VOTIRO

Votiro Disarmer Knowledge Base User Guide

February 2022

Copyright Notice

www.votiro.com

Contents

1 Changing the CA Certificate

1.1 Introduction

CA Certificates are used as the HTTPS security layer to secure communications across computer networks when using applications.

The domain name of your Votiro Disarmer appliance is used in the CA Certificate, binding the address to the certificate, enabling a secure connection. An example of an appliance address is *https://prod.paralus.votiro.com*.

The CA Certificate used with your Votiro Disarmer appliance must be a *.pem* and *.key* pair. You can convert the format of your CA Certificate using SSL Certificate software, for example OpenSSL.

1.2 Solution

1.2.1 Converting a CA Certificate

To convert a CA Certificate in *.pfx* format with password *Pa$$w0rd* to a *.pem* and *.key* pair, use the following OpenSSL commands:

```
openssl pkcs12 -in /<path-to-certificate>/certificate.pfx -out
/<path-to-certificate>/certificate.pem -nodes -passin
pass:<Pa$$w0rd>
```

```
openssl pkey -in /<path-to-certificate>/certificate.pem -out
/<path-to-certificate>/certificate.key
```

1.2.2 Applying CA Certificate to Kubernetes Cluster

To apply the *.pem* and *.key* to your Kubernetes cluster, use the following commands:

```
kubectl delete secret traefik-cert
```

```
kubectl create secret tls traefik-cert --key=/<path-to-
certificate>/certificate.key --cert=/<path-to-
certificate>/certificate.pem
```

2 Changing the Kibana Password

2.1 Introduction

Support requested this be included in VA documentation, then said to hold-off. Also awaiting context.

2.2 Solution

To change the Kibana Password:

1. Go to https://www.askapache.com/online-tools/htpasswd-generator/.
2. Enter details:
   a. Select **Encryption Algorithm** option **md5**.
   b. Select **Authentication Scheme** option **Both**.
3. Click **Generate HTPPSWD**.

   An output string is generated. For example,

   admin:$apr1$tdea7nbo$K0V/aYnScSwu27yH29IlM.
4. Go to https://www.base64encode.org/.
5. Enter the string from Step 3, click **Encode**.

   An output string is generated. For example,

YWRtaW46JGFwcjEkZTlpanlyZGckd3FvVEZCQldJZDRxMVhZY1ZSejhXLg==
6. Login to Node1 and type: *kubectl edit secret kibana-auth*.
7. Modify the file. Click **Insert**.
8. Navigate to **Auth**. Replace the existing string with the one generated in Step 5.
9. Login to Kibana with the new credentials.

3 Email Arrival Is Delayed

3.1 Introduction

This page details why the arrival of emails may be delayed and remediation actions to solve this issue.

3.2 Symptoms

- Mails arrive late in days - delayed arrival
- No errors in Votiro logs
- No specific high resource consumption

3.3 Solution

This situation might be related to Message throttling.

Get information of the Edge Connector:

```
Get-ReceiveConnector | Format-List
Name,Connection*,MaxInbound*,MessageRate*,TarpitInterval
```

3.4 Expected result

Before:

Name : Default Connector Name

ConnectionTimeout : 00:05:00

ConnectionInactivityTimeout : 00:01:00

MaxInboundConnection : 5000

MaxInboundConnectionPerSource : 20

MaxInboundConnectionPercentagePerSource : 2

MessageRateLimit : 600

MessageRateSource : IPAddress

TarpitInterval : 00:00:05

>The configuration allows maximum of 20 simultaneous connections from a single IP.

Action:

Change the parameters using syntax:

```
Set-ReceiveConnector -Identity <Put the Identity name> -
ConnectionTimeout 00:10:00)
```

After:

Name: Default Connector Name

ConnectionTimeout: 00:10:00

ConnectionInactivityTimeout: 00:01:00

MaxInboundConnection: 5000

MaxInboundConnectionPerSource: 50

MaxInboundConnectionPercentagePerSource: 5

MessageRateLimit: 600

MessageRateSource: IPAddress

TarpitInterval: 00:00:05

4 How to Obtain a Votiro Disarmer License Key

4.1 Introduction

To obtain a permanent Votiro Disarmer license key you must perform the following steps:

1. Create a MachineStats.xml file.
2. Send the MachineStats.xml file to Votiro Support.
3. Receive a license file from Votiro Support.
4. Save to license file in the appropriate folder.

The MachineStats.xml file contains information on the machine that Votiro Disarmer is installed on, such as OS version, memory size and number of cores.

Votiro Support generate a corresponding license key for Votiro Disarmer, which is required for product activation.

4.2 Obtaining a License key

Procedure

1. Using the link you received from Votiro Support, download the MachineStats.zip file to the Votiro Disarmer server.
2. Extract the zip file.
3. Open CMD with Administrator privileges.
4. Navigate to the MachineStats folder.
5. Run the following command:

   ```
   MachineKeyTool.exe -o c:\
   [FullFileOutputPath]\MachineStats.xml
   ```

   A MachineStats.xml file is created in the chosen destination folder.
6. Send the MachineStats.xml file to Votiro Support via email or via Votiro's Customer Portal.

   Votiro Support will provide a license file (VotiroLicense.xml).
7. Place the license file in the SDS-WS installation root folder. The default location is:

   C:\Program Files\Votiro\SDS Web Service.

4.3 Verifying Votiro Disarmer Activation

To verify that Votiro Disarmer has been successfully activated, navigate to the API log file (the default location is:

C:\Program Files\Votiro\SDS Web Service\Logs\API).

The following is an example of output that should appear in the log:

```
4880-1 | 17/07/2018 16:16:00.208 | 2 Info | License was
validated successfully, license details.
```

> **Note**
> It can take up to 30 minutes for the information to appear in the API log.

4.4 Renewing Your Votiro License Key

To renew your license key contact Votiro Support for a replacement VotiroLicense.xml file. Provide a new MachineStats.xml file if the OS version, memory size or number of cores in your environment have changed since receiving the last VotiroLicense.xml file.

> **WARNING!**
> Replace your license key when renewal is required. Votiro will continue running for a grace period after the renewal date, providing time for you to receive and install the new license key.

At the expiration of the grace period Votiro Disarmer services are stopped and files will not be sanitized.

5 How to Set a Profile for a Domain Group

In the Admin (Management Interface), there is an option to add a Profile for a specific Domain group.

This allows flexibility with Policy enforcement for users in diverse groups.

Instructions:

1. Open the Admin Interface
2. Select Profiles tab
3. Select Add new profile
4. Check the checkbox near: Verify against Active Directory
5. In Profile name: type the name of the domain group
6. Press on Add

6 Message Size Limits in Exchange

6.1 Introduction

This article describes why emails may not reach their destination or appear in sanitization log files.

6.2 Symptoms

The email (eml) size may increase as a result of the sanitization process. The size of the email message may then exceed the size limit set in Exchange Server.

6.3 Solution

To avoid blocked emails in Exchange servers due to message size limitations, follow this TechNet guide:

https://technet.microsoft.com/en-us/library/bb124345(v=exchg.160).aspx

6.4 Limitations

Organizational limits apply to Exchange 2016 servers, Exchange 2013 Mailbox servers, and Exchange 2010 Hub Transport servers that exist in your organization. Organizational limits that you configure on Edge Transport servers are applied to the local server.

By default the "Maximum size of a message received" is set to 10MB.

If Exchange is your responsibility change this parameter according to your organization policy. If Exchange is part of the Votiro Disarmercloud solution, contact Votiro Support.

7 Unsanitized Due to Timeout

7.1 Introduction

This article describes why files may not be sanitized due to a timeout limit being reached.

7.2 Symptoms

In some cases the process of sanitizing a complex email with file attachments may take longer then expected. In such cases the maximum processing time set in the Email-Connector configuration file is reached and the process will timeout.

In such cases, the email recipient receives the original email with the subject field changed by the addition of ***Unsanitized*** at the beginning of the original subject.

7.3 Solution

1. Open the last \ relevant Email-connector log installed on the Edge server - the logs are located by default under: C:\Program Files\Votiro\SDS-Connector\Logs.
2. Open the log with atext editor and search for "Unsanitized".
3. You should find the following:

   "UnExpected error. Passing unsanitized email."

   Just above this row you will see:

   "result is TimeOut.".
4. Next, open and browse the following XML:

   C:\Program Files\Votiro\SDS-Connector\WebApiHandlerConfig.xml.

   In the XML you will find 2 timeout values:

   - WebApiTimeoutInMS - The total length of time the SDS-Connector waits for a sanitization to be completed, in milliseconds.

     Value Range: 5000 to 180000000 Default value is 90000. This is the value you should change.
   - WebRequestTimeoutInMS - The length of time the SDS-Connector waits per API request from the SDS-WS, in milliseconds.

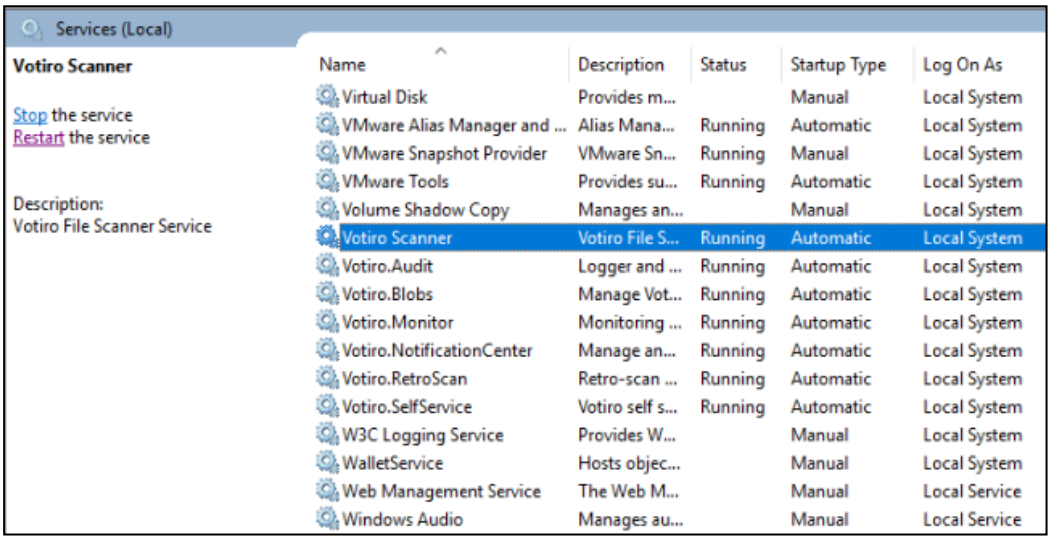
     Value Range: 5000 to 180000000, Default value is 60000.
5. Increase the value of "WebApiTimeoutInMS". Save and Close the XML file.
6. Restart the MSExchangeTransport service.

8 Votiro Disarmer Monitoring Guidelines

This article describes services installed as part of the Disarmer product for you to monitor.

To check that these services are all active and running:

1. Navigate to the Windows Services Screen: Windows > Administrative Tools > Services.
2. Locate the Votiro Disarmer Windows Services for Disarmer Engine and the Votiro Management Platform Windows Services for Disarmer Management.



3. For each of these services, ensure that the following details are displayed:
   - Status is Running
   - Startup Type is Automatic.

> **Note**
> It can take up to 30 minutes for the information to appear in the API log.

8.1 Disarmer Services - Votiro Services

Service	Description
Votiro Scanner	The Votiro Scanner service is located at: [installation_path]\Votiro\Votiro.Malware.Scanner. The Votiro Scanner service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\Votiro.Malware.Scanner\Logs.

Service	Description
Votiro.Sanitization.API	The Votiro.Sanitization.API service is located at: [instalation_ path]\Votiro\SDS Web Service. The Votiro.Sanitization.API service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\SDS Web Service\Logs\API.
Votiro.SNMC	The Votiro.SNMC service is located at: [installation_ path]\Votiro\SDS Web Service. The Votiro.SNMC service maintains a log file for all activity. The log file is located at: [installation_ path]\Votiro\SDS Web Service\Logs\SNMC. The SNMC manages n sanitization nodes. Nodes have log files that are located at: [installation_path]\Votiro\Logs\SNMC\1 ... n
Votiro.Sandbox	The Votiro.Sandbox service is located at: [instalation_ path]\Votiro\Sandbox. The Votiro.Sandbox service maintains a log file for all activity. The log file is located at: [installation_ path]\Votiro\Sandbox\Logs.

Additional health indicators:

- C:\ Drive space
- CPU load
- Memory Usage
- Uptime
- IIS Admin Service

8.2 Disarmer Management Dashboard - Votiro Services

Service	Description
Votiro.Blobs	The Votiro.Blobs service is located at: [installation_ path]\Votiro\BlobStorage. The Votiro.Blobs service maintains a log file for all activity. The log file is located at: [installation_ path]\Votiro\BlobStorage\Logs.
Votiro.NotificationCenter	The Votiro.NotificationCenter service is located at: [installation_ path]\Votiro\NotificationCenter. The Votiro.NotificationCenter service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\NotificationCenter\Logs.
Votiro.RetroScan	The Votiro.RetroScan service is located at: [installation_ path]\Votiro\RetroScan. The Votiro.RetroScan service maintains a log file for all activity. The log file is located at: [installation_ path]\Votiro\RetroScan\Logs.
Votiro Scanner	The Votiro Scanner service is located at: [installation_ path]\Votiro\Votiro.Malware.Scanner. The Votiro Scanner service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\ Votiro.Malware.Scanner\Logs.

Service	Description
Votiro.Audit	The Votiro.Audit service is located at: [installation_path]\Votiro\Audit. The Votiro.Audit service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\Audit\Logs.
Votiro.Monitor	The Votiro.Monitor service is located at: [installation_path]\Votiro\Monitor. The Votiro.Monitor service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\Monitor\Logs.
Votiro.SelfService	The Votiro.SelfService is located at: [installation_path]\Votiro\PpfSelfService. The Votiro.SelfService service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\PpfSelfService\Logs.
Votiro.Scheduler	The Votiro.Scheduler is located at: [installation_path]\Votiro\Scheduler. The Votiro.Scheduler service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\Votiro\Scheduler\Logs.
Elasticsearch	The Elasticsearch service is located at: C:\Program Files\Elastic\ElasticSearch. The Elasticsearch service maintains a log file for all activity. The log file is located at: C:\ProgramData\Elastic\Elasticsearch\logs.

Additional health indicators:

- C:\ Drive space
- CPU load
- Memory Usage
- Uptime
- IIS Admin Service

9 Introduction

When using OpenJDK with Votiro Management the version installed must support ElasticSearch. Currently only certain versions of Elasticsearch support certain versions of Oracle/OpenJDK 9, 10, 11, 12, 13.
Oracle/OpenJDK/AdoptOpenJDK 1.8.0 seems to be support for all versions as indicated by ElasticSearch Java Support Matrix page.

We recommend you check the Support Matrix.

10 Solution

10.1 Pre-requisites

10.1.1 Downloading the Installer

Download the OpenJDK installer, we recommend using OpenJDK1.8.0.242.

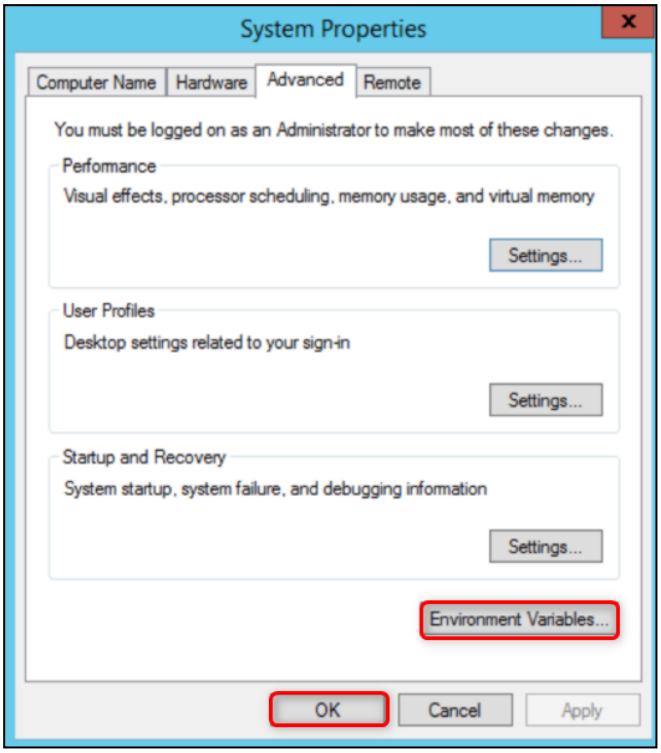
To download the Red Hat build of OpenJDK, you need to create your own Red Hat ID, click https://developers.redhat.com/download-manager/file/java-1.8.0-openjdk-1.8.0.242-3.b08.redhat.windows.x86_64.zip.

10.1.2 Procedure

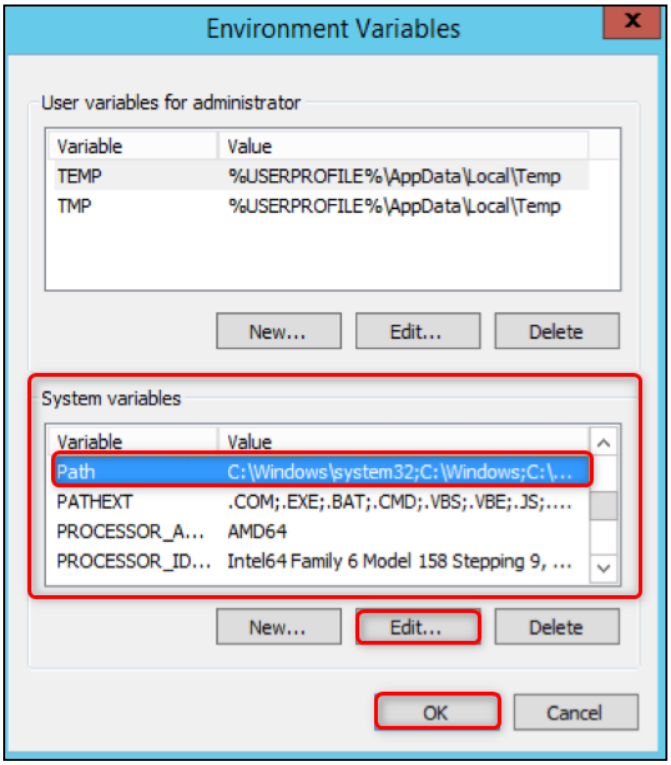
This procedure includes instructions and verification checks to ensure...

1. Before you start migrating to OpenJDK send files for CDR.
2. Verify that your Votiro Management is working as expected by downloading Original and Sanitized files from **Incident Manager**.
3. Install OpenJDK1.8.0.242. You can set the installation directory to **C:\Program Files\OpenJDK\java-1.8.0.-openjdk-1.8.0.242-3** or a directory name of your choice.
4. When the installation has successfully completed, go to your **Windows Start Menu**.

a. Search for and select **Advanced System Settings**.



b. Search for and select **Advanced System Settings**.



c. Select **Environment Variables**, then select **OK**.

5. In the **System variables** section, locate and select **Path**, then select **Edit**.
6. Copy the whole string to Notepad (or similar) and save the file as **Original.txt**. This will be your backup.
7. Duplicate the file **Original.txt** and name the file **OpenJDK.txt**.
8. Edit the **OpenJDK.txt** file.
    a. You will see **C:\ProgramData\Oracle\Java\javapath;**. The semicolon points to the Oracle Java installer.
    b. Replace **C:\ProgramData\Oracle\Java\javapath;** with **C:\Program Files\OpenJDK\java-1.8.0.-openjdk-1.8.0.242-3\bin;**.
    c. Copy the new string.
    d. Save the file **OpenJDK.txt**.
9. Return to your **Environment Variables** window.
    a. Select Path, then select **Edit**.
    b. Replace the entire string with the string you copied from **OpenJDK.txt**.
    c. Select **Save**.
10. Reboot your server.
11. Once your server is up, open a command prompt and run the following command to verify java is running:

    C:\> java -version

12. Check that all your Votiro services on Votiro Management are running correctly by sending files for CDR. It should perform exactly as before. Verify that your Votiro Management is working as expected by downloading Original and Sanitized files from **Incident Manager**. Verify statistics are updated on the dashboard.