

VOTIRO[✓]

Votiro Cloud V9.6.3

User Guide

February 2022

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	6
1.1 Votiro Cloud Technology	6
1.2 System Architecture and Data Flow	6
1.3 Positive Selection® Engine	7
1.4 Supported File Types	8
2 Installing Votiro Cloud	15
2.1 Deployment Specifications	15
2.2 Prerequisites and Considerations	15
2.2.1 Ports	16
2.2.2 Virtual Appliance Communication Settings	16
2.2.3 Syncing with an NTP Server	17
2.2.4 Using an External Storage Server	17
2.2.5 Load Balancing	17
2.2.6 Votiro Registry in Azure	18
2.3 Configuring HTTPS Traffic via a Proxy Server without Authentication on a CentOS 7 VM	18
2.3.1 Proxy Server Secure Communication	18
2.3.2 Proxy Server Information	18
2.3.3 Configuration Procedure	19
2.4 Deploying an OVF	21
2.5 Configuring the Network Environment	24
2.6 Deploying Votiro Cloud	25
2.7 Logging in to the Management Dashboard	26
2.7.1 Configuring Authentication to Active Directory	27
2.8 Configuring Password Protected Files Portal	27
2.8.1 Customizing PPF Message	28
2.8.2 Customizing the PPF Portal Logo	28
3 Using the Management Dashboard	29
3.1 Monitoring Positive Selection Activity	30
3.1.1 Monitoring Periods	32

3.1.2 Live Status	33
3.1.3 Incoming Traffic	34
3.1.4 Secure File Gateway	34
3.1.5 Protection & Business Productivity	35
3.1.6 Test File	36
3.2 Exploring Incidents	36
3.2.1 Viewing Detailed File Information	38
3.2.2 Using Filters	39
3.2.3 Searching Positive Selection Requests	40
3.2.4 Releasing Files	40
3.3 Configuring Settings	43
3.3.1 System Configuration	43
3.3.2 Active Directory	45
3.3.3 SMTP	47
3.3.4 SAML	49
3.3.5 Users	50
3.3.6 SIEM	52
3.3.7 Service Tokens	53
3.3.8 License	56
3.3.9 Policies	58
3.4 Cloud Connectors and Integrations	60
3.4.1 AWS S3	60
3.4.2 Menlo Security	67
3.4.3 Fortinet Sandbox	70
3.5 Generating Reports	72
3.5.1 Summary Report	73
3.5.2 Audit Report	76
3.5.3 System Report	78
3.5.4 Diagnostics Report	80
Appendix A Sending Logs to SIEM in CEF	82
Appendix B Defining Policies by Case	88

Appendix C Defining Policies by File Type 91

Appendix D Adding Policy Exceptions 95

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.

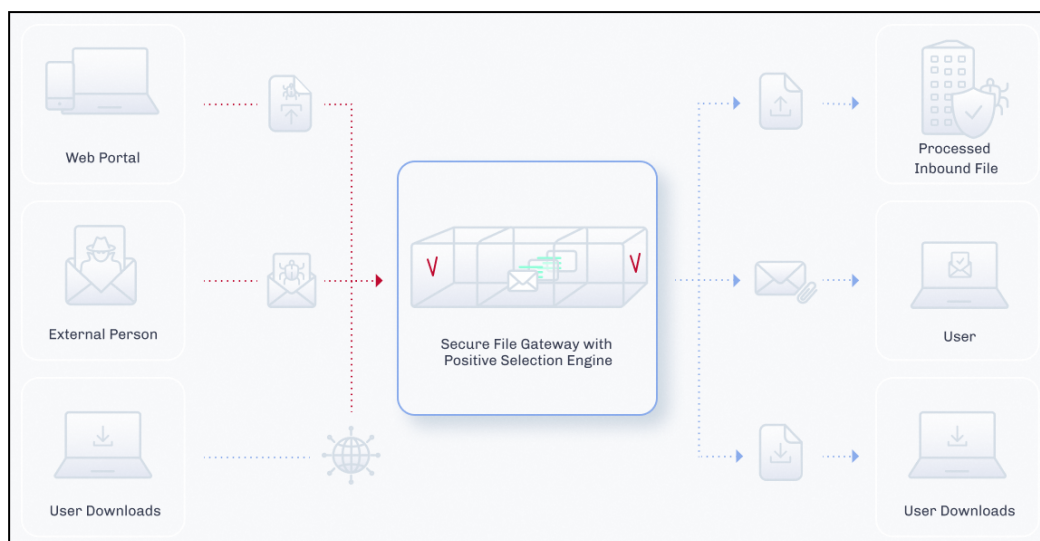
True Type Detection

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 can be blocked to prevent malicious content exploits.

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

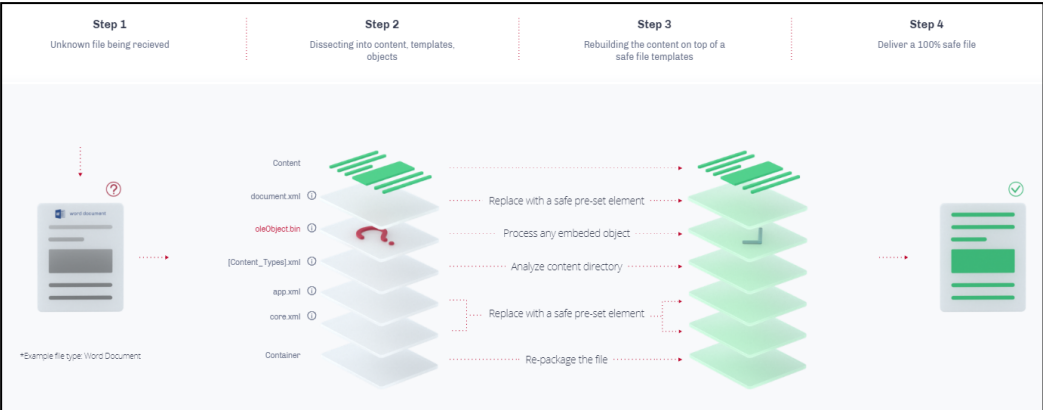
Votiro's Positive Selection® Engine is at the heart of the Votiro Cloud solution. The Positive Selection® Engine keeps only what belongs instead of searching for what does not belong.

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, wmf, 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
Binary	Binary File ^	Any Binary Files	dat, db
	Executable ^	Any Binary Files	exe, com, dll, pif, sfx, msu, msp, msi, mo
Archive	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
	ZIP File	Archives	zip
RTF	RTF Files	RTF Files	rtf

File Type in Management	File Type	Family Type	Main Extension
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
	MSG File	MSG Files	msg
	PST ^	PST Files	pst
	PST ANSI ^	PST Files	pst
	TNEF Calendar Files **	EML Files	eml
	TNEF File **	EML Files	eml
Microsoft Office	Excel	Microsoft Office	xls, xlt, xml
	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

File Type in Management	File Type	Family Type	Main Extension
	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 With Macros	Microsoft Office with Macros	pptm
	PowerPointXML ^	Microsoft Office	xml
	Printer Settings	Microsoft Office Embedded Files	bin
	Project ^	Microsoft Office	mpp
	Unknown Ole Object (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 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

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
File Type in Management	File Type	Family Type	Main Extension
Other	ACIS Solid Model File ^	CAD Files	sat
	Adobe Air ** ^	Adobe	air
	CD Audio Track Shortcut File ** ^	Media Files	cda
	CSS ^	CSS	css
	DB Files ^	Database Files	dbf, npa, dbt, wnd, tab, mdb
	Embedded Macro Files ^	Embedded File	bin
	Empty File ^	None	
	Equation Ole Object ^	OLE Object	bin
	Excel2, Excel3, Excel4, Excel5 ^	Office Files	xls
	HTML Attachments ^	HTML Files	html, htm
	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

File Type in Management	File Type	Family Type	Main Extension
	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	mxr
	Media File ^	Media Files	mp3, wav, wmv, ico, mpg, mpeg, flv, wma, mov, avi, mp2, mp4, m4a, 3gp, mts, mkv, vob
	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
	RPT ** ^	RPT Files	rpt
	RSP File ** ^	PLC Files	rsp
	Script ^	Batch Files	bat, js, php, cmd, vbs, reg, pl, lnk, py, asp
	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 will see the file size limitations are currently significant sizes.
 - ◆ Archives - 2 GB
 - ◆ Video - 2 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

2 Installing Votiro Cloud

To install Votiro Cloud quickly into your organization we will create a cluster of virtual machines (VM). We will use static IPs, one for each of the VMs and a VIP for the cluster. Each VM requires dedicated resources, see [Deployment Specifications](#) below.

To install Votiro Cloud and login to start using the Management Dashboard, follow these four steps:

- Deploy an OVF
- Configure the Network Environment
- Deploy Votiro Cloud
- Login to the Management Dashboard

IMPORTANT!

You may need to determine in advance of your installation the following:

- Unique IP addresses: one per VM, and a VIP for the cluster;
- Hostname for FQDN (use lower case alphanumeric characters).

2.1 Deployment Specifications

The following deployment specifications are for the installation of Votiro Cloud with a 3 node cluster. Scale specifications as you increase the number of nodes in your cluster.

The expected maximum performance for this configuration is 35,000 files per hour.

Table 2 Deployment Specifications

Votiro Cloud	3 Node Cluster
CPU Cores	8 per node
RAM	16 GB per node
Drive Capacity	200 GB per node, SSD
Remote Storage Support	File Storage Network. For example, SAN, NAS
Hypervisor Support	VMWare ESXi 6, Amazon Web Services, Microsoft Azure
Network Adapters	4 - 1 per node + 1 global VIP with DNS name

2.2 Prerequisites and Considerations

There are both prerequisites and a number of topics for you to consider when implementing Votiro Cloud into your environment. See sections for more details:

- [Ports](#)
- [Virtual Appliance Communication Settings](#)
- [Syncing with an NTP Server](#)

- [Using an External Storage Server](#)
- [Load Balancing](#)
- [Votiro Registry in Azure](#)

2.2.1 Ports

Network connectivity requirements enabling secure outbound and inbound communications with Votiro Cloud are detailed in the tables below.

Table 3 Outbound Firewall Rules

Outbound	Source	Destination	Port Number	Transport Protocol
Releasing Files	ovf_network	Exchange / Edge	25	tcp
Active Directory	ovf_network	Domain Controller <ul style="list-style-type: none"> ■ LDAP ■ LDAPS 	<ul style="list-style-type: none"> ■ 389 ■ 636 	<ul style="list-style-type: none"> ■ tcp ■ tcp
SIEM	ovf_network	SIEM Server	514	udp

Table 4 Inbound Firewall Rules

Inbound	Source	Destination	Port Number	Transport Protocol
SSH, SCP	Any	ovf_network	22	tcp
Processing Request	API Client	ovf_network	443	tcp
Monitoring Grafana	Grafana	ovf_network		
Monitoring Prometheus	Prometheus			

2.2.2 Virtual Appliance Communication Settings

Internal Communication Settings

For internal communications between nodes of each machine inside the VLAN, the following settings are required:

- 22/tcp
- 25/tcp
- 389/tcp (LDAP)
- 636/tcp (LDAPS)
- 2379-2380/tcp
- 6443/tcp
- 10250-10252/tcp
- 10255/tcp

- 24007 – 24008/tcp
- 49152 – 49154/tcp
- 123/udp (See [Syncing with an NTP Server below](#)).
- 514/udp
- 8472/udp

External Communication Settings

For external communications, the following settings are required:

- 22/tcp
- 443/tcp

2.2.3 Syncing with an NTP Server

When using an NTP server, as a pre-requisite you must sync with it using port **123/udp**.

2.2.4 Using an External Storage Server

In addition to the virtual appliance machines' internal storage, you can use an external storage server. Votiro Cloud can be configured to communicate with your storage server, using a mount from the external storage to the virtual appliance machines.

When external storage is configured it is used as the main storage area. Storage will contain a set of original and processed files.

The mount created results in the true storage type, such as SAN and NAS, being transparent, leading to Votiro Cloud supporting all External Storage types.

For instructions on how to configure External Storage, contact Votiro's Support team.

Note

The internal storage requirement remains at 200 GB per node. It is available for use should the external storage server link fail. Stored files are transferred from the VM to the external storage server when it becomes available.

2.2.5 Load Balancing

Votiro Cloud automatically supports load balancing using a basic internal load balancer.

Note: An external hardware-based load balancer is required in your production environment to balance between the nodes of your VM.

WARNING!

If the number of nodes reduces to two, Votiro Cloud will continue working for a maximum of two hours before processing stops.

2.2.6 Votiro Registry in Azure

This consideration is relevant when your Votiro Cloud installation includes an online environment.

To enable secure communication with your Votiro appliance, the proxy server ACL must include permission for the Votiro registry in the Azure URL.

2.3 Configuring HTTPS Traffic via a Proxy Server without Authentication on a CentOS 7 VM

Many organizations have their internet traffic routed via a proxy server rather than by direct connection from a virtual machine.

This page describes how to configure HTTPS Traffic via a proxy server without authentication on a CentOS 7 Virtual Machine.

2.3.1 Proxy Server Secure Communication

To enable secure communication between your Proxy server and Votiro's Positive Selection® Engine, set permissions by creating an ACL that includes the following locations:

- *.prod.votiro.com
- *.blob.core.windows.net

2.3.2 Proxy Server Information

Before you start the procedure, determine the following information:

- IP address of your Proxy server.
- Port number of the Proxy server used for HTTPS traffic.
- List of addresses/networks to bypass in the no_proxy setting.

■ **IMPORTANT!**

By default, all HTTPS traffic will be routed to the proxy. We want to avoid the default routing scenario because HTTPS is used for internal traffic not to be routed to the internet.

By default, when running *init* cluster, several networks are created.

First node:

- 172.17.0.1/16 docker0
- 10.244.0.0/32 flannel
- 10.244.0.1/24 cni0

The *flannel* and *cni* networks will also be created on the second and third nodes, using different IPs in their subnet.

Second node:

- 10.244.1.0/32
- 10.244.1.1/24

Third node:

- 10.244.2.0/32
- 10.244.2.1/24

Note

All of the above networks and IP addresses will be used for internal purposes, and will need to bypass the proxy.

2.3.3 Configuration Procedure

Before you begin, ensure the proxy server permissions have been set on the required locations and you have gathered the required proxy server information.

To set and configure your three nodes, follow these steps:

1. SSH to the first node in the cluster.
2. Modify the hosts file using the command:

```
vi /etc/hosts
```

This step is mandatory because the **no_proxy** parameter does not allow the use of wildcards.

3. Add the following records:
 - ◆ 172.17.0.1/16 docker
 - ◆ 10.244.0.0 flannel
 - ◆ 10.244.0.1/24 node0net
 - ◆ 10.244.1.1/24 node1net
 - ◆ 10.244.2.1/24 node2net
4. Route HTTPS traffic via Proxy to ensure the Linux OS Layer is covered by adding the following proxy settings:

- a. Enter edit mode to `/etc/environment`, using the following command:

```
vi /etc/environment
```

- b. Add the following data:

```
https_proxy=http://{Proxy-Server-IP}:{Proxy Port}
```

```
no_proxy={cluster name},{node#X IP},localhost,  
docker,cni,flannel,node0net,node1net,node2net,  
10.244.0.0,10.244.1.0,10.244.2.0
```

For example:

```
https_proxy=http://10.130.1.168:3128  
  
no_proxy=support-va,10.130.1.163,localhost,  
docker,cni,flannel, node0net,node1net,node2net,  
10.244.0.0,10.244.1.0,10.244.2.0
```

5. Create proxy settings for the Docker layer, using the following command:

```
mkdir /usr/lib/systemd/system/docker.service.d
```

6. Create a new drop-in file, using the following command:

```
vi /usr/lib/systemd/system/docker.service.d/http-proxy.conf
```

7. Add the following data:

```
[Service]  
  
#Environment="HTTP_PROXY=http://10.130.1.168:3128/"  
Environment="HTTPS_PROXY=http://10.130.1.168:3128/"  
Environment="NO_PROXY= hostname.example.com,172.10.10.10"
```

8. Reload and restart the node, using the following commands:

```
sudo systemctl daemon-reload  
  
sudo systemctl restart docker
```

9. Once the node is reloaded check the settings were successfully applied, using the following command:

```
sudo systemctl show --property=Environment docker
```

You should receive the following output:

```
Environment=HTTPS_PROXY=http://10.130.1.168:3128/ NO_PROXY=  
hostname.example.com,172.10.10.10
```

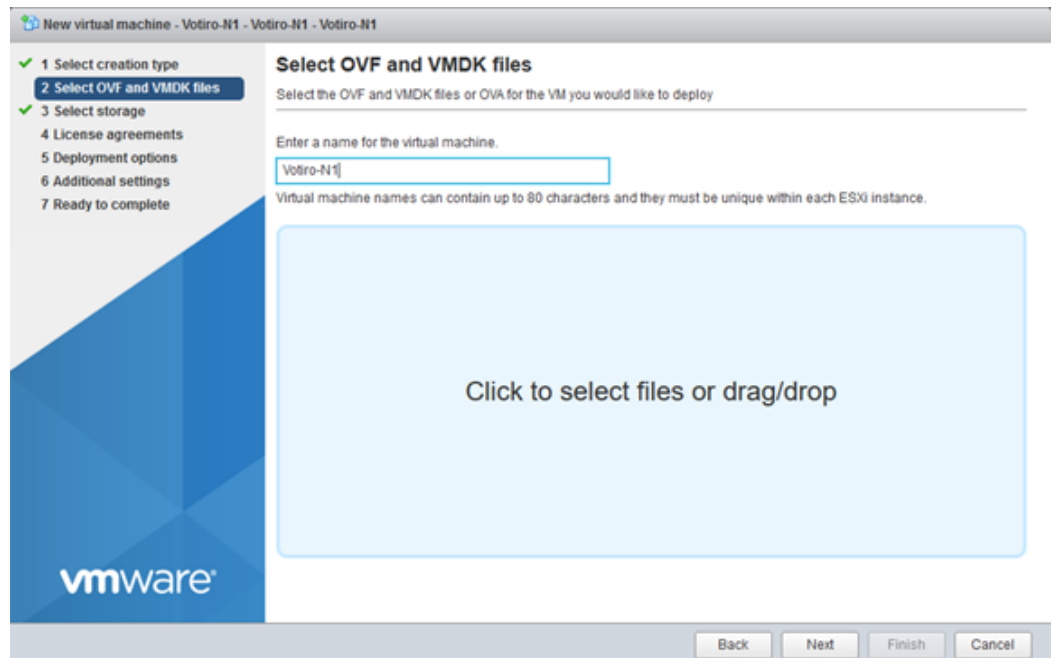
■ IMPORTANT!

Repeat Steps 1 to 9 above for the other two nodes.

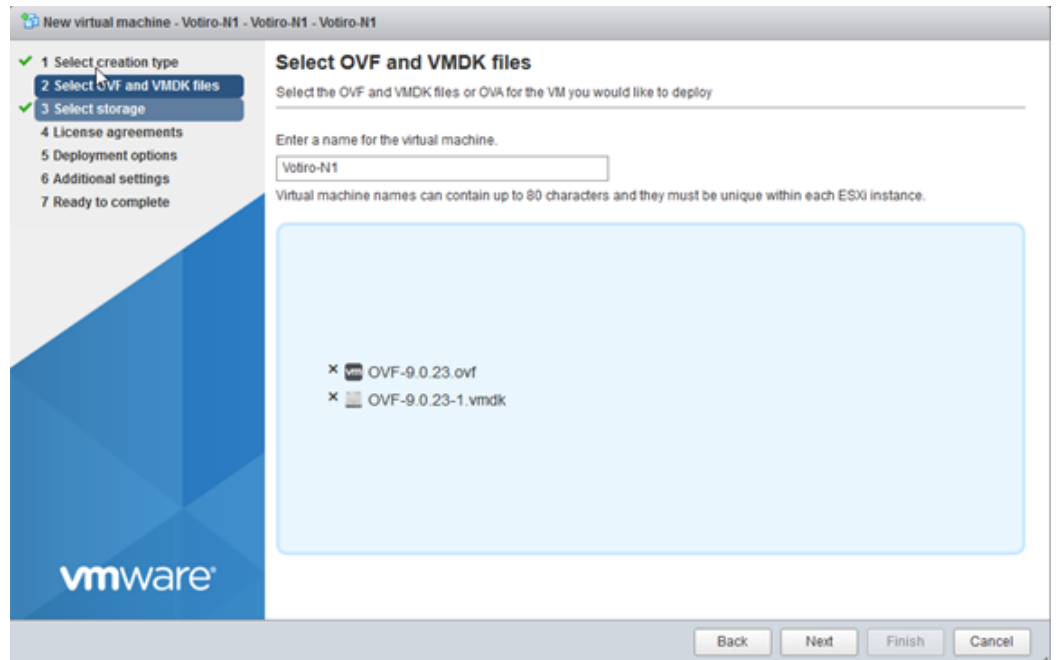
2.4 Deploying an OVF

In this step you will create the virtual machines. You will require a virtual machine for each node in your cluster.

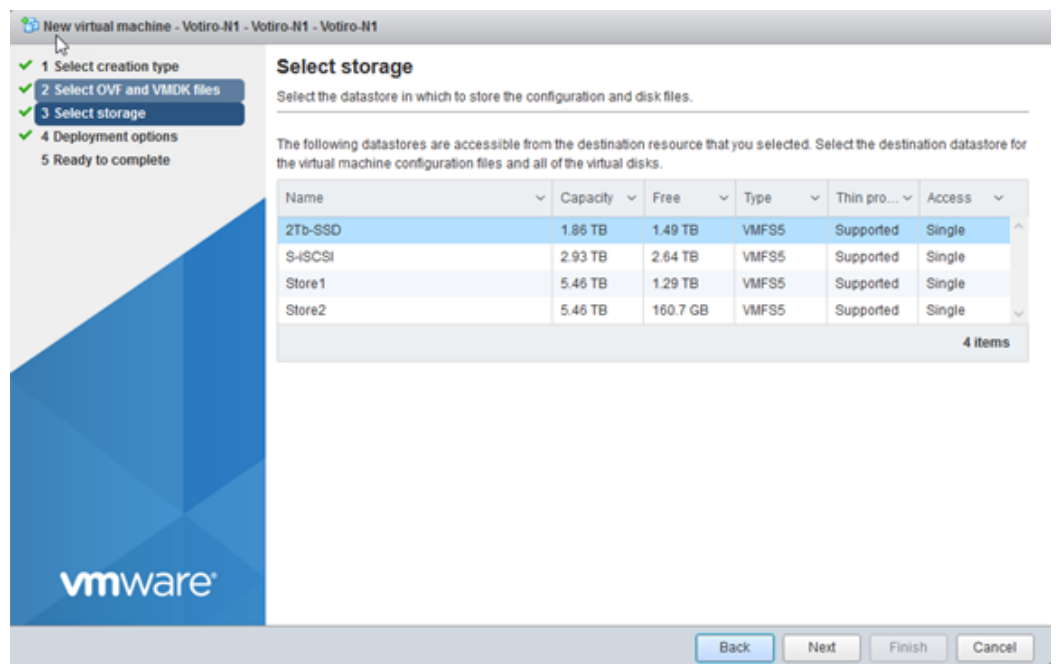
1. Deploy **OVFs**, using these specifications:
 - ◆ 8 CPU
 - ◆ 16 GB Memory
 - ◆ 200 GB Storage
2. Name each **node** uniquely using your corporate naming conventions.



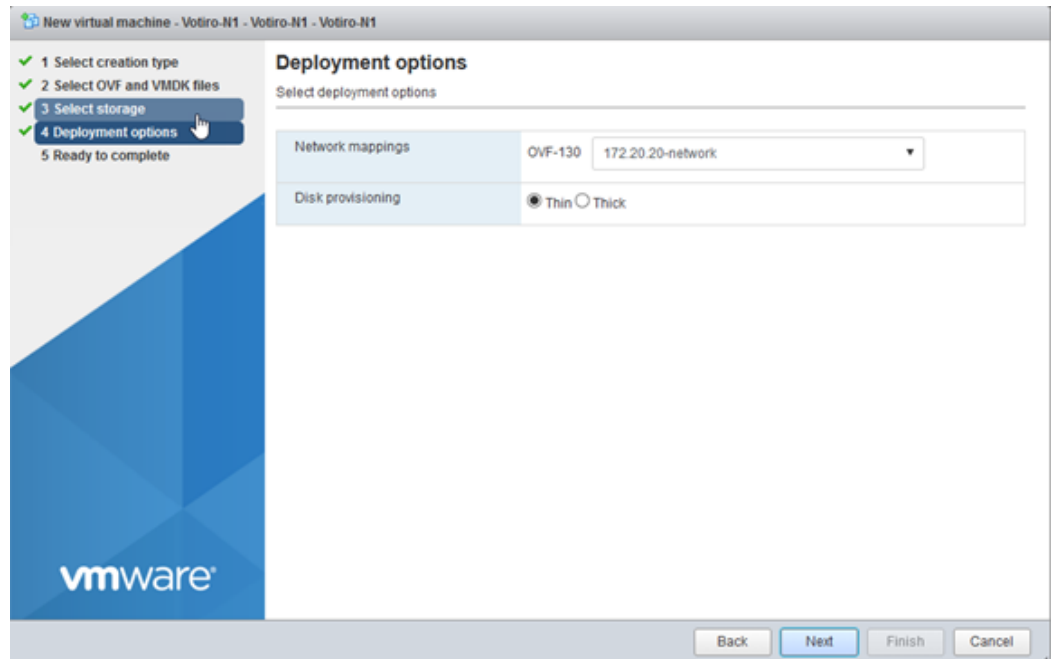
3. Select the **OVF** and **VMDK** files during deployment.



4. Select your preferred storage location. It is recommended you use **SSD storage**.



5. Select the network you would like to deploy the appliances on. You may select **Thin** or **Thick** provisioning. 200GB of storage is required for each appliance.

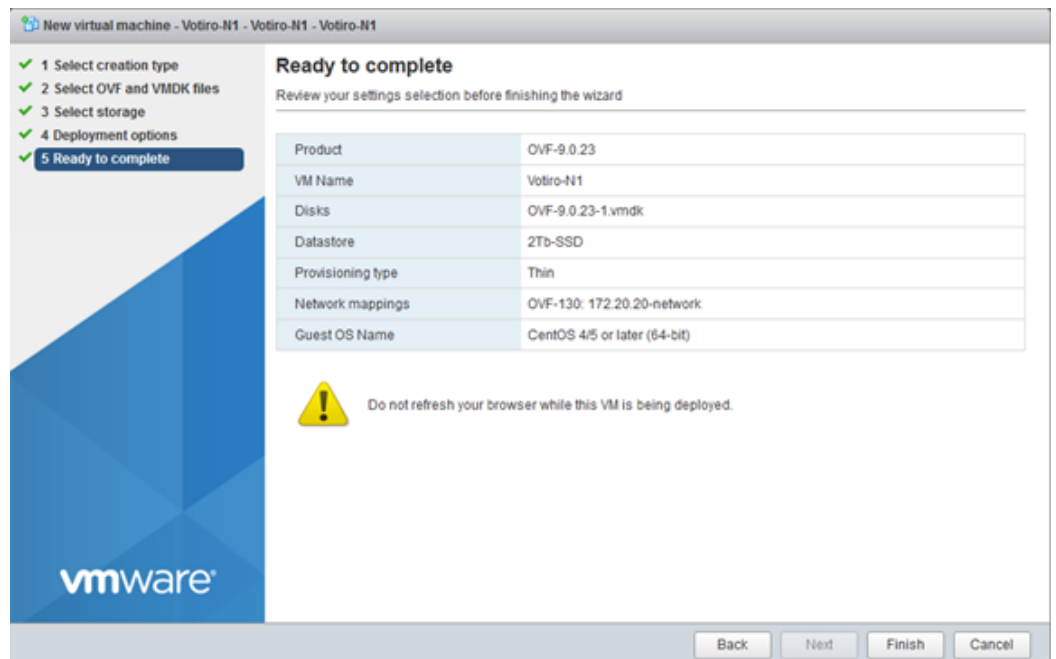


The screenshot shows the 'New virtual machine' wizard in VMware vSphere, specifically the 'Deployment options' step. The left sidebar shows a progress bar with five steps: 1. Select creation type, 2. Select OVF and VMDK files, 3. Select storage, 4. Deployment options (highlighted), and 5. Ready to complete. The main area is titled 'Deployment options' and contains a table for 'Select deployment options'.

Select deployment options	
Network mappings	OVF-130 172.20.20-network
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick

At the bottom of the wizard, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

6. To complete the deployment, click **Finish**.



The screenshot shows the 'New virtual machine' wizard in VMware vSphere, specifically the 'Ready to complete' step. The left sidebar shows a progress bar with five steps: 1. Select creation type, 2. Select OVF and VMDK files, 3. Select storage, 4. Deployment options, and 5. Ready to complete (highlighted). The main area is titled 'Ready to complete' and contains a table for 'Review your settings selection before finishing the wizard'.

Review your settings selection before finishing the wizard	
Product	OVF-9.0.23
VM Name	Votiro-N1
Disks	OVF-9.0.23-1.vmdk
Datastore	2Tb-SSD
Provisioning type	Thin
Network mappings	OVF-130: 172.20.20-network
Guest OS Name	CentOS 4/5 or later (64-bit)

Below the table, there is a yellow warning icon and the text: 'Do not refresh your browser while this VM is being deployed.'

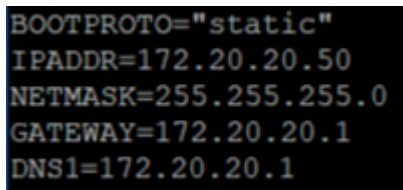
At the bottom of the wizard, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

There are now three or five virtual machines (VM).

2.5 Configuring the Network Environment

In this step you will configure network settings for each virtual machines.

1. Log in to each VM, use **root** as **login ID** and **password**.
2. Configure each VM with a static IP, Gateway and DNS server.
3. Set a **static IP** on CentOS as follows:
 - a. #ssh into the appliance and run the following command:

```
vi /etc/sysconfig/network-scripts/ifcfg-ens160
```
 - b. Select **I** for insert mode.
 - c. Modify the following fields:


```
BOOTPROTO="static"
IPADDR=172.20.20.50
NETMASK=255.255.255.0
GATEWAY=172.20.20.1
DNS1=172.20.20.1
```
 - d. To save the settings, click **Esc** and **:wq**, then click **Enter**.
 - e. For the settings to take effect, use the following command:

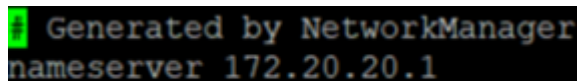
```
service network restart
```
4. For your appliance to access the internet define a **nameserver** using lower case alphanumeric characters.

Note

This step must be performed prior to [See Deploying Votiro Cloud](#)

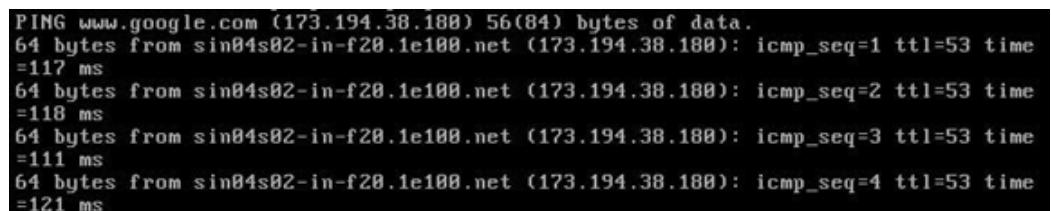
- a. To open the **resolv config** file with an editor, use the following command:

```
vi /etc/resolv.conf
```
- b. Select **I** for insert mode.
- c. At the prompt, enter **nameserver <your_dns>**.



```
Generated by NetworkManager
nameserver 172.20.20.1
```

5. Test the server. For example, enter **Ping google.com**.



```
PING www.google.com (173.194.38.180) 56(84) bytes of data.
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.180): icmp_seq=1 ttl=53 time
=117 ms
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.180): icmp_seq=2 ttl=53 time
=118 ms
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.180): icmp_seq=3 ttl=53 time
=111 ms
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.180): icmp_seq=4 ttl=53 time
=121 ms
```


6. To change node names, use the following command:

```
hostnamectl set-hostname <VotiroN1>
```

Repeat this step on all nodes.

Your machines are now configured and connected to your network.

IMPORTANT!

We recommend you change the root password on all nodes.

2.6 Deploying Votiro Cloud

1. To deploy Votiro Cloud, select one of the machines and run the command:

```
./initcluster.sh
```

2. Verify that a DNS is configured by checking the file `/etc/resolve.conf`.

Note

If a DNS is not configured, cluster deployment will fail.

3. Agree to Terms and Conditions, and continue installation, then enter **Y**.

```
This Agreement may not be altered except by agreement in writing executed by an authorized representative of each party.
If you have any questions regarding this Agreement, please call Votiro at +972-73-7374102 or send inquiries via electronic mail to: info@votiro.com.

Type (Y)es to state you have read and agree to the Terms and Conditions. (N)o to cancel: y

Enter Votiro Cluster VIP: 10.130.1.33
Enter Votiro Cluster FQDN: king-va
Would you like to use the online mode (internet connection is required) (Y)es/(N)o ? y
Restarting Docker: Ok
Restarting Kubelet: Ok
Initializing Kubernetes (Please wait): Ok
Copying Kubernetes Configs: Ok
Setting up Kubernetes network: Ok
Connecting Kubernetes nodes...
Enter node ip (leave empty to end): 10.130.1.31
Connecting node 10.130.1.31...
Ok
Enter node ip (leave empty to end): 10.130.1.32
Connecting node 10.130.1.32...
Ok
Enter node ip (leave empty to end):
Preparing all nodes: Ok
```

Note

IP addresses are required for the installation: one per machine plus one for the VIP.
For example, a 3-node cluster will need 4 IP addresses.

4. Enter the **VIP** for the Votiro Cloud cluster.
5. Enter the Votiro Cloud's **FQDN**, using lower case alphanumeric characters.
6. The **online mode** setting allows the reputation of a link to be checked, ensuring the destination is safe. Links in the form `HTTP://` and `HTTPS://` are checked, if found to be suspicious the link is removed from the file.

To select how to process files with links, use the **online mode** setting:

- a. To send links to scan, enter **Y**.
- b. To not send links to scan, enter **N**.

An internet connection is required to send links to be scanned.

- When using an external storage server, ensure all nodes in the cluster have read/write permissions. For additional information, see [Using an External Storage Server on page 17](#).

- ```

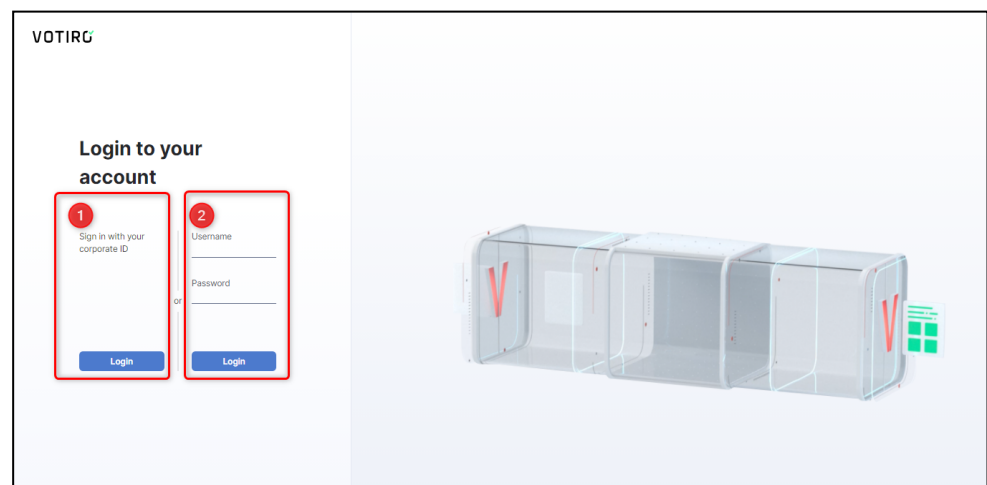
+-----+
| Please keep the following encryption keys in a safe place, they cannot be retrieved. |
+-----+
| KEY - 8710F202050211F7F0C811707064F0A0B |
| IV - 1A710C00190304020 |
| SALT - 7030000102070000 |
+-----+

```

To login to the Management Dashboard, see [Logging in to the Management Dashboard below](#).

To begin using Votiro Cloud's Management Dashboard:

- The login screen is displayed.



2. Select the login option preferred by your organization.

1. For SSO and to use your Corporate ID, click **Login** on the left side.

Or

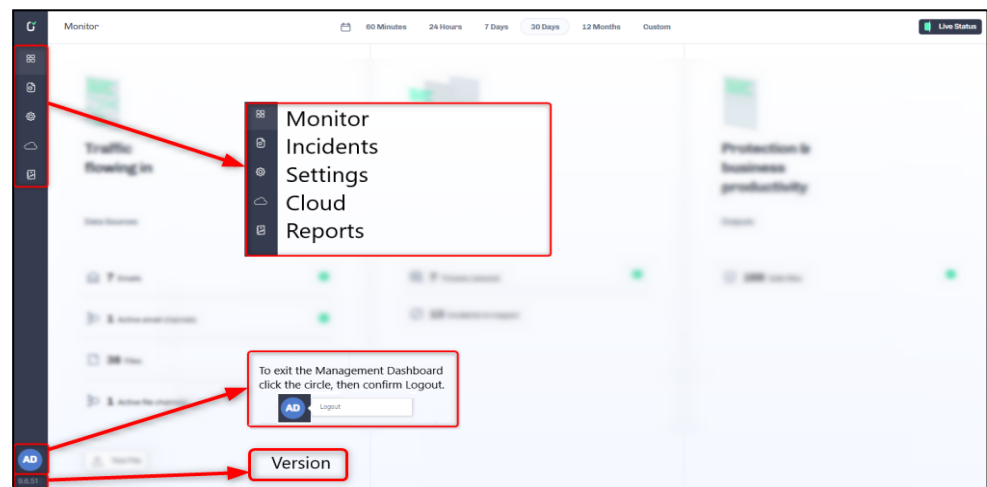
2. Type in the *username* and *password*. Click **Login** on the right side.

The *username* and *password* are the same credentials used by the user for the Active Directory server.

Examples of a *username*: VT\Jane.Smith, Jane.Smith@Votiro.com.

For further details about *usernames* and *passwords*, see the Active Directory section in the Votiro Cloud User Guide.

The Management Dashboard is displayed.



### 2.7.1 Configuring Authentication to Active Directory

Following the successful installation of Votiro Cloud, you can configure authentication to Active Directory. Define a Group and User for Votiro Authentication in Active Directory. This should be a service account with standard privileges.

#### Note

The user must be in the predefined Votiro Group.

## 2.8 Configuring Password Protected Files Portal

The Password Protected File (PPF) Portal is where the recipient of a password protected file can enter the password so the file can continue being processed by the Positive Selection® Engine engine.

You can customize the interactions between Votiro Cloud and your users, so the message is consistent with your organization's branding and style.

The root folder of your VM has an **Extras** folder, containing the following files and commands:

- Blocked\_Ppf.rtf

- Blocked.rtf
- update-block-pdf-template.sh
- update-password-protected—portal-logo.sh

You can replace the default **rtf** files with documents customized to represent your organization. Then run the command to update Votiro Cloud.

### 2.8.1 Customizing PPF Message

A message will be sent to the recipient of a PPF advising them that when they enter the password of their PPF it will be processed for positive selection, then released. This message is created from the **Blocked\_Pdf.rtf** file. You can make changes to this file and maintain consistency with your organization's branding and messaging style.

The **Blocked\_Pdf.rtf** file is used when you update the PDF. The file name must remain the same. Update Votiro Cloud from the same folder, using the following command:

```
./ update-block-pdf-template.sh
```

The PDF will be updated and used instead of the default file.

### 2.8.2 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.

## 3 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](#)
- [Generating Reports](#)

### To log in to the Management Dashboard:

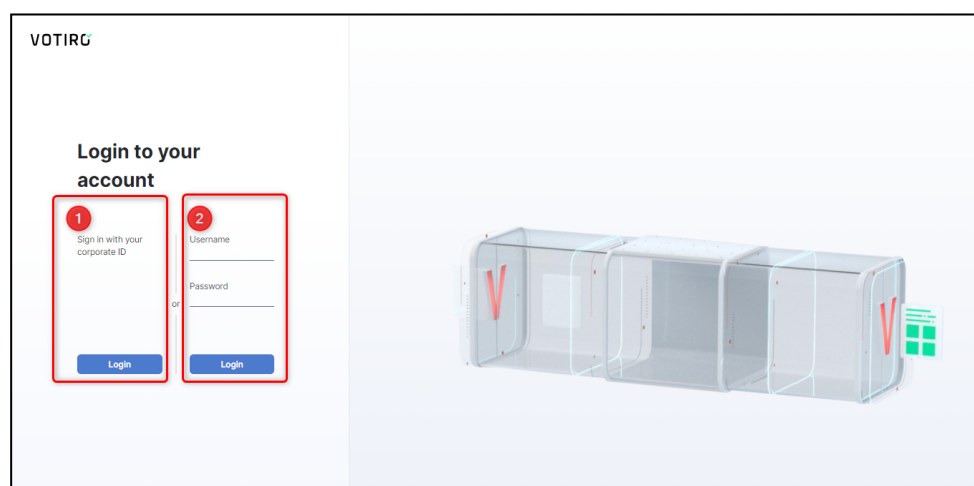
If you have configured the Management Platform to use Active Directory, only users that appear in the Active Directory group can log on.

1. On the server that is hosting the Management Platform, open a browser and navigate to:

`https://[appliancename]`

where *appliancename* is the name of the Votiro cluster FQDN hosting the Management Platform.

The login screen is displayed:



2. Select the login option preferred by your organization.

1. For SSO and to use your Corporate ID, click **Login** on the left side.

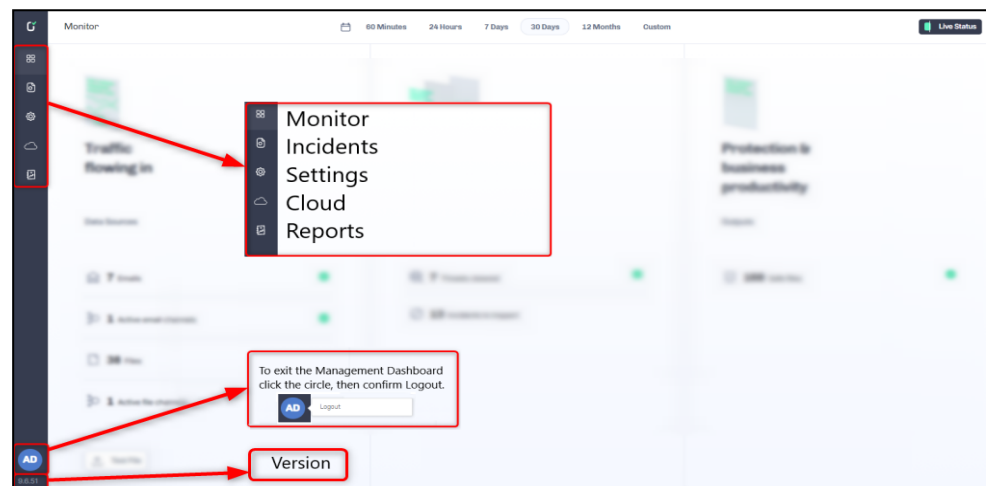
Or

2. Type in the *username* and *password*. Click **Login** on the right side.

The *username* and *password* are the same credentials used by the user for the Active Directory server.

Examples of a *username*: VT\\Jane.Smith, Jane.Smith@Votiro.com.

The Management Dashboard displays.



#### Note

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

## 3.1 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.

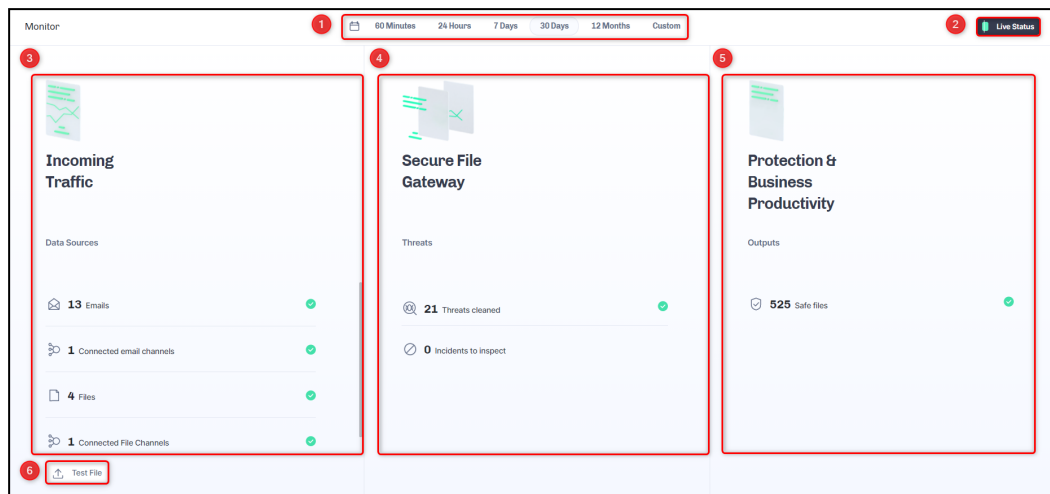
There can be more than one recent activity message for a single file if it contains more than one threat. For example, the file can contain a suspicious URL and a suspicious macro.

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

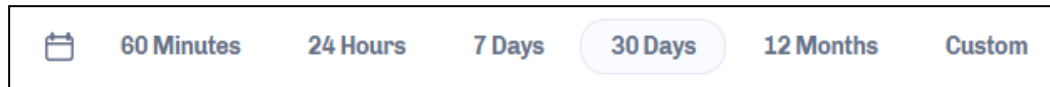
## ■ Protection & Business Productivity



| Element | Area                               | Description                                                                                                                                                                                                        |
|---------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | Monitoring Periods                 | Select the time period you wish to display monitoring information for.<br><br>See <a href="#">Monitoring Periods on the next page</a> .                                                                            |
| 2       | Live Status                        | Displays the most recent file traffic event activity flowing through Votiro Cloud.<br><br>See <a href="#">Live Status on page 33</a> .                                                                             |
| 3       | Incoming Traffic                   | Displays channel names and statistical details about files being processed for positive selection.<br><br>See <a href="#">Incoming Traffic on page 34</a> .                                                        |
| 4       | Secure File Gateway                | Displays analysis of threats found and cleaned in files being processed for positive selection.<br><br>See <a href="#">Secure File Gateway on page 34</a> .                                                        |
| 5       | Protection & Business Productivity | Displays performance details from a user's view, highlighting the positive business impact being experienced by using Votiro Cloud.<br><br>See <a href="#">Protection &amp; Business Productivity on page 35</a> . |
| 6       | Test File                          | Opens your File Manager and allows you to select a file for testing.<br><br>See <a href="#">Test File on page 36</a> .                                                                                             |

### 3.1.1 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.

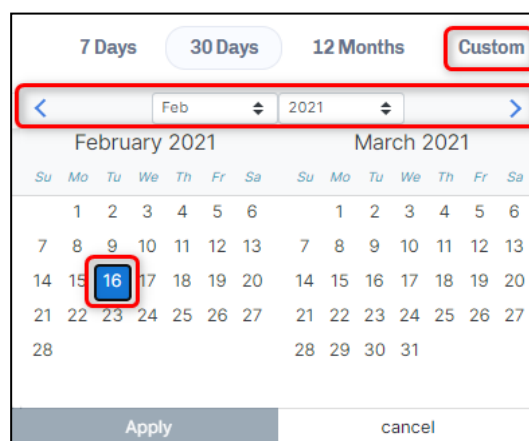


Votiro Cloud provides the following predefined settings:

| 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

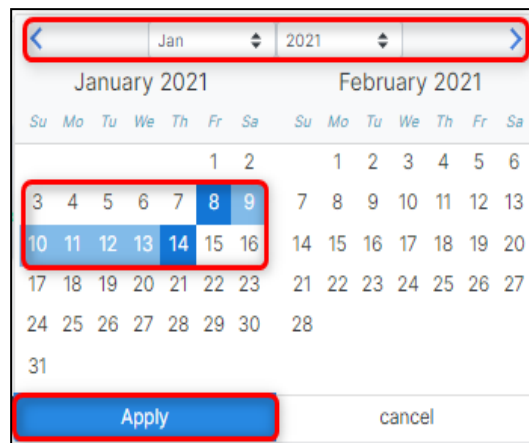
1. Click **Custom** to display the period selector.



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.



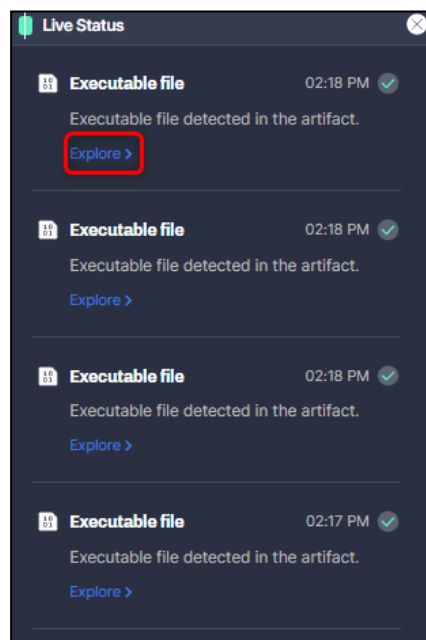
- To select an **end date**, tap a date on the calendar, the number turns blue.  
The selected period is highlighted.



- Click **Apply**.  
The custom period is displayed in the top left corner of the window:  
Statistics update to show information for the custom period.

### 3.1.2 Live Status

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

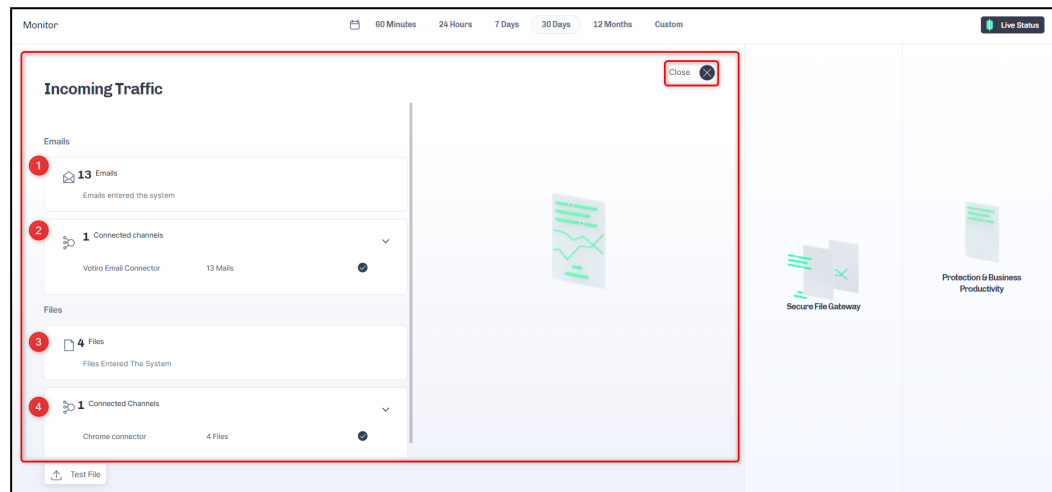


Click **Explore >** to view detailed information about the file, described in [Viewing Detailed File Information on page 38](#).

### 3.1.3 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.

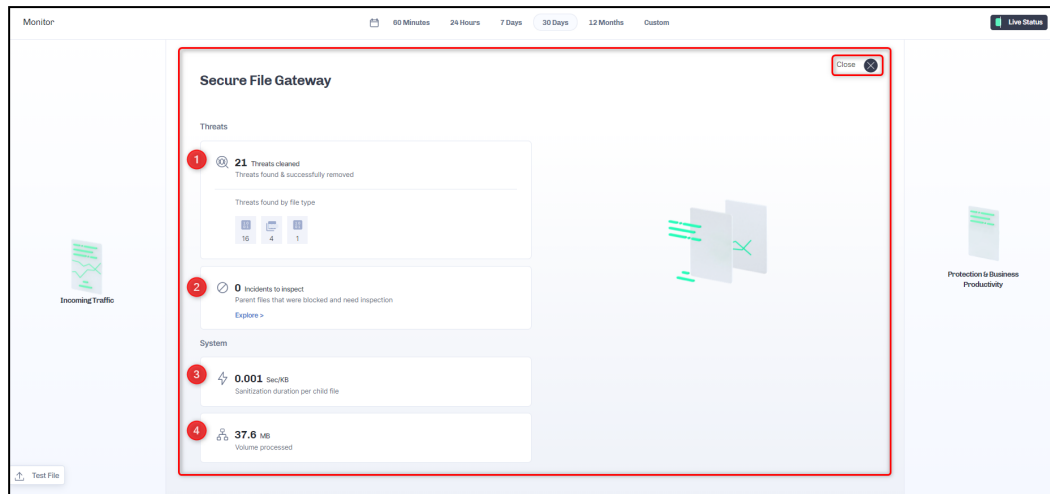


| Element | Meaning                    | Description                                                                                  |
|---------|----------------------------|----------------------------------------------------------------------------------------------|
| 1       | Emails          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

### 3.1.4 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.



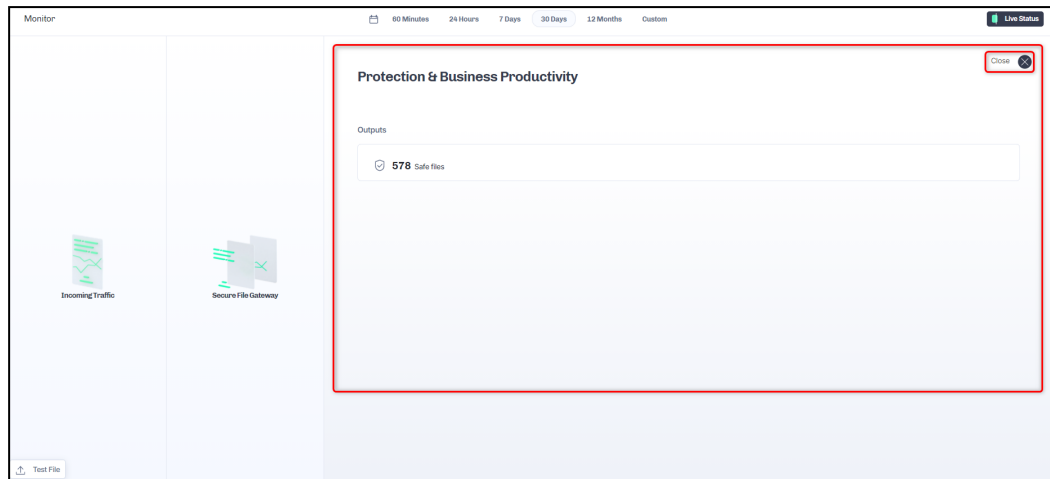
| Element | Feature                   | Description                                                                                                                                                                                             |
|---------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br>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.<br>To view details, click <b>Explore</b> .                                             |
| 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.

### 3.1.5 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. |

### 3.1.6 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.

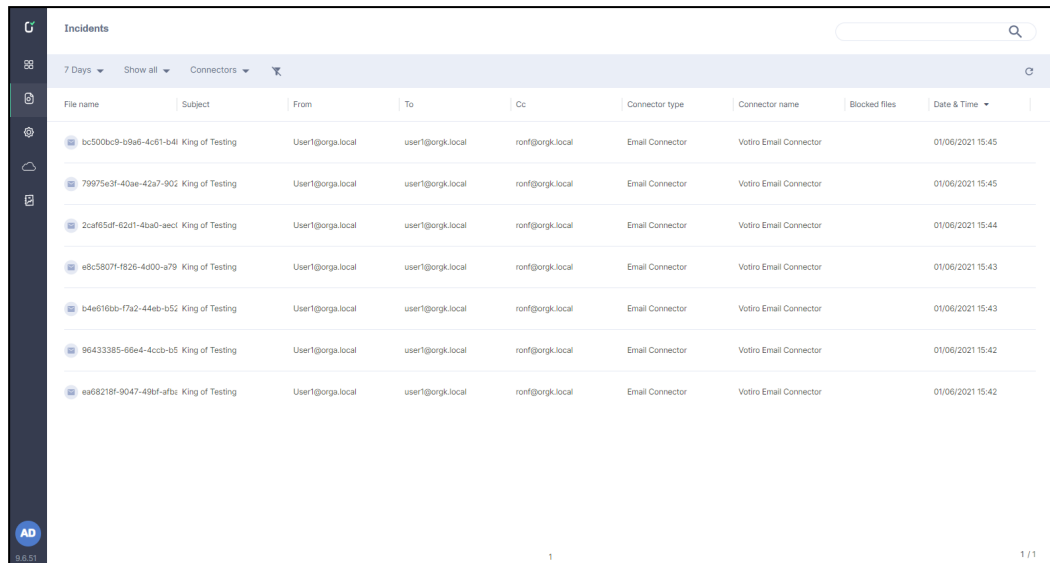
The file used for testing is stored and displayed as a regular file in Votiro Cloud. For further information, see [Viewing Detailed File Information on page 38](#).

## 3.2 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.

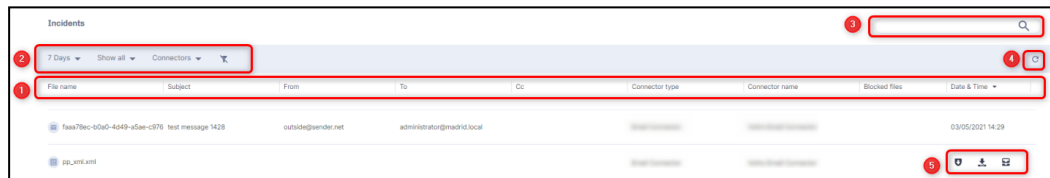
Use this page to explore incidents (blocked and processed files).



The screenshot shows the 'Incidents' page in the management dashboard. It features a search bar at the top right, a filter bar with '7 Days', 'Show all', and 'Connectors' options, and a table of incidents. The table has columns for File name, Subject, From, To, Cc, Connector type, Connector name, Blocked files, and Date & Time. The incidents listed are all 'King of Testing' emails from 'User1@orga.local' to 'user1@orgk.local' via 'Votiro Email Connector' on 01/06/2021.

| File name                   | Subject         | From             | To               | Cc              | Connector type  | Connector name         | Blocked files | Date & Time      |
|-----------------------------|-----------------|------------------|------------------|-----------------|-----------------|------------------------|---------------|------------------|
| bc500bc9-b9e6-4c61-b4f1-... | King of Testing | User1@orga.local | user1@orgk.local | ronf@orgk.local | Email Connector | Votiro Email Connector |               | 01/06/2021 15:45 |
| 79975e3f-40ae-42a7-902...   | King of Testing | User1@orga.local | user1@orgk.local | ronf@orgk.local | Email Connector | Votiro Email Connector |               | 01/06/2021 15:45 |
| 2caf65df-62d1-4ba0-aeed...  | King of Testing | User1@orga.local | user1@orgk.local | ronf@orgk.local | Email Connector | Votiro Email Connector |               | 01/06/2021 15:44 |
| e8c5807f-826-4d00-a79...    | King of Testing | User1@orga.local | user1@orgk.local | ronf@orgk.local | Email Connector | Votiro Email Connector |               | 01/06/2021 15:43 |
| b4e616b6-f7a2-44eb-b52...   | King of Testing | User1@orga.local | user1@orgk.local | ronf@orgk.local | Email Connector | Votiro Email Connector |               | 01/06/2021 15:43 |
| 96433385-66e4-4ccb-b5...    | King of Testing | User1@orga.local | user1@orgk.local | ronf@orgk.local | Email Connector | Votiro Email Connector |               | 01/06/2021 15:42 |
| ea68218f-9047-49bf-afbf...  | King of Testing | User1@orga.local | user1@orgk.local | ronf@orgk.local | Email Connector | Votiro Email Connector |               | 01/06/2021 15:42 |

The page provides the following features:



The screenshot shows the 'Incidents' page with red annotations. A red box highlights the filter bar (1). A red box highlights the search bar (2). A red box highlights the table header (3). A red box highlights the table body (4). A red box highlights the table footer (5). A red box highlights the table footer (6).

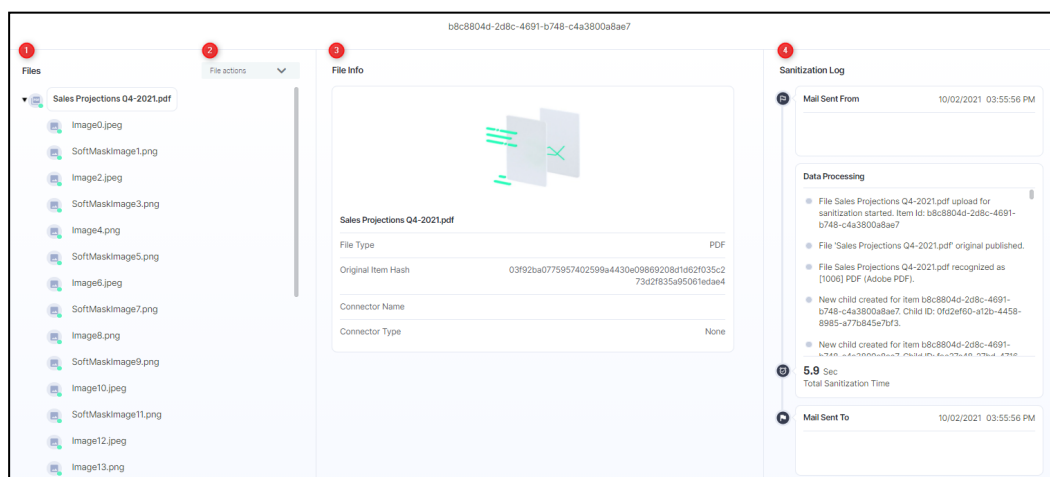
| Element | Feature      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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"> <li>File name</li> <li>Connector type</li> <li>Connector name</li> <li>Blocked files</li> <li>Date &amp; Time</li> </ul> <p>For email files (EML and TNEF formats), the following is also provided:</p> <ul style="list-style-type: none"> <li>Subject</li> <li>From</li> <li>To</li> <li>Cc</li> </ul> <p>For additional file information, tap in the file row.</p> <p>See <a href="#">Viewing Detailed File Information on the next page</a>.</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.<br><br>See <a href="#">Using Filters on the next page</a> .                                                                                                                                                                                                                                                                                                                          |
| 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.<br><br>See <a href="#">Searching Positive Selection Requests on page 40</a> .                                                                                                                                                                                                                                                                                        |
| 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"> <li>■ <b>Download original:</b> the file as it was received, before being processed for positive selection.</li> <li>■ <b>Download sanitized:</b> the processed version of the file, after being processed for positive selection.</li> <li>■ <b>Release original:</b> the original file or email is released. For additional information on releasing files, see <a href="#">Releasing Files on page 40</a>.</li> </ul> |

### 3.2.1 Viewing Detailed File Information

Detailed file information is displayed from:

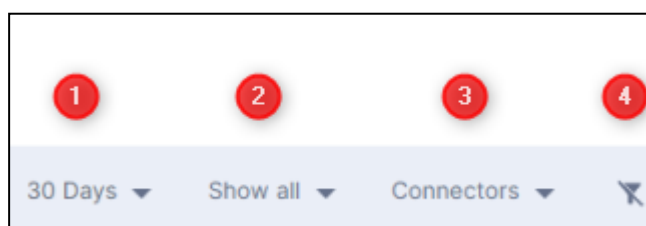
- The **Incidents** page, tap the row of the file to explore.
- The **Monitor** page's **Live Status** pane, click **Explore**.



| Element | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | <p><b>Files:</b></p> <p>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 <b>File Actions</b> list lets you perform the following actions for the file:</p> <ul style="list-style-type: none"> <li>■ <b>Explore Incidents:</b> return to the Incidents page.</li> <li>■ <b>Download original:</b> the file as it was received, before being processed for positive selection.</li> <li>■ <b>Download sanitized:</b> the processed version of the file, after being processed for positive selection.</li> <li>■ <b>Release original:</b> the original file or email is released. For additional information see <a href="#">Releasing Files on the next page</a>.</li> </ul> |
| 3       | <p><b>File Info:</b></p> <p>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"> <li>■ File Type</li> <li>■ Original Item Hash</li> <li>■ Connector Name</li> <li>■ Connector Type</li> </ul>                                                                                                                                                                                                                                                                               |
| 4       | <p><b>Sanitization Log:</b></p> <p>Provides sanitization log events that relate to the file that is currently selected in the left pane:</p> <ul style="list-style-type: none"> <li>■ <b>Mail Sent From:</b> populated with details only when files are processed from an Email connector.</li> <li>■ <b>Data Processing,</b> including Total Sanitization Time (in seconds). Use the scrolling bar on the right to see all child processing details.</li> <li>■ <b>Mail Sent To:</b> populated with details only when files are processed from an Email connector.</li> </ul>                            |

### 3.2.2 Using Filters

You can filter the file list in the following ways:



| Element | Filter            | Description                                                                                                                                                                                                                                                                                                |
|---------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | Monitoring Period | Select an option from the <b>Monitoring Period</b> list to filter according to a specific time period. The default is <b>7 Days</b> .<br><br>Select <b>Custom</b> to define a range of dates. For instructions on how to define a custom period, see <a href="#">Defining a Custom Period on page 32</a> . |
| 2       | Show              | Refines the list of files displayed, as follows: <ul style="list-style-type: none"><li>■ Show all (default)</li><li>■ Show blocked items</li><li>■ Show sanitized items</li><li>■ Show root blocked items.</li></ul>                                                                                       |
| 3       | Connector         | If you have more than one Votiro Cloud Connector installed, you can filter the file list by connector type using the <b>Connector</b> list.                                                                                                                                                                |
| 4       | Filter Icon       | Clears filter and returns to default setting.                                                                                                                                                                                                                                                              |

### 3.2.3 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.

### 3.2.4 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 page 43](#).

- 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:

**Release original email**

To

US user1@orgg.local ✕

Cc

Bcc

Release Cancel

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.

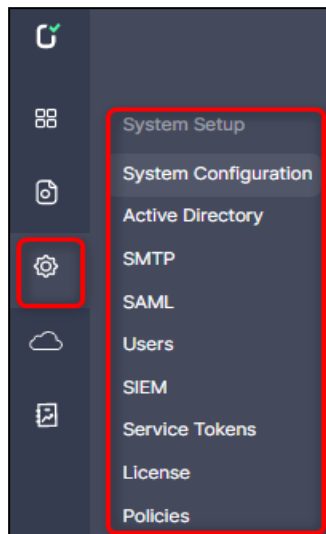
## To Release Multiple Emails:

| Incidents        |                              |                  |                  |                 |                  |                 |                        |               |  |  |
|------------------|------------------------------|------------------|------------------|-----------------|------------------|-----------------|------------------------|---------------|--|--|
| 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 | 796c5828-316-4a0a-f2d-4ec    | King of Testing2 | User1@orgg.local | king@orgg.local | user1@orgg.local | Email Connector | Votiro Email Connector | 2             |  |  |
| 18/11/2021 10:16 | MP protected .xlm            |                  |                  |                 |                  | File Connector  | Self-sanitization      | 1             |  |  |
| 18/11/2021 09:39 | SMB.helic                    |                  |                  |                 |                  | File Connector  | Self-sanitization      |               |  |  |
| 18/11/2021 09:39 | 6d70621c-1c42-4e77-b396-4ef  | King of Testing2 | User1@orgg.local | king@orgg.local | user1@orgg.local | Email Connector | Votiro Email Connector | 2             |  |  |
| 18/11/2021 09:24 | Out of document macro+FileSy |                  |                  |                 |                  | File Connector  | Self-sanitization      |               |  |  |
| 17/11/2021 14:50 | 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.

## 3.3 Configuring Settings

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



### 3.3.1 System Configuration

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

Settings

System Configuration

1

Company Name

Type in your company name

\* Name

Your company

2

File History

Select the number of days to keep files in storage

\* Days to keep

30

3

Password Protected File History

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

\* Days to keep

180

4

Date Format

Select your preferred date format

Date

DD/MM/YYYY

☒

5

Time Format

Select your preferred time format

Time

HH:mm

☒

6

System Language

Select your preferred system language

Language

en

☒

The System Configuration page contains the following fields:

| Element | Field                           | Description                                                                                                                                                                                                                         |
|---------|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | Company Name                    | Specify the name of your organization. The company name appears in activity reports. see <a href="#">Generating Reports on page 72</a> .                                                                                            |
| 2       | File History                    | Specify for how many days the system saves files. The default is <b>30</b> days.                                                                                                                                                    |
| 3       | Password Protected File History | Specify for how many days the system saves password-protected files. The default is <b>180</b> days.<br><br><b>Note</b><br>After the configured period, the original file is deleted and cannot be retrieved through the dashboard. |
| 4       | Date Format                     | Select your preferred date format for the display of information in the dashboard --either MM/DD/YYYY or DD/MM/YYYY.                                                                                                                |
| 5       | Time Format                     | Select your preferred time format for the display of information in the dashboard -- either a 12-hour clock or 24-hour clock, using the format <b>HH:MM</b> or <b>HH:MM (AM/PM)</b> .                                               |

| Element | Field           | Description                                                                                                                                                                                 |
|---------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6       | System Language | Select your preferred system language. To add languages to the list you must translate Dashboard dictionary and upload the translation.<br><br>The default language is <b>EN</b> , English. |

**Note**

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

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.

### 3.3.2 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

Type in your organization Active Directory address

\* IP / Hostname

2

Active Directory Server Port

Type in your organization Active Directory server port

\* Port

389

3

Active Directory User Group

Type in your Active Directory user group

\* Group Name

Votiro\_Users

4

Active Directory Username

Type in your Active Directory username

\* Username

5

Active Directory User Password

Type in your Active Directory user password

\* Password

6

SSL

Choose whether to use SSL

Use SSL

☐

7

Test Connection

perform a connection test to the active directory server

Test

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 <code>Votiro_Users</code> group in Active Directory can login to the Management Dashborad. |

| 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"><li>■ DOMAIN\UserName - For example, VT\Jane.Smith</li><li>■ UserName@FQDN - For example, Jane.Smith@Votiro.com</li></ul> <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 <b>Test</b> .                                                                                                                                                                                                                                                                                                           |

**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.

### 3.3.3

### SMTP

All SMTP settings are required to enable Management Dashboard features that rely on email. Configuring SMTP settings allows you to release original files from the blob. For more information, see [Releasing Files on page 40](#).

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

Settings

SMTP

1 SMTP Server Address IP / Hostname  
Type in your organization SMTP server address 127.0.0.1

2 SMTP Server Port Port  
Type in your organization SMTP server port 25

3 SMTP Server Email Username  
Type in your SMTP server email JOHN\_DOE@MYDOMAIN.COM  
SMTP User is required

4 SMTP Server Password Password  
Type in your SMTP server password

5 Test Email  
send a test email in order to check the connection

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 <b>Test</b>.</p> <ul style="list-style-type: none"> <li>If the settings are valid, a verification code is displayed in the Management Dashboard.</li> </ul> <p>The same code appears in an email message that is sent to the address you specified.</p> <div> <div> <b>Test Email</b><br/> To check the SMTP connection send a test email, click Test. </div> <div> <input type="button" value="Test"/><br/> An email has been sent containing the following number<br/> 3 5 1 8 4 </div> </div> <ul style="list-style-type: none"> <li>If the settings are invalid, an error is displayed below the button.</li> </ul> |



**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.

**3.3.4****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**.

**SAML**

- IDP Metadata address** (URL: <https://votiro-ortichon.okta.com/app/exk>)
- Issuer** (name: [Okta\\_SAML\\_Example](#))
- SAML Username identifier** (name: <http://schemas.xmlsoap.org/ws/2005/05>, Type in your username identifier (username claim))
- Admin role key** (key: [Group](#))
- Admin role value** (value: [VotiroAdmins](#))
- Help-Desk role key** (key: [Group](#))
- Help-Desk role value** (value: [VotiroHelpDesk](#))
- SOC role key** (key: [Group](#))
- 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.

### 3.3.5 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**.

Settings

**Users**


1 **Votiro Admin**  
Change Votiro admin user password. This Votiro admin role is independent of the Active-Directory group. Only the password can be changed.

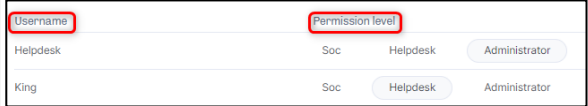
2 **Active Directory Group**  
AD Group for Votiro users

Votiro\_Users

| Username | Permission level |                        |
|----------|------------------|------------------------|
| Helpdesk | Soc              | Helpdesk Administrator |
| King     | Soc              | Helpdesk Administrator |
| RonF     | Soc              | Helpdesk Administrator |
| Soc      | Soc              | Helpdesk Administrator |

The Users page contains the following fields:

| Element | Field        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | Votiro Admin | <p>The <b>Votiro Admin</b> role provides direct administrative access to <b>Votiro Cloud</b>, independent of <b>Active Directory</b>.</p> <p>To change the <b>Votiro Admin</b> password:</p> <ol style="list-style-type: none"><li>1 Click .</li><li>2 Enter the <b>Current Password</b> and then <b>Confirm New Password</b>.</li><li>3 Click <b>Save</b>, or <b>Cancel</b>.</li></ol> <div><div>Change Password</div><div>You will not be able to recover it</div><div><div>Current Password</div><div>.....</div></div><div><div>New Password</div><div>.....</div></div><div><div>Confirm New Password</div><div>.....</div></div><div><div>CANCEL</div><div>SAVE</div></div></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"> <li>■ <b>SOC:</b> 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.</li> <li>■ <b>Helpdesk:</b> users will be able to manage the positive selection process and release of personal files and emails, in addition to SOC permissions.</li> <li>■ <b>Administrator:</b> 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.</li> </ul> <p>To set a user's <b>Permission Level</b> go to the options to the right of the <b>Username</b>, click the permission level to be granted. The level selected is highlighted.</p>  <div style="background-color: #ffe6e6; padding: 10px; border: 1px solid #ff0000;"> <p><b>WARNING!</b></p> <p>The system must have a minimum of one <b>Administrator</b> user set up in the Active Directory Group for Votiro users.</p> <p>A warning message appears if you attempt to <b>Save</b> the settings with no user set with <b>Administrator</b> permissions.</p> </div> |

### 3.3.6 SIEM

You can configure settings for saving Management event logs in a SIEM.

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

Settings

**SIEM**

1 **SIEM Server address** \* IP / Hostname  
Type in your organization SIEM server address 127.0.0.1

2 **SIEM Server port** \* Port  
Type in your organization SIEM server port 514

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.<br><br>The default is empty. When the address is empty, the server uses its own IP as an address.              |
| 2       | SIEM Server port    | Specifies the UDP port of the SIEM system collector service. Specify a positive integer between 1 and 65535. The default is 514.<br><br>For more information about SIEM logging in Management, see <a href="#">Sending Logs to SIEM in CEF on page 82</a> . |

#### 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.

### 3.3.7 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**.

Settings

**1 Service Tokens**  
A list of service tokens which allows other services to communicate with Votiro products

**2** [+ Create New](#)

**3**

|            |                                      |
|------------|--------------------------------------|
| ID         | bd7b56a2-2692-4686-9df2-ea61165a0bf9 |
| Issued To  | Ehud                                 |
| Created At | 25/01/2021 20:08                     |
| Expiration | 25/01/2022                           |

**4** [Revoke](#)

|            |                                      |
|------------|--------------------------------------|
| ID         | 6c96ea87-4fa9-409e-b882-e55470aeeb7b |
| Issued To  | or                                   |
| Created At | 03/02/2021 12:08                     |
| Expiration | 01/02/2022                           |

[Revoke](#)

| 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 <b>+ Create New</b> . For detailed steps to create a new service token, see <a href="#">Creating a Service Token below</a> .                                                                                                                                                                                                                                    |
| 3       | Service Token  | Details of the service token are displayed: <ul style="list-style-type: none"> <li>■ ID: The ID of the service token is automatically added.</li> <li>■ Issued To: Specifies the name you have given to the service token.</li> <li>■ Created At: A DateTime stamp is automatically added to the service token.</li> <li>■ Expiration.: Specifies the date the service token will expire.</li> </ul> |
| 4       | Revoke         | To remove a service token, click <b>Revoke</b> . For detailed steps to remove a service token, see <a href="#">Revoking a Service Token on the next page</a> .                                                                                                                                                                                                                                       |

## 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.       |

### Create New Service Token

Issued To

JG

Set Expiration Time

<

Feb

2022

>

Su

Mo

Tu

We

Th

Fr

Sa

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

CANCEL

CREATE

3. Click **Create**.

[illegible]

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

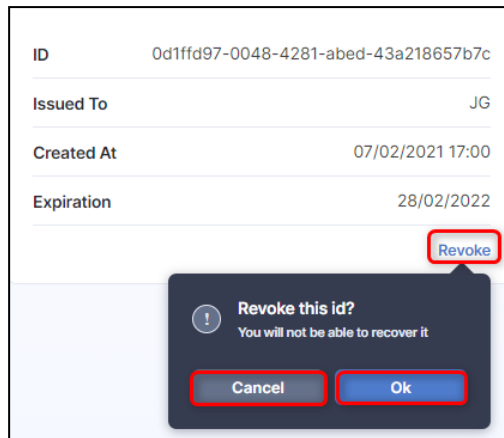
## IMPORTANT!

The service token generated is not stored by Votiro Cloud. You must copy it immediately.

- Click **OK**.
- 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.

### 3.3.8 License

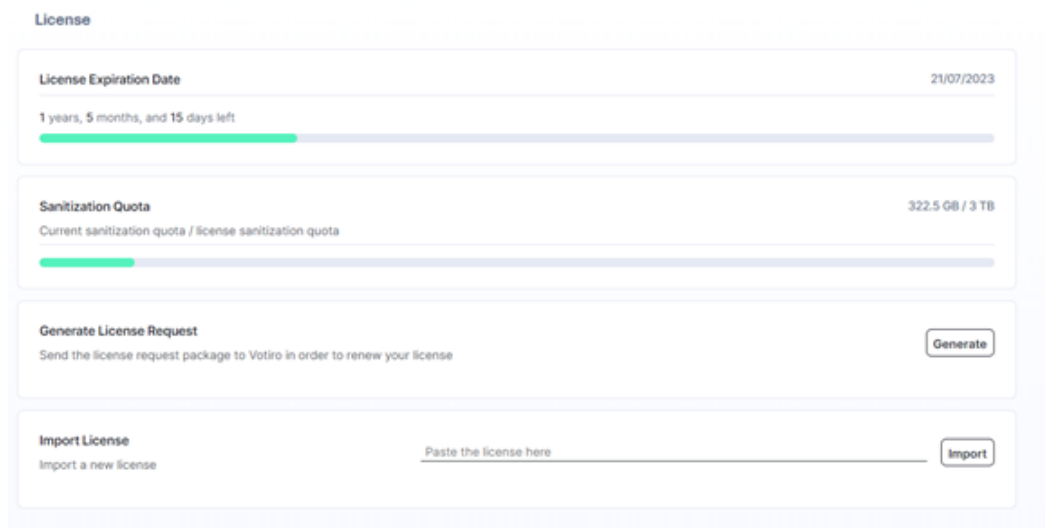
Use the License page to generate a license request, import a license key, know the date the license will expire and keep track of the file consumption against the quota.

#### 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 <a href="#">See Sanitization Quota (V9.6.3)</a> for a more complete explanation.</p>                                                                                                    |
| 3       | Generate License Request | <p>Click <b>Generate</b> to produce a license request package. The file <b>licensePackage.zip</b> 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 <b>Import</b>. Successful validation automatically updates <b>License expiration date</b> and <b>Sanitization quota</b> information. The license key disappears.</p> <div> <p><b>Note</b></p> <p>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.

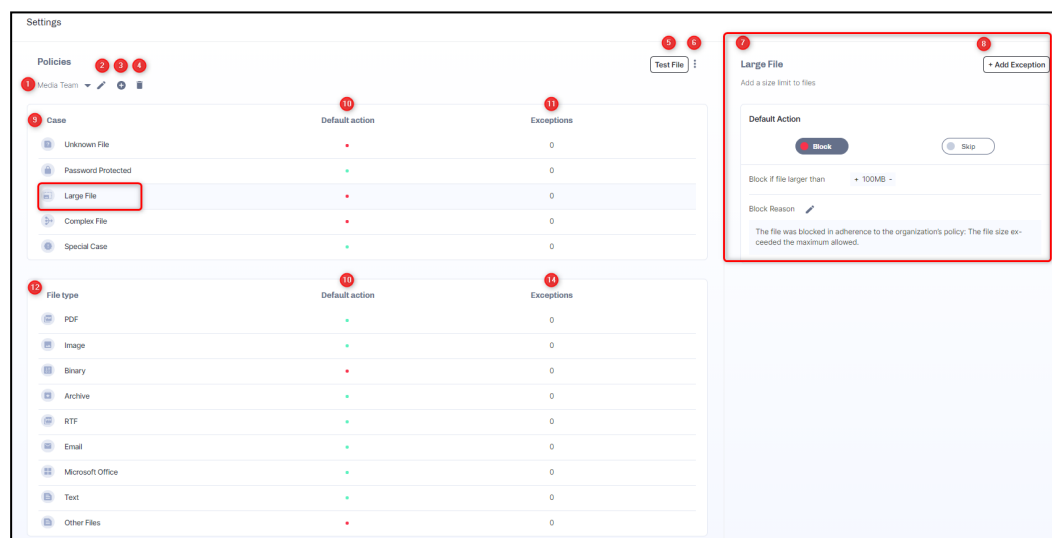
### 3.3.9 Policies

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<sup>®</sup> 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 <b>default policy</b> cannot be deleted.                            |
| 5       | Select file to test policy.                                                                                                                                           |
| 6       | Import/Export policy file.                                                                                                                                            |

| Element | Meaning                                                                                                                                                                                                                                                                                                                         |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br>A colored dot illustrates your current policy action:<br><ul style="list-style-type: none"> <li>■ Red - files will be blocked</li> <li>■ Green - files will be processed using your sanitization settings</li> <li>■ Grey - files will be skipped</li> </ul> |
| 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 88](#).
- **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 91](#).
- **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 95](#).
- **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.

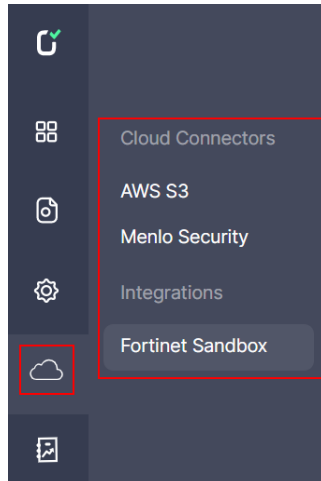
## File Blocking

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.

## 3.4 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.



### 3.4.1 AWS S3

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

The AWS S3 page contains the following fields:

| Element | Field           | Description                                         |
|---------|-----------------|-----------------------------------------------------|
| 1       | Region Endpoint | Specify the AWS region the S3 bucket is located in. |
| 2       | Queue URL       | Specify the AWS queue URL. See below for details.   |

| Element | Field        | Description                        |
|---------|--------------|------------------------------------|
| 3       | Access Key   | Specify the AWS access key.        |
| 4       | Secret Key   | Specify the AWS secret key         |
| 5       | User Profile | Specify the AWS user profile name. |

**Note**

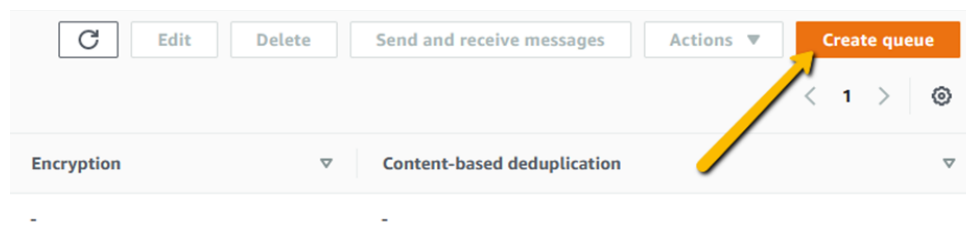
Fields marked with a \* red asterisk are mandatory, to be completed.

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.

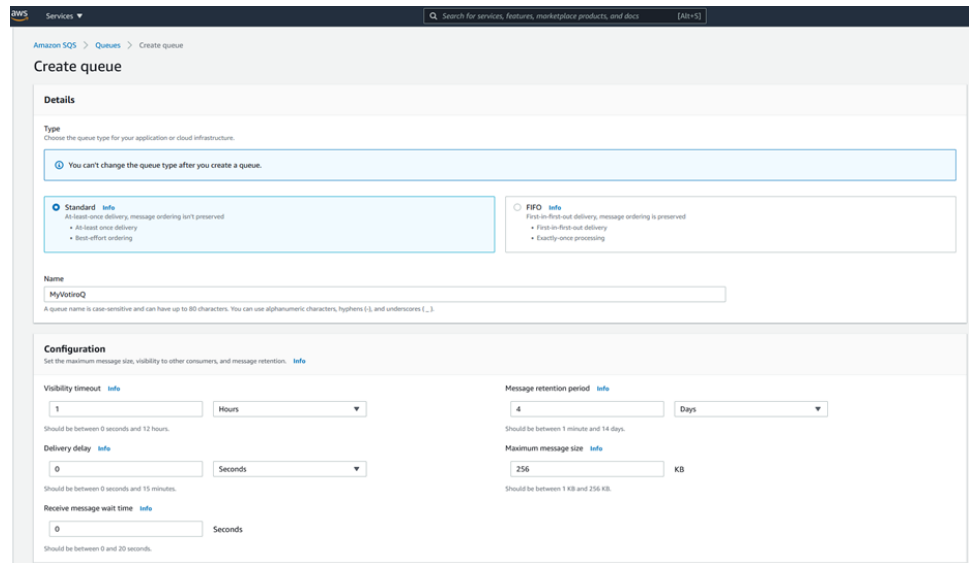
## Creating an AWS SQS Queue

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:



**Amazon SQS** > **Queues** > Create queue

### Create queue

**Details**

**Type**  
Choose the queue type for your application or cloud infrastructure.

☒ **Standard** [info](#)  
At least-once delivery, message ordering isn't preserved.  
• At least once delivery  
• Best-effort ordering

☐ **FIFO** [info](#)  
First-in-first-out delivery, message ordering is preserved.  
• First-in-first-out delivery  
• Exactly-once processing

**Name**  
MyVotiroQ  
A queue name is case-sensitive and can have up to 80 characters. You can use alphanumeric characters, hyphens (-), and underscores (\_).

**Configuration**  
Set the maximum message size, visibility to other consumers, and message retention. [info](#)

**Visibility timeout** [info](#)  
1 Hours  
Should be between 0 seconds and 12 hours.

**Delivery delay** [info](#)  
0 Seconds  
Should be between 0 seconds and 15 minutes.

**Receive message wait time** [info](#)  
0 Seconds  
Should be between 0 and 20 seconds.

**Message retention period** [info](#)  
4 Days  
Should be between 1 minute and 14 days.

**Maximum message size** [info](#)  
256 KB  
Should be between 1 KB and 256 KB.

7. For the Access policy, choose **Advanced**.
8. You may use the below template and replace <AWS\_ACCOUNT\_NUM> and <QUEUE\_NAME> with their actual values:

```

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

```

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

**▼ Redrive allow policy - Optional**  
Identify which source queues can use this queue as the dead-letter queue. [Info](#)

Select which source queues can use this queue as the dead-letter queue.

☒ Disabled  
☐ Enabled

**▼ Encryption - Optional**  
Amazon SQS provides in-transit encryption by default. To add at-rest encryption to your queue, enable server-side encryption. [Info](#)

Server-side encryption

☒ Disabled  
☐ Enabled

**▼ Dead-letter queue - Optional**  
Send undeliverable messages to a dead-letter queue. [Info](#)

Set this queue to receive undeliverable messages.

☒ Disabled  
☐ Enabled

**▼ Tags - Optional**  
A tag is a label assigned to an AWS resource. Use tags to search and filter your resources or track your AWS costs. [Learn more](#) [E](#)

| Key                                        | Value - optional                       |                                       |
|--------------------------------------------|----------------------------------------|---------------------------------------|
| <input type="text" value="Name"/>          | <input type="text" value="MyVotiroQ"/> | <input type="button" value="Remove"/> |
| <input type="button" value="Add new tag"/> |                                        |                                       |

You can add 40 more tags.

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

## Assigning the Queue to an Existing S3 Bucket

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



## 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

- Under **Destination**, select **SQS queue**.
- Under **Specify SQS queue**, select **Choose from your SQS queues**.
- Select the **SQS queue** from the list of available queues. For example:

### Destination

**i** 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

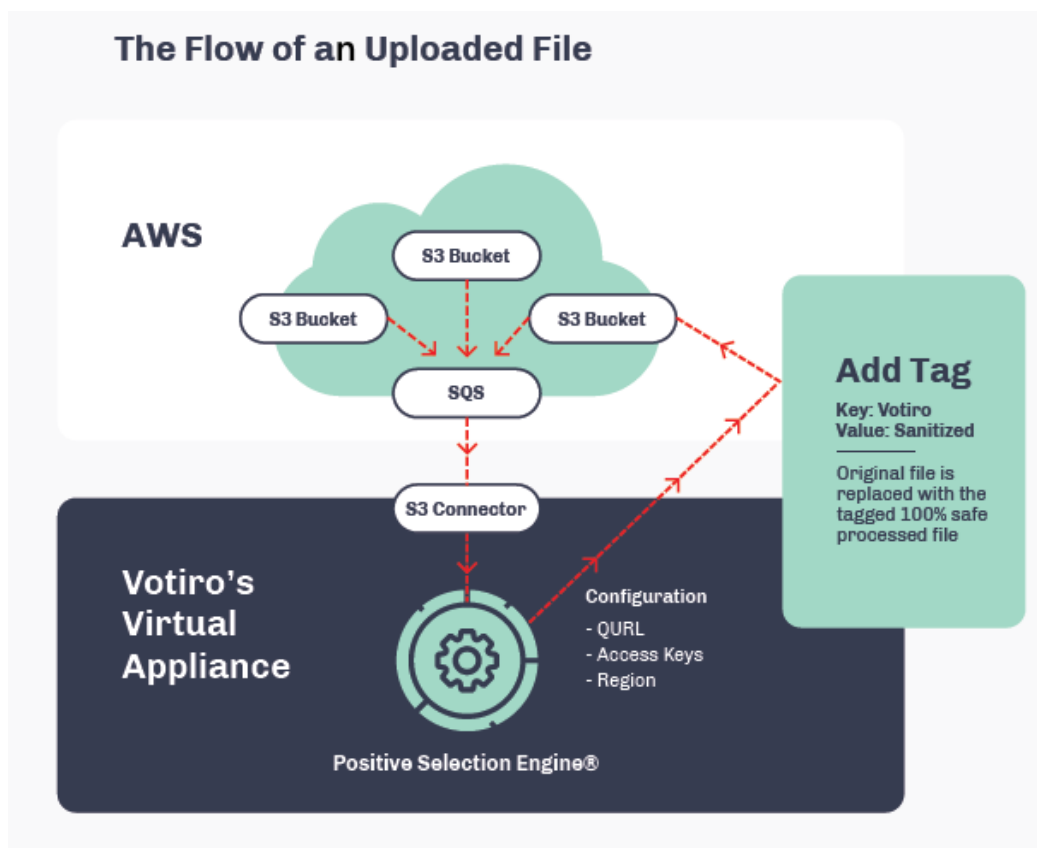
**SQS queue**

[Cancel](#) [Save changes](#)

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

## AWS S3 Flowchart

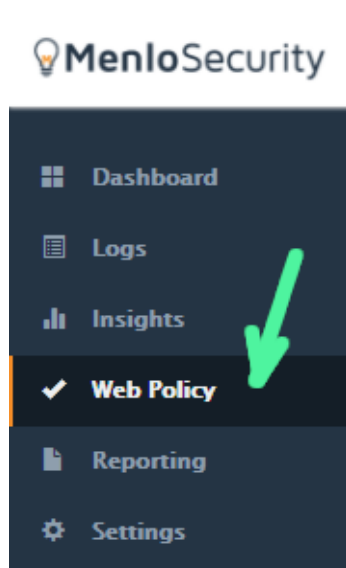
The following diagram illustrates the procedure:



### 3.4.2 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**.



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



- 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"/>            | <a href="#">Edit</a> |
| Full File Scan      | Anti-Virus Scan                        | <input type="checkbox"/>            | <a href="#">Edit</a> |
| SandBox Inspection  | Cloud-Based SandBox Inspection         | <input type="checkbox"/>            | <a href="#">Edit</a> |
| WildFire Analysis   | WildFire Malware Analysis              | <input type="checkbox"/>            | <a href="#">Edit</a> |
| Menlo File REST API | Menlo File REST API Server Integration | <input checked="" type="checkbox"/> | <a href="#">Edit</a> |

- 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 value that you generated: ecac088b-43b6-4425-b7fb-724060f90ee2.

## 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 <b>Default Policy</b> 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.

### 3.4.3 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

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 ✓/✗.

**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.

The screenshot displays the Votiro Management Dashboard. On the left, the 'Policies' section shows a table of default actions for various file types. The 'Unknown File' policy is highlighted, showing a default action of 'Sandbox' and 0 exceptions. Below this, a table lists file types (PDF, Image, Binary, Archive, RTF, Email, Microsoft Office, Text, Other Files) with their respective default actions and exception counts.

On the right, the 'Unknown File' settings are shown. The 'Default Action' is set to 'Sandbox', which is highlighted with a red box and an arrow pointing to it with the text 'Sandbox policy option'. The 'Block Reason' field is also highlighted with a red box and contains the text '[[SandboxResultList]]'. A warning message below states: 'Warning - Sandbox is not as quick as Votiro Disarmer. Files sent to Sandbox will impact your performance.'

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.

The screenshot displays the Votiro Management Dashboard. On the left, the 'Files' section shows a list of files, including 'With embedded CVE exe .pdf'. The 'File Info' section shows details for a file, including its File Type (Executable), Original Item Hash, Connector Name (Self-sanitization), and Connector Type (File Connector).

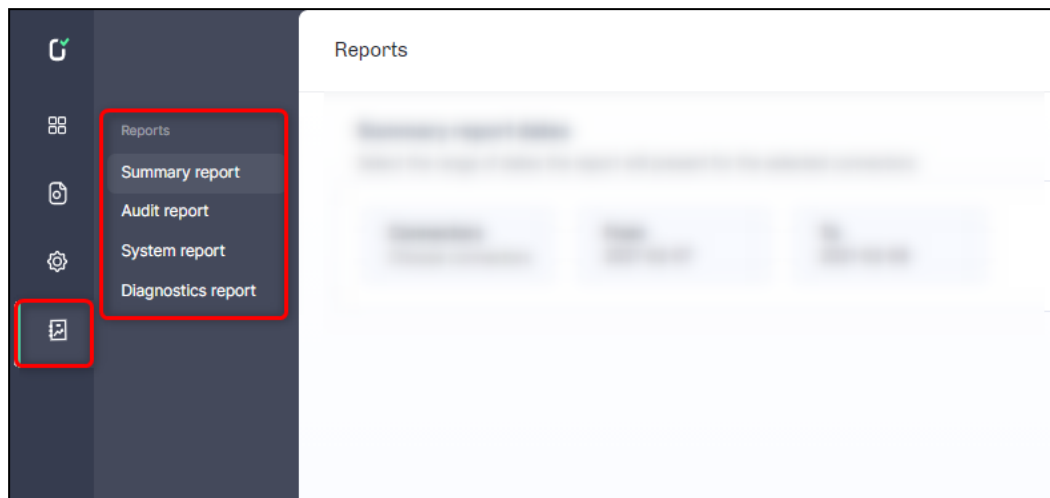
On the right, the 'Sanitization Log' details actions performed by Fortinet. The log shows a file being successfully scanned by Fortinet, with a red box highlighting the text 'successfully scanned by Fortinet'. Below this, a red box highlights the text 'Threat found by Fortinet in file'. The log also shows the total sanitization time as 0.5 Sec.

## 3.5 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:



### 3.5.1 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**.

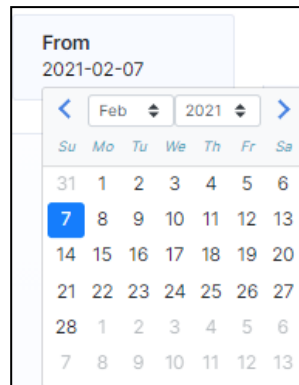
The screenshot shows a web interface titled 'Reports'. Below the title is a section 'Summary report dates' with the instruction 'Select the range of dates the report will present for the selected connectors:'. There are three input fields: 'Connectors' with the placeholder text 'Choose connectors', 'From' 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. Red boxes highlight the 'Connectors', 'From', and 'To' fields.

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

The screenshot shows a panel titled 'Connectors' with the subtitle 'Choose connectors'. It features a search bar with a magnifying glass icon and the word 'Search'. Below the search bar are the options 'Check all' and 'Uncheck all'. There is a list of connectors with checkboxes: 'None' (checked), 'File Connector' (checked), and 'LoadTestChannel' (checked). A grey bar is at the bottom of the panel.

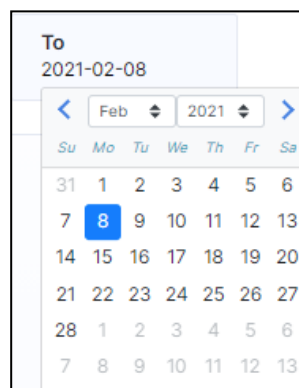
3. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:

- 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.

### 3.5.2 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.

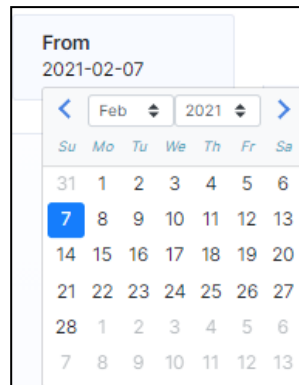
To generate an Audit report, follow these steps:

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 a subtitle "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". Both fields are highlighted with red rectangles. To the right of these fields is a blue button labeled "Generate report", also highlighted with a red rectangle.

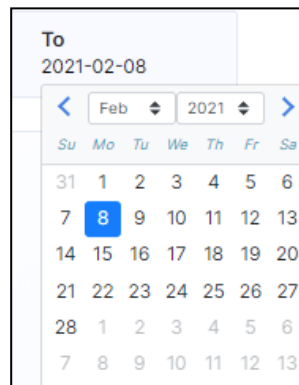
2. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:

- 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_63676692124         | 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.

### 3.5.3 System Report

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

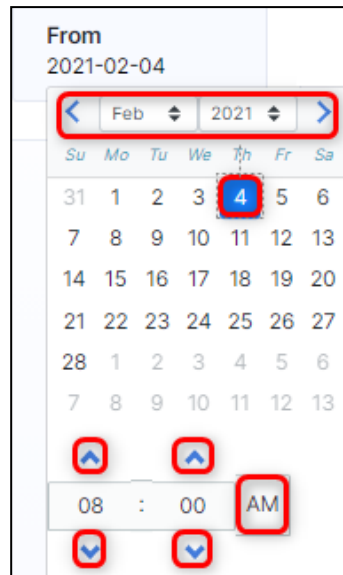
You can generate a report of all system activity performed by users of the Management Dashboard for a specified period. The exported report generates a zip file.

To generate an System report, follow these steps:

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

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:

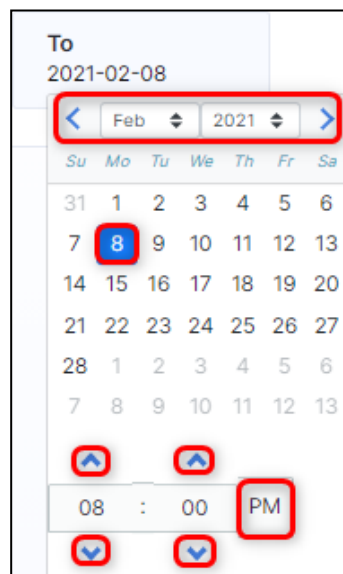
- a. To select the start range of the report, click **From**, a calendar displays.



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.



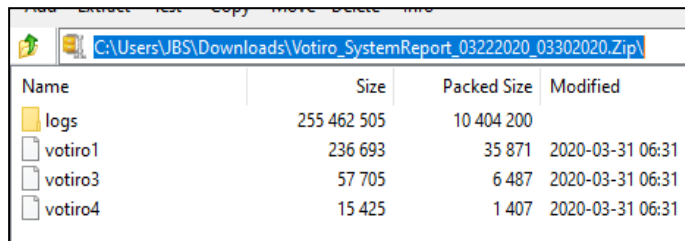
The selected date is blue. To change the end date for the report use the selection steps described in **2a** above for the day and time for report to end.

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.

### 3.5.4 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**.



Reports

**Diagnostics report time-frame**

Select the range of date and times the report will present

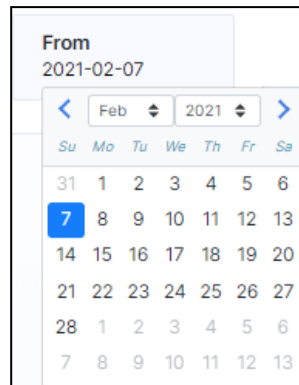
From 2021-02-07 To 2021-02-08

Generate 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:

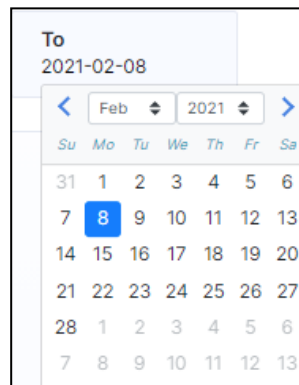


- a. To select the start date from the report, click **From**, a calendar displays.



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.

## Appendix A Sending Logs to SIEM in CEF

Votiro Cloud logs can be sent to SIEM in Common Event Format (CEF).

To enable SIEM logging, you must configure the SIEM settings in the Management Dashboard, see [SIEM on page 52](#).

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

```
CEF:0|VOTIRO|Secure File Gateway|1.0.0.0|60020010|Publish Done|4|rt=Feb 10 2021
13:03:55 dtz=00:00:00 dvchost=mng-service-siem-6bcbfccf4-4zxcj fileId=6dad7b86-07b5-
4542-b3fd-5c90af9c6009 cs3=6dad7b86-07b5-4542-b3fd-5c90af9c6009
cs3Label=Correlation Id
fileHash=c65a2b1c5847764b0534166ca2ba6f516ed336a836cacc00bf9254fd086b7973
filePath=d6188750-5aa5-471a-a416-5684456cfb09.eml suser= <User1@orga.local>
cs4=Weekly Sales Report cs4Label=Email Subject cs5=Hampshire-EC cs5Label=Connector
Name msg=File 'd6188750-5aa5-471a-a416-5684456cfb09.eml' published.
```

### CEF Message Format

The CEF message format is as follows:

```
CEF: Version | Device Vendor | Device Product | Device Version |
Signature ID |Name |Severity | Extension
```

- **Version.** Always 0.
- **Device Vendor:** Always *VOTIRO*.
- **Device Product:** Always *Secure File Gateway*.
- **Device Version:** The version of Votiro Cloud.
- **Signature ID:** Event ID. Made up of Family Id and Id, where:
  - ◆ Family Id can be one of:
    - 100, in the case of a Trace event.
    - 200, in the case of a System event.
    - 500, in the case of an Indicator event.
    - 600, in the case of an Internal Trace event.
  - ◆ Id is a five-numeral string.
- **Name:** Event Name indicates the type of event. See [Report Events on page 84](#).
- **Severity:** Indicates the urgency of the event.

**Table 5 Severity Levels**

| Level | Severity | Description                                                                          |
|-------|----------|--------------------------------------------------------------------------------------|
| 0     | Verbose  | Very fine-grained informational events that are most useful to debug an application. |

| Level | Severity | Description                                                                                                                      |
|-------|----------|----------------------------------------------------------------------------------------------------------------------------------|
| 1     | Debug    | Fine-grained informational events that are most useful to debug an application.                                                  |
| 4     | Info     | Informational messages that highlight the progress of the application at coarse-grained level.<br><br>This is the default level. |
| 5     | Notice   | Informational messages that highlight the progress of the application at the highest level.                                      |
| 6     | Warning  | Potentially harmful situations.                                                                                                  |
| 7     | Error    | Error events that might still allow the application to continue running.                                                         |
| 9     | Fatal    | Very severe error events that will presumably lead the application to abort.                                                     |

- **Extension.** This section is a placeholder for additional fields. Votiro uses this extension for these three values:
  - ◆ **Date.** Timestamp of event occurrence in the system. The extension always begins with these values:
    - rt: receiptTime. The time that the event related to the activity was received.
    - dtz: device time zone. The time zone of the server, when set, relative to UTC. Format 00:00:00.
  - ◆ **Host Name.** The name of the Votiro Cloud server in which the event occurred.
    - dvchost: deviceHostName. The host name, for example, John-PC.
  - ◆ **Additional Extensions.** The finale value is always **msg** (message). It is the human readable message of the event description. See [Report Events on the next page](#).
    - fileId: the ID associated with a file.
    - fileHash: the hash of a file.
    - filePath: the full path to the file, including the file name itself.
    - fileType: the type of file.
    - suser: sourceUserName (from). Identifies the source user by name. Only present when root file is an EML file type.
    - duser: destinationUserName (to). Identifies the destination user by name and is the user associated with the event's destination. Only present when root file is an EML file type.

**Custom String.** All custom fields have a corresponding label field, where the field itself is described.

- correlation id: match as a pair with correlation id label. For example, cs3=6dad7b86-07b5-4542-b3fd-5c90af9c6009 cs3Label=Correlation Id.
- subject: matches as a pair for EML events. For example, cs4=Weekly Sales Report, and cs4Label=Email Subject.
- connector name: match as a pair with connector name label. For example, cs5=Hampshire-EC ,and cs5Label=Connector Name.

### Notes

Certain information may be available, depending on values for certain fields, including:

- The **Publish Done** event includes the hash of the root file in the CEF.
- The **Child Item Created** event includes child file information in the CEF.
- For root **EML**, additional fields **suser** , **duser** and **subject** are in the extension.

## Report Events

Event codes respect the following 8-digit scheme:

**L L R C C T T R**

where L, R, C, T are digits [0-9].

- LL specifies the event main category.
- CC specifies the sub-category.
- TT specifies the specific event type.
- R is reserved for future use and must be ignored.

### Examples

- 50020110 represents an Indicator event (LL=50) of category Suspicious Executable File (C=20), specifying that an executable artifact (TT=11) was found.
- 10000010 represents a Trace event (LL=10) of category FTD (C=00), specifying that a discovered file type (TT=01) was found.

**Table 6 CEF Message Template Extensions**

| Category | Event Code | Sub-Category         | Event Name     | Event Description                                      |
|----------|------------|----------------------|----------------|--------------------------------------------------------|
| Trace    | 10000010   | File Type Discoverer | True File Type | File {FileName} recognized as {FileType}.              |
| Trace    | 10020100   | File Process         | File Uploaded  | File {FileName} upload for positive selection started. |

| Category | Event Code | Sub-Category | Event Name                              | Event Description                                                                                                                     |
|----------|------------|--------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Trace    | 10020130   | File Process | Child Item Created                      | New child created for item {ParentItemId}. Child ID: {ChildId}.                                                                       |
| Trace    | 10020110   | File Process | Sanitization Complete                   | File {FileName} sanitization process successfully ended.                                                                              |
| Trace    | 10020200   | File Process | File Blocked                            | File {FileName} blocked as a result of the positive selection process.                                                                |
| Trace    | 10020300   | File Process | Sanitization Timeout                    | Sanitization of the file {FileName} exceeded the time limit.                                                                          |
| Trace    | 10050000   | Blocker      | Block - Unknown File (Policy)           | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process.                             |
| Trace    | 10050010   | Blocker      | Block - Large File (Policy)             | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process.                             |
| Trace    | 10050020   | Blocker      | Block - Complex File (Policy)           | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process.                             |
| Trace    | 10050030   | Blocker      | Block - Binary File (Policy)            | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process.                             |
| Trace    | 10050040   | Blocker      | Block - Other Unsupported File (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process.                             |
| Trace    | 10050050   | Blocker      | Block - DDE (Policy)                    | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process - DDE detected.              |
| Trace    | 10050060   | Blocker      | Block - Macro (Policy)                  | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process - Suspicious macro detected. |






| Category  | Event Code | Sub-Category              | Event Name                          | Event Description                                                                                                                   |
|-----------|------------|---------------------------|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Trace     | 10050070   | Blocker                   | Block - Suspicious URL (Policy)     | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process - Suspicious URL detected. |
| Trace     | 10050080   | Blocker                   | Block - Password Protected (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process - Password Protected File. |
| Trace     | 10050100   | Blocker                   | Block - General (Policy)            | File {FileName} blocked due to your organization policy violation {Policy} in the positive selection process.                       |
| Trace     | 10050500   | Blocker                   | Block - Error                       | File {FileName} blocked due to an error in positive selection process.                                                              |
| Trace     | 10060100   | Password Protected Opener | Password Opened                     | Password Protected File {FileName} successfully opened.                                                                             |
| Trace     | 10060110   | Password Protected Opener | Password Added                      | Password Protected File {FileName} successfully closes with original password.                                                      |
| Trace     | 10060200   | Password Protected Opener | Wrong Password                      | Password Protected File {FileName} couldn't be opened.                                                                              |
| Trace     | 10080100   | Validate Signature        | Validate Signature Succeeded        | Signature Validation for file {FileName} succeeded.                                                                                 |
| System    | 20060800   | System Error              | Fatal Error                         | System error occurred during handling request of file {FileName}.                                                                   |
| System    | 21020100   | Warning                   | Low Disk Space                      | The system is running on low disk space: Used {used} of {diskSize} ({usagePercent}%), available {available}                         |
| Indicator | 50010000   | Macro Analyzer            | Suspicious Macro                    | Suspicious Office macro detected.                                                                                                   |
| Indicator | 50010010   | Macro Analyzer            | Auto Execution Macro                | Suspicious Office macro detected [Auto Execution].                                                                                  |

| Category     | Event Code | Sub-Category              | Event Name                                   | Event Description                                                                        |
|--------------|------------|---------------------------|----------------------------------------------|------------------------------------------------------------------------------------------|
| Indicator    | 50010020   | Macro Analyzer            | File System Activity Macro                   | Office macro detected [File System Activity].                                            |
| Indicator    | 50010030   | Macro Analyzer            | Out Of Document Interaction Macro            | Office macro detected [Out-Of-Document Interaction].                                     |
| Indicator    | 50010040   | Macro Analyzer            | Suspicious Office Excel 4.0 Macro            | Suspicious Office Excel 4.0 macro detected.                                              |
| Indicator    | 50010050   | Macro Analyzer            | Suspicious File System Activity Macro        | Suspicious Office macro detected [File System Activity].                                 |
| Indicator    | 50010060   | Macro Analyzer            | Suspicious Out of Document Interaction Macro | Suspicious Office macro detected [Out-Of-Document Interaction].                          |
| Indicator    | 50020010   | File Type Discoverer      | Suspicious Fake File                         | Suspicious fake file [Extension does not match file structure] detected in the artifact. |
| Indicator    | 50020020   | File Type Discoverer      | Suspicious Unknown File                      | Unknown file [Data file or unidentified file type] detected in the artifact.             |
| Indicator    | 50020110   | File Type Discoverer      | Suspicious Executable File                   | Executable file detected in the artifact.                                                |
| Indicator    | 50020120   | File Type Discoverer      | Suspicious Script File                       | Script file detected in the artifact.                                                    |
| Indicator    | 50040010   | Active Element            | External Program Run Action                  | External Program Run Action detected in file {Filename}.                                 |
| Indicator    | 50050010   | JavaScript Analyzer       | Dynamic code execution                       | Dynamic code execution detected in file {Filename}.                                      |
| Indicator    | 50060010   | Suspicious URL            | Suspicious URL detected                      | Suspicious url detected in file {FileName}, URLs: {SuspiciousUrlsList}                   |
| Indicator    | 50065010   | Xml Bomb                  | Xml Bomb detected                            | Xml Bomb detected.                                                                       |
| Indicator    | 50070050   | Suspicious File Structure | Suspicious File Structure                    | Suspicious structure detected in file {FileName}                                         |
| Indicator    | 50075050   | Svg Bomb                  | Svg Bomb detected                            | Svg Bomb detected.                                                                       |
| Indicator    | 50090200   | Validate Signature        | Validate Signature Failed                    | Signature Validation for file {FileName} failed.                                         |
| File Process | 60020010   | File Process              | Publish Complete                             | File {FileName} published.                                                               |
| File Process | 60020020   | File Process              | Publish Original Complete                    | File {FileName} original published.                                                      |

## 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 95](#).

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

**Table 7** Positive Selection Processing Options for Cases

| Case         | Processing Options                                                                                                                                                                 |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unknown File | You can block or skip these files.<br><br>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"> <li>■ <b>Return file by email with User Message:</b> Allows you to return a password protected file by email. Accept the default text notification message, or edit it.</li> <li>■ <b>User Message:</b> Allows you to edit the message sent to the recipient of the password protected file. <a href="#">See Instructions for Email User</a> below.</li> <li>■ <b>Block unsupported files with Block Reason:</b> Allows you to block unsupported files (such as Visio files). Accept the default text notification message, or edit it.</li> </ul> <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 data-bbox="667 994 1415 1236"> <p><b>Note</b></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><b>Instructions for Email User</b></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 <b>Get File</b>.</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 data-bbox="667 1823 1415 1921"> <p><b>Note</b></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 | <p>You can set a layer number. Files that are found in that layer or deeper are blocked.</p>                                                                                                                                                  |
| Special Case | <p>You will have already defined a Special Case with Votiro's support team. Click <b>Load File</b>. For more information, see <a href="#">Defining Policies on page 59</a>.</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 |
|----------------------------------------------------------------------------------------------------|----------------|------------|
|  PDF              | •              | 0          |
|  Image            | •              | 0          |
|  Binary           | •              | 0          |
|  Archive          | •              | 0          |
|  RTF              | •              | 0          |
|  Email            | •              | 0          |
|  Microsoft Office | •              | 0          |
|  Text             | •              | 0          |
|  Other Files      | •              | 0          |

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 95](#).

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

**Table 8 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"> <li>■ <b>Remove multimedia:</b> Specifies whether multimedia such as embedded video, audio, 3D annotations, and rich media annotations must be removed. Default is checked.</li> <li>■ <b>Clean embedded fonts:</b> Specifies whether embedded fonts must be processed. Default is checked.</li> <li>■ <b>Block files with suspicious links:</b> Performs a check of all links in the form HTTP:// and HTTPS:// in a PDF document. If any link is found to be suspicious, it is 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 <b>Block Reason</b> message. Default is unchecked.</li> <li>■ <b>JavaScript handling:</b> Determines how JavaScript, if found in the PDF file, is handled. <ul style="list-style-type: none"> <li>◆ Don't do anything</li> <li>◆ Remove only suspicious scripts</li> <li>◆ Remove all scripts (this is the default)</li> </ul> </li> </ul>                                                      |
| Image     | <p>By default, these files are processed for positive selection.</p> <ul style="list-style-type: none"> <li>■ <b>Add micro-changes:</b> Adds security noise to images during processing. Default is checked.</li> </ul> <div style="background-color: #f2f2f2; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>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"> <li>■ <b>Remove metadata:</b> Removes EXIF metadata from JPEG and TIFF images. Default is unchecked.</li> <li>■ <b>Max compression for lossless formats:</b> Compresses lossless image formats (PNG, BMP, and RAW) by 100%. Default is checked.</li> <li>■ <b>Compression level:</b> 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.</li> </ul> |
| Binary    | <p>The processing option is not relevant to managing binary files. You either block binary files or allow them.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| File Type | Processing Options                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Archive   | <p>By default, these files are processed for positive selection.</p> <p><b>Block zip bomb:</b> 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 <b>Block Reason</b> message. Default is checked.</p> |
| RTF       | <p>By default, these files are processed. There are no specific processing options.</p>                                                                                                                                                                                                                                                                                                                                                            |
| Email     | <p>By default, these files are processed for positive selection.</p> <ul style="list-style-type: none"> <li>■ <b>Block files with suspicious links:</b> Performs a check of all links in the form HTTP:// and HTTPS:// in the body and attachments of an email. If any link is found to be suspicious, it is removed from the file. When selected you can edit the <b>Block Reason</b> message. Default is unchecked.</li> </ul>                   |

| File Type        | Processing Options                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft Office | <p>By default, these files are processed for positive selection.</p> <ul style="list-style-type: none"> <li>■ <b>Block files with suspicious links:</b> 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 <b>Block Reason</b> message. Default is unchecked.</li> </ul> <p><b>Note</b><br/>This option is available for DOC/DOCX/XLSX file types only.</p> <ul style="list-style-type: none"> <li>■ <b>Macro handling.</b><br/>In the list, choose one of the following: <ul style="list-style-type: none"> <li>◆ <b>Don't do anything</b></li> <li>◆ <b>Remove only suspicious macros:</b> Remove all macros only if any suspicious code is found.</li> <li>◆ <b>Remove all macros:</b> Remove all macros from the document. This is the default option.</li> <li>◆ <b>Block documents containing suspicious macros:</b> Block the entire document if suspicious code is found in the macro.</li> </ul> </li> </ul> <p><b>Note</b><br/>Excel files with <b>4.0 macro</b> (also known as <b>sheet macro</b>) 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> <ul style="list-style-type: none"> <li>■ <b>Remove metadata:</b> Removes metadata, such as Author, Company, LastSavedBy, and so on. Default is unchecked.</li> <li>■ <b>Remove printer settings:</b> Removes the printerSettings1.bin (printer settings) embedded in a .xlsx file. Default is checked.</li> </ul> |
| Text             | <p>By default, these files are processed for positive selection.</p> <p><b>Block CSV with threat formula:</b> Blocks CSV files that contain formula injections. When selected you can edit the <b>Block Reason</b> message. Default is checked.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Other files      | <p>By default, these files are blocked. You can edit the <b>Block Reason</b> message.</p> <p>There are no specific sanitization processing options.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

#### Note

- Positive selection processing applies to Microsoft Office files and their embedded objects.
- Each attached file is processed recursively by running all policy rules on it.

## 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:

**Define Exception**  
Exception will be activated under the following conditions

IF File type [dropdown] Equals [dropdown] Select [dropdown]

[+]

Cancel Save

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

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

**Define Exception**  
Exception will be activated under the following conditions

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

**+** (highlighted in red box)

Cancel Save (Save highlighted in red box)

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

PDF + Add Exception

**Default Action**

Block Sanitize Allow

☒ Remove multimedia

☒ Clean embedded fonts

☐ Block files with suspicious links

JavaScript handling Remove all scripts

**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 Remove all scripts

Save Changes (highlighted in red box)

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



## Defining Exceptions for File Types



**Define Exception**  
Exception will be activated under the following conditions

IF **File type** **Not equals** **Zip**

IF **File type** **Equals** **Other types**

**checked**

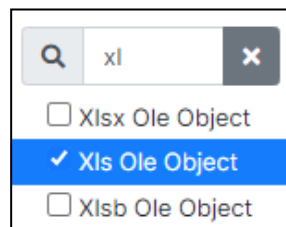
Search...

- ☐ Not Discovered Yet
- ☐ Unknown
- ☐ Empty File
- ☐ Directory
- ☐ Unrecognized
- ☐ Word
- ☐ Word (2007-2010)
- ☐ WordXML
- ☐ Excel
- ☐ Excel (2007-2010)

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.



Search: xl

- ☐ Xlsx Ole Object
- ☒ Xls Ole Object
- ☐ Xlsb Ole Object

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

## Defining Exceptions for File Size

**Define Exception**  
Exception will be activated under the following conditions

IF **File size** **is more than** **3** **MB**

IF **File size** **is less than** **5** **GB**

☐ Bytes  
☐ KB  
☐ MB  
☒ **GB**  
☐ TB

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

**Define Exception**  
Exception will be activated under the following conditions

IF **Email** **To** **equals** **joe@abc.com**

IF **Email** **From** **equals** **admin@abc.com**

IF **Email** **Recipients** **not equals** **courses.abc.com**

**Cancel** **Save**

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 title 'Define Exception' and a subtitle 'Exception will be activated under the following conditions'. The main area contains a rule configuration: 'IF' followed by a dropdown menu set to 'File extension', then 'ends with' followed by a dropdown menu set to 'ends with' (which is highlighted in blue with a checkmark), and a text field containing '.xps'. Below the 'ends with' dropdown is an unchecked checkbox labeled 'doesn't end with'. At the bottom left is a plus sign icon, and at the bottom right are 'Cancel' and 'Save' buttons.

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

**Save**

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