

ESET

Remote

Administrator

Installation Manual
and User Guide



we protect your digital worlds ©

1. Introduction	4
2. ERA – client/server architecture	5
2.1 ERA Server (ERAS).....	5
2.1.1 Requirements.....	5
2.1.2 ERAS hierarchy at large networks	6
2.1.3 Installation.....	7
2.1.4 Logs	7
2.1.5 Configuration	7
2.1.6 License keys.....	7
2.1.7 Database & information storage.....	8
2.2 ERA Console (ERAC)	8
3. Other ESET components in network environment	9
3.1 ESET client solutions.....	9
3.2 ESET Configuration Editor	9
3.2.1 Configuration layering	10
3.2.2 Key configuration entries	10
3.3 LAN Update Server -Mirror	11
3.3.1 Operation of Mirror server	12
3.3.2 Types of updates	12
3.3.3 How to enable and configure Mirror.....	13
4. ESET Remote Administrator Console in detail 15	15
4.1 Connecting to ERAS	15
4.2 ERAC – main screen.....	15
4.3 Information filtering.....	16
4.3.1 Groups	16
4.3.2 Filter	16
4.3.3 Context menu.....	17
4.3.4 Views.....	18
4.4 Tabs in ERAC.....	18
4.4.1 General description of tabs and clients	18
4.4.2 Replication & information in individual tabs	18
4.4.3 Clients tab	19
4.4.4 Threat Log tab	22
4.4.5 Firewall Log tab	22
4.4.6 Event Log tab.....	22
4.4.7 The Scan Log tab.....	23
4.4.8 Tasks tab	23
4.4.9 Reports tab	23
4.4.10 Remote Install tab	25
4.5 ERA Console setup	25
4.5.1 Connection tab.....	25
4.5.2 Columns – Show / Hide tab.....	25
4.5.3 Colors tab.....	25
4.5.4 Paths tab.....	25
4.5.5 Date / Time tab	25
4.5.6 Other Settings tab	25
4.6 Configuring ERA Server using the Console	26
4.6.1 General tab.....	26
4.6.2 Security tab	26
4.6.3 Server Maintenance tab	27
4.6.4 Logging tab	27
4.6.5 Replication tab	27

ESET Remote Administrator

Copyright © 2008 by ESET, spol. s r.o.

ESET Remote Administrator was developed by ESET, spol. s r.o.
For more information visit www.eset.com.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r.o., reserves the right to change any of the described application software without prior notice.

Customer Care Worldwide: www.eset.eu/support
Customer Care North America: www.eset.com/support

4.6.6	Updates	29
4.6.7	Other Settings tab	29
5.	Tasks	30
5.1	Configuration Task	30
5.2	On-Demand Scan task	31
5.3	Update Now task	31
6.	Installation of ESET's client solutions	32
6.1	Command line parameters for direct installation of client solutions	32
6.2	Installation methods	32
6.2.1	Direct installation with predefined XML configuration	32
6.2.2	Remote installation in general	33
6.2.3	Remote push install	34
6.2.4	Logon / email remote install	37
6.2.5	Custom remote install	39
6.3	The installer.exe agent in detail	39
6.4	Avoiding repeated installations	40
6.5	Installation process – error messages	40
6.5.1	Remote Install Diagnostics	41
7.	Deployment scenarios for ESET Remote Administrator, Mirror server and ESET client solutions	42
7.1	Small network – 1x ERAS, 1x Mirror server	42
7.1.1	Installation of HTTP Mirror server	42
7.1.2	Installation of ERA Server	43
7.1.3	Installation of ERA Console	43
7.1.4	Remote install on workstations present in the network	43
7.1.5	Remote install on notebooks currently not present in the network	44
7.2	Company with a remote subsidiary – 2x ERAS, 2x Mirror server	46
7.2.1	Installations at headquarters	46
7.2.2	Subsidiary: installation of ERA Server	47
7.2.3	Subsidiary: Installation of HTTP Mirror server	47
7.2.4	Subsidiary: Remote installation to clients	47
8.	Hints & tips	48
8.1	Export and other features of client XML configuration	48
8.2	Combined update for notebooks and mobile devices	48
8.3	Removing existing profiles	49
8.4	Scheduler setup	50
8.5	Custom install packages	51

1. Introduction

ESET Remote Administrator is an application which allows you to manage ESET's products in a networked environment. ESET Remote Administrator (ERA) is a solution which allows you to administer ESET products, including workstations and servers – from one central location. Thanks to ESET Remote Administrator's built-in task management system, you can quickly respond to new problems threats, and - last but not least – install ESET solutions on remote computers.

ESET Remote Administrator itself does not provide any other form of protection against malicious code, such as viruses and worms. ERA depends on the presence of an ESET solution on workstations or servers, such as ESET NOD32 Antivirus or ESET Smart Security.

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

- Installation of ERA Server (ERAS),
- Installation of ERA Console (ERAC),
- Installation of Mirror server,
- Installation of client computers (ESET NOD32 Antivirus, ESET Smart Security, ESET Server Edition, etc...).

NOTE: Some parts of this document will 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

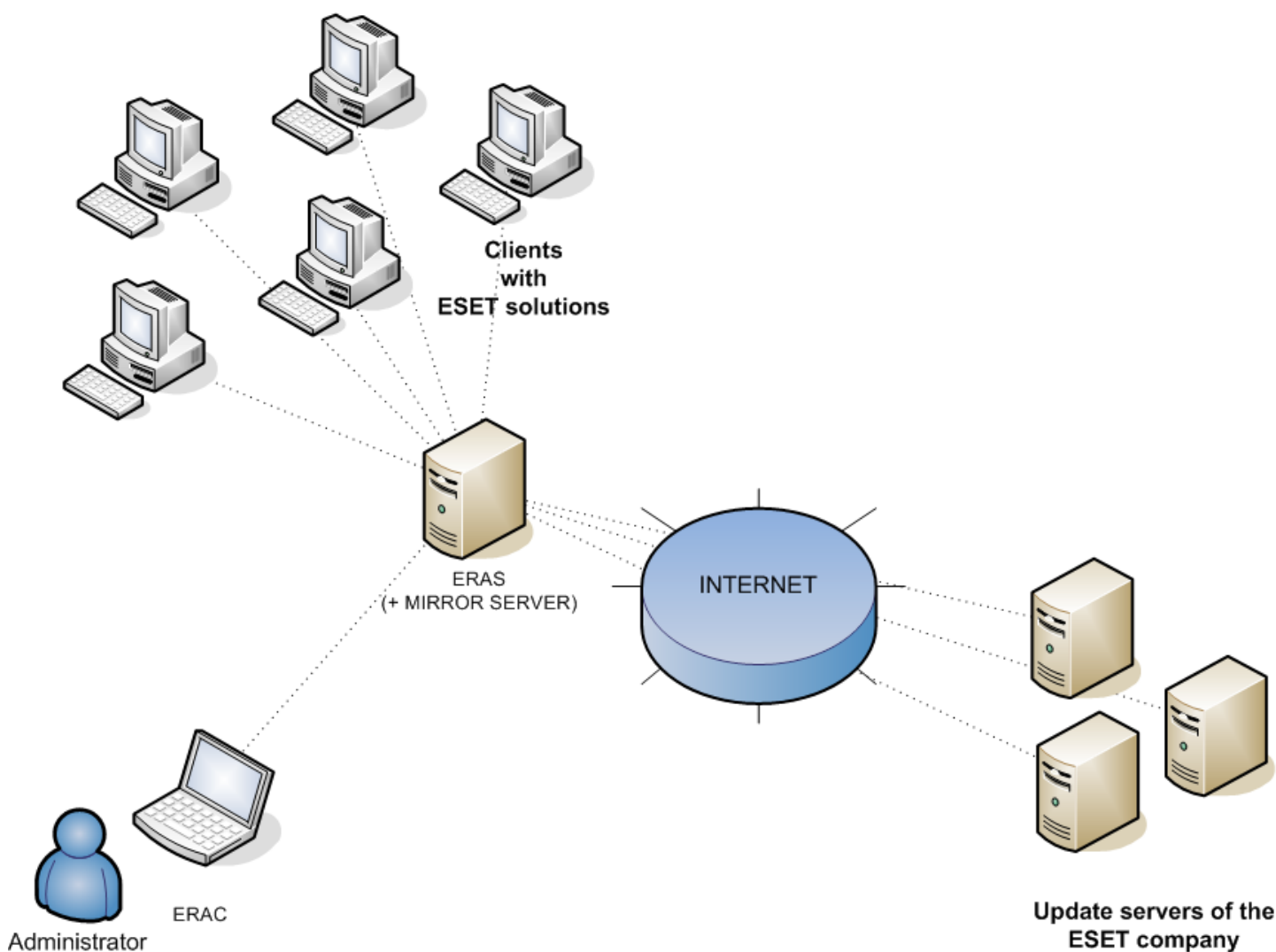


Figure 1 Simplified model of deployment: ESET for Windows clients, ESET Remote Administrator. ERAS and MIRROR SERVER can, but do not have to be installed on the same system.

2. ERA – client/server 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 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 (see section 2.1.6, “License keys”).

2.1 ERA Server (ERAS)

The server component of ERA runs as a service under the following Microsoft Windows® NT-based operating systems: NT4, 2000, XP, 2003 and Vista. The main task of this service is to collect information from clients and to send various requests to them. 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.

2.1.1 Requirements

ERAS requires a Microsoft Windows NT-based operating system (NT4, 2000, XP, 2003, Vista). The Microsoft Windows Server Edition is not necessary for ERAS to work. A computer with ERAS should be always online and accessible via computer network by:

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

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

Protocol	Port	Description
TCP	2222 (ERAS listening)	Communication between clients and ERAS
TCP	2223 (ERAS listening)	Communication between ERAC and ERAS
TCP	2221 (ERAS listening)	By default, this port offers update packages using the Mirror feature integrated in ERAS (HTTP communication)

If using all features of the program, the following network ports need to be open:

Protocol	Port	Description
TCP	2224 (ERAS listening)	Communication between the agent einstall.exe and ERAS during remote install
TCP	2846 (ERAS listening)	ERAS replication
TCP	139 (target port from the point of view of ERAS)	Copying of the agent einstall.exe from ERAS to a client using the share admin\$ during push install
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 minimum hardware configuration for the deployment of ERAS is also the minimum recommended configuration for the Microsoft Windows operating system used on the machine.

2.1.2 ERAS hierarchy at large networks

In larger networks multiple ERA Servers can be installed to perform future remote installs of client computers from servers which are more accessible. For this purpose, ERA Server offers “replication”, which allows stored information to be forwarded to a superior ERA Server (“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 ERA Server. 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). He will not need to use the VPN tunnel to access individual departments (the communications B, C, D and E) allowing him to bypass a slower communication channel through the use of ERA Server replication.

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

Another advantage to replication is that multiple users can log in with various permission levels. The administrator accessing the ERAS london1.company.com with the console (communication E) will be able to administer only clients connecting to london1.company.com, london.company.com, paris.company.com. If you connect to the central company.com (A), you will be able to control all clients located at company headquarters and departments/branches.

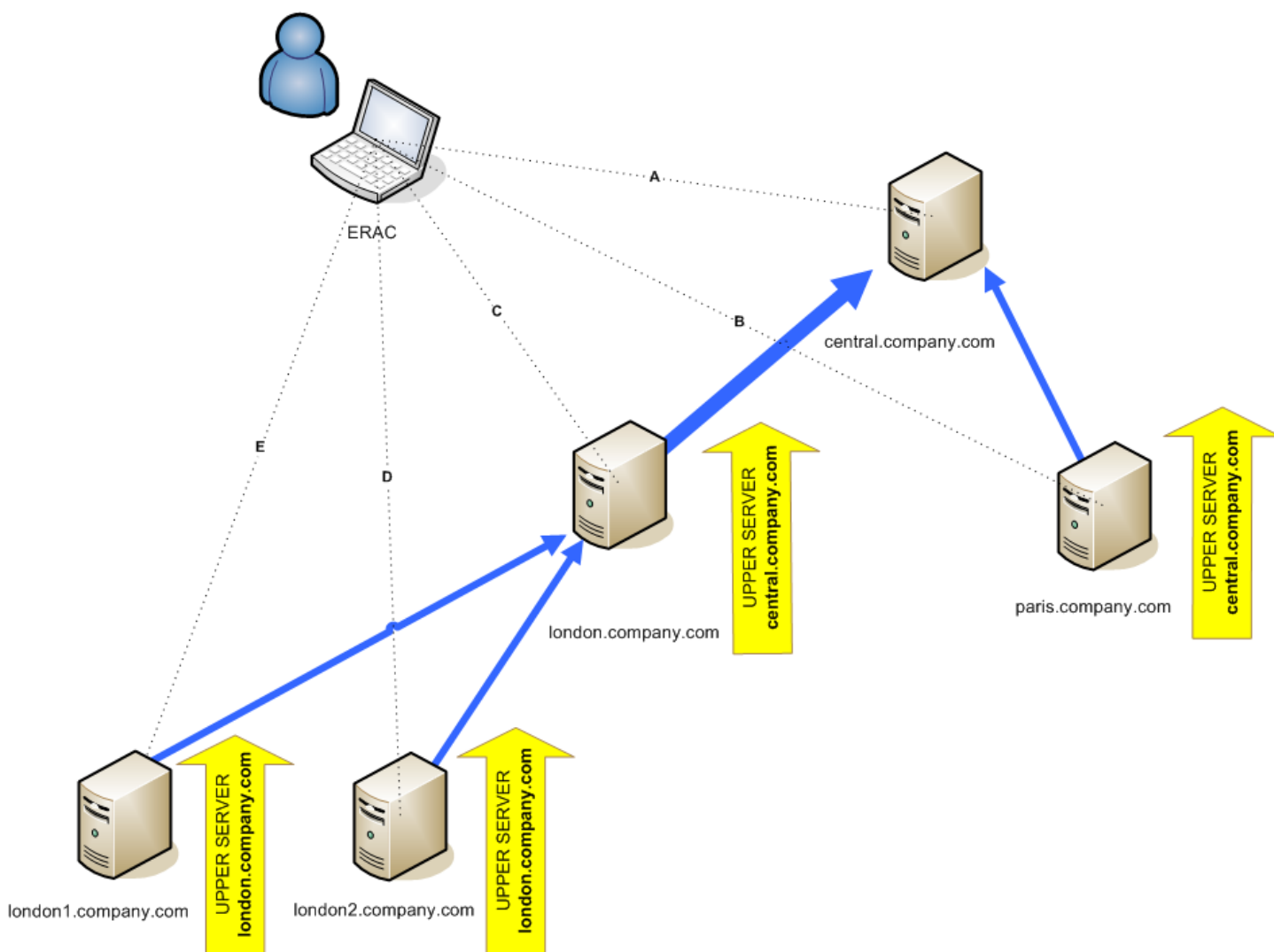


Figure 2 Replication in network consisted of headquarters and departments/subsidiaries.

2.1.3 Installation

The installation process is initiated by running the installation package. During this process, you will be prompted to upload a license key, which is a file with the `.lic` extension. If the Expert installation mode is selected, several other parameters can be defined. They can be modified later in ERAC, but in most cases there is no need to do so. The only exception is the server name. The server name should be the same as in the DNS, or the **Computer name** value of your operating system (**My Computer > Properties > Computer name** tab). The IP address of the computer can also be used. This is the most essential piece of information for performing remote installation. If the name is not specified during installation, the installer will automatically supply the value of the system variable `%COMPUTERNAME%`, which is sufficient in most cases.

By default, the ERAS program components are installed to the following folder:

```
%ProgramFiles%\Eset\Eset Remote Administrator\Server
```

and other data components such as logs, install packages, configuration, etc. are stored in:

```
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server
```

2.1.4 Logs

ERAS does not generate any output for a log file. This file is located in the folder:

```
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\logs
```

The log file titled "era.log" stores all events that take place during operation of ERAS, including error messages related to starting the ERAS service, such as a corrupt database error or license key error. The log file allows you to quickly determine the exact cause of ERAS failing to launch correctly.

NOTE: In the ERAS setup (accessible through ERAC) you can define several levels of logging including log rotation, to significantly reduce log file size and growth rate. Logging to the operating system application log can also be configured.

2.1.5 Configuration

To a certain extent, ERAS can be configured during installation (particularly in Advanced mode) or later using the ERA Console connected to the ERA Server. If need be, the `.xml` configuration files on the server can be modified. These files are located in the following directory:

```
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\configuration
```

NOTE: For security reasons, password setup is separated (into individual `.xml` files) from other setup options. Potential lost passwords (e.g. to access an ERA Server) can be resolved by deleting the `era_private.xml` file located in the Configuration folder

2.1.6 License keys

The license key is a file with the `.lic` extension, similar in structure to the `.xml` format, but protected by an electronic signature. This file is required to successfully configure ERAS. The file contains the following information:

- License owner
- Number of client machines (number of licenses)
- License expiry date

Here are four common problem scenarios related to license key files:

- **.lic file is not present**

ERAS will run in a trial mode – it will be possible to administer only two clients (workstations) for an unlimited time period.

- **.lic file is corrupt**

The ERA Server service will not launch at all. The event will be logged to the `era.log` file.

- **.lic file has expired**

If the expiry date defined in a `.lic` file is older than a current date, it is not possible to establish connection between ERAC and ERAS. ERAS will continue to accept information from clients, but will not be able to administer them.

- **The number of clients defined in a .lic file is exceeded**

This status will be displayed by an error message in ERAC. It will be not possible to administer the extra clients communicating with the ERA Server.

License keys should be stored in the folder:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\license`

During the installation of ERAS, the license key is automatically copied to the above-mentioned folder. If the license is updated or upgraded, the license key must be manually updated. The folder may contain several license files, but ERAS will always choose and work with the most suitable file with the .lic extension. Every time a new license is installed, the ERAS service must be stopped and restarted.

There are several ways to upload a license key to ERAS:

- Copy it to the above-mentioned directory where ERA Server is installed; then restart the ERAS service.
- Use the ESET Configuration Editor in ERAC and import license keys to ERA Server remotely
- Use the **Licenses** feature in ESET Smart Security/ESET NOD32 Antivirus to import license keys

2.1.7 Database & information storage

ERAS uses the MDAC (Microsoft Data Access Components) database component, while larger entries are saved to individual files in the Storage folder.

ERAS has tools built in to allow administrators to automatically perform database and stored information maintenance. This can be configured during the installation (expert level) or later through ERAC. Database maintenance leads to faster responses on database queries from ERAS and also saves hard disk space.

We recommend using the default configuration, which automatically deletes all entries older than six months. Decrease this value only in the event that the system is overwhelmed by entries from a large amount of clients.

The database is stored in the following directory:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\database`

Files related to records in the database are stored in:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\storage`

Information about client communication with ERAS is stored in individual files. These files reside in the **Storage** folder, and contain the following information:

- Client details (.xml configuration, Protection Status, Protection Features, and System Information),
- Log details (from Threat Log and Scan Log),
- Task details,
- Scheduled reports details (not directly related to the communication between a client and ERAS).

NOTE: *If the Storage folder is located on a computer with an NTFS file system, you can use the NTFS compression feature to significantly decrease its size while storing a large volume of information.*

2.2 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 console program, which is usually located in the following directory:

`%ProgramFiles%\Eset\Eset Remote Administrator\Console` (You can also open ERA Console by clicking **Start > All Programs > ESET > ESET Remote Administrator Console**)

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

ERAC outputs graphical logs in HTML that are saved locally. All other information is sent from ERAS on TCP port 2223.

3. Other ESET components in network environment

3.1 ESET client solutions

Client solutions are the security products which detect and block malicious code on workstations and servers. The primary client solutions are ESET NOD32 Antivirus 3.0 and ESET Smart Security.

Clients communicate through two main channels:

- ERA Server on TCP port 2222 in order to submit information such as logs, current configuration, threat alerts, etc. and to execute any tasks and queries from ERAS which are queued up for the client (modify configuration, perform a scan, etc.).
- The update server on a defined port using the HTTP or SMB protocols. Later in this manual we will discuss a method which allows an administrator to create a local update server or "Mirror" of the ESET update servers.

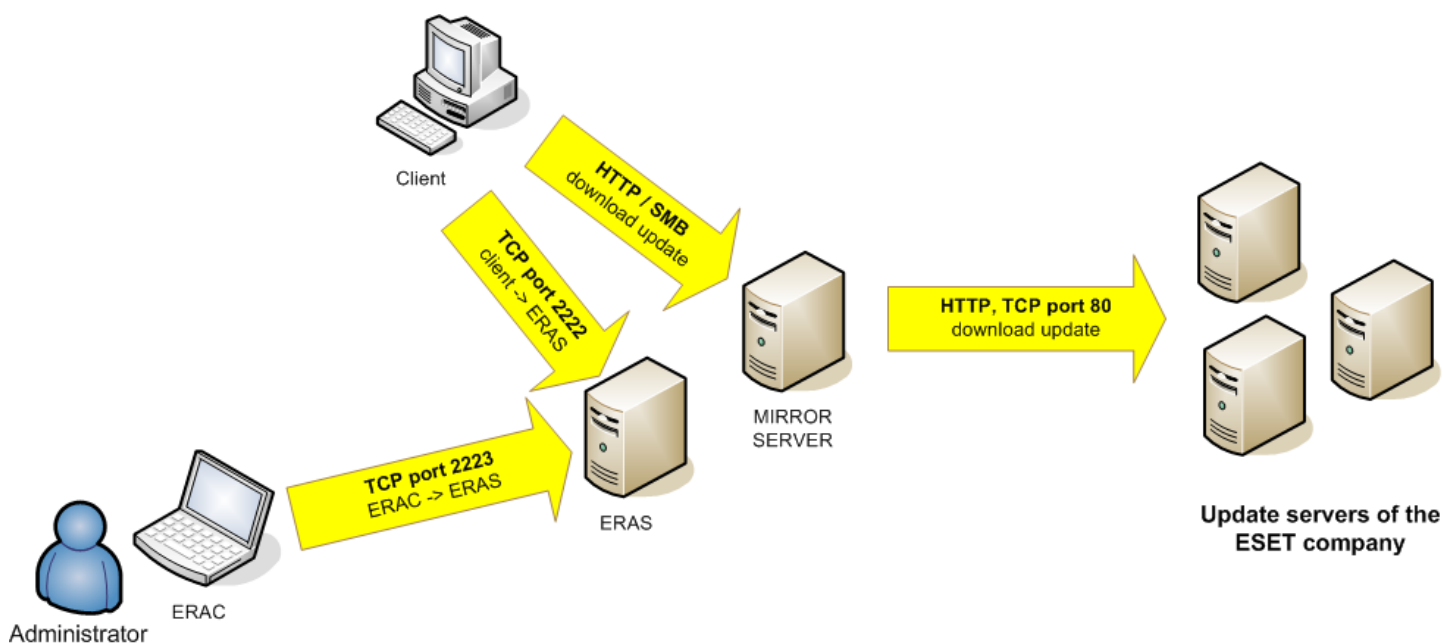


Figure 3 The most important communication channels connecting ERAS, ERAC and update servers. ERAS and MIRROR SERVER can be run on the same machine

3.2 ESET Configuration Editor

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

- Predefined configurations for installation packages
- Configurations sent as tasks to clients
- A general (.xml) configuration file

The Configuration Editor allows the administrator to remotely configure many of the parameters available in any ESET security solution, 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 Smart 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.

The Configuration Editor allows you to modify any .xml file. Please avoid modifying or rewriting the

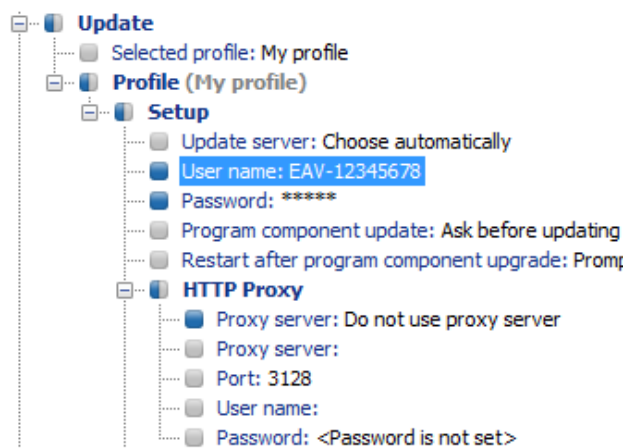
`cfgedit.xml` source file! For the Configuration Editor to work, the following files must be available: `eguiEpfw.dll`, `cfgeditLang.dll` and `eguiEpfwLang.dll`.

To access the Configuration Editor, start the ERA Console and click **Tools > ESET Configuration Editor**.

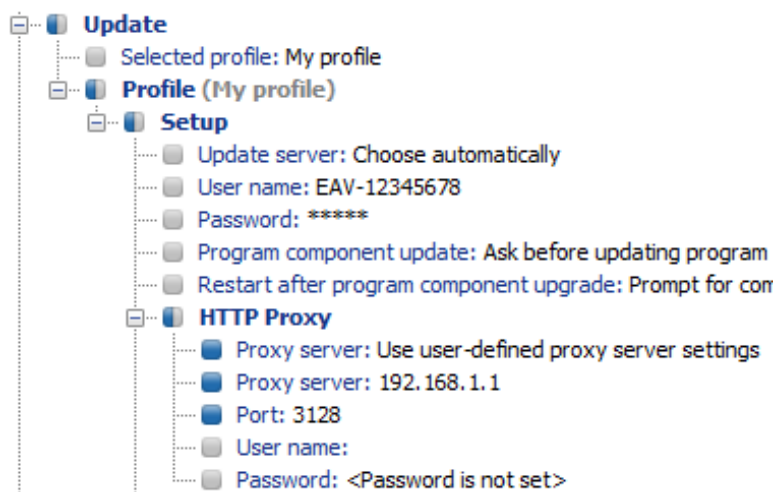
3.2.1 Configuration layering

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 those modifications which have been saved to the .xml output configuration file will be applied.

An example is shown below. In this configuration the user name and password are inserted and using a proxy server is prohibited.



The second configuration (shown below) sent to clients will ensure that previous modifications are preserved, including the user name EAV-12345678 and password, but will also allow the use of a proxy server, and defines its address and port.



3.2.2 Key configuration entries

In this section, we will explain several of the key configuration entries for ESET Smart Security available through the ESET Configuration Editor (Tools > ESET Configuration Editor). To change specific settings, select the option in the tree structure on the left and change the corresponding **Value** on the right.

- **Kernel > Setup > Remote administrator**

Here you can enable communication between client computers and the ERA Server (**Connect to Remote Administrator server**). Enter the name or IP address of the ERA Server (**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 the ERA Server. For more information, see the chapter about the configuration of ERAS – the Password for Clients option). If a password is used, the communication between clients and the ERAS will be encrypted.

- **Kernel > Setup > License keys**
Client computers require no license keys to be added or managed. License keys are used only for server products.
- **Kernel > Setup > ThreatSense.Net**
This branch defines the behavior of the ThreatSense.Net 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 ThreatSense.Net System is completely disabled. To submit files automatically with no need for user interaction, select **Submit without asking** and **Yes**, respectively. If a proxy server is used with the Internet connection, specify the connection parameters under **Kernel > Setup > Proxy server**.
- **Kernel > Setup > 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.
- **Kernel > Setup > Scheduler/Planner**
This key contains the Scheduler/Planner options, which allow the administrator to schedule regular antivirus scans, virus signature updates, etc.

NOTE: By default, all ESET security solutions contain several predefined tasks. In most cases, it should not be necessary to edit or add new ones.

- **Update**
This branch of the Configuration Editor allows you to define how virus signature and program component updates are handled on client workstations. In most cases it is necessary only to modify the predefined profile **My profile** and change the **Update server**, **User name** 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 **User name** 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 section 3.3, "LAN Update Server - Mirror".

NOTE: On mobile devices, 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 section 8.2 "Combined update for notebooks and mobile devices."

3.3 LAN Update Server -Mirror

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 instead connect to a local Mirror server on your network. The main advantages of this solution are to save Internet bandwidth and to minimize network traffic, since the mirror server connects to the Internet for updates, rather than hundreds of client machines. The only potential drawback is an outage of the Mirror server, which would prevent updates from being sent to client workstations (if it was the only server providing updates).

Warning! A Mirror server which performed a program component upgrade 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!** (see section 3.3.1 for more information on program component upgrades)

The Mirror feature is available in two locations:

- ESET Remote Administrator (Mirror physically running within ERAS, manageable from ERAC)
- ESET Smart Security Business Edition or ESET NOD32 Antivirus Business Edition (provided that the Business Edition has been activated by a license key)

It is left to the administrator to select 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 of them as central (at company headquarters) in cascade-style – similar to an ERAS configuration with multiple clients.

3.3.1 Operation of 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 user name (usually in the following form: EAV-XXXXXXX) and password.

The Mirror server which is a part of ESET Smart Security/ESET NOD32 Antivirus has an integrated HTTP server.

NOTE: *If you decide to use the integrated HTTP server (with no authentication), please ensure that it will not be accessible from outside of 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!*

Any other type of HTTP server can also be used. ESET also supports additional authentication methods (user name / password access – 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, a user name 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, we recommend that you create a unique user name (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.

NOTE: *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`

3.3.2 Types of updates

Aside from regular virus signature database updates, which can include ESET software kernel updates, program component upgrades can be downloaded on a far less frequent basis. Program upgrades usually add new features to ESET security solutions and require a reboot to finish installing. If there is a Mirror server installed in a network, program upgrades are downloaded from the Mirror server.

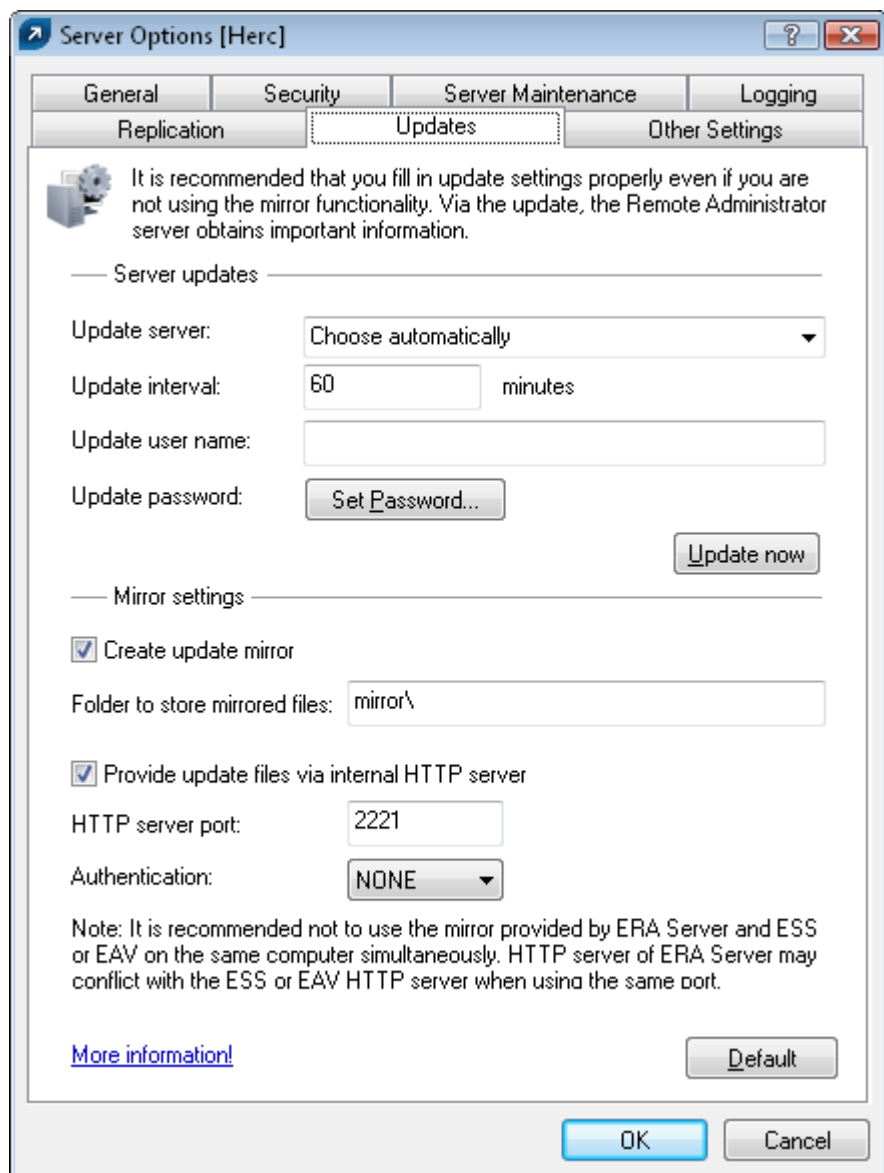
The Mirror server allows an administrator to disable automatic downloading of program upgrades from ESET's update servers (or from an upper Mirror server) and disable its distribution to clients. Distribution can later be triggered manually by the administrator (e.g. when he is sure there will be no conflict between the new version and other applications).

This feature is especially useful if the administrator wishes to download and use virus signature database updates even though there is also a new program version available to download. In this scenario, the new program version could be tested in a non-production environment before its implementation. 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 without too much delay, in order to gain access to new program features.

3.3.3 How to enable and configure Mirror

If the Mirror integrated directly into ESET Remote Administrator is used (a Business Edition component), connect to the ERAS using the ERA Console and follow these steps:

- From the ERA Console, click **Tools > Server Options...** and click the **Updates** tab.
- 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 interval (**Update interval**) for updates (we recommend sixty minutes).
- If you have selected **Choose Automatically** in the previous step, insert the user name (**Update user name**) and password (**Update password**) which was sent to you after purchase. If accessing an upper server, enter a valid domain user name and password to 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 option **Provide update files via internal HTTP server** is selected and is available on the HTTP port defined in **HTTP server port** (by default 2221).
- Set Authentication to **NONE**.
- Select the components to be downloaded. Components for all language versions to be used in the network should be selected.



The Mirror feature is also available directly from the program interface in ESET Smart Security Business Edition and ESET NOD32 Antivirus Business Edition. 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 Smart Security Business Edition or ESET NOD32 Antivirus Business Edition, follow these steps:

- Install ESET Smart Security Business Edition or ESET NOD32 Antivirus Business Edition

- From the Advanced Setup window (F5), click **Miscellaneous > License keys**. Click the **Add...** button, browse for the nod32.lic file and click **Open**. This will install the license and allow configuration of the Mirror feature.
- From the **Update** branch click the **Setup...** button and select the **Mirror** tab.
- Select the **Create update mirror** and **Provide update files via internal HTTP server** option.
- Enter the full directory path to the folder (Mirror folder) where update files are to be stored (do not reference a mapped network drive).
- The **User name** 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, as the authentication data will be entered at the client level.
- Click the **Advanced setup** button and set **Authentication** to **NONE**¹.
- select components to be downloaded (components for all language versions which will be used in the network should be selected).

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 ESET Remote Administrator, this option can be configured in ERAC through **Tools > Server Options... > Other Settings tab > Edit Advanced Settings... > ESET Remote Administrator > ERA Server > Setup > Mirror**. Enable all program language versions present in your network.

¹ For more information see section 2.1.5, "Configuration of ERA Server".

4. ESET Remote Administrator Console in detail

4.1 Connecting to ERAS

Most features in the ERA Console are available only after connecting to an ERA Server. Before the first connection, first define the server by name or IP address:

Open the ERA Console, click **File > Edit Connections...** and click the **Connection** tab.

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

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 is displayed.

Connections can be password protected. By default, there is no password to connect to an ERA Server, but we strongly recommend that one be established. To create a password to connect to an ERA Server:

Click **File > Change Password...** and then click the **Change...** button to the right of **Password for Console**.

When entering a password, there is the option to **Remember password**. Please consider the possible security risk of using this option. To delete all remembered passwords, click **File > Clear Cached Passwords...**

At the moment communication is established, the program's header will change to **Connected [server_name]**.

4.2 ERAC – main screen

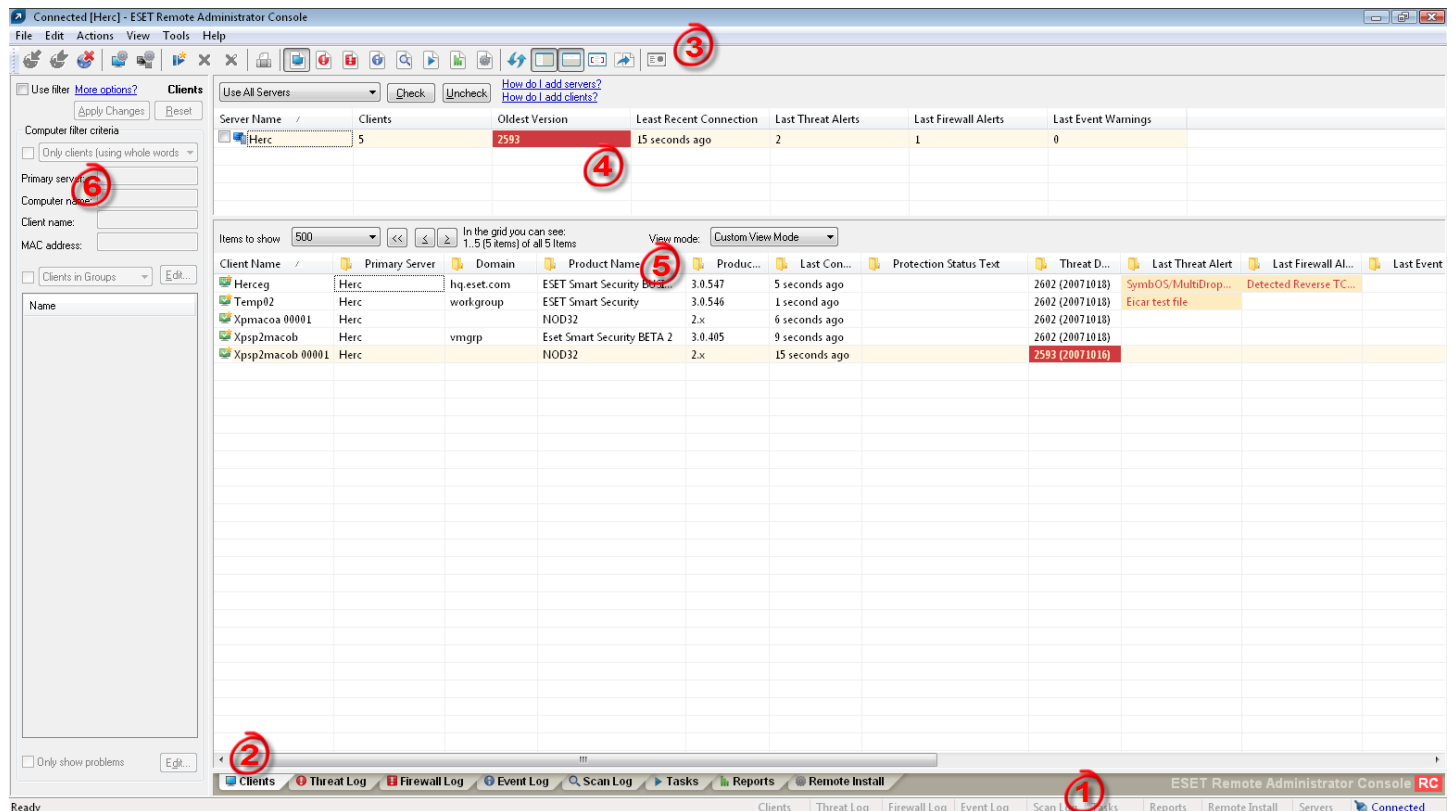


Figure 4 The main screen of ESET Remote Administrator Console

A current status of communication 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...**). The refresh progress can also be seen in the status bar.

NOTE: Press F5 to refresh displayed data.

Information is divided into several tabs (2) in order of importance. In most cases data can be (5) sorted in ascending or in descending order by clicking on an attribute, 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 a **View mode** to display attributes according to your need. For more information see section 4.3, "Information filtering".

The Server section (4) is important if you replicate ERA Servers. Here you can find summary information about the Console to which your 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. Server menu options:

- **Use All Servers**
Displays information from all ERA Servers
- **Use Only Checked Servers**
Displays information from selected ERA Servers
- **Exclude Checked Servers**
Excludes selected ERA Servers

Columns in Section 4:

- **Server Name**
Displays name of server
- **Clients**
Total number of clients connecting to the selected ERAS
- **Oldest Version**
The oldest version of virus signature database among the clients of the selected ERAS
- **Least Recent Connection**
States the longest inactivity period (interval from the last connection) among the clients of the given ERAS
- **Last Threat Alerts**
Total number of virus alerts (see the attribute **Last Threat Alert** in section 5 of Figure 4)
- **Last Firewall Alerts**
Total number of firewall alerts (see the attribute **Last Firewall Alert** in section 5 of Figure 4)
- **Last Event Warnings**
Total number of system events (see the attribute **Last Event Warning** in section 5 of Figure 4)

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 .

If replication is enabled, lower servers will automatically be displayed in the Server section (4). The most important features of ERAC are accessible from the menu or from the ERAC toolbar (3). The last section is **Computer filter criteria**(6) – see "Information filtering" in the next section.

4.3 Information filtering

ERAC offers several tools and features which provide user-friendly administration of clients and events.

4.3.1 Groups

Individual clients can be divided into groups by clicking **Edit > Groups...** in the ERA Console. Groups can later be used when applying filters or creating tasks, because those activities can be applied on whole groups of clients at the same time. Groups are independent for each ERAS and they are not replicated. The **Synchronize with Active Directory** feature allows the administrator to sort clients to groups, if the client name equals the object type "computer" at the side of Active Directory (AD) and belongs to groups in the AD.

4.3.2 Filter

Filter 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.

To activate filtering, select the **Use Filter** option in the upper left side of the ERA Console and click the **Apply Changes** button. Any future modification to the filter criteria will automatically update displayed data, unless configured otherwise in the **Tools > Console Options... > Other Settings tab**.

In the **Computer filter criteria** section you can filter ERA Servers/clients, using the following criteria:

- **Only clients (using whole word)**
Output includes only clients with names identical to the string entered

- **Only clients beginning like**
Output will list only 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 word), Exclude clients beginning like, Exclude clients like**
These options will yield opposite results to the previous three

The **Primary server**, **Computer name**, **Client name** and **MAC Address** fields accept whole strings. If any of these are populated, a database query will be run and results will be filtered based on the populated fields.

The next section allows filtering of clients by groups:

- **Clients in Groups**
Displays only clients belonging to the specified group(s)
- **Clients in other Groups or N/A**
Output will include only clients belonging to other groups, or clients which are not a member of any group. If a client belongs to both specified and non-specified groups, it will be displayed.
- **Clients in no Groups**
Displays only clients which are not a part of any group

Filtering options change slightly according to the currently active tab (Clients, Threat Log, etc.).

4.3.3 Context menu

Use the right mouse button to invoke the context menu and adjust output in columns.

- **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.
- **Inverse selection**
Perform inverted selection of entries
- **Hide selected**
Hides selected entries
- **Hide unselected**
Hides all unselected entries in the list

The last two 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 display only those 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 on 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 use the context menu and **Select by 'Charles'**. Last, right-click and select **Hide unselected** from the context menu. The CTRL key can now be released.

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.*

4.3.4 Views

In the **Clients** tab, the number of columns displayed can be adjusted by using the **View mode**: drop-down menu on the far right side of the Console. When the **Full View Mode** is active, all columns are displayed, while the **Minimal View Mode** shows only the most important columns. These modes are predefined and cannot be modified. To activate the Custom View, select **Custom View Mode**. The Custom View can be configured in **Tools > Console Options...** by clicking the **Columns – Show/Hide** tab.

4.4 Tabs in ERAC

4.4.1 General description of tabs and clients

Most of the information on 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*²

The behavior of ERAS related to certain network operations (such as renaming a PC) can be defined in ERAS Advanced Setup (For more detail, see the "Other Settings" section in Chapter 4). For example, if one of the computers in the network has been renamed, but its MAC address remained unchanged, you can avoid creating a new entry in the Clients tab.

Clients (workstations and servers with a security solution from ESET installed) that connect for the first time to ERAS are designated by a **Yes** value in the **New User** column and are marked by a small asterisk in the upper right corner of the client's icon. 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.



If a client has been configured and moved to a certain group, the **New** status can be disabled by right-clicking on the client and selecting **Reset "New" Flag**. The icon of the respective client will change to the one shown in the example below (and the attribute **New User** will change to **No**).



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

NOTE: Time values in ERAS can be displayed either in the relative mode ("2 days ago"), or in the absolute mode (20. 5. 2007).

In most cases, data in tabs can be sorted in ascending or descending order by clicking on an attribute. The drag-and-drop method can be used to reorganize the columns.

Clicking on certain values activates other tabs in order to display more detailed information. For example, if you click on 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 click on 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.

4.4.2 Replication & information in individual tabs

If an ERA Console is connected to an ERAS which is operating as an upper server, all information from lower servers will be displayed automatically, unless the lower server is not configured to allow this.

In such a scenario, the following information could 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**)

In dialog windows where such information should otherwise be present, the **Request** button is available. Clicking this button downloads missing information from a lower ERA Server. Since replication is always initiated by a lower ERA Server, the missing information should be delivered within the preset replication interval.

2 In older versions of ESET Remote Administrator, identification was based on the attributes *Computer Name* + *Primary Server*.

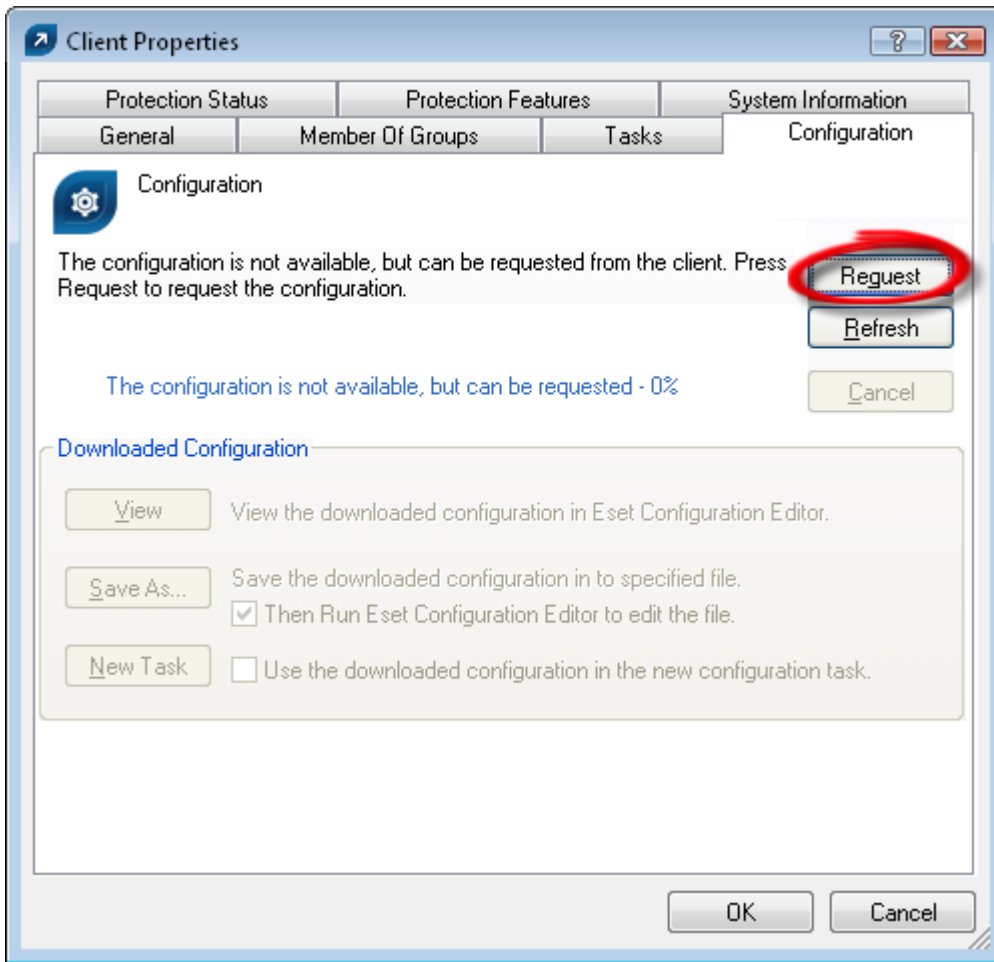


Figure 5 Click Request to retrieve missing information from inferior ERA Servers.

4.4.3 Clients tab

This tab displays general information about individual clients.

Attribute	Description
Client Name	Name identifying a client computer in ERA. New clients use the value "Computer Name". Client Name can be modified with no side effects.
Computer Name	Name of workstation / server (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of ERA Server with which a client is communicating
Domain	Domain / group name, to which a client belongs (these are not groups created in ERAS)
IP	IP address
Product Name	Name of product from ESET
Product Version	Version of the above mentioned product
Last Connected	Last connection of a client to its ERAS. All other data from a client have this timestamp, except for some data obtained by replication
Protection Status Text	Current status of the ESET security solution installed on a client
Threat DB Version	Version of virus signature database
Last Threat Alert	Last virus incident
Last Firewall Alert	Last event detected by the firewall in ESET Smart Security
Last Event Warning	Last error message

Last Files Scanned	Number of scanned files during the last On-demand scan
Last Files Infected	Number of infected files during the last On-demand scan
Last Files Cleaned	Number of cleaned (or deleted) files during the last On-demand scan
Last Scan Date	Time of the last On-demand scan
Restart Request	Is a restart required (e.g., after a program upgrade)
Restart Request Date	Time of the first request for a restart
Product Last Started	Shows when the client program was last launched
Product Install Date	Date of installation of the program
Mobile User	Clients with this attribute will perform the task "update now" each time they establish connection with ERAS (it is suitable for notebooks)
New User	See more in general description of clients
OS Name	Name of operating system
OS Platform	Operating system platform (Windows / Linux...)
HW Platform	32-bit / 64-bit
Configuration	Client also submits the .xml format of its current configuration. The attribute includes time of configuration (if there is no replication activated, it equals to the time when it had been modified for the last time)
Protection Status	General status statement. Similar in nature to the attribute Configuration
Protection Features	General status statement for program components. Similar to Configuration
System Information	Information about program component versions. Similar in nature to the attribute Configuration

NOTE: Some values are for informational purposes only and may not be current when the administrator views them at the Console. For example, at 7:00 A.M. there may have been an update error, but at 8:00 A.M. it was performed successfully. If the administrator knows this information is obsolete, he can right-click the value and select Clear "Last Threat Alert" Info, or Clear "Last Event" Info. Information about the last virus incident or last system event will be deleted. This applies to values in the columns Last Threat Alert and Last Event.

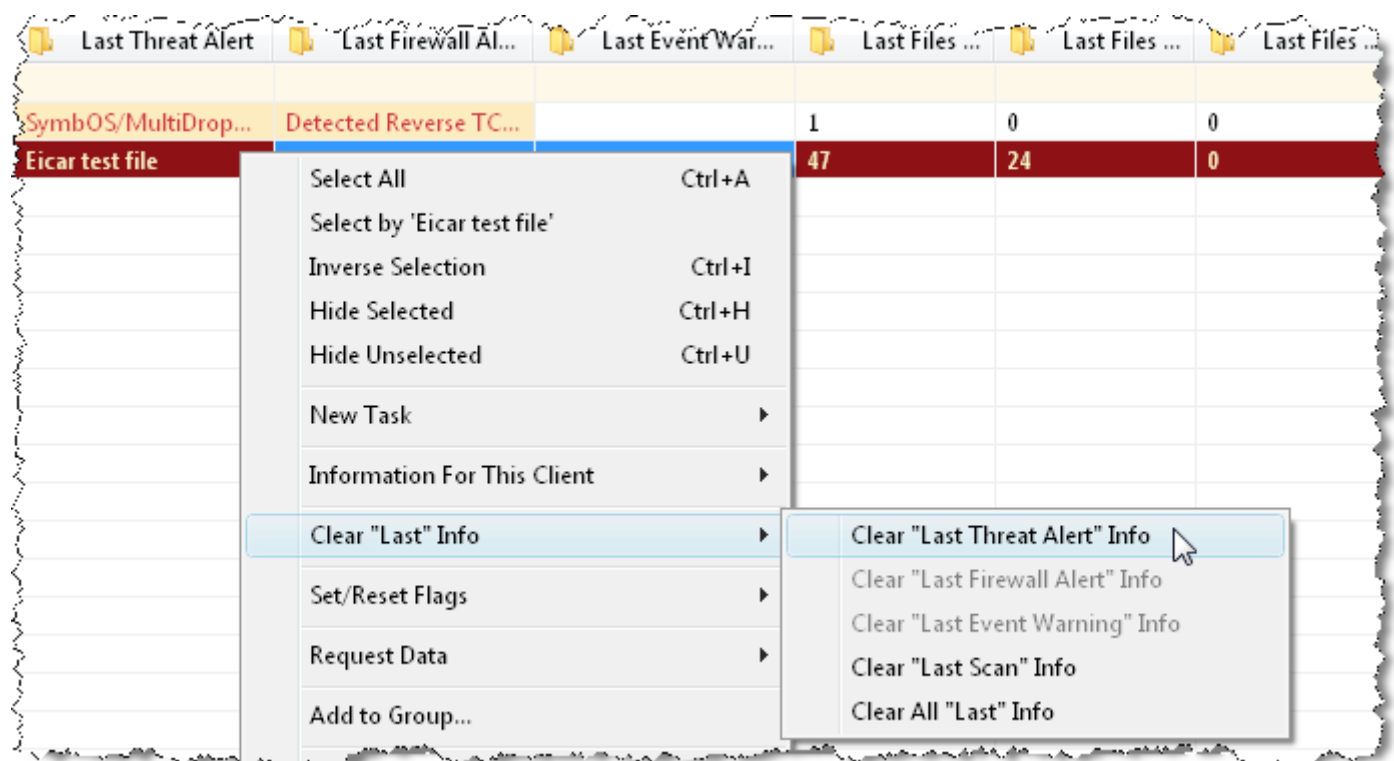


Figure 6 Obsolete events from the columns Last Threat Alert and Last Event Warning can be easily removed.

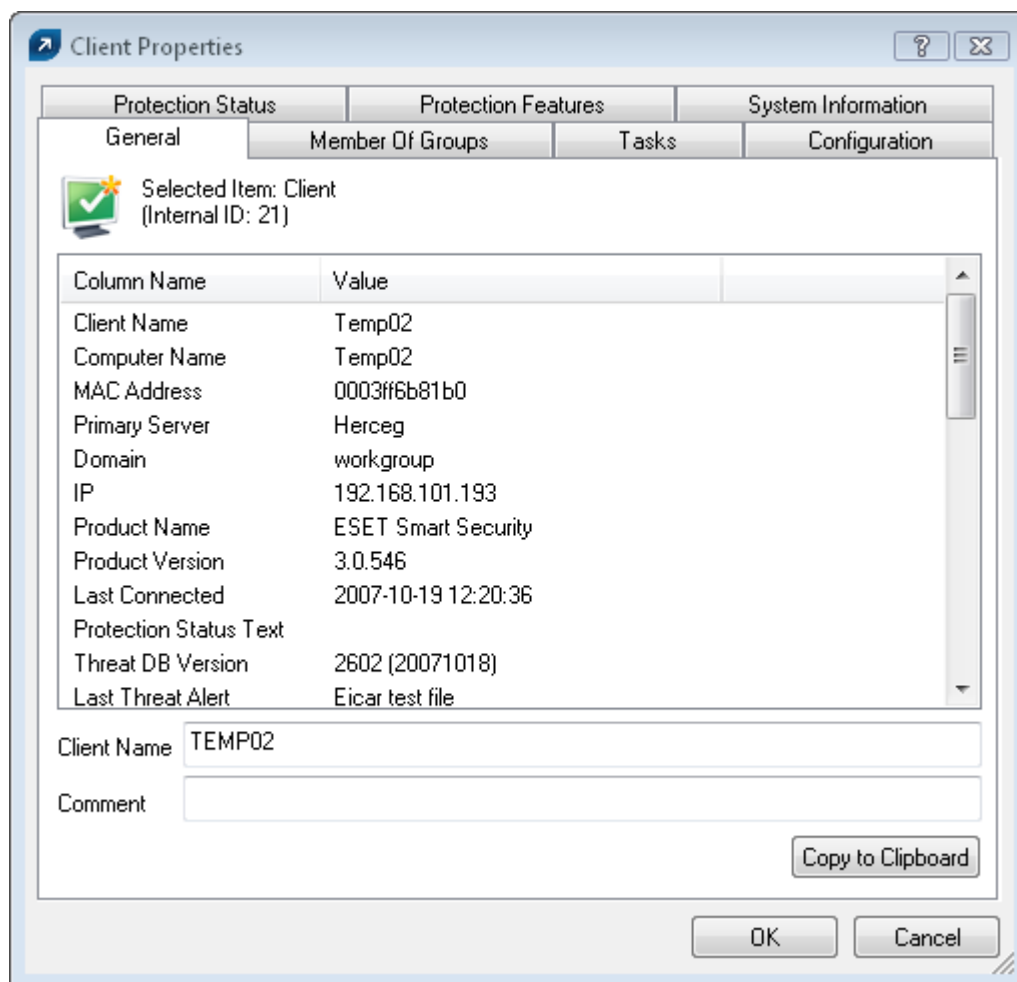


Figure 7 Detailed information about a client workstation.

The **Clients** tab offers several options after double-clicking on a client:

- **General** tab
Contains similar information to that displayed in the **Clients** tab. Here you can specify the **Client Name** - the name under which this client is visible in ERA, plus an optional comment.
- **Member Of Groups** tab
This tab lists all groups to which the client belongs. For more information please see "Information filtering" in section 4.3.
- **Tasks** tab
Tasks related to the given client. For more information see "Tasks" in Chapter 5.
- **Configuration** tab
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" in Chapter 5.
- the **Protection Status** tab
General status statement regarding all ESET programs. Some of the statements are interactive and it is possible to intervene immediately. This functionality is useful in that it prevents the need to manually define new tasks to solve the problem.
- the **Protection Features** tab
Component status for all ESET security features (Antispam, Personal firewall, etc.)
- the **System Information** tab
Detailed information about the installed program, its program component version, etc.

4.4.4 Threat Log tab

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

Attribute	Description
Threat Id	ID of the corresponding entry in the database tab
Client Name	Name of client reporting the threat alert
Computer Name	Computer name of the client reporting the threat alert
MAC Address	MAC address of the client reporting the threat alert
Primary Server	Name of the ERA Server with which a client is communicating
Date Received	Time at which the event was logged by ERAS
Date Occurred	Time when the incident took place on the client
Level	Alert level
Scanner	Name of security feature which detected the threat
Object	Object type
Name	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 logged in user when the incident occurred
Information	User-defined

4.4.5 Firewall Log tab

This tab displays information related to client firewall activity.

Attribute	Description
Firewall Id	ID of the corresponding entry in the database tab
Client Name	Name of client reporting the event
Computer Name	Computer name of the client reporting the event
MAC Address	MAC address of the client reporting the event
Primary Server	Name of the ERA Server with which the client is communicating
Date Received	Time at which the event was logged by ERAS
Date Occurred	Time when the incident took place on the client
Level	Alert level
Event	Description of the event
Source	Source IP address
Target	Target IP address
Protocol	Protocol concerned
Rule	Rule concerned
Application	Application concerned
User	Name of the logged in user when the incident occurred

4.4.6 Event Log tab

This tab shows a list of all system-related events.

Attribute	Description
Event Id	ID of the corresponding entry in the database tab
Client Name	Name of client reporting the event
Computer Name	Computer name of client reporting the event
MAC Address	MAC address of client reporting the event
Primary Server	Name of ERA Server with which a client is communicating
Date Received	Time event was logged by ERAS
Date Occurred	Time when the incident took place on client

Level	Event level
Plugin	Name of the program component reporting the event
Event	Description of the event
User	Name of the user logged in when the event occurred

4.4.7 The 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 tab
Client Name	Name of client computer where the scan was performed
Computer Name	Computer name of client computer where the scan was performed
MAC Address	MAC address of client computer where the scan was performed
Primary Server	Name of ERA Server with which the client is communicating
Date Received	Time at which the scan event was logged by ERAS
Date Occurred	Time when 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 files
Status	Status of the scan
User	Name of the logged in user when the scan took place
Type	Who started the task
Scanner	Type of scan performed
Details	Any detailed information

4.4.8 Tasks tab

The meaning of this tab is described in Chapter 5, "Tasks". The following attributes are available:

Attribute	Description
Task Id	ID of the corresponding entry in the database tab
State	Task status (Active = being applied, Finished = task was delivered to clients)
Type	Task type
Name	Task name
Description	Task description
Date Received	Time event was logged by ERAS
Comment	Optional description

4.4.9 Reports tab

The **Reports** tab is used to create statistical information – reports – in the form of graphs or charts. These can be saved and processed later in the Comma Separated Value form (or CSV) by using the ERA tools to provide graphs and graphical outputs. By default, ERA saves output in the HTML format (images are in PNG format).

ERA provides several predefined templates for reports. To select a report, use the **Report Type** drop-down menu in the middle of the window, below the **Generate Now** button.

- **Top Threats**
List of the most frequently detected threats
- **Top Clients with most Threats**
Lists the most “active” client workstations (in number of detected threats)
- **Threats Progress**
Progress of malware events (number)
- **Threats Comparative Progress**
Progress of malware events by selected threats (using filter) compared with the total number of malware
- **Threats By Scanner**
Number of threat alerts from the individual program modules
- **Threats By Object**
Number of threat alerts according to the way they attempted to infiltrate (emails, files, boot sectors)
- **Combined Top Clients / Top Threats**
Combination of the above mentioned types
- **Combined Top Threats / Threats Progress**
Combination of the above mentioned types
- **Combined Top Threats / Threats Comparative Progress**
Combination of the above mentioned types
- **Clients Report, Threats Report, Events Report, Scans Report, Tasks Report**
Typical reports that can be viewed in the Clients, Threat Log, Event Log, Scan Log or Tasks tab
- **Comprehensive Report**
Summary of:
 - **Combined Top Clients / Top Threats**
 - **Combined Top Threats / Threats Comparative Progress**
 - **Threats Progress**

In the **Filter** section you can use the **Target clients** or **Threat** drop-down menus to select which clients or viruses will be included in the report.

Other details can be configured by clicking the **Additional Settings...** button. 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 (show only clients with a “Protection State” problem), as well as choose which report format will be used (HTML, CSV).

Interval tab - This tab allows you to define an interval for which the report will be generated:

- **Current**
Only events which occurred in a chosen time period will be included in the report – e.g., 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 in 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 the option **Add also the current period** is selected, the report will include events from the last completed period up till the moment of creation.

Example:

We want to create a report including events from the last calendar week, i.e. from Sunday to next Saturday. We want this report to be generated on the next Wednesday (after Saturday).

In the **Interval** tab, select **Completed** and **1 Weeks**. In the **Scheduler** tab set **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 tab - This tab allows you to define and configure an automatic report in chosen time or intervals (Using the **Frequency** section).

Using the **Run at** spin box and the **Start** drop-down menu, enter the time and date when the report is to be generated. Click the **Select Target...** button to specify where the report is to be saved. Reports can be saved to the ERA Server (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 viewed by other employees.

To send generated reports via email, you need to enter SMTP server and sender address information as described in the Chapter 4.6, “Configuring ERA Server using the Console.”

To define a fixed date range for the report-generation process, use the options in the **Range** section. You can define

the number of generated reports (**End after**), or a date that the report-generation process is not to exceed (**End by**).

To save settings of defined reports to a template, click the **Save** or **Save as...** buttons. If you are creating a new template, click the **Save as...** button and give the template a name.

At the top of the Console window in the **Report templates** section, you can see names of templates that were already created. Next to the template names, there is information about time/intervals and when the reports are generated according to the preset templates. Click the **Generate Now** button (make sure the **Options** tab is selected) to generate a report at any moment regardless of the schedule.

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) to copy reports to other locations, add report templates to the Favorites List, etc.

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

4.4.10 Remote Install tab

This tab provides options for several remote installation methods of ESET Smart Security or ESET NOD32 Antivirus on clients. For detailed information, please see the "Remote Installation" section in Chapter 6, "Installation of ESET's client solutions."

4.5 ERA Console setup

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

4.5.1 Connection tab

This tab is related to communication between the ERA Console and ERA Server. For more details, see the beginning of Chapter 4, "ESET Remote Administrator Console in detail".

4.5.2 Columns – Show / Hide tab

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

4.5.3 Colors tab

Here you can define which colors will be associated with which events. 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**).

4.5.4 Paths tab

Here you can specify the directory to which the ERA Console will save reports downloaded from ERAS. By default, reports are saved to:

```
%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Console\reports
```

4.5.5 Date / Time tab

Appearance of the date / time columns:

- **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.

4.5.6 Other Settings tab

- **Auto Apply Changes**
If enabled, filters in individual tabs will generate new outputs upon each modification of filter settings. Otherwise, filtering will take place only after clicking the **Apply Changes** button.

- **Remote Administrator updates**
This section allows you to enable checking for new versions of ESET Remote Administrator. We recommend that you leave the default value of **Monthly**. If a new version is available, the ERA Console displays a notification at program startup.
- **Use automatic refresh**
If selected, data in individual tabs is automatically refreshed according to the designated interval.
- **Empty console recycle bins at application exit**
Select this option to automatically empty items from the internal recycle bin of the Console after exiting. You can also empty items manually by right-clicking the **Recycle Bin** icon in the **Reports** tab.
- **Show gridlines**
Select this option to separate individual cells in all tabs by gridlines.
- **Prefer showing Client as "Server/Name" instead of "Server/Computer/MAC"**
Affects the display mode for clients in some dialog windows (e.g., **New task**).
- **Use systray icon**
ERA Console will be represented by a Windows notification area icon.
- **Show on taskbar when minimized**
If the ERA Console window is minimized, it will be accessible from the Windows notification area.
- **Use highlighted systray icon when problematic clients found**
Use this option in conjunction with the **Edit** button to define events which will trigger a change in color to the ERAC icon in the notification area.

NOTE: *If the ERA Console on the administrator's PC is going to be connected at all times to an ERA Server, we recommend that you enable the **Show on taskbar** option when minimized and leave the Console minimized when inactive. If a problem occurs, the icon in the notification area will turn red – which is a signal for the administrator to intervene. We also recommend adjusting the option **Use highlighted systray icon when problematic clients found** in order to specify which events will trigger a color change of the ERAC icon.*

- **Show all groups in filter panes**
Changes the group filtration
- **Tutorial messages**
Disables (**Disable All**) or enables (**Enable All**) all informative messages
- **Warn if the server license is about to expire in X days**
If enabled, the program will display a notification X days before the license date
- **Warn if there is only X% free clients left in the server license**
If enabled, the Console will display a notification if there is less than X client slots free (each license is defined by the number of administered clients).

4.6 Configuring ERA Server using the Console

The ERA Server can be easily configured directly from ERA Console. From the Console menu, click **Tools > Server Options...**

4.6.1 General tab

The **General** tab stores general information about ERAS, license key information and statistical information about the operation of ERAS.

Click **Renew License...** to remotely install a license key to ERAS and avoid potential expiration of the license. License keys are described in detail in section 7.1.2, "Installation of ERA Server."

4.6.2 Security tab

ESET security solutions in version 3.x (ESET Smart Security, etc.) offer password protection for communication between the client and ERAS (communication at the TCP protocol, port 2222), as this communication allows for decrypted communication.

The older versions (2.x) do not have this functionality. To provide backward compatibility for older versions, the **Enable unauthenticated access for Clients** mode must be activated.

The **Security** tab contains options to adjust simultaneous usage of the program generation 2.x and 3.x.

- **Password for Console**
Enables specifying a password to protect against unauthorized changes using the ERA Console
- **Password for Clients (ESET Security Products)**
Sets 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 password for the installer agent to access the ERAS. Relevant for remote installations
- **Enable unauthenticated access for Clients (ESET Security Products)**
Enables access to ERAS for those clients which do not have a valid password specified (if current password is different from **Password for Clients**).
- **Enable unauthenticated access for Replication**
Enables access to ERAS for clients of lower ERA Servers which do not have a valid password for replication specified.
- **Enable unauthenticated access for ESET Remote Installer (Agent)**
Enables access to ERAS for those installer agents, which do not have a valid password for replication specified.

NOTE: *If authentication is enabled both in ERAS and on all [generation 3.x] clients, the option **Enable unauthenticated access for Clients** can be disabled.*

4.6.3 Server Maintenance tab

If correctly configured in the **Server Maintenance** tab, the ERAS database will be automatically maintained and optimized, with no need for further configuration. By default, entries and logs older than six months are deleted, and the **Compact & repair** task is performed every fifteen days.

For more detailed configuration, the **Server Maintenance** tab offers the following options:

- **Only keep the latest X threats for each client**
Keeps only the specified number of virus incidents for each client
- **Only keep the latest X firewall logs for each client**
Keeps only the specified number of firewall logs for each client
- **Only keep the latest X events for each client**
Keeps only the specified number of system events for each client
- **Only keep the latest X scan logs for each client**
Keeps only the specified number of scanner logs for each client
- **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 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 scan logs older than X months (days)**
Deletes all scanner logs older than the specified number of months (or days)

4.6.4 Logging tab

During operation, ERAS creates a log (**Log filename**) about its activity which is configurable (**Log verbosity**). If the **Log to text file** option 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**).

The **Log to OS application log** option allows information to be copied to the system event viewer log (accessible via Windows **Control Panel > Administrative Tools > Event viewer**).

The **Debug Log** option should be disabled under normal circumstances.

By default, the text file output is saved to the following location:

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

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's Customer Care specialists.*

4.6.5 Replication tab

The concept of "Replication" has been already mentioned in the section 2.1.2, "ERAS hierarchy at large networks." Replication is used primarily in large networks where multiple ERA Servers are installed throughout an organization, in various branches / departments.

The options in the **Replication** tab are divided into two sections:

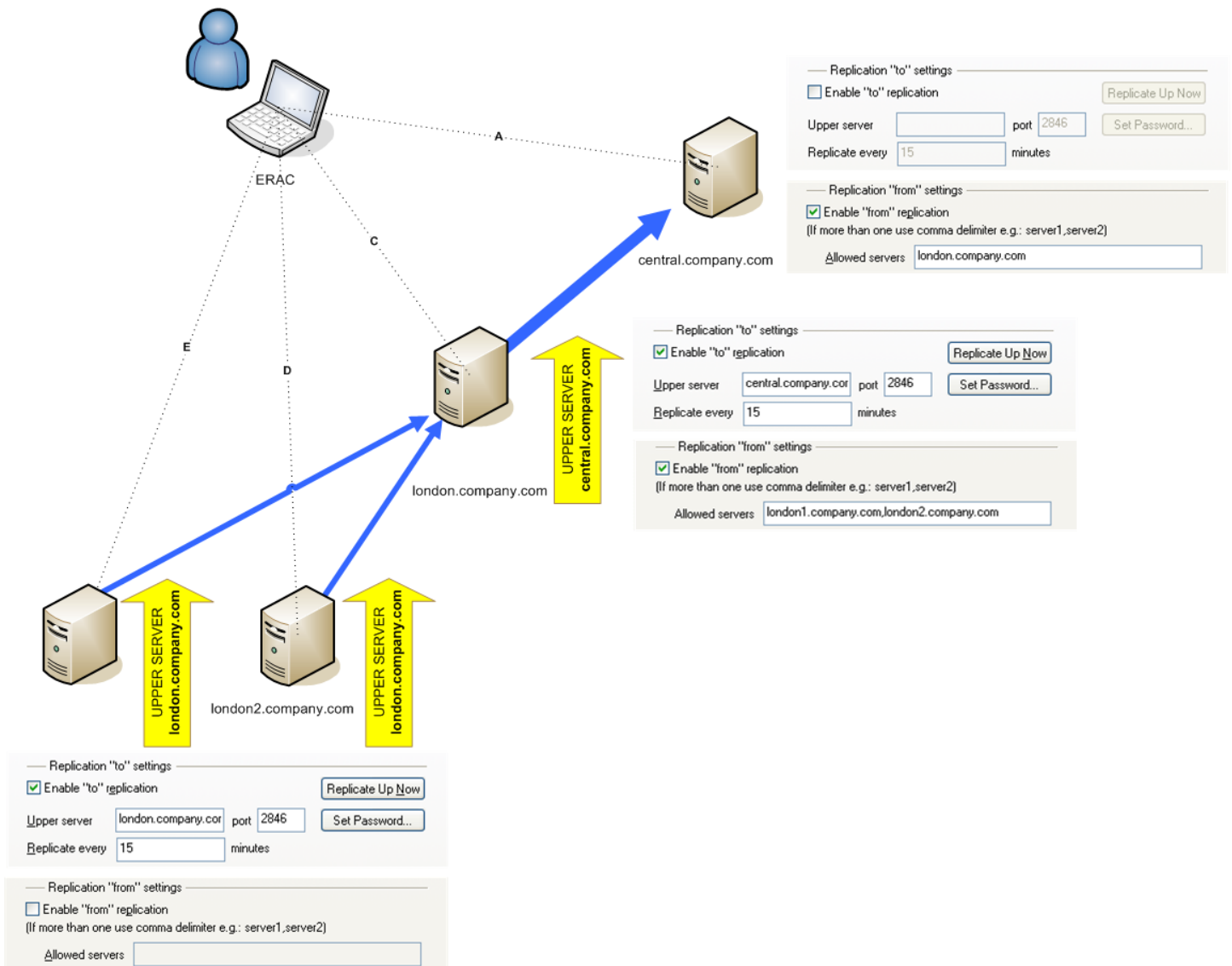
- Replication "to" settings
- Replication "from" settings

The **Replication "to" settings** section is used to configure lower ERA Servers. The option **Enable "to" replication** must be enabled and the IP address or the name of the master ERA Server (**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 option **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 described by the figure below. The beige computers represent individual ERA Servers. Each ERA Server 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.



Other options which influence the replication behavior of servers:

- **Replicate threat log, Replicate firewall log, Replicate event log, Replicate scan log**
If these options are selected, all information displayed on the **Clients, Threat Log, Firewall Log, Event Log, Scan 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.
- **Automatically replicate threat log details, Automatically replicate scan log details, Automatically replicate client details**
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: You may wonder why some logs are replicated automatically and detailed logs and client configuration logs are

replicated only on demand. The reason is that 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.

4.6.6 Updates

This tab allows you to configure the settings of the Mirror feature which are integrated into ESET Remote Administrator (ERAS). It is an alternative to the same feature which is available in the client solutions ESET Smart Security Business Edition and ESET NOD32 Antivirus Business Edition.

- **Update server**
UNC path or URL address of the update server. In most cases it is not necessary to modify the default value **Choose Automatically**, which enables updates to be automatically downloaded from ESET's servers.
- **Update interval**
Defines the amount of time between updates (the recommended value is 60 minutes)
- **Update user name**
Authentication data which grants access to update servers
- **Update password**
Authentication data which grants access to update servers
- **Update now**
Click this button to update immediately
- **Create update mirror**
If enabled, the program will allow the downloading of update files for other clients in the network to the folder defined in **Folder to store mirrored files**. If the **Provide update files via internal HTTP server** option is activated, update files will be available via the internal server (HTTP) at the specified port (**HTTP server port** –default is 2221).
- **Authentication**
Allows the administrator to set the authentication method for clients connecting to ERA Server. Select **NONE** to allow access to the HTTP server for all clients. Select **Basic** to use the basic base64 encryption. The **NTLM** method is the most complex authentication method available. It verifies the user account which is specified at the client's side in the form of user name and password, granting access to the update server.

In order for the Mirror feature to function properly, it is necessary to specify (in the Advanced Setup window) which components will be downloaded from the update servers, including language versions. Press F5 from the main program window of ESET Smart Security or ESET NOD32 Antivirus and then click the **Update** branch in the Advanced Setup tree. Click the **Setup...** button and then click the **Mirror** tab. All versions/components which will be used within the network should be selected.

4.6.7 Other Settings tab


- **SMTP settings (Server, Sender address, User name, Password)**
Some features in ESET Remote Administrator require SMTP server settings to be defined. These features include remote installation via email or generating reports to be sent to designated email addresses.
- **Allow new clients**
If disabled, no new clients will be added in the **Clients** tab – even if new clients communicate with ERA Servers, they will not be visible in the **Clients** tab.
- **Automatically reset "New" flag by new clients**
If enabled, the **New** flag is removed from clients connecting to ERAS for the first time. For more information please see section 4.4.3 "The Clients tab."
- **Ports (Console, Client, Replication port of this server, ESET Remote Installer)**
Defines ports on which ERAS will listen and wait for communication established by:
 - **Console** (by default TCP 2223)
 - **Client** (by default TCP 2222)
 - replication process (**Replication port**, by default TCP 2846)
 - remote install agent (**ESET Remote Installer**, by default TCP 2224)
- **Enable ThreatSense.Net data forwarding to ESET servers**
If enabled, ERAS will forward suspicious files and statistical information from clients to ESET's servers. In some cases it is not possible for client workstations to submit this information directly.
- **Edit Advanced Settings...**
This buttons opens the ESET Configuration Editor, where ERAS can be configured in detail.

5. Tasks

ESET Remote Administrator allows you to remotely perform tasks on client workstations. These tasks are performed at the moment the client establishes a connection to the ERA Server (on the TCP 2222), which is every five minutes.

Three types of tasks are available:

- **Configuration** – Modifies configuration of clients
- **On-Demand Scan** – Performs an On-demand scan
- **Update Now** – Forces update task

To open the task wizard from the ERA Console, press CTRL+N, click **File > New Task...** or click the icon  on the ERAC toolbar. The task wizard can also be opened by right-clicking a selected client (this option skips some dialog windows – for a complete configuration, please use either of the first two methods to open the wizard).

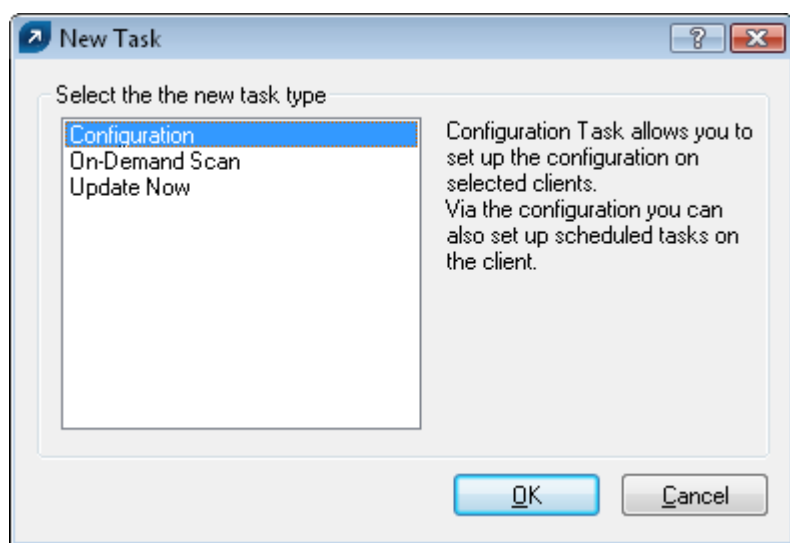


Figure 8 ERA offers three types of tasks

5.1 Configuration Task

To launch this type of task, click the **Create...** button to create a new task (.xml file). To select a previously existing .xml configuration file to be applied on remote clients, click **Select...**

NOTE: The .xml configuration files are mutually compatible regardless of their origin. This means that you can use an .xml configuration file which is assigned to an install package, downloaded from a client computer, or exported locally (e.g., from ESET Smart Security).

Modifications to configuration files are performed in the ESET Configuration Editor, described previously. Please take note of the icons associated with each setting – they will turn blue if changed. To view a selected configuration, click **View**. To modify a selected configuration, click **Edit**.

Click **Create from Template...** to open an existing .xml configuration file and use it as a starting point for a completely new configuration. After modifications, the template file remains unchanged.

Click **Next** and select all clients (individually, by groups, or by servers) which the .xml configuration file is to be applied to, by dragging and dropping them into the **Selected items** column. To move clients currently displayed in the **Clients** pane to the **Selected items** column, click **Add Special...**, select the option **Add clients loaded in the Clients pane** and then click the **Add** button. Of those clients which have been added from the Clients pane, you can further specify particular clients by selecting them from the **Servers** column and checking the **Only selected** option.

Click **Next**. The final step is to create a **Name** and **Description** for the new task. In the same dialog window, you can designate that the task be delayed (the **Apply task after** option), or automatically deleted, after it has been successfully completed on client computers. To automatically delete successfully completed tasks from the **Tasks** tab, select the **Delete tasks automatically by cleanup if successfully completed** option.

5.2 On-Demand Scan task

To create an On-demand scan task, first specify which client computers will apply the task (From a technical perspective, there are minor differences in the scan task settings between generation 2.x and 3.x).

NOTE: *If the administrator enables **On-demand Scan task for Windows NOD32** and also **On-demand Scan task for Windows ESET Security Product**, the same task can be used for both older and newer versions of the program. Select the option **Exclude this section from On-Demand Scan** to disable dual compatibility.*

To run an On-demand task on a client with ESET NOD32 version 2.x, please select **On-demand Scan task for Windows NOD32 version 2** and proceed as follows:

- Select the profile to be applied for the scan on the client (**Profile name**) – you can manually define a name not present in the list.
- Select which drives you wish to include in the scan (**Drives to scan**).
- If need be, add a new profile or modify (**Edit** button) the existing configuration of the profile from the first step.
- Select **Next** to proceed and select the clients to which the task will be applied.
- Click **Finish**.

NOTE: *On-demand scanning on clients will apply the configuration of a chosen profile + configuration of the attached .xml configuration (**Edit** button). The scanning profile is modified only temporarily while the task is performed.*

The **Scan without cleaning** option refers to the options **Scan only** and **Scan and clean** in the NOD32 module in ESET NOD32 Antivirus 2.x. The difference between these options is as follows:

- **Scan without cleaning** enabled: no action is taken with infected items if detected; scan creates a log.
- **Scan without cleaning** disabled: action taken corresponds to configuration defined for cleanable and uncleanable threats.

If there are generation 3.x solutions present on client computers (ESET Smart Security or ESET NOD32 Antivirus), then select **On-demand Scan task for Windows ESET Security Product** and follow these steps:

- Select the profile to be applied for the scan on the client (**Profile name**) – you can manually define a name not present in the list.
- Select which drives you wish to include in the scan (**Drives to scan**), or specify your own targets (**Add path**).
- Select **Next** to proceed and select the clients to which the task will be applied.
- Click **Finish**

5.3 Update Now task

To run an update task, first specify which client computers will apply the task (From a technical perspective, there are minor differences in the scan task settings between generation 2.x and 3.x).

NOTE: *If the administrator enables **On-demand Scan task for Windows NOD32** and also **On-demand Scan task for Windows ESET Security Product**, the same task can be used for both older and newer versions of the program. Select the option **Exclude this section from On-Demand Scan** to disable dual compatibility.*

The remaining steps are essentially the same for both program versions:

- Select the profile to be applied for the scan on the client (**Profile name**) – you can manually define a name not present in the list. Usually there is no need to define any profile (leave the **Specify profile name** option disabled).
- Select **Next** to proceed and select the clients to which the task will be applied.
- Click **Finish**

NOTE: *The client solutions (ESET NOD32 Antivirus, ESET Smart Security...) contain a default automatic regular update task. The **Update Now** task is therefore only a complementary and one-shot feature.*

6. Installation of ESET's client solutions

This chapter is dedicated to the installation (both direct and remote) of ESET's client solutions for Microsoft Windows operating systems.

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

6.1 Command line parameters for direct installation of client solutions

There are several parameters which can affect the installation process. They can be used either during direct installation with the administrator present at the workstation, or for remote installation. For remote installations, parameters are selected during the process of configuring installation packages – selected parameters are then applied automatically on target clients.

Additional parameters for ESET Smart Security and ESET NOD32 Antivirus can be typed after the name of the .msi installation package (e.g. **ea_nt64_ENU.msi /qn**):

- **/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
- **REBOOT="ReallySuppress"**
Suppresses restart after installation of the program
- **REBOOT="Force"**
Automatically reboots after installation
- **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 client solutions. The parameter is not required for remote installation. Installation packages contain their own .xml configuration which is applied automatically.

Parameters for ESET NOD32 Antivirus version 2.x should be typed after the file setup.exe, which can be extracted along with other files from the installation package (e.g. **setup.exe /silentmode**):

- **/SILENTMODE**
Quiet installation mode – no dialog windows are displayed
- **/FORCEOLD**
Will reinstall over a newer version
- **/CFG=" path_to_xml_file"**
During installation, parameters defined in the specified .xml files are applied to ESET client solutions. This parameter is not required for remote installation. Installation packages contain their own .xml configuration which is applied automatically.
- **/REBOOT**
Automatically reboots after the installation
- **/SHOWRESTART**
After the installation, a dialog window prompting the user to confirm rebooting is displayed
- **/INSTMFC**
Installs required MFC libraries for the Microsoft Windows 9x operating system. This parameter can be used always, even if the MFC libraries are available.

6.2 Installation methods

6.2.1 Direct installation with predefined XML configuration

With a direct installation, the administrator is present at the computer where the ESET client solution is to be installed. This method requires no further preparation and is suitable for small computer networks, or in scenarios where ESET Remote Administrator is not used.

This task can be greatly simplified with the help of a predefined .xml configuration. No further modification, such as defining update server (user name 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 3.x and 2.x of ESET client solutions:

- Version 3.x: Download the installation file (e.g., `ess_nt32_enu.msi`) from ESET's web site. Insert the .xml configuration file (`cfg.xml`) to the directory where the install file is located. If you run the installer, it 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).
- Version 2.x: Download the installation file (e.g., `ndntenst.exe`) from ESET's web site. Extract the downloaded file to a folder. The folder will contain installation files, including `setup.exe`. Copy the `nod32.xml` configuration file into the folder. Run the `setup.exe` file and the configuration within `nod32.xml` will be automatically applied. If the .xml configuration file has a different name, or it is located somewhere else, the parameter **/cfg**="*path_to_xml_file*" can be used. (e.g. `setup.exe /cfg=""\server\xml\settings.xml"` to apply the configuration stored on a network drive).

NOTE: Other parameters mentioned in the previous chapter can be used, too.

6.2.2 Remote installation in general

ESET Remote Administrator offers several methods of remote installation, listed directly below. The methods differ with respect to how installation packages are delivered to target workstations.

- Remote push installation
- Logon script remote installation
- Email remote installation

Remote installation does not necessarily have to be performed using the ERA tools – other methods are available (central distribution of MSI, LANDesk, etc.). In the end, the most important aspect is to deliver the installation file (or the agent) to clients and to ensure that it is launched under an Administrator account. For this purpose, the direct installation described in the previous section can also be used.

Remote installation by means of ESET Remote Administrator consists of these steps:

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

The first step is initiated through the ERA Console, but the install package itself is located in the ERA Server, in the following directory:

`%ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\packages`

To launch installation packages through the ERA Console, click the **Remote Install** tab and click the **Packages...** button.

Each installation package is defined by a **Name** (See (1) in Figure 9 above). The other 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. Each package contains:

- Installation files (2) of ESET's client solution
- .xml configuration file (3)
- Command line parameters(4)

The **Type** drop-down menu in section 1 extends the possibilities of ERA. In addition to remote installation, ESET client solutions can be uninstalled remotely using the **Uninstall ESET Security Products and NOD32 version 2** option. Remote installation of an external application can also be performed, by selecting **Custom package**.

NOTE: For technical reasons, the installation of older ESET solutions (version 2.x) is a separate function from the installation of generation 3.x solutions. For the same reason packages are stored in two separate folders on ERAS.

NOTE: The **Custom package** option offers a variety of methods, including the uninstallation of security solutions from other vendors (if a suitable batch command is used).

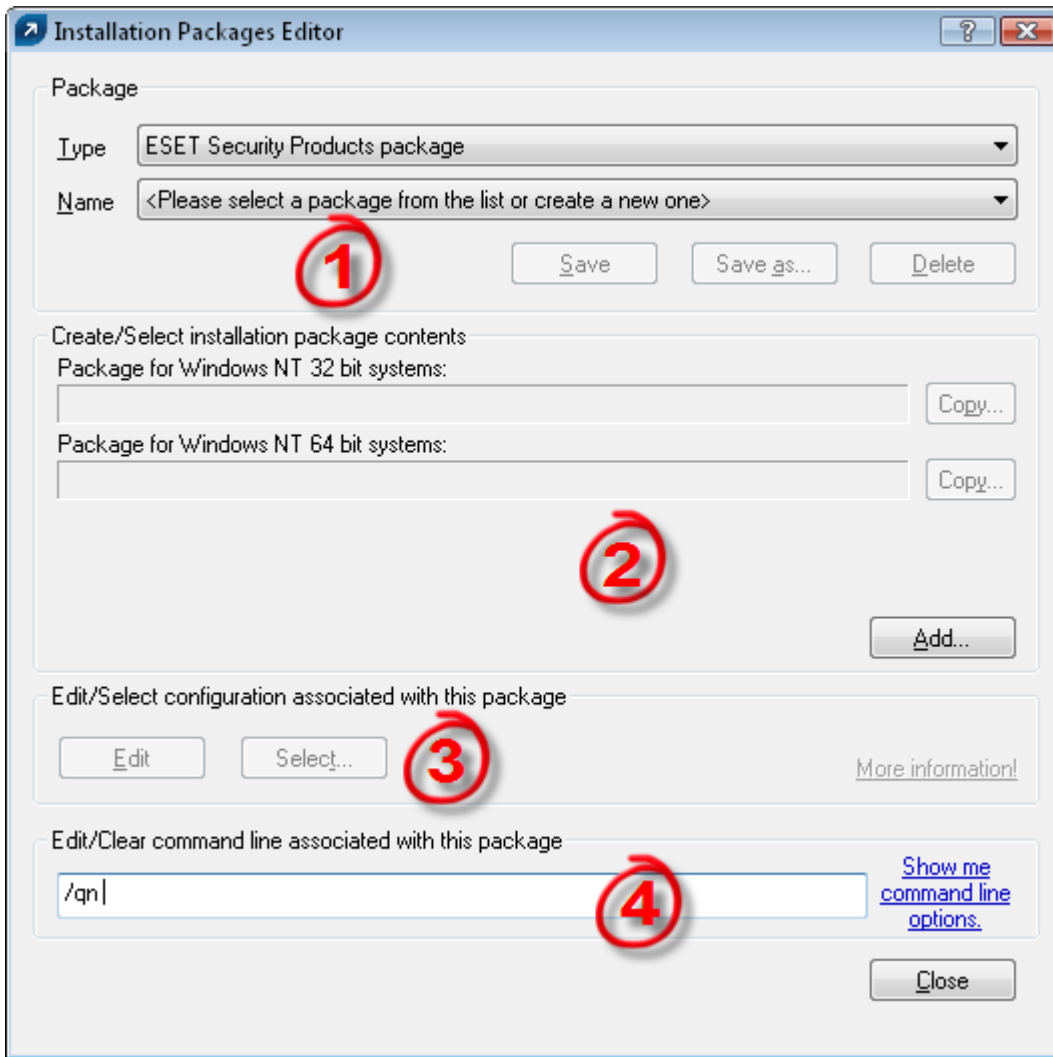


Figure 9 Dialog window of the installation packages Editor

Each package is automatically assigned an ESET Remote Installer agent, which allows for seamless installation and communication between target workstations and ERAS. The ESET Remote Installer agent is named `installer.exe` and contains the ERA Server name, and the name and type of package to which it belongs. The following chapters provide a detailed description of the agent.

6.2.3 Remote push install

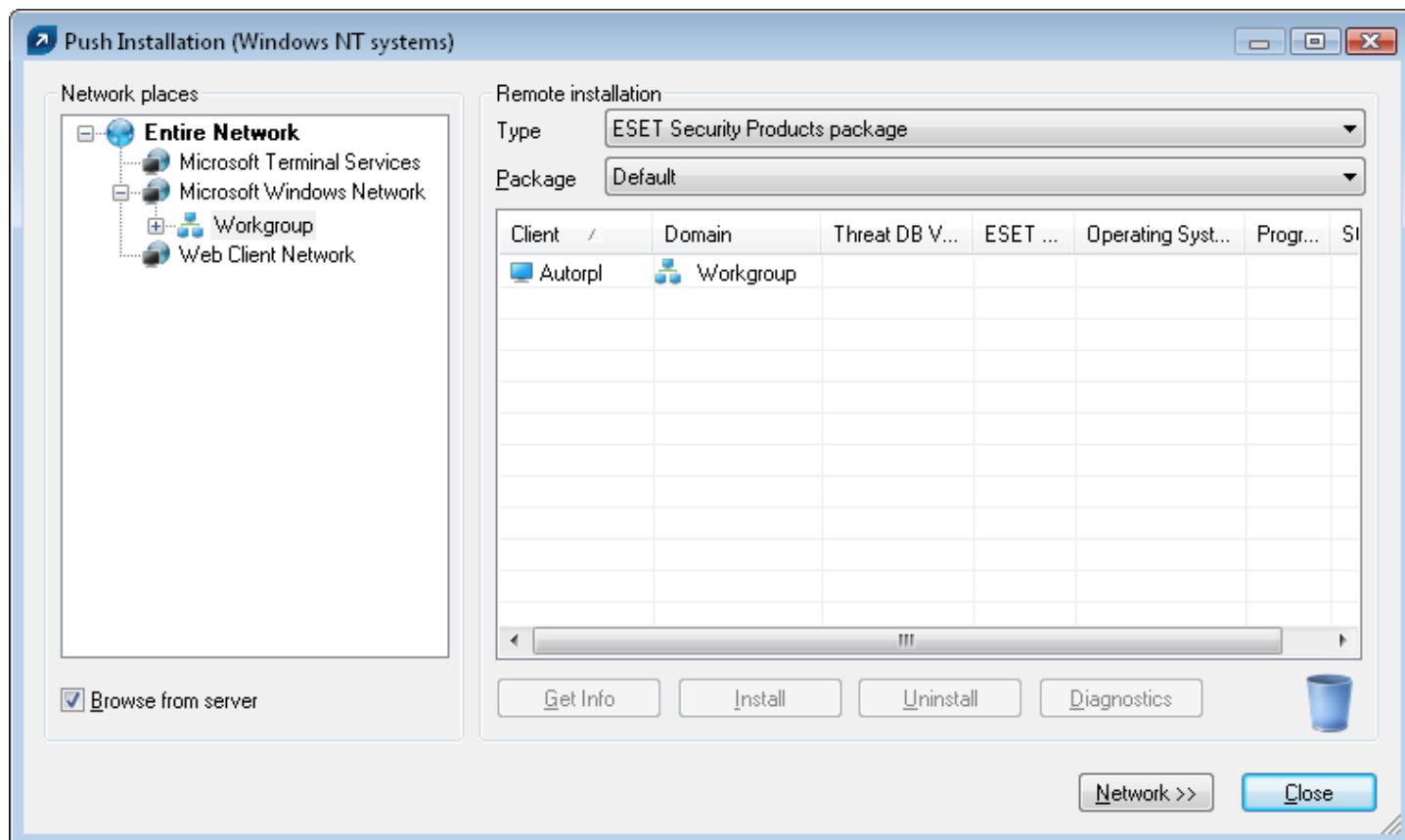
This method of remote install instantly pushes ESET client solutions to remote target computers. Target computers should be online. The following is a list of requirements (for additional requirements, see the Chapter 2 "ERAS"):

- Microsoft network client enabled (feature of network adapter)
- File sharing service enabled (feature of network adapter)
- File sharing service enabled in firewall
- Services: Remote Registry Service, Remote Service Manager, Server
- Administrator user name and password for client workstations (preferably the domain Administrator user name and password).

To initiate a push installation, follow the steps below:

- 1) Click the **Install...** button in the ERA Console (**Remote Install** tab).
- 2) In the **Network places** section on the left, browse to find the workstations where you intend to push the install package. Move them to the empty pane on the right (using the drag-and-drop method).

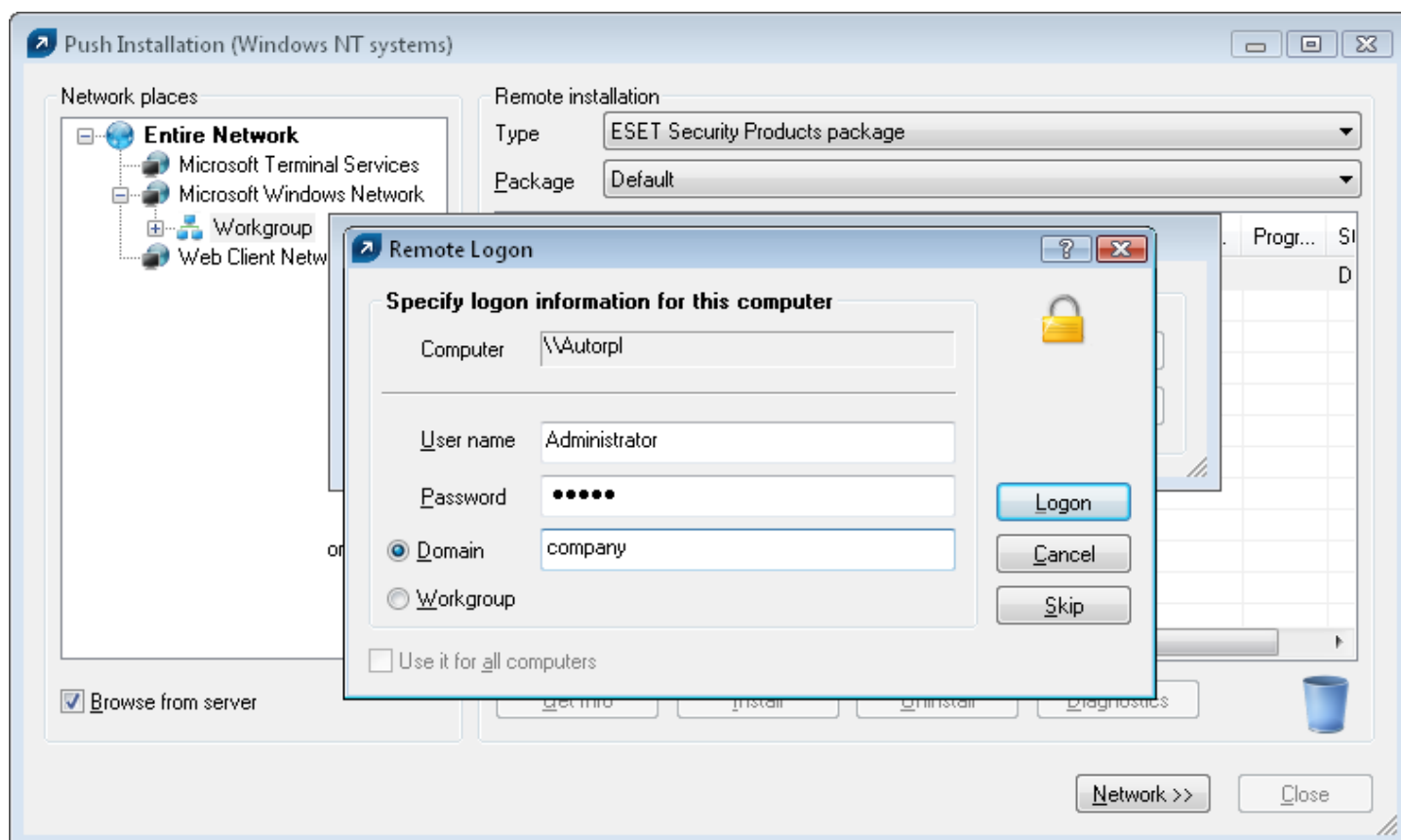
3) From the **Package** drop-down menu, select the desired install package to be delivered to target workstations.



4) In the panel on the right, select those workstations to which you intend push the package.

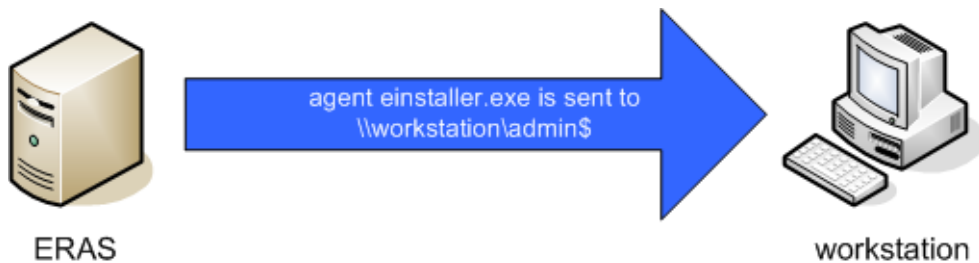
5) Click **Install** (you can also click **Get Info** to view information on selected clients).

6) In most cases, you will be prompted to insert the user name and password of the account under which the installation will take place (it must be an account with administrator rights).



7) The following operations are indicated by a progress bar and a text message. The operations are described below:

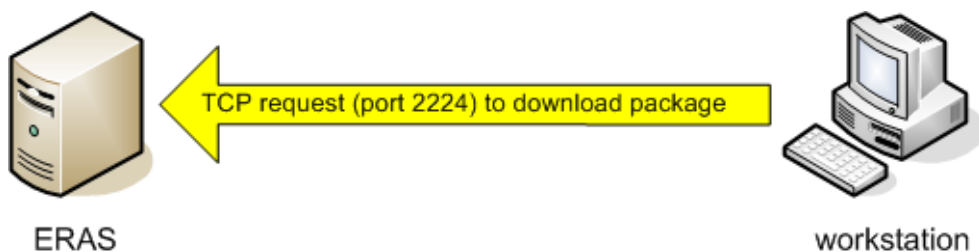
8) ERAS sends the `einstaller.exe` agent to the workstation with the help of the administrative share `admin$`.



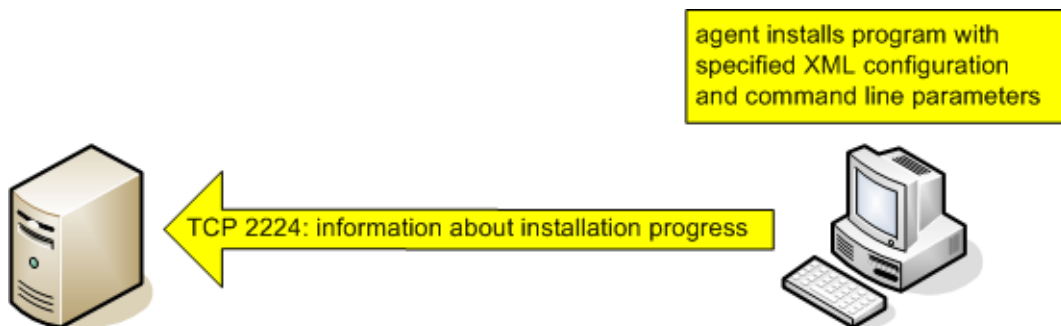
9) Agent starts as a service under the account specified in step 6.



10) Agent establishes communication with its "mother" ERAS and downloads the corresponding install package on TCP port 2224.



11) Agent installs the package under the administrator account defined in step 6; the corresponding .xml configuration and command line parameters are also applied.



12) Immediately after the installation is complete, the agent sends a message back to ERAS. Some ESET solutions require a reboot. If so, there will be a message regarding this requirement.

The context menu of the push install dialog window offers these options:

- **Get Info**
This feature detects the current status of the ESET client solution on selected workstations (requires Administrator user name and password). This feature uses the *admin\$* share.
- **Uninstall**
Program removal – the agent tries to remotely uninstall the program. The **Uninstall** mode does not take into consideration which package is selected from the **Package** menu.
- **Diagnostics**
Checks the availability of clients and services to be used in remote install. For more information see diagnostics of the remote install process.
- **Remove Installer Leftovers**
Unregisters agents from the service manager on client workstation and removes them from the hard disk. If this is completed successfully, the flag which prevents repeated installations of the package is removed (see section 6.4, "Avoiding repeated installations").

- **Logon...**
Opens a dialog window for specifying the administrator user name and password, which is otherwise displayed automatically (step 6). This feature forces logon to selected workstations.
- **Logoff**
Terminates logon session for selected workstations
- **Add Client...**
Adds individual clients (workstations) to the list. Enter IP address or the name of the client. Additional clients can be added simultaneously.

6.2.4 Logon / email remote install

The Logon and email remote install methods are very similar. They vary only in the way that the `einstaller.exe` agent is delivered to client workstations. ESET Remote Administrator allows the agent to be 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 following chapter).

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 the email attachment. If launched repeatedly, `einstaller.exe` will not trigger another installation of ESET solutions. For more information, see section 6.4, "Avoiding repeated installations."

NOTE: *The line calling the `einstaller.exe` agent from the logon script can be inserted using a text editor or other proprietary tool. Similarly, `einstaller.exe` can be sent as an email attachment by any email client. Regardless of the method used, make sure you are using the correct `einstaller.exe` file.*

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

Inserting the line (the path to `einstaller.exe`) to logon script:

- From the **Remote Install** tab, click **Export...** and select the **Type** and name of the **Package** to be installed.
- Click the ... button next to **Folder** and select the directory where `einstaller.exe` will be located and available within the network.
- In the **Share** field, make sure that the path is correct, or edit it if necessary.
- Click the ... button next to **Script Folder** to select the folder where the script is located.
- In the lower section, select the file to which the line (calling `einstaller.exe`) will be inserted.
- Click **Export to Logon Script** to insert the line.
- Location of the line can be modified in Advanced mode by clicking **Edit** and saved by clicking the **Save** button.

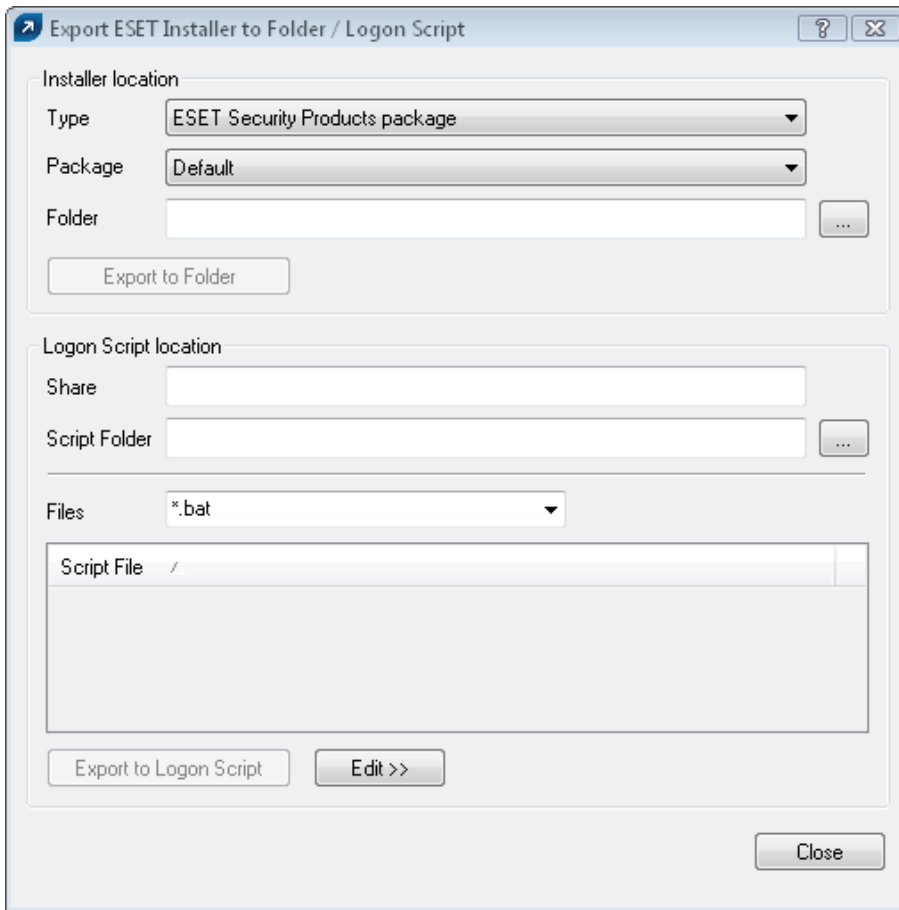


Figure 10 Export Installer to Folder / Logon Script dialog window

Attaching the agent (einstaller.exe) to email:

- Click **Email...** on the **Remote Install** tab and select the **Type** and the name of the **Package** you wish to install.
- Click **To...** to select addresses from the address book³ (or insert individual addresses).
- Insert a **Subject** in the corresponding field.
- Type a message into **Body**.
- Click **Send** to send the message.

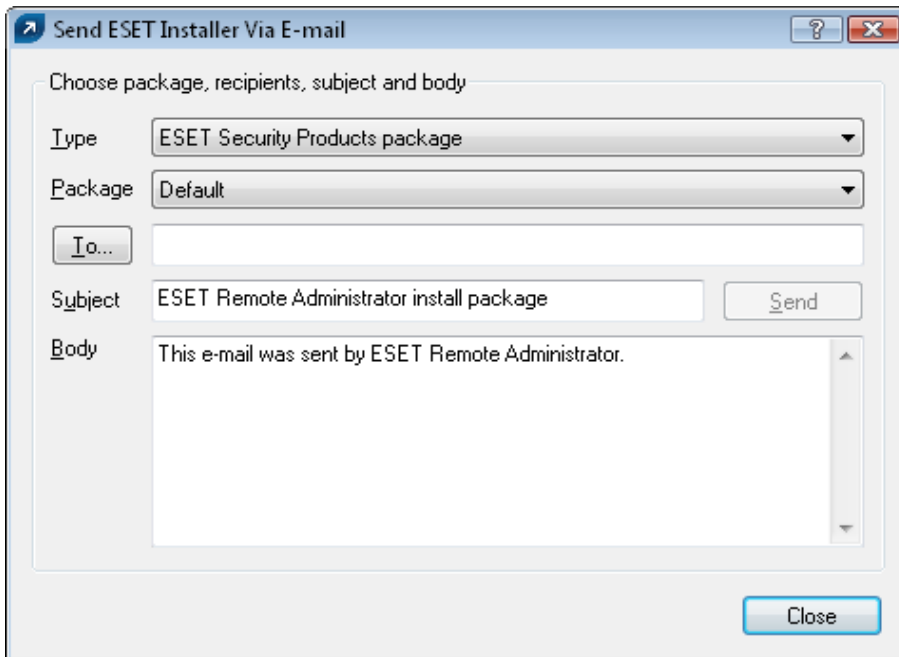
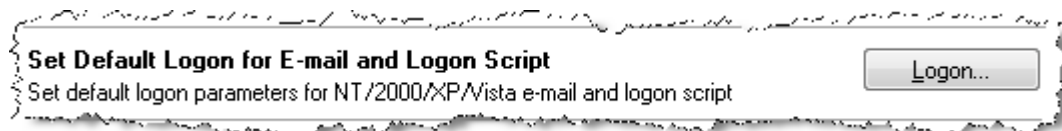


Figure 11 Send Eset Installer Via E-mail dialog window

During the process of remote installation, backward connection to ERAS takes place and the agent (einstaller.exe)

The ERA Console opens the Microsoft Outlook address book (provided it is installed on the same computer as ERAC).

adopts settings from the **Set Default Logon for E-mail and Logon Script** settings in the **Remote Install** tab.



Click **Logon...** to specify the user name and password of the account under which the installation of the package is to be performed. It must be an account with administrator rights or, preferably, a domain administrator account.

NOTE: Values inserted in the **Logon...** dialog window are forgotten after each service (ERAS) restart.

6.2.5 Custom remote install

It is not a requirement to use the tools incorporated in ESET Remote Administrator. In the end, the most important aspect is to deliver and execute the `einstaller.exe` file on client workstations.

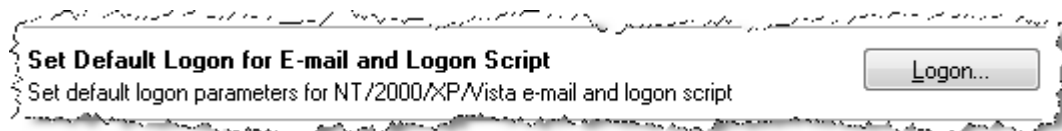
NOTE: For `einstaller.exe` to launch, the currently logged in user does not necessarily have to be an administrator. The agent adopts the required administrator user name / password / domain from the ERAS. For more information, see the end of this chapter.

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

- From the **Remote Install** tab, click **Export...** and select the **Type** and name of the **Package** to be installed.
- Click the **...** button next to **Folder** and select the directory where `einstaller.exe` will be exported.
- Click the **Export to Folder** button.
- Use the extracted `einstaller.exe` file.

NOTE: The "Direct installation 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 parameter `/qn` (for the version 3) or the parameter `/silentmode` (for the version 2). These parameters will run the installation without displaying a user interface.

During the process of remote installation, backward connection to ERAS takes place and the agent (`einstaller.exe`) adopts settings from the **Set Default Logon for E-mail and Logon Script** settings in the **Remote Install** tab.



Click **Logon...** to specify the user name and password of the account under which the installation of the package is to be performed. It must be an account with administrator rights or, preferably, the domain administrator account.

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 push installation of the corresponding package (sent via the share `admin$`)
- The installation of the package is launched, applying the associated `.xml` configuration and command line parameters under the account defined in ERAS (the **Logon...** button)

6.3 The `einstaller.exe` agent in detail

Each package is automatically assigned an ESET Remote Installer agent, which allows for seamless installation and communication between target workstations and ERAS. The ESET Remote Installer agent is named `einstaller.exe` and contains the following information:

- Name of ERA Server (+IP address of ERAS)
- Name and type of install package

The remote installation process using the `einstaller.exe` agent has two phases. First, the smaller installer (about 200 KB) `einstaller.exe` is delivered to a workstation. If all requirements are met, the agent initiates downloading of the entire install package (several MB) from ERAS.

The activity of the `einstaller.exe` agent is logged to the file `%TEMP%\einstaller.log` and if technically feasible, back to the ERA Server (target TCP port is 2224).

If the `installer.exe` agent is launched on a workstation with the Microsoft Windows NT4/2000/XP/Vista operating system:

1. `installer.exe` contacts ERAS on TCP port 2224 and adopts the user name and password defined in ERA (either during installation, or using the **Logon...** button).
2. (1) is the signal for ERAS to send the corresponding install package via `admin$`.
3. The waiting `installer.exe` collects the package and starts the installation under the defined account, applying the associated .xml configuration and command line parameters.

If the user rights are insufficient, or the user name and password is entered incorrectly, `installer.exe` tries to perform the installation under a current user (provided it has administrator rights). The corresponding install package is downloaded directly by `installer.exe` on TCP/IP port 2224.

On Microsoft Windows 95/98/Me operating systems, where there is no account hierarchy, install packages are downloaded by `installer.exe` (skipping the authentication process) and installed under a current user.

6.4 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 install package. The flag is written to the following registry key:

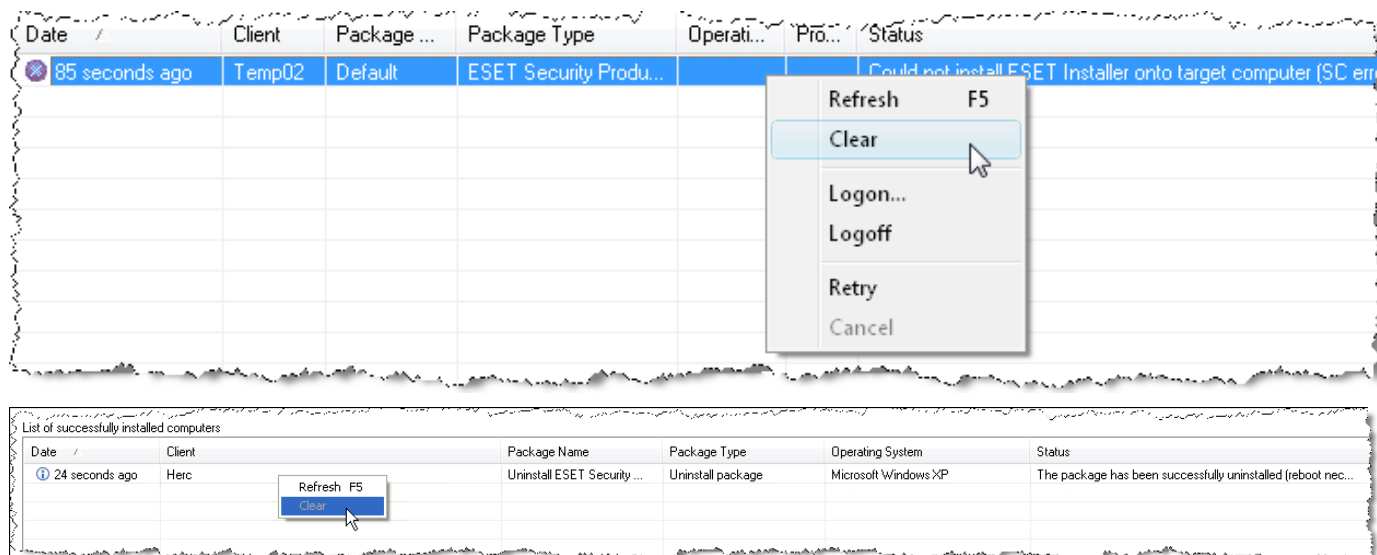
`HKEY_LOCAL_MACHINE\Software\Eset\Eset Remote Installer`

If the **Type** and **Name** of the package defined in the `installer.exe` agent matches the data in the registry, no installation is performed. This process prevents repeated installations to target workstations if the `installer.exe` agent is launched repeatedly,

The ERA Server provides an additional level of protection against repeated installations. It is performed at the moment when the installer establishes backward connection to ERAS (TCP 2224). If there is an error message related to the workstation, or the installation has been successfully completed, any additional installation attempts are denied.

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

Status 20001: ESET Installer was told to quit by the server 'X:2224'.



To prevent repeated installations from being denied by ERAS, related entries on the **Remote Install** tab must be removed. To delete such entries, right-click and select the **Clear** option from the context menu.

6.5 Installation process – error messages

During remote installations, errors may occur in two scenarios:

- When delivering the `installer.exe` agent to a remote workstation
- When launching the service `installer.exe`, i.e., during the installation itself

During a remote installation (i.e., push install), the `installer.exe` agent may display an error message consisting of the SC and GLE code. For example:

Could not set up IPC connection to target computer (SC error code 6, GLE error code 1326)

While SC error codes are primarily for internal identification, GLE codes are more important for the user. These are the typical “Win32 Error Codes”, which can be found at the following URL:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/system_error_codes.asp

The example above – GLE error 1326 – is caused by an incorrect user name and password for the account used for installation.

The most common error is GLE error 5 – Access Denied. This error may be caused by several factors:

- The firewall on the remote client may have file and printer sharing disabled
- The Server service is disabled, or file and print sharing on the network adapter is disabled
- Windows XP client workstations are not in the domain (policy)

If error messages occur after the `einstaller.exe` agent has been delivered to a target workstation, in `%TEMP%\einstaller.log`, the most important messages are sent back to the ERA Server (TCP 2224). Of course, this happens only if there is no communication problems between the workstation and ERAS.

At this point in the installation, the following messages may be encountered:

```
Eset Installer was told to quit by the server 'X:2224'.
Eset Installer could not connect to server X.
```

The first message is described in Chapter 6, “Avoiding repeated installations.” The second message is a general problem resulting from `einstaller.exe` not being able to connect back to ERAS.

6.5.1 Remote Install Diagnostics

To use the ERA remote install diagnostics tool, click the **Install...** button under the **Remote Install** tab. Once you have selected a client, click the **Diagnostics** button to verify that no errors were detected and ensure that the remote install will be successful. If any errors are detected, this process will allow the administrator to resolve these errors before attempting the remote installation.

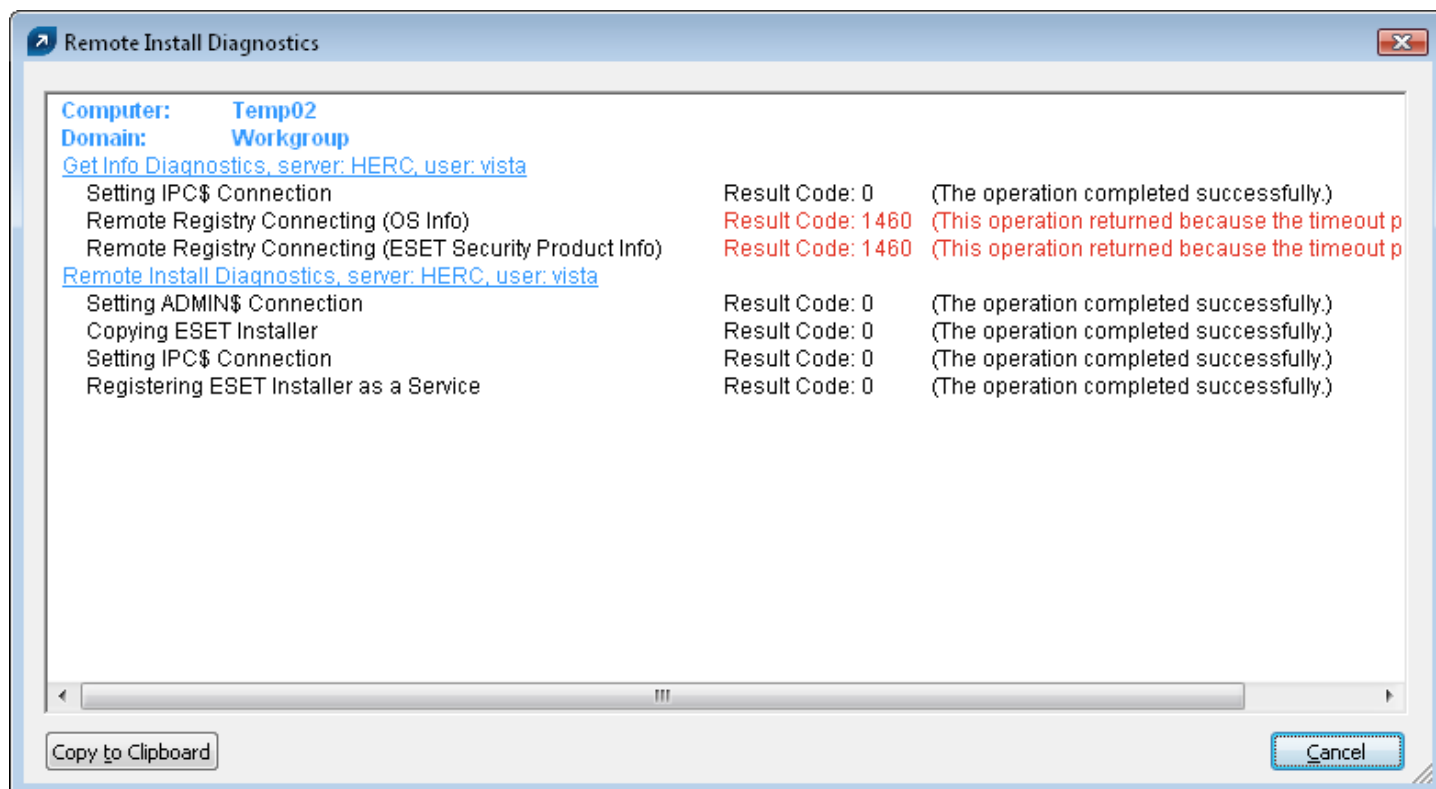


Figure 12 The diagnostics tool can detect potential problems before installation

7. Deployment scenarios for ESET Remote Administrator, Mirror server and ESET client solutions

7.1 Small network – 1x ERAS, 1x Mirror server

Suppose all clients are Microsoft Windows 2000/XP 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:

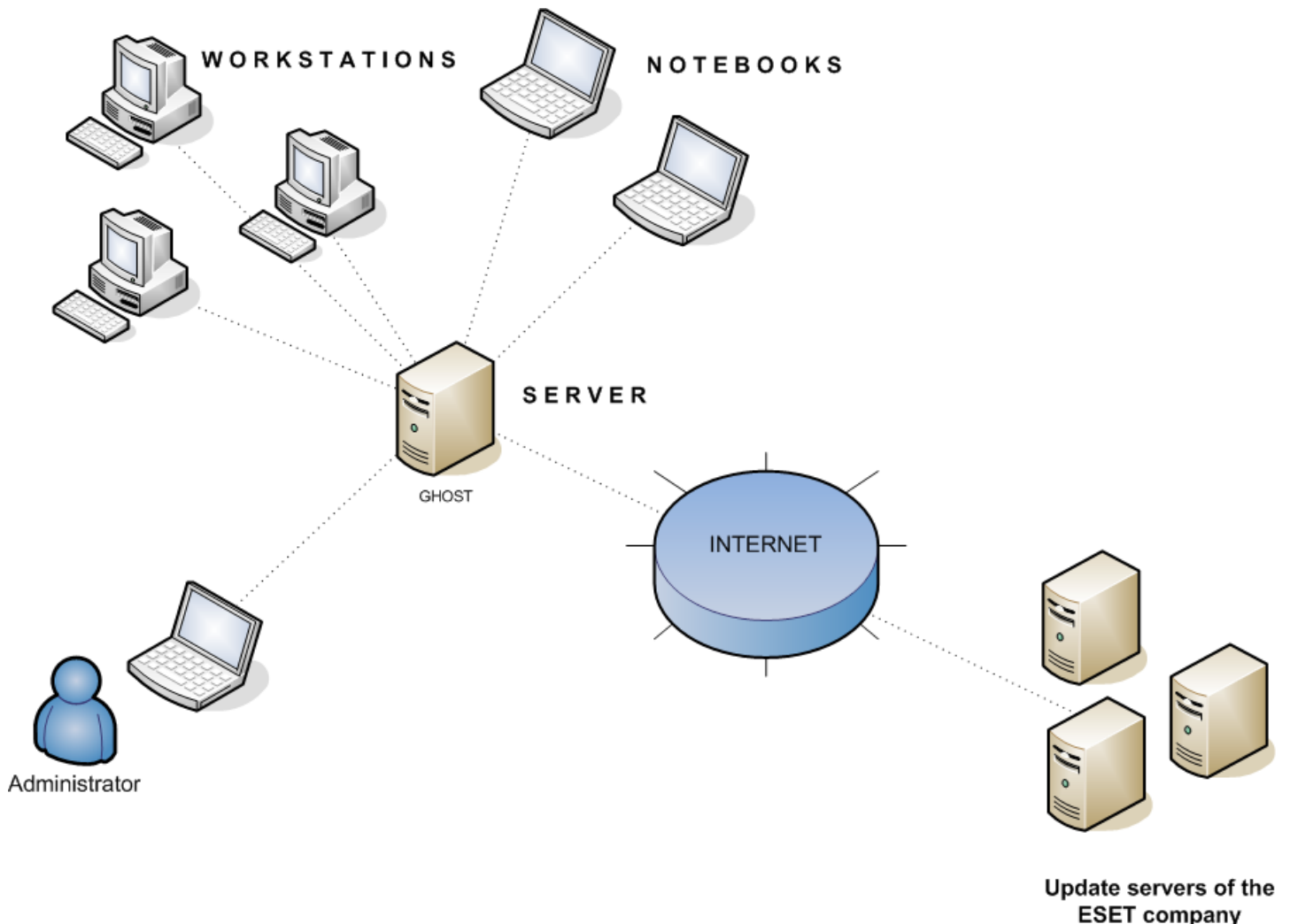


Figure 13 Network structure in a small company

7.1.1 Installation of ERA Server

Install ERA Server on the server named GHOST. During the installation, the license key file (nod32.lic) must be supplied in order to provide operation of ERAS for a defined period. After installation, the ERAS service is launched automatically. The activity of the ERAS service is recorded in the following file:

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

7.1.2 Installation of ERA Console

Install the ESET Remote Administrator Console to the administrator's PC/notebook (as shown in the lower part of the picture). If the Console is installed on the same computer as ERAS, the ERAS server name (GHOST, in our example) should be automatically inserted into the Console settings. If the Console and ERAS are installed on different computers, click **File > Edit Connections...** and click the **Connection** tab. Click the **Add/Remove...** button to add the ERA Server name.

For more information see section 4.1, "Connecting to ERAS."

7.1.3 Configuration of Mirror in ERA

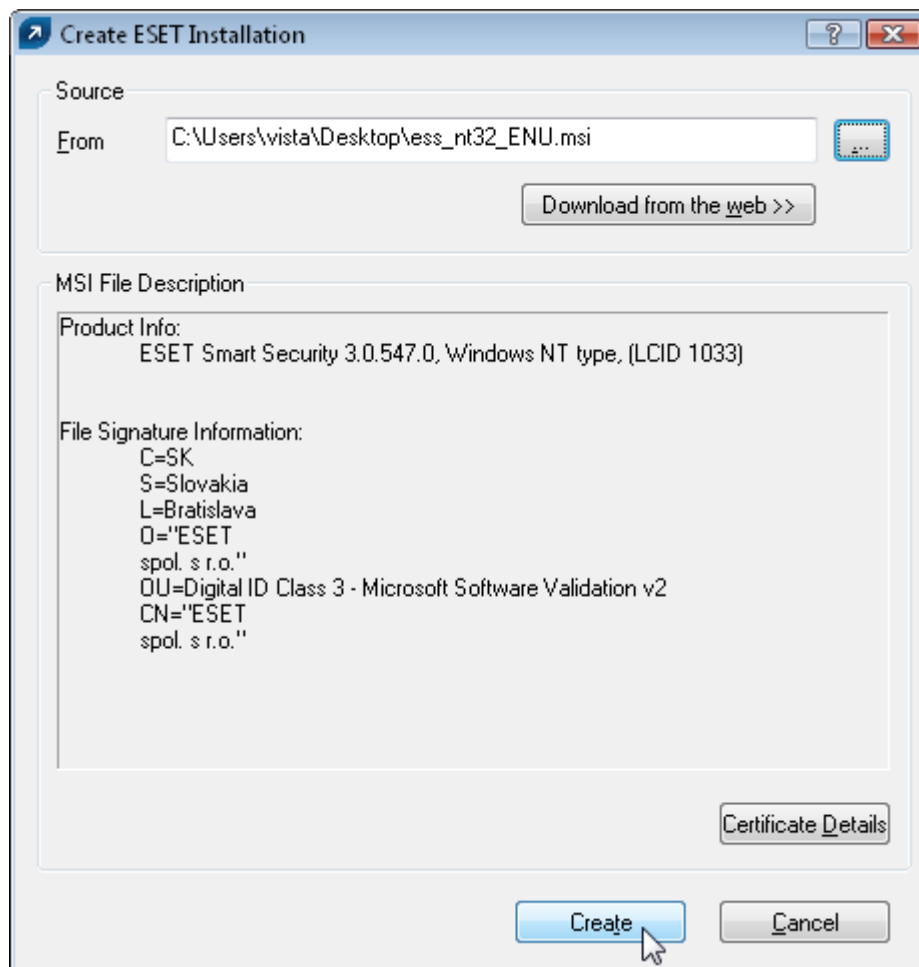
You can use the ERA Console to activate the LAN Update server - Mirror in the ERA Server. Proceed as follows:

- Connect the ERA Console to the ERA Server.
- From the ERA Console, click Tools > Server Options... and click the Updates tab.
- From the Update server: drop-down menu, select Choose Automatically (updates will be downloaded from ESET's servers), leave the Update interval at 60 minutes). Then insert Update user name (EAV-****) and Update password (click Set Password and type or paste the password you received along with the username).
- Select the Create update mirror option. Leave the default path to the folder for mirrored files. Also leave the default HTTP server port (2221). Leave Authentication at NONE.
- Go to the tab labeled Other Settings, click Edit Advance Settings... In the tree-like structure, navigate to ERA Server > Setup > Mirror > Create mirror for the selected program components. Click Edit on the right-hand side and select program components to be downloaded. Components for all language versions to be used in the network should be selected.
- In the tab Updates, click Update now to create Mirror.

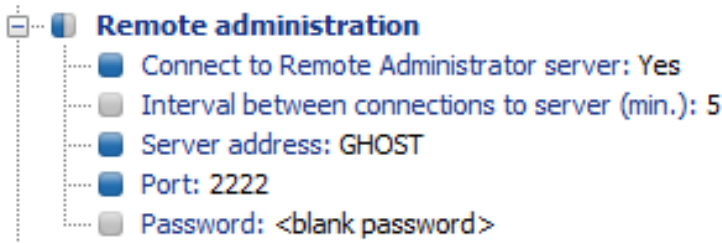
7.1.4 Remote install on workstations present in the network

Supposing that all workstations are turned on, the push installation method is the most effective method. Before starting a push install, you must first download the .msi install files for ESET Smart Security or ESET NOD32 Antivirus from ESET's web site. After this has been accomplished, follow the steps below:

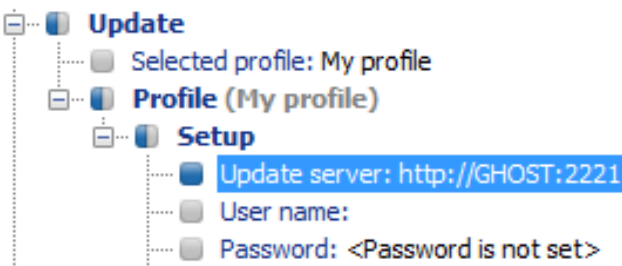
- Open the ERA Console and connect to the ERAS server (GHOST, in our example). On the **Remote Install** tab, click the **Packages...** button.
- Click **Add...** to display the **Create ESET Installation** window, and then click the ... button to insert the previously downloaded .msi install file.



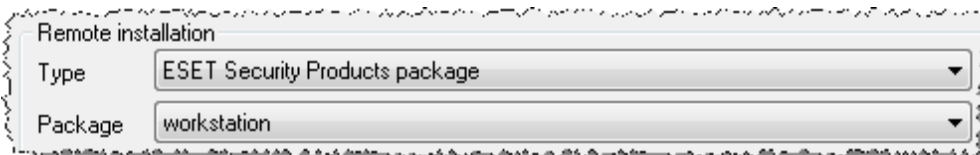
- Click **Create** to insert the installation file to the package (it may take a few minutes for the .msi files to be delivered to ERA Server).
- Click **Edit** in the **Installation Packages Editor** window to assign an .xml configuration file for the package. This configuration file will be applied later when installing the package.
- In the ESET Configuration Editor, focus primarily on the following settings:
- **ESET Smart Security > Kernel > Setup > Remote administration**
Your configuration should closely resemble the one in the picture below (the IP address can be also be entered in the **Server address** setting)



- In **ESET Smart Security, ESET NOD32 Antivirus > Update > Profile (My profile) > Setup** specify the name of the **Update server** (GHOST).



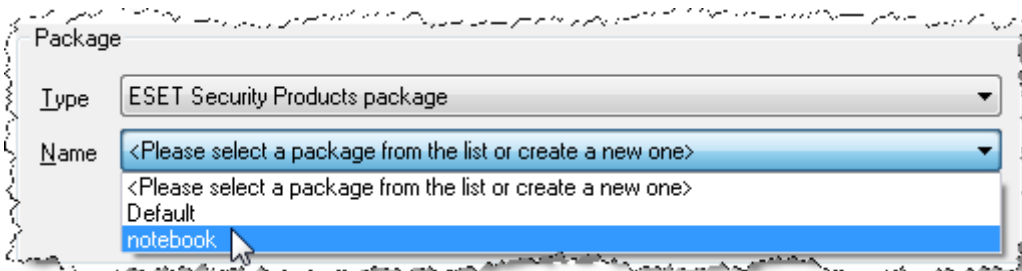
- Those are the minimum requirements for workstations as specified in our deployment scenario. Click **Console** on the right side of the ESET Configuration Editor to return to the **Installation Packages Editor** window.
- Click **Close** in the **Installation Packages Editor** dialog window. You will be prompted to define the name of the package, i.e. **workstation**. The installation package is now created.
- Last, the actual push installation process can be performed: Click the **Install...** button (**Remote Install** tab) and follow the instructions from previous chapters. It is important to select the **workstation** package as seen in the picture below:



7.1.5 Remote install on notebooks currently not present in the network

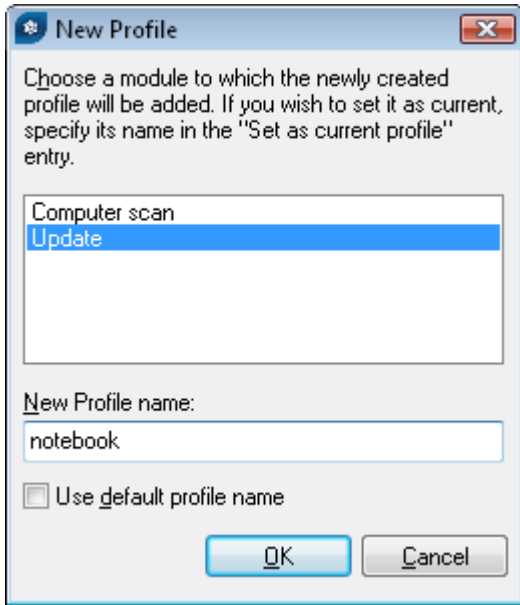
Notebooks which are sometimes outside the local network require a different type of remote installation. For these devices, the logon script method is suggested. Proceed as follows:

- Open the ERA Console and connect to the ERAS server (GHOST, in our example). On the **Remote Install** tab, click the **Packages...** button.
- Select the **Notebook** installation package from the **Name** menu.

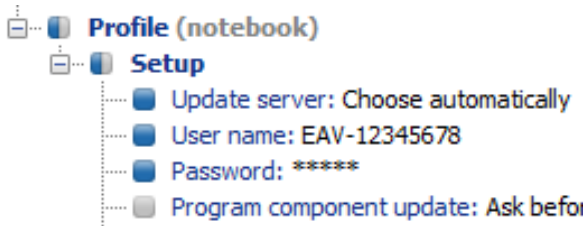


To allow notebook workstations to receive updates from the Mirror server "GHOST" (if they are connected to the network) and ESET's update servers (if they are not in the network), continue with the steps below:

- Click the **Edit** button to modify the .xml file created using the ERAC Editor in section 7.1.4.
- Navigate to **ESET Smart Security, ESET NOD32 Antivirus > Update > Profile (My profile)**.
- Right-click **Profile (My profile)** and select **New Profile...** from the context menu.
- In the **New Profile** dialog window, verify that **Update** is highlighted and then deselect the **Use default profile name** check box.
- Enter a **New Profile name**, such as **notebook**.



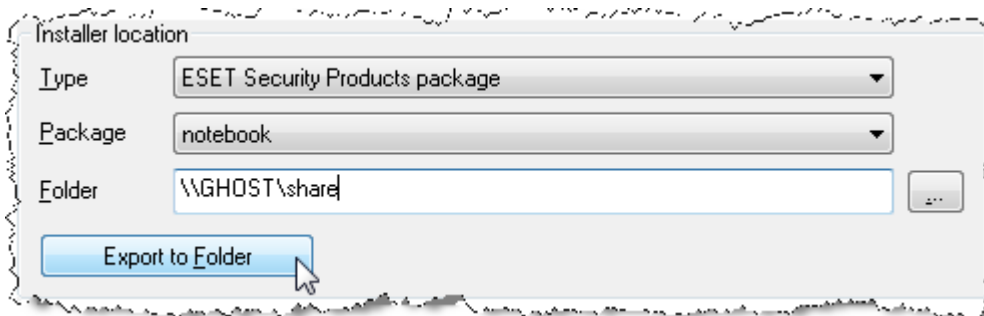
- Click **OK** to save the configuration. Now, in addition to **Profile (My profile)**, the **Profile (notebook)** appears. Click **Profile (notebook) > Setup** and configure the following three attributes as seen below:



- The **Choose Automatically** option allows updating from ESET's servers rather than the local network (Mirror), while authentication to the servers is granted by the **User name** and **Password** (supplied by ESET after purchase).
- Click **Console** on the right side of the ESET Configuration Editor to return to the **Installation Packages Editor** window.
- Click **Yes** and then **Save as...** in the **Installation Packages Editor** window and save the modified installation package as **notebooks**. Click **Close** to return to the ERA Console.

Next, the **einstaller.exe** agent needs to be added to the **notebooks** package in the logon script. Proceed as follows:

- From the **Remote Install** tab, click **Export...**
- From the **Package** drop-down menu, select **notebook** and then click the ... button to select a folder where the agent **einstaller.exe** will be saved. The selected folder should be accessible for notebooks when they connect to the company's network (or domain). For our purposes, let's use the folder defined in the UNC path: **\\GHOST\share**



- Click the **Export to Folder** button and click **OK**. The **einstaller.exe** file now resides in the **\\GHOST\share** folder.

If you already have a logon script in use for other purposes, ERAC can automatically add a line to your existing script. This will allow notebooks to receive the latest virus signature update whenever they log on to the domain. To add this line to your existing script, follow the steps below:

- Click the ... button to the right of the **Script Folder** field and select the folder where your script resides.
- From the **Remote Install** tab, click **Logon...** Enter the Windows **User name** and **Password** (and **Domain**) of the administrator, and click **OK**. The logon script will be activated using these credentials.
- Now, any time a notebook connects to the domain, the logon script will run automatically, and install the latest virus signature update.

7.2 Company with a remote subsidiary – 2x ERAS, 2x Mirror server

Let's use a copy of the previous network structure and add one subsidiary, with several clients and one server named LITTLE. Let's suppose there is a VPN channel between the headquarters and the subsidiary. 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.

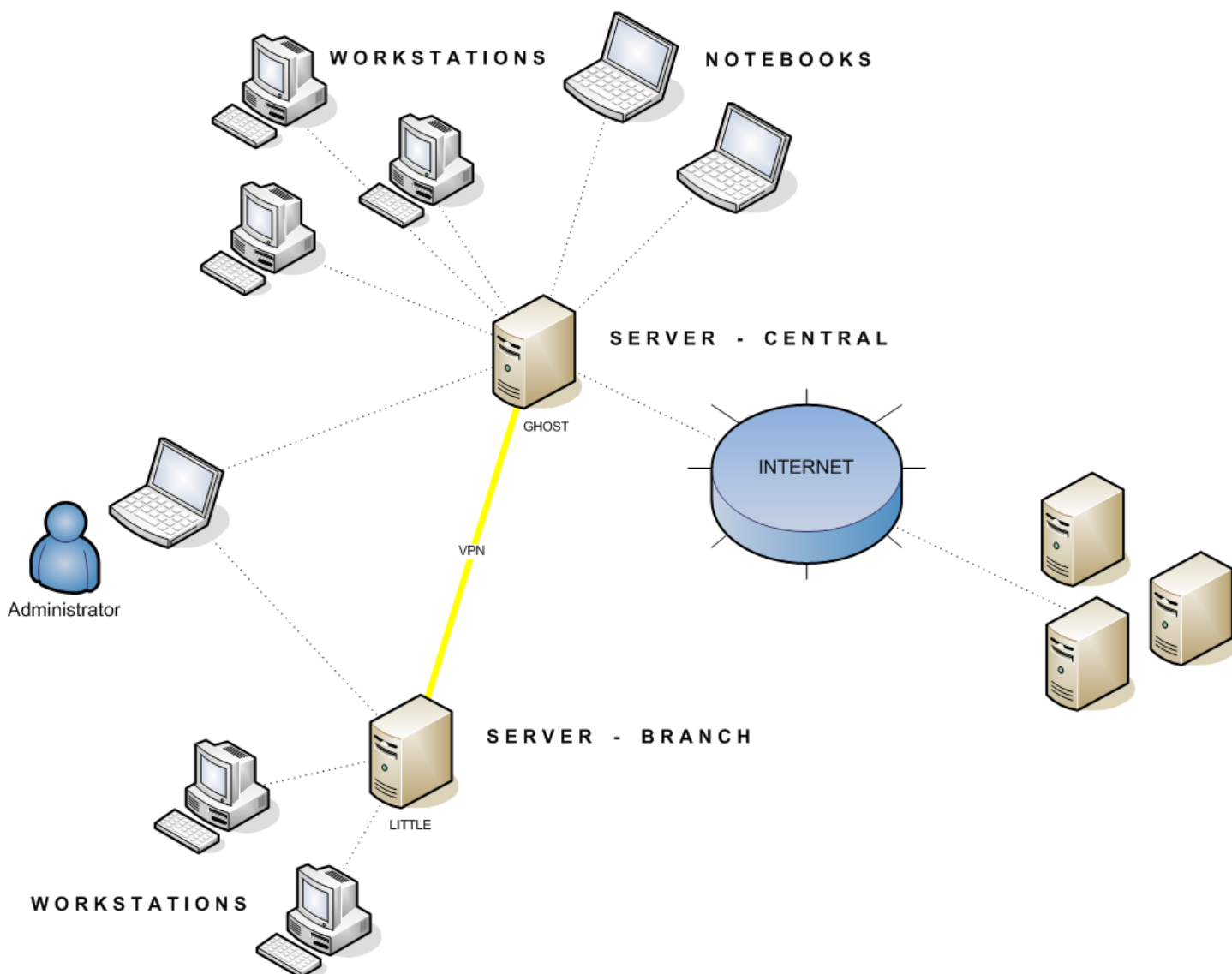
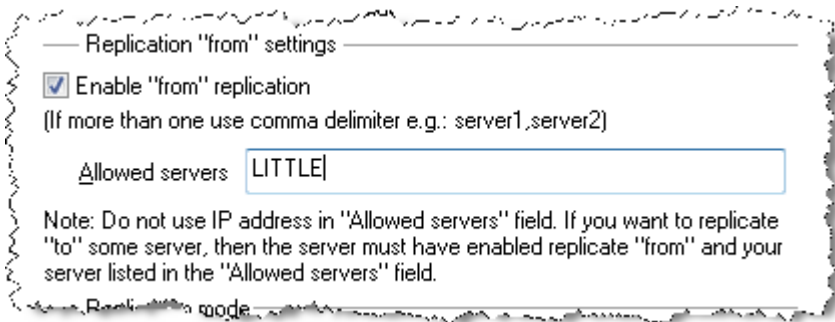


Figure 14 Network structure – company with one subsidiary.

7.2.1 Installation at headquarters

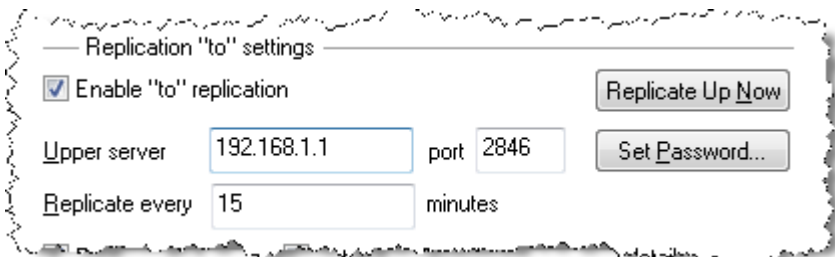
Installations of ERAS, ERAC and client workstations are very similar to the previous scenario. The only difference is in the configuration of the master ERA Server (GHOST); in this scenario, we must specify that the LITTLE server is allowed to receive updates from GHOST.

To do this, open the ERA Console which is connected to GHOST. Click **Tools > Server Options... > Replication**. Select the **Enable "from" replication** check box and enter **LITTLE** into the **Allowed servers** field.



7.2.2 Subsidiary: installation of ERA Server

As in the example above, install the second ERA Server. Again, enable and configure the replication settings. Select the option **Enable "to" replication (Tools > Server Options... > Replication)** and enter the IP address⁴ of the master ERA Server into the **Upper server** field - the IP address of the GHOST server, in our example.



7.2.3 Subsidiary: Installation of HTTP Mirror server

The Mirror server installation example of the previous model can also be used in this case. The only changes are in the sections defining:

- Source of update files
- User name and Password

As seen in Figure 14, updates for the subsidiary are not downloaded from ESET's update servers, but from the server at the headquarters (GHOST). The update source is defined by the URL address: *http://ghost:2221* (or *http://IP_address_of_ghost:2221*).

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

7.2.4 Subsidiary: Remote installation to clients

Once more, the previous model can be used, except that it is suitable to perform all operations with ERAC connected directly to the ERA Server of the subsidiary (LITTLE)⁵.

⁴ In order to avoid potential DNS translation problems when converting names to IP addresses between networks (depending on the DNS configuration).

⁵ This is done to prevent install packages from being transferred via the VPN channel, which is slower

8. Hints & tips

8.1 Export and other features of client XML configuration

From the ERA Console, select any clients in the **Clients** tab in ERA Console. Right-click and select **Configuration...** from the context menu. Click **Save As...** to export the assigned configuration of the given client to an .xml file⁶. 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.
- For configuring multiple clients; selected clients receive a previously downloaded .xml file and adopt the settings which are defined in the file (again, no new configuration is created, only assigned by the **Select...** button).

Example: An ESET solution is installed on only 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.

8.2 Combined update for notebooks and mobile devices

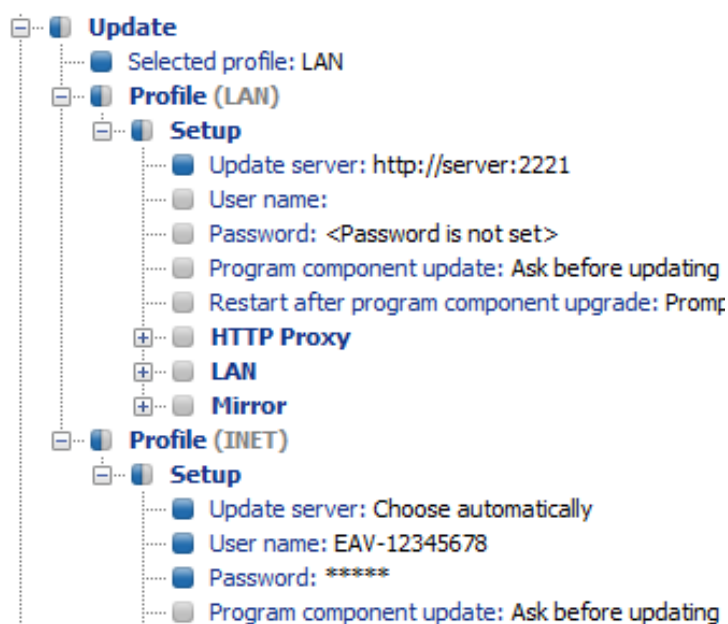
If there are any mobile devices in your local network (i.e., notebooks), we recommend that you configure a combined update from two sources, ESET's update servers and the local Update Server - Mirror. First, notebooks contact the local Mirror server, and if the connection fails (they are outside of the office), they download updates directly from ESET's servers. To allow for this functionality:

- Create two update profiles, 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 Smart Security or ESET NOD32 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 on the **Update** branch and select **New profile** from the context menu.

The result of modifications should resemble the one displayed below:

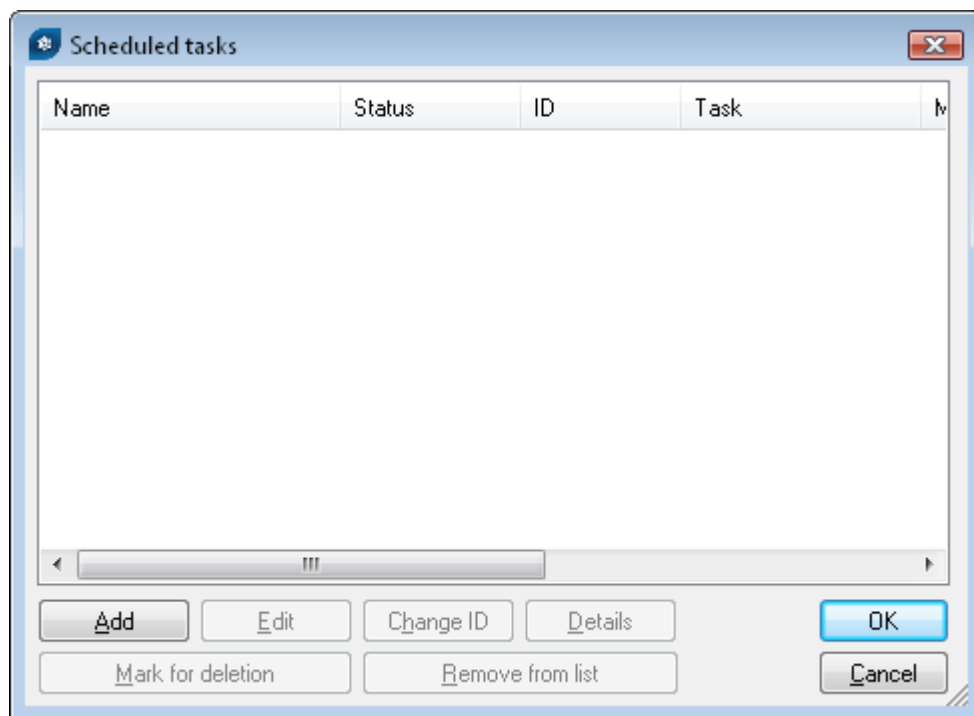


The profile **LAN** downloads updates from the company's local Mirror server (**http://server:2221**), while the profile **INET** connects to ESET's servers (**Choose Automatically**).

Next, define an update task which runs each update profile in succession. To do this, navigate to **ESET Smart**

⁶ .xml configuration files can also be extracted directly from the ESET Smart Security program interface.

Security, ESET NOD32 Antivirus > Kernel > Setup > Scheduler/Planner or NOD32 version 2 > General > Setup > Scheduler/Planner. 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** and click **Next**.
- Leave the **Interval between task execution** set to **60**. Click **Next** twice to accept the defaults and then click **Finish**.
- Select a **Primary** and **Secondary** update profile (**LAN, INET** - or vice versa) for this task.
- 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 be applied only if the update from **LAN** fails.

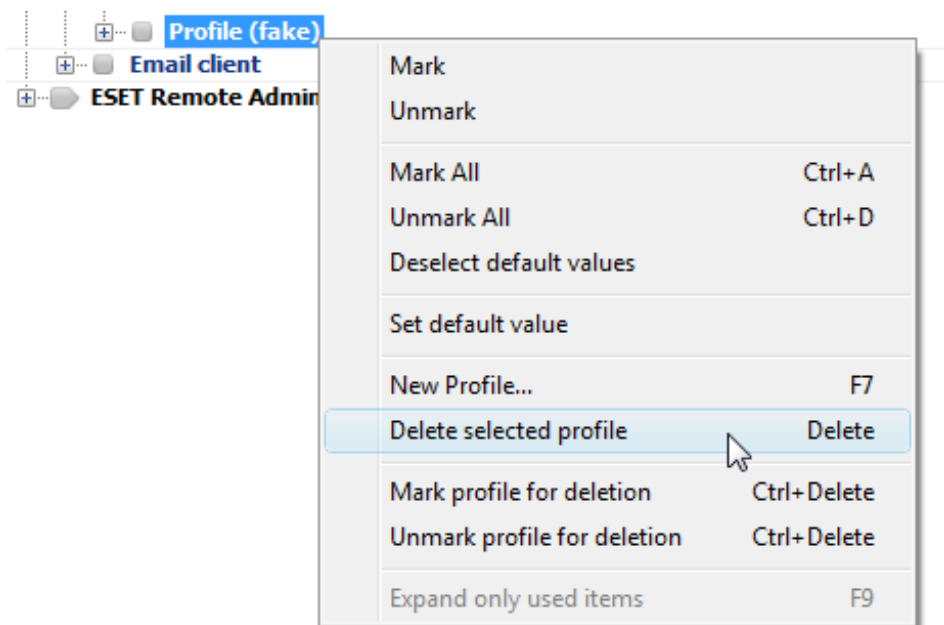
Recommendation: Export the current .xml configuration from a client (for more information, see section 8.1) and perform the above-mentioned modifications on the exported .xml file. Thus any duplications between the Scheduler and non-working profiles is avoided.

8.3 Removing existing profiles

If unused or duplicate profiles have been created on client workstations by mistake, these can be removed remotely. To remove an unwanted profile, follow the steps below:

- From the ERA Console, click the **Clients** tab and then double-click on 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 task wizard, click **Edit** to open the Configuration Editor. Press CTRL + D to unmark (grey) all settings. This helps to prevent accidental changes, as any new changes will stand out in blue.
- Right-click on the profile you wish to remove and select **Delete selected profile** from the context menu.
- Click **File > Save** and close the Configuration Editor.
- Verify that the client you selected is in the **Selected items** column on the right. Click **Next** and then click **Finish**.

The unwanted profile will be removed from the selected workstation.



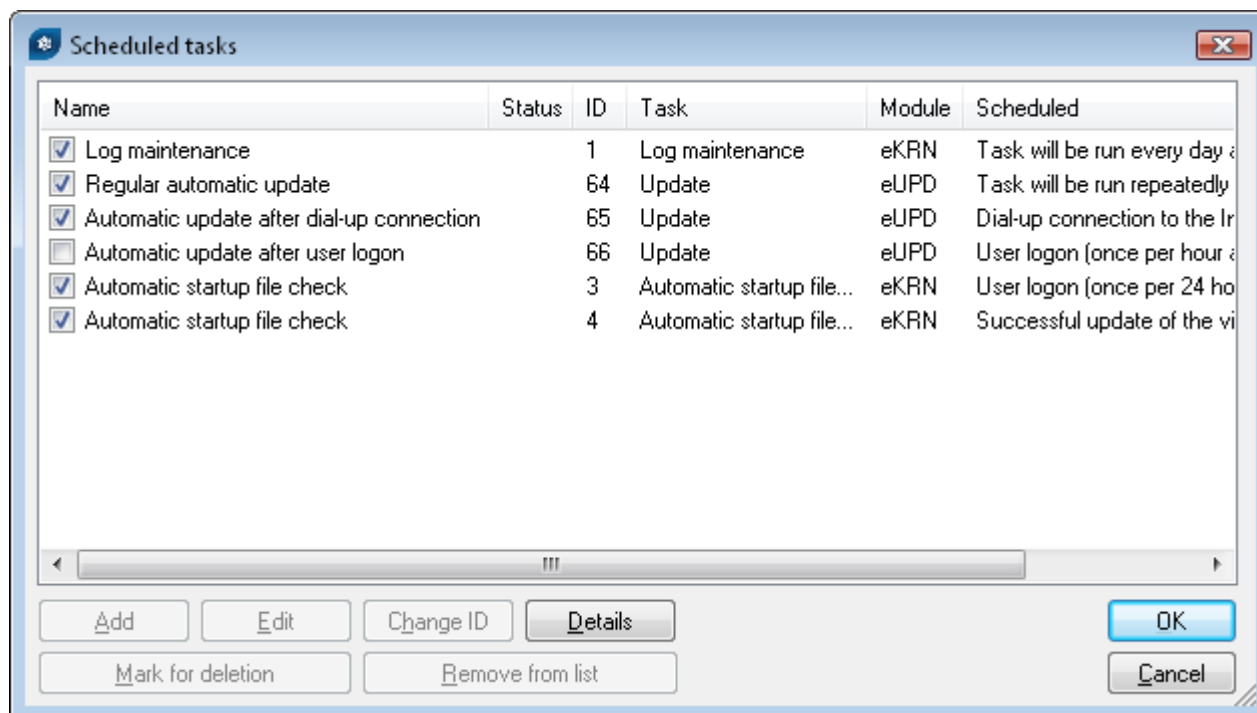
8.4 Scheduler setup

To modify scheduled tasks remotely, open the ESET Configuration Editor and navigate to **ESET Smart Security, ESET NOD32 Antivirus > Kernel > Setup > Scheduler/Planner** (or **NOD32 version 2 / General / Setup / Scheduler/Planner**) and click the **Edit** button.

If you intend to add new tasks, you can use a completely new (empty) .xml configuration. If you wish to modify or remove existing tasks, it is necessary to:

- Use an .xml configuration exported from the given client
- Or use the same IDs of the tasks you intend to Edit or Remove.

This is the resulting **Scheduled tasks** window from an exported .xml configuration:



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 functionality of the buttons in the dialog window are as follows:

- **Add...** – Adds new tasks
- **Edit** – Modifies selected tasks
- **Change ID** – Modifies ID of selected tasks
- **Details** – Summary information about the selected task
- **Select for deletion** – Application of .xml file will remove tasks 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.

NOTE: Since attribute IDs for new tasks are generated randomly, complications may occur if the administrator applies the same type of task repeatedly. Example: There are 40 client workstations in the network. The administrator adds a new task named ABC, which is assigned attribute ID 4A2B8CA5. The company purchases 10 new workstations and the administrator again applies a new task named ABC, but with an attribute ID of 8D5A6D1B.

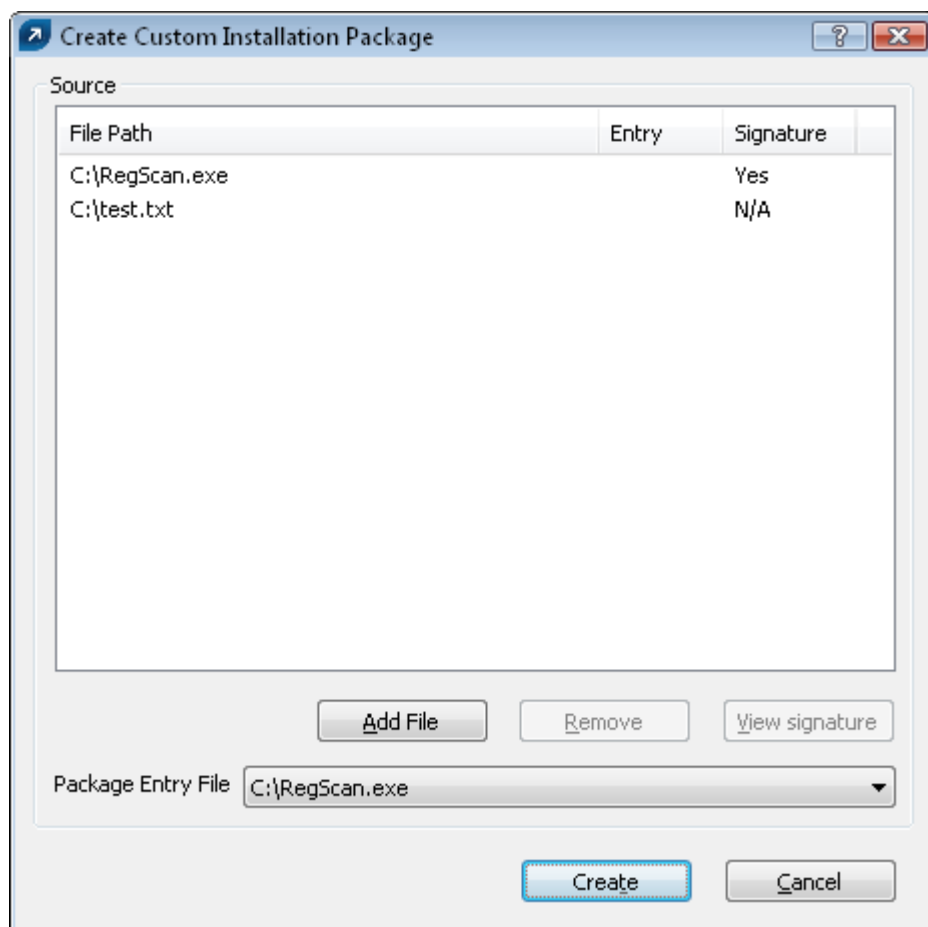
Later he decides that the ABC task should be modified. He first exports the .xml configuration from one of the original 40 forty workstations, modifies it and applies it as a configuration task to all 50 workstations. This creates a problem, because the same type of task now has two different IDs (4A2B8CA5, 8D5A6D1B). The modification will be performed correctly on the first 40 workstations, but the 10 new workstations will have a new duplicate task created. These complications can be avoided by clicking Change ID and setting a common ID when creating a task of the same type.

8.5 Custom install packages

The **Installation Packages Editor** allows the administrator to create a custom installation package.

- To open the **Installation Packages Editor** click the **Packages...** button from the **Clients** tab in ERAC.
- From the **Package Type** drop-down menu select **Custom package** and then click the **Add...** button.
- Click the **Add File** button and select the master setup file (einstaller.exe). If you wish to include a batch or logon script in the installation package, click the **Add File** button again.

Distribution of customer install packages to remote clients is very similar to the remote installation of any ESET client solution. The package is automatically extracted on target computers and the einstaller.exe file is run.



This type of package is also useful for uninstalling security software from other vendors.