

VOTIRO<sup>✓</sup>

Votiro SaaS

# Knowledge Base

**March 2025**

## Copyright Notice

The material herein is proprietary to Votiro CyberSec Ltd. This document is for informative purposes. Any unauthorized reproduction, use or disclosure of any part of this document is strictly prohibited.

Votiro CyberSec's name and logos are trademarks of Votiro CyberSec Ltd., its subsidiaries or affiliates. All other company or product names are the trademarks of their respective holders.

[www.votiro.com](http://www.votiro.com)

# Contents

<b>1 How to Integrate Azure AD Single Sign-on with Votiro using SAML Toolkit</b>	<b>4</b>
1.1 Prerequisites	4
1.2 Procedure	4
<b>2 How to Integrate SIEM with Azure Sentinel</b>	<b>12</b>
2.1 System prerequisites	12
2.2 Procedure	12
2.2.1 Manual/Offline Deployment	12
<b>3 How to Send Files to Votiro via Postman</b>	<b>24</b>
3.1 Prerequisites	24
3.2 Procedure	24
3.2.1 Generating a Service Token	24
3.2.2 Postman Setup	28
<b>4 How to Use Kibana to Troubleshoot Votiro Incidents</b>	<b>35</b>
4.1 Example of Votiro Incident	35
4.2 Procedure	35
4.2.1 Create and Configure an Index Pattern	35
4.3 Analyze the Data	37
4.3.1 Discover	38
4.3.2 Votiro Explore Incident & File Info	42
4.3.3 File Sanitization Analysis	42
<b>5 MSSP User Guide</b>	<b>45</b>
5.1 MSSP Tenant Management	45
5.2 Monitoring Tenant Activity	51
<b>6 How to Use QR Code Sanitization</b>	<b>53</b>
6.1 Disarm QR Codes behavior	53
6.2 Votiro Administrator view	58

# 1 How to Integrate Azure AD Single Sign-on with Votiro using SAML Toolkit

In this tutorial, you'll learn how to integrate Azure AD single sign-on with Votiro using SAML Toolkit to enable users to log in to the Votiro Management console using their corporate credentials.

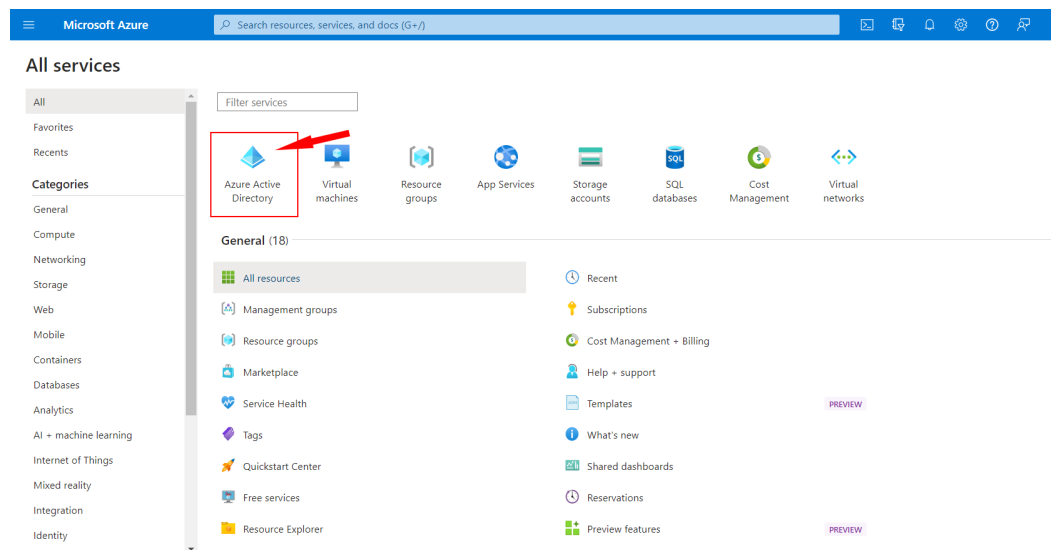
## 1.1 Prerequisites

Ensure you have the following items:

- Azure AD subscription
- Azure AD SAML Toolkit enabled on the above-mentioned subscription

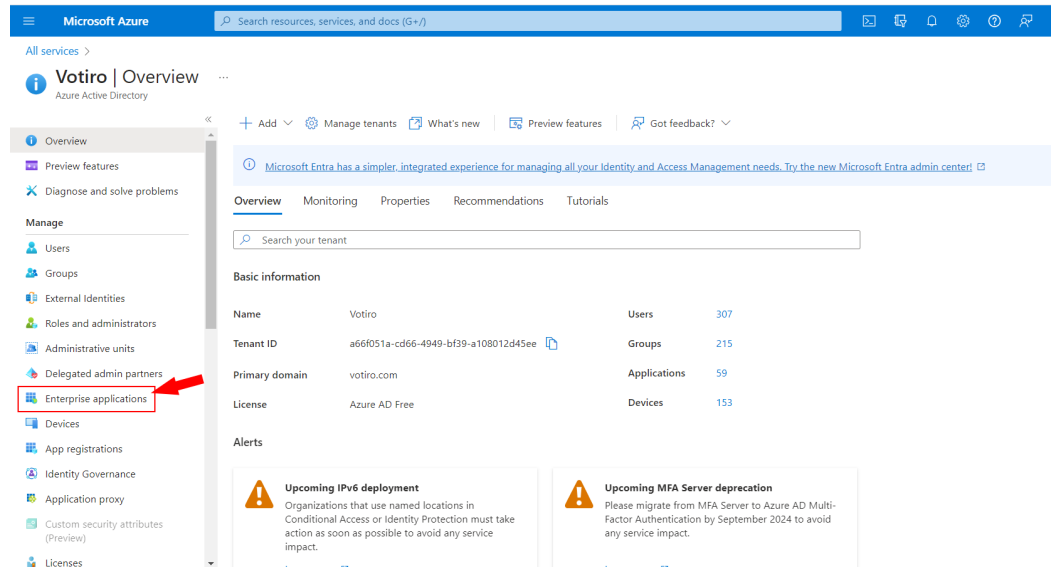
## 1.2 Procedure

1. Sign in to the [Azure portal](#).
2. Select **Azure Active Directory**.

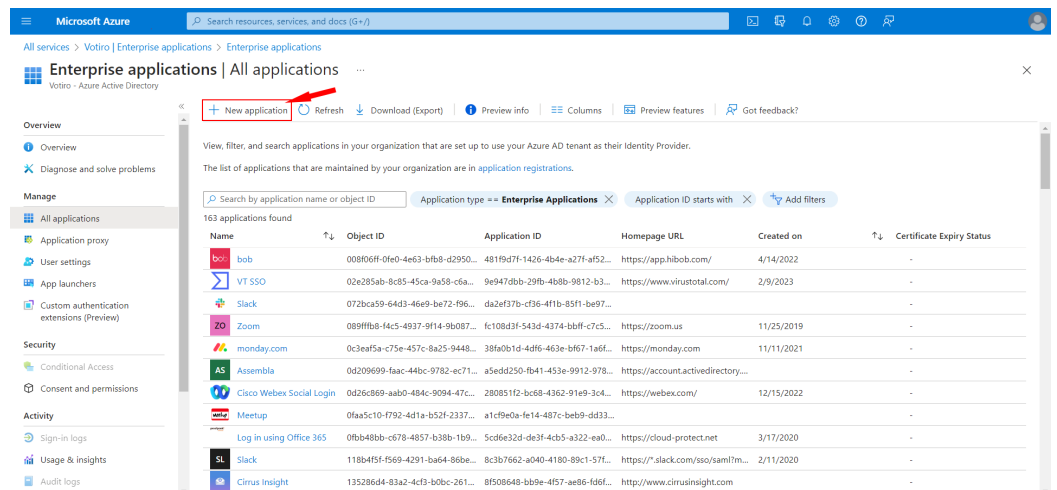


3. In the left pane, select **Enterprise applications**.





#### 4. Select New application:



#### 5. In the search field type Azure AD SAML Toolkit.

## Browse Azure AD Gallery ...

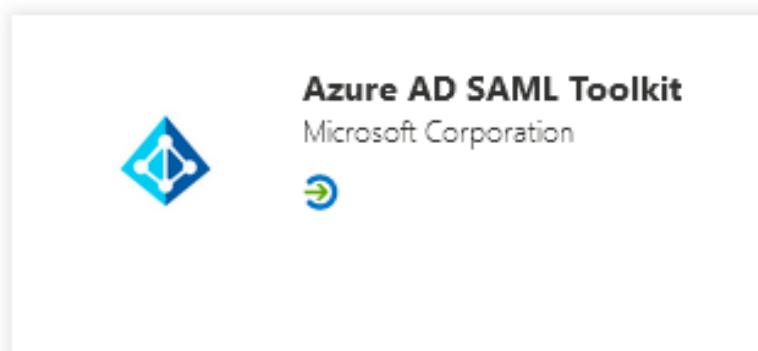
[+ Create your own application](#) [i Request new gallery app](#) |

The Azure AD App Gallery is a catalog of thousands of apps that make

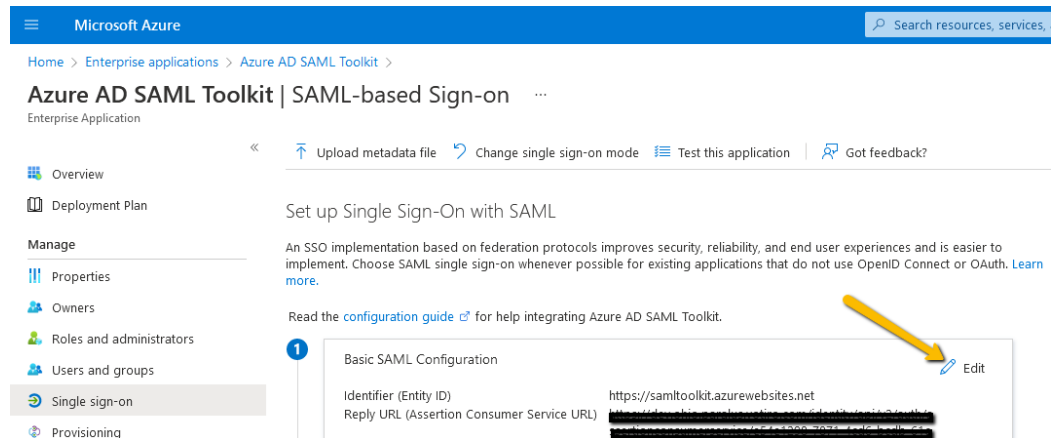
× Single Sign-on

 Federated SSO  Provisioning

### Showing 1 of 1 results



6. Lastly, select it from the results and add it. After a few moments, the app will be added to your tenant.
7. Navigate back to **Enterprise applications | All applications** and select the newly added app: **Azure AD SAML Toolkit**.
8. On the left pane, select **Single sign-on**.
9. On the **Basic SAML Configuration** page, click the pencil button to edit the configuration.



10. For **Identifier (Entity ID)**, leave as default - <https://samlt toolkit.azurewebsites.net>.
11. Both Reply URL (Assertion Consumer Service URL) and Sign on URL should be in the following format: <https://<VOTIRO-FQDN>/assertionconsumerservice>.

**Note:**

**If you're configuring SAML for SaaS cluster, please make sure to include the tenant id after the Reply URL and Sign on URL:**

[https://<VOTIRO-FQDN>/assertionconsumerservice/<TENANT\\_ID>](https://<VOTIRO-FQDN>/assertionconsumerservice/<TENANT_ID>)

12. Other fields are optional and will remain blank, lastly press the **Save** button.

Basic SAML Configuration

Save

Got feedback?

Identifier (Entity ID) \* ⓘ  
*The default identifier will be the audience of the SAML response for IDP-initiated SSO*

Default

https://samltoolkit.azurewebsites.net

✓

✓

ⓘ

Add identifier

Patterns: https://samltoolkit.azurewebsites.net

Reply URL (Assertion Consumer Service URL) \* ⓘ  
*The default reply URL will be the destination in the SAML response for IDP-initiated SSO*

Default

https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice/e54e1298-78...

✓

ⓘ

https://[redacted]/assertionconsumerservice

ⓘ

Add reply URL

Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume

Sign on URL \* ⓘ  

https://[redacted]/assertionconsumerservice

✓

Patterns: https://samltoolkit.azurewebsites.net/

Relay State (Optional) ⓘ  

Enter a relay state

Logout Url (Optional) ⓘ  

Enter a logout url

✓

13. On the **Attributes & Claims** section, click the pencil button to edit the configuration.
14. Select **Add a group claim** on the left-hand side, choose All groups, expand **Advanced options**, select **Customize the name of the group claim**, and provide it with a name, for instance, "AzureGroup1", then press the **Save** button. Also create a group with that name if you choose to use "AzureGroup1" and copy it's objectID to the Votiro UI.

## Group Claims



Manage the group claims used by Azure AD to populate SAML tokens issued to your app



This page includes previews available for your evaluation in the 'Advanced options' section.

Which groups associated with the user should be returned in the claim?

- ☐ None
- ☒ All groups
- ☐ Security groups
- ☐ Directory roles
- ☐ Groups assigned to the application

Source attribute \*

Group ID



### ^ Advanced options

☐ Filter groups (Preview)

Attribute to match



Match with



String

☒ Customize the name of the group claim

Name (required)

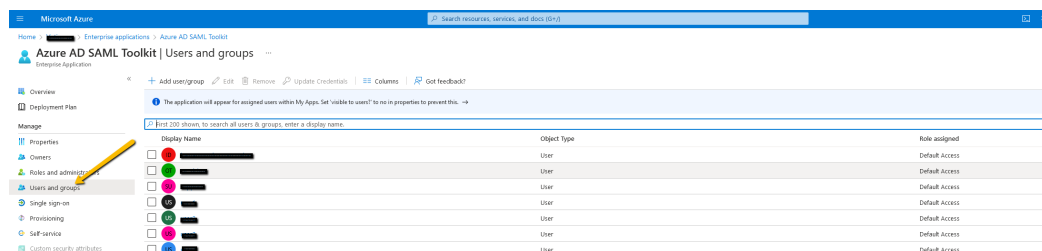
AzureGroup1

Namespace (optional)

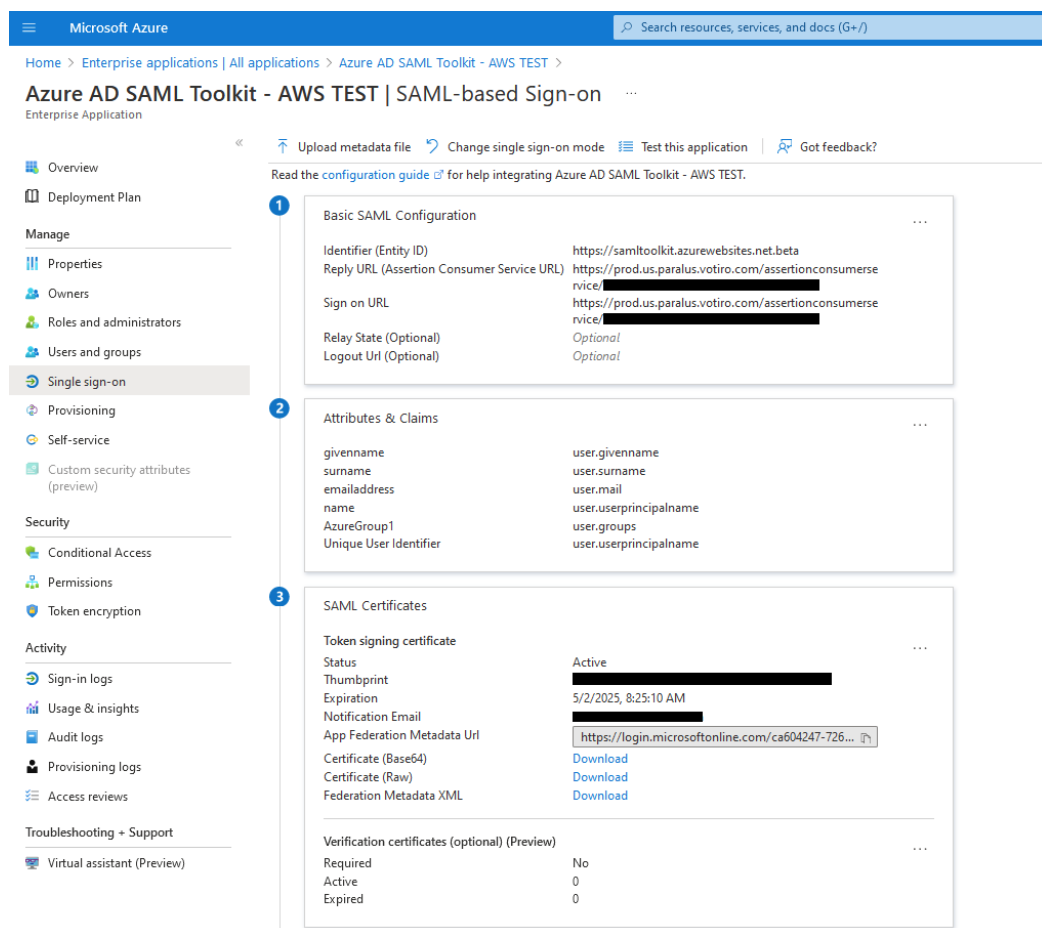
☐ Emit groups as role claims ⓘ

☐ Apply regex replace to groups claim content (Preview)

15. To avoid issues such as “User without any role”, make sure the users that should have access to the environment via SAML are listed under **Azure AD SAML Toolkit | Users and groups**.



16. Log in to Votiro’s Management console. On the left pane, click on the cogwheel, and select **SAML**. For the IDP Metadata address, copy and paste the value from the **App Federation Metadata Url** field in Azure.



17. For the Issuer, copy and paste <https://samltoolkit.azurewebsites.net> from the **Basic SAML Configuration** you configured above.

[Upload metadata file](#)
[Change single sign-on mode](#)
[Test this application](#)
[Got feedback?](#)

---

1

Basic SAML Configuration

Edit

Identifier (Entity ID)
https://samltoolkit.azurewebsites.net

18. For the SAML Username identifier, leave by default:  
<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier>
19. The Admin role key should be the value you provided for the group above in **Group Claims**, in this case, AzureGroup1.
20. The Admin role value should be the Object Id of the group in which the admin's users are members.

Home > [redacted] > Groups >

**admins**  
Group

Overview | Diagnose and solve problems

Manage

- Properties
- Members
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Applications
- Licenses
- Azure role assignments

Activity

- Access reviews
- Audit logs
- Bulk operation results

Troubleshooting + Support

- New support request

AD **admins**

Membership type: Assigned

Source: Cloud

Type: Security

Object Id: 1feef5b7-f[redacted]

Creation date: 7/6/2021, 5:07:22 AM

Copy to clipboard

Direct members

4 Total 4 User(s) 0 Group(s) 0 Device(s) 0 Other(s)

Group memberships

0 Owners 0 Total members 4

21. Press the **Save changes** button, log out from the Management console and log in with the corporate credentials. You may continue and set up the Help Desk and SOC groups, similar to what was configured for the admins group.

## 2 How to Integrate SIEM with Azure Sentinel

In this tutorial, you'll learn how to integrate SIEM with Azure Sentinel using **Votiro Solution for Microsoft Sentinel**. **Votiro Solution for Microsoft Sentinel** is a collection of Data Connectors, Parser, Workbook and Analytic Rules that are used together to analyze data.

### 2.1 System prerequisites

Ensure you have the following:

- Linux machine with at least 4 CPU cores and 8 GB RAM
- Python 2.7 or 3 installed on the Linux machine
- Rsyslog: v8/Syslog-ng: 2.1 - 3.22.1
- Syslog RFC 3164/5424
- Download and unpack the file: [Votiro-Offline.zip](#)

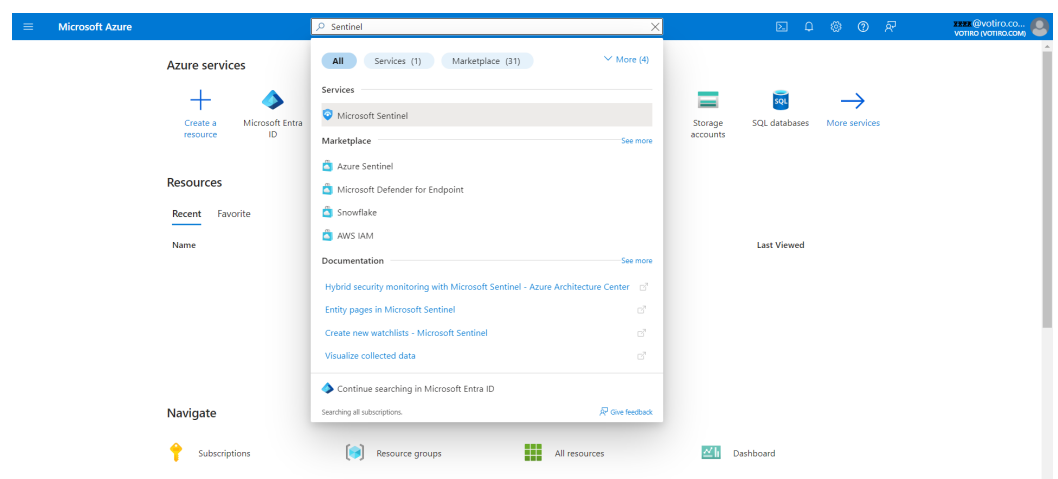
### 2.2 Procedure

#### 2.2.1 Manual/Offline Deployment

To test the solution before publishing, follow the below steps.

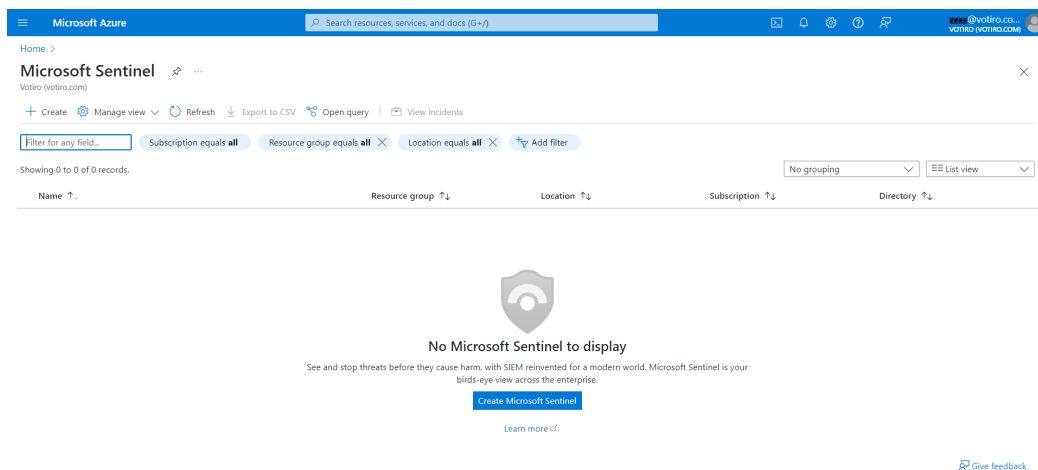
#### Deploy CEF Data Connector on Forwarder Machine

1. Sign in to the [Azure portal](#).
2. Search for **Microsoft Sentinel**.

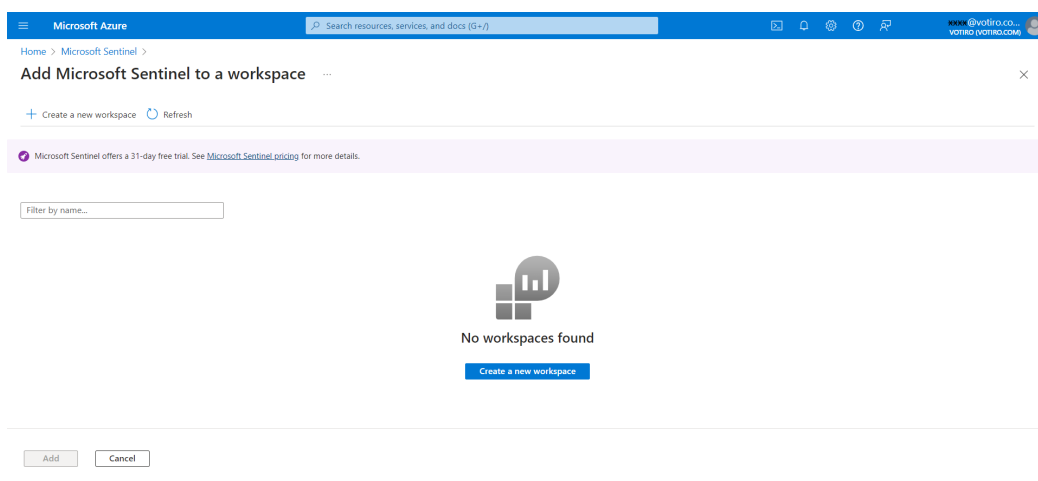


3. Select **Microsoft Sentinel** from **Services**.



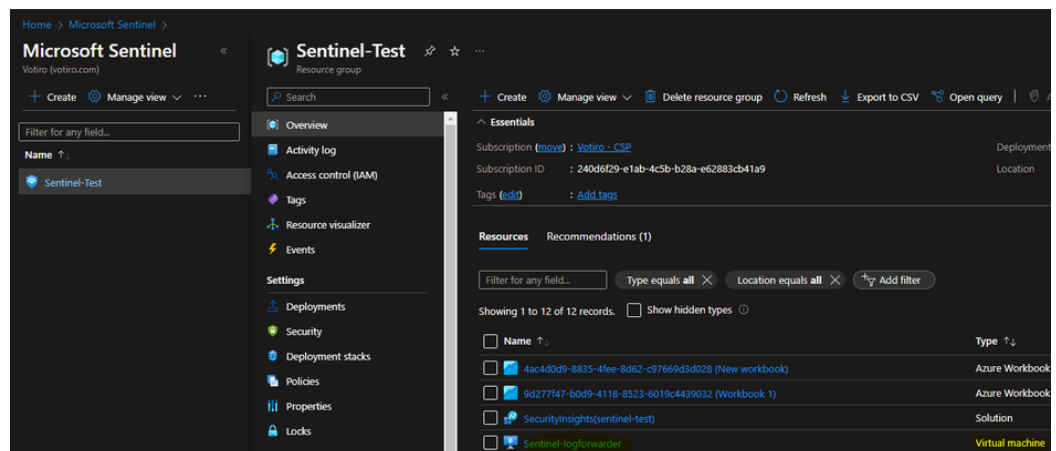


4. Press **+ Create** or **Create Microsoft Sentinel** to add **Microsoft Sentinel** to a **Workspace**:

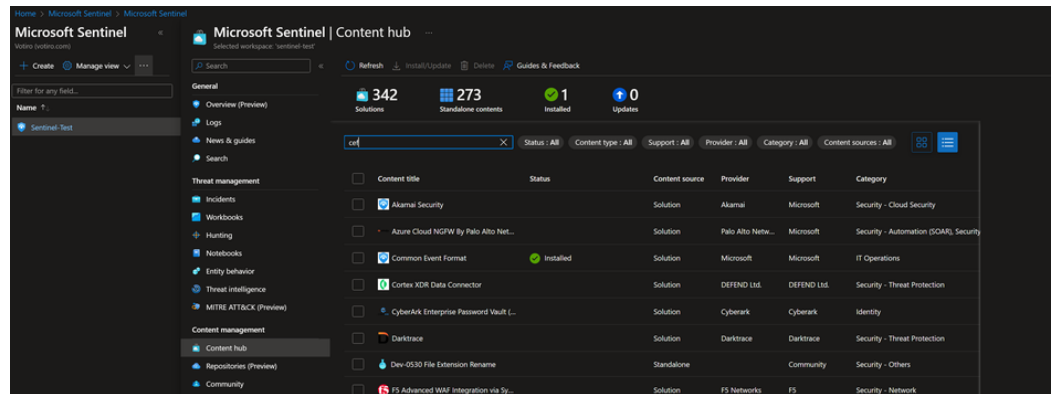


5. Press **+ Create a new workspace**:

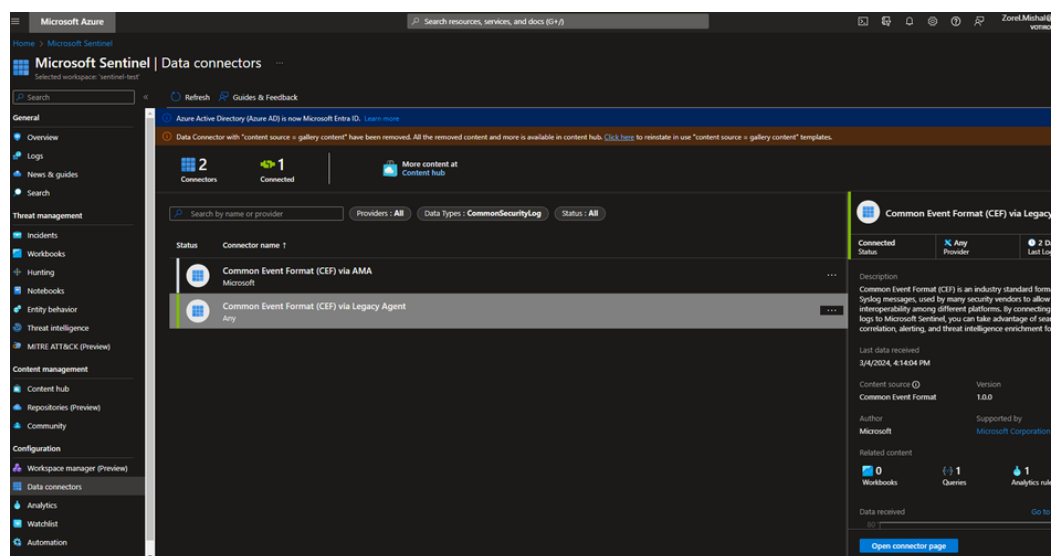
6. Create a new **Resource Group** if it does not exist yet. Then create a new machine with the system requirements mentioned above → via Resource Group > Create > select Virtual Machine (Ubuntu 22.06 server is recommended):



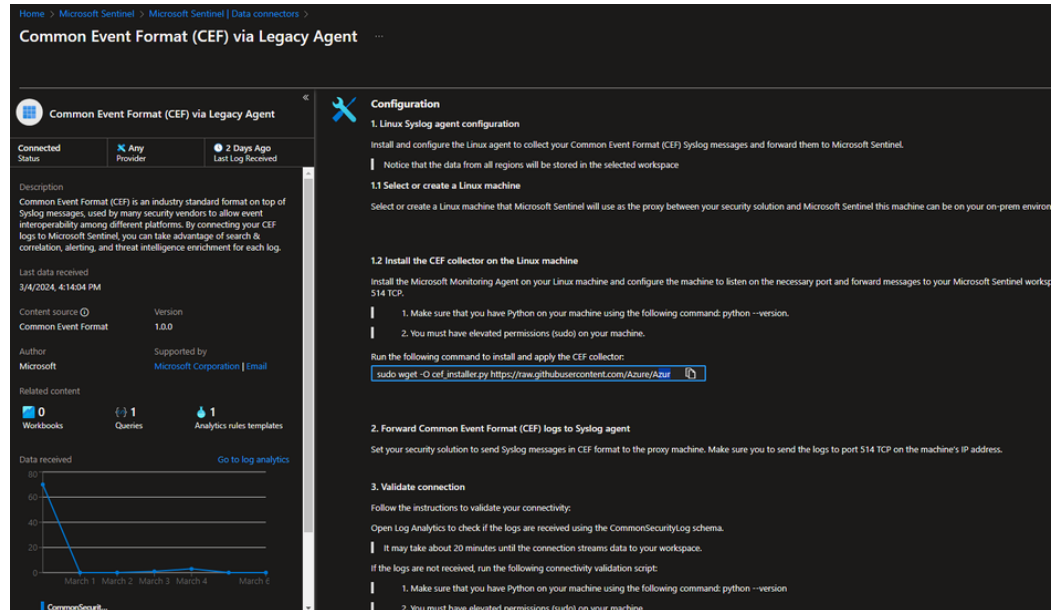
7. Select the created workspace, then go to Content Hub > Select Common Event Format (CEF) and install it:



8. Once installed, go to your workspace > Data Connectors > Open Connector Page:



9. Follow the instructions in 1.2 below, **Install the CEF collector on the Linux machine:**



10. Verify that you have Python 2.7 or Python 3 installed on the Linux machine by running:

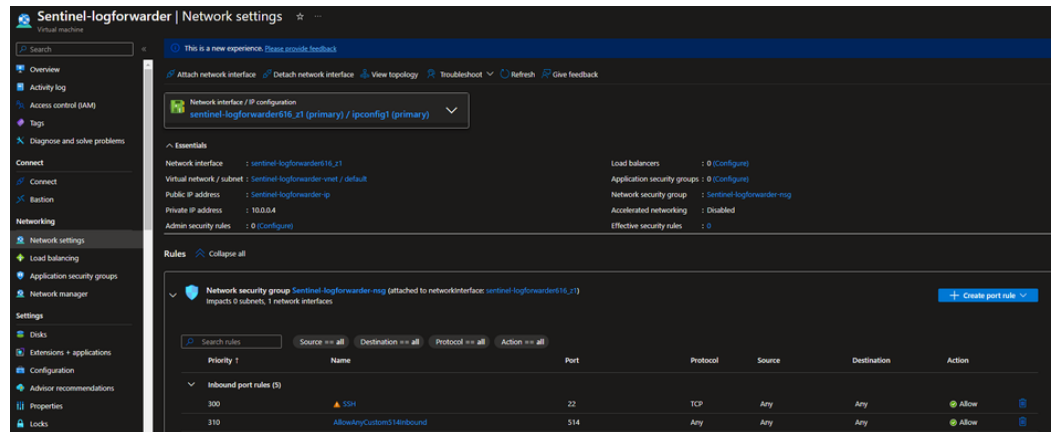
```
python --version or python3 --version
```

11. Copy the command below:

```
sudo wget -O cef_installer.py
https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/CEF/cef_installer.py&&sudo
python cef_installer.py [WorkspaceID] [Workspace Primary Key]
```

**Note:** You must have the GNU Wget package installed on the Linux machine.

12. Paste the command into the command line on your log forwarder, and replace **[WorkspaceID]** and **[Workspace Primary Key]** with their values.
13. Run the command. This installs the CEF connector and Log Analytics Agent on the forwarder machine. Once done, the connector is now listening to events on TCP port 514.
14. Verify that the port used is indeed opened via the Virtual Machine's Network settings:



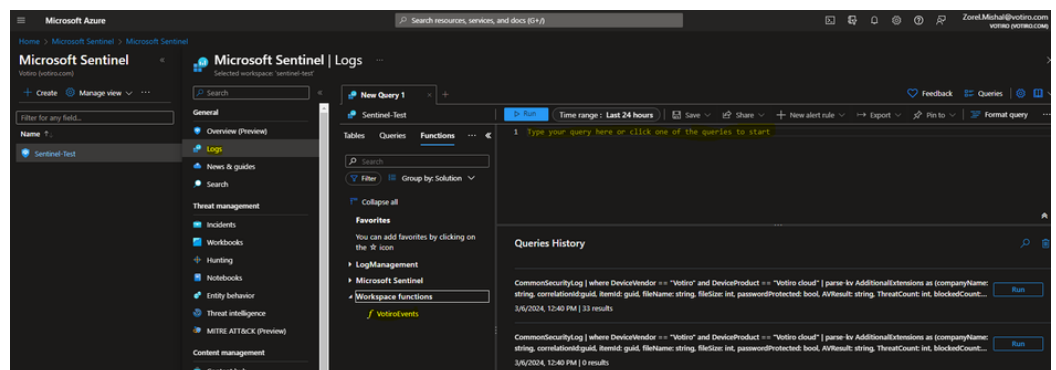
**Note:** In this case, we used TCP port 514 (default) and **Allow=any**, but the best practice is to use the TLS protocol with other ports used and restrict to specific IPs pointed to specific NAT gateways. For example, in [prod.us](#):

Name	NAT gateway ID	Connectivity...	State	State message	Primary public I...	Primary private I...
ngw-prod-egress-01	nat-013cc592b4306c371	Public	Available	–	54.234.70.44	10.240.128.14
ngw-prod-egress-02	nat-0f7ba826618ac4c93	Public	Available	–	34.237.77.26	10.240.129.207

## Deploy Parser Function

Follow the instructions to parse ingested data:

1. Copy the function code from the downloaded package file:  
**/Votiro-Offline/Parser/VotiroEvents.txt**
2. On Microsoft Sentinel → Go to your created Workspace -> Logs
3. Paste the content of **VotiroEvents.txt** in the area as shown below:



4. Then click on **Save > Save as function**. Enter the **Function name** as **VotiroEvents** and click on **Save**:

×

Save as function

Function name \*

VotiroEvents

✓

Code

dfgdfg

Legacy category \*

VotiroEvents

✓

☐ Save as computer group ⓘ

Parameters

Type	Name	Default value
Select type	Type name	Type default value

Save

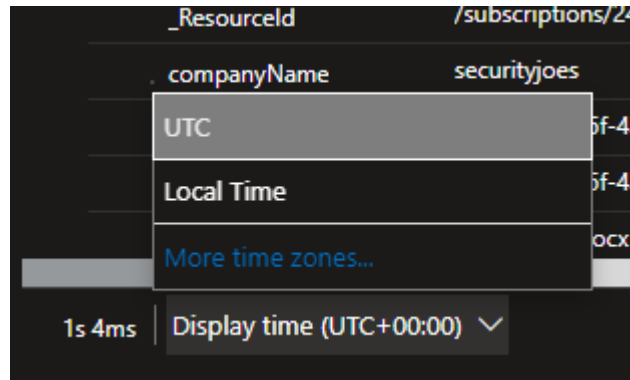
Cancel

- Try running the query to see the following type of results (adjust the time range according to data ingested):

TimeGenerated [UTC]	DeviceVendor	DeviceProduct	DeviceVersion	DeviceEventClassID	Activity	LogSeverity	FileHash
3/3/2024, 2:04:30.713 PM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	fa2742
2/29/2024, 10:03:12.734 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	fa2742
2/29/2024, 10:10:40.876 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	980489
2/29/2024, 10:11:19.147 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	980489
2/29/2024, 10:11:47.788 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	980489
2/29/2024, 10:13:17.393 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	980489
2/29/2024, 10:15:45.742 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:18:49.026 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:19:03.034 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:19:20.211 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:23:10.279 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:24:10.481 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:25:07.792 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	38c979
2/29/2024, 10:26:14.751 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	38c979
2/29/2024, 10:28:03.185 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	38c979

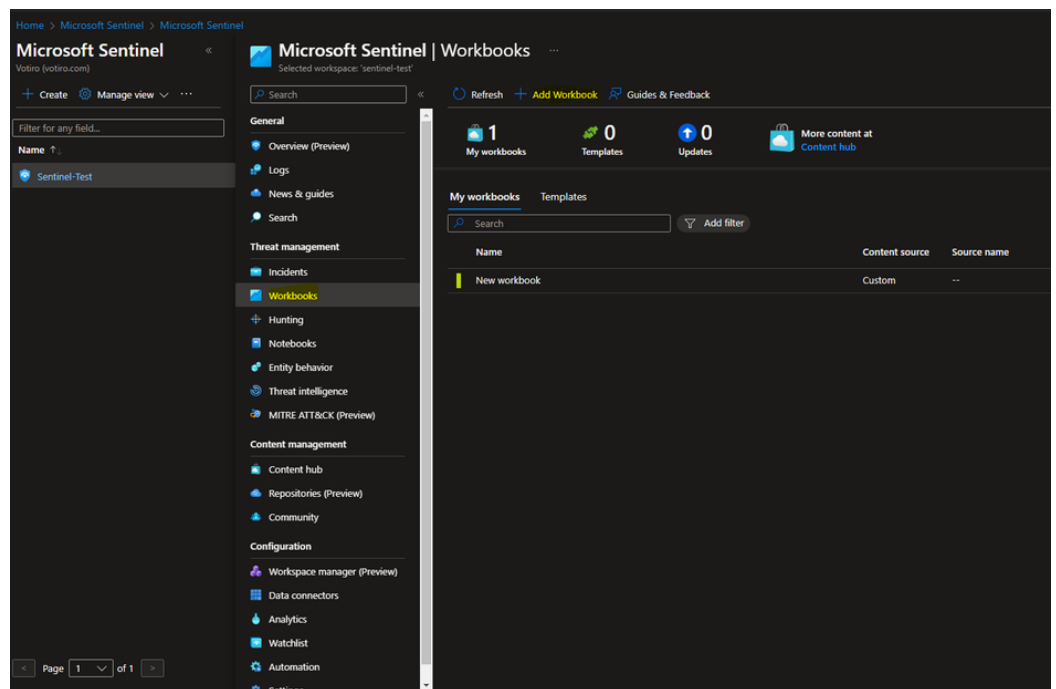
Field	Value
TenantId	6c0fa6d8-ec71-4593-8e5f-45b4f7770685
TimeGenerated [UTC]	2024-03-03T14:04:30.713Z
DeviceVendor	Votiro
DeviceProduct	Votiro cloud
DeviceVersion	1.0.0.0
DeviceEventClassID	500
Activity	Sanitization summary
LogSeverity	1
FileHash	fa2742aec57ae5a21e80a0cf7767af566ba48e0b035fa5546fc34e2898a31ad6
FileType	Word (2007-2010)
Computer	ec2-54-234-70-44.compute-1.amazonaws.com
SourceSystem	OpsManager
Type	CommonSecurityLog
_ResourceId	/subscriptions/240d6f29-e1ab-4c5b-b28a-e62883cb41a9/resourcegroups/sentinel-test/providers/microsoft.compute/virtualmachines/sentinel-logforwarder
companyName	securityjoes
correlationId	6965c187-045f-4a6b-bda5-f0321c75a43f
itemId	6965c187-045f-4a6b-bda5-f0321c75a43f
SrcFileName	saddsaDSA.docx

- Results can be viewed in **Local Time** zone by changing the option in the bottom bar:



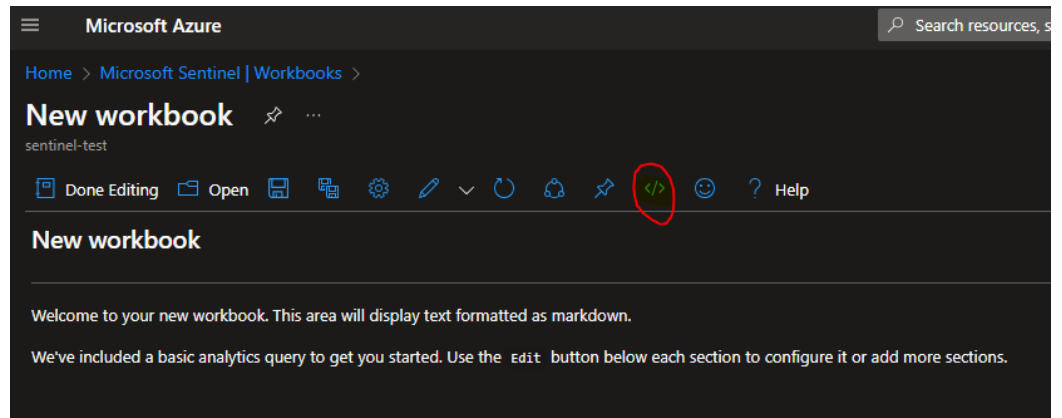
## Deploy the Workbook

1. Copy the contents of the file:  
**/Votiro-Offline/Workbooks/Votiro Monitoring Dashboard.json**
2. On Microsoft Sentinel, go to your WorkSpace > Workbooks > **Add Workbook**:

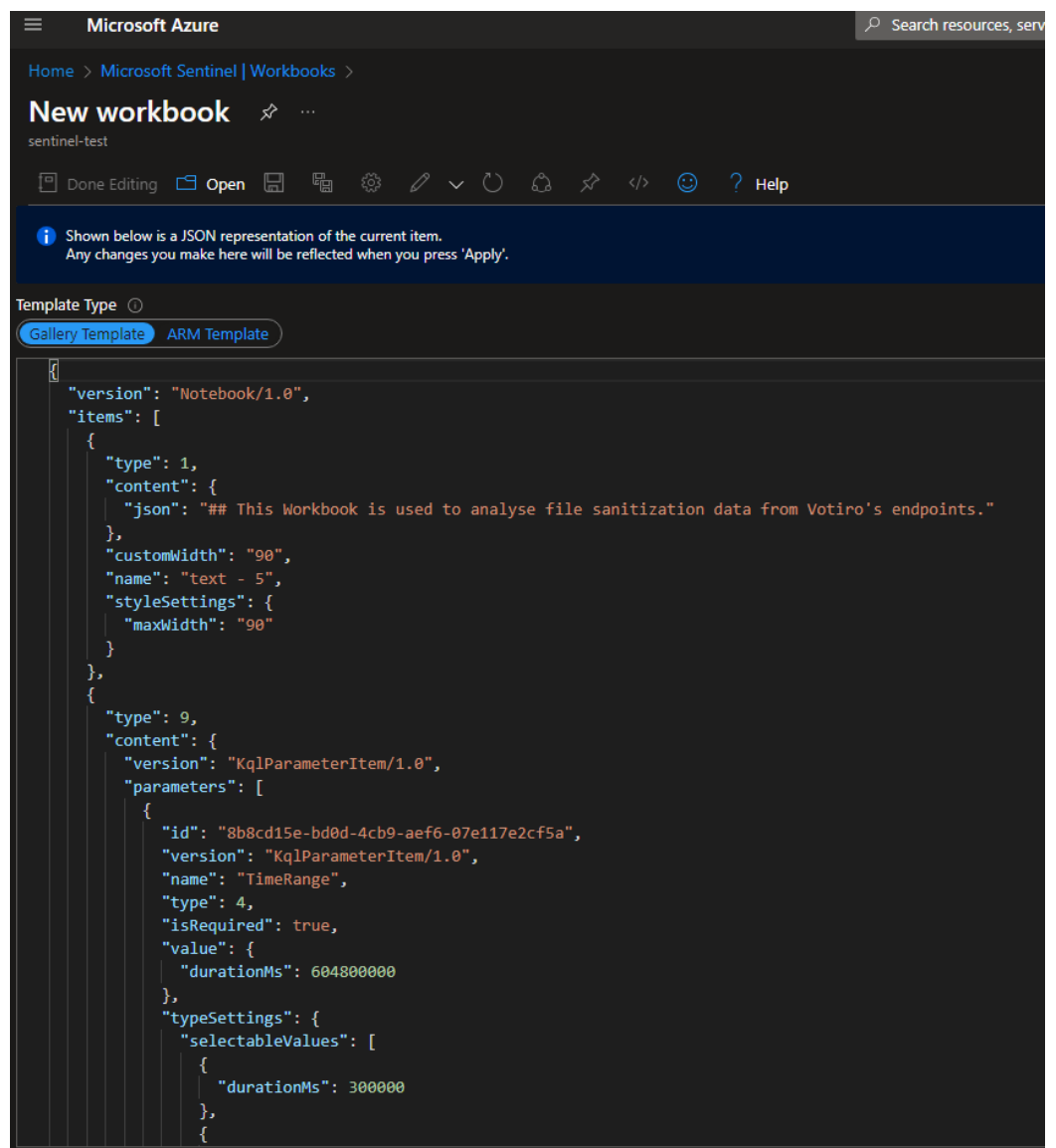


3. On the New Workbook page, click on Edit > Advanced Editor icon:





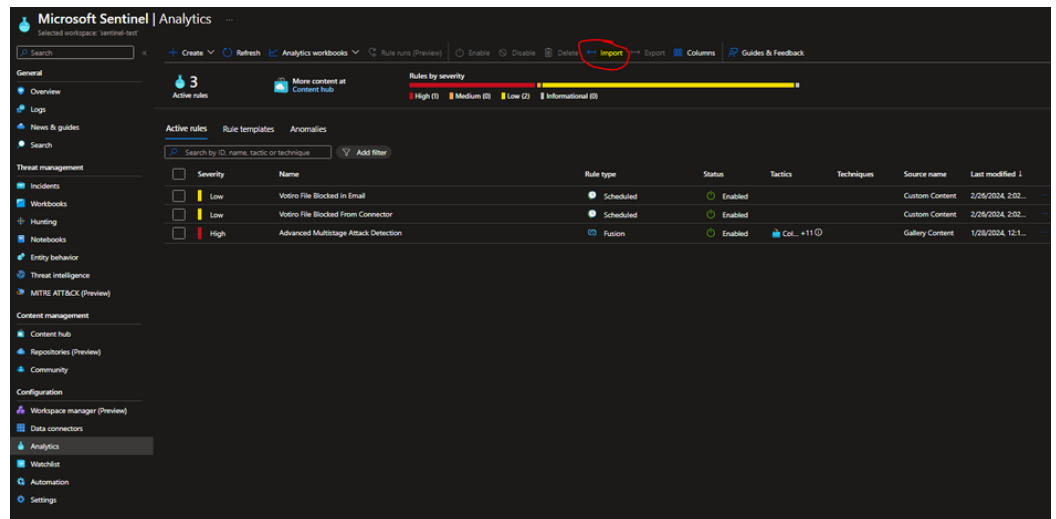
4. Replace the Gallery template contents with the copied contents, and click on **Apply**:



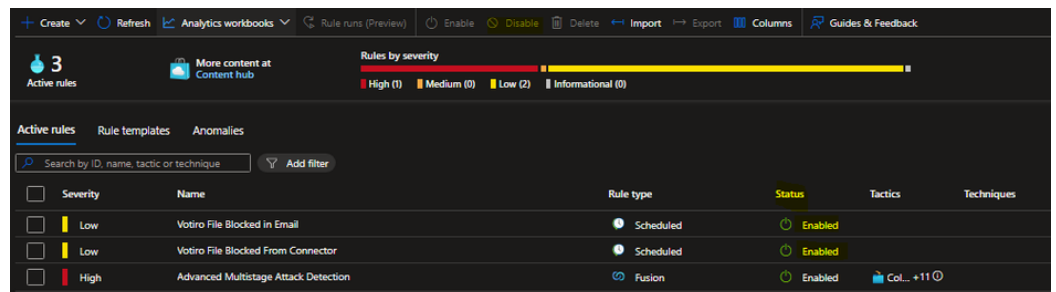
5. The Following Workbook must be visible:  
After a scroll

## Set Alert Queries for Incidents

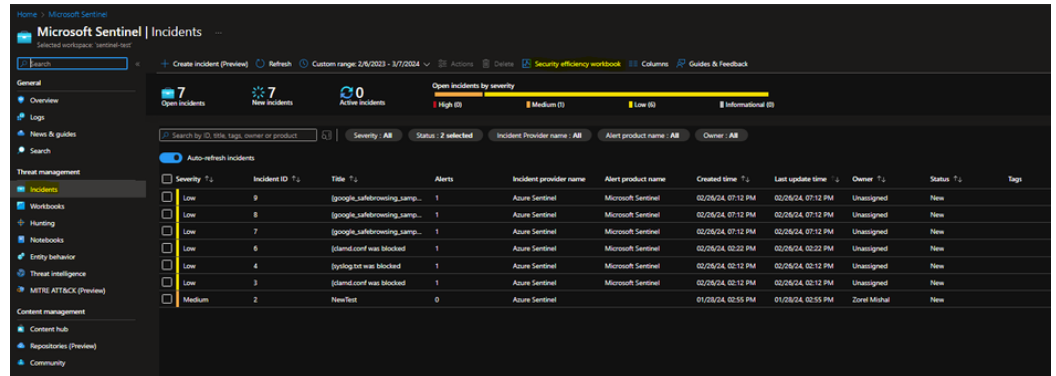
1. Go to **/Votiro-Offline/Analytic Rules**. Keep both **Votiro File Blocked FromConnector.json** and **Votiro File Blocked in Email.json** files ready.
2. On Microsoft Sentinel > Workspace, select **Analytics**.
3. Click **Import** (from the bar at the top of the screen) in the resulting dialog box, navigate to and select the JSON files one by one, and select **Open**:



4. Make sure that the status of each active rule is enabled:



5. Check for recent alerts or incidents on the **Overview** page. Incidents are also available on the **Microsoft Sentinel > Incidents** page.



Select the security efficiency workbook for a better view.

## 6. Alerts Logic:

- **Votiro File Blocked From Connector:** If the syslog message includes “blocked” under -Sanitization result- field and “false” under -password protected- field and “null” under -from- field create an alert with the following message: [file name] with hash [file hash] that was sent from connector [connector name] was blocked by Votiro due to Policy [policy name], see more detail in the following link [incident url]
- **Votiro File Blocked in Email:** If the syslog message includes “blocked” under - Sanitization result- field and “false” under -password protected- field and not “null” under -from- field create an alert with the following message: Attachment [file name] with the hash [file hash] was blocked in an email that was sent from user [from] to the following recipients [Recipients] by Votiro due to Policy [policy name], see more detail in the following link [incident URL]

## 3 How to Send Files to Votiro via Postman

Postman is an API platform for developers to design, build, test and iterate their APIs. It is an HTTP client that tests HTTP requests, utilizing a graphical user interface, through which different types of responses are returned that need to be subsequently validated. This article describes how to use Postman with Votiro.

### 3.1 Prerequisites

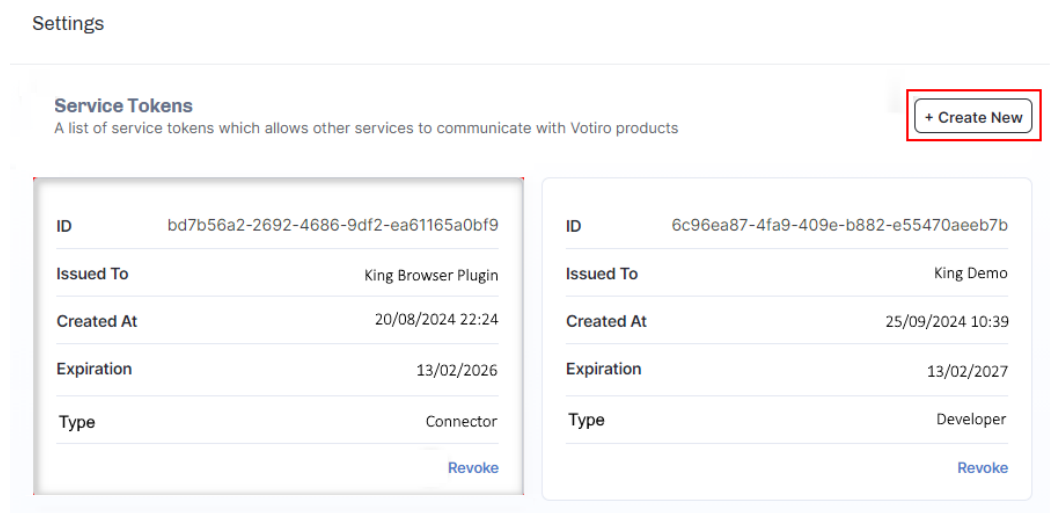
Install Postman by downloading one of the following:

- ◆ The Postman app from [Download Postman](#).
- ◆ The Postman portable app from [Postman™ portable](#).

### 3.2 Procedure

#### 3.2.1 Generating a Service Token

1. Generate a Service Token. Go to **Settings > Service Tokens > Create New** :



2. Select the token **Type**:
  - a. **Connector** - Basic integration. Allows authentication for uploading files procedure.
  - b. **Developer** - Advanced integration. For all available APIs. Handle it with caution.
3. Enter a name for the new token under **Issued To**.
4. **Set Expiration Time**
5. Press **CREATE**:

Create New Service Token

Type

Connector 

?

Connector

Developer

Issued To

King Demo

Set Expiration Time

< Feb 2027 >

Su Mo Tu We Th Fr Sa

1 2 3 4 5 6

7 8 9 10 11 12 13

14 15 16 17 18 19 20

21 22 23 24 25 26 27

28

CANCEL

CREATE

- 6. Copy and save the token string that appears on this page.

**WARNING!**

Save the token string. This page will only appear once.

Please Save Your Token, You Won't Be Able To See It Again

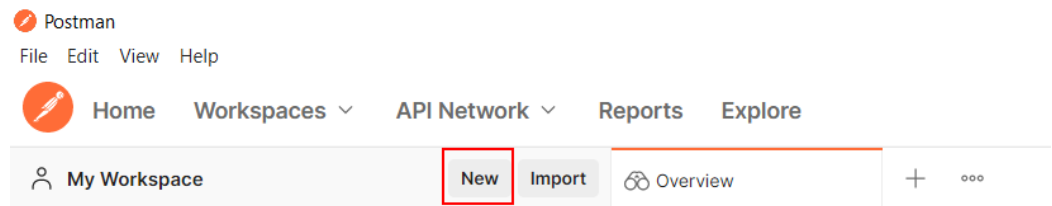
ID	ff5e09af-0867-4514-bfed-4186e86ef2fe
Issued To	Test-Token
Expiration	15/03/2023
Token	eyJhbGciOiJSUzI1NiIsImtpZCI6IjIOTMxRUM5QzA4NTlGOEVGNkM0NUY0MDExQTU0MTAzNzhGMTY5REEiLCJ0eXAiOiJKV1QiIfQ.eyJ1bmVudGVybmFsU2VydmVjZXMiLCJyb2xlIjoiaWVtZW50c3RyYXRvcilslmp0aSI6ImZmNWUwOWFmLTA4NjctNDUxNC1iZmVkLTQxODZIODZIZjJmZSIsIm5iZil6MTY0NzgZNDQxMCwiZXhwIjoxNjc4ODA5NjAwLCJpYXQiOjE2NDc4MzQ0MTB9.EYm24-YcS6RnXSCh7LiYDFAMA5d_U7Z6nBW670FOgiA6AH3tG14amRWc6wjo2LpKxNAVLbrnMUbrVUTCRTToAWABPvT47gJsIBdafP9R0sPOh0voAdbh_hjt-J9jspYuF8hu7NfukUxUVhDd3oKRnGDmWizBANbqCbXXw2fELGgWpn0VuR88y_o7vxobp5mqIqRWvQ1p3mGTEAem6si1UBHhYgvOvKMYY9TH9cxnuRbnpA-xVwGCQ8OFQuA6ITJw9ehwl34vUA22qri65-xNvWoakgXVA-tiHSpWxdgWrmeLK88wKum7dUyFfDu4rrEadvvmLFZK3eEZ1KpZOv1Dcdg

OK

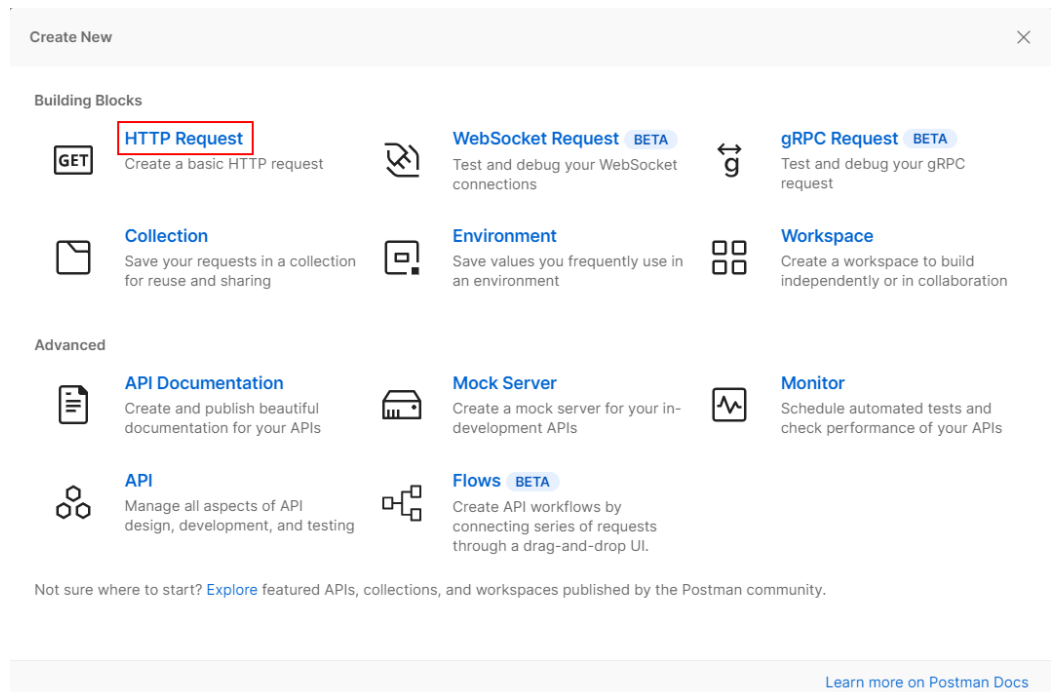
- Press **OK** to close the Token window.

### 3.2.2 Postman Setup

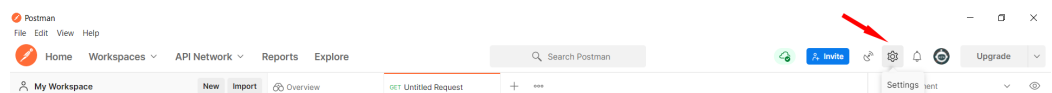
1. In the Postman app, go to **Workspaces > My Workspace** and press **New**:



2. The **Create New** window opens. Select **HTTP Request**:

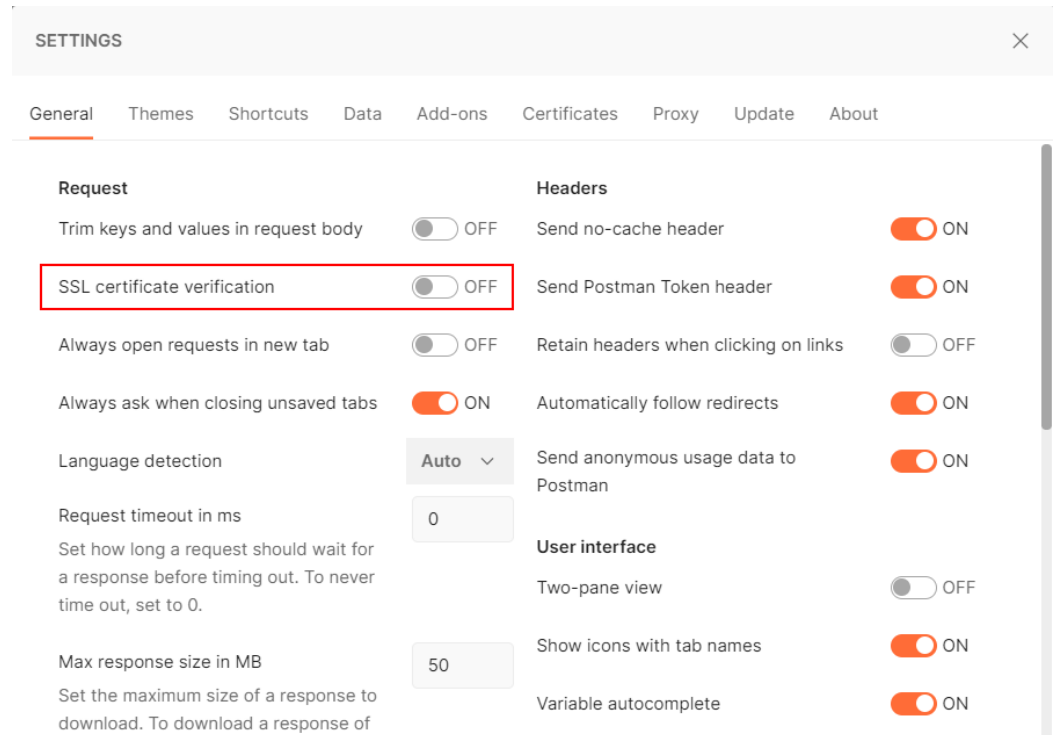


3. Press the **Settings** icon:

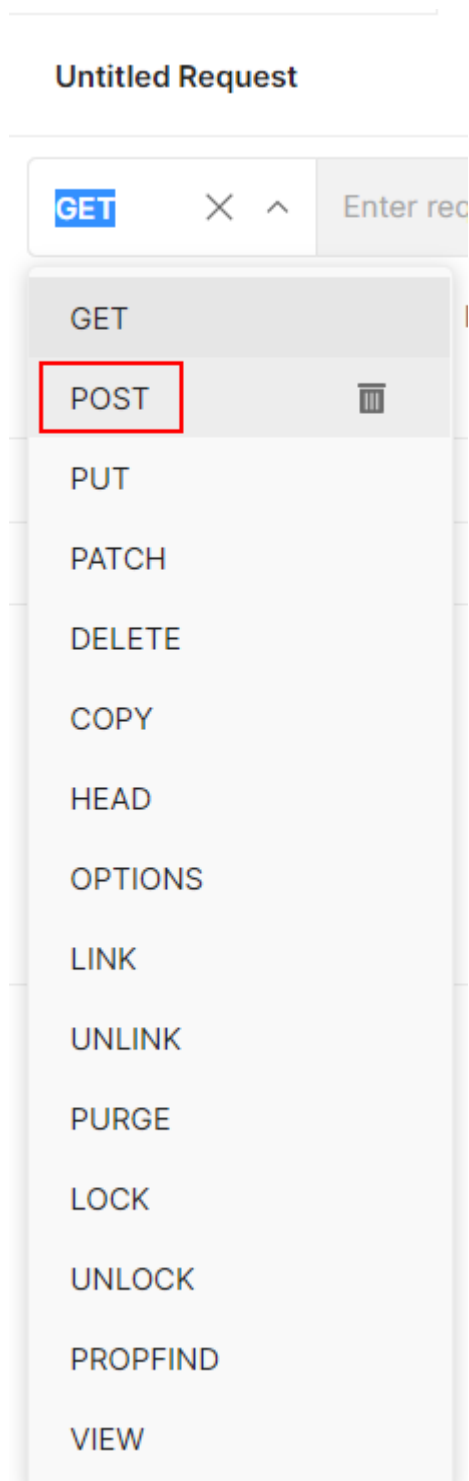


4. The **Settings** window opens. To ensure that http requests will go through even if your VA is using a self-signed certificate, toggle **SSL certificate verification** to **OFF**:



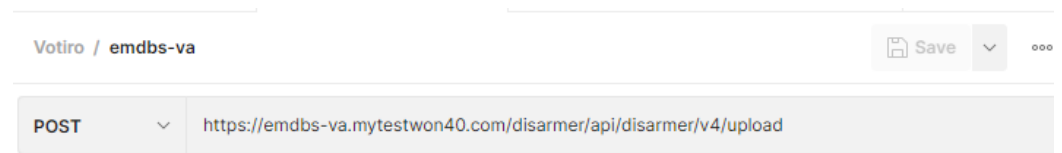


5. Close the **Settings** window.
6. Under the **Untitled Request** dropdown box, select **POST**:

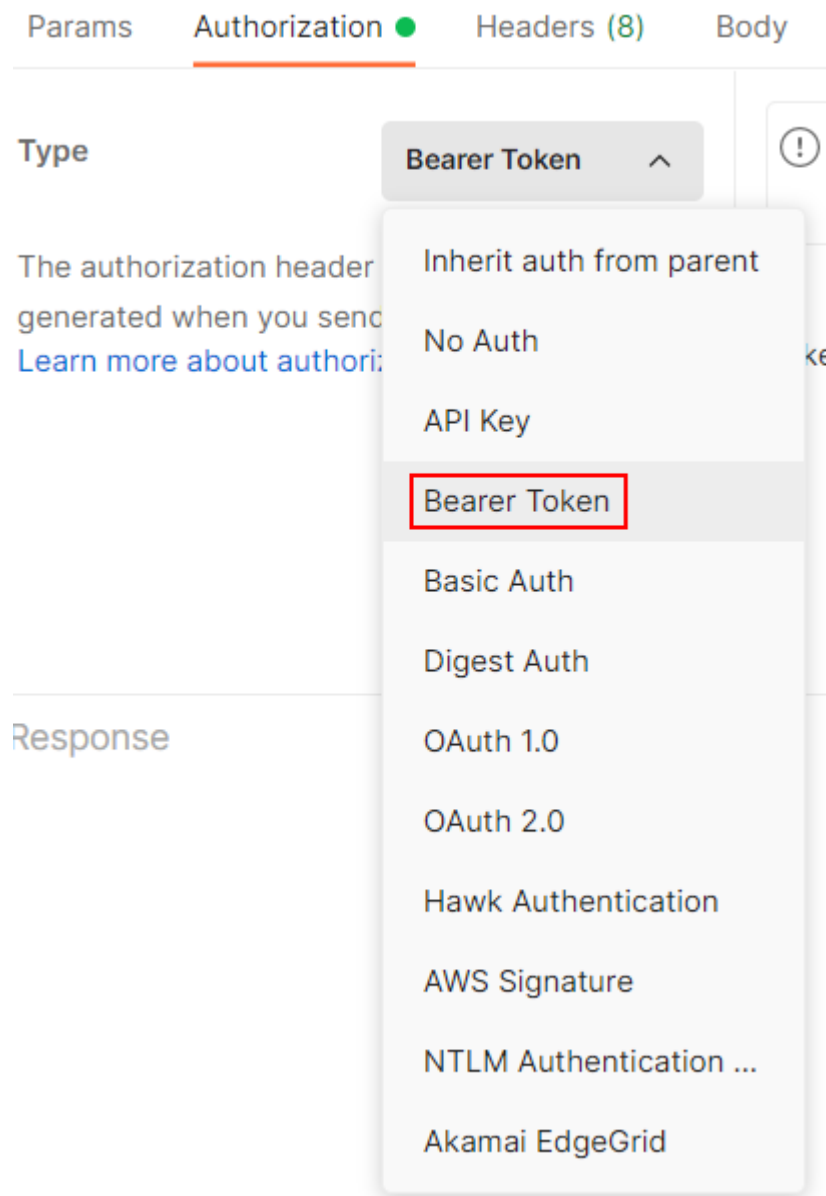


7. In the **Enter request URL** box, enter your VA FQDN in the following format:
- ```
https://<VA-FQDN>/disarmer/api/disarmer/v4/upload
```

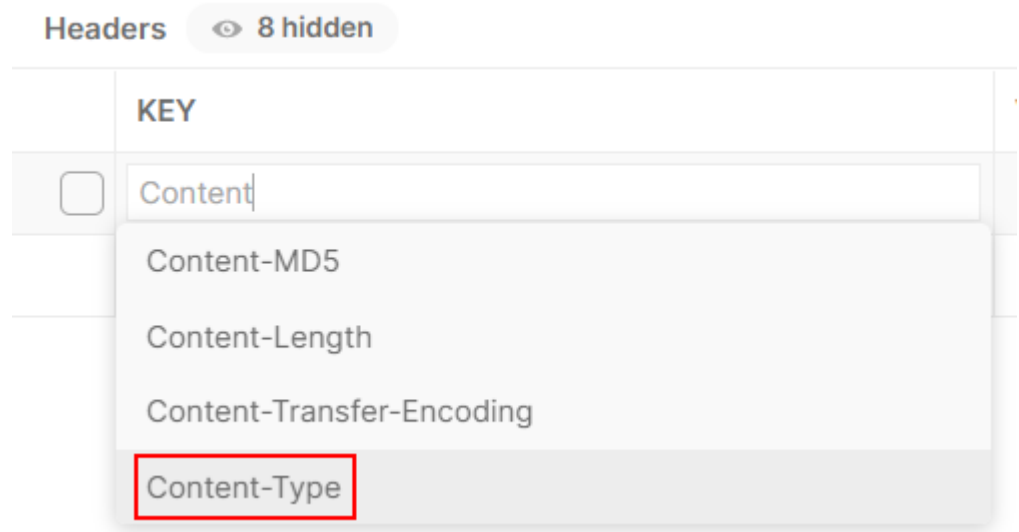
For example:



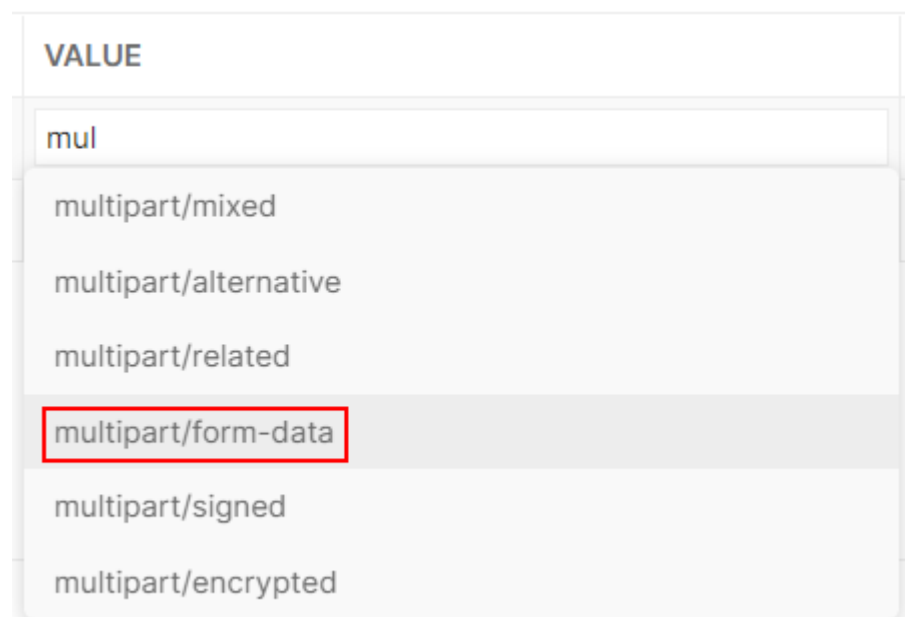
8. Select the **Authorization** tab and under the **Type** dropdown, select **Bearer Token**:



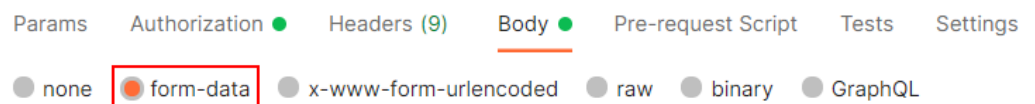
9. Select the **Headers** tab.
10. In the first row of the **Key** column, start to type **Content** until a dropdown list appears. Then select **Content-Type** from the dropdown list:



11. In first row of the **Value** column, start to type **multipart** until a dropdown list appears. Then select **multipart/form-data** from the dropdown list:



12. Select the **Body** tab and then select **form-type**:



13. In the first row of the **KEY** column, type **File**, and select **File** from the hidden dropdown list:

|                                     | KEY  |        |
|-------------------------------------|------|--------|
| <input checked="" type="checkbox"/> | File | File ▾ |
|                                     | Key  | Text   |
|                                     |      | File   |

14. In the first row of the **VALUE** column, press **Select Files** and select the desired file from the browser window that opens.
15. In the second row of the **KEY** column, type **Properties**.
16. In the second row of the **VALUE** column, enter the following:
 

```
{"PolicyName": "Default Policy", "ChannelType": "FileConnector", "ChannelId": "827b50a3-d585-4ba5-a5ca-100b09068123", "ChannelName": "API Up-Sync" }
```
17. After completing steps 13-16, the **KEY** and **VALUE** table should be identical to the below screenshot, with the exception of the file name:

Params
Authorization ●
Headers (10)
Body ●
Pre-request Script
Tests
Send

● none
● form-data
● x-www-form-urlencoded
● raw
● binary
● GraphQL

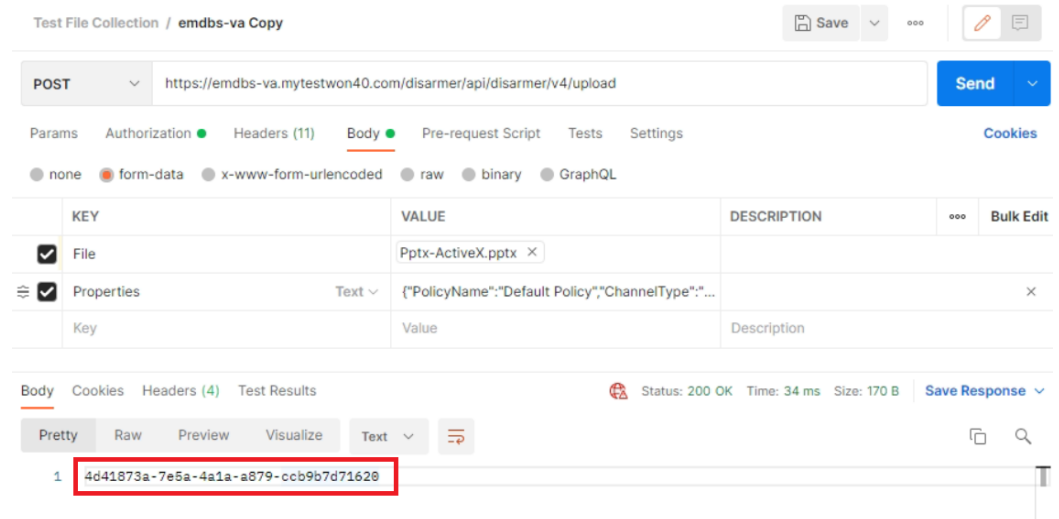
|                                     | KEY        | VALUE                                         |
|-------------------------------------|------------|-----------------------------------------------|
| <input checked="" type="checkbox"/> | File       | Pptx-ActiveX.pptx ×                           |
| <input checked="" type="checkbox"/> | Properties | {"PolicyName": "Default Policy", "ChannelT... |
|                                     | Key        | Value                                         |

18. Press the **Send** button:

POST
https://emdb-s-v4.mytest140.com/disarmer/api/disarmer/v4/upload
Send

19. You should get a HTTP/200 response and a GUID string in the body. This will be the Correlation ID of the file that you have submitted.

For example:



Test File Collection / emdbb-va Copy

POST https://emdbb-va.mytestwon40.com/disarmer/api/disarmer/v4/upload

Params Authorization Headers (11) Body Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary GraphQL

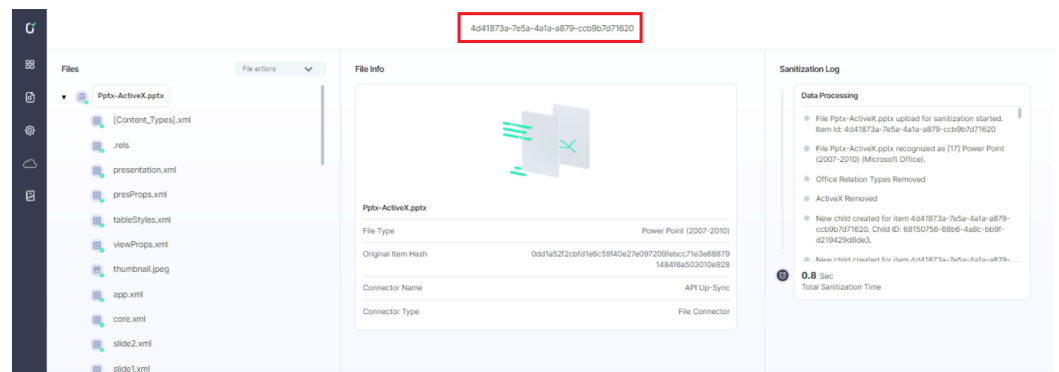
| KEY        | VALUE                                                     | DESCRIPTION | ... | Bulk Edit |
|------------|-----------------------------------------------------------|-------------|-----|-----------|
| File       | Pptx-ActiveX.pptx                                         |             |     |           |
| Properties | Text {"PolicyName": "Default Policy", "ChannelType": "... |             |     |           |
| Key        | Value                                                     | Description |     |           |

Body Cookies Headers (4) Test Results Status: 200 OK Time: 34 ms Size: 170 B Save Response

Pretty Raw Preview Visualize Text

1 4d41873a-7e5a-4a1a-a879-ccb9b7d71620

20. On the Incidents page, you will be able to see the exact string:



4d41873a-7e5a-4a1a-a879-ccb9b7d71620

Files

- Pptx-ActiveX.pptx
- [Content\_Types].xml
- .rels
- presentation.xml
- presProps.xml
- tableStyles.xml
- viewProps.xml
- thumbnail.jpeg
- app.xml
- core.xml
- slide2.xml
- slide1.xml

File Info

Pptx-ActiveX.pptx

File Type Power Point (2007-2010)

Original Item Hash 0dd1a522c0f0e6c5940e27a097209f6cc71e3e688791484f18a503010e928

Connector Name API Up-Sync

Connector Type File Connector

Sanitization Log

Data Processing

- File Pptx-ActiveX.pptx upload for sanitization started. Item ID: 4d41873a-7e5a-4a1a-a879-ccb9b7d71620
- File Pptx-ActiveX.pptx recognized as [17] Power Point (2007-2010) (Microsoft Office).
- Office Relation Types Removed
- ActiveX Removed
- New child created for item 4d41873a-7e5a-4a1a-a879-ccb9b7d71620. Child ID: 68150756-6806-4a8c-b09f-0219429d89d3

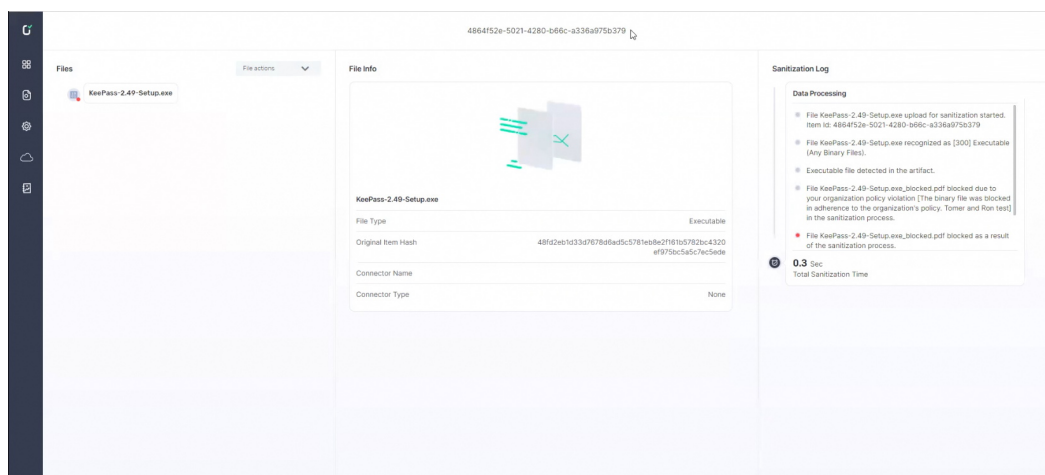
0.8 Sec Total Sanitization Time

## 4 How to Use Kibana to Troubleshoot Votiro Incidents

This page describes how to use Kibana to view and troubleshoot Votiro Incidents.

### 4.1 Example of Votiro Incident

The following screenshot displays the Votiro Item/Incident sanitization information for a file that has undergone sanitization:



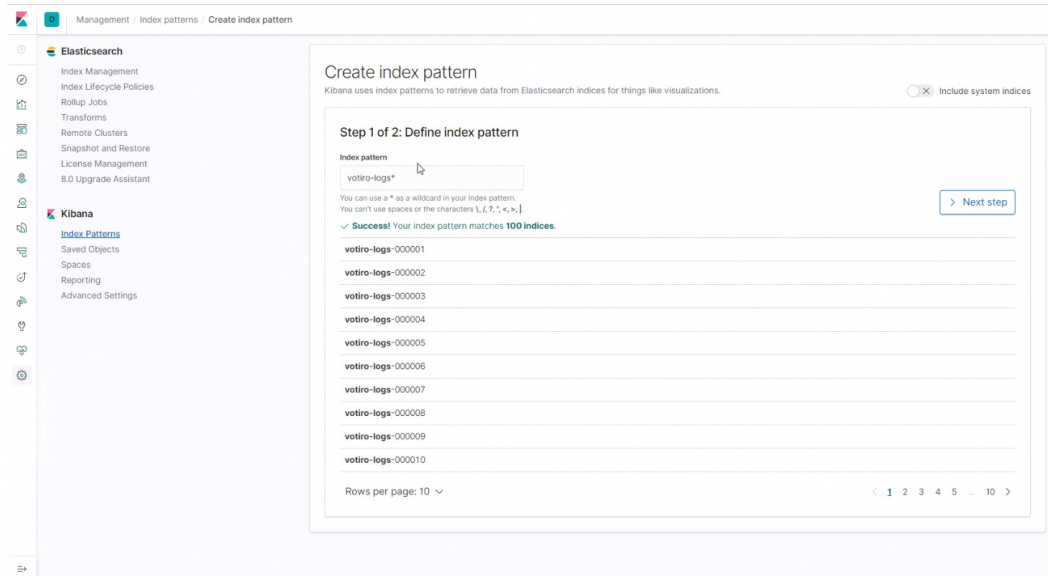
This screen shows the results of Votiro On-prem processing a file named KeePass-2.49-Setup.exe. The **File Info** pane displays some of the file properties and the **Sanitization Log** pane displays highlights of the file **Data Processing**.

### 4.2 Procedure

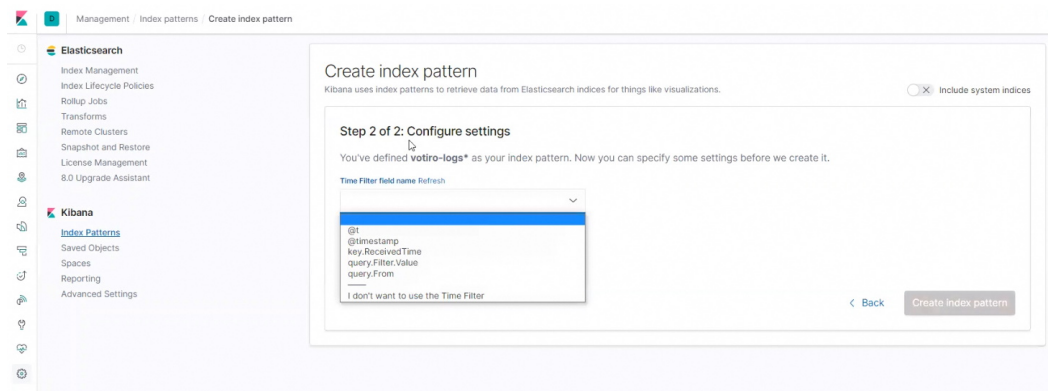
#### 4.2.1 Create and Configure an Index Pattern

To begin, you must define a Kibana index pattern.

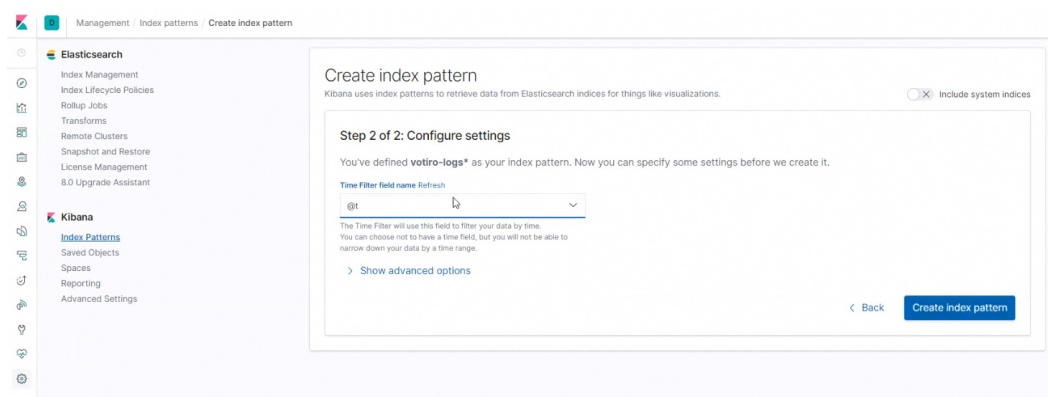
1. Login to the Kibana Discover interface with the credentials provided to you by Votiro Support.
2. Select **Create index pattern**. **Step 1 of 2 Define index pattern** appears.
3. Type **votiro-logs\*** (or similar) as the Index pattern. Kibana displays a list matching the index pattern:



4. Click on **Next step**. **Step 2 of 2 Configure settings** appears.

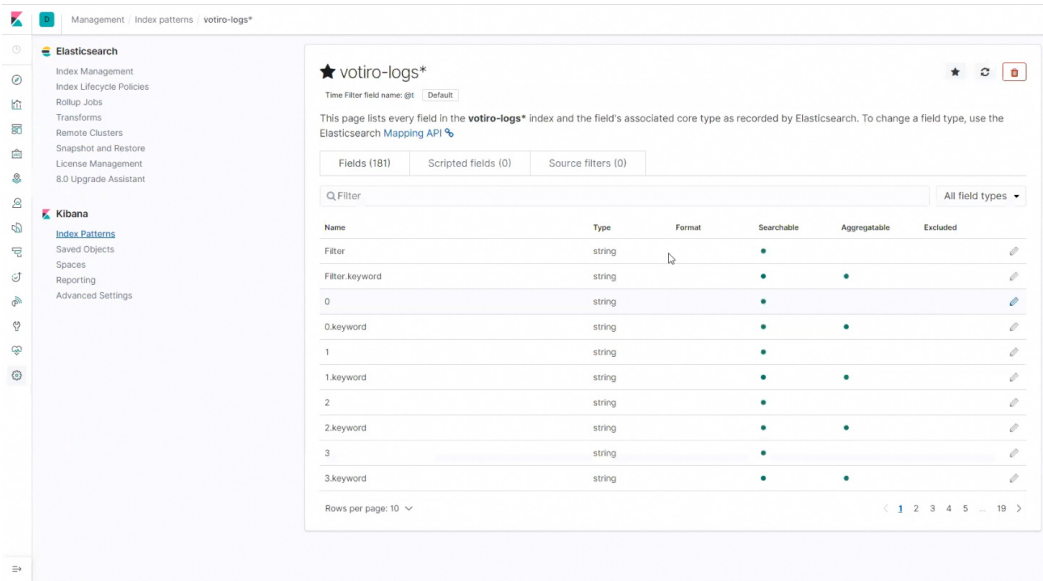


5. Select a **Time Filter field name** from the list. For example, **@t**:



6. Click on **Create index pattern**. Kibana displays every field and field type in the selected index (in this example, votiro-logs\*):



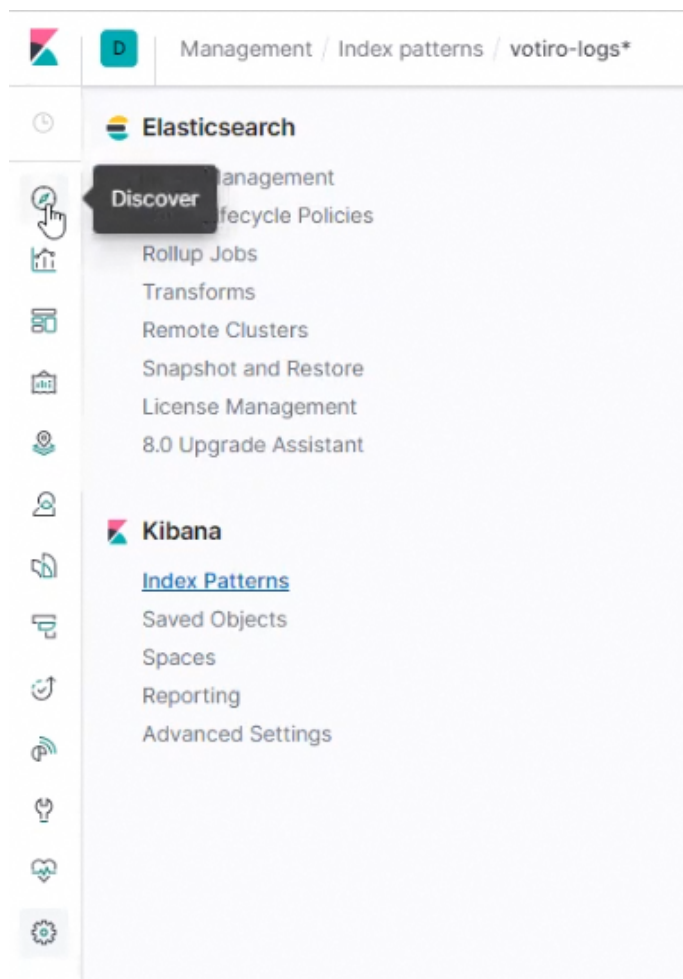


4.3 Analyze the Data

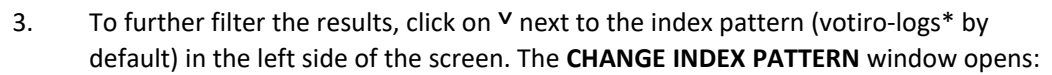
After the index pattern is created and configured, apply it to the data in Kibana's Discover mode to yield useful results by additional filtering of the data.

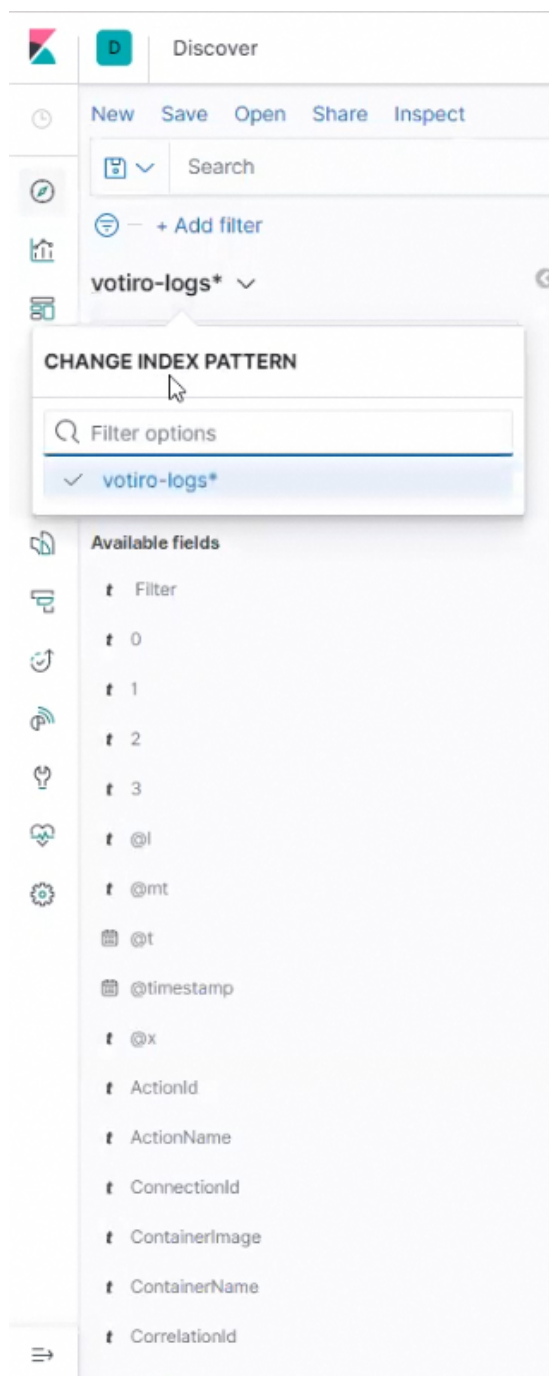
### 4.3.1 Discover

1. Click on the Discover icon on the left side of the screen:

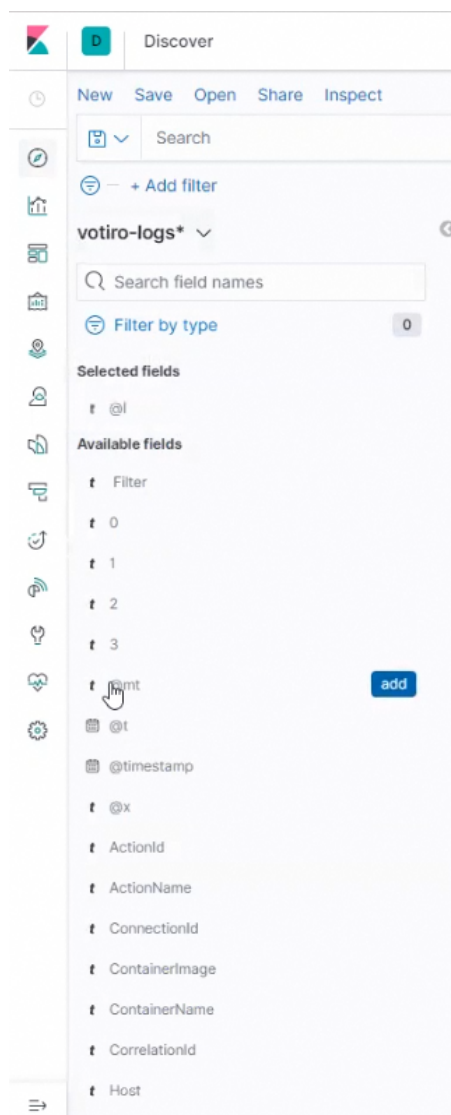


2. Kibana displays all hits that match the time filter criteria within the time range indicated (in this example, for the last 15 minutes):





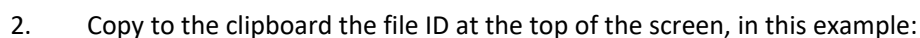
4. Move the cursor down the list of **Available fields** to select fields to filter. Then click on the **add** button to add the field to the filter:



5. In the example below, the following fields are added:
  - ◆ **@l** - level
  - ◆ **@mt** - message template
  - ◆ **@x** - exception
  - ◆ **ContainerName**
  - ◆ **CorrelationId**
6. The display of hits is now updated to show only the selected fields:



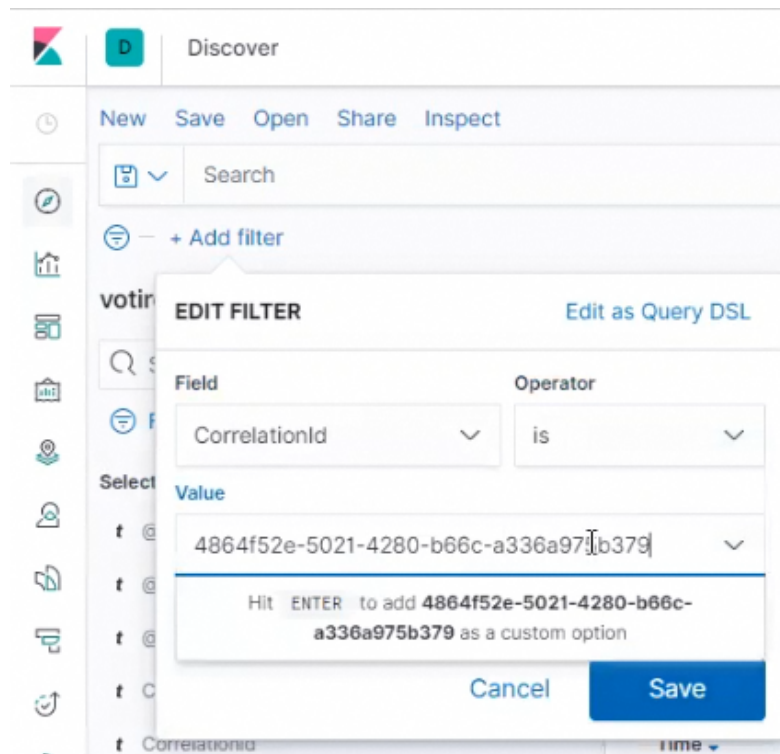
1. Open the Votiro Explore Incident:



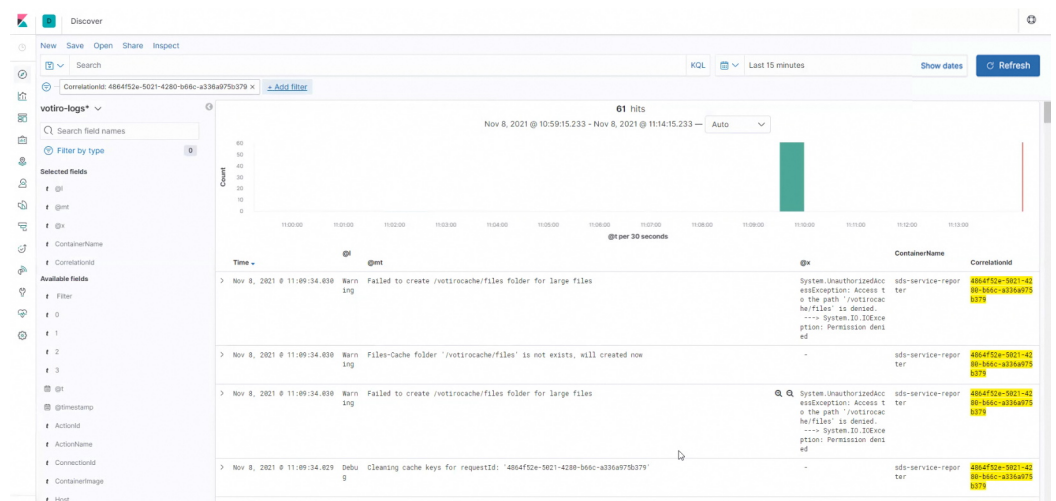
### 4.3.3 File Sanitization Analysis


1. Return to the Kibana Discover screen.
2. In the left side of the Kibana Discover screen, click on **Add filter**. The **EDIT FILTER** window opens.
3. From the **Field** list, select **CorrelationId**.
4. From the **Operator** list, select **is**.

5. In the **Value** field, paste the file ID from the clipboard .



6. Click on **Save**. The list of hits displayed is updated to show only those hits for the relevant file, according to the CorrelationId (= Votiro item).



7. To change the time frame of the display, click on the time icon . Then select the desired time interval:

The screenshot shows the Votiro Kibana interface's date range selector. At the top, a time range is set from '~ 15 minutes ago' to 'now'. Below this is a 'Quick select' section with a dropdown menu set to 'Last', a text input field containing '15', a unit dropdown set to 'minutes', and an 'Apply' button. A hand cursor is pointing at the 'Quick select' header. Underneath, there are two columns of 'Commonly used' date ranges: 'Today', 'This week', 'Last 15 minutes', 'Last 30 minutes', 'Last 1 hour', 'Last 24 hours', 'Last 7 days', 'Last 30 days', 'Last 90 days', and 'Last 1 year'. Below these is a 'Recently used date ranges' section with links for 'Today', 'This week', and 'Last 30 minutes'. At the bottom, there is a 'Refresh every' section with a text input field set to '0', a unit dropdown set to 'seconds', and a 'Start' button with a play icon.

8. To view the file processing history in Votiro, scroll down the list of hits. The selected fields displayed in the columns provide more information as to what occurred during the processing. Using the **@l** (message level), **@mt** (message template) and **@x** (exceptions) columns provides you with detailed information that can help you to troubleshoot the incident.



## 5 MSSP User Guide

A Managed Security Service Provider (MSSP) provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.

Examples of MSSP use cases supported by Votiro include:

- Creating new customers and assigning licenses by the MSSP admin
- Viewing/filtering all the MSSP customer's data on the MSSP dashboard
- Using the MSSP incidents to see/filter all the MSSP customer's incidents data
- Creating reports on each MSSP customer's data

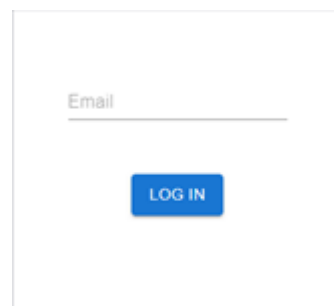
### 5.1 MSSP Tenant Management

#### 1. Login

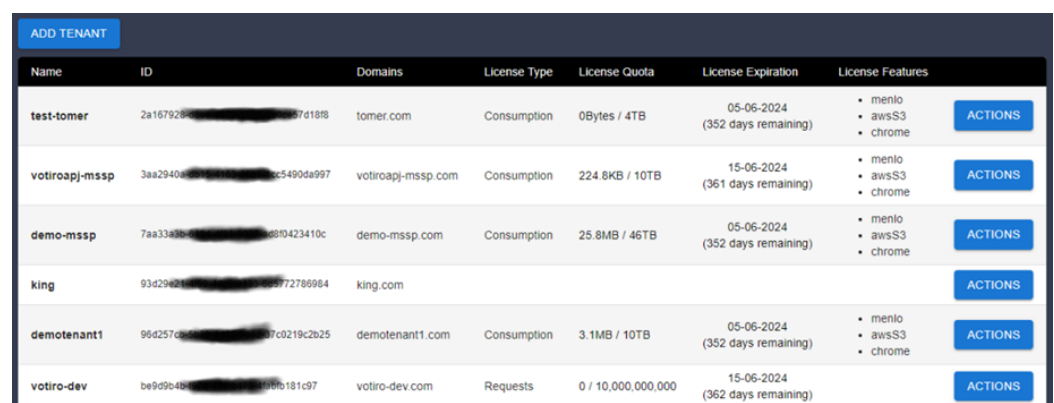
To login to MSSP Tenant Management, use the following URL address:

"https://{clusterName}/portal/#/votiro/login"

A login page will be displayed. Contact Votiro support to get the admin user credentials.



After successful login, the Votiro MSSP Tenant Management screen is displayed:



| Name           | ID                        | Domains            | License Type | License Quota      | License Expiration                 | License Features               | ACTIONS |
|----------------|---------------------------|--------------------|--------------|--------------------|------------------------------------|--------------------------------|---------|
| test-tomer     | 2a167928-...-07d18f8      | tomer.com          | Consumption  | 0Bytes / 4TB       | 05-06-2024<br>(352 days remaining) | • menlo<br>• awsS3<br>• chrome | ACTIONS |
| votiroapj-mssp | 3aa29408-...-5490da997    | votiroapj-mssp.com | Consumption  | 224.8KB / 10TB     | 15-06-2024<br>(361 days remaining) | • menlo<br>• awsS3<br>• chrome | ACTIONS |
| demo-mssp      | 7aa33a3b-...-85f0423410c  | demo-mssp.com      | Consumption  | 25.8MB / 46TB      | 05-06-2024<br>(352 days remaining) | • menlo<br>• awsS3<br>• chrome | ACTIONS |
| king           | 93d29621-...-5372786984   | king.com           |              |                    |                                    |                                | ACTIONS |
| demotenant1    | 96d257c0-...-7fc0219c2b25 | demotenant1.com    | Consumption  | 3.1MB / 10TB       | 05-06-2024<br>(352 days remaining) | • menlo<br>• awsS3<br>• chrome | ACTIONS |
| votiro-dev     | be9d9b4b-...-15f0b181c97  | votiro-dev.com     | Requests     | 0 / 10,000,000,000 | 15-06-2024<br>(362 days remaining) |                                | ACTIONS |

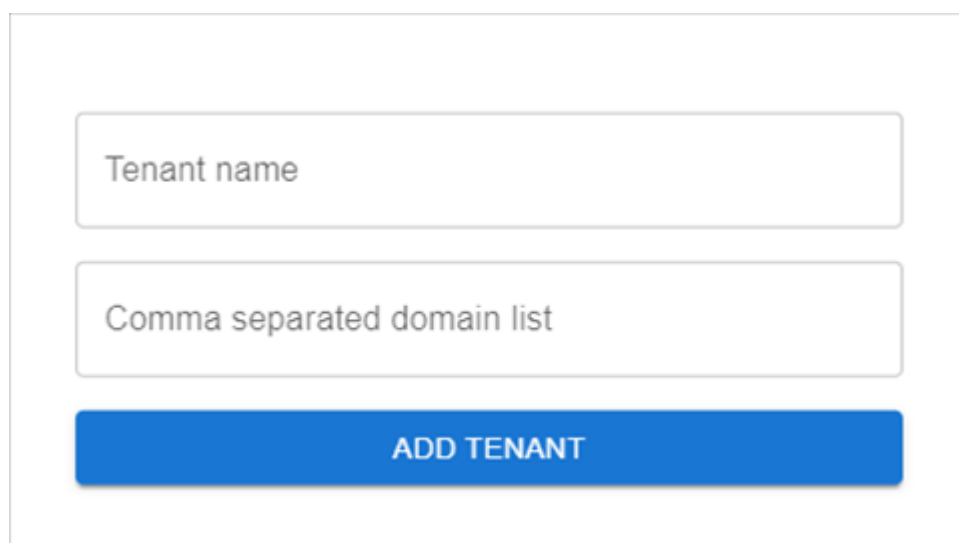
The MSSP admin can use the Tenant Management screen to:

- ◆ Add a customer tenant

- ◆ View the list of customer tenants
- ◆ View customer traffic information
- ◆ Manage each customer tenant's license
- ◆ View total actual usage compared to total license quota
- ◆ Delete customer tenants

## 2. Add a customer tenant

To add a new customer tenant, press the **ADD TENANT** button.



Enter:

- ◆ **Tenant name** - for example, King Demo
- ◆ **Comma separated domain list** - for example, kingdemo.com. If there are multiple domains, separate the domains by a comma. For example, kingdemo.com, rontest.com

After adding a new customer tenant, a default admin user will be created. Contact Votiro support to get the admin user credentials.

## 3. View the customer's tenant list

The following information is displayed on the Tenant Management screen for each tenant:

- ◆ **Name** - Tenant name as configured in creation
- ◆ **ID** - Tenant ID generated in UUID format
- ◆ **Domains** - As configured in creation
- ◆ **License Type** - The possible options are:
  - **Consumption** - count by volume usage
  - **Requests** - count by files

- ◆ **License Quota** - Actual usage / License quota, as configured in the license import. The system will display up to date tenant usage.
- ◆ **License expiration** - Expiration date and days remaining
- ◆ **License features** - Currently, the possible options are:
  - menlo
  - aws s3
  - chrome

#### 4. Import a license

To import a license for a customer tenant, press the corresponding **ACTIONS** button and select **IMPORT LICENSE**.

---

License type

REQUESTS **CONSUMPTION** OBSOLETE

---

License Usage: 110TB/50TB

Size

0

GB TB

Start date

12/06/2023

End date

19/06/2024

Feature flags

- ☐ Menlo
- ☐ AWS S3
- ☐ Chrome
- ☐ URL Reputation Coming soon

ADD LICENSE

---

Enter or select:

- ◆ License type
- ◆ License Usage
- ◆ Start date
- ◆ End date
- ◆ Feature flags (if needed)

After creating a license, the system will display the imported license in:

- ◆ Votiro MSSP Tenant Management screen
- ◆ Customer tenant Management console license page

5. **Download Analytics Report**

To download an analytics report for any of the customer's tenants, press the corresponding **ACTIONS** button and select **DOWNLOAD REPORT**.

Start date

01/05/2023

End date

19/06/2023

GENERATE REPORT

Enter the **Start date** and **End date** to select the report's time interval, and press **GENERATE REPORT**. The report will be downloaded in CSV format.

AutoSave Off Votiro\_Summary\_Extended\_Report\_For\_Tenant\_7aa33a3b-6194-4f81-9027-ad8f0423410c\_01\_05\_2023\_20\_06\_202...

File Home Insert Page Layout Formulas Data Review View Automate Help Acrobat

Clipboard Font Alignment Number

|    | A                                   | B                       | C                | D | E | F | G | H |
|----|-------------------------------------|-------------------------|------------------|---|---|---|---|---|
| 1  | Customer name                       | Ron company             |                  |   |   |   |   |   |
| 2  | Report dates                        | 01/05/2023 - 20/06/2023 |                  |   |   |   |   |   |
| 3  | Total Files processed               |                         | 16               |   |   |   |   |   |
| 4  | Total Files sanitized               |                         | 15               |   |   |   |   |   |
| 5  | Total Files blocked                 |                         | 1                |   |   |   |   |   |
| 6  | Total PPF files detected            |                         | 0                |   |   |   |   |   |
| 7  | Number of emails                    |                         | 1                |   |   |   |   |   |
| 8  | Number of threats detected          |                         | 2                |   |   |   |   |   |
| 9  | Average file size                   | 1672870 bytes           |                  |   |   |   |   |   |
| 10 | Average processing time             | 6.3325 seconds          |                  |   |   |   |   |   |
| 11 |                                     |                         |                  |   |   |   |   |   |
| 12 | License mode files                  | Consumption             |                  |   |   |   |   |   |
| 13 | License permitted files             |                         | 5.05775E+13      |   |   |   |   |   |
| 14 | Number of Files used so far         |                         | 16               |   |   |   |   |   |
| 15 | License permitted consumption quota |                         | 5.05775E+13      |   |   |   |   |   |
| 16 | License consumption used so far     |                         | 27024047         |   |   |   |   |   |
| 17 | License usage                       |                         | 0.00%            |   |   |   |   |   |
| 18 | Expiration date                     |                         | 05/06/2024 15:13 |   |   |   |   |   |
| 19 |                                     |                         |                  |   |   |   |   |   |
| 20 |                                     |                         |                  |   |   |   |   |   |

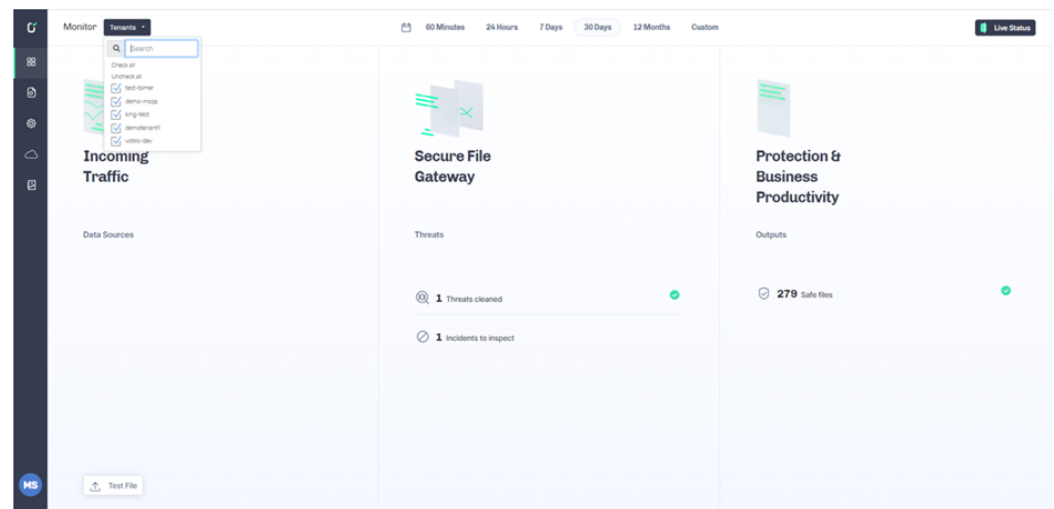
## 6. Delete a customer tenant

To delete a customer tenant, press the corresponding **ACTIONS** button and select **DELETE TENANT**.

## 5.2 Monitoring Tenant Activity

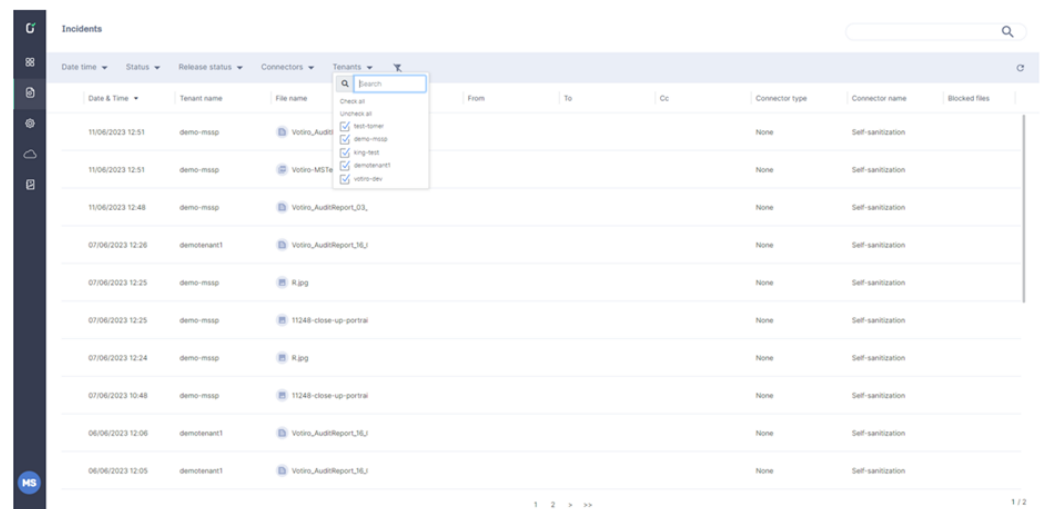
### 1. MSSP Dashboard

The MSSP user can view and filter Dashboard data by customers tenant selection.



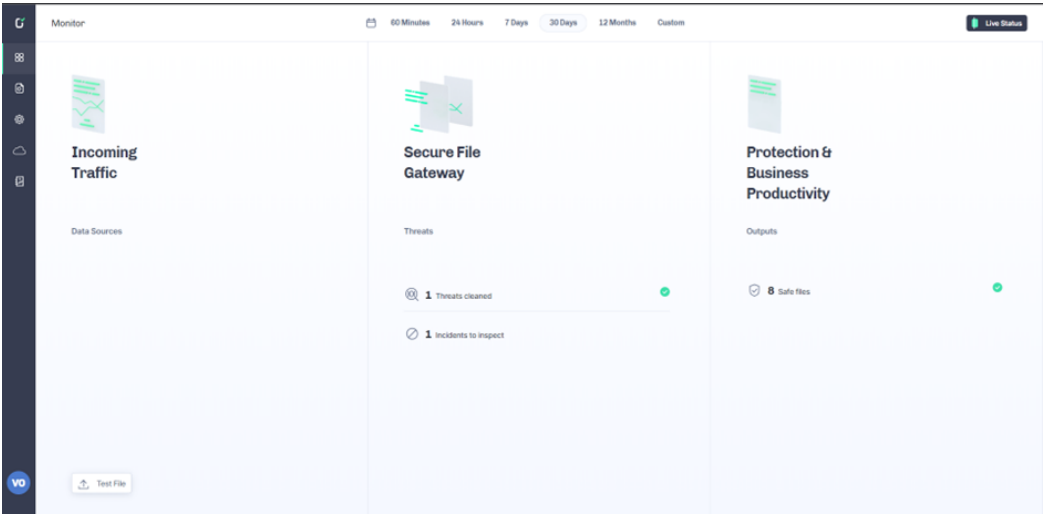
### 2. MSSP Incidents

The MSSP user can view and filter incidents data by customer tenant selection in the **Tenants** column.



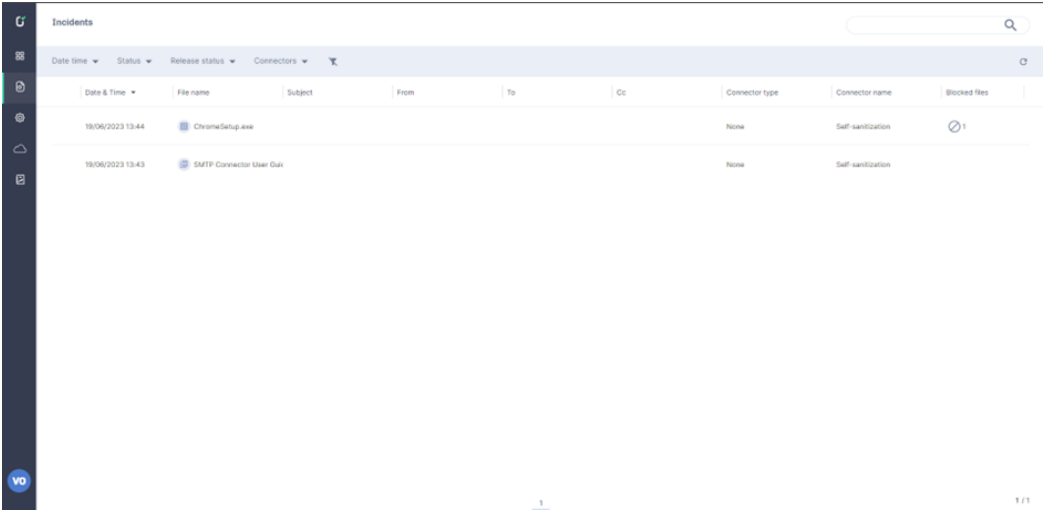
### 3. MSSP Customer's Dashboard

An MSSP customer's user can view data only from their own tenant.



4. MSSP Customer's Incidents

An MSSP customer's user can view data only from their own tenant.





## 6 How to Use QR Code Sanitization

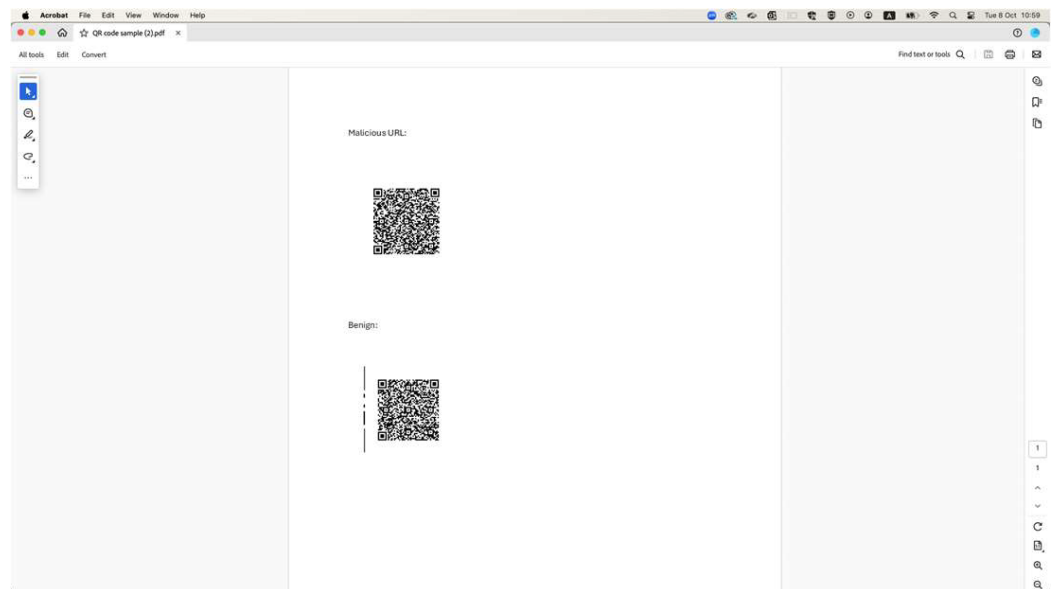
Votiro supports QR Code sanitization. This is relevant for PDFs and emails containing QR codes.

There are four options when dealing with QR codes:

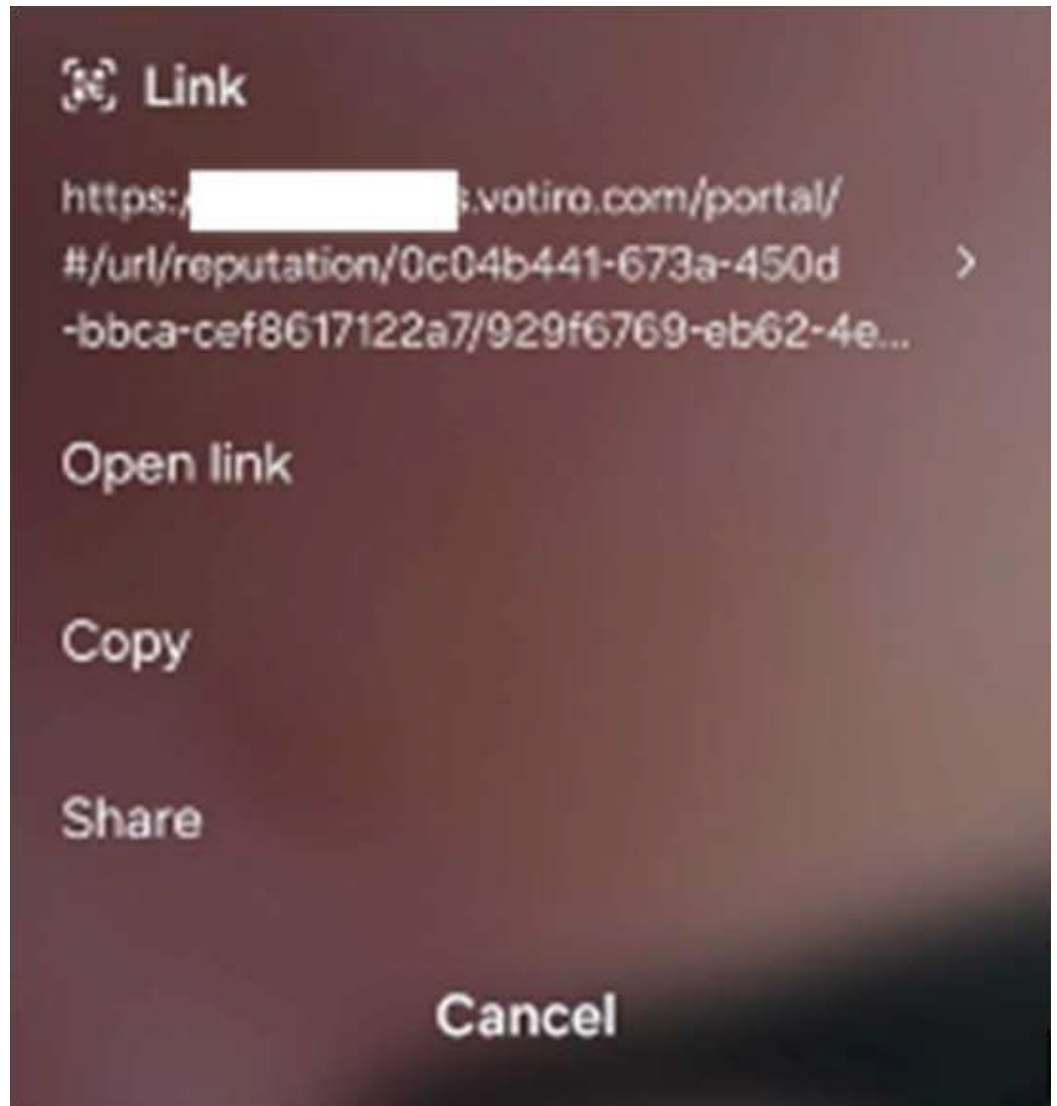
- Ignore - the QR Code is ignored. The file or email is passed on as-is.
- Detect QR Codes - detect if there is a QR Code in the file.
- Disarm QR Codes - the original QR code is rewritten with the Votiro QR Code.
- Block QR Codes - Votiro blocks the QR Code.

### 6.1 Disarm QR Codes behavior

1. The user scans the QR Code.



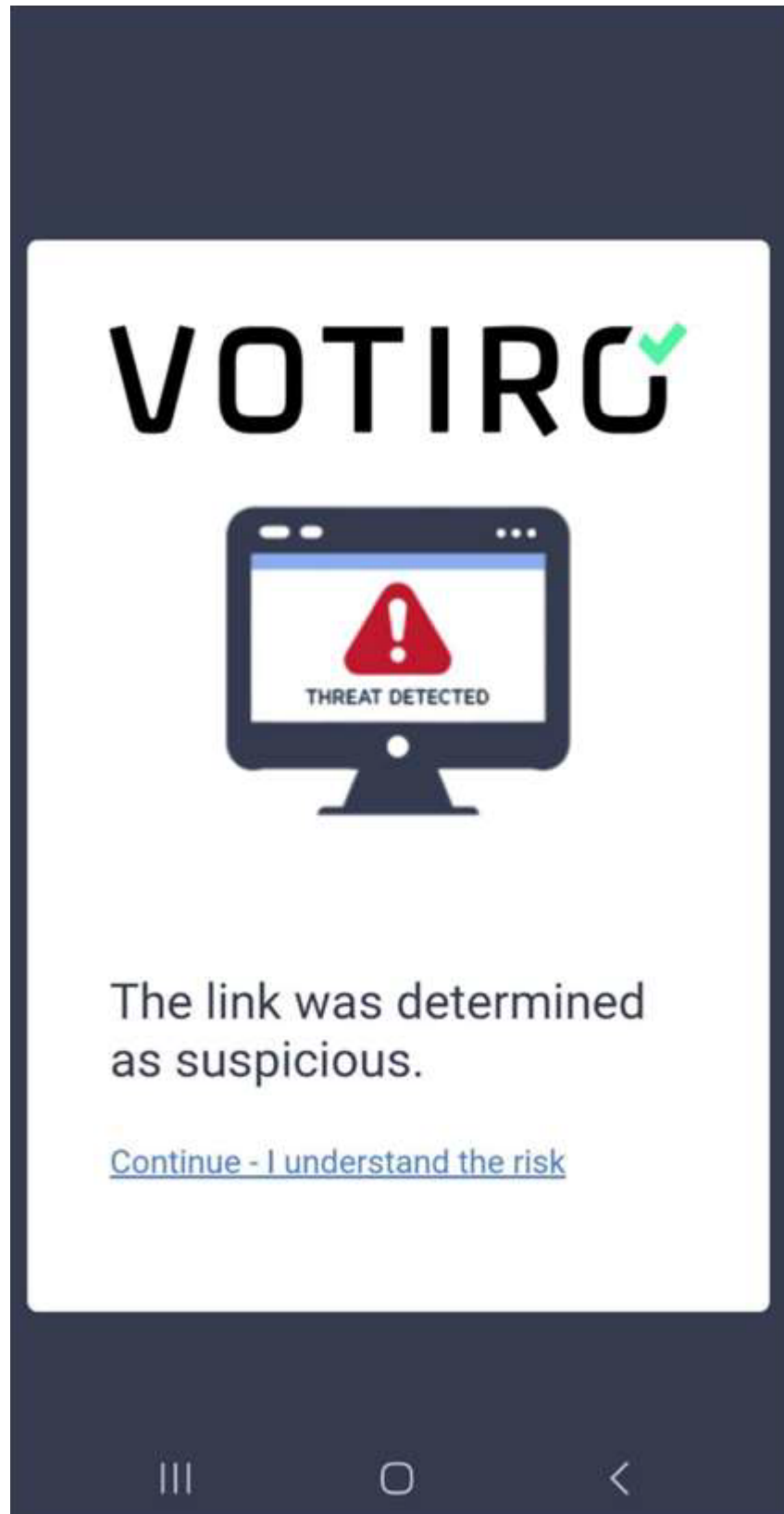
2. There will be an indication that the original QR Code was replaced with a Votiro QR Code pointing to the Votiro portal.



3. The user opens the link and is redirected to the Votiro portal. Votiro analyzes the URL for suspicious activity.



4. When the analysis completes:
  - ◆ If the URL was determined to be benign, the user will be redirected to the URL.
  - ◆ If the URL was determined as suspicious, the user will receive an indication that a threat was detected.



## 6.2 Votiro Administrator view

The file event will indicate if a:

- QR Code was detected and was rewritten by Votiro.
- Suspicious URL was detected.

For example:

