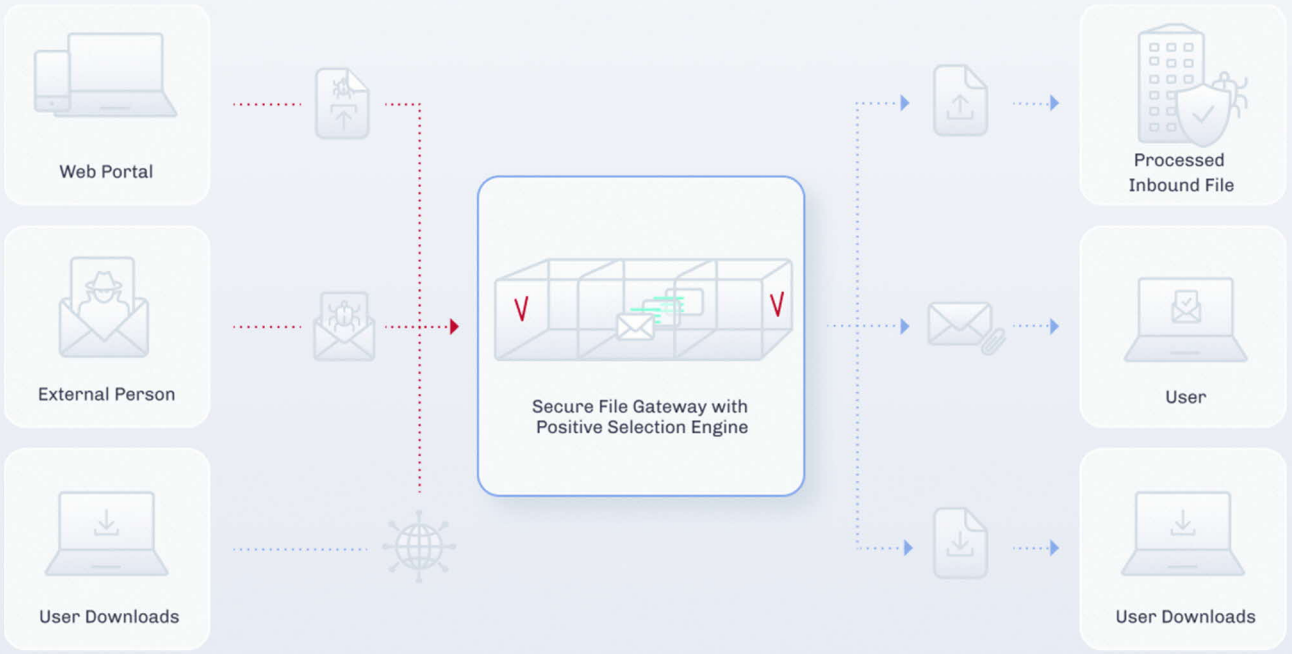
VOTIRO

Secure File Gateway

User Guide

Version 9.3

October 2020



VOTIRO

Copyright Notice

www.votiro.com

Contents

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.

1.1.1 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.

1.1.2 Content Disarm and Reconstruction (CDR)

Votiro's patented and award-winning products use next-generation CDR technology to identify and disarm malware from incoming files, then reconstruct them, while preserving the integrity and functionality of the original data before reaching your network – all in less than 1 second.

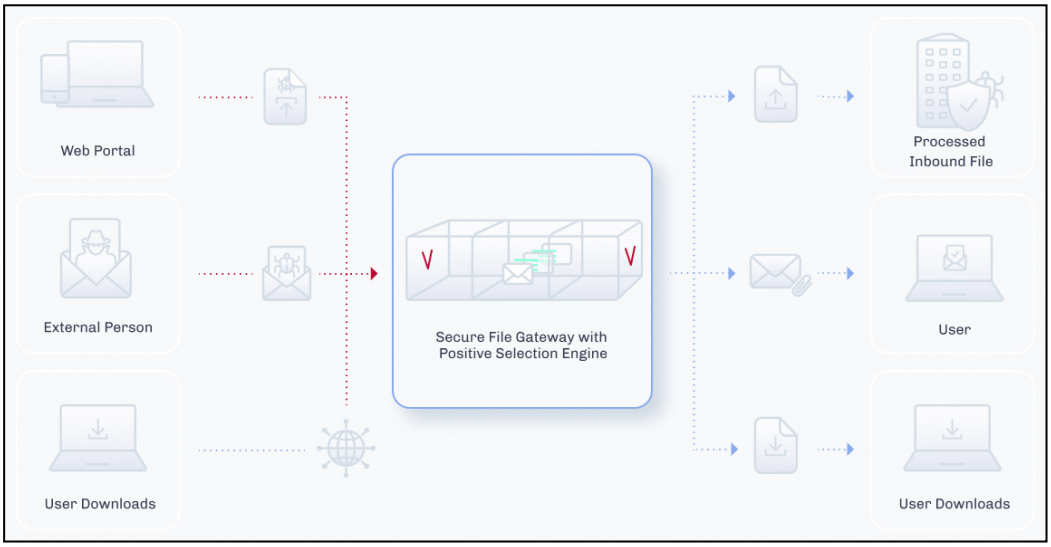
Votiro's proprietary technology allows users to safely open email attachments, download and transfer files, share content, and use removable devices – all without giving it a second thought. Supporting mobile and desktop editions of a vast arsenal of file types, including Microsoft Office, RTF, PDF (such as Adobe PDF), image, and archive files, Votiro's CDR technology provides automatic security, removing the human factor from the security process.

Positive selection is achieved through micro changes to the structure and metadata of a file. Invisible to users, these changes do not affect the file's usability but eliminate the possibility of malicious code being run from the file, thereby eliminating the threat.

By actively processing all files, without having to detect threats in advance, Secure File Gateway's protection surpasses traditional methods and removes undisclosed, advanced threats before they can enter your organization.

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

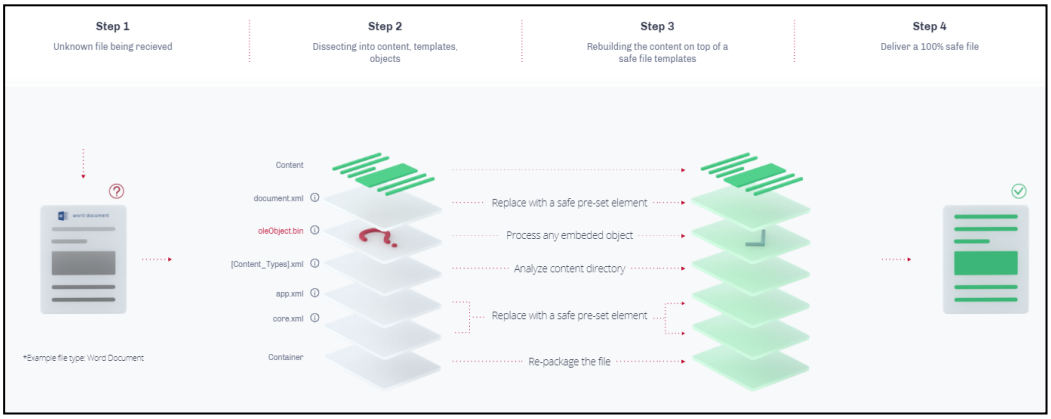
Votiro's Positive Selection Engine is at the heart of the Votiro secure file gateway solution. The Positive Selection Engine keeps only what belongs instead of searching for what does not belong.

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 following 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 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	
	TIF	Raster Image Files	tif	tiff
	WDP	Raster Image Files	Wdp	
	WMF	Vector Image Files	wmf	
Binary	Binary File ^	Any Binary Files	dat	db
	Executable ^	Any Binary Files	exe	com, dll, pif, sfx, msu, msp, msi, mo
Archive	7Z File	Archives	7z	
	CAB file	Archives	cab	wsp
	GZ File	Archives	gz	
	GZIP File	Archives	gzip	
	InstallShield CAB file ^	Archives	cab	
	LZH File ^	Archives	lzh	
	RAR File	Archives	rar	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
	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 on xml format ^	Malformed Microsoft Office	xls	
	Excel Template	Microsoft Office	xltx	
	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	
	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	dochtml
	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	
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	

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
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	
Other	ACIS Solid Model File ^	CAD Files	sat	
	Adobe Air ** ^	Adobe	air	
	Binary Excel (2007-2010) ^	Microsoft Binary Office Files	xlsb	
	CATIA Product Data File ^	CAD Files	stp	step
	CD Audio Track Shortcut File ** ^	Media Files	cda	
	CSS ^	CSS	css	
	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	
	Excel95 File ^	Unsupported 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

File Type in Management	File Type	Family Type	Main Extension	Other Extensions
	LabView ** ^	LabView	vi	
	Material Exchange Format File ** ^	Media Files	mxf	
	Media File ^	Media Files	mp3	wav, wmv, ico, mpg, mpeg, flv, wma, mov, avi, mp2, mp4, m4a, 3gp, mts, mkv, vob
	MHT File ^	MHT Files	mht	
	MST files ** ^	Installer Setup File	mst	
	p7s ^	Digital Signatures	p7s	
	Parasolid model File ** ^	CAD Files	x_t	x_b
	Pcx File ^	CAD Files	pcx	
	Pgp File ^	Encrypted Files	pgp	
	PowerPoint95 File ^	Unsupported Files	ppt	
	PreR14Dwg File ^	CAD Files	dwg	
	PreWord97 File ^	Unsupported Files	doc	
	PSD File ^	Photoshop Files	psd	
	RPT ** ^	RPT Files	rpt	
	RSP File ** ^	PLC Files	rsp	
	Script ^	Batch Files	bat	js, php, cmd, vbs, reg, pl, lnk, py, asp
	Shortcut File ^	Shortcut Files	url	
	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	

Notes

- Unknown Ole Objects: Both generic and unknown Ole objects are handled.
- Generic Ole objects will be processed, and unknown Ole objects will be blocked.

2 Installing Votiro's Secure File Gateway

To install Votiro's Secure File Gateway quickly into your organization we will create a cluster of three virtual machines (VM). We will use four static IPs, one for each of the three VMs and a VIP for the cluster. Each VM requires the following dedicated resources: 8 CPUs, 16 GB of memory and 200 GB SSD.

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!**
> Your may need to determine in advance of your installation the following:
>
> - 4 unique IP addresses;
> - Hostname for FQDN (use lower case alphanumeric characters).

2.1 Considerations

There are 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 Internal Communication
- Using an External Storage Server
- Load Balancing
- Votiro Registry in Azure

2.1.1 Ports

Network connectivity requirements enabling secure outbound and inbound communications with Votiro's Secure File Gateway are detailed in the tables below.

Table 2 Outbound Firewall Rules

Outbound	Source	Destination
Releasing Files	ovf_network	Exchange / Edge
Active Directory	ovf_network	Domain Controller
SIEM	ovf_network	SIEM Server

Table 3 Inbound Firewall Rules

Inbound	Source	Destination
SSH, SCP	Any	ovf_network
Processing Request	API Client	ovf_network
Monitoring Grafana	Grafana	ovf_network
Monitoring Prometheus	Prometheus	ovf_network

2.1.2 Virtual Appliance Communication Settings

Internal Communication Settings

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

- 6443/tcp
- 2379-2380/tcp
- 10250-10252/tcp
- 22/tcp
- 10255/tcp
- 8472/udp
- 24007 – 24008/tcp
- 49152 – 49154/tcp

External Communication Settings

For external communications, the following settings are required:

- 22/tcp
- 443/tcp

2.1.3 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.

To configure External Storage contact Votiro Support.

> **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.

2.1.4 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.

2.1.5 Votiro Registry in Azure

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

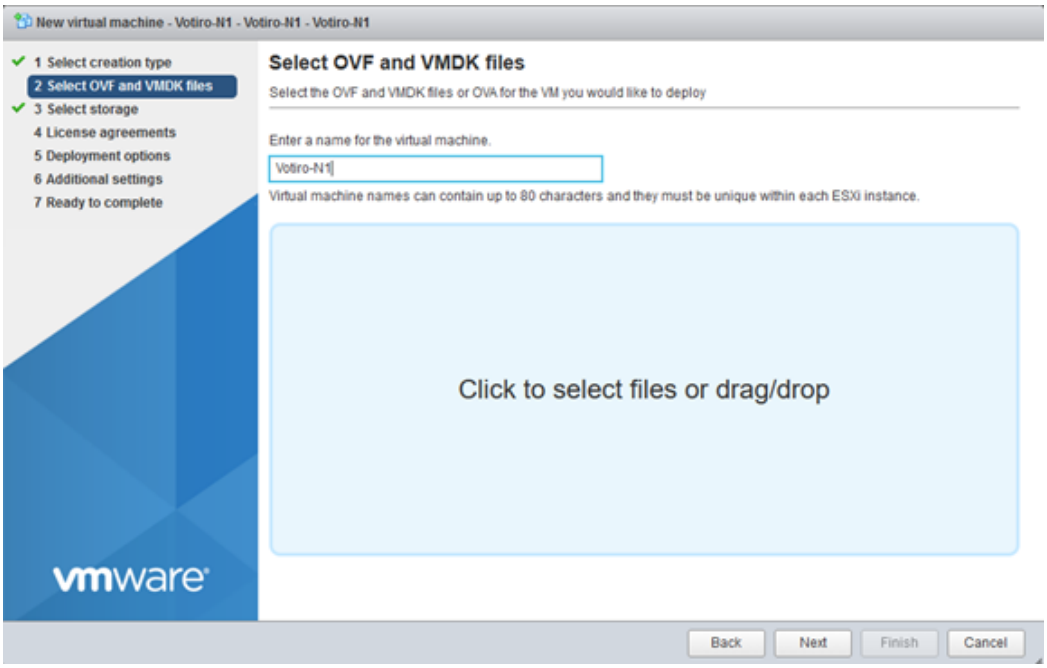
To enable secure communication with your Votiro appliance, the proxy server ACL must include permission for the Votiro registry in the Azure URL.

2.2 Deploying an OVF

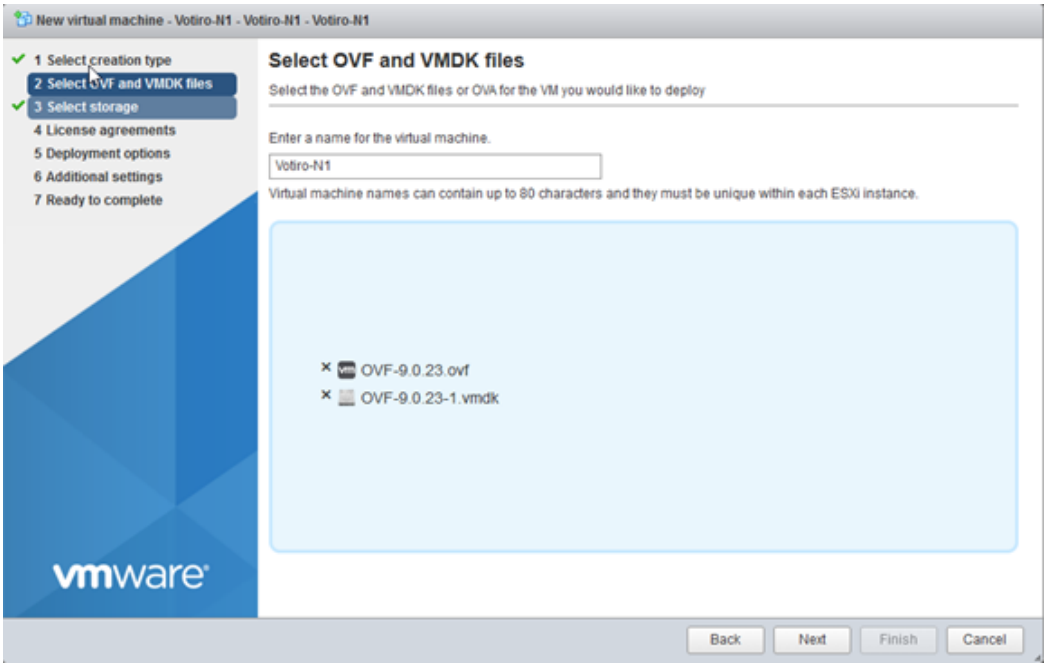
In this step you will create three virtual machines.

1. Deploy an **OVF**, three times, using these specifications:
   - 8 CPU
   - 16 GB Memory
   - 200 GB Storage

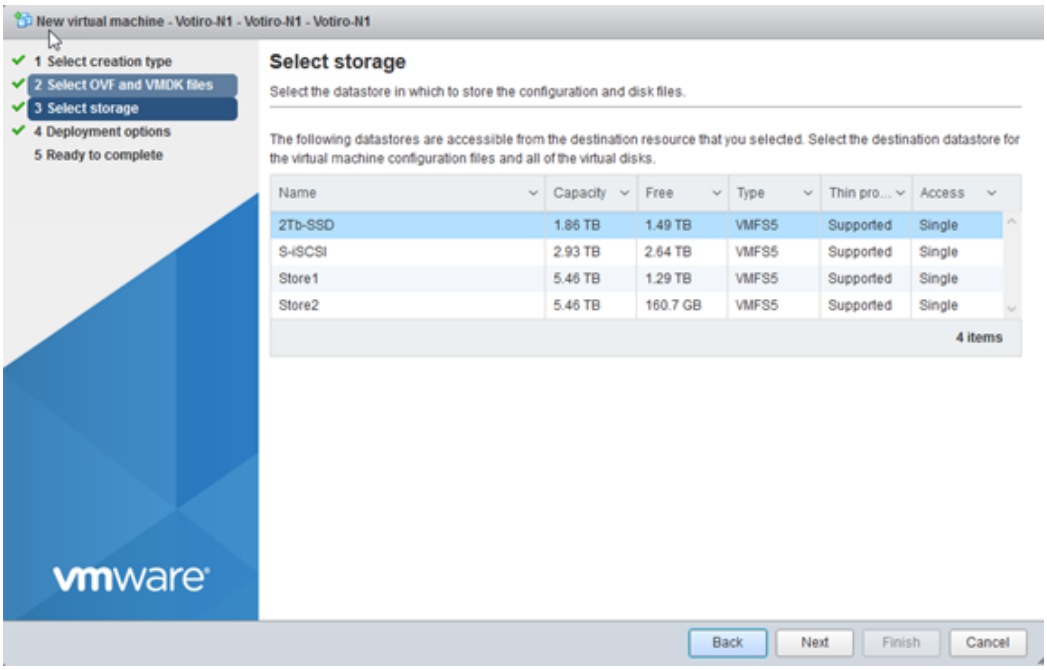
2. Name the **three nodes** using your corporate naming conventions.



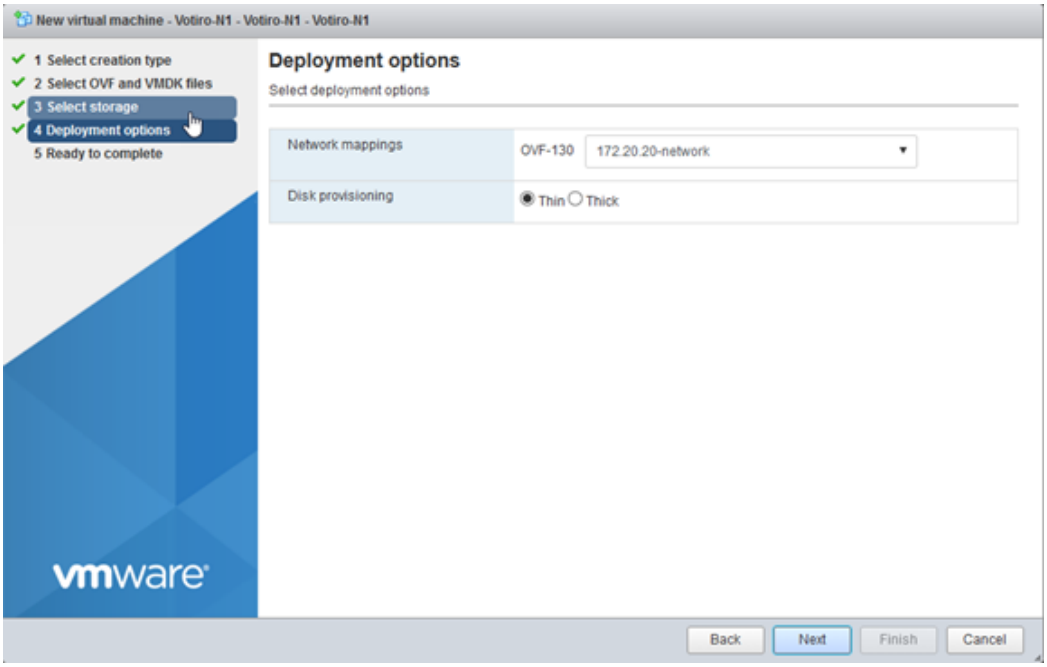
3. Select the **OVF** and **VMDK** files during deployment.



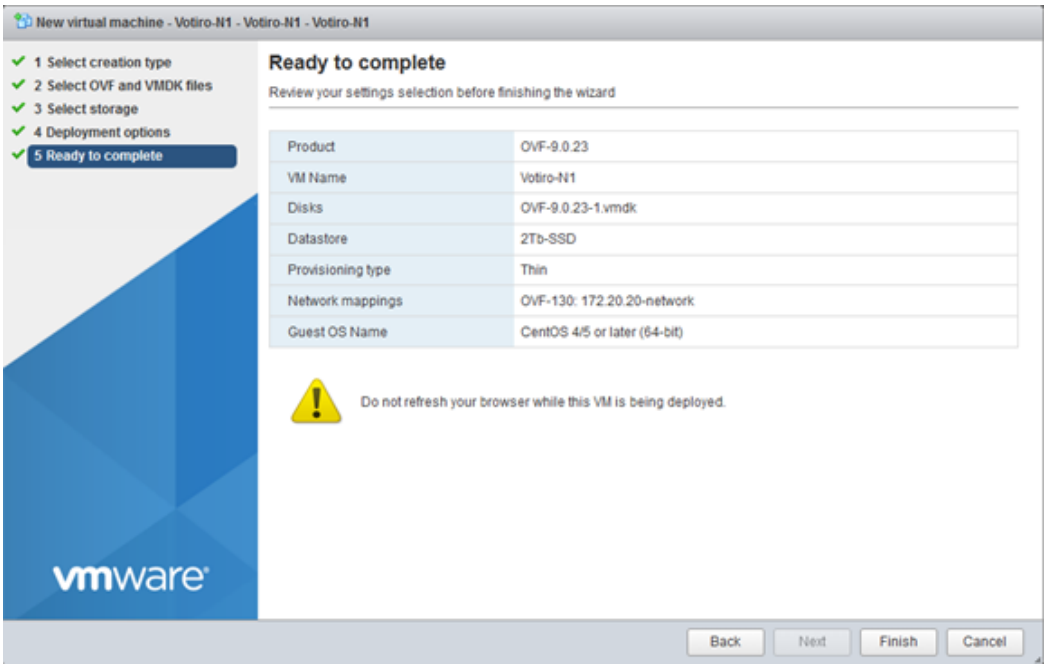
4. Select your preferred storage location. It is recommended you use **SSD storage**.



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.



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



There are now three virtual machines (VM).

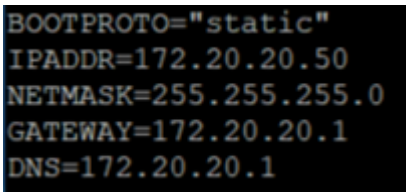
2.3 Configuring the Network Environment

In this step you will configure network settings for the three 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:

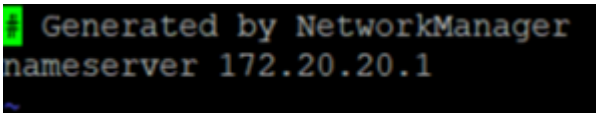
   d. To save the settings, click **Esc** and **:wq**, then click **Enter**.
   e. For the settings to take effect, use the following command:

      ```
      service network restart
      ```

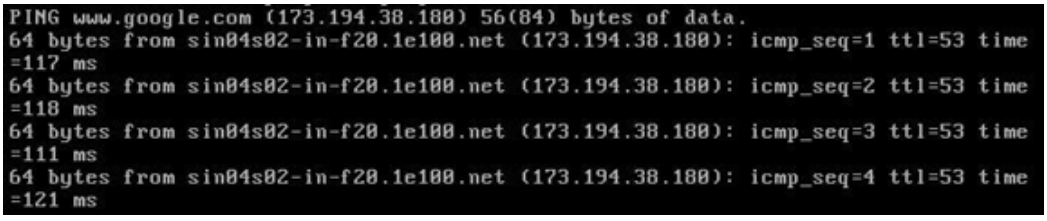
4. For your appliance to access the internet define a **nameserver** using lower case alphanumeric characters.
   a. To open the **resolv config** file with an editor, use the following command:

      ```
      vi /etc/resolv.conf
      ```

   b. Select **I** for insert mode.
   c. At the prompt, enter **nameserver <your_dns>**.

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



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

   `hostnamectl set-hostname <VotiroN1>`

   Repeat this step on all three nodes.

   There are now three machines configured and connected to your network.

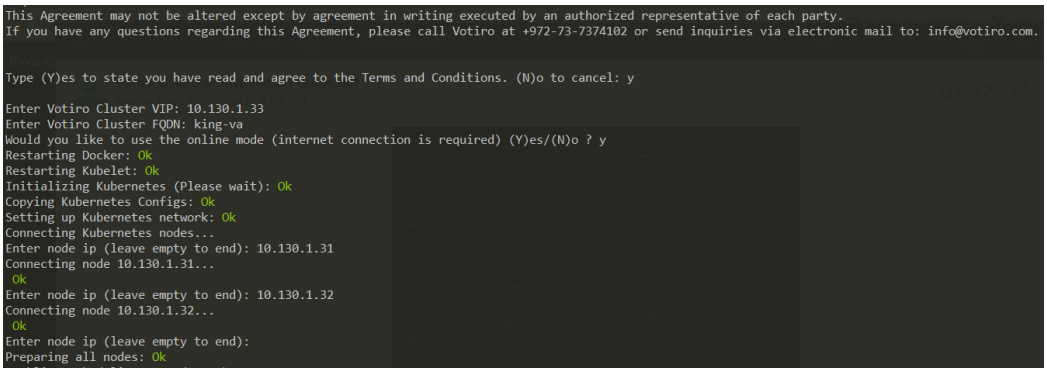
> **IMPORTANT!**
> We recommend you change the root password on all three nodes.

2.4 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**.



> **Note**
> A total of four IP addresses are required for the installation.

3. Enter the **VIP** for the Secure File Gateway cluster.
4. Enter the Secure File Gateway's **FQDN**, using lower case alphanumeric characters.
5. 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 two 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 15.

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

2.5 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 Management Dashboard is displayed.

2.5.1 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.

3 Using the Management Dashboard

The Management Dashboard enables you to perform the following procedures:

- Analyzing Positive Selection Activity
- Exploring Incidents
- Configuring System Settings
- Managing Positive Selection Policies
- Generating Reports

To log in to the Management Dashboard:

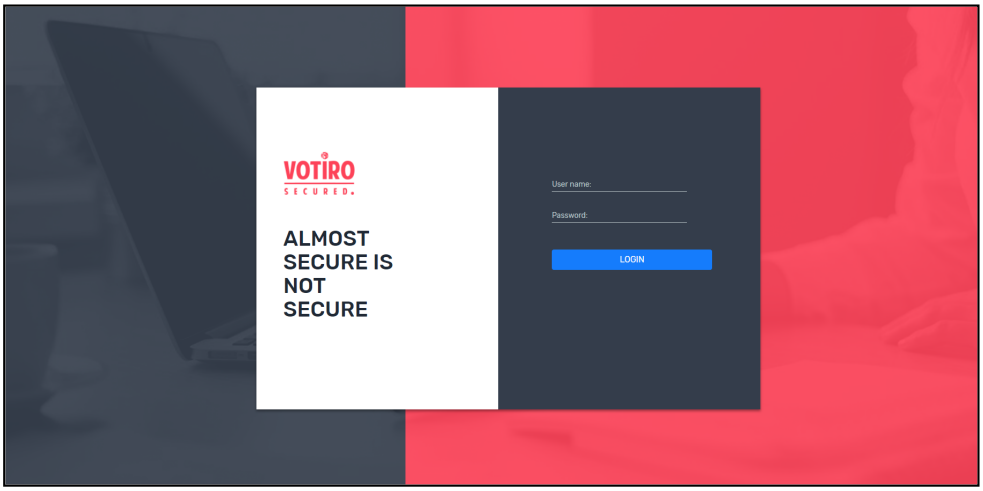
If you have configured the Management Platform to use Active Directory, only users that appear in the Active Directory group can log on.

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 and click **LOGIN**.

> **Note**
> The Management Dashboard locks down for 10 minutes after three failed login attempt of a single username.

The Management Dashboard is displayed.

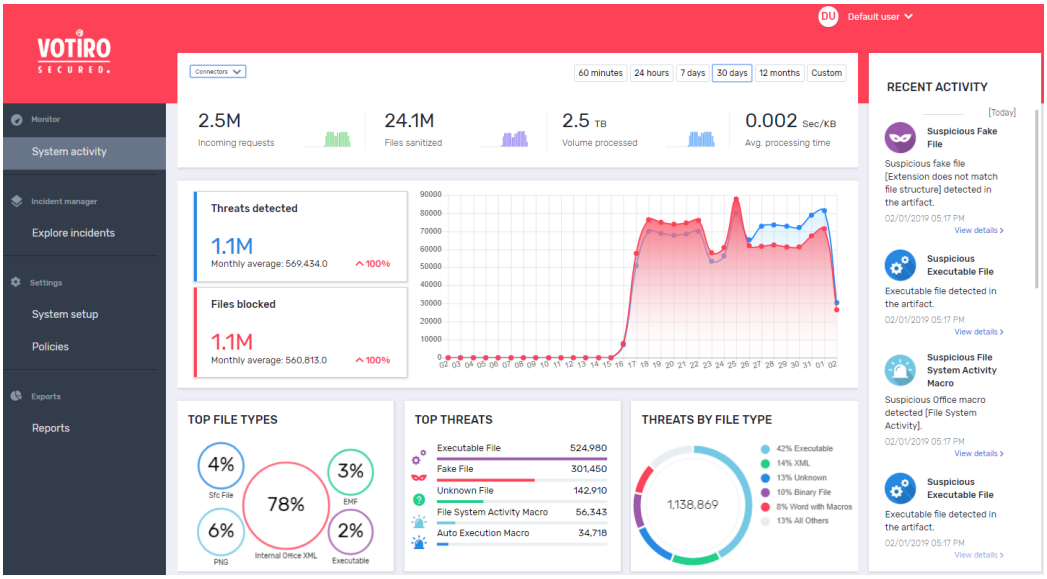
3.1 Analyzing Positive Selection Activity

The System Activity page enables monitoring and analyzing of positive selection activity, providing a summary view of threats that were found in files that passed through the system.

A file is processed for positive selection according to the policy. A threat is detected regardless of the policy, whether the file was 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 be both fake and contain a suspicious macro.

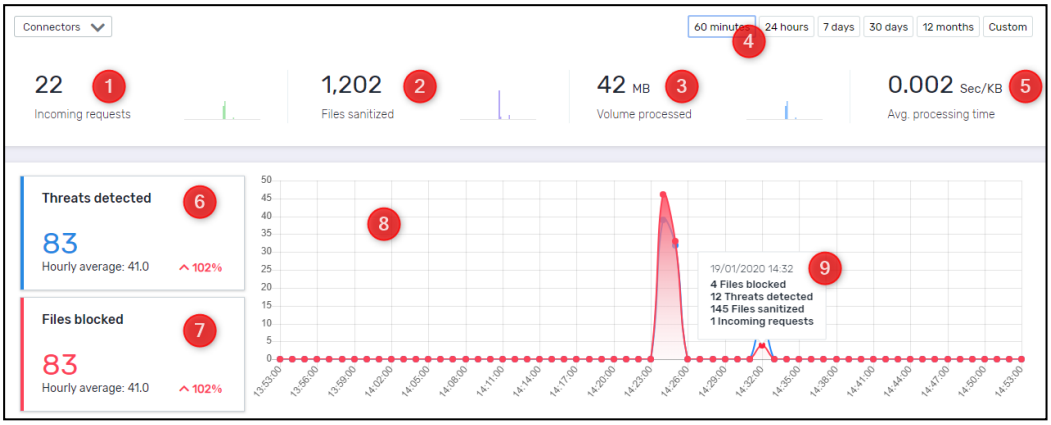
From the navigation pane on the left, click **System Activity**.



- **Central pane**: Displays statistics about the files that have gone through the system.
- **Right pane**: (Recent Activity) Displays a summary of the last ten files that were blocked.

3.1.1 Period Summary

The top area of the System Activity page is a summary of the selected period.



The following statistics are displayed:

Element	Meaning	Notes
1	Total number of requests incoming to the Positive Selection Engine.	A single, flat file, or a nested archive are both single requests.
2	Total number of files that were processed by the Positive Selection Engine.	The number includes root files and nodes.
3	Total volume that was processed by the Positive Selection Engine.	
4	The selected time period.	See Periods on the next page.
5	Average time, in kilobytes per second for processing each item in the volume displayed.	
6	Total number of threats detected, with the average.	The average is calculated according to the period currently selected: an hourly average in the case of a 60-minute period, a daily average in the case of a 24-hour period, and so on.
7	Total number of files blocked, with the average.	Clicking on **Threats Detected** and **Files Blocked** displays the threats and blocked files in the Explore Incidents view. For more information, see Exploring Incidents on page 31.
8	Graph showing threats detected and files blocked over the current time period.	
9	Summary for a specific time within the period.	

Periods

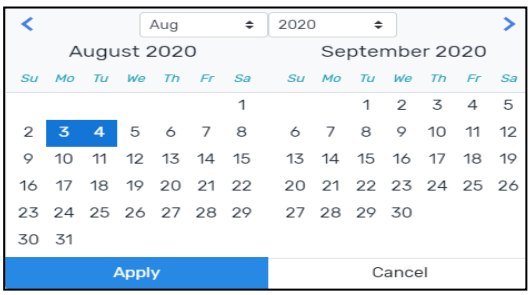
The statistics and graphs that are shown in the central pane of the System Activity page relate to the period that is currently selected. You can select a predefined period by clicking its button or define a custom period.

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

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.

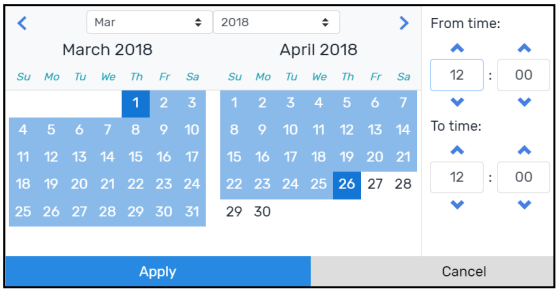
Defining a Custom Period

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



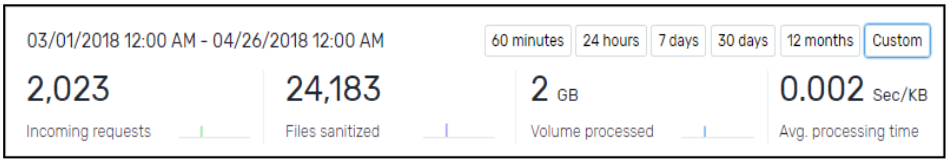
2. Navigate to the desired start month by clicking the right and left arrows or by selecting a month and year from the lists.
3. Select a start date.
4. Navigate to the desired end month.
5. Select a end date.
6. Select a time period.

The selected period is highlighted.



7. Click **Apply**

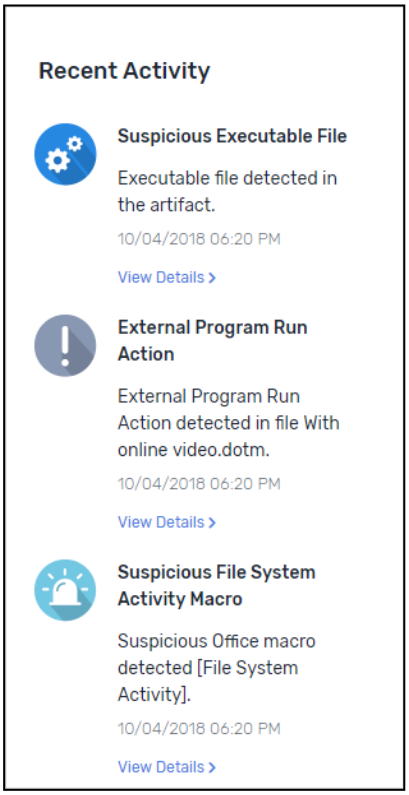
The custom period is displayed in the top left corner of the window:



Statistics and graphs update to show information for the custom period.

3.1.2 Viewing Recent Activity

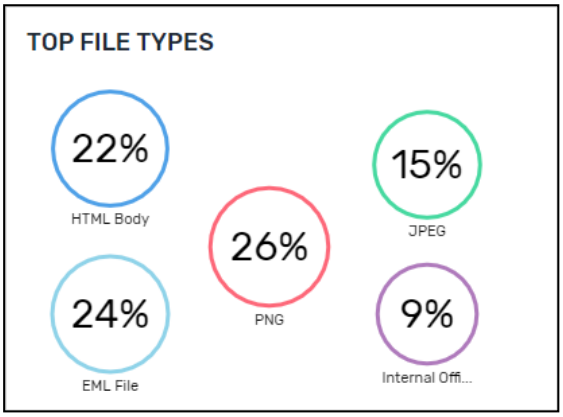
The Recent Activity pane displays the ten most recent file events.



Click **View Details** to view detailed information about the file, as described in Viewing Detailed File Information on the next page.

3.1.3 Viewing Top File Types

The Management Dashboard provides a graphic representation of the top five file types that have been processed during the selected period. The representation is according to percentages.

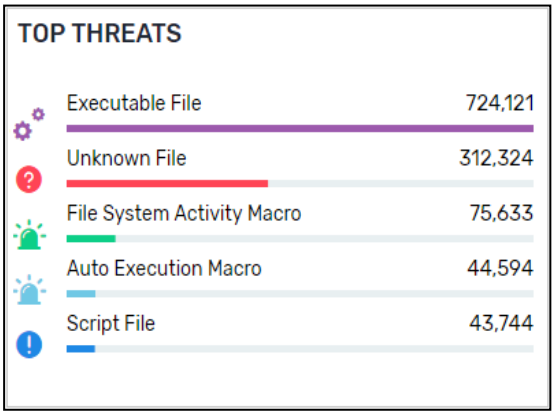


Click an area to display the related list of files in the Explore Incidents page.

For more information on exploring incidents, see Exploring Incidents on page 31.

3.1.4 Viewing Top Threats

The Management Dashboard provides a bar chart representing the top five file threats that were detected during the selected period. The representation is according to the number of threats that were found.

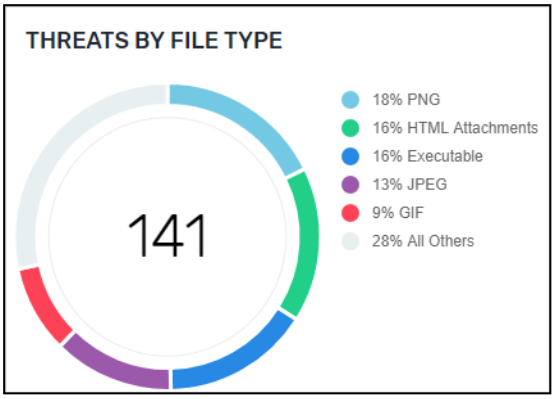


Click an item to display the related list of files in the Explore Incidents page.

For more information on exploring incidents, see Exploring Incidents on page 31.

3.1.5 Viewing Threats by File Type

The Management Dashboard provides a pie chart representing the top five threats by file type that were detected during the selected period. The representation is according to the relative percentages of file types.



Click an area to display the related list of files in the Explore Incidents page.

For more information on exploring incidents, see Exploring Incidents on page 31.

3.1.6 Filtering Lists of Files in Storage

You can view a full list of filtered files that match an area of the System Activity page:

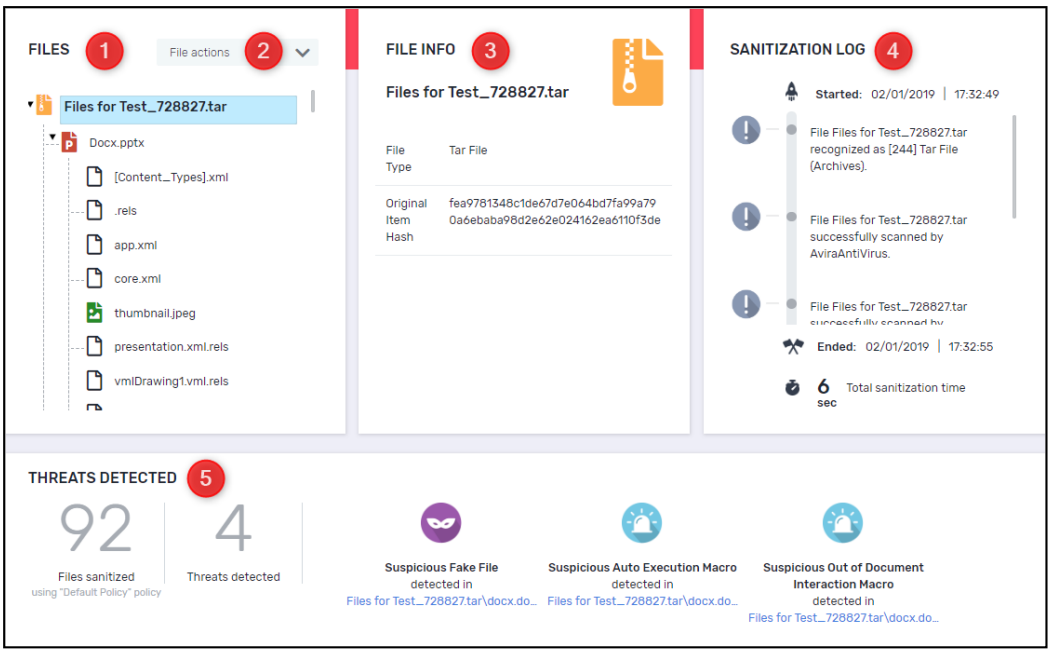
In the System Activity view, click	**To see detailed file information in the Explore Incidents page about**
Threats Detected	All threats that were detected.
Files Blocked	All files that were blocked.
A type in the **Top File Types**	All the files of the type selected.
A type in the **Top Threats**	All the files of the type selected.
A type in the **Threats by File Type**	All the files of the type selected.

In addition, clicking **View details** for a file in the **Recent Activity** panel displays details about the specific file in the Detailed File Information window, see Viewing Recent Activity on page 27.

For more information about the Explore Incidents page, see Exploring Incidents on page 31.

3.1.7 Viewing Detailed File Information

Detailed file information is displayed when you click **View Details** in the Recent Activity pane of the System Activity page, or **Details** for a file in the Explore Incidents page.



Element	Description
1	**Files**: Shows details of the file that you clicked in a previous window, in bold. The file is shown within the tree 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. Blocked files are shown in red.
2	The **File actions** list lets you perform the following actions for the file: ■ Explore Incidents. See Exploring Incidents on the next page. ■ Download the original file. See Performing Actions on Files on page 33. ■ Download the processed file. See Performing Actions on Files on page 33. ■ Release the original file if it was blocked. See Releasing the Original Version of a Blocked Email on page 33.
3	**File Info**: Provides details about the file that is currently selected in the left pane. For all file types, the following is provided: ■ File icon ■ File name, or (in the case of an email) the subject ■ File type ■ Hash Additionally, for email files (EML and TNEF formats), the following is displayed: ■ From ■ To ■ CC ■ Received date

Element	Description
4	**Sanitization Log**: Provides sanitization log events that relate to the file that is currently selected in the left pane: ■ The date and time that positive selection processing began. ■ The date and time that positive selection processing ended. ■ A list of events during the positive selection processing of the selected file. ■ The total time taken to positive selection processing the selected file.
5	**Threats Detected**: Provides summary information about the entire tree – root and nodes – that is currently displayed in the left pane: ■ The total number of files that were processed. ■ The total number of threats detected. ■ A graphic, clickable representation of each threat is presented alongside.

3.2 Exploring Incidents

The Explore Incidents page provides a deeper look at files that were processed for positive selection or blocked by the Positive Selection Engine, and that are currently stored on the server.

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

Accessing Explore Incidents

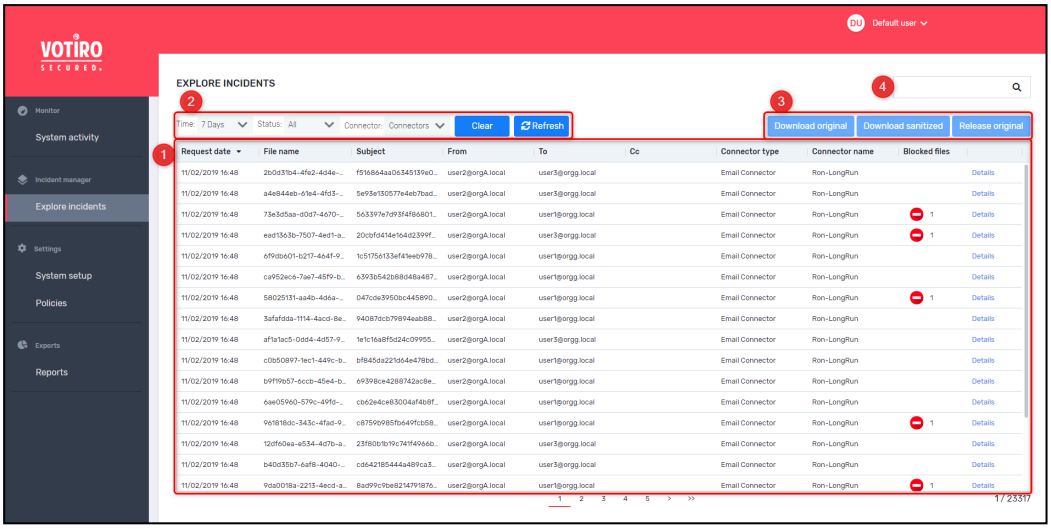
From the navigation pane on the left, click **Explore Incidents**.The *full* list of incidents that occurred in the last seven days is displayed.

Or

In the System activity view, click any of the following to see *the related details* in the Explore Incidents page:

- Threats detected
- Files blocked
- Top file types
- Top threats
- Threats by file types

For example, if you click **Files blocked** in the System activity page, the Explore Incidents page displays a filtered list of the files that were blocked.



Use this page to explore incidents (blocked and processed files) that occurred in the system. The page provides the following features:

Element	Description
1	Displays the file name, together with the date and time of the positive selection request. Double-click any file or click **Details** to see the file details in the Detailed View window.
2	Filters the list of files according to period and status. See Using Filters on the next page.
3	Perform actions on files. See Performing Actions on Files on the next page.
4	Perform a search on all the incidents in the blog. See Searching Positive Selection Requests on page 35.

3.2.1 Understanding File Details

The positive selection requests (root files) that are currently stored on the Management server are listed in the main pane of the Explore Incidents page.

The following details are displayed for all requests:

- Request date
- File name: Root request file name.
- Connector type
- Connector name
- Blocked files: Number of files in the file tree that were blocked.

For emails, additional details are shown:

- Subject
- From
- To

- CC

> **Note**
> The displayed requests might be filtered according to the manner in which you accessed the page. See Accessing Explore Incidents on page 31.

To view file details, double-click any file or click **Details** in the positive selection request line. For more information, see Viewing Detailed File Information on page 29.

3.2.2 Using Filters

You can filter the file list in the following ways:

- Select from the **Status** list to view all files, blocked files, or processed files.
- Select an option from the **Time** list to filter according to a specific time period. Select **Custom** to define a range of dates. For instructions on how to define a custom period, see Defining a Custom Period on page 26.
- If you have more than one Secure File Gateway Connector installed, you can filter the file list by connector type using the **Connector** list.

3.2.3 Performing Actions on Files

From the Explore Incidents page you can perform the following actions on the files in the blob:

- Download the file as it was before it was processed for positive selection, by clicking **Download Original**.
- Download the processed version of the file by clicking **Download sanitized**.
- Release an original file that was blocked.

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.

Usually, this procedure is performed by IT and only under unusual circumstances.

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 password

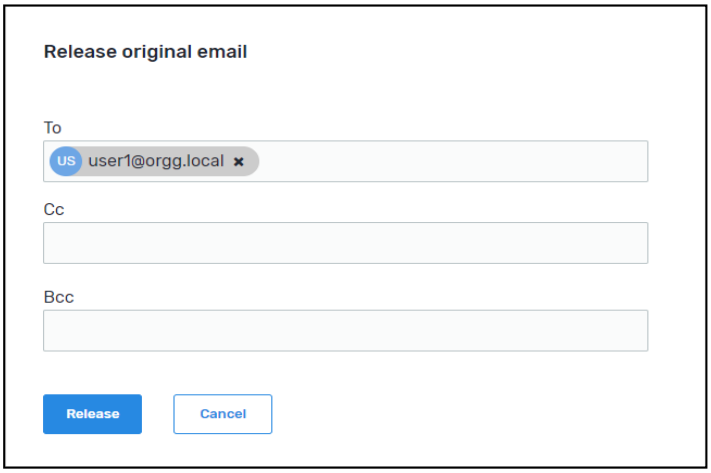
For more information, see Configuring System Settings on page 36.

- 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:

1. Click an email file in the list of blocked files, then click **Release Original**.

   The following dialog is displayed:



   The dialog shows the same email addresses as 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 needed. You cannot add email addresses.

3. Click **Release** to send the email.

Releasing the Original Version of a Blocked File

If an 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.

Usually, this procedure is performed by IT and only under unusual circumstances.

> **Note**
> To enable the release of blocked files, you must first configure the Management Platform in Secure File Gateway for Web Downloads.
> For more information, see Secure File Gateway for Web Downloads.

To release a blocked file, click a file in the list of blocked files, then click **Release Original**.

The original file is sent to the OUT folder.

3.2.4 Searching Positive Selection Requests

You can search all the positive selection requests that are shown in the Explore Incidents page using the search bar. You can search by the following details:

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

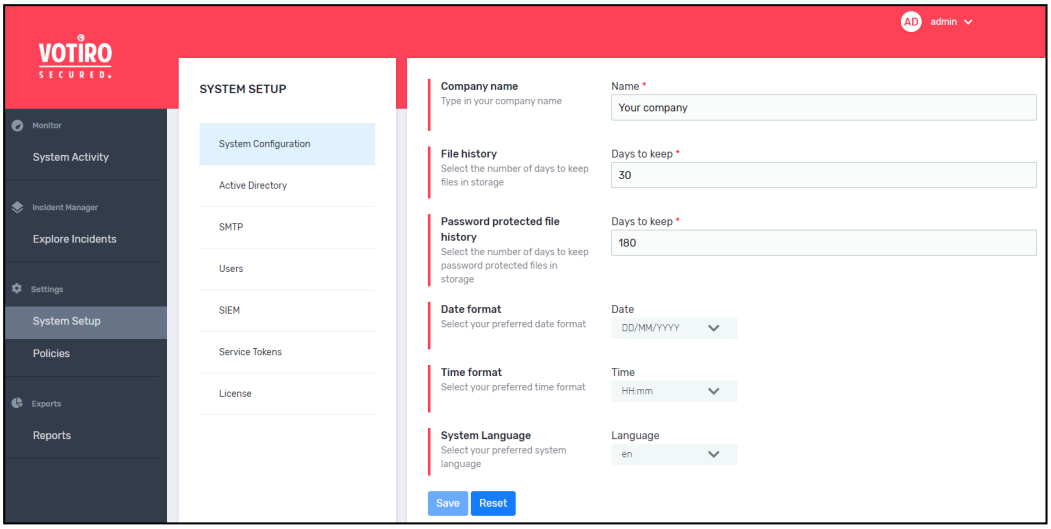
  This feature is useful for releasing a specific blocked files (see Releasing the Original Version of a Blocked Email on page 33). For example: An email that contains a file you are expecting has been blocked by Secure File Gateway. As the recipient, you receive an email notification. The PDF file that is attached to the email message contains an item ID, such as the following:

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

  To release the blocked file, copy and paste the item ID into the search bar and press Enter to display the file in the Explore Incident page. Select the file and click **Release original**.
- Positive Selection request file name

3.3 Configuring System Settings

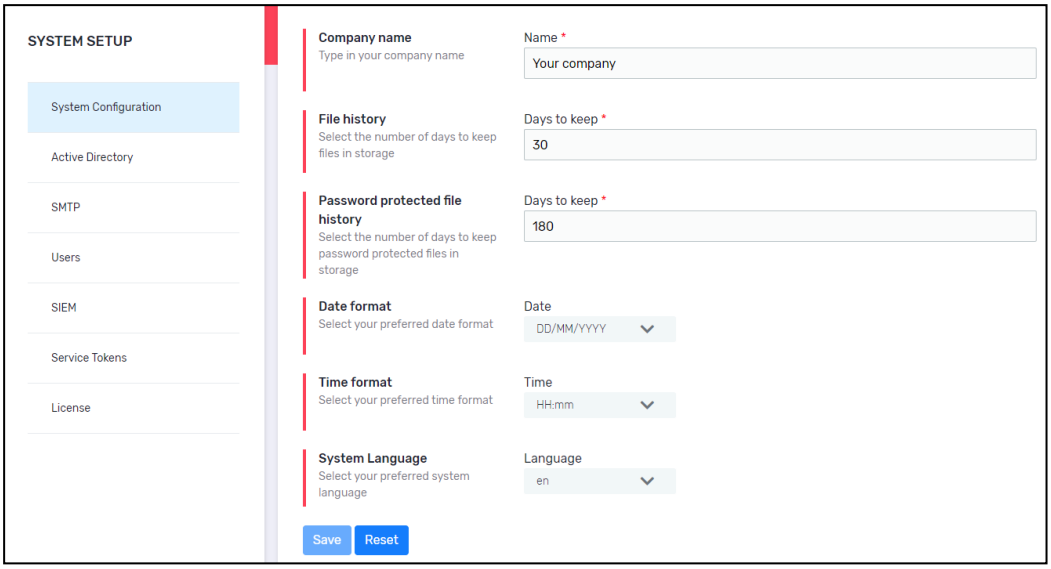
Use the System Setup page to configure settings in Votiro's Management Dashboard.



There are several active tabs in this view:

- System Configuration Tab
- Active Directory Tab
- SMTP Tab
- Users Tab
- SIEM Tab
- Service Tokens Tab
- License Tab

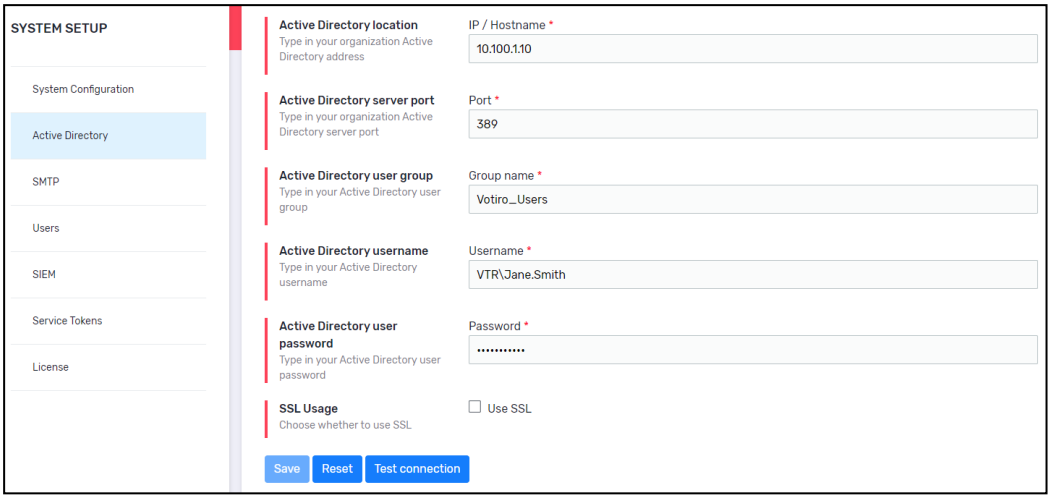
3.3.1 System Configuration Tab



The System Configuration tab contains the following fields:

Field	Description
Company name	Specifies the name of your organization. The company name appears in activity reports. For more information, see Generating a Summary Report on page 57.
File history	Specifies for how many days the system saves files. The default is 30.
Password protected file history	Specifies for how many days the system saves password-protected files. The default is 180. **Note** After the configured period, the original file is deleted and cannot be retrieved through the dashboard.
Date format	Select your preferred date format for the display of information in the dashboard --either MM/DD/YYYY or DD/MM/YYYY.
Time format	Select your preferred time format for the display of information in the dashboard -- either a 12-hour clock or 24-hour clock format.
System Language	Select your preferred language. To add languages to the list you must translate Dashboard dictionary and upload the translation.

3.3.2 Active Directory Tab



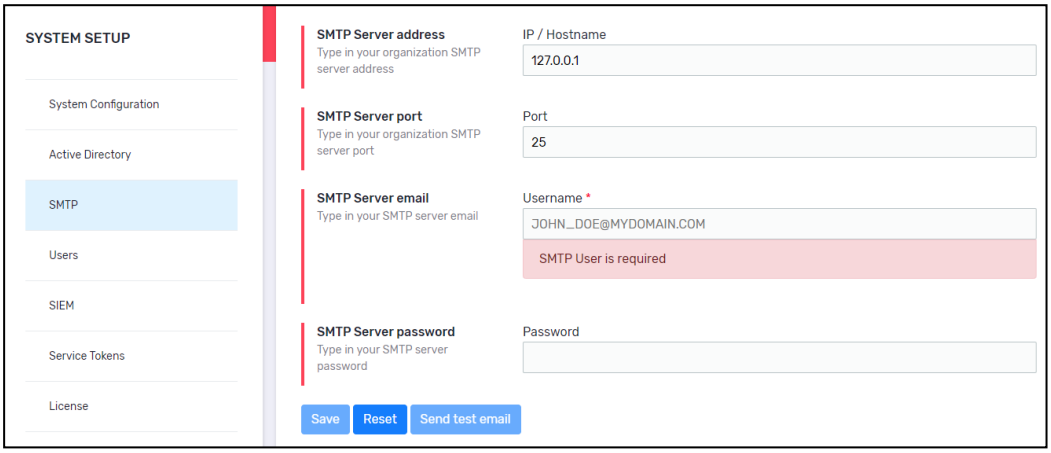
The Active directory tab contains the following fields:

Field	Description
Active Directory location	Specifies the Active Directory server that validates login.
Active Directory server port	Specifies the Active Directory server port.
Active Directory user group	Specifies the name of the Active Directory group. Only users that belong to the predefined Votiro_Users group in Active Directory can log onto Votiro Management Dashborad.
Active Directory username	Specifies the login username for the Active Directory server. Select one of two formats to use: ■ DOMAIN\UserName - For example, VT\Jane.Smith ■ UserName@FQDN - For example, Jane.Smith@Votiro.com Key: *DOMAIN* - the NetBIOS domain name *UserName* - the login name of the user *FQDN* - the domain name in full
Active Directory user password	Specifies the login password for the Active Directory server.
SSL Usage	Specify whether to use SSL.

Note

Before saving changes test the connection to Active Directory. Click Test connection.

3.3.3 SMTP Tab



All SMTP settings are required to enable Management Platform features that rely on email. Configure SMTP settings to:

- Release original files from the blob. For more information, see Releasing the Original Version of a Blocked Email on page 33.

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

Field	Description
SMTP Server address	Specifies the SMTP server that relays notifications from the Platform Management to users in your organization.
SMTP Server port	Specifies the SMTP server port.
SMTP Server email	Specifies the email address of the SMTP server user.
SMTP Server password	Specifies the password for the SMTP server user.

To test the SMTP settings, click Send test email at the bottom of the screen.

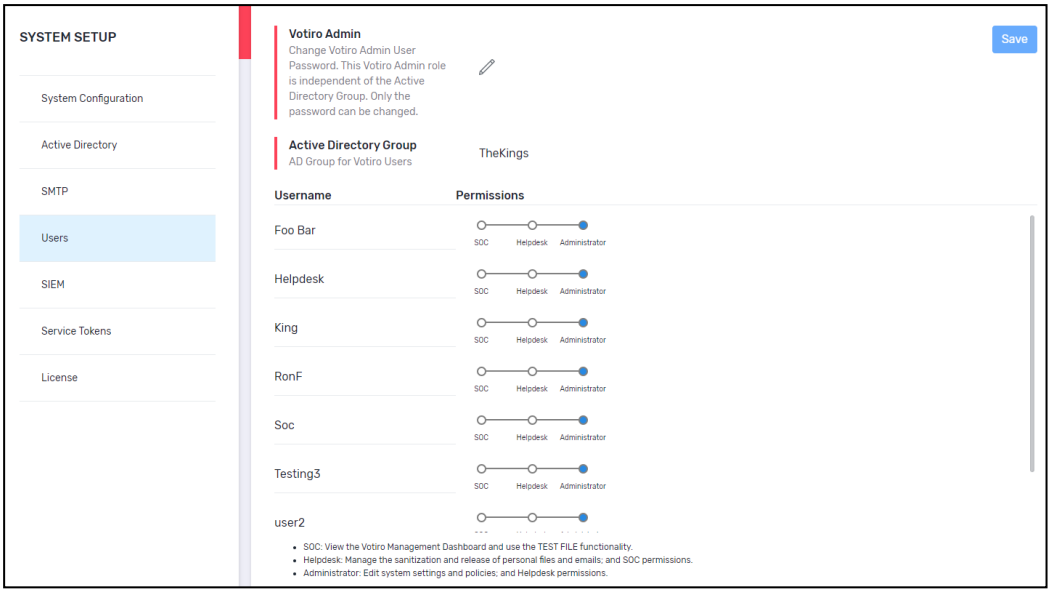
- If the settings are valid, a verification code is displayed in the Management Dashboard.

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

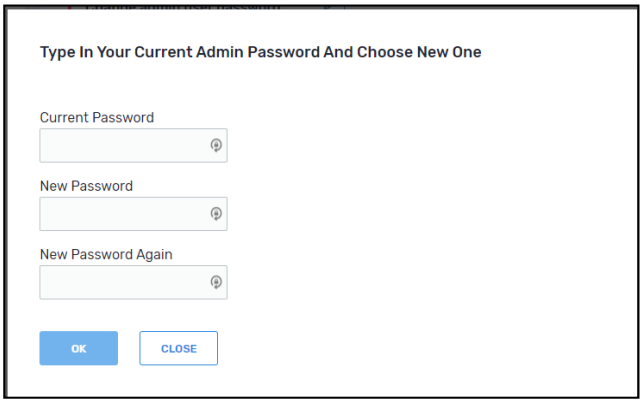
- If the settings are invalid, an error is displayed below the button.

3.3.4 Users Tab

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



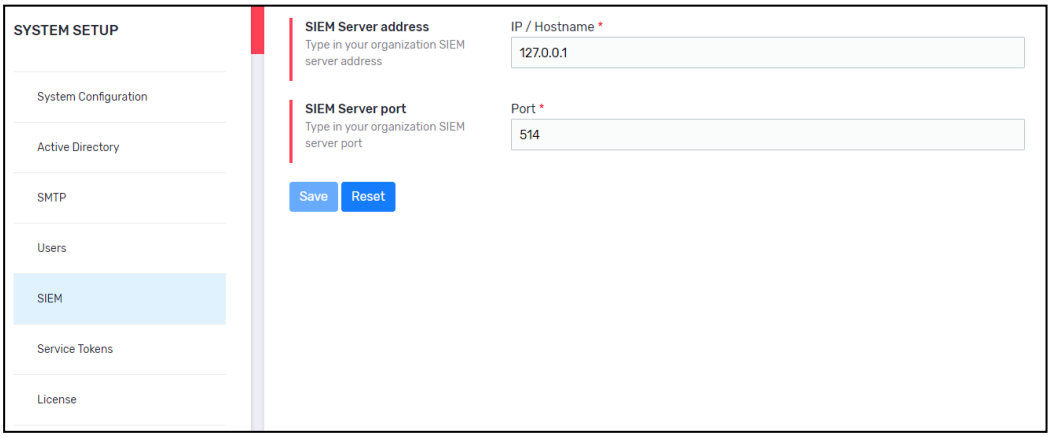
The Users tab contains the following fields:

Field	Description
Votiro Admin	The Votiro Admin role provides direct administrative access to Secure File Gateway, independent of Active Directory. To change the Votiro Admin password: 1 Click . 2 Enter the **Current Password** and the **New Password** twice. 3 Click **OK** to save. 

Field	Description
Active Directory Group	Users must be in the Votiro_Users Active Directory group. The three levels of permission are: ■ SOC: users will only be able to view the dashboard and use the TEST FILE functionality. They will not have access to personal data, or be able to change settings. ■ Helpdesk: users will be able to manage the positive selection process and release of personal files and emails, in addition to SOC permissions. ■ Administrator: users will have access to the entire system, including personal files and emails. They have permission to edit policy configurations and system settings, in addition to Helpdesk permissions. To set a user's permissions on the bar to the right of the **Username**, click the circle above the permission level to be granted. The circle changes to blue.  **Note** The system must have a minimum of one **Administrator** user setup in the Active Directory Group for Votiro users. A warning message appears if you attempt to **Save** the settings with no user set with **Administrator** permissions.

3.3.5 SIEM Tab

Use the SIEM tab to configure settings for the saving Management event logs in a SIEM.

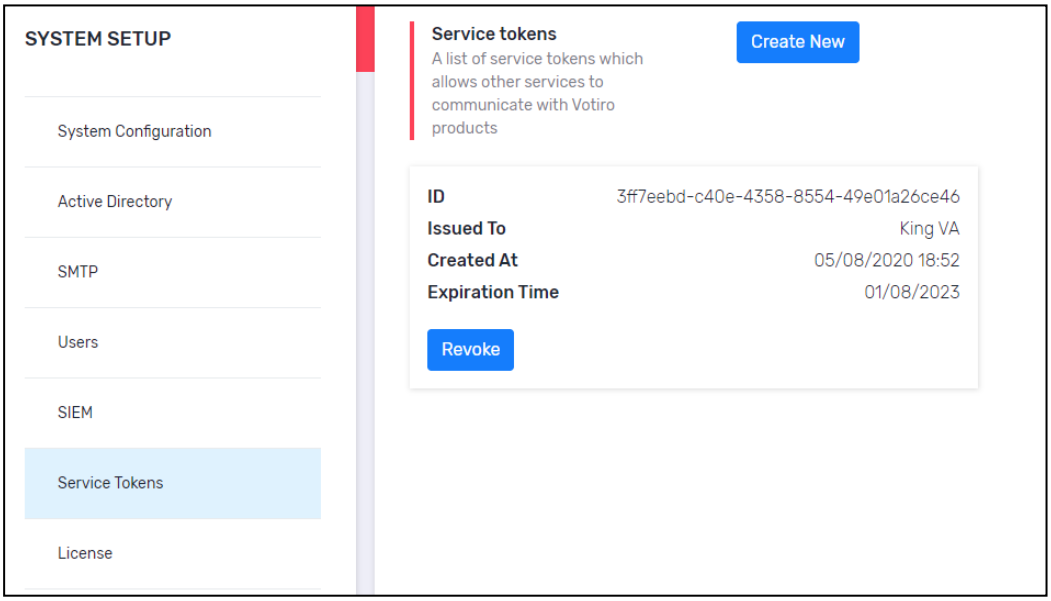


The tab contains the following configuration fields:

Field	Description
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.
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 Format on page 63.

3.3.6 Service Tokens Tab

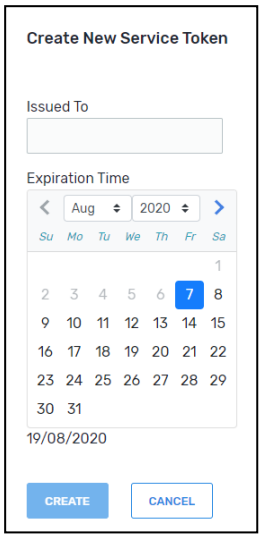
Use the Service Tokens tab to view existing service tokens and to create a new service token. Service tokens allow other services to communicate with Votiro's Secure File Gateway.



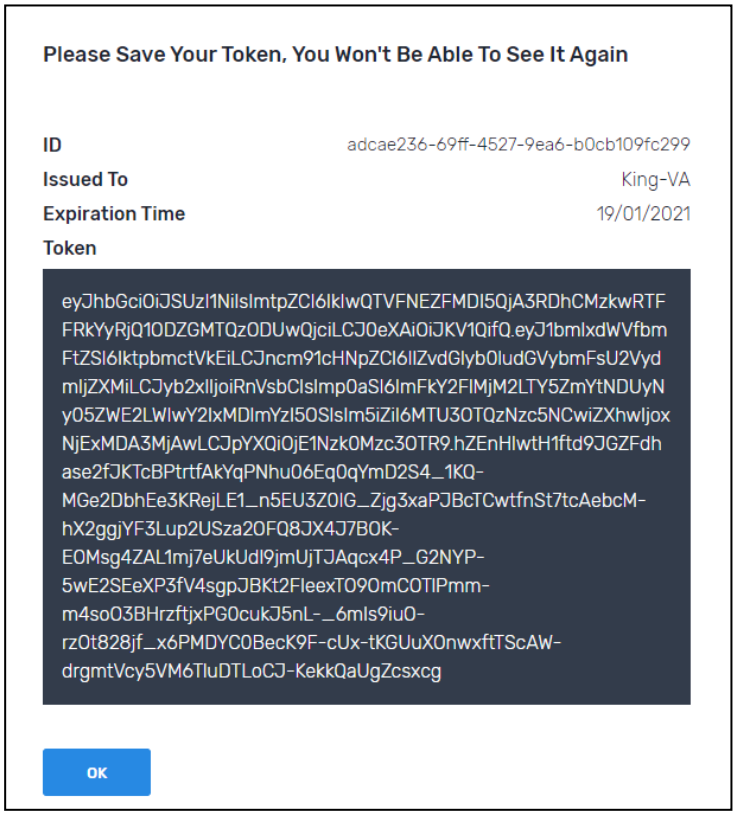
To create a new service token:

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.
Expiration Time	Specifies the date the service token will expire.



3. Click **Create**.

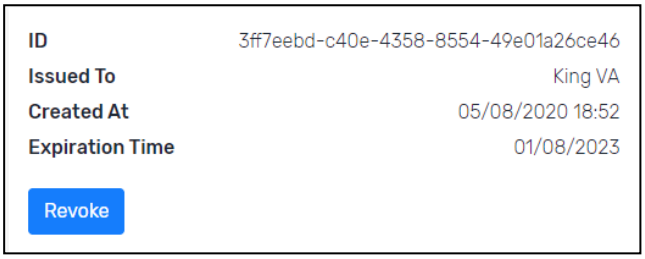


4. A service token is generated. You must copy this service token to the relevant bearer authentication headers.

> **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 tab.

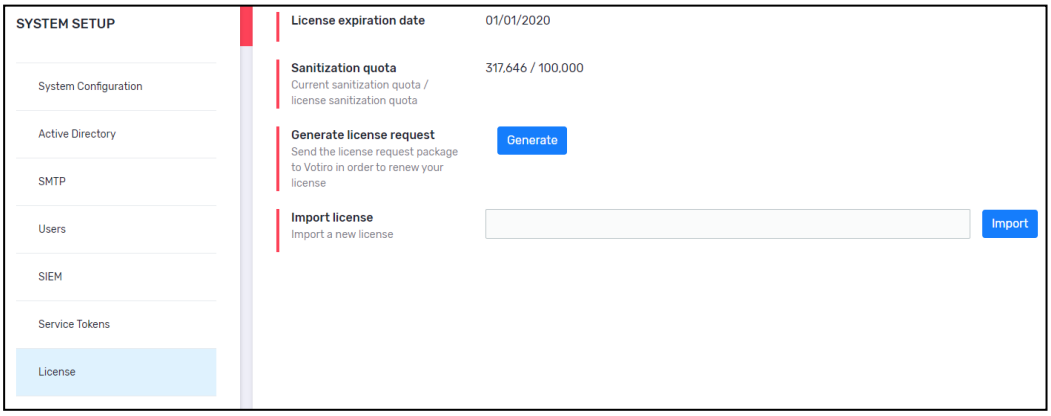


Field	Description
ID	The ID of the service token is automatically added.
Issued To	Specifies the name you have given to the service token.
Created At	A DateTime stamp is automatically added to the service token.
Expiration Time	Specifies the date the service token will expire.

To withdraw a service token, click **Revoke**.

3.3.7 License Tab

Use the License tab 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.



The tab contains the following configuration fields:

Field	Description
License expiration date	When a valid license key is imported the expiration date automatically updates to the date when processing of files will stop. At time of installation the default license is valid for 24 hours. During this time files will be processed and a license should be requested.
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.
Generate license request	Click **Generate** to produce a license request package. The file **licensePackage.zip** is generated and located in your downloads folder. Pass this file to Votiro Support. A license key will be generated and returned to you within 24 hours of receipt of the request.
Import license	Enter the license key provided by Votiro Support and click **Import**. Successful validation automatically updates **License expiration date** and **Sanitization quota** information. The license key disappears. **Note** Votiro's Secure File Gateway is activated up to five minutes after the license key import.

3.4 Managing Positive Selection Policies

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

For example, your organization’s positive selection policy might comprise the following rules:

- Process all image files and rasterize vector images.
- Block all fake files and customize the block message that the end user receives to be “Due to a recent spike in threats associated with fake files, the company has decided to block them.”
- Process all PDF files, except if they are larger than 25 MB. In such an event, the file is blocked.

Votiro's Secure File Gateway uses policy definitions that are defined in the Management Dashboard.

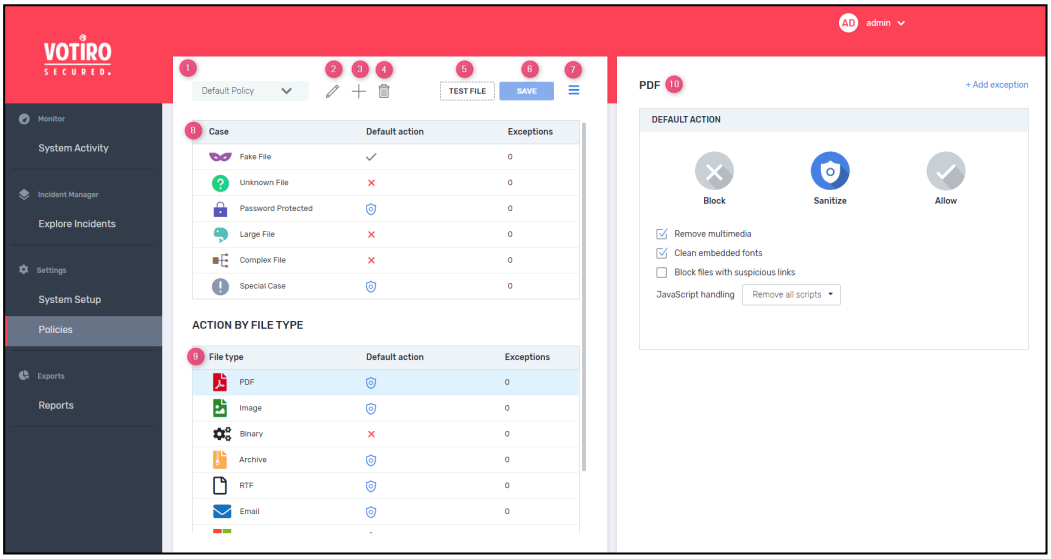
If you do not create a customized policy, Secure File Gateway uses a set default policy.

If you have custom, XML-based policy definitions, you can load these to the Management Dashboard as special cases. To learn how to include special cases, see Defining Policy Based on Special Cases on page 54.

Positive Selection Policies Dashboard

The Policies view in Votiro's Management Dashboard lets you create, edit, and manage the positive selection policies that operate in the Positive Selection Engine.

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



Element	Meaning
1	The name of the currently displayed policy. To display a policy, select from the list of defined policies.
2	Edit the policy name.
3	Add a new policy.
4	Delete current policy.
5	Select file to test policy.
6	Save current policy.
7	Import/Export policy file.
8	Displays the details of the selected policy by case.
9	Displays the details of the selected policy by file type.
10	Displays details of the item that is selected on the left. For each case or action, you can define how it must be handled.

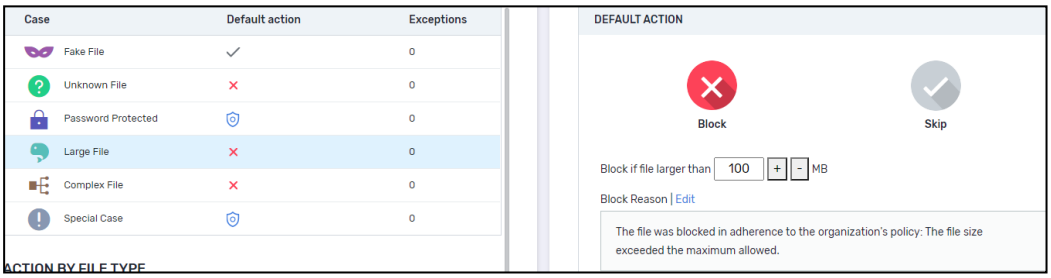
> **Note**
> Change made in policies are updated in the Positive Selection Engine every few seconds. Once updated in the Positive Selection Engine, it is available to Secure File Gateway reference clients, such as Secure File Gateway for Email or Secure File Gateway for Web Downloads.

3.4.1 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. The block file is attached to an email and can be customized for each company and for each set of criteria.

3.4.2 Defining Policy by Case



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

- Block the file
- Skip the file
- Add one or more exceptions to the policy. For more information, see Defining Exceptions on page 54.

If you choose to block the case, you can:

- Set additional options if they are provided (as in the image above)
- Edit the default block reason text

After you save the settings for the case, the display updates to show the action symbol in the Default Action column and the number of exceptions in the Exceptions column.

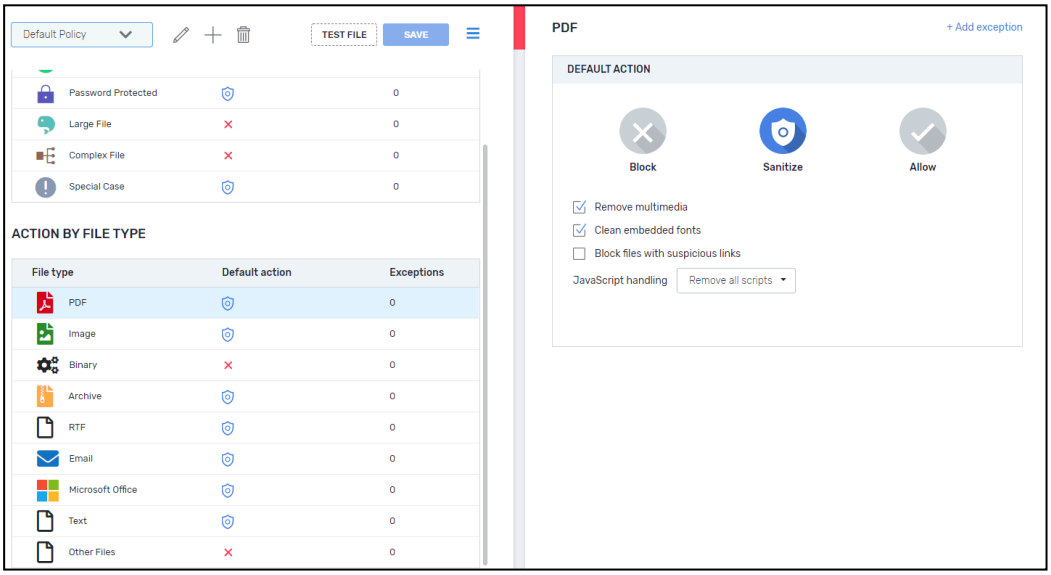
The following table describes the positive selection processing options that are available for each case:

Table 4 Positive Selection Processing Options for Cases

Case	Description	Processing Options
Fake File	Specifies how to handle any file whose extension does not match the file type.	By default, the check for fake files is skipped, but the files themselves undergo full positive selection processing -- fake files thus pose no threat at all.
Unknown File	Specifies how to handle data files or unidentified file types.	You can block or skip these. If you select Skip, the unknown file is not processed for positive selection and the original version will reach the destination folder.
Password Protected	Specifies how to handle password-protected files.	You can block or process these files. By default, the files are processed for positive selection. 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 web page where the password can be entered. When the correct password is entered, the blocked file returns to the storage server, and is processed. The processed file is then downloaded to the user's computer, or sent by email as an attachment. The password protection case in the Management Dashboard provides: ■ A user message that appears in the notification. Accept the default text or edit it. ■ A checkbox that enables you to block unsupported files (such as Visio files). **Note** This feature supports the following file types only: PDF, ZIP, 7zip, RAR, DOC, DOCX, DOT, DOTX, DOCM, DOTM, XLS, XLT, XLSX, XLTX, XLSM, PPT, PPS, POT, PPTX, PPSX, POTX and PPTM. It does not work on other file types that can be protected by a password, such as Visio files.

Case	Description	Processing Options
Large File	Specifies how to handle large files.	You can set the minimum size of files you want to block. 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.
Complex File	Specifies how to handle nested files.	You can set a layer number. Files that are found in that layer or deeper are blocked.

3.4.3 Defining Policy by File Type



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

- Block the file under all conditions. You can edit the default notification about the blocked file.
- Process the file for positive selection using default settings. You can modify the default behavior by setting options when they are provided (for example, as in the image above). You can also edit the default block reason text.
- Allow the file under all conditions.
- Add one or more exceptions to any of the previous three settings. For more information, see Defining Exceptions on page 54.

After you save the settings for the file type, the display updates to show the action symbol in the Default Action column and the number of exceptions in the Exceptions column.

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

Table 5 Positive Selection Processing Options for File Types

File Type	Description	Processing Options
PDF	Specifies how to process PDF files.	By default, these files are processed for positive selection. ■ **Remove multimedia**: Specifies whether multimedia such as embedded video, audio, 3D annotations, and rich media annotations must be removed. Default is checked. ■ **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 is found to be suspicious, the document is blocked. 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. Default is unchecked. ■ **JavaScript handling**: Determines how JavaScript, if found in the PDF file, is handled. ♦ Don't do anything ♦ Remove only suspicious scripts ♦ Remove all scripts (this is the default) ♦ Block documents containing suspicious scripts

File Type	Description	Processing Options
Image	Specifies how to handle image files.	By default, these files are processed for positive selection. ■ **Add micro-changes**: Adds security noise to images during processing. Default is checked. **Note** Increasing the noise level might enlarge the processed files, particularly in the case of png files. Unselecting noise level (off) usually preserves an image file size. ■ **Remove metadata**: Removes EXIF metadata from JPEG 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 five compression levels (from 0% to 100%) that trade off file size with image quality – the larger the file, the higher the image quality. Default is 25%.
Binary	Specifies how to handle binary files.	The processing option is not relevant to managing binary files. You either block binary files or allow them.
Archive	Specifies how to handle archives.	By default, these files are processed for positive selection. **Block zip bomb**: Detects and blocks zip files with abnormal compression ratio. These might pose a denial of service threat, consuming system resources such as CPU or disk. Any zip files with compression ratio higher than 99.8% will be considered a zip bomb and be blocked. Default is checked.
RTF	Specifies how to handle RTF files.	By default, these files are processed. There are no specific processing options.

File Type	Description	Processing Options
Email	Specifies how to handle email files. Positive selection processing is on EML files and their attachments. **Note** Each attached file is processed recursively by running all policy rules on it.	By default, these files are processed for positive selection. - **Block files with suspicious links**: Performs a check of all links in the form HTTP:// and HTTPS:// in the body and attachments of an email. If any link is found to be suspicious, the email body or attachment is blocked. Default is unchecked.

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

File Type	Description	Processing Options
Text	Specifies how to handle text files.	By default, these files are processed for positive selection. **Block CSV with threat formula**: Blocks CSV files that contain formula injections. Default is checked.
Other files	Specifies how to handle unsupported files.	By default, these files are blocked. There are no specific processing options.

3.4.4 Defining Policy Based on Special Cases

You can load a set of special cases – a **custom policy** – that has been created outside the Management Dashboard. This feature is recommended for special needs only . For more information, contact Votiro Support.

3.4.5 Defining Exceptions

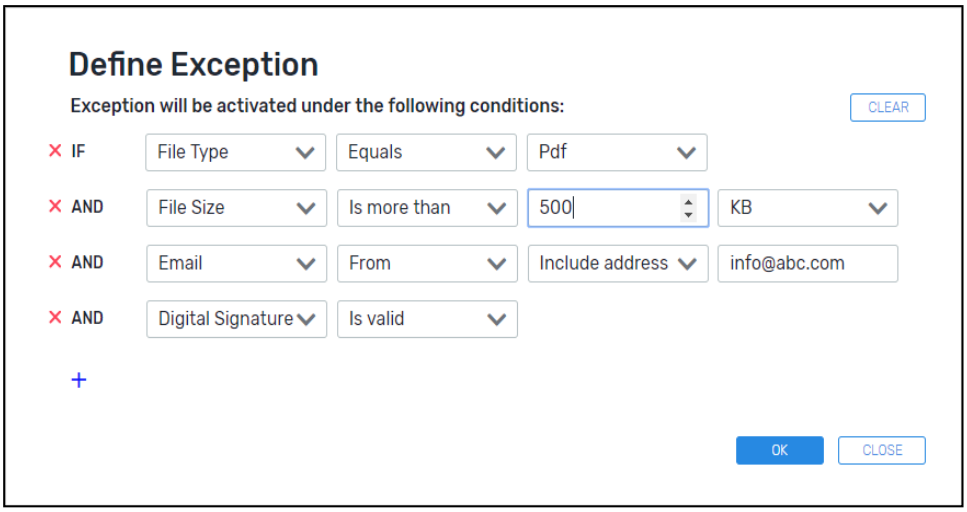
You can define one or more exceptions to any case policy or file type policy. Exceptions can be based on the following:

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

To define an exception:

1. From the navigation pane on the left, click **Policies**.
2. Click the case or file type for which you wish to define an exception.
3. In the top right corner, click **Add Exception**.

The Define Exception window appears:



4. Create a condition by selecting values from the lists or by adding free text, as needed.
5. Click the plus sign to add a condition to the exception definition. Click the x sign to delete a condition.
6. Click **OK**.

   The exception is added to the right pane. You can further edit it or delete it, as needed.

Defining Exceptions for File Types

To specify an exception for one or more file types:

1. In the leftmost list, select **File Type**.
2. In the second list, select **Equals** or **Not Equals**.
3. In the last list, select one or more relevant file types. The list displays the most common ones. To select a type that does not appear, select **Other types**, then, in the additional list that appears, select the types that meet your needs.

Defining Exceptions for File Size

To specify an exception based on on file size:

1. In the leftmost list, select **File Size**.
2. In the second list, select **Is more than** or **Is less than**

3. In the test field, type in a size.
4. In the last list, select Bytes, KB, MB, GB, or TB.

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

Defining Exceptions for Email Senders or Recipients

You can specify any of the following:

- From: For emails from a particular sender.
- 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 Exceptions for Partial and Exact Email Addresses

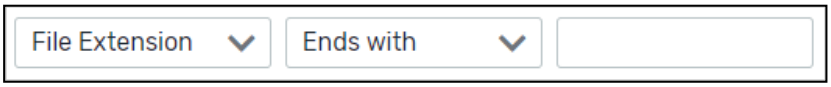
You can specify:

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

Follow these guidelines in both cases:

- You can use a @ sign in a full email address only. For example: "joe@abc.com". The following are illegal values: "@abc.com" or "joe@".
- Specify full domains only. For example: "abc.com" or "xyz.info".
- Specify usernames in a full email address only.
- Specify a single full email address when you want the exception to apply on any email message sent to that and other addresses. For example, specify "joe@abc.com" for the exception to apply on an email sent to or from "joe@abc.com" and "marie@abc.com" and "nick@techno.info".

Defining Exceptions for File Extensions



To specify a list of file type extensions:

1. In the leftmost list, select **File Extension**.
2. In the second list, select **Ends with** or **Doesn't end with**.

3. In the text field, type in the extensions you need. Separate them with commas. For example: DOC,PDF,XLSX.

Defining Exceptions for Validating Signatures

You can specify an exception for a file that is signed either with a valid or invalid digital signature.

3.5 Generating Reports

The Reporting feature provides a deeper look at positive selection activity performed by Votiro's Secure File Gateway on files and emails that enter your network.

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

- Summary Report
- Audit Report
- System Report

3.5.1 Summary Report

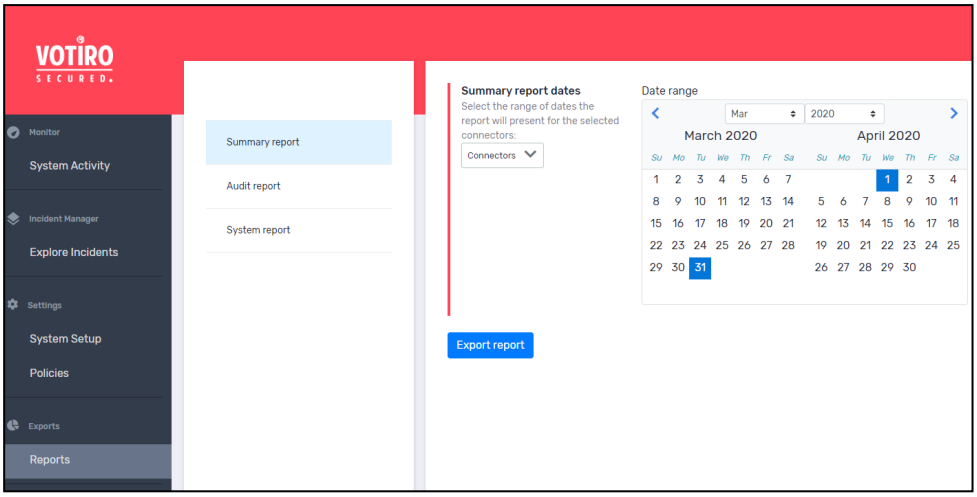
You can generate a summary report of the positive selection processing activity in your organization for a specified period.

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

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

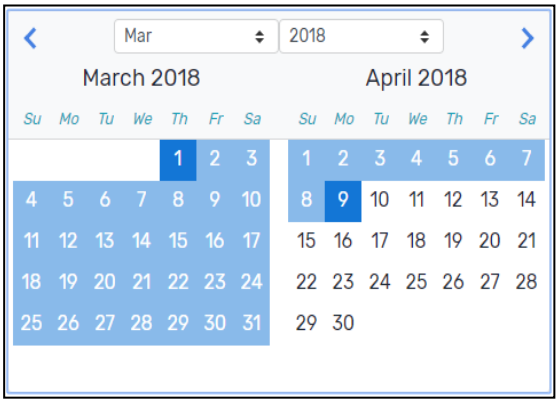
Generating a Summary Report

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



3. From the **Connectors** list, select the connectors for which to generate the report.
4. In the period selector, navigate to the desired start month either by clicking the right and left arrows or by selecting a month and year from the lists.
5. Click the start date.
6. Navigate to the desired end month.
7. Click the end date.

   The selected period is highlighted.



8. Click **Export Report**.

   The report is downloaded to your computer.

Summary Report Format and Structure

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

- Company name.
- Number of processing requests to Votiro's Positive Selection Engine.
- Number of individual files that were processed Votiro's Positive Selection Engine.

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

3.5.2 Audit Report

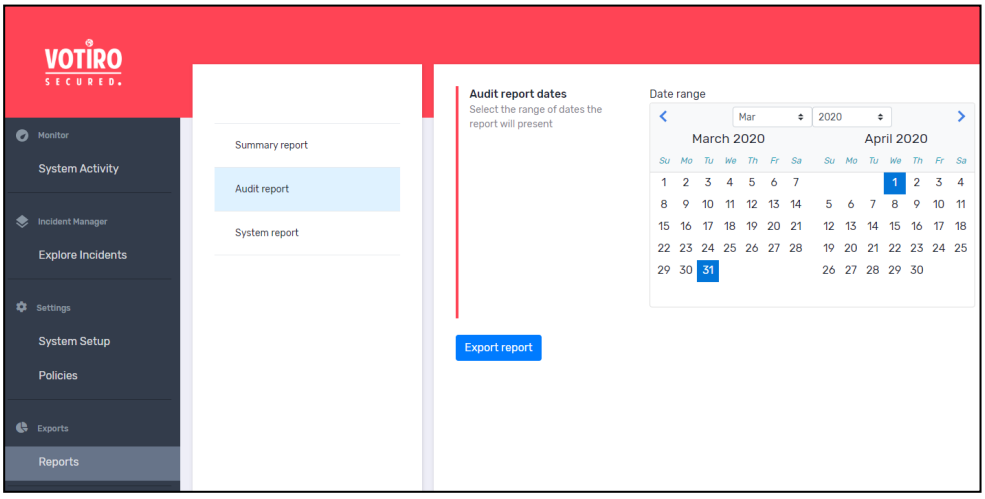
The purpose of this report is to present details of actions performed in the Management Dashboard for audit and tracking.

To protect enterprise privacy, Votiro'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.

Generating an Audit Report

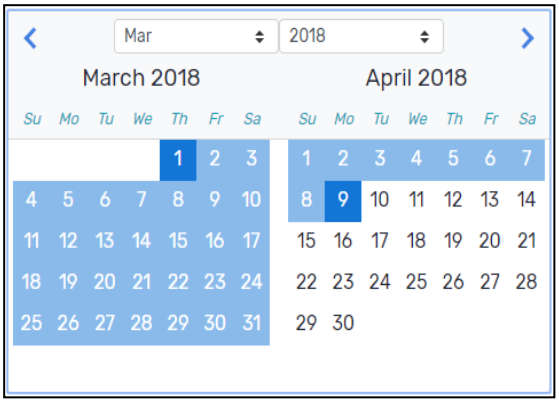
1. From the navigation pane on the left, click **Reports**.
2. Click **Audit report**.



3. In the period selector, navigate to the desired start month by clicking the right and left arrows or by selecting a month and year from the lists.
4. Click the start date.

5. Navigate to the desired end month.
6. Click the end date.

   The selected period is highlighted.



7. Click **Export Report**.

   The report is downloaded to your computer.

Audit Report Format and Structure

The audit is in CSV format. The following is an example excerpt as viewed in a spreadsheet application:

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

Information is provided for the following actions:

- Login
- Logout
- Original file download
- Processed file download
- Release original
- Policy save
- Settings save

- Roles changes
- Report export
- Policy creation

For each action, there is a datestamp (in UTC time) and a username.

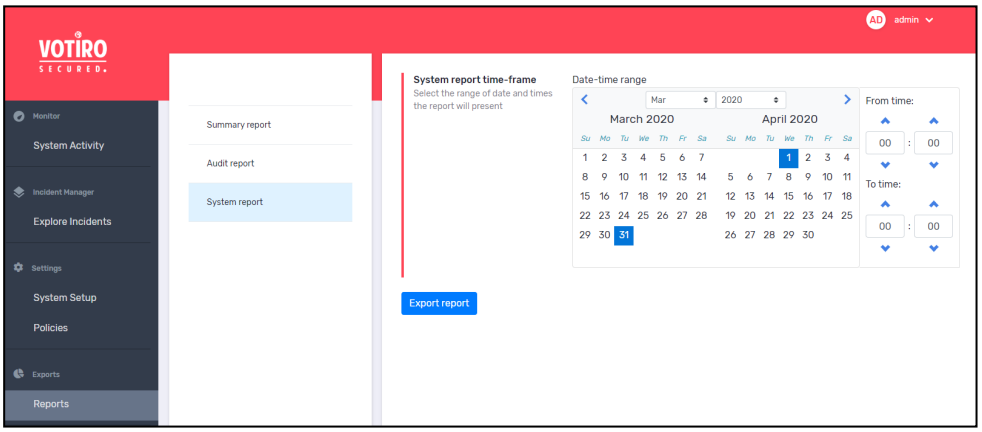
3.5.3 System Report

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.

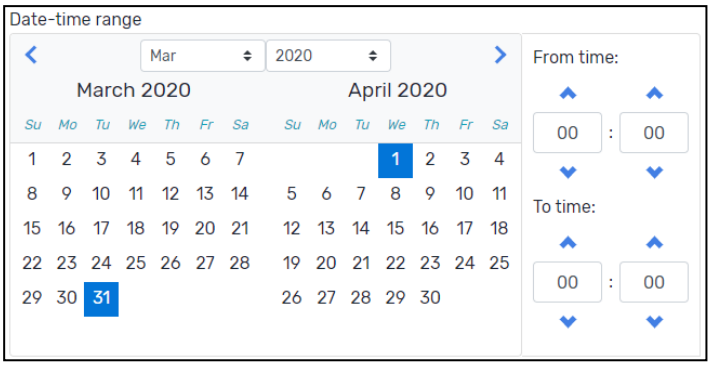
Generating a System Report

1. From the navigation pane on the left, click **Reports**.
2. Click **System report**.



3. In the period selector, navigate to the desired start month by clicking the right and left arrows or by selecting a month and year from the lists.
4. Click the start date.
5. Use the up and down arrows to select a start time. The default is 00:00.
6. Navigate to the desired end month.
7. Click the end date.
8. Use the up and down arrows to select an end time. The default is 00:00.

The selected period is highlighted.

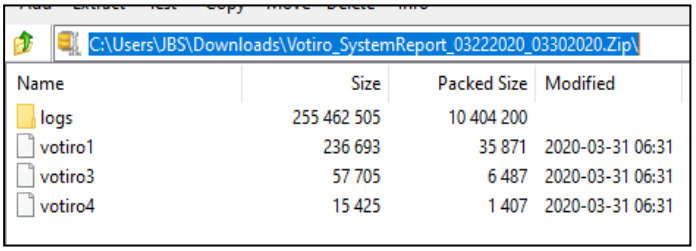


9. Click **Export Report**.

   The report is downloaded to your computer.

System Report Format and Structure

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



These files are password protected and for use by Votiro.

Appendix A Sending Logs to SIEM in CEF Format

Votiro's Secure File Gateway logs can be sent to SIEM in CEF format.

To enable SIEM logging, you must configure it in the report.xml file. The required configuration attributes are:

- **Log message format**: Must be CEF (default).
- **Address**: IP or hostname address for the Syslog server (default value = empty).
- **Port**: Syslog server port. Default port is 514.

An optional configuration attribute is:

- **AppName**: Scanner (default). The malware scanner sends antivirus update messages to SIEM.

> **Notes**
>
> - The IsActivated parameter under SiemSettings must be set to "true" in order for logs to be published.
> - For changes in the report.xml file to take effect, you must restart the Votiro.Sanitization.API and Votiro.SNMC Windows services.
> - For antivirus messages to be sent to SIEM, you must restart the Votiro Scanner service.

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

```
CEF:0|VOTIRO|SDS|7.2.0.289|20020100|Votiro Service Started|5|
rt=Sep 19 2017 05:57:38 dtz=03:00:00 dvchost=VOTIROSDSWS
msg=Votiro service started.
```

CEF Message Format

The CEF message format is as follows:

```
CEF:Version | Device Vendor | Device Product | Device Version |
Signature ID |Name |Severity | Date and host name extension
```

- **Version**. Always 0.
- **Device Vendor**: Always VOTIRO.
- **Device Product**: Always SDS.
- **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 below.
- **Severity**: Indicates the urgency of the event.

Table 6 Severity Levels

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

- **Date and host name extension**. The rest of the extension follows these three values.

  - **Date**. Timestamp of event occurrence in the system. The extension always begins with three values:
    - rt = receipt time = time the message was first reported
    - dtz = device time zone = abbreviated. See: Time Zone Abbreviations.
    - dvchost is the host name, for example, John-PC
  - **Host name**. The name of the Secure File Gateway server in which it occurred.
  - **Extension**. The last value is always msg, which stands for “message” and is the human readable message of the event description. See Report Events below.

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 7 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.
Trace	10020130	File Process	Child Item Created	New child created for item {ParentItemId}. Child ID: {ChildId}.
Trace	10020110	File Process	Positive Selection Complete	File {FileName} positive selection process successfully ended.
Trace	10020200	File Process	File Blocked	File {FileName} blocked as a result of the positive selection process.
Trace	10020300	File Process	Positive Selection Timeout	Positive selection for file {FileName} exceeded the time limit.
Trace	10050100	Blocker	Block - 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.

Category	Event Code	Sub-Category	Event Name	Event Description
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	Suspicious Auto Execution Macro	Suspicious Office macro detected [Auto Execution].
Indicator	50010020	Macro Analyzer	Suspicious File System Activity Macro	Suspicious Office macro detected [File System Activity].
Indicator	50010030	Macro Analyzer	Suspicious Out Of Document Interaction Macro	Suspicious 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	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.

Category	Event Code	Sub-Category	Event Name	Event Description
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	50070050	Suspicious File Structure	Suspicious File Structure	Suspicious structure detected in file {FileName}
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.