FORUM SYSTEMS

THE LEADER IN API SECURITY & ZERO TRUST

FORUM SYSTEMS SENTRY™ VERSION 9.1
SOFTWARE INSTALLATION GUIDE

Legal Marks

Forum Systems Sentry™ Version 9.1 Software Installation Guide, published July 2020.

D-ASF-SE-5679045

Table of Contents

INTRODUCTION TO THE SOFTWARE INSTALLATION GUIDE

Audience for the Software Installation Guide

The *Forum Systems Sentry™ Version 9.1 Software Installation Guide* is for IT or Network Administrators who will install the Forum Systems product on a Windows, Linux or Solaris x86 box that has been downloaded from the Forum Systems website.

Documentation Set

For further information, refer to additional documentation in the Forum Systems product Documentation Set included with your Forum Systems distribution:

Conventions Used

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name:	**johnsmith**
Password:	********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the Forum Systems Sentry™ Version 9.1 Web-based Administration Guide.

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

Licensing Versions

Forum Systems product is licensed in the following modes:

- as a limited evaluation version.
- as a subscriber version, licensed according to purchased product features.

SOFTWARE INSTALLATION OVERVIEW

The following listing is an overview of the steps necessary to obtain an evaluation or subscriber version of Forum Systems product software:

- Request software download from Forum Systems support team at support@forumsys.com
- Receive software download instructions via email.
- Request a Software License.
- Receive the License file.
- Import the License file.
- Access the Web Administration Interface.

These steps are detailed next.

SOFTWARE INSTALLATION PROCEDURE

Follow these steps to install and run an evaluation or subscriber version of the Forum Systems software product:

Requesting Software Download

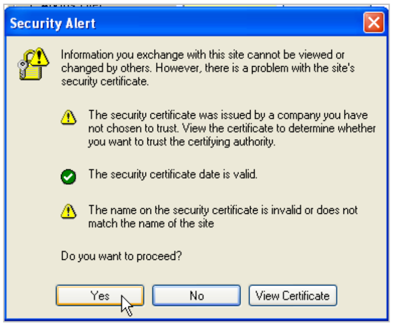
- Request a software download from the Forum Systems support team at support@forumsys.com
- You will receive an email with the download instructions.

Installing Software

Note: You must be logged in with Administrator rights (Windows) or as root (Linux/Solaris x86).

If you are installing on Windows:

1. Navigate your file system and click on the downloaded installation package.
2. The installation package Introduction screen will appear. Click **Next**.
3. The License Agreement screen appears.
4. Read the product License Agreement terms and conditions. To accept the License Agreement, check the **I accept the terms of the license agreement** radio button, and then click **Next**.
5. The Choose Install Set screen appears. Click **Next**.
6. The Choose Install Folder screen appears. Use the default location or enter a new location to install the software and click **Next**.
7. The Pre-Installation Summary screen displays a summary of install options. Click **Install** to begin the installation.
8. Once installation is complete, the Install Complete screen appears. Click **Done** to configure and start the Forum service. Your default web browser will be launched to access the Web Administration interface at https://127.0.0.1:5050.
9. A Security Alert screen appears for the default SSL Certificate used by the Forum service. Accept this Certificate to access the Web Administration interface.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

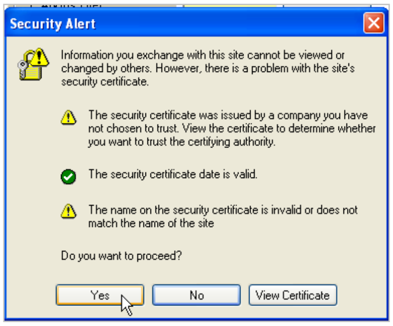
The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

If you are installing on Linux or Solaris x86:

1. Navigate your file system and set the downloaded package to be executable (**chmod +x**).
2. Run the installation file (./<install-file>.bin). The Introduction screen will appear. Verify you have the appropriate minimum system requirements and are logged in as root. Press <**ENTER**> to continue.

3. Read the license agreement and choose whether to accept it.
4. Press <**ENTER**> to accept the default Install Set.
5. Press <**ENTER**> to accept the default location, or specify the install location.
6. Review the Pre-Installation Summary and press <**ENTER**> to continue.
7. Press <**ENTER**> again to install to the location specified.
8. Press <**ENTER**> to complete the install.
9. To start the daemon, type: **service xmlserver start**.
10. To stop the daemon, type: **service xmlserver stop**.
11. Once the daemon has started, access the Web Administration interface through a web browser at https://127.0.0.1:5050.
12. A Security Alert screen appears for the default SSL Certificate used by the Forum service. Accept this Certificate to access the Web Administration interface.


Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

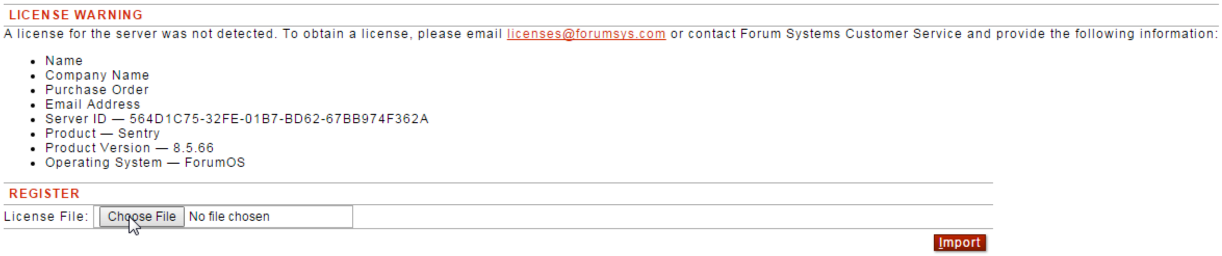
The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Requesting a Software License

If you do not have licensed software, the License Warning screen appears with instructions on how to obtain a license key to enable Forum Sentry product and features. The information required to obtain an evaluation license includes your Contact Name, Company Name, email address of Primary Contact and the displayed unique server ID. You can click directly on the licenses@forumsys.com to auto-populate your email client with the information shows. Otherwise, please copy and paste the text into your email rather than sending a screenshot of the screen. Please also include your PO reference from your purchase.


LICENSE WARNING

A license for the server was not detected. To obtain a license, please email licenses@forumsys.com or contact Forum Systems Customer Service and provide the following information:

- Name
- Company Name
- Purchase Order
- Email Address
- Server ID — 564D1C75-32FE-01B7-BD62-67BB974F362A
- Product — Sentry
- Product Version — 8.5.66
- Operating System — ForumOS

REGISTER

License File: Choose File No file chosen

Figure 1: Example License Warning Screen.

Receiving and Importing License

Once the Primary Contact receives the license file, the license.xml file needs to be imported on the server running the software. An email will be provided to the Primary Contact with example instructions as follows:

This email contains your evaluation license for Forum Systems product. Please follow the instructions below to license your installation.

1) Detach the license.xml file attached to this email
2) Go to the server where the Forum Systems product service is installed
3) Access the Sentry WebAdmin interface, go to:
   https://<device ip>:5050 where device IP is the IP address set for the MGMT interface
4) Import the license file from the WebAdmin interface.

Documentation is accessible from the Help link in the WebAdmin interface.

If you have any questions, please contact Forum Systems support at support@forumsys.com.

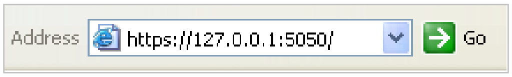
Launching the Web Administration Interface

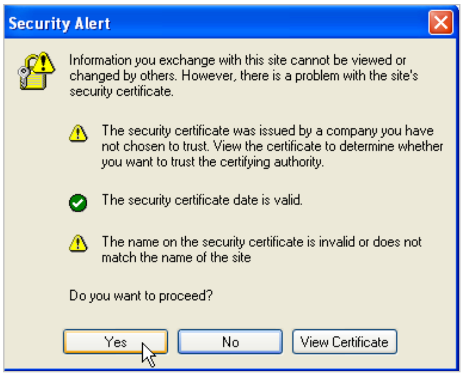
Follow these steps to launch the Web Administration interface:

1. Logon to the Web Administration interface by pointing your web browser to https://127.0.0.1:5050.
2. If you are accessing the Web Administration interface for the first time, the default SSL Certificate Security Alert screen appears. Click **Yes** to accept the SSL Certificate.
3. The Forum Systems LOGON screen appears. If this is the first time accessing the Web Administration interface, complete the default Admin setup:
   - In the User Name field, enter a **user name**.
   - In the Password field, enter a **password**.
   - In the Confirm Password field, re-enter your **password**.
   - Click **Logon**.

   These credentials will be saved for future logins.

Note: The URL for accessing the WebAdmin UI is https://127.0.0.1:5050 from the local machine or https://<ip>:5050 if accessing remotely.





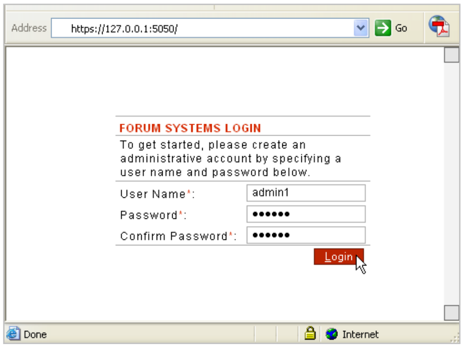
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?



FORUM SYSTEMS LOGIN

To get started, please create an administrative account by specifying a user name and password below.

User Name*: admin1

Password*: ••••••

Confirm Password*: ••••••

Licensed Elements, Supported and Available Features

The bottom of the General screen lists licensing information and a listing of supported features.

License Manager Terms

The following table displays the terms and definitions included in the License Manager:

LICENSE TERM	LICENSE ELEMENT
Forum Systems Model	Platform identification for the software.
Serial Number	Unique server identification.
Licensed to	Company name which software is registered to.
License Expiration	Date license expires.
Product Version	Version number of the product.
Server Start Date / Time	Date and time the software was installed on the server.
Server Up-Time	Length of time the software has been running since the last restart.

CLAM AV INSTALLATION FOR SOFTWARE PORT

Basic Configuration

The Forum Systems **Default AV** feature uses Clam AntiVirus software. Clam is preinstalled on the Forum Systems system, but in the case of the software port Clam must be installed and configured by the local System Administrator.

This document describes how to find and install Clam AV for your particular system, how to make sure that your Forum software port can communicate with it, and how to keep your virus definitions up to date. Following these general descriptions are specific pointers for individual operating systems.

Note: Sentry and XWall products can integrate with other anti-virus solutions; not Presidio products. The current anti-virus solution is an extensible socket interface which can accept third party interfaces.

The Clam Antivirus Website

Clam AV is open source software, available for free from **http://www.clamav.net/.** The Clam website also has more extensive documentation on the inner workings of Clam, a virus test page to manually test your files against the current version of Clam, a form for the submission of new viruses, and access to the latest virus definition files.

For the purposes of the Forum software port, the most interesting location on the Clam site is **http://www.clamav.net/binary.html#pagestart**, “binary packages and ports”. More advanced users may of course download and compile from source, but that will not be covered in this document.

Clam documentation is available from the website as well and is recommended reading for anyone using the Clam virus scanner. An online version is available at **http://www.clamav.net/doc/latest/html/**.

Clamd

The Forum Default AV integration requires Clam’s daemon, clamd, to be running and listening on a TCP socket. Depending on which operating system and version of clam is installed, this may occur automatically on clamd start, or may require additional configuration. This document assumes that clamd is not set up to listen on a TCP socket by default. Which socket is used is not important – 3310 is the clamd default, but as long as the clamd configuration files and the Forum WebAdmin interface agree on which port is to be used, any port is acceptable.

Clamd Configuration

In order to set up clamd to listen on a socket, the file **clamd.conf** must be located and modified. Its location depends on operating system – refer to the individual operating system sections for pointers on how to locate it.

Open clamd.conf with a suitable text editor. Search for the configuration setting **TCPSocket**, and make sure that it is present and not commented out (make sure the line does not start with the # character). The default setting is “**TCPSocket 3310”** but any valid socket may be used in place of the value 3310.

Now search for the setting **TCPAddr**. This sets the address that the TCP socket is available on. Forum recommends setting this to 127.0.0.1 so that connections from other machines will not be allowed, but this is not strictly necessary. If you wish to accept any and all connections, this setting may be commented out (add a # to the beginning of the line).

Finally, it is important that clamd is not also listening on a local socket. Search for the setting **LocalSocket** and either remove that line or comment it out by adding a # to the start of the line.

Many other settings are available in the clamd.conf file which may be of interest, and most clamd distributions contain a clamd.conf file with descriptive annotations on what each configuration setting controls. Some settings place log files and set which directories are used for temporary files (for example, when unzipping a file to check for viruses). Settings of this nature include **LogFile, PidFile, TemporaryDirectory,** and **DatabaseDirectory** (which points to the location of the virus definition files).

Depending on the configuration of your particular system, you may wish to move some of these directories.

Other settings control how much work clamd is willing to do before declaring a file too big or too complicated to scan (at which point it considers the file to be a bad file as though it did have a virus). Settings here include **StreamMaxLength, ArchiveMaxFileSize, ArchiveMaxRecursion, ArchiveMaxFiles,** and **ArchiveMaxCompressionRatio.** In general the shipping clamd settings will be suitable unless you expect to process unusually large attachments. **StreamMaxLength** in particular must be modified in order to enable attachments larger than a few megabytes, for example changing the value to “**StreamMaxLength 100M**”.

Running Clamd

Starting and stopping clamd and keeping it running is the responsibility of the System Administrator – ideally clamd should be started with other system daemons during startup. If clamd stops running, virus checking will begin rejecting all traffic with the error message “Partner Default_AV failed virus check”. Clamd is quite stable and is unlikely to suddenly terminate, but System Administrators who wish to maintain high availability should have an additional monitor to make sure that clamd is always running. Clamd on the Forum Systems system uses a similar method to automatically restart itself if it goes down for any reason.

If the software port is being used for a test setup, clamd may of course be started manually before testing.

Freshclam and Virus Updates

The standard way to keep a Clam installation’s virus definition files up to date is to run the included program freshclam, either on a schedule or manually. Freshclam checks the version of the two virus database files and downloads newer versions from a network of servers.

Freshclam has its own configuration file, freshclam.conf. If you make changes in clamd.conf to the various directories used, especially **DatabaseDirectory**, you must make matching changes to freshclam.conf. In general the installed setup will be quite suitable and no changes should be necessary, but verify the version of the daily file on the **Default AV** screen (for more information, refer to the **Verify CLAM AV Installation** section below) before and after your first freshclam run to make sure it and clamd are in agreement.

If setting up freshclam to run automatically (by a cron job, for example) please refer to the section on freshclam in the Clam AV manual available on the website. In particular, do not set this update to happen too frequently (more than every hour) or the clam update servers may blacklist you, and do not set your update to happen at times that are already oversubscribed (such as multiples of ten minutes past the hour).

If you wish to take control of your virus update procedure completely, you may download the virus definition files manually from the Clam website, links to main.cvd and daily.cvd are provided on the front page. Place these files in the directory pointed to by **DatabaseDirectory**, and restart your running clamd.

The present version of your database files may be seen on the **Default AV** screen in the WebAdmin. From the Navigator, select **Partners** under the **System** category.

Licensing

Default AV integration is a separately licensed feature on the system. The General Info screen in the WebAdmin will indicate whether this integration is licensed. If not, none of the antivirus screens will be accessible and no virus scanning will be performed. Clam AV itself is freely available under the GPL.

Forum AV Activation

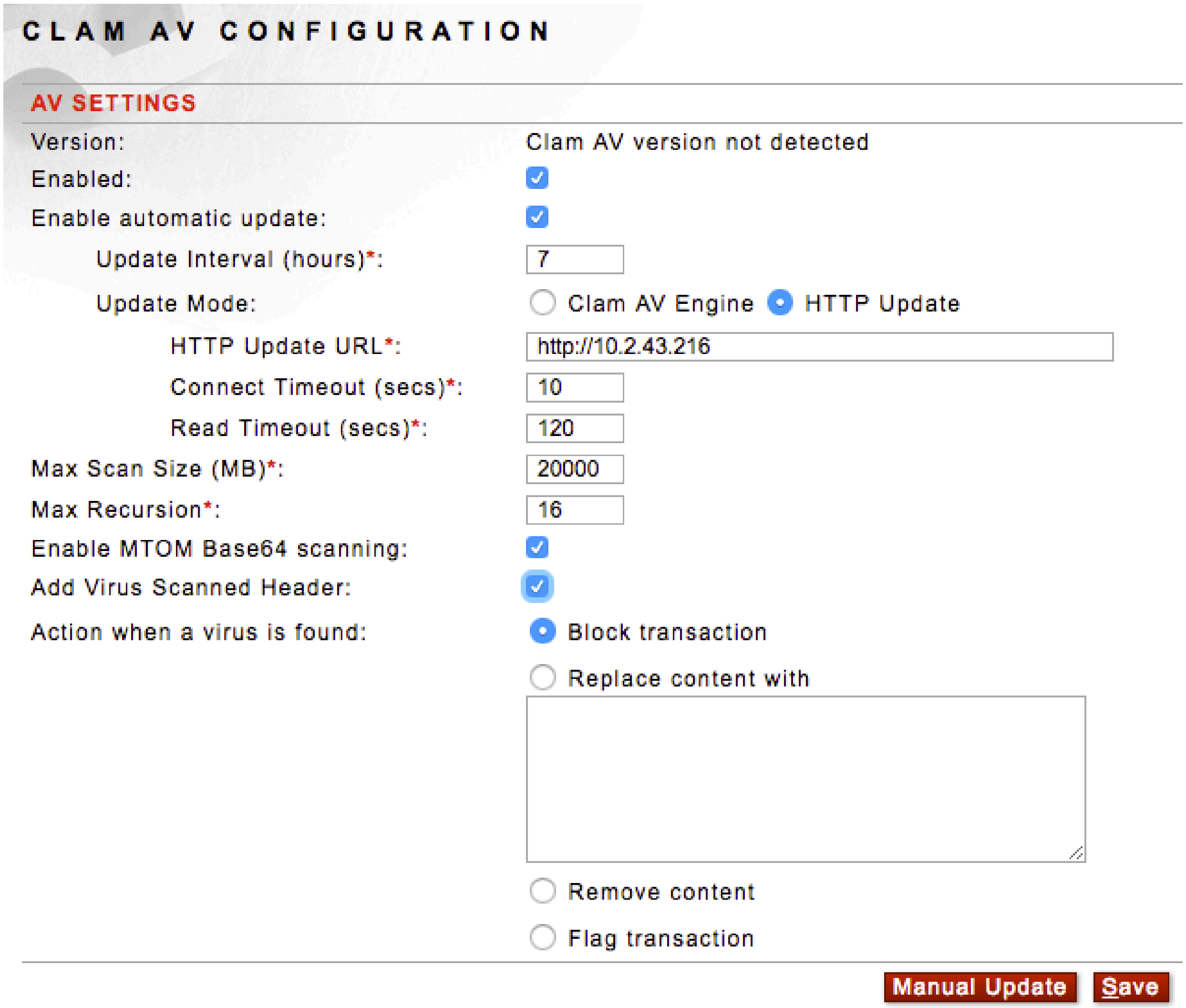
On the WebAdmin side, Clam AV integration is controlled through the **Default AV** screen. From the Navigator, select **Partners** under the **System** category. This screen displays the present running version of clamd and its virus definition files, retrieved from clamd, and allows virus scanning to be globally enabled and disabled. Finally, the socket for clamd communication may be changed on this page, defaulting to the clamd default of 3310.

Actual control of behavior when a virus is detected is controlled by the virus IDP rules, which are placed in the System IDP Group and the Default policy IDP Groups for both requests and responses. If you wish to only scan some projects for viruses, you must remove the virus rule from the System IDP Group and use a project IDP Group which does not contain the virus rule for projects you do not wish to have scanned. For more information on managing IDP Groups, refer to the *Forum Systems Sentry™ Version 6.5 IDP Rules Guide*.

Verify CLAM AV Installation

If clamd is running and Forum can successfully communicate with it, the clamd version and virus definition file versions will be visible on the **Default AV** screen that controls the integration. If this version information is not available, check that clamd is running and that the clamd socket is set to the same value in clamd.conf as in the Forum WebAdmin.

If virus scanning is enabled on the **Default AV** screen but the system cannot communicate with clamd because of a socket disagreement or because clamd is not running, all traffic will be marked as containing a virus. If virus IDP Rules are enabled, as they are by default, this will result in all traffic being rejected.



CLAM AV CONFIGURATION

AV SETTINGS

Version: Clam AV version not detected

Enabled: ☑

Enable automatic update: ☑

Update Interval (hours)*: 7

Update Mode: ○ Clam AV Engine ● HTTP Update

HTTP Update URL*: http://10.2.43.216

Connect Timeout (secs)*: 10

Read Timeout (secs)*: 120

Max Scan Size (MB)*: 20000

Max Recursion*: 16

Enable MTOM Base64 scanning: ☑

Add Virus Scanned Header: ☑

Action when a virus is found: ● Block transaction
○ Replace content with
○ Remove content
○ Flag transaction

Figure 2: Correctly Configured Default AV Setup.

Operating System Notes

There are some basic installation instructions at **http://clamav.or.id/** which should be read before performing the Clam AV installation that describe how to perform the various installs. All of the installations have their own tests which may be run (usually clamdscan runs on test files) to make sure that clamd is running properly.

Unix Style Systems in General

In general, Unix style installs will default to having the **TCPSocket** option commented out. Clamd expects to run as the clamav user with permissions to use the clam directories. These installations require some libraries other than the base clam libraries which may or may not already be installed on your system – if not, compatible versions are available **http://clamav.or.id/libs/**. See the general notes on the install screen for more about libraries at **http://clamav.or.id/**.

Linux Distributions

Some distributions, such as Debian, include clam as an installable package in their management systems, such as apt-get. Others have easily installable packages. See the binary distributions screen at **http://www.clamav.net/binary.html#pagestart** for pointers to installations for various Linux distributions.

Distributions such as Debian (which do not update frequently) may have packages that are extremely out of date – check the version of the installed Clam against the stable release version on the Clam home page. Versions prior to 0.80 are not suitable for use with Forum software.

Solaris x86

The binary distributions screen maintains links to various precompiled Solaris x86 installs. You will probably need to install libgmp, libgcc, and zlib as mentioned in the installation page at **http://clamav.or.id/** - these are available at **http://clamav.or.id/libs/**. At this time, the libgmp install also requires an additional symbolic link named libgmp.so.3 to the actual installed version.

Windows

The binary distributions screen at **http://www.clamav.net/binary.html#pagestart** includes several options for Windows users. The MS Windows (native) port is not appropriate for Forum users.

The two Windows versions that are suitable for use with the Forum Systems system are the two Cygwin-based distributions. Either choose Clam as an install option under the normal Cygwin installer (it's available in the Cygwin installer under Utils), or install Clam with its own copy of cygwin.dll. This second option is listed in the binary screen as "**MS Windows (cygwin.dll based)**", and does not require any existing Cygwin installation.

Installing the GUI is not necessary. Clamd may be set to run automatically simply by setting the start clamd script to run at system startup.

INDEX