NAME

esets.cfg − Main ESETS configuration file.

DESCRIPTION

The *esets.cfg* configuration file is used to configure ESETS modules. Under the term ESETS module we understand either main ESETS system control and scanning daemon **esets_daemon** or one of the ESETS agents introduced in the next paragraph. Note that the configuration file is stored in ESETS configuration directory. The configuration file is divided into sections corresponding to individual modules. It consists of the following sections.

[global]

Global section used to define common configuration options of main ESETS system control and scanning daemon module **esets_daemon** (see section **ESETS MODULE COMMON OPTIONS** of this manual page for details) as well as default values of the ESETS scanner common configuration options (see section **ESETS SCANNER COMMON OPTIONS** of this manual page for details).

[cgp], [cli], [dac], [ftp], [gwia], [http], [icap], [imap], [mda], [mird], [pac], [pipe], [pop3], [scan], [smfi], [smtp], [ssfi], [wwwi], [zmfi]

So called 'agent' sections (later in this document marked by string [agent]) used to define configuration options of **esets_cgp**, **esets_cli**, **esets_dac**, **esets_ftp**, **esets_gwia**, **esets_http**, **esets_icap**, **esets_imap**, **esets_mda**, **esets_mird**, **libesets_pac.so**, **esets_pipe**, **esets_pop3**, **esets_scan**, **esets_smfi**, **esets_smtp**, **esets_ssfi.so**, **esets_wwwi**, **esets_zmfi**, modules (see section **ESETS MODULE OPTIONS** of this manual page for details) as well as ESETS scanner common configuration options (see section **ESETS SCANNER COMMON OPTIONS** of this manual page for details) relevant when an appropriate agent used.

The purpose of [agent] sections implementation is that it makes possibility to define different values (related with the same configuration option) for different agents used. Lets assume one uses **esets_mda** agent to protect e-mail boxes and would like to protect also file system using **esets_dac** agent. The implementation of [agent] sections makes possible to define different ESETS scanner parameters for different kind of protection in this case.

Above discussed differentiation of the configuration options is even more sophisticated. The ESETS makes possible to define relevant configuration options individually according to the e-mail recipients and/or senders (implemented in **esets_mda**, **esets_pipe**, **esets_smfi**,**esets_smtp**, **esets_gwia** ,**esets_cli** modules) or according to the names of the users accessing file system objects (implemented in **esets_dac**, **libesets_pac.so** modules) or according to the clients (resp. servers) IP address (implemented in **esets_http**, **esets_ftp**, **esets_ssfi.so**, **esets_pop3**, **esets_imap,** modules). For this purpose a special user defined sections are introduced (later in this document marked by string [userspec]). To get further information on this functionality see section **USER SPECIFIC CONFIGURATION** of this manual page.

ESETS implements also rules concerned with inheritance of the relevant parameters from [global] to [agent] sections as well as from [agent] to [userspec] configuration sections. To get detailed information on the parameters inheritance, see section **CONFIGURATION FILE OPTIONS INHERITANCE** of this manual page.

In the present implementation of the ESETS there are three parameters types assumed to be used in the whole area of the configuration file(s):

- integer
- logical (bool)
- string

Integer parameters accept integer values, e.g.:

integer_parameter = 26

For integer parameter it is also possible to append unit K (1K = 1024), M (1M=1024*1024), G (1=1024*1024*1024), e.g.:

integer_parameter = 4K

Logical parameters accept two values: yes or no, e.g.:

bool_parameter = yes

or

bool_parameter = no

String parameters accept values which are not numbers nor logical codes. They can be put into quotation marks, e.g.:

string_parameter = "string value"

USER SPECIFIC CONFIGURATION

Agent sections (all but [global]) may contain option **user_config =** *path*. This option orders daemon **esets_daemon** to read additional user configuration options from the file specified by an argument *path*. To get description of this option, refer to section **ESETS MODULE SPECIAL OPTIONS**.

IMPORTANT: It is a mandatory to define different configuration files for different agents.

Format of this file is the same as format of ESETS main configuration file (esets.cfg) except the sections are headed with so called user specific configuration ID.

Example of an [userspec] section can be as follows:

```
[userspec]
        av_eml_footnote_modification_mask = "infected"
```

where 'userspec' is the user specific configuration ID. Meaning and lexical syntax of user specific configuration ID differs for different ESETS agents and thus its detailed description can be found in section **USER SPECIFIC CONFIGURATION** of an appropriate ESETS agent manual page.

IMPORTANT: Note that the definitions of parameters within the [userspec] sections has sense only for the ESETS scanner common configuration options (see section **ESETS SCANNER COMMON OPTIONS** of this manual page for details), i.e. all other options will be ignored regarding this functionality including all ESETS module options.

The ESETS allows also grouping of [userspec] sections. In order to define group of user specific configuration sections one has to define new section, so called parent section, where all options, assumed to be defined for all group members, have to be written. Then within individual [userspec] sections it is necessary to define parameter option **parent_id =** *parent_section_name*, where *parent_section_name* is the header name of parent section. To get description of this option, refer to the section **ESETS MODULE SPECIAL OPTIONS**.

EXAMPLE: Lets assume we have sections [peter] and [paul] to be a [userspec] sections. Thus instead of writing the same list of parameters into each of the sections area, we define new section [group] where we will pass all common parameters. The result will be as follows.

```
[group]
        av_eml_footnote_modification_mask = "infected"
        av_eml_subject_modification_mask = "infected"
        av_eml_header_modification_mask = "infected"

[peter]
        parent_id = "group"

[paul]
        parent_id = "group"
```

IMPORTANT: Note that the grouping operation is possible only among [userspec] sections appropriate to the one and the same ESETS agent module and only among [userspec] sections found within one and the same configuration file.

CONFIGURATION FILE OPTIONS INHERITANCE

The ESETS implements rules of inheritance of relevant configuration options from [global] to [agent] sections as well as from [agent] to [userspec] sections. Thanks to these rules the relevant parameters from the [global] section are taken into account also in [agent] sections, even they are not explicitly written within [agent] sections. The same relation is valid also between [agent] section and [userspec] sections.

IMPORTANT: Unless explicitly specified, the inheritance from [global] to [agent] sections is concerned with the ESETS scanner common configuration options (see section **ESETS SCANNER COMMON OPTIONS** of this manual page for details) and with the so called common ESETS module options (see section **ESETS MODULE COMMON OPTIONS** of this manual page for details). Note also that the inheritance from [agent] to [userspec] sections is concerned only with the ESETS scanner common configuration options (see section **ESETS SCANNER COMMON OPTIONS** of this manual page for details).

ESETS SCANNER COMMON OPTIONS

The ESETS scanner common configuration options define configuration of ESETS scanner kernel. These options can be specified from any ESETS module section and/or any special section. A full list of the ESETS scanner common configuration options is as follows:

action_av = *action*

type: string

default: *action* = "scan"

Defines action to be performed on all objects approaching Anti-Virus control. Possible values are "scan", "accept", "defer", "discard", "reject". Note that the values above are handled individually by every ESETS agent module. Thus to get description of the values please, refer to section **HANDLE OBJECT POLICY** of manual page of an appropriate agent.

action_av_infected = *action*

type: string

default: *action* = "reject"

Specifies the action performed on infected objects. Possible values are "accept", "defer", "discard", "reject". Note that the values above are handled individually by every ESETS agent module. Thus to get description of the values please, refer to section **HANDLE OBJECT POLICY** of manual page of an appropriate agent.

action_av_notscanned = *action*

type: string

default: *action* = "accept"

Specifies the action performed on objects that could not be scanned by anti-virus scanner, e.g. password protected archives, etc. Possible values are "accept", "defer", "discard", "reject". Note that the values above are handled individually by every ESETS agent module. Thus to get description of the values please, refer to section **HANDLE OBJECT POLICY** of manual page of an appropriate agent.

action_av_deleted = *action*

type: string

default: *action* = "discard"

Specifies the action performed on objects that has been deleted by anti-virus scanner, e.g. objects containing not relevant information after Anti-Virus cleaning process. Possible values are "accept", "defer", "discard", "reject". Note that the values above are handled individually by every ESETS agent module. Thus to get description of the values please, refer to section **HANDLE OBJECT POLICY** of manual page of an appropriate agent.

action_as = *action*

type: string

default: *action* = "accept"

Defines action to be performed on all e-mail messages approaching Anti-Spam control. Possible values are "scan", "accept", "defer", "discard", "reject". Note that the values above are handled individually by every ESETS agent module. Thus to get description of the values please, refer to section **HANDLE OBJECT POLICY** of manual page of an appropriate agent.

action_as_spam = *action*

type: string

default: *action* = "accept"

Specifies the action performed on e-mail messages found as spam. Possible values are "accept", "defer", "discard", "reject". Note that the values above are handled individually by every ESETS agent module. Thus to get description of the values please, refer to section **HANDLE OBJECT POLICY** of manual page of an appropriate agent.

action_as_notscanned = *action*

type: string

default: *action* = "accept"

Specifies the action performed on objects that could not be scanned by Anti-Spam scanner. Possible values are "accept", "defer", "discard", "reject". Note that the values above are handled individually by every ESETS agent module. Thus to get description of the values please, refer to section **HANDLE OBJECT POLICY** of manual page of an appropriate agent.

av_scan_obj_files = *yes/no*

type: bool

default: yes

Enables/disables scanning of regular files.

av_scan_obj_archives = *yes/no*

type: bool

default: yes

Enables/disables scanning of archives (.ZIP, .RAR, .ARJ, etc.).

Note that due to the on-access scanner optimization reason, the default value of this parameter is redefined by the parameter **av_scan_obj_archives** within agent sections [pac] and [dac]. Refer to libesets_pac.so(1) and esets_dac(1) manual page for details.

av_scan_obj_mime = *yes/no*

type: bool

default: yes

Enables/disables scanning of MIME archives, i.e. e-mail messages in raw format.

Note that due to the on-access scanner optimization reason, the default value of this parameter is redefined by the parameter **av_scan_obj_mime** within agent sections [pac] and [dac]. Refer to libesets_pac.so(1) and esets_dac(1) manual page for details.

av_scan_obj_mailbox = *yes/no*

type: bool

default: yes

Enables/disables scanning of various mailboxes.

Note that due to the on-access scanner optimization reason, the default value of this parameter is redefined by the parameter **av_scan_obj_mailbox** within agent sections [pac] and [dac]. Refer to libesets_pac.so(1) and esets_dac(1) manual page for details.

av_scan_obj_rtp = *yes/no*

type: bool

default: yes

Enables/disables scanning of runtime-packers.

Note that due to the on-access scanner optimization reason, the default value of this parameter is redefined by the parameter **av_scan_obj_rtp** within agent sections [pac] and [dac]. Refer to libesets_pac.so(1) and esets_dac(1) manual page for details.

av_scan_obj_sfx = *yes/no*

type: bool

default: yes

Enables/disables scanning of self-extracting archives.

Note that due to the on-access scanner optimization reason, the default value of this parameter is redefined by the parameter **av_scan_obj_sfx** within agent sections [pac] and [dac]. Refer to libesets_pac.so(1) and esets_dac(1) manual page for details.

av_scan_app_adware = *yes/no*

type: bool

default: yes

Enables/disables scanning of adware, spyware, etc.

av_scan_app_unsafe = *yes/no*

type: bool

default: no

Enables/disables scanning of potentially dangerous applications.

av_scan_app_unwanted = *yes/no*

type: bool

default: no

Enables/disables scanning of unwanted applications.

av_scan_pattern = *yes/no*

type: bool

default: yes

Enables/disables use of virus signatures database while scanning.

av_scan_heur = *yes/no*

type: bool

default: yes

Enables/disables use of heuristics method while scanning.

av_scan_adv_heur = *yes/no*

type: bool

default: yes

Enables/disables use of advanced heuristics method while scanning.

Note that due to the on-access scanner optimization reason, the default value of this parameter is redefined by the parameter **av_scan_adv_heur** within agent sections [pac] and [dac]. Refer to libesets_pac.so(1) and esets_dac(1) manual page for details.

av_scan_ext = *extlist*

type: string

default: *extlist* = ""

Defines list of only extensions of files to be scanned. The string argument *extlist* is assumed to be of the format "ext1:ext2:ext3:...", where ext1, ext2, ext3 etc. are specified extensions. If not defined, all files are scanned regardless of extension. If defined, the **av_scan_ext_exclude** parameter is ignored.

av_scan_ext_exclude = *extlist*

type: string

default: *extlist* = ""

Defines list of only extensions of files to be excluded from scanning, i.e. all files are scanned except these defined by the list. The string argument *extlist* is assumed to be of the format "ext1:ext2:ext3:...", where ext1, ext2, ext3 etc. are specified extensions. If parameter **av_scan_ext** defined, this parameter is ignored.

av_exclude = *list*

type: string

default: *list* = ""

Defines list of filesystem objects to be excluded from scanning, e.g. all files are scanned except those defined by the list. The string argument *list* is assumed to be of the format "path1:idef1:path2:idef2:...". Note, that each element of the list must be terminated by colon. Elements path1, path2 etc. are absolute paths to the files or directories excluded. Note, that to exclude directory the "/*.*" wildcard characters must be written at the end of the path. Specification idef1, idef2, etc. is reserved for the future use (write empty strings instead).

av_scan_smart = *yes/no*

type: bool

default: yes

Enables/disables so called Smart Optimization of scanner, i.e. optimal scanner settings to ensure the most efficient scanning level, while simultanneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods while applying them to specific file types. The Smart Optimization is not rigidly defined within the product. The ESET Development Team is continuously implementing new changes which then get integrated into your product via the regular updates.

av_clean_mode = *mode*

type: string

default: *mode* = "standard"

Defines cleaning mode of scanned object. Possible values are:

none No cleaning.

standard
In this mode all infected files will be cleaned by proper cleaning algorithm or deleted, except those whose deletion would cause also usefull data loss, e.g. archives containing mixture of infected and clean files, etc. Note that in ESET Mail Security and ESET Gateway Security this mode is handled in the same way as rigorous mode (see below).

strict In this mode all infected files will be cleaned by proper cleaning algorithm or deleted, except the system files. Note that in ESET Mail Security and ESET Gateway Security this mode is handled in the same way as rigorous mode (see below).

rigorous
In this mode all infected files will be cleaned by proper cleaning algorithm or deleted.

delete In this mode all infected files will be deleted.

Note that some ESETS agent modules are built to work in read-only mode, i.e. the objects scanned are not cleaned in any way and thus the parameter is ignored. To get information on the read-only mode of agent please, refer to section **HANDLE OBJECT POLICY** of manual page of an appropriate agent.

av_quarantine_enabled = *yes/no*

type: bool

default: no

If enabled, every infected object is quarantined in case it is cleaned by ESETS.

av_scan_obj_max_size = *size*

type: integer

default: *size* = 0

Specifies the maximum size *size* (measured in bytes) of a single scanned file. Zero (0) means no limit. When a scan is terminated prematurely because this limit was reached, the scanned object is considered as not scanned.

Note, for size setting is possible use base unit specification (Ki, Mi or Gi). For example 4 megabytes can be written by **av_scan_obj_max_size=4Mi**

av_scan_archive_max_level = *lvl*

type: integer

default: *lvl* = 10

Specifies the maximum level *lvl* an archive is descended, unpacked and scanned. When a scan is terminated prematurely because this limit was reached, the scanned object is considered as not scanned.

Note that due to the on-access scanner optimization reason, the default value of this parameter may be redefined within agent sections [pac] and [dac] for special case of file creation events catched by on-access scanner. This can be done by proper definition of parameters **av_create_scan_def_arch** and **av_create_scan_archive_max_level**. Refer to libesets_pac.so(1) and esets_dac(1) manual page for details.

av_scan_archive_max_size = *size*

type: integer

default: *size* = 0

Specifies the maximum unpacked size*size* (measured in bytes) of a file from archive, which will be scanned. Zero (0) means no limit. When a scan is terminated prematurely because this limit was reached, the scanned object is considered as not scanned.

Note that due to the on-access scanner optimization reason, the default value of this parameter may be redefined within agent sections [pac] and [dac] for special case of file creation events catched by on-access scanner. This can be done by proper definition of parameters **av_create_scan_def_arch** and **av_create_scan_archive_max_size**. Refer to libesets_pac.so(1) and esets_dac(1) manual page for details.

av_scan_archive_timeout = *time*

type: integer

default: *time* = 0

Specifies the maximum scanning time *time* of a single archive level object scan in seconds. Zero (0) means no timeout. When a scan is terminated prematurely because this limit was reached, the scanned object is considered as not scanned. Note that this option represents a soft limit by means the timeout is only checked in between two archive level objects scans.

av_eml_subject_modification_mask = *mask*

type: string

default: *mask* = ""

This option is used in ESET Mail Security to trigger replacement of the scanned e-mail 'Subject'

by predefined formatted text message template. A string argument *mask* is used to set mode of the text replacement. Five values of this argument are supported appropriate to the relevant status of scanning and also cleaning process of controlled e-mail messages:

clean Replace subject in clean e-mail messages.

cleaned
Replace subject in cleaned e-mail messages.

deleted Replace subject in deleted e-mail messages.

infected
Replace subject in infected e-mail messages.

notscanned
Replace subject in not scanned e-mail messages.

as_spam
Insert headers "X-ESET-Antispam: SPAM", "X-ESET-AS", "X-I-ESET-AS" into spam e-mail messages.

as_ham
Insert headers "X-ESET-Antispam: OK", "X-ESET-AS", "X-I-ESET-AS" into not spam e-mail messages.

In case the e-mail header does not contain 'Subject' header-field the parameter is ignored.

av_eml_subject_template = *template*

type: string

default: *template* = "%avstatus%"

A template used to replace original 'Subject' header-field in the scanned e-mail. The template may contain the following directives:

%avstatus%
This directive is replaced by Anti-Virus scanning status.

%virus%
This directive is replaced by virus threat detected by Anti-Virus scanner.

as_eml_subject_template = *template*

type: string

default: *template* = "[%asstatus%]"

A template used to replace original 'Subject' header-field in the scanned e-mail. The order of modification of subject is: as_eml_subject_template and then av_eml_subject_template. The template may contain the following directives:

%asstatus%
This directive is replaced by Antispam scanning status.

as_eml_header_modificatio = *yes/no*

type: bool

default: no

Add a new headers appended by antispam into email.

av_eml_header_modification_mask = *mask*

type: string

default: *mask* = ""

This option is used in ESET Mail Security to trigger insertion of the ESETS specific header-field as a predefined formatted text message template into scanned e-mail message. A string argument *mask* is used to set mode of the text replacement. Five values of this argument are supported appropriate to the relevant status of scanning and also cleaning process of controlled e-mail messages:

clean Insert header into clean e-mail messages.

cleaned
Insert header into cleaned e-mail messages.

deleted Insert header into deleted e-mail messages.

infected
Insert header into infected e-mail messages.

notscanned
Insert header into not scanned e-mail messages.

av_eml_header_template = *template*

type: string

default: *template* = "%avstatus%"

A template used to be inserted into header of the scanned e-mail. The template may contain the following directives:

%avstatus%
This directive is replaced by Anti-Virus scanning status.

%virus%
This directive is replaced by virus threat detected by Anti-Virus scanner.

av_eml_footnote_modification_mask = *mask*

type: string

default: *mask* = "clean:infected:notscanned"

This option is used in ESET Mail Security to trigger insertion of so called 'ESETS footnote' into the scanned e-mail. The ESETS footnote contains detailed information about the scanning process. A string argument *mask* is used to set mode of the text replacement. Three values of this argument are supported appropriate to the relevant status of scanning process of controlled e-mail messages:

clean Insert footnote into clean e-mail messages.

infected
Insert footnote into infected e-mail messages.

notscanned
Insert footnote into not scanned e-mail messages.

av_eml_footnote_template_clean = *template*

type: string

default: *template* = "PREDEFINED"

A template used to be inserted into clean e-mail message body. Please refer to ESETS main configuration file (esets.cfg) to get default of this parameter. The template may contain the following

directives:

%version%
This directive is replaced by Anti-Virus virus signature database version string.

%log%
This directive is replaced by Anti-Virus logging output concerned with this message.

av_eml_footnote_template_infected = *template*

type: string

default: *template* = "PREDEFINED"

A template used to be inserted into infected e-mail message body. Please refer to ESETS main configuration file (esets.cfg) to get default of this parameter. The template may contain the following directives:

%version%
This directive is replaced by Anti-Virus virus signature database version string.

%log%
This directive is replaced by Anti-Virus logging output concerned with this message.

av_eml_footnote_template_notscanned = *template*

type: string

default: *template* = "PREDEFINED"

A template used to be inserted into not scanned e-mail message body. Please refer to ESETS main configuration file (esets.cfg) to get default of this parameter. The template may contain the following directives:

%version%
This directive is replaced by Anti-Virus virus signature database version string.

%log%
This directive is replaced by Anti-Virus logging output concerned with this message.

av_eml_footnote_log_all = *yes/no*

type: bool

default: no

If enabled, ESETS footnote inserted into the e-mail body (enabled by option **av_eml_footnote_modification_mask**) will contain also logging output concerned with the clean objects of scanned e-mail messages.

ESETS MODULE OPTIONS

The ESETS module options are configuration options used to define behavior of the ESETS modules. In other words, these are all ESETS options except the ESETS scanner common options.

For the reference purposes we divide ESETS module options on the **ESETS MODULE COMMON OPTIONS**, **ESETS MODULE PRIVATE OPTIONS** and **ESETS MODULE SPECIAL OPTIONS**.

ESETS MODULE COMMON OPTIONS

These configuration file options are defined for all ESETS modules. This is a full list of the ESETS module common options:

syslog_class = *class*

type: string

default: *class* = "error:warning:summall:part"

Defines so called ESETS logging class. Following classes are supported:

error Error messages are logged (priority LOG_ERR).

warning
Warning messages are logged (priority LOG_WARNINF).

summ Summarizing lines of logging output are logged for infected objects (priority LOG_NOTICE).

summall
Summarizing lines of logging output for all scanned objects are logged (priority LOG_NOTICE).

part Particular lines of logging output are logged for infected objects (priority LOG_NOTICE).

partall Particular lines of logging output for all scanned objects are logged (priority LOG_NOTICE).

info Informational messages are logged (priority LOG_INFO).

debug Debug information messages are logged (priority LOG_DEBUG).

Refer to the section **LOGGING** of this manual page for details.

syslog_facility = *facility*

type: string

default: *facility* = "daemon"

Defines syslog facility to be used for syslog logging of the ESETS module. The following syslog facilities are supported:

none No syslog output.

kern LOG_KERN

user LOG_USER

mail LOG_MAIL

daemon
LOG_DAEMON

auth LOG_AUTH

syslog LOG_SYSLOG

lpr LOG_LPR

news LOG_NEWS

uucp LOG_UUCP

cron LOG_CRON

authpriv
LOG_AUTHPRIV

ftp LOG_FTP

local0 LOG_LOCAL0

local1 LOG_LOCAL1

local2 LOG_LOCAL2

local3 LOG_LOCAL3

local4 LOG_LOCAL4

local5 LOG_LOCAL5

local6 LOG_LOCAL6

local7 LOG_LOCAL7

To get more information on the syslog refer to the manual pages syslog(2), syslog(3)).

ESETS MODULE PRIVATE OPTIONS

To get description of ESETS MODULE PRIVATE OPTIONS of agent, please refer to an appropriate agent manual page.

ESETS MODULE SPECIAL OPTIONS

This section describes list of special options that does not fit to the other lists of options.

user_config = *path*

type: string

default: no default

This configuration option causes reading of user configuration options for an appropriate ESETS agent module from the file specified by string argument *path*. If an argument *path* is not an absolute path name, it is interpreted relative to the directory containing main ESETS configuration file esets.cfg. To get detailed information concerned with this option, see section **USER SPECIFIC CONFIGURATION** of this manual page.

parent_id = *string*

type: string

default: no default

This configuration option causes reading and setting of configuration options from special section referenced by string argument *string*. By using this mechanism grouping of so called special sections is allowed. To get detailed information concerned with this option, see section **USER SPECIFIC CONFIGURATION** of this manual page.

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