

Votiro Cloud for Web Applications

User Guide

**August 2024**

**Copyright Notice**

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

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

[www.votiro.com](http://www.votiro.com/)

**Contents**

1. [Introduction](#_bookmark0) [4](#_bookmark0)
2. [Positive Selection Policies](#_bookmark1) [5](#_bookmark1)
3. [Uploading a File for Positive Selection](#_bookmark2) [6](#_bookmark2)
   1. [Uploading a File for Positive Selection](#_bookmark3) [6](#_bookmark3)
   2. [Sync-uploading a File for Positive Selection](#_bookmark4) [6](#_bookmark4)
   3. [Request Data](#_bookmark5) [7](#_bookmark5)
   4. [Response Data](#_bookmark6) [11](#_bookmark6)
4. [Downloading a Processed File](#_bookmark7) [13](#_bookmark7)
   1. [Request Data](#_bookmark8) [13](#_bookmark8)
   2. [Response Data](#_bookmark9) [13](#_bookmark9)
5. [Downloading a Positive Selection Report](#_bookmark10) [15](#_bookmark10)
   1. [Request Data](#_bookmark11) [15](#_bookmark11)
   2. [Response Data](#_bookmark12) [15](#_bookmark12)
6. [Checking the Status of a Positive Selection Request](#_bookmark13) [19](#_bookmark13)
   1. [Request Data](#_bookmark14) [19](#_bookmark14)
7. [Responses and Error Codes](#_bookmark15) [20](#_bookmark15)
   1. [Response Data](#_bookmark16) [21](#_bookmark16)
8. [Getting Service Information](#_bookmark17) [26](#_bookmark17)
   1. [Request Data](#_bookmark18) [26](#_bookmark18)
   2. [Response Data](#_bookmark19) [26](#_bookmark19)

[Appendix A Sample Code - Sync-upload](#_bookmark20) [27](#_bookmark20)

[Appendix B Votiro API Postman Collection](#_bookmark21) [30](#_bookmark21)

# Introduction

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

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

Additional information regarding Votiro's technology, positive selection policies, and supported file types can be found in the Votiro Cloud User Guide and on the Votiro website: [https://www.votiro.com](https://www.votiro.com/).

This Votiro Cloud for Web Applications document describes the programming interface to Votiro's Positive Selection® Engine using a hosted Web Service in the cloud or on premises.

# Positive Selection Policies

A named policy is customized policy that meet your organization's requirements for processing files for positive selection of safe elements. Use the Votiro Cloud Management Dashboard to create positive selection named policies by case and by file type.

If you do not create a customized policy, Votiro's Positive Selection® Engine uses the set default policy for the case or file type being processed.

For more information, see Managing Positive Selection Policies in the Votiro Cloud User Guide.

# Uploading a File for Positive Selection

You can upload a potentially malicious file to Votiro Cloud, where it is queued for positive selection, and then processed. Positive selection policies that dictate how the file is scanned and processed can be set in Votiro Cloud.

Select from the following options when uploading a file for positive selection:

* **Upload** - this option requires calling three APIs in the order below:
  1. [See Uploading a File for Positive Selection](#_bookmark2) - this is the upload request
  2. [See Checking the Status of a Positive Selection Request](#_bookmark13) - this is the check status request called after receiving the requestId from the completed upload request
  3. [See Downloading a Processed File](#_bookmark7) - this is the download processed file request called after receiving the status from the check status request
* **Sync-upload** - this option requires calling two APIs in the order below:
  1. [See Sync-uploading a File for Positive Selection](#_bookmark4) - this is the sync-upload request. The sync-upload finishes after the file sanitization is done. The response for the sync-upload will be the requestId and status. For example:

requestId: "58be4846-9c82-4c58-8775-f3a8a935fd5c", status: "Done"

* 1. [See Downloading a Processed File](#_bookmark7) - this is the download processed file request called after receiving the status from the completed sync-upload request

**Notes**

Files up to 2 GB can be uploaded for positive selection. Uploading 0-byte files is not supported.

## Uploading a File for Positive Selection

Upload the file for positive selection with the following command:

**POST https://<*votiro\_appliance*>/disarmer/api/disarmer/v4/upload**

## Sync-uploading a File for Positive Selection

The sync-upload step combines the upload step and the check step of the positive selection process for a file. Upload the file for positive selection with the following command:

**POST https://<*votiro\_appliance*>/disarmer/api/disarmer/v4/upload-sync**

## Request Data

#### Request URL Parameters

No additional parameters are added to the request URL.

#### Request Header Parameters

Request header parameters are case sensitive.

**Table 1 Request Header Parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Description** | **Type** | **Required/ Optional** |
| Authorization | This is the Bearer <token> | string | Required |
| Content-Type | Value must be "multipart/form-data" | string | Required |

**Notes**

* For creating a token see the Votiro Cloud User Guide, Configuring System Settings.
* You can use additional recommended header keys depending on your environment, for example, **Host**, **Accept** with value "\*/\*".

#### 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.

**Table 2 Request Body Parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Description** | **Type** | **Required/ Optional** |
| File | File form-data, including: file name, file length and binary data. | string | Required |

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Description** | **Type** | **Required/ Optional** |
| Properties | Values must be associated with keys from the JSON key-value collection. For example:  {"key1":"value1"}. Optional Properties include: **PolicyName**  File name of a predefined policy rules collection (also known as **named policy**).  For PolicyName, specify the name of the policy, without any extension. For example, CXO.  **Note**   * If you do not enter a policy name, a default policy is applied. * If the PolicyName entered does not match a policy set up in Votiro Cloud, the default policy is used. A message will appear in the log.   **Password**  Allows positive selection 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.  **ChannelType**  The name of the channel type of connector being used.  For ChannelType, specify **FileConnector**. **ChannelId** and **ChannelName**  The ChannelId and ChannelName are paired.  **ChannelId** is provided by Votiro and is a unique identifier of the application.  **ChannelName** should be a human readable name, so it can be filtered by the end user (Email, Portal, etc.) | string | Required; can be empty |

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Description** | **Type** | **Required/ Optional** |
|  | **Extended request information**:  **User**, **Groups**, **Client**, **Server**, **From**, **To**, **Path** are all optional, but reserved words. These attributes are important for monitoring and analytics of our product.  **Other Key values**:  **Domain**, **User Agent**, **URL Category**, **Application ID**, or any other useful information will be populated into a dedicated UI widget. |  |  |

**Notes**

* When using the Password parameter, you must set the Password Protected case policy to **Sanitize**.
* For more information, see Managing Positive Selection Policies in the Votiro Cloud User Guide.

#### Request for Sync-upload

To manage sync-upload requests in your environment, optional content changes to the file can be made to the following:

* + - Virtual appliance address
    - Bearer token
    - Filepath
    - Policy Name
    - Channel Name
    - Channel ID

**Note**

Do not change **Channel Type**, it must remain as "FileConnector".

For more details and an example of file content changes, see [Sample Code - Sync-upload](#_bookmark20) [on page 27](#_bookmark20).

#### Request Examples

**IMPORTANT!**

The example commands use **upload**. You can also use **upload-sync**.

* + - Posting a password-protected file named *Q1Reports.zip*.

POST https://api.votiro.com/disarmer/api/disarmer/v4/upload HTTP/1.1 Host: api.votiro.com

Authorization: Bearer: <Token> Content-Length: 712692

Content-Type: multipart/form-data; boundary=<Boundary>

<Boundary>

Content-Disposition: form-data; name="File"; filename="<filepath>/*Q1Reports.zip*"

Content-Type: <Content-Type header here> (data)

Content-Disposition: form-data; name="Properties"

{"ChannelType":"FileConnector","ChannelId":"30acc6eb-16d9-4133- ae43-0f5b6d40a318","ChannelName":"ChannelFin", "Password":"psWd172","PolicyName":"Default Policy"}

<Boundary>

* + - Uploading a PDF file named *OrgChart.pdf*.

POST https://api.votiro.com/disarmer/api/disarmer/v4/upload HTTP/1.1 Host: api.votiro.com

Authorization: Bearer: <Token> Content-Length: 712692

Content-Type: multipart/form-data; boundary=<Boundary>

<Boundary>

Content-Disposition: form-data; name="File"; filename="<filepath>/*OrgChart.pdf*"

Content-Type: <Content-Type header here> (data)

Content-Disposition: form-data; name="Properties"

{"ChannelType":"FileConnector","ChannelId":"30acc6eb-16d9-4133- ae43-0f5b6d40a319","ChannelName":"ChannelHR", "PolicyName":"Default Policy"}

<Boundary>

## Response Data

#### Response Parameters

**Table 3 Response Parameters**

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Description** | **Type** |
| requestId | Upload request ID. | string (GUID) |

#### Response Examples

* + - Response to an uploaded PDF file using upload command:

4d6888d1-5ab5-4cf5-9d19-d43f16fd01d8

* + - Response to a file uploaded using upload-sync command:

{

"requestId": "4d6888d1-5ab5-4cf5-9d19-d43f16fd01d8", "status": "Done"

}

# Downloading a Processed File

**GET https://<*votiro\_appliance*>/disarmer/api/disarmer/v4/ download/<*requestId*>**

Downloads a file with a **Done** or **Blocked** status.

The download request for a blocked file returns a PDF detailing the reason the file was blocked during the positive selection process.

The file name is returned in all response headers.

## Request Data

### Request URL Parameters

Request parameters are case sensitive.

**Table 4 Request URL Parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Description** | **Type** | **Required/Optional** |
| requestId | Upload request ID | string | Required |

### Request Header Parameters

Request parameters are case sensitive.

**Table 5 Request Header Parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Description** | **Type** | **Required/Optional** |
| Authorization | Bearer <token> is used for authentication | string | Required. |

### Request Example

GET https://api.votiro.com/disarmer/api/disarmer/v4/download/ c94f00a4-7a36-4152-977d-dda71cccfb95

Authorization: "Bearer <token>"

## Response Data

### Response Body (Content Disposition)

**Table 6 Response Body (Content Disposition)**

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Description** | **Type** |
| attachment |  | string |

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Description** | **Type** |
| filename | The ASCII encoded file name.  If the file was processed 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 processed 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]

# Downloading a Positive Selection Report

**GET https://<*votiro\_appliance*>/disarmer/api/disarmer/v4/report/<*ID*>**

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

## Request Data

### Request URL Parameters

Request parameters are case sensitive.

**Table 7 Request URL Parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Description** | **Type** | **Required/Optional** |
| ID | Upload request ID | string | Required |

### Request Header Parameters

Request parameters are case sensitive.

**Table 8 Request Header Parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Description** | **Type** | **Required/Optional** |
| Authorization | Bearer <token> is used for authentication | string | Required. |

### Request Example

GET https://api.votiro.com/disarmer/api/disarmer/v4/report/ c94f00a4-7a36-4152-977d-dda71cccfb95

Authorization: "Bearer <token>"

## Response Data

The download response is a JSON object.

### Response Body

**Table 9 Response Body**

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Description** | **Type** |
| ID | Upload request ID. | string |
| relativePath | Relative path of the child from the root item. | string |
| originalFileName | Relative path of artifact file. | string |
| sanitizedFileName | Relative path of artifact file. | string |

|  |  |  |
| --- | --- | --- |
| **Parameter Description Type** | | |
| originalSize | File size in bytes of the original file. | number |
| sanitizedSize | File size in bytes of the processed file. | number |
| originalPublishStatus | Publish status of the original file. | number |
| sanitizedPublishStatus | Publish status of the processed file. | number |
| 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 |
| queueTime | Always zero, positive selection process starts immediately. | string |
| processStartTime | Time Votiro started the file processing. | string |
| processEndTime | Time Votiro processing ended. | string |
| status | Positive selection status. | string |
| Events | Events for the current artifact. | array of Events objects |
| Events.date | The date and time of the event. | string |
| Events.id | Event code. See the following table. | number |
| Events.name | Event name. | string |
| Events.message | Event textual description message. Subject to changes. | string |
| Events.severity | Urgency of the event: The valid integer values are 0-6, where 6 is the most severe. | number |
| Events.category | Category name and value. Can be one of:   * Trace - 10000000 * System - 20000000 * Indicator - 5000000 * Internal Trace - 6000000   See the following Report Events table. | number |
| Events.subCategory | The subCategory name and value are unique within the category it belongs to.  See the following Report Events table. | number |
| children | Sub-objects that were processed separately from the processed file, for example, a ZIP archive file or nested Office document. | array |
| hash | File hash code. | string |
| extendedInfo | Email metadata, if delivered. | object |

### Response Example

{

"id": "0bafef86-41e0-4ccc-a69f-00b812cb5602", "relativePath": "",

"originalFileName": "bar.json", "sanitizedFileName": "bar.json", "originalSize": 450,

"sanitizedSize": 0,

"originalPublishStatus": 0,

"sanitizedPublishStatus": 0, "fileType": {

"code": 125,

"type": "Unknown Text", "family": "Unknown Text Files"

},

"queueTime": "00:00:00",

"processStartTime": "2020-07-13T09:33:51.8399432Z", "processEndTime": "2020-07-13T09:33:56.855111Z",

"status": "OK", "events": [

{

"date": "0001-01-01T00:00:00", "id": 10020100,

"name": "File Uploaded",

"message": "File bar.json upload for sanitization started. Item Id: 0bafef86-41e0-4ccc-a69f-00b812cb5602",

"severity": 2,

"category": 10000000,

"subCategory": 10020000

}

],

"children": [], "hash":

"d598b34dc6d5e1556a00ff9df852f390fef6bc9a390ca744f12cd88ee892 99f7",

"extendedInfo": { "email": {

"headers": [], "from": {

"address": null, "displayName": null

},

"to": [],

"envelopeRecipients": [], "cc": [],

"bcc": [], "subject": null,

"body": null,

"date": "2020-07-13T13:08:08.1473082+00:00",

"attachments": [], "embeddedResources": []

}

}

}

# Checking the Status of a Positive Selection Request

**GET https://<*votiro\_appliance*>/disarmer/api/disarmer/v4/status/<*requestId*>**

Checks the processing status of a file using the *requestId* you received when uploading the file for positive selection processing.

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

**Note**

To cancel the processing of a file you can use the GET command. The Cancellation Timeout value is set by default according to the version you are using:

For SaaS: "CancellationTimeout": "01:02:30"

For on-premises VA: "CancellationTimeout": "00:02:30"

To change this value, contact our Support team for instructions.

## 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** |
| Authorization | Bearer <token> used for authentication | string | Required. |

### Request Example

GET https://api.votiro.com/disarmer/api/disarmer/v4/status/ c94f00a4-7a36-4152-977d-dda71cccfb95

Authorization: "Bearer <token>"

# 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 12 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*. |
| 401 | Unauthorized | Authentication failure due to incorrect service token. Recommended action: verify the service token. |
| 404 | Not Found | The request failed due to high load on the system. Recommended action: retry request. |
| 409 | Conflict | There was an issue with the request parameters. The response includes detailed error information. |
| 429 | Max InProgress Requests | Maximum number of concurrent sanitization requests are reached |
| 500 | Internal Server Error | The server failed to process the request. |

An error response includes the following parameters:

**Table 13 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 processed 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."

## Response Data

### Response Parameters

**Table 14 Response Parameters**

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Description** | **Type** |
| Status | The status of the positive selection request | string |

### Positive Selection Request Statuses

**Table 15 Positive Selection Request Statuses**

|  |  |
| --- | --- |
| **Status Name** | **Description** |
| NotExist | The *requestId* of the file uploaded is not found. The *requestId* may be incorrect or the positive selection report data has been removed.  **Note**: This status is not relevant for the sync-upload API. |
| Processing | The file you uploaded is being processed by Votiro Cloud.  **Note**: This status is not relevant for the sync-upload API. |
| Done | The file you uploaded is processed, and you can download the file. |
| Error | The file you uploaded was not processed because of an internal Votiro error. |
| Blocked | The file you uploaded was blocked in the positive selection process. Download the file for more information on why the file was blocked. |

### Response Example

"Done"

### 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 16 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 | Sanitization Complete | File {FileName} sanitization process successfully ended. |
| Trace | 10020200 | File Process | File Blocked | File {FileName} blocked as a result of the positive selection process. |
| Trace | 10020300 | File Process | Sanitization Timeout | Sanitization of the file  {FileName} exceeded the time limit. |
| Trace | 10050000 | Blocker | Block - Unknown File (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process. |
| Trace | 10050010 | Blocker | Block - Large File (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process. |
| Trace | 10050020 | Blocker | Block - Complex File (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process. |
| Trace | 10050030 | Blocker | Block - Binary File (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process. |
| Trace | 10050040 | Blocker | Block - Other Unsupported File (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Event Code** | **Sub- Category** | **Event Name** | **Event Description** |
| Trace | 10050050 | Blocker | Block - DDE (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process - DDE detected. |
| Trace | 10050060 | Blocker | Block - Macro (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process - Suspicious macro detected. |
| Trace | 10050070 | Blocker | Block - Suspicious URL (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process - Suspicious URL detected. |
| Trace | 10050080 | Blocker | Block - Password Protected (Policy) | File {FileName} blocked due to your organization policy violation [{Policy}] in the sanitization process - Password Protected File. |
| Trace | 10050100 | Blocker | Block - General (Policy) | File {FileName} blocked due to your organization policy violation {Policy} in the positive selection process. |
| Trace | 10050500 | Blocker | Block - Error | File {FileName} blocked due to an error in positive selection process. |
| Trace | 10060100 | Password Protected Opener | Password Opened | Password Protected File  {FileName} successfully opened. |
| Trace | 10060110 | Password Protected Opener | Password Added | Password Protected File  {FileName} successfully closes with original password. |
| Trace | 10060200 | Password Protected Opener | Wrong Password | Password Protected File  {FileName} couldn't be opened. |
| Trace | 10080100 | Validate Signature | Validate Signature Succeeded | Signature Validation for file  {FileName} succeeded. |
| System | 20060800 | System Error | Fatal Error | System error occurred during handling request of file {FileName}. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Event Code** | **Sub- Category** | **Event Name** | **Event Description** |
| System | 21020100 | Warning | Low Disk Space | The system is running on low disk space: Used {used} of {diskSize} ({usagePercent}%), available {available} |
| Indicator | 50010000 | Macro Analyzer | Suspicious Macro | Suspicious Office macro detected. |
| Indicator | 50010010 | Macro Analyzer | Auto Execution Macro | Suspicious Office macro detected [Auto Execution]. |
| Indicator | 50010020 | Macro Analyzer | File System Activity Macro | Office macro detected [File System Activity]. |
| Indicator | 50010030 | Macro Analyzer | Out Of Document Interaction Macro | Office macro detected [Out- Of-Document Interaction]. |
| Indicator | 50010040 | Macro Analyzer | Suspicious Office Excel  4.0 Macro | Suspicious Office Excel 4.0 macro detected. |
| Indicator | 50010050 | Macro Analyzer | Suspicious File System Activity Macro | Suspicious Office macro detected [File System Activity]. |
| Indicator | 50010060 | Macro Analyzer | Suspicious Out of Document Interaction Macro | Suspicious Office macro detected [Out-Of-Document Interaction]. |
| Indicator | 50020010 | File Type Discoverer | Suspicious Fake File | Suspicious fake file [Extension does not match file structure] detected in the artifact. |
| Indicator | 50020020 | File Type Discoverer | Suspicious Unknown File | Unknown file [Data file or unidentified file type] detected in the artifact. |
| Indicator | 50020110 | File Type Discoverer | Suspicious Executable File | Executable file detected in the artifact. |
| Indicator | 50020120 | File Type Discoverer | Suspicious Script File | Script file detected in the artifact. |
| Indicator | 50040010 | Active Element | External Program Run Action | External Program Run Action detected in file {Filename}. |
| Indicator | 50050010 | JavaScript Analyzer | Dynamic code execution | Dynamic code execution detected in file {Filename}. |
| Indicator | 50060010 | Suspicious URL | Suspicious URL detected | Suspicious url detected in file {FileName}, URLs:  {SuspiciousUrlsList} |
| Indicator | 50065010 | Xml Bomb | Xml Bomb detected | Xml Bomb detected. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Event Code** | **Sub- Category** | **Event Name** | **Event Description** |
| Indicator | 50070050 | Suspicious File Structure | Suspicious File Structure | Suspicious structure detected in file {FileName} |
| Indicator | 50075050 | Svg Bomb | Svg Bomb detected | Svg Bomb detected. |
| Indicator | 50090200 | Validate Signature | Validate Signature Failed | Signature Validation for file  {FileName} failed. |
| File Process | 60020010 | File Process | Publish Complete | File {FileName} published. |
| File Process | 60020020 | File Process | Publish Original Complete | File {FileName} original published. |

# Getting Service Information

**GET https://<*votiro\_appliance*>/disarmer/api/disarmer/v4/about**

Generates a file that details the API version and Votiro Cloud version of the system.

## Request Data

### Request Header Parameters

Request parameters are case sensitive.

**Table 17 Request Header Parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Description** | **Type** | **Required/Optional** |
| Authorization | Bearer <token> is used for authentication | string | Required |

### Request Example

GET https://api.votiro.com/disarmer/api/disarmer/v4/about Authorization: "Bearer <token>"

## Response Data

### Response Parameters

**Table 18 Response Parameters**

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Description** | **Type** |
| ApiVersion | The Votiro Cloud for Web Applications version | string |

### Response Example

"Votiro Cloud for Web Applications Ver: 4"

# Appendix A Sample Code - Sync-upload

To manage sync-upload requests in your environment, optional content changes to the file can be made.

using System; using System.IO;

using System.Net.Http;

using System.Net.Http.Headers; using System.Threading.Tasks; namespace ApiClientSample

{

static class Program

{

static void Main()

{

string disarmerAddress = "https://support- va/disarmer/api/disarmer/v4/upload-sync"; **//Reference 1**

string bearerToken =

"eyJhbGciOiJSUzI1NiIsImtpZCI6IkIwQTVFNEZFMDI5QjA3RDhCMzkw RTFFRkYyRjQ1ODZGMTQzODUwQjciLCJ0eXAiOiJKV1QifQ.eyJ1bmlxdW VfbmFtZSI6Im9tcml0ZXN0aW5ncG9zdG1hbiIsImdyb3Vwc2lkIjoiVm9 0aXJvSW50ZXJuYWxTZXJ2aWNlcyIsInJvbGUiOiJBZG1pbmlzdHJhdG9y IiwianRpIjoiNjI5OWVmMjItNDk2YS00M2Y5LWFmNDAtMjAzZDQyNTRlN GMwIiwibmJmIjoxNTk1MTQyNjc0LCJleHAiOjE4ODAxMzk2MDAsImlhdC I6MTU5NTE0MjY3NH0.TCheBCwie4heCf4v8cIOJ-

aT9gbVYuymvFPQoloQWUet5xyp08setMk8pTCPIgF3hWfhgo0MU22EVAH Zn506oFGF7KUeNQk2LAQMFqXaNUG1b3D2Xlmn5PNG-GVxvWbageqXC- 5bDtXAsPV0QFjV0nl0tYXyKnWIgmbXErgbXzCiRFhrDeEew1FuvW\_ VU6HEH6sCdkiGlGnL0Q\_-O5vdOqKWk5WUFRyT2S5VR5rxO\_ ezWKLfMTJXPUTJl2sBDLiuk\_ qLmWXep7LUy6fzuSPScEsWqShpWT6fl2BEpSeqmItVjMaLOVUN8KhKgSk TTzACtAGa8zWuwncJ0PdmIXTKUg"; **//Reference 2**

string filePath = @"C:\Users\omri.matari\Downloads\virtual-systems- datasheet.pdf"; **//Reference 3**

UploadFile(filePath, bearerToken, disarmerAddress).Wait ();

}

private static async Task UploadFile(string filePath, string bearerToken, string disarmerAddress)

{

using (Stream fileStream = File.OpenRead(filePath))

{

var formData = new MultipartFormDataContent

{

{

new StreamContent(fileStream), "file",

Uri.EscapeDataString(Path.GetFileName(filePath))

//Support spaces + any non-english characters in FileName

},

{

new StringContent("{\"PolicyName\":\"Default Policy\",\"ChannelType\":\"FileConnector\",\"Chann elId\":\"30acc6eb-16d9-4133-ae43- 0f5b6d40a318\",\"ChannelName\":\"API\"}"), **// Reference 4**

"properties"

}

};

using (formData)

{

using (var client = new HttpClient())

{

client.DefaultRequestHeaders.Authorization = new AuthenticationHeaderValue("Bearer", bearerToken);

HttpResponseMessage httpResponseMessage = await client.PostAsync(disarmerAddress, formData)

.ConfigureAwait(false); httpResponseMessage.EnsureSuccessStatusCode();

string result = await httpResponseMessage.Content.ReadAsStringAsync()

.ConfigureAwait(false); Console.WriteLine(result);

}

}

}

}

}

}

**Table 19 Sync-upload Parameters**

|  |  |  |
| --- | --- | --- |
| **Reference** | **Parameter** | **Description** |
| 1 | disarmerAddress | This is the address of your virtual appliance.  Change the address used in the file to match your installation address.  In the code example, change **support-va** to the name of your VA. |
| 2 | bearerToken | Change the Token to provide authentication to Votiro Cloud. |
| 3 | filePath | Set the file path to the area where download files will be located in your environment. |
| 4 | PolicyName | Define the policy, changing the name.  Additional fields for changing settings for are (optional):   * Channel Name * Channel ID   **Note**  Channel Type must remain set as "FileConnector". |

# Appendix B Votiro API Postman Collection

{

"info": {

"\_postman\_id": "c0e3ca52-5f6b-4cec-a7c7-bf9f9f6cc678", "name": "Votiro SaaS API Customer Version",

"schema": "https://schema.getpostman.com/json/collection/v2.1.0/colle ction.json"

},

"item": [

{

"name": "UPLOAD FILE:

https://prod.us.paralus.votiro.com/disarmer/api/Disarmer/ v4/upload",

"request": {

"auth": {

"type": "bearer", "bearer": [

{

"key": "token",

"value": "",

"type": "string"

}

]

},

"method": "POST", "header": [

{

"key": "Properties", "value": "

{\"ChannelType\":\"FileConnector\",\"ChannelId\":\"3 0acc6eb-16d9-4133-ae43- 0f5b6d40a318\",\"ChannelName\":\"Postman\",\"PolicyN ame\":\"API\"}",

"type": "text", "disabled": true

},

{

"key": "Authorization", "value": "",

"type": "text", "disabled": true

}

],

"body": {

"mode": "formdata", "formdata": [

{

"key": "file",

"type": "file",

"src": []

},

{

"key": "properties", "value": "

{\"ChannelType\":\"FileConnector\",\"ChannelId\":\ "30acc6eb-16d9-4133-ae43- 0f5b6d40a318\",\"ChannelName\":\"Postman\",\"Polic yName\":\"API\"}",

"type": "text"

}

]

},

"url": {

"raw": "https://prod.us.paralus.votiro.com/disarmer/api/Disarm er/v4/upload",

"protocol": "https",

"host": [ "prod.us.paralus.votiro.com"

],

"path": [ "disarmer", "api", "Disarmer", "v4",

"upload"

]

}

},

"response": []

},

{

"name": "UPLOAD-SYNC FILE:

https://prod.us.paralus.votiro.com/disarmer/api/Disarmer/v4

/upload-sync", "protocolProfileBehavior": {

"disabledSystemHeaders": {}

},

"request": {

"auth": {

"type": "bearer", "bearer": [

{

"key": "token",

"value": "",

"type": "string"

}

]

},

"method": "POST", "header": [

{

"key": "ContextIdentifier", "type": "text",

"value": "Postman", "disabled": true

},

{

"key": "Properties",

"type": "text", "value": "

{\"ChannelType\":\"FileConnector\",\"ChannelId\":\"3 0acc6eb-16d9-4133-ae43- 0f5b6d40a318\",\"ChannelName\":\"Postman\",\"PolicyN ame\":\"API\"}",

"disabled": true

},

{

"key": "Authorization", "type": "text",

"value": "", "disabled": true

}

],

"body": {

"mode": "formdata", "formdata": [

{

"key": "file",

"type": "file",

"src": []

},

{

"key": "properties", "value": "

{\"ChannelType\":\"FileConnector\",\"ChannelId\":\ "30acc6eb-16d9-4133-ae43- 0f5b6d40a318\",\"ChannelName\":\"Postman\",\"Polic yName\":\"API\"}",

"type": "text"

}

]

},

"url": {

"raw": "https://prod.us.paralus.votiro.com/disarmer/api/Disarm er/v4/upload-sync",

"protocol": "https", "host": [

"prod.us.paralus.votiro.com"

],

"path": [ "disarmer", "api", "Disarmer", "v4",

"upload-sync"

]

}

},

"response": []

},

{

"name": "GETSTATUS:

https://prod.us.paralus.votiro.com/disarmer/api/disarmer/v4

/status/[ItemID]", "protocolProfileBehavior": {

"disableBodyPruning": true, "disabledSystemHeaders": {

"accept-encoding": true, "connection": true

}

},

"request": {

"auth": {

"type": "bearer", "bearer": [

{

"key": "token",

"value": "",

"type": "string"

}

]

},

"method": "GET",

"header": [], "body": {

"mode": "formdata",

"formdata": []

},

"url": {

"raw": "https://prod.us.paralus.votiro.com/disarmer/api/disarm er/v4/status/[ItemID]",

"protocol": "https", "host": [

"prod.us.paralus.votiro.com"

],

"path": [

"disarmer", "api", "disarmer", "v4",

"status",

"[ItemID]"

]

}

},

"response": []

},

{

"name": "REPORT:

https://prod.us.paralus.votiro.com/disarmer/api/disarmer/v4

/report/[ItemID]", "protocolProfileBehavior": {

"disableBodyPruning": true, "disabledSystemHeaders": {

"accept-encoding": true, "connection": true

}

},

"request": {

"auth": {

"type": "bearer", "bearer": [

{

"key": "token",

"value": "",

"type": "string"

}

]

},

"method": "GET",

"header": [], "body": {

"mode": "formdata", "formdata": [

{

"key": "",

"value": "d15ebe79-adc1-43d8-afc8- 7588c8779f79/report",

"type": "text"

}

]

},

"url": {

"raw": "https://prod.us.paralus.votiro.com/disarmer/api/disarmer

/v4/file/report/[ItemID]", "protocol": "https", "host": [

"prod",

"us", "paralus", "votiro", "com"

],

"path": [ "disarmer", "api", "disarmer", "v4",

"report",

"[ItemID]"

]

}

},

"response": []

},

{

"name": "GETFILE:

https://prod.us.paralus.votiro.com/disarmer/api/disarmer/v4

/download/[ItemID]", "protocolProfileBehavior": {

"disableBodyPruning": true

},

"request": {

"auth": {

"type": "bearer", "bearer": [

{

"key": "token",

"value": "",

"type": "string"

}

]

},

"method": "GET",

"header": [], "body": {

"mode": "formdata", "formdata": [

{

"key": "",

"value": "ccf9c4a7-d350-45e5-ab07-99b66ec355e0", "type": "text"

}

]

},

"url": {

"raw": "https://prod.us.paralus.votiro.com/disarmer/api/disarm er/v4/download/[ItemID]",

"protocol": "https", "host": [

"prod",

"us", "paralus", "votiro", "com"

],

"path": [ "disarmer", "api", "disarmer", "v4",

"download", "[ItemID]"

]

}

},

"response": []

}

],

"event": [

{

"listen": "prerequest", "script": {

"type": "text/javascript", "exec": [

""

]

}

},

{

"listen": "test", "script": {

"type": "text/javascript", "exec": [

""

]

}

}

]

}