VOTIRO

Votiro Cloud - VA On-premises V10.0

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.

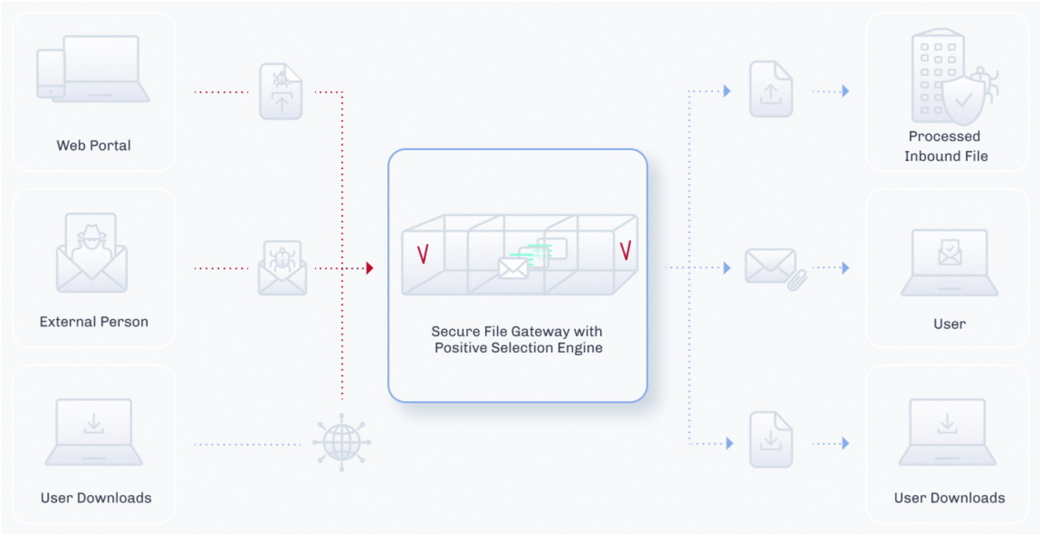
True Type Detection

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

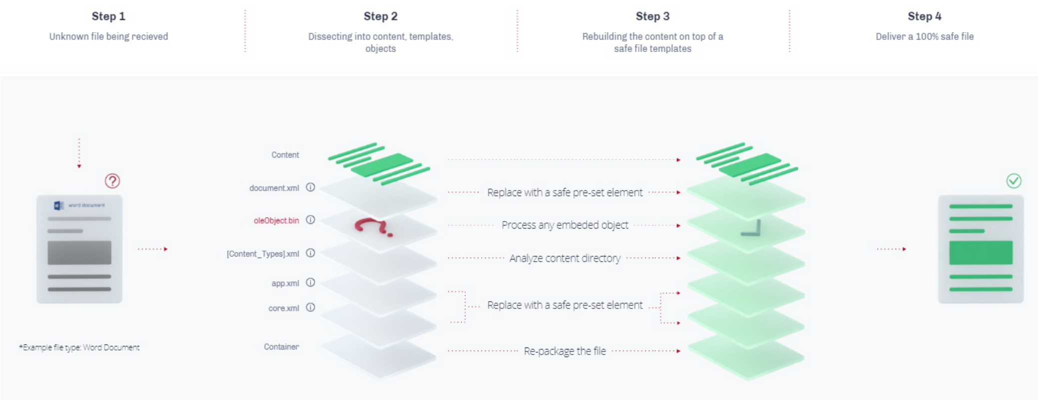
Votiro's Positive Selection® Engine is at the heart of the Votiro solution. The Positive Selection® Engine keeps only what belongs instead of searching for what does not belong.

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 On-prem. 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.

1.5 Votiro VA On-prem - Product Lifecycle Support

Votiro provides support on each release of VA On-prem for some time after issuing the next release of the product. The exact end of support dates are listed in the table below.

Customers should take into account Votiro's policies regarding enhancements and bug fixes:

- Enhancements will be applied to the next release only.
- Hot fixes will be provided for the supported versions. Other bug fixes will be applied to the next release only.

> **Note**:
> Votiro highly recommends that users regularly upgrade to the latest version of Votiro VA On-prem and not wait until the end of a release's support cycle.

Votiro VA On-prem Product Lifecycle Support

Version	Release Date	End of Support	Extended Support (Extra Fee)
v9.7	02 Jan 2023	31 Jan 2025 / v10.0 Release	31 Jan 2026
v9.9	12 May 2024	31 May 2026 / v10.1 Release	31 May 2027
v10.0	15 Sep 2025	TBD	
v10.1	ETA H1 2026		

2 Using the Management Dashboard

The Management Dashboard enables you to perform the following procedures:

- Monitoring Positive Selection Activity
- Events Dashboard
- Threat Analytics Dashboard
- Filter by Channels
- Cloud Connectors and Integrations
- Configuring Settings
- Generating Reports
- Password Protected Portal

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

2.1 Logging in to the Management Dashboard: VA on-premises

There are two ways the customer can sign in:

- Sign in with Active Directory credentials - relevant for a customer that uses Active Directory to authenticate users
- Sign in with SSO (using corporate credentials) - relevant for a customer that has integrated Votiro through SAML

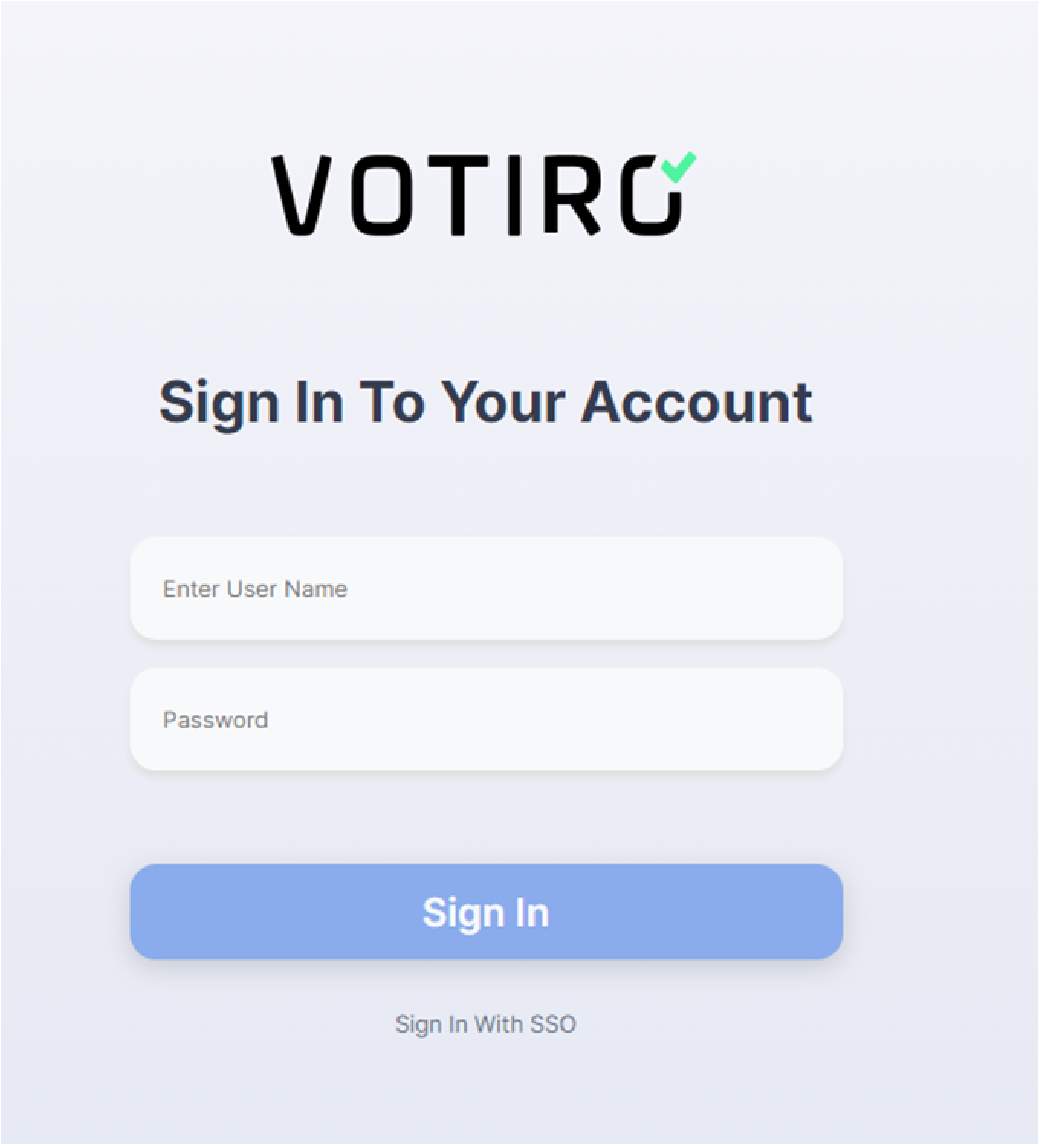
2.1.1 EULA Initial Tenant Setup

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 Active Directory credentials

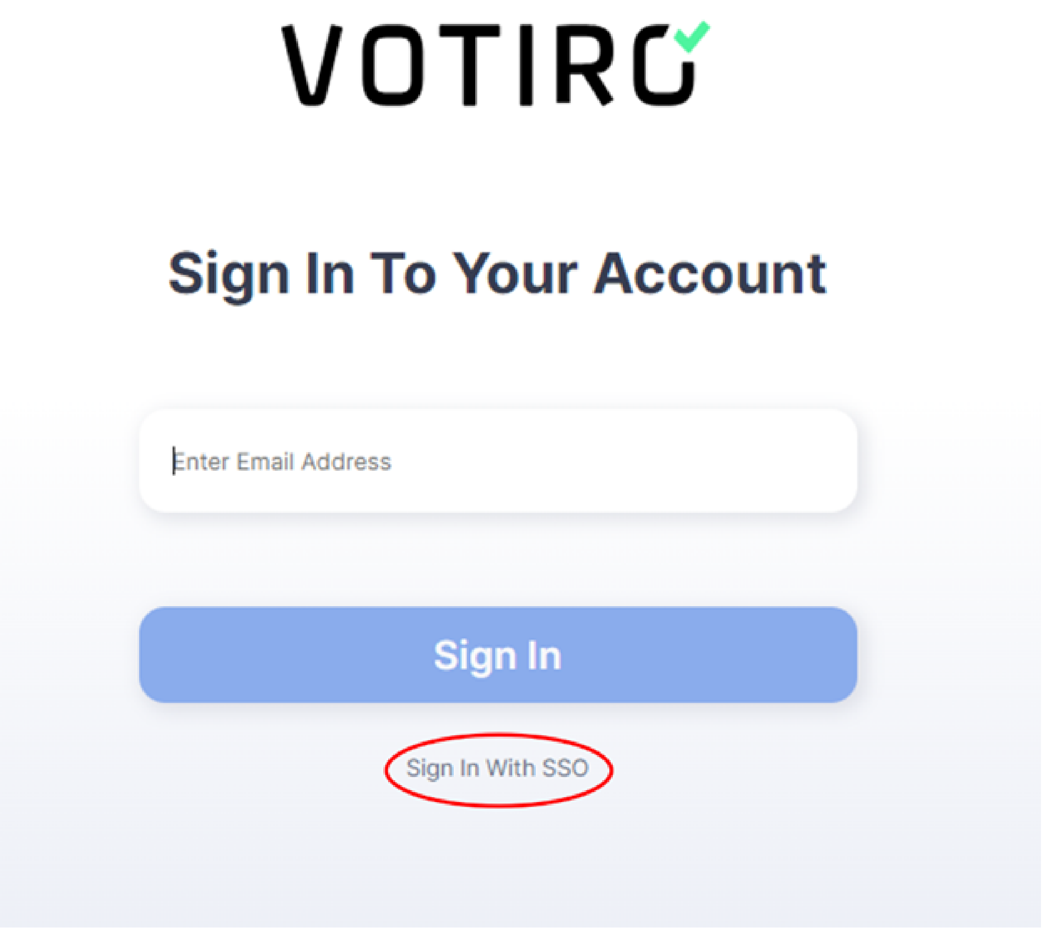
For customers who use Active Directory to authenticate users, the user must enter the Active Directory credentials:

- User Name
- Password

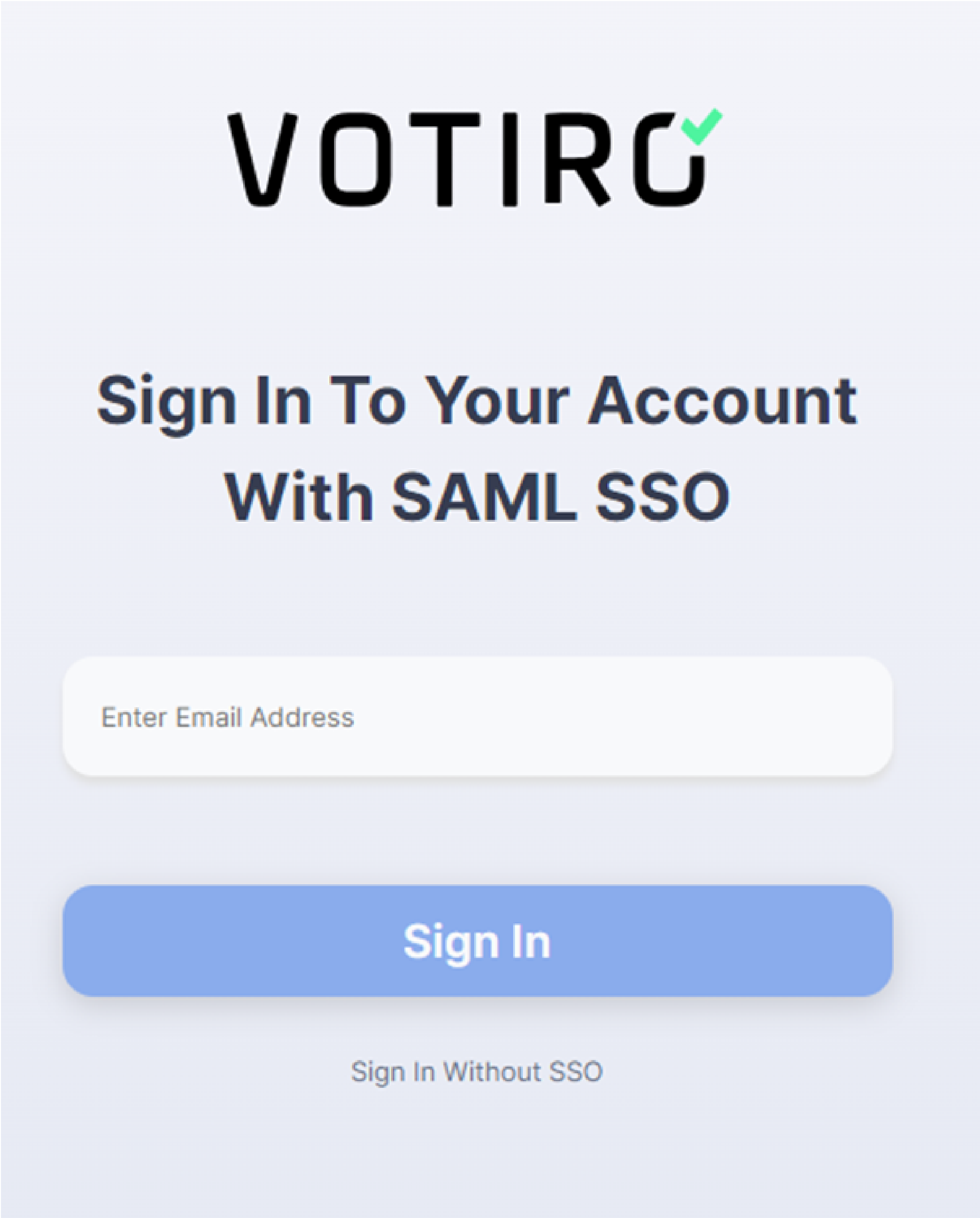

VOTIRO
Sign In To Your Account
Enter User Name
Password
Sign In
Sign In With SSO

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.

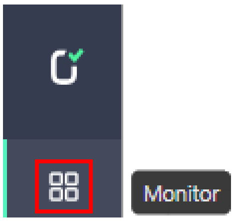
2.2 Monitor Dashboard

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.

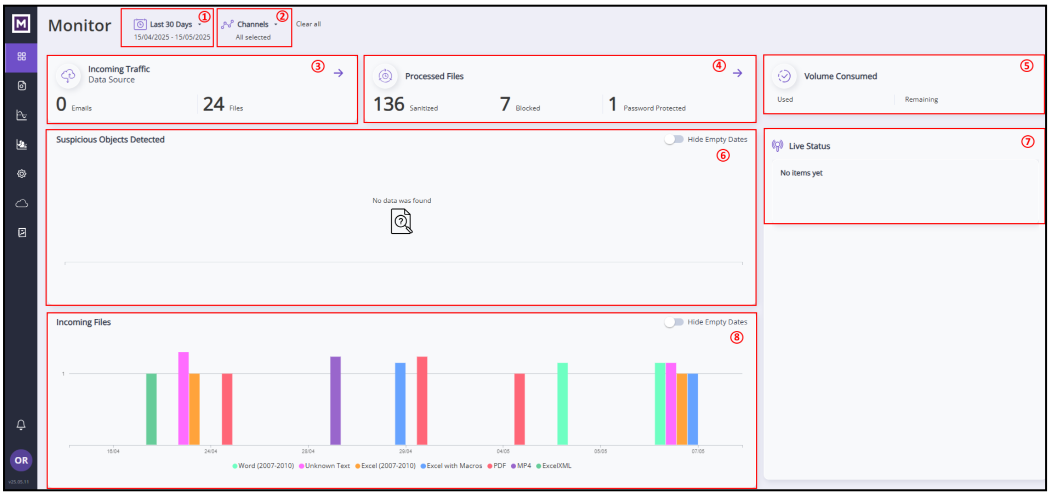
A file is processed for positive selection according to policies for the particular file type. Threats, determined by unknown elements, are detected regardless of policies, whether the file is blocked or not.

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.

2.2.1 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 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.

2.3.1 Incoming Traffic

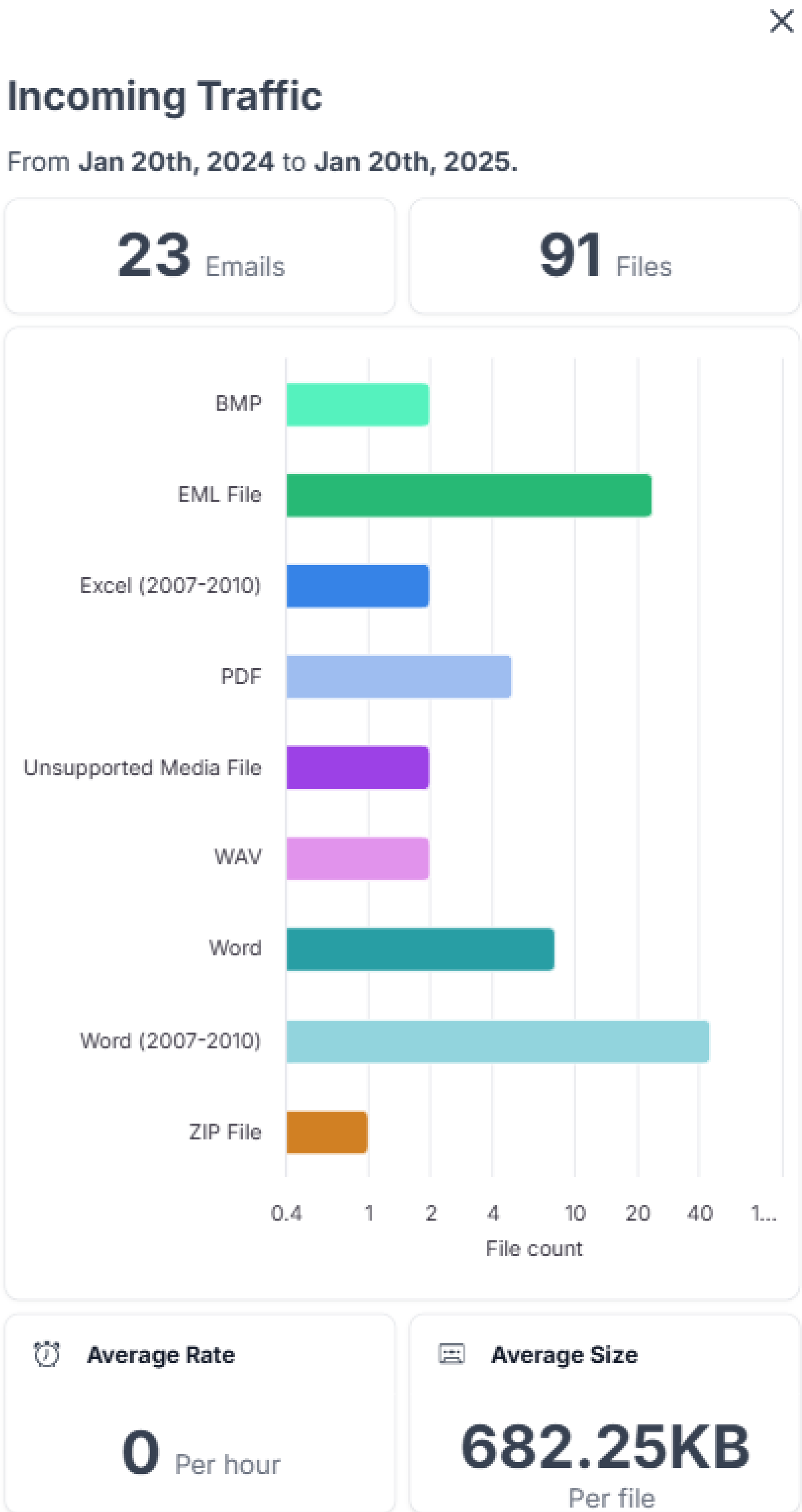
The **Incoming Traffic** pane displays the number of Emails and Files received during the selected time interval and selected channels.

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:

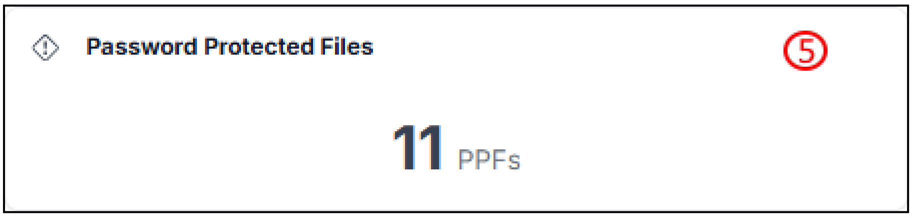


Extracting more data by drilling down

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.

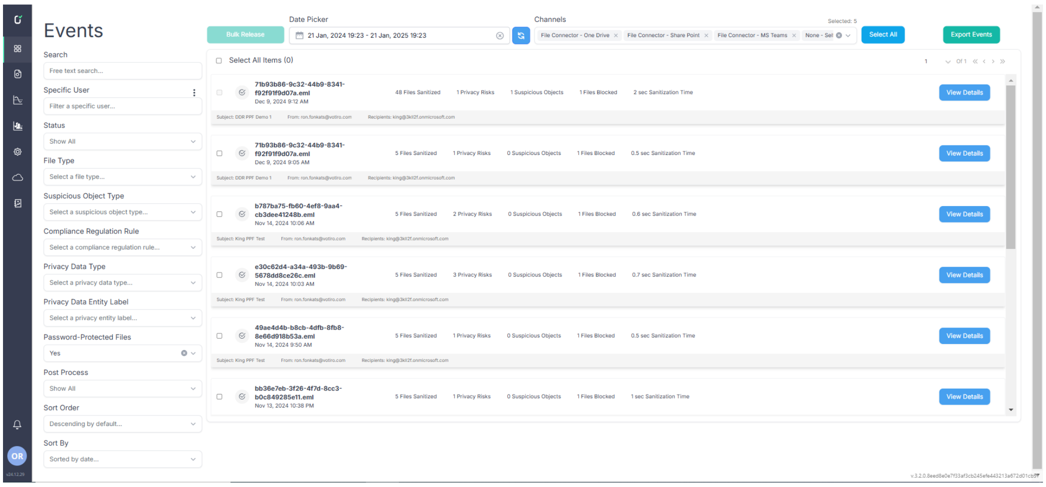
2.3.2 Password Protected Files

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:



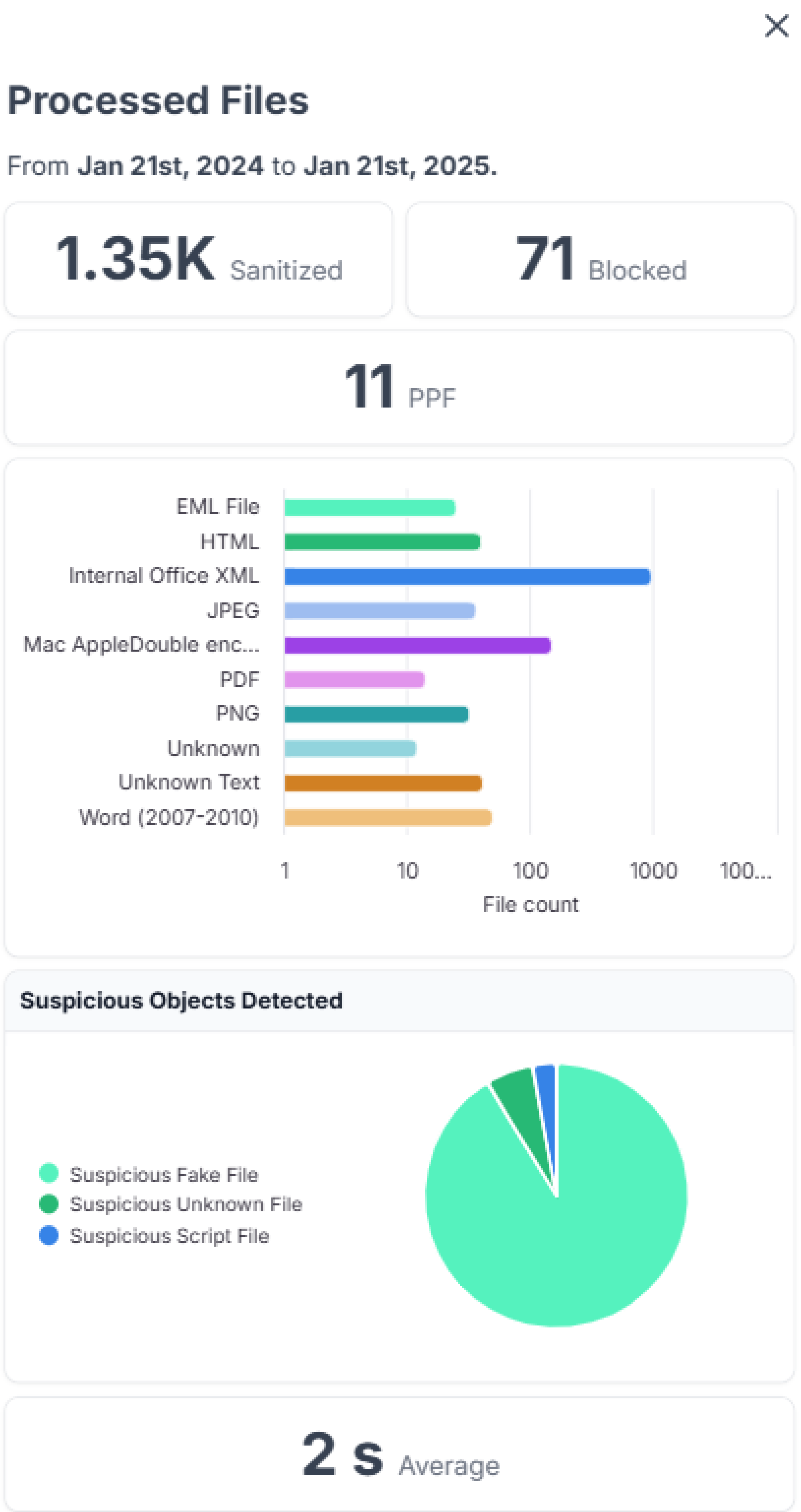
2.3.3 Processed Files

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:

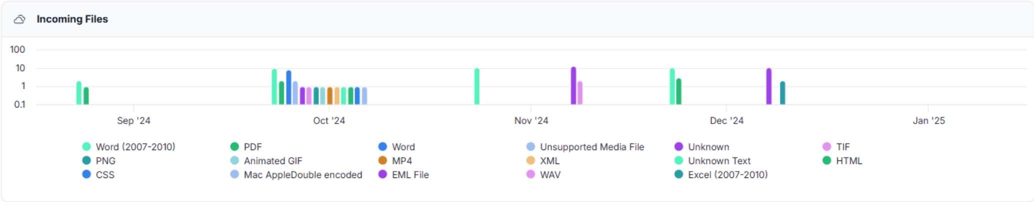

Processed Files
From Jan 21st, 2024 to Jan 21st, 2025.
1.35K Sanitized
71 Blocked
11 PPF
EML File
HTML
Internal Office XML
JPEG
Mac AppleDouble enc...
PDF
PNG
Unknown
Unknown Text
Word (2007-2010)
1
10
100
1000
100...
File count
Suspicious Objects Detected
Suspicious Fake File
Suspicious Unknown File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

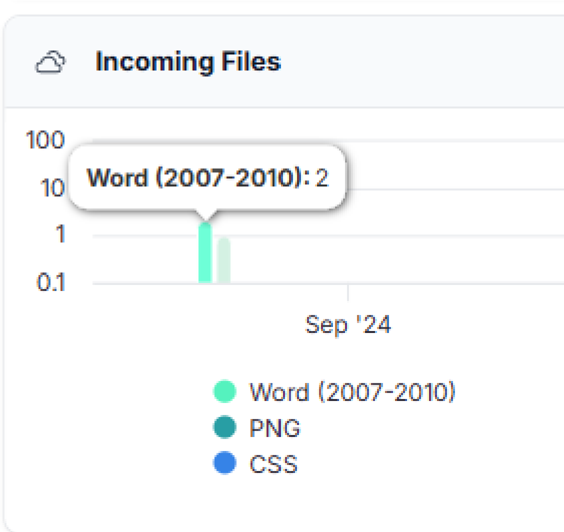
2.3.4 Incoming Files

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

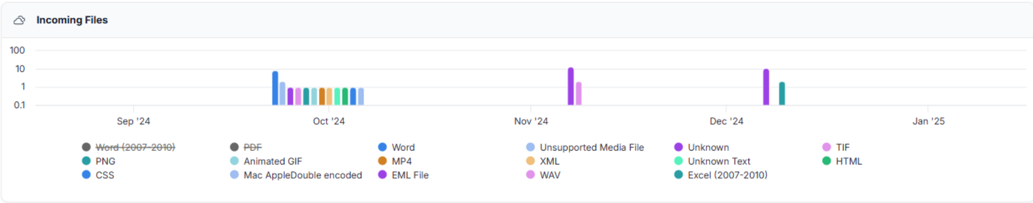


2.3.5 Filtering the Incoming Files

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.

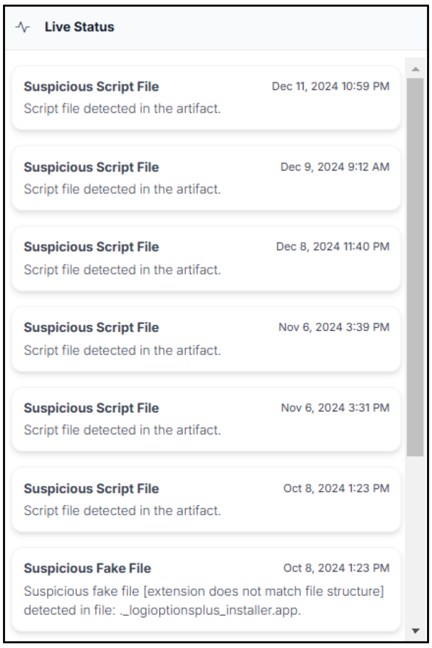


You may also remove file types from the display by clicking on the file types below the histogram. The selected file types are removed from the histogram display for the entire selected time interval. In the below example, Word (2007-2010) and PDF files were removed from the display and this is indicated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



2.3.6 Live Status

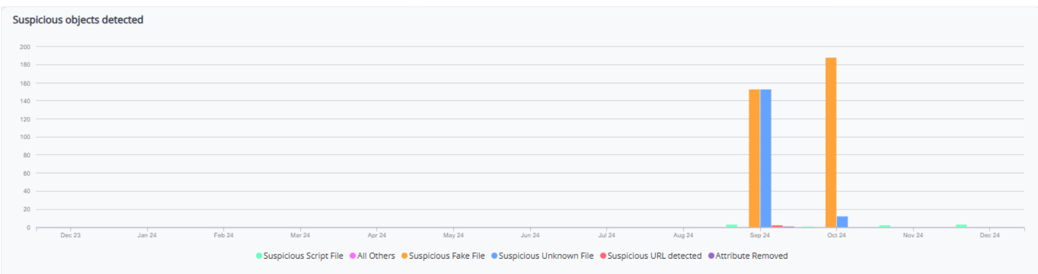
The **Live Status** pane displays the most recent file traffic events during the selected time period and for the selected channels. Any suspicious files detected along with the date and time detected and the reason the file was flagged as suspicious are displayed.



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.

2.3.7 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.

2.3.8 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 40.

2.4 Events Dashboard

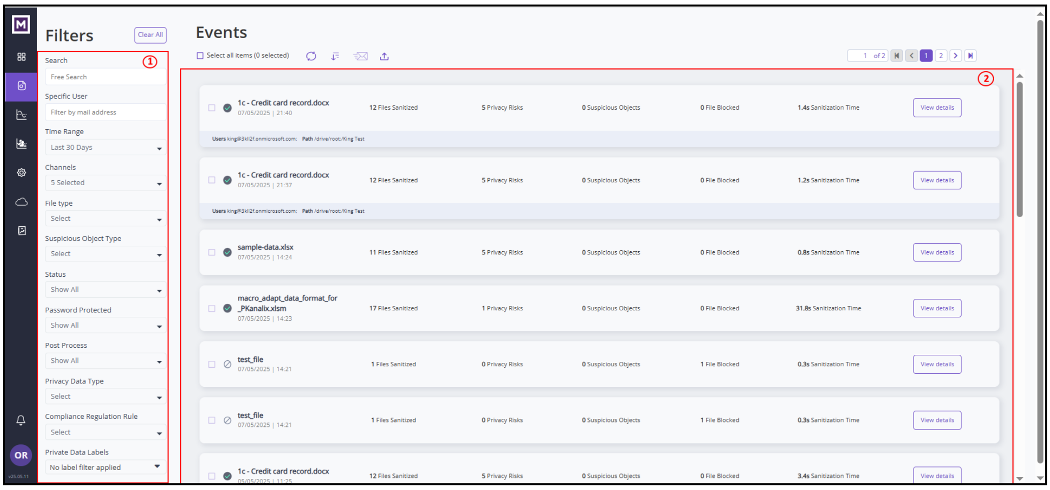
The **Events** dashboard provides you with a deeper view of files that have been processed for positive selection and are currently stored on the server. By default the full list of incidents (up to 10,000 events) that have occurred during the last seven days is displayed. You can narrow the list of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

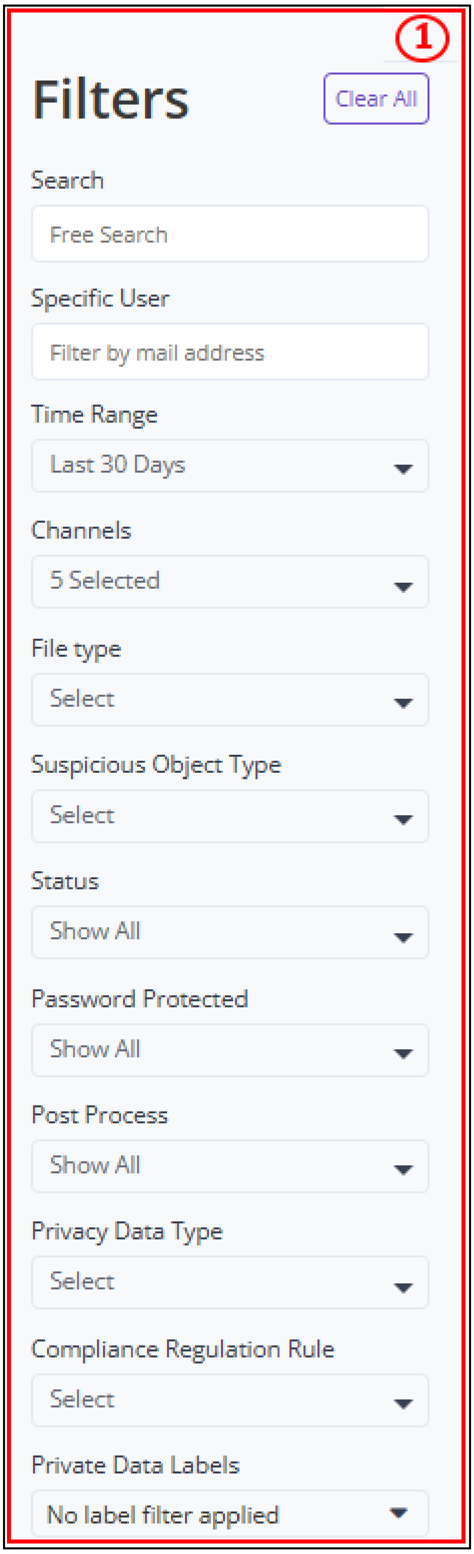
- **Bulk Release** - after selecting blocked emails from the Event Files table, clicking on this button releases all the blocked emails. See Releasing Multiple Emails for more details.
- **Export Events** - clicking on this button downloads a csv file summarizing all the Event files displayed on the 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.

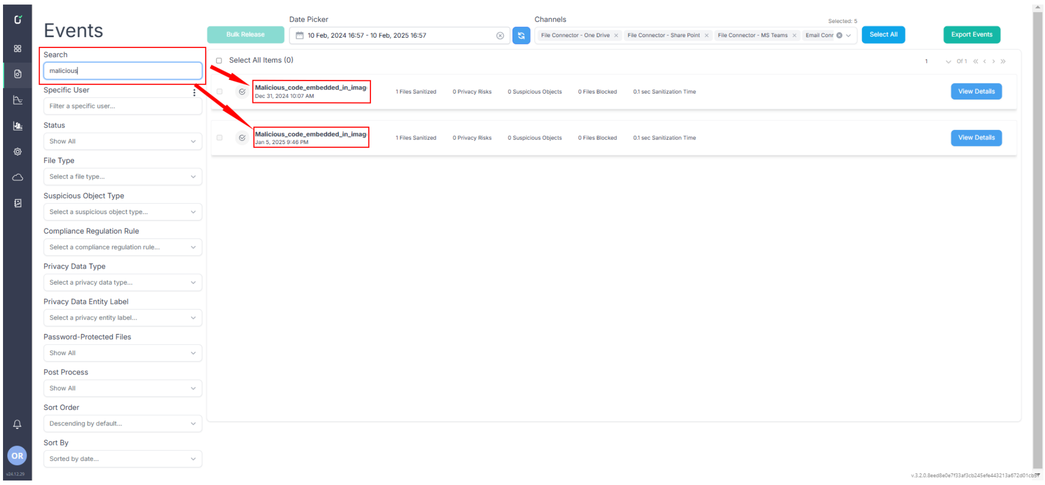
2.5 Event Filters

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

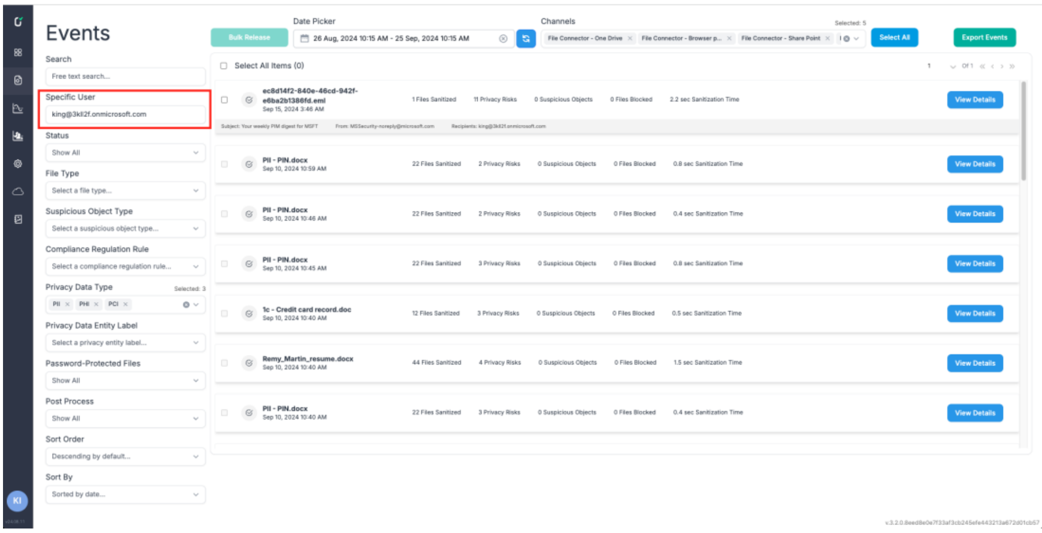


The filters available include:

- 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:



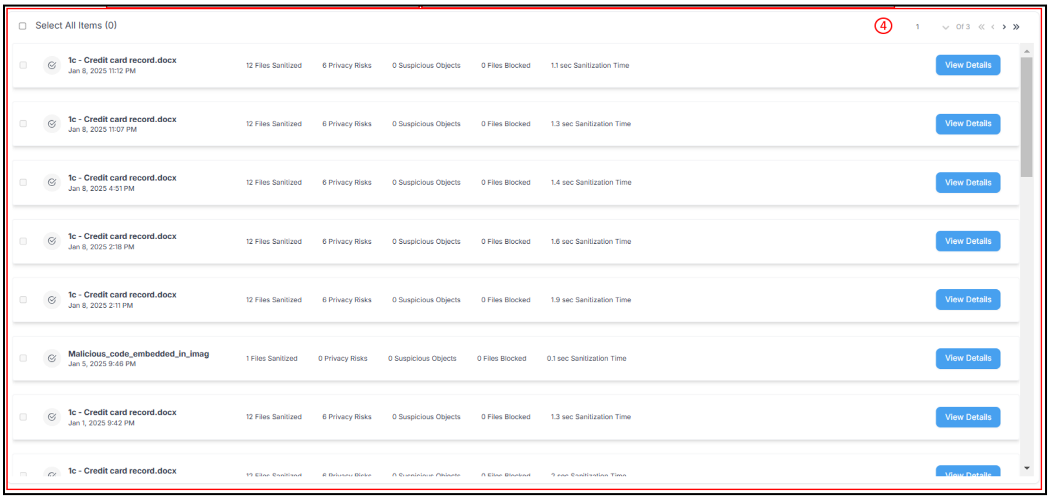
> **Note**: This filter is available for the following connectors only:
>
> - API
> - OneDrive
> - Teams
> - SharePoint
> - O365 Email
> - Browser Plugin

- 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 Files - 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 Events - 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.

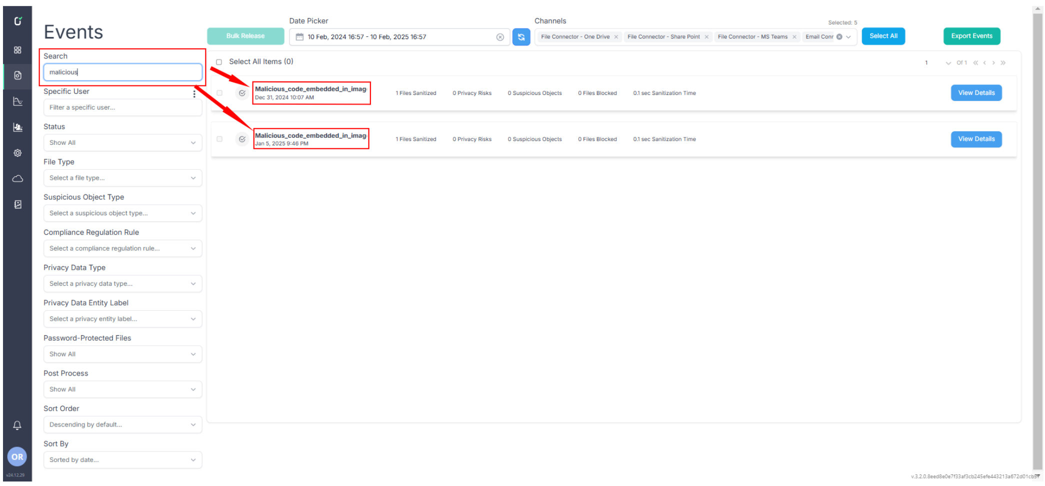
2.6 Events List

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

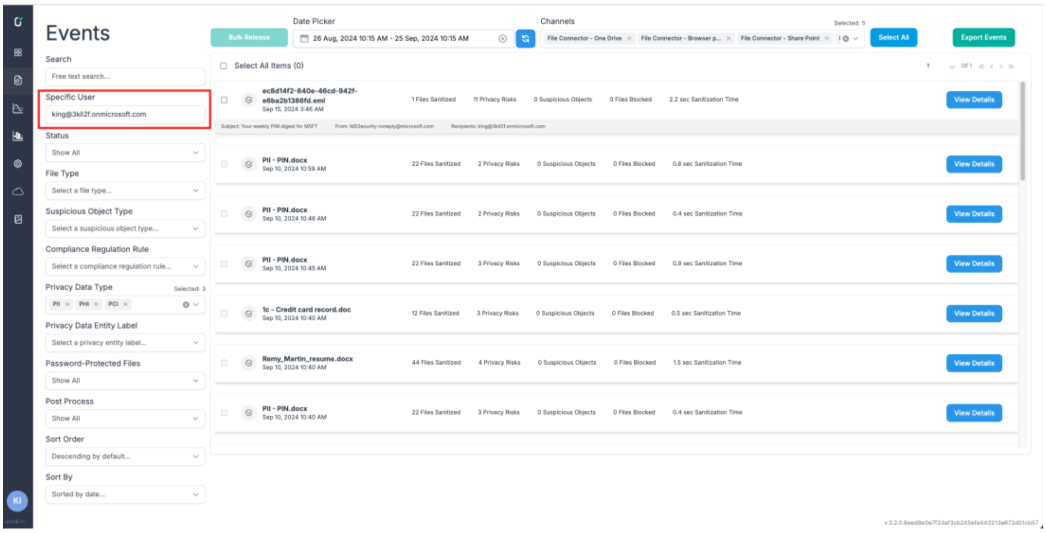


The table of files displayed includes:

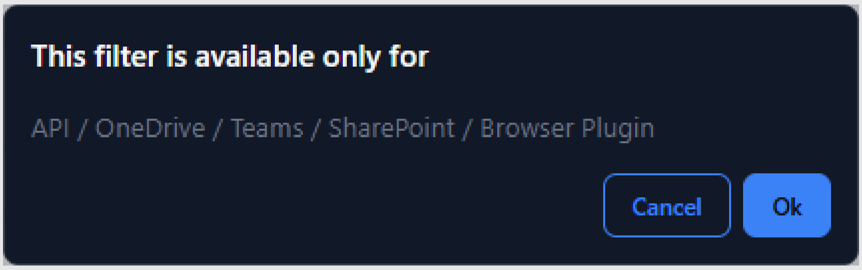
- File name
- Number of **Files Sanitized** - if the file is an archive or email, this number includes attached files
- Number of **Privacy Risks**
- Number of **Suspicious Objects**
- Number of **Files Blocked**
- **Sanitization Time** - in seconds



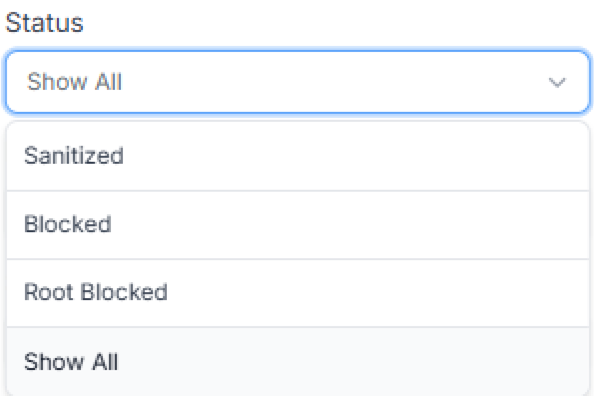
- Specific User - filter a specific user. The Event Files displayed will contain all files owned by the specific user. For example:



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.

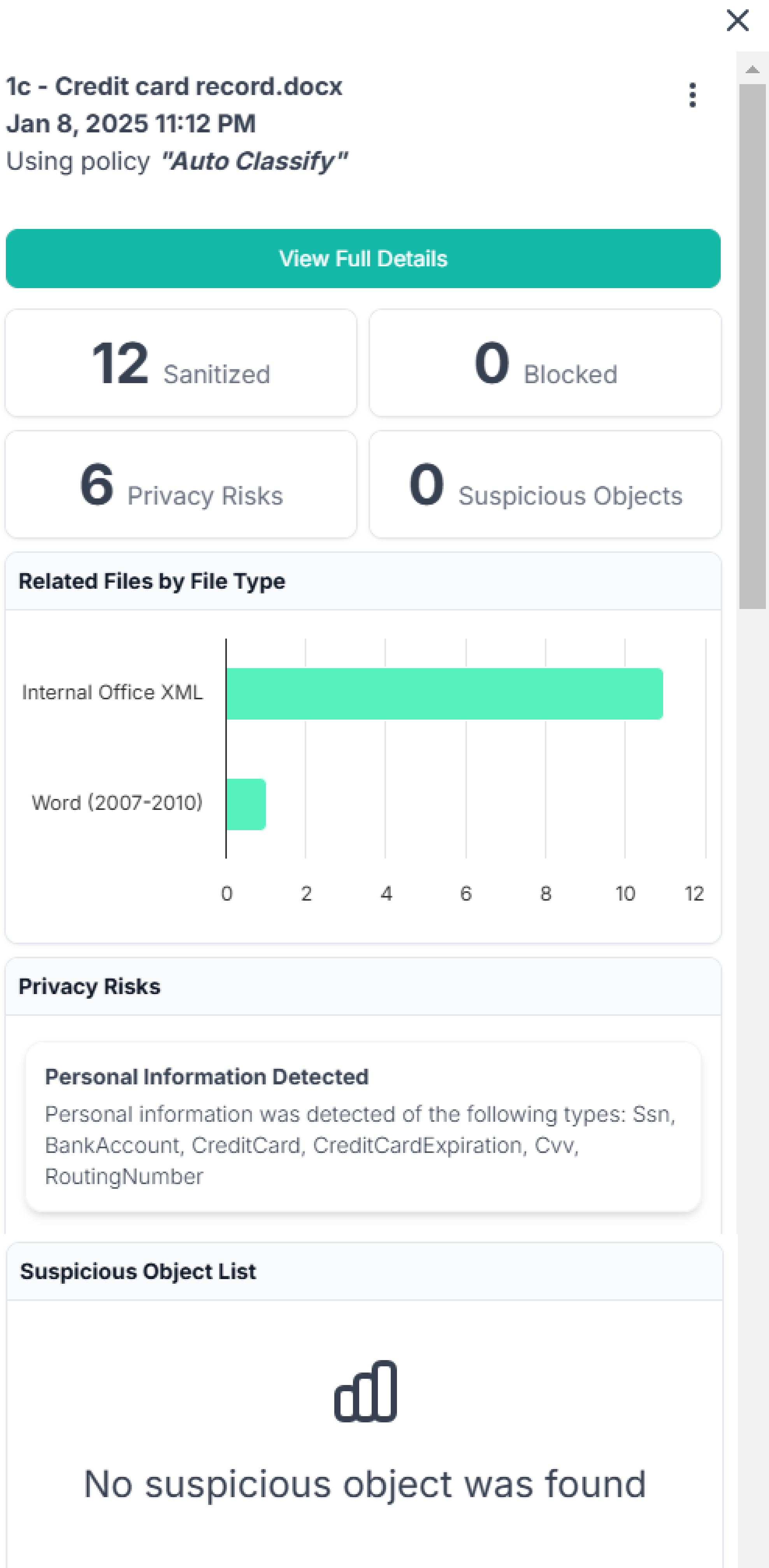
- Compliance Regulation Rule - select a compliance regulation rule from the dropdown list. The options are GDPR, CPRA, HIPAA, QuebecPrivacyAct AND APPI. These are described in Supported Regulations.
- Privacy Data Type - select a privacy data type from the dropdown list. The options are PII, PHI and 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

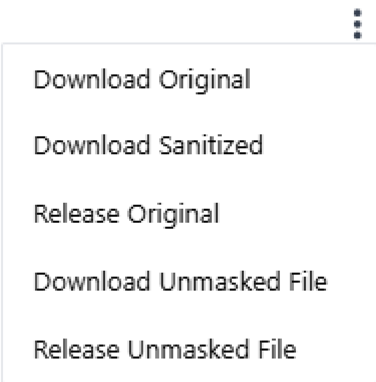
The File Details pane opens on the right side of the screen:


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**.

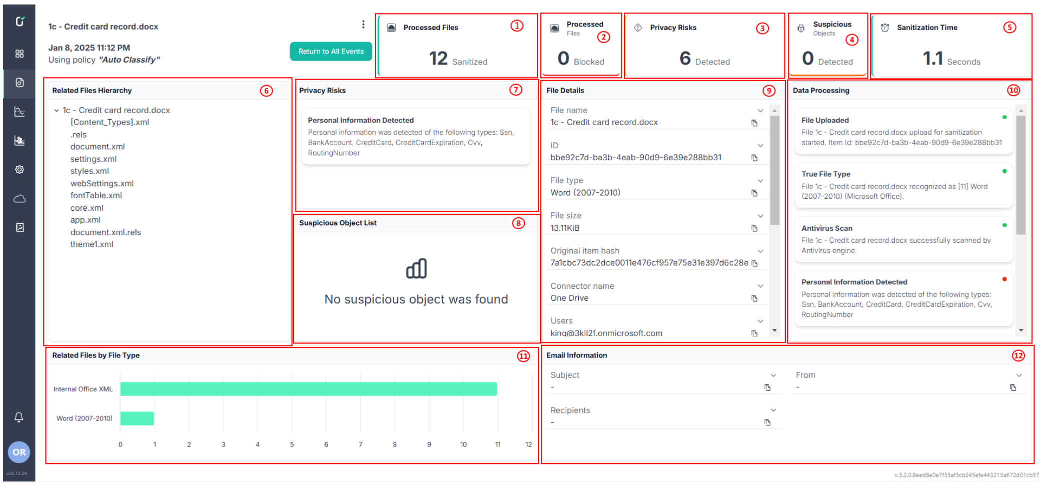
2.7.1 Download and Release file options

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:



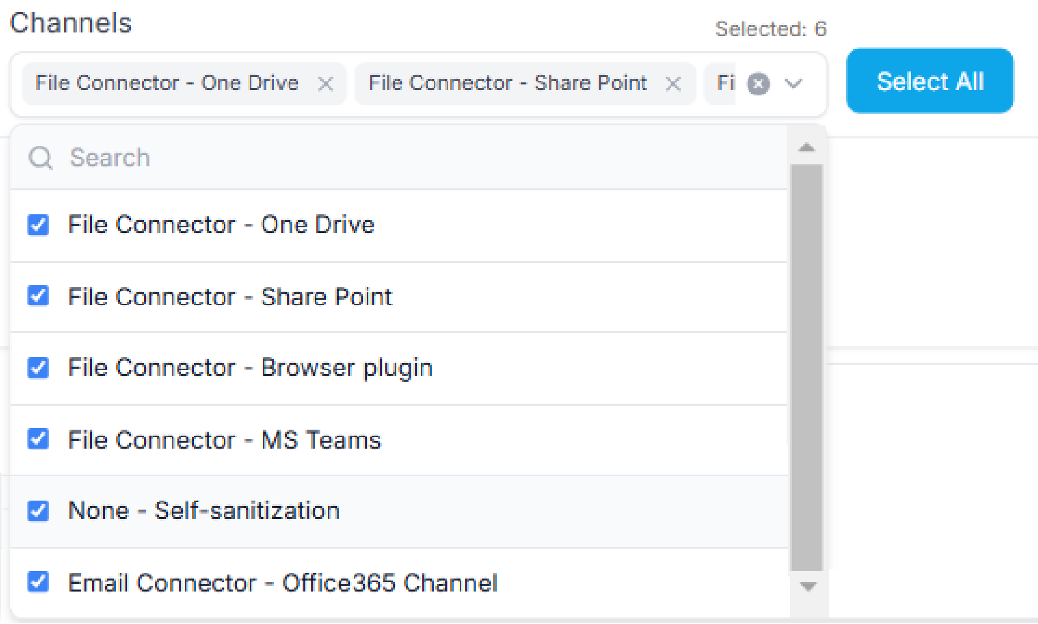
The following panes are displayed:

- **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.

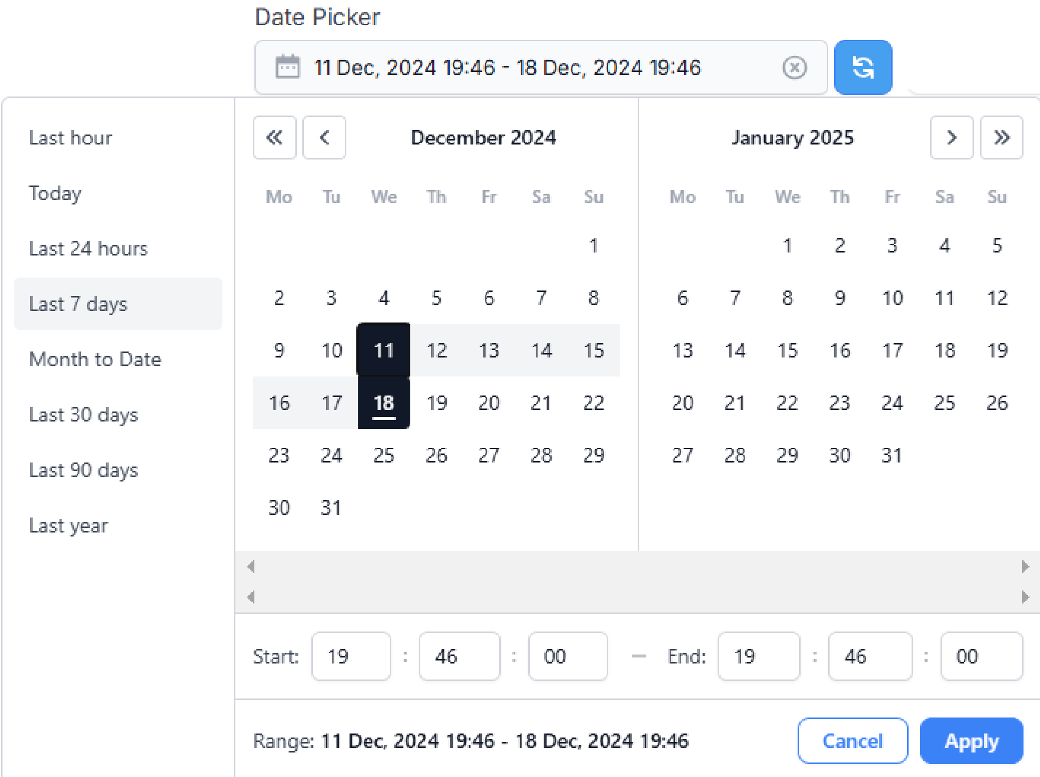


1. To display statistics for specific connectors, click on the **Channels** box.
2. Check the box next to each desired connector.
   - **None - Self-sanitization** refers to user-uploaded files through the **Test File** button on the **Policies** dashboard.
3. To select all available connectors, click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

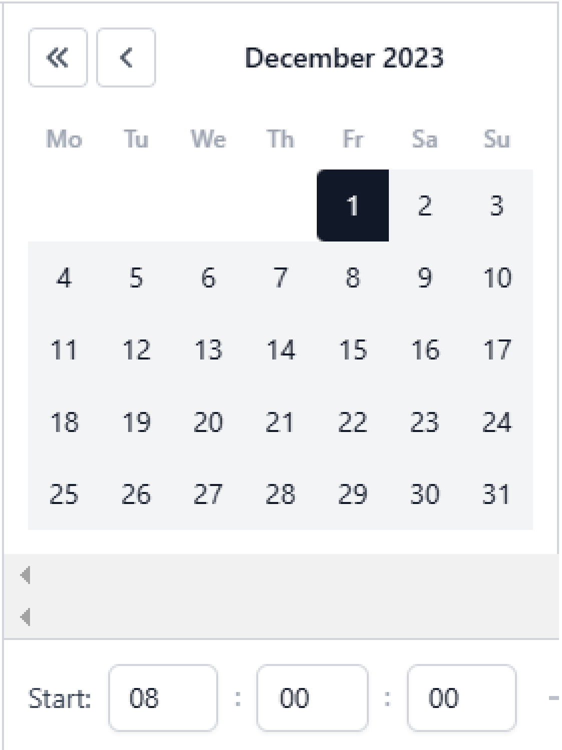


Votiro On-prem provides the following predefined settings:

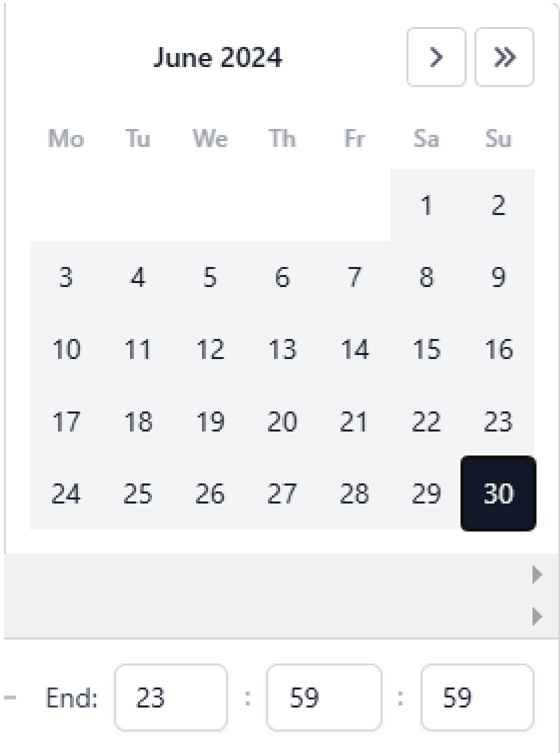
Period of Processing Activity	Meaning
Last hour	The information is for the period starting 60 minutes earlier until the current time.
Today	The information is for the period starting at 00:00 (midnight) of the current day until the current time.
Last 24 hours	The information is for the period starting 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

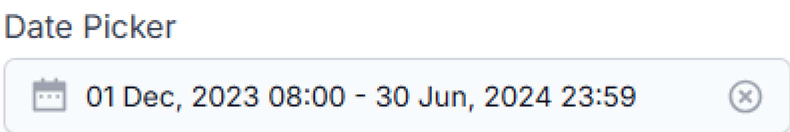
1. Click on the **Date Picker** box..
2. In the left pane, navigate to the desired start month and year by clicking the left arrow (<) to move to the previous month, or by clicking the left double arrow (<<) to jump to the same month in the previous year. If necessary, use the right arrow (>) or right 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 Retro Scan

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

Each file that enters your network is rescanned by Votiro On-prem every 3, 8 and 28 days against Anti-Virus engines. The Retro Scan capability can display whether Votiro On-prem 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 On-prem 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 On-prem 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.

2.7.6 Releasing Files

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

Limitations

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

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

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.

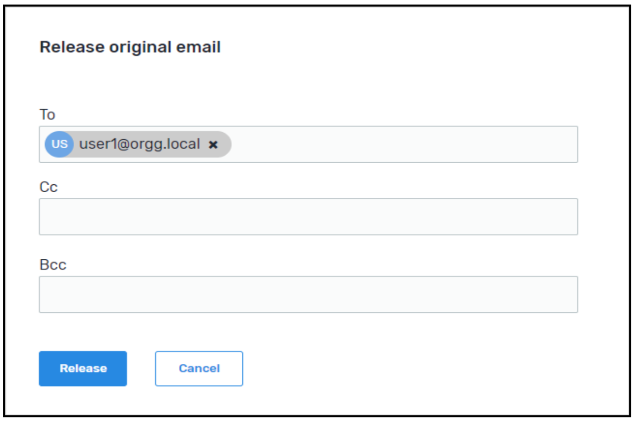
> **Note**
> To enable the release of blocked files, you must first configure the following system settings:
>
> - SMTP Server location
> - SMTP Server port
> - SMTP Server username
> - SMTP Server passwords
>
> For more information, see Configuring Settings on page 132.

- 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:

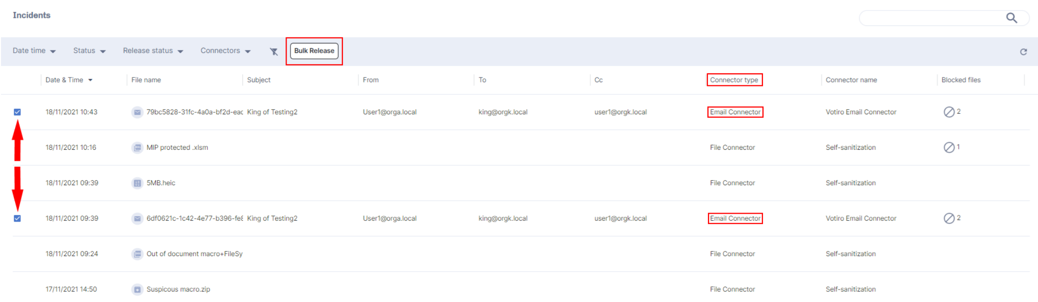


   The dialog shows the same email addresses that were included in the original email, as well as their original designations: To, Cc, or Bcc.

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).

2.8 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

2.9 Suspicious Object Types

In the Event Filters pane, select a suspicious object type to search for from the dropdown list. The options are:

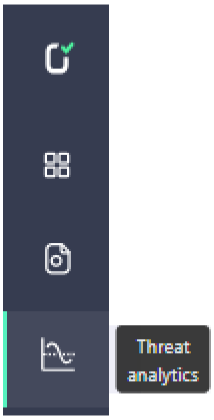
- Suspicious Macro
- Suspicious Office Excel 4.0 Macro
- Suspicious File System Activity Macro
- Suspicious Out of Document Interaction Macro
- Malicious Macro
- Suspicious Fake File
- Suspicious Unknown File
- Suspicious Executable File
- Suspicious Script File
- Suspicious Threat File Detected by Antivirus
- Max Depth detected
- Duplicate Key detected
- Complex File detected
- External Program Run Action
- External Link Path
- External Frame
- External Attached Template
- External Online Video
- External Ole Link
- External Image
- Dynamic code execution
- Suspicious URL detected
- Xml Bomb detected
- Zip Bomb detected
- Suspicious File Structure
- Svg Bomb detected
- Suspicious Threat File

- DDE detected
- Open Action Removed
- Remote Access Removed
- Xfa Script Removed
- Open Action Removed
- Script Tags Removed
- External Image Removed
- Element Removed
- Attribute Removed
- External Reference Removed

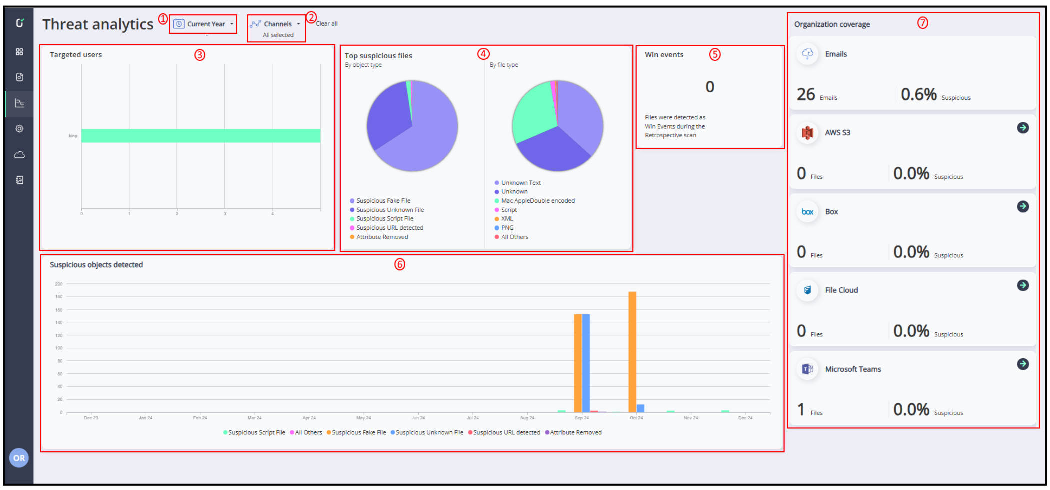
2.10 Threat Analytics Dashboard

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:

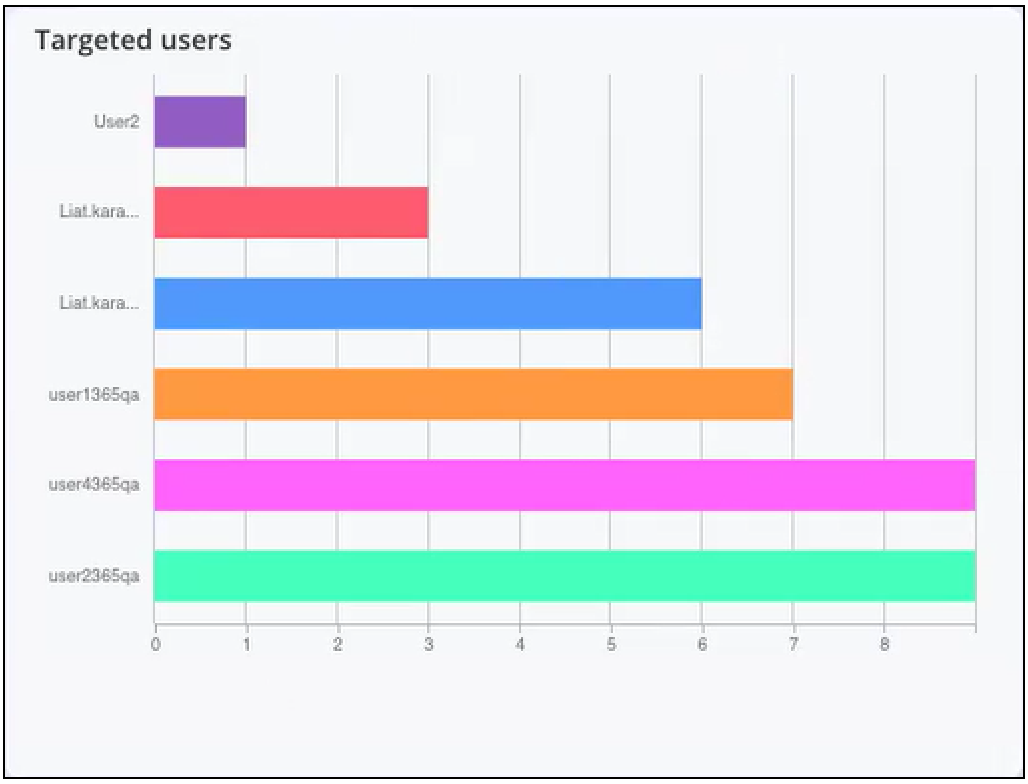


The page contains the following panes, outlined in red and numbered as in the above screenshot:

- **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 .

2.10.1 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.



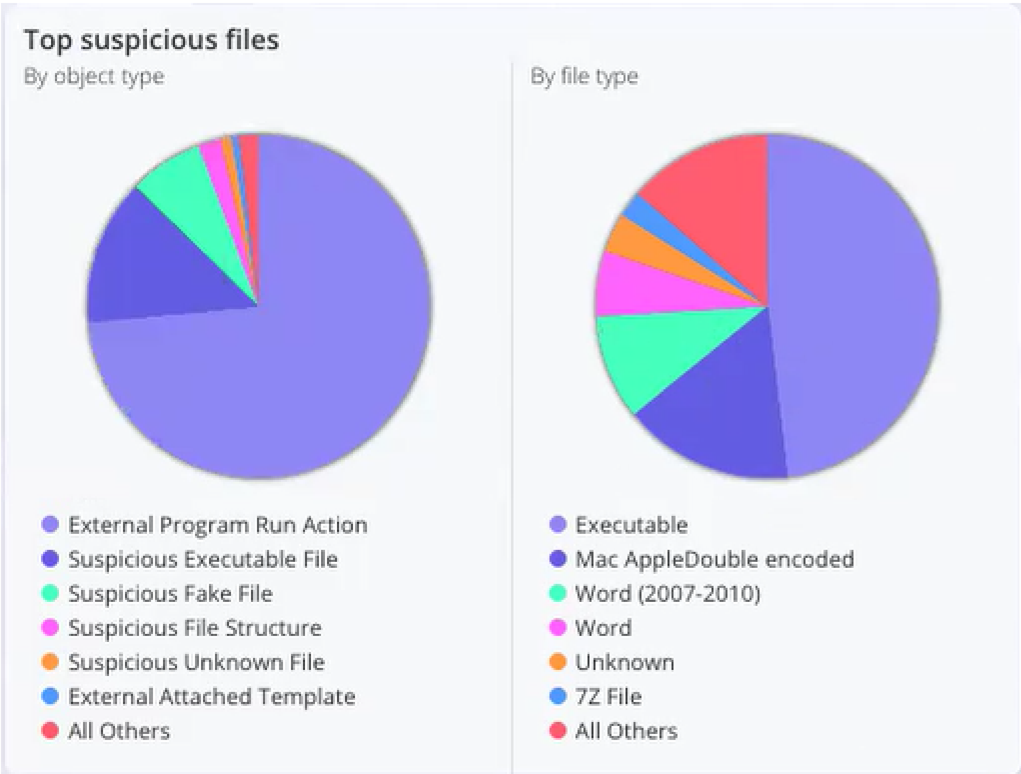
Extracting more data by drilling down

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.

2.10.2 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.

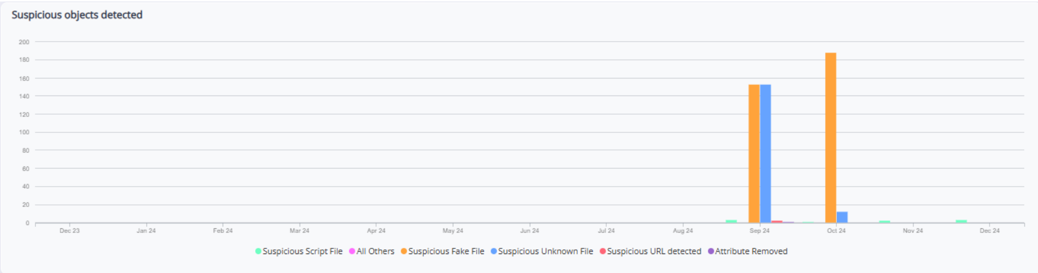


Extracting more data by drilling down

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.

2.10.3 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.

2.10.4 Retro Scan

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

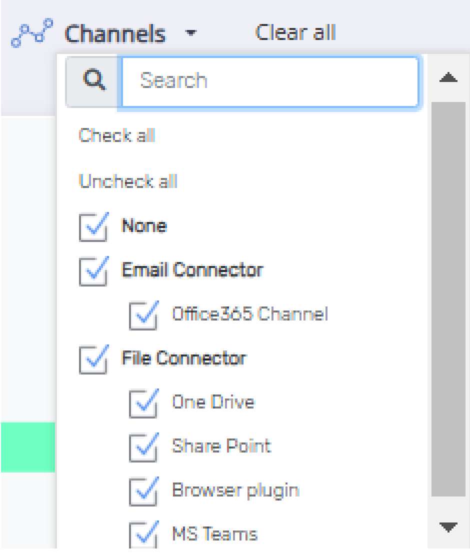
Each file that enters your network is rescanned by Votiro On-prem every 3, 8 and 28 days against Anti-Virus engines. The Retro Scan capability can display whether Votiro On-prem detected the incoming file as a threat when the Anti-Virus engine did not.

For example, suppose an incoming file was marked by the Anti-Virus engine as "clean", but Votiro On-prem 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 On-prem 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.

2.10.5 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.

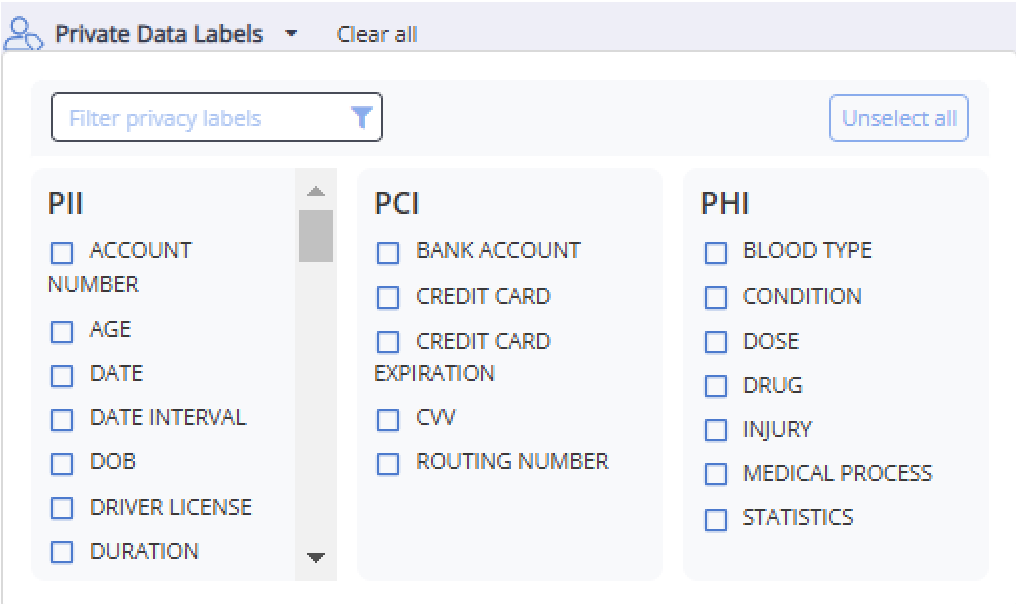


1. To display statistics for specific connectors, click on **Channels**.
2. Check the box next to each desired connector.
3. To include test files, check the **None** box.
4. To select all available connectors, click on **Check all**. To clear all the selections, click on **Uncheck all**.

Statistics update to show information for the selected Channels.

2.10.6 Filter by Private Data Labels

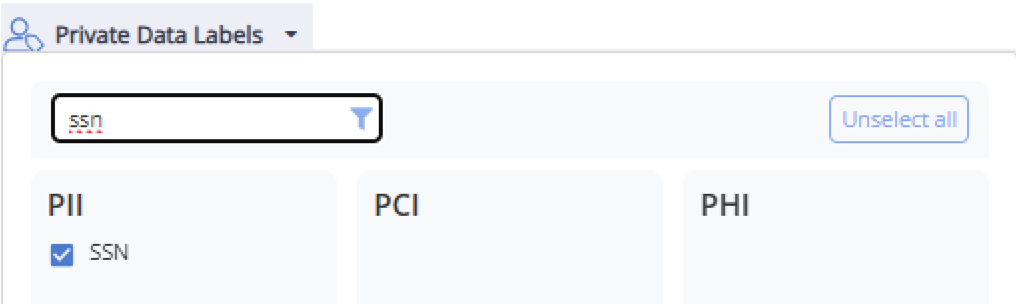
The statistics displayed on the **Privacy and Compliance** dashboard can be filtered by the **Private Data Labels** that are currently selected for each private data type selected.



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:

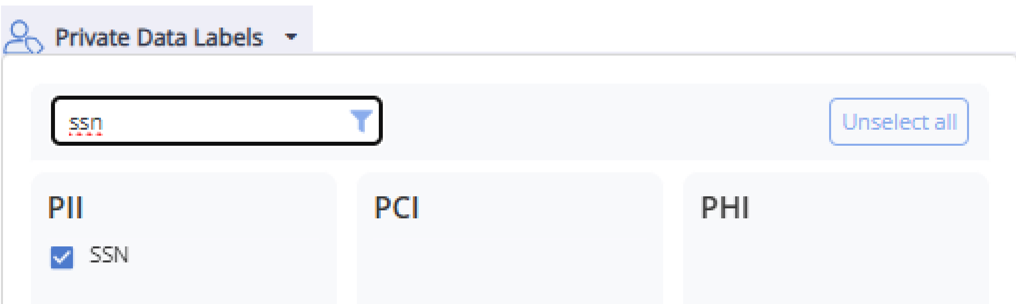


To uncheck all selected private data labels for all private data types, click on **Unselect all**.

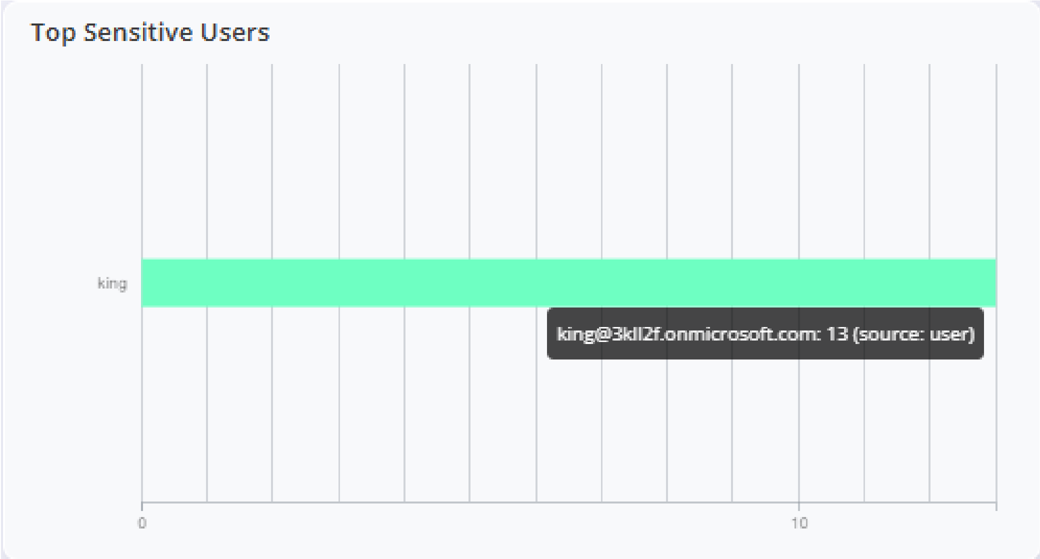
Filtering by Private Data Labels in the Privacy and Compliance Dashboard

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.



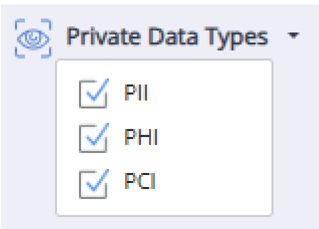
4. Click on the desired pane in the **Privacy and Compliance** dashboard, for example, the **Top Sensitive Users** pane. The statistics are updated to reflect the new selected data.



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

2.10.7 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:

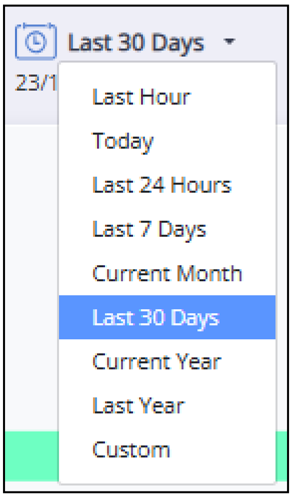
- **PII** - Personally Identifiable Information (PII) is any information connected to a specific individual that can be used to uncover that individual's identity. Examples include account number, driver license, email address, name, username, password, phone number, SSN, etc.
- **PHI** - Protected Health 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.

2.10.8 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.



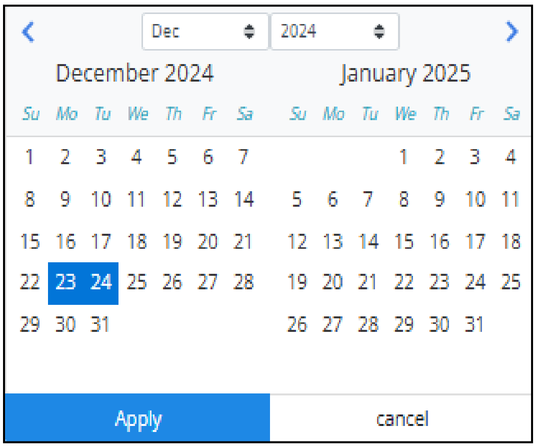
Votiro On-prem provides the following predefined settings:

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.

Period of Processing Activity	Meaning
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.

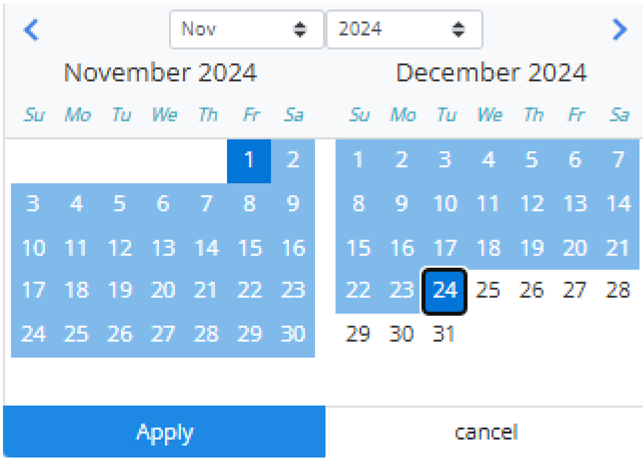


2. Navigate to the desired start month and year by clicking the blue right (>) and left (<) arrows, or by selecting a month and year using the up (^) and down (˅) arrows.

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

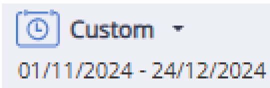
4. To select an end date, tap a date on the calendar, the number turns blue.

The selected period is highlighted.



5. Click **Apply**.

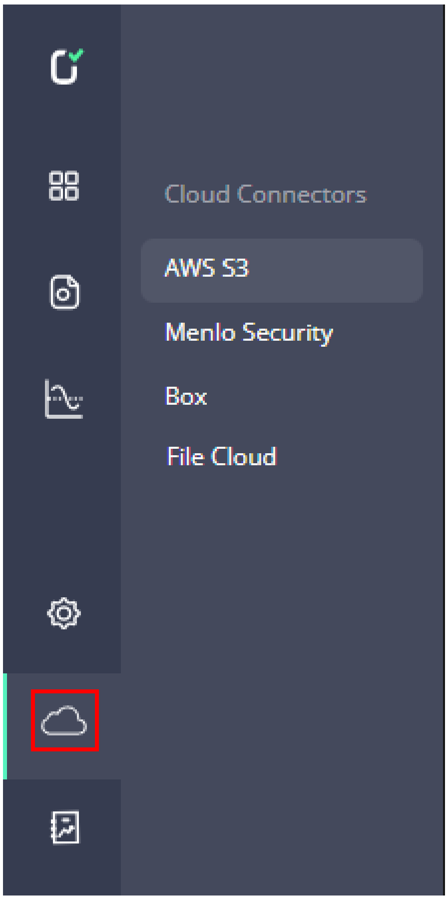
The custom period is displayed in the top left corner of the window:



Statistics update to show information for the custom period.

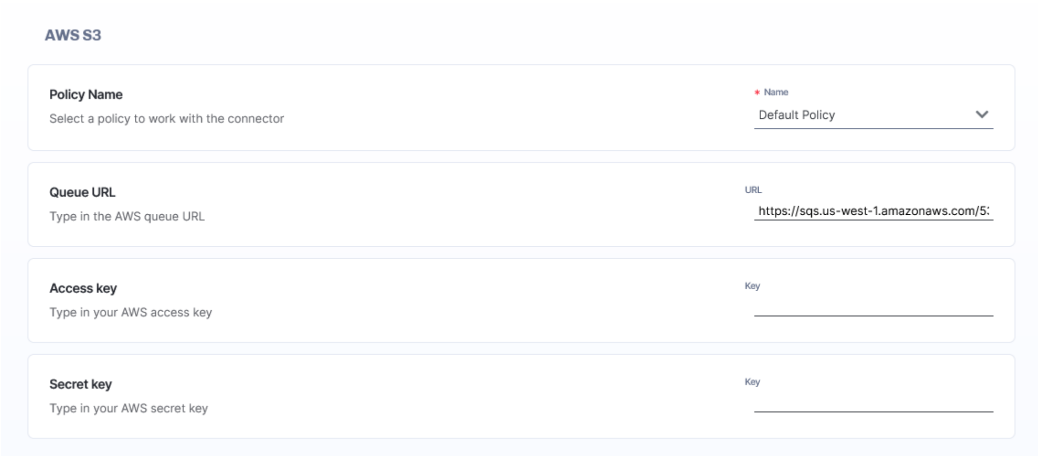
2.11 Cloud Connectors and Integrations

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



2.11.1 AWS S3 - VA On-premises

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	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.
2	Queue URL	Specify the AWS queue URL. See below for details.
3	Access Key	Specify the AWS access key of the IAM user.
4	Secret Key	Specify the AWS secret key of the IAM user.

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

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

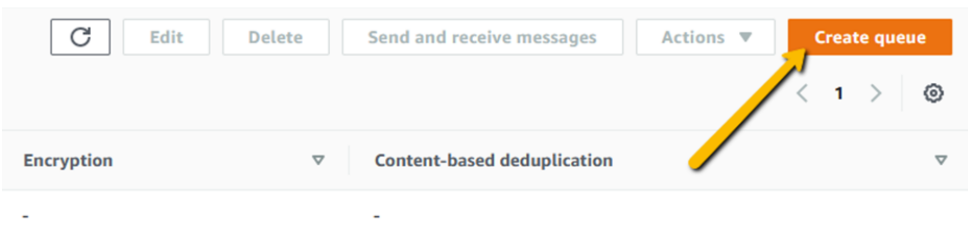
Prerequisites

- AWS SQS (Simple Queue Service) Queue (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

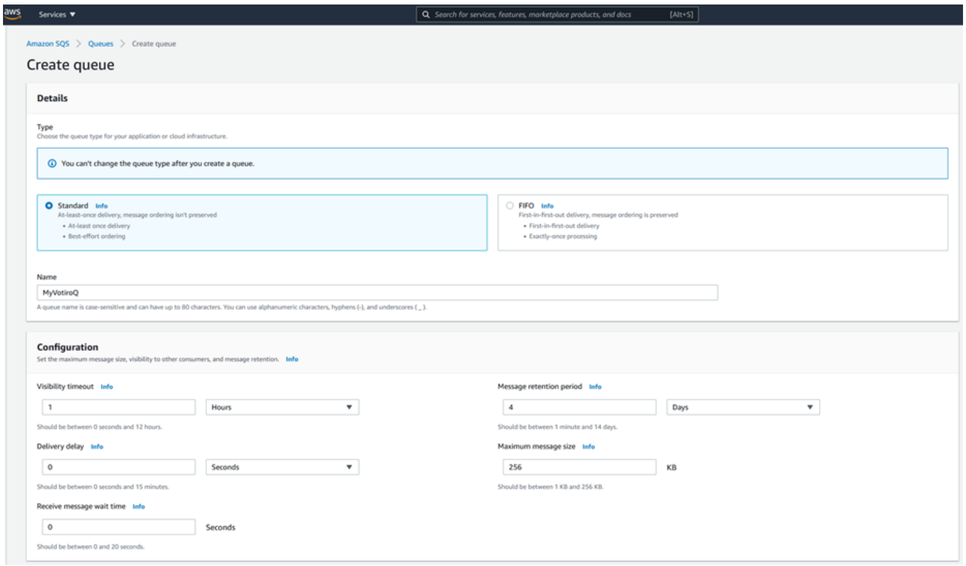
Creating an AWS SQS Queue

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:



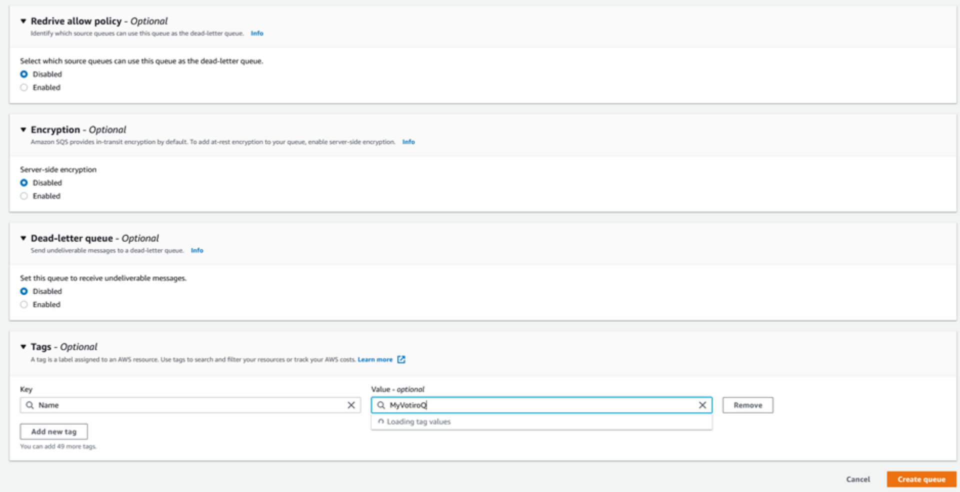
7. For the Access policy, choose **Advanced**.

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": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:*:*:<BUCKET_NAME>"
        },
```

```
            "StringEquals": {
              "aws:SourceAccount": "<AWS_ACCOUNT_NUM>"
            }
          }
        }
      }
    ]
  }
```

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:

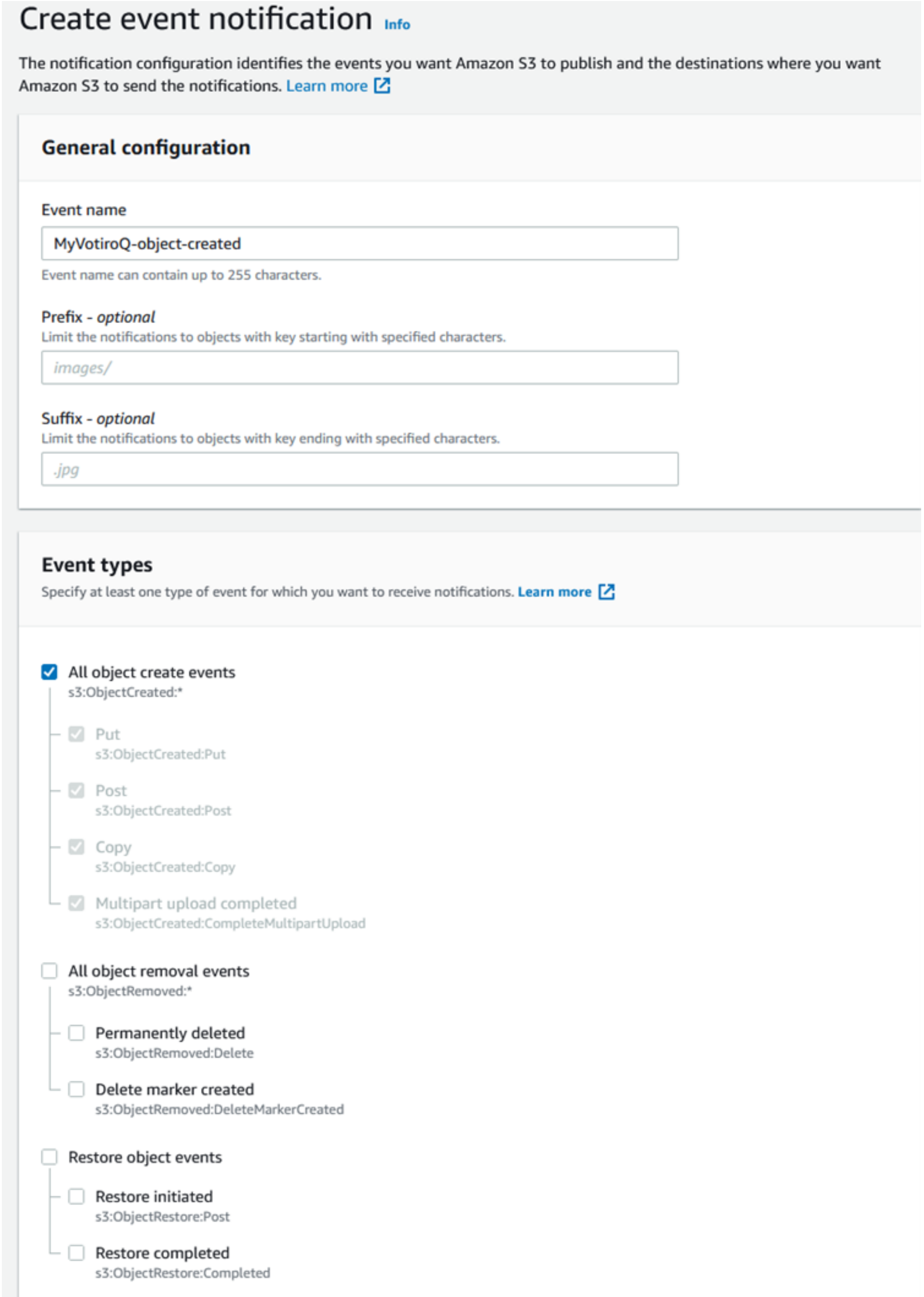


10. Other options should remain at their default values.

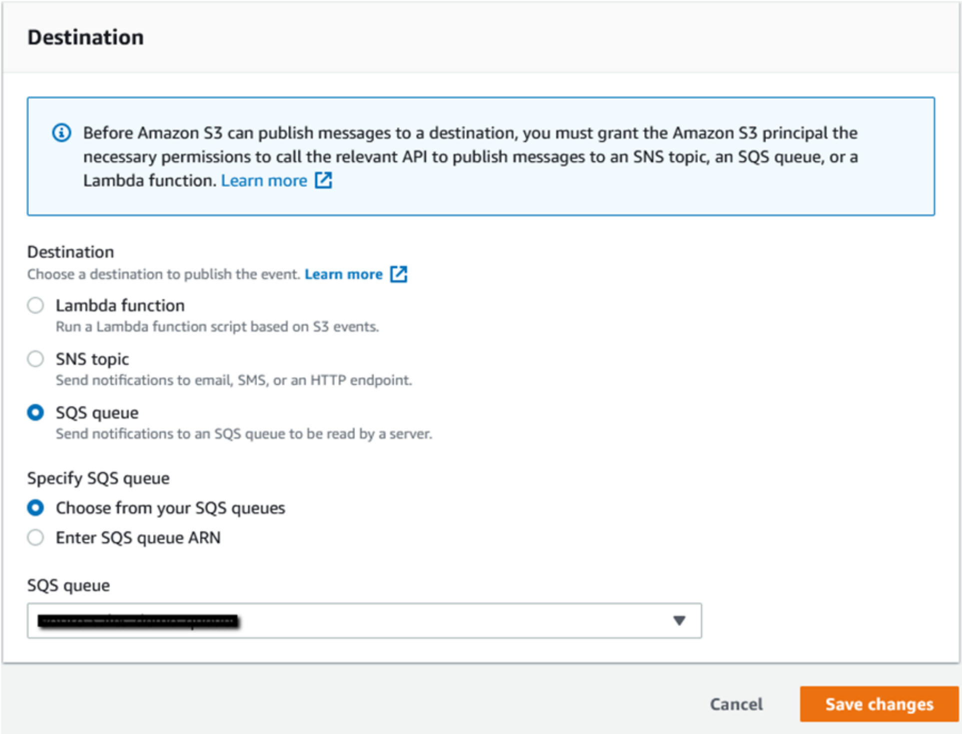
11. Click on **Create queue**.

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 **SQS queue** from the list of available queues. For example:



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

Example of an IAM User JSON Policy with Limited Access to the Bucket

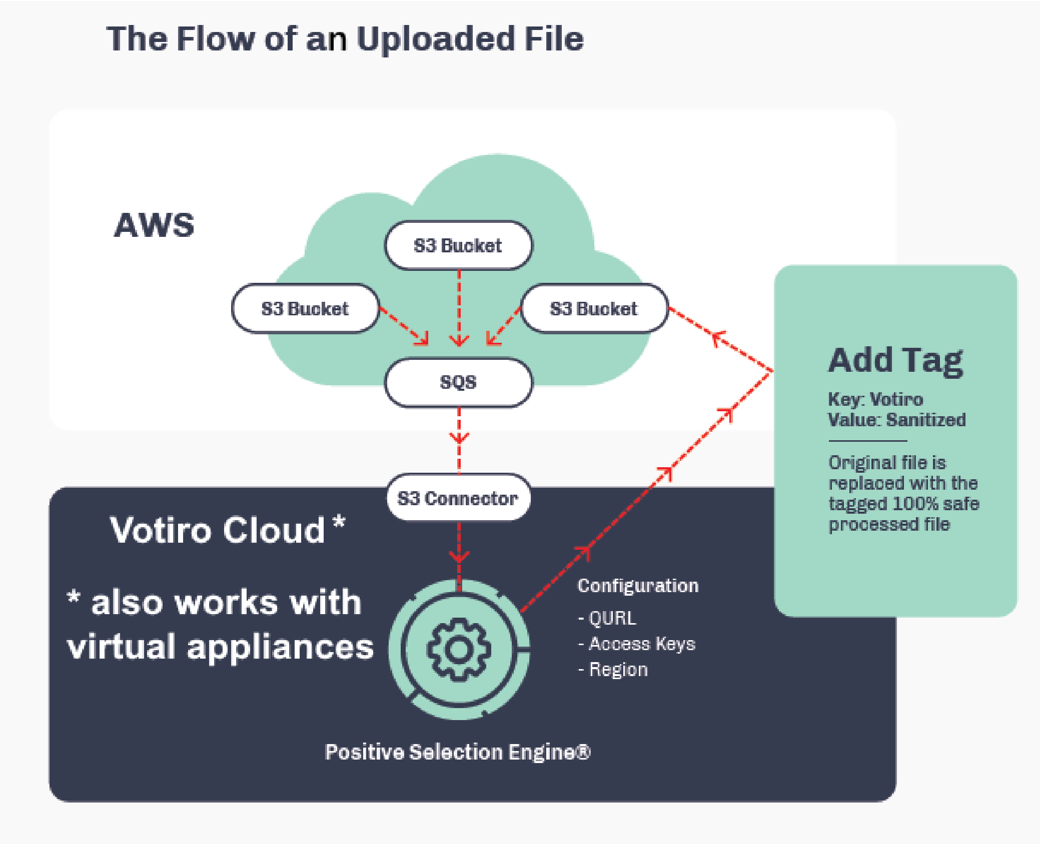
To use the example below, replace ***<AWS_ACCOUNT_NUM>***, ***<QUEUE_NAME>*** and ***<BUCKET_NAME>*** with their actual values.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:GetObjectTagging",
      "s3:DeleteObject",
      "s3:PutObjectTagging"
    ],
    "Resource": "arn:aws:s3:::<BUCKET_NAME>/*"
```

```
        },
        {
          "Effect": "Allow",
          "Action": "sqs:*",
          "Resource": "arn:aws:sqs:us-east-1:<AWS_ACCOUNT_NUM>:<QUEUE_
          NAME>"
        }
      ]
    }
```

AWS S3 Flowchart

The following diagram illustrates the procedure:



Limitations

Sanitization for large files is supported up to 3 GB.

2.11.2 Menlo Security

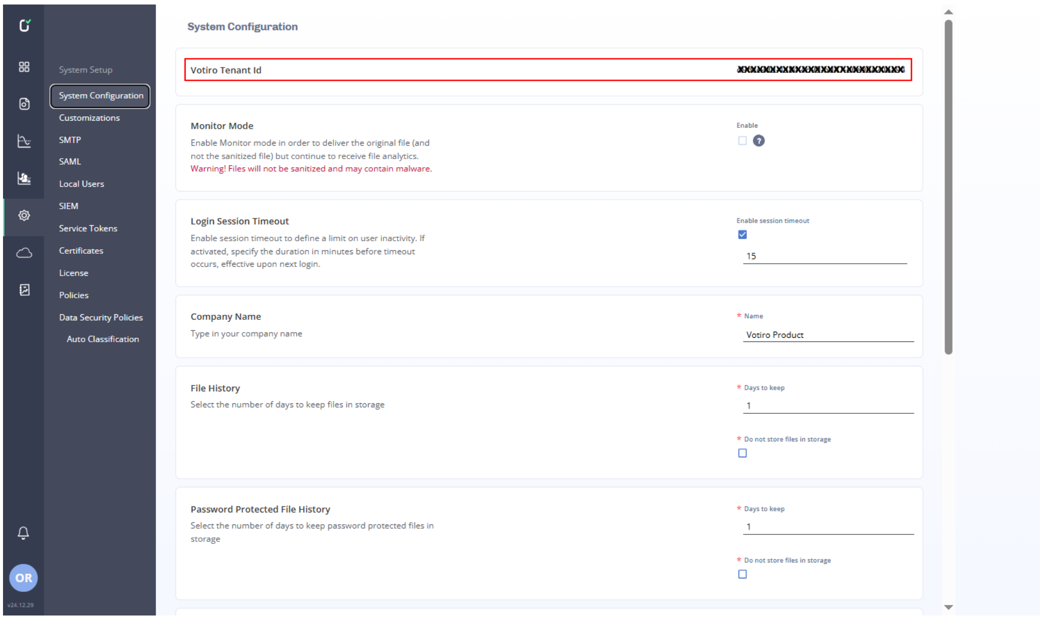
Prerequisites

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

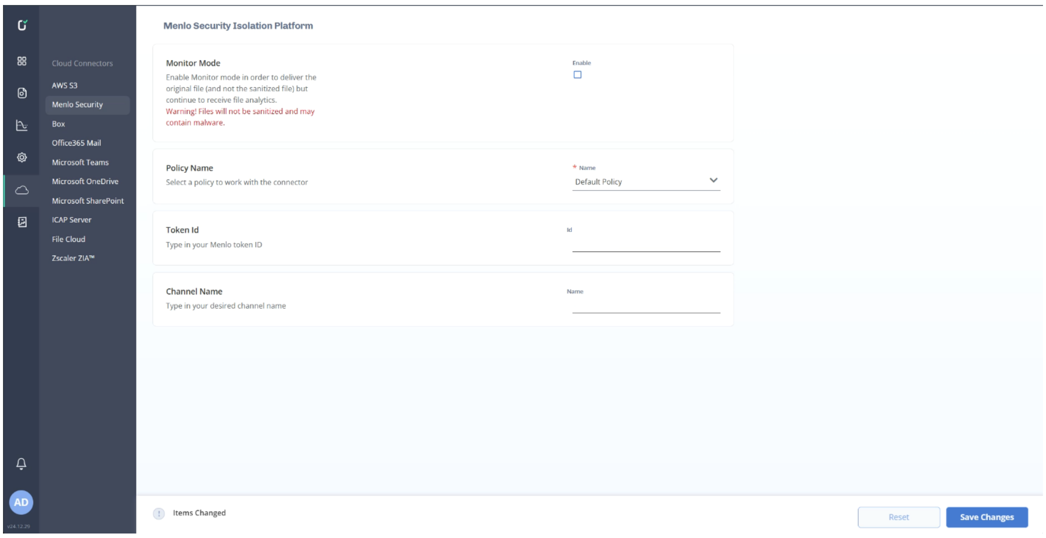
Configuration of Menlo Security in Votiro

1. Navigate to the Votiro Management Console and select **System setup** > **System Configuration**.

2. Copy the **Votiro Tenant Id** to the clipboard.



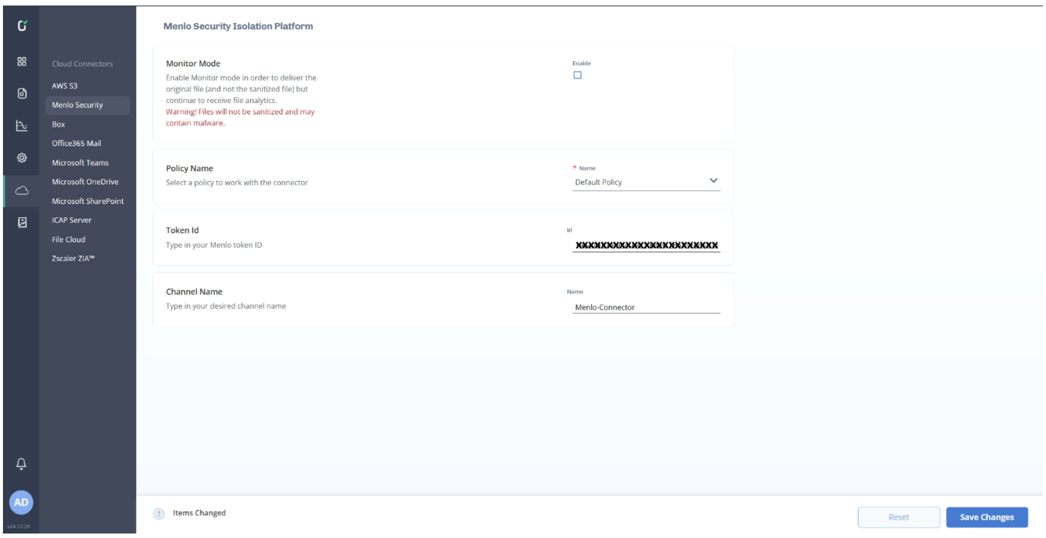
3. Navigate to **Cloud Connectors** > **Menlo Security**.



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.

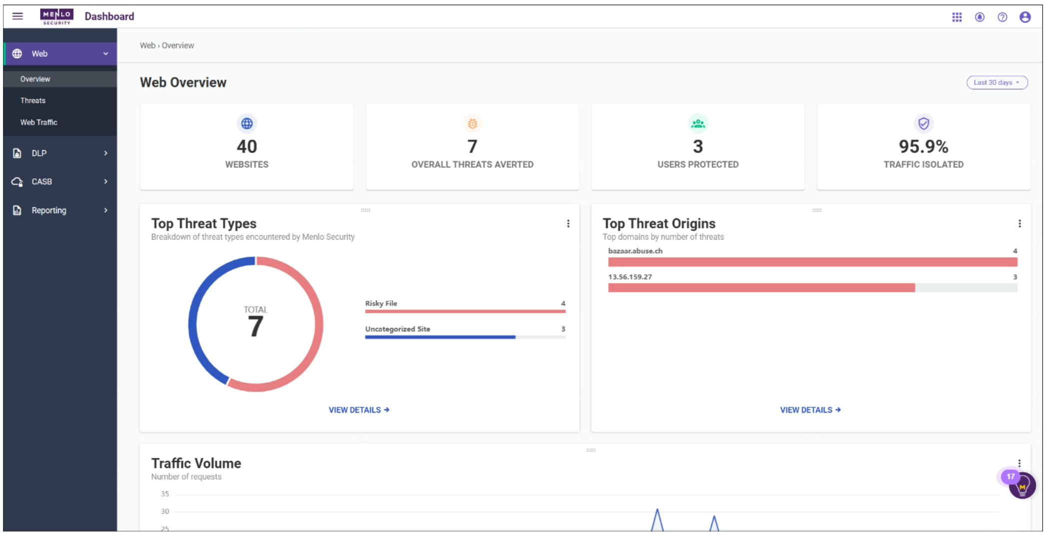
5. Paste the **Votiro Tenant Id** from the clipboard to the **Token Id** field.
6. Type a name for the **Channel Name**, for example "Menlo Connector".
7. Select a **Policy Name** to work with the connector.



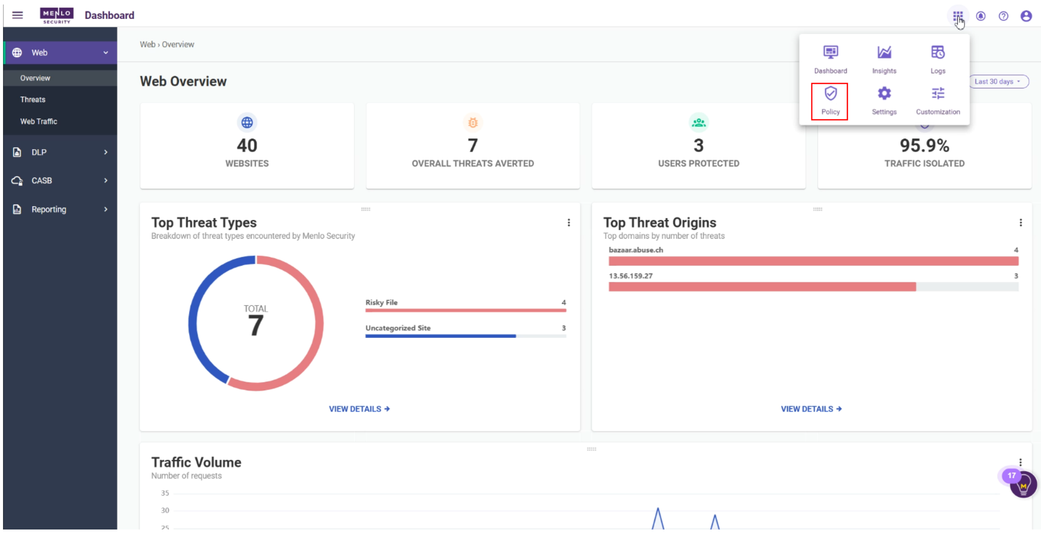
8. Click on **Save Changes**.

Configuration of the Cloud Connector to Menlo Security

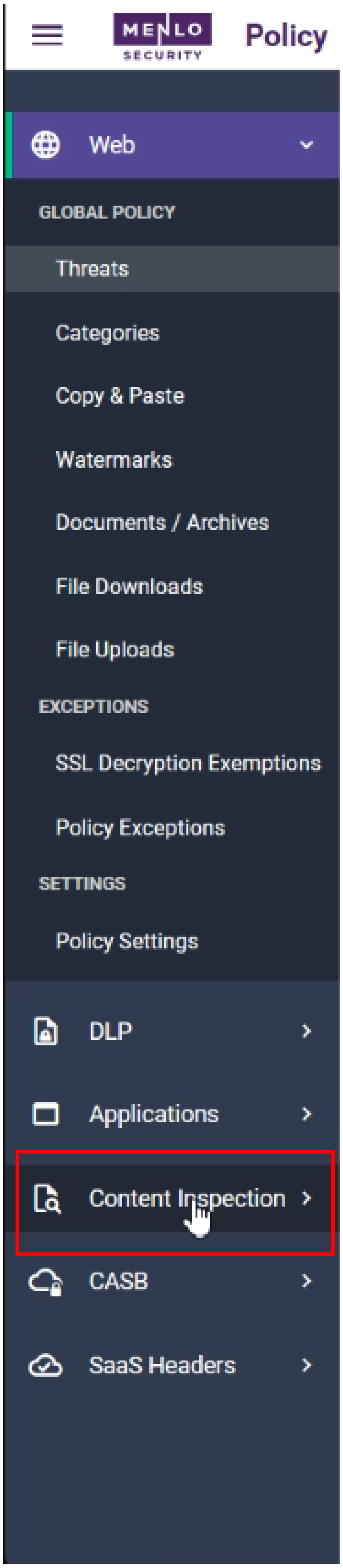
1. Login to the Menlo Administrator page at Admin Portal. The Menlo Dashboard appears:



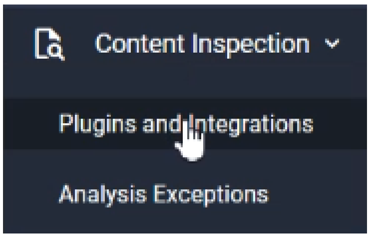
2. Click on the Apps button and select **Policy**.



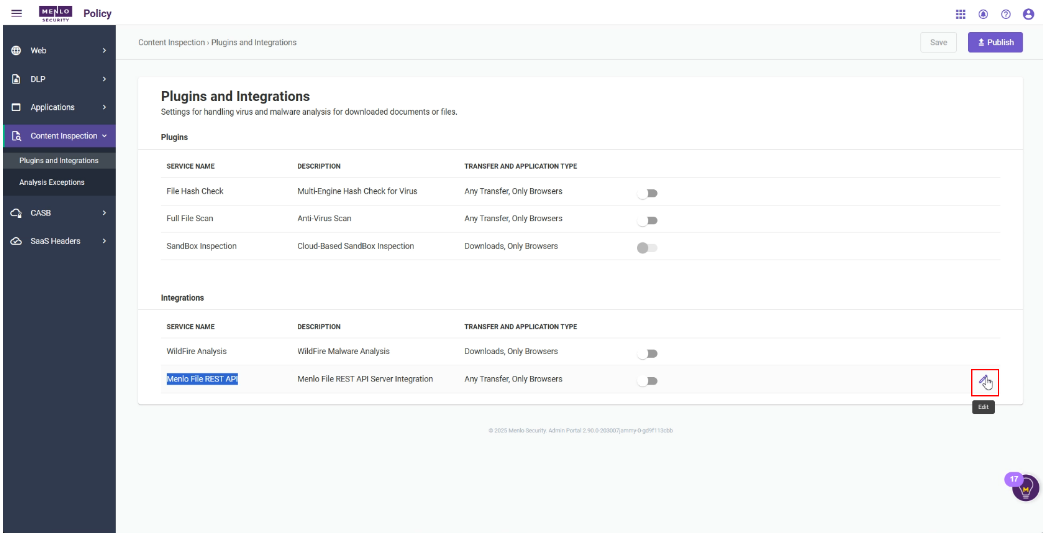
3. On the sidebar menu, click on **Content Inspection**.



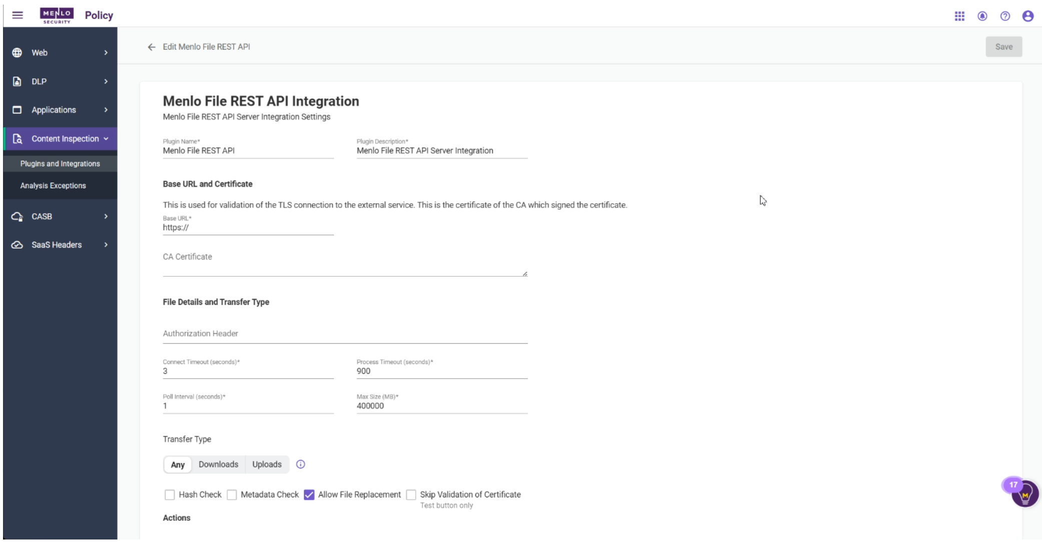
4. From the submenu that opens, click on **Plugins and Integrations**.



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.

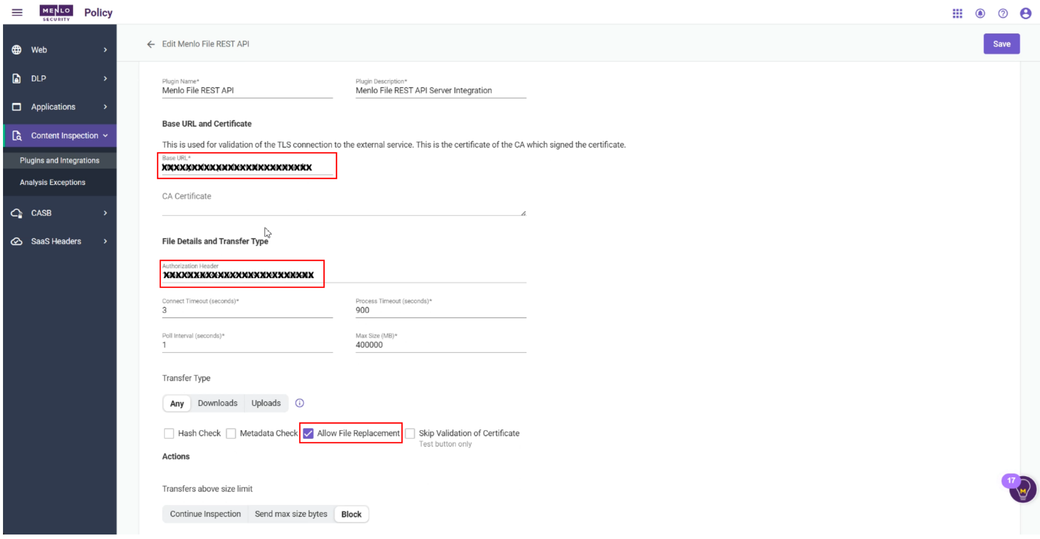


7. On the **Edit Menlo File REST API Integration** page:

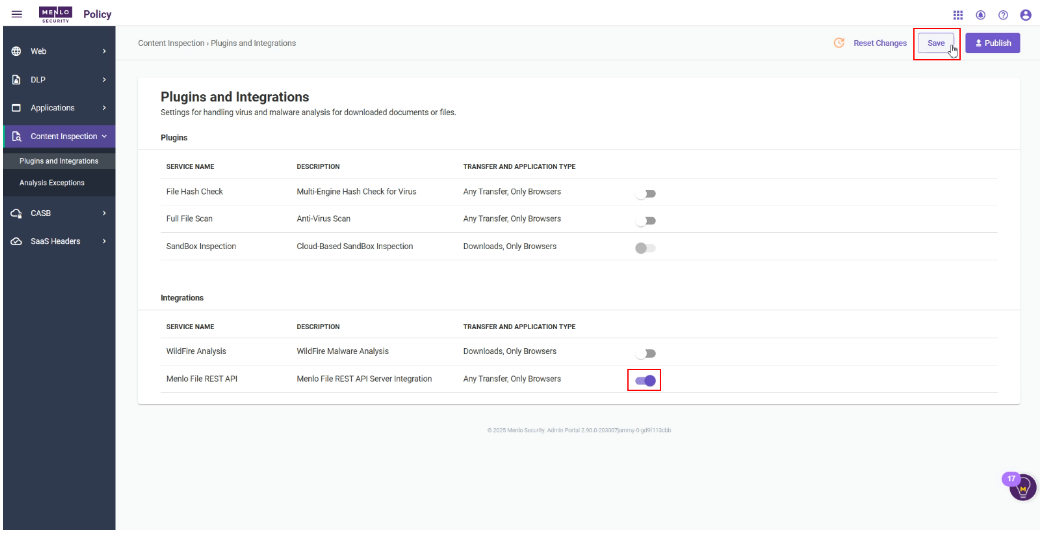
   a. In the **Base URL** field enter the value supplied by Votiro: Base URL.

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

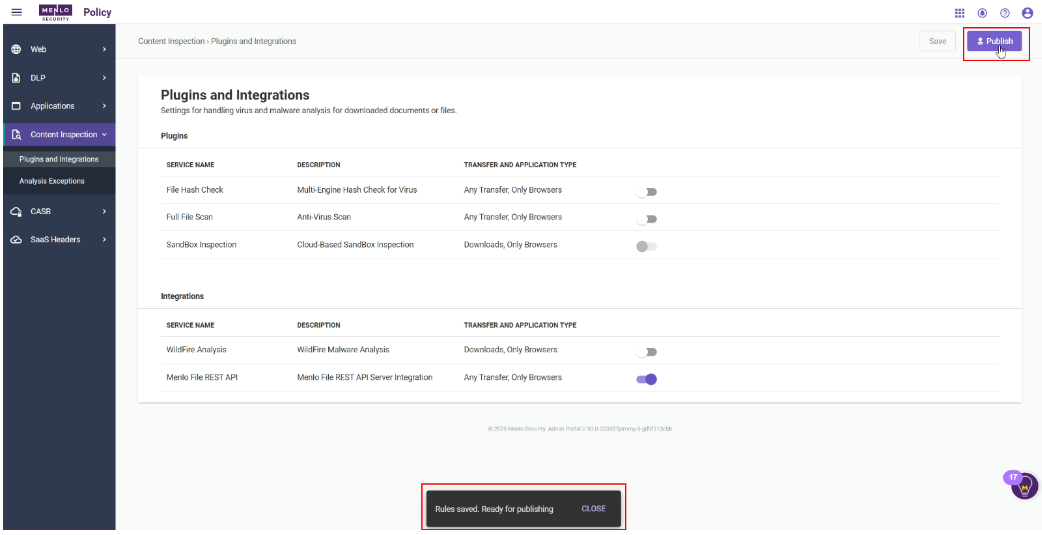
   c. Verify that the field **Allow File Replacement** is checked.



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



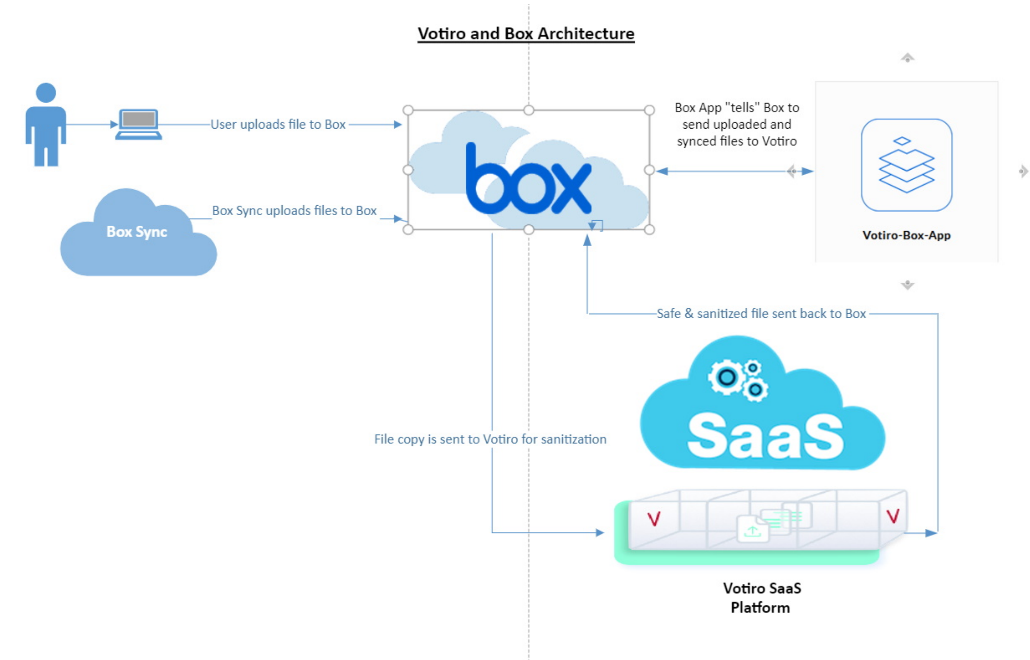
e. The message **Rules Saved. Ready for publishing** should be displayed. Click on the **Publish** button to publish the settings to the tenant.



2.11.3 Box

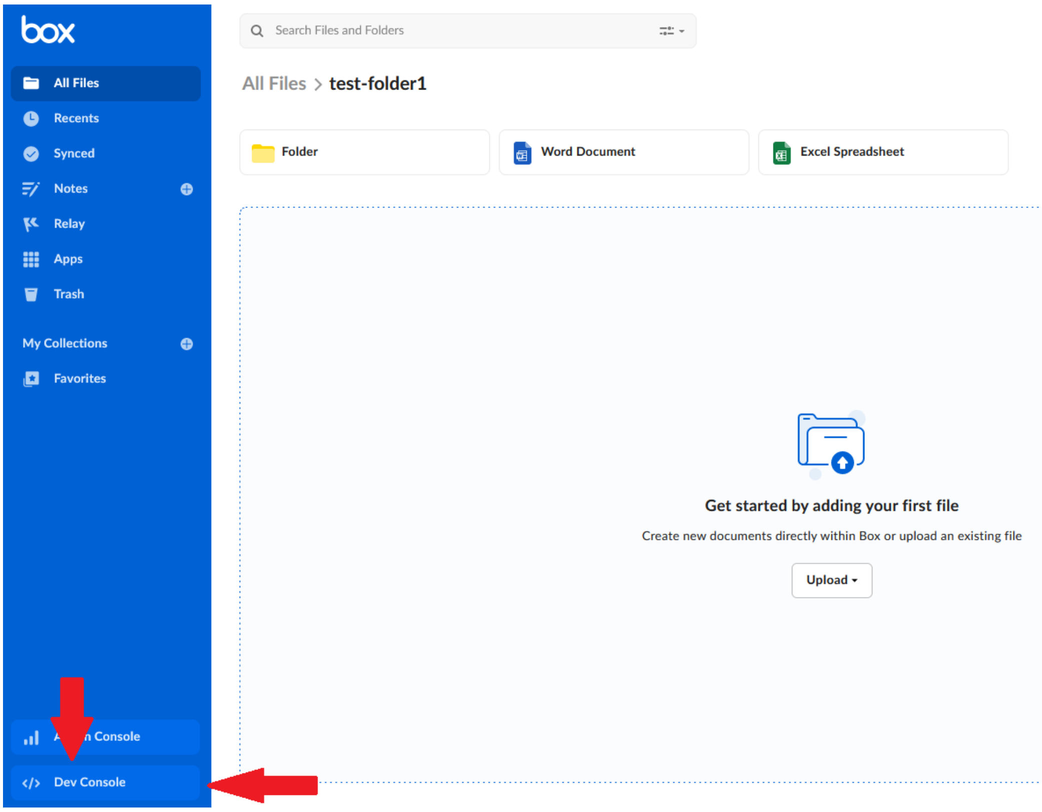
Votiro On-prem and Box

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

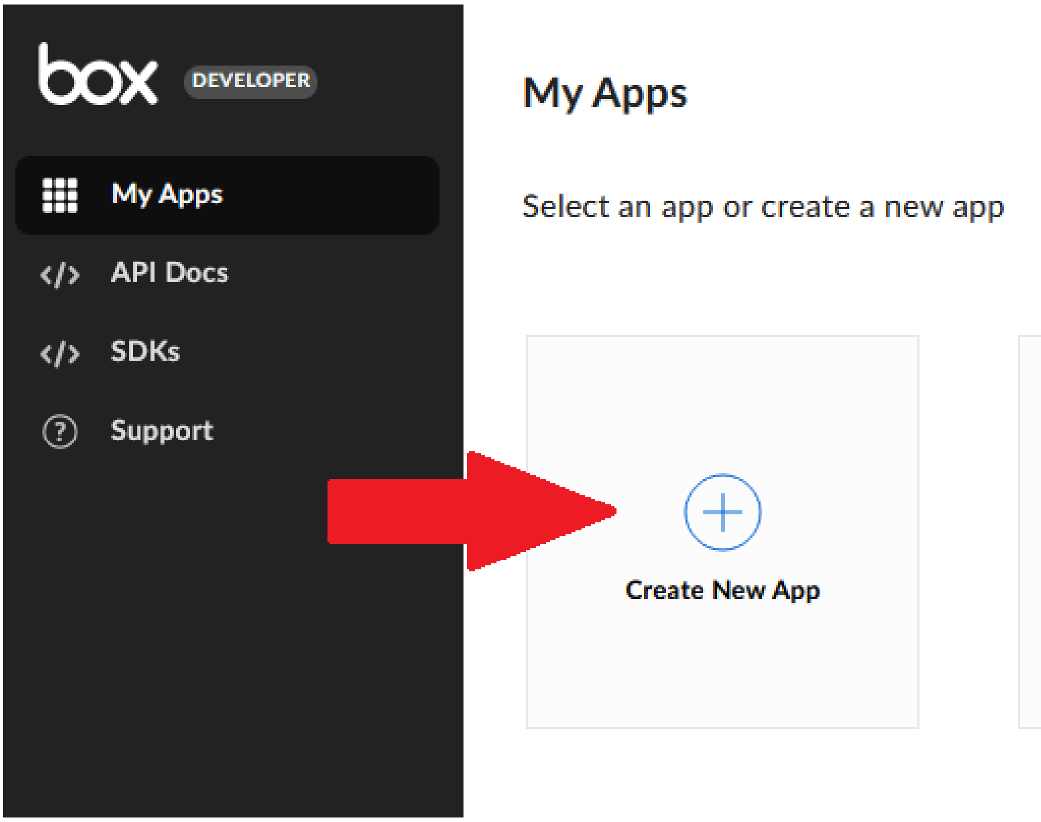


Configuration of an App in Box to Integrate with Votiro On-prem

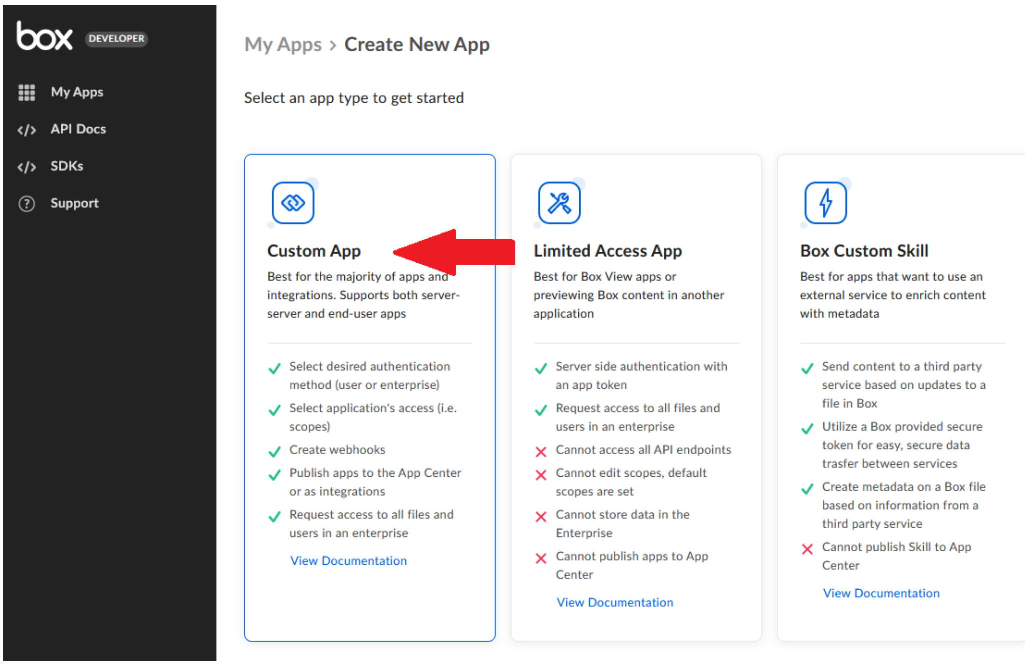
1. Login to your Box.com account with Admin privileges.
2. In the Box menu, select **Dev Console** (if you can't find the button go to Dev Console).



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



4. Select **Custom App**:

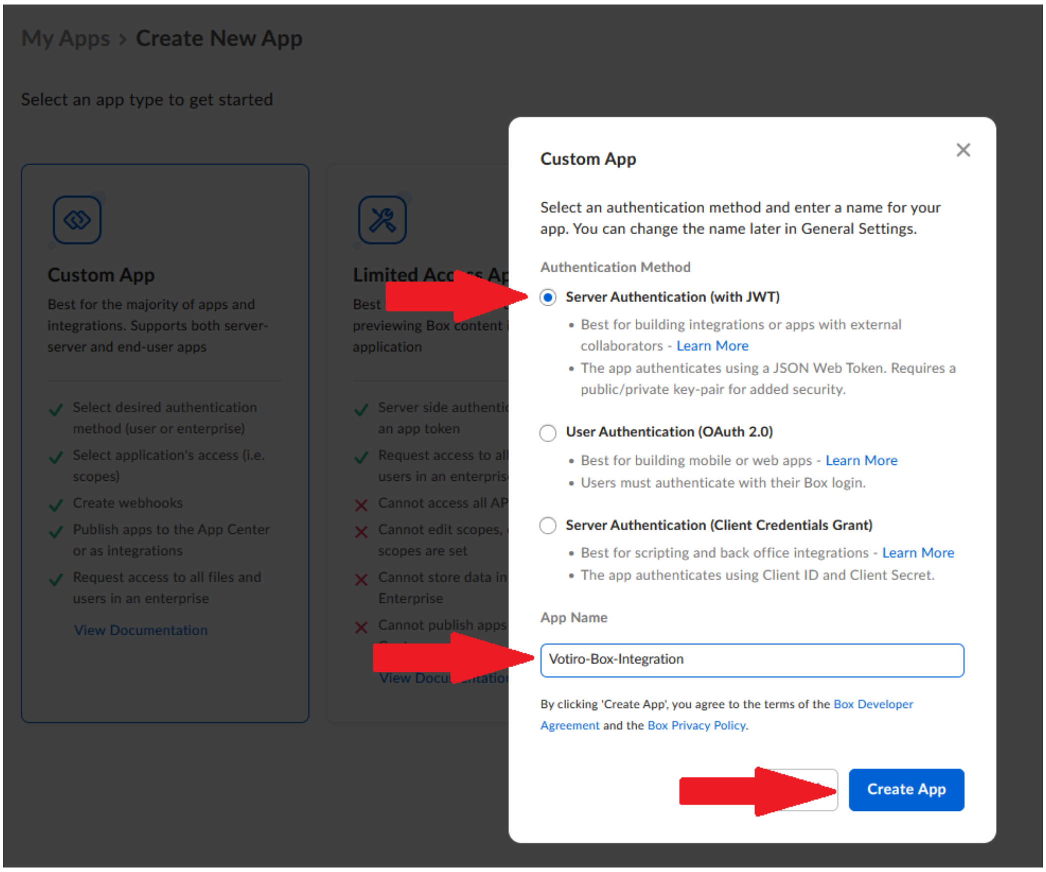


5. On the **Custom App** pane:

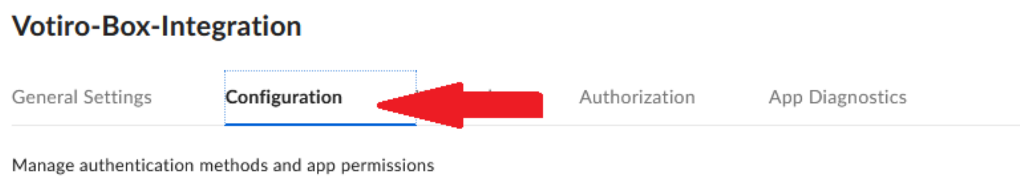
   a. Select the **Authentication Method** as **Server Authentication (with JWT)**.

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

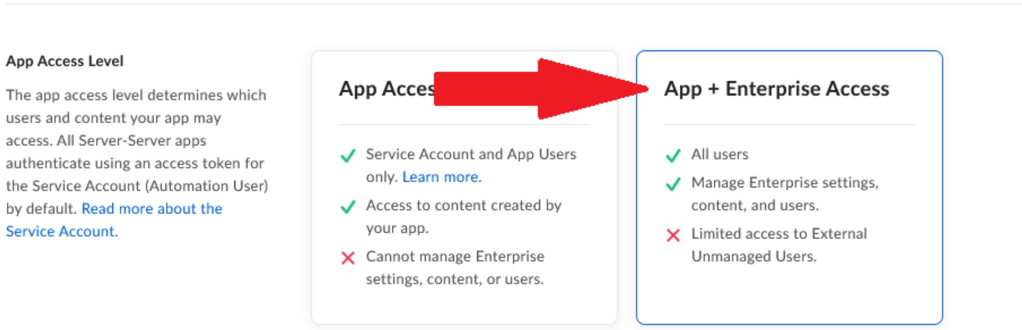
   c. Click on the **Create App** button:



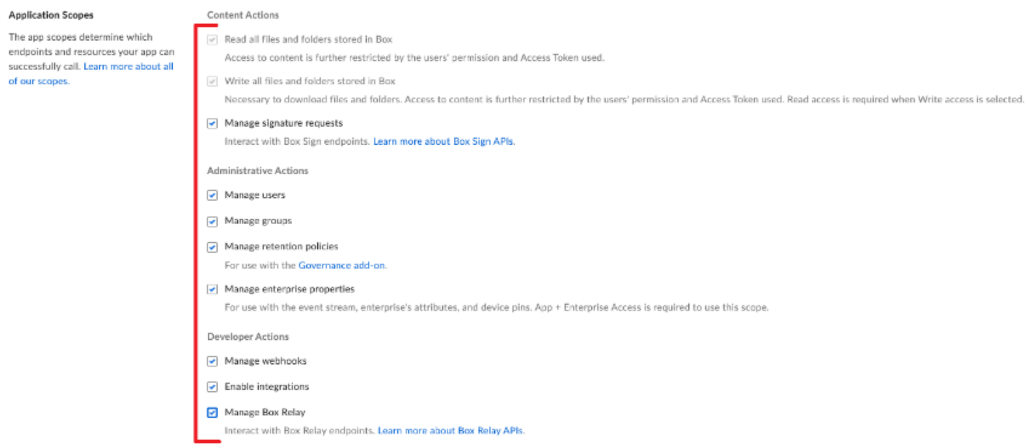
6. Select the **Configuration** tab, then select “App + Enterprise Access”:

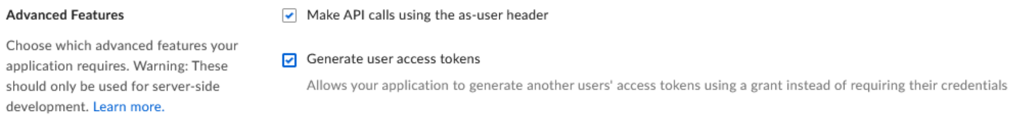


7. Select **App + Enterprise Access**.

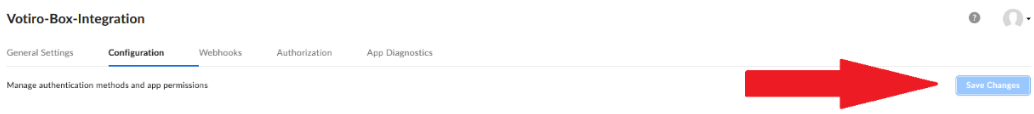


8. Make sure you check all the checkboxes under **Application Scopes** and **Advanced Features**:

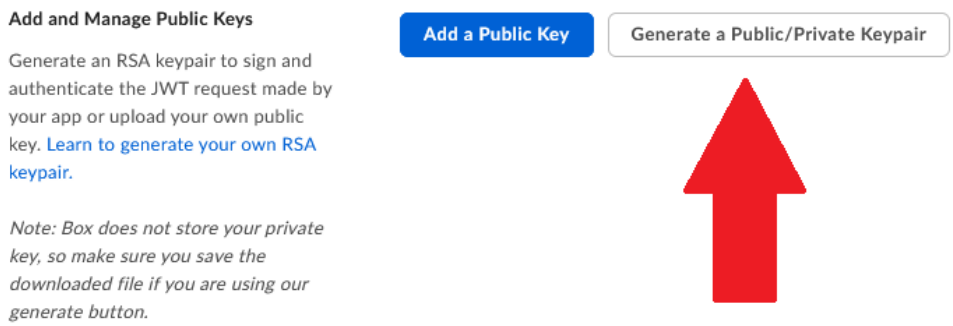


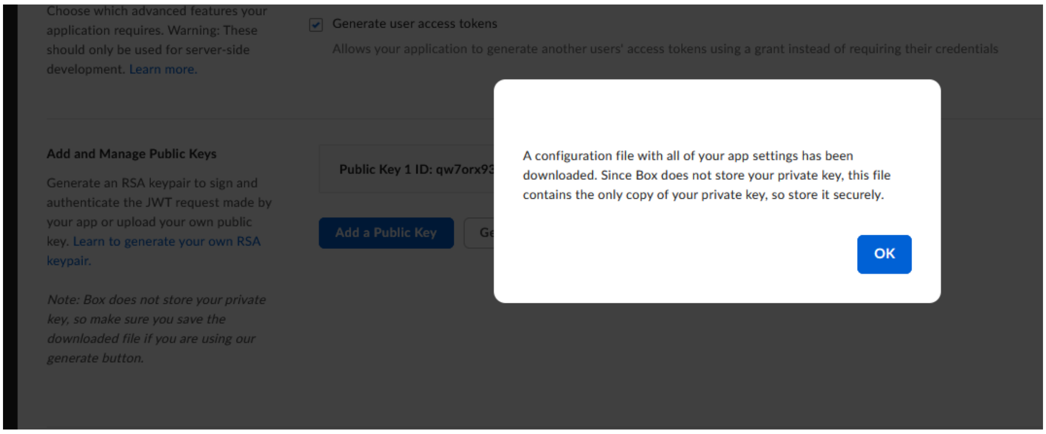


9. Click the **Save Changes** button:



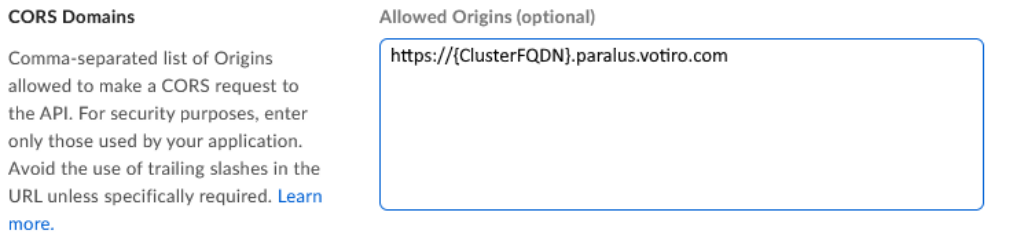
10. Scroll down to **Add and Manage Public Keys** and click on **Generate a Public/Private Keypair** (this step might require 2FA approval) and save the prompted JSON file to your machine:



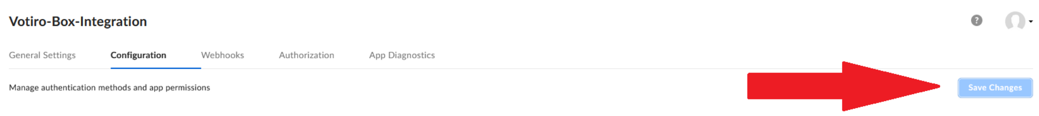


Note: If the JSON file is not downloaded, click again on **Generate a Public/Private Keypair**.

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



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

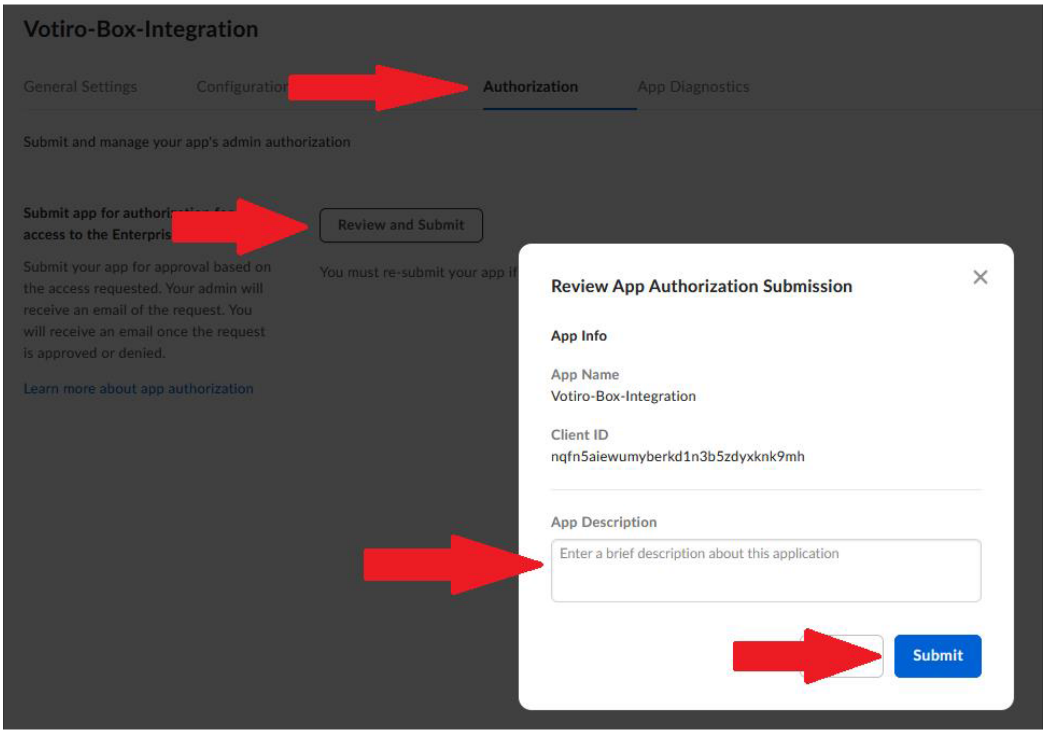


13. Select the **Authorization** tab and:

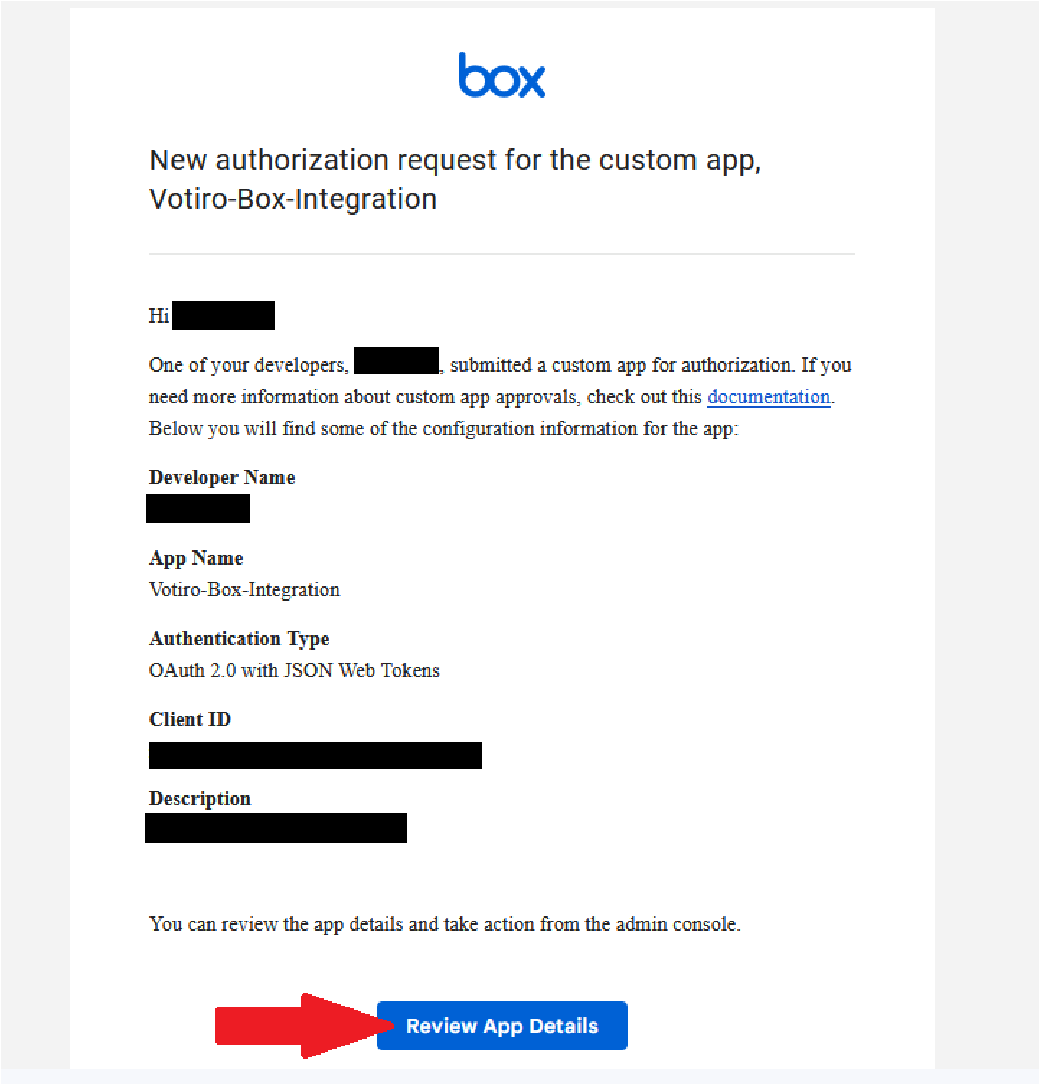
    a. Click on **Review and Submit**.

    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**:



box

New authorization request for the custom app, Votiro-Box-Integration

Hi [redacted]

One of your developers, [redacted], submitted a custom app for authorization. If you need more information about custom app approvals, check out this documentation. Below you will find some of the configuration information for the app:

Developer Name
[redacted]

App Name
Votiro-Box-Integration

Authentication Type
OAuth 2.0 with JSON Web Tokens

Client ID
[redacted]

Description
[redacted]

You can review the app details and take action from the admin console.

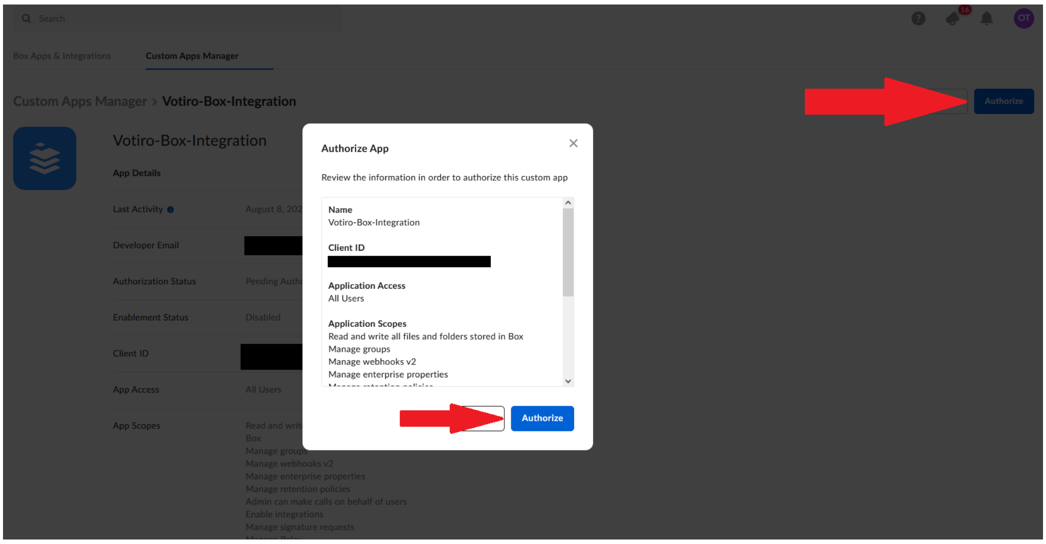
Review App Details

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.

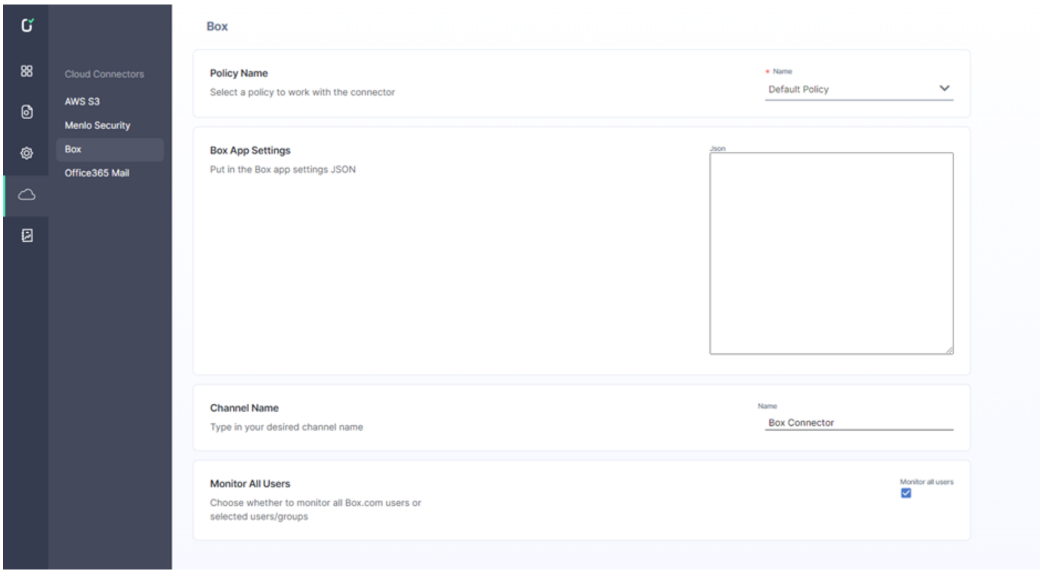
    c. Click on the **Authorize** button:



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

Configuration of the Box App in the Votiro On-prem Management Dashboard

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

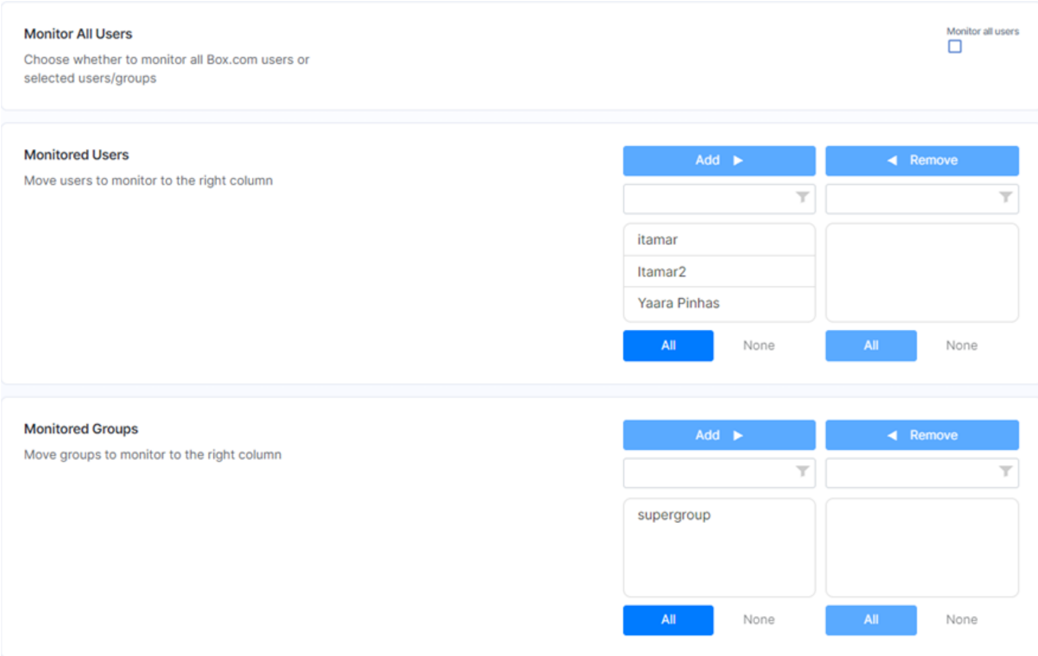


The Box page contains the following fields:

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.

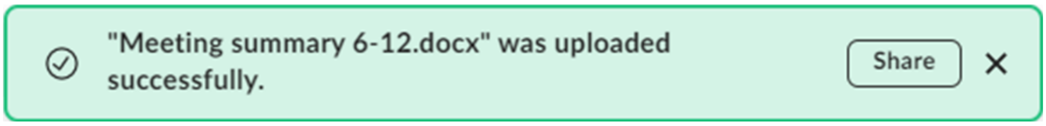
Field	Description
Box App Settings	To integrate with the Box account, add the **Public/Private Keypair** by pasting the content of the JSON file you saved to your machine when creating the Custom App in Box to integrate with Votiro On-prem. The keypair is located in the JSON file.
Channel Name	Specify 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:

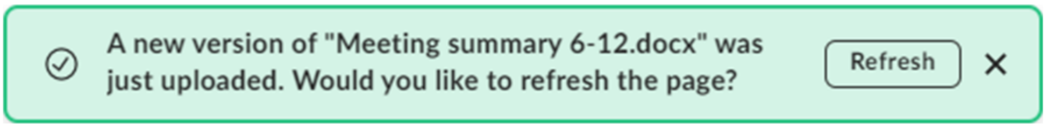


Box App Behavior when Uploading Files

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:

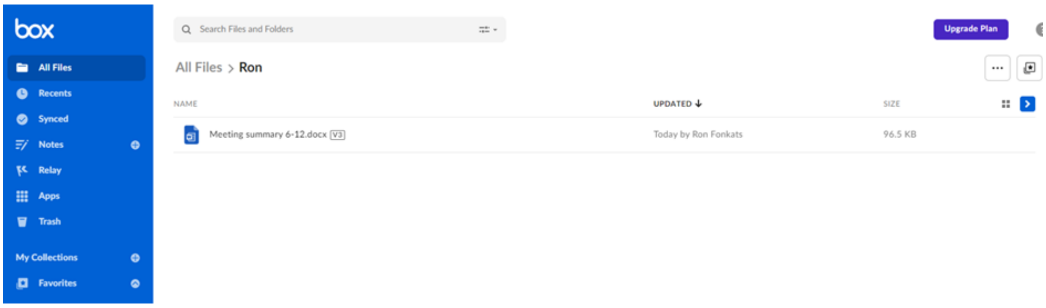


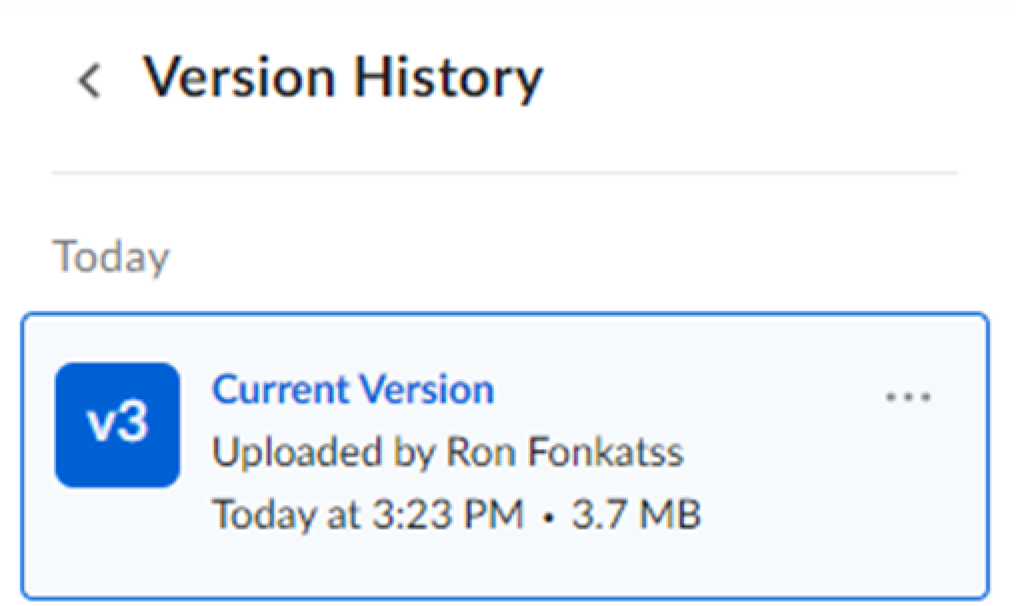
After the sanitization is successfully completed, the original file will be replaced with the sanitized file, and Box will display a message indicating that a new version of the file was uploaded:



Box App Behavior when Versioning Files

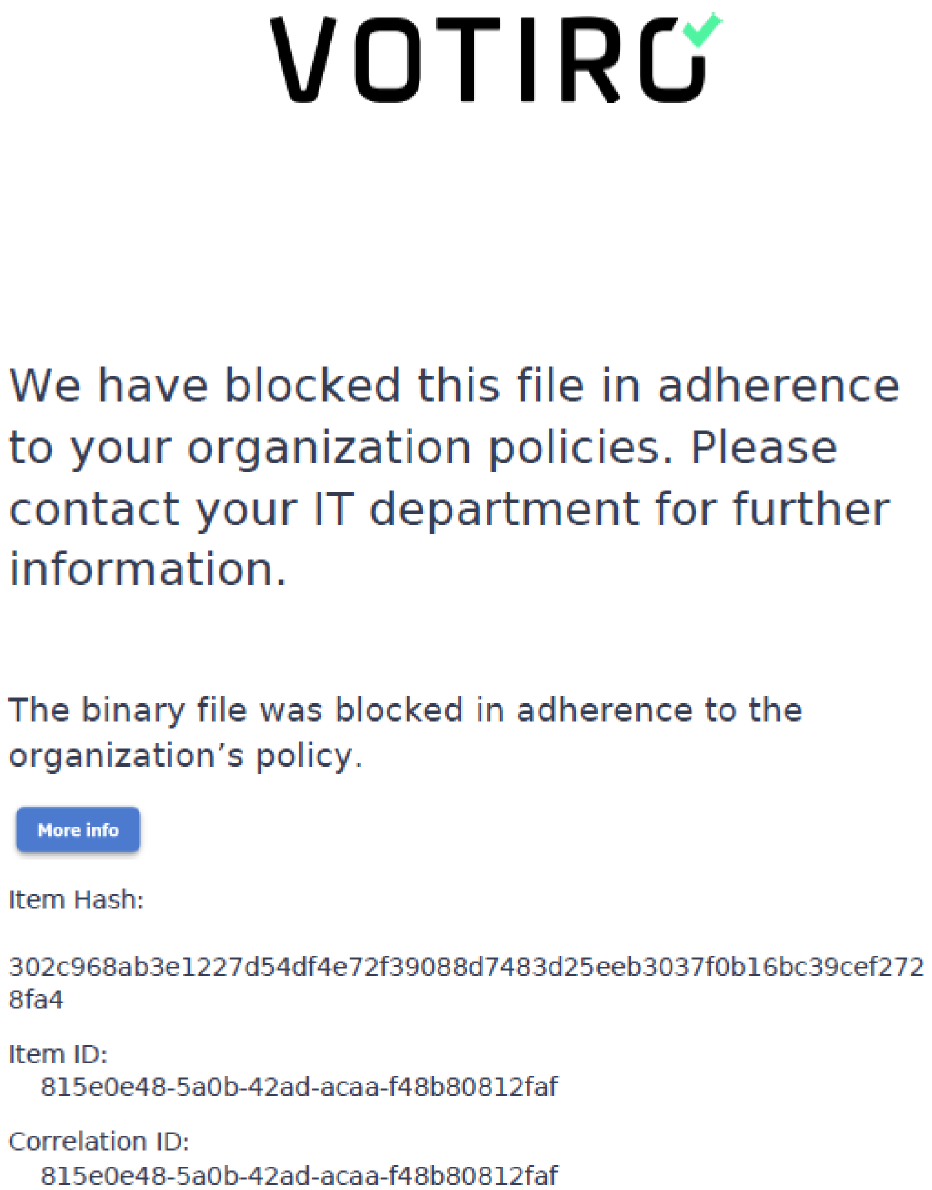
- If an uploaded file was successfully sanitized, the sanitized file will be marked by V3:





- 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:



VOTIRO

We have blocked this file in adherence to your organization policies. Please contact your IT department for further information.

The binary file was blocked in adherence to the organization's policy.

More info

Item Hash:

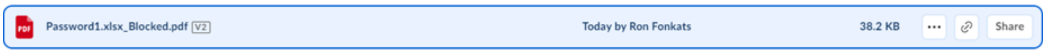
302c968ab3e1227d54df4e72f39088d7483d25eeb3037f0b16bc39cef2728fa4

Item ID:
815e0e48-5a0b-42ad-acaa-f48b80812faf

Correlation ID:
815e0e48-5a0b-42ad-acaa-f48b80812faf

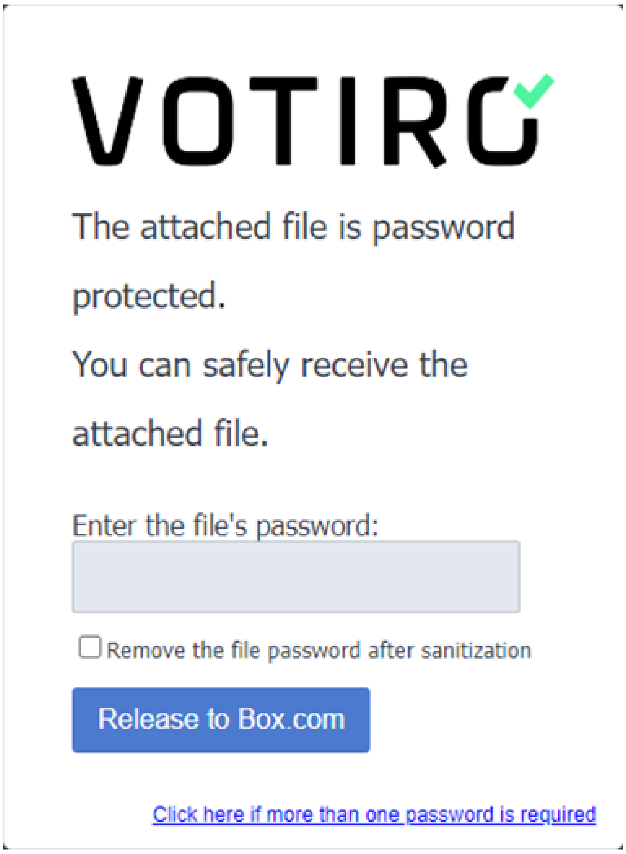
Box App Behavior for Password Protected Files

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

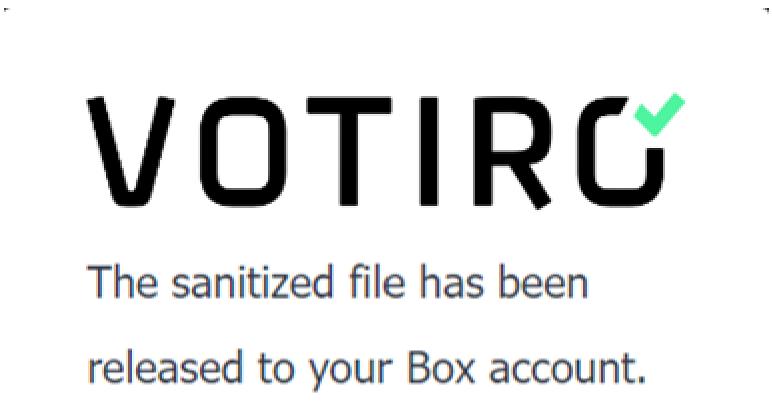


To release a password protected file that was blocked:

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.

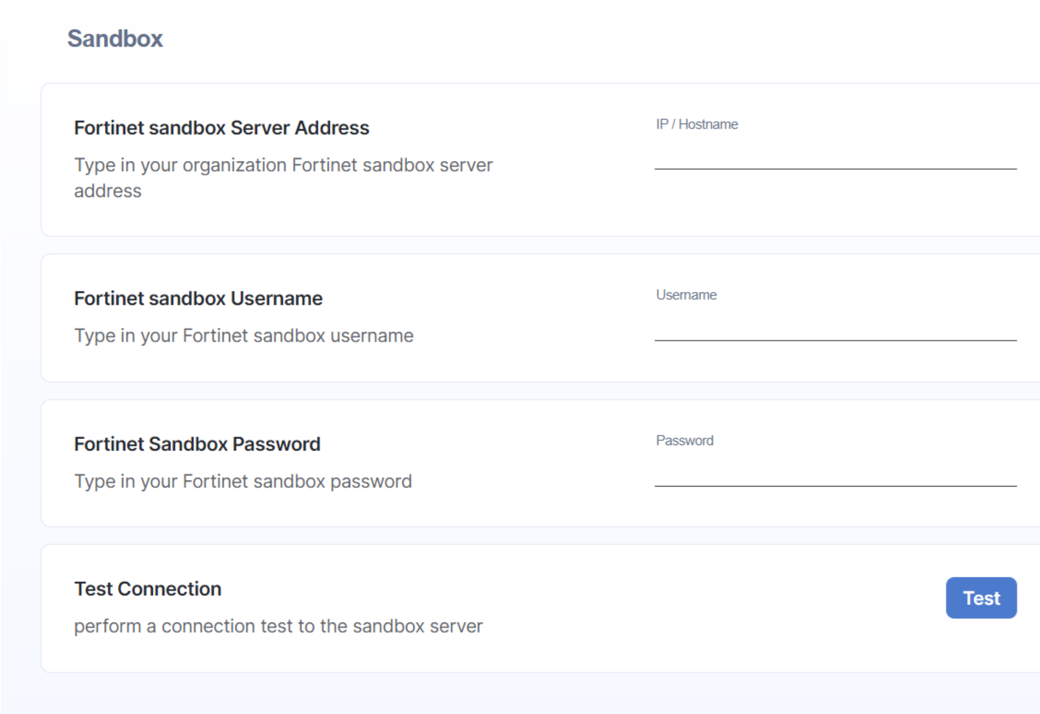
2.11.4 Fortinet Sandbox

Prerequisites

To activate Fortinet Sandbox integration, please contact Votiro support.

Configuring the Fortinet Sandbox Integration

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

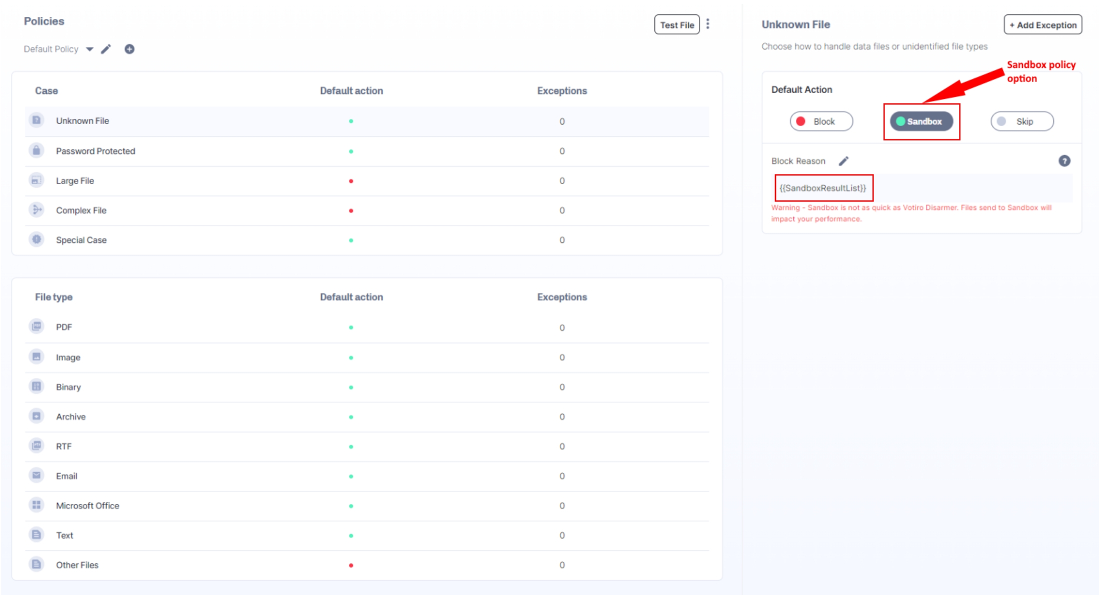


1. Enter the following fields:
   - Fortinet sandbox Server Address
   - Fortinet sandbox Username
   - Fortinet Sandbox Password
2. Press the **Test** button. This action tests the connection to the Fortinet Sandbox Server. Success/Failure is indicated by √/X.

Note: Saving the configuration will be possible only after the test connection succeeds.

Setting a Sandbox Policy

After the sandbox settings are successfully configured, a new Sandbox option will appear in the **Policies** Dashboard.



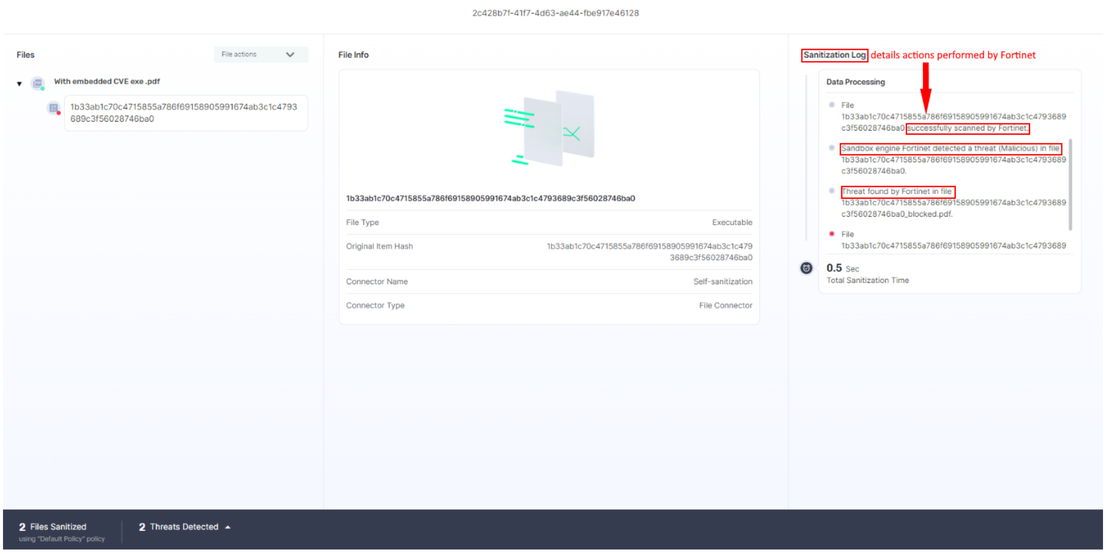
Select the **Default Action** by pressing the **Sandbox** button. The file will be either blocked or sent, depending on the outcome of the Sandbox analysis.

The **Block Reason** will display the Sandbox Result.

> **Note**: The Sandbox is not as quick as Votiro Disarmer. Files sent to the Sandbox may impact performance.

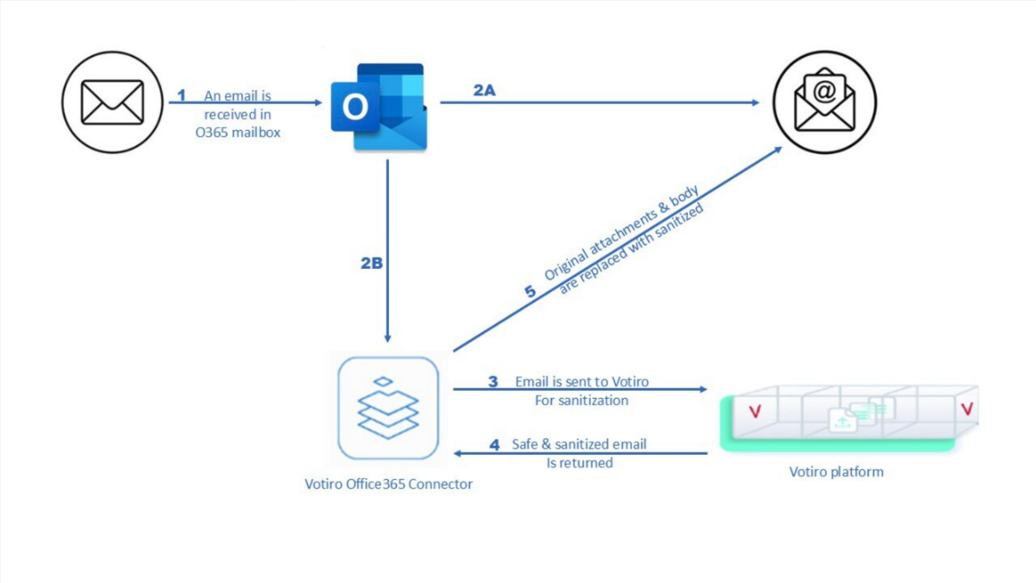
File Information from the Sandbox

The results of the Sandbox processing of the file will appear in the Sanitization log.



2.11.5 Office365 Mail

Office365 High-level Workflow

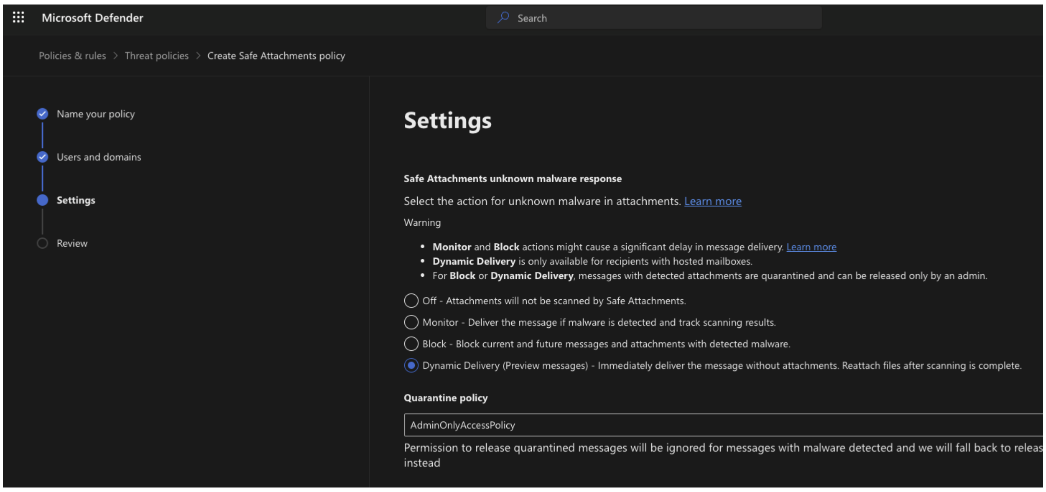


Prerequisites

Votiro VA On-prem users need to contact Votiro support with the FQDN cluster to register Votiro's O365 application.

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 On-prem. Consider selecting the **Monitor** or **Block** option instead:



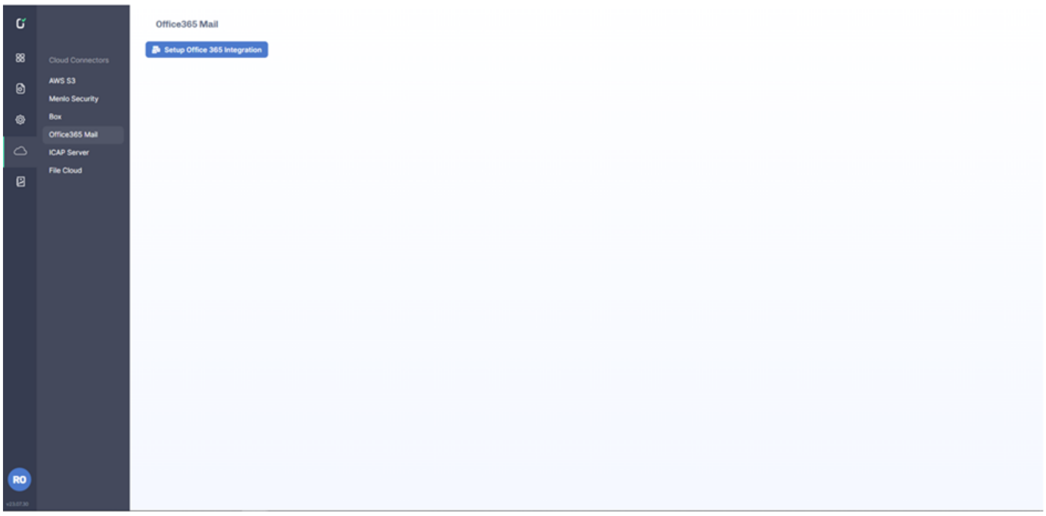
- When sending an email to a Microsoft 365 group, it can either be delivered individually to each group member's mailbox or appear as a single copy in the group's dedicated folder, depending on the group's configuration. This behavior is determined by the setting explained in the Microsoft documentation: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

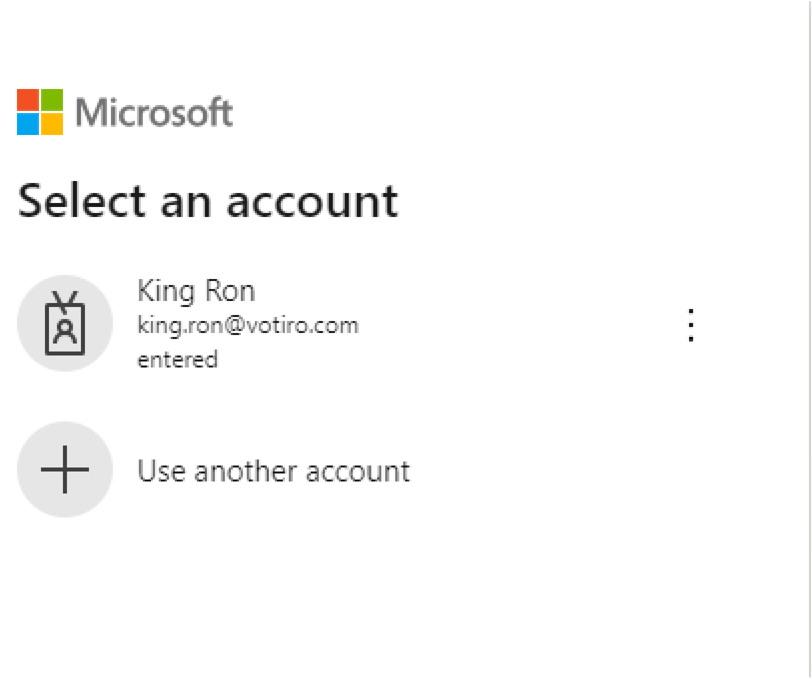
Office365 Integration Procedure

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

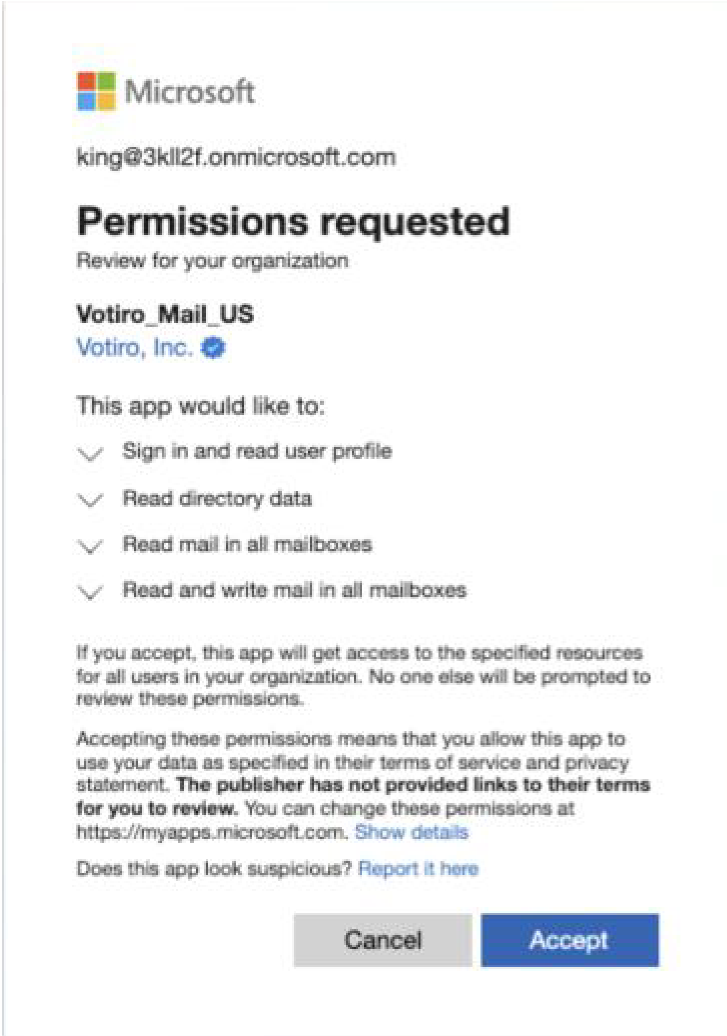


2. Click on the **Setup Office 365 Integration** button. The Votiro product will be redirected to Microsoft user authentication.

3. Select your Admin account.

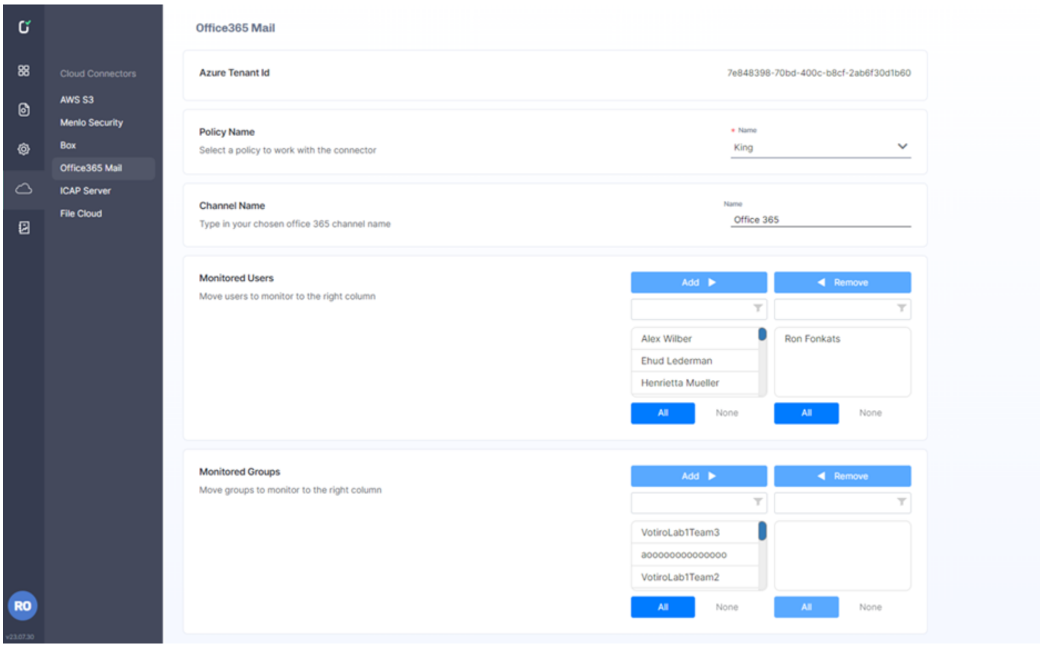


4. After authenticating with the selected Admin user, approve Votiro product permissions and click on **Approve** to complete the successful integration.



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:

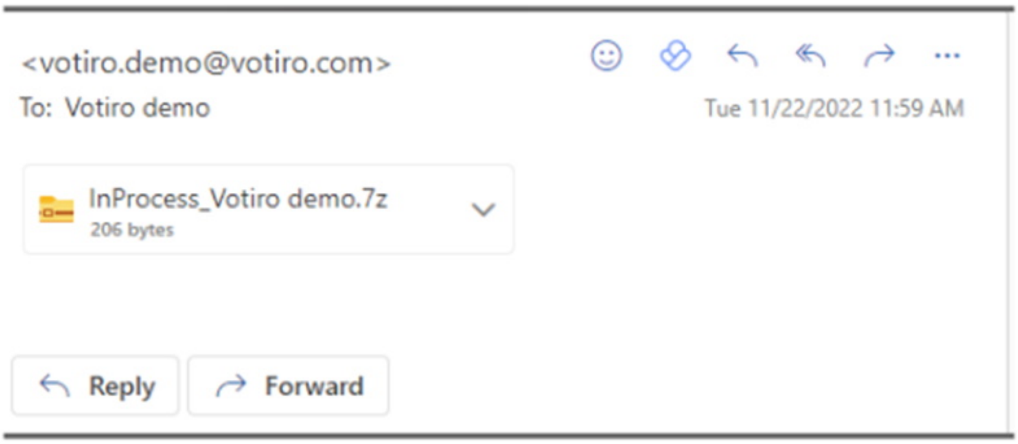
Element	Field	Description
1	Azure Tenant Id	The organization's Azure Tenant ID **Note**: This field cannot be changed.
2	Policy Name	Specify a policy for the Office 365 connector to work with. Select the **Default Policy** policy if you have not created an alternative policy to use.
3	Channel Name	Specify 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.

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**.

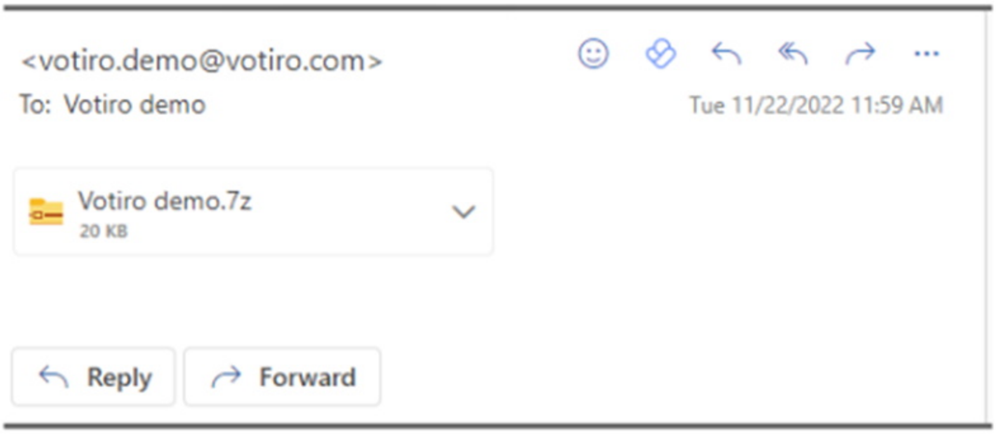
Office 365 Behavior when using the Votiro Office 365 App

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

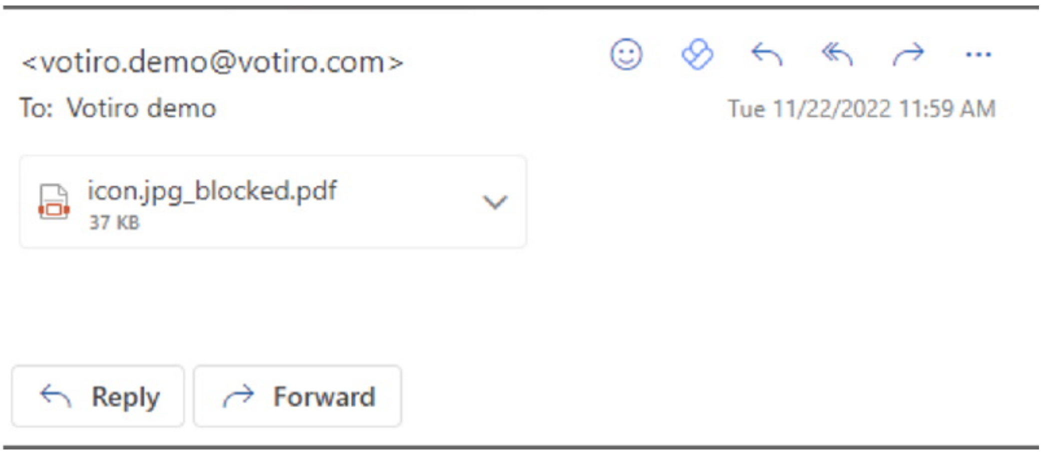


3. After the attached file completes the sanitization processing, the results are displayed.

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:

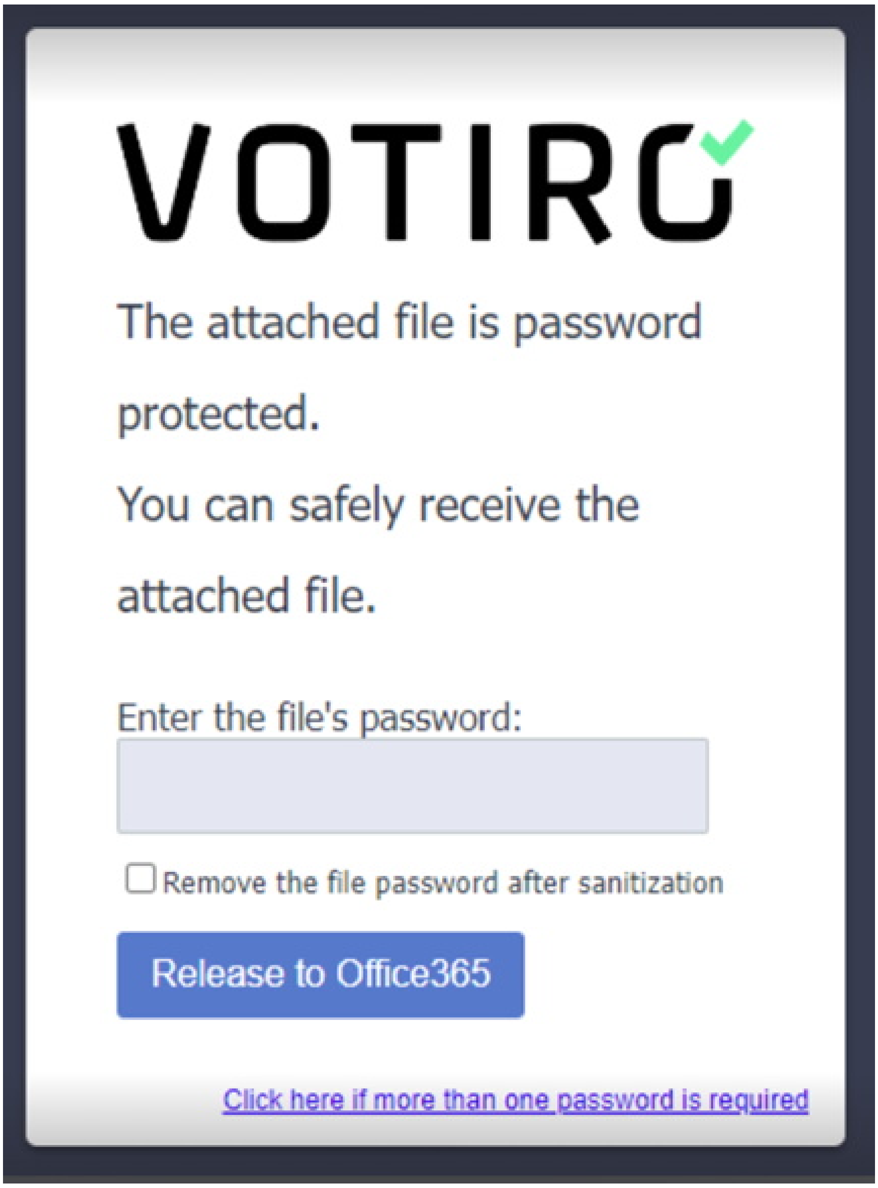
1. In Office 365, Votiro receives the email at the same time the client gets it.
2. Then we sanitize the file and replace the file (on the Microsoft Office 365 server).
3. Once the client "refreshes" the attachment, they will get the sanitized version or blocked file.
4. Till then, it all depends on 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

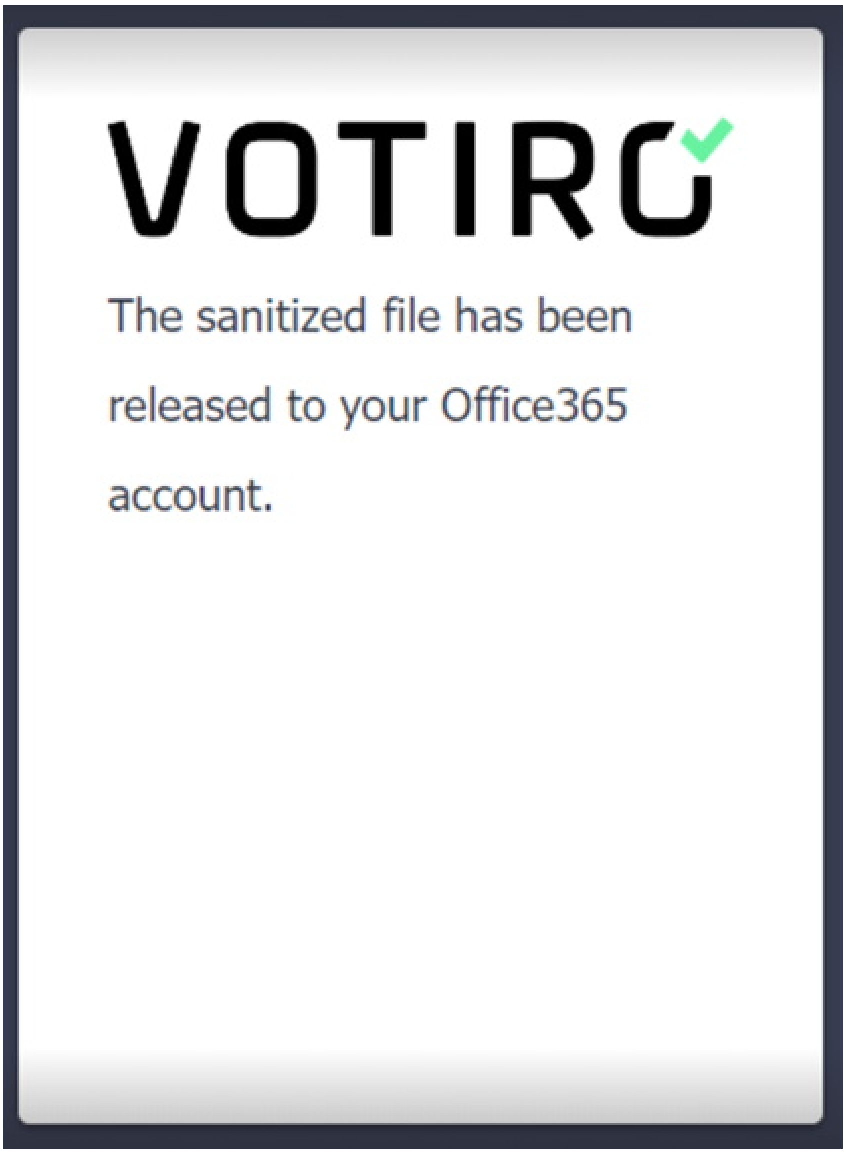
1. If the user receives an email with an attached password protected file, the attached file will be replaced with a password protected blocked PDF.

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

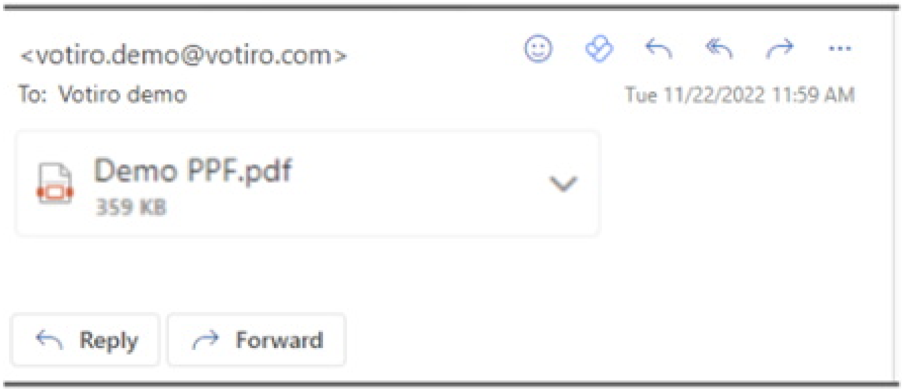
a. In the blocked PDF, click on **I have a password**. The password protected portal is displayed:



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:**

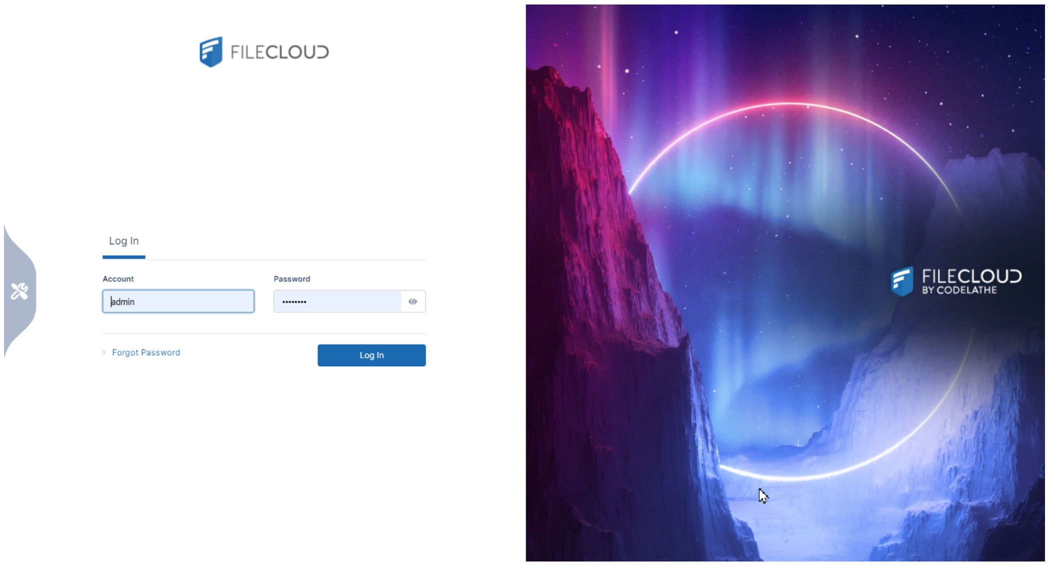


2.11.6 FileCloud

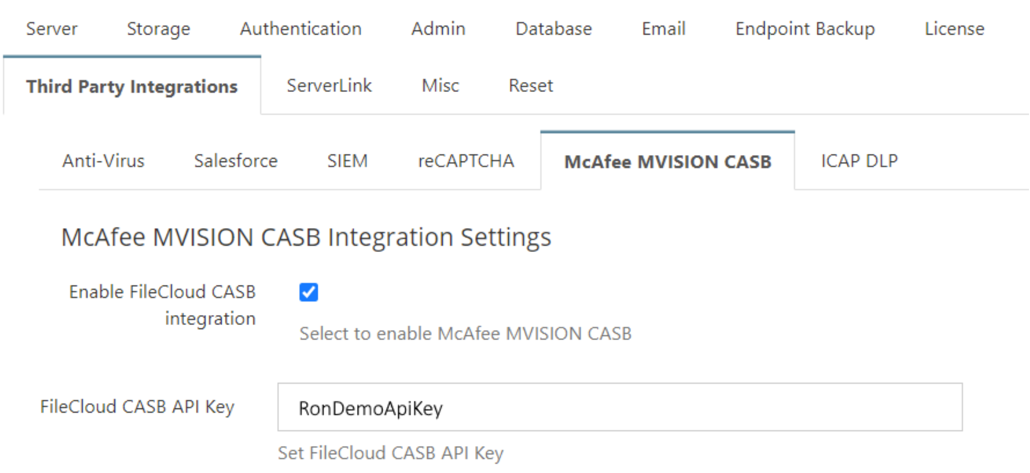
FileCloud Configuration for Integration with Votiro On-prem

To authenticate FileCloud with Votiro On-prem, generate an API key.

1. Login to your FileCloud account with Admin privileges.



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



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

Creation of a FileCloud Output Folder

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

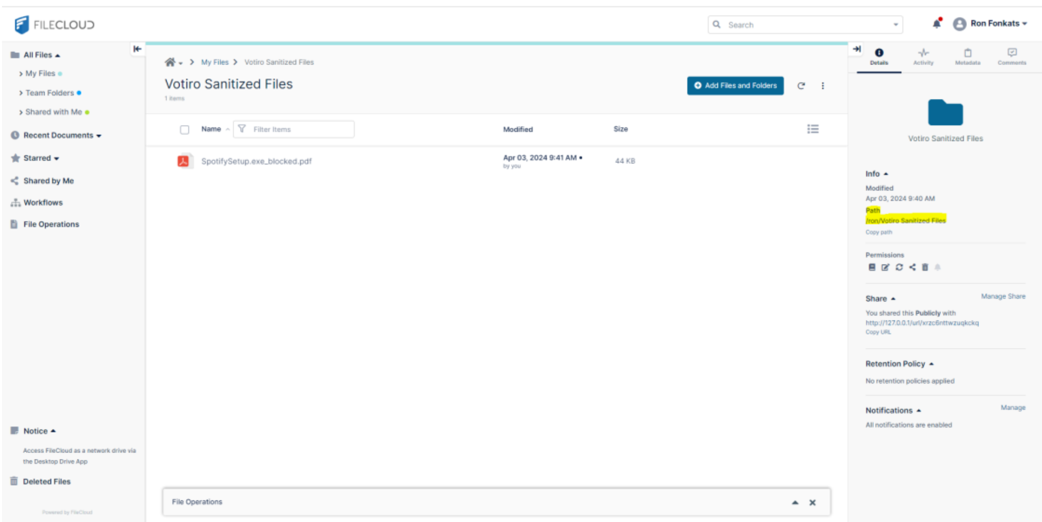
Customers can choose an output folder, and every file that a FileCloud user uploads to any desired folder will be sanitized and placed inside the designated FileCloud output folder.

1. Open the FileCloud console.

2. Select **All Files** > **My Files**.

3. Create a new folder. This will serve as the output folder.

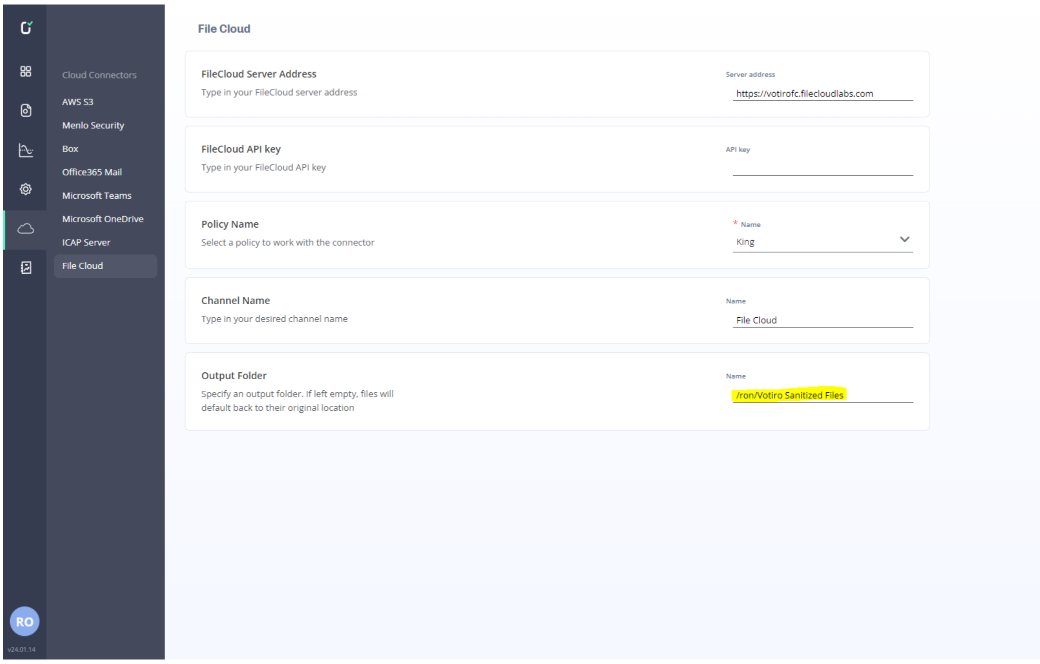
4. Copy the new folder path (it will be needed for configuration of FileCloud in the Votiro Management Dashboard).



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

Configuration of FileCloud in the Votiro On-prem Management Dashboard

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



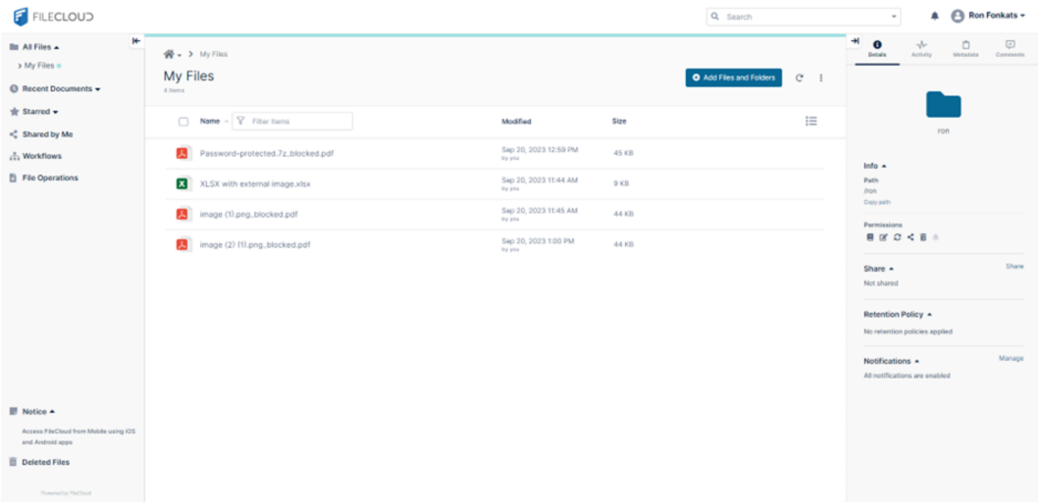
The File Cloud page contains the following fields:

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

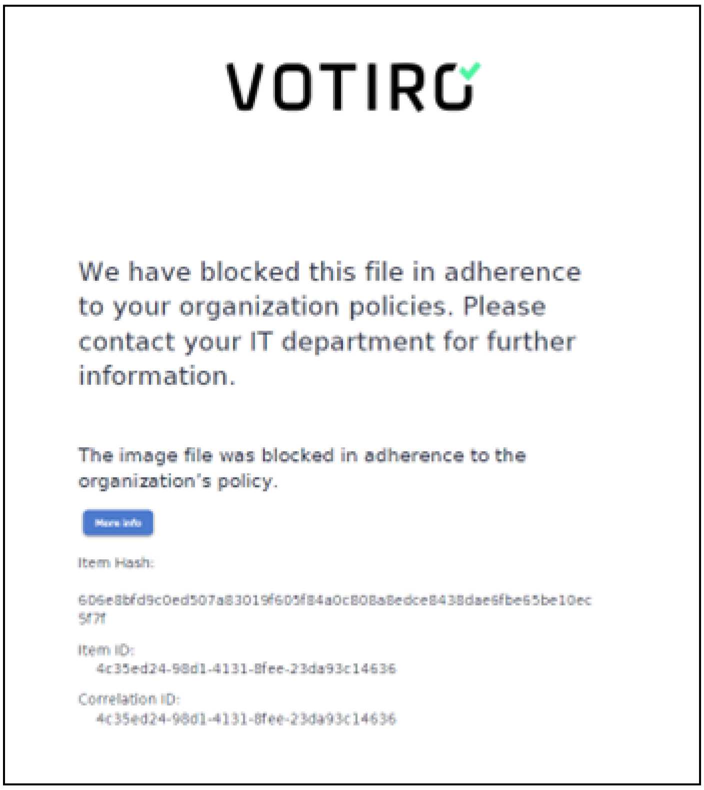
Save the configuration.

FileCloud Behavior when Uploading Files

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

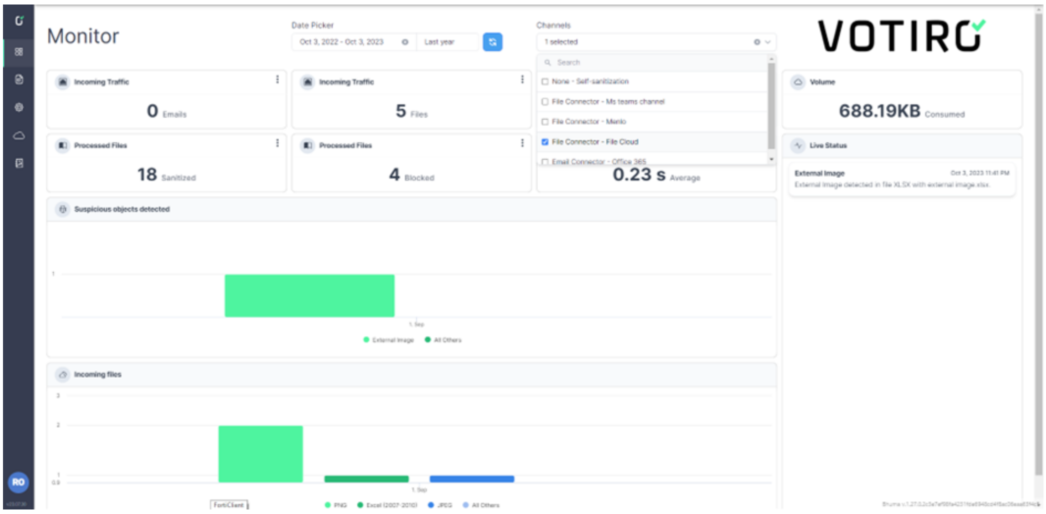


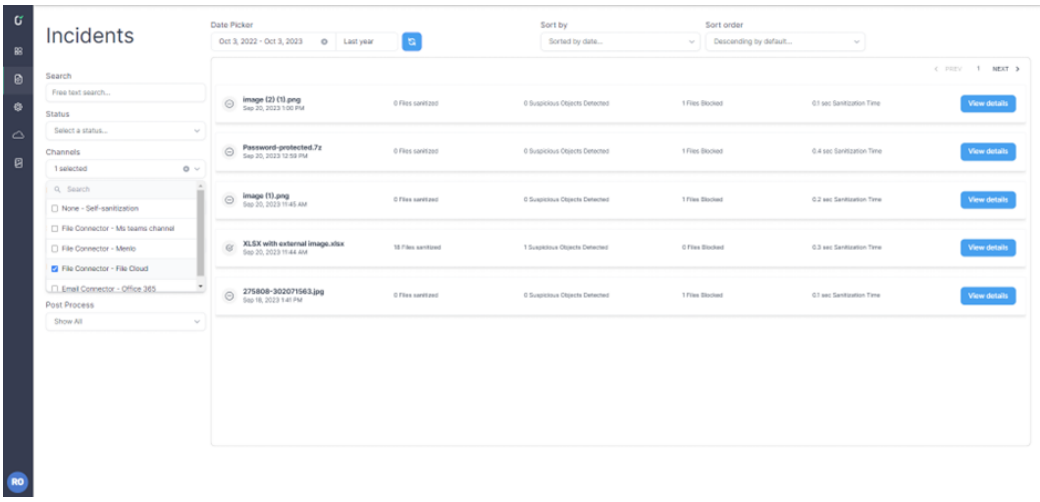
If the file was blocked, the original file is replaced by a blocked PDF that contains an explanation of the reason for blocking the file.

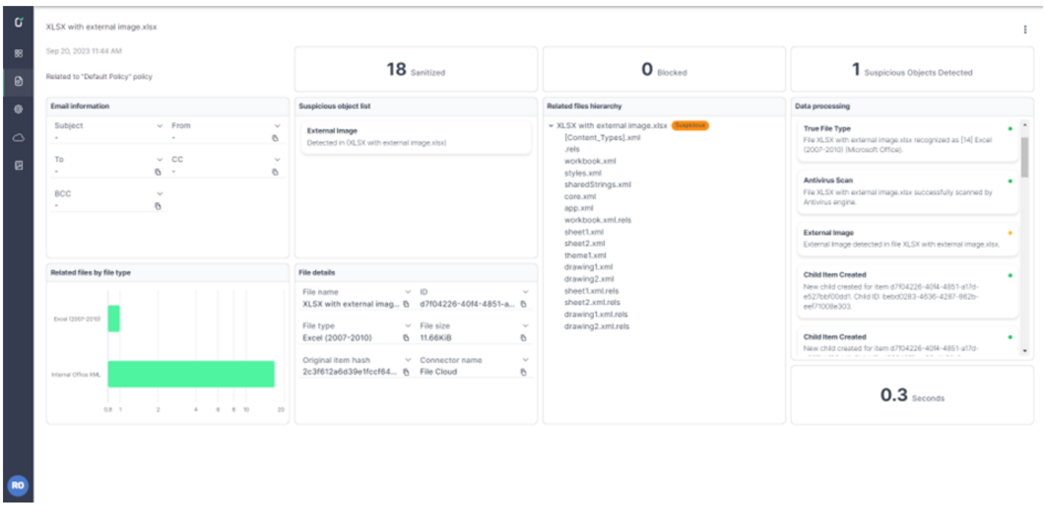


Votiro Management Console – Monitoring

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







Limitations

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

2.11.7 Chrome Browser Extension

Description

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

The browser extension can be:

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

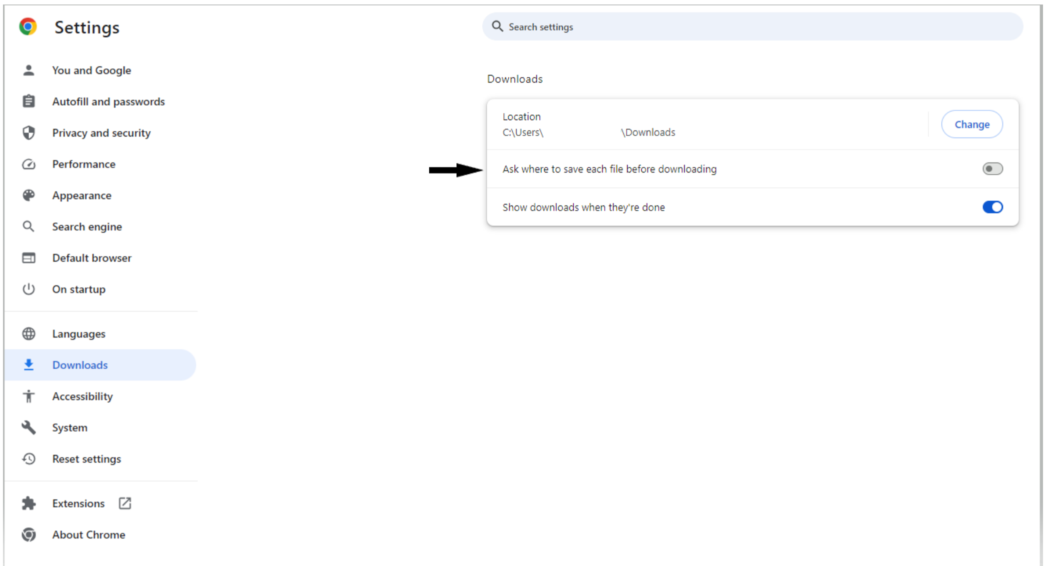
The user's manual is described at Chrome Extension User's Manual.

Limitations

- The Chrome browser extension does not work with Microsoft 365 webmail.
- The Chrome browser extension does not support the Chrome browser option to enable the user to indicate where to save each file before downloading. You must disable this option as follows:

  a. In the Chrome browser, navigate to **Settings** > **Downloads**.

  b. Disable **Ask where to save each file before downloading**.



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

Centralized Deployment using GPO (Group Policy Object)

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

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

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

Centralized Deployment Procedure

1. **Add Chrome Policy Templates**

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

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

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

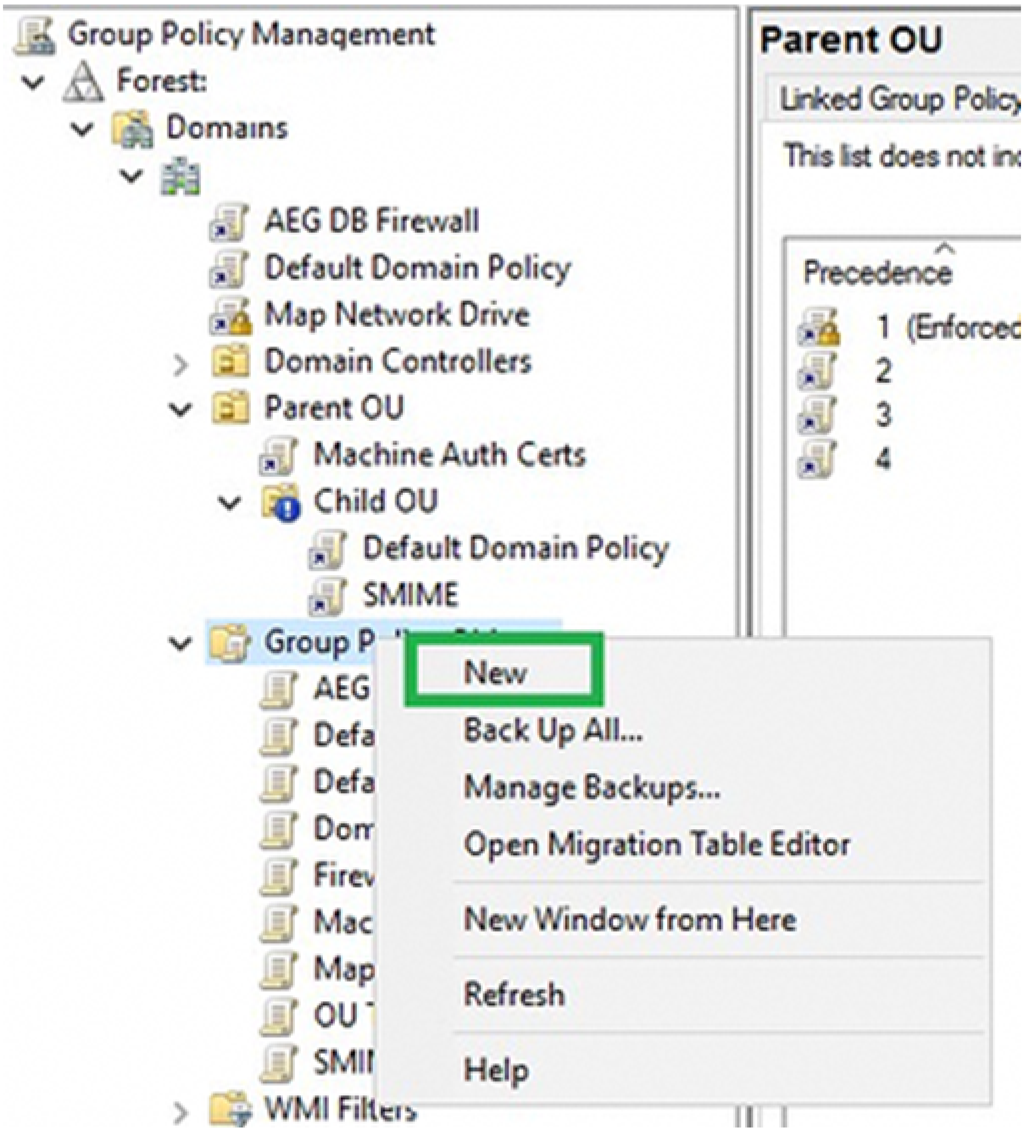
   c. Navigate to the directory in which you extracted the Google Chrome Bundle and copy to the directory *C:\Windows\PolicyDefinitions\en-US* the **chrome.adml** file located in the appropriate directory below:

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

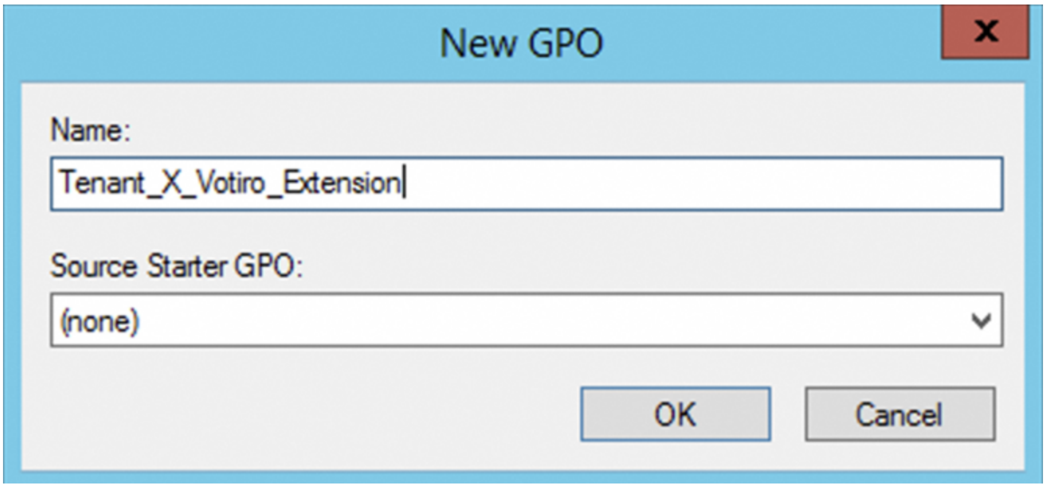
> **Note**: If a language other than en-US is desired, navigate to the appropriate language directory within the admx directory, for example, for Spanish: es-ES, and copy to the appropriate language directory within *C:\Windows\PolicyDefinitions*.

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

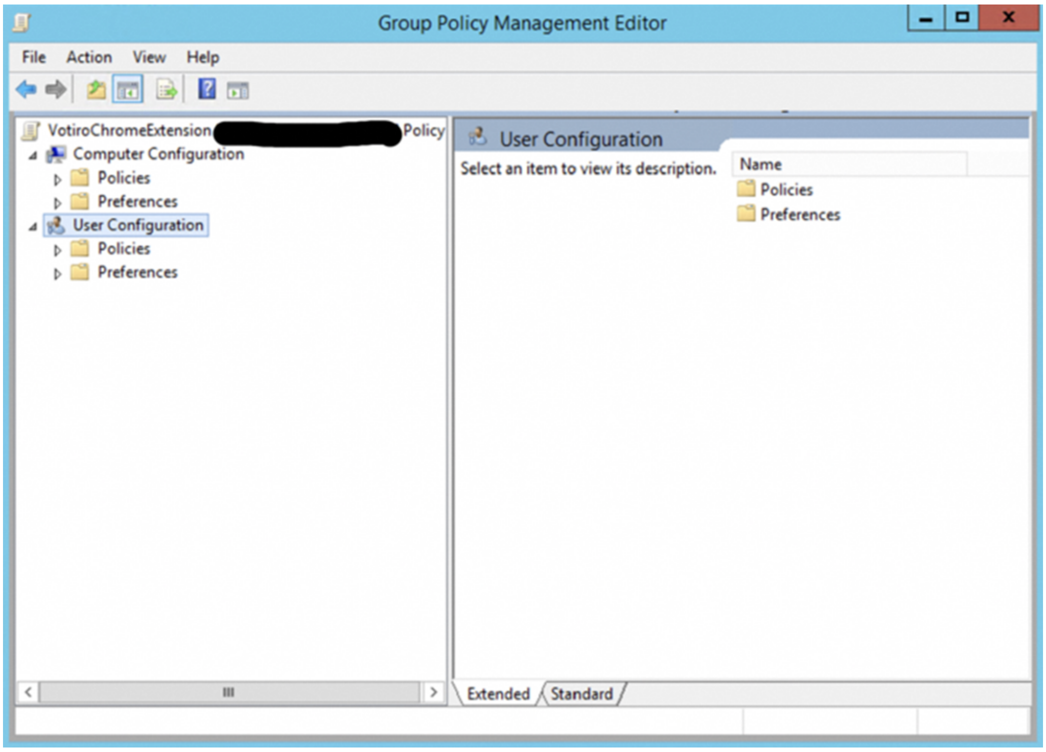
a. Right-click **Group Policy Objects**, then select **New** to create a new GPO.



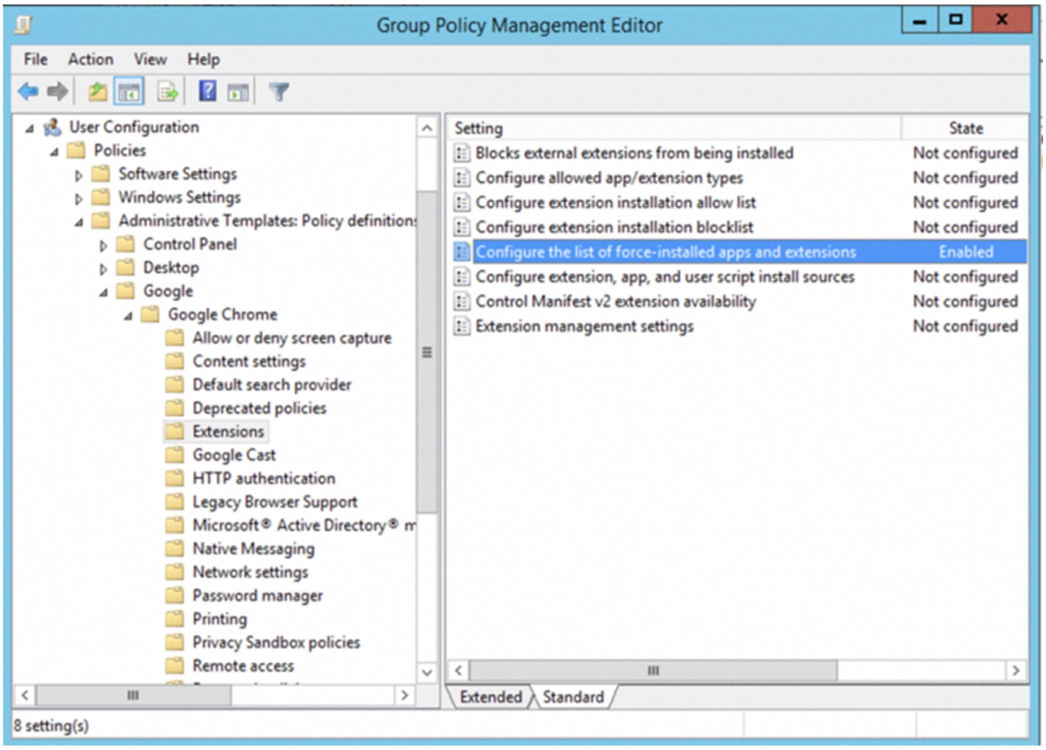
b. Enter a **Name** for the new GPO , then click **OK**.



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



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

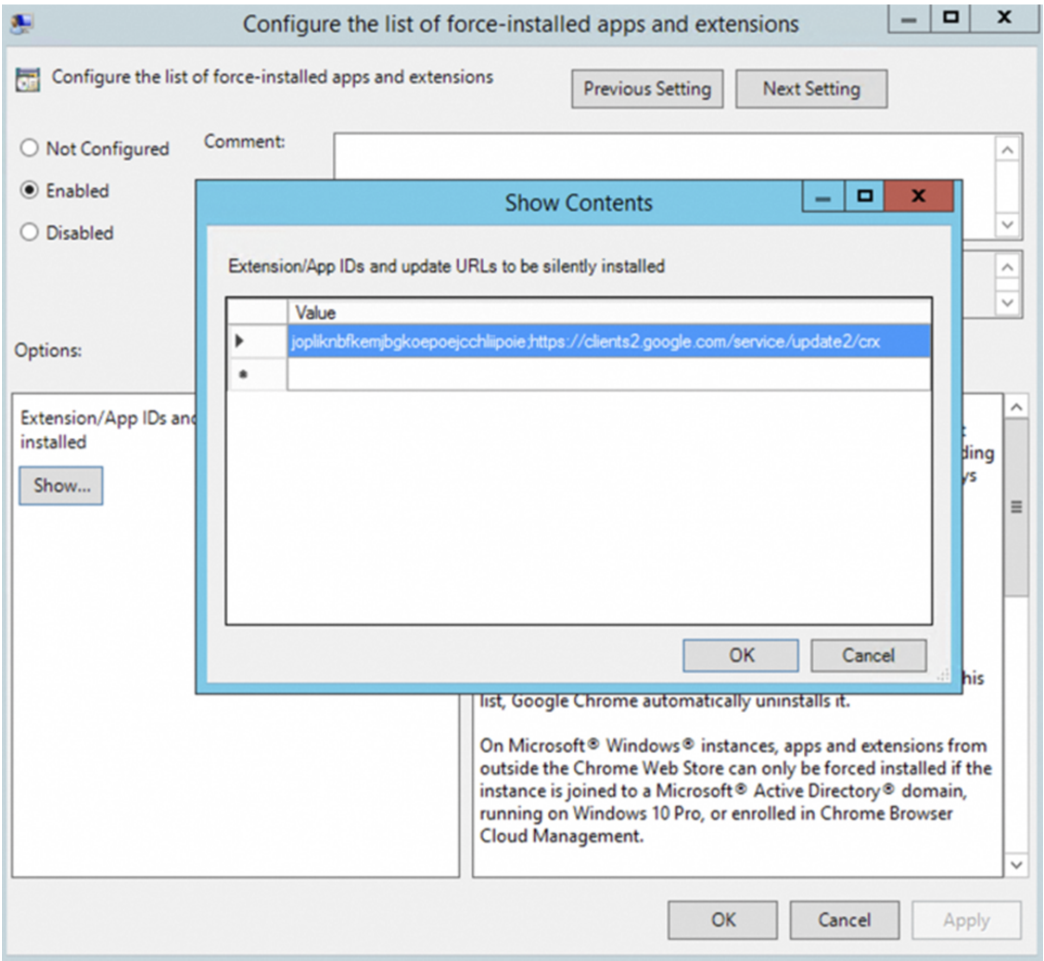


e. Select the **Enabled** radio button.

f. Click the **Show** button.

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

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



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

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

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

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

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

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

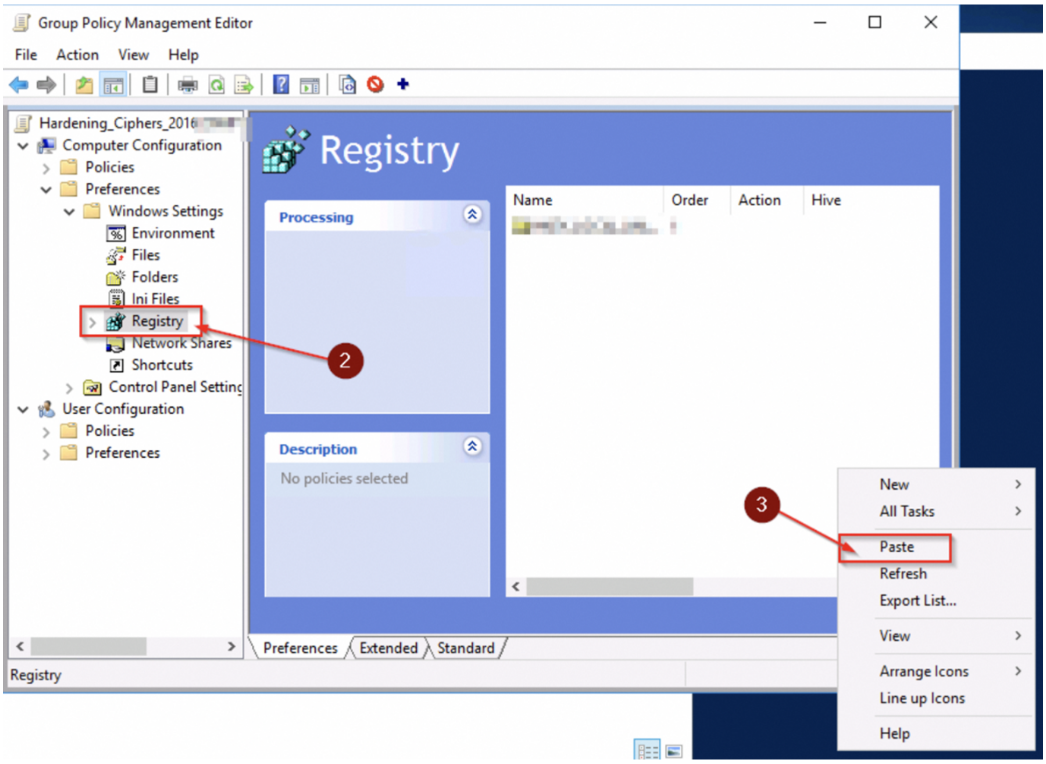
- **votiroPolicyName** – The policy that should be used in the server.
- **token** – The service token for the relevant client (should be taken from the UI)

c. Save the file and close it.

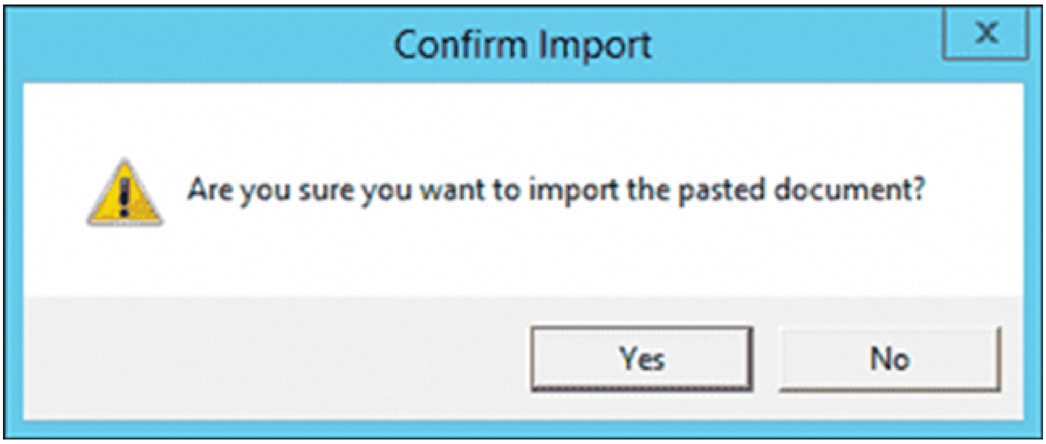
d. Right-click the xml file in File Explorer and copy it to the Windows clipboard.

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

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



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

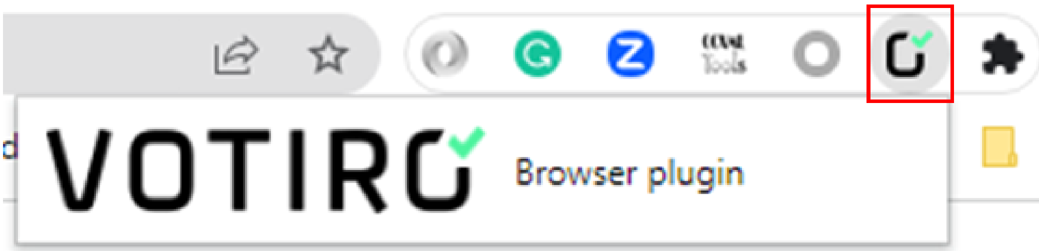


h. The GPO is created. Now you need to link it according to the organization's policy. Locate the OU or Domain you want to apply the GPO to, then right-click it and select **Link an Existing GPO...**. Then select your GPO from the list, and click **OK**.

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

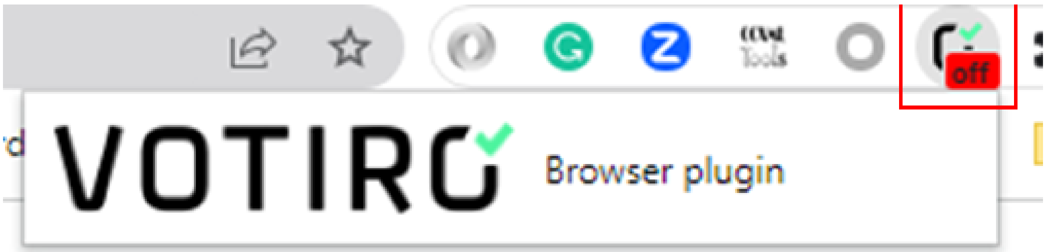
4. **Verify the Browser Extension Deployment**

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



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

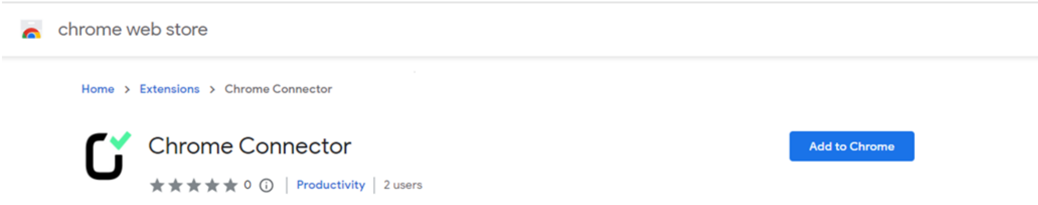
b. If there was a problem, the Votiro Chrome connector icon will be displayed as **off**:



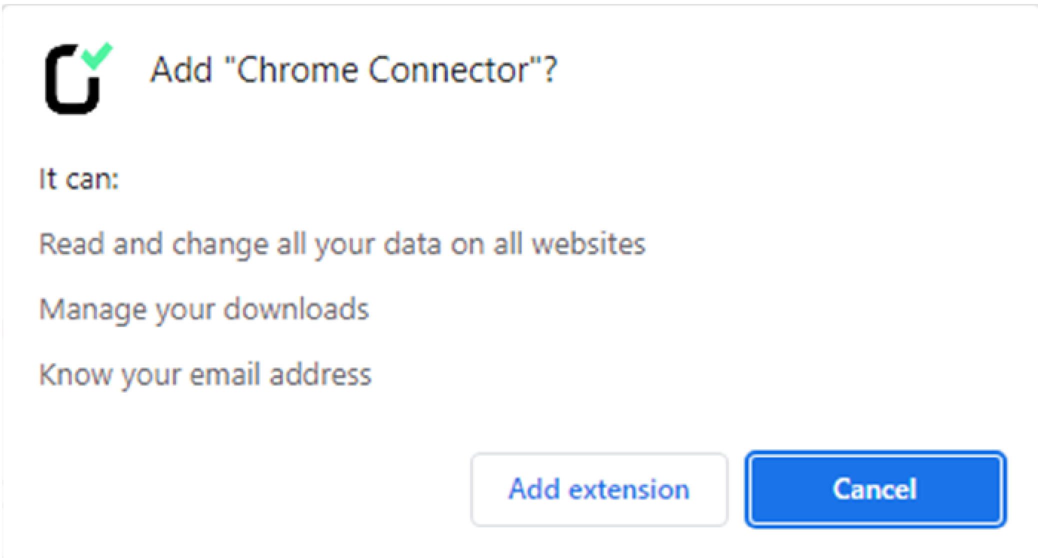
Manual Deployment

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

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



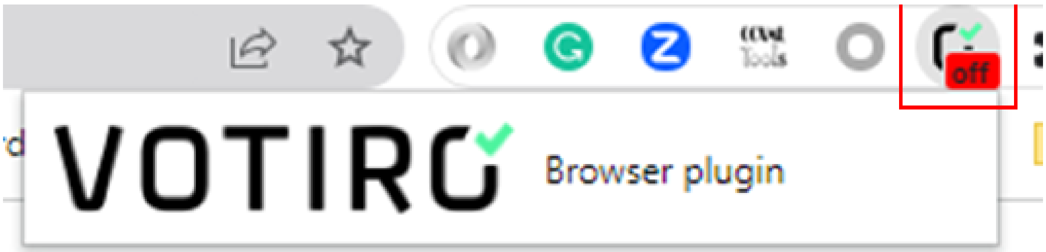
   b. Click on **Add to Chrome**. A confirmation window opens:



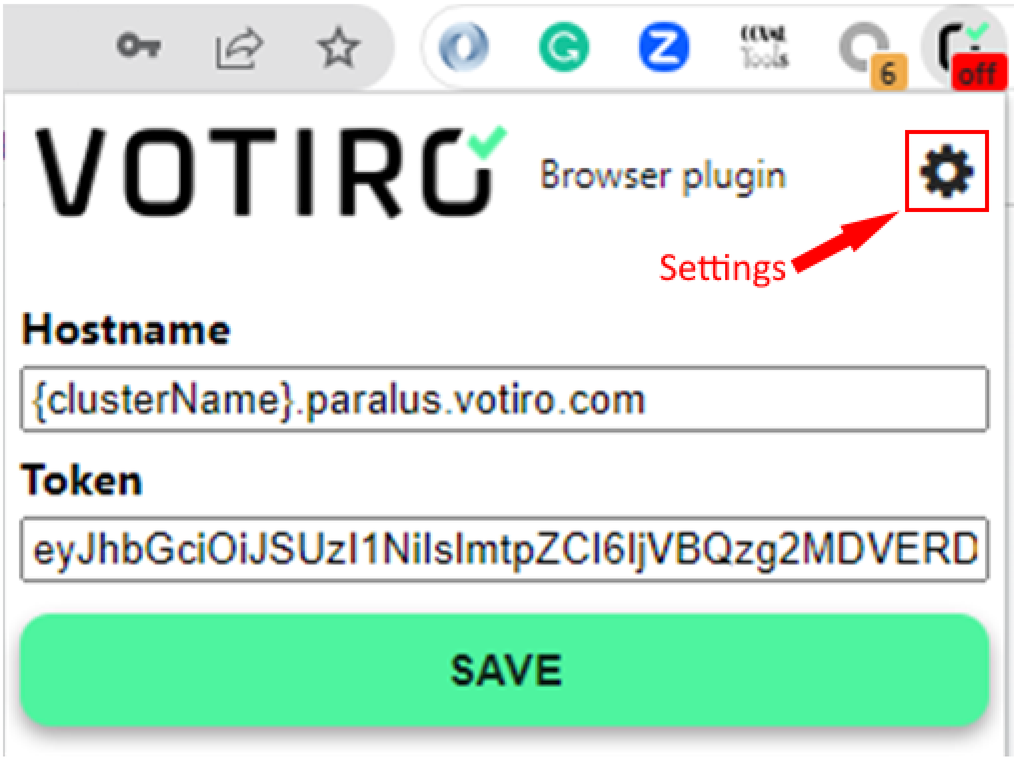
   c. Click on **Add extension**.

2. **Configure the Browser Extension**

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



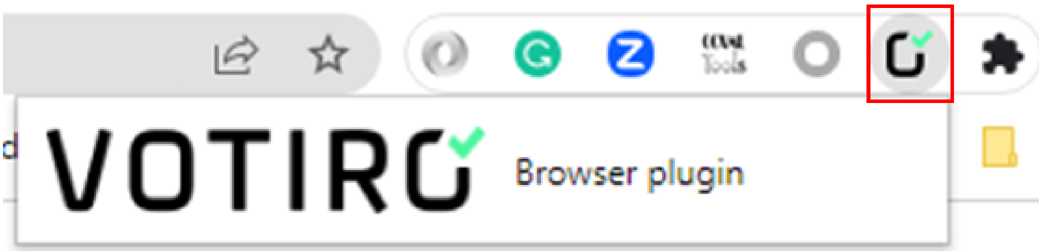
b. Click on the “Settings” icon:



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

d. Click on **SAVE**.

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

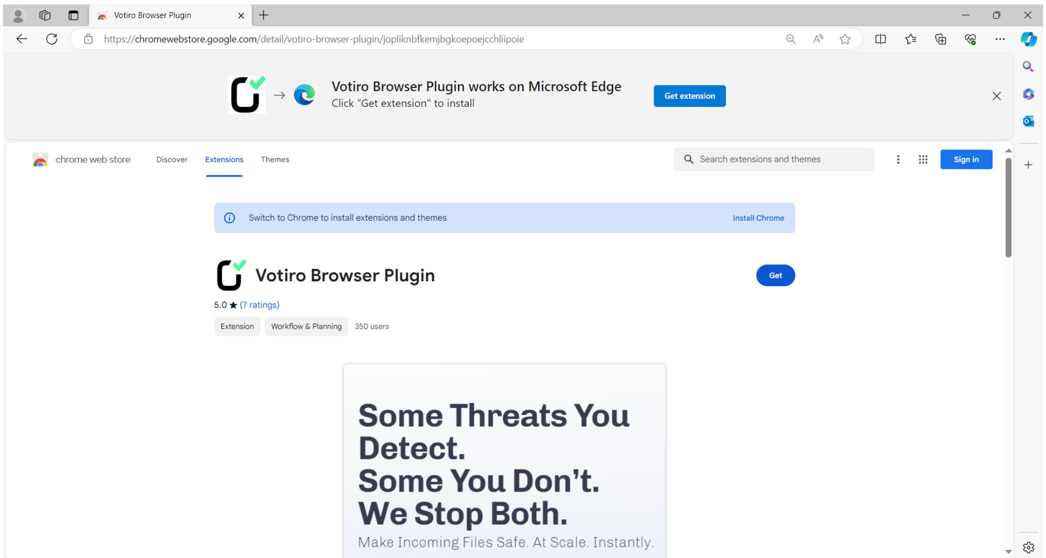


If the Votiro Chrome connector icon appears as above, each downloaded file will be sanitized by Votiro.

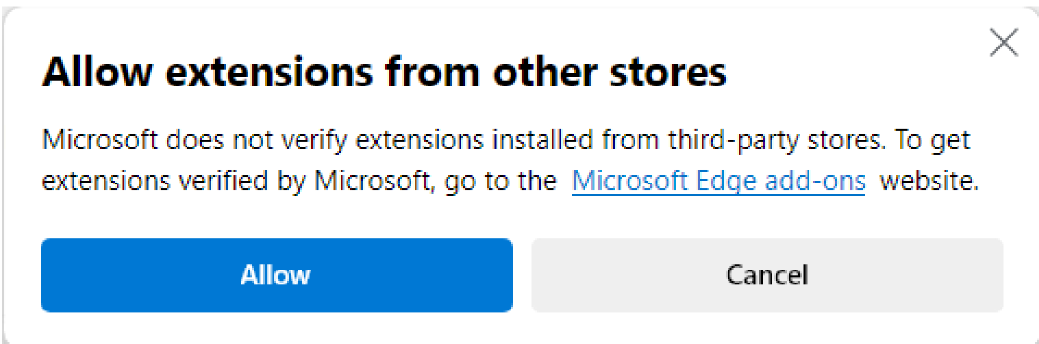
Download and Install in Microsoft Edge Browser

To deploy the Browser plugin in the Microsoft Edge browser:

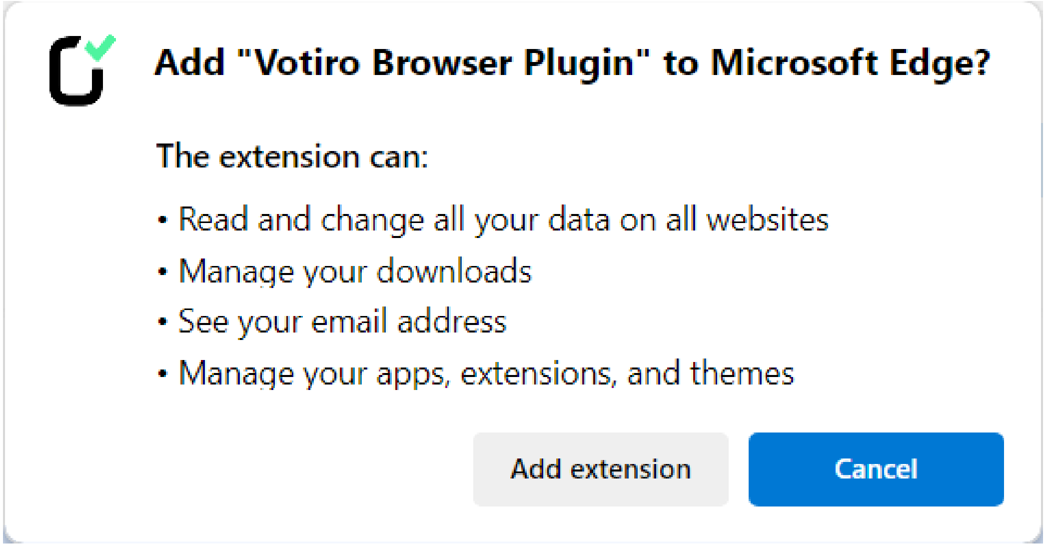
1. Paste the Chrome store extension URL to the Microsoft Edge browser: [Votiro Browser Plugin]



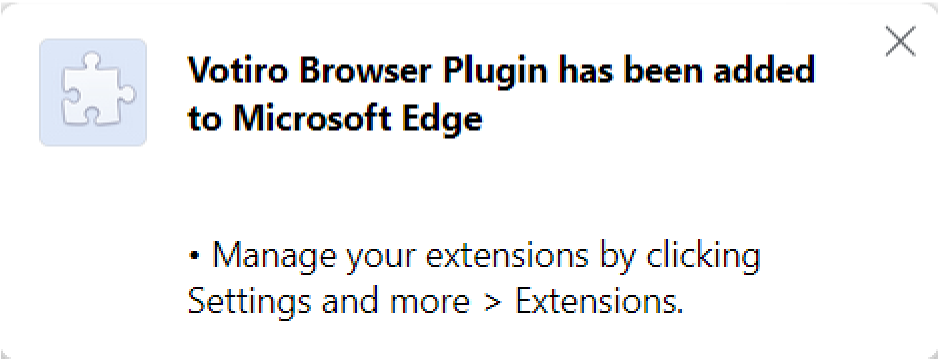
2. Click the **Get extension** or **Get** button to install.



3. Click the **Allow** button.



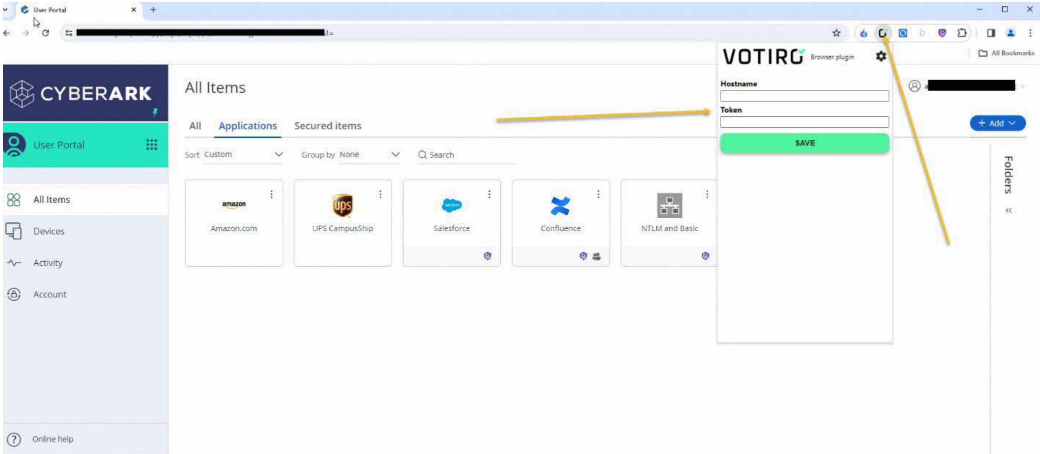
4. Click the **Add extension** button. The Votiro Browser Plugin is installed.



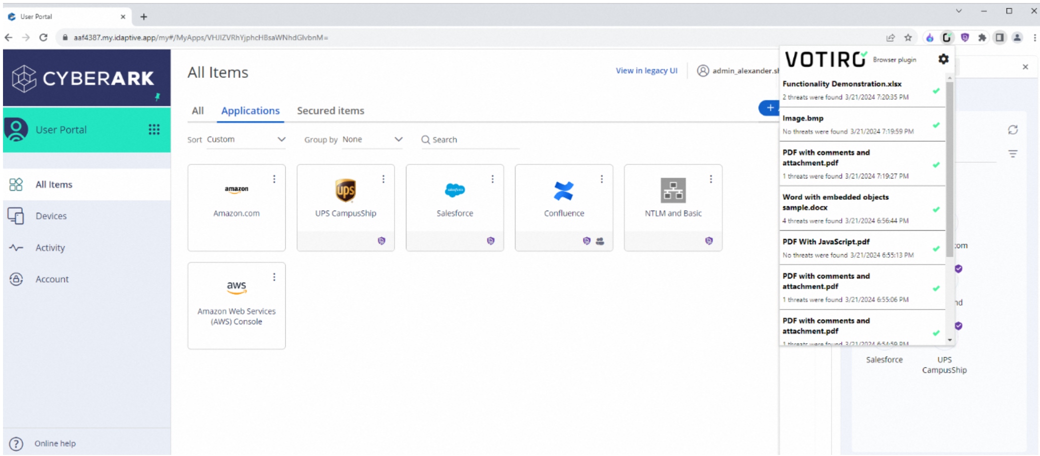
Download and Install in Cyberark Secure Browser

To deploy the Browser plugin in the Cyberark Secure Browser:

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



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



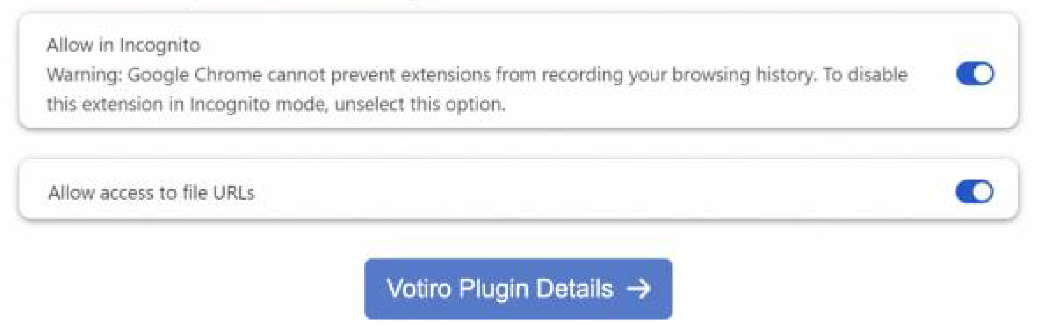
Post-Deployment Actions

Enable Downloads

In the Chrome browser:

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

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



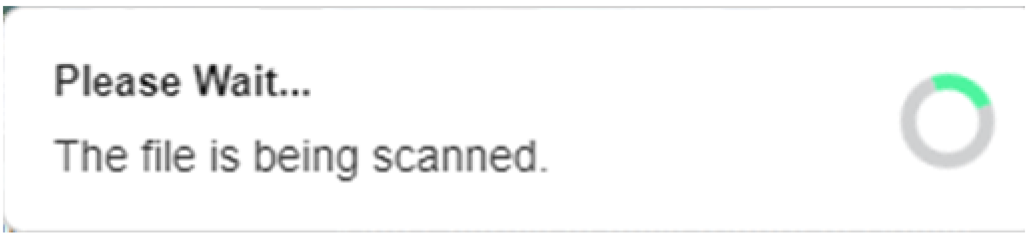
Limitations in Incognito

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

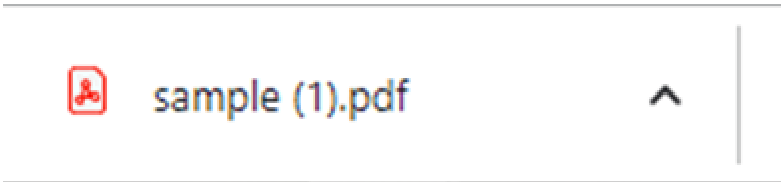
Chrome Extension User's Manual

The following features characterize the Votiro Chrome Connector extension:

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



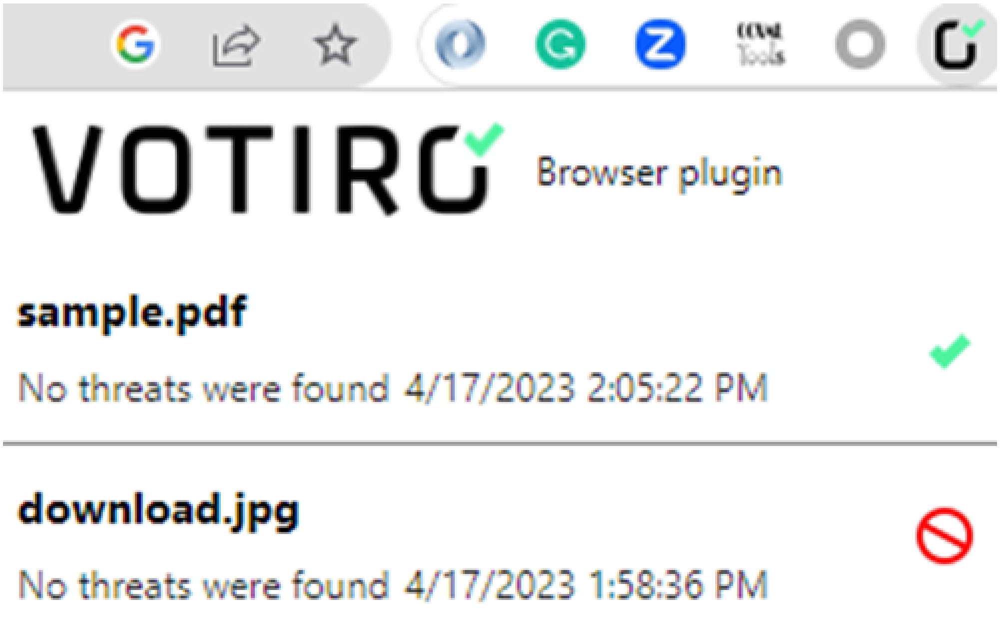
    - After download is complete, there will be an indication that the file was downloaded:



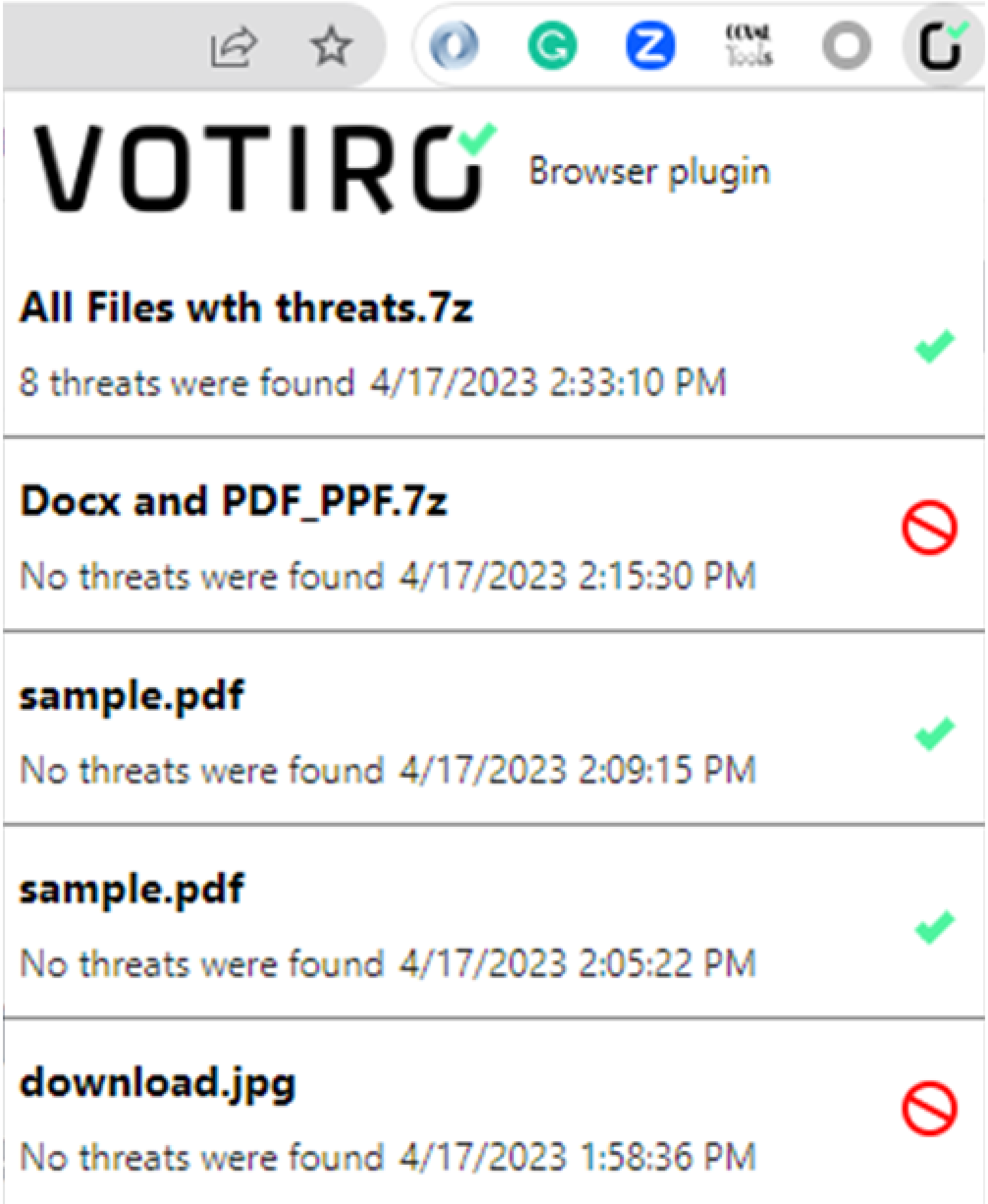
- To view downloaded files, click on the Votiro extension icon. Downloaded files will be displayed. The following information will be displayed:
  - File name
  - Threats indication
  - Time frame
  - Sanitization result icon - Sanitized/Blocked

The following examples illustrate:

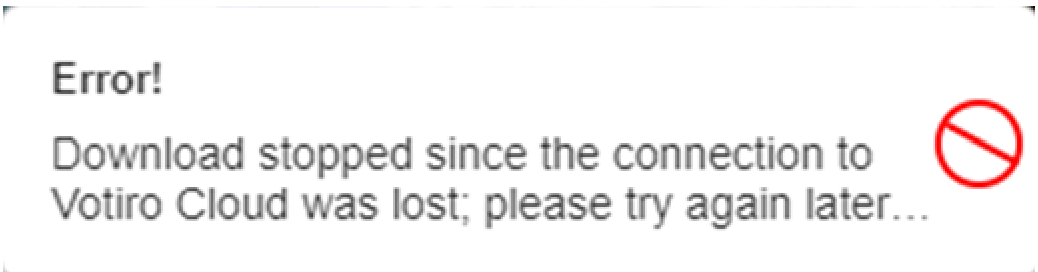
- Example 1: No threats found



- Example 2: Threats found



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

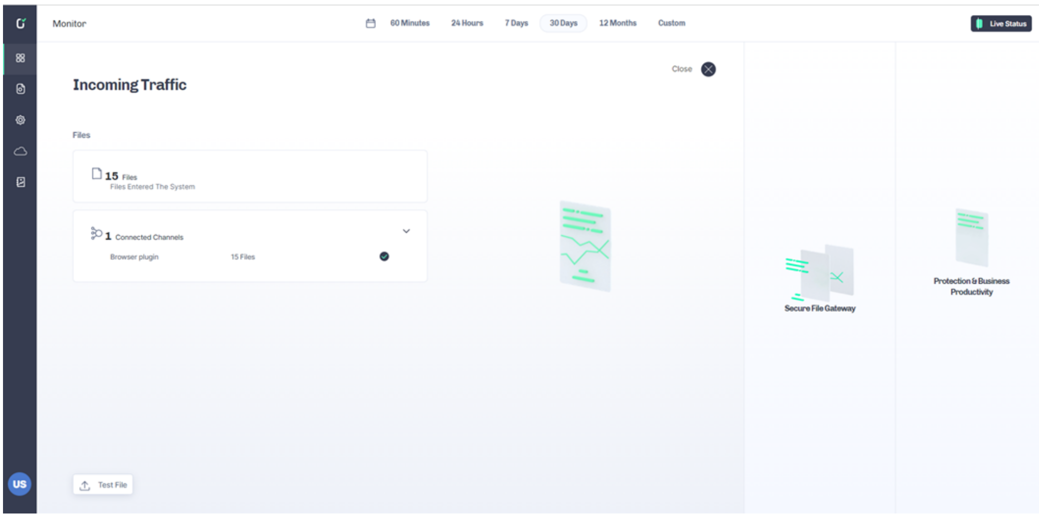


- In this case, please try again. If the problem still occurs, contact Votiro support.

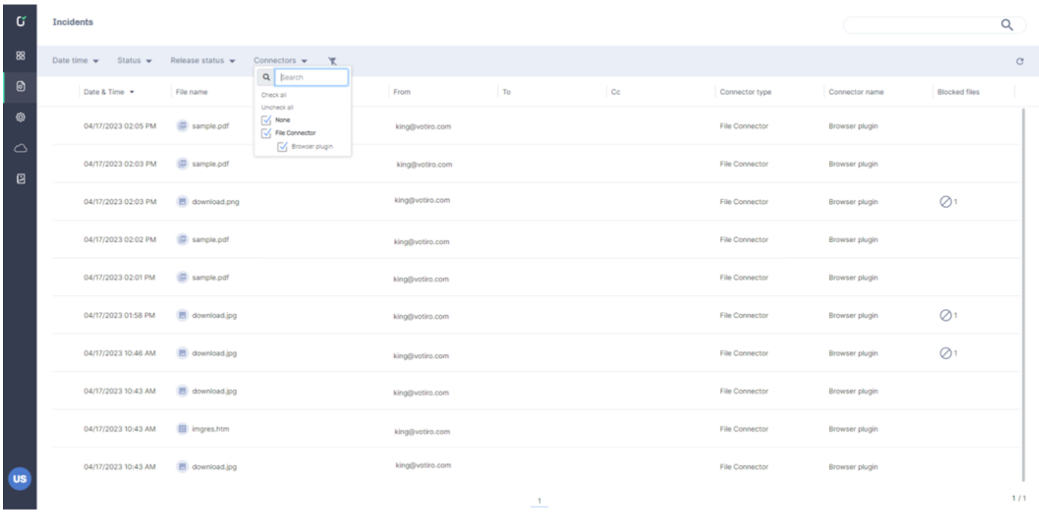
- **Votiro Management**

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

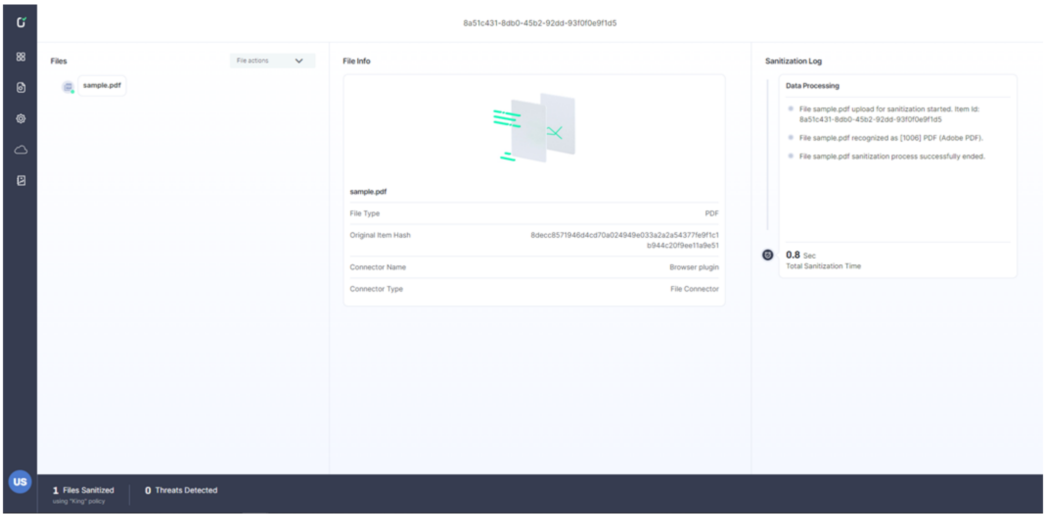
- Dashboard Monitor screen



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



- Files screen

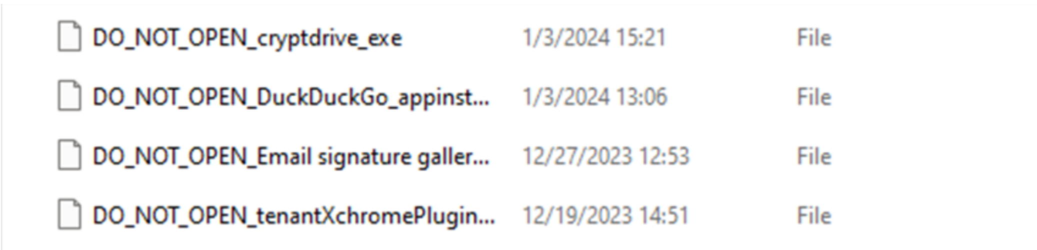


Q&A

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

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

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



A: In the Chrome browser,

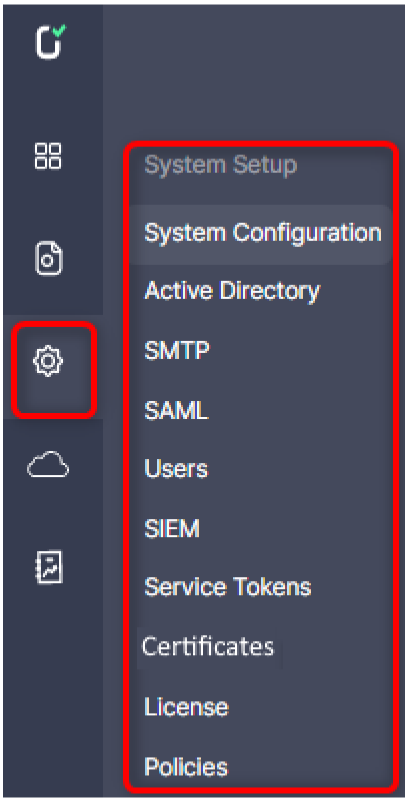
a. Navigate to **Extensions** > **Manage Extensions**, or enter **chrome://extensions** in the address box.

b. Select the Votiro extension.

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

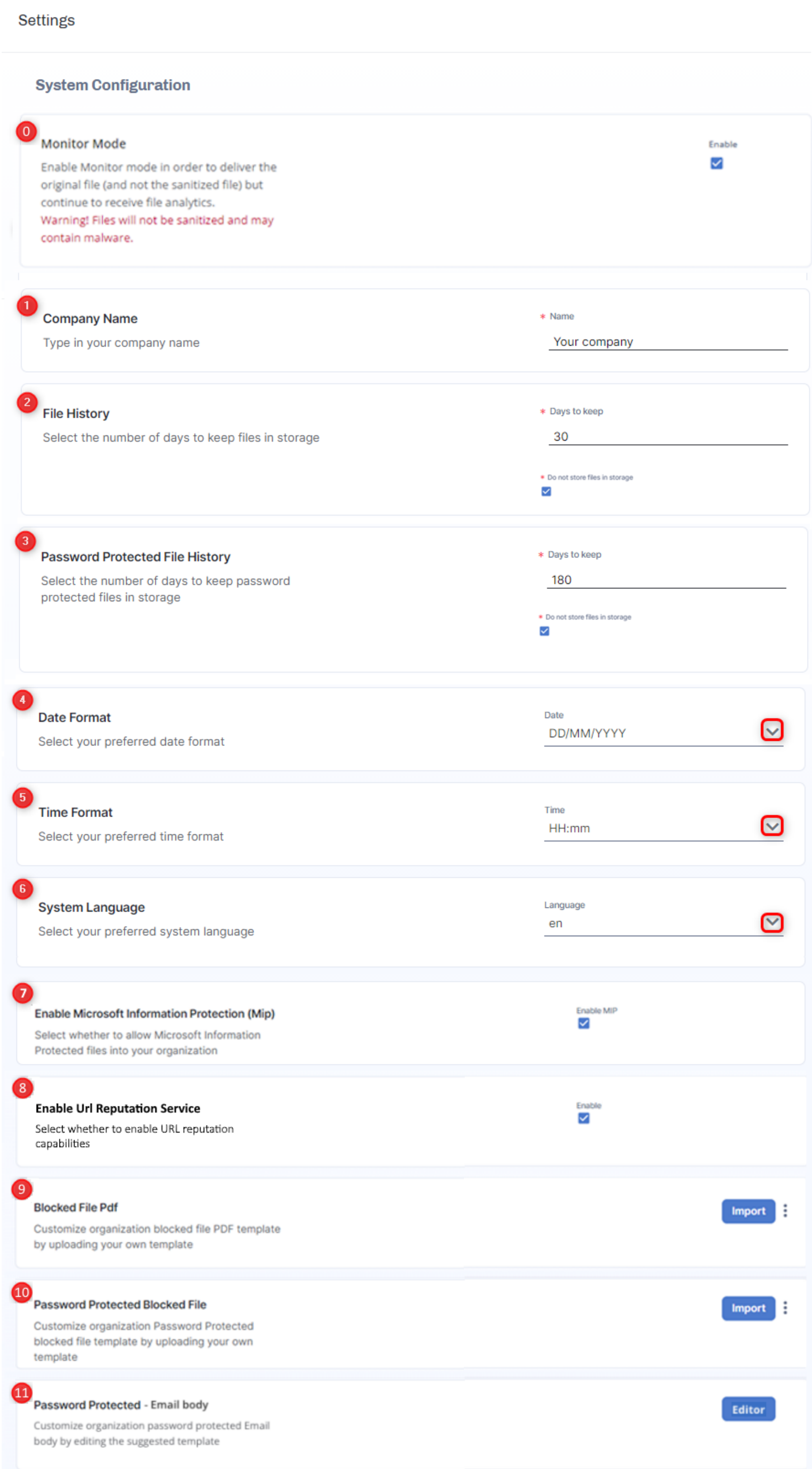
2.12 Configuring Settings

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



2.12.1 System Configuration

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


Settings
System Configuration
0
Monitor Mode
Enable Monitor mode in order to deliver the original file (and not the sanitized file) but continue to receive file analytics.
Warning! Files will not be sanitized and may contain malware.
Enable
1
Company Name
Type in your company name
* Name
Your company
2
File History
Select the number of days to keep files in storage
* Days to keep
30
* Do not store files in storage
3
Password Protected File History
Select the number of days to keep password protected files in storage
* Days to keep
180
* Do not store files in storage
4
Date Format
Select your preferred date format
Date
DD/MM/YYYY
5
Time Format
Select your preferred time format
Time
HH:mm
6
System Language
Select your preferred system language
Language
en
7
Enable Microsoft Information Protection (Mip)
Select whether to allow Microsoft Information Protected files into your organization
Enable MIP
8
Enable Url Reputation Service
Select whether to enable URL reputation capabilities
Enable
9
Blocked File Pdf
Customize organization blocked file PDF template by uploading your own template
Import
10
Password Protected Blocked File
Customize organization Password Protected blocked file template by uploading your own template
Import
11
Password Protected - Email body
Customize organization password protected Email body by editing the suggested template
Editor

The System Configuration 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. When Monitor Mode is enabled, a red frame appears when running the product to reduce confusion with connectors indication. By default, Monitor Mode is disabled for editing. To enable this feature, please contact Votiro support. **Note**: If Monitor Mode is enabled, it must be re-enabled after upgrading the VA On-prem version.
1	Company Name	Specify the name of your organization. The company name appears in activity reports. see Generating Reports on page 1.
2	File History	Specify for how many days the system saves files. The default is **30** days. If the box **Do not store files in storage** is checked, the files are stored for one hour. During that one hour time period, the original and sanitized files are available to download. At the end of the one hour time period, local storage will be deleted, and the uploaded files will not be saved in our storage. Existing original/sanitized files will be deleted as well up to 24 hours. However, files above 50MB in size will be deleted one hour after the upload. If the box **Do not store files in storage** is checked, the user will not be able to release the original file or get the original/sanitized files. The user will get an error (because we are not saving the original/sanitized files due to the Main **File History** configuration: **Do not store files in storage**). **Note**: Password-protected files will be reachable only from the password-protected portal.

Element	Field	Description
3	Password Protected File History	Specify for how many days the system saves password-protected files. The default is **180** days. **Note** After the configured period, the original file is deleted and cannot be retrieved through the dashboard. If the box **Do not store files in storage** is checked, local storage will be deleted, and the uploaded files will not be saved in our storage. Existing original/sanitized files will be deleted as well up to 24 hours from upload. However, files above 50MB in size will be deleted one hour after the upload. **Note**: When trying to download the original/sanitized file from the Management console, the user will get an error (because we are not saving the original/sanitized files due to the Main **File History** configuration: **Do not store files in storage**).
4	Date Format	Select your preferred date format for the display of information in the dashboard --either MM/DD/YYYY or DD/MM/YYYY.
5	Time Format	Select your preferred time format for the display of information in the dashboard -- either a 12-hour clock or 24-hour clock, using the format **HH:MM** or **HH:MM (AM/PM)**.
6	System Language	Select your preferred system language. To add languages to the list you must translate Dashboard dictionary and upload the translation. The default language is **EN**, English.
7	Enable Microsoft Information Protection (Mip)	Select whether to allow Microsoft Information Protected files into your organization. MIP protects data and prevents data loss across Microsoft 365 apps, services, on-premises locations, devices, and third-party apps and services. The site http://login.microsoftonline.com/ is allowed.
8	Enable Url Reputation Service	Select whether to enable URL reputation capabilities. After enabling, navigate to Votiro Policies for adjusting URL Reputation for supported file types (Email, PDF, DOC, DOCX, XLSX).
9	Blocked File PDF	Customize your organization's blocked file PDF template by uploading (importing) your own template.
10	Password Protected Blocked File	Customize your organization's Password Protected blocked file template by uploading (importing) your own template.

Element	Field	Description
11	Password Protected - Email body	Customize your organization's Password Protected Email body by editing the suggested template

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

Monitor Mode

After enabling Monitor Mode:

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

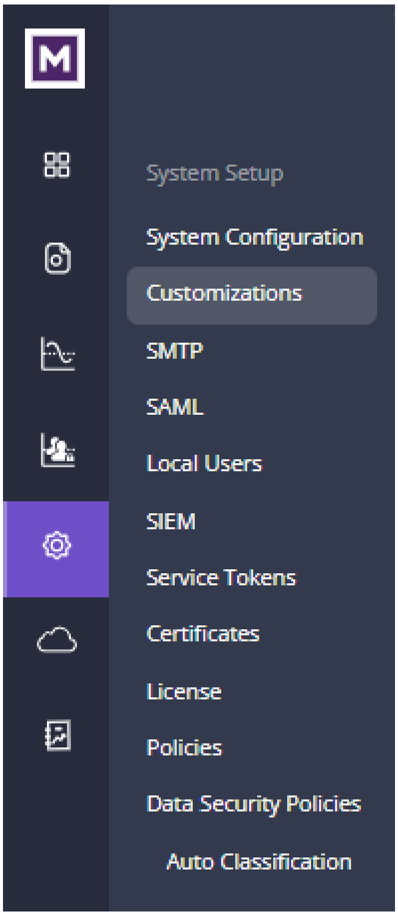
Note the current limitation:

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

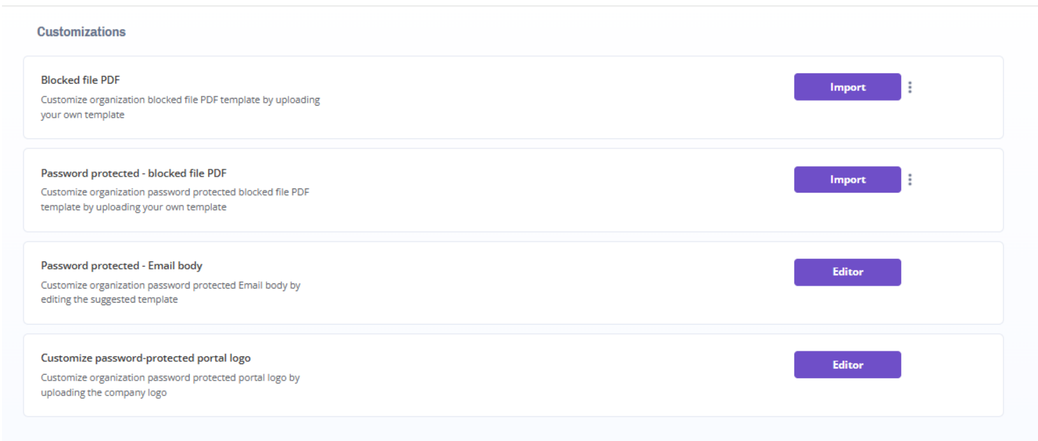
2.12.2 Customizations

The Customizations page enables the user to customize the blocked file PDF template, password protected blocked file PDF template, password protected email body and password protected portal logo.

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



The **Customizations** page is displayed:



The customizations available are:

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

- **Password protected - Email body** - customize the organization's password protected Email body by editing the suggested template
- **Customize password-protected portal logo** - customize the organization's password protected portal logo by uploading the company logo

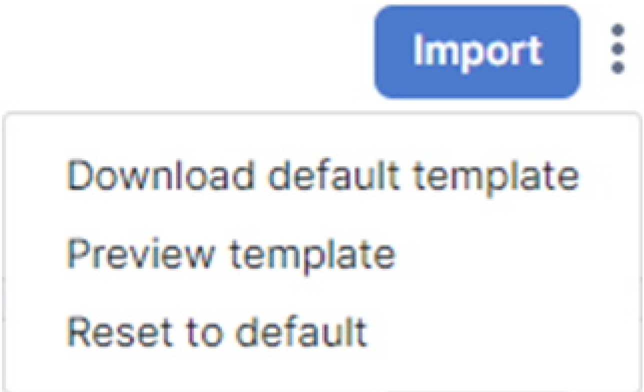
Customizing Blocked File Templates

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

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

Using the Default Template

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



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

Customizing the Default Template

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

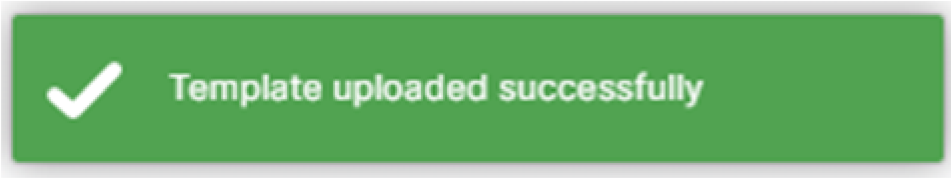
Importing a Customized Template

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

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

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

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

    Each blocked file will be replaced with the updated template.

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

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

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

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

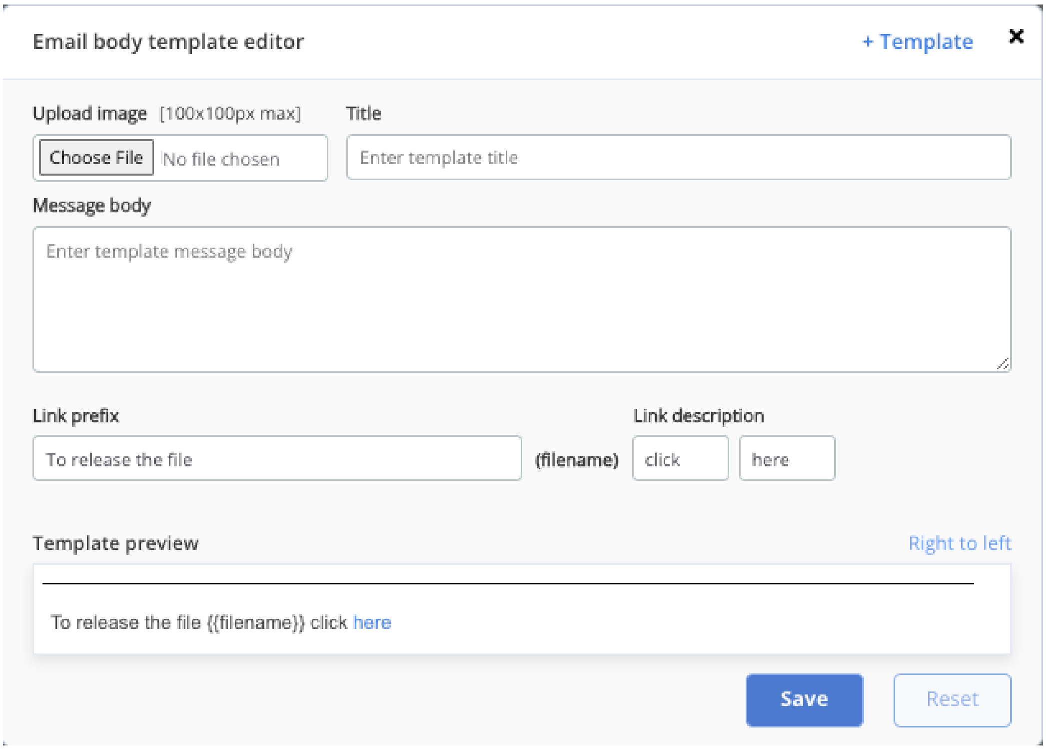
To abandon the changes click **Reset**, your system configuration settings will remain unchanged.

Customizing Email Body Templates

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

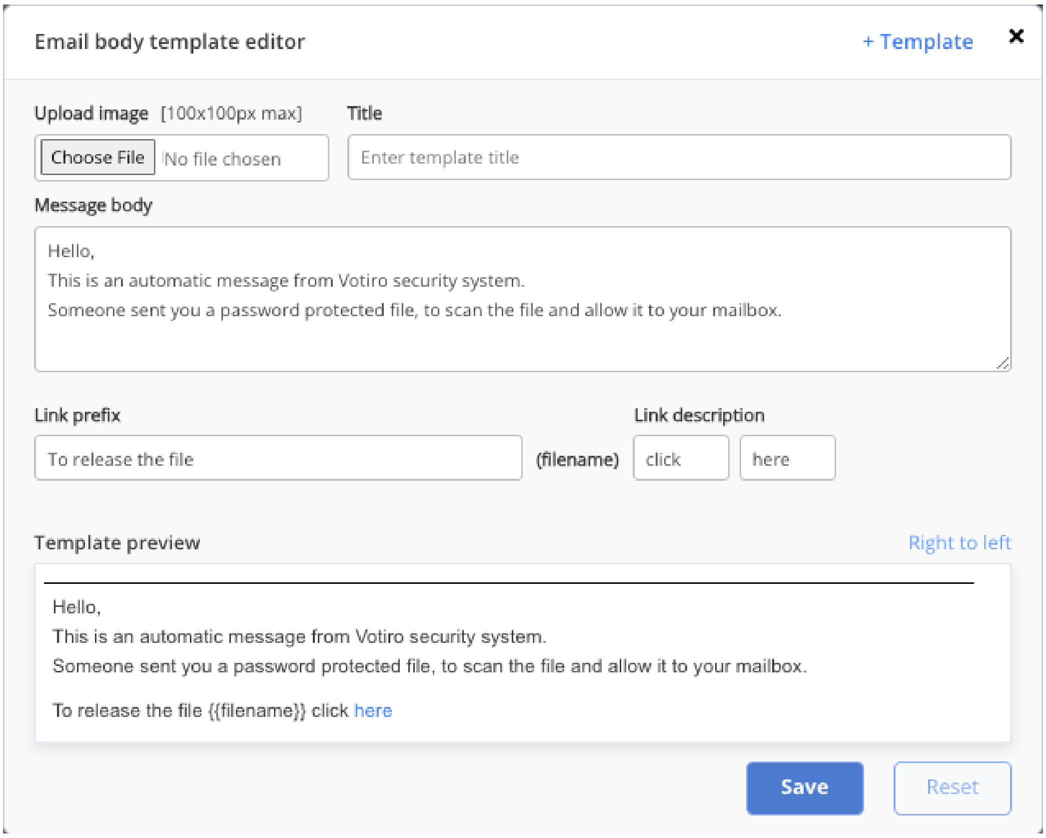
To customize the Email body template:

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

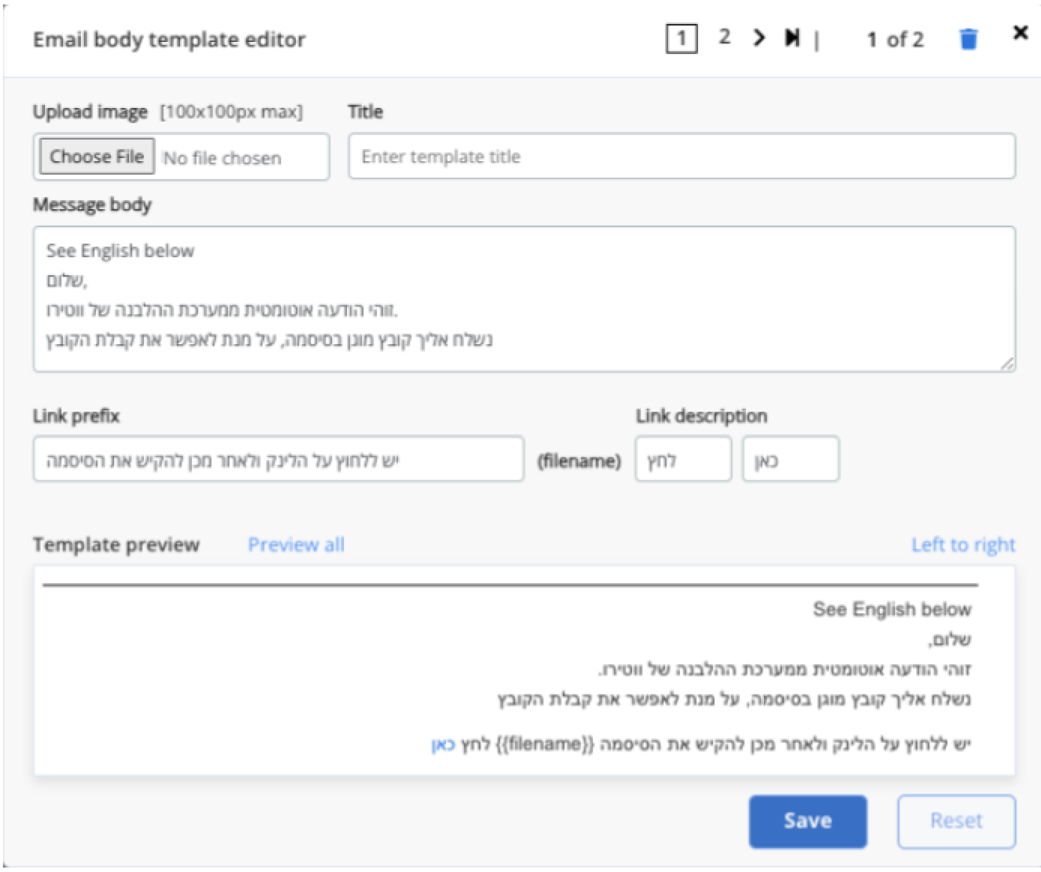


2. You can customize the template by:

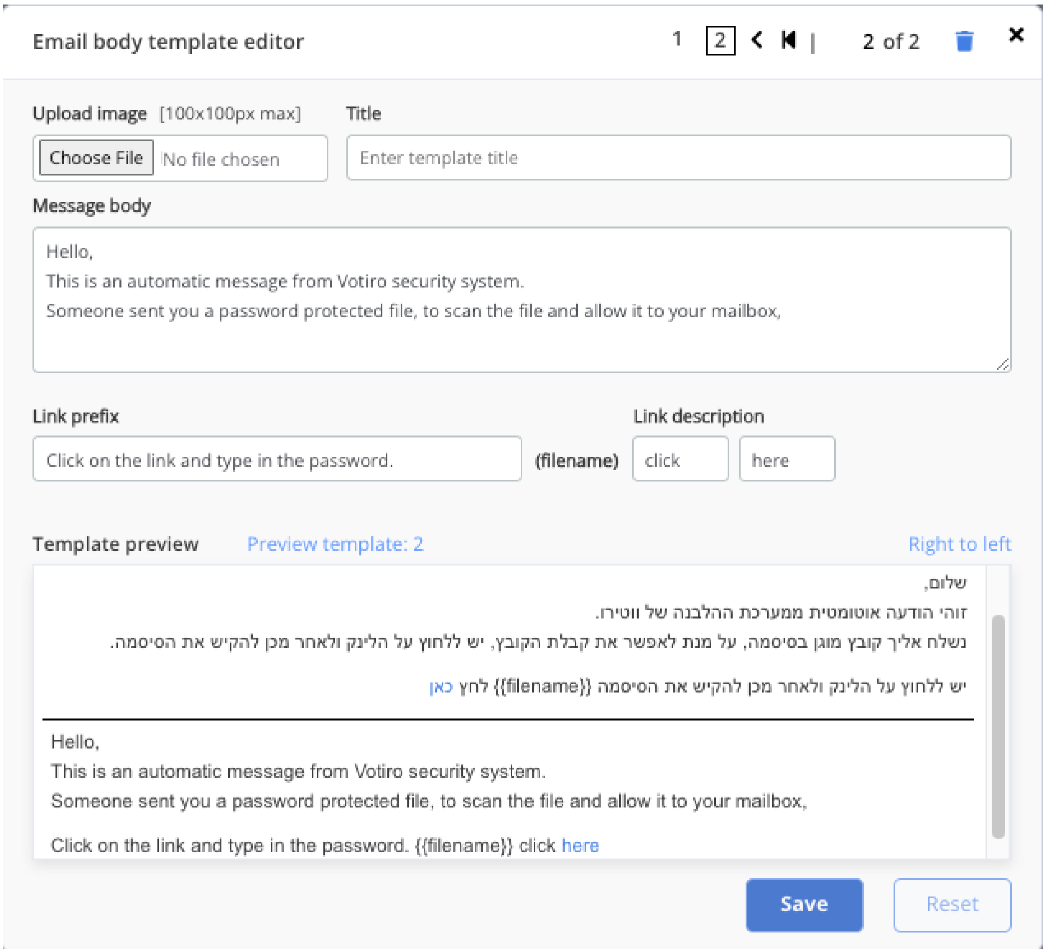
- Logo (**Upload image**) - press **Choose File** to upload an image
- **Title** - enter the template title in the text box
- **Message body** - enter the template message body in the text box
- Release file link message (**Link prefix** and **Link description**) - enter the **Link prefix** text in the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



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



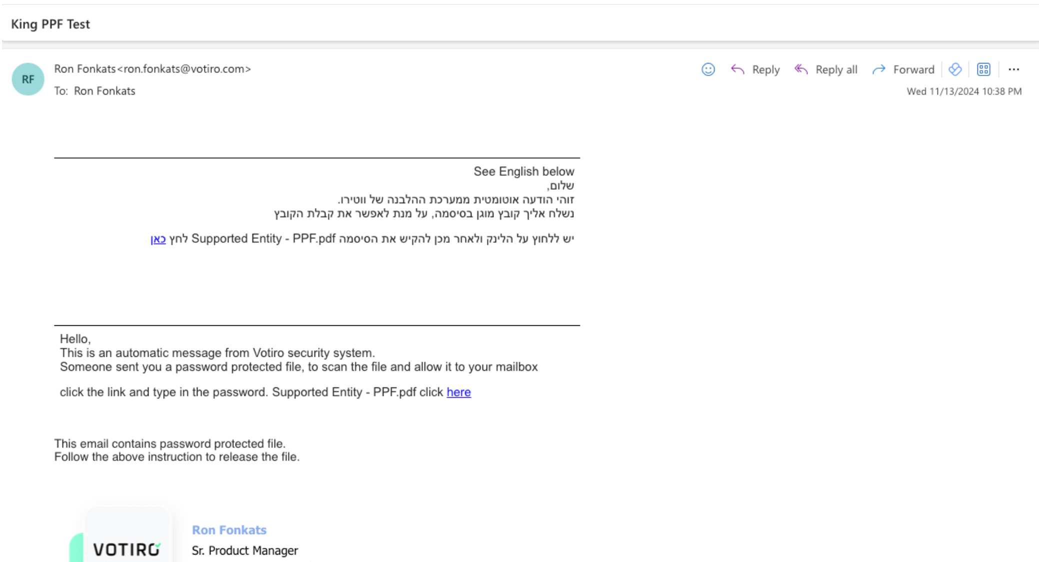
4. After entering the desired information, there are options to:
   - **Template Preview** / **Preview all** - preview templates
   - **Right to left** / **Left to right** - Set message location
   - **Reset** - reset the template to the default



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

End user view

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



Demo

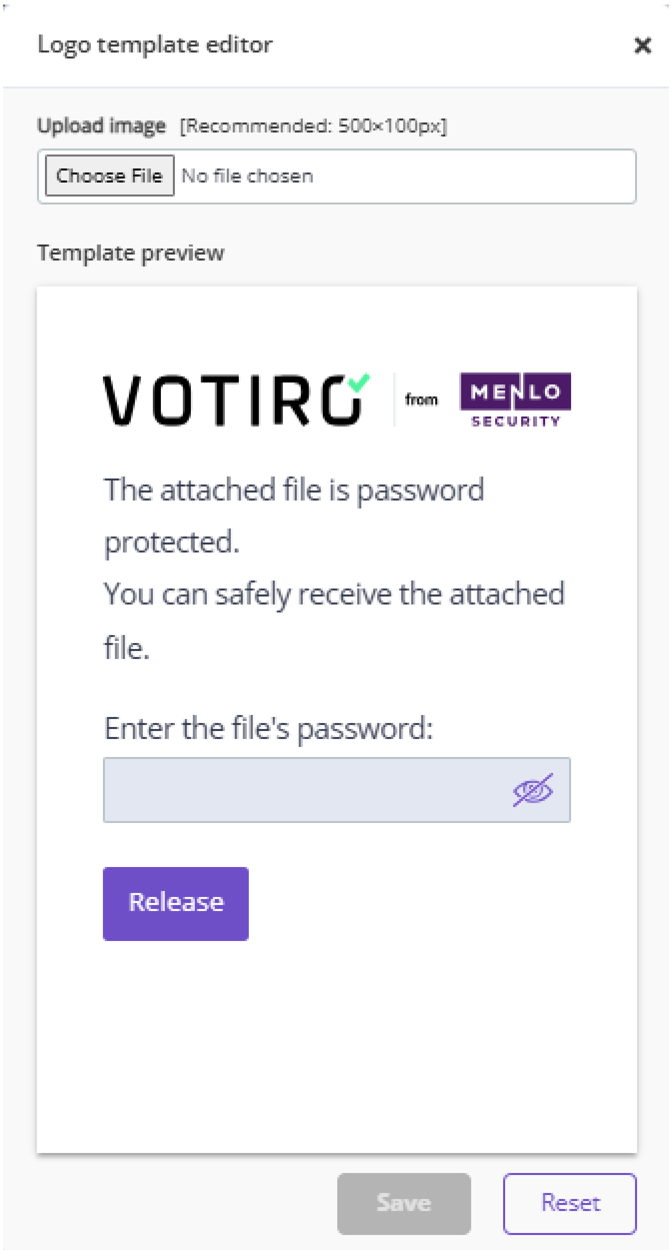
A video demonstrating customization of the Email body template is available at:

[Customize template - PPF Email message]

Customizing the Password-protected Portal Logo

To customize the Password-protected portal logo:

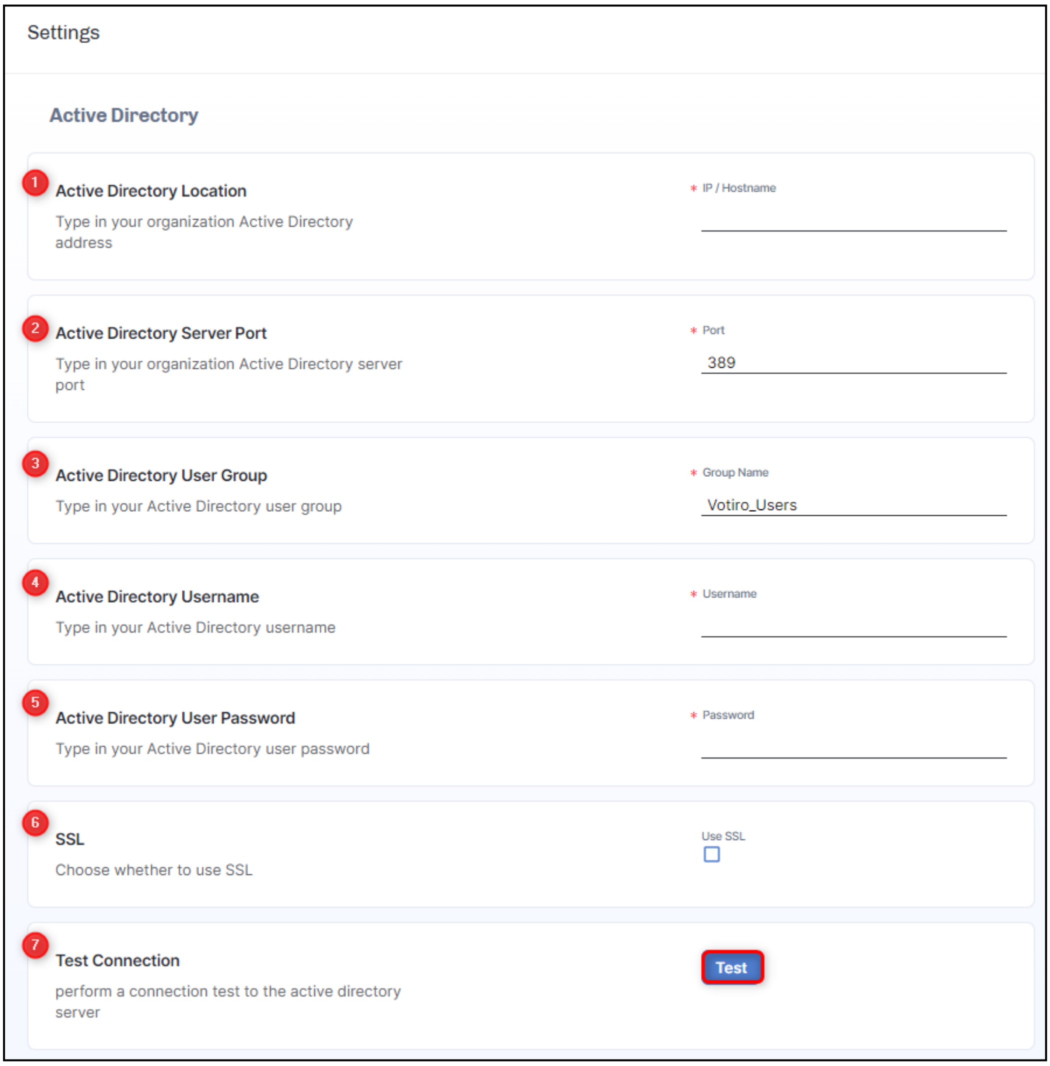
1. Click on the **Editor** button. The Logo template editor is displayed:



2. Follow the instructions detailed in [Password Protected Portal].

2.12.3 Active Directory

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



The Active directory page contains the following fields:

Element	Field	Description
1	Active Directory Location	Specify your organization's Active Directory server address that validates login.
2	Active Directory Server Port	Specify your organization's Active Directory server port. For example, 389.
3	Active Directory User Group	Specify the name of the Active Directory user group. Only users that belong to the predefined Votiro_Users group in Active Directory can login to the Management Dashborad.

Element	Field	Description
4	Active Directory Username	Specifies the login username for the Active Directory server. Select one of two formats to use: ■ DOMAIN\UserName - For example, VT\Jane.Smith ■ UserName@FQDN - For example, Jane.Smith@Votiro.com Key: *DOMAIN* - the NetBIOS domain name *UserName* - the login name of the user *FQDN* - the domain name in full
5	Active Directory User Password	Specify the login password for the Active Directory server.
6	SSL Usage	Specify whether to use SSL.
7	Test Connection	Before saving changes you should test the connection to Active Directory. To select a file for testing, click **Test**.

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

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

2.12.4 Configuring Active Directory with LDAPS

> **Note**
> This guide is relevant only for our VA on-premises product.

Prerequisites

Before you start, make sure you have:

- The LDAPS FQDN
- The certificate file in .crt format
  - If the certificate file is in .cer format, convert it to .crt by executing the following command:

    ```
    openssl x509 -inform PEM -in /<CERT_PATH>/<CERT_NAME>.cer -out /<CERT_PATH>/<CERT_NAME>.crt
    ```

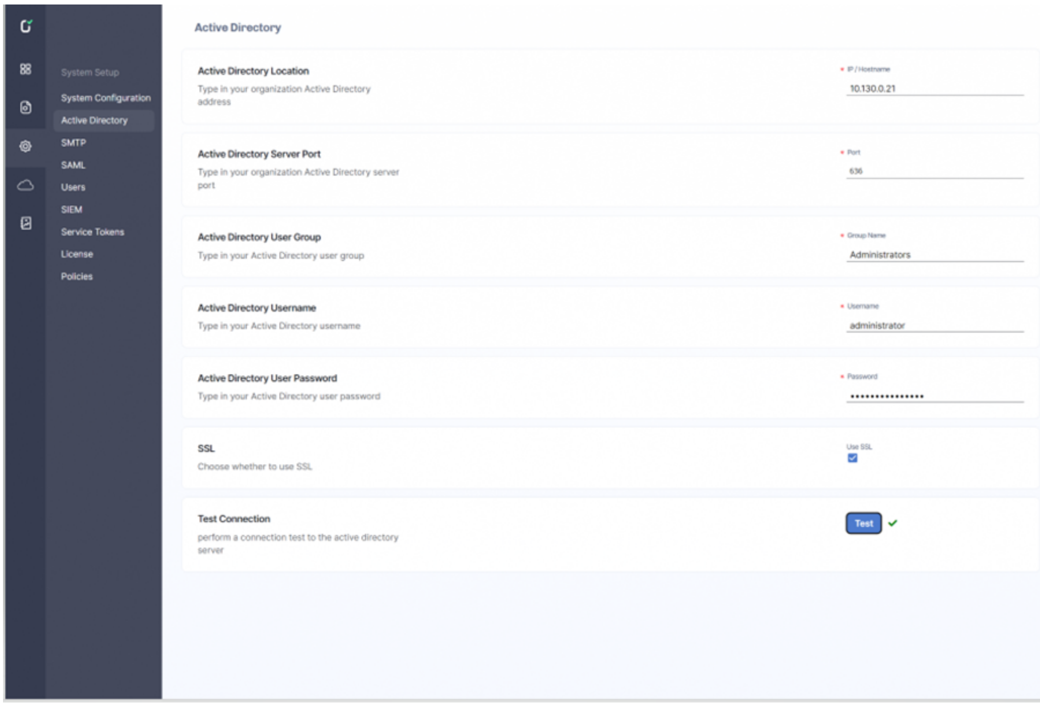
where *<CERT_PATH>* and *<CERT_NAME>* are replaced by the certificate path and certificate name.

Procedure

1. Copy the .crt file under /etc/pki/for each node.
2. Execute rollout restart for identity pods:

```
kubectl rollout restart deployment mng-service-identity-
deployment -n votiro
```

3. Login to the UI, navigate to System Setup > Active Directory and fill in the required information.
4. Make sure the username is written with the domain prefix, domain\username. See the screenshot as a reference:

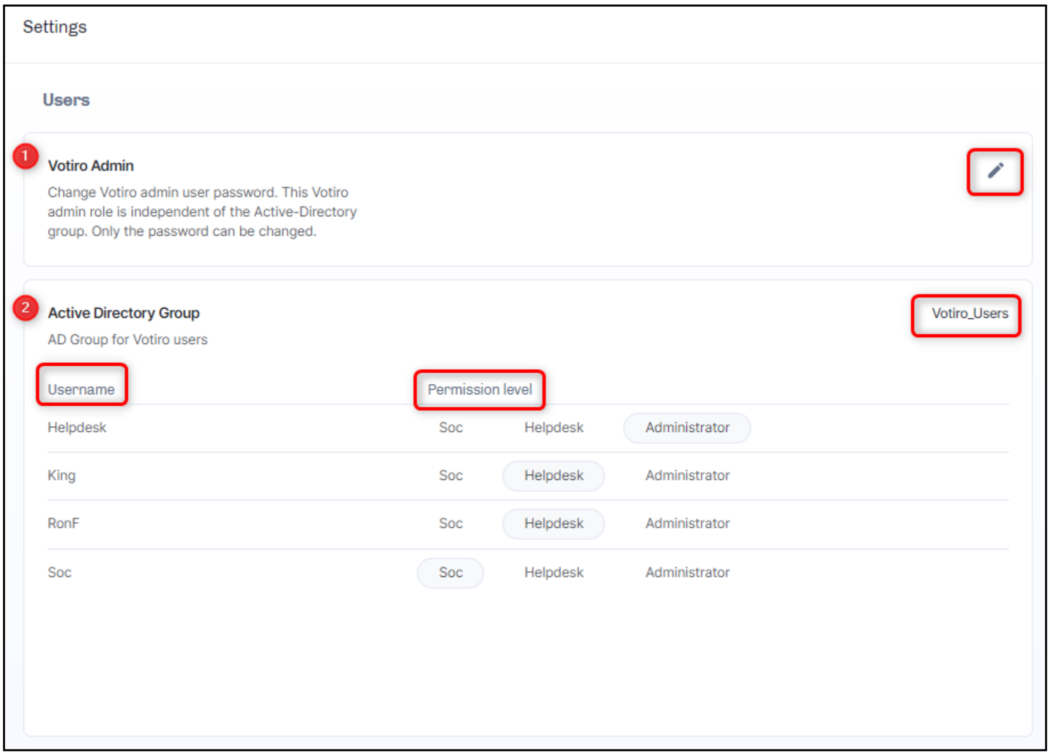


5. Verify that **Use SSL** is checked.
6. Proceed by clicking **Test**.
7. Save the changes by clicking the **Save** button.

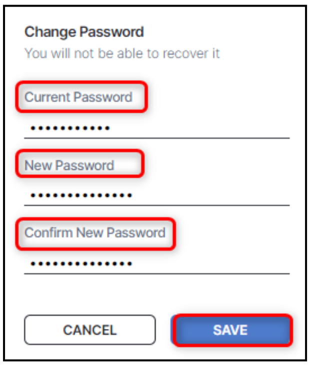
2.12.5 Active Directory Users

The Active Directory Users page enables you to change the password for the Votiro Admin role and define permissions for users of the Management Platform.

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



The Active Directory Users page contains the following fields:

Element	Field	Description
1	Votiro Admin	The Votiro Admin role provides direct administrative access to Votiro On-prem, independent of Active Directory. To change the Votiro Admin password: 1 Click . 2 Enter the **Current Password** and then **Confirm New Password**. 3 Click **Save**, or **Cancel**. 

<table>
<tr><th>Element</th><th>Field</th><th>Description</th></tr>
<tr><td>2</td><td>Active Directory Group</td><td>
Users must be in the Votiro_Users Active Directory group.
The three levels of permission are:

SOC: users will only be able to view the dashboard and use the TEST FILE functionality. They will not have access to personal data, or be able to change settings (this is the default permission for a new user).
Helpdesk: users will be able to manage the positive selection process and release of personal files and emails, in addition to SOC permissions.
Administrator: users will have access to the entire system, including personal files and emails. They have permission to edit policy configurations and system settings, in addition to Helpdesk permissions.

To set a user's Permission Level go to the options to the right of the Username, click the permission level to be granted. The level selected is highlighted.

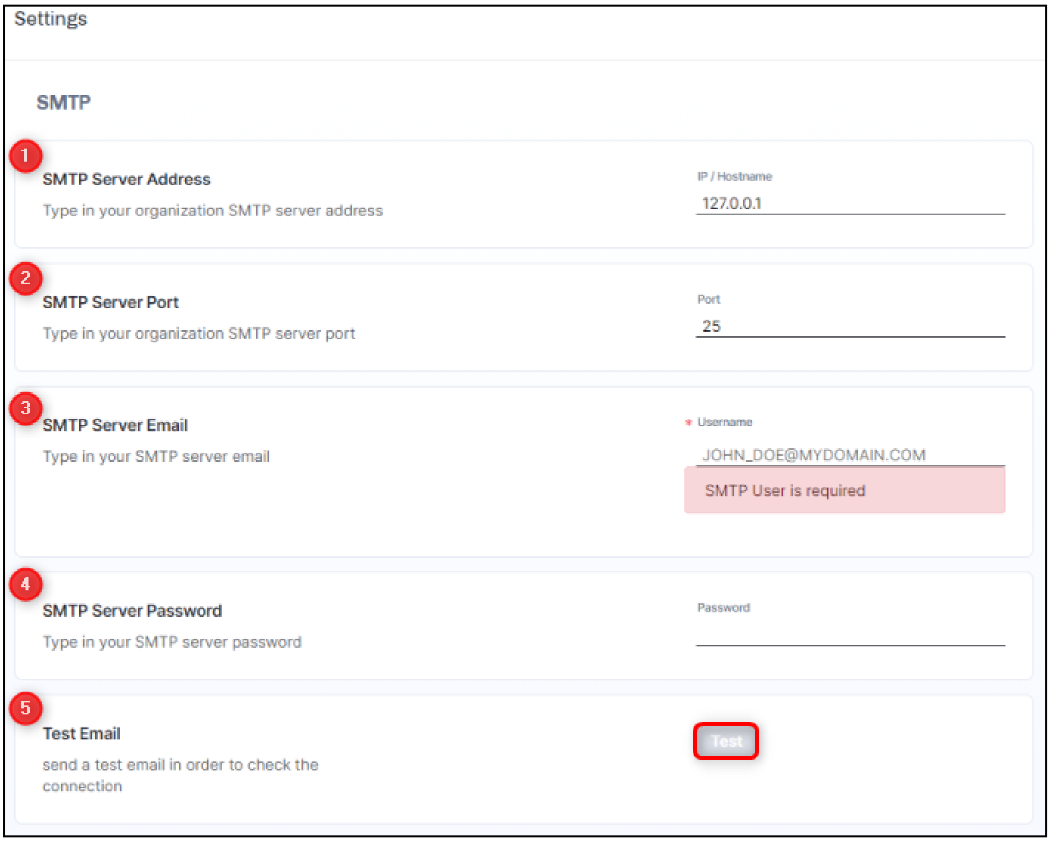

The following table details the permissions assigned to the different roles.
<table>
<tr><th>Role</th><th>View data in Dashboard and Explore Incident</th><th>Download / Release files</th><th>View/ edit connectors setting</th><th>View /edit settings</th><th>Reports</th><th>View Local Users screen</th><th>Create/ delete users
Reset password</th><th>View/ Edit Certificates</th><th>View /Edit Licenses</th></tr>
<tr><td>Soc</td><td>Yes</td><td>No</td><td>Yes/No</td><td>Yes/No</td><td>Yes</td><td>No</td><td>No</td><td>No/No</td><td>No/No</td></tr>
<tr><td>Helpdesk</td><td>Yes</td><td>Yes</td><td>Yes/No</td><td>Yes/No</td><td>Yes</td><td>Yes</td><td>No</td><td>No/No</td><td>No/No</td></tr>
<tr><td>Administrator</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes/Yes</td><td>Yes/Yes</td></tr>
</table>
WARNING!
The system must have a minimum of one Administrator user set up in the Active Directory Group for Votiro users.
</td></tr>
</table>

Element	Field	Description
		A warning message appears if you attempt to **Save** the settings with no user set with **Administrator** permissions.

2.12.6 SMTP

All SMTP settings are required to enable Management Dashboard features that rely on email. Configuring SMTP settings allows you to release original files from the blob. For more information, see Releasing Files on page 47.

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



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

Element	Field	Description
1	SMTP Server address	Specifies the SMTP server that relays notifications from the Platform Management to users in your organization.
2	SMTP Server port	Specifies the SMTP server port.

<table>
<tr><th>Element</th><th>Field</th><th>Description</th></tr>
<tr><td>3</td><td>SMTP Server email</td><td>Specifies the email address of the SMTP server user.</td></tr>
<tr><td>4</td><td>SMTP Server password</td><td>Specifies the password for the SMTP server user.</td></tr>
<tr><td>5</td><td>Test Email</td><td>To test the SMTP settings, click Test.

- If the settings are valid, a verification code is displayed in the Management Dashboard.

  The same code appears in an email message that is sent to the address you specified.

- If the settings are invalid, an error is displayed below the button.</td></tr>
</table>

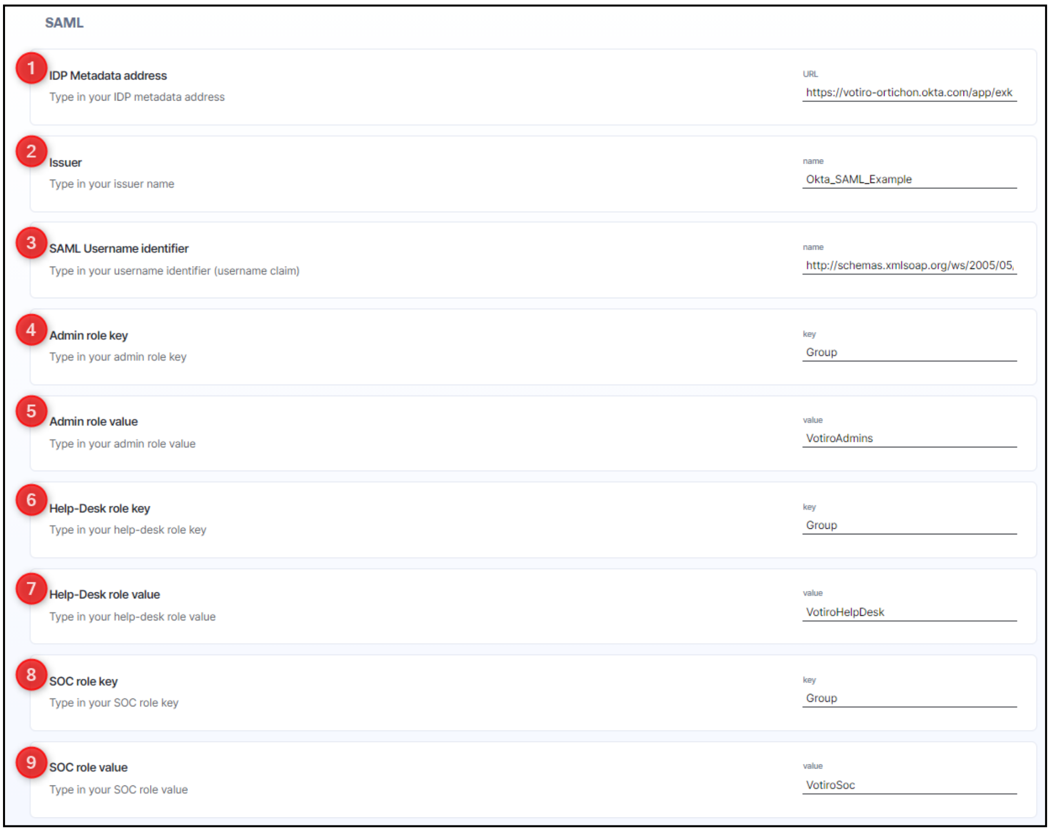
> **Note**
> Fields marked with a * red asterisk are mandatory, to be completed.

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

2.12.7 SAML

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

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



The SAML page contains the following fields:

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

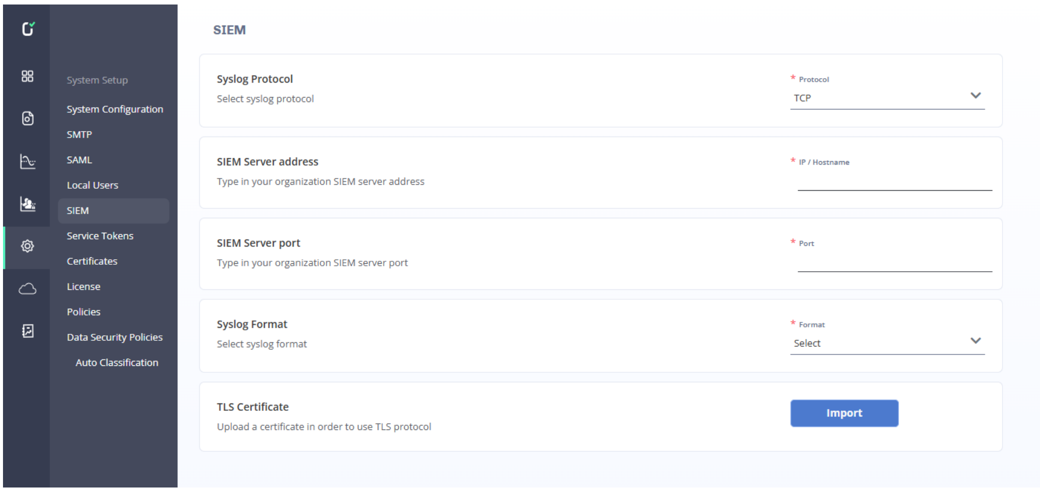
Note
Fields marked with a * red asterisk are mandatory, to be completed.

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

2.12.8 SIEM

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

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



The page contains the following configuration fields:

Element	Field	Description
1	Syslog Protocol	Specifies the Syslog message transport protocol. Select from UDP, TCP, TLS(SSL).
2	SIEM Server address	Address of the SIEM system collector service. Specify a hostname where the address represents a fully qualified hostname or an IPv4 address. The default is empty. When the address is empty, the server uses its own IP as an address. **Note**: The SIEM server address must contain the address protocol (HTTP or HTTPS).
3	SIEM Server port	Specifies the port of the SIEM system collector service. Specify a positive integer between 1 and 65535. The default is UDP port 514. For more information about SIEM logging in Management, see Syslog Events to SIEM Platforms on page 155.
4	Syslog Format	Specifies the Syslog message format. Select from CEF or LEEF.

Element	Field	Description
5	TLS Certificate	If the server mandates certificate authentication to use the TLS protocol, a TLS certificate file must be imported. After importing the certificate file, refresh the page. The certificate name and creation date are displayed. **Note** Only PFX (Personal Information Exchange) formats with no password are currently supported.

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

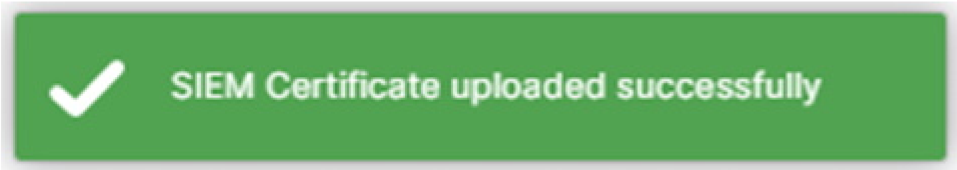
To import a TLS certificate:

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

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

c. After importing the certificate, refresh the page.

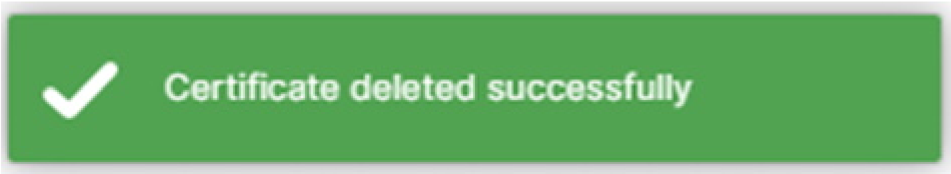
d. The certificate name and creation date are displayed. The following message appears:



To delete a certificate that was imported:

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

b. The following message appears:



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

2.12.9 Syslog Events to SIEM Platforms

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

- Each incident that is created will generate a **Sanitization summary** Syslog message.
- When an incident of an archive or eml/email is triggered, there will be a separate Syslog message for each child inside the archive/email. In this case, there will be a drill down until there are no archive/eml files inside.
  For example:
  - An eml file containing a zip file of 2 word files generates a total of 4 different syslog messages
  - A zip file of 2 word files generates a total of 3 syslog messages
  - A pdf file generates 1 syslog message
  - A docx file generates 1 syslog message
- Syslog messages support UTF8.

The CEF message format is as follows:

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

To enable SIEM logging, you must configure the SIEM settings in the Management Dashboard, see SIEM on page 153.

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

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

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

Mar 10 07:07:32 LEEF:1.0 |**Votiro**|Votiro cloud|9.6.348|500|**Sanitization summary**|5| **CompanyName**=Votiro1 **Correlation Id** = 33a5d413-3be6-4b28-b5b7-257fc2add78d

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

Votiro Sanitization summary Syslog message format

Field #	**Field name**	**Description**	**Value**
1	Timestamp	Event timestamp based on customer time	{MMM DD HH:mm:SS} For example, Mar 10 07:07:32
2	Syslog message format	Syslog message format	**CEF:0**
3	Device vendor	Vendor name	**Votiro**
4	Device name	Device name	**Votiro On-prem**
5	Device version	Product version	{Product version} For example, 9.8.100
6	Signature ID	Signature ID of the event	**500**
7	Message name	Syslog message name	**Sanitization summary**
8	Message severity level	Message severity level. **Note**: All events will be of the same severity level.	**5**
9	Company name	Customer's company name configured in the Management dashboard.	{Company name}
10	Correlation ID	Unique GUID that represents the file	{GUID}
11	Item ID	Unique GUID that represents the file. The Item ID is the same as the Correlation ID if it represents the same file. If the item ID is different, it means that the file is a child or inner file related to the parent file.	{GUID}
12	File name	File name	{character string}
13	File type	File extension	{character string} For example, pdf
14	File hash	Hash of the file	{hash (hexadecimal) string}

Field #	Field name	Description	Value
15	File size	File size in bytes	{long integer}
16	Password protected	Indicates whether the file is password protected	• **true** • **false**
17	AV result	Result from the Anti-Virus engine's scan of the file	• **Infected** • **Clean** • **Not used** (if the AV is not activated)
18	Threat count	Number of threats detected in the file	{integer}
19	Blocked count	Number of blocked files in the file	{integer}
20	Threats	Description of what threats were detected in the file	{character string} For example, Suspicious macro; external link path
21	File modification	Description of what Votiro On-prem modified in the file	{character string} For example, Removed suspicious macros; Removed external link path
22	Sanitization result	Result of Votiro On-prem's sanitization of the file	• **Sanitized** • **Partially sanitized** (indicates a parent file whose inner files are blocked / skipped) • **Skipped** • **Blocked**
23	Sanitization duration	Sanitization time for the file in ms	{integer}
24	Connector type	Type of connector	• **Email connector** • **File connector** • **Menlo connector** • **AWS S3 connector** • **Office 365 connector** • **API** • **Self-sanitization**
25	Connector name	Connector name configured by the customer in the Management Dashboard	{character string}
26	Policy name	Customer policy name	{character string}
27	Exception ID	Indicates which policy exception the file triggered	{integer}

Field #	Field name	Description	Value
28	Incident URL	URL to navigate to the incident in the Management dashboard	{https://{cluster FQDN} /app/fileDetails/ {Correlation ID}/{Item ID}}
29	Message ID	Message ID value assigned by Exchange / Office 365	• {Message ID} • "null"
30	Subject	Email subject	• {character string} • "null"
31	From	Sender's email address	• {character string} • "null"
32	Recipients	Recipients' email addresses	• {character string} • "null"

2.12.10 Audit Events to SIEM - Votiro On-prem

Overview

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

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

What is SIEM

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

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

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

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

Votiro Audit Events Syslog message format

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

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

Audit Event Types

Audit events that should be sent for every user action:

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

Out of scope:

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

Audit Event Message Examples

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

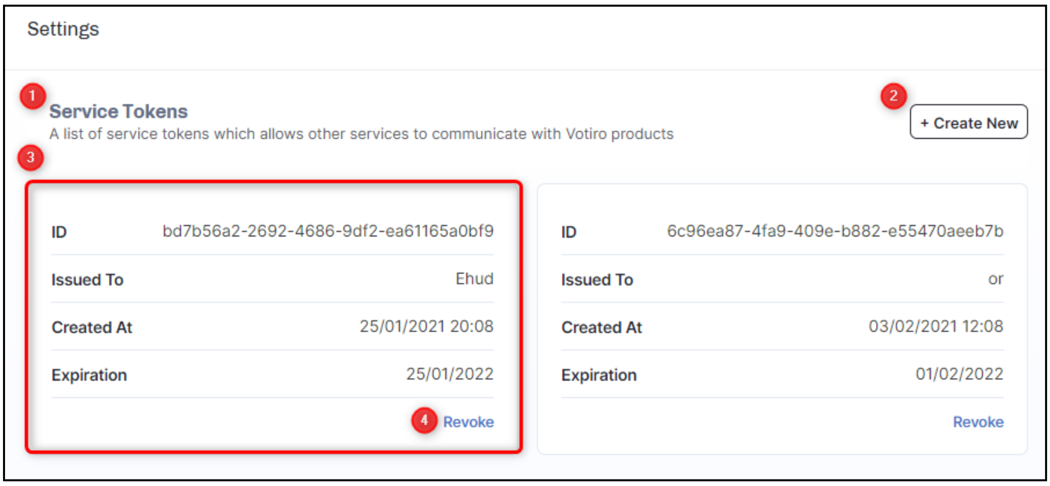
Event Message content	Example
Policy {Policy Name} has been created	Mar 10 07:07:32 CEF:0 |Votiro|Votiro cloud|600|Audit Event|5| CompanyName=Votiro CorrelationId=98061190-e3e2-438b-b9cb-88941c0a6371 msg=Policy 'King' has been created suser=Ron
Policy {Policy Name} has been updated, changes: {change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

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

2.12.11 Service Tokens

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

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



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

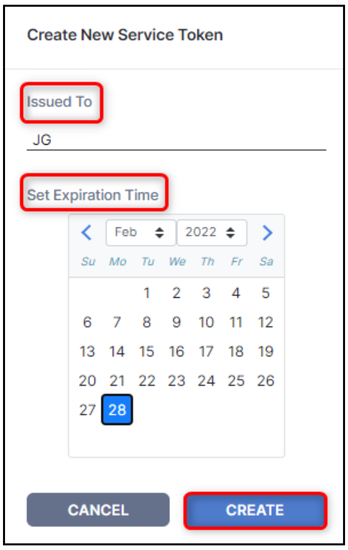
Element	Field	Description
3	Service Token	Details of the service token are displayed: ▪ ID: The ID of the service token is automatically added. ▪ Issued To: Specifies the name you have given to the service token. ▪ Created At: A DateTime stamp is automatically added to the service token. ▪ Expiration: Specifies the date the service token will expire.
4	Revoke	To remove a service token, click **Revoke**. For detailed steps to remove a service token, see Revoking a Service Token on the next page.

Creating a Service Token

To create a new service token:

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

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



3. Click **CREATE**.

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

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

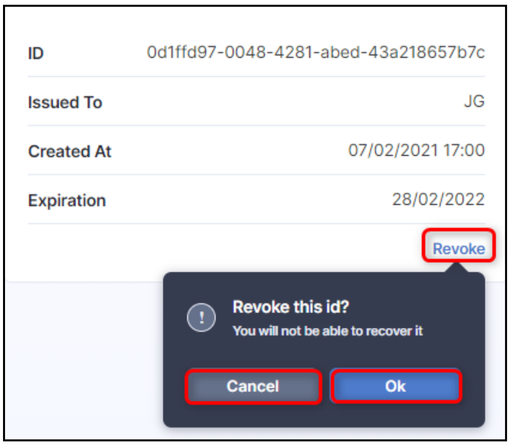
5. Click **OK**.

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

Revoking a Service Token

To withdraw a service token:

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



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

2.12.12 Certificates

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

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

Digital Certificates supported

Votiro supports the following compliance standards by default:

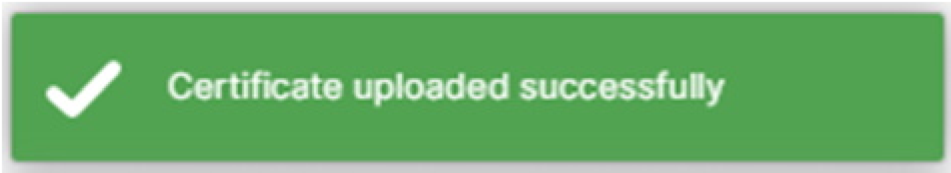
- **AATL** - The Adobe Approved Trust List (AATL) is used to distribute and maintain a list of trustworthy digital certificate issuers for Adobe Acrobat and Adobe Reader. For more details, see Adobe Approved Trust List.
- **EUTL** - The European Union Trusted Lists (EUTL) is a public list of over 200 active and legacy Trust Service Providers (TSPs) that are specifically accredited to deliver the highest levels of compliance with the EU eIDAS electronic signature regulation. For more details, see eIDAS Dashboard.
- **FPKI** - The Federal Public Key Infrastructure (FPKI) is a network of certification authorities (CAs). The Federal PKI includes USA federal, state, local, tribal, territorial, and international governments, as well as commercial organizations, that work together to provide services for the benefit of the USA federal government. For more details, see Federal PKI.
- **CCA** - The Controller of Certifying Authorities (CCA) of India certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates, the Root Certifying Authority of India(RCAI). The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to the CAs in the country. For more details, see Controller of Certifying Authorities.

Uploading a Certificate

To upload a new certificate:

1. Click on the **Add Certificate** button.
2. An explorer window opens. There is an option to select multiple files.
3. Select the desired files to upload.

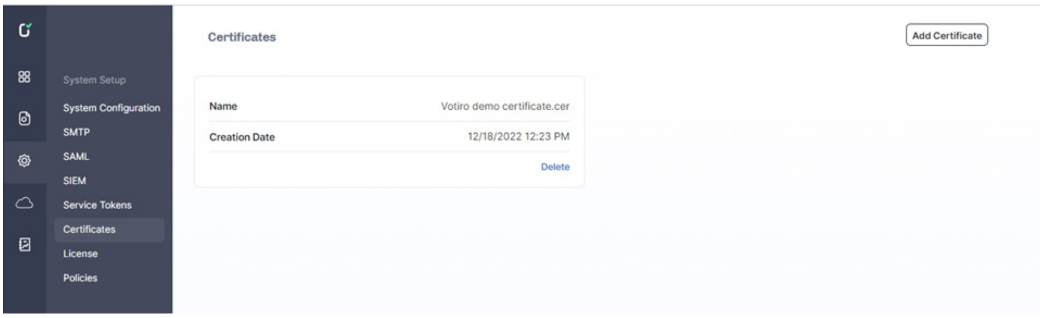
4. After a certificate file is uploaded successfully, the following message appears:



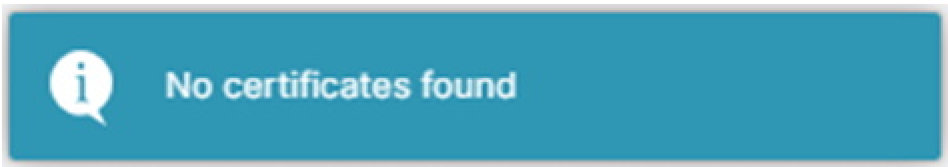
5. If the upload fails, the message **Failed to upload certificate** appears.

Viewing a Certificate

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



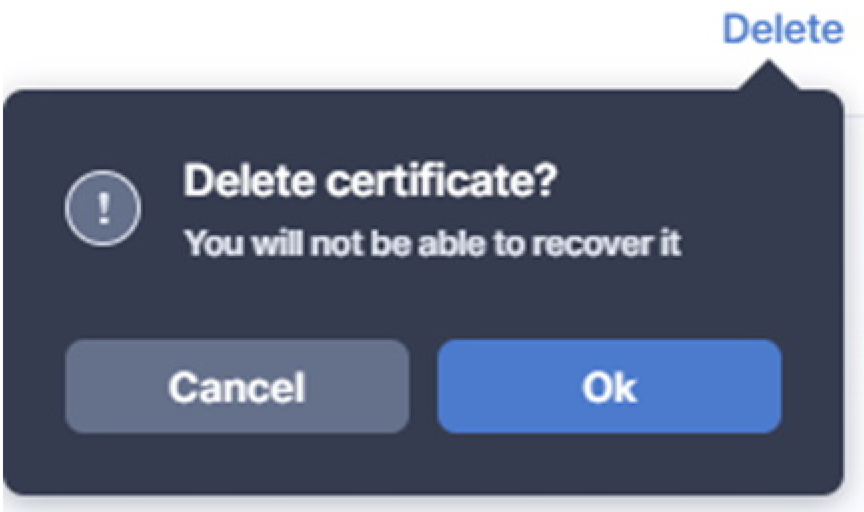
If there are no certificates, the following message appears:



Removing a Certificate

To remove a certificate:

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



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

Sanitizing a PDF with Digital Signatures

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

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

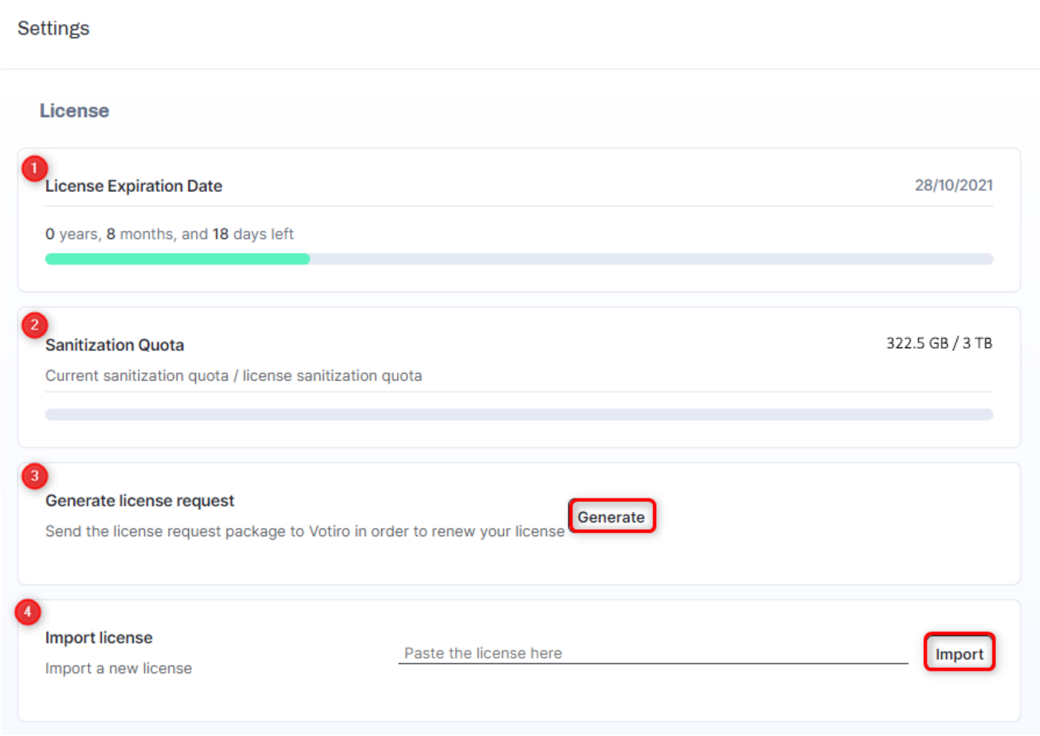
1. Select **Digital signature**.
2. Select **is valid** or **is not valid**.
3. Click on the **Save** button.

2.12.13 License

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

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

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



The license page contains the following configuration fields:

Element	Field	Description
1	License Expiration Date	When a valid license key is imported the expiration date automatically updates to the date when processing of files will stop. At time of installation the default license is valid for 24 hours. During this time files will be processed and a license should be requested.

Element	Field	Description
2	Sanitization Quota	The first figure represents the current consumed size per file. The second figure represents the licensed size quota of files to be processed. See See Sanitization Quota (V9.6.3) for a more complete explanation.
3	Generate License Request	Click **Generate** to produce a license request package. The file **licensePackage.zip** is generated and located in your downloads folder. Pass this file to Votiro Support. A license key will be generated and returned to you within 24 hours of receipt of the request.
4	Import License	Enter the license key provided by Votiro Support and click **Import**. Successful validation automatically updates **License expiration date** and **Sanitization quota** information. The license key disappears. **Note** Votiro On-prem is activated up to five minutes after the license key import.

Sanitization Quota (V9.6.3)

The Sanitization Quota will display consumed size per file.

The accumulated file size consumption is determined as follows:

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

Examples

- A 400KB PDF will be accumulated as 400KB regardless of the size of the embedded files inside the PDF.
- A 1MB image file will be accumulated as 1MB.
- A 10MB archive file containing five 10MB PDFs will be accumulated as 50MB.

- A 11MB EML file with an attached 10MB zip file that contains five 10MB PDFs will be accumulated as 50MB.

File count for an archive file or email with attachments

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

For example:

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

Other file types are not affected by these changes.

For example:

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

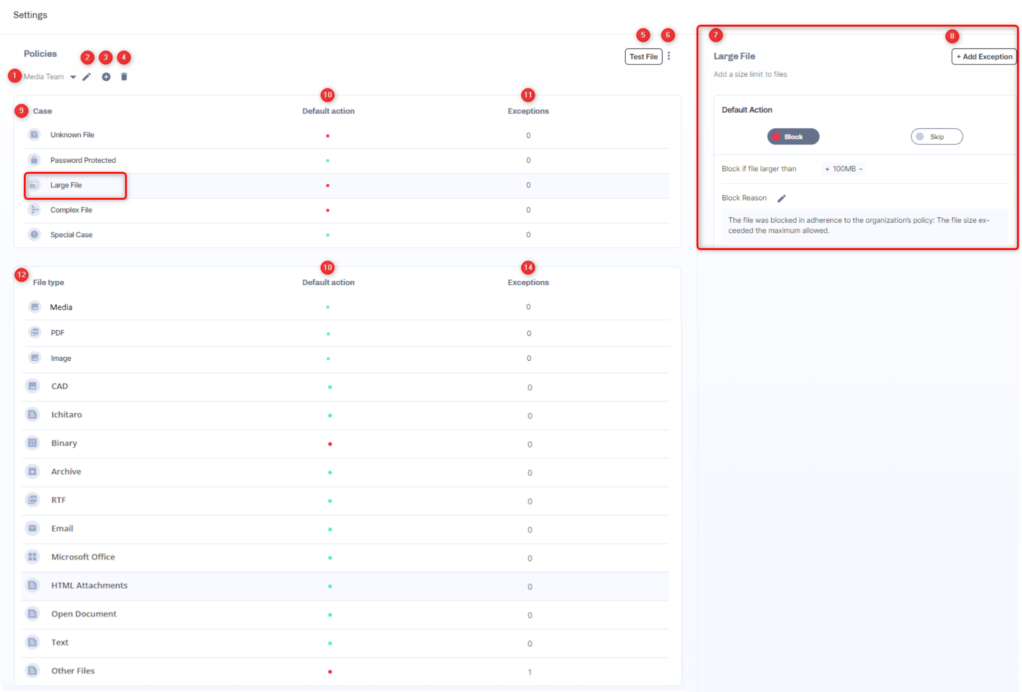
2.12.14 Policies

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

Policies Dashboard

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

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



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

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

Defining Policies

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

- **Case**: a policy using a file's characteristics, for example, password protected, size of file. For more information, see Defining Policies by Case below.
- **File Type**: a policy using a file's family, for example, PDF, Microsoft Office, images. For more information, see Defining Policies by File Type on page 176.
- **Exception**: a policy where you can define one or more exceptions to any case policy or file type policy. For more information, see Adding Policy Exceptions on page 184.
- **Special Case**: If you have custom, XML-based policy definition, you can load it to the Management Dashboard as a special case. This is also known as a **custom policy** – that has been created outside the Management Dashboard. This feature is recommended for special purposes only. For more information, contact Votiro's Support.

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

File Blocking

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

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

2.12.15 Defining Policies by Case

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

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

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

For more information about the policies page, see Policies Dashboard on page 171.

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

- Block the file under all conditions. If selected:
    - Additional options may be available for you to set.
    - You can edit the default block notification message text, **Block Reason**.
    - The **Default Action** displays a **red dot**.
- Sanitize the file. If selected:
    - Additional options may be available for you to set.
    - The **Default Action** displays a **green dot**.
- Skip the file. The **Default Action** displays a **grey dot**.
- Add one or more exceptions to the policy. The **Exceptions** displays the number of exceptions applied to the policy. For more information, see Adding Policy Exceptions on page 184.

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

Table 2 Positive Selection Processing Options for Cases

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

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

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

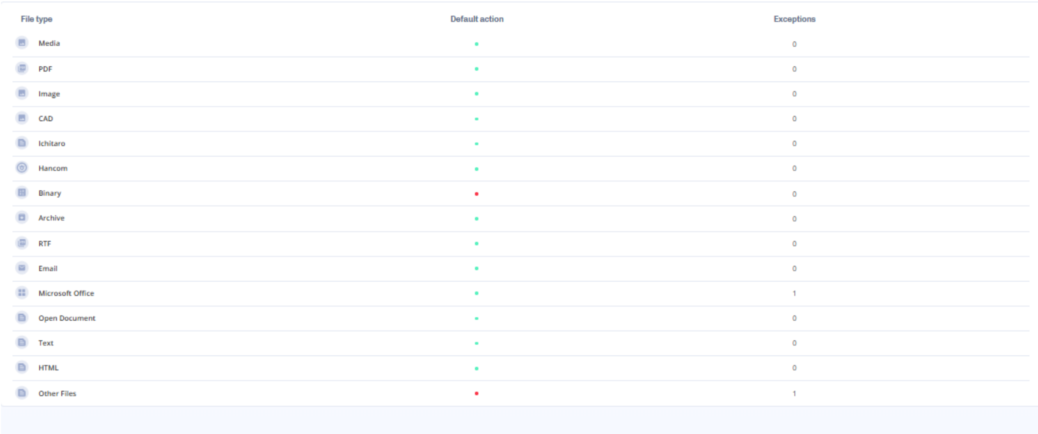
When the files are blocked, Votiro On-prem issues a block-file containing the reason it was blocked. The notification contains a link that opens a Password Protected File portal where the password can be entered. When the correct password is entered, the blocked file returns to the storage server, for processing. The processed file is then downloaded to the recipient's computer, or sent by email as an attachment.
Note
This feature supports the following file types only: PDF, ZIP, 7zip, RAR, DOC, DOCX, DOT, DOTX, DOCM, DOTM, XLS, XLT, XLSX, XLTX, XLSM, PPT, PPS, POT, PPTX, PPSX, POTX and PPTM. It does not work on other file types that can be protected by a password, such as Visio files.
<h3>Instructions for Email User</h3>
The Votiro On-prem administrator should communicate the following information and instructions to the users.
An email message with password protected files attached can be processed for positive selection and returned as an email attachment, or as a download. The user receives a message that a password protected file has been received, with the option to enter the password, then click Get File.
The password protected file is processed for positive selection, then attached to the email. This is distributed to all named recipients. If Votiro On-prem has already processed password protected files, additional users requesting files to be processed will be advised that this has already taken place.
Note
This feature supports the use of one password per email.
</td></tr>
</table>

Case	Processing Options
Large File	You can set the minimum size of files you want to block. When this option is checked, for every file that Votiro On-prem blocks, it issues a block-file containing the reason it was blocked. Accept the default text or edit it.
Complex File	You can set a layer number. The maximum layer number = 15. Files that are found in that layer or deeper are blocked.
Special Case	You will have already defined a Special Case with Votiro's support team. Click **Load File**. For more information, see Defining Policies on page 173.

2.12.16 Defining Policies by File Type

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

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



File type	Default action	Exceptions
Media		0
PDF		0
Image		0
CAD		0
Ichitaro		0
Hancom		0
Binary		0
Archive		0
RTF		0
Email		0
Microsoft Office		1
Open Document		0
Text		0
HTML		0
Other Files		1

For more information about the policies page, see Policies Dashboard on page 171.

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

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

    - The **Default Action** displays a **green dot**.
- Allow the file. The **Default Action** displays a **grey dot**.
- Add one or more exceptions to the policy. The **Exceptions** displays the number of exceptions applied to the policy. For more information, see Adding Policy Exceptions on page 184.

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

Table 3 Positive Selection Processing Options for File Types

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

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

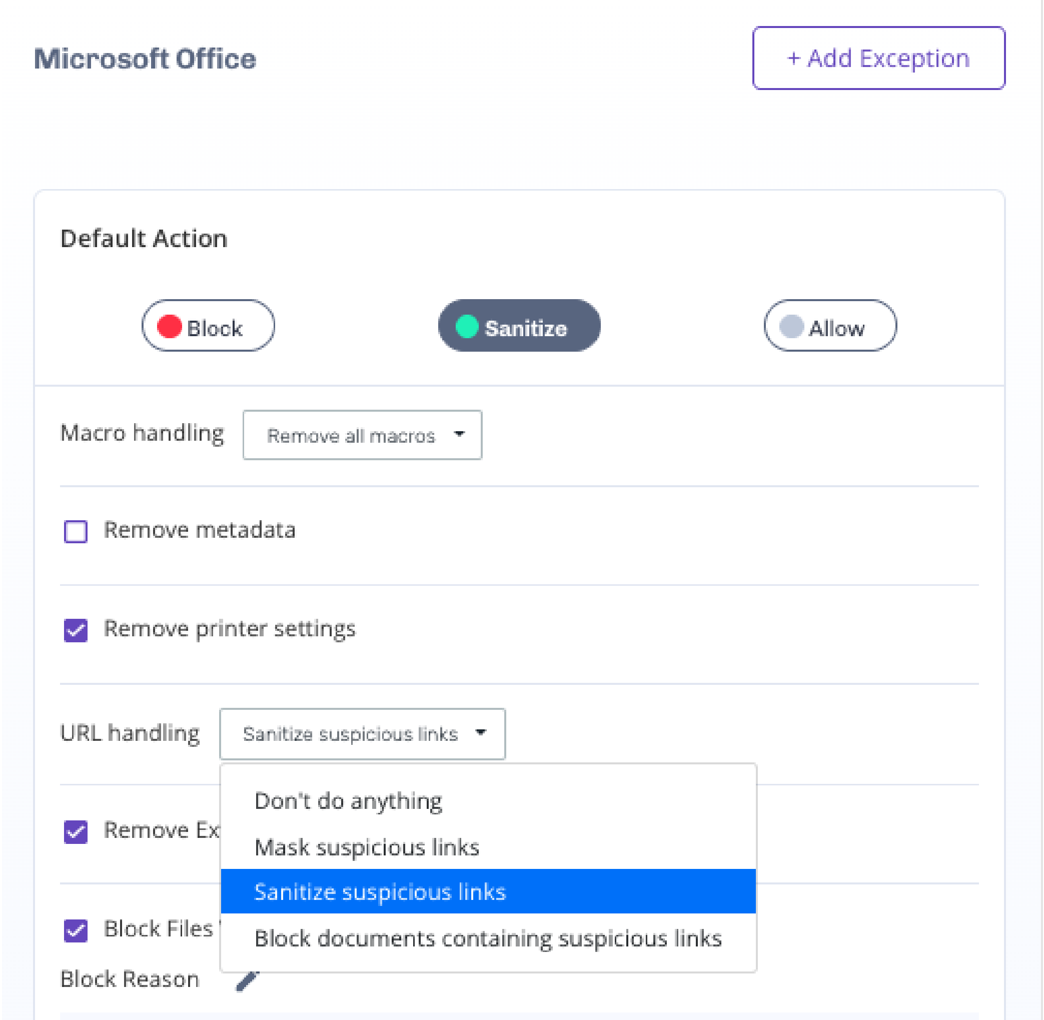
File Type	Processing Options
Archive	By default, these files are processed for positive selection. **Block zip bomb**: Detects and blocks zip files with abnormal compression ratio. These might pose a denial of service threat, consuming system resources such as CPU or disk. Any zip files with compression ratio higher than 99.8% will be considered a zip bomb and be blocked. When selected you can edit the **Block Reason** message. Default is checked. **System locale**: Select your preferred system locale. This enables you to sanitize archive files with ANSI encoding according to the selected **System locale**. The available options are: - **en_US** - English (US) - **fr_FR** - French (France) - **de_DE** - German (Germany) - **he_IL** - Hebrew (Israel) - **ja_JP** - Japanese (Japan) - **ko_KR** - Korean (Korea) - **th_TH** - Thai (Thailand) The default **System locale** is **en_US**.
CAD	**Remove VBA Macros**: Removes VBA macros from the file. Default is unchecked.
RTF	By default, these files are processed. There are no specific processing options.
HTML Attachments	There is an additional option: **Remove scripts**. This is the default action. If this option is selected, every script will be removed from the HTML Attachment file.
Email	By default, these files are processed for positive selection. - **Remove suspicious links in Email body**: The system will scan each URL in the email body, and if a suspicious link was found, the link will be removed and will be replaced with the following text: "This link was removed because it is a malicious URL". - **Include URL to Password-protected portal**: Includes a link to the Password-protected portal (see Password Protected Portal). - **Add sanitization indication in Email body**: Adds an indication of the sanitization status in the body of the Email.

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

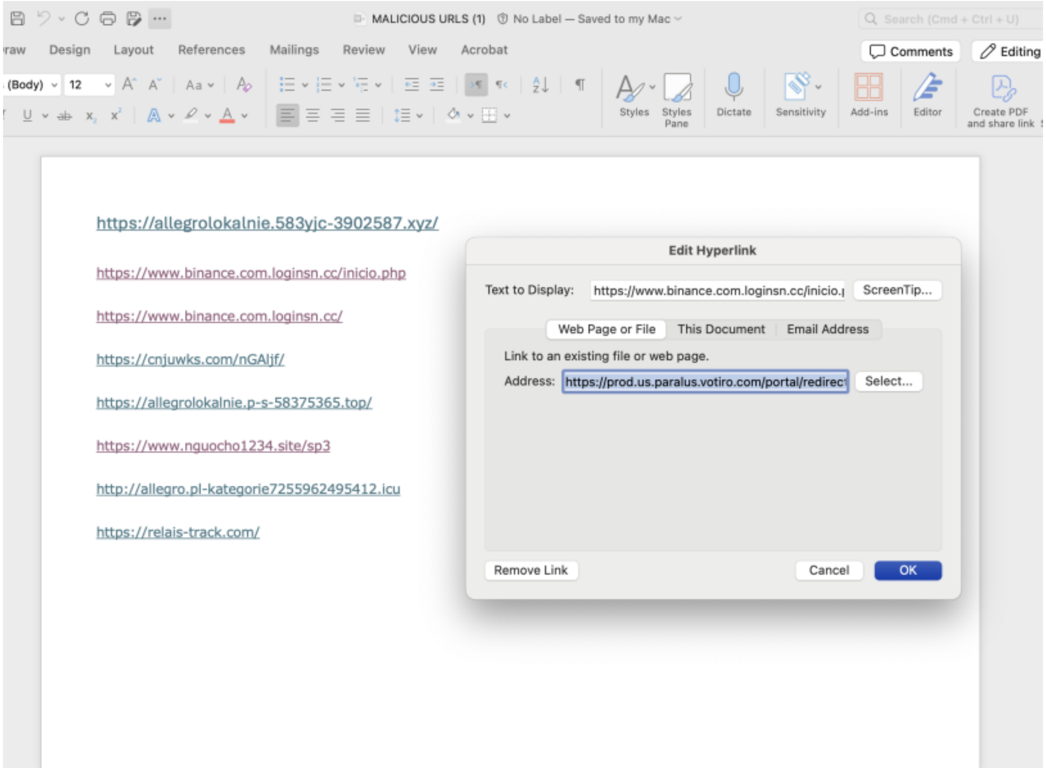
File Type	Processing Options
Text	**Note** XML and JSON files are processed according to the Text files policy. By default, these files are processed for positive selection. If any suspicious activity is detected, the file is blocked. If no suspicious activity is detected, the text file is preserved (the file hash will remain the same). **Block CSV with threat formula**: Blocks CSV files that contain formula injections.When selected you can edit the **Block Reason** message. Default is checked.
Media	The user can set Media file policy exceptions. ■ **Remove metadata**: Removes metadata from media files. Default is unchecked.
Open Document	The user can set Open Document file policy exceptions. By default, these files are sanitized. During the sanitization, the macros will not be preserved.
Ichitaro	■ **Remove macros**: Removes macros from the document. Default is checked. ■ **Preserve original Ichitaro OLE objects**: Preserves OLE controls and OLE sheets. Default is checked.
Hancom	■ **Remove macros**: Removes macros from the document. Default is checked. ■ **Remove scripts**: Removes scripts from the document. Default is checked. ■ **Remove metadata**: Removes metadata from the document. Default is checked. ■ **Remove printer settings**: Removes printer settings from the document. Default is checked. ■ **Remove Embedded Fonts**: Removes embedded fonts from the document. Default is checked. ■ **URL handling**: Selects the action to perform on a URL for Hancom files. ■ **Remove External Links**: Removes external links from the document. Default is checked.
Other files	By default, these files are blocked. You can edit the **Block Reason** message. There are no specific sanitization processing options.

2.13 Workflow - Sanitize URLs

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

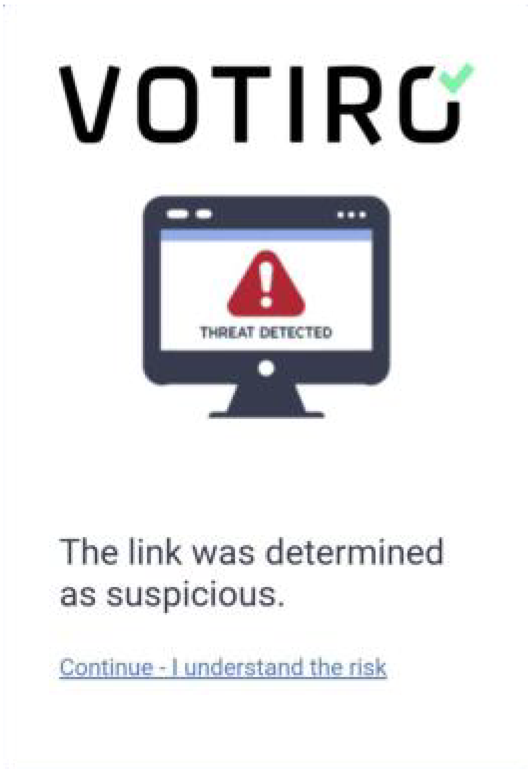


2. A protected user receives a file from a URL.
3. When the user clicks on the URL, the user will be redirected to the Votiro portal.

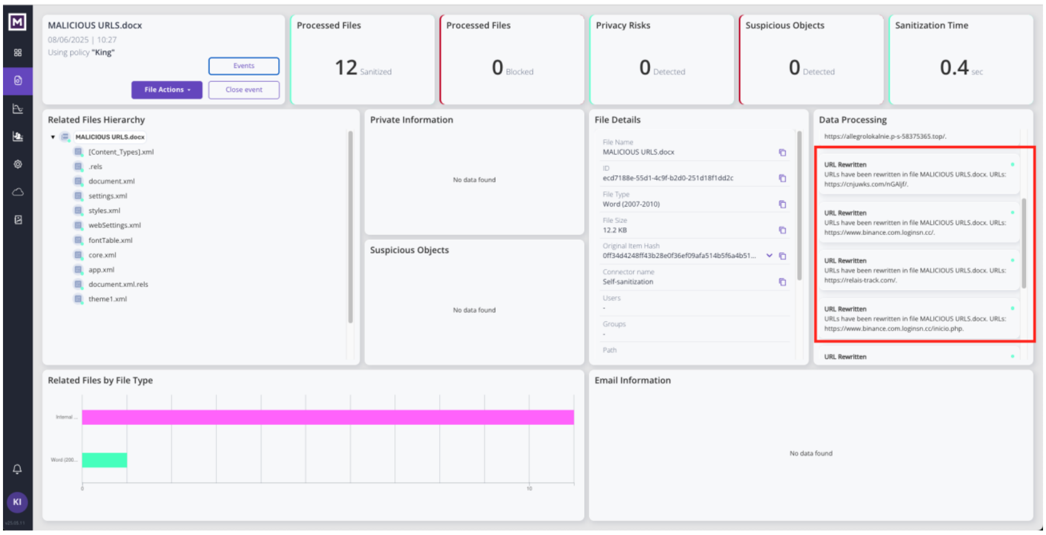


4. If the URL was determined to be benign, the user will be redirected to the desired URL.

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



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



2.13.1 Adding Policy Exceptions

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

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

- File type

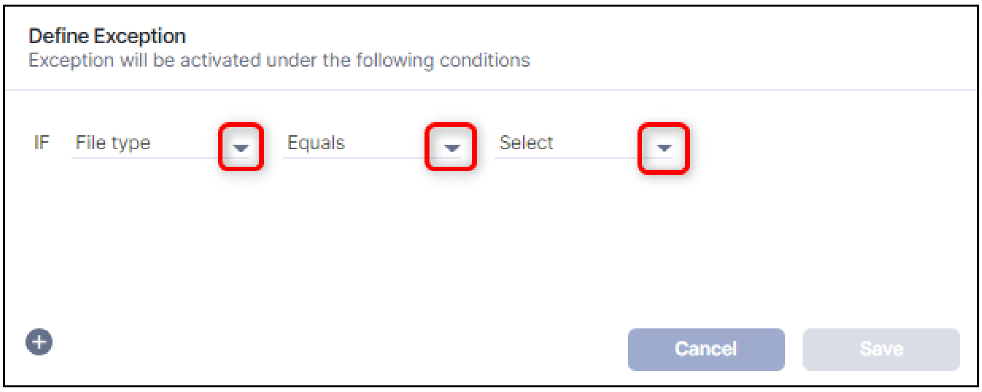
- File size
- Email (for Votiro On-prem for Email only)
- File extension
- Digital signature

For more information about the policies page, see Policies Dashboard on page 171.

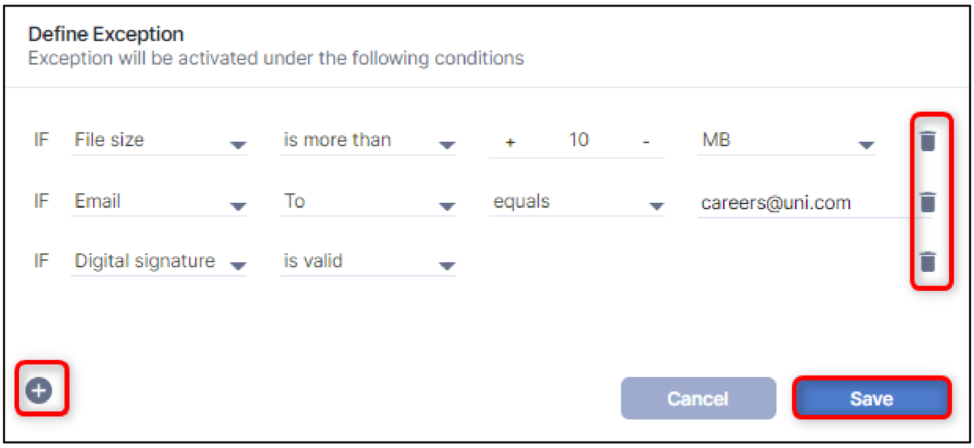
Adding an Exception:

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

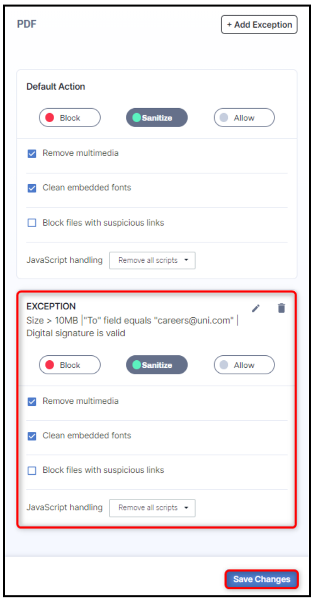
1. From the navigation pane on the left, click **Settings** > **Policies**.
2. Click the case or file type policy you wish to define an exception for.
3. In the top right corner, click **+ Add Exception**. The Define Exception window appears:



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

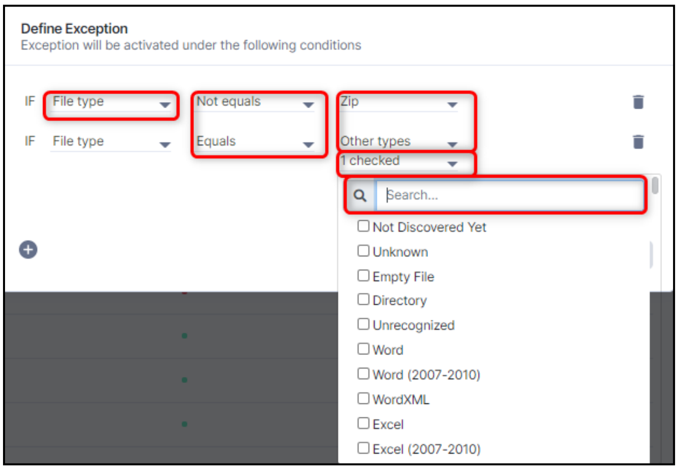


6. When your exception definition is complete you can activate the exception by clicking **Save**. To abandon the exception definition, click **Cancel**. You will return to the policy page.



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

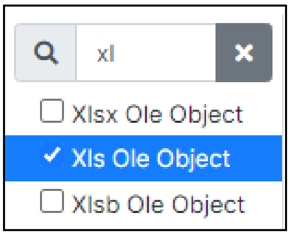
Defining Exceptions for File Types



To specify an exception for one or more file types:

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

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



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

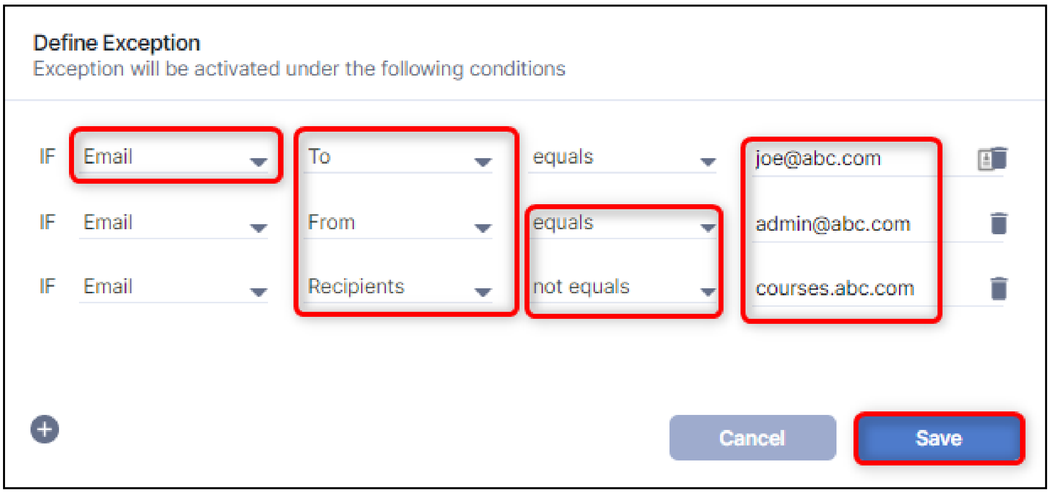
Defining Exceptions for File Size

To specify an exception based on on file size:

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

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

Defining Exceptions for Email Senders or Recipients



You can specify any of the following:

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

Defining Email and Domain Addresses - Full and Partial

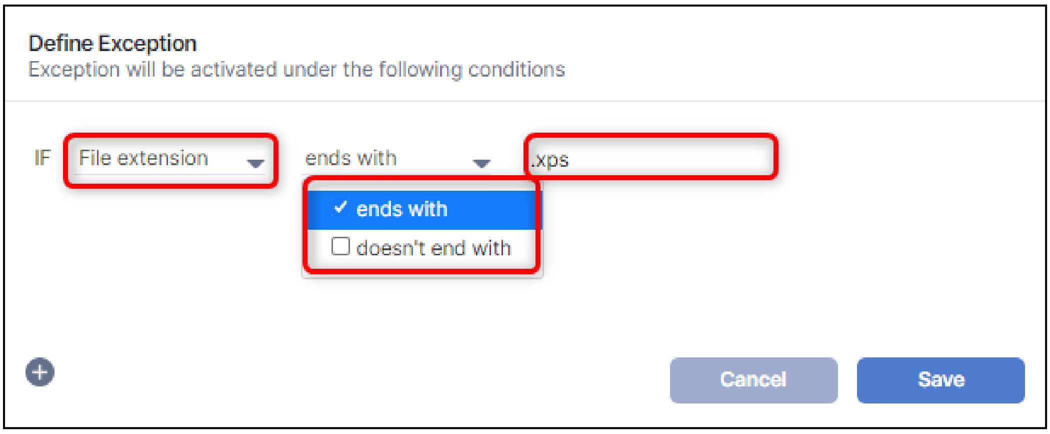
You can specify:

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

Guidelines and examples:

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

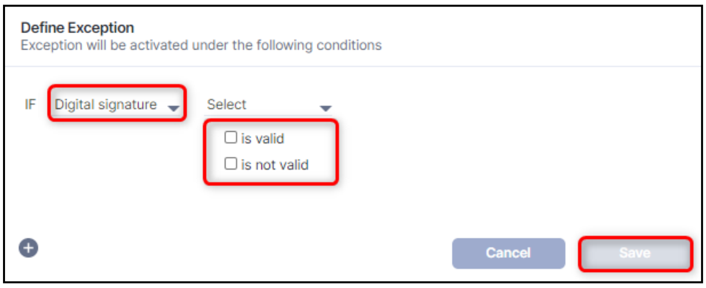
Defining Exceptions for File Extensions



To specify a list of file type extensions:

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

Defining Exceptions for Validating Signatures



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

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

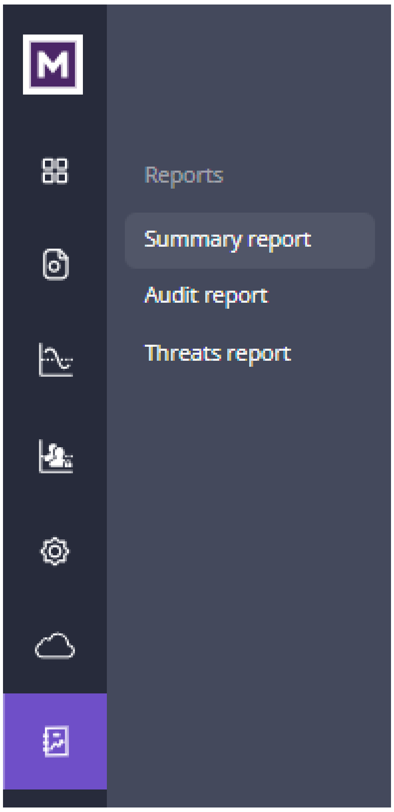
Note: Files with digital signatures from the following compliance standards are supported by Votiro and are valid by default:

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

2.14 Generating Reports

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

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



2.14.1 Summary Report

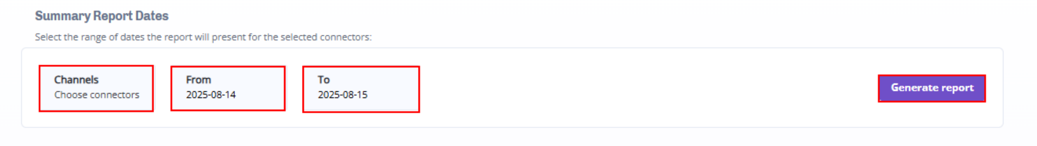
You can generate a summary report of the positive selection processing activity in your organization for a specified period.

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

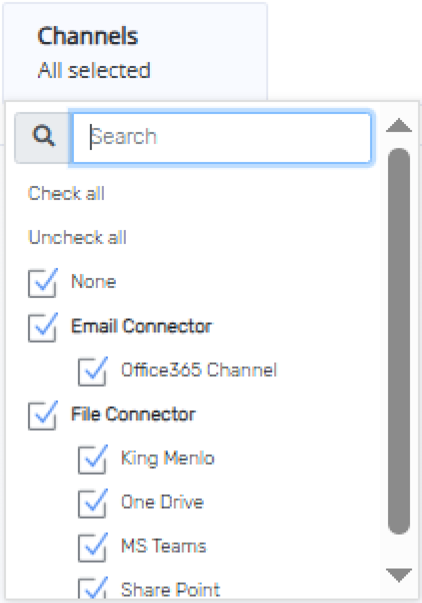
The report presents usage and security date in graphic format and also provides tips for optimizing your positive selection processing effort.

To generate a Summary report, follow these steps:

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

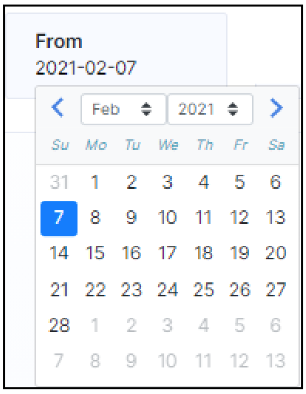


2. Click **Channels**, then select the connectors you wish to appear in the report.



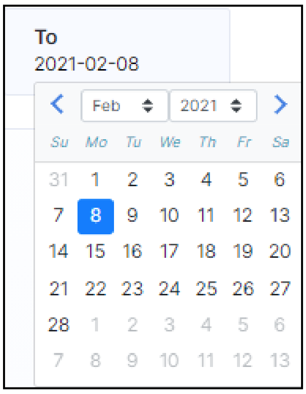
3. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:

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



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

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



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

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

Summary Report Format and Structure

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

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

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

2.14.2 Audit Report

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

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

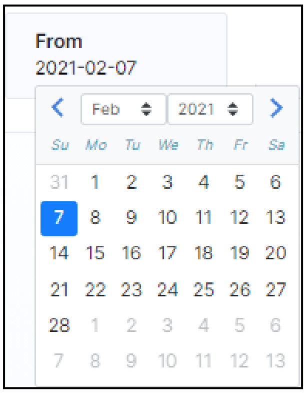
You can audit all actions that were performed by users of the Management Dashboard for a specified period. The exported report generated is a CSV file.

To generate an Audit report, follow these steps:

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

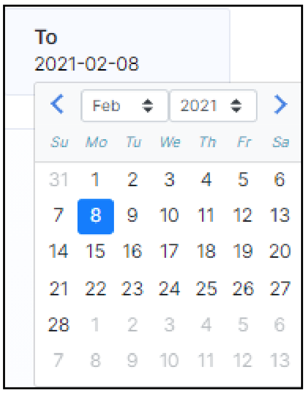
2. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:

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



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

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



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

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

Audit Report Format and Structure

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

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

1/11/2018 11:52	RonF	LoginEvent	Successful login with Full permissions	
1/11/2018 13:05	user1	PolicyAddEvent	A new policy was created	policyId: 37a0add2-b521-442c-
1/11/2018 14:46	Default (unauthoriz	LoginEvent	Successful login with Full permis	
1/11/2018 15:07	RonF	LogoutEvent	Logout	
1/11/2018 15:41	Default (unauthoriz	LoginEvent	Successful login with Full permis	
1/11/2018 16:02	Default (unauthoriz	PolicyDeleteEvent	Policy 321_deleted_63676692124	policyId: 3d24ce9e-faca-4004-
1/11/2018 16:02	Default (unauthoriz	PolicyUpdateEvent	Policy jhg was changed	policyId: aab369db-32dd-4bad-
1/11/2018 16:03	Default (unauthoriz	ConfigurationEvent	3 Configuration record/s were u	updates:
1/11/2018 16:03	Default (unauthoriz	LogoutEvent	Logout	
1/11/2018 16:03	user1	LoginEvent	Successful login with Full permis	
1/11/2018 16:03	user1	UsersEvent	1 user/s permissions were updat	updates: Updated RonF from

Information is provided for the following actions:

- Login
- Logout
- Original file download
- Processed file download
- Release original
- Policy save
- Settings save
- Roles changes
- Report export
- Policy creation
- Create user
- Delete user
- Reset password

2.14.3 Threats Report

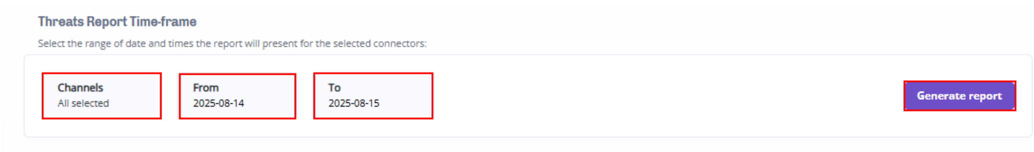
Votiro On-prem tracks threats to files submitted for testing in the Management Dashboard.

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

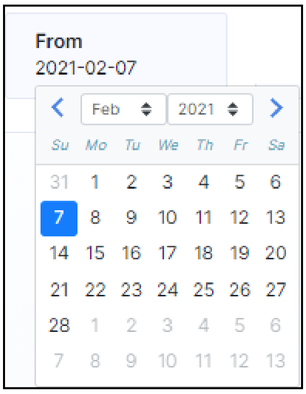
The report collects useful data of the positive selection processing activity. The threat report files generated are used internally by Votiro for support and research purposes.

To generate a Threats Report, follow these steps:

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

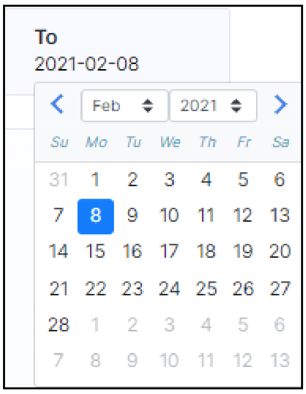


2. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:



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

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



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

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

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

Threat Report Format and Structure

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

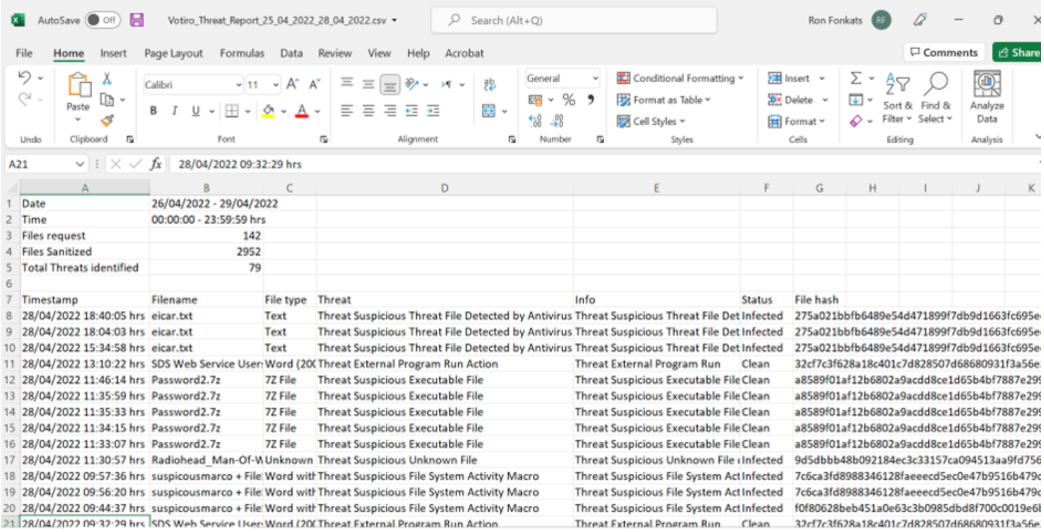
The header at the beginning of the threat report contains the following fields:

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

The body of the threat report contains the following fields:

Field	Value	Multi-values	Example
Timestamp	DD-MMM-YYYY hh:mm:ss "hrs" *Based on customer local time (Same as the Management dashboard time)	Not supported	18Mar2022 18:49:29hrs
Filename	Parent file name	Not supported	VotiroDemo.zip
File type	Parent file type	Not supported	Zip File
Threat	List of the threats that have been identified on the Parent and Children *Should be sorted as the file tree from the Management File info	Supported	Suspicious Unknown File Suspicious Unknown File
Info	List of all threats and the file names associated with these threats *Should match to the sort from the threat column Format: "Threat X detected in File Y"	Supported	Suspicious Unknown File detected in VotiroDemo1.shx Suspicious Unknown File detected in VotiroDemo2.shp
Status	Parent file status result	Not supported	Status options: Infected, Clean, Error, Unknown
File hash	Parent file hash	Not supported	7cd6773d80d4cdf28671d9e3a095 c66fdc20feaac15c4e075 4748dbd2541a7e9

Threat Report Example



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

2.15 Password Protected Portal

2.15.1 Customizing the PPF Portal Logo

You can configure the image in the PPF portal to be your organization's logo by placing an image file named **logo.png** file in the **Extras** folder. The image should be cropped and without padding. Update Votiro On-prem from the same folder, using the following command:

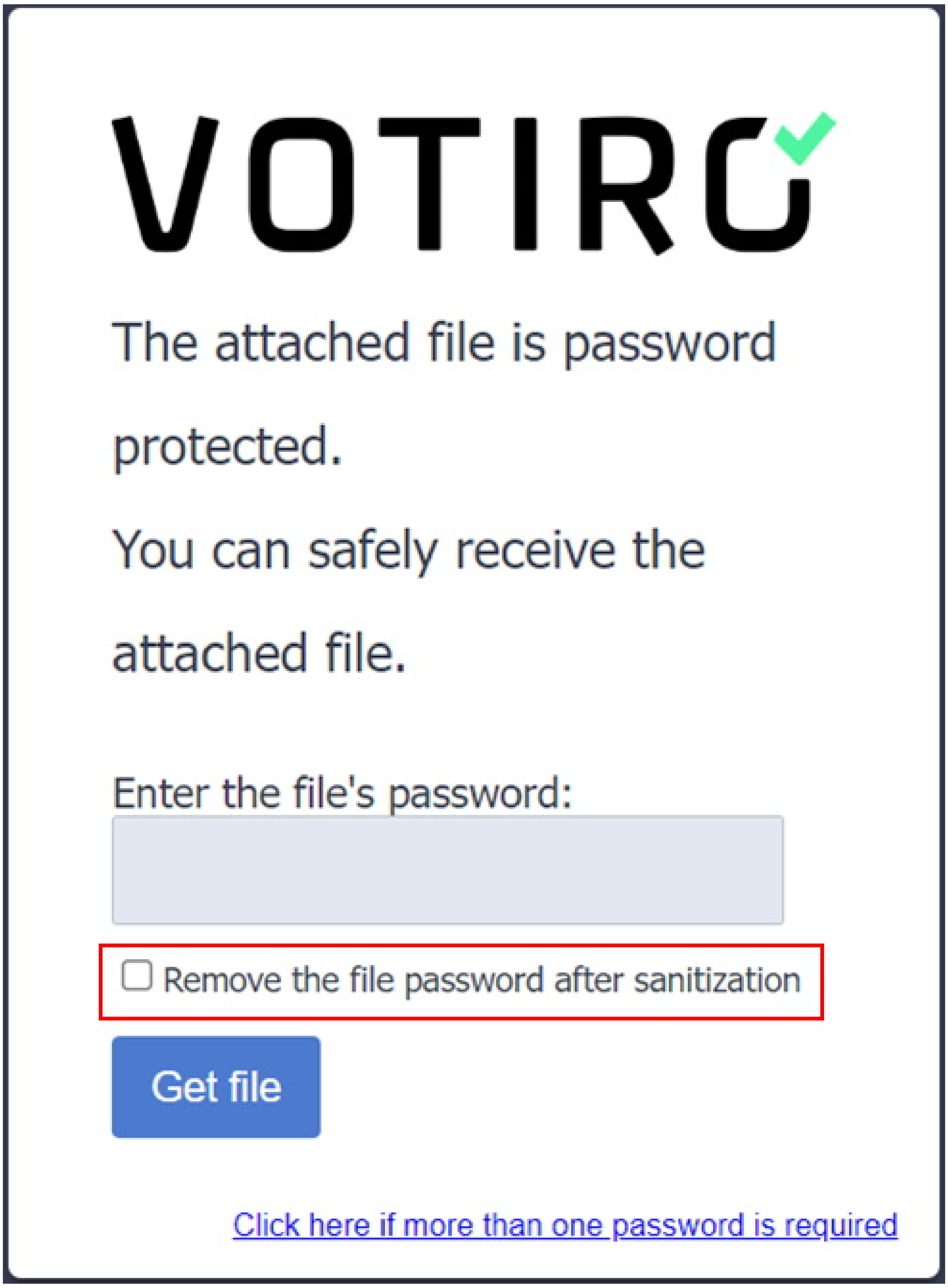
```
update-password-protected—portal-logo.sh
```

The PPF portal will be updated and use the new image instead of the default.

2.15.2 Removing PPF Encryption

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

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



If you check the box, then:

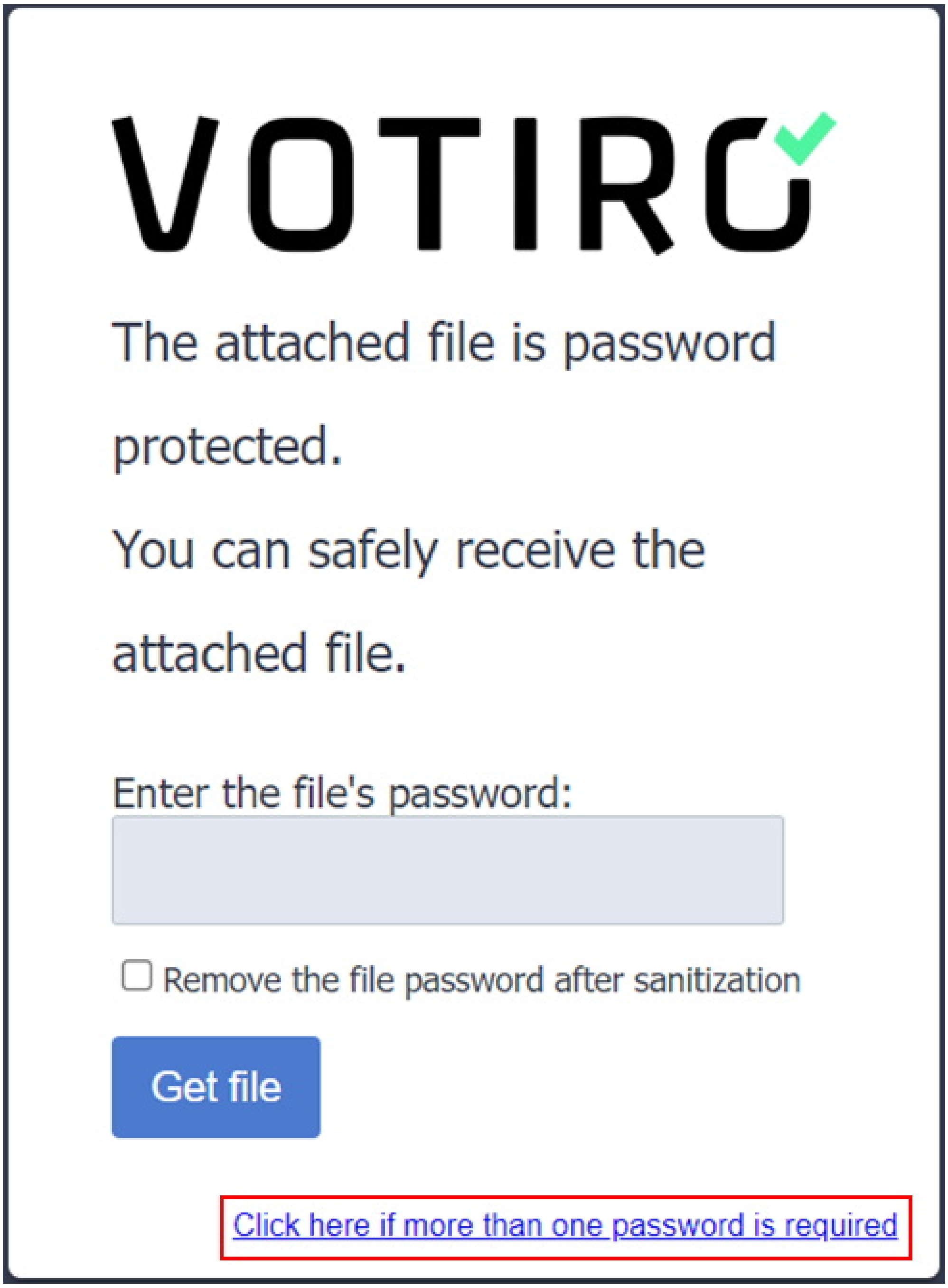
- If the file origin is email, the new email will be sent to all recipients where the sanitized file will not require any password.

- If the file origin is API, the user will download the sanitized file, which will not be password protected.

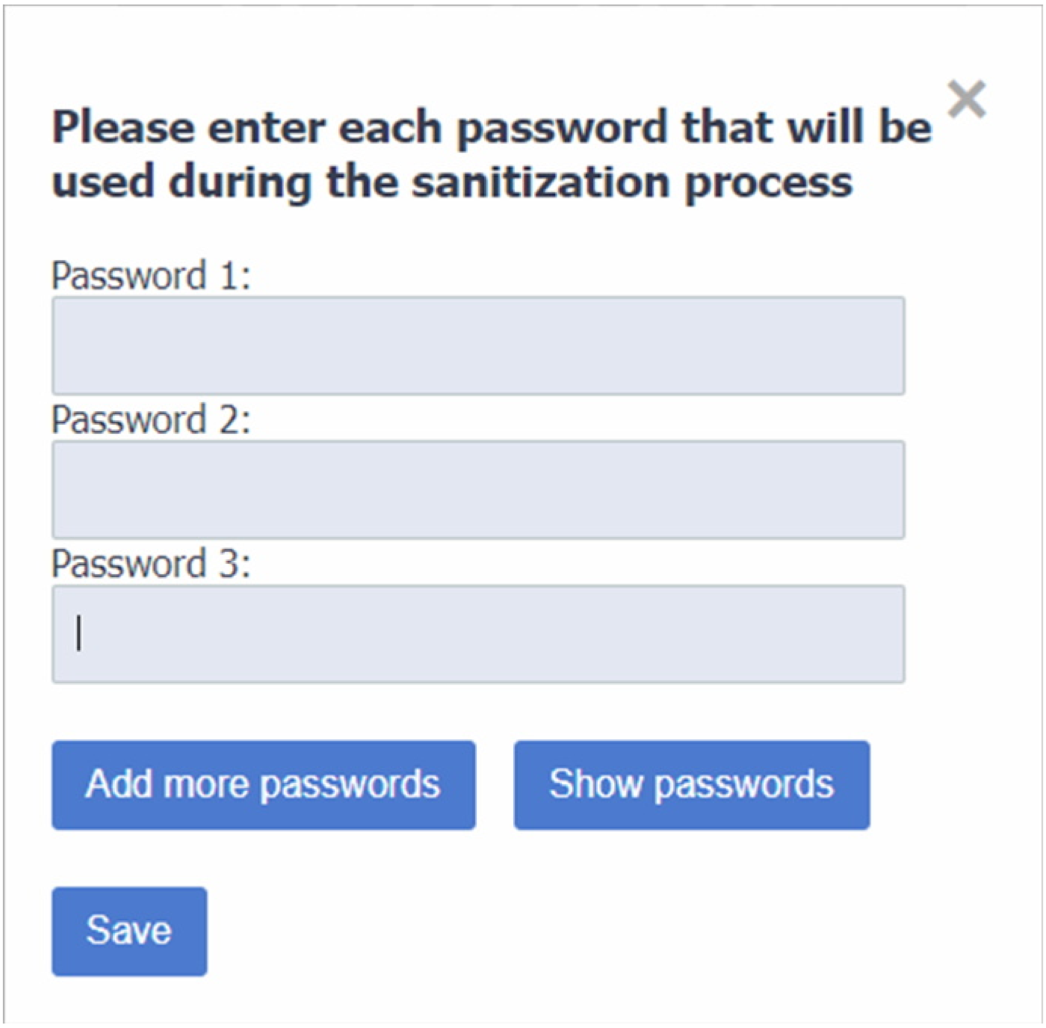
2.15.3 Support of Multiple Passwords within PPF Sanitization

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

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



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



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

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

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

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