

ESET **Remote** **Administrator**

Installation Manual
and User Guide



contents

ESET Remote Administrator

Copyright © 2009 by ESET, spol. s r. o.

ESET Smart Security 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

REV.20091106-017

1. Introduction	4
1.1 Program architecture	4
1.1.1 ERA Server (ERAS)	4
1.1.2 ERA Console (ERAC)	4
2. Installation of ERA Server and ERA Console	5
2.1 Requirements	5
2.1.1 Hardware requirements	5
2.1.2 Ports used	5
2.2 Basic Installation guide	6
2.2.1 Environment overview (network structure)	6
2.2.2 Before installation	6
2.2.3 Installation	7
2.2.3.1 Installation of ERA Server	7
2.2.3.2 Installation of ERA Console	7
2.2.3.3 How to enable and configure the Mirror	7
2.2.3.4 Database types supported by ERA Server	8
2.2.3.4.1 Basic requirements	8
2.2.3.4.2 Database connection setup	9
2.2.3.4.3 Installing over an existing database	9
2.2.3.5 Remote install to client workstations in the network	10
2.2.3.6 Remote install on notebooks currently not present in the network	10
2.3 Scenario – Installation in an Enterprise environment	10
2.3.1 Environment overview (network structure)	10
2.3.3 Installation	11
2.3.3.1 Installation at headquarters	11
2.3.3.2 Branch office: Installation of ERA Server	11
2.3.3.3 Branch office: Installation of HTTP Mirror server	11
2.3.4 Other requirements for Enterprise environments	12
3. Working with ERAC	13
3.1 Connecting to ERAS	13
3.2 ERAC – main window	13
3.3 Information filtering	14
3.3.1 Groups	14
3.3.2 Filter	15
3.3.3 Context menu	15
3.4 Tabs in ERAC	16
3.4.1 General description of tabs and clients	16
3.4.2 Replication & information in individual tabs	17
3.4.3 Clients tab	18
3.4.4 Threat Log tab	21
3.4.5 Firewall Log Tab	21
3.4.6 Event Log tab	21
3.4.7 Scan Log tab	22
3.4.8 Tasks tab	22
3.4.9 Reports tab	22
3.4.10 Remote install tab	22
3.5 ERA Console setup	22
3.5.1 Connection tab	23
3.5.2 Columns – Show / Hide tab	23
3.5.3 Colors tab	23
3.5.4 Paths tab	23
3.5.5 Date / Time tab	23
3.5.6 Other settings tab	23
3.6 Display modes	24
3.7 ESET Configuration Editor	24
3.7.1 Configuration layering	25
3.7.2 Key configuration entries	26
4. Installation of ESET client solutions	28
4.1 Direct installation	28
4.2 Remote installation	28
4.2.1 Requirements	30
4.2.2 Configuring the environment for remote installation	31

4.2.3	Remote Push Install	31	8.2.3	Database Transfer	68
4.2.4	Logon /email remote install	34	8.2.4	Database Backup	69
4.2.5	Custom remote install	36	8.2.5	Database Restore	69
4.2.6	Avoiding repeated installations	37	8.2.6	Delete Tables	69
4.3	Installation in an Enterprise environment	37	8.2.7	Install New License Key	69
5.	Administering client computers	39	8.2.8	Modify server configuration	69
5.1	Tasks	39	9. Troubleshooting	70	
5.1.1	Configuration Task	39	9.1	FAQ	70
5.1.2	On-demand Scan task	39	9.1.1	Problems installing ESET Remote Administrator to Windows server 2000/2003	70
5.1.3	Update Now task	40	9.1.2	What is the meaning of the GLE error code?	70
5.1.4	SysInspector Script Task	40	9.2	Frequently encountered error codes	70
5.2	Groups	40	9.2.1	Error messages displayed when using ESET Remote Administrator to remotely install ESET Smart Security or ESET NOD32 Antivirus	70
5.3	Policies	41	9.2.2	Frequently encountered error codes in era.log	71
5.3.1	Basic principles and operation	41	9.3	How to diagnose problems with ERAS?	71
5.3.2	How to create policies	41	10. Hints & tips	72	
5.3.3	Virtual policies	42	10.1	Scheduler	72
5.3.4	Policies and structure of ESET Configuration Editor	43	10.2	Removing existing profiles	74
5.3.5	Viewing policies	43	10.3	Export and other features of client XML configuration	74
5.3.6	Assigning policies to clients	44	10.4	Combined update for notebooks	74
5.3.6.1	Default Primary Clients Policy	44	10.5	Installation of third-party products using ERA	76
5.3.6.2	Manual assigning	44			
5.3.6.3	Policy Rules	44			
5.3.7	Deleting policies	45			
5.3.8	Special settings	45			
5.3.9	Policy deployment scenarios	46			
5.3.9.1	Each server is a standalone unit and policies are defined locally	46			
5.3.9.2	Each server is administered individually - policies are managed locally but the Default Parent Policy is inherited from the upper server	47			
5.3.9.3	Inheriting policies from an upper server	47			
5.3.9.4	Assigning policies only from the upper server	48			
5.3.9.5	Using policy rules	49			
5.3.9.6	Using local groups	49			
5.4	Notifications	50			
5.4.1	Notification Manager	50			
5.4.1.1	Notifications via SNMP TRAP	54			
5.4.2	Rule creation	54			
5.5	Detailed information from clients	55			
6. Reports	57				
7. ESET Remote Administrator Server (ERAS) setup	59				
7.1	Security tab	59			
7.2	Server Maintenance tab	59			
7.3	Mirror server	60			
7.3.1	Operation of the Mirror server	60			
7.3.2	Types of updates	61			
7.3.3	How to enable and configure the Mirror	61			
7.3.4	Mirror for clients with NOD32 version 2.x	63			
7.4	Replication tab	63			
7.5	Logging tab	65			
7.6	License management	65			
7.7	Advanced settings	66			
7.8	Other settings tab	66			
7.8.1	SMTP settings	66			
7.8.2	Ports	66			
7.8.3	New clients	67			
7.8.4	ThreatSense. Net	67			
8. ERA Maintenance tool	68				
8.1	ERA Server Information	68			
8.2	Task Type	68			
8.2.1	Stop ERA Server	68			
8.2.2	Start ERA Server	68			

1. Introduction

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

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

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

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

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

%ProgramFiles % = typically C:\Program Files

%ALLUSERSPROFILE % = typically C:\Documents and Settings\All Users

1.1 Program architecture

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

1.1.1 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, Vista and 2008. The main task of this service is to collect information from clients and to send them various requests. These requests, including configuration tasks, remote installation requests, etc., are created through the ERA Console (ERAC). ERAS is a meeting point between ERAC and client computers – a place where all information is processed, maintained or modified before being transferred to clients or to ERAC.

1.1.2 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 process console.exe, which is usually located in the following directory:

%ProgramFiles %\ESET\ESET Remote Administrator\Console

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

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

2. Installation of ERA Server and ERA Console

2.1 Requirements

ERAS works as a service, and therefore requires a Microsoft Windows NT-based operating system (NT4, 2000, XP, 2003, Vista or 2008). The Microsoft Windows Server Edition is not necessary for ERAS to work. A computer with ERAS installed on it should always be online and accessible via computer network by:

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

2.1.1 Hardware requirements

The effect on system performance is minimal. However, it depends on the number of clients, the type of database used by ERAS, on the logging level, etc. The minimum HW 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 Ports used

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

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

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 einstaller.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 einstaller.exe from ERAS to a client using the share admin\$
UDP	137 (target port from the point of view of ERAS)	"Name resolving" during remote install.
UDP	138 (target port from the point of view of ERAS)	"Browsing" during remote install
TCP	445 (target port from the point of view of ERAS)	Direct access to shared resources using TCP/IP during remote install (an alternative to TCP 139)

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

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

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

2.2 Basic Installation guide

2.2.1 Environment overview (network structure)

A company network usually consists of one local area network (LAN), therefore we suggest installing one ERAS and one Mirror server. The Mirror server can either be created in ERAS or in ESET NOD32 Antivirus Business Edition /ESET Smart Security Business Edition.

Suppose all clients are Microsoft Windows 2000/XP/Vista 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:

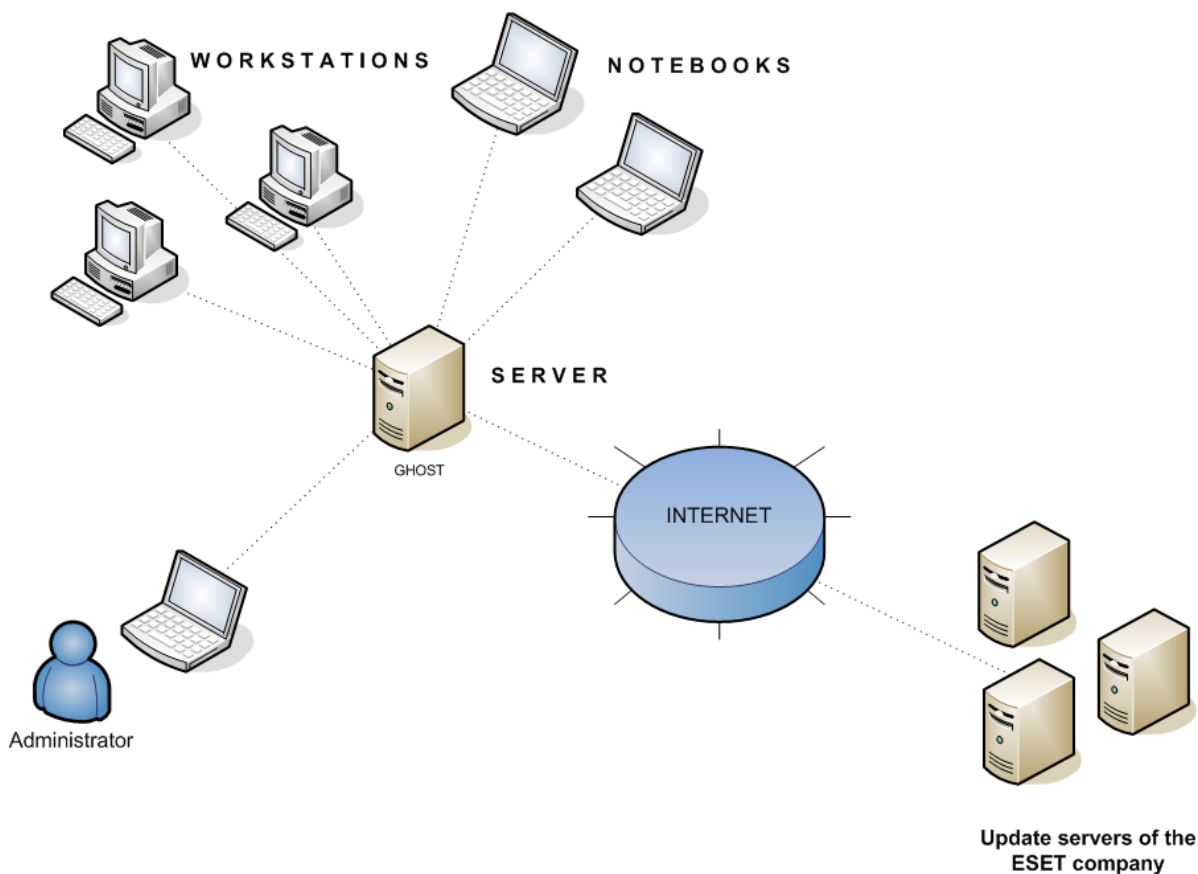


Figure 2-1

2.2.2 Before installation

Before installing, the following installation packages should be downloaded from ESET's website:

ESET Remote Administrator components:

ESET Remote Administrator – Server
ESET Remote Administrator – Console

ESET client solutions:

ESET Smart Security 4.0
ESET Smart Security 3.0
ESET NOD32 Antivirus 4.0
ESET NOD32 Antivirus 3.0
ESET NOD32 Antivirus 2.7

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

2.2.3 Installation

2.2.3.1 Installation of ERA Server

Install ERAS on the server named GHOST. You can select either Typical or Advanced installation mode.

If you select Typical mode, the program will prompt you to insert a license key – a file with the extension .lic that provides operation of ERAS for the period defined in the license. Next, the program will ask you to set update parameters (username, password and update server). However, you can proceed to the next step, and enter the update parameters later.

If you select the Advanced installation mode, the installer will offer additional parameters to be set. These parameters can be modified later via ERAC, but in most cases this is not necessary. The only exception is server name, which should be equivalent to the DNS name, or %COMPUTERNAME % value of your operating system or the IP address assigned to the computer. This is the most essential piece of information for performing remote installation. If a name is not specified during installation, the installer will automatically supply the value of the system variable %COMPUTERNAME %, which is sufficient in most cases.

It is also important to select the correct database to which ERAS information will be stored. For more information, please see section 2.2.3.4 “Database types supported by ERA Server”.

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

%ProgramFiles %\ESET\ESET Remote Administrator\Server

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

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

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

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

2.2.3.2 Installation of ERA Console

Install the ESET Remote Administrator Console to the administrator's PC/notebook (as shown at the bottom left of Figure 2–1). At the end of the Advanced installation mode enter the name of the ERA Server (or its IP address) to which ERAC will automatically connect at startup. It is labeled GHOST in our example.

After installation launch ERAC and check the connection to ERAS. By default, no password is required to connect to an ERA Server (the password text field is blank), but we strongly recommend that one be established. To create a password to connect to an ERA Server:

Click **File > Change Password...** and then modify the Password for Console by clicking the **Change...** button.

The administrator can specify a password for Administrator Access and for Read-Only Access (which only allows viewing of ERAS configuration).

2.2.3.3 How to enable and configure the Mirror

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

Proceed as follows:

1. Connect the ERA Console to the ERA Server by clicking **File > Connect**.
2. From the ERA Console click **Tools > Server Options...** and click the **Updates** tab.
3. From the **Update server** drop-down menu, select **Choose Automatically**, leave Update interval at 60 minutes. Insert **Update username** (EAV-****) and then click **Set Password...** and type or paste the password you received with your username.
4. Select the **Create update mirror** option. Leave the default path for mirrored files and HTTP server port (2221). Leave **Authentication** at NONE.
5. Click the **Other Settings** tab and click **Edit Advanced Settings...** In the advanced setup tree, navigate to **ERA Server > Setup > Mirror > Create mirror for the selected program components**. Click **Edit** on the right-hand side and select the program components to be downloaded. Components for all language versions that will be used in the network should be selected.
6. In the **Updates** tab, click **Update now** to create the Mirror.

For more detailed Mirror configuration options, please see section 7.3.3, "How to enable and configure the Mirror".

2.2.3.4 Database types supported by ERA Server

By default, the program uses the Microsoft Access (Jet Database) engine. ERAS 3.0 also supports the following databases:

- Microsoft SQL Server
- MySQL (version 4.1 and later)
- Oracle

The database type can be selected during the Advanced installation mode of ERAS. After the installation it is not possible to change the database version.

2.2.3.4.1 Basic requirements

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

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

Collation Settings

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

To activate:

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

Character set

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

2.2.3.4.2 Database connection setup

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

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

Example of a DSN connection:

DSN =ERASqlServer

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

This is an example of a complete connection string for MS SQL Server:

Driver={SQL Server}; Server=hostname; Database=ESETRADB

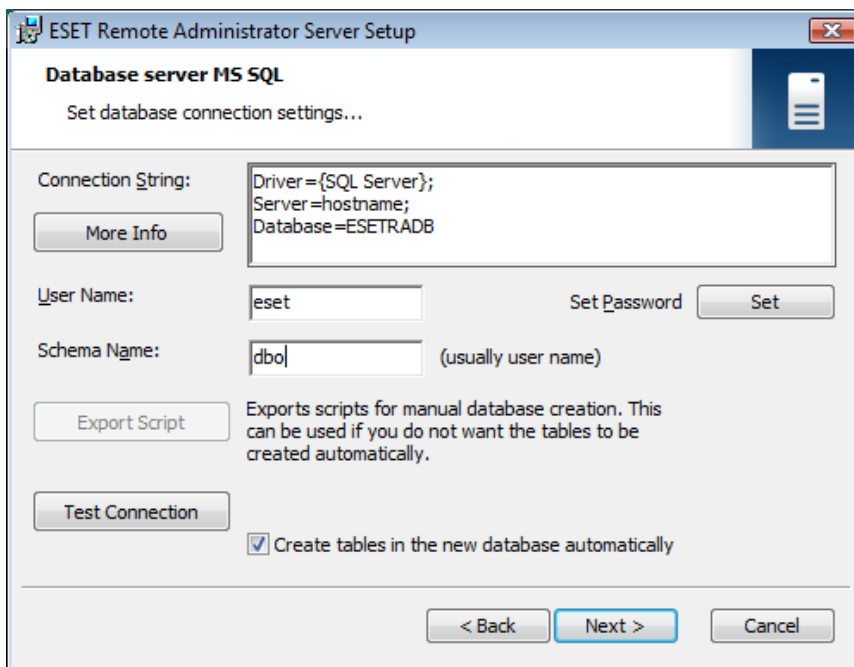


Figure 2-2

This is an example of a complete connection string for Oracle Server:

Driver={Oracle in instantclient10_1}; dbq=hostname:1521/ESETRADB

This is an example of a complete connection string for MySQL Server:

Driver={MySQL ODBC 3.51 Driver}; Server=hostname; Database=ESETRADB

Then set the **Username** and password for the connection (the **Set** button). Oracle and MS SQL Server databases also require a **Schema Name** (for MS SQL Server this is usually the same as username). Click **Test Connection** to verify the connection to the database server.

2.2.3.4.3 Installing over an existing database

If there are existing tables in the database, the installer will display a notification. To overwrite contents of an existing table, select **Overwrite** (Warning: this command deletes the contents of tables and also overwrites their structure!). Select **Ignore** to leave tables untouched.

NOTE: Selecting *Ignore* may under certain conditions cause database inconsistency errors; especially when tables are damaged or incompatible with the current version.

To cancel installation of ERAS and analyze the database manually, click **Cancel**.

2.2.3.5 Remote install to client workstations 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 website and create an installation package. You can create an XML configuration file that will automatically be applied when the package runs.

More information about remote installation can be found in chapter 4, "Installation of ESET client solutions".

2.2.3.6 Remote install on notebooks currently not present in the network

Notebooks which are outside the local network require a different type of remote installation, since installation must be performed after they logon to the domain. For these devices, the logon script method is suggested.

More information about logon script remote install can be found in chapter 4, "Installation of ESET client solutions".

2.3 Scenario – Installation in an Enterprise environment

2.3.1 Environment overview (network structure)

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

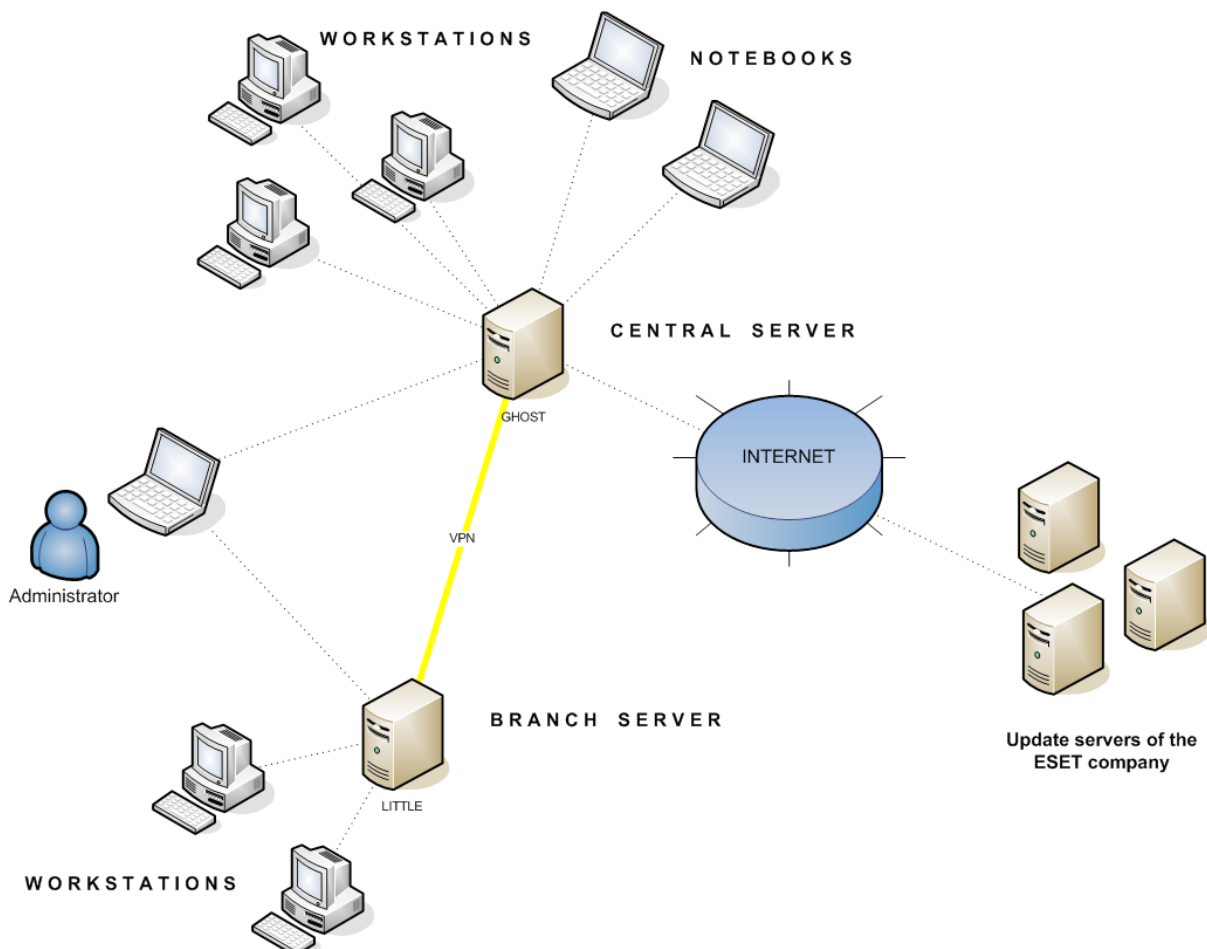


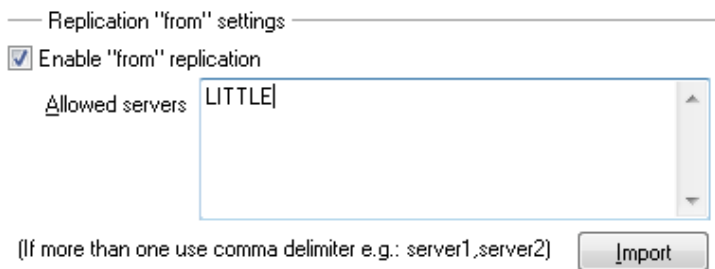
Figure 2-3

2.3.3 Installation

2.3.3.1 Installation at headquarters

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

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



— Replication "from" settings —

☒ Enable "from" replication

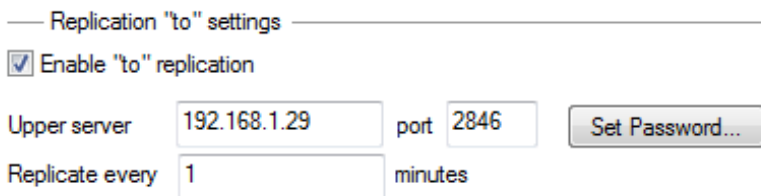
Allowed servers: LITTLE

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

Figure 2-4

2.3.3.2 Branch office: Installation of ERA Server

As in the example directly above, install the second ERAS and ERAC. Again, enable and configure the replication settings. This time select the **Enable "to" replication** check box (**Tools > Server Options... > Replication**) and define the name of the master ERAS. We recommend using the IP address of the master server¹, which is the IP address of the server GHOST.



— Replication "to" settings —

☒ Enable "to" replication

Upper server: 192.168.1.29 port: 2846

Replicate every: 1 minutes

Figure 2-5

2.3.3.3 Branch office: Installation of HTTP Mirror server

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

As seen in Figure 2–3, updates for the branch office are not downloaded from ESET's update servers, but from the server at the headquarters (GHOST). The update source is defined by the following URL address:

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

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

For more information on configuring the Mirror in ERAS, see section 7.3, "Mirror Server".

¹ In order to avoid potential DNS translation problems when converting names to IP addresses between networks (depending on the DNS configuration).

2.3.3.4. Branch office: Remote installation to clients

Once more, the previous model can be used, except that it is suitable to perform all operations with ERAC connected directly to the ERAS of the branch office (LITTLE)².

2.3.4 Other requirements for Enterprise environments

In larger networks, multiple ERA Servers can be installed to perform remote installs of client computers from servers which are more accessible. For this purpose, ERAS offers "replication" (see sections 2.3.3.1 and 2.3.3.2), which allows stored information to be forwarded to a parent ERAS ("upper server"). Replication can be configured using ERAC.

The replication feature is very useful for companies with multiple branches or remote offices. The model deployment scenario would be as follows: Install ERAS in each office and have each replicate to a central ERAS. The advantage of this configuration is especially apparent in private networks which are connected via VPN, which is usually slower – the administrator will only need to connect to a central ERAS (the communication marked by the letter A in the Figure 2.6). There is no need to use VPN to access individual departments (the communications B, C, D and E). The slower communication channel is bypassed through the use of ERAS replication.

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

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

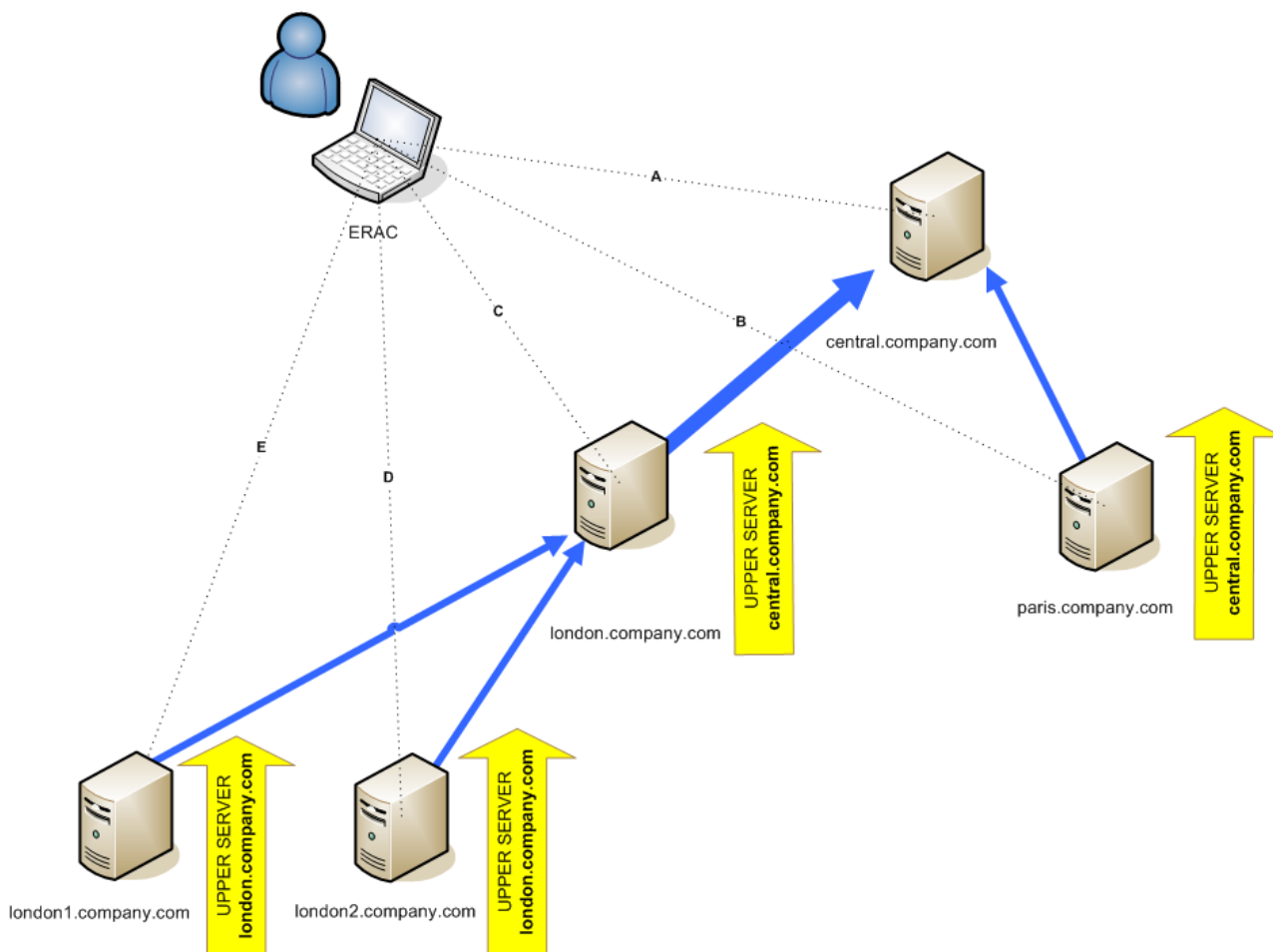


Figure 2-6

² This is done to prevent install packages from being transferred via the VPN channel, which is slower

3. Working with ERAC

3.1 Connecting to ERAS

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

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

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

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, no password is required to connect to an ERAS, but we strongly recommend that one be established. To create a password to connect to an ERAS:

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...**

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

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

On program startup, select the **Access Type** from the **Access** drop-down menu (either **Administrator** or **Read-Only**).

3.2 ERAC – main window

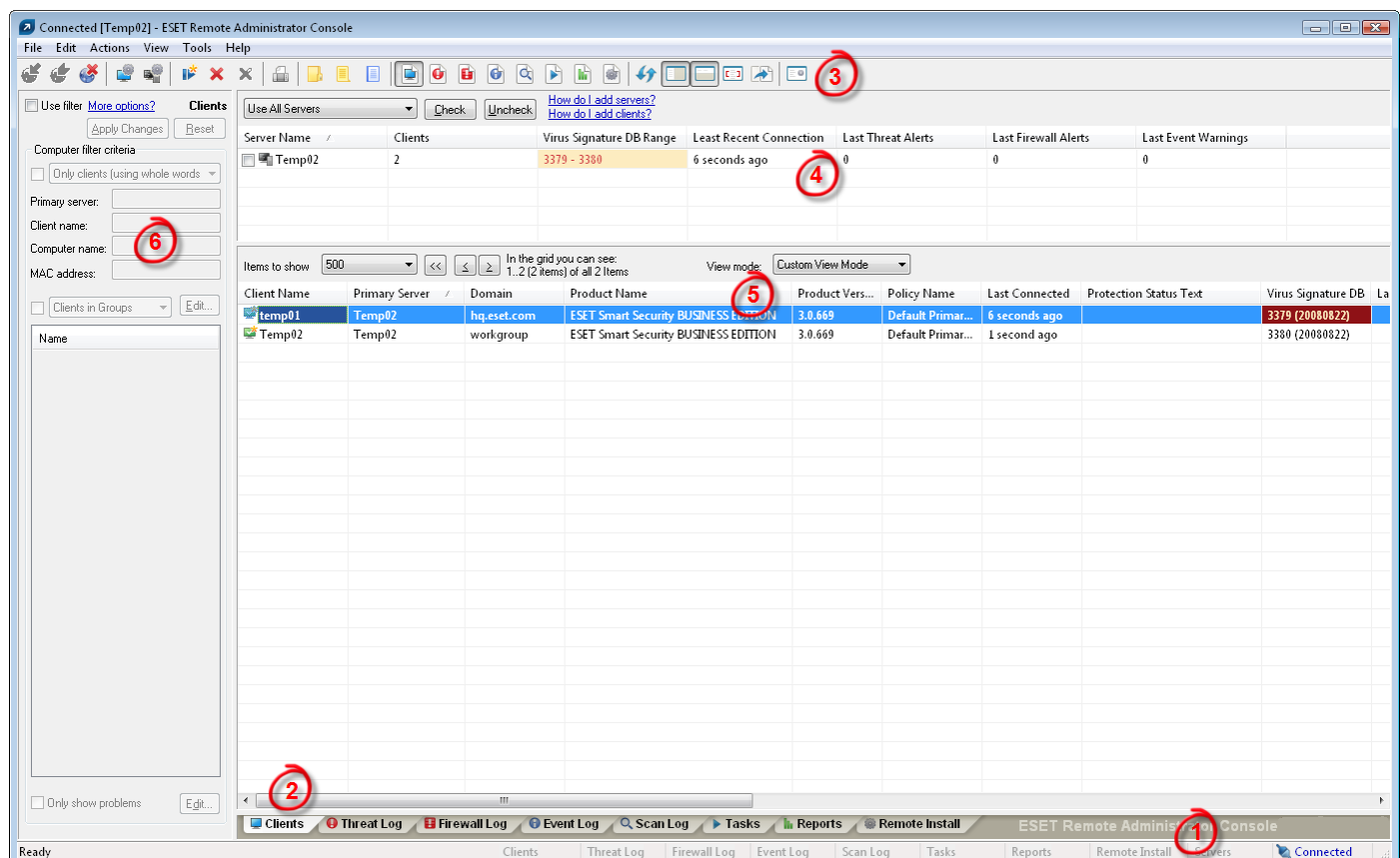


Figure 3-1 ESET Remote Administrator Console main window

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

NOTE: Press F5 to refresh displayed data.

Information is divided into several tabs in order of importance (2). In most cases data can be sorted in ascending or in descending order by clicking on an attribute (5), while a drag-and-drop operation can be used for reorganization. If multiple data rows are to be processed, you can limit them by using the **Items to show** drop-down menu and the **browse page by page** buttons. Select the View mode to display attributes according to your need (For further details, see section 3.3, "Information filtering").

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

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

Columns in Section 4:

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

If you are not currently connected, you can right-click in the Server section (4) and select **Connect to This Server** to connect to the chosen ERAS.

More information will be displayed in the Server section (4) if replication is enabled.

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

The last section is **Computer filter criteria** (6) – see section 3.3, "Information filtering".

3.3 Information filtering

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

3.3.1 Groups

Individual clients can be divided into groups by clicking **Tools > Groups Editor...** in the ERAC. Groups can later be used when applying filters or creating tasks. Groups are independent for each ERAS and are not replicated. The **Synchronize with Active Directory** feature in the Groups Editor allows the administrator to sort clients to groups, as long as the client name equals the object type "computer" at the side of Active Directory (AD) and belongs to groups in the AD.

NOTE: In order for ERAS to synchronize with Active Directory, it is not required that ERAS be installed on your Domain Controller. The Domain Controller must only be accessible from the computer where your ERAS is located. To configure authentication to your Domain Controller, go to **Tools > Server Options > Other Settings > Edit Advanced Options > ESET Remote Administrator > ERA Server > Settings > Active directory**. The format of the server name is LDAP://servername or GC://servername. When empty, global catalog (GC) is used.

For more information on group management and synching with AD at the organizational unit level (i.e., Support Dept., Marketing Dept., etc.), see section 5.2, "Groups".

3.3.2 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 ERAC and click the **Apply Changes** button. Any future modifications 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 define the filtering criteria (**Primary server, Client name, Computer name, MAC address**).

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

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

The Primary server, Client name, Computer 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 field; the logical operator AND is used.

The next section allows filtering of clients by groups:

- **Clients in Groups**
Only displays clients belonging to the specified group(s).
- **Clients in other Groups or N/A**
Output will only include 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**
Only displays clients which are not a part of any group.

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

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

3.3.3 Context menu

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

- **Select All**
Selects all entries.
- **Select by '...'**
This option allows you to right-click on any attribute, and automatically select (highlight) all other workstations or servers with the same attribute. The string ... is automatically replaced by the value of the current tab.

- **Inverse Selection**
Performs inverted selection of entries.
- **Hide Selected**
Hides selected entries.
- **Hide Unselected**
Hides all unselected entries in the list.

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

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

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

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. The **Full View Mode** displays all columns, while the **Minimal View Mode** only shows the most important columns. These modes are predefined and cannot be modified. To activate the Custom View, select **Custom View Mode**. It can be configured in the **Tools > Console Options... > Columns > Show/Hide** tab.

3.4 Tabs in ERAC

3.4.1 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 Server³

The behavior of ERAS related to certain network operations (such as renaming a PC) can be defined in ERAS Advanced Setup. It can help prevent duplicate entries in the **Clients** tab. For example, if one of the computers in the network has been renamed, but its MAC address remained unchanged, you can avoid creating a new entry in the **Clients** tab.

Clients that connect to ERAS for the first time are designated by a **Yes** value in the **New User** column. They are also marked by a small asterisk in the upper right corner of the client's icon (see Figure 3-2). 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.



Figure 3-2

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 **Set/Reset Flags > Reset "New" Flag**. The icon of the client will change to the one shown in Figure 3-3, and the attribute **New User** will change to **No**.

³ In previous versions of ERA, clients were identified by the following attributes: Computer Name + Primary Server



Figure 3-3

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

Time values in ERAS can be displayed either in the relative mode ("2 days ago"), in the absolute mode (20. 5. 2008) or in the system mode (Regional settings).

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

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.

3.4.2 Replication & information in individual tabs

If ERAC 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**)

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

In dialog windows where such information should otherwise be present, the **Request** button is available (**Actions > Properties > Configuration**). Clicking this button downloads missing information from a lower ERAS. Since replication is always initiated by a lower ERAS, the missing information should be delivered within the preset replication interval.

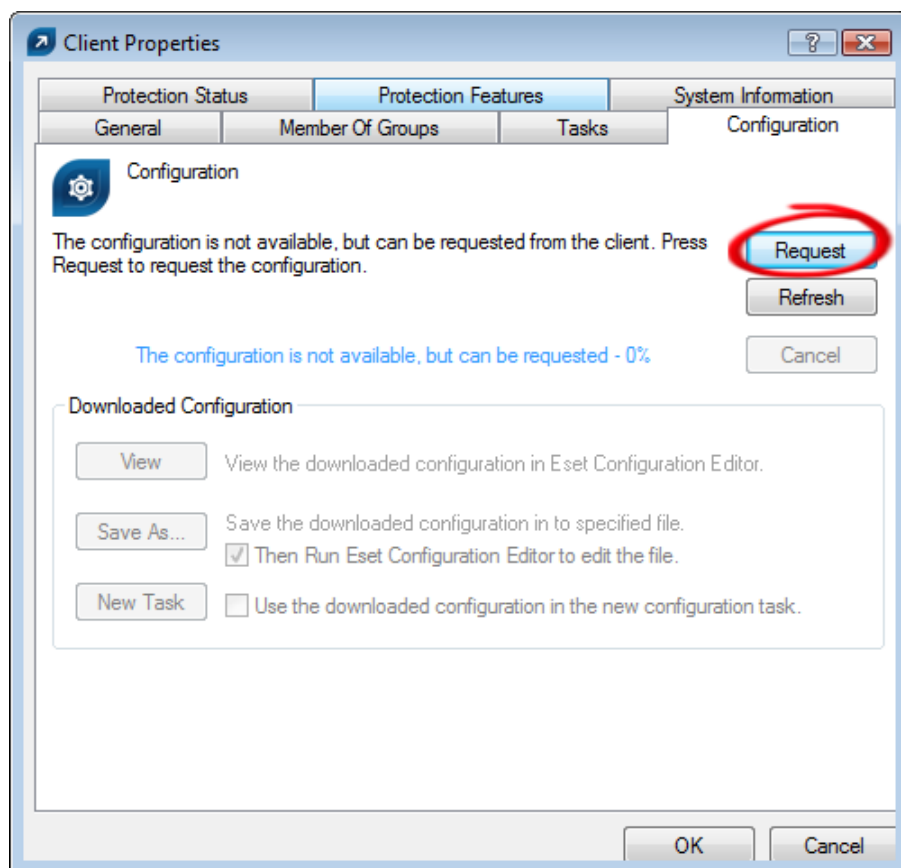


Figure 3-4 Click Request to retrieve missing information from lower ERA Servers.

3.4.3 Clients tab

This tab displays general information about individual clients.

Attribute	Description
Computer Name	Name of workstation / server (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of ERAS with which a client is communicating
Domain	Domain / group name, to which a client belongs (these are not groups created in ERAS)
IP	IP address
Product Name	Name of ESET security product
Product Version	Version of ESET security product
Policy Name	Name of policy assigned to a client
Last Connected	Time that client last connected to ERAS (All other data collected from clients includes this timestamp, except for some data obtained by replication)
Protection Status Text	Current status of the ESET security product installed on a client
Virus Signature DB	Version of virus signature database
Last Threat Alert	Last virus incident
Last Firewall Alert	Last event detected by the ESET Smart Security Personal firewall (Events from the Warning level and higher are shown)
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 last On-demand scan
Restart Request	Is a restart required (e.g., after a program upgrade)
Restart Request Date	Time of first restart request
Product Last Started	Time that client program was last launched
Product Install Date	Date that the ESET security product was installed on the client
Mobile User	Clients with this attribute will perform the task "update now" task each time they establish a connection with the ERAS (recommended for notebooks)
New Client	Newly connected computer (see section 3.4.1, "General description of tabs and clients")
OS Name	Name of client operating system

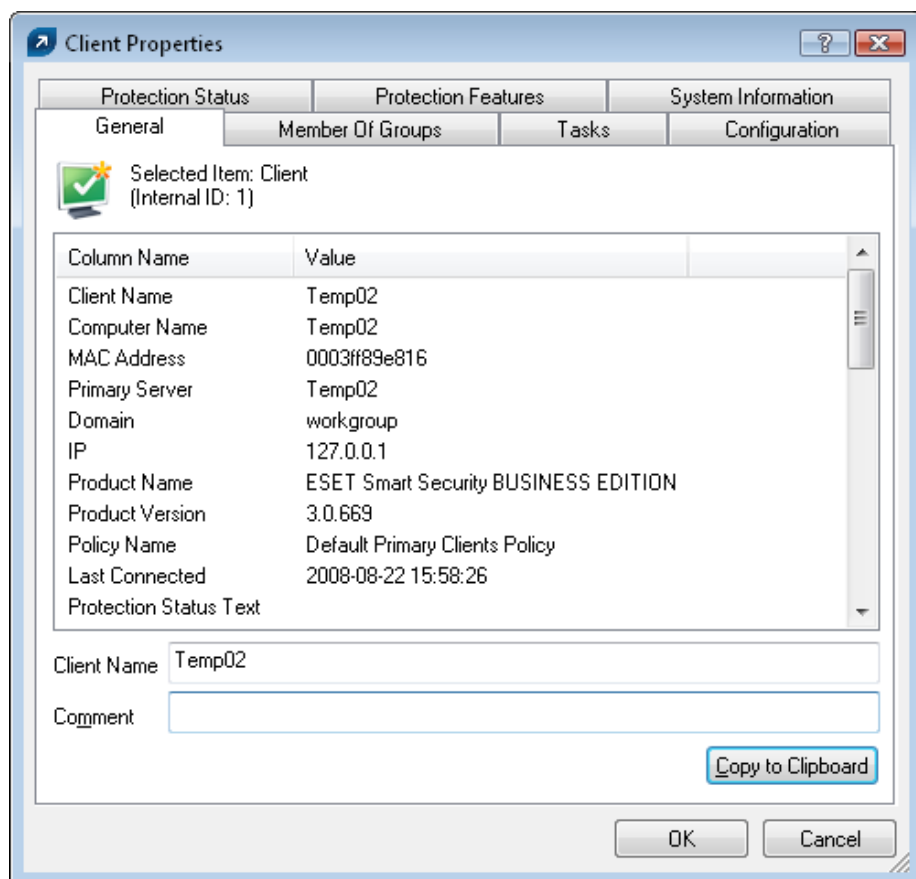


Figure 3-6 Detailed information about a client workstation.

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

- **General**

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**

This tab lists all groups to which the client belongs. For more information, see section 3.3, "Information filtering".

- **Tasks**

Tasks related to the given client. For more information see section 5.1, "Tasks".

- **Configuration**

This tab allows you to view or export the current client configuration to an.xml file. Later in this manual, we will explain how.xml files can be used to create a configuration template for new/modified.xml configuration files. For more information see section 5.1, "Tasks".

- **Protection Status**

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 a new task to solve a given protection problem.

- **Protection Features**

Component status for all ESET security features (Antispam, Personal firewall, etc.)

- **System Information**

Detailed information about the installed program, its program component version, etc.

- **SysInspector** tab

Detailed information about startup processes and processes running in the background.

3.4.4 Threat Log tab

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

Attribute	Description
Client Name	Name of client reporting the threat alert
Computer Name	Workstation/server name (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of ERAS with which a client is communicating
Date Received	Time at which the event was logged by ERAS
Date Occurred	Time at which the event occurred
Level	Alert level
Scanner	Name of security feature which detected the threat
Object	Object type
Name	Usually a folder where the infiltration is located
Threat	Name of the detected malicious code
Action	Action taken by the given security feature
User	Name of the user that was identified when the incident occurred
Information	Information about the detected threat
Details	Client log submission status

3.4.5 Firewall Log Tab

This tab displays information related to client firewall activity.

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

3.4.6 Event Log tab

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

Attribute	Description
Client Name	Name of client reporting the event
Computer Name	Name of workstation / server (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of ERAS with which a client is communicating

Date Received	Time at which the event was logged by ERAS
Date Occurred	Time at which the event occurred
Level	Alert level
Plugin	Name of the program component reporting the event
Event	Description of the event
User	Name of the user associated with the event

3.4.7 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
Client Name	Name of client where the scan was performed
Computer Name	Name of workstation / server (hostname)
MAC Address	MAC address (network adapter)
Primary Server	Name of ERAS with which a client is communicating
Date Received	Time at which the scan event was logged by ERAS
Date Occurred	Time at which the scan took place on client
Scanned Targets	Scanned files, folders and devices
Scanned	Number of checked files
Infected	Number of infected files
Cleaned	Number of cleaned (or deleted) objects
Status	Status of the scan
User	Name of the user that was identified when the incident occurred
Type	User type
Scanner	Scanner type
Details	Client log submission status

3.4.8 Tasks tab

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

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

3.4.9 Reports tab

This tab contains features which can be used to archive the activity in the network over certain time periods. The **Reports** tab is used to organize statistical information in graph or chart form. For more information, see chapter 6, "Reports".

3.4.10 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, see section 4.2, "Remote Installation".

3.5 ERA Console setup

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

3.5.1 Connection tab

This tab is used to configure the connection from ERAC to ERAS. For more detail, see chapter 3, "Working with ERAC".

3.5.2 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 (**Clients** tab). Other modes cannot be modified.

3.5.3 Colors tab

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

3.5.4 Paths tab

This tab allows you to specify the directory to which ERAC will save reports downloaded from ERAS. By default, reports are saved to:

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

3.5.5 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.

3.5.6 Other settings tab

- **Filter settings > Auto apply changes**
If enabled, filters in individual tabs will generate new outputs upon each modification of filter settings. Otherwise, filtering will only take place 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, ERAC displays a notification at program startup.
- **Other settings > Use automatic refresh**
If selected, data in individual tabs is automatically refreshed according to the designated interval.
- **Other settings > Empty console recycle bins at application exit**

Select this option to automatically empty items from the internal ERAC recycle bin after exiting. You can also empty items manually by right-clicking them in the **Reports** tab.

- **Other settings > Show gridlines**

Select this option to separate individual cells in all tabs by gridlines.

- **Other settings > 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). This option has only a visual effect.

- **Other settings > Use systray icon**

ERA Console will be represented by an icon in the Windows notification area.

- **Other settings > Show on taskbar when minimized**

If the ERAC window is minimized, it will be accessible from the Windows task bar.

- **Other settings > Use highlighted systray icon when problematic clients found**

Select 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.

If the ERAC on the administrator's PC is going to be connected at all times to ERAS, we recommend that you deselect the **Show on taskbar when minimized** option 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. However, the ERAC will disconnect if database compression is enabled on the server.

- **Other settings > Show all groups in filter panes**

Changes the group filtration.

- **Other settings > Tutorial messages**

Enables (Enable All) or Disables (Disable All) all informative messages.

3.6 Display modes

ERAC offers the user two display modes:

- Administrative mode
- Read-only mode

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

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

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

3.7 ESET Configuration Editor

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

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

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



The Configuration Editor allows the administrator to remotely configure many of the parameters available in any ESET security product, especially those installed on client workstations. It also allows the administrator to export configurations to .xml files which can later be used for multiple purposes, such as creating tasks in ERAC, importing a configuration locally in ESET 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. That is why we recommend that ERAS and ERAC be updated regularly.

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

For the Configuration Editor to function, the following files must be available: `eguiEpfw.dll`, `cfgeditLang.dll`, `eguiEpfwLang.dll` and `eset.chm`.

3.7.1 Configuration layering

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

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

An example is shown in Figure 3-7. In this configuration the username AV-1234567 and password are inserted and using a proxy server is prohibited.

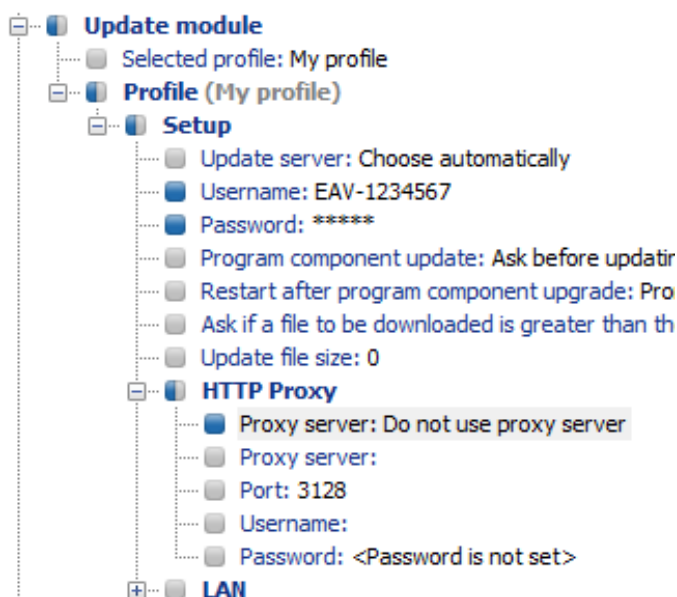


Figure 3-7

The second configuration (Figure 3-8) sent to clients will ensure that previous modifications are preserved, including the username EAV-1234567 and password, but will also allow the use of a proxy server, and defines its address and port.

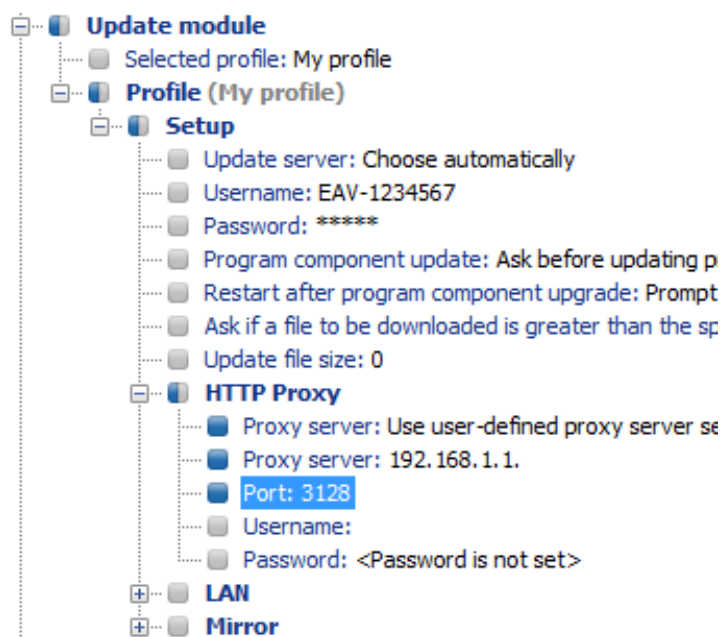


Figure 3-8

3.7.2 Key configuration entries

In this section, we explain several of the key configuration entries for ESET Smart Security and ESET NOD32 Antivirus, available through the ESET Configuration Editor:

- ESET Smart Security, ESET NOD32 Antivirus > ESET Kernel > Setup > Remote administration**
 Here you can enable communication between client computers and the ERAS (**Connect to Remote Administrator server**). Enter the name or IP address of ERAS (**Server address**). The **Interval between connections to server** option should be left at the default value of five minutes. For testing purposes, this value can be decreased to 0, which will establish a connection every ten seconds. If a password is set, use the one which was specified in ERAS. For more information, see the **Password for Clients** option in section 7.1, "Security tab". Additional information on password configuration can also be found in this section.
- ESET Kernel > Setup > License keys**
 Client computers require no license keys to be added or managed. License keys are only used for server products.
- ESET 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 without user interaction, select **Submit without asking** and **Yes**, respectively. If a proxy server is used with the Internet connection, specify the connection parameters under **ESET Kernel > Setup > Proxy server**.
 By default, the client products submit suspicious files to ERAS, which submits them to ESET's servers. Therefore, the proxy server should be correctly configured in ERAS (**Tools > Server Options > Other Settings > Edit Advanced Settings > ERA Server > 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, etc.

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

- **ESET Kernel > Setup > Default user interface values**

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

- **Update**

This branch of the Configuration Editor allows you to define how update profiles are applied. Normally, it is only necessary to modify the predefined profile **My profile** and change the **Update server, Username** and **Password** settings. If Update server is set to **Choose Automatically**, all updates will be downloaded from ESET's update servers. In this case, please specify the **Username** and **Password** parameters which were provided at the time of purchase. For information on setting client workstations to receive updates from a local server (Mirror), please see section 7.3, "Mirror server". For more information on using the scheduler, see 10.1, "Scheduler".

NOTE: On portable devices such as notebooks, two profiles can be configured – one to provide updating from the Mirror server, and the other to download updates directly from ESET's servers. For more information, see section 10.4, "Combined update for notebooks" at the end of this document.

4. Installation of ESET client solutions

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

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

4.1 Direct installation

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

This task can be greatly simplified with the help of a predefined.xml configuration. No further modification, such as defining an update server (username and password, path to a Mirror server, etc.), silent mode, scheduled scan, etc., is required during or after installation.

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

- Version 3.x: Download the installation file (e.g., ess_nt32_enu.msi) from eset.com. Copy the.xml configuration file (cfg.xml) to the directory where the install file is located. Upon execution, the installer will automatically adopt the configuration from the.xml configuration file. If the.xml configuration file has a different name or is located somewhere else, the parameter ADMINCFG="path_to_xml_file" can be used (e.g., ess_nt32_enu.msi ADMINCFG="\\server\xml\settings.xml" to apply the configuration stored on a network drive).
- Version 2.x: Download the installation file (e.g., ndntenst.exe) from eset.com. Extract the downloaded file to a folder using a file extraction program such as WinRAR. The folder will contain installation files, including setup.exe. Copy the nod32.xml configuration file to the folder. Run the setup.exe file – the configuration within nod32.xml will be automatically applied. If the.xml configuration file has a different name, or 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).

4.2 Remote installation

ERA offers several methods of remote installation. Distribution of installation packages to target workstations can be performed using the following methods:

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

Remote installation by means of ERA 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 ERAC, but the install package itself is located in ERAS, in the following directory:

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

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

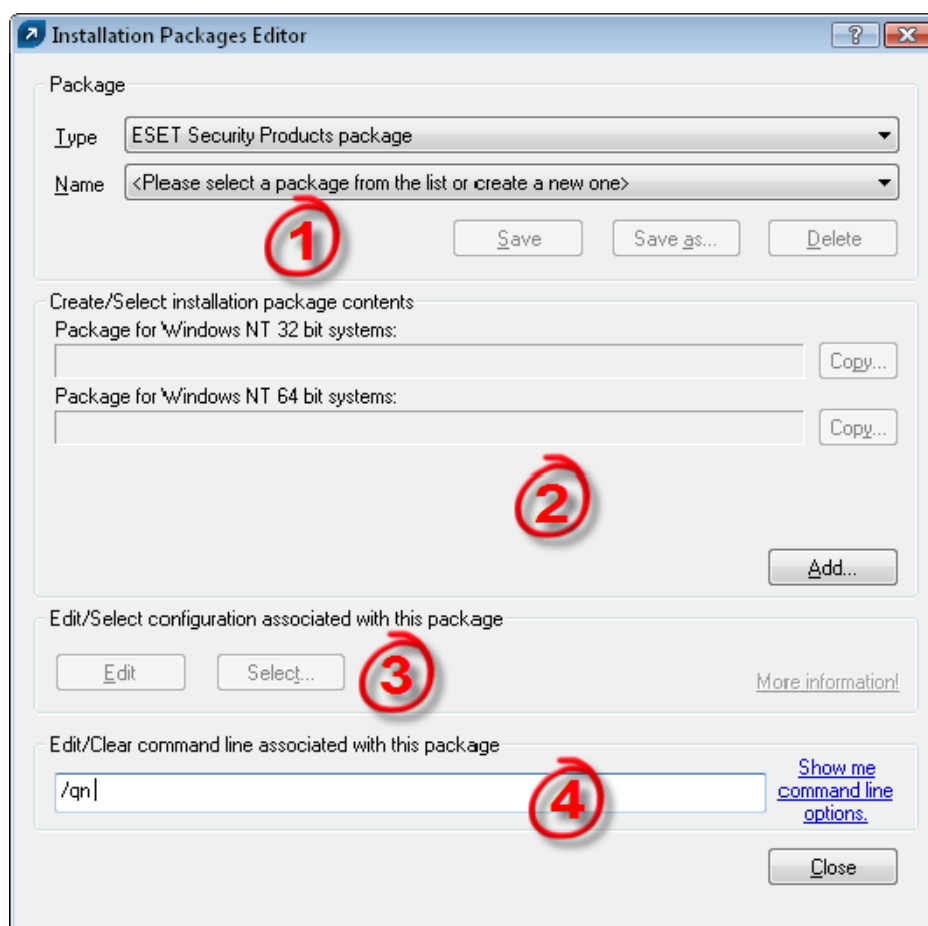


Figure 4-1 Dialog window of the Installation Packages Editor

Each installation package is defined by a Name. See (1) in Figure 4–1 above. The remaining sections of the dialog window are related to the content of the package, which is applied after it has been successfully delivered to a target workstation. Each package contains:

- ESET client solution installation files (2)
- xml configuration file for ESET client solutions (3)
- Command line parameters assigned to the package (4)

The **Type** drop-down menu in section (1) provides access to additional ERA features. In addition to remote installation, ESET security products can be uninstalled remotely using the **Uninstall ESET Security Products and NOD32 version 2** option. Remote installation of an external application can also be performed by selecting **Custom package**.

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 ERAS name, and the name and type of package to which it belongs. The following chapters provide a detailed description of the agent.

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., `eav_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 in %.

- **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 security products. The parameter is not required for remote installation. Installation packages contain their own.xml configuration, which is applied automatically.
- **PASSWORD = "password"**
You need to add this parameter when the ESS/EAV settings are password protected.

Parameters for ESET NOD32 Antivirus 2.x should be typed after the *setup.exe* filename, 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 install an older version over an installed newer version.
- **/CFG = "path_to_xml_file"**
During installation, parameters defined in the specified.xml files are applied to ESET client solutions. The parameter is not required for remote installation. Installation packages contain their own.xml configuration which is applied automatically.
- **/REBOOT**
Automatically reboots after installation.
- **/SHOWRESTART**
After the installation, a dialog window prompting the user to confirm rebooting is displayed. This parameter can only be used if combined with the *SILENTMODE* parameter.
- **/INSTMFC**
Installs MFC libraries for the Microsoft Windows 9x operating system that are required for ERA to function correctly. This parameter can always be used, even if the MFC libraries are available.

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

4.2.1 Requirements

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

- Microsoft network client enabled
- File and printer sharing service enabled
- The file sharing ports (445, 135 – 139) are accessible
- TCP/IP protocol
- Administrative share ADMIN\$ enabled
- Client can respond to PING requests
- Connectivity of ERAS and ERAC (ports 2221–2224 are accessible)
- Administrator username and password exists for client workstations (username cannot be left blank)

- Simple file sharing disabled
- Server service enabled
- Remote Registry service enabled

We highly recommend that you check all requirements before installation, especially if there are multiple workstations in the network (on the **Remote Install** tab, click **Install... > Diagnostics**).

4.2.2 Configuring the environment for remote installation

Before installing ESET security products to network computers, the administrator should appropriately prepare the environment to avoid installation failures.

For example, using the integrated Find tool, you can browse your network and find unregistered client workstations. Unregistered computers are those which are not connected to ERAS.

From the **Remote Install** tab click **Find** to browse the network. Unprotected computers are displayed on the right hand side of the window. On computers that are found and displayed in the list, you can test conditions for the operations **Push Installation**, **Copy**, and **Export**. The **Find from server** option specifies whether unprotected computers are browsed from ERAS or ERAC. We recommend that you select this option if you are connecting to an ERA Server which is located in a different network.

After you have found workstations suitable for installation of a client solution, use the *Remote Install Diagnostics* tool.

Navigate to the **Remote Install** tab and click the **Install...** button. Click **Diagnostics...** to display the **Remote Install Diagnostics** window to check installation requirements and identify potential problems.

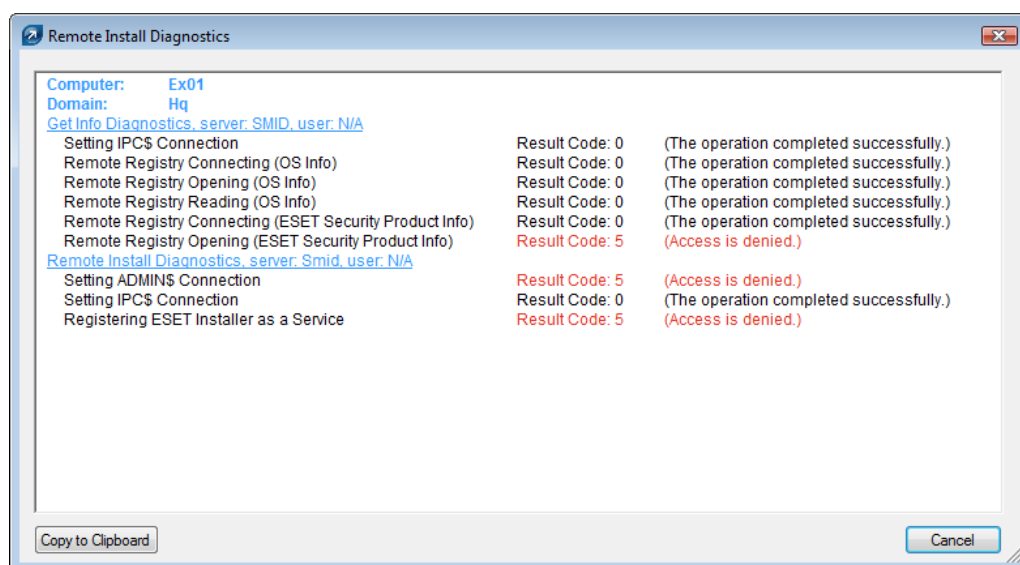


Figure 4-2 The diagnostics tool can detect potential problems before installation

The first part of the **Get Info Diagnostics** section shows information about the ESET security product installed on the computer. The second section indicates whether all installation conditions for the ESET security product have been met.

4.2.3 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 section 4.2.1, "Requirements").

To initiate a push installation, follow the steps below:

- 1) Click the **Install...** button in ERAC (**Remote Install** tab). 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). You can also use the **Add Client...** button to add the remote computer manually.

2) From the **Package** drop-down menu, select the desired install package to deliver to target workstations.

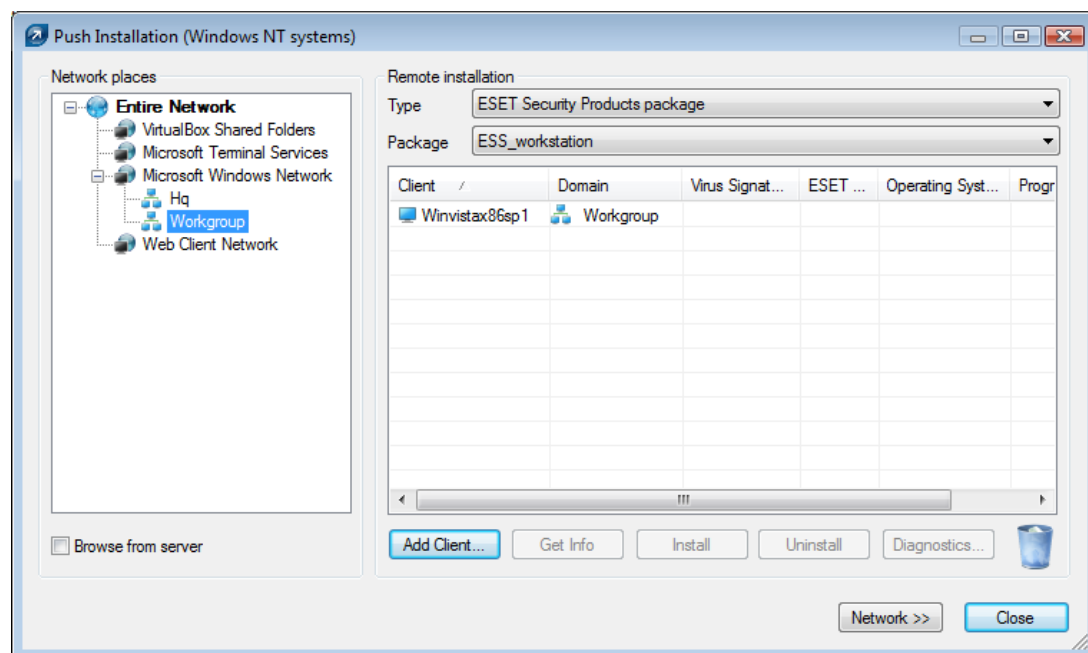


Figure 4-3

3) In the panel on the right, select the workstations that require the package.

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

5) In most cases, you will be prompted to enter the username and password of the account used to access the target workstation (it must be an account with administrator rights).

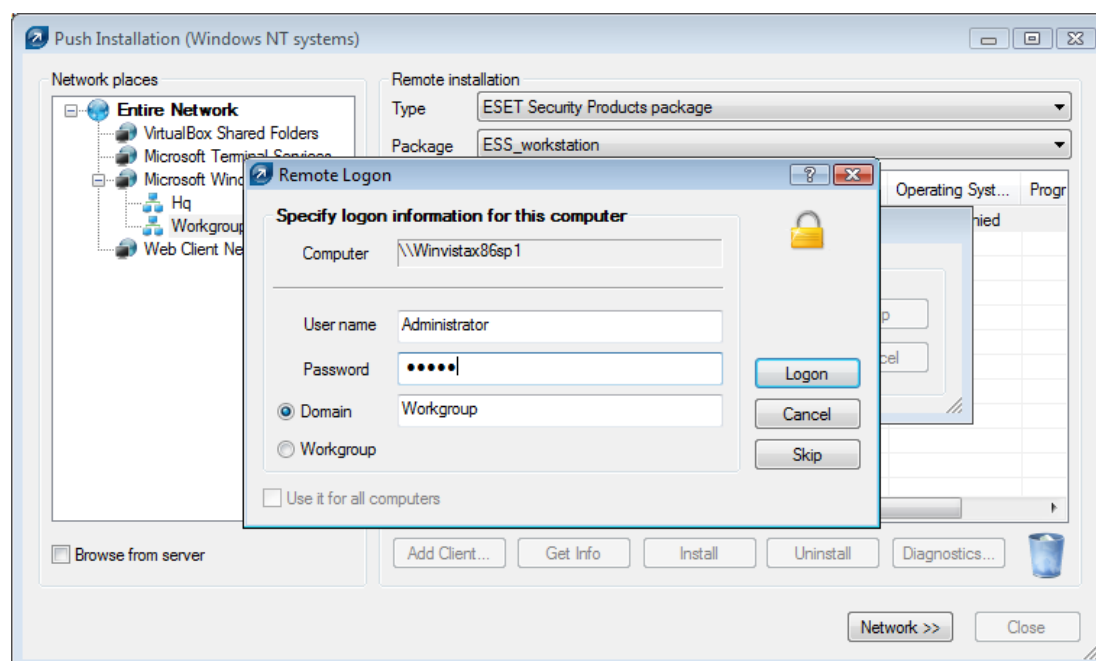


Figure 4-4

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

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

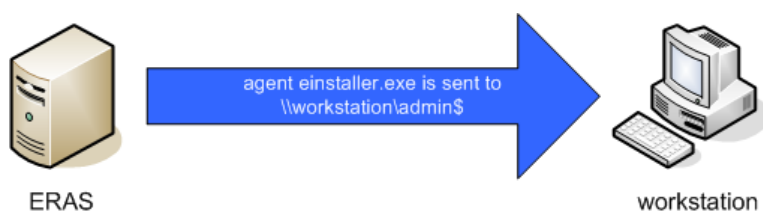
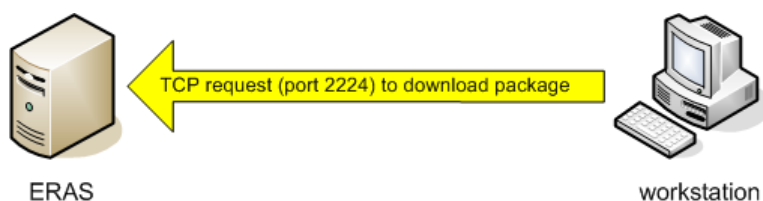


Figure 4-5

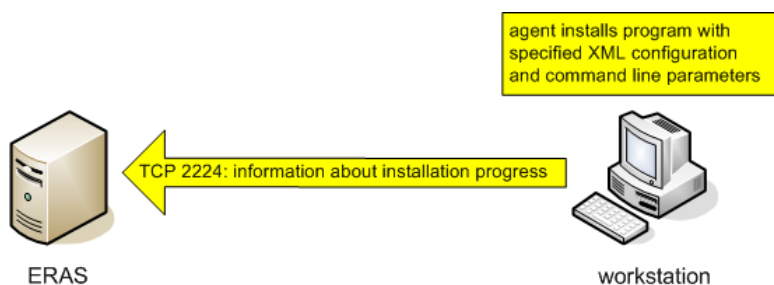
7) Agent starts as a service under the system account.



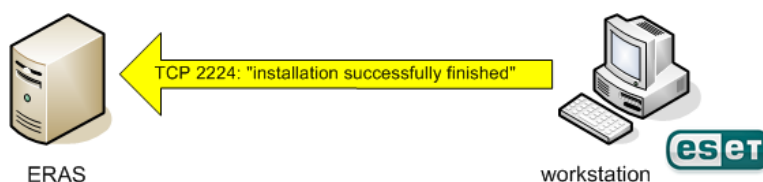
8) Agent establishes communication with its "parent" ERAS and downloads the corresponding install package on TCP port 2224.



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



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



The context menu (right-click) of the **Push Installation** dialog window offers these options:

- **Get Info**
This feature detects the current status of the ESET security product on selected workstations (requires Administrator username and password). This feature uses the admin\$ share.
- **Uninstall**
Program removal – the agent tries to remotely uninstall the ESET security product. The **Uninstall** option does not take into consideration which package is selected from the **Package** menu.
- **Diagnostics**
Checks the availability of clients and services to be used during the remote install. For more information, see section 4.2.2, "Configuring the environment for remote installation".
- **Remove Installer Leftovers**
Unregisters agents (einstaller.exe) from the service manager on client workstations 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 4.2.6, "Avoiding repeated installations").
- **Logon...**
Opens a dialog window for specifying the administrator username and password, which is otherwise displayed automatically (step 5 on page 32). This feature forces a logon to selected workstations.
- **Logoff**
Terminates logon session for selected workstations.
- **Add Client...**
Adds individual client workstations to the list. Enter the IP address or the name of the client. Additional clients can be added simultaneously.

4.2.4 Logon /email remote install

The logon and email remote install methods are very similar. They only vary in the way that the einstaller.exe agent is delivered to client workstations. ERA allows the agent to run via logon script or via email. The einstaller.exe agent can also be used individually and run via other methods (for more information, see section 4.2.5, "Custom remote install").

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 client solutions. For more information, see section 4.2.6, "Avoiding repeated installations".

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.

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

Enter the path to einstaller.exe in the logon script:

- 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 the einstaller.exe file 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 and modify the mask if necessary (**Files**).
- In the **Files** 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 by clicking **Edit >>** and saved by clicking the **Save** button.

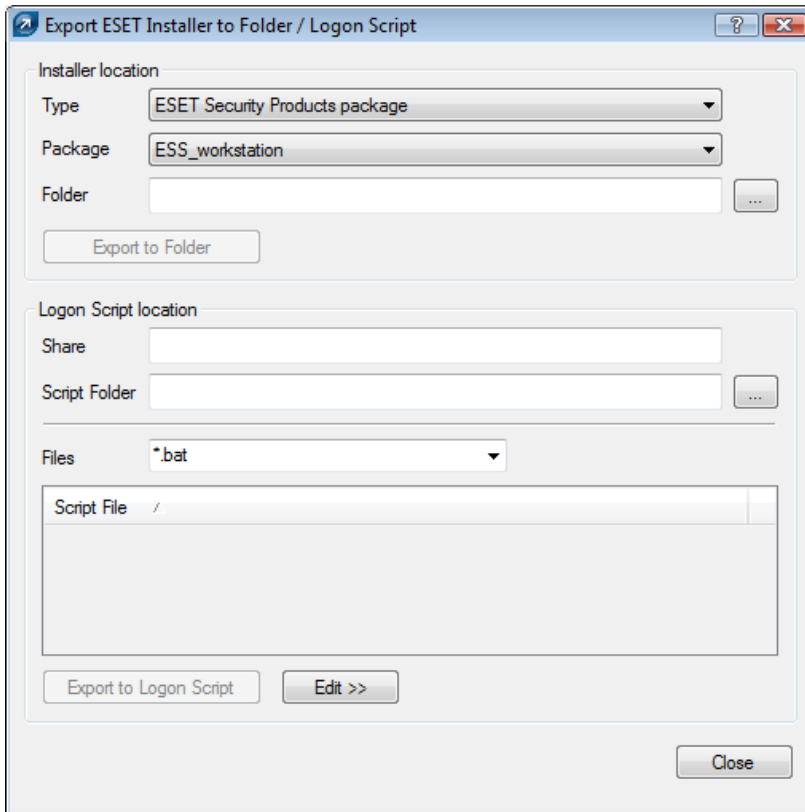


Figure 4-6 Export Installer to Folder / Logon Script dialog window

Attaching the agent (einstaller.exe) to email:

- Click **Email...** on the **Remote Install** tab and select the **Type** and name of the **Package** you wish to install.
- Click **To...** to select addresses from the address book (or insert individual addresses).
- Enter a **Subject** in the corresponding field.
- Type a message into the **Body**.
- Check the **Send compressed as .zip file** option if you wish send the agent .zip-packed.
- Click **Send** to send the message⁴.

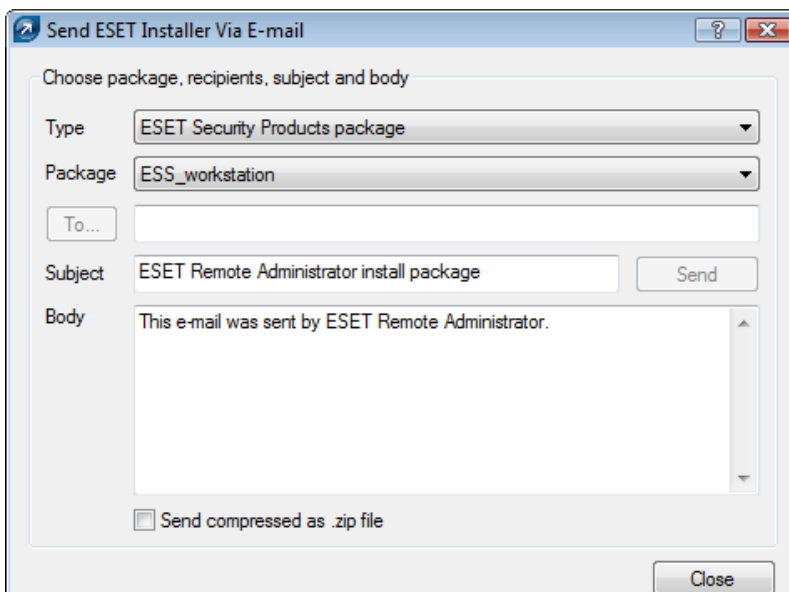


Figure 4-7 Send ESET Installer via Email dialog window

⁴ This feature uses the SMTP parameters defined on ERAS.

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

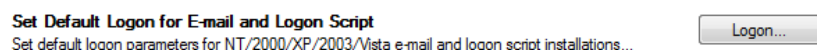


Figure 4.8

Click **Logon...** to specify the username 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.

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

4.2.5 Custom remote install

It is not a requirement to use ERA tools to remotely install ESET client solutions. In the end, the most important aspect is to deliver and execute the einstaller.exe file on client workstations.

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

The einstaller.exe file can be obtained as follows:

- 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 /qn parameter (version 3.x) or the /silentmode parameter (version 2.x). These parameters will run the installation without displaying a user interface.

During the remote installation process, 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.

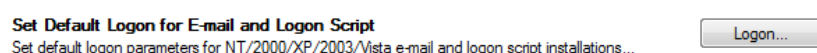


Figure 4-9

Click **Logon...** to specify the username and password of the account under which the package installation is to be performed. It must be an account with administrator rights or, preferably, a 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 new push installation (with a new agent) of the corresponding package (sent via the share *admin\$*)⁵. The new agent then starts downloading the package from ERAS via TCP/IP protocol.

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

⁵ The agent waits for an answer from ERAS (sending the package via the share *admin\$*). In the event that no answer arrives, the agent will attempt to download the install package (via the TCP/IP port 2224). In this case, the administrator username and password specified in Remote Install > Logon.. on the ERAS is not transferred and the agent attempts to install the package under the current user. On the operating systems Microsoft Windows 9x/Me, the administrative share cannot be used, therefore the agent automatically establishes a direct TCP/IP connection to the server.

4.2.6 Avoiding repeated installations

Immediately after the agent successfully completes the remote installation process, it marks the remote client with a flag prohibiting repeated installations of the same 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 einstaller.exe agent matches the data in the registry, no installation is performed. This process prevents repeated installations to target workstations if the einstaller.exe agent is launched repeatedly.

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

ERAS provides an additional level of protection against repeated installations, 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%\einstaller.log:

```
Status 20 001: Eset Installer was told to quit by the server 'X:2224'.
```

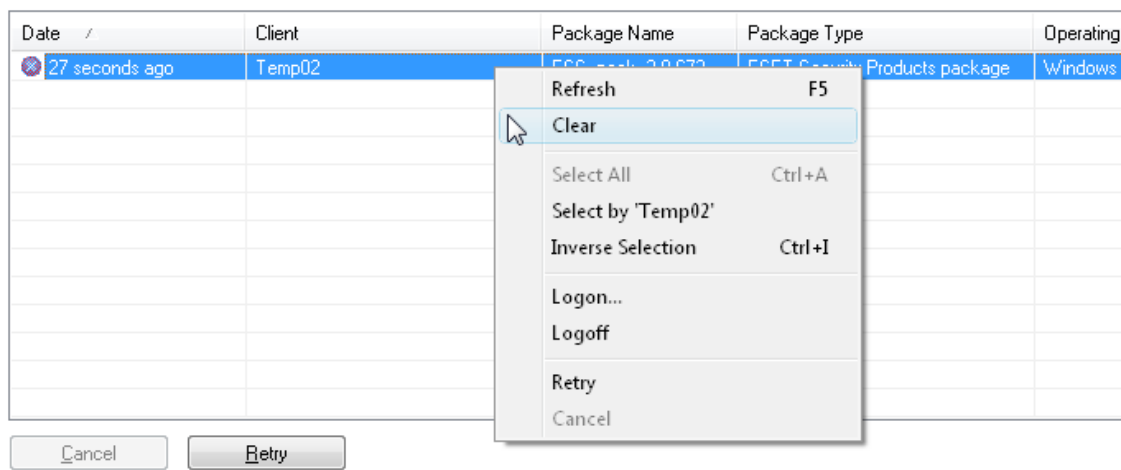


Figure 4-10

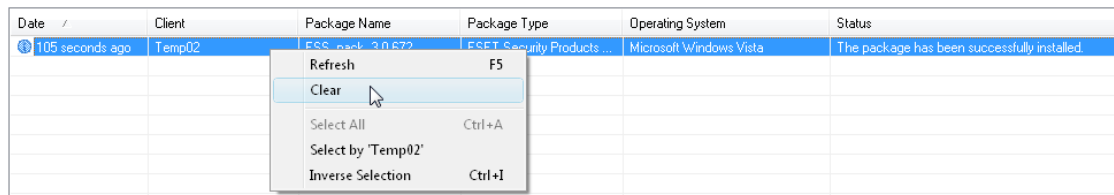


Figure 4.11

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.

4.3 Installation in an Enterprise environment

When deploying programs in large networks, it is important to use a tool capable of performing remote program installations on each and every computer in the network.

Installing through Group Policy

In the Active Directory environment, this task can be elegantly solved by a Group Policy installation. Installation uses the MSI installer, which is distributed directly to all clients connecting to the domain via Group Policy.

To configure a domain controller to automatically install ESET Smart Security or ESET NOD32 Antivirus on each workstation after logging in, proceed as follows:

- 1) Create a shared folder on your domain controller. All workstations should have "read" permission to this folder.
- 2) Copy the ESET Smart Security or ESET NOD32 Antivirus installation package (.msi) to the folder.
- 3) Insert an xml configuration file, which is to be applied to the program, to the same folder. The file should be named cfg.xml. To create a configuration file, the ESET Configuration Editor can be used. For more information see 3.7, "ESET Configuration Editor".
- 4) Click **Start > Programs > Administrative tools > Active Directory Users and Computers**.
- 5) Right-click the domain name and select **Properties > Group Policy > Edit > User Configuration**.
- 6) Right-click **Software Settings** and select **New > Package**.
- 7) In the **Open** window, specify the UNC path to the shared installation package, i.e. `\\computer_name\path\installation_package.msi` and click **Open**. Do not use the **Browse** option to locate the installation package, because it will be displayed as a local network path rather than a UNC network path.
- 8) In the next dialog window select the **Assigned** option. Then click **OK** to close the window.

By following the steps above, the installer package will be installed on each computer that enters the domain. To install the package to computers which are currently up and running, those users should log out and log back in again.

If you wish to give users the ability to accept or deny the installation of the package, select **Publish** instead of **Assigned** in step 8. The next time the user logs in, the package will be added to **Control Panel > Add or Remove programs > Add new program > Add programs from your network**. The package will then be available to users for future installations from that location.

5. Administering client computers

5.1 Tasks

Client workstations that are correctly connected to ERAS and displayed in ERAC can be configured and administered using various types of tasks. Tasks can be applied to multiple clients, or to one or more groups of clients. To apply a task to one or more client workstations, right-click them in the **Clients** pane. Then click **New Task** and select the type of task you wish to perform. Alternatively, the task wizard can be opened from the ERAC main menu by clicking **Actions > New Task**.

The next four sections will outline the individual types of tasks for client workstations, with an accompanying example scenario for each task type.

5.1.1 Configuration Task

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

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

- 1) Right-click any of the selected workstations and select **New Task > Configuration Task** from the context menu.
 - 2) The **Configuration for Clients** window will open, which serves as a configuration task wizard. You can specify the source of the configuration file by clicking **Create...**, **Select...**, or **Create from Template....**
 - 3) Click the **Create** button to open the ESET Configuration Editor and specify the configuration to be applied. Navigate to **ESET Smart Security, ESET NOD32 Antivirus > Update Module > Profile > Setup > Username and Password**.
 - 4) Insert the ESET-supplied username and password and click **Console** on the right to return to the task wizard. The path to the package is displayed in the **Create/Select configuration** field.
 - 5) If you already have a configuration file that contains the desired modifications, click **Select**, find the file and assign it to the configuration task.
 - 6) Alternatively, you can click **Create from Template**, select the .xml file and make changes if needed.
 - 7) To view or edit the configuration file that you have just created or edited, click the **View** or **Edit** buttons.
 - 8) Click **Next** to proceed to the **Selected Clients** window which shows the workstations to which the task will be delivered. In this step, you can add more clients (or groups of clients, or all clients). Click **Add Special** to add clients from selected Servers or Groups. Click **Next** to proceed to the next step.
 - 9) The last dialog window, **Task Report** shows a preview of the configuration task. Enter a name or description for the task (optional). The **Apply task after** option can be used to set the task to run after a specified date/time. The **Delete tasks automatically by cleanup if successfully completed** option deletes all tasks which have been successfully delivered to target workstations.
- Click **Finish** to register the task to run.

5.1.2 On-demand Scan task

The **New Task** context menu option contains two variants of the On-demand scan. The first option is **On-demand scan (cleaning disabled)** – this scan only creates a log, no action is taken on infected files. The second option is **On-demand scan (cleaning enabled)**.

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

- The **Configuration Section** drop-down menu allows you to select the type of ESET product for which the On-demand scan task is being defined. Select those that are installed on target workstations.
- The **Exclude this section from On-demand scan** option disables all settings in the window for the selected product type— they will not be applied on workstations with the product type defined in **Configuration section**. Therefore, all clients with the specified product will be excluded from the list of recipients. If the administrator marks clients as receivers and excludes the product using the above mentioned parameter, then the task will fail with a notification that the task could not be applied. To avoid this, the administrator should always specify clients to which the task will be assigned.
- In **Profile name** you can select a scanning profile to be applied for the task.
- In the **Drives to scan** section, select the types of drives to be scanned on client computers. If the selection is too general, you can add an exact path to objects to be scanned. Use the **Path** field or the **Add Path** button for this purpose. Select **Clear History** to restore the original list of drives to scan.
- Click **Next** to proceed to the dialog windows labeled **Select Clients** and **Task Report** which are identical to the dialog windows in the configuration task wizard (see section 5.1.1, "Configuration Task").

After the task is finished executing on the client workstations, the results are sent back to the ERAS, where they can be viewed in the **Scan Log** pane.

5.1.3 Update Now task

The purpose of this task is to force updates on target workstations (virus signature database updates as well as program component upgrades). Right-click on any workstation from the **Clients** pane and select **New Task > Update Now**. If you wish to exclude certain types of ESET security products from the task, select them in the **Configuration section** drop-down menu and select the **Exclude this section from Update Task** option. To use a specific update profile for the Update Now task, enable the **Select profile name** option and select the desired profile. You can also select **User defined profile name** and enter the profile name; the value of the field will return to default if you click **Clear History**. Then click **Next** to proceed to the dialog windows, **Select Clients** and **Task Report**. For a description of these dialogs, see section 5.1.1, "Configuration Task".

5.1.4 SysInspector Script Task

The SysInspector Script task lets you run the script on target computers. Click **Select** to choose a script to run on the target workstation. Click **View & Edit** to adjust the script. Click **Next** to proceed to the **Select Clients** and **Task Report** dialog windows which are identical to the dialog windows in the Configuration Task wizard. After the task finishes on the client workstation, the information will display in the **State** column of the **Tasks** pane.

5.2 Groups

ERAC offers several tools and features which provide user-friendly administration of clients and events. One of these features is the Groups Editor; it is useful when applying filters or creating tasks, because those activities can be applied to an entire group of clients simultaneously.

Individual clients can be divided into groups using the Group Editor in ERAC. The Group Editor can be accessed from the ERAC main menu by clicking **Tools > Groups Editor**, or by pressing CTRL + G.

The **Groups Editor** window is divided into two parts. On the left, there is a list of existing groups, and on the right, there is a list of clients. The pane on the right displays clients assigned to a group selected on the left. Similarly, all operations represented by buttons at the bottom of this window are performed on currently selected groups or clients.

To create a new group, click **Create** and select a name for the group. We recommend using a name that indicates where the computers are located (e.g., Business Department, Support, etc.). The **Description** field can be used to further describe the group (e.g., "Computers in office C", "HQ workstations", etc.). Newly created and configured groups can also be edited later.

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

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

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

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

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

The last option in the Group Editor is using automatic group creation (with corresponding clients) based on the structure defined by Active Directory. Please note that this option is only available if ERAS is installed on a system with Active Directory. To adopt the Active Directory structure, click **Synchronize with Active Directory**. A client can also be added to a group by right-clicking it in the Clients tab and selecting **Add to Group...**

Warning: *If you use the Full synchronization option, all existing groups will be deleted! Otherwise new groups and clients in groups will be added, while the existing ones will be retained.*

Detailed configuration of Active Directory synchronization can be done using the configuration editor (**ESET Remote Administrator > ERA Server > Settings > Active directory > By Groups/Active Directory Synchronization create**). By default, only **Computer security groups** and **Computer organization units** are synchronized, however, you can add another Active Directory objects by checking the desired option.

5.2.1 Filtering

If too many clients appear in the Clients pane, you can use filtering options. For more information, see section 3.3, "Information filtering".

5.3 Policies

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

5.3.1 Basic principles and operation

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

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

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

5.3.2 How to create policies

The default installation only implements one policy labeled "Server Policy". This name can be changed in the **Policy settings > Policy name field**. The policy itself is configurable from the ESET Configuration Editor – click **Edit** and define parameters for the selected ESET security product (or client). All parameters are organized into a comprehensive

structure and all items in the Editor are assigned an icon. Clients will only adopt active parameters (marked by a blue icon). All inactive (greyed out) parameters will remain unchanged on target computers. The same principle applies to inherited and merged policies – a child policy will adopt only active parameters from a parent policy.

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

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

Override any child policy – Forces all active parameters to inherited policies. If the child policy differs, the merged policy will contain all active parameters from the parent policy (even though the **"Override..."** is active for the child policy). All inactive parameters from the parent policy will adjust to the child policy. If the attribute **Override any child policy** is not enabled, settings in the child policy have priority over those in the parent policy for the resulting merged policy. Such merged policies will be applied to other policies, if they are linked to it as their parent policy.

Down replicable policy – Activates replication to child policies – i.e., it can serve as a default policy for lower servers and can also be assigned to clients connected to lower servers.



Figure 5-1: Example of policy inheritance

5.3.3 Virtual policies

In addition to created policies, as well as those replicated from other servers (see section 7.4. "Replication"), the Policy Tree also contains a Default Parent Policy and Default Primary Clients Policy, which are referred to as virtual policies.

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

The default Primary Clients Policy is located on the given server (not on upper server) in Global Policy Settings and picked up in Default policy for primary clients. It is automatically forced to newly connected clients (primary clients) of the given ERAS, unless they have already adopted some other policy from Policy Rules (for more information, see section 5.3.6, "Assigning policies to clients"). Virtual policies are links to other policies located on the same server.

5.3.4 Policies and structure of ESET Configuration Editor

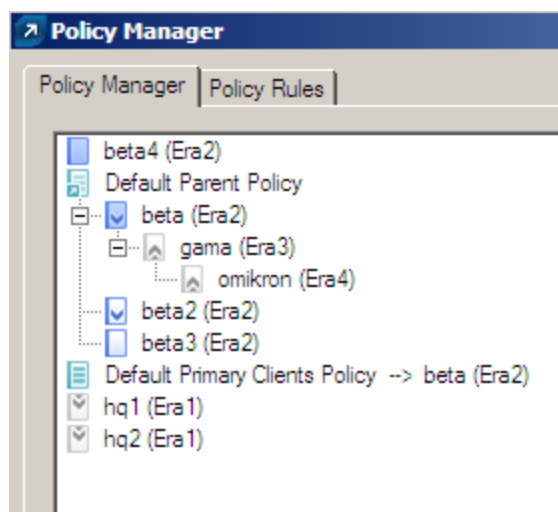






Figure 5-2

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

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


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

 Icons with blue targets – Policy was also created on the server, however, the option **Override any child policy** is selected (for more information, see section 5.3.2, "How to create policies").

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

2) Policies with grey icons originate from other servers.

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

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

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

5.3.5 Viewing policies

Policies in the Policy Tree structure can be viewed directly in the Configuration Editor by clicking **View...** or **View Merged...**

View Merged – Displays the merged policy created as a result of inheritance (the process of inheriting applies settings from the parent policy). This option is displayed by default, because the current policy is already a merged policy.

View – Displays the original policy before it was merged with a parent policy.

On lower servers, the following options are available for policies inherited from upper servers:

View Merged – Same as above

View Override Part – This button applies for policies with the attribute **Override any child policy**. This option only shows the forced part of the policy – i.e. the one which has priority over other settings in child policies.

View Non-force part – Has opposite effect of View Override Part – only displays active items, to which **Override...** is not applied.

5.3.6 Assigning policies to clients

There are two main rules for assigning policies to clients:

- 1) Local (primary) clients can be assigned any local policy or any policy replicated from upper servers.
- 2) Clients replicated from lower servers can be assigned any local policy with the **Down replicable** attribute or any policy replicated from upper servers. They cannot be forced to adopt policies from their own primary server (to do so, you must connect to that server with ERAC).

An important feature is that each client is assigned some policy (there is no such thing as clients with no policy). Also, you cannot take a policy away from a client. You can only replace it with another policy. If you do not want to apply a configuration from any policy to a client, create an empty policy.

5.3.6.1 Default Primary Clients Policy

One method of assigning policies is automatic application of the Default Primary Clients Policy, a virtual policy that is configurable in Global Policy Settings. This policy is applied to primary clients, i.e. those directly connected to that ERAS. For more information see section 5.3.3, "Virtual policies".

5.3.6.2 Manual assigning

There are two ways to manually assign policies: Right-click a client in the Clients pane and select **Add Policy** from the context menu, or click **Add Clients > Add/Remove** in the Policy Manager.

Clicking **Add Clients** in the Policy Manager opens the Add/Remove dialog window. Clients are listed on the left in the format Server/Client. If the Down replicable policy is selected, the window will also list clients replicated from lower servers. Select clients to receive the policy by using the drag-and-drop method or clicking **>>** to move them to Selected items. Newly selected clients will have a yellow asterisk, and can still be removed from Selected items by clicking the **<<** or **C** button. Click **OK** to confirm the selection.

NOTE: After confirming, if you reopen the Add/Remove dialog window, clients cannot be removed from Selected items, you can only replace the policy.

You can also add clients using the **Add Special** feature, which can add all clients at once, add selected clients, or add clients from selected servers or groups.

5.3.6.3 Policy Rules

The **Policy Rules** tool allows an administrator to automatically assign policies to client workstations in a more comprehensive way. Rules are applied immediately after the client connects to the server; they have priority over the **Default Primary Clients Policy** and over manual assigning. The **Default Primary Clients Policy** only applies if the client does not fall under any current rules. Likewise, if there is a manually assigned policy to be applied and it is in conflict with the policy rules, the configuration forced by the policy rules will take precedence.

Policy rules have a tab within the Policy Manager, where they can be created and managed. The process of creation and application is very similar to that of rule creation and management in email clients: each rule can contain one or more criteria, the higher the rule is in the list, the more important it is (it can be moved up or down).

To create a new rule, click the **New...** button. Then enter a **Name, Description, Client filter parameter** and **Policy** (a policy that will be applied to any clients matching the specified criteria).

To configure the filtering criteria, click the **Edit** button.

The available criteria are:

(NOT) FROM Primary Server – if (not) located on primary server
IS (NOT) New Client – if it is (not) a new client
HAS (NOT) New Flag – applies to clients with/without the **New Client** flag.
Primary Server (NOT) IN (specify) – if name of the primary server contains/does not contain
ERA GROUPS IN (specify) – if client belongs to the group...
ERA GROUPS NOT IN (specify) – if client does not belong to the group...
DOMAIN/WORKGROUP (NOT) IN (specify) – if client belongs/does not belong to the domain...
Computer Name Mask (specify) – if computer name is
IP Mask (specify) – if client belongs to the group defined by the IP address and mask...
IP Range (specify) – if client belongs to the group defined by the IP range ...
HAS (NOT) Defined Policy (specify) – if client does (or does not) adopt the policy ...

To remove a policy rule, click the **Delete** button from the **Policy Manager** window. Click **Run Policy Rules Now** if you want to immediately apply all rules.

5.3.7 Deleting policies

As with rule creation, deleting is only possible for policies located on the server you are currently connected to. To delete policies from other servers, you must directly connect to them with the ERAC.

NOTE: A policy may be linked to other servers or policies (as a parent policy, as a default policy for lower servers, as a default policy for primary clients, etc.). Therefore in some cases it would need to be replaced rather than deleted. To see options for deleting and replacing, click the Delete Policy button. The options described below may or may not be available, depending on the position of the given policy in the policy hierarchy.

New policy for primary clients with the currently deleted policy – Allows you to select a new policy for primary clients to substitute the one you are deleting. Primary clients can adopt the **Default policy for primary clients**, as well as other policies from the same server (either assigned manually – **Add Clients**, or forced by **Policy Rules**). As a replacement you can use any policy from the given server, or a replicated policy.

New parent policy for the currently deleted policy's children policies (if existing) – If a policy to be deleted served as a parent policy for other child policies, it must also be substituted. It can be substituted by a policy from that server, by a policy replicated from upper servers, or by the N/A flag, which means that child policies will be assigned no substitute policy. We highly recommend that you assign a substitute even if no child policy exists. Another user assigning a child policy to that policy during the deletion process would cause a conflict.

New policy for replicated clients with the currently deleted or modified policy – Here you can select a new policy for clients replicated from lower servers – those that were applied to the one you are currently deleting. As a replacement you can use any policy from the given server, or a replicated policy.

New default policy for lower servers – If the deleted policy serves as a virtual policy (see **Global Policy Settings**), it must be substituted by another one (for more information, see section 5.3.3, "Virtual policies"). As a replacement you can use any policy from the given server, or the N/A flag.

New default policy for primary clients – If the deleted policy serves as a virtual policy (see **Global Policy Settings**), it must be substituted by another one (for more information, see section 5.3.3, "Virtual policies"). You can use a policy from the same server as a replacement.

The same dialog will also open if you disable the **Down replicable** option for a policy and click **OK, Apply** or if you select another policy from the Policy Tree. This will activate the items **New policy for replicated clients with the currently deleted or modified policy** or **New default policy for lower servers**.

5.3.8 Special settings

Two additional policies are not located in the Policy Manager but in **Tools > Server Options > Other Settings > Edit Advanced Settings > ESET Remote Administrator > ERA Server > Setup > Policies**.

Interval for policy enforcement (minutes):

This feature applies to policies in the specified interval. We recommend the default setting.

Disable policy usage:

Enable this option to cancel application of policies to servers. We recommend this option if there is a problem with the policy. If you wish to avoid applying a policy to some clients, then a better solution is to assigning an empty policy.

5.3.9 Policy deployment scenarios

5.3.9.1 Each server is a standalone unit and policies are defined locally

For the purpose of this scenario suppose there is a small network with one main and two lower servers. Each server has several clients. On each server, there is at least one or more policies created. The lower servers are located at the company's branch offices; both servers are managed by their local administrators. Each administrator decides which policies are to be assigned to which clients within their servers. The main administrator does not intervene in the configurations made by the local administrators and he does not assign any policies to clients from their servers. From a server policy perspective, this means that Server A has no **Default policy for lower servers**. It also means that Server B and Server C have the N/A flag or another local policy (aside from the **Default parent policy**) set as a parent policy. (e.g., Servers B and C do not have any parent policies assigned from the upper server).

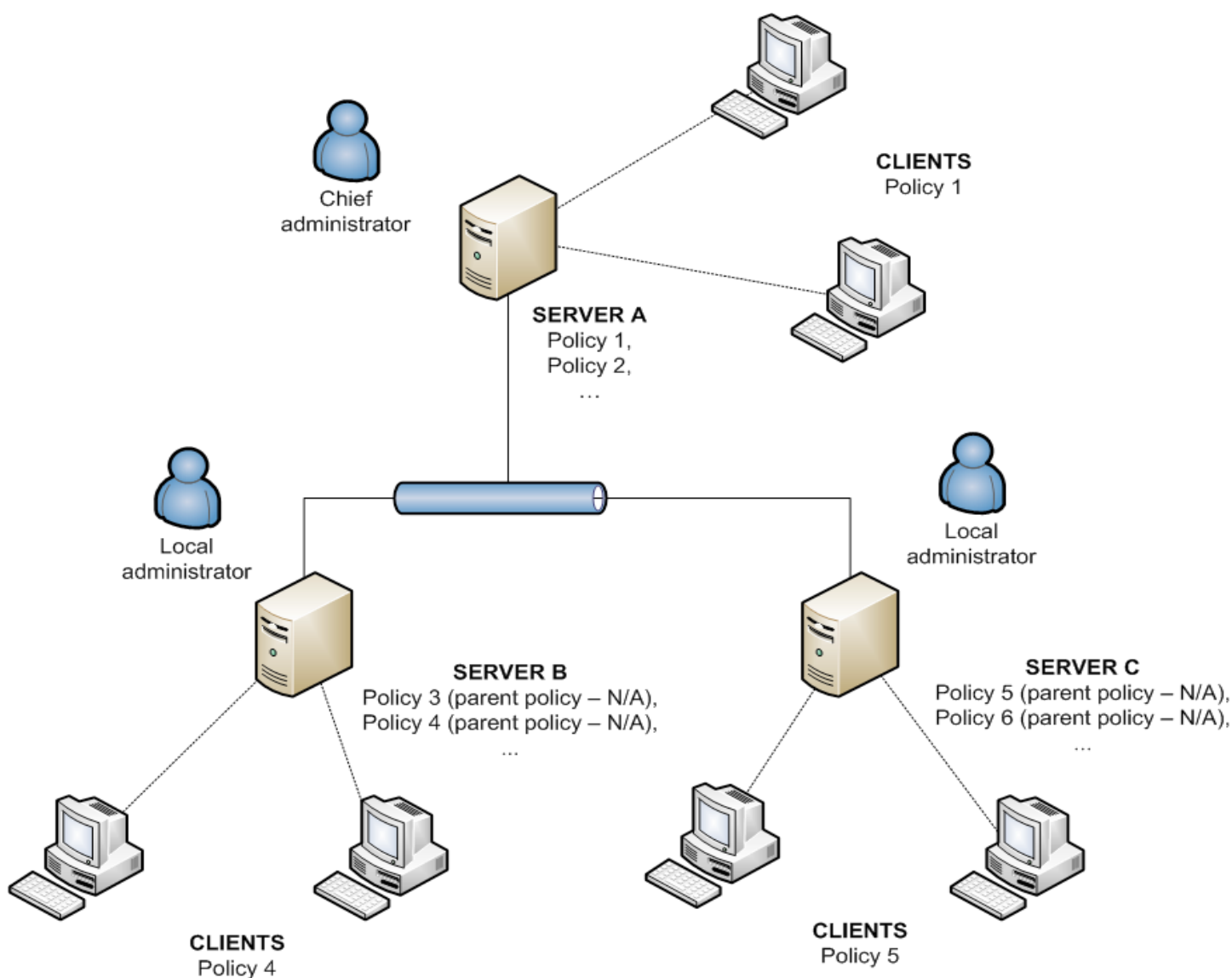


Figure 5-3

5.3.9.2 Each server is administered individually - policies are managed locally but the Default Parent Policy is inherited from the upper server

The configuration from the previous scenario also applies to this scenario. However, Server A has the Default Policy for Lower Servers enabled and policies on the lower servers inherit the configuration of the Default Parent Policy from the master server. In this scenario, the local administrators are given a large degree of autonomy to configure policies. While the child Policies on lower servers may inherit the Default Parent Policy, the local administrators can still modify it by their own policies.

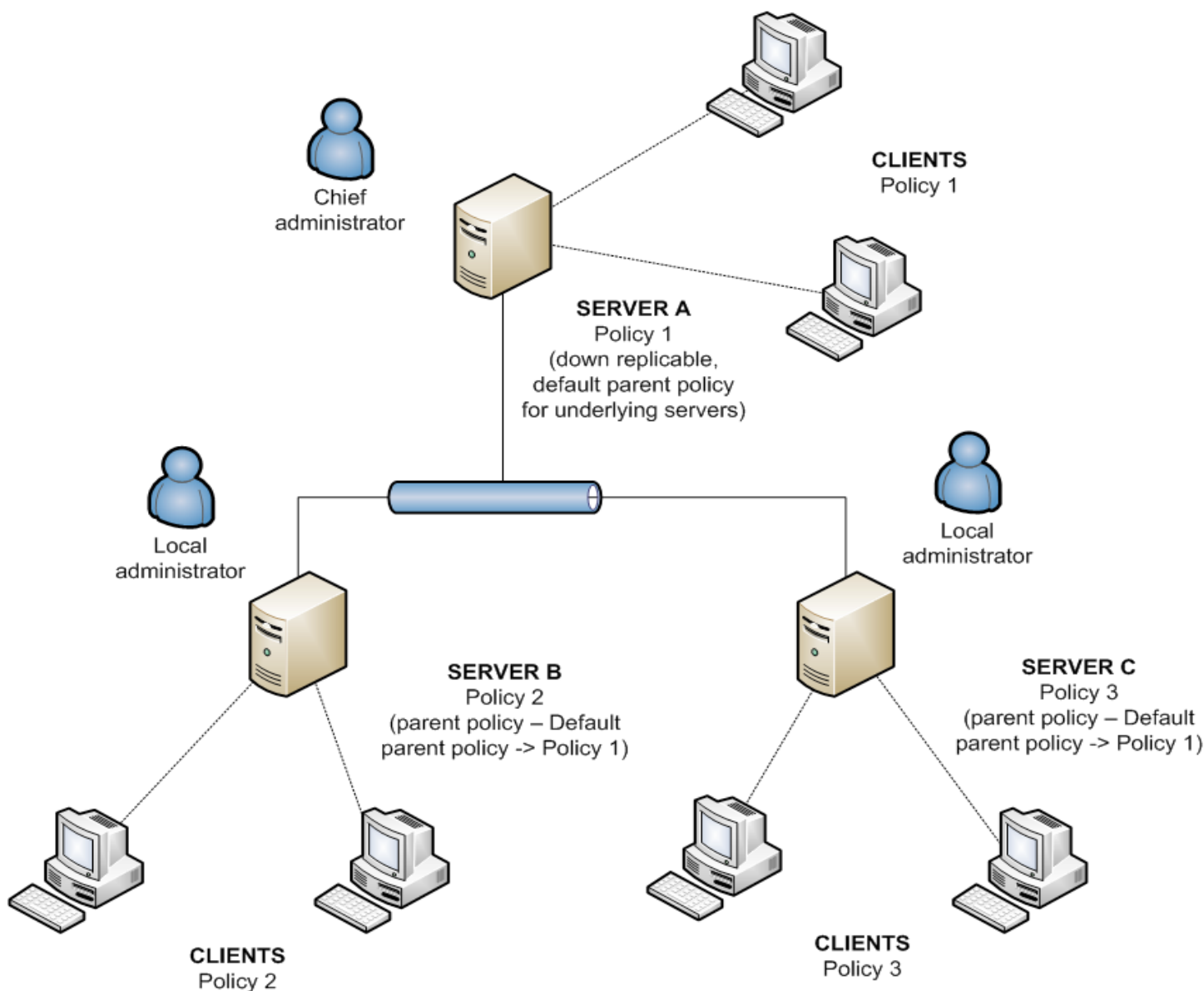


Figure 5-4

5.3.9.3 Inheriting policies from an upper server

The network model for this scenario is the same as the previous two scenarios. In addition, the master server, along with the Default Parent Policy, contains other policies, that are down replicable and serve as parent policies on the lower servers. For Policy 1 (see figure 5-5), the attribute **Override any child policy** is activated. The local administrator still has a large degree of autonomy, but the main administrator defines which policies are replicated

down and which of them serve as parent policies for local policies. The attribute **Override...** dictates that configurations set in the selected policies override those set on the local servers.

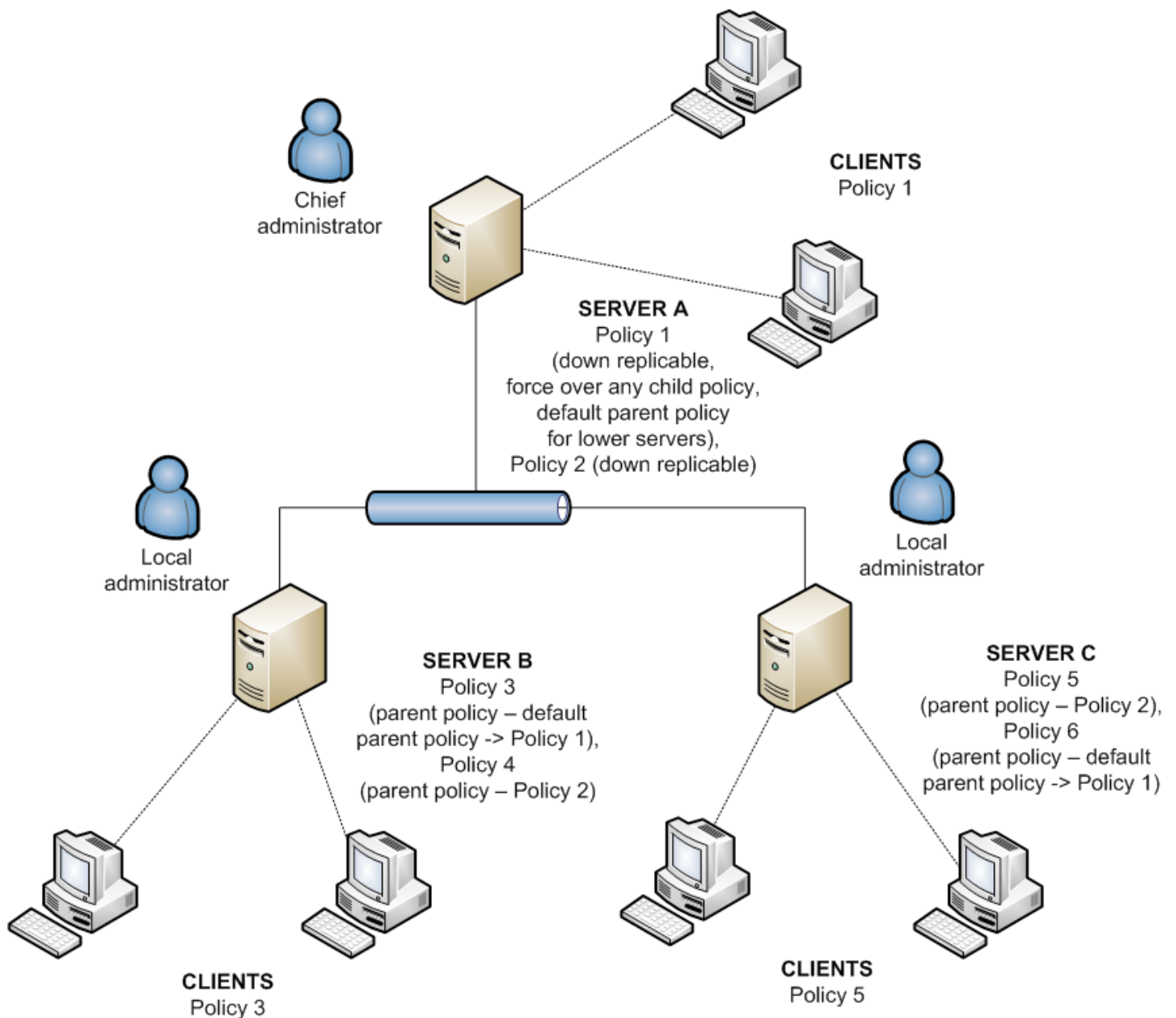


Figure 5-5

5.3.9.4 Assigning policies only from the upper server

This scenario represents a centralized system of policy management. Policies for clients are created, modified and assigned only on the main server - the local administrator has no rights to modify them. All lower servers have only one basic policy, which is empty (by default titled Server Policy). This policy serves as the Default Parent Policy for Primary Clients.

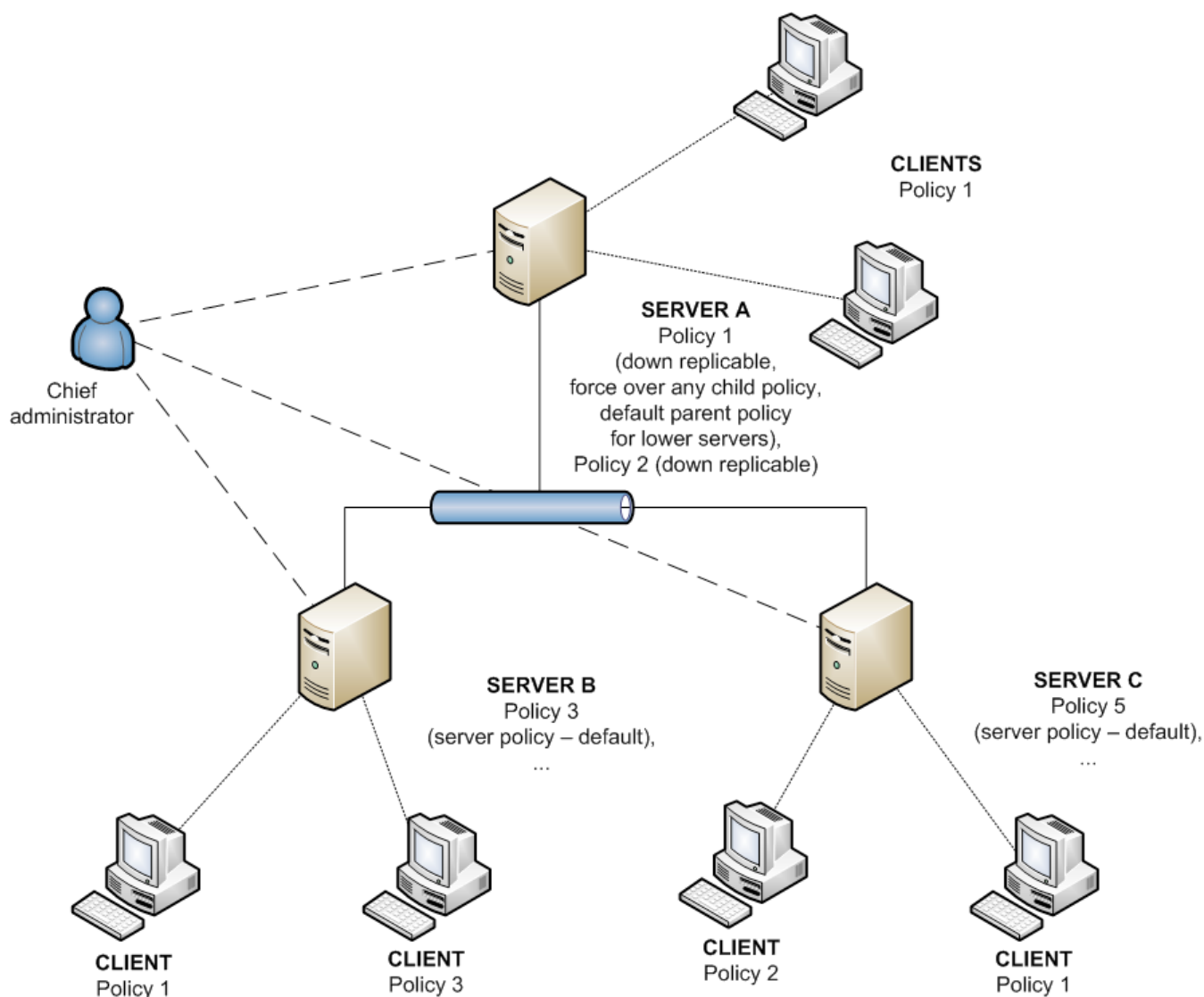


Figure 5-6

5.3.9.5 Using policy rules

Our next example involves automatically assigning policies based on policy rules. This method is complementary and should be used in combination with previously described scenarios, rather than as a standalone scenario.

If each server is managed by a local administrator, each administrator can create individual policy rules for their clients. In this scenario it is important that no conflicts exist between policy rules, such as when the upper server assigns a policy to clients based on the policy rules, while the lower server simultaneously assigns separate policies based on local policy rules.

In the end, a centralized system greatly reduces the probability of conflicts, as the entire management process takes place on the main server.

5.3.9.6 Using local groups

In some situations, assigning policies to groups of clients can complement previous scenarios. Groups can be created manually or by using the **Synchronize with Active Directory** option (see section 5.2, "Groups"). To do this, you can use one-shot assignment option (**Add Clients > Add Special**), or deliver policies automatically via **Policy Rules**.

5.4 Notifications

The ability to notify system and network administrators about important events is an essential aspect of network security and integrity. An early warning about an error or malicious code can prevent enormous losses of time and money needed to eliminate the problem later on. The next three sections outline the notification options offered by ERA.

5.4.1 Notification Manager

To open the Notification Manager main window, click **Tools > Notification Manager**.

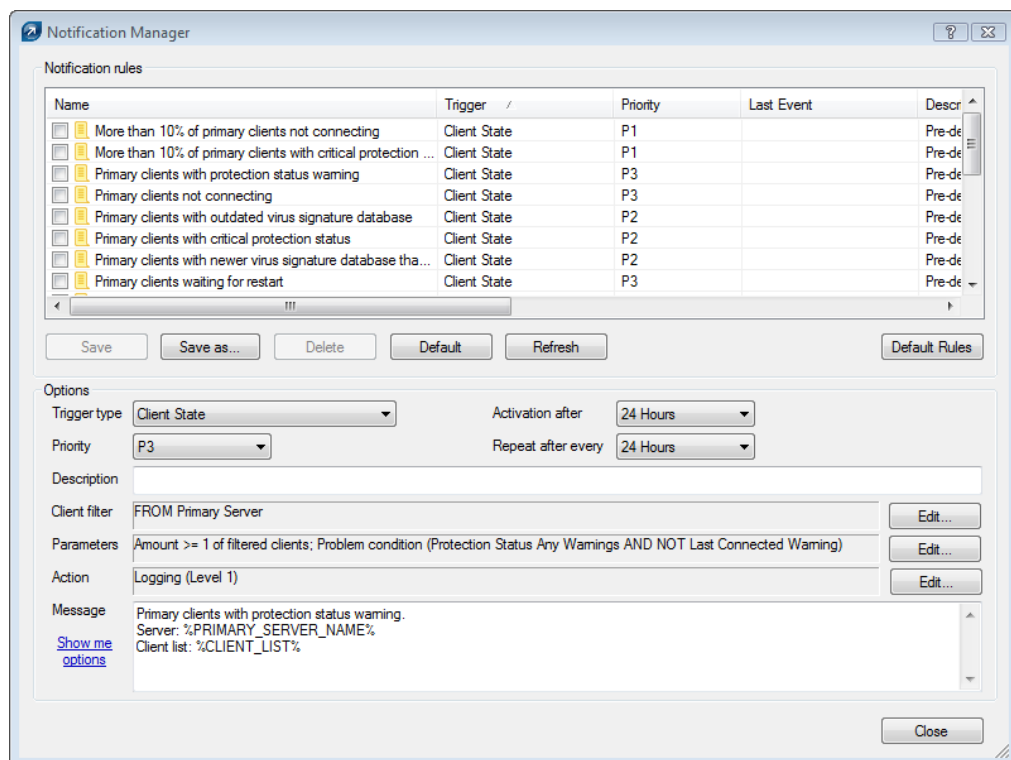


Figure 5-7: Notification Manager window

The main window is divided in two sections. The Notification rules section in the top part of the window contains a list of existing (either predefined or user defined) rules. A rule in this section must be selected to generate notification messages. By default, no notifications are enabled. Therefore, we recommend checking whether your rules are active.

The functional buttons under the list of rules include **Save** (save modifications to a rule), **Save as...** (save modifications to a rule with a new name), **Delete**, **Default** (restore default settings of a rule), and **Refresh** (update the list with default rules).

The **Options** section in the bottom half of the window provides information about the currently selected rule. All fields and options in this section are described using the sample rule from section 5.4.2, "Rule creation".

In each rule, you can specify the criteria, known as a Trigger, which activates the rule. The following triggers are available:

- **Client State** – Rule will be run if there is problem on some of the clients
- **Server State** – Rule will be run if there is problem on some of the servers
- **Finished Task Event** – Rule will be run after the specified task is finished
- **New Client Event** – Rule will run if there is a new client connecting to the server (including replicated clients)
- **New Log Event** – Rule will run if there is the specified event found in some of the logs

Based on the type of trigger, other rule options can be activated or deactivated; therefore we recommend first creating triggers when creating new rules.

The **Priority** drop-down menu allows you to set the rule priority. **P1** is the highest priority, **P5** is the lowest priority. Priority does not in any way affect the functionality of rules. To assign priority to notification messages, the %PRIORITY % variable can be used. Under the **Priority** menu, there is a **Description** field. We recommend that each rule is given a meaningful description, such as "rule that warns on detected infiltrations".

As soon as the system detects the trigger event for a certain client or clients and finds a rule to be run, the client filter is applied. The filter can be assigned to any rules in which clients are involved; to enter the client filter setup, click **Edit** in the **Client filter** section. In the window that opens, define client filtering parameters. When a rule is applied, only clients meeting the client filter criteria are taken into consideration. The filtering criteria are:

- **FROM Primary Server** – Only clients from primary server; (the negative NOT FROM can also be applied)
- **Primary Server IN** – Includes primary server in the output
- **HAS New Flag** – clients marked by the flag "New" (the negative **HAS NOT** can also be applied).
- **ERA Groups IN** – Clients belonging to the specified group
- **Domain/Workgroup IN** – Clients belonging to the specified domain
- **Computer Name Mask** – Clients with the specified computer name
- **IP Mask** – Clients falling into the specified IP mask
- **IP Range** – Clients within the specified IP address range
- **HAS Defined Policy** – Clients with the specified policy assigned (the negative **HAS NOT** can also be applied).

After you have specified a client filter for your notification rule, click **OK** and proceed to the rule parameters. Client parameters define what condition a client or a group of clients must meet in order to run the notification action. To view the available parameter, click the **Edit...** button in the **Parameters** section.

The availability of parameters depends on the selected Trigger type. The following is a complete list of parameters available by Trigger type.

The following parameters are available for Client State Triggers:

- **Amount** – Percent of clients required to activate the rule
- **Protection Status Any Warnings** – Any warning found in the Protection Status column
- **Protection Status Critical Warnings** – A critical warning found in the Protection Status column
- **Virus Signature DB version** – Problem with virus signature database (3 possible values)
 - **Previous** – Virus signature database is one version older than the current one
 - **Older or N/A** – Virus signature database is more than one version older than the current one
 - **Newer** – Virus signature database is newer than the one present on the server
- **Last Connected Warning** – The last connection was established before the specified time period
- **Has Last Threat Event** – The Threat column contains a threat warning
- **Has Last Event** – The Last Event column contains an entry
- **Has Last Firewall Event** – The Firewall Event column contains a firewall event entry
- **Has New Flag** – Client has the "New" flag
- **Waiting For Restart** – Client is waiting for restart
- **Last Scan Found Threat** – On client, the specified number of threats was found during the last scan
- **Last Scan Not Cleaned Threat** – On client, the specified number of uncleaned threats was found during the last scan

All parameters can be negated, but not all negations are usable. It is only suitable to negate those parameters that include two logical values: true and not true. For example, the parameter **Has New Flag** only covers clients with the "New" flag. The negative parameter would include all clients that are not marked by the flag.

All conditions above can be logically combined and inverted. The drop-down menu for **The rule is applied** when offers two choices:

- **all of the options are met** – Rule will only run if **all** specified parameters are met
- **any of the options is met** – Rule will run if at least **one** condition is met

The following parameters are available for the Server State Triggers:

- **Server updated** – Server is up-to-date
- **Server not updated** – Server is not up-to-date for longer than specified

- **Server logs** – The server log contains the following entry types:
 - **Errors** – Error messages
 - **Errors+Warnings** – Error messages and warning messages
 - **Filter log entries by type** – Enable this option to specify error and warning entries to be watched in the server log. Note that for notifications to work properly, the log verbosity (**Tools > Server Options > Logging**) must be set to the corresponding level. Otherwise such notification rules would never find a trigger in the server log. The following log entries are available:
 - **ADSI_SYNCHRONIZE** – Active Directory group synchronization
 - **CLEANUP** – Server cleanup tasks
 - **CREATEREPORT** – On-demand report generating
 - **DEINIT** – Server shutdown
 - **INIT** – Server startup
 - **INTERNAL** – Internal server message
 - **LICENSE** – License administration
 - **MAINTENANCE** – Server maintenance tasks
 - **NOTIFICATION** – Notification management
 - **PUSHINST** – Push install
 - **RENAME** – Internal structure renaming
 - **REPLICATION** – Server replication
 - **POLICY** – Policy management
 - **POLICYRULES** – Policy rules
 - **SCHEDREPORT** – Automatically generated reports
 - **SERVERMGR** – Internal server thread management
 - **SESSION** – Server's network connections
 - **THREATSENSE** – ThreatSense.NET – statistical information submission
 - **UPDATER** – Server update and mirror creation

An example of a helpful parameter is **UPDATER**, which sends a notification message when the Notification Manager finds a problem related to update and mirror creation in the server logs.

- **License Expiration** – License will expire in the specified number of days, or it already has expired. Select the option **Warn only if this will cause the number of clients in the license fall below the number or actual clients in the server database** to send a notification if expiration will cause the number of clients in the license to fall below the number of currently connected clients.
- **Limit license** – If percent of free clients falls under the specified value

The following parameters are available for the **New Log Event** Triggers:

- **Log type** – Select **Event Log**, **Threat Log**, or **Firewall Log**
- **Log level** – Log entry level in the given log
 - **Level 1 – Critical Warnings** – Critical errors only
 - **Level 2 – Above + Warnings** – The same as 1, plus alert notifications
 - **Level 3 – Above + Normal** – The same as 2, plus informative notifications
 - **Level 4 – Above + Diagnostic** – The same as 3, plus diagnostic notifications
- **1000 occurrences in 60 minutes** – Type the number of occurrences and select the time period to specify the event frequency that must be reached for the notification to be sent. The default frequency is 1000 occurrences in one hour.
- **Amount** – Number of clients (either absolute or in percent)

Other trigger types do not have any specific parameters.

If the specified parameters for a rule are met, the action defined by the administrator is automatically performed. To configure actions, click **Edit...** in the **Action** section. The action editor offers these options:

- **Email** – The program sends the notification text of the rule to the specified email address; enter a **Subject** and click **To** open the address book.
- **SNMP Trap** – Generates and sends SNMP notification
- **Execute (on server)** – Enable this option and specify the application to run on the server
- **Log To File (on server)** – Generates log entries in the specified log file. The **Verbosity** of this log is configurable.
- **Logging** – Records notifications to server logs; the **Verbosity** of notifications can be configured.

For this feature to work correctly, you must enable logging in the ERA Server (**Tools > Server Options > Logging**).

The notification format can be edited in the **Message** box in the bottom section of the Notification Manager main window. In the text you can use special variables, using this syntax: %VARIABLE_NAME %. To view the list of available variables, click **Show me options**.

- **Server_Last_Updated** – Last update of the server
- **Primary_Server_Name**
- **Rule_Name**
- **Rule_Description**
- **Client_Filter** – Client filter parameters
- **Client_Filter_Short** – Client filter settings (in short form)
- **Client_List** – List of clients
- **Triggered** – Date of the most recent notification sent (repeats excluded)
- **Triggered Last** – Date of the most recent notification sent (repeats included)
- **Priority** – Notification rule priority
- **Log_Text_Truncated** – Log text that activated the notification (truncated)
- **Task_Result_List** – List of finished tasks
- **Parameters** – Rule parameters
- **Last_Log_Date** – Date of the last log
- **License_Info_Merged** – License information (summary)
- **License_Info_Full** – License information (full)
- **License_Days_To_Expiry** – Days left until expiration
- **License_Clients_Left** – Free slots in the current license for clients to connect to the server
- **Actual_License_Count** – Number of clients currently connected to the server

The last parameter to be specified is time and date. Activation of the rule can be delayed to a time period ranging from one hour to three months. If you wish to activate the rule as soon as possible, set the **Activation after** drop-down menu to **ASAP**. The Notification Manager is activated every 10 minutes by default, so if you select **ASAP**, the task should run within 10 minutes. If a specific time period is selected from this menu, the action will automatically be performed after the time period has elapsed (provided that the rule condition is met).

The **Repeat after every...** menu allows you to specify a time interval after which the action will be repeated. However, the condition to activate the rule must still be met. In **Server > Other Settings > Edit Advanced Settings > ESET Remote Administrator > Server > Setup > Notifications > Interval for notification processing (minutes)** you can specify the time interval in which the server will check and execute active rules.

The default value is 10 minutes. We do not recommend decreasing it, since this may cause significant server slowdown.

By default, the Notification Manager window contains predefined rules. To activate a rule, select the check box next to the rule. The following notification rules are available. If they are activated and the rule conditions are met, they generate log entries.

- **More than 10 % of primary clients are not connecting** – If more than 10 percent of clients have not connected to the server for more than a week. The rule runs ASAP.
- **More than 10 % of primary clients with critical protection status** – If more than 10 percent of clients generated a Protection status critical warning and have not connected to the server for more than a week. The rule runs ASAP.

- **Primary clients with protection status warning** – If there is at least one client with a protection status warning that has not connected to the server for at least one week
- **Primary clients not connecting** – If there is at least one client which has not connected to the server for more than one week
- **Primary clients with outdated virus signature database** – If there is a client with a virus signature database two or more versions older than the current one that has not been disconnected from the server for more than one week
- **Primary clients with critical protection status** – If there is a client with a critical protection status warning that hasn't been disconnected for more than one week
- **Primary clients with newer virus signature database than server** – If there is a client with a newer virus signature database than that on the server and which has not been disconnected for more than one week
- **Primary clients waiting for restart** – If there is a client waiting for restart that has not been disconnected for more than one week
- **Primary clients with a non-cleaned infiltration in computer scan** – If there is a client where computer scan could not clean at least one infiltration and that client has not been disconnected for more than one week. The rule runs ASAP.
- **Completed task** – If there was a task completed on a client. The rule runs ASAP.
- **New primary clients** – If a new client has connected to the server. The rule runs ASAP.
- **New replicated clients** – If there is a new replicated client in the list of clients. The rule runs after one hour.
- **Possible virus outbreak** – If the frequency of Threat log entries on a client has exceeded 1000 critical warnings in one hour on at least 10 % of all clients.
- **Possible network attack** – If the frequency of ESET Personal firewall log entries on a client has exceeded 1000 critical warnings in one hour on at least 10 % of all clients.
- **Server updated** – If the server has been updated
- **Server not updated** – If the server has not been updated for more than five days. The rule runs ASAP.
- **Error in server text log** – If the server log contains an error entry.
- **License expiration** – If the current license will expire within 20 days and after expiration, the maximum number of client slots will be lower than the current number of clients. The rule runs ASAP.
- **License limit** – If the number of free client slots decreases under 10 % of all client slots available.

If not stated otherwise, all rules are run and repeated after 24 hours and are applied to the primary server and primary clients.

5.4.1.1 Notifications via SNMP TRAP

SNMP (Simple Network Management protocol) is a simple and wide spread management protocol suitable for monitoring and identifying of network problems. One of the operations of this protocol is TRAP, which sends specific data. In ERA, we use TRAP to send notification messages.

In order for the TRAP tool to run effectively, the SNMP protocol must be correctly installed and configured on the same computer as ERAS (**Start > Control Panel > Add or Remove programs > Add/Remove Windows Components**). The SNMP service should be configured as described in this article: <http://support.microsoft.com/kb/315154>. In ERAS, you need to activate an SNMP notification rule.

Notifications can be viewed in the SNMP manager, which must be connected to an SNMP server where the configuration file `eset_ras.mib` is imported. The file is a standard component of an ERA install, and is usually located in the folder `C:\Program Files\ESET\ESET Remote Administrator\Server\snmp\`.

5.4.2 Rule creation

The following steps demonstrate how to create a rule that will send email notification to the administrator if there is a problem with the Protection Status of any client workstations. The notification will also be saved to a file named `log.txt`.

- 1) Set the **Trigger type** drop-down menu to **Client State**
- 2) Leave the options **Priority**, **Activation after:** and **Repeat after every:** at the predefined values. The rule will automatically be assigned the priority 3 and will be activated after 24 hours.

- 3) In the **Description** field, type **protection status notification for HQ clients**
- 4) Click **Edit...** in the **Client filter** section and only activate the **ERA Groups IN** section rule condition. In the lower part of this window click the link **specify** and type **HQ** in the new window. Click **Add** and then click **OK** (twice) to confirm. This designates that the rule is only applied to clients from the HQ group.
- 5) Further specify parameters for the rule in **Parameters > Edit...** Deselect all options except for **Protection Status Any Warnings**.
- 6) Proceed to the **Action** section and click the **Edit...** button. In the **Action** window, activate **Email**, specify recipients (**To...**) and **Subject** for the email. Then select the **Log to file** check box and enter the name and path of the log file to be created. As an option, you can select the **Verbosity** of the log file. Click **OK** to save the action.
- 7) Finally, use the **Message** text area to specify the verbiage that will be sent in the body of the email when the rule is activated. Example: "The client %CLIENT_LIST % reports protection status problem".
- 8) Click **Save as...** to name the rule, e.g., "protection status problems" and select the rule in the list of notification rules.

The finished rule should resemble Figure 5–8:

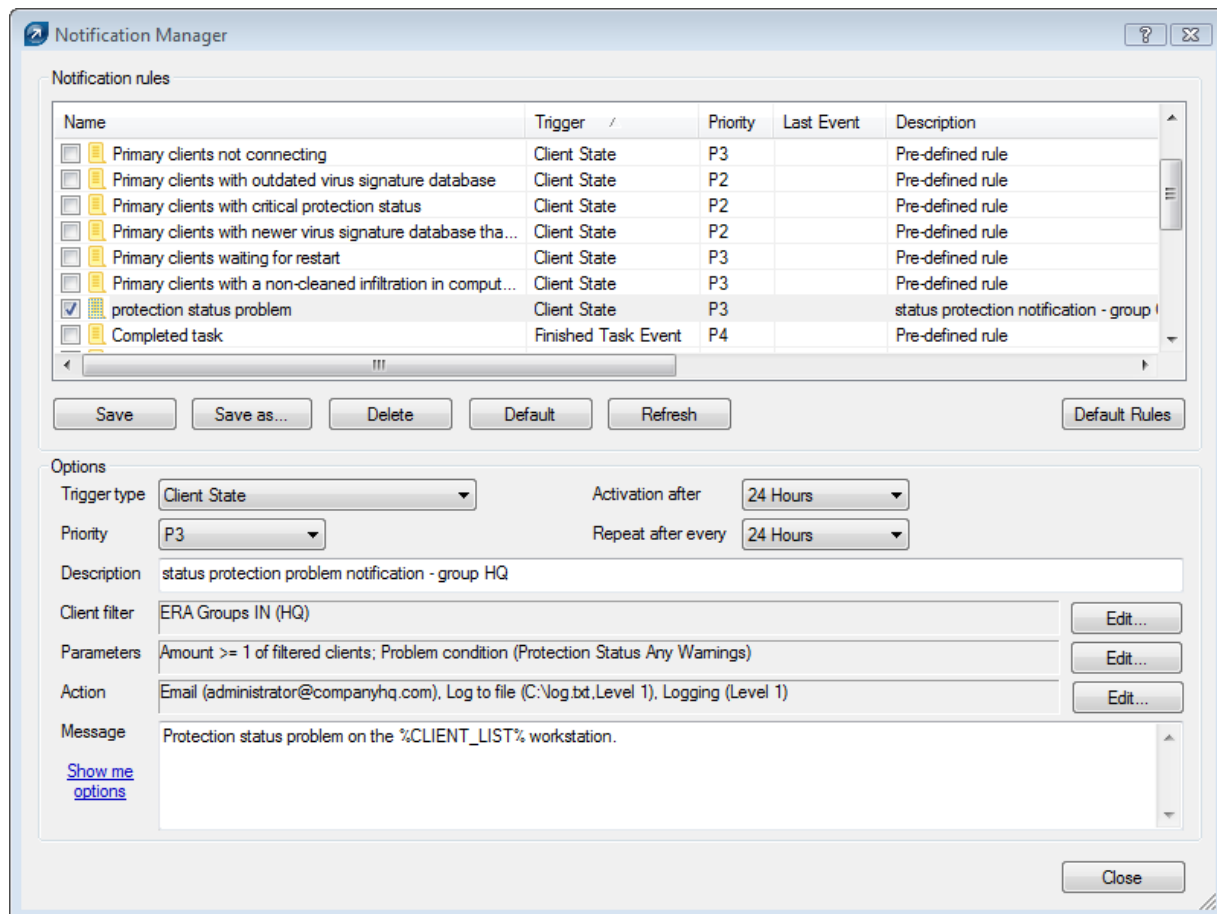


Figure 5-8 Example of notification rule

The rule is now active. If there is a problem with the protection status on a client from the HQ group, the rule will be run. The administrator will receive an email notification with an attachment containing the name of the problematic client. Click **Close** to exit the Notification Manager.

5.5 Detailed information from clients

ERA allows you to extract information about running processes, startup programs, etc. from client workstations. This information can be retrieved using the integrated ESET SysInspector tool, which is integrated directly with

ERAS. Along with other useful functions, ESET SysInspector thoroughly examines the operating system and creates system logs. To open it, click **Tools > ESET SysInspector** from the ERAC main menu.

If there are problems with a specific client, you can request an ESET SysInspector log from that client. To do this, right-click the client in the Clients pane and select **Request data – Request SysInspector Information**. Logs can only be obtained from generation 4.x products and later; earlier versions do not support this feature. Click the **log request** link to open a new window with the following options:

- **Create snapshot (remember resulting log also on the client)** – Saves a copy of the log to the client computer.
- **Include comparison to the last snapshot before specified time** – Displays a comparative log, comparative logs are created by merging the current log with a previous log if available. ERA will choose the first log that is older than the specified date.

Click **OK** to obtain the selected logs and save them to the server. To open and view the logs, proceed as follows.

ESET SysInspector options for individual client workstations can be found in the **Client Properties – SysInspector** tab. The window is divided into three sections; the top section shows text information about the most recent logs from the given client. Click **Refresh** to load the most current information.

The middle section of the **Request Options** window is almost identical to the window which appears in the above described process of requesting logs from client workstations. The **Request** button is used to get an ESET SysInspector log from the client.

The bottom section is comprised of these buttons:

- **View** – Opens the log listed in the top section directly in ESET SysInspector
- **Save As...** – Saves the current log to a file. The **Then Run ESET SysInspector Viewer to view this file** option automatically opens the log after it is saved (as it would after clicking **View**).

Generating and displaying new log files can sometimes be slowed by the local client, due to the size of the log and data transfer speed. The date and time assigned to a log in **Client Properties > SysInspector** marks the date and time of delivery to the server.

6. Reports

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

To browse and select graphical styles, use the **Style** drop-down menu in the **Report** section..

ERA provides several predefined templates for reports. To select a report, use the **Type** drop-down menu:

- **Top Threats**
List of the most frequently detected threats.
- **Top Client with most Threats**
Lists the most "active" client workstations (measured by 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 threats.
- **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 as well as choose which report format will be used (.html, .csv).

The Interval 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 (i.e., 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 to 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 following Wednesday (after Saturday).

In the **Interval** tab, select **Completed** and **1 Weeks**. Remove **Add also the current period**. 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.

The Scheduler 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** date picker to enter the time and date when the report is to be generated. Click the **Select Target...** button in the section **and store Result to** specify where the report is to be saved. Reports can be saved to ERAS (default), sent via email to a chosen address, or exported to a folder. The latter option is useful if the report is sent to a shared folder on your organization's intranet where it can be viewed by other employees.

To send generated reports via email, you need to enter the SMTP server and sender address information in **Tools > Server Options > Other settings** as described in section 7.8.1, "SMTP Settings".

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, you can find 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).

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.

7. ESET Remote Administrator Server (ERAS) setup

7.1 Security tab

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

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

The Security tab contains options which allow the administrator to use 2.x and 3.x security solutions in the same network simultaneously.

- **Password for Console (Administrator Access, Read-Only Access)**
Enables specifying a password for the administrator and limited users to protect against unauthorized changes to ERAS settings.
- **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 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 clients of lower ERA Servers 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 **Enable unauthenticated access for Clients** option can be disabled.

7.2 Server Maintenance tab

If correctly configured in the Server Maintenance tab, the ERAS database will be maintained automatically 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. All server maintenance options are accessible from **Tools > Server Options > Server Maintenance**.

The options include:

- **Only keep the latest X threats for each client**
Only keeps the specified number of virus incidents for each client.
- **Only keep the latest X firewall logs for each client**
Only keeps the specified number of firewall logs for each client.
- **Only keep the latest X events for each client**
Only keeps the specified number of system events for each client.
- **Only keep the latest X scan logs for each client**

Only keeps 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).

7.3 Mirror server

The Mirror feature allows a user to create a local update server. Client computers will not download virus signature updates from ESET's servers on the Internet, but will connect to a local Mirror server on your network instead. The main advantages of this solution are to save Internet bandwidth and to minimize network traffic, since only the mirror server connects to the Internet for updates, rather than hundreds of client machines. This configuration means it is important for the Mirror server to always be connected to the internet.

Warning: A Mirror server which performed a program component upgrade (PCU) and has not been rebooted may cause an outage. In this scenario, the server would be unable to download ANY updates or distribute them to client workstations. **DO NOT SET AUTOMATIC PROGRAM COMPONENT UPGRADES FOR ESET SERVER PRODUCTS!** This does not apply to Mirror created in ERAS.

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).

The administrator selects the method for activating the Mirror feature.

In large networks it is possible to create multiple Mirror servers (e.g., for various company departments), and establish one as central (at company headquarters) in cascade-style – similar to an ERAS configuration with multiple clients.

The administrator must insert the product license key for a purchased product and enter the username and password to enable the Mirror feature in ERAS. If the administrator uses a license key and username and password for ESET NOD32 Antivirus Business Edition, then later upgrades to ESET Smart Security Business Edition, the original license key, username and password must be replaced as well.

7.3.1 Operation of the Mirror server

The computer hosting the Mirror server should always be running, and connected to the Internet or to an upper Mirror server for replication. Mirror server update packages can be downloaded in two ways:

1. Using the HTTP protocol (recommended)
2. Using a shared network drive (SMB)

ESET's update servers use the HTTP protocol with authentication. A central Mirror server should access the update servers with a username (usually in the following form: EAV-XXXXXXX) and password.

The Mirror server which is a part of ESET Smart Security/ESET NOD32 Antivirus has an integrated HTTP server (variant 1).

NOTE: If you decide to use the integrated HTTP server (with no authentication), please ensure that it will not be accessible from outside 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. ERA also supports additional authentication methods (e.g., on Apache Web Server the .htaccess method is used).

The second method (shared network folder) requires sharing ("read" rights) of the folder containing update packages. In this scenario, a username and password of a user with "read" rights for the update folder must be entered into the client workstation.

NOTE: ESET client solutions use the SYSTEM user account and thus have different network access rights than a currently logged-in user. Authentication is required even if the network drive is accessible for "Everyone" and the current user can access them, too. Also, please use UNC paths to define the network path to the local server. Using the DISK:\ format is not recommended.

If you decide to use the shared network folder method (variant 2), we recommend that you create a unique username (e.g., NODUSER). This account would be used on all client machines for the sole purpose of downloading updates. The NODUSER account should have "read" rights to the shared network folder which contains the update packages.

For authentication to a network drive, please enter the authentication data in the full form: WORKGROUP\User, or DOMAIN\User.

In addition to authentication, you must also define the source of updates for ESET client solutions. The update source is either a URL address to a local server (http://Mirror_server_name:port) or UNC path to a network drive: (\\Mirror_server_name\share_name).

7.3.2 Types of updates

In addition to virus signature database updates (which can include ESET software kernel updates), program component upgrades are also available. Program component upgrades add new features to ESET security products and require a reboot.

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

This feature is especially useful if the administrator wishes to download and use virus signature database updates when there is also a new program version available. If an older program version is used in conjunction with the most recent virus database version, the program will continue to provide the best protection available. Still, we recommend that you download and install the newest program version to gain access to new program features.

By default, program components are not automatically downloaded and must be manually configured in ERAS. For more information see section 7.3.3., "How to enable and configure Mirror".

7.3.3 How to enable and configure the Mirror

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

- From the ERAC click **Tools > Server Options... > Updates**.
- From the **Update server:** drop-down menu, select **Choose Automatically** (updates will be downloaded from ESET's servers), or enter the URL/UNC path to a Mirror server.
- Set the Update interval for updates (we recommend sixty minutes).
- If you selected **Choose Automatically** in the previous step, insert the username (Update username) and password (Update password) which were sent after purchase. If accessing an upper server, enter a valid

domainuser 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**⁶.

NOTE: In case of problems with update, select the **Clear Update Cache** option to flush the folder with temporary update files.

- The **Mirror Downloaded PCU** option allows you to activate program components mirroring. To set up PCU mirroring go to **Other Settings > Edit Advanced Settings** and configure settings in **ESET Remote Administrator > ERA Server > Setup > Mirror (or Mirror for NOD32 version 2)**.
- Select the language components to be downloaded in **Other Settings > Edit Advanced Settings...** the branch **ERA Server > Setup > Mirror > Create Mirror for the selected program components**. Components for all language versions to be used in the network should be selected. Note that downloading a language version not installed in the network will unnecessarily increase network traffic.

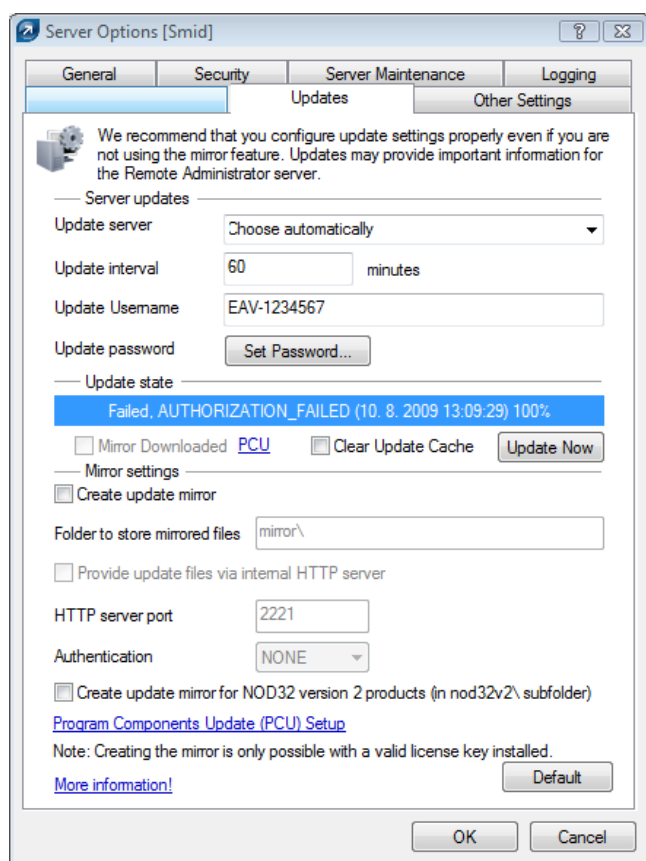


Figure 7-1

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:

- 1) Install ESET Smart Security Business Edition or ESET NOD32 Antivirus Business Edition
- 2) From the **Advanced Setup** window (F5), click **Miscellaneous > Licenses**. Click the **Add...** button, browse for the *.lic file and click **Open**. This will install the license and allow configuration of the Mirror feature.
- 3) From the **Update** branch click the **Setup...** button and select the **Mirror** tab.

⁶ For more information see the section about authentication in ERA Server.

- 4) Select the **Create update mirror** and **Provide update files via internal HTTP server** option.
- 5) Enter the full directory path to the folder (**Folder to store mirrored files**) where update files are to be stored.
- 6) The **Username** and **Password** serve as authentication data for client workstations attempting to gain access to the Mirror folder. In most cases, it is not required to populate these fields.
- 7) Set Authentication to **NONE**⁷
- 8) Select components to be downloaded⁸ (components for all language versions which will be used in the network should be selected).

NOTE: To maintain optimal functionality, we recommend that you enable downloading and mirroring of program components. If this option is disabled, only the virus signature database is updated, not program components. If the Mirror is used as a part of ERA, this option can be configured in 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.

7.3.4 Mirror for clients with NOD32 version 2.x

ESET Remote Administrator also allows an administrator to create update file copies for client computers with ESET NOD32 Antivirus 2.x installed. To do this, click **Tools > Server Options > Updates > Create update mirror NOD32 version 2 products**. This only applies to ERA; the Mirror included in the client solution of the Business Edition (v 3.x) does not contain this option.

If you have a mix of 2.x and 3.x clients in your network, we recommend that you use the Mirror integrated in ERA. If both Mirrors are activated on the same computer – one in ERAS for 2.x clients, and the other in a Business Edition client for 3.x clients – it could result in a conflict between two HTTP servers using the same TCP port.

Updates for 2.x clients are stored in the folder "nod32v2", a subfolder of the main Mirror folder. It is accessible via the URL address:

`http://Mirror_server_name:port/nod32v2`

or UNC path to a network drive:

`\\Mirror_server_name\share_name\nod32v2`

ERA is also capable of downloading program components for 2.x clients. To select program components to be downloaded, navigate to **Tools > Server Options... > the tab Other Settings > click Edit Advanced Settings... > the branch ESET Remote Administrator > ERA Server > Setup > Mirror for NOD32 version 2**. To minimize the volume of downloaded data, only select language versions that are present on your network.

7.4 Replication tab

Replication is used in large networks where multiple ERA Servers are installed (e.g., a company with several branches). For more information, see section 2.3.3, "Installation".

The options in the Replication tab (**Tools > Server Options...**) are divided into two sections:

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

The **Replication "to" settings** section is used to configure lower ERA Servers. The **Enable "to" replication** option must be enabled and the IP address or name of the master ERAS (Upper server) entered. Data from the lower server is then replicated to the master server. The **Replication "from" settings** allow master (upper) ERA Servers to accept data from lower ERA Servers, or to transfer them to their master servers. The **Enable "from" replication** must be enabled and names of lower servers should be defined (delimited by a comma).

Both of these options must be enabled for ERA Servers located anywhere in the middle of the replication hierarchy (i.e., they have both upper and lower servers).

⁷ For more information about authentication, see section 7.3.1. "Operation of the Mirror server".

⁸ Components are only displayed if they are available from ESET's update servers.

All of the previously mentioned scenarios are visible in the figure below. The beige computers represent individual ERA Servers. Each ERAS is represented by its name (which should be the same as %Computer Name %, to avoid confusion) and the corresponding settings in the replication dialog window.

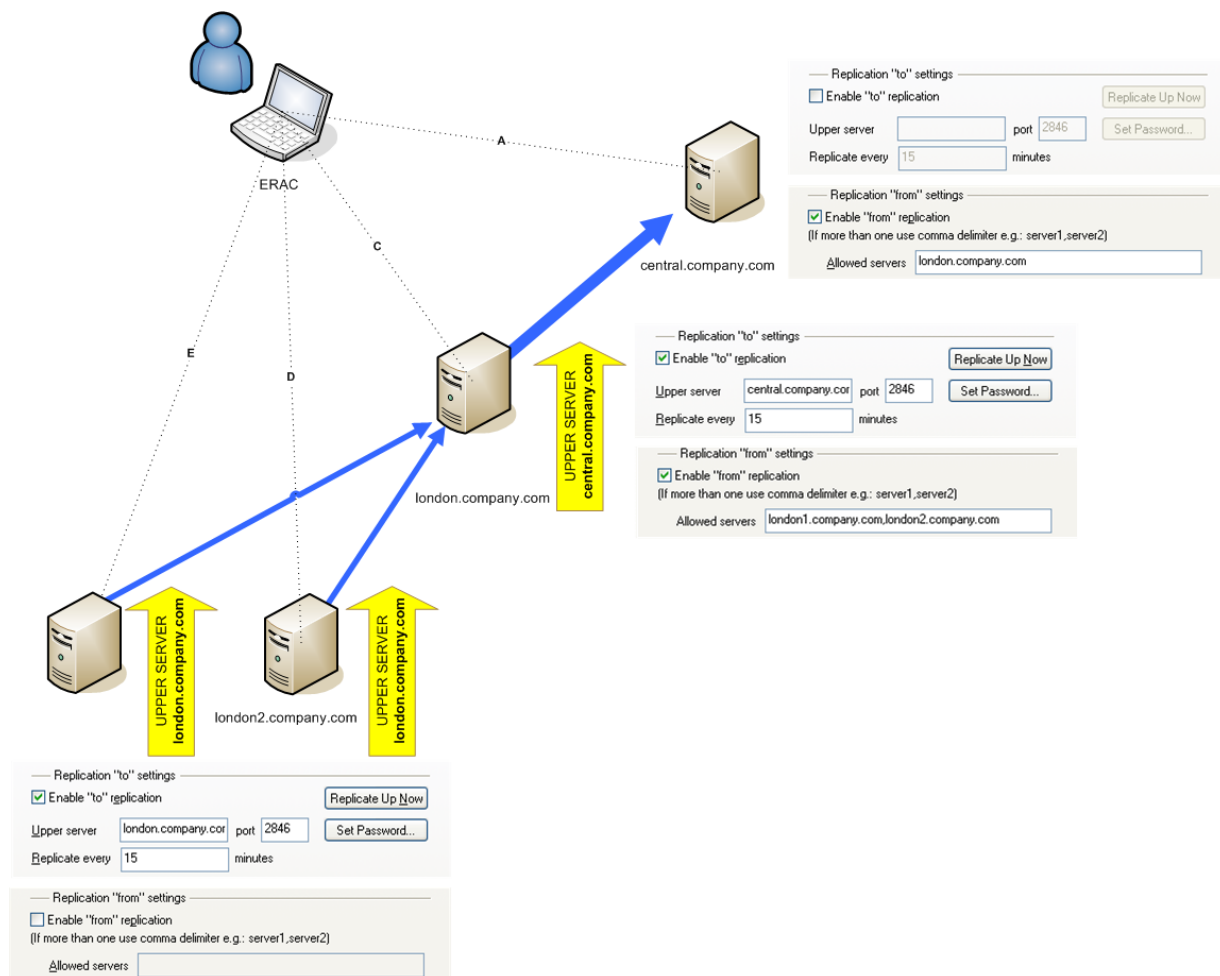


Figure 7-2

Other options which influence the replication behavior of servers include:

- **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. Enable these options to also replicate entries in those files.
- **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: Some logs are automatically replicated, while detailed logs and client configuration logs are only replicated on demand. This is because some logs contain large amounts of data that may not be relevant. For example, a scan log with the Log all files option enabled will consume a significant amount of disk space. Such information is usually not necessary and can be requested manually. Child servers do not automatically submit information about deleted clients. Therefore upper servers may continue to store information about deleted clients from lower servers. If you want to delete a client from the Client tab on upper servers, select the Enable deletion of replicated clients option on the underlying server located in **Server Options > Other Settings > Edit Advanced Settings > Setup > Replication**.

To set the log maintenance level in ERAS, click **Tools > Server Options > Other Settings > Edit Advanced Settings... > Setup > Server Maintenance**.

If you want to only replicate clients with a status change, select the **Tools > Server Options > Replication > Mark all clients for replication by "Replicate Up Now"** option.

7.5 Logging tab

While running, 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 (**Windows Control Panel > Administrative Tools > Event viewer**).

The **Database 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`

We recommend leaving the Log verbosity set to Level 2 – Above + Session Errors. Change the log level only if you are experiencing problems, or if you are advised to do so by ESET Customer Care.

Click **Tools > Server Options > Other Settings > Edit Advanced Settings... > Setup > Logging > Rotated debug log compression** to configure compression level for individual rotated logs.

7.6 License management

In order for ERA to function properly, a license key must be uploaded. After purchase, license keys are delivered along with your username and password to your email. The **License manager** serves to manage licenses.

In ERA 3.x and later, support for multiple license keys has been added. This feature makes management of license keys more convenient.

The main License Manager window is accessible from **Tools > License manager**.

To add a new license key:

1. Navigate to **Tools > License manager** or press **CTRL + L** on your keyboard.
2. Click **Browse** and find the desired license key file (license keys have the extension .lic)
3. Click **Open** to confirm
4. Verify that the license key information is correct and select **Upload to Server**
5. Click **OK** to confirm

The **Upload to Server** button is only active if you have selected a license key (using the **Browse** button). Information about the currently viewed license key is shown in this part of the window. This allows for a final check before the key is copied to the server.

The central part of the window displays information about the license key which is currently used by the server. To see details about all license keys present on the server, click the **Details...** button.

ERAS is capable of selecting the most relevant license key and merging multiple keys into one. If there is more than one license key uploaded, ERAS will always try to find the key with the most clients and furthest expiration date.

The ability to merge multiple keys works if all keys are owned by the same customer. Merging licenses is a simple process which creates a new key containing all clients involved. The expiration date of the new license key becomes the expiration date of the key that would expire first.

The bottom part of the License Manager window is dedicated to notifications when there is a problem with licenses. The available options include:

- **Warn if the server is about to expire in 20 days** – Displays a warning X days before license expires
- **Warn only if this will cause the number of clients in the license to fall below the number or actual clients in the server database** – Activate this option to only show a warning if the expiration of the license key, or a part of the license, will cause a decrease in the number of clients below the number of currently connected clients, or clients in the ERAS database
- **Warn if there is only 10 % free clients left in the server license** – Server will display a warning if the number of free client slots falls under specified value (in %)

ERAS is capable of merging multiple licenses from multiple customers. This feature must be activated by a special key. If you need a special key, please specify it in your order, or contact your local ESET distributor.

7.7 Advanced settings

To access ERA Advanced settings, click **Tools > Server Options > Other Settings > Edit Advanced Settings**.

Advanced settings include the following:

- **Maximum disk space usage (percent)**
When exceeded, some server features may not be available. When connecting to ERAS, ERAC displays a notification if the limit is exceeded.
- **Communication protocol encoding**
Defines the type of encoding. We recommend the default setting.
- **Enable MAC address renaming (from unknown to valid)**
After reinstalling from an ESET client solution that does not support sending a MAC address (e.g., ESET NOD32 Antivirus 2.x) to a client solution that does (e.g., a 3.x client), the old client record will be converted to the new one. We recommend the default setting (Yes).
- **Enable MAC address renaming (from valid to unknown)**
After reinstalling from an ESET client solution that does support sending a MAC address (e.g., ESET NOD32 Antivirus 3.x) to a client solution that does not (e.g., a 2.x client), the old client record will be converted to the new one. We recommend the default setting (No).
- **Enable MAC address renaming (from valid to another valid)**
Enables renaming of valid MAC addresses. The default value does not allow for renaming, which means that the MAC address is a part of the unique identification of clients. Disable this option if there are multiple entries for one PC. We also recommend disabling this option if a client is identified as the same client after the MAC address has been changed.
- **Enable computer name renaming**
Allows for renaming of client computers. If disabled, the computer name will be a part of the unique identification of clients.
- **Use server default logon also by push installation**
ERAS allows the user to set the username and password for logon script and email remote installation only. Enable this option to use the predefined values also for remote push installations.

7.8 Other settings tab

7.8.1 SMTP settings

- **SMTP settings (Server, Sender address, Username, Password)**
Some features in ERA require correct SMTP server configuration. Those features include remote email installation and generating reports to be sent by email.

7.8.2 Ports

Ports (Console, Client, Replication port of this server, ESET Remote Installer)

Enables you to customize ports where ERAS is listening to communications, established by:

- **Console** (by default 2223)
- **Client** (by default 2222)
- The replication process (**Replication port** – by default 2846)
- **ESET Remote Installer** (by default 2224)

7.8.3 New clients

- **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 3.4.3, “Clients tab”.

7.8.4 ThreatSense. Net

- **Enable ThreatSense. Net data forwarding to ESET servers**

If enabled, ERAS will forward suspicious files and statistical information from clients to ESET’s servers. Note that it is not always possible for client workstations to submit this information directly, due to the network configuration.

8. ERA Maintenance tool

The purpose of the ERA Maintenance tool is to execute specific tasks for server operation and maintenance. It can be accessed by clicking **Start -> Program Files -> ESET Remote Administrator -> Server**. When you launch the ERA Maintenance tool, an interactive wizard will display to help you in perform the required tasks.

8.1 ERA Server Information

The tool displays summary information about the ERA Server installed. The displayed information can be viewed in more detail in a separate window by clicking **More Information**, it can be copied by clicking **Copy to clipboard** and it can be refreshed by clicking **Refresh**. After you verify the information, proceed to the next step by clicking **Next**.

8.2 Task Type

The Maintenance tool contains a list of available tasks. At the end of each task setup, you can save the settings for the current task by clicking **Save all settings to a file**. The settings can be then used at any time in the future by clicking **Load all settings from a file**. Each individual step in a task setup also has the option to **Save all settings to a file** or **Load all settings from a file**.

8.2.1 Stop ERA Server

This task stops the ESET Remote Administrator Server service.

8.2.2 Start ERA Server

This task starts the ESET Remote Administrator Server service.

8.2.3 Database Transfer

This task allows you to convert the database format. The tool can convert between the following databases:

- MS Access
- MS SQL Server
- Oracle
- My SQL

The first step is to select the database.

If the database is an MS Access database, specify the path to the .mdb file. The path specified during ERA Server installation is used by default.

All other database formats require additional parameters to be set:

- Connection string: Special string used to identify the source database
- Username: Username for accessing the database
- Password: Password for accessing the database
- Schema name: Name of a schema (available for Oracle and MS SQL only)

Click **Load current server configuration** to use the current ERA Server settings. Click **Test Connection** to test the database connection. If the connection cannot be established, check the parameters for errors. After the database test is successful, continue by clicking **Next**.

Select the target database. Select **Replace server connection settings** to connect the server and use the new database after the conversion. Not selecting this option will cause the new database to be created without the server updating to the new database version.

For all database types besides MS Access database, select whether to create the database tables automatically (**Create tables in the database automatically**) or insert the tables into the database later (**View Script -> Save to File**) in the next step. For an MS SQL database, the **Create a new database ESETRADB automatically** option automatically creates a new MYSQL database named ESETRADB. The final step is to confirm the database conversion.

8.2.4 Database Backup

This tool allows you to create a backup file of the database. The settings in the first window are similar to those in the database conversion (see Database Transfer); in this window the source database is selected. The source database will be copied to a backup file specified in the next step.

Optional parameters in the lower part of the window enable you to overwrite the existing file (**Overwrite if exists**) as well as to stop ESET Remote Administrator Server during the backup process (**Stop server during processing task**). Click **Next** to confirm the task execution.

8.2.5 Database Restore

This task allows you to restore the database from a backup file. The settings in the first window are similar to those in the database conversion (see Database Transfer); in this window the database type is selected.

For all database types besides MS Access database select whether to create the database tables automatically (**Create tables in the database automatically**) or insert the tables into the database later (**View Script -> Save to File**) in the next step. For an MS SQL database the **Create a new database ESETRADB automatically** option automatically creates a new MySQL database named ESETRADB. The final step is to confirm the database conversion.

Select the file from which the database is to be restored in the next step. Optional parameters in the lower part of the window enable you to import a file from a different database type as selected in the previous step (**Allow import from a different type of database**) as well as to stop ESET Remote Administrator Server during database restore (**Stop server during processing task**). Click **Next** to confirm the task execution.

8.2.6 Delete Tables

This deletes the current tables in the database. As a result, the database will return to the state from right after ERA Server installation. The settings in the first window are similar to those in the database conversion (see Database Transfer); in this window the database type is selected. In the next step you will be prompted to confirm the action. Select **Yes, I agree** and then click **Next** to confirm the action.

8.2.7 Install New License Key

To insert a new license key to be used by the server enter the location of the new license key. Overwrite the existing license key if required (**Overwrite if exists**) and restart the server if required (**Force server start (in case it is not running)**). Click **Next** to confirm and complete the action.

8.2.8 Modify server configuration

This task launches the Configuration Editor (if installed). Finishing the task opens the Configuration Editor window and allows you to edit advanced ERA Server settings. These settings are also accessible via **Tools -> Server Options -> Other Settings -> Edit Advanced Settings**.

9. Troubleshooting

9.1 FAQ

This chapter contains solutions to the most frequently asked questions and problems related to installation and operation of ERA.

9.1.1 Problems installing ESET Remote Administrator to Windows server 2000/2003

Cause:

One of the possible causes may be the Terminal Server running on the system in the *execution* mode.

Solution:

Microsoft advises switching the Terminal Server to "install" mode while installing programs to a system with Terminal Server service running. This can be done either through **Control Panel > Add/Remove programs**, or by opening a command prompt and issuing the *change user /install* command. After installation, type *change user /execute* to return to the Terminal Server to execution mode. For step-by-step instructions on this process, see the following article: <http://support.microsoft.com/kb/320185>.

9.1.2 What is the meaning of the GLE error code?

Installing ESET Smart Security or ESET NOD32 Antivirus via the Remote Administrator Console can occasionally generate a GLE error. To find the meaning of any GLE error number, follow the steps below:

- 1) Open a command prompt by clicking **Start → Run**. Type **cmd** and click **OK**.
- 2) At the command prompt, type: **net helpmsg error_number**

Example: "net helpmsg 55"

Result: The specified network resource or device is no longer available.

9.2 Frequently encountered error codes

During the operation of ERA, you may encounter error messages which contain error codes indicating a problem with some feature or operation. Section 8.2.1 below outlines the most frequently encountered error codes when performing push installs, as well as errors that can be found in the ERAS log.

9.2.1 Error messages displayed when using ESET Remote Administrator to remotely install ESET Smart Security or ESET NOD32 Antivirus

SC error code 6, GLE error code 53 Could not set up IPC connection to target computer

To set up an IPC connection, these requirements should be met:

1. TCP/IP stack installed on the computer where ERAS is installed, as well as on the target computer.
2. File and Printer Sharing for Microsoft Network must be installed.
3. File sharing ports must be open (135–139, 445).
4. The target computer must answer ping requests.

SC error code 6, GLE error code 67 Could not install ESET installer on target computer

The administrative share ADMIN\$ must be accessible on the client's system drive.

SC error code 6, GLE error code 1326 Could not set up IPC connection to target computer, probably due to a wrong username or password

Administrator's username and password have not been typed incorrectly or has not been entered at all.

SC error code 6, GLE error code 1327 Could not set up IPC connection to target computer

Administrator's password field is blank. A remote push installation cannot work with a blank password field.

SC error code 11, GLE error code 5 Could not install ESET installer on target computer

The installer cannot access the client computer due to insufficient access rights (Access Denied).

SC error code 11, GLE error code 1726 Could not install NOD32 Installer onto target computer

This error code displays after a repeated attempt to install, if the Push Installation window was not closed after the first attempt.

9.2.2 Frequently encountered error codes in era.log

0x1203 – UPD_RETVAL_BAD_URL

Update module error – incorrectly entered update server name.

0x1204 – UPD_RETVAL_CANT_DOWNLOAD

This error can appear:

- when updating through HTTP
 - update server returns an HTTP error code between 400–500 except for 401, 403, 404, and 407
 - if updates are downloaded from a CISCO based server and the HTML authentication response format has been changed
- when updating from a shared folder:
 - returned error does not fall into the categories bad authentication or file not found (e.g., connection interrupted, or non existing server, etc.)
- both update methods
 - if all of the servers listed in the file upd.ver could not be found (the file is located in %ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\updfiles)
 - failed to contact the failsafe server (probably due to deletion of the corresponding ESET entries in the registry)
- incorrect proxy server configuration in ERAS
 - The administrator must specify proxy server in the format

0x2001 – UPD_RETVAL_AUTHORIZATION_FAILED

Authentication to update server failed, incorrect username or password.

0x2102 – UPD_RETVAL_BAD_REPLY

This update module error can be encountered if a proxy server is used to mediate Internet connection – namely Webwasher proxy.

0x2104- UPD_RETVAL_SERVER_ERROR

Update module error indicating an HTTP error code higher than 500. If the ESET HTTP server is being used, error 500 indicates a problem with memory allocation.

0x2105 – UPD_RETVAL_INTERRUPTED

This update module error can be encountered if a proxy server is used to mediate the Internet connection – namely Webwasher proxy.

9.3 How to diagnose problems with ERAS?

If you suspect that there is something wrong with ERAS, or if it is not functioning correctly, we recommend that you follow these steps:

1. Check the ERAS log: Click **Tools > Server Options** from the ERAC main menu. From the **Server Options** window, click the **Logging** tab and then click **View log**.
2. If you see no error messages, increase the **Log verbosity** level in the **Server Options** window to Level 5. After you have tracked down the problem, we recommend switching back to the default value.
3. You may also be able to troubleshoot problems by turning on the database debug log in the same tab – see **Debug Log**. We recommend that you only activate the **Debug log** when attempting to duplicate the problem.
4. If you see any error codes other than those mentioned in this documentation, please contact ESET Customer Care. Please describe the behavior of the program, how to replicate the problem or how to avoid it. It is very important to include the program version of all ESET security products involved (i.e., ERAS, ERAC, ESET Smart Security, ESET NOD32 Antivirus).

10. Hints & tips

10.1 Scheduler

ESET NOD32 Antivirus and ESET Smart Security contain an integrated task scheduler which allows for scheduling regular On-demand scans, updates, etc. All specified tasks are listed in the Scheduler.

The following four types of tasks can be configured using ERA:

- Run external application
- System startup file check
- On-demand computer scan
- Update

In most cases, there is no need to configure a **Run external application** task. The task **System startup file check** is a default task and we recommend not changing its parameters⁹. From an administrator's point of view, the tasks **On-demand computer scan** and **Update** are probably the most useful:

- **On-demand computer scan**

It provides regular antivirus scan (usually of local drives) on clients.

- **Update**

This task is responsible for updating ESET client solutions. It is a predefined task and by default runs every 60 minutes. Usually there is no reason to modify its parameters. The only exception is for notebooks, since their owners often connect to the Internet outside of the local networks. In this case, the update task can be modified to use two update profiles within one task. This will allow notebooks to update from the local Mirror server, as well as from ESET's update servers.

The Scheduler setup can also be found in the ESET Configuration Editor in **ESET Smart Security / ESET NOD32 Antivirus > ESET Kernel > Setup > Scheduler/Planner > Scheduler/Planner > Edit**.

For more information see section 3.7, "ESET Configuration Editor".

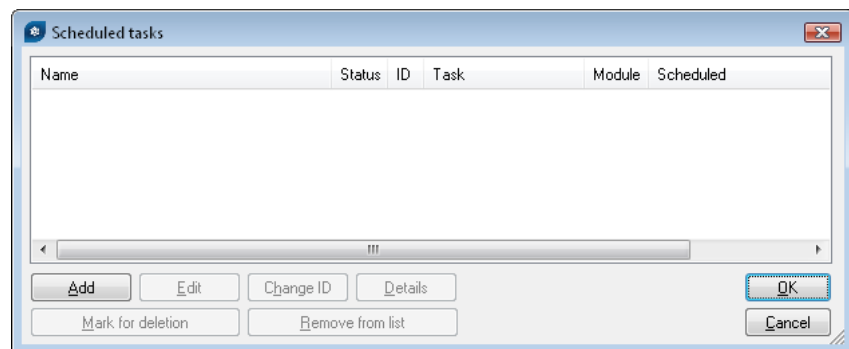


Figure 9-1

The dialog window may contain existing tasks (click **Edit** to modify them), or it may be empty. It depends on whether you have opened a configuration from a client (e.g., from a previously configured and working client), or opened a new file with the default template containing no tasks.

Every new task is assigned an attribute ID. Default tasks have decimal IDs (1, 2, 3...) and custom tasks are assigned hexadecimal keys (e.g., 4AE13D6C), which are automatically generated when creating a new task.

If the check box for a task is selected, it means that the task is active and that it will be performed on the given client.

The buttons in the Scheduled tasks window function in the following way:

- **Add** – Adds a new task
- **Edit** – Modifies selected tasks
- **Change ID** – Modifies ID of selected tasks

⁹ If no changes have been made after installation, ESET NOD32 and ESET Smart Security contain two predefined tasks of this type. The first task checks system files at each user logon, and the second task does the same after a successful virus signature database update.

- **Details** – Summary information about the selected tasks
- **Mark for deletion** – Application of.xml file will remove tasks (with the same ID) selected by clicking this button from target clients.
- **Remove from list** – Deletes selected tasks from the list. Please note that tasks removed from the list in the.xml configuration will not be removed from target workstations.

When creating a new task (**Add** button) or when editing an existing one (**Edit**), you must specify when it will run. The task can repeat after a certain period of time (each day at 12, each Friday, etc.) or it can be triggered by an event (after a successful update, the first time the computer starts each day, etc.).

The last step of the task **On-demand computer scans** shows the special settings window, where you can define which configuration will be used for scanning – i.e., which scanning profile and scan targets will be used.

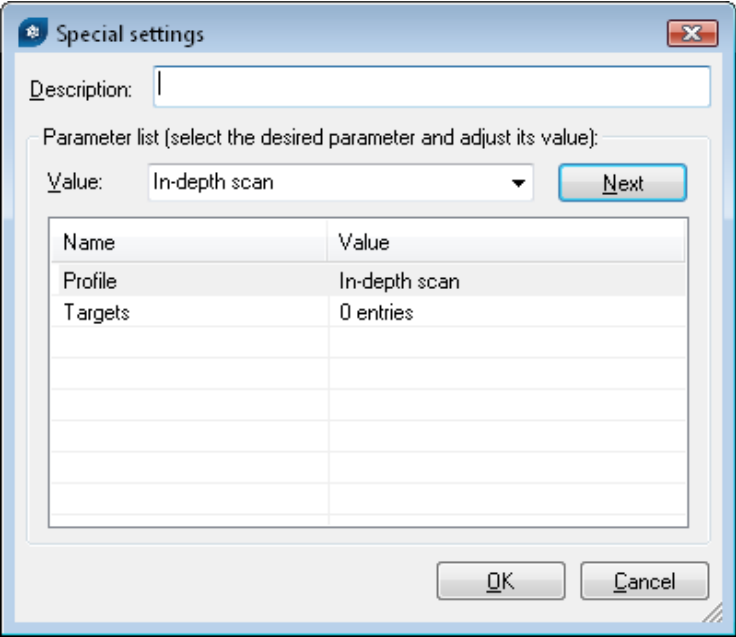


Figure 9-2

The last step of the **Update** task specifies what update profiles will run within the given task. It is a predefined task and runs every 60 minutes by default. Usually there is no reason to modify its parameters. The only exception is for notebooks, since their owners also connect to the Internet from outside of company networks. The last dialog allows you to specify two different update profiles, covering updates either from a local server or from ESET's update servers.

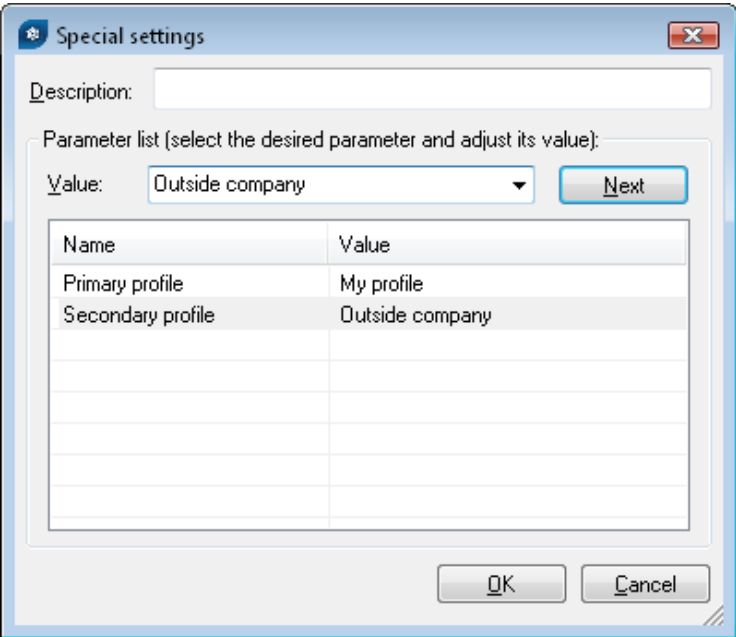


Figure 9-3

10.2 Removing existing profiles

Occasionally you may come across duplicate profiles (either update or scan profiles) that were created by mistake. To remove those profiles remotely without damaging other settings in the Scheduler, follow the steps below:

- From ERAC, click the **Clients** tab and then double-click a problematic client.
- From the **Client Properties** window, click the **Configuration** tab. Select the **Then Run ESET Configuration Editor to edit the file** and **Use the downloaded configuration in the new configuration task** options and then click the **New Task** button.
- In the new task wizard, click **Edit**.
- In the Configuration Editor, press **CTRL + D** to deselect (grey) all settings. This helps prevent accidental changes, as any new changes will stand out in blue.
- Right-click on the profile you wish to remove and select **Mark profile for deletion** from the context menu. The profile will be deleted as soon as the task is delivered to clients.

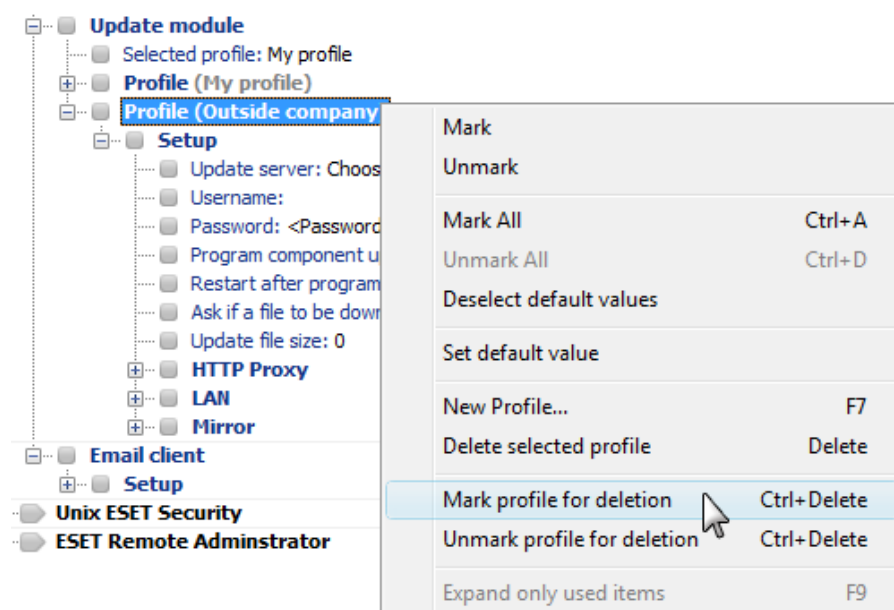


Figure 9-4

- Click the **Console** button in the ESET Configuration Editor and save the settings.
- Verify that the client you selected is in the **Selected items** column on the right. Click **Next** and then click **Finish**.

10.3 Export and other features of client XML configuration

From ERAC, select any clients in the **Clients** tab. Right-click and select **Configuration...** from the context menu. Click **Save As...** to export the assigned configuration of the given client to an.xml file¹⁰. 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 (no new configuration is created, only assigned by the **Select...** button).

Example: An ESET security product is only installed on one workstation. Adjust the settings directly through the program's user interface. When finished, export the settings to an.xml file. This.xml file can then be used for remote installations to other workstations. This method can be very useful for tasks such as fine-tuning firewall rules, if the "Policy-based" mode is to be applied.

10.4 Combined update for notebooks

If there are any mobile devices in your local network (i.e., notebooks), we recommend that you configure a combined update from two sources: ESET's update servers and the local Mirror server. First, notebooks contact

¹⁰ .xml configuration files can also be extracted directly from the ESET Smart Security program interface.

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 the **Update** branch and select **New profile** from the context menu.

The result of modifications should resemble the one displayed below:

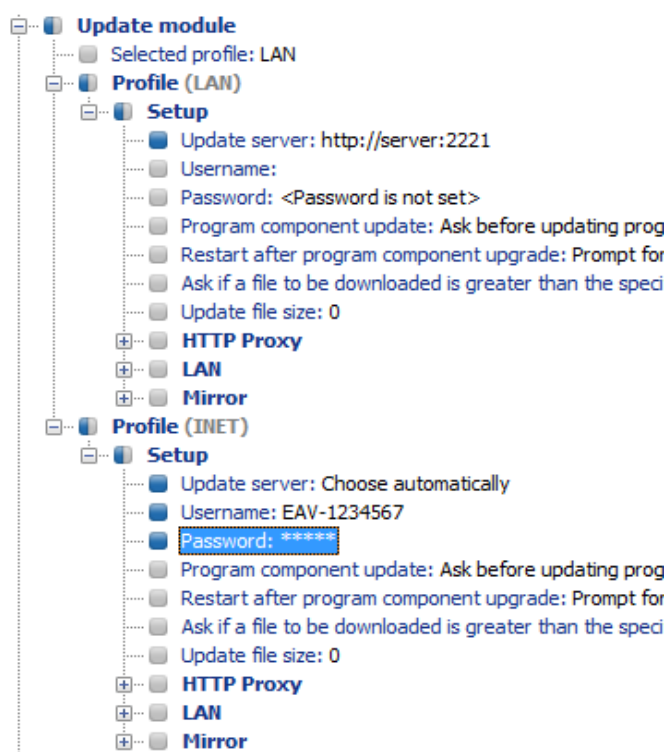


Figure 9-5

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 Security, ESET NOD32 Antivirus > Kernel > Setup > Scheduler/Planner** in the ESET Configuration Editor. Click the **Edit** button to display the **Scheduled tasks** window.

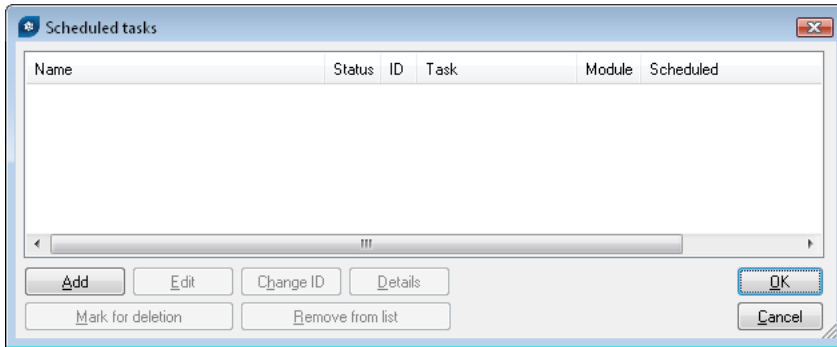


Figure 9-6

To create a new task, click **Add**. From the **Scheduled task** drop-down menu, select **Update** and click **Next**. Enter the **Task name** (e.g., "combined update"), select **Repeatedly every 60 minutes** and proceed to the selection of a primary and secondary profile.

If the notebook workstations should contact the Mirror server first, the Primary profile should be set to LAN and the Secondary profile should be set to INET. The profile INET would only be applied if the update from LAN fails.

Recommendation: Export the current.xml configuration from a client (for more information, see section 9.3) and perform the above-mentioned modifications on the exported.xml file. This will prevent any duplication between the Scheduler and non-working profiles.

10.5 Installation of third-party products using ERA

In addition to remote installation of ESET products, ESET Remote Administrator is capable of installing other programs. The only requirement is that the custom install package must be in the.msi format. The remote installation of custom packages can be performed using a process very similar to the one described in section 4.2, "Remote installation".

The main difference is in the package creation process, which is as follows:

- From ERAC, click the **Remote Install** tab.
- Click the **Packages...** button.
- From the **Package type** drop-down menu select **Custom package**.
- Click **Add...**, click **Add file** and select the desired msi package.
- Select the file from the **Package Entry File** drop-down menu and click **Create**.
- After returning to the original window you can specify command line parameters for the.msi file. The parameters are the same as for a local installation of the given package.
- Click **Save as...** to save the package.
- Click **Close** to exit the installation package editor.

The newly created custom package can be distributed to client workstations in the same manner as the remote installations described in previous chapters. A remote push install, logon or email push install will send the package to target workstations. From the moment the package is executed, installation is handled by the Microsoft Windows Installer service.