NAME

esets_ssfi.so − ESETS SafeSquid's FIlter module.

DESCRIPTION

The esets_ssfi.so is a content filter that accesses http source objects being processed by SafeSquid HTTP proxy cache. It examines (but not modifies) the content of the source object and causes blocking of the message in case the body part of the message contains infiltration.

CONFIGURATION FILE OPTIONS

The main ESETS configuration mechanism is assumed to be that using ESETS main configuration file. Note that most principles of this mechanism are described in the esets.cfg(5) manual page while this section contains only additional information related with the list of configuration file options valid for this particular module. Therefore we recommend user to become familiar with the above mentioned documentation prior reading this section.

ESETS MODULE PRIVATE OPTIONS

No options reported.

ESETS MODULE COMMON OPTIONS

To get detailed description of ESETS module common options, please refer to the section **ESETS MODULE COMMON OPTIONS** of the **esets.cfg(5)** manual page.

ESETS SCANNER COMMON OPTIONS

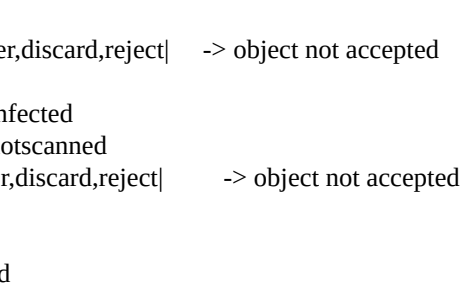
To get detailed description of ESETS scanner common options, please refer to the section **ESETS SCANNER COMMON OPTIONS** of the **esets.cfg(5)** manual page.

USER SPECIFIC CONFIGURATION

This module does not have implemented user specific configuration functionality.

HANDLE OBJECT POLICY

The Handle Object Policy (see figure below) is a mechanism that provides handling of the scanned objects depending on their scanning status. The mechanism implemented in this module is based on so called action configuration options **action_av**, **action_av_infected** and **action_av_notscanned**. To get description of these configuration options, see esets.cfg(5) manual page.



Every object processed by this module is first handled with respect to the setting of the configuration option **action_av**. Once this parameter is set to 'accept' (resp. 'defer', 'discard', 'reject') the object is accepted (resp. deferred, discarded, rejected). If the option is set to 'scan' the object is scanned for virus infiltrations and set of action configuration options 'action_av_infected' and 'action_av_notscanned' is taken into account to evaluate further handling of the object.

NOTE: Please, note that the module has been written to integrate ESETS into the environment which does not allow to modify scanned objects and thus this functionality is disabled also in the module. Particularly, this means that this module ignores setting for configuration option **av_clean_mode**.

If action 'accept' has been taken as a result of the above action options the object is accepted i.e. the access to the object is allowed. On the other hand if any of action configuration options caused other than 'accept' value, the object is blocked, i.e. access to the object is denied.

You have probably noticed that each of the action configuration options discussed above accepts a variety of the values whose list can be found in esets.cfg(5) manual page. As also stated there the values listed are

handled individually by every ESETS agent module. Thus to be consistent in the following we review the meaning of the values for this ESETS agent module.

accept Accept object on this level of Handle Object Policy, i.e. access to the object is allowed by the particular action configuration option.

scan Scan object for virus infiltrations.

defer, discard, reject
Block access to the object, i.e. the access to the object is denied by this particular action configuration option.

LOGGING

Logging functionality of the ESETS agent modules has been developed to fine tune or to troubleshoot the agent module performance. Thus all the ESETS agent modules support only logging using syslogd daemon which logs system messages on *nix systems. To get more information on this topic please, refer to manual pages syslog(2), syslog.conf(5) and syslogd(8).

Regarding ESETS agent modules, this functionality can be invoked by setting ESETS module common configuration option *syslog_facility* to value other than **none**. To get description of the introduced ESETS module common configuration options please, refer to esets.cfg(5) manual page.

Once the syslog logging enabled, the ESETS agent module messages are logged with one of the following syslog priorities:

LOG_ERR
Error messages concerned with the ESETS agent module performance are logged with this priority. Message logged with this priority usually means that error occurred during the ESETS agent module running and thus the module could not accomplish its operation or even the module process exited.

LOG_WARNING
Warning messages concerned with the ESETS agent module performance are logged or 'summary' messages concerned with action other than 'accept' taken as a consequence of object scanning status are logged with this priority.

LOG_NOTICE
The 'summary' messages concerned with action taken as a consequence of object scanning status are logged with this priority.

LOG_INFO
The common tasks are logged with this priority.

LOG_DEBUG
Debug information concerned with the ESETS agent module performance is logged with this priority.

COMMAND LINE OPTIONS

This module does not implement command line interface.

REPORTING BUGS

In order to report bugs, please visit http://www.eset.com/support <URL:http://www.eset.com/support> or use directly the support form at http://www.eset.eu/support/form <URL:http://www.eset.eu/support/form>.

COPYRIGHT

SEE ALSO

esets_cgp(1) esets_cli(1) esets_dac(1) esets_ftp(1) esets_gwia(1) esets_http(1) esets_icap(1) esets_imap(1) esets_mda(1) esets_mird(1) libesets_pac.so(1) esets_pipe(1) esets_pop3(1) esets_smfi(1) esets_smtp(1) esets_ssfi.so(1) esets_wwwi(1) esets_zmfi(1) esets(5) esets.cfg(5) esets_daemon(8) esets_inst(8) esets_lic(8) esets_quar(8) esets_scan(8) esets_set(8) esets_update(8) eset_efs_userguide.pdf eset_egs_userguide.pdf eset_ems_userguide.pdf