

VOTIRO[✓]

Secure File Gateway V9.5

User Guide

Votiro Support
May 2021

Copyright Notice

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

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

www.votiro.com

Contents

1 Introduction	5
1.1 Votiro's Secure File Gateway Technology	5
1.2 System Architecture and Data Flow	5
1.3 Positive Selection Engine	6
1.4 Supported File Types	7
2 Installing Votiro's Secure File Gateway	15
2.1 Deployment Specifications	15
2.2 Pre-requisites 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 Deploying an OVF	18
2.4 Configuring the Network Environment	21
2.5 Deploying Votiro's Secure File Gateway	22
2.6 Logging in to the Management Dashboard	23
2.6.1 Configuring Authentication to Active Directory	23
2.7 Configuring Password Protected Files Portal	23
2.7.1 Customizing PPF Message	24
2.7.2 Customizing PPF Portal Message	24
2.7.3 Customizing the PPF Portal Logo	24
3 Using the Management Dashboard	25
3.1 Monitoring Positive Selection Activity	26
3.1.1 Monitoring Periods	28
3.1.2 Live Status	29
3.1.3 Traffic Flowing In	30
3.1.4 Secure File Gateway	31

3.1.5 Protection & Business Productivity	32
3.1.6 Test File	32
3.2 Exploring Incidents	33
3.2.1 Viewing Detailed File Information	35
3.2.2 Using Filters	36
3.2.3 Searching Positive Selection Requests	37
3.2.4 Releasing Files	37
3.3 Configuring Settings	39
3.3.1 System Configuration	40
3.3.2 Active Directory	41
3.3.3 SMTP	43
3.3.4 Users	45
3.3.5 SIEM	47
3.3.6 Service Tokens	48
3.3.7 License	51
3.3.8 Policies	52
3.4 Generating Reports	54
3.4.1 Summary Report	55
3.4.2 Audit Report	57
3.4.3 System Report	59
3.4.4 Diagnostics Report	61
Appendix A Sending Logs to SIEM in CEF	63
Appendix B Defining Policies by Case	69
Appendix C Defining Policies by File Type	72
Appendix D Adding Policy Exceptions	76

1 Introduction

1.1 Votiro's Secure File Gateway Technology

Votiro's Secure File Gateway secures your organization by positively selecting safe elements of each file and email delivered to your network.

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

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

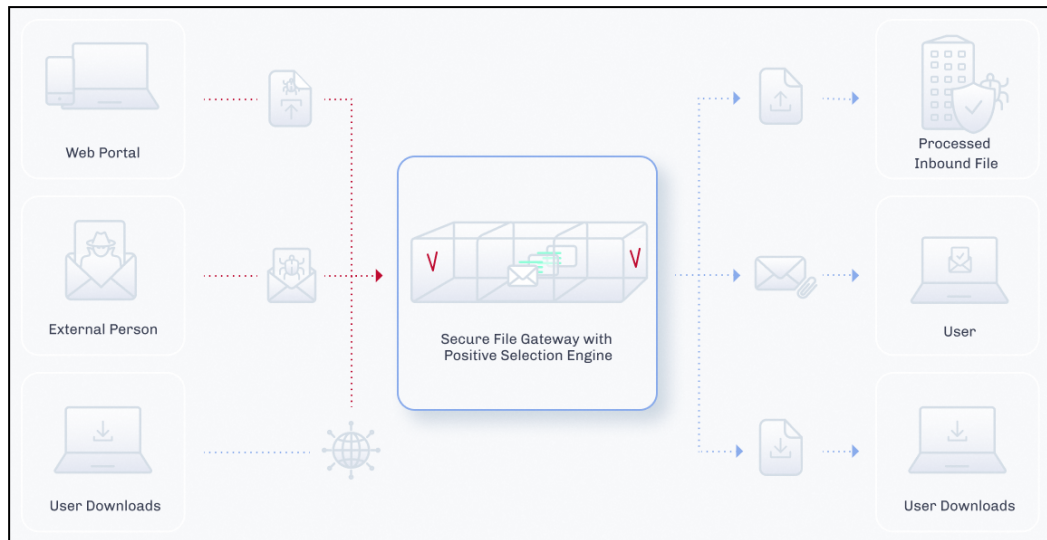
True Type Detection

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's Secure File Gateway 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 Votiro's Secure File Gateway product in relation to other key elements in the network is provided in the following diagram:



Data flows between Positive Selection Engine, Votiro's Secure File Gateway for Web Applications, Secure File Gateway for Email and Secure File Gateway 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 secure file gateway 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

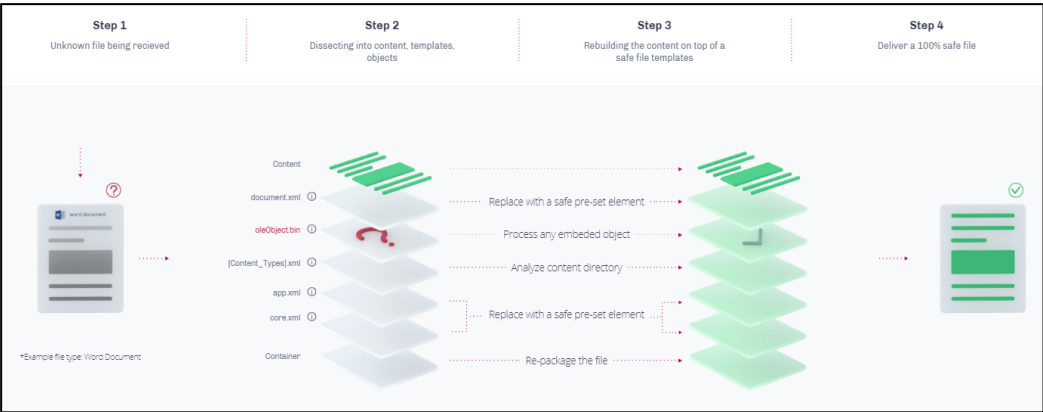
Votiro's Positive Selection Engine is at the heart of the Votiro secure file gateway solution. The Positive Selection Engine keeps only what belongs instead of searching for what does not belong.

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's Secure File Gateway. 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	Other Extensions
PDF	PDF	Adobe PDF	pdf	

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
Image	Animated GIF	Raster Image Files	gif	
	BMP	Raster Image Files	bmp	rle
	EMF	Vector Image Files	emf	
	GIF	Raster Image Files	gif	
	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, msj, 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	Including 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	Other Extensions
Email	Calendar File	Calendar Files	ics	
	DAT File ** ^	EML Files	dat	
	EML File	EML Files	eml	tmp
	Encrypted EML File	EML Files	eml, p7s, p7m	tmp
	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	
	Excel Binary	Microsoft Office Binary Files	xlsb	
	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, xml, pot

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
	Power Point (2007-2010)	Microsoft Office	pptx	ppsx, potx
	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	ppsm
	PowerPointXML ^	Microsoft Office	xml	
	Printer Settings	Microsoft Office Embedded Files	bin	
	Project ^	Microsoft Office	mpp	mpx
	Unknown Ole Object (see note)	OLE Object	bin	
	Visio ^	Microsoft Office	vsd	vss, bin
	Visio (2007-2010)	Microsoft Office	vsdx	
	Visio with Macros	Microsoft Office with Macros	vsdm	
	Word	Microsoft Office	doc	
	Word (2007-2010)	Microsoft Office	docx	dohtml
	Word Pre-2007 Template	Microsoft Office	dot	
	Word Template	Microsoft Office	dotx	
	Word with Macros	Microsoft Office with Macros	docm	dotm
	WordXML	Microsoft Office	xml	

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
Text	Text ^	Text Files	txt	delivery-status, disposition-notification, rfc822-headers, project, csv, cfg, chm, tsv, xsl, xml, xsd, bin, ini, log, xml.rels, vml, rels, doc, manifest, usp, h, abc123
	Postscript File ^	Text Files	ps	
	XML ^	Text Files	xml	
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 Extensions
Other	ACIS Solid Model File ^	CAD Files	sat	
	Adobe Air ** ^	Adobe	air	
	CATIA Product Data File ^	CAD Files	stp	step
	CD Audio Track Shortcut File ** ^	Media Files	cda	
	CSS ^	CSS	css	

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
	DB Files ^	Database Files	dbf	npa, dbt, wnd, tab, mdb
	eDrawings File ^	CAD Files	easm	
	Embedded Macro Files ^	Embedded File	bin	
	Empty File ^	None		
	Equation Ole Object ^	OLE Object	bin	
	Excel2, Excel3, Excel4, Excle5, Excel95 Files ^	Office Files	xls	
	HTML ^	HTML Files	html	htm
	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	
	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	

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
	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	
	SolidWorks File ^	CAD Files	sldasm	sldprt
	Solution User Option File ** ^	Visual Studio Files	suo	
	SQL File ** ^	SQL Files	sql	
	Statistical Files ** ^	Statistical Files	dta	sas7bdat
	Thumbnail File ^	Thumbnail Database Files	db	
	Unrecognized ^	Any Binary Files		
	VCF ^	Exchange	vcf	
	XFA ^	Xfa Files	pdf	
	ZSoft PCX Bitmap File ^	CAD Files	brd	

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 - 100 MB
 - ◆ Raster images - 100 MB
 - ◆ Text - 100 MB
 - ◆ PDF - 80 MB

- ◆ EML - 64 MB
- ◆ ICS - 5 MB
- ◆ Office - 50 MB
- ◆ Vector images - 10 MB

2 Installing Votiro's Secure File Gateway

To install Votiro's Secure File Gateway 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's Secure File Gateway and login to start using the Management Dashboard, follow these four steps:

- Deploy an OVF
- Configure the Network Environment
- Deploy Votiro's Secure File Gateway
- 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 Secure File Gateway with a 3 node cluster. Scale specifications as you increase the number of nodes in your cluster.

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

Table 2 Deployment Specifications

Secure File Gateway	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 Pre-requisites and Considerations

There are both pre-requisites and a number of topics for you to consider when implementing Votiro's Secure File Gateway 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's Secure File Gateway 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's Secure File Gateway 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's Secure File Gateway 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's Secure File Gateway automatically supports load balancing using a basic internal load balancer. We recommend that you implement a hardware-based load balancer in to your production environment to balance between the nodes of your VM.

WARNING!

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

2.2.6 Votiro Registry in Azure

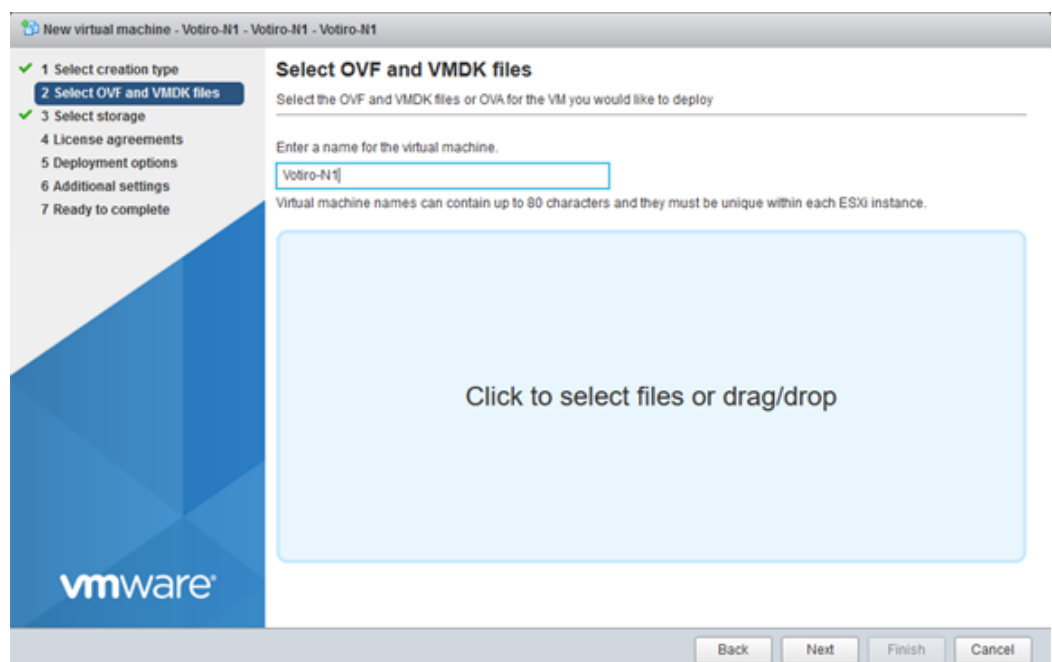
This consideration is relevant when your Secure File Gateway installation includes an online environment.

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

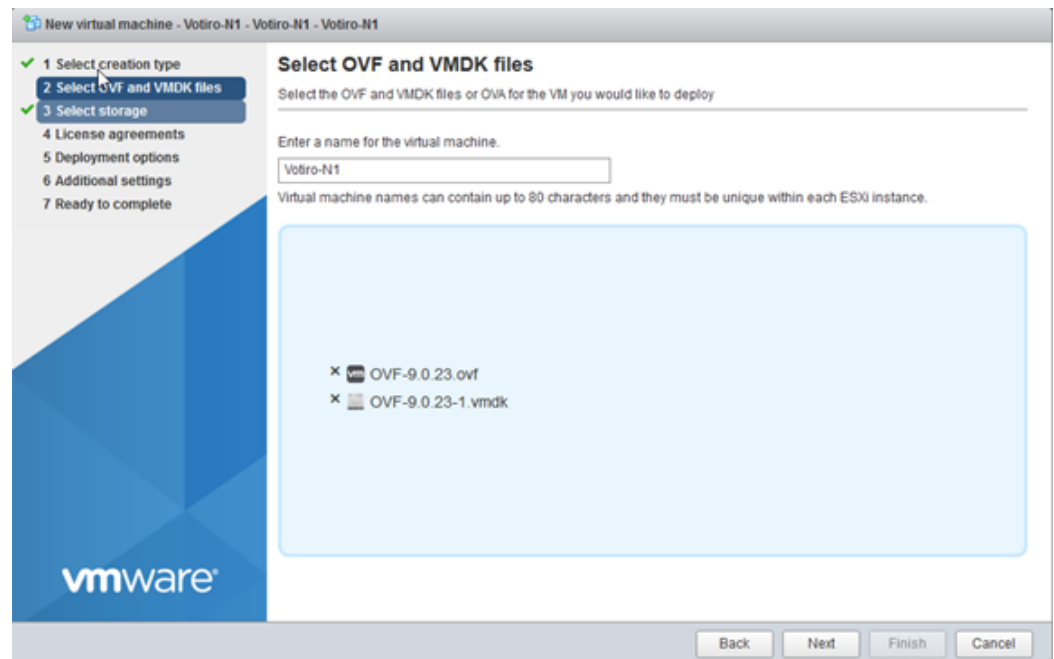
2.3 Deploying an OVF

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

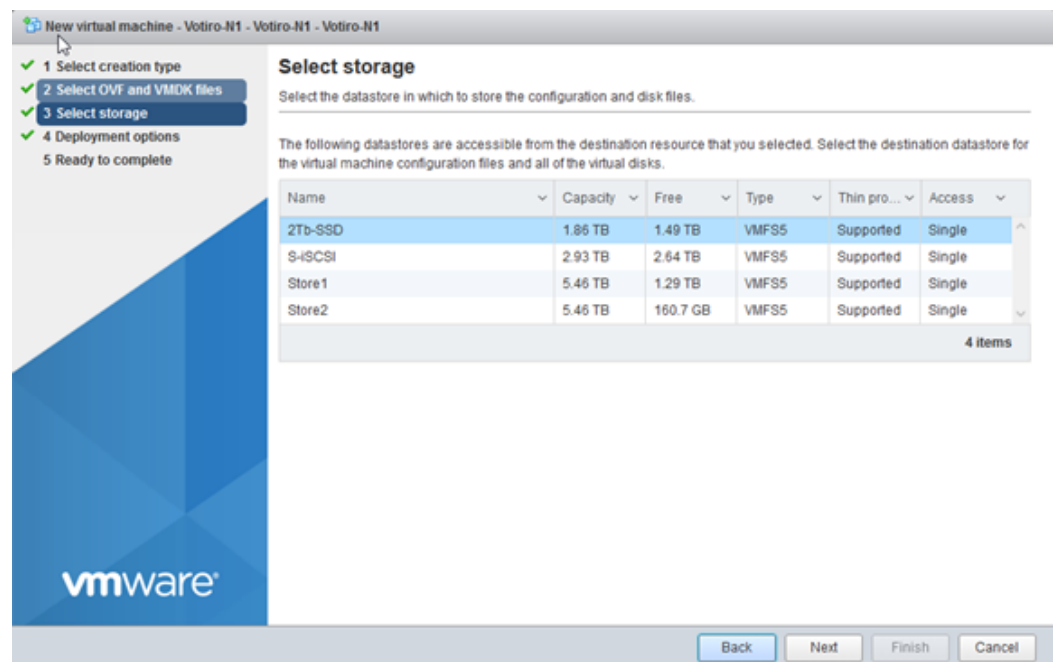
1. Deploy **OVFs**, using these specifications:
 - ◆ 8 CPU
 - ◆ 16 GB Memory
 - ◆ 200 GB Storage
2. Name each **node** uniquely using your corporate naming conventions.



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.

New virtual machine - Votiro-N1 - Votiro-N1 - Votiro-N1

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Ready to complete

Deployment options

Select deployment options

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

Back Next Finish Cancel

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

New virtual machine - Votiro-N1 - Votiro-N1 - Votiro-N1

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

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)

Do not refresh your browser while this VM is being deployed.

Back Next Finish Cancel

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

2.4 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
DNS=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.
 - 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 (173.194.38.188) 56(84) bytes of data.
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.188): icmp_seq=1 ttl=53 time
=117 ms
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.188): icmp_seq=2 ttl=53 time
=118 ms
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.188): icmp_seq=3 ttl=53 time
=111 ms
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.188): 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.

2.5

Deploying Votiro's Secure File Gateway

1. To deploy Votiro's Secure File Gateway select one of the machines and run command:

```
./initcluster.sh
```

2. 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 a one for the VIP.
For example, a 3-node cluster will need 4 IP addresses.

3. Enter the **VIP** for the Secure File Gateway cluster.
4. Enter the Secure File Gateway's **FQDN**, using lower case alphanumeric characters.
5. 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**.

Note

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

6. Enter the IP addresses of the remaining machines.

Note

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](#).

The Secure File Gateway installation has completed successfully. To login to the Management Dashboard, see [Logging in to the Management Dashboard below](#).

2.6 Logging in to the Management Dashboard

To begin using Secure File Gateway's Management Dashboard:

1. Type the Secure File Gateway cluster's **FQDN** name in your web browser. For example, `https://hostname.yourdomain.com`.

The login screen is displayed.

2. Type in the *username* and *password*. Click **LOGIN**.

The *username* and *password* are the same 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 Secure File Gateway User Guide.

The Management Dashboard is displayed.

2.6.1 Configuring Authentication to Active Directory

Following the successful installation of Votiro's Secure File Gateway 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.

2.7 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 Secure File Gateway 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 Secure File Gateway.

2.7.1 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 Secure File Gateway 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.

2.7.2 Customizing PPF Portal Message

The PDF contains a link to Votiro's PPF portal. The user is invited to input the password for the file, at which point processing for Positive Selection Engine will continue. The PPF portal message is created from the **Blocked.rtf** file. You can make changes to this file and maintain consistency with your organization's branding and messaging style.

The **Blocked.rtf** file is used when you update the PPF portal message. The file name must remain the same. Update Secure File Gateway from the same folder, using the following command:

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

The PPF portal message will be used instead of the default.

2.7.3 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 Secure File Gateway 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](#)
- [Generating Reports](#)

To log in to the Management Dashboard:

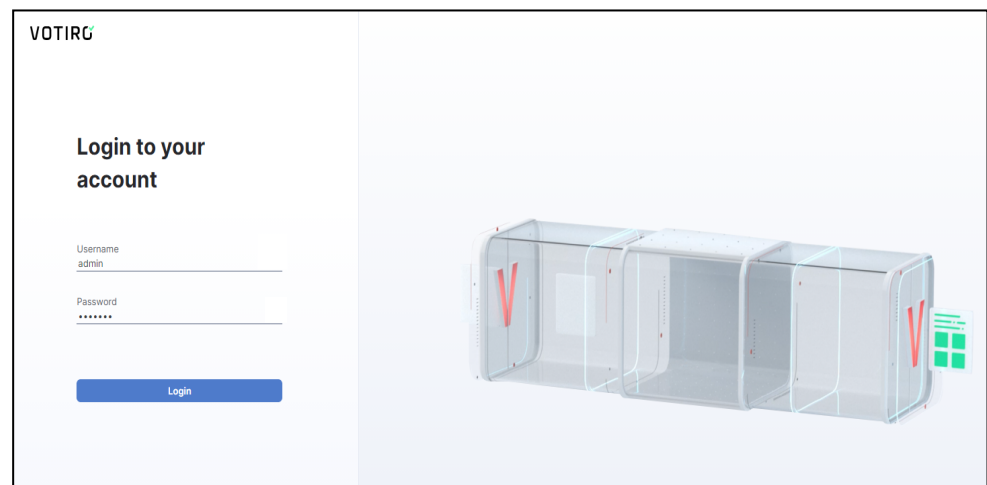
If you have configured the Management Platform to use Active Directory, only users that appear in the Active Directory group can log on.

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

`https://[appliancename]`

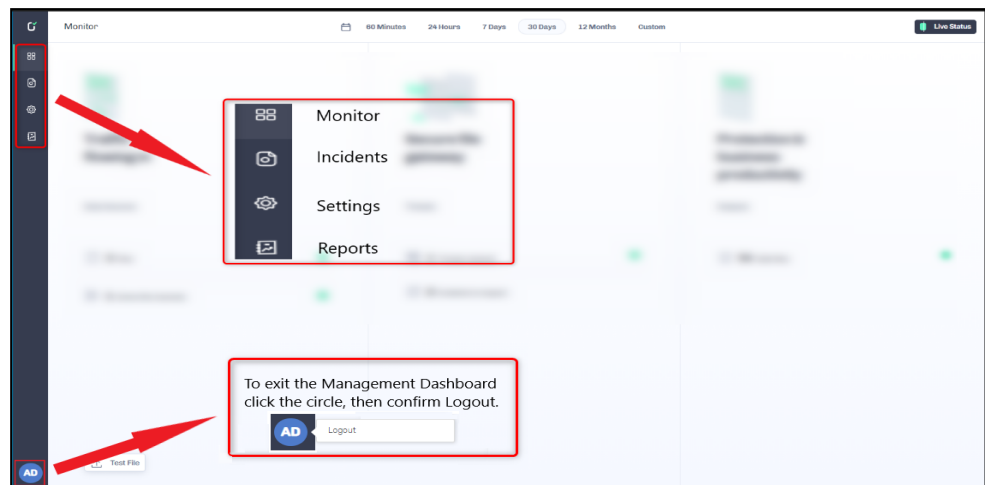
where *appliancename* is the name of the Votiro cluster FQDN hosting the Management Platform.

The login screen is displayed:



2. Type in the **Username** and **Password**, then click **LOGIN**.

The Management Dashboard is displayed.



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.

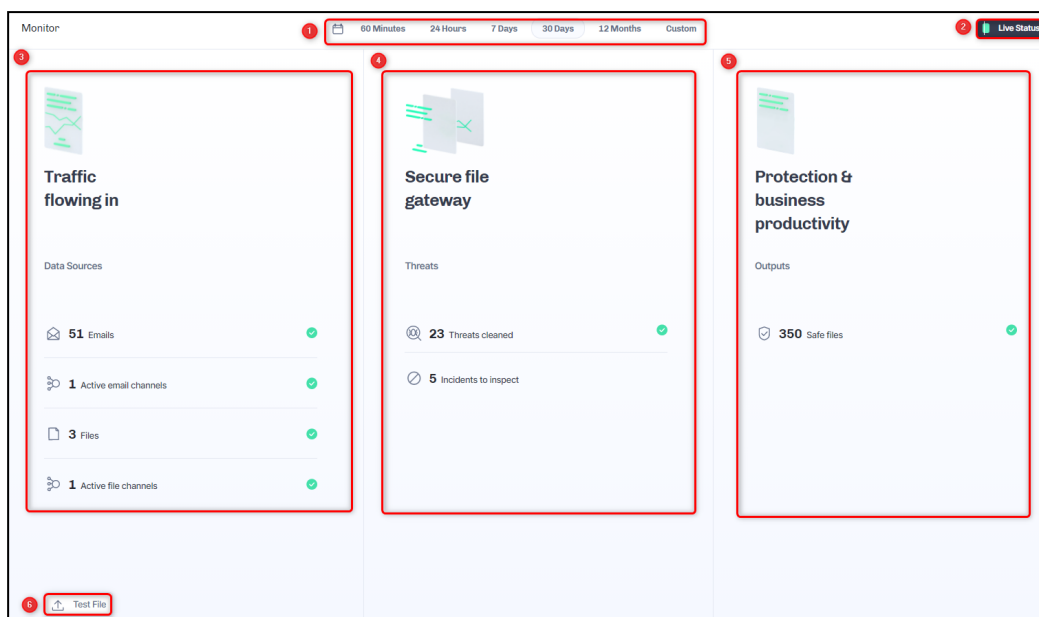
A file is processed for positive selection according to policies for the particular file type. Threats, determined by unknown elements, are detected regardless of policies, whether the file is blocked or not.

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:

- Traffic flowing in
- Secure file gateway
- Protection & business productivity

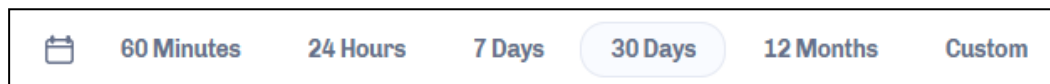


Element	Area	Description
1	Monitoring Periods	Select the time period you wish to display monitoring information for. See Monitoring Periods on the next page .
2	Live Status	Displays the most recent file traffic event activity flowing through Secure File Gateway. See Live Status on page 29 .
3	Traffic Flowing In	Displays channel names and statistical details about files being processed for positive selection. See Traffic Flowing In on page 30 .
4	Secure File Gateway	Displays analysis of threats found and cleaned in files being processed for positive selection. See Secure File Gateway on page 31 .
5	Protection & Business Productivity	Displays performance details from a user's view, highlighting the positive business impact being experienced by using Secure File Gateway. See Protection & Business Productivity on page 32 .

Element	Area	Description
6	Test File	Opens your File Manager and allows you to select a file for testing. See Test File on page 32 .

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.

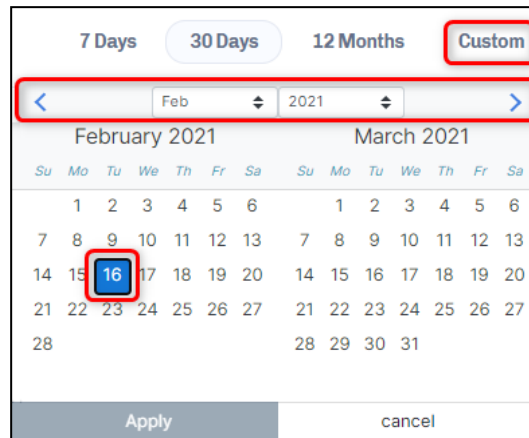


Votiro's Secure File Gateway provides the following predefined settings:

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

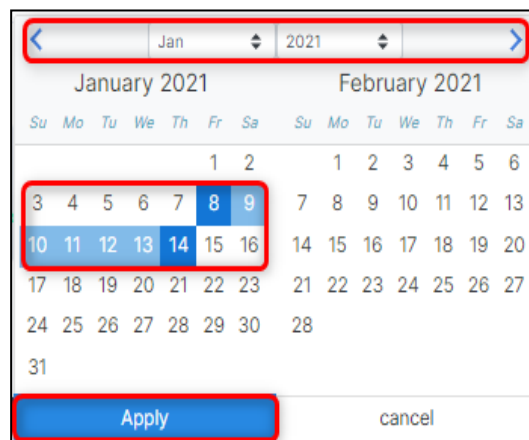
Defining a Custom Period

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



2. Navigate to the desired start month and year by clicking the right and left arrows, or by selecting a month and year using the up/down arrows.
3. To select a start date, tap a date on the calendar, the number turns blue.
4. To select an **end date**, tap a date on the calendar, the number turns blue.

The selected period is highlighted.



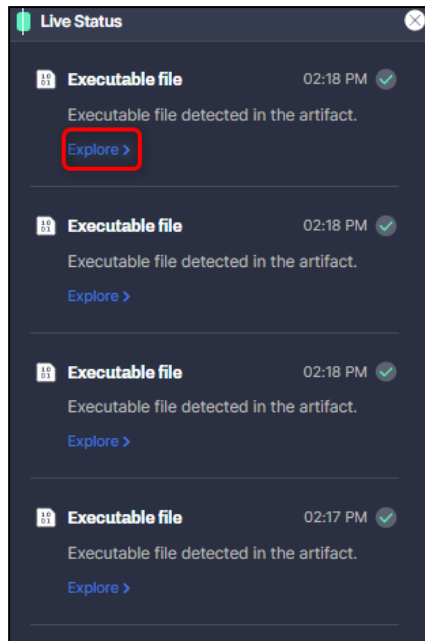
5. Click **Apply**.

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

Statistics update to show information for the custom period.

3.1.2 Live Status

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

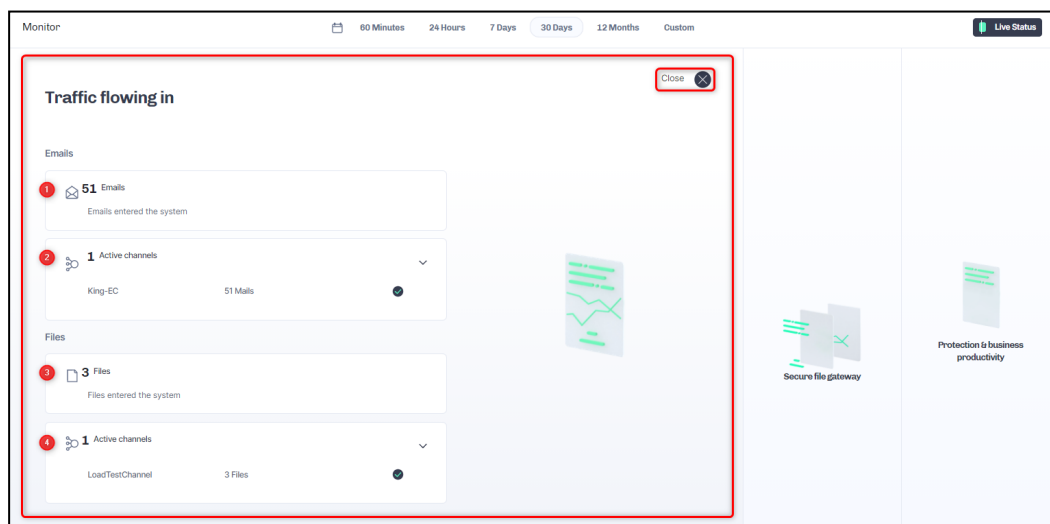


Click **Explore >** to view detailed information about the file, described in [Viewing Detailed File Information on page 35](#).

3.1.3 Traffic Flowing In

The **Traffic flowing in** pane provides details of the active email and file channels connected to Votiro's Secure File Gateway, 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.

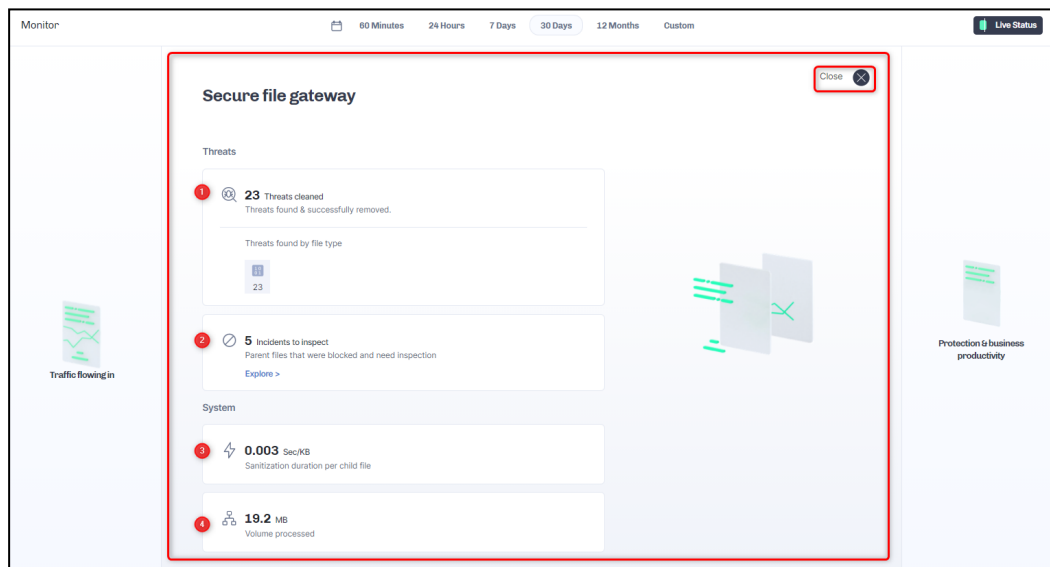


Element	Meaning	Description
1	Emails	The number of emails that entered Secure File Gateway for positive selection processing.
2	Active Channels (Email)	The number of active email channels, with details of the number of emails per named channel.
3	Files	The number of emails that entered Secure File Gateway for positive selection processing.
4	Active 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. To view details, tap a file type.
2	Incidents to Inspect	The total number of parent files that have been blocked and need inspection in the selected period is displayed. To view details, click Explore .

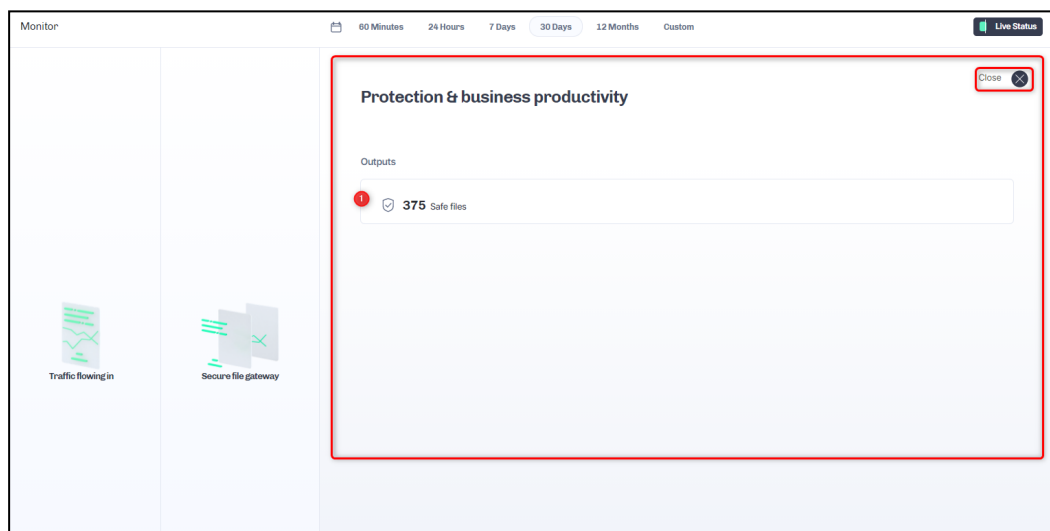
Element	Feature	Description
3	System Sanitization Speed	The system calculation of the average amount of time in Sec/KB it has taken in the period selected to sanitize a child file.
4	Volume Processed	The total volume of files that have been processed for positive selection, displayed in MB.

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 Secure File Gateway.

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 Secure File Gateway. For further information, see [Viewing Detailed File Information on page 35](#).

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).

7 Days ▾ Show all ▾ Connectors ▾ 🔍								
File name	Subject	From	To	Cc	Connector type	Connector name	Blocked files	Date & Time ▾
[📎] B2e1290-4155-4871-9161-d4d3 Fax: Dotov Ipo Y's	yarrh@igmail.com	yarrh@igmail.com	yarrh@igmail.com		None			05/05/2021 15:55
[📎] unnamed_attachment_1 (8).eml	Mavril Caboose Establishment: B...	Claudia.tosser@msf.fr	martina.altmann@gmrschlesch...	vett.frommett@msf.fr, markus.fvix...	None			05/05/2021 13:58
[📎] c531905-de3a-4147-870c-e75f [EXTERNAL] Completed: Please D...	dse_demo@docsign.net	Mark.Remetag@LibertyMutual.com			None		1	05/05/2021 12:07
[📎] c69a35a-64ed-4458-9218-a14 Re: trach n'a pas le droit d'acce...	hoizmanusa@yahoo.com	ben.keffernag@bol.org.il	itana.levi@bol.org.il, ziv.naor@bol...		None			05/05/2021 11:55
[📎] c69a35a-64ed-4458-9218-a14 Re: trach n'a pas le droit d'acce...	hoizmanusa@yahoo.com	ben.keffernag@bol.org.il	itana.levi@bol.org.il, ziv.naor@bol...		None		2	05/05/2021 11:34
[📎] c69a35a-64ed-4458-9218-a14 Re: trach n'a pas le droit d'acce...	hoizmanusa@yahoo.com	ben.keffernag@bol.org.il	itana.levi@bol.org.il, ziv.naor@bol...		None		2	05/05/2021 11:32
[📎] f56e392d-79c5-4052-01fa-40fa test message 1434	outside@sender.net	administrator@madhd.local			Email Connector	Votro Email Connector		03/05/2021 14:34
[📎] faea7bec-b0a0-4640-a5ae-c976 test message 1428	outside@sender.net	administrator@madhd.local			Email Connector	Votro Email Connector		03/05/2021 14:29
[📎] ppt_email.eml					None			03/05/2021 11:41
[📎] word_email.eml					None			03/05/2021 11:41
[📎] Excel_email.eml					None			03/05/2021 11:41
[📎] c531905-de3a-4147-870c-e75f [EXTERNAL] Completed: Please D...	dse_demo@docsign.net	Mark.Remetag@LibertyMutual.com			None			02/05/2021 15:39

The page provides the following features:

The screenshot displays the Incidenta web application interface. At the top, there's a header bar with the title 'Incidents' and a search bar (labeled 3). Below the header, a filter bar (labeled 2) contains dropdowns for '7 Days', 'Show all', and 'Connectors', along with a filter icon. The main content area is a table (labeled 1) with columns: 'File name', 'Subject', 'From', 'To', 'Cc', 'Connector type', 'Connector name', 'Blocked file', and 'Date & Time'. The table lists two incidents: one from 'fesa@tec-6060-4040-a5ae-c976' and another from 'ps_aml.txt'. To the right of each row is an actions menu (labeled 4). At the bottom right, there are icons for user management, help, and settings (labeled 5).

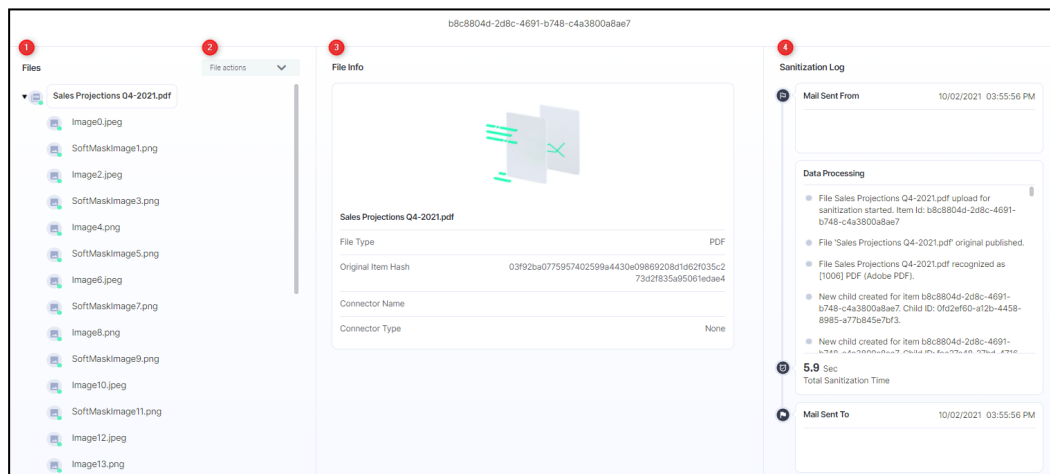
Element	Feature	Description
1	File Details	<p>Displays the file name and other information about the file. The column order can be re-arranged.</p> <p>For all file types, the following is provided:</p> <ul style="list-style-type: none"> ■ File name ■ Connector type ■ Connector name ■ Blocked files ■ Date & Time <p>For email files (EML and TNEF formats), the following is also provided:</p> <ul style="list-style-type: none"> ■ Subject ■ From ■ To ■ Cc <p>For additional file information, tap in the file row.</p> <p>See Viewing Detailed File Information on the next page.</p>
2	Filter	<p>The filter bar contains options for you to refine the list of files according to pre-defined criteria. You can also reset the filter.</p> <p>See Using Filters on page 36.</p>
3	Search	<p>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.</p> <p>See Searching Positive Selection Requests on page 37.</p>
4	Refresh	<p>Refresh the screen for recent files in the blog to be detailed on the page.</p>

Element	Feature	Description
5	Perform Actions on Files	<p>Select from the following three actions for the file selected:</p> <ul style="list-style-type: none"> ■ Download original: the file as it was received, before being processed for positive selection. ■ Download sanitized: the processed version of the file, after being processed for positive selection. ■ Release original: the original file or email is released. For additional information on releasing files, see Releasing Files on page 37.

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**.

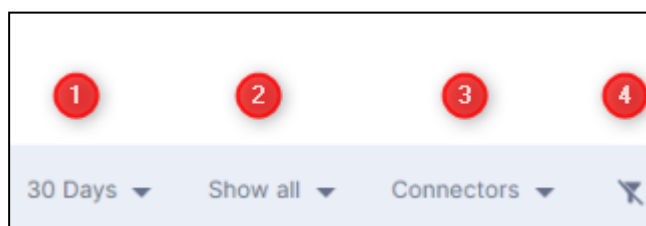


Element	Description
1	<p>Files:</p> <p>Shows details of the file that you clicked in a previous window, in bold. The file is shown within the tree summary of its parents and children. The root is at the top. Scroll up or down in the pane; click the arrows to the left of the filenames to collapse and expand the nodes, as needed.</p> <p>A red dot indicates a blocked element, a green dot indicates a known element.</p>

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

3.2.2 Using Filters

You can filter the file list in the following ways:



Element	Filter	Description
1	Monitoring Period	<p>Select an option from the Monitoring Period list to filter according to a specific time period. The default is 7 Days.</p> <p>Select Custom to define a range of dates. For instructions on how to define a custom period, see Defining a Custom Period on page 29.</p>

Element	Filter	Description
2	Show	Refines the list of files displayed, as follows: <ul style="list-style-type: none">Show all (default)Show blocked itemsShow sanitized items.
3	Connector	If you have more than one Secure File Gateway Connector installed, you can filter the file list by connector type using the Connector list.
4	Filter Icon	Clears filter and returns to default setting.

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. 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 Secure File Gateway. 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 Secure File Gateway for Web Downloads.

Note

To enable the release of blocked files, you must first configure Secure File Gateway for Web Downloads.

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

The original file is sent to the OUT folder.

Releasing the Original Version of a Blocked Email

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

Note

To enable the release of blocked files, you must first configure the following system settings:

- SMTP Server location
- SMTP Server port
- SMTP Server username
- SMTP Server passwords

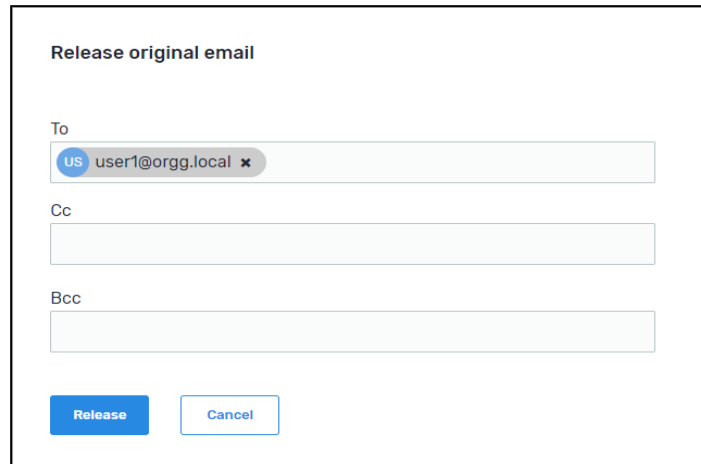
For more information, see [Configuring Settings on the next page](#).

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

To release a blocked email follow these steps:

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

The following dialog is displayed:



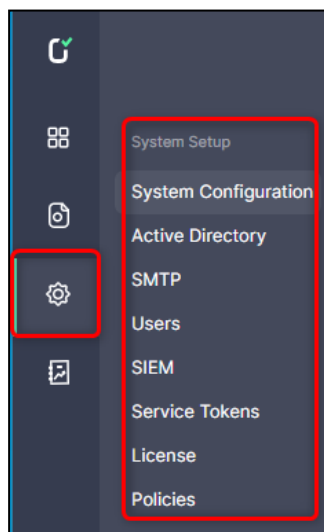
The dialog box is titled "Release original email". It contains three input fields for email addresses: "To", "Cc", and "Bcc". The "To" field is populated with "user1@orgg.local" and has a small "x" icon to its right. Below the input fields are two buttons: "Release" (in blue) and "Cancel" (in white with a blue border).

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

2. Accept the email addresses that are displayed or delete one or more, as required. You cannot add email addresses.
3. To send the email, click **Release**. The email is sent.

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

- Company Name**
Type in your company name
Name
Your company
- File History**
Select the number of days to keep files in storage
Days to keep
30
- Password Protected File History**
Select the number of days to keep password protected files in storage
Days to keep
180
- Date Format**
Select your preferred date format
Date
DD/MM/YYYY
- Time Format**
Select your preferred time format
Time
HH:mm
- 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 Generating Reports on page 54 .
2	File History	Specify for how many days the system saves files. The default is 30 days.
3	Password Protected File History	Specify for how many days the system saves password-protected files. The default is 180 days. Note After the configured period, the original file is deleted and cannot be retrieved through the dashboard.
4	Date Format	Select your preferred date format for the display of information in the dashboard --either MM/DD/YYYY or DD/MM/YYYY.

Element	Field	Description
5	Time Format	Select your preferred time format for the display of information in the dashboard -- either a 12-hour clock or 24-hour clock, using the format HH:MM or HH:MM (AM/PM) .
6	System Language	Select your preferred system language. To add languages to the list you must translate Dashboard dictionary and upload the translation. The default language is EN , English.

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 * IP / Hostname

Type in your organization Active Directory address

2 Active Directory Server Port * Port

Type in your organization Active Directory server port

389

3 Active Directory User Group * Group Name

Type in your Active Directory user group

Votiro_Users

4 Active Directory Username * Username

Type in your Active Directory username

5 Active Directory User Password * Password

Type in your Active Directory user password

6 SSL

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">■ DOMAIN\UserName - For example, VT\Jane.Smith■ UserName@FQDN - For example, Jane.Smith@Votiro.com <p>Key:</p> <p><i>DOMAIN</i> - the NetBIOS domain name</p> <p><i>UserName</i> - the login name of the user</p> <p><i>FQDN</i> - the domain name in full</p>
5	Active Directory User Password	Specify the login password for the Active Directory server.
6	SSL Usage	Specify whether to use SSL.
7	Test Connection	Before saving changes you should test the connection to Active Directory. To select a file for testing, click Test .

Note

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

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

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 37](#).

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

Settings

SMTP

1

SMTP Server Address

Type in your organization SMTP server address

IP / Hostname

127.0.0.1

2

SMTP Server Port

Type in your organization SMTP server port

Port

25

3

SMTP Server Email

Type in your SMTP server email

Username

JOHN_DOE@MYDOMAIN.COM

SMTP User is required

4

SMTP Server Password

Type in your SMTP server password

Password

5

Test Email

send a test email in order to check the connection

Test

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	<div>To test the SMTP settings, click Test.</div> <div><div><div></div><div>If the settings are valid, a verification code is displayed in the Management Dashboard.</div><div>The same code appears in an email message that is sent to the address you specified.</div></div><div><div>Test Email</div><div>To check the SMTP connection send a test email, click Test.</div><div><div>Test</div><div>An email has been sent containing the following number</div><div>3 5 1 8 4</div></div></div><div><div></div><div>If the settings are invalid, an error is displayed below the button.</div></div></div>

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 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

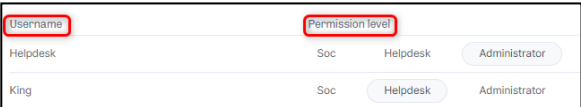
Active Directory Group
 AD Group for Votiro users

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	<div><p>The Votiro Admin role provides direct administrative access to Secure File Gateway, independent of Active Directory.</p><p>To change the Votiro Admin password:</p><ol style="list-style-type: none">Click .Enter the Current Password and then Confirm New Password.Click Save, or Cancel.</div> <div><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></div>

Element	Field	Description
2	Active Directory Group	<p>Users must be in the Votiro_Users Active Directory group.</p> <p>The three levels of permission are:</p> <ul style="list-style-type: none">■ SOC: users will only be able to view the dashboard and use the TEST FILE functionality. They will not have access to personal data, or be able to change settings.■ Helpdesk: users will be able to manage the positive selection process and release of personal files and emails, in addition to SOC permissions.■ Administrator: users will have access to the entire system, including personal files and emails. They have permission to edit policy configurations and system settings, in addition to Helpdesk permissions. <p>To set a user's Permission Level go to the options to the right of the Username, click the permission level to be granted. The level selected is highlighted.</p>  <p>WARNING!</p> <p>The system must have a minimum of one Administrator user set up in the Active Directory Group for Votiro users.</p> <p>A warning message appears if you attempt to Save the settings with no user set with Administrator permissions.</p>

3.3.5 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. 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. For more information about SIEM logging in Management, see Sending Logs to SIEM in CEF on page 63 .

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.

3.3.6 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's Secure File Gateway.

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

Creating a Service Token

To create a new service token:

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

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

3. Click **Create**.

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

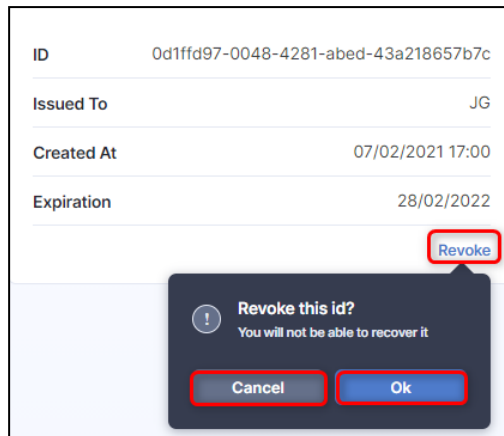
IMPORTANT!

The service token generated is not stored by Votiro's Secure File Gateway. You must copy it immediately.

5. Click **OK**.
6. A list of service tokens created are displayed on the Service Token page.

Revoking a Service Token

To withdraw a service token, click **Revoke**. A confirmation pop appears warning that a revoked service token cannot be recovered.

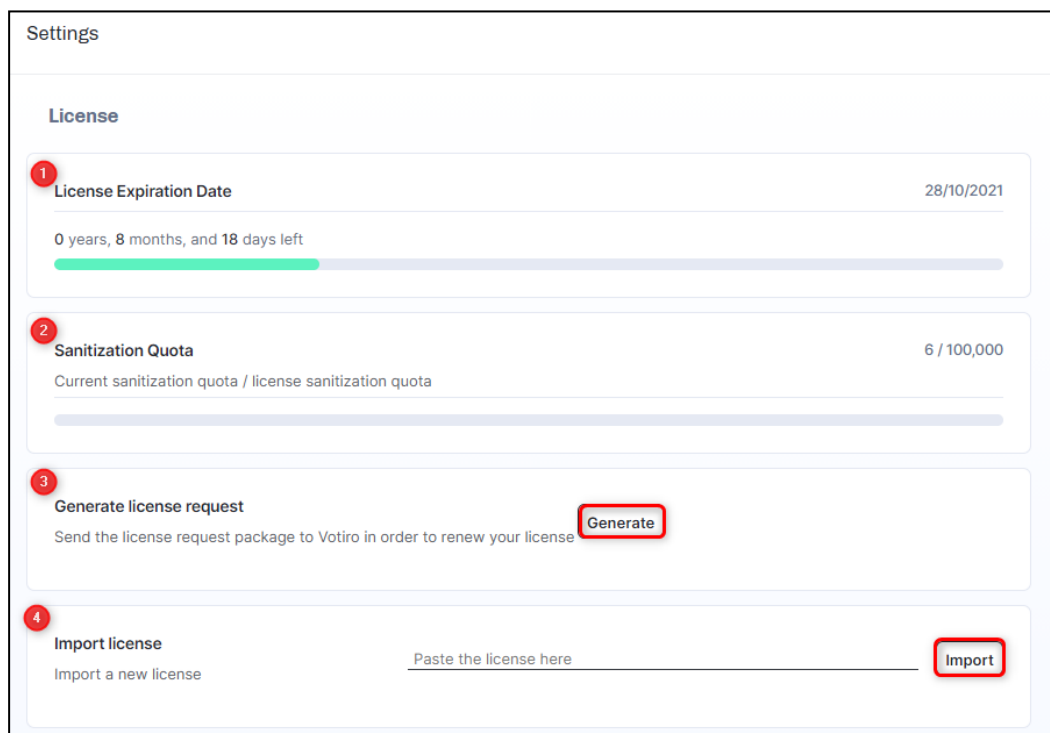


Click **OK** to continue revoking the service token, or **Cancel** to continue using the service token.

3.3.7 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 number of files processed against the quota.

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	The first figure represents the number of files that have been processed. The second figure represents the licensed quota of files to be processed.
3	Generate License Request	<p>Click Generate to produce a license request package. The file licensePackage.zip is generated and located in your downloads folder.</p> <p>Pass this file to Votiro Support. A license key will be generated and returned to you within 24 hours of receipt of the request.</p>
4	Import License	<p>Enter the license key provided by Votiro Support and click Import. Successful validation automatically updates License expiration date and Sanitization quota information. The license key disappears.</p> <div> <p>Note</p> <p>Votiro's Secure File Gateway is activated up to five minutes after the license key import.</p> </div>

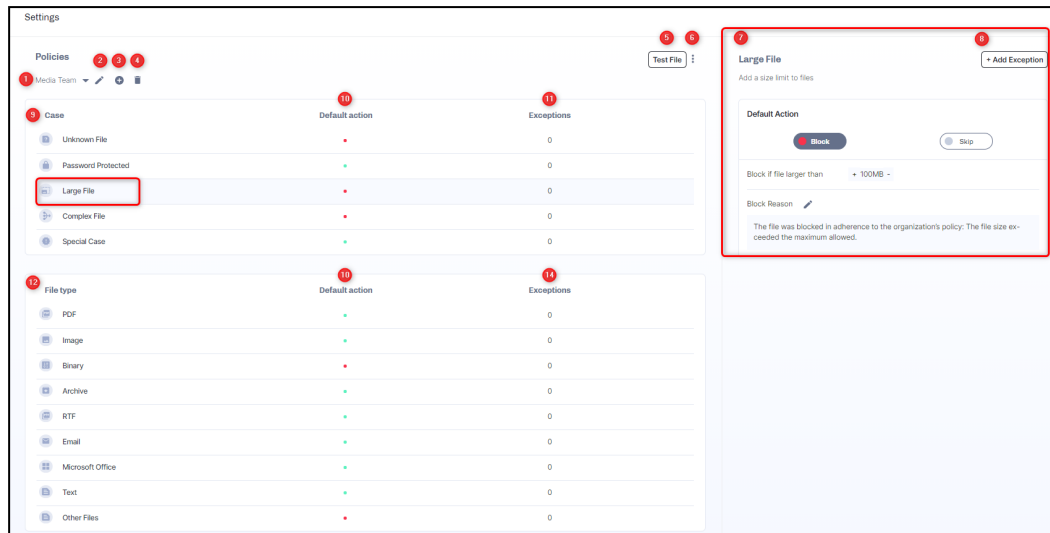
3.3.8 Policies

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

Policies Dashboard

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

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



Element	Meaning
1	The name of the currently displayed policy. To display a policy, select from the list of defined policies. You can set up policies for specific teams or individuals.
2	Edit the policy name.
3	Add a new policy.
4	Delete current policy. This element only displays when additional policies have been defined. The default policy cannot be deleted.
5	Select file to test policy.
6	Import/Export policy file.
7	Displays details of the item that is selected on the left. For each case or action, you can define how it must be handled.
8	Add an exception. For example, when managing other file types, with specific email addresses and/or URLs.
9	Displays details of the selected policy by case.
10	<p>Displays the status of the default action taken for the policy.</p> <p>A colored dot illustrates your current policy action:</p> <ul style="list-style-type: none"> Red - files will be blocked Green - files will be processed using your sanitization settings Grey - files will be skipped
11	Displays the number of exceptions defined per policy case or file type.
12	Displays the details of the selected policy by file type.

Note

Change made in policies are updated in the Positive Selection Engine every few seconds. Once updated in the Positive Selection Engine, it is available to Secure File Gateway reference clients, such as Secure File Gateway for Email or Secure File Gateway 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 69](#).
- **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 72](#).
- **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 76](#).
- **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, Secure File Gateway uses a default policy. Each case and file type has a different default policy.

File Blocking

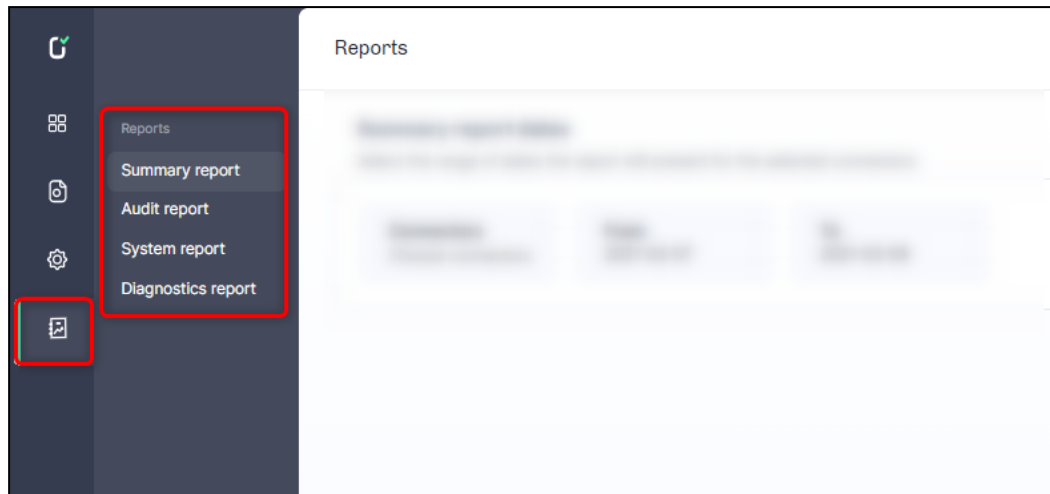
When you configure a policy to block a file, no other policy rule is applied on the file. A **block file** containing information about the blocked file and the reason it was blocked replaces the original file. You can accept the block file default text or edit it.

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 Generating Reports

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

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



3.4.1 Summary Report

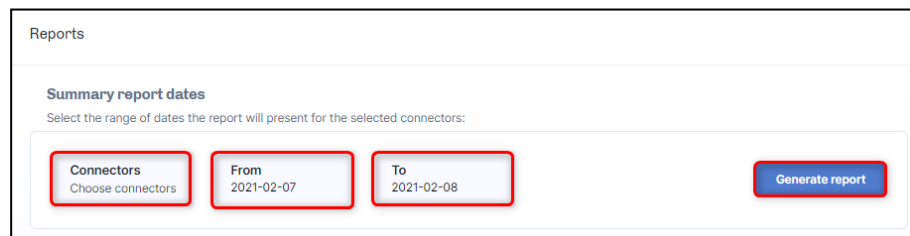
You can generate a summary report of the positive selection processing activity in your organization for a specified period.

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

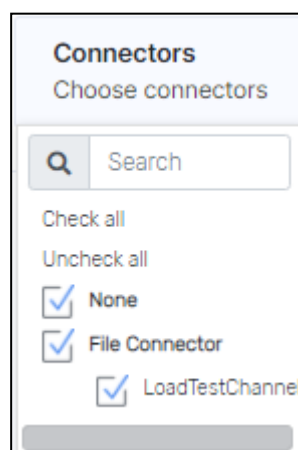
The report presents usage and security data in graphic format and also provides tips for optimizing your positive selection processing effort.

To generate a Summary report, follow these steps:

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

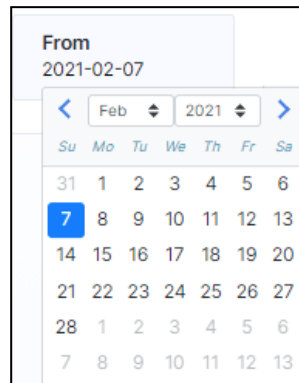


2. Click **Connectors**, then select the connectors you wish to appear in the report.



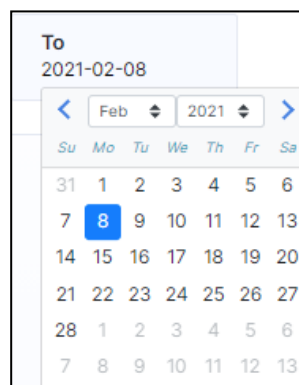
3. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:

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



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

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



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

4. Click **Generate Report**.

The Summary report is generated.

Summary Report Format and Structure

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

- Company name.
- Number of processing requests to Votiro's Positive Selection Engine.
- Number of individual files that were processed Votiro's Positive Selection Engine.
- Number of files that were blocked.
- Number of threats that attempted to enter your organization.

- Number of files that were blocked according to each positive selection policy.
- Number of files that were blocked and that were detected as threats.
- Number of files that were blocked that were not threats.
- Average processing time in seconds/KB.
- File types that passed through the Positive Selection Engine.
- Number of threats that attempted to enter your organization.
- Most threatening file types that were sent to your organization.

3.4.2 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's Secure File Gateway 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:

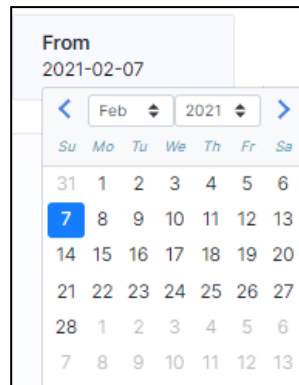
1. In the navigation pane, click **Reports > Audit report**.



The screenshot shows the 'Reports' section of the Votiro Management Dashboard. Under the 'Audit report dates' heading, there is a prompt 'Select the range of dates the report will present'. Below this, 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'.

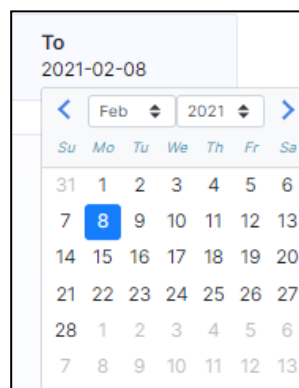
2. The default range of dates for the report is from yesterday to today. To define a date range for your report, follow these steps:

- 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.

3.4.3 System Report

Votiro's Secure File Gateway 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**.

Reports

System report time-frame

Select the range of date and times the report will present

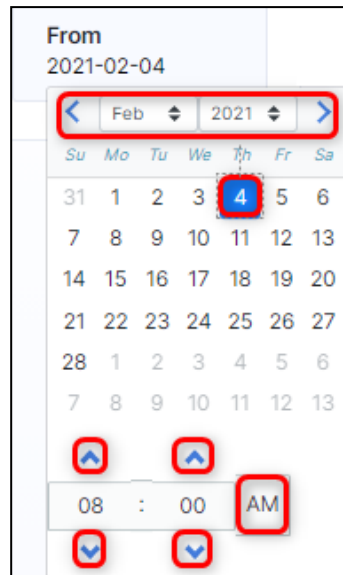
From
2021-02-04

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:

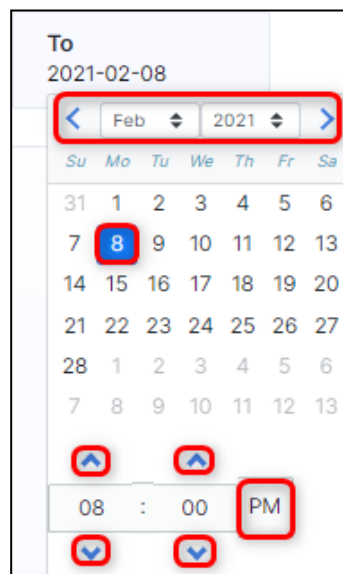
- a. To select the start range of the report, click **From**, a calendar displays.



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.



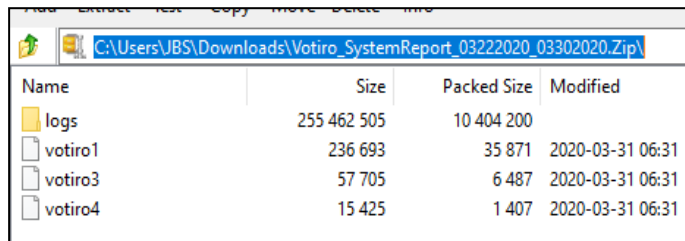
The selected date is blue. To change the end date for the report use the selection steps described in **2a** above for the day and time for report to end.

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.

3.4.4 Diagnostics Report

Votiro's Secure File Gateway 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

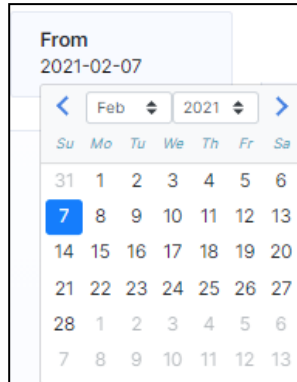
Select the range of date and times the report will present

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:

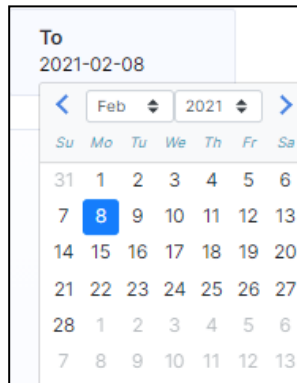
- a. To select the start date from the report, click **From**, a calendar displays.



The screenshot shows a date picker interface. At the top, it says 'From' and '2021-02-07'. Below this is a calendar for February 2021. The days of the week are abbreviated as Su, Mo, Tu, We, Th, Fr, Sa. The dates are arranged in a grid. The date 7 is highlighted in blue, indicating it is the selected start date.

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 screenshot shows a date picker interface. At the top, it says 'To' and '2021-02-08'. Below this is a calendar for February 2021. The days of the week are abbreviated as Su, Mo, Tu, We, Th, Fr, Sa. The dates are arranged in a grid. The date 8 is highlighted in blue, indicating it is the selected end date.

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's Secure File Gateway 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 47](#).

Here is an example of a SIEM message in Votiro's Secure File Gateway:

```
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 Secure File Gateway.
- **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 65](#).
- **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. 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 Secure File Gateway 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 52](#).

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 76](#).

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	<p>You can block or skip these files.</p> <p>If you select Skip, the unknown file is not processed for positive selection and the original version will reach the destination folder.</p>


















Case	Processing Options
Password Protected	<p>You can block or process these files. By default, the files are processed for positive selection.</p> <ul style="list-style-type: none"> ■ Return file by email with User Message: Allows you to return a password protected file by email. Accept the default text notification message, or edit it. ■ User Message: Allows you to edit the message sent to the recipient of the password protected file. See Instructions for Email User below. ■ Block unsupported files with Block Reason: Allows you to block unsupported files (such as Visio files). Accept the default text notification message, or edit it. <p>When the files are blocked, Secure File Gateway 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 1032 1417 1272"> <p>Note</p> <p>This feature supports the following file types only: PDF, ZIP, 7zip, RAR, DOC, DOCX, DOT, DOTX, DOCM, DOTM, XLS, XLT, XLSX, XLTX, XLSM, PPT, PPS, POT, PPTX, PPSX, POTX and PPTM. It does not work on other file types that can be protected by a password, such as Visio files.</p> </div> <p>Instructions for Email User</p> <p>The Secure File Gateway administrator should communicate the following information and instructions to the users.</p> <p>An email message with password protected files attached can be processed for positive selection and returned as an email attachment, or as a download. The user receives a message that a password protected file has been received, with the option to enter the password, then click Get File.</p> <p>The password protected file is processed for positive selection, then attached to the email. This is distributed to all named recipients. If Secure File Gateway 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 1861 1417 1962"> <p>Note</p> <p>This feature supports the use of one password per email.</p> </div>

Case	Processing Options
Large File	<p>You can set the minimum size of files you want to block.</p> <p>When this option is checked, for every file that Secure File Gateway 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 Load File. For more information, see Defining Policies on page 54.</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 52](#).

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 76](#).

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"> ■ Remove multimedia: Specifies whether multimedia such as embedded video, audio, 3D annotations, and rich media annotations must be removed. Default is checked. ■ Clean embedded fonts: Specifies whether embedded fonts must be processed. Default is checked. ■ Block files with suspicious links: Performs a check of all links in the form HTTP:// and HTTPS:// in a PDF document. If any link is found to be suspicious, 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 Block Reason message. Default is unchecked. ■ JavaScript handling: Determines how JavaScript, if found in the PDF file, is handled. <ul style="list-style-type: none"> ◆ Don't do anything ◆ Remove only suspicious scripts ◆ Remove all scripts (this is the default)
Image	<p>By default, these files are processed for positive selection.</p> <ul style="list-style-type: none"> ■ Add micro-changes: Adds security noise to images during processing. Default is checked. <div style="background-color: #f2f2f2; padding: 10px; margin: 10px 0;"> <p>Note</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"> ■ Remove metadata: Removes EXIF metadata from JPEG and TIFF images. Default is unchecked. ■ Max compression for lossless formats: Compresses lossless image formats (PNG, BMP, and RAW) by 100%. Default is checked. ■ Compression level: The processed image is compressed to preserve a reasonable image file size. You select one of four compression levels (from low to high) that trade off file size with image quality. The lower the compression level, the larger the file, and the higher the image quality. The higher the compression level, the smaller the file, and the lower the image quality. Default is 25% compression.
Binary	<p>The processing option is not relevant to managing binary files. You either block binary files or allow them.</p>

File Type	Processing Options
Archive	<p>By default, these files are processed for positive selection.</p> <p>Block zip bomb: Detects and blocks zip files with abnormal compression ratio. These might pose a denial of service threat, consuming system resources such as CPU or disk. Any zip files with compression ratio higher than 99.8% will be considered a zip bomb and be blocked. When selected you can edit the Block Reason message. Default is checked.</p>
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"> ■ Block files with suspicious links: 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 Block Reason message. Default is unchecked.

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

Appendix D Adding Policy Exceptions

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

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

- File type
- File size
- Email (for Secure File Gateway for Email only)
- File extension
- Digital signature

For more information about the policies page, see [Policies Dashboard on page 52](#).

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

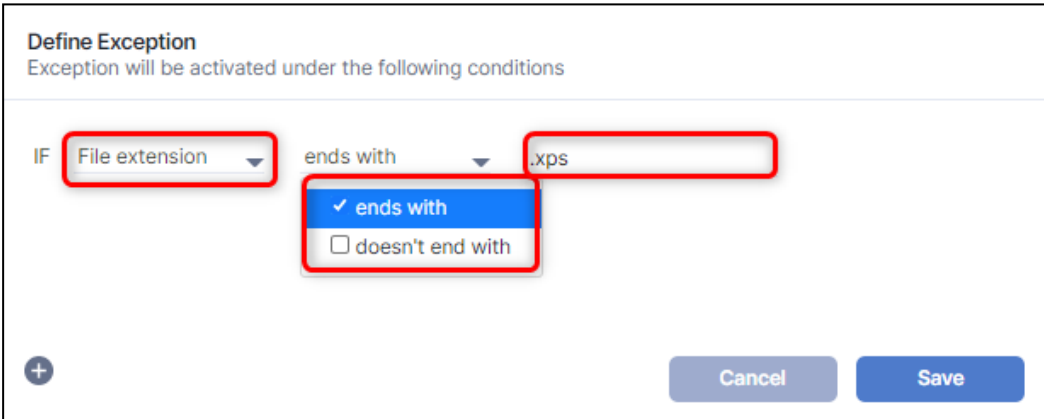
You can specify:

- 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 subtitle 'Exception will be activated under the following conditions'. It features a rule configuration interface with the following elements:

- An 'IF' label followed by a dropdown menu currently set to 'File extension'.
- A second dropdown menu set to 'ends with'.
- A text input field containing '.xps'.
- A blue button with a checkmark and the text 'ends with'.
- A grey button with a checkbox and the text 'doesn't end with'.
- A plus sign icon in a circle at the bottom left.
- 'Cancel' and 'Save' buttons at the bottom right.

Red rectangular boxes highlight the 'File extension' dropdown, the 'ends with' dropdown, the '.xps' text field, and the 'ends with' button.

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**.