Single Product Review

ESET Remote Administrator 6

Language: English
November 2014
Last Revision: 19th December 2014

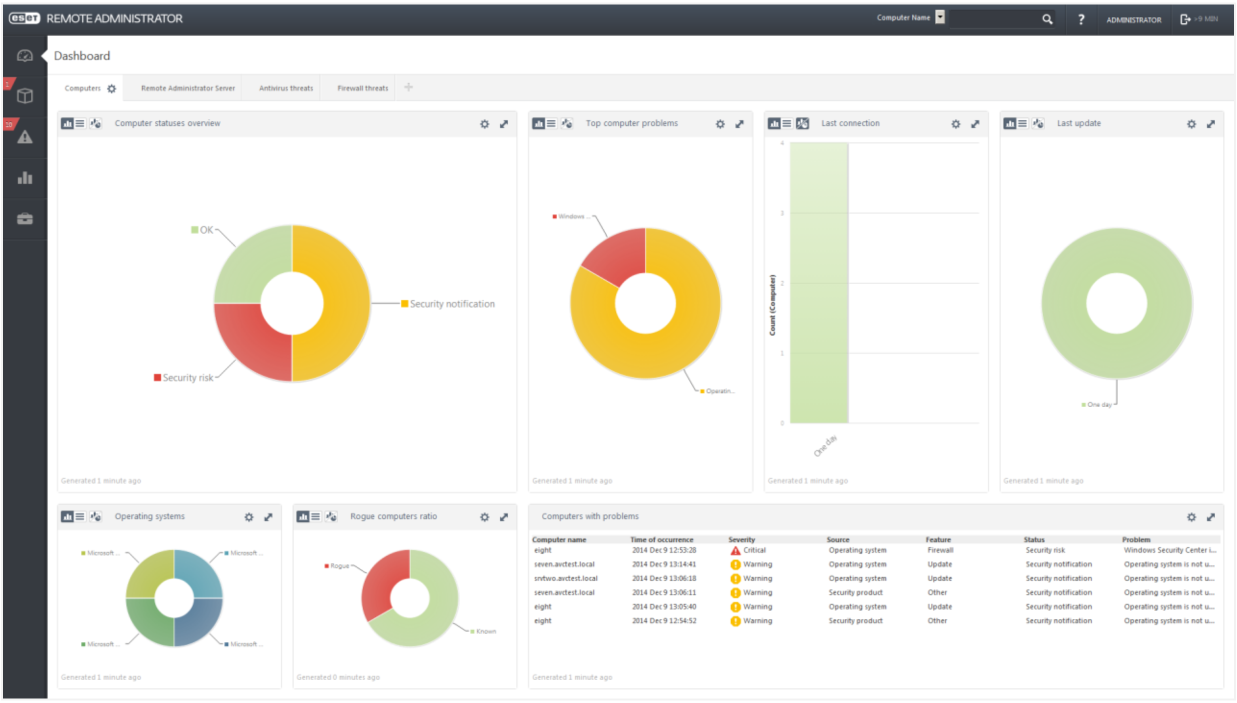
www.av-comparatives.org

Test commissioned by the vendor of the product.

Introduction

This review of ESET Remote Administrator 6 has been commissioned by ESET.

ESET Remote Administrator 6



Computer name	Time of occurrence	Severity	Source	Feature	Status	Problem
eight	2014 Dec 9 12:53:28	⚠ Critical	Operating system	Firewall	Security risk	Windows Security Center i...
seven.avctest.local	2014 Dec 9 13:14:41	! Warning	Operating system	Update	Security notification	Operating system is not u...
srvtwo.avctest.local	2014 Dec 9 13:06:18	! Warning	Operating system	Update	Security notification	Operating system is not u...
seven.avctest.local	2014 Dec 9 13:06:11	! Warning	Security product	Other	Security notification	Operating system is not u...
eight	2014 Dec 9 13:05:40	! Warning	Operating system	Update	Security notification	Operating system is not u...
eight	2014 Dec 9 12:54:52	! Warning	Security product	Other	Security notification	Operating system is not u...

Generated 1 minute ago

ESET Remote Administrator is a management console used to deploy and manage ESET endpoint protection software for PCs and mobile devices. It consists of two components, although these can be installed together on one server and then function as a single unit. The Server component is the functionality, and the Web Console provides the user interface via a web browser. This review covers the console as a whole, along with the ESET Endpoint Security and Endpoint Antivirus clients for Windows desktop systems, and ESET File Security for file servers running Windows Server.

Software versions reviewed

- ESET Remote Administrator (Server), Version 6.1.257.0
- ESET Remote Administrator (Web Console), Version 6.1.208.0
- ESET Endpoint Security 6.1.2102.0
- ESET Endpoint Antivirus 6.1.2102.0
- ESET File Security 6.0.12023.0

SUPPORTED WINDOWS OPERATING SYSTEMS

ESET Remote Administrator 6 server

Microsoft Windows Server 2012R2, 2012, 2008R2, 2008, 2003

Microsoft Windows Desktop operating systems are not officially supported, software can be installed for evaluation purposes.

ESET File Security 6

Microsoft Windows Server 2012R2, 2012, 2008R2, 2008, 2003

ESET Endpoint Security 6

Microsoft Windows 8.1, 8, 7, Vista, XP

ESET security software supported by the console

ESET Endpoint Security version 6, 5, ESET Smart Security Business Edition 4.2; Endpoint Antivirus versions 6, 5, ESET NOD32 Antivirus Business Edition 4.2, ESET Endpoint Security 6 for OS X, ESET Endpoint Antivirus 6 for OS X, ESET NOD32 Antivirus Business Edition for Mac OS X, ESET NOD32 Antivirus Business Edition for Linux Desktop, ESET File Security for Microsoft Windows Server version 6, 4.5, ESET Endpoint Security 2 for Android.

OTHER SUPPORTED PLATFORMS

ESET Remote Administrator for other platforms

Linux – majority of business Linux Distributions (SUSE, RedHat, CentOS, uBuntu, Debian, Fedora).

Other platforms that can be managed by Remote Administrator 6

OS X 10.10 Yosemite, 10.9 Mavericks, 10.8 Snow Leopard, 10.7 Leopard

Linux Desktop – majority of business Linux Distributions (SUSE, RedHat, CentOS, uBuntu, Debian, Fedora).

Android 4.0 and higher

VIRTUAL APPLIANCES AVAILABLE

ESET Remote Administrator is available as a preconfigured Linux virtual appliance in .ova format that natively support VMware ecosystem (VMware vSphere / VMware Player).

Test system

For our review, we set up a Windows domain with four test machines, all using 64-bit Windows. These are listed below, along with a note on the ESET products we installed:

Windows Server 2012 R2, domain controller and DNS server; local installation of ESET File Security 4 (to test the agent’s ability to recognise and report older versions of the product)

Windows Server 2008 R2, member server; Remote Administrator Server and Web Console; push installation of ESET File Security 6

Windows 8.1 Professional client, push installation of ESET Endpoint Security 6

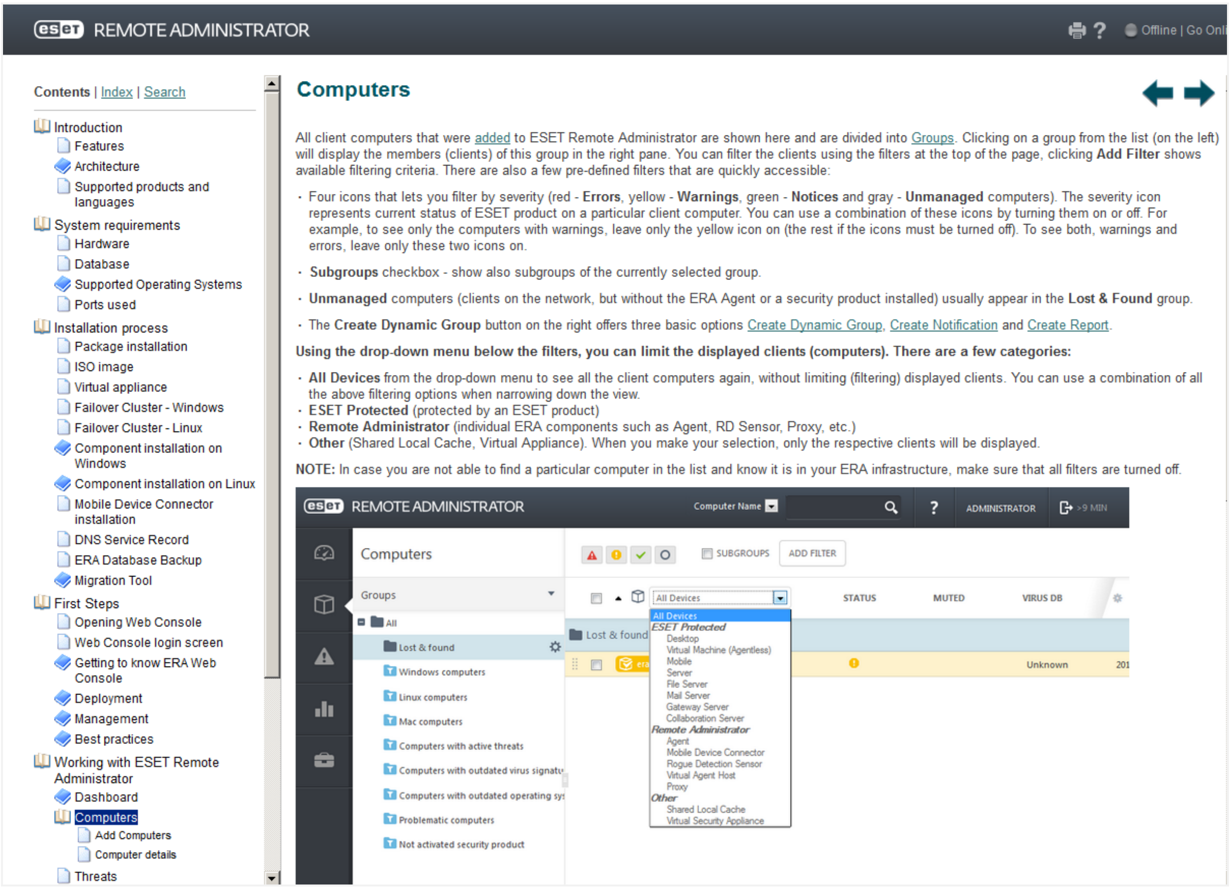
Windows 7 SP1 Professional client, push installation of ESET Endpoint Antivirus 6

Features of ESET Endpoint Security 6

Anti-malware; anti-phishing; anti-spam; firewall; web-access control; device control.

Console documentation

Local help: Clicking the ***?*** symbol in the bar at the top of the console window opens the web-based local help service. Like a Windows Help file, this has a list of topics in a left-hand panel, with the instructions for each topic shown in the larger right-hand panel:



Computers

All client computers that were added to ESET Remote Administrator are shown here and are divided into Groups. Clicking on a group from the list (on the left) will display the members (clients) of this group in the right pane. You can filter the clients using the filters at the top of the page, clicking **Add Filter** shows available filtering criteria. There are also a few pre-defined filters that are quickly accessible:

- Four icons that lets you filter by severity (red - **Errors**, yellow - **Warnings**, green - **Notices** and gray - **Unmanaged** computers). The severity icon represents current status of ESET product on a particular client computer. You can use a combination of these icons by turning them on or off. For example, to see only the computers with warnings, leave only the yellow icon on (the rest if the icons must be turned off). To see both, warnings and errors, leave only these two icons on.
- **Subgroups** checkbox - show also subgroups of the currently selected group.
- **Unmanaged** computers (clients on the network, but without the ERA Agent or a security product installed) usually appear in the **Lost & Found** group.
- The **Create Dynamic Group** button on the right offers three basic options Create Dynamic Group, Create Notification and Create Report.

Using the drop-down menu below the filters, you can limit the displayed clients (computers). There are a few categories:

- **All Devices** from the drop-down menu to see all the client computers again, without limiting (filtering) displayed clients. You can use a combination of all the above filtering options when narrowing down the view.
- **ESET Protected** (protected by an ESET product)
- **Remote Administrator** (individual ERA components such as Agent, RD Sensor, Proxy, etc.)
- **Other** (Shared Local Cache, Virtual Appliance). When you make your selection, only the respective clients will be displayed.

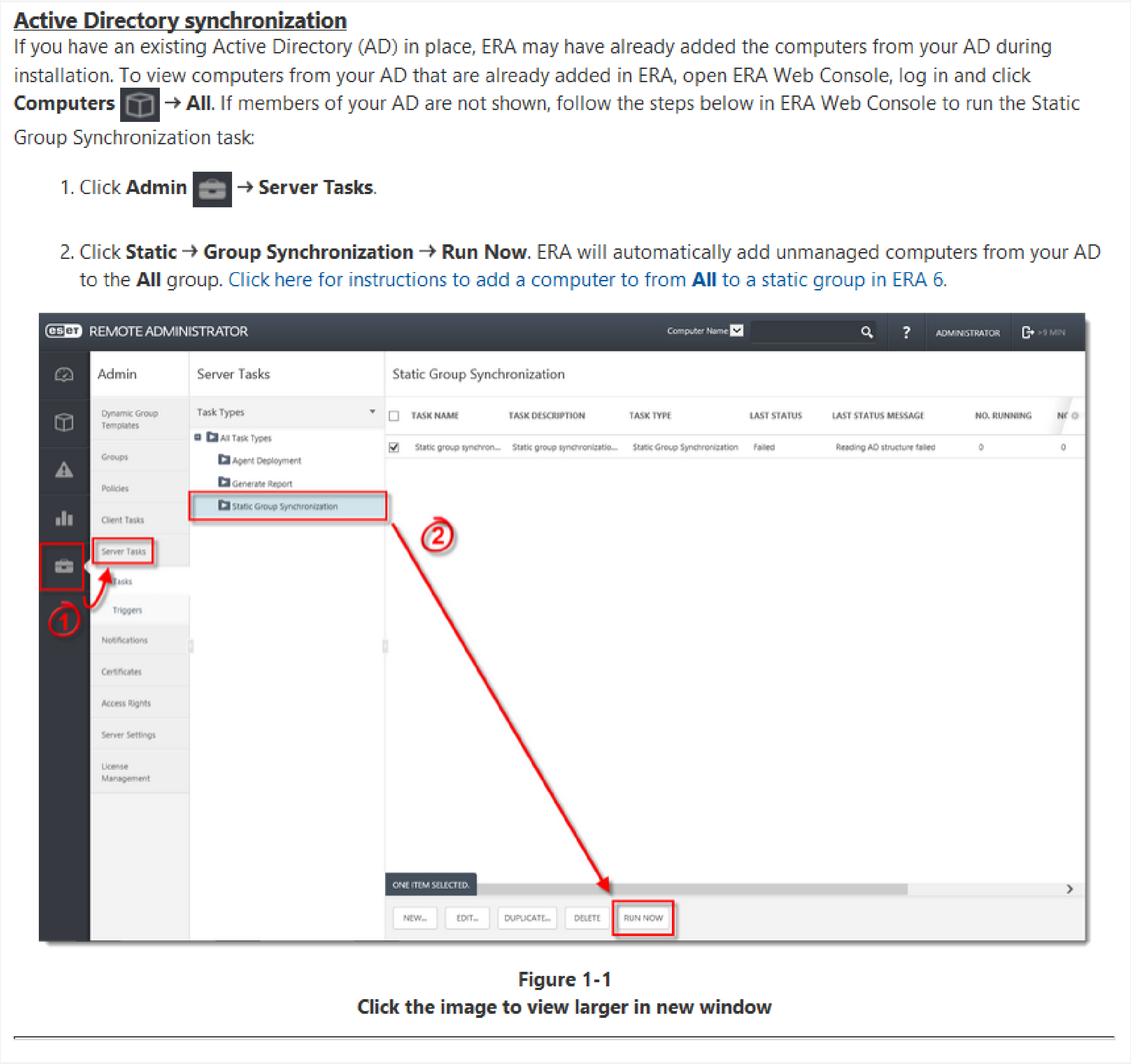
NOTE: In case you are not able to find a particular computer in the list and know it is in your ERA infrastructure, make sure that all filters are turned off.

The list of help topics is comprehensive, and we found the instructions to be clear and simple, with a fair number of screenshots.

Manuals: ESET produce two manuals for Remote Administrator 6, namely a *Quick Start Guide* (60 pages), and *an Installation Manual & User Guide* (206 pages). The Quick Start Guide provides detailed and comprehensive information regarding installation of Remote Administrator, including supported operating systems, additional software such as .NET Framework, firewall ports to be opened on the server, and the setup wizard itself. It also includes instructions for deploying endpoint protection software to clients, and provides a basic overview of the console and its functions. The Installation Manual & User Guide provides very detailed information of the management console, and includes a glossary of related terminology.

Knowledge Base: ESET's online knowledge base[1] provides comprehensive instructions for common tasks, as illustrated below.

[1] http://kb.eset.com/esetkb/index?page=content&id=SOLN3601&actp=search&viewlocale=en_US&searchid=1418720414755



Active Directory synchronization

If you have an existing Active Directory (AD) in place, ERA may have already added the computers from your AD during installation. To view computers from your AD that are already added in ERA, open ERA Web Console, log in and click **Computers** → **All**. If members of your AD are not shown, follow the steps below in ERA Web Console to run the Static Group Synchronization task:

1. Click **Admin** → **Server Tasks**.

2. Click **Static** → **Group Synchronization** → **Run Now**. ERA will automatically add unmanaged computers from your AD to the **All** group. Click here for instructions to add a computer to from **All** to a static group in ERA 6.

□	TASK NAME	TASK DESCRIPTION	TASK TYPE	LAST STATUS	LAST STATUS MESSAGE	NO. RUNNING	NO
☑	Static group synchron...	Static group synchronizatio...	Static Group Synchronization	Failed	Reading AD structure failed	0	0

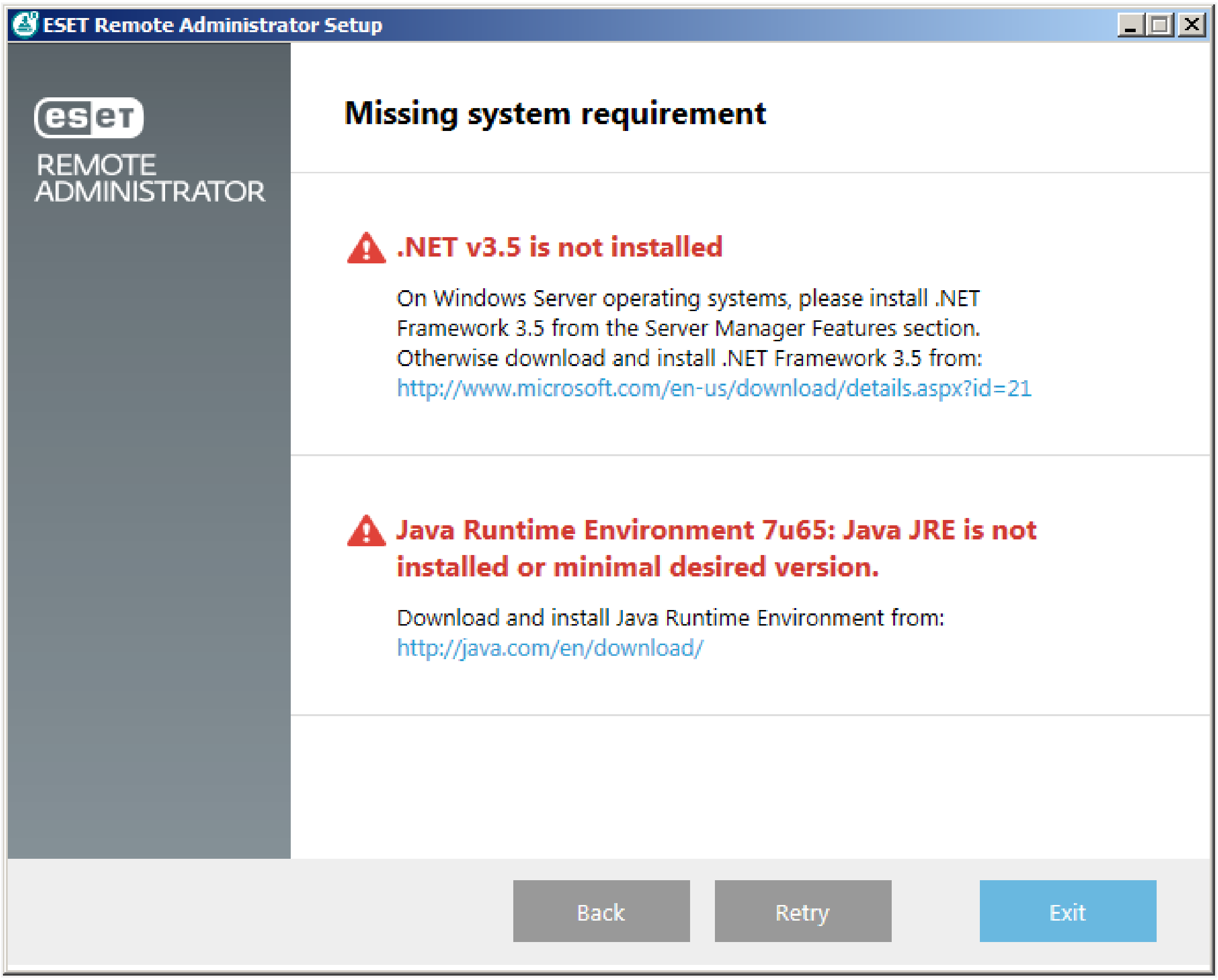
Figure 1-1
Click the image to view larger in new window

The ESET knowledge base provides outstanding assistance for common tasks. There are very clear, step-by-step instructions, very well illustrated with annotated screenshots, and some articles even include videos.

The manuals are produced to the normal very high standard we have come to expect from ESET, being well written, appropriately illustrated with screenshots, clearly laid out, and accessible via bookmarks and clickable contents pages. We read the relevant section of the appropriate manual before carrying out each task, and would highly recommend this.

Installation of the console

This involves running a single installer file, which can install both Server and Web Console products together. There are some standard steps such as accepting the licence agreement and entering a licence key. The wizard checks for prerequisite software components, and provides instructions and download links for any that are missing:



Missing system requirement

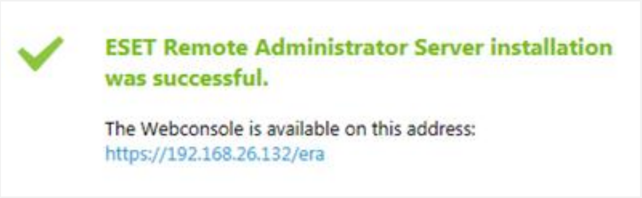
.NET v3.5 is not installed

On Windows Server operating systems, please install .NET Framework 3.5 from the Server Manager Features section. Otherwise download and install .NET Framework 3.5 from: http://www.microsoft.com/en-us/download/details.aspx?id=21

Java Runtime Environment 7u65: Java JRE is not installed or minimal desired version.

Download and install Java Runtime Environment from: http://java.com/en/download/

When the wizard has finished, the web address needed to access the console is displayed:



ESET Remote Administrator Server installation was successful.

The Webconsole is available on this address: https://192.168.26.132/era

We found installing the console to be very straightforward and trouble-free. We were able to install the .NET Framework as per the wizard's instructions, and download and install the Java Runtime Environment, without exiting the ESET wizard. When both components had been installed, we were able to continue the setup wizard by clicking the Retry button. This strikes us as very convenient.

ESET inform us that it is possible to update an installation of their previous management console, Remote Administrator 5, to the current version, using the ESET Remote Administrator Migration Wizard. This migrates the contents of the old database into the new one, and help with deployment of the new agent to machines previously managed by the older console. ESET also say that they are developing a post-install wizard, which will assist the administrator with carrying out deployment. This is to be implemented in future versions of Remote Administrator.

Preparing server and clients for deployment

Successful installation of ESET Remote Administrator 6 on the server requires the following: a valid licence; installation of Java Runtime Environment; installation of Microsoft .NET Framework; the opening of specific firewall ports. All the necessary details of these points are described in the Quick Start Guide. As noted above, the Java Runtime Environment and .NET Framework can be installed using the instructions and links provided in the Remote Administrator setup wizard.

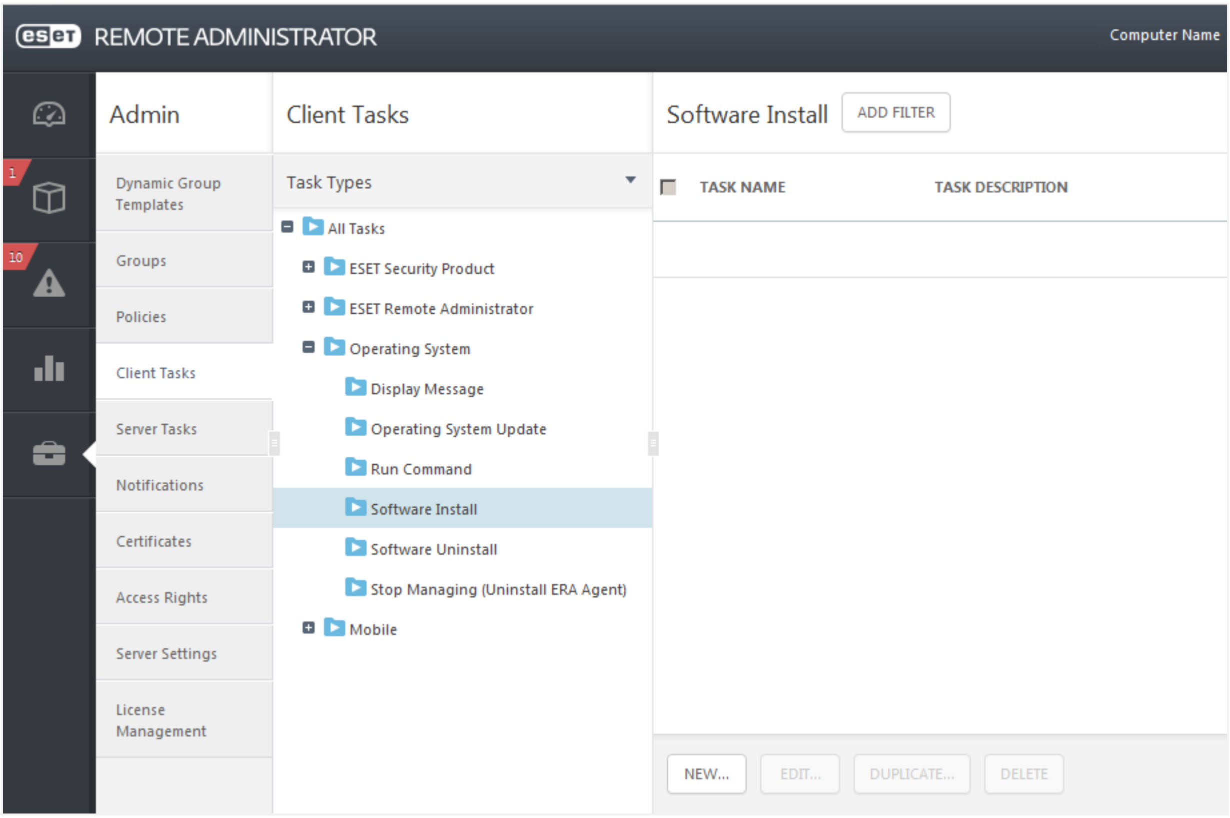
The only preparation we made to client machines before deployment was enabling *File and Printer Sharing* and *Network Discovery*.

Deploying the software

Before the endpoint protection software is deployed to clients, the ESET Agent (which enables the communication between client and management server) has to be installed on the client machines. The Agent can be installed remotely or locally. To install it remotely, a list of computers to deploy it to can be imported from Active Directory, by going to *Admin* | *Server Tasks* | *Static Group Synchronisation*. In our test, we were able to import the Computers and Domain Controllers groups very quickly and easily. It is also possible to find computers for deployment by manually typing in their IP addresses.

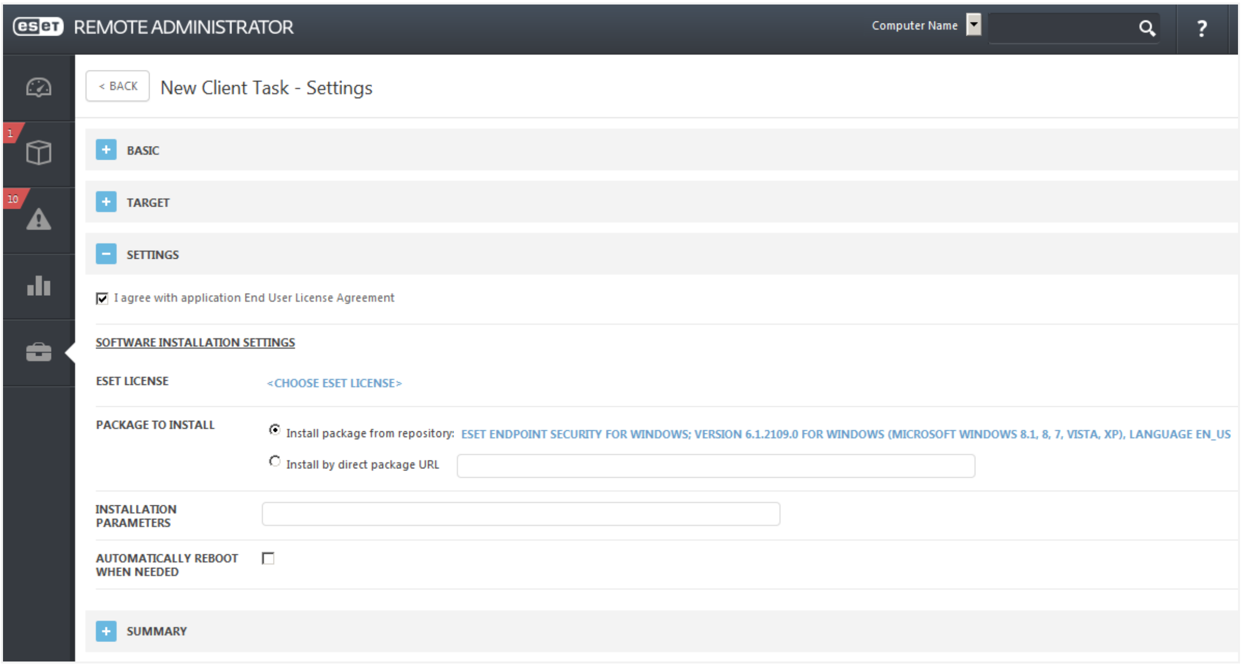
With local installation, there is a choice of putting the Agent's installer package in a shared folder and accessing it over the network from each client machine, or creating an Online Installer file to send to users by email or on a USB flash drive etc. We chose the former (Server Assisted Installation). The administrator only needs to enter the host name of the Remote Administrator server, administrator credentials, and the name of the computer group the machine is to be assigned to.

Once the agent has been deployed to the clients, the endpoint protection software can be deployed from the console. This is done by clicking the *Admin* tab, *Client Tasks*, *Software Install*, *New*; the *Client Tasks* page is shown below:



The admin then needs to enter details into the task page, such as target computers, the software package to be installed, license, administrator account credentials, and a trigger. Possible triggers include “as soon as possible”, a specific scheduled time, when a computer joins a dynamic group, or a specified Event Log event. Once *Finish* has been clicked, the installation will start as soon as the trigger time/condition is reached.

An extract from the *New Client Task* page is shown below:



☑ I agree with application End User License Agreement

SOFTWARE INSTALLATION SETTINGS

ESET LICENSE <CHOOSE ESET LICENSE>

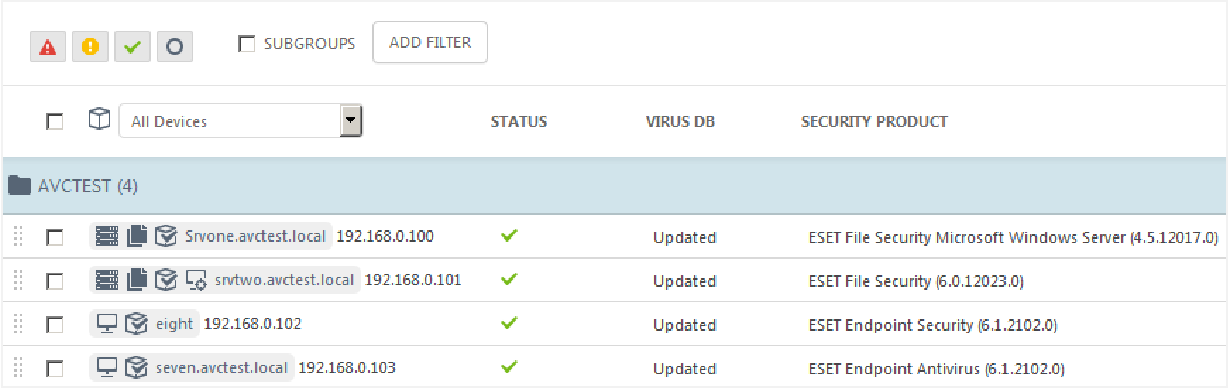
PACKAGE TO INSTALL ● Install package from repository: ESET ENDPOINT SECURITY FOR WINDOWS; VERSION 6.1.2109.0 FOR WINDOWS (MICROSOFT WINDOWS 8.1, 8, 7, VISTA, XP), LANGUAGE EN_US
○ Install by direct package URL

INSTALLATION PARAMETERS

AUTOMATICALLY REBOOT WHEN NEEDED □

We note that third-party antivirus software can be uninstalled from the console prior to installing ESET security products. This is done by creating a new task in a similar manner to an installation task but selecting *Software Uninstall | Third party antivirus software*. As our test clients had freshly installed operating systems, we were not able to test this.

When the Agent is installed on a computer, it checks for any ESET antivirus/endpoint protection software already installed (including older versions). If any is found, the agent reports this to the management server, and the existing security product can be managed from the Remote Administrator console. We tested this by installing an older version of ESET File Security (4.5) on our second server, and then deploying the RA6 Agent. After just a few minutes, the server itself and its existing ESET software were displayed in the console, along with the version 6 products:



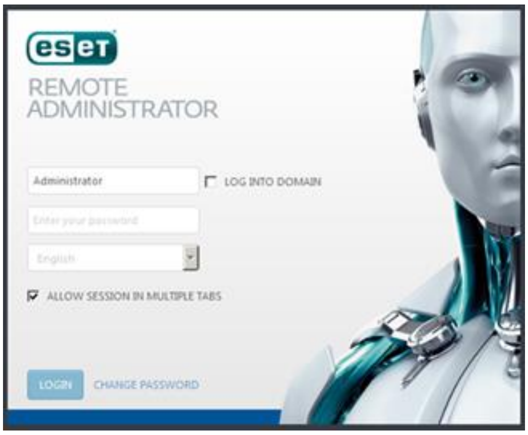
AVCTEST (4)

All Devices	STATUS	VIRUS DB	SECURITY PRODUCT
Srvone.avctest.local 192.168.0.100	✓	Updated	ESET File Security Microsoft Windows Server (4.5.12017.0)
srvtwo.avctest.local 192.168.0.101	✓	Updated	ESET File Security (6.0.12023.0)
eight 192.168.0.102	✓	Updated	ESET Endpoint Security (6.1.2102.0)
seven.avctest.local 192.168.0.103	✓	Updated	ESET Endpoint Antivirus (6.1.2102.0)

The deployment procedures for the agent as well as the endpoint protection software are clearly explained, using abundant screenshots, in the Quick Start Guide. We found both to be very straightforward.

Management Console

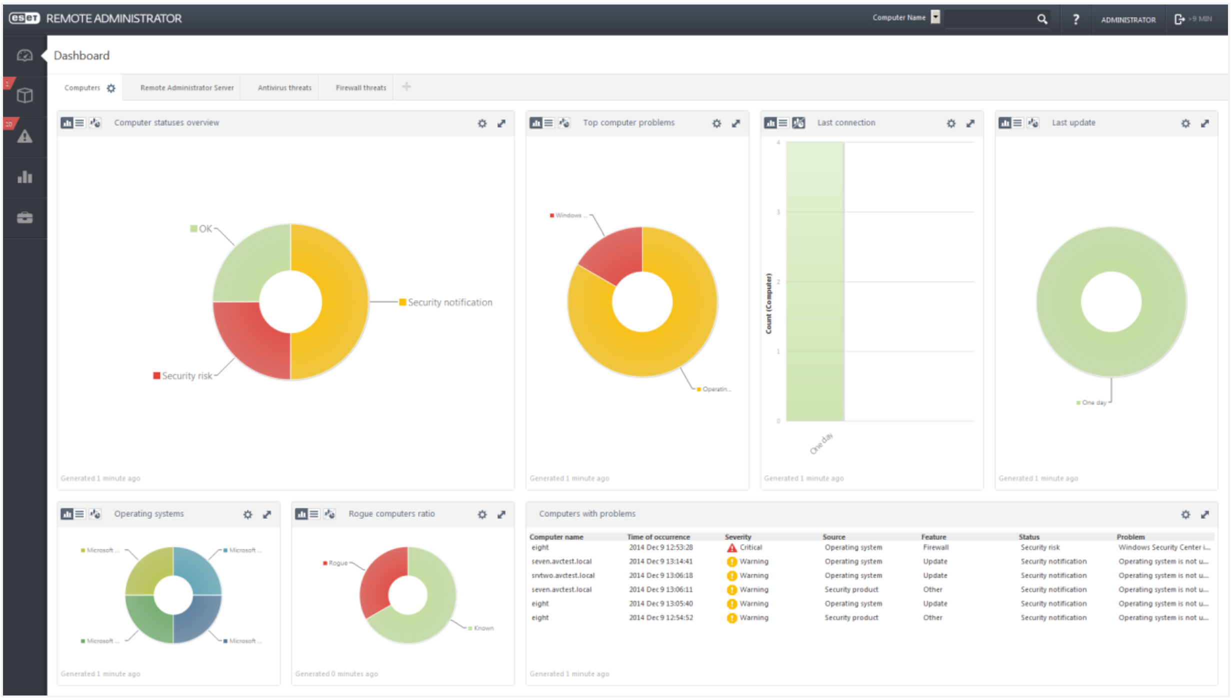
Login screen:



By default, the administrator is automatically logged out of the console after 9 minutes of inactivity. It is possible to create additional user accounts to be used with the console, by clicking *Admin | Access Rights*. ESET inform us that it is possible to assign specific rights to each user, so that a user can have e.g. just read-only permissions, with unavailable functions hidden.

Dashboard page

By default, the console shows the Computers tab of the Dashboard page. This displays the status of the computers on the networks as a number of pie charts. These include the computer status overview (proportions with/without problems); nature of the problem (if applicable); last update; last connection; percentage of different operating systems; details of problem computers.

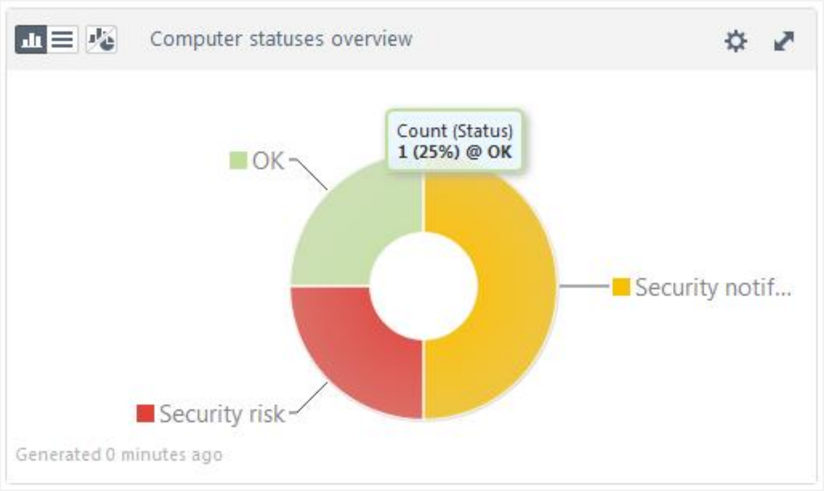


Computers with problems

Computer name	Time of occurrence	Severity	Source	Feature	Status	Problem
eight	2014 Dec 9 12:53:28	Critical	Operating system	Firewall	Security risk	Windows Security Center i...
seven.avctest.local	2014 Dec 9 13:14:41	Warning	Operating system	Update	Security notification	Operating system is not u...
srvtwo.avctest.local	2014 Dec 9 13:06:18	Warning	Operating system	Update	Security notification	Operating system is not u...
seven.avctest.local	2014 Dec 9 13:06:11	Warning	Security product	Other	Security notification	Operating system is not u...
eight	2014 Dec 9 13:05:40	Warning	Operating system	Update	Security notification	Operating system is not u...
eight	2014 Dec 9 12:54:52	Warning	Security product	Other	Security notification	Operating system is not u...

Generated 1 minute ago

Moving the mouse over a specific area of a graph shows a screen tip with details; for example, in the *Computer Statuses Overview* tile shown below, the number of machines (1) and percentage of the total (25%) for the green section – Status OK – is shown:

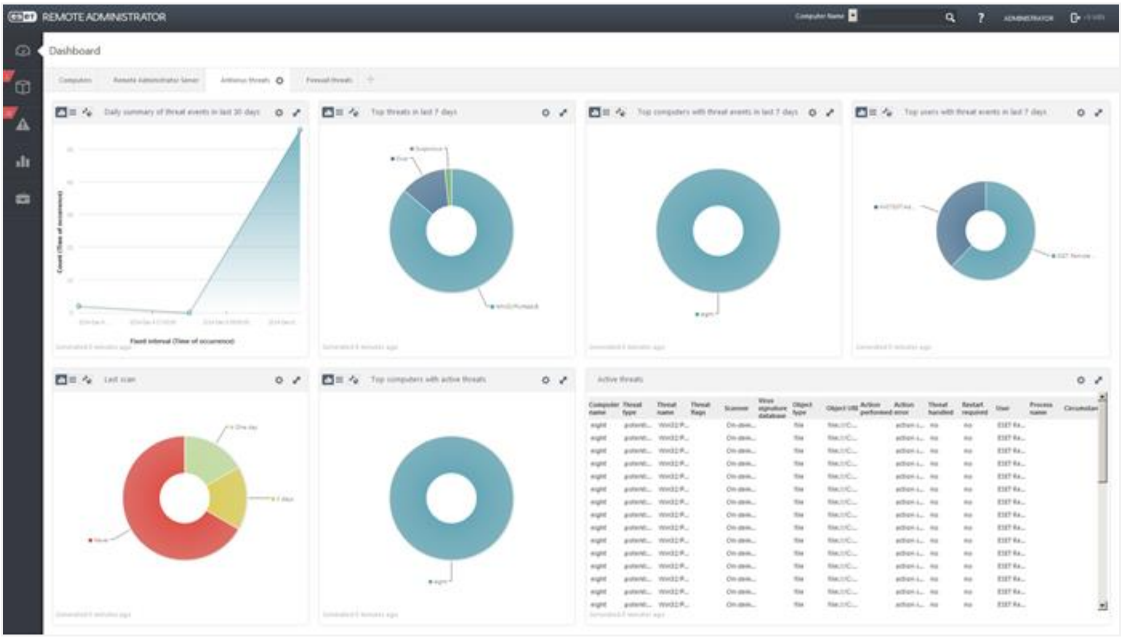


The Dashboard has three other tabs, accessed by the tab bar at the top of the pane.

These are *Remote Administrator Server, Antivirus Threats,* and *Firewall Threats*.

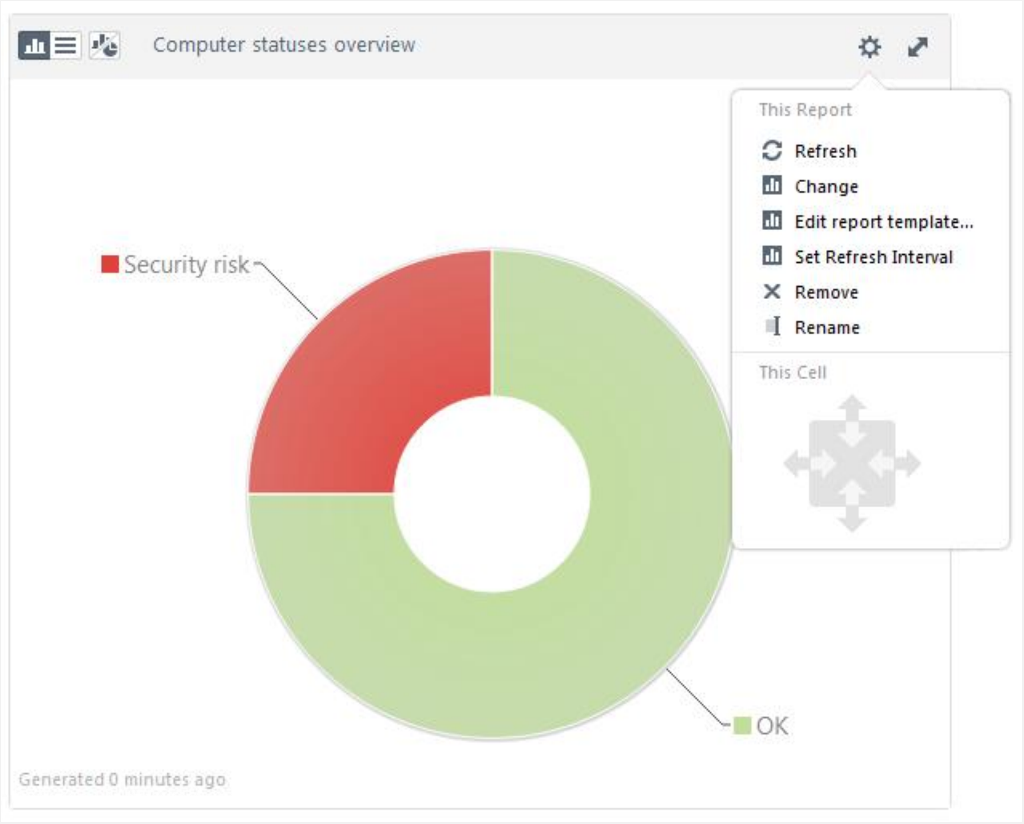
The *Remote Administrator Server* tab shows server performance items such as server network load, CPU load, database load and memory load.

The *Antivirus Threats* tab displays information on detected malware threats, including threats by user and computer, and date of last scan. This is shown below:



The *Firewall Threats* tab shows threats detected by ESET Endpoint Protection's firewall, with a very similar layout to the *Antivirus Threats* tab.

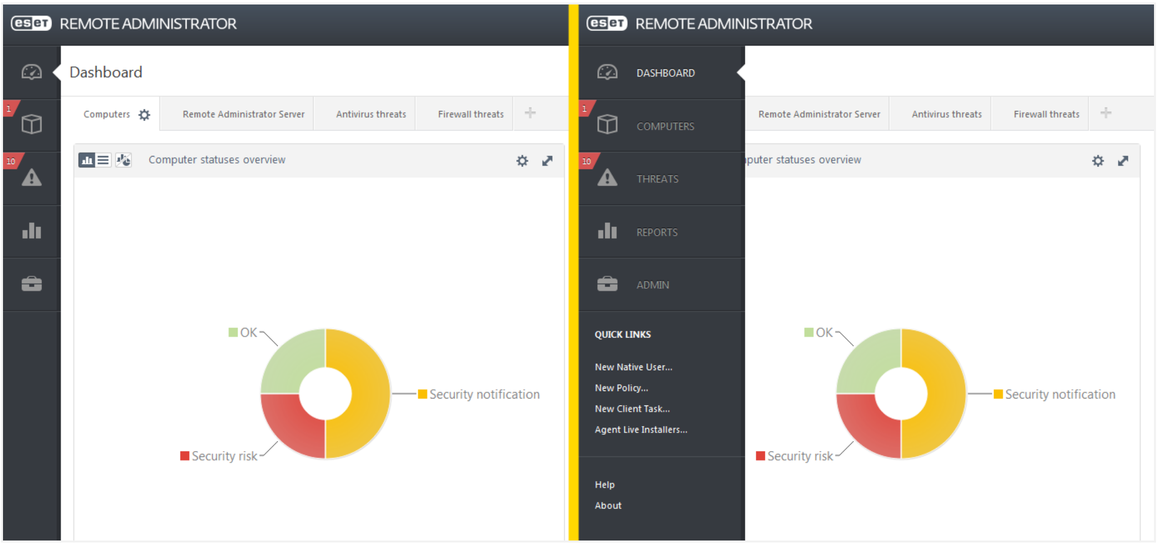
The Dashboard is highly customisable. Firstly, the type of graph displayed for each tile can be changed by clicking the cogwheel symbol top-right:



Secondly, any tile can be maximised by clicking the double-headed arrow in its top-right corner. Thirdly, individual tiles can be moved around, or removed from the display and replaced with other reports. Finally, tiles can be stretched to take up more than one space.

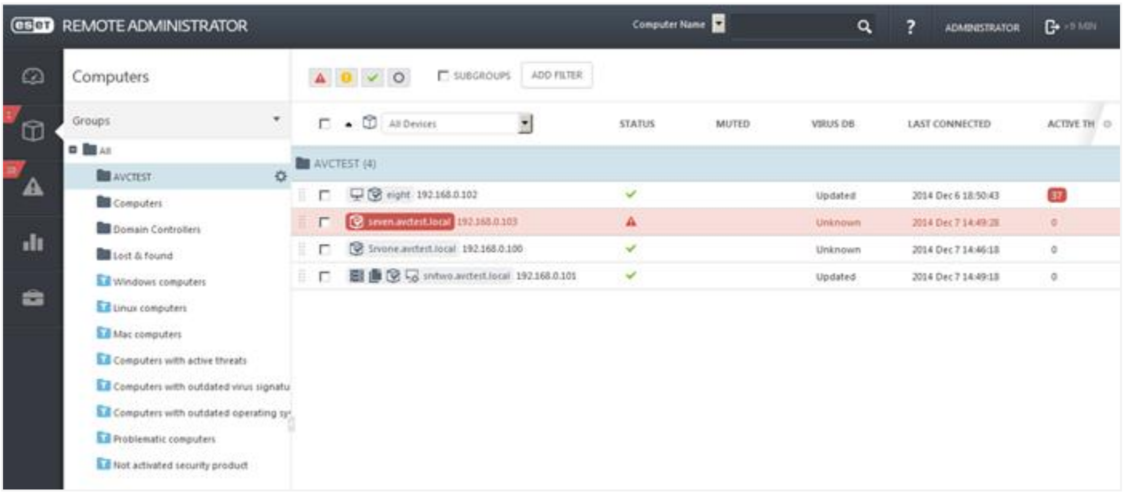
We found customising the Dashboard intuitive and very useful.

Navigating between the main pages of the console (*Dashboard, Computers, Threats, Reports, Admin*) is done using the menu bar on the left. Normally, this is minimised, as shown in the screenshot above. However, when the mouse is moved over it, it expands to show the names of each item, and additional links. This is illustrated in the 2 screenshots below, with the menu bar collapsed on the left, and expanded on the right:



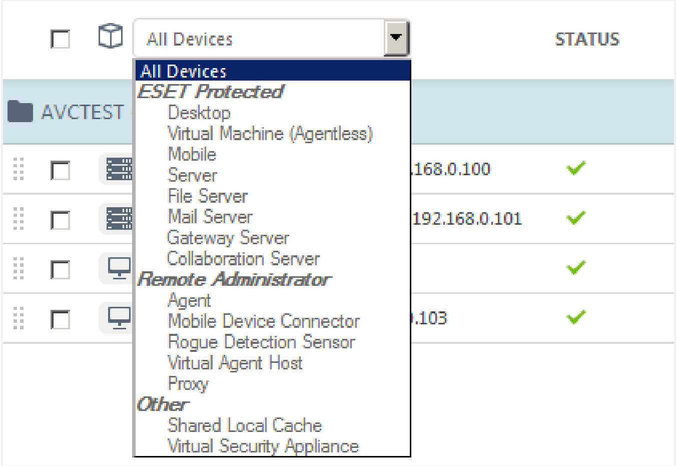
Computers page

The computers page shows the network's computers as computer groups and group members (i.e. individual computers):



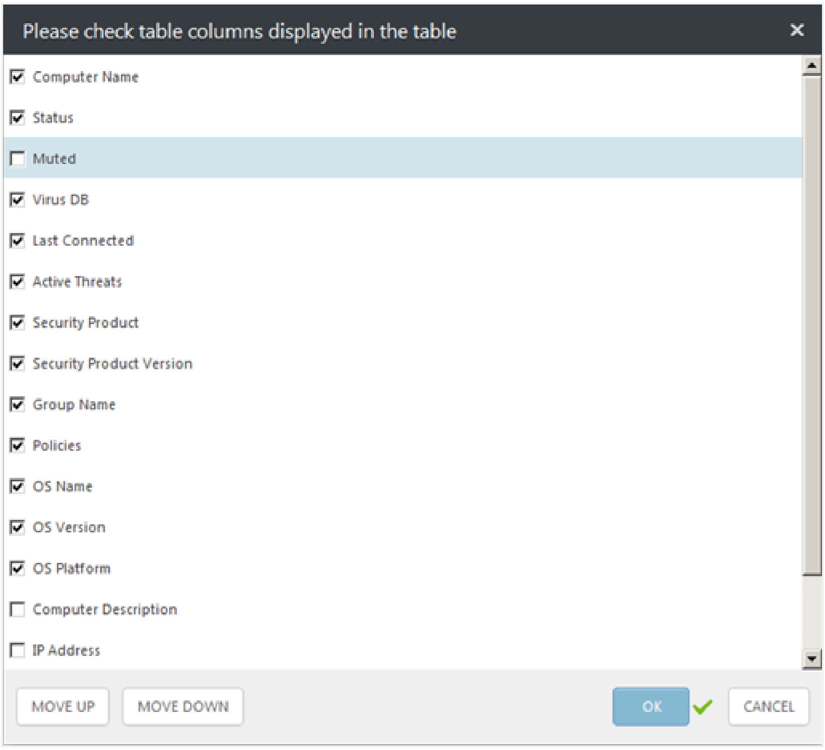
All Devices	STATUS	MUTED	VIRUS DB	LAST CONNECTED	ACTIVE TH
eight 192.168.0.102	✓		Updated	2014 Dec 6 18:50:43	37
seven.avctest.local 192.168.0.103	⚠		Unknown	2014 Dec 7 14:49:28	0
Srvone.avctest.local 192.168.0.100	✓		Unknown	2014 Dec 7 14:46:18	0
srvtwo.avctest.local 192.168.0.101	✓		Updated	2014 Dec 7 14:49:18	0

It is possible to filter the Computers page by device type:



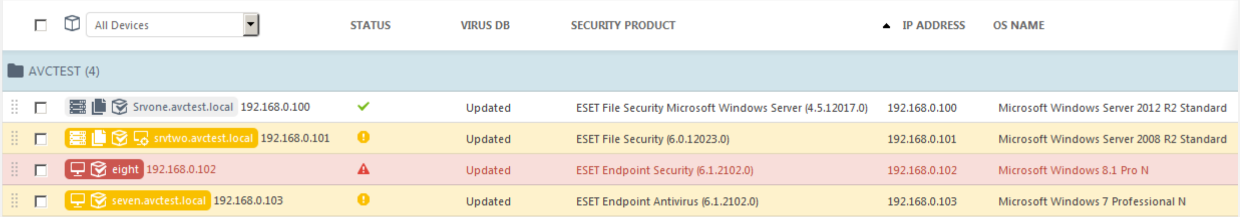
The standard layout shows the following columns: *Computer name; Status; Muted; Virus DB; Last Connected; Active Threats; Security Product; Security Product Version; Group Name; Policies; OS Name; OS Version* (precise version number); *OS Platform* (=architecture).

It is however easy to customise the columns and their order, by clicking the cogwheel in the top right of the window, then *Edit Columns*:


Please check table columns displayed in the table

☑ Computer Name
☑ Status
□ Muted
☑ Virus DB
☑ Last Connected
☑ Active Threats
☑ Security Product
☑ Security Product Version
☑ Group Name
☑ Policies
☑ OS Name
☑ OS Version
☑ OS Platform
□ Computer Description
□ IP Address

The diagram below shows how we customised ours:

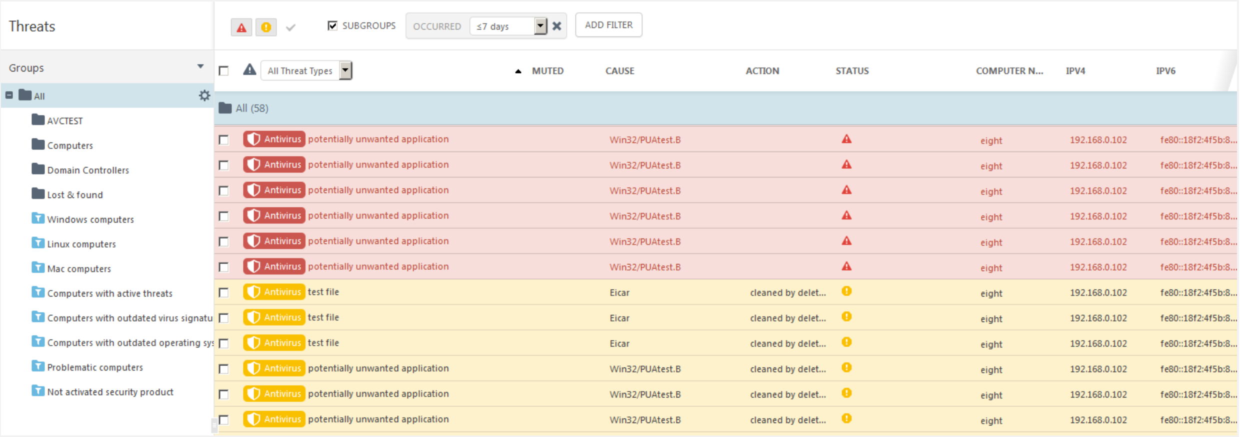


□ All Devices	STATUS	VIRUS DB	SECURITY PRODUCT	▲ IP ADDRESS	OS NAME
AVCTEST (4)					
□ Srvone.avctest.local 192.168.0.100	✓	Updated	ESET File Security Microsoft Windows Server (4.5.12017.0)	192.168.0.100	Microsoft Windows Server 2012 R2 Standard
□ srvtwo.avctest.local 192.168.0.101	!	Updated	ESET File Security (6.0.12023.0)	192.168.0.101	Microsoft Windows Server 2008 R2 Standard
□ eight 192.168.0.102	⚠	Updated	ESET Endpoint Security (6.1.2102.0)	192.168.0.102	Microsoft Windows 8.1 Pro N
□ seven.avctest.local 192.168.0.103	!	Updated	ESET Endpoint Antivirus (6.1.2102.0)	192.168.0.103	Microsoft Windows 7 Professional N

We very much like the ability to customise the *Computers* page, so that the administrator can change the items shown, and their order, to his/her particular requirements.

Computer threats page

This has a similar layout to the *Computers* page:



Threats

⚠ ❗ ✓ ☑ SUBGROUPS OCCURRED ≤7 days ✖ ADD FILTER

Groups

- All
  - AVCTEST
  - Computers
  - Domain Controllers
  - Lost & found
  - Windows computers
  - Linux computers
  - Mac computers
  - Computers with active threats
  - Computers with outdated virus signatu
  - Computers with outdated operating sys
  - Problematic computers
  - Not activated security product

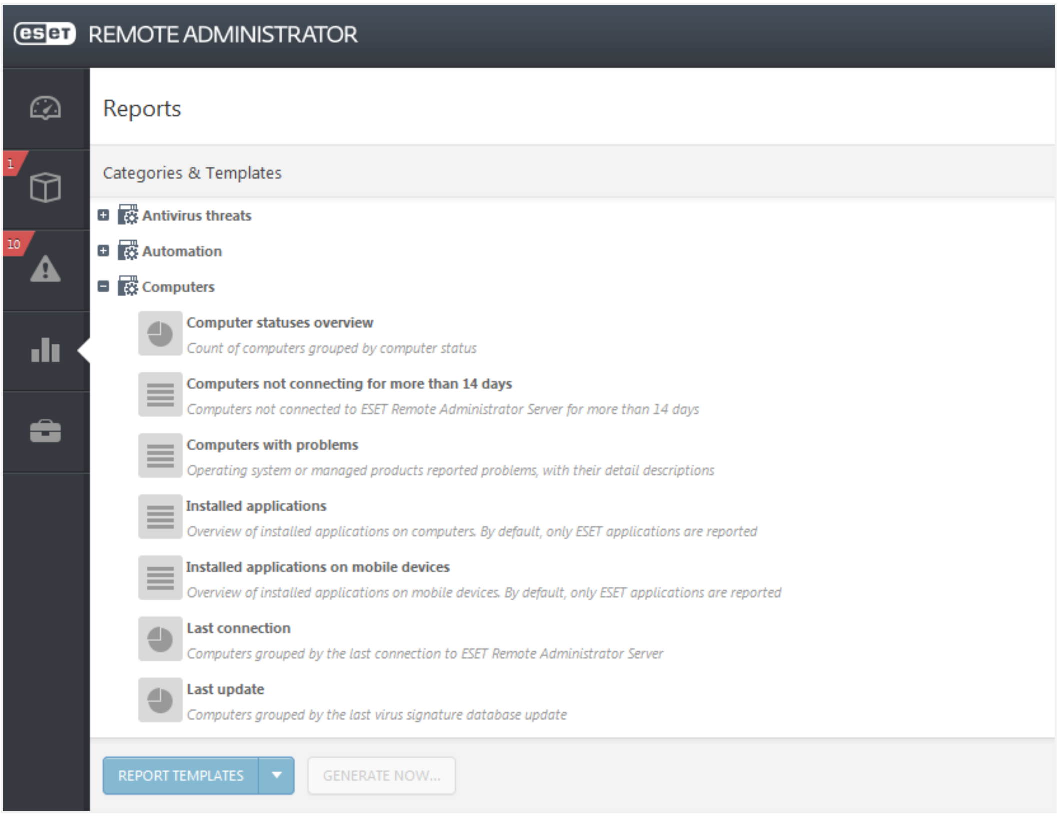
All (58)

☐	⚠ All Threat Types	▲ MUTED	CAUSE	ACTION	STATUS	COMPUTER N...	IPV4	IPV6
☐	Antivirus potentially unwanted application		Win32/PUAtest.B		⚠	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus potentially unwanted application		Win32/PUAtest.B		⚠	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus potentially unwanted application		Win32/PUAtest.B		⚠	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus potentially unwanted application		Win32/PUAtest.B		⚠	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus potentially unwanted application		Win32/PUAtest.B		⚠	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus potentially unwanted application		Win32/PUAtest.B		⚠	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus test file		Eicar	cleaned by delet...	❗	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus test file		Eicar	cleaned by delet...	❗	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus test file		Eicar	cleaned by delet...	❗	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus potentially unwanted application		Win32/PUAtest.B	cleaned by delet...	❗	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus potentially unwanted application		Win32/PUAtest.B	cleaned by delet...	❗	eight	192.168.0.102	fe80::18f2:4f5b:8...
☐	Antivirus potentially unwanted application		Win32/PUAtest.B	cleaned by delet...	❗	eight	192.168.0.102	fe80::18f2:4f5b:8...

Threats can be filtered by two types, namely antivirus and firewall. They can also be *muted*. This means that alerts for the threat are no longer shown in the menu bar, although ESET inform us that they still show up in filters and graphs. They also tell us that all alerts for a specific computer can be muted.

Reports page

This contains a very comprehensive list of events that can be included in reports, a sample of which is shown below:



Reports

Categories & Templates

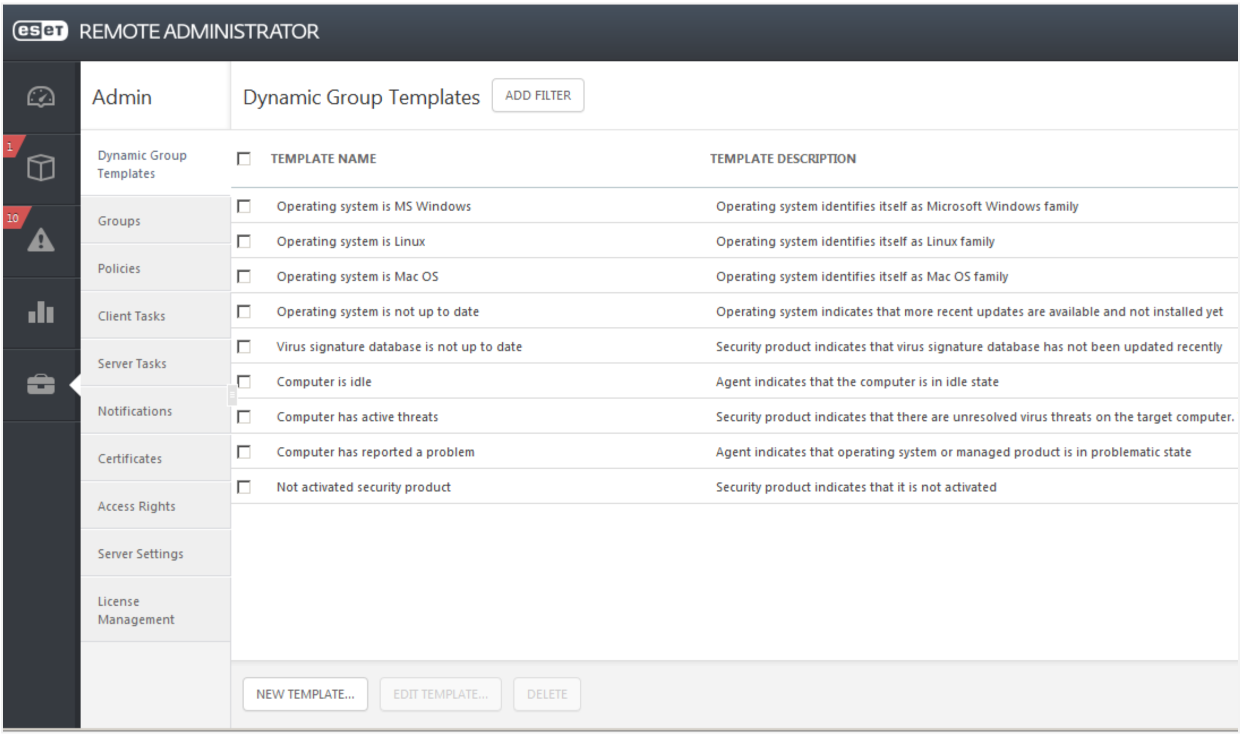
- ⊞ Antivirus threats
- ⊞ Automation
- ⊟ Computers
  - **Computer statuses overview**
    Count of computers grouped by computer status
  - **Computers not connecting for more than 14 days**
    Computers not connected to ESET Remote Administrator Server for more than 14 days
  - **Computers with problems**
    Operating system or managed products reported problems, with their detail descriptions
  - **Installed applications**
    Overview of installed applications on computers. By default, only ESET applications are reported
  - **Installed applications on mobile devices**
    Overview of installed applications on mobile devices. By default, only ESET applications are reported
  - **Last connection**
    Computers grouped by the last connection to ESET Remote Administrator Server
  - **Last update**
    Computers grouped by the last virus signature database update

Clicking the *Report Templates* button at the bottom of the page allows the admin to edit existing templates or make customised ones.

It is possible to produce a report of the *Rogue Detection Sensor*, which searches for unprotected/unregistered computers on the network, although we did not test this.

Admin page

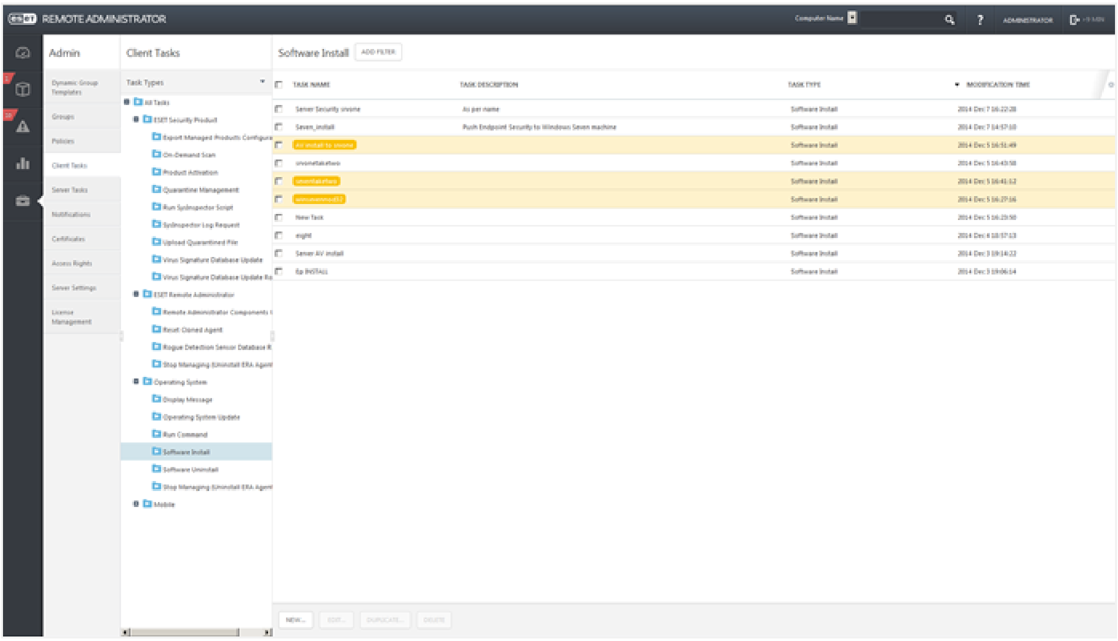
This shows a variety of tasks and settings, including Tasks for clients and servers, licence management, policies, notifications, and groups:



□	TEMPLATE NAME	TEMPLATE DESCRIPTION
□	Operating system is MS Windows	Operating system identifies itself as Microsoft Windows family
□	Operating system is Linux	Operating system identifies itself as Linux family
□	Operating system is Mac OS	Operating system identifies itself as Mac OS family
□	Operating system is not up to date	Operating system indicates that more recent updates are available and not installed yet
□	Virus signature database is not up to date	Security product indicates that virus signature database has not been updated recently
□	Computer is idle	Agent indicates that the computer is in idle state
□	Computer has active threats	Security product indicates that there are unresolved virus threats on the target computer.
□	Computer has reported a problem	Agent indicates that operating system or managed product is in problematic state
□	Not activated security product	Security product indicates that it is not activated

The page above shows the *Dynamic Group Templates* page. A computer is only shown in a dynamic group when specific, changeable criteria apply, e.g. the computer has reported a threat, or the operating system is not up to date. This allows the administrator to see which computers meet the specified criteria at any one time. ESET inform us that a computer can be a member of multiple dynamic groups at one time, but only one static group. They also tell us that membership of dynamic groups is controlled by the agent on individual computers. This means that even if the computer cannot contact the server, it can still be assigned to a dynamic group, and a corresponding action carried out by policy (please see explanation of policies below).

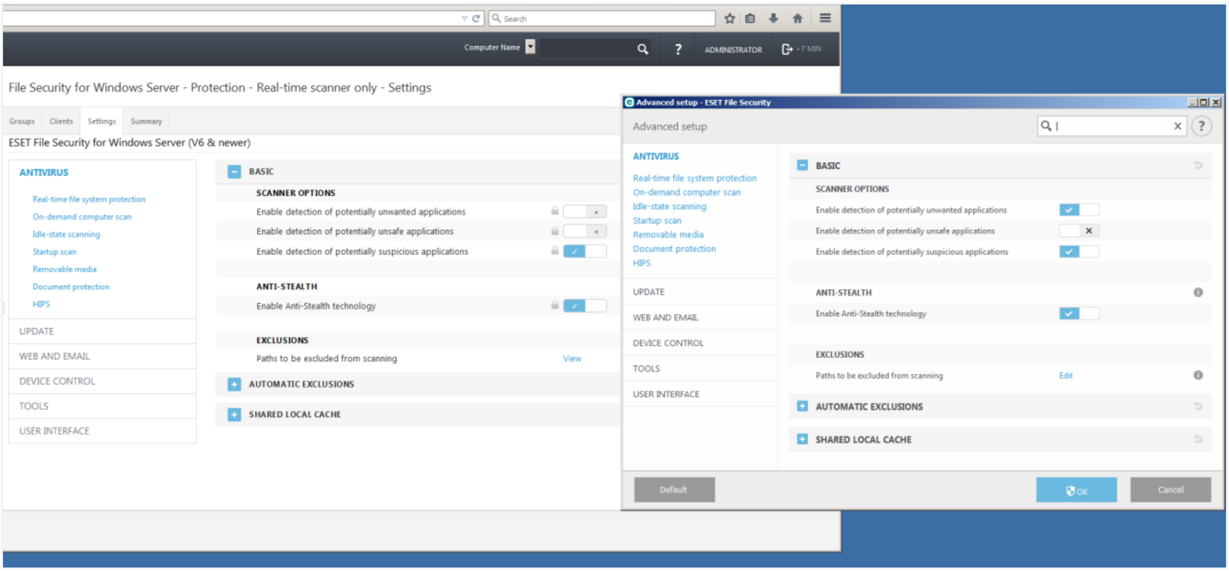
The *Client Tasks* sub-page shows all tasks that have been created by the admin, whether they have already finished, are in the process of running, or are scheduled to run in the future:



Software Install

TASK NAME	TASK DESCRIPTION	TASK TYPE	MODIFICATION TIME
Server Security sivone	As per name	Software Install	2014 Dec 7 16:22:28
Seven_install	Push Endpoint Security to Windows Seven machine	Software Install	2014 Dec 7 14:57:10
AV install to sivone		Software Install	2014 Dec 5 16:51:49
sivonetaketwo		Software Install	2014 Dec 5 16:43:58
[illegible]		Software Install	2014 Dec 5 16:41:12
[illegible]		Software Install	2014 Dec 5 16:27:16
New Task		Software Install	2014 Dec 5 16:23:50
eight		Software Install	2014 Dec 4 18:57:13
Server AV install		Software Install	2014 Dec 3 19:14:22
Ep INSTALL		Software Install	2014 Dec 3 19:06:14

The *Policies* sub-page allows clients to be configured by means of a centrally defined policy. We note that the policy configuration pages are exact replicas of the configuration pages in the client (or server) protection software. The screenshot below shows the console configuration page for File Security Real-Time Scanner settings (on the left), and its counterpart in the File Security window (on the right):



File Security for Windows Server - Protection - Real-time scanner only - Settings

ESET File Security for Windows Server (V6 & newer)

BASIC

SCANNER OPTIONS

- Enable detection of potentially unwanted applications ☒
- Enable detection of potentially unsafe applications ☒
- Enable detection of potentially suspicious applications ☑

ANTI-STEALTH

- Enable Anti-Stealth technology ☑

EXCLUSIONS

- Paths to be excluded from scanning View

AUTOMATIC EXCLUSIONS

SHARED LOCAL CACHE

Advanced setup - ESET File Security

BASIC

SCANNER OPTIONS

- Enable detection of potentially unwanted applications ☑
- Enable detection of potentially unsafe applications ☒
- Enable detection of potentially suspicious applications ☑

ANTI-STEALTH

- Enable Anti-Stealth technology ☑

EXCLUSIONS

- Paths to be excluded from scanning Edit

AUTOMATIC EXCLUSIONS

SHARED LOCAL CACHE

Policies can be assigned to Groups of computers, including Dynamic Groups. This means that if e.g. a computer entered the Dynamic Group *Computers with outdated virus signatures*, a policy could be applied which ran a signature update. Likewise, an operating system update could be run when a computer joins the Dynamic Group *Computers with outdated operating system*.

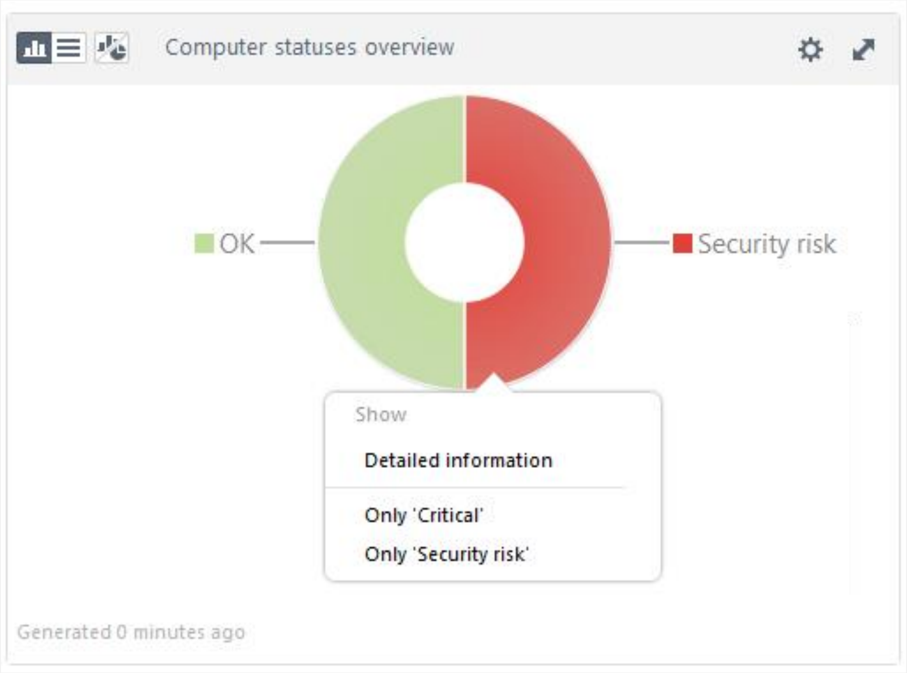
ESET inform us that once applied to a particular computer, a policy is recorded by the agent and will continue to be applied even if the computer is no longer connected to the network. This means that laptop users will continue to have the relevant policies applied when they are out of the office.

Notifications can be configured so that the administrator is informed when particular events occur, such as a certain percentage of computers on the network having an active threat. We did not test this, however.

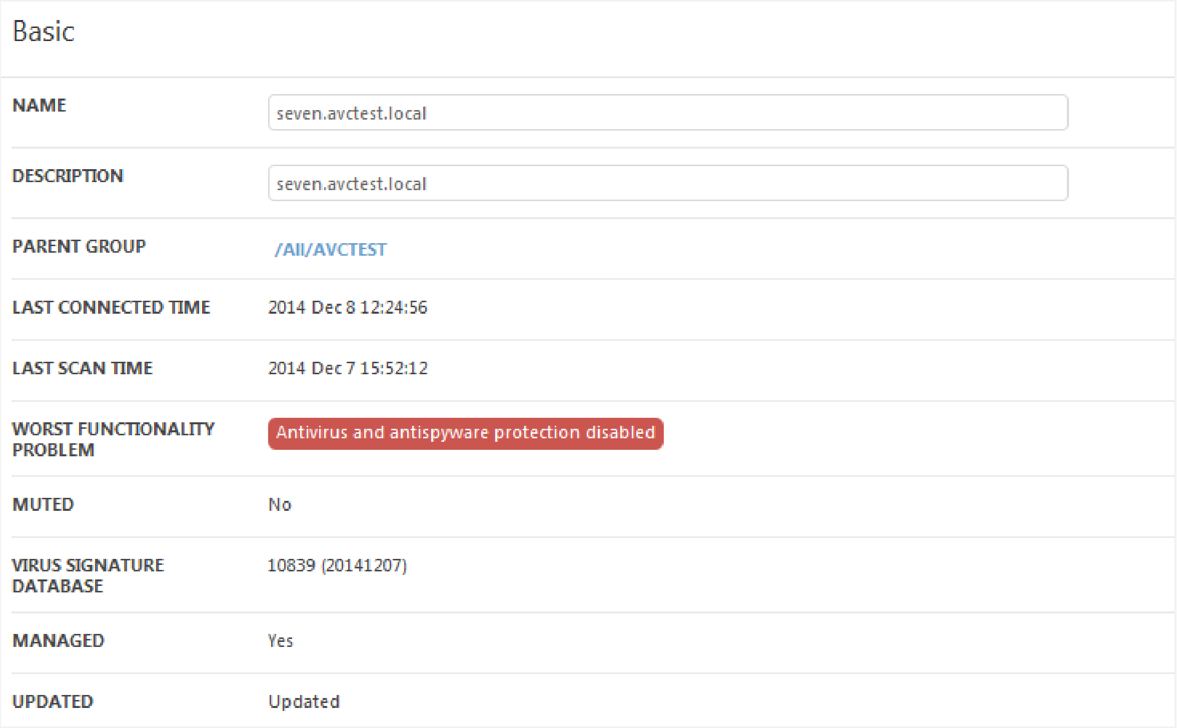
We found the Remote Administrator console intuitive to use. We like the fact that all major management areas/pages are accessed from one single menu bar. The replication of the client configuration dialogs in the policies pages of the console strikes us as ingenious, ensuring that an admin only has to learn where to find things once.

Monitoring and managing the network

The overall status of computers on the network is shown in the *Computer statuses overview* tile on the dashboard. A pie chart shows the proportion of computers without alerts (green) and with alerts (red). In the diagram below, it is easy to see that half of the computers have alerts and half do not. Right-clicking in the red area displays a shortcut menu:



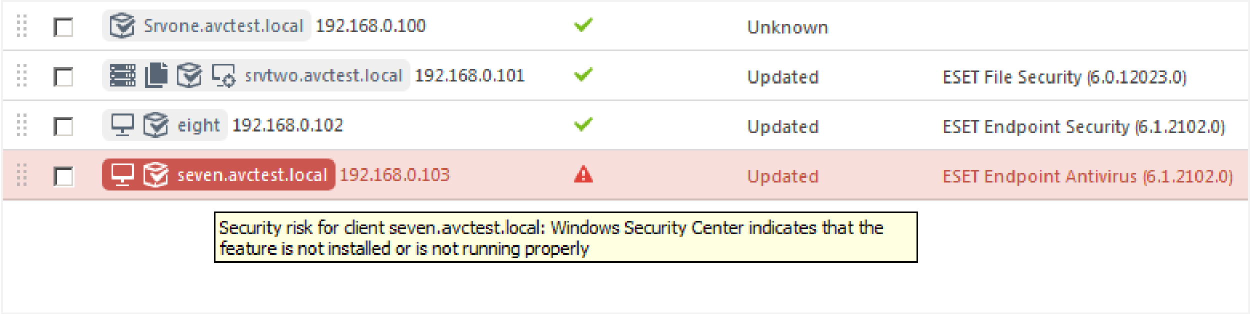
If the admin clicks *Detailed information*, a list of computers with security alerts is shown. From this, a detailed report on any individual computer can be opened, which will show the nature of the problem. An extract from such a report is shown below:



Basic

NAME	seven.avctest.local
DESCRIPTION	seven.avctest.local
PARENT GROUP	/All/AVCTEST
LAST CONNECTED TIME	2014 Dec 8 12:24:56
LAST SCAN TIME	2014 Dec 7 15:52:12
WORST FUNCTIONALITY PROBLEM	Antivirus and antispyware protection disabled
MUTED	No
VIRUS SIGNATURE DATABASE	10839 (20141207)
MANAGED	Yes
UPDATED	Updated

Additionally, the Computers page shows any computers with a security alert, e.g. a protection component being disabled. Moving the mouse over an affected computer shows a pop-up message with a description of the problem:



□	Srvone.avctest.local	192.168.0.100	✓	Unknown	
□	srvtwo.avctest.local	192.168.0.101	✓	Updated	ESET File Security (6.0.12023.0)
□	eight	192.168.0.102	✓	Updated	ESET Endpoint Security (6.1.2102.0)
□	seven.avctest.local	192.168.0.103	⚠	Updated	ESET Endpoint Antivirus (6.1.2102.0)

Security risk for client seven.avctest.local: Windows Security Center indicates that the feature is not installed or is not running properly

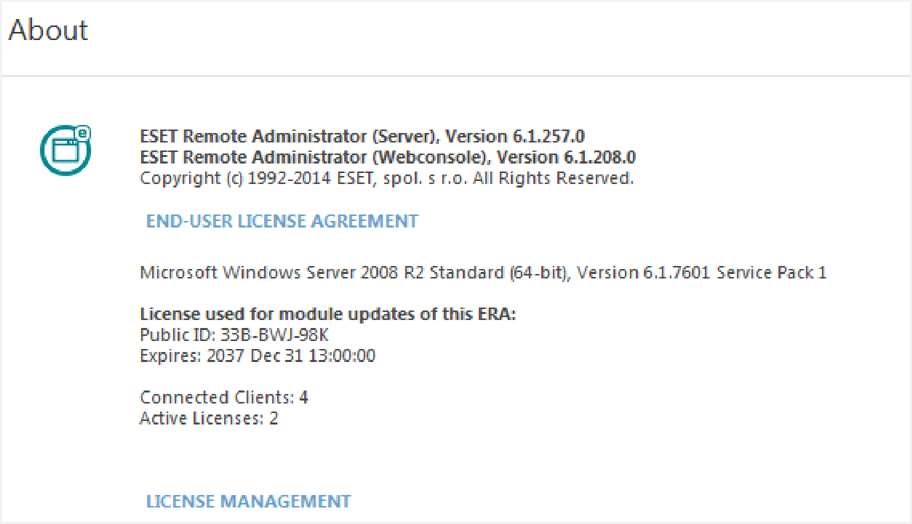
Clicking on the name of the affected computer allows the computer's detailed report to be opened.

ESET inform us that they are developing a means of reactivating disabled protection directly from the console, which will be included in a future release.

Malware finds are shown in detail on the *Threats* page of the console.

The program version of the endpoint software is shown on the *Computers* page

Licensing information: clicking the *About* link at the bottom of the menu panel shows basic licence information, with links to the *End-User Licence Agreement* and *Licence Management*:



About

ESET Remote Administrator (Server), Version 6.1.257.0
ESET Remote Administrator (Webconsole), Version 6.1.208.0
Copyright (c) 1992-2014 ESET, spol. s r.o. All Rights Reserved.

END-USER LICENSE AGREEMENT

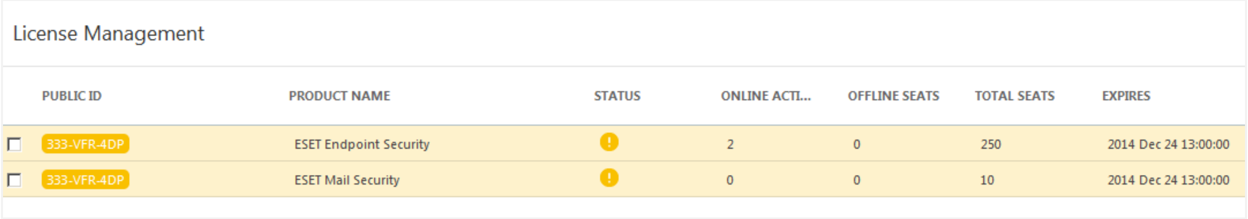
Microsoft Windows Server 2008 R2 Standard (64-bit), Version 6.1.7601 Service Pack 1

License used for module updates of this ERA:
Public ID: 33B-BWJ-98K
Expires: 2037 Dec 31 13:00:00

Connected Clients: 4
Active Licenses: 2

LICENSE MANAGEMENT

The *License Management* page, which can also be found at the bottom of the Admin menu, provides more details of individual licences:

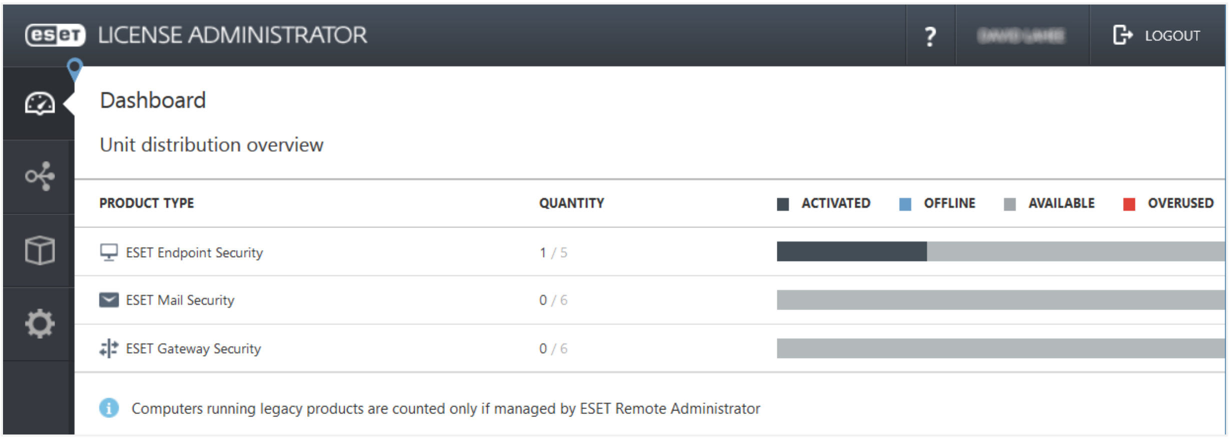


License Management

	PUBLIC ID	PRODUCT NAME	STATUS	ONLINE ACTI...	OFFLINE SEATS	TOTAL SEATS	EXPIRES
□	333-VFR-4DP	ESET Endpoint Security	!	2	0	250	2014 Dec 24 13:00:00
□	333-VFR-4DP	ESET Mail Security	!	0	0	10	2014 Dec 24 13:00:00

New licences can be assigned to existing computers using by means of a task, similar to software installation. Alternatively, a licence can be assigned using the client software on the client computer itself; when we tried this in our test, we found that the new licence was displayed almost immediately. We were able to activate our installation of File Security 4.5 using this method, as ESET provide activation credentials for older versions with each licence. In addition to the Licence Management page of the Remote Administrator console, ESET provide a separate, cloud-based console called License Administrator[2], which synchronises all licensing data with the Remote Administrator console:

[2] https://ela.eset.com



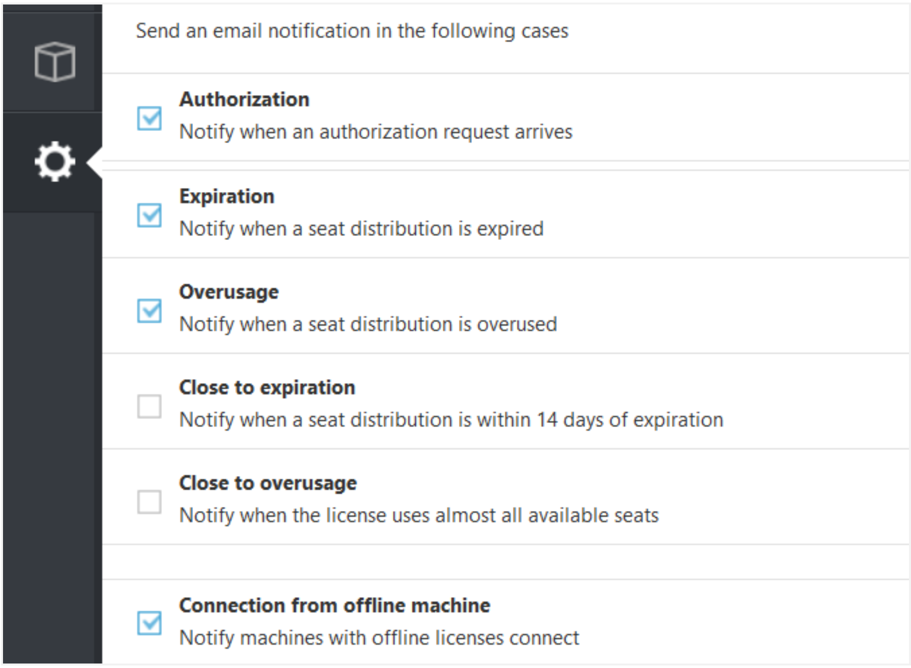
Dashboard

Unit distribution overview

PRODUCT TYPE	QUANTITY	■ ACTIVATED ■ OFFLINE ■ AVAILABLE ■ OVERUSED
ESET Endpoint Security	1 / 5	
ESET Mail Security	0 / 6	
ESET Gateway Security	0 / 6	

Computers running legacy products are counted only if managed by ESET Remote Administrator

Administrators can log in to this console from any Internet-connected computer, using an email address and password they choose themselves. The same account can be used to activate software on a client computer; this saves having to find a licence key. The License Administrator has comprehensive notification options, so that the administrator can be alerted in the event of e.g. an imminent licence expiry:



Send an email notification in the following cases

☑ **Authorization**
Notify when an authorization request arrives

☑ **Expiration**
Notify when a seat distribution is expired

☑ **Overusage**
Notify when a seat distribution is overused

□ **Close to expiration**
Notify when a seat distribution is within 14 days of expiration

□ **Close to overusage**
Notify when the license uses almost all available seats

☑ **Connection from offline machine**
Notify machines with offline licenses connect

We feel the Dashboard provides a good overview of the system security status, and makes it easy for the admin to open detailed pages for any alerts shown.

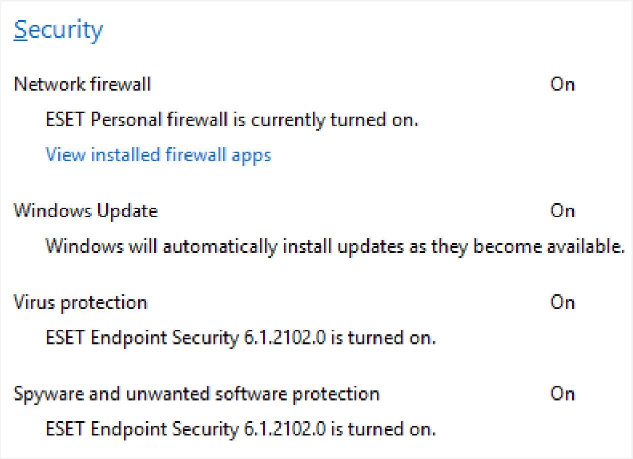
The licence management options strike us as comprehensive and very convenient.

Running updates and scans, and scheduling scans, can be done from the Computers page. The administrator simply selects the relevant computer(s) and clicks the *Tasks* button. Updates and scans can be run immediately, by clicking their respective entries in the *Tasks* menu, while clicking *New task…* allows a scheduled scan to be set.

The *Computers* page makes it very simple to carry out everyday management tasks.

Client endpoint protection software

ESET Endpoint Security 6, the client endpoint protection software, registers with Windows Action Center as firewall, antivirus and antispyware:



Security

Network firewall On

ESET Personal firewall is currently turned on.

View installed firewall apps

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

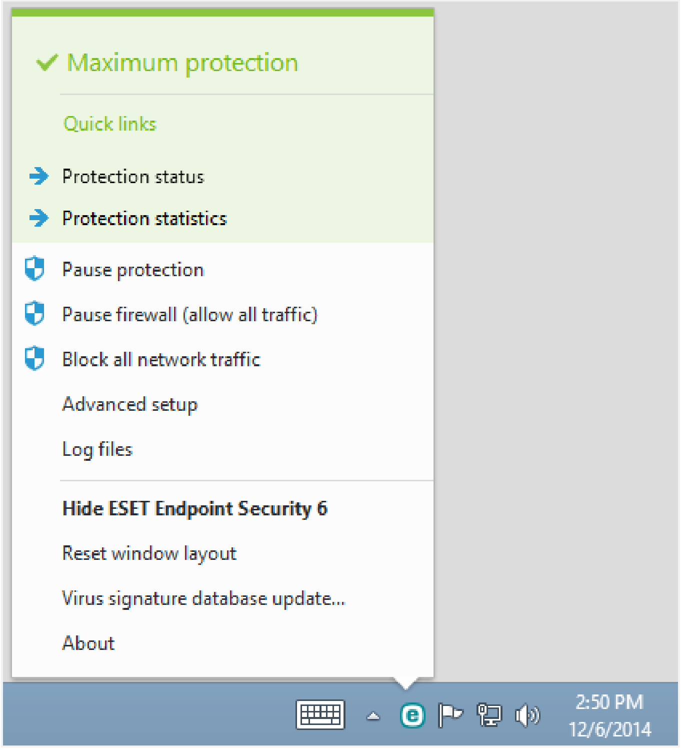
ESET Endpoint Security 6.1.2102.0 is turned on.

Spyware and unwanted software protection On

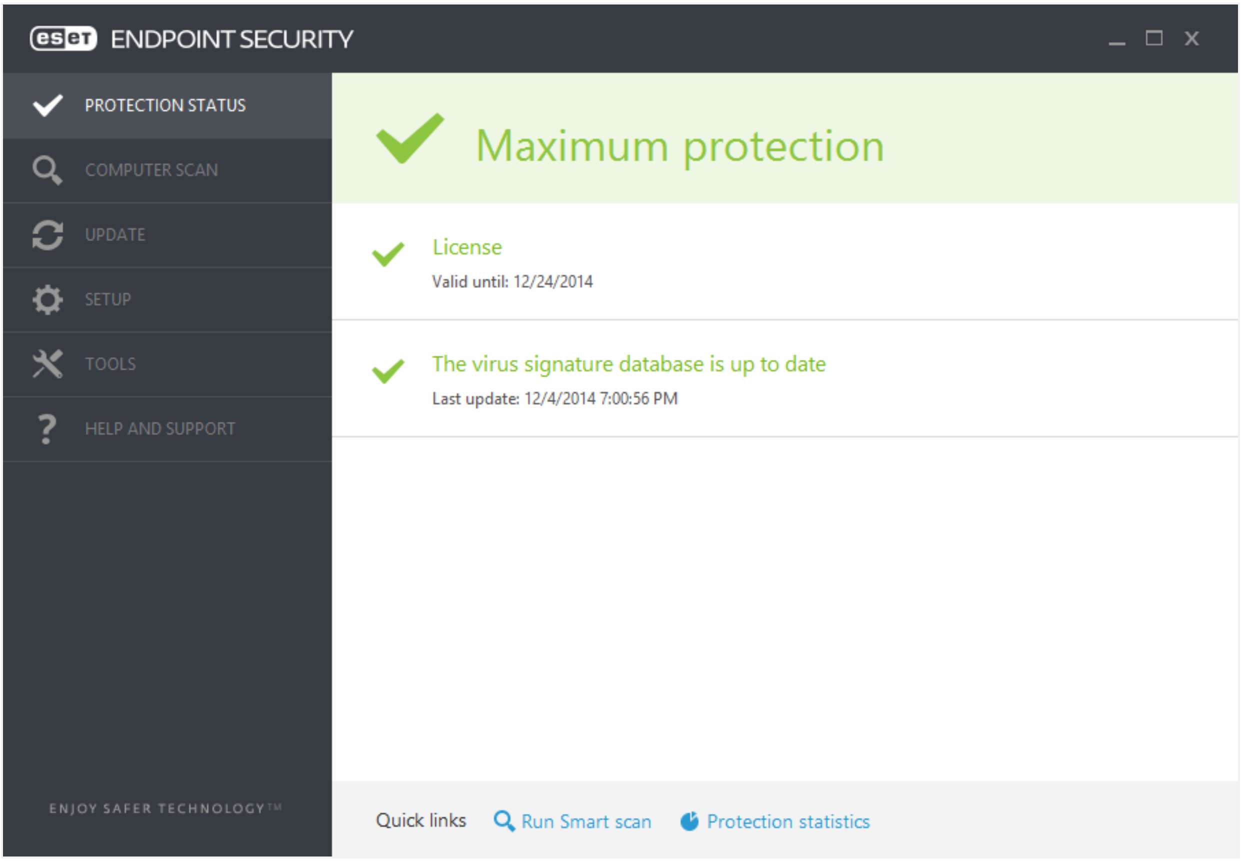
ESET Endpoint Security 6.1.2102.0 is turned on.

Windows 8's Windows Defender and Windows Firewall are both disabled, as is appropriate.

There is a System Tray icon; right-clicking this displays a menu of common tasks and information:



System status is shown in the main program window:



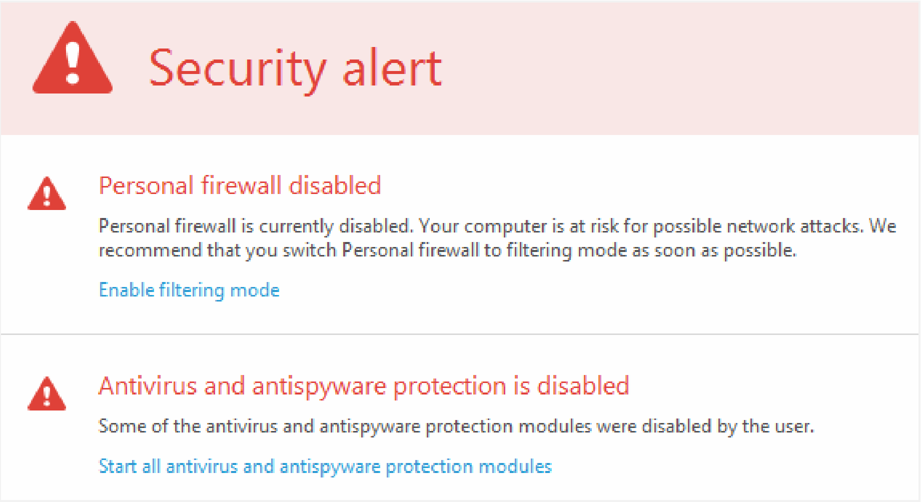
Maximum protection

License
Valid until: 12/24/2014

The virus signature database is up to date
Last update: 12/4/2014 7:00:56 PM

Updates and scans both have their own buttons in the menu bar on the left.

If the real-time protection or firewall are disabled, the status display changes to show this. Each component has its own link which reactivates the protection:

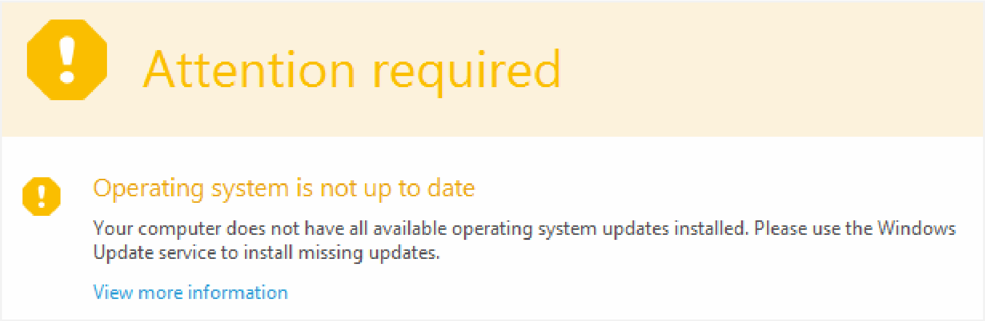


Security alert

Personal firewall disabled
Personal firewall is currently disabled. Your computer is at risk for possible network attacks. We recommend that you switch Personal firewall to filtering mode as soon as possible.
Enable filtering mode

Antivirus and antispyware protection is disabled
Some of the antivirus and antispyware protection modules were disabled by the user.
Start all antivirus and antispyware protection modules

An alert is also shown if the Windows operating system is not up to date:



Attention required

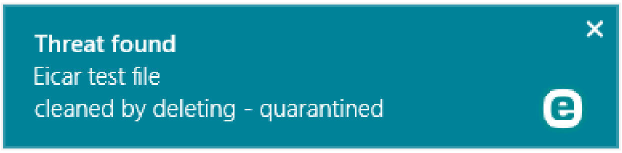
Operating system is not up to date

Your computer does not have all available operating system updates installed. Please use the Windows Update service to install missing updates.

View more information

Clicking *View more information* opens a message box which shows the missing OS updates; a link in this box conveniently opens the Windows Update window to install them.

Users without administrator credentials cannot disable protection features or uninstall the product. If the EICAR test file is downloaded, a Windows-8-style warning is displayed for a few seconds:



Threat found
Eicar test file
cleaned by deleting - quarantined

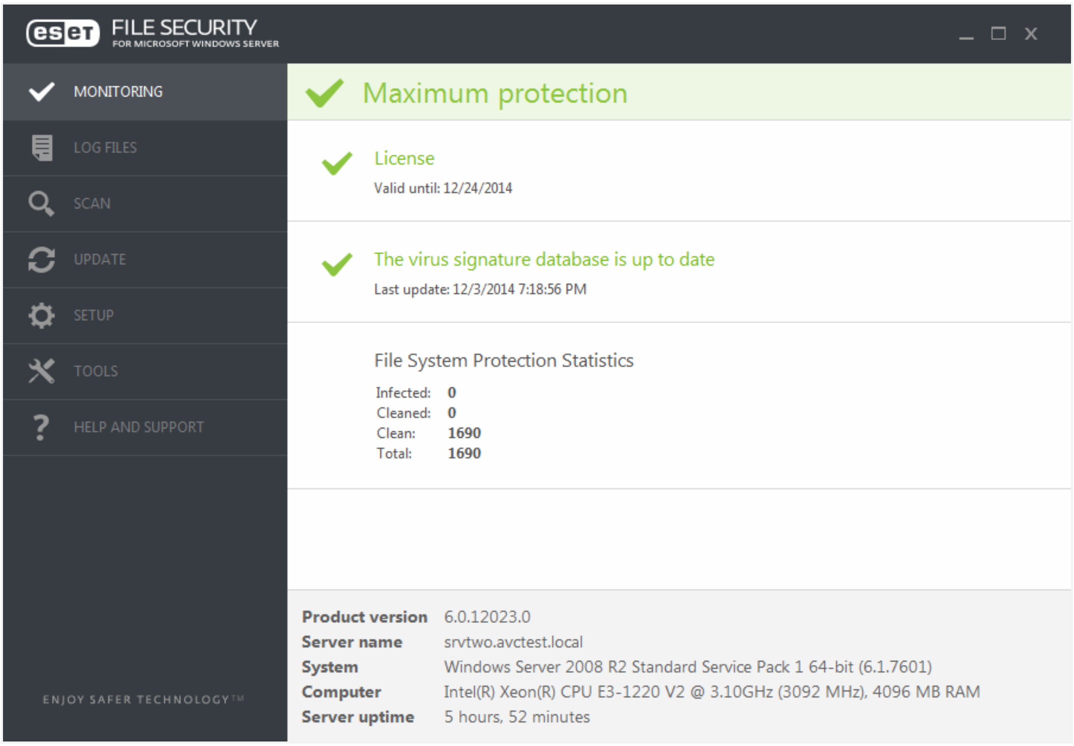
The *Tools* page of Endpoint Security displays a link to the download page for ESET SysRescue Live, which allows the user to create a bootable CD, DVD or USB flash drive that can be used to clean malware from an infected system that will not start or cannot be cleaned from within Windows.

ESET's business antivirus client for Windows, Endpoint Antivirus, has a virtually identical interface to Endpoint Security. Minor differences can be found in EA's program settings, where controls for the firewall, anti-spam and web controls are absent, due to these features not being included in the "little sister" program. The two entries in the System Tray menu relating to the firewall are also absent, for the same reason.

We feel that ESET Endpoint Security 6 is very well-designed, makes important functions and data easily accessible, and warns appropriately in the event of a problem. It cannot be disabled by unauthorised users. The new interface has been optimised for use with a touchscreen; even details such as the settings dialogs can be comfortably controlled with a finger.

Server antivirus software

The server protection software, ESET File Security, has an extremely similar design to Endpoint Security:



Maximum protection

✓ License
Valid until: 12/24/2014

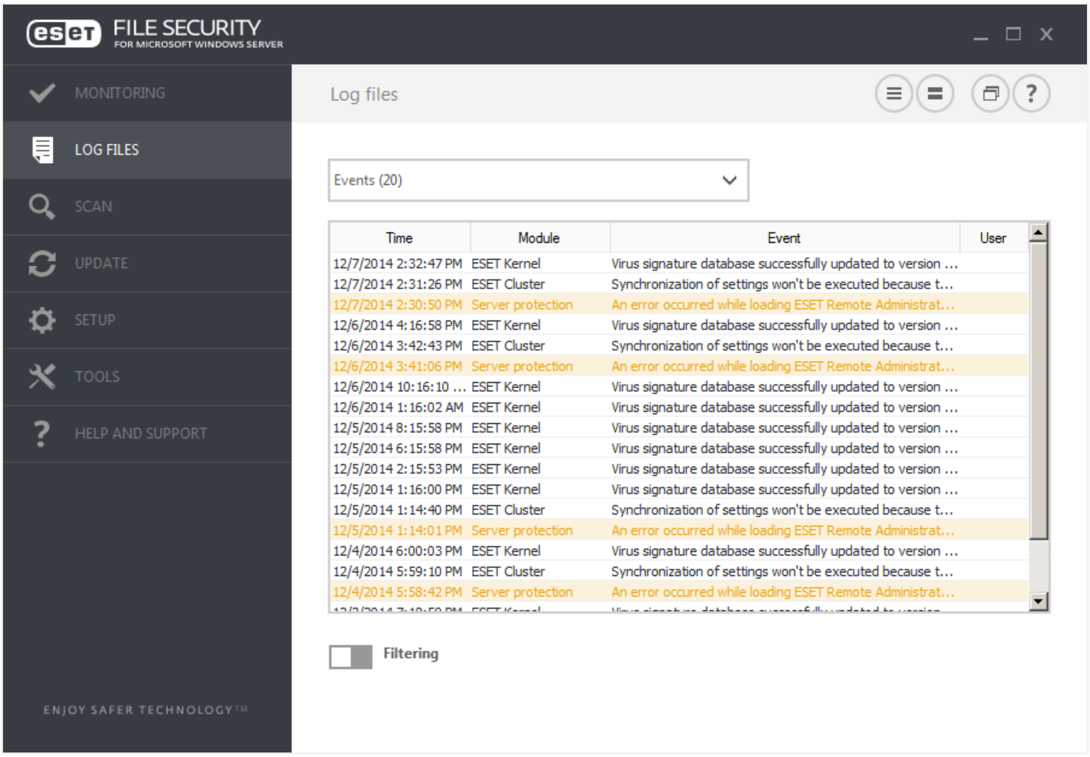
✓ The virus signature database is up to date
Last update: 12/3/2014 7:18:56 PM

File System Protection Statistics

Infected:	0
Cleaned:	0
Clean:	1690
Total:	1690

Product version	6.0.12023.0
Server name	srvtwo.avctest.local
System	Windows Server 2008 R2 Standard Service Pack 1 64-bit (6.1.7601)
Computer	Intel(R) Xeon(R) CPU E3-1220 V2 @ 3.10GHz (3092 MHz), 4096 MB RAM
Server uptime	5 hours, 52 minutes

The *Monitoring* button is equivalent to *Protection Status* in the client software. There is an additional button in File Security's menu bar, namely *Log Files*. This shows a detailed log of events:

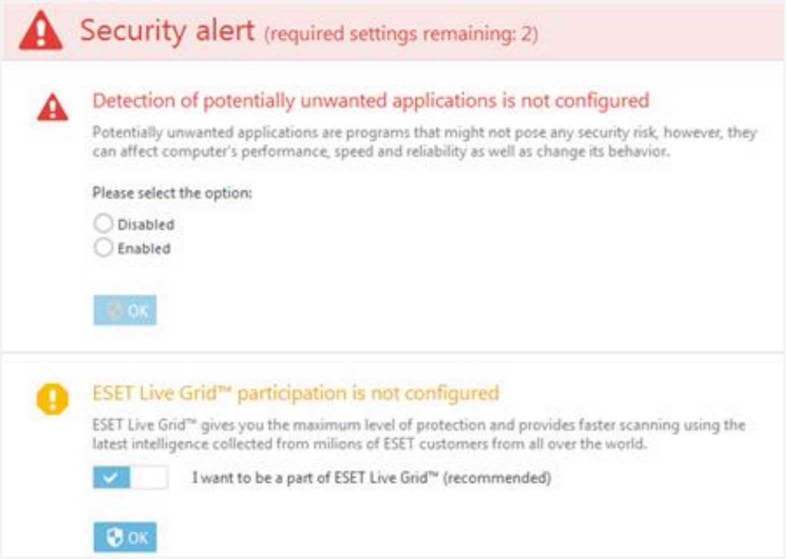


Events (20)

Time	Module	Event	User
12/7/2014 2:32:47 PM	ESET Kernel	Virus signature database successfully updated to version ...	
12/7/2014 2:31:26 PM	ESET Cluster	Synchronization of settings won't be executed because t...	
12/7/2014 2:30:50 PM	Server protection	An error occurred while loading ESET Remote Administrat...	
12/6/2014 4:16:58 PM	ESET Kernel	Virus signature database successfully updated to version ...	
12/6/2014 3:42:43 PM	ESET Cluster	Synchronization of settings won't be executed because t...	
12/6/2014 3:41:06 PM	Server protection	An error occurred while loading ESET Remote Administrat...	
12/6/2014 10:16:10 ...	ESET Kernel	Virus signature database successfully updated to version ...	
12/6/2014 1:16:02 AM	ESET Kernel	Virus signature database successfully updated to version ...	
12/5/2014 8:15:58 PM	ESET Kernel	Virus signature database successfully updated to version ...	
12/5/2014 6:15:58 PM	ESET Kernel	Virus signature database successfully updated to version ...	
12/5/2014 2:15:53 PM	ESET Kernel	Virus signature database successfully updated to version ...	
12/5/2014 1:16:00 PM	ESET Kernel	Virus signature database successfully updated to version ...	
12/5/2014 1:14:40 PM	ESET Cluster	Synchronization of settings won't be executed because t...	
12/5/2014 1:14:01 PM	Server protection	An error occurred while loading ESET Remote Administrat...	
12/4/2014 6:00:03 PM	ESET Kernel	Virus signature database successfully updated to version ...	
12/4/2014 5:59:10 PM	ESET Cluster	Synchronization of settings won't be executed because t...	
12/4/2014 5:58:42 PM	Server protection	An error occurred while loading ESET Remote Administrat...	

Filtering

After installation, the status section of the program window alerted us to two issues which needed to be resolved:



Security alert (required settings remaining: 2)

Detection of potentially unwanted applications is not configured

Potentially unwanted applications are programs that might not pose any security risk, however, they can affect computer's performance, speed and reliability as well as change its behavior.

Please select the option:

○ Disabled
○ Enabled

ESET Live Grid™ participation is not configured

ESET Live Grid™ gives you the maximum level of protection and provides faster scanning using the latest intelligence collected from milions of ESET customers from all over the world.

☑ I want to be a part of ESET Live Grid™ (recommended)

ESET inform us that their Mail Security program, which provides virus protection for mail servers (with file-server protection as an option), also uses the same interface design.

We like the fact that the interface design of the server protection software is as similar as possible to that of the client, making it familiar and easy-to-use. We also note the similarity in design between the server/client protection software and the console itself, which we also feel aids orientation.

Summary

ESET Remote Administrator 6 has a completely new, modern design.

Console installation is very simple, and the setup wizard makes it easy to install any prerequisites that are missing without even having to restart it.

The two manuals are excellent and we would recommend administrators to read the relevant instructions before carrying out a task for the first time. A good web-based local help service is also available.

The ESET agent can be deployed locally or remotely. Once this has been done, push installation of endpoint protection software is very simple.

The console dashboard shows the security status of the network as a number of colourful pie charts; these make it easy to for the administrator to navigate to details pages, for more information about the computers.

It is easy to customise individual pages of the console, so that the administrator can easily find the items he/she feels are most important.

A wealth of information and functionality is available from the console, but the design avoids overwhelming the user.

We found that we quickly got used to the design of the console, and the way it works. We had no difficulty carrying out everyday deployment, monitoring and management tasks.

We found the design and functionality of the ESET Endpoint Security 6 to be outstanding. The same interface is used in the Endpoint Antivirus client, and the File Security and Mail Security protection software, ensuring familiarity throughout.

There is obvious similarity between the design of all these programs and the console itself. This is not just a question of aesthetics, but has practical applications. For example, all the pages of the program/console are accessed from the menu bar on the right; the configuration pages for policies are exact replicas of the client configuration pages; consistent alert symbols are used throughout. We feel these similarities make it easy for the administrator to become familiar with the whole system.

Overall, we feel ESET have done a tremendous job of making a console that is powerful enough to cope with thousands of clients, but simple enough to use in SMBs as well.

Copyright and Disclaimer

AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

(December 2014)