

VOTIRO✓



# Menlo x Votiro

## Integration



x

VOTIRO✓

# About this Guide

This integration guide is for enterprise Menlo and Votiro customers who have Votiro deployed on-premises or in their corporate clouds. This integration guide is for the Menlo Browser Isolation and Votiro Secure File Gateway for Web Downloads integration.

## Integration Overview

Votiro and Menlo directly integrate. Files are streamed from Menlo to Votiro directly, which allows users to seamlessly access downloaded files.

## Installation Prerequisites

Before connecting Menlo and Votiro, you will need to have a Menlo Browser Isolation environment and a Votiro environment. Votiro sets up the Votiro environment for our customers.

Connection is simple and seamless and doesn't require additional servers.

If you have any questions during the installation process, please contact us.

Votiro Support Center: <https://support.votiro.com/>

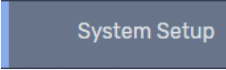
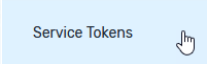
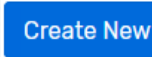
Votiro Support Email: [support@votiro.com](mailto:support@votiro.com)

Partner & MSSP Support Email: [menlo@votiro.com](mailto:menlo@votiro.com)

# Setup Procedure

## Votiro Configuration

You will need to log into your Votiro product and generate a Menlo connector token. To do this you will have to:

1. Click on System Setup 
2. Then click on Service Tokens  and Create New 
3. You will see a pop up that says Create New Service Token like so:

### Create New Service Token

Issued To

menlo

Expiration Time

< Jan 2022 >

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 29

30 31

01/31/2022

CREATE

CANCEL

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

ID

84ca8e16-eb80-4070-bf66-2a8c9ea8f080

Issued To

menlo




Expiration Time

01/31/2022

Token

eyJhbGciOiJIUzI1NiIsInR5cGU6IjY9ImVudC5kbGljaXQiOiJwbnRlcnM5bFNIcnZyZWZliiwicm9sZSI6IkFkbWluaXN0cmFob3IlLCJqdGkiOiI4NGNhOGUxNi1lYjgwLTQwNmZAtYmY2Ni0yYTlhOWVhOGEyODAlLCJuYmYiOiJE2MTF0Dc1NzMsmV4c6lMTY0MzYwNTliWCwiaWF0IjojExNTg3NTczfQk.HSzg3IK3blt5mTESFDt...\_o-j7mHz0w-wApwlsGFRpHubv8Yw7Ei56\_\_mRA8l\_Mcf4Pq\_wkizQuXH\_8G9qyYgNgaweH0nBLNZMelkeJRkxUHR-doy2x3ErDXGsyyxNigPYdKlFet7j42U6xzS\_eme6gO2dxrXkt0qZYBMkdZ11Mo0YL09k9de9WXv9BQ-DII2OUcqdzXokDs6ENUpcT4h6lyIUYS45Nr4ICz-FI2obSoWVhc-SL7JBjDI9C\_F0EdhJmZIVh6EXEmhovrgaScg7XBmM\_Pgr1V\_qN-\_1sv7N7e9swfvff2vpVK1HZx5xExZKzqmEWMe8Jmt4Q8NN9xZWg

OK

MenloApiSettings__ReturnCleanWhenBlocked	 false	App Config
VotiroDisarmerServiceSettings__AuthToken	 eyJhbGciOiAiU2ciOiJ1NiIsImtpZCI6IjcyMEU4MkZDRjE5N0Y0M0JBTUzNDgyQjM3NDAzRDQ4MkE	App Config
VotiroDisarmerServiceSettings__BaseUrl	 <a href="https://sfg.votiro.com">https://sfg.votiro.com</a>	App Config
















When complete it will look like this:

You can then define exactly what you want to happen to those particular files via Policy.




























menlo

TEST FILE

SAVE

Case	Default action	Exceptions
 Unknown File		
 Password Protected		
 Large File		
 Complex File		
 Special Case		

ACTION BY FILE TYPE

File type	Default action	Exceptions
 PDF		
 Image		
 Binary		
 Archive		
 RTF		
 Email		
 Microsoft Office		
 Text		
 Other Files		

## Menlo Configuration

In order to configure Menlo for Votiro you will need to log into Menlo as an administrator. Click

on Web Policy  and click on Content Inspection

Content Inspection and edit the Menlo File REST API to point to your Votiro for Menlo instance.

1. You will need to input the Base URL to point to your Votiro Menlo Connector.
2. You will also need to paste the SSL certificate of the Votiro instance into the Certificate area.
3. Check the box for Downloads.
4. Specify Connection timeout to 15 Seconds, Process timeout to 900 seconds, poll interval to 5 seconds, and specify your max file size for downloads.

Edit Menlo File REST API Integration

VOTIRO CONNECTOR SETTINGS

Plugin Name

Votiro Connector

Plugin Description

Menlo Votiro File REST API Server Integration

Base URL

https://menlo.prod.votiro.com

Certificate

-----BEGIN CERTIFICATE-----  
MIIDGzCCA13+gAwIBAgIEAgAuTANBgkqhkiG9w0BAQUFADBa  
MQswCQYDVQQGEwJ3  
RTESIBAGAlUECH3QmfSdG1tb331MRhwEQYDVQQLExwDclJ1

Type of Transfers

☒ Downloads ☐ Uploads

Authorization Header

7e794103-056d-42ea-aebd-ba0121578e99

Connect timeout

15 seconds

Process timeout

900 seconds

Poll Interval

5 seconds

Max Size

300 MB

Test

Cancel

Save Changes

You will want to **enable File Replacement** in Menlo.

1. The Action for transfers that cannot be processed should be set to Block.
2. The Action for transfers which are unknown should also be set to Block.
3. The Action for file sizes above size limit should be set to Continue Inspection or Block.

## Edit Menlo File REST API Integration

Process timeout  seconds

Poll Interval  seconds

Max Size  MB

Hash Check ☒

Metadata Check ☐

Allow File Replacement ☒

Skip Validation of Certificate ☐

(Test Button Only)

Action for transfers which cannot be processed ⊖ Block ⌵



Action for transfers which report an unknown outcome ⊖ Block ⌵

Action for transfers above size limit ✓ Continue Inspection ⌵

You will have to Create a Votiro Proxy Auto Configuration .data file. You can do this by Cloning the existing Standard PAC and adding SSL Inspection + Menlo Authentication. If you have SSO configured, you can use SSL Inspection + Single Sign-On.

The screenshot shows the MenloSecurity web interface. The top navigation bar includes 'Authentication', 'Admin Access Control', 'Admin Roles', and 'Proxy Auto Config'. The left sidebar has a 'Settings' menu item highlighted. The main content area is titled 'Proxy Automatic Configuration' and contains a table with two rows of proxy configurations. The first row is 'Standard' with 'No SSL Inspection + Menlo Authentication'. The second row is 'Votiro-PAC' with 'SSL Inspection + Menlo Authentication'. Both rows have a 'Location' column with a URL and an 'Actions' button. At the bottom right, there are 'Reset' and 'Save Changes' buttons.

Default	Display Name*	Proxy Mode	Location
<input type="radio"/>	Standard	No SSL Inspection + Menlo Authentication	<a href="https://pac.menlosecurity.com/votiro-6684f8c23fc/wpad.dat">https://pac.menlosecurity.com/votiro-6684f8c23fc/wpad.dat</a>
<input checked="" type="radio"/>	Votiro-PAC	SSL Inspection + Menlo Authentication	<a href="https://pac.menlosecurity.com/votiro-6684f8c23fc/copy1-wpad.dat">https://pac.menlosecurity.com/votiro-6684f8c23fc/copy1-wpad.dat</a>

To test the Menlo integration, you will need to download Proxy Switch Omega for your browser and point it to the Menlo PAX file under Settings  **Settings** and Proxy Auto Config  and copy the location of your PAX file into Proxy Switch Omega.

You can also test the integration without setting up the proxy; you can use this URL <https://safe.menlosecurity.com/fileyouwanttodownload.png> and authenticate with your Menlo account. This will now push the file to Menlo and sanitize the file through Votiro without enabling the proxy.



## Dataflow/Workflow

Below is an overview of the dataflow between Menlo and Votiro.



## Partner Configuration

Votiro hosts Partner instances on behalf of Partners. Please contact Votiro for more information on Partner Configurations.

**Contact:** [Menlo@votiro.com](mailto:Menlo@votiro.com)

## MSSP Configuration

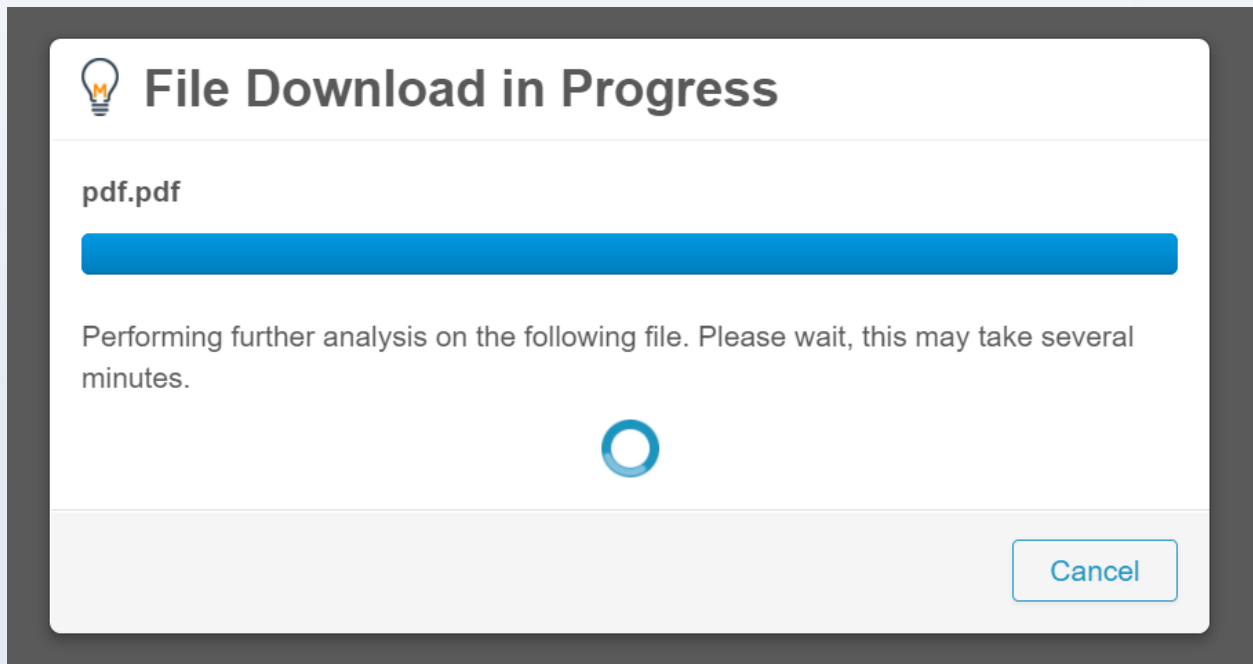
Votiro supports MSSP providers for multi-tenancy environments. Please contact Votiro for more information on MSSP Configurations.

**Contact:** [Menlo@votiro.com](mailto:Menlo@votiro.com)

## Verifying Result

Only after the configuration described above, will Menlo & Votiro sanitize the document. This can be done without using Menlo Browser Isolation. The below instructions are a **simple and fast** way to sanitize test documents in the integration.

1. Use a sample PDF with a url, such as <http://www.pdf995.com/samples/pdf.pdf>
2. Remove the text before // in the file url. Using the above example, this would be: [www.pdf995.com/samples/pdf.pdf](http://www.pdf995.com/samples/pdf.pdf)
3. Add the text from step 2 after the url <https://safe.menlosecurity.com/>
  - a. Using our example, this would be: <https://safe.menlosecurity.com/www.pdf995.com/samples/pdf.pdf>
4. This will take you to the Menlo login. Authenticate with your Menlo account with your Menlo credentials.
5. This will now push the file to Menlo and sanitize the file through Votiro without enabling the proxy.



# Votiro Integration in Menlo

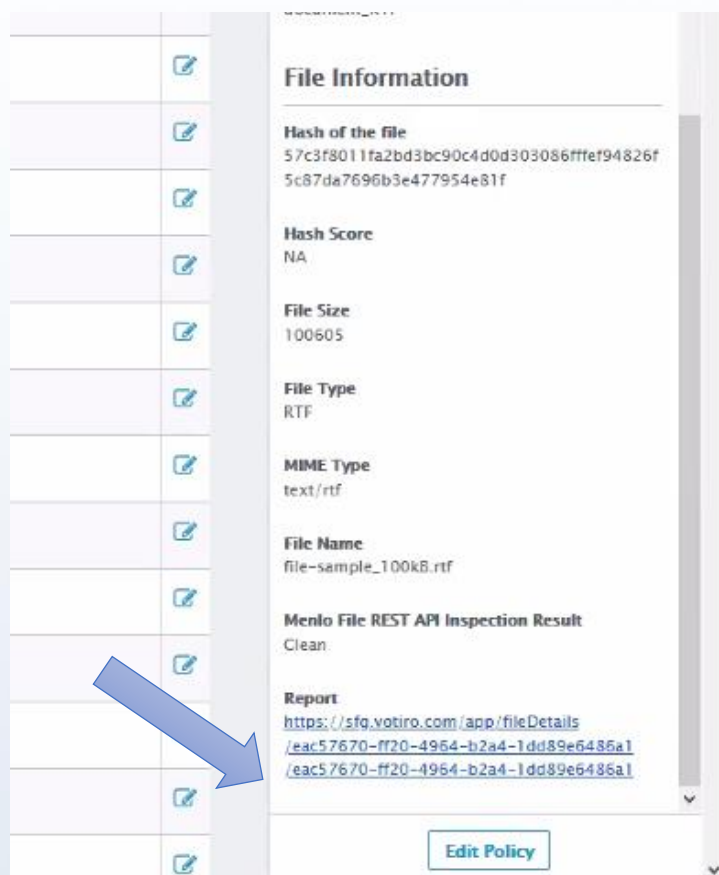
In the Menlo UI, you can see the file downloads by navigating to Logs, Web Logs, and then File Requests.

The screenshot shows the Menlo Security interface. On the left is a dark sidebar with a menu containing: Dashboard, Logs, Insights, Web Policy, Reporting, Settings, Customization, and Help. The 'Logs' menu item is highlighted with a blue arrow. The main content area has a 'Web Logs' tab selected, with a sub-tab 'All Logs' also highlighted by a blue arrow. Below the tabs are various filters including 'All groups', 'Last week', 'User ID', 'Domain', 'Category', 'Threat Type', 'All Risk Levels', and 'File Request'. The 'File Request' filter is highlighted with a blue arrow. A table of logs is displayed below the filters, with columns: Date, User ID, URL, Category, Threat Types, User Agent, Request Type, Risk, and Action. The first row shows a file request for 'https://file-examples-com.github.io/uploads/2019/09/f...' with a risk level of 'LOW' and an 'Allow' action.

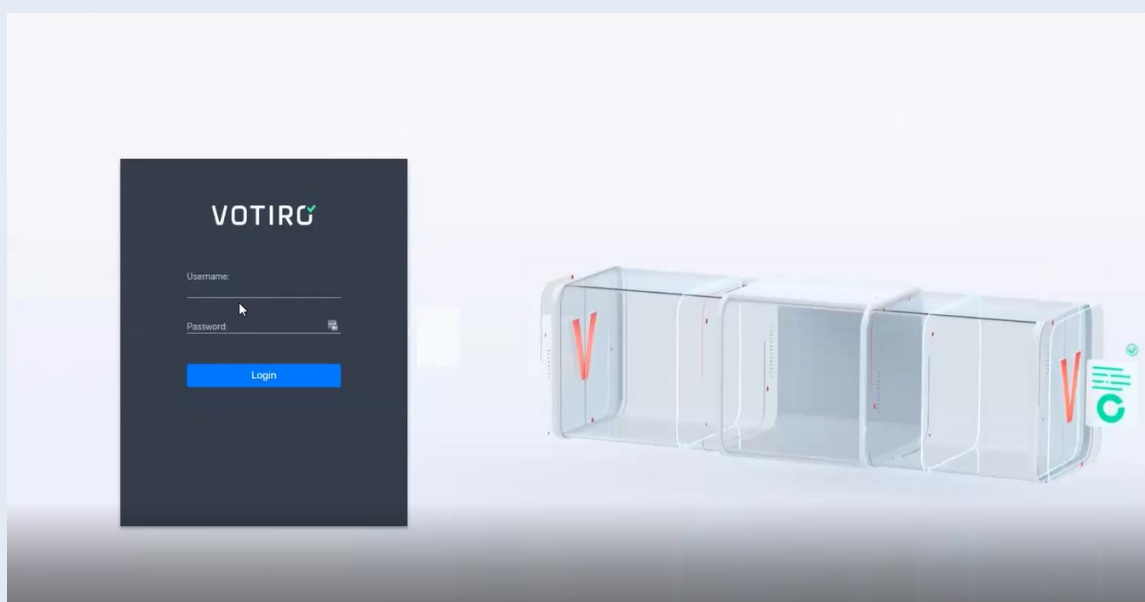
As items are downloaded, the Files are logged here.

This screenshot shows the same Menlo Security interface, but with a detailed view of a specific log entry on the right side. The entry is for a file request from 'Source IP 148.75.119.23' to 'https://file-examples-com.github.io/uploads/2019/09/f...'. The 'Access Mode' is 'Proxy' and the 'Response Code' is '200'. The 'File Information' section shows the file name 'file-sample\_100kB.txt', file size '100965', and file type 'text/plain'. The 'Menlo File REST API Inspection Result' is 'Clean'. The 'Report' section provides a link to the file details: 'https://slg.votiro.com/app/FileDetails/...'. The main table of logs is still visible on the left, showing multiple entries for file requests.

To dig into a specific file further, choose your file based on the row. Then click on the file link in the File Information section of the UI. The link will be located on the lower right hand side under "Report."



This link will take you to the Votiro interface where you can log into the Votiro dashboard and view more details around the file.



The screenshot displays the VOTIRO dashboard with a sidebar on the left containing navigation links: Monitor, System Activity, Incident Manager, Explore Incidents, Settings, System Setup, Policies, Exports, and Reports. The main content area is divided into three panels:

- FILES:** A list of files including [Content...Types].xml, .rels, document.xml, fontTable.xml, numbering.xml, settings.xml, styles.xml, webSettings.xml, app.xml, core.xml, and document.xml.rels. The file 'file-sample\_100kB.rtf' is selected.
- FILE INFO:** Details for 'file-sample\_100kB.rtf':
 

File Type	RTF Files
Original Item Hash	57c3f8011fa2bd3bc90c4d0d303086f94826f5c87da7696b3e477954e81f
Connector Name	Menlo
Connector Type	File Connector
- SANITIZATION LOG:** A log of sanitization events:
  - Started: 01/26/2021 | 09:00:43 AM
  - File file-sample\_100kB.rtf recognized as [1003] RTF Files (RTF Files).
  - File 'file-sample\_100kB.rtf' original published.
  - File file-sample\_100kB.rtf upload for sanitization started. Item Id: eac57670-#20-4964-b2a4-1dd89e6486a1
  - New child created for item eac57670-#20-4964-b2a4-1dd89e6486a1. Child ID: 84cd13b5-eee2-4a02-b480-e34c3cbb15a.
  - Ended: 01/28/2021 | 09:02:45 AM
  - Total Sanitization Time: 122.1 sec

At the bottom, a 'THREATS DETECTED' summary shows 14 Files Sanitized and 0 Threats Detected.

The security team can also access and download the original file for further investigations and threat hunting.

This screenshot shows the 'FILE INFO' section for a 'Docx file with embedded EXE'. The 'File actions' dropdown menu is open, showing options: Explore incidents, Download original, Download sanitized, and Release original. A blue arrow points to the 'Download original' option. The 'FILE INFO' panel on the right shows details for 'PromptOnlyNoD':

File Type	Exe
Original Item Hash	e2ef...
Connector Name	Men
Connector Type	File

**Please note:** If we send a response back to the Menlo API, it is marked as infected in the File Information section. However, that does not mean that the file is infected. That means that the file has been blocked by Votiro, which is based on file type or customer policy.

	HIGH	Block	
	LOW	Allow	
	LOW	Allow	
ated ...	LOW	Isolate	
ated ...	LOW	Isolate	
ated ...	LOW	Isolate	
	LOW	Allow	
ginal ...	LOW	Allow	
ated ...	LOW	Isolate	
ated ...	LOW	Isolate	
ated ...	LOW	Isolate	
ated ...	LOW	Isolate	
ated ...	HIGH	Isolate	
ated ...	LOW	Isolate	
ated ...	LOW	Isolate	

Security isolates all web content. Downloaded files or documents are analyzed by multiple scanning engines. Downloading of this file has been blocked and only safe Document Isolation access is allowed.

### File Information

**Hash of the file**  
9a30a503b2862c51c3c5acd7fbc2f1f784cf4658ccf8e87d5023a90c21c0714

**Hash Score**  
NA

**File Size**  
9

**File Type**  
Unknown

**MIME Type**  
text/plain

**File Name**  
test\_file

**Menlo File REST API Inspection Result**  
Infected

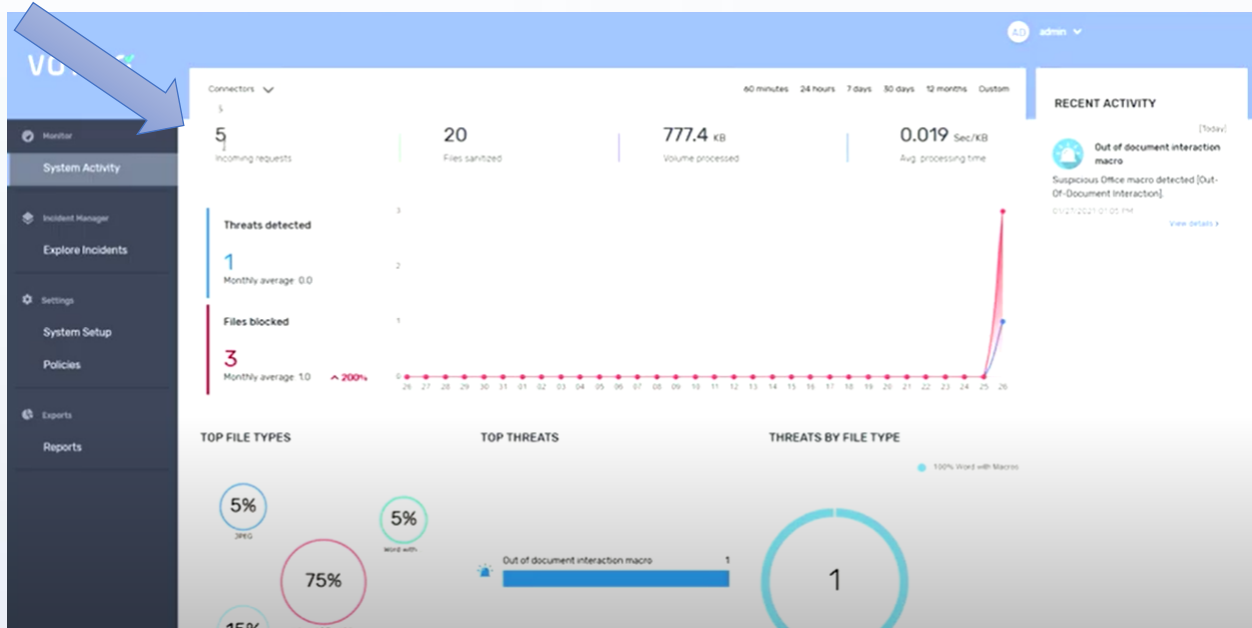
**Report**  
<https://lab.votiro.com/app/fileDetails/98695c4d-e201-460b-8ae9-ac401b683310/98695c4d-e201-460b-8ae9-ac401b683310>

[Edit Policy](#)

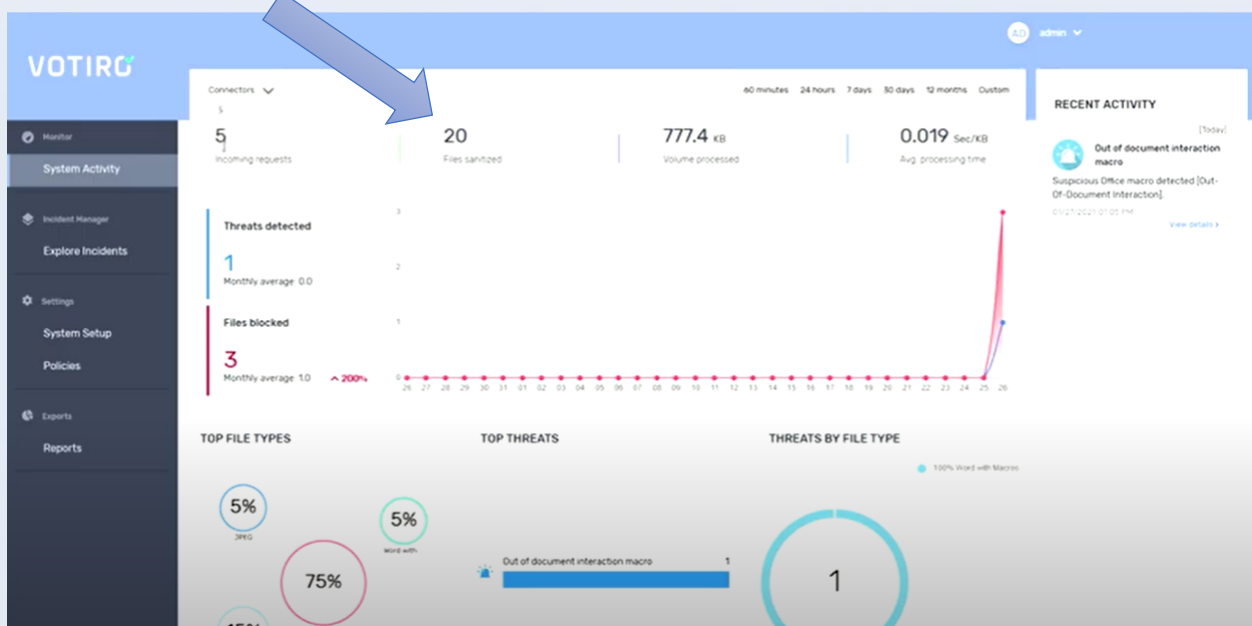
**Please note:** Votiro does not currently provide threat intelligence for files that were blocked, because we don't block based on threat intelligence or according to known threats. We process and sanitize every file, regardless of whether or not it contains a threat.

## Votiro Dashboard Overview

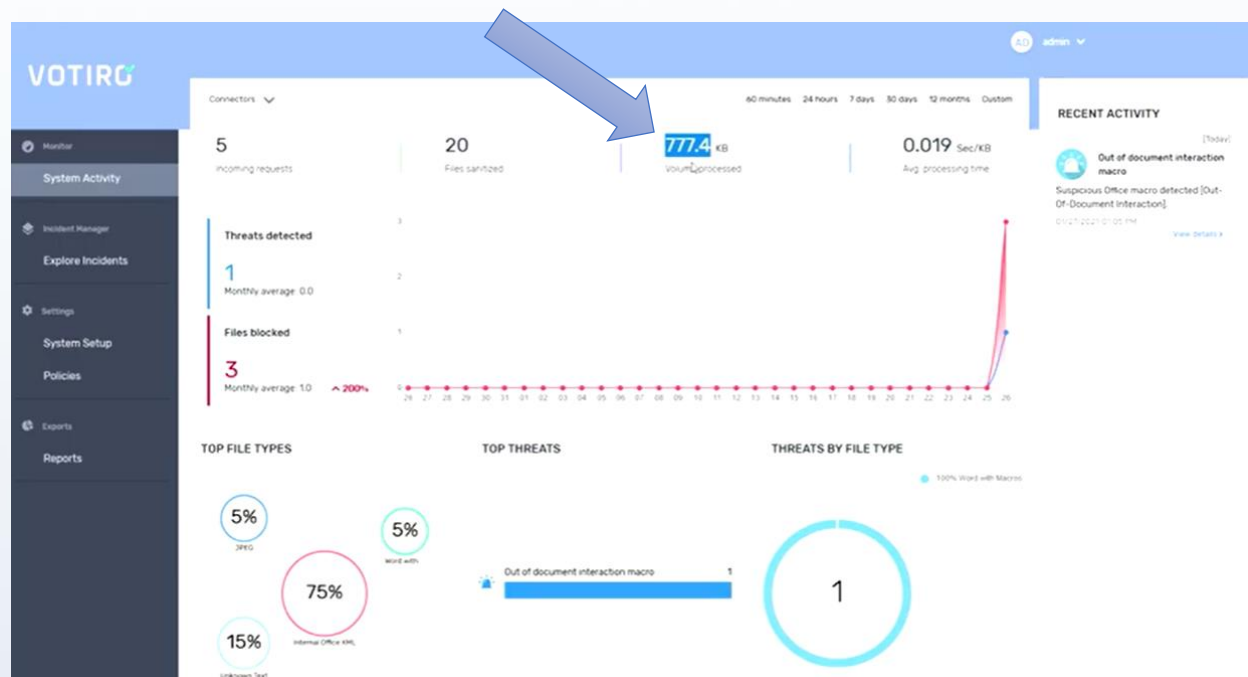
All files will flow into the Menlo UI, as shown in the previous section. Within the Votiro Dashboard, it will look similar to the below screenshot. As you see files coming through, you will see incoming requests in the upper left-hand side.



Within those incoming requests may be children files that are embedded in those primary files.



This section indicates how much data is being processed in the Votiro Solution and how fast files are being processed.



## Questions? Contact Us

Votiro Support Center: <https://support.votiro.com/>

Votiro Support Email: [support@votiro.com](mailto:support@votiro.com)

Partner & MSSP Support Email: [menlo@votiro.com](mailto:menlo@votiro.com)