

VOTIRO

Votiro Cloud - VA On-premises V9.7

User Guide

February 2024

Copyright Notice

The material herein is proprietary to Votiro CyberSec Ltd. This document is for informative purposes. Any unauthorized reproduction, use or disclosure of any part of this document is strictly prohibited.

Votiro CyberSec's name and logos are trademarks of Votiro CyberSec Ltd., its subsidiaries or affiliates. All other company or product names are the trademarks of their respective holders.

www.votiro.com

Contents

- 1 Introduction 5**
 - 1.1 Votiro Cloud Technology 5
 - 1.2 System Architecture and Data Flow 5
 - 1.3 Positive Selection® Engine 6
 - 1.4 Supported File Types 7
- 2 Using the Management Dashboard20**
 - 2.1 Logging in to the Management Dashboard: VA on-premises 20
 - 2.1.1 Sign in with Active Directory credentials 20
 - 2.1.2 Sign in with SSO (using corporate credentials) 22
 - 2.2 Monitoring Positive Selection Activity 23
 - 2.2.1 Monitoring Periods25
 - 2.2.2 Live Status 26
 - 2.2.3 Incoming Traffic27
 - 2.2.4 Secure File Gateway 28
 - 2.2.5 Protection & Business Productivity 29
 - 2.2.6 Test File29
 - 2.3 Exploring Incidents 29
 - 2.3.1 Viewing Detailed File Information31
 - 2.3.2 Using Filters 32
 - 2.3.3 Retro Scan 33
 - 2.3.4 Searching Positive Selection Requests 33
 - 2.3.5 Releasing Files 34
 - 2.4 Configuring Settings 36
 - 2.4.1 System Configuration36
 - 2.4.2 Active Directory 41
 - 2.4.3 Configuring Active Directory with LDAPS43
 - 2.4.4 SMTP 44
 - 2.4.5 SAML 46
 - 2.4.6 Users47

2.4.7 SIEM	49
2.4.8 Service Tokens	51
2.4.9 Certificates	54
2.4.10 License	56
2.4.11 Policies	58
2.5 Cloud Connectors and Integrations	61
2.5.1 AWS S3 - VA On-premises	61
2.5.2 Menlo Security	68
2.5.3 Box	70
2.5.4 Fortinet Sandbox	84
2.5.5 Office365 Mail	87
2.5.6 Chrome Browser Extension	96
2.6 Password Protected Portal	112
2.6.1 Customizing the PPF Portal Logo	112
2.6.2 Removing PPF Encryption	113
2.6.3 Support of Multiple Passwords within PPF Sanitization	114
2.7 Generating Reports	116
2.7.1 Summary Report	117
2.7.2 Audit Report	119
2.7.3 System Report	121
2.7.4 Diagnostics Report	124
2.7.5 Threats Report	125
Appendix A Syslog Events to SIEM Platforms	129
Appendix B Defining Policies by Case	133
Appendix C Defining Policies by File Type	136
Appendix D Adding Policy Exceptions	141

1 Introduction

1.1 Votiro Cloud Technology

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

Votiro Cloud 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 Cloud. This results in every file entering your organization's network being 100% safe.

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

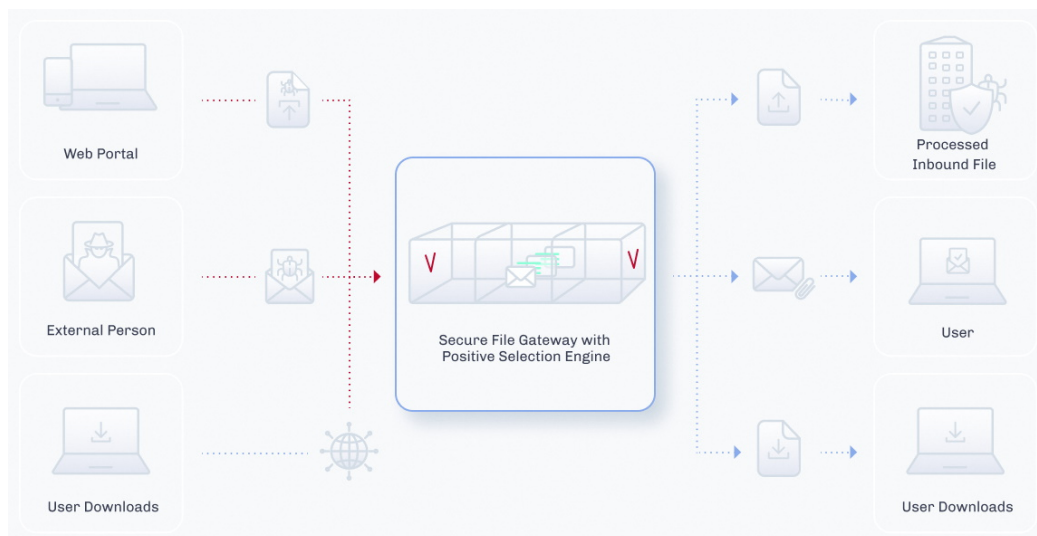
True Type Detection

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 Cloud 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

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



Data flows between Positive Selection® Engine, Votiro Cloud for Web Applications, Votiro Cloud for Email and Votiro Cloud for Web Downloads. 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 Cloud 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.

1.3 Positive Selection® Engine

Votiro's Positive Selection® Engine is at the heart of the Votiro Cloud 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 Cloud. 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.
- 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 File ** ^	Raster Image Files	pgm
	PPM File ** ^	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	
Binary	Binary File ^	Any Binary Files	dat, db
	Executable ^	Any Binary Files	exe, com, dll, pif, sfx, msu, msp, msi, mo
Archive	Bzip2 ^	Single compressed file	bz2
	7Z File	Archives	7z
	CAB file ^	Archives	cab, wsp
	GZ File	Archives	gz
	GZIP File	Archives	gzip
	InstallShield CAB file ^	Archives	cab
	LZH File ^	Archives	lzh
	RAR File	Archives	rar, rar5
	Tar File	Archives	tar
	VMware Virtual Machine Disk ^	Archives	vmdk
	Xz ^	Single compressed file	xz
	ZIP File	Archives	zip

File Type in Management	File Type	Family Type	Main Extension
RTF	RTF Files	RTF Files	rtf
Email	Calendar File	Calendar Files	ics
	DAT File ** ^	EML Files	dat
	EML File	EML Files	eml, tmp
	Encrypted EML File ^	EML Files	eml, tmp, p7s, p7m
	HTML Body ^	HTML Files	html, htm
	HTML Attachments	HTML Files	html, htm
	MSG File	MSG Files	msg
	PST ^	PST Files	pst
	PST ANSI ^	PST Files	pst
	RPMSG Files ^	Restricted Permission Message Files	rpmsg
	TNEF Calendar Files **	EML Files	eml
	TNEF File **	EML Files	eml
	VCF File	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
	Excel (2007-2010)	Microsoft Office	xlsx
	Excel95 Files	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 Files ** ^	Microsoft Office	wri
	Power Point	Microsoft Office	ppt, pps, ppsx, xml, pot
	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

File Type in Management	File Type	Family Type	Main Extension
	Unknown Ole Object (see note)	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
	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	Text ^	Text Files	txt
	Postscript File ^	Text Files	ps
	XML	Text Files	xml
	JSON	JavaScript Object Notation Files	json
	CSV	Comma-Separated Values Files	csv
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

File Type in Management	File Type	Family Type	Main Extension
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
	Media	AVI	Audio Video Interleave
DAT		Generic media	dat
MPEG		MPEG video	mpeg, mpg
WAV		Waveform Audio File Format	wav
WMV		Windows Media Video	wmv
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
WMA		Windows Media Audio	wma
MXF		Material Exchange File	mxf
Open Office	ODS	Calc Spreadsheet File	ods
	ODT	OpenOffice Document file	odt
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
AutoCAD	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 File	Express STEP Data Model Files	p21
	SFC File	Super Famicom Video Game Files	sfc
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	ACIS Solid Model File ^	CAD Files	sat

File Type in Management	File Type	Family Type	Main Extension
	Adobe Air ** ^	Adobe	air

File Type in Management	File Type	Family Type	Main Extension
	CD Audio Track Shortcut File ** ^	Media Files	cda
	CSS ^	CSS	css
	DB Files ^	Database Files	dbf, npa, dbt, wnd, tab, mdb
	Dicom File ^	Dicom Files	dcm
	Embedded Macro Files ^	Embedded File	bin
	Empty File ^	None	
	Equation Ole Object ^	OLE Object	bin
	Excel2, Excel3, Excel4, Excel5 ^	Office Files	xls
	HWP 3.0 File ^	Hancom Files	hwp
	INF File ^	INF Files	inf
	Initial Graphics Specification File ^	CAD Files	igs
	JAR ^	JAR Files	jar, jarxx
	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
	Material Exchange Format File ** ^	Media Files	mxf
	MHT File ^	MHT Files	mht
	MST files ** ^	Installer Setup File	mst
	p7s ^	Digital Signatures	p7s
	Parasolid model File ** ^	CAD Files	x_t, x_b
	Pcx File ^	CAD Files	pcx
	Pgp File ^	Encrypted Files	pgp
	PowerPoint95 File ^	Unsupported Files	ppt
	PreR14Dwg File ^	CAD Files	dwg
	PreWord97 File ^	Unsupported Files	doc
	PSD File ^	Photoshop Files	psd

File Type in Management	File Type	Family Type	Main Extension
	RPT ** ^	RPT Files	rpt
	RSP File ** ^	PLC Files	rsp
	Script ^	Batch Files	bat, js, php, cmd, vbs, reg, pl, lnk, py, asp, ps1
	Shortcut File ^	Shortcut Files	url
	Solution User Option File ** ^	Visual Studio Files	suo
	SQL File ** ^	SQL Files	sql
	Unrecognized ^	Any Binary Files	
	VCF ^	Exchange	vcf

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
 - ◆ Video - 10 GB
 - ◆ CSV - 2 GB
 - ◆ Raster images - 100 MB
 - ◆ Text - 2 GB
 - ◆ PDF - 700 MB
 - ◆ EML - 64 MB
 - ◆ ICS - 5 MB
 - ◆ Office - 50 MB
 - ◆ ExcelX - 1 GB
 - ◆ PowerPointX - 1 GB
 - ◆ WordX - 750 MB
 - ◆ Vector images - 10 MB

- ◆ Media - 10 GB
- ◆ XML and JSON - 100 MB
- AV scans are supported for file sizes up to 40 GB.

2 Using the Management Dashboard

The Management Dashboard enables you to perform the following procedures:

- [Monitoring Positive Selection Activity](#)
- [Exploring Incidents](#)
- [Configuring Settings](#)
- [Cloud Connectors and Integrations](#)
- [Password Protected Portal](#)
- [Generating Reports](#)

Note

Votiro Management Dashboard is supported using the Chrome browser only.

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

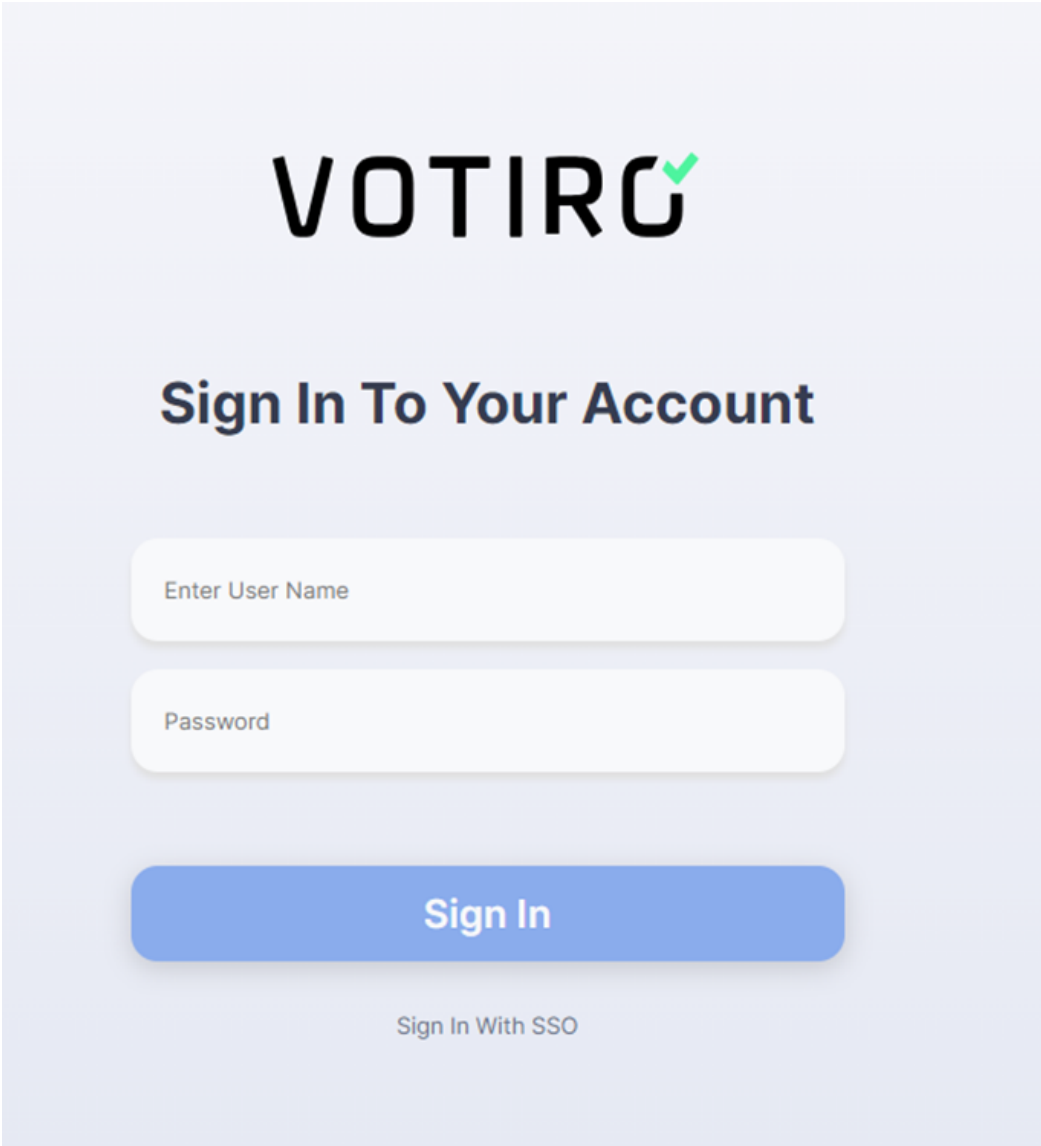
There are two ways the customer can sign in:

- 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 Sign in with Active Directory credentials

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

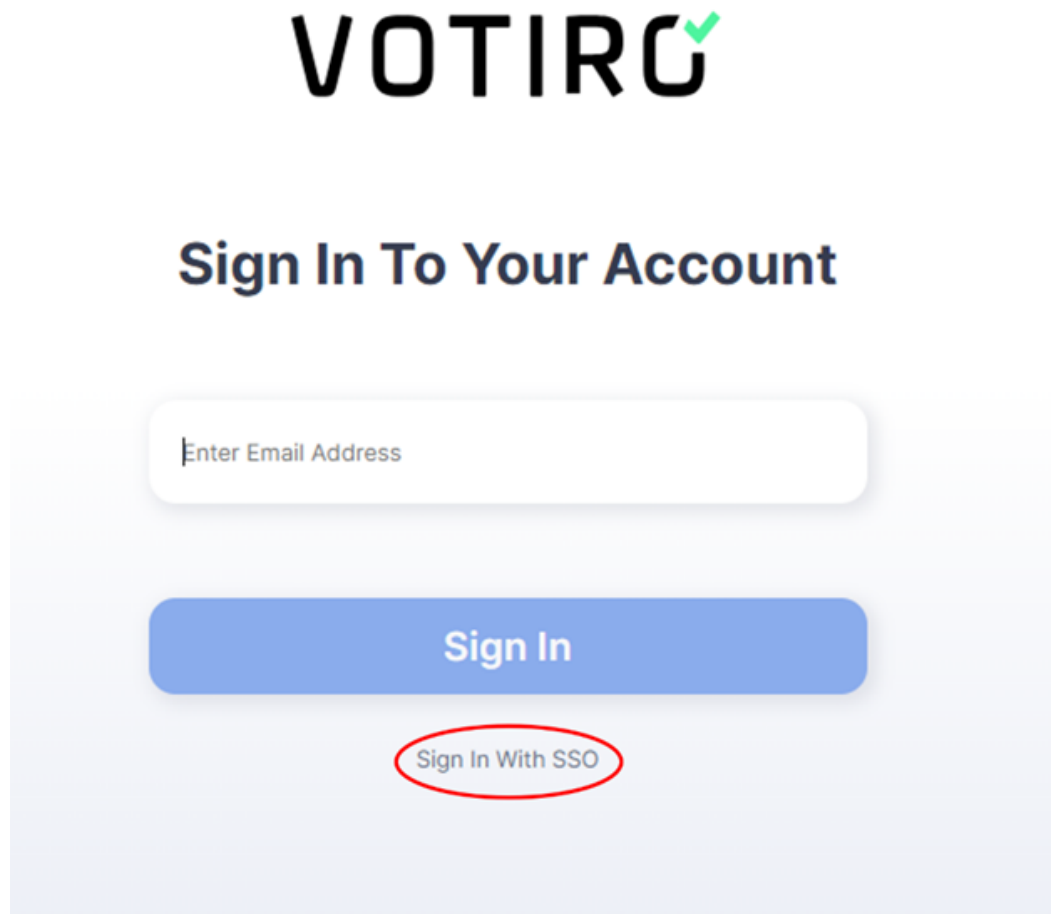
- User Name
- Password



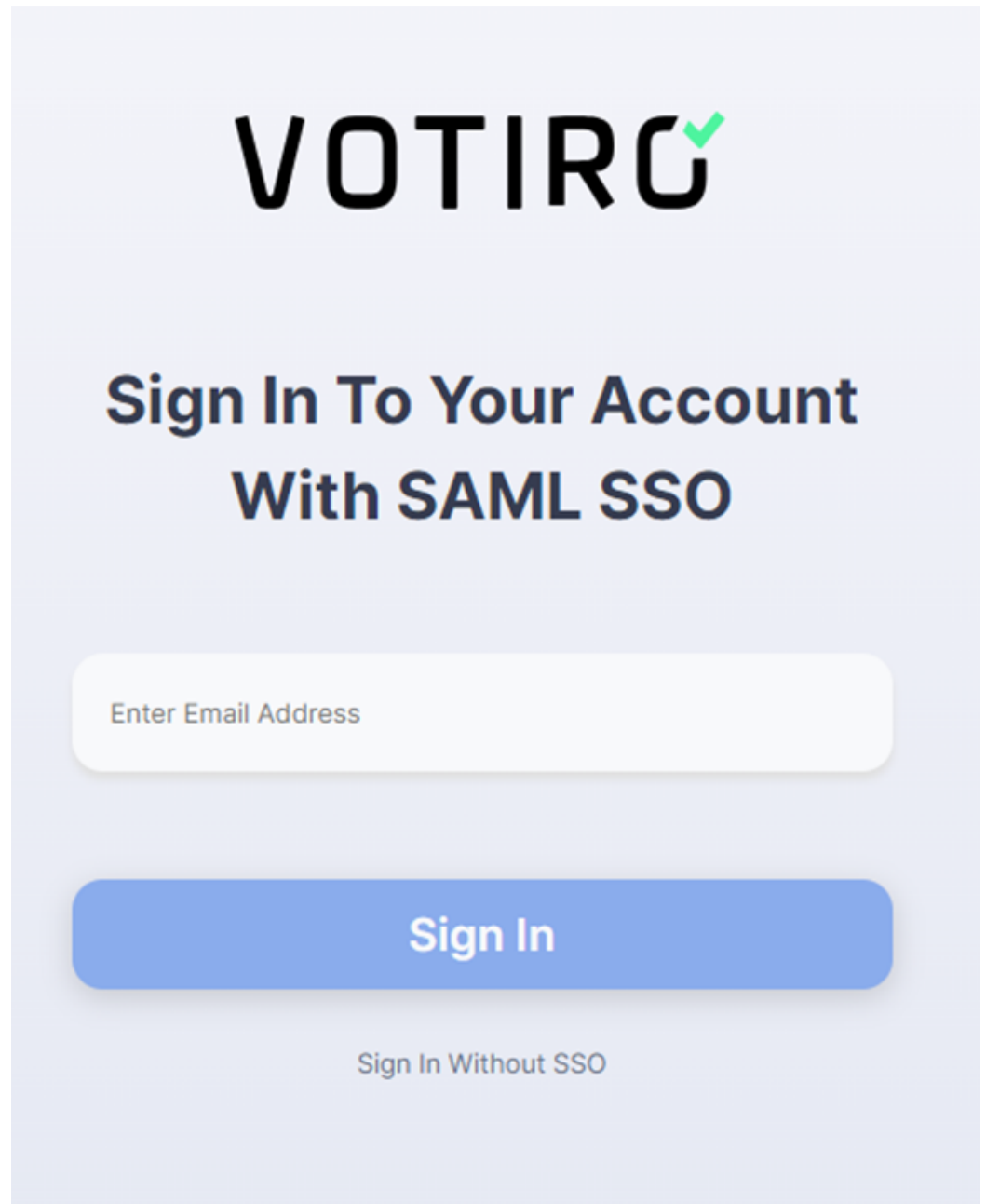
The image shows a sign-in form for VOTIRO. At the top is the VOTIRO logo. Below it is the heading "Sign In To Your Account". There are two input fields: "Enter User Name" and "Password". Below the fields is a blue "Sign In" button. At the bottom of the form is a link for "Sign In With SSO".

2.1.2 Sign in with SSO (using corporate credentials)

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



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



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

Note

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

2.2 Monitoring Positive Selection Activity

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

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

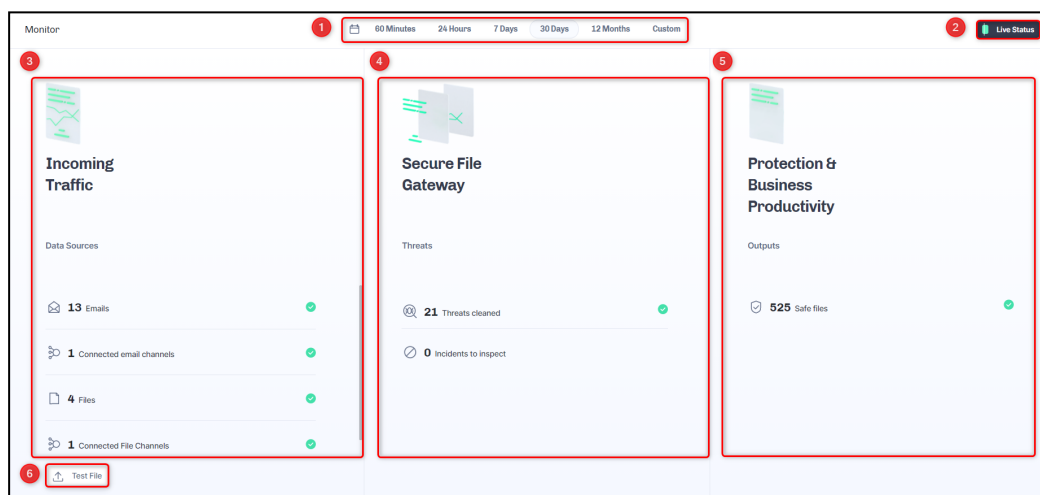
A file is processed for positive selection according to policies for the particular file type. Threats, determined by unknown elements, are detected regardless of policies, whether the file is blocked or not.

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

From the navigation pane on the left, click **Monitor**.

The process and page is divided into three main panes on your display depicting file processing activity as a file flows through the Positive Selection® Engine for the time period selected:

- Incoming Traffic
- Secure File Gateway
- Protection & Business Productivity

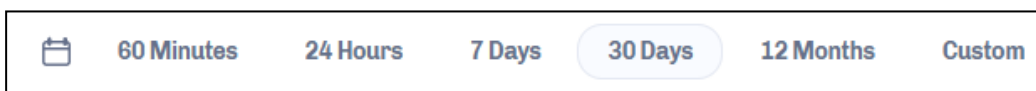


Element	Area	Description
1	Monitoring Periods	Select the time period you wish to display monitoring information for. See Monitoring Periods on the next page .
2	Live Status	Displays the most recent file traffic event activity flowing through Votiro Cloud. See Live Status on page 26 .
3	Incoming Traffic	Displays channel names and statistical details about files being processed for positive selection. See Incoming Traffic on page 27 .

Element	Area	Description
4	Secure File Gateway	Displays analysis of threats found and cleaned in files being processed for positive selection. See Secure File Gateway on page 28 .
5	Protection & Business Productivity	Displays performance details from a user's view, highlighting the positive business impact being experienced by using Votiro Cloud. See Protection & Business Productivity on page 29 .
6	Test File	Opens your File Manager and allows you to select a file for testing. See Test File on page 29 .

2.2.1 Monitoring Periods

The statistics displayed on the Monitor page relate to the period that is currently selected. You can select a predefined period by clicking its button or define a custom period.

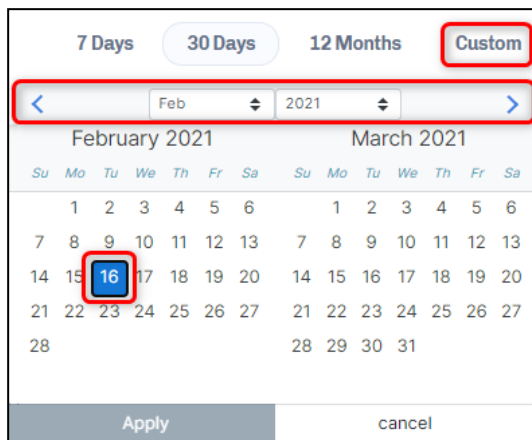


Votiro Cloud provides the following predefined settings:

Period of Processing Activity	Meaning
60 minutes	The information is for the period starting 60 minutes earlier until the current time.
24 hours	The information is for the period starting from the beginning of the current hour, 24 hours earlier, until the end of the current hour.
7 days	The information is for the seven days that end at 23:59 of the current day.
30 days	The information is for the period starting from the current date, one month earlier, until the end of the current day.
12 months	The information is for the period starting from the beginning of the current month, one year earlier, until the end of the current month.
Custom	Allows you to define the period to display information for by selecting From and To dates from a calendar selection tool.

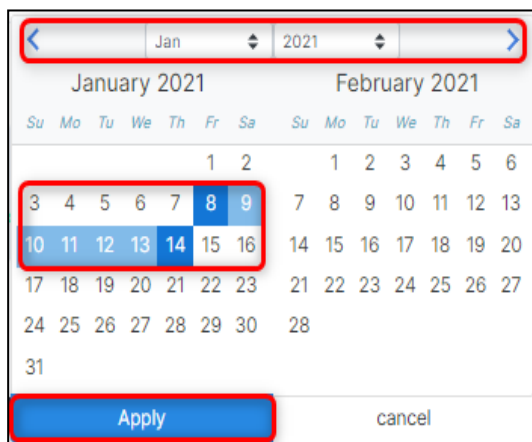
Defining a Custom Period

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



2. Navigate to the desired start month and year by clicking the right and left arrows, or by selecting a month and year using the up/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.



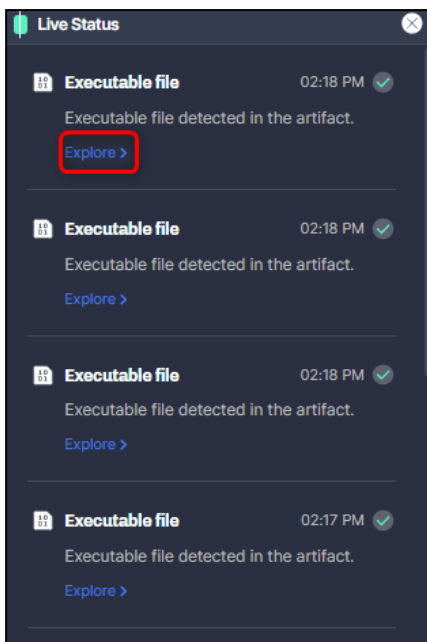
5. Click **Apply**.

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

Statistics update to show information for the custom period.

2.2.2 Live Status

Live Status displays the most recent file traffic events flowing through the Positive Selection® Engine.

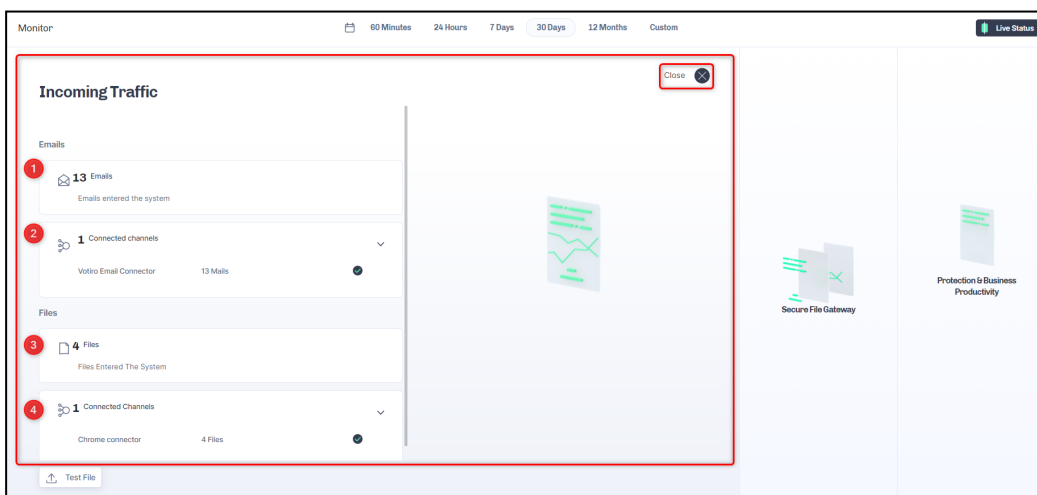


Click **Explore >** to view detailed information about the file, described in [Viewing Detailed File Information on page 31](#).

2.2.3 Incoming Traffic

The **Incoming Traffic** pane provides details of the active email and file channels connected to Votiro Cloud, and the traffic flowing in through these channels.

The channel name and statistical details of files coming into the system for positive selection displayed are for the time period selected, and highlighted at the top of the display.



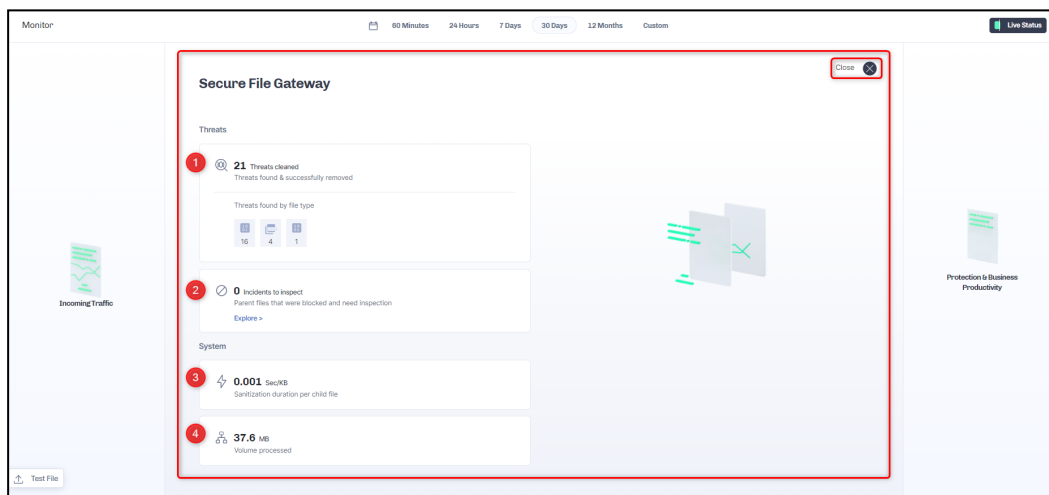
Element	Meaning	Description
1	Emails	The number of emails that entered Votiro Cloud for positive selection processing.

Element	Meaning	Description
2	Connected Channels (Email)	The number of active email channels, with details of the number of emails per named channel.
3	Files	The number of emails that entered Votiro Cloud for positive selection processing.
4	Connected Channels (Files)	The number of active file channels, with details of the number of files per named channel.

2.2.4 Secure File Gateway

The **Secure File Gateway** pane provides an insight into the effectiveness of the Positive Selection® Engine. It provides an analysis of threats found and removed from files being processed for positive selection, and the ability to inspect these threats.

System performance statistics are displayed, providing you with a snapshot view of sanitization speeds and volumes processed during the time period selected, and highlighted at the top of the display.



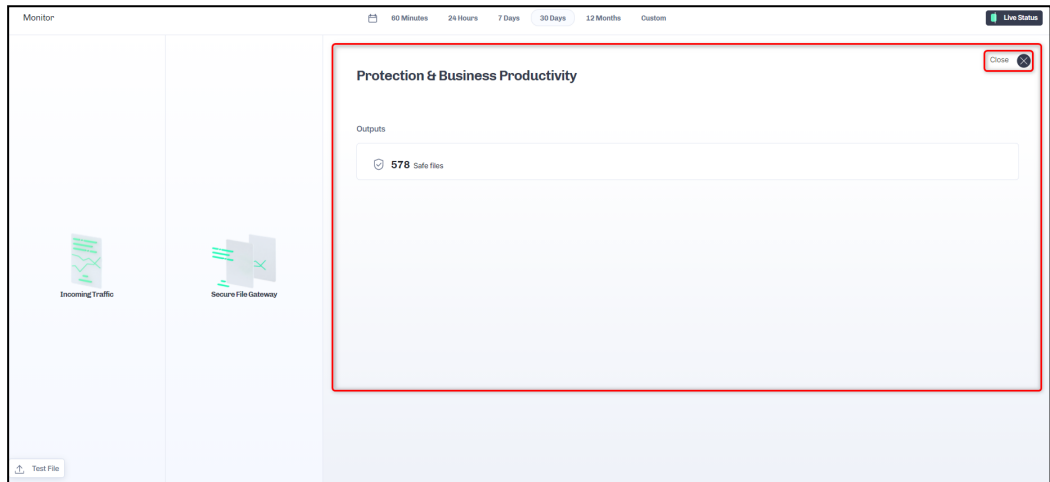
Element	Feature	Description
1	Threats Cleaned	The total number of threats found and successfully removed in the selected period is displayed. The number of threats found is divided and displayed by file type. To view details, tap a file type.
2	Incidents to Inspect	The total number of parent files that have been blocked and need inspection in the selected period is displayed. To view details, click Explore .
3	System Sanitization Speed	The system calculation of the average amount of time in Sec/KB it has taken in the period selected to sanitize a child file.
4	Volume Processed	The total accumulated consumption volume of items processed for positive selection.

Click the arrows to the right of each heading to expand and collapse the feature. Expand to display a breakdown by file type for the selected period.

2.2.5 Protection & Business Productivity

The **Protection & Business Productivity** pane provides performance details from a user's view, highlighting the positive business impact being experienced by using Votiro Cloud.

Outputs from the Positive Selection® Engine are detailed in this section.



Element	Meaning	Description
1	Safe Files	The number of safe files that have been processed for positive selection during the time period displayed.

2.2.6 Test File

To test a file 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.

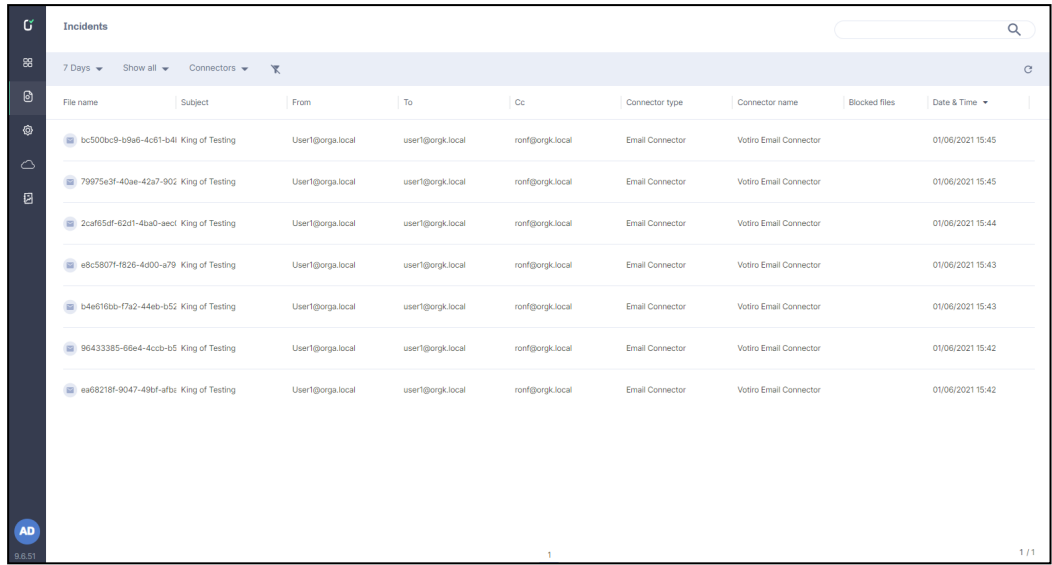
The file used for testing is stored and displayed as a regular file in Votiro Cloud. For further information, see [Viewing Detailed File Information on page 31](#).

2.3 Exploring Incidents

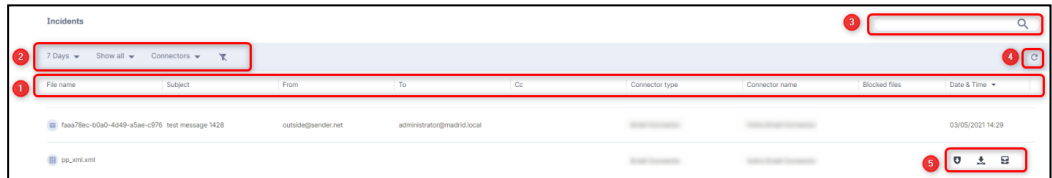
The Incidents page provides you with a deeper view of files that have been processed for positive selection and are currently stored on the server. By default the full list of incidents that have occurred during the last seven days is displayed.

From the Incidents page, you can download the original and processed files, as well as release files that have been blocked.

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



The page provides the following features:



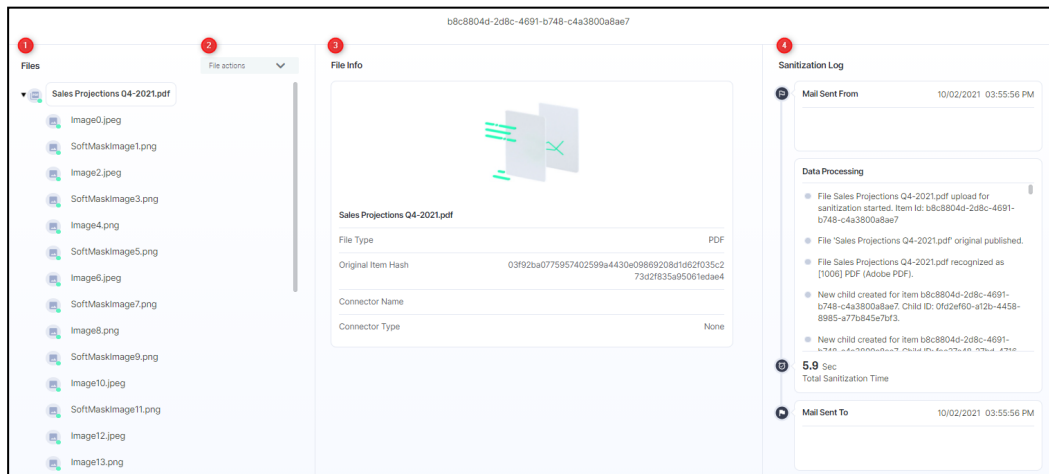
Element	Feature	Description
1	File Details	<p>Displays the file name and other information about the file. The column order can be re-arranged.</p> <p>For all file types, the following is provided:</p> <ul style="list-style-type: none"> File name Connector type Connector name Blocked files Date & Time <p>For email files (EML and TNEF formats), the following is also provided:</p> <ul style="list-style-type: none"> Subject From To Cc <p>For additional file information, tap in the file row.</p> <p>See Viewing Detailed File Information on the next page.</p>

Element	Feature	Description
2	Filter	The filter bar contains options for you to refine the list of files according to pre-defined criteria. You can also reset the filter. See Using Filters on the next page .
3	Search	The search bar allows you to enter part of the name of the file you would like to explore further. Perform a search on all the incidents in the blog. See Searching Positive Selection Requests on page 33 .
4	Refresh	Refresh the screen for recent files in the blog to be detailed on the page.
5	Perform Actions on Files	Select from the following three actions for the file selected: <ul style="list-style-type: none"> ■ Download original: the file as it was received, before being processed for positive selection. ■ Download sanitized: the processed version of the file, after being processed for positive selection. ■ Release original: the original file or email is released. For additional information on releasing files, see Releasing Files on page 34.

2.3.1 Viewing Detailed File Information

Detailed file information is displayed from:

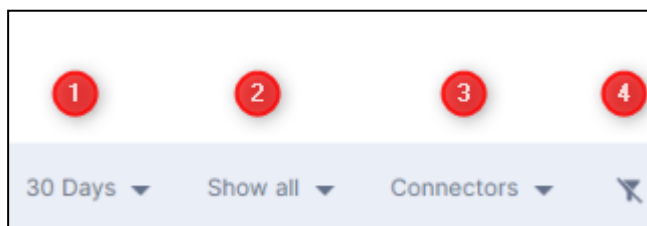
- The **Incidents** page, tap the row of the file to explore.
- The **Monitor** page's **Live Status** pane, click **Explore**.



Element	Description
1	<p>Files: Shows details of the file that you clicked in a previous window, in bold. The file is shown within the tree summary of its parents and children. The root is at the top. Scroll up or down in the pane; click the arrows to the left of the filenames to collapse and expand the nodes, as needed.</p> <p>A red dot indicates a blocked element, a green dot indicates a known element.</p>
2	<p>The File Actions list lets you perform the following actions for the file:</p> <ul style="list-style-type: none"> ■ Explore Incidents: return to the Incidents page. ■ Download original: the file as it was received, before being processed for positive selection. ■ Download sanitized: the processed version of the file, after being processed for positive selection. ■ Release original: the original file or email is released. For additional information see Releasing Files on page 34.
3	<p>File Info: Provides details about the file that is currently selected in the left pane.</p> <p>For all file types, the following details are provided:</p> <ul style="list-style-type: none"> ■ File Type ■ Original Item Hash ■ Connector Name ■ Connector Type
4	<p>Sanitization Log: Provides sanitization log events that relate to the file that is currently selected in the left pane:</p> <ul style="list-style-type: none"> ■ Mail Sent From: populated with details only when files are processed from an Email connector. ■ Data Processing, including Total Sanitization Time (in seconds). Use the scrolling bar on the right to see all child processing details. ■ Mail Sent To: populated with details only when files are processed from an Email connector.

2.3.2 Using Filters

You can filter the file list in the following ways:



Element	Filter	Description
1	Monitoring Period	Select an option from the Monitoring Period list to filter according to a specific time period. The default is 7 Days . Select Custom to define a range of dates. For instructions on how to define a custom period, see Defining a Custom Period on page 26 .
2	Show	Refines the list of files displayed, as follows: <ul style="list-style-type: none"> ■ Show all (default) ■ Show blocked items ■ Show sanitized items ■ Show root blocked items ■ Show retrospective detection items (for more information, see Retro Scan)
3	Connector	If you have more than one Votiro Cloud Connector installed, you can filter the file list by connector type using the Connector list.
4	Filter Icon	Clears filter and returns to default setting.

2.3.3 Retro Scan

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

Each file that enters your network is rescanned by Votiro Cloud every 3, 8 and 28 days against Anti-Virus engines. The Retro Scan capability can display whether Votiro Cloud 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 Cloud 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 Cloud blocked the potential real-time (Zero-day) attack when the Anti-Virus engine could not.

You can view all such incidents by selecting the **Show retrospective detection items** filter on the **Incidents** page.

2.3.4 Searching Positive Selection Requests

You can search all the positive selection requests that are shown in the **Incidents** page using the search bar. The incidents in the search results will be sorted based on their relevance to the search text.

You can search by the following details:

- File name
- From (email only)
- To (email only)

- Subject (email only)
- Item ID: Specify an item ID in GUID (globally unique identifier) format.

This feature is useful for releasing a specific blocked files (see [Releasing Files below](#)). For example, an email that contains a file you are expecting has been blocked by Votiro Cloud. As the recipient, you receive an email notification. The PDF file that is attached to the email message contains an item ID, such as the following:

```
24c5e7cf-b8f8-4f64-a945-39c1a157a896
```

Select the file and click for release or downloading.

2.3.5 Releasing Files

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

CAUTION!

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

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 Cloud for Web Downloads.

Note

To enable the release of blocked files, you must first configure Votiro Cloud for Web Downloads.

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

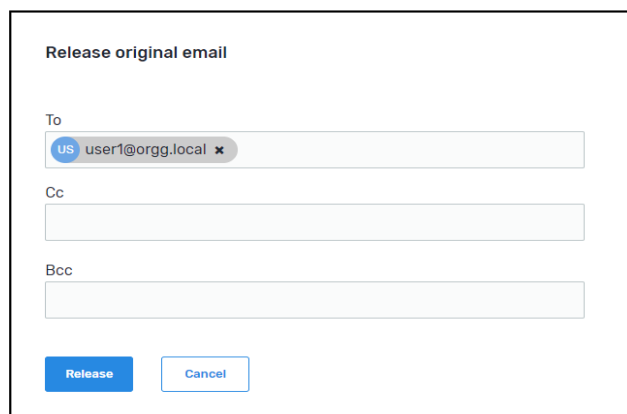
For more information, see [Configuring Settings on the next page](#).

- 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 box is titled "Release original email". It features three input fields for email addresses: "To", "Cc", and "Bcc". The "To" field is populated with "US user1@orgg.local" and has a small 'x' icon to its right. The "Cc" and "Bcc" fields are currently empty. At the bottom of the dialog, there are two buttons: a blue "Release" button and a white "Cancel" button with a blue border.

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.

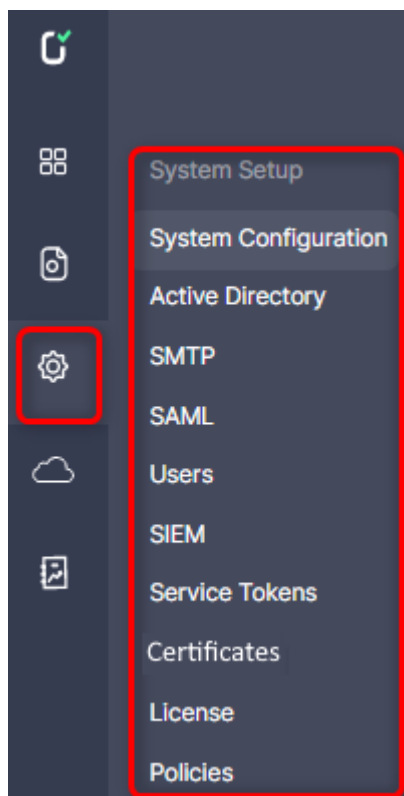
To Release Multiple Emails:

Date & Time	Status	Release status	Connectors	Bulk Release	Date & Time	File name	Subject	From	To	Cc	Connector type	Connector name	Blocked files
18/11/2021 10:43				<input checked="" type="checkbox"/>	796c5828-316-4a0a-b7d3-ee	King of Testing2	User1@borgk.local	king@borgk.local	user1@borgk.local		Email Connector	Votiro Email Connector	2
18/11/2021 10:16				<input type="checkbox"/>	MP protected .jsm						File Connector	Self-sanitization	1
18/11/2021 09:39				<input checked="" type="checkbox"/>	SMB.helic						File Connector	Self-sanitization	
18/11/2021 09:39				<input checked="" type="checkbox"/>	6d0921c-1c42-4d77-b396-fe1	King of Testing2	User1@borgk.local	king@borgk.local	user1@borgk.local		Email Connector	Votiro Email Connector	2
18/11/2021 09:24				<input type="checkbox"/>	Out of document macro+Reddy						File Connector	Self-sanitization	
17/11/2021 14:50				<input type="checkbox"/>	Suspicious macro.zip						File Connector	Self-sanitization	

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.

2.4 Configuring Settings

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



2.4.1 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

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.

1

Company Name * Name

Type in your company name Your company

2

File History * Days to keep

Select the number of days to keep files in storage 30

* Do not store files in storage

3

Password Protected File History * Days to keep

Select the number of days to keep password protected files in storage 180

* Do not store files in storage

4

Date Format Date

Select your preferred date format DD/MM/YYYY ✖

5

Time Format Time

Select your preferred time format HH:mm ✖

6

System Language Language

Select your preferred system language en ✖

7

System Locale Language

Select your preferred system locale en_US ✖

8

Enable Microsoft Information Protection (Mip) Enable MIP

Select whether to allow Microsoft Information Protected files into your organization

9

Enable Url Reputation Service Enable

Select whether to enable URL reputation capabilities

10

Blocked File Pdf Import ⋮

Customize organization blocked file PDF template by uploading your own template

11

Password Protected Blocked File Import ⋮

Customize organization Password Protected blocked file template by uploading your own template

The System Configuration page contains the following fields:

Element	Field	Description
0	Monitor Mode	<p>Monitor Mode is intended for potential customers to experience our product before purchase and has the following features:</p> <ul style="list-style-type: none"> ■ 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. <p>Monitor mode sanitizes files to gather file analytics, but the user always gets the "original" file.</p> <p>By default, Monitor Mode is disabled for editing. To enable this feature, please contact Votiro support.</p>
1	Company Name	<p>Specify the name of your organization. The company name appears in activity reports. see Generating Reports on page 116.</p>
2	File History	<p>Specify for how many days the system saves files. The default is 30 days.</p> <p>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. However, files above 50MB in size will be deleted 3 hours after the upload.</p>
3	Password Protected File History	<p>Specify for how many days the system saves password-protected files. The default is 180 days.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p>Note After the configured period, the original file is deleted and cannot be retrieved through the dashboard.</p> </div> <p>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 3 hours after the upload.</p>
4	Date Format	<p>Select your preferred date format for the display of information in the dashboard --either MM/DD/YYYY or DD/MM/YYYY.</p>
5	Time Format	<p>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).</p>

Element	Field	Description
6	System Language	<p>Select your preferred system language. To add languages to the list you must translate Dashboard dictionary and upload the translation.</p> <p>The default language is EN, English.</p>
7	System Locale	<p>Select your preferred system locale. This enables you to to sanitize archive files with ANSI encoding according to the selected System Locale.</p> <p>The available options are:</p> <ul style="list-style-type: none"> ■ 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) <p>The default locale is en_US.</p>
8	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.
9	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).
10	Blocked File PDF	Customize your organization's blocked file PDF template by uploading (importing) your own template.
11	Password Protected Blocked File	Customize your organization's Password Protected blocked file template by uploading (importing) your own 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.

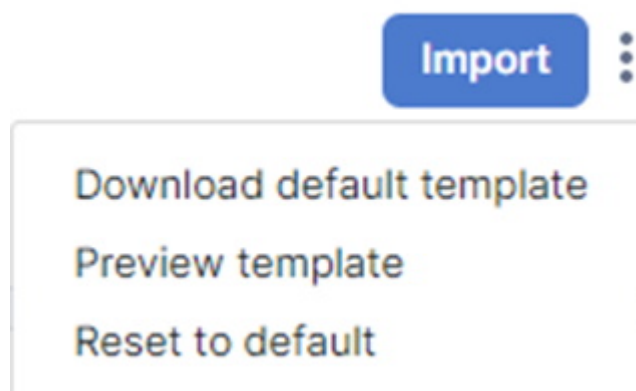
Customizing Blocked File Templates

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

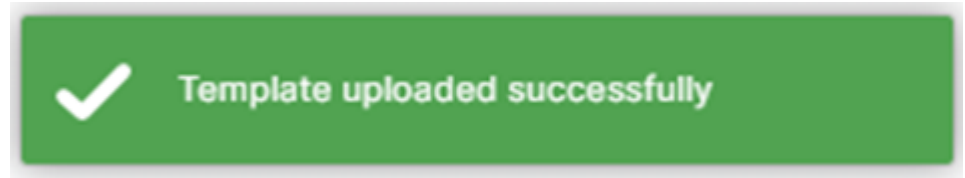
1. Download the default template by selecting **Download default template**.
2. Edit the downloaded template as desired.

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.

2.4.2 Active Directory

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

Settings

Active Directory

1 Active Directory Location * IP / Hostname

Type in your organization Active Directory address

2 Active Directory Server Port * Port

Type in your organization Active Directory server port

3 Active Directory User Group * Group Name

Type in your Active Directory user group

4 Active Directory Username * Username

Type in your Active Directory username

5 Active Directory User Password * Password

Type in your Active Directory user password

6 SSL Use SSL

Choose whether to use SSL

7 Test Connection

perform a connection test to the active directory server

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 Dashbord.

Element	Field	Description
4	Active Directory Username	<p>Specifies the login username for the Active Directory server.</p> <p>Select one of two formats to use:</p> <ul style="list-style-type: none"> ■ DOMAIN\UserName - For example, VT\Jane.Smith ■ UserName@FQDN - For example, Jane.Smith@Votiro.com <p>Key:</p> <p><i>DOMAIN</i> - the NetBIOS domain name</p> <p><i>UserName</i> - the login name of the user</p> <p><i>FQDN</i> - the domain name in full</p>
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.

2.4.3 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
```

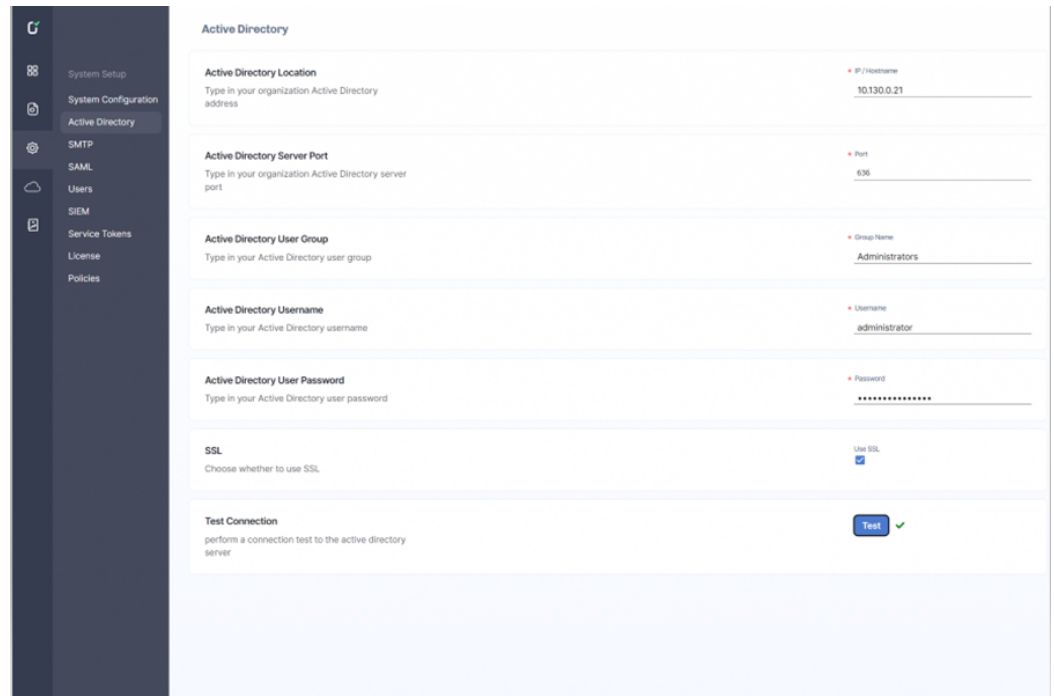
where `<CERT_PATH>` and `<CERT_NAME>` are replaced by the certificate path and certificate name.

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.

2.4.4 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 34](#).

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

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

Element	Field	Description
1	SMTP Server address	Specifies the SMTP server that relays notifications from the Platform Management to users in your organization.
2	SMTP Server port	Specifies the SMTP server port.
3	SMTP Server email	Specifies the email address of the SMTP server user.
4	SMTP Server password	Specifies the password for the SMTP server user.
5	Test Email	<p>To test the SMTP settings, click Test.</p> <ul style="list-style-type: none"> 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. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Test Email</p> <p>To check the SMTP connection send a test email, click Test.</p> <div style="float: right; text-align: right;"> <p>Test</p> <p>An email has been sent containing the following number</p> <p style="border: 1px solid gray; padding: 2px 10px;">3 5 1 8 4</p> </div> </div> <ul style="list-style-type: none"> If the settings are invalid, an error is displayed below the button.

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

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

2.4.5 SAML

Configuring SAML settings allows the Votiro Cloud 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 screenshot shows the SAML configuration page with the following fields and values:

- 1 IDP Metadata address** (URL): <https://votiro-ortichon.okta.com/app/exk>
- 2 Issuer** (name): Okta_SAML_Example
- 3 SAML Username identifier** (name): http://schemas.xmlsoap.org/ws/2005/05/
- 4 Admin role key** (key): Group
- 5 Admin role value** (value): VotiroAdmins
- 6 Help-Desk role key** (key): Group
- 7 Help-Desk role value** (value): VotiroHelpDesk
- 8 SOC role key** (key): Group
- 9 SOC role value** (value): VotiroSoc

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 role key for the administrator.
5	Admin role value	Specifies the role value for the administrator.
6	Help-Desk role key	Specifies the role key for the helpdesk.

Element	Field	Description
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.

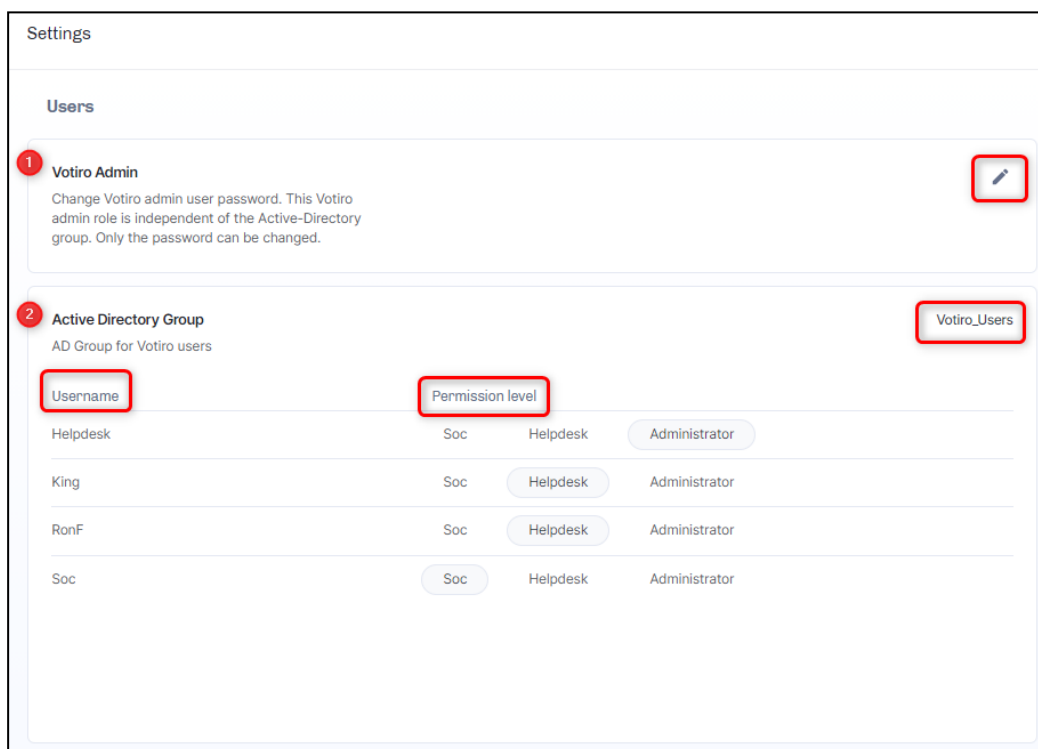
Note
Fields marked with a * red asterisk are mandatory, to be completed.

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.


2.4.6 Users


The 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 Users page, from the navigation pane on the left, click **Settings > Users**.



The Users page contains the following fields:

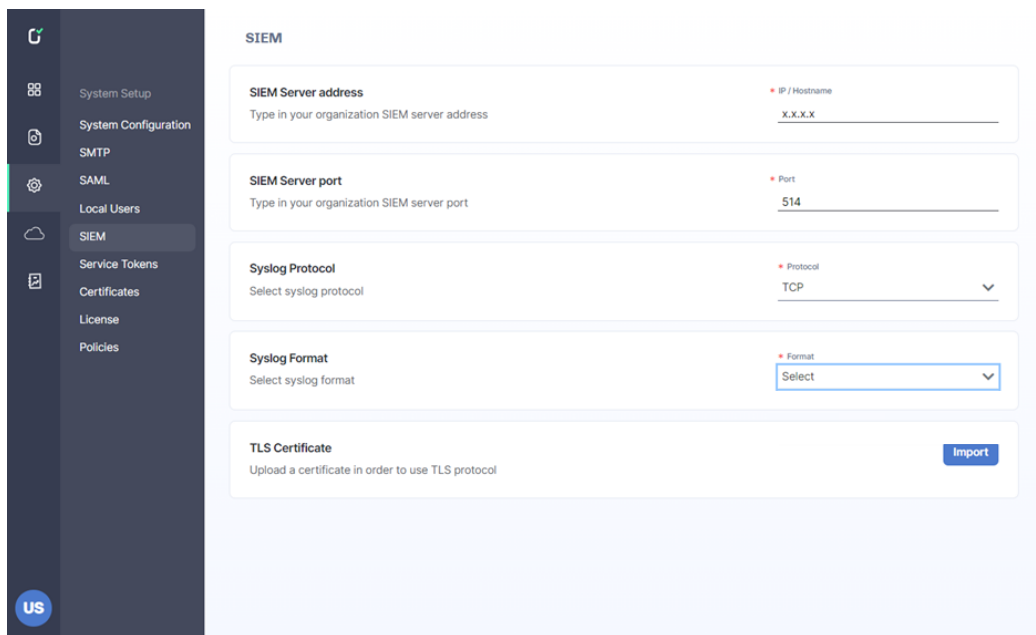
Element	Field	Description
1	Votiro Admin	<p>The Votiro Admin role provides direct administrative access to Votiro Cloud, independent of Active Directory.</p> <p>To change the Votiro Admin password:</p> <ol style="list-style-type: none"> 1 Click . 2 Enter the Current Password and then Confirm New Password. 3 Click Save, or Cancel. <div data-bbox="810 645 1114 994" style="border: 1px solid black; padding: 5px;"> <p>Change Password You will not be able to recover it</p> <p>Current Password</p> <hr/> <p>New Password</p> <hr/> <p>Confirm New Password</p> <hr/> <p>CANCEL SAVE</p> </div>

Element	Field	Description
2	Active Directory Group	<p>Users must be in the Votiro_Users Active Directory group.</p> <p>The three levels of permission are:</p> <ul style="list-style-type: none"> 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. 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. <p>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.</p>  <p>WARNING! The system must have a minimum of one Administrator user set up in the Active Directory Group for Votiro users. A warning message appears if you attempt to Save the settings with no user set with Administrator permissions.</p>

2.4.7 SIEM

You can configure SIEM setting for reporting syslog events to the SIEM platform.

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



The page contains the following configuration fields:

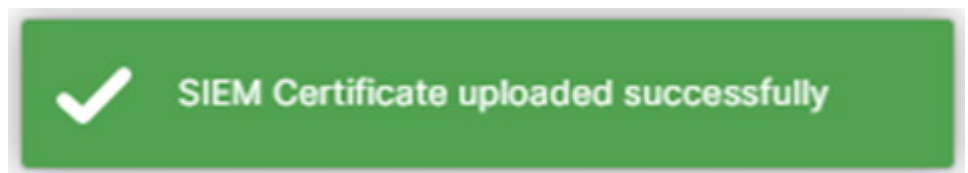
Element	Field	Description
1	SIEM Server address	Address of the SIEM system collector service. Specify a hostname where the address represents a fully qualified hostname or an IPv4 address. The default is empty. When the address is empty, the server uses its own IP as an address.
2	SIEM Server port	Specifies 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 129 .
3	Syslog Protocol	Specifies the Syslog message transport protocol. Select from UDP, TCP or TLS(SSL)
4	Syslog Format	Specifies the Syslog message format. Select from CEF or LEEF.
5	TLS Certificate	If the server mandates certificate authentication to use the TLS protocol, a TLS certificate file must be imported. After importing the certificate file, refresh the page. The certificate name and creation date are displayed. Note Only certificates in PEM (Privacy-Enhanced Mail) or PFX (Personal Information Exchange) formats are supported.

Note

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

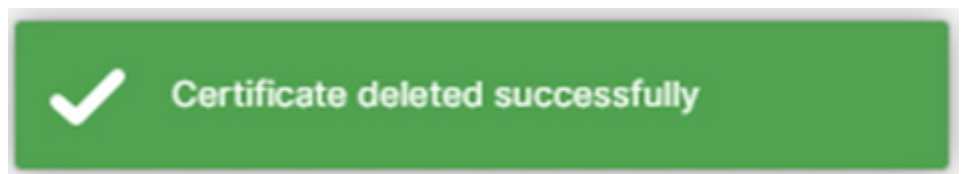
To import a TLS certificate:

- 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:

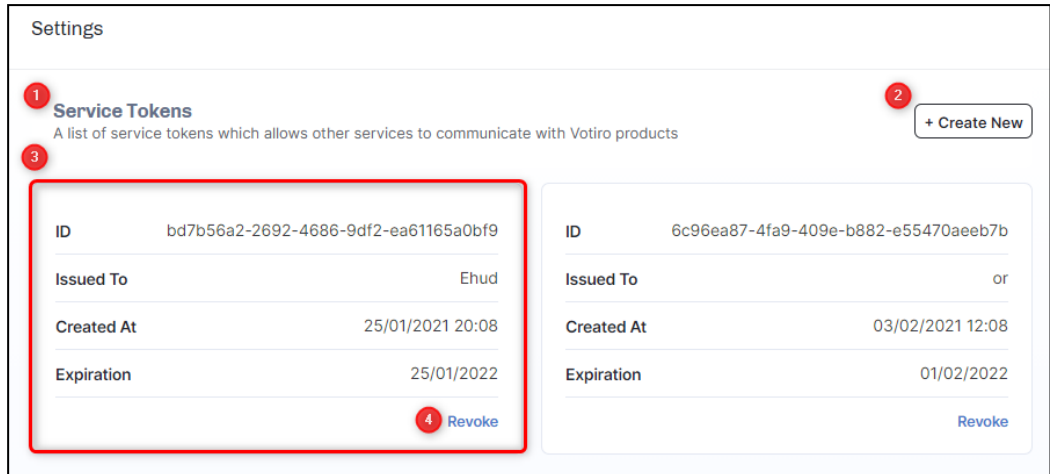


As you make changes the **Items Changed** count increases. When finished making changes at the bottom of the page select to either **Save Changes** or **Discard Changes** to the original settings.

2.4.8 Service Tokens

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

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 below .
3	Service Token	Details of the service token are displayed: <ul style="list-style-type: none"> ■ 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**.

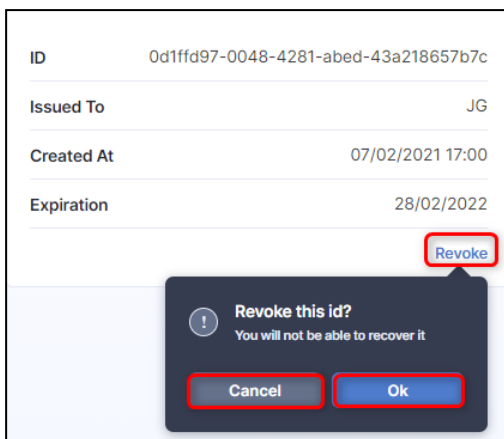
4. A service token is generated. You must copy this service token to the relevant bearer authentication headers.

IMPORTANT!
The service token generated is not stored by Votiro Cloud. 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, click **Revoke**. A confirmation pop appears warning that a revoked service token cannot be recovered.



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

2.4.9 Certificates

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

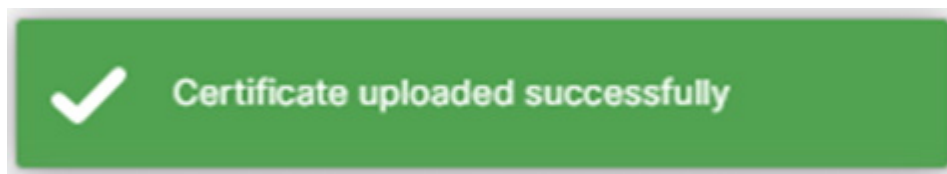
To get to the Certificates page from the navigation pane on the left, click **Settings > Certificates**.



Uploading a Certificate

To upload a new certificate:

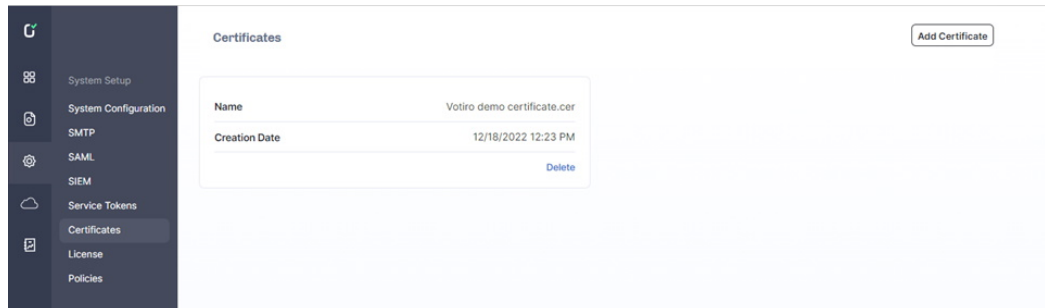
1. Click on the **Add Certificate** button.
2. An explorer window opens. There is an option to select multiple files.
3. Select the desired files to upload.
4. After a certificate file is uploaded successfully, the following message appears:



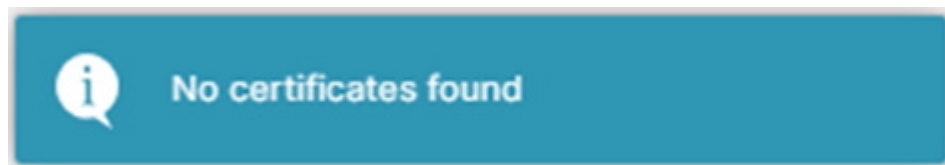
5. If the upload fails, the message **Failed to upload certificate** appears.

Viewing a Certificate

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



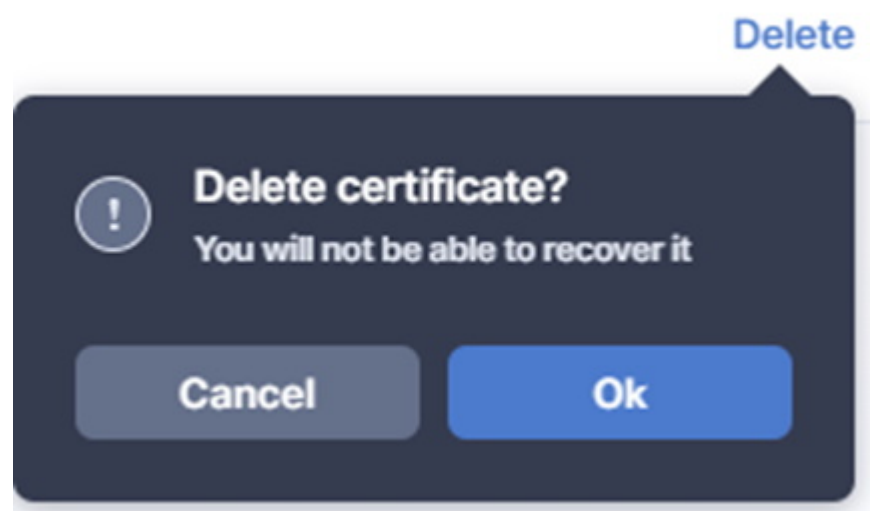
If there are no certificates, the following message appears:



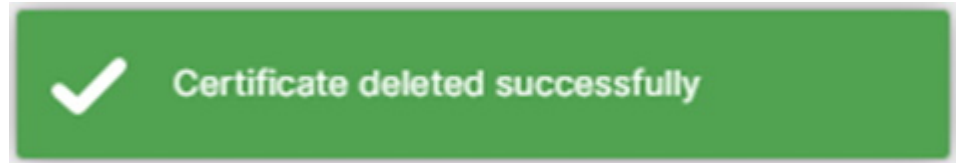
Removing a Certificate

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:

A screenshot of a web form titled "Define Exception" with the subtitle "Exception will be activated under the following conditions". The form contains two dropdown menus: "IF" with "Digital signature" selected, and "Select" with "is valid" selected. Below the "Select" dropdown are two radio button options: "is valid" (selected) and "is not valid". At the bottom right of the form are "Cancel" and "Save" buttons. The "Save" button is highlighted with a red border. A plus sign icon is visible in the bottom left corner of the form area.

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.

2.4.10 License

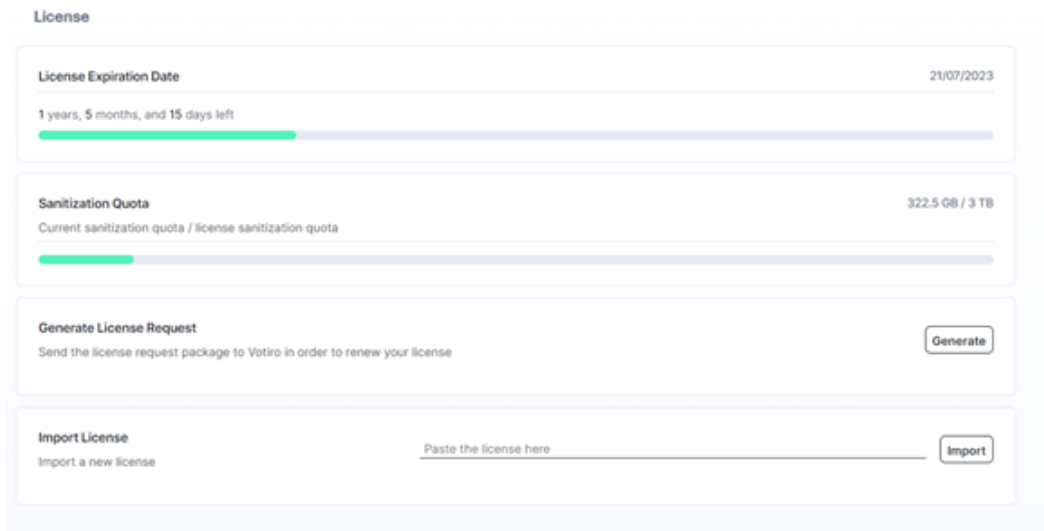
Use the License page to generate a license request, import a license key, know the date the license will expire and keep track of the file consumption against the quota.

Note

The license key issued includes information relating to your authority to use our Cloud Connectors.

To amend your license to include Cloud Connectors, contact Votiro's Support team.

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



The license page contains the following configuration fields:

Element	Field	Description
1	License Expiration Date	<p>When a valid license key is imported the expiration date automatically updates to the date when processing of files will stop.</p> <p>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.</p>
2	Sanitization Quota	<p>The first figure represents the current consumed size per file. The second figure represents the licensed size quota of files to be processed.</p> <p>See See Sanitization Quota (V9.6.3) for a more complete explanation.</p>
3	Generate License Request	<p>Click Generate to produce a license request package. The file licensePackage.zip is generated and located in your downloads folder.</p> <p>Pass this file to Votiro Support. A license key will be generated and returned to you within 24 hours of receipt of the request.</p>
4	Import License	<p>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.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note Votiro Cloud is activated up to five minutes after the license key import.</p> </div>

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.

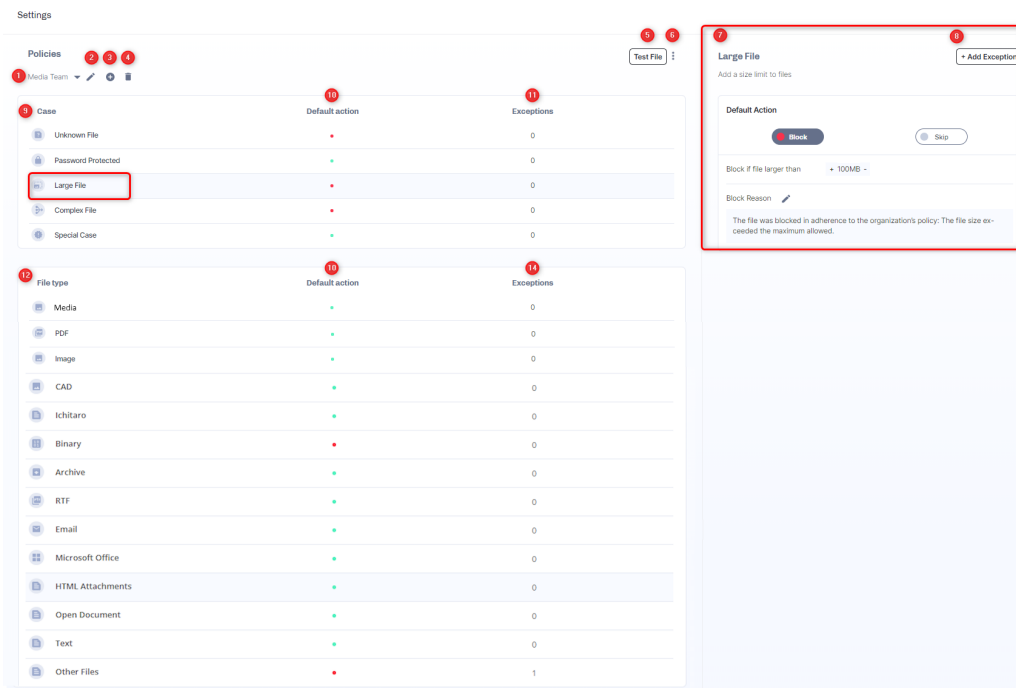
2.4.11 Policies

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

Policies Dashboard

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

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



Element	Meaning
1	The name of the currently displayed policy. To display a policy, select from the list of defined policies. You can set up policies for specific teams or individuals.
2	Edit the policy name.
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: <ul style="list-style-type: none"> ■ 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 Cloud reference clients, such as Votiro Cloud for Email or Votiro Cloud for Web Downloads.

Defining Policies

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

- **Case:** a policy using a file's characteristics, for example, password protected, size of file. For more information, see [Defining Policies by Case on page 133](#).
- **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 136](#).
- **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 141](#).
- **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 Cloud uses a default policy. Each case and file type has a different default policy.

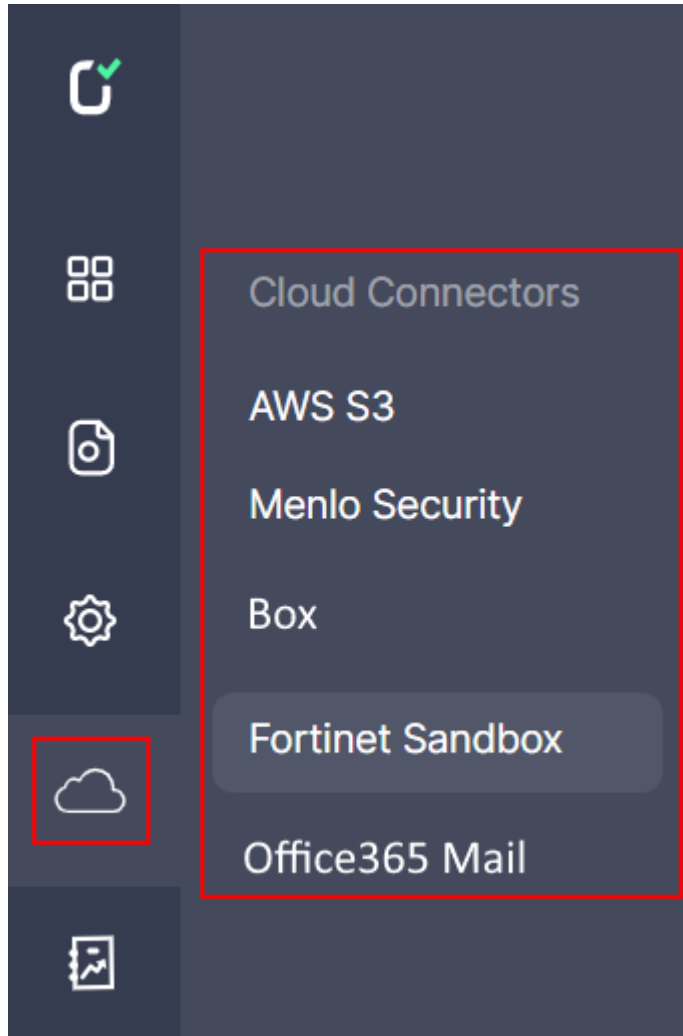
File Blocking

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.

2.5 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.



2.5.1 AWS S3 - VA On-premises

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

AWS S3

Policy Name * Name

Select a policy to work with the connector Default Policy ▼

Queue URL URL

Type in the AWS queue URL <https://sqs.us-west-1.amazonaws.com/5:>

Access key Key

Type in your AWS access key _____

Secret key Key

Type in your AWS secret key _____

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.

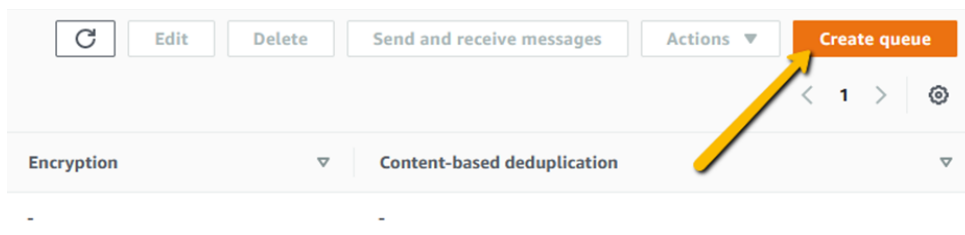
Prerequisites

- AWS SQS (Simple Queue Service) Queue (see [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

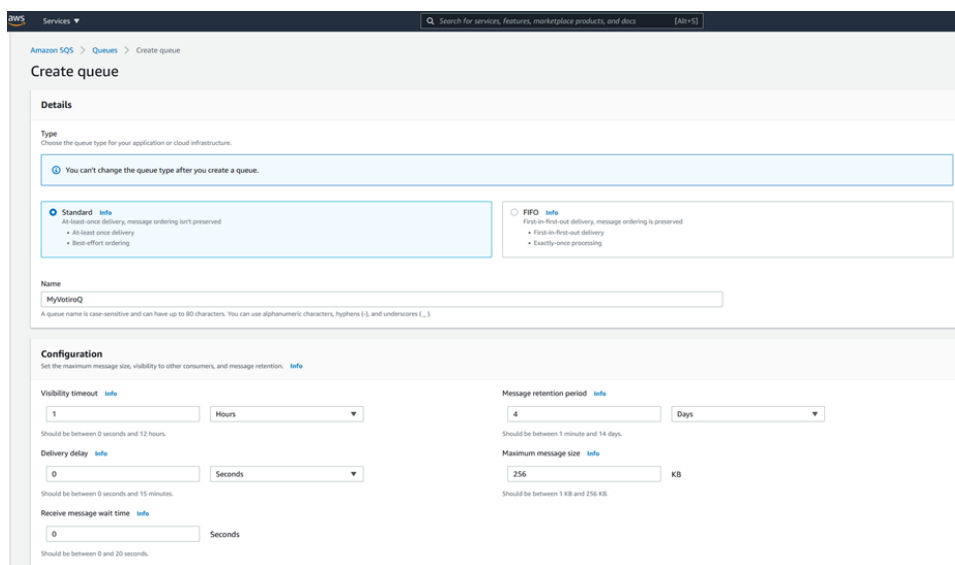
Creating an AWS SQS Queue

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": [
```


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:

Create event notification Info

The notification configuration identifies the events you want Amazon S3 to publish and the destinations where you want Amazon S3 to send the notifications. [Learn more](#)

General configuration

Event name

Event name can contain up to 255 characters.

Prefix - optional
Limit the notifications to objects with key starting with specified characters.

Suffix - optional
Limit the notifications to objects with key ending with specified characters.

Event types

Specify at least one type of event for which you want to receive notifications. [Learn more](#)

- All object create events**
s3:ObjectCreated:*
 - Put
s3:ObjectCreated:Put
 - Post
s3:ObjectCreated:Post
 - Copy
s3:ObjectCreated:Copy
 - Multipart upload completed
s3:ObjectCreated:CompleteMultipartUpload
- All object removal events**
s3:ObjectRemoved:*
 - Permanently deleted
s3:ObjectRemoved:Delete
 - Delete marker created
s3:ObjectRemoved:DeleteMarkerCreated
- Restore object events**
 - Restore initiated
s3:ObjectRestore:Post
 - Restore completed
s3:ObjectRestore:Completed

7. Under **Destination**, select **SQS queue**.
8. Under **Specify SQS queue**, select **Choose from your SQS queues**.

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

Destination

Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. [Learn more](#)

Destination
Choose a destination to publish the event. [Learn more](#)

- Lambda function
Run a Lambda function script based on S3 events.
- SNS topic
Send notifications to email, SMS, or an HTTP endpoint.
- SQS queue**
Send notifications to an SQS queue to be read by a server.

Specify SQS queue

- Choose from your SQS queues**
- Enter SQS queue ARN

SQS queue

Cancel **Save changes**

- 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>/*"
    }
  ]
}
```

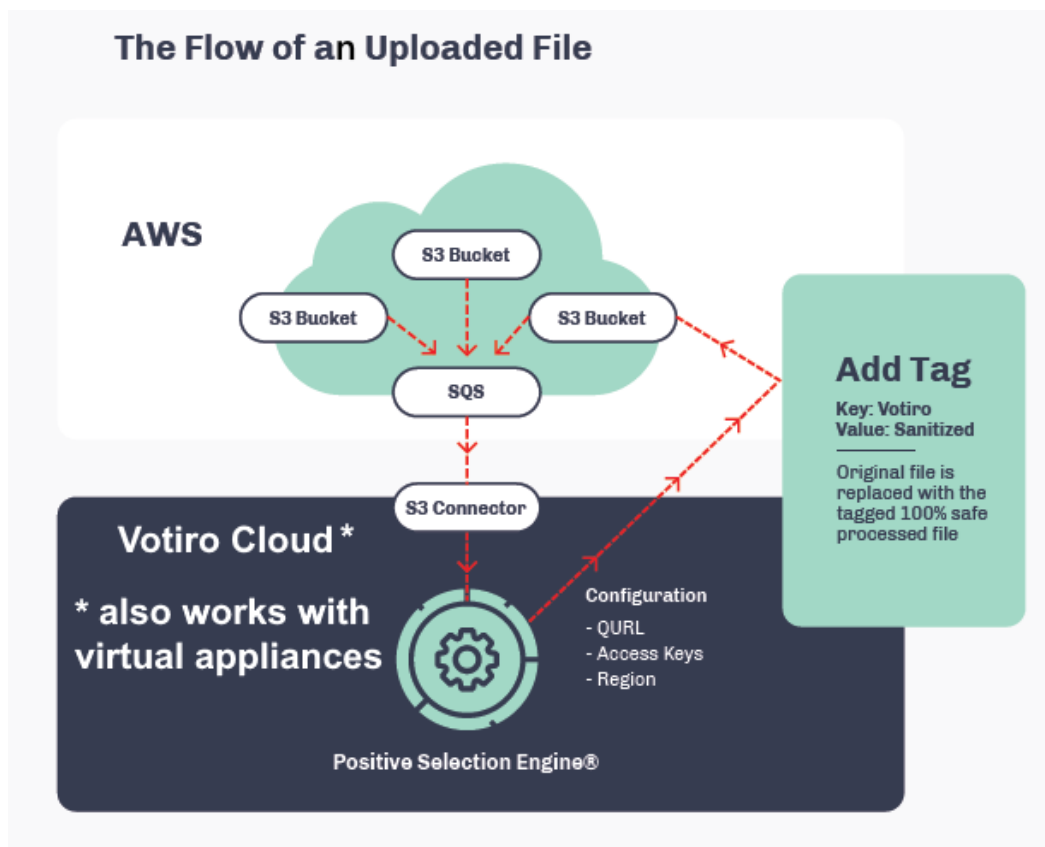
```

    "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

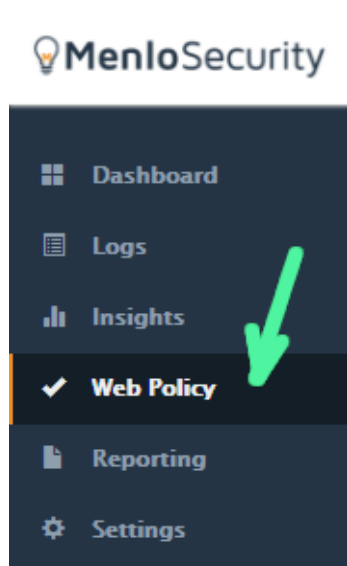
The following diagram illustrates the procedure:



2.5.2 Menlo Security

Configuration of the Cloud Connector to Menlo Security

1. Login to the Menlo Administrator page at <https://admin.menlosecurity.com>.
2. In the side pane, click on **Web Policy**.



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



4. On the **Menlo File REST API** row, click on the **Edit** button.

Service Name	Description	Enabled	
File Hash Check	Multi-Engine Hash Check for Virus	<input type="checkbox"/>	Edit
Full File Scan	Anti-Virus Scan	<input type="checkbox"/>	Edit
SandBox Inspection	Cloud-Based SandBox Inspection	<input type="checkbox"/>	Edit
WildFire Analysis	WildFire Malware Analysis	<input type="checkbox"/>	Edit
Menlo File REST API	Menlo File REST API Server Integration	<input checked="" type="checkbox"/>	Edit

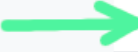
5. On the **Edit Menlo File REST API Integration** page, in the **Base URL** field enter the value supplied by Votiro: <https://my-sfg.customer.com/menlo>.

Edit Menlo File REST API Integration

MENLO FILE REST API SETTINGS

Plugin Name: Menlo File REST API

Plugin Description: Menlo File REST API Server Integration


Base URL: 

Certificate: -----BEGIN CERTIFICATE-----
MIIF3jCCA8agAwIBAgIQAf1tMPyjy1GoG7xkDjUDLTANBgkq
hkiG9w0BAQwFADCB
iDELMakGA1UEBhMCVVMxEzARBghNVBAgTCk51dyBKZXJzZXkx

6. Scroll down the page. Locate the **Authorization Header** field and enter the **tenantID** value that was provided by the Votiro support team.

Edit Menlo File REST API Integration

Type of Transfers: Downloads Uploads

Authorization Header: 

7. Click on the **Save Changes** button.
8. Once you have configured your browser to use the .pac file, you can start testing with Menlo Security.

Configuration of Menlo Security in Votiro

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

Menlo Security Isolation Platform

1 Policy Name: Select a policy to work with the connector. Name: Secondary Policy

2 Token Id: Type in your Menlo token ID. Id: _____

3 Channel Name: Type in your desired channel name. Name: _____

The Menlo Security page contains the following fields:

Element	Field	Description
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 Tenant ID, which can be obtained by contacting Votiro Support.
3	Channel Name	Specify the name of your channel. The channel name appears in the Incidents page as the name of a connector.

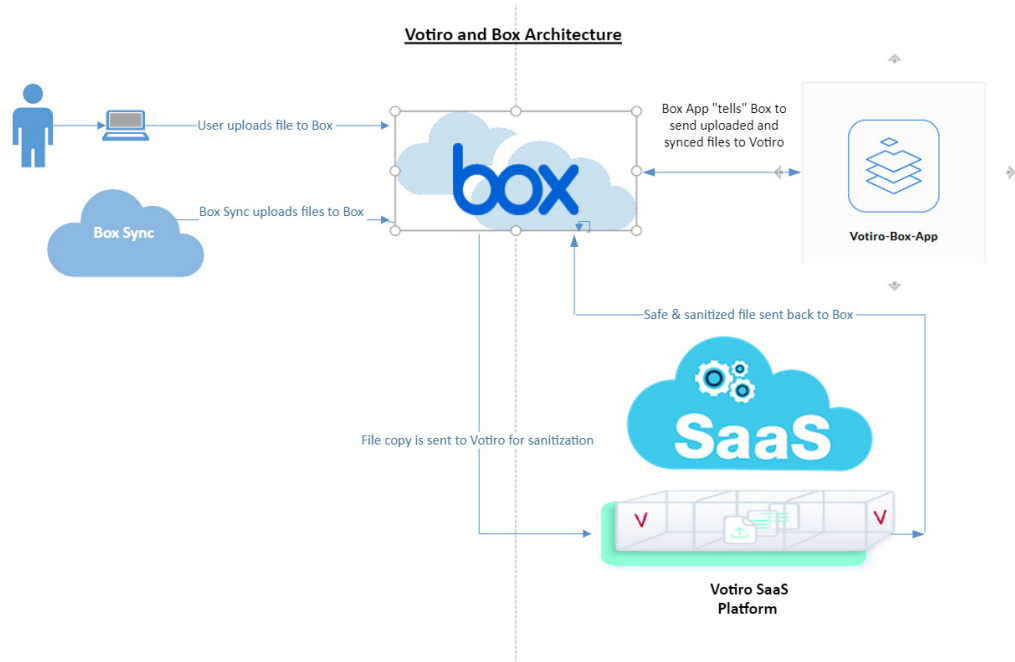
Note
Fields marked with a * red asterisk are mandatory, to be completed.

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.

2.5.3 Box

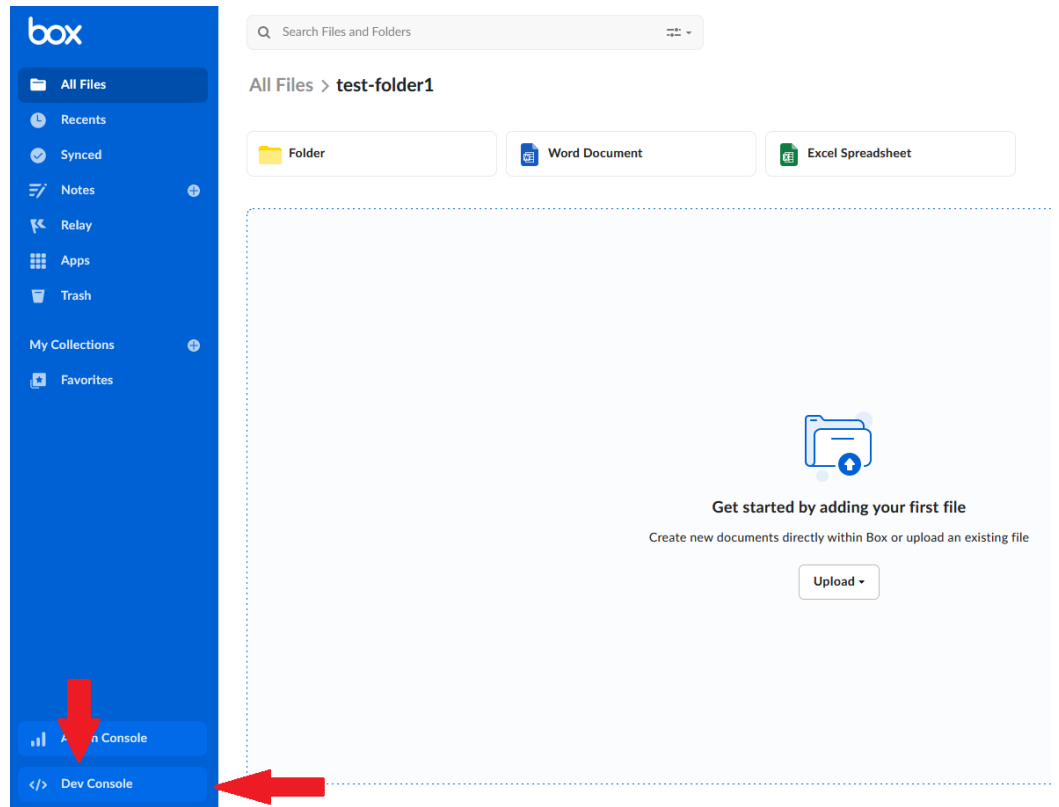
Votiro Cloud and Box

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

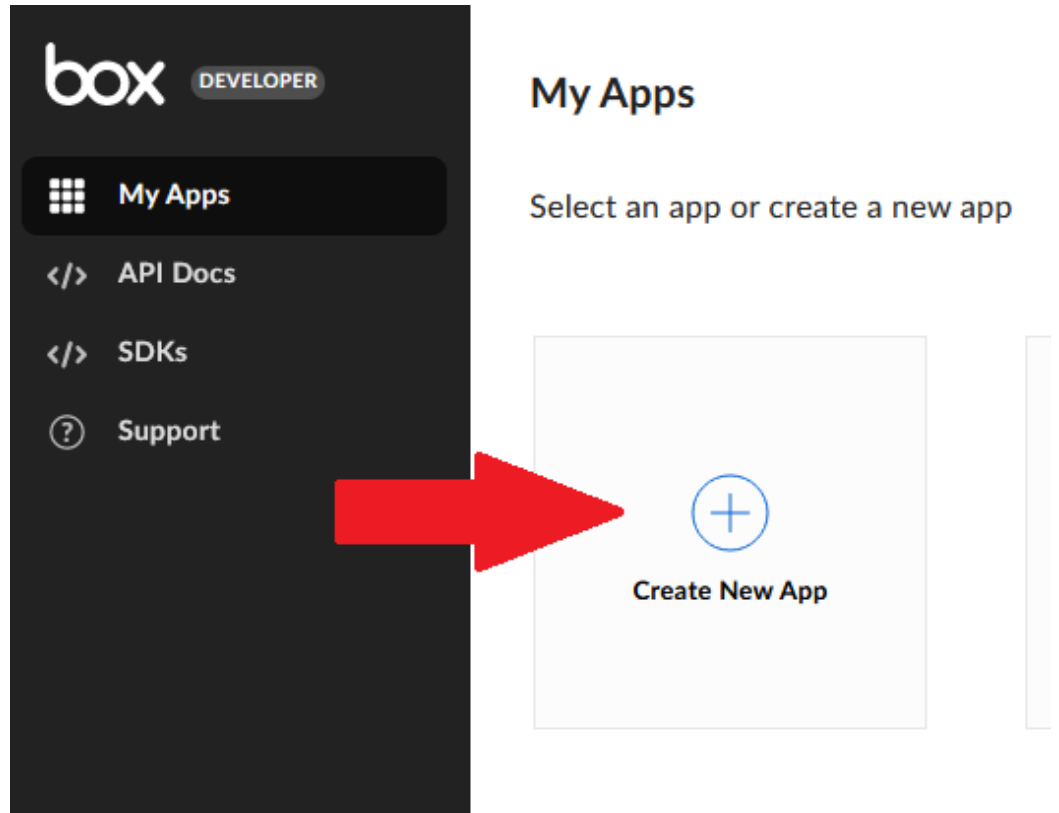


Configuration of an App in Box to Integrate with Votiro Cloud

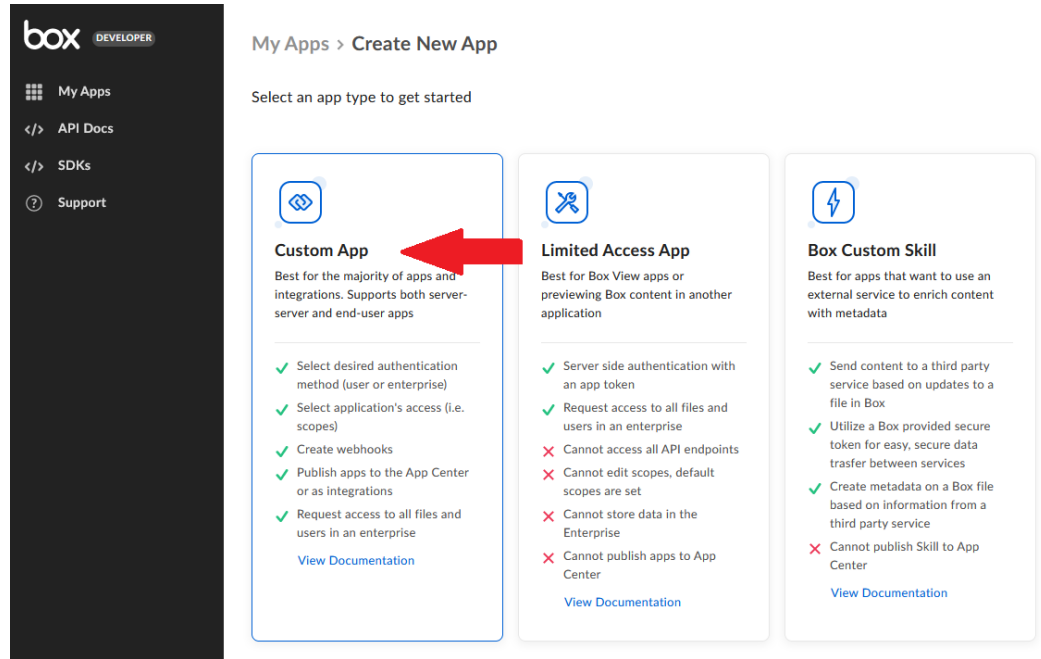
1. Login to your Box.com account with Admin privileges.
2. In the Box menu, select **Dev Console** (if you can't find the button go to [Dev Console](#)).



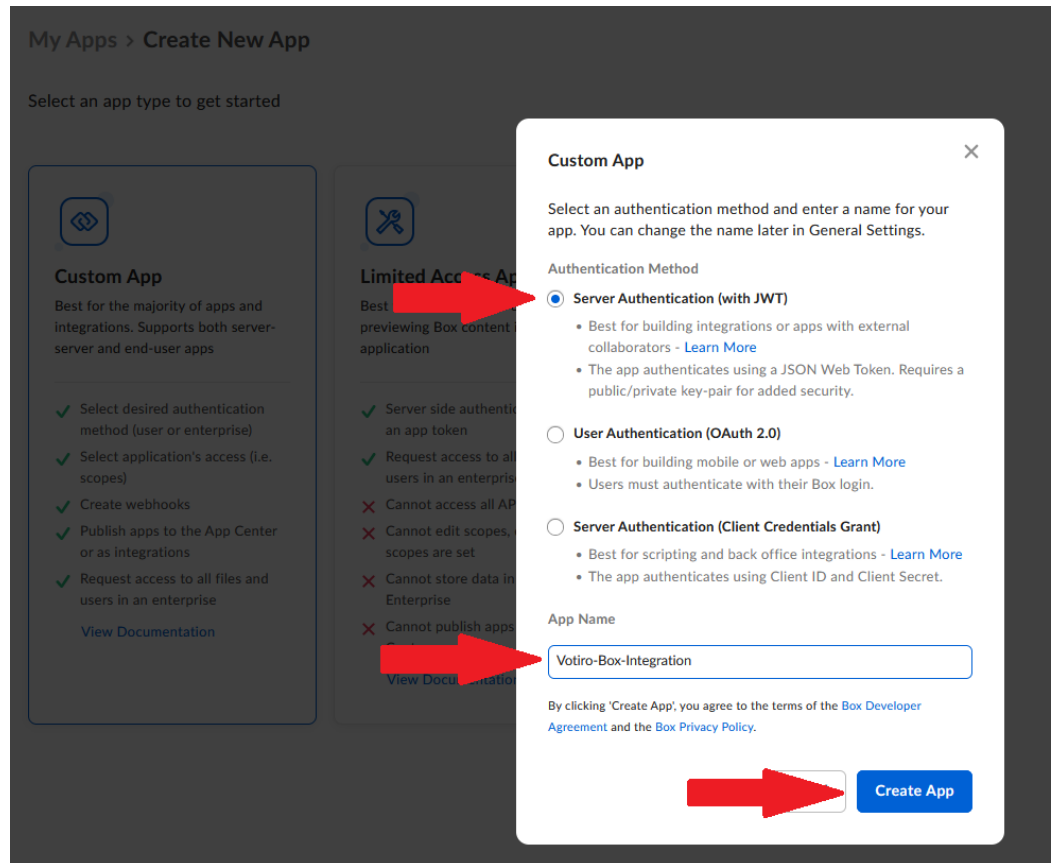
3. On the **My Apps** page, Click on the **Create New App** button:



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”:

Votiro-Box-Integration



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

App Access Level

The app access level determines which users and content your app may access. All Server-Server apps authenticate using an access token for the Service Account (Automation User) by default. [Read more about the Service Account.](#)

App Access

- ✓ Service Account and App Users only. [Learn more.](#)
- ✓ Access to content created by your app.
- ✗ Cannot manage Enterprise settings, content, or users.

App + Enterprise Access

- ✓ All users
- ✓ Manage Enterprise settings, content, and users.
- ✗ Limited access to External Unmanaged Users.

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

Application Scopes

The app scopes determine which endpoints and resources your app can successfully call. [Learn more about all of our scopes.](#)

Content Actions

- Read all files and folders stored in Box
Access to content is further restricted by the users' permission and Access Token used.
- Write all files and folders stored in Box
Necessary to download files and folders. Access to content is further restricted by the users' permission and Access Token used. Read access is required when Write access is selected.
- Manage signature requests
Interact with Box Sign endpoints. [Learn more about Box Sign APIs.](#)

Administrative Actions

- Manage users
- Manage groups
- Manage retention policies
For use with the [Governance add-on.](#)
- Manage enterprise properties
For use with the event stream, enterprise's attributes, and device pins. App + Enterprise Access is required to use this scope.

Developer Actions

- Manage webhooks
- Enable integrations
- Manage Box Relay
Interact with Box Relay endpoints. [Learn more about Box Relay APIs.](#)

Advanced Features

Choose which advanced features your application requires. Warning: These should only be used for server-side development. [Learn more.](#)

- Make API calls using the as-user header
- Generate user access tokens
Allows your application to generate another users' access tokens using a grant instead of requiring their credentials

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

Votiro-Box-Integration ⋮

General Settings **Configuration** Webhooks Authorization App Diagnostics

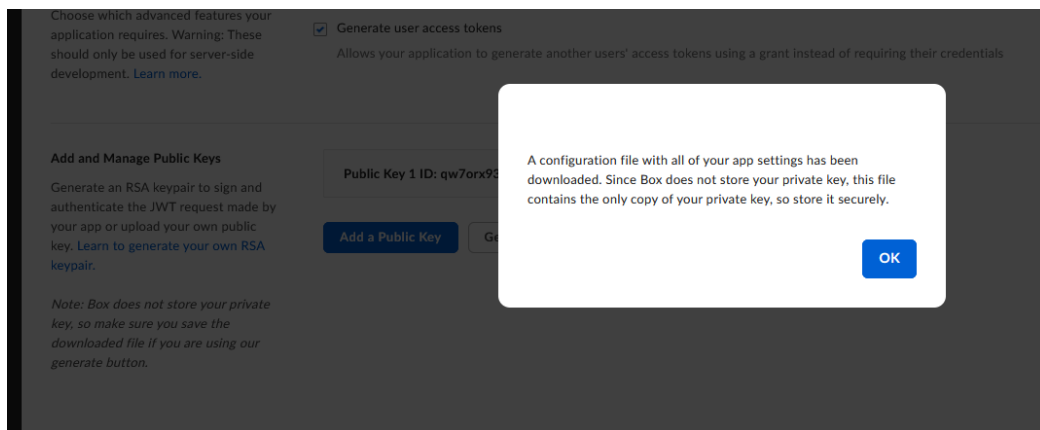
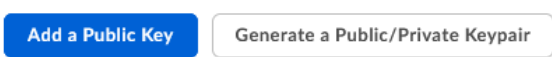
Manage authentication methods and app permissions Save Changes

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:

Add and Manage Public Keys

Generate an RSA keypair to sign and authenticate the JWT request made by your app or upload your own public key. [Learn to generate your own RSA keypair.](#)

Note: Box does not store your private key, so make sure you save the downloaded file if you are using our generate button.



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

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

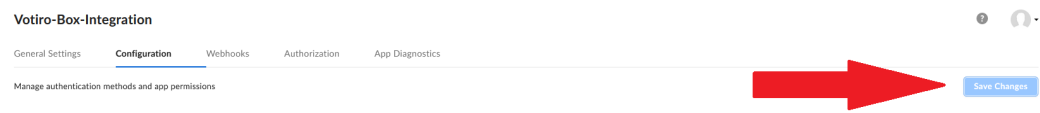
CORS Domains

Comma-separated list of Origins allowed to make a CORS request to the API. For security purposes, enter only those used by your application. Avoid the use of trailing slashes in the URL unless specifically required. [Learn more.](#)

Allowed Origins (optional)

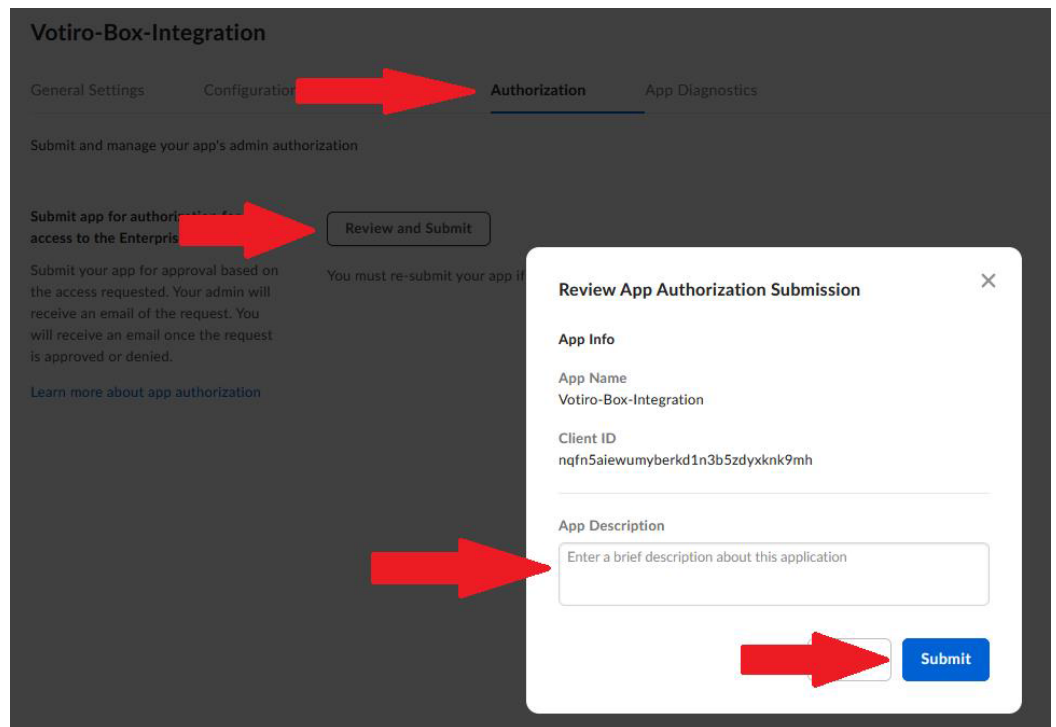
https://{ClusterFQDN}.paralus.votiro.com

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

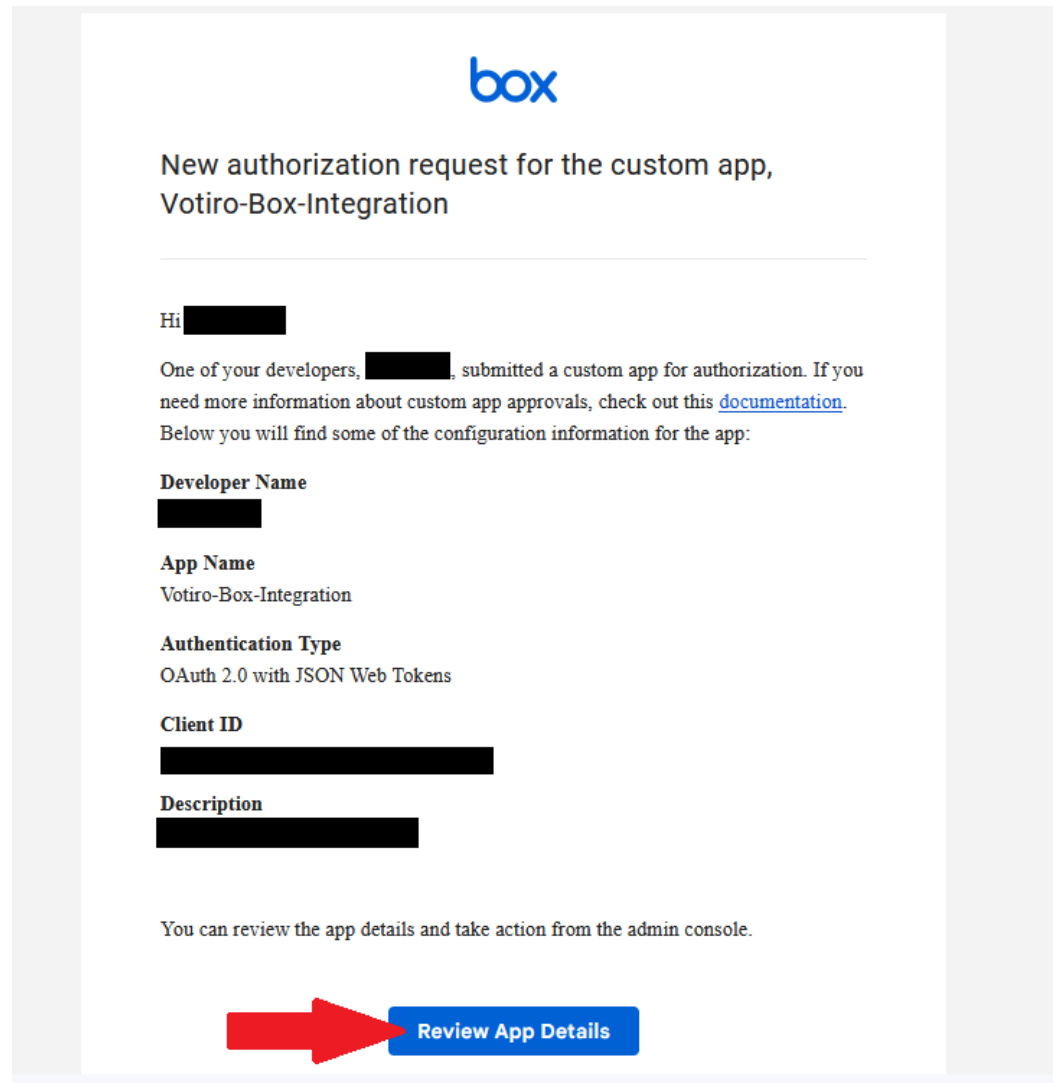


13. Select the **Authorization** tab and:
 - a. Click on **Review and Submit.**
 - b. Type an **App Description**

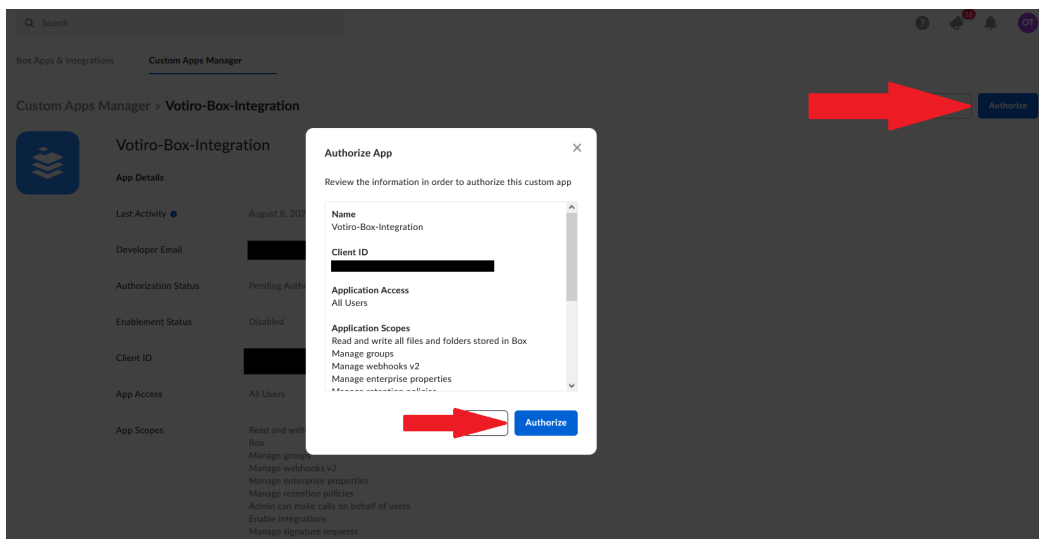
c. Click on the **Submit** button:



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



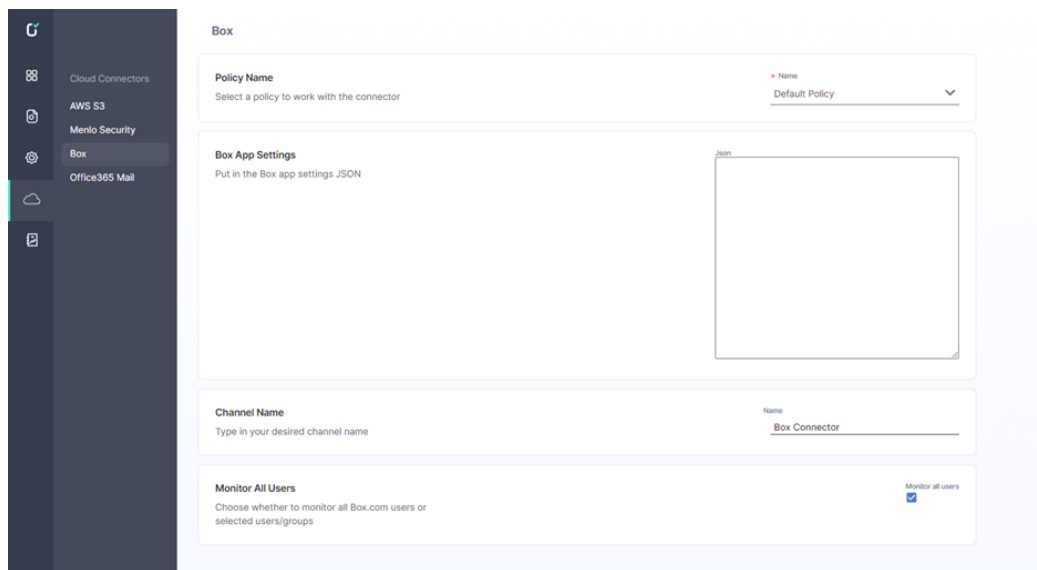
15. You'll get redirected to **Box.com** again.
 - a. Go to the **Custom Apps Manager** and select your new app.
 - b. Click **Authorize** and review your app settings.
 - c. Click on the **Authorize** button:



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

Configuration of the Box App in the Votiro Cloud 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 Cloud. 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:

Monitor All Users Monitor all users

Choose whether to monitor all Box.com users or selected users/groups

Monitored Users

Move users to monitor to the right column

Add ▶
◀ Remove

itamar

Itamar2

Yaara Pinhas

All
None
All
None

Monitored Groups

Move groups to monitor to the right column

Add ▶
◀ Remove

supergroup

All
None
All
None

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:

✔ "Meeting summary 6-12.docx" was uploaded successfully.

Share

✕

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:

✔ A new version of "Meeting summary 6-12.docx" was just uploaded. Would you like to refresh the page?

Refresh

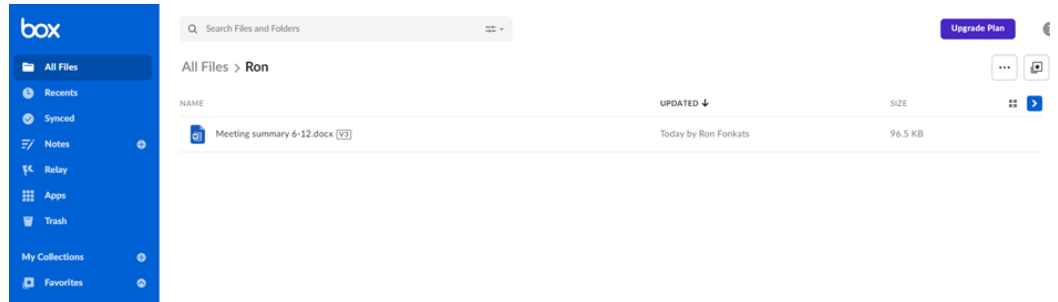
✕

Box App Behavior when Versioning Files

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

Votiro CyberSec Ltd. Proprietary

Page 80



< Version History

Today

v3

Current Version

Uploaded by Ron Fonkats

Today at 3:23 PM • 3.7 MB

...

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

 VA-ClosingFWports-v1.0.sh_Blocked.pdf  Today by Ron Fonkats 36.6 KB

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



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

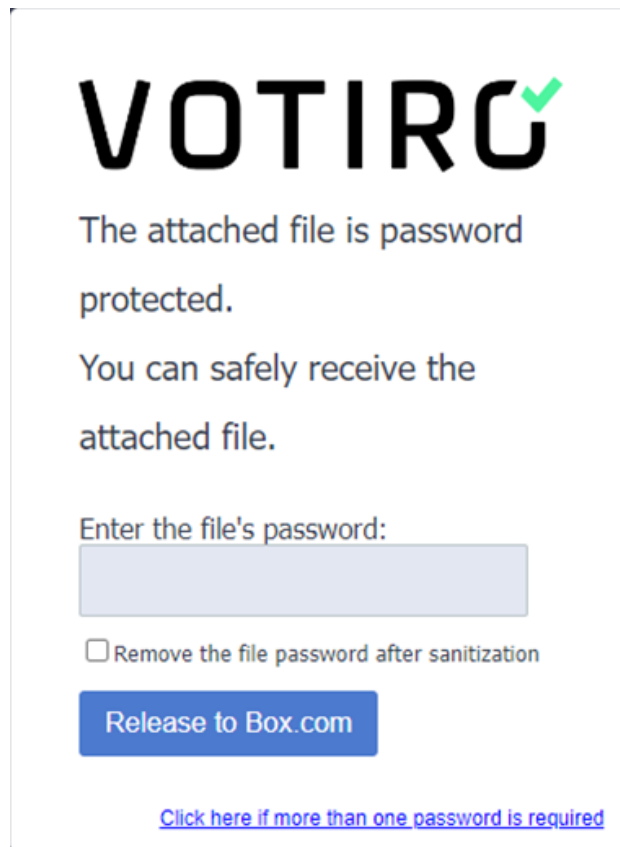
Box App Behavior for Password Protected Files

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

 Password1.xlsx_Blocked.pdf  Today by Ron Fonkats 38.2 KB   Share

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:



The screenshot shows a web interface for VOTIRO. At the top is the VOTIRO logo. Below it, the text reads: "The attached file is password protected. You can safely receive the attached file." There is a text input field labeled "Enter the file's password:". Below the input field is a checkbox labeled "Remove the file password after sanitization". A blue button labeled "Release to Box.com" is positioned below the checkbox. At the bottom of the form, there is a blue hyperlink that says "Click here if more than one password is required".

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



The sanitized file has been
released to your Box account.

The sanitized file appears in Box marked by V3:

 Password1.xlsx [V3]

Today by Ron Fonkats

58 KB

2.5.4 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**.

Sandbox

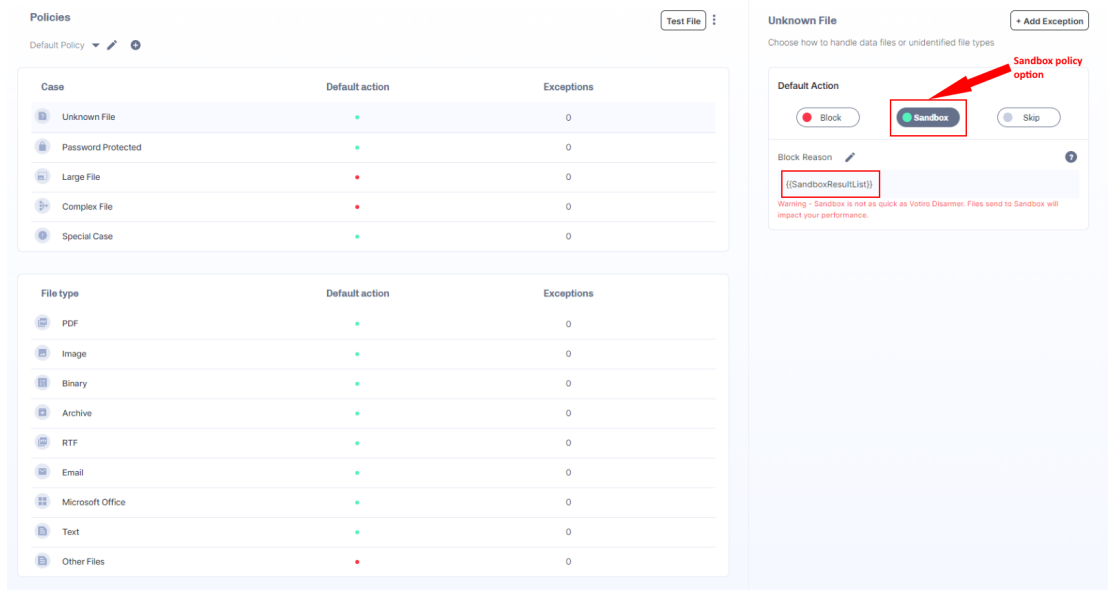
Fortinet sandbox Server Address Type in your organization Fortinet sandbox server address	IP / Hostname _____
Fortinet sandbox Username Type in your Fortinet sandbox username	Username _____
Fortinet Sandbox Password Type in your Fortinet sandbox password	Password _____
Test Connection perform a connection test to the sandbox server	<input type="button" value="Test"/>

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.



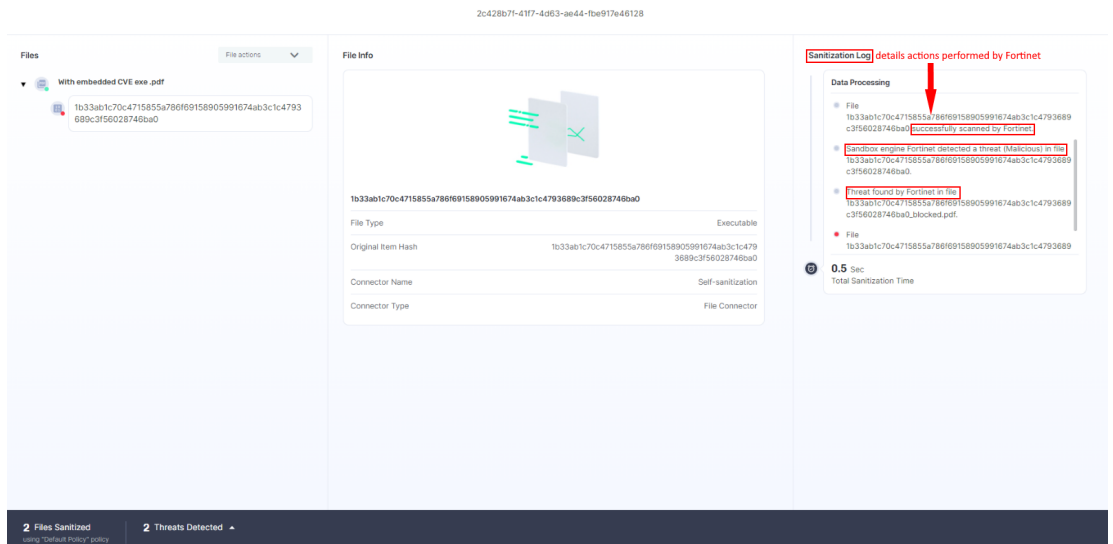
Select the **Default Action** by pressing the **Sandbox** button. The file will be either blocked or sent, depending on the outcome of the Sandbox analysis.

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.

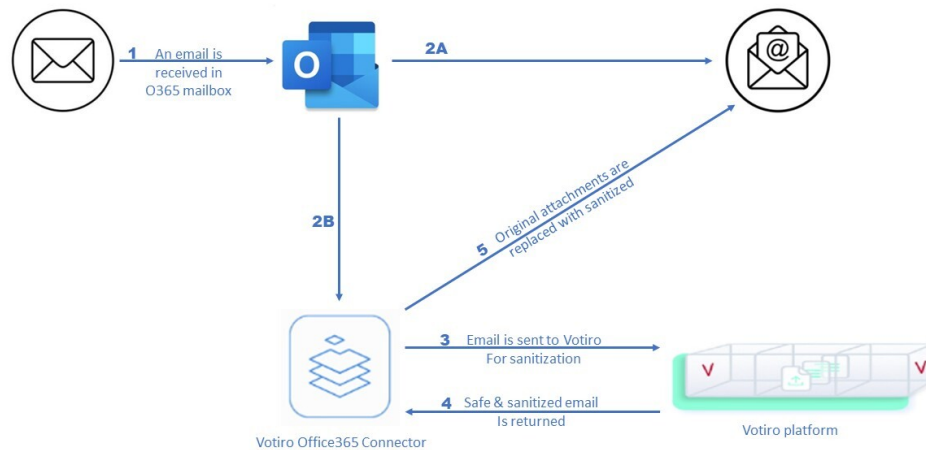
File Information from the Sandbox

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



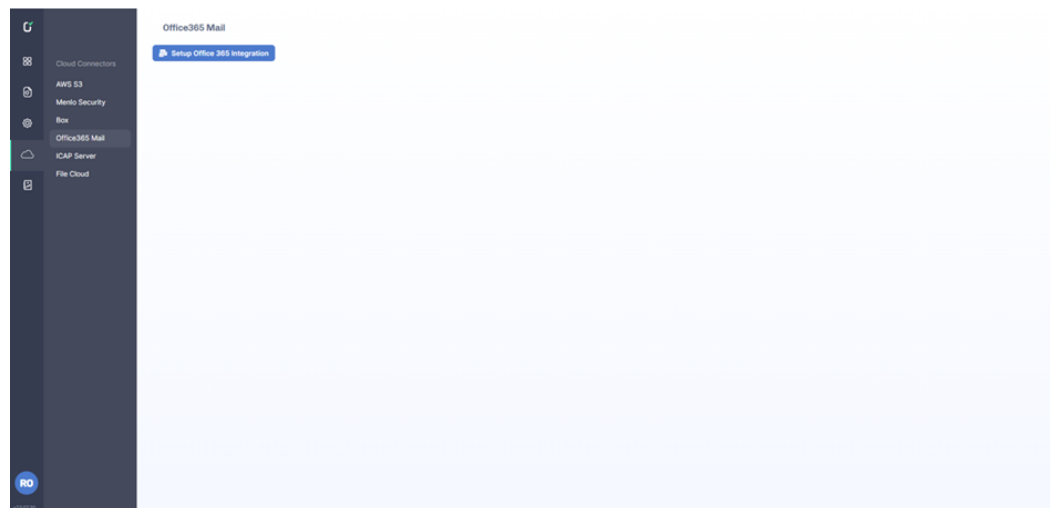
2.5.5 Office365 Mail

Office365 High-level Workflow

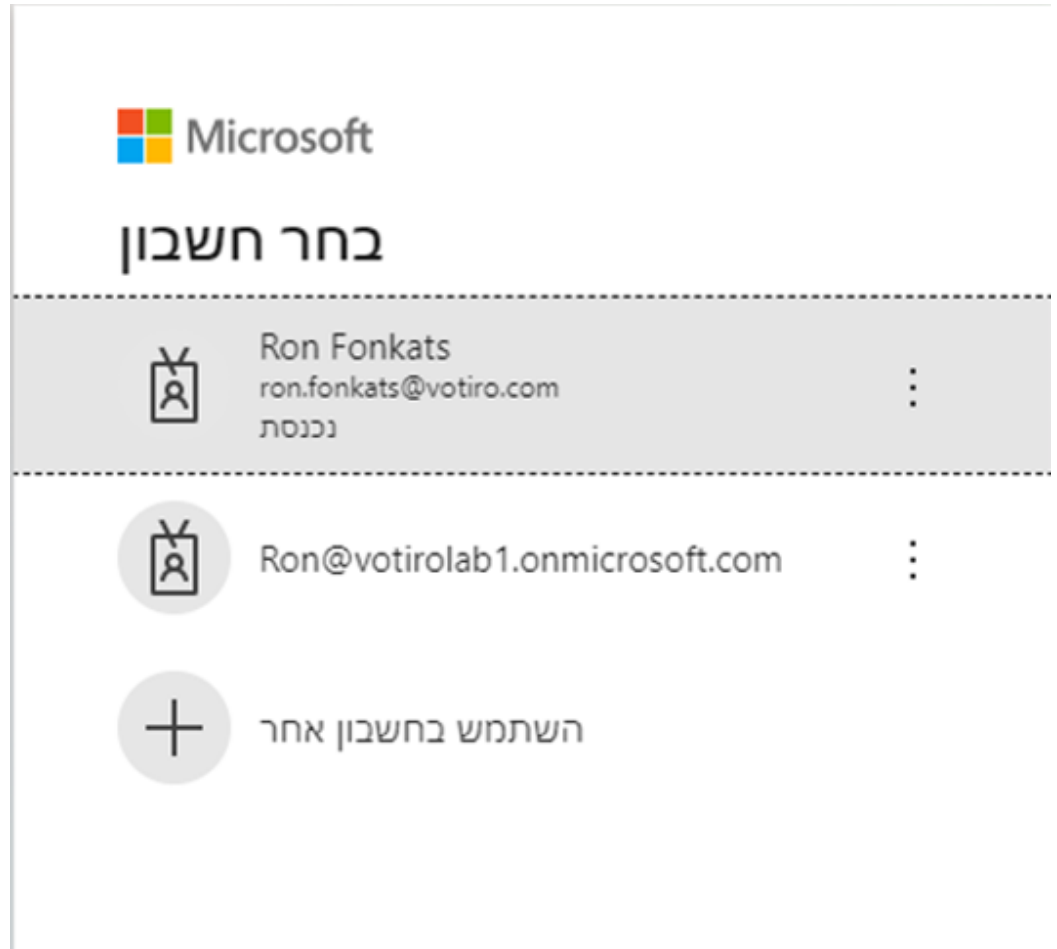


Office365 Integration

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.



ron@votirolab1.onmicrosoft.com

Permissions requested

Review for your organization

VotiroO365Reg

Not Verified

This app is not sponsored by Microsoft or your organization.

This application requests:

- ✓ Sign in and read user profile
- ✓ Read all groups
- ✓ Read all users' full profiles
- ✓ Read and write mail in all mailboxes
- ✓ Send mail as any user
- ✓ Read directory data
- ✓ Read all group memberships

If you agree, this app will have access to the specified resources for all users in the organization. No one else will be notified to review these permissions.

Accepting these permissions means that you allow this application to use data as specified in the terms of service and the publisher's privacy policy. **The advertiser did not provide links to its terms for review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

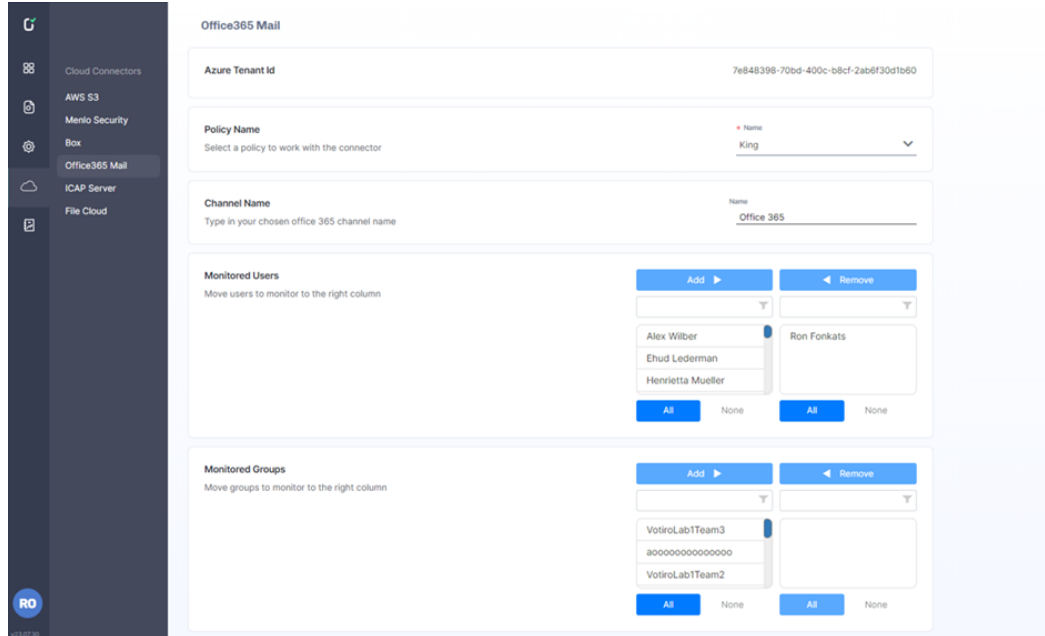
Does this app look suspicious? [Report her here](#)

void

get

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:

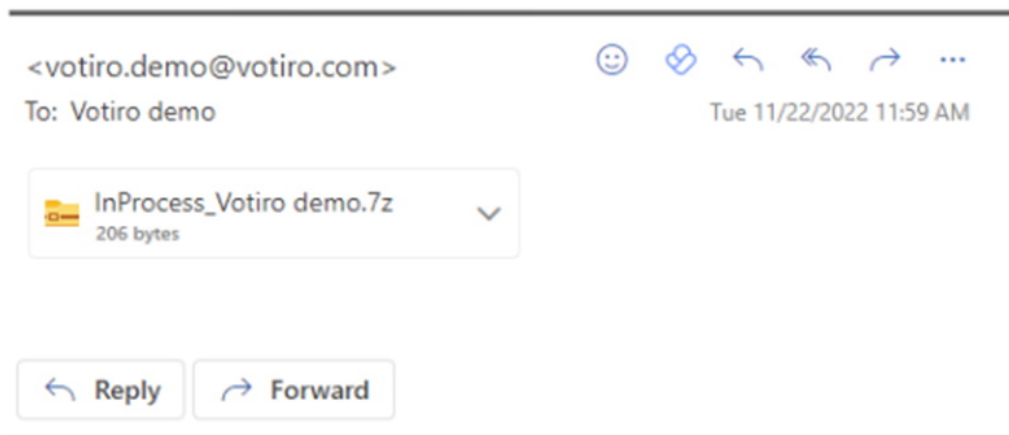
Element	Field	Description
1	Azure Tenant Id	The organization's Azure Tenant ID Note: This field cannot be changed.
2	Policy Name	Specify a policy for the Office 365 connector to work with. Select the Default Policy policy if you have not created an alternative policy to use.
3	Channel Name	Specify the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

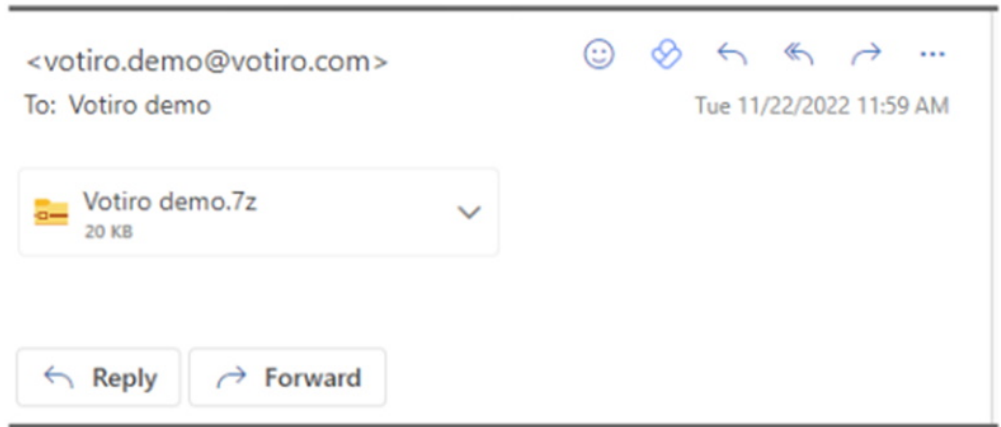
Office 365 Behavior when using the Votiro Office 365 App

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

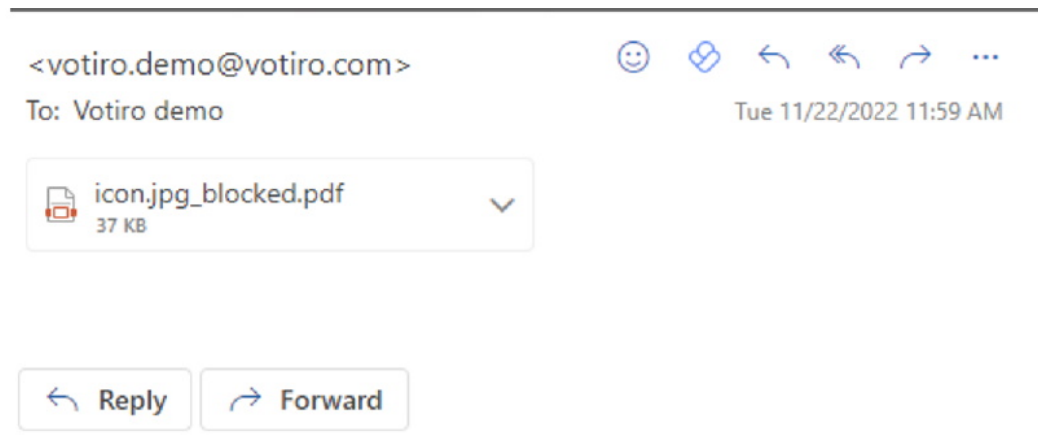


3. After the attached file completes the sanitization processing, the results are displayed.

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



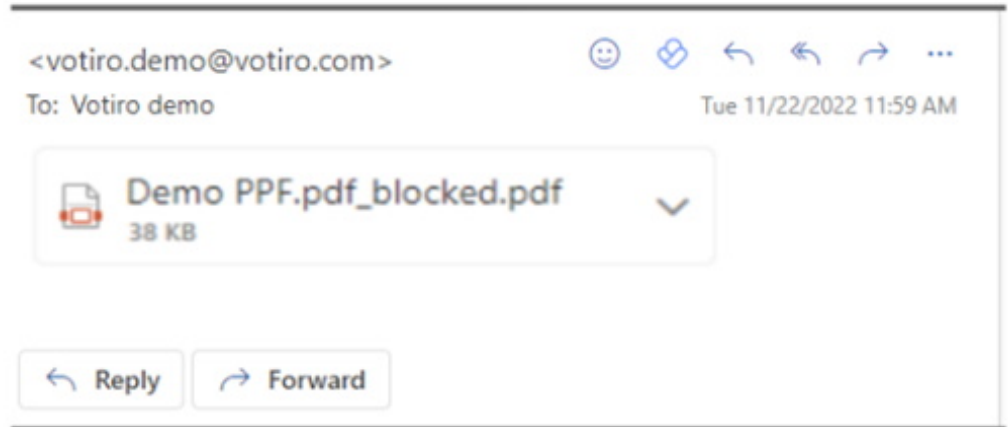
- b. If the attachment was blocked, a blocked PDF file will replace the original attachment.



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

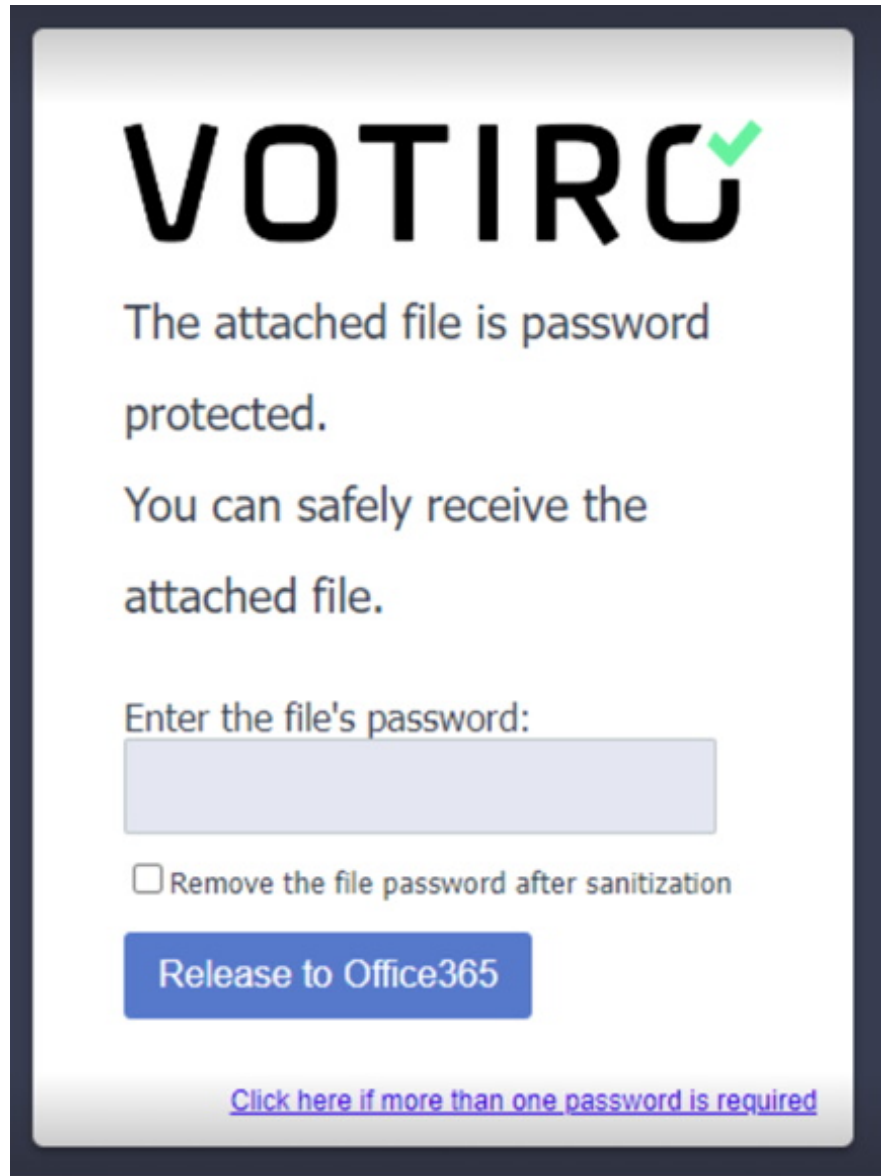
Office 365 App Behavior for Password Protected Files

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:

The image shows a screenshot of a web portal for VOTIRO. At the top, the VOTIRO logo is displayed in large black letters with a green checkmark on the 'O'. Below the logo, the text reads: "The attached file is password protected." followed by "You can safely receive the attached file." There is a text input field labeled "Enter the file's password:". Below the input field is a checkbox labeled "Remove the file password after sanitization". A blue button with the text "Release to Office365" is positioned below the checkbox. At the bottom of the portal, there is a blue hyperlink that says "Click here if more than one password is required".

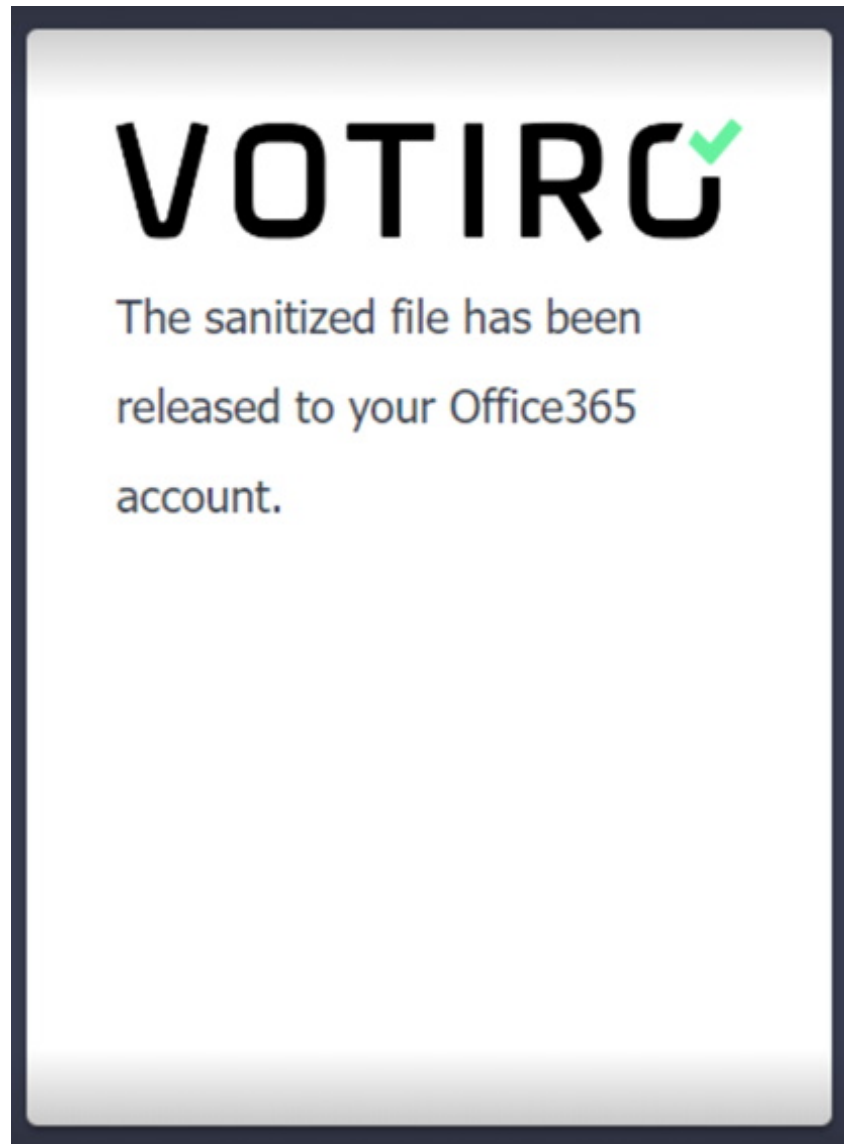
VOTIRO

The attached file is password protected.

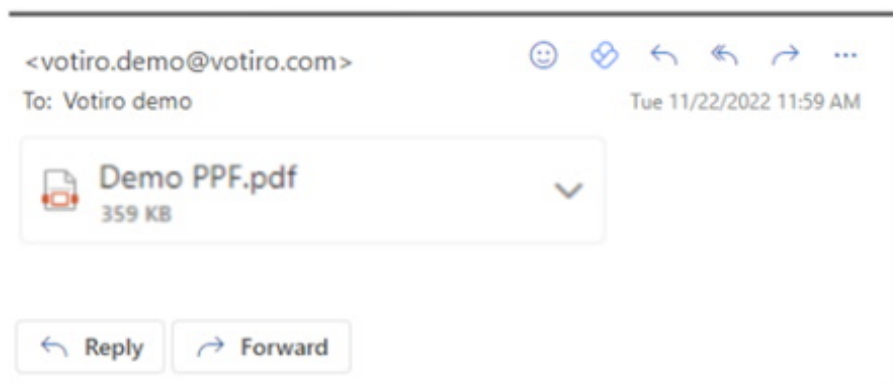
You can safely receive the attached file.

Enter the file's password:

- 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:**



2.5.6 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.

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 Incognito mode.

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

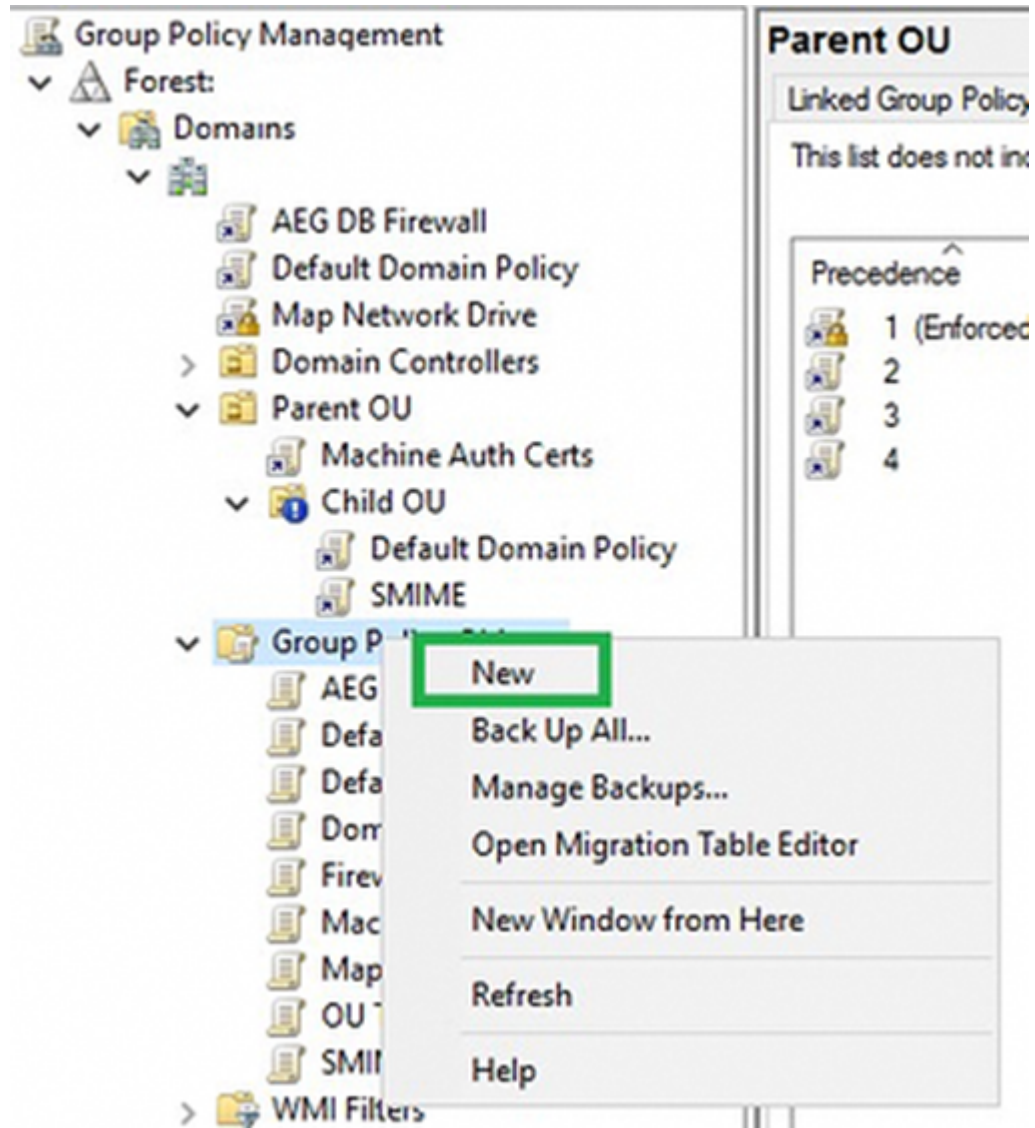
1. Add Chrome Policy Templates

- 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\adm*x
 - for the 32 bit bundle:
*\GoogleChromeEnterpriseBundle\Configuration\adm*x
- 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\adm*x\en-US
 - for the 32-bit bundle:
*\GoogleChromeEnterpriseBundle\Configuration\adm*x\en-US

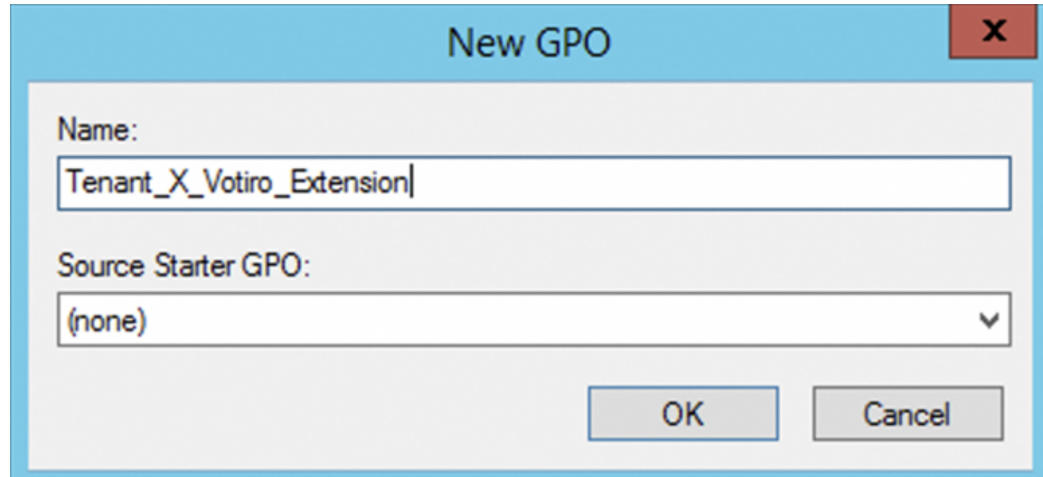
Note: If a language other than en-US is desired, navigate to the appropriate language directory within the admx directory, for example, for Spanish: es-ES, and copy to the appropriate language directory within *C:\Windows\PolicyDefinitions*.

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

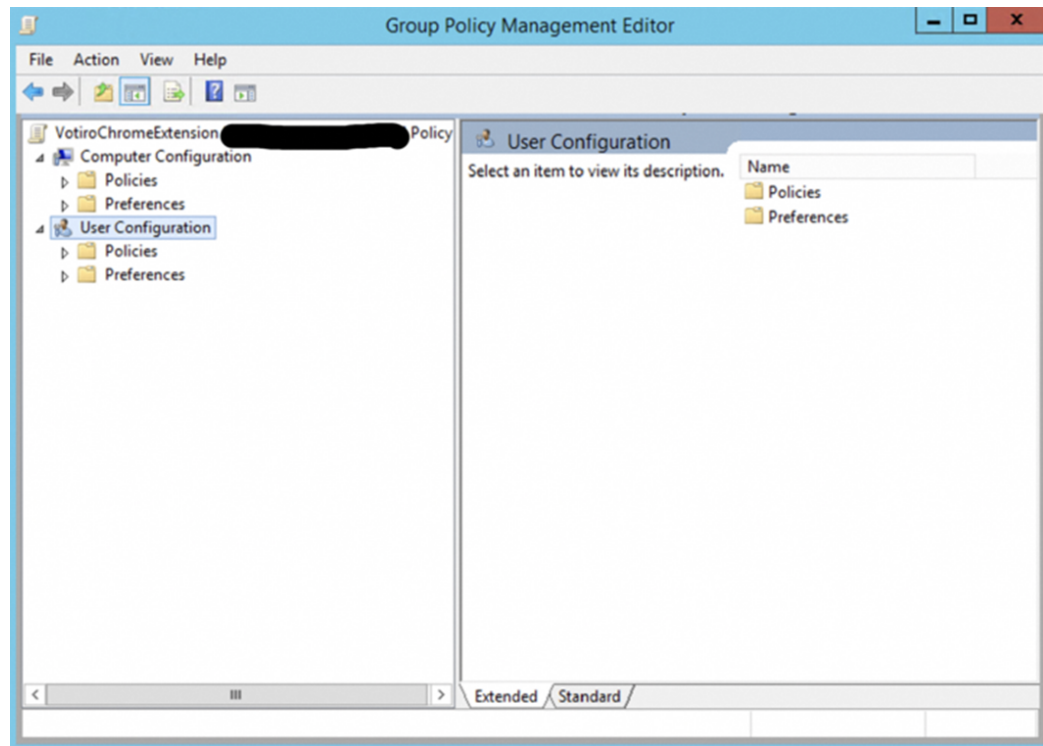
- a. Right-click **Group Policy Objects**, then select **New** to create a new GPO.



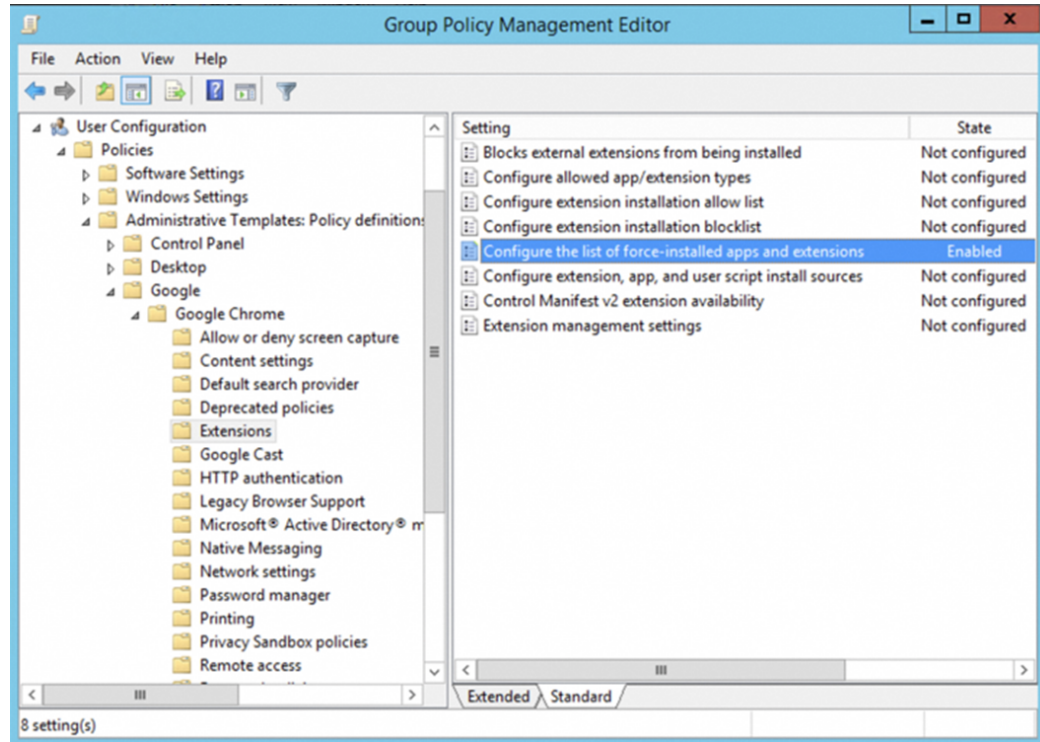
- b. Enter a **Name** for the new GPO , then click **OK**.



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

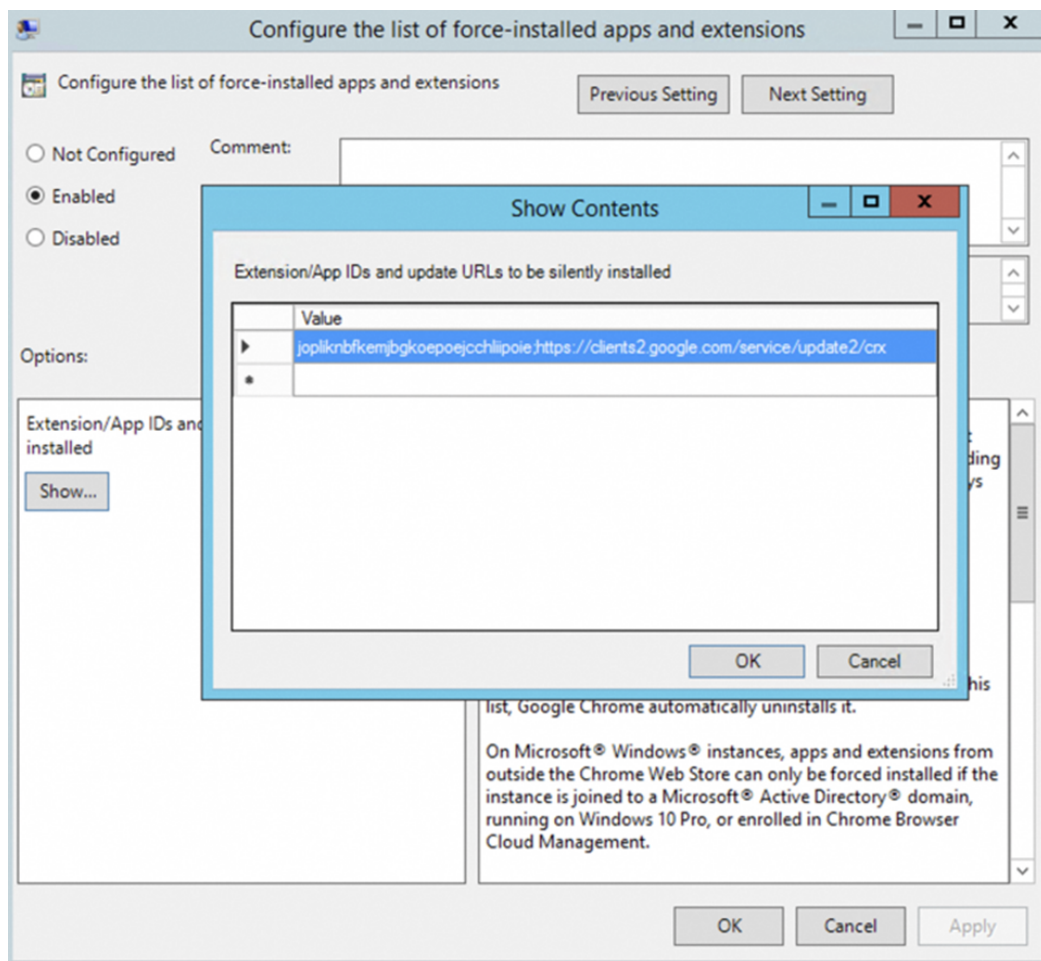


- d. To force-install extensions, go to *User Configuration\Administrative Templates\Google\ Google Chrome\Extensions*. Go to the setting **Configure the list of force-installed apps and extensions** and double click it.



- 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:

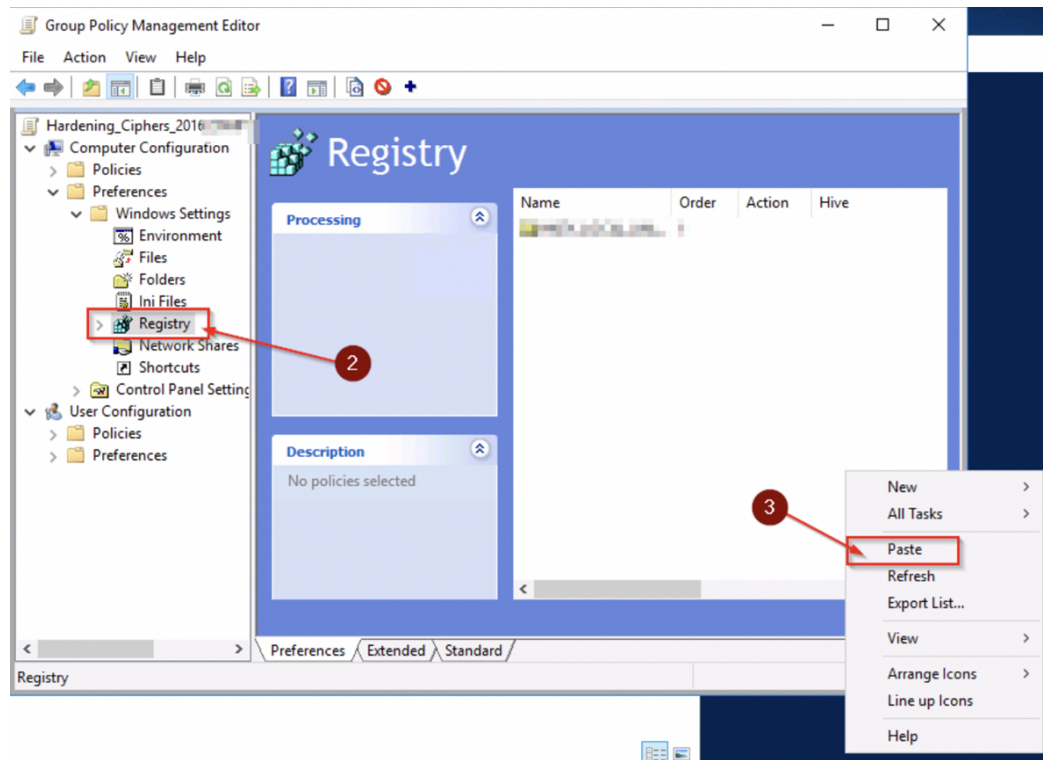
jopliknbfkemjbgkoepoejchliipoie;https://clients2.google.com/service/update2/crx



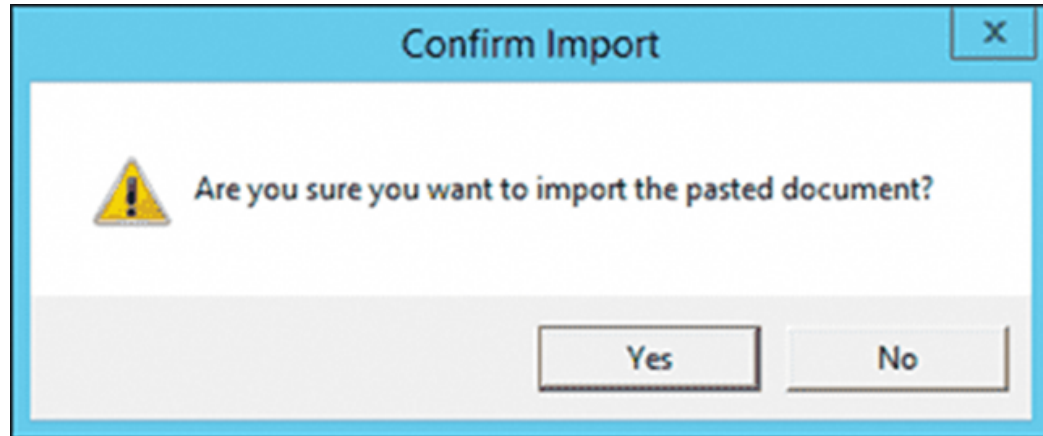
3. **Import xml to the group policy (to update the registry)**

- 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/close. Fail open is 0 and fail close is 1.
 - **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**.

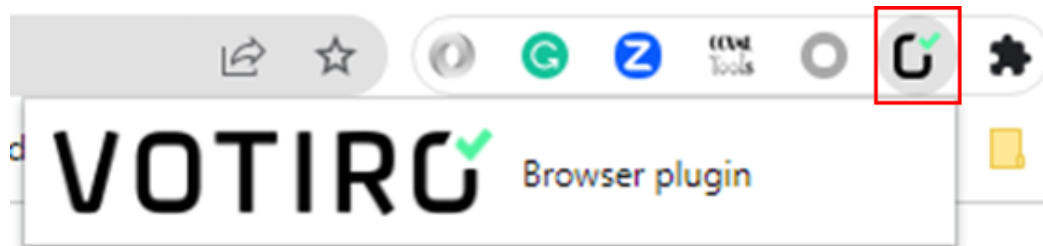


- h. The GPO is created. Now you need to link it according to the organization’s policy. Locate the OU or Domain you want to apply the GPO to, then right-click it and select **Link an Existing GPO...**. Then select your GPO from the list, and click **OK**.

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

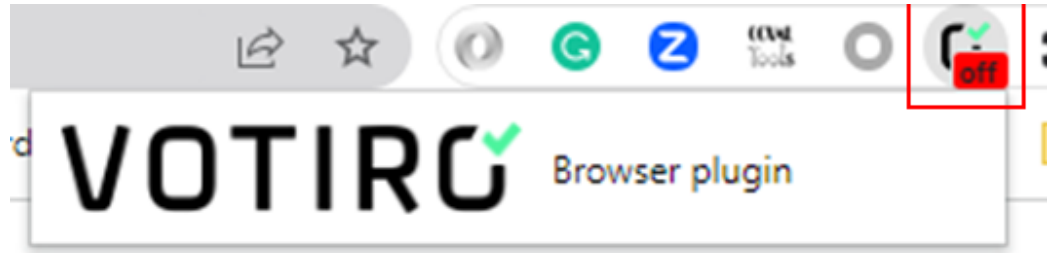
4. **Verify the Browser Extension Deployment**

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



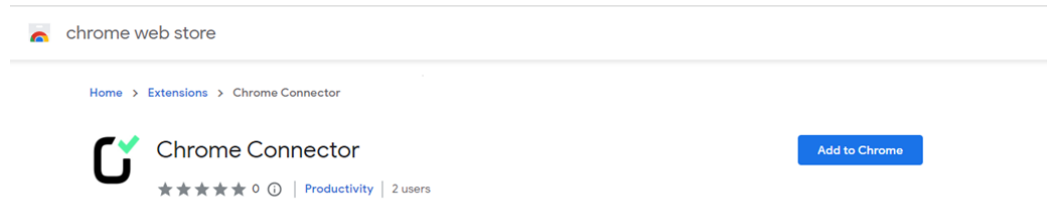
If the Votiro Chrome connector icon appears as above, each downloaded file will be sanitized by Votiro.

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

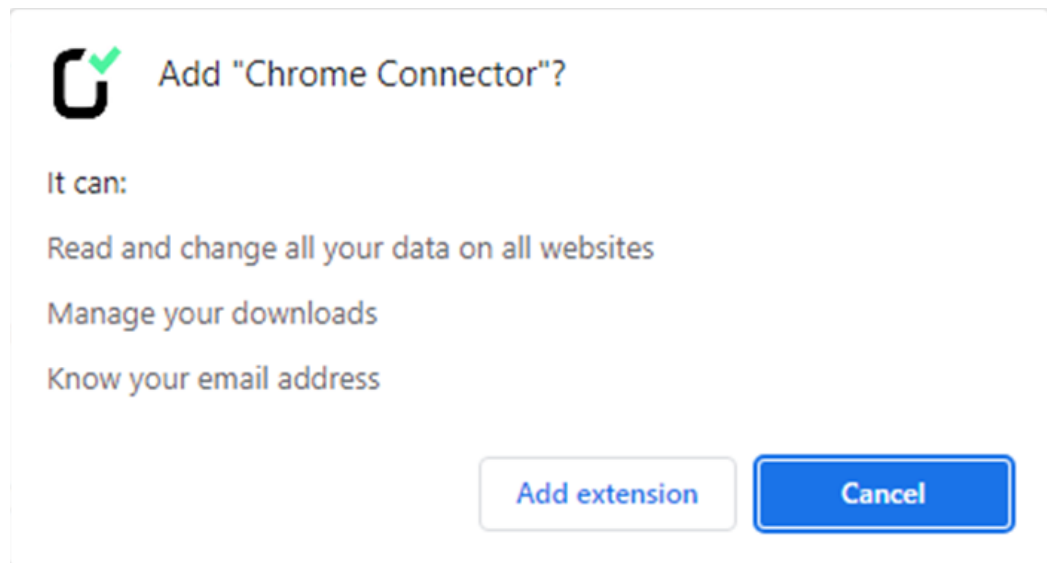


Manual Deployment

1. **Install the extension from Google chrome web store**
 - a. Go to the following link in Chrome: [Votiro Chrome Connector](#)

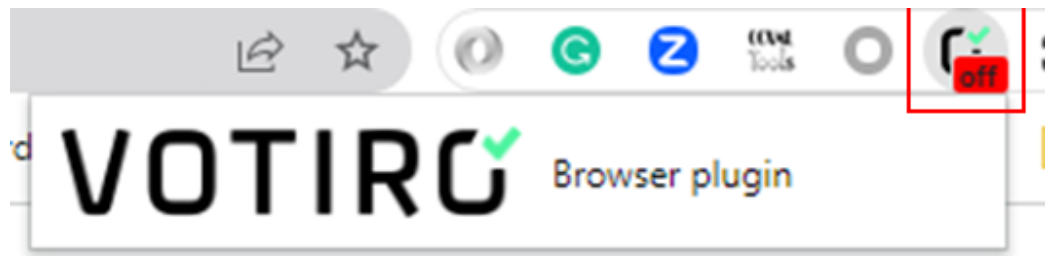


- b. Click on **Add to Chrome**. A confirmation window opens:

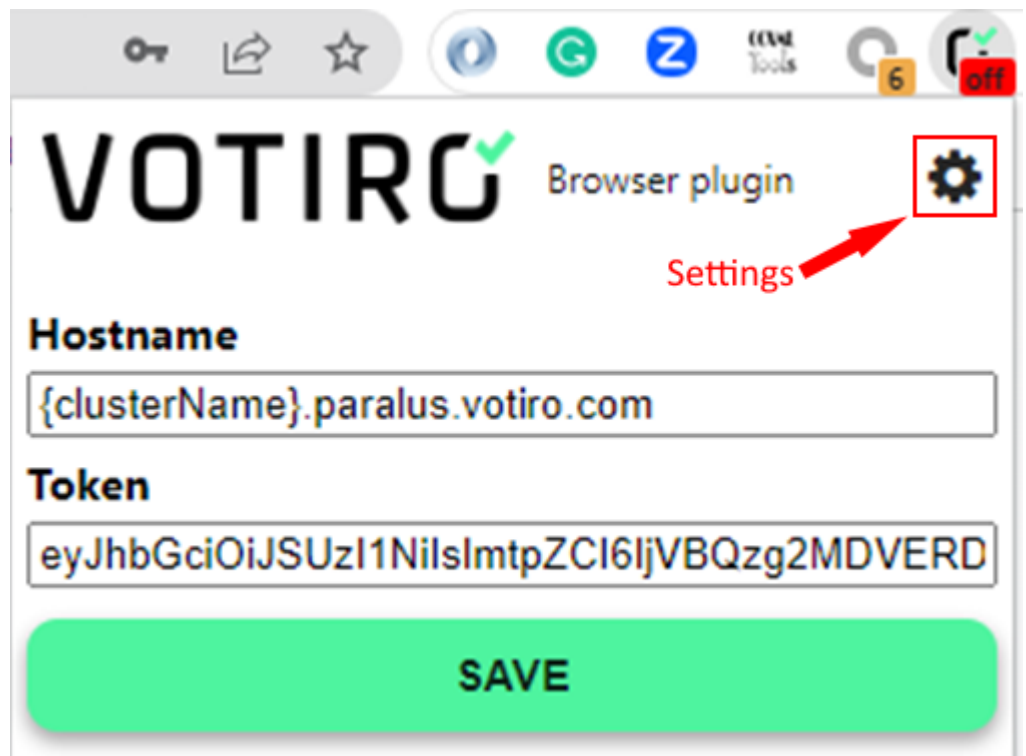


- c. Click on **Add extension**.
2. **Configure the Browser Extension**

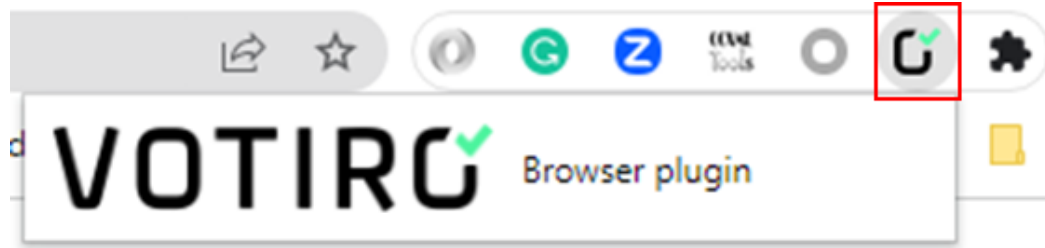
- a. The Chrome connector icon will be displayed with the **off** icon.



- 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.

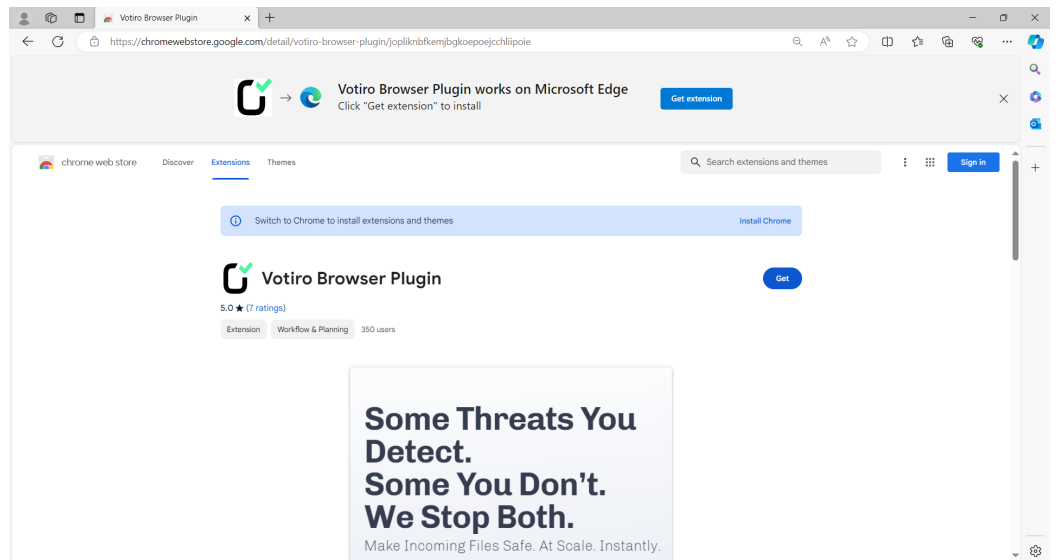


If the Votiro Chrome connector icon appears as above, each downloaded file will be sanitized by Votiro.

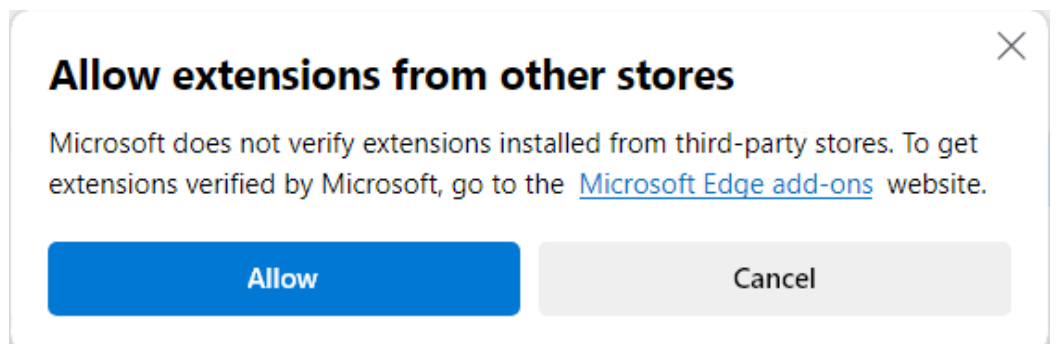
Download and Install in Microsoft Edge Browser

To deploy the Browser plugin in the Microsoft Edge browser:

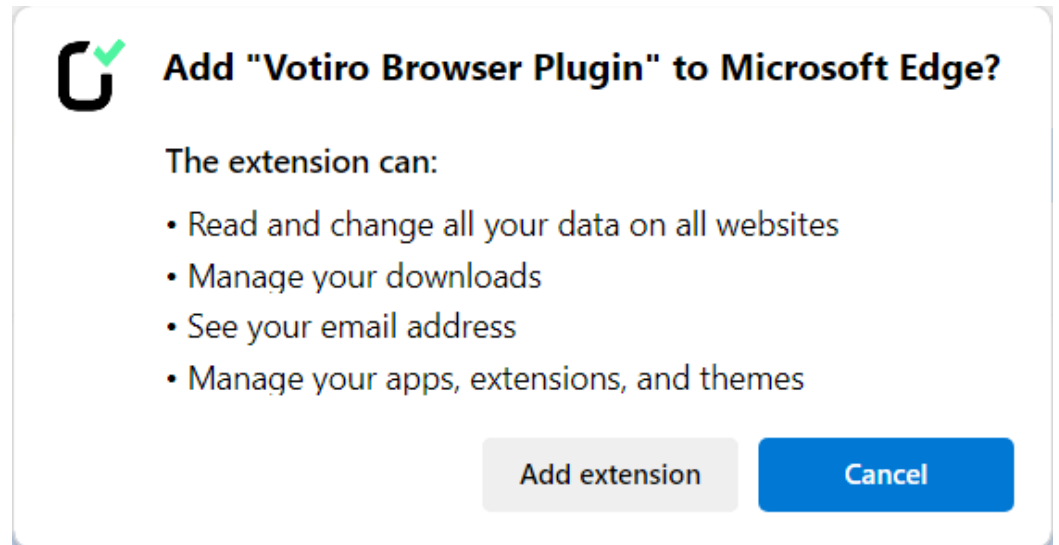
1. Paste the Chrome store extension URL to the Microsoft Edge browser:
[Votiro Browser Plugin](#)



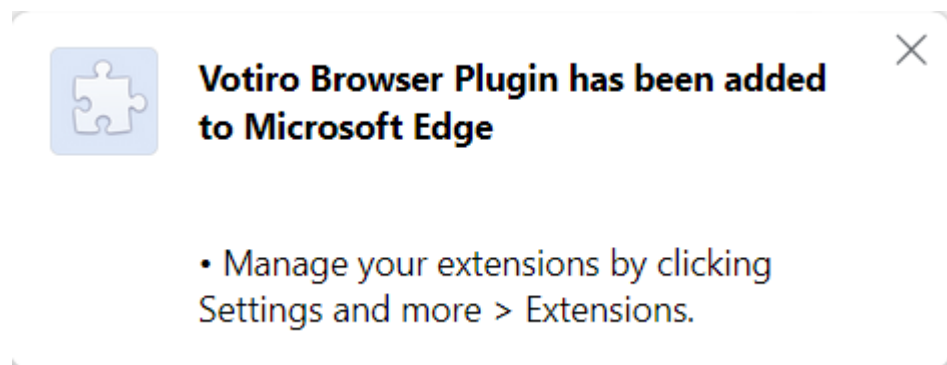
2. Click the **Get extension** or **Get** button to install.



3. Click the **Allow** button.



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



Post-Deployment Actions

After deploying the Votiro Chrome Browser Plugin, you need to ensure that **Allow access to file URLs** is enabled.

In the Chrome browser:

1. Navigate to **Extensions > Manage Extensions**, or enter **chrome://extensions** in the address box.
2. Select the Votiro extension.
3. Check **Allow access to file URLs**.

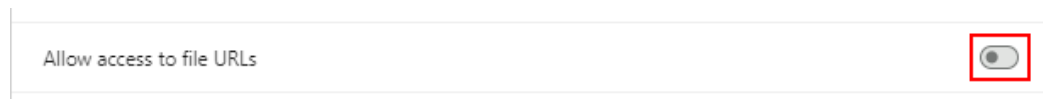


Chrome Extension User's Manual

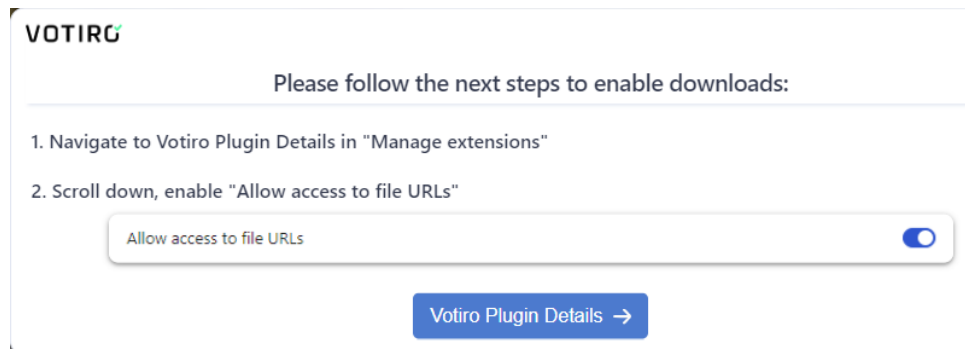
The following features characterize the Votiro Chrome Connector extension:

- **Downloading files**

- ◆ If **Allow access to file URLs** is disabled in the Votiro Chrome Connector extension:



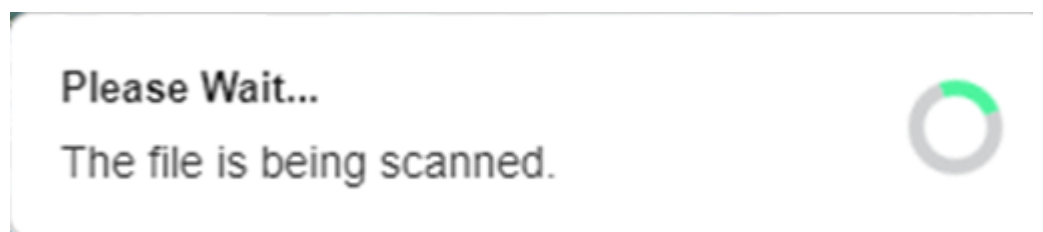
- i. The Votiro plugin prompts a user with a pop-up window to enable this option:



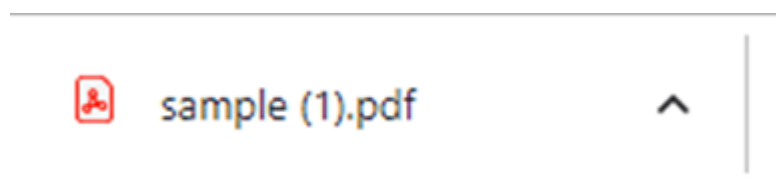
- ii. Click on **Votiro Plugin Details** ->. The user is led to Votiro Browser Plugin > Manage Extensions.
- iii. Toggle the switch to ensure that **Allow access to file URLs** is enabled.



- ◆ 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:

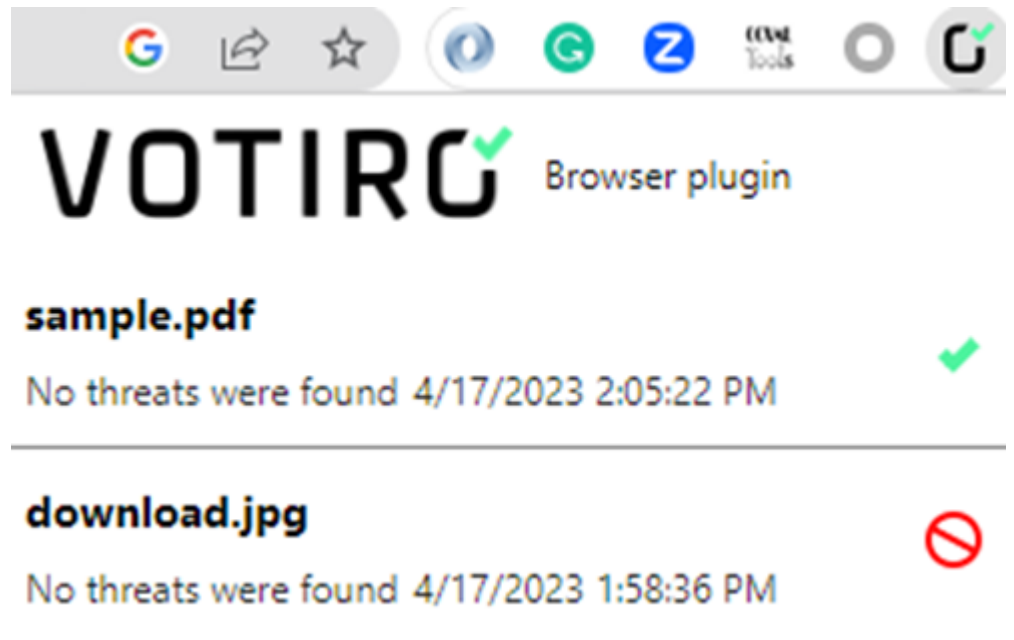


- ◆ To view downloaded files, click on the Votiro extension icon. Downloaded files will be displayed. The following information will be displayed:

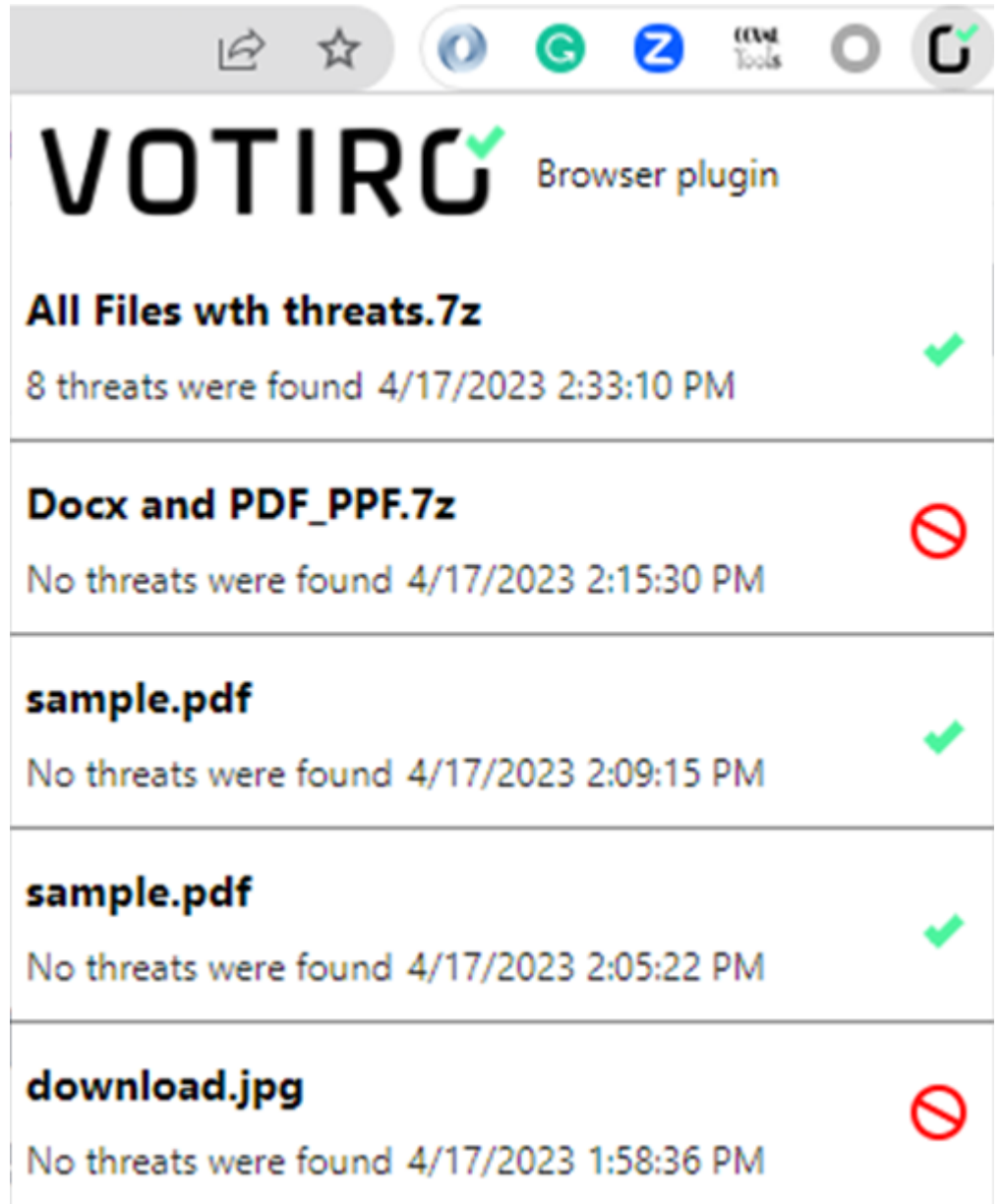
- File name
- Threats indication
- Time frame
- Sanitization result icon - Sanitized/Blocked

The following examples illustrate:

- Example 1: No threats found

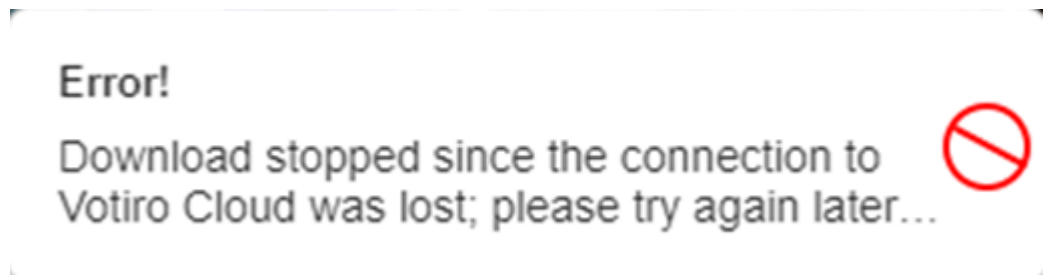


- Example 2: Threats found



■ **Error handling**

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

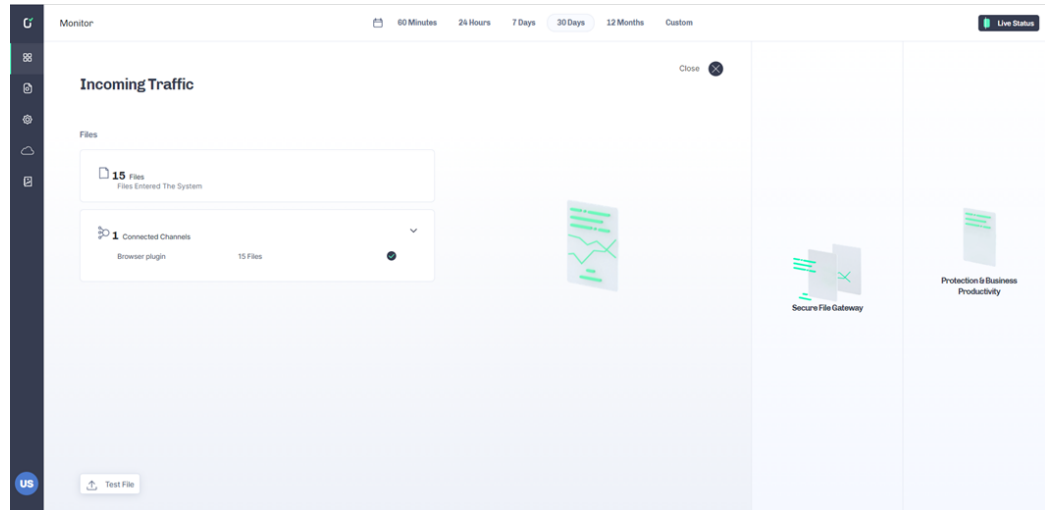


- ◆ In this case, please try again. If the problem still occurs, contact Votiro support.

■ **Votiro Management**

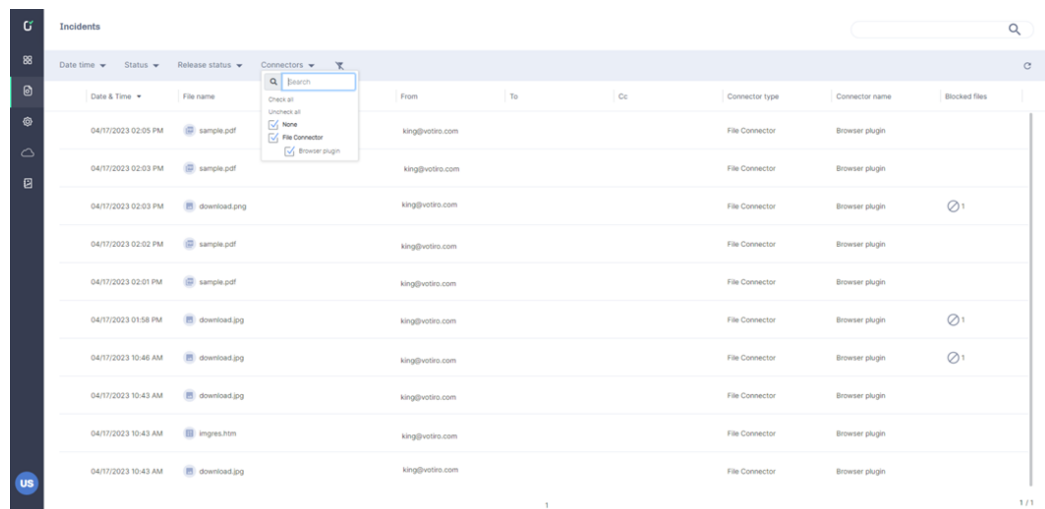
The following screens illustrate the behavior of the Chrome Connector extension in Votiro's management screens:

◆ **Dashboard Monitor screen**

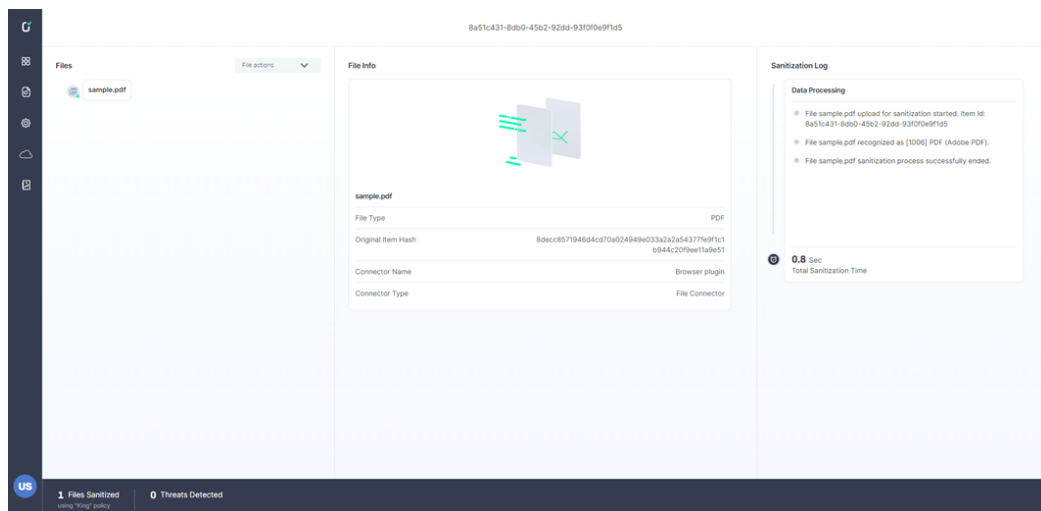


◆ **Incidents screen**

- 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?

DO_NOT_OPEN_cryptdrive_exe	1/3/2024 15:21	File
DO_NOT_OPEN_DuckDuckGo_appinst...	1/3/2024 13:06	File
DO_NOT_OPEN_Email signature galler...	12/27/2023 12:53	File
DO_NOT_OPEN_tenantXchromePlugin...	12/19/2023 14:51	File

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**.

2.6 Password Protected Portal

2.6.1 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 Cloud from the same folder, using the following command:


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

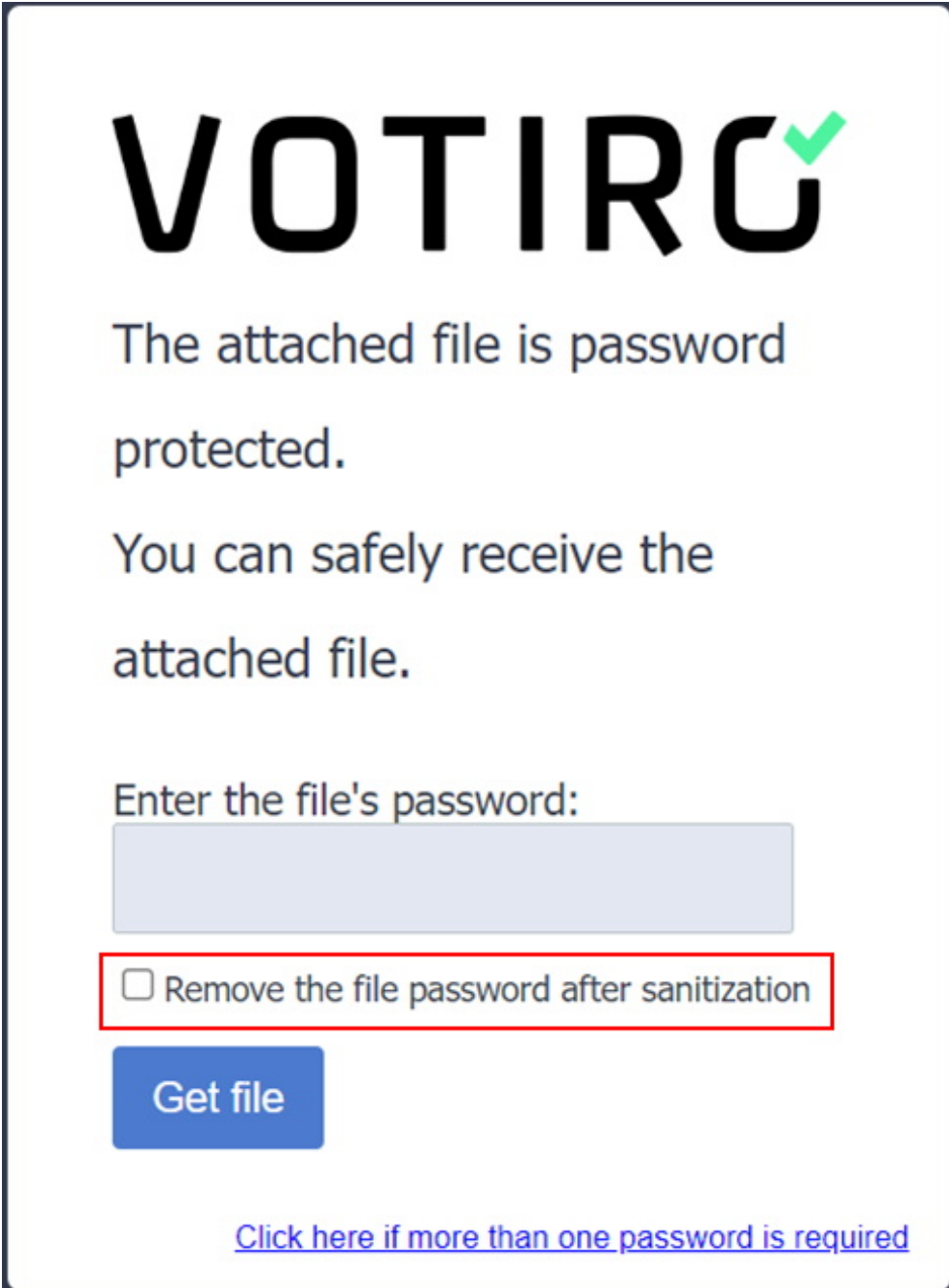
The PPF portal will be updated and use the new image instead of the default.

2.6.2 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:



VOTIRO

The attached file is password protected.

You can safely receive the attached file.

Enter the file's password:

Remove the file password after sanitization

[Get file](#)

[Click here if more than one password is required](#)

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.

2.6.3 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](#):

VOTIRO

The attached file is password protected.

You can safely receive the attached file.

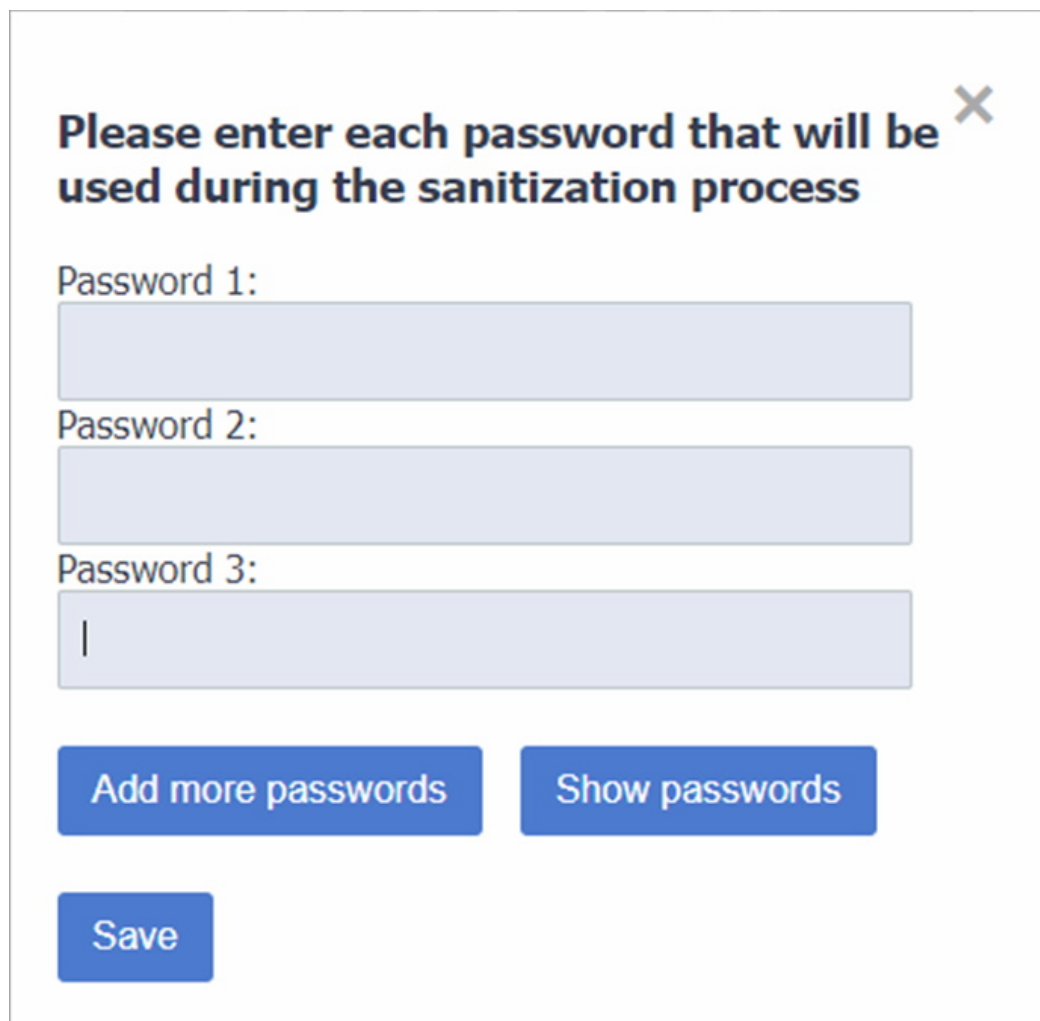
Enter the file's password:

Remove the file password after sanitization

[Get file](#)

[Click here if more than one password is required](#)

- The following pop-up window will be displayed:



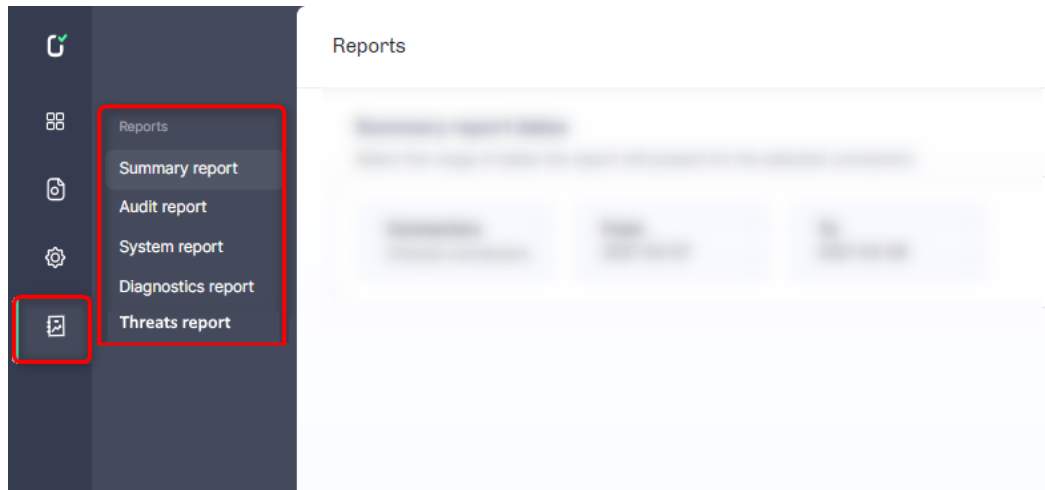
The screenshot shows a pop-up window with a close button (X) in the top right corner. The main heading reads "Please enter each password that will be used during the sanitization process". Below this, there are three text input fields labeled "Password 1:", "Password 2:", and "Password 3:". The "Password 3:" field contains a vertical cursor. At the bottom of the window, there are three buttons: "Add more passwords", "Show passwords", and "Save".

- 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).
- After entering all the passwords, press **Save**.
- 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).

2.7 Generating Reports

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

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



2.7.1 Summary Report

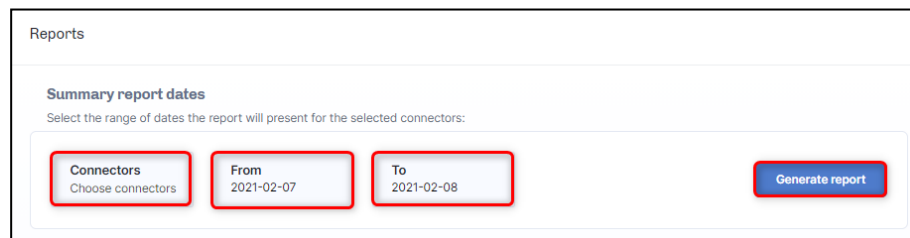
You can generate a summary report of the positive selection processing activity in your organization for a specified period.

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.

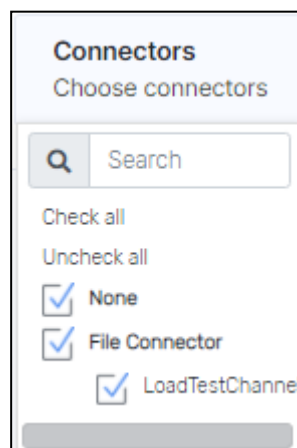
The report presents usage and security data in graphic format and also provides tips for optimizing your positive selection processing effort.

To generate a Summary report, follow these steps:

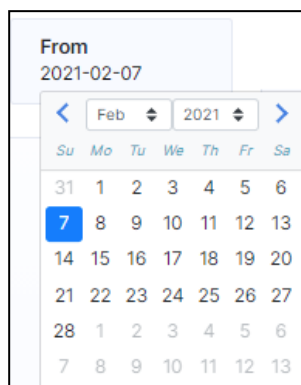
1. In the navigation pane, click **Reports > Summary report**.



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

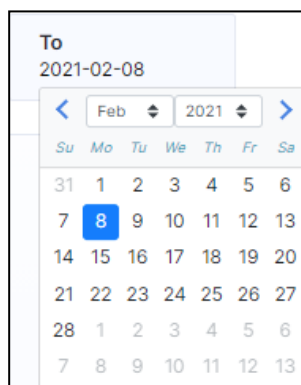


3. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:
 - a. To select the start date from the report, click **From**, a calendar displays.



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.

2.7.2 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 Cloud 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:

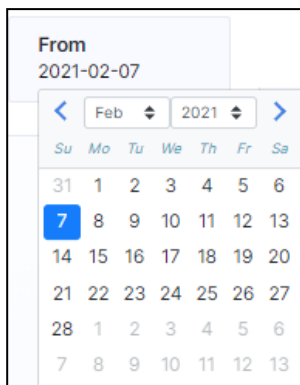
1. In the navigation pane, click **Reports > Audit report**.



The screenshot shows a web interface for generating an audit report. At the top, it says "Reports". Below that, the section is titled "Audit report dates" with the instruction "Select the range of dates the report will present". There are two input fields: "From" with the date "2021-02-07" and "To" with the date "2021-02-08". A blue "Generate report" button is located to the right of these fields.

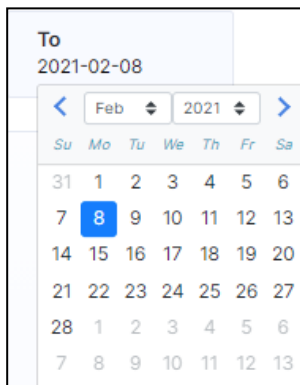
2. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:

- 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 timestamp (in UTC time), a username, and a description of the action logged.

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

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

Information is provided for the following actions:

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

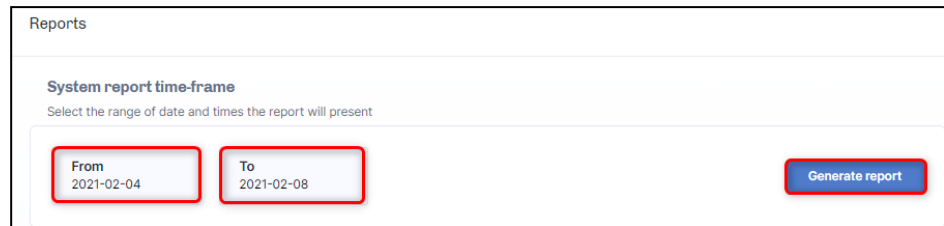
2.7.3 System Report

Votiro Cloud tracks system activity and other actions that were performed in the Management Dashboard.

You can generate a report of all system activity performed by users of the Management Dashboard for a specified period. The exported report generates a zip file.

To generate an System report, follow these steps:

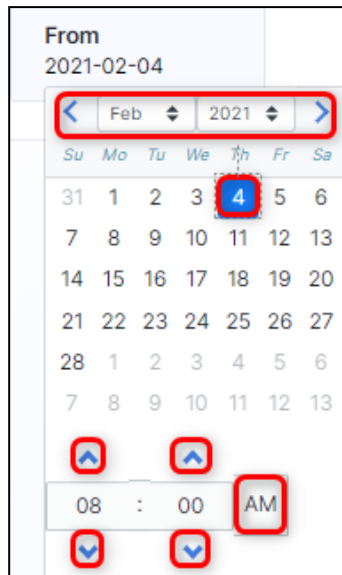
1. In the navigation pane, click **Reports > System report**.



The screenshot shows a web interface for configuring a system report. At the top, the word "Reports" is displayed. Below it, the section is titled "System report time-frame" with the instruction "Select the range of date and times the report will present". There are two input fields: "From" with the value "2021-02-04" and "To" with the value "2021-02-08". A blue "Generate report" button is located to the right of these fields. Red boxes highlight the "From" and "To" fields in the original image.

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:

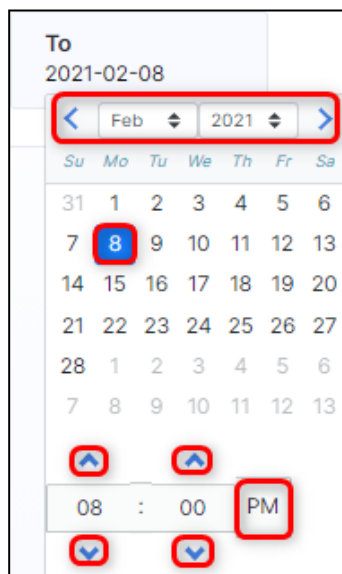
- a. To select the start range of the report, click **From**, a calendar displays.



The selected date is blue. To change the date and time navigate to the desired 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.

To set the time of the report to begin, use the up and down arrows at the bottom of the calendar, using the AM/PM button as required.

- b. To select the start range of 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 for the day and time for report to end.

- 3. Click **Generate Report**.

The System report is generated.

System Report Format and Structure

The output generated is in zip format. The following is an example excerpt when system files are extracted:

Name	Size	Packed Size	Modified
logs	255 462 505	10 404 200	
votiro1	236 693	35 871	2020-03-31 06:31
votiro3	57 705	6 487	2020-03-31 06:31
votiro4	15 425	1 407	2020-03-31 06:31

These files are password protected and for use by Votiro.

2.7.4 Diagnostics Report

Votiro Cloud tracks system activity and other actions performed in the Management Dashboard.

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

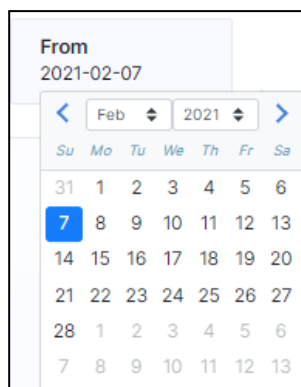
The report collects useful data of the positive selection processing activity. The diagnostics files generated are used internally by Votiro for support and research purposes.

To generate a Diagnostics Report, follow these steps:

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

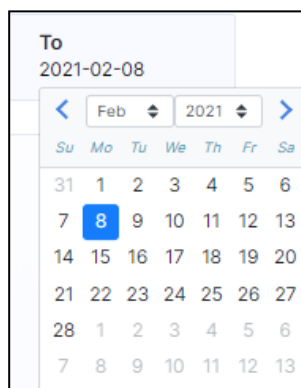
2. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:

- 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 Diagnostics report is generated.

Diagnostics Report Format and Structure

The output generated is in zip format. The database folder and additional files are password protected. The diagnostics files generated are used internally by Votiro for support and research purposes.

2.7.5 Threats Report

Votiro Cloud 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.

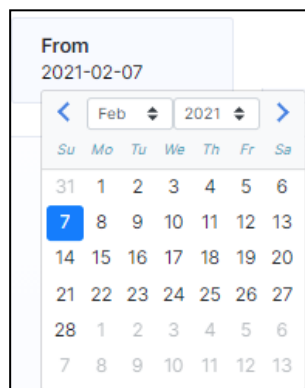
The report collects useful data of the positive selection processing activity. The threat report files generated are used internally by Votiro for support and research purposes.

To generate a Threats Report, follow these steps:

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

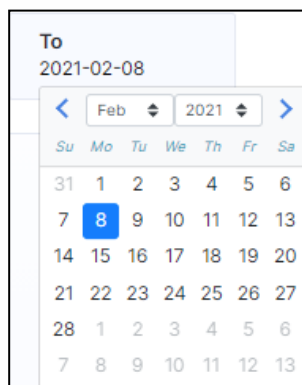


2. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:



- 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

Date	Time	Files request	Files Sanitized	Total Threats identified	Timestamp	Filename	File type	Threat	Info	Status	File hash
26/04/2022 - 29/04/2022	00:00:00 - 23:59:59 hrs	142	2952	79							
28/04/2022 18:40:05 hrs	eicar.txt						72 File	Threat Suspicious Threat File Detected by Antivirus	Threat Suspicious Threat File Det	Infected	275a021bbfb6489e544471899f7db9d1663fc695e
28/04/2022 18:04:03 hrs	eicar.txt						72 File	Threat Suspicious Threat File Detected by Antivirus	Threat Suspicious Threat File Det	Infected	275a021bbfb6489e544471899f7db9d1663fc695e
28/04/2022 15:34:58 hrs	eicar.txt						72 File	Threat Suspicious Threat File Detected by Antivirus	Threat Suspicious Threat File Det	Infected	275a021bbfb6489e544471899f7db9d1663fc695e
28/04/2022 13:10:22 hrs	SDS Web Service User:Word (200						72 File	Threat External Program Run Action	Threat External Program Run	Clean	32c7c3f628a18c401c7d828507d68680931f3a56e
28/04/2022 11:46:14 hrs	Password2.7z						72 File	Threat Suspicious Executable File	Threat Suspicious Executable File	Clean	a8589f01af12b6802a9acdd8ce1d65b4b7887e29f
28/04/2022 11:35:59 hrs	Password2.7z						72 File	Threat Suspicious Executable File	Threat Suspicious Executable File	Clean	a8589f01af12b6802a9acdd8ce1d65b4b7887e29f
28/04/2022 11:35:33 hrs	Password2.7z						72 File	Threat Suspicious Executable File	Threat Suspicious Executable File	Clean	a8589f01af12b6802a9acdd8ce1d65b4b7887e29f
28/04/2022 11:34:15 hrs	Password2.7z						72 File	Threat Suspicious Executable File	Threat Suspicious Executable File	Clean	a8589f01af12b6802a9acdd8ce1d65b4b7887e29f
28/04/2022 11:33:07 hrs	Password2.7z						72 File	Threat Suspicious Executable File	Threat Suspicious Executable File	Clean	a8589f01af12b6802a9acdd8ce1d65b4b7887e29f
28/04/2022 11:30:57 hrs	Radiohead_Man-Of-W						Unknown File	Threat Suspicious Unknown File	Threat Suspicious Unknown File	Infected	9d5d5bb48b092184ec3c33157ca094513aa9fd756
28/04/2022 09:57:36 hrs	suspiciousmarco + File Word with						File System Activity Macro	Threat Suspicious File System Activity Macro	Threat Suspicious File System Act	Infected	7c6ca3fd8988346128faeecd5ec0e47b9516b479c
28/04/2022 09:56:20 hrs	suspiciousmarco + File Word with						File System Activity Macro	Threat Suspicious File System Activity Macro	Threat Suspicious File System Act	Infected	7c6ca3fd8988346128faeecd5ec0e47b9516b479c
28/04/2022 09:44:37 hrs	suspiciousmarco + File Word with						File System Activity Macro	Threat Suspicious File System Activity Macro	Threat Suspicious File System Act	Infected	f0f806288eb451a0e63c3b0985dbd8f700c0019e6f
28/04/2022 09:42:29 hrs	SDS Web Service User:Word (200						Threat External Program Run Action	Threat External Program Run	Threat External Program Run	Clean	32c7c3f628a18c401c7d828507d68680931f3a56e

Appendix A Syslog Events to SIEM Platforms

Votiro Cloud 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 49](#).

Here is an example of a SIEM CEF message in Votiro Cloud:

```
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=5m6def67073ea7cf9aa3a68899f10fcdd074440efd60fa04e94774e9434ee152
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 Cloud:

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 Cloud
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

Field #	Field name	Description	Value
14	File hash	Hash of the file	{hash (hexadecimal) string}
15	File size	File size in bytes	{long integer}
16	Password protected	Indicates whether the file is password protected	<ul style="list-style-type: none"> • true • false
17	AV result	Result from the Anti-Virus engine's scan of the file	<ul style="list-style-type: none"> • 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 Cloud modified in the file	{character string} For example, Removed suspicious macros; Removed external link path
22	Sanitization result	Result of Votiro Cloud's sanitization of the file	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • {Message ID} • "null"
30	Subject	Email subject	<ul style="list-style-type: none"> • {character string} • "null"
31	From	Sender's email address	<ul style="list-style-type: none"> • {character string} • "null"
32	Recipients	Recipients' email addresses	<ul style="list-style-type: none"> • {character string} • "null"

Appendix B 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
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 58](#).

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 141](#).

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
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.

Case	Processing Options
Password Protected	<p>You can block or process these files. By default, the files are processed for positive selection.</p> <ul style="list-style-type: none"> ■ 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. <p>When the files are blocked, Votiro Cloud 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.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note</p> <p>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.</p> </div> <p>Instructions for Email User</p> <p>The Votiro Cloud administrator should communicate the following information and instructions to the users.</p> <p>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.</p> <p>The password protected file is processed for positive selection, then attached to the email. This is distributed to all named recipients. If Votiro Cloud has already processed password protected files, additional users requesting files to be processed will be advised that this has already taken place.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note</p> <p>This feature supports the use of one password per email.</p> </div>

Case	Processing Options
Large File	<p>You can set the minimum size of files you want to block.</p> <p>When this option is checked, for every file that Votiro Cloud blocks, it issues a block-file containing the reason it was blocked. Accept the default text or edit it.</p>
Complex File Special Case	<p>You can set a layer number. Files that are found in that layer or deeper are blocked.</p> <p>You will have already defined a Special Case with Votiro's support team. Click Load File. For more information, see Defining Policies on page 60.</p>

Appendix C 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	•	1
CAD	•	0
Ichitaro	•	0
Binary	•	0
Archive	•	0
RTF	•	0
Email	•	0
Microsoft Office	•	0
HTML Attachments	•	0
Open Document	•	0
Text	•	0
Other Files	•	1

For more information about the policies page, see [Policies Dashboard on page 58](#).

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 141](#).

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	<p>By default, these files are processed for positive selection.</p> <ul style="list-style-type: none"> ■ 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. ■ Block files with suspicious links: Performs a check of all links in the form HTTP:// and HTTPS:// in a PDF document. If any link is found to be suspicious, the file is blocked. The suspicious link is not removed from the file. When this option is checked, for every file that the Positive Selection® Engine blocks, it issues a block-file containing the reason it was blocked. Accept the default block reason, or edit it. When selected you can edit the Block Reason message. Default is unchecked. ■ JavaScript handling: Determines how JavaScript, if found in the PDF file, is handled. <ul style="list-style-type: none"> ◆ Don't do anything ◆ Remove only suspicious scripts ◆ Remove all scripts (this is the default)

File Type	Processing Options
Image	<p>By default, these files are processed for positive selection.</p> <ul style="list-style-type: none"> ■ Add micro-changes: Adds security noise to images during processing. Default is checked. <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p>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.</p> </div> <ul style="list-style-type: none"> ■ 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.
Binary	<p>The processing option is not relevant to managing binary files. You either block binary files or allow them.</p>
Archive	<p>By default, these files are processed for positive selection.</p> <p>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.</p>
CAD	<p>Remove VBA Macros: Removes VBA macros from the file. Default is unchecked.</p>
RTF	<p>By default, these files are processed. There are no specific processing options.</p>
HTML Attachments	<p>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.</p>

File Type	Processing Options
Email	<p>By default, these files are processed for positive selection.</p> <ul style="list-style-type: none"> ■ 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".
<p>Microsoft Office</p> <div data-bbox="400 1055 691 1503" style="background-color: #f2f2f2; padding: 5px;"> <p>Note</p> <ul style="list-style-type: none"> ■ 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. </div>	<p>By default, these files are processed for positive selection.</p> <ul style="list-style-type: none"> ■ 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. <div data-bbox="707 790 1409 891" style="background-color: #f2f2f2; padding: 5px;"> <p>Note</p> <p>This option is available for DOC/DOCX/XLSX file types only.</p> </div> <ul style="list-style-type: none"> ■ Macro handling. In the list, choose one of the following: <ul style="list-style-type: none"> ◆ 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. <div data-bbox="707 1323 1409 1529" style="background-color: #f2f2f2; padding: 5px;"> <p>Note</p> <p>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).</p> </div> <ul style="list-style-type: none"> ■ 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	<div data-bbox="707 293 1407 421" style="background-color: #f2f2f2; padding: 5px;"> <p>Note XML and JSON files are processed according to the Text files policy.</p> </div> <p>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).</p> <p>Block CSV with threat formula: Blocks CSV files that contain formula injections. When selected you can edit the Block Reason message. Default is checked.</p>
Media	<p>The user can set Media file policy exceptions.</p> <ul style="list-style-type: none"> <li data-bbox="707 786 1407 851">■ Remove metadata: Removes metadata from media files. Default is unchecked.
Open Document	<p>The user can set Open Document file policy exceptions. By default, these files are sanitized. During the sanitization, the macros will not be preserved.</p>
Other files	<p>By default, these files are blocked. You can edit the Block Reason message.</p> <p>There are no specific sanitization processing options.</p>

Appendix D 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 Cloud for Email only)
- File extension
- Digital signature

For more information about the policies page, see [Policies Dashboard on page 58](#).

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:

The screenshot shows a 'Define Exception' dialog box. The title is 'Define Exception' and the subtitle is 'Exception will be activated under the following conditions'. The main content area shows a rule structure: 'IF File type [dropdown] Equals [dropdown] Select [dropdown]'. Each dropdown menu is highlighted with a red square. At the bottom left is a plus sign icon, and at the bottom right are 'Cancel' and 'Save' buttons.

4. Define at least one condition to base the exception on. Create a condition by selecting values from lists, or entering text, as appropriate.

- To add another condition to the exception definition, click the plus (+) icon. To delete a condition, click the trash icon.

Define Exception
Exception will be activated under the following conditions

IF	File size	is more than	+	10	-	MB	
IF	Email	To	=	careers@uni.com			
IF	Digital signature	is valid					

Cancel Save

- 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.

PDF + Add Exception

Default Action

Block Sanitize Allow

Remove multimedia

Clean embedded fonts

Block files with suspicious links

JavaScript handling

EXCEPTION

Size > 10MB | "To" field equals "careers@uni.com" | Digital signature is valid

Block Sanitize Allow

Remove multimedia

Clean embedded fonts

Block files with suspicious links

JavaScript handling

Save Changes

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

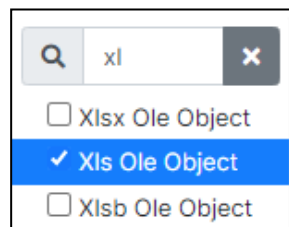
Defining Exceptions for File Types



To specify an exception for one or more file types:

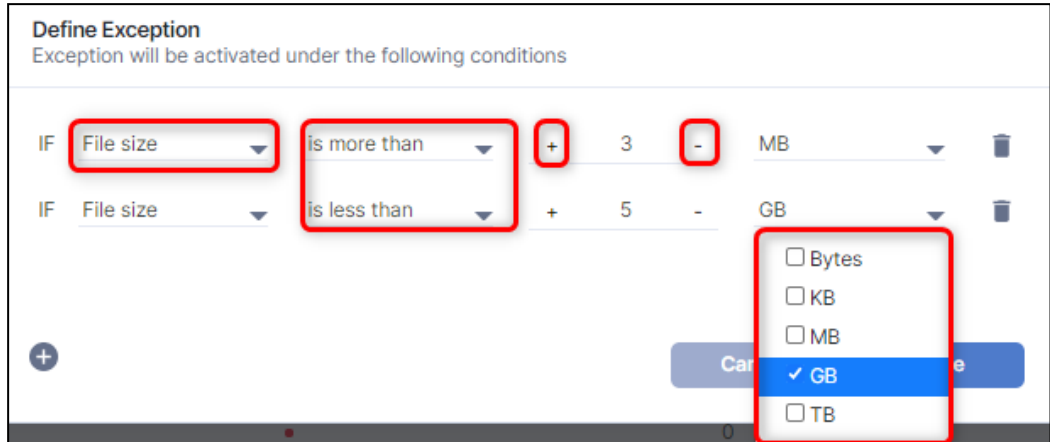
1. In the leftmost list, select **File Type**.
2. In the second list, select **Equals** or **Not Equals**.
3. In the last list, select one or more relevant file types. The list displays the most common types.

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



4. Proceed to Step 6 in [See Adding an Exception](#): in this section.

Defining Exceptions for File Size



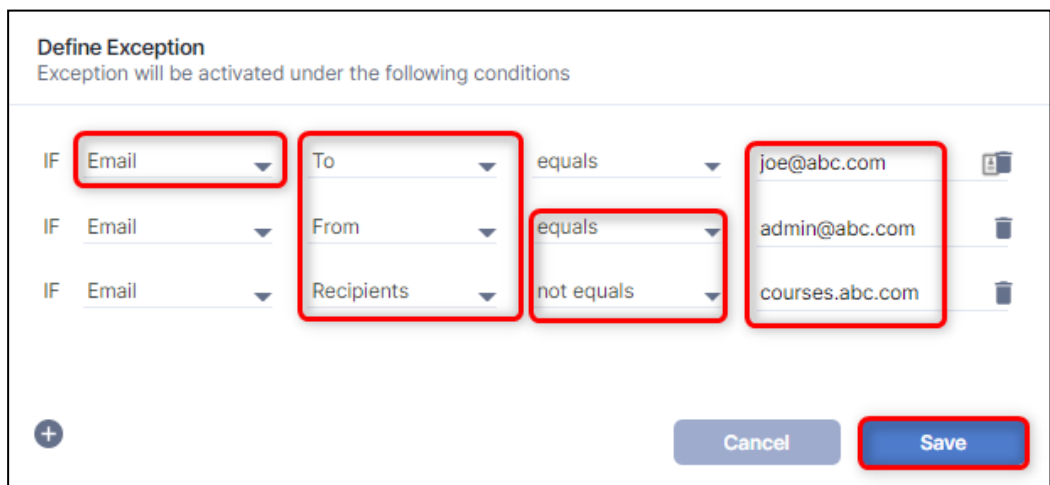
To specify an exception based on on file size:

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 [See 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

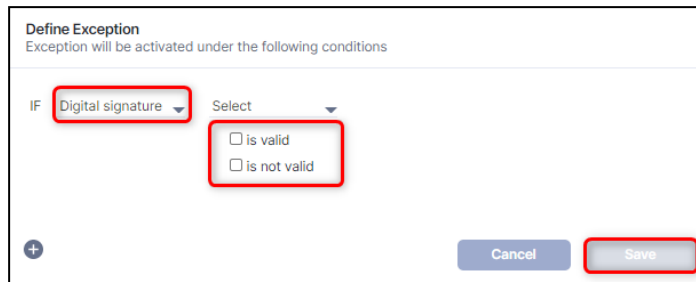
The screenshot shows a 'Define Exception' dialog box with the following elements:

- Title:** Define Exception
- Subtitle:** Exception will be activated under the following conditions
- IF:** A dropdown menu with 'File extension' selected.
- ends with:** A dropdown menu with 'ends with' selected.
- Text field:** A text input field containing '.xps'.
- Options:** A list of options: 'ends with' (checked) and 'doesn't end with' (unchecked).
- Buttons:** '+', 'Cancel', and 'Save'.

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 [See Adding an Exception](#): in this section.

Defining Exceptions for Validating Signatures



Define Exception
Exception will be activated under the following conditions

IF **Digital signature** Select

- is valid
- is not valid

+ Cancel Save

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