CLAMWALL

Antivirus Mercury/32 daemon

Version 1.1.0

Introduction

Clamwall is a program that uses ClamAV daemon as antivirus filter. It uses direct TCP communication with ClamD for maximum possible performance.

Clamwall is antivirus protection on the server level. It works for all local accounts automatically without any special software on the client side. You can use any post program on the client side.

If you do not have ClamD running then you can download and install the binaries from http://www.ararat.cz/eng/show.php?clamwall

Fresh installation instructions:

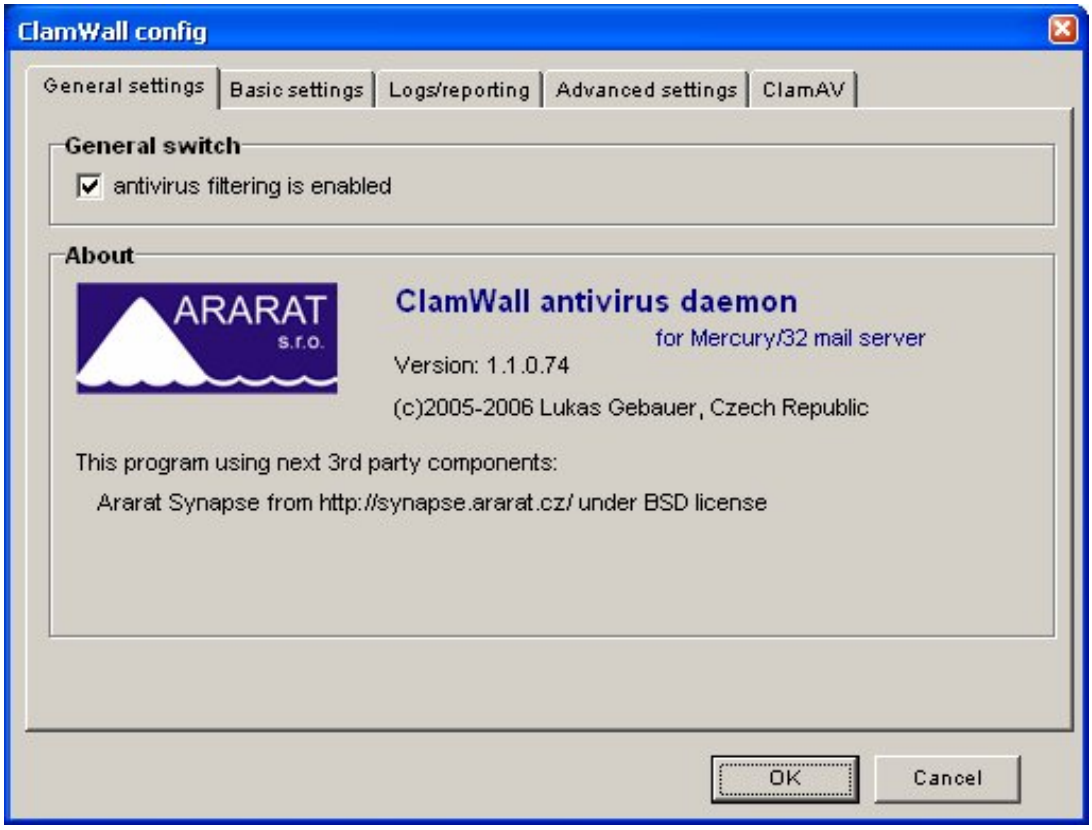
1) Stop your Mercury/32.
2) Run Clamwall installer.
3) Install ClamAV Daemon or get information about some running ClamAV daemon on your network.
4) Run Mercury/32
5) Use Configuration | Clamwall to configure

Uninstall

You can uninstall Clamwall using your Control Panel | Add/Remove Programs. Do this the same way that you uninstall any other application. This will not uninstall ClamAV itself.

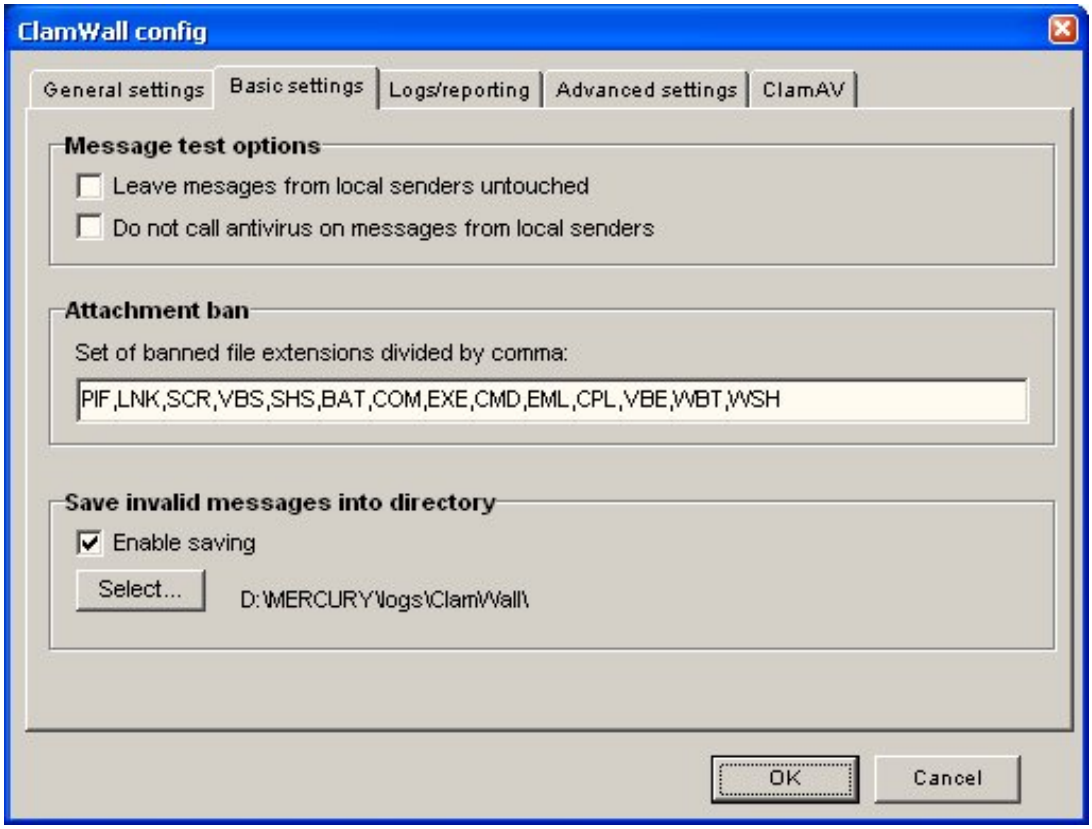
Clamwall Configuration screens:

*The **[section] item** are the items in the clamwall.ini file.*



General Switch

Enables the Clamwall antivirus daemon



Message test options

You can turn off Clamwall processing for all messages produced by local mail system and Clamwall is used for messages delivered by SMTP only. ***[Clamwall] NoLocal***

Only messages from SMTP are checked by antivirus when this option is turned on. It not affects checks for banned extensions! ***[Clamwall] NoLocalScan***

Attachment ban

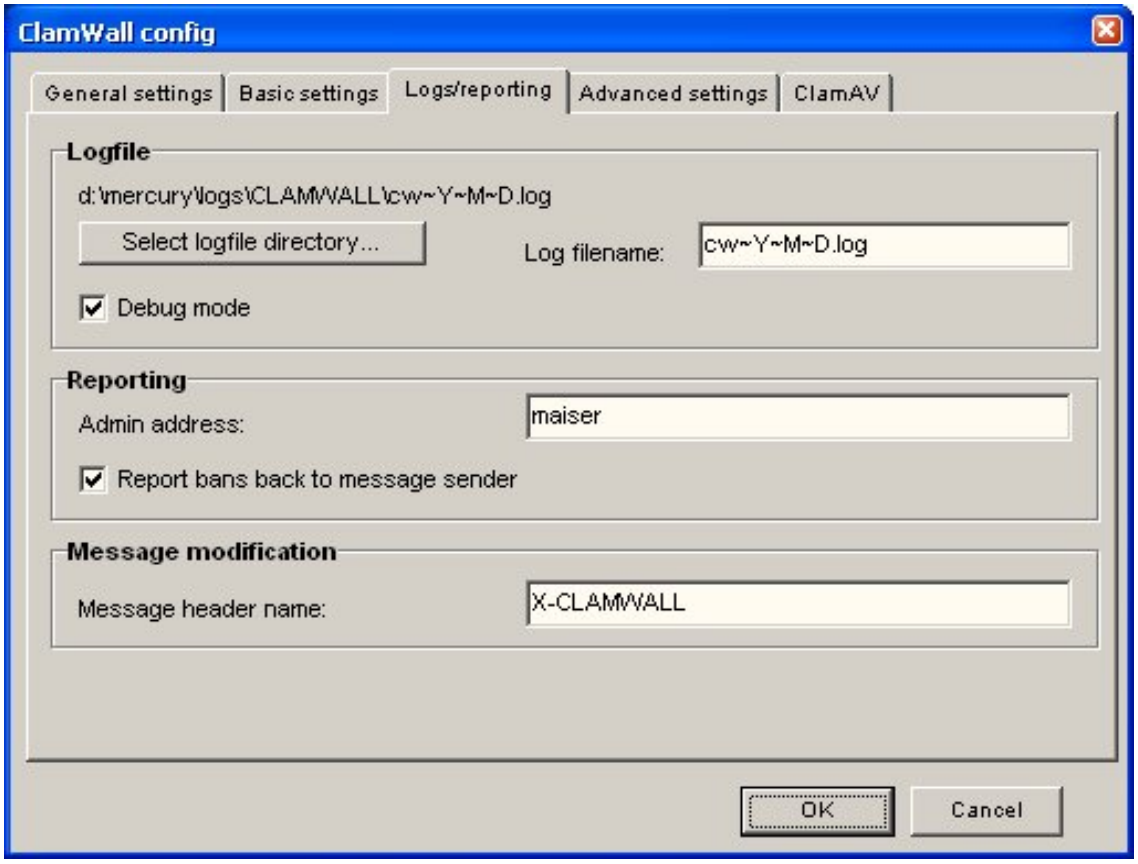
Set of filename extensions what will be prohibited by Clamwall. Recommended set is:

PIF,LNK,SCR,VBS,SHS,BAT,COM,EXE,CMD,EML,CPL,VBE,WBT,WSH

When Clamwall detects an attachment with one of these file extensions, then the message is rejected. ***[Clamwall] BanExtensions***

Save invalid messages into directory

You can pass directory here for storing rejected messages here. (Directory name must end with backslash!) Messages are stored in CNM format for easy manual delivery to destination mailboxes. ***[Clamwall] SaveDir***



Logfile

File for Clamwall logging. You can use the same name macros as you can for log file names in Mercury. ***[Clamwall] logfile***

If Debug mode is checked, Clamwall writes debugging information to your logfile. **[Clamwall] Debug**

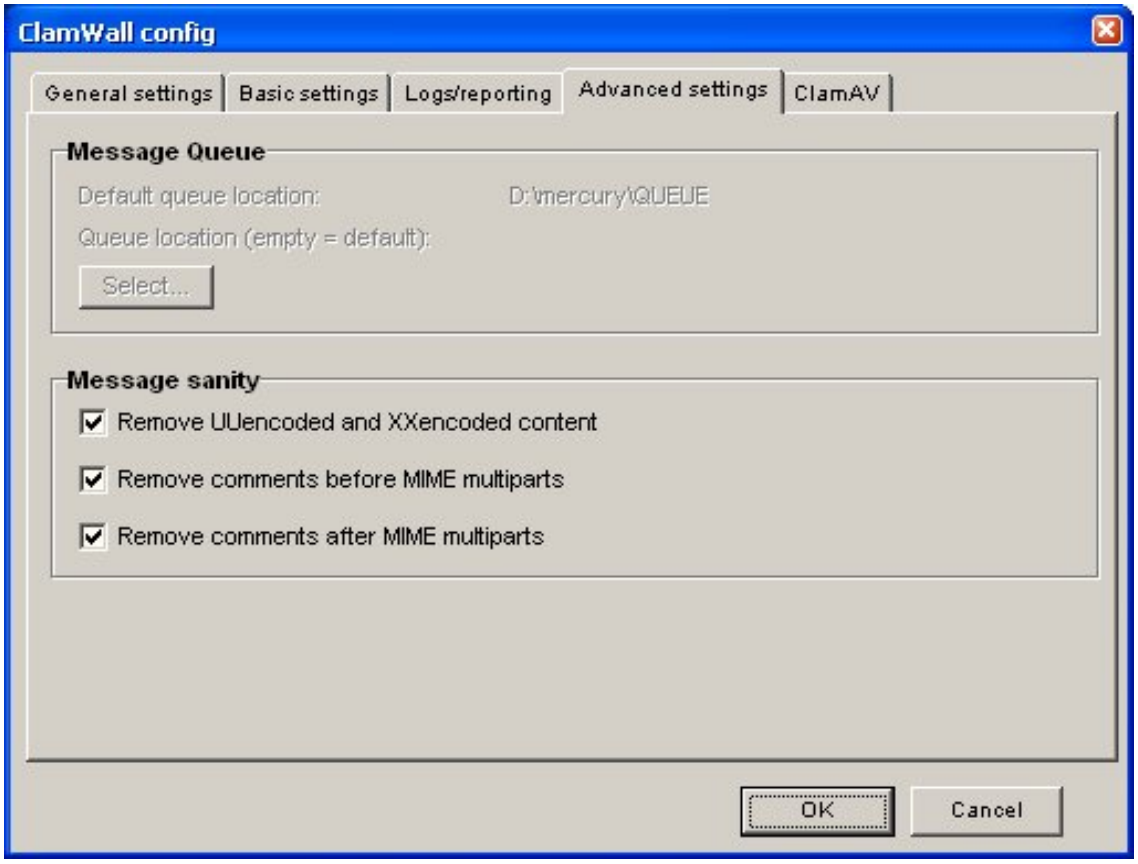
Reporting

Local mail account what will be used as sender of error messages generated by Clamwall. ***[Clamwall] AdminMail***

When Clamwall detects some attachment with one of banned file extension, then message is rejected and Clamwall send error message to original message sender. When Clamwall see virus in mail message, then Clamwall not send back any error message. Sending of error messages is controlled by this configuration option.

Message modification

Message header name for Clamwall information written to processed mails. Default is 'X-CLAMWALL'. ***[Clamwall] TagName***



Message queue

This is directory with Mercury/32 queue. If you don't specify this, then automatic detection is used. If automatic detection fails, then you can specify your queue directory here to override automatic detection process.

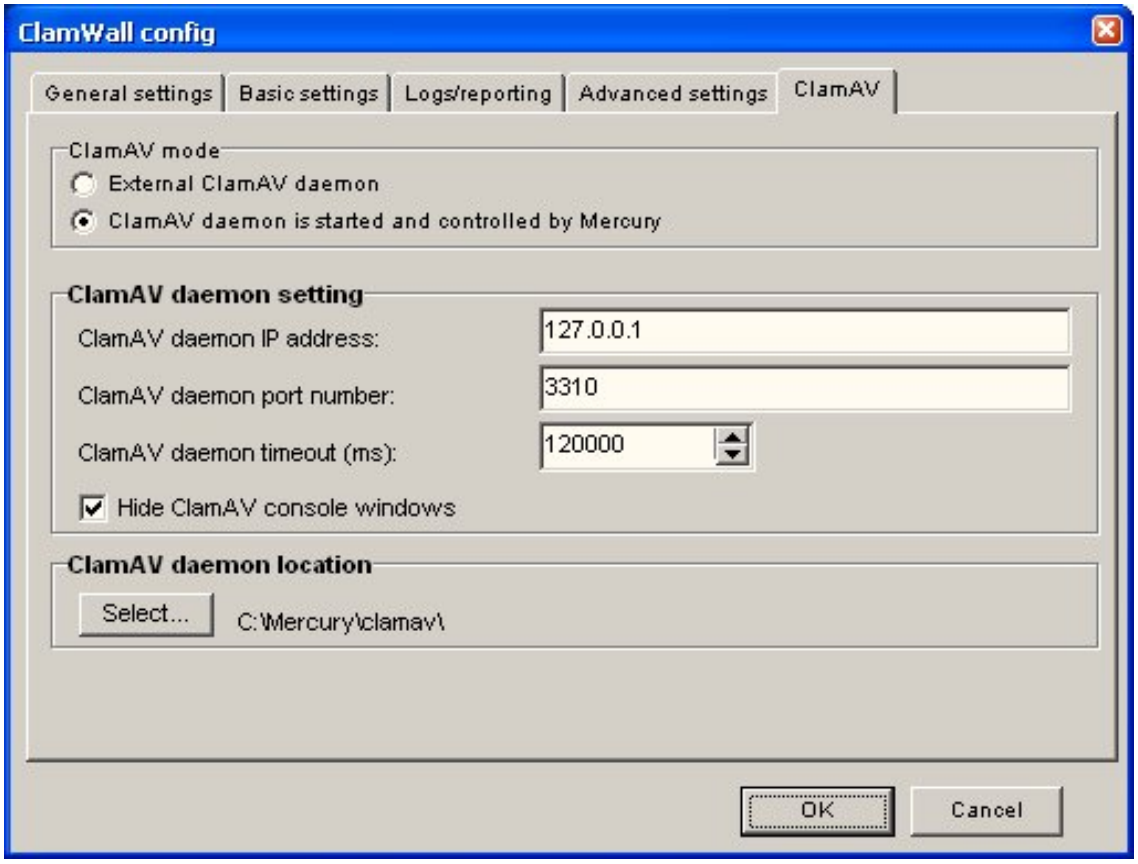
When you are using Mercury/32 version 4.1 or higher, this directive is ignored because Spamwall uses a new job accessing code! ***[Clamwall] Queue***

Message sanity

Remove UUencoded or XXencoded content from message. It is used as non-MIME attachment transport. This kind of attachment transport is very obsolete and is used as bypass of other MIME based content filters. ***[Clamwall] UUKill***

Delete content after end of multipart message to real end of message. It cannot contain useful information in multipart message, but some malformed content here can confuse some mailer programs. ***[Clamwall] ClearPostPart***

Delete content after message headers to begin of multipart content. It cannot contain useful information in multipart message (usually contains some disclaimer like "this is IME multipart message…"), but some malformed content here can confuse some mailer programs. ***[Clamwall] ClearPrePart***



ClamAV mode

You can turn on the mode where ClamWall can run ClamD.exe and FreshClam.Exe. ClamWall will start these two applications when it is necessary and leave it running. When Mercury is closed, Clamwall will close these two applications as well. Clamwall controls the operation of these two applications and when this applications crashes or is manually closed, Clamwall will start them as required. ***[ClamAV] ClamSelf***

ClamAV daemon setting

The IP address of your ClamAV Daemon. If you are running ClamD on the same computer, use 127.0.0.1.***[ClamAV] ClamIP***

Port used by your ClamAV daemon. Default value is 3310. ***[ClamAV] ClamPort***

Timeout (in milliseconds) for communication with antivirus. ***[ClamAV] ScanTimeout***

Set to 1 for hide ClamD and Freshclam on console. (In ClamSelf mode only) ***[ClamAV] ClamHide***

ClamAV daemon location

When you turn on ClamSelf, you must specify local directory of your ClamAV installation here (it is directory name without trailing backslash). ClamD.exe, FreshClam.Exe, ClamD.conf and FreshClam.conf must exist in this directory. Don't forget to configure ClamAV configuration files! ***[ClamAV] ClamDir***