ESET

REMOTE ADMINISTRATOR 5

Installation Manual and User Guide

(intended for product version 5.3 and higher)

Click here to download the most recent version of this document

ESET REMOTE ADMINISTRATOR 5

Customer Care Worldwide: http://support.eset.com

REV. 3/1/2016

Contents

1. Introduction

ESET Remote Administrator (ERA) is an application which allows you to manage ESET's products in a networked environment, including workstations and servers – from one central location. With ESET Remote Administrator's built-in task management system, you can install ESET security solutions on remote computers and quickly respond to new problems and threats.

ESET Remote Administrator itself does not provide any other form of protection against malicious code. ERA depends on the presence of an ESET security solution on workstations or servers, such as ESET Endpoint Antivirus or ESET Endpoint Security.

To perform a complete deployment of an ESET security solutions portfolio, the following steps must be taken:

- Installation of ERA Server (ERAS),
- Installation of ERA Console (ERAC),
- Installation on client computers (ESET Endpoint Antivirus, ESET Endpoint Security, etc...).

NOTE: Some parts of this document use system variables which refer to an exact location of folders and files:

%ProgramFiles% = typically *C:\Program Files*
%ALLUSERSPROFILE% = typically *C:\Documents and Settings\All Users*

1.1 What's new in ESET Remote Administrator version 5.3

ESET Remote Administrator version 5.3

- Remote push installation improvements and new methods (WMI)
- Support for IPv6
- Command-line interface and API improvements (more commands)
- 64bit API available
- Duplicate clients can now be merged
- Package management improvements

Click here if you use ESET Remote Administrator version 6.x

ESET Remote Administrator version 5.2

- API with documented source code and command-line console
- Remote deployment for Linux and Apple Mac
- Reports in PDF documents
- Dual IP address reporting
- Basic network Actions (Wake-on-LAN, Ping, RDP session, Message, Shutdown, Custom) are now available from the console
- Remote installation of custom packages with redirected output
- Simplified log forwarding

ESET Remote Administrator version 5.1

- Adding new supported product - ESET File Security for Microsoft SharePoint Server
- Adding new supported product - ESET Security 4.5 for Kerio
- Upgrade for supported product - ESET File Security For Microsoft Windows Server
- Upgrade for supported product - ESET Mail Security For Microsoft Exchange Server
- Upgrade for supported product - ESET Mail Security For IBM Lotus Domino
- Upgrade for supported product - ESET Gateway Security for Microsoft Forefront TMG
- Upgrade for supported product - Endpoint Security for Android
- Adding remote install method for Endpoint Security for Android
- Upgrade for supported product - ESET Endpoint Security
- Upgrade for supported product - ESET Endpoint Antivirus
- Dashboard improvements - in-browser edit mode for dashboard templates
- Policies - visual policy manager UI re-design while adding further policy meta-data
- SMTPs mail server support for notifications and reports
- Replication scheme: Ability to skip verification of incoming lower server versus predefined static list
- Apple Open Directory and OpenLDAP support for network search and group synchronization
- Policy migration to convert v3/v4-settings to v5-compatible configuration

ESET Remote Administrator version 5.0

- Web Dashboard for administrators - comprehensive overview of reports in your web browser
- Remote Installation - new design
- Protection Features - new task for managing protection features on clients
- Run Scheduled Task - new task to immediately trigger a scheduled task on a client
- User Manager - tool for managing accounts and passwords for console access
- HIPS tab - information about HIPS related events from clients
- Web Control tab - information about Web Control related events from clients
- Device Control tab - information about Device Control related events from clients
- Antispam tab - information about spam-related events from clients
- Greylist tab - information about Greylist related messages from clients
- Search for computers in the network - new search tasks and design
- Supports installation over previous ERA versions (4.x, 3.x) including data migration
- Reports - new reports, new design, support for web dashboards

1.2 Program architecture

Technically, ESET Remote Administrator consists of two separate components: ERA Server (ERAS) and ERA Console (ERAC). You can run an unlimited number of ERA Servers and Consoles on your network as there are no limitations in the license agreement for their use. The only limitation is the total number of clients your installation of ERA can administer.

ERA Server (ERAS)

The server component of ERA runs as a service under the following Microsoft Windows® NT-based operating systems 8. The main task of this service is to collect information from clients and to send them various requests. These requests, including configuration tasks, remote installation requests, etc., are created through the ERA Console (ERAC). ERAS is a meeting point between ERAC and client computers – a place where all information is processed, maintained or modified before being transferred to clients or to ERAC.

ERA Console (ERAC)

ERAC is the client component of ERA and is usually installed on a workstation. This workstation is used by the administrator to remotely control ESET solutions on individual clients. Using ERAC, the administrator can connect to the server component of ERA – on TCP port 2223. The communication is controlled by the process console.exe, which is usually located in the following directory:

%ProgramFiles%\ESET\ESET Remote Administrator\Console

When installing ERAC, you may need to enter the name of an ERAS. Upon startup, the console will automatically connect to this server. ERAC can also be configured after installation.

1.3 Supported products and languages

ESET Remote Administrator 5.3 is able to deploy, activate (with Username/Password) or manage the following ESET products:

Manageable via ESET Remote Administrator 5	Up to product version
ESET Endpoint Security for Windows	5.x
ESET Endpoint Antivirus for Windows	5.x
ESET File Security for Microsoft Windows Server	4.x
ESET NOD32 Antivirus 4 Business Edition for Mac OS X	4.x
ESET NOD32 Antivirus 4 Business Edition for Linux Desktop	4.x
ESET Mail Security for Microsoft Exchange Server	4.x
ESET Mail Security for IBM Lotus Domino	4.x
ESET Security for Microsoft Windows Server Core	4.x
ESET Security for Microsoft SharePoint Server	4.x
ESET Security for Kerio	4.x
ESET NOD32 Antivirus Business Edition	4.2.76
ESET Smart Security Business Edition	4.2.76
ESET Mobile Security for Symbian	1.x
ESET Mobile Security for Windows Mobile	1.x
ESET Mobile Security for Android	3.x

Supported languages

Language	Code
English (United States)	ENU
Chinese Simplified	CHS
Chinese Traditional	CHT
French (France)	FRA
German (Germany)	DEU
Italian (Italy)	ITA
Japanese (Japan)	JPN
Korean (Korea)	KOR
Polish (Poland)	PLK
Portuguese (Brazil)	PTB
Russian (Russia)	RUS
Spanish (Chile)	ESL
Spanish (Spain)	ESN

2. Installation of ERA Server and ERA Console

2.1 Requirements

ERAS works as a service, and therefore requires a Microsoft Windows NT-based operating system. Although the Microsoft Windows Server Edition is not necessary for ERAS to work, we recommend installing ERAS on server-based operating systems for smooth operation. A computer with ERAS installed on it should always be online and accessible via computer network by:

- Clients (usually workstations)
- PC with ERA Console
- Other instances of ERAS (if replicated)

NOTE: ESET Remote Administrator 5 supports installation over previous versions 19 including data migration.

2.1.1 Software and database requirements

ERA Server

32-bit operating systems:	Windows 2000 and later (see the **Note**)
64-bit operating systems:	Windows XP and later
Databases:	Microsoft Access (built-in) Microsoft SQL Server 2005 and later MySQL 5.0 and later ORACLE 9i and later Click here for more details 17
Windows Installer:	2.0 and later
Web Dashboard:	Internet Explorer 7.0 and later Mozilla Firefox 3.6 and later Google Chrome 9 and later
HTTP Server:	Same as ERA Server requirements, but it requires SP2 and later on Windows XP
Networking:	IPv4 is fully supported IPv6 is supported from Windows Vista and later

ERA Console

32 bit operating systems:	Windows 2000 and later (see the **Note**)
64 bit operating systems:	Windows XP and later
Windows Installer:	2.0 and later
Internet Explorer:	7.0 and later

Note:

- ERA Console is not supported on Microsoft Windows Server Core 2008 and Microsoft Windows Server Core 2012. ERA Server is supported on these operating systems, but will not support integration with Microsoft Access Database.
- To start the ERA Console, ESET Configuration Editor and the ERA Maintenance Tool on Windows 2000, the *gdiplus.dll* file must be present on your system. Click here to download this file. Extract the file from the installation package and copy it to the directory *C:\WINNT\system32\*.

- The HTTPS Server role is not supported on Windows 2000, so the Dashboard and Mirror functions will not function in HTTPS mode on this operating system. To use the Dashboard feature on a Windows 2000 server, edit your settings so that the Dashboard no longer defaults to run in HTTPS mode.
- Remote installation for Linux/MAC Security products and some RDP/Shutdown Console Actions functions are not supported on Windows 2000.
- Some operating systems will require you to update trusted root certificates before a successful push installation can be performed. You can update these certificates by running the Windows Update service or by manually importing the latest versions.
- If you use an administrator account to configure SMTP access in **Tools** > **Server Options** > **Other settings** (for IIS or Exchange), outgoing email may not work.
- Some functions (RDP, Shutdown) from **Network Actions** 31 are not available on Windows 2000.

2.1.2 Performance requirements

Server performance may vary depending on the following parameters:

1. Database used

- MS Access database - installed with the server by default. We recommend this solution when servicing hundreds of clients. However, there is a 2GB size limit for the database. Consequently, you will need to activate cleanups on the server and define an interval (under **Tools** > **Server Options** > **Server Maintenance**) for removing old data.
- Other databases (MySQL, MSSQL, ORACLE) require a separate installation, but may result in better server performance. It is essential to use suitable hardware for each database engine (mainly ORACLE) and follow the technical recommendations of its distributor.
- If you choose ORACLE as your database solution, you must set the number of cursors higher than the **Maximum number of active connections** value (under **Tools** > **Server Options** > **Advanced** > **Edit Advanced Settings** > **Advanced**; the default is set to 500). The final number of cursors must take into account the number of lower servers (if replication is used) and cursors that are used by other applications accessing the database engine.
- Typically, the server's performance is higher when using external databases (i.e., installed on a different physical machine).

2. Client connection interval settings

- The client connection interval is set to 10 minutes by default in ESET Endpoint Security / ESET Endpoint Antivirus. If you need the client status to update more or less frequently than the default interval, you can modify this configuration. Keep in mind that a shorter client connection interval will affect server performance.

3. Average number of events reported by clients per connection

- Any information sent from client to server is listed under the particular event (for example, threat log, event log, scan log, or configuration change). This parameter cannot be changed directly, but it can be altered if other settings relevant to it are changed. For example, in advanced server configuration (under **Tools** > **Server Options** > **Server Maintenance**) you can set up the maximum amount of logs that can be accepted by the server (this setting includes clients that connect directly as well as replicated clients). In regular operation the long-term average can be estimated at 1 event every 4 hours per client.

4. Hardware used

For **small installations (under 1000 clients connecting to the ERA Server):**

- Processor type - Pentium IV compatible processor, 2.0 GHz or higher
- RAM - 2 GB
- Network - 1 Gbit

For **medium installations (1000 - 4000 clients connecting to the ERA Server)** we recommend splitting the installation to two computers:

ERA Server:

- Processor type - Pentium IV compatible processor, 2.0 GHz or higher
- RAM - 2 GB
- Network - 1 Gbit

Database Server:

- Processor type - Pentium IV compatible processor, 2.0 GHz or higher
- RAM - 2 GB
- Network - 1 Gbit

Or, you can install both ERA Server and database on one computer:

- Processor type - Pentium IV compatible processor, multi-core, 3.0 GHz or higher
- RAM - 4 GB
- Network - 1 Gbit
- HDD - Raid 0 or SSD Hard drive or both

NOTE: If ERA Server and database are installed on one computer we do not recommend using the MS Access Database because its 2GB size limit necessitates regular database cleanups. Also note that the MS SQL Express Database has only a 4GB size limit.

For **large installations (4000-10 000 clients connecting to the ERA Server)** we recommend splitting the installations to 2 computers and using either MS SQL or Oracle database:

ERA Server:

- Processor type - Pentium IV compatible processor, multi-core, 3.0 GHz or higher
- RAM - 4 GB
- Network - 1 Gbit

Database Server:

- Processor type - Pentium IV compatible processor, multi-core, 3.0 GHz or higher
- RAM - 4 GB
- Network - 1 Gbit
- HDD - Raid 0 or SSD disc or both

For extra large installations (10000 to 20000 clients on one ERA Server) we recommend splitting the installations to 2 computers and using either MS SQL or Oracle database:

ERA Server:

- Processor type - Pentium IV compatible processor, multi-core, 3.0 GHz or higher
- RAM - 8 GB
- Network - 1 Gbit
- HDD - Raid 0 or SSD disc or both

Database Server:

- Processor type - Pentium IV compatible processor, multi-core, 3.0 GHz or higher
- RAM - 8 GB
- Network - 1 Gbit
- HDD - Raid 0 or SSD disc or both

NOTE: All hardware configurations listed above represent the minimum requirements for running ERA. We recommend using a more robust configuration for best performance. We strongly advise using the minimum hardware recommended for your server's operating system when accounting for the number of clients to be serviced. For more information about the database types used and their limits, see Database types supported by

ERA Server 17.
To manage very large numbers of clients, we recommend that you split the load between several servers using replication.

Overload

If a server is overloaded (for example, when connecting 20,000 clients to a server with capacity to service 10,000 clients at a 10 minute interval) some of the clients connected will be skipped. On average, every second client connection will be serviced, as if the client connection interval were set to 20 minutes instead of 10. Every service denial will be logged as follows: "*<SERVERMGR_WARNING> ServerThread: maximum number of threads for active connections reached (500), the server will skip this connection*". Service denials may also occur during temporary server overloads.

You can change the value under the **Maximum number of active connections** (the default is 500) in the advanced server settings, but we recommend doing so only in exceptional cases (for example, when solving specific issues). Should there be an overabundance of system resources and database engine performance, you can use this setting to adjust the overall performance of the server.

Data transfer over a network

During a server's standard operation, we can estimate that a client connecting every 10 minutes will report 0.04 events per connection, which is 1 event reported every 4 hours per client. This will produce ~2 kilobytes of traffic per connection.

In a virus outbreak scenario, with a client reporting 7 events every time it connects, traffic may increase up to 240 kilobytes per connection. If you use compression (default) the data transferred will be approximately 50% smaller in size, i.e., about 120 kilobytes per connection.

The data includes direct client connections and omits replicated connections. Replication occurs much less often and serves to send new events from lower servers. The verbosity level of automatically replicated events can be configured in the advanced settings of the server (under **Tools** > **Server Options** > **Advanced** > **Edit Advanced Settings** > **Replication**). In the Server maintenance section you can configure the maximum level of logs that the upper server will accept (this setting applies clients that connect directly and replicated clients).

Storage capacity requirements

A clean installation of ESET Remote Administrator with an MS Access database requires up to 60 MB of disk space.

Most of the storage space is used by client events that are stored in the database and to a repository on the disk (the default directory is *C:\Documents and Settings\All Users\Application Data\Eset\ESET Remote Administrator\Server*). ERA requires that at least 5% of the disk be free. If this minimum is exceeded the server will stop receiving some of the client events. This setting can be found under **Tools** > **Server Options** > **Advanced** > **Edit Advanced Settings** > **Advanced** > **Maximum disk space usage**. Approximately 10GB per 1000 clients of free disk space is required for regular operation under the default cleanup settings (deleting events older than 3 months).

Case study

A server using an MS Access database that has clients connecting to it every 5 minutes and reporting 7 events (for example, threat log, event log, scan log, configuration change, etc.) per connection on average can temporarily service up to 3000 clients. This scenario depicts a temporary overload situation, such as reporting during a virus outbreak.

If the server uses an external MySQL database and the client connection interval is set to 10 minutes (generating 0.02 events per connection in average) the maximum number of clients the server will be able to service increases to 30,000. Such a scenario exhibits optimal database performance, with clients reporting a relatively small number of events.

In regular operation, using an MS Access database and a client connection interval of 10 minutes enables the server to service a maximum of 10,000 clients.

2.1.3 Ports used

The chart below lists the possible network communications used when ERAS is installed. The process EHttpSrv.exe listens on TCP port 2221 and the process era.exe listens on TCP ports 2222, 2223, 2224 and 2846. Other communications occur using native operating system processes (e.g., ”NetBIOS over TCP/IP”).

Protocol	Port	Description
TCP	2221 (ERAS listening)	Default port used by the Mirror feature integrated in ERAS (HTTP version)
TCP	2222 (ERAS listening)	Communication between clients and ERAS
TCP	2223 (ERAS listening)	Communication between ERAC and ERAS

For all program features to function properly, ensure that the following network ports are open:

Protocol	Port	Description
TCP	2224 (ERAS listening)	Communication between the agent *einstaller.exe* and ERAS during remote install
TCP	2225 (ERAS listening)	Communication between the ESET Dashboard HTTP Server and ERAS
TCP	2846 (ERAS listening)	ERAS replication.
TCP	2226 (ERA Command-line Console)	Connection between ERAS and the Command-line Console
TCP	139 (target port from the point of view of ERAS)	Copying of the agent *einstaller.exe* from ERAS to a client using the share admin$
UDP	137 (target port from the point of view of ERAS)	“Name resolving” during remote install.
UDP	138 (target port from the point of view of ERAS)	“Browsing” during remote install
TCP	445 (target port from the point of view of ERAS)	Direct access to shared resources using TCP/IP during remote install (an alternative to TCP 139)

The predefined ports 2221, 2222, 2223, 2224, 2225 and 2846 can be changed if they are already in use by other applications.

To change the default ports used by ERA, click **Tools** > **Server Options...** To change port 2221, select the **Updates** tab and change the HTTP server port value. Ports 2222, 2223, 2224, 2225 and 2846 can be modified in the **Ports** section of the Other Settings 119 tab.

The predefined ports 2222, 2223, 2224 and 2846 can also be modified during advanced install mode (ERAS).

2.1.4 Computer Search

In order to be able to manage the desired remote computers via ERA Server it is essential the computers can be pinged (ICMP echo request) from the ERA Server . If the target computer is behind a firewall, make sure the ports used 12 to communicate with the ERA Server are enabled (not prohibited by the firewall).

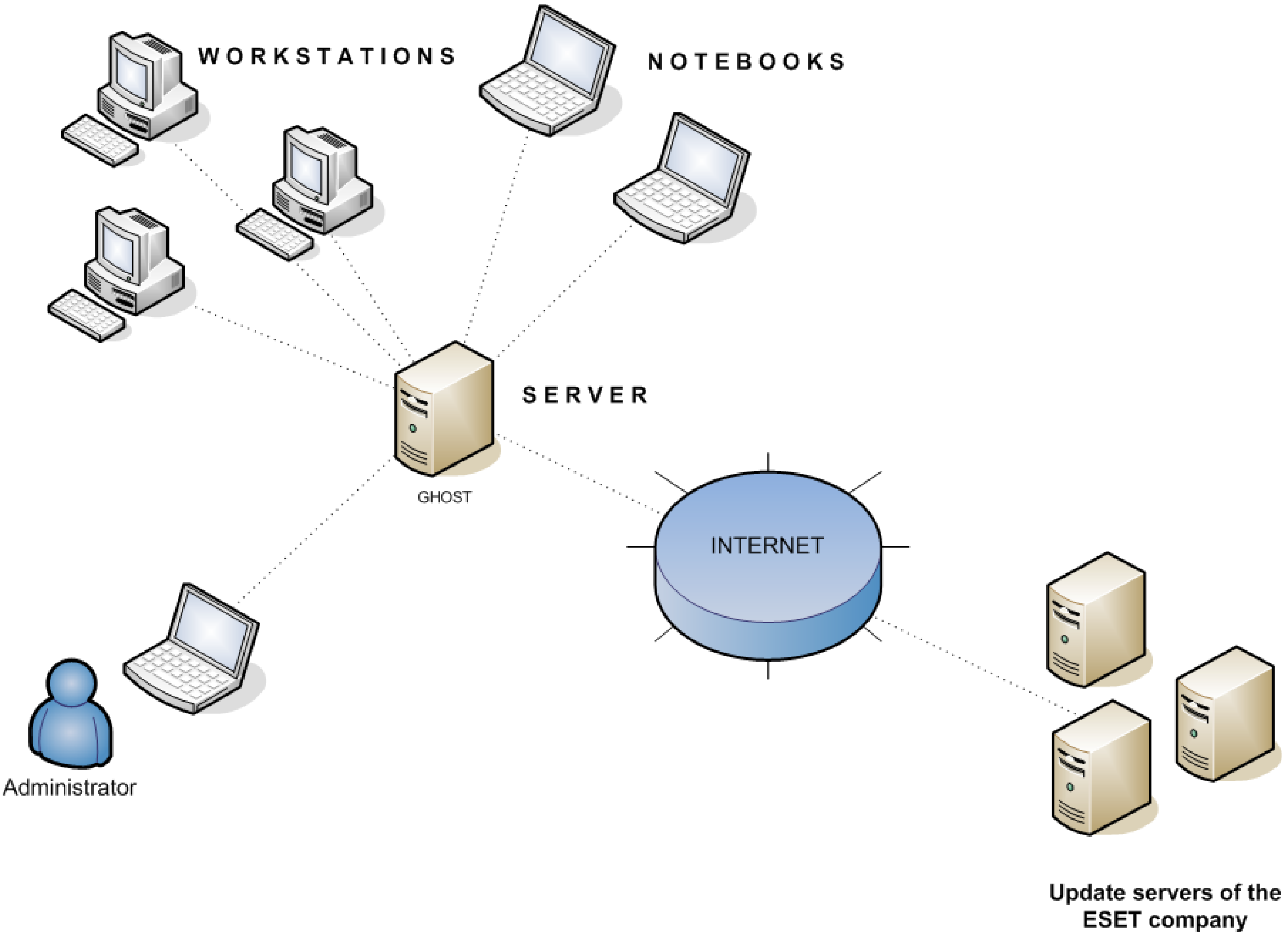
The computers visible to the ERA Server can be seen in the **Computers** tab of **Remote Install** tab of ERA Console. The list of computers is the result of **Default Search Task**. You can alter the configuration of **Default Search Task** or create a new Search Task by clicking **Add new...** and going through the **Network Search Task Wizard: Scan Methods** 45 wizard.

2.2 Basic Installation guide

2.2.1 Environment overview (network structure)

A company network usually consists of one local area network (LAN), therefore we suggest installing one ERAS and one Mirror server. The Mirror server can either be created in ERAS or in ESET Endpoint Antivirus / ESET Endpoint Security.

Suppose all clients are Microsoft Windows workstations and notebooks, networked within a domain. The server named GHOST is online 24/7 and can be a Windows workstation, Professional, or Server Edition (it does not have to be an Active Directory Server). In addition, suppose that notebooks are not present in the company's network during the installation of ESET client solutions. The network structure may resemble the one displayed below:



2.2.2 Before installation

Before installing, the following installation packages should be downloaded from ESET website.

ESET Remote Administrator components

ESET Remote Administrator – Server
ESET Remote Administrator – Console

ESET client/server solutions

See Supported products and languages 7

NOTE: Only download the client solutions you will use on client workstations.

2.2.3 Installation

2.2.3.1 Installation of ERA Server

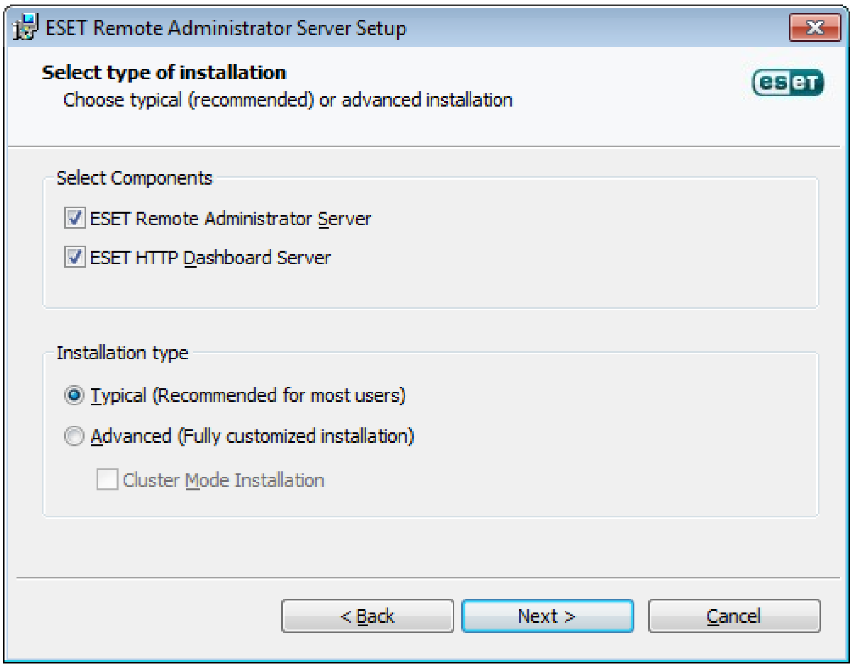
Install ERAS on the server named GHOST (see the example in Environment overview 13). To begin, select the components you want to install. There are two options, **ESET Remote Administrator Server** and **ESET HTTP Dashboard 39 Server**.

For most applications, both components will be installed. You may choose to install the two components on different computers (for example, installing ESET HTTP Dashboard Server on a publicly visible computer while installing ERAS on a computer that is accessible only from a local intranet). Or, you may choose not to use ESET HTTP Dashboard Server.

NOTE: We recommend installing ERAS on a machine running a server operating system.

NOTE: Both the Dashboard and the Mirror server use the same HTTP server (which is installed automatically). So even if you deselect the Dashboard server at the time of the installation, you can enable it later in ESET Configuration Editor (**ERAC** > **Tools** > **Server Options** > **Advanced** > **Dashboards** > **Use local dashboard**).

After choosing the desired components, select either **Typical** or **Advanced** installation mode.


ESET Remote Administrator Server Setup

Select type of installation

Choose typical (recommended) or advanced installation

Select Components

☑ ESET Remote Administrator Server

☑ ESET HTTP Dashboard Server

Installation type

● Typical (Recommended for most users)

○ Advanced (Fully customized installation)

□ Cluster Mode Installation

- If you select **Typical mode**, the program will prompt you to insert a license key (a file with the extension .lic or .zip) that authorizes operation of ERAS for the period defined in the license. Next, the program will ask you to set the update parameters (username, password and update server). You can also proceed to the next step and enter the update parameters later by selecting the check box next to **Set update parameters later** and clicking **Next**.

- Selecting **Advanced installation mode** will allow you to configure additional installation parameters. These parameters can be modified later via the ERAC, but in most cases this is not necessary. The only exception is server name, which should match the DNS name or %COMPUTERNAME% value of your operating system, or the IP address assigned to the computer. This is the most essential piece of information for performing a remote installation. If a name is not specified during installation the installer will automatically supply the value of the system variable %COMPUTERNAME%, which is sufficient in most cases. It is also important to select the database in which ERAS information will be stored. For more information see the chapter titled Database types supported by ERA Server 17. See also Cluster Mode Installation 15.

NOTE: When installing ERAS on a Windows 2000 operating system, we do not recommend using DNS, use the full connection string instead.

Important: Microsoft Windows security policies limit local user account permissions. As a consequence, you may not be able to execute related network operations. Running the ERA service under a local user account may result in push installation issues (e.g., when installing remotely from domain to workgroup). When using Windows Vista, Windows Server 2008 or Windows 7, we recommend running the ERA service under accounts with sufficient networking rights. You can specify the user account under which you want to run ERA in **Advanced installation mode**.

Note: Although ERA Server has full Unicode support, there are situations when the server converts characters to ANSI or vice versa (for example, email, computer name). In such situations the **Language for non-Unicode programs** setting should be used. We recommend that you change this setting to match the server environment locale even if you are not using a localized version of ERA (i.e., you are using the English language mutation). You can find this setting under **Control panel** > **Regional and language options** in the **Advanced** tab.

ERAS program components are installed by default to the following directory:

%ProgramFiles%\ESET\ESET Remote Administrator\Server

Other data components such as logs, installation packages, configuration, etc. are stored in the following directory:

%ALLUSERSPROFILE%\Application Data \ESET\ESET Remote Administrator\Server

ERAS is launched automatically after installation. The activity of the ERAS service is recorded in the following location:

%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\logs\era.log

Command line installation

ERAS can be installed using the following command line parameters:

/q - Silent installation. No user intervention is possible. No dialog windows are displayed.

/qb - No user intervention is possible, but installation progress is indicated by a progress bar.

Example: *era_server_nt32_ENU.msi /qb*

The parameters and configuration of a command line installation can be supplemented by the administrator's *.xml* configuration file, the "*cfg.xml*", which must be in the same folder as the ERA *.msi* installation file. The configuration file can be created in the ESET Configuration Editor and allows you to configure various ERA settings. See the ESET Configuration Editor 58 section for more details.

2.2.3.1.1 Cluster Mode Installation

The **Advanced installation** scenario also allows you to activate the **Cluster Mode Installation**. If the Cluster Mode Installation is enabled you will need to specify the path to a cluster shared data folder that is fully accessible for all cluster nodes (i.e. all nodes must have read/write permissions for this folder). It can either be a quorum disk or a UNC shared folder. If a shared folder is used, you must enable sharing for **Computers** in the shared folder's properties. The cluster node name must then be added to **Share Permissions** with full rights.

NOTE: We do not recommend using an IP Address when defining a shared folder for the cluster.

It is necessary to install ERA Server individually on all cluster nodes. After each ERA Server installation, the ERA Service auto startup needs to be changed to manual. When the ERA Server is installed on all nodes, create the generic service (era_server). The generic service should be dependent of the network name resource in the Cluster administrator.

If anything other than the built-in MS Access database is used, it is important to make sure that all ERA Server nodes connect to the same database. In the next steps it is also important to set the name of the cluster node where ERA is to be installed as the server name.

Important: It is necessary to configure the ESET Remote Administrator Server service (ERA_SERVER) as the cluster's Generic Service in the Cluster Administrator console.

Uninstallation

If you plan to uninstall ERA Server, the cluster group must be online in order for the uninstall process to proceed:

1) Break the cluster by bringing down one of the nodes.

2) Let failover complete to make sure the other node(s) are working.

3) Uninstall ESET Remote Administrator from the disabled node.

4) Restart the node.

5) Relink the node.

6) Repeat the steps above for any additional node(s) in the cluster.

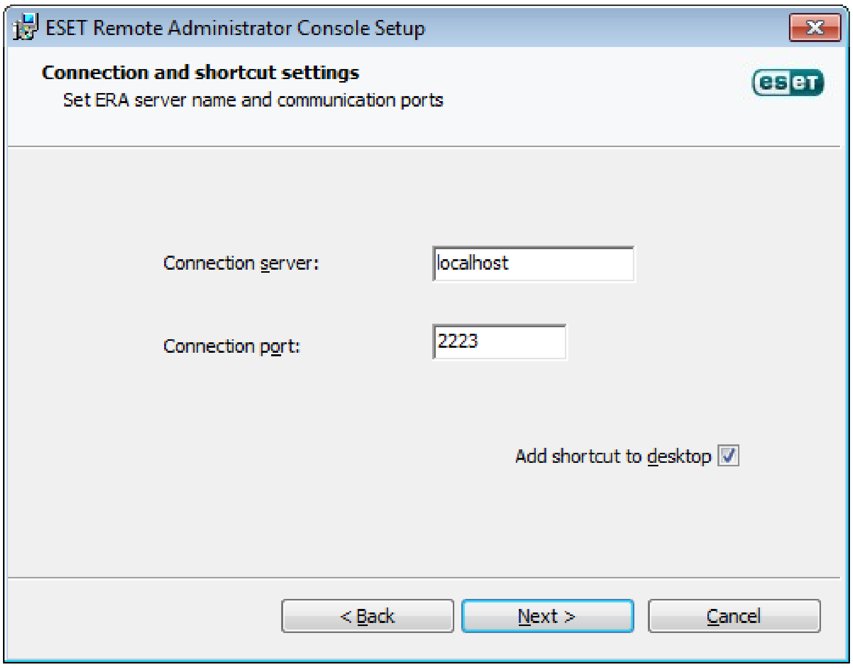
Upgrading ERA installed in cluster mode

By Cluster Mode reinstallation, it is neccessary to take the cluster ERA service group offline by selecting **Take Offline** in the Cluster Administrator console. Then reinstall ERA on all cluster nodes and bring cluster ERA service group online again.

2.2.3.2 Installation of ERA Console

Install the ESET Remote Administrator Console to the administrator's PC/notebook, or directly on the server.

At the end of the Advanced installation mode enter the name of the ERA Server (or its IP address) to which ERAC will automatically connect at startup. It is labeled GHOST in our example.



ESET Remote Administrator Console Setup

Connection and shortcut settings

Set ERA server name and communication ports

Connection server: localhost

Connection port: 2223

Add shortcut to desktop ☑

After installation launch ERAC and check the connection to ERAS. By default, no password is required to connect to an ERA Server (the password text field is blank), but we strongly recommend that one be established. To create a password to connect to an ERA Server click **File** > **Change Password...** and then modify the Password for Console by clicking the **Change...** button.

NOTE: The administrator can specify a user account and a password with access to the ESET Remote Administrator Console. The administrator can also specify the level of access. For more information, see the chapter User Manager 108. The ERAC needs to be installed on the computer, from which you want to access the ERAS with the account defined in the User Manager.

2.2.3.3 Mirror

You can use the ERA Console to activate the LAN Update server – the Mirror in the ERA Server. This server can then be used to update workstations located in the LAN. By activating the Mirror you will decrease the volume of data transferred through your Internet connection.

Proceed as follows:

1) Connect the ERA Console to the ERA Server by clicking **File** > **Connect**.

2) From the ERA Console click **Tools** > **Server Options**... and click the **Updates** tab.

3) From the **Update** server drop-down menu, select **Choose Automatically**, leave Update interval at 60 minutes. Insert Update username (EAV-***) and then click **Set Password**... and type or paste the password you received with your username.

4) Select the **Create update mirror** option. Leave the default path for mirrored files and HTTP server port (2221). Leave Authentication at NONE.

5) Click the **Advanced** tab and click **Edit Advanced Settings...**. In the advanced setup tree, navigate to ERA Server > **Setup** > **Mirror** > **Create mirror for the selected program components**. Click **Edit** on the right-hand side and select the program components to be downloaded. Components for all language versions that will be used in the network should be selected.

6) In the **Updates** tab, click Update now to create the **Mirror**.

For more detailed Mirror configuration options please see How to enable and configure the Mirror 118.

2.2.3.4 Database types supported by ERA Server

By default, the program uses the Microsoft Access (Jet Database) engine. ERAS 5 also supports the following databases:

- Microsoft SQL Server 2005 and later
- MySQL 5.0 and later
- Oracle 9i and later

The database type can be selected during Advanced installation of ERAS. After installation it is not possible to change the database type directly from ERA, however you can do so using the ERA Maintenance Tool 148.

NOTE:

- Microsoft Access database is not supported on Windows Server Core 2008 and Windows Server Core 2012.
- SQL Server Express has a 4 GB database size limit.
- Microsoft Access database has 2 GB database size limit.
- When using MySQL on Microsoft Windows 2000, we recommend that you use ODBC Driver 5.1.8 or later to establish a database connection 18.
- In case of MySQL ERAS uses MyISAM DB engine by default. If someone prefers InnoDB to MyISAM, he can change the database creation script during the Advanced Installation of ERAS.

2.2.3.4.1 Basic requirements

First, it is necessary to create the database on a database server. The ERAS installer is capable of creating an empty MySQL database, which is automatically named ESETRADB.

By default, the installer automatically creates a new database. To create the database manually, select **Export Script**. Make sure that the **Create tables in the new database automatically** option is deselected.

Collation Settings

Sorting will be realized according to the default settings of each database. It is required to activate CASE INSENSIVITY (CI).

To activate:

- For MS SQL and MySQL a COLLATE must be set up with the CI activated
- For ORACLE a NLS_SORT must be set up with the CI activated
- For MS Access no action is required because CI is already activated

Character set

It is important to use the UNICODE character set (UTF-8 is recommended), especially when clients have specific locales or if ERA itself is working in a localized version. If there is no plan for replication and all clients connect to the same server, you can use the character set for the locale of ERA that you want to install.

Authentication

We recommend that you use default database authentication. When using Windows/domain authentication, verify whether your account has enough rights to connect to a database. When using Microsoft SQL Server, use the DSN connection 18 string format.

MARS (Multiple Active Result Sets)

If a MS SQL database is used, an ODBC driver with MARS support is required for smooth operation. Otherwise the server will operate less effectively and log the following error message to the server log:

Database connection problem. It is strongly recommended to use odbc driver that supports multiple active result sets (MARS). The server will continue to run but the database communication may be slower. See the documentation or contact ESET support for more information.

If the problem occurs with other than a MS SQL database the server logs the following message to the server log and stops:

Database connection problem. Updating the odbc driver may help. You can also contact ESET support for more information.

Drivers without MARS support:

- SQLSRV32.DLL (2000.85.1117.00)
- SQLSRV32.DLL (6.0.6001.18000) - natively contained in Windows Vista and Windows Server 2008

Native driver with MARS support:

- SQLNCLI.DLL (2005.90.1399.00)

2.2.3.4.2 Database connection setup

After a new database is created, you must specify connection parameters for the database server using one of two options:

1. Using DSN (data source name)
   To open DSN manually, open the OBCD
   Date Source Administrator
   (Click **Start > Run** – and enter *odbcad32.exe*).

   Example of a DSN connection:
   DSN =ERASqlServer

   Important: The use of the *System DSN* is recommended for ERA to work properly.

   Important: On a 64-bit operating system, *odbcad32.exe* must be run from the *%SystemRoot%**SysWOW64*\ folder.

To make sure that the installation under MSSQL with Windows/Domain authentication is successful, make sure you use DSN format when entering the connection string.

2. Directly, using a complete connection string
   All required parameters must be specified – driver, server and name of database.

   This is an example of a complete connection string for MS SQL Server:
   Driver ={SQL Server}; Server =hostname; Database =ESETRADB

   This is an example of a complete connection string for Oracle Server:
   Driver ={Oracle in instantclient10_1}; dbq =hostname: 1521/ESETRADB

   This is an example of a complete connection string for MySQL Server:
   Driver ={MySQL ODBC 3.51 Driver}; Server =hostname; Database =ESETRADB

   Click **Set** and specify the **Username** and **Password** for your connection. Oracle and MS SQL Server database connections also require a **Schema Name**.

   Click **Test Connection** to verify the connection to the database server.

NOTE: We recommend using the database server authentication instead of windows/domain authentication.

2.2.3.5 Installation over previous versions

ESET Remote Administrator 5.3 supports installation over previous versions, including data migration. You do not need to perform migration from ESET Remote Administrator version 5.0. Migration of ESET Remote Administrator 4.x data is possible, but no longer supported.

NOTE: We recommend that you only reinstall when no clients are connected because the ERA Server Service is stopped and all connections are terminated during the reinstallation process. Database migration can be performed before or after reinstallation (see the chapter Database Transfer 149 for more information).

Installation of ERA Server

1. Download the installation file to your server. Double-click the installer file to begin installation.

2. Select **Typical** or **Advanced** installation, similar to a clean installation of ERA Server 14.

- **Typical installation** - You will be prompted for your license key file (*.lic), passwords and update data. There are two migration modes: **Import only configuration mode** creates empty tables in a new database; **Full import mode** imports all data from the database. Selecting **Create backup of current database** (default) will create a backup before making any changes to the database. **Activate default automatic clean up for old records** can be selected to improve database maintenance.

- **Advanced installation** - You will be prompted for your license key file (*.lic), the account used to run the ERA Server service, ports used for communication, passwords and update data, SMTP Server settings (optional), logging 110 settings and database migration settings (described under **Typical installation** above). During advanced installation, you will be asked if you want to migrate older policies (Windows desktop v3 and v4) to new (Windows desktop v5) policies. The migration is performed using default settings, so if you want to configure the migration, we recommend using the Policy Migration Wizard 87 after your upgrade is complete.

NOTE: If the installer finds any existing tables in the current database, a prompt will be displayed. To overwrite the contents of an existing table, click **Overwrite** (***Warning:*** this will delete the contents of tables and overwrite their structure!). Click **Ignore** to leave tables untouched. Clicking **Ignore** may cause database inconsistency errors, especially when tables are damaged or incompatible with the current version.

If you want to analyze the current database manually, click **Cancel** to abort the installation of ERAS.

Installation of ERA Console

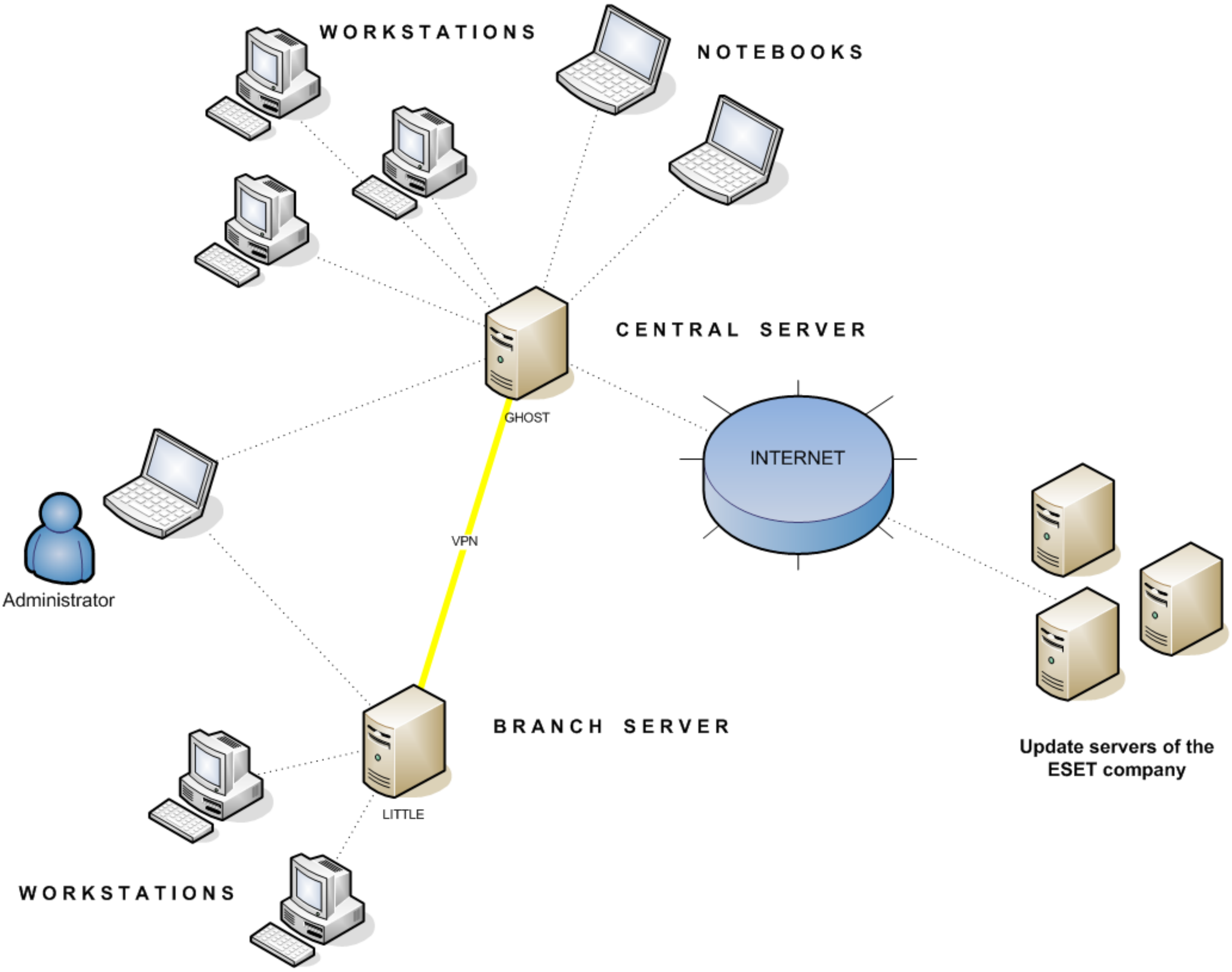
1. Download the installation file to your server. Double-click the installation file to begin installation.

2. Proceed as described in the chapter Installation of ERA Console 16.

2.3 Scenario - Installation in an Enterprise environment

2.3.1 Environment overview (network structure)

Below is a copy of the previous network structure with one additional branch office, several clients and one server named LITTLE. Let's suppose there is a slow VPN channel between the headquarters and the branch office. In this scenario, the Mirror server should be installed on the server LITTLE. We will also install a second ERA Server on LITTLE in order to create a more user-friendly environment and minimize the volume of transferred data.

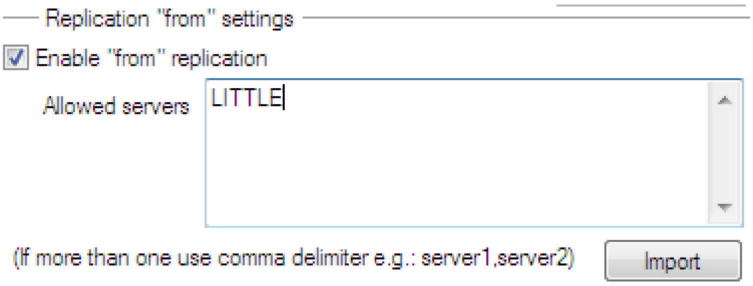


2.3.2 Installation

2.3.2.1 Installation at headquarters

Installations of ERAS, ERAC and client workstations are very similar to the previous scenario. The only difference is in the configuration of the master ERAS (GHOST). In **Tools** > **Server Options...** > **Replication** select the **Enable "from" replication** check box and enter the name of the secondary server in **Allowed servers**. In our case, the lower server is named LITTLE.

If there is a password for replication set on the upper server (**Tools** > **Server Options...** > **Security** > **Password for replication**), then that password must be used for authentication from the lower server.



Replication "from" settings

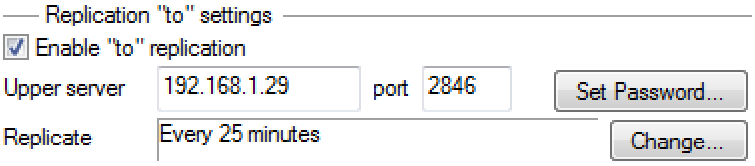
☑ Enable "from" replication

Allowed servers: LITTLE

(If more than one use comma delimiter e.g.: server1,server2)

2.3.2.2 Branch office: Installation of ERA Server

As in the example directly above, install the second ERAS and ERAC. Again, enable and configure the replication settings. This time select the **Enable "to" replication** check box (**Tools** > **Server Options...** > **Replication**) and define the name of the master ERAS. We recommend using the IP address of the master server, which is the IP address of the server GHOST.



Replication "to" settings

☑ Enable "to" replication

Upper server: 192.168.1.29 port: 2846

Replicate: Every 25 minutes

2.3.2.3 Branch office: Installation of HTTP Mirror server

The Mirror server installation configuration in the previous scenario can also be used in this case. The only changes are in the sections defining the username and password.

As in the figure from Environment overview 20 chapter, updates for the branch office are not downloaded from ESET's update servers, but from the server at the headquarters (GHOST). The update source is defined by the following URL address:

http://ghost:2221 (or http://IP_address_of_ghost:2221)

By default, there is no need to specify a username or password, because the integrated HTTP server requires no authentication.

For more information on configuring the Mirror in ERAS, see the chapter titled Mirror Server 116.

2.3.2.4 Branch office: Remote installation to clients

Once more, the previous model can be used, except that it is suitable to perform all operations with the ERAC connected directly to the ERAS of the branch office (in our example: LITTLE). This is done to prevent installation packages from being transferred via the VPN channel, which is slower.

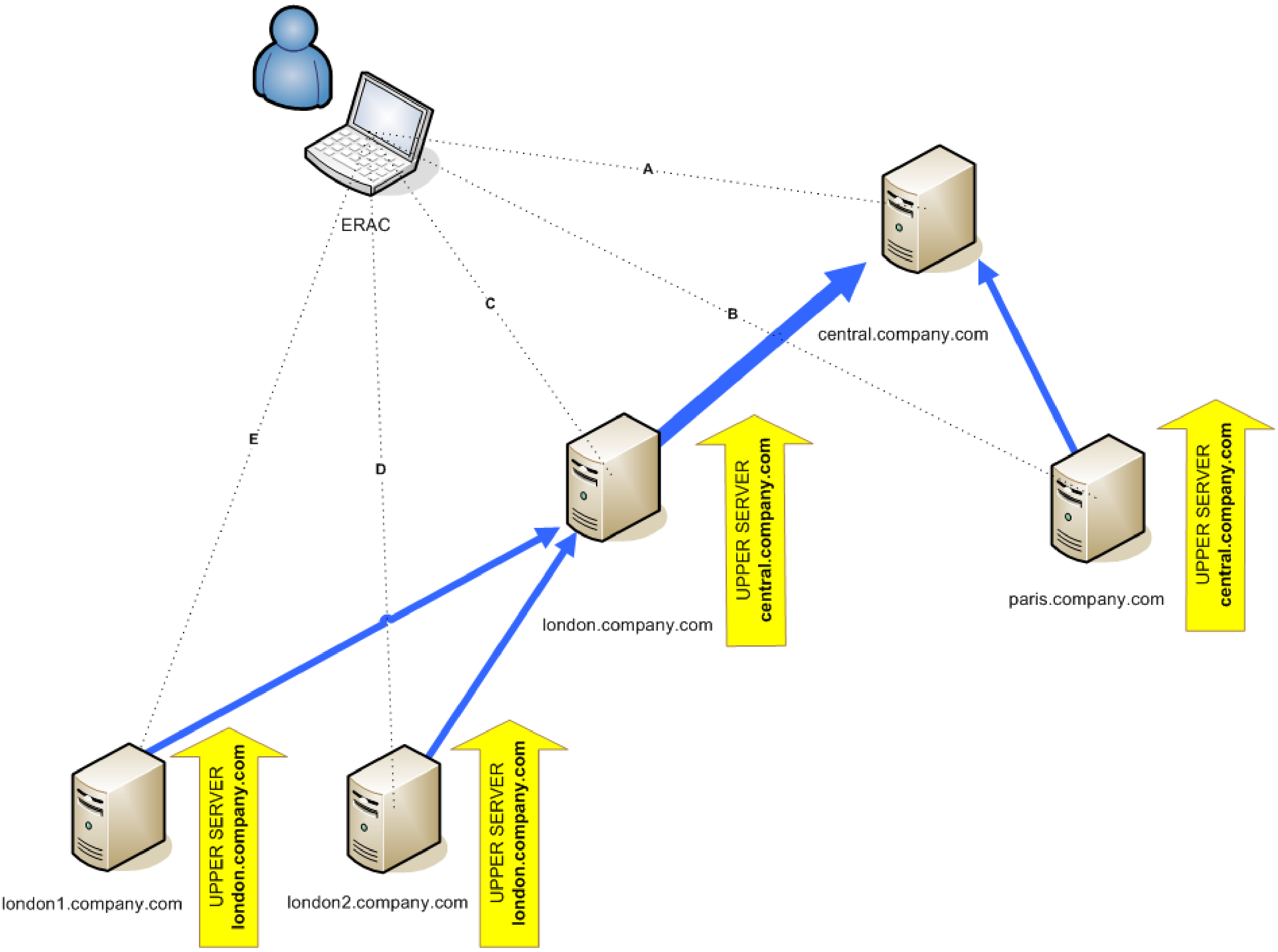
2.3.3 Other requirements for Enterprise environments

In larger networks, multiple ERA Servers can be installed to perform remote installs of client computers from servers which are more accessible. For this purpose, ERAS offers *replication* (see chapter Installation at headquarters 21 and Branch office: Installation of ERA Server 21), which allows stored information to be forwarded to a parent ERAS (*upper server*). Replication can be configured using ERAC.

The replication feature is very useful for companies with multiple branches or remote offices. The model deployment scenario would be as follows: Install ERAS in each office and have each replicate to a central ERAS. The advantage of this configuration is especially apparent in private networks which are connected via VPN, which is usually slower – the administrator will only need to connect to a central ERAS (the communication marked by the letter A in the figure below). There is no need to use VPN to access individual departments (the communications B, C, D and E). The slower communication channel is bypassed through the use of ERAS replication.

The replication setup allows an administrator to define which information will be transferred to upper servers automatically at a preset interval, and which information will be sent upon request from the upper server administrator. Replication makes ERA more user-friendly and also minimizes network traffic.

Another advantage of replication is that multiple users can log in with various permission levels. The administrator accessing the ERAS london2.company.com with the console (communication D) can only control clients connecting to london2.company.com. The administrator accessing the central company.com (A) can control all clients located at company headquarters and departments/branches.



3. Working with ERA Console

3.1 Connecting to ERA Server

Most features in ERAC are only available after connecting to ERAS. Define the server by name or IP address before connecting:

Open the ERAC and click **File** > **Edit Connections...** (or **Tools** > **Console Options...**) and click the **Connection** tab.

Click the **Add/Remove...** button to add new ERA Servers or to modify currently listed servers. Pick the desired server in the **Select connection** drop-down menu. Then, click the **Connect** button.

NOTE: ERAC fully supports the IPv6 protocol. The address should be in the *[ipv6address]:port* format, for example *[::1]:2223*.

Other options in this window:

- **Connect to selected server on the console startup** - If this option is selected, the console will automatically connect to the selected ERAS on startup.
- **Show message when connection fails** - If there is a communication error between ERAC and ERAS, an alert will be displayed.

There are two authentication types available:

ERA Server

The user authenticates with ERAS credentials. By default no password is required to connect to ERAS, but we strongly recommend that one be established. To create a password to connect to ERAS:

Click **File** > **Change Password...** (or **Tools** > **Server Options** > **Security**) and then click the **Change...** button next to **Password for Console**.

When entering a password you can check the **Remember password** option. Please consider the possible security risks associated with this option. To delete all remembered passwords click **File** > **Clear Cached Passwords...**.

If you wish to set or change the user accounts for the Console-Server authentication, use the User Manager 108 tool.

Windows/Domain

Users authenticate with Windows/Domain user credentials. In order for the Windows/Domain authentication to work properly ERAS needs to be installed under the Windows/Domain account with sufficient rights. You must also enable this feature in **Tools** > **Server Options...** > **Advanced** tab > **Edit Advanced Settings...** > **ESET Remote Administrator** > **ERA Server** > **Setup** > **Security**:

Allow Windows/Domain authentication - Enables/disables Windows/Domain authentication.

Administrator groups – Allows you to define groups for which Windows/Domain authentication will be enabled.

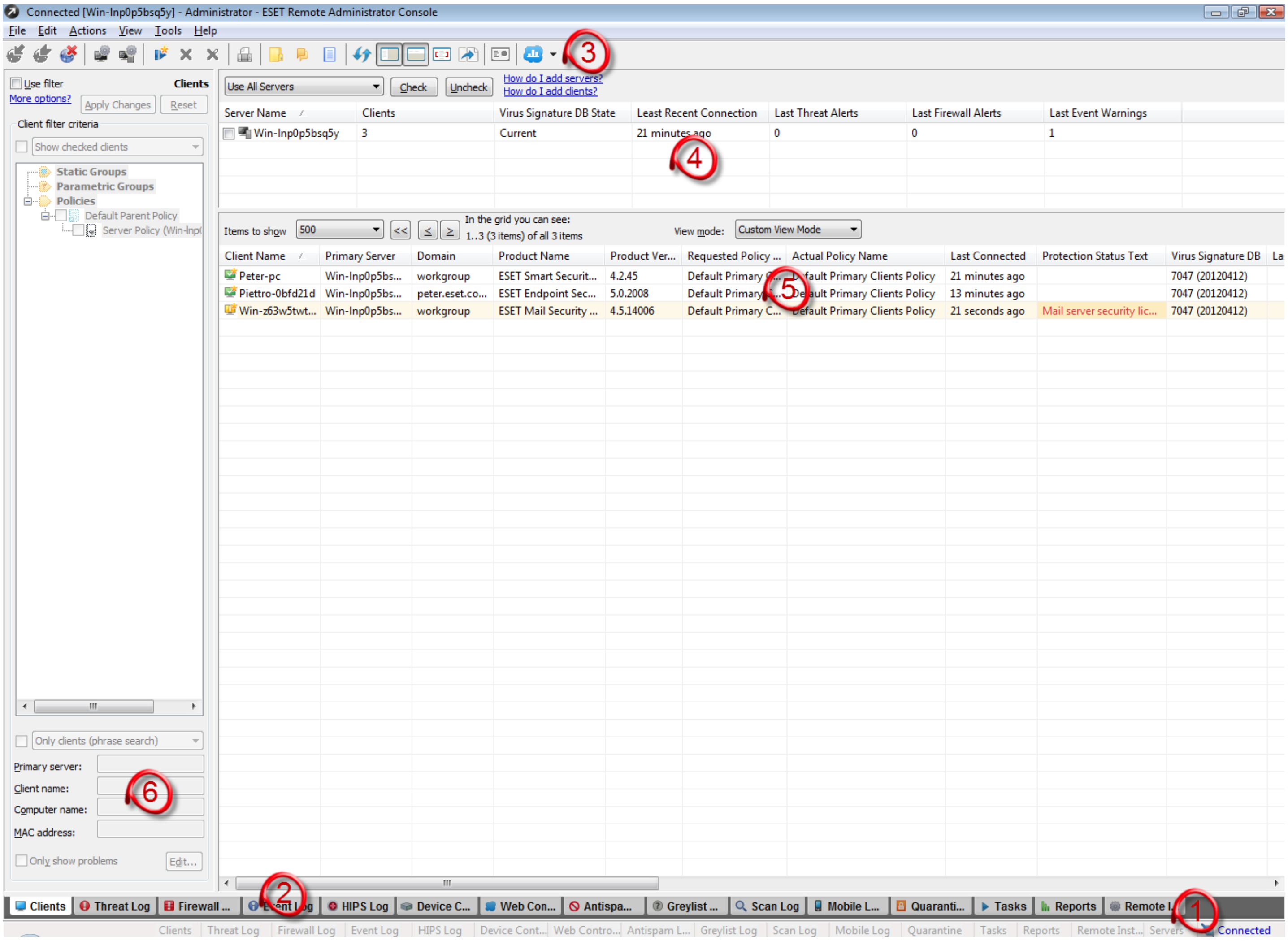
Read only groups – Allows you to define groups with read-only access.

When communication has been established the program's header will change to **Connected [server_name]**.

Alternatively you can click **File** > **Connect** to connect to ERAS.

NOTE: Communication between ERAC and ERAS is encrypted (AES-256).

3.2 ERA Console - main window



Server Name	Clients	Virus Signature DB State	Least Recent Connection	Last Threat Alerts	Last Firewall Alerts	Last Event Warnings
Win-Inp0p5bsq5y	3	Current	21 minutes ago	0	0	1

In the grid you can see:
1..3 (3 items) of all 3 items

Client Name	Primary Server	Domain	Product Name	Product Ver...	Requested Policy ...	Actual Policy Name	Last Connected	Protection Status Text	Virus Signature DB	La
Peter-pc	Win-Inp0p5bs...	workgroup	ESET Smart Securit...	4.2.45	Default Primary C...	Default Primary Clients Policy	21 minutes ago		7047 (20120412)	
Piettro-0bfd21d	Win-Inp0p5bs...	peter.eset.co...	ESET Endpoint Sec...	5.0.2008	Default Primary C...	Default Primary Clients Policy	13 minutes ago		7047 (20120412)	
Win-z63w5twt...	Win-Inp0p5bs...	workgroup	ESET Mail Security ...	4.5.14006	Default Primary C...	Default Primary Clients Policy	21 seconds ago	Mail server security lic...	7047 (20120412)	

The current communication status between ERAC and ERAS is displayed in the status bar (**1**). All necessary data from ERAS is refreshed regularly (Default is every minute. See **Tools** > **Console Options** > **Other Settings** > **Use automatic refresh (min)**. The refresh progress can also be seen in the status bar.

NOTE: Press F5 to refresh displayed data.

Information is divided into several tabs 28 in order of importance (**2**). Most of the information on tabs is related to the connected clients. In most cases data can be sorted in ascending or in descending order by clicking on an attribute (**5**), while a drag-and-drop operation can be used for reorganization. If multiple data rows are to be processed, you can limit them by using the **Items to show** drop-down menu and the **browse page by page** buttons. Select the **View mode** to display attributes according to your need (for further details, see chapter Information filtering 25. If you need to print certain information from the tabs, see the chapter Page Setup 25 for more information.

The Server section (**4**) is important if you replicate ERA Servers. This section displays summary information about the Console to which ERAS is connected, as well as information about child or "lower" ERA Servers. The Servers drop-down menu in section **4** will influence the scope of information displayed in section **5**.

- **Use All Servers -** Displays information from all ERA Servers – section (**5**).
- **Use Only Selected Servers -** Displays information from selected ERA Servers – section (**5**).
- **Exclude Selected Servers -** Excludes information from selected ERA Servers.

Columns in Section **4**:

- **Server Name -** Displays name of server.

- **Clients -** Total number of clients connecting to or in the database of the selected ERAS.
- **Virus Signature DB Range -** Version of virus signature databases among the clients of the selected ERAS.
- **Least Recent Connection -** Time elapsed since the least recent connection to the server.
- **Last Threat Alerts -** Total number of virus alerts (see the attribute **Last Threat Alert** in section **5**).
- **Last Firewall Alerts -** The total number of firewall alerts.
- **Last Event Warnings -** Total number of current events (see the attribute **Last Event** in section **5**).

If you are not currently connected, you can right-click in the Server section (**4**) and select **Connect to This Server** to connect to the chosen ERAS. More information will be displayed in the Server section (**4**) if replication is enabled.

The most important features of ERAC are accessible from the main menu or from the ERAC toolbar (**3**).

The last section is **Computer filter criteria** (**6**) – see the chapter titled Information filtering 25.

NOTE: We strongly recommend using the Context menu 27 to administer clients and filter information. It is a quick way to run tasks, manage groups and policies, filter data and more.

3.2.1 Page Setup

In the **Page Setup** window, you can set parameters for printing the content of tabs in the ERA Console:

WYSIWYG – Prints tabs exactly as you see them (What You See Is What You Get).

Print – Prints tabs in grayscale. Only black and white colors are used.

Print icon – Prints also icons displayed next to client names.

Print header – Inserts the string defined in **Header** in the upper left corner. Use the default header, or write your own header into the **Header** field.

Print Logo – Inserts the string defined in **Logo path** in the upper right corner. The ESET logo is printed by default. You can upload your own logo by clicking the **"..."** button next to this option and choosing the logo from your harddrive.

Number pages – Inserts page number at the bottom section of the printed page.

Preview – Click to display a print page preview.

3.3 Information filtering

ERAC offers several tools and features for the easy administration of clients and events. Having an advanced filtering system can often be priceless, especially on systems with a large number of clients, when the displayed information needs to be grouped and easily manageable. There are several tools in ERAC that allow you to efficiently sort and filter information about the connected clients.

Filter 26 allows the administrator to display only information related to specific servers or client workstations. To show the filter options, click **View** > **Show/Hide Filter Pane** from the ERAC menu.

View mode

The number of columns displayed in the **Clients** tab can be adjusted by using the **View mode** drop-down menu on the right side of the Console. The **Full View Mode** displays all columns, while the **Minimal View Mode** shows only the most important columns. These modes are predefined and cannot be modified. To customize your view, select any of the available **Custom View Modes**. They can be configured under **Tools** > **Console Options...** > **Columns - Show/Hide** tab.

Note: You can change the order of columns (drag & drop) and their size in every view mode.

3.3.1 Filter

To activate filtering, select **Use filter** in the upper left side of the ERAC. Any future modifications to the filter criteria will automatically update displayed data, unless configured otherwise in **Tools** > **Console Options...** > **Other Settings**.

Define the filtering criteria in the **Client filter criteria** section. Clients can belong to multiple groups and policies. Assigning a client to a static or parametric group can prove very useful, not only for filtering purposes, but also for activities such as reporting. To learn more about group management see the chapter titled Group Manager 82. Using policies for client segregation can also serve multiple functions. For more information about policy creation and management see the chapter Policies 84.

The first filtering tool is the group and policy selecting section. There are three options available:

- **Show checked clients** – Clients in selected groups/policies will be displayed in the **Clients** panel.
- **Hide checked clients** – Clients in groups/policies that are not selected and clients in no groups will be displayed in the **Clients** panel. If a client is a member of multiple groups and one of the groups is checked, the client will not be displayed.
- **Hide checked clients, ignore multi-membership** – Clients in groups/policies that are not selected and clients in no groups will be displayed. If a client is a member of more groups and on of the groups is checked, the client will be displayed.
- **Show clients in no groups** – Only clients that do not belong to any group/policy will be displayed.

NOTE: When checking a group from the list, all its subgroups will be checked as well.

In the lower part of the **Filter** section you can specify another set of parameters:

- **Only clients (using whole words)** – Output only includes clients with names identical to the string entered.
- **Only clients beginning like (?,*)** – Output will only list clients with names beginning with the specified string.
- **Only clients like (?,*)** – Output will list only clients with names containing the specified string.
- **Exclude clients (using whole words), Exclude clients beginning like (?,*), Exclude clients like (?,*)** – These options will yield results opposite to the previous three.

The **Primary server**, **Client name**, **Computer name** and **MAC Address** fields accept strings based on the criteria defined in the drop-down menu above. If any of these are populated, a database query will be run and results will be filtered based on the populated field (the logical operator AND can be used). You can either use whole strings, or wildcards (?,*).

The last option is problem based filtering – outputs will only include clients with the specified problem type. To display a selection of problems, select **Only show problems** and click **Edit...** Select the problems you wish to be displayed and click **OK** to show a list of clients with the selected problems.

All changes made to the filtering configuration will be applied after clicking **Apply Changes**. To restore defaults, click **Reset**. To automatically generate new outputs after each modification of the filtering settings, click **Tools** > **Console Options...** > **Other Settings...** and select **Auto apply changes**.

NOTE: The filter criteria in the last section may vary depending on the currently active tab. The criteria are customized to effectively sort the logs. For example, you can sort the logs by the level of verbosity in the firewall log to display only the type of logs you need to review.

You can also sort the data in the tabs by selecting the time interval for which you want the items to be displayed. For more information on how to use the **Date filter**, see the Date Filter 27 chapter.

3.3.2 Context menu

Use the right mouse button to invoke the context menu and adjust output in columns. Context menu options include:

- **Select All** – Selects all entries.
- **Select by '...'** – This option allows you to right-click on any attribute and automatically select (highlight) all other workstations or servers with the same attribute. The string ... is automatically replaced by the value of the current tab.
- **Inverse Selection** – Performs inverted selection of entries.
- **Hide Selected** – Hides selected entries.
- **Hide Unselected** – Hides all unselected entries in the list.

NOTE: The options may vary depending on the currently active window.

- **Show/Hide Columns** – Opens the **Console Options** > Columns - Show/Hide 56 window where you can define columns that will be available in the selected pane.

The **Hide Selected/Unselected** options are effective if further organization is needed after using previous filtering methods. To disable all filters set by the context menu, click **View** > **Cropped View**, or click the icon on the ERAC toolbar. You can also press **F5** to refresh displayed information and disable filters.

Example:

- To only display clients with threat alerts:
  In the **Clients** tab, right-click on any empty pane with Last Virus Alert and choose **Select by '...'** from the context menu. Then, again from the context menu, click **Hide Selected**.
- To display threat alerts for clients ”Joseph” and ”Charles”:
  Click the **Threat Log** tab and right-click any attribute in the Client Name column with the value Joseph. From the context menu click **Select by 'Joseph'**. Then, press and hold the CTRL key, right-click and click **Select by 'Charles'**. Finally, right-click and select **Hide Unselected** from the context menu and release the CTRL key.

The CTRL key can be used to select/deselect specific entries and the SHIFT key can be used to mark/unmark a group of entries.

NOTE: Filtering can also be used to facilitate the creation of new tasks for specific (highlighted) clients. There are many ways to use filtering effectively, please experiment with various combinations.

3.3.3 Date Filter

The **Date Filter** is located in the lower right corner of every tab in ERAC. By specifying the **DateTime Interval**, you can easily sort data from a selected time period.

Last X Hours/Days/Weeks/Months/Years – Select the specified number and time. This will limit the items in the current tab and only the items from this time interval will be displayed. For example, if you select *Last 10 Days*, all items from the last 10 days will be displayed.

Last X – From the drop-down menu, select the predefined time interval for which you want the items to be shown.

All before (inclusive) / All after (inclusive) – Select the check box next to **All before (inclusive)** or **All after (inclusive)** and specify a time and date. All items before / after this time and date will be displayed.

All in interval – Select a time and date from-to. Items from this time interval will be shown.

NOTE: You can use a **Date filter** in every log to specify the time interval for which you want the data to be shown in the tab. You also have the option set the level of verbosity in the tabs (where applicable) to sort the data by relevance. The **Date filter** will display data that is already filtered through the **Items to show** filter - these filters are dependent. This means that it will apply the filter only on already filtered data.

3.4 Tabs in ERA Console

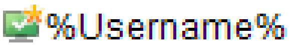
3.4.1 General description of tabs and clients

Most of the information in tabs is related to the connected clients. Each client connected to ERAS is identified by the following attributes:

Computer Name (client name) + MAC Address + Primary Server

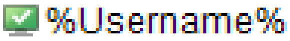
The behavior of ERAS in relation to certain network operations (such as renaming a PC) can be defined in ERAS Advanced Setup. This can help prevent duplicate entries in the **Clients** tab. For example, if one of the computers in the network has been renamed, but its MAC address remains unchanged, a new entry will not be created in the **Clients** tab.

Clients that connect to ERAS for the first time are designated by a **Yes** value in the **New Client** column. They are also marked by a small asterisk in the upper right corner of the client's icon (see the figure below). This feature allows an administrator to easily detect a newly connected computer. This attribute can have different meanings depending on the administrator's operating procedures.



%Username%

If a client has been configured and moved to a certain group, the New status can be disabled by right-clicking the client and selecting **Set/Reset Flags** > **Reset "New" Flag**. The client's icon will change to the one shown in the figure below and the value in the **New Client** column will switch to **No**.



%Username%

NOTE: The Comment attribute is optional in all three tabs. The administrator may insert any description here (e.g., *"Office No. 129"*).

Time values in ERAS can be displayed either in the relative mode (*"2 days ago"*), in absolute mode (20.5.2009) or in system mode (Regional settings).

In most cases data can be sorted in ascending or in descending order by clicking an attribute, while a drag-and-drop operation can be used for reorganization.

Use the **Items to show** option to sort data you want to display in a tab. Set the number of logs you want to display (default is 200 for all logs) and the time period from which you want the logs to be displayed (from last 7 days, by default). Setting the time period to **Do not limit time** is not recommended in larger networks, as this may cause a severe load on the database - and possibly decreasing the performance.

NOTE: You can use a **Date filter** in every log to specify the time interval from which you want the data to be shown in the tab. You also have the option to set the level of verbosity in the tabs (where applicable) to sort the data by relevance. The **Date filter** will display data that is already filtered through the **Items to show** filter - these filters are dependent.

Double-clicking certain values activates other tabs and displays more detailed information. For example, if you double-click a value in the **Last Threat Alert** column, the program will move to the **Threat Log** tab and display Threat Log entries related to the given client. If you double-click a value which contains too much information to be displayed in a tabbed view, a dialog window will open showing detailed information about the corresponding client.

3.4.2 Replication & information in individual tabs

If ERAC is connected to an ERAS which is operating as an upper server, clients from the lower servers will be displayed automatically. The types of replicated information can be configured on the lower server in **Tools** > **Server Options** > **Replication** > **Replicate "to" settings**.

In this scenario, the following information may be missing:

- Detailed alert logs (**Threat Log** tab)
- Detailed On-demand scanner logs (**Scan Log** tab)
- Detailed current client configurations in the.xml format (the **Clients** tab, the **Configuration** column, **Protection Status**, **Protection Features**, **System Information**)

Information from the ESET SysInspector program may also be missing. ESET SysInspector is integrated with generation 4.x ESET products and later.

If the information cannot be found in the dialog windows of the program, click the **Request** button (available under **Actions** > **Properties** > **Configuration**). Clicking this button will download missing information from a lower ERAS. Since replication is always initiated by a lower ERAS, the missing information will be delivered within the preset replication interval.

On the upper server you can set the level of logs that will be received by the server (**Tools** > **Server Options** > **Advanced** > **Edit Advanced Settings...** > **ESET Remote Administrator** > **ERA Server** > **Setup** > **Server Maintenance** > **.... logs to accept**).

NOTE: This option applies to all clients connected to the server (not only the replicated ones).

3.4.3 Clients tab

This tab displays general information about individual clients, the information displayed is based on the View mode 25 set in ESET Remote Administrator.

Attribute	Description
Client Name	Name of Client (Can be changed in the Client's properties dialog - General tab)
Computer Name	Name of workstation / server (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of ERAS with which a client is communicating
Domain	Domain / group name, to which a client belongs (these are not groups created in ERAS)
IP	IPv4 or IPv6 address
Product Name	Name of ESET product
Product Version	Version of ESET product
Requested Policy Name	Name of policy requested for a client by a user or server. Requested policy will sync with actual policy after a client connects to ERAS and if there are no policy rules which disallow to assign requested policy.
Actual Policy Name	Name of policy successfully assigned to a client after connecting to ERAS.
Last Connected	Time that client last connected to ERAS (All other data collected from clients includes this timestamp, except for some data obtained by replication)
Protection Status Text	Current status of the ESET security product installed on a client
Virus Signature DB	Version of virus signature database
Last Threat Alert	Last virus incident
Last Firewall Alert	Last event detected by the ESET Endpoint Security Personal firewall (Events from the Warning level and higher are shown)
Last Event Warning	Last error message
Last Files Scanned	Number of files scanned during the last On-demand scan
Last Files Infected	Number of infected files found during the last On-demand scan
Last Files Cleaned	Number of files cleaned (or deleted) during the last On-demand scan
Last Scan Date	Date of last On-demand scan

Restart Request	Is a restart required (for example, after a program upgrade)
Restart Request Date	Time of first restart request
Product Last Started	Time that client program was last launched
Product Install Date	Date that the ESET security product was installed on the client
Roaming User	Clients with this attribute will perform the "update now" task each time they establish a connection with the ERAS (recommended for notebooks). The update is only performed if the client's virus signature database is not up to date. This feature is useful for users that have not been connected to ERAS for a long time, and this task triggers the update immediately (even before the regular update task).
New Client	Newly connected computer (see General description of tabs and clients 28)
OS Name	Name of client operating system
OS Platform	Operating system platform (Windows / Linux...)
HW Platform	32-bit / 64-bit
Configuration	Client's current.xml configuration (including date/time that the configuration was created)
Protection Status	General status statement (Similar in nature to the Configuration attribute)
Protection Features	General status statement for program components (Similar to Configuration attribute)
System Information	Client submit system information to ERAS (including the time that the system information was submitted)
SysInspector	Clients with the ESET SysInspector tool installed can submit logs from this application.
Custom Info 1, 2, 3	Custom Information to be displayed specified by the administrator (this option can be configured in ERAC through **Tools > Server Options... > Advanced tab > Edit Advanced Settings...** > ESET Remote Administrator > ERA Server > Setup > Other settings > Client custom info 1, 2, 3).
Comment	A short comment describing the client (entered by the administrator)

NOTE: Some of these values are intended for informational purposes only, and may not be current at the time the administrator views them in the console. For example, information about an update error that occurred at 7 a.m. does not necessarily mean the update was not completed successfully at 8 a.m. **Last Threat Alert** and **Last Event Warning** may be counted among such values. If the administrator knows that given information is obsolete, it can be cleared by right-clicking and selecting **Clear Info** > **Clear "Last Threat Alert" Info** or **Clear "Last Event Warning" Info**. Information about the last virus incident or the last system event will be deleted.

Double-clicking a client will display additional options in the **Client** tab:

- **General** – Contains similar information to that displayed in the Clients tab. You can use it to change the Client Name – the name under which a client is visible in ERA and add an optional comment.
- **Member Of Groups** – This tab lists all groups to which the client belongs. For more information, see Information filtering 25.
- **Tasks** – displays tasks related to the given client. For more information see Tasks 77.
- **Configuration** – This tab allows you to view or export the current client configuration to an.xml file. Later in this manual, we will explain how *.xml* files can be used to create a configuration template for *new/modified.xml* configuration files. For more information see Tasks 77.
- **Protection Status** – This is a general status overview of all ESET programs. Some of the statements are interactive and allow immediate intervention. This functionality is useful because it eliminates the need to manually define a new task for solving given protection issues.
- **Protection Features** – Component status for all ESET security features (Antispam, Personal firewall, etc.)
- **System Information** – Detailed information about the installed program, its program component version, etc.
- **SysInspector** – Detailed information about the startup processes and processes running in the background.
- **Quarantine** – Contains a list of quarantined files. Quarantined files can be requested from a client and saved to a local disk.

To execute network actions for specific client(s), right-click a client (or clients) and select **Network Action** 31 from the context menu.

If you happen to have duplicate clients in this tab, you can merge 31 them.

3.4.3.1 Merge duplicate clients

Imagine that in a computer managed by ERA Server you change the network adapter, thus the MAC address of the computer changes. You connect the computer to ERA Server, but now the freshly connected computer is a duplicate of the old (previously connected) computer. In this scenario, you can delete the old computer from the **Clients** tab of ERA Console or merge the two computers to keep the logs from the old computer and have them associated with the new computer.

To merge two computers, navigate to the **Clients** tab of ERA Console, select the two computers, right-click the selection and click **Merge Duplicates...** in the context menu. In the **Merge duplicate clients** window you can choose which client should be kept and click **Merge clients**. If you happened to chose the worse client to be kept (for example, the one that hadn't connected to the ERA Server for a long period), you would see a warning about the wrong selection.

NOTE: When merging two computers, the logs are associated with the kept computer but the Tasks, Quarantine and group/policy assignment of the deleted computer are deleted.

3.4.3.2 Network Actions

You can execute different network actions on clients managed by ERA Server. If you right-click a client in the **Clients** tab of ERA Console and select **Network Actions**, you are presented with several options: **Ping**, **Wake On LAN**, **Share**, **Shutdown/Restart**, **Message**, **RDP** or **Custom...** . These network actions correspond to Windows network actions and have the same functionality.
Every network action you run (except the Ping) will inform you about the state of the action via a progress bar in the dialog window. The table below lists the available network actions, the generic windows command they execute (unless implemented another way in ERA Server) and some of the prerequisites. In many cases, not all **Prerequisites** have to be satisfied or additional prerequisites are not mentioned here. This table is contains the recommended course of action to resolve most issues.

Network Action	Command	Prerequisites
ping	-	• ICMP enabled on firewall
Wake on Lan	-	• Network card of the selected computers must support the standard Magic Packet format • Wake On Lan must be configured in BIOS of the selected computers and configured in their network card • more information in the dialog window itself
Share	*explorer.exe \\**<computer>***	• sharing enabled on the target computer • firewall exception for sharing
Shutdown/ Restart	*shutdown /s /t <timeout> /c "<reason_comment>" /f /m **<computer>*** • when restart is selected, there is /r instead of /s • if „Reason comment“ is empty, there is no /c "<reason_comment>" • if „Force applications to close“ is unchecked, there is no /f • if „abort shutdown action“ is checked, it is	• Remote Registry service enabled • Windows Management Instrumentation service enabled • Windows Management Instrumentation (WMI) firewall exception • current Windows user on the console computer must have administrator permissions on the target computer (this assumes a domain environment)

	always only *shutdown /a /m* ***<computer>***	• running it under administrator account on the local computer • Add credential: a. Look up the Credential Manager of Windows b. Click the Add a Windows Credential c. Enter the name of the target computer (or IP address), username and password on that target computer
Message	*msg.exe /SERVER:**<computer>** * "a"* But, on Windows 2000 it is: *net send **<computer>***	• registry change: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server Name: AllowRemoteRPC Type: REG_DWORD Value: 1 • run ERA under the administrator account on the local computer • Add credential: a. Look up the Credential Manager of Windows b. Click the Add a Windows Credential c. Enter the name of the target computer (or IP address), username and password on that target computer
RDP	*mstsc.exe /v **<computer>***	
custom - you can execute any custom command valid for **cmd.exe**		

The **Command** is executed on the computer where the ERA console is running (so executing the **Command** using **cmd.exe** on the console computer should behave exactly the same and can be used to determine what is wrong). The ***<computer>*** is replaced by the target computer host name or IP address based on "Use hostname instead of IP address when executing a Network Action" setting in **Tools > Console Options > Other Settings** in ERA Console.

Some commands work better in a domain environment – when logged in as a domain user (which has administrator privileges on the target computer) there is no need to **Add credential**.

3.4.4 Threat Log tab

This tab contains detailed information about individual virus or threat incidents.

Attribute	Description
Client Name	Name of client reporting the threat alert
Computer Name	Workstation/server name (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of ERAS with which a client is communicating
Date Received	Time at which the event was logged by ERAS
Date Occurred	Time at which the event occurred
Level	Alert level
Scanner	Name of security feature which detected the threat
Object	Object type
Name	Usually a folder where the infiltration is located
Threat	Name of the detected malicious code

Action	Action taken by the given security feature
User	Name of the user that was identified when the incident occurred
Information	Information about the detected threat
Details	Client log submission status

3.4.5 Firewall Log tab

This tab displays information related to client firewall activity.

Attribute	Description
Client Name	Name of client reporting the event
Computer Name	Workstation/server name (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of ERAS with which a client is communicating
Date Received	Time at which the event was logged by ERAS
Date Occurred	Time at which the event occurred
Level	Alert level
Event	Description of the event
Source	Source IP address
Target	Target IP address
Protocol	Protocol concerned
Rule	Firewall Rule concerned
Application	Application concerned
User	Name of the user that was identified when the incident occurred

3.4.6 Event Log tab

This tab shows a list of all system-related events (based on the ESET security product program components).

Attribute	Description
Client Name	Name of client reporting the event
Computer Name	Name of workstation / server (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of ERAS with which a client is communicating
Date Received	Time at which the event was logged by ERAS
Date Occurred	Time at which the event occurred
Level	Alert level
Plugin	Name of the program component reporting the event
Event	Description of the event
User	Name of the user associated with the event

3.4.7 HIPS Log tab

This tab shows all HIPS-related activity.

Attribute	Description
Hips Id	ID of the corresponding entry in the database (ID has the form: HIPS Number)
Client Name	Name of client reporting the HIPS message
Primary Server	Name of the ERA Server a client is communicating with
Date Received	Time at which the event was logged by ERAS
Date Occured	Time at which the event occurred
Level	Emergency level of the event
Application	Name of the application that generated the HIPS log. It has the format of a UNC path to the executable of the application
Operation	Detected activity that affects the target application
Target	Application file that generated the HIPS log. Its in the format of a path to the file in the application installation folder

Action	Action that was taken by HIPS based on the current active mode/rule

NOTE: By default, the logging of HIPS activity is disabled. To enable logging of this activity or change settings, go to **Tools** > **Server Options** > **Server Maintenance** > **Log Collecting Parameters** 109.

3.4.8 Device Control Log

This tab shows detailed logs of Device control activity.

Attribute	Description
Device Control Id	ID of the corresponding entry in the database
Client Name	Name of client reporting the event
Primary Server	Name of ERAS with which a client is communicating
Date Received	Time at which the event was logged by ERAS
Date Occurred	Time at which the event occurred
Level	Alert level
User	Name of the user associated with the event
Group	Group the client that reported the activity belongs to
Device class	Type of the removable device (USB storage,DVD...)
Device	Given name and serial number (if available) of the removable device
Event	Event reported by the Device control feature
Action	Action taken by the given security feature

NOTE: By default, the logging of Device Control activity is disabled. To enable logging of this activity or change settings, go to **Tools** > **Server Options** > **Server Maintenance** > **Log Collecting Parameters** 109.

3.4.9 Web Control Log

This tab shows detailed logs of Web Control activity.

Attribute	Description
Web Control Id	ID of the corresponding entry in the database
Client Name	Name of client reporting the event
Primary Server	Name of ERAS with which a client is communicating
Date Received	Time at which the event was logged by ERAS
Date Occurred	Time at which the event occurred
Level	Alert level
User	Name of the user associated with the event
Group	Group the client that reported the activity belongs to
URL	URL of the blocked webpage
URL Mask	URL mask of the blocked webpage
URL Category	URL category of the blocked webpage
Action	Action taken by the given security feature

NOTE: By default, the logging of Web Control activity is disabled. To enable logging of this activity or change settings, go to **Tools** > **Server Options** > **Server Maintenance** > **Log Collecting Parameters** 109.

3.4.10 Antispam Log tab

This tab shows all Antispam-related activity.

Attribute	Description
Antispam ID	ID of the corresponding entry in the database (ID has the form: Antispam Number)
Client Name	Name of client reporting the SpamAS message
Primary Server	Name of the ERA Server a client is communicating with
Date Received	Time the event was logged by ERAS
Date Occured	Time the event occurred
Sender	Email address of the sender of the message marked as spam
Recipients	Recipient of the message marked as spam
Subject	Subject of the message marked as spam

Score	Spam rating (the probability of the message to be a spam message) in percentage
Reason	Reason why this message was marked as spam
Action	Action taken for this message

NOTE: By default, the logging of Antispam activity is disabled. To enable logging of this activity or change settings, go to **Tools** > **Server Options** > **Server Maintenance** > **Log Collecting Parameters** 109.

3.4.11 Greylist Log tab

This tab shows all Greylisting-related activity.

Attribute	Description
Greylist Id	ID of the corresponding entry in the database (ID has the form: Greylist Number)
Client Name	Name of client reporting the event
Primary Server	Name of ERAS with which a client is communicating
Date Received	Time the event was logged by ERAS
Date Occured	Time the event occurred
HELO domain	Domain name used by the sending server to identify itself towards the receiving server
IP address	IP address of the sender of the message
Sender	E-mail address of the sender of the message
Recipient	E-mail address of the recipient of the message
Action	Action taken by the given security feature
Time remaining	Time left before the message is rejected or verified and delivered

NOTE: By default, the logging of greylisting activity is disabled. To enable logging of this activity or change settings, go to **Tools** > **Server Options** > **Server Maintenance** > **Log Collecting Parameters** 109.

3.4.12 Scan Log tab

This tab lists results of On-demand computer scans that were started remotely, locally on client computers, or as scheduled tasks.

Attribute	Description
Scan Id	ID of the corresponding entry in the database (ID is in the form: Scan Number)
Client Name	Name of client where the scan was performed
Computer Name	Name of workstation / server (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of the ERA Server a client is communicating with
Date Received	Time at which the scan event was logged by ERAS
Date Occurred	Time at which the scan took place on client
Scanned Targets	Scanned files, folders and devices
Scanned	Number of checked files
Infected	Number of infected files
Cleaned	Number of cleaned (or deleted) objects
Status	Status of the scan
User	Name of the user that was identified when the incident occurred
Type	User type
Scanner	Scanner type
Details	Client log submission status

3.4.13 Mobile Log tab

This tab displays detailed logs from the mobile phones connected to ERA Server.

Attribute	Description
Mobile Id	Network ID of the mobile device
Client Name	Name of client where action was performed
Computer Name	Name of workstation / server (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of the ERA Server a client is communicating with
Date Received	Time at which the event was logged by ERAS
Date Occurred	Time at which the event took place on client
Level	Alert level
Log Type	Type of a log (e.g. Security Audit Log, SMS Antispam Log)
Event	Description of the event
Object Type	Object to which the event is related (e.g. SMS, file, ...)
Object Name	Particular object to which the event is related (e.g. SMS sender phone number, path to file, ...)
Action	Action performed (or error encountered) during the event

3.4.14 Quarantine tab

This tab consolidates all quarantine entries in your network.

Attribute	Description
Quarantine Id	ID number of the quarantined object assigned in order of occurrence
Hash	File hash code
DateReceived	Time at which the scan event was logged by ERAS
Occurred First	Time passed from the first occurrence of the quarantined item
Occurred Last	Time passed from the latest occurrence of the quarantined item
Object Name	Usually a folder where the infiltration is located
File Name	Name of the quarantined file
Extension	Type of extension of the quarantined file
Size	Size of the quarantined file
Reason	Reason for quarantining - usually a description of the threat type
Client Count	Number of clients quarantining the object
Hits	Number of times the object was quarantined
File	Indicates whether the object was requested to be downloaded to the server

NOTE: Please note that the fields **Object Name**, **File Name** and **Extension** shows first three objects only. For detailed information open the Properties window either by pressing the **F3** key or by double-clicking the selected item.

Centralized quarantine provides an overview of quarantined files which are stored locally on the clients with an option to request them on demand. When a file is requested, it is copied to the ERA Server in a safe, encrypted form. For safety reasons, decryption is performed upon saving the file to the disk. For instructions on working with quarantined files, see chapter Restore/Delete from Quarantine Task 80.

NOTE: Centralized quarantine requires installation of EAV/ESS version 4.2 or newer on clients.

3.4.15 Tasks tab

The meaning of this tab is described in the chapter titled Tasks 77. The following attributes are available:

Attribute	Description
State	Task status (Active = being applied, Finished = task was delivered to clients)
Type	Task type
Name	Task name
Description	Task description
Date to deploy	Task execution time /date
Date Received	Time at which the event was logged by ERAS
Details	Task log submission status
Comment	A short comment describing the client (entered by the administrator)

3.4.16 Reports tab

The **Reports** tab is used to turn statistical information into graphs or charts. These can be saved and processed later in the Comma Separated Value format (*.csv*) by using ERA tools to provide graphs and graphical outputs. By default, ERA saves output in HTML format. Most of the reports related to infiltrations are generated from the Threat log.

1. Dashboard 39 **Templates** – Templates for the web dashboard reports. A dashboard is a set of reports that is available online using a web browser. The dashboard layout is fully customizable for each administrator. Double-click a template to display a preview of the report used in the dashboard.

2. **Report Templates** – Templates for static reports. At the top of the Console window in the **Report templates** section, you can see the names of templates that were already created. Next to the template names, you can find information about time/intervals and when reports are generated according to the preset templates. You can create new templates, or edit existing predefined templates (shown below):

- **Clients Overview** – Shows the protection statuses of all clients.
- **Clients with Active Threats** – Shows clients with active threats (threats that were not cleaned during the scan) along with information about the active threats.
- **Comprehensive Network Attacks Report** – Shows a comprehensive report about network attack activity.
- **Comprehensive SMS Report** – Shows a comprehensive report about SMS spam activity.
- **Comprehensive SPAM Report** – Shows a comprehensive report about email spam activity.
- **Comprehensive Threats Report** – Shows a comprehensive report about all found threats.
- **Custom Info Summary** – Shows a comprehensive report with user-defined information (needs to be defined first).
- **Top Problematic Clients** – Shows clients with the greatest number of problems (based on the reports above).

Clicking **Default Templates** will reset the predefined templates to their original state (this action will not affect custom created templates).

- **Options**

Click **Generate Now** (make sure the **Options** tab is selected) to generate a report at any moment regardless of the schedule. Select the output type from the drop-down menu next to this option. This defines the file type of the generated report (HTML, ZIP or PDF).

Report

Type – Type of report based on the predefined templates. It can be modified for predefined templates or selected for the custom created templates. Clicking on **...** (next to this option) shows reports that can be used for the **Custom Comprehensive report**.

Style – You can modify the color and layout of the report using this drop-down menu.

Filter

Target clients - You can specify if you want the report to collect **All** the data or the data from **Only Selected Clients/Servers/Groups**,or you can **Exclude Selected Clients/Servers/Groups**. The clients/servers/groups can be specified after clicking **...** next to the **Target clients** drop-down menu in the **Add**/**Remove** dialog window.

Threat – You can also specify if you want the report to show **All** threats, **Only Selected Threats** or **Exclude Selected Threats**. The threats can be specified after clicking **...** next to this drop-down menu in the **Add**/**Remove** dialog window.

Other details can be configured by clicking **Additional Settings...** . These settings apply mostly to data in the heading and in the types of graphical diagrams used. However, you can also filter data according to the status of chosen attributes as well as choose which report format will be used (.html, .csv).

- **Interval**

Current – Only events which occurred during a chosen time period will be included in the report, for example, if a report is created on Wednesday and the interval is set to **Current Week**, then the events from Sunday, Monday, Tuesday, and Wednesday will be included.

Completed – Only events which occurred during a chosen, closed period will be included in the report (for example, the entire month of August, or a whole week from Sunday to next Saturday). If **Add also the current period** is selected, the report will include events from the last completed period up to the moment of creation.

Example:

We want to create a report including events from the last calendar week, for example, from Sunday to next Saturday. We want this report to be generated on the following Wednesday (after Saturday). In the **Interval** tab, select **Completed** and **1 Week**. Remove **Add also the current period**. In the **Scheduler** tab set the **Frequency** to **Weekly** and select **Wednesday**. The other settings can be configured according to the administrator‘s discretion.

From / To – Use this setting to define a period for which the report will be generated.

- **Scheduler**

Frequency – Allows you to define and configure an automatic report for a specified time or in intervals.

After scheduling the report, click **Select Target...** to specify where the report is to be saved. Reports can be saved to ERAS (default), sent via email to a chosen address, or exported to a folder. The latter option is useful if the report is sent to a shared folder on your organization‘s intranet where it can be can be viewed by other employees. If you use this option, select the output file type (HTML, ZIP or PDF). You can use variables (%) in the path of the folder. Variables are not case sensitive. These variables add custom info to the generated report. If you end the folder path with the "\" symbol, reports are written directly into this folder and data is overwritten. The following variables are supported:

Variable	Description
%INTERVAL%	The interval for which the report is being generated, as returned from CReport::GetIntervalString(INTERVALSTRING_FOLDER).
%DATE%	Current date ("YYYY-MM-DD").
%TIME%	Current time ("HH-MM-SS").
%DATETIME%	Current date and time ("YYYY-MM-DD HH-MM-SS").
%TIMESTAMP%	Current date and time, unixtime in hex, 8 digits.
%RND4%	Random value, 4 hex digits, almost unique (not recommended).
%DDATE%	Current date, dense ("YYYYMMDD").
%DTIME%	Current time, dense ("HHMMSS").
%YEAR%, %MONTH%, %DAY%, %HOUR%, %MINUTE%, %SECOND%	Current date / time parts as digits (4 for year, 2 for others).

%COUNTER%	5-digit decimal counter, beginning at 1.
%COUNTER1%, %COUNTER2%, %COUNTER3%, %COUNTER4%, %COUNTER5%	1/2/3/4/5-digit decimal counter, beginning at 1.
%CCOUNTER%	5-digit decimal conditional counter (1st iteration is erased, 2nd iteration is "00002")
%CCOUNTER1%, %CCOUNTER2%, %CCOUNTER3%, %CCOUNTER4%, %CCOUNTER5%	1/2/3/4/5-digit decimal conditional counter.
%UCOUNTER%	5-digit decimal underscore counter (1st iteration is erased, 2nd iteration is "_00002")
%UCOUNTER1%, %UCOUNTER2%, %UCOUNTER3%, %UCOUNTER4%, %UCOUNTER5%	1/2/3/4/5-digit decimal underscore counter.
%%	Single % sign.

For example, if you enter the path in the form : *C:\Reports\%INTERVAL%_%COUNTER%"*, the folder names will be generated as *C:\Reports\Day 2012-02-02_00001; C:\Reports\Day 2012-02-02_00002* and so on.

To send generated reports via email, you need to enter the SMTP server and sender address information in **Tools** > **Server Options** > **Other settings**.

3. **Generated Reports** – Previously generated reports can be viewed in the **Generated Reports** tab. For more options, select individual (or multiple) reports and use the context menu (right-click). You can sort the reports by the **Report Name**, the **Date** the report was generated, the **Template Name** and the **Location** of the report. Click **Open** or double-click a report in the list to open the report. Clicking a report in the list will show a preview in the lower section (if this option is selected).

Templates placed in the **Favorites** list can be used later to immediately generate new reports. To move a template to Favorites, right-click the report and select **Add to Favorites** from the context menu.

3.4.16.1 Dashboard

A **Dashboard** is a set of reports that are automatically updated with new data that give a comprehensive overview of the system's state. Each user with access to the ERAC and a login has an individual set of dashboards that they can fully customize. These settings are stored directly on the server, so the user has access to the same dashboard from any browser.

The dashboard feature uses the ERA HTTP server by default, communication through port 443. The ports and certificates (for HTTPS) can be changed in **Advanced Server options** in the ERA Console. The **Dashboard** and the **Dashboard connection options** can also be accessed from the ERAC Main program window in the toolbar (blue cloud icon).

NOTE: The administrator needs to prepare a template for each report before it can be used in the dashboard. Otherwise, the data in the reports may not be displayed correctly.

NOTE: By default, the **Dashboard** is started using the https protocol with a self-signed certificate. This may trigger the following warning message in the web browser: *The security certificate presented by this website was not issued by a trusted certificate authority*. Note that when using HTTP, your user names and passwords will be transmitted in plaintext. This can be particularly unsafe when using Windows/Domain logins.

The installer can generate a self-signed certificate for you. Some browsers may display a warning when encountering a self-signed certificate. You can also provide your own certificate either during the advanced installation mode or anytime later by the ESET Configuration Editor. The provided certificate can be signed by a trusted certificate authority or using your own certificate root. The following X.509 certificate and private key formats are supported:

- ASN – ASN.1 DER encoded certificate and key in separate files.
- PEM – Base64 encoded ASN with extra headers, certificate and key in separate files.

- PFX – Certificate and private key in a single container file.

It is not possible to use a certificate and a key in different formats.You can change the protocol to http clicking **Dashboard** (blue cloud icon) in the main program window of the ERAC and then **Configure...**, or you can define your own certificate (in PEM file format, X.509 base64 encoded) using the ESET Configuration Editor (**Tools** > **Server** > **Options** > **Advanced** > **Edit Advanced Settings...** > **Remote Administrator** > **ERA Server** > **Settings** > **Dashboards** > **Local certificate key**/**Local certificate**).

NOTE: The Dashboard also supports IPv6 protocol. For example, *http://[::1]:8080*.

There is a set of predefined templates (shown below) for the **Dashboard**, or you can create a custom template.

- **Antispam Action Summary** – Shows a summary of all antispam engine activity.
- **Antispam Score composition** - Shows the composition of the spam score and the number of rated messages.
- **Client Connection Overview** – Shows an overview of client connections based on the time and the status of their connection.
- **Client CustomInfo 1 Summary** - Shows a comprehensive report with user-defined information (needs to be defined first).
- **Client CustomInfo 2 Summary** – Shows a comprehensive report with user-defined information (needs to be defined first).
- **Client CustomInfo 3 Summary** – Shows a comprehensive report with user-defined information (needs to be defined first).
- **Clients of Groups** – Shows the client count of selected groups.
- **Clients of Groups to All** – Shows the ratio of client count of selected groups to all overall client count (as a percentage).
- **Clients with Active Threats** – Shows clients with active threats (not cleaned during the scan) along with information about the active threats.
- **Greylist Action Summary** – Shows all greylisted messages and action taken.
- **Managed and Unmanaged Computers** – Shows computers that are currently connecting to the ERA Server (managed computers) and computers that don't (unmanaged computers). This is based on the default search task.
- **Os Name Summary** – Shows the number and the type of client operating systems.
- **Product Summary** – Shows the number and the type of client security products.
- **Protection Status Summary** – Shows the number of clients and their security status.
- **SMS Spam Progress** – Shows progress of SMS Spam.
- **Server Database Load** – Shows the complete amount of time the database was used by all threads.
- **Server Database Queries** – Shows the amount of SQL queries performed on the database.
- **Server Hardware Load** – Shows the CPU and the RAM usage of the server machine.
- **Server Status Monitoring** – Shows the server status along with information about the virus database update.
- **Threats Comparative Progress** – Progress of malware events by selected threats (using filter) compared with the total number of threats.
- **Threats Progress** – Progress of malware events (number).
- **Threats By Object** – Number of threat alerts according to attack vector (emails, files, boot sectors).
- **Threats By Scanner** – Number of threat alerts from the individual program modules.
- **Top Clients by Disconnection** – Shows top clients sorted by their last connection date.
- **Top Clients with most Network Attacks** – Shows top clients with most network attacks.
- **Top Clients with most SMS Spam** – Shows top clients with most SMS spam.
- **Top Clients with most Spam** – Shows top clients with most spam messages.
- **Top Clients with most Threats** – Lists the most ”active” client workstations (measured by number of detected threats).
- **Top Greylist Mail Recipients** – Shows top recipients of greylisted messages.
- **Top Greylist Mail Senders** – Shows top senders of greylisted messages.
- **Top Network Attacks** – Shows top network attacks.
- **Top Network Attacks Sources** – Shows top network attack sources.
- **Top SMS Spammers** – Shows top SMS spammers for specified targets.
- **Top Spam Recipients** – Shows top recipients of spam messages.
- **Top Spam Senders** – Shows top senders of spam messages.
- **Top Threats** – List of the most frequently detected threats.
- **Top Threats by Spread** – Shows top threats by spread.
- **Top Users with most Threats** – Lists the most ”active” users (measured by the number of detected threats).
- **Unregistered Computers** – Shows all unmanaged computers - computers that are not connecting to the ERA Server. It also shows the time at which a new unmanaged computer was found.

Existing report templates can be imported/exported from/to an *.xml* file by clicking **Import.../Export...** . Name conflicts during the import (existing and imported templates with the same name) are resolved by assigning a random string after the name of an imported template.

To save the settings of defined reports to a template, click **Save** or **Save as...** . If you are creating a new template, click **Save as...** and give the template a name. Clicking **Default Templates** will reset the predefined templates to their original state (this action will not affect custom created templates).

- **Options**

Preview Report – Clicking this button will generate the dashboard and show a preview.

Report

Type – Type of report, based on the predefined templates. It can be modified for predefined templates that have been used for the creation of custom templates.

Filter

Target clients – You can specify if you want the report to collect **All** data or data from **Only Selected Clients/ Servers/Groups**, or you can **Exclude Selected Clients/Servers/Groups**. The clients/servers/groups can be specified after clicking the **...** button next to the **Target clients** drop-down menu in the **Add/Remove** dialog window.
Threat – You can also specify if you want the report to show **All** threats, **Only Selected Threats** or **Exclude Selected Threats**. Threats can be specified by clicking **...** next to this drop-down menu in the **Add/Remove** dialog window.

Other details can be configured by clicking **Additional Settings...** . These settings apply mostly to data in the heading and in the types of graphical diagrams used. However, you can also filter data according to the status of selected attributes. Additionally, you can select which report format will be used (.html, .csv).

- **Interval**

Time - **Last X Minutes/Hours/Days/Weeks/Months/Years** from which you want the data to be in the report. The time is based on the time the incident was reported to ERA.

- **Refresh**

Browser Refresh Interval – Select the time interval for the refresh of new data received from the web server.
Server Refresh Interval – Select the time interval during which the data will be sent to the web server.

3.4.16.1.1 Dashboard Web Servers List

Click the arrow next to the the Dashboard icon in the main menu to configure the **Dashboard Web Servers** connection options.

- **Dashboard Web Servers** – List of all available dashboard web servers.
- **Remove** – Clicking this button removes the selected dashboard web server from the list.
- **Set As Default** – Sets the selected dashboard web server as default. This will be available first in the drop-down menu (after clicking the arrow next to the dashboard icon) and will open first after clicking the dashboard icon itself.
- **Protocol** – You can choose between http and https with a self signed certificate.
- **Host name or IP address** – Displays the Host name or the IP address of the selected dashboard web server. Alternatively, you can enter a new Host name or IP address and click **Add/Save** to save the data and add the dashboard web server to the list.
- **Comment** – Optional comment/description for the selected dashboard web server.

NOTE: The Dashboard also supports the IPv6 protocol. For example, *http://[::1]:8080*.

3.4.16.2 Example report scenario

To maintain your clients' network security at the top level, you will need to have a good overview of the network's security status. You can easily create reports with full details about threats, updates, client product versions, etc. (for more information, see the Reports 37 section). Typically, a weekly report will provide all the necessary information. However, there may be situations during which additional vigilance is necessary, as in the event of a found threat.

To provide an example, we will create a parametric group called *Quarantine*. This group will contain only computers in which a threat was detected and cleaned during the most recent on-demand scan. Set this condition by selecting the checkbox next to **HAS Last Scan Found Threat**. To create this parametric group, follow the instructions in the Parametric Groups 83 section.

NOTE: When creating the *Quarantine* group, verify that the **Sticky** option is disabled. This ensures that the computer will be assigned dynamically and removed once the conditions are no longer met.

Create the *Quarantine Computers* report. To create a report for this parametric group, follow the instructions in the Reports 37 section.

The specific settings for our example are as follows:

- **Options** section settings:

Type:	Quarantine Report with Details
Style:	Blue Scheme
Target clients:	Only Selected Groups
Threat:	n/a

- **Interval** wildcard settings:

Current:	Day

- **Scheduler** wildcard settings:

Frequency:	Daily
Every:	1 day

TIP: You can store results to the report database or set a folder where report copies will be stored. Reports can also be sent via email. All these setting are available after clicking **Select Target...**

Generated reports can be reviewed in the **Generated Reports** wildcard in the **Reports** section.

Summary: We created the parametric group *Quarantine*, containing computers on which a threat was reported during the most recent on-demand scan. Next, we created an automated report that will inform us, daily, what computers belong to the *Quarantine* group, giving us a good overview of the status of our client network so we can keep potential threats under control.

TIP: If you want to see the last scan log details, you can use the **Scan Report with Details** report type.

3.4.17 Remote Install tab

This tab provides options for several remote installation methods of ESET Endpoint Security or ESET Endpoint Antivirus on clients. For detailed information, see Remote Installation 61.

1. To search for computers, you can use the default search task or create a new one. To create a new search task, click **Add New...** to start the Network Search Task Wizard 45. To run a search task, click **Run**. To modify a search task, right-click a task and click **Edit**.

2. Search results can be filtered using the **Search Result Filter** tool in the section below. Filtering the results does not affect the actual search task. Additional search criteria in the drop-down menu:

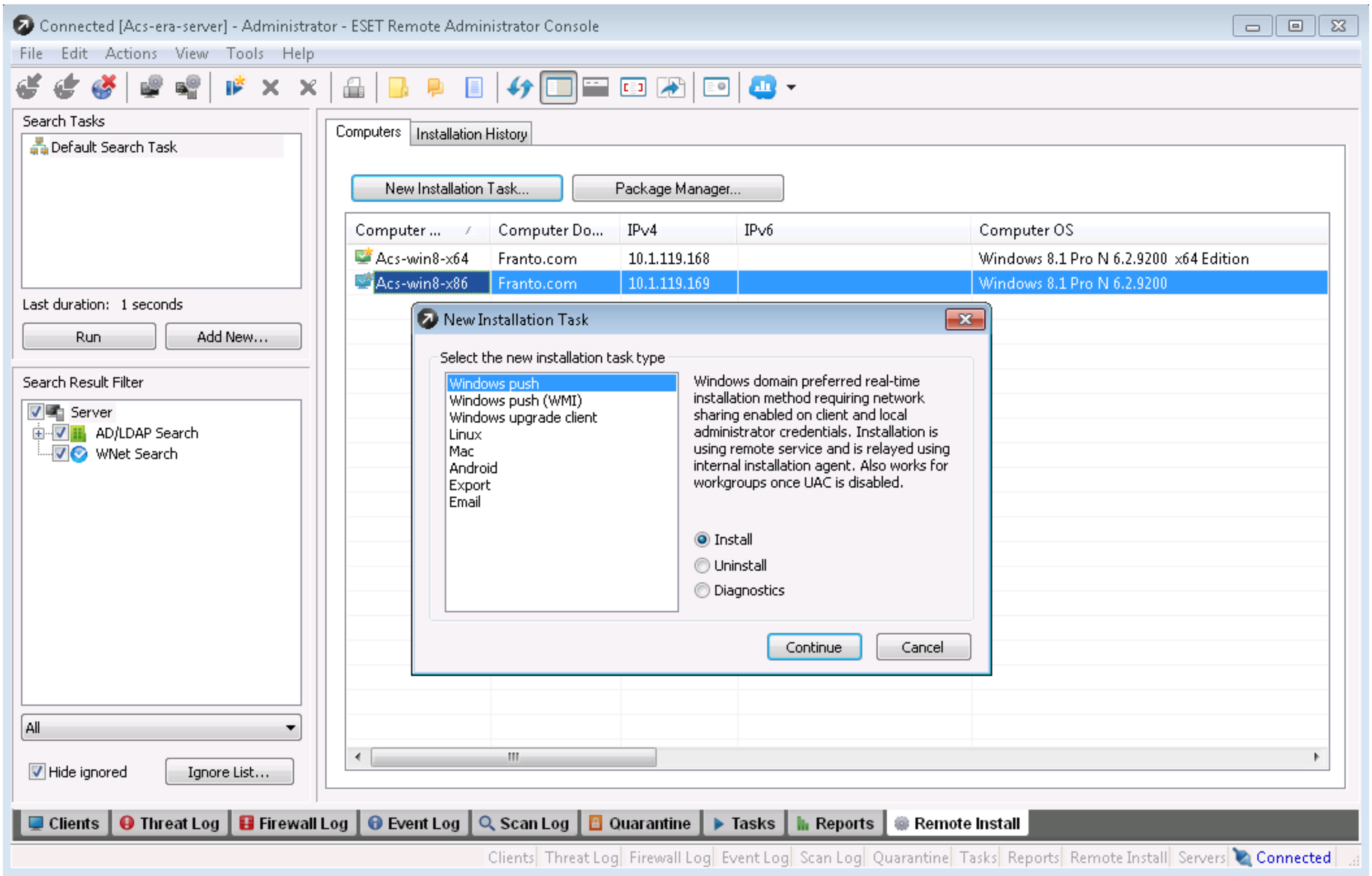
- **All** – Shows all computers visible to ERAS.

- **Unmanaged / New** – Shows computers that are not listed in the **Clients** tab of ERA Console.

- **Managed with Last Connected Warning** – Shows computers that are listed in the **Clients** tab of ERA Console which have not connected in a while (3 days by default). The time interval is configurable in menu **Tools** > **Console Options...** > **Colors** > **Clients: Last Connected** > **Specify the time interval for last connected warning coloring**.

- **Hide ignored** – By default, this option is active. It hides computers on the ignore list created by the administrator. To add any computer to the **Ignore List**, simply right-click the desired computer and from the context menu select **Add to Ignore List...** . You can also edit the Ignore List by clicking **Ignore List...** and applying the desired changes in the **Remote Install Ignore List** window.

3. The search results for the current search task are shown in the **Computers** section. From here, you can manage installation packages 46 by clicking **Package Manager...** and run a Remote push install 63 by clicking **New Installation Task...**.


Connected [Acs-era-server] - Administrator - ESET Remote Administrator Console
File Edit Actions View Tools Help
Search Tasks
Default Search Task
Last duration: 1 seconds
Run
Add New...
Search Result Filter
Server
AD/LDAP Search
WNet Search
All
Hide ignored
Ignore List...
Computers
Installation History
New Installation Task...
Package Manager...
Clients Threat Log Firewall Log Event Log Scan Log Quarantine Tasks Reports Remote Install
Clients Threat Log Firewall Log Event Log Scan Log Quarantine Tasks Reports Remote Install Servers Connected

Computer ...	Computer Do...	IPv4	IPv6	Computer OS
Acs-win8-x64	Franto.com	10.1.119.168		Windows 8.1 Pro N 6.2.9200 x64 Edition
Acs-win8-x86	Franto.com	10.1.119.169		Windows 8.1 Pro N 6.2.9200

New Installation Task

Select the new installation task type

Windows push
Windows push (WMI)
Windows upgrade client
Linux
Mac
Android
Export
Email

Windows domain preferred real-time installation method requiring network sharing enabled on client and local administrator credentials. Installation is using remote service and is relayed using internal installation agent. Also works for workgroups once UAC is disabled.

● Install
○ Uninstall
○ Diagnostics

The context menu (right-click) of the **Computers** tab offers the following specific options along with the generic context menu options of ERA Console:

- **Add to Ignore List...** – To add the selected computers to the **Ignore List**
- **WMI Information...** – To specify the WMI logon information of a computer.
- **Properties** – Opens the **Properties** window where you can find all important information about the selected computer.

For the other context menu options, see the Context menu 27 chapter.

3.4.17.1 Network Search Task Wizard

A search task is a set of parameters used to search your network for computers. Search tasks are stored directly on the server, so they are available for all administrators.

You can use the predefined default search task, which is run periodically (it can also be triggered manually) and searches the entire network. Search results from this task are stored on the server. This task can also be edited, but once initiated it can not be stopped until it finishes.

Custom task parameters are stored on the server, but their search results are only sent to the console from which they were run. These search tasks can only be initiated manually.

To create a new search task click **Add New...** The **Network Search Task Wizard: Scan Methods** window will open where you can choose the methods to be used to search the network (you can choose multiple search methods):

- **Active Directory / LDAP** – This option lets you select the branches of the active directory you want to search for computers, you can also **include disabled computers**.
- **Windows Networking (WNet)** – Searches the computers in your windows network.
- **Shell** – Searches all computers in your network locations (windows network neighborhood).
- **IP Address** – Lets you select the **IP range** / **IP mask** to be used during the search, or you can define a **custom IP address list**. The computers are searched by accessing their ports (which can be configured). You can also use a ping (this is recommended particularly when searching for Linux computers).
- **Custom computer list** – Define a custom list of computers or import a custom list of computers from a *.txt file using **Import From File**.

In addition, you can **Use WMI to get additional information about found computers**.

Click **Next** and in the next screen you have the option to decide if the selected search task will be saved temporarily (deselect the check box next to **Save in Search Tasks panel**) or permanently in the **Search Tasks panel** (this is the default option) and if the task is supposed to be run (this is the default option) right after clicking **Finish** or not (deselect the check box next to **Run now**).

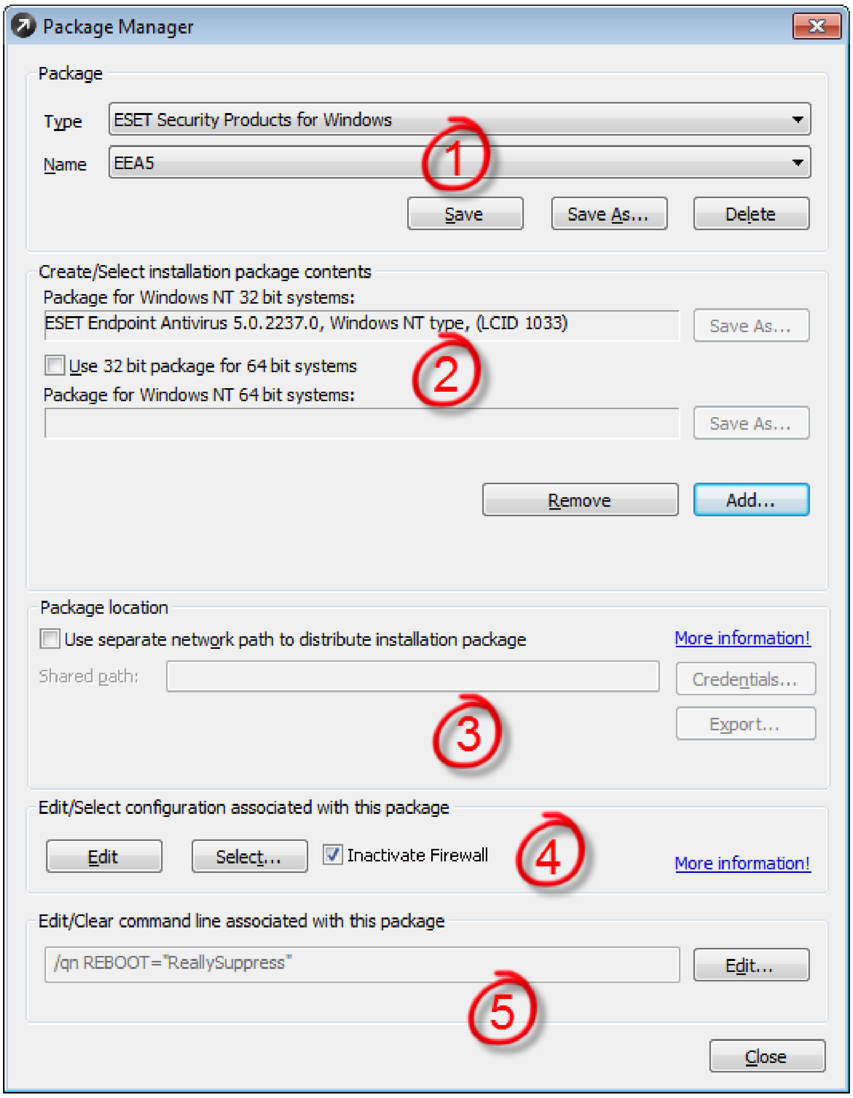
To run the task later, click **Run** in the **Remote install** tab.

NOTE: If the service is running under the local system account, no computers may be found using the Shell and the Wnet search. This is because the local system account doesn`t have the permissions to perform such a search. To resolve this issue change users or use a different search method.

NOTE: If you wish to increase the speed of search task when evaluating IP ranges and WMI information, increase the value of **Maximum number of search threads** at *Tools > ESET Configuration Editor > Remote Administrator > ERA Server > Settings > Remote Install*.

3.4.17.2 Package Manager

Remote installation is initiated through ERAC. To manage the installation packages in the ERAC, click the **Remote Install** tab and select the **Computers** tab. Click **Package Manager...** to open the **Package Manager** window.



Package Manager

Package

Type: ESET Security Products for Windows

Name: EEA5

Create/Select installation package contents

Package for Windows NT 32 bit systems:

ESET Endpoint Antivirus 5.0.2237.0, Windows NT type, (LCID 1033)

☐ Use 32 bit package for 64 bit systems

Package for Windows NT 64 bit systems:

Package location

☐ Use separate network path to distribute installation package

Shared path:

Edit/Select configuration associated with this package

☑ Inactivate Firewall

Edit/Clear command line associated with this package

/qn REBOOT="ReallySuppress"

Each installation package is defined by a **Name** ((1) in the figure above). The remaining sections of the dialog window are related to the content of the package, which is applied after it has been successfully delivered to a target workstation.

The **Type** drop-down menu in section (1) provides access to additional ERA features. In addition to remote installation, ESET security products can be uninstalled remotely using the **Uninstall ESET Security Products for Windows and NOD32 version 2** task. Remote installation of an external applications can also be performed by selecting **Custom package**. This is particularly useful if you want to run various scripts and executables on the client machine, including uninstall tools for third-party security products or standalone cleaning tools. You can specify custom command-line parameters for use by the **Package entry file**. See Installation of third party products using ERA 158 for more details.

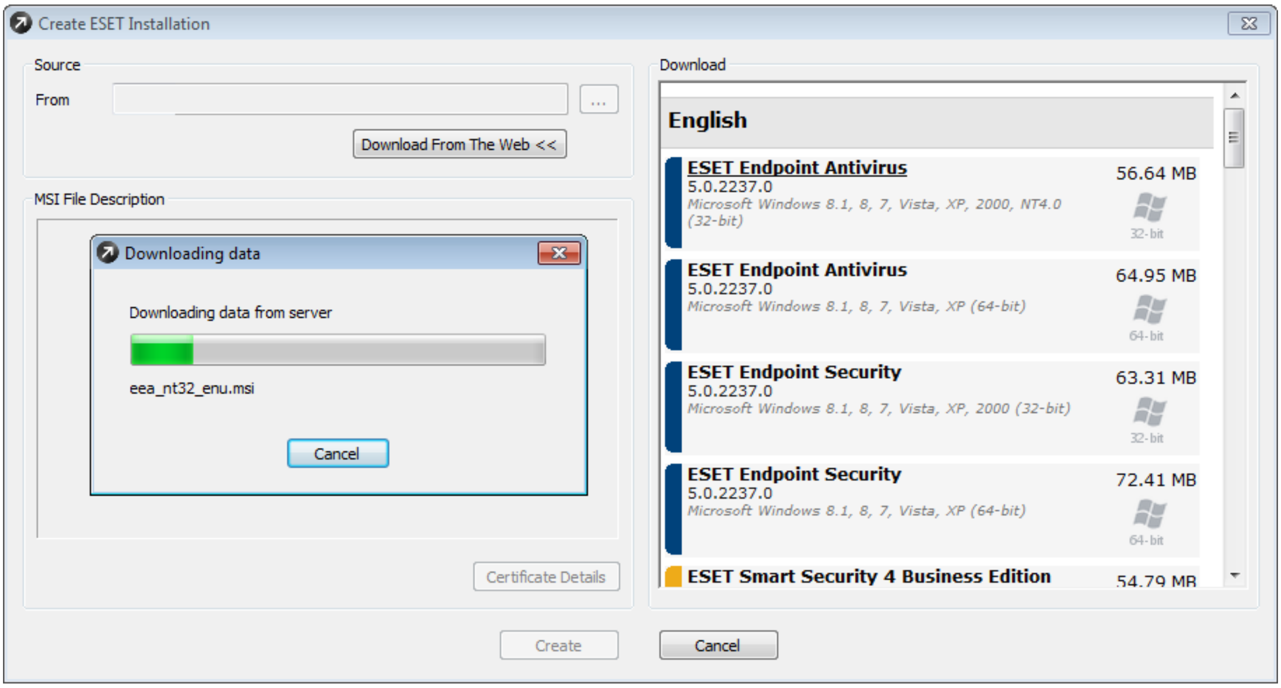
Each package is automatically assigned an ESET Remote Installer agent, which allows for seamless installation and communication between target workstations and theERAS. The ESET Remote Installer agent is named *einstaller.exe* and contains the ERAS name and the name and type of package to which it belongs. The following section provides a detailed description of the installer agent.

ESET client solution installation files (2)

Click **Add...** to select an installation package source. You have 2 options:

1. Select an installation package locally by clicking browse (...).

2. Click **Download From The Web** (recommended). A list of packages should appear in the **Download** section. Select your desired package in the appropriate language and select a destination folder to start the download.



Downloading data from server

eea_nt32_enu.msi

English

ESET Endpoint Antivirus 5.0.2237.0 Microsoft Windows 8.1, 8, 7, Vista, XP, 2000, NT4.0 (32-bit) 56.64 MB 32-bit

ESET Endpoint Antivirus 5.0.2237.0 Microsoft Windows 8.1, 8, 7, Vista, XP (64-bit) 64.95 MB 64-bit

ESET Endpoint Security 5.0.2237.0 Microsoft Windows 8.1, 8, 7, Vista, XP, 2000 (32-bit) 63.31 MB 32-bit

ESET Endpoint Security 5.0.2237.0 Microsoft Windows 8.1, 8, 7, Vista, XP (64-bit) 72.41 MB 64-bit

ESET Smart Security 4 Business Edition 54.79 MB

Note: For **ESET Security Products for Windows** packages, it makes sense to select the check box next to **Use 32 bit package for 64 bit systems** if you are installing ESET Remote Administrator Server or Console only. This option should not be used when installing endpoint products (for example, ESET Endpoint Security or ESET Endpoint Antivirus) because on 64-bit systems a 64-bit version of that product must be installed (the installation will fail when trying to install a 32 bit version).

Package location (3)

The installation packages are located on the ERAS server in the following directory:

%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\packages

You can choose a different network location for remote installation packages here.

XML configuration file for ESET client solutions (4)

When you create a new installation package, the primary server password to connect to your ERA Server will be left blank. Click **Edit** to edit the .xml configuration for this package and set the password (if needed) in the **Remote administration** branch of the respective product.

The **Inactivate Firewall** setting is enabled by default in order to have the firewall of ESET Endpoint Security turned off so that next connection attempt of ERA Server to a particular client is not blocked. You can turn the Firewall on at a later time by sending a Configuration Task 78 to the client. In that configuration task you would look up the following item: "*Windows desktop v5 > Personal firewall > Settings > Firewall system integration: Personal firewall inactive*" and select **All features active**.

Note: When enabling or disabling **Inactivate Firewall** there are actually two setting properties modified. One is visible in ESET Configuration Editor and one is only visible from the .xml configuration file. If any of those two setting properties is not set (one is set and one is not) or do not have a value of range of 1 - 10, for example, you select the option **Only scan application protocols** in the **Value** field, then the **Inactivate Firewall** check-box is completely filled with blue color.

If you have a password configured for the ERA server (configurable at **Tools** > **Server Options** > **Security** > **Password for Clients (ESET Security Products)**) then that password will be automatically used in the package created, so that client machines that use that password to connect to the ERA server. If you change the password of ERA server after the fact, managed clients will not be able to connect to the server even if **Enable unauthenticated access for Clients (ESET Security Products)** is enabled on the ERA server. In this case you would have to send a Configuration Task 78 to the managed clients.

Command-line parameters assigned to the package (5)

There are several parameters 48 that can affect the installation process. They can be used either during direct installation with the administrator present at the workstation, or remote installation.

3.4.17.2.1 Command Line Options

For remote installations, parameters are selected during the process of configuring installation packages – selected parameters are then applied automatically on target clients.

The additional parameters for ESET Endpoint Security and ESET Endpoint Antivirus can be also typed after the name of the *.msi* installation package (e.g., *eea_nt64_ENU.msi /qn*) in case of executing the remote installation via command line interface of the hosting operating system:

- **/qn** - Quiet installation mode – no dialog windows are displayed.
- **/qb!** - No user intervention is possible, but the installation process is indicated by a progress bar in %.
- **REBOOT =”ReallySuppress”** – Suppresses restart after installation of the program.
- **REBOOT =”Force”** – Automatically reboots after installation.
- **REMOVE=...** – Disables the installation of a selected component. Command parameters for each component are listed below:

  Emon – Email client protection
  Antispam – Antispam protection
  Dmon – Document protection
  ProtocolScan – Protocol filtering
  Firewall – Personal Firewall
  eHttpServer – Update mirror server
  eDevmon – Device control
  MSNap – Microsoft NAP
  eParental – Web control

- **REBOOTPROMPT =””** – After installation, a dialog window prompting the user to confirm rebooting is displayed (can’t be used along with */qn*).
- **ADMINCFG =”path_to_xml_file”** – During installation, parameters defined in the specified.xml files are applied to ESET security products. This parameter is not required for remote installation. Installation packages contain their own *.xml* configuration which is applied automatically.
- **PASSWORD=”password”** – Add this parameter if ESET client product settings are password protected.
- **/SILENTMODE** – Quiet installation mode – no dialog windows are displayed.
- **/FORCEOLD** – Will install an older version over an installed newer version.
- **/CFG =”path_to_xml_file”** – During installation, parameters defined in the specified *.xml* files are applied to ESET client solutions. The parameter is not required for remote installation. Installation packages contain their own *.xml* configuration which is applied automatically.
- **/REBOOT** – Automatically reboots after installation.
- **/SHOWRESTART** – After the installation, a dialog window prompting the user to confirm that they want to restart is displayed. This parameter can only be used if combined with the *SILENTMODE* parameter.
- **/INSTMFC** – Installs MFC libraries for the Microsoft Windows 9x operating system that are required for ERA to function correctly. This parameter can always be used, even if the MFC libraries are available.

NOTE: If UAC is enabled on your client solutions, the default UAC security settings on Windows Vista/7/2008 will require user confirmation before executing any program. Trying to remotely install client solutions and using any of the parameters above may require user interaction. To avoid user interaction, run the installation using the following command: *C:\Windows\System32\msiExec.exe -i path_to_the_msi_file /qb!*

ADMINCFG="path_tp_the_xml_file" REBOOT="ReallySupress" where *C:\Windows\System32\msiExec.exe -i* is the executable of the windows installer component and the install parameter and *path_to_the_msi_file /qb! ADMINCFG="path_tp_the_xml_file" REBOOT="ReallySupress"* is the path to the installation file and the settings file of the security product followed by the user interaction suppress parameter.

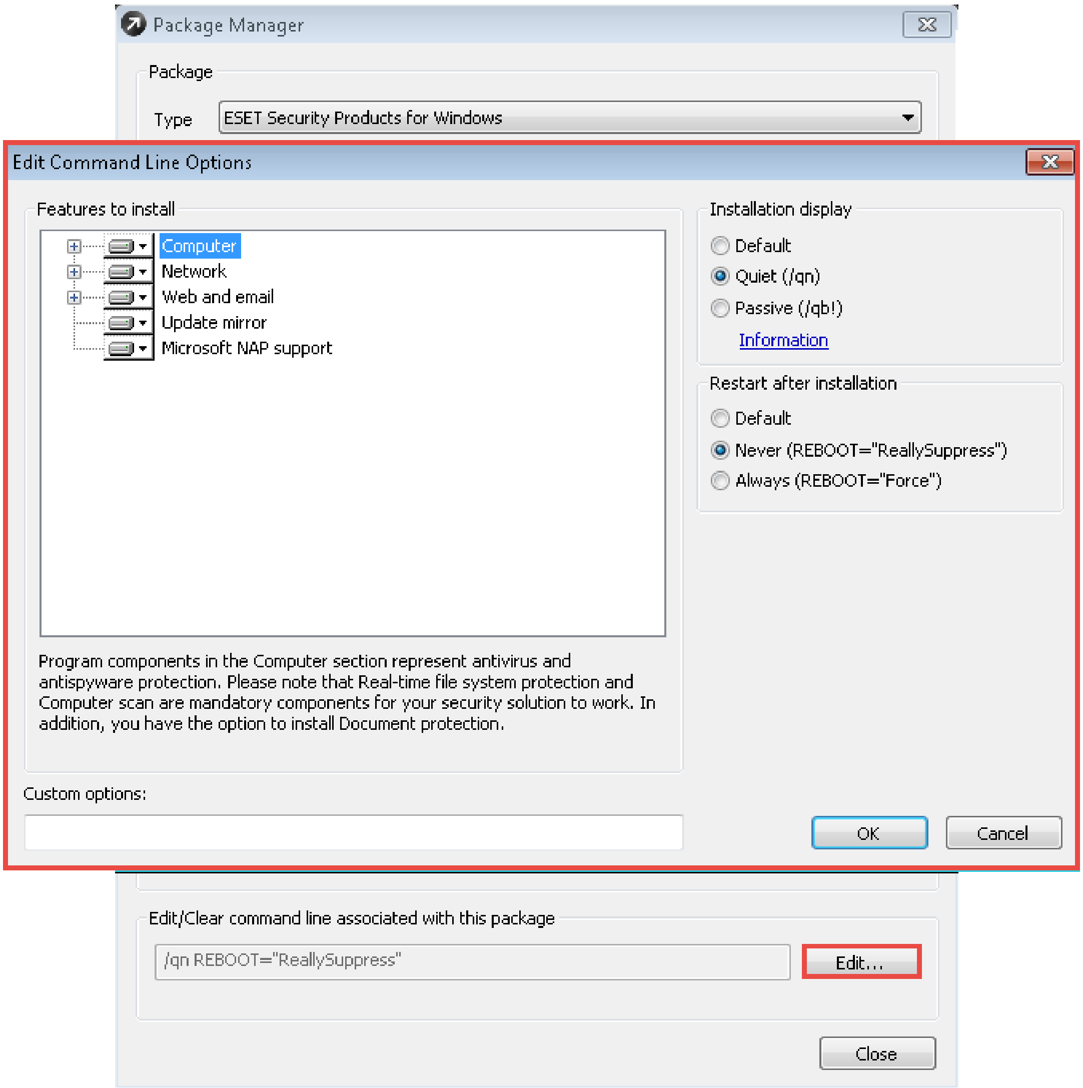
Under **Create/Select installation package contents** (2), the administrator can create a standalone install package with a predefined configuration from an existing install package (click **Save As**). Such installation packages can be run manually on the client workstation where the program is to be installed. The user only needs to run the package and the product will install without connecting back to ERAS during the installation.

NOTE: Adding a configuration to the *.msi* installation file means that the digital signature of this file will no longer be valid.

Important: On Microsoft Windows Vista and later we strongly recommend that you perform a silent remote installation (the */qn*, */qb* parameter). Otherwise interaction with a user might cause the remote installation to fail due to timeout.

3.4.17.2.2 Installation Package Options

For remote installations, parameters are selected during the process of configuring installation packages – selected parameters are then applied automatically on target clients.



Package Manager

Package

Type: ESET Security Products for Windows

Edit Command Line Options

Features to install

- Computer
- Network
- Web and email
- Update mirror
- Microsoft NAP support

Program components in the Computer section represent antivirus and antispyware protection. Please note that Real-time file system protection and Computer scan are mandatory components for your security solution to work. In addition, you have the option to install Document protection.

Installation display

○ Default
● Quiet (/qn)
○ Passive (/qb!)

Information

Restart after installation

○ Default
● Never (REBOOT="ReallySuppress")
○ Always (REBOOT="Force")

Custom options:

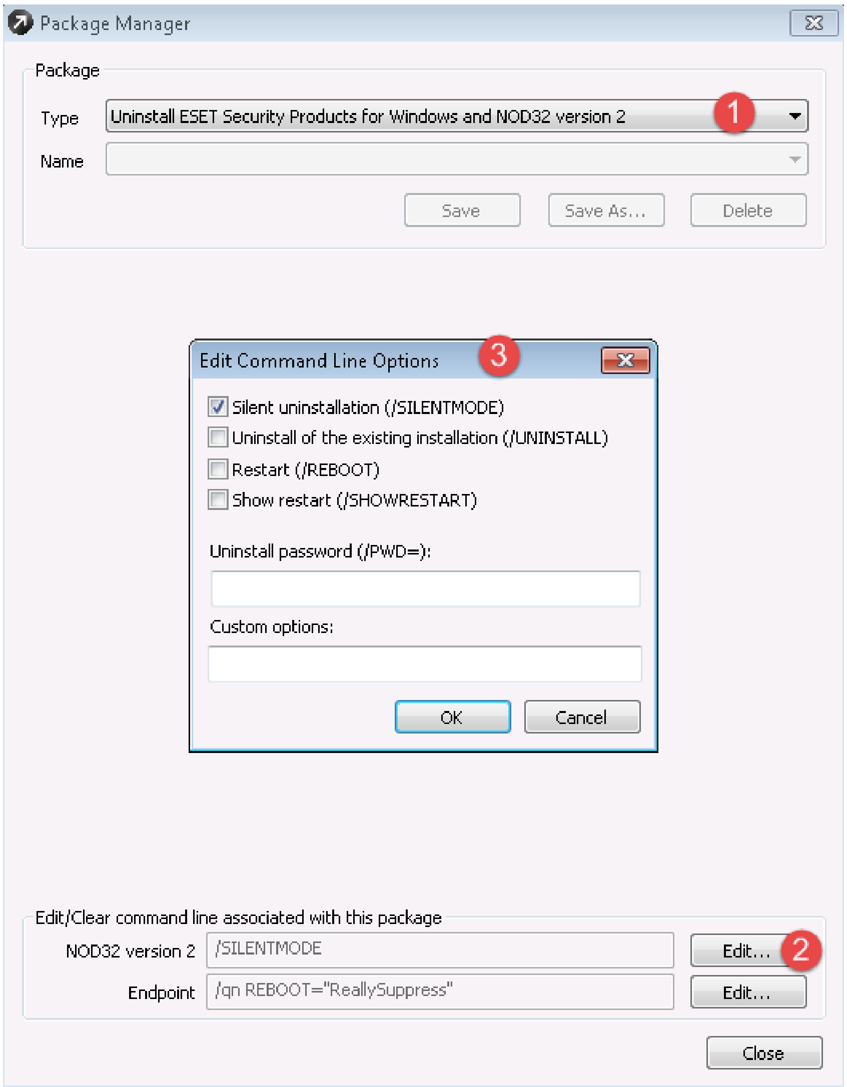
Edit/Clear command line associated with this package

/qn REBOOT="ReallySuppress"

As shown in the image above you have the option to select which parts of the package you do not want to be installed. Optionally you can use additional parameters 48 for ESET Endpoint Security and ESET Endpoint Antivirus in the **Custom options** input field.

3.4.17.2.3 ESET Endpoint Antivirus Uninstall Options

For remote uninstallation (push uninstall) of ESET Endpoint Antivirus, the default configuration can be modified by clicking **Edit...** next to the **NOD32 version 2** field in **Package Manager** after you select **Uninstall ESET Security Products for Windows and NOD32 version 2** .



Package Manager

Package

Type: Uninstall ESET Security Products for Windows and NOD32 version 2

Name:

Edit Command Line Options

☑ Silent uninstallation (/SILENTMODE)

□ Uninstall of the existing installation (/UNINSTALL)

□ Restart (/REBOOT)

□ Show restart (/SHOWRESTART)

Uninstall password (/PWD=):

Custom options:

Edit/Clear command line associated with this package

NOD32 version 2: /SILENTMODE

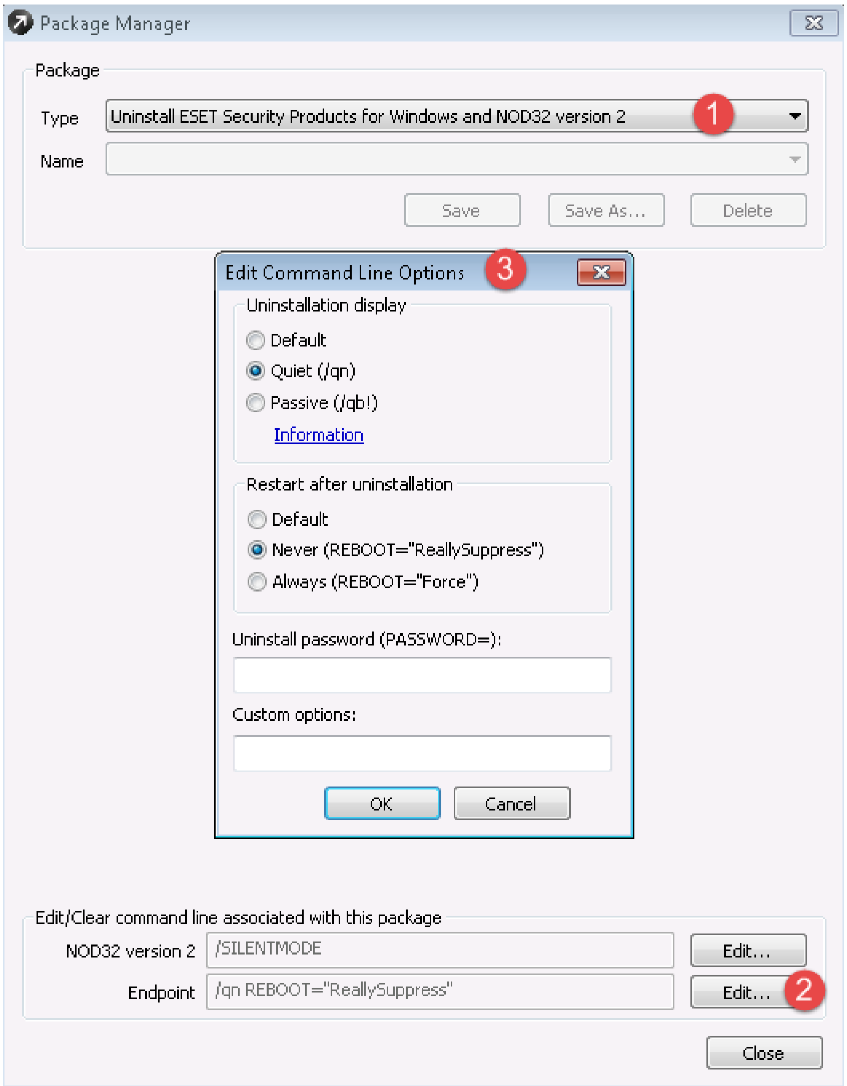
Endpoint: /qn REBOOT="ReallySuppress"

The **Edit Command Line Options** window lets you apply several options such as **Silent uninstallation** (no confirmation is required from the user of the target machine), **Restart** (after uninstallation the target machine will be restarted) and more. If you select any of those options, they will be transferred as parameters into the field of **NOD32 version 2** of **Package Manager** window after closing the **Edit Command Line Options** window via the **OK** button.

In the **Custom options** field of the **Edit Command Line Options** window you can type additional command line parameters 48. For example, you could use */L*v "my_log.log"* to write the uninstall logs to the *my_log.log* file. Afterward you would have to look up that log file via Windows search. Alternatively, you could use the absolute path for the *my_log.log* file in the **Custom options** field.

3.4.17.2.4 ESET Endpoint Security Uninstall Options

For remote removal (uninstall) of ESET Endpoint Security the default configuration can be modified by clicking **Edit...** next to **Endpoint** in the **Package Manager** window once you select **Uninstall ESET Security Products for Windows and NOD32 version 2**.



Package Manager

Package

Type: Uninstall ESET Security Products for Windows and NOD32 version 2

Name:

Edit Command Line Options

Uninstallation display

○ Default
● Quiet (/qn)
○ Passive (/qb!)

Restart after uninstallation

○ Default
● Never (REBOOT="ReallySuppress")
○ Always (REBOOT="Force")

Uninstall password (PASSWORD=):

Custom options:

Edit/Clear command line associated with this package

NOD32 version 2: /SILENTMODE

Endpoint: /qn REBOOT="ReallySuppress"

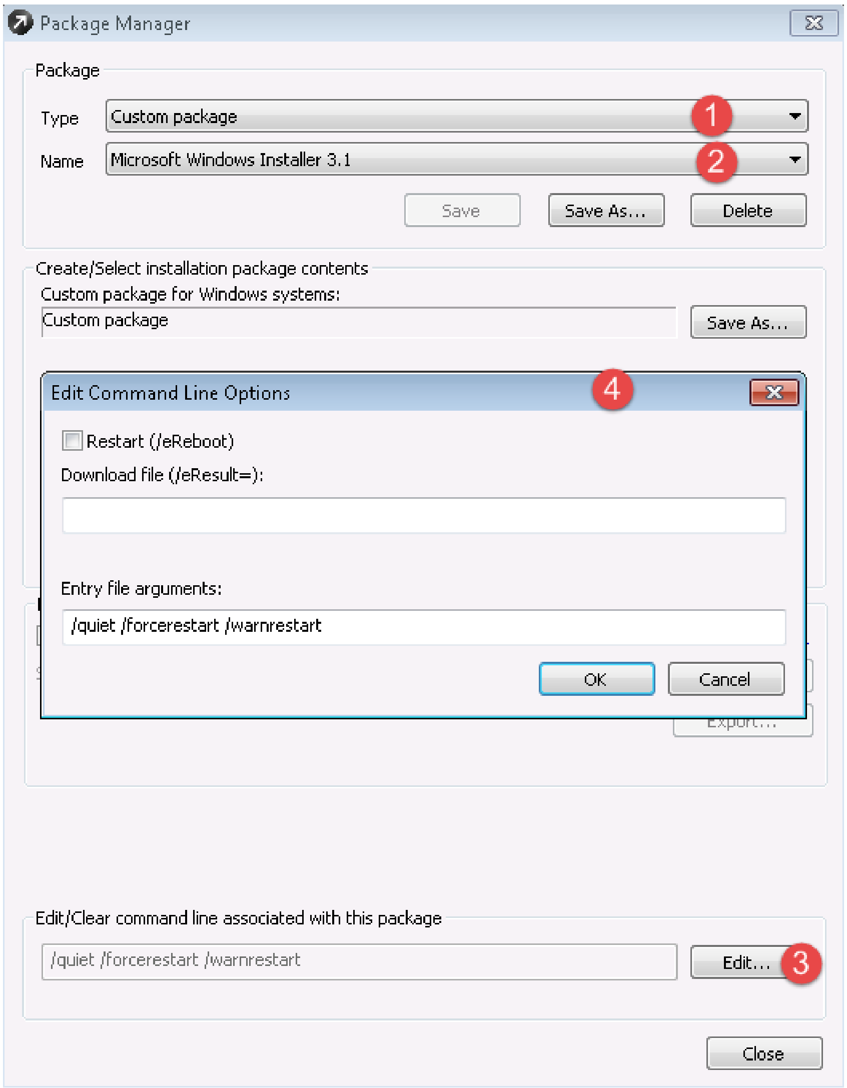
Once the **Edit Command Line Options** window opens, you can alter the selected options, for example, you may choose a **Passive** uninstallation (the user of the target machine would see the uninstallation process) or you can force the reboot of the target machine after uninstallation is finished.

In the **Custom options** field of the **Edit Command Line Options** window you can type additional command line parameters 48. For example, you could use */L*v "my_log.log"* in order to write the uninstall logs to the *my_log.log* file. Afterward you would have to look up that log file via Windows search. Alternatively, you could use absolute path for the *my_log.log* file in the **Custom options** field.

NOTE: If you choose "Default" in one of the options, then no parameters will be applied for that option.

3.4.17.2.5 Custom Package Command Line Options

When configuring a **Custom package** in **Package Manager**, while your custom package supports some custom parameters, then you can define any of the supported parameters in the **Entry file arguments** field of the **Edit Command Line Options** window. Click **Edit** next to the **Edit/Clear command line associated with this package** field to open the **Edit Command Line Options** window.



Type: Custom package

Name: Microsoft Windows Installer 3.1

Custom package for Windows systems: Custom package

□ Restart (/eReboot)

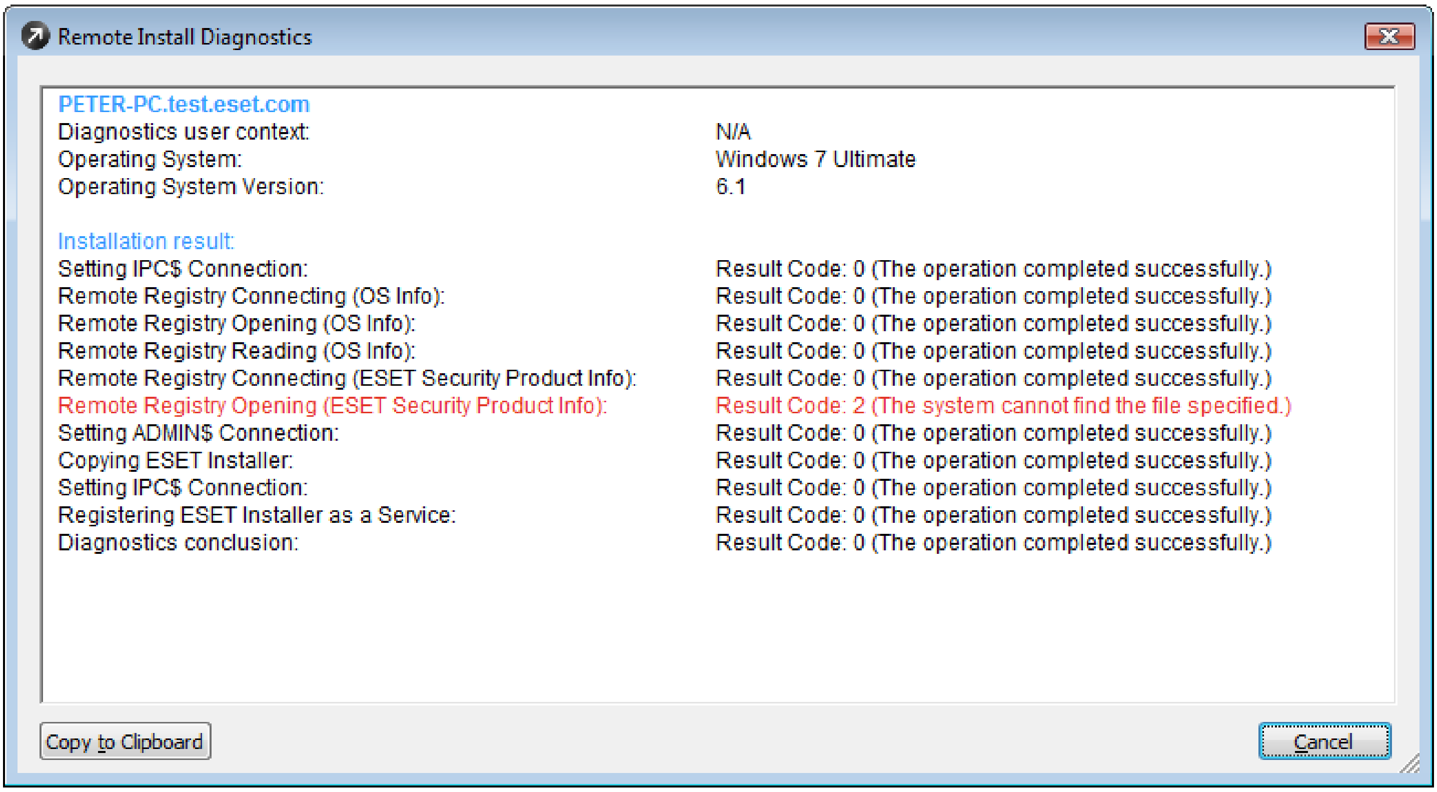
Download file (/eResult=):

Entry file arguments: /quiet /forcerestart /warnrestart

Edit/Clear command line associated with this package: /quiet /forcerestart /warnrestart

If your custom script is going to write the results to a file on the target machine, you can define the name of that file in the **Download file (/eResult=)** field of the **Edit Command Line Options** window, so that the ERA Server can download that file after the installation of custom package has been carried out and you can view the content of the result file via the internal viewer 55 of ERA Console.

3.4.17.3 Remote Install Diagnostics



```
PETER-PC.test.eset.com
Diagnostics user context:                                N/A
Operating System:                                        Windows 7 Ultimate
Operating System Version:                                6.1

Installation result:
Setting IPC$ Connection:                                 Result Code: 0 (The operation completed successfully.)
Remote Registry Connecting (OS Info):                    Result Code: 0 (The operation completed successfully.)
Remote Registry Opening (OS Info):                       Result Code: 0 (The operation completed successfully.)
Remote Registry Reading (OS Info):                       Result Code: 0 (The operation completed successfully.)
Remote Registry Connecting (ESET Security Product Info): Result Code: 0 (The operation completed successfully.)
Remote Registry Opening (ESET Security Product Info):    Result Code: 2 (The system cannot find the file specified.)
Setting ADMIN$ Connection:                               Result Code: 0 (The operation completed successfully.)
Copying ESET Installer:                                  Result Code: 0 (The operation completed successfully.)
Setting IPC$ Connection:                                 Result Code: 0 (The operation completed successfully.)
Registering ESET Installer as a Service:                 Result Code: 0 (The operation completed successfully.)
Diagnostics conclusion:                                  Result Code: 0 (The operation completed successfully.)
```

- **Setting IPC$ Connection**:

  The Administrator should have local admin permissions on all client computers.

  The shared resources must be installed and enabled on the client.

  The network firewall must have the shared resources enabled (ports 445 and 135-139).

  Windows Administrator password cannot be blank.

  The option “Use Simple file sharing” can not be activated in a mixed environment of workgroups and domains.

  Make sure that the Server service is being executed on the client machine.

- **Remote Registry Connecting (OS Info)**:

  The Remote Registry Service must be enabled and started on the client.

- **Remote Registry Opening (OS Info)**:

  Above + The Administrator must have full control permissions over the client's registry.

- **Remote Registry Reading (OS Info)**:

  The Administrator must have read permissions over the client's registry. If the operation above is completed successfully, this operation should too.

- **Remote Registry Connecting (ESET Security Product Info)**:

  The Administrator must have full control permissions for the HKEY_LOCAL_MACHINE/SOFTWARE/ESET (or the entire HKEY_LOCAL_MACHINE/SOFTWARE branch).

- **Remote Registry Opening (ESET Security Product Info)**:

  Make sure that the Remote Registry service is running on the client computer.

- **Setting ADMIN$ Connection**:

  Administrative share ADMIN$ must be enabled.

- **Copying ESET Installer**:

  Ports 2222, 2223 and/or 2224 must be opened on the server and must be allowed on the network firewall.

- **Setting IPC$ Connection**:

  If this operation was completed successfully in the get info diagnostics, it should complete successfully here.

- **Registering ESET Installer as a Service**:

  Make sure you have sufficient rights to run the einstaller.exe on the target computer(s).

NOTE: If there should be an error during the diagnostics, you can start troubleshooting based on this information. See the chapter Requirements 62 before installation and the Frequently encountered error codes 152 chapter to analyze error codes.

3.4.17.4 Installation History

The **Installation History** tab of the **Remote Install** tab contains a list of tasks and their attributes. It shows tasks in progress, tasks waiting to be executed and finished tasks. Here you can modify the number of items to be viewed and also right-click the tasks on the list for management/maintenance options. Use the **Items to show** pull down menu to increase/decrease the number of items viewed per page and the adjacent navigation buttons to swap between the pages available.

You can also filter the information shown in the Installation History tab. Check the **Use filter** option on the left pane to activate the filter. Then, define the Tasks filter criteria - **Only computers like (?,*)/Exclude computers like (?,*)**. Type the computer name in the **Computer name:** field. You can also use wildcards; for example: *Com* and not the whole word Computer. Clicking the **Reset** button will delete the filter criteria and deactivate the filter.

- **Task Name** – Name of the task, for predefined tasks is the same as task type.
- **Task Type** – Type of the task, for more information see the chapter Tasks 77.
- **State** – Current completion state of the task.
- **Description** – Short description of the task action.
- **Date To Deploy** – Time to/passed from the task execution.
- **Date Received** – Time to/passed from the task reception at its execution point.
- **Comment** – Note assigned to the install task.

Double-clicking an install task will show the **Properties** window.

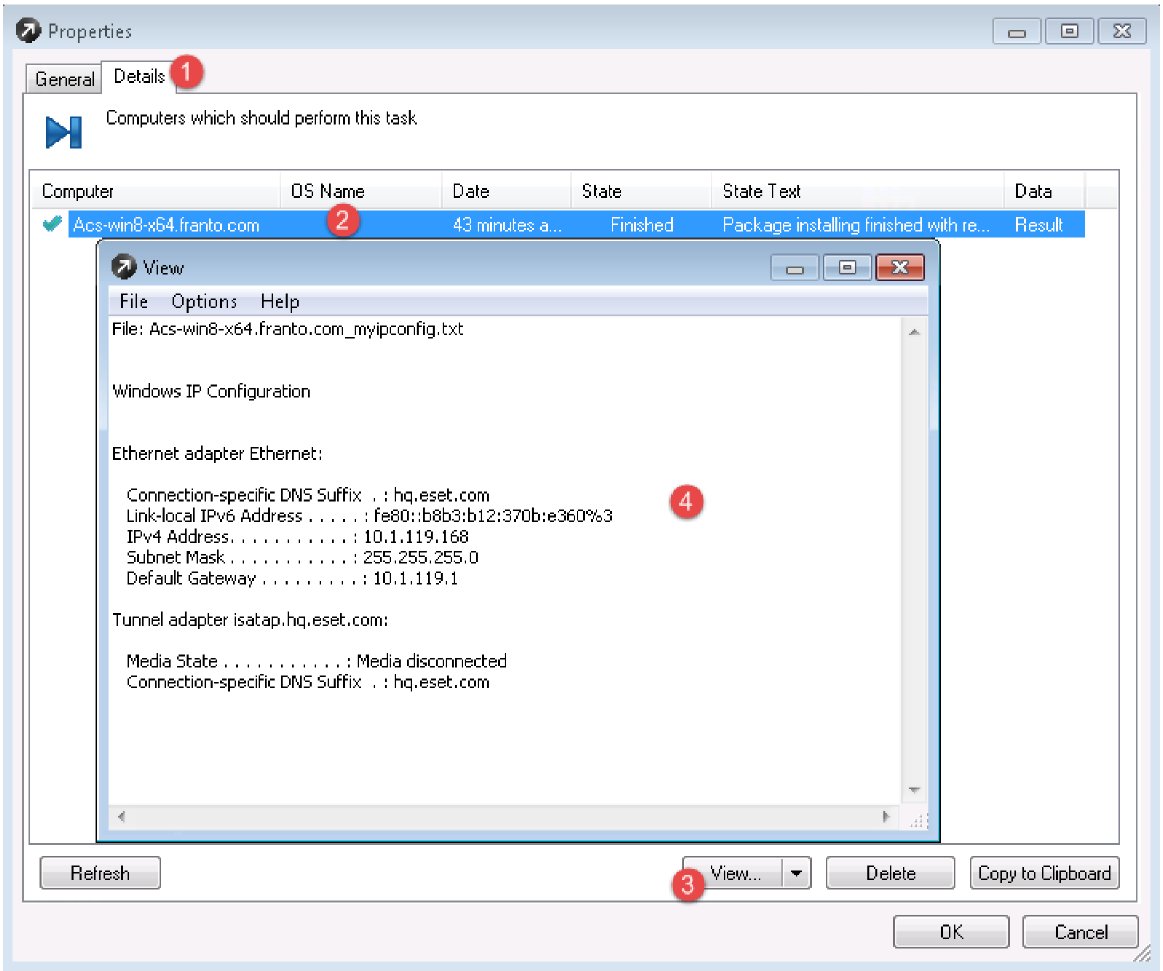
3.4.17.4.1 Run Task Again

If you want to run a task from the **Installation History** tab of the **Remote Install** tab again, right-click the desired task (or multiple tasks selected) and select **Run Task Again...** from the context menu. The launched **Run Task Again** wizard is similar to the New Installation Task 43 wizard. You can click **Continue** to continue to the **Computers Logon Settings** screen, or you can alter the task to be run prior to clicking **Continue**.

Every task you run again will generate a new record (row) in the **Installation History** tab. If a task was completed in the ***Finished with Warning*** state, double-click the task, in the **Properties** window click the **Details** tab and view the **State Text** for more information. If the **State Text** is trimmed, hover over it with your cursor to display the full text.

3.4.17.4.2 View the content of a result file

If the installation of a custom package creates a result file on the target machine and you defined the name of that result file when configuring the custom package 52, you will be able to view the content of that file in ERA Console. To do so, double-click the finished task in the **Details** tab of the **Installation History** 54 window, select a computer and click **View...**



Computer	OS Name	Date	State	State Text	Data
✓ Acs-win8-x64.franto.com		43 minutes a...	Finished	Package installing finished with re...	Result

```
File: Acs-win8-x64.franto.com_myipconfig.txt


Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : hq.eset.com
   Link-local IPv6 Address . . . . . : fe80::b8b3:b12:370b:e360%3
   IPv4 Address. . . . . . . . . . . : 10.1.119.168
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.119.1

Tunnel adapter isatap.hq.eset.com:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : hq.eset.com
```

3.5 ERA Console Options

ERA Console can be configured in the menu **Tools** > **Console Options...**

3.5.1 Connection

To access ERA Console settings go to the main ERAC menu **Tools** > **Console Options...** or **File** > **Edit Connections....** This tab is is used to configure the connection from ERAC to ERAS. For more detail, see chapter Connecting to ERAS 23.

The **Connection** tab lets you select which server you want to connect and whether you want to connect to that selected server at the ERA Console startup. The console can only be connected to one server at a time. If you want to add replicated servers, you need to set up replication in menu Tools/Server Options/Replication Settings... 113

NOTE: The port for connecting to ERA Server can be customized under **Tool** > **Server Options** > **Other Settings** tab (see chapter Other Settings 119).

Add/Remove... - use it to add new ERA Servers, or modify existing servers. Clicking this option will open the **Connection Edit** window. To add a new connection, enter the IP Address or the Hostname of the Server, Port to be used by the connection and a comment (optional). Click the **Add/Save** button to add the connection to the list of servers at the top of this window. Select a specific server for further options: you can either **Remove** it, use the **Remove All** option or edit the connection (similar to creating a new connection).

- **Connect to selected server on the console startup** – The console will automatically connect to a predefined ERA Server.

- **Show message when connection fails** – If there is a communication error, an alert will be displayed.

3.5.2 Columns

This tab allows you to specify which attributes (columns) are displayed in individual tabs. Changes will be reflected in the Custom View Mode (Clients tab 29). Other modes cannot be modified.

To display a column on a particular tab, click on the tab name in the tab list and check the column(s) you want displayed.

- **Select pane** – Choose the pane for which you wish to alter the selection of columns to show.

- **Select columns to show** – Select the columns you want to be displayed in the pane. Choose carefully to include all the information you need in the pane, but keep the view of the data transparent at the same time.

- **Clear All** – Unchecks all checkboxes in the **Select columns to show** window for the selected pane.

- **Set All** – Checks all checkboxes in the **Select columns to show** window for the selected pane.

- **Default** – Resets all checkboxes in the **Select columns to show** window to default for the selected pane.

- **All to default** – Resets all checkboxes in the **Select columns to show** window to default for all panes.

3.5.3 Colors

This tab allows you to associate different colors with specific system-related events, in order to better highlight problematic clients (Conditional Highlighting). For example, clients with a slightly outdated virus signature database (**Clients: Previous Version**) could be distinguished from clients with an obsolete one (**Clients: Older Versions or N/A**).

Assign a specific color to panes and columns by selecting them in the **Pane and Column** list. Then select in what color they should be shown.

NOTE: The column **Clients: Older Version or N/A** color is used when the version of ESET Endpoint Security Virus Database on the client is not added or older than on the server. It is also used when the version of ESET Security product on the server is older than on the client or not added.

In the column **Clients: Last connected**, the interval when to use the coloring can be specified.

3.5.4 Paths

To access ERA Console settings go to the main ERAC menu **Tools** > **Console Options...**

The **Paths** tab lets you select where your reports generated by the ERA Console should be stored. To learn more about generating and viewing reports refer to the Reports 37 chapter of this help file.

3.5.5 Date/Time

The **Date/Time** pane lets you customize advanced options for ERA Console. Also, here you can select the desired time format displayed across the records in the ERA Console window.

- **Absolute** – Console will display absolute time (e.g., *"14:30:00"*).

- **Relative** – Console will display relative time (e.g., *”2 weeks ago”*).

- **Regional** – Console will display time according to regional settings (taken from the Windows settings).

- **Recalculate UTC time to your local time (use local time)** – Select this check box to recalculate to your local time. Otherwise, GMT – UTC time will be displayed.

3.5.6 Panes

The **Panes** tab lets you choose which tabs/panes 28 will be visible in the ERA Console.

In the **Visible panes** section, select the panes/tabs you want to be visible at the bottom of ERA Console and click **OK**.

Notes:

- Hidden tab will be also turned to visible after clicking on the related item in the View menu of ERA Console .
- A tab can be hidden directly from the context menu of tabs/panes list by clicking **Hide Tab**.
- It is not possible to hide all the tabs, at least one tab must remain visible.

3.5.7 Other Settings

The **Other settings** pane lets you configure advanced options of ESET ERA Console.

1. Filter settings

Auto Apply Changes – If enabled, filters in individual tabs will generate new outputs each time the filter settings are modified. Otherwise the filtering will only take place after you click **Apply Changes**.

NOTE: If ERA Console has a full-time connection to an ERA Server from the administrator’s PC, we recommend that you select **Show on taskbar when minimized** and leave the console minimized when inactive. If a problem occurs, the systray icon will turn red – which is a signal for the administrator to intervene. We also recommend that you enable **Use highlighted systray icon when problematic clients found** – events triggering the change of the icon color.

Remote administrator updates – This section allows you to check for new versions of ESET Remote Administrator. We recommend that you use the default value (**monthly**). If a new version is available, the ERA Console will display a notification at startup.

2. Other settings

- **Use automatic refresh** – Automatic data refresh in individual tabs on your specified interval.
- **Show gridlines** – Select this option to separate individual cells in all tabs using gridlines.
- **Prefer showing Client as "Server/Name" instead of "Server/Computer/MAC"** – Affects the display mode for clients in some dialog windows (for example, **New task**). This change is visual only.
- **Use systray icon** – ERA Console will be represented by a Windows system tray icon.
- **Show on taskbar when minimized** – If the ERA Console window is minimized, it will be accessible from the Windows taskbar.
- **Use highlighted systray icon when problematic clients found** – Click **Edit** next to this setting to specify events that will trigger a change of the systray icon color.

Note: The systray icon will also change if the ignore list is updated, the default search task is finished, a new client is added or a client is deleted. This does not necessarily happen immediately, there could be a delay of 5-15 seconds plus the time needed to merge (in general the merging happens instantly).

- **Use hostname instead of IP address when executing a Network action** - When executing network actions on a client (described in the Clients tab 29 section), you can select to use a hostname instead of an IP address.
- **Optional information messages** – Disables (**Disable All**) or enables (**Enable All**) all informative messages. If enabled, blue, underlined messages will be displayed in the ERA Console. Click these messages to view hints and tips about how to use the product.

3.6 Display modes

ERAC offers the user two display modes:

- **Administrative mode** – The administrative mode of ERAC gives the user full control over all features and settings, as well as the ability to administer all client workstations connected to it.

- **Read-only mode** – The read-only mode is suitable for viewing the status of ESET client solutions connecting to ERAS; creation of tasks for client workstations, creation of install packages and remote installation are not allowed. The License Manager, Policy Manager and Notification Manager are also inaccessible. Read-only mode does allow the administrator to modify ERAC settings and generate reports.

The Display mode is selected at each console startup in the **Access** drop-down menu, while the password to connect to ERAS can be set for either display mode. Setting a password is especially useful if you want some users to be given full access to ERAS and others read-only access. To set the password, click **Tools** > **Server Options...** > **Security** and click the **Change...** button next to Password for Console (Administrator Access) or (Read-Only Access) or use the User Manager 108 tool.

3.7 ESET Configuration Editor

The ESET Configuration Editor is an important component of the ERAC and is used for several purposes. Some of the most important are the creation of the following:

- Predefined configurations for installation packages

- Configurations sent as tasks or policies to clients

- A general (.xml) configuration file

Configuration Editor is a part of ERAC and is represented mainly by the *cfgedit.** files.

The Configuration Editor allows the administrator to remotely configure many of the parameters available in any ESET security product, especially those installed on client workstations. It also allows the administrator to export configurations to .xml files which can later be used for multiple purposes, such as creating tasks in ERAC, importing a configuration locally in ESET Endpoint Security, etc.

The structure used by the Configuration Editor is an *.xml* template which stores the configuration in a tree-like structure. The template is stored in the *cfgedit.exe* file. That is why we recommend that ERAS and ERAC be updated regularly.

Warning: The Configuration Editor allows you to modify any *.xml* file. Please avoid modifying or rewriting the *cfgedit.xml* source file.

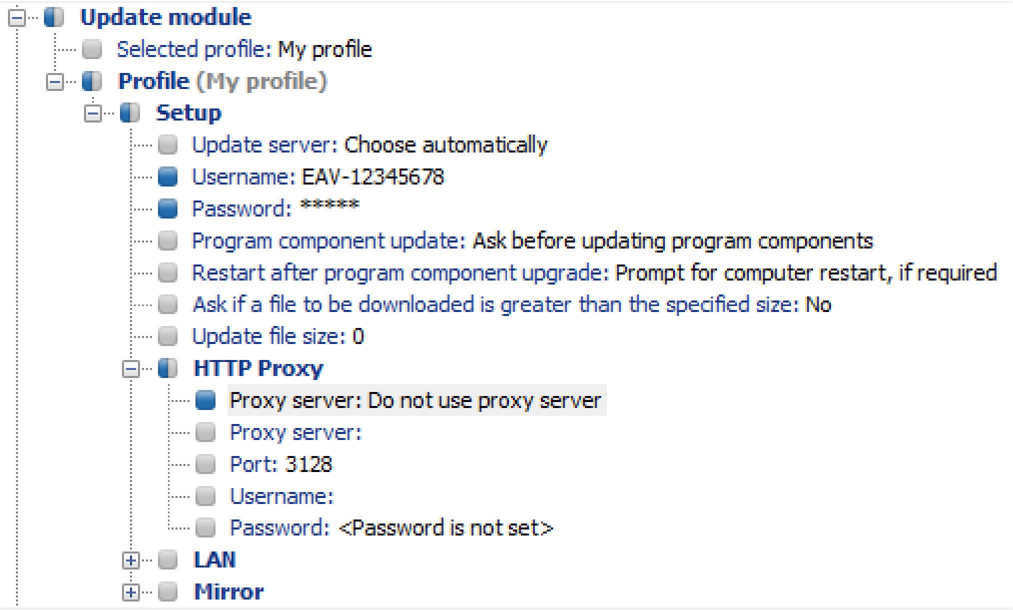
For the Configuration Editor to function, the following files must be available: *eguiHipsRa.dll, eguiHipsRaLang.dll, eguiRuleManagerRa.dll* and *eset.chm.*

3.7.1 Configuration layering

If a value is changed in the Configuration Editor, the change is marked by a blue symbol 🟦. Any entry with the grey icon ⬜ has not been changed and will not be written to the *.xml* output configuration.

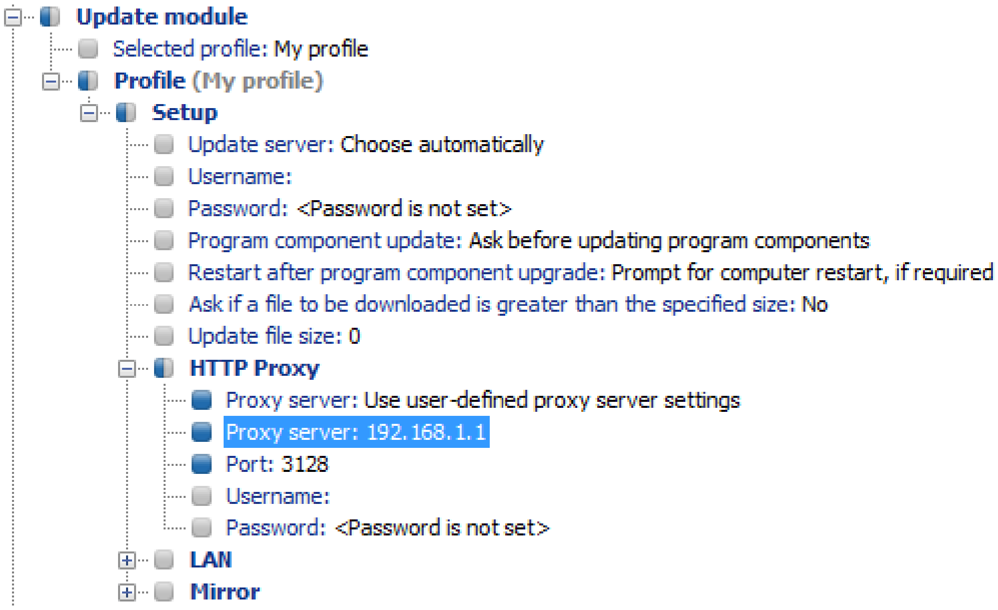
When applying a configuration to clients, only modifications which have been saved to the *.xml* output configuration file will be applied (🟦) All other items (⬜) will remain unchanged. This behavior allows for gradual application of several different configurations without undoing previous modifications.

An example is shown in the figure below. In this configuration the username *EAV-12345678* and password are inserted and using a proxy server is prohibited.



- Update module
  - ⬜ Selected profile: My profile
  - Profile (My profile)
    - Setup
      - ⬜ Update server: Choose automatically
      - 🟦 Username: EAV-12345678
      - 🟦 Password: *****
      - ⬜ Program component update: Ask before updating program components
      - ⬜ Restart after program component upgrade: Prompt for computer restart, if required
      - ⬜ Ask if a file to be downloaded is greater than the specified size: No
      - ⬜ Update file size: 0
      - HTTP Proxy
        - 🟦 Proxy server: Do not use proxy server
        - ⬜ Proxy server:
        - ⬜ Port: 3128
        - ⬜ Username:
        - ⬜ Password: <Password is not set>
      - ⬜ LAN
      - ⬜ Mirror

The second configuration (shown in the figure below) sent to clients will ensure that previous modifications are preserved, including the username *EAV–12345678* and password. This configuration will also allow the use of a proxy server and defines its address and port.



- Update module
  - ⬜ Selected profile: My profile
  - Profile (My profile)
    - Setup
      - ⬜ Update server: Choose automatically
      - ⬜ Username:
      - ⬜ Password: <Password is not set>
      - ⬜ Program component update: Ask before updating program components
      - ⬜ Restart after program component upgrade: Prompt for computer restart, if required
      - ⬜ Ask if a file to be downloaded is greater than the specified size: No
      - ⬜ Update file size: 0
      - HTTP Proxy
        - 🟦 Proxy server: Use user-defined proxy server settings
        - 🟦 Proxy server: 192.168.1.1
        - 🟦 Port: 3128
        - ⬜ Username:
        - ⬜ Password: <Password is not set>
      - ⬜ LAN
      - ⬜ Mirror

3.7.2 Key configuration entries

In this section, we explain several of the key configuration entries for Windows product line v3 and v4:

- **Windows product line v3 and v4** > **ESET Kernel** > **Settings** > **Remote administration**
  Here you can enable communication between client computers and the ERAS (**Connect to Remote Administrator server**). Enter the name or IP address of ERAS (**Primary/secondary server address**). The **Interval between connections to server** option should be left at the default value of five minutes. For testing purposes, this value can be decreased to 0, which will establish a connection every ten seconds. If a password is set, use the one which was specified in ERAS. For more information, see the **Password for Clients** option in the Security tab 107 chapter. Additional information on password configuration can also be found in this section.

- **ESET Kernel** > **Settings** > **License keys**
  Client computers require no license keys to be added or managed. License keys are only used for server products.

- **ESET Kernel** > **Settings** > **ESET Live Grid**
  This branch defines the behavior of the ESET Live Grid Early Warning System, which allows submission of suspicious files for analysis to ESET's labs. When deploying ESET solutions to a large network, the **Submit suspicious files** and **Enable submission of anonymous statistical information** options are particularly important: If these are set to **Do not submit** or **No**, respectively, the ESET Live Grid System is completely disabled. To submit files automatically without user interaction, select **Submit without asking** and **Yes**, respectively. If a proxy server is used with the Internet connection, specify the connection parameters under **ESET Kernel > Setup > Proxy server**.
  By default, the client products submit suspicious files to ERAS, which submits them to ESET's servers. Therefore, the proxy server should be correctly configured in ERAS (**Tools > Server Options > Advanced > Edit Advanced Settings > ERA Server > Setup > Proxy server**).

- **ESET Kernel** > **Settings** > **Protect setup parameters**
  Allows the administrator to password-protect the setup parameters. If a password is established, it will be required in order to access the setup parameters on client workstations. However, the password will not affect any changes to the configuration made from ERAC.

- **ESET Kernel** > **Settings** > **Scheduler / Planner**
  This key contains the Scheduler/Planner options, which allow the administrator to schedule regular antivirus scans, etc.

NOTE: By default, all ESET security solutions contain several predefined tasks (including regular automatic update and automatic check of important files on startup). In most cases, it should not be necessary to edit or add new tasks.

- **ESET Kernel** > **Settings** > **Default user interface values**
  The settings under Default user interface values (i.e., **Show splash screen**/**Don't show splash screen**) only apply modifications to the client's default settings. The client's settings can then be managed on a per-user basis and cannot be changed remotely. To change the setting remotely the **Suppress user settings** option must be set to **Yes**. The **Suppress user settings** option is only available for clients running 4.0 or later ESET security products.

- **Module**
  This branch of the Configuration Editor allows you to define how update profiles are applied. Normally, it is only necessary to modify the predefined profile **My profile** and change the **Update server**, **Username** and **Password** settings. If Update server is set to **Choose Automatically**, all updates will be downloaded from ESET's update servers. In this case, please specify the **Username** and **Password** parameters which were provided at the time of purchase. For information on setting client workstations to receive updates from a local server (Mirror), please see the chapter titled Mirror server 116. For more information on using the scheduler, see chapter Scheduler 155.

NOTE: On portable devices such as notebooks, two profiles can be configured; one to provide updating from the Mirror server and the other to download updates directly from ESET's servers. For more information, see the Combined update for notebooks 157 chapter at the end of this document.

4. Installation of ESET client solutions

This chapter is dedicated to the installation of ESET client solutions for Microsoft Windows operating systems. Installations can be performed directly 61 on workstations, or remotely 46 from ERAS. This chapter also outlines alternative methods of remote installation.

NOTE: Although it is technically feasible, we do not recommend that the remote installation feature be used to install ESET products to servers (workstations only).

Important: Administrators, who use Microsoft Remote Desktop connection to access remote client computers should read following article before remotely installing ESET Smart Security.

4.1 Direct installation

For a direct installation, the administrator must be present at the computer where the ESET security product will be installed. This method requires no further preparation and is suitable for small computer networks or in scenarios where ERA is not used.

You can use a predefined.xml configuration to make direct installation easier. No further modification, such as defining an update server (username and password, path to a Mirror server, etc.), silent mode, scheduled scan, etc., is required during or after installation.

There are differences in applying the .xml configuration format between versions 5.x, 4.x, 3.x and 2.x of ESET client solutions:

- Version 5.x: Apply the same steps as for the Version 4.x.

NOTE: You can install ESET Security products for Linux and Mac using v.5 clients.

- Version 4.x: Download the installation file (for example, *ess_nt32_enu.msi*) from *eset.com* and create your own installation package in the **Installation Packages Editor**. Edit/Select the configuration that you want to associate with this package, click **Copy...** next to the **Package for Windows NT xx bit systems** and save the package as an **ESET Install Msi File With Configuration (*.msi)**.

  NOTE: Adding a configuration to the *.msi* installation file means the digital signature of this file will no longer be valid. In addition, the steps from version 3.x apply to version 4.x as well.

- Version 3.x: Download the installation file (for example, *ess_nt32_enu.msi*) from *eset.com*. Copy the configuration file (*cfg.xml*) to the directory where the install file is located. Upon execution, the installer will automatically adopt the configuration from the *.xml* configuration file. If the *.xml* configuration file has a different name or is located somewhere else, the parameter *ADMINCFG ="path_to_xml_file"* can be used (e.g., *ess_nt32_enu.msi ADMINCFG ="\\server\xml\settings.xml"* to apply the configuration stored on a network drive).

NOTE: If you are installing ESET Smart Security (includes personal firewall) you must allow sharing and remote administration in these solutions. If you do not the network communication between such clients and the ERA Server would be blocked.

4.2 Remote Installation

Remote Installation eliminates the need to pre-install or physically install security products on client computers. ERA offers several methods of remote installation.

Remote installation by means of ERA consists of the following steps:

- Creation of installation packages

  First, check the requirements 62 for remote installation.

  Then, create installation packages 46 which are distributed to the clients.

- Distribution of packages to client workstations (push installation method, logon script, email, upgrade, external solution):

Check/configure your network environment for remote installation.

Distribute the installation packages to clients. There are several methods of remote installation:

Remote Push Install 63. This is the most effective method to distribute security products to your clients.

You can also perform a logon /email remote install 65.

If you do not want to use either of the methods above, you can perform a custom remote install 68.

If some clients have older ESET security products installed you can upgrade them to the latest version, see the chapter upgrade the client 69. If they have the latest version see the chapter avoiding repeated installations 69. To install packages in a large enterprise environment you can see the following chapter 75.

4.2.1 Requirements and limitations

Remote installation requires a correctly configured TCP/IP network that provides reliable client/server communication. Installing a client solution using ERA imposes stricter conditions on the client workstation than a direct installation. The following conditions should be met for remote installation:

Windows

- Microsoft network client enabled
- File and printer sharing service enabled
- File sharing ports (445, 135 – 139) are accessible
- Administrative share ADMIN$ enabled
- Administrator username and password exists for client workstations (username cannot be left blank)
- Simple file sharing disabled
- Server service enabled

NOTE: Recent versions of Microsoft Windows (Windows Vista, Windows Server 2008 and Windows 7) use security policies limiting local user account permissions so that the user may not be able to execute specific network operations. If your ERA service is running on a local user account, push installation issues may occur in certain specific network configurations (for example, when installing remotely from a domain to a workgroup). When using Windows Vista, Windows Server 2008 or Windows 7, we recommend that you only run the ERA service on accounts with sufficient networking rights. To specify the user account on which you want to run ERA, navigate to **Start** > **Control Panel** > **Administrative Tools** > **Services**. Select the ESET Remote Administrator Server service from the list and click **Log On**. ESET Remote Administrator 5 embeds this setting in the Advanced installation scenario so you must select **Advanced** → **Fully customized installation** during installation.

Important: If you are using the **Window push** installation method on Windows Vista, Windows Server 2008, or Windows 7 target workstations, make sure that your ERA Server as well as the target workstations are in a domain.If the ERA Server and the target computer are not in a domain you must disable UAC (User Access Control) on the target computer. To do so, click **Start** > **Control Panel** > **User Accounts** > **Turn User Account control on or off**. Alternatively, you can open the Msconfig utility (click **Start**, type **Msconfig** into the search field and press **Enter**) and then click **Tools** and select **Disable UAC (requires reboot)**.

We highly recommend that you review requirements before installation, especially if there are multiple workstations in the network:
In the **Remote Install** tab select the **Computers** tab, select the relevant client(s), click **New Installation Task**, select **Windows push**, select **Diagnostics**, click **Continue**, set the Logon Information 68 of selected client(s) by clicking **Set for All...** or by clicking **Set Credentials...** (after selecting a specific client in the **Computers Logon Settings** window), click **Next** and click **Finish**.

Remote installation for Linux/MAC Security products is not supported on Windows 2000.

Important: Administrators who use Microsoft Remote Desktop connection to access remote client computers should read the following article before remotely installing ESET Smart Security.

4.2.1.1 Requirements for Linux/Mac Push install

Make sure that all client workstations are configured correctly before you perform a remote installation.

Linux

1. Computer must be able to connect to the server via SSH
2. SSH Account must have admin rights - This means that you need to execute the installation under the root user (UID=0) or a user that has sudo rights.

Mac

1. Computer must be able to connect to the server via SSH
2. SSH Account must have admin rights - This means that you need to execute the installation under a user that is an administrator.

Note: This feature is supported by ESET NOD32 Antivirus Business Edition for Mac OS X 4.1.94 and ESET NOD32 Antivirus Business Edition for Linux Desktop 4.0.79 and all later versions for both platforms.

4.2.1.2 WMI Requirements

WMI remote installation method requires the following:

- On the target computer, WMI must be enabled and started. It is enabled by default.
- User account used for remote connection must have administrative privileges.
- WMI connection must be allowed in the firewall on the target computer - it requires the port 135 to be enabled for DCOM (Distributed Component Object Model) for incoming connections. Also, one of the ports above 1024 (usually 1026-1029) must be enabled.

  Default Windows firewall can be configured by executing the following command on the target machine:

  ```
  netsh firewall set service RemoteAdmin enable
  ```
- Account for connecting to the remote computer should be a domain account and must have local Adminstrator privileges.

  WMI can also be used if the account is a local account, but on the remote system User Account Control (UAC) should be disabled.

For more information see http://msdn.microsoft.com/en-us/library/aa826699%28v=vs.85%29.aspx

4.2.2 Remote Push Install

Remote installation pushes ESET client solutions to remote computers. Push installation is the most effective installation method, and requires that all target workstations be online. Before starting a push installation, download the .msi install files for ESET Endpoint Security or ESET Endpoint Antivirus from the ESET website and create an installation package. You can create an .xml configuration file that will automatically be applied when the package runs. Please see Requirements 62 prior to installation.

To initiate a push installation from the **Remote Installation** tab, follow the steps below:

1. Once computers targeted for remote installation are listed in the **Computers** tab, select all or some of them and click **New Installation Task...** to open the New Installation Task 71 window. Leave the **Windows push** and **Install** settings selected click **Continue**.
2. Set the logon information for computers in the list (Click **Set Credentials...** to set the credentials of the highlighted/selected computer, use **Set for All...** to apply the credentials to all the computers in the list). This

must be done while using an account with administrator rights. You can still add clients to the list in this step by using the **Add Clients Special** feature.

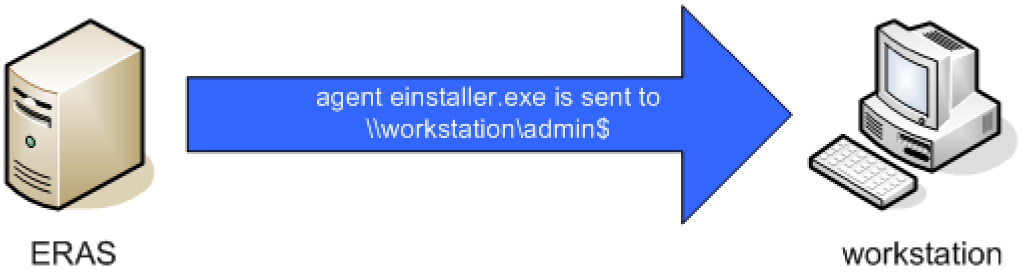
3. Select the desired installation package 46 to deliver to target workstations.
4. Set the time when the task is to be run and click **Finish**.

You can view the push installation task status in the Installation History 54 tab. For details of diagnostic results, select the desired task and press **F4**. The **Properties** window shows up in the **Details** tab, where you can view remote install diagnostics results by clicking **View All Logs/View Selected Logs**.

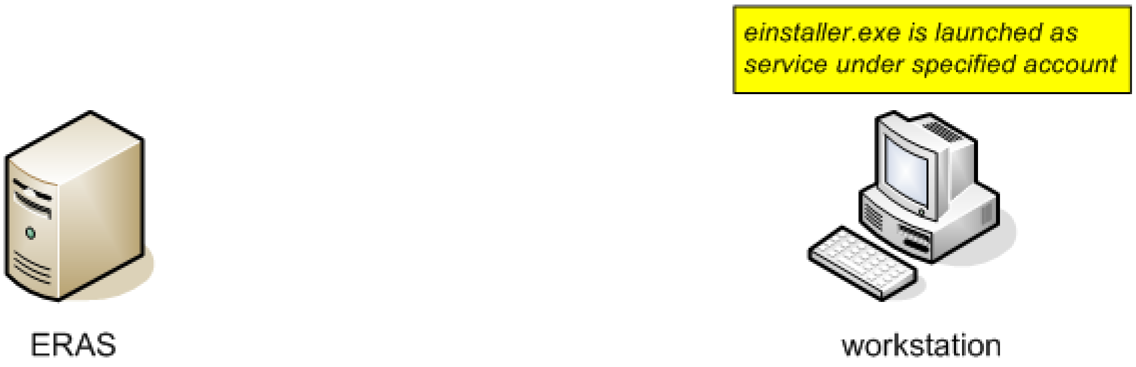
NOTE: The maximum number of concurrent push installation threads is set to 20 by default. If you send a push installation task to a number of computers exceeding this limit, the additional computers will be put into queue and will wait for the threads to be free. We do not recommend increasing this value for performance reasons; however if you consider it necessary you can change the limit in the Configuration Editor (**ESET Remote Administrator** > **ERA Server** > **Setup** > **Remote Install**).

Details of the remote installation process are described below:

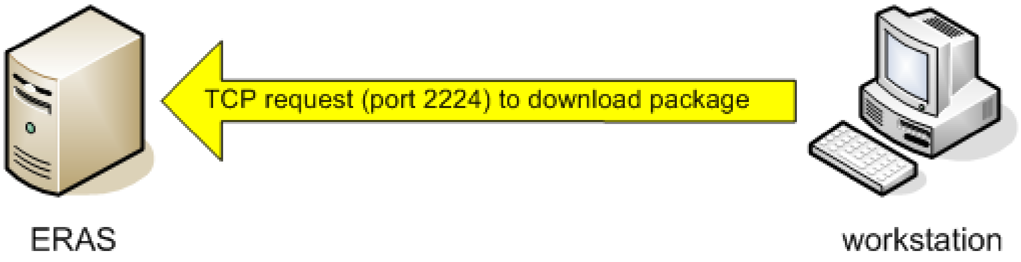
5. ERAS sends the *einstaller.exe* agent to the workstation with the help of the administrative share admin$.



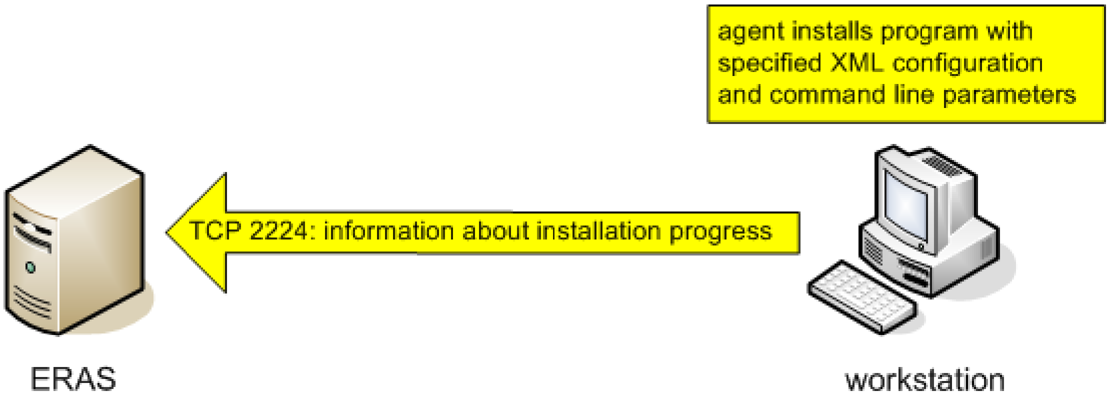
6. Agent starts as a service under the system account.


einstaller.exe is launched as service under specified account
ERAS
workstation

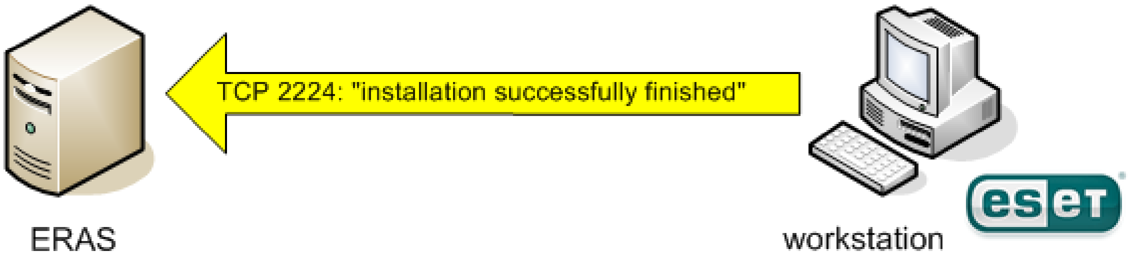
7. Agent establishes communication with its ”parent” ERAS and downloads the corresponding install package on TCP port 2224.



8. Agent installs the package under the administrator account defined in step 2; the corresponding *.xml* configuration and command line parameters are also applied.


agent installs program with specified XML configuration and command line parameters
TCP 2224: information about installation progress
ERAS
workstation

9. Immediately after the installation is complete, the agent sends a message back to ERAS. Some ESET security products require a reboot and will prompt you if necessary.



4.2.3 Logon / email remote install

The logon and email remote installation methods are very similar. They only vary in the way that the *einstaller.exe* agent is delivered to client workstations. ERA allows the agent to run via logon script or via email. The *einstaller.exe* agent can also be used individually and run via other methods (for more information, see the chapter Custom remote install 68).

The logon method works well for notebooks that are often used outside the local network. Installation is performed after they log onto the domain.

While the logon script runs automatically when the user logs on, the email method requires intervention on the part of the user who must launch the einstaller.exe agent from an email attachment. If launched repeatedly, einstaller.exe will not trigger another installation of ESET client solutions. For more information see chapter Avoiding repeated installations 69.

For a step-by-step guide on how to export the ESET Installer to Folder / Logon Script or how to send it via e-mail, see this chapter 66.

Remote installation of ESET Security Products for Android

Important: Before you proceed, read this chapter 89 first.

1. Click the **New Installation Task...** button in the Remote Install tab of ERA Console, select **Android** and click **Continue**.
2. Click the **...** button near the **Attachment** field, then browse for the location where you saved your ESET Security product for Android (*.apk* file), select that application and click **OK**.
3. Enter the email address of the user, review or edit the information in the **Subject** and **Description** fields and click the **...** button next to the configuration link (right under the description field). This will open the **Configuration Link Settings** window, where you can configure how the product connects to ERA.

Note: This link will configure the ESET Security product for Android, which needs to be installed (You can send a link with the installation file to the user, or you can send the application directly, as described in Step 1).

4. The **Server** and **Port** fields are predefined based on your current ERA Server. If there is a password required for

the users to connect to the server, type it into the **Password** field. Otherwise, you can leave this field blank. If you use a password, the **Add current SIM as trusted** option must be selected. It is selected by default to prevent the mobile phone from being locked when trying to connect to the ERA Server. These basic settings will be sent to the client. For advanced settings (such as the update **Username** and **Password**), the client needs to be connected to the ERA Server and you can distribute these settings using a Policy 84.

4.2.3.1 Export ESET Installer to Folder / Logon Script

You can use a text editor or other proprietary tool to insert the line calling *einstaller.exe* into the logon script. Similarly, *einstaller.exe* can be sent as an email attachment using any email client. Regardless of the method used, make sure you are using the correct *einstaller.exe* file.

For *einstaller.exe* to launch, the currently logged in user does not necessarily have to be an administrator. The agent adopts the required administrator username/password/domain from ERAS. For more information, see the end of this chapter.

Enter the path to einstaller.exe in the logon script

1. Select an entry in the **Remote Install** tab and click **New Installation Task**, select **Export** and click **Continue** to proceed to the **Export Type** screen.

2. At the **Export Type** screen the following options are available:

- **Export to Folder for Windows** - This option is suitable if you want to distribute the *einstaller.exe* to computers used by users that have no administrative privileges. The administration logon credentials will be obtained from the ERA server when the installer connects to it, unless the *einstaller.exe* is run by a user with administrative privileges.

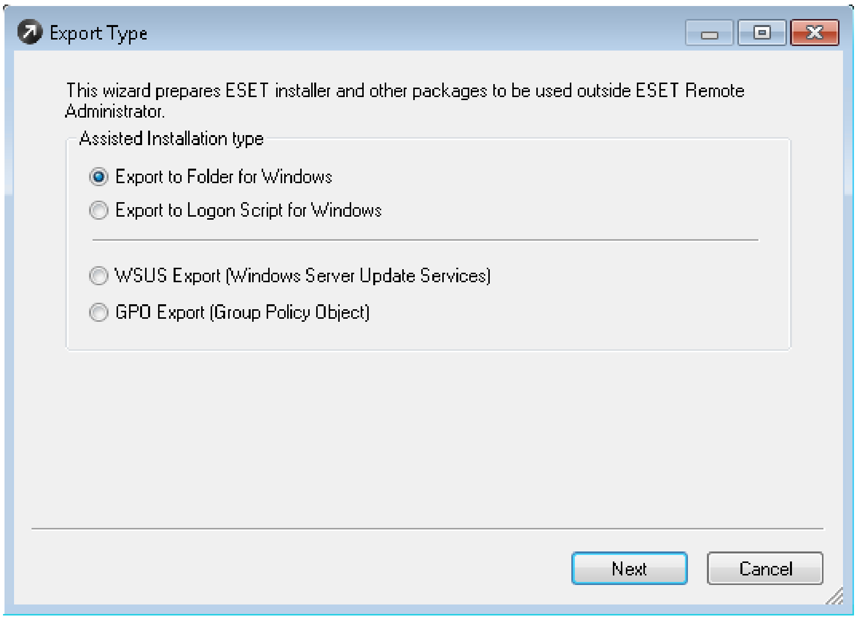
- **Export to Logon Script for Windows** - It is the same as **Export to Folder for Windows**, but in the **Finished** screen you obtain the link to the export folder so that it can be used in the logon script of computers to be managed.

- **WSUS Export (Windows Server Update Services)** - The option downloads the complete installation package you select in the next step as an executable **.msi* installation file and the installation package might be distributed to the desired computers as part of WSUS.

- **GPO (Group Policy Object)** - The option downloads the complete installation package you select in the next step and the installation package might be distributed to the desired computers via GPO.

3. Click browse (**...**) next to **Folder** in the **Export Folder** section to select the directory where the *einstaller.exe* file (or the *.msi installer) will be exported (if **Export to Logon Script for Windows** is selected), and then click **Next**.

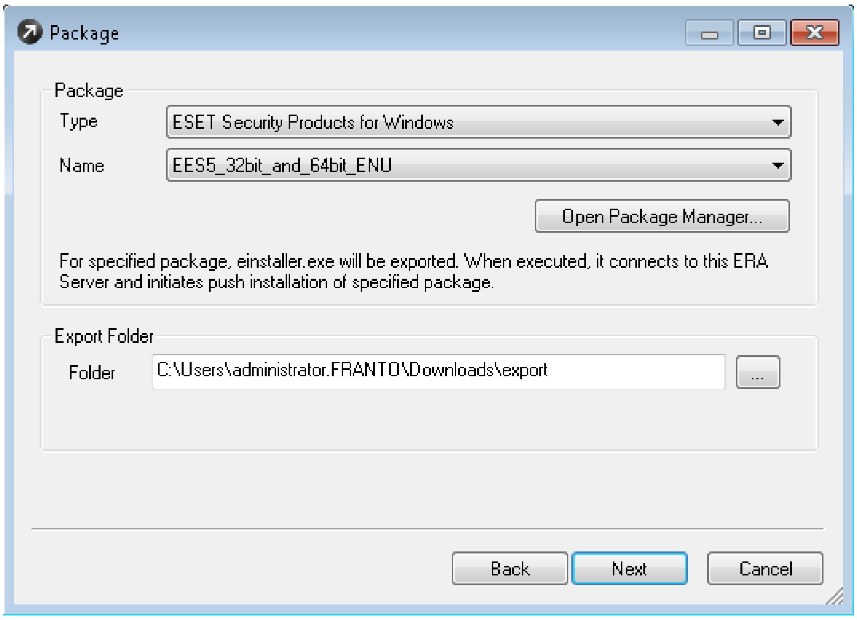
4. At this point you end up on the **Finished** step.



This wizard prepares ESET installer and other packages to be used outside ESET Remote Administrator.

Assisted Installation type

● Export to Folder for Windows
○ Export to Logon Script for Windows
○ WSUS Export (Windows Server Update Services)
○ GPO Export (Group Policy Object)



Package

Type: ESET Security Products for Windows

Name: EES5_32bit_and_64bit_ENU

For specified package, einstaller.exe will be exported. When executed, it connects to this ERA Server and initiates push installation of specified package.

Export Folder

Folder: C:\Users\administrator.FRANTO\Downloads\export

Attaching the agent (einstaller.exe) to email

1. Click **New Installation Task...** in the **Remote Install** tab, select **Email** and then click **Continue**.

2. Select the **Type** and name of the **Package** you want to install and then click **Next**.

Note: To uninstall ESET security products from the user's computer, select **Uninstall ESET Security Products for Windows and NOD32 version 2** from the **Type** drop-down menu.

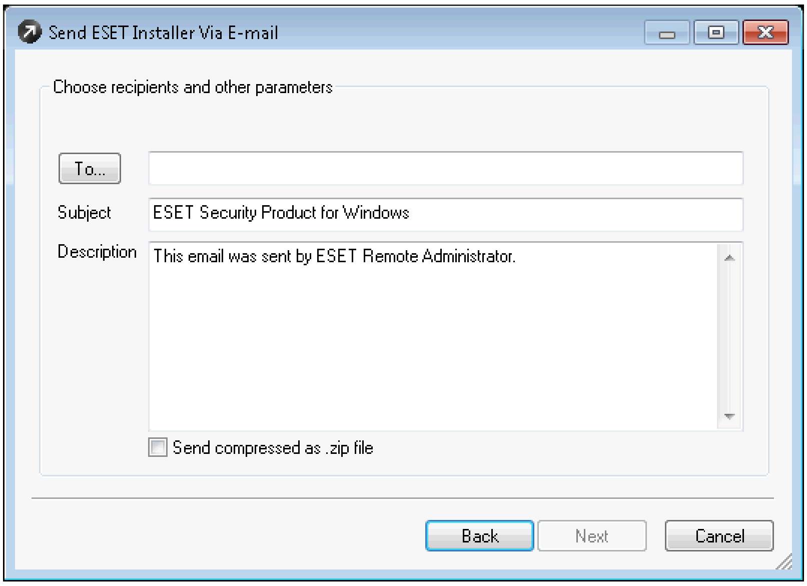
3. Click **To...** to select addresses from the address book (or insert individual addresses).

4. Enter a **Subject** in the corresponding field.

5. Enter a message in the **Body**.

6. Select the check box next to **Send compressed as .zip file** if you want to send the agent as a zipped package.

7. Click **Send** to send the message.



Choose recipients and other parameters

Subject: ESET Security Product for Windows

Description: This email was sent by ESET Remote Administrator.

□ Send compressed as .zip file

During the remote installation process, reverse connection to ERAS takes place and the agent (*einstaller.exe*) adopts settings from the Default Logon 68 information you defined in the **Settings** 73 window (the window shows up after clicking the **Settings...** button visible in the **New Installation Task** window if the **Email** option is selected).

The account under which the installation of the package is to be performed must be an account with administrator rights or, preferably, a domain administrator account. Values inserted in the **Default Logon...** dialog window are forgotten after each service (ERAS) restart.

4.2.3.2 Default Logon / Logon Information

The **Default Logon** or **Logon Information** window lets you set the user credentials and domain information required to access your client computer on the network and manage the ESET product installed.

The required client data are:

- **User name**
- **Password**
- **Domain/Workgroup**

After you enter the data, press **Set Logon** (in the **Default Logon** window) or **OK** (in the **Logon Information** window) to save the information on the server.

NOTE: Please note that this information will only remain stored on the server until the next server restart.

NOTE: If you see the *The logon information is already stored on the server* message in the **Default Logon** window, the settings have already been stored on the server. If you want to change the stored settings, click **Overwrite** and continue setting up the new logon information.

4.2.4 Custom remote install

It is not a requirement that you use ERA tools to remotely install ESET client solutions. Regardless of the method you use, you must distribute the *einstaller.exe* file to client workstations.

For *einstaller.exe* to launch, the user currently logged in does not necessarily have to be an administrator. The agent adopts the required administrator username/password/domain from ERAS. For more information, see the end of this chapter.

The *einstaller.exe* file can be obtained as follows:

- In the **Computers** tab (in the **Remote Install** tab), click **New Installation Task...,** select **Export** and then click **Continue.**
- Select **Export to Folder for Windows** and click **Next**. Select the **Type** and **Name** of the **Package** to be installed.
- Click browse (**...**) next to **Folder**, select the directory where *einstaller.exe* will be exported and click **Select Folder**.
- Click **Next** to export the *einstaller.exe* file and then click **Finish**.
- Use the extracted *einstaller.exe* file.

NOTE: The *"Direct installation* 61 *with predefined XML configuration"* method can be used in situations where it is possible to provide administrator rights for the installation. The *.msi* package is launched using the */qn* parameter (versions 5.x, 4.x, 3.x). These parameters will run the installation without displaying a user interface.

The username and password of the account under which the installation of the package is to be performed must be an account with administrator rights or, preferably, a domain administrator account.

During the remote installation process the Agent connects to ERAS adopts settings from the **Default Logon** 68 option.

If the *einstaller.exe* agent is started manually on a target workstation, the remote installation is handled in the following way:

- The *einstaller.exe* agent sends a request to ERAS (TCP port 2224).
- ERAS starts a new push installation (with a new agent) of the corresponding package (sent via the share *admin$*). The agent waits for an answer from ERAS (sending the package via the share *admin$*). In the event that no answer arrives, the agent will attempt to download the install package (via the TCP/IP port 2224). In this case, the

administrator username and password specified in **Default Logon** 68 option on the ERAS is not transferred and the agent attempts to install the package under the current user. On the operating systems Microsoft Windows 9x/ Me, the administrative share cannot be used, therefore the agent automatically establishes a direct TCP/IP connection to the server. The new agent then starts downloading the package from ERAS via TCP/IP protocol.

The installation of the package is launched, applying the associated .xml parameters under the account defined in ERAS (the **Default Logon** 68 option).

4.2.5 Windows Upgrade Client

This type of installation is designated for clients with ESS/EAV version 4.2 and later. Beginning with version 4.2, a new upgrade mechanism was implemented that allows ERA to initiate the upgrade process on the client side without the need of the *einstaller.exe* agent. This mechanism works in a manner similar to the program component update, or PCU, which upgrades clients to a newer version of the program. For version 4.2 and later ESS/EAV clients, we strongly recommend this type of upgrade.

NOTE: If a custom configuration file has been defined for the installation package it will be ignored during the upgrade.

The **Windows Upgrade Client** option of **New Installation Task** command allows you to remotely upgrade a client/ group of clients.

1) Click the **Add Clients Special** button in the first step if you want to use the selection tool to choose which clients to upgrade. After you finish making your selections click **Next** to continue.

NOTE: Clicking **Add Clients Special** opens a new window in which you can add clients by server (in the **Servers** section) or by group (in the **Groups** section).

2) In the **Task settings** window you can:

- use the respective pull-down menus to select the the **Name** of an ESET product package that will be used to upgrade your client(s). Alternatively you can open the Package Manager 46 to modify the existing packages.
- change the default name and description of your upgrade task, select **Apply task** now if you want the task to execute immediately or **Apply task later** if you want to setup a later date for the task execution.

3) Click **Finish** to complete the configuration of your upgrade client task.

NOTE: This task works only on clients that connect directly to the primary server. Clients from replicated servers will be ignored.

4.2.6 Avoiding repeated installations

Immediately after the agent successfully completes the remote installation process, it marks the remote client with a flag prohibiting repeated installations of the same installation package. The flag is written to the following registry key:

HKEY_LOCAL_MACHINE\Software\ESET\ESET Remote Installer

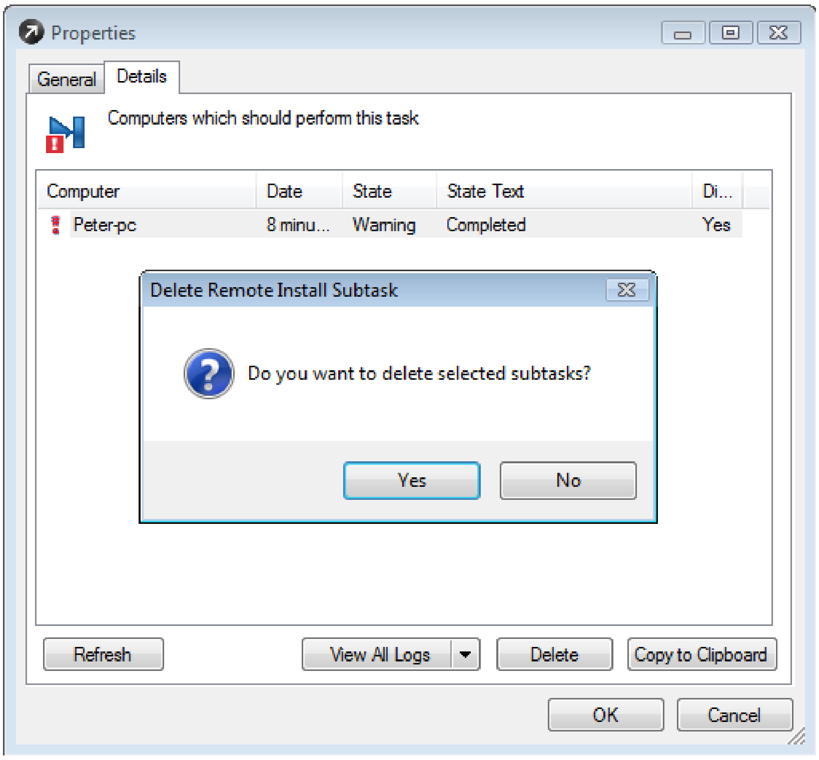
If the Type and Name of the package defined in the *einstaller.exe* agent match the data in the registry, the installation will not be performed. This prevents repeated installations from targeting the same workstations.

NOTE: The remote push install method ignores this registry key.

ERAS provides an additional feature to prevent repeated installations that activates when the installer establishes backward connection to ERAS (TCP 2224). If the installation has been successfully completed any additional installation attempts will be denied.

The agent records the following error to the installer log located in *%TEMP%\einstaller.log*:

Eset Installer was told to quit by the server 'X:2224'.


Properties

General | Details

Computers which should perform this task

Computer	Date	State	State Text	Di...
Peter-pc	8 minu...	Warning	Completed	Yes

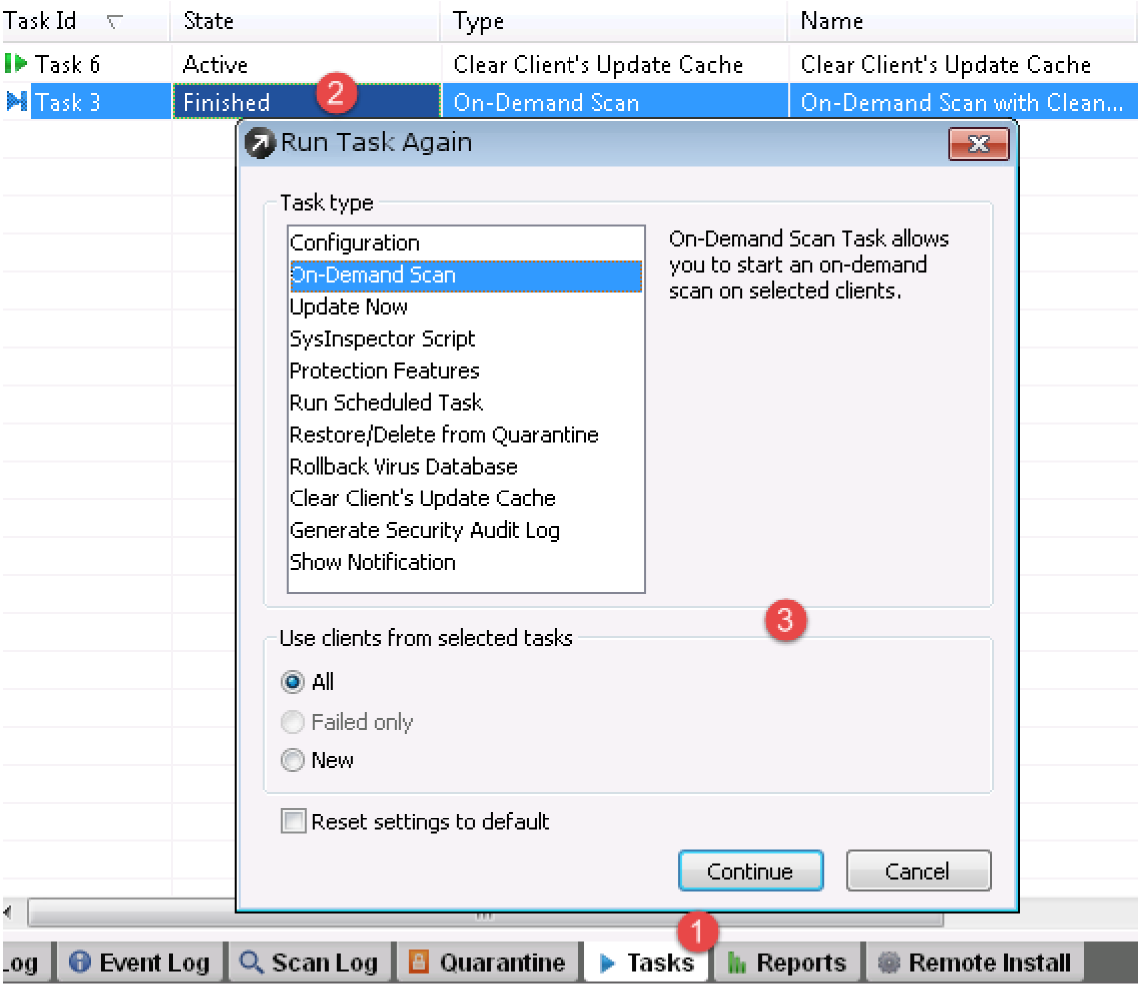
Delete Remote Install Subtask

Do you want to delete selected subtasks?

To prevent repeated installations from being denied by ERAS the related entries in the **Remote Install Task details** tab must be removed. To delete an entry, select it, click on the **Delete** button and confirm by pressing **Yes**.

4.2.7 Run Task Again

Any task initiated from the **Clients** tab by right-clicking a client and selecting **New Task** from the context menu can be found in the **Tasks** tab. Any of these tasks can be run again by right-clicking the desired task and selecting **Run Task Again...** from the context menu.



Task Id	State	Type	Name
Task 6	Active	Clear Client's Update Cache	Clear Client's Update Cache
Task 3	Finished	On-Demand Scan	On-Demand Scan with Clean...

Run Task Again

Task type

- Configuration
- On-Demand Scan
- Update Now
- SysInspector Script
- Protection Features
- Run Scheduled Task
- Restore/Delete from Quarantine
- Rollback Virus Database
- Clear Client's Update Cache
- Generate Security Audit Log
- Show Notification

On-Demand Scan Task allows you to start an on-demand scan on selected clients.

Use clients from selected tasks

● All
○ Failed only
○ New

□ Reset settings to default

The **Run Task Again** window presents several options:

- Click **continue** to continue to the original dialog window of the task to be run.
- select the clients to which the task to be run should apply (**All** - all clients involved in the task previously, **Failed only** - the clients for which the task failed previously, **New** - the clients you would select in one of the subsequent dialog windows).
- select a different task to be run.
- **Reset settings to default** - if you modified the default settings of a task you ran previously, you can select **Reset settings to default** to have the task run again using default settings.

4.2.8 New Installation Task

After clicking **New Installation Task...** from the **Remote Install** tab, select the Remote installation 63 type you want to use from the following options:

- **Windows push** - Executes remote installation of ESET client solutions on selected remote computers as a service. The installation method requires local administration credentials to push the installation agent to the target computer. Remote computers must have network sharing enabled and be online.
- **Windows push (WMI)** - New feature in ESET Remote Administrator 5.3, which locates and executes an installation package located on a network share defined in the task details 73.
  What is WMI (Windows Management Instrumentation manual on MSDN)?

- **Windows upgrade client** - The most reliable way to upgrade ESET antivirus solutions (version 4.2 and later) on managed workstations. No administrator credentials are required, but the remote computer must have network sharing enabled.

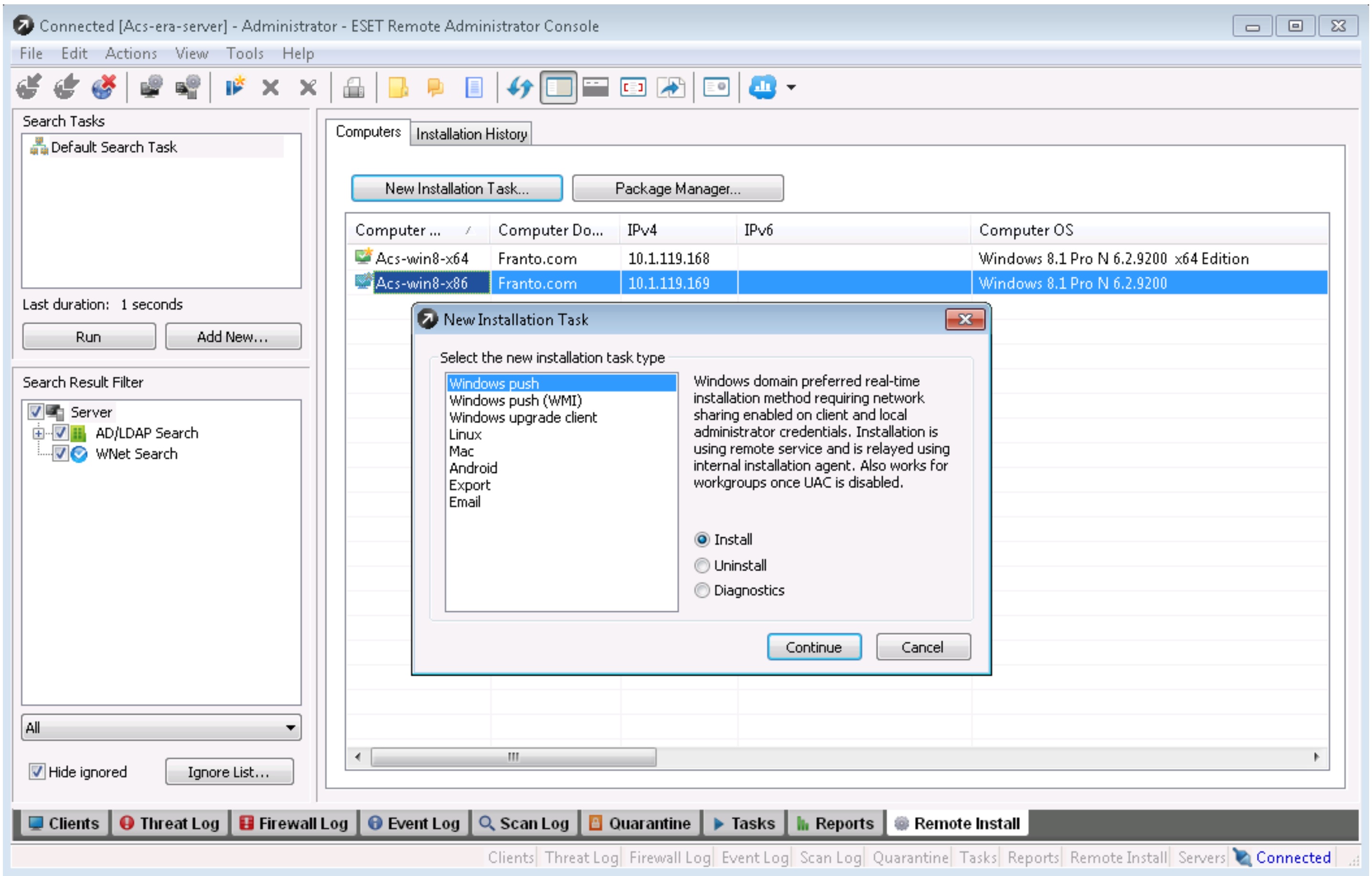
- **Linux** - Command-line installation of ESET client solutions on most Linux distributions with enabled SSH access.

- **Mac** - Command-line installation of ESET client solutions on computers with the Mac OS X operating system with SSH access allowing execution of installation package.

- **Android** - Send easy-to-follow download instructions to Android-powered devices and enable single-click enrollment.

- **Export** - Export 66 the desired package as executable installer (*einstaller.exe* file) in order to deploy ESET client solutions on computers outside ESET Remote Administrator. If you want to use the WMI method with the exported installer, click **Settings...** and select this export method prior to proceeding with the export 66.

- **Email** - The ERA Agent installer will be sent to users in an email 67 with instructions to complete installation.



Connected [Acs-era-server] - Administrator - ESET Remote Administrator Console

Computer ...	Computer Do...	IPv4	IPv6	Computer OS
Acs-win8-x64	Franto.com	10.1.119.168		Windows 8.1 Pro N 6.2.9200 x64 Edition
Acs-win8-x86	Franto.com	10.1.119.169		Windows 8.1 Pro N 6.2.9200

New Installation Task

Select the new installation task type

Windows push
Windows push (WMI)
Windows upgrade client
Linux
Mac
Android
Export
Email

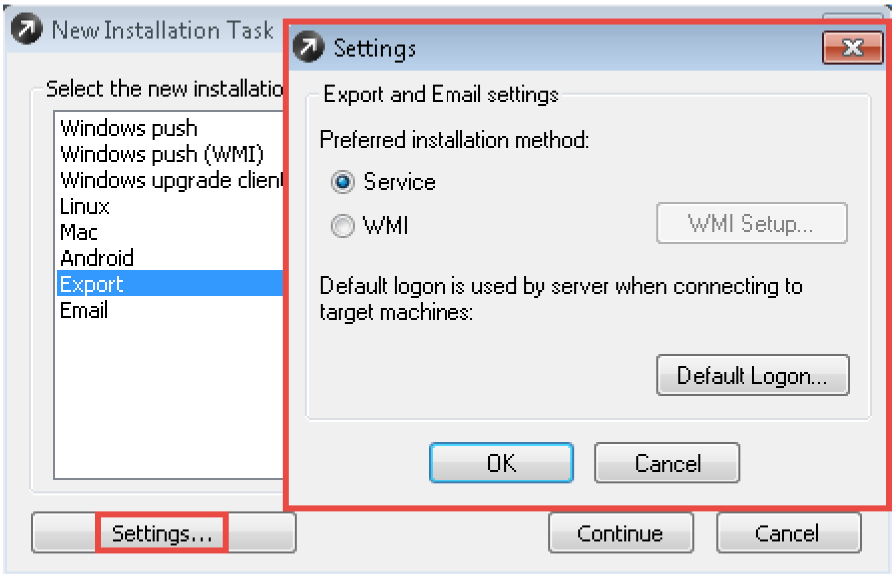
Windows domain preferred real-time installation method requiring network sharing enabled on client and local administrator credentials. Installation is using remote service and is relayed using internal installation agent. Also works for workgroups once UAC is disabled.

● Install
○ Uninstall
○ Diagnostics

Last duration: 1 seconds

4.2.8.1 Additional settings

When you choose the **Export** 66 or **Email** 66 method when initiating a **New Installation Task** 71, you can click **Settings** to configure additional options.



Preferred installation method:

● Service

○ WMI

Default logon is used by server when connecting to target machines:

Preferred installation method

- **Service** - This method is selected by default even if you do not access the **Settings** dialog.
- **WMI** - Select this method if you want the installer to be available through WMI for the target computers and click **WMI Setup...** to proceed to **Configure Installer Sharing** 73.

Default logon... 68 - Setting up username and password for a Windows NT-based system.

4.2.8.2 Configure Installer Sharing

If you want to execute a **Windows push (WMI)** installation 71 or if you choose the **Email** or **Export** option in the **New Installation Task** window and select **WMI** as your **preferred installation method**, you must define the access details of the shared location by clicking **WMI Setup...**

After clicking **WMI Setup...** the **Configure Installer Sharing** window will be displayed. Follow the steps below to configure installer sharing:

1. Click **Export...** to browse to your desired export folder (shared location).

2. Click **Credentials** to set the access credentials for the selected shared location. The **Access Credentials** window will be displayed.

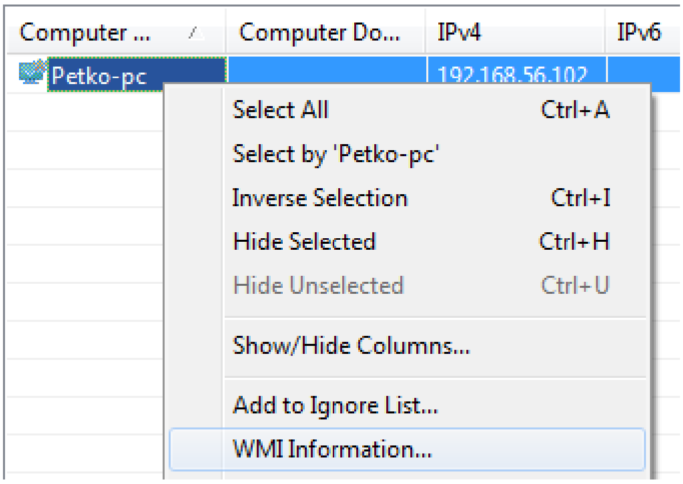
You can use environment variables in the path to shared location (if local file is selected) if they are configured in the operating system.

Note: Even if a shared location is used to distribute the installation package, the target computer still needs TCP/IP visibility of ERA Server.

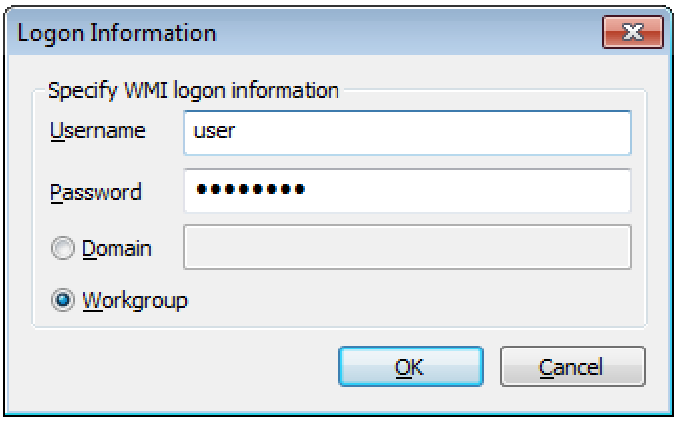
4.2.8.3 WMI Information

To display and edit the WMI information of a managed computer, follow the steps below:

1. Right-click a computer and select **WMI Information...** from the context menu.



2. Specify **WMI logon information** and click **OK**.



Username: user

Password: •••••••••

○ Domain

● Workgroup

3. Wait until the information is downloaded from the computer to the ERA Console.

4. WMI information should be displayed after a few seconds.

4.2.8.4 WSUS Export

If you want some ESET client solutions to be installed as part of **WSUS (Windows Server Update Services)** you can export 66 the installer package from ERA Server 5.3 while with **WSUS Export (Windows Server Update Services)** enabled.

Detailed information on installation and configuration of **WSUS** is available as a step-by-step guide at https://technet.microsoft.com/en-us/library/dd939822(v=ws.10).aspx

WSUS only distributes packages signed by a certificate that is installed on the WSUS server. You can generate this certificate using Local Update Publisher (*LUP*). Use the Certificates MMC Snap-in to install the certificate on the WSUS server.

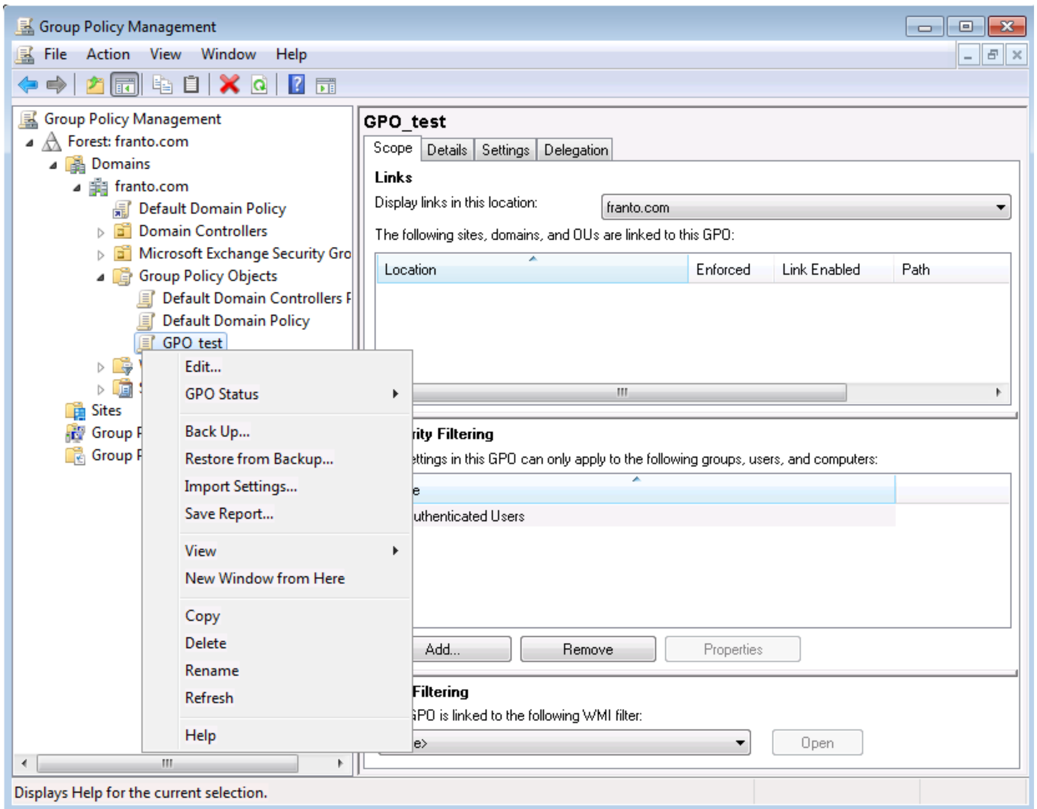
Add both the exported 66 installer *.msi* file and the configuration *.xml* file to the package created by *LUP* and approve the package in *LUP*. With these steps complete, the approved package should be delivered as part of Windows Updates.

4.2.8.5 GPO Export

If you want to deploy ESET client solutions as part of Group Policy Software Installation in Active Directory in a domain environment, you can export 66 the installer package from ERA Server 5.3 while choosing the **GPO Export (Group Policy Object)** option. Copy the exported *.msi* installer and *.xml* configuration file to a shared folder (with read access) available to the target computers to be managed by a common GPO.

Create a new GPO in or link an existing GPO to the desired Active Directory Organization Unit in the Group Policy Management Console.

1. Right-click your GPO and click **Edit...**



Display links in this location: franto.com

The following sites, domains, and OUs are linked to this GPO:

ttings in this GPO can only apply to the following groups, users, and computers:

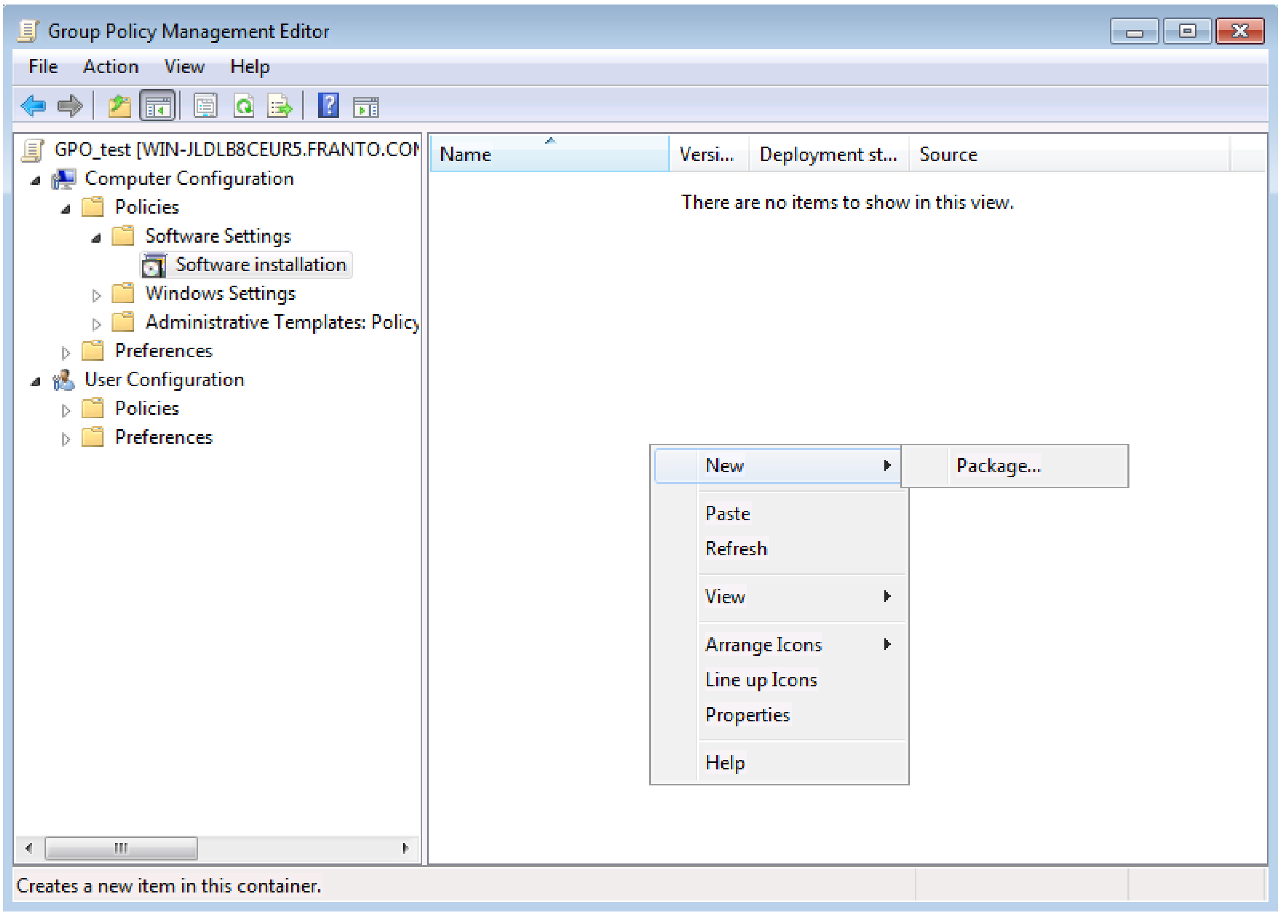
uthenticated Users

PO is linked to the following WMI filter:

e>

Displays Help for the current selection.

2. In the **Group Policy Management Editor** window under *Computer Configuration* (or User Configuration) > *Policies* > *Software Settings* > *Software Installation* right-click the blank area, select **New** and click **Package...**



3. Browse to the *.msi* installer you copied into the shared folder.

4. Type the network path to the *.msi* installer you copied to the shared folder and then select one of the following deploy methods

   a. **Assign** - install the software

   b. **Publish** - offer the software in Add/Remove programs (User-assigned GPO's only)

   c. **Advanced** - to configure the Assigned or Published options, and to apply modifications to the package

5. Administering client computers

5.1 Tasks

Client workstations that are correctly connected to ERAS and displayed in ERAC can be configured and administered using various types of tasks.

Stage I - **New Task**.

1) To apply a task to one or more client workstations, select and right-click the workstations in the **Clients** pane to open the Context menu 27.

2) Click **New Task** and select the type of task you want to perform.

NOTE: Alternatively, the task wizard can be opened from the ERAC main menu by clicking **Actions > New Task**.

Stage II - Select one of the following tasks:

- Configuration Task 78
- On-demand Scan (Cleaning Disabled/Cleaning Enabled) 78
- Update Now 79
- SysInspector Script Task 79
- Protection Features 79
- Run Scheduled Task 80
- Restore/Delete From Quarantine Task 80
- Rollback Virus Database 80
- Clear Client`s Update Cache 81
- Generate Security Audit Log 81
- Show Notification 81

3) Select your desired task and perform the task-specific actions described in each of the following chapters.

Stage III - **Select Clients**

4) You can modify your client selections in the **Select Clients** window, which will appear once you have set up the task. You can refine your client selection by adding clients from the **All items** client overview tree (left half of the window) to the **Selected items** list (right half of the window) or by removing the client entries that are already on the list.

   NOTE: Click **Add Special ...** to open a new window in which you can add clients from the **Clients pane** or add clients by **Server** and/or **Groups**.

Stage IV - Finishing the Task 81.

The following sub-chapters outline the individual task types for client workstations. An example scenario is given for each task type.

NOTE: The **ERA Update Check** window will pop up when the specified time interval elapses or when a new product version is available. To download the latest product update from ESET's website, click **Visit Update Web Site**.

All tasks available in the **Tasks** tab can be run again by right-clicking the desired task (or multiple selected tasks) and choosing **Run Task Again...** from the context menu. The **Run Task Again** wizard is similar to the **New Task** wizard. Click **Continue** to proceed to the next screen or alter the task to be run prior to clicking **Continue**.

Every task you run again will generate a new record (row) in the **Tasks** tab.

5.1.1 Configuration Task

Configuration tasks are used to modify protection settings on client workstations. These tasks are delivered to client workstations in configuration packages which contain the modification parameters. The *.xml* files created in the ESET Configuration Editor or exported from clients are also compatible with configuration tasks. The example below demonstrates how to create a configuration task that changes the username and password on target computers. Any switches and options not used in this example will follow at the end of this chapter.

First, designate the workstations to which the task is to be delivered. Mark those workstations in the **Clients** pane in ERAC.

1) Right-click any of the selected workstations and select **New Task** > **Configuration Task** from the context menu.
2) The **Configuration for Clients** window will open, which serves as a configuration task wizard. You can specify the source of the configuration file by clicking **Create...**, **Select...**, or **Create from Template...**
3) Click the **Create** button to open the ESET Configuration Editor and specify the configuration to be applied. Navigate to **Windows product line v3 and v4** > **Update module** > **Profile** > **Settings** > **Username** and **Password**.
4) Insert the ESET-supplied username and password and click **Console** on the right to return to the task wizard. The path to the package is displayed in the **Create/Select configuration** field.
5) If you already have a configuration file that contains the desired modifications, click **Select**, find the file and assign it to the configuration task.
6) Alternatively, you can click **Create from Template**, select the *.xml* file and make changes if needed.
7) To view or edit the configuration file that you have just created or edited, click the **View** or **Edit** buttons.
8) Click **Next** to proceed to the **Select Clients** window which shows the workstations to which the task will be delivered. In this step, you can add clients from selected Servers or Groups. Click **Next** to proceed to the next step.
9) The last dialog window, **Task Report** shows a preview of the configuration task. Enter a name or description for the task (optional). The **Apply task after** option can be used to set the task to run after a specified date/time. The **Delete tasks automatically by cleanup if successfully completed** option deletes all tasks which have been successfully delivered to target workstations.
10) Click **Finish** to register the task to run.

5.1.2 On-Demand Scan Task

The **New Task** context menu option contains two variants of the On-demand scan. The first option is **On-Demand scan...** - it executes an in-depth scan and cleaning of infected files concerning **Memory**, **Local Drives Boot** and **Local Drives** by default. The second option is **On-Demand Scan (Cleaning Disabled)...** – this scan only creates a log, no action is taken on infected files.

The **On-Demand Scan** window uses the same default settings for both variants, with the exception of the **Scan without cleaning** option. This option determines whether the scanner should or should not clean infected files. The example below demonstrates how to create an On-demand scan task.

1) The **Configuration Section** drop-down menu allows you to select the ESET product for which the On-demand scan task is being defined. Select your product(s) installed on target workstations.

   NOTE: Select **Exclude this section from On-demand scan** to disable all settings in the window for the selected product type – they will not be applied on workstations with the product type defined in the **Configuration** section. Therefore, all clients with the specified product will be excluded from the list of recipients. If the administrator marks clients as receivers and excludes the product using the above-mentioned parameter, then the task will fail with a notification that the task could not be applied. To avoid this, the administrator should always specify clients to which the task will be assigned.
2) In **Profile name** you can select a scanning profile to be applied for the task.

3) In the **Drives to scan** section, select the types of drives to be scanned on client computers. If the selection is too general, you can add an exact path to objects to be scanned. Use the **Path** field or click **Add Path** to specify your selection. Select **Clear History** to restore the original list of drives to scan.

4) Click **Next** to proceed to the dialog windows labeled **Select Clients** and **Task Report**, which are described in detail in the Tasks 77 chapter.

5) After the task has run client workstations, task results are sent back to the ERAS and can be viewed in ERAC in the **Scan Log** pane.

5.1.3 Update Now Task

The purpose of this task is to force updates on target workstations (virus signature database updates as well as program component upgrades).

1) Right-click on any workstation from the **Clients** pane and select **New Task** > **Update Now**.

2) If you wish to exclude certain types of ESET security products from the task, select them in the **Configuration section** drop-down menu and select the **Exclude this section from Update Task** option.

3) To use a specific update profile for the **Update Now** task, enable the **Specify profile name** option and select the desired profile. You can also select **User defined profile name** and enter the profile name; the value of the field will return to default if you click **Clear History**.

4) Then click **Next** to proceed to the dialog windows, **Select Clients** and **Task Report**. For a description of these dialogs, see chapter Tasks 77.

5.1.4 SysInspector Script Task

The SysInspector Script task lets you run scripts on target computers. It is used to remove unwanted objects from the system. For more details see the ESET SysInspector 159 help page.

1) After completing Stage I and Stage II described in chapter Tasks 77 click **Select** to choose a script to run on the target workstation.

2) Click **View & Edit** to adjust the script.

3) Click **Next** to proceed to the **Select Clients** and **Task Report** dialog windows which are described in detail in the Tasks 77 chapter.

4) After the task finishes on the client workstation, the information will display in the **State** column of the **Tasks** pane.

NOTE: SysInspector script tasks are supported only by ESET Endpoint Security/ESET Endpoint Antivirus version 4.0 and later.

5.1.5 Protection Features

This task allows the administrator to modify the status of the protection features of the security product (Windows ESET Security Products version 5 and later).

1. There are three stages to each protection feature - **Don`t change**, **Temporary Deactivate** and **Activate**. You can toggle these by selecting the check box next to each feature. If the protection feature is being deactivated (Temporary Deactivation), you can set a **Time interval of Temporary Deactivation**. This interval can be from 10 minutes to **Until next restart** (disables the feature completely until the next computer restart).
2. Then, select the clients for which you want to modify the protection features and finish the task 81.

NOTE: Use caution when disabling protection features, as this is a potential security risk. The client will be notified any time a protection feature is disabled.

5.1.6 Run Scheduled Task

This task will trigger a scheduled task that will run on the client immediately. You can either select a **Predefined** task from the client scheduler, or select a task **By ID**. Every scheduled task has an ID, so you can either select a task from the drop-down menu or type an ID. To view every task in the scheduler on a specific client, start this task from the context menu in the **Client** tab.

Select the task you want to run on a client(s), then select the clients for which you want to modify the protection features and finish the task 81.

5.1.7 Restore/Delete from Quarantine Task

With this task you can restore or delete specified quarantined objects from the client quarantine.

1) After you open the **Restore/Delete from Quarantine** window (see the chapter Tasks 77) select an action to be performed - either **Restore** or **Delete** - on the quarantined object.

   NOTE: When you restore an object from the quarantine that is still detected as a threat, you might want to consider excluding this object from further scanning using the **Add exclusion too** option to prevent the object from being scanned and quarantined again. Note that not all objects can be excluded, for example trojan horses or viruses. Attempt to exclude such files will lead to an error. If you want to exclude clean files (not detected as a threat), do it directly on the client or using ESET Configuration Editor (policy,task,etc.).

2) Select a condition by which quarantined objects are to be restored/deleted and click **Next**.

   NOTE: If you opened the Restore/Delete from Quarantine window by right-clicking a quarantine entry directly from the **Quarantine** tab (and selecting **Restore/Delete from Quarantine task**) you will not need to specify conditions (the **By hash** option will automatically be selected and the hash code of the quarantined file used as an identifier).

3) Select the clients for your restore/delete operation (see the chapter Tasks 77) and click **Next**.

4) Review your settings in the **Task Report** window, enter a name for your task, specify the time when you want to apply the task (and cleanup options if desired), and click **Finish** to confirm. See the chapter Tasks 77 for more details.

5.1.8 Rollback Virus Database

If you suspect that a new update of the virus database may be unstable or corrupt, you can rollback to the previous version and disable any updates for a chosen period of time. Alternatively, you can enable previously disabled updates.

Warning: Due to a critical bug causing blue screen errors, make sure you apply the Rollback Virus Database Task to ESET Endpoint Antivirus and ESET Endpoint Security version at least 5.0.2225.0 and newer.

1) Disable/Enable virus database updates

   Disable for X hours – The virus database of the client(s) will be rolled back to the previous versions (based on a client-created snapshot) and any update for the selected client(s) will be disabled for the selected time period. You can also select **Infinite** and disable updates completely. Use caution when disabling database updates completely, as this is a potential security risk.

   Warning: The option **Infinite** remains active even after a client computer restart.

   Enable previously disabled updates – Updating of the virus database will be enabled again.

2) Select the clients for this task and click **Next**.

3) Review your settings in the **Task Report** window, enter a name for your task, specify the time you would like to apply the task (and cleanup options if desired), and then click **Finish** to confirm. See chapter Tasks 77 for more details.

5.1.9 Clear Client`s Update Cache

This task works for ESET Security Products version 5 and later. If you suspect that the virus database update was not successful, you can clear the client`s update cache and the latest update will be downloaded again.

1) Start the task and click **Next**.

2) Select the clients for this task and click **Next**.

3) Review your settings in the **Task Report** window, enter a name for your task, specify the time you would like to apply the task (and cleanup options if desired), and then click **Finish** to confirm. See chapter Tasks 77 for more details.

5.1.10 Generate Security Audit Log Task

This task applies to ESET Mobile Security only.

Security Audit checks: battery level, Bluetooth status, free disk space, device visibility, home network and running processes. A detailed report will be generated, indicating whether or not the item value is below the specified threshold or if it could represent a potential security risk (e.g., device visibility turned on, etc.).

To run security audit on the phone:

1) Right-click the client's name from the **Clients** pane and select **New Task** > **Generate Security Audit Log** from the context menu.

2) Click **Next** to proceed to the **Select Clients** and **Task Report** windows. For a description of these windows, see the chapter titled Tasks 77.

5.1.11 Show Notification Task

This task applies to ESET Mobile Security only.

To send a notification (e.g., a warning message) to the phone:

1) Right-click the client's name from the **Clients** pane and select **New Task** > **Show Notification** from the context menu.

2) Type the notification **Title** and message **Body** in the appropriate fields and select the notification **Verbosity**.

3) Click **Next** to proceed to the **Select Clients** and **Task Report** windows. For a description of these windows, see the chapter titled Tasks 77.

5.1.12 Finishing the Task

In the last dialog window, task preview is displayed. It contains all task parameters and enables the user to click **Back** and perform modifications if necessary.

The second part of the window contains the following settings:

- **Name** – Name of the task.
- **Description** – Task description.
- **Apply task after** – Time to deploy task on client computers.
- **Delete tasks automatically by cleanup if successfully completed** – Automatically deletes all successfully performed tasks.
- **Randomly delay start time up to X minutes** – The task will be randomly delayed concerning the selected computers. So if you have several computers selected, then the task will be be sent to each of them in a different time, not at once.

Note: The random delay is available only for ESET business products version 5 and newer.

5.2 Group Manager

Group Manager is a powerful tool for managing your clients, separating them into different groups and applying different settings, tasks, restrictions, etc. It is easily accessible via **Tools > Group Manager** or **CTRL+G**. Groups are independent for each ERAS and are not replicated.

You can create your own groups to fit your needs in your company network, or simply synchronize ERAC client groups with your Microsoft Active Directory using the **Active Directory Synchronization** wildcard from the main Group Manager window.

There are two main types of client groups:

- Static Groups 82
- Parametric Groups 83

Both Static and Parametric Groups can be used in various places within ERA, which significantly improves client management capabilities.

5.2.1 Static Groups

Static groups are created to separate clients in your network into named groups and subgroups. For example, you can create a Marketing group that will contain all marketing clients and also create specialized subgroups — Local sales, EMEA Management, etc.

The Static Groups main window is divided into two parts. The left side contains existing, hierarchically displayed groups and subgroups. Clients included in the selected group are listed on the right side of the window. By default, only clients in the selected group are listed. If you wish to see clients included in subgroups of the currently selected group, select the check box next to **Show clients in subgroups** on the right side of the window.

To create a new group, click **Create** and enter a name for the group. A new group is created as a subgroup of the currently selected parent group. If you wish to create a new main group, select the root of the hierarchical tree – **Static Groups**. The **Parent group** field contains the name of the parent group for the newly created group (i.e., "/" for the root). We recommend using a name that indicates where the computers are located (e.g., *Business Department, Support* etc.). The Description field can be used to further describe the group (e.g., "*Computers in office C*", *"HQ workstations*" etc.). Newly created and configured groups can also be edited later.

NOTE: When a task is sent to the Parent group, all workstations that belong to its subgroup(s) will accept this task as well.

It is also possible to create empty groups for future use.

Click **OK** to create the group. Its name and description will appear on the left and the **Add/Remove** button will become active. Click this button to add clients you would like included in the group (either double-click or drag-and-drop them from left to right). To find and add clients, enter all or part of a client name in the **Quick search** field and all clients containing the typed string will be displayed. To mark all clients, click **Select All**. Click **Refresh** to check for any new clients recently connected to the server.

If manually selecting clients is not convenient you can click **Add Special...** for more options.

Select the **Add clients loaded in the Clients pane** option to add all clients displayed in the client section, or select the **Only selected** option. To add clients that already belong to another server or group, select them from the lists on the left and right and click **Add**.

Click **OK** in the **Add/Remove** dialog window to return to the main Static Group Manager window. The new group should be displayed with its corresponding clients.

Click **Add/Remove** to add or remove clients from groups, or click **Delete** to delete an entire group. Click **Copy to Clipboard** to copy the client and group lists. To refresh the group clients click **Refresh**.

You can also **Import/Export** currently selected group clients to an *.xml* file.

5.2.2 Parametric Groups

In addition to static groups, parametric groups can be very useful. Client stations are dynamically assigned to a certain parametric group when the group's conditions are met. The advantage of parametric groups is the ability to use them in various places, including filters, policies, reports and notifications.

The Parametric Groups main window is composed of four sections. **Parametric Groups** lists the parent groups and subgroups that have been created. When you have selected a certain group from the **Parametric Groups list**, clients that belong to the currently selected group are listed in the **Selected Group** section.

NOTE: When a parent group is selected, the list contains subgroup members as well.

Parameters set for a selected group are listed in the **Parameters** section of the window. You can edit or add parameters at any time by clicking **Edit...**.

The **Synchronization status** section displays a progress bar for the synchronization process.

1. To create a new group, click **Create...**. The new group will be created as a subgroup of the currently selected parent group. If you wish to create a main group, select the root of the hierarchical tree — **Parametric Groups**. The **Parent group** field contains the name of the parent group for the newly created group (i.e., "/" for the root). Enter a **Name** and a short **Description** for the new group.

2. The next step is to create **Client filter parameters**, which can be done in the **Rule Editor** by selecting options after clicking **Edit...** Here, you can specify the conditions necessary for the rule to be triggered and applied. Select the condition and specify it by clicking **Specify** next to the rule in the **Parameters** window below. You can also choose whether you want this rule to be applied only when **all of the conditions are met**, or if **any of the conditions are met**.

3. If you select the check box next to **Sticky**, clients will be automatically added to this group when they match the conditions, but will never be removed. The content of a sticky group can be reset manually at the root level.

NOTE: This parameter can only be set when creating a new group.

To edit an existing group, select it from the **Parametric Groups list** and then click **Edit...** in the bottom of the window. For group deletion, select the desired group and click **Delete**.

You can manually refresh the group list by clicking **Refresh**. To import a group from a file select a group in the **Parametric Groups** section under which you want the new group to be imported and click **Import...** Confirm your selection by clicking **Yes**. Locate the file you want to import and click **Open**. The group (and all of its subgroups) will be imported under the selected location. To export a group (and all of its subgroups) select it in the **Parametric Groups** section, click the arrow on **Import...** and select **Export...** Click **Yes** to confirm, select a name and a location for your export file and click **Save**.

NOTE: You can use your mouse to drag and drop groups already in the **Parametric Groups** section.

NOTE: You can conveniently use the parametric groups for filtering data or clients. For example, you want to generate reports only for computers with Windows XP. Create a parametric group only for computers with the specific operating system and use this group in the filter target. You can also set your own **Custom Client Data** when creating an installation package 46 - (**Configuration Editor** > **Kernel** > **Settings** > **Remote Administration**). Set this option (Custom Client Data) as a parameter for a parametric group and every user that installs this package becomes a member of this group.

5.2.3 Active Directory / LDAP Synchronization

Active Directory Synchronization uses automatic group creation (with corresponding clients) based on the structure defined by Active Directory. It allows the administrator to sort clients to groups, as long as the client name matches the object type *computer* in the Active Directory (AD) and belongs to groups in the AD.

There are two main options that determine the manner of synchronization:

- **Synchronize groups** allows you to choose which AD groups will be synchronized. Select **All groups** to synchronize the complete AD tree structure whether or not the AD groups contain ERA clients. The next two options (**Only groups containing ERA Server clients** and **Only groups containing ERA primary server clients**) will synchronize only groups containing existing ERA clients.

- The **Synchronization type** defines whether the AD groups to be synchronized will be added to the existing AD/ LDAP groups (**AD/LDAP groups import**), or if the existing AD/LDAP groups will be completely replaced by those to be synchronized (**AD/LDAP groups synchronize**).

- **Synchronized branches** allows you to select particular branches of the **Active Directory/LDAP** to be synchronized. Click **Configure** to select what branches of Active Directory/LDAP will be synchronized with groups. By default, all branches are marked/selected.

Note: Click **More information!** to display additional information about the Active Directory / LDAP synchronization settings and rules.

- To configure the synchronization interval between the AD/LDAP and the ERA Server, click **Change...** next to the **Synchronize** option. Select the desired frequency of the synchronization in the **AD/LDAP Synchronization Scheduled Interval (in server local time)** dialog window. The selected frequency will be displayed next to the **Synchronize** option.

Detailed configuration of Active Directory synchronization can be performed using the **Configuration Editor** (**Remote Administrator** > **ERA Server** > **Settings** > **Groups** and **Active directory / LDAP**). You can add other Active Directory/ LDAP objects by selecting the check box(es) next to the desired option(s).

Clicking **Synchronize Now** triggers the synchronization (based on the options configured above).

NOTE: For ERAS to synchronize with Active Directory, ERAS does not need to be installed on your domain controller. The domain controller only needs to be accessible from the computer where your ERAS is located. To configure authentication to your domain controller, go to **Tools** > **Server Options** > **Advanced** > **Edit Advanced Settings** > **Remote Administrator** > **ERA Server** > **Settings** > **Active directory / LDAP**.

5.3 Policies

Policies are in many ways similar to **Configuration tasks**, except they are not one-shot tasks sent to one or more workstations. Rather, they provide continuous maintenance of certain configuration settings for ESET security products. In other words, a **Policy** is a configuration that is forced to a client.

5.3.1 Basic principles and operation

Access the Policy Manager by selecting **Tools** > **Policy Manager...** The Policy Tree on the left lists the policies that are present on individual servers. The right side is divided into four sections – **Policy settings**, **Policy configuration**, **Policy action** and **Global policy settings** – the options in these sections enable an administrator to manage and configure policies.

The primary functions of the Policy Manager include creating, editing and removing policies. Clients receive policies from ERAS. ERAS can use multiple policies which can inherit settings from each other or from policies from an upper server.

The system of adopting policies from an upper server is called *inheritance*; policies that are created as a result of inheritance are referred to as *merged policies*. Inheritance is based on the Parent – Child principle, i.e. a child policy inherits settings from a parent policy.

5.3.2 How to create policies

The default installation only implements one policy called ”Server Policy”. The policy itself is configurable from the ESET Configuration Editor – click **Edit Policy...** and define parameters for the selected ESET security product (or client). All parameters are organized into a comprehensive structure and all items in the Editor are assigned an icon. Clients will only adopt active parameters (marked by a blue icon). All inactive (greyed out) parameters will remain unchanged on target computers. The same principle applies to inherited and merged policies – a child policy will adopt only active parameters from a parent policy.

ERA Servers allow for multiple policies (**New Policy Child...**). The following options are available for new policies: **Policy name**, linking to a **Parent policy** and **Policy configuration** (configuration can be empty, you can copy merged policy configuration from a policy in the drop down menu, copied from an *.xml* configuration file or you can use the **Firewall Rules Merge Wizzard**). Policies can only be created on the server you are currently connected to via ERAC. To create a policy on a lower server you need to connect directly to that server.

Each policy has two basic attributes: **Override any child policy** and **Down replicable policy**. These attributes define how active configuration parameters are adopted by child policies.

- **Override any child policy** – Forces all active parameters to inherited policies. If the child policy differs, the merged policy will contain all active parameters from the parent policy (even though the **Override...** is active for the child policy). All inactive parameters from the parent policy will adjust to match the child policy. If **Override any child policy** is not enabled, settings in the child policy have priority over those in the parent policy for the resulting merged policy. Such merged policies will be applied to any additional child policies of the policy that was edited.

- **Down replicable policy** – Activates replication of policies to lower servers, for example, a policy can serve as the default policy for lower servers and can also be assigned to clients connected to lower servers.

Policies can also be imported/exported from/to an *.xml* file or imported from Groups. For more information see chapter titled Importing/Exporting policies 86.

5.3.3 Virtual policies

In addition to created policies, as well as those replicated from other servers (see chapter Replication tab 113), the Policy Tree also contains a default parent policy, which is referred to as a virtual policy.

The default parent policy is located on an upper server in the **Global** policy settings and selected as **Default policy for lower servers**. If the server is not replicated, this policy is empty (will be explained later on).

The default primary clients policy is located on the given server (not on an upper server) in Global Policy settings and picked up in default policy for primary clients. It is automatically forced to newly connected clients (primary clients) of the given ERAS, unless they have already adopted some other policy from Policy Rules (for more information, see chapter Assigning policies to clients 87). Virtual policies are links to other policies located on the same server.

5.3.4 Role and purpose of policies in the policy tree structure

Each policy in the **Policy Tree** is assigned an icon on the left. The meaning of icons are as follows:

1) Policies with blue icons refer to those present on the given server. There are three subgroups of blue icons:

Icons with white targets – Policy was created on that server. In addition, it is not down replicable, which means it is not assigned to clients from lower servers and also it does not serve as a parent policy for child servers. These policies can only be applied within the server – to clients connected to the server. It can also serve as a parent policy for another policy from the same server.

Icons with blue targets – Policy was also created on the server, however, the option **Override any child policy** is selected (for more information, see chapter How to create policies 85).

Icons with downward arrows – these policies are replicated and have **Down replicable policy** is enabled. You can apply these policies on the given server and on its child servers.

Icons for the default **Server Policy**.

2) Policies with gray icons originate from other servers.

Icons with upward arrows – These policies are replicated from child servers. They can only be viewed or deleted with the option **Delete Policy Branch**. This option will not delete the policy itself, it will only remove the policy from the Policy Tree. Therefore they can reappear after replication. If you do not want to display policies from lower servers, use the option **Hide foreign servers policies not used in policy tree**.

Icons with downward arrows – These policies are replicated from upper servers. They can be used as Parent policies for other policies, assigned to clients (**Add Clients**) or removed (**Delete Policy**). Please note that deleting will only delete the policy – it will reappear after replication from the upper server (unless the attribute **Down replicable policy** has been disabled on the upper server).

NOTE: To move and assign policies within the structure, you can either select the parent policy, or drag-and-drop it with the mouse.

Existing policy rules can be imported/exported from/to an *.xml* file by clicking **Import/Export Policies**. If an existing and an imported policy both use the same name, a random string will automatically be added after the name of the imported policy.

5.3.5 Viewing policies

Policies in the **Policy Tree** structure can be viewed directly in the **Configuration Editor** by clicking **View Policy** > **View...** or **View Merged...**.

View Merged – Displays the merged policy created as a result of inheritance (the process of inheriting applies settings from the parent policy). This option is displayed by default, because the current policy is already a merged policy.

View – Displays the original policy before it was merged with a parent policy.

On lower servers, the following options are available for policies inherited from upper servers:

View Merged – Same as above.

View Override Part – This button applies for policies with the attribute **Override any child policy**. This option only shows the forced part of the policy – i.e. the one which has priority over other settings in child policies.

View Non-force part – Has opposite effect of View Override Part – only displays active items, to which Override… is not applied.

NOTE: You can double-click on a policy tree item to view merged.

5.3.6 Importing/Exporting policies

The Policy Manager allows you to import/export policies and policy rules. Existing policies can be imported/ exported from/to an *.xml* file by clicking **Import/Export Policies**. The policies can furthermore be imported from groups by clicking the **Import from Groups...** button. Policy rules can be imported/exported by clicking **Import...** or **Export...** and, in addition, they can be created using the **Policy Rules Wizard**.

Name conflicts (the existing and the imported policy names are identical) are solved during the import by adding a random string to the name of the imported policy. If a conflict cannot be resolved in this fashion (usually due to the new name being too long) the import finishes with the warning *Unresolved policy name conflict*. The solution is to delete or rename the conflicting policies or policy rules.

5.3.7 Policy Migration Wizard

The **Policy migration wizard** helps you create a new **Windows desktop v5 policy**, or update your existing **Windows desktop v5** policy using the settings from your existing Windows product line v3 and v4 policies. You can migrate all policies during installation over a previous version, but to customize all settings for the migration we recommend that you use the **Policy migration wizard**.

To migrate policies:

1. Select the check box(es) next to policies that you want to migrate settings from.
2. If an Endpoint policy already exists, select one of the following settings:

- **Replace existing Endpoint policy and use only source settings** - The existing policy will be completely replaced by the newly created (**Windows desktop v5**) policy and the settings from the original (**Windows product line v3 and v4**) policy will be used.
- **Merge policies and do not replace conflicting Endpoint settings** - Existing and migrated policies will be merged and existing settings in the Windows desktop v5 policy will not be overwritten by settings from the Windows product line v3 and v4 policy.
- **Merge policies and replace conflicting Endpoint settings** - Existing and migrated policies will be merged and the conflicting settings will be replaced with the original (v3/v4) settings.

3. Wait for the process to finish, times will vary depending on the number of policies being migrated. Click **Finish** when you see the message **Policy migration is complete**.

5.3.8 Assigning policies to clients

There are two main rules for assigning policies to clients:

1. Local (primary) clients can be assigned any local policy or any policy replicated from upper servers.
2. Clients replicated from lower servers can be assigned any local policy with the **Down replicable** attribute or any policy replicated from upper servers. They cannot be forced to adopt policies from their own primary server (to do so, you must connect to that server with ERAC).

An important feature is that each client is assigned some policy (there is no such thing as clients with no policy). Also, you cannot take a policy away from a client. You can only replace it with another policy. If you do not want to apply a configuration from any policy to a client, create an empty policy.

5.3.8.1 Default Primary Clients Policy

One method of assigning policies is automatic application of the **Server Policy**, a virtual policy that is configurable in **Global** policy settings. This policy is applied to primary clients, i.e. those directly connected to that ERAS. For more information see chapter Virtual policies 85.

5.3.8.2 Manual assigning

There are two ways to manually assign policies: Right-click a client in the **Clients** pane and select **Set Policy** from the context menu, or click **Add Clients** > **Add/Remove** in the Policy Manager.

Clicking **Add Clients** in the Policy Manager opens the **Set/Remove** dialog window. Clients are listed on the left in the format Server/Client. If the **Down replicable policy** is selected, the window will also list clients replicated from lower servers. Select clients to receive the policy by using the drag-and-drop method or clicking **>>** to move them to **Selected items**. Newly selected clients will have a yellow asterisk and can still be removed from **Selected items** by clicking the **<<** or **C** button. Click **OK** to confirm the selection.

NOTE: After confirming, if you reopen the **Set/Remove** dialog window, clients cannot be removed from **Selected items**, you can only replace the policy.

You can also add clients using the **Add Special** feature, which can add all clients at once, add selected clients or add clients from selected servers or groups.

5.3.8.3 Policy Rules

The **Policy Rules** tool allows an administrator to automatically assign policies to client workstations in a more comprehensive way. Rules are applied immediately after the client connects to the server; they have priority over the **Server Policy** and over manual assignments. The **Server Policy** only applies if the client does not fall under any current rules. Likewise, if there is a manually assigned policy to be applied and it is in conflict with the policy rules, the configuration forced by the policy rules will take precedence.

If each server is managed by a local administrator, each administrator can create individual policy rules for their clients. In this scenario it is important that no conflicts exist between policy rules, such as when the upper server assigns a policy to clients based on the policy rules, while the lower server simultaneously assigns separate policies based on local policy rules.

Policy rules can be created and managed from the **Policy rules** tab in Policy Manager.. The process of creation and application is very similar to that of rule creation and management in email clients: each rule can contain one or more criteria; the higher the rule is in the list, the more important it is (it can be moved up or down).

To create a new rule, click **New Rule** and select whether you want to **Create New** or use the Policy Rules Wizard 89. Then enter a **Name**, **Description**, **Client filter parameter** and **Policy** (a policy that will be applied to any clients matching the specified criteria).

To configure the filtering criteria, click **Edit**:

(NOT) FROM Primary Server – If (not) located on primary server.
IS (NOT) New Client – If it is (not) a new client.
HAS (NOT) New Flag – Applies to clients with/without the New Client flag.
Primary Server (NOT) IN (specify) – If name of the primary server contains/does not contain...
ERA GROUPS IN (specify) – If client belongs to the group...
ERA GROUPS NOT IN (specify) – If client does not belong to the group...
DOMAIN/WORKGROUP (NOT) IN (specify) – If client belongs/does not belong to the domain...
Computer Name Mask (specify) – If computer name is ....
HAS IPv4 Mask (specify) – If client belongs to the group defined by the IPv4 address and mask...
HAS IPv4 Range (specify) – If client belongs to the group defined by the IPv4 range...
HAS IPv6 Mask (specify) – If client belongs to the group defined by the IPv6 address and mask...
HAS IPv6 Range (specify) – If client belongs to the group defined by the IPv6 range...
HAS (NOT) Defined Policy (specify) – If client does (or does not) adopt the policy...
Product Name (NOT) IN – If product name is...
Product Version IS (NOT) – If product version is...
Client Custom Info Mask 1, 2, 3(NOT) IN – If Client Custom Info contains...
Client Comment Mask (NOT) IN –
HAS (NOT) Protection Status (specify) – If client's protection status is...
Virus Signature DB Version IS (NOT) – If virus signature database is...
Last Connection IS (NOT) older than (specify) – If last connection is older than...
IS (NOT) Waiting For Restart – If client is waiting for restart.

Policy rules can be imported from or exported to an *.xml* file. Policy rules can also be created automatically by using the Policy Rules Wizard 89, which allows you to create a policy structure based on the existing group structure and then map created policies to groups by creating correspondent policy rules. For more information on importing/ exporting policy rules see chapter titled Importing/Exporting policies 86.

To remove a policy rule, click **Delete Rule....**

Click **Run Policy Rule Now...** if you want to immediately apply the activated rule.

5.3.8.3.1 Policy Rules Wizard

The Policy Rules Wizard allows you to create a policy structure based on the existing group structure and map created policies to groups by creating corresponding policy rules.

1. In the first step you are prompted to organize your group. If you do not have a desired group structure configuration you can click Group Manager 82 to setup your groups and then click **Next**.
2. In step two, you will be prompted to specify which of the categories of client groups will be affected by the new policy rule. After selecting the desired check boxes click **Next**.
3. Choose the **Parent policy**.
4. In the final step you will see a simple process status message. Click **Finish** to close the **Policy Rules Wizard** window.

Your new policy rule will appear in the list in the **Policy Rules** tab. Select the check box next to your rule name to activate a specific rule.

For more information on importing/exporting policy rules and name conflicts see the chapter Importing/Exporting policies 86.

5.3.9 Policies for mobile clients

A user with an ESET Product installed on their mobile device has more control over the settings and the behavior of their software than a user with a notebook/desktop with an ESET product installed. For this reason, there is no need to continuously force a policy to mobile users, because the user might want to change or adjust certain settings. We recommend that you use the technique demonstrated below to create a policy for mobile clients:

Create an empty policy (default policy for clients)

1. Click **Tools > Policy Manager**.
2. Click **Add New Policy** to create an empty policy with no modified settings. In the Policy configuration section, select **Create empty policy configuration**.
3. Click **Add clients** and select the mobile users you want to manage with this policy.
4. Click the Policy Rules 88 tab and click **New**.
5. Select this policy in the **Policy** drop-down menu and click **Edit.**
6. Select the **IS New Client** rule condition, in the **Parameters** field click IS to change the rule condition to **IS NOT New Client** and then click **OK** two times.
7. Click **OK** and then click **Yes** when asked if you want to save your settings.
8. This policy will be applied to the client every time they connect to ERA.

Create a one-time policy (start-up policy for clients)

1. Click **Tools > Policy Manager**.
2. Click **Add New Policy** to create an empty policy with no modified settings. In the Policy configuration section, select **Create empty policy configuration**.
3. Configure the settings you want to apply to mobile clients and save the configuration.
4. Click **Add clients** and assign the mobile users you want to manage with this policy.
5. Click the Policy Rules 88 tab and click **New**.
6. Select this policy in the **Policy** drop-down menu and click **Edit**.
7. Select the **IS New Client** rule condition and click **OK** two times.

8. Click **OK** and then click **Yes** when asked if you want to save your settings.

When the mobile clients connect to ERA for the first time, they receive the settings from the **One-time policy**. The next time they connect to ERA, they receive an **empty policy** and their settings will not be affected.

5.3.10 Deleting policies

As with rule creation, deleting is only possible for policies located on the server you are currently connected to. To delete policies from other servers, you must directly connect to them with the ERAC.

NOTE: A policy may be linked to other servers or policies (as a parent policy, as a default policy for lower servers, as a default policy for primary clients, etc.), therefore, in some cases it would need to be replaced rather than deleted. To see options for deleting and replacing, click **Delete Policy...**. The options described below may or may not be available, depending on the position of the given policy in the policy hierarchy.

- **New policy for primary clients with the currently deleted policy** – Allows you to select a new policy for primary clients to substitute the one you are deleting. Primary clients can adopt the **Default policy for primary clients**, as well as other policies from the same server (either assigned manually – **Add Clients** or forced by **Policy Rules**). As a replacement you can use any policy from the given server or a replicated policy.

- **New parent policy for the currently deleted policy's children policies** – If a policy to be deleted served as a parent policy for other child policies, it must also be substituted. It can be substituted by a policy from that server, by a policy replicated from upper servers, or by the N/A flag, which means that child policies will be assigned no substitute policy. We highly recommend that you assign a substitute even if no child policy exists. Another user assigning a child policy to that policy during the deletion process would cause a conflict.

- **New policy for replicated clients with the currently deleted or modified policy** – Here you can select a new policy for clients replicated from lower servers – those that were applied to the one you are currently deleting. As a replacement you can use any policy from the given server or a replicated policy.

- **New default policy for lower servers** – If the deleted policy serves as a virtual policy (see section **Global Policy Settings**), it must be substituted by another one (for more information, see chapter Virtual policies 85). As a replacement you can use any policy from the given server or the N/A flag.

- **New default policy for primary clients** – If the deleted policy serves as a virtual policy (see section **Global Policy Settings**), it must be substituted by another one (for more information, see chapter Virtual policies 85). You can use a policy from the same server as a replacement.

The same dialog will also open if you disable the **Down replicable** option for a policy and click **OK, Apply** or if you select another policy from the Policy Tree. This will activate the items **New policy for replicated clients with the currently deleted or modified policy** or **New default policy for lower servers**.

5.3.11 Special settings

Two additional policies are not located in the Policy Manager but in **Tools** > **Server Options** > **Advanced** > **Edit Advanced Settings** > **ESET Remote Administrator** > **ERA Server** > **Settings > Policies**.

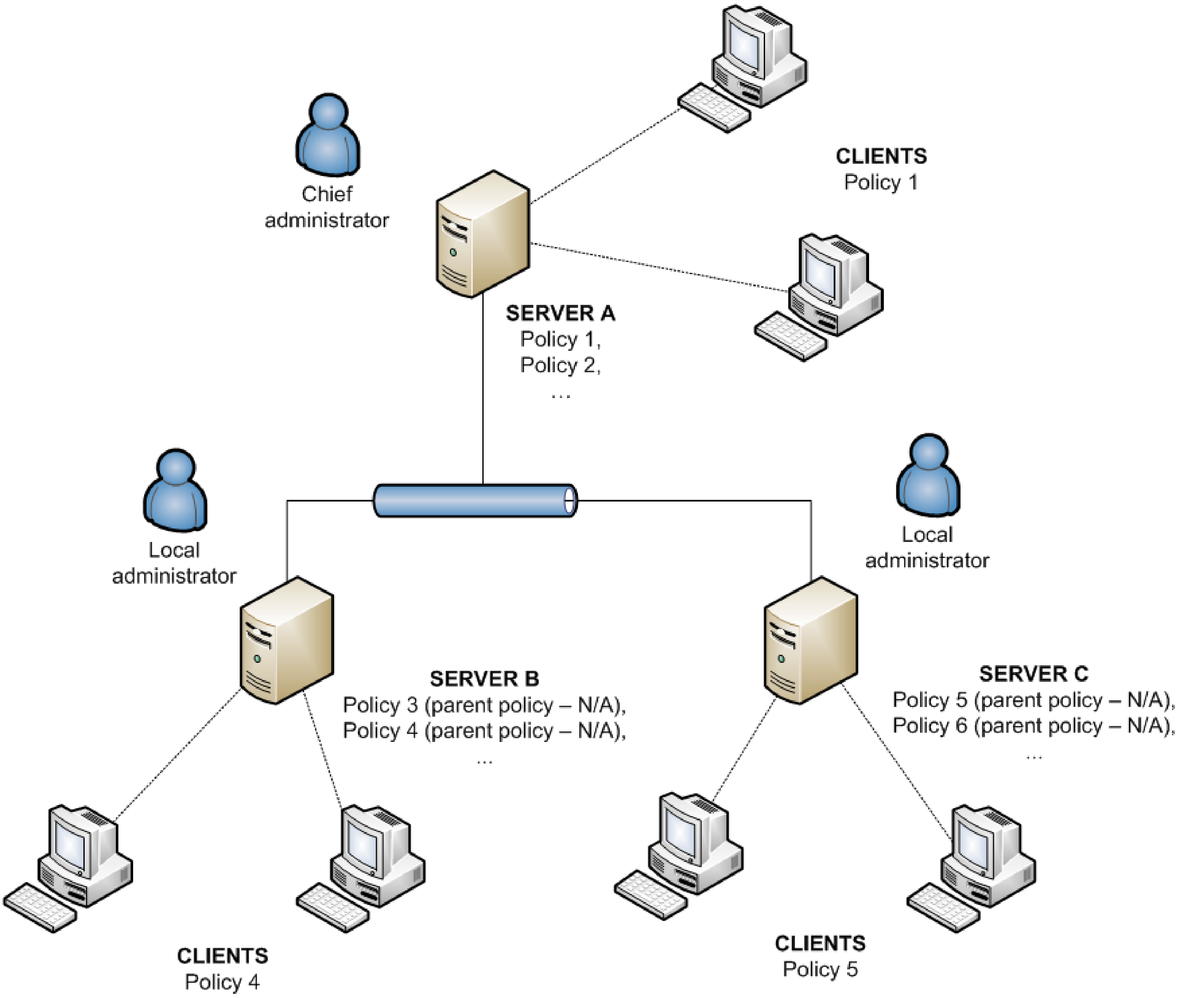
- **Interval for policy enforcement (minutes)** - This feature applies to policies in the specified interval. We recommend the default setting.

- **Disable policy usage** - Enable this option to cancel the application of policies to servers. We recommend this option if there is a problem with the policy. If you want to avoid applying a policy to some clients, a better solution is to assign them to an empty policy.

5.3.12 Policy deployment scenarios

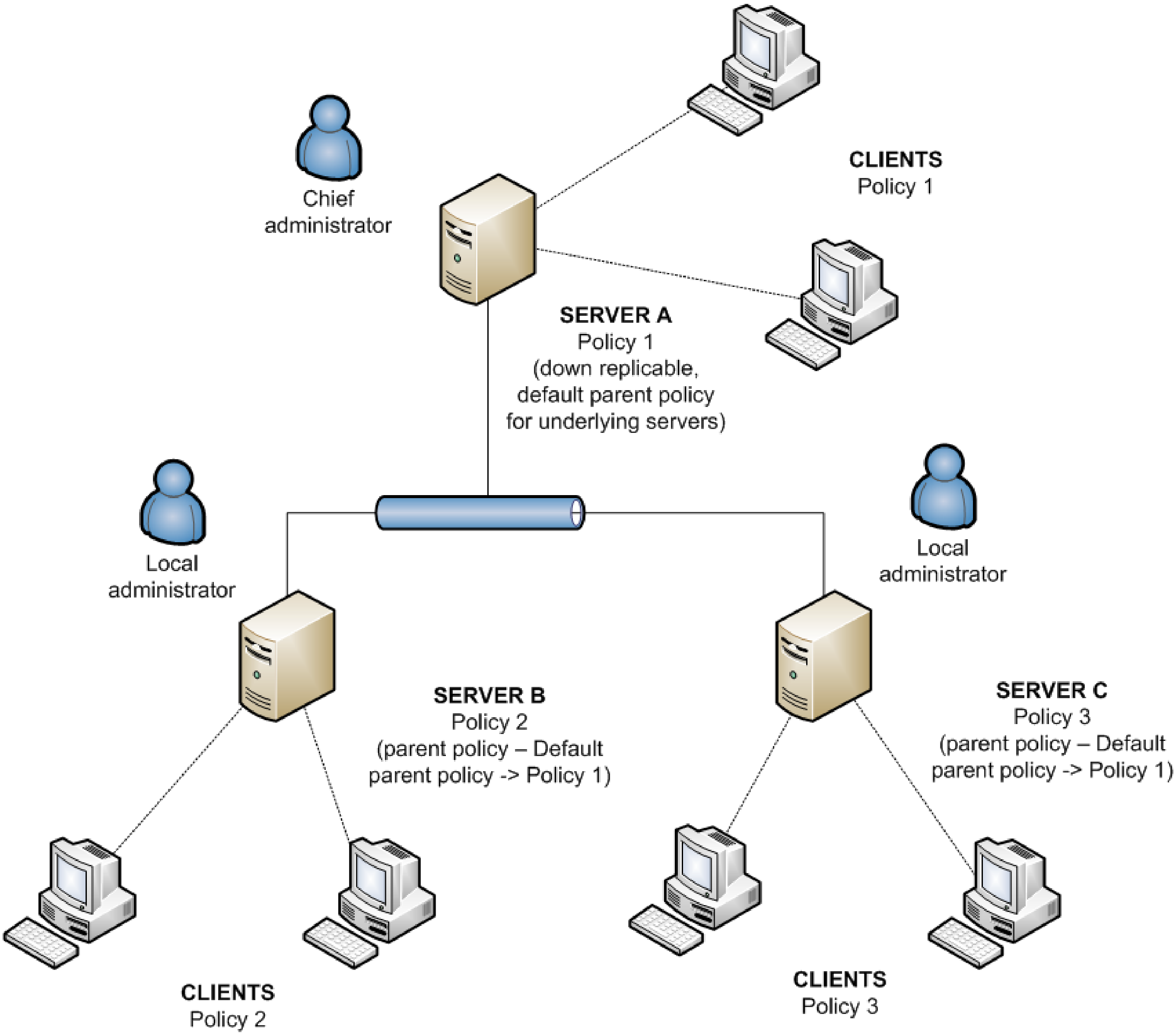
5.3.12.1 Each server is a standalone unit and policies are defined locally

For the purpose of this scenario suppose there is a small network with one main and two lower servers. Each server has several clients. On each server, there is at least one or more policies created. The lower servers are located at the company's branch offices; both servers are managed by their local administrators. Each administrator decides which policies are to be assigned to which clients within their servers. The main administrator does not intervene in the configurations made by the local administrators and he does not assign any policies to clients from their servers. From a server policy perspective, this means that Server A has no **Default policy for lower servers**. It also means that Server B and Server C have the N/A flag or another local policy (aside from the **Default parent policy**) set as a parent policy. (e.g., Servers B and C do not have any parent policies assigned from the upper server).



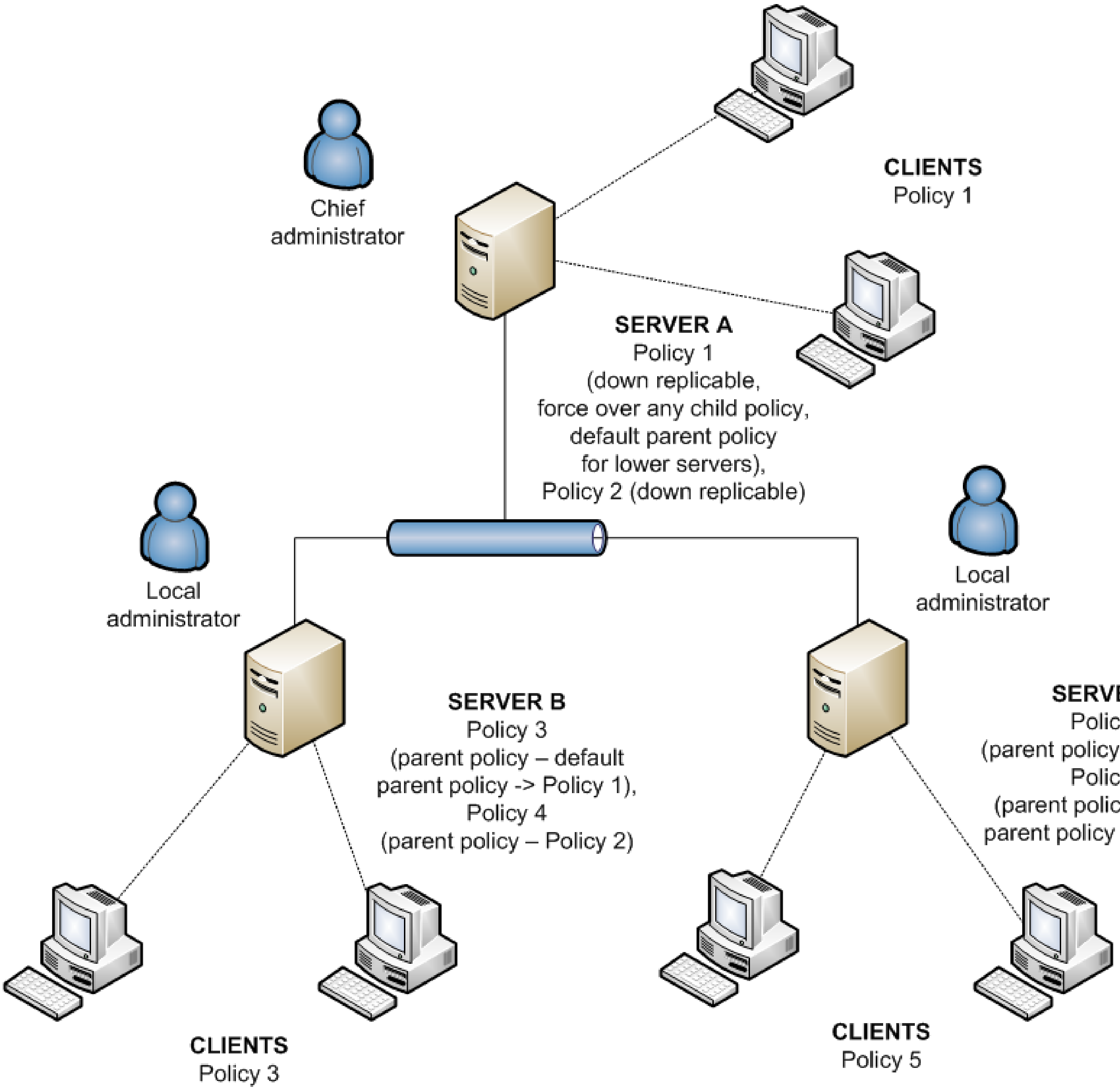
5.3.12.2 Each server is administered individually - policies are managed locally but the Default Parent Policy is inherited from the upper server

The configuration from the previous scenario also applies to this scenario. However, Server A has the Default Policy for Lower Servers enabled and policies on the lower servers inherit the configuration of the Default Parent Policy from the master server. In this scenario, the local administrators are given a large degree of autonomy to configure policies. While the child Policies on lower servers may inherit the Default Parent Policy, the local administrators can still modify it by their own policies.


Chief administrator
CLIENTS
Policy 1
SERVER A
Policy 1
(down replicable, default parent policy for underlying servers)
Local administrator
Local administrator
SERVER B
Policy 2
(parent policy – Default parent policy -> Policy 1)
SERVER C
Policy 3
(parent policy – Default parent policy -> Policy 1)
CLIENTS
Policy 2
CLIENTS
Policy 3

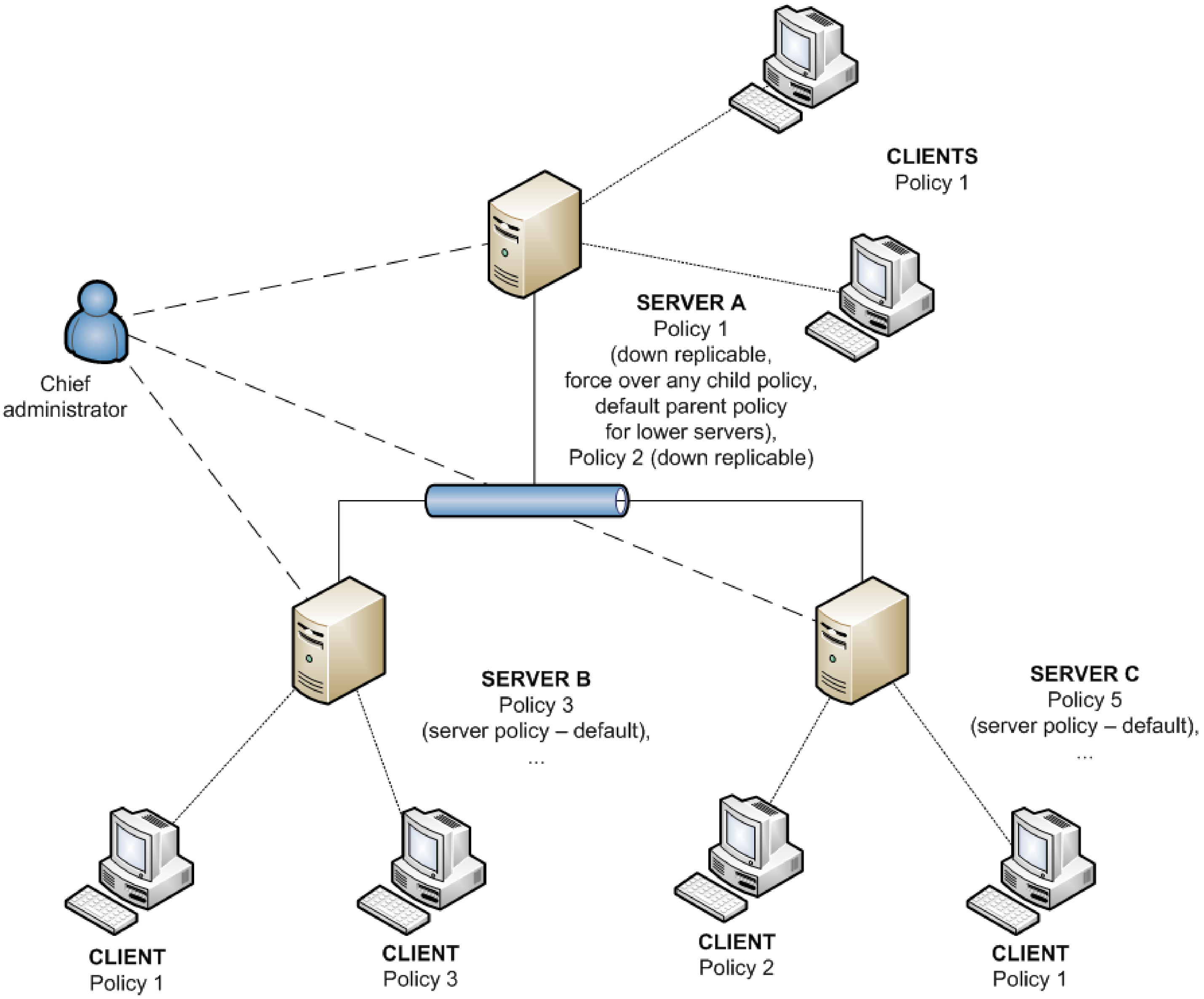
5.3.12.3 Inheriting policies from an upper server

The network model for this scenario is the same as the previous two scenarios. In addition, the master server, along with the Default Parent Policy, contains other policies, that are down replicable and serve as parent policies on the lower servers. For Policy 1 (see the figure below), the attribute **Override any child policy** is activated. The local administrator still has a large degree of autonomy, but the main administrator defines which policies are replicated down and which of them serve as parent policies for local policies. The attribute **Override…** dictates that configurations set in the selected policies override those set on the local servers.



5.3.12.4 Assigning policies only from the upper server

This scenario represents a centralized system of policy management. Policies for clients are created, modified and assigned only on the main server - the local administrator has no rights to modify them. All lower servers have only one basic policy, which is empty (by default titled Server Policy). This policy serves as the Default Parent Policy for Primary Clients.



5.3.12.5 Using groups

In some situations, assigning policies to groups of clients can complement previous scenarios. Groups can be created manually or by using the **Active Directory Synchronization** option.

Clients can be added to groups either manually (**Static Groups**) or automatically — by the group properties (**Parametric Groups**). See chapter Group Manager 82 for more details.

To assign a policy to a group of clients, you can use the one-time assignment option in **Policy Manager** (**Add Clients > Add Special**), or deliver policies automatically via **Policy Rules**.

One of the possible scenarios is as follows:

The administrator wants to assign different policies for clients belonging to different AD groups and change the client's policy automatically when the client is moved to another AD group.

1) The first step is to set **Active Directory Synchronization** in **Group Manager** according to your needs. The important thing here is to properly schedule the AD synchronization (possible options: hourly, daily, weekly, monthly).

2) After the first successful synchronization, the AD groups appear in the **Static Groups** section.

3) Create a new policy rule and mark **ERA Groups IN** and/or **ERA Groups NOT IN** as a rule condition.

4) Specify the AD groups that you want to add to the condition.

5) In the next step define the policy that will be applied to clients matching the rule condition(s) and press **OK** to save the rule.

NOTE: Steps 3 - 5 can be replaced by using the **Policy Rules Wizard**, which allows you to create a policy structure based on the existing group structure and map created policies to groups by creating corresponding policy rules.

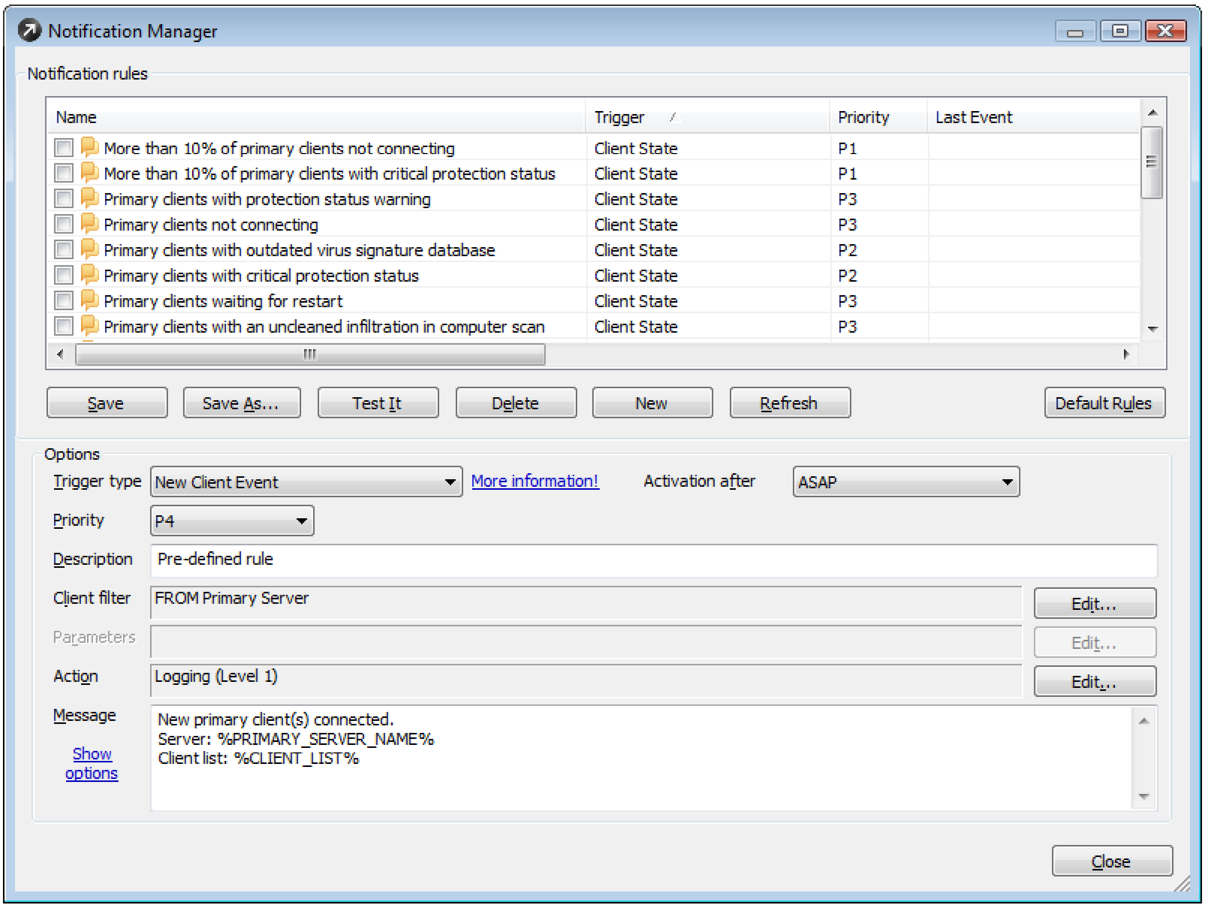
This way it is possible to define a particular policy rule for each AD group. Assigning a certain policy to a certain client now depends on the client's membership in a certain AD group. Since the AD synchronization is scheduled to occur regularly, all changes in the client's AD groups membership are refreshed and taken into account when a policy rule is applied. In other words, policies are applied to clients automatically depending on their AD group. Once the rules and policies are defined thoroughly, no more intervention regarding policy application is needed from the administrator.

The main advantage of this approach is direct, automatic linking between AD group membership and policy assignment.

5.4 Notification Manager

The ability to notify system and network administrators about important events is an essential aspect of network security and integrity. An early warning about an error or malicious code can prevent the enormous loss of time and money often needed to eliminate such problems later on. The next three sections outline the notification options offered by ERA.

To open the **Notification Manager** main window, click **Tools** > **Notification Manager**.



Name	Trigger	Priority	Last Event
□ More than 10% of primary clients not connecting	Client State	P1	
□ More than 10% of primary clients with critical protection status	Client State	P1	
□ Primary clients with protection status warning	Client State	P3	
□ Primary clients not connecting	Client State	P3	
□ Primary clients with outdated virus signature database	Client State	P2	
□ Primary clients with critical protection status	Client State	P2	
□ Primary clients waiting for restart	Client State	P3	
□ Primary clients with an uncleaned infiltration in computer scan	Client State	P3	

Trigger type: New Client Event

Activation after: ASAP

Priority: P4

Description: Pre-defined rule

Client filter: FROM Primary Server

Parameters:

Action: Logging (Level 1)

Message:

```
New primary client(s) connected.
Server: %PRIMARY_SERVER_NAME%
Client list: %CLIENT_LIST%
```

The main window is divided in two sections:

1. The **Notification rules** section in the top part of the window contains a list of existing (either predefined or user-

defined) rules. A rule in this section must be selected to generate notification messages. By default, no notifications are enabled. Therefore, we recommend checking whether your rules are active. The functional buttons under the list of rules include **Save** (save modifications to a rule), **Save as...** (save modifications to a rule with a new name), **Delete**, **Test It** (clicking this button will immediately trigger the rule and send a notification), **New** (use this button to create new rules), **Refresh** and **Default Rules** (update the list with default rules).

By default, the **Notification Manager** window contains predefined rules. To activate a rule, select the check box next to the rule. The following notification rules are available. If they are activated and the rule conditions are met, they generate log entries.

- **More than 10% of primary clients are not connecting** – If more than 10 percent of clients have not connected to the server for more than a week; the rule runs ASAP if this is the case.
- **More than 10% of primary clients with critical protection status** – If more than 10 percent of clients generated a Protection status critical warning and have not connected to the server for more than a week the rule runs ASAP if this is the case.
- **Primary clients with protection status warning** – If there is at least one client with a protection status warning that has not connected to the server for at least one week.
- **Primary clients not connecting** – If there is at least one client that has not connected to the server for more than one week.
- **Primary clients with outdated virus signature database** – If there is a client with a virus signature database two or more versions older than the current one and has not been disconnected from the server for more than one week.
- **Primary clients with critical protection status** – If there is a client with a critical protection status warning that has not been disconnected for more than one week.
- **Primary clients with newer virus signature database than server** – If there is a client with a more recent virus signature database than the one on the server and that has not been disconnected for more than one week.
- **Primary clients waiting for restart** – If there is a client waiting for a restart that has not been disconnected for more than one week.
- **Primary clients with a non-cleaned infiltration in computer scan** – If there is a client on which a computer scan could not clean at least one infiltration and that client has not been disconnected for more than one week; the rule runs ASAP if this is the case.
- **Completed task** – If there was a task completed on a client; the rule runs ASAP if this is the case.
- **New primary clients** – If a new client has connected to the server; the rule runs ASAP if this is the case.
- **New replicated clients** – If there is a new replicated client in the list of clients; the rule runs after one hour if this is the case.
- **Possible virus outbreak** – If the frequency of Threat log entries on a client has exceeded 1000 critical warnings in one hour on at least 10% of all clients.
- **Possible network attack** – If the frequency of ESET Personal firewall log entries on a client has exceeded 1000 critical warnings in one hour on at least 10% of all clients.
- **Server updated** – If the server has been updated.
- **Server not updated** – If the server has not been updated for more than five days; the rule runs ASAP if this is the case.
- **Error in server text log** – If the server log contains an error entry.
- **License expiration** – If the current license will expire within 20 days and after expiration, the maximum number of client slots will be lower than the current number of clients; the rule runs ASAP if this is the case.
- **License limit** – If the number of free client slots decreases under 10% of all client slots available.

If not stated otherwise, all rules are run and repeated after 24 hours and are applied to the primary server and primary clients.

2. The **Options** section in the bottom half of the window provides information about the currently selected rule. All fields and options in this section are described using the sample rule from chapter Rule creation 104.

In each rule, you can specify the criteria, known as a **Trigger**, which activates the rule. The following triggers are available:

- Client State 98 – Rule will be run if there is a problem on some of the clients.

- Server State 99 – Rule will be run if there is a problem on some of the servers.
- Finished Task Event 101 – Rule will be run after the specified task is finished.
- New Client Event 101 – Rule will run if there is a new client connecting to the server (including replicated clients).
- Outbreak Event 101 – Rule will be run if there is an outbreak of incidents on a significant amount of clients.
- Received Log Event 102 – Rule will be run in case the administrator wants to be notified about logs in a certain time interval.

Based on the type of trigger other rule options can be activated or deactivated, therefore we recommend to set the trigger type first when creating new rules 104.

The **Priority** drop-down menu allows you to select rule priority. **P1** is the highest priority, **P5** is the lowest priority. Priority does not in any way affect the functionality of rules. To assign priority to notification messages, the *%PRIORITY%* variable can be used. Under the **Priority** drop-down menu, there is a **Description** field. We recommend that each rule is given a meaningful description, such as *"rule that warns on detected infiltrations"*.

The notification format can be edited in the **Message** field in the bottom section of the Notification Manager main window. In the text you can use special variables *%VARIABLE_NAME%*. To view the list of available variables click **Show me options**.

- **Rule_Name**

- **Rule_Description**

- **Priority** – Notification rule priority (P1 is the highest priority).
- **Triggered** – Date of the most recent notification sent (repeats excluded).
- **Triggered_Last** – Date of the most recent notification sent (repeats included).
- **Client_Filter** – Client filter parameters.
- **Client_Filter_Short** – Client filter settings (in short form).
- **Client_List** – List of clients.
- **Parameters** – Rule parameters.

- **Primary_Server_Name**

- **Server_Last_Updated** – Last update of the server.
- **Virus_Signature_DB_Version** – Latest virus signature database version.
- **Pcu_List** – Latest list of all PCUs.
- **Pcu_List_New_Eula** – Latest list of all PCUs with a new EULA.
- **Last_Log_Date** – Date of the last log.
- **Task_Result_List** – List of finished tasks.
- **Log_Text_Truncated** – Log text that activated the notification (truncated).
- **License_Info_Merged** – License information (summary).
- **License_Info_Full** – License information (full).
- **License_Days_To_Expiry** – Days left until license expiration.
- **License_Expiration_Date** – Nearest expiration date.
- **License_Clients_Left** – Free slots in the current license for clients to connect to the server.
- **Actual_License_Count** – Number of clients currently connected to the server.

5.4.1 Client State

Define client filtering parameters in the **Client filter** window. When a rule is applied, only clients meeting the client filter criteria are taken into consideration. The filtering criteria are:

- **FROM Primary Server** – Only clients from primary server (the negative NOT FROM can also be applied).
- **Primary Server IN** – Includes primary server in the output.
- **HAS New Flag** – clients marked by the flag *"New"* (the negative HAS NOT can also be applied).
- **ERA Groups IN** – Clients belonging to the specified group.
- **Domain/Workgroup IN** – Clients belonging to the specified domain.
- **Computer Name Mask** – Clients with the specified computer name.
- **HAS IPv4 Mask** – Clients falling into the specified IPv4 mask.
- **HAS IPv4 Range** – Clients within the specified IPv4 address range.
- **HAS IPv6 Network Prefix** – Clients with the specific IPv6 Network Prefix.
- **HAS IPv6 Range** – Clients within the specified IPv6 address range.
- **HAS Defined Policy** – Clients with the specified policy assigned (the negative HAS NOT can also be applied).

After you have specified a client filter for your notification rule, click **OK** and proceed to the rule parameters. Client parameters define what condition a client or a group of clients must meet in order to run the notification action. To view the available parameter, click the **Edit...** button in the **Parameters** section.

The availability of parameters depends on the selected Trigger type. The following parameters are available for Client State Triggers:

- **Protection Status Any Warnings** – Any warning found in the Protection Status column.
- **Protection Status Critical Warnings** – A critical warning found in the Protection Status column.
- **Virus Signature DB version** – Problem with virus signature database (6 possible values):

- **Previous** – Virus signature database is one version older than the current one.
- **Older or N/A** – Virus signature database is more than one version older than the current one.
- **Older than 5 versions or N/A** – Virus signature database is more than 5 versions older than the current one.
- **Older than 10 versions or N/A** – Virus signature database is more than 10 versions older than the current one.
- **Older than 7 days or N/A** – Virus signature database is more than 7 days older than the current one.
- **Older than 14 days or N/A** – Virus signature database is more than 14 days older than the current one.

- **Last Connected Warning** – The last connection was established before the specified time period.
- **Has Last Threat Event** – The Threat column contains a threat warning.
- **Has Last Event** – The Last Event column contains an entry.
- **Has Last Firewall Event** – The Firewall Event column contains a firewall event entry.
- **Has New Flag** – Client has the "New" flag.
- **Waiting For Restart** – Client is waiting for restart.
- **Last Scan Found Threat** – On the client, the specified number of threats was found during the last scan.
- **Last Scan Not Cleaned Threat** – On the client, the specified number of uncleaned threats was found during the last scan.

All parameters can be negated, but not all negations are usable. It is only suitable to negate those parameters that include two logical values: true and not true. For example, the parameter **Has New Flag** only covers clients with the *"New"* flag. The negative parameter would include all clients that are not marked by the flag.

All conditions above can be logically combined and inverted. **The rule is applied when** drop down-menu offers two choices:

- **all of the options are met** – Rule will only run if **all** specified parameters are met.

- **any of the options is met** – Rule will run if at least **one** condition is met.

If the specified parameters for a rule are met, the action defined by the administrator is automatically performed. To configure actions, click **Edit...** in the Action 103 section.

Activation of the rule can be delayed to a time period ranging from one hour to three months. If you wish to activate the rule as soon as possible, select **ASAP** from the **Activation after** drop-down menu. The Notification Manager is activated every 10 minutes by default, so if you select **ASAP**, the task should run within 10 minutes. If a specific time period is selected from this menu, the action will automatically be performed after the time period has elapsed (provided that the rule condition is met).

The **Repeat after every...** menu allows you to specify a time interval after which the action will be repeated. However, the condition to activate the rule must still be met. In **Server** > **Advanced** > **Edit Advanced Settings** > **ESET Remote Administrator** > **Server** > **Setup** > **Notifications** > **Interval for notification processing (minutes)** you can specify the time interval in which the server will check and execute active rules.

The default value is 10 minutes. We do not recommend decreasing it, since this may cause significant server slowdown.

5.4.2 Server State

The **Server rule parameters** window lets you setup parameters to trigger a specific server-state-related rule that is then applied to sending notifications. To setup a parameter, click the radio button next to a specific condition. This will activate the adjacent active elements of the GUI to allow you modify the parameter(s) of a condition.

- **Server updated** – Server is up to date
- **Server not updated** – Server is not up to date for longer than specified
- **Audit log** – The **Audit Log** monitors and logs all changes to the configuration and performed actions by all ERAC users. You can filter the log entries by type, see **Server log**.
- **Server log** – The server log contains the following entry types:

  - **Errors** – Error messages

  - **Errors+Warnings** – Error messages and warning messages

  - **Errors+Warnings+Info(Verbose)** - Error, warning and informative messages

- **Filter log entries by type** – Enable this option to specify error and warning entries to be watched in the server log. Note that for notifications to work properly the log verbosity (**Tools > Server Options > Logging**) must be set to the corresponding level. Otherwise such notification rules would never find a trigger in the server log. The following log entries are available:

– **ADSI_SYNCHRONIZE** – Active Directory group synchronization.
– **CLEANUP** – Server cleanup tasks.
– **CREATEREPORT** – On-demand report generating.
– **DEINIT** – Server shutdown.
– **INIT** – Server startup.
– **INTERNAL 1** – Internal server message.
– **INTERNAL 2** – Internal server message.
– **LICENSE** – License administration.
– **MAINTENANCE** – Server maintenance tasks.
– **NOTIFICATION** – Notification management.
– **PUSHINST** – Push install.
– **RENAME** – Internal structure renaming.
– **REPLICATION** – Server replication.
– **POLICY** – Policy management.
– **POLICYRULES** – Policy rules.
– **SCHEDREPORT** – Automatically generated reports.
– **SERVERMGR** – Internal server thread management.
– **SESSION** – Server's network connections.
– **SESSION_USERACTION** - Various user actions.
– **THREATSENSE** – ESET Live Grid – Statistical information submission.
– **UPDATER** – Server update and mirror creation.

One example of a helpful parameter is UPDATER, which sends a notification message when the Notification Manager finds a problem related to update and mirror creation in the server logs.

- **License Expiration** – License will expire in the specified number of days, or it already has expired. Select **Warn only if this will cause the number of clients in the license to fall below the number of actual clients in the server database** to send a notification if expiration will cause the number of clients in the license to fall below the number of currently connected clients.

- **Limit license** – If the percententage of free clients falls under the specified value.

If the specified parameters for a rule are met, the action defined by the administrator is automatically performed. To configure actions, click **Edit...** in the Action 103 section.

Activation of the rule can be delayed to a time period ranging from one hour to three months. If you wish to activate the rule as soon as possible, select **ASAP** from the **Activation after** drop-down menu. The Notification Manager is activated every 10 minutes by default, so if you select **ASAP**, the task should run within 10 minutes. If a specific time period is selected from this menu, the action will automatically be performed after the time period has elapsed (provided that the rule condition is met).

The **Repeat after every...** menu allows you to specify a time interval after which the action will be repeated. However, the condition to activate the rule must still be met. In **Server** > **Advanced** > **Edit Advanced Settings** > **ESET Remote Administrator** > **Server** > **Setup** > **Notifications** > **Interval for notification processing (minutes)** you can specify the time interval in which the server will check and execute active rules.

The default value is 10 minutes. We do not recommend decreasing it, as this may cause significant server slowdown.

5.4.3 Finished Task Event

Rule will be triggered after the selected tasks are completed. In **Default** settings, all task 77 types are selected.

If the specified parameters for a rule are met, the action defined by the administrator is automatically performed. To configure actions, click **Edit...** in the Action 103 section.

Activation of the rule can be delayed to a time period ranging from one hour to three months. If you wish to activate the rule as soon as possible, select ASAP from the **Activation after** drop-down menu. The Notification Manager is activated every 10 minutes by default, so if you select **ASAP**, the task should run within 10 minutes. If a specific time period is selected from this menu, the action will automatically be performed after the time period has elapsed (provided that the rule condition is met).

5.4.4 New Client Event

Define new client filtering parameters in the **Client filter** window. When a rule is applied, only clients meeting the client filter criteria are taken into consideration. The filtering criteria are:

- **FROM Primary Server** – Only clients from primary server (the negative NOT FROM can also be applied)
- **Primary Server IN** – Includes primary server in the output
- **HAS New Flag** – clients marked by the flag *"New"* (the negative HAS NOT can also be applied).
- **ERA Groups IN** – Clients belonging to the specified group.
- **Domain/Workgroup IN** – Clients belonging to the specified domain.
- **Computer Name Mask** – Clients with the specified computer name.
- **HAS IPv4 Mask** – Clients falling into the specified IPv4 mask.
- **HAS IPv4 Range** – Clients within the specified IPv4 address range.
- **HAS IPv6 Network Prefix** – Clients with the specified IPv6 address range.
- **HAS IPv6 Range** – Clients within the specified IPv6 address range.
- **HAS Defined Policy** – Clients with the specified policy assigned (the negative HAS NOT can also be applied).

If the specified parameters for a rule are met, the action defined by the administrator is automatically performed. To configure actions, click **Edit...** in the Action 103 section.

Activation of the rule can be delayed to a time period ranging from one hour to three months. If you wish to activate the rule as soon as possible, select **ASAP** from the **Activation after** drop-down menu. The Notification Manager is activated every 10 minutes by default, so if you select **ASAP**, the task should run within 10 minutes. If a specific time period is selected from this menu, the action will automatically be performed after the time period has elapsed (provided that the rule condition is met).

5.4.5 Outbreak Event

This notification is triggered as soon as the defined criteria for an outbreak of incidents is met and does not report every single incident or incidents exceeding the defined criteria.

Define filtering parameters for an Outbreak Event in the **Client filter** window. When a rule is applied, only clients meeting the client filter criteria are taken into consideration. The filtering criteria are:

- **FROM Primary Server** – Only clients from primary server (the negative NOT FROM can also be applied).
- **Primary Server IN** – Includes primary server in the output.
- **HAS New Flag** – clients marked by the flag *"New"* (the negative HAS NOT can also be applied).
- **ERA Groups IN** – Clients belonging to the specified group.

- **Domain/Workgroup IN** – Clients belonging to the specified domain.
- **Computer Name Mask** – Clients with the specified computer name.
- **HAS IPv4 Mask** – Clients falling into the specified IPv4 mask.
- **HAS IPv4 Range** – Clients within the specified IPv4 address range.
- **HAS IPv6 Network Prefix** – Clients with the specified IPv6 address range.
- **HAS IPv6 Range** – Clients within the specified IPv6 address range.
- **HAS Defined Policy** – Clients with the specified policy assigned (the negative HAS NOT can also be applied).

After you have specified a client filter for your notification rule, click **OK** and proceed to the rule parameters. Client parameters define what condition a client or a group of clients must meet in order to run the notification action. To view the available parameter, click the **Edit...** button in the **Parameters** section.

- **Log type** – Select the type of the log you want to monitor.
- **Log level** – Log entry level in the given log
  - **Level 1 – Critical Warnings** – Critical errors only.
  - **Level 2 – Above + Warnings** – The same as 1, plus alert notifications.
  - **Level 3 – Above + Normal** – The same as 2, plus informative notifications.
  - **Level 4 – Above + Diagnostic** – The same as 3, plus diagnostic notifications.
- **1000 occurrences in 60 minutes** – Type the number of occurrences and select the time period to specify the event frequency that must be reached for the notification to be sent. The default frequency is 1000 occurrences in one hour.
- **Amount** – Number of clients (either absolute or in percent).

The **Throttle interval** is the time interval used for sending the notifications. For example, if the throttle interval is set to 1 hour, the data is collected in the background and you will get the notification every hour (in case the outbreak still exists and the trigger is active).

5.4.6 Received Log Event

This option is used when you want to be notified about every log in certain time interval.

Define client filtering parameters in the **Client filter** window. When a rule is applied, only clients meeting the client filter criteria are taken into consideration. The filtering criteria are:

- **FROM Primary Server** – Only clients from primary server (the negative NOT FROM can also be applied).
- **Primary Server IN** – Includes primary server in the output.
- **HAS New Flag** – clients marked by the flag *"New"* (the negative HAS NOT can also be applied).
- **ERA Groups IN** – Clients belonging to the specified group.
- **Domain/Workgroup IN** – Clients belonging to the specified domain.
- **Computer Name Mask** – Clients with the specified computer name.
- **HAS IPv4 Mask** – Clients falling into the specified IPv4 mask.
- **HAS IPv4 Range** – Clients within the specified IPv4 address range.
- **HAS IPv6 Network Prefix** – Clients with the specified IPv6 address range.
- **HAS IPv6 Range** – Clients within the specified IPv6 address range.
- **HAS Defined Policy** – Clients with the specified policy assigned (the negative HAS NOT can also be applied).

After you have specified a client filter for your notification rule, click **OK** and proceed to the rule parameters. Client parameters define what condition a client or a group of clients must meet in order to run the notification action. To view the available parameter, click the **Edit...** button in the **Parameters** section.

- **Log type** – Select the type of the log you want to monitor.

- **Log level** – Log entry level in the given log
  - **Level 1 – Critical Warnings** – Critical errors only.
  - **Level 2 – Above + Warnings** – The same as 1, plus alert notifications.
  - **Level 3 – Above + Normal** – The same as 2, plus informative notifications.
  - **Level 4 – Above + Diagnostic** – The same as 3, plus diagnostic notifications.

If the specified parameters for a rule are met, the action defined by the administrator is automatically performed. To configure actions, click **Edit...** in the Action 103 section.

The **Throttle interval** is the time interval used for sending the notifications. For example, if the throttle interval is set to 1 hour, the data is collected in the background and you will get the notification every hour (in case the trigger is still active).

5.4.7 Action

If the specified parameters for a rule are met, the action defined by the administrator is automatically performed. To configure actions, click **Edit...** in the **Actions** section. The action editor offers these options:

- **E-mail** – The program sends the notification text of the rule to the specified email address; in **Subject** you can specify the subject. Click **To** to open the address book.

- **SNMP Trap** – Generates and sends SNMP notifications.

- **Execute (on server)** - Enable this option and specify application to be run on the server. Enter the full path to the application.

- **Log To File** – Generates log entries in the specified log file. Enter the full path to the folder; the **Verbosity** of notifications can be configured.

- **Log to Syslog** – Record notifications to system logs; the **Verbosity** of notifications can be configured.

- **Logging** – Logs notifications to server logs; the **Verbosity** of notifications can be configured.

- **Execute Report** – After selecting this option, the **Template name** drop-down menu becomes clickable. Here, select a template you want to use for the report. For more information about the templates, see the chapter Reports 37.

For this feature to work correctly, you must enable logging in the ERA Server (**Tools** > **Server Options** > **Logging**).

5.4.8 Notifications via SNMP Trap

SNMP (Simple Network Management protocol) is a simple and wide spread management protocol suitable for monitoring and identifying network problems. One of the operations of this protocol is TRAP, which sends specific data. In ERA, we use TRAP to send notification messages to SNMP.

Notifications can be viewed in the SNMP manager, which must be connected to an SNMP server where the configuration file *eset_ras.mib* is imported. The file is a standard component of an installation of ERA, and is usually located in the "*C:\Program Files\ESET\ESET Remote Administrator\Server\*" folder.

NOTE: For notifications to work, both the SNMP Service and SNMP TRAP services must be running in the Windows operating system hosting the ERA Server. Additionally, you must have software that can read and display SNMP TRAP information running.

For Windows 2000

In order for the TRAP tool to run effectively, the SNMP protocol must be installed and configured on the same computer as ERAS. You can add the SNMP protocol under **Start** > **Control Panel** > **Add or Remove programs** > **Add/ Remove Windows Components**. The SNMP service should be configured as described in the following Microsoft Knowledge Base article: http://support.microsoft.com/kb/315154. In ERAS, you must activate an SNMP notification rule.

5.4.9 Rule creation example

The following steps demonstrate how to create a rule that will send email notification to the administrator if there is a problem with the Protection Status of any client workstations. The notification will also be saved to a file named *log.txt*.

1) Set the **Trigger type** drop-down menu to **Client State**.
2) Leave the options **Priority, Activation after:** and **Repeat after every:** at the predefined values. The rule will automatically be assigned priority 3 and will be activated after 24 hours.
3) In the **Description** field, type **protection status notification for clients in HQ group**.
4) Click **Edit...** in the **Client filter** section and only activate the **ERA Groups IN** section rule condition. In the lower part of this window click the link **specify** and type *HQ* in the new window. Click **Add** and then click **OK** (twice) to confirm. This designates that the rule is only applied to clients from the HQ group.
5) Further specify parameters for the rule in **Parameters > Edit...** Deselect all options except for **Protection Status Any Warnings**.
6) Proceed to the **Action** section and click the **Edit...** button. In the **Action** window, activate **Email**, specify recipients (**To...**) and **Subject** for the email. Then select the **Log to file** check box and enter the name and path of the log file to be created. As an option, you can select the **Verbosity** of the log file. Click **OK** to save the action.
7) Finally, use the **Message** text area to specify the verbiage that will be sent in the body of the email when the rule is activated. Example: *"The client %CLIENT_LIST% reports protection status problem"*.
8) Click **Save as...** to name the rule, e.g., *"protection status problems"* and select the rule in the list of notification rules.

The rule is now active. If there is a problem with the protection status on a client from the HQ group, the rule will be run. The administrator will receive an email notification with an attachment containing the name of the problematic client. Click **Close** to exit the Notification Manager.

5.5 Detailed information from clients

ERA allows you to extract information about running processes, startup programs, etc. from client workstations. This information can be retrieved using the integrated ESET SysInspector tool, which is integrated directly with ERAS. Along with other useful functions, ESET SysInspector thoroughly examines the operating system and creates system logs. To open it, click **Tools** > **ESET SysInspector** from the ERAC main menu.
If there are problems with a specific client, you can request an ESET SysInspector log from that client. To do so, right-click the client in the **Clients** pane and select **Request data** – **Request SysInspector Information**. Logs can only be obtained from generation 4.x products and later; earlier versions do not support this feature. A window with the following options will appear:

- **Create snapshot (remember resulting log also on the client)** – Saves a copy of the log to the client computer.
- **Include comparison to the last snapshot before specified time** – Displays a comparative log, comparative logs are created by merging the current log with a previous log if available. ERA will choose the first log that is older than the specified date.

Click **OK** to obtain the selected logs and save them to the server. To open and view the logs, proceed as follows:

ESET SysInspector options for individual client workstations can be found in the **Client Properties** – **SysInspector** tab. The window is divided into three sections; the top section shows text information about the most recent logs from the given client. Click **Refresh** to load the most current information.

The middle section of the **Request Options** window is almost identical to the window which appears in the above described process of requesting logs from client workstations. The **Request** button is used to get an ESET SysInspector log from the client.

The bottom section is comprised of these buttons:

- **View** – Opens the log listed in the top section directly in ESET SysInspector.
- **Save As...** – Saves the current log to a file. **Then Run ESET SysInspector Viewer to view this file** option automatically opens the log after it is saved (as it would after clicking **View**).

Generating and displaying new log files can sometimes be slowed by the local client, due to the size of the log and data transfer speed. The date and time assigned to a log in **Client Properties** > **SysInspector** marks the date and time of delivery to the server.

5.6 Firewall Rules Merge Wizard

Firewall Rules Merge Wizard allows you to merge the firewall rules for selected clients. This is especially useful when you need to create a single configuration containing all firewall rules that were gathered by clients in learning mode. The resulting configuration can then be sent to clients via a configuration task or can be applied as a policy.

The wizard is accessible from the **Tools** drop-down menu and from the context menu in the **Clients** tab after right-clicking selected clients (the selected clients are then automatically added to the selected items in the first step).

NOTE: To perform this action successfully, all selected clients must have the latest configuration stored (sent or replicated) on the server. You need to choose the clients or groups of clients from which the firewall rules will be merged. In the next step you will see a list of selected clients and their configuration status. If a client's configuration is not on the server, you can request it by clicking the **Request** button. Finally, you will be able to choose which of the merged rules are to be used in the configuration and save them to an *.xml* file.

6. ERA Server Options

ERA Server can be easily configured directly from ERA Console connected to ERA Server - the option **Tools** > **Server Options...**.

6.1 General

The **General** tab shows the basic ERA Server information:

- **Server information** - In this section, you can see the basic ERA Server information. Click the Change Password... button to open the Security 107 tab of the ERA Server Options.
- **License information** - Shows the number of ESET Security products client licenses you have purchased and the current version of the NOD32 antivirus system or ESET Endpoint Security on the server's computer. If your license has expired and you have acquired a new one, click the License manager 106 button to open a dialog where you can browse for a new license to activate ERA.
- **Virus signature DB version** - Shows the current version of the virus signature DB version (based on the provided update information and security products used).
- **Performance** - Shows the Server-Client connection and general performance information.

6.1.1 License management

In order for ERA to function properly, a license key must be uploaded. After purchase, license keys are delivered along with your username and password to your email. The **License manager** serves to manage licenses.

In ERA 3.x and later, support for multiple license keys has been added. This feature makes management of license keys more convenient.

The main License Manager window is accessible from **Tools** > **License manager**.

To add a new license key:

1) Navigate to **Tools** > **License manager** or press **CTRL + L** on your keyboard.

2) Click **Browse** and find the desired license key file (license keys have the extension *.lic*).

3) Click **Open** to confirm.

4) Verify that the license key information is correct and select **Upload to Server.**

5) Click **OK** to confirm.

The **Upload to Server** button is only active if you have selected a license key (using the **Browse** button). Information about the currently viewed license key is shown in this part of the window. This allows for a final check before the key is copied to the server.

The central part of the window displays information about the license key which is currently used by the server. To see details about all license keys present on the server, click the **Details...** button.

ERAS is capable of selecting the most relevant license key and merging multiple keys into one. If there is more than one license key uploaded, ERAS will always try to find the key with the most clients and furthest expiration date.

The ability to merge multiple keys works if all keys are owned by the same customer. Merging licenses is a simple process which creates a new key containing all clients involved. The expiration date of the new license key becomes the expiration date of the key that would expire first.

The bottom part of the License Manager window is dedicated to notifications when there is a problem with licenses. The available options include:

- **Warn if the server is about to expire in 20 days** – Displays a warning X days before license expires
- **Warn only if this will cause the number of clients in the license to fall below the number or actual clients in the**

server database – Activate this option to only show a warning if the expiration of the license key or a part of the license will cause a decrease in the number of clients below the number of currently connected clients, or clients in the ERAS database

- **Warn if there is only 10% free clients left in the server license** – Server will display a warning if the number of free client slots falls under specified value (in %)

ERAS is capable of merging multiple licenses from multiple customers. This feature must be activated by a special key. If you need a special key, please specify it in your order, or contact your local ESET distributor.

6.2 Security

Versions 3.x and later of ESET security solutions (ESET Endpoint Security, etc.) offer password protection for decrypted communication between the client and the ERAS (communication at the TCP protocol, port 2222). Earlier versions (2.x) do not have this functionality. To provide backward compatibility for earlier versions, **Enable unauthenticated access for Clients** must be selected. The **Security** tab contains options that allow the administrator to use 2.x and 3.x security solutions in the same network simultaneously.

Protection for communication with an ERA Server.

NOTE: If authentication is enabled both in the ERAS and on all (generation 3.x and later) clients, **Enable unauthenticated access for Clients** can be disabled.

Console security settings

- **Use Windows/Domain authentication -** Enables Windows/Domain authentication and allows you to define administrator groups (with full access to the ERA Server) as well as groups with read-only access (select **Treat all other users as with read-only access**). If this check box is selected, the option **Allow read-only access for Windows/domain users with no ERA Server User assigned** becomes active and can be selected. This option ensures that these users can not change settings in the ERAC. If you want to assign ERA Server users, click **User Manager**.
- The user console access can be managed through the User Manager 108 tool.

Server security settings

- **Password for clients** – Sets the password for clients accessing the ERAS.
- **Password for replication** – Sets password for lower ERA Servers if replicated to the given ERAS.
- **Password for ESET Remote Installer (Agent)** – Sets the password for the installer agent to access the ERAS (relevant for remote installations).
- **Enable unauthenticated access for Clients (ESET Security Products)** – Enables access to the ERAS for clients that do not have a valid password specified (if the current password is different from the **Password for clients**).
- **Enable unauthenticated access for Replication** – Enables access to the ERAS for clients of lower ERA Servers that do not have a valid password for replication specified.
- **Enable unauthenticated access for ESET Remote Installer (Agent)** – Enables access to the ERAS for ESET Remote Installers that do not have a valid password specified.

NOTE: **Default** only restores predefined settings - it does not reset your passwords.

NOTE: If you want to increase security, you can use complex passwords. Go to **Tools** > **ESET Configuration Editor** > **Remote Administration** > **ERA Server** > **Settings** > **Security** > **Requires complex password** and set this option to **Yes**. With this option enabled, every new password has to be at least 8 characters long, contain a lowercase and an uppercase letter and a non-letter character.

6.2.1 User Manager

The **User Manager** tools allows you to administer user accounts for Console-Server authentication. The Administrator (full-access) and Read-Only accounts are predefined.

Click **New** to add a new user account for the Console-Server authentication. Define the **User Name**, the **Password** and the specific **Permissions**.

The **Description** field is for custom descriptions of the user, and is not mandatory.

The **Permissions** define the level of access the user has and the specific tasks he can perform. You can change the Console Access Password 108 for each user accessing the console by selecting the specific user, and then click **Change...** next to **Password for console authentication**.

NOTE: The permissions for the predefined accounts (Administrator and Read-Only) can't be modified.

You can attach one or more **Windows/Domain authentication groups** to a selected ERA Server user. If a Windows/ Domain group is assigned to multiple users, first user from the list of users will be used. The up and down arrows next to the list of user define the order of users.

6.2.2 Console Access Password

To change the Console access password, click **File** > **Change Password** or change the password using the User Manager 108. Enter your old password, then the new password twice (for confirmation). If you select the check box next to **Also change password stored in cache**, the cached password used on the start of the application (so the user does not need to type it in every time he accesses the ERAC) will be changed.

NOTE: Passwords you set in this dialog are sent directly to the server. This means that the change is performed immediately after clicking **OK** and can not be reversed.

6.3 Server Maintenance

If correctly configured in the **Server Maintenance** tab, the ERA Server database will be maintained automatically and optimized with no need for further configuration. You can define the following cleanup settings:

- **Log collecting parameters...** – Defines the level of logs which are received by the server.
- **Cleanup Settings...** – Deletes the logs by time parameter.
- **Advanced Cleanup Settings...** – Deletes the logs by count of log records.

Specify how many log entries should be kept after the cleanup and the level of logs which are received by the server. For example, if you choose **Delete all threat logs except last 600000 records** in Advanced Cleanup Settings by Count of Log Records 110 and the level of Log Collecting Parameters 109 for **Threats** is defined as **Level 3 - Above +Normal**, the last 600000 records that contain information about critical errors, alert notifications and informative notifications will be kept in the Database. You can also limit the log entries using the Cleanup by Time Parameter 109 .

Cleanup scheduler – Performs the above selected options at the specified interval. Click **Change...** next to this option to set the time parameters. Click **Clean Up Now** to start the cleanup immediately.

Compact & repair scheduler - Compacts the database in the specified time interval at the specified hour. Compacting and repairing eliminates inconsistencies and glitches and makes communication with the database faster. Click **Change...** next to this option to set the time parameters. Click **Compact Now** to start a compact & repair immediately.

NOTE: Both the **Cleanup** and the **Compact & repair** tools are time and resource intensive, so we recommend scheduling them to run when there is minimum load on the server (for example run the Cleanup at night, and the Compact & repair on weekends).

By default, entries and logs older than three/six months are deleted and the **Compact & repair** task is performed every fifteen days.

6.3.1 Log Collecting Parameters

Define the level of logs that are sent to the server. Select the verbosity level for each type of log using the corresponding drop-down menus.

None – No logs will be sent to the server. Because the client does not log anything using this setting, ERA can not receive any logs.

Level 1 - Critical Warnings – Critical errors only. Critical errors are not logged to the **Web Control** or **Device Control** tabs because the client can not produce such logs.

Level 2 - Above + Warnings – The same as level 1 plus alert notifications.

Level 3 - Above + Normal – The same as level 2 plus informative notifications. This verbosity level is called **Informational** instead of **Normal** on the client side.

Level 4 - Above + Diagnostics – The same as level 3 plus diagnostic notifications. This verbosity level needs to be set on the client side too, the default setting on the client is **Informational** logging level.

All – All logs will be received.

6.3.2 Cleanup by Time Parameter

Main cleanup settings for cleanup by time interval:

- **Delete Clients not connected for the last X months (days)** – Deletes all clients that have not connected to ERAS for more than the specified number of months (or days).
- **Delete Threat logs older than X months (days)** – Deletes all virus incidents (detected threats) older than the specified number of months (or days).
- **Delete Firewall logs older than X months (days)** – Deletes all firewall logs older than the specified number of months (or days).
- **Delete Event logs older than X months (days)** – Deletes all system events older than the specified number of months (or days).
- **Delete HIPS logs older than X months (days)** – Deletes all HIPS (Host-based Intrusion Prevention System) logs older than the specified number of months (or days).
- **Delete Device Control logs older than X months (days)** – Deletes all Device Control logs older than the specified number of months (or days).
- **Delete Web Control logs older than X months (days)** – Deletes all Web Control logs older than the specified number of months (or days).
- **Delete Antispam logs older than X months (days)** – Deletes all antispam logs older than the specified number of months (or days).
- **Delete Greylist logs older than X months (days)** – Deletes all greylist logs older than the specified number of months (or days).
- **Delete Scan logs older than X months (days)** – Deletes all scanner logs older than the specified number of months (or days).
- **Delete Mobile logs older than X months (days)** – Deletes all mobile logs older than the specified number of months (or days).
- **Delete quarantine entries with no clients that are older than X months (days)** – Deletes all quarantine entries that are not assigned to any client and are older than the specified number of months (or days).
- **Delete Unregistered computers entries that are older than X months (days)** – Deletes all unregistered computer entries (computers that are not managed by ERA) older than the specified number of months (or days).
- **Delete Tasks entries with done state only that are older than X months (days)** – Deletes all Tasks entries for Tasks

that are finished and done older than the specified number of months (or days).

- **Delete all Tasks entries that are older than X months (days)** – Deletes all Task entries (in any state) older than the specified number of months (or days).

6.3.3 Advanced Cleanup Settings by Count of Log Records

Advanced cleanup settings for cleanup by count of log records:

- **Delete Threat logs except last X records** – Deletes all virus incidents (detected threats) except the specified number of records.
- **Delete Firewall logs except last X records** – Deletes all firewall logs except the specified number of records.
- **Delete Event logs except last X records** – Deletes all system events except the specified number of records.
- **Delete HIPS logs except last X records** – Deletes all HIPS (Host-based Intrusion Prevention System) logs except the specified number of records.
- **Delete Device Control logs except last X records** – Deletes all Device Control logs except the specified number of records.
- **Delete Web Control logs except last X records** – Deletes all Web Control logs except the specified number of records.
- **Delete Antispam logs except last X records** – Deletes all antispam logs except the specified number of records.
- **Delete Greylist logs except last X records** – Deletes all greylist logs except the specified number of records.
- **Delete Scan logs except last X records** – Deletes all scanner logs except the specified number of records.
- **Delete Mobile logs except last X records** – Deletes all mobile logs except the specified number of records.

6.4 Logging

To set parameters for database maintanance, select **Tools/Server options** from the main ERA Console menu. Database maintanance provides options for keeping the logs transparent and enables compression of the main ERA database on a regular basis to preserve space.

1. Audit log

Audit log monitors and logs all changes to the configuration and performed actions by all ERAC users.

- If **Log to text file** is selected, new log files will be created (**Rotate when greater than X MB**) and deleted on a daily basis (**Delete rotated logs older than X days**). You can also change the log verbosity in the drop-down menu to the left.

Click View Log 112 to display the current Audit Log.

- **Log to OS application log** allows information to be copied to the system event viewer log (**Windows Control Panel** > **Administrative Tools** > **Event viewer**). You can also change the log verbosity in the drop-down menu to the left.
- **Log to Syslog** sends a syslog message to the specified syslog server on a specified port (default server is localhost, default port is 514) .For advanced syslog settings go to **Tools** > **Server Options** > **Advanced** >**Edit Advanced Settings...** > **Setup** > **Logging** . You can edit the syslog options here - syslog server name, syslog server port, syslog facility and the syslog verbosity.

NOTE: Syslog severity must be configured for each log type. For the server log, it is the setting **Syslog facility for server log**, for the debug log it is the setting **Syslog facility for debug log**. For these logs, the syslog severity is as follows:

ERA Verbosity	**Syslog Severity**
Level 1 (Informational)	LOG_INFO //6

Level 2 (Error)	LOG_INFO //3
Level 3 (Warning)	LOG_INFO //4
Level 4,5 (Debug)	LOG_INFO //7

The **Verbosity** of a log means the level of detail in a log and the information included.

- **Level 1 - Users and groups** – Log user and group related activity (static groups, parametric groups, add/remove client from a group, etc.).
- **Level 2 - Above + Client actions** – Above + all ERA client-related activity (set/clear new flag, set client policy, request data, etc.).
- **Level 3 - Above + Tasks and notifications** – Above + all Tasks-related activity (create/delete Task, create/delete Notification, etc.).
- **Level 4 - Above + Reports** – Above + all report-related activity (create/delete Report, select/delete Report Template).
- **Level 5 - All events** – All Log-related activity (clear HIPS Log, clear Threat Log, etc.).

2. Server log

While running, the ERA Server creates a server log (**Log filename**) about its activity which is configurable (**Log verbosity**).

NOTE: The text file output is by default saved to the file *%ALLUSERSPROFILE%\Application Data\Eset\ESET Remote Administrator\Server\logs\era.log*

- If **Log to text file** is selected, new log files will be created (**Rotate when greater than X MB**) and deleted on a daily basis (**Delete rotated logs older than X days**).

NOTE: In the **Log to text file** section we recommend leaving **Log verbosity** at *Level 2 – Above + Session Errors* and increasing it only if you experience a problem, or if advised to do so by ESET Customer Care.

- **Log to OS application log** allows information to be copied to the system event viewer log (**Windows Control Panel** > **Administrative Tools** > **Event viewer**).

- **Log to Syslog** sends a syslog message to the specified syslog server on a specified port (default server is localhost, default port is 514) .For advanced syslog settings go to **Tools** > **Server Options** > **Advanced** >**Edit Advanced Settings...** > **Setup** > **Logging .** Here you can edit the syslog options - syslog server name, syslog server port, syslog facility and the syslog verbosity.

The **Verbosity** of a log means the level of detail in a log and the information included.

- **Level 1 - Critical Information** – Faulty behavior (in this case, please contact ESET Customer Care).
- **Level 2 - Above + Important Session Information** – Information about server communication (who logged on to the ERA Server, when and why).
- **Level 3 - Above + Various Information** – Information about internal processes on the ERA Server.
- **Level 4 - Above + Installer** – Information about the einstaller.exe agent (information about the ERA Server - agent connection/disconnection and the results).
- **Level 5 - Above + Clients** – Client information (information about the ERA Server, client connection/disconnection and the results).

NOTE: We recommend leaving the Log verbosity set to Level 2 – Above + Session Errors. Change the log level only if you are experiencing problems, or if you are advised to do so by ESET Customer Care.

3. The database **Debug Log** option should be disabled under normal circumstances - it is used for troubleshooting database problems. Click **Tools** > **Server Options** > **Advanced** > **Edit Advanced Settings...** > **Setup** > **Logging** > **Rotated debug log compression** to configure the compression level for individual rotated logs.

6.4.1 Audit Log Viewer

The **Audit Log** monitors and logs all changes to configuration and actions performed by ERAC users. This helps the administrator keep track of all ERAC-related activity, including potential unauthorized access.

NOTE: The Audit Log Viewer displays changes logged to the database. The Audit Log doesn't include other logs (such as file log and others).

On the left side, you can see the **Filter** used to filter **Audit Log** entries. You can also select the number of **Items to show** from the drop-down menu in this module on the upper right side below the list of **Audit log** entries.

Filter:

- **From/To** – Select the specific time from/to during which you want the logs to be filtered. Selecting both options and selecting times creates a time interval.
- **User** – Enter the user(s) for which you want the logs to be displayed.
- **Domain login name** – Enter the domain login name of the user(s) for which you want the logs to be displayed.
- **IP address** – Select the desired option (**Address**, **Range** or **Mask**) and enter the address(es) in the appropriate fields. These options are common for both IPv4 and IPv6 addresses.
- **Action types** – Select the actions that you want shown in the audit logs. By default, all of them are selected and therefore displayed.
- **Apply filter** – Clicking this button immediately applies the filter parameters to the **Audit log**.
- **Default** – Clicking this button resets the filter parameters to their default state.

List of Audit log entries:

- **Date** – Date when the action was performed. This date and time is based on the server machine time settings.
- **User** – ERACuser that performed the action.
- **Login Name** – Windows domain login name of the user that performed the action. This is only displayed when the Windows/Domain login type is used.
- **Console IP Address** – IP Address of the console from which the action was performed by the ERAC user.
- **Action** – Action that was performed by the user.
- **Object** – Number of objects affected by this action.

NOTE: Additional information (if available) is shown after double-clicking on a particular line in the log.

6.5 Replication

To set the ERA Server settings, click **Tools** > **Server options** from the main program window of the ERA Console.

Replication is used in large networks where multiple ERA Servers are installed (e.g., a company with several branches). The **Replication settings** tab lets you set up data replication between multiple ERA Servers running in your network. To learn how to setup multiple ERA Servers in your organization see chapter Setting up RA servers in large networks 113.

To set up replication use the following replication options:

Replication "to" settings

- **Enable "to" replication** – Enables replication in a large network as described in the chapter Replication 113.
- **Upper server** – IP address or name of the upper ERA server, which will collect data from the local ERA server.
- **Port** - Specifies port used for replication.

- **Replicate every XX minutes** – Sets the replication interval.
- **Replicate: Threat log**, **Firewall log**, **Event log**, **Scan log**, **Mobile log**, **Quarantine log** - if these options are selected, all information displayed on the Clients, Threat Log, Firewall Log, Event Log, Scan Log, Tasks tab, Mobile Log and Quarantine Log is replicated in individual columns and lines. Information not stored directly in the database, but in individual files (i.e., *.txt* or *.xml* format) may not be replicated. Enable these options to also replicate entries in those files.
- **Automatically replicate: Client details**, **Threat log details**, **Scan log details**, **Mobile log details**, **Quarantine files** - these options enable automatic replication of the complementary information stored in individual files (they can also be downloaded on demand by clicking **Request**).
- **Log type** – Defines the type of events to be replicated (alert, event, scan) to the upper ERA server.
- **Automatically replicate...** – Enables periodic replication. When not enabled the replication can be triggered manually.

Replication "to" status

- **Replicate Up Now** – Initiates the replication process.
- **Mark all clients for replication** – If enabled, all clients will be replicated, including those with no changes.

Replication “From” settings

- **Enable “from” replication** – Enables the local ERA server to collect data from other servers listed in the **Allowed servers** field. Use a comma to separate multiple ERA servers.
- **Allow replication from any server** – If this check box is checked, you can replicate from any server. Checking this check box disables the **Allowed servers** field.

6.5.1 Replication in large networks

Replication is used in large networks where multiple ERA Servers are installed (e.g., a company with several branches). For more information, see chapter Installation 21.

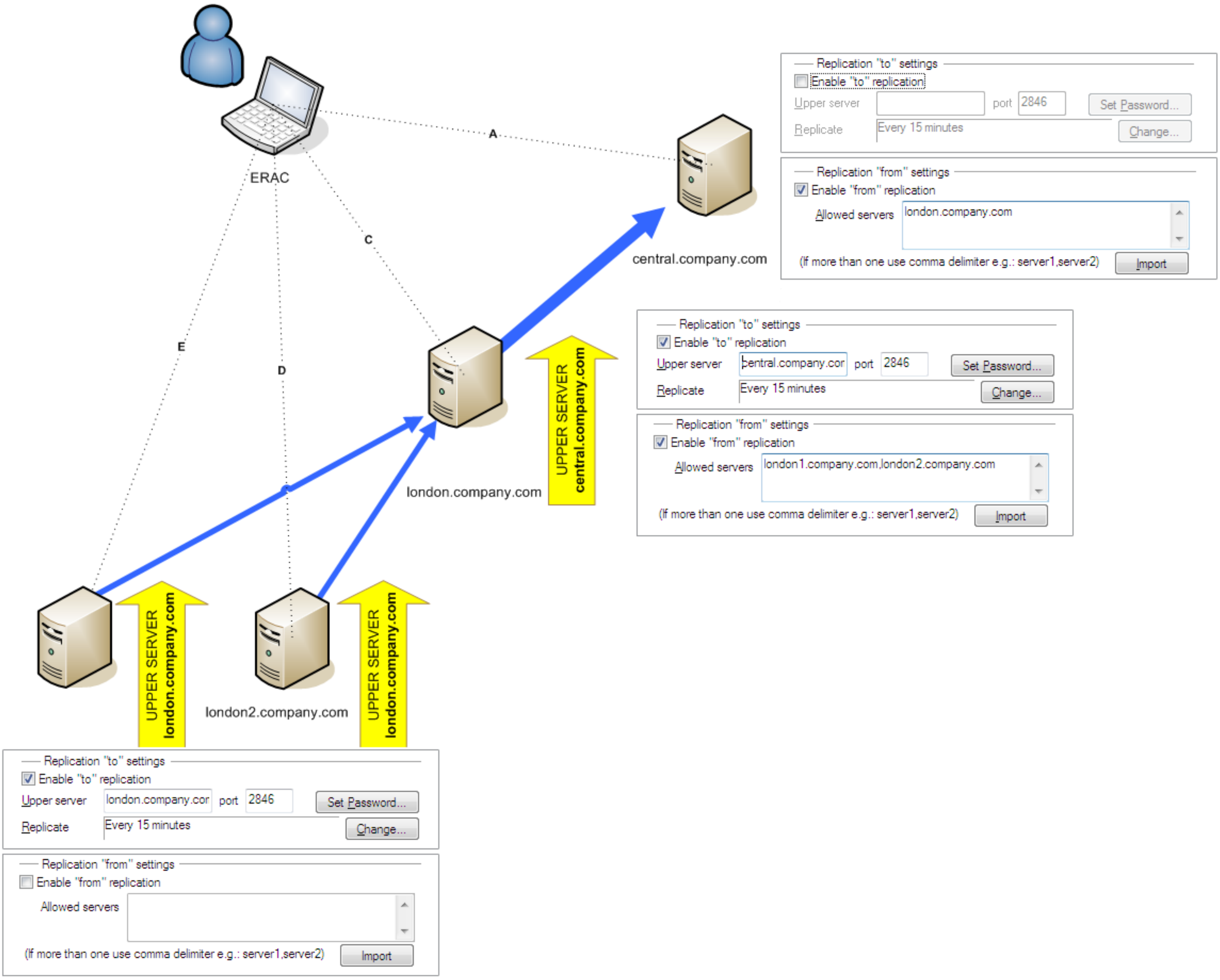
The options in the Replication tab (**Tools > Server Options...**) are divided into two sections:

- Replication “to“ settings
- Replication “from“ settings

The **Replication ”to“ settings** section is used to configure lower ERA Servers. The **Enable “to” replication** option must be enabled and the IP address or name of the master ERAS (Upper server) entered. Data from the lower server is then replicated to the master server. The **Replication ”from“ settings** allow master (upper) ERA Servers to accept data from lower ERA Servers, or to transfer them to their master servers. The **Enable “from“ replication** must be enabled and names of lower servers should be defined (delimited by a comma).

Both of these options must be enabled for ERA Servers located anywhere in the middle of the replication hierarchy (i.e., they have both upper and lower servers).

All of the previously mentioned scenarios are visible in the figure below. The beige computers represent individual ERA Servers. Each ERAS is represented by its name (which should be the same as *%Computer Name%* to avoid confusion) and the corresponding settings in the replication dialog window.


ERAC
A
C
D
E
central.company.com
london.company.com
london2.company.com
UPPER SERVER central.company.com
UPPER SERVER london.company.com
UPPER SERVER london.company.com

Replication "to" settings
☐ Enable "to" replication
Upper server port 2846 Set Password...
Replicate Every 15 minutes Change...

Replication "from" settings
☑ Enable "from" replication
Allowed servers london.company.com
(If more than one use comma delimiter e.g.: server1,server2) Import

Replication "to" settings
☑ Enable "to" replication
Upper server central.company.cor port 2846 Set Password...
Replicate Every 15 minutes Change...

Replication "from" settings
☑ Enable "from" replication
Allowed servers london1.company.com,london2.company.com
(If more than one use comma delimiter e.g.: server1,server2) Import

Replication "to" settings
☑ Enable "to" replication
Upper server london.company.cor port 2846 Set Password...
Replicate Every 15 minutes Change...

Replication "from" settings
☐ Enable "from" replication
Allowed servers
(If more than one use comma delimiter e.g.: server1,server2) Import

Other options that influence the replication behavior of servers include:

- **Replicate threat log**, **Replicate firewall log**, **Replicate event log**, **Replicate scan log**, **Replicate mobile log**, **Replicate quarantine log**
  If these options are selected, all information displayed on the **Clients**, **Threat Log**, **Firewall Log**, **Event Log**, **Scan Log**, **Mobile Log**, **Quarantine Log** and **Tasks** tab is replicated in individual columns and lines. Information not stored directly in the database, but in individual files (i.e., *.txt* or*.xml* format), may not be replicated. Enable these options to also replicate entries in those files.

- **Automatically replicate threat log details**, **Automatically replicate scan log details**, **Automatically replicate client details**, **Automatically replicate mobile log details**, **Automatically replicate quarantine files**
  These options enable automatic replication of the complementary information stored in individual files. They can also be downloaded on demand by clicking the **Request** button).

NOTE: Some logs are automatically replicated, while detailed logs and client configuration logs are only replicated on demand. This is because some logs contain large amounts of data that may not be relevant. For example, a scan log with the Log all files option enabled will consume a significant amount of disk space. Such information is usually not necessary and can be requested manually. Child servers do not automatically submit information about deleted clients. Therefore upper severs may continue to store information about deleted clients from lower servers. If you want to delete a client from the Client tab on upper servers, select the Enable deletion of replicated clients option on the underlying server located in **Server Options** > **Advanced** > **Edit Advanced Settings** > **Setup** > **Replication**.

To set the log maintenance level in ERAS, click **Tools** > **Server Options** > **Advanced** > **Edit Advanced Settings...** > **Setup** > **Server Maintenance**.

If you want to only replicate clients with a status change, select the **Tools** > **Server Options** > **Replication** > **Mark all**

clients for replication by "Replicate Up Now" option.

6.6 Updates

The **Updates** window, located in the **Server Options** module, serves to define update parameters for the ESET Remote Administrator Server. The window is divided into two sections: the upper one lists server updates options; the one below is dedicated to update mirror parameters. Since version 2.0, the ESET Remote Administrator Server includes the Mirror server 116 feature which creates a local update server for client workstations.

Descriptions of all elements and features are included below:

- **Update server** – This is ESET's update server. It is recommended that you use the predefined value (Autoselect)
- **Update interval** – Specifies the maximum interval between two consequent checks for the availability of new update files
- **Update user name** – Username of the user used by ESET Remote Administrator to authenticate to update server(s)
- **Update password** – password belonging to the given username

Regular Virus Signature Database and program component updates are key elements in ensuring timely detection of threats. However, network administrators managing large networks may occasionally experience update-related issues such as false alarms or module-related issues. There are three options for connecting to an update server:

- **Regular update** – The virus signature database is updated from regular update servers by the time they are released.
- **Pre-release update** – If the this option is enabled, beta-modules will be downloaded during the update. This is not recommended in a production environment, only for testing purposes.
- **Delayed update** – Enable this option to receive updates with a delay of 12 hours, i.e., updates tested in a production environment and considered to be stable.

To launch an update task to download all of the most recent components for ESET Remote Administrator, click **Update now**. Updates may contain important components or functionalities; therefore it is vital to make sure that updates work properly and automatically. If you experience problems updating, select **Clear Update Cache** to clear the temporary update files folder. The **Mirror Downloaded PCU** option becomes active when a PCU (*PCU - Program Component Upgrade*) upgrade is downloaded and needs to be confirmed manually. Click this button to see all available PCU Updates and the EULA. To set up PCU mirroring go to **Advanced** > **Edit Advanced Settings** and configure settings in **ESET Remote Administrator** > **ERA Server** > **Setup** > **Mirror**.
Configuration of a mirror in the ESET Remote Administrator Server is the same as it is in ESET Endpoint Antivirus Business Edition and ESET Endpoint Security Business Edition. Descriptions of important mirror elements are included below:

- **Create update mirror** – Activates the mirror feature. If this option is disabled, no update copies are created.
- **Create mirror for the selected program components** – Allows user to specify language variants and types of program components that will be created in the mirror.
- **Populate mirror with selected program component updates only on demand** – If enabled, PCUs are not automatically mirrored. If you want to enable PCU mirroring, select the **Mirror downloaded PCU** option in **Tools** > **Server Options** > **Updates**
- **Mirror folder** – Local or network directory dedicated to store update files.
- **Enable update distribution via HTTP** – Enables you to access updates using an internal HTTP server.
- **HTTP server port** – Defines the port on which the ESET Remote Administrator Server will provide update services.
- **HTTP server authentication** – Defines the method of authentication used for accessing update files. The following options are available: **NONE**, **Basic**, **NTLM**. Select **Basic** to use the base64 encoding with basic authentication. The option **NTLM** provides encoding using a safe encoding method. For authentication, users created on the workstation sharing update files are used.

Click **Default** in the section below to restore predefined values for all features in this window.

NOTE: If the HTTP server method is in use, we recommended a maximum of 400 clients updating from one mirror. In large networks with more clients, we recommend balancing mirror updates among more ERA (or ESS/EAV) mirror servers. If the mirror needs to be centralized on a single server, we recommend using another type of HTTP server, such as Apache. ERA also supports additional authentication methods (e.g., on Apache Web Server the .htaccess method is used).

The administrator must insert the product license key for a purchased product and enter the username and password to enable the Mirror feature in the ERAS. If the administrator uses a license key, username and password for ESET Endpoint Antivirus Business Edition, then later upgrades to ESET Endpoint Security Business Edition, the original license key, username and password must be replaced as well.

NOTE: ESET Endpoint Antivirus clients can also be updated using a ESET Endpoint Security license, but not vice versa.

6.6.1 Mirror server

The Mirror feature allows a user to create a local update server. Client computers will not download virus signature updates from ESET's servers on the Internet, but will connect to a local Mirror server on your network instead. The main advantages of this solution are to save Internet bandwidth and to minimize network traffic, since only the mirror server connects to the Internet for updates rather than hundreds of client machines. This configuration means it is important for the Mirror server to always be connected to the internet.

Warning: A Mirror server which performed a program component upgrade (PCU) and has not been rebooted may cause an outage. In this scenario, the server would be unable to download ANY updates or distribute them to client workstations. DO NOT SET AUTOMATIC PROGRAM COMPONENT UPGRADES FOR ESET SERVER PRODUCTS!

The Mirror feature is available in two locations:

- ESET Remote Administrator (Mirror physically running within ERAS, manageable from ERAC)
- ESET Endpoint Security Business Edition or ESET Endpoint Antivirus Business Edition (provided that the Business Edition has been activated by a license key).
- The Mirror is also available in ESET Endpoint Security and ESET Endpoint Antivirus. See documentation for the appropriate client product for more information.

The administrator selects the method for activating the Mirror feature.

In large networks it is possible to create multiple Mirror servers (e.g., for various company departments), and establish one as central (at company headquarters) in cascade-style – similar to an ERAS configuration with multiple clients.

The administrator must insert the product license key for a purchased product and enter the username and password to enable the Mirror feature in the ERAS. If the administrator uses a license key, username and password for ESET Endpoint Antivirus Business Edition, then later upgrades to ESET Endpoint Security Business Edition, the original license key, username and password must be replaced as well.

NOTE: ESET Endpoint Antivirus clients can also be updated using a ESET Endpoint Security license, but not vice versa. This also applies for the ESET Endpoint Antivirus and ESET Endpoint Security.

6.6.1.1 Operation of the Mirror server

The computer hosting the Mirror server should always be running, and connected to the Internet or to an upper Mirror server for replication. Mirror server update packages can be downloaded in two ways:

1. Using the HTTP protocol (recommended)
2. Using a shared network drive (SMB)

ESET's update servers use the HTTP protocol with authentication. A central Mirror server should access the update servers with a username (usually in the following form: *EAV-XXXXXXX*) and password.

The Mirror server which is a part of ESET Endpoint Security/ESET Endpoint Antivirus has an integrated HTTP server (variant 1).

NOTE: If you decide to use the integrated HTTP server (with no authentication), please ensure that it will not be accessible from outside your network (i.e., to clients not included in your license). The server must not be accessible from the Internet.

By default, the integrated HTTP server listens at TCP port 2221. Please make sure that this port is not being used by any other application.

NOTE: If the HTTP server method is in use, we recommend a maximum of 400 clients updating from one mirror. In large networks with more clients, we recommend balancing mirror updates among more ERA (or ESS/EAV) mirror servers. If the mirror needs to be centralized on a single server, we recommend using another type of HTTP server, such as Apache. ERA also supports additional authentication methods (e.g., on Apache Web Server the .htaccess method is used).

The second method (shared network folder) requires sharing (“read” rights) of the folder containing update packages. In this scenario, the username and password of a user with ”read” rights for the update folder must be entered into the client workstation.

NOTE: ESET client solutions use the SYSTEM user account and thus have different network access rights than a currently logged-in user. Authentication is required even if the network drive is accessible for ”Everyone” and the current user can access them, too. Also, please use UNC paths to define the network path to the local server. Using the *DISK:* format is not recommended.

If you decide to use the shared network folder method (variant 2), we recommend that you create a unique username (e.g., NODUSER). This account would be used on all client machines for the sole purpose of downloading updates. The NODUSER account should have ”read” rights to the shared network folder which contains the update packages.

For authentication to a network drive, please enter the authentication data in the full form: *WORKGROUP\User* or *DOMAIN\User*.

In addition to authentication, you must also define the source of updates for ESET client solutions. The update source is either a URL address to a local server (*http://Mirror_server_name:port*) or UNC path to a network drive: (*\\Mirror_server_name\share_name*).

6.6.1.2 Types of updates

In addition to virus signature database updates (which can include ESET software kernel updates), program component upgrades are also available. Program component upgrades add new features to ESET security products and require a reboot.

The Mirror server allows an administrator to disable automatic downloading of program upgrades from ESET‘s update servers (or from an upper Mirror server) and disable its distribution to clients. Distribution can later be triggered manually by the administrator, if he is sure there will be no conflict between the new version and existing applications.

This feature is especially useful if the administrator wishes to download and use virus signature database updates when there is also a new program version available. If an older program version is used in conjunction with the most recent virus database version, the program will continue to provide the best protection available. Still, we recommend that you download and install the newest program version to gain access to new program features.

By default, program components are not automatically downloaded and must be manually configured in ERAS. For more information see chapter How to enable and configure Mirror 118.

6.6.1.3 How to enable and configure the Mirror

If the Mirror is directly integrated into ERA, connect to ERAS using ERAC and follow these steps:

- From the ERAC click **Tools** > **Server Options...** > **Updates**.
- From the **Update server**: drop-down menu, select **Choose Automatically** (updates will be downloaded from ESET's servers), or enter the *URL/UNC* path to a Mirror server.
- Set the Update interval for updates (we recommend sixty minutes).
- If you selected **Choose Automatically** in the previous step, insert the username (Update username) and password (Update password) which were sent after purchase. If accessing an upper server, enter a valid domain username and password for that server.
- Select the **Create update mirror** option and enter a path to the folder which will store the update files. By default this is a relative path to the Mirror folder. As long as the check box next to **Provide update files via internal HTTP server** is selected, updates are available on the HTTP port defined in **HTTP server port** (by default 2221). Set **Authentication** to **NONE** (For more information see chapter Operation of the Mirror server 116).

NOTE: In case of problems with updates, select the **Clear Update Cache** option to flush the folder in which temporary update files are stored.

- The **Mirror Downloaded PCU** option allows you to activate mirroring of program components. To set up PCU mirroring go to **Advanced > Edit Advanced Settings** and configure settings in **ESET Remote Administrator** > **ERA Server** > **Setup > Mirror**.
- Select the language components to be downloaded in **Advanced** > **Edit Advanced Settings...** the branch **ERA Server** > **Setup** > **Mirror** > **Create Mirror for the selected program components**. Components for all language versions to be used in the network should be selected. Note that downloading a language version not installed in the network will unnecessarily increase network traffic.

The Mirror feature is also available directly from the program interface in ESET Endpoint Security Business Edition and ESET Endpoint Antivirus Business Edition, ESET Endpoint Security or ESET Endpoint Antivirus. It is left to the administrator's discretion as to which is used to implement the Mirror server.

To activate and launch the Mirror server from ESET Endpoint Security Business Edition or ESET Endpoint Antivirus Business Edition, follow these steps:

1) Install ESET Endpoint Security Business Edition , ESET Endpoint Antivirus Business Edition (client version 4.X), ESET Endpoint Security or ESET Endpoint Antivirus.
2) In the **Advanced Setup** window (F5), click **Miscellaneous** > **Licenses**. Click **Add...** , browse for the **.lic* file and click **Open**. This will install the license and allow configuration of the Mirror feature.
3) From the **Update** branch click **Setup...** and click the **Mirror** tab.
4) Select the check boxes next to **Create update mirror** and **Provide update files via internal HTTP server**.
5) Enter the full directory path to the folder (**Folder to store mirrored files**) where update files are to be stored.
6) The **Username** and **Password** serve as authentication data for client workstations attempting to gain access to the Mirror folder. In most cases, it is not required to populate these fields.
7) Set Authentication to **NONE**.
8) Select components to be downloaded (components for all language versions which will be used in the network should be selected). Components are only displayed if they are available from ESET's update servers.

NOTE: To maintain optimal functionality, we recommend that you enable downloading and mirroring of program components. If this option is disabled, only the virus signature database is updated, not program components. If the Mirror is used as a part of ERA, this option can be configured in the ERAC through **Tools** > **Server Options...** > **Advanced** tab > **Edit Advanced Settings...** > **ESET Remote Administrator** > **ERA Server** > **Setup** > **Mirror**. Enable all program language versions present in your network.

NOTE: To configure the mirror to use the HTTPS protocol for the client updates, navigate to **ERAC** > **Tools** > **Server Options...** > **Advanced** tab > **Edit Advanced Settings...** > **ESET Remote Administrator** > **ERA Server** > **Setup** > **Mirror** > **Protocol** > **HTTPS**.

6.7 Other Settings

In the **Other Settings** tab, you can set up an **SMTP** server address to use while sending installation packages via email and an administrator email address which will be used in email sent by the administrator. If authentication is required by the server, specify the appropriate username and password.

Note: You can secure the connections by selecting a security protocol from the **Secure connection** drop down menu. Available are **TLS**, **SSL** and **Auto**, where the available protocol is selected automatically.

New Clients

- **Allow new clients** – when selected, new clients are added automatically to the client list upon their first connection to the ERA Server. Clients imported via replication from other ERA servers will be added to the client list automatically during replication.
- **Automatically reset "New" flag by new clients** – when selected, new clients will not be flagged as new automatically on their first connection to the ERAS. For more details see the **Clients** tab description.

Ports – enables you to customize ports

- **Console**: port used by ERA Console for connecting to ERA Server (2223 by default).
- **Client**: port used by ESET client for connecting to ERA Server (2222 by default).
- **Replication port of this server**: port used by ERA for replication to an upper ERA Server (2846 by default).
- **ESET Remote Installer (Agent)**: port used by remote install agent for remote installation (ESET Remote Installer, by default 2224).
- **Web Server**: port used for connection to the Web Server, (2225) by default.

NOTE: For changes in port configuration to take effect, NOD32 ERA Server service must be restarted.

ESET Live Grid

- **Gathering** - ERAS will forward suspicious files and statistical information from clients to ESET servers on a specified time interval. In some cases it is not possible to gather this information directly from clients.

Dashboards

- **Configure Web Servers List...** – Click here to access the Dashboard Web Servers List 42.

6.8 Advanced

The **Advanced** tab in the **Server Options** window allows you to access and modify the advanced settings for the server via the ESET Configuration Editor. You can open the Configuration Editor by clicking the **Edit Advanced Settings...** button on this tab. Please read the warning message and proceed carefully.

Advanced settings include the following:

- **Maximum disk space usage (percent)** – When exceeded, some server features may not be available. When connecting to ERAS, ERAC displays a notification if the limit is exceeded.
- **Preferred communication protocol encoding** – Defines the type of encoding. We recommend the default setting.
- **Enable MAC address renaming (from unknown to valid)** – After reinstalling from an ESET client solution that does not support sending a MAC address (e.g., ESET Endpoint Antivirus 2.x) to a client solution that does (e.g., a 3.x client), the old client record will be converted to the new one. We recommend the default setting (Yes).

- **Enable MAC address renaming (from valid to unknown)** – After reinstalling from an ESET client solution that does support sending a MAC address (e.g., ESET Endpoint Antivirus 3.x) to a client solution that does not (e.g., a 2.x client), the old client record will be converted to the new one. We recommend the default setting (No).

- **Enable MAC address renaming (from valid to another valid)** – Enables renaming of valid MAC addresses. The default value does not allow for renaming, which means that the MAC address is a part of the unique identification of clients. Disable this option if there are multiple entries for one PC. We also recommend disabling this option if a client is identified as the same client after the MAC address has been changed.

- **Enable computer name renaming** – Allows for renaming of client computers. If disabled, the computer name will be a part of the unique identification of clients.

- **Also use default server logon during push installation** – ERAS allows the user to set the username and password for logon script and email remote installation only. Enable this option to use the predefined values also for remote push installations.

7. ERA Command-line Console

The ERA Command-line console is a tool that allows you to execute tasks and manage clients directly from the command line, either by starting the ERA Command-line Console tool from the folder where ERA Console is located, or by typing *eracmd.exe* in the command prompt.

The ERA Command-line Console uses the ERA API 147 to communicate with the ERA Server.

When you start the ERA Command-line Console, you will be asked to submit your login credentials. If you leave these parameters blank, default values will be used.

Note: The ERA Command-line console supports the autocomplete function. Start typing a command into the console and press TAB to complete the command. Pressing TAB multiple times cycles through all available options. Pressing the UP/DOWN arrows cycles through the history of entered commands. Pressing ESC returns you to the previous text, pressing ESC twice erases the text completely.

Syntax from command-line:

```
eracmd.exe  --connectionparameters [command arguments [-commandflags]]  [;command arguments -commandflags]
```

Example:

```
eracmd.exe --s 127.0.0.1 version server -format csv
eracmd.exe --aa
```

Once started, the ERA command-line console automatically attempts to connect to the server. If the connection is successful, eracmd starts processing commands. If a command is not specified, eracmd starts in shell mode, where the user can write commands and see the result directly. To view a list of available commands, type the command `HELP COMMANDS.`

Syntax from shell mode:

```
[command arguments [-commandflags]]  [;command arguments -commandflags]
```

For arguments with white spaces, use quotes to contain all of the words as a single argument. To have a quotation mark inside of such argument, use double quotation mark. For example, "Say ""hello"" please" will be interpreted as 'Say "hello" please'

Two words connected to each other (one of them with quotation marks) will be connected. For example, "Say "hello will be interpreted as 'Say hello'

In the ERA command-line console, commands and keywords are not case sensitive. Only arguments used to query the database can be case sensitive.

@-replacing:

Any part of a command can be taken from a file. The file path should be surrounded by the @ symbol. When this syntax is used, the content of the specified file is used to take its place. If the file contains more lines, those lines are connected by commas and treated as a single line. This allows you to save to the file the argument list that will be used in next command. Empty lines are skipped. To suppress this functionality, the @ symbol must be surrounded by quotation marks.

Examples:

The file *myconnection.txt* contains the text '*--s 192.168.0.1*', and then the command *eracmd.exe @myconnection@* to show clients id where name *-like "*@*"* will be used as *eracmd.exe --s 192.168.0.1 show clients id where name -like *@**

This example creates a configuration task for clients with the word 'notebook' in their name:

show client id where client_name -like *Notebook* -out notebookID.txt -format csv -header none

task config c:\task_config_01.xml @notebookID.txt@

Commands 124:

Type HELP COMMANDS into the terminal to view a list of available commands, type HELP <command> to view instructions specific to a certain command. Commands can have mandatory parameters as well as optional parameters that you can specify using a keyword. Optional parameters called by a keyword can be used in any order after mandatory parameters are given. A command starts right after connection parameters, no prefix is needed. If no command is present in the command line, eracmd will start in shell mode. Multiple commands can be specified in one line, us a semicolon (;) to separate commands. To execute a script file containing multiple commands, use the command SCRIPT <scriptFileName>. In a script file, commands are separated by line breaks.

Command flags:

Command flags define the general behavior of a command, such as output format, or error handling. Command flags must be appended after a command and its arguments to function correctly. Place a dash (-) before each flag keyword to identify it. To see a list of flags, type the command HELP FLAGS.

Comments:

When in shell mode, comments can be used in scripts or in command line arguments. A comment begins with # and continues to the end of the current line. The command separator does not end a comment. If # is used in a quoted sequence, it does not start a comment and is used as a normal part of the quoted text instead.

Shell mode:

In shell mode, press TAB to activate context-sensitive autocomplete. Use the command `HISTORY` to enable, disable or clear command history. To choose a command from history, use the UP and DOWN arrows. To revert changes made by TAB or UP/DOWN, press ESC.

Startup script:

To have specific commands executed when shell mode is started, add them to the startup script.

The default startup script file is located in ProgramData (All Users\Application Data) in ESET\ESET Remote Administrator\Console\eracmd_startup.txt. An alternative path can be specified using the --startup eracmd.exe argument (for example, eracmd.exe --startup startup_script.txt).

The script is not executed as a separate subscript (using the "script" command), but it is executed as if the commands were typed directly into the console in shell mode (flags set in the startup script using the "set" command remain set in shell mode).

The "set save" command can be used to save current flag values to the startup script, overwriting the startup script file if it exists.

If an exit command is used in the startup script, commands following the exit command will not be executed, but eracmd.exe will not exit shell mode.

Formatting styles

Header and field flags can be used to specify formatting styles:

- keyword - constant texts are used (suitable for automatic post-processing)

- pretty - translatable texts are used (suitable for output for the user)

Header flag affects table headers (column names). Field flag affects table field values.

Connection parameters

Parameters pertaining to connection to the ERA server must be specified as command-line parameters. Eracmd.exe only processes commands if the connection is established successfully. All connection parameters use the double dash (--) prefix.

--*s server:port*: Server to connect to. Default value: `localhost:2226`

--*u username*: Era server username. If the username starts with a domain prefix, it will be used as domain authentication username. This command cannot be used in combination with --ud or --uc. Default value: `Administrator`

--*ud username*: Domain authentication username. Cannot be used in combination with --u or --uc.

--*uc*: Use current Windows session credentials. Cannot be used in combination with --u or --ud.

--*p password*: Era server or domain authentication password. Cannot be used in combination with --pa. Default value: "" (blank password).

--*pa*: Prompts for password. After starting console, it will be possible to enter password displaying * only. Cannot be used in combination with --p.

--*aa*: Ask for all the connection parameters. If specified, no other connection parameters can be specified.

--*startup*: Alternative startup script path. The startup script is automatically executed at the beginning of shell mode.

7.1 Command flags

Flags can be used to define some generic command behavior, or to specify output from each command. To set the default value for each flag, use the SET command. Flags are appended after a command and its arguments. Below is a list of available flags:

`-format` Output format. Possible values: *csv, table*. Default value: *csv* (in command-line mode), *table* (in shell mode).

`-delim` Delimiter for the CSV output. If used with the argument "", the system delimiter will be used (which is also the default value). If a system delimiter is not set, ',' is used. Since semicolon is used as the command separator, use quotation marks to specify it as a delimiter. Default value: "" (system delimiter, ',' if not set).

`-out` Redirects output to a file. See also -mode and -enc flags. If used with the argument "", redirection will be disabled (which is also the default behavior). Default value: "" (redirection disabled).

`-mode` File output mode. Possible values: o (overwrite the file), a (append to the end of the file). Default value: o (overwrite the file).

`-enc` File output encoding. Possible values: *ansi, utf8*, *utf16*. Default value: *utf8*.

`-header` Table header type. Possible values: *keyword* (use keywords as used in the show command arguments, for example, client_name), *pretty* (use more readable, translatable column names, for example Client Name), *none* (header is not shown). Default value: *keyword*.

`-paged` Paged output. If enabled, the user is prompted to press a key after each page. Possible values: *true, false*. Default value: *false*.

`-tableclip` Clip tables to fit the screen. This is applied only when outputting a table to a console window. Possible values: *true, false*. Default value: *true*.

`-color` Use multiple colors when displaying content in the console window. Possible values: *true, false*. Default value: *true*.

`-field` Table field formatting style. Possible values: *keyword* (use constant keywords, for example, finished_with_warning), *pretty* (use more readable, translatable texts, for example, "Finished with warning"). Default value: *keyword*.

`-onerror` What to do if an error occurs while executing a command. If stop is set, the execution of a command sequence stops immediately. If continue is set, the execution continues with the following commands. The whole sequence ends with an error status if any commands have failed. Possible values: *stop, continue*. Default value: *stop*.

7.2 Commands

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
clearinfo	Clears specified information from a client. It is possible to clear Last Threat Alert, Last Firewall Alert, Last Event Warning, Last Scan and Custom Info.	clearinfo <data type> <clients>	**data type** Comma-separated list of types of information to be cleared. Possible values: threat,firewall,event,scan,custom **clients** Comma-separated list of client IDs (or * for all clients). Type 'show client *' to see the list of clients.	clearinfo firewall *
client comment	Sets client comment.	client comment <client ID> <comment>	**client ID** ID of the client for which the comment will be set. To see the information of existing clients including client ID type 'show client *' **comment** Comment for the client.	client comment 1 Problematic
client delete	Deletes clients from the server.	client delete <client ID> [<nowait>]	**client ID** Comma-separated list of IDs of clients to be deleted. **nowait** Do not wait for the result of processing the request on the server. Possible value: nowait	client delete 1,5,9 nowait
client new	Sets or resets the 'new' flag for a client on the server.	client new <client ID> <action>	**client ID** Comma-separated list of IDs of the clients on which to set or reset the 'new' flag. **action** Whether to set or reset the 'new' flag. Possible values: set, reset	client new 1 reset
client rename	Renames a client on the server.	client rename <client ID> <name>	**client ID** ID of the client to rename. **name** New name for the client.	client rename 1 new_client_name
client roaming	Sets or resets the 'roaming user' flag for a client on the server.	client roaming <client ID> <action>	**client ID** Comma-separated list of IDs of the clients to set or	client roaming 1 set

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
			reset the 'roaming user' flag. **action** Whether to set or reset the 'roaming user' flag. Possible values: set, reset	
cls	Clears the console output.	cls		cls
echo	Displays an argument as a message. If the argument is missing, only a new line is added to the output.	echo [<message>]	**message** Message to display. Could contain multiple values which are concatenated.	echo "hello world" echo "Report created with ID: ",@reportId.csv@ echo
encrypt	Encrypts a password for using in configuration. Two types of encryption are used: 'server' which is used for passwords defined by the era server (replication, client, installer, users), and 'other' which is used for passwords defined by other services (smtp, update, ...). As a result, this command shows the encrypted password, which can be used for creating configuration files. If a password is not specified, the user will be prompted to enter passwords - characters in the password field will be displayed as asterisks.	encrypt <encryptionType> [<password>]	**encryptionType** Type of encryption. Possible values: server, other, hash, int64 **password** Password to encrypt.	encrypt server MyReplicationPassword6578 encrypt other MySmnpPwdBfx5 encrypt hash MyLockPass2 encrypt int64 580076500
errmsg	Shows error message for an error code.	errmsg <code>	**code** Error code to look up an error message for.	errmsg 2001
exit	Terminates the command line console if used from shell mode. Stops the current script file execution if used in a script file.	exit		

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
getdata	Gets the specified set of information from a particular client or about a particular policy for a local file. Some information might be unavailable on the server, to refresh that information use the REQUEST command. Configuration, Protection Features, Protection Status and System Information is refreshed automatically for clients on primary server.	getdata <data type> <data ID> <file>	**data type** Type of data to get. Possible values: Client: sysinspector (SysInspector Log), configuration (Configuration XML), protection_status (Protection Status), protection_features (Protection Features), system_information (System Information); Policy: policy (Policy XML, only for policies not replicated from upper server), policy_merged (Merged Policy XML, created as a result of inheritance by applying settings from upper policy), policy_override (Policy Override Part XML, only for policies replicated from upper server), policy_nonoverride (Policy Non-Override Part XML) **data ID** ID of the data entity (client or policy) to download data from. **file** Destination local file path.	getdata configuration 1 c:\file.xml
group	Shows defined groups and group information.	group [<tree>]	**tree** Use tree mode to show the groups with the group inheritance.	group
group assign	Assigns one or more clients to a static group.	group assign <group ID> <clients>	**group ID** ID of a group to assign clients to. **clients** Comma-separated IDs of clients to be assigned to the specified group. Or use * for all clients. Type 'show client *' to see the list of clients and their details including their IDs.	group assign 1 3,4

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
group create	Creates a static or parametric group.	group create <type> <name> [description <description>] [parentID <parent ID>] [paramsXML <params XML>] [sticky <sticky>]	**type** Type of the new group (possible values: static, parametric) **name**, **description**, **parent ID**, **params XML**, **sticky** - for help type `help group create` in the eracmd.exe	group create static new_group
group delete	Deletes an existing static or parametric group with all it's subgroups.	group delete <group ID>	**group ID** ID of a group to be deleted. Type 'group' to see the existing groups and their IDs.	group delete 2
group export	Exports static or parametric groups to a local XML file.	group export <type> <group ID> <filename> [<tree>]	**type** Type of groups to export. Possible values: static, parametric **group ID** ID of the group or ID of the root group of the subtree to export. If * is used and tree is TRUE, the whole group tree will be exported. **filename** Path to the .xml file to import groups from. **tree** By default the whole subtree (with the group as root) is exported. Use '`false`' value to not export the subtree.	group export static * gr_static.xml group export parametric 2 gr_parametric.xml false
group import	Imports static or parametric groups from a local XML file. If a group with the same path already exists, it will be changed (for example, specified client relations will be added to the existing group).	group import <type> <parent ID> <filename> [<relations>]	**type** Type of groups to import. Possible values: `static`, `parametric` **parent ID** ID of the parent group. The groups will be imported under this group in the group tree. If * is used, the subtree will be imported under the groups tree root. **filename** Path to the .xml file to import	group import static * gr_static.xml true group import parametric 2 gr_parametric.xml

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
			groups from. **relations** Imports client relations of the specified static group if the '`true`' value is used. The default value is '`false`'.	
group remove	Removes one or more clients from a static group.	group remove <group ID> <clients>	**group ID** , **clients** Same as for 'group assign'.	group remove 1 3,4
group update	Updates a static or parametric group with the specified parameters.	group update <group ID> [name <name>] [description <description>] [parentID <parent ID>] [paramsXML <params XML>]	**group ID** ID of the group to be updated. **name**, **description**, **parent ID**, **params XML**, **sticky** - for help type `help group update` in the eracmd.exe	group update 2 newname
help	Shows information about using ERA Command-line Console. Use the argument to select a more specialized help.	help [<command 1>] [<command 2>]	**command 1** Command to show help for (first word of command name). Possible values: <command name>, flags, commands **command 2** Command to show the help for (second word of command name).	help version help commands help help
history	Enables or disables persistent autosaves of shell mode command history after the console is closed. This is disabled by default.	history [<action>]	**action** If omitted, the current state of saving history after the console quits will be shown. Possible values: true (enable), false (disable), clear (erase the command history), list (show current saved history content)	history true
license	Shows server license information.	license		license
license add	Uploads the specified license key file or files to the ERA server.	license add <filename>	**filename** Comma-separated list of paths of license key files to upload.	license add c:\era.lic
license details	Shows information about partial license keys loaded by the ERA	license details		license details

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
	server.			
license replace	Uploads a license key file or files to the ERA server and replaces all old license files with the uploaded license key(s).	license replace <filename>	**filename** Comma-separated list of paths of license key files to replace with.	license replace c:\era.lic
logforward	Shows or sets current log forwarding settings. There are two ways of using this command: 1. To display the state of a particular log forwarding setting, use the first parameter <type> or use the command without any parameter to show current log forwarding settings of all logs. 2.To set log forwarding settings, the <type> and <enable> parameters are mandatory. Other parameters ([level <level>], [severity <severity>] and [facility <facility>]) are optional. If an optional parameter is omitted, the value will remain unchanged.	logforward [<type>] [<enable>] [level <level>] [severity <severity>] [facility <facility>]	**type** Type of log to be displayed or updated. Possible values: event, threat, firewall, hips, antispam, greylist, scan, mobile, device_control, web_control **enable** Determines whether forwarding has to be enabled or disabled. Possible values: true, false **level** Level of the log to be processed by log forwarding. Possible values: critical, warning, normal, diagnostics **severity** SysLog severity value. Possible values: informational, error, warning, debug **facility** SysLog facility value. Possible values: 0 to 23	logforward logforward scan logforward eventlog true level warning logforward threat false
password	Changes a security password of the ERA server. For empty password use "". If old and new passwords are not specified, the user will be prompted to enter passwords - typed passwords will be displayed as asterisks. This command cannot set passwords which are parts of server configuration. For such passwords, use	password <passwordType> [<oldPassword> <newPassword>]	**passwordType** Type of password to set. Possible values: replication, client, installer, currentuser **oldPassword** Old password. It is possible to use an ERA server administrator password. **newPassword** New password.	password currentuser password replication oldPass1 newPass2

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
	command SERVERCFG SET or SERVERCFG SETPWD.			
path	Shows or sets the current working directory used as a base for all relative paths (when specifying script path or data file paths).	path [<action>] [<path>]	**action** Action. Possible values: get (show the current working directory), set (set to the path specified as the next argument), script (set to the path of the current script). Default value: get **path** New working directory. If it is a relative path, it is considered relative to the previous working directory.	path path set d:\scripts path script
policy	Shows defined policies with policy information. If the argument 'tree' is present, shows a tree hierarchy of policies.	policy [<tree>]	**tree** Use tree mode to show the policies with the policy inheritance.	policy policy tree
policy assign	Assigns the specified policy to the specified clients. Note that it is not possible to assign any policy to any client. If the client list contains replicated clients, the policy must be down-replicable. Policy from lower servers cannot be assigned.	policy assign <policy ID> <clients>	**policy ID** The assigned policy. Possible values: <policy ID>, !DefaultClientsPolicy **clients** Comma-separated list of client IDs (or * for all clients).	policy assign 10 1,2,5,9 policy assign !DefaultClientsPolicy *

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
policy create	Creates a policy with the specified parameters on the server. Shows the ID of the new policy if successfully created.	policy create <name> <config XML> [parentID <parent ID>] [description <description>] [overrideAnyChild <override any child>] [downReplicable <down replicable>] [defaultForClients <default for clients>] [defaultForLowerServers <default for lower servers>]	**name** Name for the new policy. **config XML** XML file with the configuration for the new policy. **parent ID** ID of the parent of the new policy. **description** Description of the new policy. **override any child** Sets the 'Override any child policy' flag for the new policy. Possible values: true, false. Default value: false **down replicable** Set 'Down replicable policy' flag for the new policy. Possible values: true, false. Default value: false **default for clients** Set the policy as the default policy for clients. Possible values: true, false. Default value: false **default for lower servers** Set the policy as the default policy for lower servers. Possible values: true, false. Default value: false	policy create new_policy policy.xml

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
policy delete	Deletes a policy and allows you to set replacements for the deleted policy. Unneeded replacements are ignored.	policy delete <policy ID> [child_policies <child policies parent replacement>] [primary_clients <primary clients policy replacement>] [replicated_clients <replicated clients policy replacement>] [primary_clients_default <primary clients default policy replacement>] [lower_servers_default <lower servers default policy replacement>] [whole_branch <delete whole branch>]	**policy ID** ID of the policy to delete. **child policies parent replacement** New parent policy for the currently deleted policy's child policies. Possible values: <policy ID>, !DefaultUpperServerPolicy, !Not Available **primary clients policy replacement** New policy for primary clients with the currently deleted policy. Possible values: <policy ID>, !DefaultClientsPolicy **replicated clients policy replacement** ID of the new policy for replicated clients with the currently deleted policy. **primary clients default policy** Replacement ID of the new default policy for primary clients. **lower servers default policy** New default policy for lower servers. Possible values: <policy ID>, !NotAvailable **delete whole branch** If the whole branch (the specified policy including child polices) should be deleted. Possible values: true, false Default value: false	policy delete 2 primary_clients 4

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
policy export	Exports the specified policies from the local server to an XML file. All policies, single policy or a policy tree with the specified root can be exported.	policy export <policy ID> <filename> [<tree>]	**policy ID** The ID of the policy to be exported. Use * to export all policies. **filename** Path to the .xml file to which the policy is going to be exported. **tree** Its default value is 'true' and it means the specified policy will be exported including its entire subtree. If you use the 'false' value, the subtree of a specified policy will not be exported.	policy export * all_policies.xml policy export 3 policy3.xml true
policy import	Imports all policies from an XML file. Previously defined policies will not be changed. If a policy name already exists, the new (imported) policy will be renamed.	policy import <filename>	**filename** Path to the .xml file the policies are supposed to be imported from.	policy import policyBackup.xml

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
policy update	Updates a policy configuration with the specified parameters.	policy update <ID> [name <name>] [parentID <parent ID>] [configXML <config XML>] [description <description>] [overrideAnyChild <override any child>] [downReplicable <down replicable>] [defaultForClients <default for clients>] [defaultForLowerServers <default for lower servers>] [replicated_clients <replicated clients policy replacement>] [lower_servers_default <lower servers default policy replacement>] [primary_clients_default <primary clients default policy replacement>]	**ID** ID of the updated policy. **name** New name for the updated policy. **parent ID** New ID of the parent for the updated policy. Possible values: <policy ID>, !NoPolicy (the updated policy will have no parent) **config XML** XML file with the new configuration for the updated policy. **description** New description of the updated policy. **override any child** New value of the 'Override any chlid policy' flag for the updated policy. Possible values: true, false **down replicable** New value of the 'Down replicable policy' flag for the updated policy. Possible values: true, false **default for clients** Set the policy as the default policy for clients. Possible values: true, false **default for lower servers** Set the policy as the default policy for lower servers. Possible values: true, false	policy update 123 name policy1 parentID 1 configXML policy.xml overrideAnyChild TRUE defaultForLowerServers FALSE

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
			replicated clients policy replacement New policy for replicated clients with the currently updated policy. Possible values: <policy ID>, !DefaultClientsPolicy, !NotAvailable **lower servers default policy replacement** New default policy for lower servers. Possible values: <policy ID>, !DefaultClientsPolicy, !NotAvailable **primary clients default policy replacement** ID of the new default policy for primary clients.	
report	Shows static or dashboard report templates or generated reports. In the case of generated reports, only the reports located on the server are shown.	report <type>	**type** Report type. Possible values: static, dashboard, generated	report static
report create	Creates a static or dashboard report template.	report create <type> <name> <config XML> [active <active>] [description <description>]	**type** Type of the newly created report template. Possible values: static, dashboard **name** Name of the created report template. **config XML** Path to .xml file with the configuration for the created report template. The first <INFO> found in the file is applied to the newly created report template. Name, description and report template type from command line are used instead of these	report create static new_template C:\config.xml

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
			values in the .xml file. **active** Active state of the created report template. Not applicable to dashboard templates (ignored if specified). Possible values: true, false. Default value: false. **description** Description of the new report template.	
report delete	Deletes a static or dashboard report template.	report delete <report ID>	**report ID** ID of the report template to be deleted. To see the available IDs, execute: 'report static', 'report dashboard'.	report delete 2
report export	Exports report templates to a local XML file. Templates that use incompatible types are skipped.	report export <type> <templates> <filename>	**type** Report type. Possible values: static, dashboard **templates** Comma-separated list of report template IDs (use * for all templates of the given type). To see the available IDs, execute the 'report generated' api command. **filename** Path to the .xml file to export templates to.	report export static * c:\reports_static.xml report export dashboard 2,3 c:\reports_dashboard.xml
report generate	To generate static reports based on defined report template just like the "Generate Static Now" button does in the ERA console.	report generate <template ID> <directory>	**template ID** ID of desired template. To see the template IDs execute the 'report statistic' api command. **directory** Path to the desired directory where the report files will be created.	report generate 3 C:\era_statistics
report import	Imports report templates from a local XML file. Templates specified in the XML file which have incompatible types are	report import <type> <filename>	**type** Report type. Possible values: static, dashboard **filename** Path to the .xml file to import templates from.	report import static c:\reports_static.xml report import dashboard c:\reports_dashboard.xml

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
	skipped.			
report server	The same feature as downloading a report stored on the server using the "Generated Reports" tab in the ERA console.	report server <generated template ID> <directory>	**generated template ID** ID of a generated report template stored on the server. To see the IDs of existing reported templates, execute the 'report generated' command. **directory** Path to the desired directory where the report file will be downloaded.	report server 1 C:\era_reports
report update	Changes the parameters or configuration of a report template.	report update <report ID> [configXML <config XML>] [active <active>] [description <description>]	**report ID** ID of the report template to be updated. **config XML** Path to the .xml file with the new configuration for report templates that are being updated. First <INFO> found in the file is applied to the updated report template. If set, the description from the command line is used instead of the value in the XML. Otherwise, it is left unchanged. The report template type specified in the XML is ignored - report template type cannot be changed by update. **active** Active state of the updated report template. Not applicable to dashboard templates (ignored if specified). Possible values: true, false **description** Description of the updated report template.	report update 1 configXML C:\new_config.xml

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
request	Requests the current version of various data to be transferred from a client to the ERA server. It is possible to request SysInspector Information, Configuration, Protection Status, Protection Features and System Information. Requested data will be received as soon as the client connects to the primary server and the data is available. On replicated clients the request first needs to be replicated. Configuration, Protection Features, Protection Status and System Information is refreshed automatically for clients on the primary server.	request <data type> <clients> [si_compare <compare date>] [<si_snapshot>]	**data type** Comma-separated list of types of data to be requested. Possible values: sysinspector, configuration, protection_status, protection_features, system_information **clients** Comma-separated list of client IDs (or * for all clients). **compare date** If used, compares the requested log with a previous one specified by date and time in UTC in the format YYYY-MM-DD hh:mm:ss (e.g. "2014-01-21 10:43:00"). Used only when requesting SysInspector Information. **si_snapshot** Saves the log locally on the client workstation. Used only when requesting SysInspector Information.	request protection_features * request sysinspector,config 1,2,8 si_compare "2014-01-01 01:02:03" si_snapshot
restart	Restarts the ERA server. The console (commandline) is immediately disconnected after the restart.	restart [<full>]	**full** Use this parameter for full restart of ERA server. The action is logged in the audit log.	restart restart full
rule	Shows policy rules.	rule		rule

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
rule create	Creates a new policy rule	rule create <xml> <name> <policy ID> [desc <description>] [priority <priority>] [enabled <enable>]	**xml** Source XML file, created by exporting existing rule. **name** Policy rule name. **policy ID** ID of related policy. Only following types could be used: default clients policy, local policies, down-replicable policies from upper server. Possible values: , !DefaultClientsPolicy **description** Policy rule description. **priority** Policy rule priority. Possible values: top,bottom Default value: bottom **enable** Initial state of created policy rule. Possible values: true, false Default value: true	rule create "c:\my data \exportedPolicy.xml" myNewPolicy 3 desc "New policy rule" priority top enabled false
rule delete	Deletes a policy rule	rule delete <policy rule ID>	**policy rule ID** ID of the policy rule to delete.	rule delete 3
rule import	Imports policy rules from an XML file. The already defined rules will not be changed. If a rule name already exists, the new (imported) rule is renamed.	rule import <file path>	**file path** XML file path to import rules from.	rule import d:\rule.xml
rule export	Exports policy rules to an XML file.	rule export <rules> <file path>	**rules** Comma-separated list of IDs of the rules (or * for all rules). **file path** XML file path to import rules to.	rule export 1,2 d:\rule.xml

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
rule update	Changes parameters or configuration of a policy rule. Parameters which are not specified will remain unchanged.	rule update <policy rule ID> [xml <config xml>] [desc <description>] [policy <policy ID>] [priority <priority>] [enabled <enable>]	**policy rule** ID of the policy rule to update. **config xml** Configuration XML file, created by exporting existing rule. **description** New description of the policy rule. **policy ID** New related policy ID. Possible values: , !DefaultClientsPolicy **priority** Priority change of the policy rule. Possible values: up,down,top,bottom **enable** New state of the policy rule. Possible values: true, false	rule update 2 xml d:\rule.xml enabled true
runnow	Runs a specified server action immediately.	runnow <actions>	**actions** Actions to run. Possible values: cleanup, compact, replicate, replicate_with_mark_all_clients, update, update_with_clear_cache, apply_policy_rules, synchronize_parametric_groups	runnow update runnow cleanup,compact
scanlog	Shows the content of the specified scan log.	scanlog <ID>	**ID** ID of a required scan log.	scanlog 1
script	Executes a batch of commands in an external file.	script <filename>	**filename** Path to the file containing commands. Commands can be separated by a new line or a semicolon.	script c:\eraGetClientsInfo.txt
servercfg get	Downloads the current server configuration to the specified local file.	servercfg get <filename>	**filename** Local file path to save downloaded configuration to.	servercfg get d:\era_config.xml
servercfg list	Shows available configuration settings which can be modified directly by the SERVERCFG SET and	servercfg list		servercfg list

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
	SERVERCFG SETPWD commands.			
servercfg put	Uploads the server configuration from a local XML file.	servercfg put <filename>	**filename** Local XML file path to upload.	servercfg put d: ew_config.xml
servercfg set	Assigns a value to a particular configuration setting. Use command SERVERCFG LIST to show all available settings.	servercfg set <name=value>	**name=value** Name of the setting and a value to assign.	servercfg set port_con=2223 servercfg set mirror_enabled=1
servercfg setpwd	Assigns a value to a particular configuration setting through password prompt. The typed values are displayed as asterisks, so it is useful for entering passwords. Use the command SERVERCFG LIST to show all available settings. This command cannot set server security passwords - use the PASSWORD command for that.	servercfg setpwd <name>	**name** Name of the setting to be set.	servercfg setpwd ps_password_smtp
set	Gets, sets or saves values of flags. Flags are used to specify command output and other common settings. To see a list of available flags, use the HELP FLAGS command. Setting a flag takes effect for all subsequent commands in the current script file or for all subsequent commands in shell mode (if used directly in shell mode). The flag can be overridden for a single command by specifying a command flag after the command.	set [<flag name>] [<flag value>]	**flag name** Use the flag name without the initial dash. Use the command HELP FLAGS to see a list of available flags. If not specified, current values for all flags are printed. Alternatively, "save" can be used to save the current flags state to the startup file (use the second argument to specify an alternative startup file path). **flag value** Use the command HELP FLAGS for available values. If not specified, current value of the flag is printed.	set set enc set enc utf8 set format table set paged true set save set save startup.txt

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
show	Shows data from the specified table. Use "count" instead of column list to get the row count only.	show <table name> <list of columns> [where <where>] [group by <group by>] [order by <order by>] [skip <skip>] [limit <limit>]	**table name** Use command SHOW TABLES to see available tables. **list of columns** Comma-separated list. Use command SHOW COLUMNS to see the list of columns for the specified table. Use * for all columns. Use "count" to get row count only. Possible values: <column name>, *, count where Comma-separated list of conditions in format <column><comparison operator><value> (e.g. ID>3) or <column> <IN operator> (<comma_separated_values_list>). The following comparison operators are allowed: = (or -EQ), != (or -NE), <= (or -LE), >= (or -GE), < (or -LT), > (or -GT). The following IN operators are allowed: -IN or -NOTIN. For text columns, -LIKE and -NOTLIKE with a text value with wildcards (* - zero or more characters, ? - exactly one character) can be used instead of a comparison operator. **group by** Comma-separated list of columns to group by. Rows with corresponding values in all of these columns will be shown as one row. **order by** Comma-separated list of columns to order by. After each column name, -ASC (default)	show client * show client client_name show client ID, client_name WHERE ID>4, configuration -IN (ready, requested) ORDER BY client_name LIMIT 5 show client * WHERE product_name -LIKE *endpoint* show client count WHERE ID>4 show client * where group_ID=4 show client * where requested_policy_ID -IN (2,3) show event * where client_group_ID=4 show event * where client_requested_policy_ID -IN (2,3)

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
			or -DESC can be specified for ascending or descending order. **skip** How many rows to skip at the beginning. **limit** Max. count of rows to show.	
show columns	Shows available columns for the specified table.	show columns [for] <table name>	**table name** Table to show the columns for. Use the SHOW TABLES command to get available table names.	show columns for client
show tables	Shows available tables that can be used in the SHOW command.	show tables		show tables
task config	Creates a configuration task using a configuration file. Shows the ID of the new task if successfully created.	task config <configuration file> <clients> [name <name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>]	**configuration file** XML file from configuration editor. **clients** Comma-separated list of client IDs (or * for all clients). **name** Task name. **description** Task description. **apply after** UTC time when the task has to be applied in one of the following formats: YYYY-MM-DD hh:mm:ss, YYYY-MM-DD hh:mm, YYYY-MM-DD hh, YYYY-MM-DD. For example (date with time): "2014-01-21 10:43". Example (date without time): "2014-01-21". **delete if completed** Use If the task has to be deleted after successfully completion. Possible values: true, false. Default value: false.	task config d:\task_config_01.xml 1,4,5 name "Config01" description "email client protection config"
task scan	Creates a scan task. Shows the ID of the new task if successfully	task scan <clients> [name <name>] [description	**clients** Comma-separated list of client IDs (or * for all clients).	task scan 1,3

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
	created.	<description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>] [exclude <exclude>] [windows_profile <profile>] [windows_targets <windows targets>] [windows_no_cleaning <no cleaning>] [windows_shutdown_after_scan <shutdown>] [windows_allow_shutdown_cancel <allow cancel>] [linux3_targets <linux3 targets>] [linux3_no_cleaning <no cleaning>] [linux_profile <profile>] [linux_targets <linux targets>] [linux_no_cleaning <no cleaning>] [mobile_targets <mobile targets>] [mobile_no_cleaning <no cleaning>] [max_delay <max delay>]	**name** Task name. **description** Task description. **apply after** UTC time when the task has to be applied in one of the following formats: YYYY-MM-DD hh:mm:ss, YYYY-MM-DD hh:mm, YYYY-MM-DD hh, YYYY-MM-DD. For example (date with time): "2014-01-21 10:43". Example (date without time): "2014-01-21". **delete if completed** If the task has to be deleted after successfully completed. Possible values: true, false. Default value: false. **exclude** Comma-separated list of sections to exclude from the scan task. Possible values: windows, linux3, linux, mobile. **profile** Scan profile name. Possible values: !InDepthScan, !MyProfile, !SmartScan, !ContextMenuScan, <user-defined profile name>. Default value: !InDepthScan **windows targets** Comma-separated list of windows targets to scan. Possible values: !Memory, !RemovableDrivesBoot, !RemovableDrives, !LocalDrivesBoot, !LocalDrives, !RemoteDrives, !AllDrivesBoot, !AllDrives, <custom path> Default	

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
			value: !Memory, !LocalDrivesBoot, !LocalDrives **no cleaning** Scan without cleaning. Possible values: true, false. Default value: false **shutdown** Shutdown computer after scan. Possible values: true, false. Default value: false **allow cancel** Allow an user to cancel the shutdown. Possible values: true, false. Default value: false **linux3 targets** Comma-separated list of linux3 paths to scan. Default value: / **linux targets** Comma-separated list of linux paths to scan. Default value: / **mobile targets** Comma-separated list of mobile targets to scan. Possible values: !All, <custom path> Default value: !All **max delay** Max. random delay in minutes.	

COMMAND	DESCRIPTION	SYNTAX	PARAMETERS	EXAMPLE
task update	Creates an update task. Shows the ID of the new task if successfully created.	task update <clients> [name <name>] [description <description>] [applyAfter <apply after>] [deleteIfCompleted <delete if completed>] [exclude <exclude>] [windows_profile <windows profile>] [max_delay <max delay>]	**clients** Comma-separated list of client IDs (or * for all clients). **name** Task name. **description** Task description. **apply after** UTC time when the task has to be applied in one of the following formats: YYYY-MM-DD hh:mm:ss, YYYY-MM-DD hh:mm, YYYY-MM-DD hh, YYYY-MM-DD. For example (date with time): "2014-01-21 10:43". Example (date without time): "2014-01-21". **delete if completed** Use if the task has to be deleted after successfully being completed. Possible values: true, false. Default value: false **exclude** Comma-separated list of sections to exclude from the update task. Possible values: windows, linux3, linux, mobile **windows profile** Profile name for windows section. **max delay** Max. random delay in minutes.	task update 2,4,6 name "Update01" exclude windows task update *
version	Shows the current version of the Command-line Console, API and ERA server.	version [<component>]	**component** Which component's version should be displayed. If missing, all versions are shown. Possible values: cmd, api, server	version version cmd

8. ERA API

You can interact with the ERA Server via the ERA API. The API uses the same commands 124 as the ERA Command-line Console 121. In fact, the command-line console uses the ERA API to communicate with the ERA Server.

API files can also be downloaded from http://www.eset.com/int/download/business/detail/family/241/

Online API documentation: http://help.eset.com/era/5/en-US/api/

9. ERA Maintenance Tool

The purpose of the ESET Remote Administrator Maintenance Tool is to execute specific tasks for server operation and maintenance. It can be accessed by clicking **Start** > **Programs** > **ESET** > **ESET Remote Administrator Server** > **ESET Remote Administrator Maintenance Tool**. When you launch the ERA Maintenance tool, an interactive wizard will display to help you in performing the required tasks.

After you start the ESET Remote Administrator Maintenance Tool and click **Next**, you can see the ERA Server information window. The tool displays summary information about the ERA Server installed. The displayed information can be viewed in more detail in a separate window by clicking **More Information**, it can be copied by clicking **Copy to clipboard** and it can be refreshed by clicking **Refresh**. After you verify the information, proceed to the next step by clicking **Next** and select a task:

- Stop ERA Server 148
- Start ERA Server 148
- Database Transfer 149
- Database Backup 149
- Database Restore 150
- Delete Tables 150
- Storage Backup 150
- Storage Restore 150
- Install New License Key 150
- Modify server configuration 151

At the end of each task setup, you can save the settings for the current task by clicking **Save all settings to a file**. The settings can be then used at any time in the future by clicking **Load all settings from a file**. Each individual step in a task setup also has the option to **Save all settings to a file** or **Load all settings from a file**.

9.1 Stop ERA Server

This task stops the ESET Remote Administrator Server service.

NOTE: Name of the service is ERA_SERVER. Executable for this service is "*C:\Program Files\ESET\ESET Remote Administrator\Server\era.exe*".

9.2 Start ERA Server

This task starts the ESET Remote Administrator Server service.

NOTE: Name of the service is ERA_SERVER. Executable for this service is "*C:\Program Files\ESET\ESET Remote Administrator\Server\era.exe*".

9.3 Database Transfer

This task allows you to convert the database format. The tool can convert between the following databases:

- MS Access
- MS SQL Server
- Oracle
- MySQL

The first step is to check the database connection. This step is common for all tasks, except when uploading a new license key and modifying server configuration.

If the database is an MS Access database, specify the path to the *.mdb* file. The path specified during ERA Server installation is used by default.

All other database formats require additional parameters to be set:

- Connection string: Special string used to identify the source database
- Username: Username for accessing the database
- Password: Password for accessing the database
- Schema name: Name of a schema (available for Oracle and MS SQL only)

Click **Load current server configuration** to use the current ERA Server settings. Click **Test Connection** to test the database connection. If the connection cannot be established, check the parameters for errors. After the database test is successful, continue by clicking **Next**.

Then, select the target database. Select **Replace server connection settings** to connect the server and use the new database after successful conversion. Not selecting this option will cause the new database to be created without the server updating to the new database version.

For all database types besides MS Access database, select whether to create the database tables automatically (**Create tables in the database automatically**) or insert the tables into the database later (**View Script** > **Save to File**) in the next step. For an MySQL database, the **Create a new database ESETRADB automatically** option automatically creates a new MS SQL database named ESETRADB. The final step is to confirm the database conversion.

9.4 Database Backup

This tool allows you to create a backup file of the database. The settings in the first window are similar to those in the database conversion (see chapter Database Transfer 149); in this window the source database is selected. The source database will be copied to a backup file specified in the next step.

Optional parameters in the lower part of the window enable you to overwrite the existing file (**Overwrite if exists**) as well as to stop ESET Remote Administrator Server during the backup process (**Stop server during processing task**). Click **Next** to confirm the task execution.

9.5 Database Restore

This task allows you to restore the database from a backup file. The settings in the first window are similar to those in the database conversion (see chapter Database Transfer 149); in this window the database type is selected.

For all database types besides MS Access database select whether to create the database tables automatically (**Create tables in the database automatically**) or insert the tables into the database later (**View Script** > **Save to File**) in the next step. For an MS SQL database the **Create a new database ESETRADB automatically** option automatically creates a new MS SQL database named ESETRADB. The final step is to confirm the database restore.

Select the file from which the database is to be restored in the next step. Optional parameters in the lower part of the window enable you to import a file from a different database type as selected in the previous step (**Allow import from a different type of database**) as well as to stop ESET Remote Administrator Server during database restore (**Stop server during processing task**). Click **Next** to confirm the task execution.

9.6 Delete Tables

This deletes the current current content of tables in the database. As a result, the database will return to the state it was in immediately following the installation of the ERA Server. The settings in the first window are similar to those in the database conversion (see chapter Database Transfer 149); in this window the database type is selected. In the next step you will be prompted to confirm the action. Select **Yes, I agree** and then click **Next** to confirm the action.

NOTE: If an MS SQL, MySQL or Oracle database is used, we recommend that you stop the ERA Server before deleting the tables.

If an MS Access database is used, it will be replaced with the default empty database.

9.7 Storage Backup

This task will perform a storage backup, which will save all data from the storage folder (*C:\ProgramData\ESET\ESET Remote Administrator\Server\storage\* by default) to an external dump file(*.dmp). Stored in this folder are some important server logs and configurations. Click the envelope symbol in the lower part to browse to the folder where you want the storage to be backed up and enter a file name. You can also choose whether you want to **Overwrite if exists**, in case you want to overwrite an already existing .dmp file. It is recommended that you leave the option **Stop server during processing task** selected, because the storage backup task can cause a decrease in server performance. Clicking **Next** and then **Start** will start the task.

9.8 Storage Restore

This task will perform a storage restore from a previously saved dump(*.dmp) file. See the storage backup task for more information. Click the envelope symbol in the lower part to browse to the folder where the dump file is located. It is recommended that you leave **Stop server during processing task** selected, because the storage restore task can cause a decrease in server performance. Clicking **Next** and then **Start** will start the task.

9.9 Install New License Key

To insert a new license key to be used by the server enter the location of the new license key.

Overwrite the existing license key if required (**Overwrite if exists**) and restart the server if required (**Force server start (in case it is not running)**). Click **Next** to confirm and complete the action.

9.10 Modify server configuration

This task launches the Configuration Editor (if installed). Finishing the task opens the Configuration Editor window and allows you to edit advanced ERA Server settings. These settings are also accessible via **Tools** > **Server Options** > **Advanced** > **Edit Advanced Settings**.

NOTE: In order for this feature to work, ERA Console must be installed. You can also save server settings to an .xml file and upload it later using the **Load all settings from file** option.

9.11 Command Line Interface

ESET Remote Administrator Maintenance Tool (ERAtool.exe) can also work as a command line tool, integrating into scripts. When the tool is run, it parses the parameters, executing each action in the specified order. If no arguments are given, the interactive wizard is run instead.

The following commands are supported:

- */startserver* or */startservice* – starts the ESET Remote Administrator Server service
- */stopserver* or */stopservice* – stops the ESET Remote Administrator Server service
- */gui* – launch the interactive wizard after finishing all tasks

Any parameter that doesn't start with a slash is interpreted as a filename of the configuration script that should be executed. Configuration scripts are created by saving settings in the interactive wizard.

NOTE: ERAtool.exe requires elevated administrator rights; if the script that calls ERAtool.exe doesn't have the rights necessary, Windows may display an interactive prompt for elevation or run the tool in a separate console process (losing the tool output).

10. Troubleshooting

10.1 FAQ

This chapter contains solutions to the most frequently asked questions and problems related to installation and operation of ERA.

10.1.1 Problems installing ESET Remote Administrator to Windows server 2000/2003

Cause:

One of the possible causes may be the Terminal Server running on the system in the *execution* mode.

Solution:

Microsoft advises switching the Terminal Server to *"install"* mode while installing programs to a system with Terminal Server service running. This can be done either through **Control Panel** > **Add/Remove programs** or by opening a command prompt and issuing the *change user /install* command. After installation, type *change user / execute* to return the Terminal Server to execution mode. For step-by-step instructions on this process, see the following article: http://support.microsoft.com/kb/320185.

10.1.2 What is the meaning of the GLE error code?

Installing ESET Endpoint Security or ESET Endpoint Antivirus via the ESET Remote Administrator Console can occasionally generate a GLE error. To find the meaning of any GLE error number, follow the steps below:

1) Open a command prompt by clicking **Start** > **Run**. Type *cmd* and click **OK**.
2) At the command prompt, type: *net helpmsg error_number*

Example: *net helpmsg 55*

Example result: The specified network resource or device is no longer available.

10.2 Frequently encountered error codes

During the operation of ERA, you may encounter error messages which contain error codes indicating a problem with some feature or operation. The following chapters outline the most frequently encountered error codes when performing push installs, as well as errors that can be found in the ERAS log.

10.2.1 Error messages displayed when using ESET Remote Administrator to remotely install ESET Smart Security or ESET NOD32 Antivirus

SC error code 6, GLE error code 53 Could not set up IPC connection to target computer
To set up an IPC connection, these requirements should be met:

1. TCP/IP stack installed on the computer where ERAS is installed, as well as on the target computer.

2. File and Printer Sharing for Microsoft Networks must be installed.

3. File sharing ports (135-139, 445) must be open .

4. The target computer must answer ping requests.

The following are some of the most commonly seen error codes, below each is the recommended troubleshooting action to take:

> **SC error code 6, GLE error code 67 Could not install ESET installer on target computer**
> The administrative share *ADMIN$* must be accessible on the client's system drive.

SC error code 6, GLE error code 1326 Could not set up IPC connection to target computer, probably due to a wrong username or password
Administrator's username and password have not been typed incorrectly or have not been entered at all.

SC error code 6, GLE error code 1327 Could not set up IPC connection to target computer
Administrator's password field is blank. A remote push installation cannot work with a blank password field.

SC error code 11, GLE error code 5 Could not install ESET installer on target computer
The installer cannot access the client computer due to insufficient access rights (Access Denied).

SC error code 11, GLE error code 1726 Could not install ESET Installer onto target computer
This error code displays after repeated attempts to install if the Push Installation window was not closed after the first attempt.

Failure during the package install - exit code 1603. Description: Fatal error.
Exit code 1603 is generic and can have several causes. For a push installation, the 2 most frequent causes are:

1. The target machine is not in a domain. To resolve this, disable UAC (User Access Control) on the target machine. Applies to Windows Vista, Windows 7 and Windows 8 (8.1) machines.
2. An ESET client solution was uninstalled prior to installation, but the target machine has not been rebooted. Reboot the target machine to resolve this issue.

10.2.2 Frequently encountered error codes in era.log

0x1203 – UPD_RETVAL_BAD_URL
Update module error – incorrectly entered update server name.

0x1204 – UPD_RETVAL_CANT_DOWNLOAD
This error can appear:

- when updating through HTTP
  - update server returns an HTTP error code between 400–500 except for 401, 403, 404, and 407
  - if updates are downloaded from a CISCO based server and the HTTP authentication response format has been changed
- when updating from a shared folder:
  - returned error does not fall into the categories bad authentication or file not found (e.g., *connection interrupted* or *non existing server*, etc.)
- both update methods
  - if all of the servers listed in the file *upd.ver* could not be found (the file is located in *%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\updfiles*)
  - failed to contact the failsafe server (probably due to deletion of the corresponding ESET entries in the registry)
- incorrect proxy server configuration in ERAS
  - The administrator must specify the proxy server in the proper format.

0x2001 – UPD_RETVAL_AUTHORIZATION_FAILED
Authentication to update server failed, incorrect username or password.

0x2102 – UPD_RETVAL_BAD_REPLY
This update module error can be encountered if a proxy server is used to mediate Internet connection – namely Webwasher proxy.

0x2104 – UPD_RETVAL_SERVER_ERROR
Update module error indicating an HTTP error code higher than 500. If the ESET HTTP server is being used, error 500 indicates a problem with memory allocation.

0x2105 – UPD_RETVAL_INTERRUPTED
This update module error can be encountered if a proxy server is used to mediate the Internet connection – namely Webwasher proxy.

10.3 How to diagnose problems with ERAS?

If you suspect that there is something wrong with ERAS or if it is not functioning correctly, we recommend that you follow these steps:

1) Check the ERAS log: Click **Tools** > **Server Options** from the ERAC main menu. From the **Server Options** window, click the **Logging** tab and then click **View log**.

2) If you see no error messages, increase the **Log verbosity** level in the **Server Options** window to Level 5. After you have tracked down the problem, we recommend switching back to the default value.

3) You may also be able to troubleshoot problems by turning on the database debug log in the same tab – see section **Debug Log**. We recommend that you only activate the **Debug log** when attempting to duplicate the problem.

4) If you see any error codes other than those mentioned in this documentation, please contact ESET Customer Care. Please describe the behavior of the program, how to replicate the problem or how to avoid it. It is very important to include the program version of all ESET security products involved (i.e., ERAS, ERAC, ESET Endpoint Security, ESET Endpoint Antivirus).

11. Hints & tips

11.1 Scheduler

ESET Endpoint Antivirus and ESET Endpoint Security contain an integrated task scheduler which allows for scheduling regular computer scans, updates, etc. All specified tasks are listed in the Scheduler.

Following types of tasks can be configured using ERA:

- Run external application
- Log maintenance
- Computer scan
- Create a computer status snapshot
- Update
- Automatic startup file check

In most cases, there is no need to configure a **Run external application** task. The task **Automatic startup file check** is a default task and we recommend not changing its parameters. If no changes have been made after installation, ESET NOD32 and ESET Endpoint Security contain two predefined tasks of this type. The first task checks system files at each user logon, the second task does the same after a successful virus signature database update. From an administrator's point of view, the tasks C**omputer scan** and **Update** are probably the most useful:

- **Computer scan** – It provides regular antivirus scan (usually of local drives) on clients.
- **Update** – This task is responsible for updating ESET client solutions. It is a predefined task and by default runs every 60 minutes. Usually there is no reason to modify its parameters. The only exception is for notebooks, since their owners often connect to the Internet outside of the local networks. In this case, the update task can be modified to use two update profiles within one task. This will allow notebooks to update from the local Mirror server, as well as from ESET's update servers.

The Scheduler setup can also be found in the **ESET Configuration Editor** in **Windows product line v3 and v4** > **ESET Kernel** > **Settings** > **Scheduler/Planner** > **Edit**.

For more information see chapter ESET Configuration Editor 58.

The dialog window may contain existing tasks (click **Edit** to modify them) or it may be empty. It depends on whether you have opened a configuration from a client (e.g., from a previously configured and working client) or opened a new file with the default template containing no tasks.

Every new task is assigned an attribute ID. Default tasks have decimal IDs (1, 2, 3...) and custom tasks are assigned hexadecimal keys (e.g., *4AE13D6C*), which are automatically generated when creating a new task.

If the check box for a task is selected, it means that the task is active and that it will be performed on the given client.

The buttons in the Scheduled tasks window function in the following way:

- **Add** – Adds a new task
- **Edit** – Modifies selected tasks
- **Change ID** – Modifies ID of selected tasks
- **Details** – Summary information about the selected tasks
- **Mark for deletion** – Application of *.xml* file will remove tasks (with the same ID) selected by clicking this button from target clients.

- **Remove from list** – Deletes selected tasks from the list. Please note that tasks removed from the list in the.xml configuration will not be removed from target workstations.

When creating a new task (**Add** button) or when editing an existing one (**Edit**), you must specify when it will run. The task can repeat after a certain period of time (each day at 12, each Friday, etc.) or it can be triggered by an event (after a successful update, the first time the computer starts each day, etc.).

The last step of the task **On-demand computer scans** shows the special settings window, where you can define which configuration will be used for scanning – i.e., which scanning profile and scan targets will be used.

The last step of the **Update** task specifies what update profiles will run within the given task. It is a predefined task and runs every 60 minutes by default. Usually there is no reason to modify its parameters. The only exception is for notebooks, since their owners also connect to the Internet from outside of company networks. The last dialog allows you to specify two different update profiles, covering updates either from a local server or from ESET's update servers.

11.2 Removing existing profiles

Occasionally you may come across duplicate profiles (either update or scan profiles) that were created by mistake. To remove those profiles remotely without damaging other settings in the Scheduler, follow the steps below:

- From ERAC, click the **Clients** tab and then double-click a problematic client.
- From the **Client Properties** window, click the **Configuration** tab. Select the **Then Run ESET Configuration Editor to edit the file** and **Use the downloaded configuration in the new configuration task** options and then click the **New Task** button.
- In the new task wizard, click **Edit**.
- In the Configuration Editor, press **CTRL + D** to deselect (grey) all settings. This helps prevent accidental changes, as any new changes will stand out in blue.
- Right-click on the profile you wish to remove and select **Mark profile for deletion** from the context menu. The profile will be deleted as soon as the task is delivered to clients.

Click the **Console** button in the ESET Configuration Editor and save the settings.

- Verify that the client you selected is in the **Selected items** column on the right. Click **Next** and then click **Finish**.

11.3 Export and other features of client XML configuration

From ERAC, select any clients in the **Clients** tab. Right-click and select **Configuration...** from the context menu. Click **Save As...** to export the assigned configuration of the given client to an *.xml* file (*.xml* configuration files can also be extracted directly from the ESET Endpoint Security program interface). The *.xml* file can be used afterwards for various operations:

- For remote installations, the *.xml* file can be used as a template for a predefined configuration. This means that no new *.xml* file is created and the existing *.xml* file is assigned (**Select...**) to a new install package. The *.xml* configuration files can also be extracted directly from the ESET Endpoint Security program interface.
- For configuring multiple clients, selected clients receive a previously downloaded *.xml* file and adopt the settings which are defined in the file (no new configuration is created, only assigned by the **Select...** button).

Example

An ESET security product is only installed on one workstation. Adjust the settings directly through the program's user interface. When finished, export the settings to an *.xml* file. This *.xml* file can then be used for remote installations to other workstations. This method can be very useful for tasks such as fine-tuning firewall rules, if the *"Policy-based"* mode is to be applied.

11.4 Combined update for notebooks

If there are any mobile devices in your local network (i.e., notebooks), we recommend that you configure a combined update from two sources: ESET's update servers and the local Mirror server. First, notebooks contact the local Mirror server, and if the connection fails (they are outside of the office), they download updates directly from ESET's servers. To allow for this functionality:

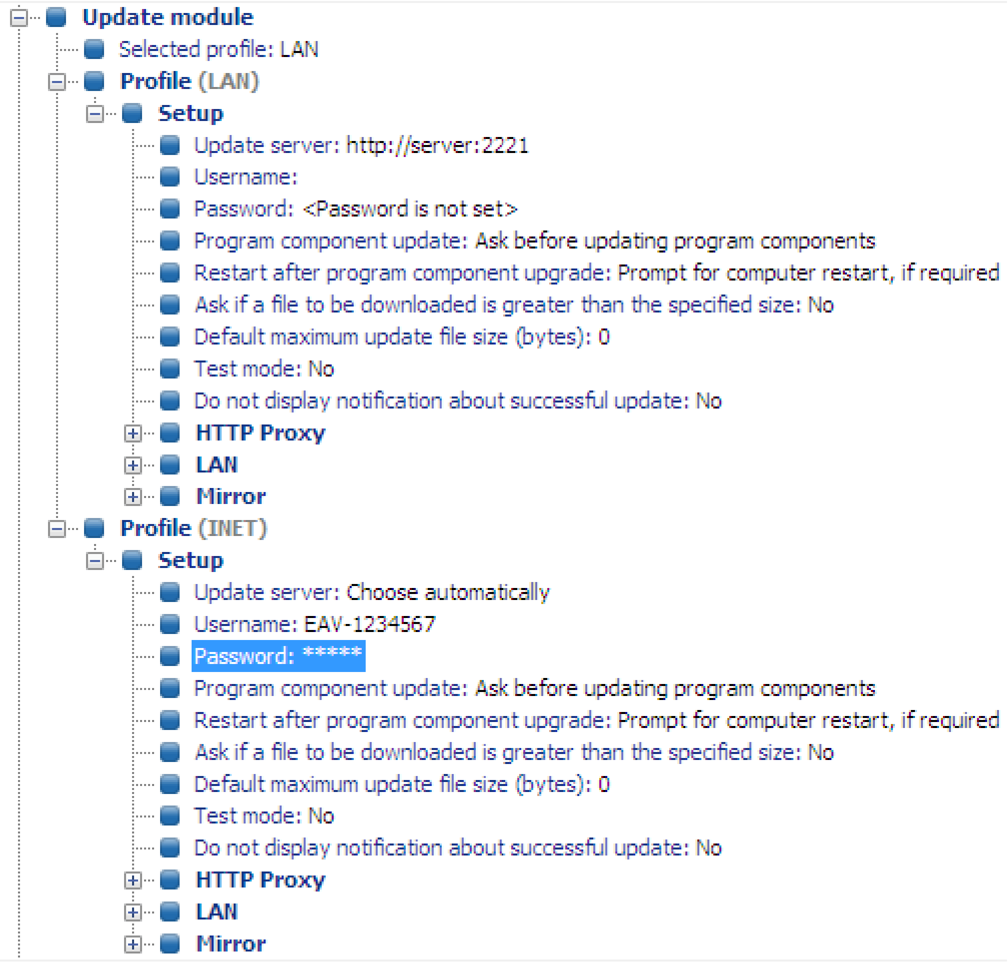
- Create two update profiles, Export and other features of client XML configuration 156 one directed to the Mirror server (referred to as "LAN" in the following example) and the second one to ESET's update servers (INET)

- Create a new update task or modify an existing update task through the Scheduler (**Tools** > **Scheduler** from the main program window of ESET Endpoint Security or ESET Endpoint Antivirus).

The configuration can be made directly on notebooks or remotely using the ESET Configuration Editor. It can be applied either during installation or anytime later as a configuration task.

To create new profiles in ESET Configuration Editor, right-click the **Update** branch and select **New profile** from the context menu.

The result of modifications should resemble the one displayed below:



```
Update module
    Selected profile: LAN
    Profile (LAN)
        Setup
            Update server: http://server:2221
            Username:
            Password: <Password is not set>
            Program component update: Ask before updating program components
            Restart after program component upgrade: Prompt for computer restart, if required
            Ask if a file to be downloaded is greater than the specified size: No
            Default maximum update file size (bytes): 0
            Test mode: No
            Do not display notification about successful update: No
        HTTP Proxy
        LAN
        Mirror
    Profile (INET)
        Setup
            Update server: Choose automatically
            Username: EAV-1234567
            Password: *****
            Program component update: Ask before updating program components
            Restart after program component upgrade: Prompt for computer restart, if required
            Ask if a file to be downloaded is greater than the specified size: No
            Default maximum update file size (bytes): 0
            Test mode: No
            Do not display notification about successful update: No
        HTTP Proxy
        LAN
        Mirror
```

The profile LAN downloads updates from the company's local Mirror server (*http://server:2221*), while the profile INET connects to ESET's servers (**Choose Automatically**). Next, define an update task which runs each update profile in succession. To do this, navigate to **Windows product line v3 and v4** > **ESET Kernel** > **Settings** > **Scheduler/Planner** in the ESET Configuration Editor. Click the **Edit** button to display the **Scheduled tasks** window.

To create a new task, click **Add**. From the **Scheduled task** drop-down menu, select **Update** and click **Next**. Enter the **Task name** (e.g., *"combined update"*), select **Repeatedly every 60 minutes** and proceed to the selection of a primary and secondary profile.

If the notebook workstations should contact the Mirror server first, the Primary profile should be set to LAN and the Secondary profile should be set to INET. The profile INET would only be applied if the update from LAN fails.

Recommendation: Export the current *.xml* configuration from a client (for more information, see chapter How to diagnose problems with ERAS? 154) and perform the above-mentioned modifications on the exported *.xml* file. This will prevent any duplication between the Scheduler and non-working profiles.

11.5 Installation of third party products using ERA

In addition to the remote installation of ESET products, ESET Remote Administrator is capable of installing other programs. The only requirement is that the custom install package must be in the *.msi* format. The remote installation of custom packages can be performed using a process very similar to the one described in Remote Push Install 63.

The main difference is in the package creation process, which is as follows:

1) From ERAC, click the **Remote Install** tab.

2) Select the **Computers** tab and click the **Package Manager** button.

3) From the Package type drop-down menu select **Custom package**.

4) Click **Create...**, click **Add file** and select the desired *.msi* package.

5) Select the file from the **Package entry file** drop-down menu and click **Create**.

6) After returning to the original window click **Save as...** to save the package.

7) If you want to you can specify command line parameters for the *.msi* file. The parameters are the same as for a local installation of the given package. Do not forget to click **Save** in the Package section of the **Package Manager** window afterward.

8) Click **Close** to exit the installation package editor.

The newly created custom package can be distributed to client workstations in the same manner as the remote installations described in previous chapters. A remote push install, logon or email push install will send the package to target workstations. When the package is opened, installation is handled by the Microsoft Windows Installer service. After completing the custom installation, ERAS can download a file from the client that contains install results data. To specify a result file, add the **/eResult** parameter to the command line associated with the package after you save the custom package. After running the custom install task, you can download the result files from ERAS in the **Task Details** window.

NOTE: There is a 100MB size limit for custom third-party installation packages.

12. ESET SysInspector

12.1 Introduction to ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and displays gathered data in a comprehensive way. Information like installed drivers and applications, network connections or important registry entries can help you to investigate suspicious system behavior be it due to software or hardware incompatibility or malware infection.

You can access ESET SysInspector two ways: From the integrated version in ESET Security solutions or by downloading the standalone version (SysInspector.exe) for free from ESET’s website. Both versions are identical in function and have the same program controls. The only difference is how outputs are managed. The standalone and integrated versions each allow you to export system snapshots to an *.xml* file and save them to disk. However, the integrated version also allows you to store your system snapshots directly in **Tools** > **ESET SysInspector** (except ESET Remote Administrator).

Please allow some time while ESET SysInspector scans your computer. It may take anywhere from 10 seconds up to a few minutes depending on your hardware configuration, operating system and the number of applications installed on your computer.

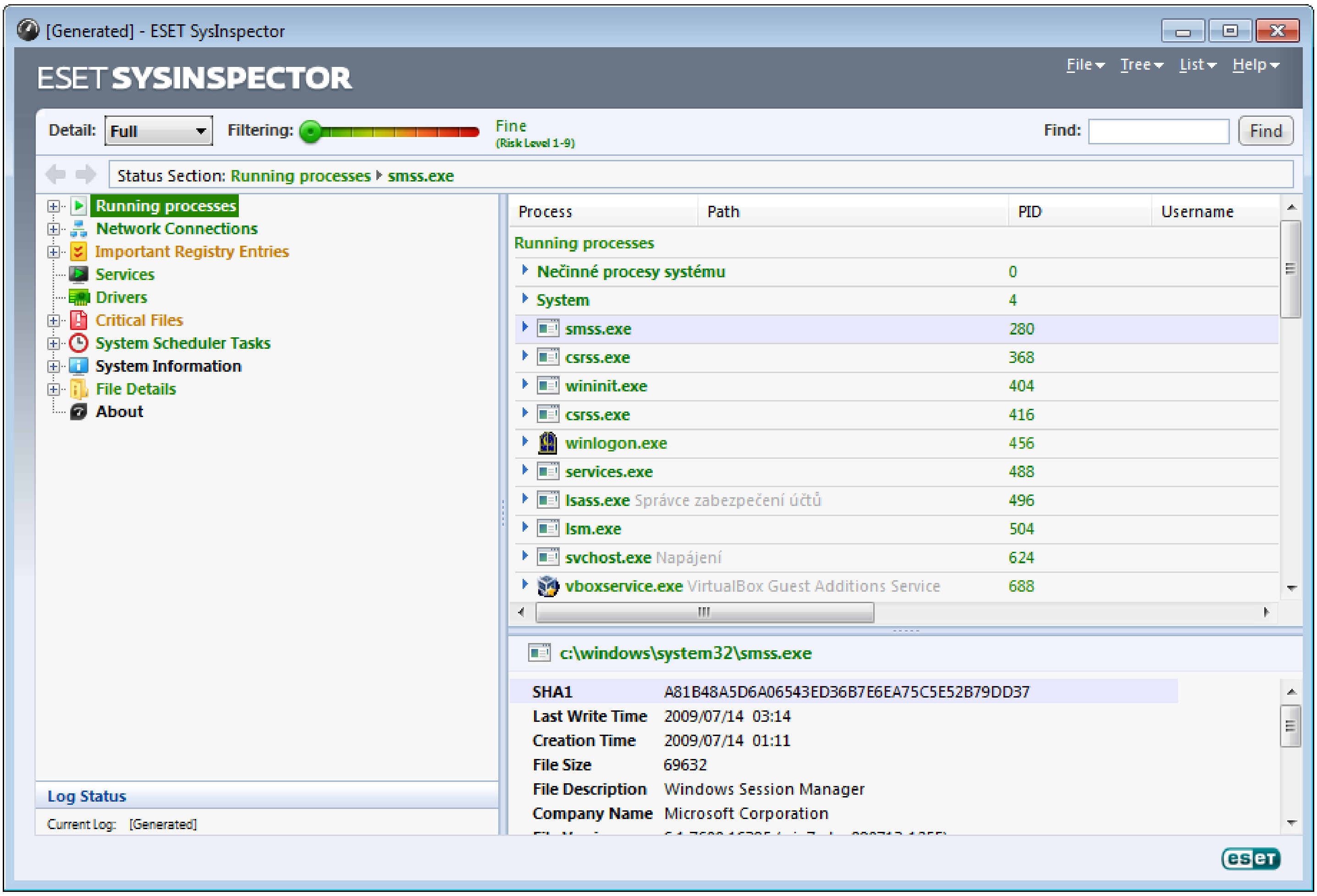
12.1.1 Starting ESET SysInspector

To start ESET SysInspector, simply run the *SysInspector.exe* executable you downloaded from ESET's website.

Please wait while the application inspects your system, which could take up to several minutes depending on your hardware and data to be gathered.

12.2 User Interface and application usage

For clarity the Main window is divided into four major sections – Program Controls located on the top of the Main window, the Navigation window on the left, the Description window on the right in the middle and the Details window on the right at the bottom of the Main window. The Log Status section lists the basic parameters of a log (filter used, filter type, is the log a result of a comparison etc.).



Detail: Full

Filtering: Fine (Risk Level 1-9)

Find:

Status Section: Running processes ▸ smss.exe

Process	Path	PID	Username
Running processes			
Nečinné procesy systému		0	
System		4	
smss.exe		280	
csrss.exe		368	
wininit.exe		404	
csrss.exe		416	
winlogon.exe		456	
services.exe		488	
lsass.exe Správce zabezpečení účtů		496	
lsm.exe		504	
svchost.exe Napájení		624	
vboxservice.exe VirtualBox Guest Additions Service		688	

c:\windows\system32\smss.exe

SHA1	A81B48A5D6A06543ED36B7E6EA75C5E52B79DD37
Last Write Time	2009/07/14 03:14
Creation Time	2009/07/14 01:11
File Size	69632
File Description	Windows Session Manager
Company Name	Microsoft Corporation

Log Status

Current Log: [Generated]

12.2.1 Program Controls

This section contains the description of all program controls available in ESET SysInspector.

File

By clicking **File** you can store your current system status for later investigation or open a previously stored log. For publishing purposes we recommend that you generate a log **Suitable for sending**. In this form, the log omits sensitive information (current user name, computer name, domain name, current user privileges, environment variables, etc.).

NOTE: You may open previously stored ESET SysInspector reports by simply dragging and dropping them into the Main window.

Tree

Enables you to expand or close all nodes and export selected sections to Service script.

List

Contains functions for easier navigation within the program and various other functions like finding information online.

Help

Contains information about the application and its functions.

Detail

This setting influences the information displayed in the Main window to make the information easier to work with. In "Basic" mode, you have access to information used to find solutions for common problems in your system. In the "Medium" mode, the program displays less used details. In "Full" mode, ESET SysInspector displays all the information needed to solve very specific problems.

Item filtering

Item filtering is best used to find suspicious files or registry entries in your system. By adjusting the slider, you can filter items by their Risk Level. If the slider is set all the way to the left (Risk Level 1), then all items are displayed. By moving the slider to the right, the program filters out all items less risky than current Risk Level and only display items which are more suspicious than the displayed level. With the slider all the way to the right, the program displays only known harmful items.

All items labeled as risk 6 to 9 can pose security risk. If you are not using a security solution from ESET, we recommend that you scan your system with ESET Online Scanner if ESET SysInspector has found any such item. ESET Online Scanner is a free service.

NOTE: The Risk level of an item can be quickly determined by comparing the color of the item with the color on the Risk Level slider.

Search

Search can be used to quickly find a specific item by its name or part of its name. The results of the search request are displayed in the Description window.

Return

By clicking the back or forward arrow, you may return to previously displayed information in the Description window. You may use the backspace and space keys instead of clicking back and forward.

Status section

Displays the current node in Navigation window.

Important: Items highlighted in red are unknown, which is why the program marks them as potentially dangerous. If an item is in red, it does not automatically mean that you can delete the file. Before deleting, please make sure that files are really dangerous or unnecessary.

12.2.2 Navigating in ESET SysInspector

ESET SysInspector divides various types of information into several basic sections called nodes. If available, you may find additional details by expanding each node into its subnodes. To open or collapse a node, double-click the name of the node or alternatively click ⊞ or ⊟ next to the name of the node. As you browse through the tree structure of nodes and subnodes in the Navigation window you may find various details for each node shown in the Description window. If you browse through items in the Description window, additional details for each item may be displayed in the Details window.

The following are the descriptions of the main nodes in the Navigation window and related information in the Description and Details windows.

Running processes

This node contains information about applications and processes running at the time of generating the log. In the Description window you may find additional details for each process such as dynamic libraries used by the process and their location in the system, the name of the application's vendor and the risk level of the file.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

NOTE: An operating system comprises of several important kernel components running 24/7 that provide basic and vital functions for other user applications. In certain cases, such processes are displayed in the tool ESET SysInspector with file path beginning with \??\. Those symbols provide pre-launch optimization for those processes; they are safe for the system.

Network connections

The Description window contains a list of processes and applications communicating over the network using the protocol selected in the Navigation window (TCP or UDP) along with the remote address where to which the application is connected to. You can also check the IP addresses of DNS servers.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

Important Registry Entries

Contains a list of selected registry entries which are often related to various problems with your system like those specifying startup programs, browser helper objects (BHO), etc.

In the Description window you may find which files are related to specific registry entries. You may see additional details in the Details window.

Services

The Description window Contains a list of files registered as windows Services. You may check the way the service is set to start along with specific details of the file in the Details window.

Drivers

A list of drivers installed in the system.

Critical files

The Description window displays content of critical files related to the Microsoft windows operating system.

System Scheduler Tasks

Contains a list of tasks triggered by Windows Task Scheduler at a specified time/interval.

System information

Contains detailed information about hardware and software along with information about set environmental variables, user rights and system event logs.

File details

A list of important system files and files in the Program Files folder. Additional information specific for the files can be found in the Description and Details windows.

About

Information about version of ESET SysInspector and the list of program modules.

12.2.2.1 Keyboard shortcuts

Key shortcuts that can be used when working with the ESET SysInspector include:

File

Ctrl+O	opens existing log
Ctrl+S	saves created logs

Generate

Ctrl+G	generates a standard computer status snapshot
Ctrl+H	generates a computer status snapshot that may also log sensitive information

Item Filtering

1, O	fine, risk level 1-9 items are displayed
2	fine, risk level 2-9 items are displayed
3	fine, risk level 3-9 items are displayed
4, U	unknown, risk level 4-9 items are displayed
5	unknown, risk level 5-9 items are displayed
6	unknown, risk level 6-9 items are displayed
7, B	risky, risk level 7-9 items are displayed
8	risky, risk level 8-9 items are displayed
9	risky, risk level 9 items are displayed
-	decreases risk level
+	increases risk level
Ctrl+9	filtering mode, equal level or higher
Ctrl+0	filtering mode, equal level only

View

Ctrl+5	view by vendor, all vendors
Ctrl+6	view by vendor, only Microsoft
Ctrl+7	view by vendor, all other vendors
Ctrl+3	displays full detail
Ctrl+2	displays medium detail
Ctrl+1	basic display
BackSpace	moves one step back
Space	moves one step forward
Ctrl+W	expands tree
Ctrl+Q	collapses tree

Other controls

Ctrl+T	goes to the original location of item after selecting in search results
Ctrl+P	displays basic information about an item
Ctrl+A	displays full information about an item
Ctrl+C	copies the current item's tree
Ctrl+X	copies items
Ctrl+B	finds information about selected files on the Internet
Ctrl+L	opens the folder where the selected file is located
Ctrl+R	opens the corresponding entry in the registry editor
Ctrl+Z	copies a path to a file (if the item is related to a file)
Ctrl+F	switches to the search field
Ctrl+D	closes search results
Ctrl+E	run service script

Comparing

Ctrl+Alt+O	opens original / comparative log
Ctrl+Alt+R	cancels comparison
Ctrl+Alt+1	displays all items
Ctrl+Alt+2	displays only added items, log will show items present in current log
Ctrl+Alt+3	displays only removed items, log will show items present in previous log
Ctrl+Alt+4	displays only replaced items (files inclusive)
Ctrl+Alt+5	displays only differences between logs
Ctrl+Alt+C	displays comparison
Ctrl+Alt+N	displays current log
Ctrl+Alt+P	opens previous log

Miscellaneous

F1	view help

Alt+F4	close program
Alt+Shift+F4	close program without asking
Ctrl+I	log statistics

12.2.3 Compare

The Compare feature allows the user to compare two existing logs. The outcome of this feature is a set of items not common to both logs. It is suitable if you want to keep track of changes in the system, a helpful tool for detecting activity of malicious code.

After it is launched, the application creates a new log which is displayed in a new window. Navigate to **File** > **Save log** to save a log to a file. Log files can be opened and viewed at a later time. To open an existing log, use **File** > **Open log**. In the main program window, ESET SysInspector always displays one log at a time.

The benefit of comparing two logs is that you can view a currently active log and a log saved in a file. To compare logs, use the option **File** > **Compare log** and choose **Select file**. The selected log will be compared to the active one in the main program windows. The comparative log will display only the differences between those two logs.

NOTE: If you compare two log files, select **File** > **Save log** to save it as a ZIP file; both files are saved. If you open this file later, the contained logs are automatically compared.

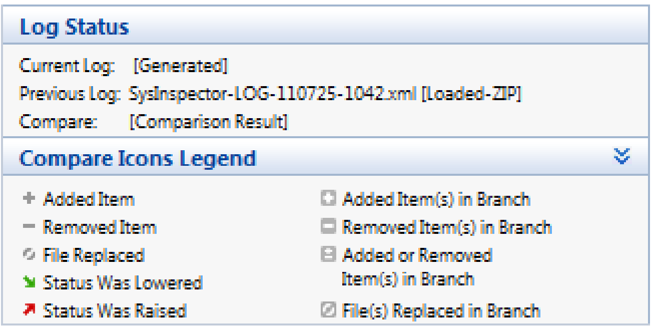
Next to the displayed items, ESET SysInspector shows symbols identifying differences between the compared logs.

Items marked by a – can only be found in the active log and were not present in the opened comparative log. Items marked by a + were present only in the opened log and are missing in the active one.

Description of all symbols that can be displayed next to items:

- + new value, not present in the previous log
- ⊞ tree structure section contains new values
- – removed value, present in the previous log only
- ⊟ tree structure section contains removed values
- ⟳ value / file has been changed
- ⧄ tree structure section contains modified values / files
- ↘ the risk level has decreased / it was higher in the previous log
- ↗ the risk level has increased / it was lower in the previous log

The explanation section displayed in the left bottom corner describes all symbols and also displays the names of logs which are being compared.



Log Status

Current Log: [Generated]
Previous Log: SysInspector-LOG-110725-1042.xml [Loaded-ZIP]
Compare: [Comparison Result]

Compare Icons Legend

+ Added Item	⊞ Added Item(s) in Branch
– Removed Item	⊟ Removed Item(s) in Branch
⟳ File Replaced	⊟ Added or Removed Item(s) in Branch
↘ Status Was Lowered	
↗ Status Was Raised	⧄ File(s) Replaced in Branch

Any comparative log can be saved to a file and opened at a later time.

Example

Generate and save a log, recording original information about the system, to a file named previous.xml. After changes to the system have been made, open ESET SysInspector and allow it to generate a new log. Save it to a file named *current.xml*.

In order to track changes between those two logs, navigate to **File** > **Compare logs**. The program will create a comparative log showing differences between the logs.

The same result can be achieved if you use the following command line option:

SysIsnpector.exe current.xml previous.xml

12.3 Command line parameters

ESET SysInspector supports generating reports from the command line using these parameters:

/gen generate a log directly from the command line without running the GUI
/privacy generate a log excluding sensitive information
/zip store the resulting log directly on the disk in a compressed file
/silent suppress the display of the log generation progress bar
/help, /? display information about the command line parameters

Examples

To load a specific log directly in the browser, use: *SysInspector.exe "c:\clientlog.xml"*
To generate a log to a current location, use: *SysInspector.exe /gen*
To generate a log to a specific folder, use: *SysInspector.exe /gen="c:\folder\"*
To generate a log to a specific file/location, use: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
To generate a log excluding sensitive information directly in a compressed file, use: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
To compare two logs, use: *SysInspector.exe "current.xml" "original.xml"*

NOTE: If the name of the file/folder contains a gap, then should be taken into inverted commas.

12.4 Service Script

Service script is a tool that provides help to customers that use ESET SysInspector by easily removing unwanted objects from the system.

Service script enables the user to export the entire ESET SysInspector log, or its selected parts. After exporting, you can mark unwanted objects for deletion. You can then run the modified log to delete marked objects.

Service Script is suited for advanced users with previous experience in diagnosing system issues. Unqualified modifications may lead to operating system damage.

Example

If you have a suspicion that your computer is infected by a virus which is not detected by your antivirus program, follow the step-by-step instructions below:

- Run ESET SysInspector to generate a new system snapshot.
- Select the first item in the section on the left (in the tree structure), press Shift and select the last item to mark all items.
- Right click the selected objects and select the **Export Selected Sections To Service Script** context menu option.
- The selected objects will be exported to a new log.
- This is the most crucial step of the entire procedure: open the new log and change the – attribute to + for all objects you want to remove. Please make sure you do not mark any important operating system files/objects.
- Open ESET SysInspector, click **File** > **Run Service Script** and enter the path to your script.
- Click **OK** to run the script.

12.4.1 Generating Service script

To generate a script, right-click any item from the menu tree (in the left pane) in the ESET SysInspector main window. From the context menu, select either the **Export All Sections To Service Script** option or the **Export Selected Sections To Service Script** option.

NOTE: It is not possible to export the service script when two logs are being compared.

12.4.2 Structure of the Service script

In the first line of the script's header, you can find information about the Engine version (ev), GUI version (gv) and the Log version (lv). You can use this data to track possible changes in the .xml file that generates the script and prevent any inconsistencies during execution. This part of the script should not be altered.

The remainder of the file is divided into sections in which items can be edited (denote those that will be processed by the script). You mark items for processing by replacing the "-" character in front of an item with a "+" character. Sections in the script are separated from each other by an empty line. Each section has a number and title.

01) Running processes

This section contains a list of all processes running in the system. Each process is identified by its UNC path and, subsequently, its CRC16 hash code in asterisks (*).

Example:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In this example a process, module32.exe, was selected (marked by a "+" character); the process will end upon execution of the script.

02) Loaded modules

This section lists currently used system modules.

Example:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In this example the module khbekhb.dll was marked by a "+". When the script runs, it will recognize the processes using that specific module and end them.

03) TCP connections

This section contains information about existing TCP connections.

Example:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

When the script runs, it will locate the owner of the socket in the marked TCP connections and stop the socket, freeing system resources.

04) UDP endpoints

This section contains information about existing UDP endpoints.

Example:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

When the script runs, it will isolate the owner of the socket at the marked UDP endpoints and stop the socket.

05) DNS server entries

This section contains information about the current DNS server configuration.

Example:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Marked DNS server entries will be removed when you run the script.

06) Important registry entries

This section contains information about important registry entries.

Example:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = “C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe” /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

The marked entries will be deleted, reduced to 0-byte values or reset to their default values upon script execution. The action to be applied to a particular entry depends on the entry category and key value in the specific registry.

07) Services

This section lists services registered within the system.

Example:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

The services marked and their dependant services will be stopped and uninstalled when the script is executed.

08) Drivers

This section lists installed drivers.

Example:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

When you execute the script, the drivers selected will be stopped. Note that some drivers won't allow themselves to be stopped.

09) Critical files

This section contains information about files that are critical to proper function of the operating system.

Example:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

The selected items will either be deleted or reset to their original values.

12.4.3 Executing Service scripts

Mark all desired items, then save and close the script. Run the edited script directly from the ESET SysInspector main window by selecting the **Run Service Script** option from the File menu. When you open a script, the program will prompt you with the following message: **Are you sure you want to run the service script “%Scriptname%”?** After you confirm your selection, another warning may appear, informing you that the service script you are trying to run has not been signed. Click **Run** to start the script.

A dialog window will confirm that the script was successfully executed.

If the script could only be partially processed, a dialog window with the following message will appear: **The service script was run partially. Do you want to view the error report?** Select **Yes** to view a complex error report listing the operations that were not executed.

If the script was not recognized, a dialog window with the following message will appear: **The selected service script is not signed. Running unsigned and unknown scripts may seriously harm your computer data. Are you sure you want to run the script and carry out the actions?** This may be caused by inconsistencies within the script (damaged heading, corrupted section title, empty line missing between sections etc.). You can either reopen the script file and correct the errors within the script or create a new service script.

12.5 FAQ

Does ESET SysInspector require Administrator privileges to run ?

While ESET SysInspector does not require Administrator privileges to run, some of the information it collects can only be accessed from an Administrator account. Running it as a Standard User or a Restricted User will result in it collecting less information about your operating environment.

Does ESET SysInspector create a log file ?

ESET SysInspector can create a log file of your computer's configuration. To save one, select **File** > **Save Log** from the main menu. Logs are saved in XML format. By default, files are saved to the *%USERPROFILE%\My Documents* directory, with a file naming convention of "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". You may change the location and name of the log file to something else before saving if you prefer.

How do I view the ESET SysInspector log file ?

To view a log file created by ESET SysInspector, run the program and select **File** > **Open Log** from the main menu. You can also drag and drop log files onto the ESET SysInspector application. If you need to frequently view ESET SysInspector log files, we recommend creating a shortcut to the SYSINSPECTOR.EXE file on your Desktop; you can then drag and drop log files onto it for viewing. For security reasons Windows Vista/7 may not allow drag and drop between windows that have different security permissions.

Is a specification available for the log file format? What about an SDK ?

At the current time, neither a specification for the log file or an SDK are available since the program is still in development. After the program has been released, we may provide these based on customer feedback and demand.

How does ESET SysInspector evaluate the risk posed by a particular object ?

In most cases, ESET SysInspector assigns risk levels to objects (files, processes, registry keys and so forth) using a series of heuristic rules that examine the characteristics of each object and then weight the potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1 - Fine (green) to 9 - Risky (red). In the left navigation pane, sections are colored based on the highest risk level of an object inside them.

Does a risk level of "6 - Unknown (red)" mean an object is dangerous ?

ESET SysInspector's assessments do not guarantee that an object is malicious – that determination should be made by a security expert. What ESET SysInspector is designed for is to provide a quick assessment for security experts so that they know what objects on a system they may want to further examine for unusual behavior.

Why does ESET SysInspector connect to the Internet when run ?

Like many applications, ESET SysInspector is signed with a digital signature "certificate" to help ensure the software was published by ESET and has not been altered. In order to verify the certificate, the operating system contacts a certificate authority to verify the identity of the software publisher. This is normal behavior for all digitally-signed programs under Microsoft Windows.

What is Anti-Stealth technology ?

Anti-Stealth technology provides effective rootkit detection.

If the system is attacked by malicious code that behaves as a rootkit, the user may be exposed to data loss or theft. Without a special anti-rootkit tool, it is almost impossible to detect rootkits.

Why are there sometimes files marked as "Signed by MS", having a different "Company Name" entry at the same time ?

When trying to identify the digital signature of an executable, ESET SysInspector first checks for a digital signature embedded in the file. If a digital signature is found, the file will be validated using that information. If a digital signature is not found, the ESI starts looking for the corresponding CAT file (Security Catalog - *%systemroot%*

\system32\catroot) that contains information about the executable file processed. If the relevant CAT file is found, the digital signature of that CAT file will be applied in the validation process of the executable.

This is why there are sometimes files marked as "Signed by MS", but having a different "CompanyName" entry.

Example:

Windows 2000 includes the HyperTerminal application located in *C:\Program Files\Windows NT*. The main application executable file is not digitally signed, but ESET SysInspector marks it as a file signed by Microsoft. The reason for this is a reference in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* pointing to *C:\Program Files\Windows NT\hypertrm.exe* (the main executable of the HyperTerminal application) and *sp4.cat* is digitally signed by Microsoft.

13. ESET SysRescue

ESET SysRescue is a utility which enables you to create a bootable disk containing one of the ESET Security solutions - it can be ESET NOD32 Antivirus, ESET Smart Security or even some of the server-oriented products. The main advantage of ESET SysRescue is the fact that ESET Security solution runs independent of the host operating system, while it has a direct access to the disk and the entire file system. This makes it possible to remove infiltrations which normally could not be deleted, e.g., when the operating system is running, etc.

13.1 Minimum requirements

ESET SysRescue works in the Microsoft Windows Preinstallation Environment (Windows PE) version 2.x, which is based on Windows Vista.

Windows PE is a part of the free package Windows Automated Installation Kit (Windows AIK), and therefore Windows AIK must be installed before creating ESET SysRescue (http://go.eset.eu/AIK). Due to the support of the 32-bit version of Windows PE, it is necessary to use a 32-bit installation package of ESET Security solution when creating ESET SysRescue on 64-bit systems. ESET SysRescue supports Windows AIK 1.1 and higher.

NOTE: Since Windows AIK is over 1 GB in size, a high-speed internet connection is required for smooth download.

ESET SysRescue is available in ESET Security solutions version 4.0 and higher.

Supported operating systems

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 with KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 with KB926044
- Windows XP Service Pack 3

13.2 How to create rescue CD

To launch the ESET SysRescue wizard, click **Start** > **Programs** > **ESET** > **ESET Remote Administrator** > **ESET SysRescue**.

First, the wizard checks for the presence of Windows AIK and a suitable device for the boot media creation. If Windows AIK is not installed on the computer (or it is either corrupt or installed incorrectly), the wizard will offer you the option to install it, or to enter the path to your Windows AIK folder (http://go.eset.eu/AIK).

NOTE: Since Windows AIK is over 1 GB in size, a high-speed internet connection is required for smooth download.

In the next step 171, select the target media where ESET SysRescue will be located.

13.3 Target selection

In addition to CD/DVD/USB, you can choose to save ESET SysRescue in an ISO file. Later on, you can burn the ISO image on CD/DVD, or use it some other way (e.g. in the virtual environment such as VMware or VirtualBox).

If you select USB as the target medium, booting may not work on certain computers. Some BIOS versions may report problems with the BIOS - boot manager communication (e.g. on Windows Vista) and booting exits with the following error message:

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attemping to read the boot configuration data
```

If you encounter this message, we recommend selecting CD instead of USB medium.

13.4 Settings

Before initiating ESET SysRescue creation, the install wizard displays compilation parameters in the last step of the ESET SysRescue wizard. These can be modified by clicking the **Change...** button. The available options include:

- Folders 172
- ESET Antivirus 172
- Advanced 173
- Internet protocol 173
- Bootable USB device 173 (when the target USB device is selected)
- Burning 173 (when the target CD/DVD drive is selected)

The **Create** button is inactive if no MSI installation package is specified, or if no ESET Security solution is installed on the computer. To select an installation package, click the **Change** button and go to the **ESET Antivirus** tab. Also, if you do not fill in username and password (**Change** > **ESET Antivirus**), the **Create** button is greyed out.

13.4.1 Folders

Temporary folder is a working directory for files required during ESET SysRescue compilation.

ISO folder is a folder, where the resulting ISO file is saved after the compilation is completed.

The list on this tab shows all local and mapped network drives together with the available free space. If some of the folders here are located on a drive with insufficient free space, we recommend that you select another drive with more free space available. Otherwise compilation may end prematurely due to insufficient free disk space.

External applications – Allows you to specify additional programs that will be run or installed after booting from a ESET SysRescue medium.

Include external applications – Allows you to add external programs to the ESET SysRescue compilation.

Selected folder – Folder in which programs to be added to the ESET SysRescue disk are located.

13.4.2 ESET Antivirus

For creating the ESET SysRescue CD, you can select two sources of ESET files to be used by the compiler.

ESS/EAV folder – Files already contained in the folder to which the ESET Security solution is installed on the computer.

MSI file – Files contained in the MSI installer are used.

Next, you can choose to update the location of (.nup) files. Normally, the default option **ESS/EAV folder/MSI file** should be set. In some cases, a custom **Update folder** can be chosen, e.g., to use an older or newer virus signature database version.

You can use one of the following two sources of username and password:

Installed ESS/EAV – Username and password will be copied from the currently installed ESET Security solution.

From user – Username and password entered in the corresponding text boxes will be used.

NOTE: ESET Security solution on the ESET SysRescue CD is updated either from the Internet or from the ESET Security solution installed on the computer on which the ESET SysRescue CD is run.

13.4.3 Advanced settings

The **Advanced** tab lets you optimize the ESET SysRescue CD according to the amount of memory on your computer. Select **576 MB and more** to write the content of the CD to the operating memory (RAM). If you select **less than 576 MB**, the recovery CD will be permanently accessed when WinPE will be running.

In the **External drivers** section, you can insert drivers for your specific hardware (usually network adapter). Although WinPE is based on Windows Vista SP1, which supports a large range of hardware, occasionally hardware is not recognized. This will required that you add a driver manually. There are two ways of introducing a driver into an ESET SysRescue compilation - manually (the **Add** button) and automatically (the **Aut. Search** button). In the case of manual inclusion, you need to select the path to the corresponding .inf file (applicable *.sys file must also be present in this folder). In the case of automatic introduction, the driver is found automatically in the operating system of the given computer. We recommend using automatic inclusion only if ESET SysRescue is used on a computer that has the same network adapter as the computer on which the ESET SysRescue CD was created. During creation, the ESET SysRescue driver is introduced into the compilation so you do not need to look for it later.

13.4.4 Internet protocol

This section allows you to configure basic network information and set up predefined connections after ESET SysRescue.

Select **Automatic private IP address** to obtain the IP address automatically from DHCP (Dynamic Host Configuration Protocol) server.

Alternatively, this network connection can use a manually specified IP address (also known as a static IP address). Select **Custom** to configure the appropriate IP settings. If you select this option, you must specify an **IP address** and, for LAN and high-speed Internet connections, a **Subnet mask**. In **Preferred DNS server** and **Alternate DNS server**, type the primary and secondary DNS server addresses.

13.4.5 Bootable USB device

If you have selected a USB device as your target medium, you can select one of the available USB devices on the **Bootable USB device** tab (in case there are more USB devices).

Select the appropriate target **Device** where ESET SysRescue will be installed.

Warning: The selected USB device will be formatted during the creation of ESET SysRescue. All data on the device will be deleted.

If you choose the **Quick format** option, formatting removes all the files from the partition, but does not scan the disk for bad sectors. Use this option if your USB device has been formatted previously and you are sure that it is not damaged.

13.4.6 Burn

If you have selected CD/DVD as your target medium, you can specify additional burning parameters on the **Burn** tab.

Delete ISO file – Check this option to delete the temporary ISO file after the ESET SysRescue CD is created.

Deletion enabled – Enables you to select fast erasing and complete erasing.

Burning device – Select the drive to be used for burning.

Warning: This is the default option. If a rewritable CD/DVD is used, all the data on the CD/DVD will be erased.

The Medium section contains information about the medium in your CD/DVD device.

Burning speed – Select the desired speed from the drop-down menu. The capabilities of your burning device and the type of CD/DVD used should be considered when selecting the burning speed.

13.5 Working with ESET SysRescue

For the rescue CD/DVD/USB to work effectively, you must start your computer from the ESET SysRescue boot media. Boot priority can be modified in the BIOS. Alternatively, you can use the boot menu during computer startup – usually using one of the F9 - F12 keys depending on the version of your motherboard/BIOS.

After booting up from the boot media, ESET Security solution will start. Since ESET SysRescue is used only in specific situations, some protection modules and program features present in the standard version of ESET Security solution are not needed; their list is narrowed down to **Computer scan**, **Update**, and some sections in **Setup**. The ability to update the virus signature database is the most important feature of ESET SysRescue, we recommend that you update the program prior starting a Computer scan.

13.5.1 Using ESET SysRescue

Suppose that computers in the network have been infected by a virus which modifies executable (.exe) files. ESET Security solution is capable of cleaning all infected files except for *explorer.exe*, which cannot be cleaned, even in Safe mode. This is because *explorer.exe*, as one of the essential Windows processes, is launched in Safe mode as well. ESET Security solution would not be able to perform any action with the file and it would remain infected.

In this type of scenario, you could use ESET SysRescue to solve the problem. ESET SysRescue does not require any component of the host operating system, and is therefore capable of processing (cleaning, deleting) any file on the disk.

14. Appendix - Third Party License

ESET acknowledges that Software includes third party code that is subject to following third party licenses:

3-clause BSD License ("New BSD License")

Copyright (c) <YEAR>, <OWNER>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>
Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>
Copyright (c) 2006-2007 The Written Word, Inc.
Copyright (c) 2007 Eli Fant <elifantu@mail.ru>
Copyright (c) 2009 Daniel Stenberg
Copyright (C) 2008, 2009 Simon Josefsson
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the copyright holder nor the names of any other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.“
