

fsav.conf

<support@F-Secure.com>

Juha AuteroSami Mäkinen-Okubo2002-10-26

Name

fsav.conf — configuration file for F-Secure Anti-Virus for Linux

DESCRIPTION

`/etc/fsav.conf` is the default configuration file for F-Secure Anti-Virus for Linux. This manual page documents the format of the file.

Every configuration line consists of two fields, the *option name* field and the *option value* field. These two fields are separated by one or more spaces or tabs. Empty lines or lines starting with “#” are ignored. Options specified in the command line override options specified in the configuration file. Following *option names* are available:

`enginedirectory <directory path>`

This option specifies the directory where scanner engines are located. The default value is `/opt/f-secure/fsav/lib/`.

`databasedirectory <directory path>`

This option specifies the directory where database files are located. The default value is `/var/opt/f-secure/fsav/databases/`.

`installdirectory <directory path>`

This option specifies the directory where F-Secure Anti-Virus for Linux is installed.

`updatedirectory <directory path>`

This option specifies the directory that is used as work directory when updating database files from F-Secure web site.

`socketname <filename>`

The name of the socket used to communicate between fsav and fsavd. The default value is `/tmp/.fsav`.

`action {disinfect,delete,rename}`

The action to be performed on infected files. It can be either *disinfect*, *rename* or *delete*. You can have several *action* lines to specify several actions.

`logfile { <file path>, syslog, stderr, none}`

Set the server error and activity log file location. If the value is a file path, the server writes log entries into the file. If the value is *syslog*, the server writes log entries to syslog. If the value is *stderr*, the server writes log entries to stderr. If the value is *none*, the server logging is disabled.

The default log file is syslog (see `syslog(3)`, `syslogd(8)`, `syslog.conf(5)` for more information). The default syslog facility is `LOG_DAEMON` and the facility can be changed with *syslogfacility* configuration

option. The log priorities are following: access log = LOG_NOTICE (fsavd start/stop, dbupdate ja engine start messages), warnings = LOG_WARNING (scan failures, infections and suspected messages), errors = LOG_ERR (dbupdate, I/O and out of memory errors).

syslogfacility { <facility name> }

The syslog facility (see syslog(3), syslogd(8), syslog.conf(5) for more information). The default syslog facility is LOG_DAEMON. Possible facility names are listed in syslog(3) manual page.

extensions <extensions list>

This option specifies the list of filename extensions that are scanned when scanning directories or archives. You can use following wild card characters:

*

match zero or more characters in a sequence,

?

match any single character,

.

if given alone match extensionless files.

The default value is .,acm,app,arj,asd,asp,avb,ax,bat,bin,boo,bz2,cab,ceo,chg,cmd,cnv,com,cpl,csc,dat,dll,do?,drv,eml,exe,gz,hlp,hta,htm,html,htt,inf,ini,js,jse,lnk,lzh,map,mdb,mht,mif,mp?,msg,mso,nws,obd,obt,ocx,ov?.p?t,pci,pdf,pgm,pif,pot,pp?,prc,pwz,rar,rtf,sbf,scr,shb,shs,sys,tar,td0,tgz,tlb,tsp,tt6,vbe,vbs,vwp,vxd,wb?,wiz,wml,wpc,ws?,xl?,zip,zl?,{*

scanexecutables <{on,off,yes,no,1,0}>

Enable executable scanning. If file has any of user/group/other executable bits set, the file is scanned regardless of the file extension.

maxnestedarchives <number>

Set the maximum number of nested archives (an archive containing other an archive) for the archive scanning. If the fsavd encounters an archive which contains more nested archives than the value, a scan error is reported for the file.

If the value is set to 0, the encountered archive is scanned but if the archive contains an other archive, a scan error is reported for the file.

The default value for the option is 5.

archivescanning <{on,off,yes,no,1,0}>

Enable/disable archive scanning. The default is enabled.

mimescanning <{on,off,yes,no,1,0}>

Enable/disable MIME message scanning. The default is enabled.

scantimeout <number>

Set the default time limit for a single file scan or disinfect task in seconds. If the scan or disinfect task takes longer than the specified value, a scan error is reported for the file.

If the value is set to 0 (default), the scan timeout is disabled and the file is scanned until the scan is over or a scan error occurs.

engineinstancemax <number>

Set maximum number of concurrent scan engines of same type. The default is 4.

ignore <scan result message>

Ignore scan result which starts with the same text as given string. This option applies only to scan errors and to some MIME suspicions. The scan result is silently ignored by fsav command-line interface but fsavd still logs the scan result to fsavd's log, if specified. For example "ignore Password protected file" will suppress any scan errors caused by password protected file and exit status of fsav command-line interface is not affected. The file is scanned to the end but if no other scan results are detected, *the file is treated as clean*.

WARNING! Ignoring any messages may leave malicious content undetected!

EXAMPLE

```
# This is configuration file for F-Secure Anti-Virus for Linux 4.52
```

```
#
```

```
# (C) 2002-2004 F-Secure Corporation
```

```
#
```

```
## Directory where scan engine databases are located.
```

```
basedirectory /var/opt/f-secure/fsav/databases/
```

```
## Directory where scan engines are located.
```

```
enginedirectory /opt/f-secure/fsav/lib/
```

```
## Directory where the F-Secure Anti-Virus for Linux is installed.
```

```
installdirectory /opt/f-secure/fsav
```

```
## Directory from where the new databases are loaded.
```

```
updatedirectory /var/opt/f-secure/fsav/update
```

```
## Uncomment the following to enable disinfection on infected files by default.
```

```
#action disinfect
```

```
## Uncomment the following to enable file rename on infected files by default
#action rename
```

```
## Uncomment the following to enable file delete on infected files by default
#action delete
```

```
## Set the time limit for a single scan task in seconds.
## If time limit is exceeded, a scan error is reported for a file.
## Uncomment the following to set scan time limit to 30 seconds.
#scantimeout      30
```

```
## Uncomment the following to set maximum nested archives to 10.
#maxnestedarchives 10
```

```
## Set the server logfile location. The value can be one of the following:
```

```
## none    - disable logging,
## stderr  - write log to stderr,
## syslog  - write log to syslogd(8),
## <file>  - write log to <file>.
```

```
## Uncomment ONE of the following to set server's log file location.
```

```
#logfile      none
#logfile      stderr
#logfile      syslog
#logfile      /var/opt/f-secure/fsav/log/scan.log
```

```
## Set the name of UNIX domain socket used for communication between
## client and server. If not given, path /tmp/.fsav-<UID> is used
## instead. Uncomment the following to set server socket.
#socketname /var/opt/f-secure/fsav/run/.fsav
```

```
## Set the list of file extensions to be scanned.
```

```
extensions      ..acm,app,arj,asd,asp,avb,ax,bat,bin,boo,bz2,cab,ceo,chg,
.cmd,cnv,com,cpl,csc,dat,dll,do?,drv,eml,exe,gz,hlp,hta,htm,html,htt,inf,ini,js,
jse,lnk,lzh,map,mdb,mht,mif,mp?,msg,mso,nws,obd,obt,ocx,ov?,p?t,pci,pdf,pgm,pif,
pot,pp?,prc,pwz,rar,rtf,sbf,scr,shb,shs,sys,tar,td0,tgz,tlb,tsp,tt6,vbe,vbs,vwp,
vxd,wb?,wiz,wml,wpc,ws?,xl?,zip,zl?,*
```

```
## Uncomment the following to disable executable scanning by default
#scanexecutables off
```

```
## Uncomment the following to ignore scan errors or suspected
## infections described in string from fsav command-interface output.
##
## WARNING! Ignoring these messages may leave malicious content undetected!
##
#ignore Password protected file
#ignore MIME decompression error
```

#ignore Partial MIME message
#ignore Invalid MIME header found

AUTHORS

F-Secure Corporation

Copyright

Copyright (c) 1999-2004 F-Secure Corporation. All Rights Reserved. Portions Copyright (c) 2001-2004 Kaspersky Labs.

SEE ALSO

fsav(1) and fsavd(8)

For more information, see F-Secure products home page (<http://www.F-Secure.com/anti-virus/webclub/>).