Installing ClamAV Antivirus Software

Agiloft can be used with ClamAV antivirus software to scan attached files in a knowledgebase. This topic describes how to set up antivirus detection in Agiloft, using the ClamAV open source antivirus toolkit. When implemented, the antivirus protection only scans attached files and has no effect on the rest of the operating system. For more information, see www.clamav.net.

There are two possible ways to implement ClamAV with Agiloft:

- Using `CommandLineVirusDetector` command line utility.
- Using `SocketVirusDetector` to go through a socket connection.

If you have any other antivirus software installed, add its installation directory to the ClamAV exception list.

- When using `SocketVirusDetector`, ClamAV must be run as a service.
- ClamAV signatures are updated daily at 8pm server time.

If you're using a version of Agiloft prior to 2019_01, make modifications to the file located at `D:\Agiloft\jboss\bin\ewjbossrun.bat` instead of `D:\Agiloft\wildfly\bin\standalone.conf.bat` in the Setting Up Virus Detection sections.

Exceptions

The ClamAV anti-virus is set up by default to exclude the Agiloft TMP directory (for example, `C:\Agiloft\tmp`), which is the preferred setting. The TMP directory is used by Agiloft for storing temporary data, such as data for an import, and running anti-virus scans on that directory would severely impact performance.

Additionally, if you have any other antivirus software installed, you should add its installation directory to the ClamAV exception list. This cannot be done by default and must be done manually.

Installing ClamAV

First, install ClamAV.

1. Download ClamAV during initial Agiloft installation, or from the following location: https://www.clamav.net/downloads
2. Install it to a directory in your instance of Agiloft, for instance at `D:/Agiloft/ClamAV`.
3. Create a new directory to install updates, for instance at `D:/Agiloft/ClamAV/database`.
4. Copy the example config files from the `conf_examples` directory to install the root directory.
5. Make the following changes to the `clamd.conf.example` file:
    a. Rename the file from `clamd.conf.example` to `clamd.conf`.
    b. Comment out or delete the Example instruction.
    c. The PidFile should be at `D:/Agiloft/ClamAV/clamd.pid`.
    d. The LogFile should be at `D:/Agiloft/ClamAV/clamd.log`.
    e. The database directory should be at `D:/Agiloft/ClamAV/database`.
    f. The TCPSocket should be 3310.
    g. The TCPAddr should be 127.0.0.1.
6. In the `freshclam.conf.sample` file, make the following changes:
    a. Rename the file from `freshclam.conf.sample` to `freshclam.conf`.
    b. Comment out or delete the Example instruction.
7. Run `freshclam.exe` and update the virus database.

Setting up Virus Detection with ~~CommandLineVirusDetector~~

`CommandLineVirusDetector` has two parameters: `command line` and `path to temp directory` where files uploaded to the Agiloft knowledgebase are stored. To add additional parameters, change the file located at `D:\Agiloft\wildfly\bin\standalone.conf.bat`

1. Run JBoss AS with the following parameters:
   - DAntiVirusUtils.virus-detector-class=com.supportwizard.utils.av.clam.CommandLineVirusDetector
   - DCommandLineVirusDetector.command-line="D:/Agiloft/ClamAV/clamscan.exe"
   - DCommandLineVirusDetector.temp-dir="D:/Agiloft/tmp/av"

Setting up Virus Detection with SocketVirusDetector

SocketVirusDetector has three parameters: `host`, `port` and `socket timeout`. To add additional parameters, change the file located at `D:\Agiloft\wildfly\bin\standalone.conf.bat`

1. Run ClamAV as a service, typically `D:\Agiloft\ClamAV\clamd.exe`.
2. Run JBoss AS with the following parameters:
    - -DAntiVirusUtils.virus-detector-class=com.supportwizard.utils.av.clam.SocketVirusDetector
    - -DSocketVirusDetector.host=127.0.0.1
    - -DSocketVirusDetector.port=3310
    - -DSocketVirusDetector.timeout=500