Contents

1. Introduction ......................................................... 4
  1.1 System requirements ........................................... 4
  1.2 Types of protection ............................................. 4
  1.3 User interface ................................................... 4

2. Installation ........................................................... 5
  2.1 Typical installation ............................................. 5
  2.2 Custom installation ............................................ 6

3. Work with ESET File Security ............................... 7
  3.1 eShell .............................................................. 7
    3.1.1 Usage ......................................................... 8
    3.1.2 Commands .................................................... 11
    3.1.2.1 Context - AV ............................................ 13
    3.1.2.2 Context - AV EMAIL ................................. 15
    3.1.2.3 Context - AV EMAIL GENERAL ..................... 16
    3.1.2.4 Context - AV EMAIL GENERAL LIMITS ARCHIVE 16
    3.1.2.5 Context - AV EMAIL GENERAL LIMITS OBJECTS 17
    3.1.2.6 Context - AV EMAIL GENERAL OBJECTS .......... 18
    3.1.2.7 Context - AV EMAIL GENERAL OPTIONS .......... 19
    3.1.2.8 Context - AV EMAIL GENERAL OTHER ............ 20
    3.1.2.9 Context - AV EMAIL PROTOCOL POP3 .......... 21
    3.1.2.10 Context - AV EMAIL PROTOCOL POP3S .......... 22
    3.1.2.11 Context - AV LIMITS ARCHIVE .................. 23
    3.1.2.12 Context - AV LIMITS OBJECTS .................... 24
    3.1.2.13 Context - AV NETFILTER ......................... 24
    3.1.2.14 Context - AV NETFILTER PROTOCOL SSL ....... 26
    3.1.2.15 Context - AV NETFILTER PROTOCOL SSL CERTIFICATE .................................................. 27
    3.1.2.16 Context - AV OBJECTS ............................... 28
    3.1.2.17 Context - AV OPTIONS .............................. 30
    3.1.2.18 Context - AV OTHER ................................. 32
    3.1.2.19 Context - AV REALTIME ............................. 33
    3.1.2.20 Context - AV REALTIME DISK ..................... 34
    3.1.2.21 Context - AV REALTIME EVENT ................... 35
    3.1.2.22 Context - AV REALTIME EXECUTABLE ............ 37
    3.1.2.23 Context - AV REALTIME EXECUTABLE FROM REMOVABLE ........................................... 46
    3.1.2.24 Context - AV REALTIME LIMITS ARCHIVE ....... 38
    3.1.2.25 Context - AV REALTIME LIMITS OBJECTS ........ 39
    3.1.2.26 Context - AV REALTIME OBJECTS ............... 39
    3.1.2.27 Context - AV REALTIME ONWRITE ............... 42
    3.1.2.28 Context - AV REALTIME ONWRITE ARCHIVE .... 43
    3.1.2.29 Context - AV REALTIME OPTIONS ............... 43
    3.1.2.30 Context - AV REALTIME OTHER .................. 45
    3.1.2.31 Context - AV REALTIME REMOVABLE ............ 46
    3.1.2.32 Context - AV WEB ..................................... 47
    3.1.2.33 Context - AV WEB ADDRESSMGMT ................ 48
    3.1.2.34 Context - AV WEB LIMITS ARCHIVE ............. 50
    3.1.2.35 Context - AV WEB LIMITS OBJECTS ............. 50
    3.1.2.36 Context - AV WEB OBJECTS ...................... 51
    3.1.2.37 Context - AV WEB OPTIONS ....................... 53
    3.1.2.38 Context - AV WEB OPTIONS BROWSERS .......... 55
    3.1.2.39 Context - AV WEB OTHER .......................... 56
    3.1.2.40 Context - AV WEB PROTOCOL HTTP ............. 56
    3.1.2.41 Context - AV WEB PROTOCOL HTTPS ............ 57
    3.1.2.42 Context - GENERAL ................................. 58
    3.1.2.43 Context - GENERAL ACCESS ........................ 58
    3.1.2.44 Context - GENERAL ESHELL ......................... 60
    3.1.2.45 Context - GENERAL ESHHELL COLOR ............ 61
    3.1.2.46 Context - GENERAL ESHHELL OUTPUT ............ 68
    3.1.2.47 Context - GENERAL ESHHELL STARTUP .......... 69
    3.1.2.48 Context - GENERAL ESHHELL VIEW ............... 69
    3.1.2.49 Context - GENERAL PERFORMANCE ............... 72
    3.1.2.50 Context - GENERAL PROXY ......................... 73
    3.1.2.51 Context - GENERAL QUARANTINE RESCAN .......... 74
    3.1.2.52 Context - GENERAL REMOTE ........................ 75
    3.1.2.53 Context - GENERAL REMOTE SERVER PRIMARY .... 75
    3.1.2.54 Context - GENERAL REMOTE SERVER SECONDARY .................................................. 77
    3.1.2.55 Context - GENERAL TS.NET ......................... 78
    3.1.2.56 Context - GENERAL TS.NET STATISTICS .......... 80
    3.1.2.57 Context - SCANNER ................................. 81
    3.1.2.58 Context - SCANNER LIMITS ARCHIVE ............ 83
    3.1.2.59 Context - SCANNER LIMITS OBJECTS ............ 83
    3.1.2.60 Context - SCANNER OBJECTS ...................... 84
    3.1.2.61 Context - SCANNER OPTIONS ....................... 86
    3.1.2.62 Context - SCANNER OTHER ........................ 88
    3.1.2.63 Context - SERVER ..................................... 90
    3.1.2.64 Context - TOOLS ....................................... 90
    3.1.2.65 Context - TOOLS ACTIVITY ......................... 91
    3.1.2.66 Context - TOOLS LOG ............................... 92
    3.1.2.67 Context - TOOLS LOG CLEANING .................. 95
    3.1.2.68 Context - TOOLS LOG OPTIMIZE ................... 95
    3.1.2.69 Context - TOOLS NOTIFICATION ................... 96
    3.1.2.70 Context - TOOLS NOTIFICATION EMAIL .......... 96
    3.1.2.71 Context - TOOLS NOTIFICATION MESSAGE FORMAT .................................................. 99
    3.1.2.72 Context - TOOLS NOTIFICATION MESSAGE CHECK .................................................. 103
    3.1.2.73 Context - TOOLS NOTIFICATION WINPOPUP ....... 100
    3.1.2.74 Context - TOOLS SCHEDULER ....................... 101
    3.1.2.75 Context - TOOLS SCHEDULER EVENT ............. 102
    3.1.2.76 Context - TOOLS SCHEDULER FAILSAFE .......... 103
    3.1.2.77 Context - TOOLS SCHEDULER PARAMETERS CHECK .................................................. 103
    3.1.2.78 Context - TOOLS SCHEDULER PARAMETERS EXTERNAL .................................................. 104
    3.1.2.79 Context - TOOLS SCHEDULER PARAMETERS SCANID .................................................. 105
    3.1.2.80 Context - TOOLS SCHEDULER PARAMETERS UPDATE .................................................. 106
    3.1.2.81 Context - TOOLS SCHEDULER REPEAT ............. 107
    3.1.2.82 Context - TOOLS SCHEDULER STARTUP ........... 107
    3.1.2.83 Context - UPDATE ..................................... 108
    3.1.2.84 Context - UPDATE CONNECTION ................... 111
    3.1.2.85 Context - UPDATE MIRROR ......................... 112
    3.1.2.86 Context - UPDATE MIRROR CONNECTION .......... 114
    3.1.2.87 Context - UPDATE MIRROR SERVER ............... 115
    3.1.2.88 Context - UPDATE NOTIFICATION ............... 116
    3.1.2.89 Context - UPDATE PROXY ............................ 117
    3.1.2.90 Context - UPDATE SYSTEM .......................... 119

3.2 Automatic exclusions ............................................ 119

3.3 Import and export settings ................................... 120

3.4 Remote administration ......................................... 120

3.5 Licenses .......................................................... 121

4. Glossary ............................................................ 122
  4.1 Types of infiltration ........................................... 122
    4.1.1 Viruses ..................................................... 122
    4.1.2 Worms ....................................................... 122
    4.1.3 Trojan horses ............................................... 122
    4.1.4 Rootkits ...................................................... 123
    4.1.5 Adware ........................................................ 123
    4.1.6 Spyware ....................................................... 123
    4.1.7 Potentially unsafe applications ....................... 124
    4.1.8 Potentially unwanted applications ................... 124
1. Introduction

ESET File Security for Microsoft Server Core is an integrated solution specially designed for the Microsoft Windows Server Core environment. ESET File Security delivers effective and robust protection against various types of malware and provides two types of protection: Antivirus and Antispyware.

Some key features of ESET File Security:

- **Automatic Exclusions** — automatic detection and exclusion of critical server files for easy operation.
- **eShell** (ESET Shell) - new command line control interface that offers advanced users and administrators more comprehensive options to manage ESET products.
- **SelfDefense** — technology that protects ESET security solutions from being modified or deactivated.


1.1 System requirements

Supported Operating Systems:

- Microsoft Windows Server 2008 (x86 and x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012

Hardware requirements depend on the operating system version in use. We recommend reading the Microsoft Windows Server product documentation for more detailed information on hardware requirements.

1.2 Types of protection

There are two types of protection:

- **Antivirus protection**
- **Antispyware protection**

Antivirus and Antispyware protection is one of the basic functions of the ESET File Security product. This protection guards against malicious system attacks by controlling file, email and Internet communication. If a threat with malicious code is detected, the Antivirus module can eliminate it by blocking it and then cleaning, deleting or moving it to quarantine.

1.3 User interface

ESET File Security has command line interface called eShell, which was designed to be as intuitive as possible.
2. Installation

After purchasing ESET File Security, the installer can be downloaded from ESET's website (www.eset.com) as an .msi package. Once you launch the installer, the installation wizard will guide you through the basic setup. There are two types of installation available with different levels of setup details:

1. Typical Installation
2. Custom Installation

**NOTE:** We highly recommend installing ESET File Security on a freshly installed and configured OS, if possible. However, if you do need to install it on an existing system, the best to do is to uninstall previous version of ESET File Security, restart the server and install the new ESET File Security afterwards.

2.1 Typical Installation

Typical installation mode quickly installs ESET File Security with minimal configuration during the installation process. Typical installation is the default installation mode and is recommended if you do not have particular requirements for specific settings yet. After ESET File Security has been installed on your system, you can modify the options and configuration settings at any time. This user guide describes these settings and functionality in detail. The Typical installation mode settings provide excellent security coupled with ease of use and high system performance.

After selecting the installation mode and clicking Next, you will be prompted to enter your username and password. This plays a significant role in providing constant protection to your system, as your username and password allows automatic virus signature database Updates.

Enter the username and password, which you received after the purchase or registration of the product, into the corresponding fields. If you do not currently have your username and password available, it can be entered directly from the program at a later time.

The next step is to configure the ThreatSense.Net Early Warning System. The ThreatSense.Net Early Warning System helps ensure that ESET is immediately and continuously informed about new infiltrations in order to quickly protect its customers. This system allows new threats to be submitted to ESET's Threat Lab, where they are analyzed, processed and added to the virus signature database. By default, the Enable ThreatSense.Net Early Warning System option is selected. Click Advanced setup... to modify detailed settings about the submission of suspicious files.

The next step in the installation process is to configure Detection of potentially unwanted applications. Potentially unwanted applications are not necessarily malicious, but can often negatively affect the behavior of your operating system. See the Potentially unwanted applications chapter for more details.

These applications are often bundled with other programs and may be difficult to notice during the installation process. Although these applications usually display a notification during installation, they can easily be installed without your consent.

Select the Enable detection of potentially unwanted applications option to allow ESET File Security to detect this type of applications. If you do not wish to use this functionality, select Disable detection of potentially unwanted applications.

The final step in Typical installation mode is to confirm the installation by clicking the Install button.
2.2 Custom installation

Custom installation is designed for those who would like to configure ESET File Security during the installation process.

After selecting the installation mode and clicking Next, you will be prompted to select a destination location for the installation. By default, the program installs in C:\Program Files\ESET\ESET File Security. Click Browse... to change this location (not recommended).

Next, Enter your Username and Password. This step is the same as the Typical installation mode step (see "Typical installation").

After entering your username and password, click Next to proceed to Configure your Internet connection.

If you use a proxy server, it must be correctly configured for virus signature updates to work correctly. If you would like to have the proxy server configured automatically, select the default setting I am unsure if my Internet connection uses a proxy server. Use the same settings as Internet Explorer (Recommended) and click Next. If you do not use a proxy server, select the I do not use a proxy server option.

If you prefer to enter the proxy server details yourself, you can configure the proxy server settings manually. To configure your proxy server settings, select I use a proxy server and click Next. Enter the IP address or URL of your proxy server in the Address field. In the Port field, specify the port where the proxy server accepts connections (3128 by default). If your proxy server requires authentication, enter a valid Username and Password to grant access to the proxy server. Proxy server settings can also be copied from Internet Explorer if desired. Once the proxy server details are entered, click Apply and confirm the selection.

Click Next to proceed to Configure automatic update settings. This step allows you to designate how automatic program component updates will be handled on your system. Click Change... to access the advanced settings.

If you do not want program components to be updated, select the Never update program components option. Select the Ask before downloading program components option to display a confirmation window before downloading program components. To download program component upgrades automatically, select the Always update program components option.

NOTE: After a program component update, a restart is usually required. We recommend selecting the Never restart computer option. The latest component updates will come into effect after the next server restart (whether it is scheduled, manual or otherwise). You can choose Offer computer restart if necessary if you would like to be reminded to restart the server after the components were updated. With this setting, you can restart the server right away or postpone the restart and perform it at a later time.

The next installation window offers the option to set a password to protect your program settings. Select the Protect configuration settings with a password option and choose a password to enter in the New password and Confirm new password fields.

The next two installation steps, ThreatSense.Net Early Warning System and Detection of potentially unwanted applications are the same as the Typical installation mode steps (see "Typical installation").

Click Install in the Ready to install window to complete installation.
3. Work with ESET File Security

3.1 eShell

eShell (short for ESET Shell) is a command line interface for ESET File Security. eShell has all the features and options that the GUI normally gives you. eShell lets you configure and administer the whole program. It also provides you with the option of using automation by running scripts in order to configure, modify configuration or perform an action.

This section explains how to navigate and use eShell as well as lists all the commands with the description of what particular command is used for and what it does.

There are two modes in which eShell can be run:

- **Interactive mode** - this is useful when you want to work with eShell (not just execute single command) for tasks such as changing configuration, viewing logs, etc. You can also use interactive mode if you are not familiar with all the commands yet. Interactive mode will make it easier for you when navigating through eShell. It also shows you available commands you can use within a particular context.

- **Single command / Batch mode** - you can use this mode if you only need to execute a command without entering the interactive mode of eShell. This can be done from the Windows Command Prompt by typing in `eshell` with appropriate parameters. For example:

```
eshell set av document status enabled
```

**NOTE**: In order to run eShell commands from Windows Command Prompt or to run batch files, you need to have this function enabled first (command `set general access batch` needs to be executed in interactive mode). For further information about the set batch command click [here](#).

To enter interactive mode of eShell, navigate to a directory where you have installed the ESET File Security (e.g. `C:\Program Files\ESET\ESET File Security\`) and simply type in `eshell` and press the Enter key. If you want to avoid navigating to this folder each time you wish to enter eShell you can use SETX command. For example:

```
SETX Path %Path%;"C:\Program Files\ESET\ESET File Security"
```

Reboot of the server is required in order to load new variables. After this, you can run the eShell just by typing `eshell` from any place.

When you run eShell in interactive mode a status screen will display.
If you want to get a quick overview and some guidance, you can use `guide` command to see this information.

It shows you some basic examples of how to use eShell with Syntax, Prefix, Command path, Abbreviated forms, Aliases, etc. This is basically a quick guide to eShell.

**NOTE:** Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

### 3.1.1 Usage

**Syntax**

Commands must be formatted in the correct syntax to function and can be composed of a prefix, context, arguments, options, etc. This is the general syntax used throughout the eShell:

```
[prefix] [command path] <command> [arguments]
```

**Example (this activates document protection):**

```
SET     AV DOCUMENT     STATUS     ENABLED
```

- **SET** - a prefix
- **AV DOCUMENT** - path to a particular command, a context where this command belong
- **STATUS** - the command itself
- **ENABLED** - an argument for the command

Using `HELP` or `?` with a command will display the syntax for that particular command. For example, `CLEANLEVEL HELP` will show you the syntax for `CLEANLEVEL` command:

SYNTAX:

```
[get] | restore cleanlevel
      set cleanlevel none | normal | strict
```

You may notice that `[get]` is in brackets. It designates that the prefix `get` is default for the `cleanlevel` command. This means that when you execute `cleanlevel` without specifying any prefix, it will actually use the default prefix (in this case `get cleanlevel`). Using commands without a prefix saves time when typing. Usually `get` is the default prefix for most commands, but you need to be sure what the default prefix is for particular command and that it is exactly what you want to execute.

**NOTE:** Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

**Prefix / Operation**

A prefix is an operation. The `GET` prefix will give you information about how a certain feature of ESET File Security is configured or show you the status (such as `GET AV STATUS` will show you current protection status). The `SET` prefix will configure functionality or change its status (`SET AV STATUS ENABLED` will activate protection).

```
Syntax:  [prefix] [command path] <command> [arguments]
```

For example, to activate document protection enter:

```
set AV DOCUMENT STATUS ENABLED
```

**Operation**

The command may or may not support any of the operations. Operations change the meaning of the command. For example `get av status` returns the status of antivirus protection while `set av status enabled` enables antivirus protection. An example of a command with no prefix is `exit`.

Available are the following operations:

- `get`, `set`, `select`, `add`, `remove` (prefixes)
- `clear`, `start`, `stop`, `pause`, `resume` (commands)
- `import`, `export` (context)

For the meaning of the operation in relation to the specific command see `help`. Enter: `{command} ?`
These are the prefixes that eShell lets you use. A command may or may not support any of the prefixes:

- **GET** - returns current setting/status
- **SET** - sets value/status
- **SELECT** - selects an item
- **ADD** - adds an item
- **REMOVE** - removes an item
- **CLEAR** - removes all items/files
- **START** - starts an action
- **STOP** - stops an action
- **PAUSE** - pauses an action
- **RESUME** - resumes an action
- **RESTORE** - restores default settings/object/file
- **SEND** - sends an object/file
- **IMPORT** - imports from a file
- **EXPORT** - exports to a file

Prefixes such as **GET** and **SET** are used with many commands, but some commands (such as **EXIT**) do not use a prefix.

**Command path / Context**

Commands are placed in contexts which form a tree structure. The top level of the tree is root. When you run eShell, you are at the root level:

```
eShell>
```

You can either execute a command from here, or enter the context name to navigate within the tree. For example, when you enter **TOOLS** context, it will list all commands and sub-contexts that are available from here.

```
.. Administrator\Windows\system32\cmd.exe - eshell
.. Administrator\Windows\system32\cmd.exe - eshell
.. Administrator\Windows\system32\cmd.exe - eshell
.. Administrator\Windows\system32\cmd.exe - eshell
.. Administrator\Windows\system32\cmd.exe - eshell
.. Administrator\Windows\system32\cmd.exe - eshell
.. Administrator\Windows\system32\cmd.exe - eshell
.. Administrator\Windows\system32\cmd.exe - eshell
.. Administrator\Windows\system32\cmd.exe - eshell
.. Administrator\Windows\system32\cmd.exe - eshell
```

Yellow items are commands you can execute and grey items are sub-contexts you can enter. A sub-context contain further commands.

If you need to return back to a higher level, use **..** (two dots). For example, say you are here:

```
eShell av options>
```

Type **..** and it will get you up one level, to:

```
eShell av>
```

If you want to get back to root from **eShell av options>** (which is two levels lower from root), simply type **.. ..** (two dots and two dots separated by space). By doing so, you will get two levels up, which is root in this case. You can use this no matter how deep within the context tree you are. Use the appropriate number of **..** as you need to get to the desired level.

The path is relative to the current context. If the command is contained in the current context, do not enter a path. For example, to execute **GET AV STATUS** enter:

```
GET AV STATUS - if you are in the root context (command line shows eShell>)
GET STATUS - if you are in the context AV (command line shows eShell av>)
.. GET STATUS - if you are in the context AV OPTIONS (command line shows eShell av options>)
```
Argument
An argument is an action which is performed for a particular command. For example, command `CLEANLEVEL` can be used with following arguments:

- `none` - Do not clean
- `normal` - Standard cleaning
- `strict` - Strict cleaning

Another example are the arguments `ENABLED` or `DISABLED`, which are used to enable or disable a certain feature or functionality.

Abbreviated form / Shortened commands
eShell allows you to shorten contexts, commands and arguments (provided the argument is a switch or an alternative option). It is not possible to shorten a prefix or argument that are concrete values such as a number, name or path.

Examples of the short form:

```
set status enabled    =>    set stat en
add av exclusions C:\path\file.ext  =>  add av exc C:\path\file.ext
```

In a case where two commands or contexts start with same letters (such as `ABOUT` and `AV`, and you enter `A` as shortened command), eShell will not be able to decide which command of these two you want to run. An error message will display and list commands starting with "A" which you can choose from:

```
eShell>a
The following command is not unique: a
The following commands are available in this context:
   ABOUT - Shows information about program
   AV - Changes to context av
```

By adding one or more letters (e.g. `AB` instead of just `A`) eShell will execute `ABOUT` command since it is unique now.

**NOTE:** When you want to be sure that a command executes the way you need, we recommend that you do not abbreviate commands, arguments, etc. and use the full form. This way it will execute exactly as you need and prevent unwanted mistakes. This is especially true for batch files / scripts.

Aliases
An alias is an alternative name which can be used to execute a command (provided that the command has an alias assigned). There are few default aliases:

```
(global) help - ?
(global) close - exit
(global) quit - exit
(global) bye - exit
warnlog - tools log events
virlog - tools log detections
```

"(global)" means that the command can be used anywhere regardless of current context. One command can have multiple aliases assigned, for example command `EXIT` has alias `CLOSE`, `QUIT` and `BYE`. When you want to exit eShell, you can use the `EXIT` command itself or any of its aliases. Alias `VIRLOG` is an alias for command `DETECTIONS` which is located in `TOOLS LOG` context. This way the detections command is available from `ROOT` context, making it easier to access (you don't have to enter `TOOLS` and then `LOG` context and run it directly from `ROOT`).

eShell allows you to define your own aliases. Click [here](#) to see how you can create an alias.

Protected commands
Some commands are protected and can only be executed after entering a password. Read more about password-protected commands by clicking [here](#).

Guide
When you run the `GUIDE` command, it will display a "first run" screen explaining how to use eShell. This command is available from the `ROOT` context (`eShell>`).

Help
When the `HELP` command is used alone, it will list all available commands with prefixes as well as sub-contexts within the current context. It will also give you a short description to each command / sub-context. When you use
HELP as an argument with a particular command (e.g. CLEANLEVEL HELP), it will give you details for that command. It will display SYNTAX, OPERATIONS, ARGUMENTS and ALIASES for the command with a short description for each.

Command history
eShell keeps history of previously executed commands. This applies only to the current eShell interactive session. Once you exit eShell, the command history will be dropped. Use the Up and Down arrow keys on your keyboard to navigate through the history. Once you find the command you were looking for, you can execute it again, or modify it without having to type in the entire command from the beginning.

CLS / Clear screen
The CLS command can be used to clear screen. It works the same way as it does with Windows Command Prompt or similar command line interfaces.

EXIT / CLOSE / QUIT / BYE
To close or exit eShell, you can use any of these commands (EXIT, CLOSE, QUIT or BYE).

3.1.2 Commands
This section lists all available eShell commands with description for each command.

NOTE: Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

Commands contained within ROOT context:

ABOUT
Lists information about the program. It shows name of the product installed, version number, installed components (including version number of each component) and basic information about the server and the operating system that ESET File Security is running on.

CONTEXT PATH:

    root

BATCH
Starts eShell batch mode. This is very useful when running batch files / scripts and we recommend using it with batch files. Put START BATCH as the first command in the batch file or script to enable batch mode. When you enable this function, no interactive input is prompted (e.g. entering a password) and missing arguments are replaced by defaults. This ensures that the batch file will not stop in the middle because eShell is expecting the user to do something. This way the batch file should execute without stopping (unless there is an error or the commands within the batch file are incorrect).

CONTEXT PATH:

    root

SYNTAX:

    [start] batch

OPERATIONS:

    start - Starts eShell in batch mode

CONTEXT PATH:

    root

EXAMPLES:

    start batch - Starts eShell batch mode

CONNECT
Connects to the ESET kernel.

CONTEXT PATH:

    root
GUIDE
Displays first run screen.

CONTEXT PATH:

ROOT

PASSWORD

Normally, to execute password-protected commands, you are prompted to type in a password for security reasons. This applies to commands such as those that disable antivirus protection and those that may affect ESET File Security functionality. You will be prompted for password every time you execute such command. You can define this password in order to avoid entering password every time. It will be remembered by eShell and automatically be used when a password-protected command is executed. This means that you do not have to enter the password every time.

NOTE: Defined password works only for the current eShell interactive session. Once you exit eShell, this defined password will be dropped. When you start eShell again, the password needs to be defined again.

This defined password is also very useful when running batch files / scripts. Here is an example of a such batch file:

```
eshell start batch "&" set password plain <yourpassword> "&" set status disabled
```

This concatenated command above starts a batch mode, defines password which will be used and disables protection.

CONTEXT PATH:

ROOT

SYNTAX:

```
[get] | restore password
set password [plain <password>]
```

OPERATIONS:

```
get - Show password
set - Set or clear password
restore - Clear password
```

ARGUMENTS:

```
plain - Switch to enter password as parameter
password - Password
```

EXAMPLES:

```
set password plain <yourpassword> - Sets a password which will be used for password-protected commands
restore password - Clears password
```

EXAMPLES:

```
get password - Use this to see whether the password is configured or not (this is only shows only stars "*", does not list the password itself), when no stars are visible, it means that there is no password set
set password plain <yourpassword> - Use this to set defined password
restore password - This command clears defined password
```

STATUS

Shows information about the current protection status of ESET File Security (similar to GUI).

CONTEXT PATH:

ROOT
SYNTAX:

[get] | restore status
set status disabled | enabled

OPERATIONS:

get - Show antivirus protection status
set - Disable/Enable antivirus protection
restore - Restores default settings

ARGUMENTS:

disabled - Disable antivirus protection
enabled - Enable antivirus protection

EXAMPLES:

get status - Shows current protection status
set status disabled - Disables protection
restore status - Restores protection to default setting (Enabled)

VIRLOG
This is an alias of the DETECTIONS command. It is useful when you need to view information about detected infiltrations. Click here to see details about this command and how to use it.

WARNLOG
This is an alias of the EVENTS command. It is useful when you need to view information about various events. Click here to see details about this command and how to use it.

3.1.2.1 Context - AV

ANTISTEALTH
Enable Anti-Stealth.

SYNTAX:

[get] | restore antistealth
set antistealth disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

CLEANLEVEL
Cleaning level.

SYNTAX:

[get] | restore cleanlevel
set cleanlevel none | normal | strict
OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- none - Do not clean
- normal - Standard cleaning
- strict - Strict cleaning

EXCLUSIONS

Exclusions.

SYNTAX:

- [get] | clear exclusions
- add | remove exclusions <exclusion>

OPERATIONS:

- get - Returns current setting/status
- add - Add item
- remove - Removes item

ARGUMENTS:

- exclusion - Excluded file/folder/mask

EXTENSIONS

Scanned/excluded extensions.

SYNTAX:

- [get] | restore extensions
- add | remove extensions <extension> | /all | /extless

OPERATIONS:

- get - Returns current setting/status
- add - Add item
- remove - Removes item
- restore - Restores default settings/object/file

ARGUMENTS:

- extension - Extension
- all - All files
- extless - Extensionless files

RESTART

Restarts the ESET kernel.

SYNTAX:

- restart

SELFDEFENSE
Self-defense.

SYNTAX:

```
[get] | restore selfdefense
set selfdefense disabled | enabled
```

OPERATIONS:

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:

- `disabled` - Disables function/deactivates setting
- `enabled` - Enables function/activates setting

STATUS

Antivirus protection status.

SYNTAX:

```
[get] | restore status
set status disabled | enabled
```

OPERATIONS:

- `get` - Show antivirus protection status
- `set` - Disable/Enable antivirus protection
- `restore` - Restores default settings/object/file

ARGUMENTS:

- `disabled` - Disable antivirus protection
- `enabled` - Enable antivirus protection

3.1.2.2 Context - AV EMAIL

CLIENTS

Email clients.

SYNTAX:

```
[ get ] clients
add | remove clients <path>
```

OPERATIONS:

- `get` - Returns current setting/status
- `add` - Adds item
- `remove` - Removes item

ARGUMENTS:

- `path` - Application path

With filtering by application only, you must specify which applications serve as email clients. If an application is not marked as an email client, email may not be scanned.
3.1.2.3  Context - AV EMAIL GENERAL

CLEANLEVEL
Cleaning level.

SYNTAX:

    [get] | restore cleanlevel
    set cleanlevel none | normal | strict

OPERATIONS:

    get - Returns current setting/status
    set - Sets value/status
    restore - Restores default settings/object/file

ARGUMENTS:

    none - Do not clean
    normal - Standard cleaning
    strict - Strict cleaning

EXTENSIONS
Scanned/excluded extensions.

SYNTAX:

    [get] | restore extensions
    add | remove extensions <extension> | /all | /extless

OPERATIONS:

    get - Returns current setting/status
    add - Add item
    remove - Removes item
    restore - Restores default settings/object/file

ARGUMENTS:

    extension - Extension
    all - All files
    extless - Extensionless files

3.1.2.4  Context - AV EMAIL GENERAL LIMITS ARCHIVE

LEVEL
Archive nesting level.

SYNTAX:

    [get] | restore level
    set level <number>

OPERATIONS:

    get - Returns current setting/status
    set - Sets value/status
RESTORE - Restores default settings/object/file

ARGUMENTS:

number - Level from 1 to 20 or 0 for default settings

SIZE
Maximum size of file in archive (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

3.1.2.5 Context - AV_EMAIL GENERAL LIMITS OBJECTS

SIZE
Maximum archive size (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

TIMEOUT
Maximum scan time for archives (sec.).

SYNTAX:

[get] | restore timeout
set timeout <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Time in seconds or 0 for default settings
3.1.2.6  Context - AV EMAIL GENERAL OBJECTS

ARCHIVE
Scan archives.
SYNTAX:
\[
\text{[get]} \mid \text{restore archive}
\]
\[
\text{set archive disabled} \mid \text{enabled}
\]
OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file
ARGUMENTS:
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

EMAIL
Scan email files.
SYNTAX:
\[
\text{[get]} \mid \text{restore email}
\]
\[
\text{set email disabled} \mid \text{enabled}
\]
OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file
ARGUMENTS:
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

RUNTIME
Scan runtime packers.
SYNTAX:
\[
\text{[get]} \mid \text{restore runtime}
\]
\[
\text{set runtime disabled} \mid \text{enabled}
\]
OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file
ARGUMENTS:
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

SFX
Scan self-extracting archives.

SYNTAX:

[get] | restore sfx
set sfx disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.7  Context - AV EMAIL GENERAL OPTIONS

ADVHEURISTICS

Use advanced heuristics.

SYNTAX:

[get] | restore advheuristics
set advheuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

HEURISTICS

Use heuristics.

SYNTAX:

[get] | restore heuristics
set heuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNSAFE

Detection of potentially unsafe applications.
SYNTAX:

[get] | restore unsafe
set unsafe disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNWANTED
Detection of potentially unwanted applications.

SYNTAX:

[get] | restore unwanted
set unwanted disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.8 Context - AV EMAIL GENERAL OTHER

LOGALL
Log all objects.

SYNTAX:

[get] | restore logall
set logall disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

OPTIMIZE
Smart optimization.

SYNTAX:
[get] | restore optimize

set optimize disabled | enabled

OPERATIONS:
get  - Returns current setting/status
set  - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.9 Context - AV EMAIL PROTOCOL POP3

COMPATIBILITY

Compatibility setup.

SYNTAX:
[get] | restore compatibility
set compatibility compatible | both | effective

OPERATIONS:
get  - Returns current setting/status
set  - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
compatible - Maximum compatibility level
both - Medium compatibility level
effective - Maximum efficiency

Not all email clients may work properly in conjunction with POP3 filtering in standard mode. The following settings allow adjustment of the compatibility level to resolve potential conflicts. However, increasing the compatibility level may lead to decreased efficiency of the Internet Monitor, or inability to take advantage of all its features.

PORTS

Ports used by POP3.

SYNTAX:
[get] | restore ports
set ports [<string>]

OPERATIONS:
get  - Returns current setting/status
set  - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
string - Port numbers separated by a comma

USE
Check POP3.

SYNTAX:

[get] | restore use
set use disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.10 Context - AV EMAIL PROTOCOL POP3S

COMPATIBILITY

Compatibility setup.

SYNTAX:

[get] | restore compatibility
set compatibility compatible | both | effective

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

compatible - Maximum compatibility level
both - Medium compatibility level
effective - Maximum efficiency

Not all email clients may work properly in conjunction with POP3S filtering in standard mode. The following settings allow adjustment of the compatibility level to resolve potential conflicts. However, increasing the compatibility level may lead to decreased efficiency of the Internet Monitor, or inability to take advantage of all its features.

MODE

POP3S filtering mode.

SYNTAX:

[get] | restore mode
set mode none | ports | clients

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
- Do not use POP3S protocol checking
- Use POP3S protocol checking for selected ports
- Use POP3S protocol checking for applications marked as email

**PORTS**
Ports used by POP3.

**SYNTAX:**

```
[get] | restore ports
set ports [<string>]
```

**OPERATIONS:**

- *get* - Returns current setting/status
- *set* - Sets value/status
- *restore* - Restores default settings/object/file

**ARGUMENTS:**

- *string* - Port numbers separated by a comma

---

**3.1.2.11 Context - AV LIMITS ARCHIVE**

**LEVEL**
Archive nesting level.

**SYNTAX:**

```
[get] | restore level
set level <number>
```

**OPERATIONS:**

- *get* - Returns current setting/status
- *set* - Sets value/status
- *restore* - Restores default settings/object/file

**ARGUMENTS:**

- *number* - Level from 1 to 20 or 0 for default settings

---

**SIZE**
Maximum size of file in archive (kB).

**SYNTAX:**

```
[get] | restore size
set size <number>
```

**OPERATIONS:**

- *get* - Returns current setting/status
- *set* - Sets value/status
- *restore* - Restores default settings/object/file

**ARGUMENTS:**

- *number* - Size in kB or 0 for default settings
3.1.2.12  Context - AV LIMITS OBJECTS

SIZE
Maximum archive size (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

TIMEOUT
Maximum scan time for archives (sec.).

SYNTAX:

[get] | restore timeout
set timeout <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Time in seconds or 0 for default settings

3.1.2.13  Context - AV NETFILTER

AUTOSTART
Run HTTP and POP3 application protocol content filtering automatically.

SYNTAX:

[get] | restore autostart
set autostart disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EXCLUDED
Applications excluded from protocol filtering.

SYNTAX:

\[
\text{[get]} \text{ excluded} \\
\text{add | remove excluded <path>}
\]

OPERATIONS:

- get - Returns current setting/status
- add - Add item
- remove - Removes item

ARGUMENTS:

- path - Applications path

MODE
Redirect traffic for filtering.

SYNTAX:

\[
\text{[get]} | \text{ restore mode} \\
\text{set mode ports | application | both}
\]

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- ports - HTTP and POP3 ports
- application - Applications marked as Internet browsers or email clients
- both - Ports and applications marked as Internet browsers or email clients

STATUS
Enable HTTP and POP3 application protocol content filtering.

SYNTAX:

\[
\text{[get]} | \text{ restore status} \\
\text{set status disabled | enabled}
\]

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting
3.1.2.14  Context - AV NETFILTER PROTOCOL SSL

BLOCKSSL2
Block encrypted communication utilizing the obsolete protocol SSL v2.

SYNTAX:

[get] | restore blockssl2

set blockssl2 disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EXCEPTIONS
Apply created exceptions based on certificates.

SYNTAX:

[get] | restore exceptions

set exceptions disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

MODE
SSL filtering mode.

SYNTAX:

[get] | restore mode

set mode allways | ask | none

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

allways - Always use SSL checking
ask - Ask about non-visited sites (exclusions can be set)
none - Do not use SSL protocol checking
3.1.2.15  Context - AV NETFILTER PROTOCOL SSL CERTIFICATE

ADDTOBROWSERS
Add the root certificate to known browsers.

SYNTAX:

[get] | restore addtobrowsers
set addtobrowsers disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

NOTE: To properly check SSL-encrypted traffic, the root certificate for ESET, spol. s.r.o used to sign certificates will be added to the Trusted Root Certification Authorities (TRCA) certificate store.

EXCLUDED
List of certificates excluded from content filtering.

SYNTAX:

[get] excluded
remove excluded <name>

OPERATIONS:

get - Returns current setting/status
remove - Removes item

ARGUMENTS:

name - Certificate name

NOTTRUSTED
Not trusted if the certificate is invalid or corrupt.

SYNTAX:

[get] | restore nottrusted
set nottrusted ask | block

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

ask - Ask about certificate validity
block - Block communication that uses the certificate

TRUSTED
List of trusted certificates.

SYNTAX:

```plaintext
[get] trusted
remove trusted <name>
```

OPERATIONS:

- **get** - Returns current setting/status
- **remove** - Removes item

ARGUMENTS:

- **name** - Certificate name

**UNKNOWNROOT**

Unknown root - if the certificate cannot be verified using the TRCA certificate store.

SYNTAX:

```plaintext
[get] | restore unknownroot
set unknownroot ask | block
```

OPERATIONS:

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

ARGUMENTS:

- **ask** - Ask about certificate validity
- **block** - Block communication that uses the certificate

**3.1.2.16 Context - AV OBJECTS**

**ARCHIVE**

Scan archives.

SYNTAX:

```plaintext
[get] | restore archive
set archive disabled | enabled
```

OPERATIONS:

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

ARGUMENTS:

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**BOOT**

Scan boot sectors.

SYNTAX:

```plaintext
[get] | restore boot
```
set boot disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EMAIL
Scan email files.

SYNTAX:
[get] | restore email
set email disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

FILE
Scan files.

SYNTAX:
[get] | restore file
set file disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

MEMORY
Scan memory.

SYNTAX:
[get] | restore memory
set memory disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

RUNTIME
Scan runtime packers.

SYNTAX:

[get] | restore runtime
set runtime disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SFX
Scan self-extracting archives.

SYNTAX:

[get] | restore sfx
set sfx disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.17 Context - AV OPTIONS

ADVHEURISTICS
Use advanced heuristics.

SYNTAX:

[get] | restore advheuristics
set advheuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
**set** - Sets value/status

**restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**ADWARE**

Detection of Adware/Spyware/Riskware.

**SYNTAX:**

```
[get] | restore adware
```

```
set adware disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**HEURISTICS**

Use heuristics.

**SYNTAX:**

```
[get] | restore heuristics
```

```
set heuristics disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**SIGNATURES**

Use signatures.

**SYNTAX:**

```
[get] | restore signatures
```

```
set signatures disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting
ARGUMENTS:

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**UNSAFE**

Detection of potentially unsafe applications.

**SYNTAX:**

```
[get] | restore unsafe
set unsafe disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**UNWANTED**

Detection of potentially unwanted applications.

**SYNTAX:**

```
[get] | restore unwanted
set unwanted disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**3.1.2.18  Context - AV OTHER**

**LOGALL**

Log all objects.

**SYNTAX:**

```
[get] | restore logall
set logall disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

OPTIMIZE
Smart optimization.
SYNTAX:

```
[get] | restore optimize
set optimize disabled | enabled
```

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

3.1.2.19 Context - AV REALTIME

AUTOSTART
Start real-time protection automatically.
SYNTAX:

```
[get] | restore autostart
set autostart disabled | enabled
```

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

CLEANLEVEL
Cleaning level
SYNTAX:

```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- none - Do not clean
normal - Standard cleaning
strict - Strict cleaning

EXTENSIONS
Scanned/excluded extensions.
SYNTAX:
  [get] | restore extensions
  add | remove extensions <extension> | /all | /extless

OPERATIONS:
  get - Returns current setting/status
  add - Add item
  remove - Removes item
  restore - Restores default settings/object/file

ARGUMENTS:
  extension - Extension
  all - All files
  extless - Extensionless files

STATUS
Real-time computer protection status.
SYNTAX:
  [get] | restore status
  set status disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  disabled - Disables function/deactivates setting
  enabled - Enables function/activates setting

3.1.2.20 Context - AV REALTIME DISK
FLOPPY
Scan removable media.
SYNTAX:
  [get] | restore floppy
  set floppy disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file
ARGUMENTS:

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**LOCAL**

Scan local drives.

**SYNTAX:**

```
[get] | restore local
set local disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**NETWORK**

Scan network drives.

**SYNTAX:**

```
[get] | restore network
set network disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
- **enabled** - Enables function/activates setting

**3.1.2.21 Context - AV REALTIME EVENT**

**CREATE**

Scan files on creation.

**SYNTAX:**

```
[get] | restore create
set create disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EXECUTE
Scan files on execution.

SYNTAX:

\[[ \text{get} ] \mid \text{restore execute} \]
\text{set execute disabled} \mid \text{enabled}

OPERATIONS:

- \text{get} - Returns current setting/status
- \text{set} - Sets value/status
- \text{restore} - Restores default settings/object/file

ARGUMENTS:

- \text{disabled} - Disables function/deactivates setting
- \text{enabled} - Enables function/activates setting

FLOPPYACCESS
Scan on floppy access.

SYNTAX:

\[[ \text{get} ] \mid \text{restore floppyaccess} \]
\text{set floppyaccess disabled} \mid \text{enabled}

OPERATIONS:

- \text{get} - Returns current setting/status
- \text{set} - Sets value/status
- \text{restore} - Restores default settings/object/file

ARGUMENTS:

- \text{disabled} - Disables function/deactivates setting
- \text{enabled} - Enables function/activates setting

OPEN
Scan files on opening.

SYNTAX:

\[[ \text{get} ] \mid \text{restore open} \]
\text{set open disabled} \mid \text{enabled}

OPERATIONS:

- \text{get} - Returns current setting/status
- \text{set} - Sets value/status
- \text{restore} - Restores default settings/object/file

ARGUMENTS:

- \text{disabled} - Disables function/deactivates setting
- \text{enabled} - Enables function/activates setting
SHUTDOWN
Scan on computer shutdown.
SYNTAX:

[get] | restore shutdown

set shutdown disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.22 Context - AV REALTIME EXECUTABLE ADVHEURISTICS
Enable advanced heuristics on file execution.
SYNTAX:

[get] | restore advheuristics

set advheuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.23 Context - AV REALTIME EXECUTABLE FROMREMOVABLE ADVHEURISTICS
Enable advanced heuristics on file execution from removable media.
SYNTAX:

[get] | restore advheuristics

set advheuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EXCLUSION
USB drive exclusions.
SYNTAX:

[get] | restore exclusion
    select exclusion none | <drive> | all

OPERATIONS:

get - Returns current setting/status
select - Selects item
restore - Restores default settings/object/file

ARGUMENTS:
none - Deselect all drives
drive - Letter of a drive to select/deselect
all - Select all drives

NOTE: Use this option to allow exceptions from scanning using Advanced heuristics on file execution. Advanced heuristics settings for hard drives will be applied to selected devices.

3.1.2.24  Context - AV REALTIME LIMITS ARCHIVE

LEVEL
Archive nesting level.
SYNTAX:

[get] | restore level
    set level <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
number - Level from 1 to 20 or 0 for default settings

SIZE
Maximum size of file in archive (kB).
SYNTAX:

[get] | restore size
    set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
3.1.2.25  Context - AV REALTIME LIMITS OBJECTS

SIZE
Maximum archive size (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

TIMEOUT
Maximum scan time for archives (sec.).

SYNTAX:

[get] | restore timeout
set timeout <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Time in seconds or 0 for default settings

3.1.2.26  Context - AV REALTIME OBJECTS

ARCHIVE
Scan archives.

SYNTAX:

[get] | restore archive
set archive disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
BOOT
Scan boot sectors.
SYNTAX:

[get] | restore boot
set boot disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EMAIL
Scan email files.
SYNTAX:

[get] | restore email
set email disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

FILE
Scan files.
SYNTAX:

[get] | restore file
set file disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

MEMORY
Scan memory.
SYNTAX:

[get] | restore memory
set memory disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

RUNTIME

Scan runtime packers.

SYNTAX:

[get] | restore runtime
set runtime disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SFX

Scan self-extracting archives.

SYNTAX:

[get] | restore sfx
set sfx disabled | enabled

OPERATIONS:

g - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
3.1.2.27 Context - AV REALTIME ONWRITE

ADVHEURISTICS
Enable advanced heuristics for new and modified files.

SYNTAX:

[get] | restore advheuristics

set advheuristics disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

RUNTIME
Scan new and modified runtime archives.

SYNTAX:

[get] | restore runtime

set runtime disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SFX
Scan new and modified self-extracting archives.

SYNTAX:

[get] | restore sfx

set sfx disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
3.1.2.28  Context - AV REALTIME ONWRITE ARCHIVE

LEVEL

Archive nesting depth.

SYNTAX:

  [get] | restore level

  set level <number>

OPERATIONS:

  get - Returns current setting/status

  set - Sets value/status

  restore - Restores default settings/object/file

ARGUMENTS:

  number - Level (0 - 20)

SIZE

Maximum size of a scanned archived file (kB).

SYNTAX:

  [get] | restore size

  set size <number>

OPERATIONS:

  get - Returns current setting/status

  set - Sets value/status

  restore - Restores default settings/object/file

ARGUMENTS:

  number - Size (kB)

3.1.2.29  Context - AV REALTIME OPTIONS

ADVHEURISTICS

Use advanced heuristics.

SYNTAX:

  [get] | restore advheuristics

  set advheuristics disabled | enabled

OPERATIONS:

  get - Returns current setting/status

  set - Sets value/status

  restore - Restores default settings/object/file

ARGUMENTS:

  disabled - Disables function/deactivates setting

  enabled - Enables function/activates setting

ADWARE
Detection of Adware/Spyware/Riskware.

SYNTAX:

\[ \text{get} | \text{restore adware} \]

\hspace{1cm} \text{set adware disabled | enabled} \]

OPERATIONS:

\text{get} - Returns current setting/status

\text{set} - Sets value/status

\text{restore} - Restores default settings/object/file

ARGUMENTS:

\text{disabled} - Disables function/deactivates setting

\text{enabled} - Enables function/activates setting

HEURISTICS

Use heuristics.

SYNTAX:

\[ \text{get} | \text{restore heuristics} \]

\hspace{1cm} \text{set heuristics disabled | enabled} \]

OPERATIONS:

\text{get} - Returns current setting/status

\text{set} - Sets value/status

\text{restore} - Restores default settings/object/file

ARGUMENTS:

\text{disabled} - Disables function/deactivates setting

\text{enabled} - Enables function/activates setting

SIGNATURES

Use signatures.

SYNTAX:

\[ \text{get} | \text{restore signatures} \]

\hspace{1cm} \text{set signatures disabled | enabled} \]

OPERATIONS:

\text{get} - Returns current setting/status

\text{set} - Sets value/status

\text{restore} - Restores default settings/object/file

ARGUMENTS:

\text{disabled} - Disables function/deactivates setting

\text{enabled} - Enables function/activates setting

UNSAFE

Detection of potentially unsafe applications.

SYNTAX:
[get] | restore unsafe

set unsafe disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNWANTED
Detection of potentially unwanted applications.

SYNTAX:

[get] | restore unwanted

set unwanted disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.30 Context - AV REALTIME OTHER

LOGALL
Log all objects.

SYNTAX:

[get] | restore logall

set logall disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

OPTIMIZE
Smart optimization.

SYNTAX:

[get] | restore optimize
set optimize disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
     disabled - Disables function/deactivates setting
     enabled - Enables function/activates setting

3.1.2.31 Context - AV REALTIME REMOVABLE BLOCK
Block removable media.

SYNTAX:
[get] | restore block
set block disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
     disabled - Disables function/deactivates setting
     enabled - Enables function/activates setting

EXCLUSION
Allowed removable media.

SYNTAX:
[get] | restore exclusion
select exclusion none | <drive> | all

OPERATIONS:
get - Returns current setting/status
select - Selects item
restore - Restores default settings/object/file

ARGUMENTS:
     none - Deselect all drives
     drive - Letter of a drive to select/deselect
     all - Select all drives

NOTE: Use this option to enable access to removable media (CD, floppy disks, USB drives). Marking a media results in removing access restrictions when attempting to access that specific media.
3.1.2.32  Context - AV WEB

BROWSERS
Internet browsers.

SYNTAX:

[get] browsers

add | remove browsers <path>

OPERATIONS:

get - Returns current setting/status

add - Add item

remove - Removes item

ARGUMENTS:

path - Applications path

NOTE: To increase security, we recommend that you mark any application used as an Internet browser by checking the appropriate box. If an application is not marked as a web browser, data transferred using that application may not be scanned.

CLEANLEVEL
Cleaning level.

SYNTAX:

[get] | restore cleanlevel

set cleanlevel none | normal | strict

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

none - Do not clean

normal - Standard cleaning

strict - Strict cleaning

EXTENSIONS
Scanned/excluded extensions.

SYNTAX:

[get] | restore extensions

add | remove extensions <extension> | /all | /extless

OPERATIONS:

get - Returns current setting/status

add - Add item

remove - Removes item

restore - Restores default settings/object/file
ARGUMENTS:

- extension - Extension
- all - All files
- extless - Extensionless files

STATUS

Web access protection.

SYNTAX:

- [get] | restore status
- set status disabled | enabled

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

3.1.2.33 Context - AV WEB ADDRESSMGMT

ADDRESS

Address management in the selected list.

SYNTAX:

- [get] | clear address
- add | remove address <address>
- import | export address <path>

OPERATIONS:

- get - Returns current setting/status
- add - Add item
- remove - Removes item
- import - Imports from file
- export - Exports to file
- clear - Removes all items/files

ARGUMENTS:

- address - Address
- path - File path

LIST

Address list management.

SYNTAX:

- [get] | restore list
- set list <listname> disabled | enabled
select | remove list <listname>
add list allowed <listname> | blocked <listname> | excluded <listname>

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  select - Select for editing
  add - Add item
  remove - Removes item

ARGUMENTS:
  listname - List name
  disabled - Do not use list
  enabled - Use list
  allowed - List of allowed addresses
  blocked - List of blocked addresses
  excluded - List of addresses excluded from filtering

NOTE: To edit the selected list (marked with - x) use the av web addressmgmt address Command.

NOTIFY
Notify when applying address from the list.

SYNTAX:
  [get] | restore notify
  set notify disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  disabled - Disables function/deactivates setting
  enabled - Enables function/activates setting

WHITELISTED
Allow access only to HTTP addresses in the list of allowed addresses.

SYNTAX:
  [get] | restore whitelisted
  set whitelisted disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.34  Context - AV WEB LIMITS ARCHIVE
LEVEL
Archive nesting level.
SYNTAX:

[get] | restore level
set level <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Level from 1 to 20 or 0 for default settings

SIZE
Maximum size of file in archive (kB).
SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

3.1.2.35  Context - AV WEB LIMITS OBJECTS
SIZE
Maximum archive size (kB).
SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings
TIMEOUT
Maximum scan time for archives (sec.).

SYNTAX:

[get] | restore timeout
set timeout <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Time in seconds or 0 for default settings

3.1.2.36  Context - AV WEB OBJECTS
ARCHIVE
Scan archives.

SYNTAX:

[get] | restore archive
set archive disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

BOOT
Scan boot sectors.

SYNTAX:

[get] | restore boot
set boot disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

EMAIL
Scan email files.
SYNTAX:

[get] | restore email
set email disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

FILE
Scan files.

SYNTAX:

[get] | restore file
set file disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

MEMORY
Scan memory.

SYNTAX:

[get] | restore memory
set memory disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

RUNTIME
Scan runtime packers.

SYNTAX:

[get] | restore runtime
set runtime disabled | enabled

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

SFX
Scan self-extracting archives.

SYNTAX:
- [get] | restore sfx
- set sfx disabled | enabled

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

3.1.2.37 Context - AV WEB OPTIONS

ADVHEURISTICS
Use advanced heuristics.

SYNTAX:
- [get] | restore advheuristics
- set advheuristics disabled | enabled

OPERATIONS:
- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

ADWARE
Detection of Adware/Spyware/Riskware.

SYNTAX:
- [get] | restore adware
- set adware disabled | enabled
OPERATIONS:

- **get**: Returns current setting/status
- **set**: Sets value/status
- **restore**: Restores default settings/object/file

ARGUMENTS:

- **disabled**: Disables function/deactivates setting
- **enabled**: Enables function/activates setting

HEURISTICS

Use heuristics.

SYNTAX:

```
[get] | restore heuristics
set heuristics disabled | enabled
```

OPERATIONS:

- **get**: Returns current setting/status
- **set**: Sets value/status
- **restore**: Restores default settings/object/file

ARGUMENTS:

- **disabled**: Disables function/deactivates setting
- **enabled**: Enables function/activates setting

SIGNATURES

Use signatures.

SYNTAX:

```
[get] | restore signatures
set signatures disabled | enabled
```

OPERATIONS:

- **get**: Returns current setting/status
- **set**: Sets value/status
- **restore**: Restores default settings/object/file

ARGUMENTS:

- **disabled**: Disables function/deactivates setting
- **enabled**: Enables function/activates setting

UNSAFE

Detection of potentially unsafe applications.

SYNTAX:

```
[get] | restore unsafe
set unsafe disabled | enabled
```

OPERATIONS:

- **get**: Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNWANTED
Detection of potentially unwanted applications.

SYNTAX:

[get] | restore unwanted
set unwanted disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.38 Context - AV WEB OPTIONS BROWSERS

ACTIVEMODE
Active mode for Internet browsers.

SYNTAX:

[get] activemode
add | remove activemode <path>

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item

ARGUMENTS:

path - Applications path

NOTE: Programs added to the list are automatically added to the Internet browsers list.
3.1.2.39  Context - AV WEB OTHER

LOGALL
Log all objects.

SYNTAX:

   [get] | restore logall
   set logall disabled | enabled

OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   disabled - Disables function/deactivates setting
   enabled - Enables function/activates setting

OPTIMIZE
Smart optimization.

SYNTAX:

   [get] | restore optimize
   set optimize disabled | enabled

OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   disabled - Disables function/deactivates setting
   enabled - Enables function/activates setting

3.1.2.40  Context - AV WEB PROTOCOL HTTP

PORTS
Ports used by HTTP.

SYNTAX:

   [get] | restore ports
   set ports [<string>]

OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   string - Port numbers separated by a colon
USE
Scan HTTP.
SYNTAX:

  [get] | restore use
  set use disabled | enabled

OPERATIONS:

  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:

  disabled - Disables function/deactivates setting
  enabled - Enables function/activates setting

3.1.2.41  Context - AV WEB PROTOCOL HTTPS

MODE
HTTPS filtering mode.
SYNTAX:

  [get] | restore mode
  set mode none | ports | browsers

OPERATIONS:

  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:

  none - Do not use protocol checking
  ports - Use HTTPS protocol checking for selected ports
  browsers - Use HTTPS protocol checking for applications marked as browsers that use selected ports

PORTS
Ports used by HTTPS protocol.
SYNTAX:

  [get] | restore ports
  set ports [<string>]

OPERATIONS:

  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:

  string - Port numbers delimited by a comma
3.1.2.42  Context - GENERAL

CONFIG
Import/export settings.

SYNTAX:
   import | export config <path>

OPERATIONS:
   import - Imports from file
   export - Exports to file

ARGUMENTS:
   path - File path

LICENSE
License management.

SYNTAX:
   [get] license
   import license <path>
   export license <ID> <path>
   remove license <ID>

OPERATIONS:
   get - Returns current setting/status
   remove - Removes item
   import - Imports from file
   export - Exports to file

ARGUMENTS:
   path - License file path
   ID - License ID

3.1.2.43  Context - GENERAL ACCESS

ADMIN
Administrator rights settings protection.

SYNTAX:
   [get] | restore admin
   set admin disabled | enabled

OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

BATCH
Execute commands entered as arguments when eShell is running.

SYNTAX:

```
[get] | restore batch
```

```
set batch disabled | <time> | always
```

OPERATIONS:

```
get - Returns current setting/status
```

```
set - Sets value/status
```

```
restore - Restores default settings/object/file
```

ARGUMENTS:

```
disabled - Disabled
```

```
time - Time interval in minutes (1 - 1440 minutes)
```

```
always - Always
```

PASSWORD
This password is used for password-protected commands. Normally, to execute a password-protected commands you are prompted to type in a password. This is for security reasons. It applies to commands such as those that disable antivirus protection and those that may affect ESET File Security functionality. You will be prompted for password every time you execute such command. Alternatively, you can define this password for your current eShell session and you will not be prompted to enter password. For more details click here.

For interactive password input (recommended) leave parameters empty. To reset password enter empty password.

CONTEXT PATH:

```
general access
```

SYNTAX:

```
[get] | restore | set password
```

OPERATIONS:

```
get - Show password
```

```
set - Set password
```

```
restore - Reset password
```

EXAMPLES:

```
get password - Use this to see whether the password is configured or not (this is only shows only stars "*", does not list the password itself), when no stars are visible, it means that there is no password set
```

```
set password - Use this to set password, simply enter your password (if no password is entered, settings protection is not used)
```

```
restore password - This command clears existing password (settings protection will not be used)
```

GUI EQUIVALENT:

```
click here to see how this is configured via GUI
```
3.1.2.44 Context - GENERAL ESHELL

ALIAS

Alias management.

SYNTAX:

[get] | clear | restore alias
add alias [.] <alias>=<command>
remove alias <alias>
import | export alias <path>

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item
import - Imports from file
export - Exports to file
restore - Restores default settings/object/file

ARGUMENTS:

. - Create global alias
alias - New alias
command - Associated command (command validity not checked)
alias - Alias to delete
path - File path

LISTER

Use lister.

SYNTAX:

[get] | restore lister
set lister disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
3.1.2.45  Context - GENERAL ESHELL COLOR

ALIAS

Alias color.

SYNTAX:

[get] | restore alias

set alias [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

COMMAND

Command color.

SYNTAX:

[get] | restore command

set command [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:

black - Black
navy - Navy blue
grass - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

CONTEXT
Context color.

SYNTAX:

[get] | restore context

set context [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
grass - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

DEFAULT
Base color.

SYNTAX:

[get] | restore default

set default [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

DISABLED
N/A color.

SYNTAX:

[get] | restore disabled

set disabled [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

ERROR
Color of error messages.

SYNTAX:
[get] | restore error

set error [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

INTERACTIVE

Interactive operations color.

SYNTAX:

[get] | restore interactive

set interactive [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
grass - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

LIST 1

List color 1.

SYNTAX:

[get] | restore list 1
set list1 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

LIST2
List color 2.

SYNTAX:

[get] | restore list2

set list2 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
SUCCESS
Status OK color.

SYNTAX:

[get] | restore success

set success [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

black - Black
navy - Navy blue
green - Grass green
ltblue - Light blue
brown - Brown
purple - Purple
olive - Olive green
ltgray - Light gray
gray - Gray
blue - Blue
green - Green
cyan - Cyan
red - Red
magenta - Magenta
yellow - Yellow
white - White

WARNING
Color of warning messages.

**SYNTAX:**

```
[get] | restore warning
```

```
set warning [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan |
red | magenta | yellow | white]
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **black** - Black
- **navy** - Navy blue
- **grass** - Grass green
- **ltblue** - Light blue
- **brown** - Brown
- **purple** - Purple
- **olive** - Olive green
- **ltgray** - Light gray
- **gray** - Gray
- **blue** - Blue
- **green** - Green
- **cyan** - Cyan
- **red** - Red
- **magenta** - Magenta
- **yellow** - Yellow
- **white** - White

3.1.2.46  Context - GENERAL ESHELL OUTPUT

**UTF8**

UTF8 encoded output.

**SYNTAX:**

```
[get] | restore utf8
```

```
set utf8 disabled | enabled
```

**OPERATIONS:**

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

**ARGUMENTS:**

- **disabled** - Disables function/deactivates setting
enabled - Enables function/activates setting

NOTE: For correct display, command line should use a TrueType font like 'Lucida Console'.

3.1.2.47 Context - GENERAL ESHELL STARTUP
LOADCOMMANDS
Load all commands on startup.

SYNTAX:

[get] | restore loadcommands

set loadcommands disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

STATUS
Display protection status on startup.

SYNTAX:

[get] | restore status

set status disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.48 Context - GENERAL ESHELL VIEW
CMDHELP
Display help on command failure.

SYNTAX:

[get] | restore cmdhelp

set cmdhelp disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

COLORS

Use colors.

SYNTAX:

[get] | restore colors
set colors disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

FITWIDTH

Trim text to fit width.

SYNTAX:

[get] | restore fitwidth
set fitwidth disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

GLOBAL

Display global commands.

SYNTAX:

[get] | restore global
set global disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

HIDDEN
Display hidden commands.
SYNTAX:

[get] | restore hidden
set hidden disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

OPERATIONS
Display operations in commands list.
SYNTAX:

[get] | restore operations
set operations disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SHORTLIST
Display short command list on context change.
SYNTAX:

[get] | restore shortlist
set shortlist disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SYNTAXHINT
Display command syntax hints.

SYNTAX:

```
[get] | restore syntaxhint
set syntaxhint disabled | enabled
```

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

VALUESONLY

Display only values without description.

SYNTAX:

```
[get] | restore valuesonly
set valuesonly disabled | enabled
```

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

3.1.2.49 Context - GENERAL PERFORMANCE

SCANNERS

Number of running scans.

SYNTAX:

```
[get] | restore scanners
set scanners <number>
```

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- number - Count (1 - 20)
3.1.2.50  Context - GENERAL PROXY

ADDRESS
Proxy server address.
SYNTAX:

[get] | restore address  
  set address [<string>]

OPERATIONS:
get - Returns current setting/status  
set - Sets value/status  
restore - Restores default settings/object/file

ARGUMENTS:

  string - Address

DETECT
Detects proxy server configuration.
SYNTAX:

detect

LOGIN
Login name.
SYNTAX:

[get] | restore login  
  set login [<string>]

OPERATIONS:
get - Returns current setting/status  
set - Sets value/status  
restore - Restores default settings/object/file

ARGUMENTS:

  string - Name

PASSWORD
Proxy server password.
SYNTAX:

[get] | restore password  
  set password [plain <password>]

OPERATIONS:
get - Returns current setting/status  
set - Sets value/status  
restore - Restores default settings/object/file

ARGUMENTS:

  plain - Switch to entering password as parameter
password - Password

PORT
Port
SYNTAX:

[get] | restore port
    set port <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Port number

USE
Use proxy server.

SYNTAX:

[get] | restore use
    set use disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.51 Context - GENERAL QUARANTINE RESCAN
UPDATE
Scan quarantined files after every update.

SYNTAX:

[get] | restore update
    set update disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
3.1.2.52 Context - GENERAL REMOTE

INTERVAL
Connection interval (minutes).
SYNTAX:

  [get] | restore interval
  set interval <number>

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file
ARGUMENTS:
  number - Time in minutes (1 - 1440)

USE
ERA Server connection.
SYNTAX:

  [get] | restore use
  set use disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file
ARGUMENTS:
  disabled - Disables function/deactivates setting
  enabled - Enables function/activates setting

3.1.2.53 Context - GENERAL REMOTE SERVER PRIMARY

ADDRESS
ERA Server address.
SYNTAX:

  [get] | restore address
  set address [<string>]

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file
ARGUMENTS:
  string - Address

ENCRYPT
Block unencrypted connection.

SYNTAX:

[get] | restore encrypt
set encrypt disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

PASSWORD

ERA Server password.

SYNTAX:

[get] | restore password
set password [plain <password>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

plain - Switch to entering password as parameter
password - Password

PORT

ERA Server port.

SYNTAX:

[get] | restore port
set port <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Port number
3.1.2.54  Context - GENERAL REMOTE SERVER SECONDARY

ADDRESS
ERA Server address.

SYNTAX:

   [get] | restore address
   set address [<string>]

OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   string - Address

ENCRYPT
Block uncrypted connection.

SYNTAX:

   [get] | restore encrypt
   set encrypt disabled | enabled

OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   disabled - Disables function/deactivates setting
   enabled - Enables function/activates setting

PASSWORD
ERA Server password.

SYNTAX:

   [get] | restore password
   set password [plain <password>]

OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   plain - Switch to entering password as parameter
   password - Password

PORT
ERA Server port.
SYNTAX:

```
[get] | restore port
set port <number>
```

OPERATIONS:

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

ARGUMENTS:

- **number** - Port number

### 3.1.2.55 Context - GENERAL TS.NET

**EXCLUSION**

Exclude from submission.

SYNTAX:

```
[get] | restore exclusion
add | remove exclusion <exclusion>
```

OPERATIONS:

- **get** - Returns current setting/status
- **add** - Add item
- **remove** - Removes item
- **restore** - Restores default settings/object/file

ARGUMENTS:

- **exclusion** - Extension

**FROM**

Contact e-mail.

SYNTAX:

```
[get] | restore from
set from [<string>]
```

OPERATIONS:

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

ARGUMENTS:

- **string** - E-mail address

**LOGING**

Log creation.

SYNTAX:

```
[get] | restore loging
set loging disabled | enabled
```
OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SENDING
Submission of suspicious files.

SYNTAX:
[get] | restore sending
set sending none | ask | auto

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
none - Do not submit
ask - Confirm before sending for analysis
auto - Send for analysis without confirmation

VIA
Means of file submission.

SYNTAX:
[get] | restore via
set via auto | ra | direct

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
auto - By means of Remote Administrator or directly to ESET
ra - By means of Remote Administrator
direct - Directly to ESET

WHEN
When to submit suspicious files.

SYNTAX:
[get] | restore when
set when asap | update
OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  asap - As soon as possible
  update - During update

3.1.2.56 Context - GENERAL TS.NET STATISTICS

SENDING
Statistic information submission.

SYNTAX:

[get] | restore sending
  set sending disabled | enabled

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  disabled - Disables function/deactivates setting
  enabled - Enables function/activates setting

WHEN
Submission of anonymous statistical information.

SYNTAX:

[get] | restore when
  set when asap | update

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  asap - As soon as possible
  update - During update
3.1.2.57  Context - SCANNER

CLEANLEVEL
Cleaning level.
SYNTAX:

   [get] | restore cleanlevel
   set cleanlevel none | normal | strict

OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
   restore - Restores default settings/object/file

ARGUMENTS:
   none - Do not clean
   normal - Standard cleaning
   strict - Strict cleaning

EXTENSIONS
Scanned/excluded extensions.
SYNTAX:

   [get] | restore extensions
   add | remove extensions <extension> | /all | /extless

OPERATIONS:
   get - Returns current setting/status
   add - Add item
   remove - Removes item
   restore - Restores default settings/object/file

ARGUMENTS:
   extension - Extension
   all - All files
   extless - Extensionless files

PROFILE
Computer scan profile management.
SYNTAX:

   [get] profile
   select | remove profile <name>
   add profile new: <name> [copyfrom: <name>]

OPERATIONS:
   get - Returns current setting/status
   select - Selects item
   add - Add item
remove - Removes item

ARGUMENTS:

name - Profile name
new - New profile
copyfrom - Copy settings from profile

NOTE: Other context commands refer to the active profile (marked with - x). For the active profile selection use select scanner profile <profile name>.

SCAN

Computer scan.

SYNTAX:

[get] | clear scan
start scan [readonly]
pause | resume | stop scan <ID> | all

OPERATIONS:

get - Show running and completed scans
start - Run computer scan for the selected profile
stop - Stop scan
resume - Continue paused scan
pause - Pause scan
clear - Remove completed scans from list

ARGUMENTS:

readonly - Scan without cleaning
ID - Scan ID for command execution
all - Execute command for all scans

TARGET

Scan targets for active profile.

SYNTAX:

[get] target
add | remove target <path>

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item

ARGUMENTS:

path - Path/Scan target

NOTE: For boot sector scan enter X:\$\{Boot\} where 'x' is the name of scanned disk.
3.1.2.58  Context - SCANNER LIMITS ARCHIVE

LEVEL
Archive nesting level.

SYNTAX:

[get] | restore level
set level <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Level from 1 to 20 or 0 for default settings

SIZE
Maximum size of file in archive (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

3.1.2.59  Context - SCANNER LIMITS OBJECTS

SIZE
Maximum archive size (kB).

SYNTAX:

[get] | restore size
set size <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

number - Size in kB or 0 for default settings

TIMEOUT
Maximum scan time for archives (sec.).
SYNTAX:

```
[get] | restore timeout
set timeout <number>
```

OPERATIONS:

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:

- `number` - Time in seconds or 0 for default settings

3.1.2.60  Context - SCANNER OBJECTS

**ARCHIVE**

Scan archives.

SYNTAX:

```
[get] | restore archive
set archive disabled | enabled
```

OPERATIONS:

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:

- `disabled` - Disables function/deactivates setting
- `enabled` - Enables function/activates setting

**BOOT**

Scan boot sectors.

SYNTAX:

```
[get] | restore boot
set boot disabled | enabled
```

OPERATIONS:

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:

- `disabled` - Disables function/deactivates setting
- `enabled` - Enables function/activates setting

**EMAIL**

Scan email files.

SYNTAX:

```
[get] | restore email
```
set email disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

FILE
Scan files.

SYNTAX:

[get] | restore file
set file disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

MEMORY
Scan memory.

SYNTAX:

[get] | restore memory
set memory disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

RUNTIME
Scan runtime packers.

SYNTAX:

[get] | restore runtime
set runtime disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SFX
Scan self-extracting archives.

SYNTAX:

[get] | restore sfx
set sfx disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.61 Context - SCANNER OPTIONS
ADVHEURISTICS
Use advanced heuristics.

SYNTAX:

[get] | restore advheuristics
set advheuristics disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

ADWARE
Detection of Adware/Spyware/Riskware.

SYNTAX:

[get] | restore adware
set adware disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

HEURISTICS
Use heuristics.

SYNTAX:
[get] | restore heuristics
set heuristics disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

SIGNATURES
Use signatures.

SYNTAX:
[get] | restore signatures
set signatures disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

UNSAFE
Detection of potentially unsafe applications.

SYNTAX:
[get] | restore unsafe
set unsafe disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:

- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

UNWANTED

Detection of potentially unwanted applications.

SYNTAX:

[get] | restore unwanted

set unwanted disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

3.1.2.62 Context - SCANNER OTHER

ADS

Scan alternate data streams (ADS).

SYNTAX:

[get] | restore ads

set ads disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

LOGALL

Log all objects.

SYNTAX:

[get] | restore logall

set logall disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
LOWPRIORITY
Run background scans with low priority.

**SYNTAX:**

- `[get]` | restore lowpriority
- set lowpriority disabled | enabled

**OPERATIONS:**

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

**ARGUMENTS:**

- `disabled` - Disables function/deactivates setting
- `enabled` - Enables function/activates setting

OPTIMIZE
Smart optimization.

**SYNTAX:**

- `[get]` | restore optimize
- set optimize disabled | enabled

**OPERATIONS:**

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

**ARGUMENTS:**

- `disabled` - Disables function/deactivates setting
- `enabled` - Enables function/activates setting

PRESERVETIME
Preserve last access timestamp.

**SYNTAX:**

- `[get]` | restore preservetime
- set preservetime disabled | enabled

**OPERATIONS:**

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

**ARGUMENTS:**

- `disabled` - Disables function/deactivates setting
- `enabled` - Enables function/activates setting
SCROLL

Scroll scan log.

SYNTAX:

[get] | restore scroll

set scroll disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.63 Context - SERVER

AUTOEXCLUSIONS

Automatic exclusions management.

SYNTAX:

[get] | restore autoexclusions

select autoexclusions <server>

OPERATIONS:

get - Returns current setting/status
select - Selects item
restore - Restores default settings/object/file

ARGUMENTS:

server - Server name

3.1.2.64 Context - TOOLS

QUARANTINE

Quarantine.

SYNTAX:

[get] quarantine

add quarantine <path>

send | remove | restore quarantine <ID>

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item
restore - Restores default settings/object/file
send - Sends item/file
ARGUMENTS:

path - File path
ID - Quarantined file ID

STATISTICS

Statistics.

SYNTAX:

[get] | clear statistics

OPERATIONS:

get - Show statistics
clear - Reset statistics

SYSINSPECTOR

SysInspector.

SYNTAX:

[get] sysinspector

add | remove sysinspector <name>

export sysinspector <name> to:<path>

OPERATIONS:

get - Returns current setting/status
add - Add item
remove - Removes item
export - Exports to file

ARGUMENTS:

name - Comment
path - File name (.zip or .xml)

3.1.2.65  Context - TOOLS ACTIVITY

FILESYSTEM

Filesystem.

SYNTAX:

[get] filesystem [<count>] [seconds | minutes | hours [<year>-<month>]]

NETWORK

Network activity.

SYNTAX:

[get] network [<count>] [seconds | minutes | hours [<year>-<month>]]

ARGUMENTS:

count - Number of records to show
seconds - Sampling 1 second
minutes - Sampling 1 minute
hours - Sampling 1 hour
year - Show records for year
month - Show records for month

3.1.2.66 Context - TOOLS LOG

DETECTIONS
This is useful when you need to view information about detected infiltrations.

CONTEXT PATH:

root

SYNTAX:

[get] detections [count <number>] [from <year>-<month>-<day> <hour>:<minute>:<second>] [to <year>-<month>-<day> <hour>:<minute>:<second>]
clear detections

OPERATIONS:

get - Returns current setting/status
clear - Removes all items/files

ARGUMENTS:

count - Show selected number of records
number - Number of records
from - Show records from the specified time
year - Year
month - Month
day - Day
hour - Hour
minute - Minute
second - Second
to - Show records until the selected time

ALIASES:

virlog

EXAMPLES:

get detections from 2011-04-14 01:30:00 - Displays all infiltrations detected after 14th of April 2011 01:30:00
(when defining date, you need to include time as well for the command to work properly)
clear detections - Clears the whole log

EVENTS
This is useful when you need to view information about various events.

SYNTAX:

[get] events [count <number>] [from <year>-<month>-<day> <hour>:<minute>:<second>] [to <year>-<month>-<day> <hour>:<minute>:<second>]
clear events

OPERATIONS:

get - Returns current setting/status
clear - Removes all items/files
ARGUMENTS:

- **count**: Show selected number of records
- **number**: Number of records
- **from**: Show records from the specified time
- **year**: Year
- **month**: Month
- **day**: Day
- **hour**: Hour
- **minute**: Minute
- **second**: Second
- **to**: Show records until the selected time

ALIASES:

- **warnlog**

EXAMPLES:

- **get events from 2011-04-14 01:30:00** - Displays all events that occurred after 14th of April 2011 01:30:00 (when defining date, you need to include time as well for the command to work properly)
- **clear events** - Clears the whole log

FILTER

Minimum verbosity of events to display.

SYNTAX:

```
[get] | restore filter
```

```
set filter [[none] [critical] [errors] [warnings] [informative] [diagnostic] [all]] [smart]
```

OPERATIONS:

- **get** - Returns current setting/status
- **set** - Sets value/status
- **restore** - Restores default settings/object/file

ARGUMENTS:

- **none**: No records
- **critical**: Critical errors
- **errors**: Errors
- **warnings**: Warnings
- **informative**: Informative records
- **diagnostic**: Diagnostic records
- **all**: All records
- **smart**: Smart filtering

SCANNERS

'Computer scan' log or log list.

SYNTAX:

```
[get] scanners [id <id>] [count <number>] [from <year>-<month>-<day> <hour>:<minute>:<second>] [to <year>-
```
clear scanners

OPERATIONS:

get - Returns current setting/status

clear - Removes all items/files

ARGUMENTS:

id - Show computer scan details with ID
id - Scan ID

count - Show only selected number of records

number - Number of records

from - Show only records from the selected time

year - Year

month - Month

day - Day

hour - Hour

minute - Minute

second - Second

to - Show only records from the selected time

VERBOSITY

Minimum logging verbosity.

SYNTAX:

[get] | restore verbosity

set verbosity critical | errors | warnings | informative | diagnostic

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

critical - Critical errors

to - Critical errors

to - Errors

to - Warnings

informative - Informative records

to - Informative records

diagnostic - Diagnostic records

to - Diagnostic records
3.1.2.67 Context - TOOLS LOG CLEANING

TIMEOUT

Log record lifetime (days).

SYNTAX:

[get] | restore timeout

set timeout <number>

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

number - Days (1 - 365)

USE

Automatic log deletion.

SYNTAX:

[get] | restore use

set use disabled | enabled

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting

enabled - Enables function/activates setting

3.1.2.68 Context - TOOLS LOG OPTIMIZE

LEVEL

Optimization by exceeding the number of unused records (percentage).

SYNTAX:

[get] | restore level

set level <number>

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

number - Percentage of unused records (1 - 100)

USE
Automatic log optimization.

SYNTAX:

\[
\text{[get]} | \text{restore use} \\
\text{set use disabled | enabled}
\]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.69 Context - TOOLS NOTIFICATION

VERBOSITY

Minimum verbosity for notifications.

SYNTAX:

\[
\text{[get]} | \text{restore verbosity} \\
\text{set verbosity critical | errors | warnings | informative | diagnostic}
\]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

critical - Critical errors
errors - Errors
warnings - Warnings
informative - Informative records
diagnostic - Diagnostic records

3.1.2.70 Context - TOOLS NOTIFICATION EMAIL

FROM

Senders email address.

SYNTAX:

\[
\text{[get]} | \text{restore from} \\
\text{set from \text{[<string>]}}
\]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:
  string - E-mail address

LOGIN
Login name.

SYNTAX:
  [get] | restore login
  set login [string]

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  string - Name

PASSWORD
Password.

SYNTAX:
  [get] | restore password
  set password [plain <password>]

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  plain - Switch to entering password as parameter
  password - Password

SERVER
SMTP server address.

SYNTAX:
  [get] | restore server
  set server [string]

OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file

ARGUMENTS:
  string - Address

TO
Recipients e-mail address.
SYNTAX:

[get] | restore to
set to [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - E-mail address

USE

Sending events by email.

SYNTAX:

[get] | restore use
set use disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.71 Context - TOOLS NOTIFICATION MESSAGE

ENCODING

Warning messages encoding.

SYNTAX:

[get] | restore encoding
set encoding nolocal | localcharset | localencoding | ISO-2022-JP

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

nolocal - Do not use national alphabet characters
localcharset - Use national alphabet characters
localencoding - Use national alphabet characters and encoding
ISO - Use ISO-2022-JP encoding (For japanese version only)
3.1.2.72 Context - TOOLS NOTIFICATION MESSAGE FORMAT

DETECTION
Format of threat warning messages.

SYNTAX:

\[
\text{[get]} \mid \text{restore detection}
\]
\[
\text{set detection} \ [\text{<string>}] 
\]

OPERATIONS:

- \text{get} - Returns current setting/status
- \text{set} - Sets value/status
- \text{restore} - Restores default settings/object/file

ARGUMENTS:

- \text{string} - Message format

Message format options:

- \%TimeStamp\% - Date and time of the event
- \%Scanner\% - Module that has detected the event
- \%ComputerName\% - Computer name
- \%ProgramName\% - Program which has caused the event
- \%ErrorDescription\% - Error description

For message format, you need to replace key words (listed here between percent sign “%”) with the corresponding values.

NOTE: ESET File Security virus messages and warnings have default format. Changing this format is not recommended. You can change the format in case when you are using automatic email handling system.

EVENT
Event format.

SYNTAX:

\[
\text{[get]} \mid \text{restore event}
\]
\[
\text{set event} \ [\text{<string>}] 
\]

OPERATIONS:

- \text{get} - Returns current setting/status
- \text{set} - Sets value/status
- \text{restore} - Restores default settings/object/file

ARGUMENTS:

- \text{string} - Message format

Message format options:

- \%TimeStamp\% - Date and time of the event
- \%Scanner\% - Module that has detected the event
- \%ComputerName\% - Computer name
- \%ProgramName\% - Program which has caused the event
%InfectedObject% - Infected object (file, e-mail, ...)

%VirusName% - Virus name

For massage format, you need to replace key words (listed here between percent sign “%”) with the corresponding values.

NOTE: ESET File Security virus messages and warnings have default format. Changing this format is not recommended. You can change the format in case when you are using automatic email handling system.

3.1.2.73 Context - TOOLS NOTIFICATION WINPOPUP

ADDRESS
Send notifications to computer names.

SYNTAX:

[get] | restore address

   set address [<string>]

OPERATIONS:

   get - Returns current setting/status

   set - Sets value/status

   restore - Restores default settings/object/file

ARGUMENTS:

   string - Computer name separated by a comma

TIMEOUT
Interval of sending to LAN computers.

SYNTAX:

[get] | restore timeout

   set timeout <number>

OPERATIONS:

   get - Returns current setting/status

   set - Sets value/status

   restore - Restores default settings/object/file

ARGUMENTS:

   number - Interval in seconds (1 - 3600)

USE
Send events to LAN computers.

SYNTAX:

[get] | restore use

   set use disabled | enabled

OPERATIONS:

   get - Returns current setting/status

   set - Sets value/status

   restore - Restores default settings/object/file
ARGUMENTS:

- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

3.1.2.74  Context - TOOLS SCHEDULER

**ACTION**

Scheduled task action.

**SYNTAX:**

```
[get] action
```

```
set action external | logmaintenance | startupcheck | status | scan | update
```

**OPERATIONS:**

- get - Returns current setting/status
- set - Sets value/status

**ARGUMENTS:**

- external - Run external application
- logmaintenance - Log maintenance
- startupcheck - Startup scan
- status - Create a computer status snapshot
- scan - Computer scan
- update - Update

**TASK**

Scheduled tasks.

**SYNTAX:**

```
[get] | select task [<ID>]
```

```
set task <ID> disabled | enabled
add task <task_name>
remove | start task <ID>
```

**OPERATIONS:**

- get - Returns current setting/status
- set - Sets value/status
- select - Selects item
- add - Add item
- remove - Removes item
- start - Starts task

**ARGUMENTS:**

- ID - Task ID
- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting
- task_name - Task name
TRIGGER
Task execution.
SYNTAX:

[get] trigger

set trigger once | repeat | daily | weekly | event

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

once - Once
repeat - Repeatedly
daily - Daily
weekly - Weekly
event - Event triggered

3.1.2.75 Context - TOOLS SCHEDULER EVENT

INTERVAL
Run the task only once within the specified interval (hours).
SYNTAX:

[get] interval

set interval <hours>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

hours - Time in hours (1 - 720 hours)

TYPE
Event triggered task.
SYNTAX:

[get] type

set type startup | startuponedaily | dialup | engineupdate | appupdate | logon | detection

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

startup - Computer start
startuponedaily - The first time the computer starts each day
dialup - Dial-up connection to the Internet/VPN
engineupdate - Virus signature update
appupdate - Program component update
logon - User logon
detection - Threat detection

3.1.2.76 Context - TOOLS SCHEDULER FAILSAFE

EXECUTE
Action to take if the task is not run.
SYNTAX:

[get] execute
set execute asap | iftimeout | no

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
asap - Run the task as soon as possible
iftimeout - Run the task immediately if the time since its last execution exceeds specified interval
no - Do not run with delay

NOTE: To set a limit enter SET TOOLS SCHEDULER EDIT FAILSAFE TIMEOUT <HOURS>.

TIMEOUT
Task interval (hours).
SYNTAX:

[get] timeout
set timeout <hours>

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
hours - Time in hours (1 - 720 hours)

3.1.2.77 Context - TOOLS SCHEDULER PARAMETERS CHECK

LEVEL
Scan level.
SYNTAX:

[get] level
set level [before_logon | after_logon | most_frequent | frequent | common | rare | all]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status

ARGUMENTS:
before_logon - Files run before user logon
after_logon - Files run after user logon
most_frequent - Only the most frequently used files
frequent - Frequently used files
common - Commonly used files
rare - Rarely used files
all - Registered files

PRIORITY
Scan priority.

SYNTAX:

[get] priority
set priority [normal | low | lowest | idle]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

normal - Normal
low - Lower
lowest - Lowest
idle - When idle

3.1.2.78  Context - TOOLS SCHEDULER PARAMETERS EXTERNAL

ARGUMENTS
Arguments.

SYNTAX:

[get] arguments
set arguments <arguments>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status

ARGUMENTS:

arguments - Arguments

DIRECTORY

Work folder.

SYNTAX:

[get] directory
set directory <path>

OPERATIONS:

get - Returns current setting/status
**set** - Sets value/status

**ARGUMENTS:**

`path` - Path

**EXECUTABLE**

Executable file.

**SYNTAX:**

```
[get] executable
set executable <path>
```

**OPERATIONS:**

- `get` - Returns current setting/status
- `set` - Sets value/status

**ARGUMENTS:**

`path` - Path

---

**3.1.2.79  Context - TOOLS SCHEDULER PARAMETERS SCAN**

**PROFILE**

Scan profile.

**SYNTAX:**

```
[get] profile
set profile <profile>
```

**OPERATIONS:**

- `get` - Returns current setting/status
- `set` - Sets value/status

**ARGUMENTS:**

`profile` - Profile name

**READONLY**

Scan without cleaning.

**SYNTAX:**

```
[get] readonly
set readonly disabled | enabled
```

**OPERATIONS:**

- `get` - Returns current setting/status
- `set` - Sets value/status

**ARGUMENTS:**

`disabled` - Disables function/deactivates setting
`enabled` - Enables function/activates setting

**TARGET**

Scan targets.

**SYNTAX:**
OPERATIONS:

- get - Returns current setting/status
- add - Add item
- remove - Removes item
- clear - Removes all items/files

ARGUMENTS:

- path - Scan path/Target

3.1.2.80  Context - TOOLS SCHEDULER PARAMETERS UPDATE

PRIMARY

Update profile.

SYNTAX:

```
[get] primary
set primary [<profile>]
```

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status

ARGUMENTS:

- profile - Profile name

SECONDARY

Alternate update profile.

SYNTAX:

```
[get] secondary
set secondary [<profile>]
```

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status

ARGUMENTS:

- profile - Profile name
3.1.2.81  Context - TOOLS SCHEDULER REPEAT
INTERVAL
Task interval (minutes).
SYNTAX:
   [get] interval
   set interval <minutes>
OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
ARGUMENTS:
   minutes - Time in minutes (1 - 720 hours)

3.1.2.82  Context - TOOLS SCHEDULER STARTUP
DATE
Task will be run on the selected date.
SYNTAX:
   [get] date
   set date <year>-<month>-<day>
OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
ARGUMENTS:
   year - Year
   month - Month
   day - Day
DAYS
Run the task on the selected days.
SYNTAX:
   [get] days
   set days [none] [monday] [tuesday] [wednesday] [thursday] [friday] [saturday] [sunday] [all]
OPERATIONS:
   get - Returns current setting/status
   set - Sets value/status
ARGUMENTS:
   none - No specified day
   monday - Monday
   tuesday - Tuesday
   wednesday - Wednesday
Thursday - Thursday
Friday - Friday
Saturday - Saturday
Sunday - Sunday
all - Every day

TIME
Task will be run at the selected time.
SYNTAX:
[get] time
  set time <hour>:<minute>:<second>
OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
ARGUMENTS:
  hour - Hour
  minute - Minute
  second - Second

3.1.2.83 Context - UPDATE
CACHE
Clear update cache.
SYNTAX:
  clear cache

COMPONENTS
Update program components.
SYNTAX:
  [get] | restore components
  set components never | allways | ask
OPERATIONS:
  get - Returns current setting/status
  set - Sets value/status
  restore - Restores default settings/object/file
ARGUMENTS:
  never - Do not update
  allways - Always update
  ask - Ask before downloading program components

LOGIN
Login username.
SYNTAX:
[get] | restore login
set login [<string>]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
string - Name

NOTE: Please enter the Username and Password received after purchase or activation. We strongly recommend that you copy (Ctrl+C) from your registration email and paste it (Ctrl+V).

PASSWORD
Password.

SYNTAX:
[get] | restore password
set password [plain <password>]

OPERATIONS:
get - Show password
set - Set of delete password
restore - Restores default settings/object/file

ARGUMENTS:
plain - Switch to enter password as parameter
password - Password

NOTE: Please enter the Username and Password received after purchase or activation. We strongly recommend that you copy (Ctrl+C) from your registration email and paste it (Ctrl+V).

PRERELEASE
Enable pre-release updates.

SYNTAX:
[get] | restore prerelease
set prerelease disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

PROFILE
Update profile management.

SYNTAX:
[get] profile
select | remove profile <name>
add profile new: <name> [copyfrom: <name>]

OPERATIONS:

get - Returns current setting/status
select - Selects item
add - Add item
remove - Removes item

ARGUMENTS:

name - Profile name
new - New profile
copyfrom - Copy setting from profile

NOTE: Other context commands refer to the active profile (marked with - x). For the active profile selection use
select update profile <profile name>.

SERVER

Update servers.

SYNTAX:
[get] | restore server
select | add | remove server <server>

OPERATIONS:

get - Returns current setting/status
select - Selects item
add - Add item
remove - Removes item
restore - Restores default settings/object/file

ARGUMENTS:

server - Server address

STATUS

Show update status.

SYNTAX:
[get] status

UPDATE

Update.

SYNTAX:
start | stop update

OPERATIONS:

start - Run update
stop - Cancel update
3.1.2.84  Context - UPDATE CONNECTION

DISCONNECT
Disconnect from server after update.

SYNTAX:

[get] | restore disconnect
set disconnect disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

LOGIN
Username.

SYNTAX:

[get] | restore login
set login [<string>]

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Name

PASSWORD
Password.

SYNTAX:

[get] | restore password
set password [plain <password>]

OPERATIONS:
get - Show password
set - Set or delete password
restore - Restores default settings/object/file

ARGUMENTS:

plain - Switch to enter password as parameter
password - Password

RUNAS
Connect to LAN as.
SYNTAX:

```
[get] | restore runas

set runas system | current | specified
```

OPERATIONS:

- **get**: Returns current setting/status
- **set**: Sets value/status
- **restore**: Restores default settings/object/file

ARGUMENTS:

- **system**: System account (default)
- **current**: Current user
- **specified**: Specified user

### 3.1.2.85 Context - UPDATE MIRROR

**COMPONENTS**

Update program components.

SYNTAX:

```
[get] | start | restore components

set components disabled | enabled
```

OPERATIONS:

- **get**: Returns current setting/status
- **set**: Sets value/status
- **start**: Start update
- **restore**: Restores default settings/object/file

ARGUMENTS:

- **disabled**: Disables function/deactivates setting
- **enabled**: Enables function/activates setting

**FOLDER**

Folder to store mirrored files.

SYNTAX:

```
[get] | restore folder

set folder [<string>]
```

OPERATIONS:

- **get**: Returns current setting/status
- **set**: Sets value/status
- **restore**: Restores default settings/object/file

ARGUMENTS:

- **string**: Folder path

**LOGIN**

Username.
SYNTAX:

```
[get] | restore login
set login [<string>]
```

OPERATIONS:

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:

```
string - Name
```

**PASSWORD**

Password.

SYNTAX:

```
[get] | restore password
set password [plain <password>]
```

OPERATIONS:

- `get` - Show password
- `set` - Set or delete password
- `restore` - Restores default settings/object/file

ARGUMENTS:

```
plain - Switch to enter password as parameter
password - Password
```

**USE**

Create update mirror.

SYNTAX:

```
[get] | restore use
set use disabled | enabled
```

OPERATIONS:

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

ARGUMENTS:

```
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting
```

**VERSIONS**

Update version management.

SYNTAX:

```
[get] | restore versions
select versions <version>
```
OPERATIONS:

get - Show available versions
select - Select/Deselect update version
restore - Restores default settings/object/file

ARGUMENTS:
version - Version name

3.1.2.86 Context - UPDATE MIRROR CONNECTION

DISCONNECT

Disconnect from server after update.

SYNTAX:

[get] | restore disconnect
    set disconnect disabled | enabled

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

LOGIN

Username.

SYNTAX:

[get] | restore login
    set login [<string>]

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

string - Name

PASSWORD

Password.

SYNTAX:

[get] | restore password
    set password [plain <password>]

OPERATIONS:

get - Show password
set - Set or delete password
restore - Restores default settings/object/file

ARGUMENTS:

plain - Switch to enter password as parameter
password - Password

RUNAS

Connect to LAN as.

SYNTAX:

[get] | restore runas
     set runas system | current | specified

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

system - System account (default)
current - Current user
specified - Specified user

3.1.2.87 Context - UPDATE MIRROR SERVER

AUTHENTICATION

Use authentication.

SYNTAX:

[get] | restore authentication
     set authentication none | basic | ntlm

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:

none - No
basic - Basic
ntlm - NTLM

PORT

Port.

SYNTAX:

[get] | restore port
     set port <number>

OPERATIONS:

get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
number - Port number

USE
Provide update files via internal HTTP server.

SYNTAX:

[get] | restore use
set use disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

3.1.2.88 Context - UPDATE NOTIFICATION
DOWNLOAD
Ask before downloading update.

SYNTAX:

[get] | restore download
set download disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file

ARGUMENTS:
disabled - Disables function/deactivates setting
enabled - Enables function/activates setting

HIDE
Do not display notification about successful update.

SYNTAX:

[get] | restore hide
set hide disabled | enabled

OPERATIONS:
get - Returns current setting/status
set - Sets value/status
restore - Restores default settings/object/file
ARGUMENTS:

- disabled - Disables function/deactivates setting
- enabled - Enables function/activates setting

SIZE

Ask if an update file is greater than (kB).

SYNTAX:

```
[get] | restore size
set size <number>
```

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- number - File size (kB)

NOTE: To disable update notifications enter 0.

3.1.2.89 Context - UPDATE PROXY

LOGIN

Username.

SYNTAX:

```
[get] | restore login
set login [<string>]
```

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- string - Name

MODE

HTTP proxy setup.

SYNTAX:

```
[get] | restore mode
set mode global | noproxy | userdefined
```

OPERATIONS:

- get - Returns current setting/status
- set - Sets value/status
- restore - Restores default settings/object/file

ARGUMENTS:

- global - Use global proxy server settings
noproxy - Do not use proxy server
userdefined - Connection through a proxy server

**PASSWORD**
Password.

**SYNTAX:**

```bash
[get] | restore password
set password [plain <password>]
```

**OPERATIONS:**

- `get` - Show password
- `set` - Set or delete password
- `restore` - Restores default settings/object/file

**ARGUMENTS:**

- `plain` - Switch to enter password as parameter
- `password` - Password

**PORT**
Proxy server port.

**SYNTAX:**

```bash
[get] | restore port
set port <number>
```

**OPERATIONS:**

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

**ARGUMENTS:**

- `number` - Port number

**SERVER**
Proxy server.

**SYNTAX:**

```bash
[get] | restore server
set server [<string>]
```

**OPERATIONS:**

- `get` - Returns current setting/status
- `set` - Sets value/status
- `restore` - Restores default settings/object/file

**ARGUMENTS:**

- `string` - Server address
3.1.2.90 Context - UPDATE SYSTEM

NOTIFY
Notify about missing updates from level.

SYNTAX:

[get] | restore notify

set notify no | optional | recommended | important | critical

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

no - No

optional - Optional

recommended - Recommended

important - Important

critical - Critical

RESTART

Restart computer after program component update.

SYNTAX:

[get] | restore restart

set restart never | ask | auto

OPERATIONS:

get - Returns current setting/status

set - Sets value/status

restore - Restores default settings/object/file

ARGUMENTS:

never - Do not restart

ask - Ask before restart

auto - Restart automatically

3.2 Automatic exclusions

The developers of server applications and operating systems recommend excluding sets of critical working files and folders from antivirus scans for most of their products. Antivirus scans may have a negative influence on a server’s performance, lead to conflicts and even prevent some applications from running on the server. Exclusions help minimize the risk of potential conflicts and increase the overall performance of the server when running antivirus software.

ESET File Security identifies critical server applications and server operating system files and automatically adds them to the list of Exclusions. Once added to the list, the server process/application will be enabled (by default) with the following result:

1) If an application/operating system exclusion remains enabled (Autoexclusions), any of its critical files and folders
will be added to the list of files excluded from scanning (to see the list of current exclusions use `av exclusions` command). Every time the server is restarted, the system performs an automatic check of exclusions and restores any exclusions that may have been deleted from the list. This is the recommended setting, if you wish to make sure the recommended Automatic exclusions are always applied. To see what applications/operating systems are excluded, use `server autoexclusions` command.

2) If the user disables an application/operating system exclusion, its critical files and folders remain on the list of files excluded from scanning. However, they will not be automatically checked and renewed on the **Exclusions** list every time the server is restarted (see point 1 above). We recommend this setting for advanced users, who wish to remove or modify some of the standard exclusions. If you wish to have removed the exclusions from the list without restarting the server, you will need to remove them manually from the list (use exclusions command, e.g. `av exclusions remove C:\pagefile.sys`).

Any user-defined exclusions entered manually under using `exclusions` command will not be affected by the settings described above.

The Automatic exclusions of server applications/operating systems are selected based on Microsoft’s recommendations. For details, please see the following links:

- [http://support.microsoft.com/kb/822158](http://support.microsoft.com/kb/822158)
- [http://support.microsoft.com/kb/245822](http://support.microsoft.com/kb/245822)
- [http://support.microsoft.com/kb/823166](http://support.microsoft.com/kb/823166)

### 3.3 Import and export settings

Importing and exporting configurations of ESET File Security is available by using `config` command.

To export configuration use `general export config <path>` (replace `<path>` with the destination and file name you want the configuration to be exported to, e.g. `general export config c:\installers\configuration.xml`).

To import configuration use `general import config <path>` (e.g. `general import config c:\installers\configuration.xml`).

Both import and export use the `.xml` file type. Import and export are useful if you need to backup the current configuration of ESET File Security to be able to use it later. The export settings option is also convenient for users who wish to use their preferred configuration of ESET File Security on multiple systems - they can easily import an `.xml` file to transfer the desired settings.

### 3.4 Remote administration

ESET Remote Administrator (ERA) is a powerful tool to manage security policy and to obtain an overview of the overall security within a network. It is especially useful when applied to larger networks. ERA not only increases the security level, but also provides ease-of-use in the administration of ESET File Security on client machines.

Remote administration setup options are available under context `GENERAL REMOTE`.

You can configure remote administration by specifying the following:

- **Server address**: Network address of the server where the ERA Server is installed.
- **Primary server, Secondary server**: Usually, only Primary server needs to be configured. If you are running multiple ERA servers on the network, you can opt to add another, Secondary ERA server connection. It will serve as the fallback solution. So if the Primary server becomes inaccessible, the ESET security solution will automatically contact the Secondary ERAs. Concurrently, it will attempt to reestablish the connection to the Primary server. After this connection is active again, ESET security solution will switch back to the Primary server. Configuring two remote administration server profiles is best used for mobile clients with notes connecting both from the local network and from outside the network.

Optional settings:
**Port**: This is a predefined server port used for connection. We recommend that you leave the default port setting of 2222. In case your ERA server is using different port, you the port of your ERA server.

**Password**: Allows you to enter a password to connect to the ERA Server, if required.

**Encrypt**: Use this option to block connection to ERA servers where unauthenticated access is enabled.

**Interval**: (connections interval in min.) This designates the frequency that ESET File Security will connect to the ERA Server. If it is set to 0, information will be submitted every 5 seconds. Default is set to 10 min.

Once you have everything configured, you can activate remote administration (see below for details).

Examples:

- To specify ERA server navigate to **GENERAL REMOTE SERVER PRIMARY** context and execute `set address <servername>` (replace `<servername>` with your ERA server’s host name or IP address).
- To activate remote administrator, execute `set use enabled` command from within **GENERAL REMOTE** context (alternatively you can use `general remote set use enabled` command from eShell root). ESET File Security will use previously specified settings to connect to the ERA Server.

### 3.5 Licenses

Command **License** allows you to manage the license keys for ESET File Security. After purchase, license key file is delivered to you along with your username and password. The license key is a text file containing information about the purchased product: the owner, number of licenses, and the expiration date.

Examples:

- To add new license, execute `general import license <path>` command (replace `<path>` with the exact path where the license file is located in, e.g. `general import license c:\eset_licenses\nod32.lic`).
- To export license (in case you want to use it on other server, in case of server migration, etc.), execute `general export license <ID> <path>` command (replace `<ID>` by the license ID, which can be seen by using `general get license` Command, also replace `<path>` with the path where you want the license to be exported to).
- You can also remove the license using the `general remove license <ID>` (replace `<ID>` by the license ID, which can be seen by using `general get license` Command, e.g. `general remove license 2` if you have multiple licenses on one server and want to remove license ID #2).
4. Glossary

4.1 Types of infiltration

An infiltration is a piece of malicious software trying to enter and/or damage a user's computer.

4.1.1 Viruses

A computer virus is an infiltration that corrupts existing files on your computer. Viruses are named after biological viruses, because they use similar techniques to spread from one computer to another.

Computer viruses mainly attack executable files and documents. To replicate, a virus attaches its “body” to the end of a target file. In short, this is how a computer virus works: after execution of the infected file, the virus activates itself (before the original application) and performs its predefined task. Only after that is the original application allowed to run. A virus cannot infect a computer unless a user, either accidentally or deliberately, runs or opens the malicious program by him/herself.

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. On the other hand, some viruses do not cause any damage – they only serve to annoy the user and demonstrate the technical skills of their authors.

It is important to note that viruses (when compared to trojans or spyware) are increasingly rare because they are not commercially enticing for malicious software authors. Additionally, the term “virus” is often used incorrectly to cover all types of infiltrations. This usage is gradually being overcome and replaced by the new, more accurate term “malware” (malicious software).

If your computer is infected with a virus, it is necessary to restore infected files to their original state – i.e., to clean them by using an antivirus program.

Examples of viruses are: OneHalf, Tenga, and Yankee Doodle.

4.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. The basic difference between a virus and a worm is that worms have the ability to replicate and travel by themselves – they are not dependent on host files (or boot sectors). Worms spread through email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours or even minutes of their release. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a “means of transport” for other types of infiltrations.

If your computer is infected with a worm, we recommend you delete the infected files because they likely contain malicious code.

Examples of well-known worms are: Lovsan/Blaster, Stration/Warezov, Bagle, and Netsky.

4.1.3 Trojan horses

Historically, computer trojan horses have been defined as a class of infiltrations which attempt to present themselves as useful programs, thus tricking users into letting them run. But it is important to note that this was true for trojan horses in the past– today, there is no longer a need for them to disguise themselves. Their sole purpose is to infiltrate as easily as possible and accomplish their malicious goals. “Trojan horse” has become a very general term describing any infiltration not falling under any specific class of infiltration.

Since this is a very broad category, it is often divided into many subcategories:

- **Downloader** – A malicious program with the ability to download other infiltrations from the Internet
- **Dropper** – A type of trojan horse designed to drop other types of malware onto compromised computers
• **Backdoor** – An application which communicates with remote attackers, allowing them to gain access to a system and to take control of it

• **Keylogger** – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers

• **Dialer** – Dialers are programs designed to connect to premium-rate numbers. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used

Trojan horses usually take the form of executable files with the extension .exe. If a file on your computer is detected as a trojan horse, it is advisable to delete it, since it most likely contains malicious code.

**Examples of well-known trojans are:** NetBus, Trojandownloader. Small.ZL, Slapper

4.1.4 **Rootkits**

Rootkits are malicious programs that grant Internet attackers unlimited access to a system, while concealing their presence. Rootkits, after accessing a system (usually exploiting a system vulnerability), use functions in the operating system to avoid detection by antivirus software: they conceal processes, files and Windows registry data, etc. For this reason, it is almost impossible to detect them using ordinary testing techniques.

There are two levels of detection to prevent rootkits:

1) When they try to access a system. They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).

2) When they are hidden from the usual testing. ESET File Security users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

4.1.5 **Adware**

Adware is a short for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is frequently bundled with freeware programs, allowing their creators to cover development costs of their (usually useful) applications.

Adware itself is not dangerous – users will only be bothered with advertisements. Its danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, please pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This means that adware may often access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry. If there is a file detected as adware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

4.1.6 **Spyware**

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user's contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program's installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory – they appear to be antispyware programs, but in fact they are spyware programs themselves.
If a file is detected as spyware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

4.1.7 Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes. ESET File Security provides the option to detect such threats.

"Potentially unsafe applications" is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program that records each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

4.1.8 Potentially unwanted applications

Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes are:

- New windows you haven't seen previously are opened
- Activation and running of hidden processes
- Increased usage of system resources
- Changes in search results
- Application communicates with remote servers