



Clam AntiVirus 0.98
User Manual

Contents

1	Introduction	4
1.1	Features	4
1.2	Mailing lists and IRC channel	6
1.3	Virus submitting	6
2	Base package	6
2.1	Supported platforms	6
2.1.1	UNIX	6
2.1.2	Windows	7
2.2	Binary packages	7
3	Installation	7
3.1	Requirements	7
3.2	Installing on shell account	8
3.3	Adding new system user and group	8
3.4	Compilation of base package	9
3.5	Compilation with clamav-milter enabled	9
3.6	Running unit tests	9
3.7	Reporting a unit test failure bug	10
4	Configuration	11
4.1	clamd	11
4.1.1	On-access scanning	11
4.2	clamav-milter	12
4.3	Testing	12
4.4	Setting up auto-updating	13
4.4.1	Closest mirrors	14
4.5	ClamAV Active Malware Report	14
5	Usage	15
5.1	Clam daemon	15
5.2	Clamdscan	17
5.3	Clamuko	18
5.4	Output format	18
5.4.1	clamscan	18
5.4.2	clamd	19

6	LibClamAV	20
6.1	Licence	20
6.2	Supported formats and features	20
6.2.1	Executables	20
6.2.2	Mail files	20
6.2.3	Archives and compressed files	21
6.2.4	Documents	21
6.2.5	Data Loss Prevention	22
6.2.6	Others	22
6.3	API	22
6.3.1	Header file	22
6.3.2	Initialization	22
6.3.3	Database loading	23
6.3.4	Error handling	24
6.3.5	Engine structure	24
6.3.6	Limits	25
6.3.7	Database checks	25
6.3.8	Data scan functions	26
6.3.9	Memory	28
6.3.10	Forking daemons	29
6.3.11	clamav-config	29
6.3.12	Example	29
6.4	CVD format	29
6.5	Contributors	30
6.6	Donors	40
6.7	Graphics	46
6.8	OpenAntiVirus	46
7	Core Team	47
8	Emeritus Team	47

ClamAV User Manual, © 2007 - 2013 Sourcefire, Inc. Authors: Tomasz Kojm
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; either version 2 of the License, or (at your option) any later version.

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.

1 Introduction

Clam AntiVirus is an open source (GPL) anti-virus toolkit for UNIX, designed especially for e-mail scanning on mail gateways. It provides a number of utilities including a flexible and scalable multi-threaded daemon, a command line scanner and advanced tool for automatic database updates. The core of the package is an anti-virus engine available in a form of shared library.

1.1 Features

- Licensed under the GNU General Public License, Version 2
- POSIX compliant, portable
- Fast scanning
- Supports on-access scanning (Linux and FreeBSD only)
- Detects over 1 million viruses, worms and trojans, including Microsoft Office macro viruses, mobile malware, and other threats
- Built-in bytecode interpreter allows the ClamAV signature writers to create and distribute very complex detection routines and remotely enhance the scanner's functionality
- Scans within archives and compressed files (also protects against archive bombs), built-in support includes:
 - Zip (including SFX)
 - RAR (including SFX)
 - 7Zip
 - ARJ (including SFX)
 - Tar
 - CPIO
 - Gzip
 - Bzip2
 - MS OLE2
 - MS Cabinet Files (including SFX)
 - MS CHM (Compiled HTML)