Votiro Disarmer API

User Guide

Version 3

February, 2020

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

Votiro's Disarmer exposes a REST API for adding Disarmer's protection to any application. The Votiro solution disarms threats from documents stored, accessed, shared, and collaborated on across multiple devices and data sources. In addition to email, file servers, and desktop applications, Votiro Disarmer offers various capabilities to help secure structured data, in many known formats, across the entire organization.

Maintaining full functionality of safe files, Votiro Disarmer protects against all known and unknown malicious content threats.

Additional information regarding Disarmer technology, sanitization policies, and supported file types can be found in the Votiro Disarmer User Guide and on the Votiro website: https://www.votiro.com.

This API document describes the programming interface to Votiro's Disarmer engine using a hosted Web Service in the cloud or on premises.

2 Sanitization Policies

A named policy is customized policy that meet your organization's requirements. Use the Votiro Management Dashboard to create a named policy.

If you do not create a customized policy, the Disarmer engine uses a set default policy.

For more information, see Managing Sanitization Policies in the Disarmer User Guide.

3 Responses and Error Codes

Votiro uses conventional HTTP response codes to indicate the success or failure of an API request. In general, codes in the 2xx range indicate success, codes in the 4xx range indicate an error that failed because of the information provided (for example, a required parameter was omitted), and codes in the 5xx range indicate an error with Votiro's servers.

Table 1 Error Codes

Status Code	Code Value	Description
200	OK	The request was successful.
400	Bad Request	The request included a non-existent resource, for example, an incorrect RequestID.
409	Conflict	There was an issue with the request parameters. The response includes detailed error information.
429	Too many requests	The request queue is full.
500	Internal Server Error	The server failed to process the request.

An error response includes the following parameters:

Table 2 Error Response Parameters

Parameter	Description	Type
Errors	List of error description objects.	list
Errors [n] Description	The ASCII encoded file name. If the file was sanitized successfully, this is the file name. If the file was blocked, then the suffix _blocked.pdf is appended to the file name.	string

Error Response Example

```
{
   "Errors": [
      {
         "Description": "File name is empty."
      }
   ]
```

```
}
```

4 Uploading a File for Sanitization

You can upload a potentially malicious file to the Votiro server, where it is queued for sanitization, and then sanitized. Sanitization policies that dictate how the file is scanned and sanitized can be set in Votiro Disarmer.

Select from the following options when uploading a file for sanitization:

- Upload
- Syncupload

4.1 Uploading a File for Sanitization

The upload step is followed by the check step. Upload the file for sanitization with the following command:

POST http[s]://<*base address*>/v3/upload/file?**filename**=<*filename*>

For information on the check step, see Checking the Status of a Sanitization Request on page 13.

4.2 Syncuploading a File for Sanitization

The syncupload step combines the upload step and the check step of the process to sanitize a file. Upload the file for sanitization with the following command:

POST http[s]://<*base address*>/v3/syncupload/file?**filename**=<*filename*>&timeout=*@seconds*

4.3 Request Data

Request URL Parameters

It is recommended to encode the URL using URL Encoding. This means that the file name can contain Unicode characters.

Request parameters are case sensitive.

Table 3 Request URL Parameters

Parameter	Description	Type	Required/optional
base address	The base address is configured when you install the Votiro API, or configured directly by Votiro.	string	Required
filename	Name of the file that you are uploading for sanitization. To achieve the most accurate sanitization, you must include the file extension. The file name and file extension should be identical to the file that the user received.	string	Required

Parameter	Description	Type	Required/optional
PolicyName	File name of a predefined policy rules collection (also called **named policy**). For PolicyName, specify the name of the policy, without any extension. For example, XML. If you do not enter a policy name, a default policy is applied.	string	Optional
Password	Allows sanitization of password-protected archive files with the following file types: 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. Password will be used only with PolicyName.	string	Optional
Timeout	The timeout parameter is associated with syncupload only. It is the maximum time allowed for the syncupload process to complete, expressed as a value in seconds. Should the command timeout before the sanitization process completes, the return message advises this. The command remains active. You can choose to resubmit the syncupload command, or use a GET command to check the request status. **Notes** ■ If a timeout parameter is not added, the default value is 600 seconds. ■ The maximum time allowed is 3600 seconds.	string	Optional

Note

Uploading 0-byte files is not supported.

Request Header Parameters

Request header parameters are case sensitive.

Table 4 Request Header Parameters

Parameter	Description	Type	Required/optional
Ocp-Apim-Subscription-Key	IF you are using the Votiro Cloud API, this is the subscription key you received from Votiro. IF you are using the Votiro API on premises, this is the subscription key you defined in the webapi.xml file.	string	For Votiro Cloud API - Required. For Votiro API on premises - required only if defined in the Disarmer engine.
Content-Type	Value must be "Application/octet-stream"	string	Required
ContextIdentifier	Identifier that enables easy identification.	string	Optional

Request Body

In the request body, supply the content of the file. The content should contain the file's binary data, that is, in the same way it is saved in the user's storage.

Request Examples

> **IMPORTANT!**
> The example commands use 'upload'. You can also use 'syncupload'.

- Posting a password-protected file named test.zip, providing the password 123456 and the context identifier joe.

```
POST https://api.votiro.com/v3/upload/file?filename
=test.zip&policyname=xxxxxx&password=123456 HTTP/1.1

Content-Length: 712692

Content-Type: application/octet-stream

Accept: */*

Ocp-Apim-Subscription-Key: <YOUR SUBSCRIPTION KEY>

ContextIdentifier: joe
```

Notes

- When using the Password parameter, you must set the password-protected policy to Allow. For more information, see Managing Sanitization Policies in the Votiro Disarmer User Guide.
- The password must be provided via the URL using the format password=<password and encoded....
  In case of a password-protected 7-Zip file that is being delivered with a wrong password, file will be blocked with an "error in sanitization process".

- Uploading a PDF file

```
POST https://api.votiro.com/v3/upload/file?filename =test.pdf
HTTP/1.1

Content-Length: 712692

Content-Type: application/octet-stream

Accept*/*: Ocp-Apim-Subscription-Key: <YOUR SUBSCRIPTION KEY

[Actual File Binary Content]
```

- Uploading a PDF file with a Unicode name

```
POST
https://api.votiro.com/v3/upload/file?filename=%2F%E3%83%86%E3
%82%B9%E3%83%88.pdf HTTP/1.1

Content-Length: 712692

Content-Type: application/octet-stream

Accept*/*: Ocp-Apim-Subscription-Key: <YOUR SUBSCRIPTION KEY>
[Actual File Binary Content]
```

- Uploading file using a named policy

```
POST
https://api.votiro.com/v3/upload/file?filename=test.zip&Policy
Name =xxxxxx HTTP/1.1

Content-Length: 712692

Content-Type: application/octet-stream

Accept*/*:

Ocp-Apim-Subscription-Key: <YOUR SUBSCRIPTION KEY>

[Actual File Binary Content]
```

4.4 Response Data

Response Parameters

Table 5 Response Parameters

Parameter	Description	Type
RequestID	Upload request ID.	string
PolicyName	Contains the name of predefined policy rules collection (named policy), instead of policy rules.	string

Response Examples

- Response to an uploaded PDF file

```
{
  "RequestID": "4d6888d1-5ab5-4cf5-9d19-d43f16fd01d8"
}
```

- Response to a file uploaded using a named policy

```
{
  "RequestID": "4d6888d1-5ab5-4cf5-9d19-d43f16fd01d8",
  "UsedNamedPolicy": "Sales and Marketing"
}
```

4.5 Load Balancing and High Availability

VotiroDisarmer supports load balancing and high availability. This can be achieved by using either of these two options:

- An application delivery controller.
- A Layer 7 load balancer that supports sticky-session and HTTP cookie-based load balancing.

You can set the cookie generated by the load balancer for reuse by the API request.

5 Checking the Status of a Sanitization Request

GET http[s]://*<base address>*/v3/file/*<RequestID>*/status

Checks the processing status of a file using the RequestID you received when uplaoding the file for saniztizaton.

The sanitization process relies on polling. If no polling takes place for over 60 seconds there is a chance the sanitization request may be deleted. You can configure setting values for the polling interval and the keep alive interval attributes. See Votiro Disarmer User Guide, Configuring the Management Platform.

> **Note**
> To cancel the sanitization of a file you can stop the GET command. The cancellation may take upto 60 seconds to take effect.

5.1 Request Data

Request URL Parameters

Request parameters are case sensitive.

Table 6 Request URL Parameters

Parameter	Description	Type	Required/optional
RequestID	Upload request ID	string	Required

Request Header Parameters

Request parameters are case sensitive.

Table 7 Request Header Parameters

Parameter	Description	Type	Required/optional
Ocp-Apim-Subscription-Key	IF you are using the Votiro Cloud API, this is the subscription key you received from Votiro. IF you are using the Votiro API on premises, this is the subscription key you defined in the webapi.xml file.	string	For Votiro Cloud API - Required. For Votiro API on premises - required only if defined in the Disarmer engine.

Request Example

```
GET https://api.votiro.com/v3/file/c94f00a4-7a36-4152-977d-
dda71cccfb95/status HTTP/1.1

Ocp-Apim-Subscription-Key: <YOUR SUBSCRIPTION KEY>
```

5.2 Response Data

Response Parameters

Table 8 Response Parameters

Parameter	Description	Type
Status	The status of the sanitization request	string

Sanitization Request Statuses

Table 9 Sanitization Request Statuses

Status Name	Description
Queued	The file you uploaded is in the sanitization queue.
Processing	The file you uploaded is being processed by the Votiro system.
Done	The file you uploaded is sanitized, and you can download the file.
Error	The file you uploaded was not sanitized because of an internal Votiro error.
Blocked	The file you uploaded was blocked in the sanitization process. Download the file for more information on why the file was blocked.
LimitExceeded	Exceeded the number of uploads.

Response Example

```
{

   "Status": Done

}
```

6 Downloading a Sanitized File

GET http[s]://<*base address*>/v3/file/<*RequestID*>

Downloads a file with a Done or Blocked status.

The download request for a blocked file returns a PDF with the reason the file was blocked during the sanitization process.

The file name is returned in all response headers.

6.1 Request Data

Request URL Parameters

Request parameters are case sensitive.

Table 10 Request URL Parameters

Parameter	Description	Type	Required/optional
RequestID	Upload request ID	string	Required

Request Header Parameters

Request parameters are case sensitive.

Table 11 Request Header Parameters

Parameter	Description	Type	Required/optional
Ocp-Apim-Subscription-Key	IF you are using the Votiro Cloud API, this is the subscription key you received from Votiro. IF you are using the Votiro API on premises, this is the subscription key you defined in the webapi.xml file.	string	For Votiro Cloud API - Required. For Votiro API on premises - required only if defined in the Disarmer engine.

Request Example

```
GET https://api.votiro.com/v3/file/c94f00a4-7a36-4152-977d-
dda71cccfb95 HTTP/1.1

Ocp-Apim-Subscription-Key: <YOUR SUBSCRIPTION KEY>
```

6.2 Response Data

Response Body (Content Disposition)

Table 12 Response Body (Content Disposition)

Parameter	Description	Type
attachment		string

Parameter	Description	Type
filename	The ASCII encoded file name. If the file was sanitized successfully, this is the file name. If the file was blocked, then the suffix _ blocked.pdf is added to the file name.	string
filename*	The UTF-8 URL encoded file name. If the file was sanitized successfully, this is the file name. If the file was blocked, then the suffix _ blocked.pdf is added to the file name.	string

Response Example

```
HTTP/1.1 200 OK Content-Type: application/octet-stream Server: Microsoft-HTTPAPI/2.0

Content-Disposition: attachment;

filename=test.pdf;

filename*=UTF-8''test.pdf Date: Fri. 13 Nov 2016 13:21:59

[Actual File Binary Content]
```

7 Downloading a Sanitization Report

GET http[s]://<*base address*>/v3/file/<*RequestID*>/report

Generates a report that details which engines were executed on each item and sub-item during the sanitization process.

7.1 Request Data

Request URL Parameters

Request parameters are case sensitive.

Table 13 Request URL Parameters

Parameter	Description	Type	Required/optional
RequestID	Upload request ID	string	Required

Request Header Parameters

Request parameters are case sensitive.

Table 14 Request Header Parameters

Parameter	Description	Type	Required/optional
Ocp-Apim-Subscription-Key	IF you are using the Votiro Cloud API, this is the subscription key you received from Votiro. IF you are using the Votiro API on premises, this is the subscription key you defined in the webapi.xml file.	string	For Votiro Cloud API - Required. For Votiro API on premises - required only if defined in the Disarmer engine.

Request Example

```
GET https://api.votiro.com/v3/file/c94f00a4-7a36-4152-977d-dda71cccfb95/report HTTP/1.1

Ocp-Apim-Subscription-Key: <YOUR SUBSCRIPTION KEY>
```

7.2 Response Data

Response Body

Table 15 Response Body

Parameter	Description	Type
FileName	Relative path of artifact file.	string

Parameter	Description	Type
FileType	File type information for the current artifact as determined by Votiro File Type Discoverer.	object
FileType.Code	File type code	number
FileType.Type	Artifact file type description	string
FileType.Family	Artifact file type family description	string
Events	Events for the current artifact.	array of Event objects
Event.Id	Event code. See the following table.	number
Event.Details	Event textual description. Subject to changes.	string
Event.Severity	Urgency of the event: The valid integer values are 0-6, where 6 is the most severe.	number
Event.Category	Category. Can be one of: ■ Trace ■ System ■ Indicator	object
Event.SubCategory	Subcategory. See the following table. The subcategory name is unique within the category that is belongs to.	object
Event.Value	Event type. It is unique within the subcategory that is belongs to.	number
Event.Name	SubCategory name. See the following table.	string
Children	Sub-objects that were processed separately from the sanitized file, for example, a ZIP archive file or nested Office document.	array

Response Example

```
HTTP/1.1 200 OK

{

   "FileName": "sample_file.ppt",

   "FileType": {

      "Code": 16,
```

```
    "Type": "Power Point",
    "Family": "Microsoft Office"
  },
  "Events": [
    {
      "Id": 10000010,
      "Details": "File sample_file.ppt was recognized as [16]
      Power Point (Microsoft Office)",
      "Severity": 2,
      "Category": {
      "Value": 10000000,
      "Name": "Trace"
      },
      "SubCategory": {
      "MainCategory": {
      "Value": 10000000,
      "Name": "Trace" },
    "Value": 0,
    "Name": "File Type Discoverer" },
    "Value": 10,
    "Name": "File Type Discoverer"
    },
    {
    "Id": 10010010,
    "Details": "File sample_file.ppt was successfully scanned by
    AV AviraAntiVirus",
    "Severity": 2,
    "Category": {
    "Value": 10000000,
    "Name": "Trace"
    },
    "SubCategory": {
```

```
"MainCategory": {
"Value": 10000000,
"Name": "Trace"
},
"Value": 10000,
"Name": "AV Scan"
}, "Value": 10,
"Name": "AV Scan"
},
{
"Id": 10020110,
"Details": "File sample_file.ppt sanitization process
successfully ended",
"Severity": 2,
"Category": {
"Value": 10000000,
"Name": "Trace"
},
"SubCategory": {
"MainCategory": {
"Value": 10000000,
"Name": "Trace" },
"Value": 20000,
"Name": "File Process"
},
"Value": 110,
"Name": "File Process" }
],
"Children": []
}
```


Report Events

Event codes respect the following 8-digit scheme:

LLRCCTTR

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 16 CEF Message Template Extensions

Category	Event Code	Event Name	Sub-Category	Event Description
Trace	10000010	True File Type	File Type Discoverer	File {FileName} was recognized as {FileType}.
Trace	10010010	Antivirus Scan	Antivirus	File {FileName} was successfully scanned by AV {AVEngine}.
Trace	10020100	File Uploaded	File Process	File {FileName} upload for sanitization started.
Trace	10020110	Sanitization Done	File Process	File {FileName} sanitization process successfully ended.
Trace	10020200	File Blocked	File Process	File {FileName} was blocked as a result of the sanitization process.
Trace	10030100	API Limit Exceeded	API	File {FileName} upload request for sanitization exceeded the limit number of uploads.
Trace	10050100	Block - Policy	Blocker	File {FileName} was blocked due to your organization policy violation [{Policy}] in the sanitization process.
Trace	10050200	Block - Antivirus	Blocker	Virus found by {AVEngine} in file {FileName}.
Trace	10050300	Block- Sandbox	Blocker	Threat found by {SandboxName} in file {FileName}.
Trace	10050500	Block - Error	Blocker	File {FileName} was blocked due to an error in Sanitization process.

Category	Event Code	Event Name	Sub-Category	Event Description
Trace	10060100	Password Opened	Password Protected Opener	Password Protected File {FileName} successfully opened.
Trace	10060110	Password Added	Password Protected Opener	Password Protected File {FileName} successfully closes with original password.
Trace	10060200	Wrong Password	Password Protected Opener	Password Protected File {FileName} couldn't be opened.
Trace	10070010	Sandbox Scan	Sandbox	File {FileName} successfully scanned by {SandboxName}.
System	20010100	Antivirus Update Error	Antivirus	{AVEngine} signatures update process failed.
System	20010200	Antivirus Update	Antivirus	{AVEngine} signatures update process ended successfully.
System	20010300	Antivirus License Error	Antivirus	{AVEngine} license is invalid. License update is required.
System	20020000	Votiro Service Starting	Service	{ServiceName} is starting.
System	20020100	Votiro Service Started	Service	{ServiceName} service started.
System	20020110	Votiro Service Stopped	Service	{ServiceName} service stopped.
System	20030400	License Expired	License	License has expired, in {DaysToShutDown} days SDS will stop working, please renew your license.
System	20040500	Url Connection Error	UrlReputation	Url Reputation service '{0}' cannot be reached.
System	20050600	Votiro Sandbox Service Error	Sandbox	Votiro sandbox service '{SandboxName}' cannot be reached.
System	20050700	Sandbox Service Error	Sandbox	Sandbox service '{SandboxName}' cannot be reached.
Indicator	50010000	Suspicious Macro	Macro Analyzer	Suspicious Office macro detected.
Indicator	50010010	Suspicious Auto Execution Macro	Macro Analyzer	Suspicious Office macro detected [Auto Execution].

Category	Event Code	Event Name	Sub-Category	Event Description
Indicator	50010020	Suspicious File System Activity Macro	Macro Analyzer	Suspicious Office macro detected [File System Activity].
Indicator	50010030	Suspicious Out Of Document Interaction Macro	Macro Analyzer	Suspicious Office macro detected [Out-Of-Document Interaction].
Indicator	50010040	Suspicious Office Excel 4.0 Macro	Macro Analyzer	Suspicious Office Excel 4.0 macro detected.
Indicator	50020010	Suspicious Fake File	File Type Discoverer	Suspicious fake file [Extension does not match file structure] was detected in the artifact.
Indicator	50020020	Suspicious Unknown File	File Type Discoverer	Unknown file [Data file or unidentified file type] was detected in the artifact.
Indicator	50020110	Suspicious Executable File	File Type Discoverer	Executable file was detected in the artifact.
Indicator	50020120	Suspicious Script File	File Type Discoverer	Script file was detected in the artifact.
Indicator	50030100	Suspicious Threat File	AV	AV {AVEngine} detects a threat ({ThreatType}) in file {FileName}.
Indicator	50040010	External Program Run Action	Active Element	External Program Run Action detected in file {Filename}.
Indicator	50050010	Dynamic code exception	JavaScript Analyzer	Dynamic code exception detected in file {Filename}.
Indicator	50060010	Suspicious URL detected	Suspicious URL	Suspicious url detected in file {FileName}, URLs: {SuspiciousUrlsList}
Indicator	50070050	Suspicious File Structure	Suspicious File Structure	Suspicious structure detected in file {FileName}
Indicator	50080100	Suspicious Sandbox Threat File	Sandbox	Sandbox engine {SandboxName} detected a threat ({ThreatName}) in file {FileName}.

8 Getting Service Information

GET http[s]://<*base address*>/v3/info

Generates a JSON file that details the API version and Disarmer version of the system.

8.1 Request Data

Request Header Parameters

Request parameters are case sensitive.

Table 17 Request Header Parameters

Parameter	Description	Type	Required/optional
Ocp-Apim-Subscription-Key	IF you are using the Votiro Cloud API, this is the subscription key you received from Votiro. IF you are using the Votiro API on premises, this is the subscription key you defined in the webapi.xml file.	string	For Votiro Cloud API - Required. For Votiro API on premises - required only if defined in the Disarmer engine.

Request Example

```
GET https://api.votiro.com/v3/info HTTP/1.1

Ocp-Apim-Subscription-Key: <YOUR SUBSCRIPTION KEY>
```

8.2 Response Data

Response Parameters

Table 18 Response Parameters

Parameter	Description	Type
ApiVersion	The Disarmer API version	string
SdsVersion	The Disarmer version	string

Response Example

```
{
      "ApiVersion": "3",
      "SdsVersion": "2.2.2.333"
}
```