

VOTIRO[✓]

Votiro SaaS

Knowledge Base

July 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

Contents

1 How to Integrate Azure AD Single Sign-on with Votiro using the Entra SAML Toolkit	5
1.1 Prerequisites	5
1.2 Configure the Azure Portal	5
1.3 Configure the Votiro Management Console	8
2 How to Integrate SIEM with Azure Sentinel	11
2.1 System prerequisites	11
2.2 Procedure	11
2.2.1 Manual/Offline Deployment	11
3 How to Integrate Votiro with Google Workspace	23
3.1 Procedure	23
3.1.1 Create a Host	24
3.1.2 Configure content compliance rule for emails received from Votiro	25
3.1.3 Configure Content compliance rule for emails sent to Votiro	29
3.1.4 Votiro Cloud for Sanitization	30
3.1.5 Spam Rule	31
3.1.6 Prevent Email Authentication Protocol Failures	31
3.1.7 How To Resolve Google's SPAM Email Alert On SaaS	32
4 How to Send Files to Votiro via Postman	34
4.1 Prerequisites	34
4.2 Procedure	34
4.2.1 Generating a Service Token	34
4.2.2 Postman Setup	38
5 How to Use Kibana to Troubleshoot Votiro Incidents	45
5.1 Example of Votiro Incident	45
5.2 Procedure	45
5.2.1 Create and Configure an Index Pattern	45
5.3 Analyze the Data	47
5.3.1 Discover	48
5.3.2 Votiro Explore Incident & File Info	52

- 5.3.3 File Sanitization Analysis52
- 6 MSSP User Guide 55**
 - 6.1 MSSP Tenant Management55
 - 6.2 Monitoring Tenant Activity 61
- 7 How to Use QR Code Sanitization 63**
 - 7.1 Disarm QR Codes behavior 63
 - 7.2 Votiro Administrator view 68
- 8 URL Protection 69**
 - 8.1 Workflow - Sanitize URLs69

1

How to Integrate Azure AD Single Sign-on with Votiro using the Entra SAML Toolkit

This tutorial demonstrates how to integrate the Microsoft Entra SAML Toolkit App with Votiro, enabling users to access the Votiro Management console using their corporate credentials.

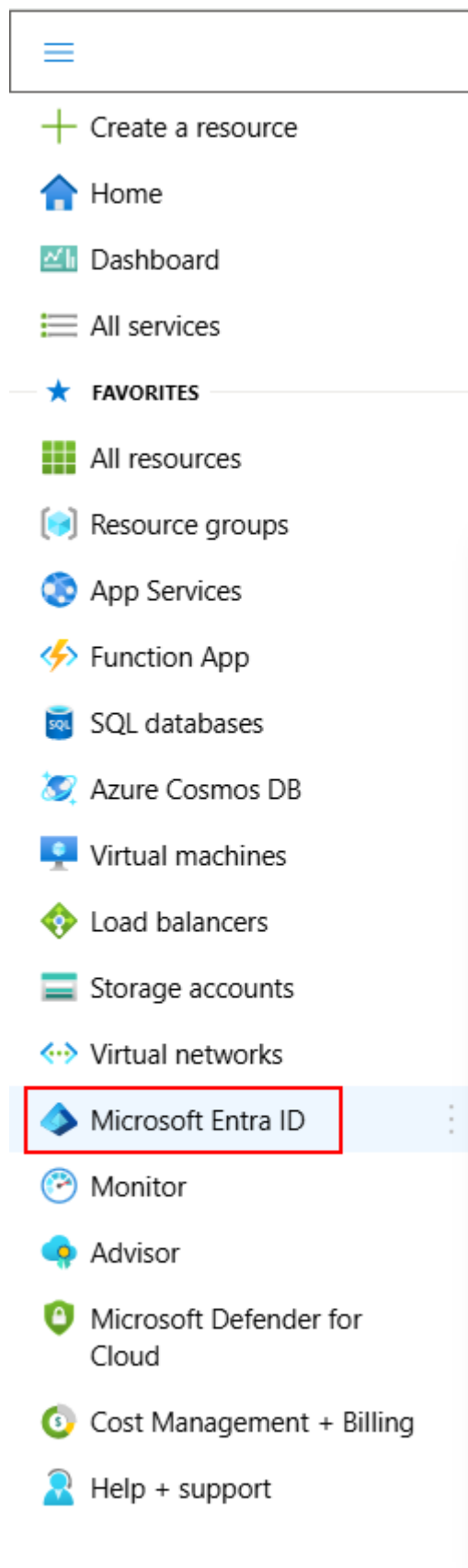
1.1 Prerequisites

Ensure you have the following items:

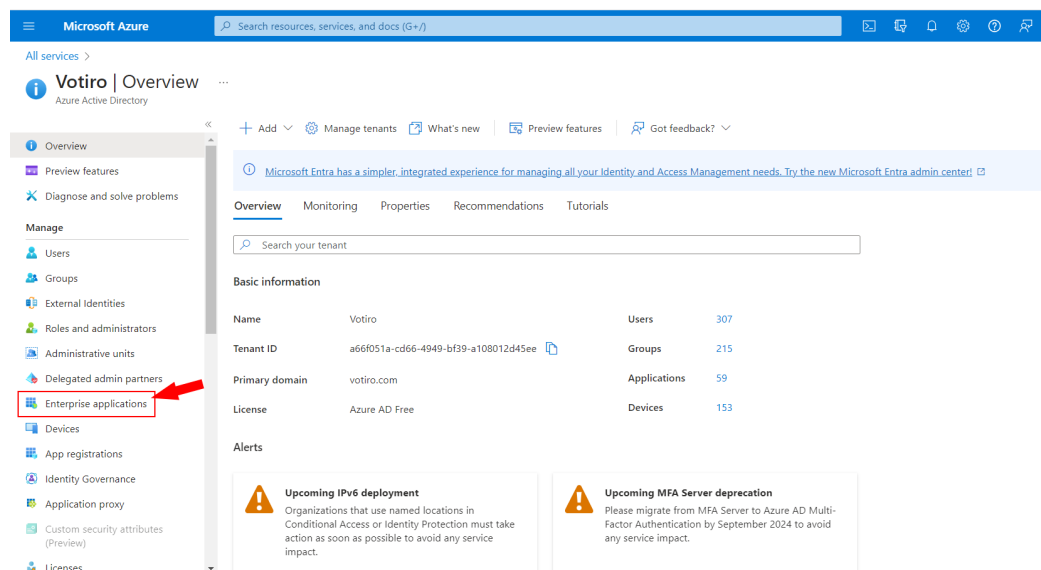
- Azure AD subscription
- Azure AD SAML Toolkit enabled on the above-mentioned subscription
- Admin permissions
- **Votiro Tenant Id** - this can be obtained from the Votiro Management console. Navigate to **System settings** > **System Configuration**.

1.2 Configure the Azure Portal

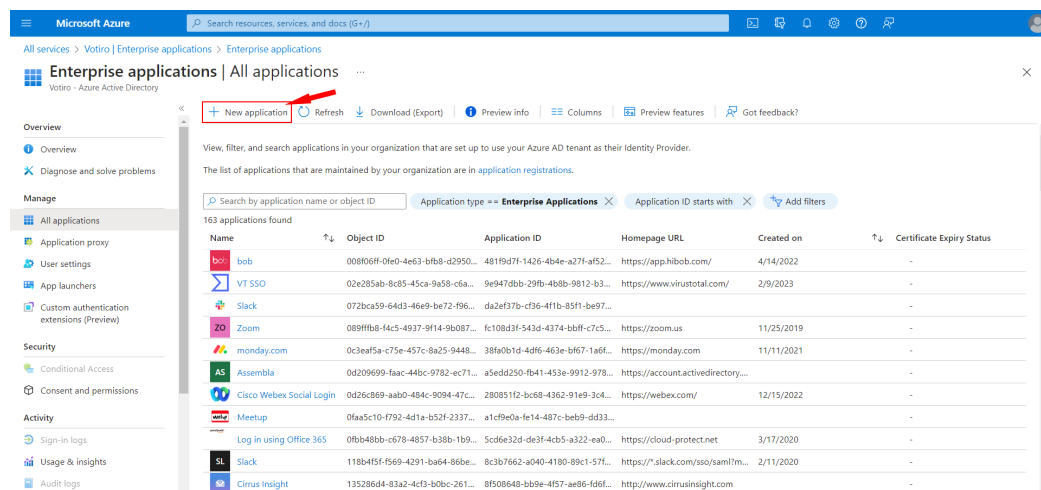
1. Sign in to the [Azure portal](#).
2. In the left pane, open the **portal menu** and select **Microsoft Entra ID**.



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



4. Select New application:

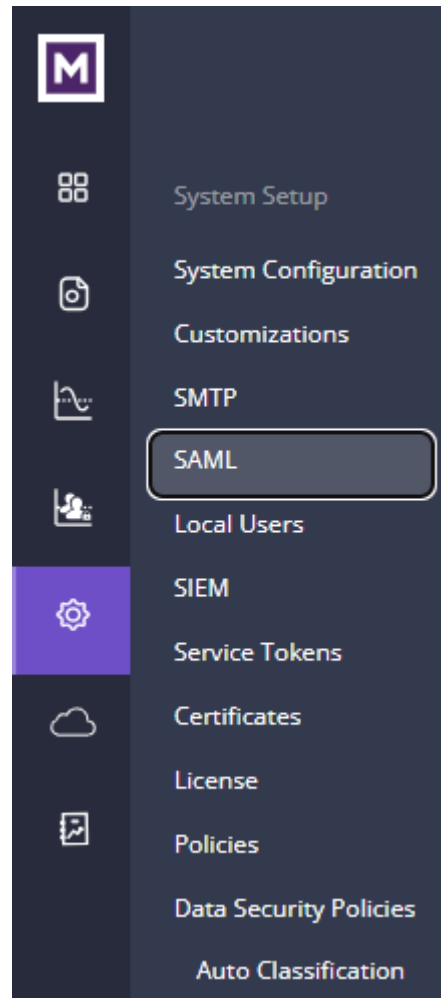


5. In the search field type **Azure AD SAML Toolkit**. In the **Search by application name or object ID** field, type "toolkit" to locate the **Microsoft Entra SAML Toolkit** and select it.
6. You will be prompted to select a new name for the application in a separate window, and once you have completed this step, click **Create**.
7. After a few moments, the app will be added to your tenant and is presented as an **Overview**.
8. Under **Getting Started**, select **Assign users and groups** to add the desired groups. Consider creating three groups with different permission levels to match Votiro's side (Admins, HelpDesk, Soc). Ensure they are created under the same domain name.
9. Select **Single sign-on** located under **Users and Groups**.

10. Select the Single Sign-On method: **SAML**, and click **Edit** under **Basic SAML Configuration**, and fill in as follows:
 - a. For **Identifier (Entity ID)**, leave as default - <https://samltoolkit.azurewebsites.net>.
 - b. Both **Reply URL (Assertion Consumer Service URL)** and **Sign on URL** should be in the following format: https://<Votiro-FQDN>/assertionconsumerservice/<Votiro_TenantID>.
 - c. Click **Save**.
11. In the **Attributes & Claims** section, click **Edit**.
 - a. Click **+ Add a Group claim**.
 - b. Under **Which groups associated with the user should be returned in the claim?**, select **Groups assigned to the application** to direct a user's lookup to the groups assigned to the app, as configured in [step 8](#).
 - c. Under **Advanced Options**, check **Customize the name of the group claim**. Name the Group Claim as "VotiroGroups" under **Name**.
 - d. Click **Save**.

1.3 Configure the Votiro Management Console

1. Log in to Votiro's Management console using a local user account.
2. On the left pane, click on the cogwheel, and select **SAML**.



3. The SAML configuration page is displayed:

- a. For the **IDP Metadata address**, copy and paste the value from the **App Federation Metadata Url** field in Azure.
 - b. For the **Issuer**, copy and paste the value from the **Identifier (Entity ID)** the unique ID identifier field in Azure.
 - c. For the **SAML Username identifier**, leave by default:
<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier>
 - d. The **Admin role key** should be the value you provided for the group above in **Group Claims**, in this example, "VotiroGroups".
 - e. The **Admin role value** should be the Object Id of the group "admins".
 - f. For **Help-Desk role key**, enter the name of the group claim - in this example, "VotiroGroups".
 - g. For **Help-Desk role value**, enter the ObjectID of group "HelpDesk".
 - h. For **SOC role key**, enter the name of the group claim - in this example, "VotiroGroups".
 - i. For **SOC role value**, enter the ObjectID of the group "Soc".
4. Save your changes.
 5. Log out as the local user from the Management console.
 6. Log in to the Votiro Management console with corporate credentials using SAML Single Sign On. For more information, see [Logging in to the Management Dashboard: VA on-premises](#).

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](#)

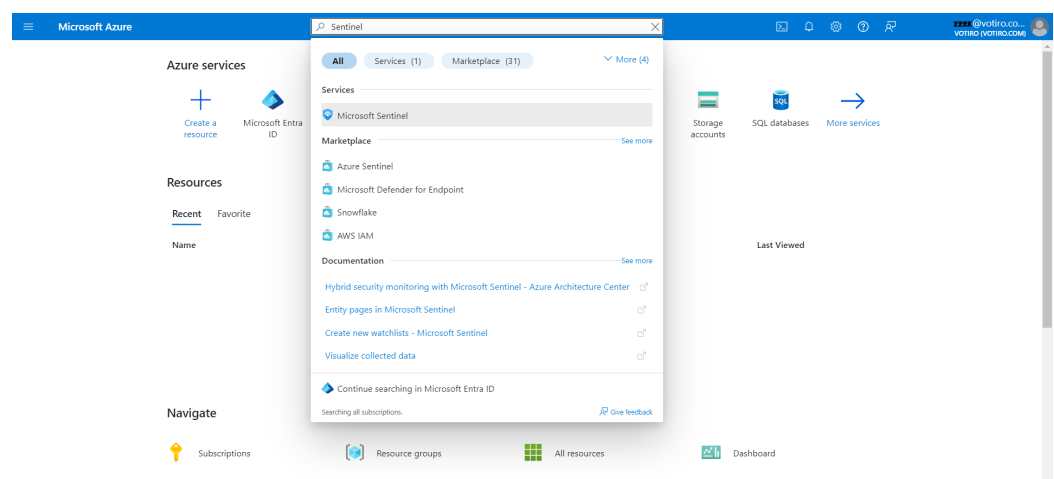
2.2 Procedure

2.2.1 Manual/Offline Deployment

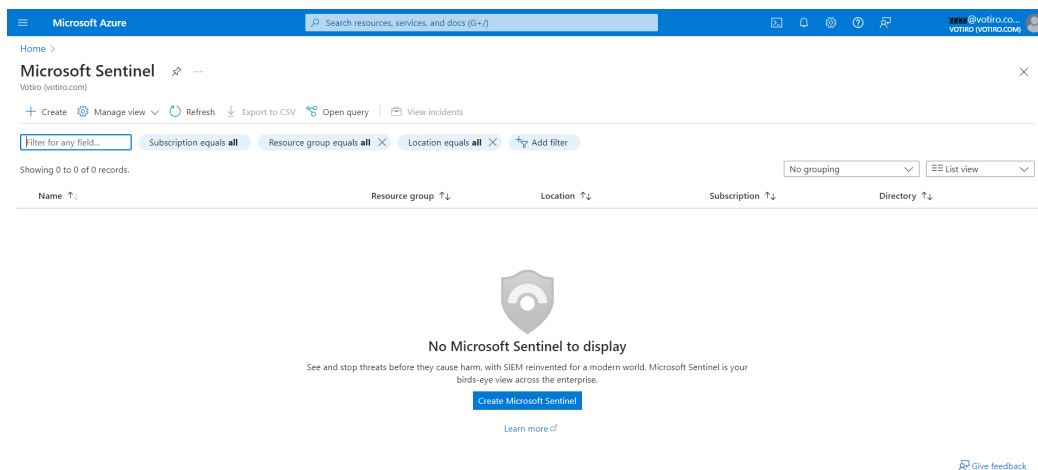
To test the solution before publishing, follow the below steps.

Deploy CEF Data Connector on Forwarder Machine

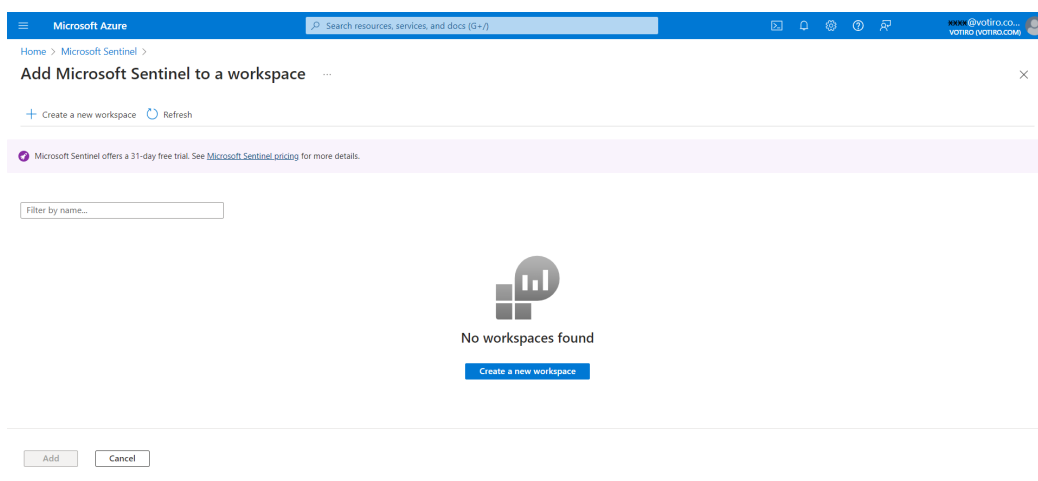
1. Sign in to the [Azure portal](#).
2. Search for **Microsoft Sentinel**.



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**:

Microsoft Azure

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace >

Create Log Analytics workspace

Basics Tags Review + Create

Basics

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

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

Subscription *

Resource group *

[Create new](#)

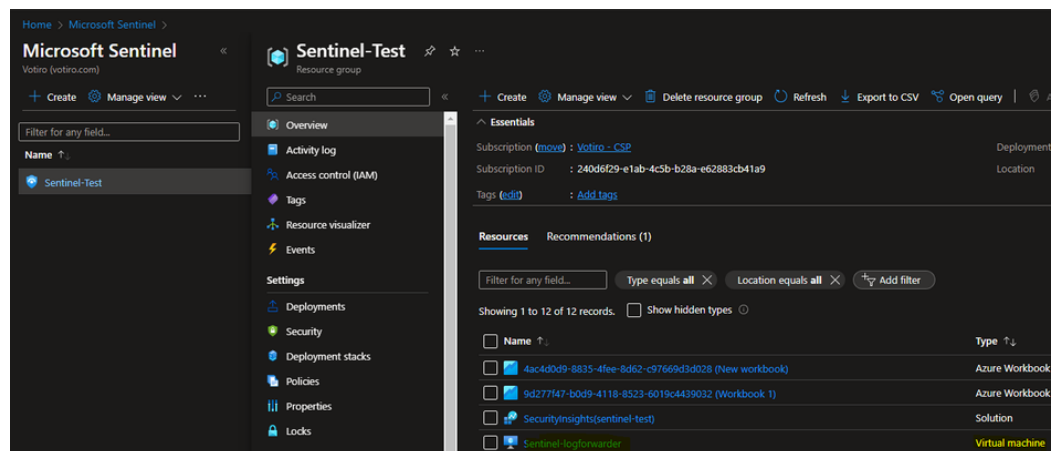
Instance details

Name *

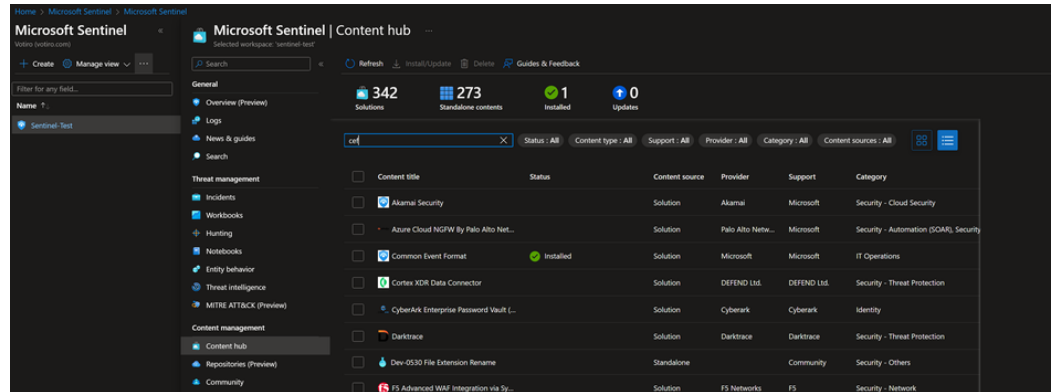
Region *

[Review + Create](#) < Previous Next: Tags >

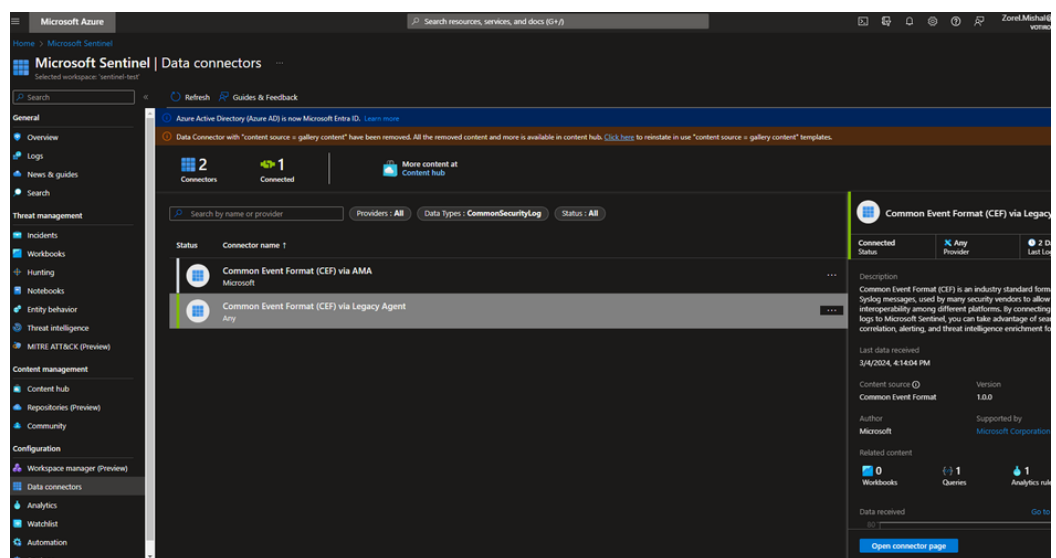
6. Create a new **Resource Group** if it does not exist yet. Then create a new machine with the system requirements mentioned above → via Resource Group > Create > select Virtual Machine (Ubuntu 22.06 server is recommended):



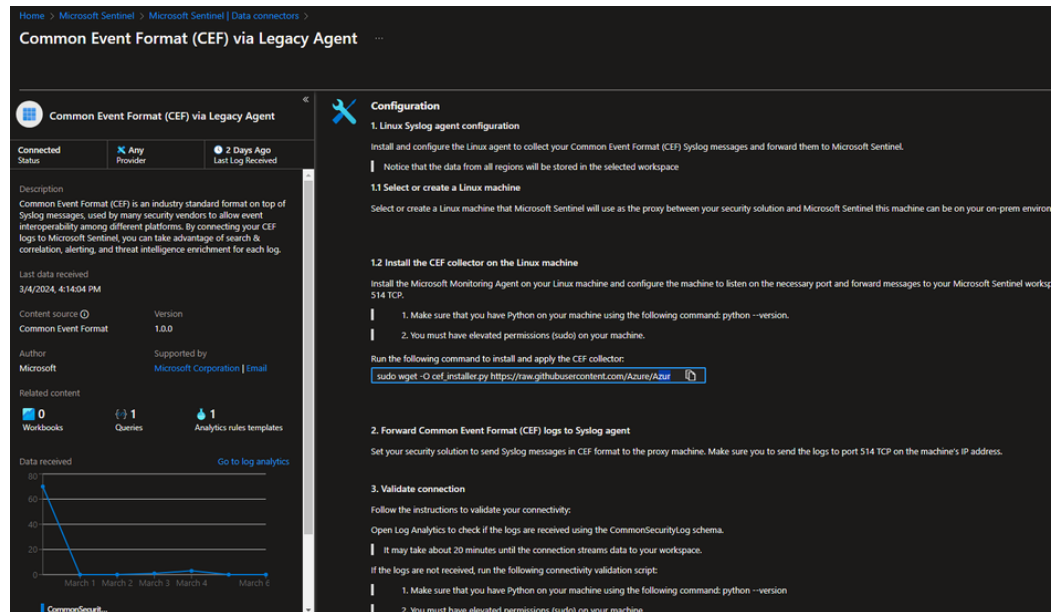
7. Select the created workspace, then go to Content Hub > Select Common Event Format (CEF) and install it:



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:

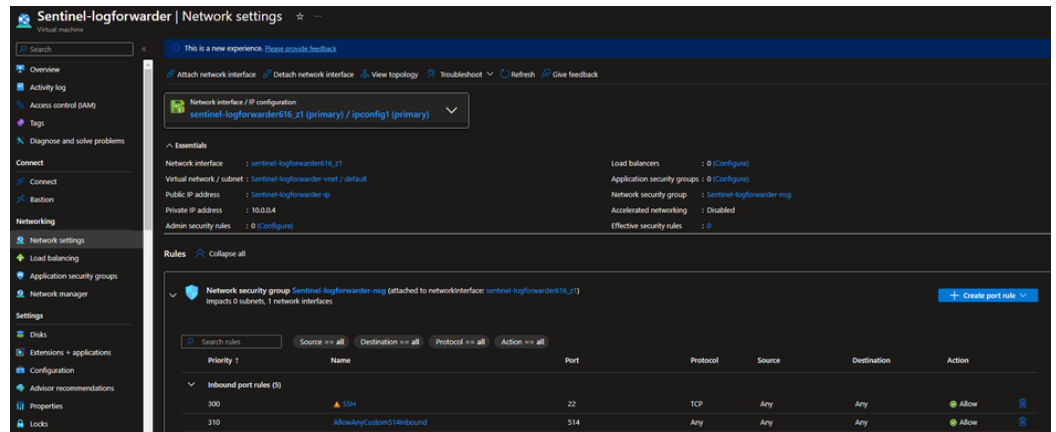
```
python --version or python3 --version
```

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:



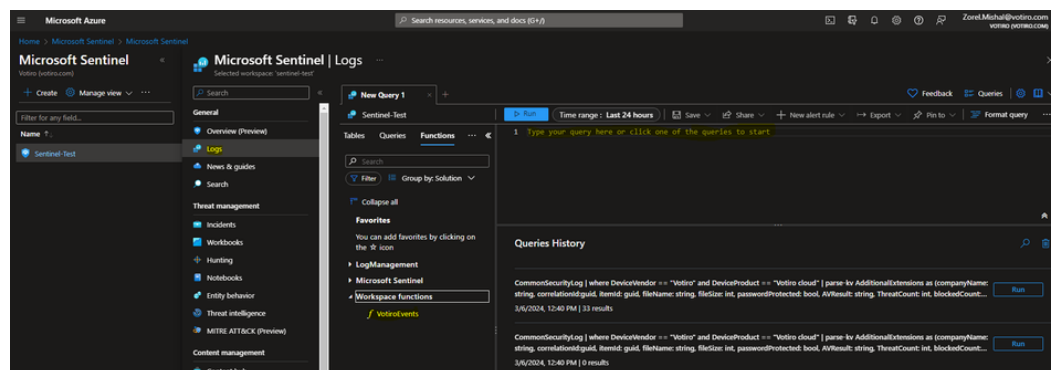
Note: In this case, we used TCP port 514 (default) and **Allow=any**, but the best practice is to use the TLS protocol with other ports used and restrict to specific IPs pointed to specific NAT gateways. For example, in [prod.us](#):

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

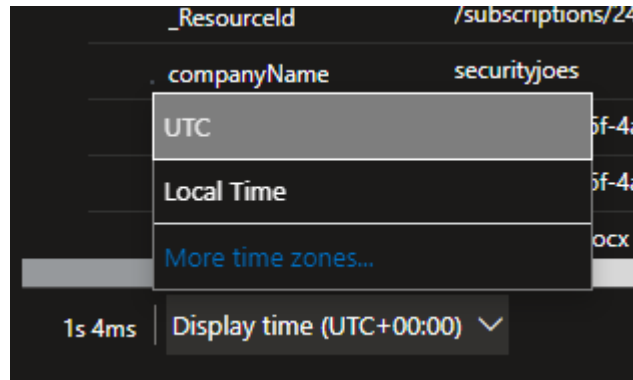
Cancel

- 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

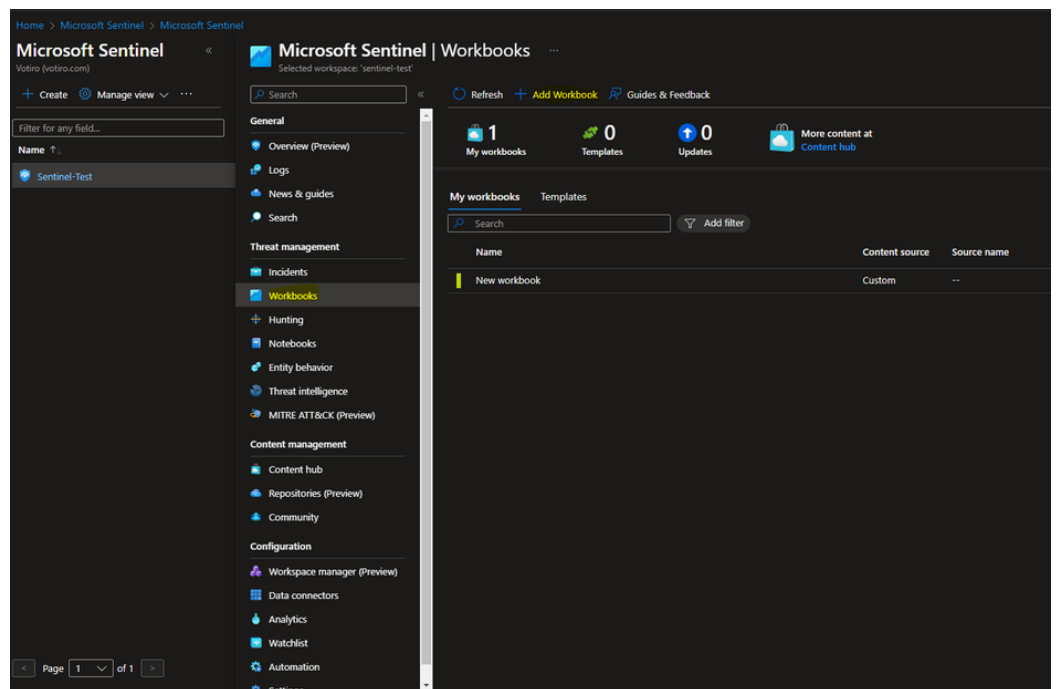
Field	Value
TenantId	6c0fa6d8-ec71-4593-8e5f-45b4f7770685
TimeGenerated [UTC]	2024-03-03T14:04:30.713Z
DeviceVendor	Votiro
DeviceProduct	Votiro cloud
DeviceVersion	1.0.0.0
DeviceEventClassID	500
Activity	Sanitization summary
LogSeverity	1
FileHash	fa2742aec57ae5a21e80a0cf7767af566ba48e0b035fa5546fc34e2898a31ad6
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:

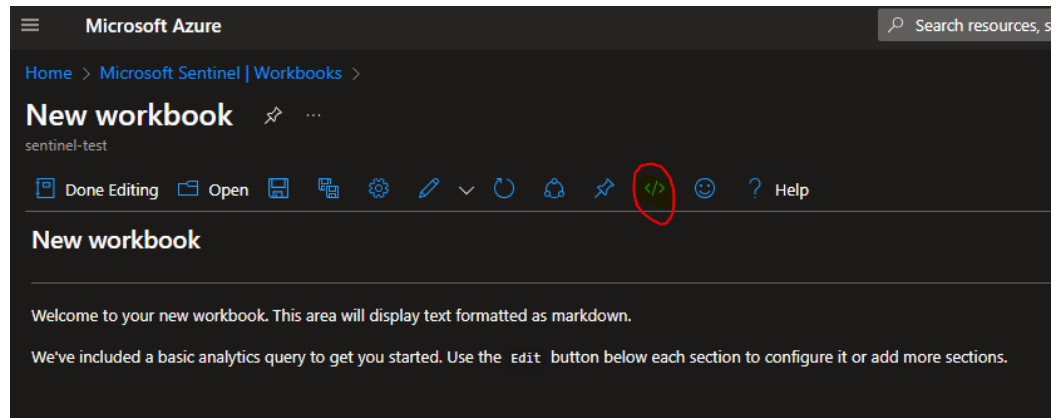


Deploy the Workbook

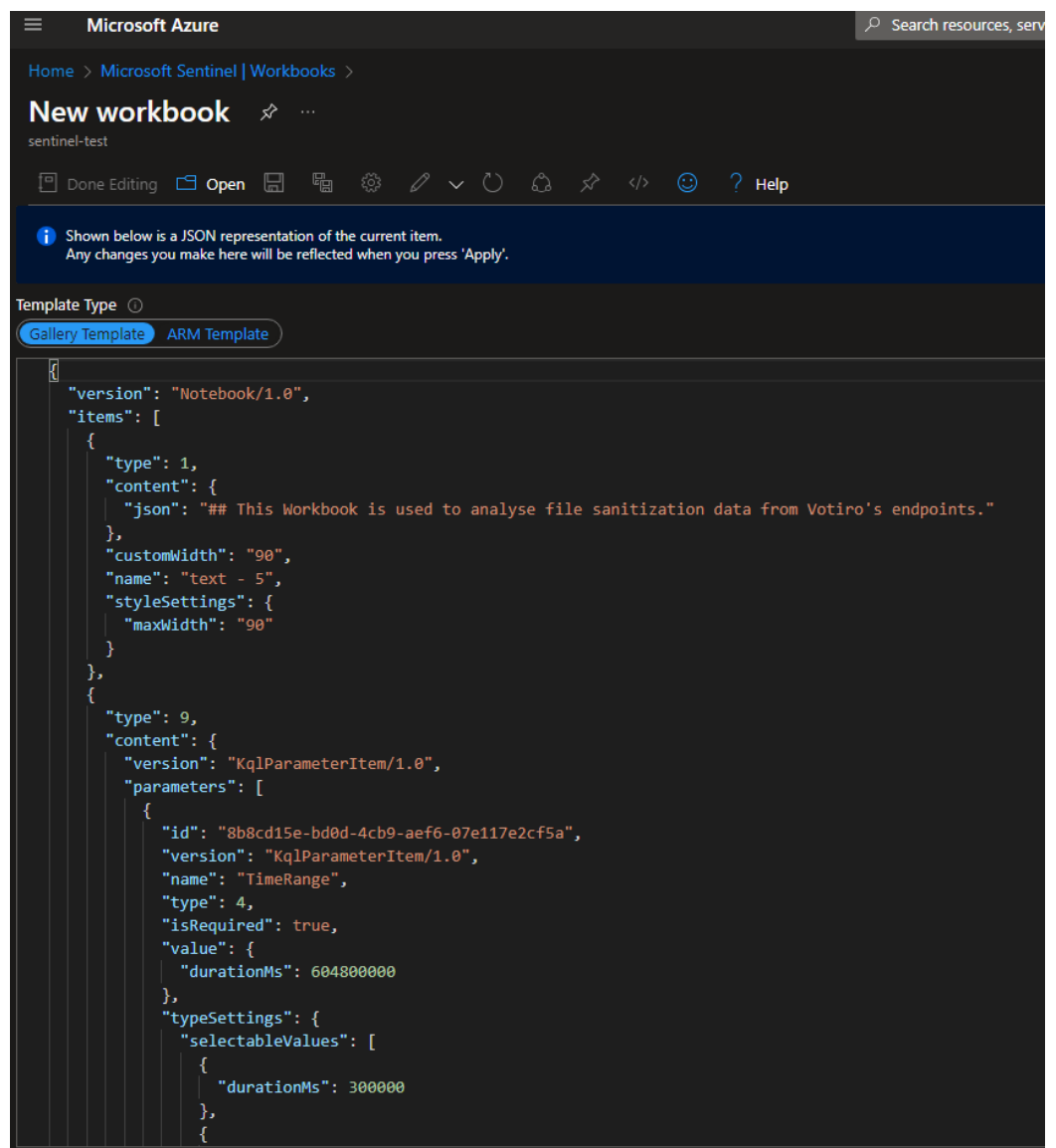
1. Copy the contents of the file:
/Votiro-Offline/Workbooks/Votiro Monitoring Dashboard.json
2. On Microsoft Sentinel, go to your WorkSpace > Workbooks > **Add Workbook**:



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



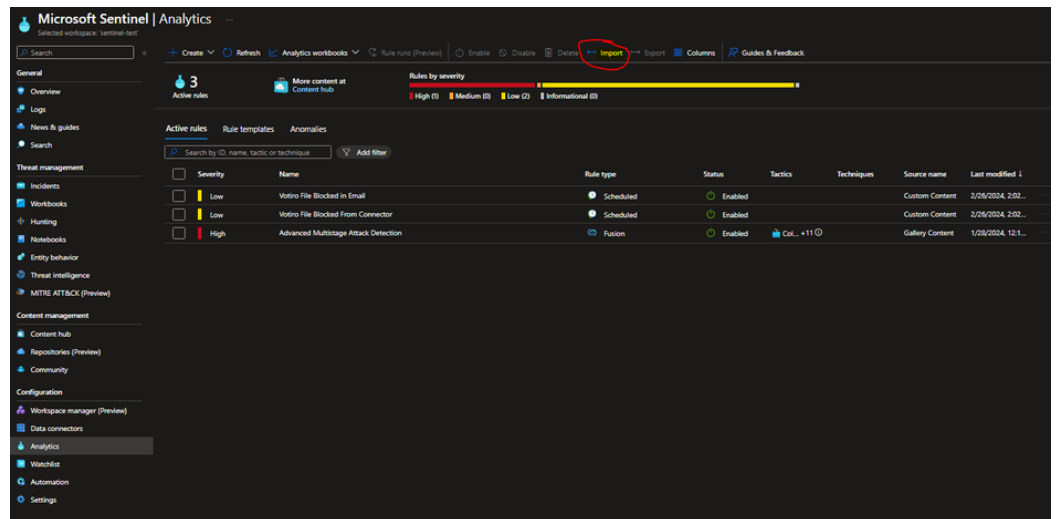
4. Replace the Gallery template contents with the copied contents, and click on **Apply**:



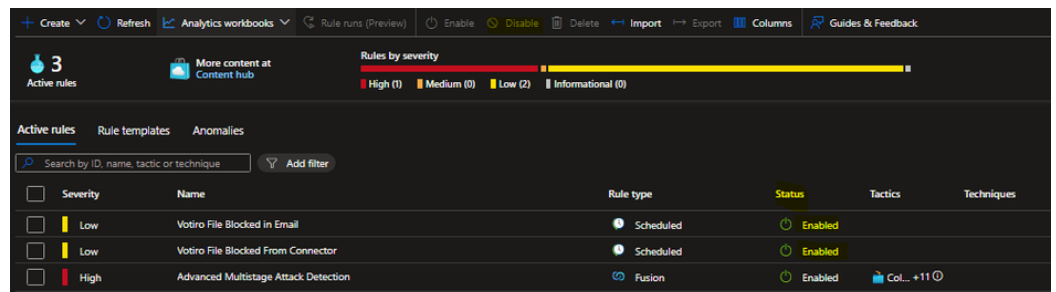
5. The Following Workbook must be visible:
After a scroll

Set Alert Queries for Incidents

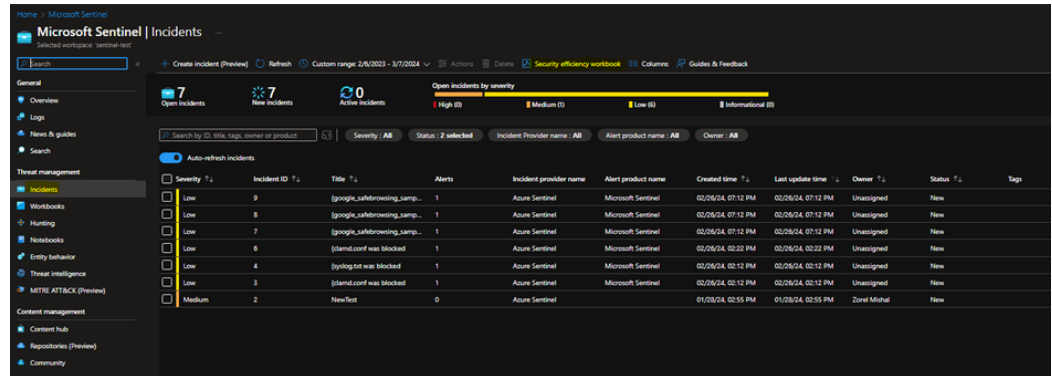
1. Go to **/Votiro-Offline/Analytic Rules**. Keep both **Votiro File Blocked FromConnector.json** and **Votiro File Blocked in Email.json** files ready.
2. On Microsoft Sentinel > Workspace, select **Analytics**.
3. Click **Import** (from the bar at the top of the screen) in the resulting dialog box,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

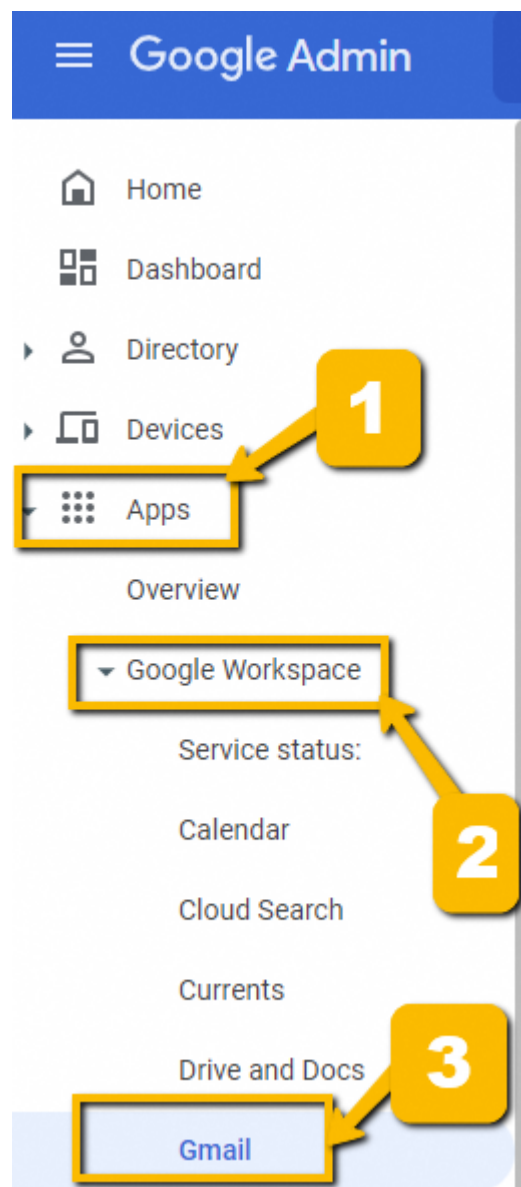
- **Votiro File Blocked From Connector:** If the syslog message includes “blocked” under -Sanitization result- field and “false” under -password protected- field and “null” under -from- field create an alert with the following message: [file name] with hash [file hash] that was sent from connector [connector 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 Integrate Votiro with Google Workspace

In this tutorial, you'll learn how to integrate Votiro with Google Workspace (formerly G Suite).

3.1 Procedure

1. Sign in to the [Google Admin console](#) with your Google Workspace account.
2. In the left pane, navigate to Apps > **Google Workspace** > **Gmail**



3. On the **Settings for Gmail** page, scroll down and select **Spam, phishing, and malware**

4. Move the cursor over **Inbound gateway** and click the pencil button to edit the settings:

Inbound gateway If you use email gateways to route incoming email, please enter them here to improve spam handling [Learn more](#)

☒ Enable

1. Gateway IPs

IP addresses / ranges
<div></div>

[ADD](#)

☒ Automatically detect external IP (recommended)

☐ Reject all mail not from gateway IPs

☒ Require TLS for connections from the email gateways listed above

2. Message Tagging

☐ Message is considered spam if the following header regexp matches

[i](#) Most changes take effect in a few minutes. [Learn more](#)
You can view prior changes in the [Audit log](#)

CANCEL SAVE

5. Enter the IP address provided by Votiro.
6. Verify that the following boxes are checked:
 - ◆ **Automatically detect external IP (recommended)**
 - ◆ **Require TLS for connections from the email gateways listed above**
7. Click **SAVE**.

3.1.1 Create a Host

8. Navigate back to **Settings for Gmail** and select **Hosts**.

Hosts ▼

Add mail hosts for use in advanced routing, for example to direct messages to Microsoft Exchange.

9. Click **Add route**.
 - a. Type a name, for example: "Forward to Votiro Cloud".
 - b. For the option **Specify email server**, select **Single host** and type the host name provided to you by Votiro support.
 - c. Check **Require mail to be transmitted via secure (TLS) connection (Recommended)**.
 - d. Check **Require CA signed Certificate (Recommended)**.
 - e. Check **Validate certificate hostname (Recommended)**.
 - f. Click on **Test TLS connection**:

Test TLS connection

TLS connection validated on January 16, 2025 4:45 PM

- g. Click on **SAVE**.

Edit mail route

Name

[Learn more](#)

Workspace to Votiro Cloud

This field is required.

1. Specify email server

Only ports numbered 25, 587, and 1024 through 65535 are allowed.

Single host ▼

: 25

2. Options

- ☐ Perform MX lookup on host
- ☒ Require mail to be transmitted via a secure (TLS) connection (Recommended)
 - ☒ Require CA signed certificate (Recommended)
 - ☒ Validate certificate hostname (Recommended)

[Test TLS connection](#)

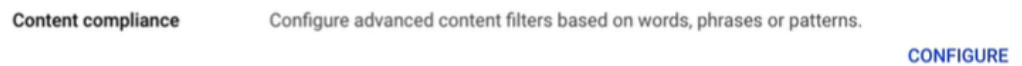
CANCEL **SAVE**

3.1.2 Configure content compliance rule for emails received from Votiro

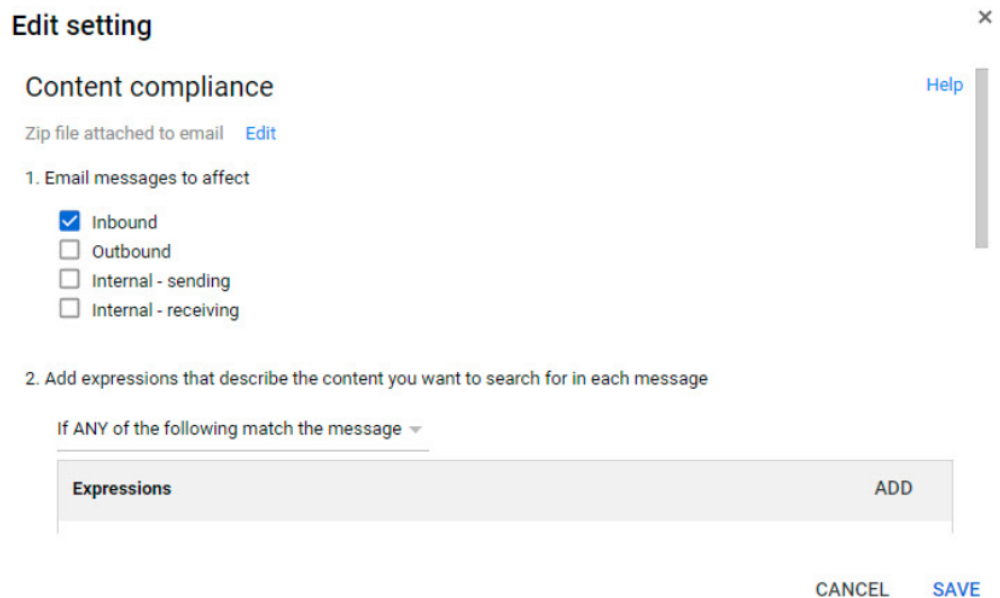
10. Return to **Settings for Gmail** and select **Compliance**:



11. Under **Content compliance**, select **CONFIGURE**.



- a. Specify a name for the new rule, for example "To Votiro Cloud to Workspace"
- b. For **Email messages to affect**, check **Inbound**.
- c. For **Add expressions that describe the content you want to search for in each message**, select **If ANY of the following match the message** and click **ADD**.



- d. Select **Metadata match, Attribute, Source IP** and **Match type**.
- e. Select **Source IP is within the following range** and enter the IP addresses provided by Votiro support.
- f. Click **SAVE**.

Edit setting

Metadata match ▼

Attribute

Source IP ▼

Match type

Source IP is within the following range ▼

CANCEL

SAVE

- g. Add another expression, select **Advanced content match**, **Location**, **Full headers**, **Match type**, **Contains text**.
- h. In **Content**, enter "X-MTConnectorResult".
- i. Click **SAVE**.

Edit setting

Advanced content match ▼

Location

Full headers ▼

Match type

Contains text ▼

Content

X-MTConnectorResult

CANCEL SAVE

- j. For 3 - If the above expressions match, do the following: Under **Route** select **Change route** and make sure **Normal routing** is selected.
- k. Under Encryption, check **Require secure transport (TLS)**.
- l. Click **Show options**.
 - i. Under **Account types to affect**, check the following boxes:
 - **Users**
 - **Groups**
 - **Unrecognized / Catch-all**
 - ii. Click **SAVE**.

[Hide options](#)

A. Address lists

- ☐ Use address lists to bypass or control application of this setting
- ☐ Bypass this setting for specific addresses / domains
- ☐ Only apply this setting for specific addresses / domains

B. Account types to affect

- ☒ Users
- ☒ Groups
- ☒ Unrecognized / Catch-all

C. Envelope filter

- ☐ Only affect specific envelope senders
- ☐ Only affect specific envelope recipients

[CANCEL](#) [SAVE](#)

3.1.3 Configure Content compliance rule for emails sent to Votiro

12. By now, you should have one rule enabled for Content compliance. Click on **ADD ANOTHER RULE** for traffic sent from Google Workspace to Votiro.
 - a. Specify a name, for example "Workspace to Votiro Cloud".
 - b. Under **Email messages to affect**, check **Inbound**.
 - c. For **Add expressions that describe the content you want to search for in each message**, select **If ALL of the following match the message** and click **ADD**,
 - i. Select **Metadata match, Attribute, Source IP** and **Match type**.
 - ii. Select **Source IP is not within the following range** and enter the IP addresses provided by Votiro support.
 - iii. Click **SAVE**.

2. Add expressions that describe the content you want to search for in each message

If ALL of the following match the message ▼

Expressions

Metadata match: Source IP is not within the range [redacted]

Edit

ADD

- d. For 3 - If the above expressions match, do the following: Under **Route**, select **Change route** and make sure "Forward to Votiro Cloud" is selected.
- e. Under **Encryption**, check **Require secure transport (TLS)**.
- f. Click **Show options**.
 - i. Under **Account types to affect**, check the following boxes:
 - **Users**
 - **Groups**
 - **Unrecognized / Catch-all**
 - ii. Click **SAVE**

Note: It can take a while for the changes to be applied.

13. After the rules are successfully configured:
 - a. Send a test email.
 - b. Under Reporting > Email Log Search, see if the message was routed through Votiro's Cloud instance.
 - c. Verify you're able to see the sanitized email in Votiro's dashboard.

3.1.4 Votiro Cloud for Sanitization

If incoming traffic is not from the IPs listed above, send it for sanitization.

14. Create a new rule "Sanitized Emails To Google Workspace".
15. Under **Email messages to affect**, check **Inbound**.
16. For **Add expressions that describe the content you want to search for in each message**, select **If ANY of the following match the message** and click **ADD**.
17. For **Advanced content match**, select:

- a. **Location:** Full headers
 - b. **Match Type:** Contains text:
 - c. **Content:** X-MTConnectorResult
18. For **Metadata match**, select:
- a. **Attribute**
 - b. **Source IP**
 - c. **Match type**
 - d. For **Source IP is within the following range**, enter the IP addresses provided by Votiro support.
19. Under **Route**, select **Change route** and set to **Normal Routing**.
20. Under Encryption (onward delivery only), check **Require secure transport (TLS)**.
21. Click **Show options**.
- a. Under **Account types to affect**, check the following boxes:
 - **Users**
 - **Groups**
 - **Unrecognized / Catch-all**
22. Click **SAVE**.

The result of these actions is that for any email with the **X-MTConnectorResult** header and originating from the listed IPs, it is routed to the user's mailboxes as usual, since it has been sanitized.

3.1.5 Spam Rule

23. Select **Spam, phishing, and malware**.
24. Add a rule "Trusted Votiro Relay Servers".
25. Select **Options to bypass filters and warning banners**:
 - a. **Bypass spam filters for internal senders**
 - b. **Bypass spam filters for messages from senders or domains in selected lists**
26. Create a new list and name it "Votiro Relay Allow Addresses".
27. Enter the IP addresses provided by Votiro support.

3.1.6 Prevent Email Authentication Protocol Failures

To prevent email authentication protocol failures (DKIM, DMARC, and SPF), it is necessary to manually add Google's MX server prefix so that authentication checks are performed on the correct IP address of the originating sender.

This will prevent legitimate emails from being sent to your spam folder or flagged as suspicious.

To do so, follow the steps below:

1. In the Google Workspace Admin console, navigate to Menu > **Apps > Google Workspace > Gmail > Spam, Phishing, and Malware**.
2. Select your top-level organization on the left, scroll to the **Inbound gateway** setting, then click Edit.
3. Click **Add** and enter the IP range of the region. For example: 209.85.128.0/17

Note: Verify the IP range, as it may differ depending on the customer's location. Hint: Check the IP in the email header and look for similar [here](#).

4. At the bottom, ensure that the **Automatically detect external IP (recommended)** box is checked.
5. Save your changes and retest the configuration.

3.1.7 How To Resolve Google's SPAM Email Alert On SaaS

When utilizing Votiro's relay servers for SMTP traffic, our customers may encounter emails flagged as suspicious and in the "spam" folder. This occurs because the SPF (Sender Policy Framework) check fails, as Votiro's servers are not the original source IP that generated the email.

In this case, Gmail examines the "Received: from" message headers to identify the first public IP address not in the Gateway IP list and treats this IP address as the source IP for the message. This IP address is used for SPF authentication and spam assessment.

We must ensure that Google can continue to scan for the source IP received from the header in the flow to authenticate the source IP and not the first public IP address in the mail flow, as this is not the sender's source IP.

To address this issue, Google requires you to configure Votiro's servers as an inbound mail gateway. The instructions to do this are outlined in the article [Set up an inbound mail gateway](#). A summary of these instructions as applied to Votiro are as follows:

1. In the Google Admin console, navigate to Menu > **Apps > Google Workspace > Gmail > Spam, Phishing and Malware**.
2. Select your top-level organization on the left, scroll to the **Inbound gateway** setting, then click **Edit**. The Inbound gateway settings open on the page.
3. Click **Add** and enter the IP range: 209.85.128.0/17 in the **Add IP address/range** box. Verify this range, as it may differ depending on the customer's location (Hint: Check the IP in the email header).
4. At the bottom, ensure that the **Automatically detect external IP—(Optional)** box is checked.
5. At the bottom, click **Save**. Note that the changes may take time before going into effect.

6. Test the configuration again.

To summarize, by ensuring that the IP range is on the "Inbound" list, we allow Google to scan the first public IP address that is NOT on the list.

Here is an example of how it should look when an SPF check passes from "DocuSign".

Hops	Submitting host	Receiving host	Time	Delay	Type	→
1	docuSign.net ([127.0.0.1])	SE102F81.corp.docuSign.net	9/17/2024 12:26:23 PM		Microsoft SMTPSVC(10.0.17763.1697)	
2	SE102F81.corp.docuSign.net (se-c101-f51-81.corp.docuSign.net [10.101.81.9])	mailsea.docuSign.net (Postfix)	9/17/2024 12:26:23 PM	0 seconds	ESMTP	
3	mailsea.docuSign.net (mailsea.docuSign.net [64.207.219.9])	mx.google.com	9/17/2024 12:26:24 PM	1 second	ESMTPS	
4		mail-qt1-f198.google.com	9/17/2024 12:26:26 PM	2 seconds	SMTP	
5	mail-qt1-f198.google.com (209.85.160.198)	votiro-relay2.prod.votiro.com (10.241.50.238)	9/17/2024 12:26:26 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	
6	votiro-relay2 (10.241.50.238)	SDSConnector2	9/17/2024 12:26:26 PM	0 seconds	SDSConnector2 Ver: 1.8.0.0	
7	votiro-relay2.prod.votiro.com (ec2-44-206-222-91.compute-1.amazonaws.com [44.206.222.91])	mx.google.com	9/17/2024 12:26:50 PM	24 seconds	ESMTPS	
8		2002:a50:d78e:0b0:5c3:d892:1034	9/17/2024 12:26:50 PM	0 seconds	SMTP	

4 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.

4.1 Prerequisites

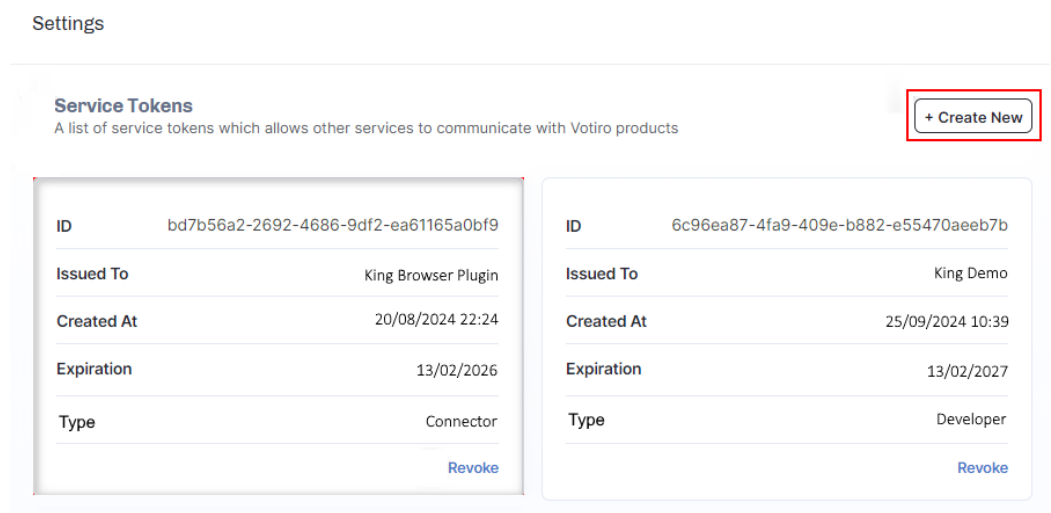
Install Postman by downloading one of the following:

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

4.2 Procedure

4.2.1 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

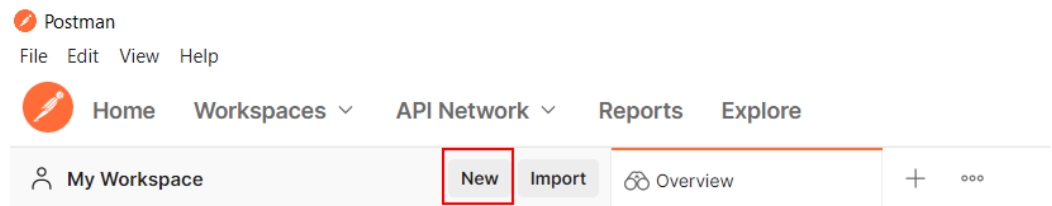
eyJhbGciOiJSUzI1NiIsImtpZCI6IjIOTMxRUM5QzA4NTIiGOEVGNkM0NUY0MDExQTU0MTAzNzhGMTY5REEiLCJ0eXAiOiJKV1QiIfQ.eyJ1bmVudGVybmFsU2VydmVjZXMiLCJyb2xlIjoiaWwtaW5pc3RyYXRvcilslmp0aSI6ImZmNWUwOWFmLTA4NjctNDUxNC1iZmVkLTQxODZlODZlZjJmZSIsIm5iZil6MTY0NzgZNDQxMCwiZXhwIjoxNjc4ODA5NjAwLCJpYXQiOiE2NDc4MzQ0MTB9.EYm24-YcS6RnXSCh7LiYDFAMA5d_U7Z6nBW670FOgiA6AH3tG14amRWc6wjo2LpKxNAVLbrnMUbrVUTCRTToAWABPvT47gJsIBdafP9R0sPOh0voAdbh_hjt-J9jspYuF8hu7NfukUxUVhDd3oKRnGDmWizBANbqCbXXw2fELGgWpn0VuR88y_o7vxobp5mqLqRWvQ1p3mGTEAem6si1UBHhYgvOvKMYY9TH9cxnuRbnPA-xVwGCQ8OFQuA6ITJw9ehwl34vUA22qri65-xNvWoakgXVA-tiHSpWxdgWrmeLK88wKum7dUyFfDu4rrEadvvmLFZK3eEZ1KpZOv1Dcdg

OK

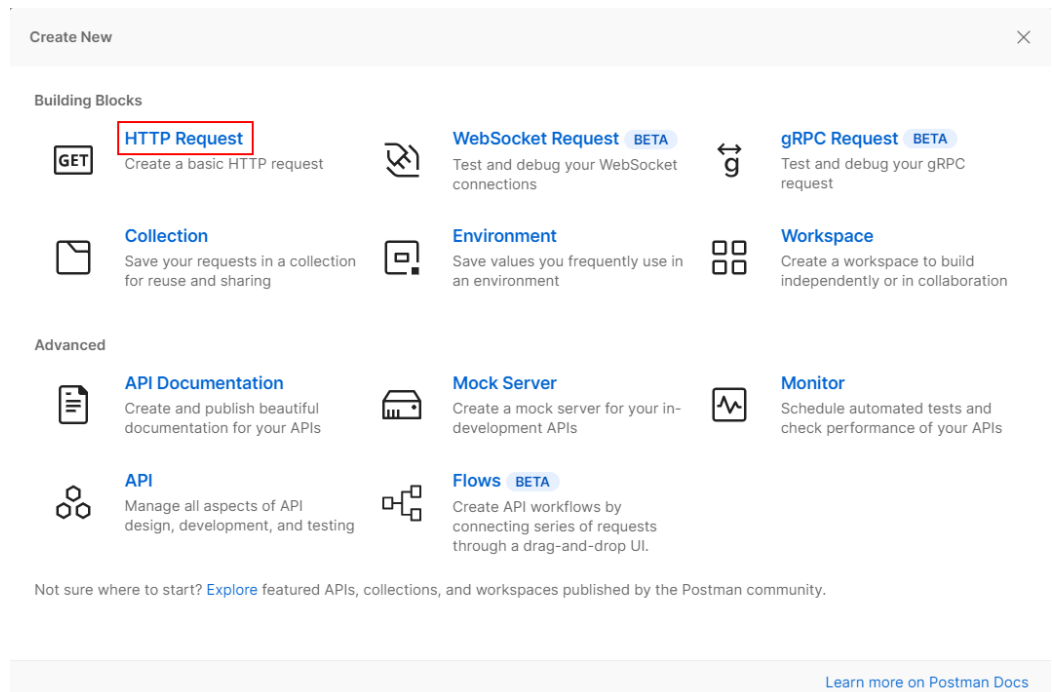
- Press **OK** to close the Token window.

4.2.2 Postman Setup

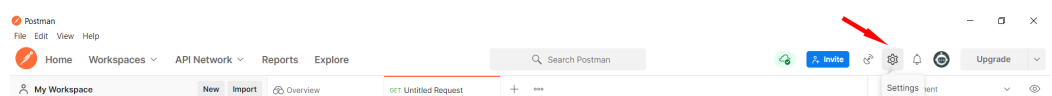
1. In the Postman app, go to **Workspaces > My Workspace** and press **New**:



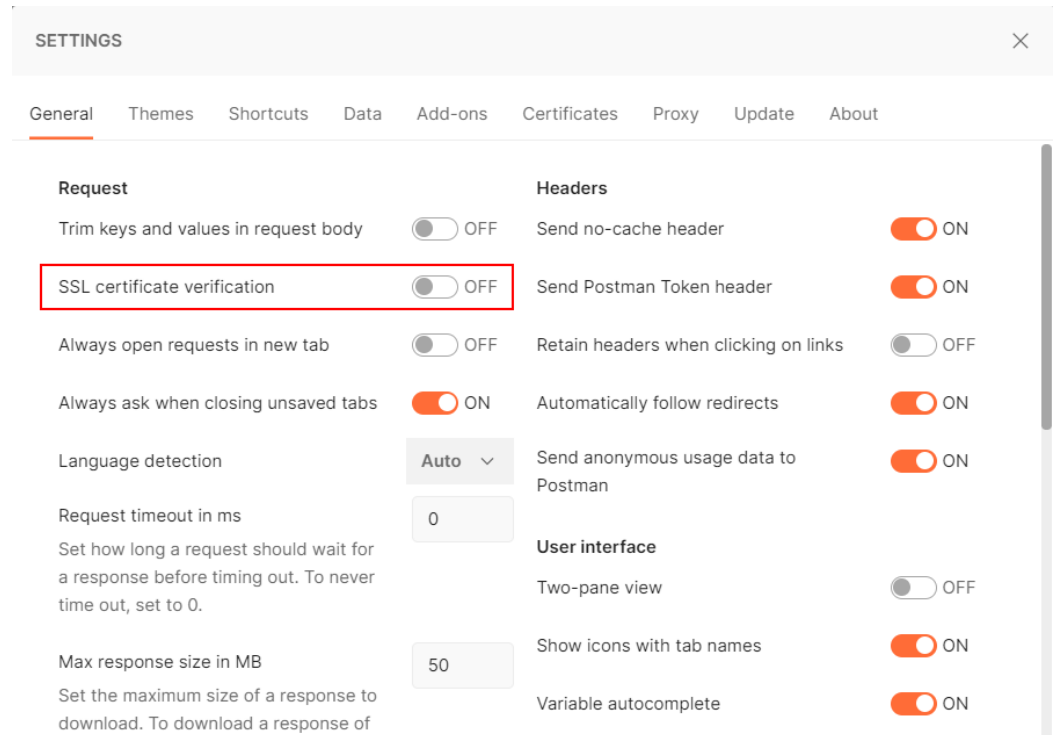
2. The **Create New** window opens. Select **HTTP Request**:



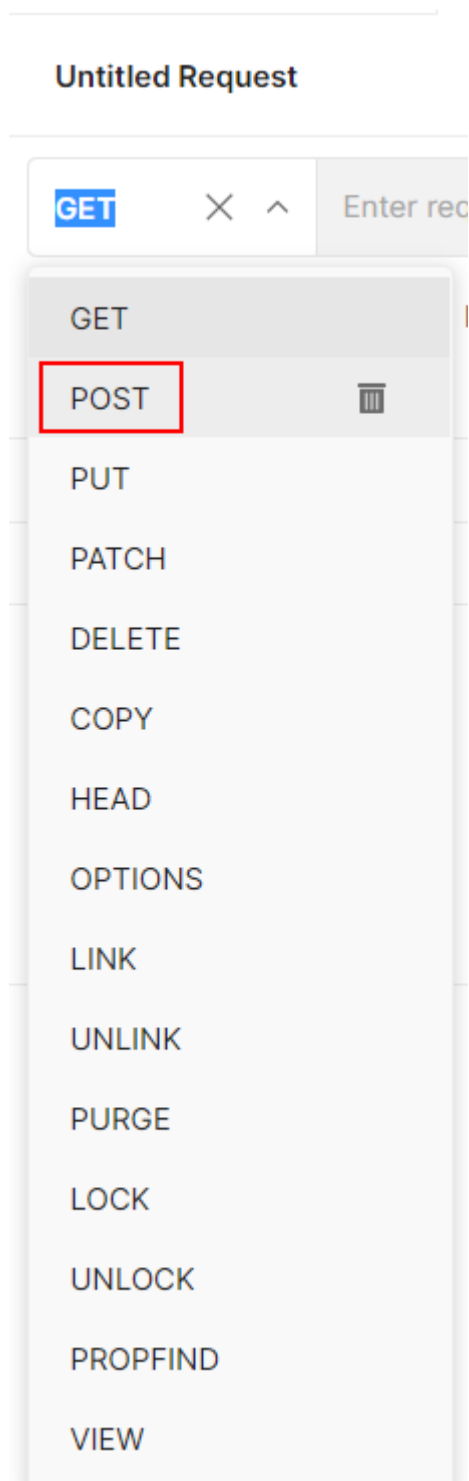
3. Press the **Settings** icon:



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**:

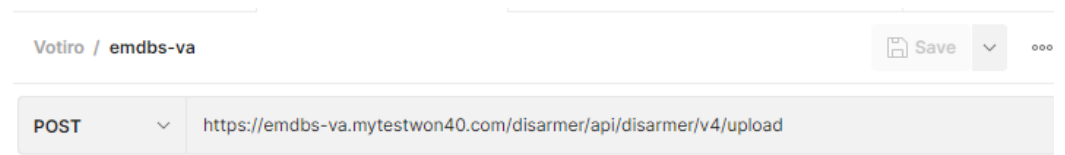


5. Close the **Settings** window.
6. Under the **Untitled Request** dropdown box, select **POST**:

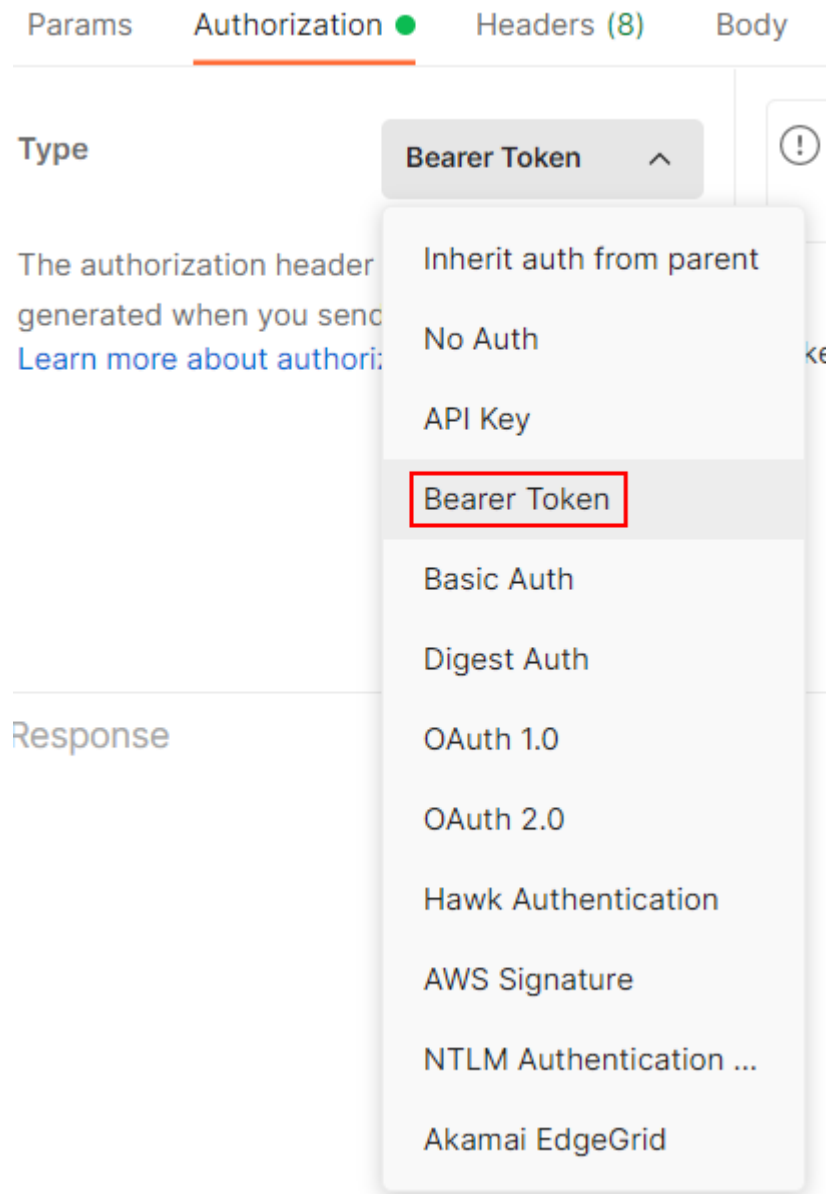


7. In the **Enter request URL** box, enter your VA FQDN in the following format:
`https://<VA-FQDN>/disarmer/api/disarmer/v4/upload`

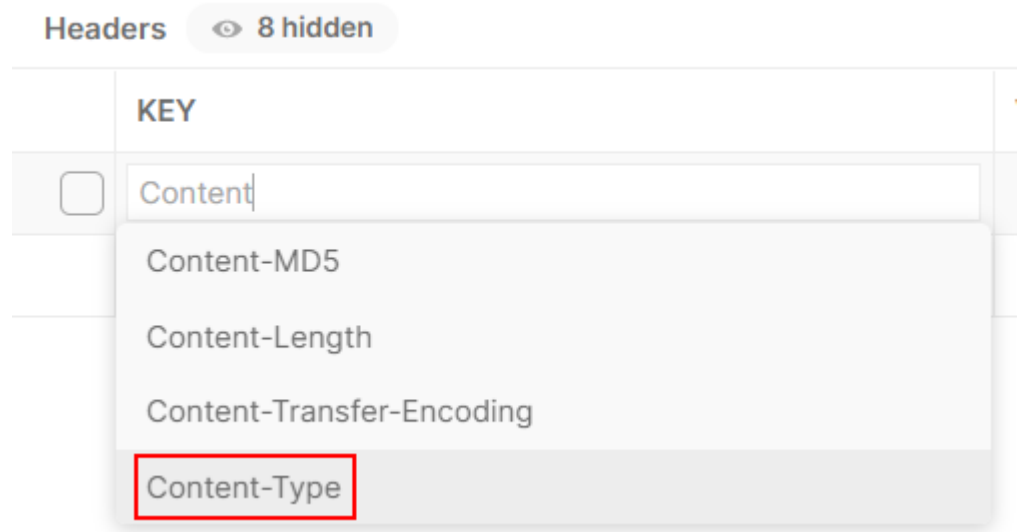
For example:



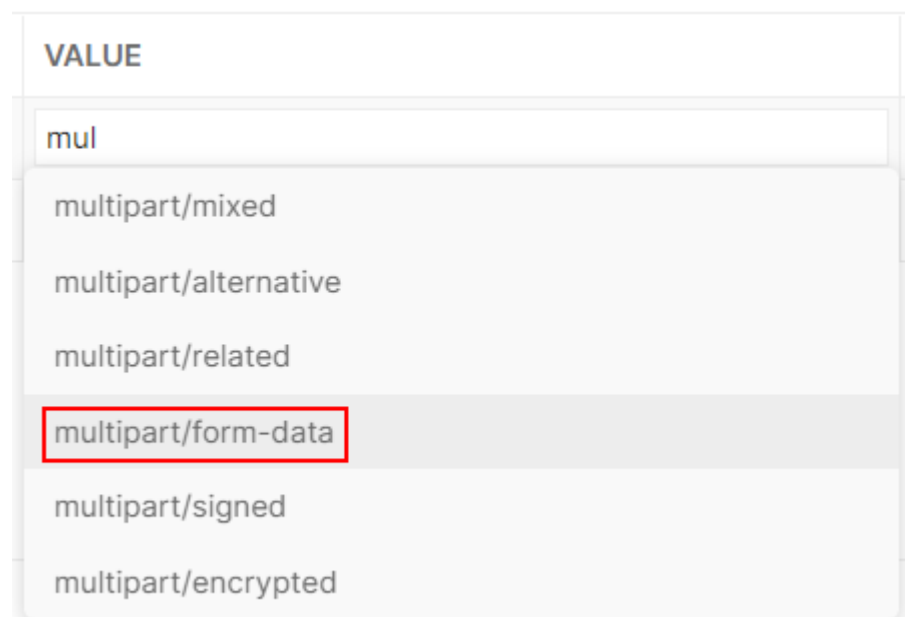
8. Select the **Authorization** tab and under the **Type** dropdown, select **Bearer Token**:



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

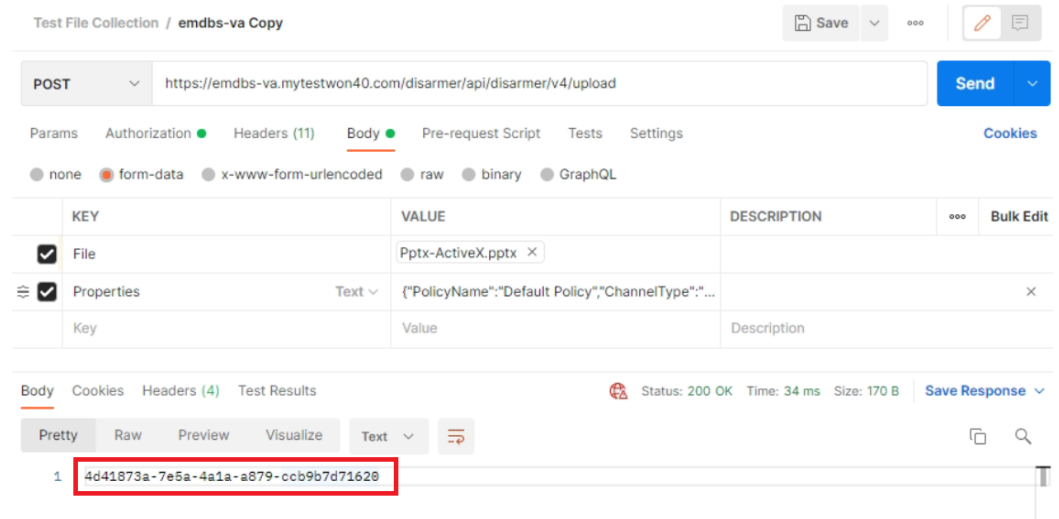
	KEY	VALUE
<input checked="" type="checkbox"/>	File	Pptx-ActiveX.pptx ×
<input checked="" type="checkbox"/>	Properties	{"PolicyName": "Default Policy", "ChannelT...
	Key	Value

18. Press the **Send** button:

POST
https://emdb-s-v-a.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

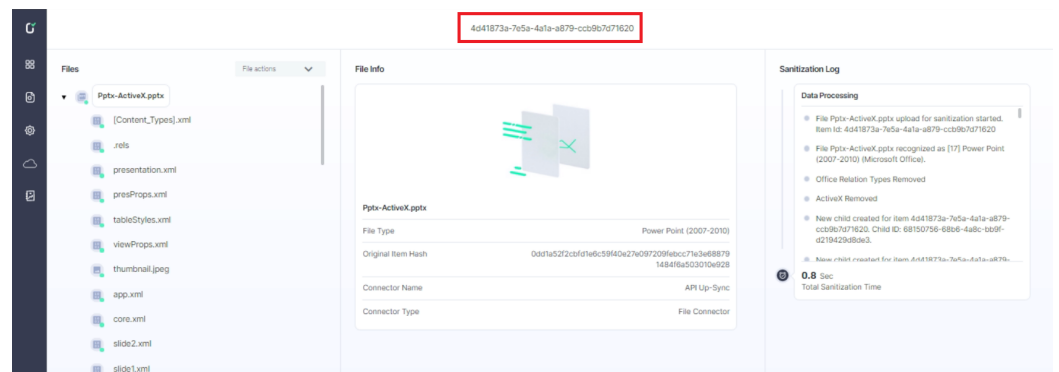
KEY	VALUE	DESCRIPTION	...	Bulk Edit
File	Pptx-ActiveX.pptx			
Properties	Text {"PolicyName": "Default Policy", "ChannelType": "...			
Key	Value	Description		

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 0dd1a52f2c0f0e6c5940e27a097209f6cc71e3e688791484f18a503010e928

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-bb9f-0219429d89d3
- New child created for item 4d41873a-7e5a-4a1a-a879-ccb9b7d71620. Child ID: 68150756-6806-4a8c-bb9f-0219429d89d3

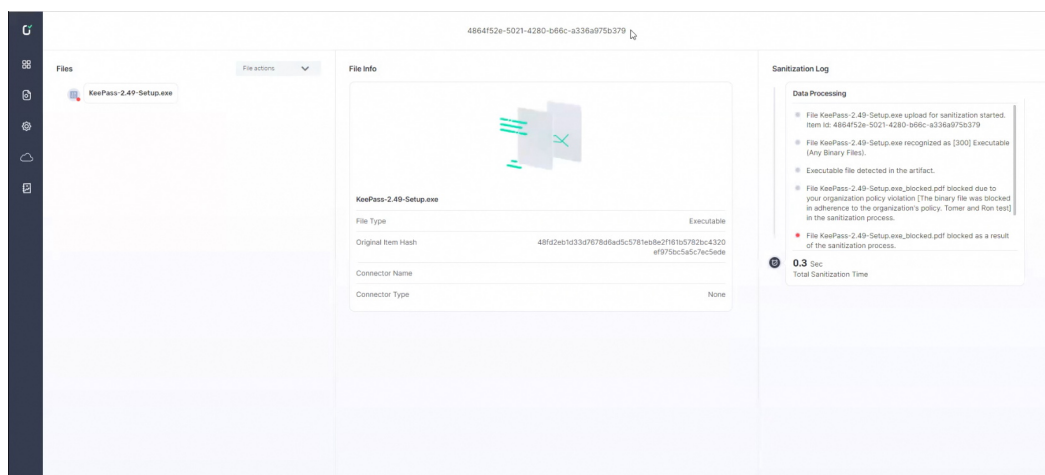
0.8 Sec Total Sanitization Time

5 How to Use Kibana to Troubleshoot Votiro Incidents

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

5.1 Example of Votiro Incident

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



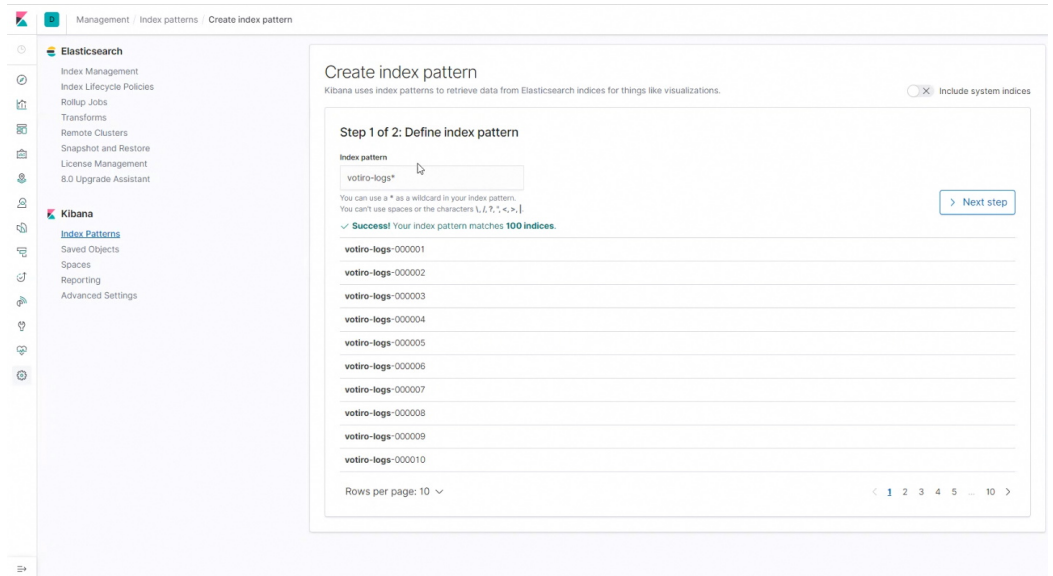
This screen shows the results of Votiro On-prem processing a file named KeePass-2.49-Setup.exe. The **File Info** pane displays some of the file properties and the **Sanitization Log** pane displays highlights of the file **Data Processing**.

5.2 Procedure

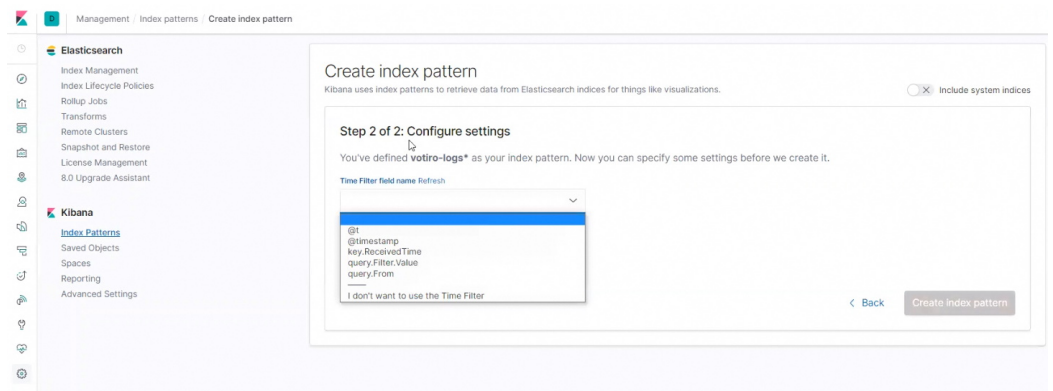
5.2.1 Create and Configure an Index Pattern

To begin, you must define a Kibana index pattern.

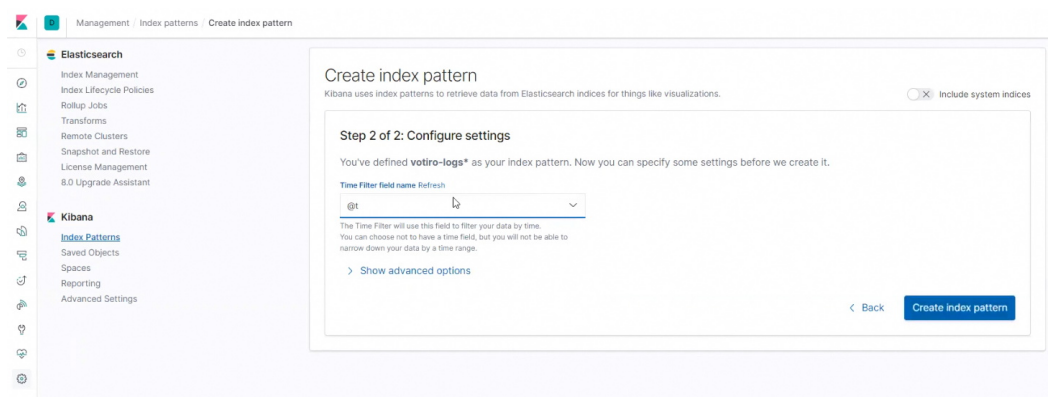
1. Login to the Kibana Discover interface with the credentials provided to you by Votiro Support.
2. Select **Create index pattern**. **Step 1 of 2 Define index pattern** appears.
3. Type **votiro-logs*** (or similar) as the Index pattern. Kibana displays a list matching the index pattern:



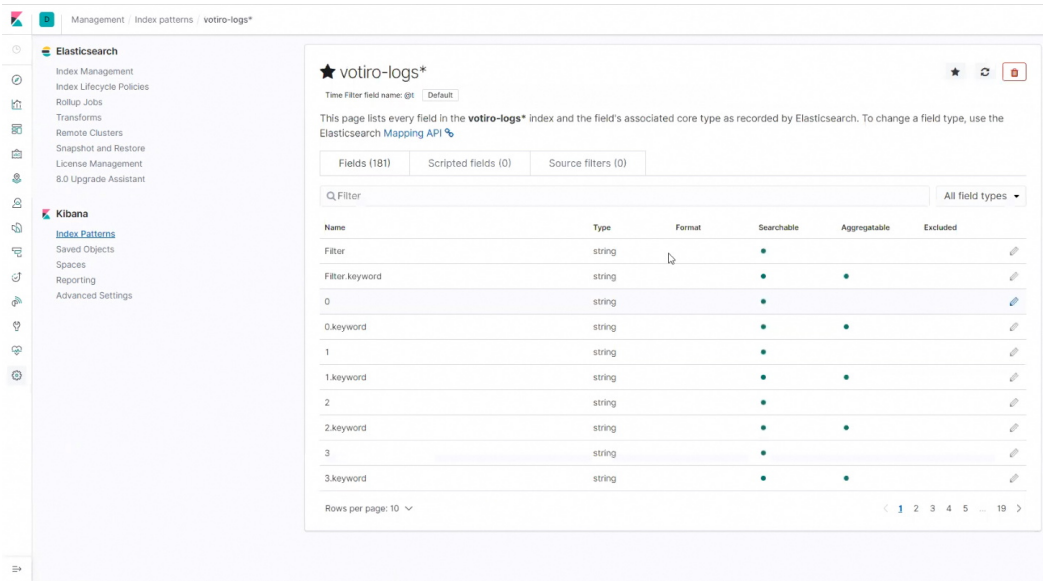
4. Click on **Next step**. **Step 2 of 2 Configure settings** appears.



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*):

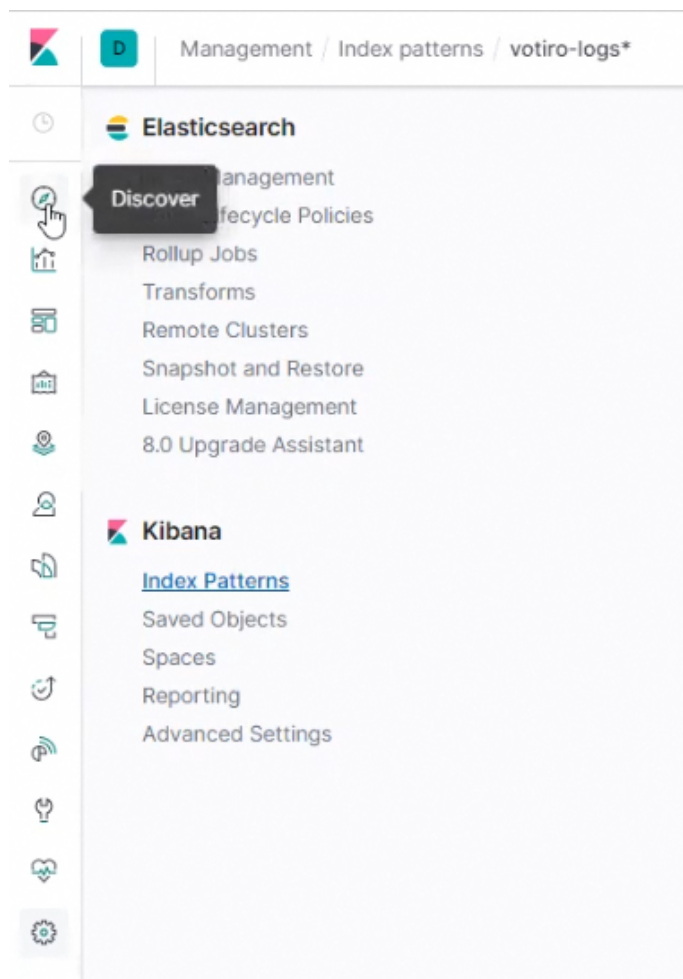


5.3 Analyze the Data

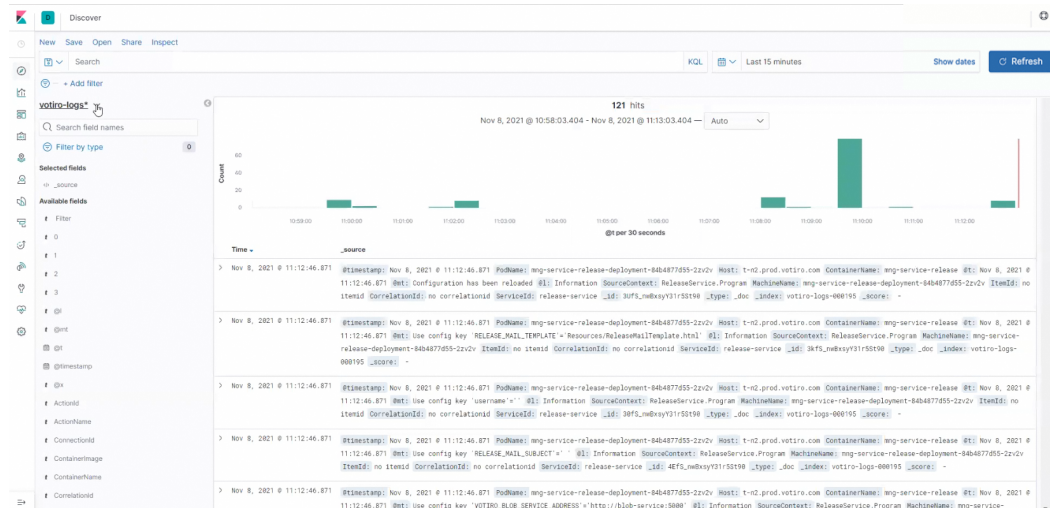
After the index pattern is created and configured, apply it to the data in Kibana's Discover mode to yield useful results by additional filtering of the data.

5.3.1 Discover

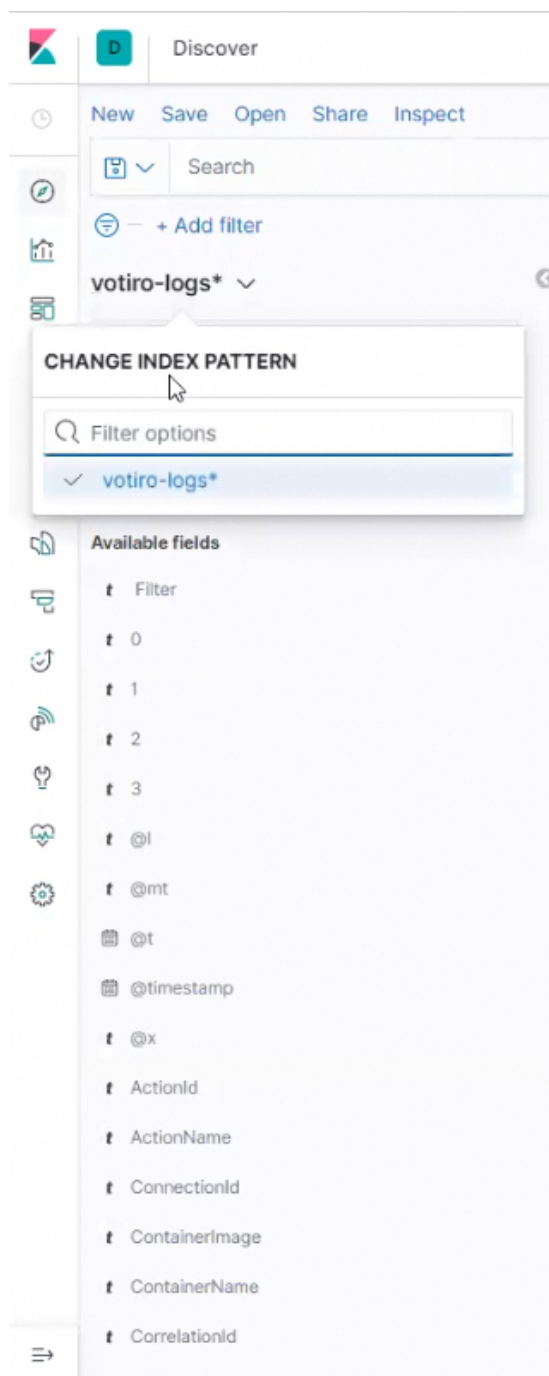
1. Click on the Discover icon on the left side of the screen:



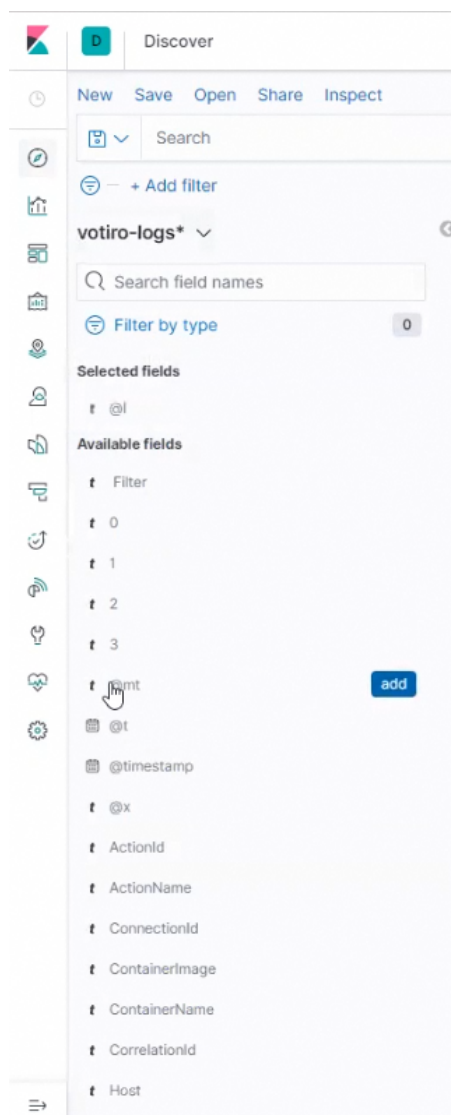
2. Kibana displays all hits that match the time filter criteria within the time range indicated (in this example, for the last 15 minutes):



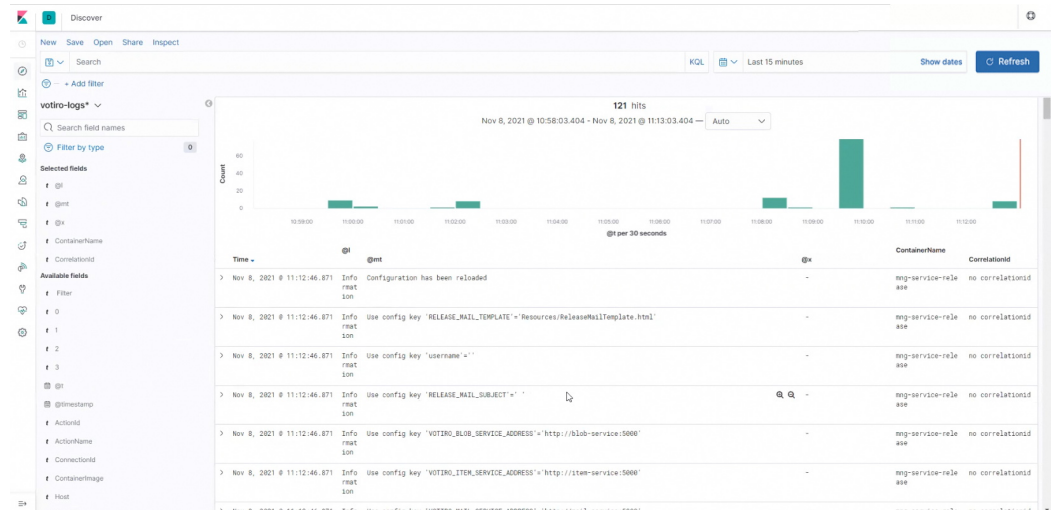
- To further filter the results, click on **▼** next to the index pattern (votiro-logs* by default) in the left side of the screen. The **CHANGE INDEX PATTERN** window opens:



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:



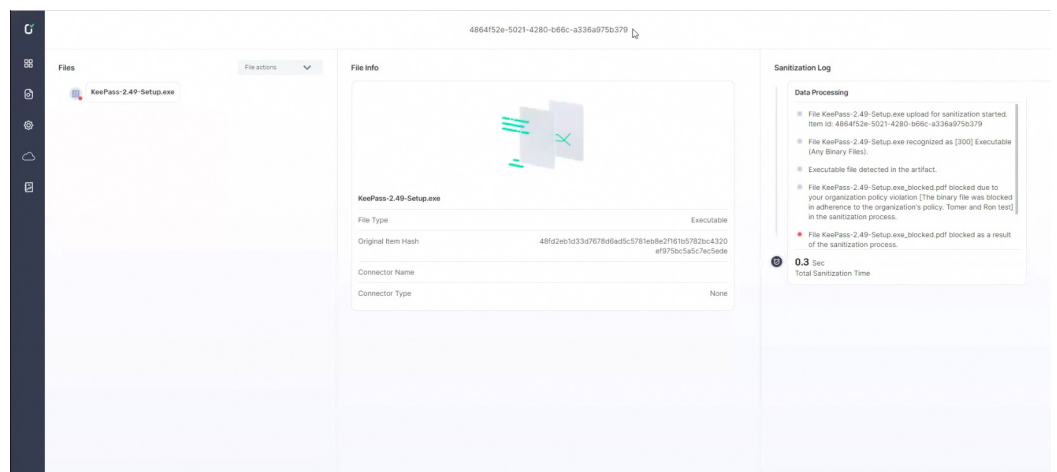
5. In the example below, the following fields are added:
 - ◆ **@l** - level
 - ◆ **@mt** - message template
 - ◆ **@x** - exception
 - ◆ **ContainerName**
 - ◆ **CorrelationId**
6. The display of hits is now updated to show only the selected fields:



5.3.2 Votiro Explore Incident & File Info

To examine a specific file that was processed by Votiro On-prem, the threat ID is obtained from the Votiro Item/Incident sanitization information.

1. Open the Votiro Explore Incident:



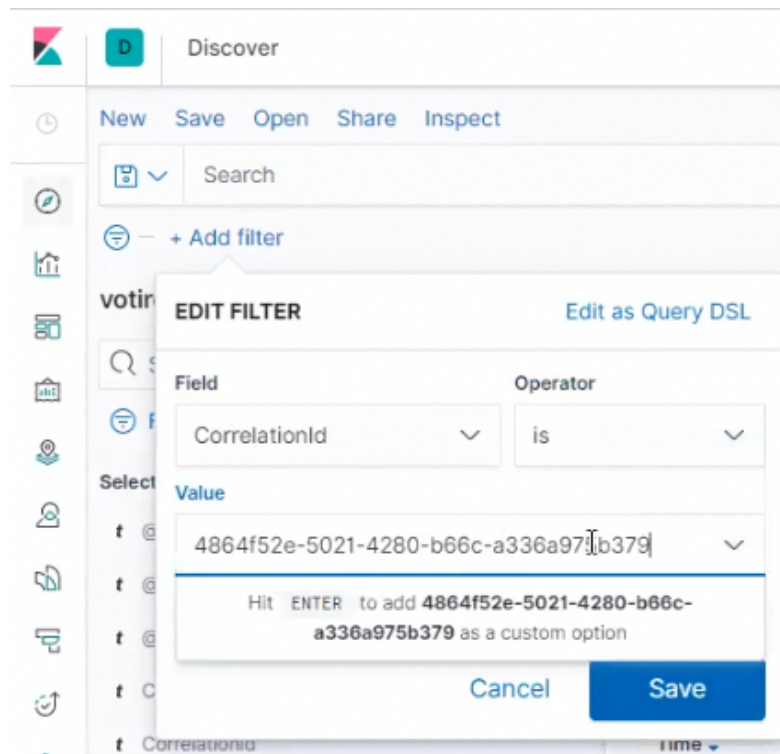
2. Copy to the clipboard the file ID at the top of the screen, in this example:

4864f52e-5021-4280-b66c-a336a975b379

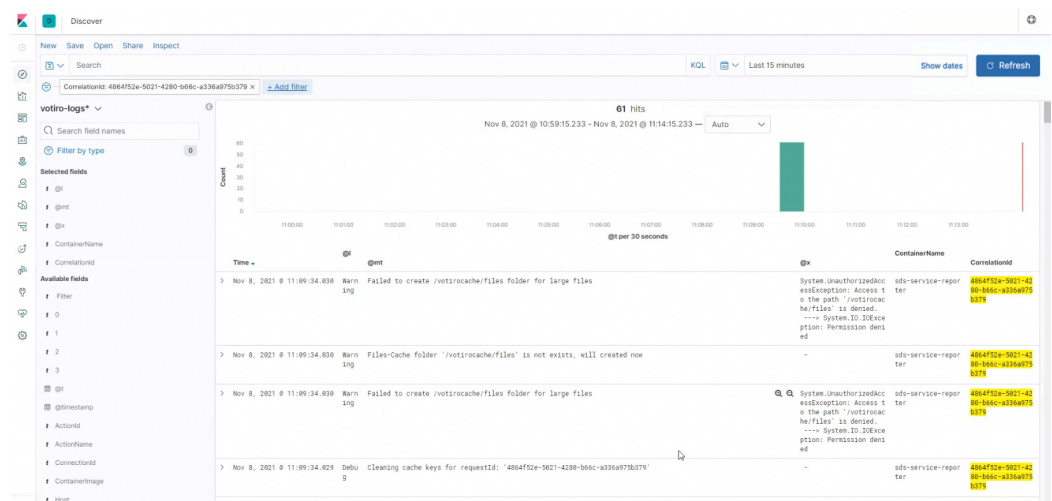
5.3.3 File Sanitization Analysis


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 Kibana date range selector. At the top, it displays the current range as '~ 15 minutes ago → 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 'Apply' button. Underneath the 'Quick select' section is a 'Commonly used' section with a grid of links: '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 that is a 'Recently used date ranges' section with links for 'Today', 'This week', and 'Last 30 minutes'. At the bottom 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.

6 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

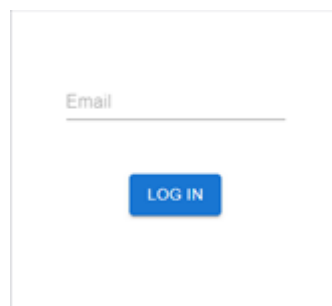
6.1 MSSP Tenant Management

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:

ADD TENANT						
Name	ID	Domains	License Type	License Quota	License Expiration	License Features
test-tomer	2a167928-07d1818	tomer.com	Consumption	0Bytes / 4TB	05-06-2024 (352 days remaining)	<ul style="list-style-type: none"> menlo awsS3 chrome
votiroapj-mssp	3aa29408-5490da997	votiroapj-mssp.com	Consumption	224.8KB / 10TB	15-06-2024 (361 days remaining)	<ul style="list-style-type: none"> menlo awsS3 chrome
demo-mssp	7aa33a3b-0423410c	demo-mssp.com	Consumption	25.8MB / 46TB	05-06-2024 (352 days remaining)	<ul style="list-style-type: none"> menlo awsS3 chrome
king	93d29d21-72786984	king.com				
demotenant1	96d257c0-0219c2b25	demotenant1.com	Consumption	3.1MB / 10TB	05-06-2024 (352 days remaining)	<ul style="list-style-type: none"> menlo awsS3 chrome
votiro-dev	be9d9d4b-181c97	votiro-dev.com	Requests	0 / 10,000,000,000	15-06-2024 (362 days remaining)	

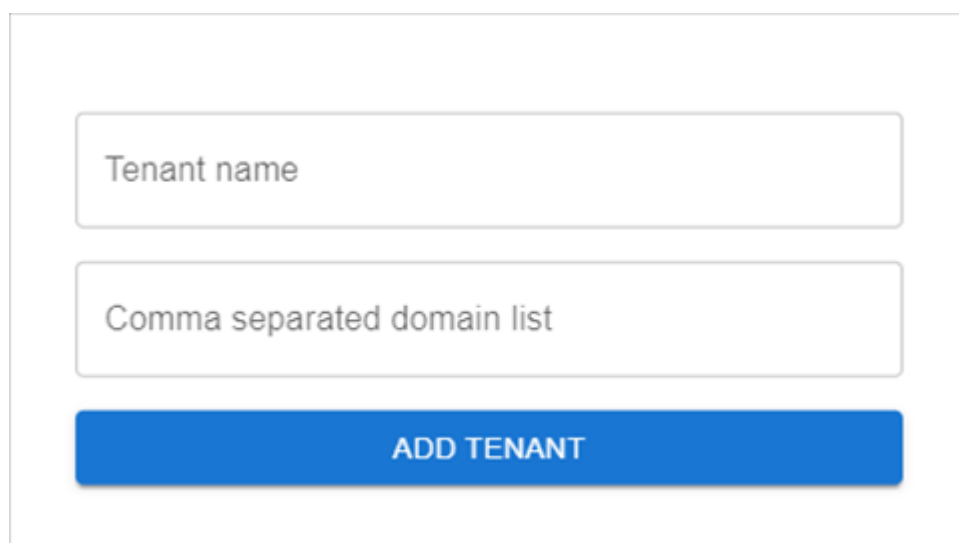
The MSSP admin can use the Tenant Management screen to:

- ◆ 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								

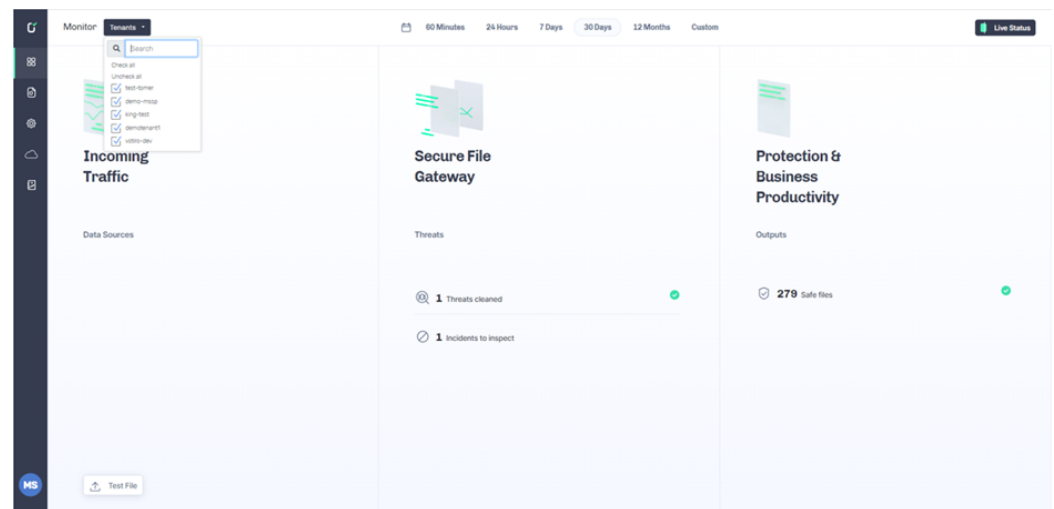
6. Delete a customer tenant

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

6.2 Monitoring Tenant Activity

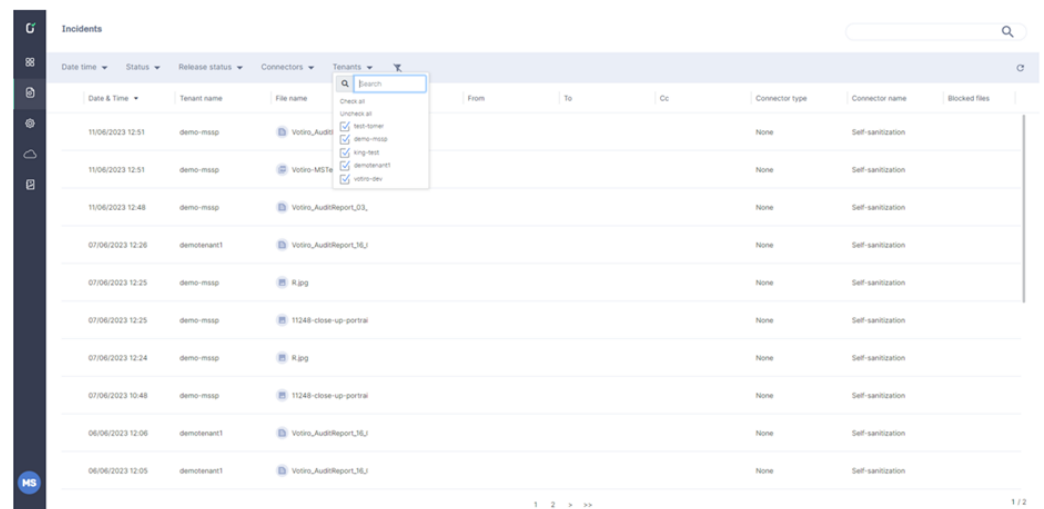
1. MSSP Dashboard

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



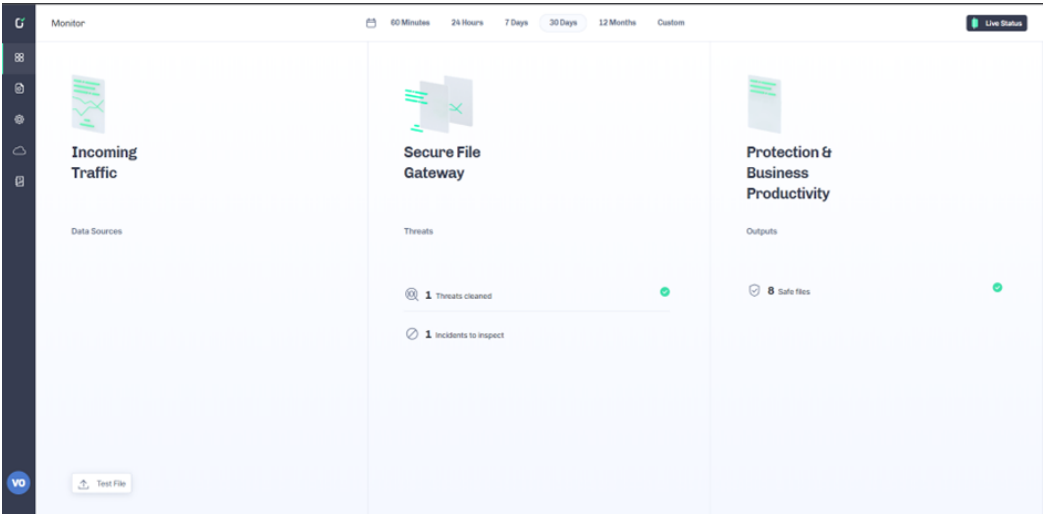
2. MSSP Incidents

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



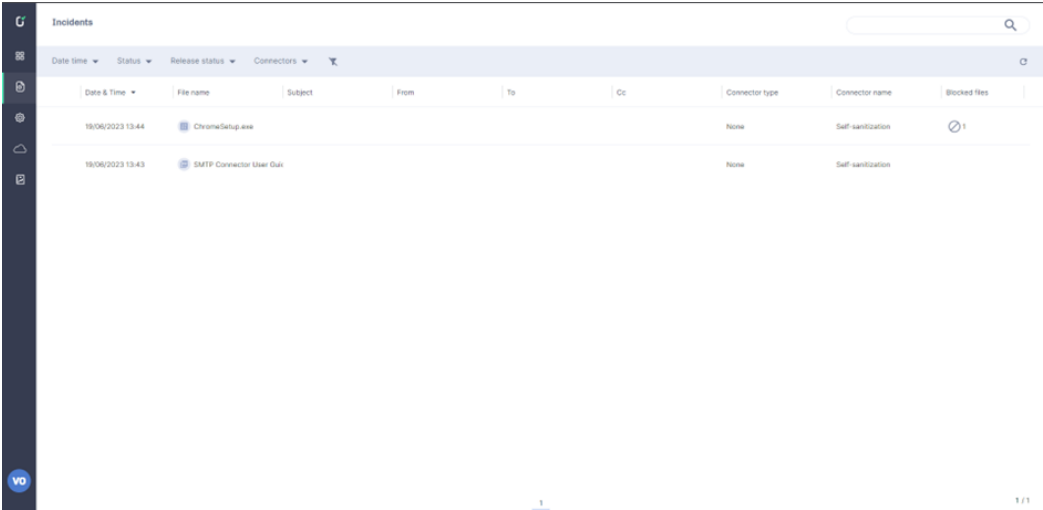
3. MSSP Customer's Dashboard

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.



7 How to Use QR Code Sanitization

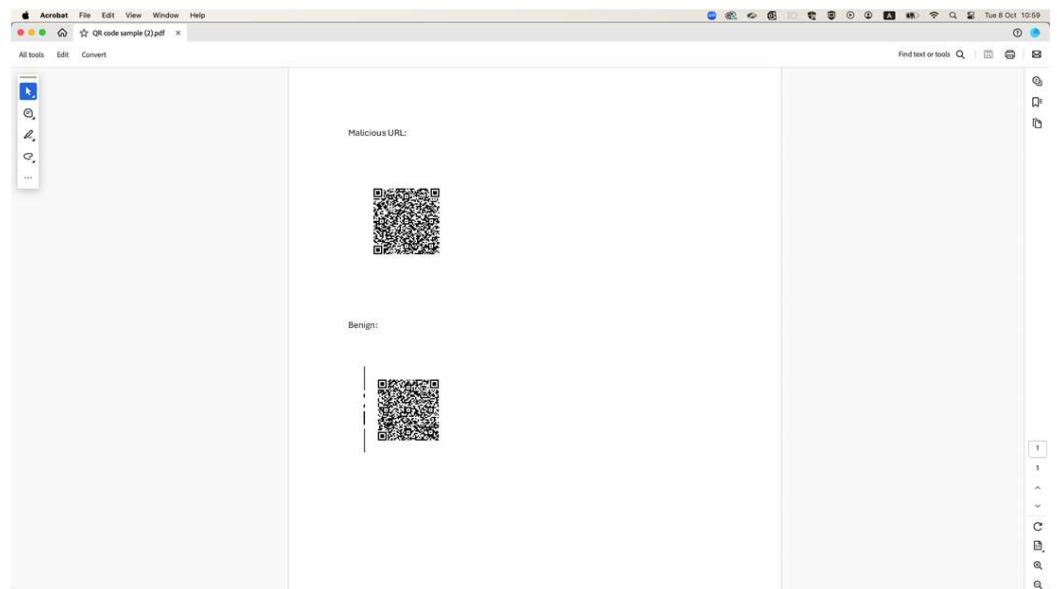
Votiro supports QR Code sanitization. This is relevant for PDFs and emails containing QR codes.

There are four options when dealing with QR codes:

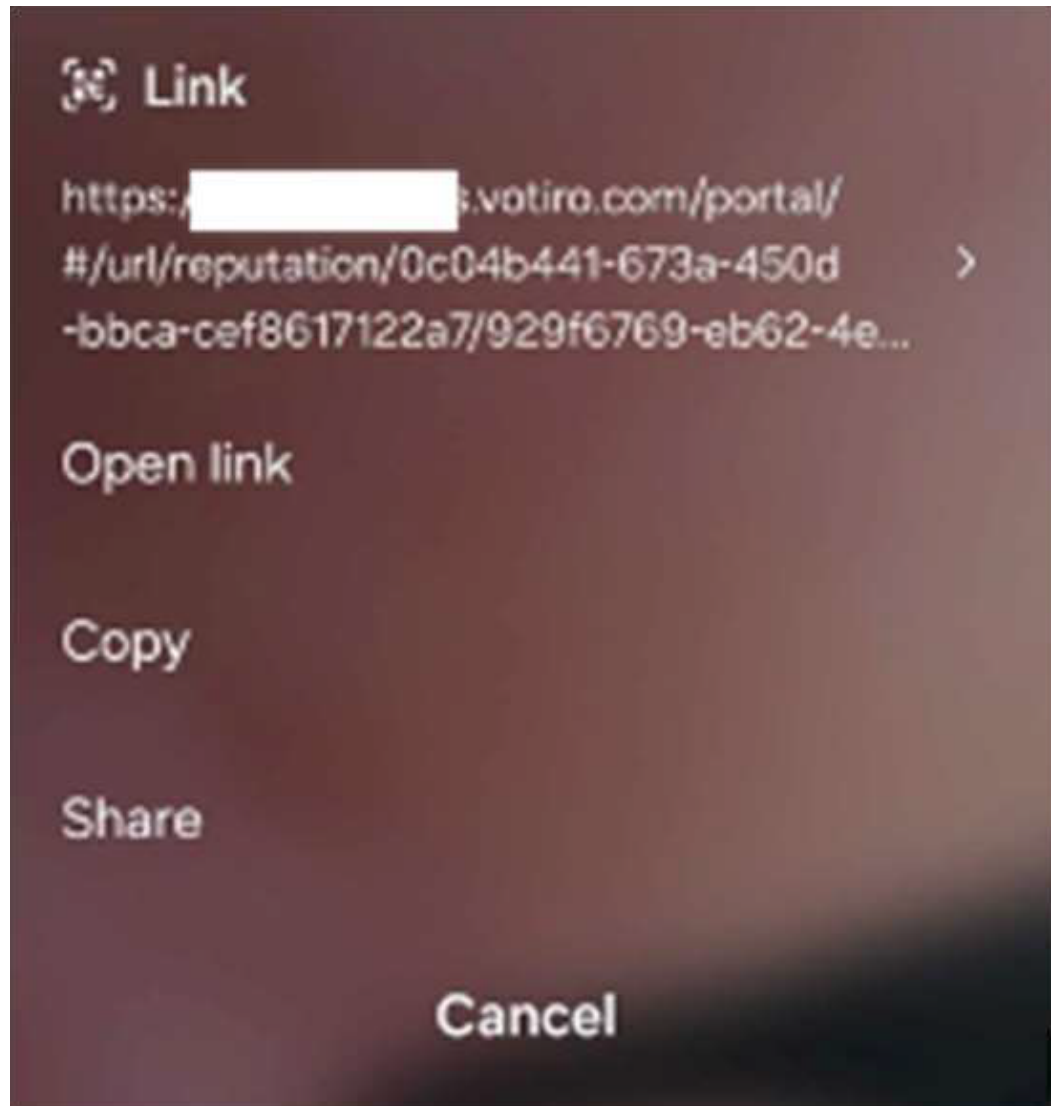
- Ignore - the QR Code is ignored. The file or email is passed on as-is.
- Detect QR Codes - detect if there is a QR Code in the file.
- Disarm QR Codes - the original QR code is rewritten with the Votiro QR Code.
- Block QR Codes - Votiro blocks the QR Code.

7.1 Disarm QR Codes behavior

1. The user scans the QR Code.



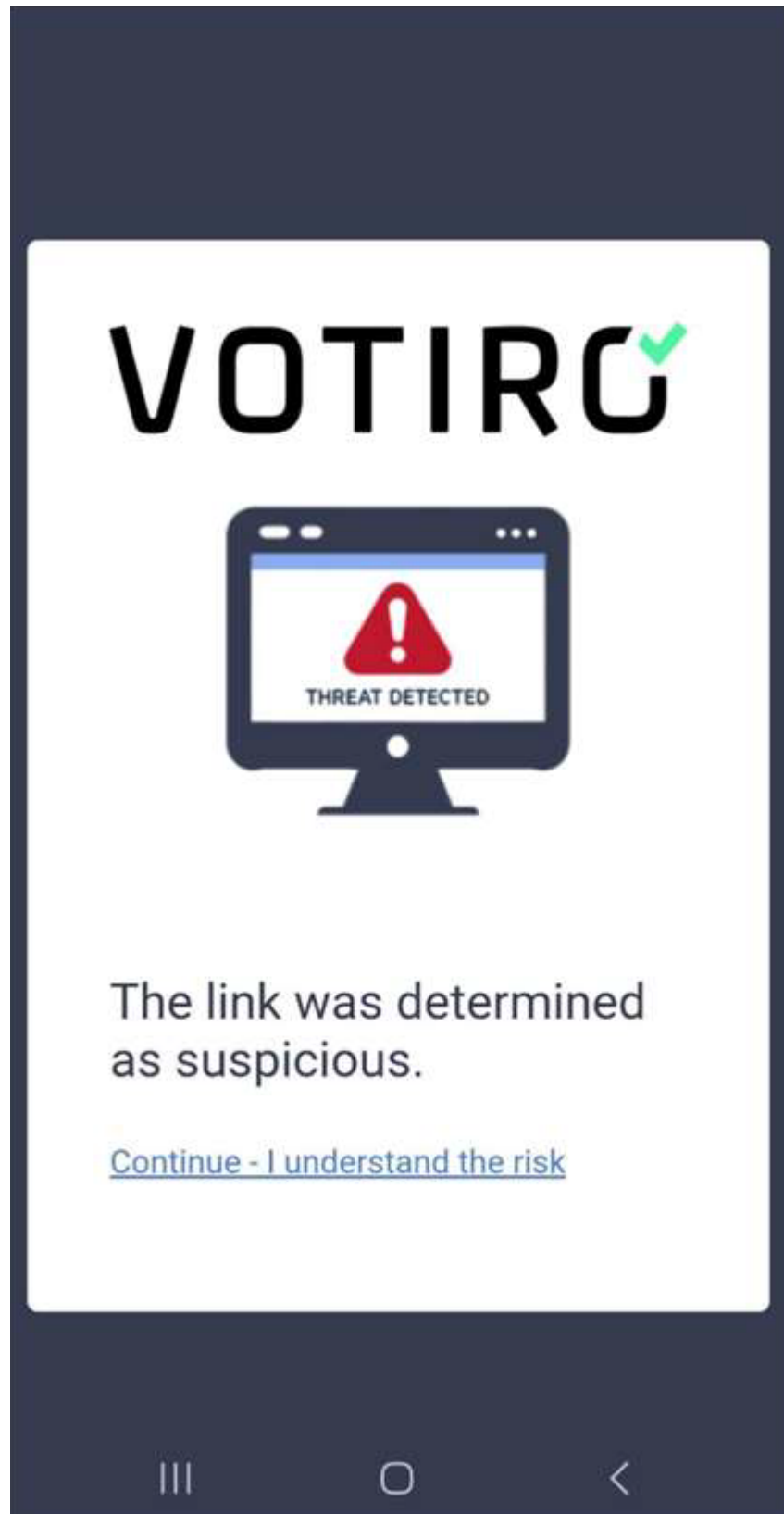
2. There will be an indication that the original QR Code was replaced with a Votiro QR Code pointing to the Votiro portal.



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.

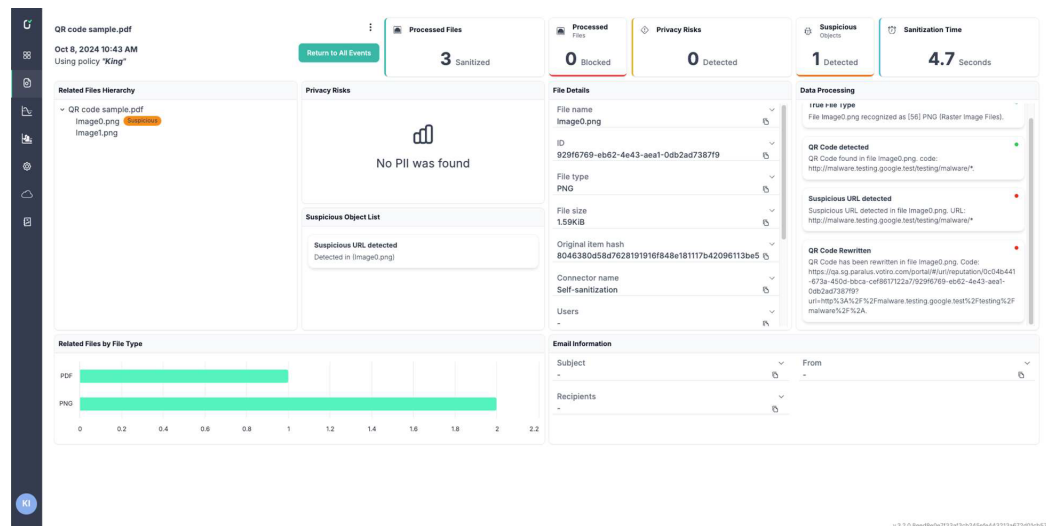


7.2 Votiro Administrator view

The file event will indicate if a:

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

For example:



8 URL Protection

For file types PDF, Word and Excel the user can define how to handle suspicious URLs.

There are four possible actions:

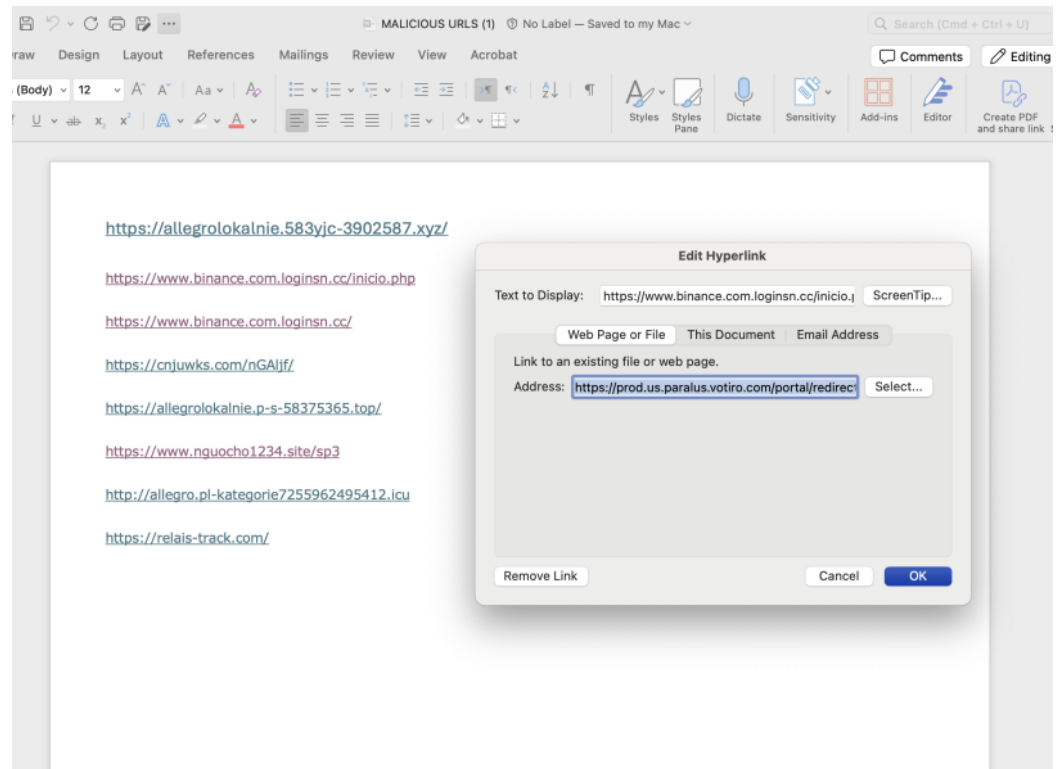
- **Don't do anything** - the URL is passed as-is.
- **Mask suspicious links** - the URL is masked if it is determined to be suspicious.
- **Sanitize suspicious links** - the URL is redirected to the Votiro portal for analysis.
- **Block document containing suspicious links** - the entire document is blocked if the URL is determined to be suspicious. This is the default action.

8.1 Workflow - Sanitize URLs

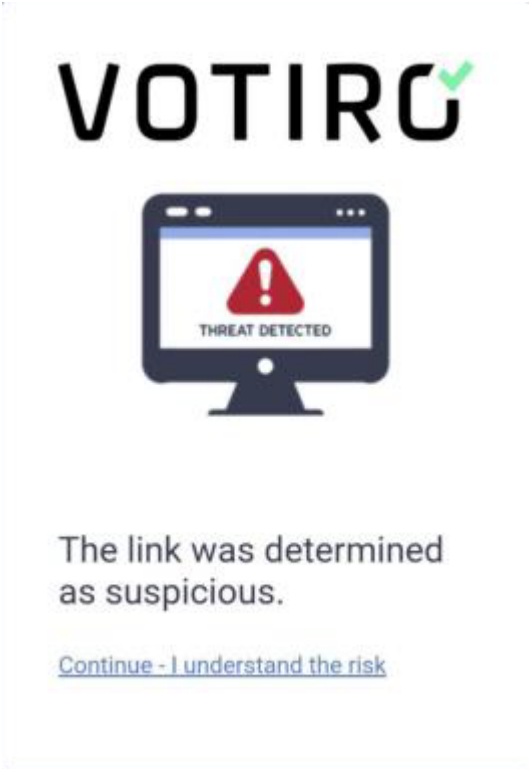
1. The user defines URL handling of PDF, Word and Excel files. See [URL Protection](#):

The screenshot shows the 'Microsoft Office' configuration page for URL protection. At the top right is a '+ Add Exception' button. The main configuration area is titled 'Default Action' and contains three radio buttons: 'Block' (red), 'Sanitize' (green, selected), and 'Allow' (blue). Below this is the 'Macro handling' section with a dropdown menu set to 'Remove all macros'. There are two checkboxes: 'Remove metadata' (unchecked) and 'Remove printer settings' (checked). The 'URL handling' section has a dropdown menu set to 'Sanitize suspicious links', which is open, showing four options: 'Don't do anything', 'Mask suspicious links', 'Sanitize suspicious links' (highlighted in blue), and 'Block documents containing suspicious links'. Below the dropdown are two checkboxes: 'Remove Ex' (checked) and 'Block Files' (checked). At the bottom is a 'Block Reason' field with a pencil icon.

2. A protected user receives a file from a URL.
3. When the user clicks on the URL, the user will be redirected to the Votiro portal.



4. If the URL was determined to be benign, the user will be redirected to the desired URL.
5. If the URL was determined to be suspicious, the user will receive a warning that a threat was detected.



6. Votiro administrator view - the file event will indicate that the URL was detected and was rewritten by Votiro.

