DRAFT

Signature configuration UI

User Manual

Contents

DRAFT

ClamAV for Windows - Signature configuration UI - User Manual,
© 2010 Sourcefire, Inc.
Authors: Török Edvin
This document is distributed under the terms of the GNU General Public License v2.

Clam AntiVirus is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2 of the License.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

ClamAV and Clam AntiVirus are trademarks of Sourcefire, Inc.

DRAFT

CHAPTER 1
Overview

ClamAVallows users to deploy and use their own (or third party) virus signatures in addition to the official virus signatures. The virus signature database updater (`freshclam`) can also be adapted to the user's environment.

This is usually done by editing the configuration file `freshclam.conf`, and copying the custom signatures to the database directory.

However **ClamAV for Windows** protects the database directory against changes, even if those changes are attempted by a user with *Administrator* privileges. A new tool is needed to make these changes: **Signature configuration UI** (SigUI).

1.1. Features

Using *SigUI* an *Administrator* can:

- Configure `freshclam` to use a proxy
- Configure which mirror `freshclam` should use
- Configure updates of custom signatures by `freshclam`
- Manually copy virus signature databases to **ClamAV**'s database directory
- Deploy an existing `freshclam.conf` [1] to multiple machines

1.2. Using SigUI

1.2.1. Launching the application

The application can be launched from the *Start Menu*: Start → All Programs → ClamAV for Windows → SigUI 

[1] created using SigUI

DRAFT

Or you can navigate to the installation directory of **ClamAV for Windows**[1], and from the `clamav` subfolder launch `sigui.exe`:

In either case you must run this program with administrative privileges. On *Windows Vista* and later you will get the UAC popup to grant Administrator privileges to the application [2]. On earlier versions you will need to login as `Administrator`.

1.2.2. How it works

When changing `freshclam` settings via the UI, it first verifies that the settings are syntactically correct, and saves them in `freshclam.conf`.

When installing custom signatures, `SigUI` verifies that **ClamAV**can successfully load the databases, and install only those that are successfully loaded.

Any changes you make will not take effect immediately, but only the next time the databases are reloaded. This usually happens each hour. You can reload the databases immediately by opening the **ClamAV for Windows** user interface [3], and clicking on **Update Now**.

DRAFT

[1] `C:\Program Files\ClamAV for Windows` by default

[2] If you are running as a user that has Administrator privileges, this is a simple "I Allow/Continue" style popup, otherwise it asks you for a login and password of a user with Administrator privileges

[3] from the tray, or the desktop

CHAPTER 2
Usage examples

2.1. Configuring a proxy

Freshclam by default attemps to connect to the Internet directly. If you can only access the Internet by using a proxy, then you should configure the proxy using SigUI.

If you have already configured a system wide proxy setting, then easiest is to just press the *Retrieve system proxy settings* button on the *Updater configuration* tab. This will retrieve the proxy settings from Internet Explorer, and display them in the *Proxy settings* section. If the settings are correct, click *Save settings*.

You can also manually input the proxy settings:

- Tick the *Proxy required for Internet access* checkbox
- Set the proxy server and port in the *Proxy server:* and *Proxy port:* fields
- If the proxy requires a username and password, then tick the *Authentication required* checkbox
  - Enter the username in the *Proxy username:* field
  - Enter the password in the *Proxy password:* field [1]
- Check that the settings are correct
- Click *Save settings*

To test whether the proxy settings work, click *Run freshclam to test configuration*. This will run freshclam, and display an error if it failed to connect through the proxy. See Section 3.3 for details.

[1] Note that the password will be saved as cleartext in freshclam.conf

DRAFT

2.2. Choosing a mirror

`Freshclam` by default uses the `database.clamav.net` mirror. Although this works well most of the time, you can get better download speeds by using a mirror from your country:

- Open SigUI
- Open the *Download Official Signatures from mirror* dropdown [1]
- Mirrors are of the form `db.XY.clamav.net`, where *XY* is your two-letter country-code
- Select the mirror corresponding to your country
- Click *Save settings*

You can also enter the hostname of the mirror you wish to use, instead of choosing one from the dropdown. This mirror can be a server on your own network too. See Section 2.4.

2.3. Deploying custom signature updates

In addition to the official virus signatures, you can use your own signatures, or signatures provided by third-parties. To deploy them you have these choices:

- Put your custom signatures on your own webserver. See Section 2.3.1
- Put your custom signatures on a network share. See Section 2.3.2
- Manually copy your custom signatures each time you change them. See Section 2.3.4
- Write and deploy a script that copies the signatures to a local drive, and runs SigUI in command-line mode. See Section 2.3.6

The signatures are not loaded in the running ClamAV immediately. See Section 3.5.

[1] On the *Updater configuration* tab, in the *Signature sources* section

DRAFT

2.3.1. Deploying your own signatures from a webserver

If you have written your own signatures and want to deploy them to multiple **ClamAV for Windows** installations on your network, then the easiest is to put the signatures on your webserver (in your LAN).

The custom signature can be in any format that ClamAV understands. See `http://www.clamav.net/doc/latest/signatures.pdf` section 3 "Signature formats" for details about the format. All the signature files, except CVD, are ASCII files. Both Unix (LF) and Windows-style (CR+LF) line-endings are accepted. CVD files are binary files though, so you should not modify them. The format of signatures is determined based on the database extension (in a case insensitive manner), so you must make sure to preserve the file's contents and extension when copying it. (You can safely rename the file, as long as you preserve the extension).

Since these files are not digitally signed [1], it is your responsibility to ensure that the signature files are not altered (by malware, etc.).

Deploying a new signature file is easy:

- Copy the signature to your webserver, at a location of your choice
- Open SigUI
- Click the *Add* button next to the *Custom signature URLs* section
- Enter the full URL to your new signature file
- Click OK.
- Click *Save settings*
- See Section 3.4 for details
- You can repeat this operation on each machine that has **ClamAV for Windows** installed, or you can automate it, see Section 2.3.6

2.3.2. Deploying your own signatures from a network share

This is similar to downloading a signature file from a webserver, see Section 2.3.1. Except you have to add an UNC path instead of an `http://` URL.

However **ClamAV for Windows** requires this UNC path to be readable by the SYSTEM account. Usually network shares, and network mapped drives are not accessible to this user. If you have made them accessible (it is out of scope for this document to discuss how), then you can of course use them in SigUI.

[1] Official `CVD` files are digitally signed

DRAFT

2.3.3. Deploying third-party signatures

If you want to deploy third-party signatures that are not in `CVD` format [1], you can do so with some additional steps:

- Download the third-party signatures to your server
- Check their integrity by comparing against the third-party supplied checksum and digital signatures. There usually are scripts to accomplish this
- Copy the signatures to your webserver, at a location of your choice
- Make sure you preserve the extension of the files, as the signature format is determined based on the extension
- Add the full URL path to these signatures to `freshclam.conf` using SigUI. See Section 3.4

Note that if you add third-party signatures memory usage will increase (depending on the complexity and size of the signatures), and performance may be different.

Note that the downloaded signature files will all be placed in the same directory. Hence you must make sure you don't have two URLs that, when downloaded, have the same filename. The UI will warn you if you try to do that[2].

2.3.4. Manually copying custom signatures to database directory

If you want **ClamAV** to use a custom signature, you just need to copy it to its database directory. However, as explained earlier in this document, that directory is protected against changes so you need to use SigUI to copy the databases.

This can be achieved by using the *Local signature management* tab:

- Click *Add*
- This will open the standard *Open file(s)* dialog
- Select the file(s) you want to add
- Click *Open*

[1] freshclam supports third-party signatures in CVD format, but there are no such signatures yet

[2] the two URLs with same filenames will just keep overwriting the same file

DRAFT

- The files will show up in the *New signatures* list

At this point the files haven't been installed yet. The databases currently installed can be seen in the *Installed signatures* list. By default you should see `main.cvd`,`daily.cvd`, and `bytecode.cvd` [1].

You want your new signatures to show up in the *Installed signatures*, so the next step is clicking on *Verify and Install signatures*. This will perform the following:

- Copy all the signatures to a (protected) temporary staging directory [2].
- Test the signatures by loading each one[3]. CVD files also have their digital signature checked.
- The signatures that pass verification are installed in the real database directory
- **ClamAV for Windows** will load them the next time it updates the database (usually once ah hour)
- If there are signatures that fail verification an error message will be shown, with details on why the signatures failed to load.

2.3.5. Removing signature files

If you want to remove one of your signatures, you can select the file in the *Installed signatures* list, and click *Delete*. This will erase the file from the disk! Note that you can delete the files automatically downloaded by `freshclam` too, but they will just reappear at the next update. The only file you can't delete is daily.cvd and daily.cld. The presence of one these files is essential to the proper operation of the **ClamAV** engine.

2.3.6. Automating signature and configuration file deployments on a network

The graphical mode of SigUI is useful for making local changes to `freshclam.conf` and the database directory. However if you want to automate the process (call it from a script), there is a commandline interface too:

- You must run it as Administrator user. Otherwise you get the UAC popup, which is not what you want in a script.

[1] Or .cld once they are updated. CVD files change into CLD files upon an update. Of course if the updater didn't run yet you won't see any files there

[2] `clamav\staging_dir` subdirectory

[3] Using `libclamav.dll` only, they are not loaded in the realtime engine

DRAFT

- If you want to copy signatures to the database directory:
  - Create a file `signatureslist` with the full path to the signatures you want to install, one on a line. Don't quote or escape the filenames, just write them as is.
  - Run:

    ```
    "C:\Program Files\ClamAV for Windows\clamav\SigUI.exe" -i
        <signatureslist
    ```

  - Another alternative is to pipe it the output of another program [1]:

    ```
    echo '<databasepath>' | "C:\Program Files\ClamAV for
       Windows\clamav\SigUI.exe" -i
    ```

  - SigUI will test each database by loading them, and prints progress messages to the standard output.
  - SigUI will print error messages on failed database loads to the standard error
  - The exitcode will be 0 if all signatures were successfully installed, and nonzero if some signatures failed to install

  Note that using `freshclam`'s support for custom signature URLs is usually a better solution, you will only need to deploy the modified `freshclam.conf`.

- Deploying a modified `freshclam.conf`:
  - Create a `freshclam.conf` on one machine with SigUI
  - Test it, see Section 3.3
  - Write a script to automatically invoke `SigUI.exe` on each machine on your network (for example using a logon script, or a `msi` installer)
  - Have it execute this command:

    ```
    "C:\Program Files\ClamAV for Windows\clamav\SigUI.exe" -w
        <new\_freshclam.conf
    ```

  - Alternatively you can pipe it the freshclam.conf:

    ```
    somecommand | "C:\Program Files\ClamAV for Windows\clamav
       \SigUI.exe" -w
    ```

  - SigUI will test the config file for syntactic correctness, and install it if it is valid

[1] Interactively entering the filenames from the commandprompt won't work

DRAFT

2.4. Setting up a local mirror

If you have a lot of ClamAV installations on your local network, then you can setup `freshclam` as described in the answer for *I'm running ClamAV on a lot of clients on my local network* at `http://www.clamav.net/lang/en/support/faq/faq-cvd/`. Once you've setup the local mirror you can configure it:

- Open SigUI
- Enter the hostname, or IP address of your local mirror in the *Download official signatures from mirror:* field
- Click *Save settings*
- Click *Run freshclam to test configuration.* See Section 3.3

Another option is to setup a caching proxy, and set ClamAV to use that. See Section 2.1.

DRAFT

DRAFT

CHAPTER 3
User interface

3.1. Updater configuration

When you open SigUI the *Updater configuration* tab is open, see Figure 3.1.

It has 2 sections:

3.1.1. Proxy settings

If *Proxy required for Internet access* is not ticked, then `freshclam` will connect directly to the internet.

If it is ticked, then the *server* and *port* fields, and *Authentication required* checkbox will be enabled.

If the *Authentication required* checkbox is ticked the *username* and *password* fields will be enabled too.

The *Retrieve system proxy settings* will attempt to retrieve the proxy settings from Internet Explorer, and fill the above fields.

See Section 2.1 for an example.

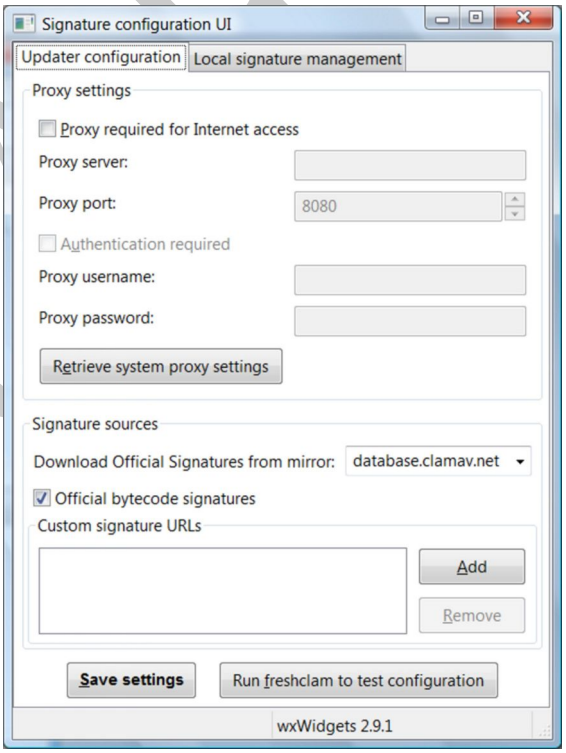

Figure 3.1: Updater configuration

3.1.2. Signature sources

Here you can configure what databases will `freshclam` automatically download.

DRAFT

Download Official Signatures from mirror allows you to choose the mirror that `freshclam` will use to download the virus databases. You can either enter a custom hostname, or select one from the list (preferably the one that matches your countrycode). See Section 2.2 for an example.

Official bytecode signatures is by default enabled. If you want to disable it, untick it. But you must be aware that you will miss some detections, or even bugfixes.

Custom signature URLs is a list of custom URLs that `freshclam` will download and install as new virus signature databases. You can use the *Add* and *Remove* buttons to manage the list. The list accepts `http://` URLs, or UNC pathes. See Section 2.3 for detailed examples.

3.1.3. Saving configuration and testing

Pressing the *Save settings* will validate all the fields on this tab, and save the settings to `freshclam.conf`. If there is anything wrong an error message will be shown.

Pressing the *Run freshclam to test configuration* will test whether the new `freshclam.conf` works as expected. If this results in error you should fix it, otherwise your custom databases won't be used.[1]

3.2. Local signature management

This tab allows you to manage the signatures installed in the database directory, see Figure 3.2.

There upper section, *New signatures* shows the signatures you are about to install, and the bottom section, *Installed signatures* shows the already installed signatures. You can manage the top list using the *Add* and *Remove* button (Add launches a standard *Open file* dialog).

The bottom list is managed by SigUI and `freshclam`. You can press *Verify and Install signatures* to validate and copy the signatures from the list above to the one below. Signatures are only copied after they have been verified as valid, an error is shown for malformed signatures. See Section 2.3.4 for an example.

[1] The official ones should still be downloaded correctly even in case of errors, unless freshclam.conf is very broken

DRAFT

The *Delete* button will delete the actual signatures files from disk, it should be used only if you know what you are doing (a confirmation message is shown prior to delete of course).

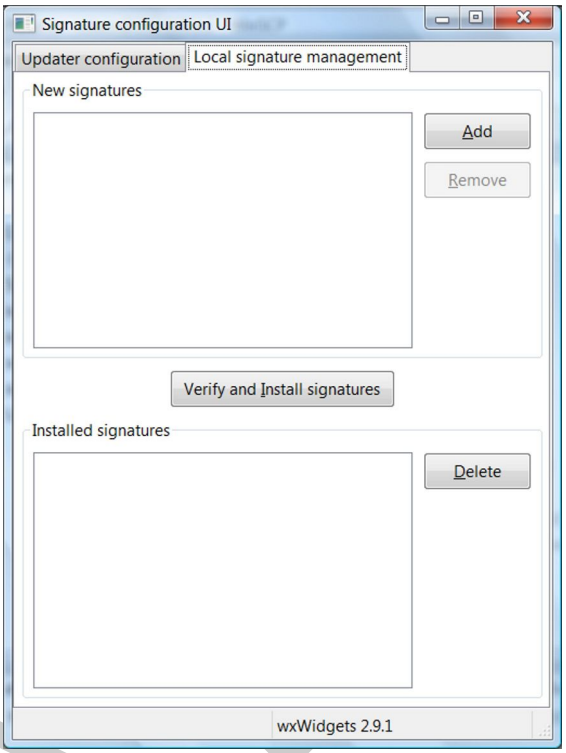

Figure 3.2: Local signature management

3.3. Run freshclam to test configuration

Pressing this button will launch `freshclam`, and opens a window to show its output, see Figure 3.3.

The output shows the progress of the update, and any error messages from `freshclam`. It is recommended that once you change `freshclam.conf`, by clicking *Save settings*, to test it by clicking on *Run freshclam to test configuration*.

The window has a button to forcefully terminate `freshclam`, but this should only be used if for some reason it hangs. Note that by default the timeout for connecting to a remote server is 30 seconds, so you should wait at least 30 seconds before terminating it.

Once `freshclam` finishes the button changes to a *Close window* button, that can be safely pressed to dismiss the window.

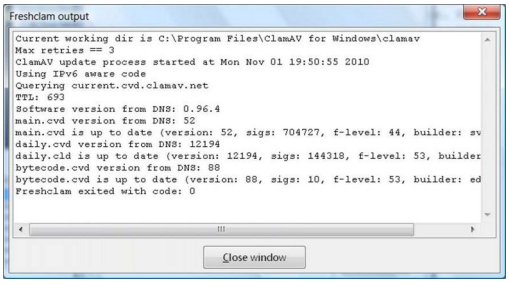

Figure 3.3: SigUI: Freshclam output window

3.4. Custom URLs

The *Custom signature URLs* section on the *Updater configuration* page allows you to add custom URLs.

DRAFT

Freshclam will automatically download these each time it updates the official signatures (usually once an hour).
If your webserver supports `If-Modified-Since` headers, it will only download the new database if it is newer than the already installed one.

Digital signatures are checked only for CVD signatures[1]. Freshclam automatically tests all signatures (for syntactic correctness) after downloading, but before installing them. If a signature file is malformed it is not installed and an error is logged.

Usage:

- Click Add to add a new URL, press OK when done
- If the URL is not in the correct format, an error message is shown. Correct the URL and press OK again.
- The new URL shows up in the *Custom signature URLs* section
- Add as many URLs as needed
- You can remove an URL by clicking the *Remove* button. **WARNING**: If the database was already downloaded it won't remove the downloaded signature file from the disk. See Section 2.3.5 on how to do that.
- Check that you entered the correct URLs.
- Click *Save settings*.
- Click *Run freshclam to test configuration* to make sure freshclam is able to correctly download the signatures. Freshclam will only install signatures that are in the syntactically correct. See Section 3.3

Note that the downloaded signature files will all be placed in the same directory. Hence you must make sure you don't have two URLs that, when downloaded, have the same filename. The UI will warn you if you try to do that. [2].

3.5. Update now

Any changes you make to `freshclam.conf` and the databases won't take effect immediately. They will take effect the next time the signatures are updated (usually

[1] because they are the only ones that contain such signatures
[2] the two URLs with same filenames will just keep overwriting the same file

DRAFT

once an hour). To reload the signatures immediately open the **ClamAV for Windows** user interface from the tray (or desktop icon), and click on *Update Now*. Once the database is updated, it will be reloaded as soon as the system is idle.

DRAFT

DRAFT

CHAPTER 4
Copyright and License

The Signature configuration UI is released under the GNU General Public License version 2.


```
Copyright (C) 2010 Sourcefire, Inc.

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License version 2 as
published by the Free Software Foundation.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston,
MA 02110-1301, USA.
```


DRAFT

DRAFT

Glossary

ClamAV Clam AntiVirus engine, see `http://www.clamav.net`. 3, 4, 7–9, 21

CVD ClamAV Virus Database. A file that contains multiple signature types, and a digital signature. This is the format in which the official signatures are distributed. 7, 8, 16

daily.cld A daily.cvd, after `freshclam` updated it. 9

daily.cvd An important database file for **ClamAV**. Contains often updated virus signatures, file type definitions, engine configuration, and whitelists. 9, 21

database.clamav.net database.clamav.net is a round robin record that tries to equally balance the traffic between the best database mirrors.. 6

freshclam **ClamAV**'s signature databases updater application. 3–6, 9–11, 13–16, 21

freshclam.conf The configuration file for `freshclam`. 3–5, 8–10, 14–16

hostname DNS name of a server. 6

mirror A server holding an exact copy of the original server, for better load balancing and bandwidth purposes.. 6, 14

SigUI ClamAV for Windows - Signature Configuration User Interface. The application documented in this manual. 8, 10

SYSTEM account A highly privileged account. This is the account used by system services. You cannot login as SYSTEM. 7

UAC User Account Control, a security infrastructure introduced in Windows Vista. 9

UNC path Uniform Naming Convention path. A path of the form `\\ComputerName \\SharedFolder \\Resource`, or a long UNC path starting with `\\?\`. 7, 14

DRAFT