2.17.6 Microsoft OneDrive

> **Note**: Votiro supports scaling up to 10K files per hour.

Prerequisites

- The organization's OneDrive account is ready to use.
- The user installing has admin privileges.

Limitations

- OneDrive integration with Votiro is supported for OneDrive for Business (Enterprise) only.
- OneDrive integration with Votiro is not supported for OneDrive Personal.
- Sanitization starts one minute after uploading a file to OneDrive. The Microsoft notification for an alert resource has an average latency of less than one minute and a maximum latency of five minutes. For more information on the Microsoft latency to expect between an event happening in the service and the delivery of the change notification, see the article Latency.
- If Microsoft detects a file as malware, the Votiro engine will not be able to sanitize the file.
- OneDrive is for Individual use – Users & Group. When protecting a group, all group members are protected. The OneDrive sanitization is applied on the user's “My Files” documents library.
- Quick Access is a replicate of SharePoint sites. This is related to SharePoint protected sites.

Votiro Sanitization Disclaimer for OneDrive with Sync Clients

Votiro's OneDrive integration is designed to proactively sanitize files as they are uploaded, using advanced Content Disarm and Reconstruction (CDR) and Data Detection & Redaction (DDR) technologies. As part of this process, files may be **blocked/masked** from completing upload or distribution if:

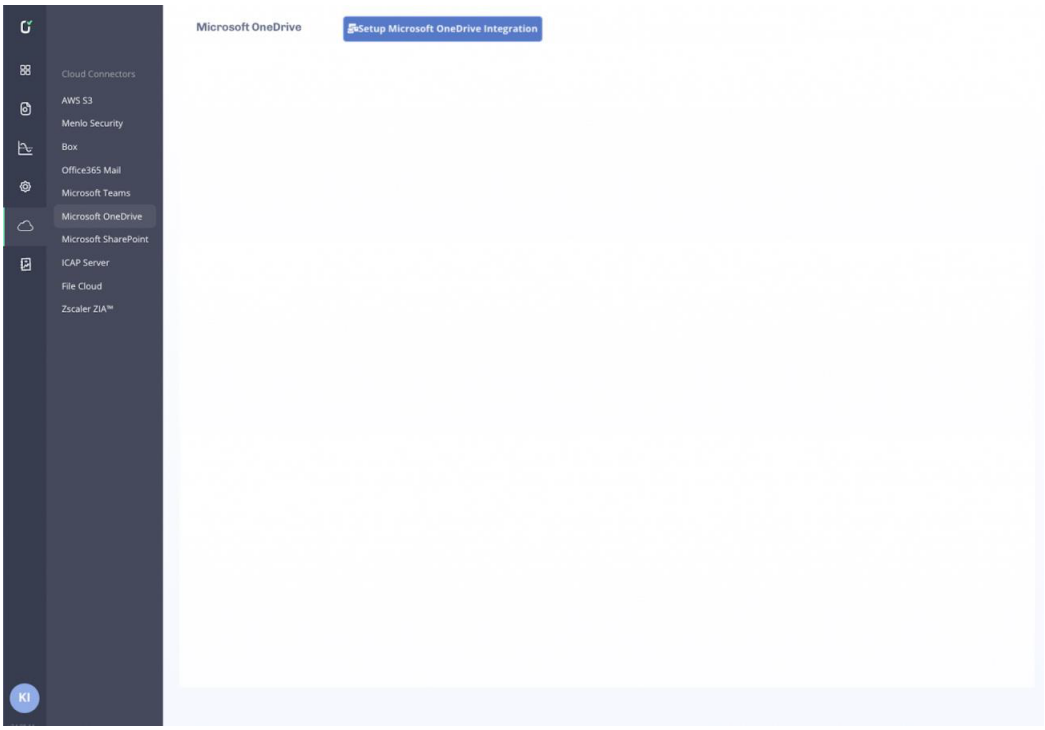
- A threat is detected based on known malware signatures or malicious behaviors
- The file type is unsupported or cannot be confidently sanitized
- A customer-defined policy (e.g., unrecognized extensions or sensitive content) instructs the system to block it

When using Microsoft OneDrive in conjunction with local sync folders (OneDrive Sync Client), end users may experience blocked file uploads or synchronization delays. This occurs when a file placed in a synced folder is intercepted and blocked by Votiro’s sanitization engine due to the reasons outlined above.

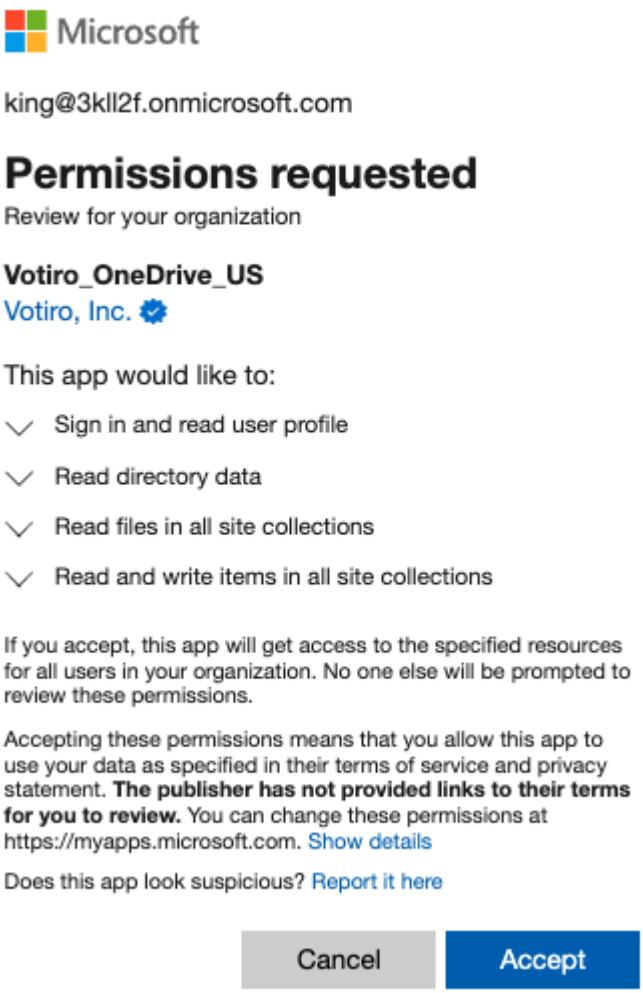
> **CAUTION!** Blocked files may appear to the end user as unsynced, missing, or failed uploads in their local OneDrive folder. This is expected behavior designed to prevent unsafe or non-compliant files from reaching the organization's cloud storage.
>
> We recommend informing end users of this protection mechanism and advising them to contact IT or Security teams if they encounter persistent sync issues that may be related to Votiro policy enforcement.

Microsoft OneDrive Configuration for Integration with Votiro

1. Enter the Votiro Management Console.
2. Navigate to **Cloud Connectors** > **Microsoft OneDrive** through the left pane.
3. Click on **Setup Microsoft OneDrive Integration**.



4. Select a user with admin permissions and **Accept** the Votiro App permissions.



5. After accepting the permissions, the user will be redirected to Votiro OneDrive configuration. After the setup completes, the **Azure Tenant ID** is displayed.

Configuration of OneDrive in the Votiro Management Dashboard

Our OneDrive integration provides two options:

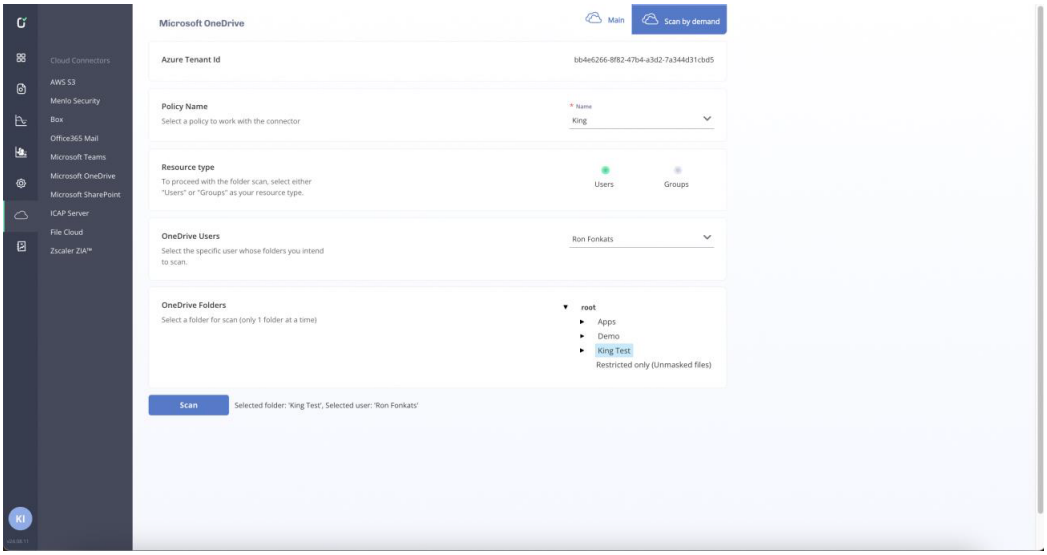
- Scan on demand
- Dynamic scanning

Scan on demand

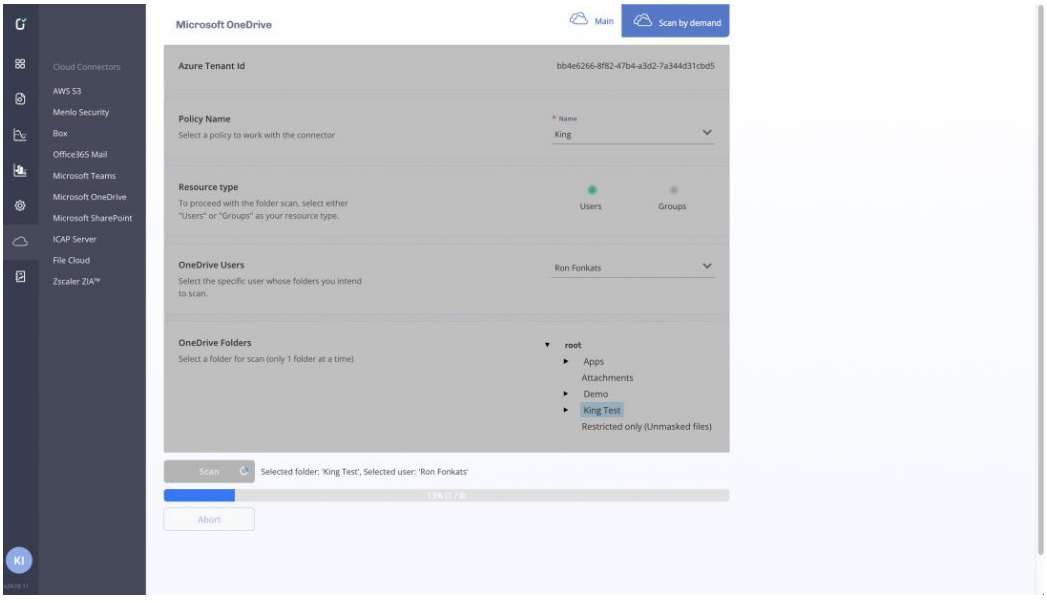
Our product provides the option to scan data at rest. The customer is able to choose specific OneDrive folders to scan.

To perform the scan:

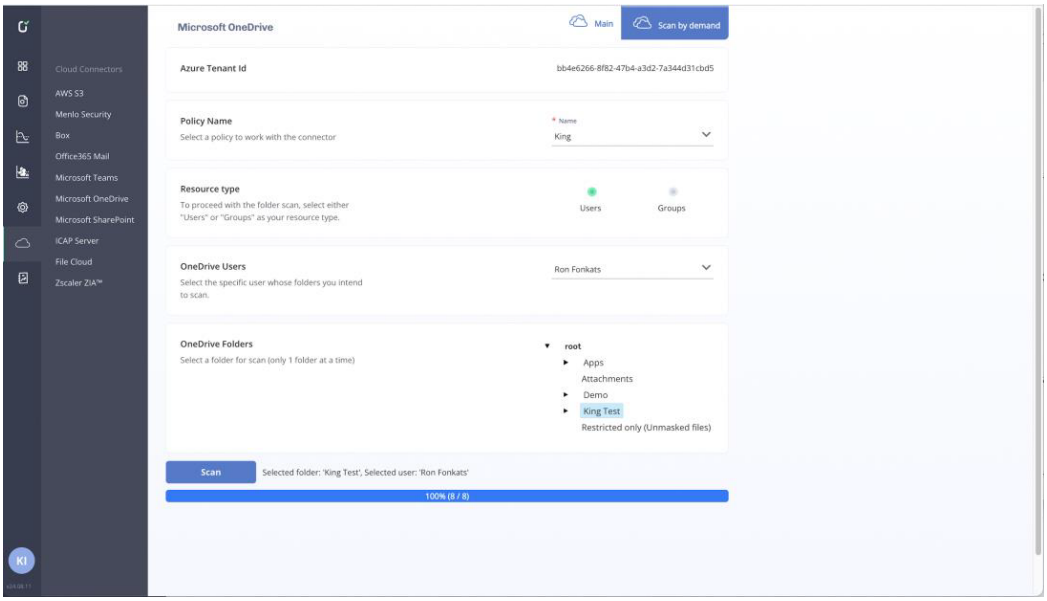
1. Choose a **Policy Name** - this will be displayed inside the Sanitized File Info.
2. Choose a **Resource type** - **Users** or **Groups**.
3. Select the **OneDrive Users** or **OneDrive Groups**.
4. Select the **OneDrive Folders** to scan.
5. Click on **Scan**.



6. All selected files will then be sent to the sanitization process, and our product will then begin to analyze the selected files. A progress bar indicates the percentage of the files completed. To halt the scan, press the **Abort** button.



7. After sanitization is completed for all the files, the progress bar will reach 100%.



Limitations

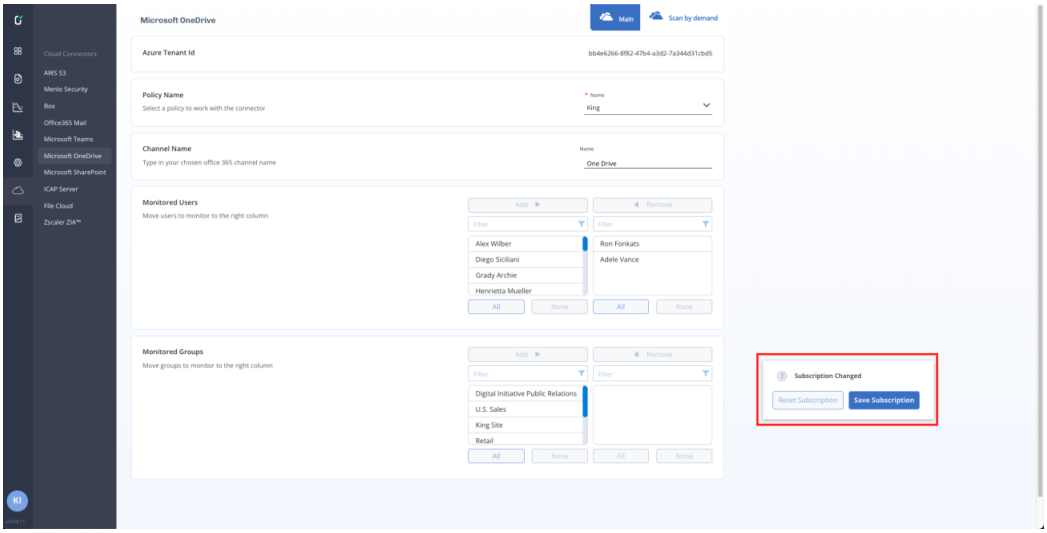
When running a scan on demand, the sanitization performance will depend on the system load. During peak usage, the sanitization could be slower.

Dynamic scanning

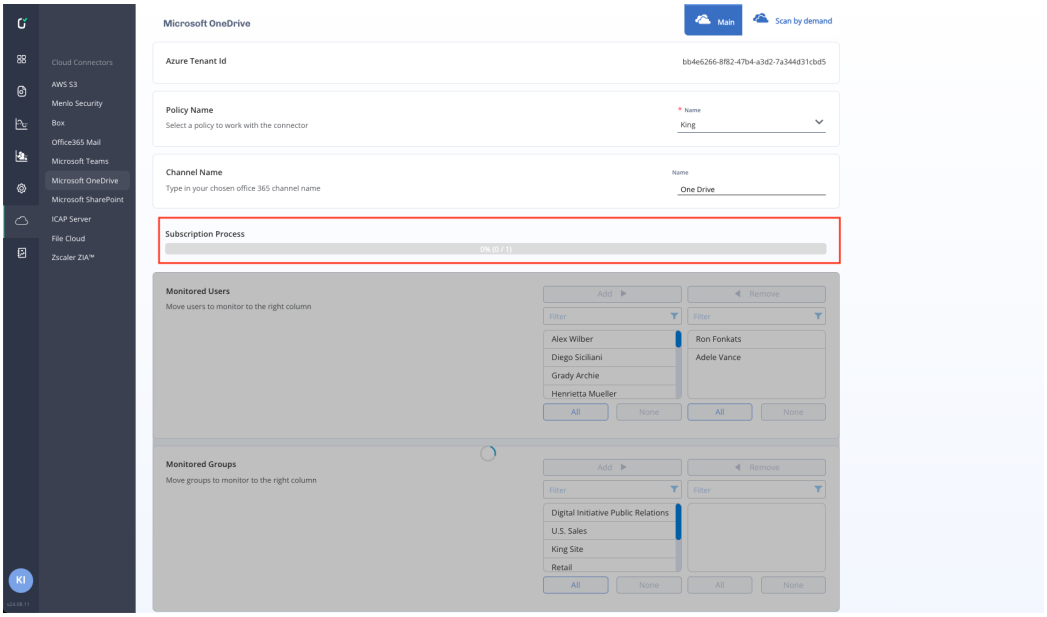
To activate dynamic scanning, on the Microsoft OneDrive Votiro Management Console, enter the following fields:

1. **Policy Name** - Specify a policy for the OneDrive connector to work with. This will be displayed inside the Sanitized File Info.
2. **Channel Name** - Specify the name of your channel. The channel name appears on the Events page as the name of a channel.
   - There will be an option to filter events with this channel name.
   - There will be an option to filter reports with this channel name.
3. **Monitored Users** - Select the users to be protected by Votiro. Select users and click on the **Add** button. The selected users will move to the right column. When each one of the monitored users uploads a file to OneDrive, the file will be sanitized.
4. **Monitored Groups** - Select groups and click on the **Add** button. The selected users will move to the right column. When any user in the monitored groups uploads a file to OneDrive, the file will be sanitized.

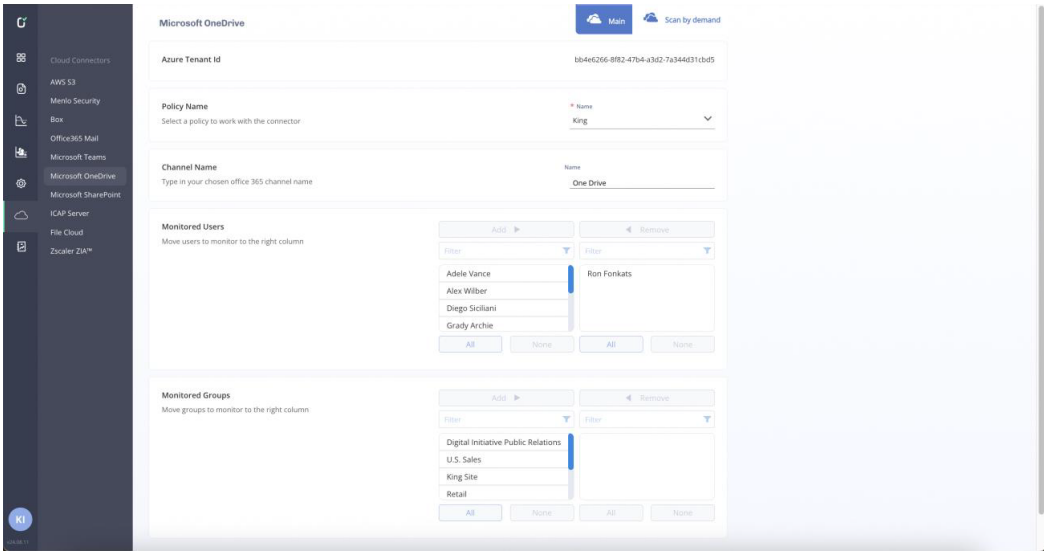
When adding/removing users/groups, there will be a **Subscription Changed** notification.



After confirming the subscription change, the subscription process will start.

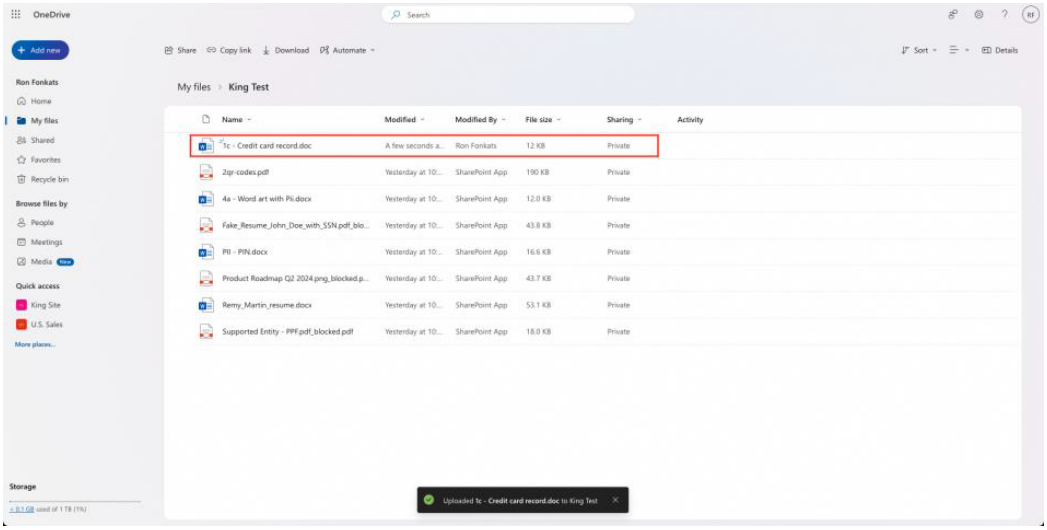


After the subscription process completes, the updated users/groups list will be displayed.



OneDrive behavior when using the Votiro OneDrive App

1. When a protected user uploads a file to OneDrive, there will be an indication that the file was uploaded.

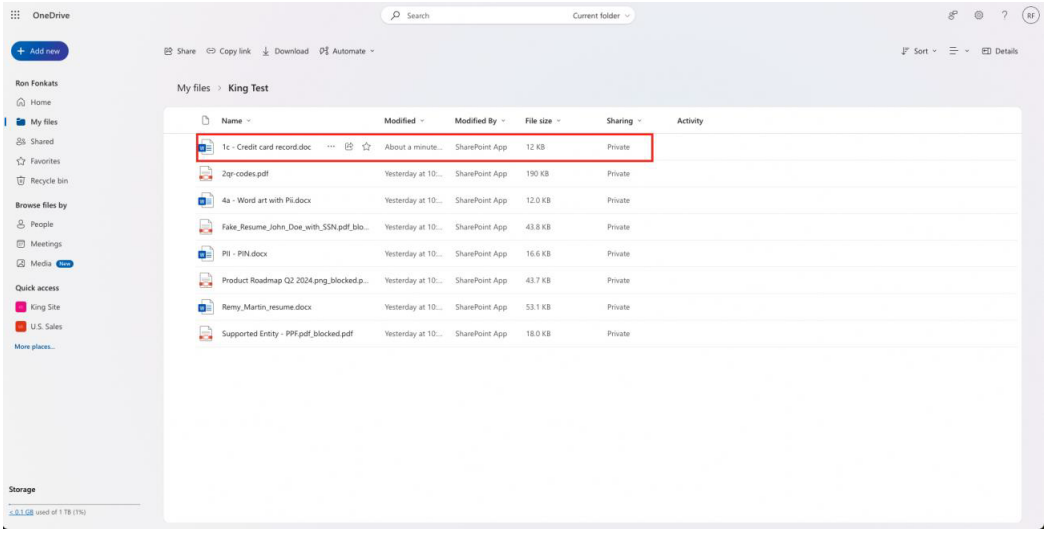


2. Votiro App will detect that there is a new file uploaded.
3. Votiro App will send the file to sanitization.

> **Note**
> It may take up to one minute before the file is sent to sanitization (this is a Microsoft limitation).

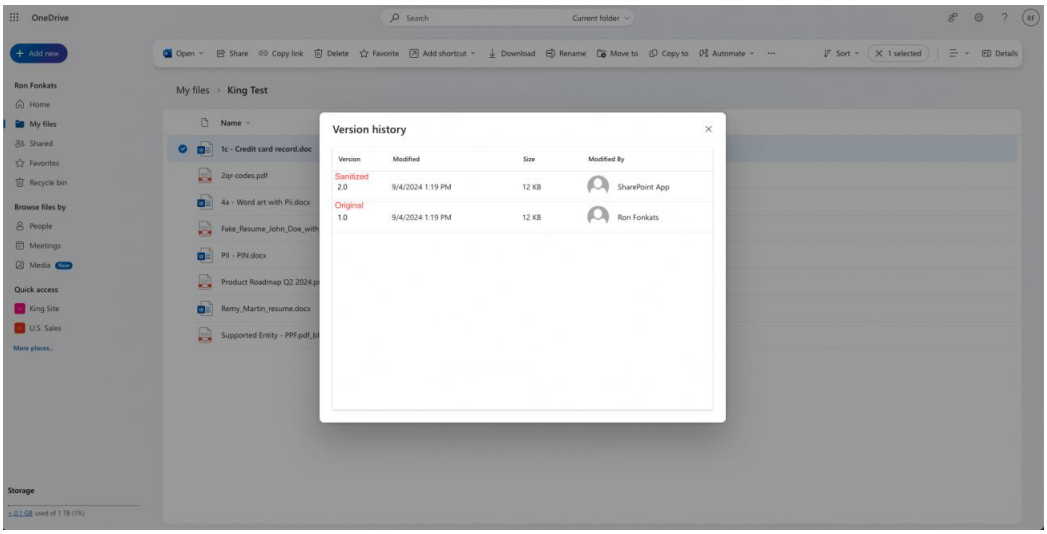
4. The file will be scanned for suspicious activity/Privacy risks.
5. The Votiro engine will remediate any suspicious activity/Privacy risk (according to Policy).

6. When the sanitization completes, the sanitized file will be replaced in the OneDrive folder.



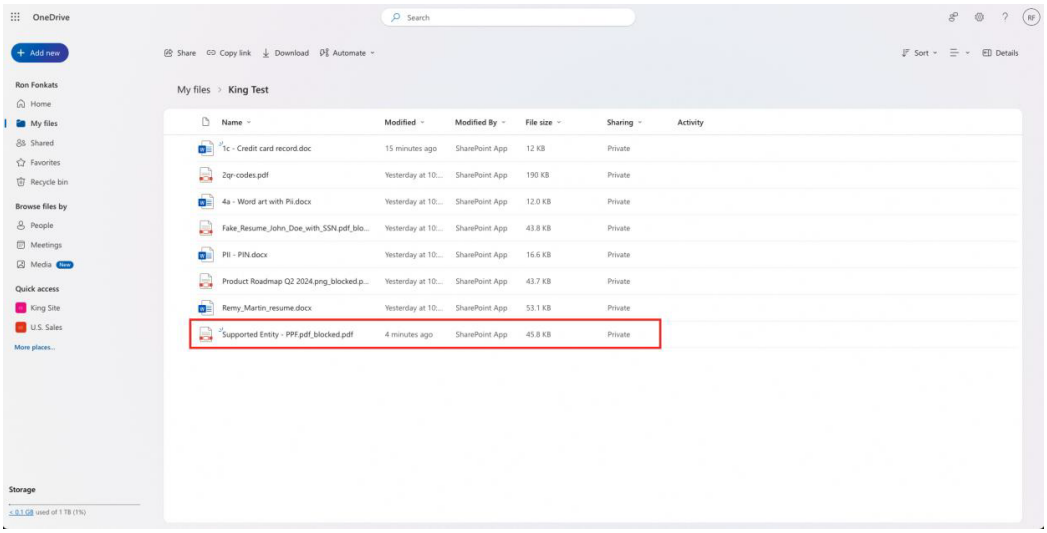
How to check if the file is the sanitized version

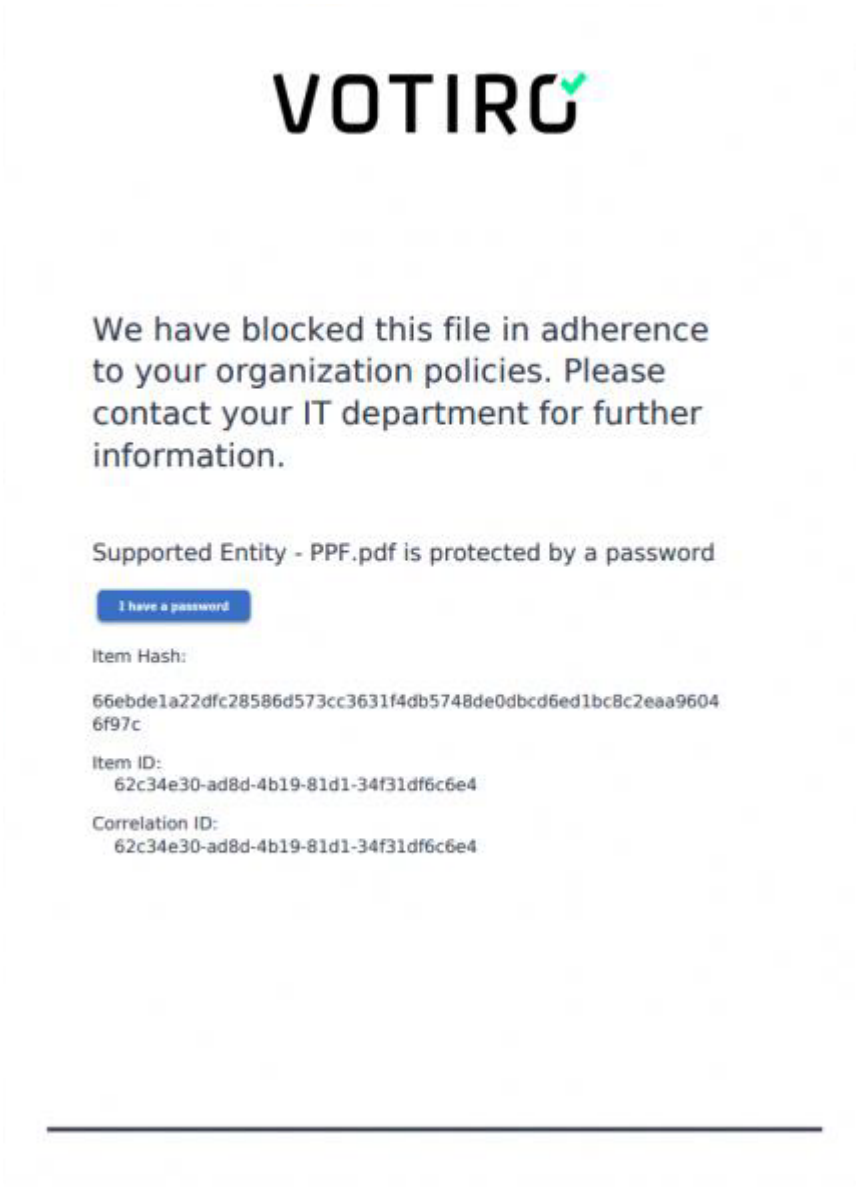
There will be a modification indicator. The sanitized file will be displayed as **Modified By SharePoint App**. You can see this indication in the main view **Version history** window.



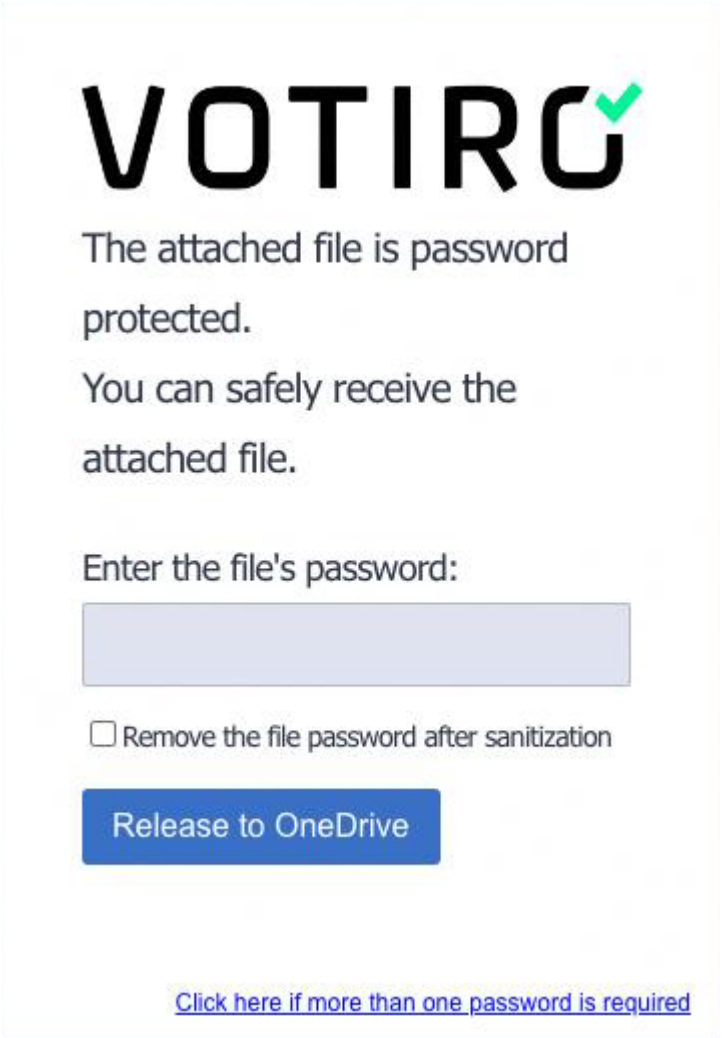
OneDrive behavior with Password Protected Files

1. The protected user uploads password-protected files to OneDrive.
2. The files will be sent to sanitization.
3. The sanitized files will be blocked PDF files with instructions on how to release the files.


OneDrive
Search
Add new
Share
Copy link
Download
Automate
Sort
Details
Ron Fonkats
Home
My files
Shared
Favorites
Recycle bin
Browse files by
People
Meetings
Media
Quick access
King Site
U.S. Sales
More places...
Storage
My files > King Test
Name
Modified
Modified By
File size
Sharing
Activity
1c - Credit card record.doc
15 minutes ago
SharePoint App
12 KB
Private
2qr-codes.pdf
Yesterday at 10...
SharePoint App
190 KB
Private
4a - Word art with Pii.docx
Yesterday at 10...
SharePoint App
12.0 KB
Private
Fake_Resume_John_Doe_with_SSN.pdf_blo...
Yesterday at 10...
SharePoint App
43.8 KB
Private
PII - PIN.docx
Yesterday at 10...
SharePoint App
16.6 KB
Private
Product Roadmap Q2 2024.png_blocked.p...
Yesterday at 10...
SharePoint App
43.7 KB
Private
Remy_Martin_resume.docx
Yesterday at 10...
SharePoint App
53.1 KB
Private
Supported Entity - PPF.pdf_blocked.pdf
4 minutes ago
SharePoint App
45.8 KB
Private

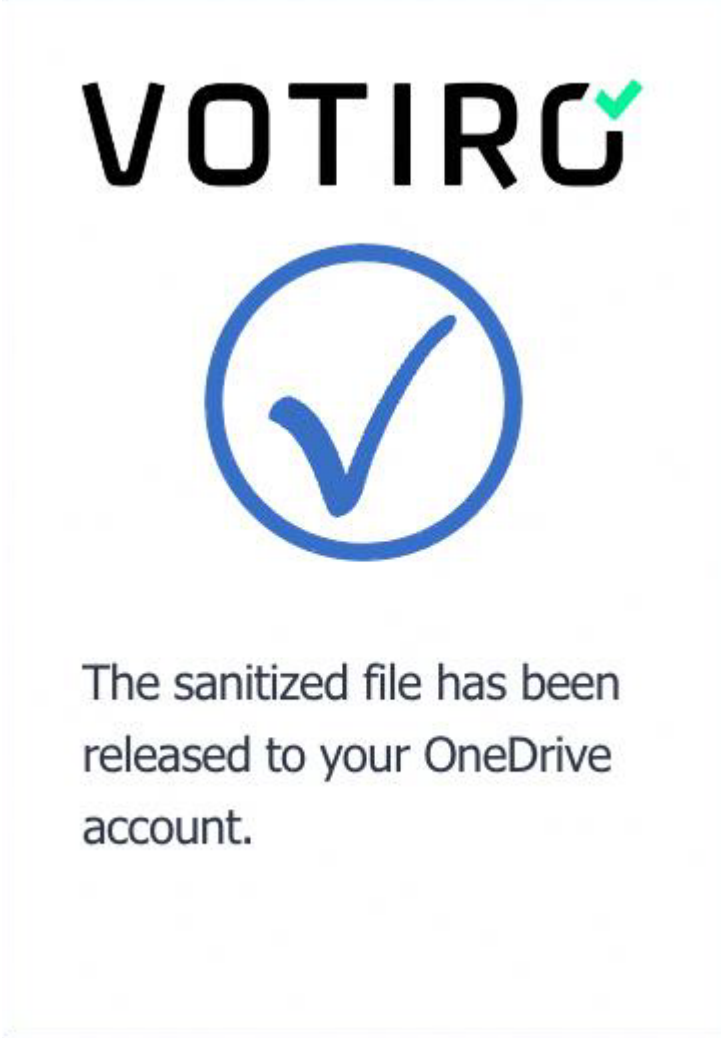

VOTIRO
We have blocked this file in adherence to your organization policies. Please contact your IT department for further information.
Supported Entity - PPF.pdf is protected by a password
I have a password
Item Hash:
66ebde1a22dfc28586d573cc3631f4db5748de0dbcd6ed1bc8c2eaa96046f97c
Item ID:
62c34e30-ad8d-4b19-81d1-34f31df6c6e4
Correlation ID:
62c34e30-ad8d-4b19-81d1-34f31df6c6e4

4. Click on **I have a password**.
5. The user will be redirected to the Votiro Portal for releasing the file.

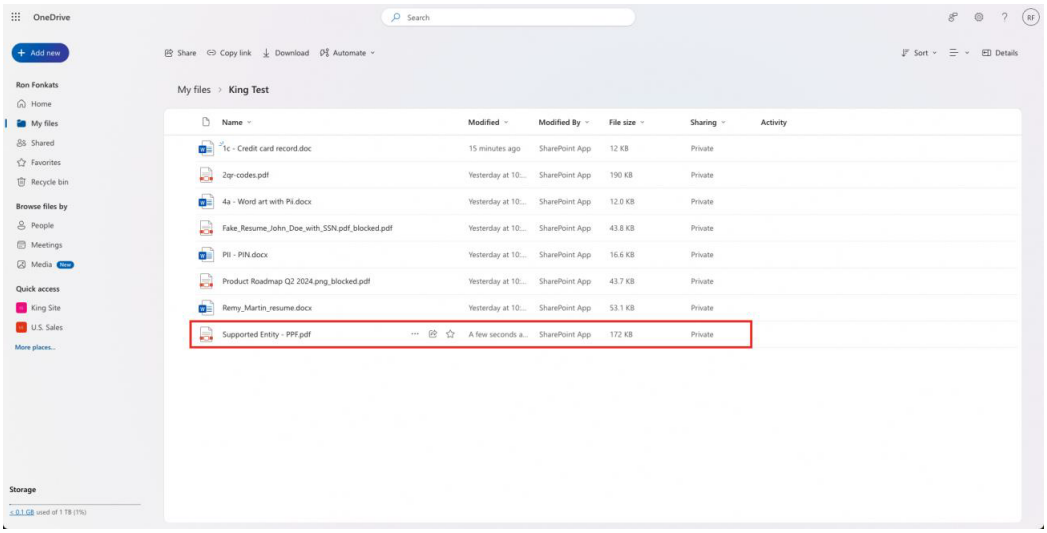


6. Enter the file's password and click on **Release to OneDrive**.
7. After executing the Release option, the file will be sent to sanitization.

8. After the sanitization completes, the sanitized file will be sent to the OneDrive folder.



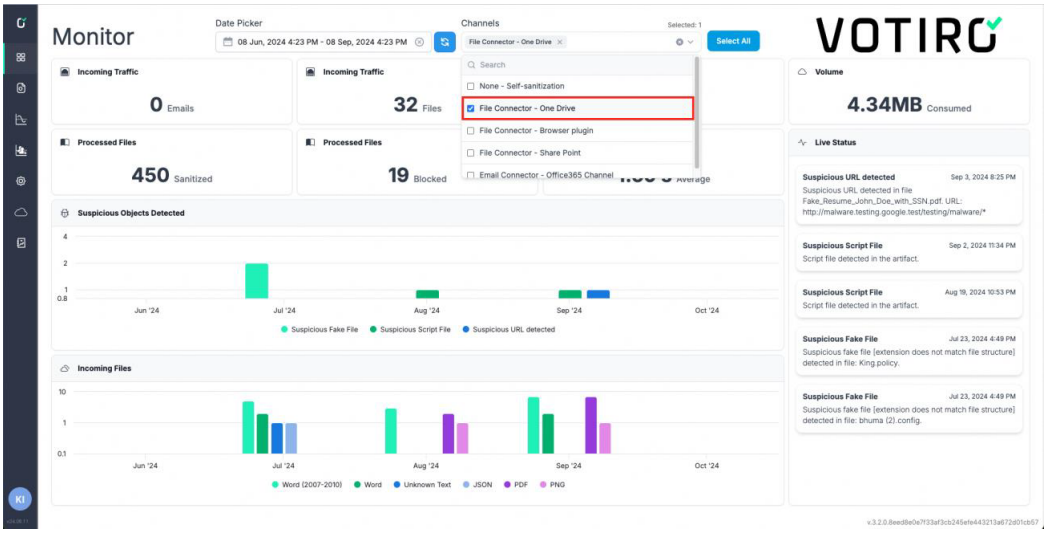
9. Navigate back to the OneDrive folder.
10. The sanitized file will be displayed.



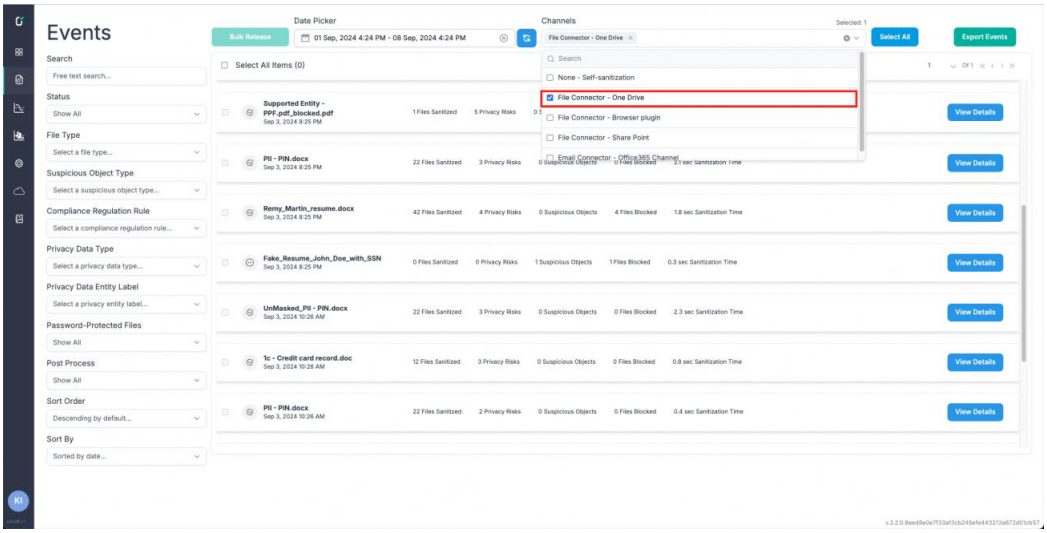
How to get insights by using the Management Dashboard

There are several ways to get insights on OneDrive uploaded files:

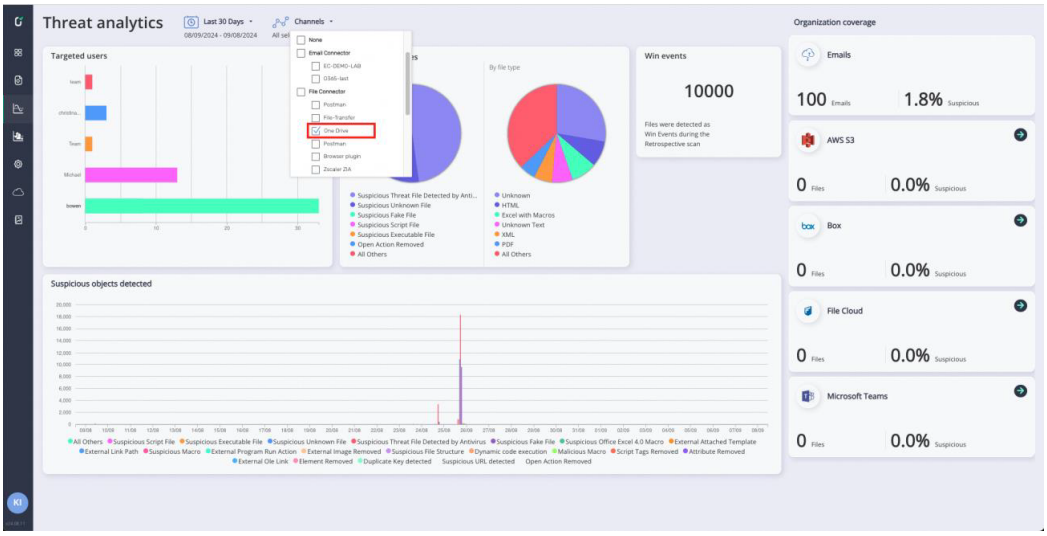
- **Monitor screen** - There is an option to see OneDrive insights by filtering the Monitor dashboard with OneDrive channel.



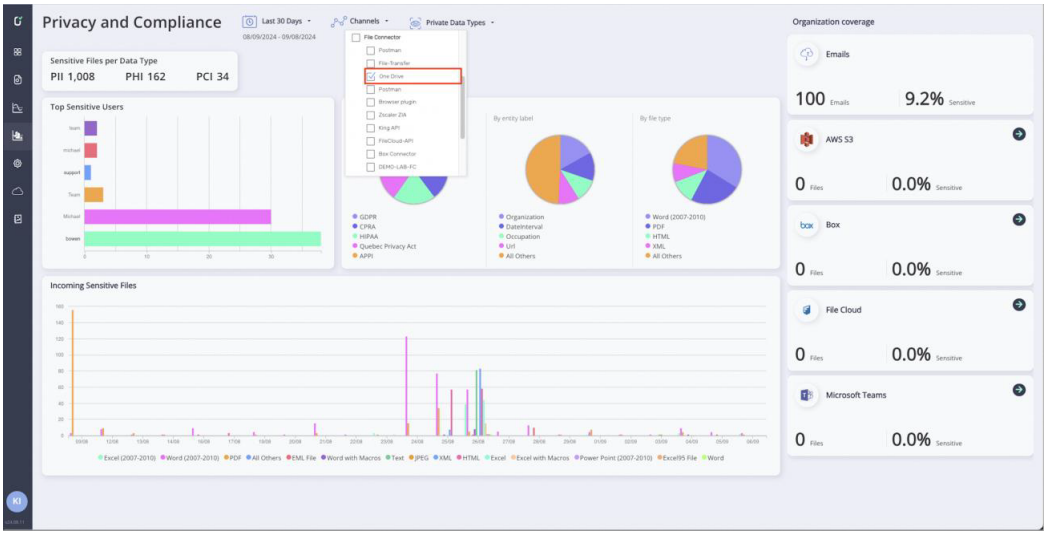
- **Events screen** - There is an option to see OneDrive events by filtering the Events list with OneDrive channel.



- **Threat Analytics Dashboard**
  - Get insights on the Threat Analytics – Top targeted users, Suspicious objects, win events and more.
  - Filter on OneDrive channel, and see all related data.



- **Privacy and Compliance Dashboard**
  - Get insights on Privacy and Compliance – Top sensitive users, Detected data per Regulation, data label, per file type
  - Filter on OneDrive channel, and see all related data.



2.17.7 Microsoft SharePoint

> **Note**: Votiro supports scaling up to 10K files per hour.

Prerequisites

- The Organization's SharePoint account is ready to use.
- The user performing the installation has admin privileges.

Votiro Sanitization Disclaimer for SharePoint with Sync Clients

Votiro's SharePoint integration is designed to proactively sanitize files as they are uploaded, using advanced Content Disarm and Reconstruction (CDR) and Data Detection & Redaction (DDR) technologies. As part of this process, files may be **blocked/masked** from completing upload or distribution if:

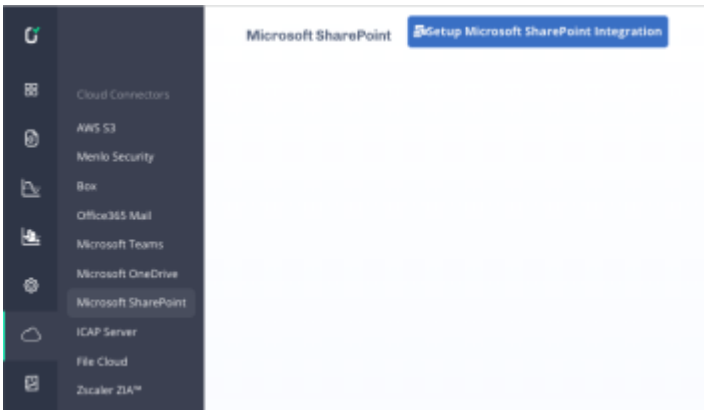
- A threat is detected based on known malware signatures or malicious behaviors
- The file type is unsupported or cannot be confidently sanitized
- A customer-defined policy (e.g., unrecognized extensions or sensitive content) instructs the system to block it

When using Microsoft SharePoint in conjunction with local sync folders (OneDrive Sync Client), end users may experience blocked file uploads or synchronization delays. This occurs when a file placed in a synced folder is intercepted and blocked by Votiro’s sanitization engine due to the reasons outlined above.

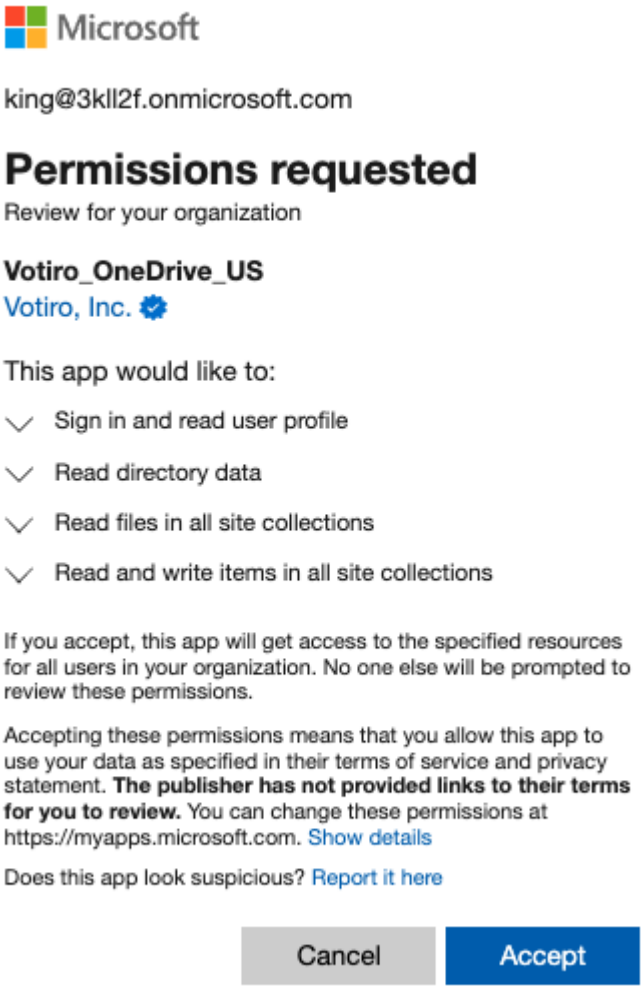
> **CAUTION!** Blocked files may appear to the end user as unsynced, missing, or failed uploads in their local OneDrive folder. This is expected behavior designed to prevent unsafe or non-compliant files from reaching the organization's cloud storage.
>
> We recommend informing end users of this protection mechanism and advising them to contact IT or Security teams if they encounter persistent sync issues that may be related to Votiro policy enforcement.

Microsoft SharePoint Configuration for Integration with Votiro

1. Enter the Votiro Management Console.
2. Navigate to **Cloud Connectors** > **Microsoft SharePoint**.
3. Click on **Setup Microsoft SharePoint Integration**.



4. Select a user with admin permissions and click on **Accept** in the **Permissions Requested** window.



5. After accepting the permissions, the user will be redirected to the Votiro SharePoint configuration. After the subscription completes, the Azure Tenant ID is displayed.

Configuration of Microsoft SharePoint Scan in the Votiro Management Dashboard

The Votiro SharePoint integration currently supports Scan on Demand only.

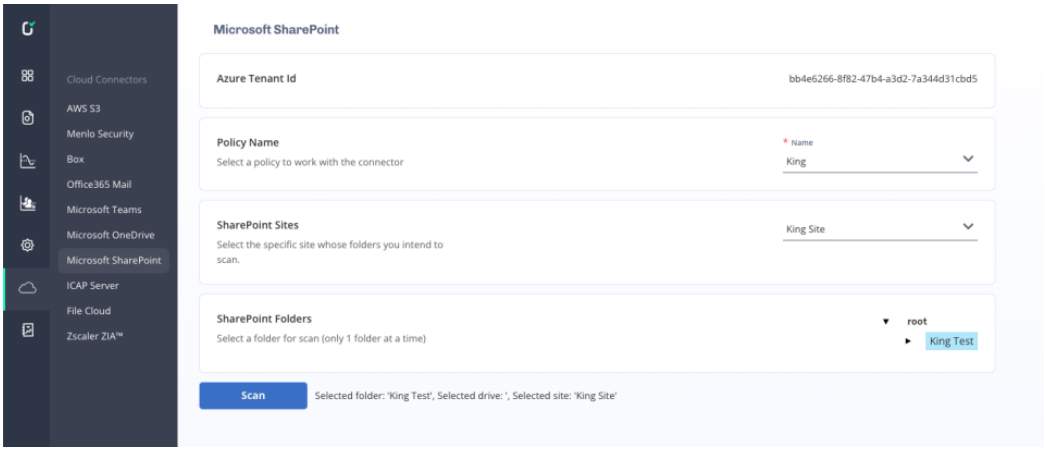
Scan on Demand

Our product provides the option to scan data at rest. The customer is able to choose specific SharePoint sites and select specific folders to scan.

To perform the scan, open the SharePoint screen in the Votiro Management dashboard:

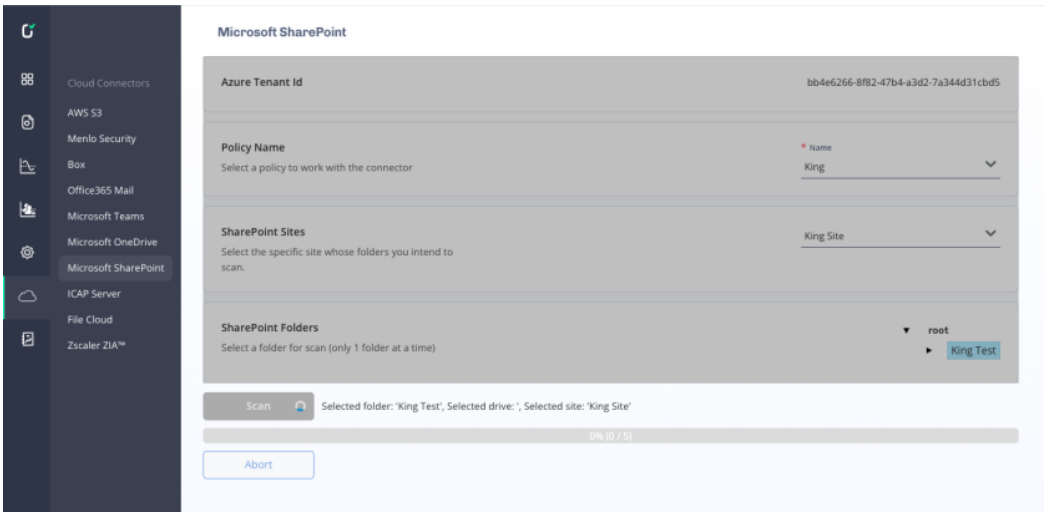
1. Select a **Policy Name**. This is the policy to work with the SharePoint connector. This will be displayed inside the Sanitized File Info.
2. Select the **SharePoint Site**. This site contains the folders to be scanned.

3. Select the **SharePoint Folder** to scan. Only one folder at a time can be scanned.
4. Press the **Scan** button to execute the scan.

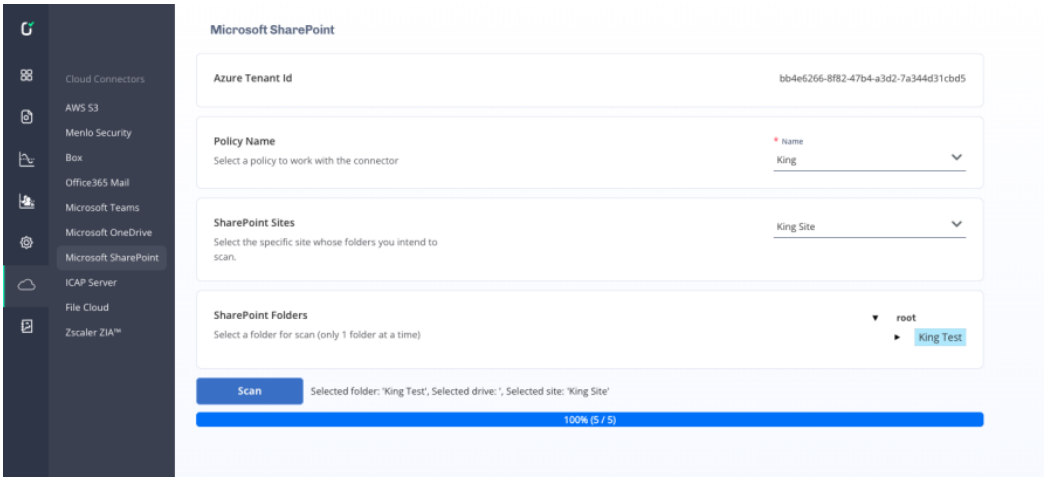


After initiating the scan:

1. Votiro will analyze the existing files.
2. All files will be sent to the sanitization process.
3. A progress bar will indicate the percentage completed.
4. The user can stop the scan by clicking on the **Abort** button.



5. After sanitization is completed for all files, the progress bar will display 100%.

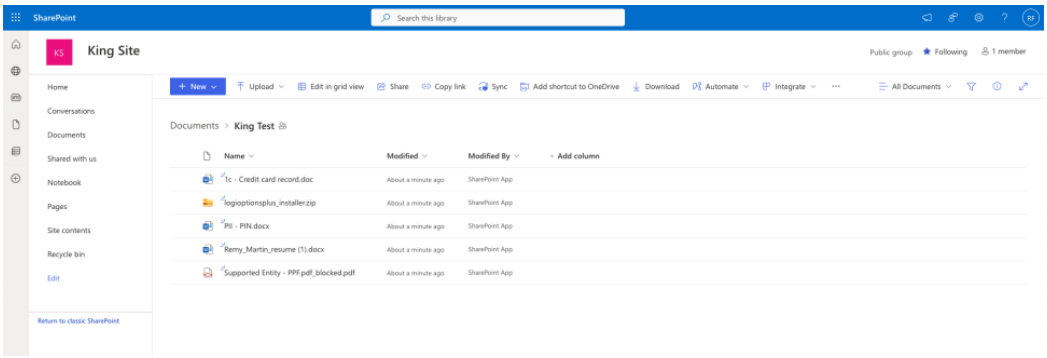


Limitations

When running a scan on demand, the sanitization performance will depend on the system load. During peak usage, the sanitization could be slower.

SharePoint behavior when using the Votiro SharePoint App

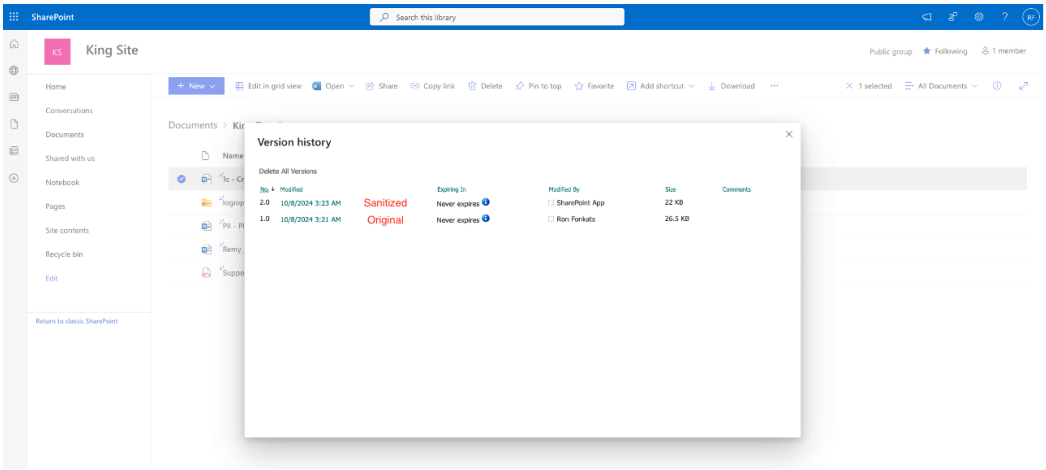
- When executing SharePoint scan on demand, all files will be sent to Votiro for sanitization.
- The files will be scanned for suspicious activity and privacy risks.
- The Votiro engine will remediate any suspicious activity and privacy risk (according to the selected Policy).
- When the sanitization completes, the sanitized file will be replaced in the SharePoint folder.



How to check if the file is the sanitized version

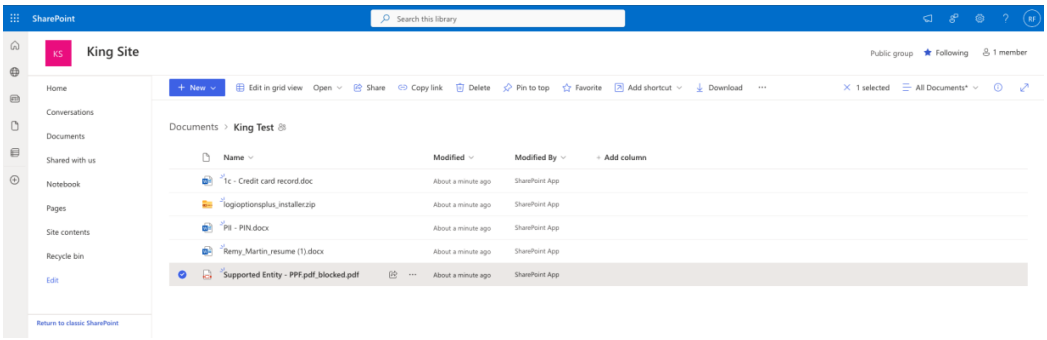
There will be an indication if the file was modified in the **Version history**:

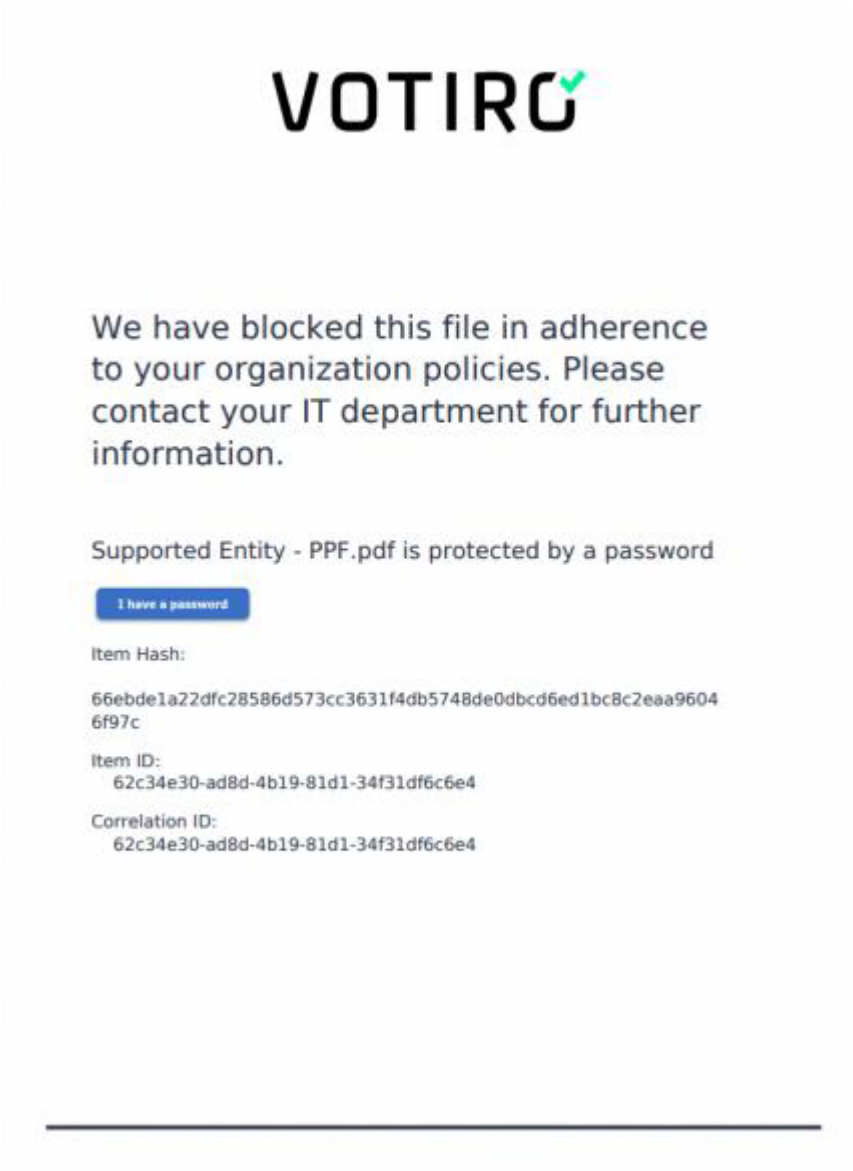
- The file will be marked **Sanitized** next to the modification date-time.
- The **Modified By** column will display **SharePoint App**.


SharePoint
Search this library
King Site
Public group
Following
1 member
Home
Conversations
Documents
Shared with us
Notebook
Pages
Site contents
Recycle bin
Edit
Return to classic SharePoint
New
Edit in grid view
Open
Share
Copy link
Delete
Pin to top
Favorite
Add shortcut
Download
1 selected
All Documents
Documents
Version history
Delete All Versions
No.
Modified
Expiring In
Modified By
Size
Comments
2.0
10/8/2024 3:23 AM
Sanitized
Never expires
SharePoint App
22 KB
1.0
10/8/2024 3:21 AM
Original
Never expires
Ron Fonkats
26.5 KB

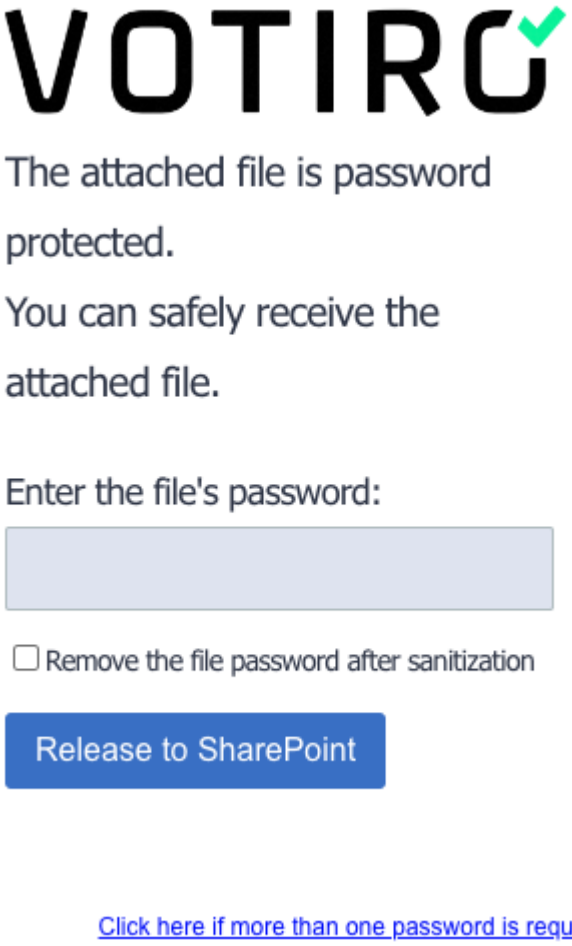
SharePoint behavior with Password Protected Files

1. A sanitized file that is a blocked PDF file contains instructions on how to release the file.

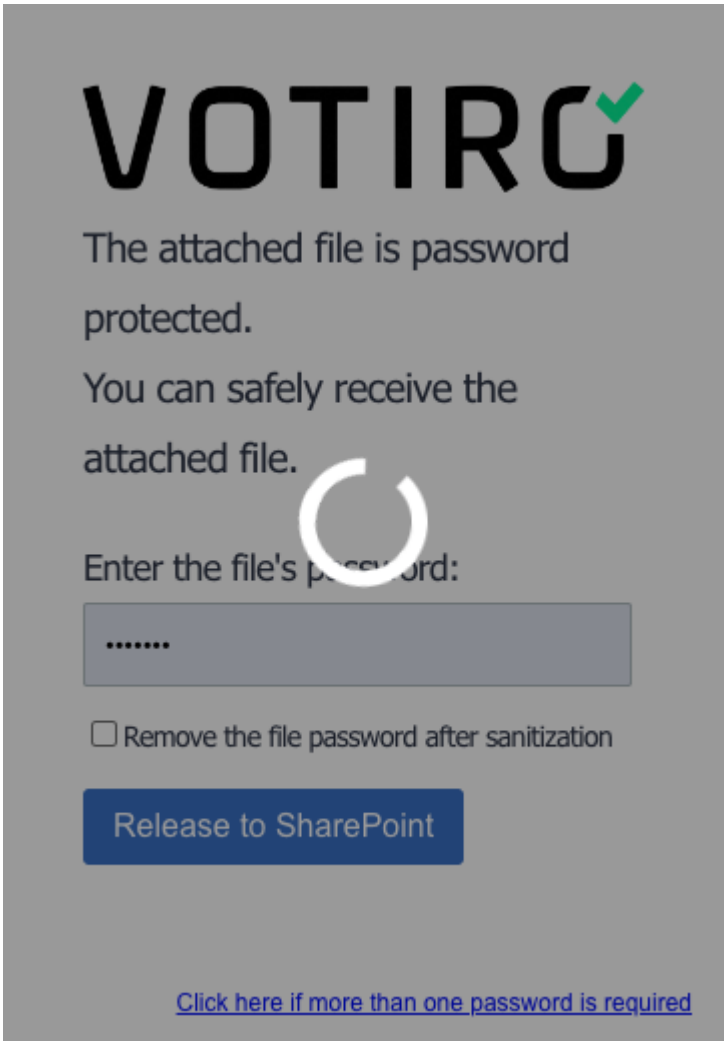




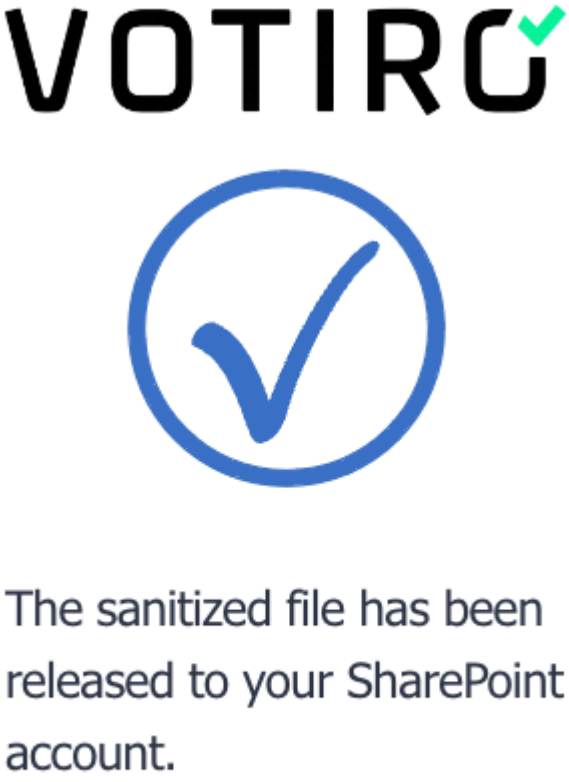
2. Click on **I have a password**".
3. The user will be redirected to the Votiro Portal to release the file.



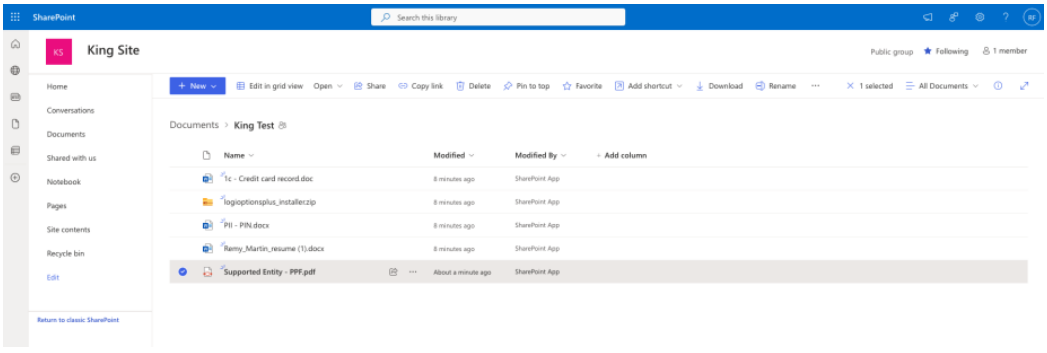
4. Enter the correct password and click on **Release to SharePoint**.
5. After executing the Release option, the file will be sent to sanitization.



6. After the sanitization completes, the sanitized file will be sent to the SharePoint folder.



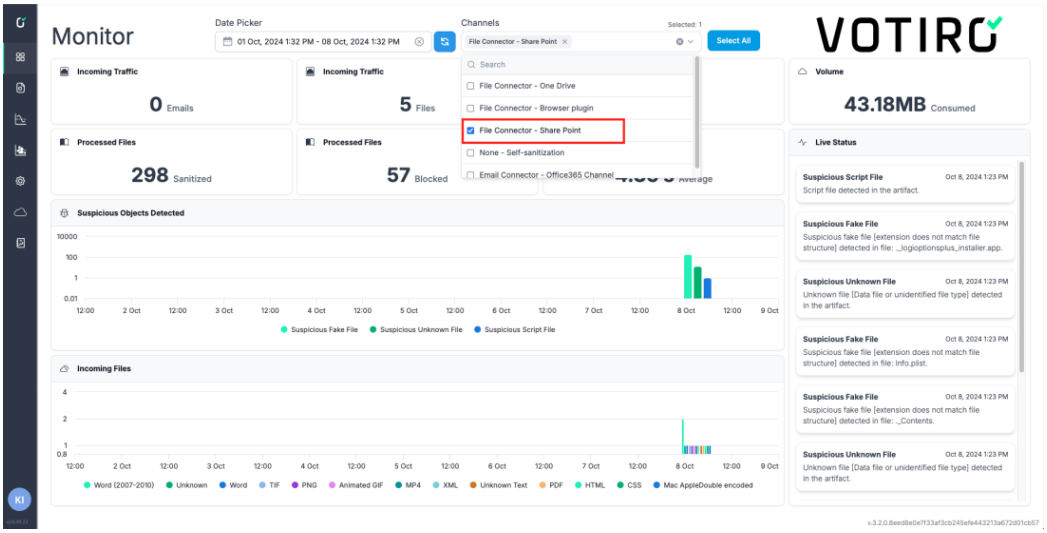
7. Navigate back to the SharePoint folder. The sanitized file will be displayed.



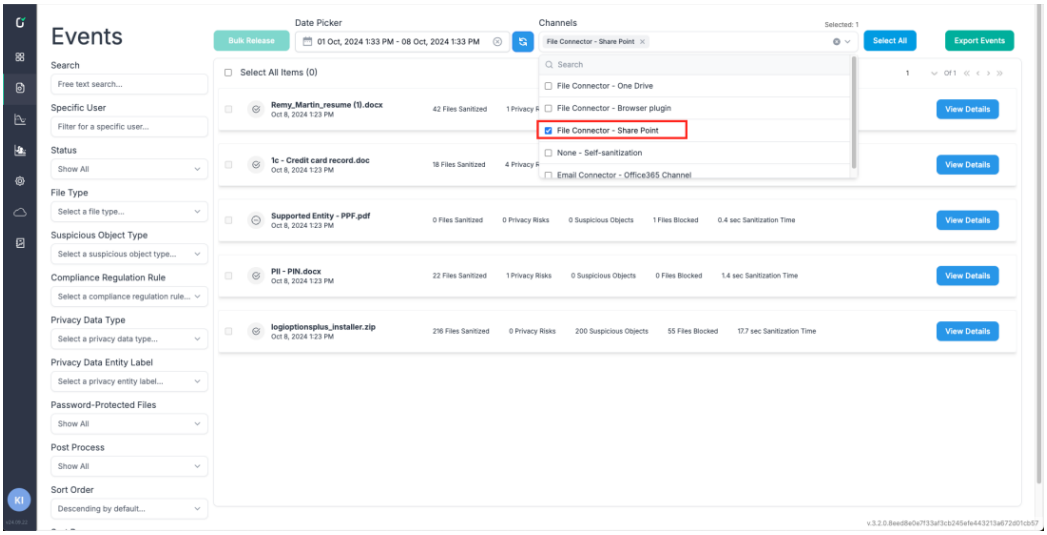
How to get insights using the Management Dashboard

There are several ways to get insights on SharePoint sanitized files.

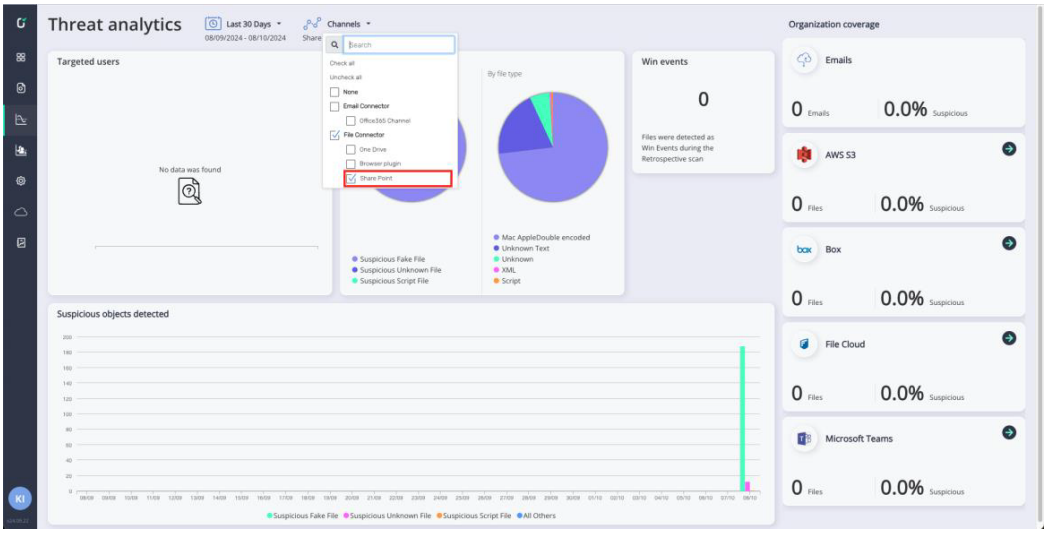
- Monitor screen - there is an option to see SharePoint insights by filtering the Monitor dashboard by SharePoint channel.



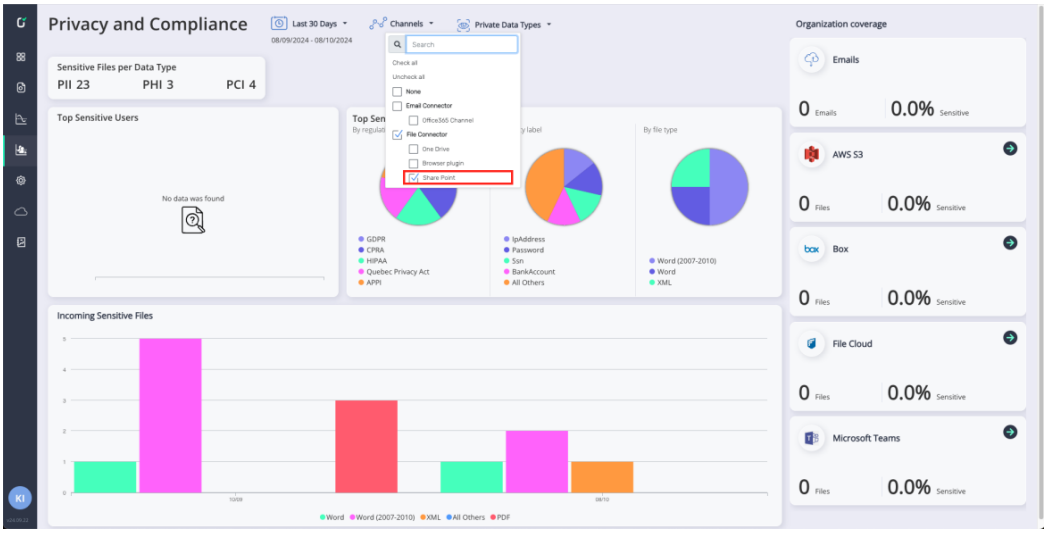
- Events screen - there is an option to see SharePoint events by filtering the Events list by SharePoint channel.



- Threat Analytics Dashboard - get insights on the Threat Analytics, including suspicious objects, win events and more. Filter by SharePoint channel, and see all related data.



- Privacy and Compliance Dashboard - get insights on the Privacy and Compliance, including detected data per Regulation, data label, per file type. Filter by SharePoint channel, and see all related data.



Limitations

- Sanitization is supported in the root document library only (the Documents folder). Other document library folders are not supported.
- If Microsoft detects a file as malware, the Votiro engine will not be able to sanitize the file.

2.17.8 ICAP Connector

Introduction

Some organizations use a reverse proxy server like F5 for security purposes.

It is situated outside the organizational network in a Demilitarized Zone (DMZ). Public requests are directed to this server, which forwards them to their final destination based on its configurations and organizational policies.

ICAP (Internet Content Adaptation Protocol) is a protocol used for content analysis and content filtering.

It can also be employed for inserting advertisements, virus scanning, content translation, or language translation. ICAP reads the HTTP headers of incoming HTTP requests and processes these requests according to established rules.

As a result, integrating Proxy and ICAP offers a powerful combination that provides significant business value and a comprehensive solution.

Votiro now supports the integration of ICAP by receiving ICAP requests, forwarding them for sanitization, and routing them back to the Votiro ICAP-F5 server so they can reach the final destination.

Limitations

The following limitations apply to ICAP connector-supported products:

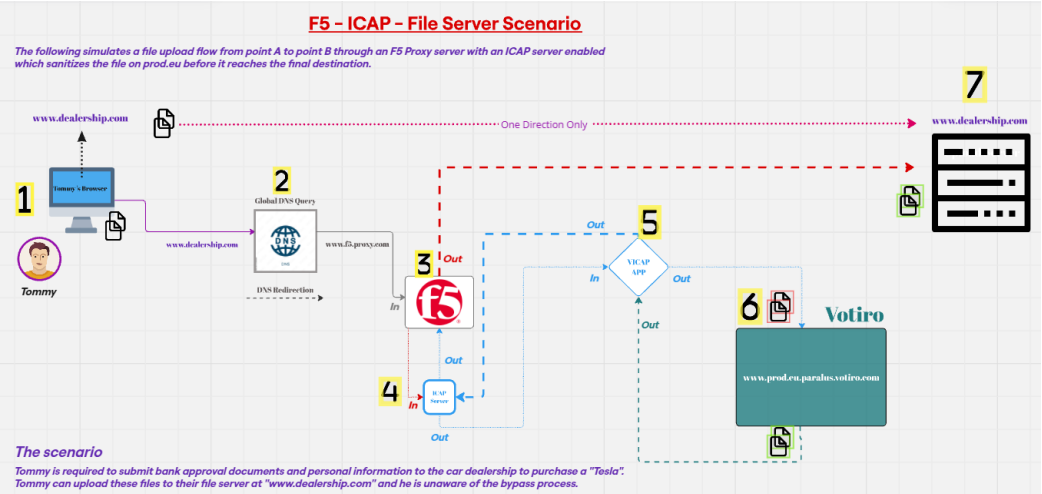
- F5 - Only uploads are supported.
- Squid - Both uploads and downloads are supported.

Workflow inside the F5 server

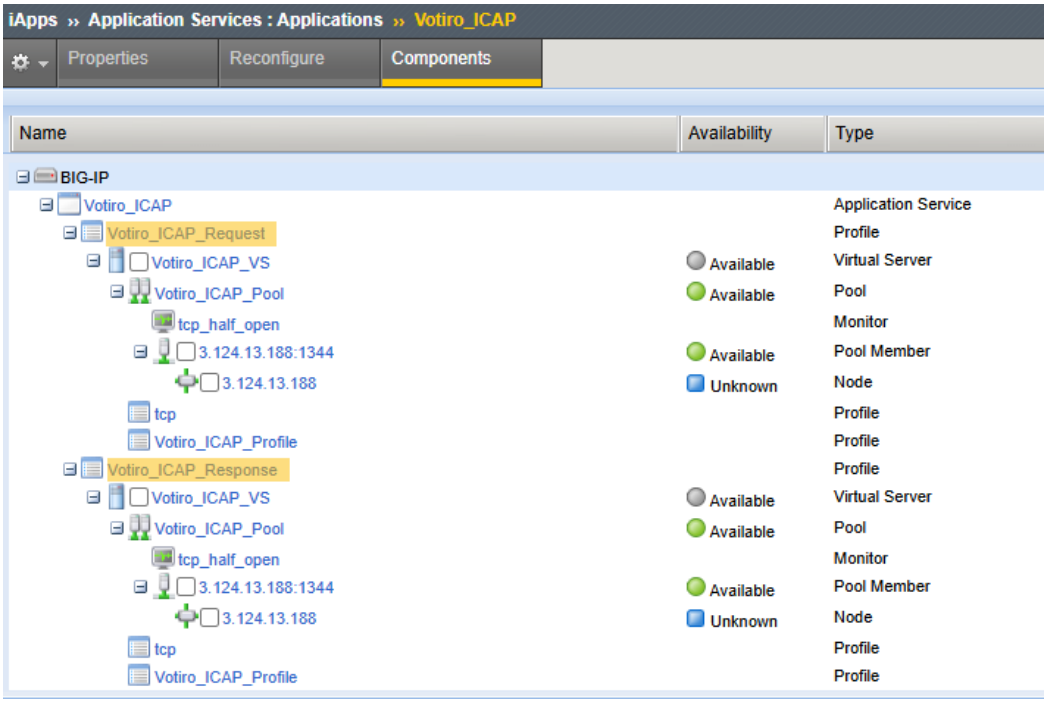
1. The Client uploads files to a specific URL via a web browser or IP address.
2. Traffic arrives at the F5® BIG-IP® Local Traffic Manager™ (LTM) Public IP.
3. The F5® Local Traffic Manager™ forwards HTTP requests to the F5 LTM Standard - Virtual-server (F5 Private IP).
4. The F5 Standard-Virtual-server transfers the HTTP request to the Internal-virtual-server (Pre-Confgured By Template).
5. The F5 Internal-Virtual-server transfers the HTTP request to the ICAP Pool, which contains Votiro’s ICAP endpoint address (Pre-Configured).
6. The Votiro-ICAP server sends the original file for sanitization and responds with the sanitized file to the F5 LTM Internal-Virtual-server.
7. The Internal-Virtual-server forwards the request to the F5 LTM Standard-Virtual server.
8. The F5 LTM Standard-Virtual server transfers the HTTP request to the Web server.
9. The sanitized file is uploaded.

To simplify, a user uploads a document to a company's web server for approval. The document is then sent from F5 to Votiro SaaS for sanitization and forwarded to the web server, awaiting customer service review.

The following topology provides a more explicit visual representation of the process:



The image below is a snapshot of a BIG-IP F5 Load Balancer configuration used to manage server traffic flow:



The following is an explanation of the above screenshot:

BIG-IP Hierarchy:

- **Votiro_ICAP**: Represents the primary application service. serves as a parent container for all related ICAP configurations.
- **Votiro_ICAP_Request**: A subset profile of the ICAP service handling requests.
  - **Votiro_ICAP_VS** (Virtual Server): Represents the entry point for client traffic.
    - **Votiro_ICAP_Pool**: A pool that manages backend servers. Pools contain multiple pool members.
      - **tcp_half_open** (Monitor): Ensures pool members are available using a health check method.
      - **Pool Members**:
        - `3.124.13.188:1344` (**Available**): This pool member is active and ready to process traffic.
        - `3.124.13.188` (**Unknown**): Node status not determined.
    - **tcp**: Another monitor
- **Votiro_ICAP_Profile**: Indicates a specific profile configuration for ICAP.

Architectural Flow:

The flow of this configuration can be summarized as follows:

1. The Client traffic arrives at the Virtual Server (Votiro_ICAP_VS).
2. The Virtual Server routes the traffic to a Pool (Votiro_ICAP_Pool).
3. The Pool Members (3.124.13.188:1344 and others) handle the request if marked Available.
4. Monitors (e.g., tcp_half_open) check the health of the pool members.
5. If a pool member is unavailable, traffic will not be routed to it.
6. Profiles (Votiro_ICAP_Profile) are applied to ensure specific protocol-level behavior.

How to Configure ICAP on the F5 BIG IP Proxy Server and Set Up Your Web Server for File Uploads

Considerations

- This guide will cover BIG-IP version 16.1.5.1 build 0.13.7.
- The Amazon Machine Image (AMI) used is “F5 BIG-IP 16.1.5.1-0.13.7 BYOL - All Modules 2Boot,” its AMI ID is ami-0cedc3bcc72cda188.
- This basic setup does not cover file uploads with secure HTTP/TLS Certificates.
- This guide does not cover ICAP handling or filtering as this is done on the customer side but this is generally made by the iRule feature handled by the “Votiro_ICAP_ Request adapt” profile.

Configuring F5 BIG-IP

1. You can launch an EC2 instance using your image or get one from the Marketplace . Then you need to obtain the appropriate license.
2. You can log in using the Public IPv4 DNS address or the IP address via the management port 8443.

3. Download the Votiro_icap.tmpl file. This template simplifies the creation of ICAP-related elements (such as nodes, pools, internal virtual servers, and profiles) in one centralized location. The newly created request and response adaptation profiles can be assigned to standard virtual servers, enabling them to utilize the Votiro ICAP Server.
4. Connect to your F5® BIG-IP® server.

Create the Local Traffic Manager™ (LTM) Internal-virtual-server

1. In the left pane menu, navigate to **iApps** > **Templates**.
2. Click on **Import**, then select the downloaded template file “Votiro_icap.tmpl" and click on **upload**.
3. To create a new application from the template, go to iApps, click on **Application Services**, and select **Create**.
4. Choose an appropriate name for the application, such as "Votiro_ICAP_Prod_SG.”
5. In the **Template** section, open the drop-down menu and select the template name.
6. In the section labeled **ICAP Pool**, ensure that the option **create a new pool** is selected.
7. Under **Node/IP**, enter the IP address of Votiro's ICAP server that corresponds to your region.
8. Verify that Port 1344 is in use.
9. Under the **Create request and response adapt profiles** section, select the **service down actions** that you would like to receive when the service is unavailable, according to your preferences. It is advisable to choose the **reset** option.
10. Maintain all other configurations as they are and click on **Finish**. The **Components** map will be displayed.
11. On the same screen, navigate to **Properties**. Open the drop-down menu and change the setting from **Basic** to **Advanced**.
12. Uncheck the box labeled **Strict Updates (recommended)** and click on **Update**. This will allow us to modify specific configurations that were previously unchangeable in the next step.
13. Navigate to **Local Traffic** > **Profiles** : **Services** : **ICAP** and select **Votiro_ICAP_Profile**.
14. Contact Votiro support to obtain the Votiro ICAP endpoint. Then, in the **Settings** section under **URL**, paste the fully qualified domain name (FQDN) of Votiro’s ICAP server in the following format: *<icap://fqdn/vicap>* and then click on **update**.
15. Navigate to the **Pools** section under **Pool List**. You will find the **Votiro_ICAP_Pool**, which should be highlighted in green to indicate that it is available. Click on it.
16. Go to **Configurations** followed by **Health Monitors**. Scroll down through the available health check profiles and select **tcp_half_open**. Click the left arrow to add it and make it **Active**, then click on **Update**.

17. You should now have an application named **Votiro_ICAP_VS** running as an LTM internal virtual server. To verify this, navigate to **Local Traffic** and select **Virtual Servers**.

18. Because this server type is classified as “internal,” it does not have an IP address and will appear grayed out. However, if you hover your mouse over it, a status message will display: **Available (Disabled Parent) - The virtual server is available. Its main purpose is to hold the ‘Votiro_ICAP_Profile'**.

Setting up the Web Upload Server on F5® BIG-IP®

Assuming your organization already has a web server, you must configure a virtual server to utilize it.

Create the Local Traffic Manager™ (LTM) Standard-virtual-server

Local Traffic Section

1. Go to the **Virtual Servers** section and click on **Create**.
2. Under **General Properties**, set a name, preferably the name of your upload server.
3. Under **Source Address**, set the subnet to **0.0.0.0/0** to accept traffic from any location.
4. In the **Destination Address/Mask** field, enter your internal private IP address, which is located in the upper left corner of the management console.
5. Set the desired **Service Port** according to your setup; for example, choose 80 for HTTP.
6. In the **Configuration** section, change the setting from **Basic** to **Advanced**. Ensure that it includes the following options:
   - HTTP Profile (Client): **HTTP**
   - Request Adaptation Profile - **Votiro_ICAP_Request**
   - Source Address Translation: **Auto Map**
7. Click on **Finish**.

Pools Section

1. Go to **Pools** and click on **Create**.
2. Give your pool a name that relates to your web server.
3. Select **tcp_half_open** to be used as the health monitor.
4. In the **Resources** section, set the Node Name to match your web server name, along with your web server's public IP address and the upload port (e.g., 5000).
5. Click on **Add**. If your web server is online, it should display a "Green” status.
6. Navigate to **Virtual Servers** and select your newly created virtual server.

7. Navigate to the **Resources** tab and select the pool name you previously created under the **Default pool** section.

Configuring the Votiro Management Console

For further instructions to complete the ICAP setup, contact Votiro support.

ICAP Server Configuration in the Votiro Management Console

ICAP traffic is displayed in the Management dashboard under Data source > File connector > ICAP Server.

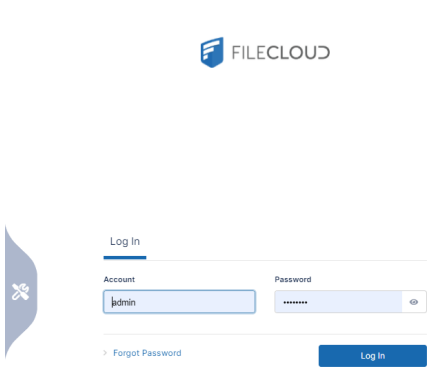
The user can view and filter ICAP incidents by using the ICAP channel name in the filter channels.

2.17.9 FileCloud

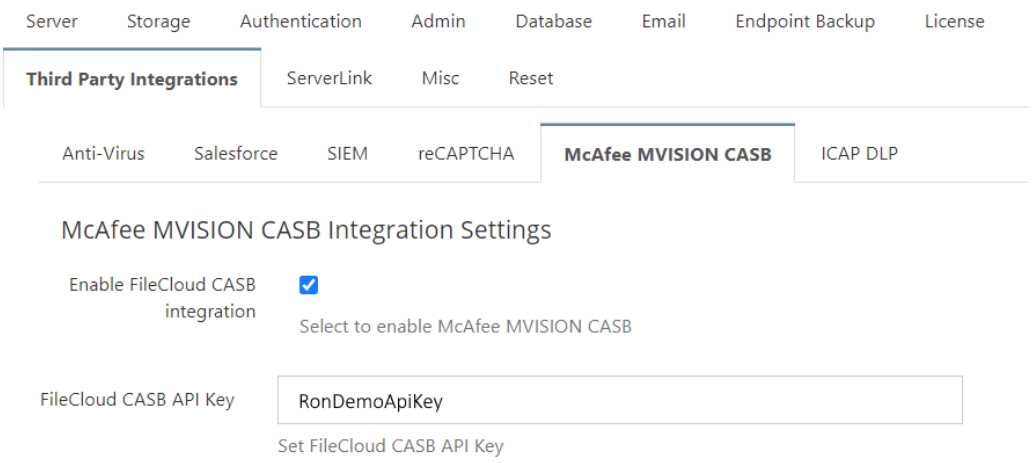
FileCloud Configuration for Integration with Votiro

To authenticate FileCloud with Votiro, generate an API key.

1. Login to your FileCloud account with Admin privileges.



2. In the Admin portal navigation pane, click **Settings**, and then select **Third Party Integrations**.
3. Select the **McAfee MVISION CASB** tab.
4. Select the checkbox **Enable FileCloud CASB integration**.
5. Change the value of the **FileCloud CASB API Key** to any alphanumeric string.
6. Click **Save**.



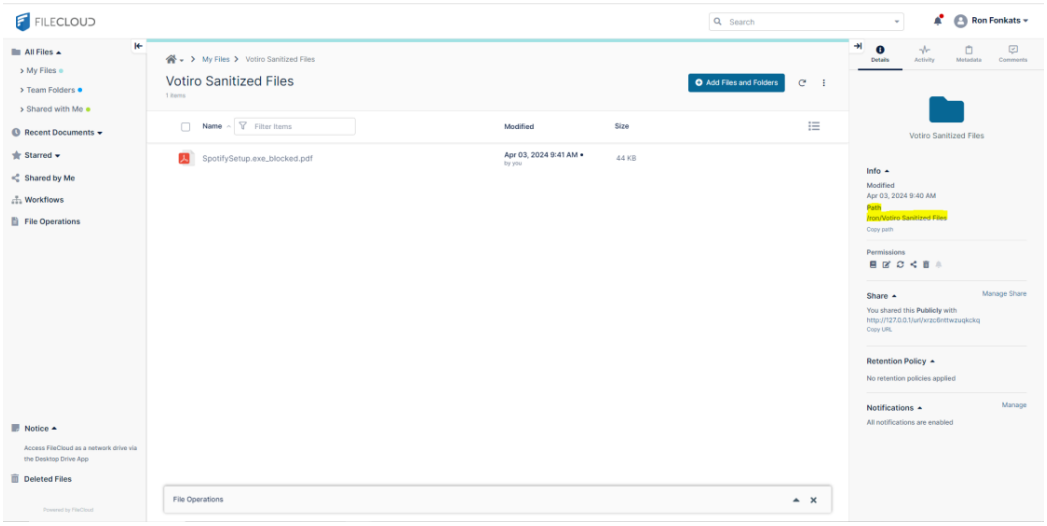
7. Add the value of the **FileCloud CASB API Key** to McAfee MVISION CASB.

Creation of a FileCloud Output Folder

Our new product solution offers our customers a new way to handle sanitized files.

Customers can choose an output folder, and every file that a FileCloud user uploads to any desired folder will be sanitized and placed inside the designated FileCloud output folder.

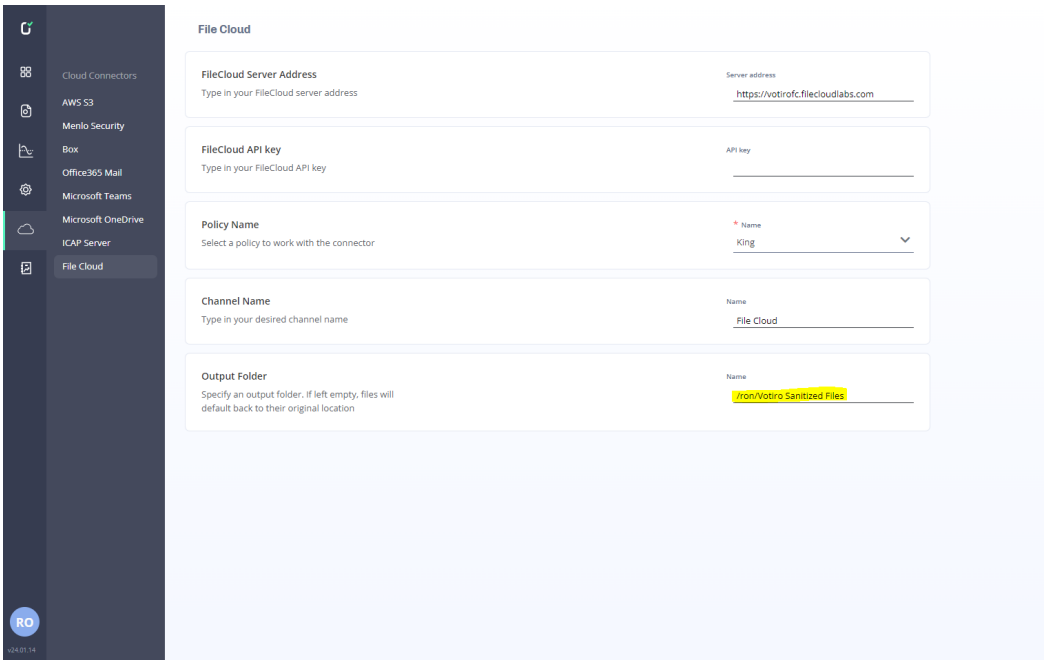
1. Open the FileCloud console.
2. Select **All Files** > **My Files**.
3. Create a new folder. This will serve as the output folder.
4. Copy the new folder path (it will be needed for configuration of FileCloud in the Votiro Management Dashboard).



5. Share the new output folder with any users that need to have access to it.

Configuration of FileCloud in the Votiro Management Dashboard

To get to the File Cloud page, from the navigation pane on the left, click **Cloud Connectors and Integrations** > **File Cloud**.



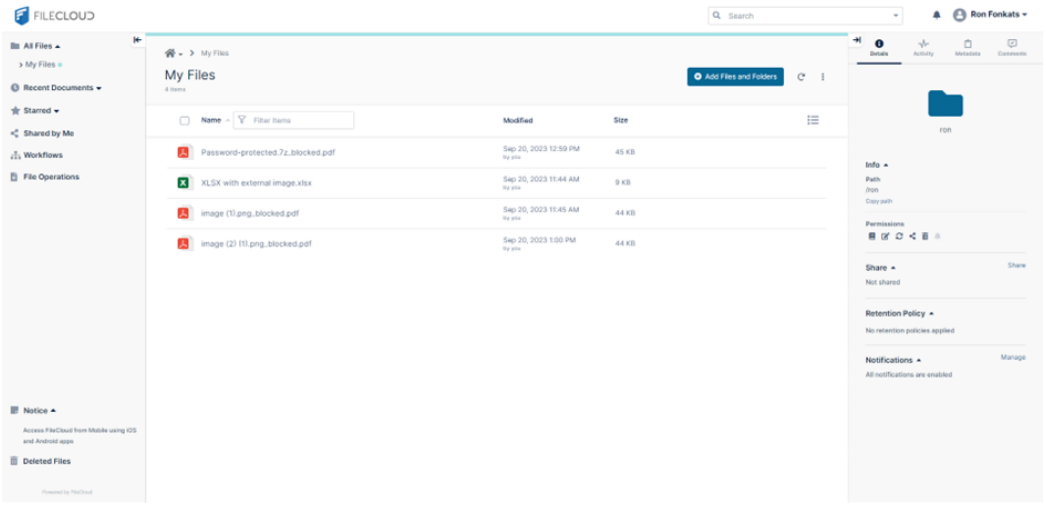
The File Cloud page contains the following fields:

Field	Description
FileCloud Server Address	Specify the FileCloud server address. The address must include **https://**
FileCloud API key	Specify the FileCloud API key.
Policy Name	Specify a policy for the FileCloud connector to work with. Select the **Default Policy** if you have not created an alternative policy to use.
Channel Name	Specify the name of your channel. The channel name appears in the Incidents page as the name of a connector. In the example above, the channel name is "File Cloud".
Output Folder	Specify an output folder to contain sanitized files (the folder that was configured in FileCloud, as described in Creation of a FileCloud Output Folder). If left empty, files will default back to their original location.

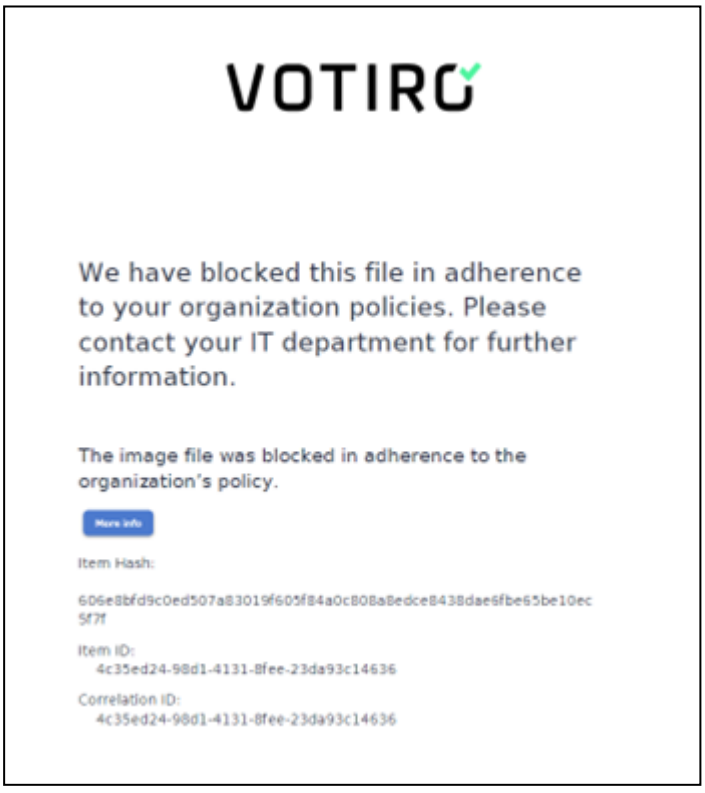
Save the configuration.

FileCloud Behavior when Uploading Files

1. Any file upload will be directed to the Votiro sanitization process.
2. After the file is uploaded, it is deleted and then replaced by a sanitized version of the file upon completion of the sanitization process. Note that this process may take some time, and therefore the sanitized file will not be displayed immediately.

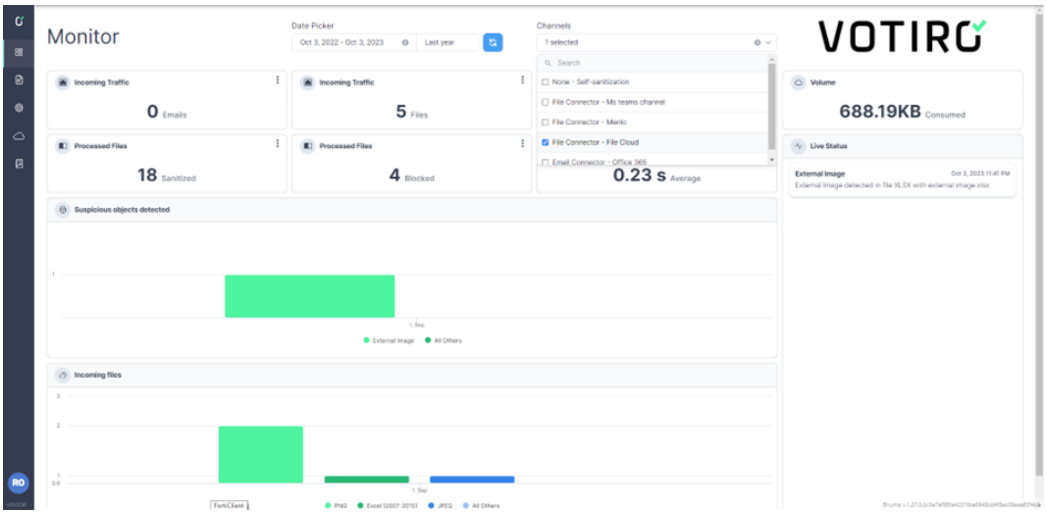


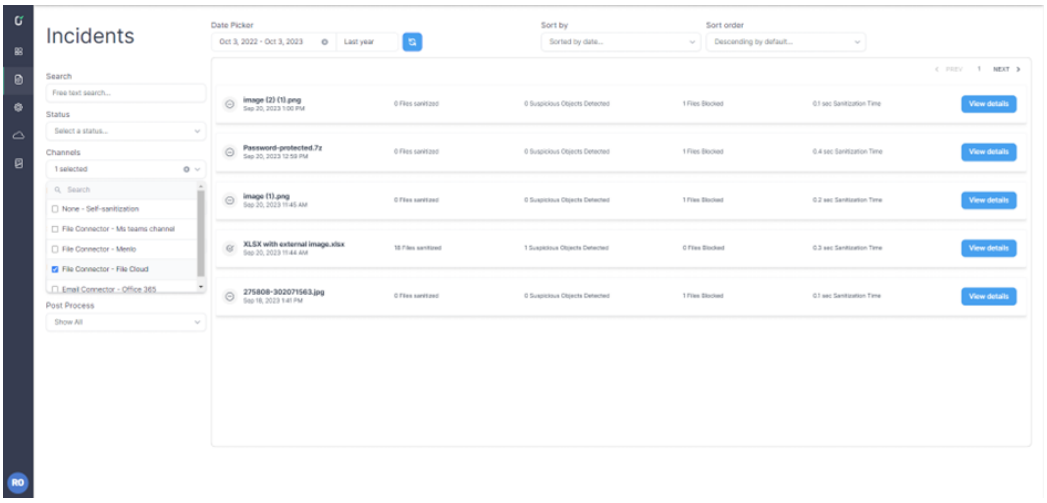
If the file was blocked, the original file is replaced by a blocked PDF that contains an explanation of the reason for blocking the file.

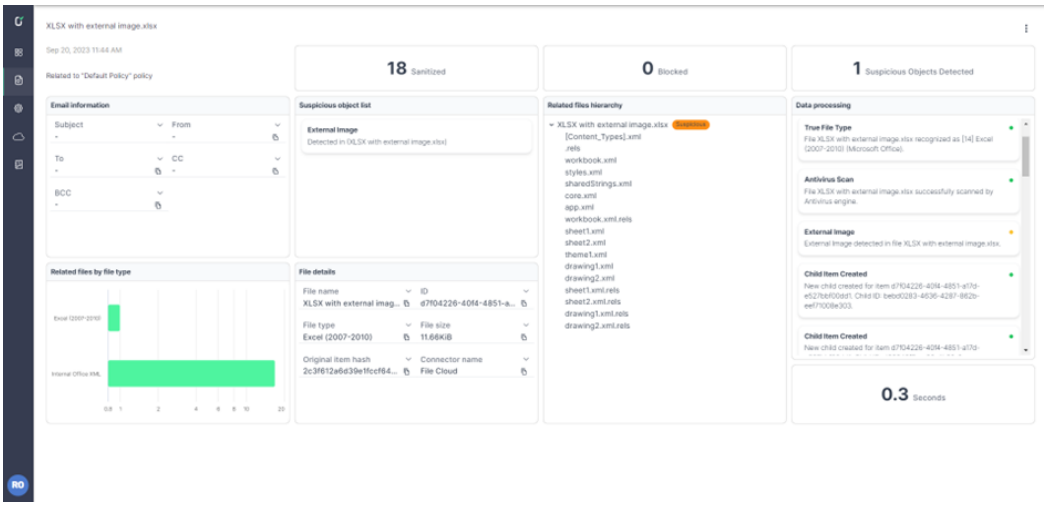


Votiro Management Console – Monitoring

For monitoring and further investigation, browse the Votiro Management console to get more information on the uploaded files.







Limitations

- The supported file size is up to 2 GB.
- When uploading an entire folder for sanitization, the folder will not be preserved, and the sanitized files will be retrieved without the original folder structure.

2.17.10 Chrome Browser Extension

Description

This document describes the installation, deployment and usage of Votiro's Chrome browser extension.

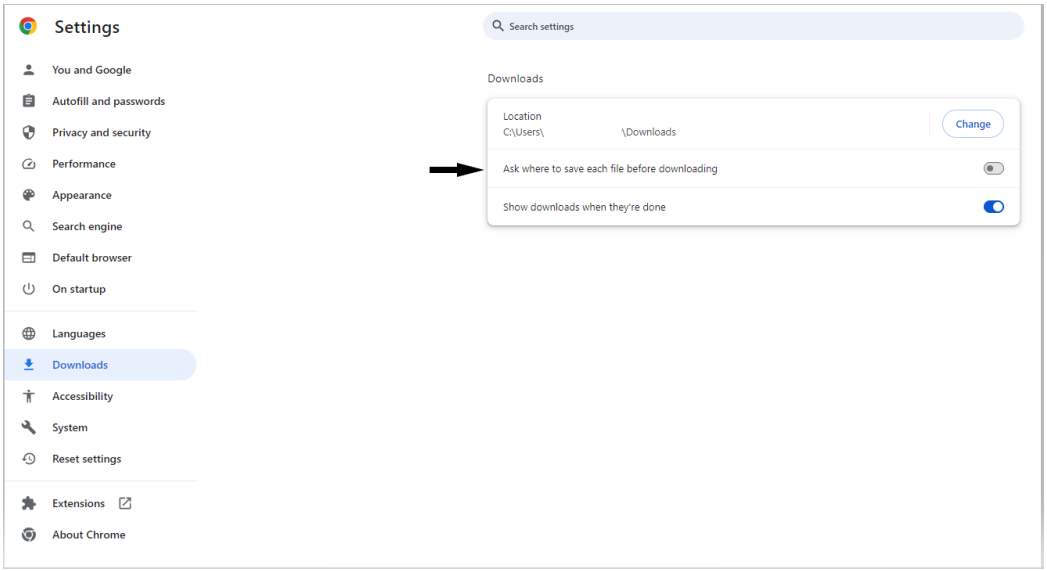
The browser extension can be:

- downloaded and installed by centralized deployment using GPO (Group Policy Object). See Centralized Deployment using GPO (Group Policy Object).
- downloaded and installed manually. See Manual Deployment.
- downloaded and installed in the Microsoft Edge browser.
- downloaded and installed in the Cyberark Secure Browser.

The user's manual is described at Chrome Extension User's Manual.

Limitations

- The Chrome browser extension does not work with Microsoft 365 webmail.
- The Chrome browser extension does not support the Chrome browser option to enable the user to indicate where to save each file before downloading. You must disable this option as follows:
    a. In the Chrome browser, navigate to **Settings** > **Downloads**.
    b. Disable **Ask where to save each file before downloading**.



- Base64 images are directly embedded inside the webpage as text (inside HTML or CSS). Because they are part of the page itself, they don't require a separate URL and therefore cannot be "whitelisted" regularly.
  Base64 images are just images converted into text using a special encoding called Base64. Instead of storing an image file (like .jpg or .png), Base64 turns the image into a long string of letters, numbers, and symbols.
  Regular images are stored as files on a server, and the browser loads them using a URL (https://example.com/image.png).

Centralized Deployment using GPO (Group Policy Object)

To deploy Votiro's Chrome extension using GPO, the domain admin must implement the following steps:

1. Update the domain controller group policy with Google's Chrome extension.
2. Central installation of the extension from the Google web store to users.
3. Central configuration of the extension's parameters in the Registry (for Windows, this depends on the operating system).

While this document refers to GPO steps explicitly, the deployment can be done by most standard tools for domain policy management (such as Microsoft Configuration Manager (formerly System Center Configuration Manager (SCCM)), PolicyPak and others).

Centralized Deployment Procedure

1. **Add Chrome Policy Templates**

   a. On your domain controller, navigate to the URL Chrome browser for Windows, and download the correct 32 or 64 bit zip bundle. Extract the Google Chrome bundle to your desired location, for example: C:\temp

   b. Navigate to the directory in which you extracted the Google Chrome Bundle and copy to the directory *C:\Windows\PolicyDefinitions* the **chrome.admx** file located in the appropriate directory below:

   - for the 64 bit bundle: *\GoogleChromeEnterpriseBundle64\Configuration\admx*
   - for the 32 bit bundle: *\GoogleChromeEnterpriseBundle\Configuration\admx*

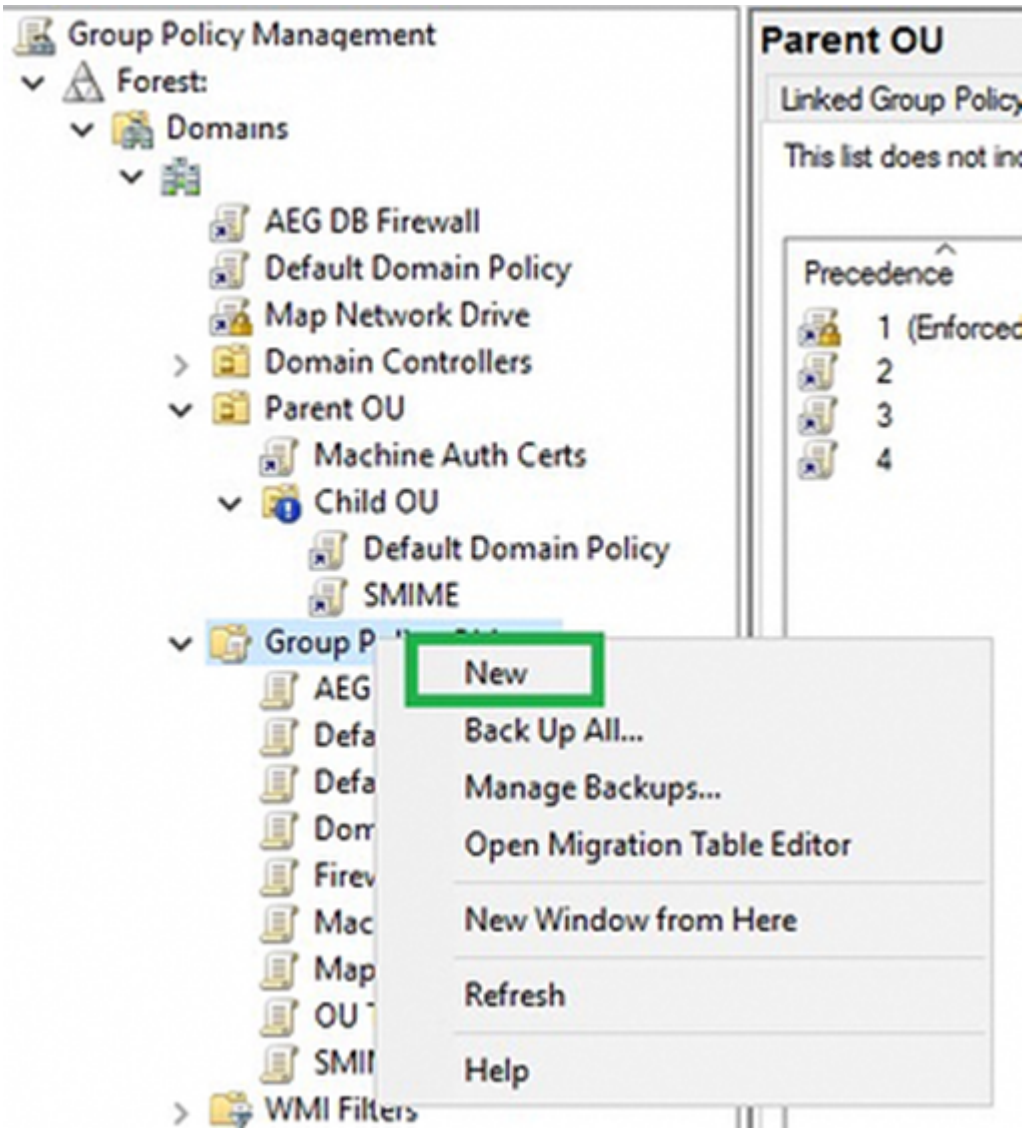
   c. Navigate to the directory in which you extracted the Google Chrome Bundle and copy to the directory *C:\Windows\PolicyDefinitions\en-US* the **chrome.adml** file located in the appropriate directory below:

   - for the 64-bit bundle: *\GoogleChromeEnterpriseBundle64\Configuration\admx\en-US*
   - for the 32-bit bundle: *\GoogleChromeEnterpriseBundle\Configuration\admx\en-US*

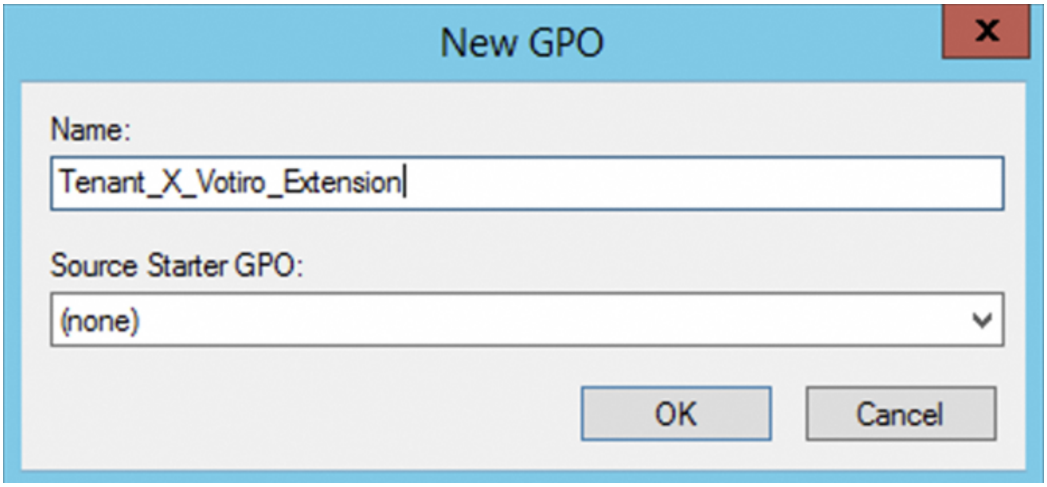
> **Note**: If a language other than en-US is desired, navigate to the appropriate language directory within the admx directory, for example, for Spanish: es-ES, and copy to the appropriate language directory within *C:\Windows\PolicyDefinitions*.

2. **Create a Group Policy setting to deploy the Chrome extension**

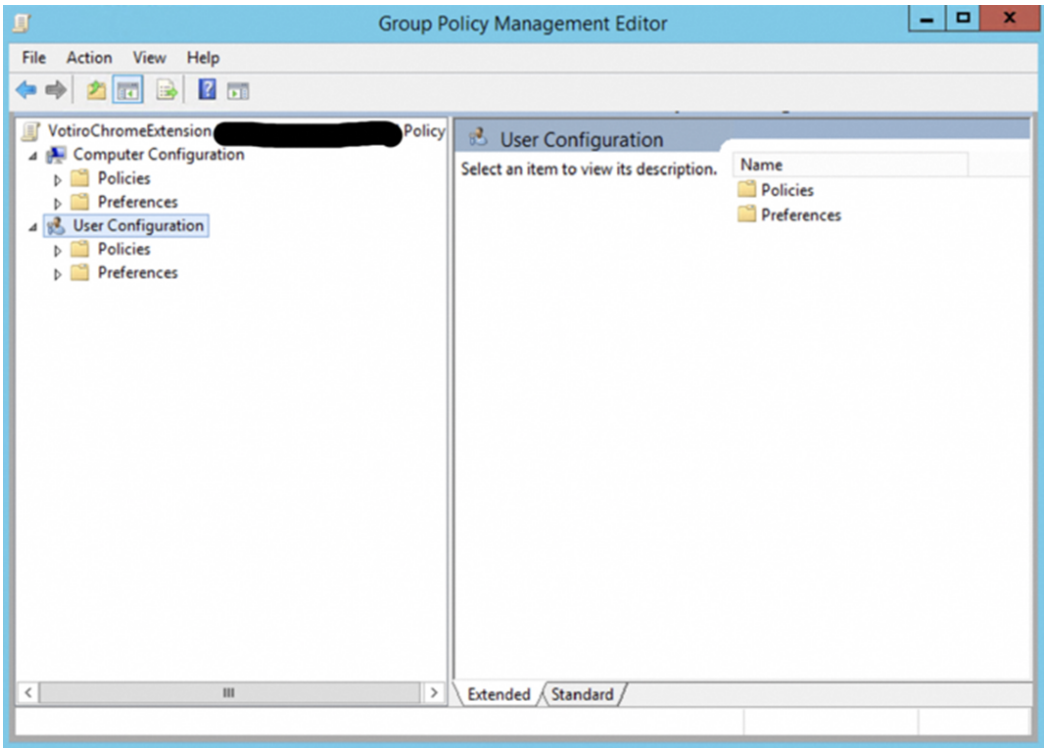
a. Right-click **Group Policy Objects**, then select **New** to create a new GPO.



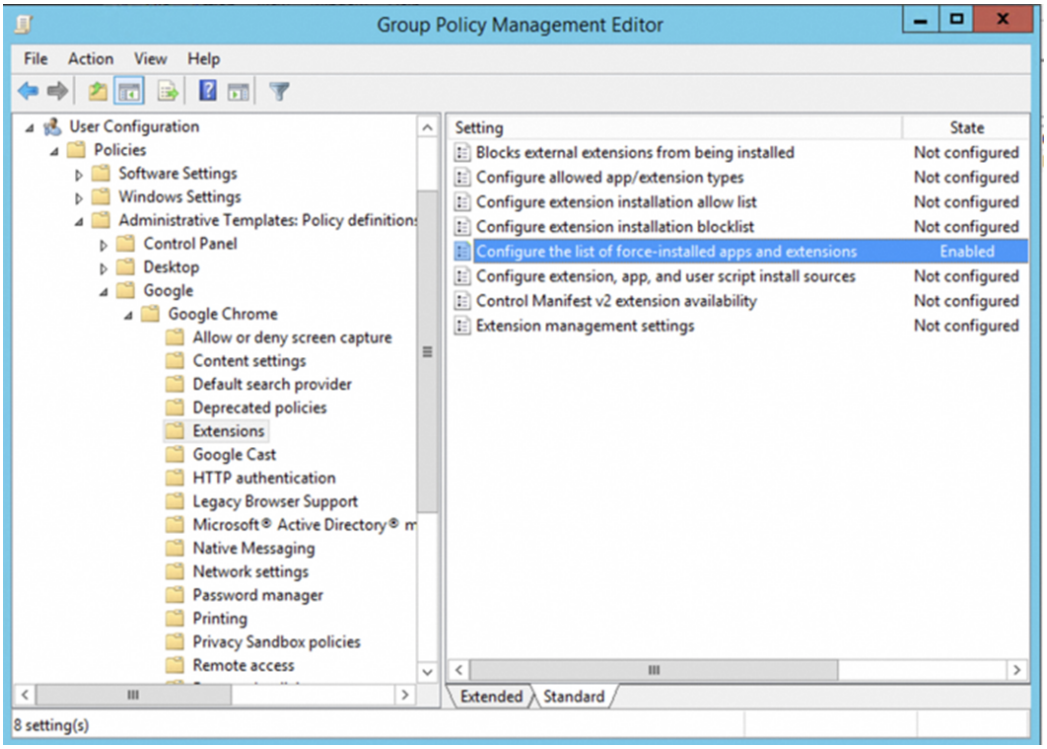
b. Enter a **Name** for the new GPO , then click **OK**.



c. Right-click the GPO, and select **Edit**.



d. To force-install extensions, go to *User Configuration\Administrative Templates\Google\ Google Chrome\Extensions*. Go to the setting **Configure the list of force-installed apps and extensions** and double click it.

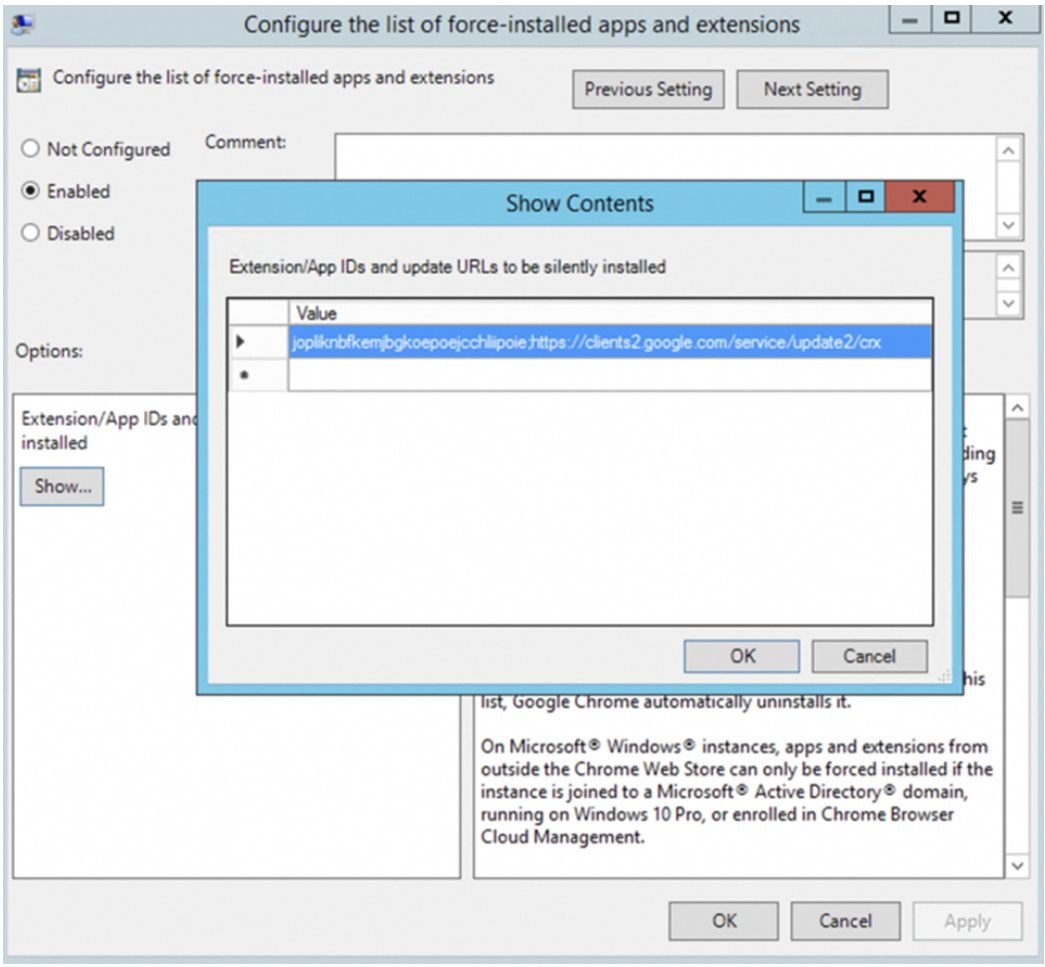


e. Select the **Enabled** radio button.

f. Click the **Show** button.

g. In the **Show Contents** window, enter following string (this string points to our extension in the Google web store) in the **Value** field:

jopliknbfkemjbgkoepoejcchliipoie;https://clients2.google.com/service/update2/crx



3. **Import xml to the group policy (to update the registry)**

   a. Download and save the following xml file locally: tenantXchromePlugin.xml

   b. Open the file for editing and update to match the relevant customer, as following:

   - **hostname** – The cluster you work with (i.e., qa.sg.paralus.votiro.com).
   - **isAudit** – When the value is:
     - true (1) - files are not sanitized, but still appear on our Incidents page.
     - false (0) - files are sanitized.
   - **isFailOpen** – Fail-open and Fail-close error handling:
     - isFailOpen = 1: In case of an error in Votiro, the original file will be downloaded

- isFailOpen = 0: In case of an error in Votiro, the file will be not downloaded.

> **Note**:
> When a change is made to the registry, the registry should be backed up and then reloaded with the updated values.

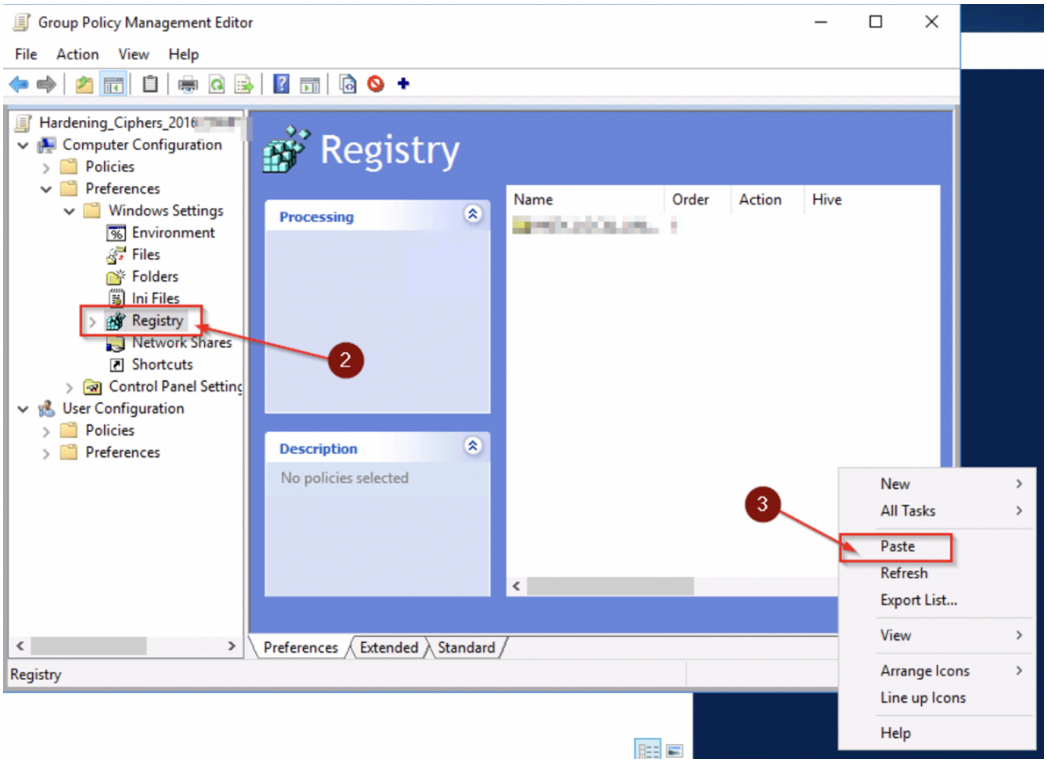
- **votiroPolicyName** – The policy that should be used in the server.
- **token** – The service token for the relevant client (should be taken from the UI)

c. Save the file and close it.

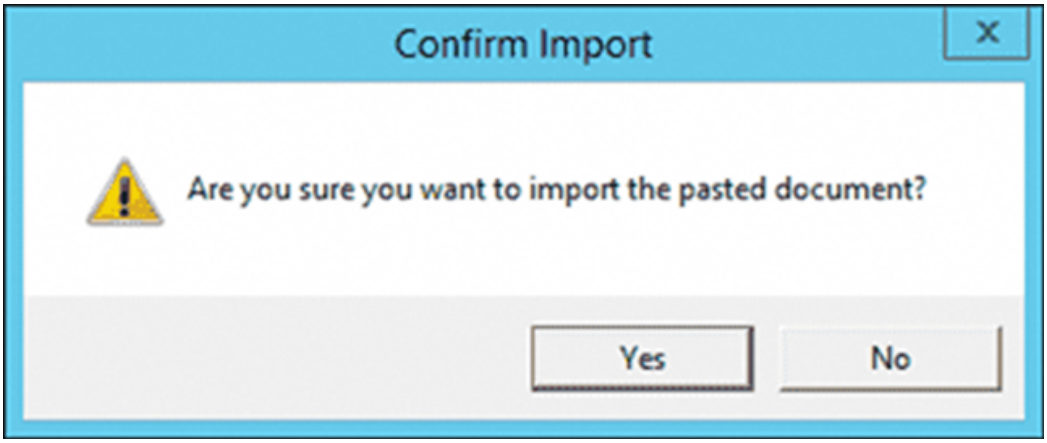
d. Right-click the xml file in File Explorer and copy it to the Windows clipboard.

e. In the Group Policy Editor, navigate to *Computer Configuration > Preferences > Windows Settings > Registry*.

f. Right-click the white pane on the right. In the context menu, select Paste (or press CTRL+V if you don't see the paste menu).



g. The **Confirm Import** window opens. Click **Yes**.

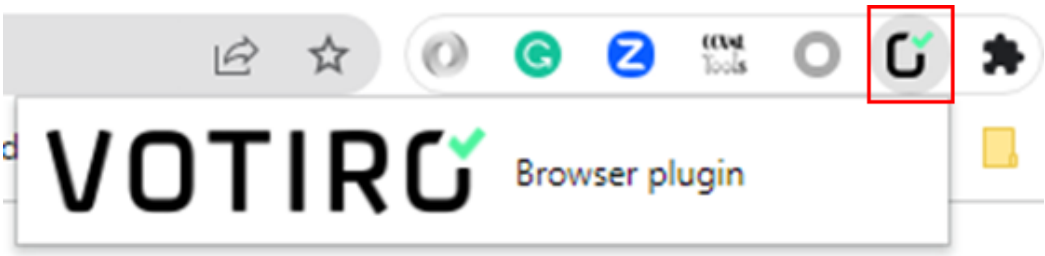


h. The GPO is created. Now you need to link it according to the organization's policy. Locate the OU or Domain you want to apply the GPO to, then right-click it and select **Link an Existing GPO...**. Then select your GPO from the list, and click **OK**.

> **Note**: The policy contains both user configurations and computer configurations, so make sure the policy is applied on both computers and users.

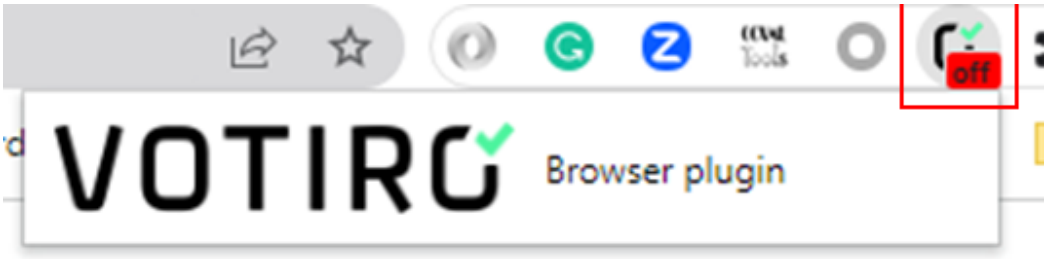
4. **Verify the Browser Extension Deployment**

a. Open the Chrome browser. The Votiro Chrome connector icon will be displayed.



If the Votiro Chrome connector icon appears as above, each downloaded file will be sanitized by Votiro.

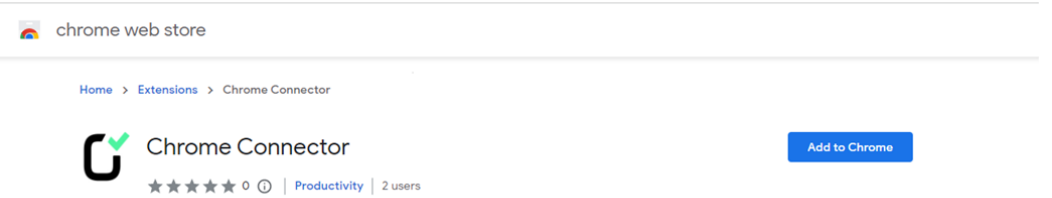
b. If there was a problem, the Votiro Chrome connector icon will be displayed as **off**:



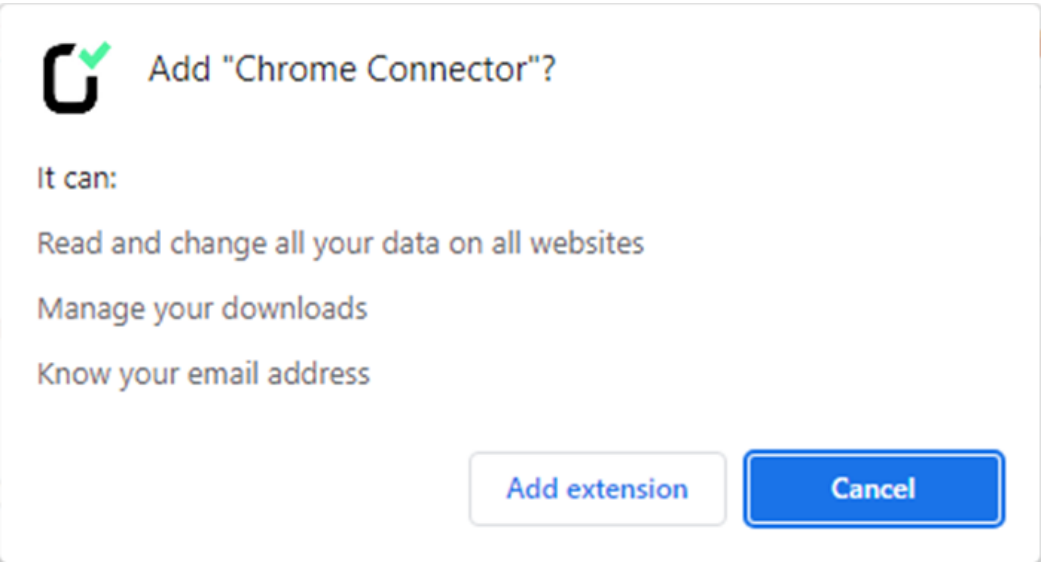
Manual Deployment

1. **Install the extension from Google chrome web store**

   a. Go to the following link in Chrome: Votiro Chrome Connector



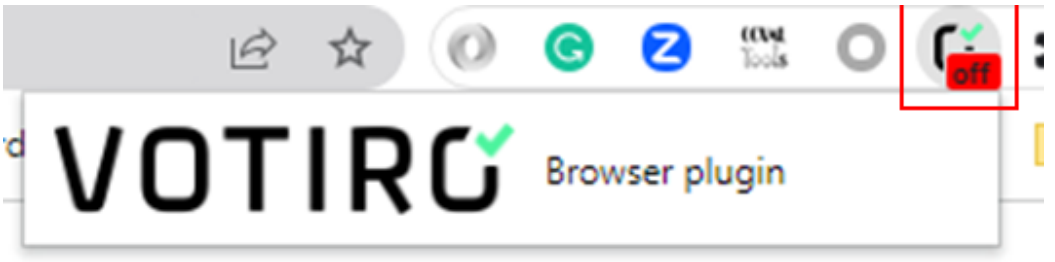
   b. Click on **Add to Chrome**. A confirmation window opens:



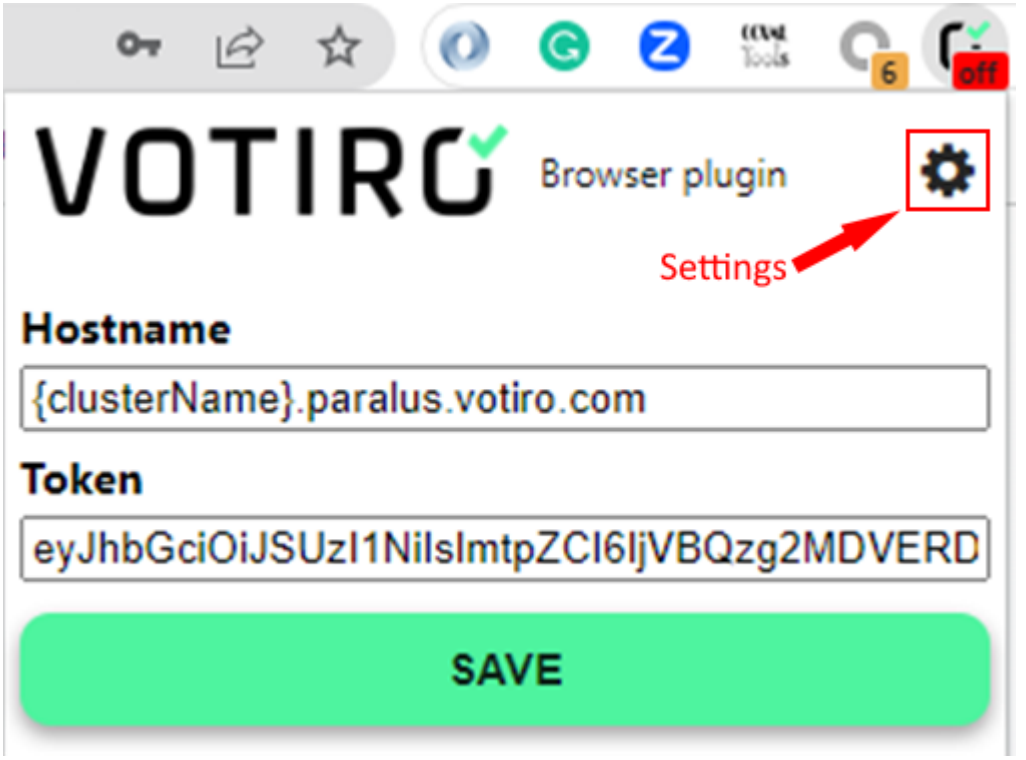
   c. Click on **Add extension**.

2. **Configure the Browser Extension**

a. The Chrome connector icon will be displayed with the **off** icon.



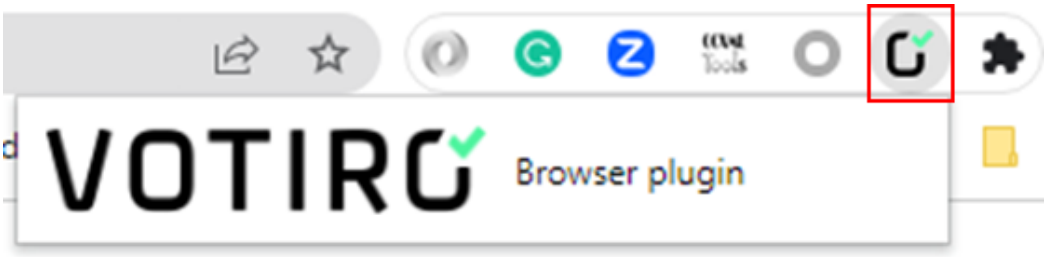
b. Click on the “Settings” icon:



c. Copy and paste the **Hostname** and **Token** from the Votiro Management console as in the above example.

d. Click on **SAVE**.

e. After saving, the Chrome connector extension will be activated. The Chrome connector icon will not be displayed with the **off** icon.

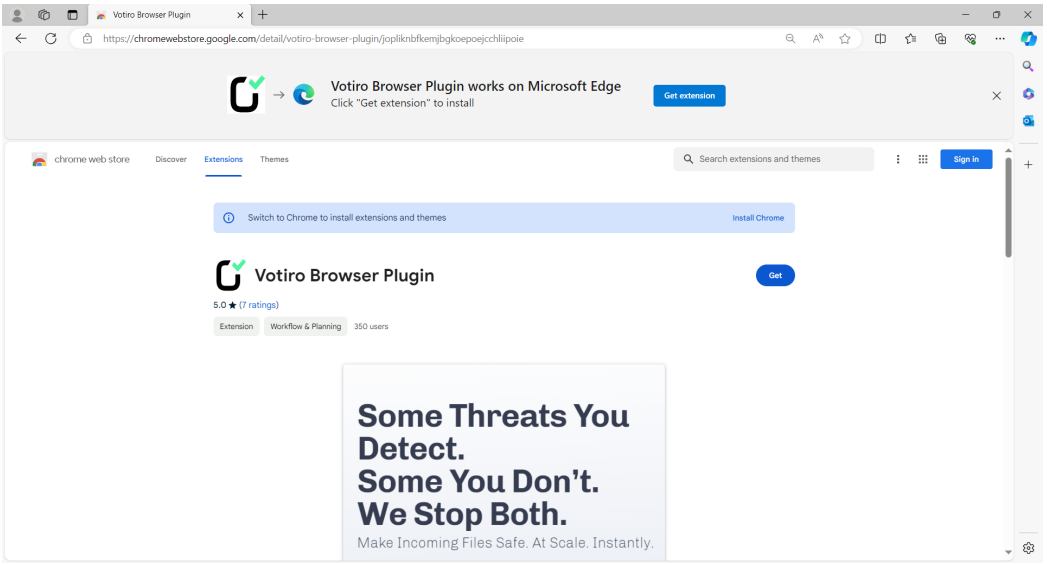


If the Votiro Chrome connector icon appears as above, each downloaded file will be sanitized by Votiro.

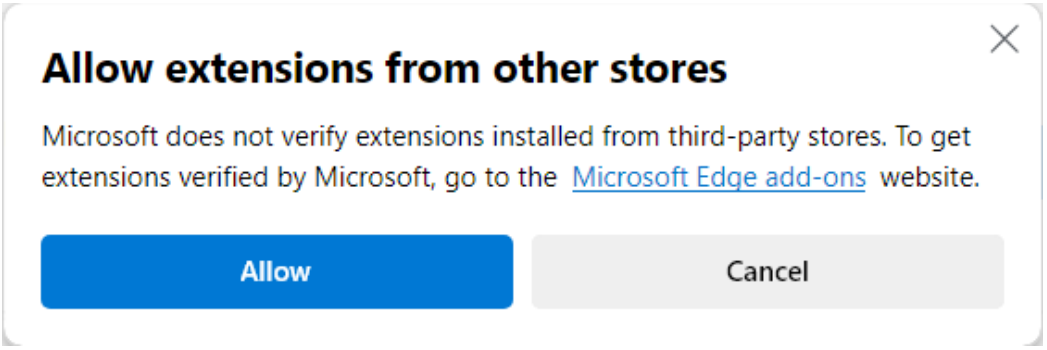
Download and Install in Microsoft Edge Browser

To deploy the Browser plugin in the Microsoft Edge browser:

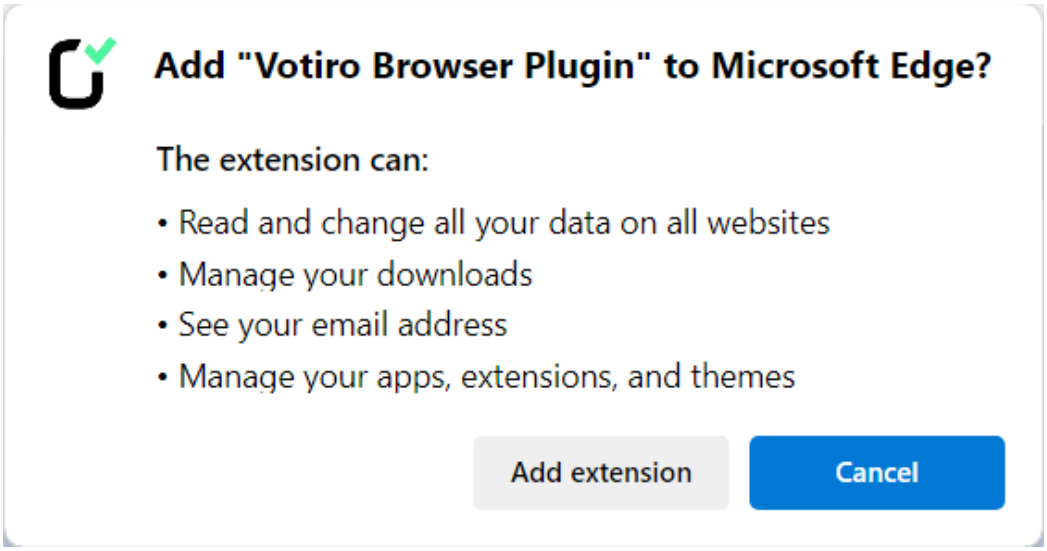
1. Paste the Chrome store extension URL to the Microsoft Edge browser: Votiro Browser Plugin



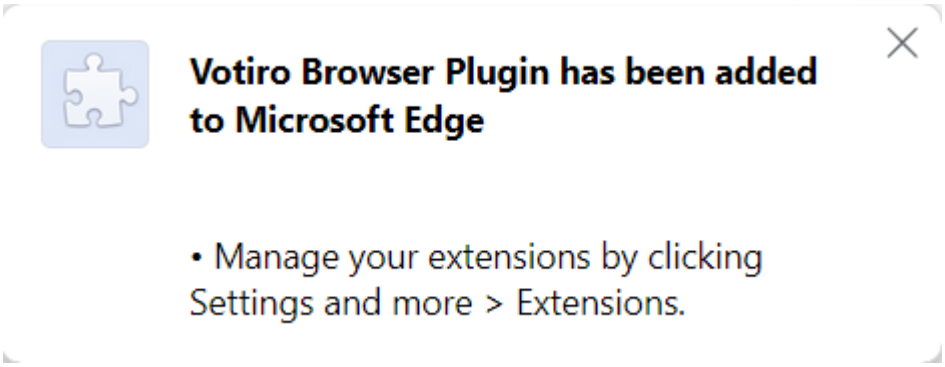
2. Click the **Get extension** or **Get** button to install.



3. Click the **Allow** button.



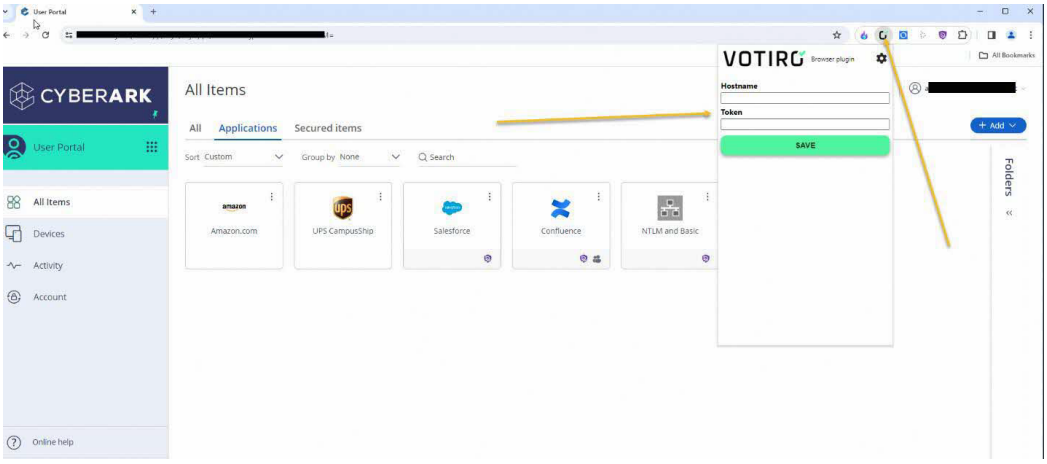
4. Click the **Add extension** button. The Votiro Browser Plugin is installed.



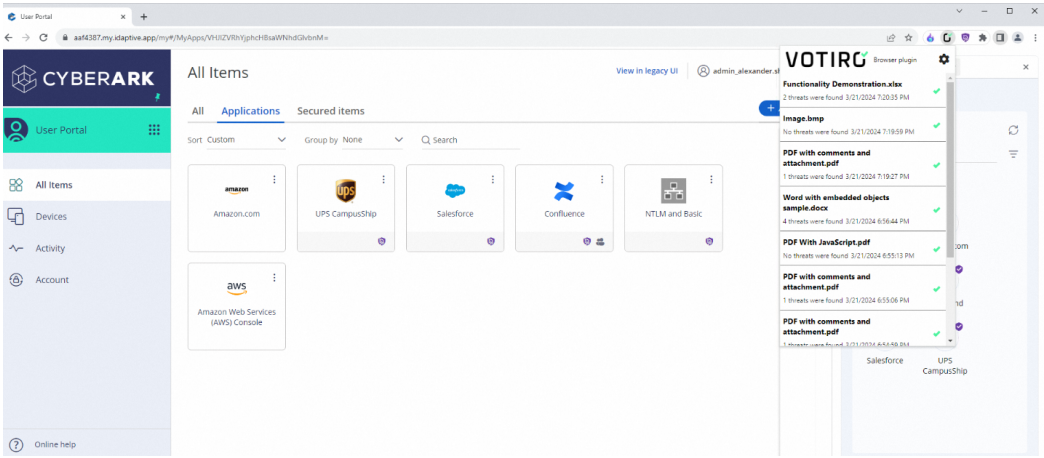
Download and Install in Cyberark Secure Browser

To deploy the Browser plugin in the Cyberark Secure Browser:

1. Deploy the Browser plugin to Chrome using the appropriate deployment procedure (centralized or manual).
2. Open and authenticate to the Cyberark Secure Browser.
3. Navigate to the CyberArk **User Portal** and add the Votiro Browser plugin to the **Applications**.
   - Enter the **Hostname** for the cluster you work with.
   - Enter the **Token** generated using the procedure described in Service Tokens.



4. After the plugin is successfully installed and configured, you can test file downloads. You can see threat detection history by clicking Votiro's plugin.



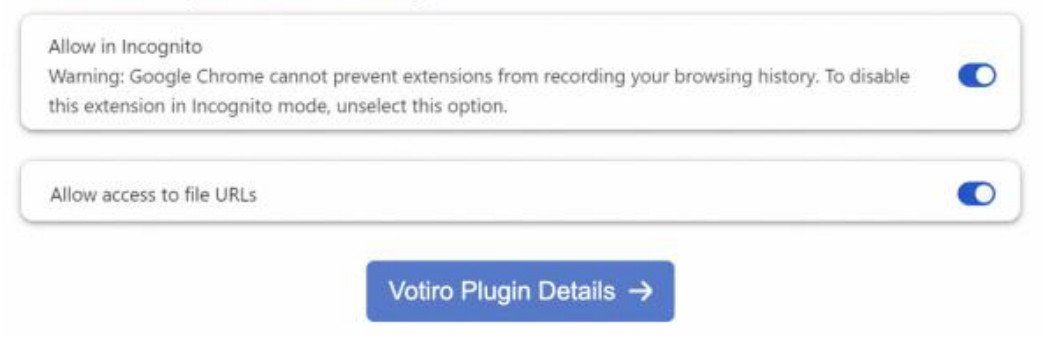
Post-Deployment Actions

Enable Downloads

In the Chrome browser:

1. Navigate to **Extensions** > **Manage Extensions**, or enter **chrome://extensions** in the address box.
2. Navigate to **Votiro Plugin Details** in **Manage extensions**.
3. Scroll down, and enable the following:
   - Check **Allow access to file URLs**.
   - Check **Allow in Incognito**.

Note:
When deploying the browser plugin, each end user will need to enable these options to be able to download files while using the Browser plugin. Because it may disrupt the workflow, this should be taken into account by the organization.



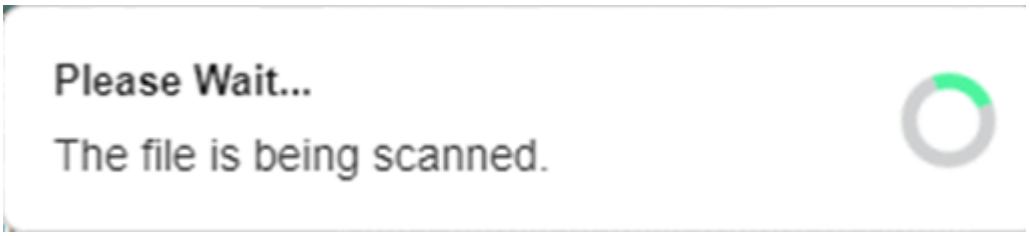
Limitations in Incognito

- The end user will be prompted to enable this option.
- If the end user does not enable the option, files will not be downloaded. In this case, the end user can browse through Incognito and then will be able to download files.
- A prompt cannot be issued from the Incognito window.
- Because of Chrome's strict policy, there is no way to force the app on Incognito without the user's express permission.

Chrome Extension User's Manual

The following features characterize the Votiro Chrome Connector extension:

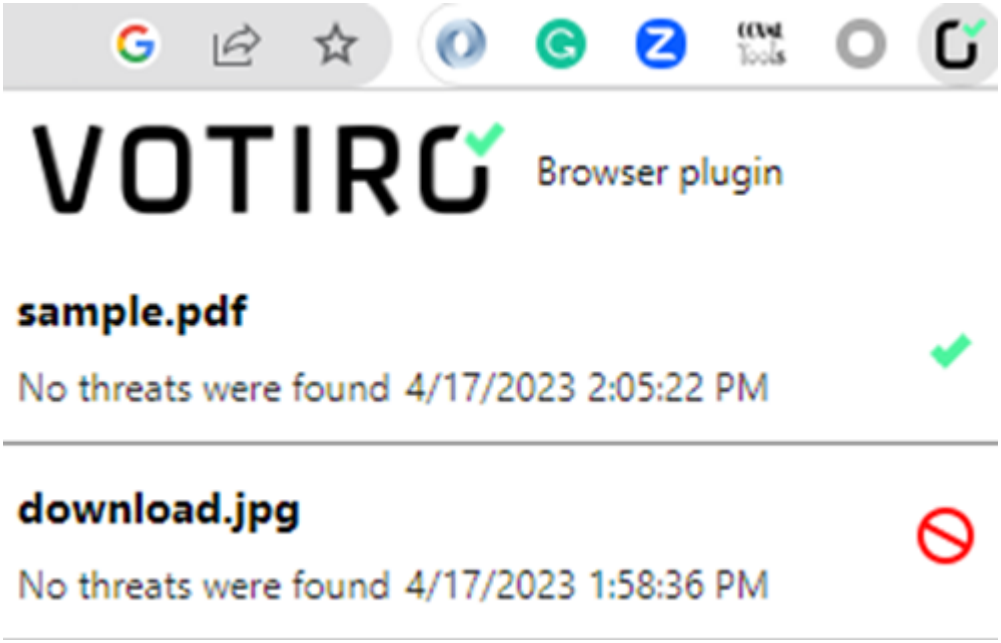
- **Downloading files**
  - When downloading a file, a Votiro popup will display in the bottom right of the screen:



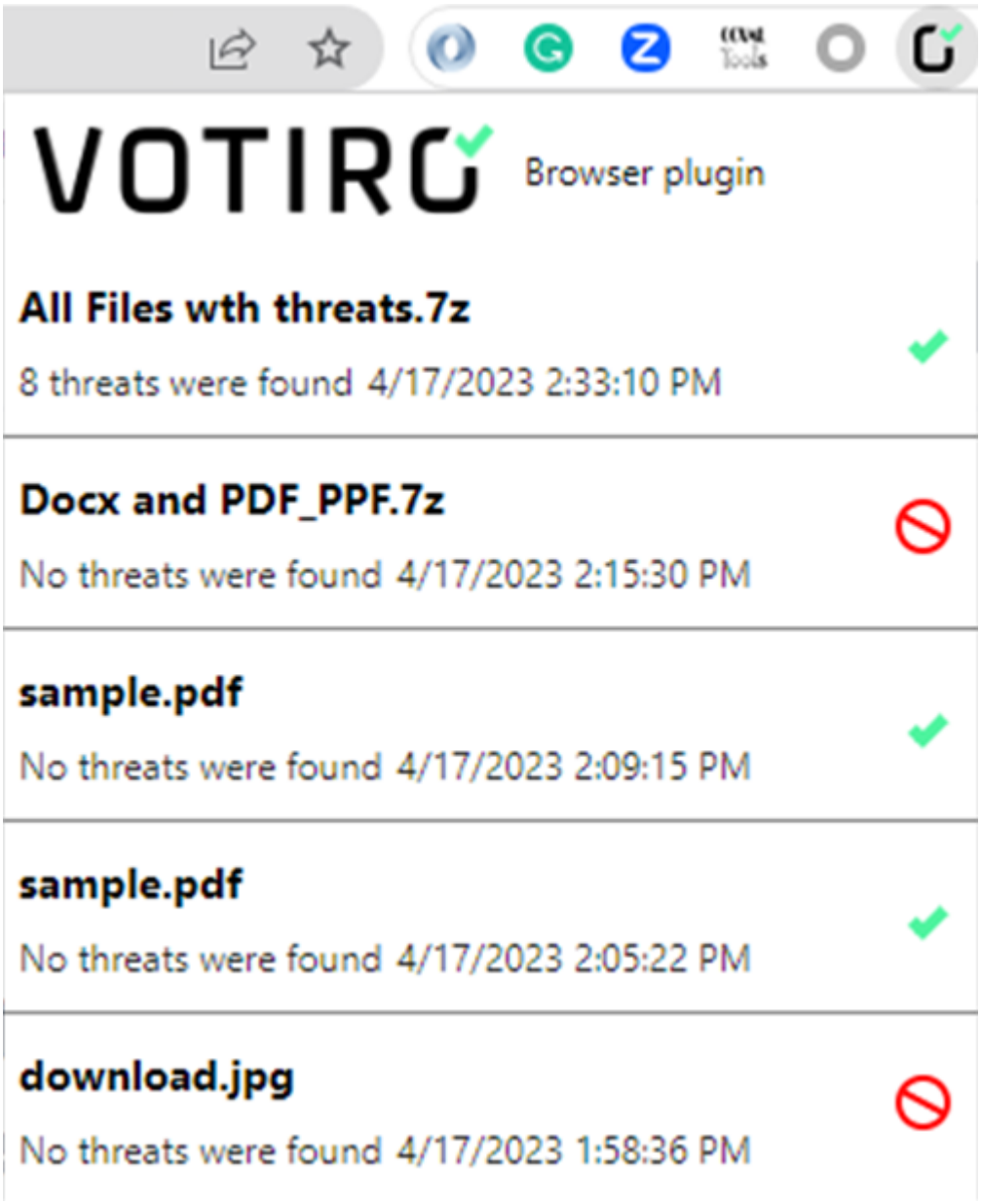
  - After download is complete, there will be an indication that the file was downloaded:

- To view downloaded files, click on the Votiro extension icon. Downloaded files will be displayed. The following information will be displayed:
  - File name
  - Threats indication
  - Time frame
  - Sanitization result icon - Sanitized/Blocked

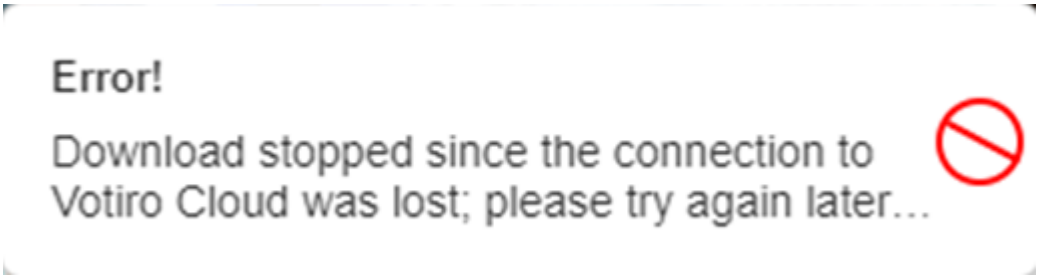
  The following examples illustrate:
  - Example 1: No threats found



  - Example 2: Threats found



- If there is an error while downloading a file, a popup window will display:

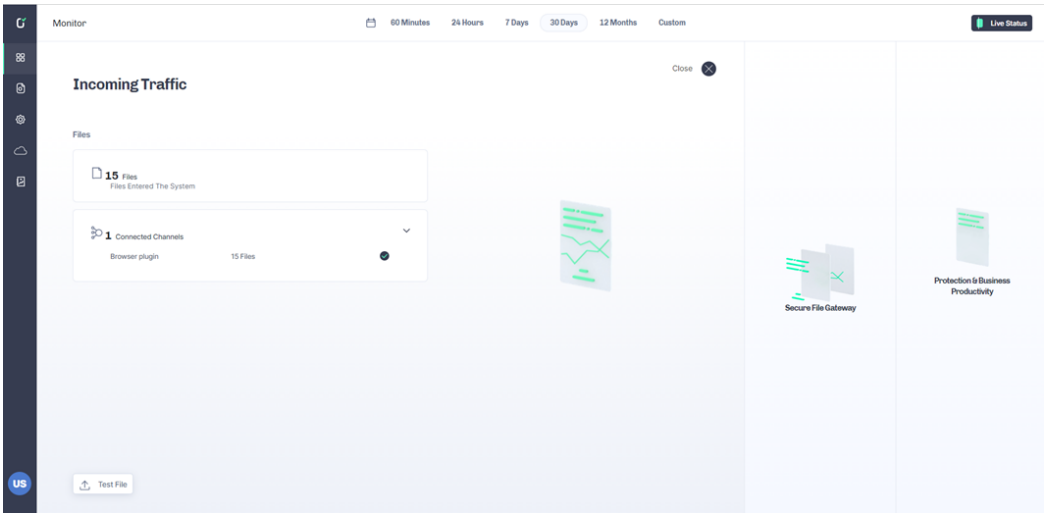


- In this case, please try again. If the problem still occurs, contact Votiro support.

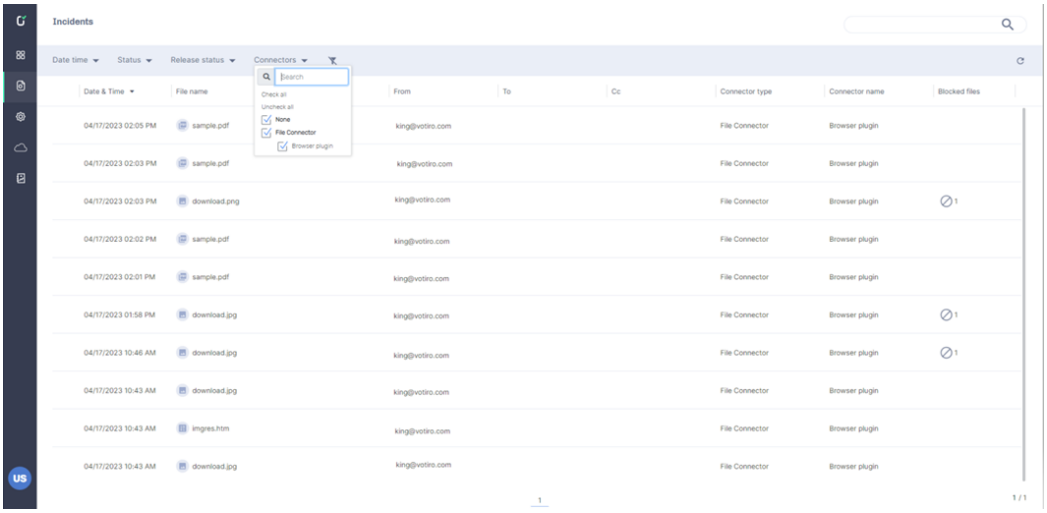
- **Votiro Management**

The following screens illustrate the behavior of the Chrome Connector extension in Votiro's management screens:

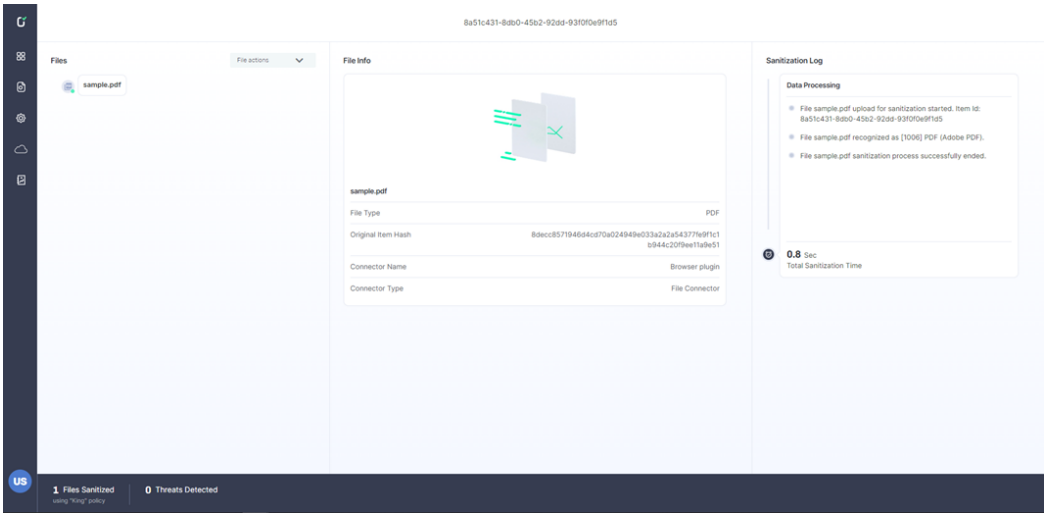
- Dashboard Monitor screen



- Incidents screen
  - There is an option to view and filter incidents from the Browser extension.



- Files screen

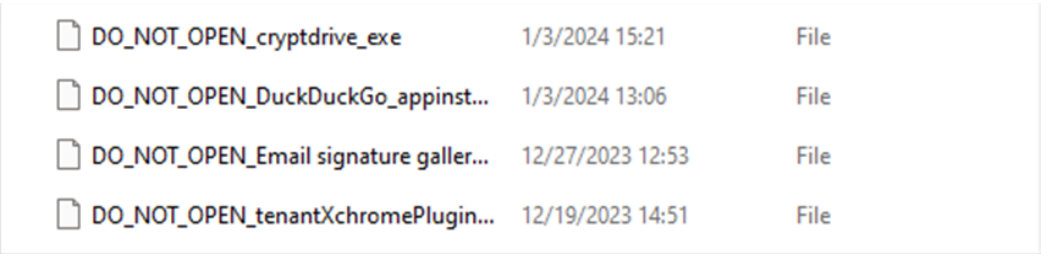


Q&A

Q: If we deploy the Browser plugin widely using GPO, can we prevent users from disabling the Browser Plugin?

A: A customer that uses GPO can control whether users can access/remove/add browser extensions.

Q: When the Browser plugin is deployed, how can we prevent **DO_NOT_OPEN_** from being appended to the beginning of the downloaded file names?



A: In the Chrome browser,

a. Navigate to **Extensions** > **Manage Extensions**, or enter **chrome://extensions** in the address box.

b. Select the Votiro extension.

c. Check **Allow access to file URLs.**

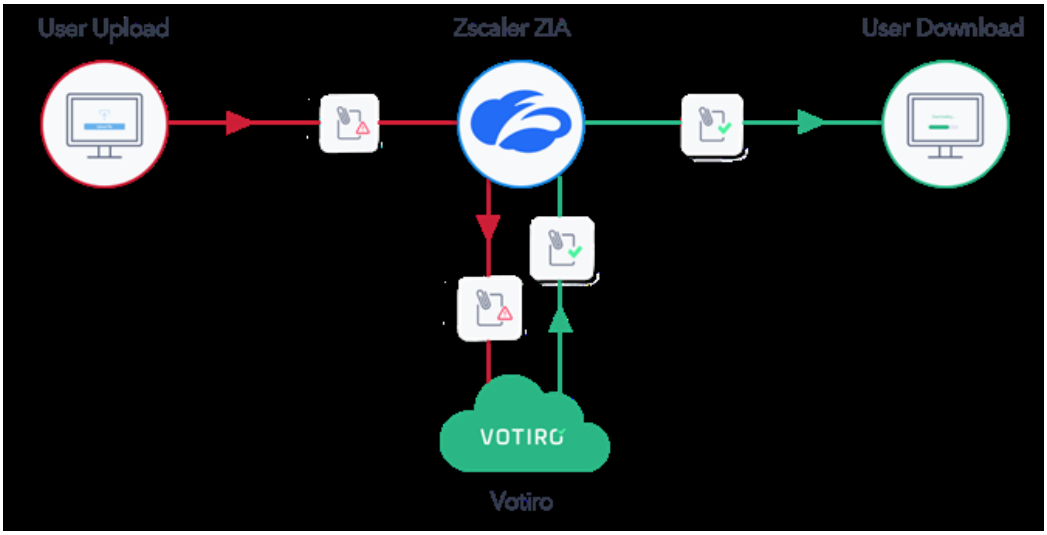
2.17.11 Zscaler Integration with Votiro

Zscaler Isolation and Votiro CDR Integration

Zscaler Isolation and Votiro enable users to access, view, and download the content they need—seamlessly and without risk. Improve the security of traffic passing through the ZIA platform with Votiro.

- Reduce the risk of malware and malicious code by only allowing known good files through!
- Zero-day threat prevention: Votiro strips out unknown bad code. This complements ZIA by mitigating novel and unverified threats.
- Improved compliance: Sanitizing files while maintaining the original file format helps prevent data breaches and ensure the sanitized files align with secure industry standards.
- Reduced attack surface: Votiro Cloud sanitizes every file passing through ZIA; together, this reduces the risk of cyberattacks originating from file-borne threats.
- Ability to scale: Votiro Cloud and Zscaler ZIA are cloud-based solutions that enable organizations to scale traffic and file ingestion based on their expected workload.

Votiro and Zscaler Workflow



Configuring the Votiro Management Dashboard

Prerequisites

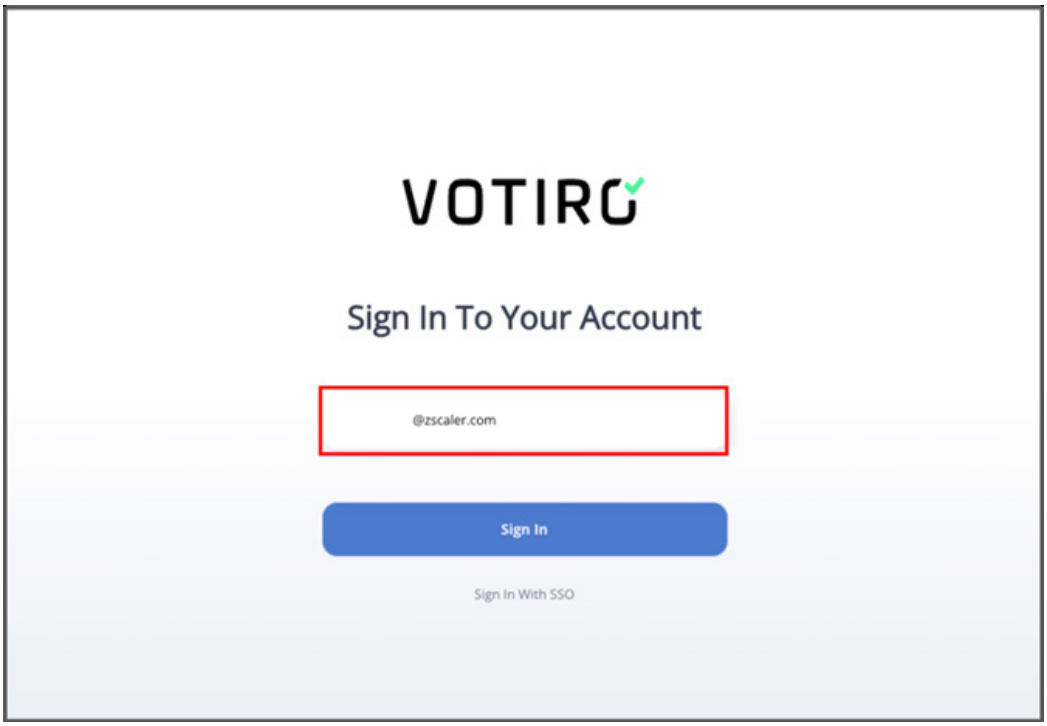
- A licensed Votiro tenant
- Votiro administrator account

Configure the Votiro Service Token

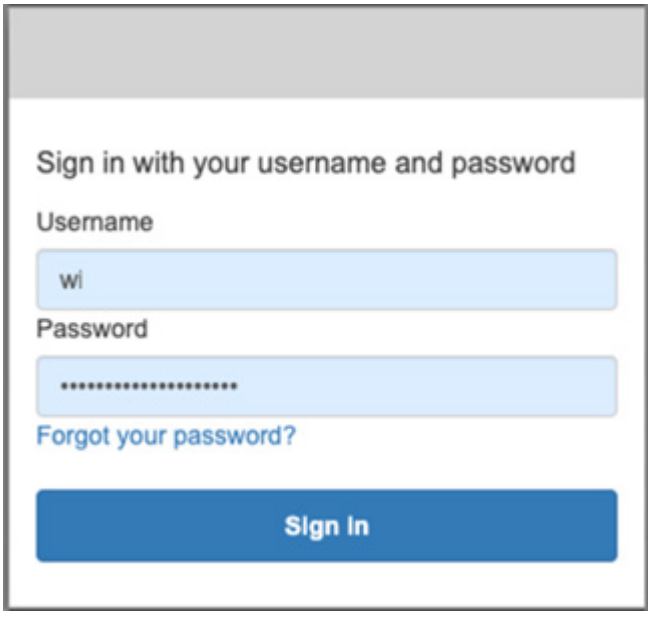
To begin using Votiro and Zscaler Isolation, you must first log in to the Votiro Management Dashboard and obtain a Service Token.

To create the Service Token:

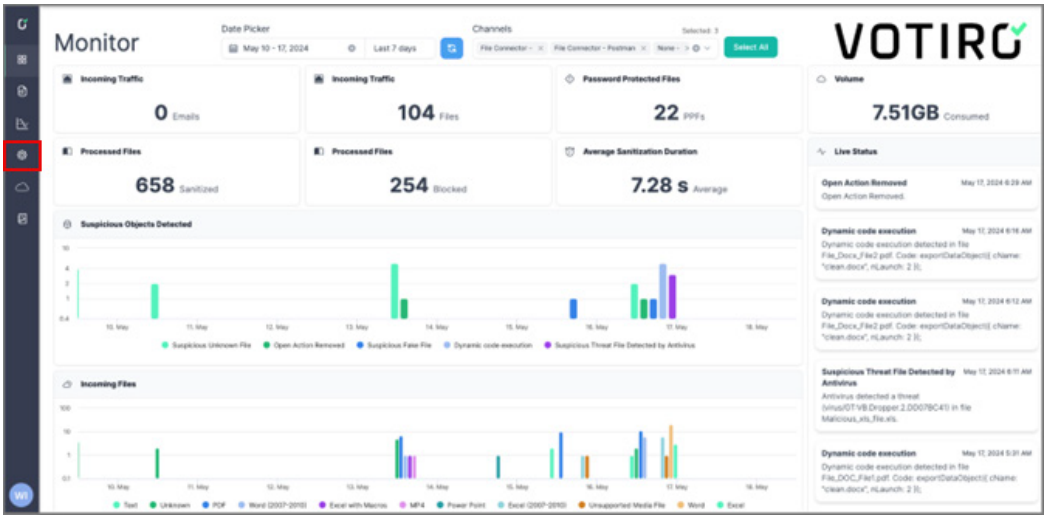
1. Provide the email address registered in the Votiro tenant, then click **Sign in**.



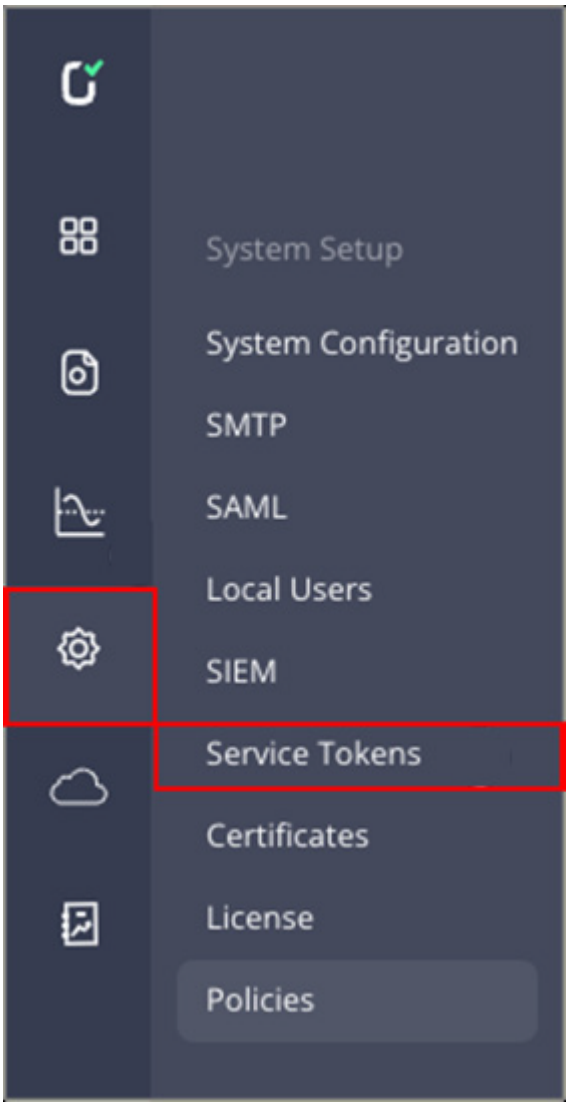
2. Provide your Votiro administrator username and password, then click **Sign in**. The **Votiro Monitor** page is displayed.



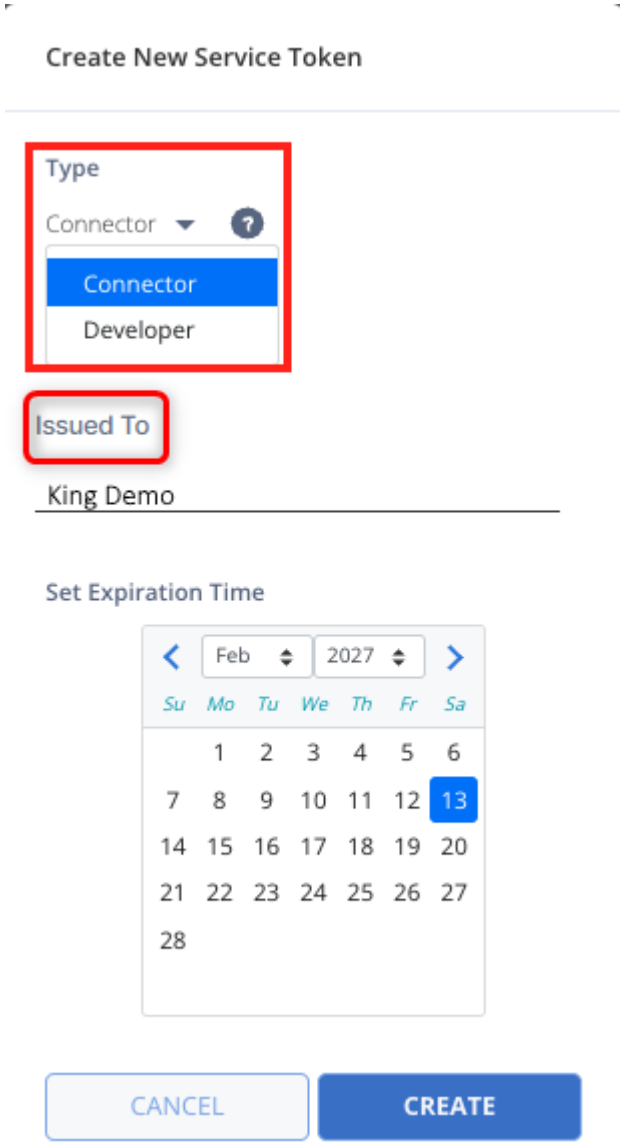
3. Select **Settings** (the Gear icon).



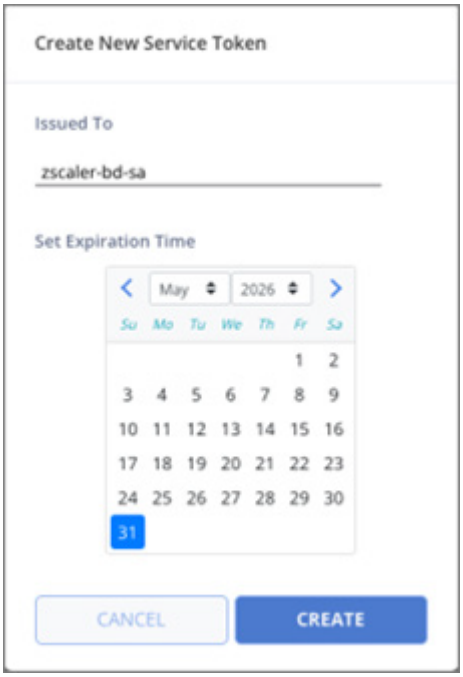
4. Select **Service Tokens**.



5. Select **Create New** in the **Service Tokens** page.



6. 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.
7. Enter a name for the Service Token in the **Issued To** Field.
8. Set the expiration date.
9. Click **Create**. The **Service Token** is displayed.



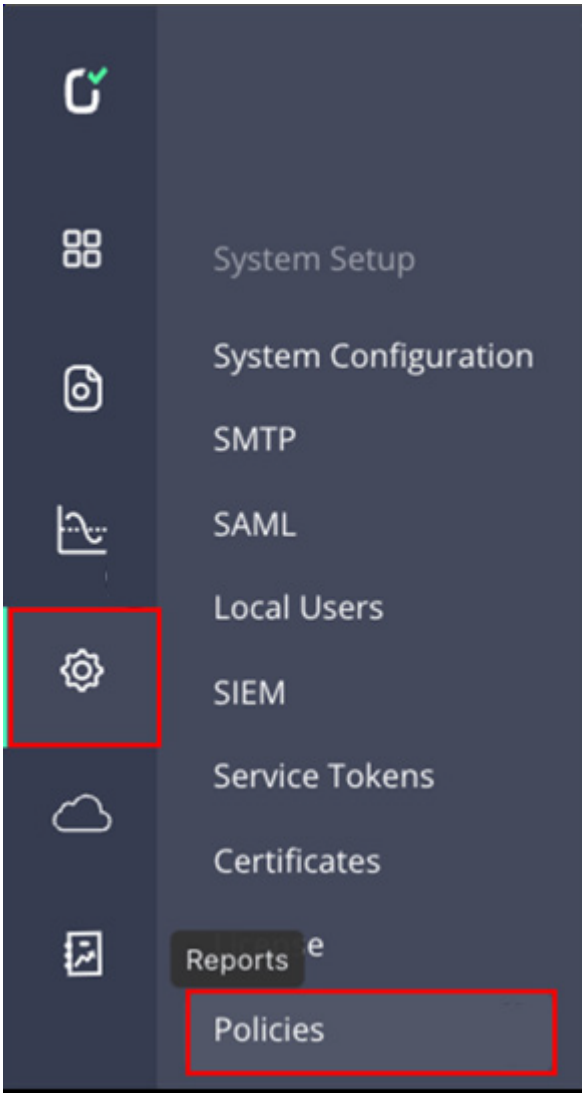
10. Copy and save the **Token** text in a secure location, then click **OK**.

> **Note**: You won't see the Service Token again.

Configure Votiro Policies for Zscaler

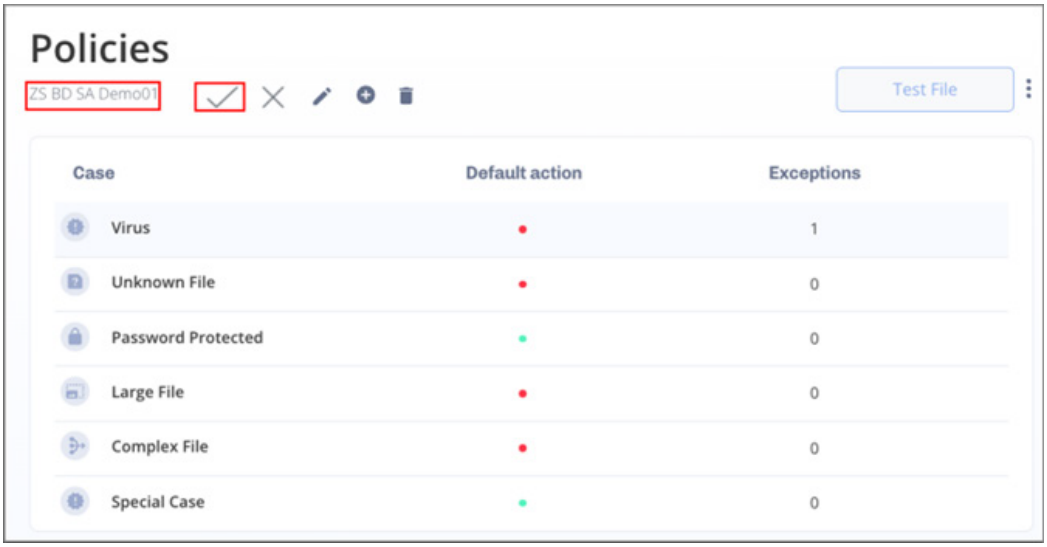
To create a policy:

1. Click **Settings**.
2. Select **Policies**.



3. On the **Policies** page, click the add icon ⊕

4. Provide a name for the new policy and click the checkmark icon ✓ to save the new policy.



Note: In this example, you are keeping the policy with the default actions. For more information regarding Votiro's policy options, refer to Policies.

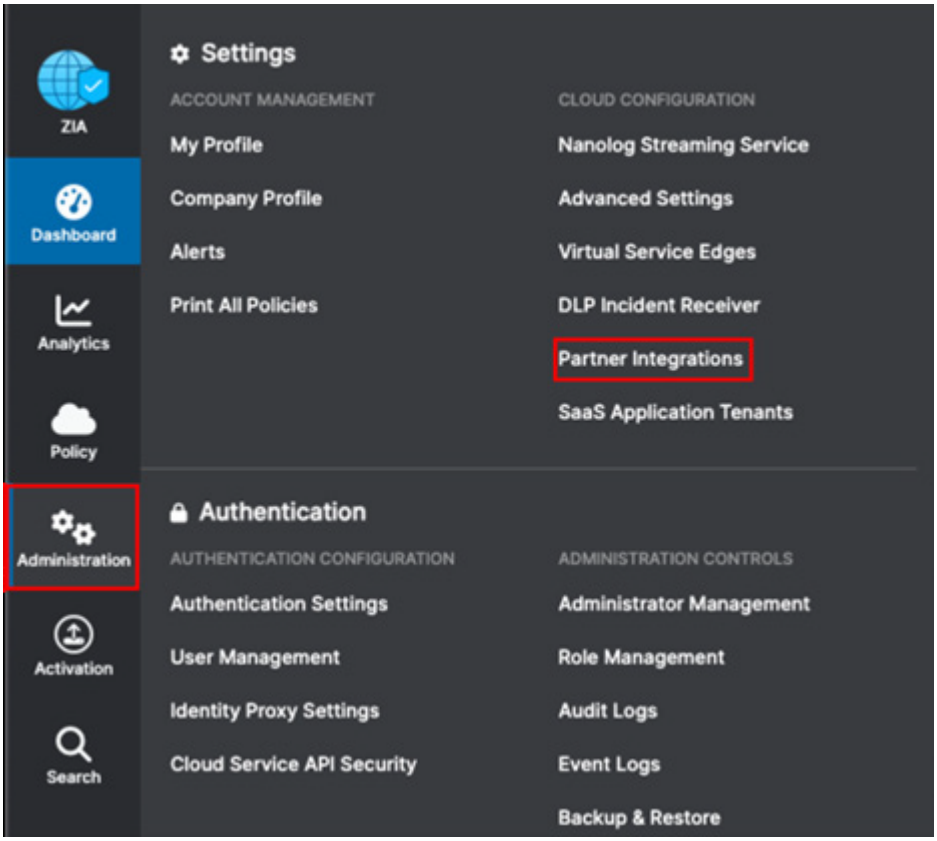
Configuring the ZIA Admin Portal

Prerequisites

- A licensed Zscaler Internet Access Tenant
- Votiro Service Token

Enable Votiro Partner Integration

1. Log in to the ZIA Admin Portal.
2. Go to **Administration** > **Partner Integrations**.

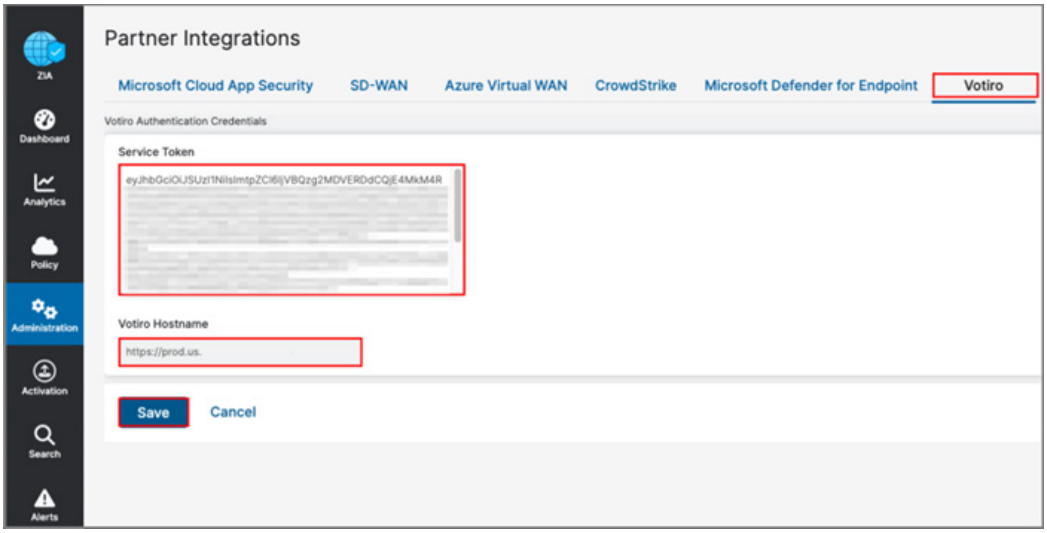


3. Select **Votiro**:

   a. In **Service Token**, enter the Service Token created in Configure the Votiro Service Token.

   b. In Votiro **Hostname**, enter the Votiro Tenant URL.

   c. Click **Save**.



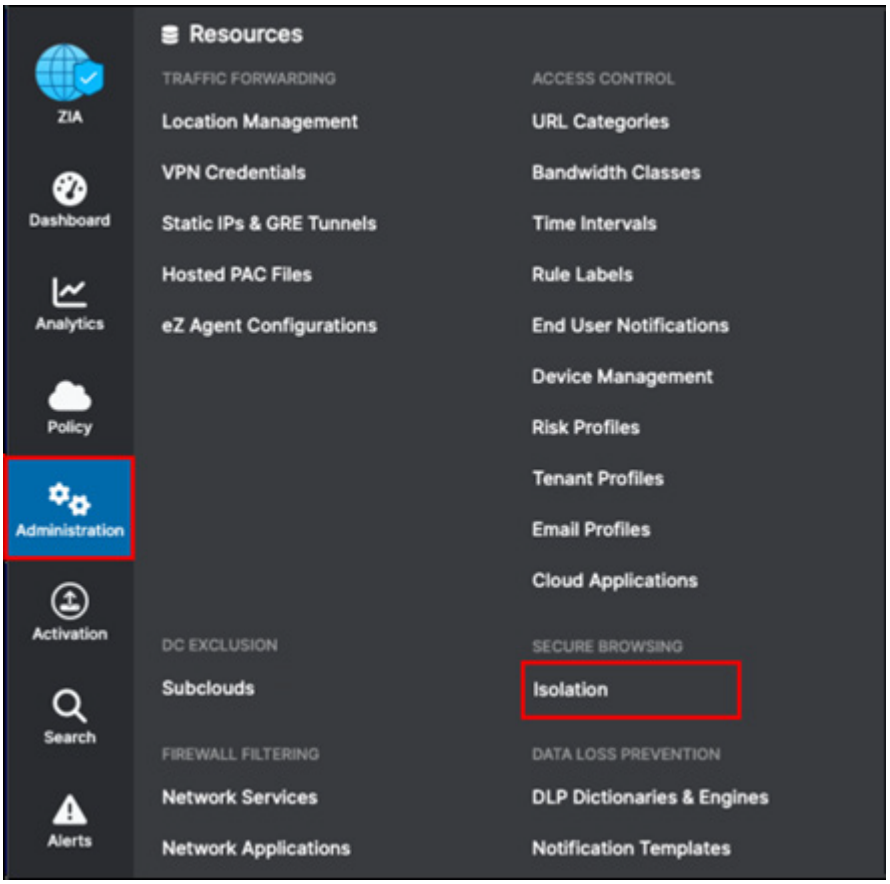
Configuring ZIA Isolation

Prerequisites

- Zscaler Isolation license
- Configure Isolation Profile

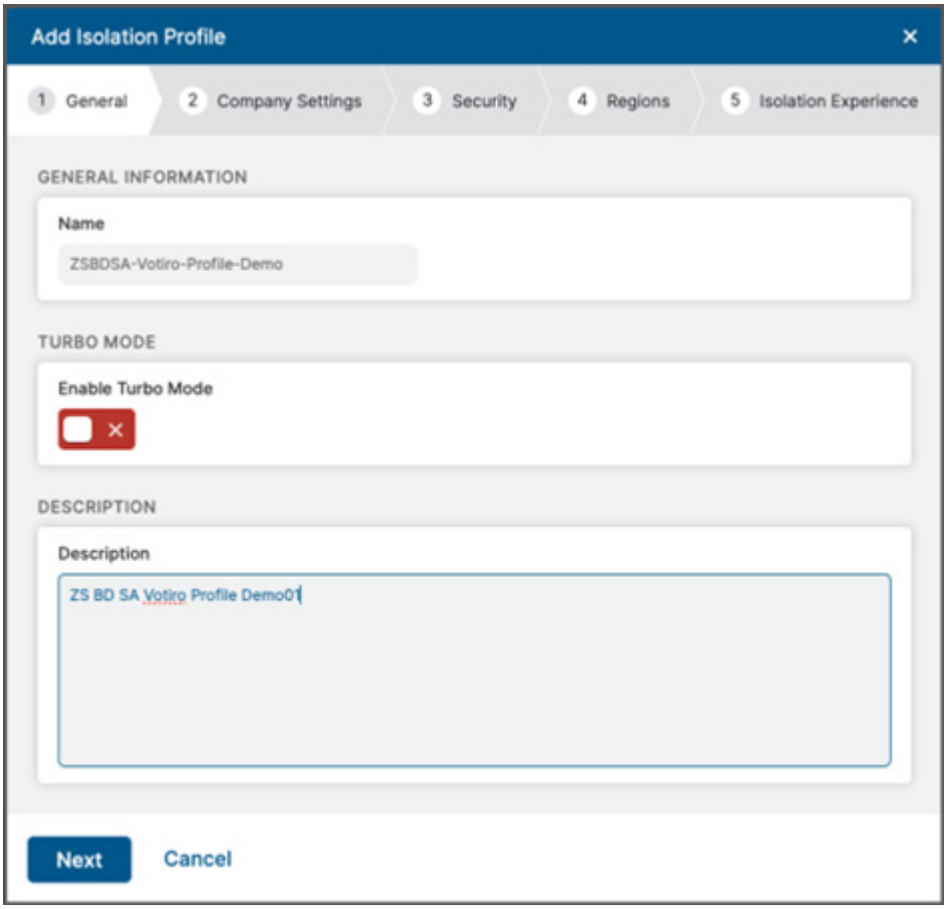
Votiro Integration within the Zscaler Isolation

1. In the ZIA Admin Portal, select **Administration** > **Isolation**.



2. Click **Add Profile**.

3. In the **Add Isolation Profile** window, enter the following fields:
   - **Name**: Enter a name for the ZIA isolation profile.
   - **Description**: (Optional) Enter a description of the profile.



4. Click **Next**.

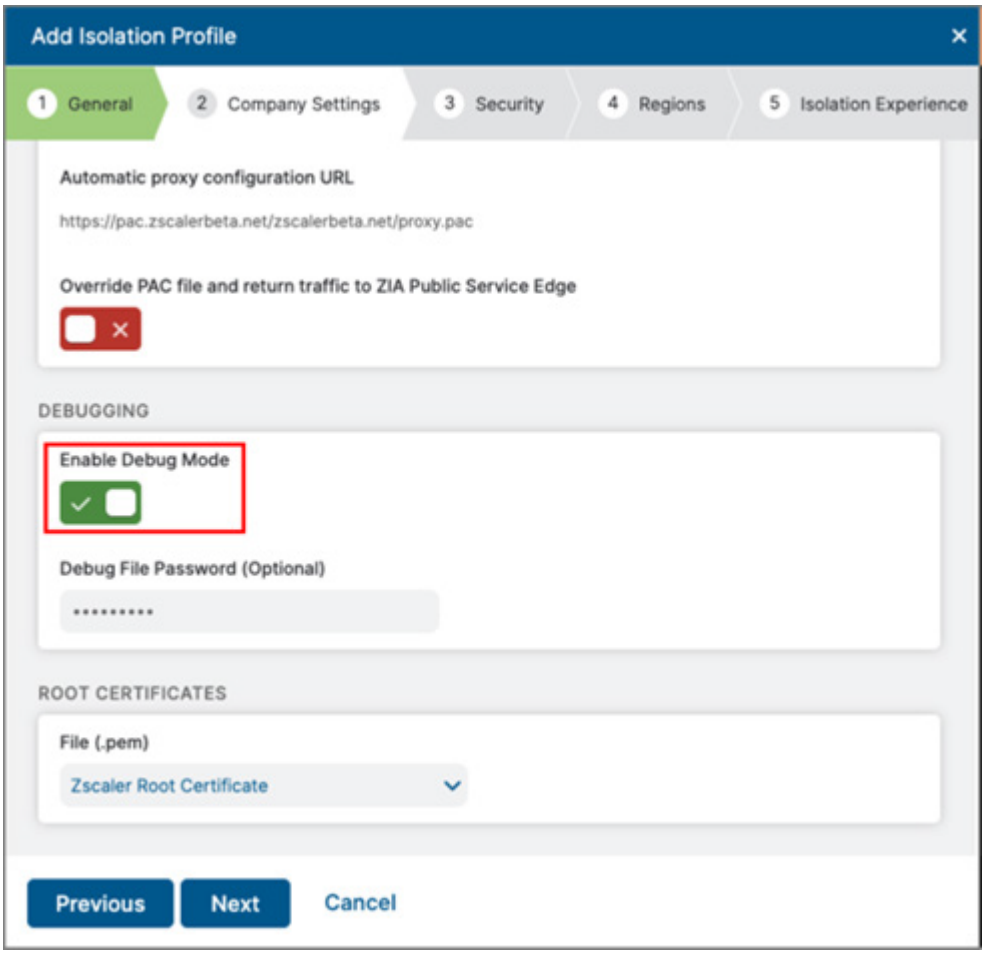
5. On the Company Settings tab, choose to use either the recommended PAC file URL or your own manually configured PAC file URL:

    a. If you select **Use recommended PAC file URL**, the **Automatic proxy configuration URL** field is populated by default with the recommended PAC file from your Hosted PAC Files list in ZIA. The isolation browser configures the PAC file within the endpoint experience containers, and any traffic to the internet from the isolated browser is also forwarded through the ZIA cloud.

    b. Enable or disable **Override PAC File and return traffic to the ZIA Public Service Edge**. The ZIA Public Service Edges use auto-geoproximity, meaning that the traffic is returned to the service edge closest to the location of the user, not the location of the isolation browser.

    c. Enable or disable **Debug Mode**. If you enable it, you can optionally create a Debug File Password for the ZIP file that is created at the end of a debug troubleshoot. Make sure to share the password with the user associated with the isolation profile.

d. In the **Root Certificates** section, select at least one certificate from the **File (.pem)** drop-down menu. The Zscaler Root Certificate that ZIA uses for SSL inspection appears by default in the drop-down menu. If your organization uses custom root certificates for SSL inspection, you can add them before creating isolation profiles.



6. On the **Security** tab:

   a. Enable or disable **Allow local browser rendering**.

   b. Enable or disable **Allow Application Deep Linking**.

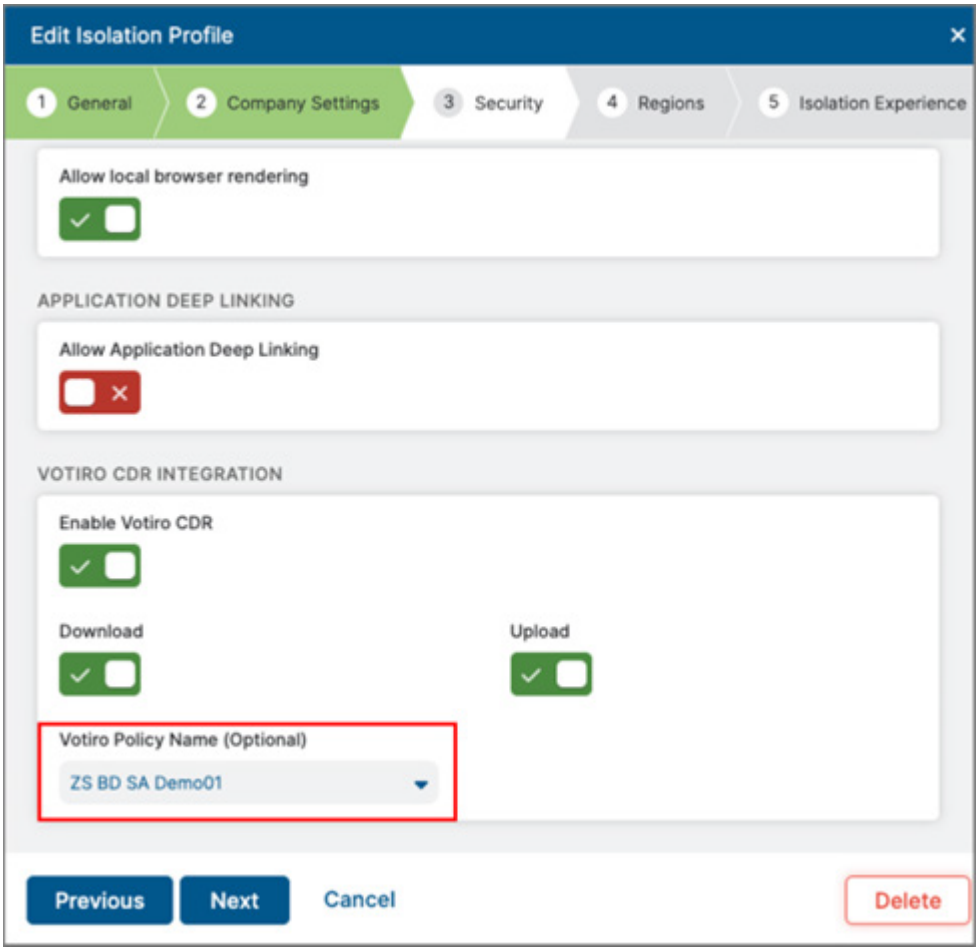
   c. In the **Votiro CDR Integration** section:

      i. **Enable Votiro CDR**: Enable to allow downloaded files to be sanitized by CDR while in Isolation.

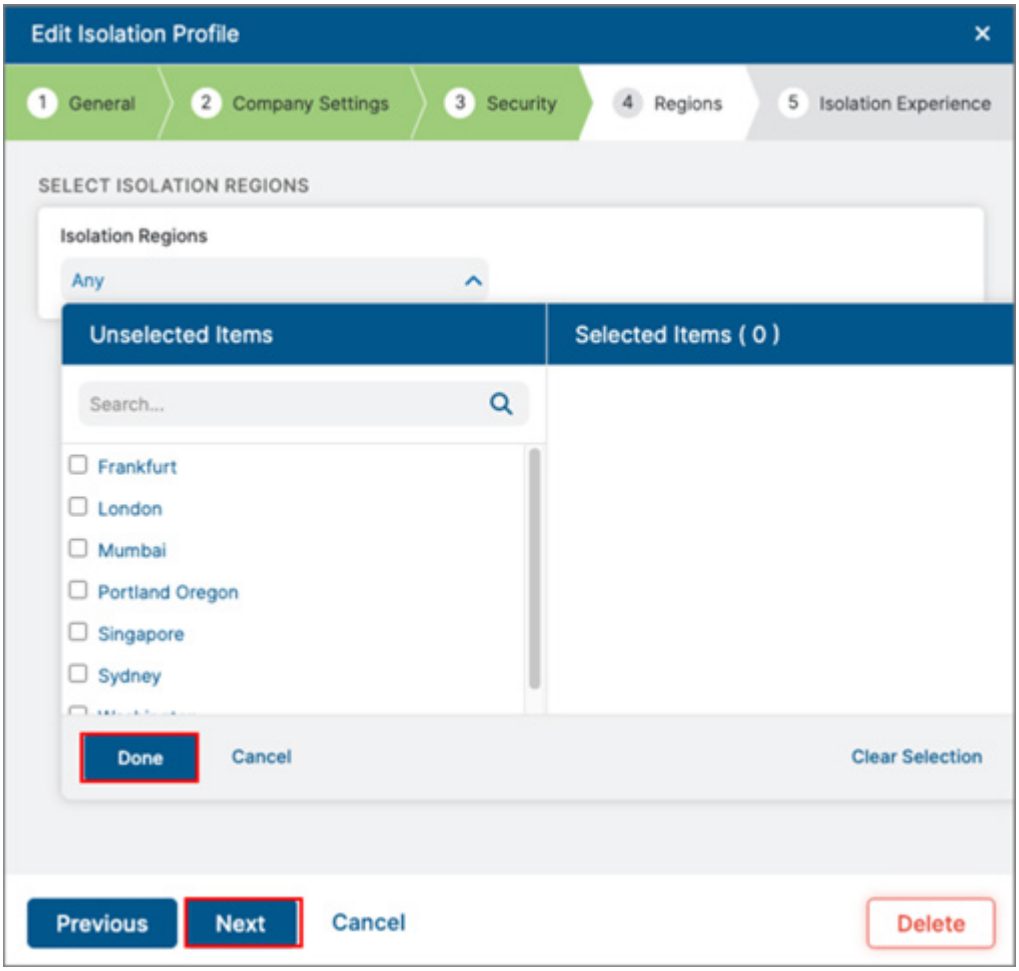
      ii. **Download**: Enable to allow Votiro to sanitize downloaded files.

      iii. **Upload**: Enable to allow Votiro to sanitize uploaded files.

      iv. **Votiro Policy Name**: (Optional) Select a Votiro policy from the drop-down menu. If none is selected, the default Votiro policy is applied.



7. Click **Next**.
8. On the **Regions** tab:
    a. From the drop-down menu, select at least two regions. The isolation containers are leased to the user only from the selected regions based on the least network latency.
    b. Click **Done**.



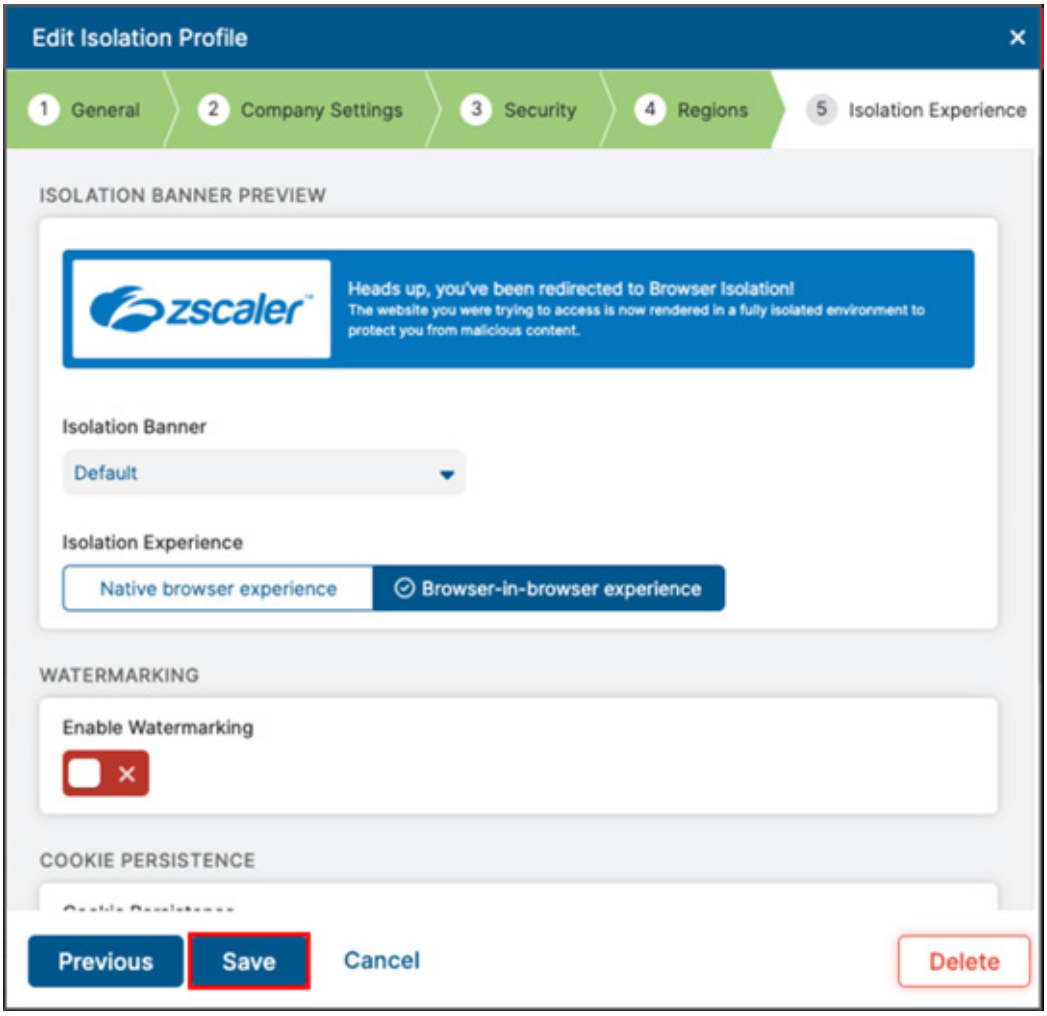
9. Click **Next**.

10. On the **Isolation Experience** tab:

    a. From the drop-down menu, select an **Isolation Banner**. The option you choose shows a preview banner in the window. Choose from existing banners or create custom isolation banners to use for your isolation profiles. To learn more, see Adding a Banner Theme for the Isolation End User Notification in ZIA.

    b. Select the **Isolation Experience** mode:

    - **Native browser experience**: This mode provides the user with a browsing experience similar to accessing the native web page with a typical browser. The user can customize this view.
    - **Browser-in-browser experience**: This mode provides the user with the complete look and feel of an isolated session experience. To learn more, see User Experience Modes in Isolation.

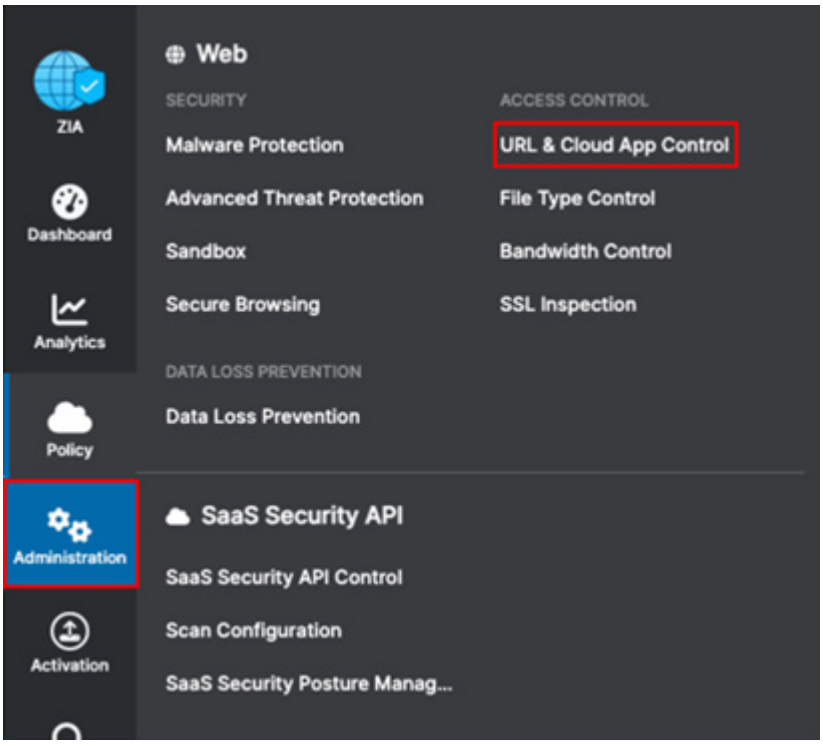


11. Click **Save**.

Configure Zscaler URL Filtering Policy

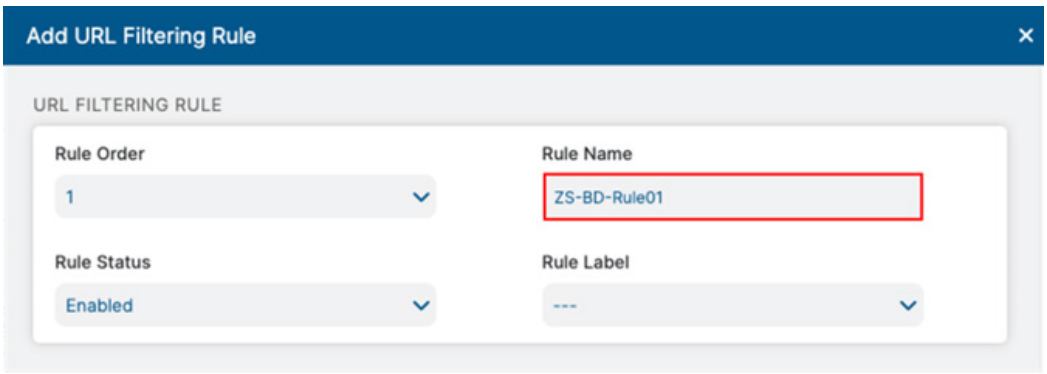
After the Votiro integration is enabled, and the Isolation profile is configured, you must create a URL filtering rule, and then associate the isolation profile.

1. In the ZIA Admin Portal, select **Administration** > **URL & Cloud App Control**.



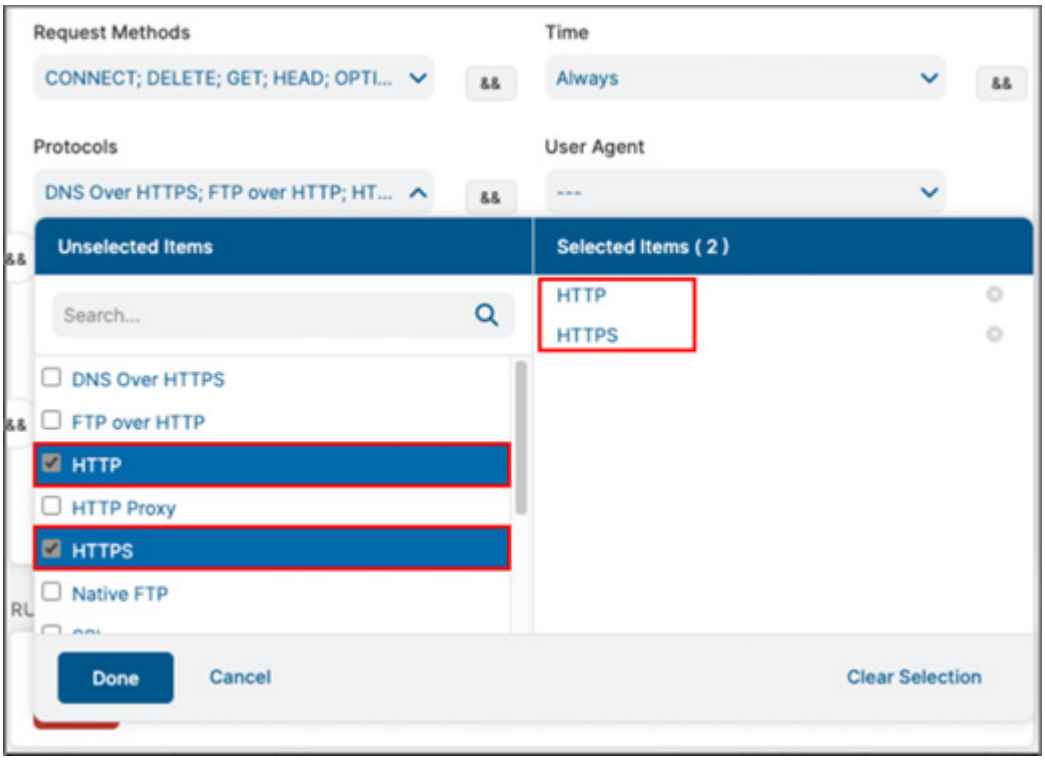
2. Click **Add URL Filtering Rule**.

   a. Enter a **Rule Name** for the new rule.



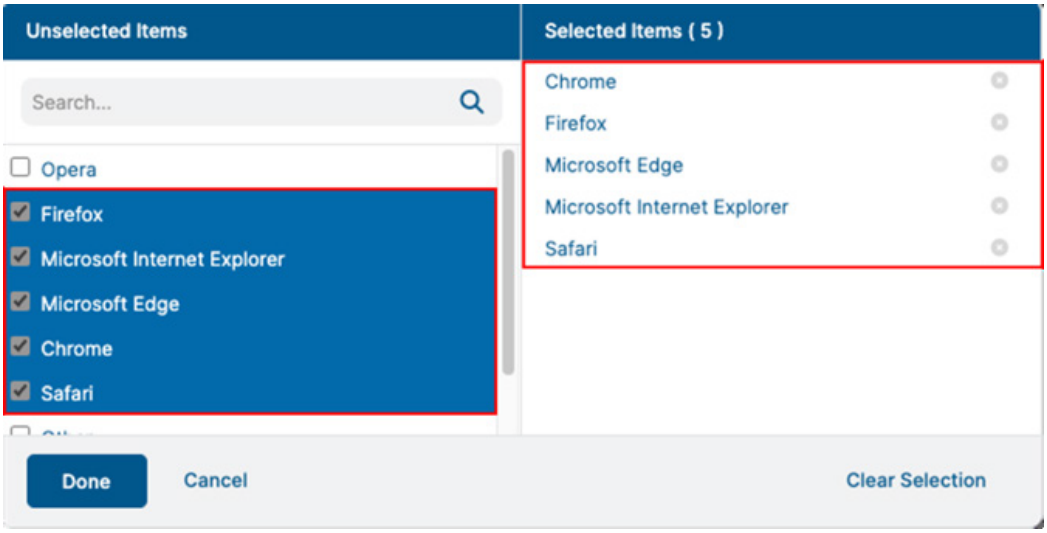
3. In the Protocols option, select **HTTP** and **HTTPS**.

Note: These are the only protocols supported by Zscaler's Isolation solution.



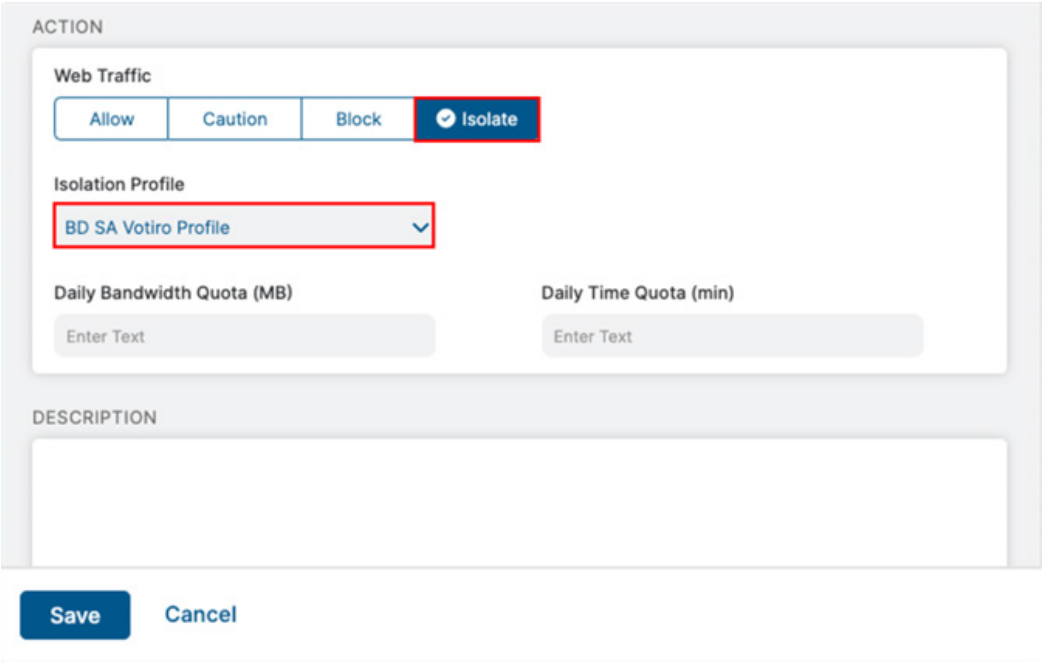
4. Click **Done**.

5. In the User Agent option, select the browser criteria for which this rule must be applied.



6. In the **Action** section under **Web Traffic**, select **Isolate**.

a. Under **Isolation Profile**, select the profile created in Configuring ZIA Isolation.



7. Click **Save**.

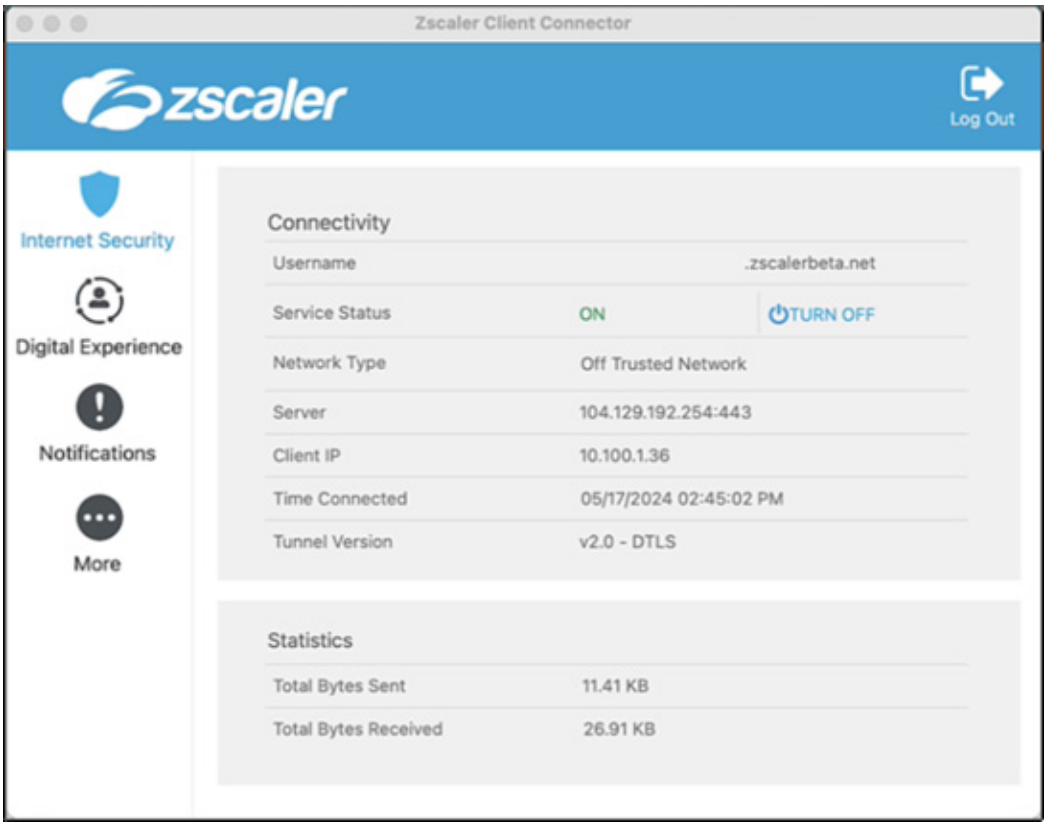
Testing ZIA Isolation and Votiro CDR

Prerequisites

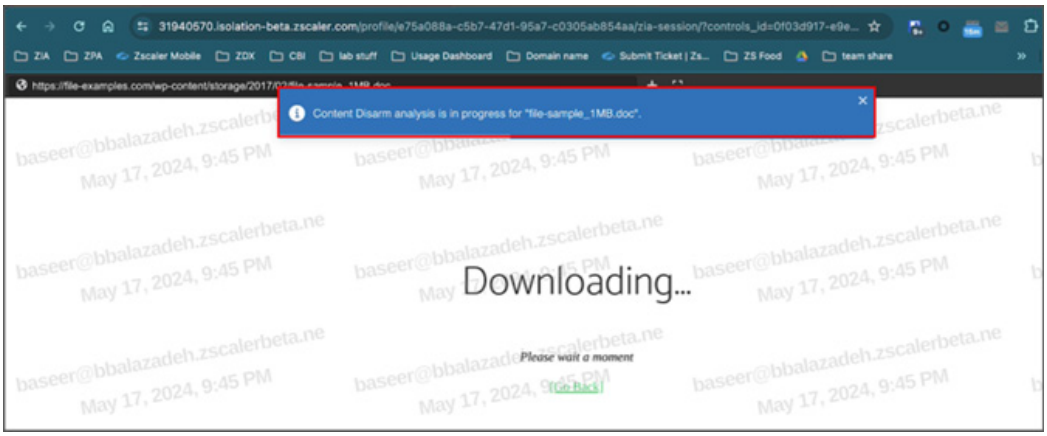
- Votiro tenant configuration
- Isolation Profile

End-to-End Testing

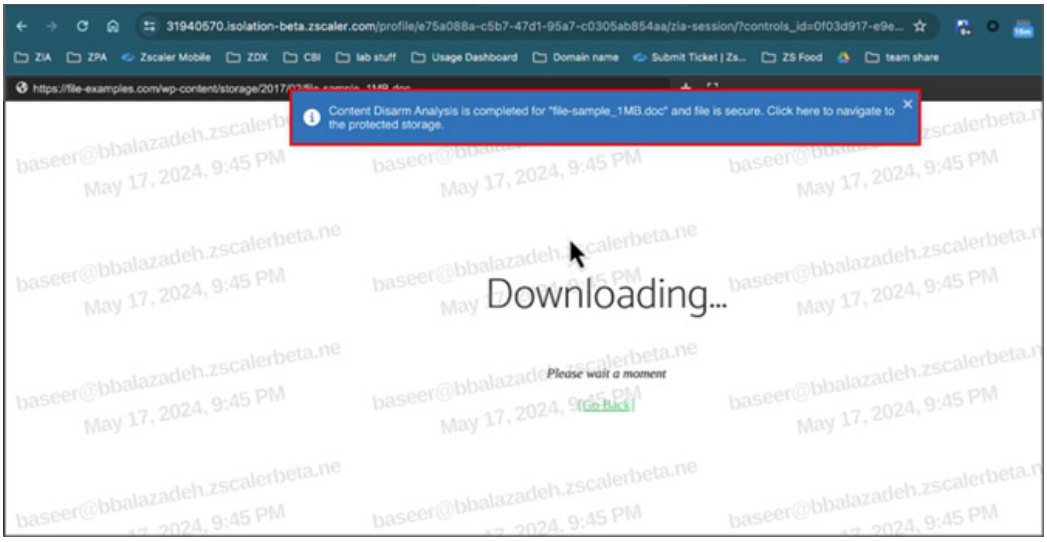
1. Connect to Zscaler Client Connector.



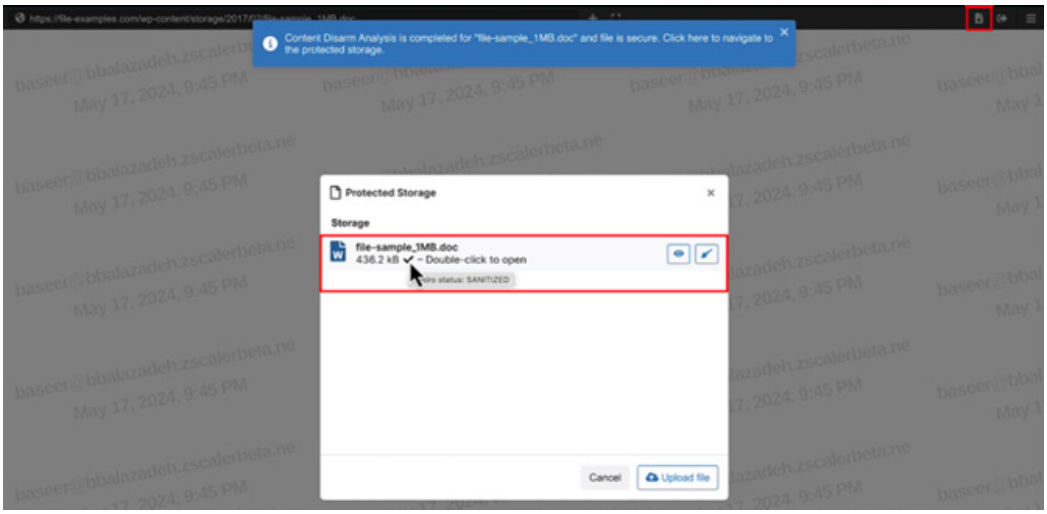
2. When downloading a file that matches the URL Filtering Policy, the request is redirected to Zscaler Isolation and the Content Disarm analysis process starts.



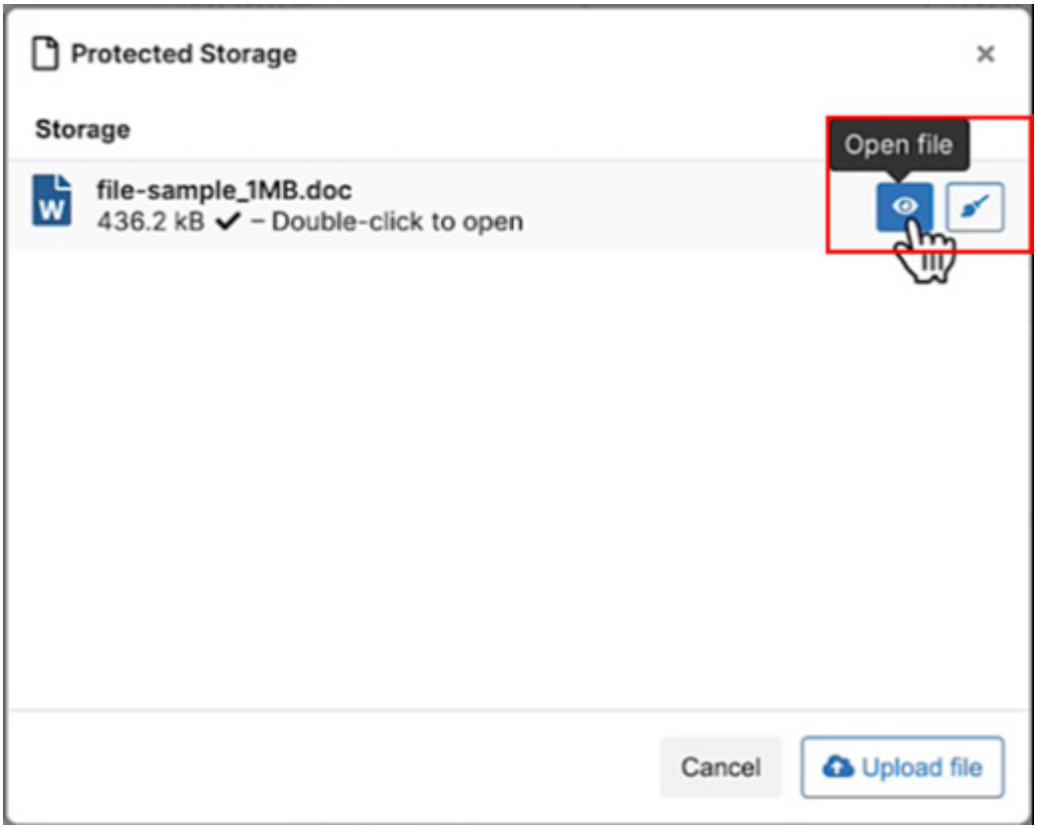
3. After the CDR analysis is complete, the banner message in the following figure is displayed.



4. Go to **Protected Storage** to open the sanitized file.

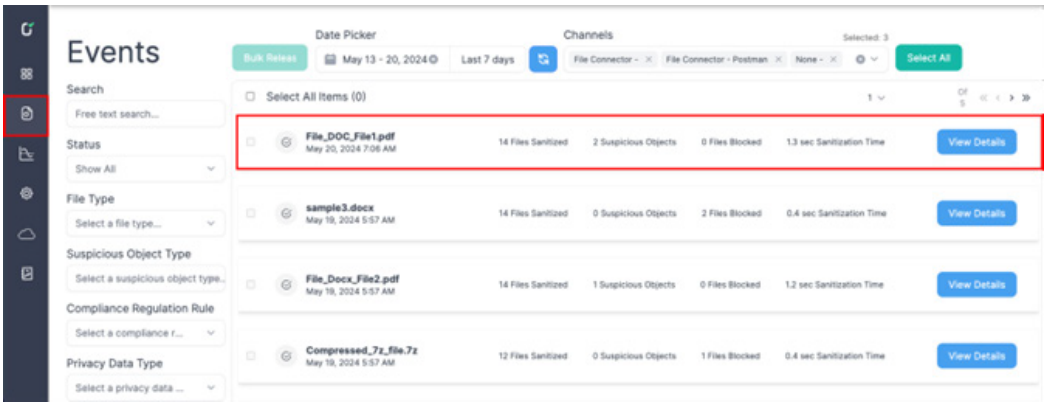


5. Click the **View** icon to open the sanitized file within Isolation.

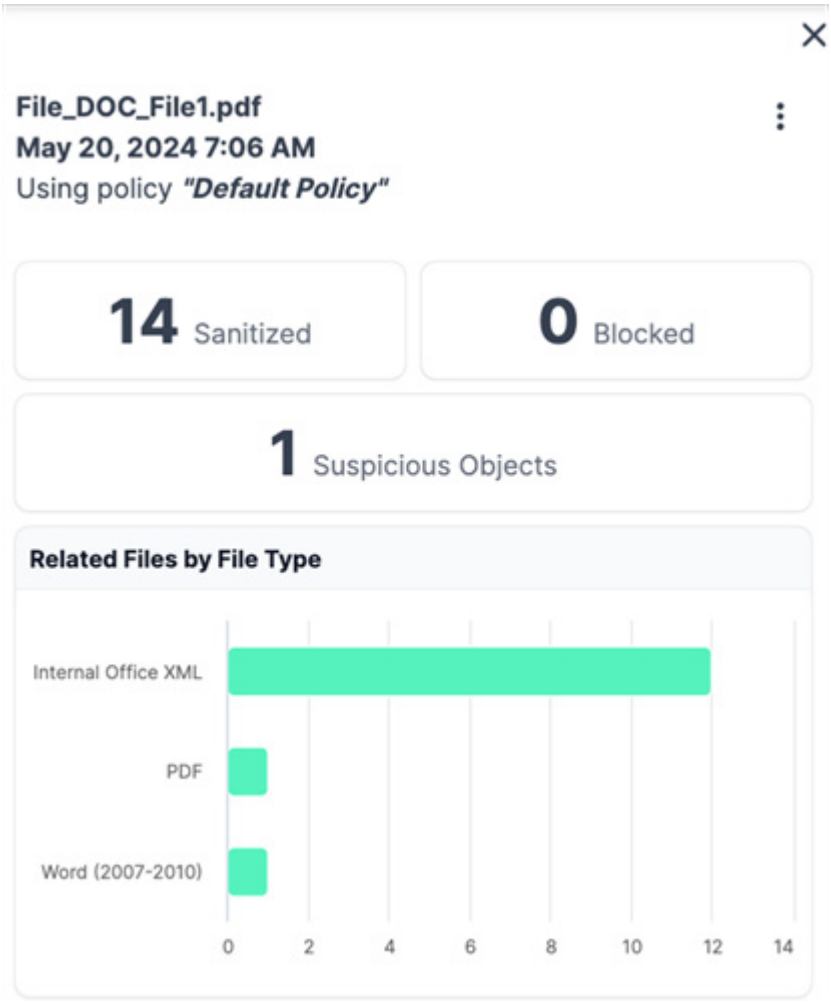


Analyzing Events in the Votiro Management Dashboard

1. Log in to the Votiro Management Dashboard, then click **Events**.



2. Click **View Details**.



Use Cases

The following sections describe the use cases for a Zscaler and Votiro integration.

Use Case 1: Download of Files to Managed Endpoints

Customers use ZIA and the associated services to ensure that no malicious files are downloaded onto managed end points. However, in certain circumstances, they also must ensure that the file downloaded is sanitized so that certain active content and file capabilities are turned off. This approach ensures that the files are not weaponized in the future or used for any malicious purpose.

To achieve this, customers use file sanitization CDR solutions such as Votiro. Customers expect that the files downloaded onto the end user's computer are sanitized by Votiro so that the file delivered to the user is not only benign, but also has any capabilities that can later be used to weaponize the file or make the file vulnerable are turned off or sanitized.

The CDR service is expected to perform actions such as removing printer settings, sanitizing files with dynamic data exchange (DDE), removing metadata, removing external links, removing suspicious links, removing external images, removing macros, VBA macros, etc.

Use Case 2: Upload of Files to Private and SaaS Web Applications

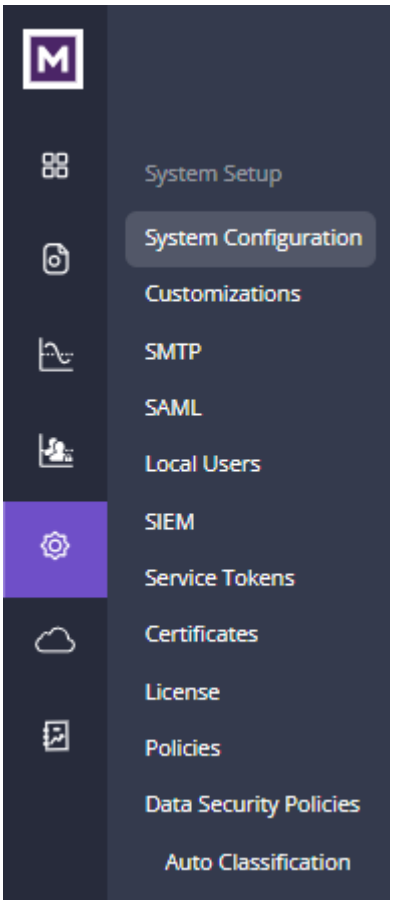
Customers have private or SaaS applications that are critical in nature. In some cases, however, these applications must be accessed from unmanaged devices.

The user on the other end of these devices could be employees or third-party contractors. In some cases, uploading files to the application becomes a critical part of the user workflow. For example, an insurance agent or an investment broker could need to upload client documents to an internal web portal for legal and documentation purposes.

Secure access to these applications is provided by the user of browser isolation, however if the user is allowed to upload files to the application, it becomes critical to ensure that the files being uploaded to the application are not malicious or do not make the application itself vulnerable due to vulnerabilities in the uploaded file. In such cases, the use of a CDR solution such as Votiro to sanitize the uploaded files ensures application security.

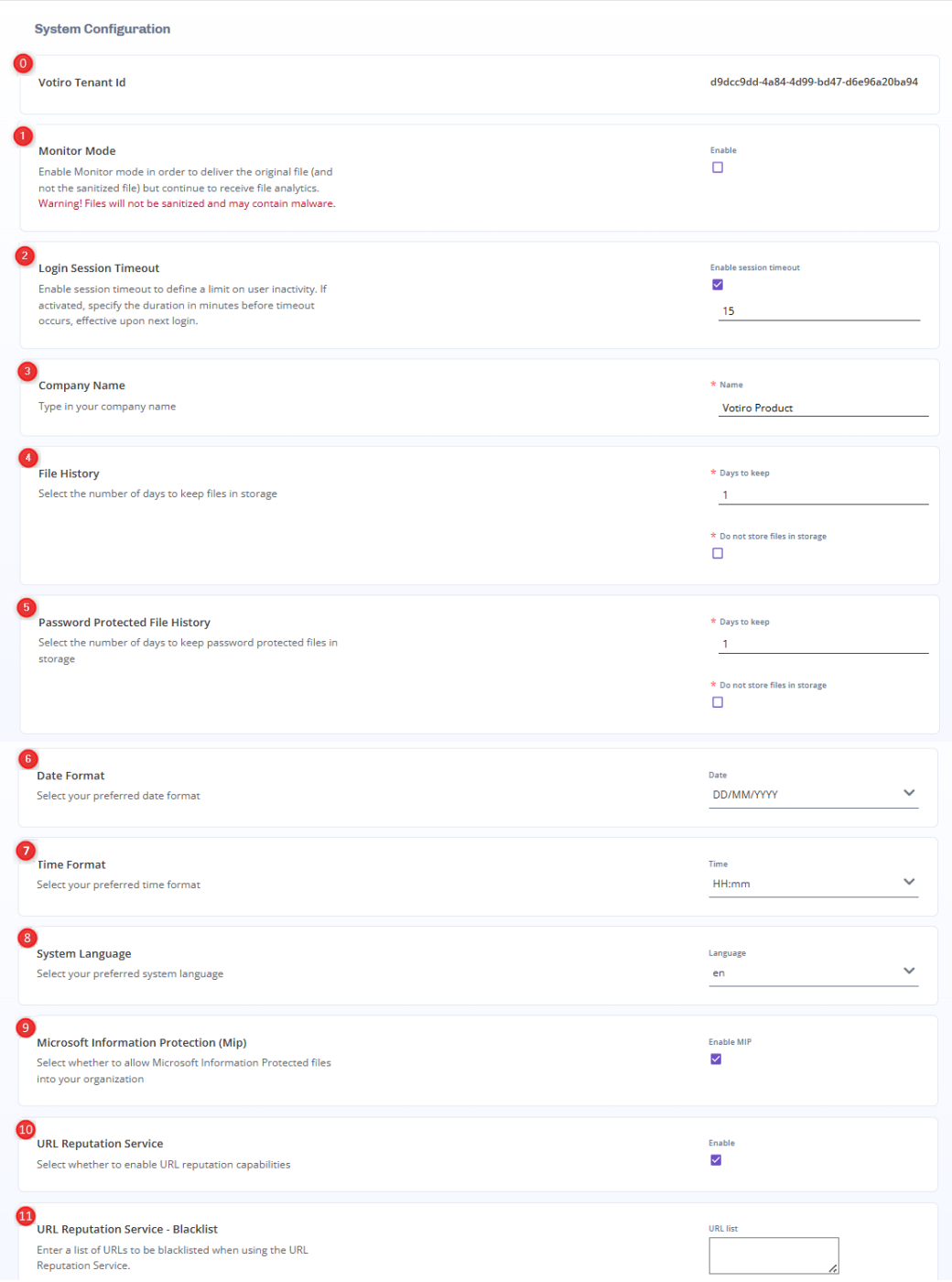
2.18 Configuring Settings

Use the System Setup page to configure settings in Votiro's Management Dashboard.



2.18.1 System Configuration

To get to the System Configuration page, from the navigation pane on the left, click **Settings** > **System Configuration**.



The System Configuration page contains the following fields:

Element	Field	Description
0	Votiro Tenant Id	Votiro Tenant Id

Element	Field	Description
1	Monitor Mode	Monitor Mode is intended for potential customers to experience our product before purchase and has the following features: ■ Experience and test our product with the customer's files. ■ Get insights and analytics using our Management dashboards. ■ Does not interrupt the organization's workflow. Monitor Mode sanitizes files to gather file analytics, but the user always gets the "original" file. When Monitor Mode is enabled, a red frame appears when running the product to reduce confusion with connectors indication. By default, Monitor Mode is disabled for editing. To enable this feature, please contact Votiro support.
2	Login Session Timeout	Enable session timeout to define a limit on user inactivity. If activated, specify a duration in minutes before timeout occurs, effective upon next login.
3	Company Name	Specify the name of your organization. The company name appears in activity reports. See Generating Reports on page 314.

Element	Field	Description
4	File History	Specify the number of days to keep files in storage. The default is **30** days. If the box **Do not store files in storage** is checked, standard files are stored for five minutes. After "PublishDone", standard files are deleted. The files aren't saved in the blob, only in Votiro cache, as part of the sanitization process. During that five minute time period, the original and sanitized files are available to download. At the end of the that time period, local storage will be deleted, and the uploaded files will not be saved in our storage. Existing original/sanitized files will be deleted as well up to 24 hours. However, large files, above 50MB in size, will be deleted one hour after the upload. If the box **Do not store files in storage** is checked, the user will not be able to release the original file or get the original/sanitized files. The user will get an error (because we are not saving the original/sanitized files due to the Main **File History** configuration: **Do not store files in storage**). **Note**: Password-protected files will be reachable only from the password-protected portal.
5	Password Protected File History	Specify the number of days the system saves password-protected files in storage. The default is **180** days. **Note** After the configured period, the original file is deleted and cannot be retrieved through the dashboard. If the box **Do not store files in storage** is checked, local storage will be deleted, and the uploaded files will not be saved in our storage. Existing original/sanitized files will be deleted as well up to 24 hours from upload. However, files above 50MB in size will be deleted one hour after the upload. **Note**: When trying to download the original/sanitized file from the Management console, the user will get an error (because we are not saving the original/sanitized files due to the Main **File History** configuration: **Do not store files in storage**).
6	Date Format	Select your preferred date format for the display of information in the dashboard --either MM/DD/YYYY or DD/MM/YYYY.

Element	Field	Description
7	Time Format	Select your preferred time format for the display of information in the dashboard -- either a 12-hour clock or 24-hour clock, using the format **HH:MM** or **HH:MM (AM/PM)**.
8	System Language	Select your preferred system language. To add languages to the list you must translate Dashboard dictionary and upload the translation. The default language is **EN**, English.
9	Microsoft Information Protection (Mip)	Select whether to allow Microsoft Information Protected files into your organization. MIP protects data and prevents data loss across Microsoft 365 apps, services, on-premises locations, devices, and third-party apps and services. The site http://login.microsoftonline.com/ is allowed.
10	Url Reputation Service	Select whether to enable URL reputation capabilities. After enabling, navigate to Votiro Policies for adjusting URL Reputation for supported file types (Email, PDF, DOC, DOCX, XLSX).
11	Url Reputation Service - Blacklist	Enter a list of URLs to be blacklisted when using the URL Reputation Service.

Note

Fields marked with a red asterisk * are mandatory, to be completed.

Monitor Mode

After enabling Monitor Mode:

- All files from every source will be sent to Votiro product inspection and analysis.
- The customer will receive the original file.
- The customer will be able to get a full experience of using our product.
- The customer will be able to get insightful analytics on threat activity and PII (Personal Identifiable Information) using the Votiro Management console.

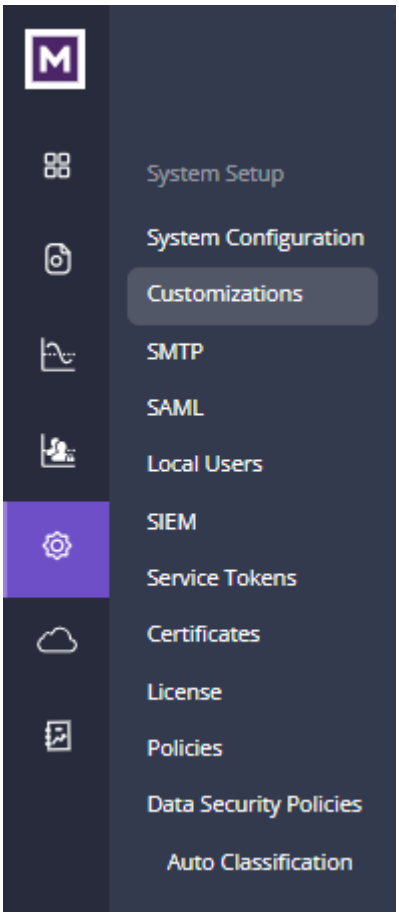
Note the current limitation:

- When Monitor Mode is enabled, it is enforced on all file sources. There is no option to specify only one file source to be in Monitor Mode.

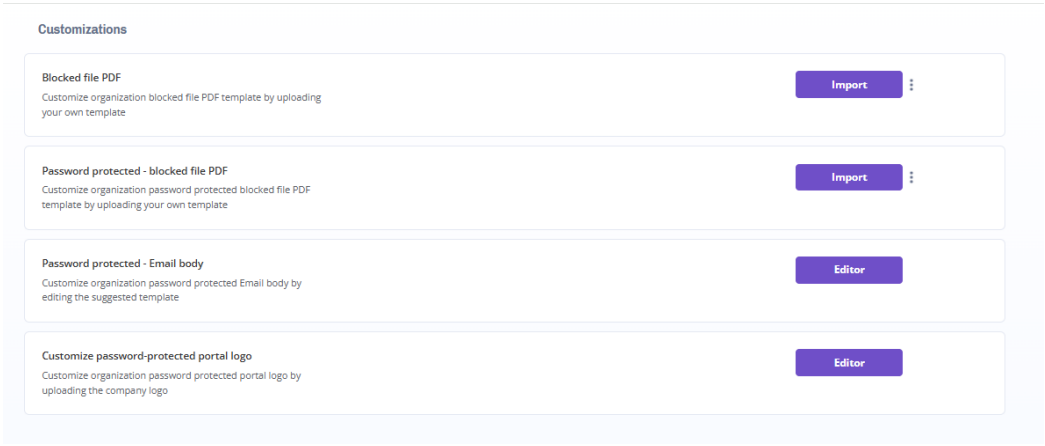
2.18.2 Customizations

The Customizations page enables the user to customize the blocked file PDF template, password protected blocked file PDF template as well as the password protected email body.

To get to the Customizations page from the navigation pane on the left, click **Settings** > **Customizations**.



The **Customizations** page is displayed:



The customizations available are:

- **Blocked file PDF** - customize the organization's blocked file PDF template by uploading your own template. See Customizing Blocked File Templates.

- **Password protected - blocked file PDF** - customize the organization's password protected blocked file PDF template by uploading your own template. See See Customizing Blocked File Templates.
- **Password protected - Email body** - customize the organization's password protected Email body by editing the suggested template

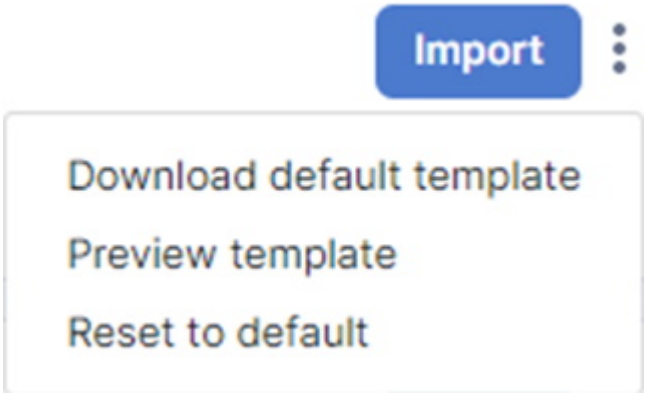
Customizing Blocked File Templates

Votiro provides a default blocked file template to the customer. The customer then has three options:

- Use the default template as is
- Customize the default template
- Import a customized template

Using the Default Template

1. Click on the three dots to the right of the **Import** button.
   The following menu opens:



2. Select **Download default template**.
3. The default template is downloaded.

Customizing the Default Template

1. Download the default template by selecting **Download default template**.
2. Edit the downloaded template as desired.

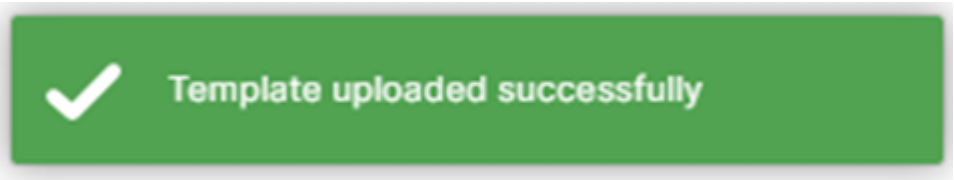
Importing a Customized Template

To upload a blocked file PDF template or Password Protected blocked file template:

1. Click on the **Import** button.
2. An explorer window opens. Navigate to the desired template file to import and select it.
3. The import process begins, and a progress bar is displayed.

4. When the import process completes, a message is displayed.

    a. If the import is successful, the following message appears:

    Each blocked file will be replaced with the updated template.

    b. If the import is unsuccessful, an error message is displayed:

    - If the template file type is not RTF, the following message appears:
      The uploaded template should be an RTF file
    - For any other error, the following message appears:
      The upload template process failed. Please contact Votiro support.

As you make configuration changes the **Items Changed** count increases.

To save the changes click **Save Changes**. A confirmation message will appear advising that you will not be able to recover the previous configuration settings. Click **OK** to proceed with saving the changes made to the configuration settings, or click **Cancel** to return.

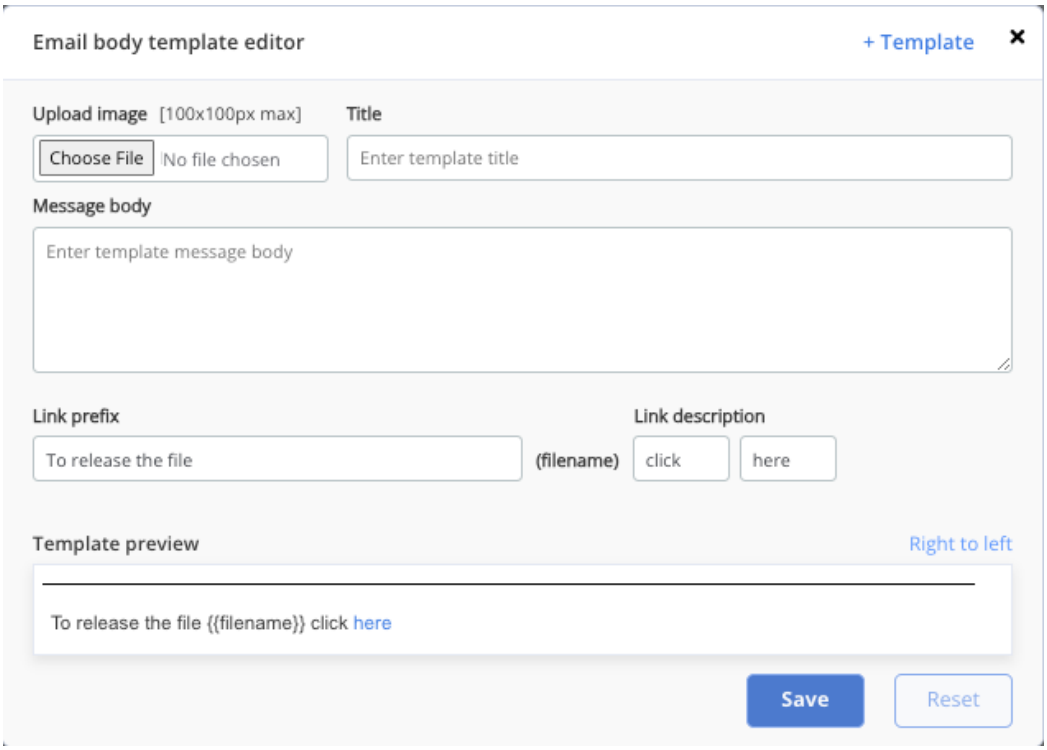
To abandon the changes click **Reset**, your system configuration settings will remain unchanged.

Customizing Email Body Templates

> **Note**:
> Currently the customized email template is not supported in the TNEF email format.

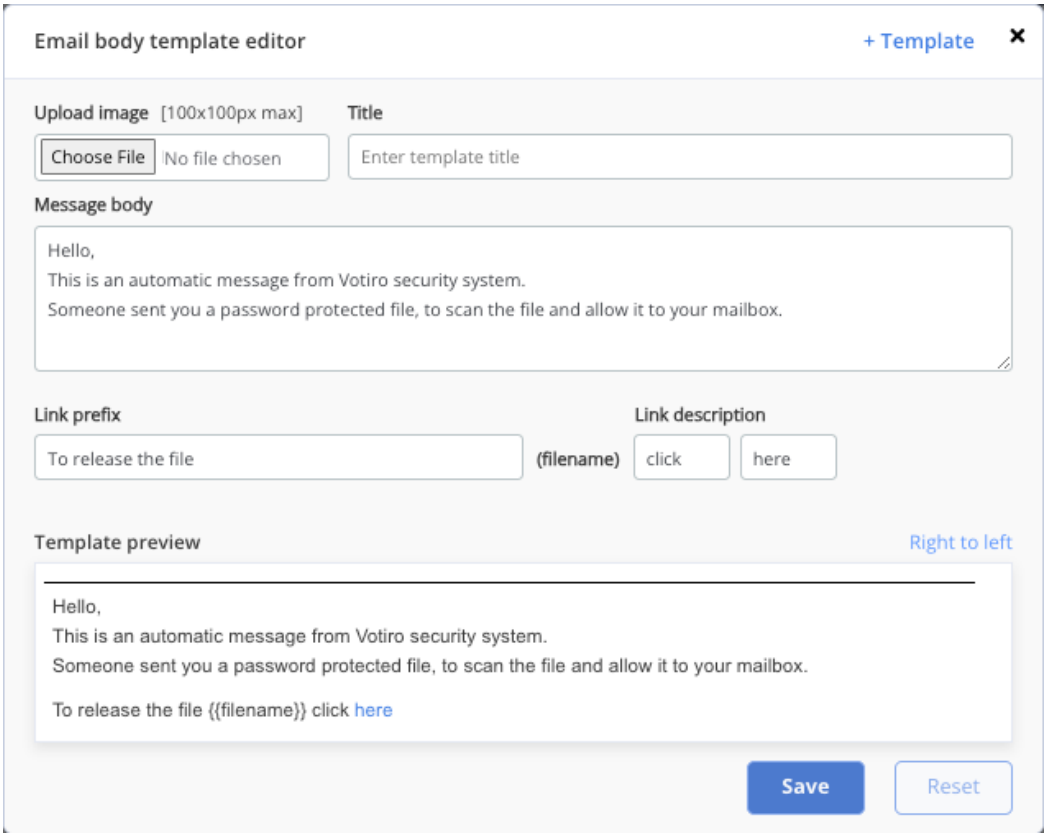
To customize the Email body template:

1. Click on the **Editor** button.

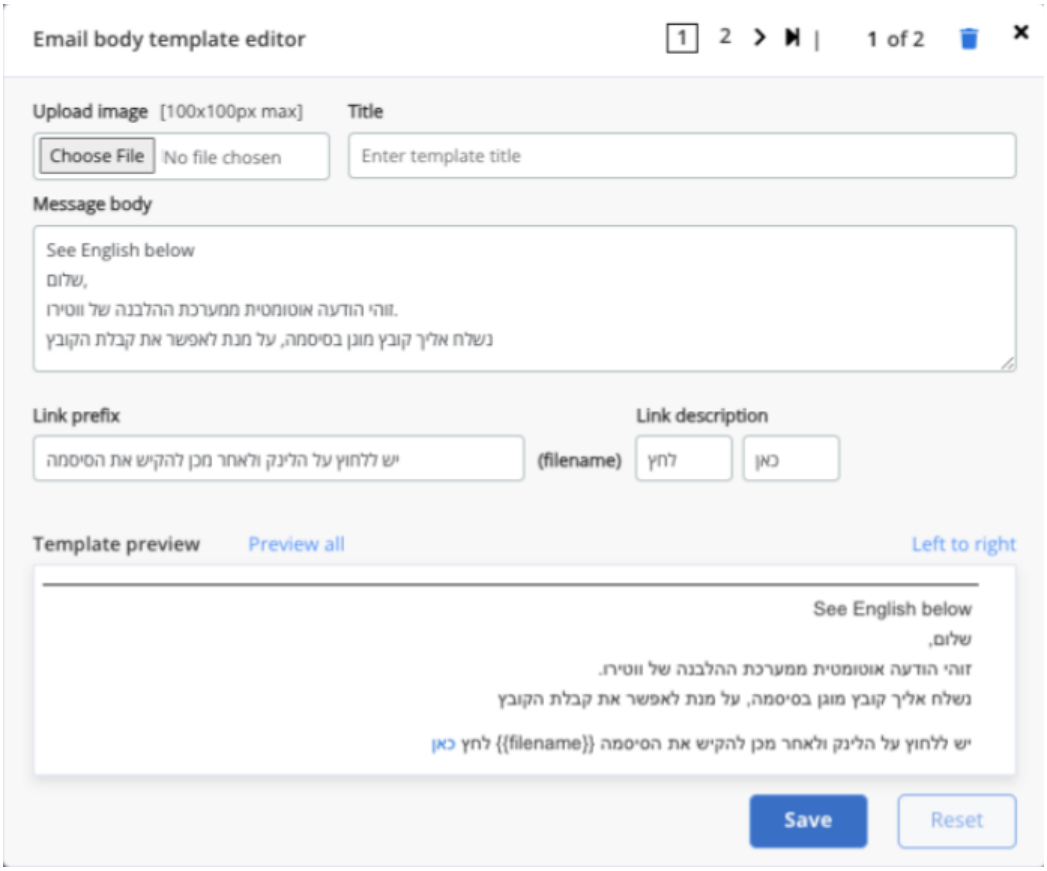


2. You can customize the template by:

- Logo (**Upload image**) - press **Choose File** to upload an image
- **Title** - enter the template title in the text box
- **Message body** - enter the template message body in the text box
- Release file link message (**Link prefix** and **Link description**) - enter the **Link prefix** text in the text box, and the **Link description** in the two boxes.

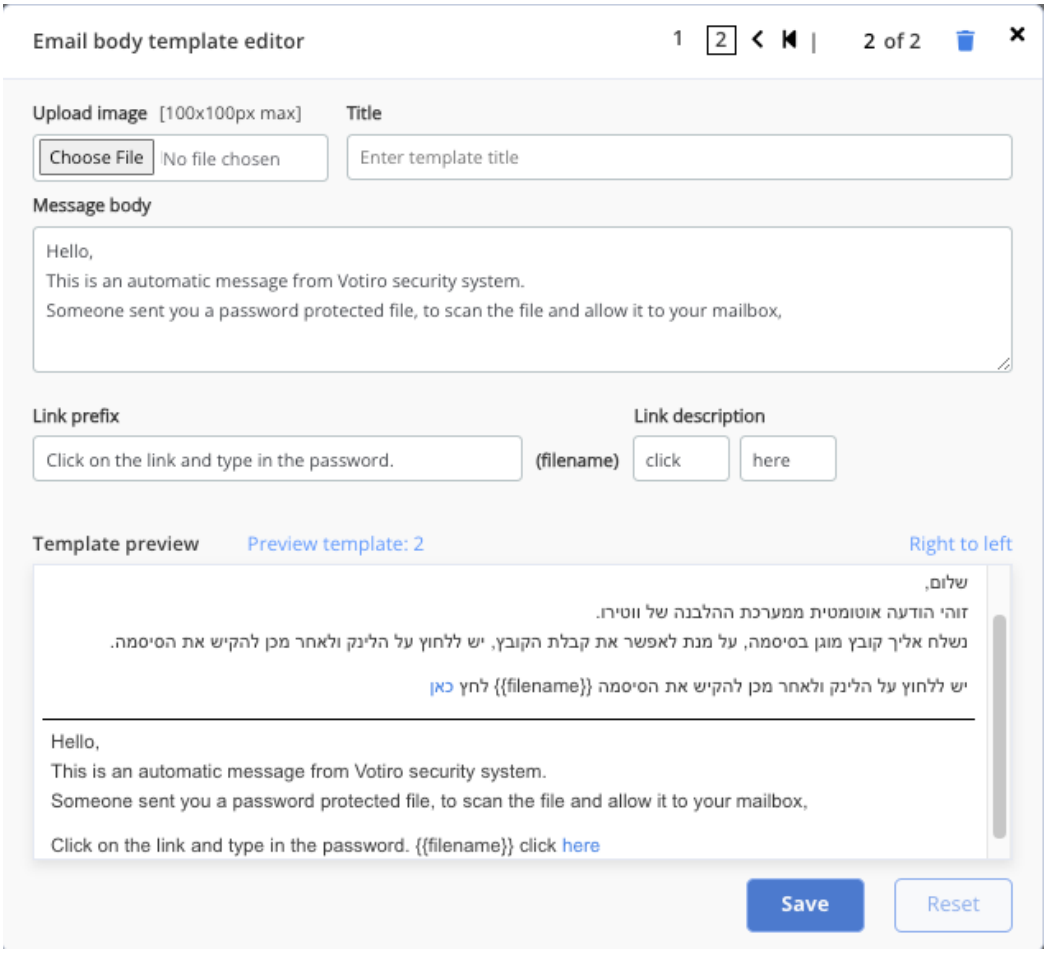


3. You can create up to two templates by clicking on the **+ Template** button.



4. After entering the desired information, there are options to:

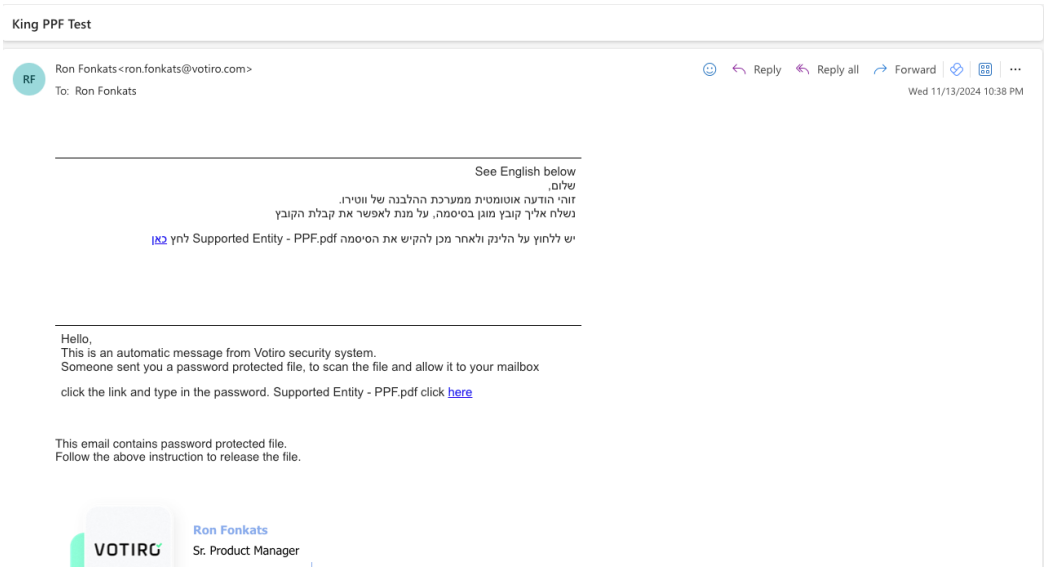
- **Template Preview** / **Preview all** - preview templates
- **Right to left** / **Left to right** - Set message location
- **Reset** - reset the template to the default



5. After reviewing the template changes, click on the **Save** button.

End user view

The following is an example of what the end user sees in the email:



Demo

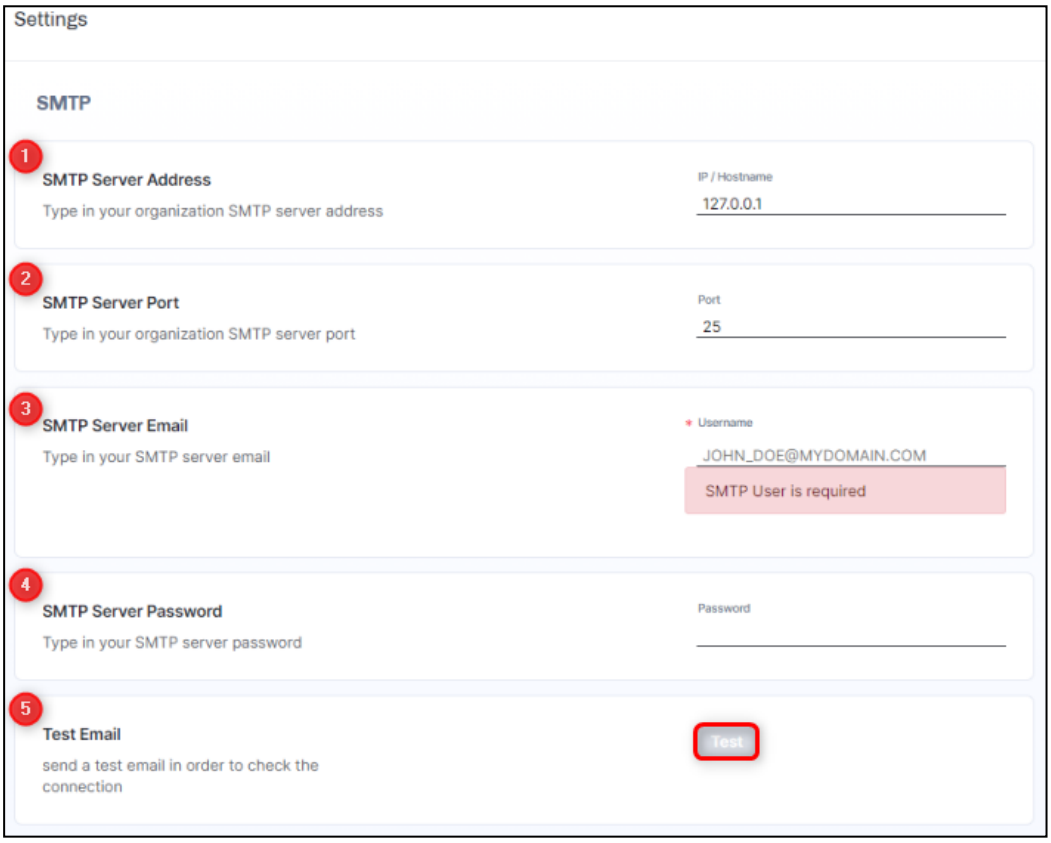
A video demonstrating customization of the Email body template is available at:

Customize template - PPF Email message

2.18.3 SMTP

All SMTP settings are required to enable Management Dashboard features that rely on email. Configuring SMTP settings allows you to release original files from the blob. For more information, see Releasing Files on page 1.

To get to the SMTP page, from the navigation pane on the left, click **Settings** > **SMTP**.



The SMTP page contains the following fields for configuring the connection to an SMTP server:

Element	Field	Description
1	SMTP Server Address	Specifies the SMTP server that relays notifications from the Platform Management to users in your organization.
2	SMTP Server Port	Specifies the SMTP server port.
3	SMTP Server Email	Specifies the email address of the SMTP server user.
4	SMTP Server Password	Specifies the password for the SMTP server user.

Element	Field	Description
5	Test Email	To test the SMTP settings, click **Test**. ■ If the settings are valid, a verification code is displayed in the Management Dashboard. The same code appears in an email message that is sent to the address you specified.  ■ If the settings are invalid, an error is displayed below the button.

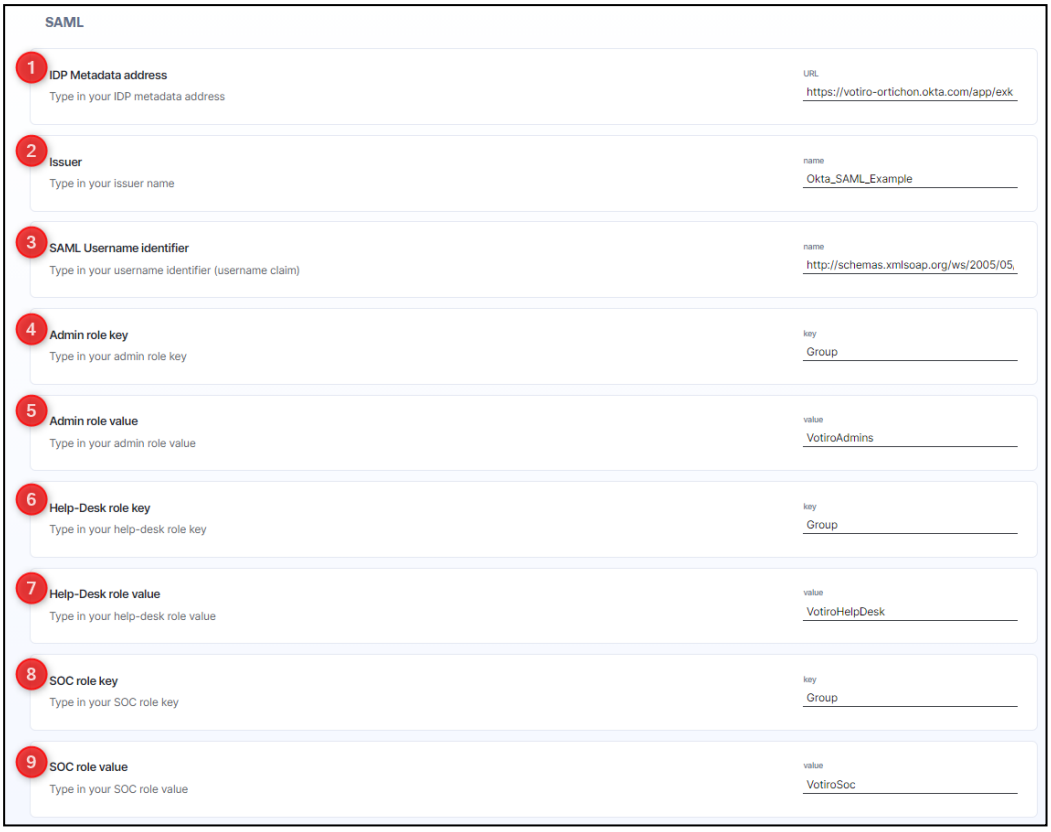
> **Note**
> Fields marked with a * red asterisk are mandatory, to be completed.

As you make changes the **Items Changed** count increases. When finished making changes at the bottom of the page select to either **Save Changes** or **Reset** to the original settings.

2.18.4 SAML

Configuring SAML settings allows the Votiro application to use single sign-on (SSO) technology to authenticate a user signed-in to their organization's systems.

To get to the SAML page, from the navigation pane on the left, click **Settings** > **SAML**.



The SAML page contains the following fields:

Element	Field	Description
1	IDP Metadata address	Specifies your IDP metadata address.
2	Issuer	Specifies the name of the issuer.
3	SAML Username identifier	Specifies the username of the identifier, also know as the claim.
4	Admin role key	Specifies the claim group name (i.e. "AzureGroupo1").
5	Admin role value	Specifies the object ID of a desired group listed under **Azure AD SAML Toolkit** > **Groups**.
6	Help-Desk role key	Specifies the role key for the helpdesk.
7	Help-Desk role value	Specifies the role value for the helpdesk.
8	SOC role key	Specifies the role key for the SOC.
9	SOC role value	Specifies the role value for the SOC.

Note

Fields marked with a * red asterisk are mandatory, to be completed.

As you make changes the **Items Changed** count increases. When finished making changes at the bottom of the page select to either **Save Changes** or **Reset** to the original settings.

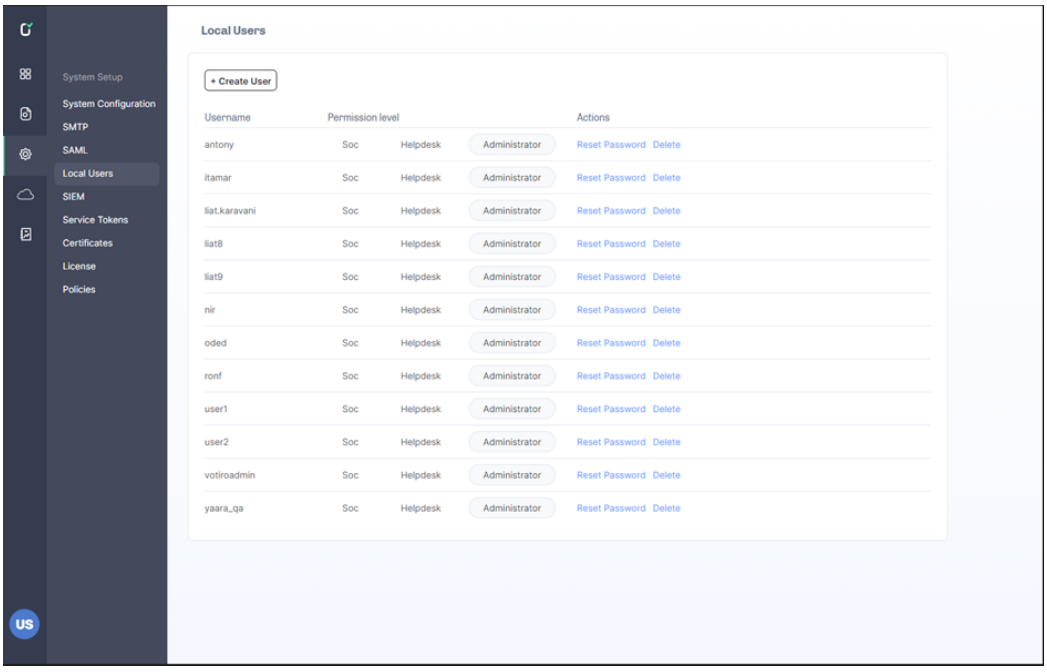
2.18.5 Local Users - SaaS

This feature enables the customer to add, delete and manage local users who can access the Management dashboard. The feature is relevant for SaaS customers only.

The feature has the following capabilities:

- The customer can
  - Create a user
  - Delete a user
  - Reset a user's password
  - Assign roles to a user
- The created users can log in to the Management dashboard and perform actions based on the assigned user role.
- Up to 20 local users per tenant are supported.
- AWS forgot password flow is not supported.

To get to the Local Users page, from the navigation pane on the left, click **Settings** > **Local Users**.



The Local Users page contains the following fields:

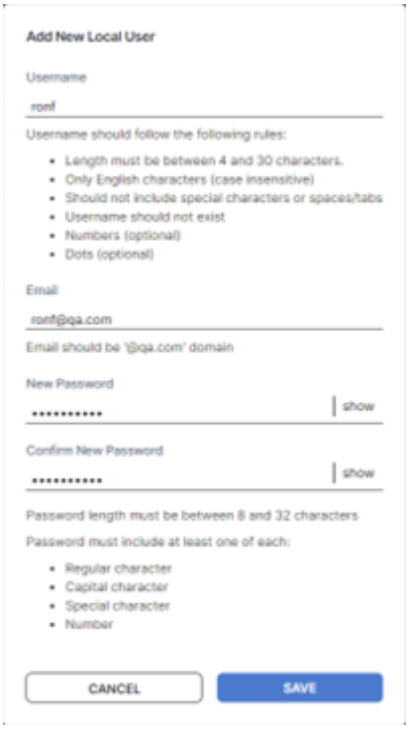
Element	Field	Description
1	Create User	Clicking on this button opens the **Add New Local User** window
2	Username	Specifies the name of the user.

Element	Field	Description
3	Permission level	Specifies the user's role value. The options are **Soc**, **Helpdesk** or **Administrator**
4	Actions	Specifies the possible actions. The options are **Reset Password** or **Delete**.

Add New Local User

To create a new user:

1. Click on **Add New Local User**.
2. In the window that opens, type the **Username**. Note the Username syntax rules displayed in the window.



3. Type the **Email** address.

> **Note**
> The system will display the **Username** with the tenant domain prefix. The user cannot change the tenant domain, unless there is more than one domain under the tenant; in this case, the user may select the tenant domain.

4. Type the **New Password** and **Confirm New Password**. Note the Password syntax rules.
5. Select the action to take:
   - To create the new user, click on **Save**. If successful, the user will be created and displayed in the user list.

- To cancel the user creation, click on **Cancel**. The user is not created and the user list is redisplayed.

Assign a Permission Level

The customer can assign the user a role:

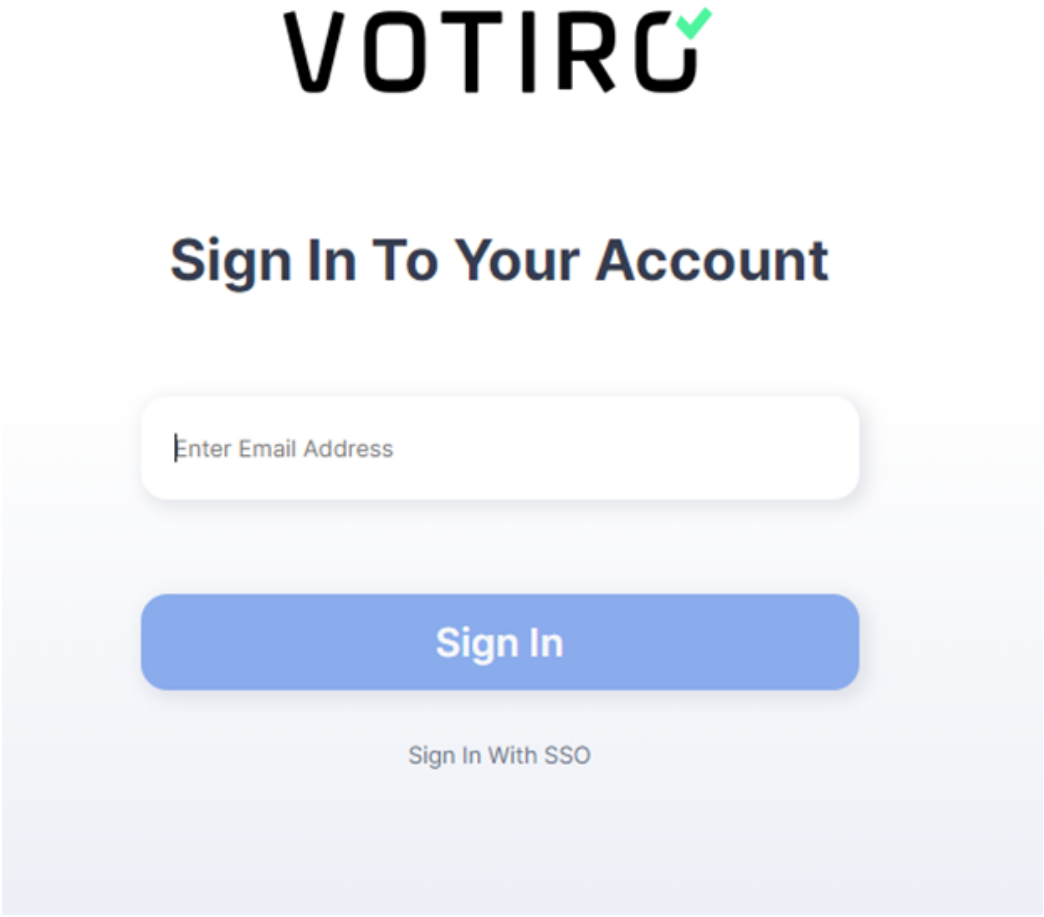
- **Soc** - cannot view the Local Users screen (this is the default permission for a new user)
- **Helpdesk** - can view the Local Users screen, but cannot perform any actions
- **Administrator** - can view the Local Users screen and can perform all actions

The following table details the permissions assigned to the different roles.

Role	View data in Dashboard and Explore Incident	Download / Release files	View/edit connectors setting	View/edit settings	Reports	View Local Users screen	Create/delete users Reset password	View/Edit Certificates	View/Edit Licenses
Soc	Yes	No	Yes/No	Yes/No	Yes	No	No	No/No	No/No
Helpdesk	Yes	Yes	Yes/No	Yes/No	Yes	Yes	No	No/No	No/No
Administrator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes/Yes	Yes/Yes

New Local User Initial Login

The new user sees the following login screen:

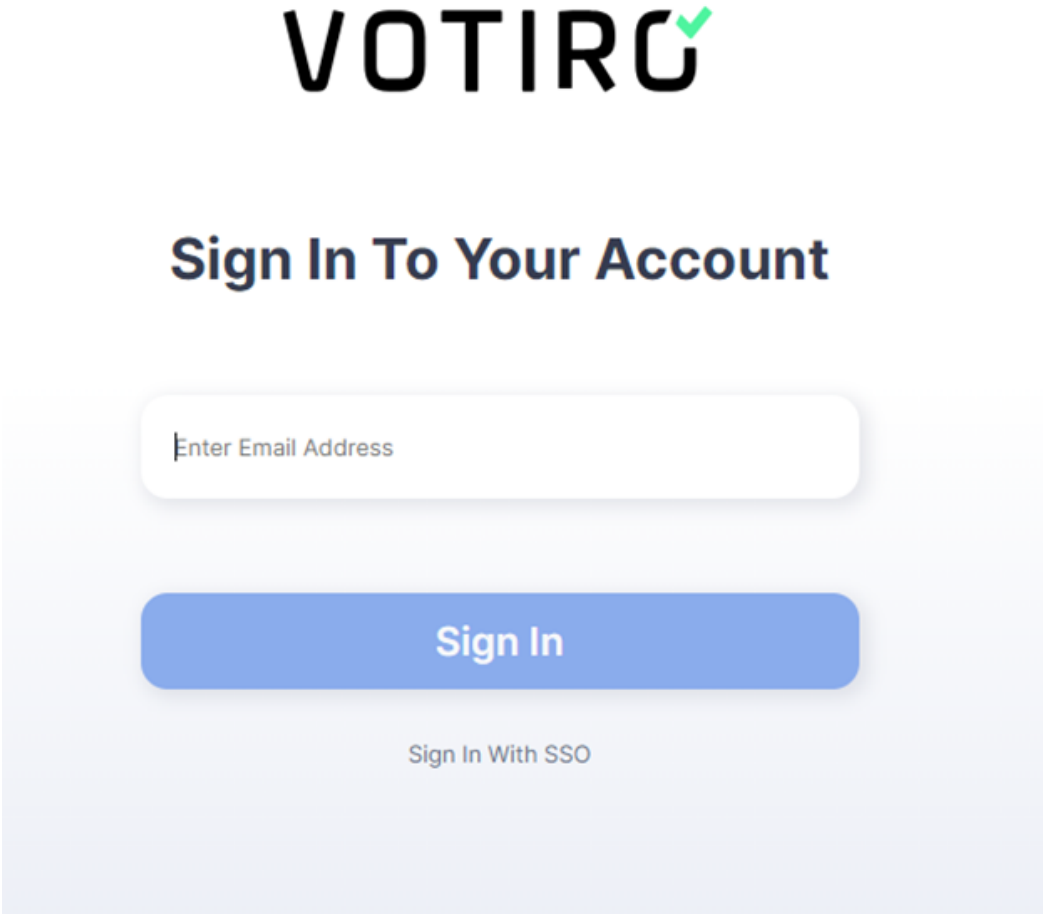


There are two ways the customer can sign in:

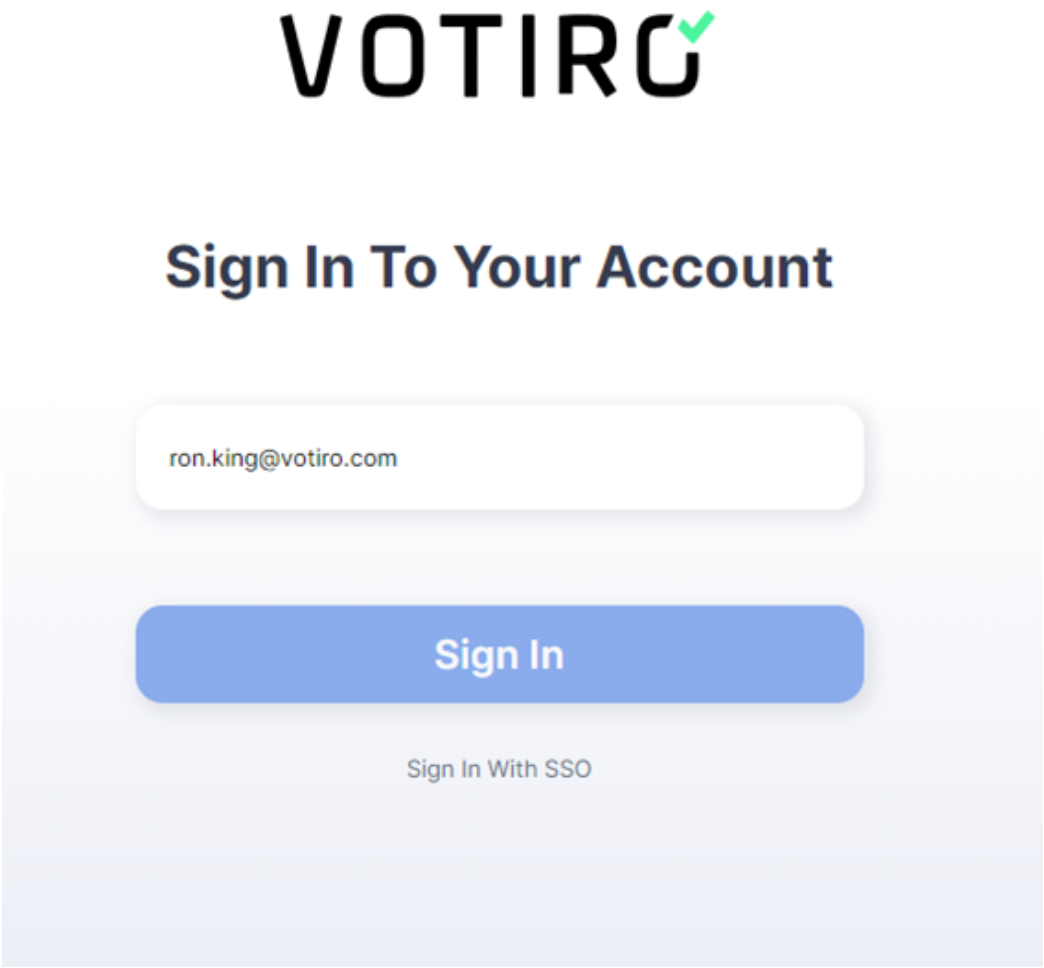
- Sign in with Votiro credentials - relevant for a customer that has setup local users
- Sign in with SSO (using corporate credentials) - relevant for a customer that has integrated Votiro through SAML

Sign In with Votiro credentials

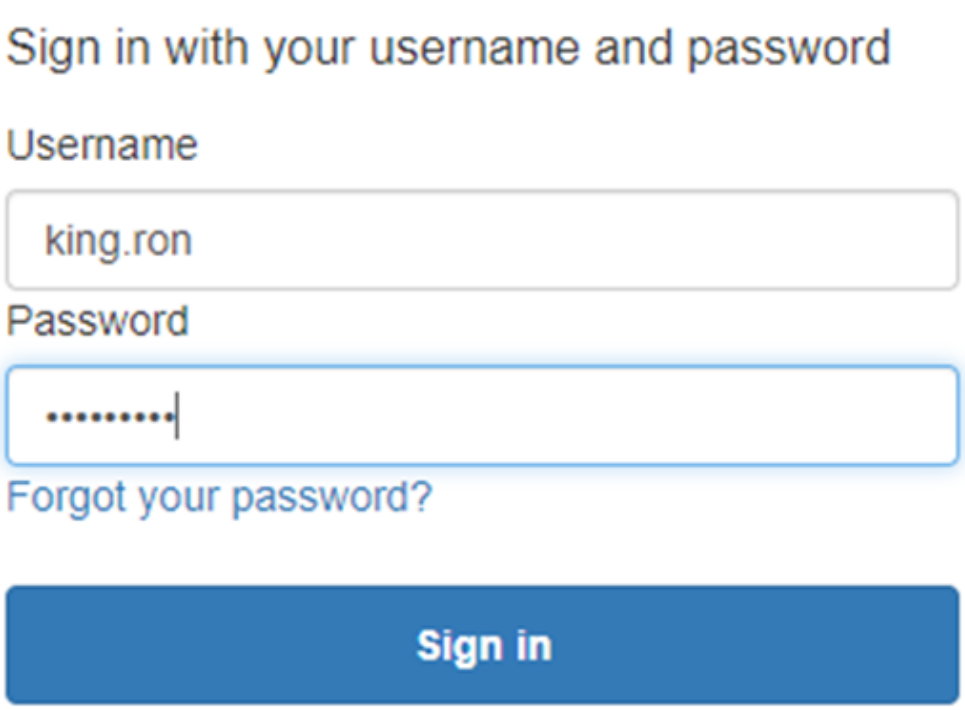
1. Sign in with Votiro credentials. Enter the local user email address to sign in to the Votiro Management console.



2. For example, ron.king@votiro.com



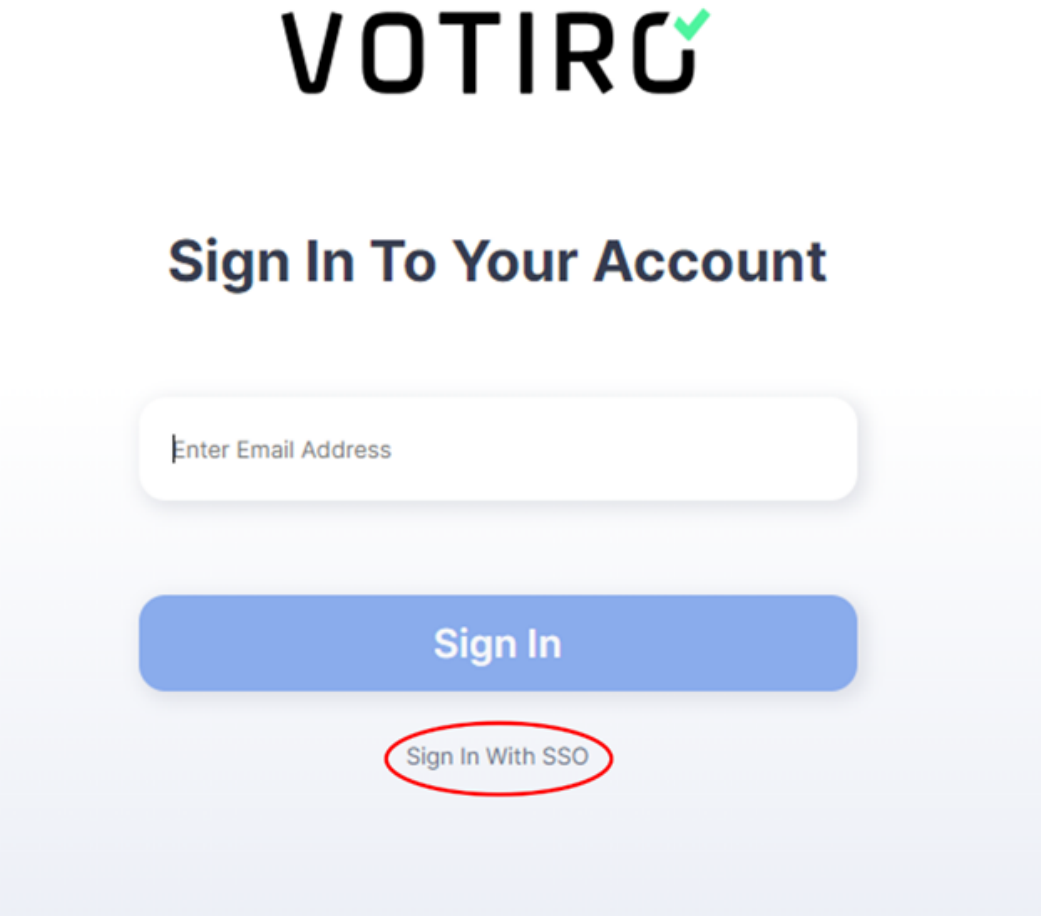
3. Press **Sign In**. An authentication window opens:



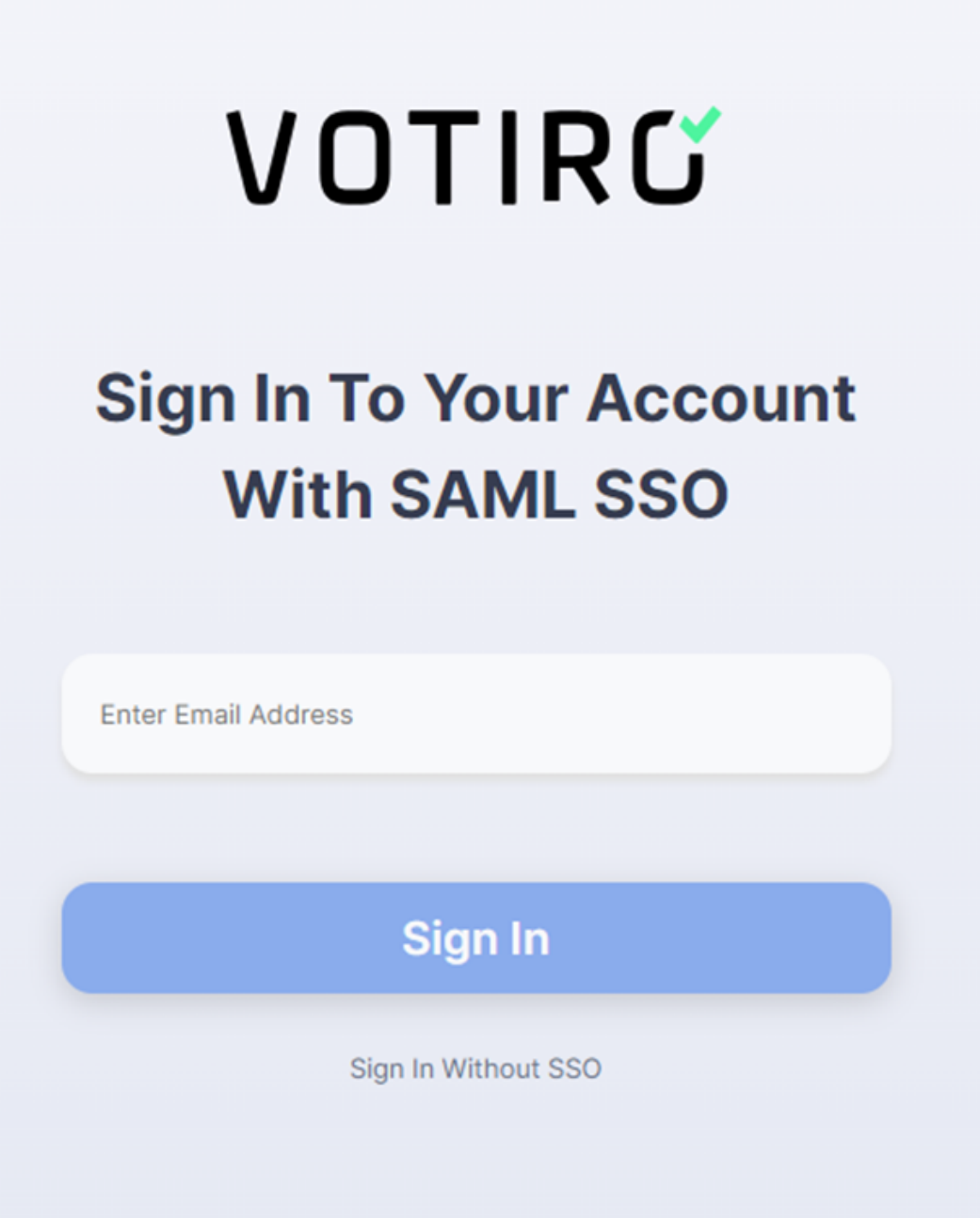
4. Enter the login credentials and press **Sign In**. The Management console is displayed.

Sign in with SSO (using corporate credentials)

1. The customer can enter his corporate credentials to sign in to the Votiro Management console using SSO. Click on **Sign In With SSO**.



2. The following screen is displayed. Enter the Email address and click on **Sign In**.



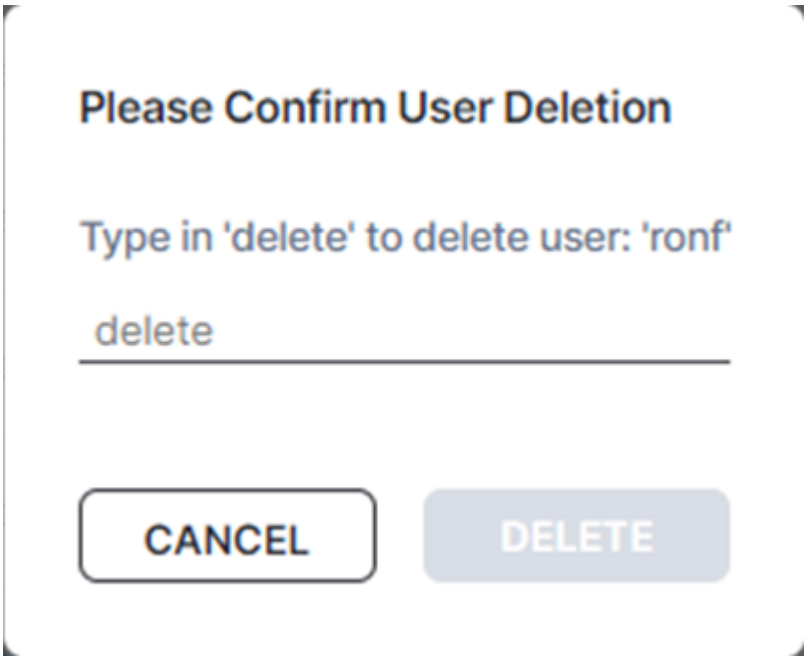
3. The customer is redirected to the corporate Identity Provider for authentication. After authentication is successful, the Management console is displayed.

> **Note**
> The Management Dashboard locks down for 10 minutes following three failed login attempts by a single username.

Delete a user

A user with Administrator role can delete a user.

1. Click on **Delete** in the user's row in the Local Users screen. The following confirmation window opens:

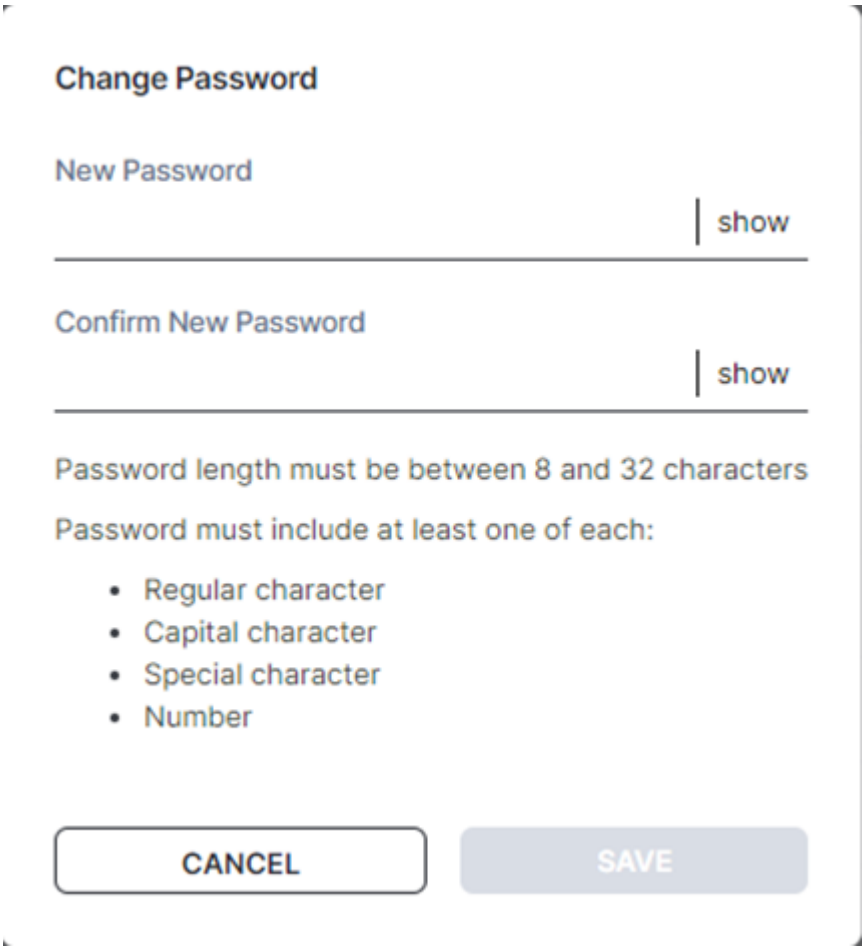


2. To delete the user, type **delete** and click on **DELETE**. To cancel and return to the Local Users screen, click on **CANCEL**.

Reset a user's password

A user with Administrator role can reset a user's password.

1. Click on **Reset Password** in the user's row in the Local Users screen. The following window opens:



2. Type a **New Password** and **Confirm New Password**. Note the password syntax rules. Then click on **SAVE** to save the new password, or **CANCEL** to cancel the reset password operation and return to the Local Users screen.

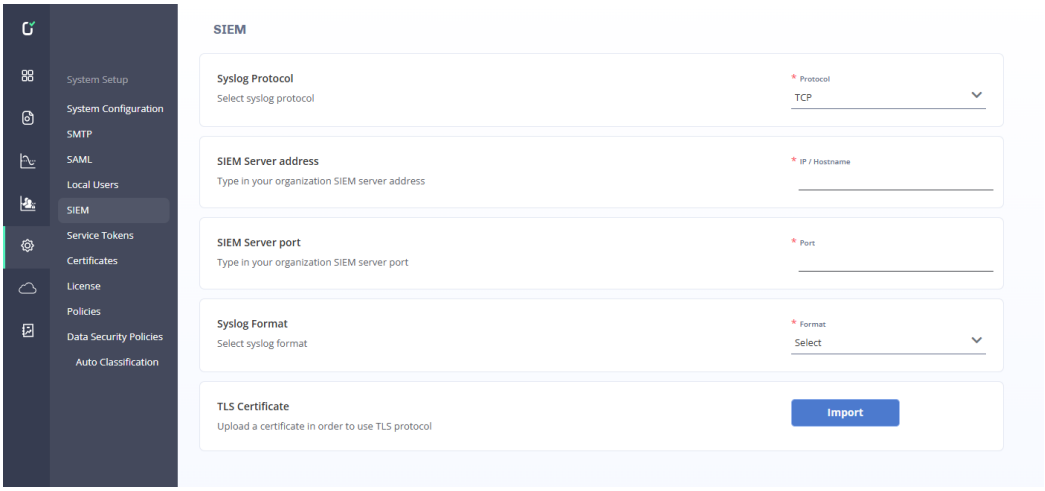
2.18.6 SIEM

You can configure SIEM setting for reporting syslog events to the SIEM platform. Votiro also supports sending security events (sanitization summary) directly to an AWS S3 Bucket.

To get to the SIEM page, from the navigation pane on the left, click **Settings** > **SIEM**.

Management Configuration when Syslog Protocol is not AWS S3

The SIEM configuration parameters displayed depend on the selected **Syslog Protocol**. The following configuration parameters are displayed if the selected Protocol is UDP/ TCP/ TLS/ HTTP Logs (Sumo Logic):



The page contains the following configuration fields:

Element	Field	Description
1	Syslog Protocol	Specifies the Syslog message transport protocol. Select from UDP, TCP, TLS(SSL) or HTTP Logs (Sumo Logic).
2	SIEM Server address	Address of the SIEM system collector service. Specify a hostname where the address represents a fully qualified hostname or an IPv4 address. The default is empty. When the address is empty, the server uses its own IP as an address. **Note**: The SIEM server address must contain the address protocol (HTTP or HTTPS).
3	SIEM Server port	Specifies the port of the SIEM system collector service. Specify a positive integer between 1 and 65535. The default is UDP port 514. For more information about SIEM logging in Management, see Syslog Events to SIEM Platforms on page 274.
4	Syslog Format	Specifies the Syslog message format. Select from CEF or LEEF.
5	TLS Certificate	If the server mandates certificate authentication to use the TLS protocol, a TLS certificate file must be imported. After importing the certificate file, refresh the page. The certificate name and creation date are displayed. **Note** Only PFX (Personal Information Exchange) formats with no password are currently supported.

> **Note**
> Fields marked with a * red asterisk are mandatory, to be completed.

To import a TLS certificate:

a. Click on the **Import** button.

b. An explorer window opens. Navigate to the desired certificate file to import and select it.

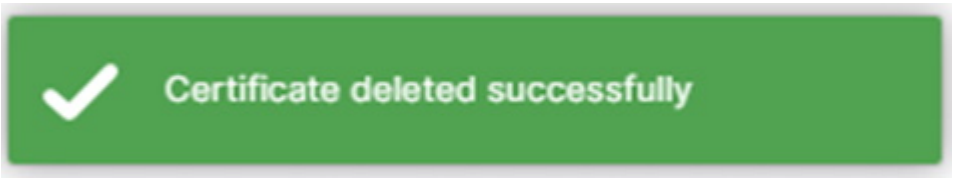
c. After importing the certificate, refresh the page.

d. The certificate name and creation date are displayed. The following message appears:

To delete a certificate that was imported:

a. Click on the **Delete** button.

b. The following message appears:

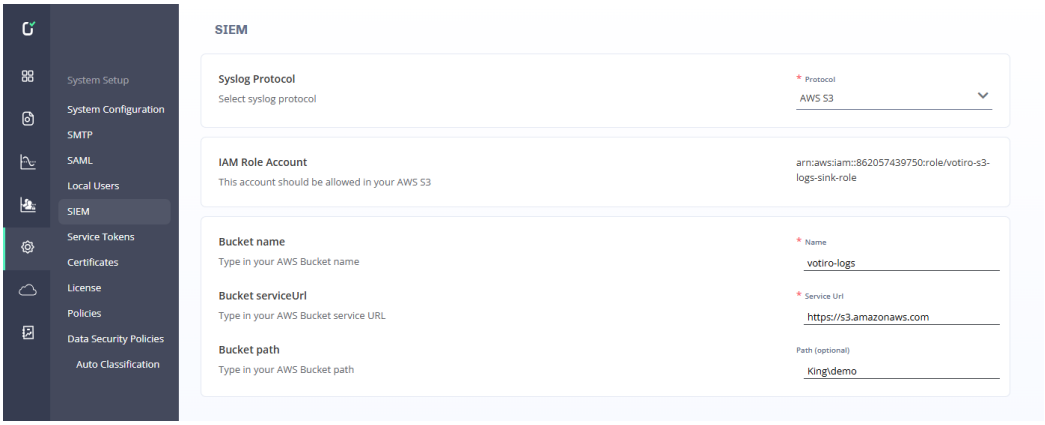


As you make changes the **Items Changed** count increases. When finished making changes at the bottom of the page select to either **Save Changes** or **Discard Changes** to the original settings.

Management Configuration for AWS S3

For each file sanitization, a new event (JSON format) will be created on the S3 bucket, and you will be able to parse the event data and perform automated actions as part of the SIEM activity.

The following configuration parameters are displayed if the selected Protocol is AWS S3:

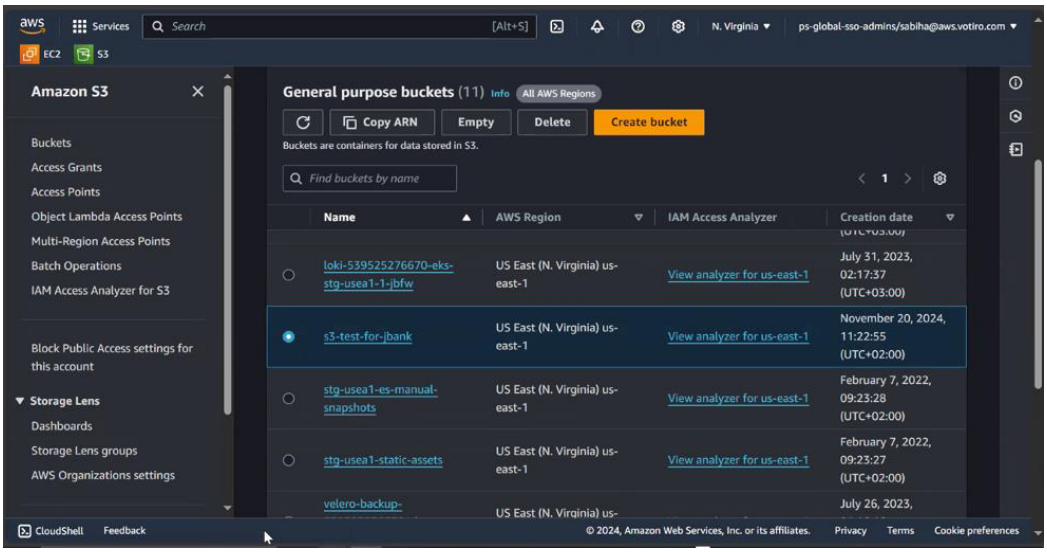


The page contains the following fields:

Element	Field	Description
1	Syslog Protocol	Specifies the Syslog message transport protocol. Select AWS S3.
2	IAM Role Account	Specify the account for each region for authentication.
3	Bucket name	Specify the AWS S3 bucket name.
4	Bucket serviceUrl	Specify the AWS Bucket service URL (Default - https://s3.amazonaws.com).
5	Bucket path	Specify the AWS Bucket path (folder)

The following steps describe the procedure:

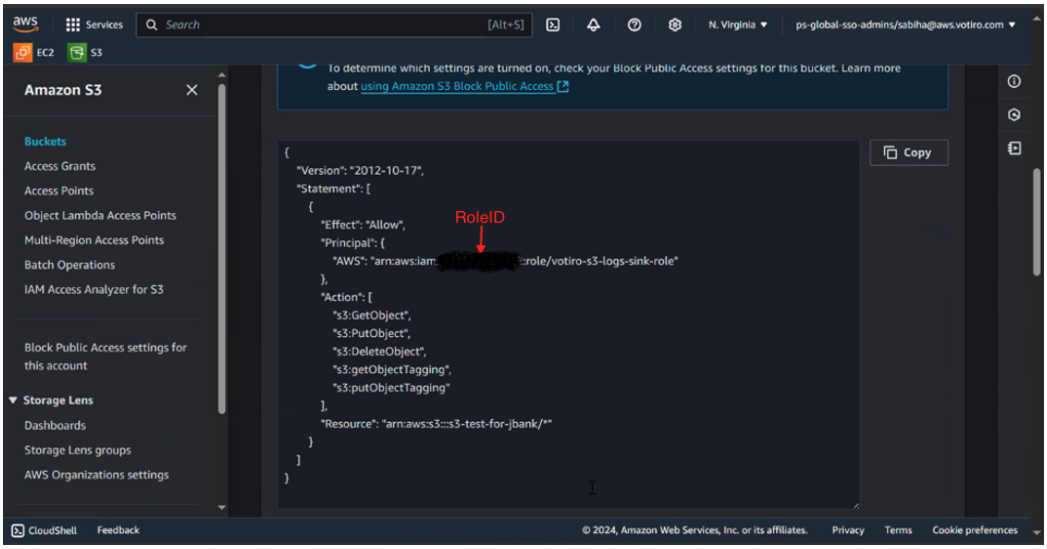
1. AWS S3 Bucket creation



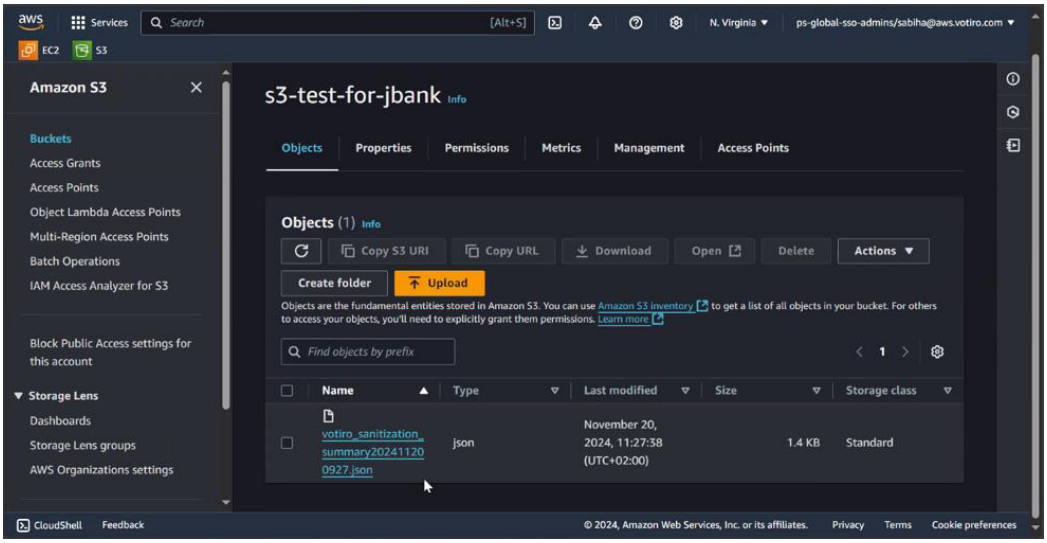
2. Bucket permission – IAM Role. Use the following code as an example:

```
{
   "Version": "2012-10-17",
```

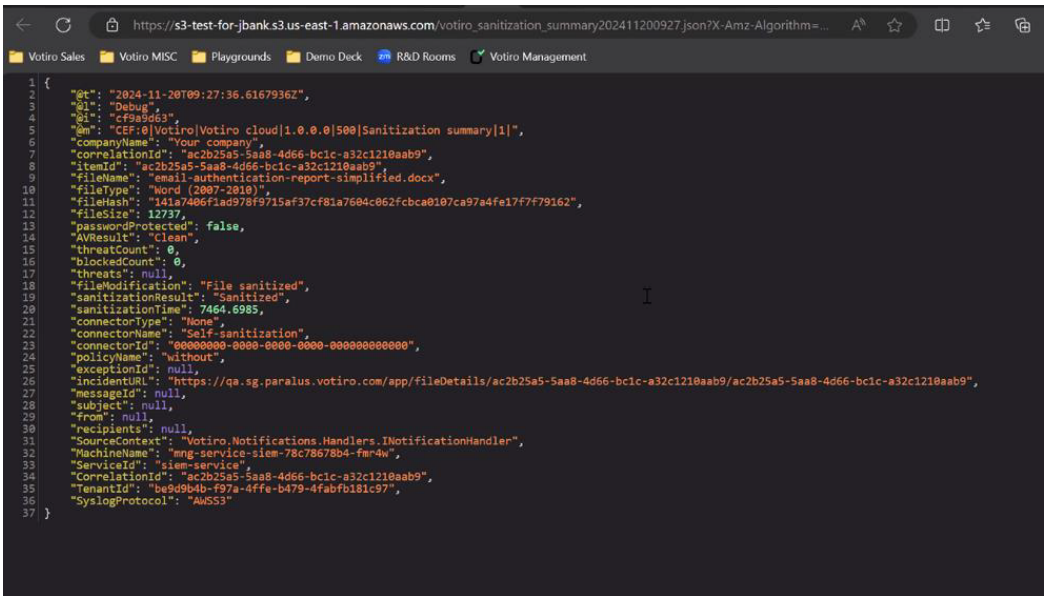
```
"Statement": [
   {
      "Effect": "Allow",
      "Principal": {
         "AWS": "arniam::{ID}:role/votiro-s3-logs-sink-
         role"
      },
      "Action": [
         "s3:GetObject",
         "s3:PutObject",
         "s3:DeleteObject",
         "s3:getObjectTagging",
         "s3:putObjectTagging"
      ],
      "Resource": "arns3:::<Your-S3-Bucket>/*"
   }
]
}
```



3. Sanitization Summary Event
   Place the following bucket configuration with the IAM Role account from the Management AWS S3 configuration (see step 1: AWS S3 Bucket creation).



4. Event message structure
   Event for each file sanitization Template – “votiro_sanitization_summary {TimeStamp}.json.
   The Event message value is described in Syslog Events to SIEM Platforms.



2.18.7 Syslog Events to SIEM Platforms

Votiro logs can be sent to SIEM in Common Event Format (CEF) or Log Event Extended Format (LEEF).

- Each incident that is created will generate a **Sanitization summary** Syslog message.
- When an incident of an archive or eml/email is triggered, there will be a separate Syslog message for each child inside the archive/email. In this case, there will be a drill down until there are no archive/eml files inside.
  For example:

- An eml file containing a zip file of 2 word files generates a total of 4 different syslog messages
- A zip file of 2 word files generates a total of 3 syslog messages
- A pdf file generates 1 syslog message
- A docx file generates 1 syslog message

- Syslog messages support UTF8.

The CEF message format is as follows:

	Fields 1 - 8	Fields 9 - 32
Separator	|	Space
Field name	Not used	See the table below
Format	Value	Field name=Value
Multiple values	Not supported	Separated by semicolon ";"

To enable SIEM logging, you must configure the SIEM settings in the Management Dashboard, see SIEM on page 269.

Here is an example of a SIEM CEF message in Votiro On-prem:

Mar 10 07:07:32|**CEF:0**|Votiro|Votiro cloud|9.6.348|500|Sanitization summary|5| **CompanyName**=Votiro1 **CorrelationId**=33a5d413-3be6-4b28-b5b7-257fc2add78d **ItemId**= 33a5d413-3be6-4b28-b5b7-257fc2add78d **fileName**=KingDemo.pdf **FileType**=pdf **fileHash**=5m6def67073ea7cf9aa3a68899f10fcdd074440efd60fa04e94774e9434eel52 **fileSize**=4020211 **PasswordProtected**=false **AVResult**=Clean **ThreatCount**=1 **BlockedCount**=0 **Threats**=Dynamic code execution **fileModification**=Java Script removed **SanitizationResult**= Sanitized **SanitizationTime**=1700 **ConnectorType**=File connector **connectorName**=Ron file connector **ConnectorID**=9098ddf2-7904-4e70-bff7-293b5e62f61c **policyName**=Ron file connector policy **ExceptionId**=null **incidentURL** = https://{clusterFQDN}/app/fileDetails/33a5d413-3be6-4b28-b5b7-257fc2add78d/33a5d413-3be6-4b28-b5b7-257fc2add78d **MessageId**=null **Subject**=null From=null **Recipients**=null

Here is an example of a SIEM LEEF message in Votiro:

Mar 10 07:07:32 LEEF:1.0 |**Votiro**|Votiro cloud|9.6.348|500|**Sanitization summary**|5| **CompanyName**=Votiro1 **Correlation Id** = 33a5d413-3be6-4b28-b5b7-257fc2add78d **ItemId**= 33a5d413-3be6-4b28-b5b7-257fc2add78d fileName=KingDemo.pdf **FileType**=pdf **fileHash**=5m6def67073ea7cf9aa3a68899f10fcdd074440efd60fa04e94774e9434eel52 **fileSize**=4020211 **Password protected** = false AV Result= clean ThreatCount= 1 BlockedCount= 0 Threats= Dynamic code execution fileModification = Java Script removed SanitizationResult= Sanitized SanitizationTime= 1700 **Connector Type**= File connector **connectorName**= Ron file connector **ConnectorID**= 9098ddf2-7904-4e70-bff7-293b5e62f61c **policyName**= Ron file connector policy **ExceptionId**= null **incidentURL** = https://{clusterFQDN}/app/fileDetails/33a5d413-3be6-4b28-b5b7-257fc2add78d/33a5d413-3be6-4b28-b5b7-257fc2add78d **MessageId**= null **Subject**= null **From**= null **Recipients**= null

Votiro Sanitization summary Syslog message format

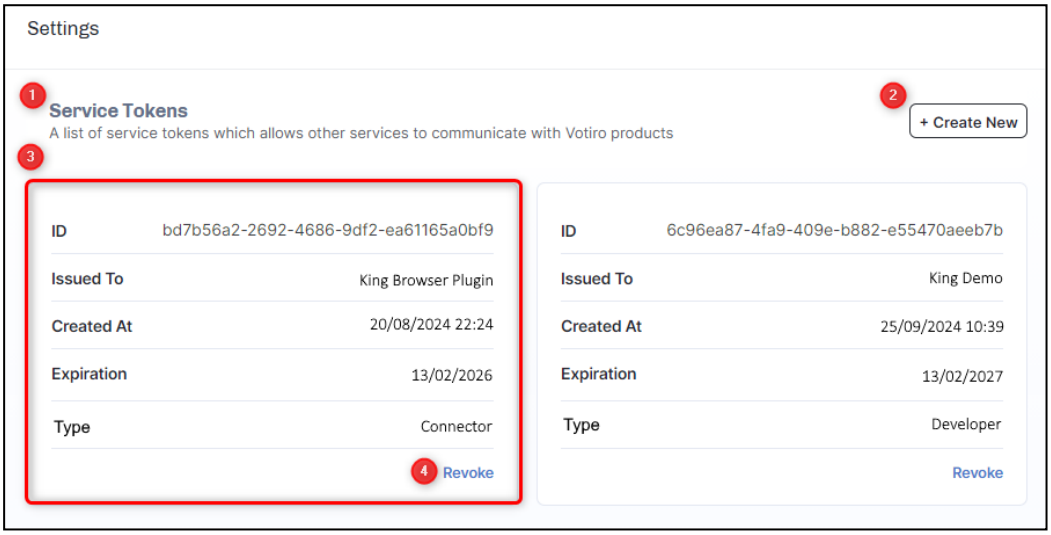
Field #	Field name	Description	Value
1	Timestamp	Event timestamp based on customer time	{MMM DD HH:mm:SS} For example, Mar 10 07:07:32
2	Syslog message format	Syslog message format	**CEF:0**
3	Device vendor	Vendor name	**Votiro**
4	Device name	Device name	**Votiro**
5	Device version	Product version	{Product version} For example, 9.8.100
6	Signature ID	Signature ID of the event	**500**
7	Message name	Syslog message name	**Sanitization summary**
8	Message severity level	Message severity level. **Note**: All events will be of the same severity level.	**5**
9	Company name	Customer's company name configured in the Management dashboard.	{Company name}
10	Correlation ID	Unique GUID that represents the file	{GUID}
11	Item ID	Unique GUID that represents the file. The Item ID is the same as the Correlation ID if it represents the same file. If the item ID is different, it means that the file is a child or inner file related to the parent file.	{GUID}
12	File name	File name	{character string}
13	File type	File extension	{character string} For example, pdf
14	File hash	Hash of the file	{hash (hexadecimal) string}
15	File size	File size in bytes	{long integer}
16	Password protected	Indicates whether the file is password protected	• **true** • **false**
17	AV result	Result from the Anti-Virus engine's scan of the file	• **Infected** • **Clean** • **Not used** (if the AV is not activated)
18	Threat count	Number of threats detected in the file	{integer}

Field #	Field name	Description	Value
19	Blocked count	Number of blocked files in the file	{integer}
20	Threats	Description of what threats were detected in the file	{character string} For example, Suspicious macro; external link path
21	File modification	Description of what Votiro modified in the file	{character string} For example, Removed suspicious macros; Removed external link path
22	Sanitization result	Result of Votiro's sanitization of the file	• **Sanitized** • **Partially sanitized** (indicates a parent file whose inner files are blocked / skipped) • **Skipped** • **Blocked**
23	Sanitization duration	Sanitization time for the file in ms	{integer}
24	Connector type	Type of connector	• **Email connector** • **File connector** • **Menlo connector** • **AWS S3 connector** • **Office 365 connector** • **API** • **Self-sanitization**
25	Connector name	Connector name configured by the customer in the Management Dashboard	{character string}
26	Policy name	Customer policy name	{character string}
27	Exception ID	Indicates which policy exception the file triggered	{integer}
28	Incident URL	URL to navigate to the incident in the Management dashboard	{https://{cluster FQDN} /app/fileDetails/ {Correlation ID}/{Item ID}}
29	Message ID	Message ID value assigned by Exchange / Office 365	• {Message ID} • "null"
30	Subject	Email subject	• {character string} • "null"
31	From	Sender's email address	• {character string} • "null"
32	Recipients	Recipients' email addresses	• {character string} • "null"

2.18.8 Service Tokens

Use the Service Tokens page to view existing service tokens, create new service tokens and revoke existing service tokens. Service tokens allow other services to communicate with Votiro.

To get to the Service Tokens page, from the navigation pane on the left, click **Settings** > **Service Tokens**.



Element	Field	Description
1	Service Tokens	The service tokens created for use are displayed on this page.
2	Create New	To create a new service token, click **+ Create New**. For detailed steps to create a new service token, see Creating a Service Token on the next page.

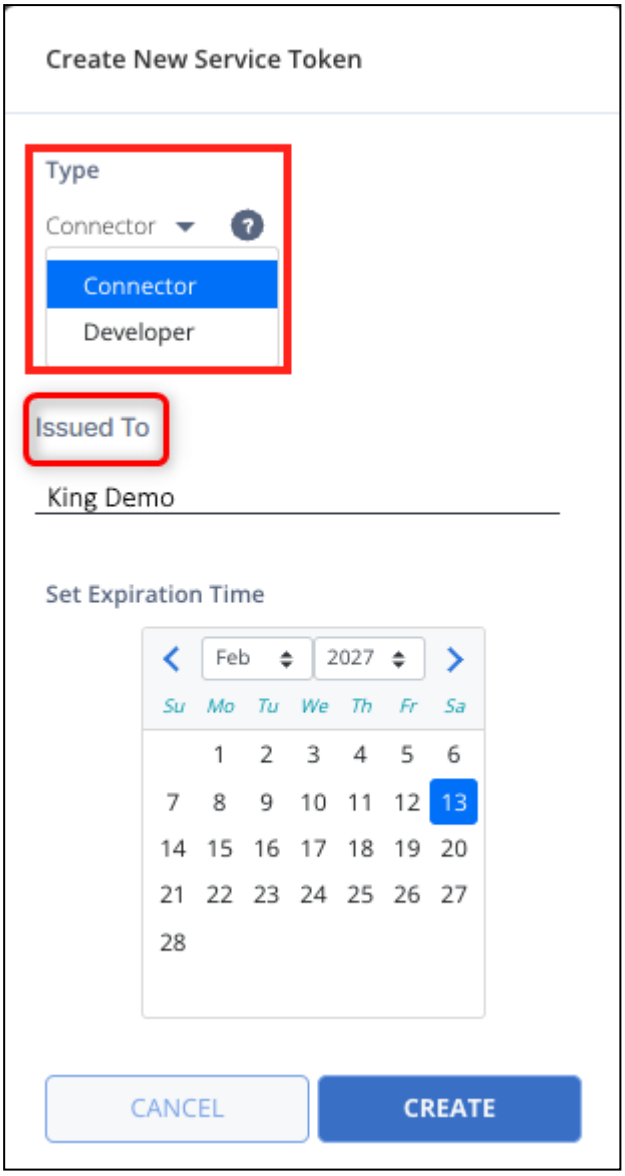
Element	Field	Description
3	Service Token	Details of the service token are displayed: ■ **ID**: The ID of the service token is automatically added. ■ **Issued To**: Specifies the name you have given to the service token. ■ **Created At**: A DateTime stamp is automatically added to the service token. ■ **Expiration**: Specifies the date the service token will expire. ■ **Type**: ♦ **Connector** - Basic integration. Allows authentication for uploading files procedure. This token has access to the APIs used for the classic classic flow of upload-GetStatus-download. Should be used by classic connectors that try to upload a file and get the sanitized version. If the connector needs statistical data on items, etc., it should use developer token. ♦ **Developer** - Advanced integration. Has access to all console APIs (Upload, download, get Items statistics, basically every API that is exposed to the console user). That's the kind of token that our UI uses, because it also needs access to configurations, item statistics etc. This should be used only by integrations that require access to information, config etc, and not only classic flow of upload-GetStatus-download. Handle it with caution.
4	Revoke	To remove a service token, click **Revoke**. For detailed steps to remove a service token, see Revoking a Service Token on page 281.

Creating a Service Token

To create a new service token:

1. Click **Create New**.
2. Complete **Create New Service Token** fields.

Field	Description
Type	Specifies the token type.
Issued To	Specifies the name you have given to the service token.
Set Expiration Time	Specifies the date the service token will expire.



3. Click **CREATE**.

4. A service token is generated. You must copy this service token to the relevant bearer authentication headers.

> **IMPORTANT!**
> The service token generated is not stored by Votiro. You must copy it immediately.

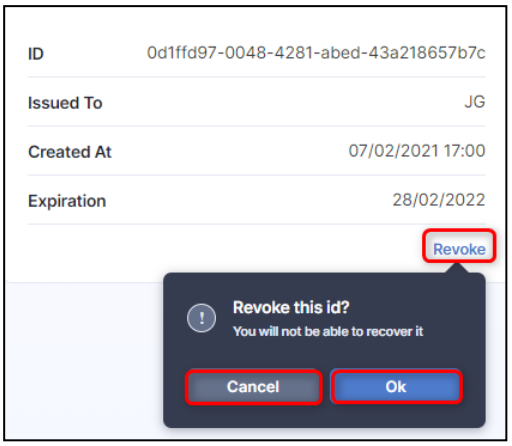
5. Click **OK**.

6. A list of service tokens created are displayed on the Service Token page.

Revoking a Service Token

To withdraw a service token:

1. Click **Revoke**. A confirmation pop appears warning that a revoked service token cannot be recovered.



2. Click **OK** to continue revoking the service token, or **Cancel** to continue using the service token.

2.18.9 Certificates

Use the Certificates page to import PDF digital signatures through the Management console and sanitize PDF files with digital signatures without corrupting them.

To get to the Certificates page from the navigation pane on the left, click **Settings** > **Certificates**.

Digital Certificates supported

Votiro supports the following compliance standards by default:

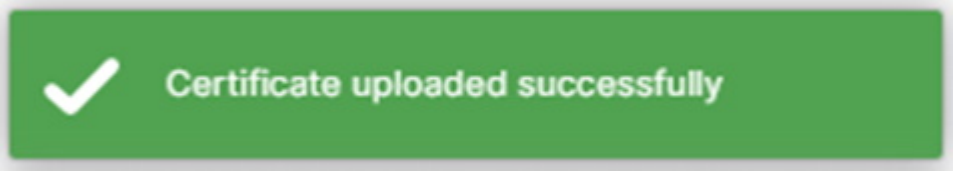
- **AATL** - The Adobe Approved Trust List (AATL) is used to distribute and maintain a list of trustworthy digital certificate issuers for Adobe Acrobat and Adobe Reader. For more details, see Adobe Approved Trust List.
- **EUTL** - The European Union Trusted Lists (EUTL) is a public list of over 200 active and legacy Trust Service Providers (TSPs) that are specifically accredited to deliver the highest levels of compliance with the EU eIDAS electronic signature regulation. For more details, see eIDAS Dashboard.

- **FPKI** - The Federal Public Key Infrastructure (FPKI) is a network of certification authorities (CAs). The Federal PKI includes USA federal, state, local, tribal, territorial, and international governments, as well as commercial organizations, that work together to provide services for the benefit of the USA federal government. For more details, see Federal PKI.
- **CCA** - The Controller of Certifying Authorities (CCA) of India certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates, the Root Certifying Authority of India(RCAI). The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to the CAs in the country. For more details, see Controller of Certifying Authorities.

Uploading a Certificate

To upload a new certificate:

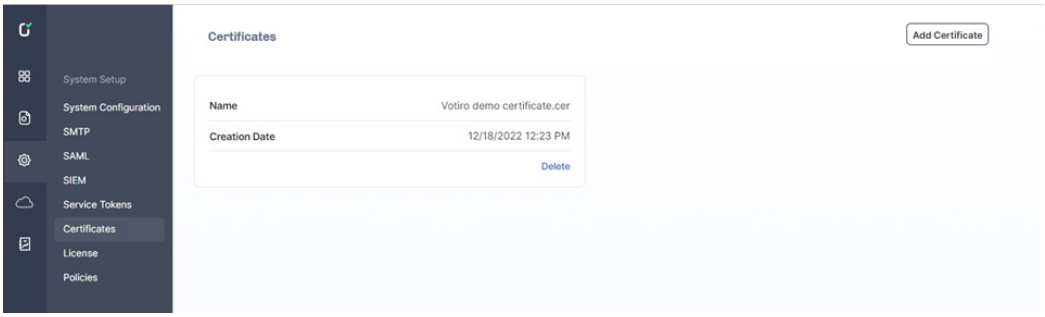
1. Click on the **Add Certificate** button.
2. An explorer window opens. There is an option to select multiple files.
3. Select the desired files to upload.
4. After a certificate file is uploaded successfully, the following message appears:



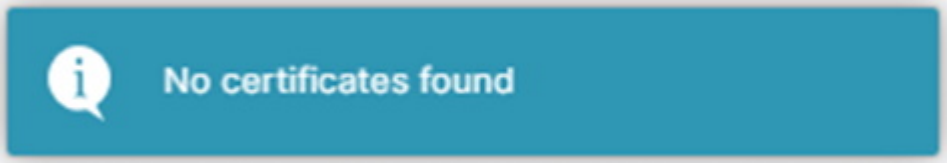
5. If the upload fails, the message **Failed to upload certificate** appears.

Viewing a Certificate

The Certificates page displays the **Name** and **Creation Date** of the current existing certificates:



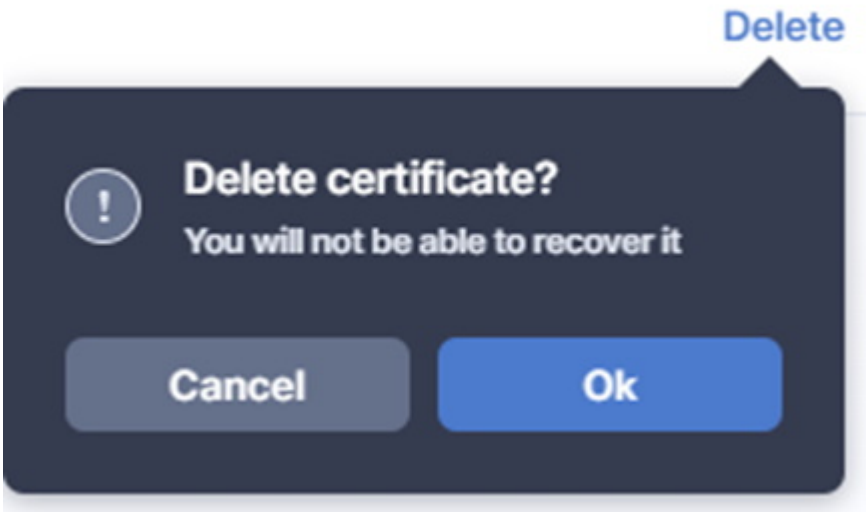
If there are no certificates, the following message appears:



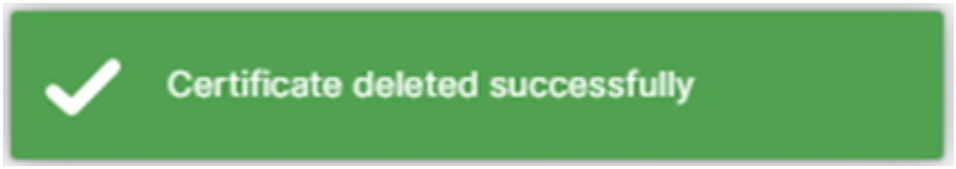
Removing a Certificate

To remove a certificate:

1. Click on the **Delete** button.
2. A confirmation window opens:



3. Click on the **Ok** button.
4. If the removal is successful, the following message appears:



Sanitizing a PDF with Digital Signatures

To successfully sanitize a PDF with digital signatures, define a policy exception on the Policies page:

To specify an exception for a file with a digital signature,

1. Select **Digital signature**.
2. Select **is valid** or **is not valid**.
3. Click on the **Save** button.

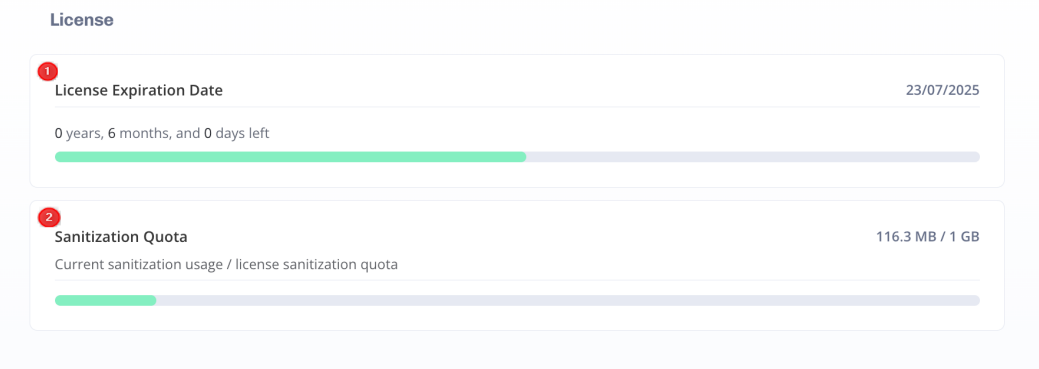
2.18.10 License

Use the License page to generate a license request, import a license key, know the date the license will expire and keep track of the file consumption against the quota.

> **Note**
> The license key issued includes information relating to your authority to use our Cloud Connectors.
> To amend your license to include Cloud Connectors, contact Votiro's Support team.

To get to the License page, from the navigation pane on the left, click **Settings** > **License**.

For the SaaS version:



The license page contains the following configuration fields:

Element	Field	Description
1	License Expiration Date	When a valid license key is imported the expiration date automatically updates to the date when processing of files will stop. At time of installation the default license is valid for 24 hours. During this time files will be processed and a license should be requested.
2	Sanitization Quota	The first figure represents the current consumed size per file. The second figure represents the licensed size quota of files to be processed. See See Sanitization Quota (V9.6.3) for a more complete explanation.

Sanitization Quota (V9.6.3)

The Sanitization Quota will display consumed size per file.

The accumulated file size consumption is determined as follows:

- The accumulation is based on the original file size and not on the file size after sanitization.
- The accumulation is for each file that the customer sends to sanitization except EML and archive files.
- For EML or archive files, the file size accumulation will be based on all the files embedded inside the EML/archive, including all nested EMLs/archives.
- Password protected files will be counted only once.
- For customers with a V9.6.2 license who upgrade to the new version, the license page will still display the Sanitization Quota based on files.

Examples

- A 400KB PDF will be accumulated as 400KB regardless of the size of the embedded files inside the PDF.
- A 1MB image file will be accumulated as 1MB.
- A 10MB archive file containing five 10MB PDFs will be accumulated as 50MB.
- A 11MB EML file with an attached 10MB zip file that contains five 10MB PDFs will be accumulated as 50MB.

File count for an archive file or email with attachments

We count the actual number of files that were sanitized regardless of whether multiple files were compressed to an archive file or multiple files were attached to the email file .

For example:

- An archive file has 5 children - it will be counted as 6 files instead of 1 file.

- An EML has 5 attachments - it will be counted as 6 files instead of 1 file.

Other file types are not affected by these changes.

For example:

- A PDF file with 5 embedded images/files/etc. will be counted as 1 file.
- A Word file with embedded images/files/etc will be counted as 1 file.

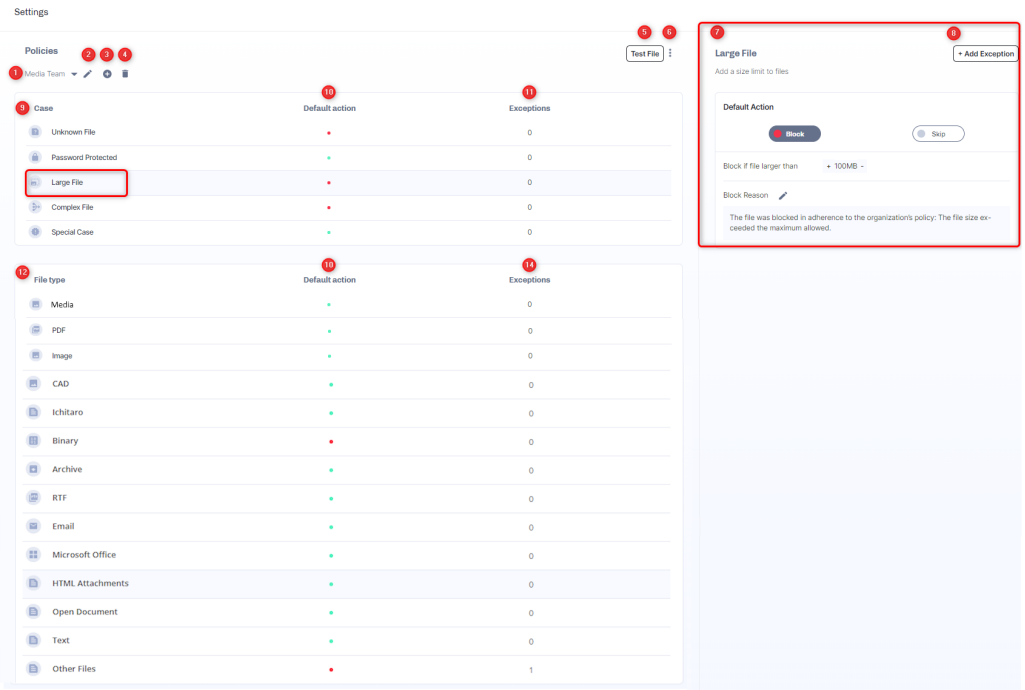
2.18.11 Policies

A positive selection policy defines the manner in which you handle a file matching a set of criteria that enters your network. The policy can determine how files are processed, including whether files are blocked or permitted.

Policies Dashboard

From the Policies Dashboard you can create, edit, and manage the positive selection policies operating in the Positive Selection® Engine as traffic flows through.

To get to the Policy dashboard, from the navigation pane on the left, click **Settings** > **Policies**.



Element	Meaning
1	The name of the currently displayed policy. To display a policy, select from the list of defined policies. You can set up policies for specific teams or individuals.
2	Edit the policy name.

Element	Meaning
3	Add a new policy.
4	Delete current policy. This element only displays when additional policies have been defined. The **default policy** cannot be deleted.
5	Select file to test policy.
6	Import/Export policy file.
7	Displays details of the item that is selected on the left. For each case or action, you can define how it must be handled.
8	Add an exception. For example, when managing other file types, with specific email addresses and/or URLs.
9	Displays details of the selected policy by case.
10	Displays the status of the default action taken for the policy. A colored dot illustrates your current policy action: ■ Red - files will be blocked ■ Green - files will be processed using your sanitization settings ■ Grey - files will be skipped
11	Displays the number of exceptions defined per policy case or file type.
12	Displays the details of the selected policy by file type.

Note

Change made in policies are updated in the Positive Selection® Engine every few seconds. Once updated in the Positive Selection® Engine, it is available to Votiro On-prem reference clients, such as Votiro On-prem for Email or Votiro On-prem for File Transfer.

Defining Policies

You can customize policies in a variety of ways, depending on your organization's requirements. They are by:

- **Case**: a policy using a file's characteristics, for example, password protected, size of file. For more information, see Defining Policies by Case on the next page.
- **File Type**: a policy using a file's family, for example, PDF, Microsoft Office, images. For more information, see Defining Policies by File Type on page 292.
- **Exception**: a policy where you can define one or more exceptions to any case policy or file type policy. For more information, see Adding Policy Exceptions on page 303.
- **Special Case**: If you have custom, XML-based policy definition, you can load it to the Management Dashboard as a special case. This is also known as a **custom policy** – that has been created outside the Management Dashboard. This feature is recommended for special purposes only. For more information, contact Votiro's Support.

If you do not create a customized policy, Votiro On-prem uses a default policy. Each case and file type has a different default policy.

File Blocking

When you configure a policy to block a file, no other policy rule is applied on the file. A **block file** containing information about the blocked file and the reason it was blocked replaces the original file. You can accept the block file default text or edit it.

A **block file** is a document that replaces an original file that was blocked. It is attached to an email and can be customized for each company, and for each type of case or file type.

2.18.12 Defining Policies by Case

Policies have default settings that you can customize to meet your organization's requirements.

To define a policy by case, from the navigation pane on the left, click **Settings** > **Policies**.

For more information about the policies page, see Policies Dashboard on page 287.

When defining a policy by case, you can perform the following actions:

- Block the file under all conditions. If selected:
  - Additional options may be available for you to set.
  - You can edit the default block notification message text, **Block Reason**.
  - The **Default Action** displays a **red dot**.
- Sanitize the file. If selected:
  - Additional options may be available for you to set.
  - The **Default Action** displays a **green dot**.
- Skip the file. The **Default Action** displays a **grey dot**.
- Add one or more exceptions to the policy. The **Exceptions** displays the number of exceptions applied to the policy. For more information, see Adding Policy Exceptions on page 303.

The following table describes the positive selection processing options that are available for each case:

Table 2 Positive Selection Processing Options for Cases

Case	Processing Options
Virus	■ Block: If a virus is detected in the file by the AV engine, the file will be blocked. ■ Skip: The file is not processed for positive selection and the original version will reach the destination folder. **Note**: Offline AV signature updates are supported for offline VA env for ClamAV only.
Unknown File	You can block or skip these files. If you select Skip, the unknown file is not processed for positive selection and the original version will reach the destination folder.

<table>
<tr><th>Case</th><th>Processing Options</th></tr>
<tr><td>Password Protected</td><td>
You can block or process these files. By default, the files are processed for positive selection.

Return file by email with User Message: Allows you to return a password protected file by email. Accept the default text notification message, or edit it.
User Message: Allows you to edit the message sent to the recipient of the password protected file. See <a>Instructions for Email User below.
Block unsupported files with Block Reason:Allows you to block unsupported files (such as Visio files). Accept the default text notification message, or edit it.

When the files are blocked, Votiro issues a block-file containing the reason it was blocked. The notification contains a link that opens a Password Protected File portal where the password can be entered. When the correct password is entered, the blocked file returns to the storage server, for processing. The processed file is then downloaded to the recipient's computer, or sent by email as an attachment.
<blockquote>Note
This feature supports the following file types only: PDF, ZIP, 7zip, RAR, DOC, DOCX, DOT, DOTX, DOCM, DOTM, XLS, XLT, XLSX, XLTX, XLSM, PPT, PPS, POT, PPTX, PPSX, POTX and PPTM. It does not work on other file types that can be protected by a password, such as Visio files.</blockquote>
<h2>Instructions for Email User</h2>
The Votiro administrator should communicate the following information and instructions to the users.

An email message with password protected files attached can be processed for positive selection and returned as an email attachment, or as a download. The user receives a message that a password protected file has been received, with the option to enter the password, then click Get File.

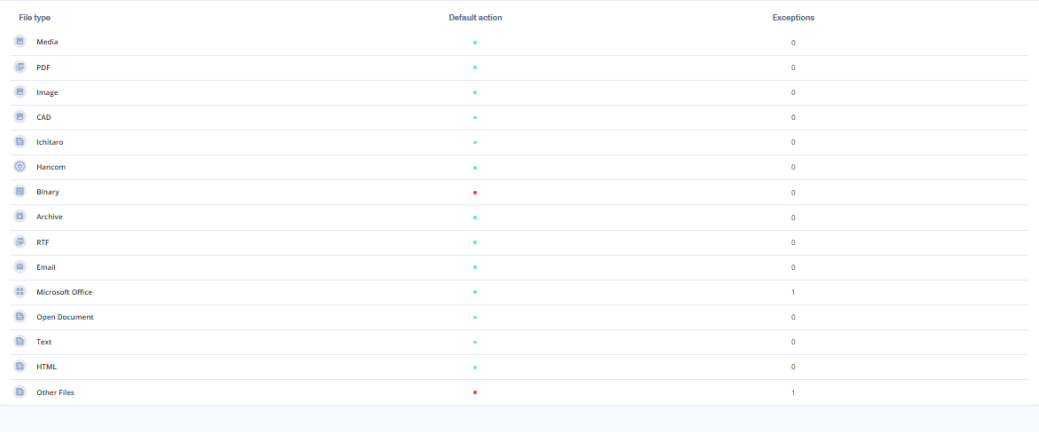
The password protected file is processed for positive selection, then attached to the email. This is distributed to all named recipients. If Votiro has already processed password protected files, additional users requesting files to be processed will be advised that this has already taken place.
<blockquote>Note
This feature supports the use of one password per email.</blockquote>
</td></tr>
</table>

Case	Processing Options
Large File	You can set the minimum size of files you want to block. When this option is checked, for every file that Votiro blocks, it issues a block-file containing the reason it was blocked. Accept the default text or edit it.
Complex File	You can set a layer number. The maximum layer number = 15. Files that are found in that layer or deeper are blocked.
Special Case	You will have already defined a Special Case with Votiro's support team. Click **Load File**. For more information, see Defining Policies on page 288.

2.18.13 Defining Policies by File Type

Policies have default settings that you can customize to meet your organization's requirements.

To define a policy by file type, from the navigation pane on the left, click **Settings** > **Policies**.



For more information about the policies page, see Policies Dashboard on page 287.

When defining a policy by file type, you can perform the following actions:

- Block the file under all conditions. If selected:
  - You can edit the default block notification message text, **Block Reason**.
  - Additional options may be available for you to set.
  - The **Default Action** displays a **red dot**.
- Sanitize the file. If selected:
  - You can modify the default behavior by customizing the option settings available.
  - If available, you can edit the default block notification message text, **Block Reason**.

- The **Default Action** displays a **green dot**.

- Allow the file. The **Default Action** displays a **grey dot**.
- Add one or more exceptions to the policy. The **Exceptions** displays the number of exceptions applied to the policy. For more information, see Adding Policy Exceptions on page 303.

The following table describes the processing options that are available for each file type:

Table 3 Positive Selection Processing Options for File Types

File Type	Processing Options
PDF	By default, these files are processed for positive selection. ■ **Remove multimedia**: Specifies whether multimedia such as embedded video, audio, 3D annotations, and rich media annotations must be removed. Default is checked. ■ **Remove metadata**: Specifies whether metadata must be removed. Metadata includes information about the document, such as author, keywords, copyright information, etc. Default is unchecked. ■ **Clean embedded fonts**: Specifies whether embedded fonts must be processed. Default is checked. Cleaning embedded fonts can: ♦ Remove unused characters – Only keeps the characters actually used in the document (called subset fonts). ♦ Deduplicate fonts – If the same font is embedded more than once, it consolidates them. ♦ Fix font metadata or corruption – Some tools repair malformed font data. (Fonts can technically be exploited to carry malicious code (in very rare and advanced attack scenarios)). ♦ Reduce file size – All of the above help shrink the PDF file size. ■ **JavaScript handling**: Determines how JavaScript, if found in the PDF file, is handled. ♦ Don't do anything ♦ Remove only suspicious scripts ♦ Remove all scripts (this is the default) ■ **QR Code handling**: Selects the action to perform on a QR code. ♦ Ignore - the QR Code is ignored. The file is passed on as-is. This is the default. ♦ 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. ■ **URL handling**: Selects the action to perform on a URL. ♦ 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. **Note**: Sanitization will remove empty file attachments.

File Type	Processing Options
Image	By default, these files are processed for positive selection. ■ **Add micro-changes**: Adds security noise to images during processing. Default is checked. **Note** Increasing the noise level might enlarge the processed files, particularly in the case of png files. Unselecting noise level (off) usually preserves an image file size. ■ **Remove metadata**: Removes EXIF metadata from JPEG, JPG and TIFF images. Default is unchecked. ■ **Remove external image**: Removes references to external image files in SVG image files. Default is unchecked. ■ **Remove external references**: Remove external references from SVG files to eliminate hidden vulnerabilities and ensure secure file handling. ■ **Max compression for lossless formats**: Compresses lossless image formats (PNG, BMP, and RAW) by 100%. Default is checked. ■ **Compression level**: The processed image is compressed to preserve a reasonable image file size. You select one of four compression levels (from low to high) that trade off file size with image quality. The lower the compression level, the larger the file, and the higher the image quality. The higher the compression level, the smaller the file, and the lower the image quality. Default is 25% compression.
Binary	The processing option is not relevant to managing binary files. You either block binary files or allow them.

File Type	Processing Options
Archive	By default, these files are processed for positive selection. **Block zip bomb**: Detects and blocks zip files with abnormal compression ratio. These might pose a denial of service threat, consuming system resources such as CPU or disk. Any zip files with compression ratio higher than 99.8% will be considered a zip bomb and be blocked. When selected you can edit the **Block Reason** message. Default is checked. **System locale**: Select your preferred system locale. This enables you to sanitize archive files with ANSI encoding according to the selected **System locale**. The available options are: ■ **en_US** - English (US) ■ **fr_FR** - French (France) ■ **de_DE** - German (Germany) ■ **he_IL** - Hebrew (Israel) ■ **ja_JP** - Japanese (Japan) ■ **ko_KR** - Korean (Korea) ■ **th_TH** - Thai (Thailand) The default **System locale** is **en_US**.
CAD	**Remove VBA Macros**: Removes VBA macros from the file. Default is unchecked.
RTF	By default, these files are processed. There are no specific processing options.
HTML Attachments	There is an additional option: **Remove scripts**. This is the default action. If this option is selected, every script will be removed from the HTML Attachment file.

File Type	Processing Options
Email	By default, these files are processed for positive selection. ■ **Remove suspicious links in Email body**: The system will scan each URL in the email body, and if a suspicious link was found, the link will be removed and will be replaced with the following text: "This link was removed because it is a malicious URL". ■ **Include URL to Password-protected portal**: Includes a link to the Password-protected portal (see Password Protected Portal). ■ **Add sanitization indication in Email body**: Adds an indication of the sanitization status in the body of the Email. ■ **QR Code handling**: Selects the action to perform on a QR code. ♦ Ignore - the QR Code is ignored. The email is passed on as-is. This is the default. ♦ 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

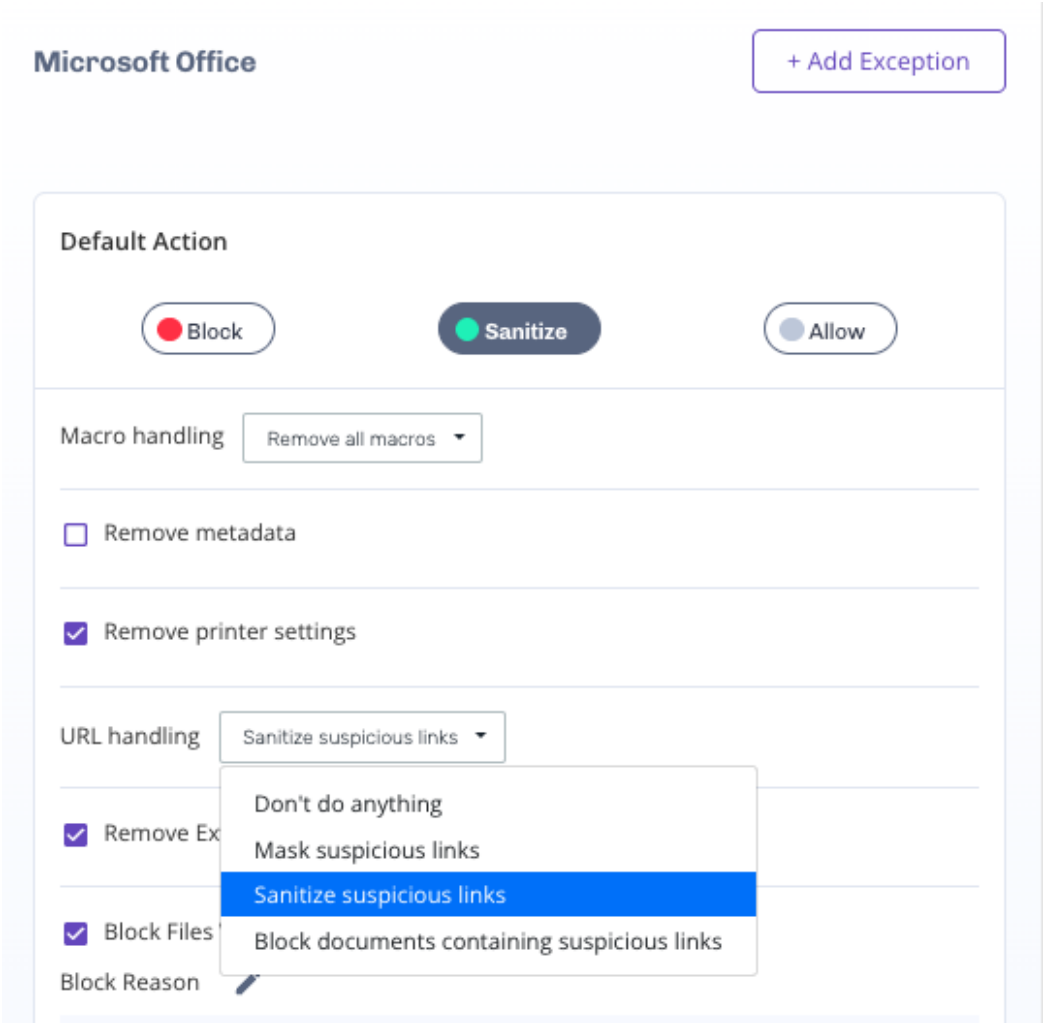
File Type	Processing Options
Microsoft Office **Note** - Positive selection processing applies to Microsoft Office files and their embedded objects. - Each attached file is processed recursively by running all policy rules on it.	By default, these files are processed for positive selection. - **Block files with suspicious links**: Performs a check of all links in the form HTTP:// and HTTPS:// in Microsoft Word files. If any link is found to be suspicious, it is removed from the file. When selected you can edit the **Block Reason** message. Default is unchecked. **Note** This option is available for DOC/DOCX/XLSX file types only. - **Macro handling**. In the list, choose one of the following: ♦ **Don't do anything** ♦ **Remove only suspicious macros**: Remove all macros only if any suspicious code is found. ♦ **Remove all macros**: Remove all macros from the document. This is the default option. ♦ **Block documents containing suspicious macros**: Block the entire document if suspicious code is found in the macro. - **URL handling**: Selects the action to perform on a URL for Word or Excel files. ♦ 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. **Note** Excel files with **4.0 macro** (also known as **sheet macro**) are automatically blocked. It is common practice to use VBA macros. Excel files with VBA macros are checked for suspicious code (see options above). - **Remove metadata**: Removes metadata, such as Author, Company, LastSavedBy, and so on. Default is unchecked. - **Remove printer settings**: Removes the printerSettings1.bin (printer settings) embedded in a .xlsx file. Default is checked. - **Remove external links**: Removes links that can point to locations external to the office files. If unchecked (default), suspicious elements are not detected.

File Type	Processing Options
	■ **Block files with Dynamic Data Exchange (DDE)**: Blocks all files with DDE. Default is unchecked.
Text	**Note** XML and JSON files are processed according to the Text files policy. By default, these files are processed for positive selection. If any suspicious activity is detected, the file is blocked. If no suspicious activity is detected, the text file is preserved (the file hash will remain the same). **Block CSV with threat formula**: Blocks CSV files that contain formula injections.When selected you can edit the **Block Reason** message. Default is checked.
Media	The user can set Media file policy exceptions. ■ **Remove metadata**: Removes metadata from media files. Default is unchecked.
Open Document	The user can set Open Document file policy exceptions. By default, these files are sanitized. During the sanitization, the macros will not be preserved.
Ichitaro	■ **Remove macros**: Removes macros from the document. Default is checked. ■ **Preserve original Ichitaro OLE objects**: Preserves OLE controls and OLE sheets. Default is checked.

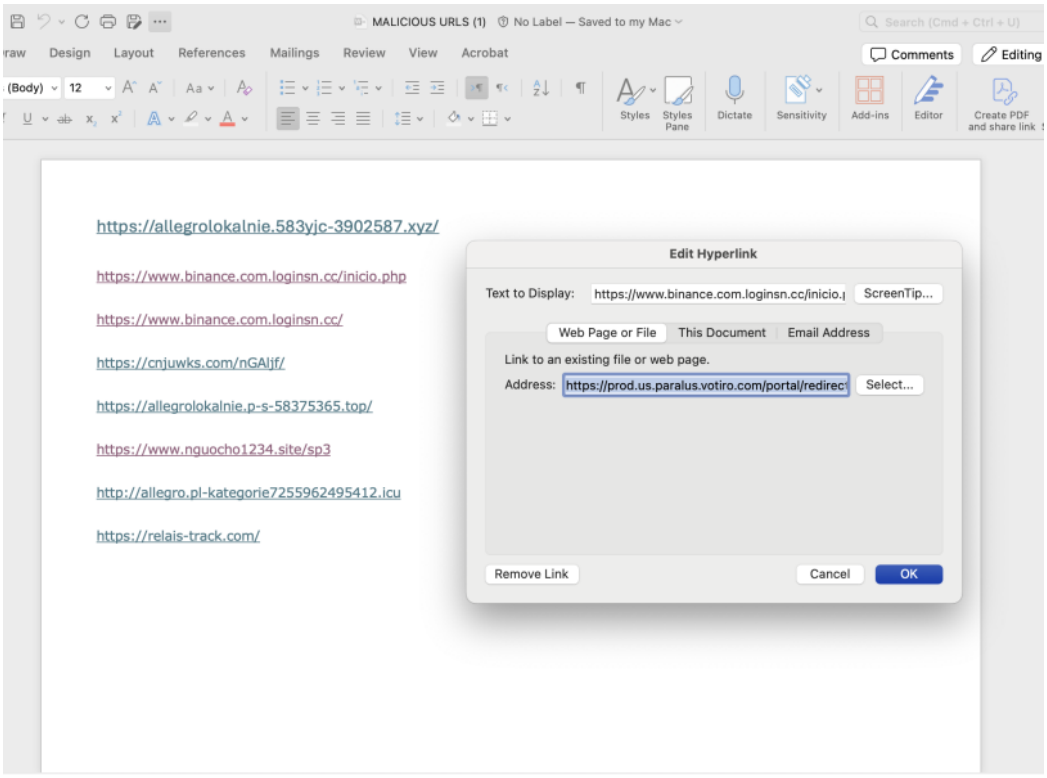
File Type	Processing Options
Hancom	■ **Remove macros**: Removes macros from the document. Default is checked. ■ **Remove scripts**: Removes scripts from the document. Default is checked. ■ **Remove metadata**: Removes metadata from the document. Default is checked. ■ **Remove printer settings**: Removes printer settings from the document. Default is checked. ■ **Remove Embedded Fonts**: Removes embedded fonts from the document. Default is checked. ■ **URL handling**: Selects the action to perform on a URL for Hancom files. ♦ 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. ■ **Remove External Links**: Removes external links from the document. Default is checked.
Other files	By default, these files are blocked. You can edit the **Block Reason** message. There are no specific sanitization processing options.

Workflow - Sanitize URLs

1. The user defines URL handling of PDF, Word and Excel files:

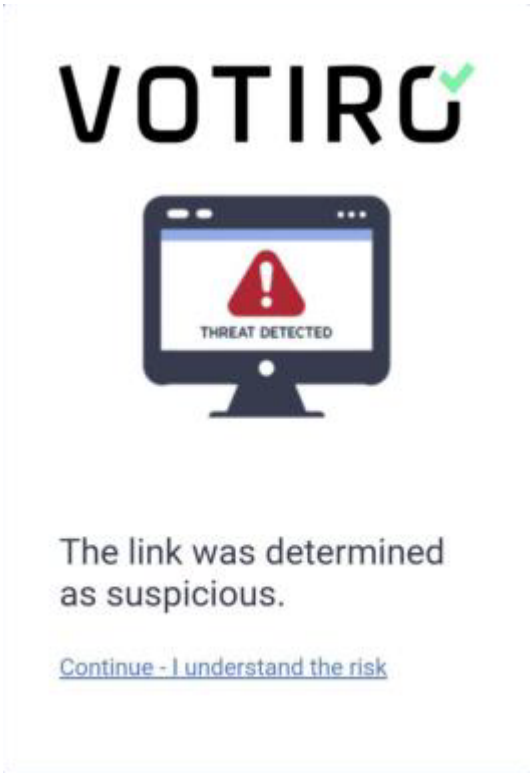


2. A protected user receives a file from a URL.
3. When the user clicks on the URL, the user will be redirected to the Votiro portal.

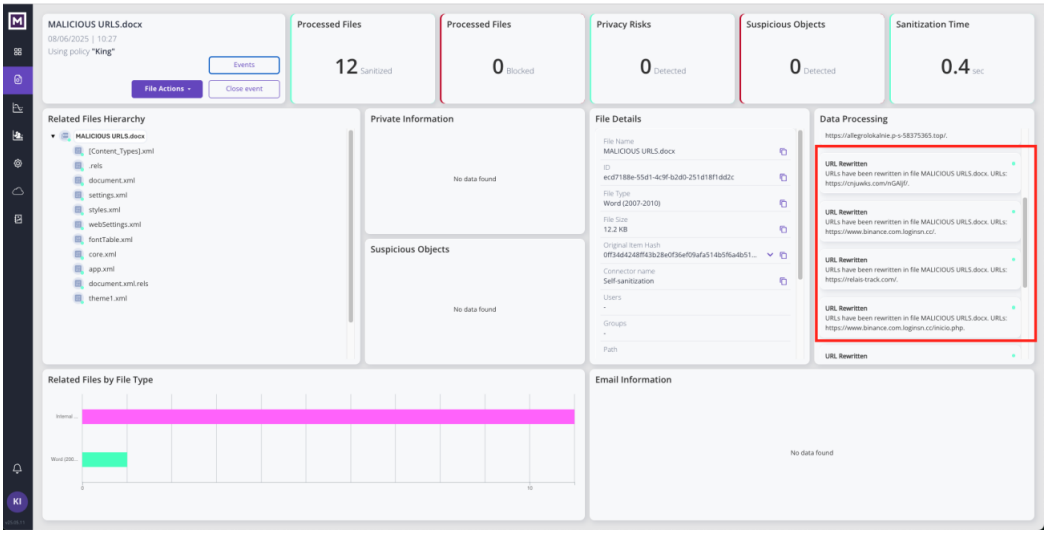


4. If the URL was determined to be benign, the user will be redirected to the desired URL.

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.



2.18.14 Adding Policy Exceptions

Policies have default settings that you can customize to meet your organization's requirements, including adding exceptions.

You can define one or more exceptions to any case policy or file type policy. Exceptions can be based on the following criteria:

- File type

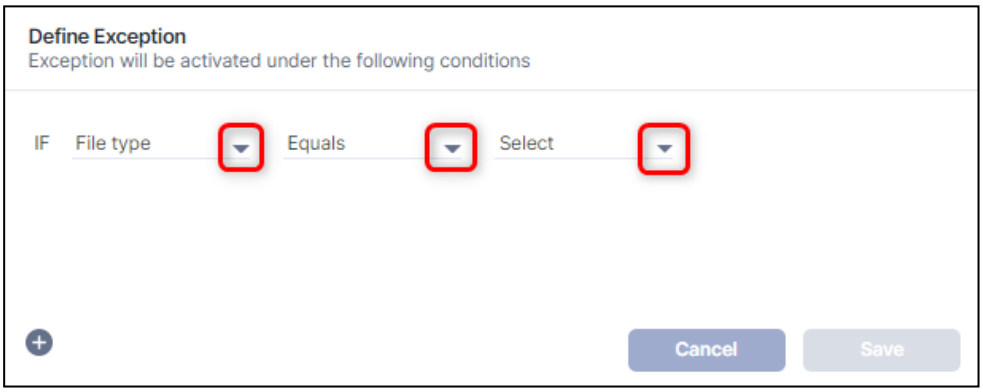
- File size
- Email (for Votiro On-prem for Email only)
- File extension
- Digital signature

For more information about the policies page, see Policies Dashboard on page 287.

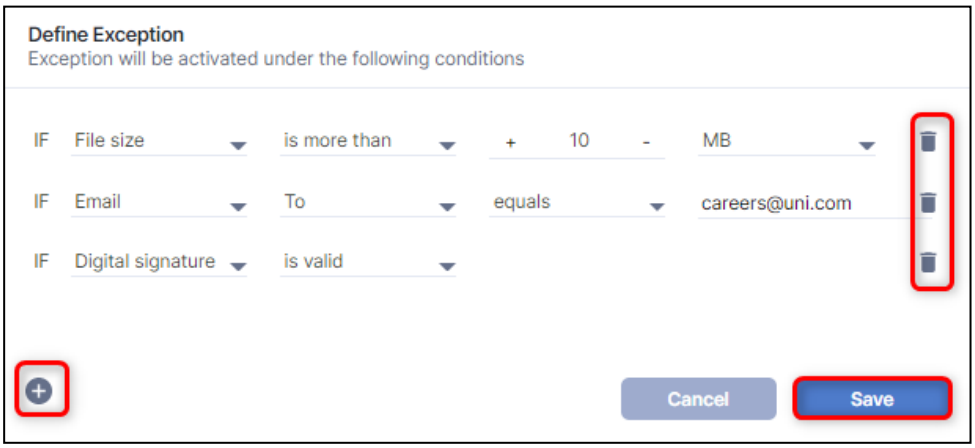
Adding an Exception:

To add an exception to a policy, follow these steps:

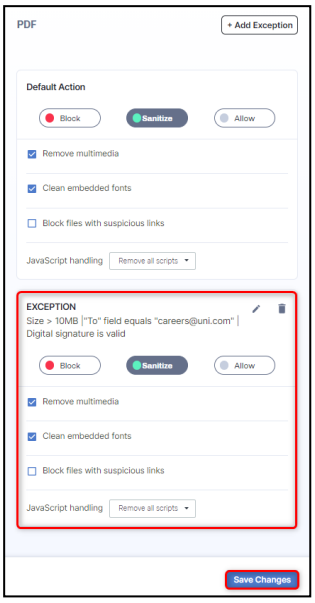
1. From the navigation pane on the left, click **Settings** > **Policies**.
2. Click the case or file type policy you wish to define an exception for.
3. In the top right corner, click **+ Add Exception**. The Define Exception window appears:



4. Define at least one condition to base the exception on. Create a condition by selecting values from lists, or entering text, as appropriate.
5. To add another condition to the exception definition, click the plus (+) icon. To delete a condition, click the trash icon.

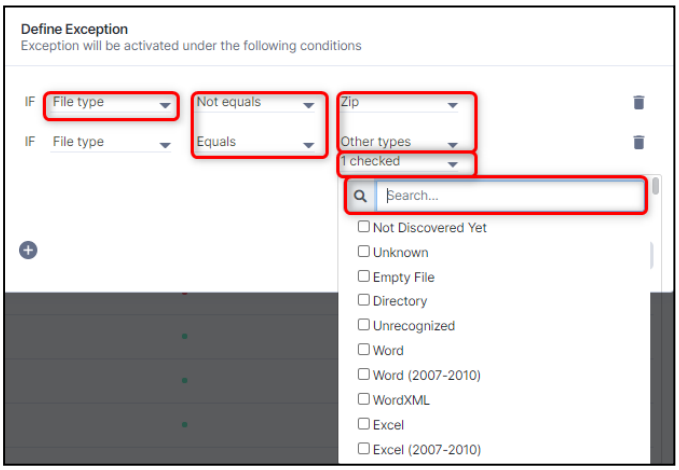


6. When your exception definition is complete you can activate the exception by clicking **Save**. To abandon the exception definition, click **Cancel**. You will return to the policy page.



7. The exception is added to the right pane. To add the exception to the policy, click **Save Changes**.

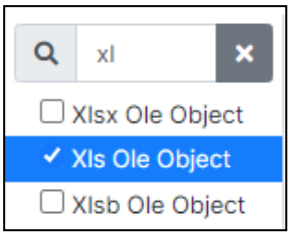
Defining Exceptions for File Types



To specify an exception for one or more file types:

1. In the leftmost list, select **File Type**.
2. In the second list, select **Equals** or **Not Equals**.
3. In the last list, select one or more relevant file types. The list displays the most common types.

To select a type that does not appear in the list, select **Other types**. Click **checked** to activate the **|Search**bar. Enter search criteria and select one or more file types.



4. Proceed to Step 6 in Adding an Exception: in this section.

Defining Exceptions for File Size

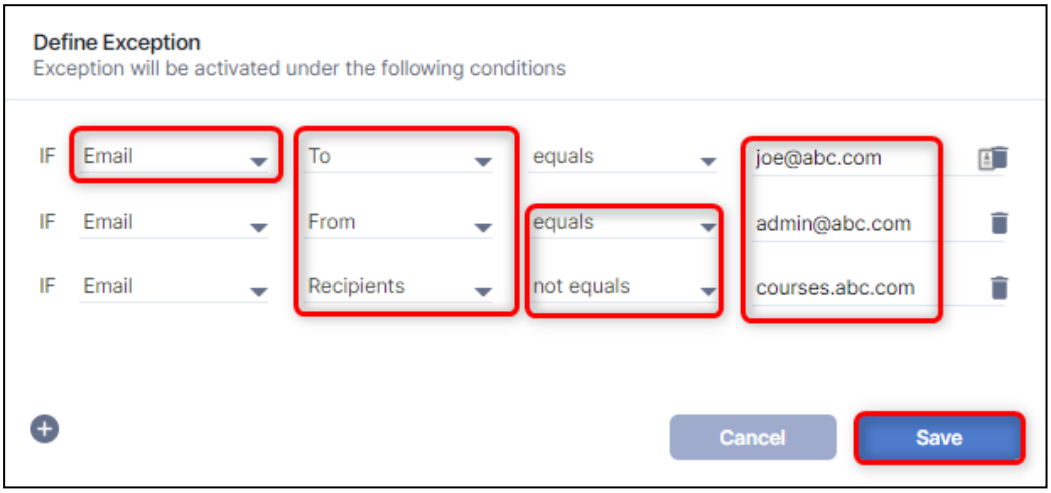
To specify an exception based on on file size:

1. In the leftmost list, select **File Size**.
2. In the second list, select **Is more than** or **Is less than**.
3. In the input field, type in a numeric value for the size, or use the **+** and **-** buttons.
4. In the last list, select Bytes, KB, MB, GB, or TB.
5. Proceed to Step 6 in Adding an Exception: in this section.

Note

- File sizes are measured in bytes.
- Files up to 100 MB can be uploaded for positive selection processing.

Defining Exceptions for Email Senders or Recipients



You can specify any of the following:

- From: For emails from a particular sender, or a specific domain.
- To: For emails to a particular recipient.
- CC: For emails to a particular CC-ed recipient.
- Recipients: For emails to recipients that appear in To, CC, or BCC fields.

Defining Email and Domain Addresses - Full and Partial

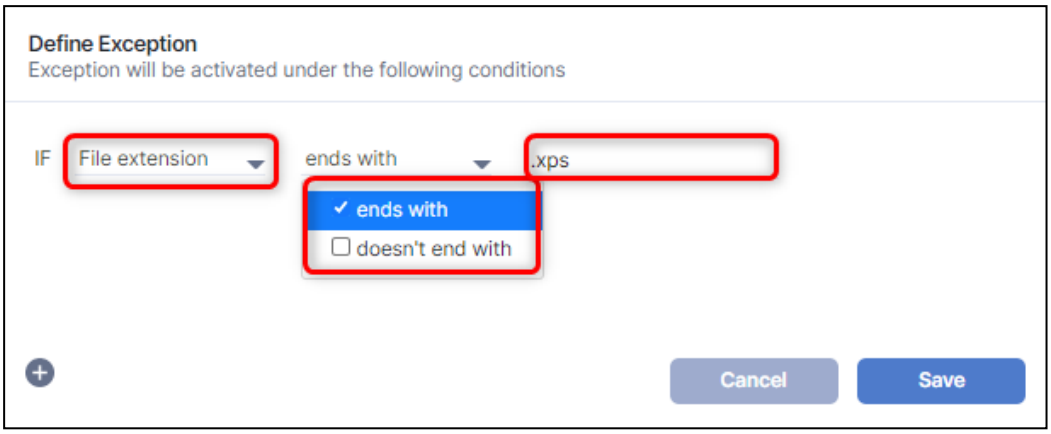
You can specify:

- An exact email or domain address by selecting **Equals** or **Not Equals**.
- A partial domain address by selecting **Include address**.

Guidelines and examples:

- Specify a full email address, including the **@** sign. For example, *joe@abc.com*.
- Partial email addresses are not accepted. For example, *@abc.com* or *joe@*.
- Specify full or partial domains. For example, *abc.com* or *courses.xyz.info*

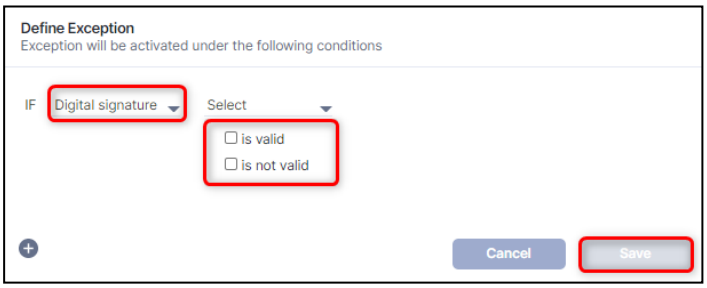
Defining Exceptions for File Extensions



To specify a list of file type extensions:

1. In the leftmost list, select **File Extension**.
2. In the second list, select **Ends with** or **Doesn't end with**.
3. In the text field, type in the extensions you need. Separate them with commas. For example: DOC,PDF,XLSX.
4. Proceed to Step 6 in Adding an Exception: in this section.

Defining Exceptions for Validating Signatures



To specify an exception for a file with a digital signature, select **Is valid** or **Is not valid**.

A signature is considered valid if it contains a valid timestamp from a trusted Timestamp Authority (TSA). This timestamp proves the signature's integrity and validity at a specific point in time, even if the signing certificate has expired.

Note: Files with digital signatures from the following compliance standards are supported by Votiro and are valid by default:

- **AATL** - Adobe Approved Trust List
- **EUTL** - European Union Trusted Lists
- **FPKI** - (US) Federal Public Key Infrastructure
- **CCA** - (India) Controller of Certifying Authorities

2.18.15 Audit Events to SIEM

Overview

For a large enterprise, there will be many security products deployed. The SOC (Security Operations Center) team must handle many products, which all generate alerts/cases regarding potential cyber attacks. Because it is almost impossible to attend to every management console, and because there is a need to correlate between different systems, almost every enterprise uses a single pane of glass (SPOG). The SPOG in the context of SIEM (Security Information and Event Management) software refers to a unified dashboard that consolidates data, insights, and controls from various security tools, providing a comprehensive view of an organization's security posture in one place. This allows security teams to monitor, analyze, and respond to threats more effectively, rather than juggling multiple interfaces.

There are different standard ways to communicate to the SIEM. The most popular one is the Syslog. Votiro's Syslog messages include all the important information related to the sanitized files and can help correlate this information to other IOCs (Indicators Of Compromise) and to define automation for remediation.

What is SIEM

Security Information and Event Management (SIEM) is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure.

SIEM collects security data from network devices, servers, domain controllers, and more. SIEM stores, normalizes, aggregates, and applies analytics to that data to discover trends, detect threats, and enable organizations to investigate any alerts.

Votiro logs can be sent to SIEM in Common Event Format (CEF) or Log Event Extended Format (LEEF).

To enable SIEM logging, you must configure the SIEM settings in the Management Dashboard.

Votiro Audit Events Syslog message format

Field #	Field name	Description	Value
1	Timestamp	Event timestamp based on customer time	{MMM DD HH:mm:SS} For example, Mar 10 07:07:32
2	Syslog message format	Syslog message format	For CEF format: **CEF:0** For LEEF format: **LEEF:1.0**
3	Device vendor	Vendor name	**Votiro**
4	Device name	Device name	**Votiro**
5	Device version	Product version	{Product version} For example, 9.8.100

Field #	Field name	Description	Value
6	Signature ID	Signature ID of the event	**600**
7	Message name	Syslog message name	**Audit event**
8	Message severity level	Message severity level (numeric) **Note**: All events will be of the same severity level.	**5**
9	Company name	Customer's company name (string) configured in the Management dashboard.	{Company name}
10	Correlation ID	Unique GUID that represents the event ID	{GUID}
11	msg	Message content	(string) see the event message template below
12	suser	The user that performed that action	{character string}
13	Changes	Will display the changes that were performed in the actions. *Relevant only for events where changes were made	{character string} For example, pdf

Audit Event Types

Audit events that should be sent for every user action:

- Login - success, failure
- Files actions - Download original/sanitized, Release original
- Release PPF (Only for email v10.0)
- System configuration
- SMTP
- SAML
- Active Directory
- Users/Local users
- SIEM
- Service Token (Created, Deleted)
- License (License expiration date)
- CDR Policies actions (changes performed on policies)

Out of scope:

- Customization (Out of scope for v10.0)
- Connectors (Out of scope for v10.0)
- DDR Policies actions (Out of scope for v10.0)
- Download/Release unmasked (Out of scope for v10.0)

Audit Event Message Examples

Event Message content	Example
User {username} logged in to Management	Mar 10 07:07:32 CEF:0 | Votiro|Votiro cloud|600|Audit Event|5|CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=User 'Ron' logged in to Management suser=Ron
User {username} failed to authenticate	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=User 'Ron' failed to authenticate suser=Ron
Original file {File Name} has been downloaded by User {username}	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=Original file 'RonIsTheKing.docx' has been downloaded suser=Ron
Sanitized file {File Name} has been downloaded by User {username}	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=Sanitized file "RonIsTheKing.docx" has been downloaded suser=Ron
Original file {File Name} has been released by User {username}	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=Original file 'RonIsTheKing.docx' has been released suser=Ron

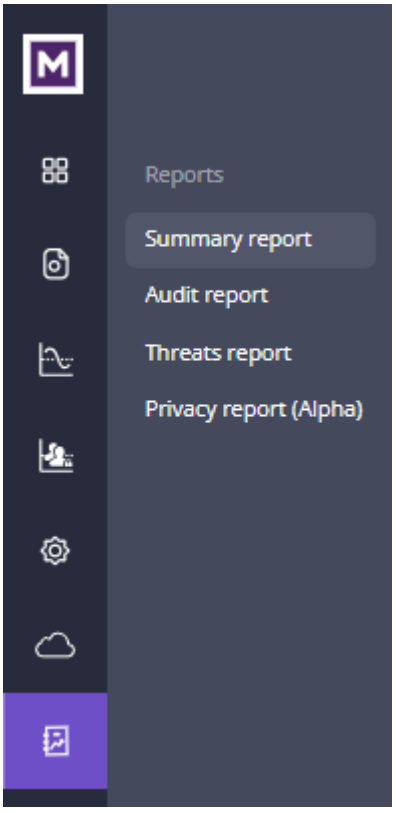
Event Message content	Example
Policy {Policy Name} has been created	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=Policy 'King' has been created suser=Ron
Policy {Policy Name} has been updated, changes: {change description} {oldValue} {newValue}	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=Policy 'King' has been updated changes=PDF case command has been changed oldValue=Blocked newValue=Sanitized suser=Ron
	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=9806 1190-e3e2-438bb9cb-88941c0a6371 msg=Policy 'King' has been updated changes=Exception has been added to PDF case has been changed oldValue=null newValue=null suser=Ron
Policy {Policy Name} has been deleted	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=Policy 'King' has been deleted suser=Ron
Report {Report Name} has been exported	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=Report "Audit report" has been exported suser=Ron
Configuration {Configuration Key} has been updated {oldValue} {newValue}	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=Configuration "Blob files days to keep" has been updated oldValue=180 newValue=90 suser=Ron

Event Message content	Example
Role has been changed for user {userName} {oldValue} {newValue}	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=Role has been changed for user 'King' oldValue=SOC newValue=Helpdesk suser=Ron

2.19 Generating Reports

The Reporting feature provides a deeper look at positive selection activity performed by Votiro on file and email traffic flowing through your network.

From the Reports page in the Management Dashboard, you can generate the following reports:



2.19.1 Summary Report

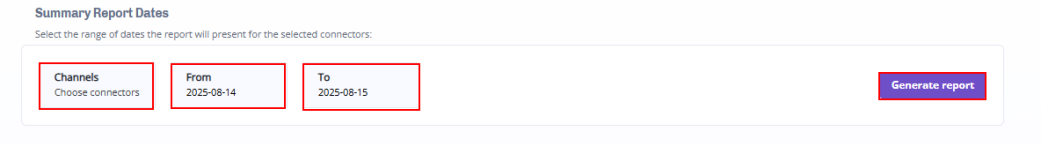
You can generate a summary report of the positive selection processing activity in your organization for a specified period.

The report collects useful data of the activity for all stakeholders. For example, the system administrator can use this report for making data-driven decisions to optimize the company's policy, for maximum security and minimum interference to your business.

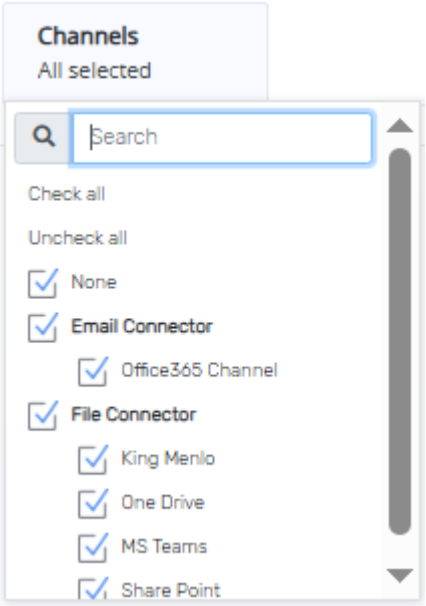
The report presents usage and security date in graphic format and also provides tips for optimizing your positive selection processing effort.

To generate a Summary report, follow these steps:

1. In the navigation pane, click **Reports** > **Summary report**.

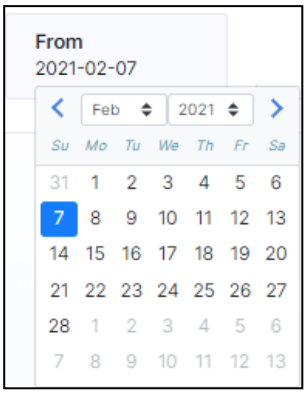


2. Click **Channels**, then select the connectors you wish to appear in the report.



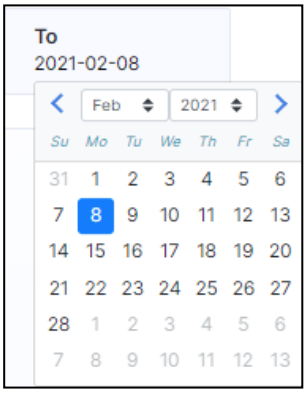
3. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:

a. To select the start date from the report, click **From**, a calendar displays.



The selected date is blue. To change the start date navigate to the desired start month and year by clicking the right and left arrows, or by selecting a month and year using the up/down arrows. Then tap the day for the report to start from.

b. To select the end date from the report, click **To**, a calendar displays.



The selected date is blue. To change the end date for the report use the selection steps described in **3a** above, tapping the day for the report to end.

4. Click **Generate Report**. The Summary report is generated.

Summary Report Format and Structure

The report is in PDF format and provides the following information:

- Company name.
- Number of processing requests to Votiro's Positive Selection® Engine.
- Number of individual files that were processed Votiro's Positive Selection® Engine.
- Number of files that were blocked.
- Number of threats that attempted to enter your organization.
- Number of files that were blocked according to each positive selection policy.
- Number of files that were blocked and that were detected as threats.

- Number of files that were blocked that were not threats.
- Average processing time in seconds/KB.
- File types that passed through the Positive Selection® Engine.
- Number of threats that attempted to enter your organization.
- Most threatening file types that were sent to your organization.

2.19.2 Audit Report

The purpose of this report is to present details of actions performed in the Management Dashboard for audit and tracking.

To protect enterprise privacy, Votiro tracks every login, change, request for file download and other actions that were performed in the Management Dashboard.

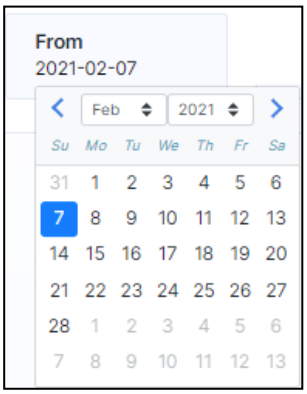
You can audit all actions that were performed by users of the Management Dashboard for a specified period. The exported report generated is a CSV file.

To generate an Audit report, follow these steps:

1. In the navigation pane, click **Reports** > **Audit report**.

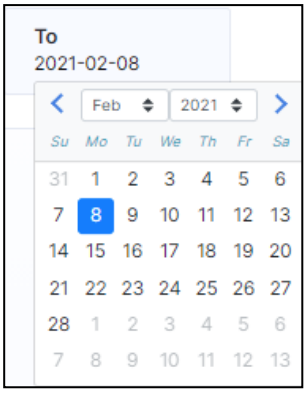
2. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:

   a. To select the start date from the report, click **From**, a calendar displays.



   The selected date is blue. To change the start date navigate to the desired start month and year by clicking the right and left arrows, or by selecting a month and year using the up/down arrows. Then tap the day for the report to start from.

   b. To select the end date from the report, click **To**, a calendar displays.



The selected date is blue. To change the end date for the report use the selection steps described in **2a** above, tapping the day for the report to end.

3. Click **Generate Report**. The Audit report is generated.

Audit Report Format and Structure

The audit information is output in CSV format and includes: a datestamp (in UTC time), a username, and a description of the action logged.

The following is an example excerpt as viewed in a spreadsheet application:

1/11/2018 11:52	RonF	LoginEvent	Successful login with Full permissions	
1/11/2018 13:05	user1	PolicyAddEvent	A new policy was created	policyId: 37a0add2-b521-442c-
1/11/2018 14:46	Default (unauthori	LoginEvent	Successful login with Full permis	
1/11/2018 15:07	RonF	LogoutEvent	Logout	
1/11/2018 15:41	Default (unauthori	LoginEvent	Successful login with Full permis	
1/11/2018 16:02	Default (unauthori	PolicyDeleteEvent	Policy 321_deleted_6367669212	policyId: 3d24ce9e-faca-4004-
1/11/2018 16:02	Default (unauthori	PolicyUpdateEvent	Policy jhg was changed	policyId: aab369db-32dd-4bad-
1/11/2018 16:03	Default (unauthori	ConfigurationEvent	3 Configuration record/s were u	updates:
1/11/2018 16:03	Default (unauthori	LogoutEvent	Logout	
1/11/2018 16:03	user1	LoginEvent	Successful login with Full permis	
1/11/2018 16:03	user1	UsersEvent	1 user/s permissions were upda	updates: Updated RonF from

Information is provided for the following actions:

- Login
- Logout
- Original file download
- Processed file download
- Release original
- Policy save
- Settings save
- Roles changes
- Report export
- Policy creation

- Create user
- Delete user
- Reset password

2.19.3 Threats Report

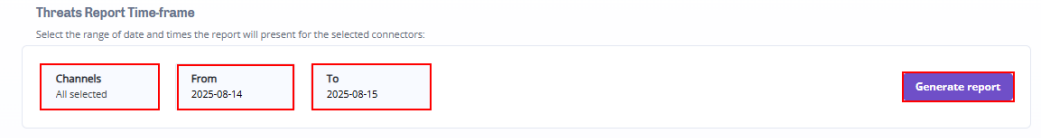
Votiro tracks threats to files submitted for testing in the Management Dashboard.

You can generate a threat report of the activity in your organization for a specified period.

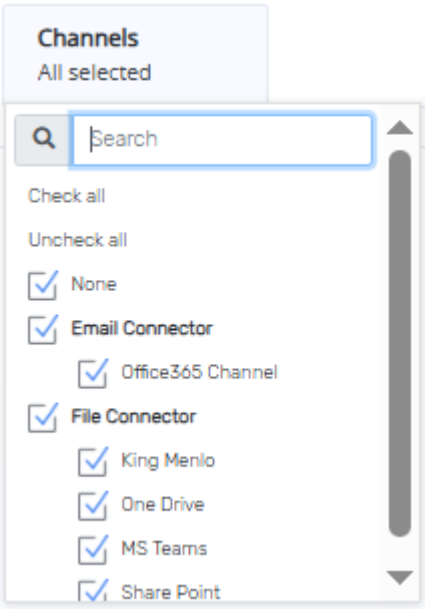
The report collects useful data of the positive selection processing activity. The threat report files generated are used internally by Votiro for support and research purposes.

To generate a Threats Report, follow these steps:

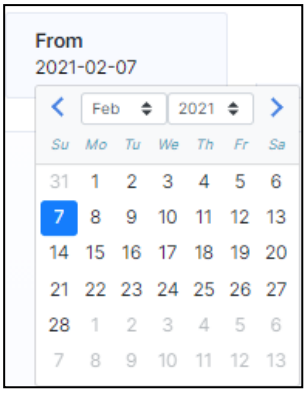
1. In the navigation pane, click **Reports** > **Threats report**.



2. Click **Channels**, then select the connectors you wish to appear in the report.

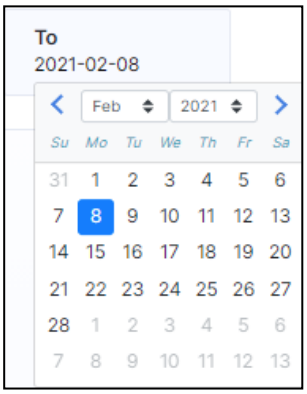


3. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:



a. To select the start date from the report, click **From**, a calendar displays.

The selected date is blue. To change the start date navigate to the desired start month and year by clicking the right and left arrows, or by selecting a month and year using the up/down arrows. Then tap the day for the report to start from.



b. To select the end date from the report, click **To**, a calendar displays.

The selected date is blue. To change the end date for the report use the selection steps described in **2a** above, tapping the day for the report to end.

4. Click **Generate Report**. The Threats report is generated.

Threat Report Format and Structure

The output generated is in csv format. The threat report file name is in the format **Votiro_Threat_Report_***<From date>*_*<To date>***.csv**, where *<From date>* and *<To date>* specify the date range selected by the user.

The header at the beginning of the threat report contains the following fields:

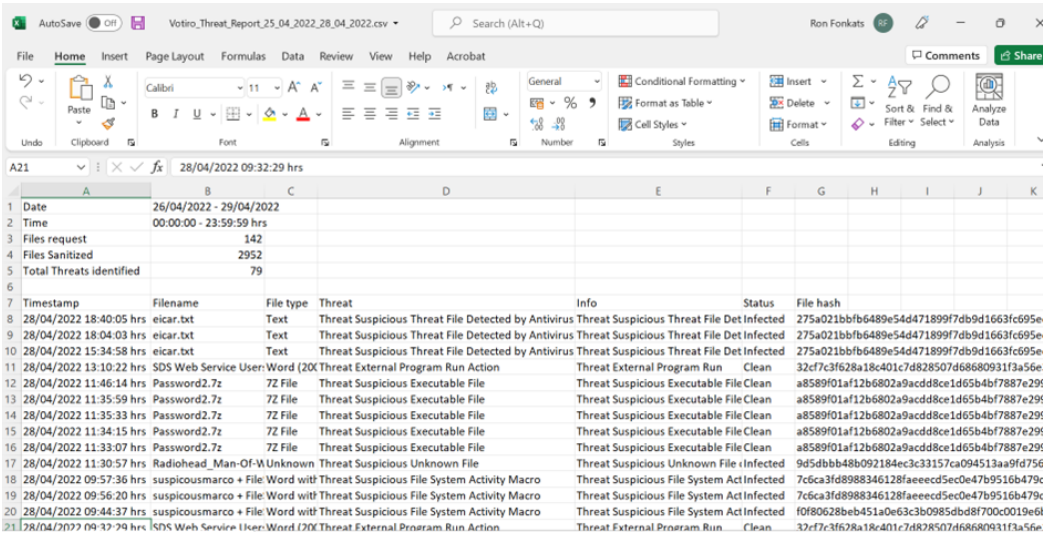
- **Date** - Date of generated data, or *<start date>* **-** *<end date>*
- **Time** - Time-frame period of the generated data (based on customer local time)
- **Files request** - Number of files requested to be checked in the time-frame period
- **Files Sanitized** - Number of files sanitized in the time-frame period

- **Total Threats Identified** - Number of threats identified in the time-frame period

The body of the threat report contains the following fields:

Field	Value	Multi-values	Example
Timestamp	DD-MMM-YYYY hh:mm:ss ”hrs” *Based on customer local time (Same as the Management dashboard time)	Not supported	18Mar2022 18:49:29hrs
Filename	Parent file name	Not supported	VotiroDemo.zip
File type	Parent file type	Not supported	Zip File
Threat	List of the threats that have been identified on the Parent and Children *Should be sorted as the file tree from the Management File info	Supported	Suspicious Unknown File Suspicious Unknown File
Info	List of all threats and the file names associated with these threats *Should match to the sort from the threat column Format: “Threat X detected in File Y”	Supported	Suspicious Unknown File detected in VotiroDemo1.shx Suspicious Unknown File detected in VotiroDemo2.shp
Status	Parent file status result	Not supported	Status options: Infected, Clean, Error, Unknown
File hash	Parent file hash	Not supported	7cd6773d80d4cdf28671d9e3a095c66fdc20feaac15c4e0754748dbd2541a7e9

Threat Report Example



	A	B	C	D	E	F	G
1	Date	26/04/2022 - 29/04/2022					
2	Time	00:00:00 - 23:59:59 hrs					
3	Files request	142					
4	Files Sanitized	2952					
5	Total Threats identified	79					
6							
7	Timestamp	Filename	File type	Threat	Info	Status	File hash
8	28/04/2022 18:40:05 hrs	eicar.txt	Text	Threat Suspicious Threat File Detected by Antivirus	Threat Suspicious Threat File Det	Infected	275a021bbfb6489e54d471899f7db9d1663fc695e
9	28/04/2022 18:04:03 hrs	eicar.txt	Text	Threat Suspicious Threat File Detected by Antivirus	Threat Suspicious Threat File Det	Infected	275a021bbfb6489e54d471899f7db9d1663fc695e
10	28/04/2022 15:34:58 hrs	eicar.txt	Text	Threat Suspicious Threat File Detected by Antivirus	Threat Suspicious Threat File Det	Infected	275a021bbfb6489e54d471899f7db9d1663fc695e
11	28/04/2022 13:10:22 hrs	SDS Web Service User:	Word (20(	Threat External Program Run Action	Threat External Program Run	Clean	32cf7c3f628a18c401c7d828507d68680931f3a56e
12	28/04/2022 11:46:14 hrs	Password2.7z	7Z File	Threat Suspicious Executable File	Threat Suspicious Executable File	Clean	a8589f01af12b6802a9acdd8ce1d65b4bf7887e29
13	28/04/2022 11:35:59 hrs	Password2.7z	7Z File	Threat Suspicious Executable File	Threat Suspicious Executable File	Clean	a8589f01af12b6802a9acdd8ce1d65b4bf7887e29
14	28/04/2022 11:35:33 hrs	Password2.7z	7Z File	Threat Suspicious Executable File	Threat Suspicious Executable File	Clean	a8589f01af12b6802a9acdd8ce1d65b4bf7887e29
15	28/04/2022 11:34:15 hrs	Password2.7z	7Z File	Threat Suspicious Executable File	Threat Suspicious Executable File	Clean	a8589f01af12b6802a9acdd8ce1d65b4bf7887e29
16	28/04/2022 11:33:07 hrs	Password2.7z	7Z File	Threat Suspicious Executable File	Threat Suspicious Executable File	Clean	a8589f01af12b6802a9acdd8ce1d65b4bf7887e29
17	28/04/2022 11:30:57 hrs	Radiohead_Man-Of-W	Unknown	Threat Suspicious Unknown File	Threat Suspicious Unknown File	Infected	9d5dbbb48b092184ec3c33157ca094513aa9fd756
18	28/04/2022 09:57:36 hrs	suspicousmarco + File:	Word with	Threat Suspicious File System Activity Macro	Threat Suspicious File System Act	Infected	7c6ca3fd8988346128faeeecd5ec0e47b9516b479c
19	28/04/2022 09:56:20 hrs	suspicousmarco + File:	Word with	Threat Suspicious File System Activity Macro	Threat Suspicious File System Act	Infected	7c6ca3fd8988346128faeeecd5ec0e47b9516b479c
20	28/04/2022 09:44:37 hrs	suspicousmarco + File:	Word with	Threat Suspicious File System Activity Macro	Threat Suspicious File System Act	Infected	f0f80628beb451a0e63c3b0985dbd8f700c0019e6
21	28/04/2022 09:32:29 hrs	SDS Web Service User:	Word (20(	Threat External Program Run Action	Threat External Program Run	Clean	32cf7c3f628a18c401c7d828507d68680931f3a56e

2.19.4 Privacy Report

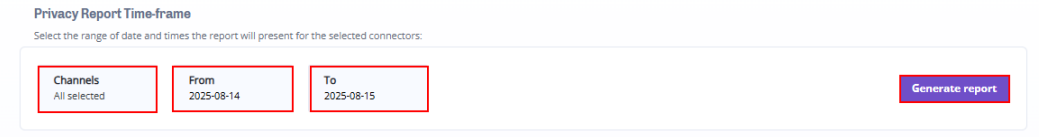
Votiro tracks files containing sensitive data submitted for testing in the Management Dashboard.

You can generate a privacy report of the activity in your organization for a specified period.

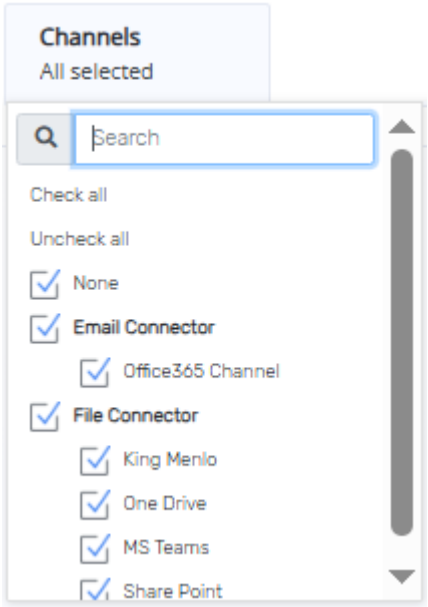
The report collects statistics of the sensitive data activity. The privacy report files generated are used internally by Votiro for support and research purposes.

To generate a Privacy Report, follow these steps:

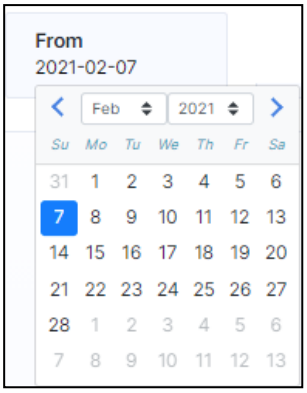
1. In the navigation pane, click **Reports** > **Privacy report**.



2. Click **Channels**, then select the connectors you wish to appear in the report.

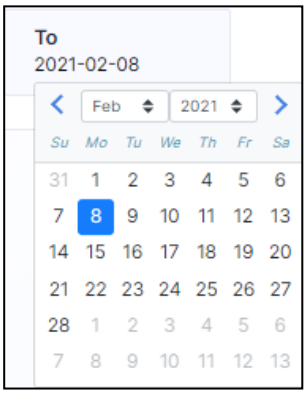


3. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:



a. To select the start date from the report, click **From**, a calendar displays.

The selected date is blue. To change the start date navigate to the desired start month and year by clicking the right and left arrows, or by selecting a month and year using the up/down arrows. Then tap the day for the report to start from.



b. To select the end date from the report, click **To**, a calendar displays.

The selected date is blue. To change the end date for the report use the selection steps described in **2a** above, tapping the day for the report to end.

4. Click **Generate Report**. The Privacy report is generated.

Privacy Report Format and Structure

The report is in PDF format and provides the following information:

- Company name
- Organization Privacy Overview - histogram displaying:
  - Total files with privacy data according to privacy data type
  - Total sensitive users
- Sensitive Users view - histogram displaying:
  - Number of files with privacy data type by user
- Data Type observation - pie charts displaying:

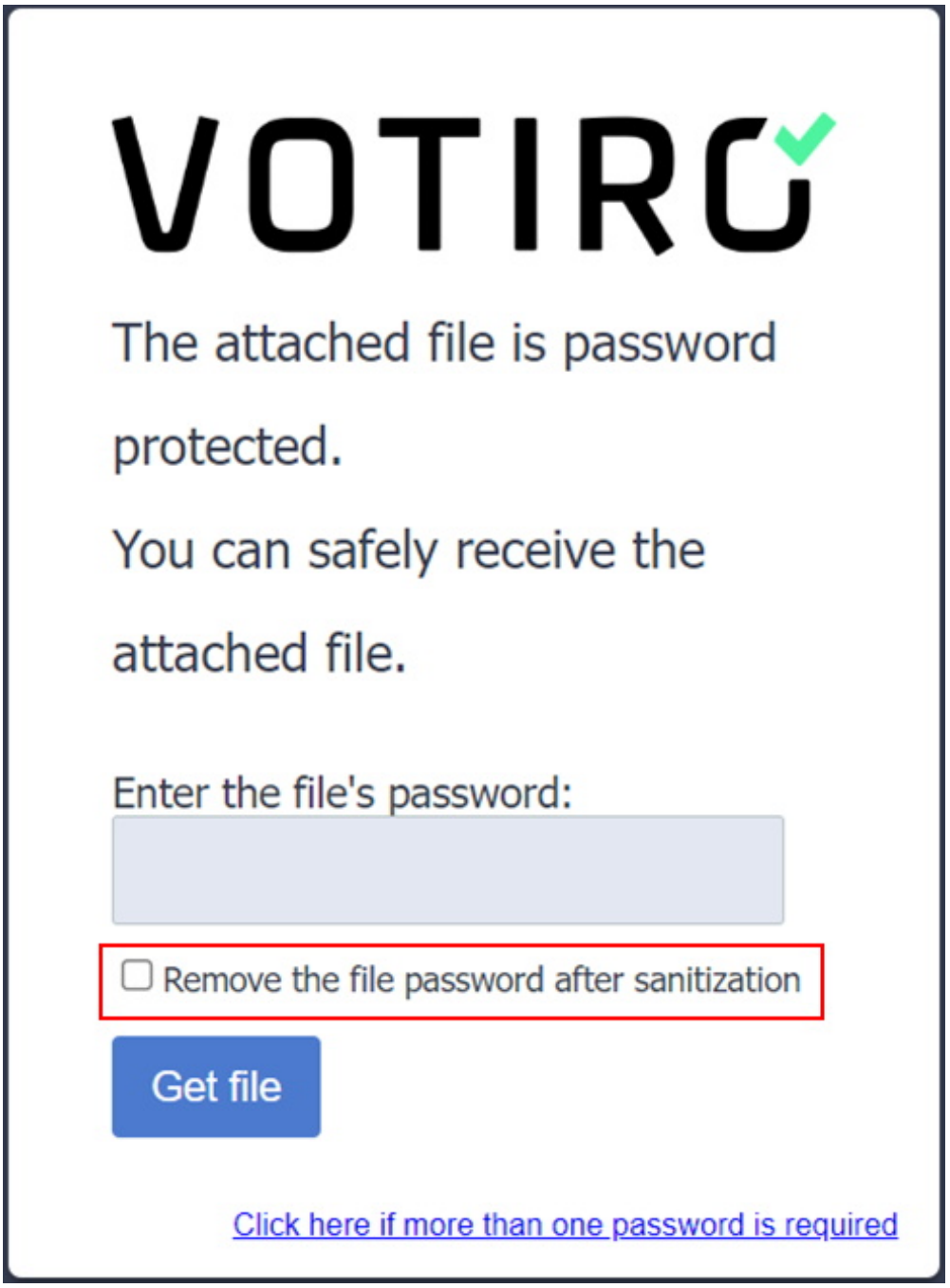
- Data Type by Label
- Sensitive data by channel

2.20 Password Protected Portal

2.20.1 Removing PPF Encryption

> **Note**
> To enable this feature, please contact Votiro support.

You can remove file password protection after sanitization by checking the following box:



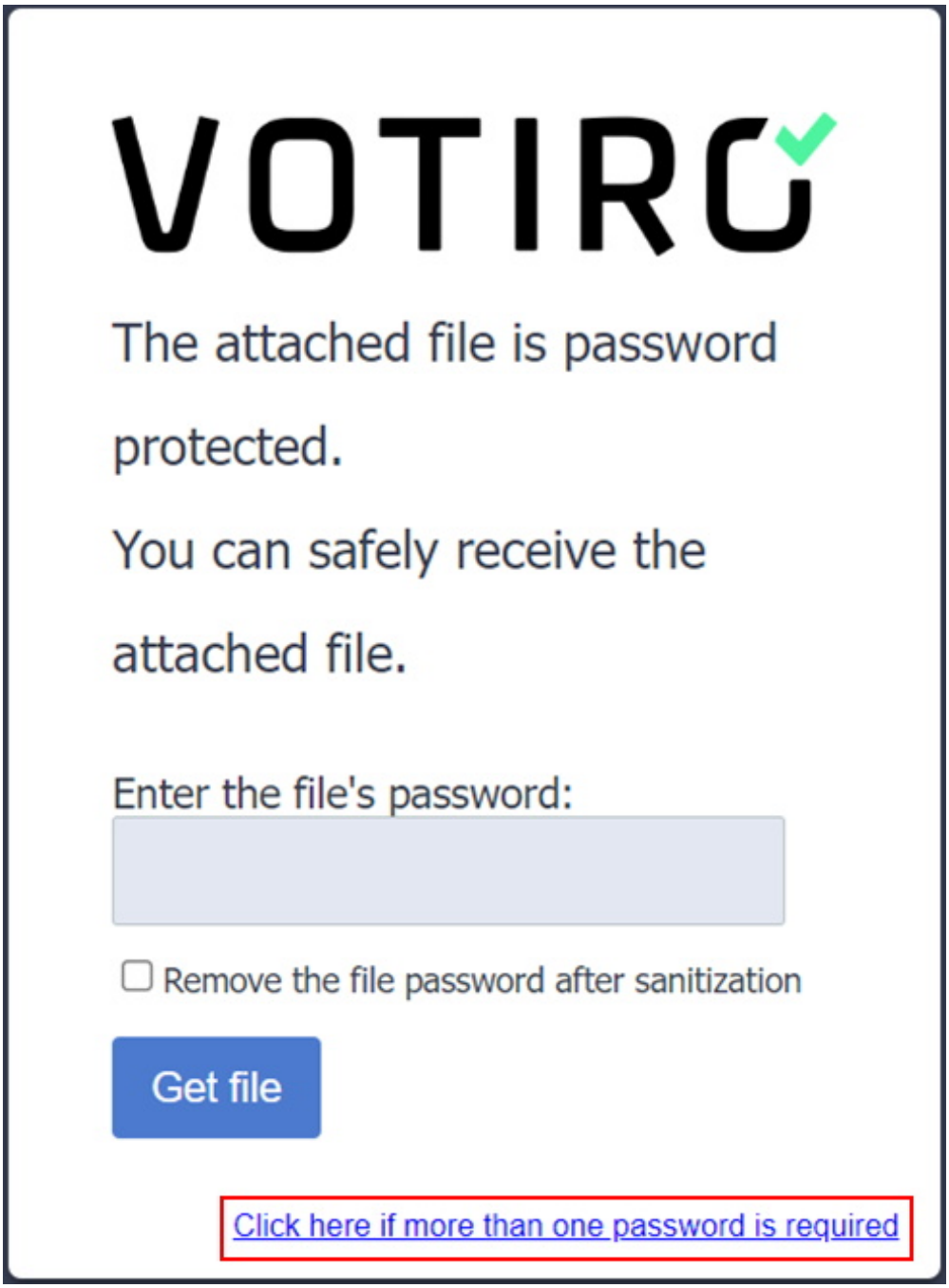
If you check the box, then:

- If the file origin is email, the new email will be sent to all recipients where the sanitized file will not require any password.
- If the file origin is API, the user will download the sanitized file, which will not be password protected.

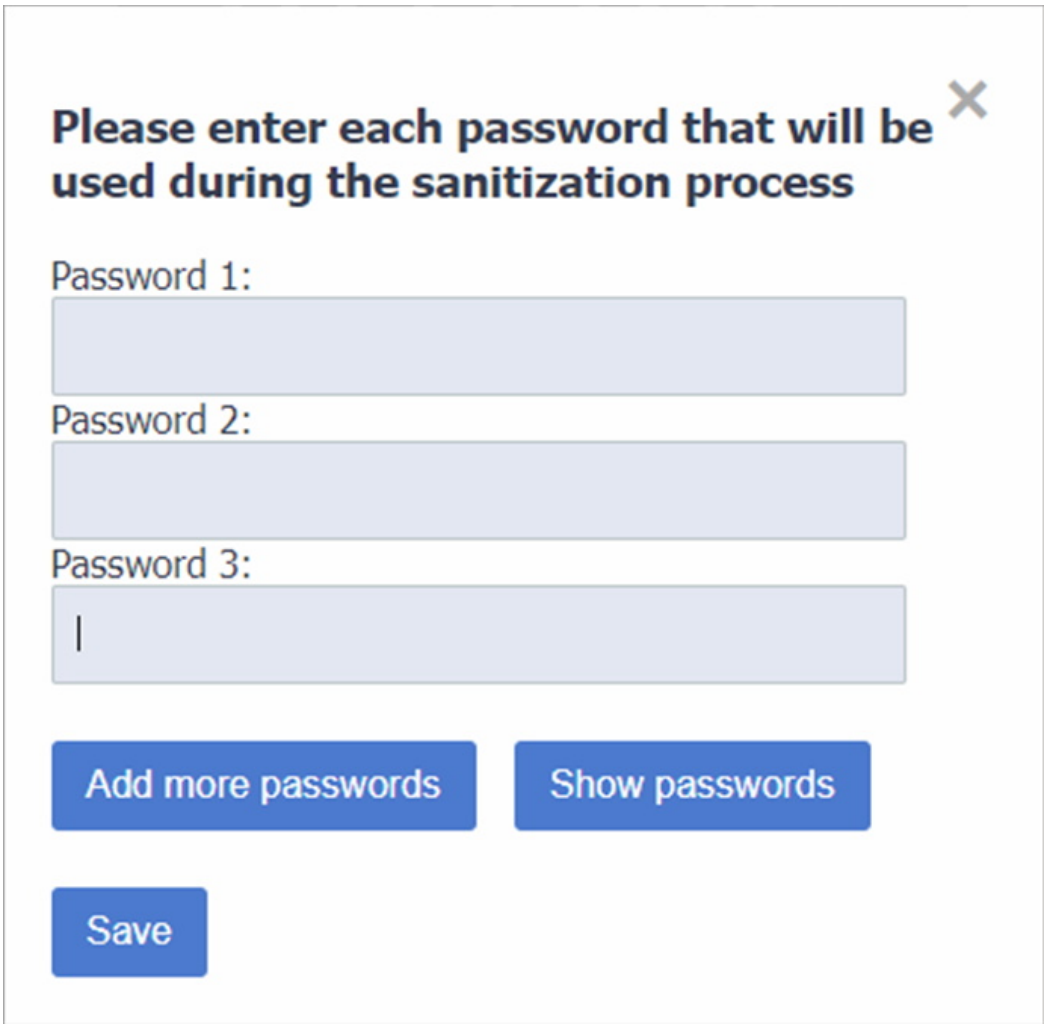
2.20.2 Support of Multiple Passwords within PPF Sanitization

If a file, such as an archive, contains multiple files within it, and the multiple files are each password protected:

1. **Enter the files's password** in the box.
2. If there are multiple passwords, click on the link: **Click here if more than one password is required**:



3. The following pop-up window will be displayed:



4. Enter the passwords using the available text boxes. To enter more than three passwords, press **Add more passwords** (You may enter up to 10 passwords).

> **Note**: To bolster security, the portal will automatically lock for 10 minutes after three consecutive failed password attempts, preventing brute-force attacks.

5. After entering all the passwords, press **Save**.

6. When the user clicks on **Get file** or **Release file by mail**, the system will sanitize all files with the provided passwords (depending on the **Remove the file password after sanitization** checkbox selection for the parent and all other PPF children).