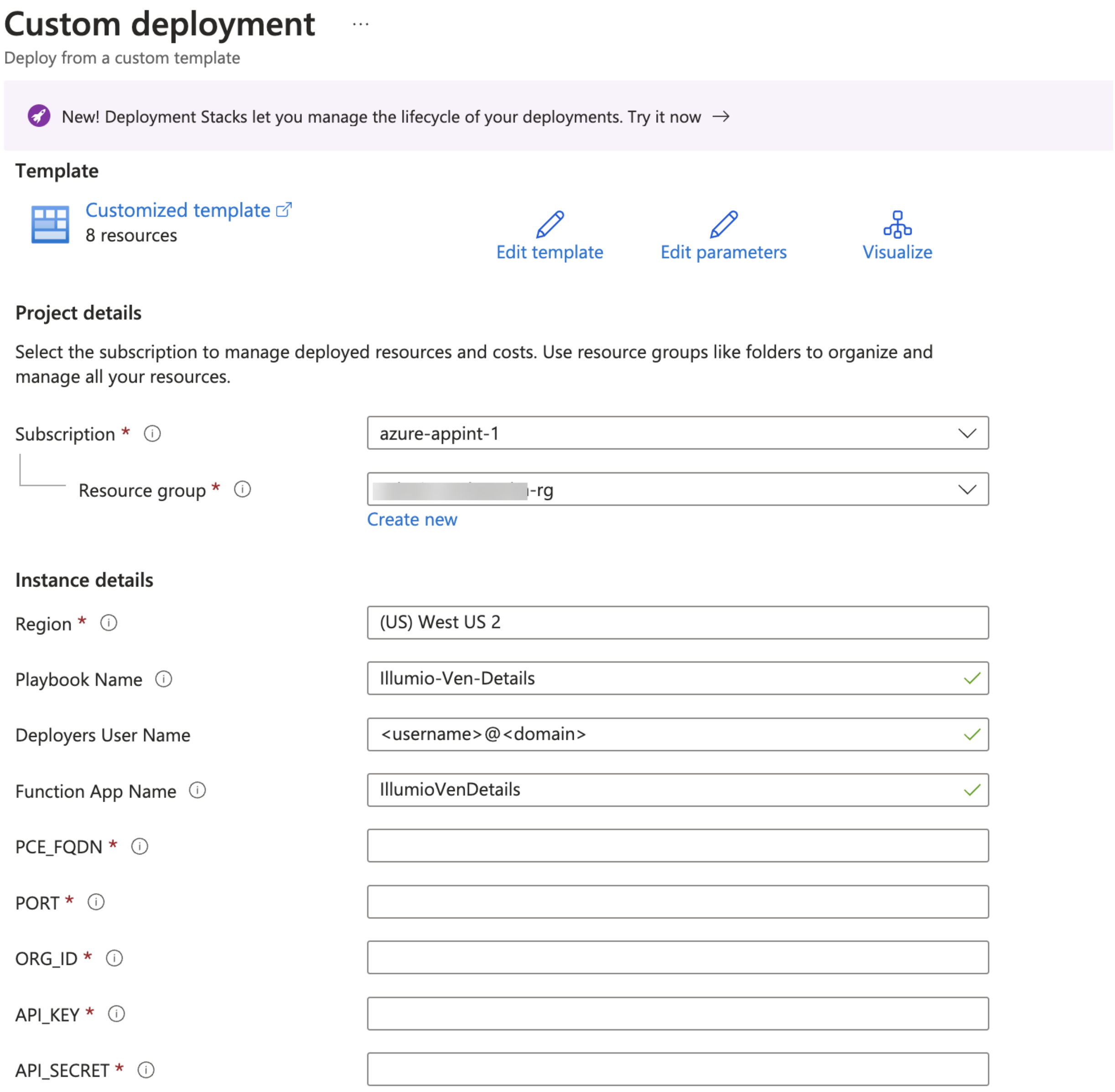
About the Get VEN Details Playbook

This playbook contains a collection of procedures that respond to a Microsoft Sentinel Alert.

1. After an alert is triggered, its body is sent to a function app.
2. The function talks to the PCE using the API key and API secret.
3. After the VEN details are fetched from the PCE, the playbook constructs a table with the relevant information.
4. The table includes the alert title, severity, VEN details like the IP address, hostname and labels, and a description of the alert. The table is sent out in an email.

Deploy the Get VEN Details Playbook

You can deploy the playbook using this ARM template: Illumio Get Ven Details.



Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Template

Customized template

8 resources

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-appint-1
Resource group *	[redacted]-rg

Create new

Instance details

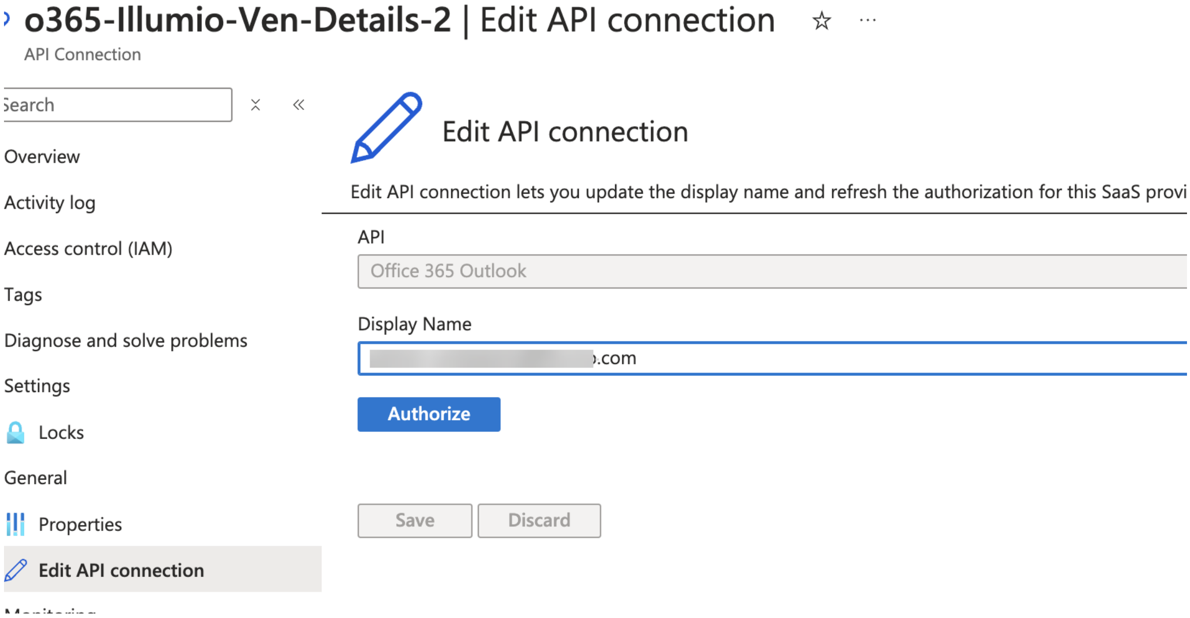
Region *	(US) West US 2
Playbook Name	Illumio-Ven-Details ✓
Deployers User Name	<username>@<domain> ✓
Function App Name	IllumioVenDetails ✓
PCE_FQDN *	
PORT *	
ORG_ID *	
API_KEY *	
API_SECRET *	

This playbook creates API connections, because it needs to query and interact with Outlook 365 and Microsoft Sentinel.

1. Make sure to provide the deployer's user name as the email address.
2. Provide the PCE FQDN, port, Org Id, API key, and API secret, and then click **Next**.
3. Follow the rest of the wizard steps to deploy the playbook.

After you have deployed the playbook, use the following procedure to authorize the API connections:

1. Go to API connections.
2. Ensure that the connections are authorized, as shown in the following screenshot:

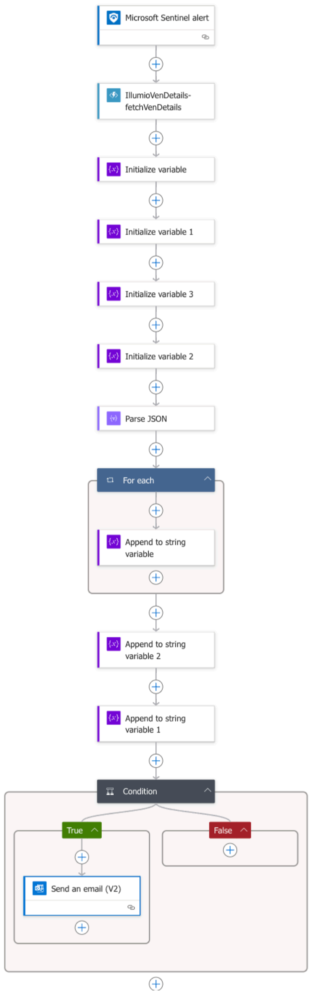


Edit API connection lets you update the display name and refresh the authorization for this SaaS provi

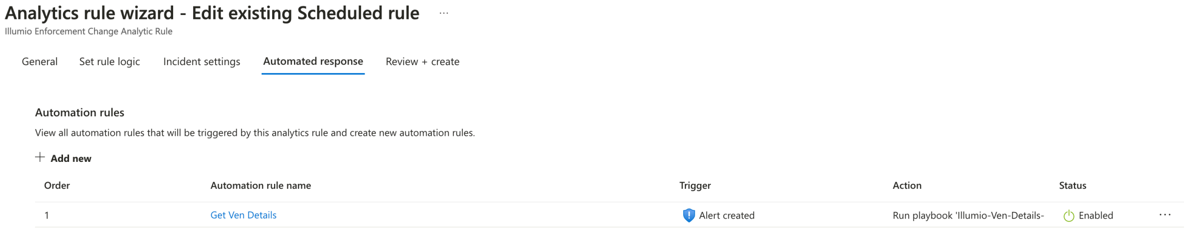
API: Office 365 Outlook

Display Name: [redacted].com

This ensures that the procedures can interact with Microsoft Sentinel and Outlook 365 while the playbook is executing.
3. Go to Logic Apps and navigate to the name of the logic app that was set during deployment.



4. Ensure that API connections are authorized for the playbook to operate correctly.
5. After you have deployed the playbook, you can edit the automated response of any of the analytics rules that are part of the Illumio Sentinel Integration to include the playbook.


Analytics rule wizard - Edit existing Scheduled rule ...

Illumio Enforcement Change Analytic Rule

Automation rules

View all automation rules that will be triggered by this analytics rule and create new automation rules.

Order	Automation rule name	Trigger	Action	Status
1	Get Ven Details	Alert created	Run playbook 'Illumio-Ven-Details-	Enabled

Illumio On-Premises PCE Support for Microsoft Sentinel

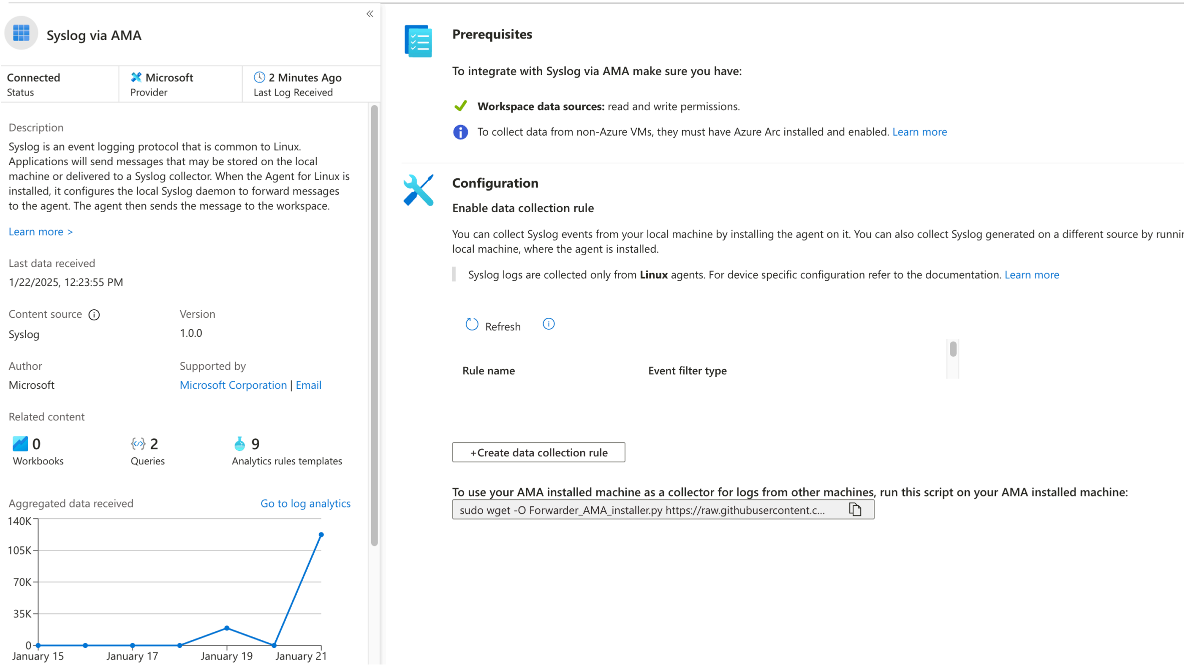
Illumio Sentinel Solution can now receive events from the Illumio On-Premises PCE. All of the Illumio Sentinel Integration features, such as Analytics Rules and Workbooks, now support On-Premises PCE events.

NOTE
Illumio On-Premises PCE version 24.2.10 and later is supported.

Configure the Illumio On-Premises PCE to Forward Events to Illumio Sentinel Solution

Use the following procedure to configure the On-Premises PCE to forward events to Illumio Sentinel Solution.

1. Navigate to **Sentinel** > **Content Hub** > **Install Syslog solution**.
2. After you have installed Syslog solution, install the **Syslog via AMA** data connector.
3. Use one of the following options to forward events:
   - Set up a virtual machine in Azure (Windows or Linux) to collect events and forward them to Sentinel.
   - Set up a system outside of the Azure environment to collect events and forward them to Sentinel.
4. For Virtual Machines, set up an outside Azure environment: Install and Manage the Azure Monitor Agent.
5. While you configure Syslog via AMA, select **Create a data collection rule**. You must create a data collection rule that is separate from the one that you created for the SaaS PCE. After you have created the rule, you can select the VM to collect the events from if the VM is within the Azure environment.



Syslog via AMA

Connected
Status

Microsoft
Provider

2 Minutes Ago
Last Log Received

Description

Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector. When the Agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to the workspace.

Learn more >

Last data received

1/22/2025, 12:23:55 PM

Content source: Syslog

Version: 1.0.0

Author: Microsoft

Supported by: Microsoft Corporation | Email

Related content

0 Workbooks

2 Queries

9 Analytics rules templates

Aggregated data received

Go to log analytics

Prerequisites

To integrate with Syslog via AMA make sure you have:

✓ **Workspace data sources:** read and write permissions.

To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. Learn more

Configuration

Enable data collection rule

You can collect Syslog events from your local machine by installing the agent on it. You can also collect Syslog generated on a different source by runnir local machine, where the agent is installed.

Syslog logs are collected only from **Linux** agents. For device specific configuration refer to the documentation. Learn more

Rule name	Event filter type

To use your AMA installed machine as a collector for logs from other machines, run this script on your AMA installed machine:

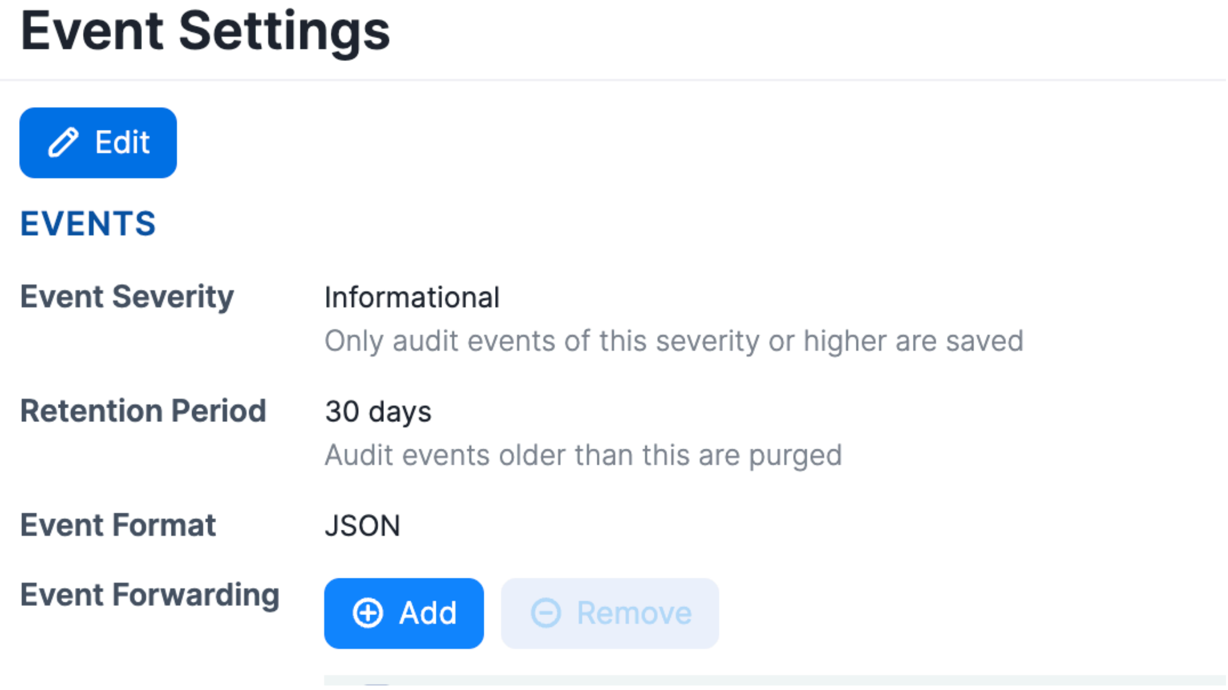
```
sudo wget -O Forwarder_AMA_installer.py https://raw.githubusercontent.c...
```

6. After you create the data collection rule, run the script shown in the preceding image on the VM.
7. Make sure that the data collection rule and the VM are in the same region (such as us-west-2).

Next, you need to configure the PCE.

Configure the PCE for the Illumio Sentinel Solution

- Within the PCE, navigate to **Event Settings**.



Event Settings

EVENTS

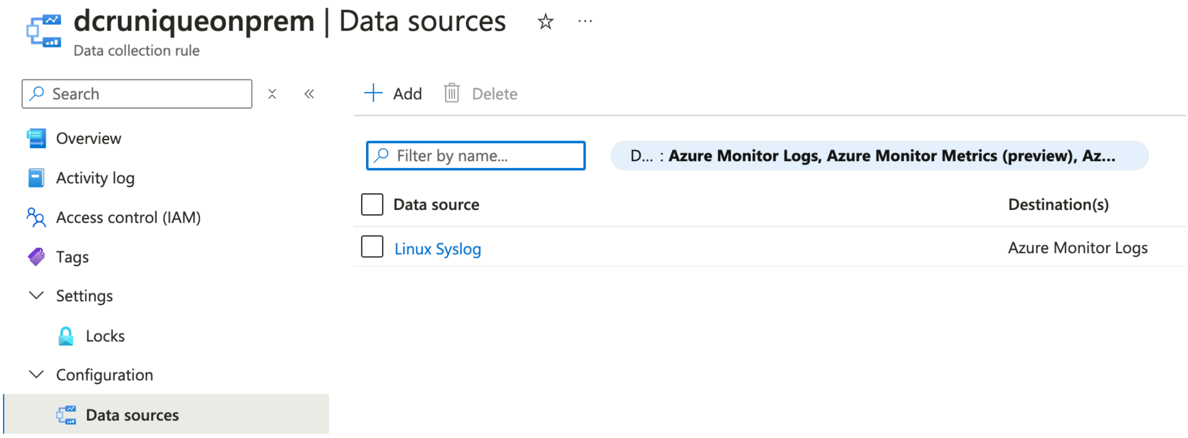
Event Severity: Informational
Only audit events of this severity or higher are saved

Retention Period: 30 days
Audit events older than this are purged

Event Format: JSON

Event Forwarding

1. Select **Add** > **Add Repository**.
2. Input the IP address of the VM and specify the port as 514 TCP.
3. If TLS is enabled, make sure to upload the trusted CA bundle and save the setting. If the PCE can communicate with the VM, then you have successfully saved the setting.
4. Log into the VM using a secure connection and check `/var/log/syslog/<appropriate directory for your OS>` to see the events that the PCE is forwarding.
5. Next, make sure that the data collection rule has a virtual machine selected under **Resources** and that **Linux Syslog** is a data source:

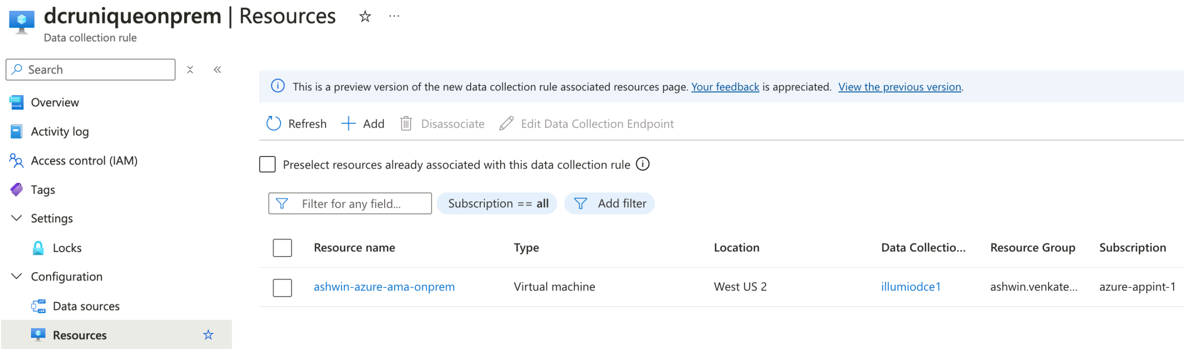


dcruniqueonprem | Data sources ☆ ···

Data collection rule

D... : **Azure Monitor Logs, Azure Monitor Metrics (preview), Az...**

□ Data source	Destination(s)
□ Linux Syslog	Azure Monitor Logs



dcruniqueonprem | Resources ☆ ···

Data collection rule

This is a preview version of the new data collection rule associated resources page. Your feedback is appreciated. View the previous version.

□ Preselect resources already associated with this data collection rule ⓘ

□	Resource name	Type	Location	Data Collectio...	Resource Group	Subscription
□	ashwin-azure-ama-onprem	Virtual machine	West US 2	illumiodce1	ashwin.venkate...	azure-appint-1

6. After you configure event forwarding to **Syslog via AMA**, do the following:
   a. Navigate to **Sentinel** > **Lo**gs.
   b. Run the following query:

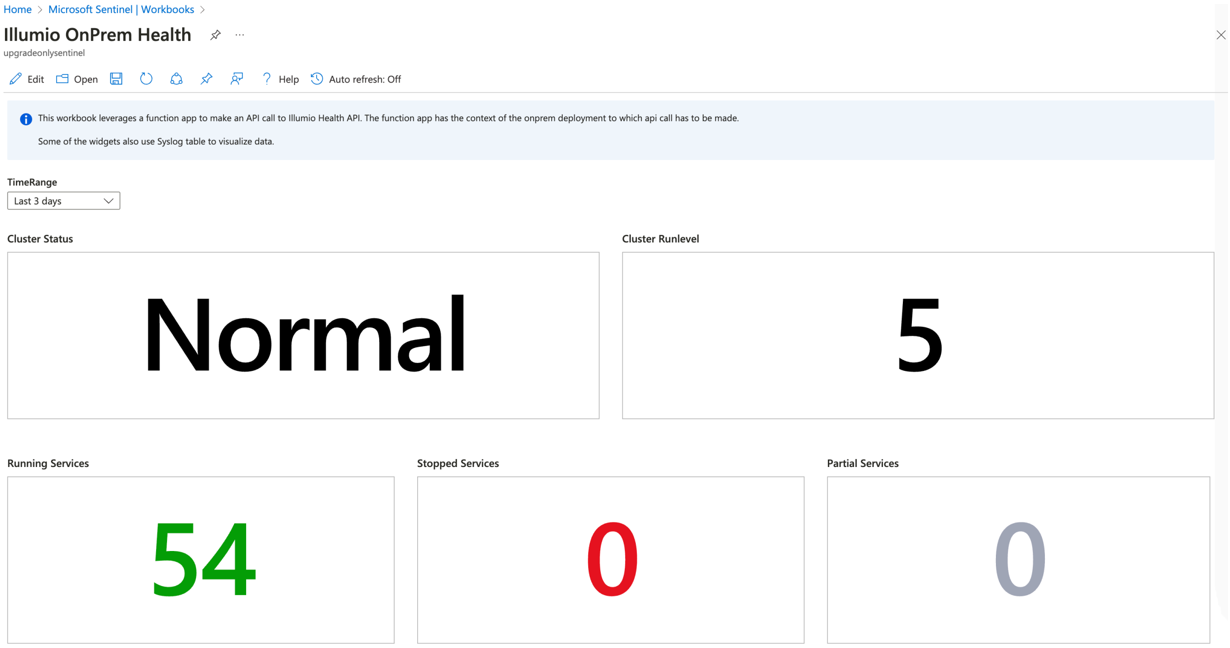
```
Syslog
| where SyslogMessage has 'illumio_pce/agent'

Syslog
| where SyslogMessage has 'illumio_pce/collector'
```

NOTE

Version 3.4.0 includes two new parsers, **IllumioSyslogAuditEvents** and **IllumioSyslogNetworkTrafficEvents**. These parsers are part of workspace functions.

About the Illumio OnPrem Health Workbook

This workbook provides a summary of the PCE's health. It also contains sections about **Disk Latency**, **Traffic Ingestion Stats**, **VEN Heartbeat Stats**, **VEN Policy Stats**, **Traffic Database Summary**, and **Policy Database Summary**, as shown in the following figure:



This workbook leverages a function app to make an API call to Illumio Health API. The function app has the context of the onprem deployment to which api call has to be made.

Some of the widgets also use Syslog table to visualize data.

TimeRange: Last 3 days

Cluster Status: Normal

Cluster Runlevel: 5

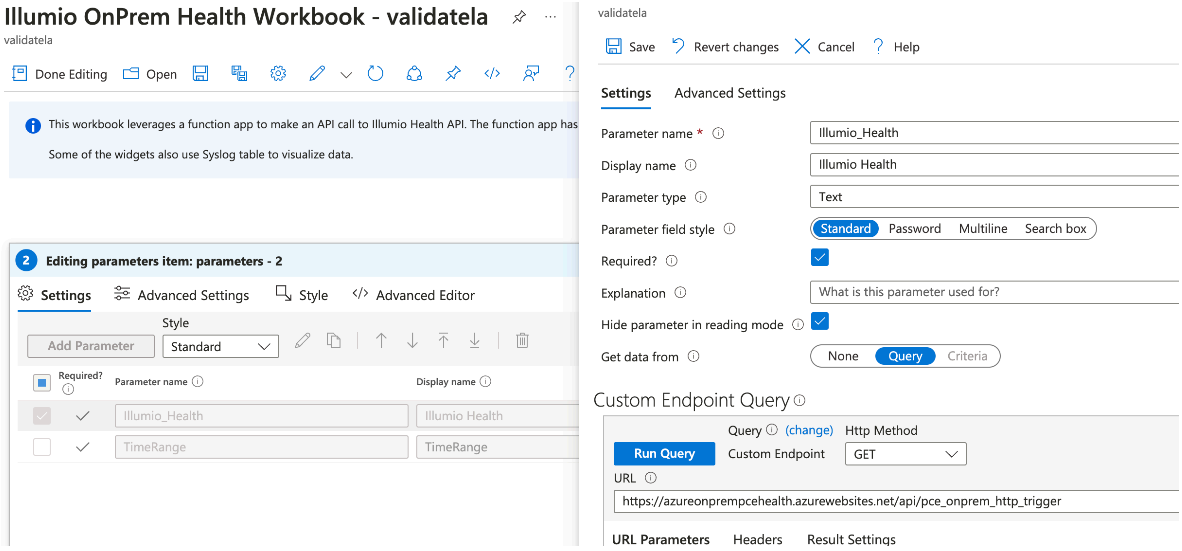
Running Services: 54

Stopped Services: 0

Partial Services: 0

The workbook uses a function app to make HTTP requests to the PCE, so configure the workbooks to invoke a custom HTTP endpoint:

1. Open the OnPrem Health workbook and click Edit next to the Illumio Health parameter.
2. Select the Illumio_Health parameter and click the edit (pencil) icon.



This workbook leverages a function app to make an API call to Illumio Health API. The function app has

Some of the widgets also use Syslog table to visualize data.

Style: Standard

Required?	Parameter name	Display name
✓	Illumio_Health	Illumio Health
✓	TimeRange	TimeRange

Parameter name *: Illumio_Health

Display name: Illumio Health

Parameter type: Text

Parameter field style: [✓ Standard] Password Multiline Search box

Required?: ☑

Explanation: What is this parameter used for?

Hide parameter in reading mode: ☑

Get data from: None [✓ Query] Criteria

Custom Endpoint Query

Query (change): Custom Endpoint

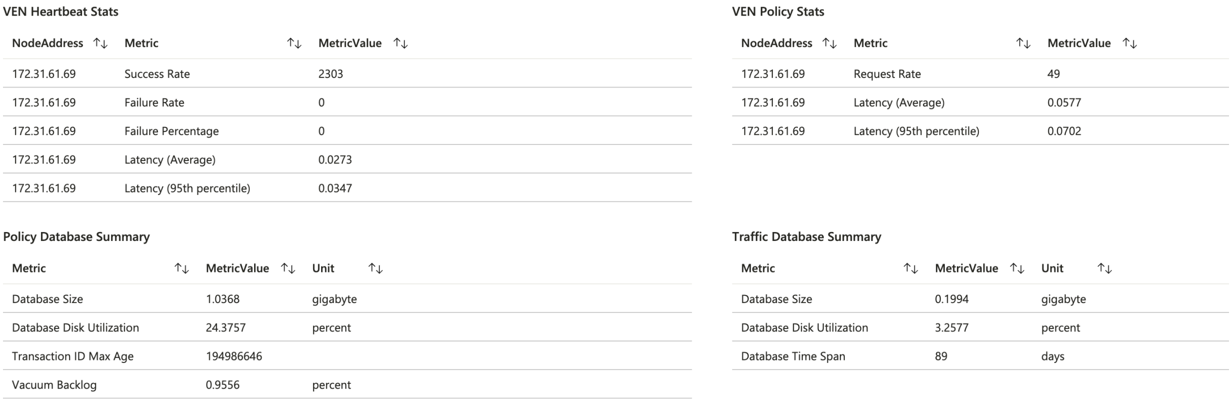
Http Method: GET

URL: https://azureonprempcehealth.azurewebsites.net/api/pce_onprem_http_trigger

3. Edit the **Custom Endpoint Query** URL to point to the HTTP trigger in the function app that has been deployed:
   a. Navigate to the function app and select **OnPremHealthFunctionApp**.
   b. Select **Get Function App**, copy the URL, and replace the value in the URL field for **Custom Endpoint Query**.

Every time the workbook refreshes or reloads, it will invoke the HTTP trigger function and make the API call to pull the Illumio_Health information from the PCE.

The Illumio OnPrem Health workbook provides a summary of the health of the PCE. It also contains sections for **Disk Latency**, **Traffic Ingestion Stats**, **VEN Heartbeat Stats**, **VEN Policy Stats**, **Traffic Database Summary**, and **Policy Database Summary** sections.



VEN Heartbeat Stats

NodeAddress	Metric	MetricValue
172.31.61.69	Success Rate	2303
172.31.61.69	Failure Rate	0
172.31.61.69	Failure Percentage	0
172.31.61.69	Latency (Average)	0.0273
172.31.61.69	Latency (95th percentile)	0.0347

VEN Policy Stats

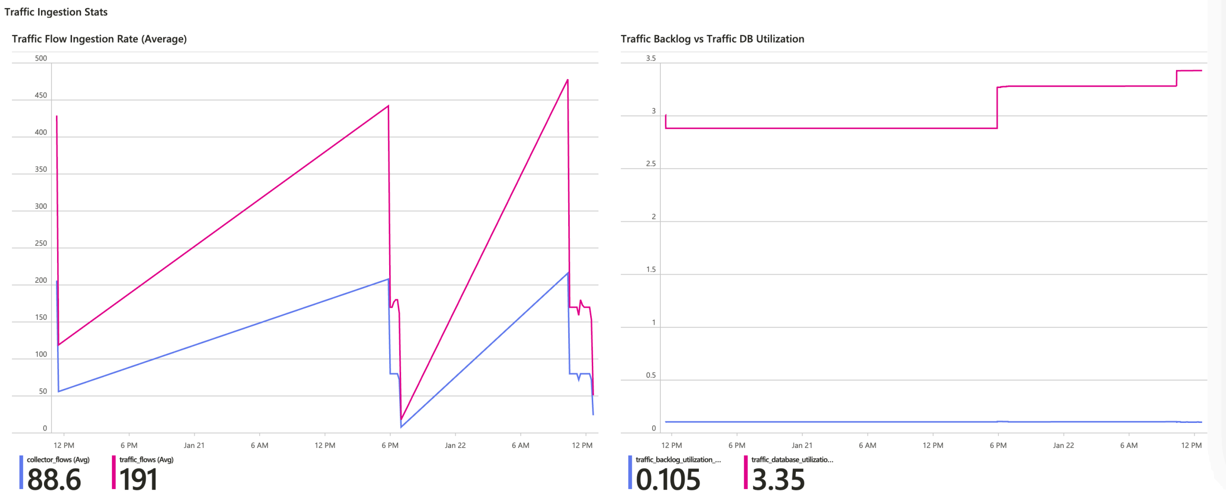
NodeAddress	Metric	MetricValue
172.31.61.69	Request Rate	49
172.31.61.69	Latency (Average)	0.0577
172.31.61.69	Latency (95th percentile)	0.0702

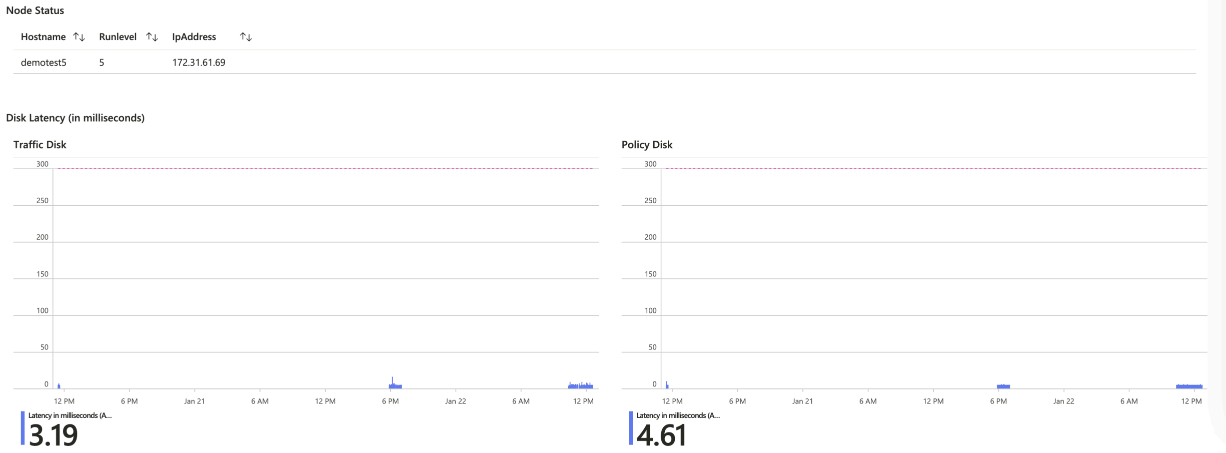
Policy Database Summary

Metric	MetricValue	Unit
Database Size	1.0368	gigabyte
Database Disk Utilization	24.3757	percent
Transaction ID Max Age	194986646	
Vacuum Backlog	0.9556	percent

Traffic Database Summary

Metric	MetricValue	Unit
Database Size	0.1994	gigabyte
Database Disk Utilization	3.2577	percent
Database Time Span	89	days

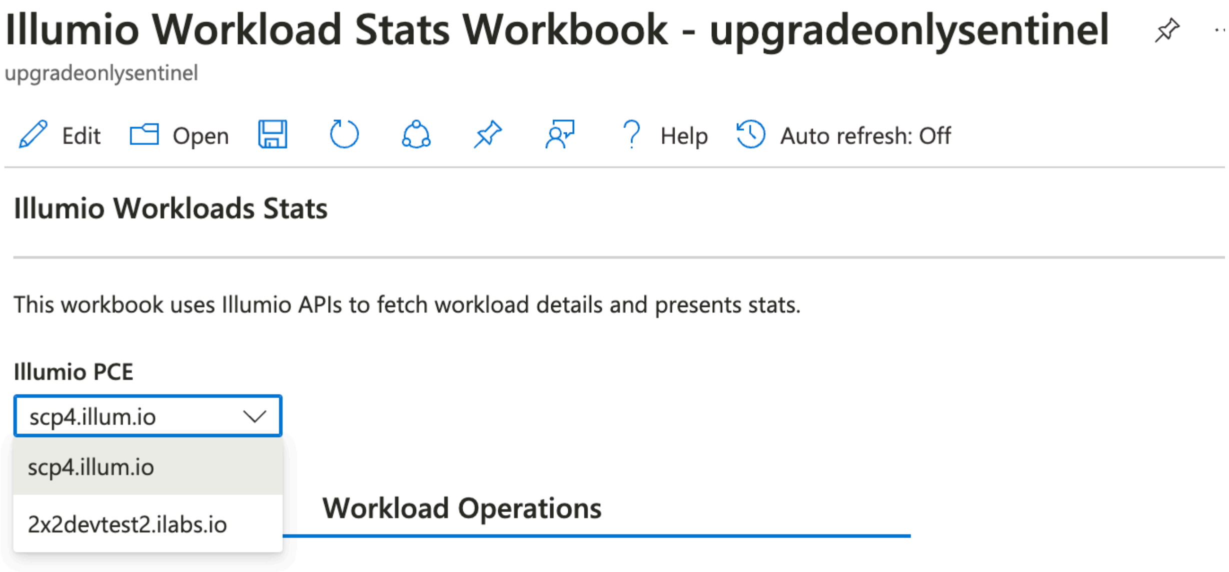




Node Status

Hostname	Runlevel	IpAddress
demotest5	5	172.31.61.69

All workbooks now include a drop-down list to select which PCE you want to load the stats for.



Illumio Workload Stats Workbook - upgradeonlysentinel

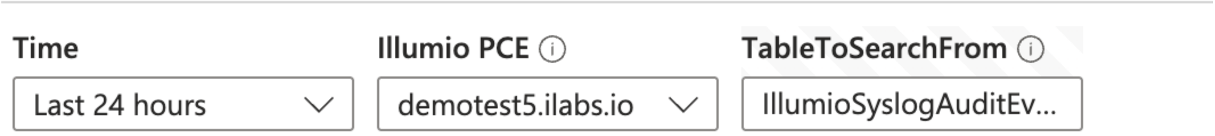
upgradeonlysentinel

Illumio Workloads Stats

This workbook uses Illumio APIs to fetch workload details and presents stats.

Illumio PCE: scp4.illum.io

A hidden parameter has also been added to each workbook to help you decide which table should be parsed for events at runtime.



Time: Last 24 hours

Illumio PCE: demotest5.ilabs.io

TableToSearchFrom: IllumioSyslogAuditEv...

Changes to the Function App

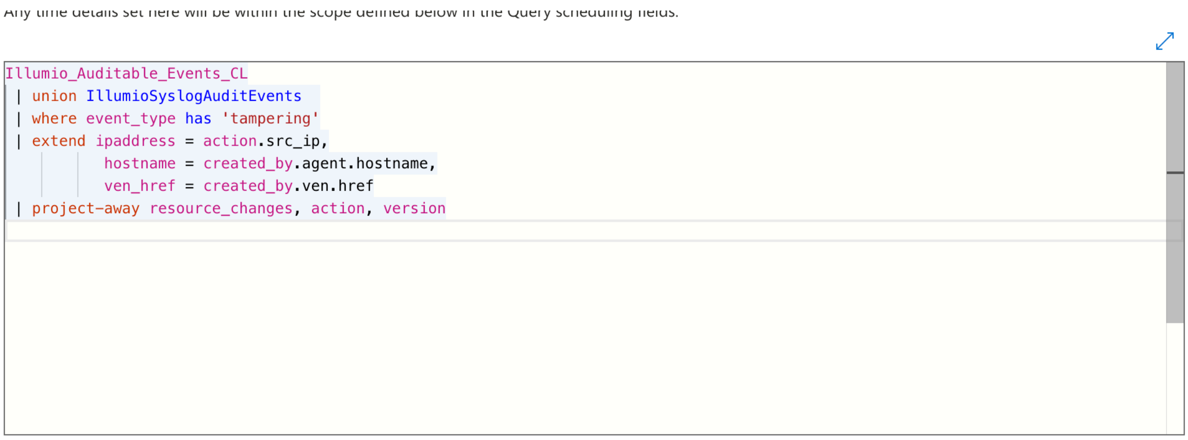
To add context to the PCE, add the following environment variables to the function app:

```
ONPREM_API_KEY
ONPREM_API_SECRET
ONPREM_PCE_FQDN
ONPREM_PCE_ORGID
ONPREM_PCE_PORT
Ex:
ONPREM_API_KEY: <api_>
ONPREM_API_SECRET: <secret>
ONPREM_PCE_FQDN: <devtest0.ilabs.io>
ONPREM_PCE_ORGID: 1ONPREM_PCE_PORT: 443
```

Note that each workbook now has a selector for PCE FQDN. For example, if you have an On-Premises PCE and a SaaS PCE, you can use either PCE instance to view stats. The logic for choosing the relevant PCE is fetched from the Illumio_Workloads_Summarized_API_CL custom table. The TimedApiFunctionApp updates this table every hour. If this table is empty and you want to see the workbooks right away, you can force the function to run manually to update the table. After that, the workbook widgets should display data.

Changes to Analytics Rules

As of version 3.4.0, each Analytics Rule can query both syslog and custom tables for events and then raise incidents.



Any time details set here will be within the scope defined below in the Query scheduling fields.

```
Illumio_Auditable_Events_CL
 | union IllumioSyslogAuditEvents
 | where event_type has 'tampering'
 | extend ipaddress = action.src_ip,
          hostname = created_by.agent.hostname,
          ven_href = created_by.ven.href
 | project-away resource_changes, action, version
```

Troubleshooting Sentinel

To monitor or troubleshoot function app executions, use the queries in the following sections:

Verify Data Ingestion with the Logs Ingestion API

Use the following steps to verify if data is being ingested with the Logs Ingestion API.

1. Search for metrics in portal.azure.com.
2. Open a new workbook and set the resource type to **Data Collection Rules**.
3. Select the data collection rule that has been configured for the function app.
4. Select the metrics that you want to monitor.
5. Adjust the time range and click **Run Metrics** to provide a graph of the activity so far.

If the graph is a flat line that indicates no activity, verify that the time range that you selected is correct.

Verify that the Data Collection Rule has been provided with the necessary permissions and that you have waited for at least 45 minutes after provisioning the rule.

Query for Errors in Function App Execution

If there are errors with function app execution, do the following:

1. Go to function app > logs.
2. Select a time range and type in the following queries:

```
a. traces | where message has 'Error'
b. exceptions
```

- If exceptions list 403 for QueueTrigger, then it's a permission error on the Data Collection Rule where permissions may not have been set properly or they have been set but are still being applied.
- If exceptions list 401 for TimedAPIFunctionApp, then it's an authorization error. If the API key or secret is incorrect, then the function will complain with a 401 error.
- If exceptions list 404 for QueueTrigger/QueueManager and the message lists the "python-queue-items" and "python-queue-items-backlog" queues, this means that there are no

messages in the queues yet and this function is polling them to find out if there are any messages

Monitor Messages from the SQS Function

Look for the following to monitor messages from the SQS function:

```
Suppose queue is empty,
logging.info("[AWSQueue] There are no messages in SQS, attempting to
enqueue files
seen so far"
```

```
Suppose function has run >=90% of allotted time, then
logging.warn('[AWSQueue]SQS Queue manager has run close to 90 percentage of
max time.
Flushing files to queue before termination')
```

```
Suppose event file is skipped,
logging.warn('[AWSQueue] Skipping file since logs to be consumed is {}, but
file is
{}'.format(LOGS_TO_CONSUME, file_path))
```

```
Suppose a read limit is reached, then
logging.warn('[AWSQueue] Have processed {} files and hence exiting'.format
(files_processed))Suppose event file is skipped,
logging.warn('[AWSQueue] Skipping file since logs to be consumed is {},
but file is {}'.format(LOGS_TO_CONSUME, file_path))
```

Monitor Event Ingestion with QueueTrigger Logs

Use the following to monitor event ingestion with QueueTrigger logs:

```
{"Trigger":"Queue", "Type":"event_stats", "total_events": total_events,
 "sqs_ids_seen_so_far": sqs_ids_seen_so_far, "aggregated_file_size":
  accumulated_file_size}
{"Trigger":"Queue", "stream_name":stream_name, "Type":"file_stats", "link":
link,
 "bucket": bucket, "sqs_message_id": messageId, "file_size_bytes":
file_size}
```

Use traces or AppTraces to monitor for the preceding messages.

Use this example query that lists all the SQS ids seen so far:

```
AppTraces
| where  OperationName has 'QueueTriggerFuncApp' and Message
has 'event_stats'
| extend event_stats = parse_json(Message)
| project total_events = toint(event_stats.total_events),
aggregated_file_size_in_bytes
 = toint(event_stats.aggregated_file_size), file_count =
  toint(event_stats.sqs_ids_seen_so_far)
| summarize total_events = sum(total_events), total_bytes_ingested_in_bytes
=
 sum(aggregated_file_size_in_bytes), total_sqs_processed = sum(file_count)
| extend TotalMegabytesIngested =
total_bytes_ingested_in_bytes / 1024.0 / 1024.0
| project total_events, TotalMegabytesIngested, total_sqs_processed

AppTraces
| where OperationName has 'QueueTriggerFuncApp' and Message
has 'event_stats'
| extend event_stats = parse_json(Message)
| project
  total_events = toint(event_stats.total_events),
  aggregated_file_size_in_bytes = toint(event_stats.aggregated_file_size),
  sqs_count = toint(event_stats.sqs_ids_seen_so_far),
  _ResourceId
| summarize
  total_events = sum(total_events),
  total_bytes_ingested_in_bytes =
sum(aggregated_file_size_in_bytes)/ 1024.0 / 1024.0,
  total_files_processed = sum(sqs_count)
by _ResourceId
```

Verify That AWS Credentials Can Access SQS

If users have provided the correct inputs and TimedSQSFunctionApp is throwing permissions errors or a 404 error about accessing the SQS URL, then use the following commands:

```
export AWS_ACCESS_KEY_ID=''
export AWS_SECRET_ACCESS_KEY=''
export AWS_REGION=''

aws sqs get-queue-attributes --queue-url <QUEUE_URL> --attribute-names
ApproximateNumberOfMessages

aws sqs receive-message --queue-url <QUEUE_URL>
```

Verify That the Connection Works As Expected

If `TimedApiFunctionApp` throws errors, verify that the connection is working as expected and that the API key, API secret, FQDN, Org ID, and port are correct. Use the following curl command to the endpoint:

```
https://<pce_fqdn>.ilabs.io:<port>/api/v2/health
```

Monitor Skipped Network Traffic Messages

For example, if networkTrafficLogTypes has been set to blocked and allowed, TimedSQSFunctionApp will log the following messages:

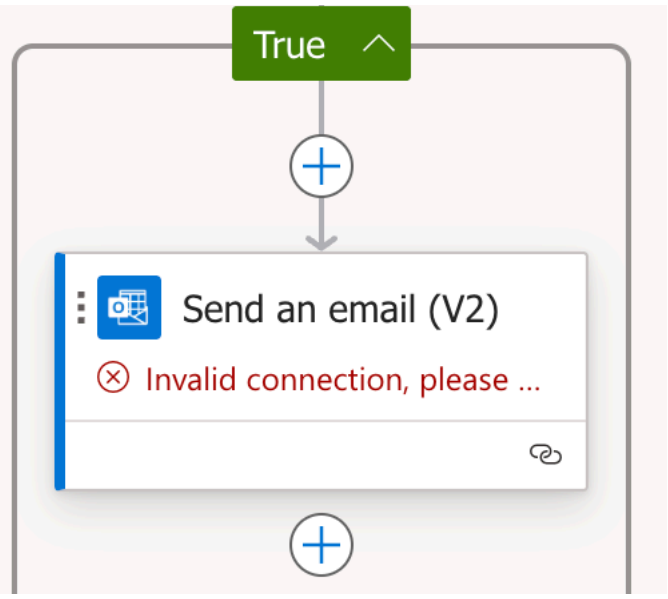
```
traces | where message has 'Skipping network traffic'

"[AWSQueue] Skipping network traffic file since logs to be consumed is
blocked,allowed but file is <sqs file link>"
```

Troubleshooting Playbooks

Use the information in the following topics to troubleshoot the playbooks.

Playbook Lists an Invalid Connection

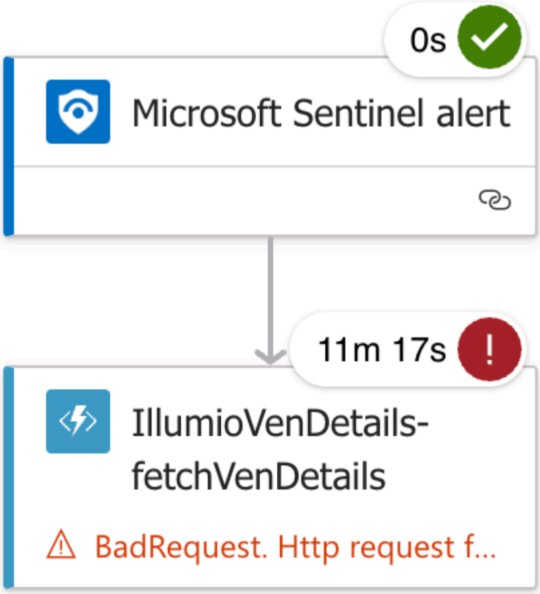
If the playbook lists an invalid connection, ensure that the API connection is authorized. After it is authorized, refresh the logic app and the "Invalid connection" error message should not display anymore.



Invalid connection, please ...

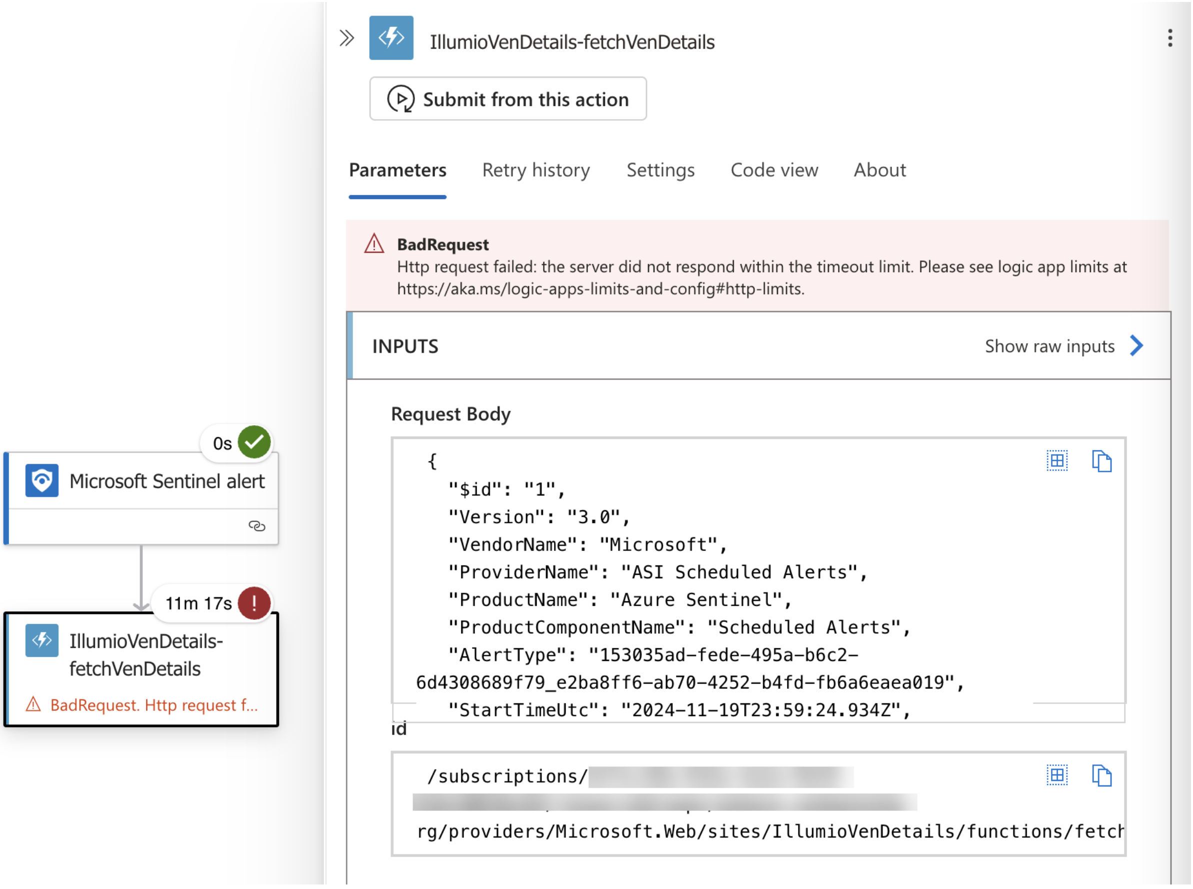
Execution of Procedure in Workflow Stuck

If the execution of a procedure in a workflow is stuck, identify the inputs to that procedure.



BadRequest. Http request f...

In this example, you would click the **fetchVenDetails** box to view the inputs for **fetchVenDetails** to get additional information.



BadRequest. Http request f...

BadRequest
Http request failed: the server did not respond within the timeout limit. Please see logic app limits at https://aka.ms/logic-apps-limits-and-config#http-limits.

```
{
  "$id": "1",
  "Version": "3.0",
  "VendorName": "Microsoft",
  "ProviderName": "ASI Scheduled Alerts",
  "ProductName": "Azure Sentinel",
  "ProductComponentName": "Scheduled Alerts",
  "AlertType": "153035ad-fede-495a-b6c2-
6d4308689f79_e2ba8ff6-ab70-4252-b4fd-fb6a6eaea019",
  "StartTimeUtc": "2024-11-19T23:59:24.934Z",
```

```
/subscriptions/[redacted]
rg/providers/Microsoft.Web/sites/IllumioVenDetails/functions/fetch
```

Public Access to Storage Account Disabled

If public access to the storage account is disabled, you need to configure the function app to talk to the storage account using a private network. See Configure a Private Network [24] for more information.

Troubleshooting On-Premises PCE Support for Sentinel

Use the information in the following topics to troubleshoot On-Premises PCE support for Sentinel.

Troubleshooting Linux or Windows Virtual Machines

Use the following information to troubleshoot Linux or Windows VMs.

- How to use the Linux operating system (OS) Azure Monitor Agent Troubleshooter
- How to use the Windows operating system (OS) Azure Monitor Agent Troubleshooter
- Syslog troubleshooting guide for Azure Monitor Agent for Linux
- Troubleshooting guidance for the Azure Monitor agent on the Windows Arc-enabled server

Check the Health of the Agents Sending Data to Your Workspace

Run this query to list the VMs that haven't reported a heartbeat in the last five minutes:

```
Heartbeat
| where TimeGenerated > ago(24h)
| summarize LastCall = max(TimeGenerated) by Computer, _ResourceId
| where LastCall < ago(5m)
```

Check the Data Recorder Association with a Virtual Machine

NOTE

This procedure applies to a Linux VM.

1. Navigate to `/etc/microsoft/azuremonitoragent/config-cache/configchunks`.
2. If the data collection rule has been associated correctly, there will be a .json file in the directory.
3. After the contents are categorized, the output will contain:

```
{"dataSources":[{"configuration":{"facilityNames":
["local5","local6","local7"],"logLevels":
["Info","Notice","Warning","Error","Critical","Alert","Emergency"]},"id":
"sysLogsDataSource--1469397783","kind":"syslog","streams":
```

```
[{"stream":"LINUX_SYSLOGS_BLOB","solution":"LogManagement"}],"sendToChann
els":["ods-153035ad-fede-495a-b6c2-6d4308689f79"]}],"channels":
[{"endpoint":"https://153035ad-fede-495a-
b6c2-6d4308689f79.ods.opinsights.azure.com","tokenEndpointUri":"https://
illumiodce1-515u.westus2-1.handler.control.monitor.azure.com/
subscriptions/427ec20a-816a-4a2a-9b28-61b13053bc83/resourceGroups/
ashwin.venkatesha-rg/providers/Microsoft.Compute/virtualMachines/ashwin-
azure-ama-onprem/agentConfigurations/
dcr-438cd9d794af4d34be6c6c9a19f5367b/channels/ods-153035ad-fede-495a-
b6c2-6d4308689f79/issueIngestionToken?
operatingLocation=westus2&platform=linux&includeMeConfig=true&api-
version=2022-06-02","id":"ods-153035ad-fede-495a-
b6c2-6d4308689f79","protocol":"ods"}]}
```

Environment Variables for the Function App

You can use the following environment variables to modify how the function app works.

```
[
 {
   "name": "API_KEY",
   "value": "<key>",
   "slotSetting": false
  },
  {
    "name": "API_SECRET",
    "value": "<secret>",
    "slotSetting": false
  },
  {
    "name": "APPINSIGHTS_INSTRUMENTATIONKEY",
    "value": "<key>",
    "slotSetting": false
  },
  {
   "name": "APPLICATIONINSIGHTS_CONNECTION_STRING",
   "value": "<string>",
   "slotSetting": false
  },
  {
   "name": "AUDIT_LOGS_CUSTOM_TABLE",
   "value": "Custom-Illumio_Auditable_Events_CL",
   "slotSetting": false
  },
  {
   "name": "AWS_KEY",
   "value": "<key>",
   "slotSetting": false
  },
  {
   "name": "AWS_REGION_NAME",
   "value": "<region>",
   "slotSetting": false
  },
  {
    "name": "AWS_SECRET",
    "value": "<secret>",
    "slotSetting": false
  },
  {
    "name": "AZURE_CLIENT_ID",
    "value": "<client-id from entra app>",
    "slotSetting": false
  },
  {
      "name": "AZURE_CLIENT_SECRET",
      "value": "<secret from entra>",
      "slotSetting": false
    },
    {
      "name": "AZURE_TENANT_ID",
      "value": "<tenant id from entra>",
      "slotSetting": false
    },
    {
      "name": "AzureWebJobs.Replicator.Disabled",
      "value": "1",
      "slotSetting": false
    },
    {
      "name": "AzureWebJobsStorage",
      "value": "DefaultEndpointsProtocol=https;AccountName=
       illumiostorage;AccountKey=<key>;
       EndpointSuffix=core.windows.net",
      "slotSetting": false
    },
    {
      "name": "DCE_ENDPOINT",
      "value": "<dce endpoint>",
      "slotSetting": false
    },
    {
      "name": "DCR_ID",
      "value": "<dcr_id>",
      "slotSetting": false
    },
    {
      "name": "FLOW_LOGS_CUSTOM_TABLE",
      "value": "Custom-Illumio_Flow_Events_CL",
      "slotSetting": false
    },
    {
      "name": "FUNCTIONS_EXTENSION_VERSION",
      "value": "~4",
      "slotSetting": false
    },
    {
      "name": "FUNCTIONS_WORKER_RUNTIME",
      "value": "python",
      "slotSetting": false
    },
    {
      "name": "LOG_ANALYTICS_URI",
      "value": "<LA url>",
      "slotSetting": false
    },
    {
      "name": "logTypes",
      "value": "All",
      "slotSetting": false
```

```
},
{
  "name": "MAX_QUEUE_MESSAGES_MAIN_QUEUE",
  "value": "150",
  "slotSetting": false
},
{
  "name": "MAX_SCRIPT_EXEC_TIME_MINUTES",
  "value": "60",
  "slotSetting": false
},
{

  "name": "networkTrafficLogTypes",
  "value": "all",
  "slotSetting": false
},
{
  "name": "ORG_ID",
  "value": "8",
  "slotSetting": false
},
{
   "name": "PCE_FQDN",
   "value": "<fqdn>",
   "slotSetting": false
},
{
   "name": "PCE_PORT",
   "value": "443",
   "slotSetting": false
},
{
  "name": "SCHEDULE_AWS_SQS",
  "value": "0 */5 * * * *",
  "slotSetting": false
},
{
  "name": "SCHEDULE_AZURE_QUEUE_MANAGER",
  "value": "0 */5 * * * *",
  "slotSetting": false
},
{
  "name": "SCHEDULE_ILLUMIO_API_POLLING",
  "value": "0 */2 * * * *",
  "slotSetting": false
},
{
  "name": "SQS_FILES_READ_LIMIT",
  "value": "200",
  "slotSetting": false
},
{
  "name": "SQS_QUEUE_URL",
  "value": "<sqs url>",
    "slotSetting": false
  },
  {
    "name": "WEBSITE_RUN_FROM_PACKAGE",
    "value": "<package zip>",
    "slotSetting": false
  },
  {
    "name": "WORKLOADS_API_LOGS_CUSTOM_TABLE",
    "value": "Custom-Illumio_Workloads_Summarized_API_CL",
    "slotSetting": false
  },
  {
    "name": "WORKSPACE_ID",
    "value": "<workspace id>",
    "slotSetting": false
  }
]
```

SCHEDULE_ILLUMIO_API_POLLING: This is a cron schedule that defines how frequently the Illumio API should be polled.

SCHEDULE_AZURE_QUEUE_MANAGER: This is a cron schedule that defines how frequently the Azure Queue Manager should run.

SCHEDULE_AWS_SQS: This is a cron schedule that defines how frequently AWS SQS should be polled for new messages.

SQS_FILES_READ_LIMIT: This is a limit that defines how many messages can be consumed for each execution of TimedSQSFunctionApp. If the function app is the "premium" type, add the `AzureFunctionsJobHost__functionTimeout` environment variable and assign -1 as its value. For the consumption app, the maximum duration an app can run for is 10 minutes, but for the premium app, you can override this value.