VOTIRO

Votiro Cloud - SaaS

User Guide

October 2025

Copyright Notice

www.votiro.com

Contents

1 Introduction

1.1 Votiro Technology

Votiro secures your organization by positively selecting safe elements of each file and email delivered to your network.

Votiro is unlike traditional detection-based file security solutions that scan for suspicious elements and block some malicious files from entering your organization. Instead, threats to your network from unknown and malicious elements of a file are simply not included in the file delivered by Votiro. This results in every file entering your organization's network being 100% safe.

Votiro protects your organization from all sources of file exploit attempts that are processed through various channels such as email, web uploads, web downloads, or any supported custom application.

Votiro is enterprise-oriented, fast to deploy, easy to integrate, and seamless. It also eliminates the reliance on users' assessment of the safety of incoming emails or files.

Votiro implements a multi-layer security mechanism that integrates several critical components to eliminate cyber threats that attempt to penetrate an organization.

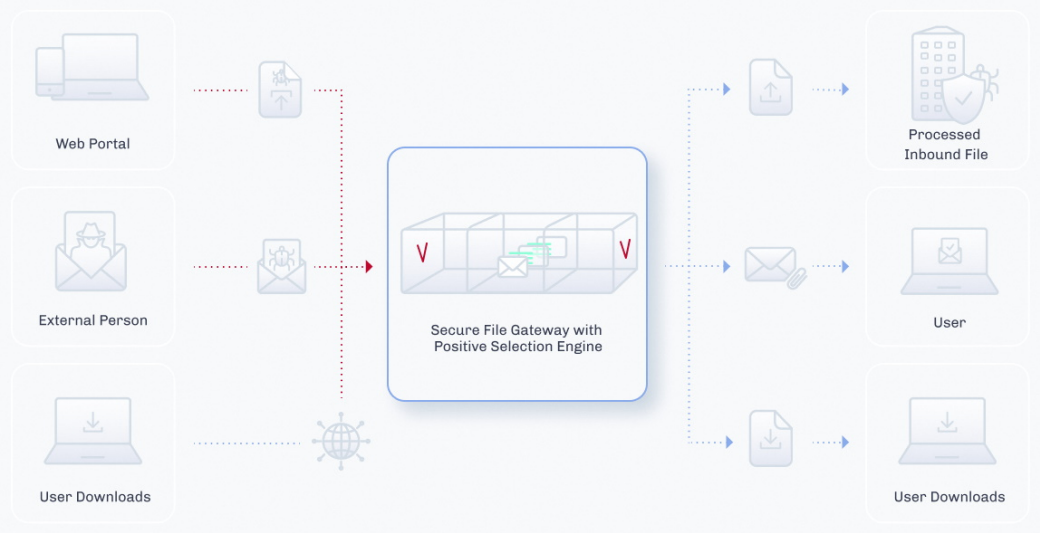
True Type Detection

True Type Detection (TTD) determines a file’s type by comparing the extension associated with the file with the specifications dictated by the vendor for that file type. For example, Microsoft Corporation has specified that a file with the extension .docx is a Microsoft Word document. In order for Word to open the file correctly, the file attributes must meet specific criteria designated by Microsoft. TTD verifies the criteria set by Microsoft are met before the file is processed.

When TTD is used in the Votiro solution and specified by the applied policy, files with content that does not match the file extension criteria are considered as "suspicious fake files".

1.2 System Architecture and Data Flow in Votiro

A general view of the Votiro product in relation to other key elements in the network is provided in the following diagram:



Data flows between Positive Selection® Engine, Votiro API Integration, Votiro On-prem for Email and Votiro On-prem for File Transfer. Communication consists of multiple bi-directional messages that include queuing, tracking, file transfers and reports.

Votiro's Positive Selection® Engine is at the heart of the Votiro solution. The Positive Selection® Engine is provided with a front-end Management Dashboard that is used for the following:

- Monitoring and analyzing positive selection activity in the Positive Selection® Engine.
- Creating and editing positive selection policies that are regularly updated in the Positive Selection® Engine.
- Storing metadata that describes the files, along with the original and processed files themselves for incident management identification.

The Votiro product image is based on Ubuntu 22.04 and hardened according to CIS Server Level 1.

1.3 Positive Selection® Engine

Votiro's Positive Selection® Engine is at the heart of the Votiro solution. The Positive Selection® Engine keeps only what belongs instead of searching for what does not belong.

Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Positive Selection singles out only the safe elements of each file, ensuring every file that enters your organization is 100% safe.

Positive Selection processing involves four steps:

- Step 1: Unknown file is received into your organization.
- Step 2: The file is dissected into content, templates and objects.
- Step 3: The file is rebuilt using content on top of a safe file template.
- Step 4: Delivery of 100% safe file into your organization.

An example of Votiro's Positive Selection® Engine processing a file is provided in the following diagram:

1.4 Supported File Types

The File Types table lists the file types and attributes supported by Votiro SaaS. The information is arranged according to the categories that appear in the **Action by File Type** area of the **Policies** page in the Votiro Management Dashboard.

- Types marked with ^ are scanned by the Positive Selection® Engine and their true file type is verified based on their structure. The files are not modified by this process. To allow files that have only detection, go to the Policies dashboard and create an exception under **Other files**. For more information, see Adding Policy Exceptions.
- Types marked with ** are obsolete. They are not recommended as filters in a production environment. Support for these types might be discontinued in a later version.

Table 1 File Types

File Type in Management	File Type	Family Type	Main Extension
PDF	PDF	Adobe PDF	pdf
	XFA	Xfa Files	pdf

File Type in Management	File Type	Family Type	Main Extension
Image	Animated GIF	Raster Image Files	gif
	BMP	Raster Image Files	bmp
	EMF	Vector Image Files	emf
	GIF	Raster Image Files	gif
	HEIF	Raster Image Files	heic, heif
	JPEG	Raster Image Files	jpeg, jpg, emf, jp2
	PNG	Raster Image Files	png, emf
	Portable Gray Map Image ** ^	Raster Image Files	pgm
	PPM ** ^	Raster Image Files	ppm
	SVG	Vector Images Files	svg
	TIF	Raster Image Files	tif, tiff
	WDP	Raster Image Files	Wdp
	WMF	Vector Image Files	wmf
	ICO	Icon Image Files	ico
	PCX	Picture Exchange Files	pcx
	WEBP	Raster Image Files	webp
Binary	Binary ^	Any Binary Files	dat, db
	Executable ^	Any Binary Files	exe, com, dll, pif, sfx, msu, msp, msi, mo

File Type in Management	File Type	Family Type	Main Extension
Archive	Bzip2 ^	Single compressed file	bz2
	7Z	Archives	7z
	CAB ^	Archives	cab, wsp
	GZ	Archives	gz
	GZIP	Archives	gzip
	InstallShield CAB ^	Archives	cab
	JAR ^	Java ARchive Files	jar, jarxx
	LZH ^	Archives	lzh
	RAR	Archives	rar, rar5
	Tar	Archives	tar
	VMware Virtual Machine Disk ^	Archives	vmdk
	Xz ^	Single compressed file	xz
	ZIP	Archives	zip
RTF	RTF	RTF Files	rtf
Email	Calendar	Calendar Files	ics
	DAT ** ^	EML Files	dat
	EML	EML Files	eml, tmp
	Encrypted EML ^	EML Files	eml, tmp, p7s, p7m
	HTML Body	HTML Files	html, htm
	HTML Attachments	HTML Files	html, htm
	MSG	MSG Files	msg
	PST ^	PST Files	pst
	PST ANSI ^	PST Files	pst
	RPMSG ^	Restricted Permission Message Fles	rpmsg
	TNEF Calendar **	EML Files	eml
	TNEF **	EML Files	eml
	VCF	Virtual Contact Files	vcf

File Type in Management	File Type	Family Type	Main Extension
Microsoft Office	Excel	Microsoft Office	xls, xlt, xml

File Type in Management	File Type	Family Type	Main Extension
	Excel5, Excel95 ^	Office Files	xls

File Type in Management	File Type	Family Type	Main Extension
	Excel2, Excel3, Excel4, Excel5 ^	Office Files	xls
	Excel (2007-2010)	Microsoft Office	xlsx
	Excel95	Office	xls
	Excel Binary	Microsoft Office Binary Files	xlsb
	Excel on xml format ^	Malformed Microsoft Office	xls
	Excel Template	Microsoft Office	xltx, xltm
	Excel with Macros	Microsoft Office with Macros	xlsm
	ExcelXML	Microsoft Office	xml
	Internal Office XML ^	Text Files	xml, xml.rels, rels, vml
	Macro File ^	Office Macro Files	bin
	Obsolete Office ** ^	Windows Write File	wri
	Power Point	Microsoft Office	ppt, pps, ppsx, xml, pot
	PowerPoint95 ^	Unsupported Files	ppt
	PreWord97 ^	Unsupported Files	doc
	Power Point (2007-2010)	Microsoft Office	pptx
	Power Point Slide (2007-2010)	Microsoft Office	sldx
	Power Point Slide with Macros (2007-2010)	Microsoft Office with Macros	sldm
	Power Point Template	Microsoft Office	potx
	Power Point Template with Macros	Microsoft Office with Macros	potm
	Power Point with Macros	Microsoft Office with Macros	pptm
	PowerPointXML ^	Microsoft Office	xml
	Printer Settings	Microsoft Office Embedded Files	bin
	Project ^	Microsoft Office	mpp
	Unknown Ole Object	OLE Object	bin
	Visio	Microsoft Office	vsd
	Visio (2007-2010)	Microsoft Office	vsdx
	Visio with Macros	Microsoft Office with Macros	vsdm
	Word	Microsoft Office	doc
	Word (2007-2010)	Microsoft Office	docx

File Type in Management	File Type	Family Type	Main Extension
	Word Pre-2007 Template	Microsoft Office	dot
	Word Template	Microsoft Office	dotx
	Word Template with Macros	Microsoft Office	dotm
	Word with Macros	Microsoft Office with Macros	docm
	WordXML	Microsoft Office	xml
Text	INI ^	Configuration Files	ini
	Text ^	Text Files	txt
	PostScript ^	PostScript Files	ps
	XML	Text Files	xml
	JSON	JavaScript Object Notation Files	json
	CSV	Comma-Separated Values Files	csv
	HTML ^	HTML Files	html, htm
Apple iWork	PAGES ^	Apple text document	pages
	PAGES.ZIP ^	Apple text zip document	pages.zip
	NUMBERS ^	Apple spreadsheet file	numbers
	NUMBERS.ZIP ^	Apple spreadsheet zip file	numbers.zip
	KEY ^	Apple Keynote file	key
	KEY.ZIP ^	Apple Keynote zip file	key.zip
Ole	Bmp Ole Object	OLE Object	bin
	Docm Ole Object	OLE Object	bin
	Docx Ole Object	OLE Object	bin
	Dotx Ole Object	OLE Object	bin
	Pdf Ole Object	OLE Object	bin
	Pptm Ole Object	OLE Object	bin
	Pptx Ole Object	OLE Object	bin
	Slide Ole Object	OLE Object	bin
	SlideM Ole Object	OLE Object	bin
	SlideX Ole Object	OLE Object	bin
	Xls Ole Object	OLE Object	xls
	Xlsx Ole Object	OLE Object	bin
	Equation Ole Object ^	OLE Object	bin

File Type in Management	File Type	Family Type	Main Extension
Media	AVI	Audio Video Interleave	avi
	DAT	Generic media	dat
	MPEG	MPEG video	mpeg, mpg
	WAV	Waveform Audio File Format	wav
	WMV	Windows Media Video	wmv
	MP2 ^	MPEG-1 Audio Layer-2 File	mp2
	MP3	MPEG-1 Audio Layer-3	mp3
	MP4	MPEG-4 multimedia	mp4
	M4A	MPEG-4 audio	m4a
	MOV	Apple QuickTime Movie	mov
	3GP	3GPP multimedia	3gp
	M4V	Apple MPEG-4	m4v
	MKV	Matroska Video	mkv
	MTS ^	MPEG Transport Stream file	mts
	WMA	Windows Media Audio	wma
	MXF	Material Exchange Format File	mxf
	CD Audio Track Shortcut ** ^	CD Audio track pointer Files	cda
	FLV ^	Flash Video Files	flv
	VOB ^	Video Object file	vob
Open Office	ODS	Calc Spreadsheet File	ods
	ODT	OpenOffice Document file	odt
Hancom Office	HWP	Hancom Document file	hwp
	HWPX	Hancom Document open format file	hwpx
	SHOW	Hancom presentation file	show
	CELL	Hancom spreadsheet file	cell
Certificate	CRT ^	Security Certificate File	crt
	CRL ^	Certificate Revocation List	crl
	CER ^	Third-party Certificate Authority File	cer

File Type in Management	File Type	Family Type	Main Extension
CAD	DWF ^	AutoDesk Design Web Format File	dwf
	DWG	AutoCAD Drawing File	dwg
	DWS	AutoCAD Drawing Verification File	dws
	DWT	AutoCAD Drawing Template File	dwt
	DXF	AutoCAD Drawing Exchange Format File	dxf
	JWW	Java Web-Workflows Data file	jww
	P21	Express STEP Data Model Files	p21
	SFC	Scadec Feature Comment file	sfc
	ACIS Solid Model ^	CAD Files	sat
	CATIA Product Data ^	CAD Files	stp, step
	eDrawings ^	CAD Files	easm
	Initial Graphics Specification ^	CAD Files	igs
	Parasolid model ** ^	CAD Files	x_t, x_b
	Pcx ^	CAD Files	pcx
	PreR14Dwg ^	CAD Files	dwg
	SolidWorks ^	CAD Files	sldasm, sldprt
	ZSoft PCX Bitmap ^	CAD Files	brd
Ichitaro	JTD	Ichitaro Document file	jtd
	JTDC	Ichitaro Compressed Document file	jtdc
DocuWorks	XDW ^	DocuWorks Image file	xdw

File Type in Management	File Type	Family Type	Main Extension
Other	Adobe Air ** ^	Adobe	air
	CSS ^	Cascading Style Sheet Files	css
	Data ^	Model Item Data Files	data
	DB ^	Database Files	dbf, npa, dbt, wnd, tab, mdb
	Dicom ^	Dicom Files	dcm
	Embedded Macro ^	Embedded File	bin
	Empty ^	Empty File (None)	
	INF ^	INF Files	inf
	LabView ** ^	LabView	vi
	Mac AppleSingle encoded ^	Mac OS Files	"._" prefix
	Mac AppleDouble encoded ^	Mac OS Files	"._" prefix
	Mac OS X folder information ^	Mac OS Files	ds_store
	Mac OS X crash log ^	Mac OS Files	crash
	MHT ^	MHT Files	mht
	MST ** ^	Installer Setup File	mst
	p7s ^	Digital Signatures	p7s
	Pgp File ^	Encrypted Files	pgp
	PSD ^	Photoshop Files	psd
	RPT ** ^	RPT Files	rpt
	RSP ** ^	PLC Files	rsp
	Script ^	Batch Files	bat, js, php, cmd, vbs, reg, pl, lnk, py, asp, ps1
	Shortcut ^	Shortcut Files	url
	Solution User Option ** ^	Visual Studio Files	suo
	SQL ^	SQL Files	sql
	Tableau ^	Tableau Files	twb, tbm, twbx, hyper, tds, tdsx
	Unrecognized ^	Any Binary Files	

Anomalies and Limitations

Processing files for positive selection so you only receive secure content occasionally results in some known anomalies and limitations. These include:

- Unknown Ole Objects: both generic and unknown Ole objects are handled.
- Generic Ole objects will be processed, and unknown Ole objects will be blocked.
- File names with more than 101 non-English characters may not be included.
- As you can see, the file size limitations are currently significant sizes:
  - Archives - 2 GB
  - CSV - 2 GB
  - Raster images - 100 MB
  - Text - 100 MB
  - PDF - 700 MB
  - EML - 64 MB
  - ICS - 5 MB
  - Office - 50 MB
  - ExcelX - 1 GB
  - PowerPointX - 1 GB
  - WordX - 750 MB
  - Visio - 1 GB
  - Vector images - 10 MB
  - Media - 10 GB
  - XML and JSON - 100 MB
- AV scans are supported for file sizes up to 40 GB.

2 Using the Management Dashboard

The Management Dashboard enables you to perform the following procedures:

- Monitoring Positive Selection Activity
- Exploring Incidents
- Configuring Settings
- Cloud Connectors and Integrations
- Password Protected Portal
- Generating Reports

> **Note**
> Votiro Management Dashboard is supported using the Chrome browser only.

2.1 Logging in to the Management Dashboard: SaaS

There are two ways the customer can sign in:

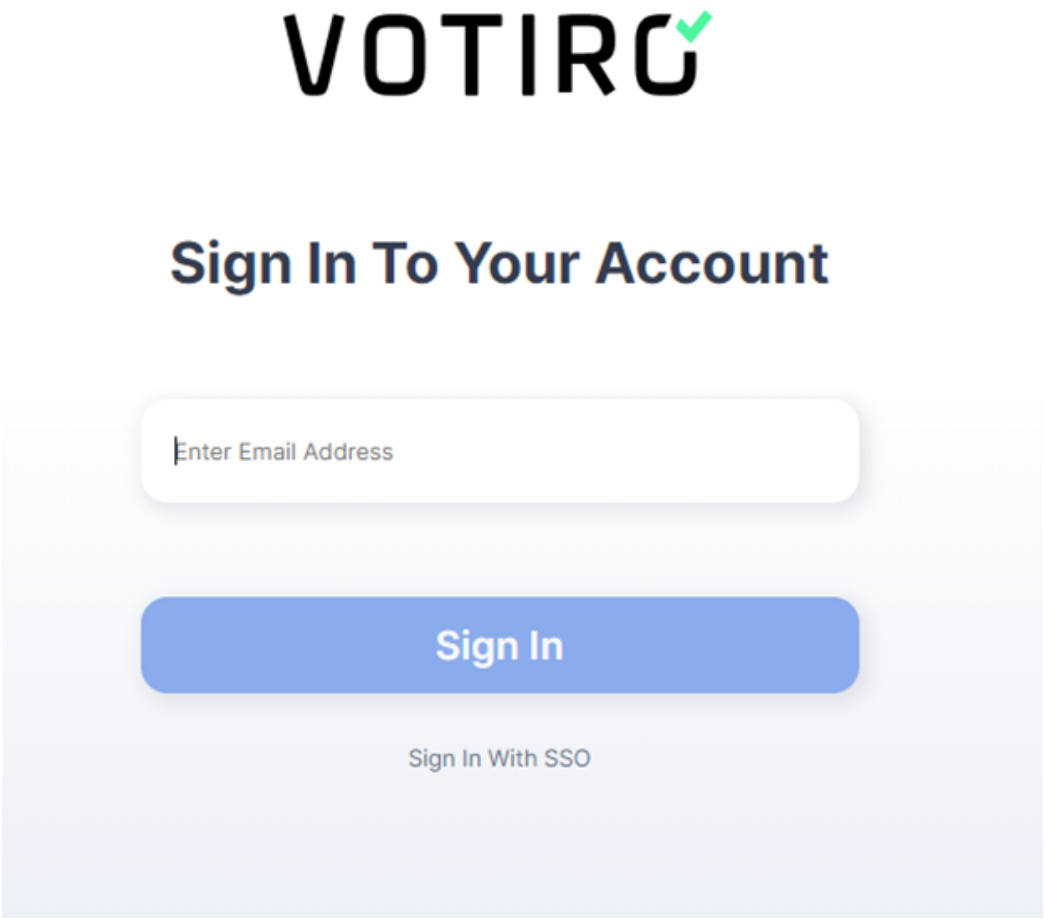
- Sign in with Votiro credentials - relevant for a customer that has setup local users
- Sign in with SSO (using corporate credentials) - relevant for a customer that has integrated Votiro through SAML

2.1.1 EULA Initial Tenant Setup

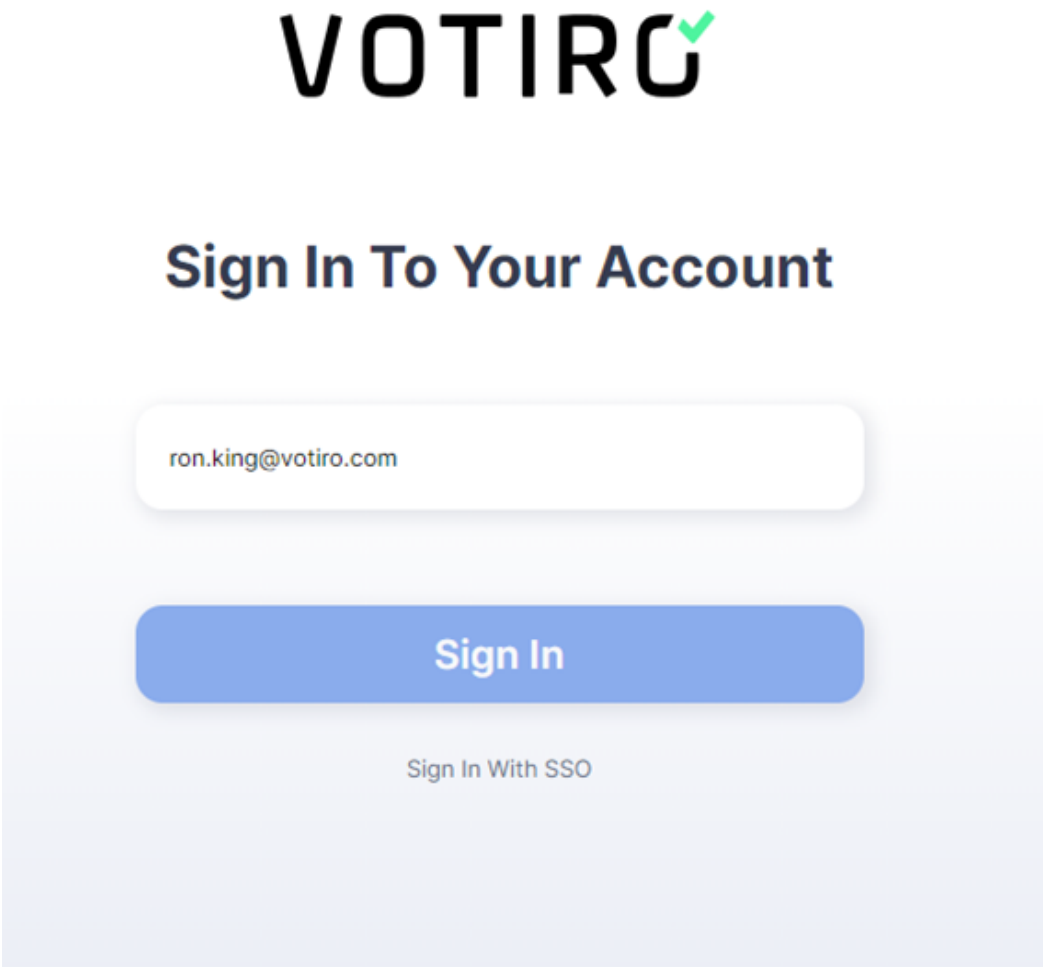
A new tenant's admin user must agree to the Menlo End User License Agreement (EULA) upon their first login before they can use the product.

2.1.2 Sign In with Votiro credentials

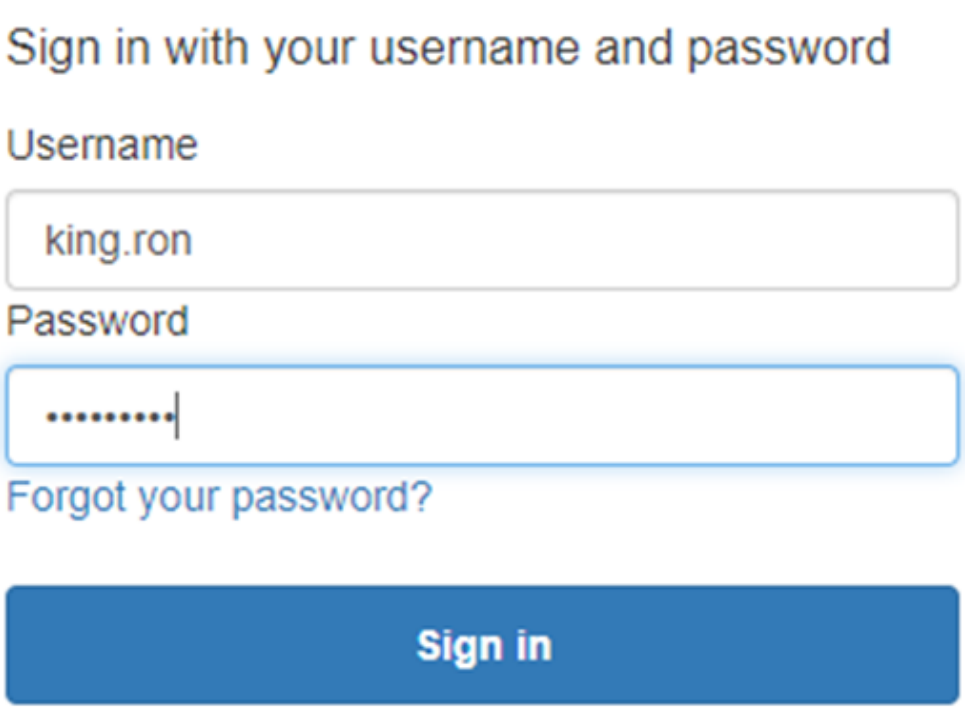
1. Sign in with Votiro credentials. Enter the local user email address to sign in to the Votiro Management console.



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



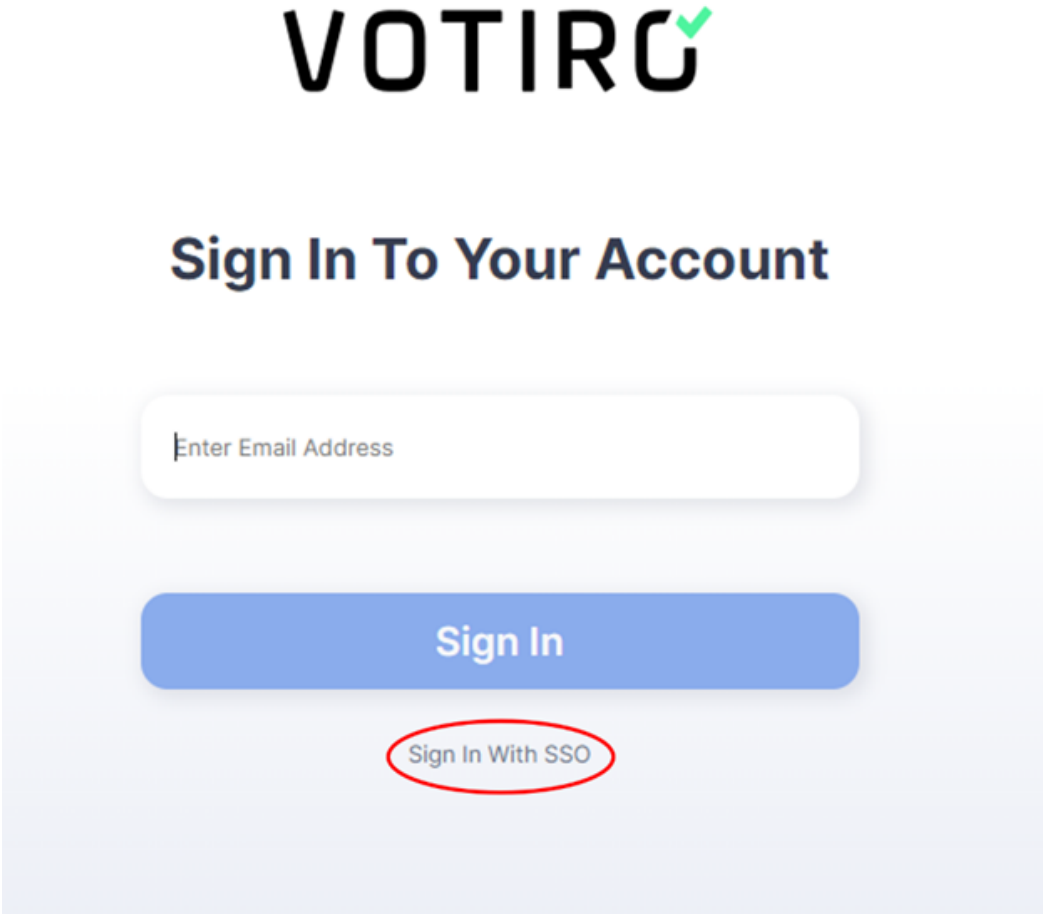
3. Press **Sign In**. An authentication window opens:



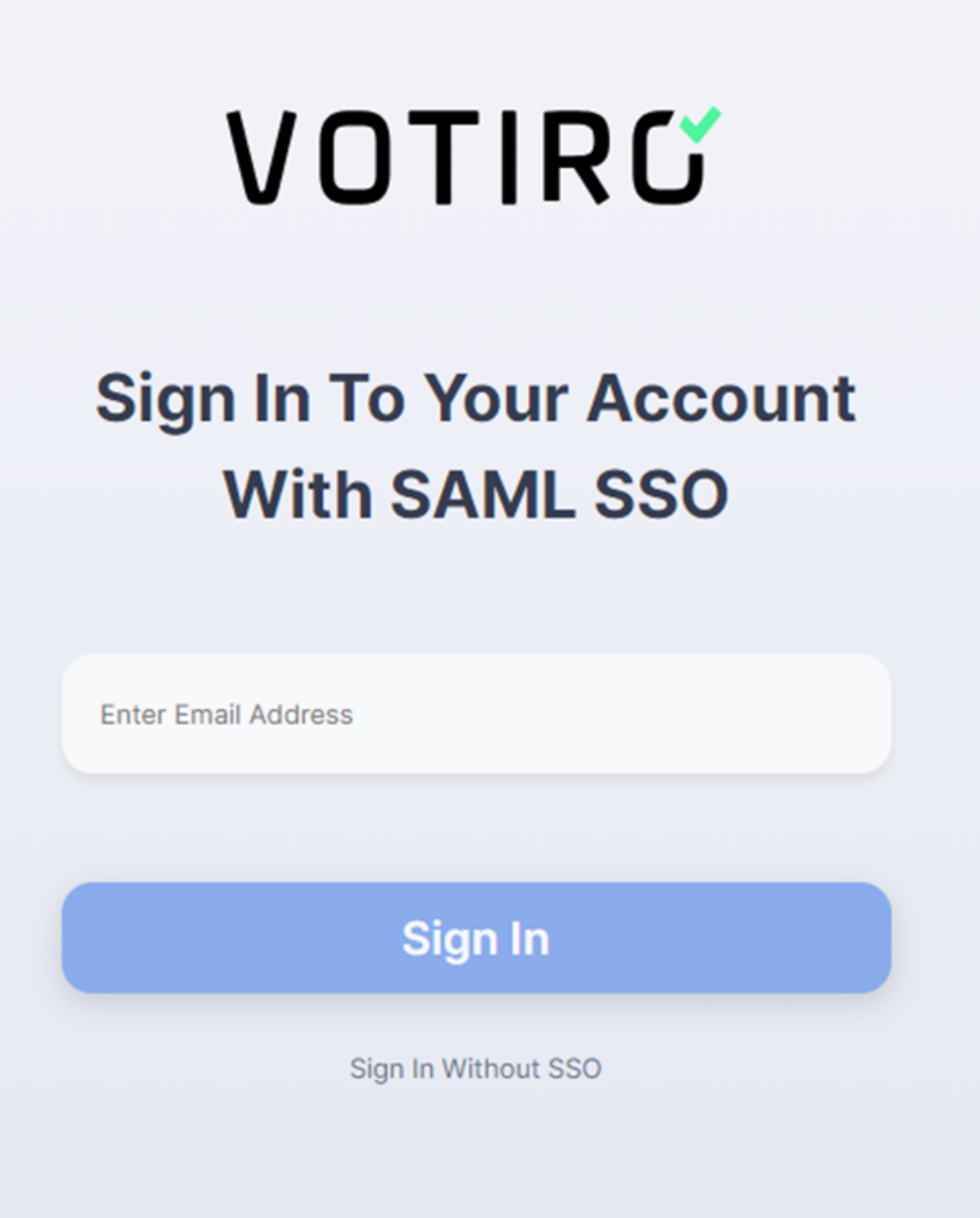
4. Enter the login credentials and press **Sign In**. The Management console is displayed.

2.1.3 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.

2.2 Monitoring Positive Selection Activity

The Monitoring Positive Selection Activity page allows monitoring and analyzing of traffic throughput as files are processed for known elements. Any unknown elements within a file

are identified and do not transfer to the newly constructed template received by the user.

A file is processed for positive selection according to policies for the particular file type. Threats, determined by unknown elements, are detected regardless of policies, whether the file is blocked or not.

There can be more than one recent activity message for a single file if it contains more than one threat. For example, the file can contain a suspicious URL and a suspicious macro.

From the navigation pane on the left, click **Monitor**. See the description of the **Monitor** dashboard at Monitor Dashboard.

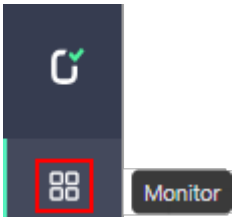
2.3 Monitor Dashboard

The **Monitor** dashboard allows monitoring and analyzing of traffic throughput as files are processed for known elements. Any unknown elements within a file are identified and do not transfer to the newly constructed template received by the user.

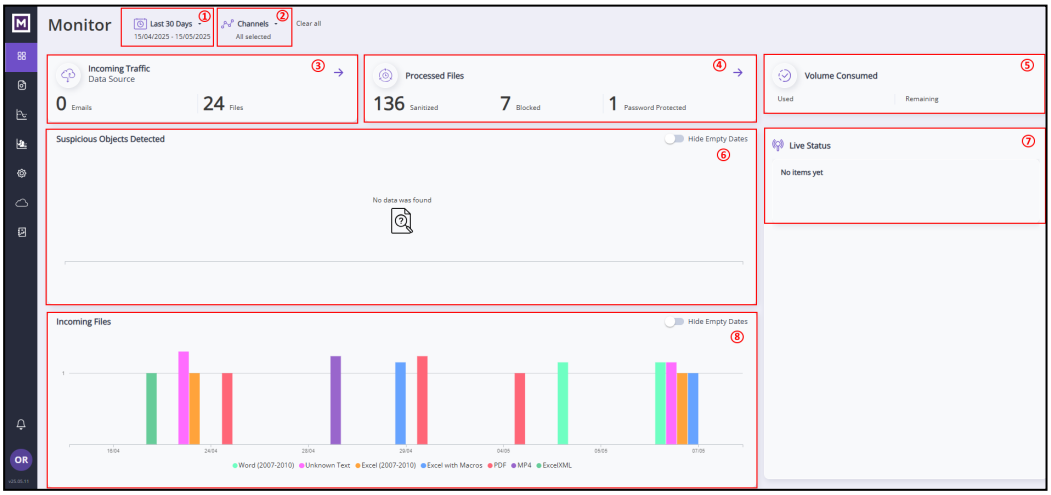
A file is processed for positive selection according to policies for the particular file type. Threats, determined by unknown elements, are detected regardless of policies, whether the file is blocked or not.

There can be more than one recent activity message for a single file if it contains more than one threat. For example, the file can contain a suspicious URL and a suspicious macro.

From the navigation pane on the left, click the **Monitor** icon in the navigation pane on the left:



The **Monitor** dashboard is displayed:



The page contains the following panes, outlined in red and numbered as in the above screenshot:

- **1** Time interval - filters the display by the selected time period. See Filter by Time Period.
- **2** Channels - filters the display by the selected channels. See Filter by Channels.
- **3** Incoming Traffic - displays the number of Emails and files received during the selected time period and for the selected channels. See Incoming Traffic.
- **4** Processed Files - displays the number of sanitized, blocked and password protected files received during the selected time period and for the selected channels. See Processed Files.
- **5** Volume Consumed - displays the volume of the files processed and the volume remaining (in appropriate units: Bytes, KB, MB, GB, TB)
- **6** Suspicious Objects Detected - displays a histogram chart of suspicious objects detected during the selected time period. See Suspicious Objects Detected.
- **7** Live Status - displays the most recent file traffic events. See Live Status.
- **8** Incoming Files - displays the incoming file traffic by file type during the selected time period and for the selected channels. See Incoming Files.

2.3.1 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.

2.3.2 Incoming Traffic

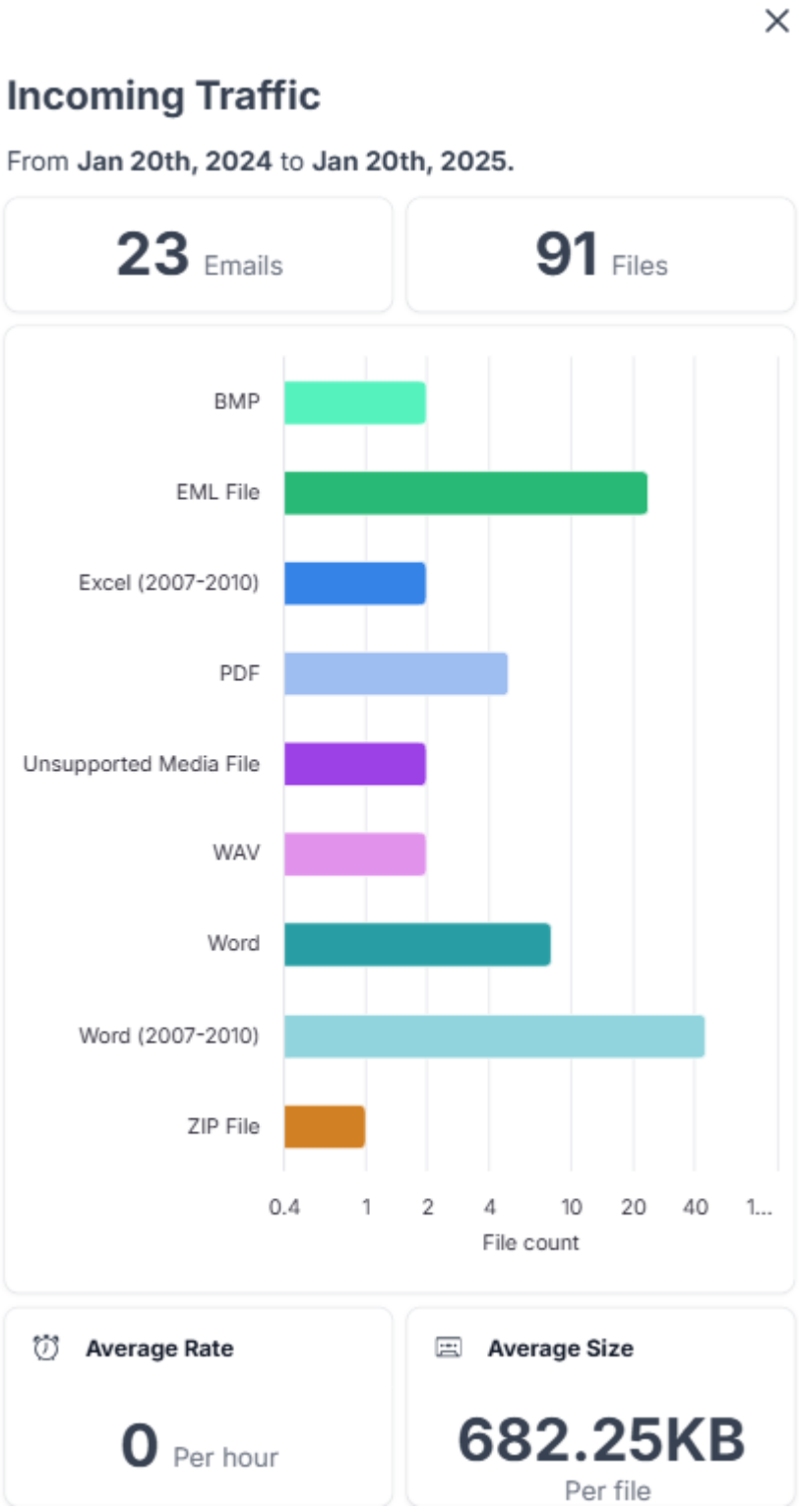
The **Incoming Traffic** pane displays the number of Emails and Files received during the selected time interval and selected channels.

The **Incoming Traffic** pane (**3**) displays the number of Emails and the number of Files received during the selected time interval and selected channels. This includes attachments to emails. For more details, see File count for an archive file or email with attachments.

Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart.

To view a breakdown of emails and file types, click on either pane. A new pane opens on the right-side of the page:

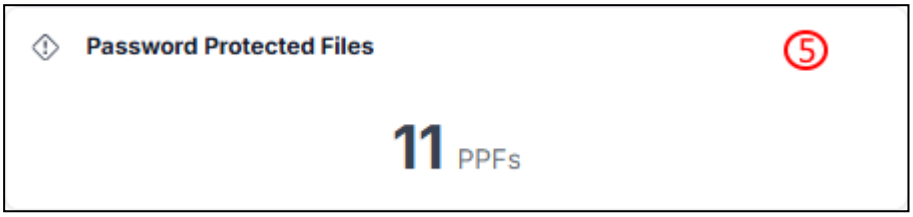


Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart. For more details, see Operational workflow.

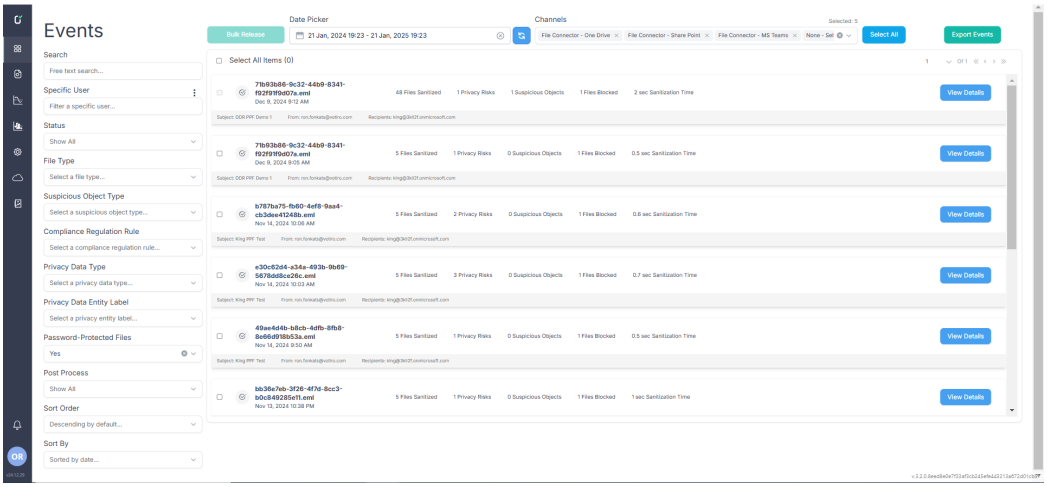
2.3.3 Password Protected Files

The **Password Protected Files** pane (5) displays the number of password protected files processed during the selected time interval and selected channels.



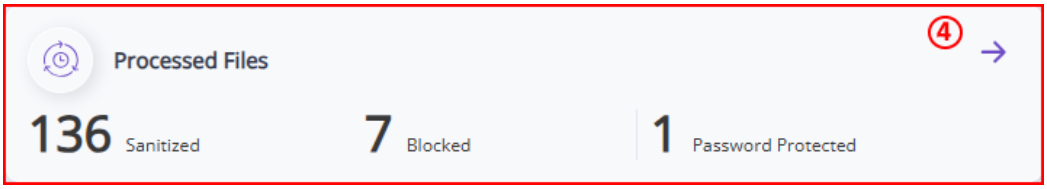
Extracting more data by drilling down

To display details of the password protected files, click on the pane. The **Events** page opens:



2.3.4 Processed Files

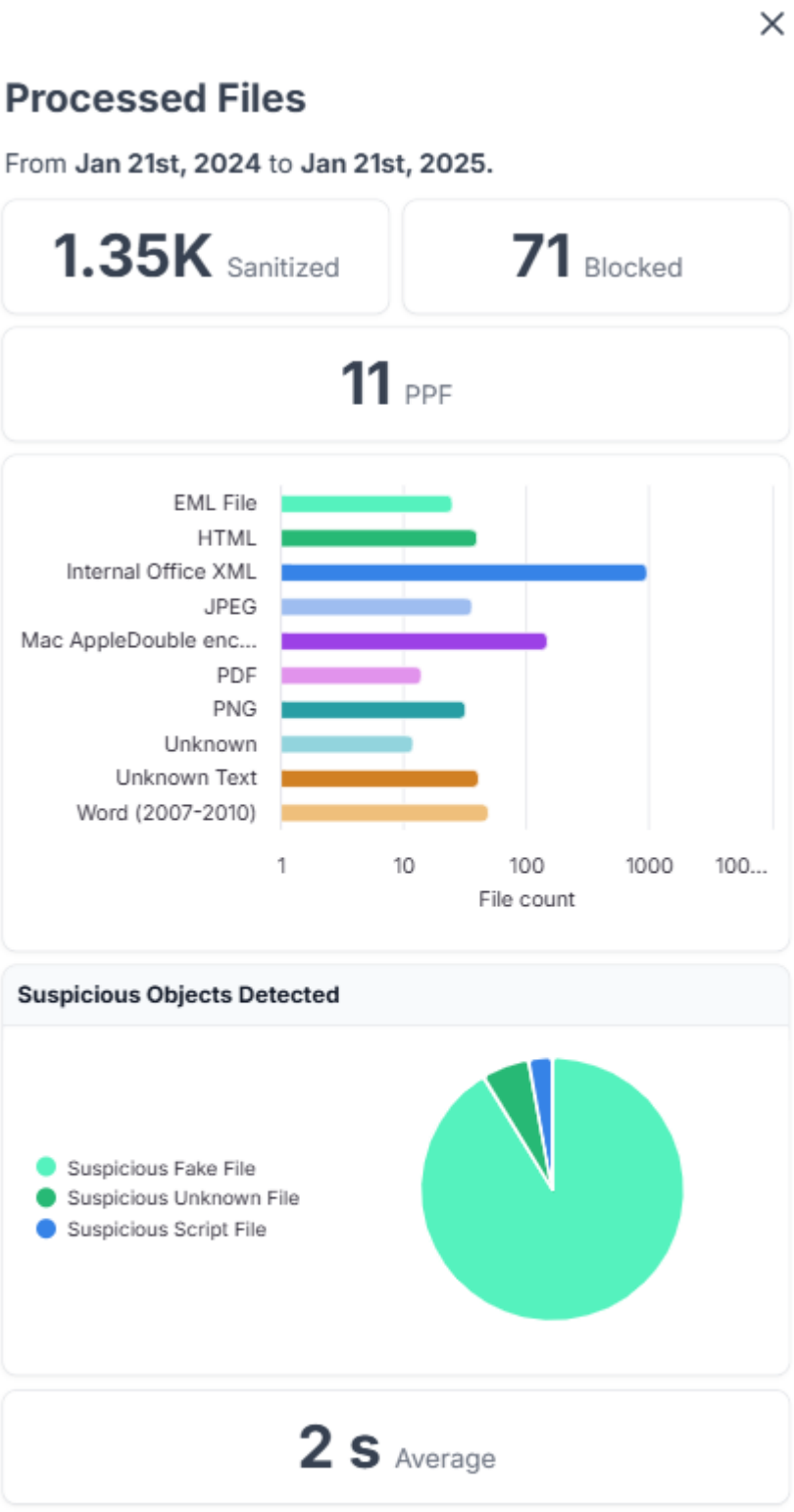
The **Processed Files** pane displays the number of Sanitized, Blocked and Password Protected Files processed during the selected time interval and selected channels.



Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart.

To view a breakdown of emails and file types, click on either pane. A new pane opens on the right-side of the page:

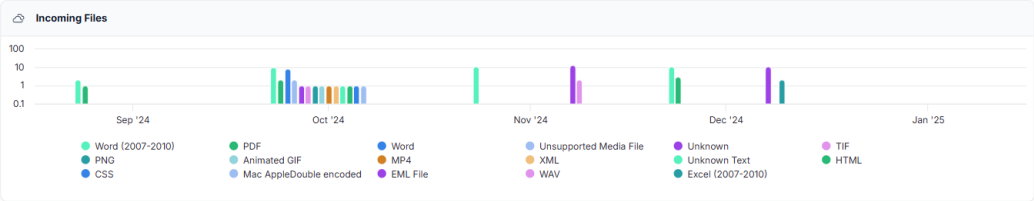

Processed Files
From Jan 21st, 2024 to Jan 21st, 2025.
1.35K Sanitized
71 Blocked
11 PPF
EML File
HTML
Internal Office XML
JPEG
Mac AppleDouble enc...
PDF
PNG
Unknown
Unknown Text
Word (2007-2010)
1
10
100
1000
100...
File count
Suspicious Objects Detected
Suspicious Fake File
Suspicious Unknown File
Suspicious Script File
2 s Average

Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart. For more details, see Operational workflow.

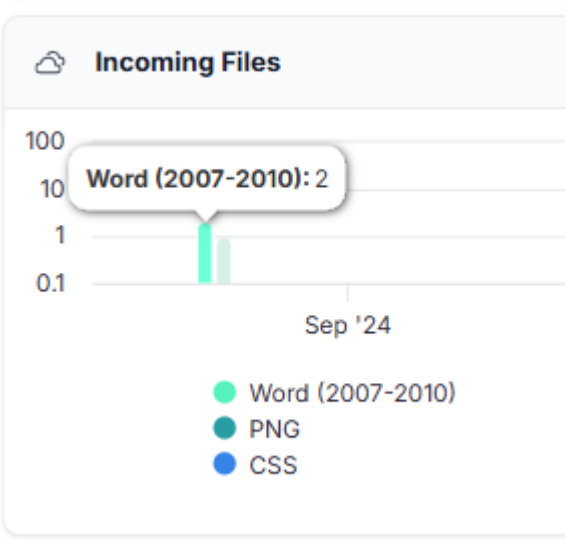
2.3.5 Incoming Files

The **Incoming Files** pane displays histograms of the file types and emails received during the selected time interval and for the selected channels.

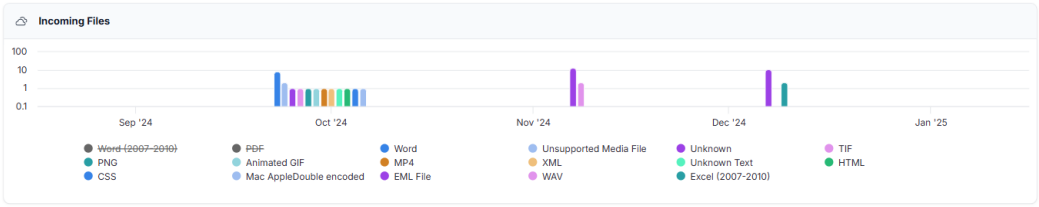


2.3.6 Filtering the Incoming Files

You may view the number of files processed for each file type in a selected time interval by moving the cursor over the desired histogram. For example, in the screenshot below, the cursor is moved over the green histogram to display **Word (2007-2010): 2** files processed during September 2024.

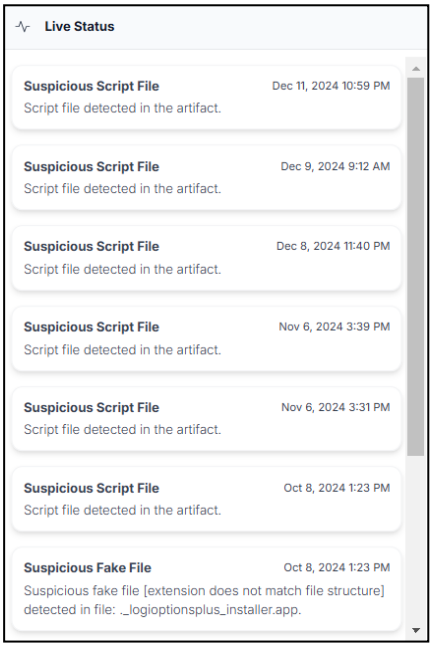


You may also remove file types from the display by clicking on the file types below the histogram. The selected file types are removed from the histogram display for the entire selected time interval. In the below example, Word (2007-2010) and PDF files were removed from the display and this is indicated by the file type names having a strike-through line.



2.3.7 Live Status

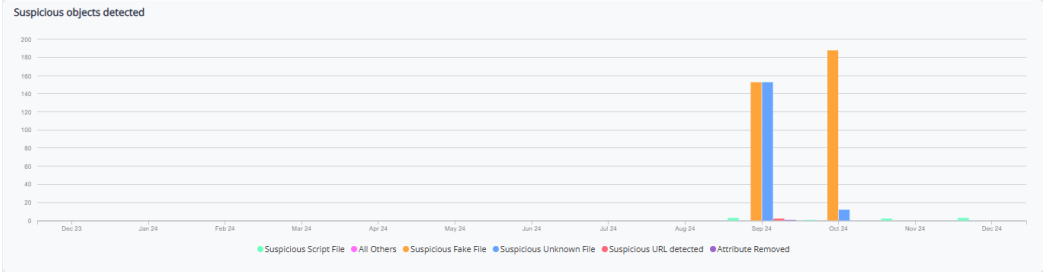
The **Live Status** pane displays the most recent file traffic events during the selected time period and for the selected channels. Any suspicious files detected along with the date and time detected and the reason the file was flagged as suspicious are displayed.



To view more information on a flagged file, click on the row of the file in the **Live Status** pane. A new pane view opens on the right-hand side of the **Monitor** dashboard page displaying more details about the file. See File Details for more information.

2.3.8 Suspicious Objects Detected

The **Suspicious Objects Detected** pane displays a histogram chart of the suspicious objects detected in the processed files for the time period selected. The files are displayed according to their object or file types, such as Suspicious Fake File, Attribute Removed, etc.



Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart. For more details, see Operational workflow.

2.3.9 Test File

To test a file, from the Management Dashboard navigate to **Settings** > **Policies** and click **Test File**. Your file manager opens for you to navigate to the file you want to test, and select it for testing. When testing has completed successfully a link is returned to the page. Click **Details** to see information about the file used for testing, including the sanitization log.

The file used for testing is stored and displayed as a regular file in Votiro. For further information, see File Details on page 42.

2.4 Events Dashboard

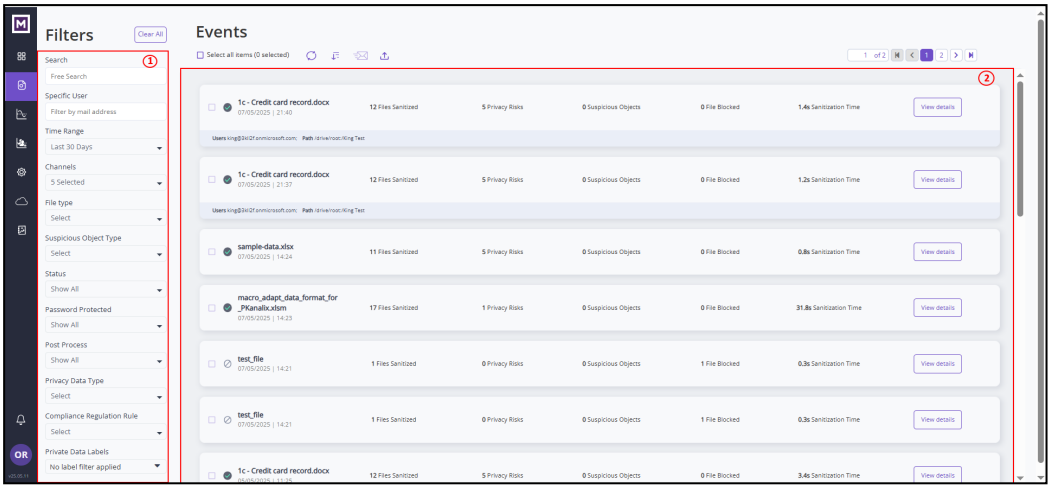
The **Events** dashboard provides you with a deeper view of files that have been processed for positive selection and are currently stored on the server. By default the full list of incidents (up to 10,000 events) that have occurred during the last seven days is displayed. You can narrow the list of incidents by using filters (see Event Filters).

From the **Events** dashboard, you can release files that have been blocked.

Use this page to explore incidents (blocked and processed files).

From the navigation pane on the left, click the **Events** icon in the navigation pane on the left:

The **Events** dashboard is displayed:



The page contains the following panes, outlined in red and numbered as in the above screenshot:

- **1** Event filters - filters the display by additional event filters. See Event Filters.
- **2** Events List - displays the files received during the selected time period and for the selected channels and event filters. See Events List.

The Events page also contains the following controls:

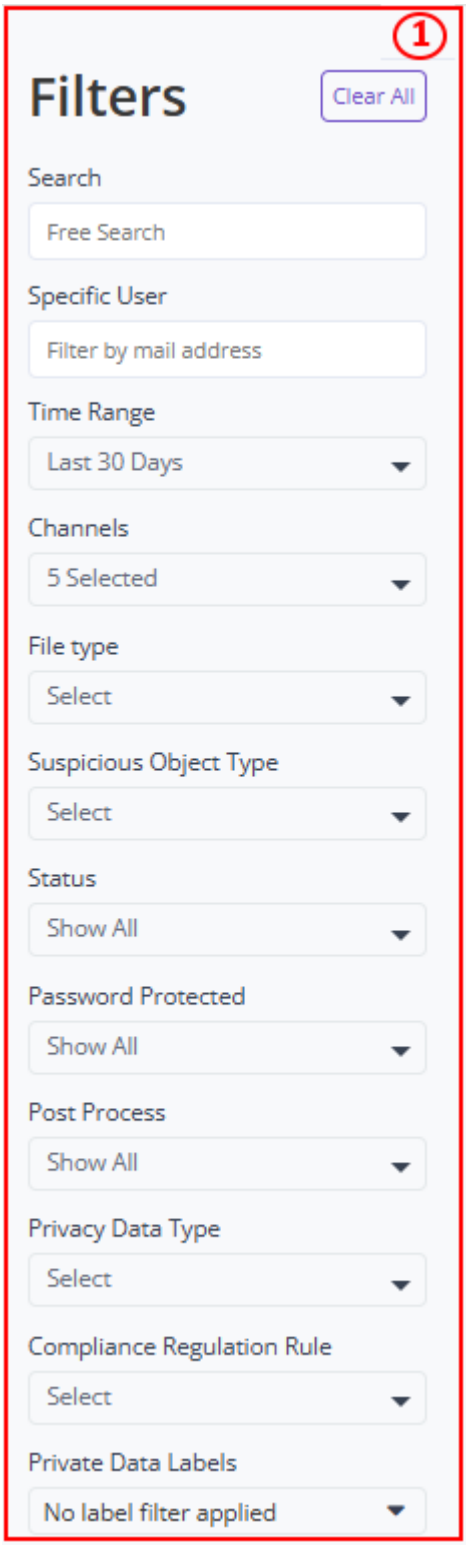
- **Bulk Release** - after selecting blocked emails from the Event Files table, clicking on this button releases all the blocked emails. See Releasing Multiple Emails for more details.
- **Export Events** - clicking on this button downloads a csv file summarizing all the Event files displayed on the page. The following data is included in the csv file:
  - Date & Time
  - Filename
  - Subject - for emails
  - From - for emails
  - Recipients - for emails
  - Blocked Files
  - Suspicious Objects
  - File Type
  - Sanitization Time (Seconds)
  - Item ID
  - Hash
  - Connector Type
  - Connector Name

- Link

- **View Details** (in the Event Files pane) - clicking on this button displays details for the file in the corresponding row. See File Details.

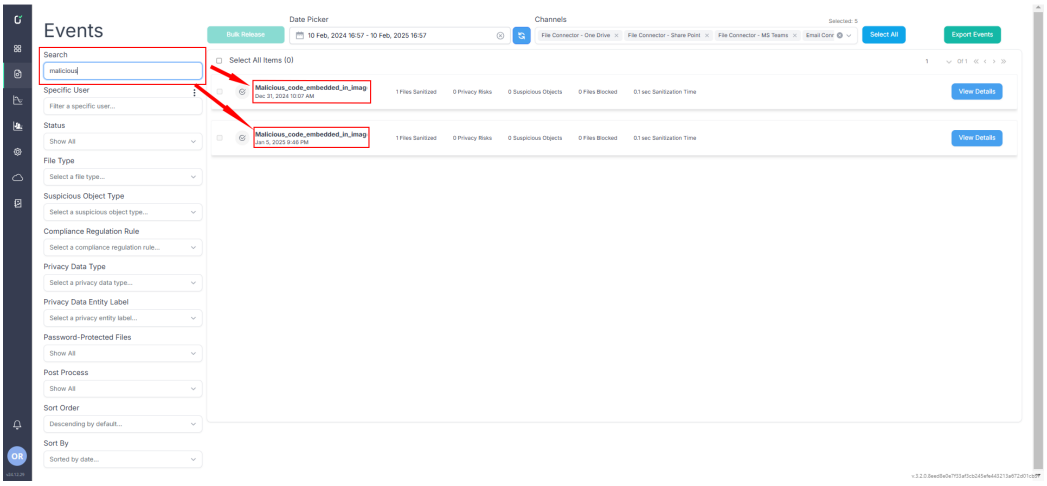
2.5 Event Filters

The Event Filters pane allows you to filter the Events files displayed.

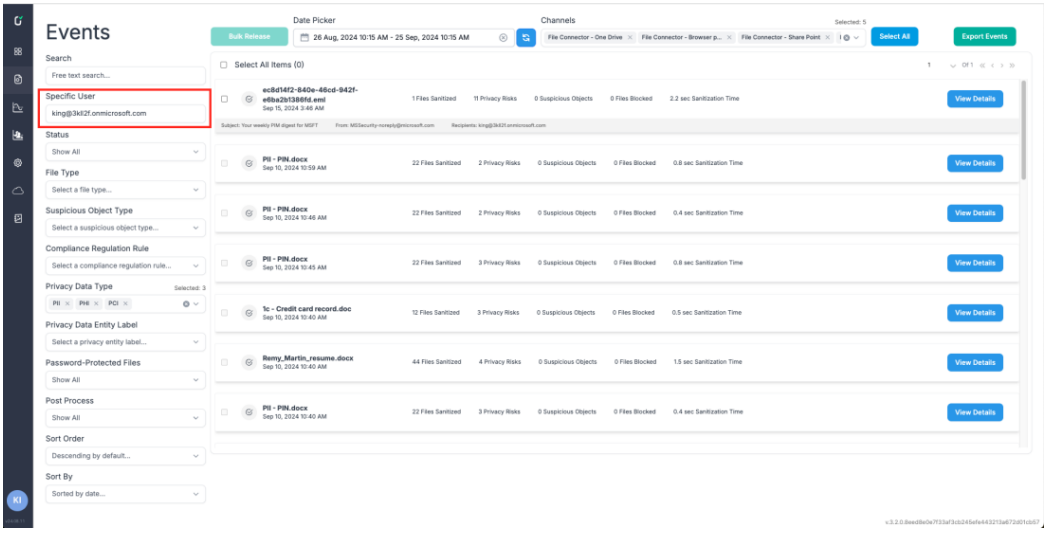


The filters available include:

- Search - free text search. The Event Files displayed will contain all file names that contain the search text. For example:



- Specific User - filter a specific user by specifying the user's full email address. The Event Files displayed will contain all file names associated with the specific user's email address. For example:



Note: This filter is available for the following connectors only:

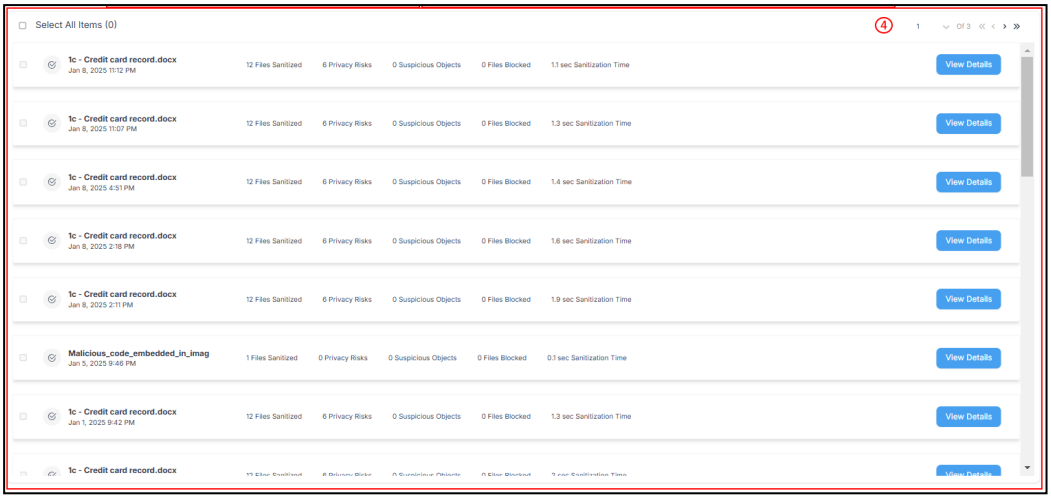
- API
- OneDrive
- Teams
- SharePoint
- O365 Email
- Browser Plugin

- Time Range - select the time range from the dropdown list.
- Channels - select the file connector from the dropdown list.

- File Type - select a file type from the dropdown list. The default is all possible file types are displayed. The options are described in File Types.
- Suspicious Object Type - select a suspicious object type to search for from the dropdown list. The options are described in Suspicious Object Types.
- Status - filters the display by the selected status. The options are:
  - Show All - display all events. This is the default.
  - Sanitized - display events with sanitized files only.
  - Blocked - display events that have at least one blocked file, including inner files.
  - Root Blocked - display events where the root file is blocked.
- Password Protected - select whether to display password-protected files. The options are:
  - Show All - display all files. This is the default.
  - Yes - display password-protected files only
  - No - do not display password-protected files
- Post Process - select
  - Show All
  - Released Incidents - blocked emails that were released
  - Retroscan Findings - incidents found using the Retrospective findings filter on the Events page
- Privacy Data Type - select a privacy data type to search for from the dropdown list. The options are described in Supported Data Types.
- Compliance Regulation Rule - select a compliance regulation rule to search for from the dropdown list. The options are described in Supported Regulations.
- Private Data Labels - select a privacy entity label to search for from the dropdown list. Private Data Labels are described in Supported Data Labels.

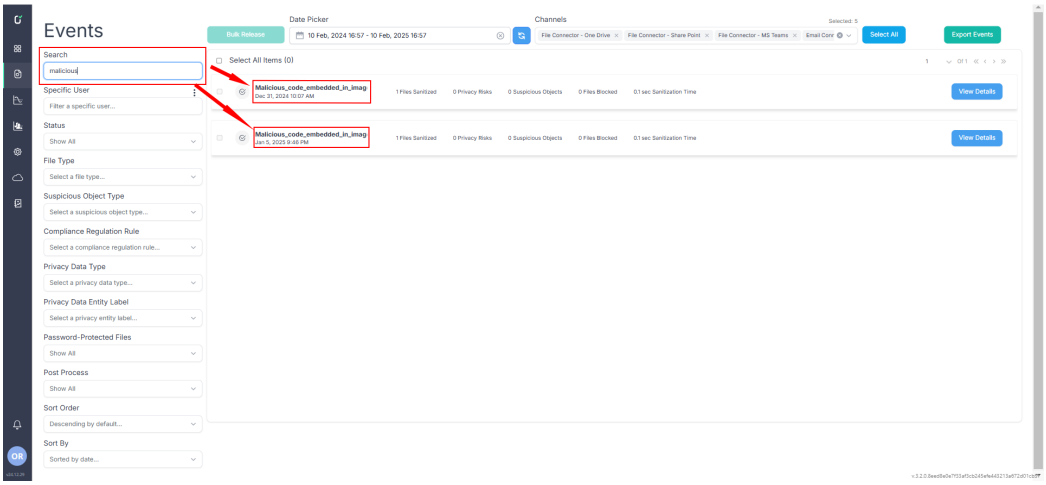
2.6 Events List

The Events List pane displays a list of files processed for the selected time period and the selected channels and selected filters.

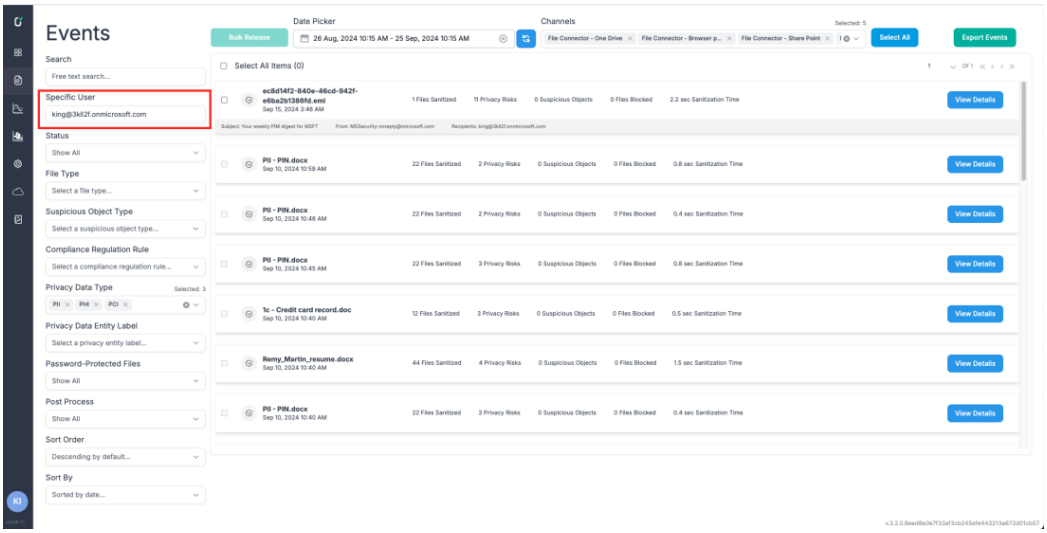


The table of files displayed includes:

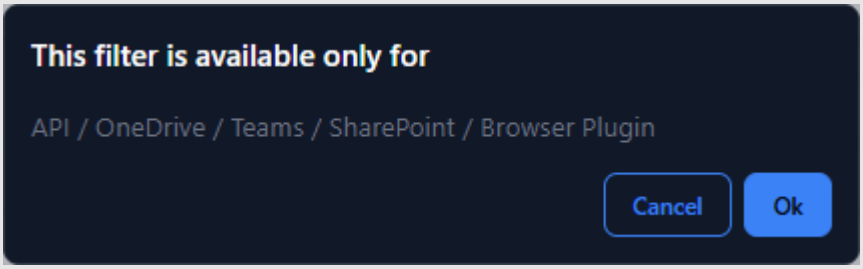
- File name
- Number of **Files Sanitized** - if the file is an archive or email, this number includes attached files
- Number of **Privacy Risks**
- Number of **Suspicious Objects**
- Number of **Files Blocked**
- **Sanitization Time** - in seconds



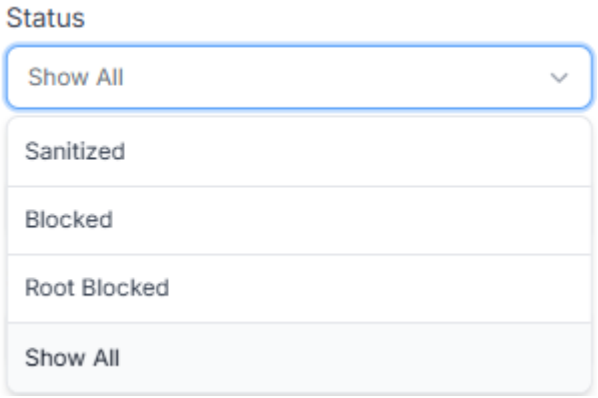
- Specific User - filter a specific user. The Event Files displayed will contain all files owned by the specific user. For example:



Note: This filter is available for the following connectors only:



- Status - filters the display by the selected status. The options are:



  The default is **Show All**.

- File Type - select a file type from the dropdown list. The default is all possible file types are displayed. The options are described in File Types.
- Suspicious Object Type - select a suspicious object type from the dropdown list. The options are described in Suspicious Object Types.

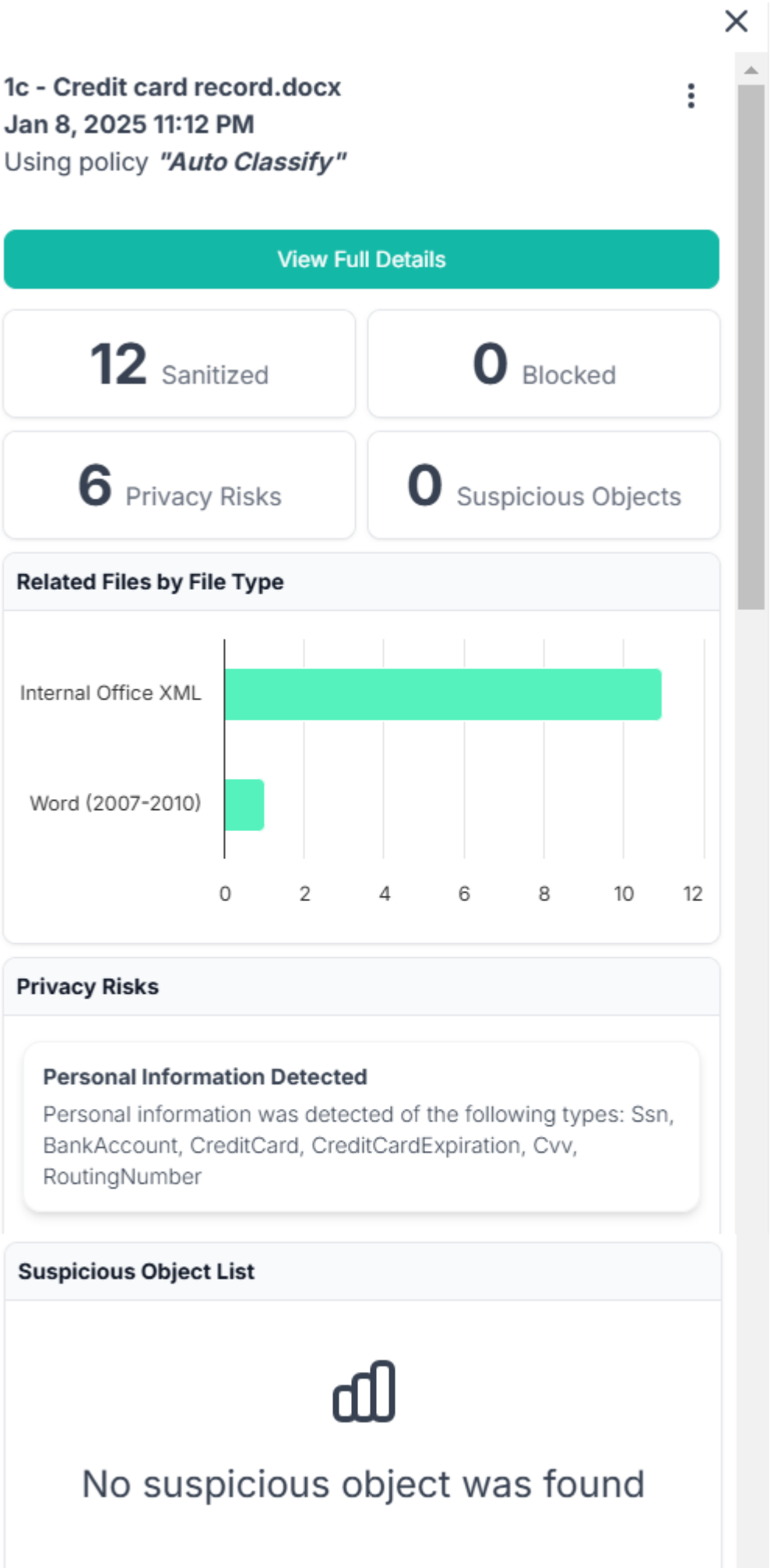
- Compliance Regulation Rule - select a compliance regulation rule from the dropdown list. The options are GDPR, CPRA, HIPAA, QuebecPrivacyAct AND APPI. These are described in Supported Regulations.
- Privacy Data Type - select a privacy data type from the dropdown list. The options are PII, PHI and PCI. These are described in Supported Data Types.
- Privacy Data Entity Label - select a privacy entity label from the dropdown list. Private Data Labels are described in Supported Data Labels.
- Password-Protected Files - select whether to display password-protected files. The options are:
  - Yes - display password-protected files only
  - No - do not display password-protected files
  - Show All - display all files. This is the default.
- Post Process - select from:
  - Released Events - blocked emails that were released
  - Retroscan Findings - incidents found using the Retrospective findings filter on the Events page
  - Show All
- Sort Order - select the sort order . The options are:
  - Ascending - display the earliest files first.
  - Descending - display the latest files first. This is the default.
- Sort By - select the sort argument. The options are:
  - Date

2.6.1 File Details

To view more details of a file listed in the Event Files table, click on the **View Details** button on the right side of the row containing the file. See File Details for more information.

2.7 File Details

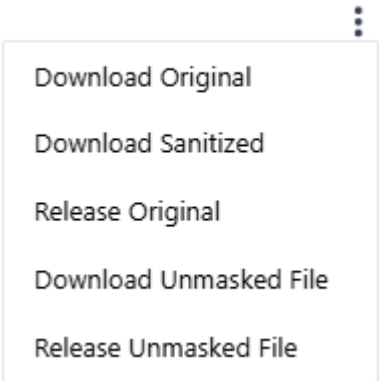
The File Details pane opens on the right side of the screen:


1c - Credit card record.docx
Jan 8, 2025 11:12 PM
Using policy "Auto Classify"
View Full Details
12 Sanitized
0 Blocked
6 Privacy Risks
0 Suspicious Objects
Related Files by File Type
Internal Office XML
Word (2007-2010)
0
2
4
6
8
10
12
Privacy Risks
Personal Information Detected
Personal information was detected of the following types: Ssn, BankAccount, CreditCard, CreditCardExpiration, Cvv, RoutingNumber
Suspicious Object List
No suspicious object was found

The file details are displayed according to the selection from the **Related Files Hierarchy**.

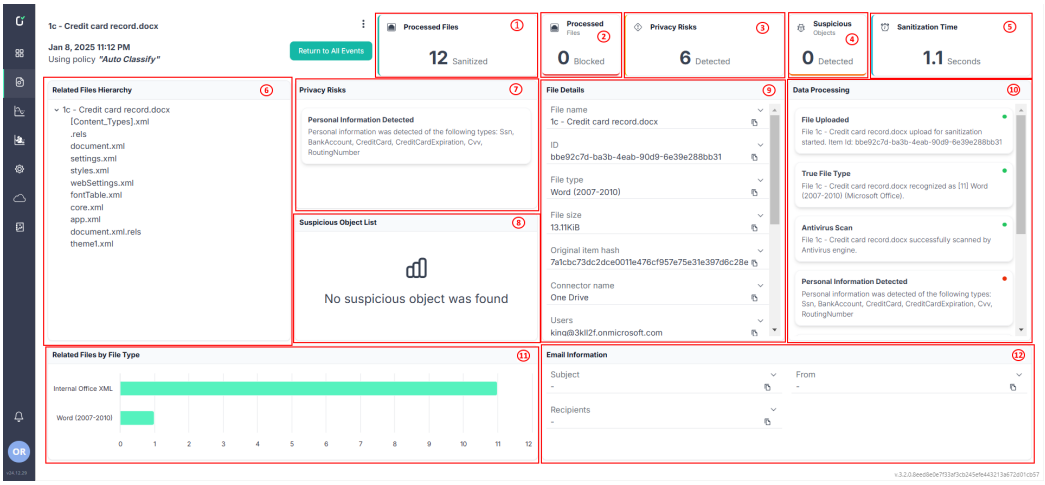
2.7.1 Download and Release file options

To select more options for the file, click on the 3 dots icon at the top right of this pane and select the desired download or release option:



2.7.2 View Full Details

To view more file details, click on the **View Full Details** button:



The following panes are displayed:

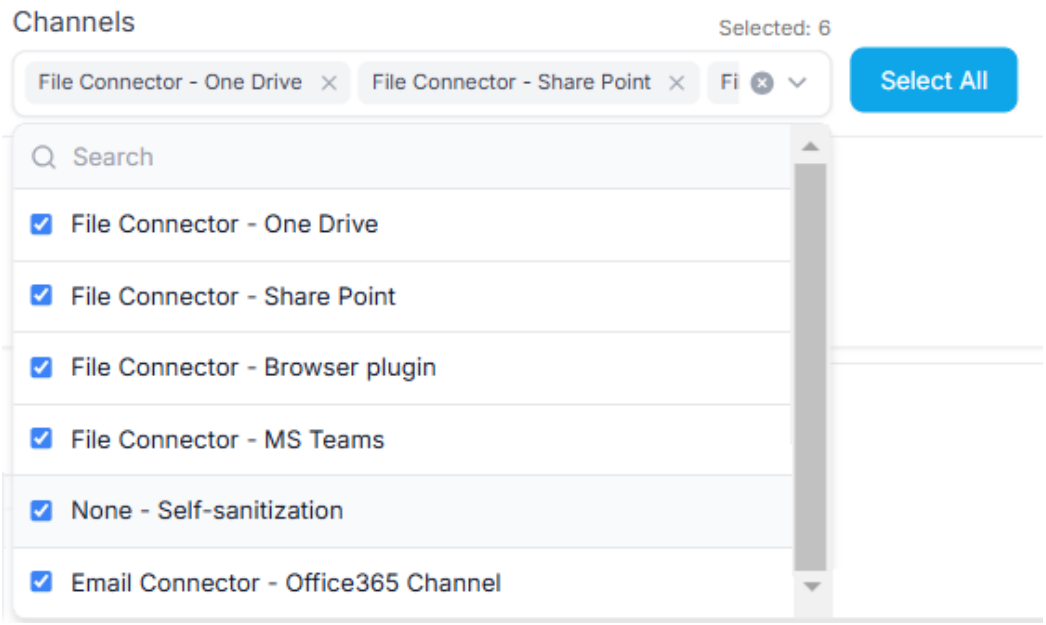
- **1** Processed Files (Sanitized) - number of files sanitized
- **2** Processed Files (Blocked) - number of files blocked
- **3** Privacy Risks - number of privacy risks detected
- **4** Suspicious Objects - number of suspicious objects detected
- **5** Sanitization Time - sanitization time in seconds
- **6** Related Files Hierarchy - displays attached files

- **7** Privacy Risks - displays Personal Information Detected (if any) and Personal Information Masked (if any)
- **8** Suspicious Object List - displays list of suspicious objects detected (if any)
- **9** File Details - displays the following file attributes:
  - File name
  - ID
  - File type
  - File size
  - Original item hash
  - Connector name
  - Users
  - Path
  - Groups
  - Client
  - Server
  - From
  - To
- **10** Data Processing - displays the high-level sanitization logs trail, including:
  - File Uploaded
  - True File Type
  - AntiVirus Scan
  - CDR process logs
  - DDR process logs
  - Sanitization Done
- **11** Related Files by File Type - displays a histogram of related files by file type
- **12** Email Information - including:
  - Subject
  - From
  - Recipients

2.7.3 Channels

The statistics displayed on the Monitor and Events pages relate to the file and email connectors that are currently selected. If you have more than one Votiro Connector

installed, you can filter the file list by Connector using the **Channels** list.

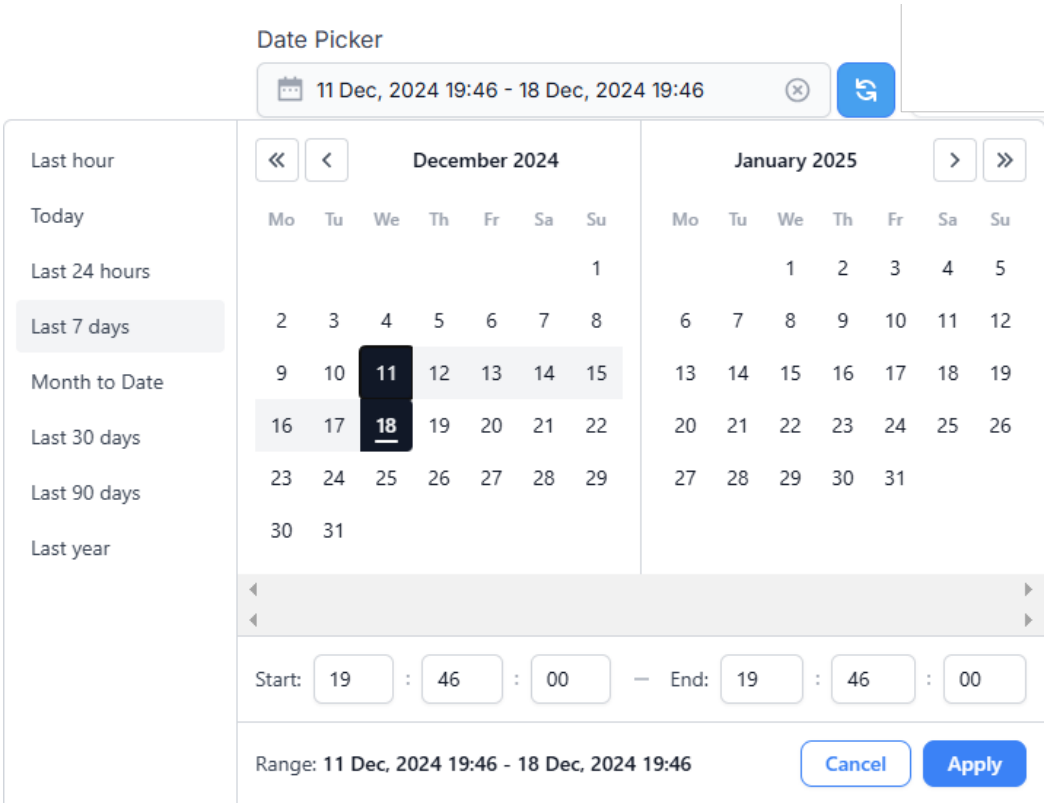


1. To display statistics for specific connectors, click on the **Channels** box.
2. Check the box next to each desired connector.
    - **None - Self-sanitization** refers to user-uploaded files through the **Test File** button on the **Policies** dashboard.
3. To select all available connectors, click on **Select All**.

Statistics update to show information for the selected Channels.

2.7.4 Date Picker

The statistics displayed on the Monitor and Events pages relate to the period that is currently selected. You can select a predefined period by clicking on the **Date Picker** box.

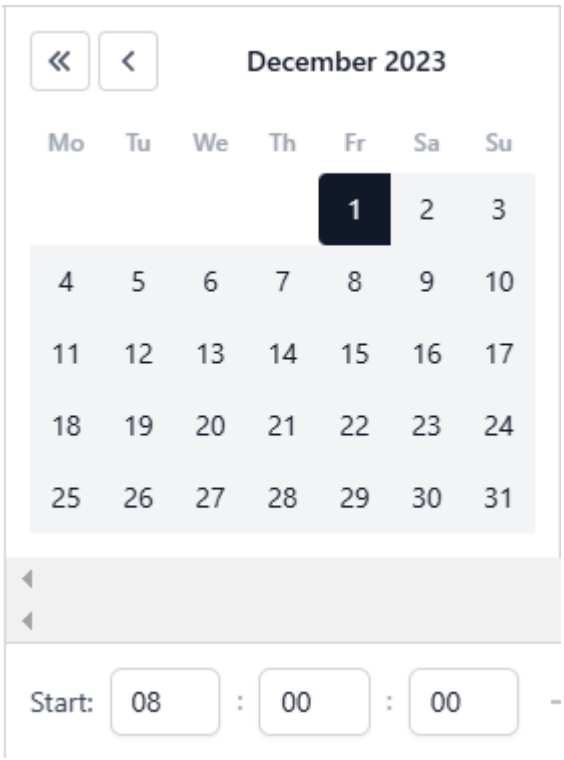


Votiro provides the following predefined settings:

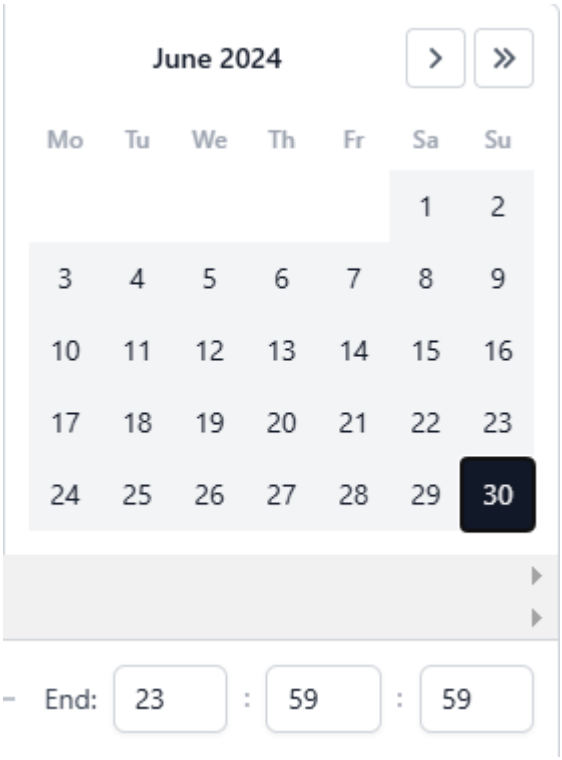
Period of Processing Activity	Meaning
Last hour	The information is for the period starting 60 minutes earlier until the current time.
Today	The information is for the period starting at 00:00 (midnight) of the current day until the current time.
Last 24 hours	The information is for the period starting from the current time, 24 hours earlier, until the current time.
Last 7 days	The information is for the period starting from the current time, 7 days earlier, until the current time. This is the default option.
Month to Date	The information is for the period starting at 00:00 (midnight) of the first day of the month until the current time.
Last 30 days	The information is for the period starting from the current date and time, one month earlier, until the current time.
Last 90 days	The information is for the period starting from the current date and time, three months earlier, until the current time.
Last year	The information is for the period starting from the current date and time, one year earlier, until the current time.
Custom	Allows you to define the period to display information for by selecting from and to dates and times from the calendar selection tool.

Defining a Custom Period

1. Click on the **Date Picker** box..
2. In the left pane, navigate to the desired start month and year by clicking the left arrow (<) to move to the previous month, or by clicking the left double arrow (<<) to jump to the same month in the previous year. If necessary, use the right arrow (>) or right double arrow (>>) to go forward in time.
3. After reaching the desired starting month in the left pane, click on the desired starting day of the month. The box containing the selected day of the month is highlighted in black.
4. In the **Start** boxes below the month, type the desired starting time. For example:



5. In the right pane, navigate to the desired end month and year by clicking the right arrow (>) to move to the next month, or by clicking the right double arrow (>>) to jump to the same month in the next year. If necessary, use the left arrow (<) or left double arrow (<<) to go back in time.
6. After reaching the desired ending month in the right pane, click on the desired ending day of the month. The box containing the selected day of the month is highlighted in black.
7. In the **End** boxes below the month, type the desired ending time. For example:



8. Click **Apply**. The custom period is displayed in **Date Picker** box.

Statistics update to show information for the custom period.

2.7.5 Releasing Files

You can release the original version of a file or a blocked email from the Incidents page.

> **CAUTION!**
> These procedures should be performed by a system administrator, and only in special circumstances.

Limitations

Release of original files is not supported for the AWS S3, Box, Menlo cloud connectors.

Releasing the Original Version of a Blocked File

If a file has been blocked, you can release it from the blob and send it to the OUT folder configured in Votiro On-prem for File Transfer.

> **Note**
> To enable the release of blocked files, you must first configure Votiro On-prem for File Transfer.

To release a blocked file from the Incidents page, click **Release Original**.

The original file is sent to the OUT folder.

Releasing the Original Version of a Blocked Email

If an email has been blocked, you can release it from the blob and send it to one or more email recipients.

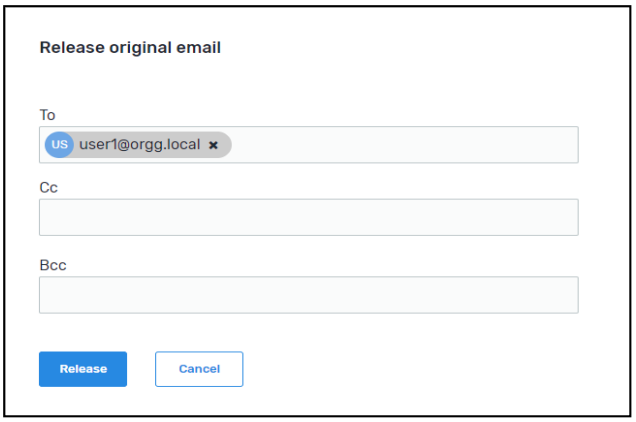
> **Note**
> To enable the release of blocked files, you must first configure the following system settings:
>
> - SMTP Server location
> - SMTP Server port
> - SMTP Server username
> - SMTP Server passwords
>
> For more information, see Configuring Settings on page 244.

- If the released file is of type EML, the original sender's email address appears in the email that contains the attachment.
- If the released file is of another type, the email address of the user defined for the SMTP Server username setting appears as sender in the email that contains the attachment.

To release a blocked email follow these steps:

1. On the Incidents page, tap an email file, then click icon to **Release Original**.

   The following dialog is displayed:

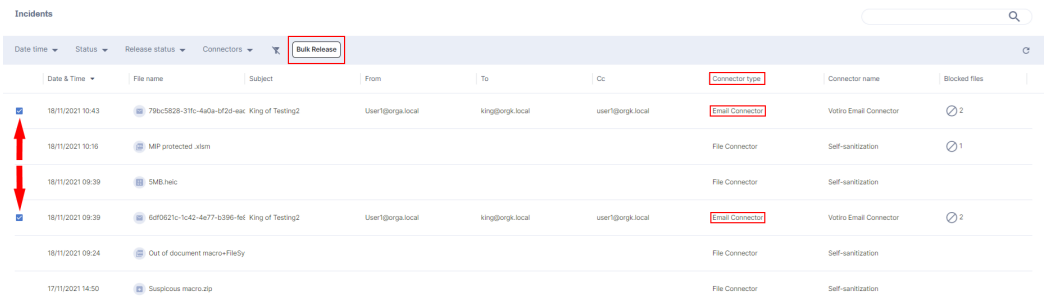


   The dialog shows the same email addresses that were included in the original email, as well as their original designations: To, Cc, or Bcc.

2. Accept the email addresses that are displayed or delete one or more, as required. You cannot add email addresses.

3. To send the email, click **Release**. The email is sent.

Releasing Multiple Emails



1. On the Incidents page, check the box at the beginning of each row of an email. An email is identified as such when the **Connector type** is **Email Connector**.

2. Click **Bulk Release** to send the emails.

> **Note**
> **Bulk Release** supports the Votiro Email connector only (Office 365 is not supported).

2.7.6 Retro Scan

This feature highlights the value of Votiro's Zero-day protection against Anti-Virus engine signature deficiencies.

Each file that enters your network is rescanned by Votiro every 3, 8 and 28 days against Anti-Virus engines. The Retro Scan capability can display whether Votiro detected the incoming file as a threat when the Anti-Virus engine did not.

For example, suppose an incoming file was marked by the Anti-Virus engine as "clean", but Votiro marked it as "malicious". Now suppose that the Anti-Virus signatures were later updated and when the file was rescanned the Anti-Virus engine marked it as "malicious". This means that Votiro blocked the potential real-time (Zero-day) attack when the Anti-Virus engine could not.

You can view all such incidents by selecting the **Retrospective findings** filter on the **Events** page.

2.8 File Types

In the Event Filters pane, select a file type to search for from the dropdown list. The default is all possible file types are displayed. The options are:

- Not Discovered Yet
- Unknown
- Empty File
- Directory
- Unrecognized
- Huge File
- Word
- Word (2007-2010)
- WordXML
- Excel
- Excel (2007-2010)
- ExcelXML
- Power Point
- Power Point (2007-2010)
- PowerPointXML
- Visio
- Project
- Obsolete Office Files
- Excel with Macros
- Word with Macros
- Power Point with Macros

- Excel on xml format
- Power Point Template
- Word Template
- Excel Template
- Macro File
- Word Pre 2007 Template
- Power Point Slide (2007-2010)
- Power Point Slide with Macros (2007-2010)
- Printer Settings
- Binary Excel (2007-2010)
- Visio (2007-2010)
- Visio with Macros
- WordXML Macro Enabled
- Model item data
- Open Word
- Open Spreadsheet
- WEBP
- Pcx File
- ICO
- JPEG
- WMF
- EMF
- GIF
- TIF
- BMP
- PNG
- Portable Gray Map Image File
- PPM File
- WDP
- Animated GIF
- SVG
- HEIF

- MP2
- MP3
- M4A
- WAV
- WMA
- AVI
- MOV
- MP4
- MPEG
- WMV
- 3GP
- M4v
- MKV
- FLV
- Corrupted PNG
- Unsupported Media File
- Material Exchange Format File
- CD Audio Track Shortcut File
- Text
- XML
- Postscript File
- Internal Office XML
- ShiftJisText
- Unknown Text
- JSON
- INI
- Script
- Embedded Macro Files
- Certificate
- EML File
- DAT File
- TNEF File

- TNEF Calendar Files
- MSG File
- Encrypted EML File
- Restricted Permission Message
- ZIP File
- RAR File
- 7Z File
- GZip File
- RAR5 File
- CAB File
- InstallShield CAB File
- VMware Virtual Machine Disk
- Tar File
- LZH File
- XZ File
- BZIP2 File
- Executable
- MST files
- Binary File
- JTD File
- JTDC File
- Encrypted Ichitaro File
- DICOM File
- Thumbnail File
- Statistical Files
- LabView
- VCF
- RTF Files
- DXF File
- Adobe Air
- PDF
- PST ANSI

- PST
- RPT
- JAR
- HTML
- INF File
- SQL File
- MHT File
- Calendar File
- CSS
- DWG File
- PreR14Dwg File
- DWS File
- DWT File
- JWW File
- p7s
- DWF File
- HTML Body
- HTML Attachments
- XFA
- PSD File
- V-nas BFO File
- XDW File
- SolidWorks File
- Parasolid model File
- Initial Graphics Specification File
- ZSoft PCX bitmap File
- CATIA Product Data File
- eDrawings File
- ACIS Solid Model File
- Sfc File
- P21 File
- Shortcut File

- RSP File
- Solution User Option File
- Pgp File
- Tableau Workbook
- Tableau Packaged Workbook
- Tableau Hyper Data Base File
- HWP File
- Excel95 File
- PreWord97 File
- HWP 3.0 File
- PowerPoint95 File
- HWPX File
- HML File
- Excel2 File
- Excel3 File
- Excel4 File
- IQY File
- SLK File
- SettingContent-ms File
- Unknown Ole Object
- Docx Ole Object
- Docm Ole Object
- Dotx Ole Object
- Xlsx Ole Object
- Pptx Ole Object
- Bmp Ole Object
- Pdf Ole Object
- Equation Ole Object
- Slide Ole Object
- SlideX Ole Object
- SlideM Ole Object
- Xls Ole Object

- Pptm Ole Object
- Jtd Ole Object
- Doc Ole Object
- JustFocuse Slide Ole Object
- JustFocuse Presentation Ole Object
- Hwp Ole Object
- Xlsb Ole Object
- Link Ole Object
- DB Files
- Mac AppleSingle encoded
- Mac AppleDouble encoded
- Mac OS X folder information
- MAC OS X crash log
- Apple iWork

2.8.1 Retro Scan

This feature highlights the value of Votiro's Zero-day protection against Anti-Virus engine signature deficiencies.

Each file that enters your network is rescanned by Votiro every 3, 8 and 28 days against Anti-Virus engines. The Retro Scan capability can display whether Votiro detected the incoming file as a threat when the Anti-Virus engine did not.

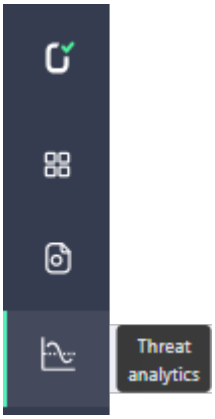
For example, suppose an incoming file was marked by the Anti-Virus engine as "clean", but Votiro marked it as "malicious". Now suppose that the Anti-Virus signatures were later updated and when the file was rescanned the Anti-Virus engine marked it as "malicious". This means that Votiro blocked the potential real-time (Zero-day) attack when the Anti-Virus engine could not.

You can view all such incidents by selecting the **Retrospective findings** filter on the **Events** page.

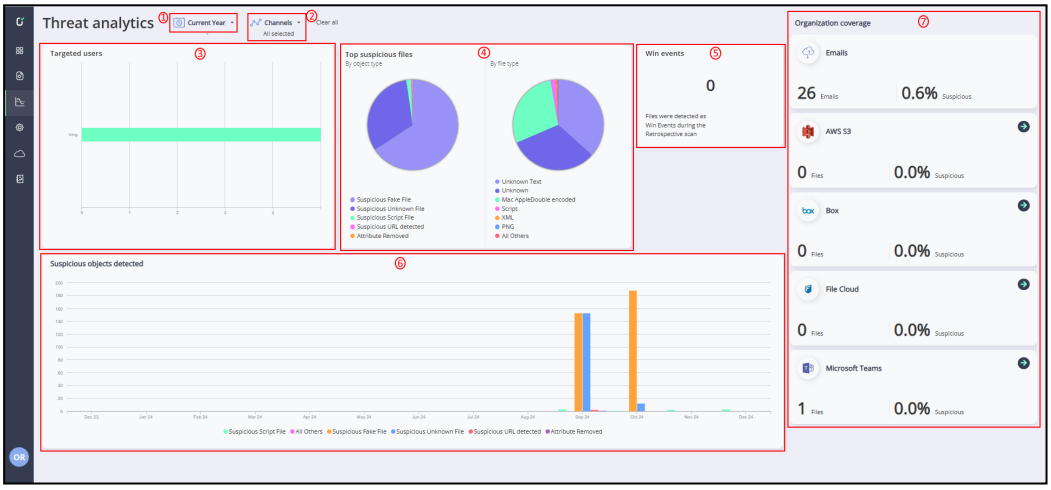
2.9 Threat Analytics Dashboard

The **Threat Analytics** dashboard displays data about suspicious files or objects.

From the navigation pane on the left, click the **Threat Analytics** icon:



The **Threat Analytics** page is displayed:

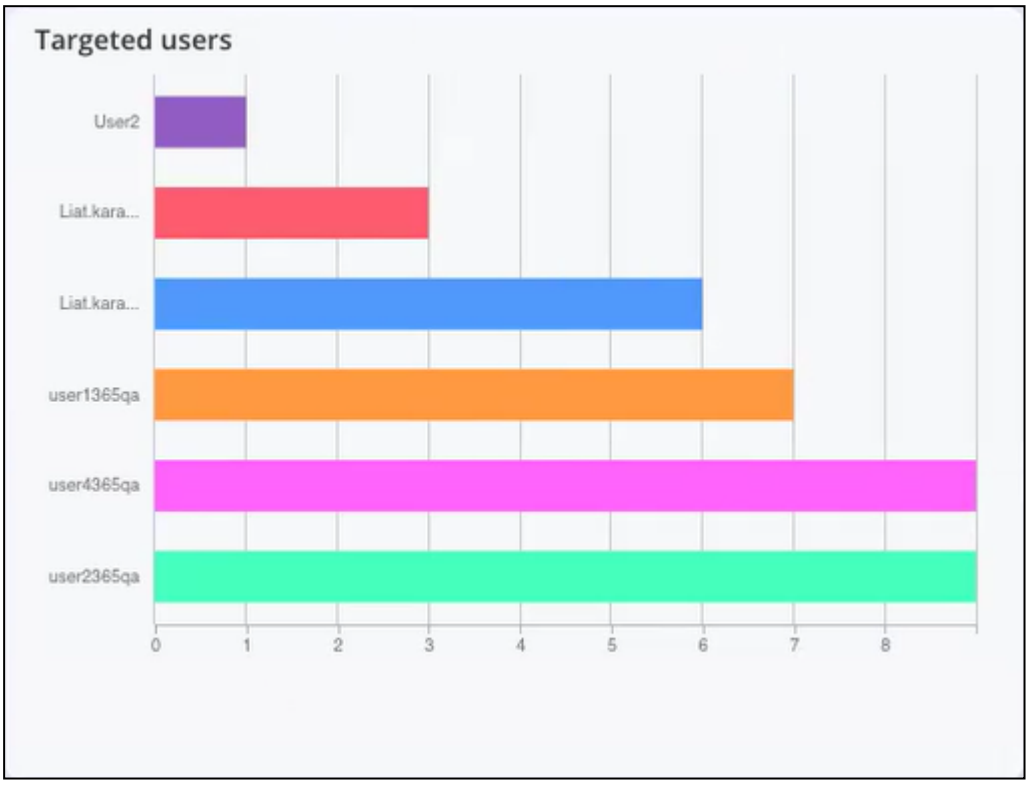


The page contains the following panes, outlined in red and numbered as in the above screenshot:

- **1** Time interval - filters the display by the time period selected. See Filter by Time Period.
- **2** Channels - filters the display by the channels selected. See Filter by Channels.
- **3** Targeted Users - displays the top users targeted with suspicious files. See Targeted users.
- **4** Top suspicious files - displays pie charts of the top suspicious files. See Top Suspicious Files.
- **5** Win events - displays the number of Win events detected during the retrospective scan. See Retro Scan.
- **6** Suspicious objects detected - displays a histogram chart of suspicious objects detected during the selected time period. See Suspicious Objects Detected.
- **7** Organization Coverage - displays a breakdown of sensitive files per channel. See Organization Coverage.

2.9.1 Targeted users

The Targeted users pane displays a histogram of the top ten users targeted with suspicious files. Each user is represented by a histogram. The length of the histogram corresponds to the number of suspicious files, which is plotted on the horizontal axis.



Extracting more data by drilling down

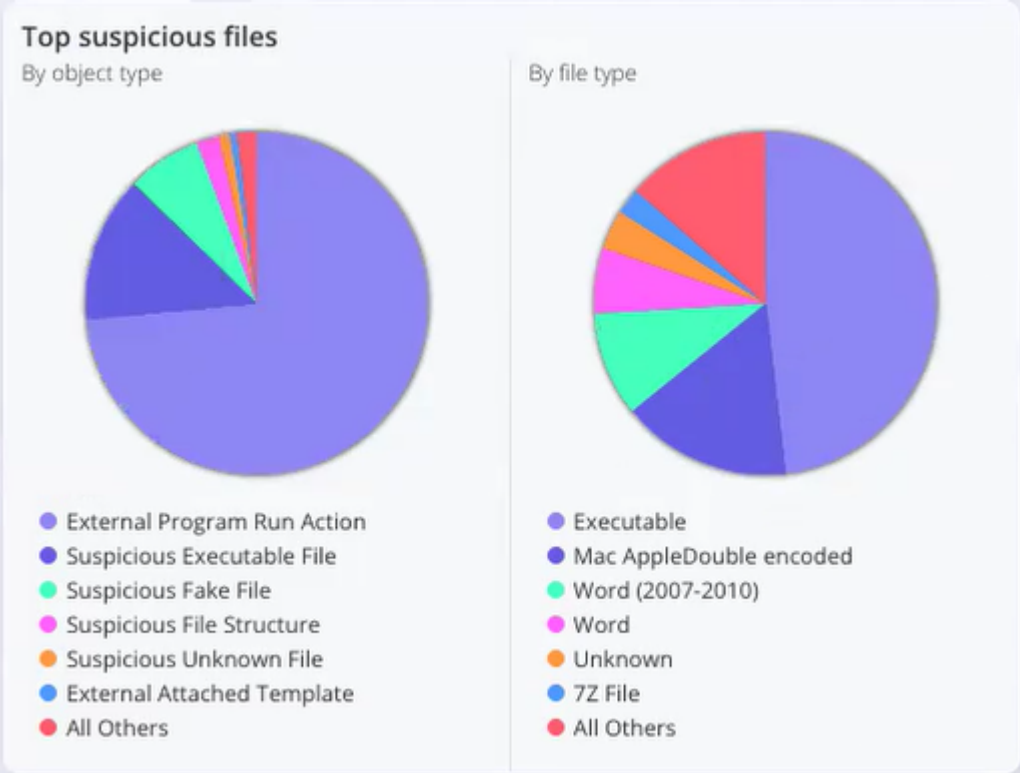
The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart. For more details, see Operational workflow.

2.9.2 Top Suspicious Files

The two pie charts displayed in the **Top Suspicious Files** pane relate to the top ten suspicious files containing sensitive data according to the following categories:

- **By object type** - files classified according to object type. These include, among others:
  - **External Program Run Action**
  - **Suspicious Executable File**
  - **Suspicious Fake File**
  - **Suspicious File Structure**
  - **Suspicious Unknown File**
  - **External Attached Template**

- **By file type** - files classified according to file type, such as Executable, Word, PDF, EML, etc.

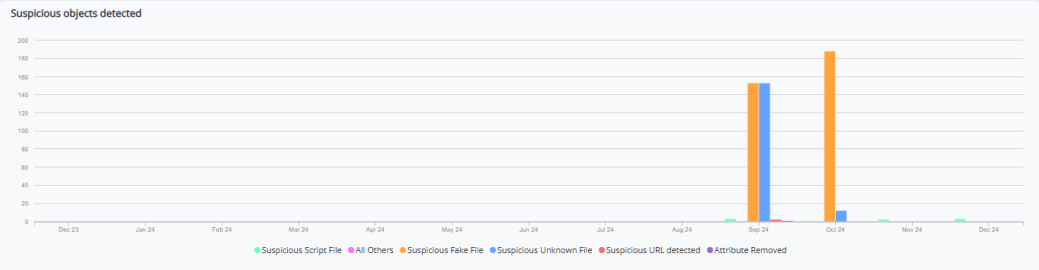


Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart. For more details, see Operational workflow.

2.9.3 Suspicious Objects Detected

The **Suspicious objects detected** pane displays a histogram chart of the suspicious objects detected in the processed files for the time period selected. The files are displayed according to their object or file types, such as Suspicious Fake File, Attribute Removed, etc.



Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart. For more details, see Operational workflow.

2.9.4 Retro Scan

This feature highlights the value of Votiro's Zero-day protection against Anti-Virus engine signature deficiencies.

Each file that enters your network is rescanned by Votiro every 3, 8 and 28 days against Anti-Virus engines. The Retro Scan capability can display whether Votiro detected the incoming file as a threat when the Anti-Virus engine did not.

For example, suppose an incoming file was marked by the Anti-Virus engine as "clean", but Votiro marked it as "malicious". Now suppose that the Anti-Virus signatures were later updated and when the file was rescanned the Anti-Virus engine marked it as "malicious". This means that Votiro blocked the potential real-time (Zero-day) attack when the Anti-Virus engine could not.

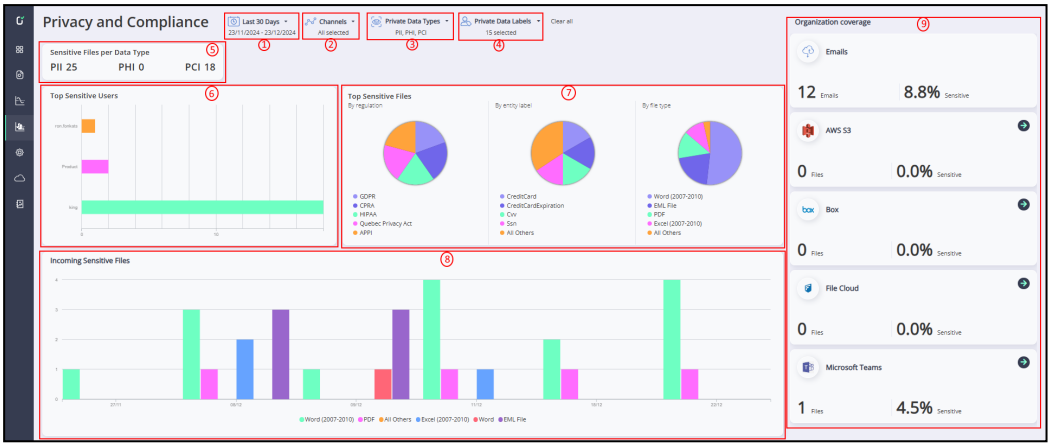
You can view all such incidents by selecting the **Retrospective findings** filter on the **Events** page.

2.10 Privacy and Compliance Dashboard

The **Privacy and Compliance** dashboard displays data about files containing sensitive data.

From the navigation pane on the left, click the **Privacy and Compliance** icon:

The **Privacy and Compliance** dashboard is displayed:

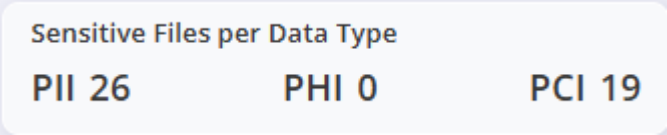


The page contains the following panes, outlined in red and numbered as in the above screenshot:

- **1** Time interval - filters the display by the time period selected. See Filter by Time Period.
- **2** Channels - filters the display by the channels selected. See Filter by Channels.
- **3** Private Data Types - filters the display by the private data types selected. See Filter by Private Data Types.
- **4** Private Data Labels - filters the display by the private data labels selected. See Filter by Private Data Labels.
- **5** Sensitive Files per Data Type - displays the number of files containing the selected private data types according to the private data labels selected. See Sensitive Files per Data Type.
- **6** Top Sensitive Users - displays histograms of the number of files for the top five users containing the selected private data types according to the private data labels selected. See Top Sensitive Users.
- **7** Top Sensitive Files - displays pie charts for the top five sensitive files. See Top Sensitive Files.
- **8** Incoming Sensitive Files - displays histograms of the incoming files containing sensitive data. See Incoming Sensitive Files.
- **9** Organization Coverage - displays a breakdown of sensitive files per channel. See Organization Coverage.

2.10.1 Sensitive Files per Data Type

The statistics displayed in the **Sensitive Files per Data Type** pane relate to the **Private Data Types** and **Private Data Labels** that are currently selected.



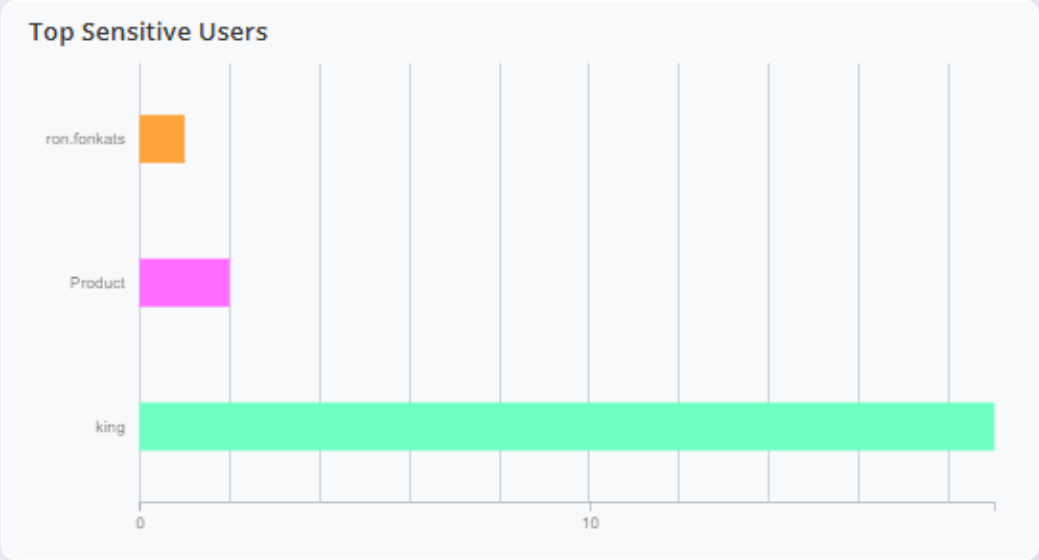
The statistics displayed include all files containing the selected private data types and selected private data labels.

Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart. For more details, see Operational workflow.

2.10.2 Top Sensitive Users

The histogram displayed in the **Top Sensitive Users** pane relate to the top ten users who own files containing sensitive data according to the private data types and private data labels that are currently selected.



Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart. For more details, see Operational workflow.

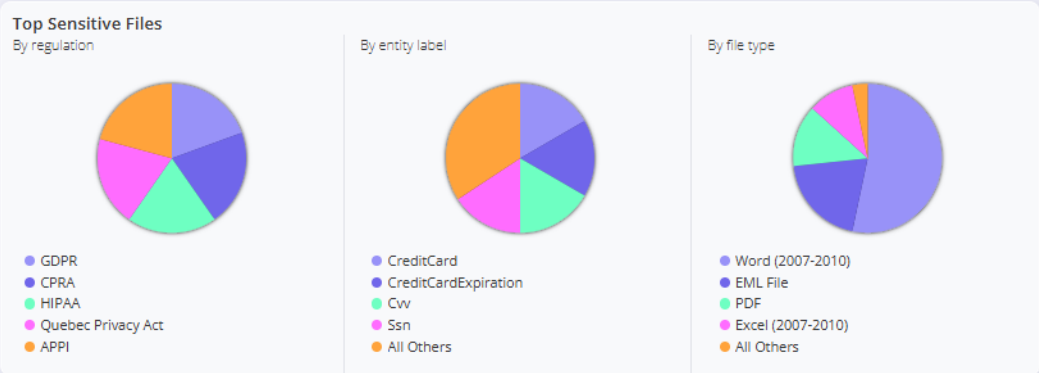
2.10.3 Top Sensitive Files

The three pie charts displayed in the **Top Sensitive Files** pane relate to the top five files containing sensitive data according to the following categories:

- **By regulation** - files classified according to private data categorized by a regulatory body. These include:
  - **GPDR** - General Data Protection Regulation (Regulation (EU) 2016/679). This is a regulation on information privacy in the European Union (EU) and the European Economic Area (EEA).
  - **CPRA** - California Privacy Rights Act of 2020. This is the State of California's consumer privacy law.

- **HIPAA** - Health Insurance Portability and Accountability Act of 1996 (also known as the Kennedy–Kassebaum Act). This is the set of national standards for the protection of certain health information in the USA.
- **Quebec Privacy Act** - “The Privacy Legislation Modernization Act” or "Law 25". This is the Province of Quebec's privacy law, and is comparable to the EU's GPDR.
- **APPI** - Japan's Act on the Protection of Personal Information is a federal personal information protection law to regulate the handling of personal information by individuals and organizations, including government agencies, businesses, and nonprofits.

- **By entity label** - files classified by private data label. See Filter by Private Data Labels.
- **By file type** - files classified according to file type, such as Word, PDF, EML, etc.



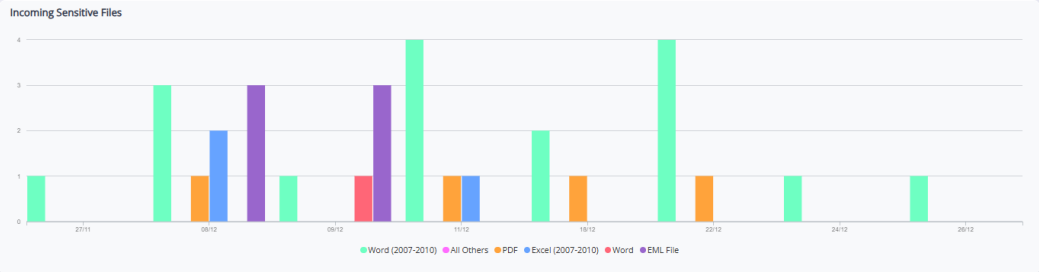
Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart. For more details, see Operational workflow.

2.10.4 Incoming Sensitive Files

The **Incoming Sensitive Files** pane displays a histogram chart of the incoming files containing sensitive data according to the selected private data types and private data labels for the time period selected. The files are displayed according to their file types, such as Word, PDF, EML, etc.

In the example below, the time period is **Last 30 Days**:

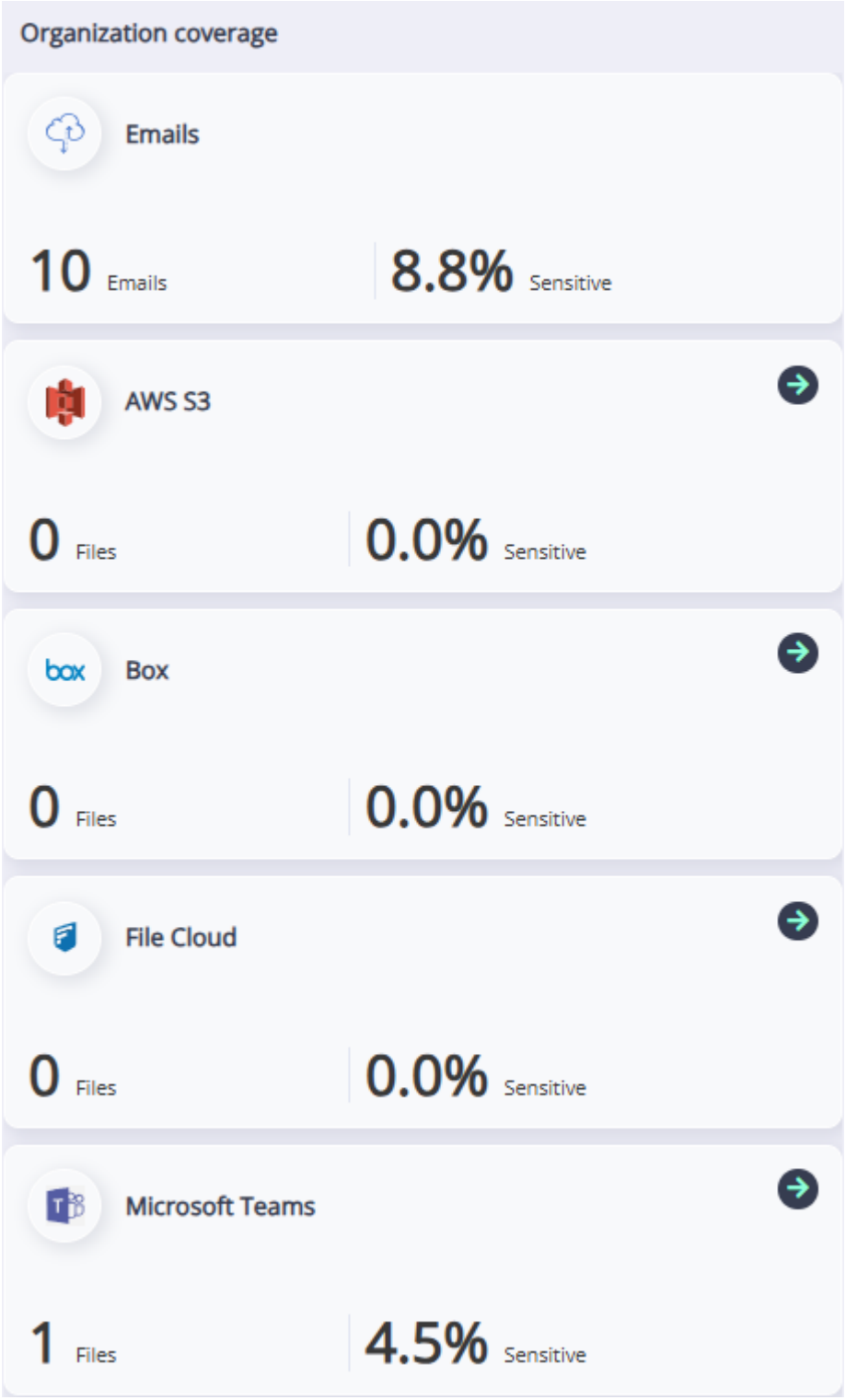


Extracting more data by drilling down

The displayed data can be modified by filtering and more data can be displayed by drilling down in the chart. For more details, see Operational workflow.

2.10.5 Organization Coverage

The **Organization Coverage** pane displays a breakdown of sensitive files per channel according to the private data types and private data labels that are currently selected within the selected time period.



For each channel, the following is displayed:

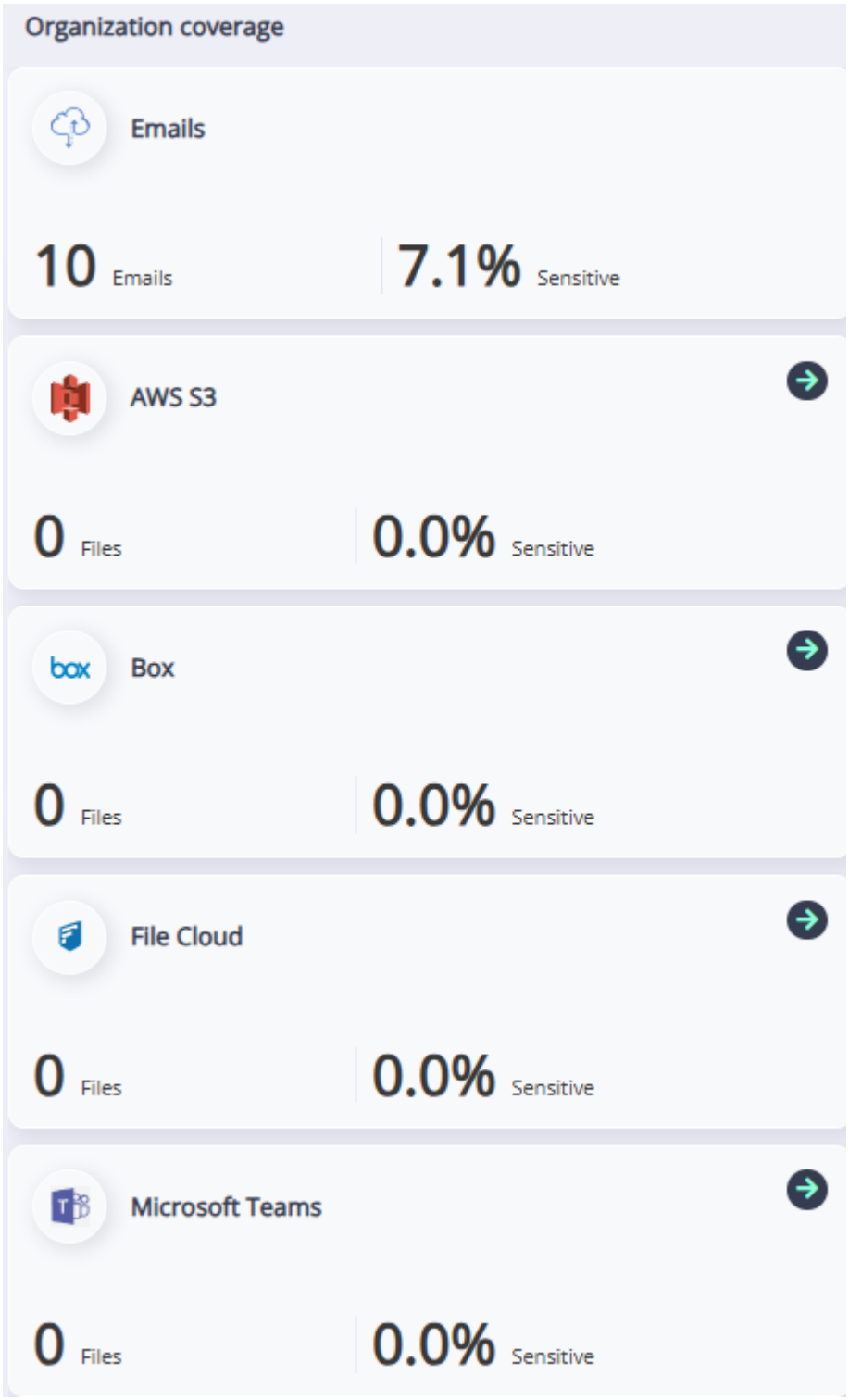
- Number of files or emails - the number of sensitive files or emails received according to the private data types and private data labels that are currently selected within the selected time period
- % Sensitive - the percentage of the total files or emails that are sensitive

Filtering the display

To filter the view by specific data labels, use **Filter privacy labels** to filter the list for the desired data label. For example, to view only sensitive files containing SSN:

1. In **Private Data Labels**, click on **Unselect all**.
2. Enter the desired private data label in the **Filter privacy labels** box. For example, ssn.
3. Check the box next to the desired privacy data label. For example, SSN.

4. Click on the **Organization coverage** pane. The statistics are updated to reflect the new selected data.



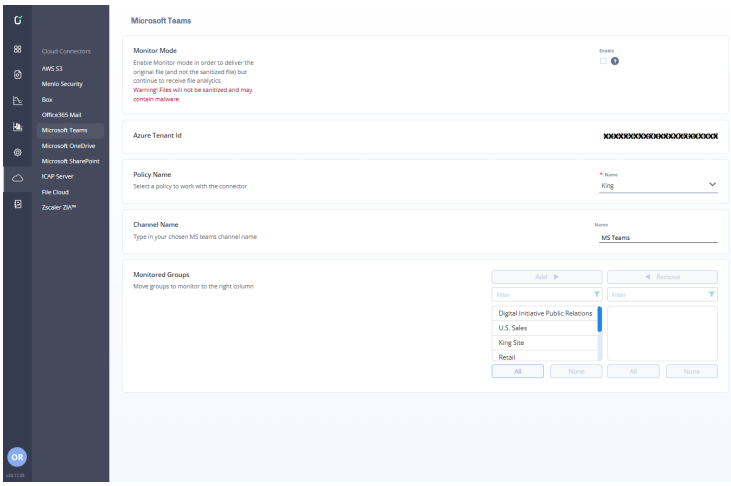
5. The **Private Data Labels** are updated to show the filtered selection:

Configuring an integration

There is an option that allows the user to configure an integration directly from the **Organization coverage** pane. This option can be useful if the displayed statistics for a specific integration are not as expected (for example, the display shows 0.0% Sensitive) or the user viewing the display sees a need to change the integration configuration in the Votiro Management Console.

For example:

1. To configure the Microsoft Teams integration, click on the icon on the right side of the Microsoft Teams box.
2. The **Microsoft Teams** page in the Cloud Connectors menu opens:



2.11 Supported File Formats

2.11.1 Supported File Formats

Votiro's DDR solution supports the following file formats for detection and masking:

- Email
- PDF
- Word
- Excel
- Images (Supported only within a PDF)

2.12 Supported Data Labels

2.12.1 Supported Data Types

Detection and masking of privacy data is implemented based on three types of data types:

- **PII** - Personally Identifiable Information (PII) is any information connected to a specific individual that can be used to uncover that individual's identity. See Table 1 PII data labels for a detailed list of PII data labels.
- **PHI** - Protected Health Information (PHI) is any information in the medical record or designated record set that can be used to identify an individual. See Table 2 PHI data labels for a detailed list of PHI data labels.
- **PCI** - Payment Card Industry (PCI) data apply to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. See Table 3 PCI data labels for a detailed list of PCI data labels.

2.12.2 Supported Data Labels

The tables below list all the privacy data labels for each data type.

Table 1 PII data labels

Label	Description	Policy & Regulatory Compliance
Account number	Customer account or membership identification number Examples: *Policy No. 10042992; Member ID: HZ-5235-001*	HIPAA_SAFE_HARBOR, CCI
Age	Numbers associated with an individual's age Examples: *27 years old; 18 months old* When given in years, only the number is flagged, but both number and time unit are flagged when given in other units like months or weeks Also includes age ranges Examples: *29-35 years old; 18+; A man in his forties*	GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI

Label	Description	Policy & Regulatory Compliance
Date	Specific calendar dates, which can include days of the week, dates, months, or years Examples: *Friday, Dec. 18, 2002; Dated: 02/03/97* **Note**: If no calendar date is specified, days of the week are not flagged: e.g. *Your appointment is on Monday* **Note**: Indexical terms are not flagged: e.g. *yesterday; tomorrow*	HIPAA_SAFE_HARBOR, Quebec Privacy Act, CCI
Date interval	Broader time periods, including date ranges, months, seasons, years, and decades Examples: *2020-2021; 5-9 May; January 1984*	HIPAA_SAFE_HARBOR, CCI
DOB	Dates of birth Example: *Born: March 7, 1961*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI
Driver license	Driver's permit numbers Example: *DL# 134711-320* Includes International Driving Permits (IDP) and Pilot's licenses	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI
Duration	Periods of time, specified as a number and a unit of time Example: *8 months; 2 years*	
Email address	Email addresses Example: *info@private-ai.com*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI, CCI
Event	Names of events or holidays Examples: *Olympics; Yom Kippur*	

Label	Description	Policy & Regulatory Compliance
Filename	Names of computer files, including the extension or filepath Example: *Taxes/2012/brad-tax-returns.pdf*	CCI
Gender	Terms indicating gender identity, including slang terms. Note that performance is stronger for terms that are more likely to occur in formal documents, such as "male", "transgender", "non-binary", "female", "M", "F", etc. Other terms, such as "woman", "gentleman", etc., may not be captured in every context. Examples: *female; trans*	CPRA, GDPR, GDPR Sensitive, APPI Sensitive
Healthcare number	Healthcare numbers and health plan beneficiary numbers Example: *Policy No.: 5584-486-674-YM* Includes medical record numbers, health insurance policy/account numbers, and member IDs, for example, German Sozialversicherungsnummer (also used as SSN), Philippine PhilHealth ID number, Ukrainian VHI number	CPRA, GDPR, HIPAA, Quebec Privacy Act, APPI
IP address	Internet IP address, including IPv4 and IPv6 formats Examples: *192.168.0.1*;*2001:db8:0:0:0:8a2e::7334*	CPRA, GDPR, HIPAA, Quebec Privacy Act, APPI
Language	Names of natural languages Examples: *Korean; French*	GDPR, GDPR Sensitive, APPI Sensitive
Location	Metaclass for any named location reference; See subclasses below Examples: *Eritrea; Lake Victoria* May co-occur with Organization when the context refers explicitly to the organization's location Example: The patient was transferred to *Northwest General Hospital*	GDPR, HIPAA_SAFE_HARBOR, APPI, CCI

Label	Description	Policy & Regulatory Compliance
Location address	Full or partial physical mailing addresses, which can include: building name or number, street, city, county, state, country, zip code Examples: *25/300 Adelaide T., Perth WA 6000, Aus.* *145 Windsor St.* Mail to: *Kollwitzstr 13, 10405, Berlin*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI, CCI
Location address street	A subclass of **Location address**, covering: a building number and street name, plus information like a unit numbers, office numbers, floor numbers and building names, where applicable Examples: *25/300 Adelaide T., Perth WA 6000, Aus.* *145 Windsor St.* Mail to: *Kollwitzstr 13, 10405, Berlin*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI, CCI
Location city	Municipality names, including villages, towns, and cities Examples: *Toronto; Berlin; Denpasar*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI, CCI
Location coordinate	Geographic positions referred to using latitude, longitude, and/or elevation coordinates Example: We're at *40.748440 and -73.984559*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI
Location country	Country names Examples: *Canada; Namibia*	GDPR, APPI, CCI
Location state	State, province, territory, or prefecture names Examples: *Ontario; Arkansas*; Ich lebe in *NRW*	GDPR, APPI, CCI

Label	Description	Policy & Regulatory Compliance
Location zip	Zip codes (including Zip+4), postcodes, or postal codes Examples: *90210; B2N 3E3* Optimized for various English-speaking locales (Australia, Canada, United Kingdom, United States), as well as international equivalents	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI, CCI
Marital status	Terms indicating marital status Examples: *single; common-law; ex-wife; married*	APPI Sensitive
Money	Names and/or amounts of currency Examples: *15 pesos; $94.50*	CCI
Name	Names of individuals, not including personal titles such as 'Mrs.' or 'Mr.' Examples: *Dwayne Johnson*; Mr. *Khanna*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI
Name family	Names indicating a person's family or community; often a last name in Western cultures and first name in Eastern cultures Examples: *François Truffaut; Ozu Yasujirō*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI
Name given	Names given to an individual, usually at birth; often first / middle names in Western cultures and middle / last names in Eastern cultures Examples: *François Truffaut; Ozu Yasujirō*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI
Name medical professional	Full names, including professional titles and certifications, of medical professional, such as doctors and nurses Example: *Attending physician: Dr. Kay Martinez, MD*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI

Label	Description	Policy & Regulatory Compliance
Numerical PII	Numerical PII (including alphanumeric strings) that doesn't fall under other categories. See also a section below on international variants as some of them are mapped to this category, for example, Belgian BTW nummer or European VAT number. Includes the following: numbers in the medical field, such as device serial numbers, POS codes, NPI numbers, etc.; computer numbers like MAC addresses, cookie IDs, VPNs, error codes, access codes, message IDs, etc.; business-related numbers like DUNS numbers, company registration numbers, provider IDs, etc.; numbers related to purchasing, like order IDs, transaction numbers, confirmation numbers, tracking numbers, etc.; also numbers assigned to various forms of IDs, files, documents, proceedings, invoices, claim IDs, record IDs, etc.	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI, CCI
Occupation	Job titles or professions Examples: *professor; actors; engineer; CPA*	Quebec Privacy Act, APPI, CCI
Organization	Names of organizations or departments within an organization Examples: *BHP; McDonald's; LAPD* May co-occur with LOCATION when the context refers explicitly to the organization's location, for example, Donations can be brought to *Royal Canadian Legion Branch 43*	Quebec Privacy Act, APPI, CCI
Organization medical facility	Names of medical facilities, such as hospitals, clinics, pharmacies, etc. Examples: *Northwest General Hospital;* *Union Family Health Clinic*	Quebec Privacy Act, APPI
Origin	Terms indicating nationality, ethnicity, or provenance Examples: *Canadian; Sri Lankan*	CPRA, GDPR, GDPR Sensitive, Quebec Privacy Act, APPI Sensitive

Label	Description	Policy & Regulatory Compliance
Passport number	Passport numbers, issued by any country Examples: *PA4568332; NU3C6L86S12*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI
Password	Account passwords, PINs, access keys, or verification answers Examples: *27%alfalfa; temp1234* *My mother's maiden name is Smith*	CPRA, APPI, CCI
Phone number	Telephone or fax numbers Example: *+4917643476050*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI
Physical attribute	Distinctive bodily attributes, including terms indicating race Examples: *I'm 190cm tall; He belongs to the Black students' association*	CPRA, GDPR, GDPR Sensitive, APPI Sensitive
Political affiliation	Terms referring to a political party, movement, or ideology Examples: *liberal; Republican*	CPRA, GDPR, GDPR Sensitive, Quebec Privacy Act, APPI Sensitive
Religion	Terms indicating religious affiliation Examples: *Hindu; Presbyterian*	CPRA, GDPR, GDPR Sensitive, Quebec Privacy Act, APPI Sensitive

Label	Description	Policy & Regulatory Compliance
Sexuality	Terms indicating sexual orientation, including slang terms Examples: *bisexual; gay; straight*	CPRA, GDPR, GDPR Sensitive, APPI Sensitive
SSN	Social Security Numbers or international equivalent government identification numbers Examples: *078-05-1120; ***-***-3256*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI
Time	Expressions indicating clock times Examples: *19:37:28; 10pm EST*	CCI
URL	Internet addresses Example: *www.private-ai.com*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, CCI
Username	Usernames, login names, or handles Examples: *privateairocks; @_PrivateAI*	CPRA, GDPR, APPI
Vehicle ID	Vehicle identification numbers (VINs), vehicle serial numbers, and license plate numbers Examples: *5FNRL38918B111818; BIF7547*	CPRA, GDPR, HIPAA_SAFE_HARBOR, APPI, CCI
Zodiac sign	Names of Zodiac signs Examples: *Aries; Taurus*	

Table 2 PHI data labels

Label	Description	Policy & Regulatory Compliance
Blood type	Blood types Example: She's *type AB positive*	CPRA, GDPR, Quebec Privacy Act
Condition	Names of medical conditions, diseases, syndromes, deficits, disorders Examples: *chronic fatigue syndrome; arrhythmia; depression*	CPRA, GDPR, Quebec Privacy Act, APPI Sensitive
Dose	Medically prescribed quantity of a medication Example: *limit intake to 700 mg/day*	HIPAA_SAFE_HARBOR, Quebec Privacy Act, CCI
Drug	Medications, vitamins, and supplements Examples: *advil; Acetaminophen; Panadol*	HIPAA_SAFE_HARBOR, CCI
Injury	Bodily injuries, including mutations, miscarriages, and dislocations Examples: *I broke my arm; I have a sprained wrist*	CPRA, GDPR, Quebec Privacy Act, APPI Sensitive
Medical process	Medical processes, including treatments, procedures, and tests Examples: *heart surgery; CT scan*	CPRA, GDPR, Quebec Privacy Act, APPI Sensitive, CCI
Statistics	Medical statistics Example: *18% of patients*	Quebec Privacy Act

Table 3 PCI data labels

Label	Description	Policy & Regulatory Compliance
Bank account	Bank account numbers and international equivalents, such as IBAN Example: *Acct. No.: 012345-67*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI, CCI
Credit card	Credit card numbers Examples: *0123 0123 0123 0123* ***** **** ****4252* Includes debit, ATM, Direct Debit, PrePay, Charge Cards, and support for cards that do not have 16 digits such as American Express or China UnionPay cards. Flags mentions of complete numbers as well as the last four digits only.	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI, CCI
Credit card expiration	Expiration date of a credit card Example: *Expires: July 2023; Exp: 02/28*	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI

Label	Description	Policy & Regulatory Compliance
CVV	3- or 4-digit card verification codes and equivalents Example: *CVV: 080* Includes institution-specific variants: American Express: CID (card ID), CVD (card verification data) CSC / 3CSC (card security code) China UnionPay: CVN (card validation number) CIBC Mastercard: SPC (signature panel code) Discover: CID (card ID), CVD (card verification data) ELO (Brazil): CVE (Elo verification code) JCB (Japan Credit Bureau): CAV (card authentication value) Mastercard: CVC (card validation code) VISA: CVV (card verification value)	CPRA, GDPR, HIPAA_SAFE_HARBOR, Quebec Privacy Act, APPI, CCI
Routing number	Routing number associated with a bank or financial institution Example: *012345678* Includes international equivalents: Canadian & British sort codes, Australian BSB numbers, Indian Financial System Codes, Branch/transit numbers, Institution numbers, and Swift codes	CCI

2.13 Supported Regulations

2.13.1 Supported Regulations

The following regulations are supported:

- **GPDR** - General Data Protection Regulation (Regulation (EU) 2016/679). This is a regulation on information privacy in the European Union (EU) and the European Economic Area (EEA). It is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in and outside of the European Union (EU). For more details, see General Data Protection Regulation - GPDR.

- **CPRA** - California Privacy Rights Act of 2020. This is the State of California's consumer privacy law. This law allows consumers to prevent businesses from sharing their personal data, correct inaccurate personal data, and limit businesses' usage of "sensitive personal information", which includes precise geolocation, race, ethnicity, religion, genetic data, private communications, sexual orientation, and specified health information. For more details, see The California Privacy Rights Act of 2020.
- **HIPAA** - Health Insurance Portability and Accountability Act of 1996 (also known as the Kennedy–Kassebaum Act). This is the set of national standards for the protection of certain health information in the USA. The HIPAA safe harbor de-identification method is the process of removing the patient's and the patient's relatives, household members, and employers' designated identifiers. The HIPAA safe harbor de-identification process is complete if the covered organization has no full information. For more details, see Health Information Privacy.
- **Quebec Privacy Act** - “The Privacy Legislation Modernization Act” or "Law 25". This is the Province of Quebec's privacy law, and is comparable to the EU's GPDR. For more details, see Quebec's Private Sector Privacy Act.
- **APPI** - Japan's Act on the Protection of Personal Information is a federal personal information protection law to regulate the handling of personal information by individuals and organizations, including government agencies, businesses, and nonprofits. For more details, see Act on the Protection of Personal Information.

2.14 Supported Languages

2.14.1 Supported Languages

The table below lists the core languages supported.

Language	ISO Code	Supported Regional Varieties
Dutch	nl	The Netherlands
English	en	Australia, Canada, United Kingdom, United States
French	fr	Canada (Quebec), France, Switzerland
German	de	Germany, Belgium, Austria, Switzerland
Hindi	hi	India
Italian	it	Italy, Switzerland
Japanese	ja	Japan
Korean	ko	Korea
Mandarin (simplified)	zh-Hans	China, Singapore
Portuguese	pt	Brazil, Portugal
Russian	ru	Russia
Spanish	es	Mexico, Spain

Language	ISO Code	Supported Regional Varieties
Tagalog	tl	Philippines
Ukrainian	uk	Ukraine

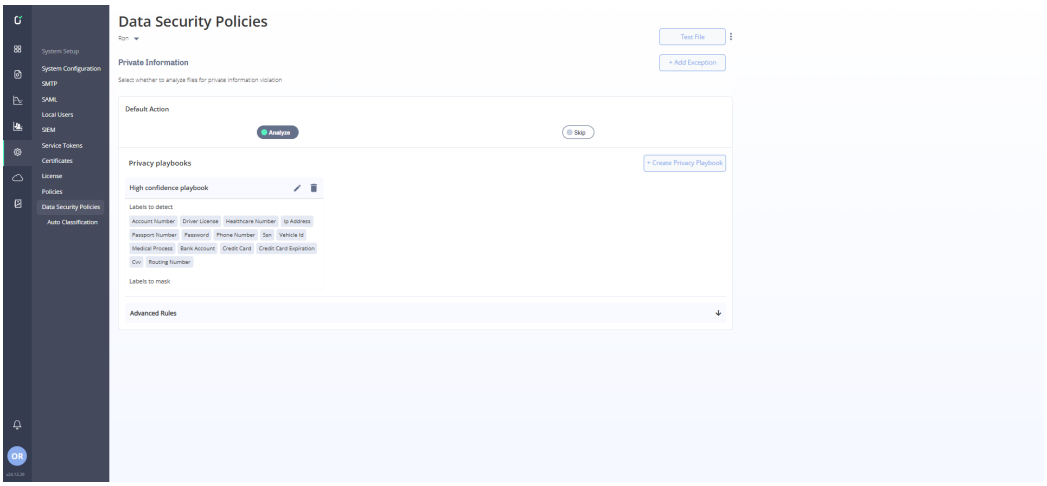
2.15 DDR Granular Policy Control

2.15.1 Overview

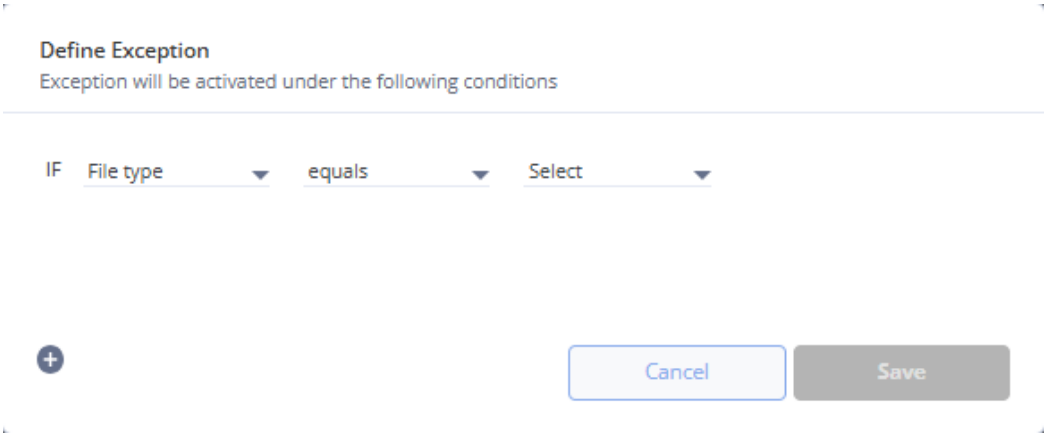
Votiro's DDR product provides granular policy controls to prevent sensitive data leaks. These controls sanitize files in real-time according to organization data privacy policies that are applied to employees and departments. This ensures proactive data protection while enabling safe file sharing.

2.15.2 Procedure

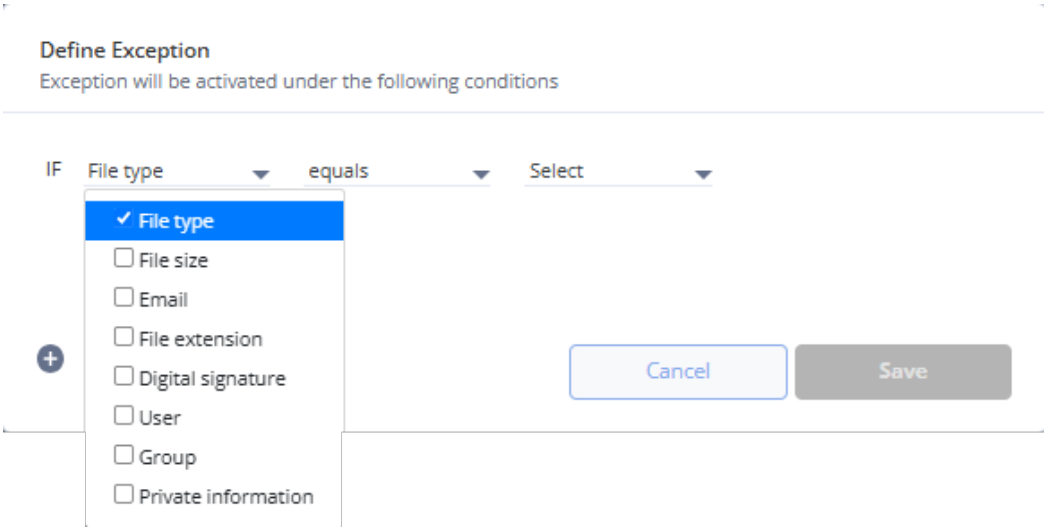
1. In the Management Console, navigate to **System setup** > **Data Security Policies**.



2. Click on the **+ Add Exception** button. The **Define Exception** window opens:



3. Clicking on the first drop-down menu displays the possible options:



The following table displays the options available when adding exceptions.

> **Note**:
> Exceptions based on file type, file size, email, file extension and digital signature are described in Adding Policy Exceptions.

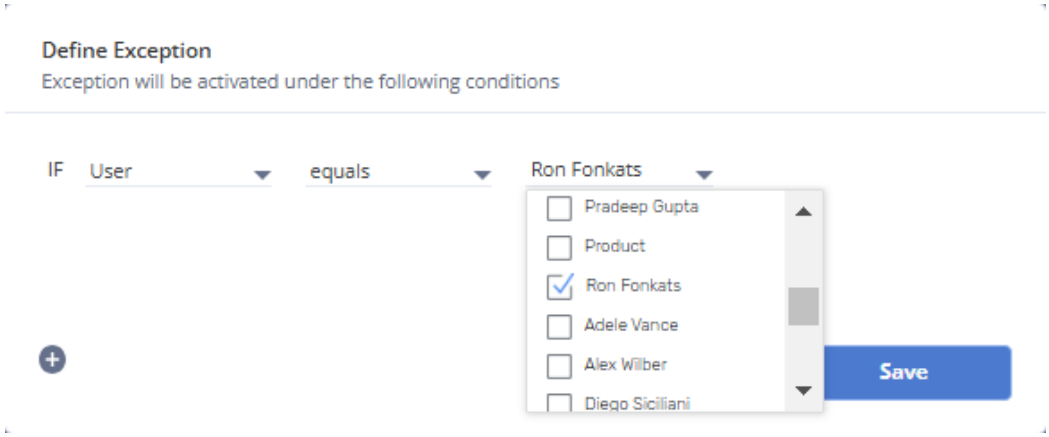
Option	Comparison Operators	Values
User	equals, not equals	*<user name>*
Group	equals, not equals	*<group name>*

> **Note**:
> Sanitization will be based on the defined policies and exceptions.
> For Office subscribers, the organization's users and groups will be listed in the dropdown menu for selection.

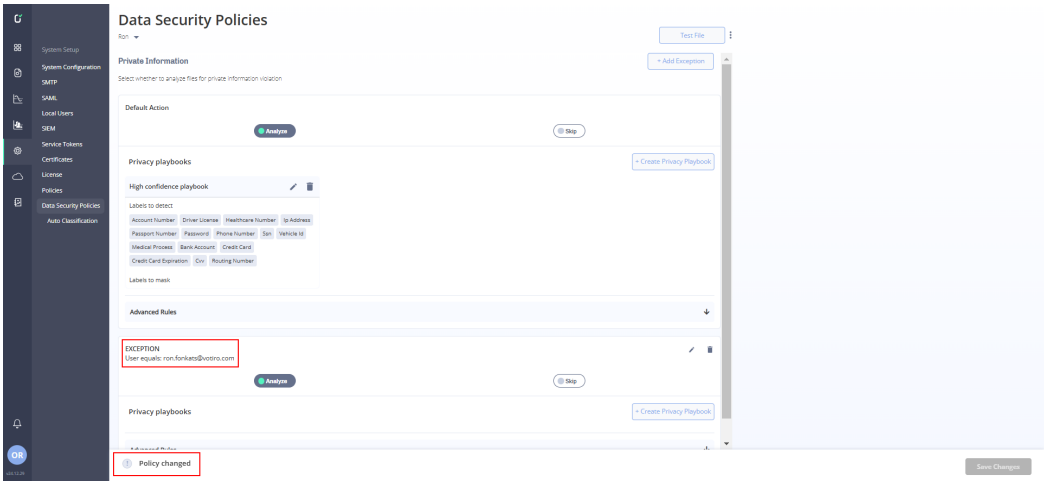
The following examples illustrate how to define exceptions.

Setting a policy for a user

1. Select **User** from the **IF** menu.
2. Select **equals** or **not equals** from the comparison operators menu.
3. Select the user from the **Select users** menu.

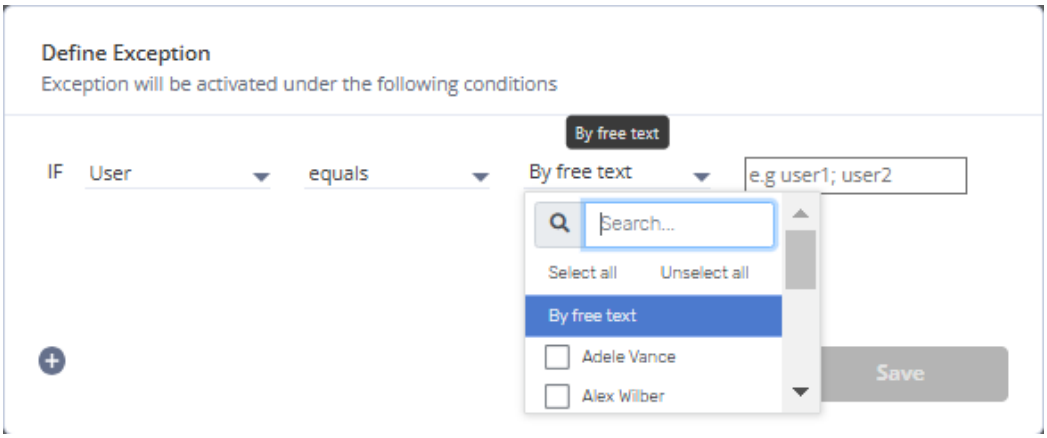


4. Click on the **Save** button.
5. The **Data Security Policies** page is updated:



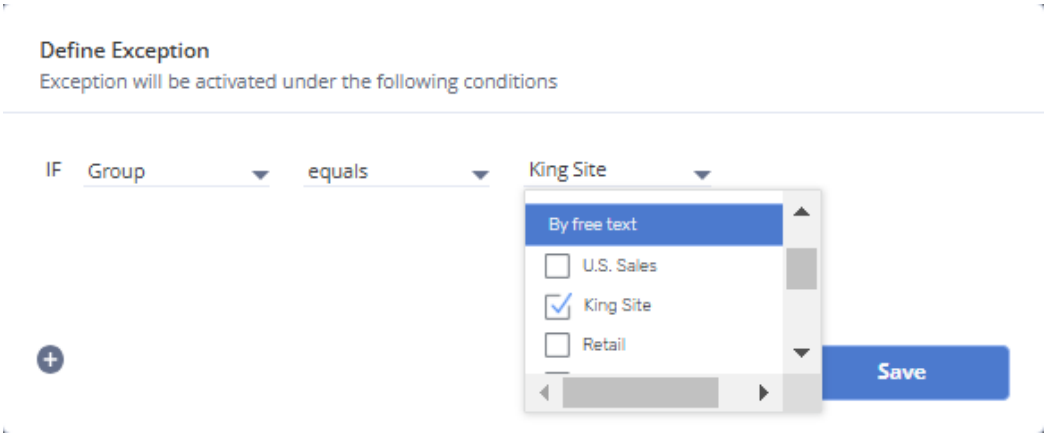
Note

There is also an option to add an exception by a free text for other integrations such as API, RBI, etc.:



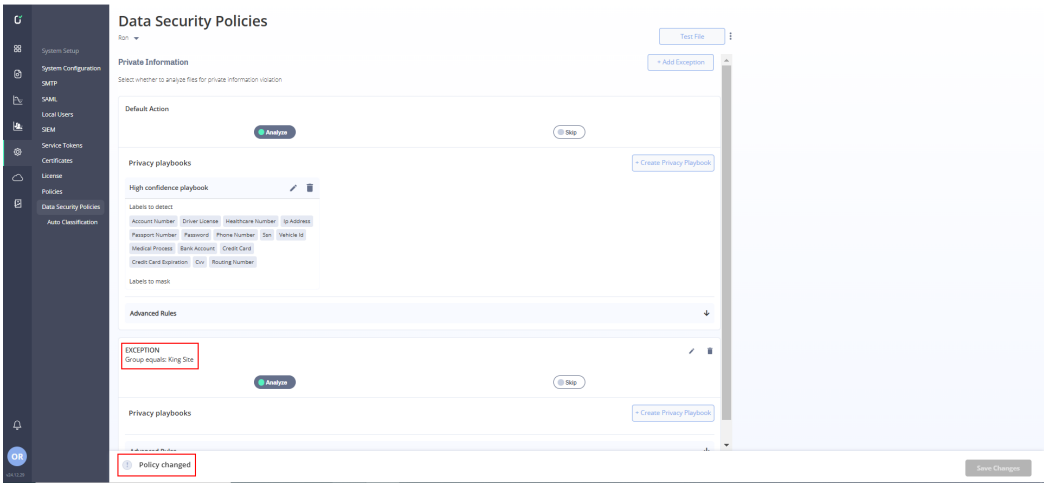
Setting a policy for a group

1. Select **Group** from the **IF** menu.
2. Select **equals** or **not equals** from the comparison operators menu.
3. Select the group from the **Select groups** menu.



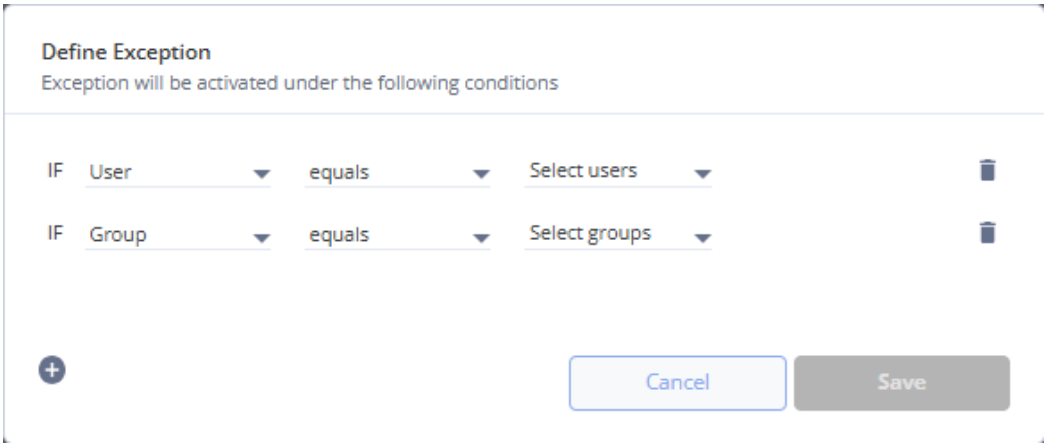
4. Click on the **Save** button.

5. The **Data Security Policies** page is updated:



Defining additional exceptions

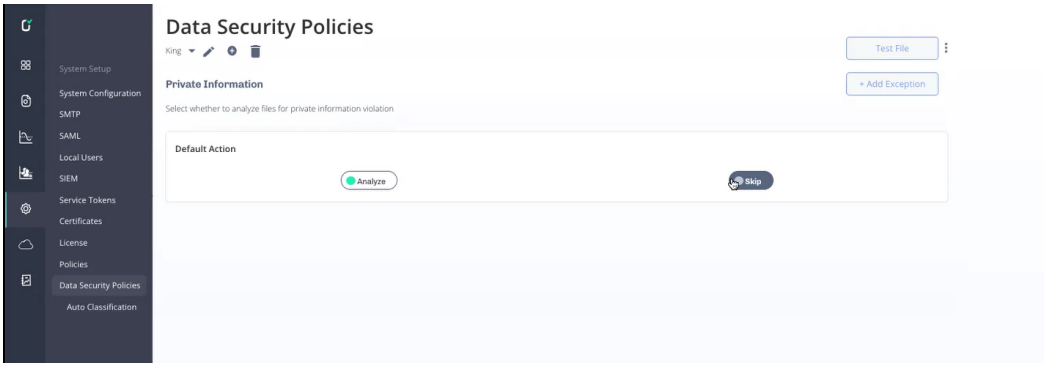
You may add additional exceptions by clicking on the ⊕ button in the **Define Exception** window:



2.16 Data Security Policies

Votiro detects privacy risks in data. If sensitive information like PII, PCI, or PHI is sent to unauthorized users, Votiro will detect and mask that data while it is in-motion, so the recipient receives anonymized data.

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



The Data Security Policies page contains the following fields:

Element	Field	Description
0	Private Information	Select whether to analyze files for private information violation. ■ **Analyze** - Analyze sensitive data. Selecting this option opens the Privacy Playbooks option. ■ **Skip** - Do not analyze sensitive data. This disables the Privacy Playbooks option.
1	Privacy Playbooks	This option is displayed if **Analyze** is selected in Private Information.

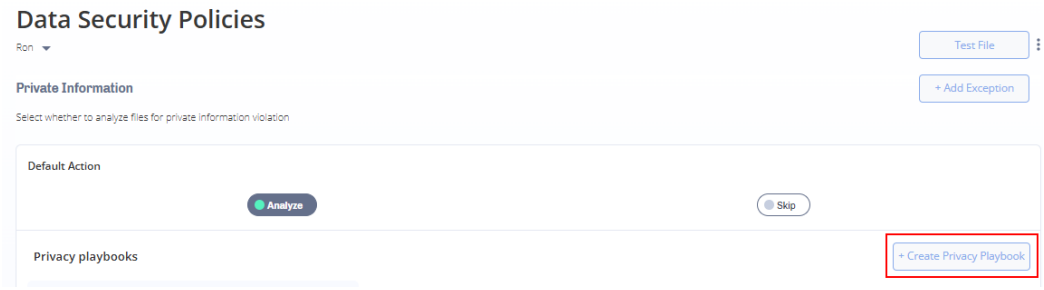
2.16.1 Privacy Playbooks

You can determine what sensitive data to detect and mask by creating a Privacy Playbook. You can create a Privacy Playbook using the wizard.

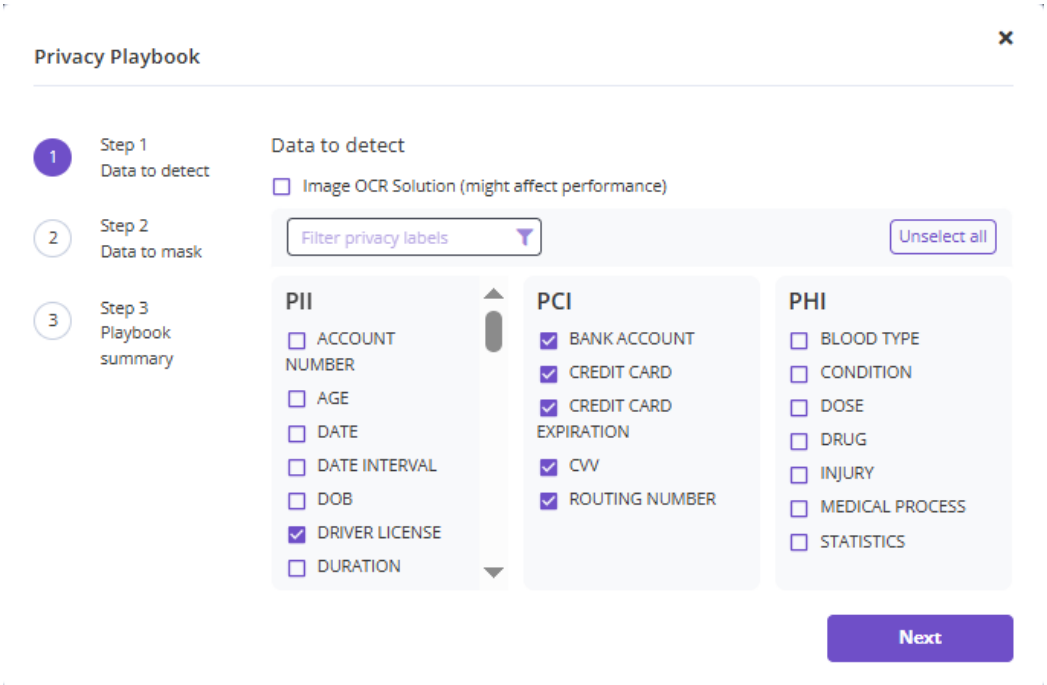
Creating a Privacy Playbook using the wizard

To create a Privacy Playbook:

1. In **Private Information**, click on **Analyze**.
2. In Privacy Playbooks, click on **+ Create Privacy Playbook**.

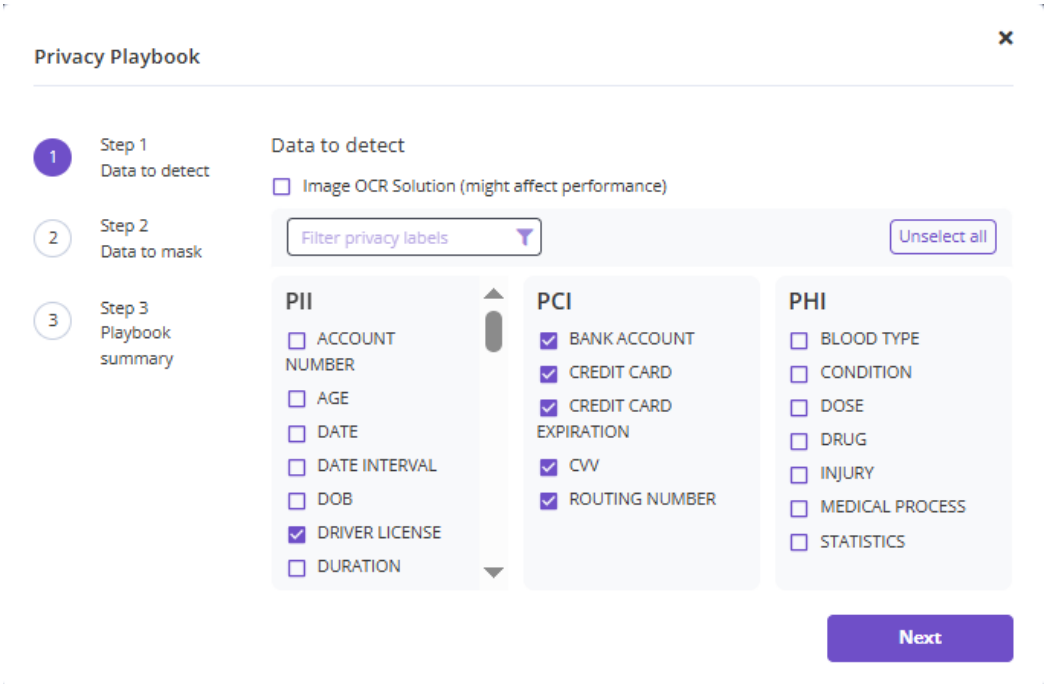


3. The Privacy Playbook window opens:



4. Select the data to detect from the available options. There are three types of data:

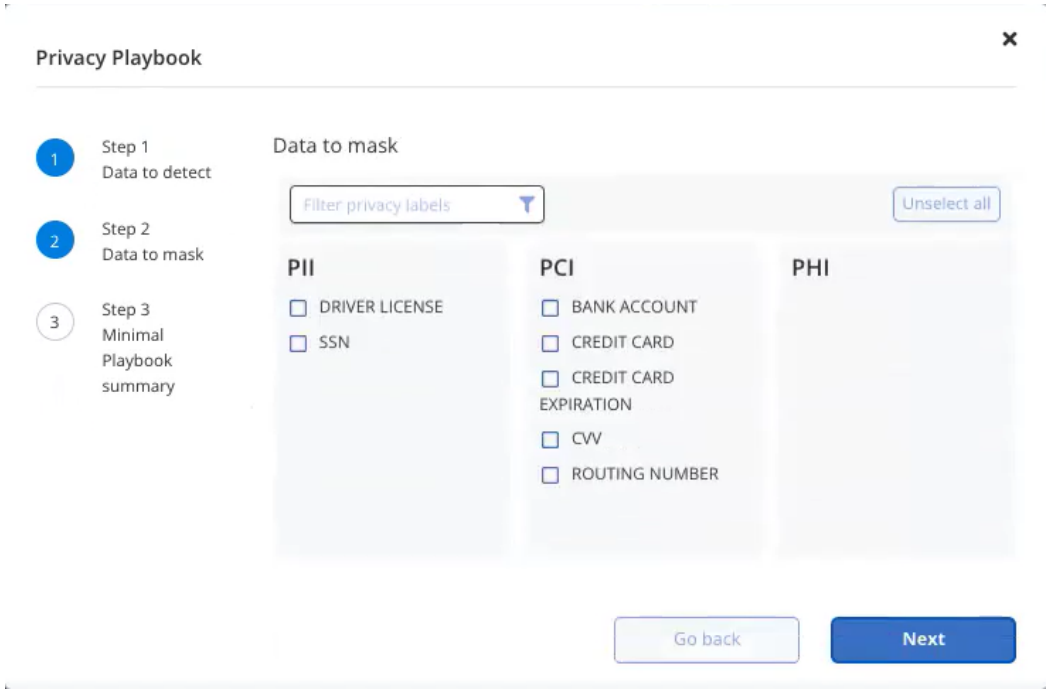
- **PII** - Personally Identifiable Information (PII) is any information connected to a specific individual that can be used to uncover that individual's identity, such as their social security number, full name, email address or phone number.
- **PCI** - Payment Card Industry (PCI) data includes payment card processing data such as bank account number or credit card credentials.
- **PHI** - Protected Health Information (PHI) is any information in the medical record or designated record set that can be used to identify an individual, such as blood type, for example.



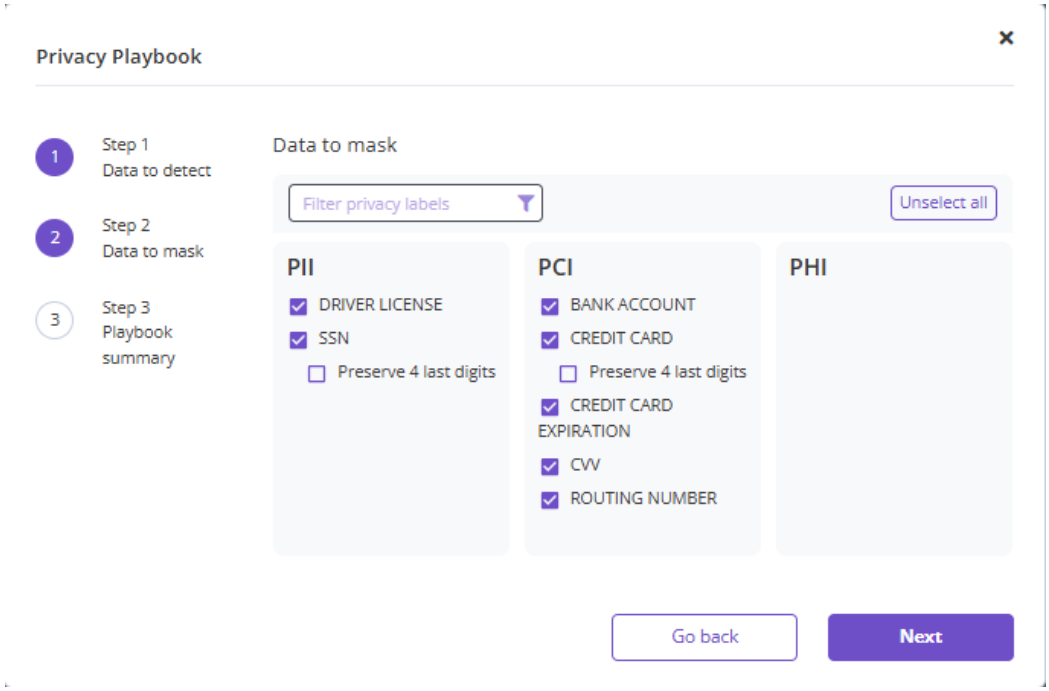
5. Optionally, select **Image OCR Solution** if you wish to use optical character recognition to detect the selected data from a snapshot of the file containing the data. Currently, this option is available only for images within pdf files. Note that this option may affect performance.

6. You may use the **Filter privacy labels** box to search for selected data items.

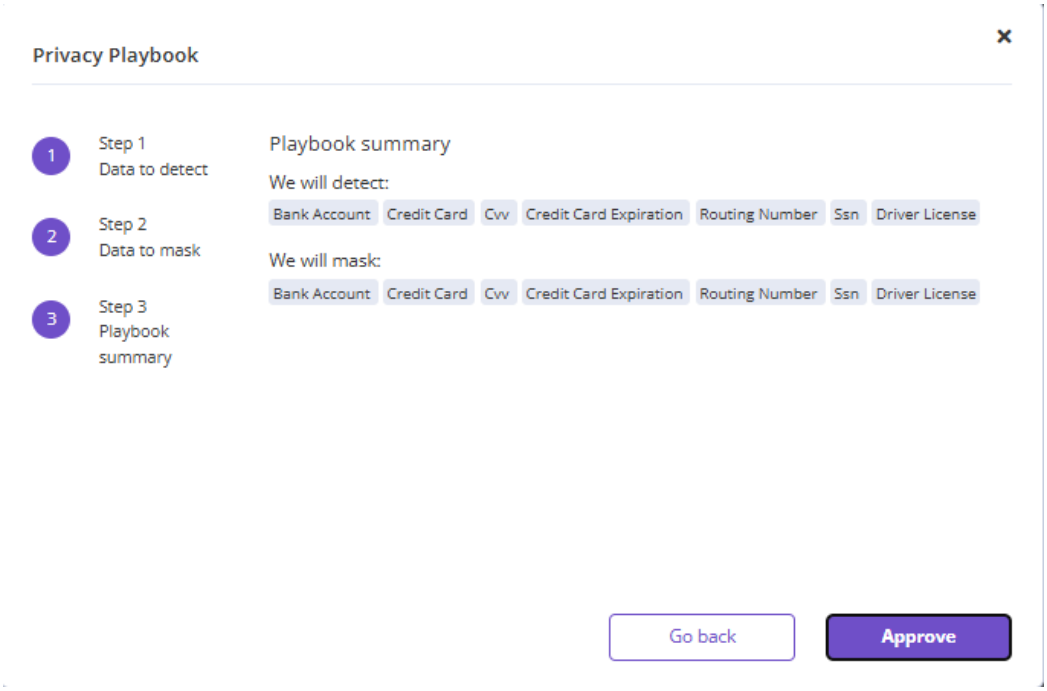
7. After selecting the data to detect, click **Next**. The Privacy Playbook wizard advances to **Step 2 Data to mask**. For example:



8. Select which data will be masked (not displayed) in the output report. Note that there is an option to partially mask some data items such as SSN or credit card number. For example:

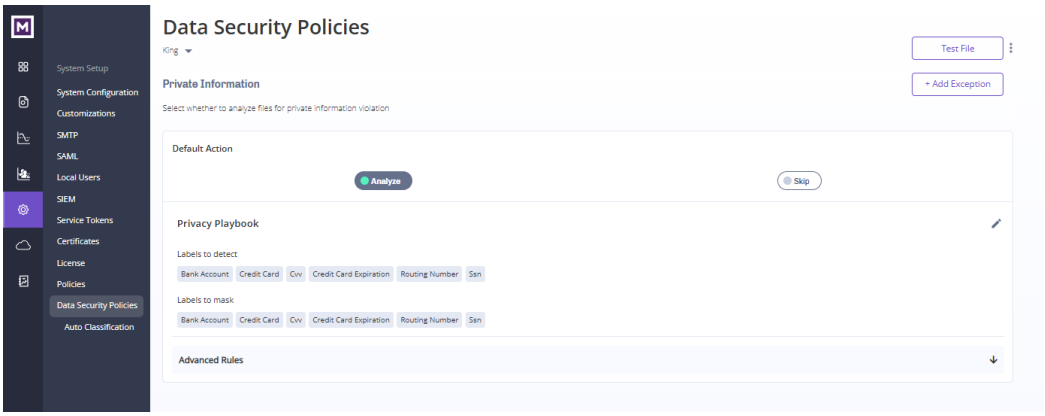


9. After selecting the data to mask, click **Next**. The Privacy Playbook wizard advances to **Step 3 Playbook Summary**.



10. The Playbook Summary displays the data to detect at the selected minimal level of confidence and the data to mask. To accept the displayed data values and criteria, click **Approve**. To modify, click **Go back**.

11. After approving the Playbook, the Playbook is displayed in the Data Security Policies dashboard:



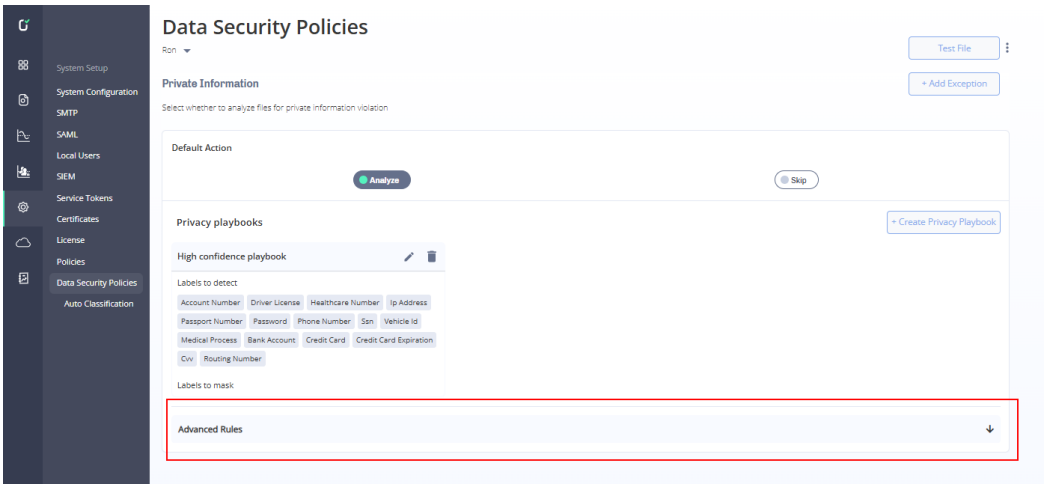
12. You may use the edit or delete icons to modify or delete a Playbook.

2.16.2 DDR Advanced Rules

You can build custom policy rules based on Regular Expressions (Regex) patterns according to the organization's unique identifiers. Votiro's engine will detect the unique identifiers and will mask the data according to policy.

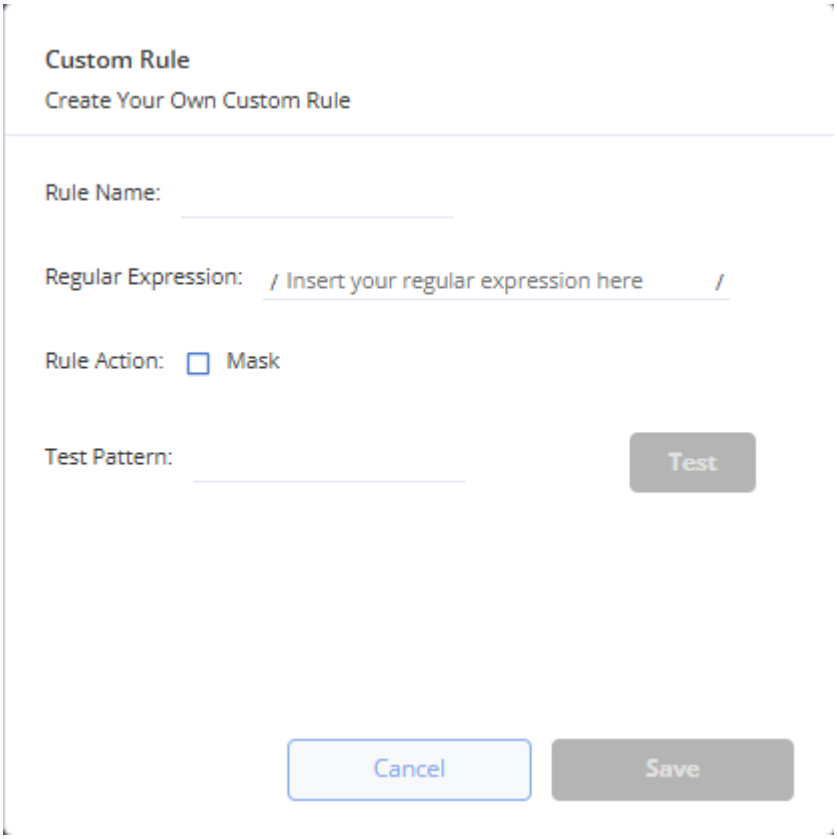
To create a custom rule:

1. From the navigation pane on the left, click **Settings** > **Data Security Policies**.



2. Click on **Advanced Rules**.

3. Click on the **+ Create Custom Rule** button. The **Custom Rule** window opens:



4. Enter the fields in the **Custom Rule** window:

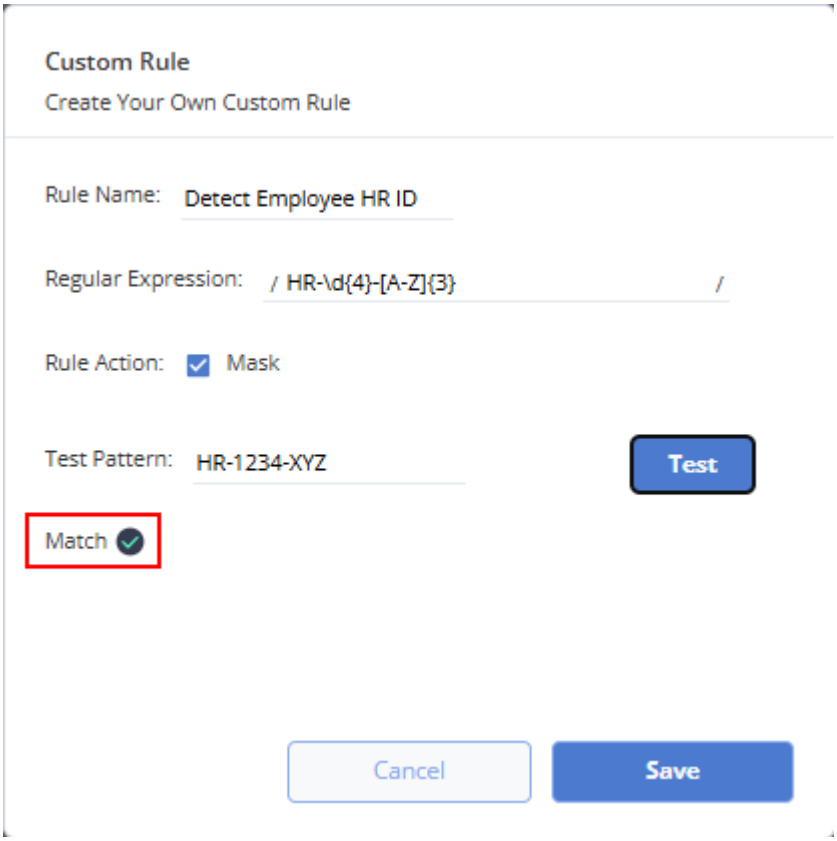
a. For **Rule Name**, enter appropriate text.

b. For **Regular Expression**, enter a regex pattern.

c. For **Rule Action**, to mask the detected pattern, check the **Mask** box.

d. Enter the **Test Pattern**.

e. To test the regex pattern vs the test pattern, click on **Test**. For example:

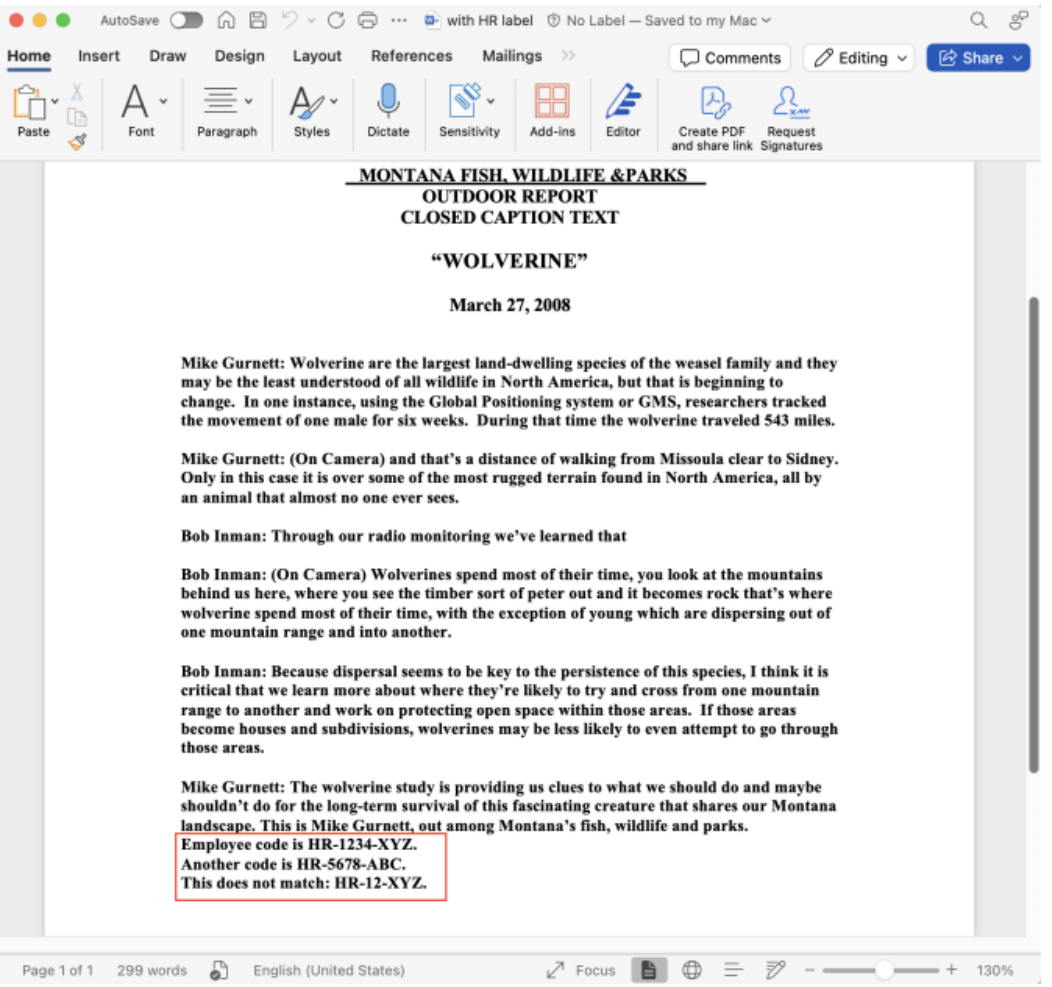


f. If a **Match** is displayed as in the above example, click on **Save** to save the rule. The new rule is displayed on the **Data Security Policies** page:

g. To modify the rule, click on the edit icon. To delete the rule, click on the delete icon.

5. After setting the desired custom rules, the document content will be scanned and actions taken accordingly.

a. For example, the original document without masking is displayed:



MONTANA FISH, WILDLIFE &PARKS
OUTDOOR REPORT
CLOSED CAPTION TEXT

"WOLVERINE"

March 27, 2008

Mike Gurnett: Wolverine are the largest land-dwelling species of the weasel family and they may be the least understood of all wildlife in North America, but that is beginning to change. In one instance, using the Global Positioning system or GMS, researchers tracked the movement of one male for six weeks. During that time the wolverine traveled 543 miles.

Mike Gurnett: (On Camera) and that's a distance of walking from Missoula clear to Sidney. Only in this case it is over some of the most rugged terrain found in North America, all by an animal that almost no one ever sees.

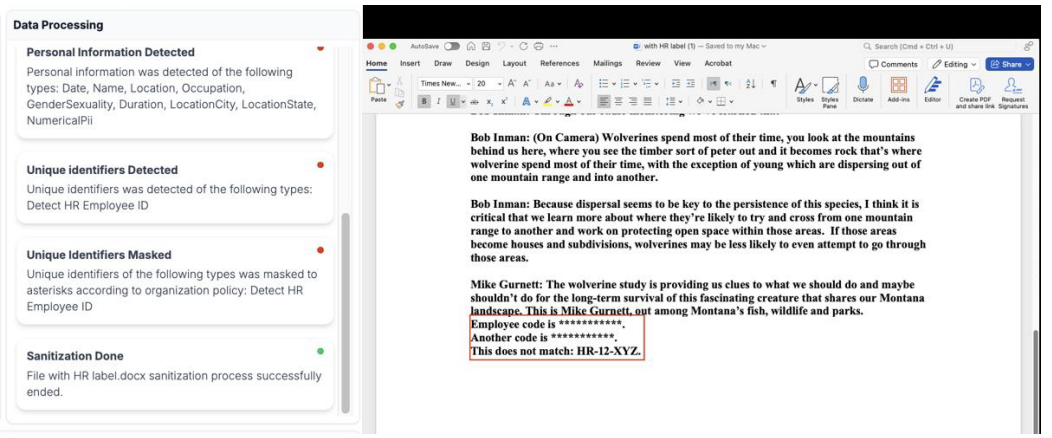
Bob Inman: Through our radio monitoring we've learned that

Bob Inman: (On Camera) Wolverines spend most of their time, you look at the mountains behind us here, where you see the timber sort of peter out and it becomes rock that's where wolverine spend most of their time, with the exception of young which are dispersing out of one mountain range and into another.

Bob Inman: Because dispersal seems to be key to the persistence of this species, I think it is critical that we learn more about where they're likely to try and cross from one mountain range to another and work on protecting open space within those areas. If those areas become houses and subdivisions, wolverines may be less likely to even attempt to go through those areas.

Mike Gurnett: The wolverine study is providing us clues to what we should do and maybe shouldn't do for the long-term survival of this fascinating creature that shares our Montana landscape. This is Mike Gurnett, out among Montana's fish, wildlife and parks.
Employee code is HR-1234-XYZ.
Another code is HR-5678-ABC.
This does not match: HR-12-XYZ.

b. In the sanitized version, the test pattern and relevant data field are masked:



2.16.3 DDR Auto-Classification

Votiro's Auto-Classification solution is based on Microsoft Purview Sensitive Labels. Integrating Votiro DDR and Microsoft Purview Sensitive Labels creates a comprehensive data protection and compliance solution that leverages the strengths of both platforms. The admin can create Microsoft Sensitivity labels and set desired Votiro DDR policies to perform auto-classification based on a document's sensitive data.

2.16.4 Key Capabilities

- **Content Inspection** - Automatically scans and analyzes files, emails, and other content for sensitive information.
- **Policy-Driven Labeling** - Administrators define policies to specify when and how labels should be applied.

  For example:

  - Apply a "Confidential" label if a document contains a credit card number.
  - Apply a "Highly Confidential" label if the file contains sensitive legal or healthcare terms.
- **Real-Time Auto-Classification** - Automatically applies labels as content is created, modified, or shared within Microsoft 365 apps like Word, Excel, and Outlook. Ensures that sensitive content is secured immediately upon detection.

2.16.5 Benefits of Automatic Labeling

- **Efficiency** - Reduces the burden on employees to manually label content, ensuring consistent application of policies.
- **Accuracy** - Minimizes errors and oversights, improving the reliability of data classification and protection.
- **Compliance**- Helps meet regulatory requirements by automating data protection and classification processes.
- **Scalability** - Enables large organizations to apply data governance at scale without manual intervention.

2.16.6 Prerequisites

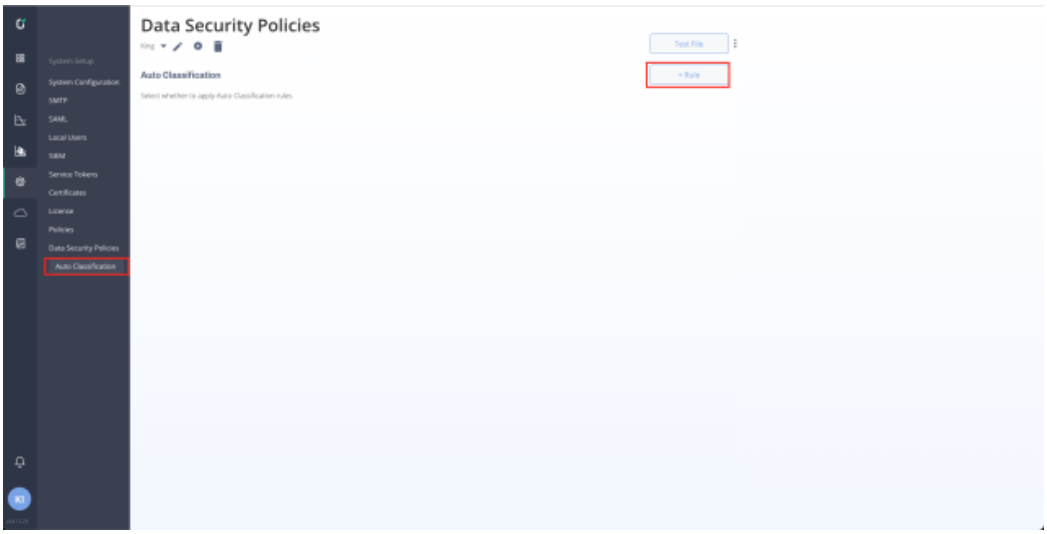
Microsoft Purview sensitivity labels are available to use.

To learn how to create Microsoft sensitivity labels, see Create and configure sensitivity labels and their policies.

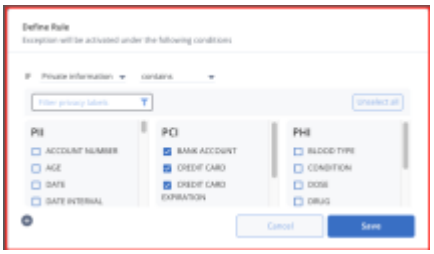
> **Note**:
> If masking is enabled, Auto-Classification will be applied after masking is implemented.

2.16.7 Procedure

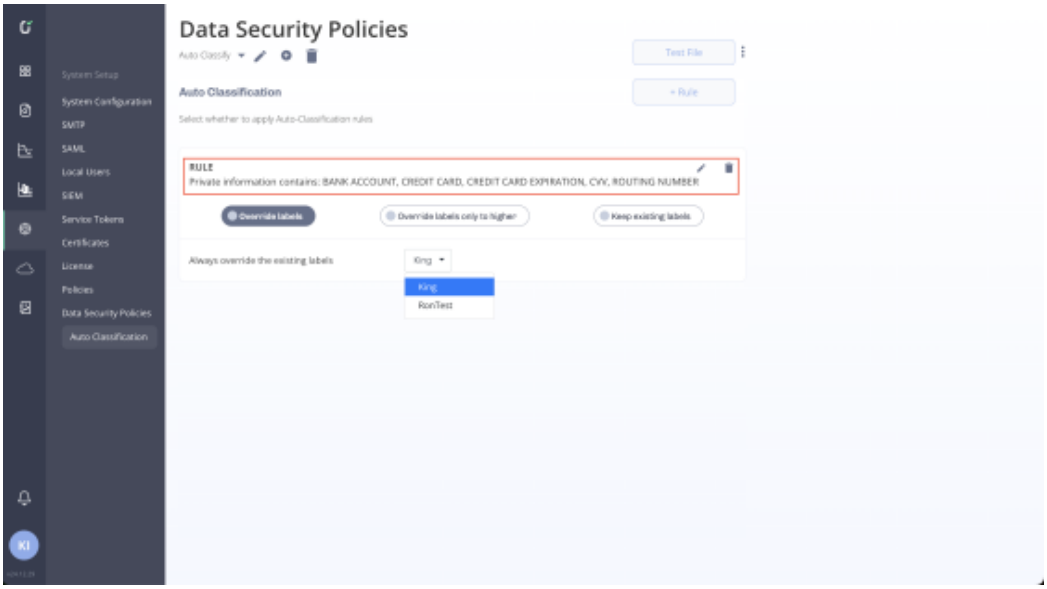
1. From the navigation pane on the left, click **Settings** > **Auto Classification**.



2. Click on **+ Rule** to create a new rule. The **Define Rule** window opens:

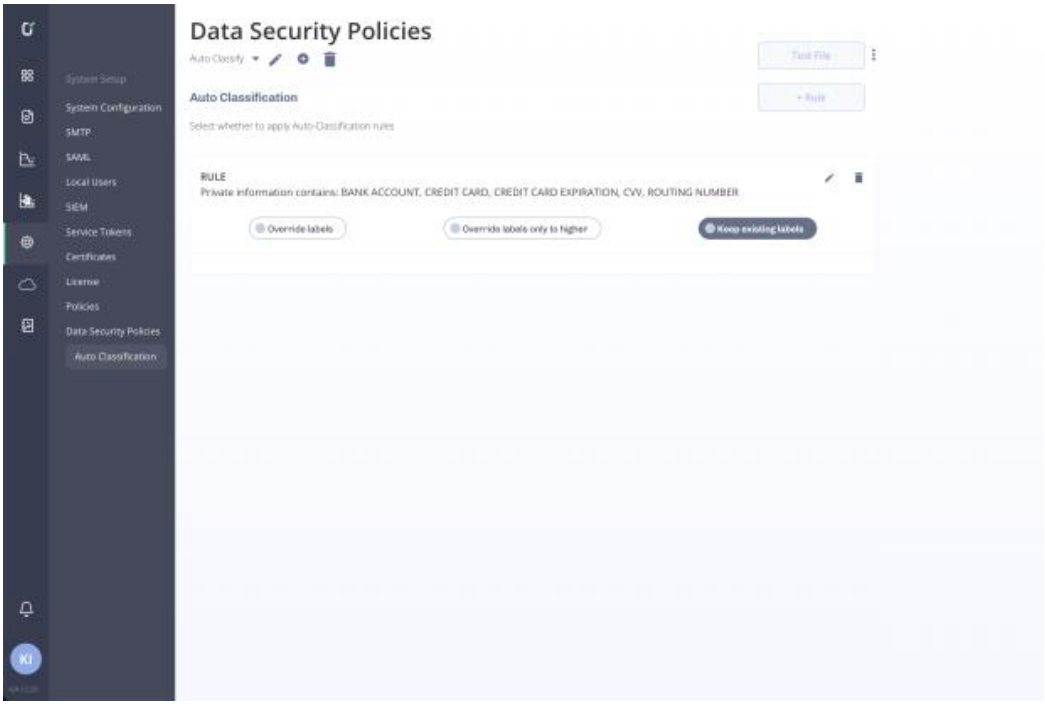


3. Select the desired data labels and click on **Save**. The new rule is displayed on the Auto Classification page:



4. After creating a rule, select one of the three policy actions to apply:

- **Keep existing labels** - This is the default. Votiro will analyze the existing label only, without modification. This action is equivalent to “Only Analyze” mode.



- **Override labels only to higher** - Votiro will analyze the existing label and will override the label only if the sensitive content matches a higher priority level. The user will be able to choose which label to set in this case.

> **Note**:
> Priority is set on Microsoft sensitivity labels.
> Behavior will be the same for files without labels.

For example:

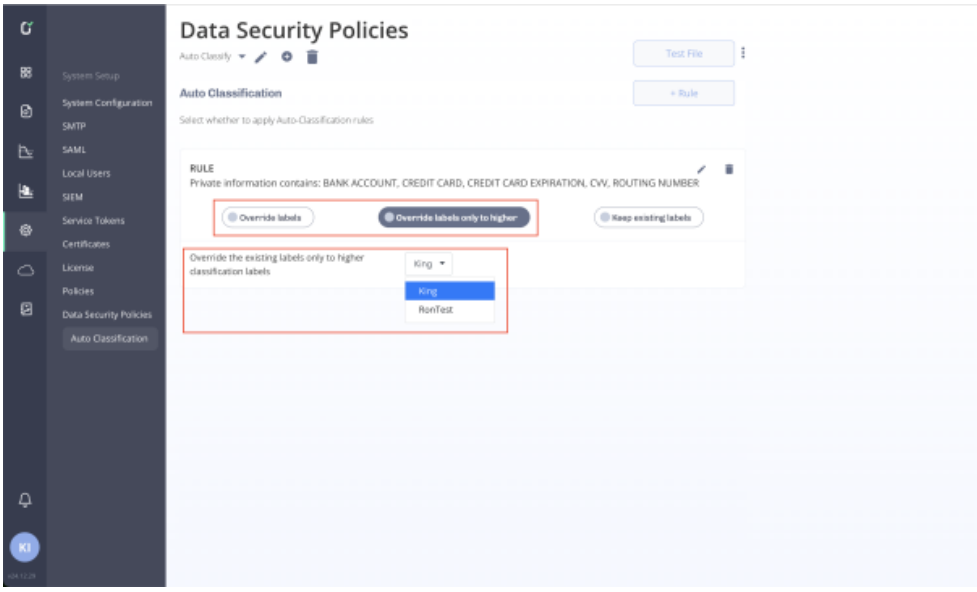
i. There are two available labels:
   - Confidential – Priority 1 (Low)
   - Highly Confidential – Priority 2 (Higher)

ii. The user labels the file as Confidential.

iii. The file is sent by email/other Microsoft Apps (OneDrive, SharePoint, Teams).

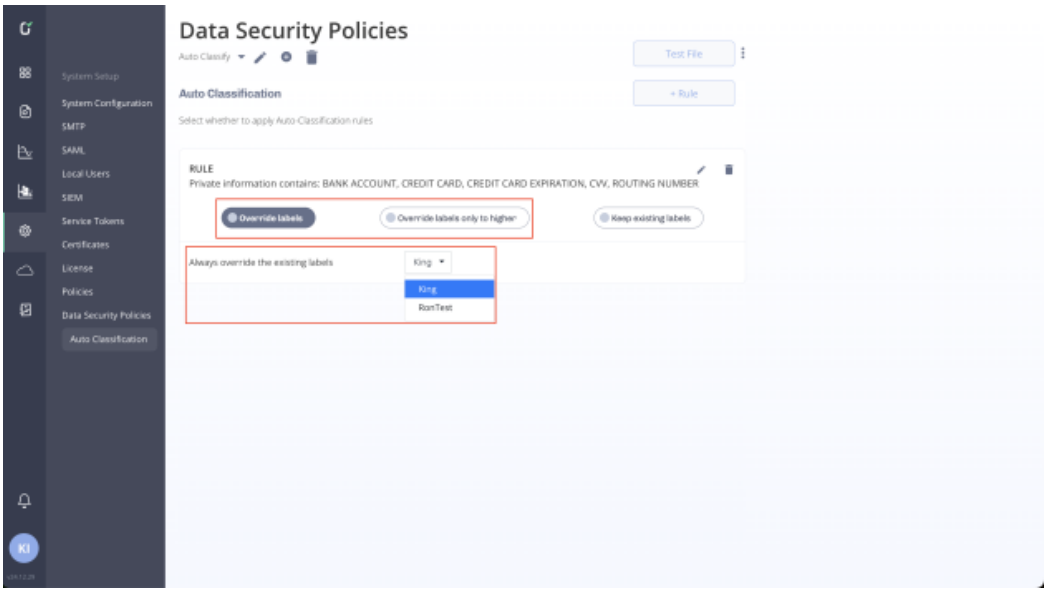
iv. Votiro analyzes the file-sensitive content and detects that the content matches the Highly Confidential label.

v. Votiro auto-classifies the file with a Highly Confidential label.



- **Override labels** - Votiro will analyze the existing label and will always override to the desired label.

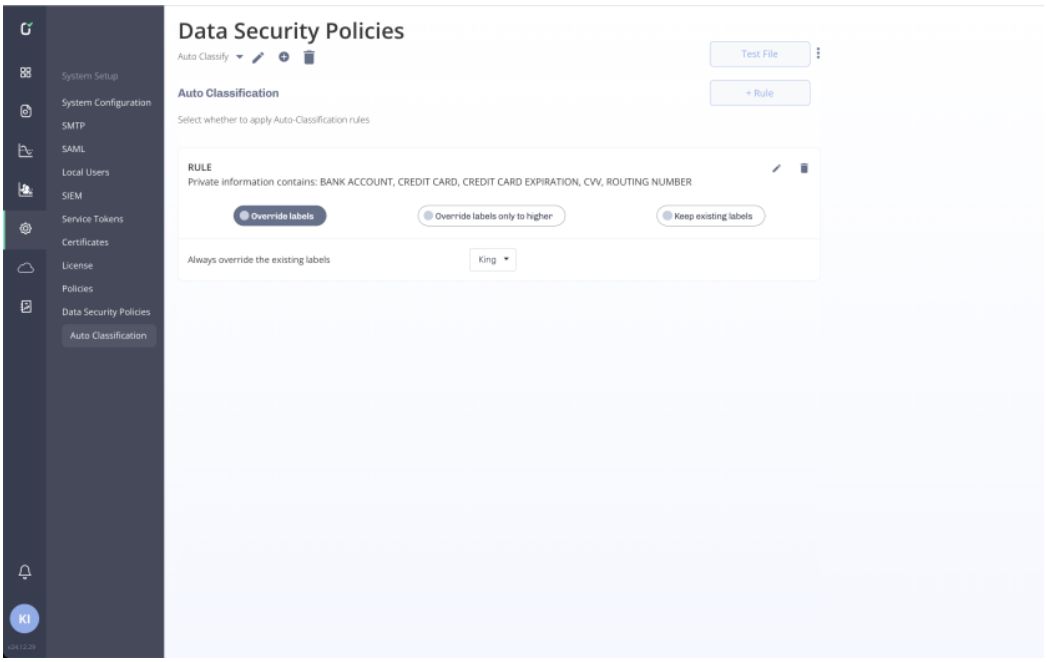
> **Note**:
> Behavior will be the same for files without labels.



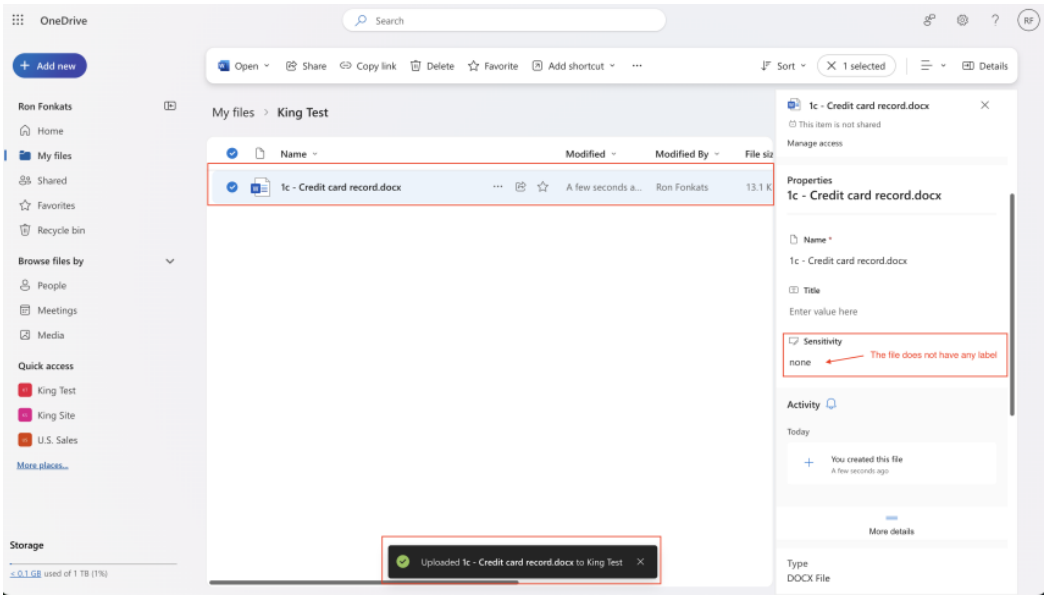
2.16.8 E2E Workflow

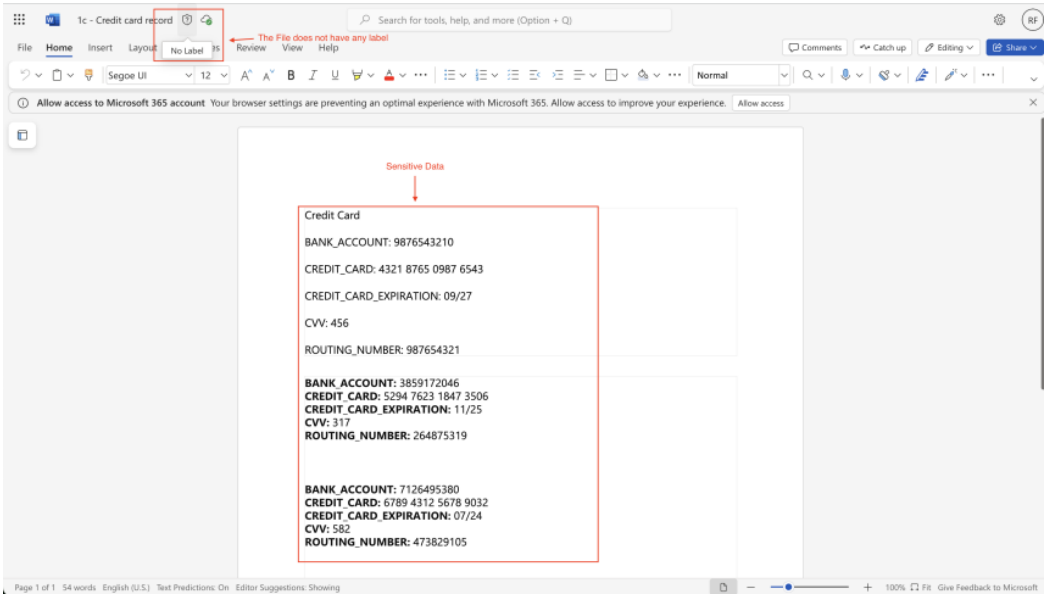
The following example illustrates a Votiro Auto-Classification use case of users uploading files to OneDrive without sensitive labels.

1. The administrator configures the Auto-Classification rule.

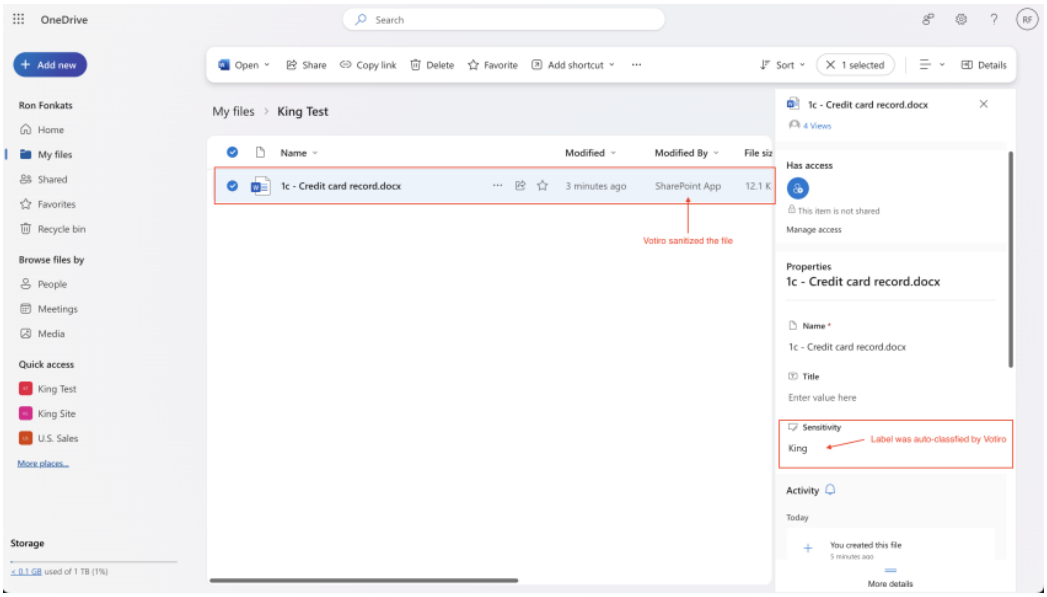


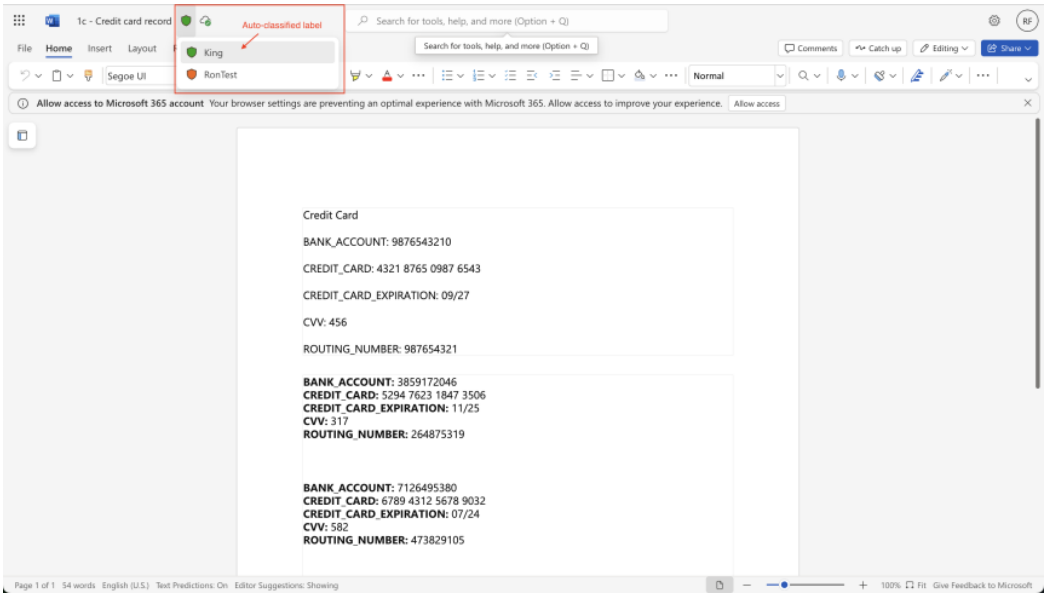
2. A user uploads a file to OneDrive. The file does not have any label, and the file contains sensitive data.



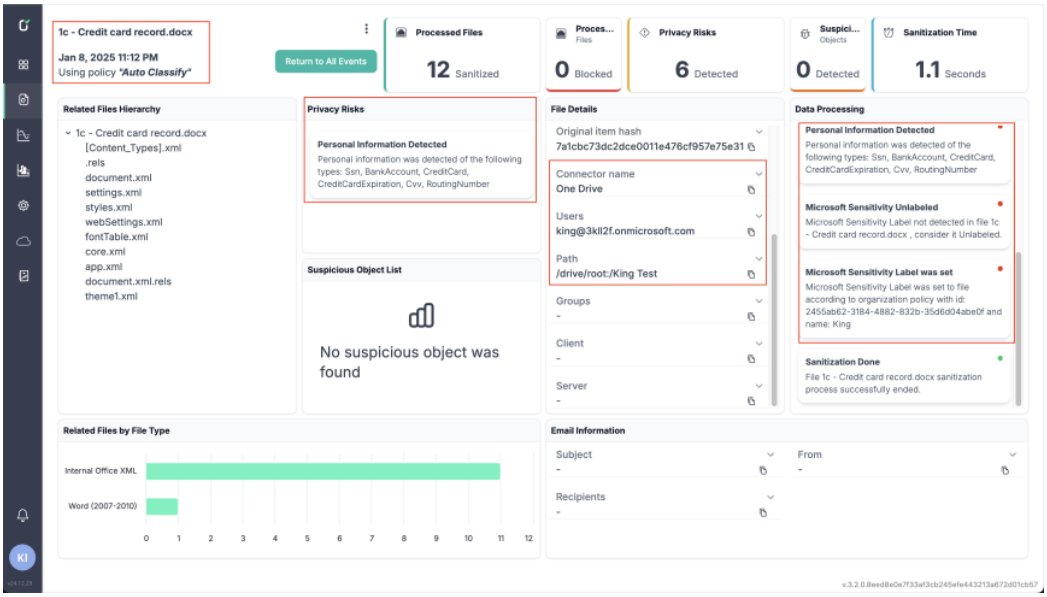


3. Votiro sanitizes the file and auto-classifies the file based on the detected sensitive data and matched rules.



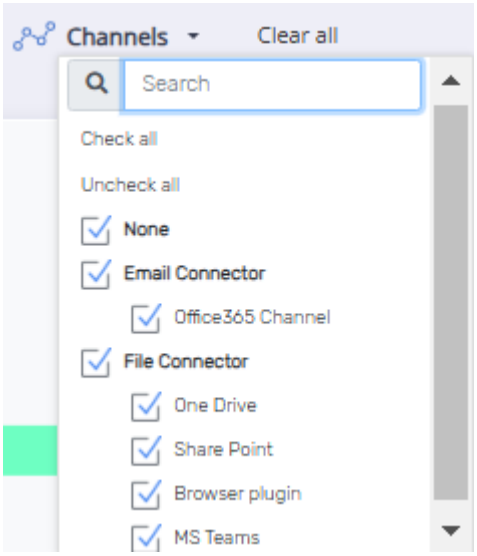


4. Votiro Analytics are available on the **Events** page:



2.16.9 Filter by Channels

The statistics displayed in the DDR dashboards relate to the file and email connectors that are currently selected. If you have more than one connected integration installed, you can filter the file list by Connector using the **Channels** list.

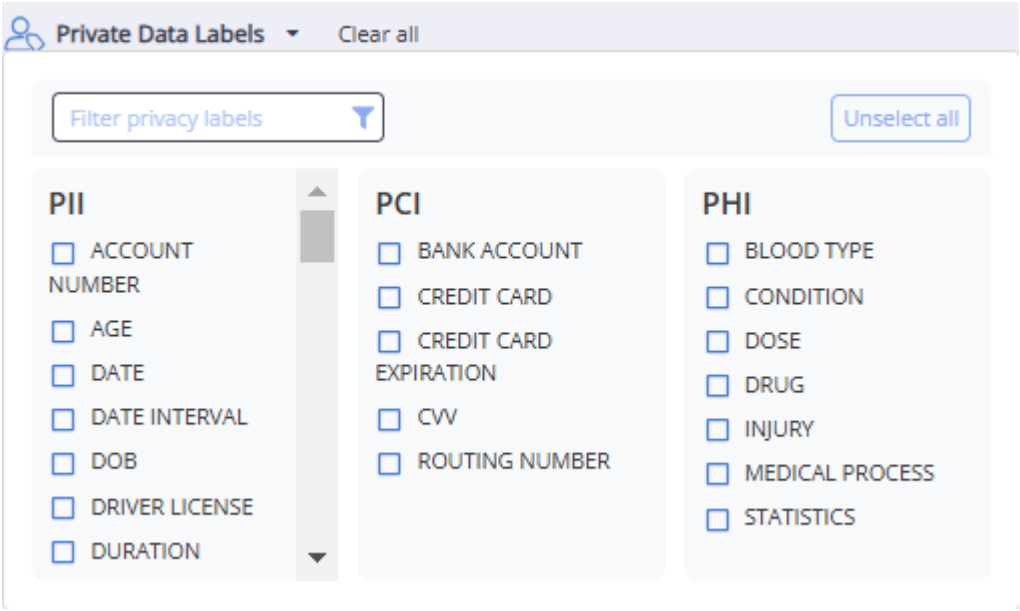


1. To display statistics for specific connectors, click on **Channels**.
2. Check the box next to each desired connector.
3. To include test files, check the **None** box.
4. To select all available connectors, click on **Check all**. To clear all the selections, click on **Uncheck all**.

Statistics update to show information for the selected Channels.

2.16.10 Filter by Private Data Labels

The statistics displayed on the **Privacy and Compliance** dashboard can be filtered by the **Private Data Labels** that are currently selected for each private data type selected.



Select one or more of the **Private Data Labels** by checking the appropriate boxes in each **Private Data Type** category :

- PII - Personally Identifiable Information (PII) is any information connected to a specific individual that can be used to uncover that individual's identity. See Table 1 PII data labels for a detailed list of PII data labels.
- PHI - Protected Health Information (PHI) is any information in the medical record or designated record set that can be used to identify an individual. See Table 2 PHI data labels for a detailed list of PHI data labels.
- PCI - Payment Card Industry (PCI) data apply to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. See Table 3 PCI data labels for a detailed list of PCI data labels.

Use **Filter privacy labels** to filter the list for a specific data label. For example, to see if SSN was checked:

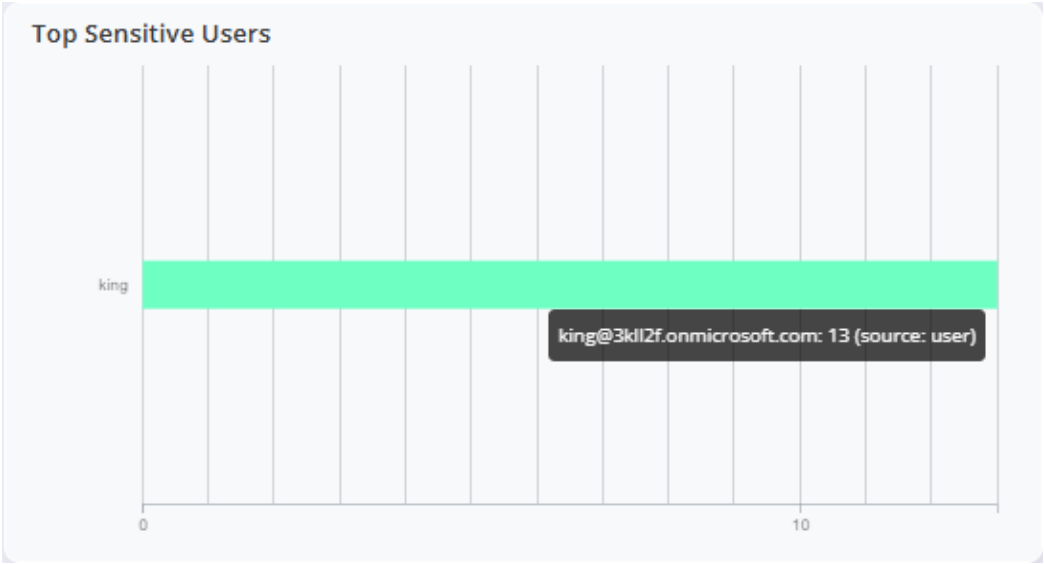
To uncheck all selected private data labels for all private data types, click on **Unselect all**.

Filtering by Private Data Labels in the Privacy and Compliance Dashboard

To filter the view by specific data labels, use **Filter privacy labels** to search for and filter the list for the desired data label. For example, to view only sensitive files containing SSN:

1. In **Private Data Labels**, click on **Unselect all**.
2. Enter the desired private data label in the **Filter privacy labels** box. For example, ssn.
3. Check the box next to the desired privacy data label. For example, SSN.

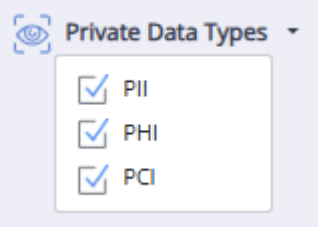
4. Click on the desired pane in the **Privacy and Compliance** dashboard, for example, the **Top Sensitive Users** pane. The statistics are updated to reflect the new selected data.



5. The **Private Data Labels** are updated to show the filtered selection:

2.16.11 Filter by Private Data Types

The statistics displayed on the **Privacy and Compliance** dashboard can be filtered by the **Private Data Types** that are currently selected.



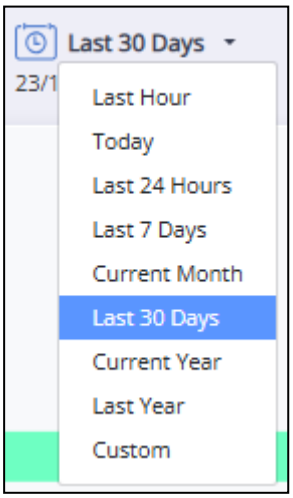
Select one or more of the private data types by checking the appropriate boxes:

- **PII** - Personally Identifiable Information (PII) is any information connected to a specific individual that can be used to uncover that individual's identity. Examples include account number, driver license, email address, name, username, password, phone number, SSN, etc.
- **PHI** - Protected Health Information (PHI) is any information in the medical record or designated record set that can be used to identify an individual. Examples include blood type, condition, dose, etc.
- **PCI** - Payment Card Industry (PCI) data apply to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. Examples include bank account, credit card, routing number, etc.

2.16.12 Filter by Time Period

The statistics displayed in the DDR dashboards relate to the time period that is currently selected.

You can select a predefined time period by clicking its button or define a custom period.

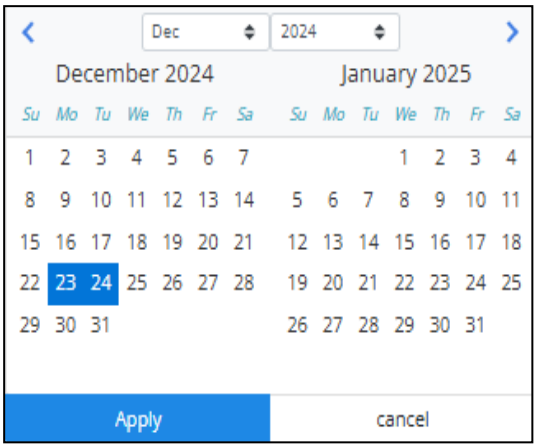


Votiro provides the following predefined settings:

Period of Processing Activity	Meaning
Last Hour	The information is for the period starting 60 minutes earlier until the current time. The time interval displayed is by minute.
Today	The information is for the period starting from 00:00 of the current day until the current time. The time interval displayed is by hour.
Last 24 Hours	The information is for the period starting from the beginning of the current time, 24 hours earlier, until the current time. The time interval displayed is by hour.
Last 7 Days	The information is for the period starting from the beginning of the current time, seven days earlier, until the current time. The time interval displayed is by day.
Current Month	The information is for the period starting from 00:00 of the first day of the current month until the current time. The time interval displayed is by day.
Last 30 Days	The information is for the period starting from the current time, one month earlier, until the current time. The time interval displayed is by day.
Current year	The information is for the period starting from 00:00 of the first day of the current year until the current time. The time interval displayed is by month.
Last Year	The information is for the period starting from the beginning of the current time, one year earlier, until the current time. The time interval displayed is by month.
Custom	Allows you to define the period to display information for by selecting from and to dates from a calendar selection tool.

Defining a Custom Period

1. Click **Custom** to display the period selector.

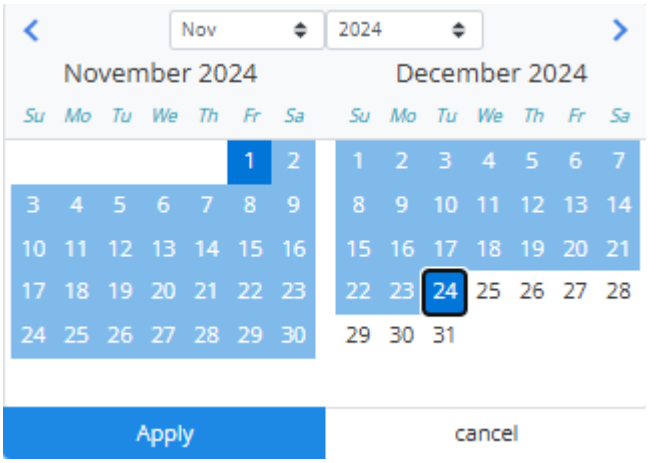


2. Navigate to the desired start month and year by clicking the blue right (>) and left (<) arrows, or by selecting a month and year using the up (^) and down (ˇ) arrows.

3. To select a start date, tap a date on the calendar, the number turns blue.

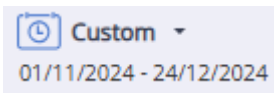
4. To select an end date, tap a date on the calendar, the number turns blue.

   The selected period is highlighted.



5. Click **Apply**.

   The custom period is displayed in the top left corner of the window:



   Statistics update to show information for the custom period.

2.16.13 Operational workflow

The operational workflow is to filter the dashboard by the filters option, and then perform drill down to see related events details.

The charts displayed in the **Privacy and Compliance** and **Monitor** dashboards can be filtered to fine tune the statistics further. Drilling down is performed to:

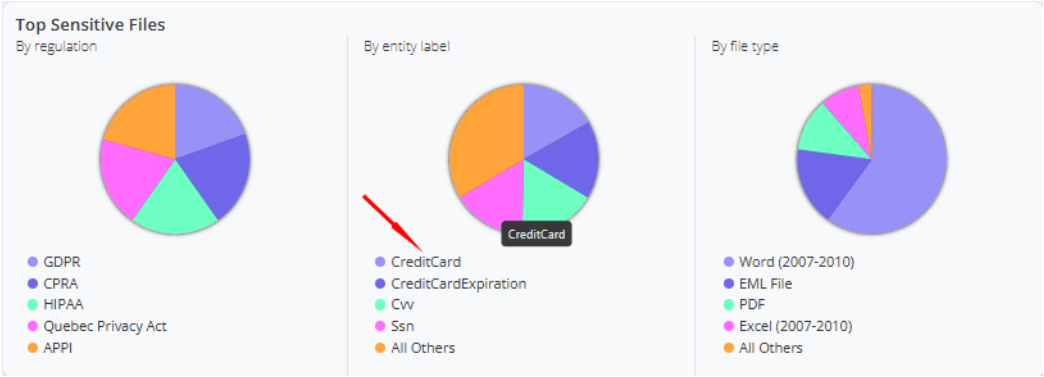
- Filter the display to add/remove data to/from charts
- View the number of files in a chart
- View more details of files or objects

2.16.14 Filtering the display

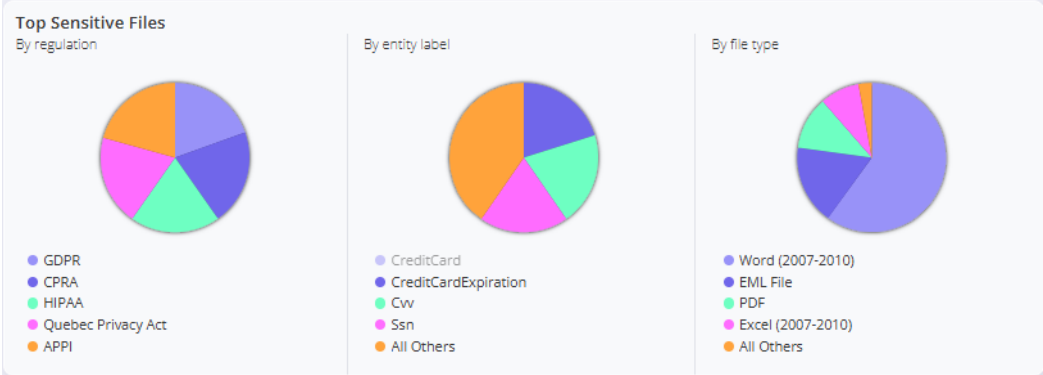
Filtering by removing categories from a chart

To remove a file category from the display:

1. Click on the file category in the chart legend. For example, to remove the CreditCard category from the chart, move the cursor over CreditCard and click.



2. The display is updated to remove the selected category from the chart and the category is grayed out in the chart legend.



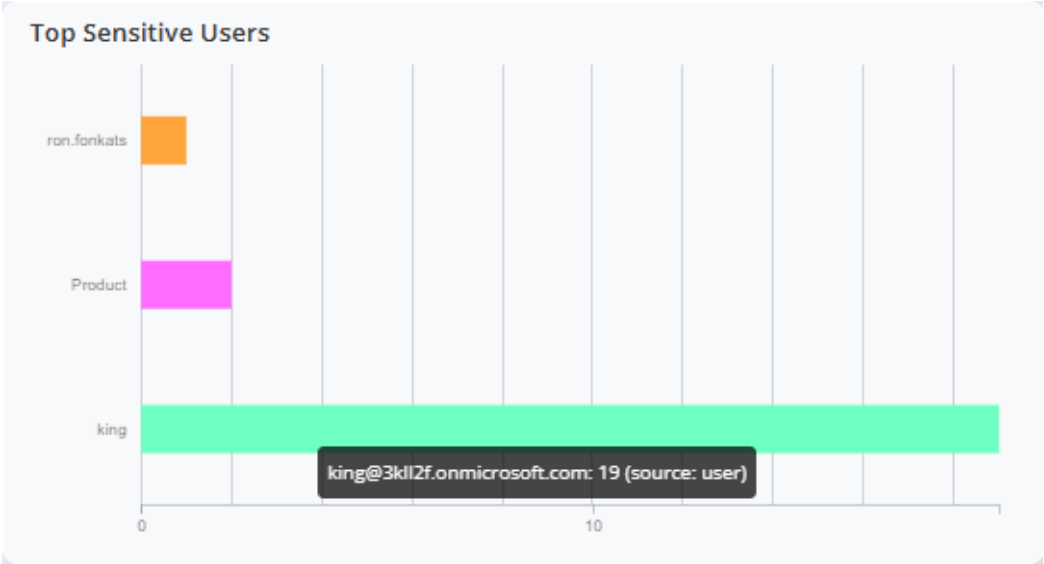
Filtering by restoring categories to a chart

To restore a category that was removed from the chart, click on the grayed-out category in the chart legend.

2.16.15 Viewing the number of files or objects

To view the number of files in a chart, move the cursor over the appropriate histogram in the chart.

For example, in the **Top Sensitive Users** chart, moving the cursor over the histogram representing the user "king" displays that there were 19 files identified as sensitive for that user:

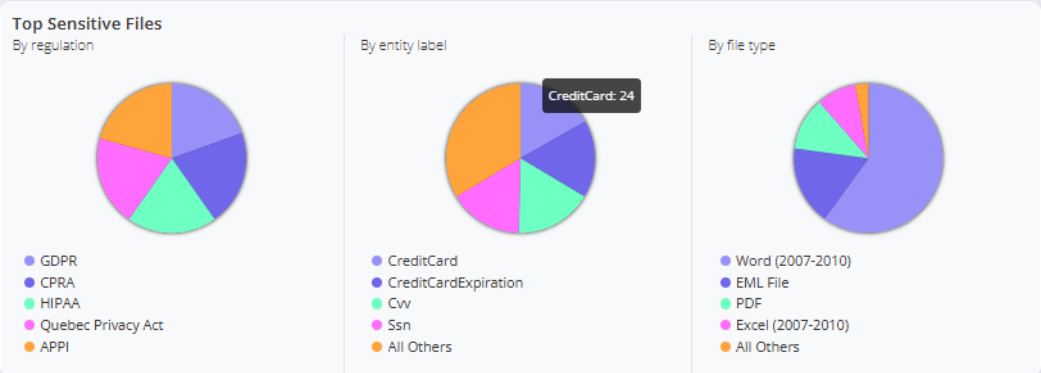


2.16.16 Drill down to view file details

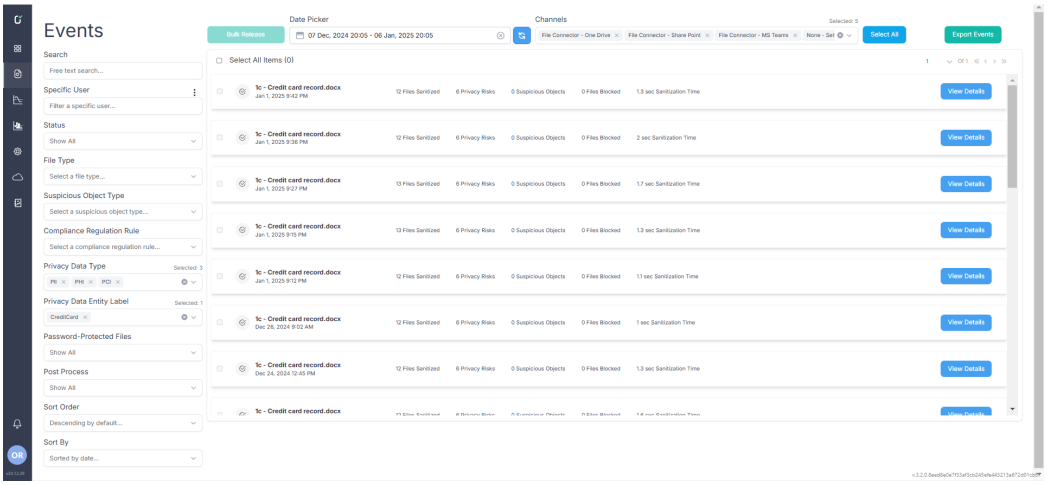
To view more file details for a specific data category, click on the data category in the appropriate chart. This opens the **Events** page for the specific data category and displays all the files containing that data category .

For example, to view the file details for all CreditCard files:

1. Click on the colored region representing CreditCard files in the chart displaying **Sensitive Files By entity label**:

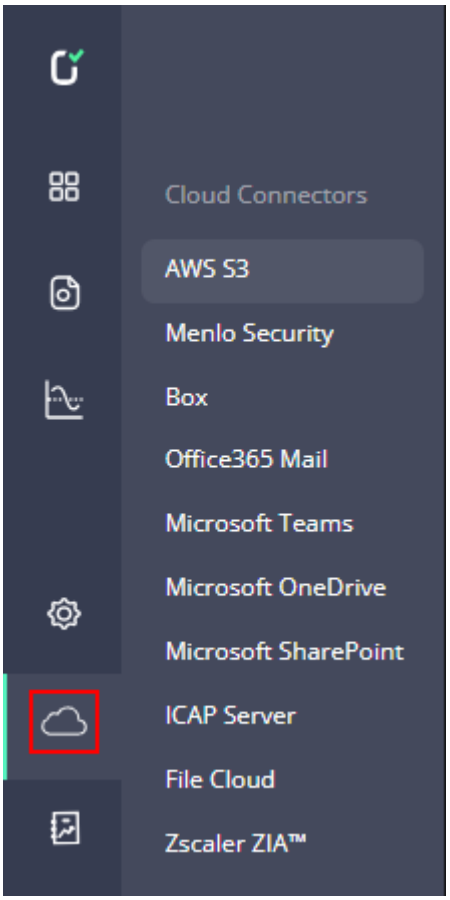


2. The **Events** page opens and displays all 24 CreditCard files:



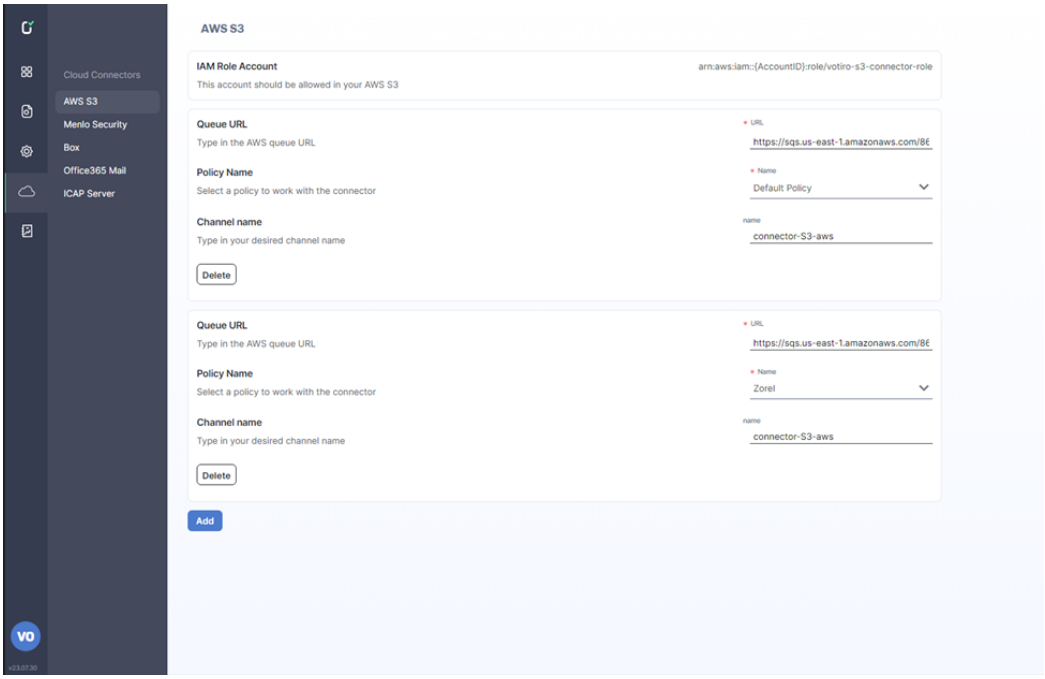
2.17 Cloud Connectors and Integrations

Use the Cloud Connectors and Integrations menu to configure settings in Votiro's Management Dashboard for specified connectors and application integrations.



2.17.1 AWS S3 - SaaS

To get to the AWS S3 page, from the navigation pane on the left, click **Cloud** > **AWS S3**.



The AWS S3 page contains the following fields:

Element	Field	Description
1	IAM Role Account	The AWS IAM user. This account applies to every SQS. Copy the value in this field and paste into the AWS configuration.
2	Queue URL	Specify the AWS queue URL. See below for details.
3	Policy Name	Specify a policy for the AWS S3 connector to work with. Select the **Default Policy** if you have not created an alternative policy to use.
4	Channel name	The AWS S3 connector name

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

Multiple SQS

You may configure more than one SQS associated with a single IAM Role Account.

To add an SQS:

1. Click on the **Add** button.
2. In the new table that opens, enter the following fields for the SQS:
   - Queue URL
   - Policy Name
   - Channel name

To remove an SQS, click on the **Delete** button associated with the SQS.

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.

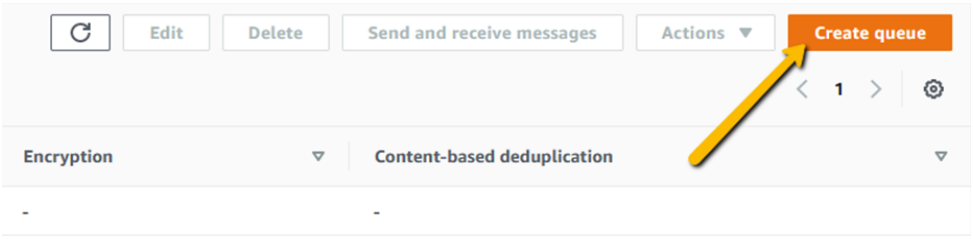
Prerequisites

- AWS SQS (Simple Queue Service) Queue (see See Creating an AWS SQS Queue for details)
- Amazon S3 (Simple Storage Service) bucket
- AWS IAM (Identity and Access Management) user that has access to SQS and S3

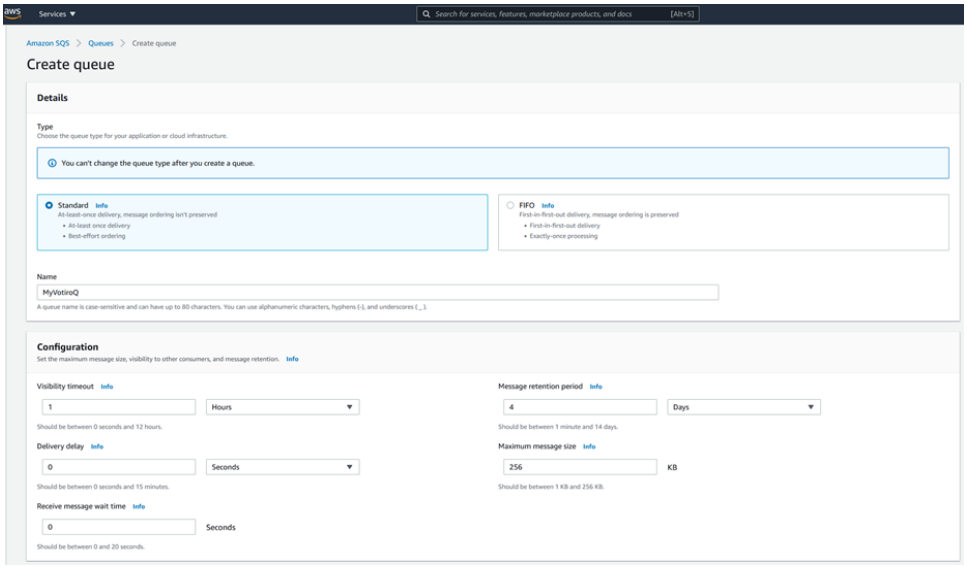
Creating an AWS SQS Queue

You must create an AWS SQS (Simple Queue Service) Queue for S3 bucket integration.

1. Login to your AWS account.
2. Navigate to **Simple Queue Service**.
3. Click on **Create queue**.



4. Under **Type**, select **Standard**.
5. Enter a **Name** for the queue.
6. Modify the values according to the example below:

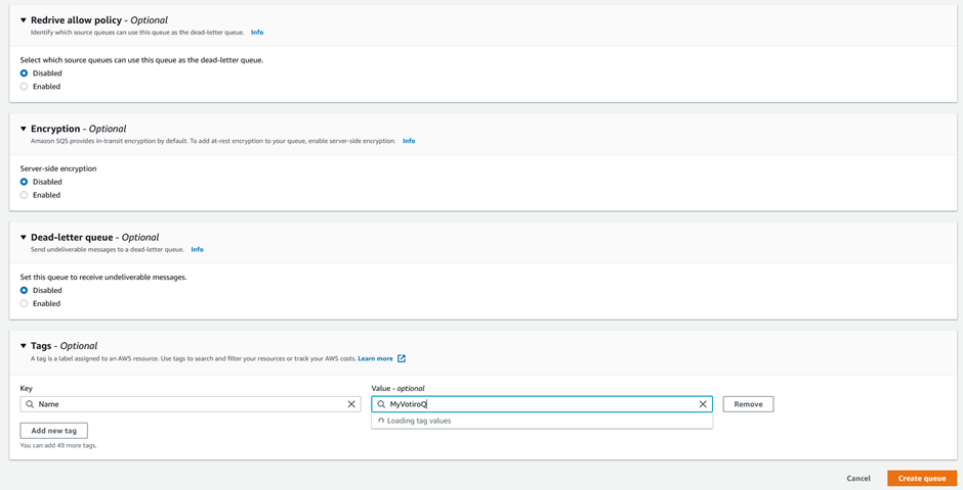


7. For the Access policy, choose **Advanced**.

8. You may use the below template and replace ***<AWS_ACCOUNT_NUM>***, ***<QUEUE_NAME>*** and ***<BUCKET_NAME>*** with their actual values:

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
    {
       "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
         "Service": "s3.amazonaws.com"
      },
      "Action": [
         "SQS:SendMessage"
      ],
      "Resource": "arn:aws:sqs:us-east-1:<AWS_ACCOUNT_NUM>:<QUEUE_NAME>",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AWS_ACCOUNT_NUM>"
         }
         "ArnLike": {
            "aws:SourceArn": "arn:aws:s3:*:*:<BUCKET_NAME>"
         },
      }
   }
   }
   ]
}
```

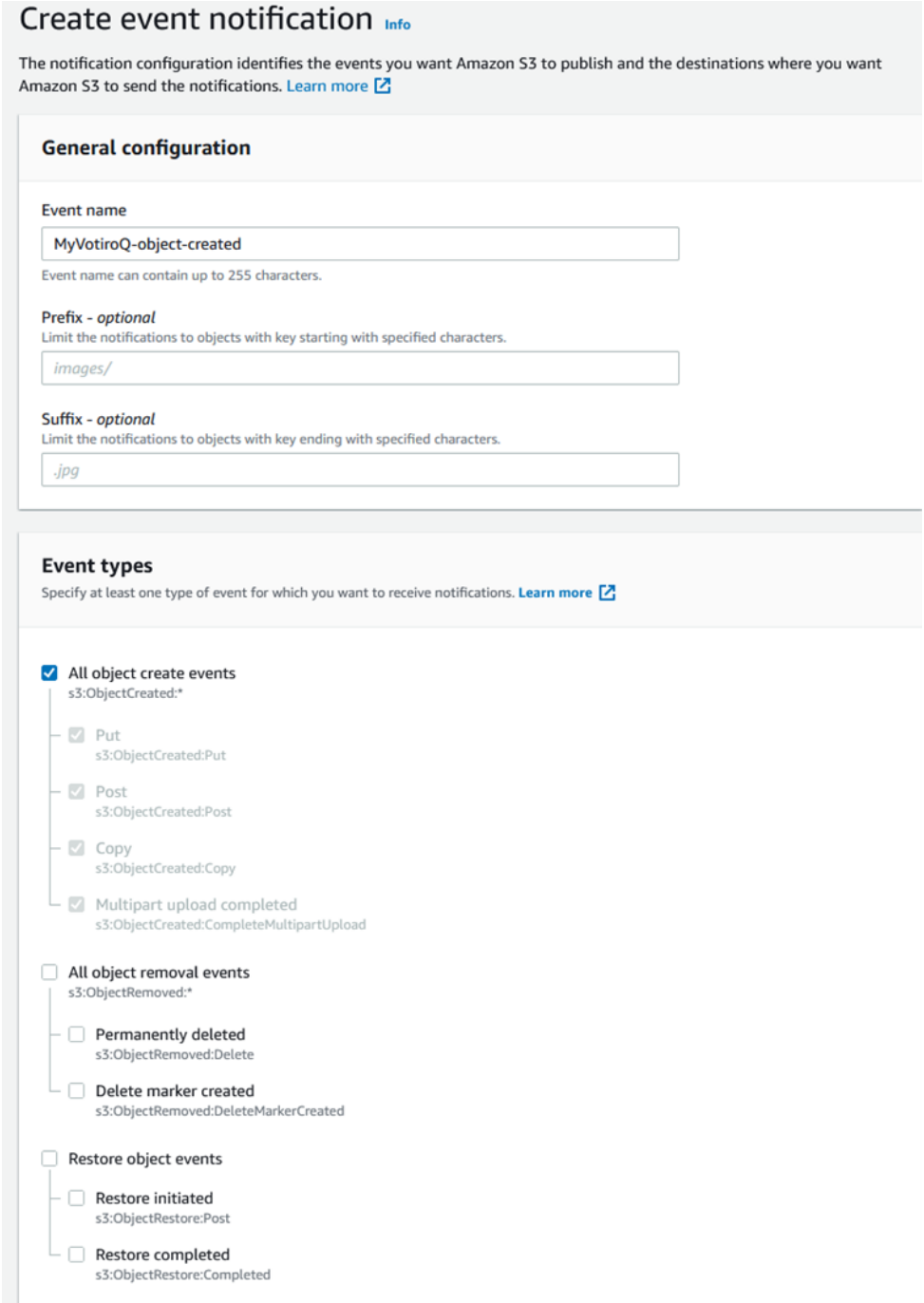
9. Under **Tags**, you may create an optional tag for the queue by setting **Key** to "Name" and **Value** to the queue name, for example:



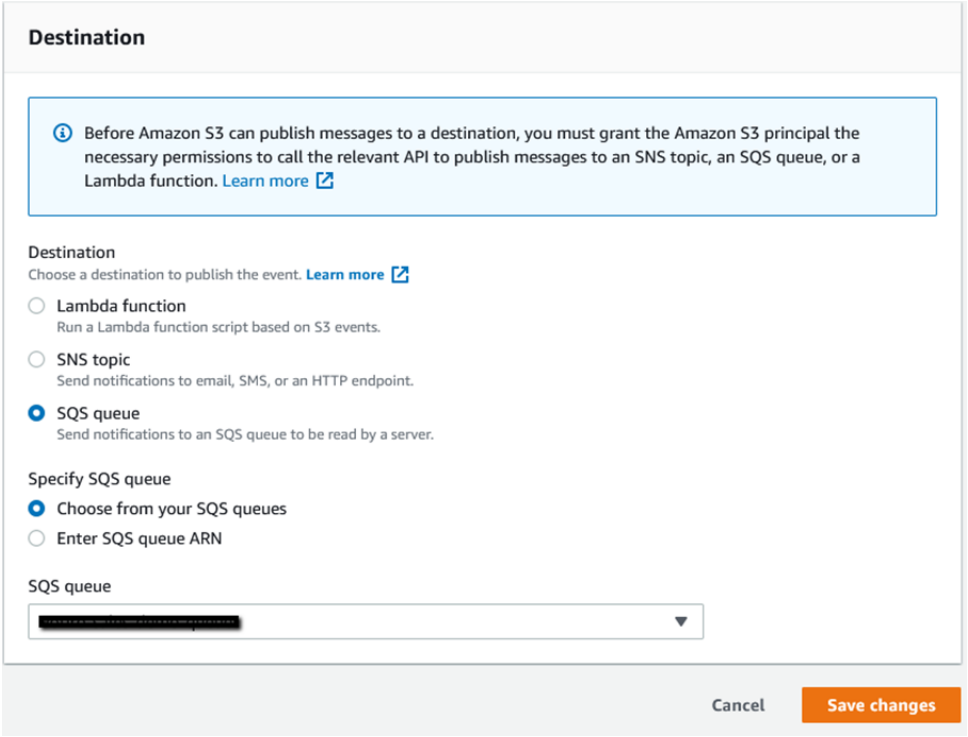
10. Other options should remain at their default values.
11. Click on **Create queue**.

Assigning the Queue to an Existing S3 Bucket

1. Navigate to the desired bucket.
2. Select the **Properties** tab.
3. Scroll down to **Event notifications**.
4. Click on **Create event notifications**.
5. Set the **Event name** to the desired name.
6. Under **Event types**, select **All object create events**. For example:



7. Under **Destination**, select **SQS queue**.
8. Under **Specify SQS queue**, select **Choose from your SQS queues**.
9. Select the newly created **SQS queue** from the list of available queues. For example:



10. To save the SQS queue configuration, click on **Save changes**.

11. Add the following statements to the SQS Access Policy, and replace ***<AWS_IAM_USER_ACCOUNT_NUM>***, **<AWS_ACCOUNT_NUM>**, ***<VOTIRO-S3-CONNECTOR-ROLE>*** and ***<BUCKET_NAME>*** with their actual values:

```
{
   "Sid":"Votiro_receiver_statement",
   "Effect": "Allow",
   "Principal": {
      "AWS": "arn:aws:iam::<AWS_IAM_USER_ACCOUNT_
      NUM>:role/<VOTIRO-S3-CONNECTOR-ROLE>"
   },
   "Action": [
      "SQS:ChangeMessageVisibility",
      "SQS:DeleteMessage",
      "SQS:ReceiveMessage"
   ],
   sqs:<REGION>:<CUSTOMER_AWS_ACCOUNT_NUM>:<QUEUE_NAME>
}
```

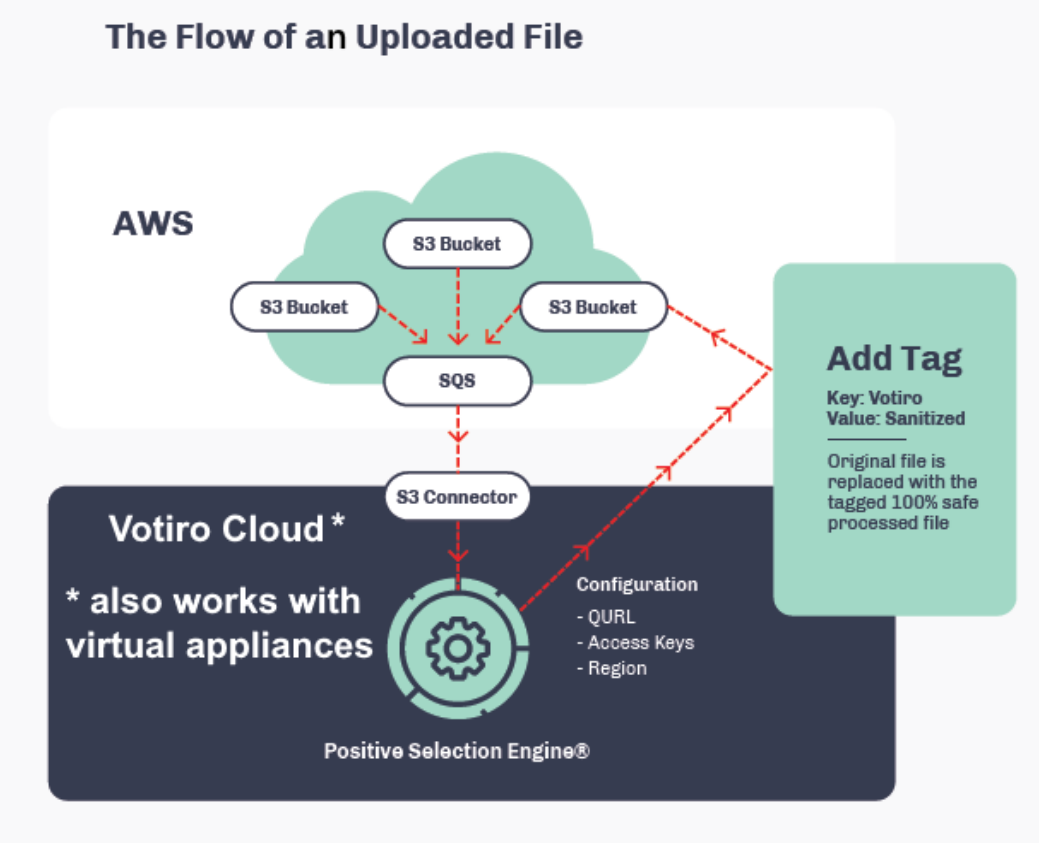
12. In the S3 Permission add the following policy:

To use the example below, replace ***<AWS_ACCOUNT_NUM>***, ***<QUEUE_NAME>*** and ***<BUCKET_NAME>*** with their actual values.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::<AWS_IAM_USER_ACCOUNT_
            NUM>:role/<VOTIRO-S3-CONNECTOR-ROLE>"
         },
         "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject",
            "s3:GetObjectTagging",
            "s3:PutObjectTagging"
         ],
         "Resource": [
            "arn:aws:s3:::<BUCKET_NAME>/*"
         ]
      }
   ]
}
```

AWS S3 Flowchart

The following diagram illustrates the procedure:



Limitations

Sanitization for large files is supported up to 3 GB.

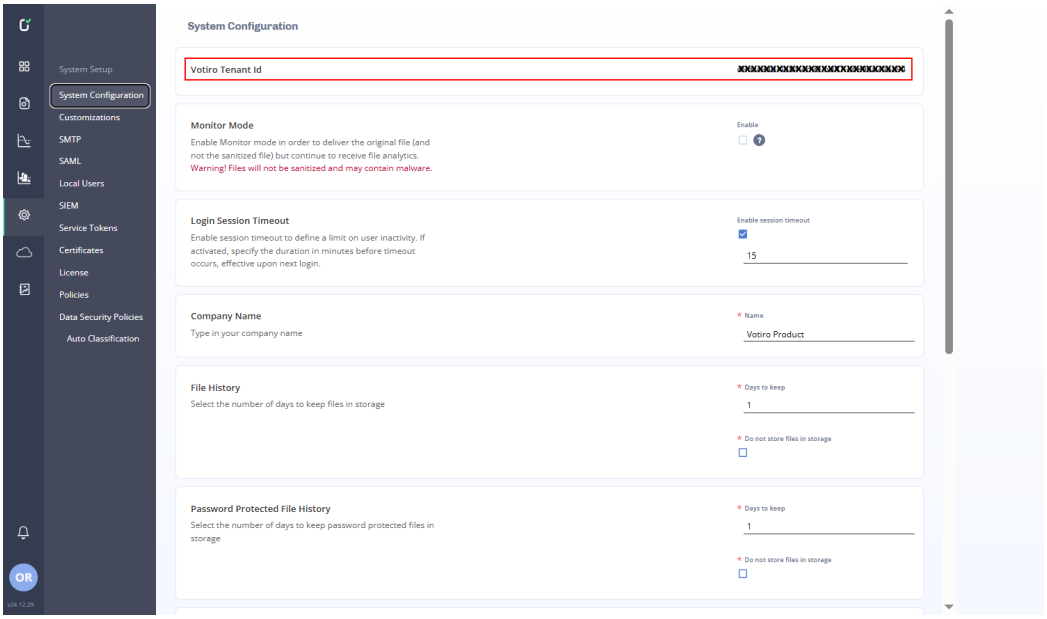
2.17.2 Menlo Security

Prerequisites

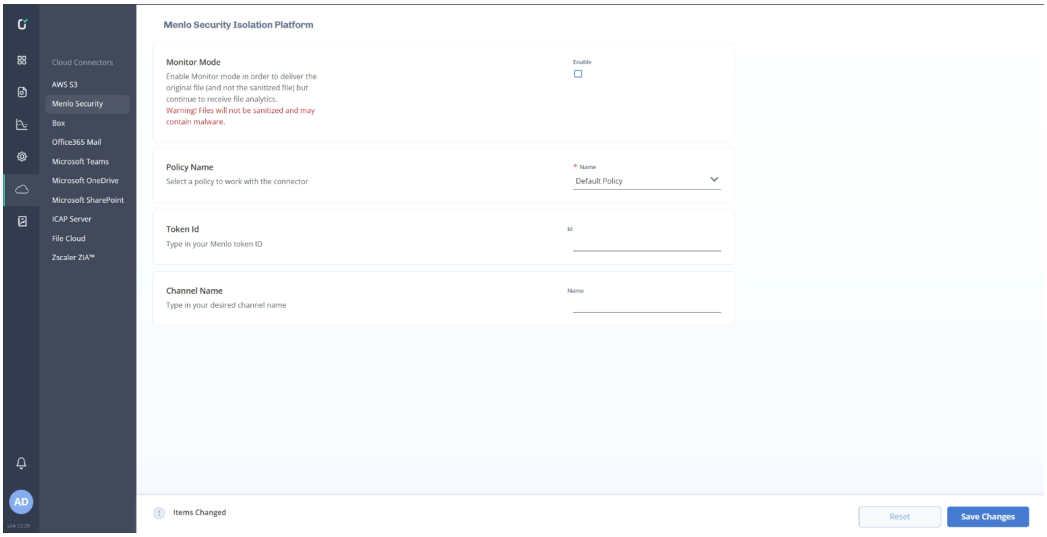
You need to import the Menlo Root CA certificate. See Menlo Security Production SSL Inspection Root CA Certificate.

Configuration of Menlo Security in Votiro

1. Navigate to the Votiro Management Console and select **System setup** > **System Configuration**.
2. Copy the **Votiro Tenant Id** to the clipboard.



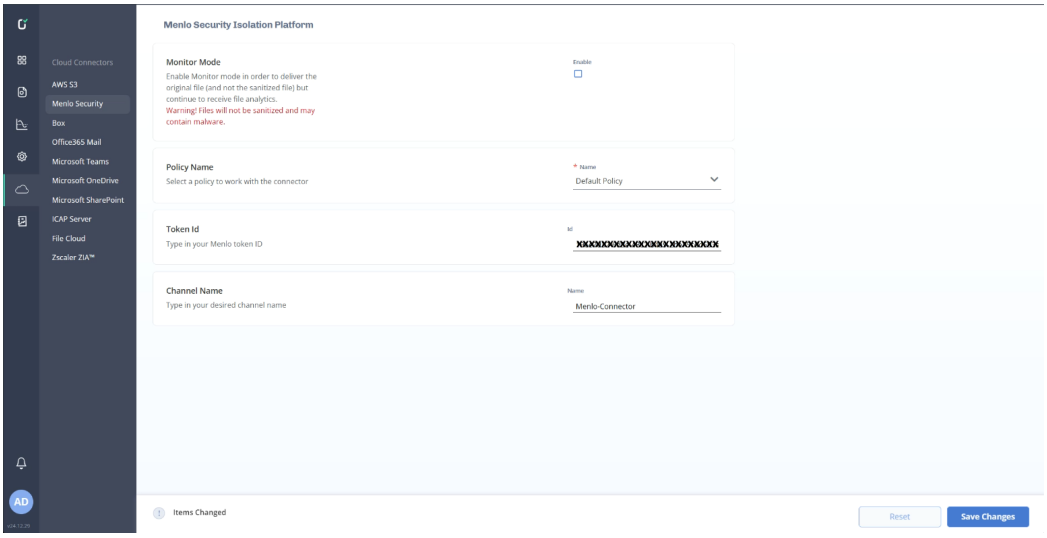
3. Navigate to **Cloud Connectors** > **Menlo Security**.



4. The Menlo Security page contains the following fields:

Element	Field	Description
0	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. By default, Monitor Mode is disabled for editing. To enable this feature, please contact Votiro support.
1	Policy Name	Specify a policy for the Menlo Security connector to work with. Select the **Default Policy** policy if you have not created an alternative policy to use.
2	Token Id	Specify the Votiro Tenant ID, which can be obtained from the System Configuration page.
3	Channel Name	Specify the name of your channel. The channel name appears in the Incidents page as the name of a connector.

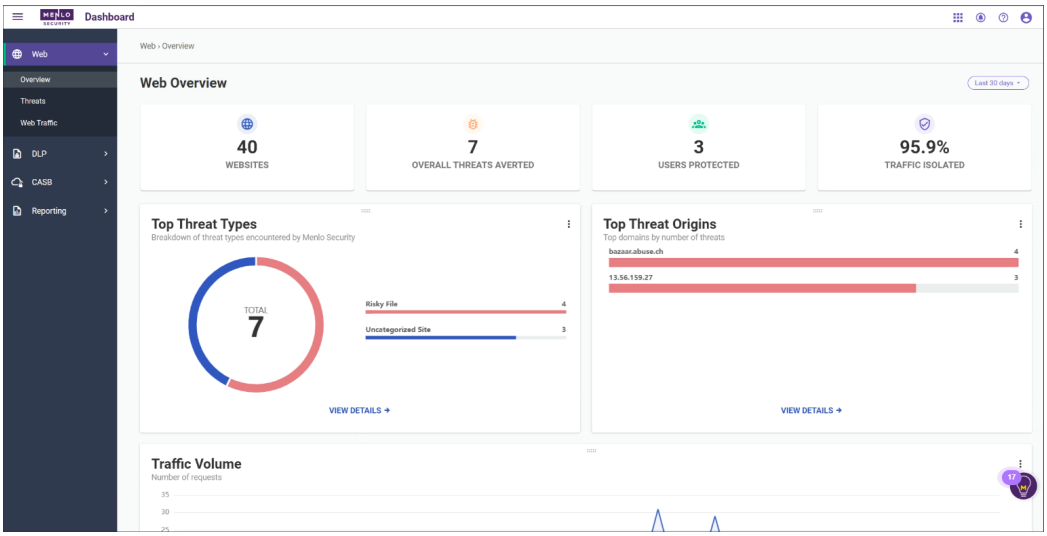
5. Paste the **Votiro Tenant Id** from the clipboard to the **Token Id** field.
6. Type a name for the **Channel Name**, for example "Menlo Connector".
7. Select a **Policy Name** to work with the connector.



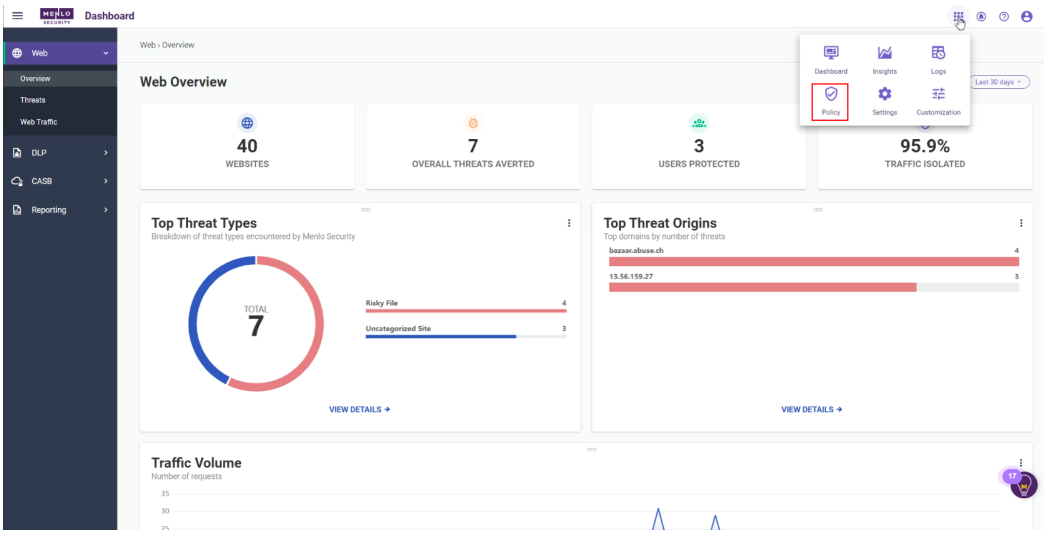
8. Click on **Save Changes**.

Configuration of the Cloud Connector to Menlo Security

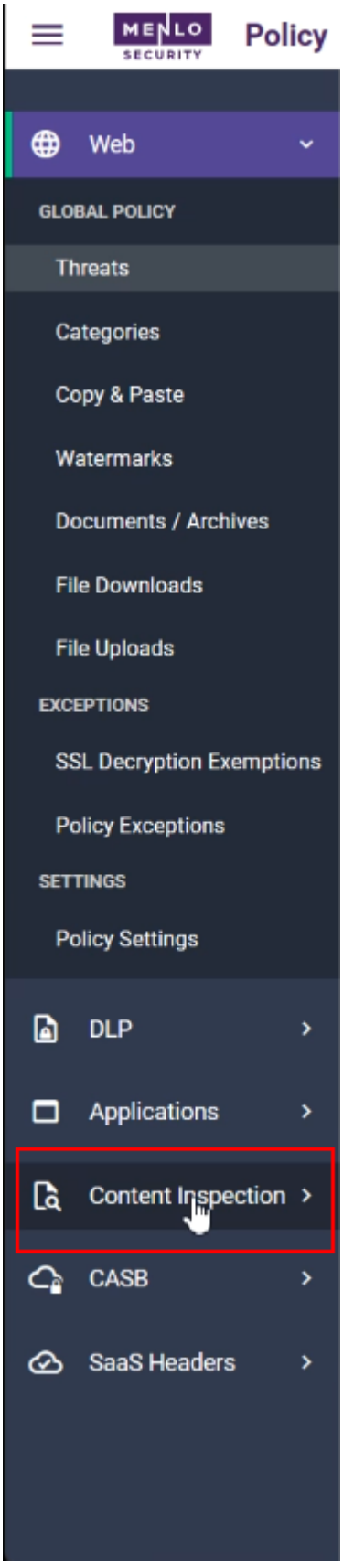
1. Login to the Menlo Administrator page at Admin Portal. The Menlo Dashboard appears:



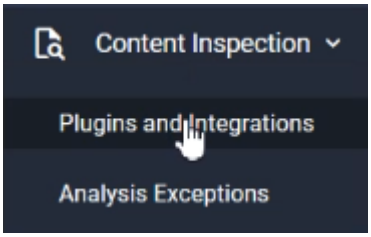
2. Click on the Apps button and select **Policy**.



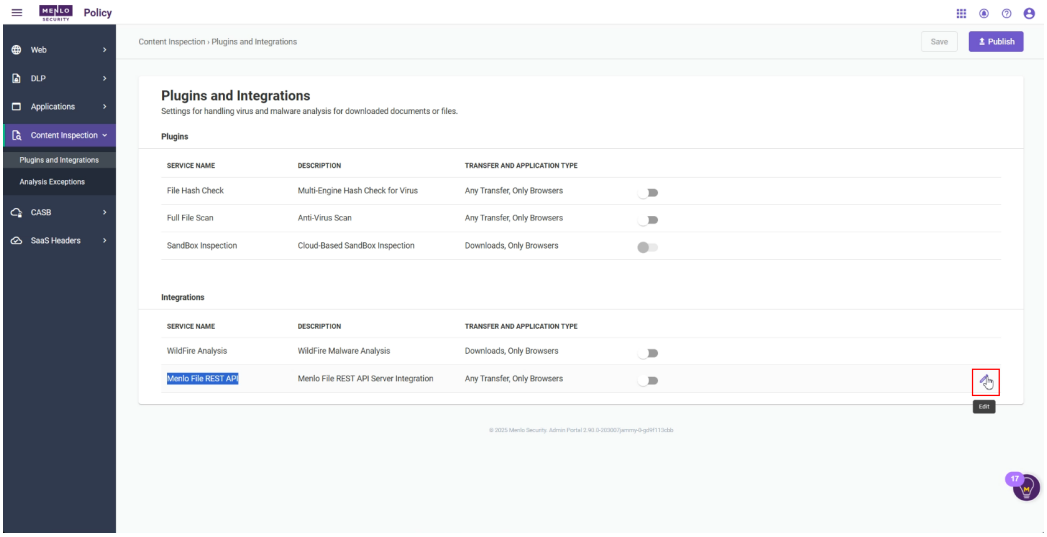
3. On the sidebar menu, click on **Content Inspection**.



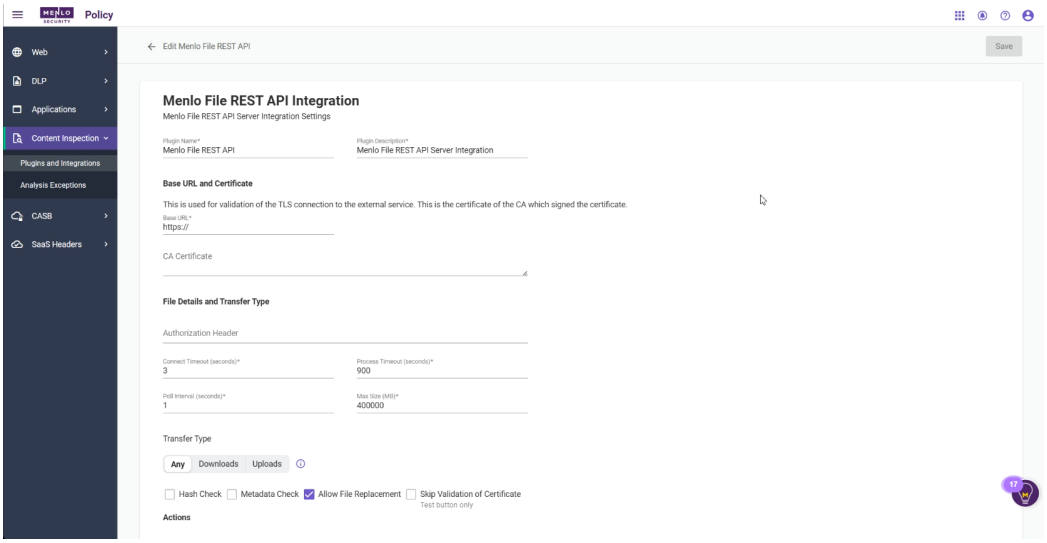
4. From the submenu that opens, click on **Plugins and Integrations**.



5. The **Plugins and Integrations** page is displayed. In the **Integrations** section, go to the **Menlo File REST API** row and click on the Edit icon at the end of the row.



6. The **Menlo File REST API Integration** page is displayed.

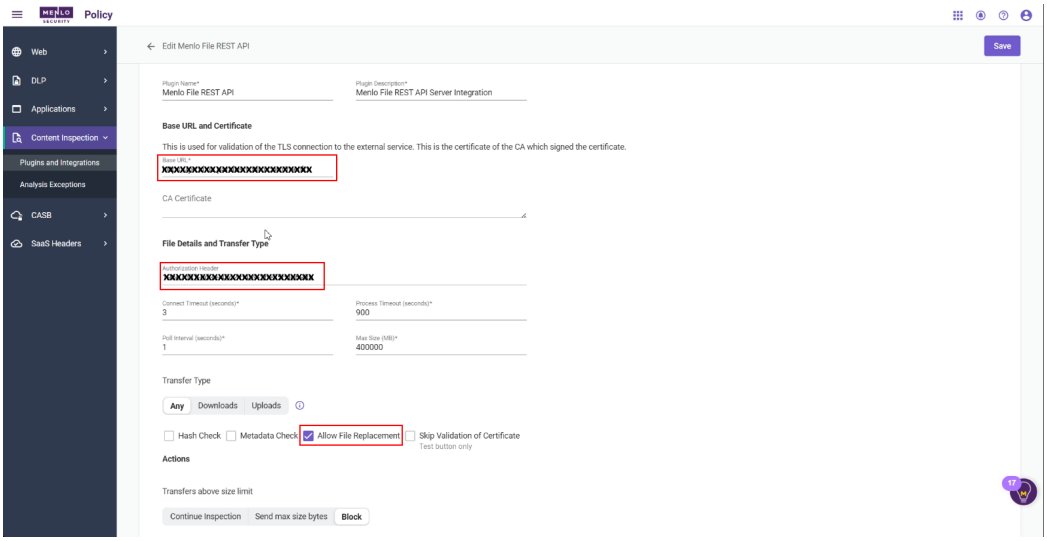


7. On the **Edit Menlo File REST API Integration** page:

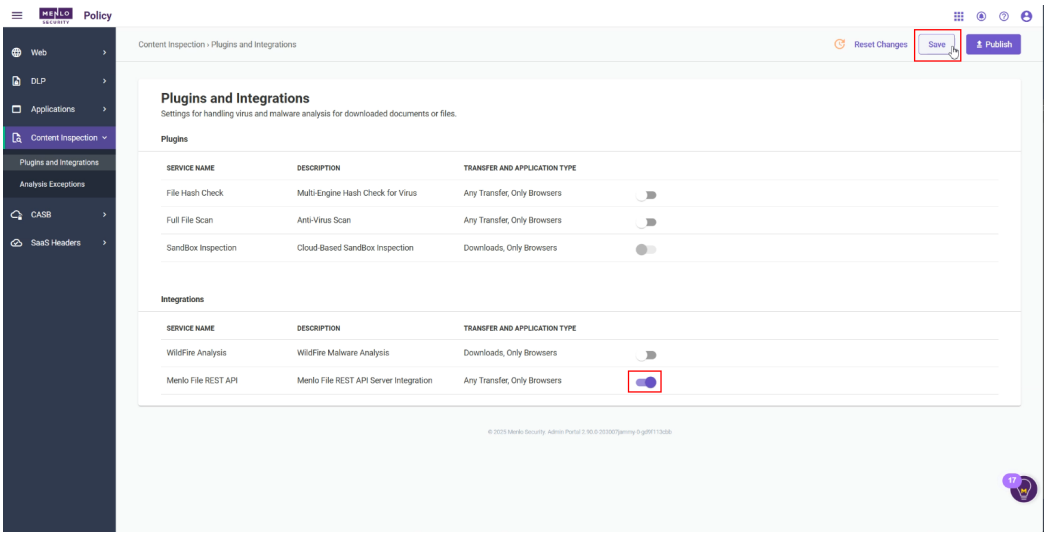
   a. In the **Base URL** field enter the value supplied by Votiro: Base URL.

   b. In the **Authorization Header** field, paste the Votiro Tenant Id you saved.

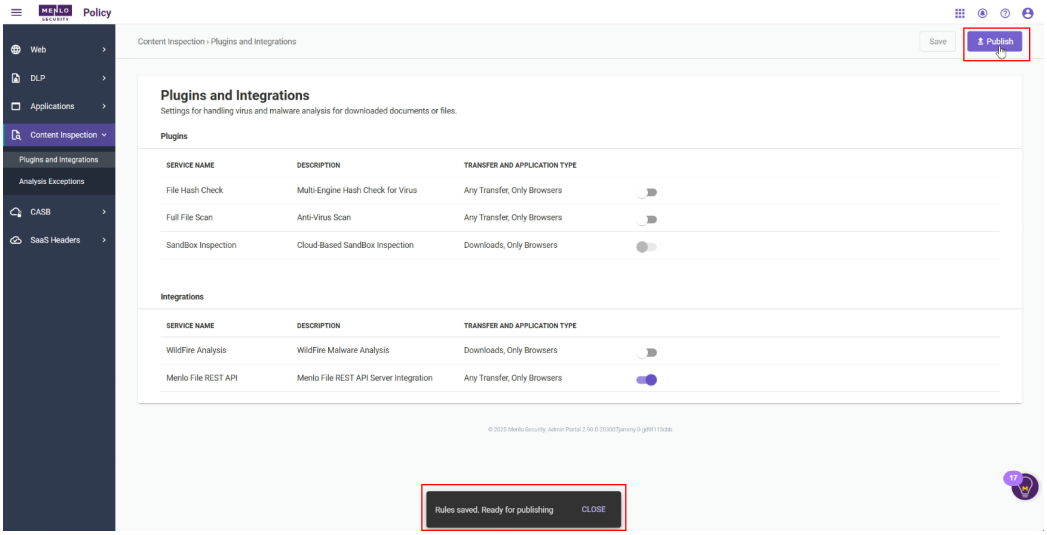
   c. Verify that the field **Allow File Replacement** is checked.



d. Toggle the **Menlo File REST API** switch to ON and then click on the **Save** button.



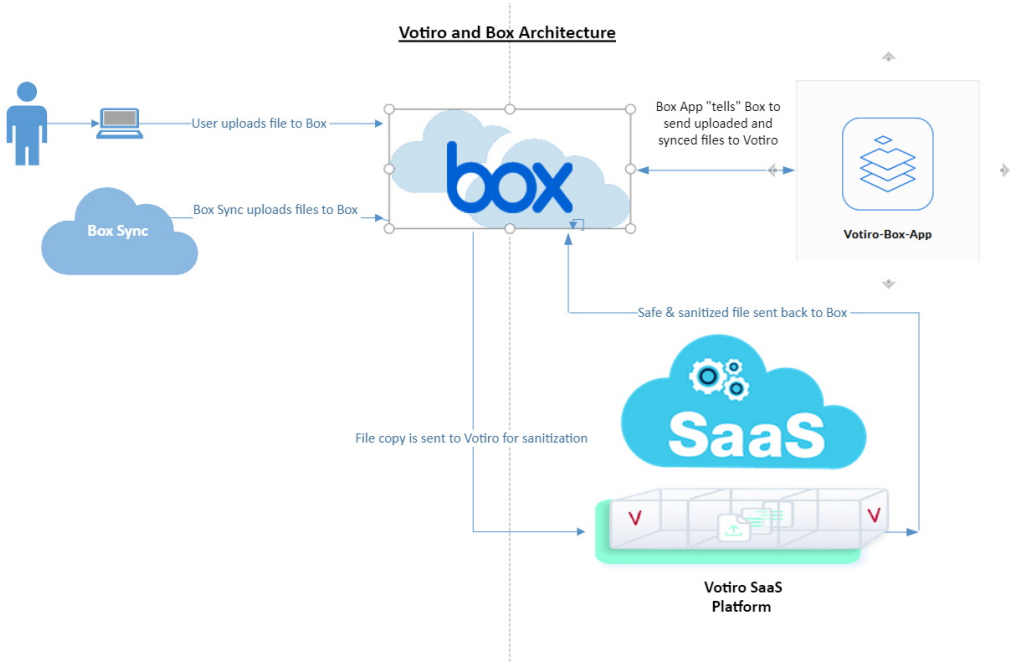
e. The message **Rules Saved. Ready for publishing** should be displayed. Click on the **Publish** button to publish the settings to the tenant.



2.17.3 Box

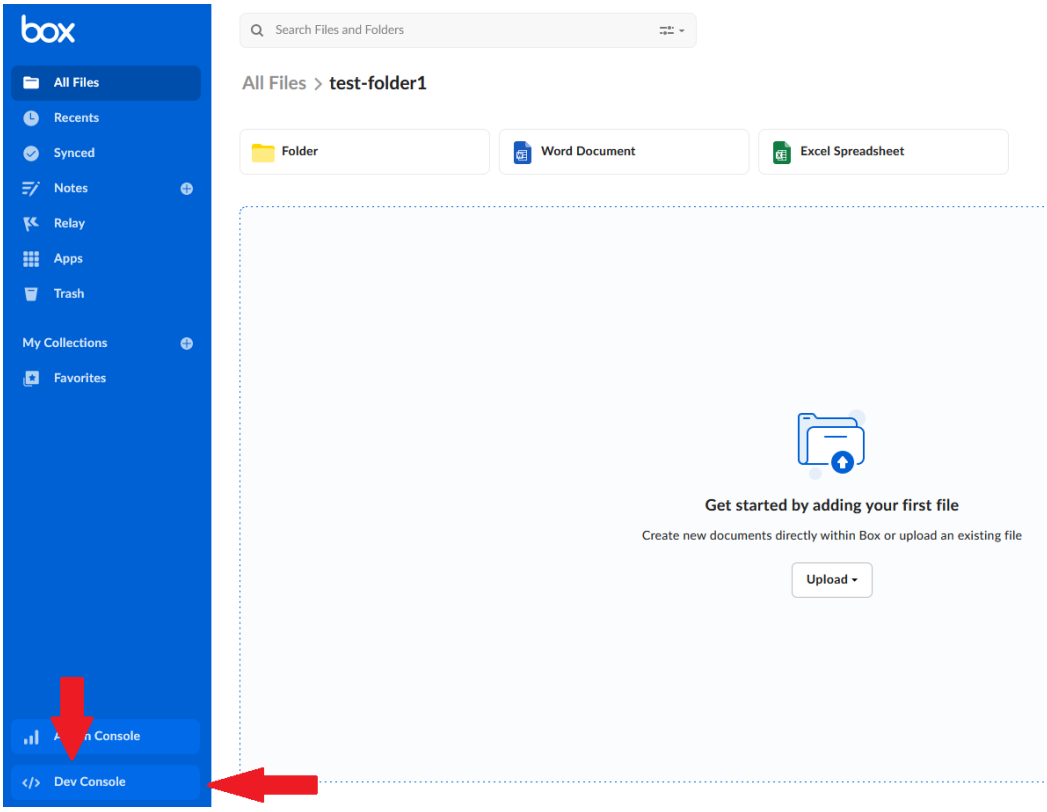
Votiro and Box

The diagram below describes the architecture of the Votiro - Box interface;

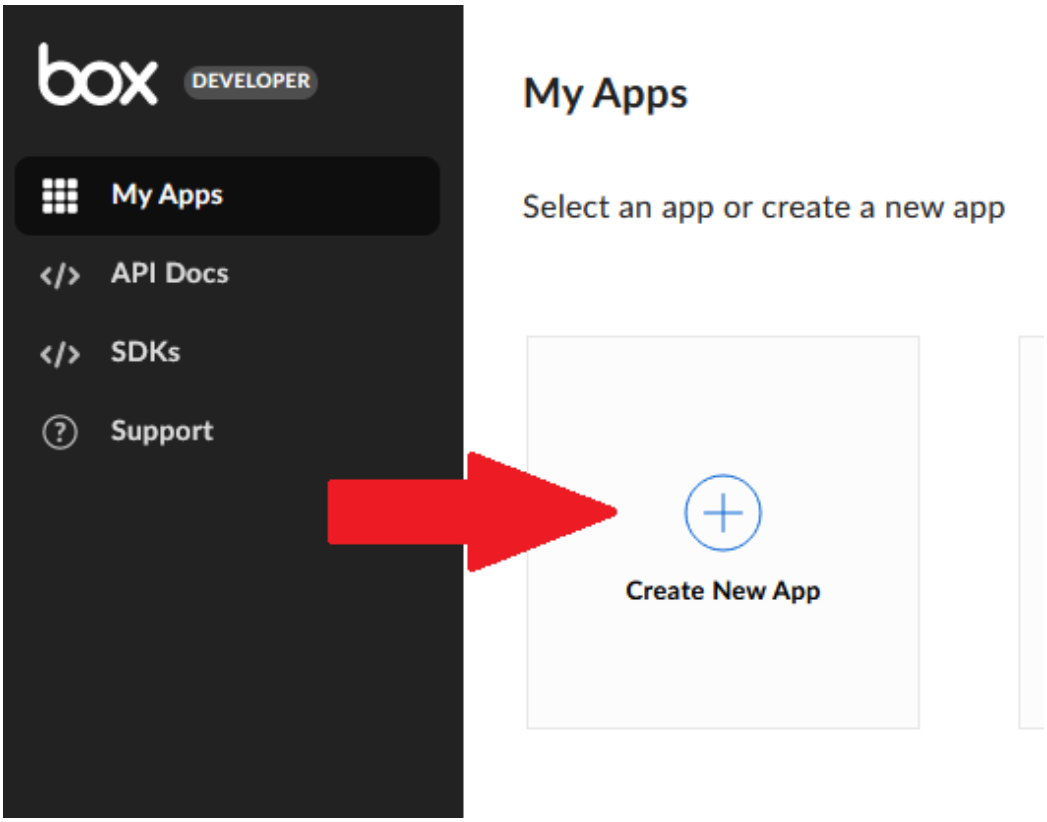


Configuration of an App in Box to Integrate with Votiro

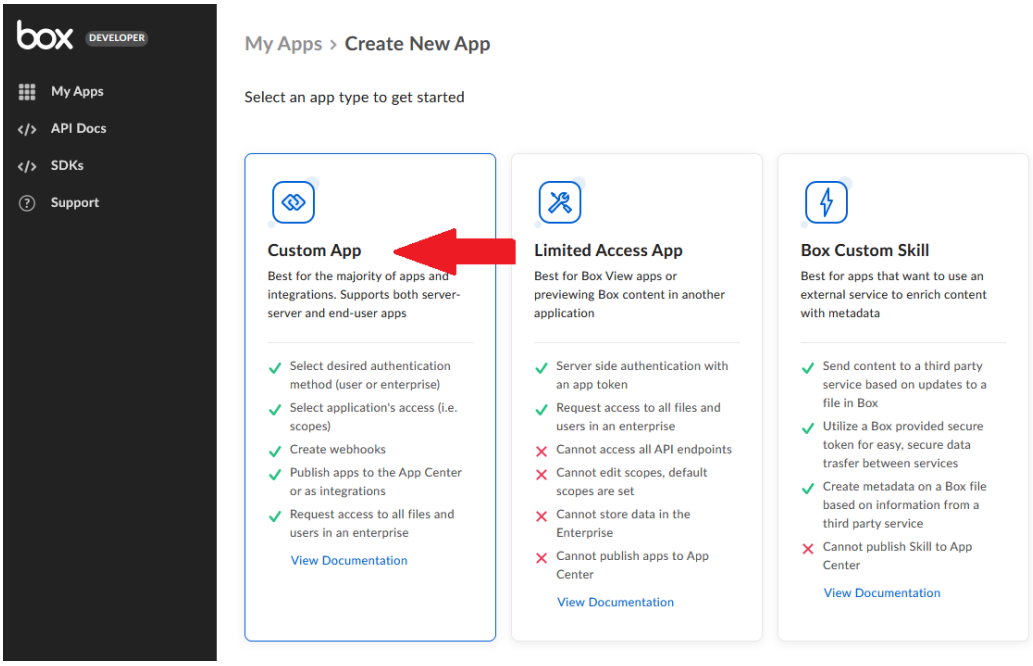
1. Login to your Box.com account with Admin privileges.
2. In the Box menu, select **Dev Console** (if you can't find the button go to Dev Console).



3. On the **My Apps** page, Click on the **Create New App** button:



4. Select **Custom App**:

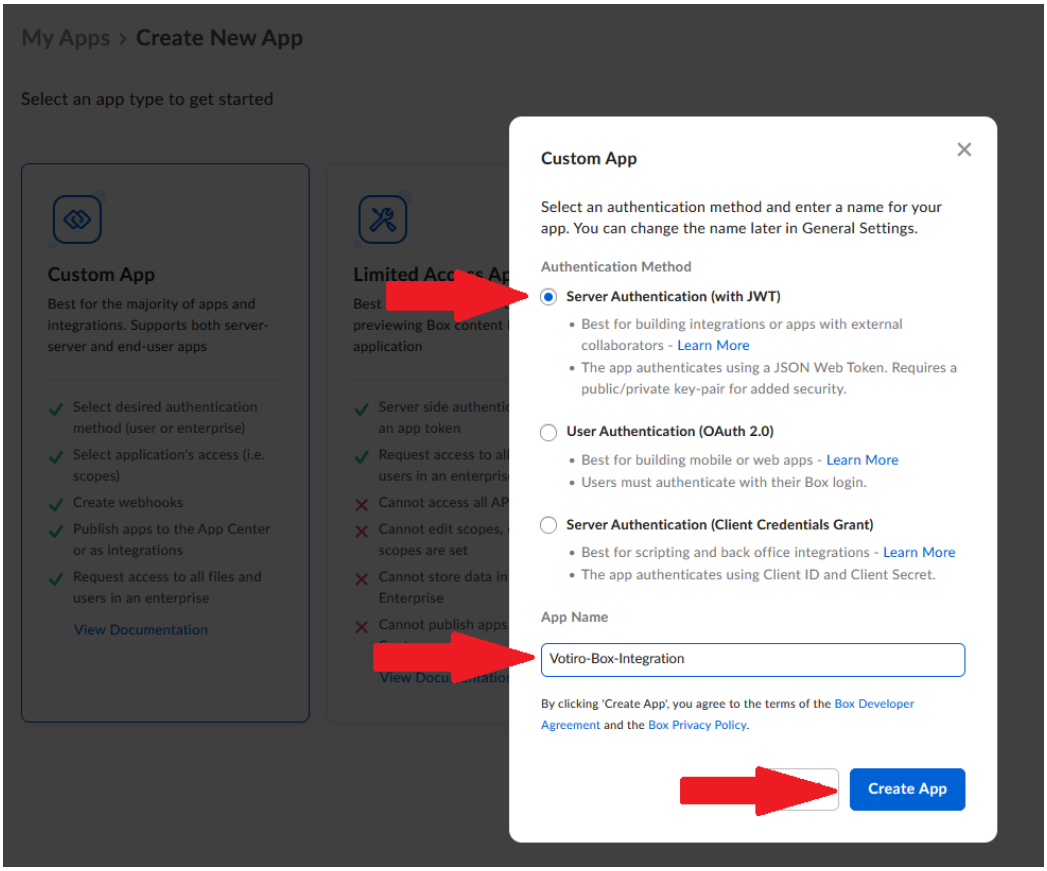


5. On the **Custom App** pane:

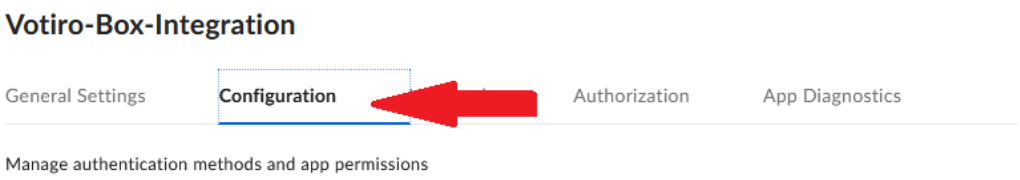
   a. Select the **Authentication Method** as **Server Authentication (with JWT)**.

   b. Type in an **App Name** (for example, Votiro-Box-Integration).

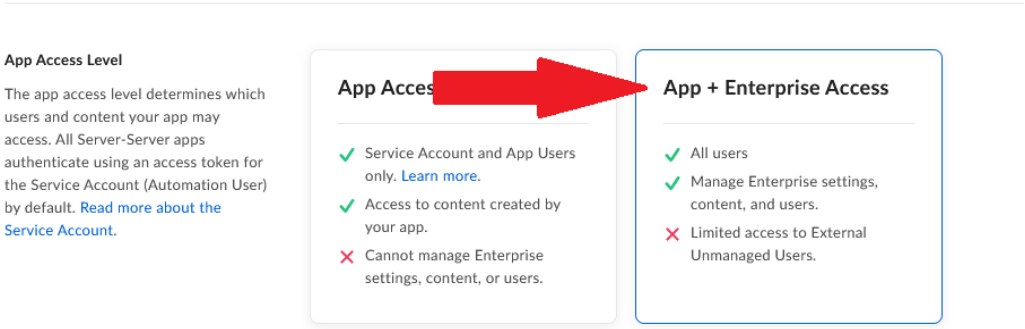
   c. Click on the **Create App** button:



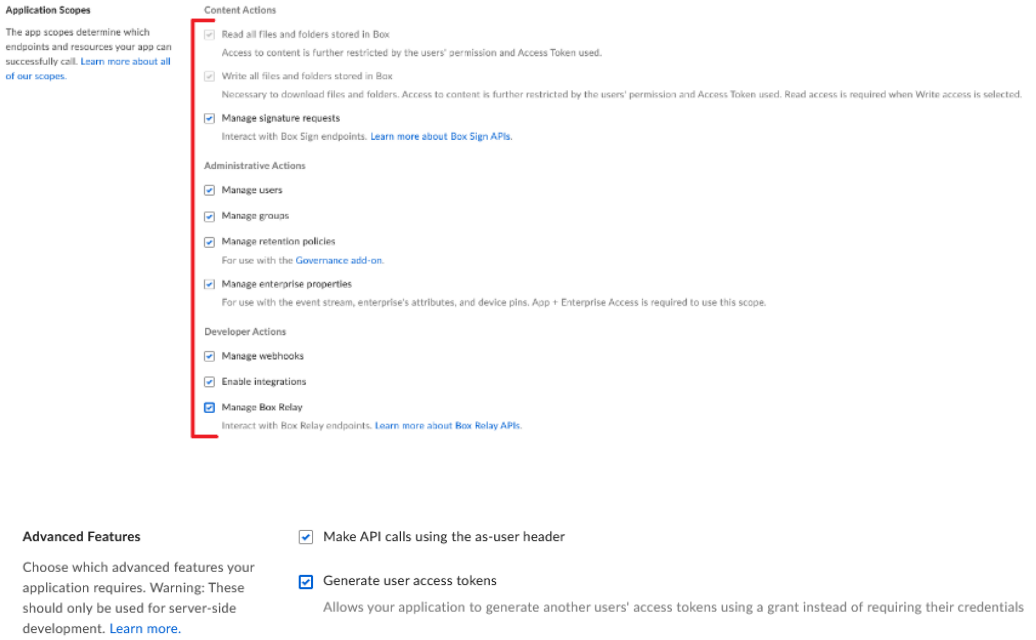
6. Select the **Configuration** tab, then select “App + Enterprise Access”:



7. Select **App + Enterprise Access**.

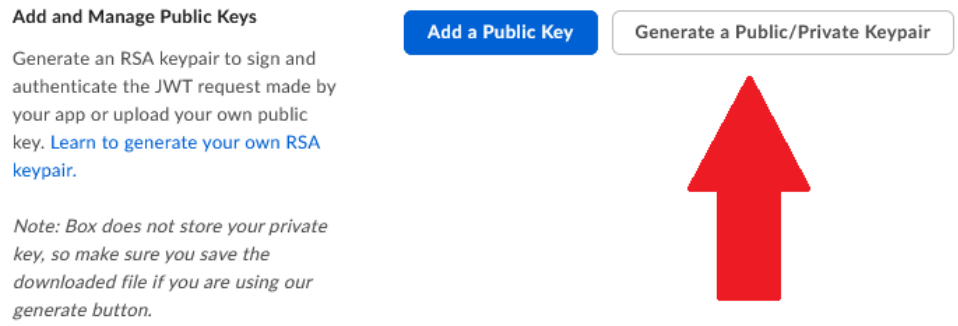


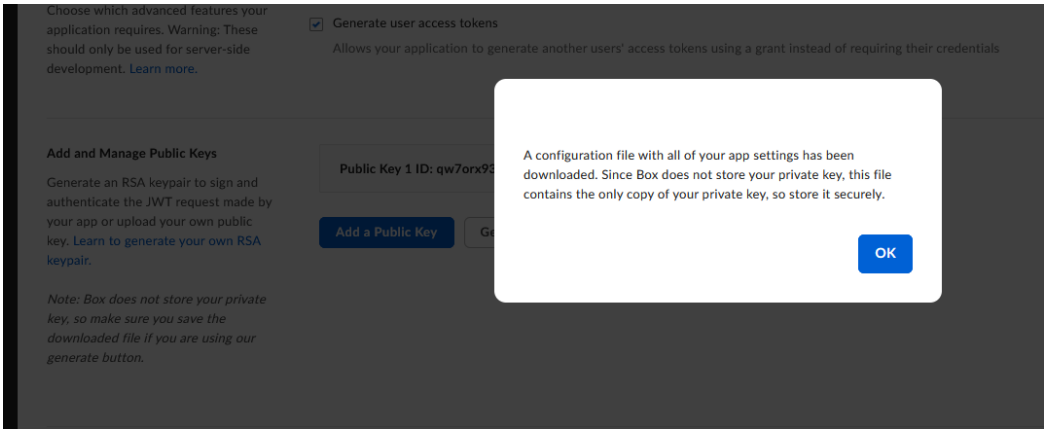
8. Make sure you check all the checkboxes under **Application Scopes** and **Advanced Features**:



9. Click the **Save Changes** button:

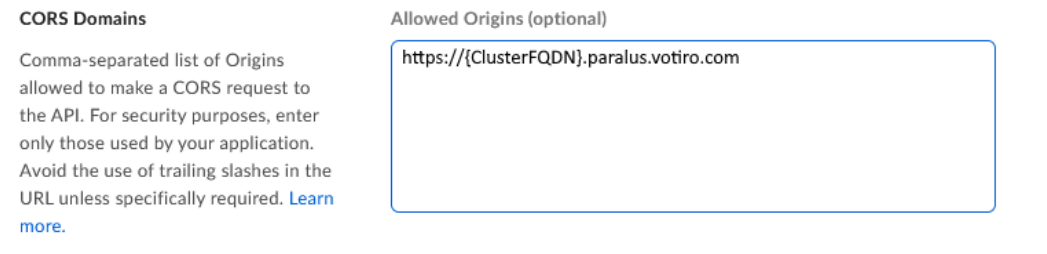
10. Scroll down to **Add and Manage Public Keys** and click on **Generate a Public/Private Keypair** (this step might require 2FA approval) and save the prompted JSON file to your machine:





> **Note**: If the JSON file is not downloaded, click again on **Generate a Public/Private Keypair**.

11. Add the Votiro URL to the **Allowed Origins** section:



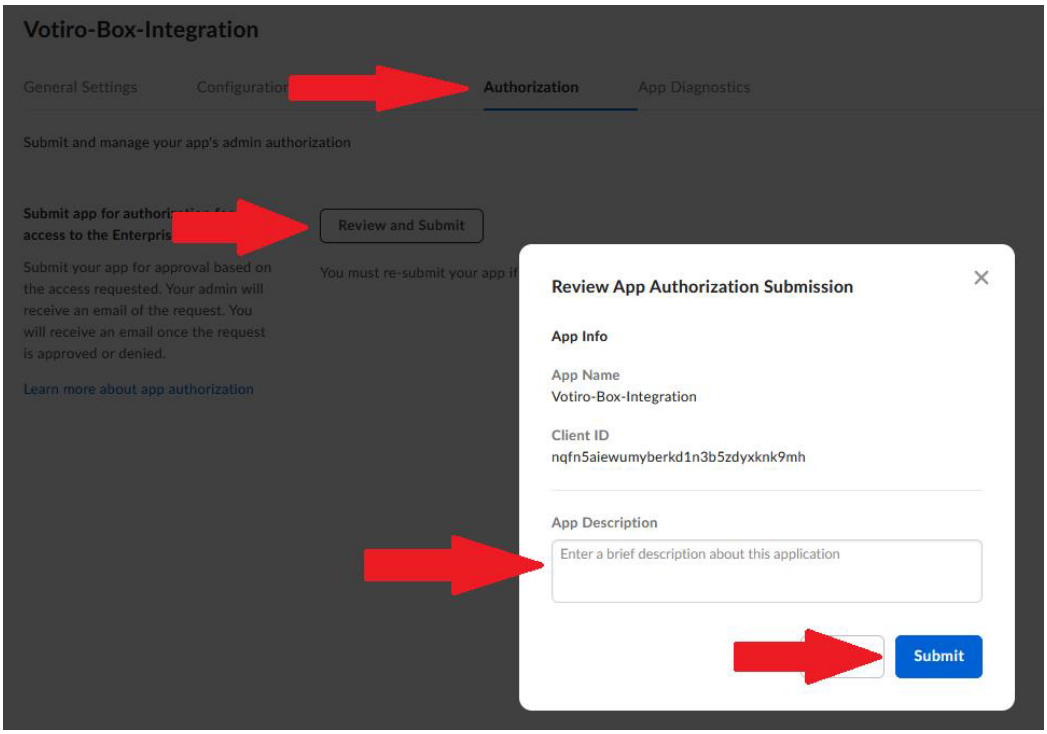
12. Click the **Save Changes** button again:

13. Select the **Authorization** tab and:

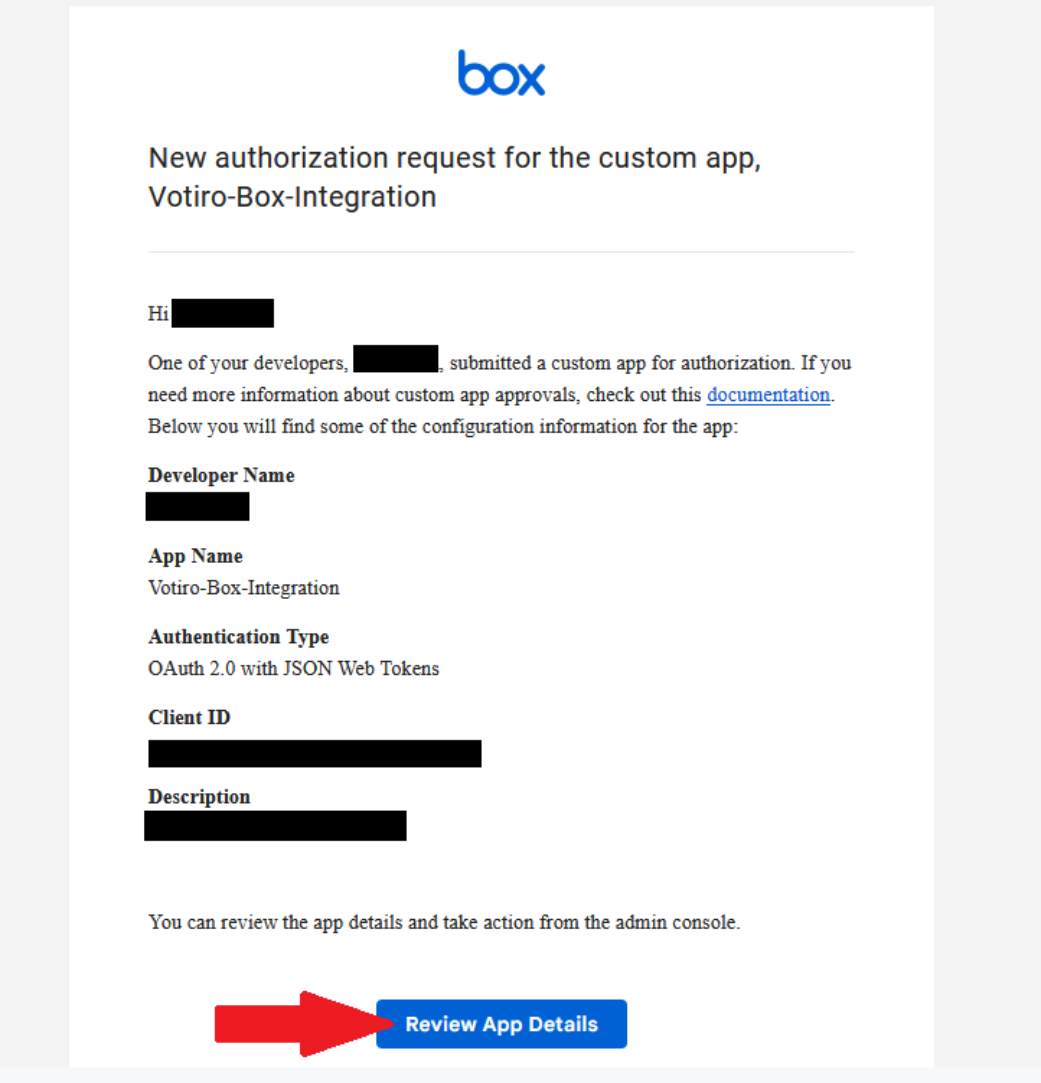
    a. Click on **Review and Submit**.

    b. Type an **App Description**

c. Click on the **Submit** button:



14. Your **Box** admin should receive a confirmation email, similar to the screenshot below.
Click on **Review App Details**:

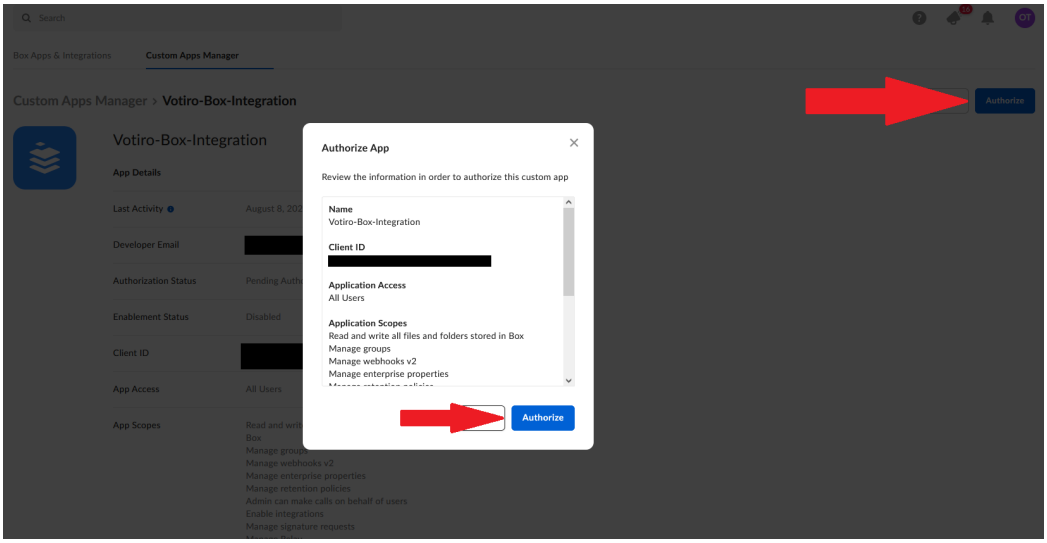


15. You'll get redirected to **Box.com** again.

    a. Go to the **Custom Apps Manager** and select your new app.

    b. Click **Authorize** and review your app settings.

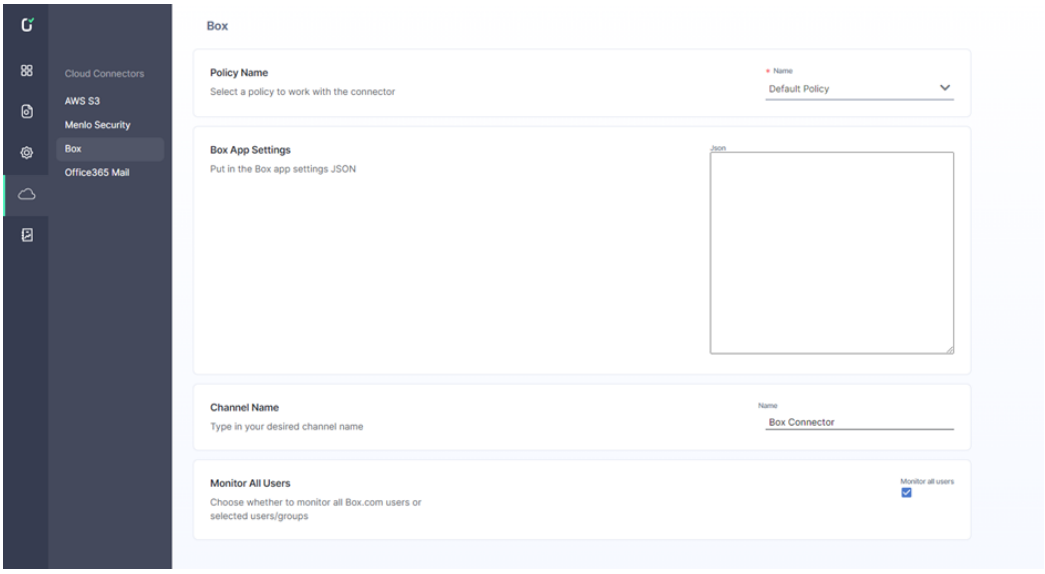
    c. Click on the **Authorize** button:



16. After the Box app is configured, you must configure it in the Votiro Management Dashboard, as described in the following section.

Configuration of the Box App in the Votiro Management Dashboard

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

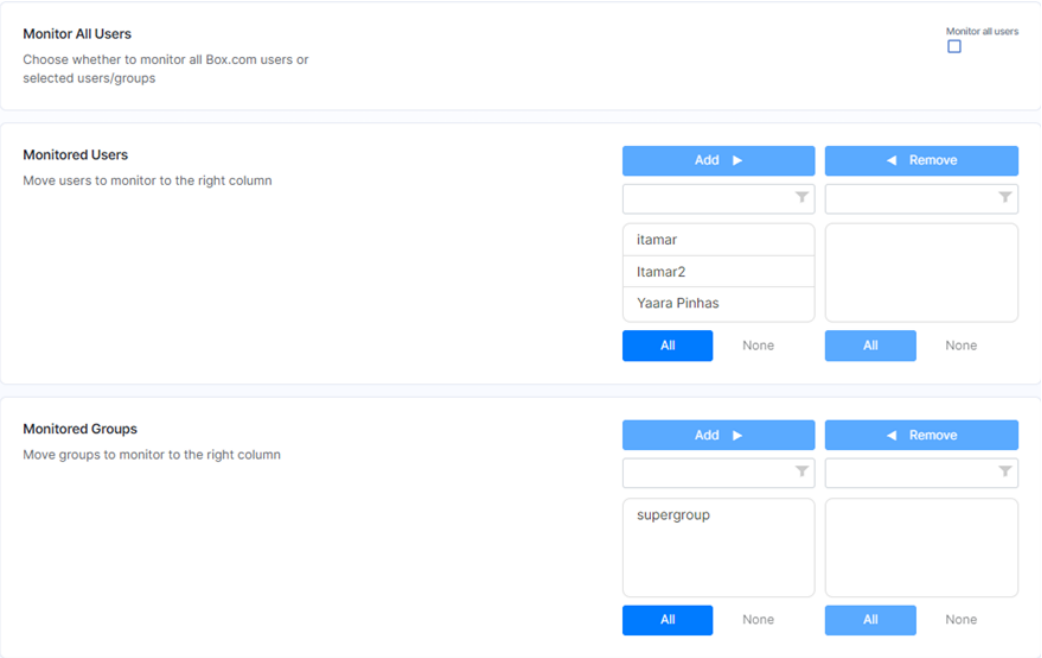


The Box page contains the following fields:

Field	Description
Policy Name	Specify a policy for the Box connector to work with. Select the **Default Policy** if you have not created an alternative policy to use.

Field	Description
Box App Settings	To integrate with the Box account, add the **Public/Private Keypair** by pasting the content of the JSON file you saved to your machine when creating the Custom App in Box to integrate with Votiro. The keypair is located in the JSON file.
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 "Box Connector".
Monitor All Users	Check this box to enable all users under the Box enterprise account to perform sanitization when uploading files to Box. *
*Monitored Users	* displayed only if **Monitor All Users** is not checked. The left column will contain all users under the Box enterprise account. To authorize specific users to be able to sanitize files, select the users from the left column and click **Add**. To deny sanitization authorization to specific users, select the users from the right column and click **Remove**. To add/remove all/no users, click the **All**/**None** buttons in the respective column.
*Monitored Groups	* displayed only if **Monitor All Users** is not checked. The left column will contain all groups under the Box enterprise account. To authorize specific groups to be able to sanitize files, select the groups from the left column and click **Add**. To deny sanitization authorization to specific groups, select the groups from the right column and click **Remove**. If a group is enabled/disabled for sanitization, all the group users are enabled/disabled even if the group users were not enabled/disabled in the **Monitored Users** field.

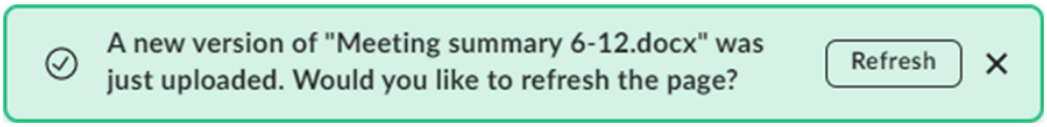
* If you uncheck **Monitor All Users**, the following options are displayed:



Box App Behavior when Uploading Files

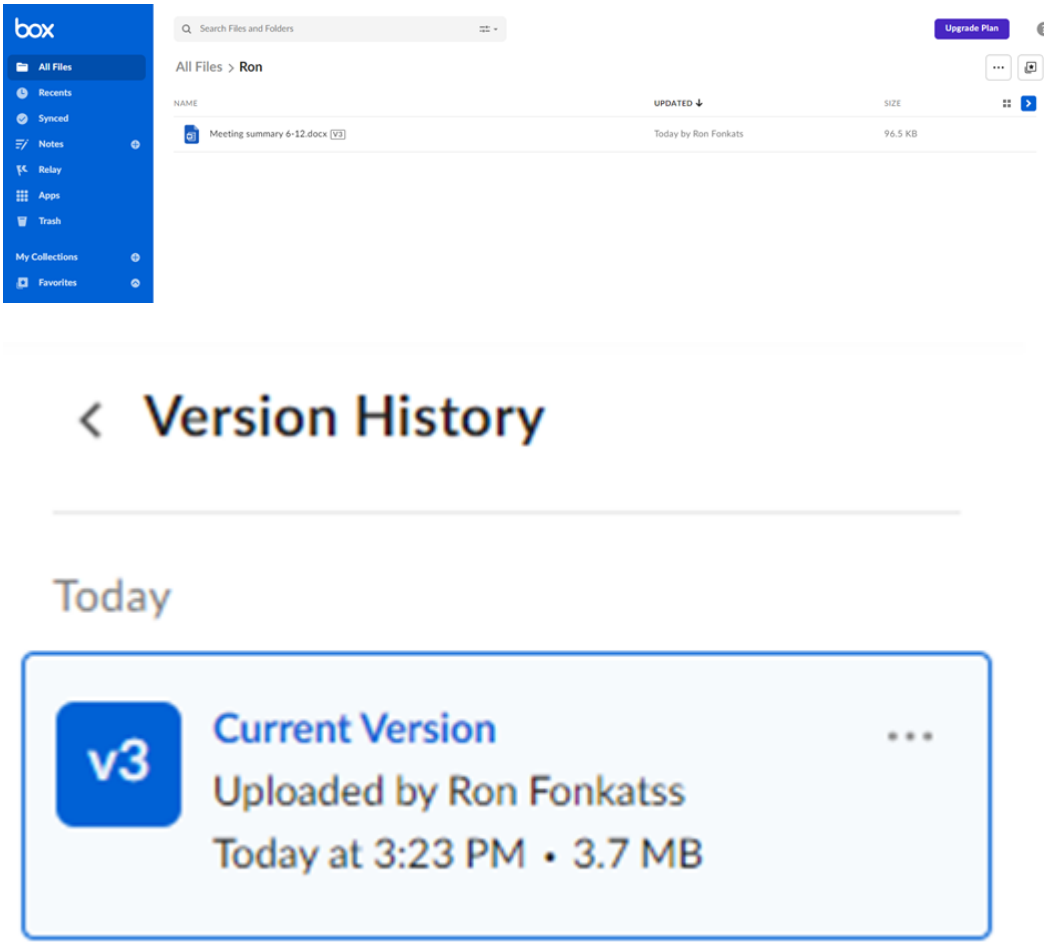
Each file that an authorized user uploads to Box will be automatically send to sanitization. When the user uploads a file, Box will display a message:

After the sanitization is successfully completed, the original file will be replaced with the sanitized file, and Box will display a message indicating that a new version of the file was uploaded:



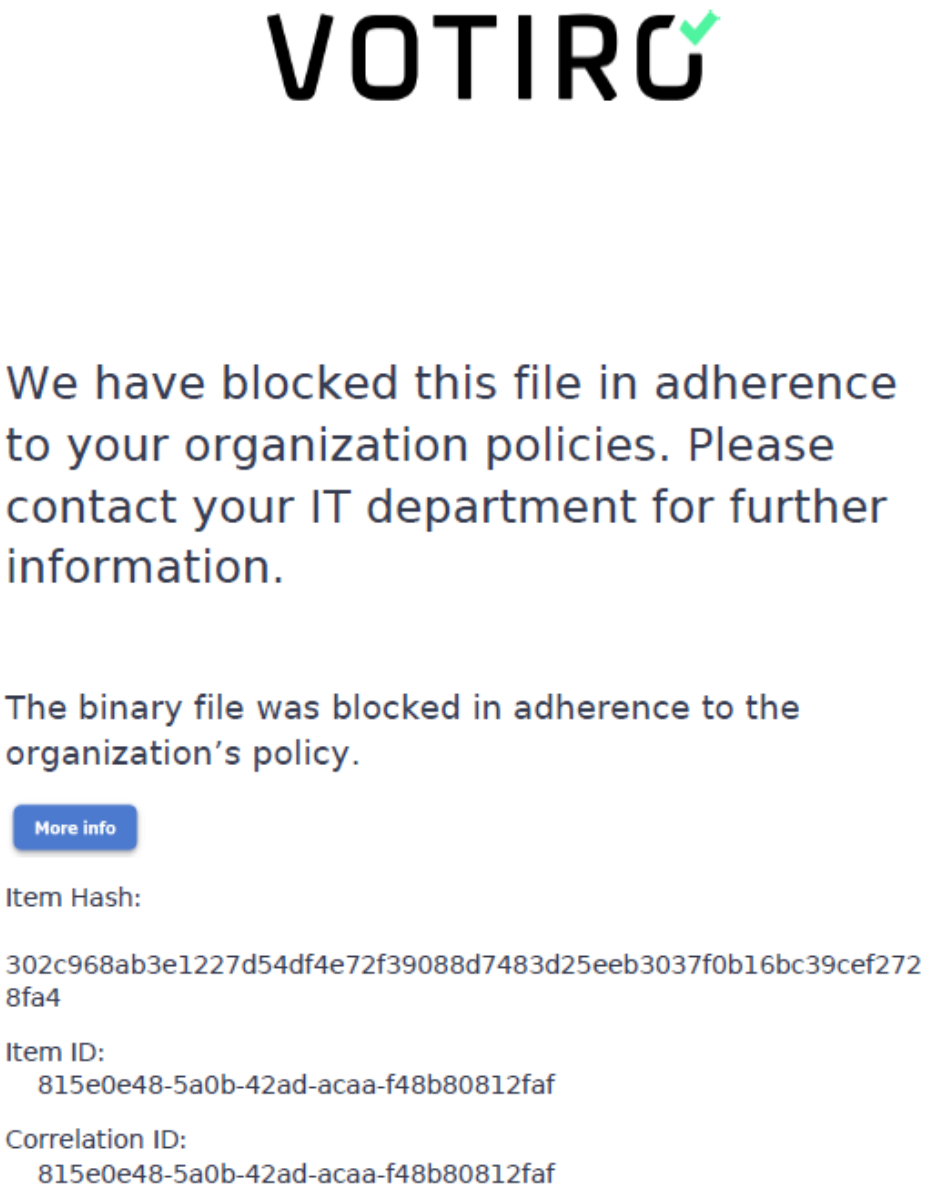
Box App Behavior when Versioning Files

- If an uploaded file was successfully sanitized, the sanitized file will be marked by V3:



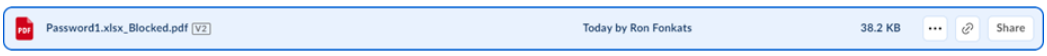
- If the uploaded file was blocked, a blocked PDF file appears marked by V2:

The contents of the blocked file PDF will be similar to:



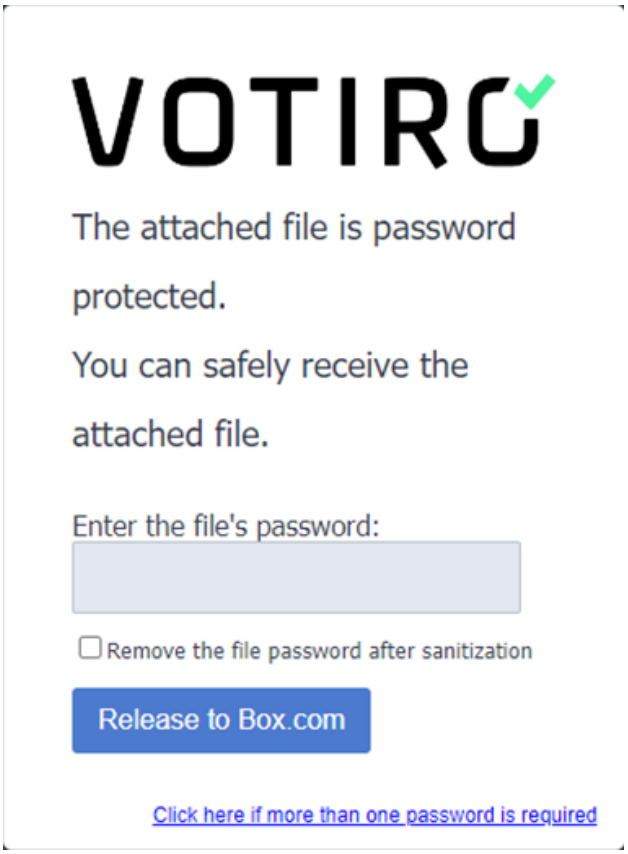
Box App Behavior for Password Protected Files

If the user uploaded a password protected file, the original file will be replaced with a password protected blocked PDF marked by V2:

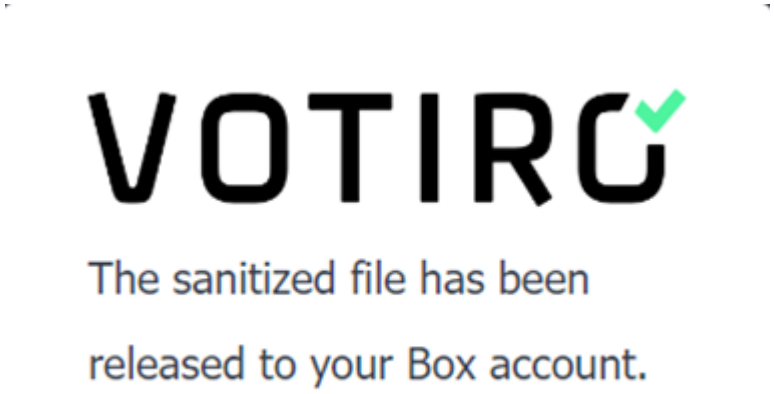


To release a password protected file that was blocked:

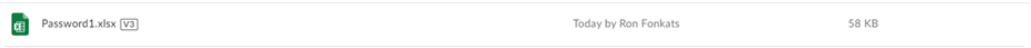
1. Click on **I have a password** in the blocked PDF. The password protected portal is displayed:



2. Enter the file's correct password and click on **Release to Box.com**. Votiro displays the message:



The sanitized file appears in Box marked by V3:

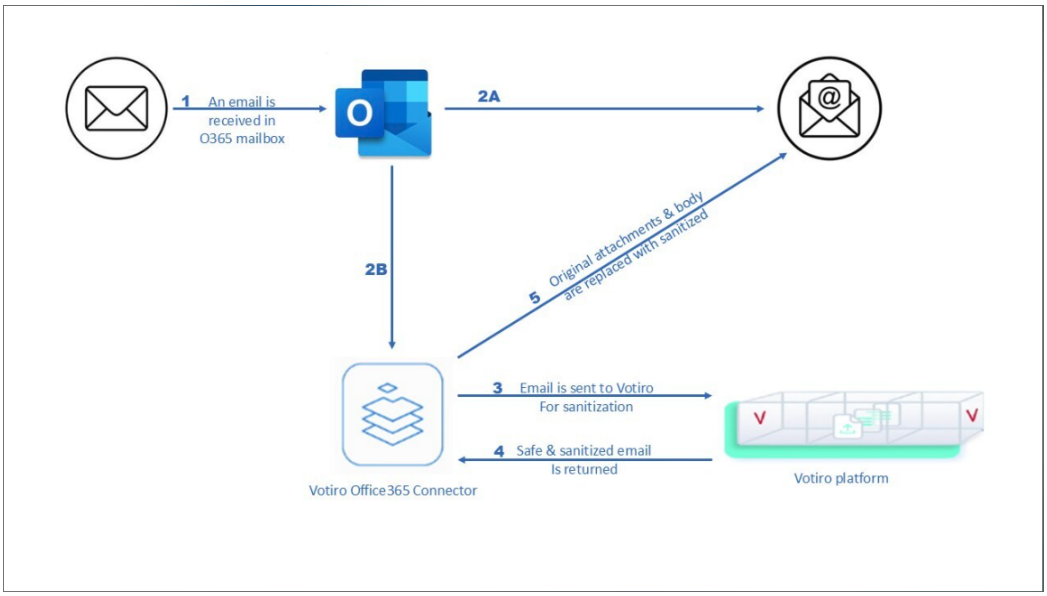


Limitations

Sanitization of uploaded files by external users is not supported.

2.17.4 Office365 Mail

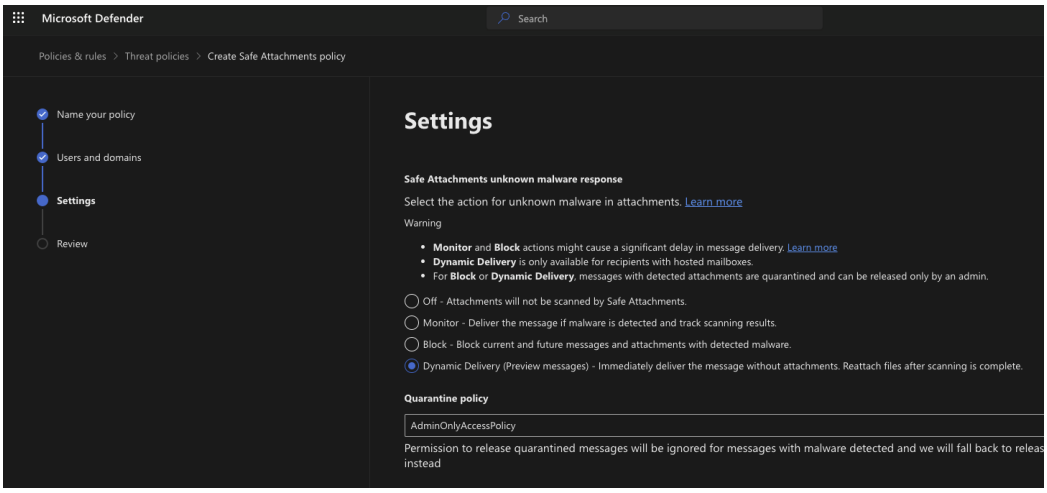
Office365 High-level Workflow



Office365 Integration Limitations

- Office365 native integration does not update emails using an Apple native client (as opposed to Outlook for Mac/iPhone).

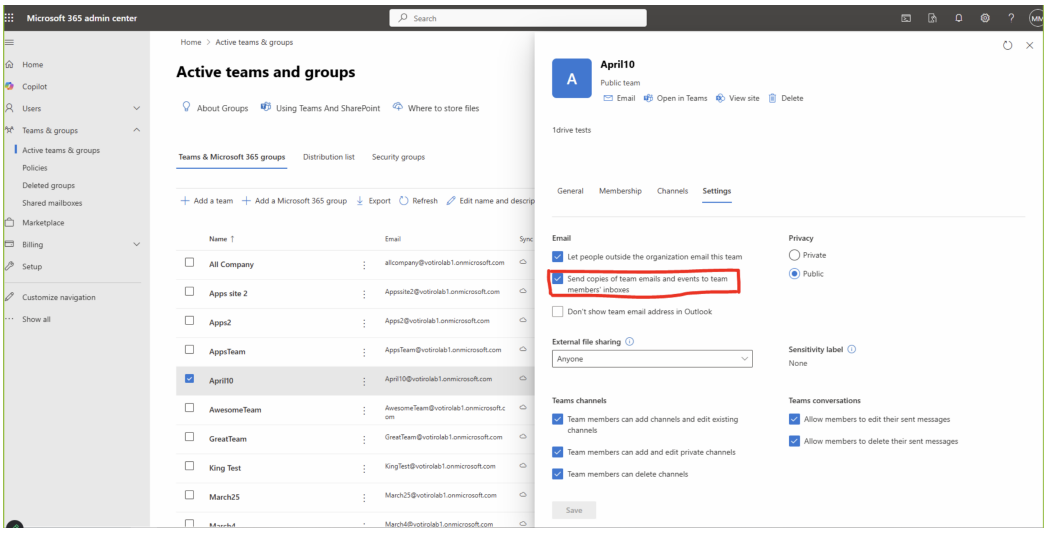
- If you are using Microsoft Defender for Office 365 (previously known as Office 365 ATP), enabling **Dynamic Delivery** can cause missing attachments when using Votiro. Consider selecting the **Monitor** or **Block** option instead:



- When sending an email to a Microsoft 365 group, it can either be delivered individually to each group member's mailbox or appear as a single copy in the group's dedicated folder, depending on the group's configuration. This behavior is determined by the setting explained in the Microsoft documentation: Send copies of group conversations to group members' inboxes.

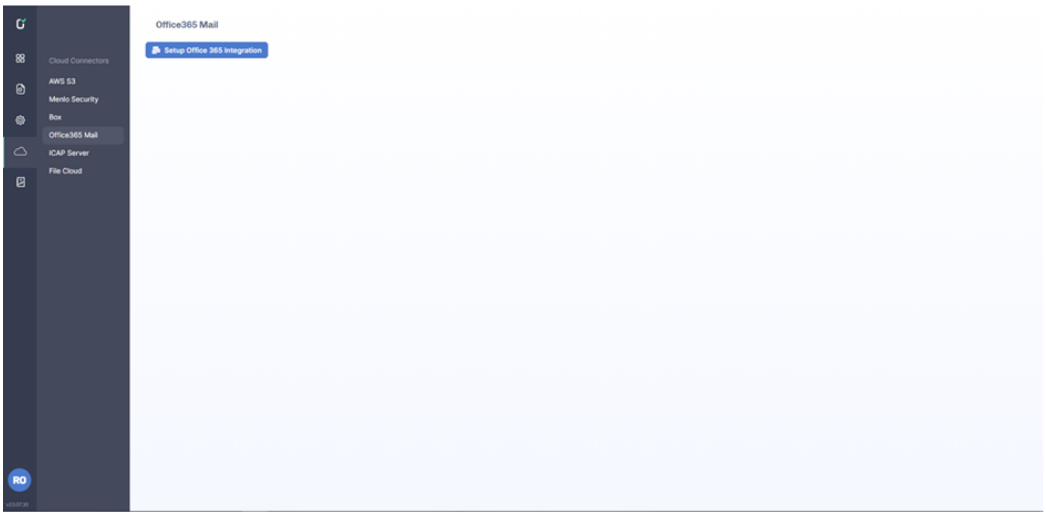
If the setting "Send copies of group conversations and events to group members" is enabled, and the group members are protected, Votiro will receive individual notifications for each recipient, and the email will be sanitized accordingly. For example, sending a message to Apps@votiro.com results in multiple items appearing under Prod US.

However, if this setting is disabled, Votiro does not—and cannot—receive notifications for those messages. In such cases, the message is stored in the group's folder as part of a Microsoft resource type called a *conversation*, which our application permissions do not allow us to monitor or subscribe to for notifications. In this case, sending a mail with a suspicious link to a protected group results in the file not being blocked. When sending a mail with a suspicious link to a protected group, the file is not blocked. See Create subscription.



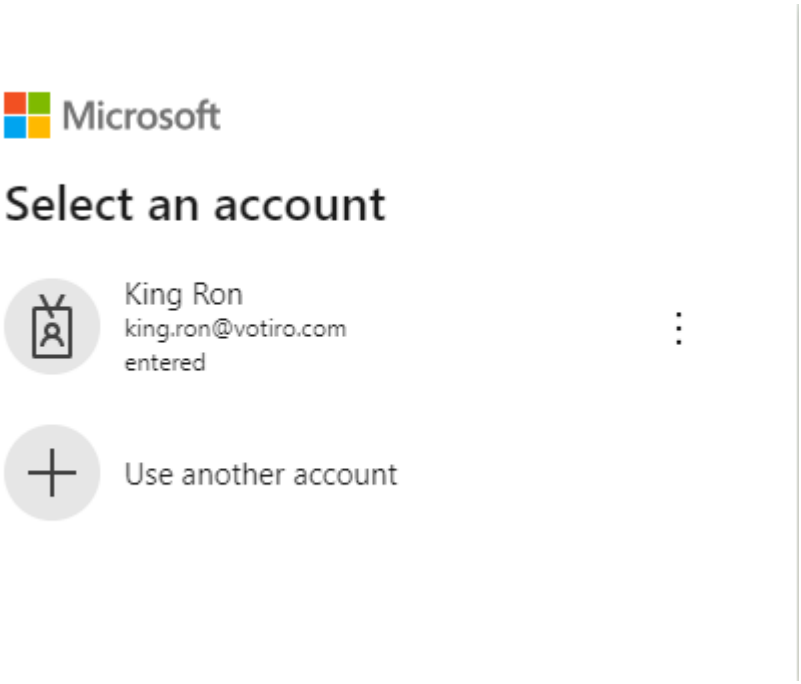
Office365 Integration Procedure

1. Enter the Management Console as the Admin of Office365 Mail and navigate to **Cloud Connectors and Integrations** > **Office365 Mail**.

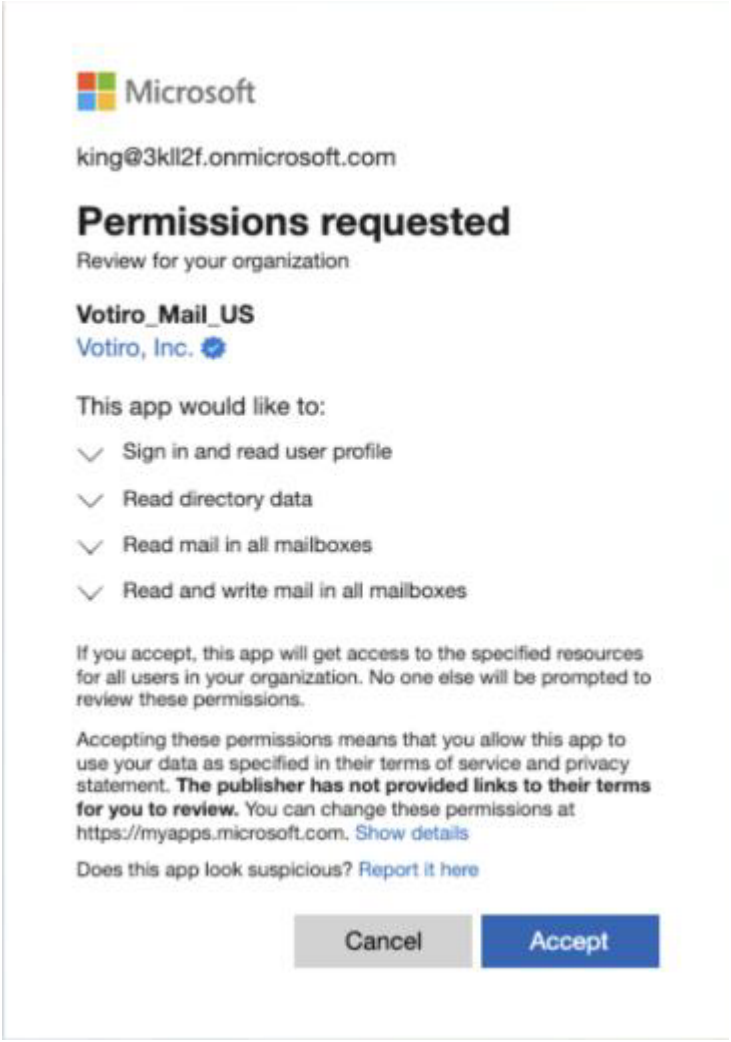


2. Click on the **Setup Office 365 Integration** button. The Votiro product will be redirected to Microsoft user authentication.

3. Select your Admin account.

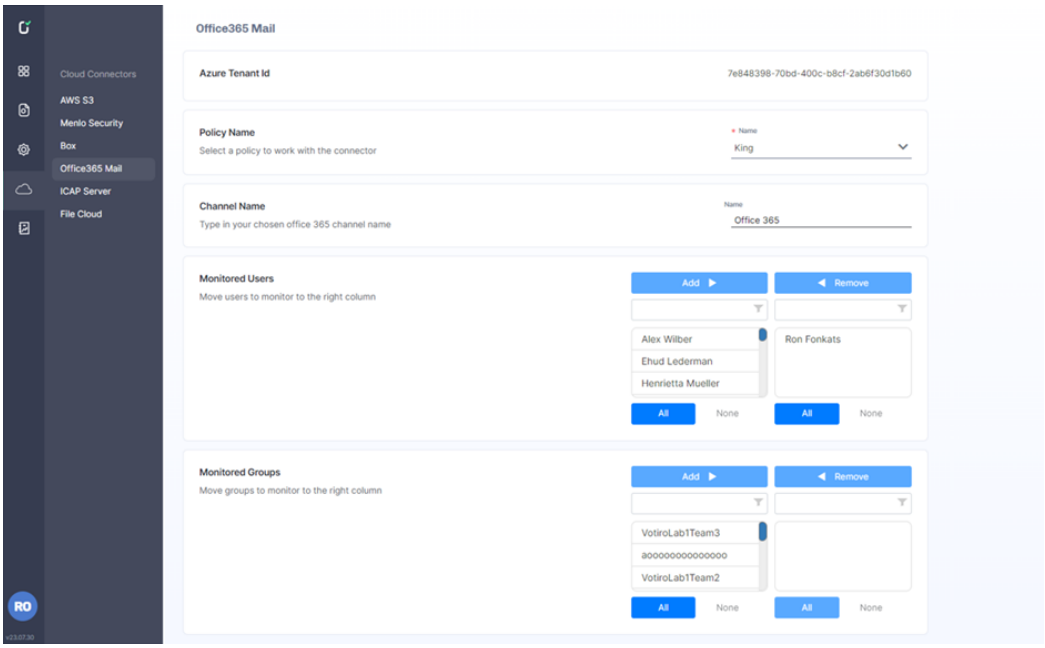


4. After authenticating with the selected Admin user, approve Votiro product permissions and click on **Approve** to complete the successful integration.



5. After successful integration, the Votiro Management console will display the Office365 Mail configuration screen.

Office365 Configuration



The **Office365 Mail** page contains the following fields:

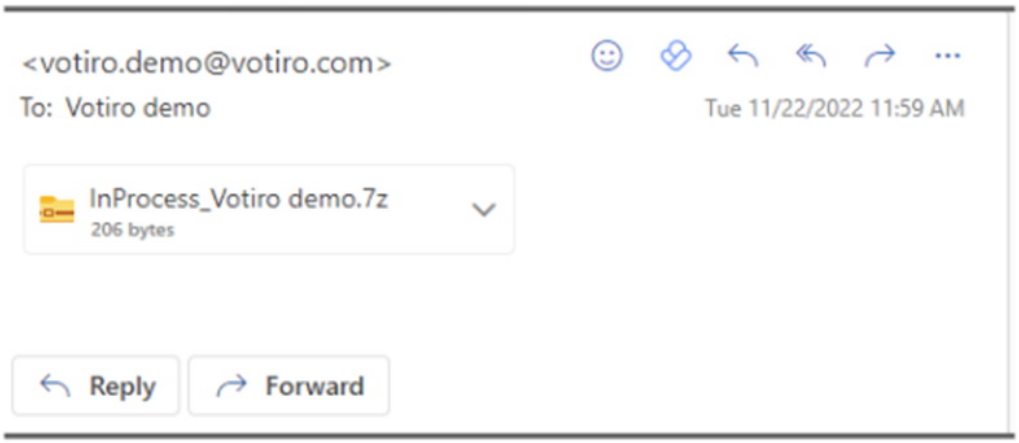
Element	Field	Description
1	Azure Tenant Id	The organization's Azure Tenant ID **Note**: This field cannot be changed.
2	Policy Name	Specify a policy for the Office 365 connector to work with. Select the **Default Policy** policy if you have not created an alternative policy to use.
3	Channel Name	Specify the name of your channel. The channel name appears on the Incidents page as the name of a connector.
4	Monitored Users	The left column will contain all users under the Azure tenant account. To authorize specific users to be able to sanitize files, select the users from the left column and click Add. To deny sanitization authorization to specific users, select the users from the right column and click Remove. To add/remove all/no users, click the All/None buttons in the respective column.

Element	Field	Description
5	Monitored Groups	The left column will contain all groups under the Azure tenant account. To authorize specific groups to be able to sanitize files, select the groups from the left column and click Add. To deny sanitization authorization to specific groups, select the groups from the right column and click Remove. If a group is enabled/disabled for sanitization, all the group users are enabled/disabled even if the group users were not enabled/disabled in the Monitored Users field. **Note**: ■ Only Microsoft 365 Groups are presented. ■ Distribution List and Security Groups are not presented.

1. Select a **Policy Name** from the given options. You can define a new policy from the **Policies** tab. In the example above, the **Policy Name** is "Office 365 Policy".
2. Type a **Channel Name**. In the example above, the **Channel Name** is "Office 365".
3. When finished making changes, click on **Save Changes**.

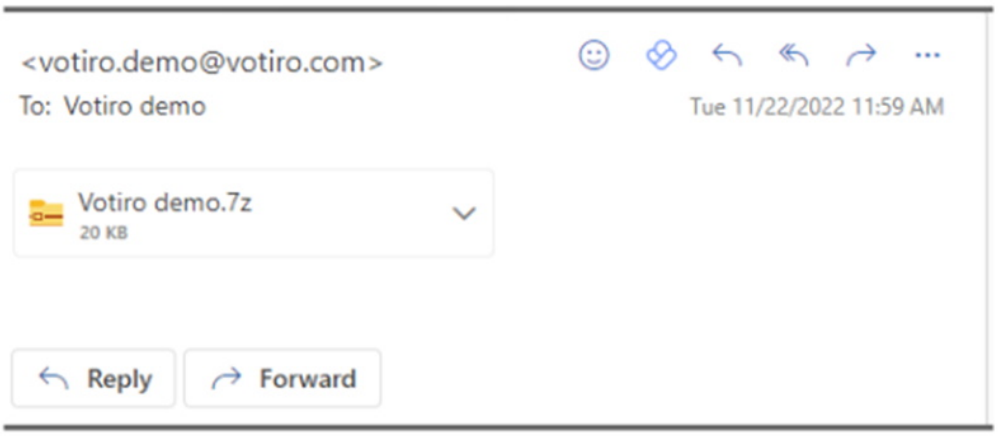
Office 365 Behavior when using the Votiro Office 365 App

1. When sending email with attachments to the protected users/groups, the attachments will be sent to the Votiro engine for sanitization.
2. While the attachments are undergoing sanitization by Votiro, the recipient's mailbox attachment will be replaced with an **InProcess_***<filename>* attachment:

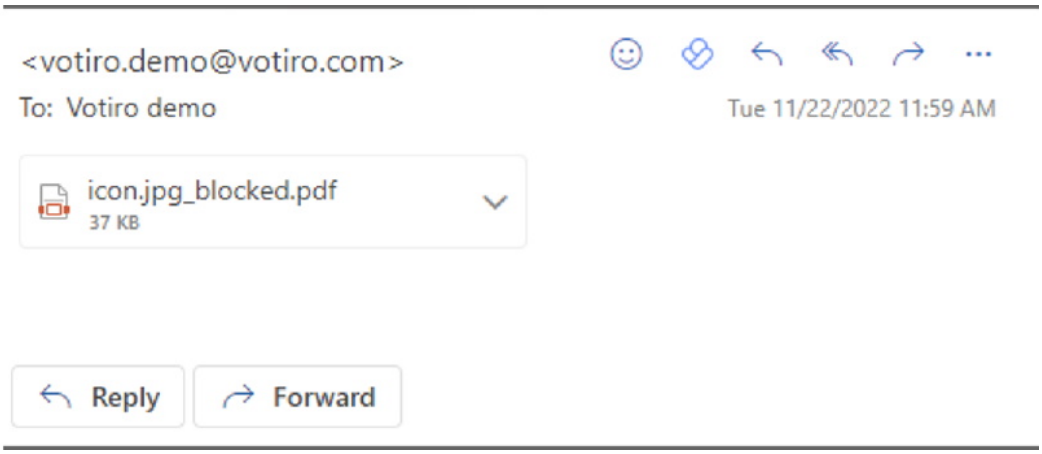


3. After the attached file completes the sanitization processing, the results are displayed.

a. If the attachment was sanitized successfully, the sanitized file will be displayed in the mailbox:



b. If the attachment was blocked, a blocked PDF file will replace the original attachment.



4. The sanitization rate is a maximum of 6900 emails per hour.

Note: There may be a delay before the client receives the sanitized attachment or blocked PDF, due to:

1 In Office 365, Votiro receives the email at the same time the client gets it.

2 Then we sanitize the file and replace the file (on the Microsoft Office 365 server).

3 Once the client "refreshes" the attachment, they will get the sanitized version or blocked file.

4 Till then, it all depends on the client, and we have no control over it (some clients will go to the server on every click, some will do it periodically).

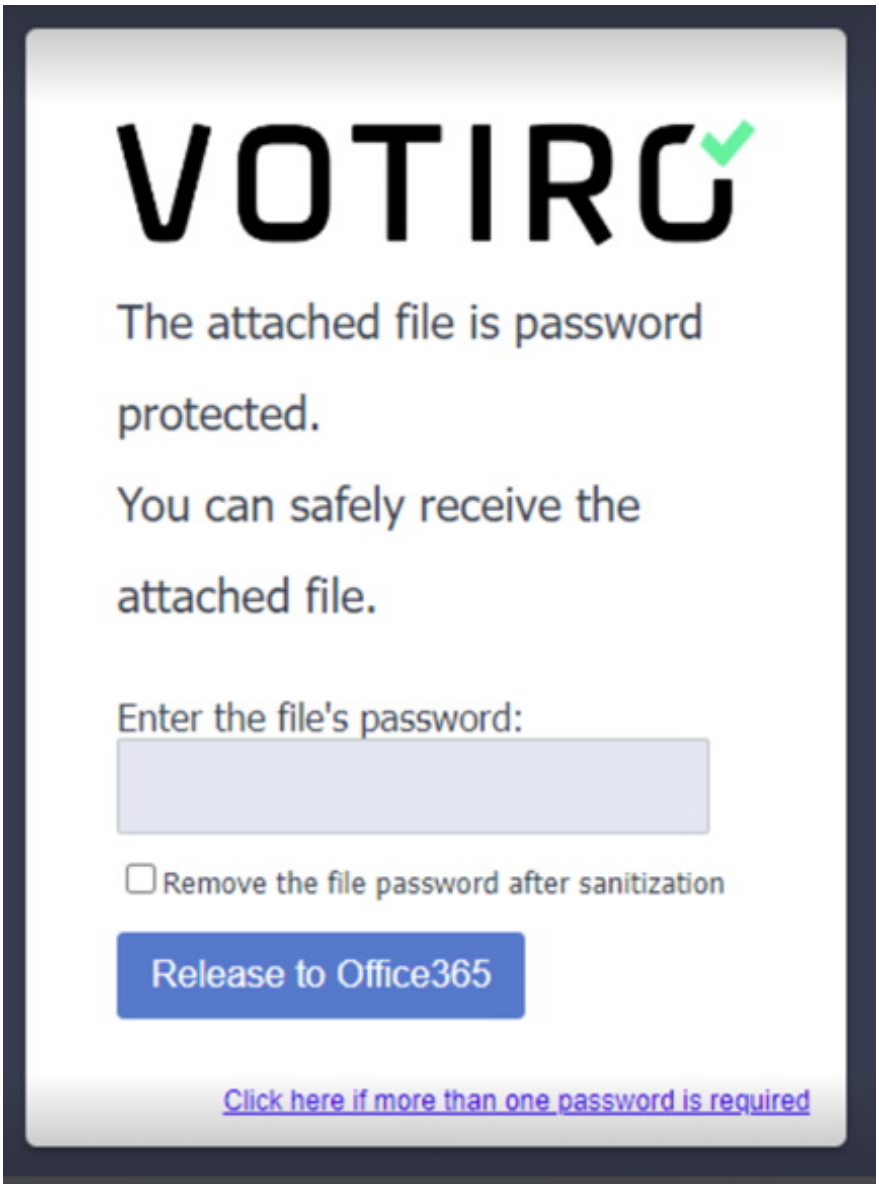
5 For some clients, it will take a while until the client will re-query the server and get the blocked PDF.

Office 365 App Behavior for Password Protected Files

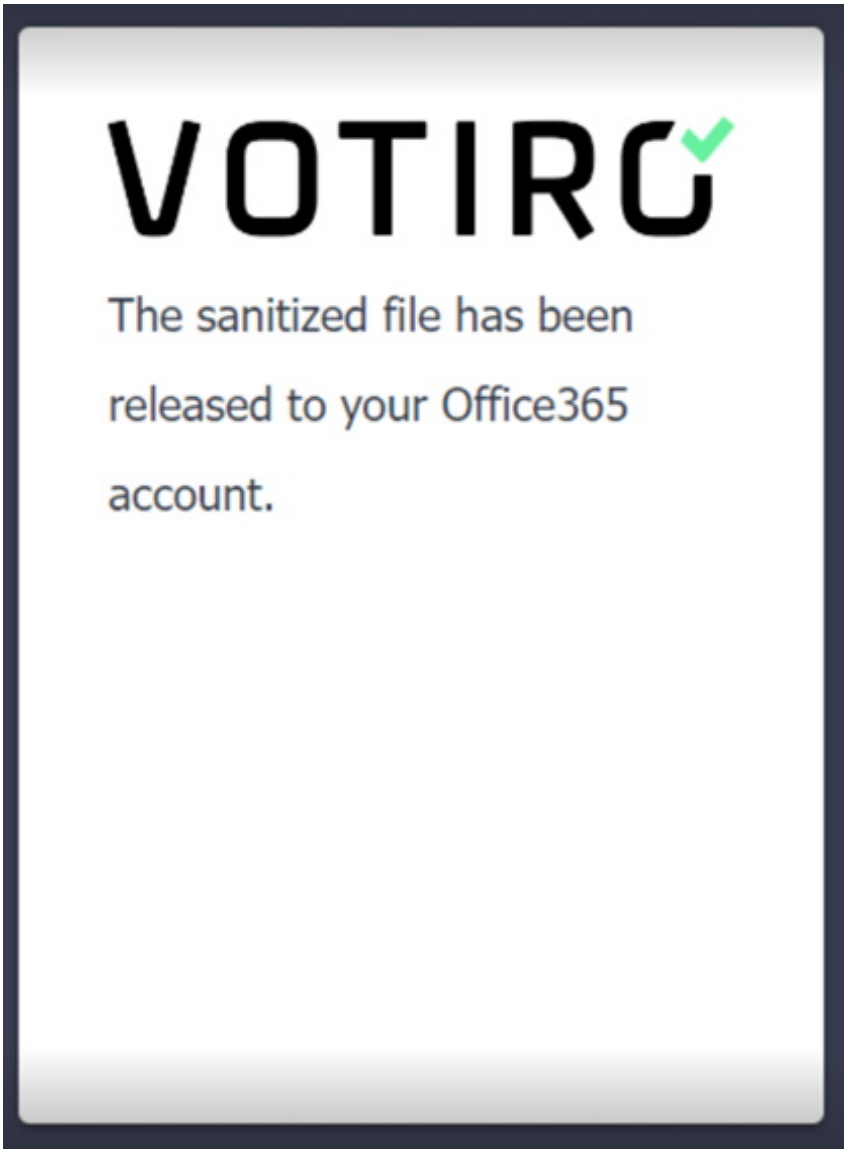
1. If the user receives an email with an attached password protected file, the attached file will be replaced with a password protected blocked PDF.

2. To release a password protected file that was blocked:

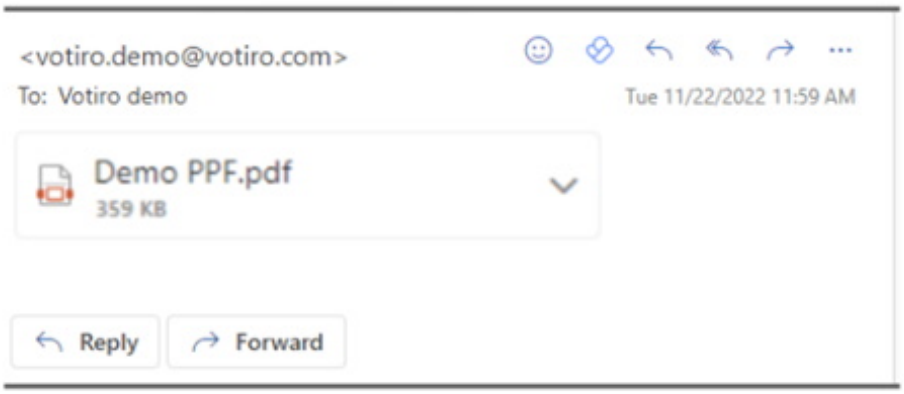
a. In the blocked PDF, click on **I have a password**. The password protected portal is displayed:



b. **Enter the file's password** and click on **Release to Office 365**. Votiro displays the message:



c. **The attachment will be replaced with the sanitized password protected file:**



2.17.5 Microsoft Teams

Overview

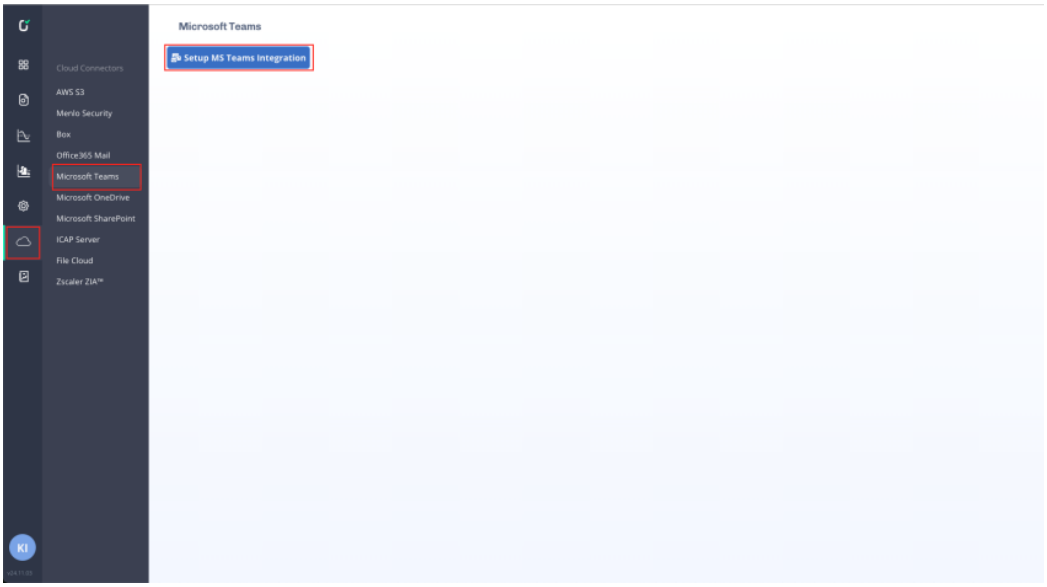
Experience seamless file sharing and robust security within MS Teams, now available with a quick and easy setup and complemented by advanced analytics for actionable insights, designed for stability and reliability to enhance your collaboration workflow.

Prerequisites

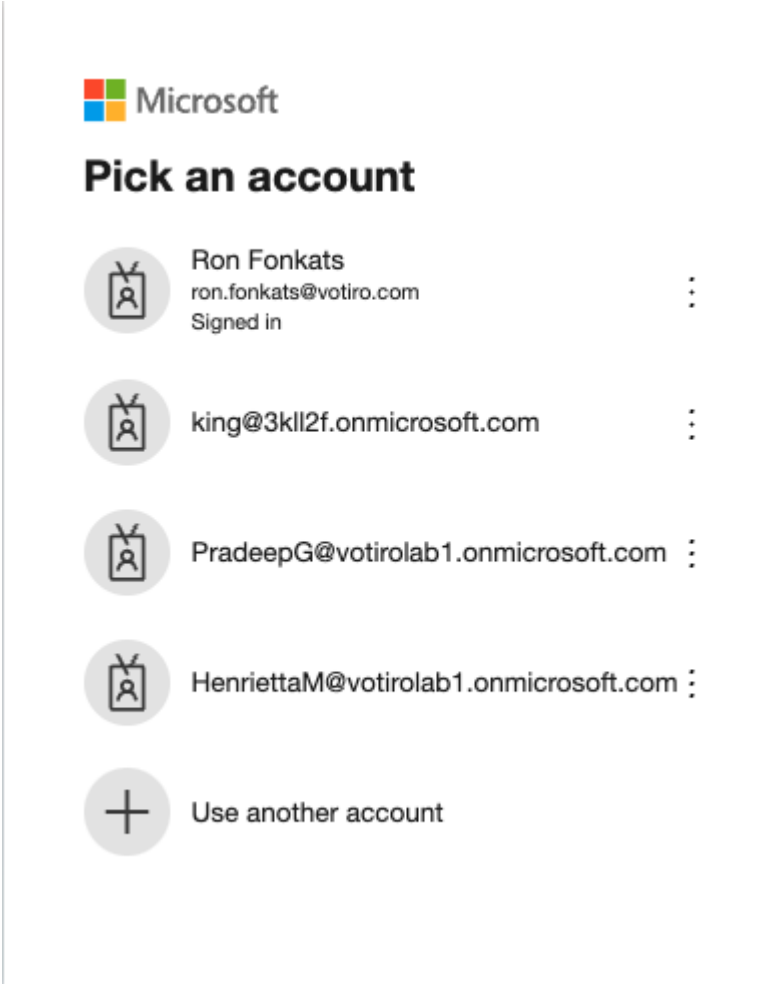
Only an admin with full privileges can setup integration.

Microsoft Teams Integration Setup with Votiro

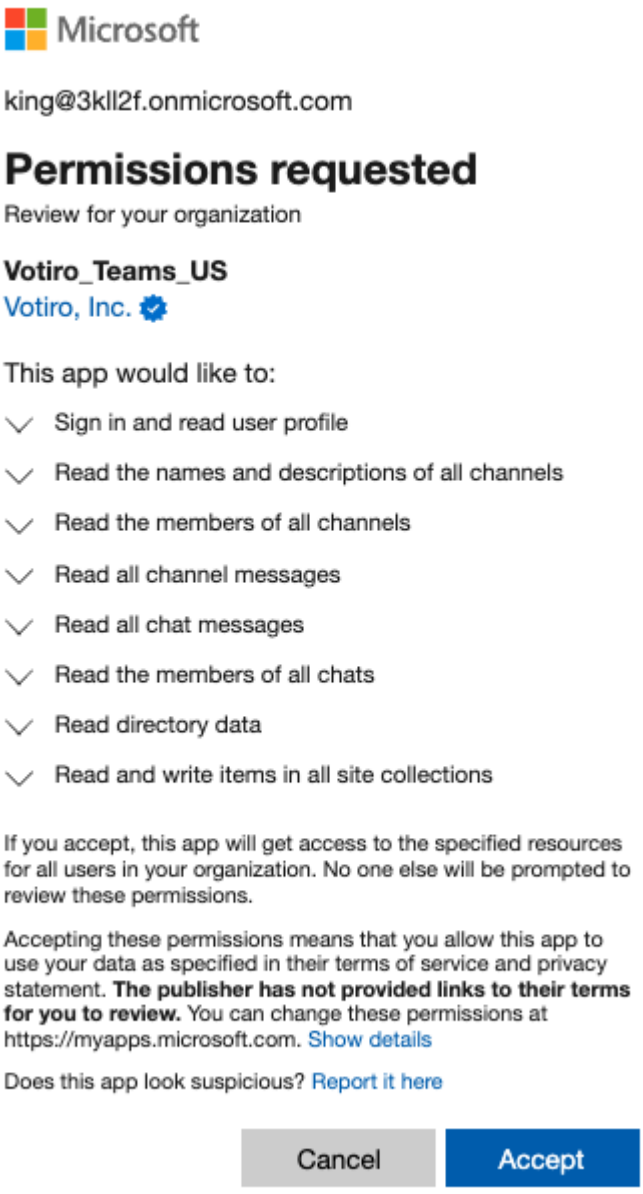
1. Navigate to to the Votiro Management console > **Cloud Connectors** > **Microsoft Teams** and click on **Setup MS Teams Integration**.



2. Pick an Admin account and perform Microsoft Authentication:



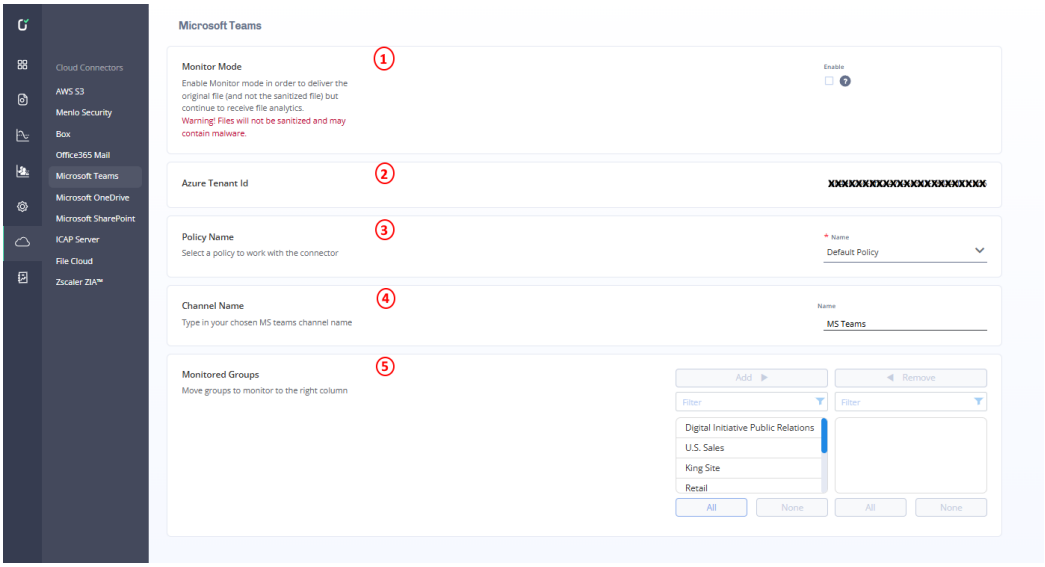
3. **Accept** the requested permissions.



4. After successful integration, the user will be led to MS Teams configuration page.

Configuration of Teams in the Votiro Management Dashboard

To get to the Teams page, from the navigation pane on the left, click **Cloud Connectors** > **Microsoft Teams**.



The **Microsoft Teams** page contains the following fields:

Element	Field	Description
1	Monitor Mode	Default - disabled (unchecked). If Monitor Mode is enabled, the original unsanitized file is received, but file analytics are available. **Note**: If Monitor Mode is enabled, files will not be sanitized and may contain malware. To enable Monitor Mode, contact Votiro support.
2	Azure Tenant Id	The organization's Azure Tenant ID **Note**: This field cannot be changed.
3	Policy Name	Specify a policy for the MS Teams connector to work with. Select **Default Policy** if you have not created an alternative policy to use.
4	Channel Name	Specify the name of your channel. Default - MS Teams
5	Monitored Groups	The left column will contain all groups under the Azure tenant account. To authorize specific groups to be able to sanitize files, select the groups from the left column and click Add. To deny sanitization authorization to specific groups, select the groups from the right column and click Remove. If a group is enabled/disabled for sanitization, all the group users are enabled/disabled even if the group users were not enabled/disabled in the Monitored Users field. By default no group is protected. **Note**: Only Microsoft 365 groups that have Teams enabled are presented.

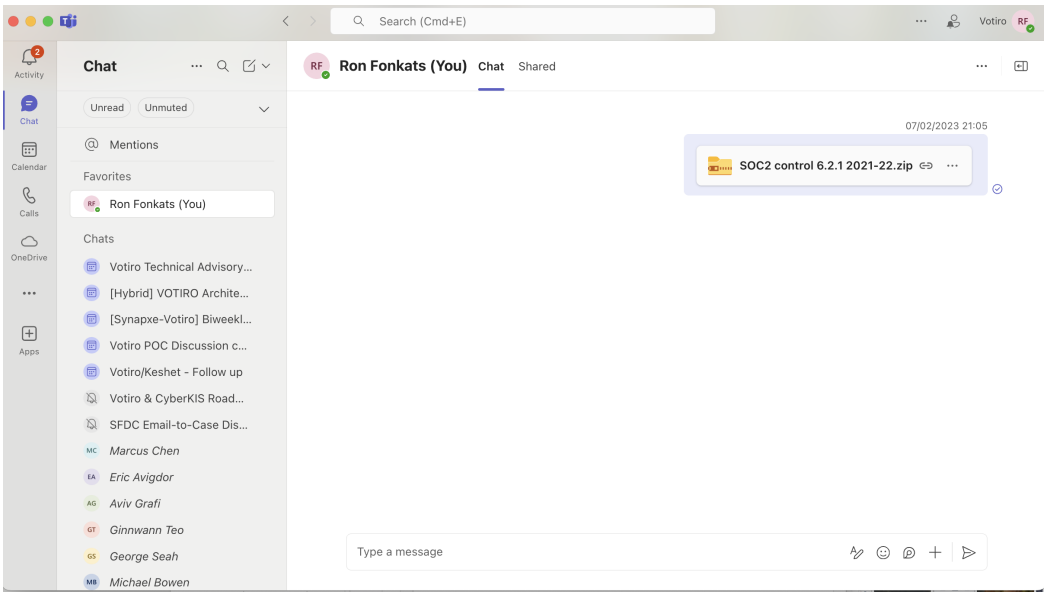
Obtaining full file upload functionality

To obtain full file upload functionality with MS Teams, you must also configure OneDrive to work together with MS Teams. The customer needs to set protected groups in Teams and also set protected users in OneDrive.

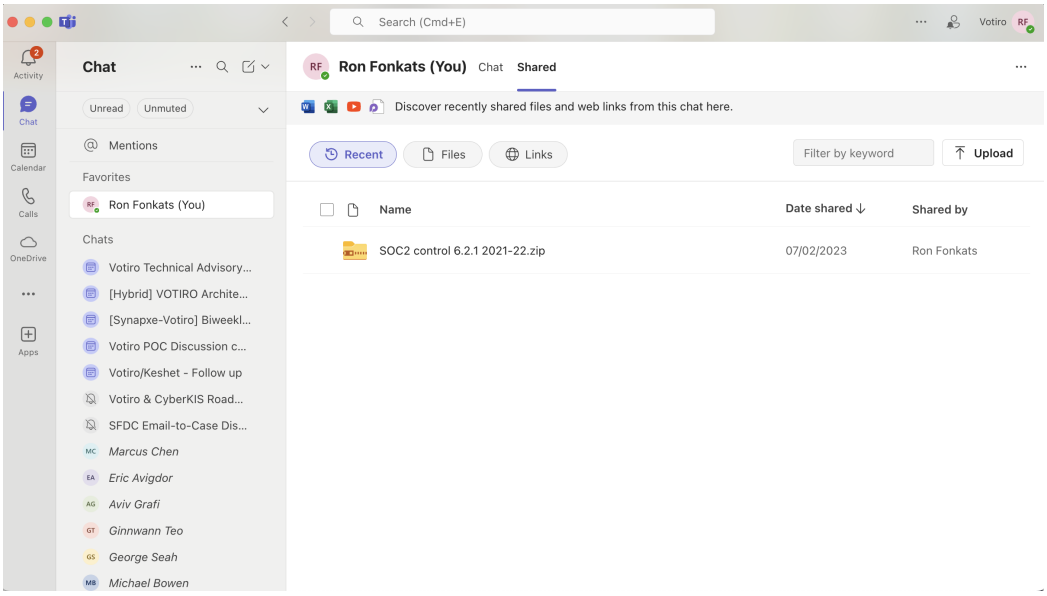
See the Chat and Channel use cases below and how to address them by adding the right connector and protected list.

Chat

- Upload a file to the **Chat main screen**. The Teams connector will handle it.

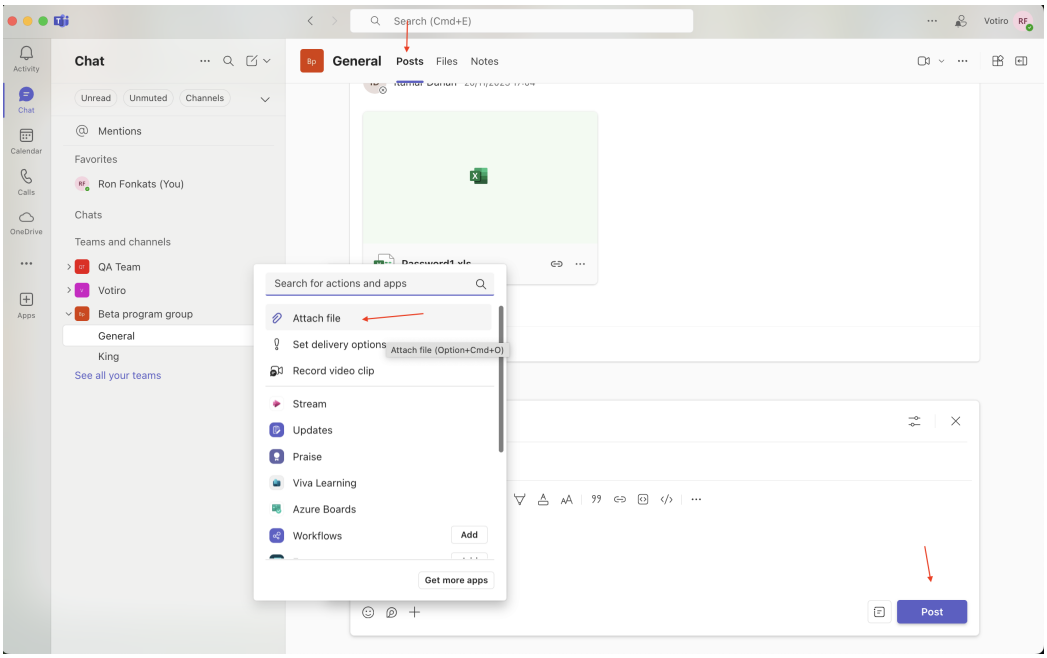


- Upload a file to the **Chat Shared screen**. The Teams connector will handle it.

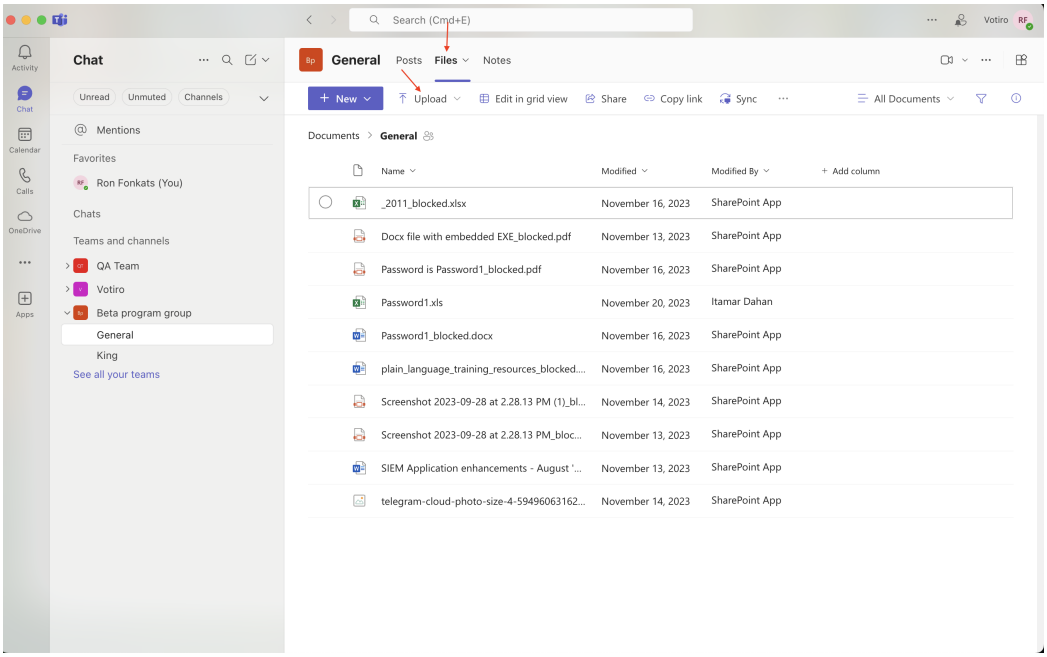


Channel

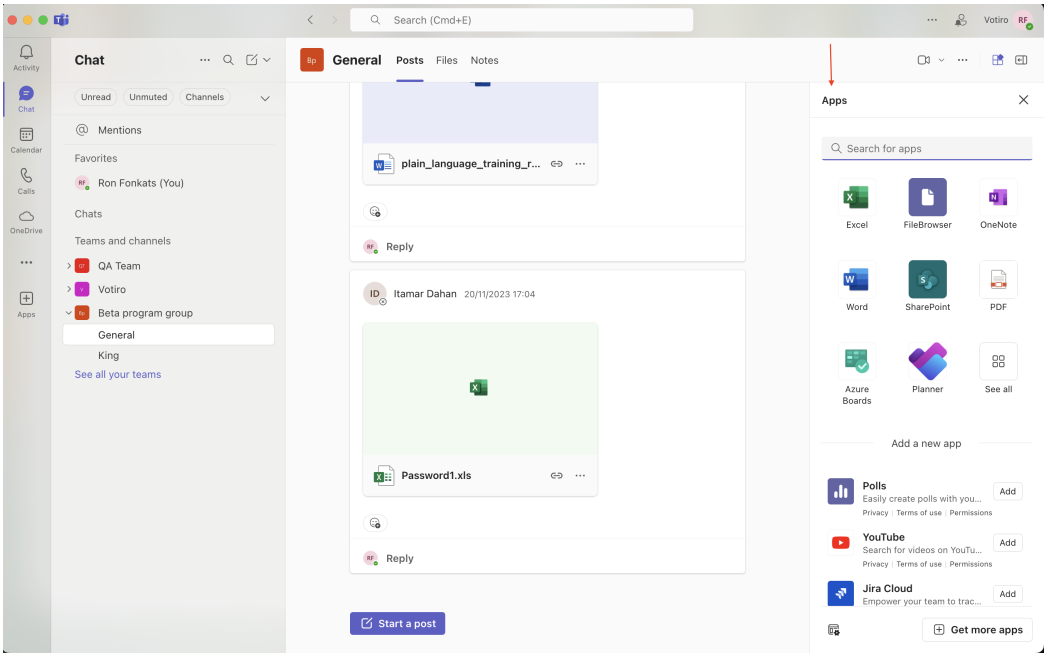
- Send a post using the **Posts** screen. The Teams connector will handle it.



- Upload files to the **Files** screen. The SharePoint connector will handle it.



- Create a new file using **Apps**. The SharePoint connector will handle it.



Working with external users

The following use cases apply when sending/receiving to/from external users.

Sending files to outside the organization (Internal user to External user)

- Protected internal user sends files in chat to an external user - **Supported**
- Protected internal user sends files in the channel to an external user (inside the organization channel) - **Supported**
- Protected internal user sends files in an external channel to an external user (outside the organization channel) - **Currently not supported**

Receiving files from outside the organization (External user to Internal protected user)

- External user sends files in chat to internal user - **Currently not supported**
- External user sends files in an external channel to an internal user - **Currently not supported**
- External user sends files in an internal channel to an internal user - **Supported**

Workflow

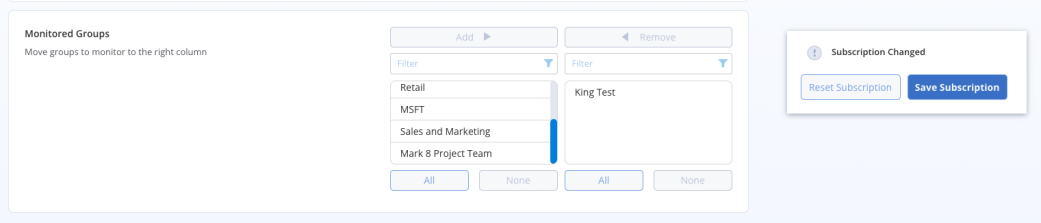
Protected groups

To start protecting MS Teams organization groups, select which groups will be monitored by Votiro. The Monitored Groups has two columns:

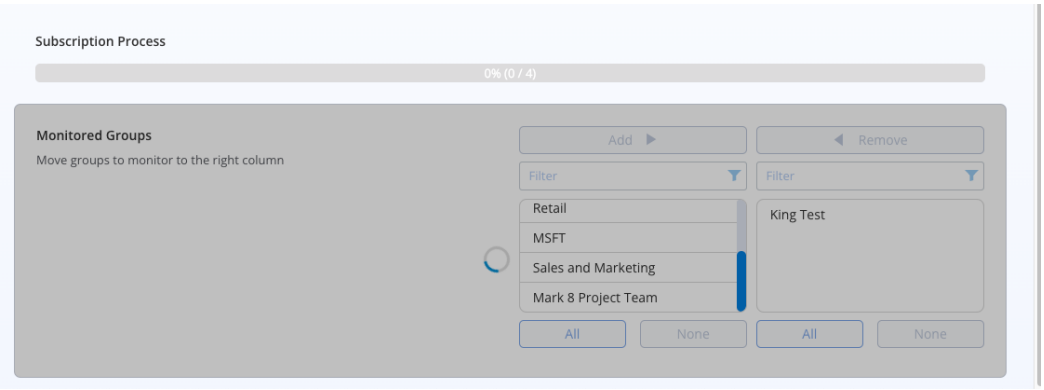
- Available groups (left column)
- Monitored groups (right column)

To set monitored groups, select from the available groups and:

1. Click on **Add**.
2. Click on **Save Subscription**.



3. After saving the subscription, Votiro will protect each group member. There will be an indication of the subscription process:



4. After adding the groups, the selected groups will move to the **Monitored Groups** (right) column.
5. To remove monitored groups, selected the desired groups from the right column and click on **Remove**.

Sanitization process

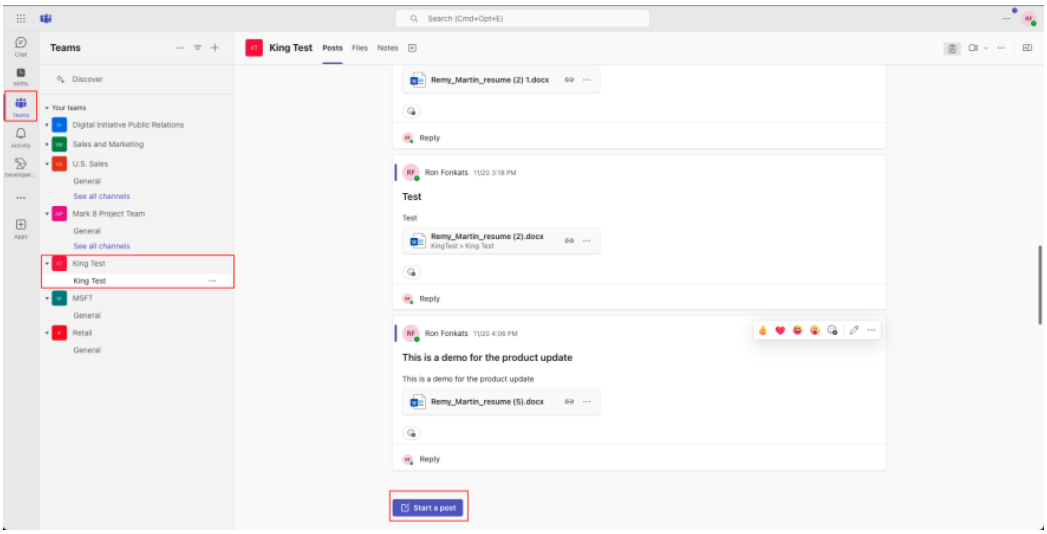
Once a group becomes Monitored, sanitization will be activated when uploading files to MS Teams for each group member.

The sanitization will be applied to:

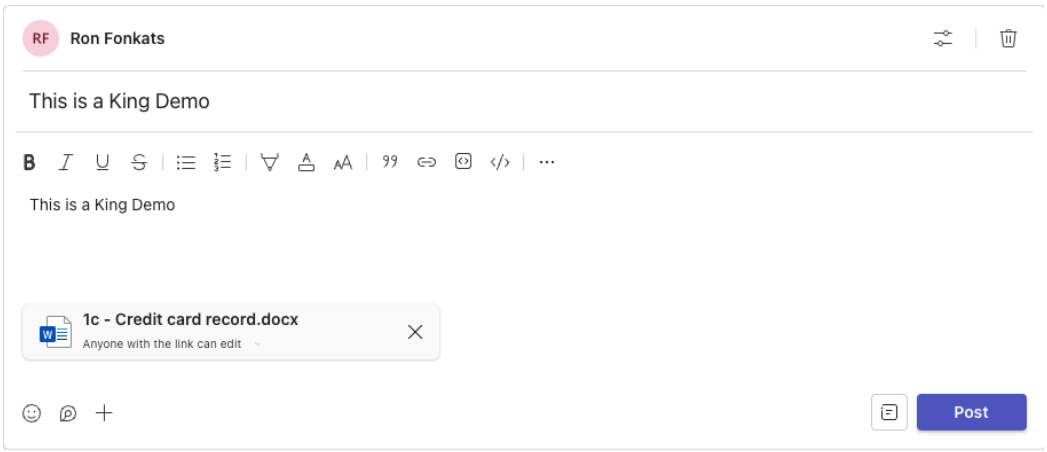
- Channels
- Chats

The following example illustrates sanitization of a channel post.

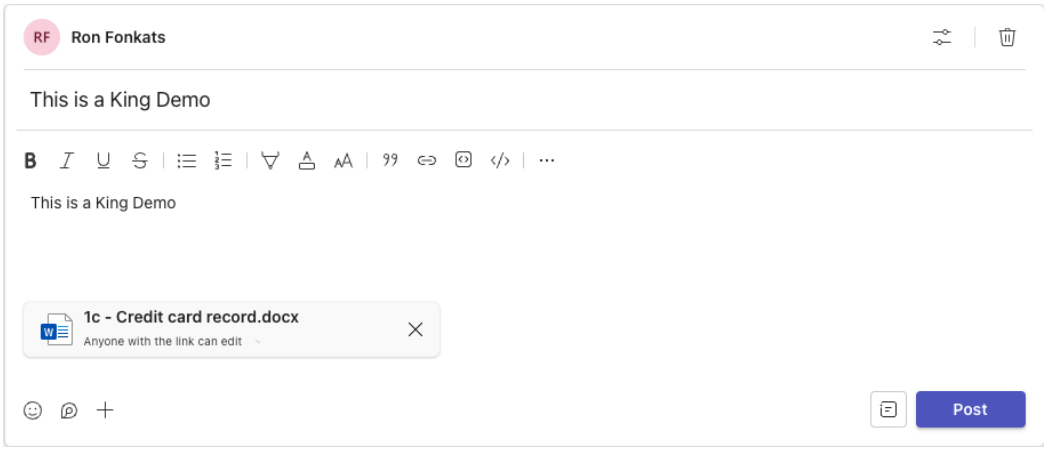
1. Start a new post:



2. Attach a file to the post:

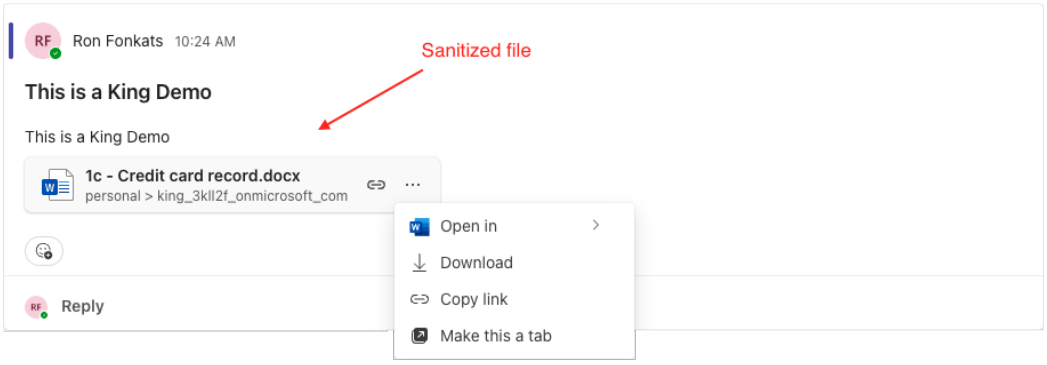


3. Post a message:

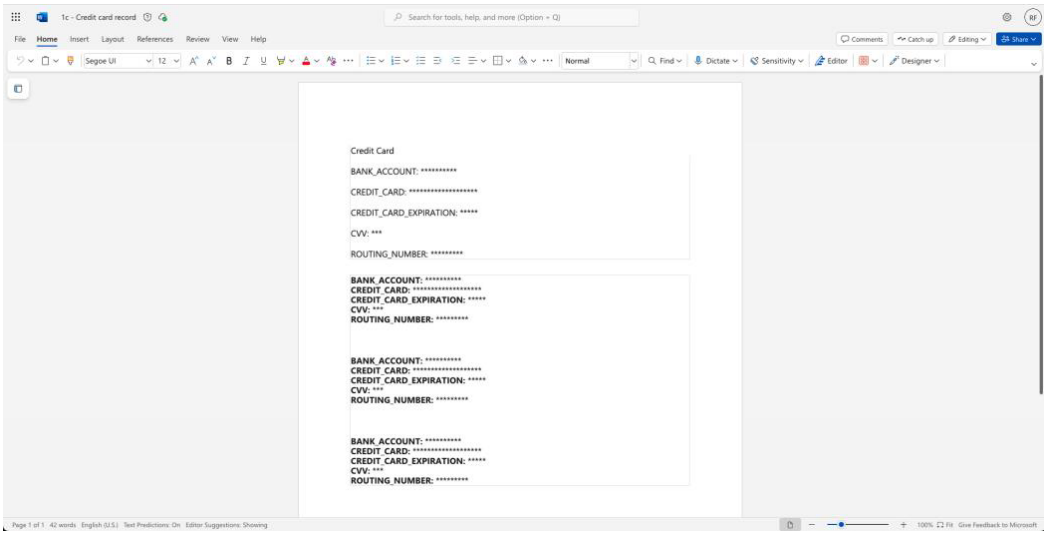


4. From the moment the file is posted in the channel, the file will be sent for sanitization in a matter of seconds.

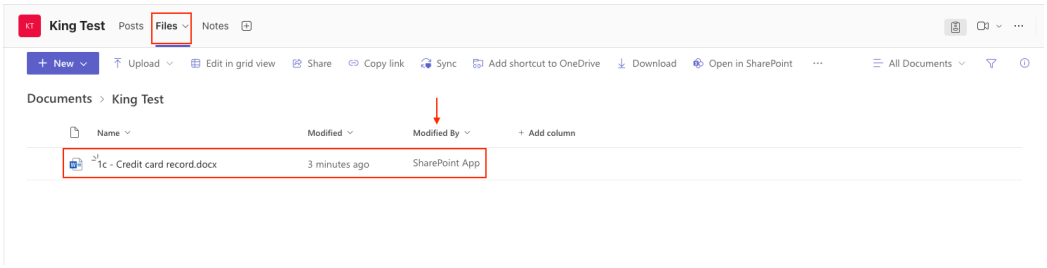
5. After sanitization has completed, the sanitized file will be replaced in the post message:



6. In the sanitized file version, if a file was detected with sensitive data, the sensitive data is masked according to organization policy:



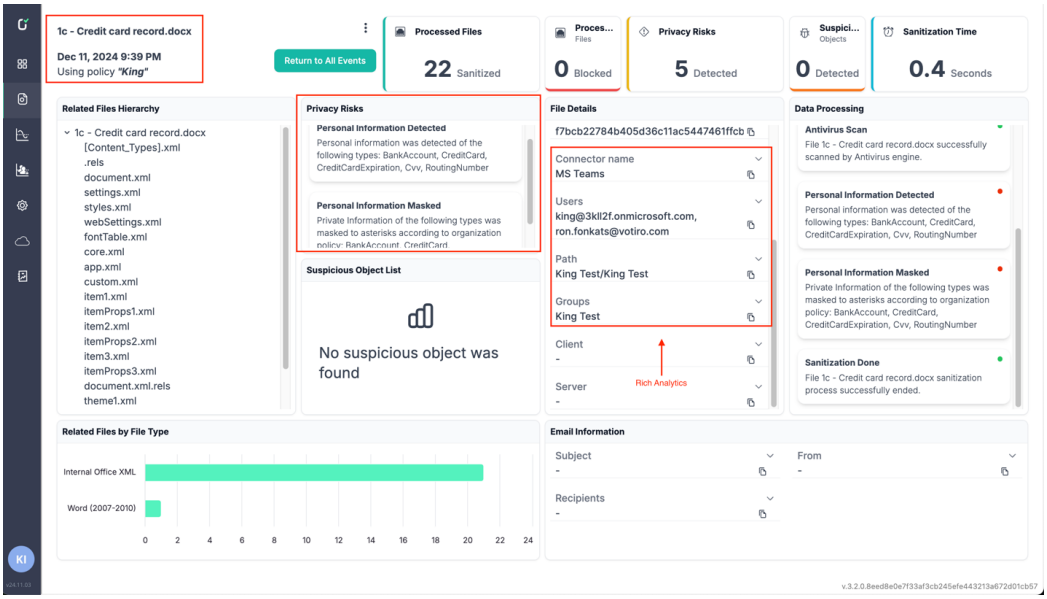
7. To verify that the file is indeed the sanitized version, the user can browse to the **Files** tab. There is an indication that the file was modified by **SharePoint App** (= Votiro).



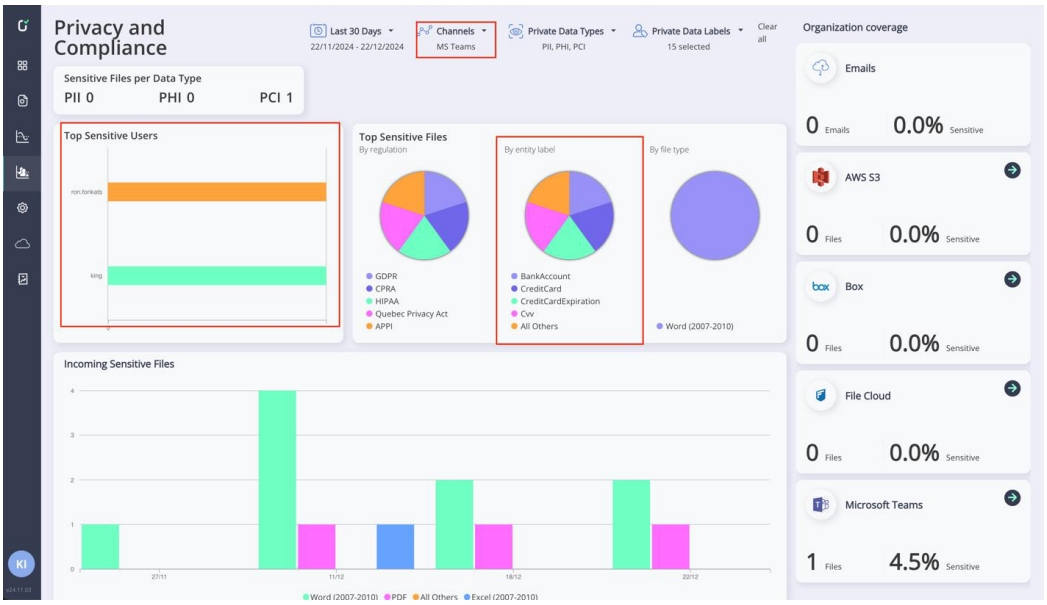
Votiro Analytics

File analytics are available from the:

- **Events** page



- **Privacy and Compliance Dashboard**



Limitations

- Sanitization is not supported when performing file actions “Copy” and “Move”.
- Sanitization is not supported for direct images in chat (with preview option).
- Sanitization is supported up to 100MB file size.
- A newly created team can take 10 minutes to be displayed in the initial setup.
- Communication sites are not supported.