Menlo x Votiro

Integration

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/

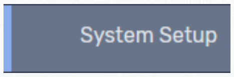
Votiro Support Email: support@votiro.com

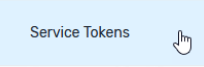
Partner & MSSP Support Email: menlo@votiro.com

Setup Procedure

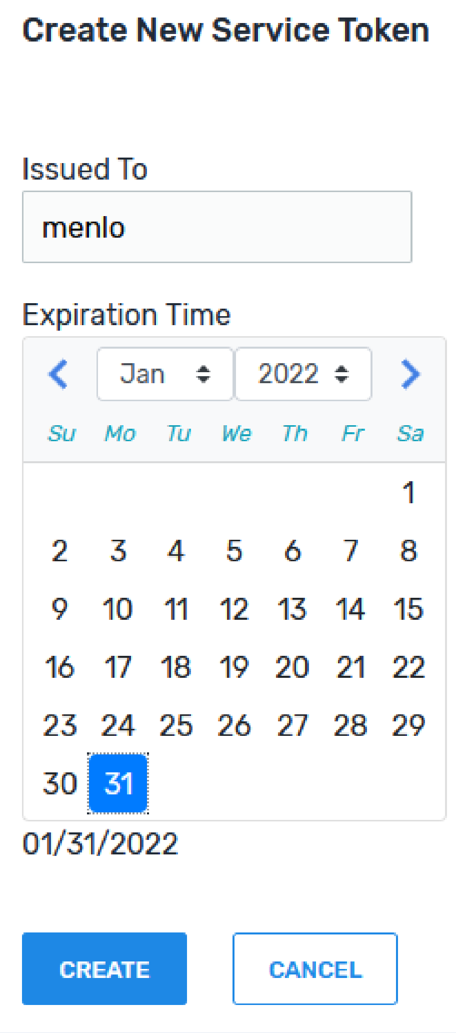
Votiro Configuration

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

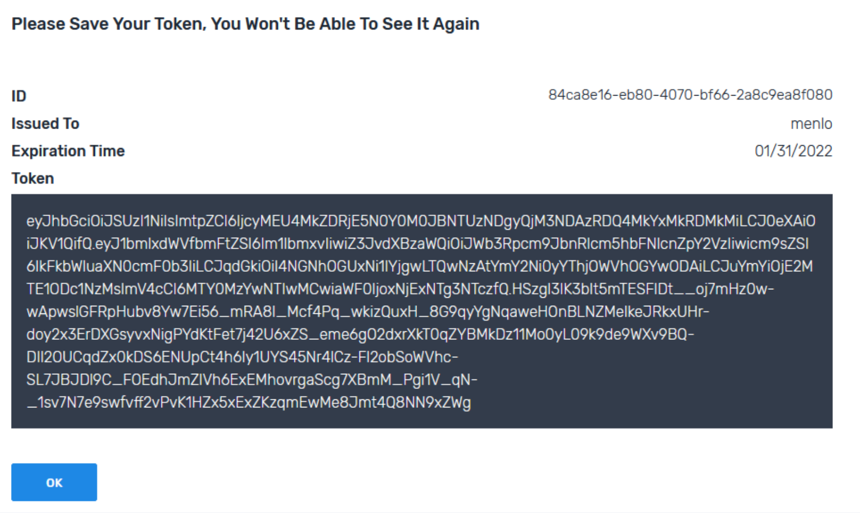
Expiration Time

< 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

You will need to create a name for the token and specify the date. Please be sure to click on the date number and Create. You will see a window with your new token. **Please make a copy of this token for later use**.



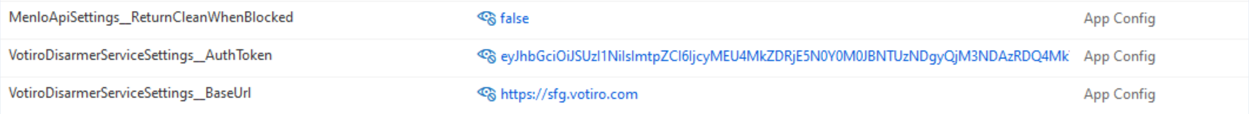
Please Save Your Token, You Won't Be Able To See It Again

ID	84ca8e16-eb80-4070-bf66-2a8c9ea8f080
Issued To	menlo
Expiration Time	01/31/2022

Token

```
eyJhbGciOiJSUzI1NiIsImtpZCI6IjcyMEU4MkZDRjE5N0Y0M0JBNTUzNDgyQjM3NDAzRDQ4MkYxMkRDMkMiLCJ0eXAiO
iJKV1QifQ.eyJ1bmlxdWVfbmFtZSI6Im1lbmxvIiwiZ3JvdXBzaWQiOiJWb3Rpcm9JbnRlcm5hbFNlcnZpY2VzIiwicm9sZSI
6IkFkbWluaXN0cmF0b3IiLCJqdGkiOiI4NGNhOGUxNi1lYjgwLTQwNzAtYmY2Ni0yYThjOWVhOGYwODAiLCJuYmYiOjE2M
TE1ODc1NzMsImV4cCI6MTY0MzYwNTIwMCwiaWF0IjoxNjExNTg3NTczfQ.HSzgI3IK3bIt5mTESFIDt__oj7mHz0w-
wApwslGFRpHubv8Yw7Ei56_mRA8I_Mcf4Pq_wkizQuxH_8G9qyYgNqaweH0nBLNZMeIkeJRkxUHr-
doy2x3ErDXGsyvxNigPYdKtFet7j42U6xZS_eme6gO2dxrXkT0qZYBMkDz11Mo0yL09k9de9WXv9BQ-
DIl2OUCqdZx0kDS6ENUpCt4h6ly1UYS45Nr4ICz-FI2obSoWVhc-
SL7JBJDI9C_F0EdhJmZIVh6ExEMhovrgaScg7XBmM_Pgi1V_qN-
_1sv7N7e9swfvff2vPvK1HZx5xExZKzqmEwMe8Jmt4Q8NN9xZWg
```

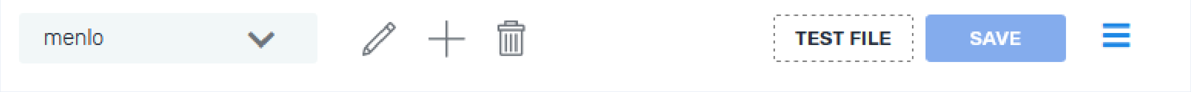
Next you will have to configure the Votiro Menlo API connector. You will need the Base URL which is the Votiro server name and token that will allow for Votiro File sanitization. In the Votiro Menlo connector you will specify the Votiro server, Votiro Auth Token, preferred settings when processing.



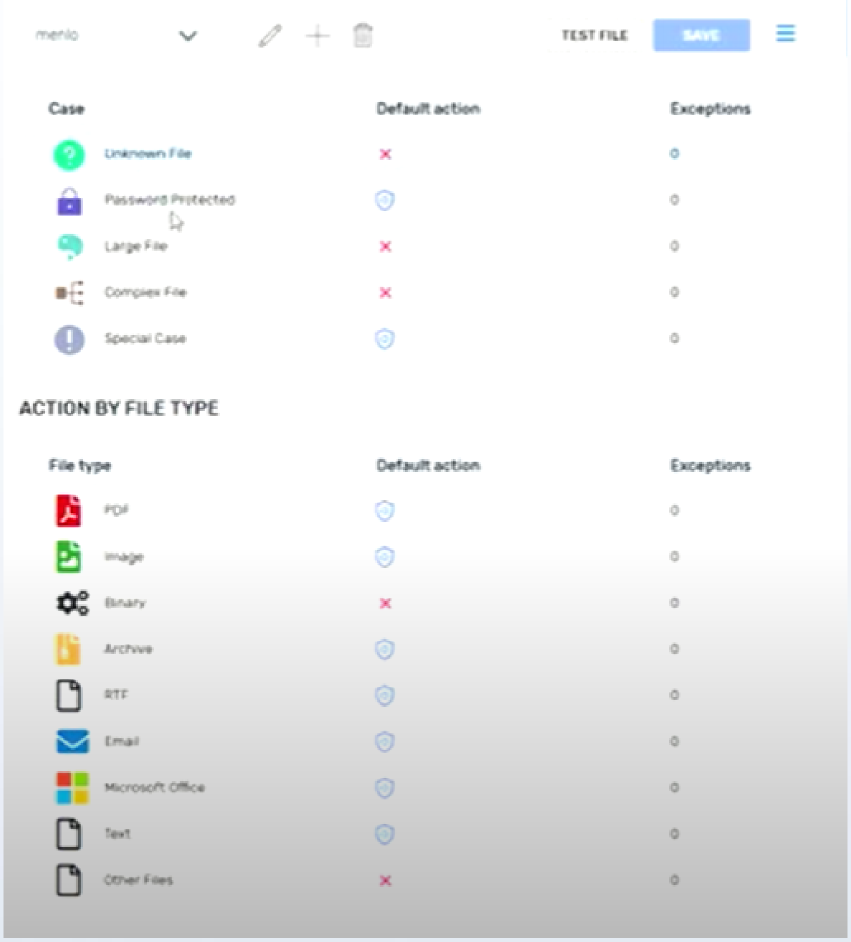
MenloApiSettings__ReturnCleanWhenBlocked	false	App Config
VotiroDisarmerServiceSettings__AuthToken	eyJhbGciOiJSUzI1NiIsImtpZCI6IjcyMEU4MkZDRjE5N0Y0M0JBNTUzNDgyQjM3NDAzRDQ4Mk	App Config
VotiroDisarmerServiceSettings__BaseUrl	https://sfg.votiro.com	App Config

In the Votiro UI you will create a Menlo file processing Policy. By going into Policies and clicking on the Plus button + and type in Menlo for the policy name here.

When complete it will look like this:



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

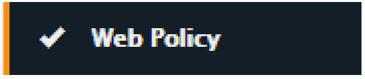


Case	Default action	Exceptions
Unknown File	✕	0
Password Protected	🛡	0
Large File	✕	0
Complex File	✕	0
Special Case	🛡	0

ACTION BY FILE TYPE

File type	Default action	Exceptions
PDF	🛡	0
Image	🛡	0
Binary	✕	0
Archive	🛡	0
RTF	🛡	0
Email	🛡	0
Microsoft Office	🛡	0
Text	🛡	0
Other Files	✕	0

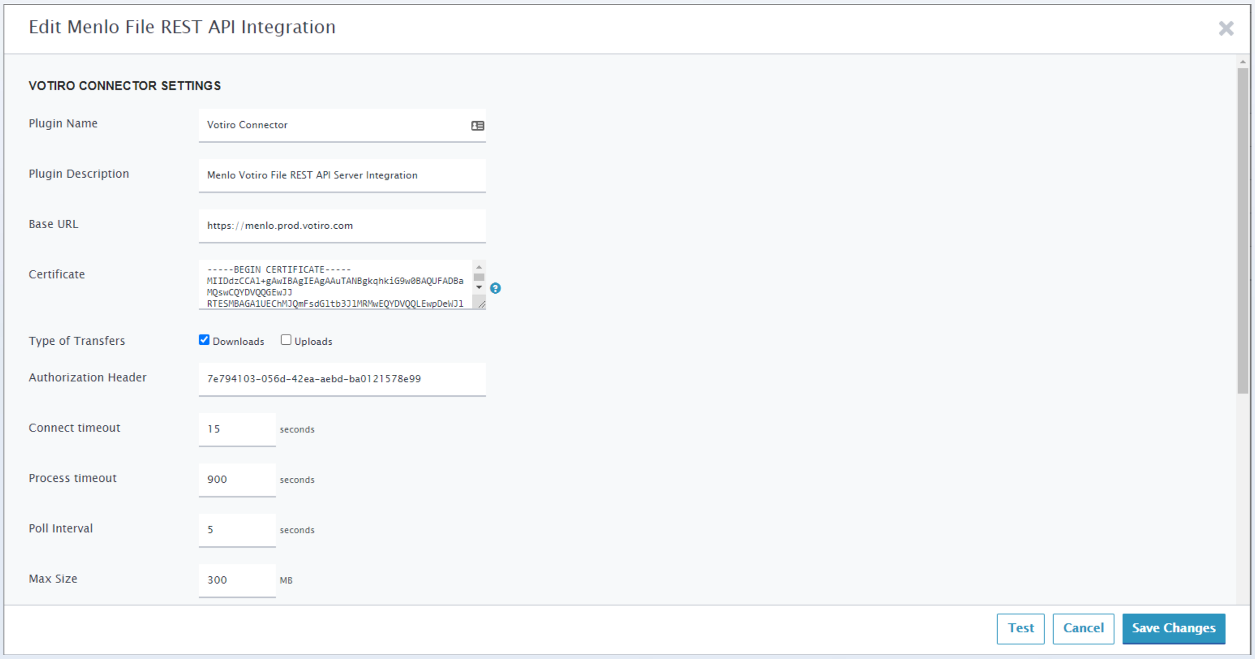
Menlo Configuration

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

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.



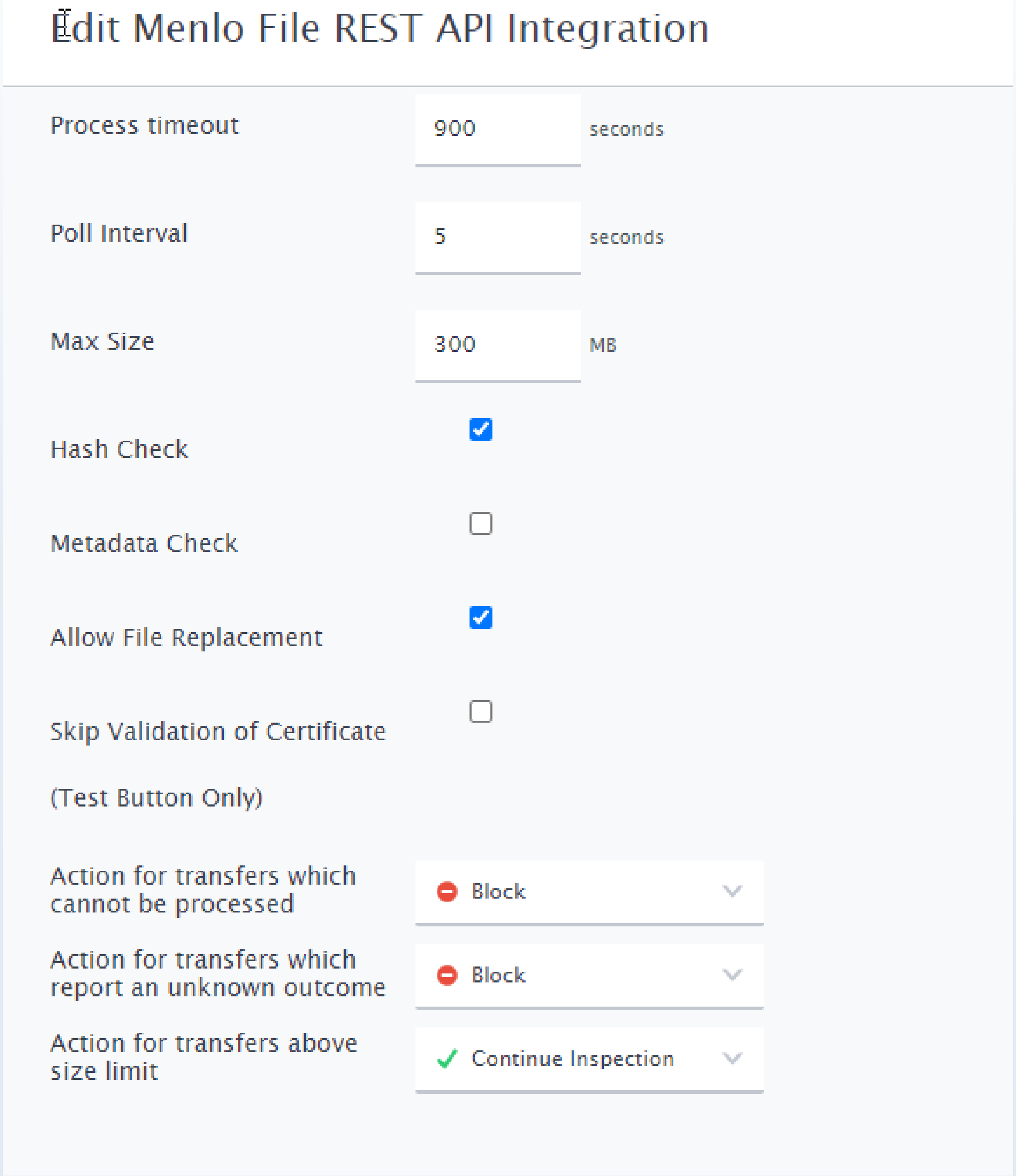
Edit Menlo File REST API Integration

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----- MIIDdzCCA1+gAwIBAgIEAgAAuTANBgkqhkiG9w0BAQUFADBa MQswCQYDVQQGEwJJ RTESMBAGA1UEChMJQmFsdGltb3J1MRMwEQYDVQQLEwpDeWJ1
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

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

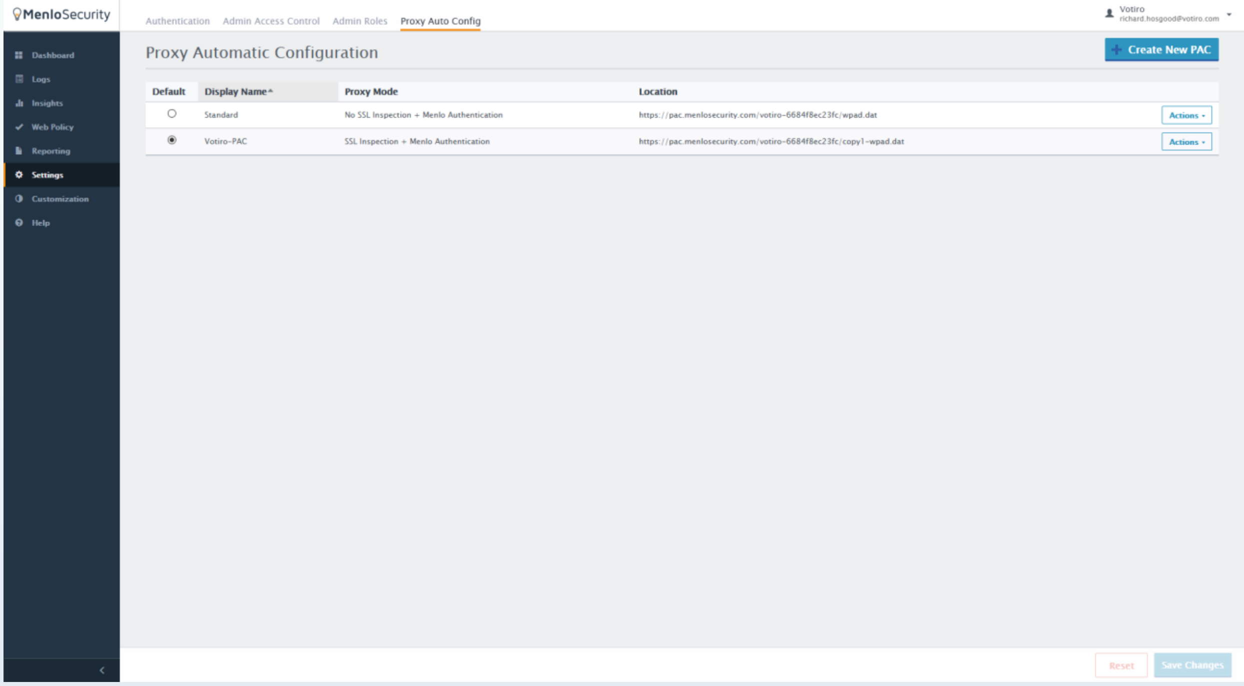
1. The Action for transfers that cannot be processed should be set to Block.
2. The Action for transfers which are unknown should also be set to Block.
3. The Action for file sizes above size limit should be set to Continue Inspection or Block.



Edit Menlo File REST API Integration

Process timeout	900 seconds
Poll Interval	5 seconds
Max Size	300 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.



Proxy Automatic Configuration

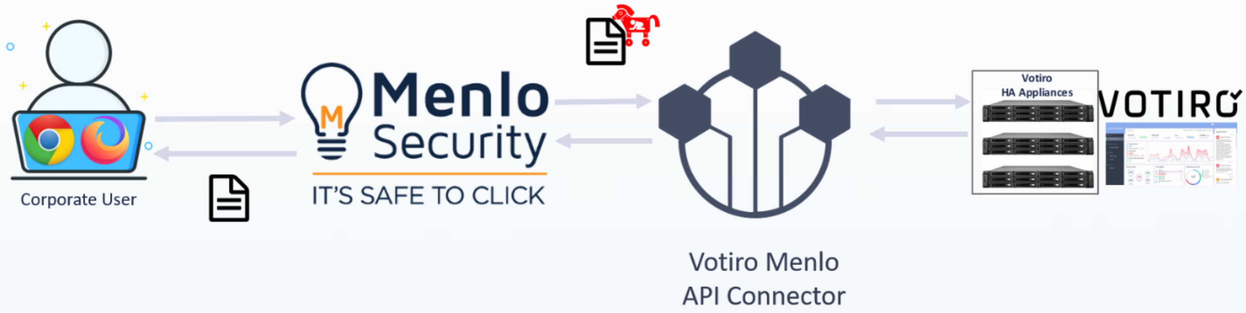
Default	Display Name	Proxy Mode	Location	
○	Standard	No SSL Inspection + Menlo Authentication	https://pac.menlosecurity.com/votiro-6684f8ec23fc/wpad.dat	Actions
●	Votiro-PAC	SSL Inspection + Menlo Authentication	https://pac.menlosecurity.com/votiro-6684f8ec23fc/copy1-wpad.dat	Actions

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 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

MSSP Configuration

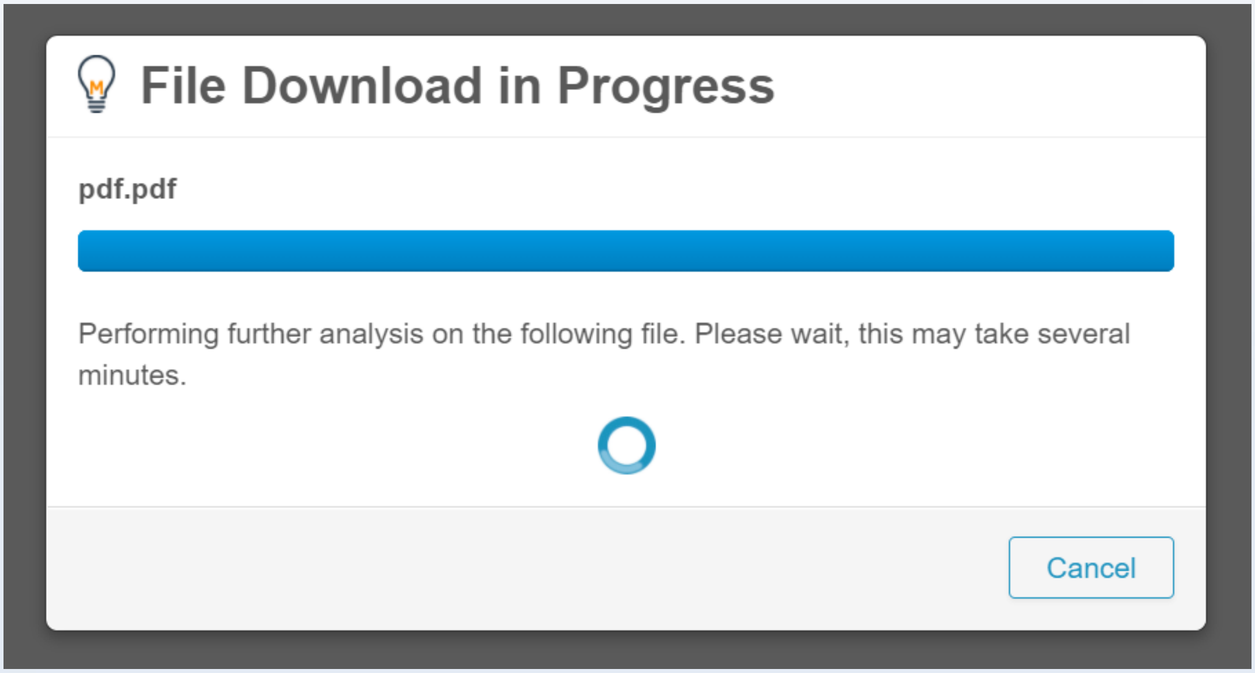
Votiro supports MSSP providers for multi-tenancy environments. Please contact Votiro for more information on MSSP Configurations.

Contact: 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
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.



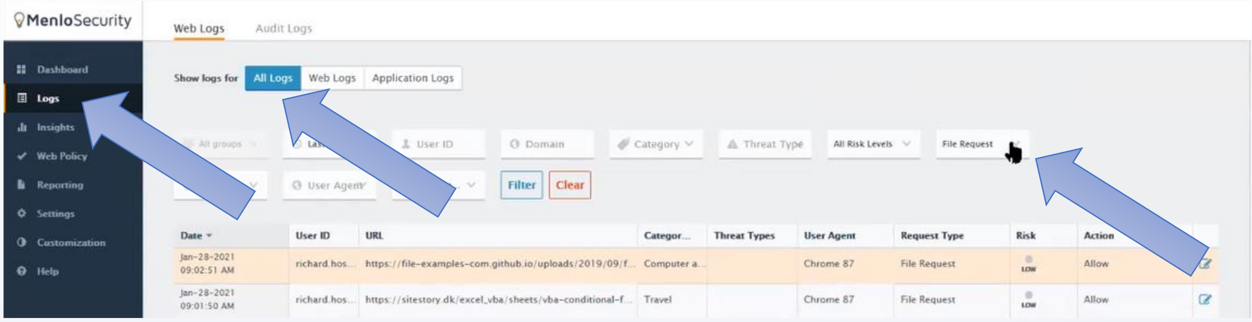
File Download in Progress

pdf.pdf

Performing further analysis on the following file. Please wait, this may take several minutes.

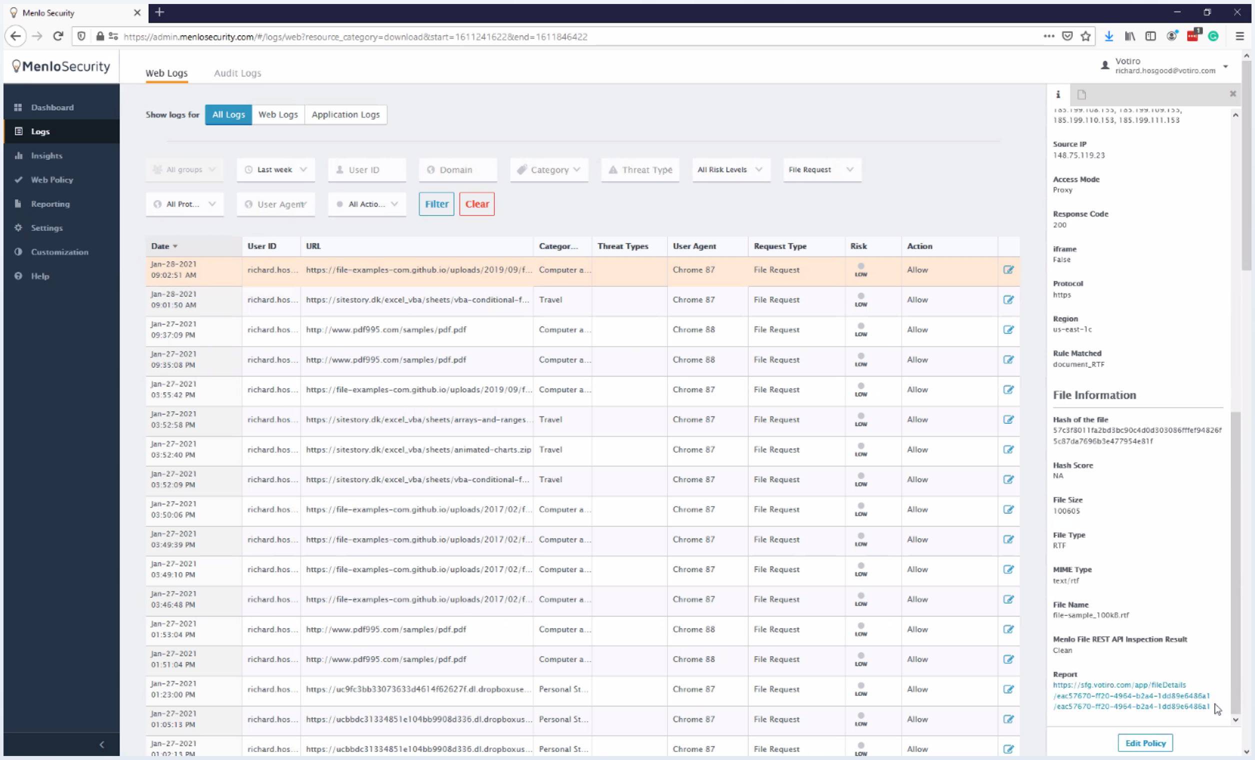
Votiro Integration in Menlo

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



Date	User ID	URL	Categor...	Threat Types	User Agent	Request Type	Risk	Action
Jan-28-2021 09:02:51 AM	richard.hos...	https://file-examples-com.github.io/uploads/2019/09/f...	Computer a...		Chrome 87	File Request	LOW	Allow
Jan-28-2021 09:01:50 AM	richard.hos...	https://sitestory.dk/excel_vba/sheets/vba-conditional-f...	Travel		Chrome 87	File Request	LOW	Allow

As items are downloaded, the Files are logged here.



Date	User ID	URL	Categor...	Threat Types	User Agent	Request Type	Risk	Action
Jan-28-2021 09:02:51 AM	richard.hos...	https://file-examples-com.github.io/uploads/2019/09/f...	Computer a...		Chrome 87	File Request	LOW	Allow
Jan-28-2021 09:01:50 AM	richard.hos...	https://sitestory.dk/excel_vba/sheets/vba-conditional-f...	Travel		Chrome 87	File Request	LOW	Allow
Jan-27-2021 09:37:09 PM	richard.hos...	http://www.pdf995.com/samples/pdf.pdf	Computer a...		Chrome 88	File Request	LOW	Allow
Jan-27-2021 09:35:08 PM	richard.hos...	http://www.pdf995.com/samples/pdf.pdf	Computer a...		Chrome 88	File Request	LOW	Allow
Jan-27-2021 03:55:42 PM	richard.hos...	https://file-examples-com.github.io/uploads/2019/09/f...	Computer a...		Chrome 87	File Request	LOW	Allow
Jan-27-2021 03:52:58 PM	richard.hos...	https://sitestory.dk/excel_vba/sheets/arrays-and-ranges...	Travel		Chrome 87	File Request	LOW	Allow
Jan-27-2021 03:52:40 PM	richard.hos...	https://sitestory.dk/excel_vba/sheets/animated-charts.zip	Travel		Chrome 87	File Request	LOW	Allow
Jan-27-2021 03:52:09 PM	richard.hos...	https://sitestory.dk/excel_vba/sheets/vba-conditional-f...	Travel		Chrome 87	File Request	LOW	Allow
Jan-27-2021 03:50:06 PM	richard.hos...	https://file-examples-com.github.io/uploads/2017/02/f...	Computer a...		Chrome 87	File Request	LOW	Allow
Jan-27-2021 03:49:39 PM	richard.hos...	https://file-examples-com.github.io/uploads/2017/02/f...	Computer a...		Chrome 87	File Request	LOW	Allow
Jan-27-2021 03:49:10 PM	richard.hos...	https://file-examples-com.github.io/uploads/2017/02/f...	Computer a...		Chrome 87	File Request	LOW	Allow
Jan-27-2021 03:46:48 PM	richard.hos...	https://file-examples-com.github.io/uploads/2017/02/f...	Computer a...		Chrome 87	File Request	LOW	Allow
Jan-27-2021 01:53:04 PM	richard.hos...	http://www.pdf995.com/samples/pdf.pdf	Computer a...		Chrome 88	File Request	LOW	Allow
Jan-27-2021 01:51:04 PM	richard.hos...	http://www.pdf995.com/samples/pdf.pdf	Computer a...		Chrome 88	File Request	LOW	Allow
Jan-27-2021 01:23:00 PM	richard.hos...	https://uc9fc3bb33073633d4614f62627f.dl.dropboxuse...	Personal St...		Chrome 87	File Request	LOW	Allow
Jan-27-2021 01:05:13 PM	richard.hos...	https://ucbbdc31334851e104bb9908d336.dl.dropboxus...	Personal St...		Chrome 87	File Request	LOW	Allow
Jan-27-2021 01:02:13 PM	richard.hos...	https://ucbbdc31334851e104bb9908d336.dl.dropboxus...	Personal St...		Chrome 87	File Request	LOW	Allow

185.199.108.153, 185.199.109.153,
185.199.110.153, 185.199.111.153

Source IP
148.75.119.23

Access Mode
Proxy

Response Code
200

iframe
False

Protocol
https

Region
us-east-1c

Rule Matched
document_RTF

File Information

Hash of the file
57c3f8011fa2bd3bc90c4d0d303086fffef94826f
5c87da7696b3e477954e81f

Hash Score
NA

File Size
100605

File Type
RTF

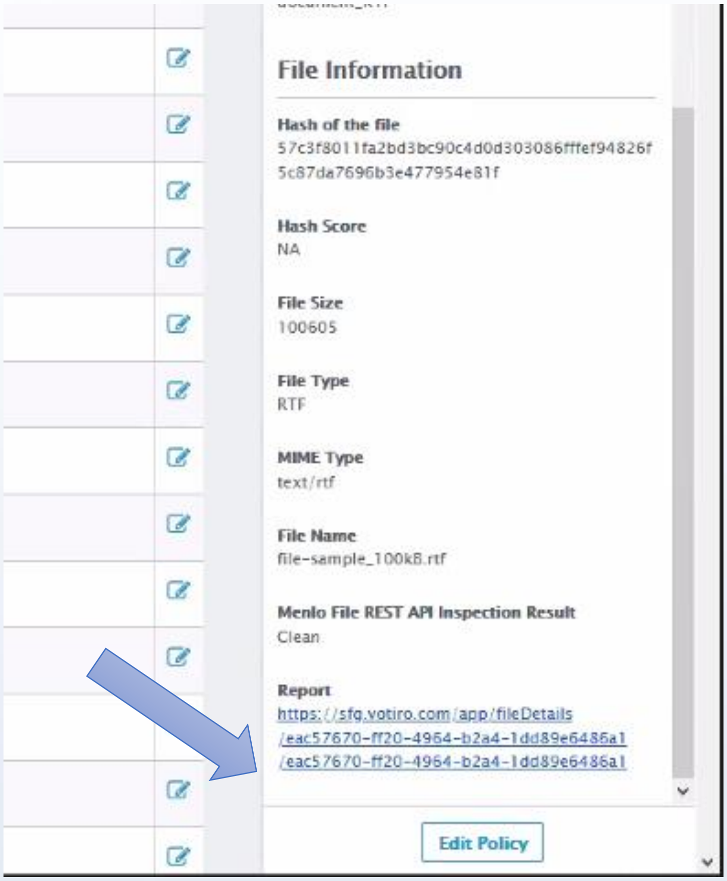
MIME Type
text/rtf

File Name
file-sample_100kB.rtf

Menlo File REST API Inspection Result
Clean

Report
https://sfg.votiro.com/app/fileDetails
/eac57670-ff20-4964-b2a4-1dd89e6486a1
/eac57670-ff20-4964-b2a4-1dd89e6486a1

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.”



File Information

Hash of the file
57c3f8011fa2bd3bc90c4d0d303086fffef94826f5c87da7696b3e477954e81f

Hash Score
NA

File Size
100605

File Type
RTF

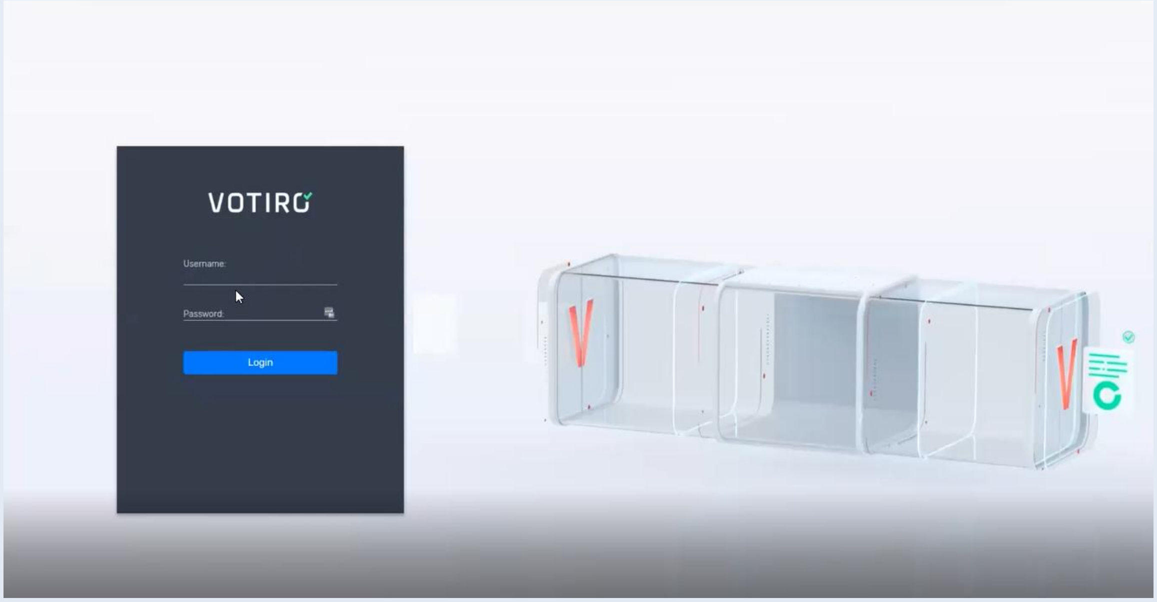
MIME Type
text/rtf

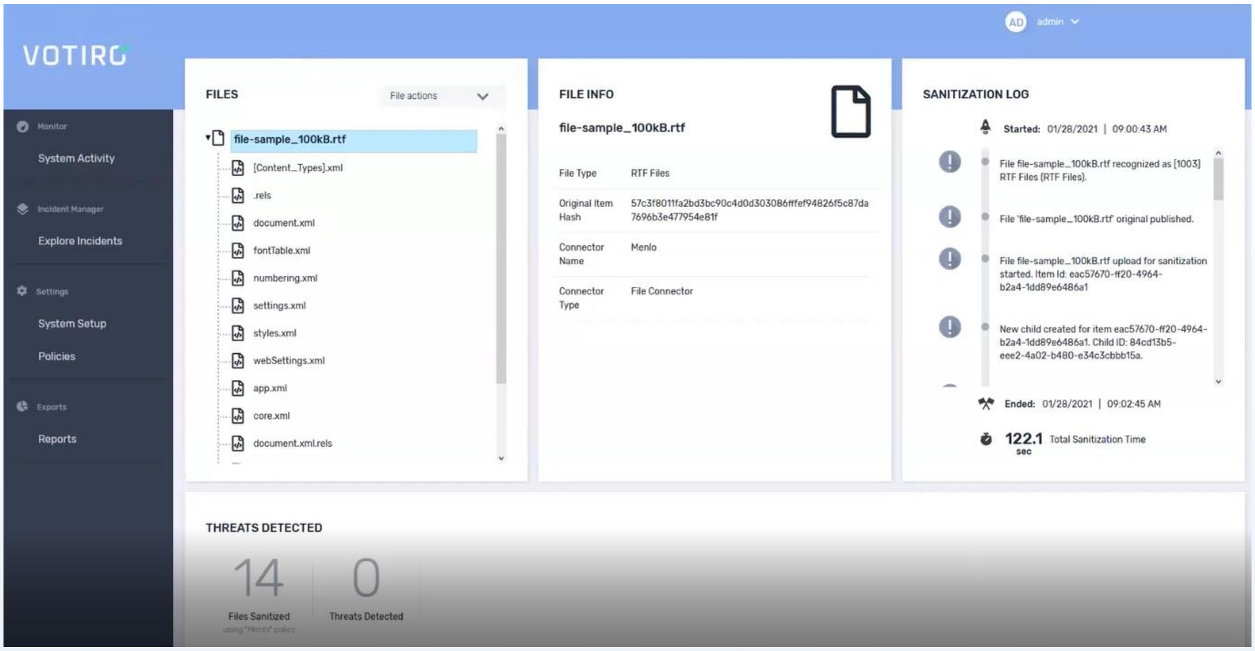
File Name
file-sample_100kB.rtf

Menlo File REST API Inspection Result
Clean

Report
https://sfg.votiro.com/app/fileDetails/eac57670-ff20-4964-b2a4-1dd89e6486a1/eac57670-ff20-4964-b2a4-1dd89e6486a1

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





FILE INFO

file-sample_100kB.rtf

File Type	RTF Files
Original Item Hash	57c3f8011fa2bd3bc90c4d0d303086fffef94826f5c87da7696b3e477954e81f
Connector Name	Menlo
Connector Type	File Connector

SANITIZATION LOG

Started: 01/28/2021 | 09:00:43 AM

File file-sample_100kB.rtf recognized as [1003] RTF Files (RTF Files).

File 'file-sample_100kB.rtf' original published.

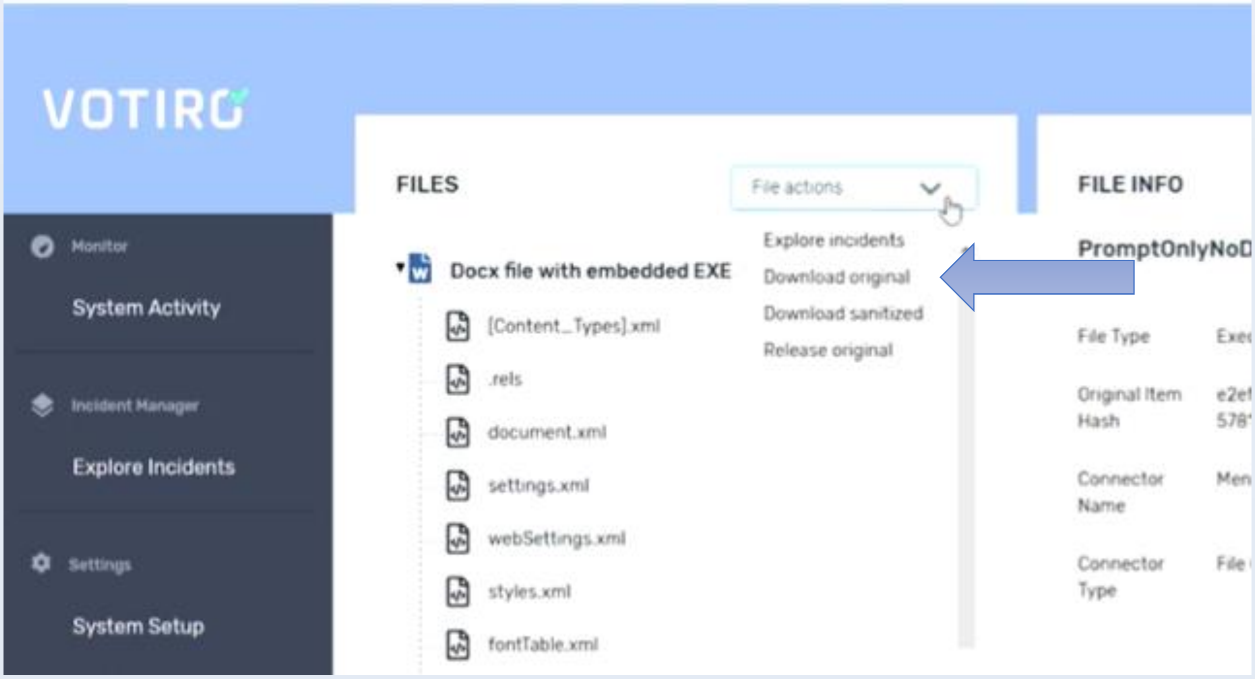
File file-sample_100kB.rtf upload for sanitization started. Item Id: eac57670-ff20-4964-b2a4-1dd89e6486a1

New child created for item eac57670-ff20-4964-b2a4-1dd89e6486a1. Child ID: 84cd13b5-eee2-4a02-b480-e34c3cbbb15a.

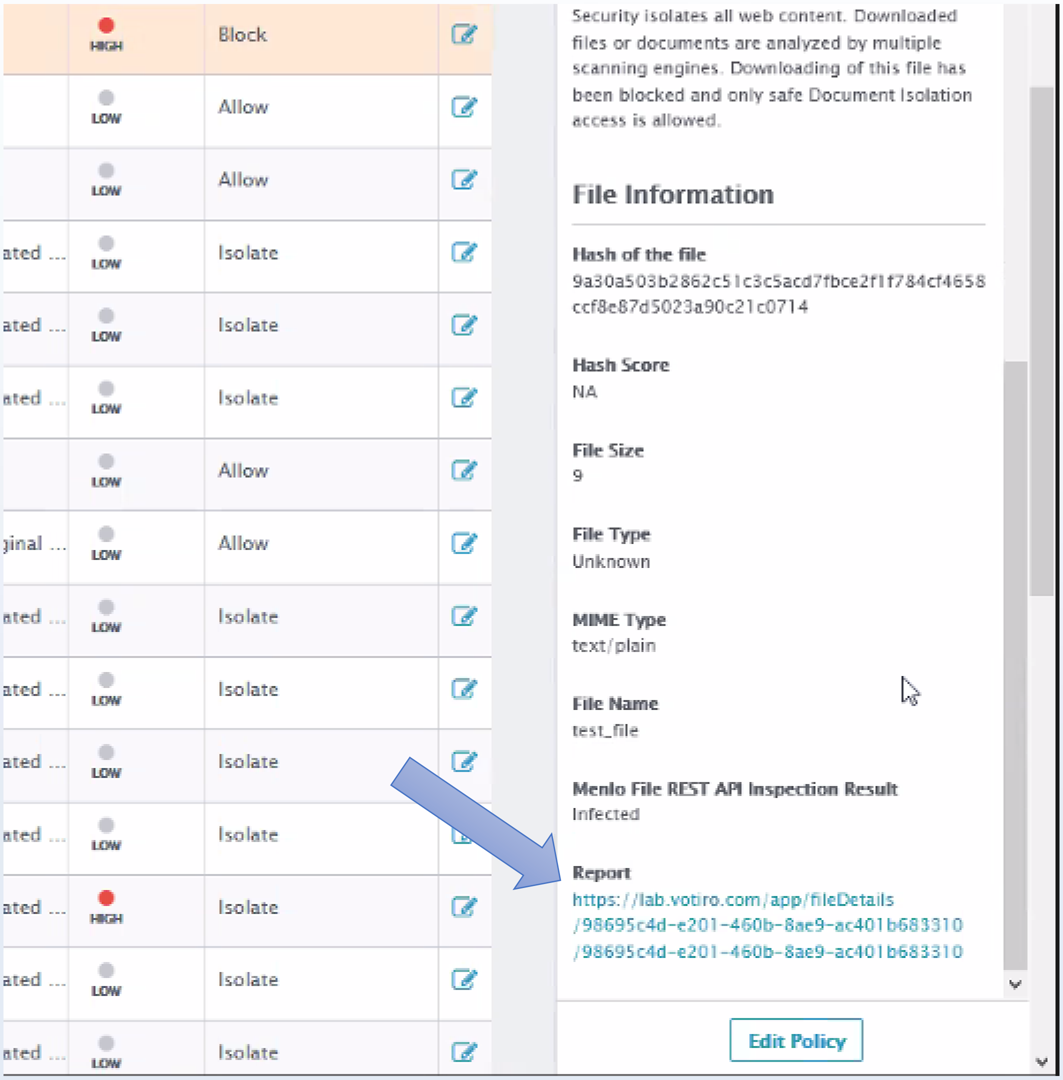
Ended: 01/28/2021 | 09:02:45 AM

122.1 sec Total Sanitization Time

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



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
9a30a503b2862c51c3c5acd7fbce2f1f784cf4658ccf8e87d5023a90c21c0714

Hash Score
NA

File Size
9

File Type
Unknown

MIME Type
text/plain

File Name
test_file

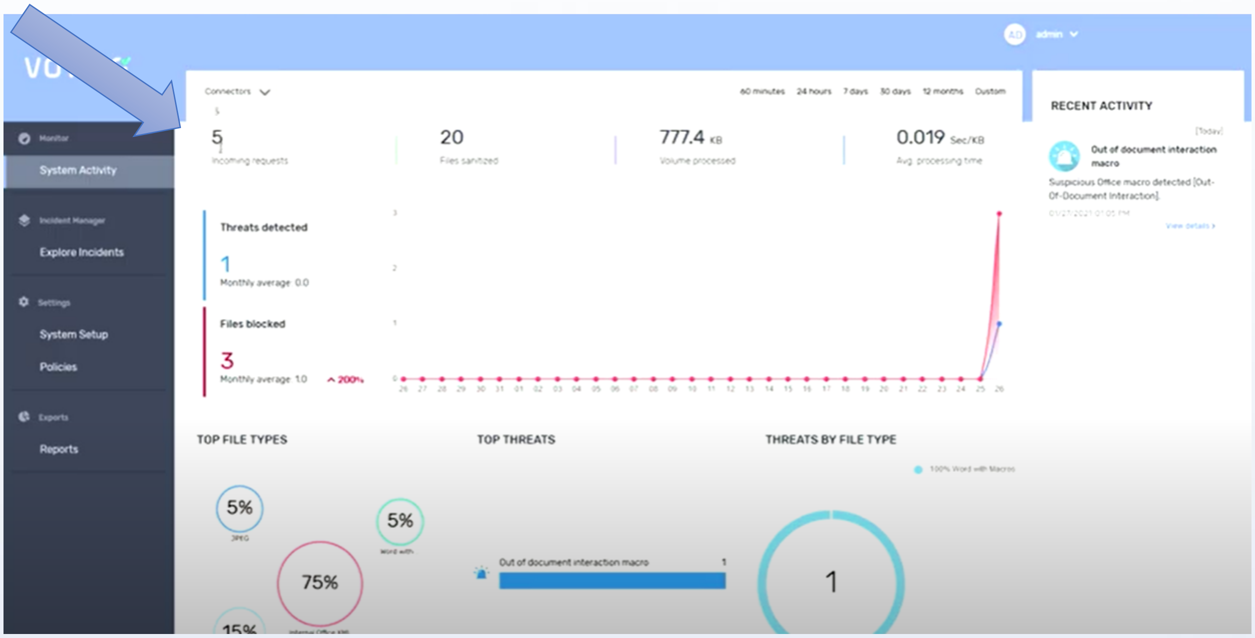
Menlo File REST API Inspection Result
Infected

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

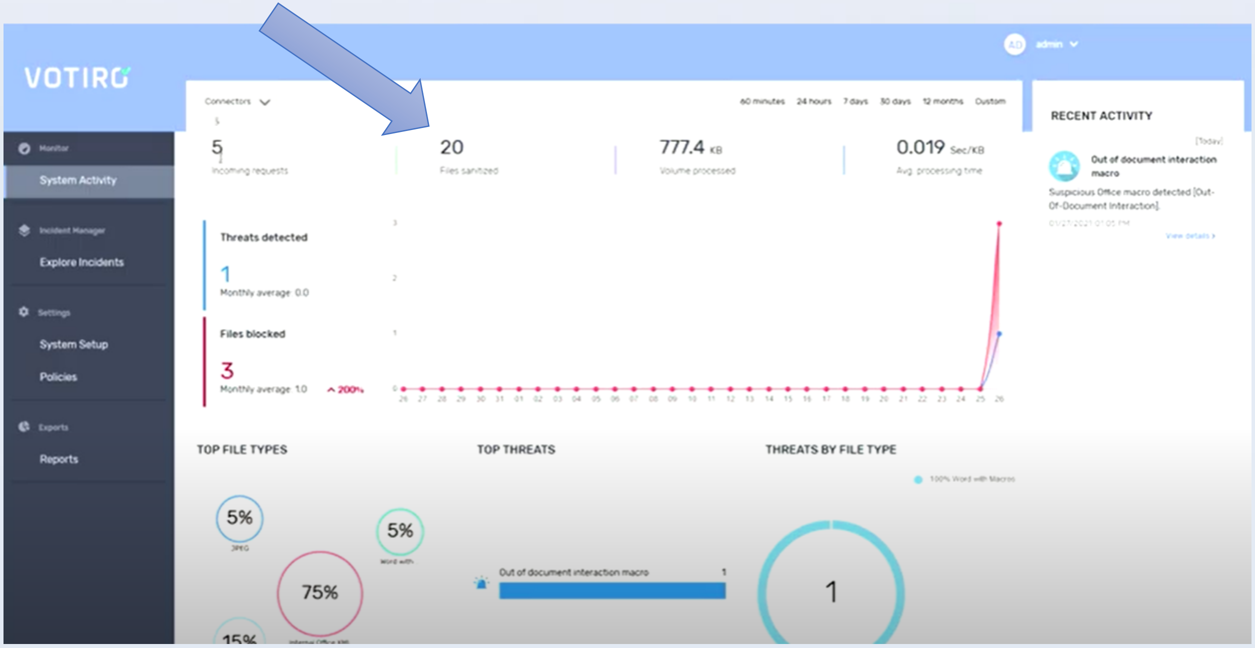
Please note: Votiro does not currently provide threat intelligence for files that were blocked, because we don't block based on threat intelligence or according to known threats. We process and sanitize every file, regardless of whether or not it contains a threat.

Votiro Dashboard Overview

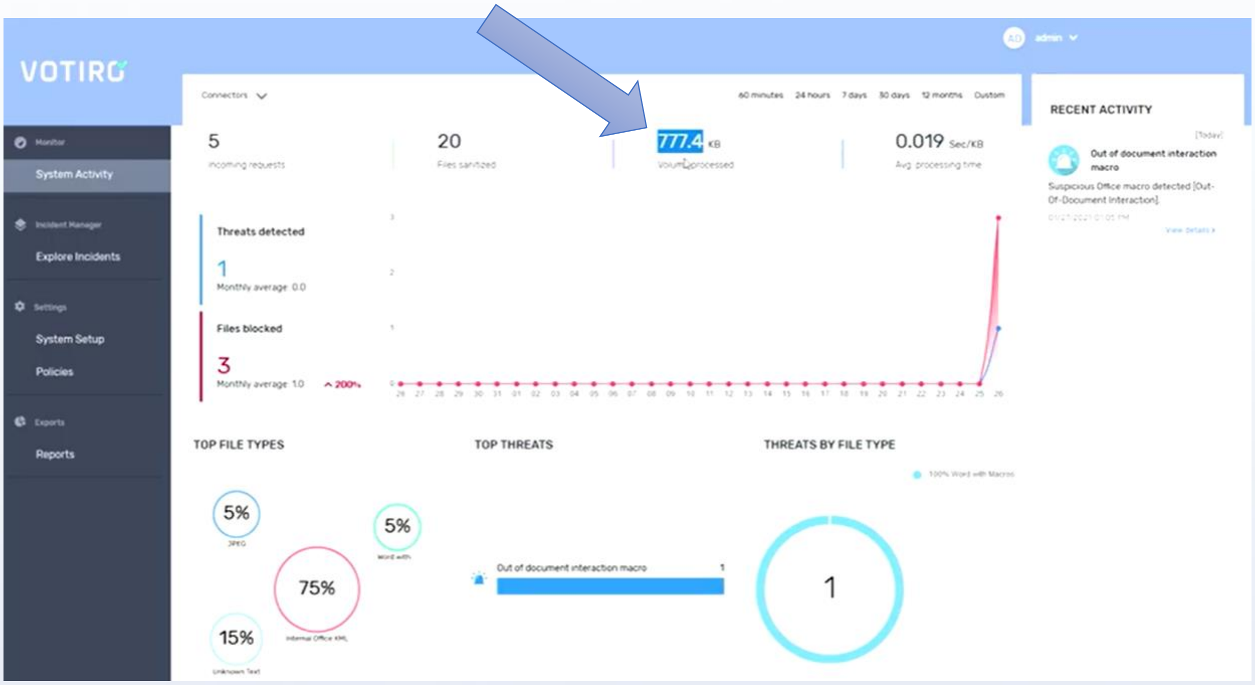
All files will flow into the Menlo UI, as shown in the previous section. Within the Votiro Dashboard, it will look similar to the below screenshot. As you see files coming through, you will see incoming requests in the upper left-hand side.



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.



5 Incoming requests

20 Files sanitized

777.4 KB Volume processed

0.019 Sec/KB Avg. processing time

Threats detected

1 Monthly average: 0.0

Files blocked

3 Monthly average: 1.0 ^ 200%

TOP FILE TYPES

5% JPEG

5% Word with

75% Internal Office XML

15% Unknown Text

TOP THREATS

Out of document interaction macro 1

THREATS BY FILE TYPE

1

RECENT ACTIVITY

[Today]

Out of document interaction macro

Suspicious Office macro detected [Out-Of-Document Interaction].

01/27/2021 01:05 PM

Questions? Contact Us

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

Votiro Support Email: support@votiro.com

Partner & MSSP Support Email: menlo@votiro.com