IT Security Products for Corporate Users

Review of IT Security Suites for Corporate Users, 2011

Language: English
September 2011
Last revision date: 27th September 2011
www.av-comparatives.org

Contents

Introduction

Aim of the review

In this report, we have assessed the ease of installation and use of a number of business antivirus packages. Many vendors make a range of different business products, ranging from very small networks with about 10 PCs, to vast international corporations with thousands of computers in various different locations. Our test scenario is a company that might use Microsoft Small Business Server. This means up to 75 users, with a single domain. There would be a primary server that functions as the domain controller and Microsoft Exchange server, plus a possible second server (Premium Add-On for Small Business Server 2011). At the other end of the scale, some Small Business Server users may only have 10 PCs in total. As Small Business Server is configured to make administration easy for small businesses, including those without full-time IT support staff, we also considered the suitability of the business antivirus products for such small networks. In some cases, we felt that an IT-literate business owner would be able to install and configure the product without any specialist IT training.

Test environment

Given that three generations of Windows software are currently in common use, not to mention both 32-bit and 64-bit architectures, we used a variety of client PCs to deploy the software to, to test the ability of the package to cope with different Windows versions and architectures.
Our test network was made up of the following machines:

Main server
Windows Server 2008 R1 x64, Service Pack 2, and Microsoft Exchange Server 2007 [version 08.01.0240.006]. Functions: domain controller, DNS server, mail server.

Secondary server
Windows Server 2008 R2 x64, Service Pack 1. Functions: file server

Client PCs
Windows 7 Enterprise x64 Service Pack 1
Windows 7 Enterprise x86 Service Pack 1
Windows Vista Business x86 Service Pack 2
Windows XP Professional x86 Service Pack 3

Active Directory OUs
In order to test each software package's ability to use Active Directory to deploy software to specific groups of computers, we created two OUs within our domain, called 32 and 64. Not surprisingly, we put our 32-bit OS clients into the first OU, and the 64-bit client and secondary server into the second. In the event that separate deployment processes were required to deploy 32 and 64-bit client software, we would be able to select the relevant computers very easily if the package's AD integration were good.

Client computer preparation

All the computers used for the review had all important Windows updates installed as at 1st June 2011. To save time, we configured the images used for all client PCs and the secondary server to allow file sharing and Remote Desktop access; for the Windows XP client, simple file sharing was disabled; for the Windows 7/Vista clients, and the secondary server, network discovery was enabled.

These measures seemed sensible in that most of them are required to allow the push install of any business security software. Remote Desktop access was convenient for our administration, but also allowed us to see whether RDP access was blocked by the firewall of any of the endpoint protection packages.

Tasks and features reviewed

Downloading the software

Previous reviews have noted that downloading the entire business package can sometimes involve locating numerous individual files, which can be time-consuming and irritating. We thus considered the ease of carrying out this small but vital task.

Using the manual to prepare for installation

As business security software packages are much more complex than consumer antivirus programs, it is very advisable to consult the manufacturer's manual before starting on any major task, such as installing the management software. A good manual can make the difference between a quick, easy installation and a slow and frustrating installation. Because of the numerous features available in business security software, multiple possible installation scenarios, and potential tasks that need to be performed, full manuals can be very long, frequently over 100 pages. Because of this, we consider that good indexing is essential. It is unreasonable to expect administrators to read an entire manual before getting started; they will want to find the section relevant to the task in hand and read just that. A good manual will be logically organised into relevant sections, such as system preparation, installation, deployment and maintenance, each with suitable subsections. There needs to be a clear index of these sections and subsections, and it makes sense to take full advantage of the bookmarking and linking options provided in Adobe Reader. If entries in the table of contents and bookmarks pane are linked to the corresponding bookmark in the text, going to the page is as simple as clicking on the item in the contents page or bookmarks pane. This makes it very much quicker and easier to navigate through a long and complex document.

In this section of each individual product report, we have commented on the overall content, layout and indexing of the manual and in particular the section on installing the management software. We looked for an overview of how the package functions, and details of the computer(s) on which the software was to be installed, along with system requirements, and any additional software that needed to be installed.

Installation of the administration software

In many cases, installing the management software is very simple and straightforward. Consequently we have not described this in very much detailed, but have pointed out any relevant options such as custom installation, and any additional software required, e.g. variants of SQL server to host the security software's database. We have also noted any points which we found confusing or complicated.

The administration console

The management console is arguably the most important element, in terms of interface at least, in a business security software package. It allows the administrator to deploy, configure, monitor and maintain the security software throughout the network, so its features and interface are of critical importance. Inevitably, many consoles are so rich in terms of features that we could not provide a full description of these within the scope of this review. However, we have described the layout of each console, and tried to indicate how easy it is to find essential everyday status reports and functionality.

Using the manual to prepare for deployment

Deploying the endpoint protection software to client PCs on the network is likely to be the most important single task that the administrator will use the console for. Any failures in the process can cost time and money, so it essential that it should run smoothly first time. A well-written manual is an enormous help in this respect, and so we consulted the relevant section of each manual to see if the instructions were clear and comprehensive. In particular, we looked for details of client preparation, such as enabling file sharing, as failure to configure such things correctly will result in installation failing. We would expect many companies to have 3 generations of Windows client operating systems in concurrent use (Windows 7, Vista and XP), along with both 32-bit and 64-bit architectures. Consequently we looked out for necessary instructions relating to particular Windows architectures or versions. As mentioned above, we do not expect the administrator to have to read the entire manual before deployment, only the relevant section of it. We thus consider it very important that any critical information on client preparation, or any other element that could cause problems with or failure of the deployment, be located in the deployment section of the manual, thus ensuring that the administrator will read it before beginning the process.

Deploying client software using push install

In this section we describe the actual deployment process (we have assumed that the necessary client preparation, as described in the manual, has already been carried out). One of the factors we consider is the process of selecting individual PCs or groups of PCs for deployment, and to what extent Active Directory can be used. As mentioned above, we created two OUs (called 32 and 64) to see whether the deployment wizard would allow us to select these individually, or only the entire domain or forest can be used, or Active Directory is not used at all. Another important element that we looked at is the status display of installation progress. Previous reviews have noted a lack of real-time information in many cases, and we wanted to see if this has improved. We also considered the general speed and ease of the deployment process.

Client software

In many cases, the program interface of the client endpoint protection software is similar or even identical to its consumer counterpart. Other manufacturers have opted for different interfaces, which may be more suited to use by an administrator than a standard user, or be very minimalist in nature. We do not feel that there is any right or wrong answer here, and it is up to potential users of the software to decide for themselves whether they feel each interface is suitable for their own particular environment. There are a couple of specific points which we think should be considered carefully, however. It would seem very prudent to ensure that disabling any element of the endpoint protection can be password protected in some way, either by a dedicated password, or by making it accessible only to Windows administrator accounts. However, we do think that small businesses in particular will find it useful if the administrator *is* able to temporarily disable protection locally, rather than from the console, e.g. in order to install some programs which require antivirus protection to be turned off during installation.

Exchange server protection

In most (but not all) cases, a separate program is provided by the manufacturer to provide Exchange Server protection, i.e. scan Exchange mailboxes for malware (spam protection may also be included). We considered the instructions in the manual for installing this, details of the actual installation process and any additional software needed. In some cases, the interface of the Exchange Server protection module has its own separate console, in which case we have described the major elements of this and its layout. In other cases, control of the Exchange Server protection is incorporated into the main management console, or even the server's own antivirus program

interface, in which case we have briefly described the additional elements relating to mail protection.

Tested Products

The following vendors participated in the tests and review:

AVIRA	**www.avira.com**
Bitdefender	**www.bitdefender.com**
eScan	**www.escan.com**
ESET	**www.eset.com**
G DATA	**www.gdata.de**
Kaspersky	**www.kaspersky.com**
McAfee	**www.mcafee.com**
Symantec	**www.symantec.com**
Trend Micro	**www.trendmicro.com**

Summary of the products tested

All of the products we tested could be used successfully in small or medium-sized businesses. For the purposes of this review, we have defined "medium-sized" as a business with up to 75 PCs (the maximum number supported by Microsoft's Small Business Server), with a full-time professional IT administrator. By "small" we mean a business without its own full-time IT administrator, where network administration is carried out part-time by an IT-literate owner or member of staff with other responsibilities. In practice, this is likely to mean fewer than about 25 PCs. Needless to say, each of the products we reviewed had its strengths and weaknesses, which we have summarised in the table below. We would also like to point out particular areas of excellence we found in the products.

Avira's documentation is outstanding. Its full manual is comprehensive, well written, bookmarked and indexed in fine detail, contains a sensible number of screenshots, and is very professionally produced. The How-To guides are much shorter, but clearly explain and illustrate the essential steps in the procedures they cover. For a professional administrator, Avira's installation and deployment procedures are especially simple, fast and trouble-free. As a result, we feel that for medium-sized business with IT staff, Avira manages to get just a fraction ahead of the competition in overall performance, even though the overall standard is very high.

Using **Bitdefender** to protect our small business network particularly is quick, simple and unproblematic. The manual explains clearly how to install and deploy the software, and the procedure is simple in practice. The management console gives the administrator the ability to carry out a wide range of tasks and audits, not only for the antivirus software, but also for the entire Windows system. There is very little to criticise, and the management features make the software very suitable for medium-sized business networks.

eScan's corporate suite is in many ways well designed and easy to use. Local installation of the management console and Exchange protection is quick and easy. It is one of the handful vendors who provides Web Integration, so there is no need for a Microsoft CAL for managing AV on a machine, which is not part of your domain/AD.

ESET and **Symantec** have both produced client software which is exceptionally well designed and easy to use, for experienced as well as less-experienced administrators. In both cases, standard users can see the protection status and carry out essential tasks such as updating, using a very familiar program interface. Administrators have easy access to a wider range of functions, while standard users are blocked from any risky actions such as disabling protection.

G Data excels in its simple, trouble-free installation and deployment processes, and console design. Although its functionality is comprehensive, the G Data console provides a very clear and simple interface that never threatens to overwhelm the administrator. Incorporating the Exchange protection interface into the same console makes for very simple and convenient administration of the entire suite.

Kaspersky's business software range includes Small Office Security (for up to 10 PCs and a file server), and the Work Space/Business Space/Enterprise Space/Total Space range. Work Space Security covers client PCs and smartphones; Business Space extends this by covering file servers;

Enterprise Space adds protection for mail servers and groupware servers (including solutions for both Microsoft Exchange Server and Lotus Notes); Total Space additionally covers Internet Gateways. We tested the Enterprise Space software, looking at protection for client PCs, file servers and Microsoft Exchange Server.

McAfee is a leader in the area of deploying client software. Although many of the other products offer local installation of the client software, McAfee makes this especially easy, using a link in a web page or email, and a very simple process that still manages to offer essential options. The remote push installation is also exceptional, with a simple yet highly effective wizard that offers comprehensive yet simple client selection, plus a choice of component selection and links to advanced options, on a single, uncluttered page. McAfee's client software is also outstanding for networks with a full-time IT administrator. Its interface is almost revolutionary in its simplicity, essentially showing just a status report on its main page. Administrators will however find detailed configuration options easily available from a single menu.

Trend Micro is a first-class candidate for small networks, due to extremely simple installation and deployment routines, and very user-friendly client software. But not only for small networks, also will administrators of large networks be happy with this solution.

We are happy to report that all products reviewed in this report received the AV-Comparatives Seal of Approval. The products performed well in their primary functions, as it can be expected from established business security products. IT Administrators may find some products fit their needs better than other products because they address a specific set of feature they are looking for.

Synoptic Table

We present here an overview of the products, which can be used to help make your decision. Please try the products on your own system before making a purchase decision based on this review. All vendors offer trial versions of their products and have qualified resellers in most countries. The review and the table below contain our subjective appraisal based on the tests and the publicly available information on the vendors' websites.

	AVIRA	Bitdefender	eScan	ESET	G Data	Kaspersky	McAfee	Symantec	Trend Micro
Installation / Deployment	★★★★★	★★★★½	★★★★	★★★★½	★★★★★	★★★★½	★★★★★	★★★★½	★★★★½
Console	★★★★½	★★★★½	★★★★	★★★★	★★★★★	★★★★½	★★★★	★★★★½	★★★★½
Client Software	★★★★½	★★★★	★★★★	★★★★★	★★★★½	★★★★½	★★★★★	★★★★★	★★★★½
Manual	★★★★★	★★★★½	★★★★	★★★★½	★★★	★★★★	★★★★	★★★★	★★★★½
Overall Assessment	★★★★½	★★★★½	★★★★	★★★★½	★★★★½	★★★★½	★★★★½	★★★★½	★★★★½
Award	AV comparatives APPROVED Corporate Product 2011	AV comparatives APPROVED Corporate Product 2011	AV comparatives APPROVED Corporate Product 2011	AV comparatives APPROVED Corporate Product 2011	AV comparatives APPROVED Corporate Product 2011	AV comparatives APPROVED Corporate Product 2011	AV comparatives APPROVED Corporate Product 2011	AV comparatives APPROVED Corporate Product 2011	AV comparatives APPROVED Corporate Product 2011

AVIRA

Tested Software:

Avira Security Management Center 2.6
Avira AntiVir Professional 10.2
Avira AntiVir Server 10.0
Avira AntiVir Exchange 8.3

Introduction

Avira make a single line of traditional local security products (as well as offering cloud-based services). The components (workstation antivirus, fileserver antivirus, management console and antivirus/antispam for Exchange) can be combined as appropriate to cover any size of network.

Software version reviewed

Avira Security Management Center 2.6
Avira AntiVir Professional 10.2
Avira AntiVir Server 10.0
Avira AntiVir Exchange 8.3

Downloading the software

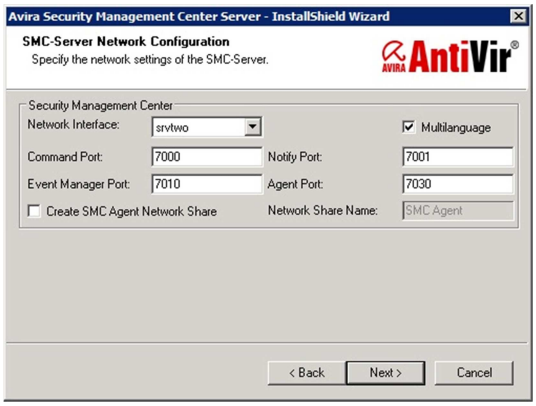
To protect our Windows network with Avira, we needed to download four software packages. These are Avira Security Management Center, the administration console; Avira AntiVir Professional, the antivirus program for client PCs; Avira AntiVir Server, for file-server protection; and Avira AntiVir Exchange, for protecting Microsoft Exchange Server. For each package there are two .PDF files: a highly detailed manual, and a much more succinct How To guide.

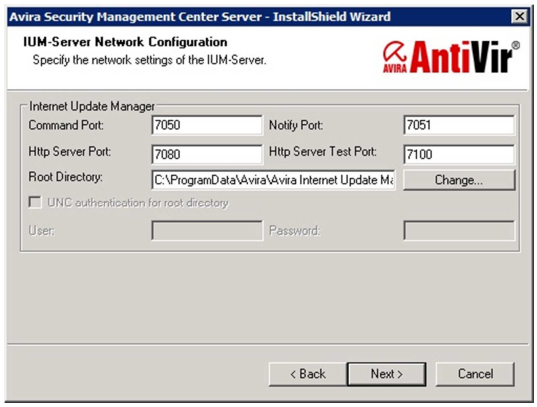
Using the manual to prepare for installation

As mentioned, Avira produce two user guides for the Security Management Center. The User Manual has 117 pages, and gives very detailed information on the functionality, installation and use of the software. It is very professionally produced, and indexed in fine detail, making it easy to find particular sections. There are an appropriate number of screenshots. The How To guide is considerably shorter at 39 pages, and at first glance does not create a favourable impression. Although there is an index at the start, this is not displayed in Adobe Reader's navigation pane, meaning that the document can only be navigated using the thumbnails function. It has not been so neatly formatted, and in places it is clear that the text has not been written or checked by a native English speaker. However, despite these deficiencies, the document is a gem. It provides all the information needed to install the management software quickly and easily, with abundant screenshots. The English may be a little clumsy in places but it is always perfectly clear what is meant. We used the How To guide to prepare for our installation and felt it was the ideal companion for this process.

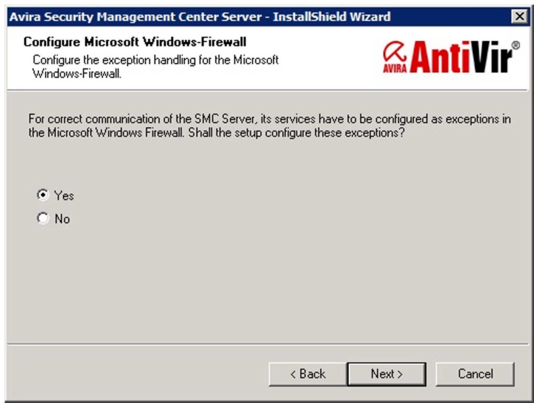
Installation of the administration software

Avira's management software comes in two parts. The Management Center Server, which provides the functionality, is installed on a server; the Management Center Frontend provides the interface, and can be installed on the server or the administrator's workstation. There are a number of steps to the Server installation, though few are remotely complicated. There is the usual licence agreement to accept, a choice of location for the installation folder, and then two dialogs for configuring the ports used by the program:





Although these dialogs might appear a little daunting to the uninitiated, the How To guide makes it clear that the settings can be left at default, and notes a few other ports which should not be used by other programs. Setup then asks for domain admin credentials for the program to use, and a username and password to allow access the console. Next, the wizard informs us that it needs to create exceptions for Windows Firewall:

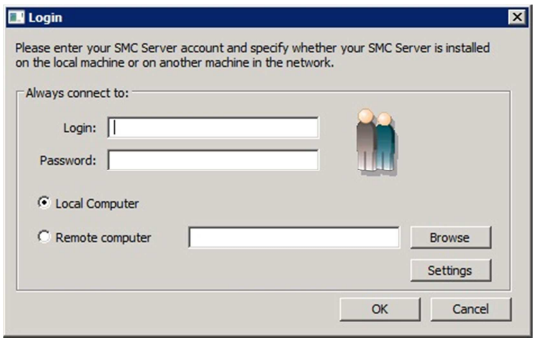


Installation then starts, and is quickly completed.

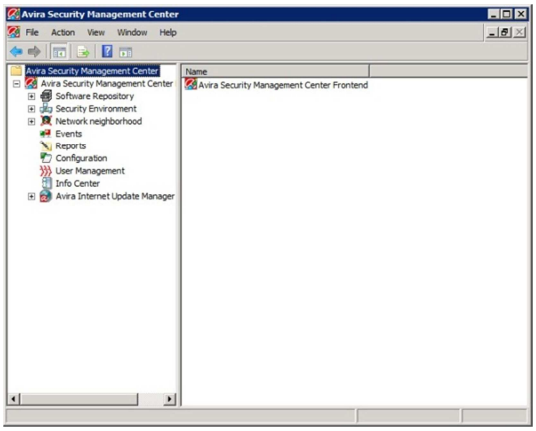
The next step is to set up the Frontend (user interface); we chose to install this on the same server. It is a very quick and simple process, with a licence agreement to accept, and a chance to choose the installation folder.

The administration console

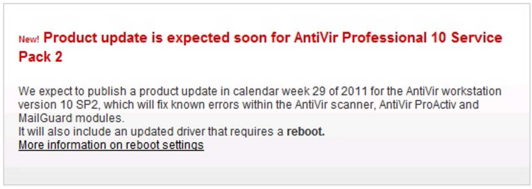
The Avira Security Management Center Frontend is started from a shortcut on the Windows Start Menu. It is necessary to log in each time, using the credentials entered during setup:



The console uses the familiar MMC format, with a tree of menu items in the narrower left-hand pane, and a right-hand pane displaying the details of the item selected on the left:



The left-hand pane shows a number of configuration/information items. Software Repository manages the installation packages to be deployed; Security Environment is used to create groups of PCs for software deployment; Network Neighbourhood, like its namesake in older versions of Windows, shows computers on the network, sorted by domain/workgroup; Events shows e.g. warning messages; Configuration shows a modest number of server settings that can be changed; User Management controls console user credentials; Internet Update Manager contains settings for the update server function. Info Center is an innovative and useful item, which gives news of upcoming service packs and updates for the software, such as the item below:



By and large, the standard format of the console, and sensible naming policy, make it very easy to find one's way around the management software. It might not be immediately apparent what Security Environment and Network Neighbourhood are used for, but this is clearly explained in the documentation, as we will see.

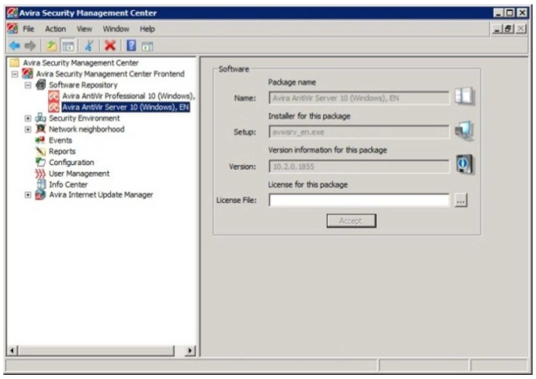
Using the manual to prepare for deployment

Having been so impressed with the How-To guide when installing the management software, we used this again, in preference to the full manual, to deploy the antivirus software to the clients. For this task too, the guide was excellent, giving very clear and simple instructions. We should point out, however, that the guide covers deployment of the management agent separately, before deploying the antivirus software.

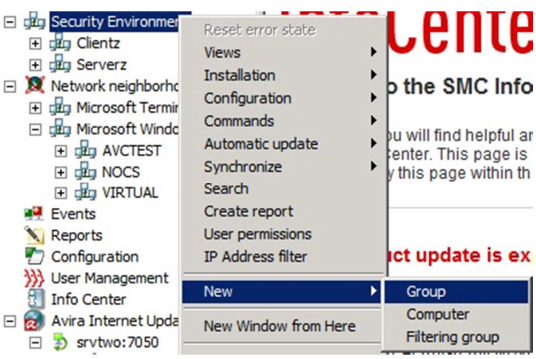
We decided to ignore this, and attempt to install the AV program first; it transpires that this is entirely possible, and that the agent software is installed simultaneously with the antivirus. We are not aware of any reason why it would be necessary to deploy the agent separately, and suggest that Avira could make their short and practical guide even shorter and more practical by skipping the instructions for this.

Deploying client software using push install

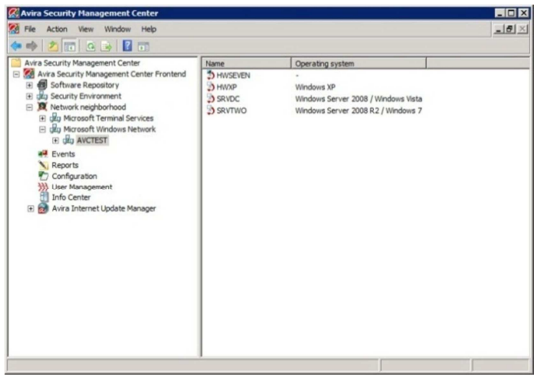
The first step in deployment is to create installation packages. This is done by right-clicking Software Repository, pointing to New, and clicking on Software. We are then able to browse to the downloaded antivirus packages. We had enthusiastically already unzipped the original zip files; this turned out to be a waste of time, as the wizard will only accept the original compressed .exe or .zip format. Having located the correct file, the console shows the selected package; it is then necessary to assign a licence to it:



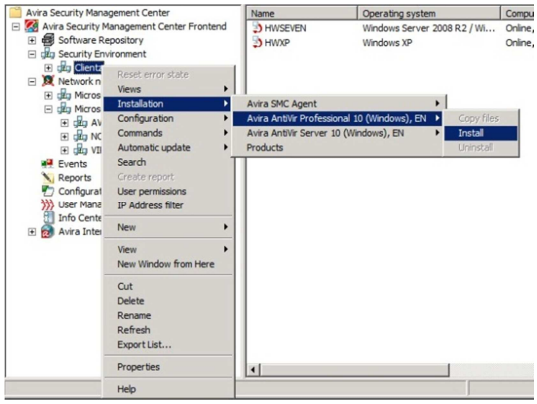
The next step is to create groups for installation. There are separate Avira AntiVir programs for workstations and servers, but each of these copes with 32 and 64-bit architecture. We thus needed to create a group for servers and a group for workstations. Creating groups is achieved by right-clicking Security Environment, pointing to New, and clicking Group:



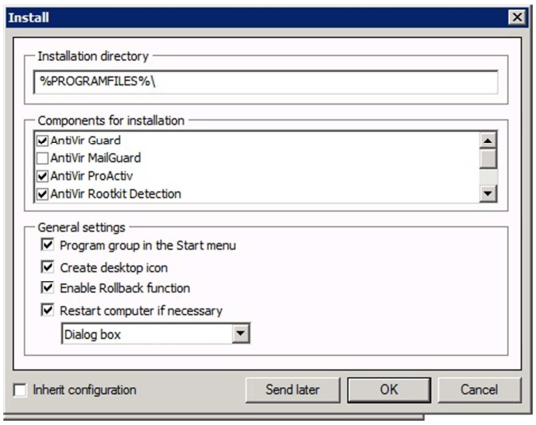
Having created our groups, we next need to populate them with computers. If you are using Active Directory you can use this to populate and synchronize your security environment. We used Network Neighbourhood, and chose the appropriate domain or workgroup (OUs are not shown):



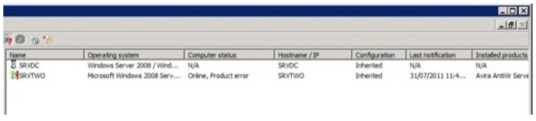
Computers can be selected by standard Windows methods, such as Ctrl + A, Ctrl + Click, and then dragged to the appropriate group in Security Environment in the left-hand pane. We put our clients and servers into their respective groups. As mentioned above, we ignored the manual and went straight to antivirus deployment (rather than first deploying the management agent separately). Installation is started by right-clicking the appropriate group, pointing to Installation, then the required program, and then clicking Install:



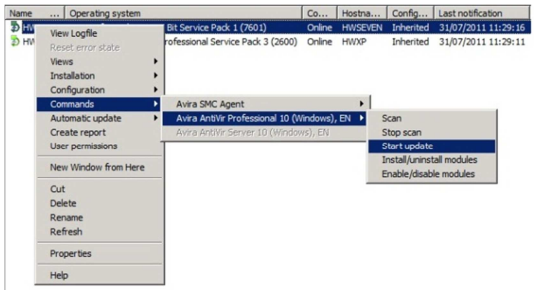
A dialog box appears, asking for administrator credentials. If you are logged on as a domain admin, you can simply select "Use the server's current account". Then comes a dialog with options for the installation directory, components, and restart options:



We felt that this was a very simple yet effective way of letting the administrator choose sensible options. By default, only the AntiVir guard (traditional antivirus) component is selected; we chose to install some additional components, such as AntiVir ProActiv (behavioural detection), but not the firewall. We left "Restart computer if necessary" selected, although in fact none of the computers was automatically restarted after installation. Clicking on OK then starts the deployment process. The console shows a real-time display of progress, but the first installation (workstations) went so surprisingly fast that we were unable to take screenshots of this in time! The real-time display of server installation is shown below; the "Product Error" status only meant that the program needed updating after deployment.



Updating the computer after AV deployment was extremely intuitive and quick. Right-clicking on the PC in the main pane produces a shortcut menu with logical submenus, from which the Update command can be run:

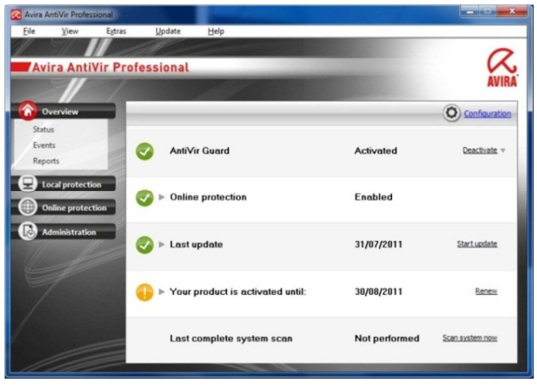


A dialog box then asks whether the update should run silently, or display the standard AntiVir update progress box.

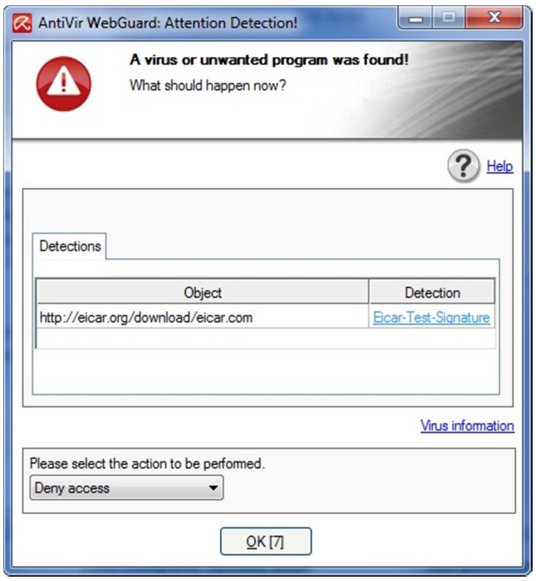
We were actually astonished at how extraordinarily quick, simple and trouble-free the entire deployment process was. Compared to other traditional business antivirus products, Avira is in a class of its own. The concise and relevant How To guide, combined with a simple and intuitive program interface, plus very speedy and reliable operation, made the entire installation process very efficient and painless.

Client Software

The workstation antivirus software, AntiVir Professional, uses exactly the same interface as its free counterpart for home users. It is a familiar modern design, with a narrow left-hand pane containing menu items, and a much larger right-hand details pane. By default, the program opens on the Status page:

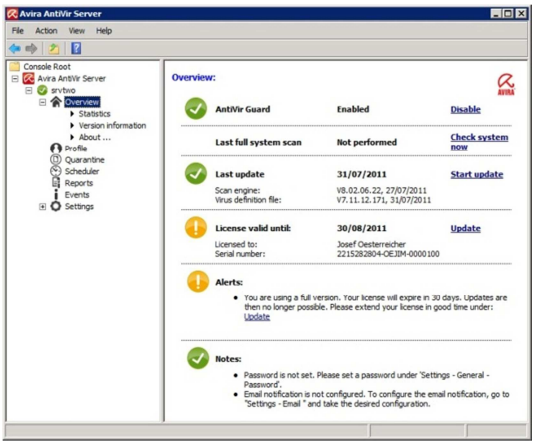


The main pane shows the status of real-time and online protection, date of last update, licence expiry, and date of last system scan. Items whose status is good are marked with a green circle with a tick (checkmark), while those whose status indicates a risk are marked with an exclamation mark in an orange circle. Links in the relevant sections allow the real-time protection to be temporarily disabled (this can be done even when logged on as a standard user), an update to be started, and a full system scan run. When we attempted to download the EICAR test virus, AntiVir blocked the webpage and download, and showed the following message box:



The default action (in this case Deny Access) is applied after 10 seconds, and the dialog box closes. No user interaction is actually required, although a quick-witted experienced user could change the action if so desired. However, it might cause less technically proficient users to worry, given that the message disappears quickly, before giving adequate time to read it. In general, we would say that the AntiVir workstation software is fine for advanced users, making essential functionality easily accessible, although some refinements for less IT-literate users might be helpful.

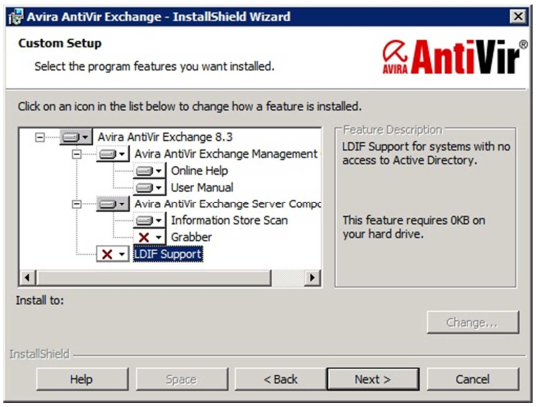
AntiVir Server, which provides standard antivirus protection for Windows Server operating systems, has a very similar layout, but in the form of an MMC console, which for system administrators is probably ideal:



Exchange Server Protection

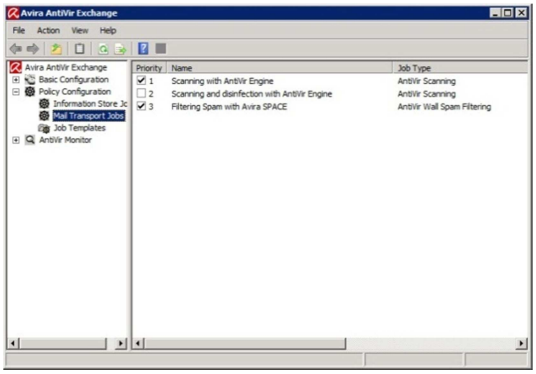
Antivirus and antispam services for Microsoft Exchange are provided by Avira AntiVir Exchange. This only protects the Exchange functions, so the AntiVir Server program needs to be installed on the Exchange server too. As with the other Avira products, AntiVir Exchange has a How To guide and a full manual. Again the manual is extensive and very professionally produced, while the How To guide covers only the essentials, and could be deemed a little rough around the edges. Indeed, one heading has not been translated from the original German: "Spamfiltering mit separaten Quarantänen". However, this should not prove incomprehensible to an English speaker, and is obviously relevant, whereas some administrators may question the significance of the high-quality photo on the cover of the manual: a gentleman who appears to have escaped from a hair-gel advertisement.

Installation of AntiVir Exchange is very straightforward, and both the manual and How-To guide consequently say little about it. There is one thing we feel is missing; the component selection includes something called a Grabber, and there is no mention in the wizard itself, or any of the documentation, what this is:



Apart from this, the installation is simple. Some Microsoft C++ runtime libraries are installed first; then come product language selection (English or German), licence agreement, component selection, path to configuration data, email address for notifications, proxy server details, and licence file.

The AntiVir Exchange program interface again uses the MMC format:



There are only 3 top-level items in the tree in the left-hand pane of the console: Basic Configuration, Policy Configuration, and AntiVir Monitor. However, each of these has several components and sub-components, meaning that there is a wealth of configuration options available. In fact, the scope of the console is so great that trying to investigate and describe all the functions available would be a daunting task. We decided to consult the How To guide for the AntiVir Exchange console, having been so impressed with its counterpart for the Security Management Center. The guide contains details of the most important functions and

clear, concise instructions for carrying out common tasks, suitably illustrated with relevant screenshots. The areas covered are:

- Creation of new email filters
- Configuration of the email filter
- Activation of the information store job
- Quarantine
- Summary reports (quarantine)
- Update settings
- Updating via proxy server
- Removing additions in subject line
- Blocking unwanted attachments
- Advanced spam filtering
- Adding a receiver automatically to the whitelist
- Password protected archives

Given the complexity of the options available in the console, we feel that having such a concise guide to help find the most important features easily is essential, especially for any administrators less experienced with Microsoft Exchange and its protection.

Conclusion

Amongst the conventional LAN-based security solutions we have reviewed here, Avira stands out clearly for its ease and speed of installation. There are a number of reasons for this. Firstly, the simple, concise How To guides allows the administrator to find essential information quickly, and explain clearly what needs to be done. Any additional software components needed such as C++ libraries, are installed automatically by the Avira installer. The design of the MMC consoles means that the user does not feel overwhelmed by too many features, and the user interface is intuitive and consistent. Client preparation is minimal, and the installation program runs quickly and reliably. Although the Avira software is suitable for use in enterprise networks, the fact that it installs so rapidly and easily makes it especially suitable for small business networks, where it does not make sense to spend a long time preparing the automated installation of just a few client PCs. We also feel that Avira would be ideal for less experienced administrators, as its installation is so simple and trouble-free.

Deployment areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)
★★★★	★★★★½

Overview:

Installation/Deployment	★★★★★
Console	★★★★½
Client Software	★★★★½
Manual	★★★★★
Overall	★★★★½

Bitdefender

Tested Software:

BitDefender Management Server 3.5
BitDefender Client Security 3.5
BitDefender Security for Windows Servers 3.5

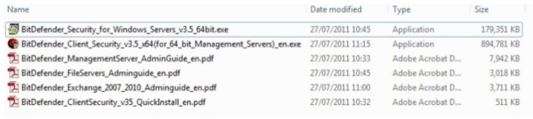
Introduction

Bitdefender's business solutions are designed for small and medium networks. BitDefender Security for Windows Servers provides protection for file servers, Exchange servers, other mail servers, and SharePoint. BitDefender Management Server is used to deploy and manage BitDefender Client Security, which protects Windows Clients. The same management console also connects with BitDefender Antivirus for Mac (Business Edition) for Apple Mac clients and two server solutions for Linux, FreeBSD or Solaris; BitDefender Security for Samba and BitDefender Security for Mail Servers. Unix-based client BitDefender Antivirus Scanner for Unices is only available as a stand-alone solution.

Software version reviewed

BitDefender Management Server 3.5
BitDefender Client Security 3.5
BitDefender Security for Windows Servers 3.5

Downloading the software



To protect our network with Bitdefender, we downloaded 2 software packages and four manuals. BitDefender Security for Windows Servers provides file and mail server protection, and BitDefender Client Security includes both the management console and the client software. Both are available for 32 and 64-bit server systems. Both Client Security packages contain client software for x32/x64 architectures, so we downloaded the 64-bit version for our server, and used it to install both 32 and 64-bit clients.

Using the manual to prepare for installation

The Management Server Admin Guide is a comprehensive PDF document of 418 pages. We found the layout and indexing to be very good, so we were quickly able to find the relevant sections to get started with the installation of the management software. An initial section gives an overview of the system, including architecture. The section on installation clearly describes the system requirements, and notes that Microsoft SQL Server Express Edition is included in the installation package. Relevant screenshots are used where necessary.

Installation of the administration software

Installation of the management server was a very straightforward process. Double-clicking the .exe starts a very standard installation wizard. This includes the usual licence agreement to accept, and a choice of Default or Custom installations; we chose the former. This informs us that Microsoft SQL Server 2005 Express Edition will be installed (the Custom option would allow for alternative database types). The final page of the wizard informs us of the ports that are used, with a note that these must be accessible:

The Default installation we used was an extremely quick and simple process. We noted that it created four Bitdefender services and a desktop shortcut to the management console.

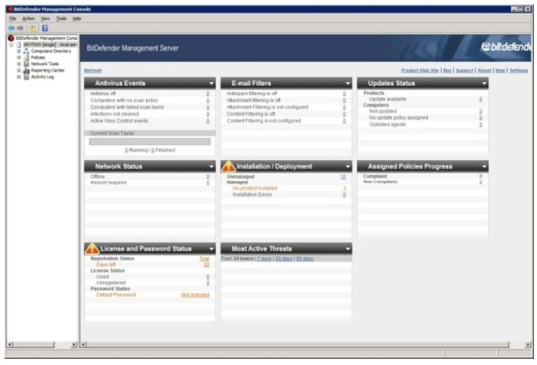
The administration console

We hit a small snag when opening the console for the first time. A username and password must be entered to access the console; these are pre-filled, but our first attempt at login

failed, and the password field was then cleared. We looked in the manual to find the default password, as no mention of this had been made during setup; it took some searching to find it (it's in the section on upgrading older versions), and we would suggest that putting it in a more obvious place would help.

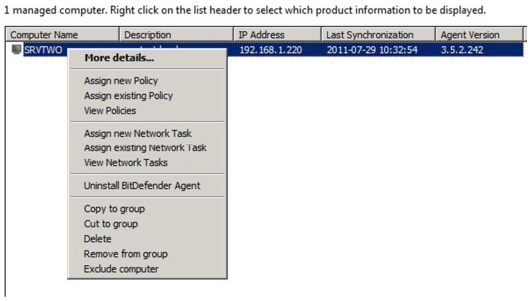
Having successfully entered the login details, we were able to see the console. It uses the familiar Microsoft Management Console as its foundation, with a narrow left-hand pane containing a tree of options, and a much larger right-hand pane to show the option selected. The default page shows an overview of the system, with 8 tiles showing important status components: Antivirus Events, Email Filters, Updates Status, Network Status, Installation/Deployment, Assigned Policies Progress, License and Password Status, and Most Active Threats.

Any area with any sort of risk is shown with any obvious warning triangle for that tile, and details of the relevant item in orange text:

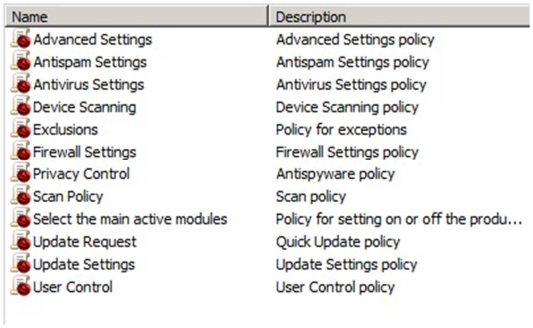


The main headings in the tree in the left-hand pane of the console are Computers Directory, Policies, Network Tools, Reporting Center, and Activity Log.

Computers Directory shows the computers in the management groups created during deployment (see below). Right-clicking on computers in this view produces a shortcut menu of tasks and policies:



Policies allow a range of settings for the antivirus software to be easily pushed out to the clients:



Network Tools includes Tasks, which allows a wide range of Windows-related tasks to be carried out, such as restart, shutdown, install Windows Updates, list current users, and configure automatic updating. Auditing enables the administrator to audit system information such as installed software, services, memory usage and so on. Reporting Center produces reports on antivirus-related issues, such installation and deployment, malware detections, and update status. Activity Log is a log of server activity, which can be set to show more or fewer events, depending on importance.

Using the manual to prepare for deployment

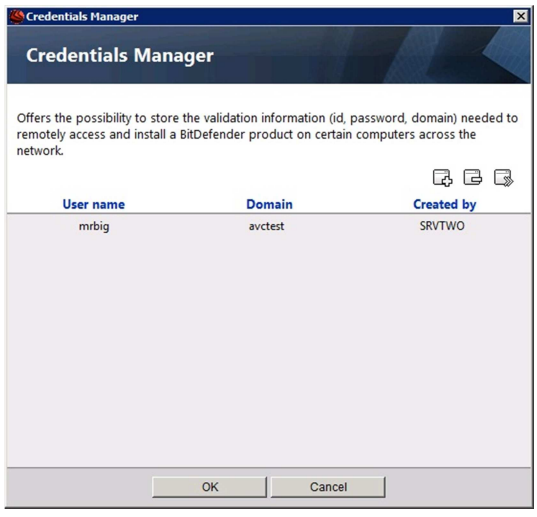
The manual has an entire section entitled Installing Client Products, which covers the installation on client PCs of the BitDefender Management Agent. This allows remote management of the client, and is a necessary step in the deployment of client antivirus software. The first section, Prepare Computers for Deployment, lists the configuration needed on clients to allow the remote

installation to work. It then goes on to describe how to provide administrative credentials for the installation task; Bitdefender has a very simple tool called Credentials Manager, which permanently stores administrator usernames/passwords to be used for deployments, meaning that they don't have to be re-entered each time. The manual then goes on to describe the deployment of the Management Agent. Installation of the client antivirus software itself is then described in the next section, Client Deployment Tools. We felt that the manual was well organised and clearly written, meaning that it was easy to find and take in the relevant sections before carrying out the deployment.

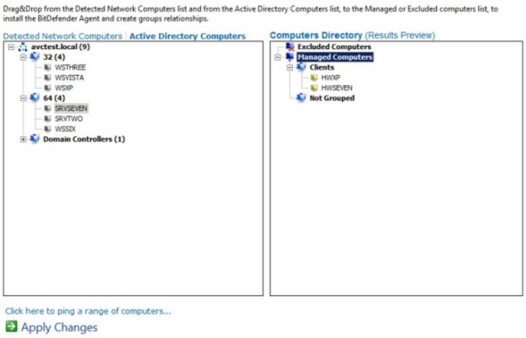
Deploying client software using push install

In accordance with the manual's instructions, we started by preparing the client PCs for the installation. This task is quite straightforward, and entails opening 3 ports on the client firewall (or deactivating it); turning off Simple File Sharing in Windows XP, and temporarily disabling User Account Control on Windows Vista. There is a sensible note in the manual to remove any existing antivirus software before installing Bitdefender, but this does not apply in our case.

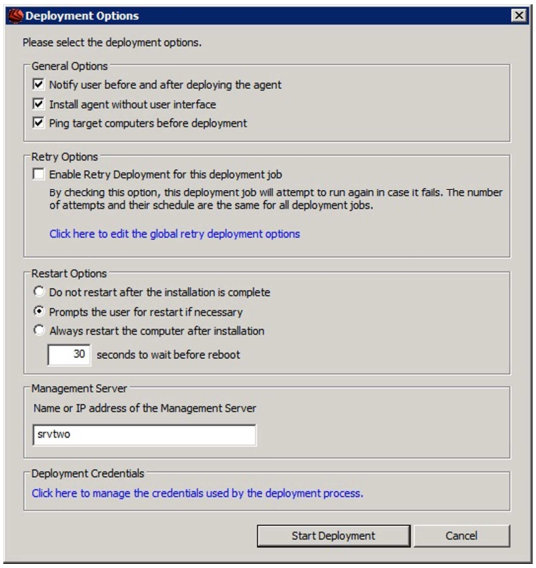
We then entered the admin credentials in the Credentials Manager, meaning that they would be saved for any future deployments:



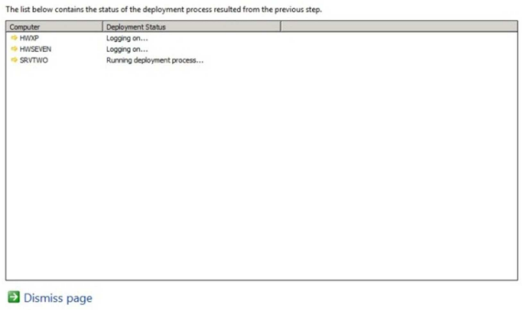
We then used the Network Builder tool to create groups of client PCs to deploy the Management Agent to. This offers a list of computers, either individually or as Active Directory domains/OUs. We chose to use the latter for our installation:



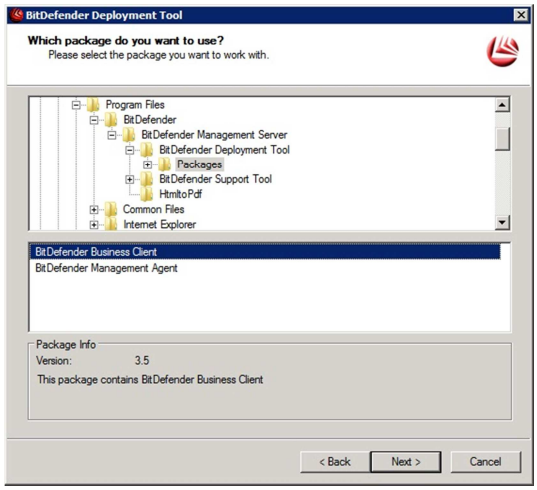
New sub-groups of Managed Computers can be created to put individual clients in, or an entire domain or OU can be dragged across from left to right, to become a new group within Managed Computers. This method of selecting clients is very simple, effective and intuitive. When we had created and populated our management groups, we clicked on Apply Changes, which brought up the deployment options dialog box:



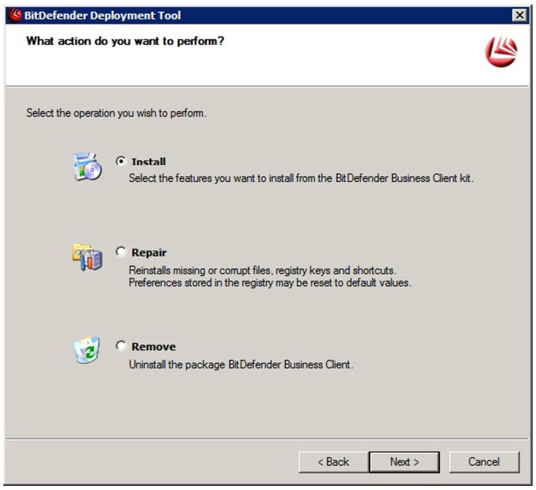
Clicking on Start Deployment begins the process, and the console then shows a reasonably detailed progress report of the installation:



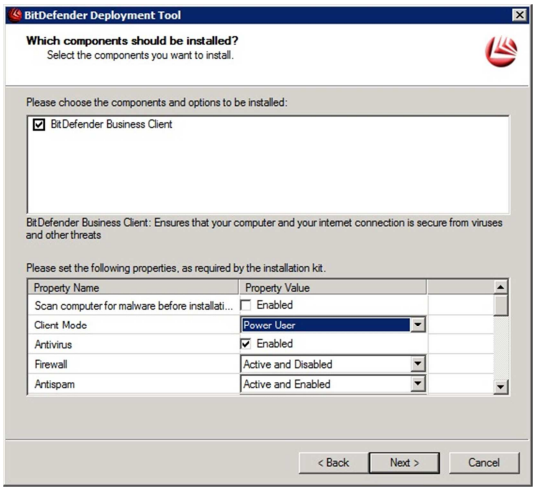
This completed the installation of the Management Agent, meaning that the next task was to deploy the client antivirus software to the managed clients. For this, we used the Deployment Tool, as described in the manual. The first step is to choose between creating an unattended installation package, and automatically installing/uninstalling/repairing a product (we chose the latter). The wizard then asks which installation package should be used:



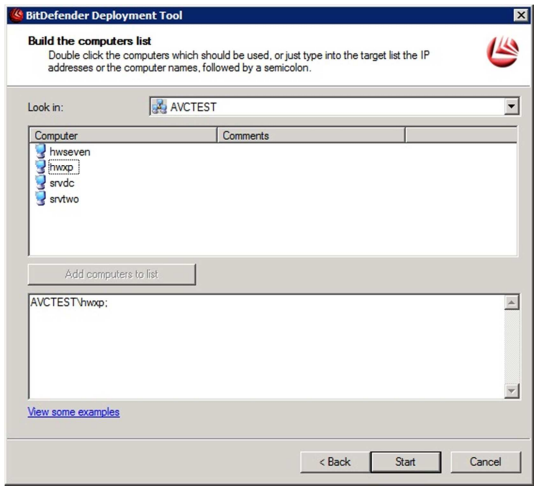
We selected the BitDefender Business Client, as the Management Agent was already installed. We then chose the option to install (as opposed to repair or uninstall) the client software:



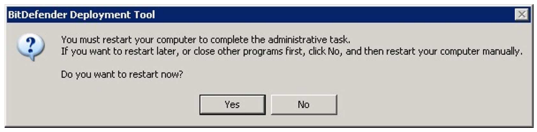
The following step allows for pre-configuration of the client software, with options to activate or deactivate antivirus, firewall and antispam components. Client Mode allows the administrator to decide whether or not users can configure the client software themselves (e.g. switch off the firewall or antimalware protection). An administrative password can be set, meaning that only an administrator can make such changes. There is also a means of scanning the client PC for malware before installation:



We felt this was an excellent range of options, allowing administrators to easily configure the software in advance. The final step is to choose the computers to be installed:



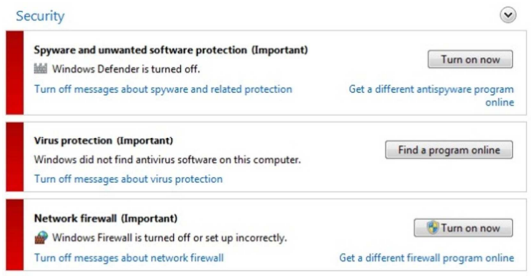
Clicking on Start begins the deployment process. A simple status display shows that the job has started/finished. On the client computer, message boxes pop up to indicate that installation has started/finished, and then that a reboot is necessary:



To summarise, we would say that the deployment process is quick, simple, and unproblematic. However, we did wonder why the management agent and client antivirus software have to be deployed separately, and whether it might not be possible to simplify the procedure even more by deploying them together.

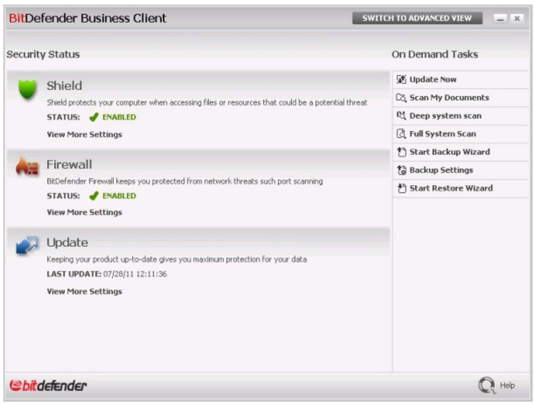
Client Software

The client software is accessible from a familiar Bitdefender icon in the System Tray. We were surprised to see that the software did not register itself as an antivirus, antispyware or firewall program in Windows 7's Action Center, even though the BitDefender Business Client does provide all three of these functions:



We did note, however, that the Action Center icon had been disabled, so there were no warning messages.

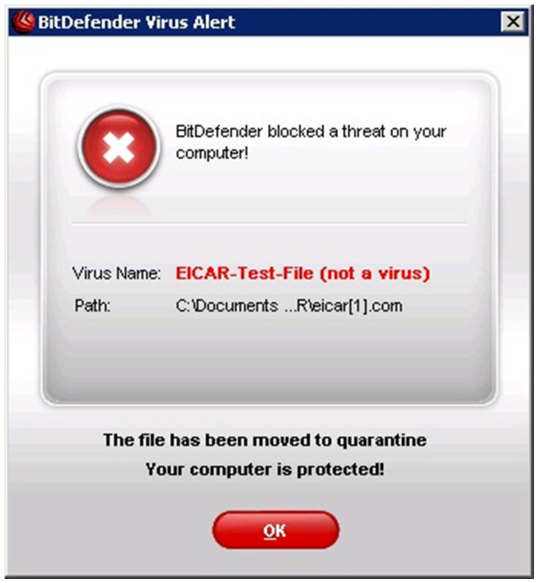
The main program window has a very simple design, with three horizontal stripes showing the status of the Shield (antimalware protection), firewall, and updates. A vertical column on the right-hand side of the window contains a menu of simple user tasks, such as updating, scanning, and backing up. This simple interface is ideal for the average user, presenting simply and clearly the most important status information and tasks.



If the administrator sets the Client Mode to Power User during the deployment (see above), the Advanced View will allow the user to make significant configuration changes, such as temporarily disabling the firewall or malware protection. This is unaffected by the status of the Windows user, i.e. whether they have admin privileges or not. However, as mentioned above, these settings can be password protected by the administrator, to prevent standard users making any changes.

If antivirus protection is disabled, the Bitdefender System Tray icon changes from red to grey, and the Shield status display changes to "Disabled" in red, with a red cross.

These warnings are relatively insignificant and might be overlooked by an inexperienced user. There is no fast method of reactivating the protection, only returning to the advanced settings. When we attempted to download the EICAR test virus, the Bitdefender software immediately produced a message box which clearly informed us that the threat had been stopped and the computer was protected; no user interaction was required at all.



We noted that the Bitdefender software also includes an anti-phishing toolbar for Internet Explorer.

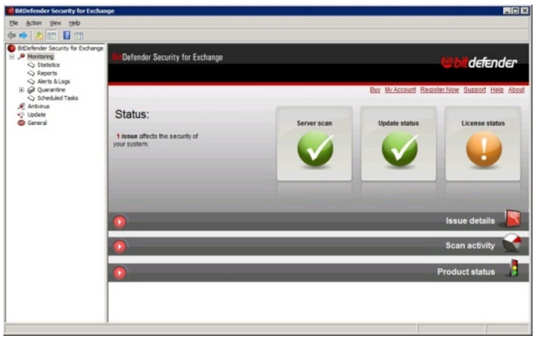
Server Protection

BitDefender Security for Windows Servers provides malware protection for both file server and Exchange Server functions. There are additional components for protecting SharePoint servers and other mail servers, although we did not install these. There are two manuals relating to the components we installed, namely BitDefender Security for File Servers, and BitDefender Security for Exchange. As both components use a common installation file and more-or-less identical consoles, there is some overlap between the two manuals.

Setup involves running the .exe file, which starts an installation wizard. This includes the usual licence agreement, the opportunity to scan the server for malware before installation, and a component selection:

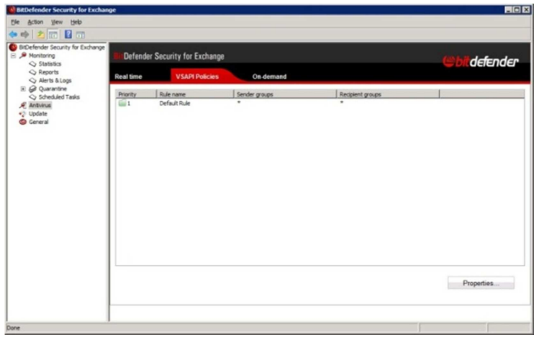
We were initially confused as to why Exchange and Mail Servers were listed as separate items, and attempted to install both, but a message box informed us that they cannot be installed together. We thus presumed that "Mail Server" relates to non-Exchange mail systems, and deselected it. Other stages of the installation include the option of submitting incident reports to Bitdefender to improve the product, and specifying a sender's email address for this function. The setup process is quick and simple.

The BitDefender Security for Windows Servers installs two separate consoles, again based on the Microsoft Management Console, for the Exchange Server Security and File Server Security. The Exchange console is shown below:

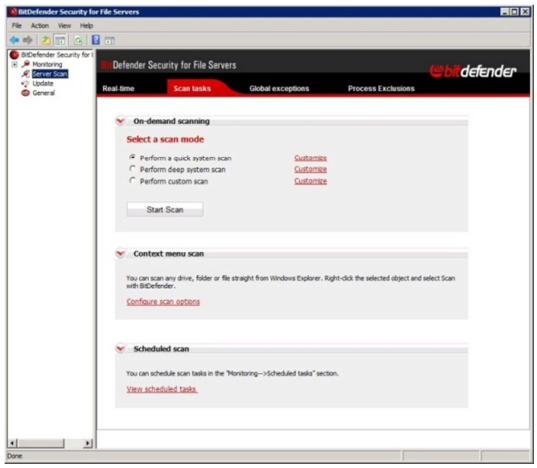


It opens with a status display in the main pane, showing the status of server scans, updates and licensing. Clicking on one of the three main status buttons expands the

relevant section in the lower half of the window to show the details. The tree in the left-hand pane includes links to Monitoring, Antivirus, Update, and General. These have sub-options, in the form of tabs at the top of the main pane. For example, Antivirus has the sub-options Real Time, VSAPI Policies, and On-Demand:



The File Server Security console is virtually identical, with some different sub-options where appropriate, e.g. scanning options:



The consoles are clear and simple, making it easy to find specific tasks or information. There is one exception: it is unclear to us how to get back to the initial status page, other than by restarting the console or using the "Back" button. When we attempted to download the EICAR test virus, the download was blocked, although no warning message appeared. Looking at the log file showed clearly that the "threat" had been discovered and deleted, however.

Conclusion

We found using Bitdefender to protect our small business network particularly quick, simple and unproblematic. The manual explains clearly how to install and deploy the software, and the procedure is simple in practice. The management console gives the administrator the ability to carry out a wide range of tasks and audits, not only for the antivirus software, but also for the entire Windows system. There is very little to criticise, and the management features make the software very suitable for medium-sized business networks.

Bitdefender's management console gives the administrator the ability to carry out a wide range of tasks and audits, not only for the antivirus software, making it very suitable for medium-sized business networks.

Deployment areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)
★★★★	★★★★½

Overview:

Installation/Deployment	★★★★½
Console	★★★★½
Client Software	★★★★
Manual	★★★★½
Overall	★★★★½

eScan

Tested Software:

eScan Management Console 11.0.1139.1043
eScan Corporate Protection Center 11.0
MailScan 6.4.0

Introduction

MicroWorld make 3 ranges of security software, namely Home/Home Office, Small Business, and Corporate/Enterprise. We have looked at the Corporate Edition in this review.

Software version reviewed

eScan Management Console 11.0.1139.1043
eScan Corporate Protection Center 11.0
MailScan 6.4.0

Downloading the software

The management console and client software come together in the form of one single .exe file, plus one hotfix, which we ran after the main installation process. There is another .exe file for MailScan, the Exchange protection. There is one manual for the management console, although there was no link to this on the software download page, and we had to search the website to find it. The manual for MailScan was being revised at the time of the review and so was temporarily unavailable.

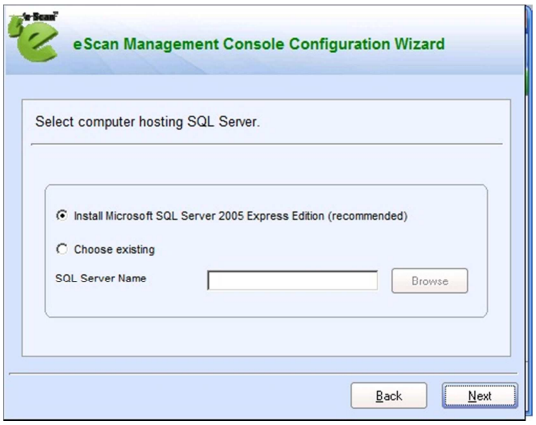
Using the manual to prepare for installation

The manual is very comprehensive, at 124 pages. There is a very detailed and comprehensive table of contents showing the titles of all sections and subsections. The items in the table of contents have been linked to relevant bookmarks, so having found the item you want, you simply click on it to go straight to the relevant section. There are bookmarks within the document, and these can be used to navigate using the Bookmarks Pane in Adobe Reader. Navigating through the manual is thus very quick and easy. Whilst there are occasional reproductions of individual icons from the program interface, there are no screenshots as such. We feel this is a shame, as screenshots are such a simple and effective way of quickly explaining the functioning of software.

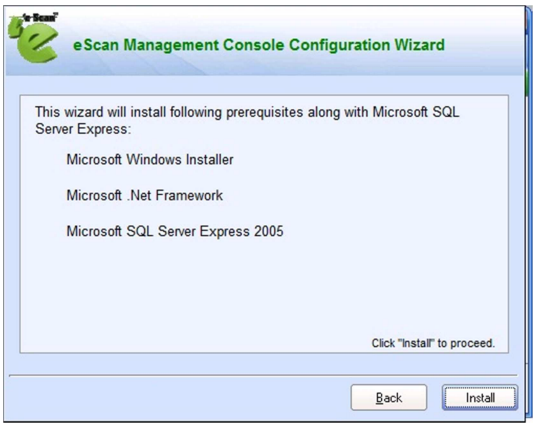
The manual doesn't actually explain the installation of the management console at all. However, it turns out that the process is so simple that this is not a problem.

Installation of the administration software

Installing the eScan Management Console is a very quick and easy process, and the lack of instructions in the manual did not matter at all in our case. Double-clicking the installation file starts a setup wizard, with the usual licence agreement to accept and a choice of installation folder location. The wizard then asks if we want to use Microsoft SQL Server 2005 Express Edition (included), or use an existing SQL Server installation (we chose the former):

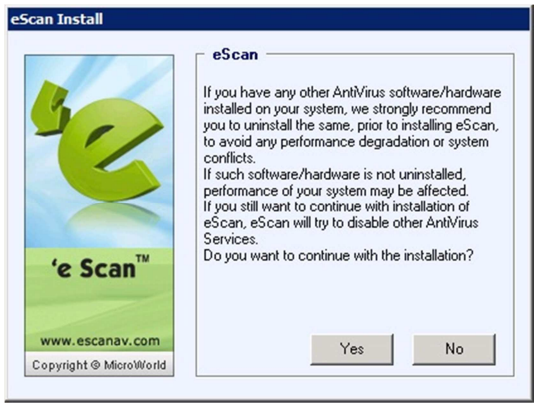


We are informed of the additional components that will be installed:

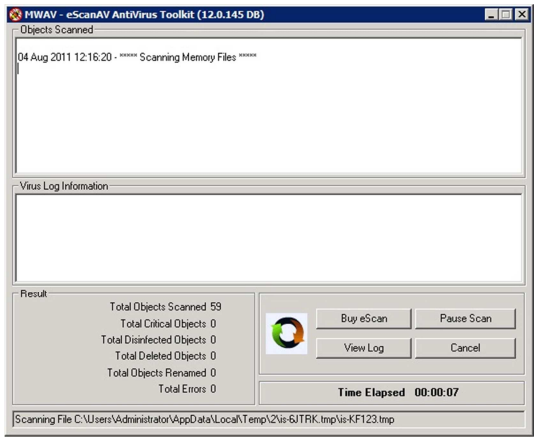


The wizard next informs us that it will "proceed with eScan installation", meaning the antivirus protection for the server itself. There is almost no interaction required here;

we just have to confirm a warning about removing existing antivirus software:



When the eScan antivirus software has been installed on the server, it runs a quick scan:



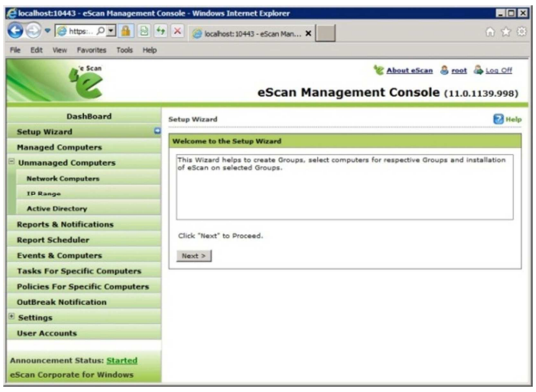
In summary, the setup process is very straightforward, and installs both the management console and server antivirus software quickly and easily.

The administration console

eScan's management console is web-based. The first time we attempted to open it, the following message box appeared:

As we were using Windows Server's default Internet Explorer Enhanced Security Configuration, we had to reconfigure this to allow the ActiveX component to install. Opening the console then produces a certificate error; however, there are clear instructions in the manual on how to import the certificate, which we followed successfully.

The console has a familiar layout, with a narrow left-hand pane containing menu items, and a larger right-hand pane to show the details of the item selected:



By default, the console opens on the setup wizard page; this is the default client deployment method, described below. Other items in the menu are Managed Computers, Unmanaged Computers, Reports and Notifications, Report Scheduler, Events and Computers, Tasks for Specific Computers, Policies for Specific Computers, Outbreak Notification, Settings, and User Accounts.

Managed Computers displays those machines on which eScan software has already been deployed. It allows tasks to be performed on individual computers or groups. Unmanaged Computers allows machines to be selected, either by domain or IP address range, and added to groups for deployment. Reports and Notifications can be used to inform the administrator about malware detected, update status and so on. Tasks for Specific Computers allows specific components of the client software to be activated or deactivated, scans to be started and definition updates to be downloaded. Policies for Specific Computers enables the administrator to change settings e.g. for action to be taken on malware discovery. Outbreak Notification can be used

to send out a warning in the event that the number of infections exceeds a certain number within a certain time. Settings allows configuration of e.g. proxy servers and FTP settings. Finally, User Accounts can be used to create accounts for access to the admin console.

Using the manual to prepare for deployment

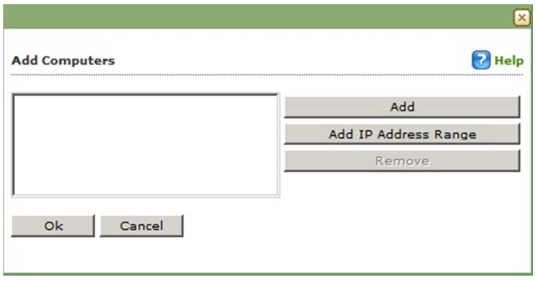
The section relating to client preparation before deployment doesn't actually contain the instructions itself, but has a hyperlink to a page on eScan's website. Whilst we found this a little strange, the website gave concise instructions for preparing XP, Vista and Windows 7 clients for deployment, which we followed. The manual itself contains a section on client deployment using the setup wizard. The instructions given are clear and simple, though we particularly missed screenshots here.

Deploying client software using push install

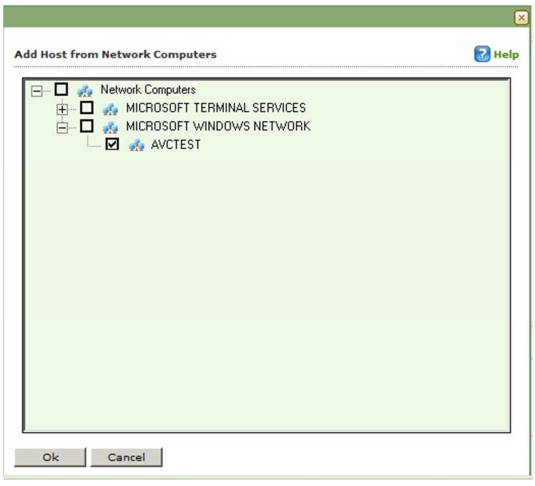
The Setup Wizard is started by clicking on the appropriate link in the console. We noticed that despite disabling the Enhanced Security Configuration in Internet Explorer, clicking "Install" on every ActiveX prompt, restarting the browser and then the server, every time we started the Setup Wizard, a prompt to allow installation of ActiveX components always appeared. We are unsure if this affected functionality, but it is certainly irritating.

The first step is to create a group or groups of computers for installation. Creating different groups allows the installation options to be varied; if the administrator is content to use the same options for all computers, one group can be used. Clients then need to be added to the group, which can be done by clicking "Add IP/Host" or "Add Host from Network Computers":

"Add IP/Host" allows individual hostnames, individual IP addresses, or a range of IP addresses, to be added:

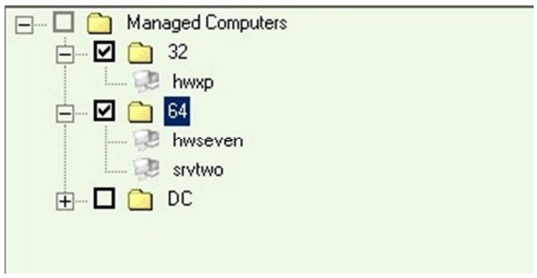


"Add Host from Network Computers" allows specific domains or workgroups to be added, though there does not appear to be an option to add specific OUs of a domain:

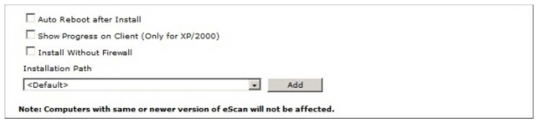


We found that groups can only be deleted immediately after creation. It's possible to move clients out of the group and into another, but not to remove the group later. We would say that creating groups and assigning computers would work well if the admin is familiar with the console and is certain of the group structure before starting the process. It's not ideal for anyone who is

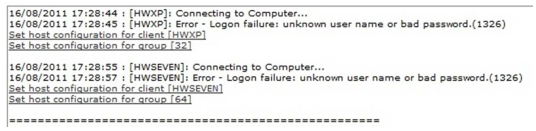
new to the software and undecided about which groups to use.
The groups which are to be installed can now be selected:



The final step is to select the installation options, which include rebooting after installation, omitting the client firewall component, and the installation path:



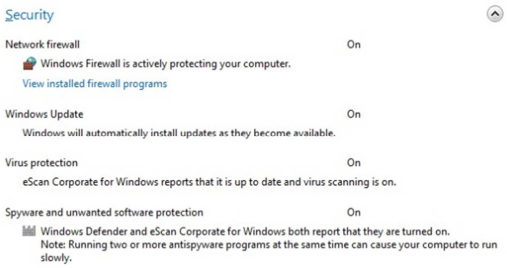
After clicking on Next, we saw the following message:



The term "Error – login failure" is a little worrying, but the situation and the appropriate action are clearly described in the manual. Clicking on the link entitled "Set host configuration for group..." allowed us to enter administrator credentials for each of our two test groups. We then restarted the Setup Wizard, which rapidly completed successfully. We would suggest that the manufacturers might like to change the wording of the message to sound less alarming.

Client Software

The client software installs a system tray icon, and registers itself in the Windows 7 Action Center as the antivirus and antispyware program. Although the eScan firewall is installed, it is not activated by default, so Action Center shows Windows Firewall as the active firewall protection:

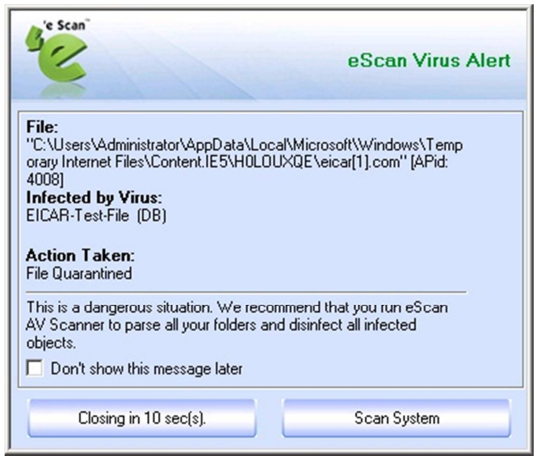


The program interface is essentially identical to that used in eScan's consumer Internet Security Suite:

To the uninitiated, the unique design can appear rather confusing. The 7 main protection components (file antivirus, spam protection, firewall etc.) are represented by icons in a horizontal row at the bottom of the window. The icons are very artistic, but for many people it will not be immediately clear what they represent. We are also concerned that when the file antivirus component is deactivated, the small warning symbol that appears next to its icon does not stand out sufficiently, especially given that four of the seven components are deactivated by default and show the same symbol. However, having become familiar with the interface, the administrator will find that essential status information and configuration options are actually very easy to find. The three buttons in the top part of the window, Scan, Update and Tools, give quick access to the most important functions. Scan gives an excellent

choice of scan types, including setting up a scheduled scan. However, we noticed that on most of our computers, a number of configuration options (such as setting up scheduled scans and deactivating real-time protection) were disabled, even when logged on as a domain administrator. Micro World inform us that these functions can be enabled from the console.

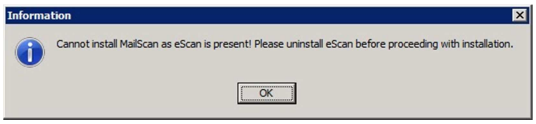
When we tried to download the EICAR test file, eScan blocked the download and displayed the following warning message:



The message informs us that the file has been quarantined, and no user interaction is required (although a scan is recommended). The warning disappears after 10 seconds, which is probably fine for users who are familiar with it; for some users, however, 10 seconds will not be long enough to read and understand the message, and they may be concerned that the PC has become infected.

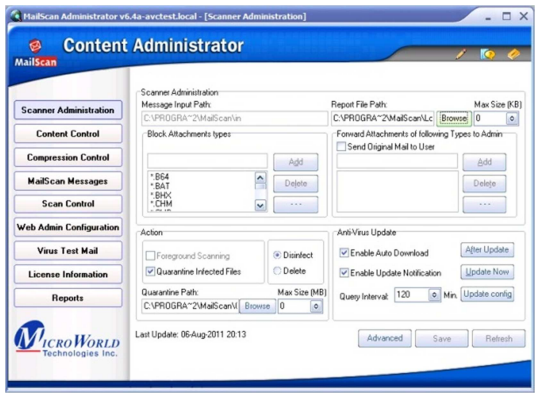
Exchange Server Protection

To begin with, we should mention an important point for administrators who wish to install eScan Antivirus and MailScan Exchange Server protection on the same server. MailScan has to be installed first, and eScan second. We were not aware of this, and so when we attempted to install MailScan, the following message box appeared:



We thus had to uninstall eScan, and reinstall it after installing MailScan. Naturally we would suggest to MicroWorld that informing users of the necessary installation order, via the manual or initial message in the setup wizard, would be very helpful.

Having got over this initial hurdle, we found installing MailScan to be a straightforward process, involving accepting a licence agreement, choosing an installation folder, selecting the Exchange Server role, and entering a password for notifications. The MailScan Adminstrator Console follows the standard pattern of a column of menu items on the left, and a large display panel on the right:



We think it would be fair to describe the main panel of the window as utilitarian, in that eScan have not wasted any time on aesthetics. It is, however, clear and functional. The console opens by default on the Scanner Administration page, which provides message scanning options. Content Control allows the administrator to check the content of emails, and add a disclaimer to outgoing messages. Compression control can compress outgoing attachments for faster transmission, while MailScan Messages allows messages to be sent to senders/recipients whose messages have been found to contain e.g. malware. Scan Control allows rules to be created that enable or disable scanning of

messages to or from specific users. Web Admin Configuration has options for the web-based version of the console, while Virus Test Mail is a very useful function that sends an email containing the EICAR test virus to a local Exchange mailbox. This allows the administrator to test whether virus scanning is working properly. Licence Information is self-explanatory, whilst Reports allows specific information to be extracted from the logs.

Despite its somewhat primitive appearance, the MailScan Administrator provides a number of very useful functions in a very easily accessible format.

Conclusion

eScan's corporate suite is in many ways well designed and easy to use. Local installation of the management console and Exchange protection is quick and easy. The program windows allow easy access to all important functions (even if the interface of the client software is initially a little confusing). The manual for the management console is well-written and very easy to navigate, due to excellent indexing and bookmarking. There are one or two minor irritations such as the lack of information about the correct installation order on the Exchange server, although we are confident that MicroWorld will rectify these. The eScan security software package could be used successfully for large or small businesses.

Deployment areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)
★★★½	★★★★

Overview:

Installation/Deployment	★★★★
Console	★★★★
Client Software	★★★★
Manual	★★★★
Overall	★★★★

ESET

Tested Software:

ESET Smart Security Business Edition

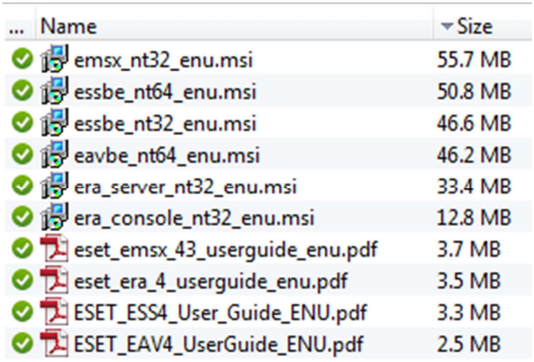
Introduction

ESET make a single line of business products for Windows, which can be used for both large and small networks. With endpoint protection for client PCs, there is a choice of Business Editions of NOD32 Antivirus or ESET Smart Security; the latter additionally includes a client firewall and local spam filtering. ESET Mail Security provides complete antivirus protection for the Microsoft Exchange server, i.e. it covers both host protection (file server function) and the mail server function. The ESET Remote Administrator (ERA) package allows remote installation, monitoring and management of the software. ERA is provided free with the Business Edition of the client antivirus software (Smart Security or NOD32).There are 32 and 64-bit versions of both client and server programs. We note that ESET additionally provide antivirus solutions for Linux and Mac OS X clients, as well as Linux servers.

Downloading the software

ESET's website is essentially very clear and well designed, although we were just a little bit confused about the server products. It was not initially clear to us that ESET Mail Security is a complete antivirus solution, covering both host protection and mail server functions, so we incorrectly assumed that we would need to install NOD32 on our mail server as well, to provide host protection.

To protect our network with ESET software, we actually needed to download 6 separate packages. These were: Smart Security Business Edition, 32 and 64-bit versions, for the client PCs; NOD32 Business Edition for the file server; Mail Security for the Exchange server; Remote Administrator Server and Remote Administrator Console for central management of the software. We also needed 4 manuals: one each for Smart Security, NOD32, Mail Security, plus one manual to cover the two remote administration packages.



...	Name	Size
	emsx_nt32_enu.msi	55.7 MB
	essbe_nt64_enu.msi	50.8 MB
	essbe_nt32_enu.msi	46.6 MB
	eavbe_nt64_enu.msi	46.2 MB
	era_server_nt32_enu.msi	33.4 MB
	era_console_nt32_enu.msi	12.8 MB
	eset_emsx_43_userguide_enu.pdf	3.7 MB
	eset_era_4_userguide_enu.pdf	3.5 MB
	ESET_ESS4_User_Guide_ENU.pdf	3.3 MB
	ESET_EAV4_UserGuide_ENU.pdf	2.5 MB

ESET provided us with a username and password, plus a separate licence key file, to cover the file server and client antivirus programs, and the remote administration software. They also provided a second username and password, plus licence key file, for the Exchange antivirus software.

Using the manual to prepare for installation

The Remote Administrator manual comes in the form of a PDF file. It is very comprehensive, at 107 pages. Fortunately, it is laid out very clearly in logical sections, with suitable headings for the sections and subsections. This makes it very easy to find a particular section using the navigation pane in Adobe Reader, or the very detailed table of contents at the start of the manual. Both contain links to bookmarks, so that clicking on the section heading or page number conveniently takes the reader directly to that section. There are relevant screenshots where necessary.

The first section covers new features in the latest version, and gives an overview of the architecture: the Remote Administrator Server runs as a service (normally on a server) and is responsible for communication with the client PCs, while the Remote Administrator Console is installed on the administrator's workstation, connects to the Remote Administrator Server, and provides the interface for controlling it remotely.

The Installation section of the manual starts by providing comprehensive system requirements for the computers used for the

ERA Server and Console software, including possible databases on the server. There are also details of the data traffic produced by client/server communications, and the storage capacity using the default MS Access database. Finally, there is information on the ports used for client/server communications. Prior to installation, we opened all 9 ports mentioned here on our server's firewall.

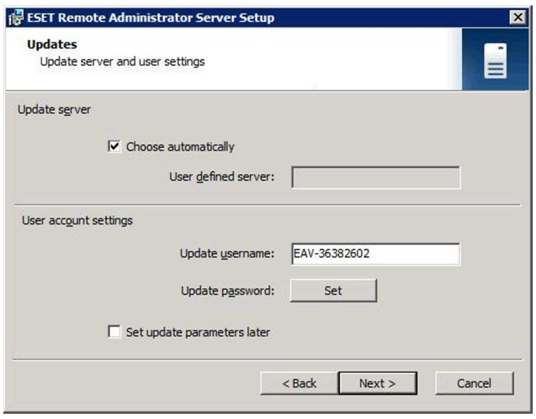
The Installation section then continues with an overview of the network structure, and a checklist of packages to be downloaded, including client software. Instructions on the actual installation are concise but include important points such as running the ERA service using an admin account. There are sections on installation using a command line, cluster mode installation, and in an enterprise environment with more than one office.

Having looked at the initial sections of the manual, we felt confident that we had acquired a good overview of how the ERA software works, and that our system had been suitably prepared. The very clear layout and indexing of the manual meant that it was easy to find the parts relevant to our small business network, and skip sections that apply to larger enterprises with more complex networks.

Please note that ESET also produce a Quick Start Guide, an 8-page document with the essential information needed to download and install the management server and deploy client software.

Installation of the administration software

Installing the ERA Server software is a standard process of double-clicking an MSI file and completing a setup wizard. Steps include accepting a licence agreement, choosing between standard and custom installations (we chose standard), locating a licence key file, setting passwords for various administration tasks, and entering a username and password for updates. The need to enter both a licence key AND the username/password combination may be a little confusing to some users, but is described in the installation section of the manual:

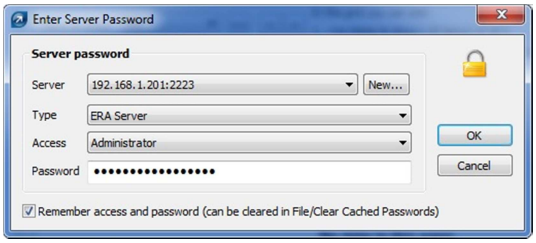


On completion of the installation wizard, we noted that ESET had created two Windows services for remote administration.

Installing the ERA Console software on a workstation also involves running an MSI file and going through a wizard. This gives the choice of standard or custom installations (we chose standard), and installation folder. Installation is very quick and easy, and creates a Desktop shortcut to ESET Remote Administrator Console, with which the console can easily be started.

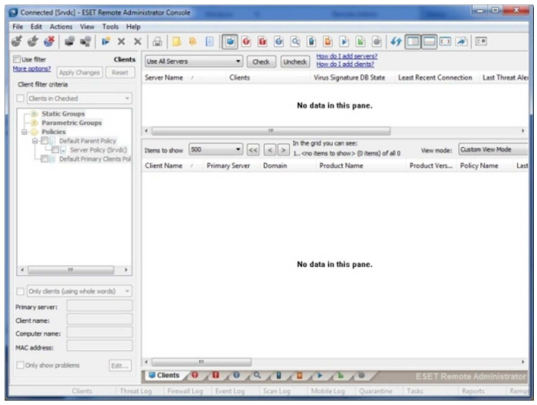
The administration console

Starting the console involves entering server details and credentials into a logon dialog box:

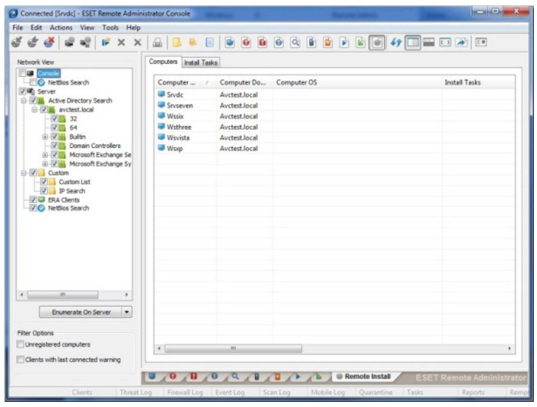


When it opens, the main console window is essentially similar to Windows' MMC consoles. There is a narrow left-hand "tree" pane and a much bigger right-hand "details" pane. Rather worryingly, the default view shows the message "No data in this pane" in both the

main pane and a secondary horizontal pane above it:



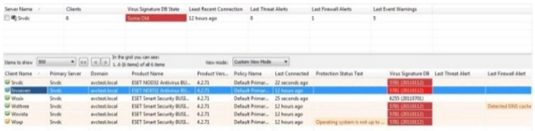
This left us feeling that connection must have been unsuccessful. In particular, the column heading "Server Name" in the top right-hand pane made us think that the name of our administration server should appear here if connection had been successful. Consulting the manual did not provide any assistance, as its explanatory diagram shows both right-hand panes of the console populated with computers, which actually increased our feeling that something was wrong. It transpires that changing the view from the standard Clients Pane to Remote Install Pane (using View menu, toolbar icon or tab at the bottom of the window) brings up a comprehensive tree of search options in the left-hand pane, with the appropriate details in the right-hand pane:



Once we had discovered this view, it became apparent that everything was working correctly. However, we only stumbled across this view through trial and error. We feel that a simple screenshot in the manual, showing the *default* console view, together with a brief explanation of how to change views, would avoid potential confusion for anyone unfamiliar with ESET's console. We also note that the console appears a little daunting in its scope, with menus, a toolbar and the row of tabs along the bottom. However, there is a considerable degree of duplication, with the views shown on the tabs being repeated both on the toolbar and in the menus.

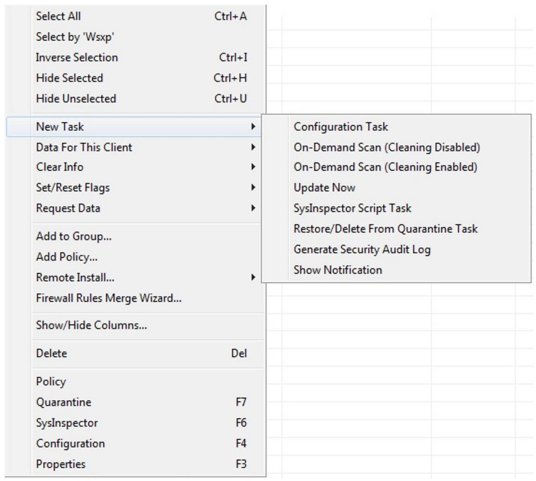
Once the antivirus software has been deployed to some clients, the Clients pane becomes populated, and it becomes easier to see how the console works. The row of tabs along the bottom of the main pane allows switching between major views, including Clients, various logs, Quarantine, Tasks, Reports and Remote Install:

The Clients view lists installed clients, along with the server that manages them, and comprehensive status information. This includes administrative server and domain, product name and version, policy name, last connection, protection status, virus signature version, and last threats, as shown below:



Additional columns not shown in the screenshot above are: Last Event Warning, Last Files Scanned, Last Files Infected, Last Files Cleaned, Last Scan Date, Restart Request, OS Name, Custom Info, and Comment.

This view can also be used to launch a variety of tasks and show data, by right-clicking on a client (or selecting multiple and right-clicking), which produces the following context menu:



The Threat Log and Firewall Log respectively show alerts created by malware discovery and attempted network attacks; the Event Log shows routine maintenance events, such as updates and submission of data to ESET; the Scan Log shows the results of client antivirus scans. The Mobile Log is not applicable to our review as it relates to mobile devices such as smartphones. Quarantine shows a list of malicious programs quarantined by client PCs, while Tasks shows both current and completed tasks such as installation. Reports allows the administrator to search the database with specific queries, such as client PCs or users with most threats. The Remote Install tab is described in the section on deployment below.

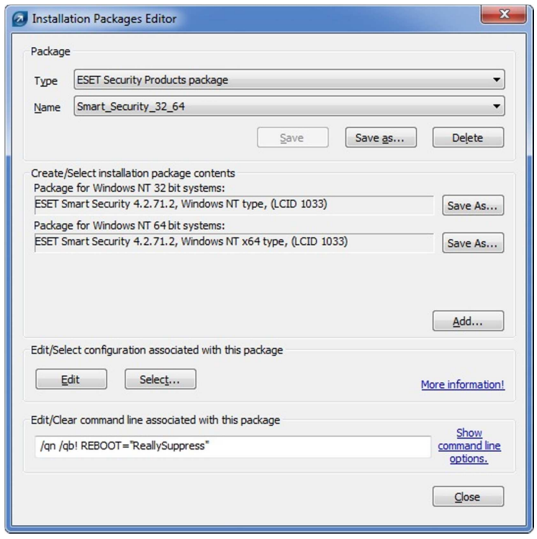
Using the manual to prepare for deployment

ESET's manual has a section entitled "Installation of ESET client solutions". This gives comprehensive details of all possible means of deploying the antivirus software to clients, including local installation on each client computer by the administrator (details of how to do this are of course found in the client software's own manual). Right at the beginning of the installation section are helpful notes about installing servers, and how to configure remote installation without disrupting Remote Desktop access to the client PCs. The ERA manual also lists four possible means of remote installation: remote push; logon script; email; upgrade.

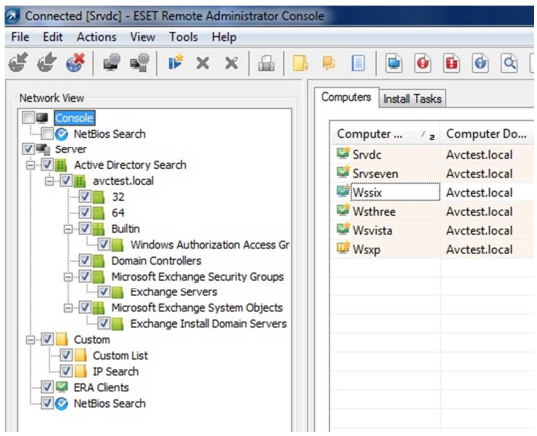
All four methods of remote installation require the same preparation, which is described first. This involves creating installation packages for the client software, based on the MSI installers, which can be adapted by the use of xml configuration files and/or command line switches. A comprehensive list of the latter is provided. There is also a detailed but clear list of client configuration requirements, such as services to be enabled and ports to be opened. A note at the end of this section points out additional steps needed on newer versions of Windows that incorporate User Account Control. The manual goes on to describe a very useful feature of the software, Push Installation Diagnostics, which runs a check on client PCs to see if they have been correctly configured for remote installation. ESET have been very thorough in their preparation of the deployment instructions, which are clear and include every important detail.

Deploying client software using push install

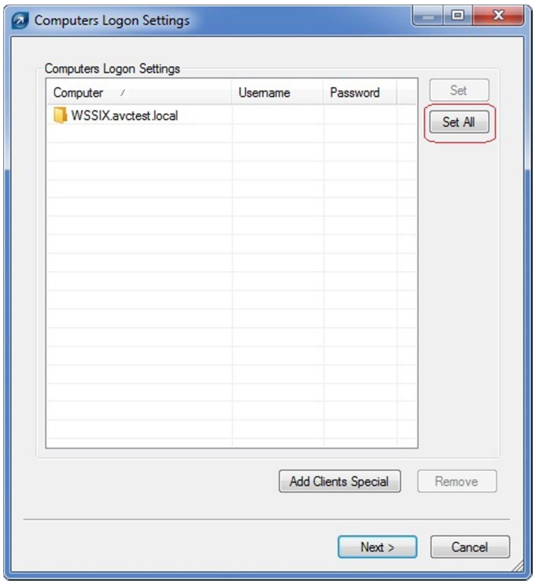
The procedure for running a push installation is very straightforward, and well described in the manual. In the console, click on the Remote Install tab, then Computers. First of all, a suitable installation package has to be created. This is done by right-clicking in empty space in the main pane, and selecting Manage Packages. The dialog box that appears allows the administrator to select the MSI installation files to be used, plus a configuration file and command-line switches. ESET client software has two different MSI installers, for 32 and 64-bit Windows respectively; however, the dialog box allows both installers to be included in one package, and the appropriate installer will automatically be applied to each client PC on the basis of its architecture. The screenshot below shows the package we created with 32 and 64-bit installers for Smart Security:



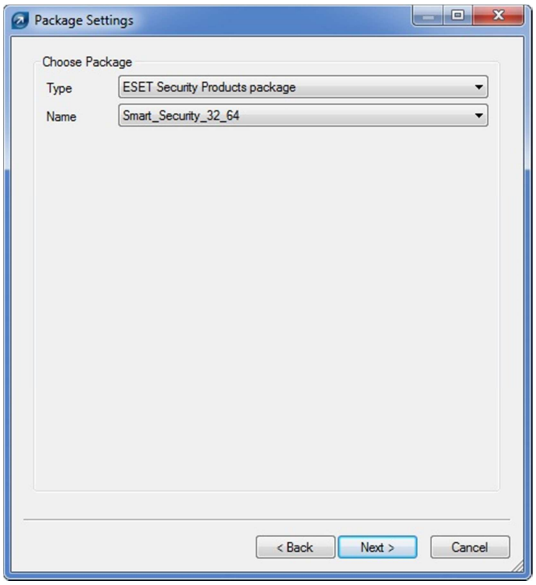
Having created the installation package, the next step is to select the PCs to be installed from the list in the console window. Fortunately, the tree view in the left-hand pane allows numerous options for selecting PCs, including Active Directory Operation Units (our test OUs being "32" and "64"):



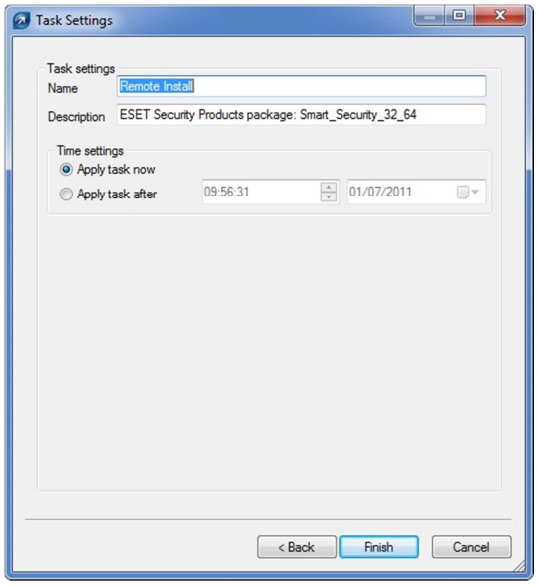
To continue, right-click on the selected PCs and then click Push Installation. The first step of the resulting wizard asks for administrator username and password, whereby there is the choice of using different credentials for different machines, or one set for all (Set All):



After this, the installation package is selected:



The final step is to give the installation task a name, and select a time for it to run:

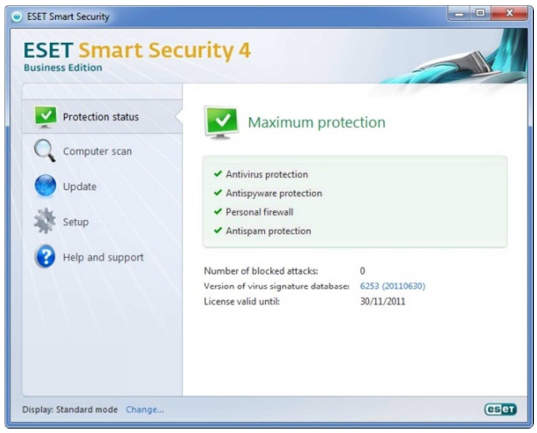


Clicking Finish starts the push installation process. The status display in the console is limited to a very short description, such as "In Progress" or "Finished".

In our test, we found that installation ran smoothly. The software installed on our 32-bit XP, Vista and Windows 7 clients, and the 64-bit Windows 7 PC, the system automatically selecting the correct version for the architecture on each machine.

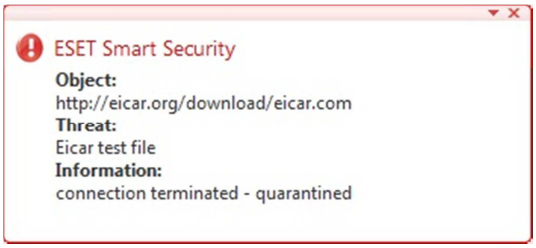
Client Software

ESET Smart Security Business Edition client software registers itself in Windows 7's Action Center as antivirus, antispyware and firewall software. The program's interface is virtually identical to its home counterpart. It has a very clear, simple, modern interface, with a menu panel in a left-hand column, and details displayed in a larger right-hand panel.



By default, the window opens on the Protection Status page, which clearly shows whether the essential features are working correctly. In the event that a component is deactivated, the warning message on the status page includes a link to reactivate the feature. The most important features, updating and scanning, are easily accessible from the menu panel on the left.

Attempting to download the EICAR test virus immediately brings up an ESET message box, informing us that the threat has been dealt with. No user interaction is required:

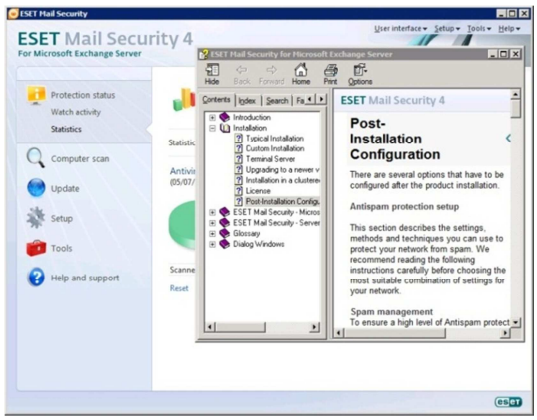


Disabling the real-time protection or firewall can only be done with administrator rights. Attempting to do either when logged on with a non-admin account brings up a Windows 7 User Account Control prompt, requiring administrator credentials to be entered. We regard this as an excellent solution.

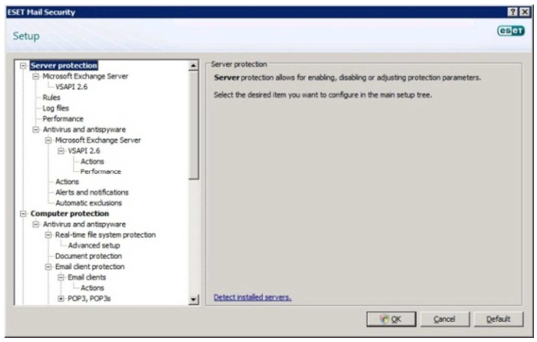
Exchange Server Protection

ESET Mail Security is a single program that combines antivirus protection for both Exchange Server and file server functions; no additional antivirus program is needed for the server running Microsoft Exchange Server. Installation is a very straightforward procedure with standard steps such as accepting the licence agreement and entering a licence key. There is a full description of the setup process in the accompanying manual, but for most administrators this will not be necessary. The program interface is essentially identical to the client software described above. When opening the window for the first time, the Help window automatically opens too, showing the section on essential post-installation configuration. This describes,

amongst other things, three means of dealing with suspected spam messages (deleting, quarantining, forwarding), and their respective advantages and disadvantages, so that the administrator can make an informed decision.



The Exchange Server options can be configured in a separate node in the Advanced Setup tree:



Although there are various options available for scanning the file system for malware, we did not find any means of scanning mailboxes specifically. ESET inform us that continuous scanning of mailboxes and attachments is carried out automatically.

Conclusion

Using ESET software to protect our small business network was very straightforward. By and large the website makes clear which product does what, although an extra word of explanation on the server products would not go amiss. The manuals are well written and clearly laid out, making it easy to find what you need to complete the installation and configuration. In general, ESET's business software is simple, well designed and easy to use, and can be recommended for large or small networks.

Deployment areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)
★★★★	★★★★½

Overview:

Installation/Deployment	★★★★½
Console	★★★★
Client Software	★★★★★
Manual	★★★★★
Overall	★★★★½

G Data

Tested Software:

G Data AntiVirus Administrator 11.0
G Data AntiVirus Client 11.0
G Data MailSecurity for Exchange 11.0

Introduction

G Data make a wide range of antivirus products for small, medium and large businesses. We tested G Data AntiVirus Enterprise, which consists of antivirus software for client PCs and servers, Exchange Server protection, and a central management console.

Software version reviewed

G Data AntiVirus Administrator 11.0
G Data AntiVirus Client 11.0
G Data MailSecurity for Exchange 11.0

Downloading the software

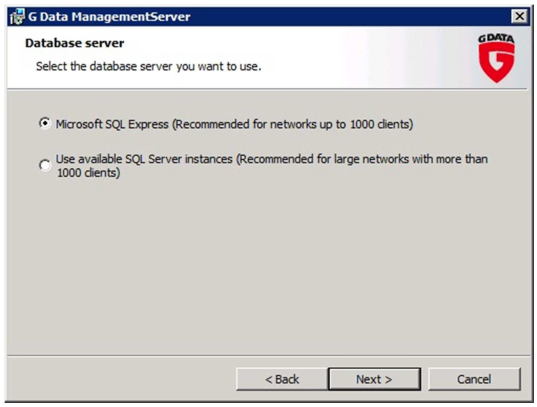
The management console and client software are available to download as a single zip file that contains all the software and documentation.
The MailSecurity program also comes as a single zip file containing the setup program.

Using the manual to prepare for installation

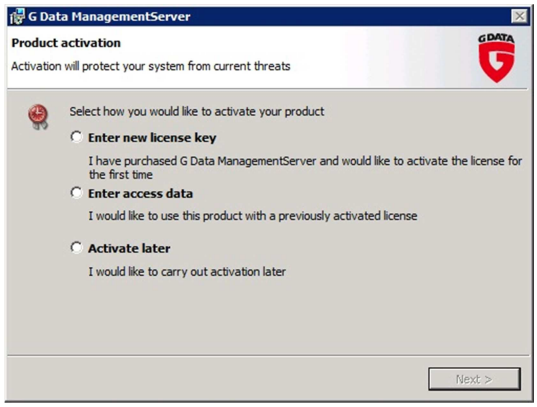
Rather confusingly, there are two versions of the manual, one entitled International (2,077 KB) and one called USA (2,078 KB). We were unable to find any difference between them, and so regard them as identical. Both are 120 pages long.
The section of the manual relating to installation is very well written, providing the right information in the right order. It gives an overview of the components to be installed, and the order in which this should be done. There is a detailed but very clear list of system requirements for all possible server and client operating systems, including Linux. There are even instructions on how to do an initial malware scan on computers using the bootable installation CD.
The manual provides detailed step-by-step instructions on installation, which make very clear what must be done at each stage. It notes that when installing the Management Server software (the functionality of the management software), the G Data Administrator (the interface) will be automatically installed too, but the Administrator can also be installed separately on any number of workstations.
There are two flaws in the manual, despite the excellence of the text. Firstly, there are no screenshots as such anywhere in the manual. In a few places, individual icons are shown, but there is not one single picture of an entire window or dialog box. The saying "A picture paints a thousand words" is never more applicable than in software manuals, and screenshots make it very easy to orientate oneself when using a manual to assist with installation. We are very surprised that G Data have not included any at all, and suggest that this is a significant omission. The second problem is bookmarking, or rather the lack of it. The table of contents at the beginning is very simple (it has a total of 10 items in it), and there is no link functionality, i.e. clicking on an item in the table does not go to that page. There are also no bookmarks, meaning that the only way to navigate through the document is using Adobe Reader's thumbnails feature. However, given the lack of screenshots, it's impossible to tell one page of text from another. In short, the only way to find anything is to keep scrolling laboriously through page by page. It happens that there is a quite comprehensive index at the back (albeit also without link functionality), but this is not mentioned at all in the table of contents, so we only found it by chance whilst scrolling through. We feel that despite being well written, the manual is poorly produced, making it very frustrating to use.

Installation of the administration software

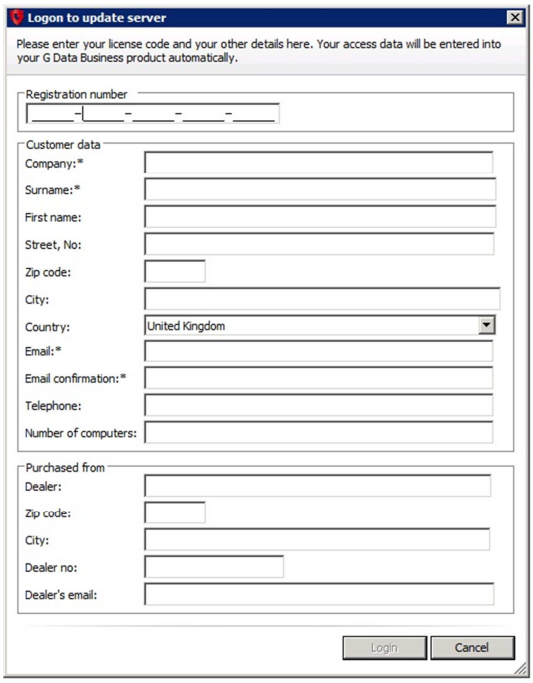
The installation wizard is started by running Setup.exe. There is the usual licence agreement to accept, the option of making the server a main, secondary or subnet server (useful for enterprises with multiple servers and sites), and a choice of using Microsoft SQL Server Express (included with the G Data package) or connecting to an existing SQL Server installation:



We chose to install the Express edition. Installation then starts; in just a few minutes it is complete, and the wizard asks us to enter a licence key:



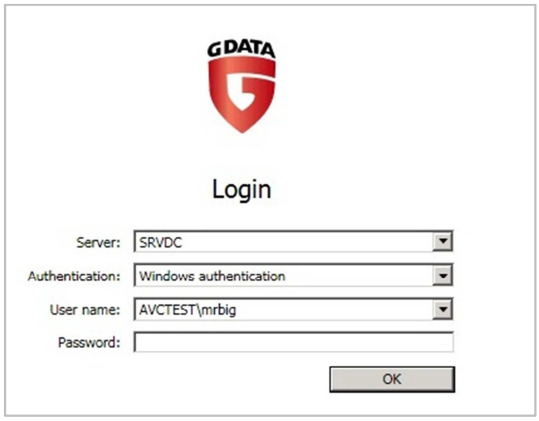
We chose to enter our (new) licence key, and were then presented with the following form:



In addition to the licence key, the required items are company, surname and email address. Other fields can be left blank. This is the end of the installation process, which is very quick and straightforward. On completion, the management console opens, and the deployment wizard starts; however, we chose to cancel it, in order to see how to start the process manually later.

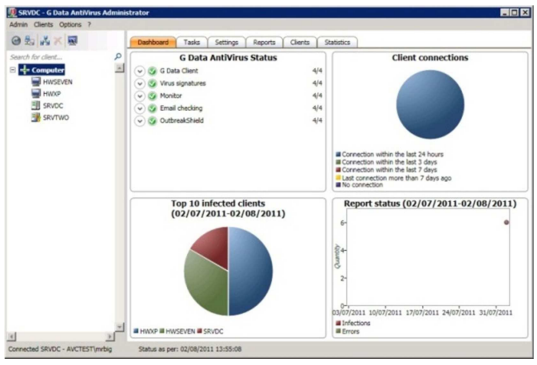
The administration console

G Data's management console is called the G Data Administrator. It is necessary to log on before using it; fortunately, Windows credentials are accepted:

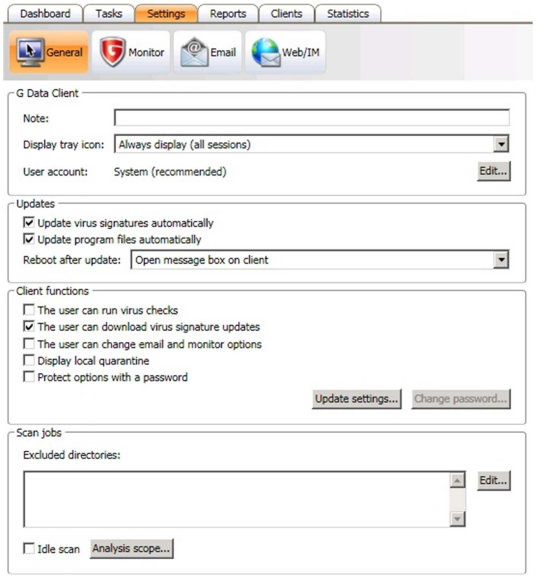


The console is not MMC-based, but has a similar layout nonetheless. A narrow left-hand

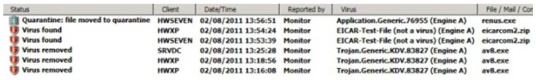
pane shows an alphabetical list of computers, which can display either all computers in the domain, or just those to which the G Data software has already been deployed.



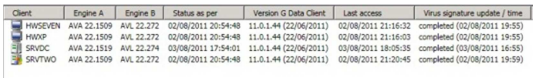
In default mode (Dashboard), the main pane of the window shows a graphical status report. This can give an overview of all computers (by clicking on Computer in the left-hand pane), or show details of any individual computer (by clicking on its name in the left-hand pane). There are four distinct panels: AntiVirus Status, which gives the status of individual components and virus signatures; Client Connections, which shows when the client PC(s) last connected to the server; Infected Clients, showing whether malware has been found on the PC(s); and Report Status, which shows infections and errors in the form of a graph. The Antivirus Status panel can be used to put right any of the problems displayed, e.g. by running an update on any clients shown as out-of-date. The Dashboard is a very effective way of showing the current status of PCs on the network, and correcting any problems found. Our one criticism of it is that the text is a little small to be read comfortably. Other functionality in the G Data Administrator is reached by clicking on the tabs along the top of the main pane: Tasks, Settings, Reports, Clients, and Statistics. Tasks can be used to run scan jobs, either one-off or scheduled. Settings contains configuration options, subdivided into General (shown below), Monitor, Email and Web/IM.



Reports shows a detailed analysis of malware found:



Clients shows a detailed status report of the antivirus status of each PC:



Statistics is subdivided into Clients, Detection Method, Virus Hit List, and Hit List Infected Clients. Clients shows a further summary of the status of client protection, while the other three tabs show detailed statistics of malware infections in graphical form.

Overall, we found the console particularly clear and simple, giving a clear overview of important information, and easy access to the most important tasks.

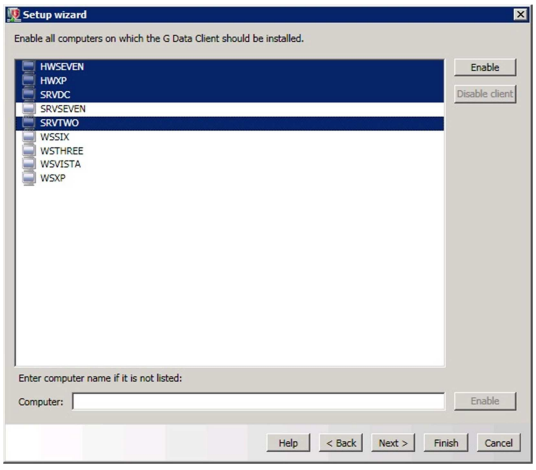
Using the manual to prepare for deployment

The lack of screenshots and bookmarks in the manual, already mentioned above, is particularly frustrating when trying to find help with deployment of the antivirus software to the clients. The instructions are buried within a section describing the different functions of the console. We only

found them by a combination of searching for relevant terms like "deployment" and "installation", and laborious scrolling. Although deployment is a simple procedure, we felt that the instructions given were just too brief, and we were confused about how to start the process; the instructions start with the words "Activating this function...", but there is no indication as to what "this function" is. Finding out would involve scrolling back through the untitled sections of the manual until a recognisable point of reference could be found. The absence of screenshots is a further drawback, as the user cannot easily relate each step of the process with the description in the manual. Preparation of clients for the installation is shown clearly as a list of necessary steps; this was the only part that we felt was adequately described. Once again we felt frustrated by the poor production of the manual, especially as it could so easily be improved, with some screenshots, titles/bookmarks, and a little re-organisation of the text (such as a separate section on client deployment).

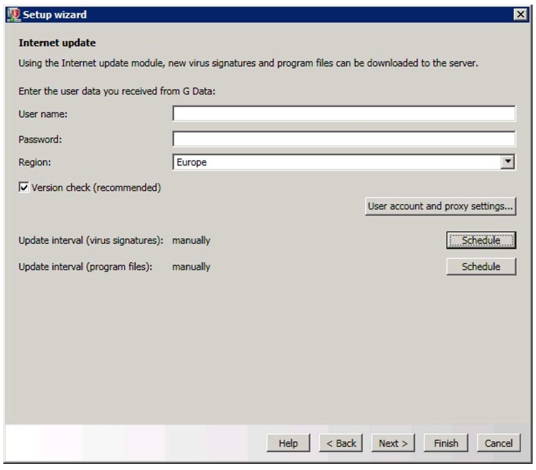
Deploying client software using push install

Fortunately, deploying the software is actually very easy without the manual. We started our search with the menus at the top of the Administrator window, and the Setup Wizard is the first item on the first menu (Admin). The first step is to select the computers for deployment. The wizard shows a list of the computers registered in our domain, regardless of whether they are running or not:



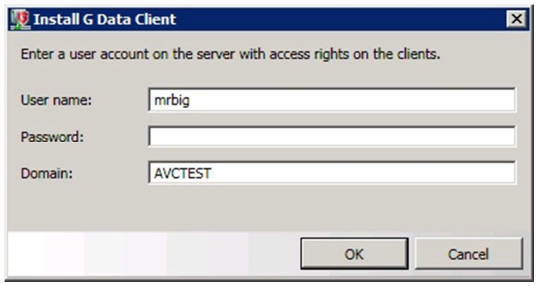
There is no means of selecting OUs at this stage, but individual computers can be selected from the list using standard windows methods, such as Ctrl + A or Ctrl + click (it is possible to create computer groups in the Administrator and assign these to Active Directory OUs, but this needs to be done before deployment; the process is very briefly described in the manual, but unfortunately the section is very difficult to find, due to the very poor indexing).

Once the selection has been made, clicking Enable marks them for installation. The next step in the wizard involves entering user credentials, proxy server information, and setting the update interval for virus signatures and program files:

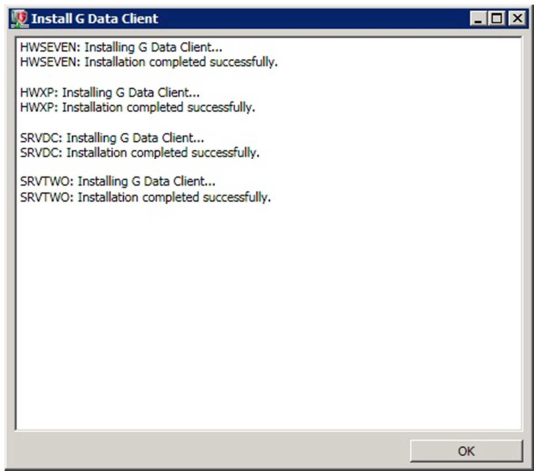


.

After this, the wizard asks for an email address for notifications, and domain admin credentials for the installation:



The wizard then begins deployment, and there is a very simple progress display:

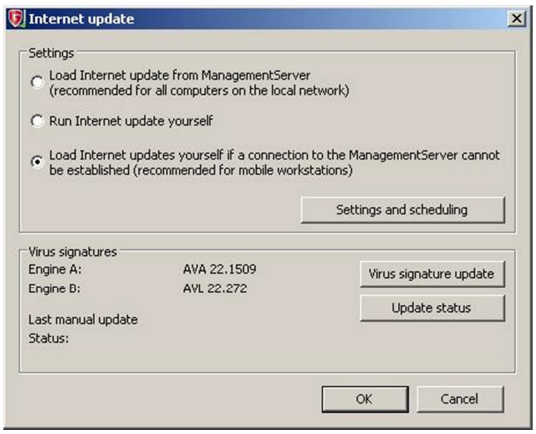


We found that the deployment completed so quickly that a more advanced real-time display would be unnecessary. We would describe the whole deployment process as being exceptionally quick, simple and trouble-free, and not bettered by any other product in our test.

Client Software

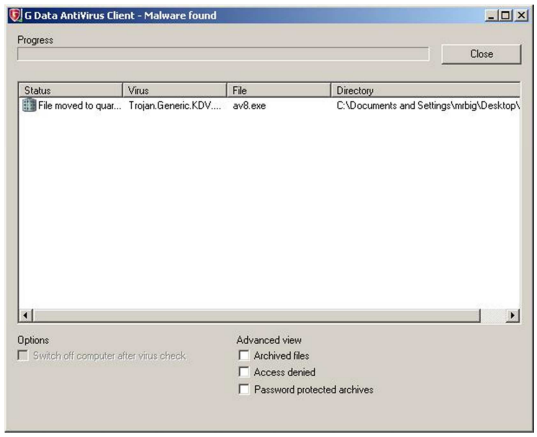
G Data is unique among the programs that we have tested, in that the client software has a minimal interface. About the only obvious sign that the software has been installed is a system tray icon. Right-clicking this produces a very short menu, the only entries being About and Internet Update:

Clicking About displays a simple message box with minimal system information; clicking Internet Update shows the following dialog box:



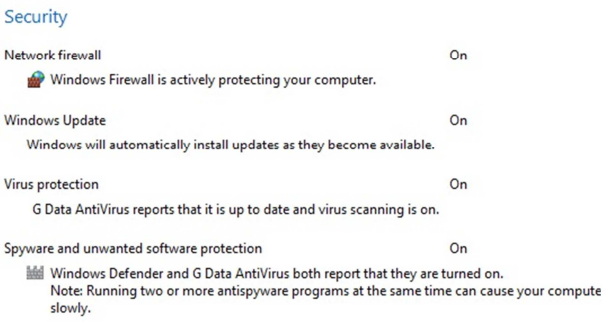
Apart from this, there is no interface or indeed any indication that the program is installed; there are no program shortcuts in the Start Menu or anywhere else, not even an entry in Add/Remove Programs. However, four G Data services can be found in the Microsoft Services console, and the same number of G Data processes can be seen in the Task Manager's process list. We did get a visible indication of G Data's presence on our workstations when we tried to download the EICAR test file. The web page was blocked, with the following warning message:

Attempting to copy a malware file over the LAN to our workstation produced the following message box:

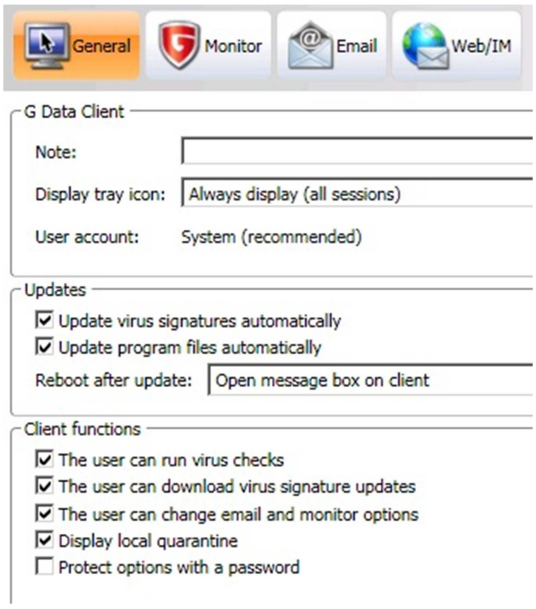


No user interaction is required, and it can be seen that the file has been moved to quarantine, although this is not exactly obvious.

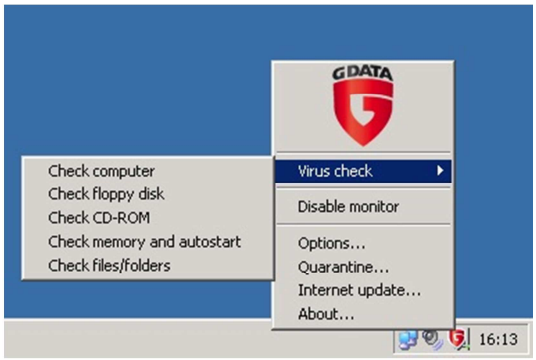
On our Windows 7 workstations, we could see that G Data had registered itself in Action Center as the antivirus and antispyware components:



The amount of user interface shown can actually be configured in the Administrator under Settings. The Monitor tab can be used to enable or disable virus notifications. The General tab can be used to hide or display the System Tray icon, and enable or disable functionality, such as allowing the user to run virus checks or switch the protection off ("change email and monitor options"):



Using these options, the System Tray shortcut menu can be extended to show the following options:



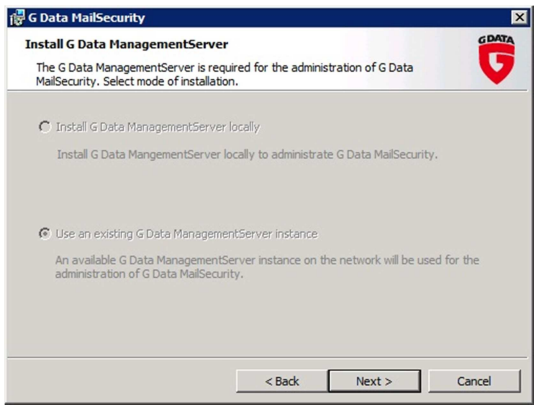
The ability to change critical client settings (such as disabling the monitor) can be password protected, meaning that its use can be limited to administrators, which is an excellent solution.

G Data's minimalist client software interface is certainly innovative and easy to configure from the console. It lets the administrator choose the functionality and visible interface available to the user.

Exchange Server Protection

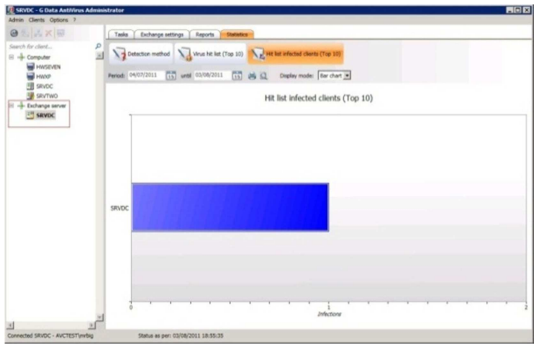
Installing G Data MailSecurity for Exchange is very quick and easy. Running setup.exe starts a very standard installation wizard, with a licence agreement to accept, and a choice of installation folder. The setup program recognised that the Management Server

software had already been installed on our server, and so greyed out the options for installing this:

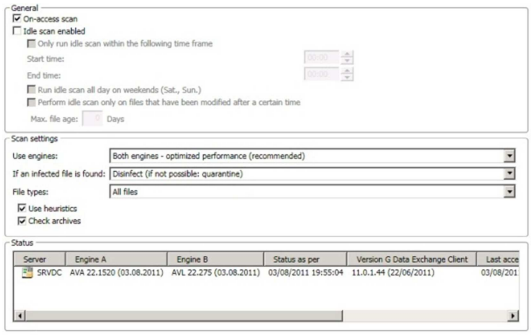


After that, the wizard asks us to confirm the server name, and then installation is complete.

MailSecurity for Exchange uses the same Administrator console as the AntiVirus software. We opened up the Administrator window to see that MailSecurity had integrated itself into the interface, in the form of a second item in the tree in the left-hand pane, called Exchange Server:



We find that sharing the console with the AntiVirus program is an excellent solution. The administrator can control both elements from one window, and the uniform interface means that finding one's way around the Exchange protection is child's play. MailSecurity also has tabs at the top of the main pane of the window: Tasks, Exchange Settings, Reports, and Statistics. Tasks allows single or scheduled scan jobs to be created, while Exchange settings provides a range of configuration options:



Reports allows detailed statistical analysis of events, and Statistics shows malware detection in graphical form. We did not find a manual for MailSecurity in the package we downloaded, although we feel that it is so simple to install and use that a manual is not essential.

Conclusion

G Data's software stands out as being extremely quick and easy to install and configure. The management console used for both AntiVirus and MailSecurity elements is very clear, simple, intuitive and consistent. We feel that the package would be particularly suitable for less experienced administrators, due to its simplicity and ease of use. Unfortunately, the manual is extremely frustrating to use, despite being essentially well written, because of its poor production. However, it could be very easily improved with some screenshots, and proper indexing and bookmarks, and we would urge G Data to do this. The minimalist client software is unique in its simplicity, and allows the administrator a high degree of control over the interface the user sees.

Deployment areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)
★★★★	★★★★½

Overview:

Installation/Deployment	★★★★★
Console	★★★★★
Client Software	★★★★½
Manual	★★★
Overall	★★★★½

Kaspersky

Tested Software:

Kaspersky Security Center 9.0
Kaspersky Endpoint Security for Windows 8.1
Kaspersky Security for Microsoft Exchange Servers 8.0

Software tested

The following versions of the software were downloaded and installed for our review:
Kaspersky Security Center 9.0
Kaspersky Endpoint Security for Windows 8.1
Kaspersky Security for Microsoft Exchange Servers 8.0

Downloading the software

Kaspersky make the setup files for the Administration Server and Endpoint Security available for download in the form of a single file. Documentation is downloaded separately as individual .PDF files. The Exchange Server software also came as a single file, with a single manual in .PDF format.

Using the manual to prepare for installation

Kaspersky provide extensive documentation for their business suite. There is the Administrator's Guide, which describes using the Security Center for daily administration tasks; the Implementation Guide, which provides detailed information on the installation procedure for all the components of Security Center; the Getting Started Guide, which contains step-by-step instructions for rapid deployment of the client software; and the Reference Guide, which is an overview of the Security Center and its features. At the time of testing, only the Administrator's Guide was available (as the product was still at the beta stage at the time). This is a comprehensive document at 108 pages. It includes an overview of the other documentation available and additional sources of help, such as the Kaspersky website and forums. The Administrator's Guide is very clearly laid out and indexed, with a comprehensive table of contents at the beginning. All the sections and subsections are bookmarked, and so can be accessed with a single click from the contents table or Adobe Reader's bookmarks pane. Although there are relatively few screenshots, those that are included are relevant and appropriately annotated. Instructions are concise and clear, using bold type for menu items and dialog buttons etc. within the application, which is very helpful.

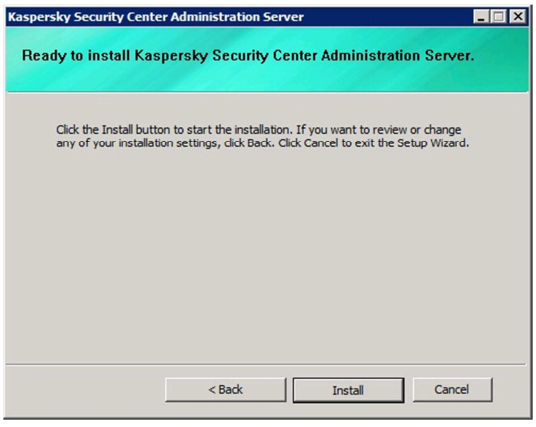
The Administrator's Guide does not actually include installation or deployment instructions; these are included in the Implementation Guide, which was not yet available at the time of testing. Consequently, we were not able to comment on Kaspersky's installation instructions for the software, although we would expect them to be of the same excellent standard found in the Administrator's Guide.

Using the manual to prepare for deployment

As mentioned above, the Implementation Guide (which contains installation and deployment instructions) was not yet available at the time this review was written.

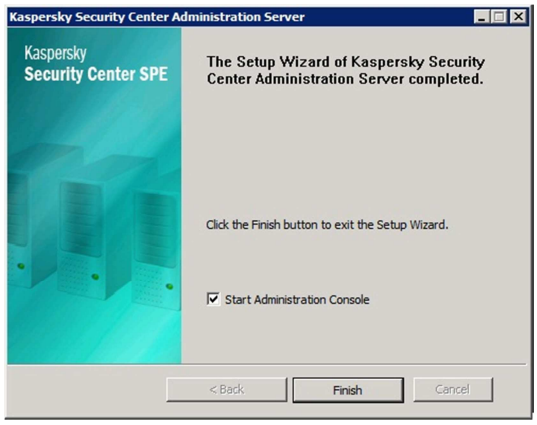
Installation of the management console

Installation was very straightforward. The setup wizard asks us to agree to the usual licence agreement, gives us a choice of Typical or Custom installation (we chose the former), and then informs us that it is ready to begin:

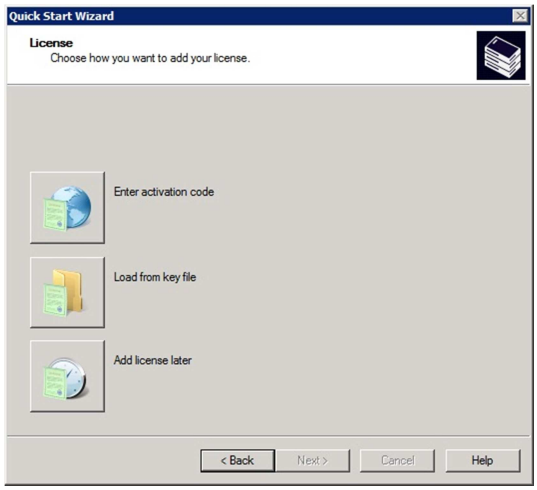


Clicking Install on this dialog box then starts the installation. There is an additional licence

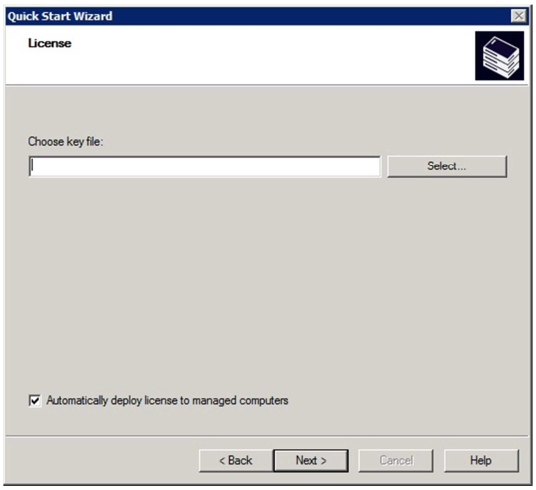
agreement, for the Windows Console Plug-in, and then setup is complete:



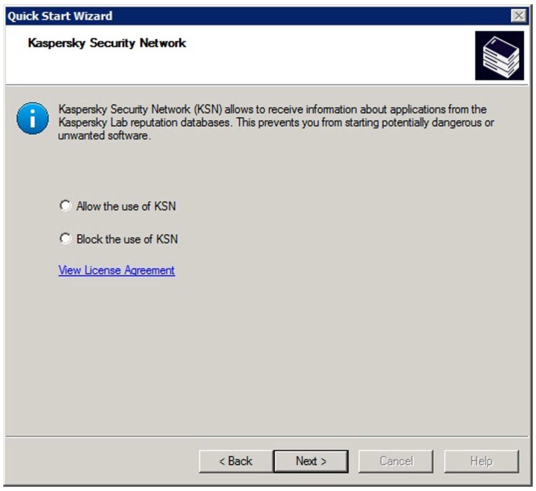
By default, the setup wizard starts the Administration Console when setup is completed, and this in turn starts the "Quick Start Wizard", for initial configuration tasks. First of all, Quick Start asks if we want to enter a licence key:



The wizard allows us to browse to the location of the key file, and to deploy the same key to managed computers on the network:



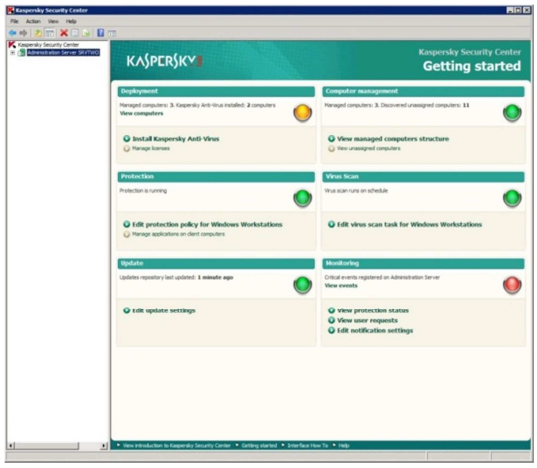
Next, the Quick Start Wizard asks about receiving reputation information from the Kaspersky Security Network:



The wizard then asks for an email address for notifications, and if a proxy server is used. On completion, Quick Start offers to show us the computers it has discovered on the network, and asks us whether we want to start deployment immediately. In order to assess the deployment options offered by the console, we declined.

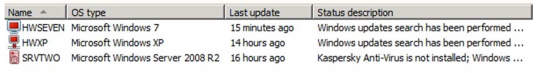
The management interface

Kaspersky's Administration Console uses the familiar Microsoft Management Console (mmc) framework. This consists of a narrow left-hand pane with various options, and a much wider right-hand pane to display the chosen option. It opens with the main page of the Administration Server selected:



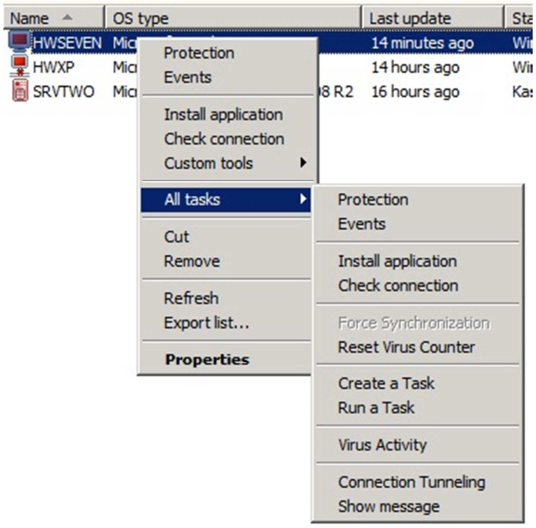
This main page is divided into 6 sections: Deployment, Computer Management, Update, Monitoring, Protection and Virus Scan. All of these have their own status displays, in the form of a "traffic light" button, showing green, amber or red for problem/warning/safe states respectively. Each section has links to relevant tasks, e.g. the Deployment section has a link entitled "Install Kaspersky Anti-Virus". This page provides a simple, at-a-glance overview of the state of the network, with easy access to any important tasks that need doing.

The left-hand pane of the window, consistent with mmc windows, contains a folder tree with more detailed options: Managed Computers, Reports and Notifications, Administration Server Tasks, Tasks for Specific Computers, Application Management, Event and Computer Selections, Unassigned Computers, and Repositories. Managed Computers shows the status of computers to which the management agent has been deployed, giving the system administrator a clear overview of the protection state of the network:

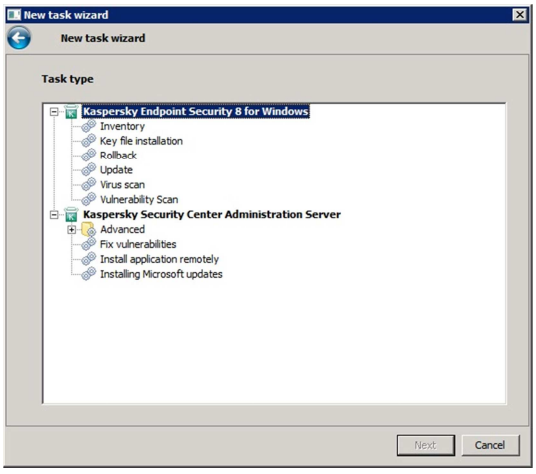


Name	OS type	Last update	Status description
HWSEVEN	Microsoft Windows 7	15 minutes ago	Windows updates search has been performed ...
HWXP	Microsoft Windows XP	14 hours ago	Windows updates search has been performed ...
SRVTWO	Microsoft Windows Server 2008 R2	16 hours ago	Kaspersky Anti-Virus is not installed; Windows ...

The screenshot below shows only a small selection of the available columns, and we have changed the order of these from the default. The Managed Computers section can be used to carry out a number of everyday tasks. Selecting multiple computers for a task follows standard Windows procedures such as Ctrl + A to select all, Ctrl + Click to select individual PCs. Right-clicking the selection then allows a number of tasks to be carried out:



"Create a Task" gives the following choice of everyday tasks, including updating and scanning:



Reports and Notifications shows the current state of the network (protection, deployment, update etc.) in the form of pie charts:

Application Management allows the administrator to define allowed and blocked programs on users' computers, using the application control feature of the client software; Event and Computer Selections gives the administrator an easy means of picking out particular ranges of client PCs or events; Unassigned Computers allows new computers to be added to existing management groups; the Repositories section enables management of e.g. installation packages, updates and licences.

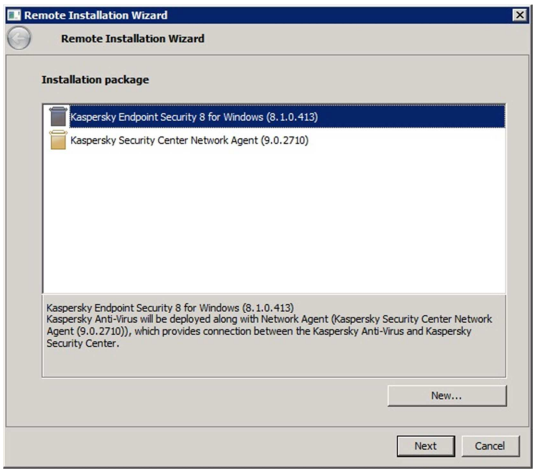
Using the manual to prepare for deployment

This is not applicable, as the manual was not available at the time of testing, due to the beta status of the software (see above).

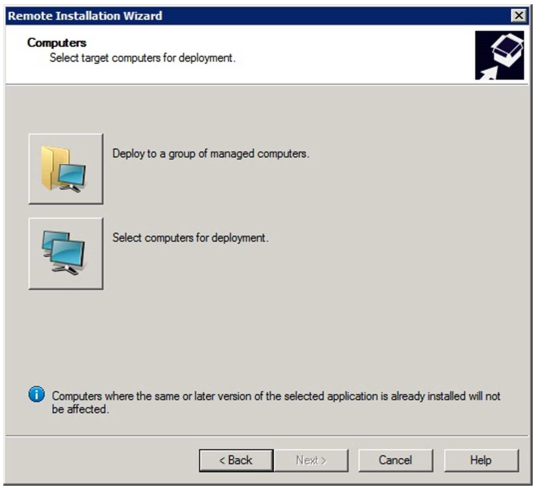
Deploying the client software using push install

As with many Windows programs, the Kaspersky Administration Console offers more than one way of achieving certain tasks. The first of the six items on the main Administration Server page is "Deployment", with a link entitled "Install Kaspersky Anti-Virus"; this is very obvious, so we used this to install the software.

The first step in the deployment wizard is to choose the package to be installed. There is a choice of Kaspersky Endpoint Security for Windows and the Kaspersky Security Center Network Agent:

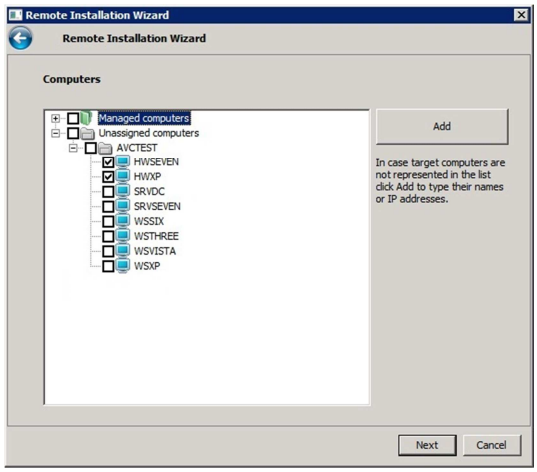


Installing the Endpoint Security program also installs the Network Agent, enabling remote administration via the console. We selected Kaspersky Endpoint Security for Windows. The next step is to select the computers to be installed. There is a choice of groups of already-managed computers (which might be useful if installing a new version of the software to PCs which already have the Network Agent), and selecting computers for deployment:

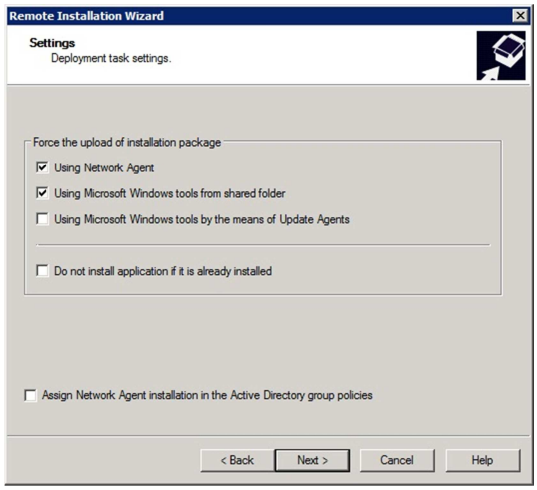


As none of our client PCs had the Network Agent installed, we chose the second option. This produces a list of domains/workgroups on the local network, and allows the administrator to select individual PCs from these. There is no means of selecting OU groups from Active Directory, however. We note that the wizard lists all client PCs in the

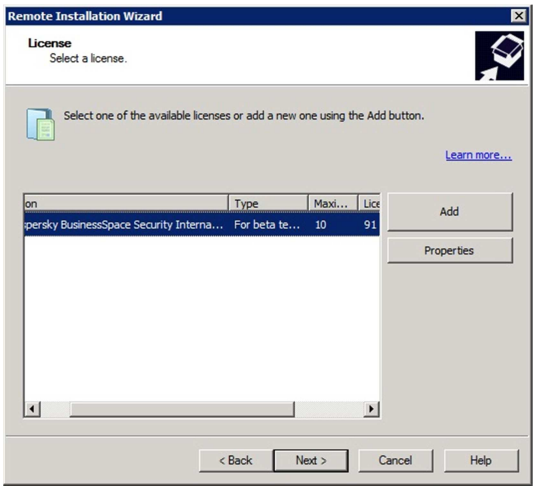
domain, regardless of whether these computers are actually running or not.



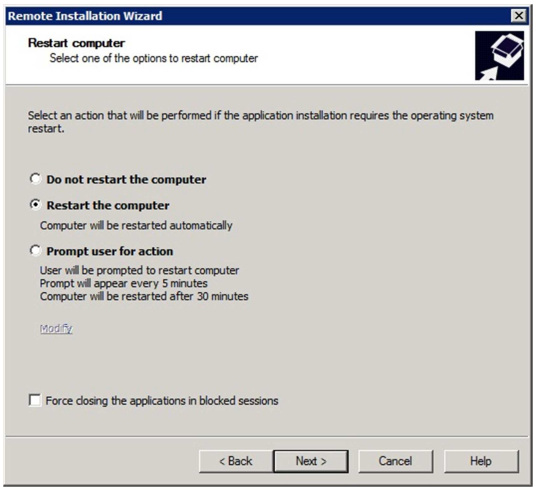
We selected the relevant client computers from the list. The wizard then provides some installation options, including the obviously sensible "Do not install application if it is already installed". We left these with their default settings:



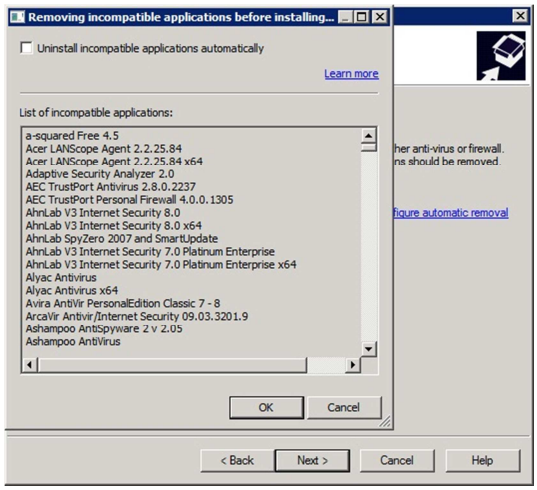
The wizard then asks for a licence to be selected. As we had earlier selected the option "Deploy licence to managed computers" during console installation, the same licence was pre-selected by the deployment wizard:



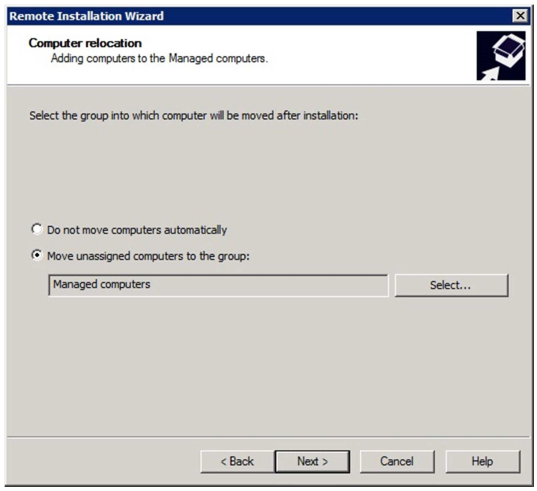
After this, the wizard asks what action should be taken on client computers if a restart is needed; we opted for "Restart the computer".



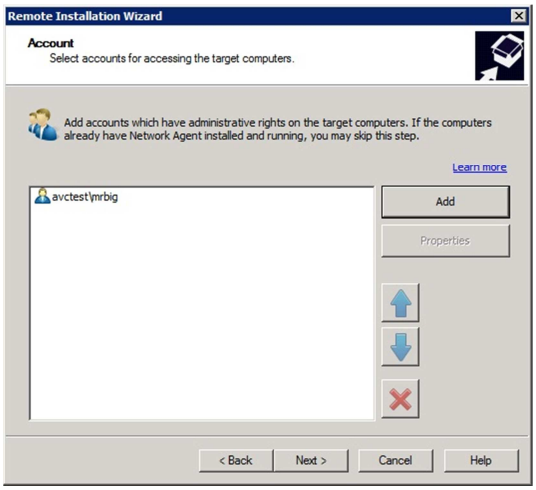
In the next step, Kaspersky's deployment wizard informs us that existing antivirus and firewall software must be removed before deployment, and provides a list of applications which can be removed automatically, along with the option to do this:



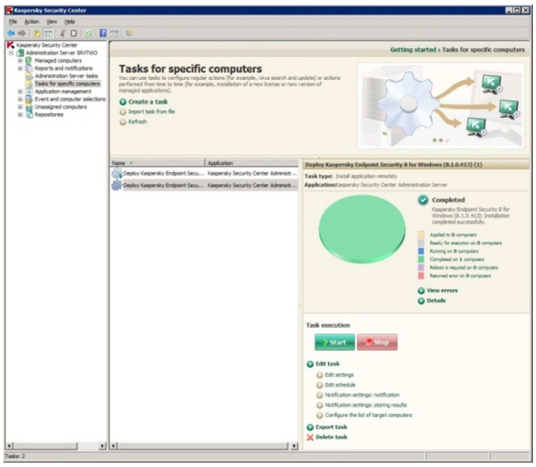
As there was no pre-existing AV software on our test clients, we moved on to the next step, which gives the option of moving the installed PCs to the "Managed Computers" group in the console:



We chose to accept this option, to make administration easier. Next we need to choose an account with admin rights to use for the installation, and then deployment begins.



The final page of the wizard invites us to click "Next" to show details of the deployment, which takes us back to the main console, with a clear, coloured diagram showing deployment status:



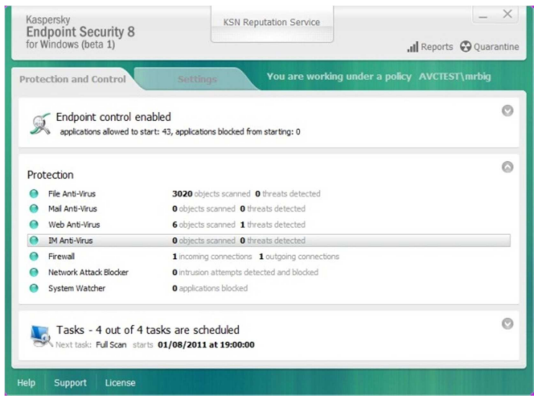
This shows the total progress in the form of a pie chart with the percentage of computers in particular states, and a clear legend of the colours used adjacent. This can be seen in more detail below:

This real-time display of deployment progress is one of the very best we have seen in corporate antivirus products.

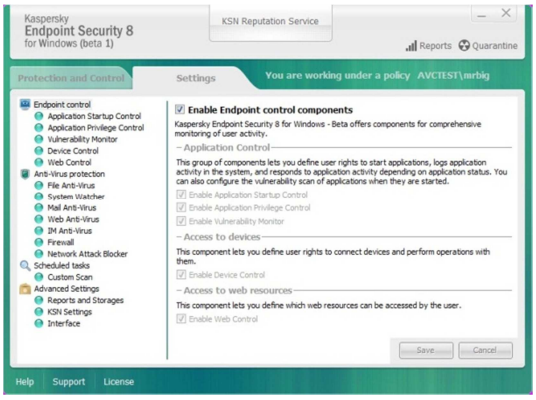
Client antivirus software

From the Action Center in our Windows 7 client, we can see that Kaspersky Endpoint Security 8 for Windows registers itself as an antivirus and antispyware application, and firewall:

The software has a System Tray icon, familiar to users of Kaspersky's home products. Double-clicking this opens the main program window:

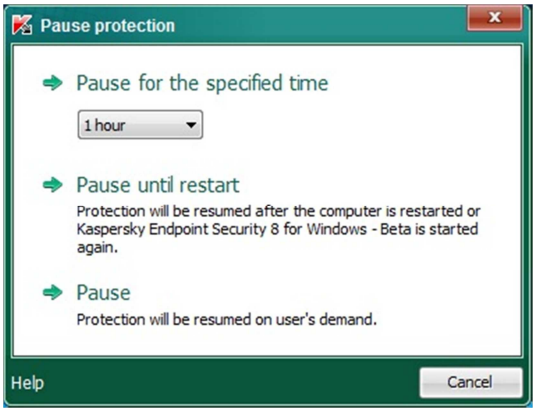


The program interface is something of a departure from standard antivirus programs. The window is divided into 3 main horizontal stripes, entitled Endpoint Control, Protection, and Tasks. Protection shows the status of the more traditional components of security suites, such as antivirus and firewall. Endpoint Control shows applications, devices and web pages that have been allowed or blocked. Tasks shows scheduled scans and updates. Two tabs at the top of the window allow switching the main pane between the normal status display described above, and Settings:



The new interface for Kaspersky Endpoint Security shows the status of every single component of the suite, and is quite logical once you get used to it. It is rather more complicated than traditional antivirus interfaces, though Kaspersky tell us that it is designed to be used by system administrators rather than standard users.

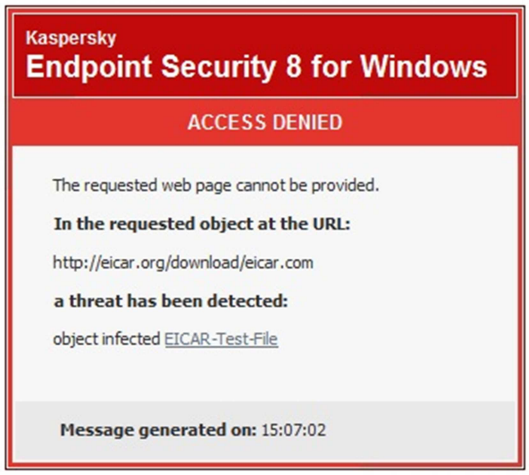
Right-clicking the System Tray icon produces a shortcut menu, which includes the entry Pause Protection. Clicking on this brings up the following dialog box:



This would allow the administrator to temporarily disable the protection, e.g. to install a program. This feature is available regardless of whether the logged-on user has administrative privileges or not, but can be password protected to prevent unauthorised use..

When we attempted to download the EICAR test file, the web page and download were

blocked, and the following message was shown:



We feel that many non-expert PC users, on seeing this message, might worry that the threat has been detected but not stopped, and call technical support for assistance. We would suggest that it would be better if the warning were to say "a threat has been detected and deleted" or "a threat has been blocked".

Exchange Server protection

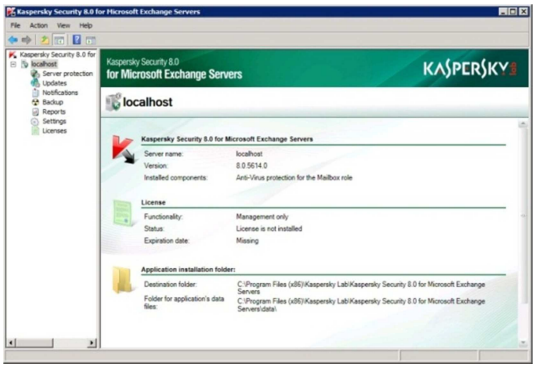
Kaspersky Security 8.0 for Microsoft Exchange Servers provides protection only for the Exchange Server component of the server; Kaspersky Antivirus for Windows Servers must be installed additionally to cover file server protection.

Double-clicking the installation file for Kaspersky Security for Exchange produces a window showing the required components and their installation status:

In our case, we see that we already have the required .NET Framework, Windows Installer and Microsoft Management Console, but that we will need to install Microsoft SQL Server 2008 Express Edition. Very conveniently, there is a link built in to the notification line, which takes us to the Microsoft download page for the SQL Server Express 2008. It is then a very simple task to download the installation file for this software. There is also a link to the manual available from the same window.

The manual notes that a local instance of SQL Server must be used for the Kaspersky Security database; care must be taken to configure this correctly during the SQL Server Express installation, otherwise Kaspersky Security setup will fail.

When Kaspersky Security 8.0 for Microsoft Exchange Servers has been successfully installed, the console can be opened. This is also based on Microsoft's MMC, and has a very simple tree of options in the left-hand pane:



Clicking on "localhost" produces a brief overview of the local server, as shown in the screenshot above. Server Protection provides settings for scans, exclusions, and mailbox protection; Updates allows the administrator to choose the source and frequency of updates; Notifications notifies the admin about infected, corrupted and protected objects, and system errors; Backup (rather confusingly named) is a quarantine area, where suspicious items are sent; Reports allows the admin to extract specific information from the logs; Settings allows

notification, diagnostics and storage configurations to be changed; Licences shows existing licences and allows new ones to be added. The console is very simple and clear, making it easy to find the required function quickly and easily.

Conclusion

Kaspersky Security Center 9.0 retains all the strengths of the previous version, i.e. easy navigation through the Microsoft Management Console Interface, quick access to important features, and excellent real-time reporting on deployment. The design of the client software, Kaspersky Endpoint Security 8.0, is innovative and rational, though it is aimed at administrators rather than end users. Manuals for the new software have not yet been produced, and so we are unable to comment on them. Kaspersky Security 8.0 for Microsoft Exchange Servers is straightforward to install, and has a very simple, clear console, making it easy to use.

Deployment areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)
★★★★	★★★★½

Overview:

Installation/Deployment	★★★★½
Console	★★★★½
Client Software	★★★★½
Manual	★★★★
Overall	★★★★½

McAfee

Tested Software:

McAfee SaaS Endpoint Protection 5.2.0
McAfee Security Service for Exchange 7.0

Introduction

McAfee make a wide range of business security products for large and small networks. We tested their SaaS (Software as a Service) Total Protection Suite, which is designed for small and medium businesses. It includes SaaS Endpoint Protection (antivirus for client PCs and file servers) and Security Service for Exchange (Exchange server protection).

Software version reviewed

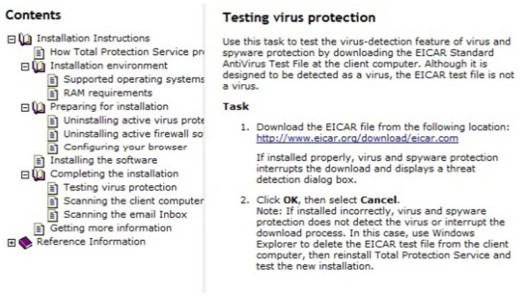
McAfee SaaS Endpoint Protection 5.2.0
McAfee Security Service for Exchange 7.0

Installation methods

There are two methods of installing McAfee SaaS Endpoint Protection: locally on individual PCs, by clicking on a link in a web page or email, or remotely, by pushing the software out centrally. This may not be clear to anyone signing up for the trial version of the software, however, as we found out when we did this ourselves. The email which arrived after registration contained a section entitled "INSTALLING ENDPOINT PROTECTION ON ONE OR MORE COMPUTERS" (capitals are McAfee's), which described installing the software by clicking on the hyperlink from every machine that needs to be installed. There was a hyperlink in this section to "detailed installation instructions", which led to a more comprehensive description of the same process on McAfee's website. Nowhere in the mail was there any suggestion that a centralised push installation is possible, or any other link to installation documentation. We would urge McAfee to review the email they send out to trial users, as the one we received effectively hid a major component of the suite's functionality. As we were initially misled into thinking that the local installation via hyperlink was the only means of deploying the software, we used this method to install two of our test computers. It was extremely simple, and ideal for small businesses with only a few computers, so we have described it here, as well as the push installation process.

Using the online instructions to prepare for local installation

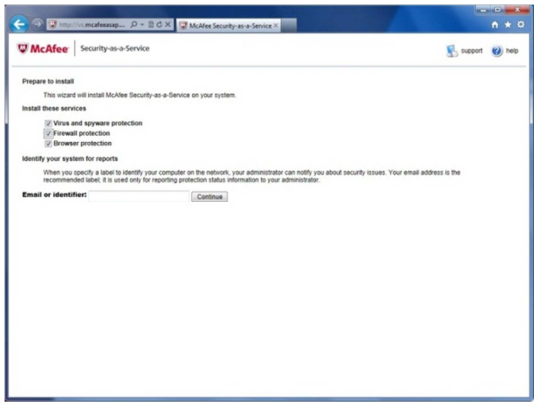
As mentioned above, the email from McAfee with the installation hyperlink also includes a link to installation instructions. This opens the program's online help function. The instructions given are very concise, and there are no screenshots, but everything is explained adequately; as we shall see, the installation process is very simple. The help service covers system requirements, uninstalling existing antivirus software, installing the McAfee SaaS software, and even testing it using the EICAR test file:



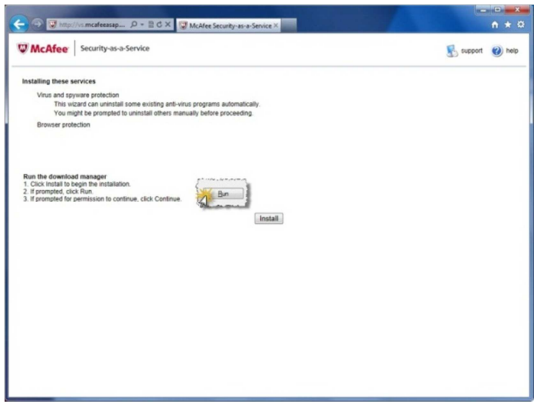
In summary, the online help is very clear and simple, and entirely suitable for the straightforward installation process it describes.

Installing the software locally

Local installation of McAfee SaaS Endpoint Protection is started by clicking on a link in an email. This opens up a webpage which allows a simple choice of protection components to be selected, namely Virus and Spyware, Firewall, and Browser. There is also the opportunity to enter an email address for security notifications:

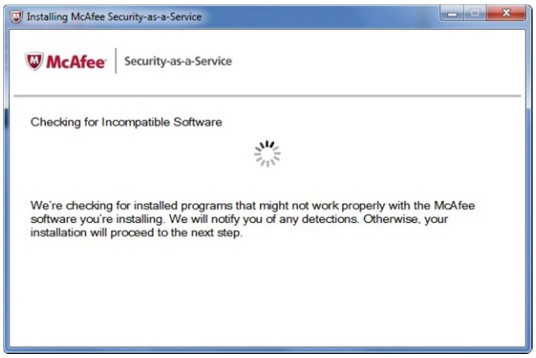


The next page has a message about pre-existing antivirus software, noting that some can be uninstalled automatically, but other programs may have to be removed manually. There is a single button to click to start the installation:

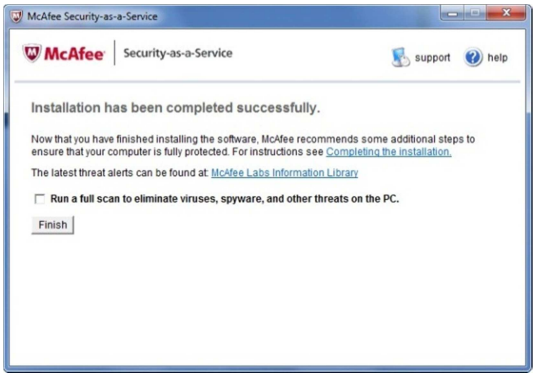


Next comes a final notice in the web browser, indicating that pop-up blockers may need to be deactivated:

After this, a McAfee SaaS information window pops up, informing us of the state of the installation. There are no decisions to be made or buttons to click as part of the installation:



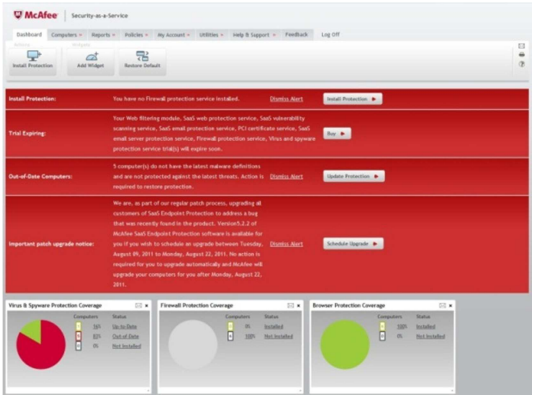
After just a couple of minutes, the information window informs us that installation has finished:



Clicking on the "Completing the installation" link opens the program's help file. A full malware scan can be run by ticking the box before clicking Finish.

The web console

The administration console for McAfee SaaS Endpoint Protection is web-based (i.e. accessed via a browser), or to be more specific, it is Internet based, i.e. it runs on McAfee's Internet servers, not on a local server. Login details are provided by McAfee when purchasing the software or signing up for the trial. The opening page (Dashboard) displays important alerts, for things such as out-of-date protection, on an unmissable red background:



Below the alerts are no less than 14 boxes containing individual status reports for every conceivable aspect of the software (the screenshot above is cut off at the bottom for reasons of space). Sensibly, Virus & Spyware Protection Coverage and other protection items are found at the top. Fortunately it is possible to close any of the boxes deemed unnecessary, or drag them to a different position. The Restore Default button on the toolbar at the top brings them back if necessary, while Add Widget can be used to add or restore individual status boxes.

Tabs at the top of the page include Computers; Reports; Policies; My Account; Utilities; Help and Support. Each of these has its own menu for detailed aspects of the relevant area. The Reports menu has 14 items on it; there is certainly no lack of detail available.

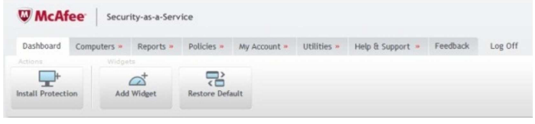
The console arguably makes the most important items (alerts, important status items, and the Install Protection button used to deploy software) easily accessible. Unfortunately, we cannot help but feel that the number of different items displayed on the dashboard makes it rather overwhelming. Only when we had dismissed some of the alerts and closed some of the status boxes did we feel that we had some sort of overview. Regarding the numerous status boxes, and the multiple menu items associated with each of the tabs at the top, we feel that McAfee might have overdone the idea of many items each showing a little bit of information, and that perhaps a smaller number of items each showing somewhat more information might not be better. Given the neat and standard layout of the Exchange console, and especially the extraordinarily clear, simple and efficient design used for the client software and deployment wizard, we wondered whether McAfee might be able to make the design of the web console a little less daunting.

Using the manual to prepare for deployment using push installation

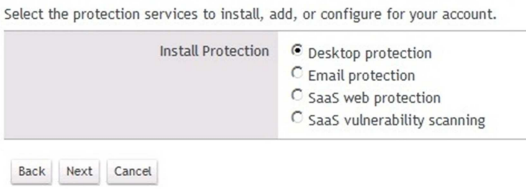
There are two PDF documents available from the Help menu in the online console, the Product Guide and Installation Guide, the latter obviously being relevant here. The Installation Guide is 41 pages long; given that it only covers installation, this actually makes it very comprehensive. It is also very easy to navigate. There is an extensive table of contents at the beginning, with links to bookmarks in the document, so that clicking on an item in the table goes straight to that page. The bookmarks feature in Adobe Reader can also be used to find relevant headings and go straight to that section. Finding the section on push installation was thus very easy. The instructions are concise, clear, and cover all necessary aspects, including system requirements and preparation for the client computers to be installed, and the administrative computer/server used to run the push install process. There are no screenshots anywhere in the manual, although we find the push installation to be so simple that this scarcely matters.

Deploying the software using push installation

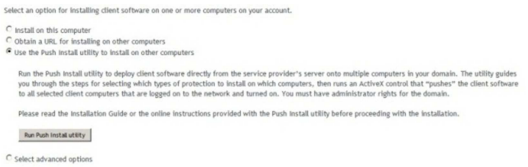
To use the push installer, the administrator logs on to the online console. Downloading the utility is started by clicking on the Install Protection button at the top of the page:



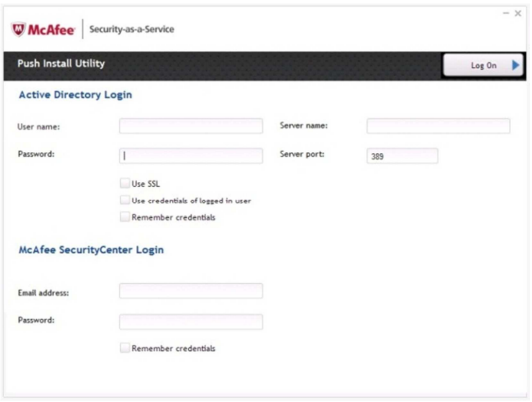
Next, select Desktop Protection:



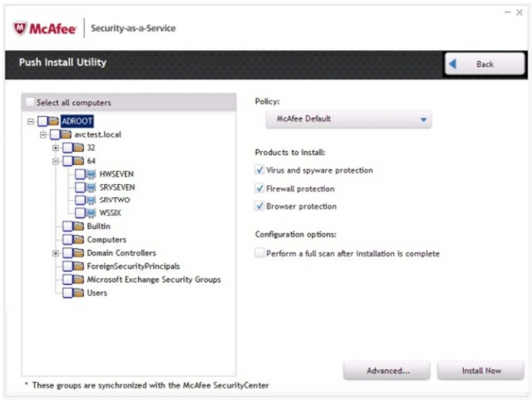
Then select the Push Utility option, and click on Run Push Utility:



The installation file for the push utility can then simply be run on the local computer, or saved to be run later or on a different computer (we chose the latter). We executed the push utility on our server, and were prompted to enter credentials for our McAfee Security Center and Active Directory (it appears that both are necessary):

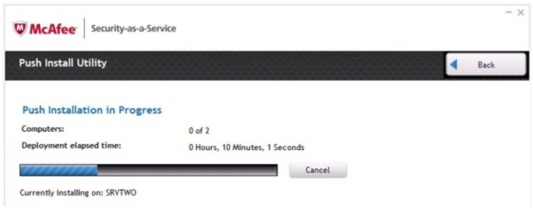


After logging in, we were able to choose computers to install from an Active Directory tree:



We note that it is possible to select anything from the entire AD forest to an individual computer, including OUs, with a couple of clicks. The same page of the wizard enables individual protection components (e.g. firewall) to be selected or deselected for installation, and the Advanced button allows these options to be configured individually for specific computers. There is also the option to scan computers for malware after installation. Having selected the required computers and options, the administrator can start deployment by clicking on Install Now. We would suggest that McAfee's deployment wizard is outstanding, offering all the essential deployment options in a single, unbeatably simple and clear dialog box, ideal for large or small networks, and should serve as a model for other manufacturers to copy.

Once deployment has started, the wizard displays a simple but useful progress bar:



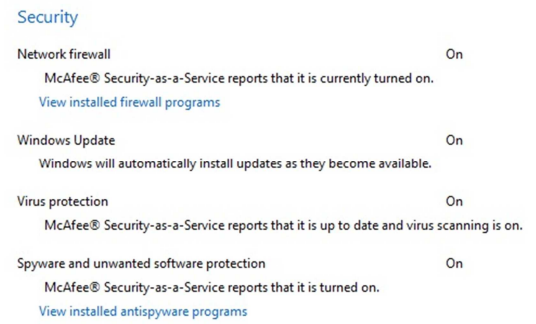
We noticed that the first phase of deployment is downloading the client software from the Internet, which took several minutes, but once this had been done, the actual installation process is very quick (approximately 2 minutes).

After the deployment, we found that Remote Desktop connections to the clients PCs had

been blocked, and it was necessary to log on locally and set the network connection type to Trusted to re-enable the RDP access. We feel it would be helpful if the deployment section of the manual explained that this will happen, and how to re-enable Remote Desktop access using policies that can be applied either locally or via the Administrative Web Console.

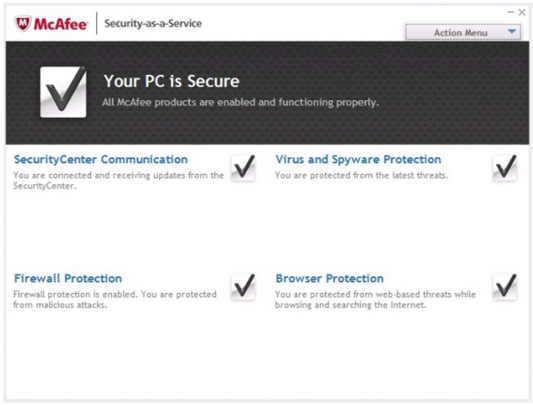
Client Software

McAfee SaaS Endpoint registers itself in Windows 7 Action Center as the firewall, antivirus and antispyware applications:

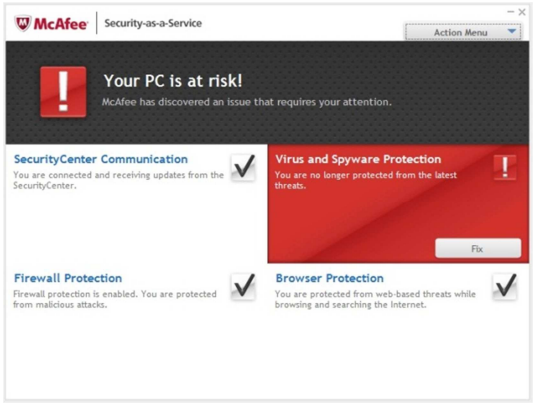


There is a System Tray icon, similar to the ones found in McAfee consumer products. Right-clicking it produces a very simple shortcut menu:

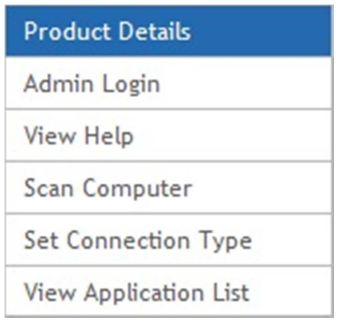
Clicking Open Console (or double-clicking the tray icon) brings up the main program window:



The program interface is extremely simple. The window is essentially one large status display, with a black horizontal strip at the top showing the overall security state, and four headings in the lower part of the window, showing the components of the software: Security Center Communication, Virus and Spyware Protection, Firewall Protection, and Browser Protection. Each shows a tick (checkmark) symbol when the component is functioning normally. In the event of a risk, the affected component appears in red, with a big button marked Fix. The example below shows the program when the antivirus component has been disabled:



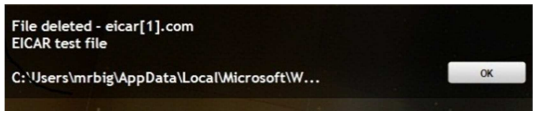
There is normally only one control feature in the entire window, the Action Menu button in the top right-hand corner. Clicking on this produces the following menu:



Product Details gives an overview of the components, and allows both malware protection and the firewall to be turned on or off, if the user has administrator privileges (the feature is sensibly disabled for standard users). Set Connection Type allows the firewall to be set for trusted or untrusted networks, or custom (e.g. opening specific ports). The Application List enables applications to be allowed or blocked. Scan Computer gives a choice of full or custom scans, although there is no means of scheduling a scan (this can be done quite easily from the console, however). It is not possible to run an update from the program window, but the shortcut menu produced by right-clicking the System Tray icon does allow this.

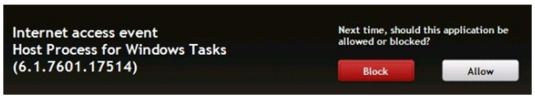
The very simple design of the program means that users are presented with the cleanest of interfaces, but an administrator can easily find necessary functions from the simple menu.

When we attempted to download the EICAR test virus, a huge McAfee message box, covering the lower quarter of the screen, appeared:



The message clearly states that the "virus" has been deleted; no user action is required or possible, other than clicking OK to close the message box.

We were a little concerned to see, somewhat later, a similar dialog box, asking whether Internet access should be allowed for the "Host process for Windows tasks":



This is not a question that a standard user could be expected to answer, and apart from the Windows version number, there is no further information to help an administrator decide (even if this particular process is recognisable). Many standard users would be tempted to click Block, which would of course deny Internet access to an essential Windows component. We feel this is out of keeping with the otherwise extremely simple and user-friendly interface. If we were using the software ourselves, we would be tempted to deselect the McAfee firewall in the installation process, and use Windows Firewall instead.

There was one other small cause for concern with the client software. We were unable to find any means of adding exceptions to the scan, i.e. there seems to be no means of whitelisting specific files or folders in a full system scan. This may be present some problems e.g. for IT professionals who legitimately use some tools such as keyloggers that could be regarded as "potentially unwanted".

Exchange Server Protection

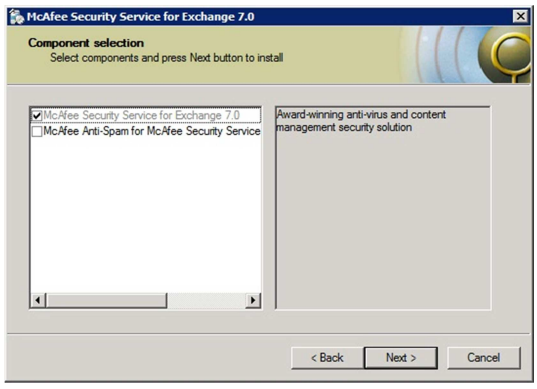
McAfee SaaS Total Protection includes two possible means of email protection. One is entirely cloud-based, and involves redirecting the MX records for the user's domain to McAfee's servers, where mail is scanned for malware and spam before being sent on to the customer's own local mail server or hosted Exchange service. The second method is a more traditional program to be installed on the local Microsoft Exchange server. Logging on to the Internet console and selecting Install Email Protection leads to a page with links to instructions for both methods; we were a little confused by this, as it was not clear whether we needed to configure both services, or only one, and in this case which one would be appropriate. McAfee inform us

that most companies use one or the other, although they could be used together; the cloud-based service minimises wasted incoming traffic in the form of spam, while the local server-based solution has the advantage of checking internal mail. For companies using a hosted Exchange service rather than their own local Exchange server, only the cloud option is possible. We would suggest that putting this simple explanation of the two methods on the relevant page of the Internet console would be very helpful.

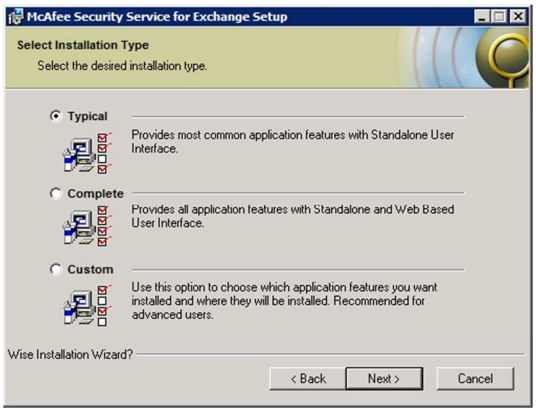
We did not test the cloud-based service, but noted that the instructions for configuring the MX records, and smart host or relay for outbound message filtering, appear clear and comprehensive.

The manual for McAfee Security Service for Exchange is very extensive, at 108 pages. However, it is very well indexed, with clear section headings, making it very easy to find the right section very quickly. The setup guide is comprehensive, and includes abundant screenshots. There are detailed step-by-step instructions on how to test the installation when it is up and running, as well as everyday maintenance tasks.

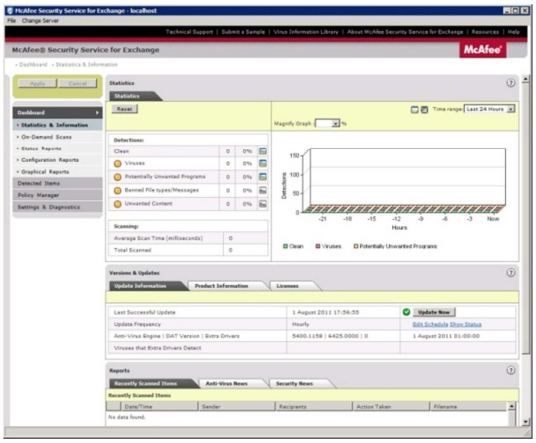
Installing McAfee Security Service for Exchange on a local Exchange server is a very straightforward process. Double-clicking the setup file starts an installation wizard, which has the usual licence agreement, and asks for a key to be entered. There is a choice of installation folder location, and the option of installing McAfee's antispam service (which we declined):



There is then a choice of setup types, Typical, Complete or Custom (we chose Typical):



Setup is then completed very quickly, and we can look at the Exchange protection console. This does not use the MMC console, but is laid out in a similar fashion, with a narrow left-hand panel containing menu items, and a much larger right-hand pane displaying the details:



Our initial impression of the console was that the text is very small. Administrators over a certain age may need to put on their reading glasses or adjust the DPI settings of the Windows fonts. The fact that nearly the entire interface is one shade or another of grey unfortunately exacerbates the legibility problem; slightly darker grey text on a slightly lighter grey background does not make for ease of reading. Using some colour for the title surrounds would also make the items stand out more. Having resolved the magnification problem, we can see that the

opening page of the console displays some useful information. There is a statistics section, showing the number of viruses, potentially unwanted programs (PUPs), banned files and items of unwanted content that have been detected. This information is shown in table form and as a graph, which unfortunately is also rather small. There is a section called Versions & Updates, which shows details of virus signatures, product information and licences (using tabs to switch between items). Finally, a section marked Reports shows Recently Scanned Items, Anti-Virus News, and Security News. Other sub-menus of the Dashboard section include On-Demand Scan, Status Reports, Configuration Reports and Graphical Reports. The remaining top-level menu items in the left-hand panel are Detected Items (with submenus for specific types, such as viruses and PUPs); Policy Manager, with numerous submenus for different types of scan); Settings and Diagnostics (again with numerous sub-menus). To sum up, the console has a wealth of reporting and configuration options, but a very simple and clear means of accessing them via the panel of menus and expanding submenus in the left-hand column.

Conclusion

Local installation of McAfee's SaaS Endpoint Protection make it an ideal choice for very small companies with no dedicated IT support staff, as it is no more complicated to install and use than, say, Skype or iTunes. Installation instructions are simple but perfectly adequate. For larger networks, the push installer is a model of quick and easy deployment, the manual being excellent but virtually unnecessary. The client software interface is almost revolutionary in its simplicity, but still gives administrators easy access to essential functions. One minor concern is the "chatty" firewall, although Windows Firewall could easily be selected instead.

The Security Service for Exchange console is very straightforward to install and use, with a simple interface giving access to a wide range of options and features. We would however urge McAfee to improve legibility by using larger and clearer text. The manual is clear, comprehensive and well indexed. We feel that McAfee would help (potential) customers understand its products much better if they included a little extra information in the emails they send to trial users (and possibly paying customers) and on the page of the web console relating to email protection. We would also suggest that the web console could do with a somewhat simpler design.

Deployment areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)
★★★★½	★★★★½

Overview:

Installation/Deployment	★★★★★
Console	★★★★
Client Software	★★★★★
Manual	★★★★
Overall	★★★★½

Symantec

Tested Software:

Symantec Endpoint Protection Manager 12.1
Symantec Endpoint Protection 12.1
Symantec Mail Security for Microsoft Exchange 6.5

Introduction

Symantec produce a range of security software for business, called Symantec Endpoint Protection. There are three variants: the Small Business Edition, for up to 100 users; the Cloud edition, for up to 250 users; and the enterprise edition, suitable for hundreds or thousands of users. Symantec Mail Security for Microsoft Exchange is a separate product for Exchange Server protection.

Software version reviewed

Symantec Endpoint Protection Manager 12.1
Symantec Endpoint Protection 12.1
Symantec Mail Security for Microsoft Exchange 6.5

Downloading the software

This is extremely straightforward, as the entire Endpoint Protection package comes in the form of one zip file containing all the software and documentation.

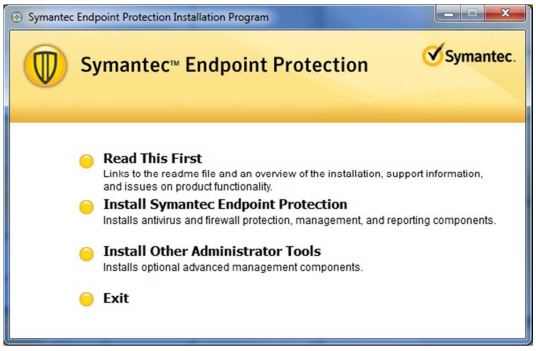
The Mail Protection is a separate item, but again in the form of a single file with both program and manuals enclosed.

Using the manual to prepare for installation

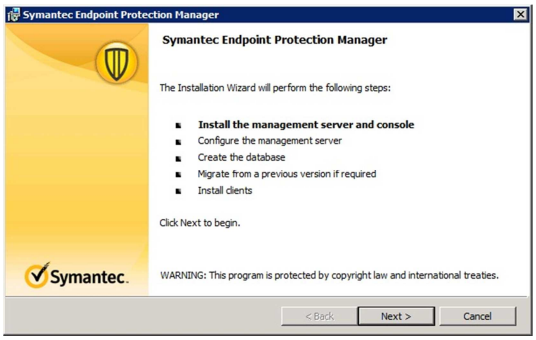
The Symantec Endpoint Protection package includes 4 manuals in PDF form, of which two appeared to be relevant to our installation task. Getting Started is a very brief 28-page overview of the software, system requirements and installation procedure. In practice, we would say that it is too simplified to be used on its own. The Implementation Guide is a much more comprehensive manual with over 1,000 pages. It is very well structured with a highly detailed table of contents, providing an overview of the different sections and subsections. Inevitably, its sheer size means that finding the relevant section can sometimes take a while. For a small business installation, only a relatively small subset of the total information will be relevant, but this has to be found amongst the many non-relevant sections. We also noted that there are no screenshots at all in the Implementation Guide, which we consider to be a pity. Symantec tell us that they make a small business version of the manual, at 351 pages, although this was not included in the package we were sent for testing.

Installation of the administration software

Installing the Symantec Endpoint Protection Manager on the server is a straightforward process. Double-clicking Setup.exe brings up a list of options, including installation:



Clicking Install Symantec Endpoint Protection starts the installation wizard. The first page of this shows the steps involved:



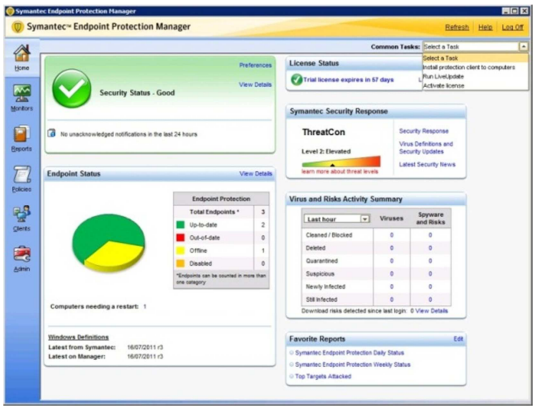
There is a choice of default or custom installation. The default is shown as being suitable for networks with less than 100 clients, and uses the built-in database, while custom should be used for systems with more than 100 clients, and allows the configuration to be customised:

We opted for the default installation for our small business network, and this was very quick and easy. The steps are: entering administrator credentials to be used to access the console, along with an email address for alerts; the server name/IP address; and deciding whether to submit anonymous system data, including detected threats, to Symantec for analysis. After installation, we noted that there was a new folder entitled Symantec Endpoint Protection Manager in the All Programs section of the Start Menu, from which the console can be started.

The administration console

The manual notes that there are two ways of accessing the console: locally from the machine on which it is installed, as described above, or remotely, using a web browser and typing in the server's IP address (or hostname) and port number. Both methods provide exactly the same functionality; we have used screenshots of the local console here. When the console is first opened, the Welcome Page is displayed, which offers quick access to important functions such as a product tour, server settings and client deployment:

This Welcome Page can be set not to start automatically in future. Closing it shows the main console window:

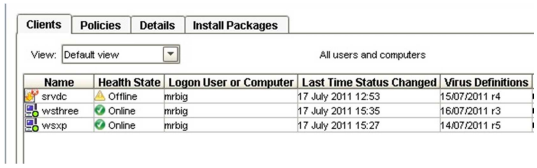


The window opens on the status page, which gives an overview of system protection. A large status display in the top left-hand corner shows the overall state of security on the network, with a big tick (checkmark) in a green circle if all is well. Below this is a section entitled Endpoint Status, which shows in the form of a pie chart how many clients are up to date, out of date, offline or protected. This is a very easy way of showing the state of the network at a glance.

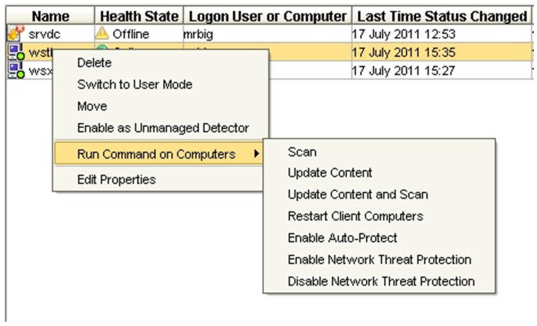
In the top right-hand corner of the console window is a small box showing the licence status (number of days until licence expiry), and below this a larger area with a graphical display of Symantec's estimated current threat level. Under that is a customisable display of malware detected and action taken, and a section with links to the administrator's most commonly used reports. Finally, there is a

drop-down menu at the top of the console, entitled Common Tasks. This contains the options "Install protection client to computers", "Run LiveUpdate", and "Activate License". Thus the most important tasks and information are easily accessible from the console's home page.

The left-hand column of the Endpoint Protection Manager window is a menu bar with icons for other areas of administration: Monitors, Reports, Policies, Clients, and Admin. The Clients tab gives an overview of the client PCs on which the software has been deployed, together with their status:



This can be used to carry out everyday administration tasks, such as updating, scanning or restarting the client PCs (as shown below). This can be done on individual or multiple PCs, and selecting a number of PCs can be done using standard Windows Explorer techniques, such as Ctrl + Click.

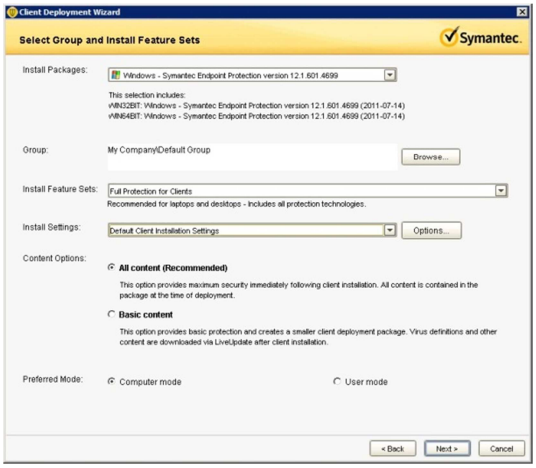


Using the manual to prepare for deployment

The section on planning the installation gives an overview of the steps required, including considering the network architecture (very valuable for large and multi-site networks), system requirements for the computers to be installed, preparing computers for installation, installing the management server, installing client PCs, and post-installation tasks.

Deploying client software using push install

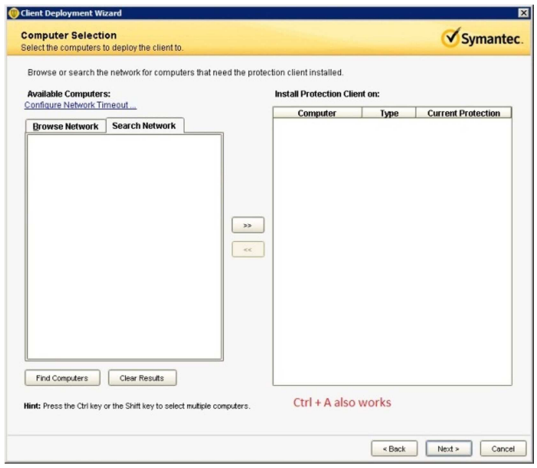
Deployment is started from the home page of the console, by selecting Install Protection Client to Computers from the Common Tasks menu. There is a choice of New Package Deployment or Existing Package Deployment; as this is our first deployment, we chose the former. The next step is to choose the software package to be deployed, along with the features, settings and installation mode:



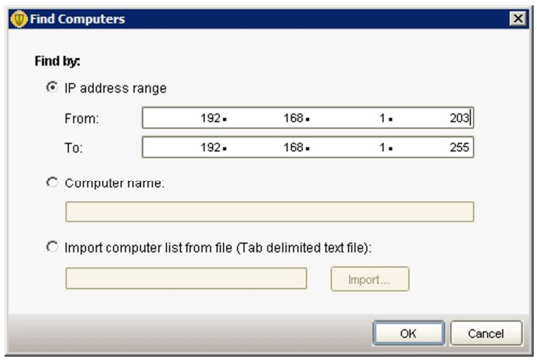
Amongst the options offered on this page of the wizard are the choice of Windows or Mac client software, whereby the Windows package includes separate versions for 32 and 64-bit clients; feature sets optimised for maximum protection or maximum PC performance; a choice of a smaller installation package that is fast to install, or a larger package with all updates included. The latter option is obviously valuable if installing clients remotely over a WAN; pushing out a smaller installation package and letting the clients update themselves is clearly a sensible policy in this scenario.

The next step is to choose the preferred installation method, the choice being: Web link and Email; Remote Push; Save Package (creates the install package but does not deploy it). We chose the Remote Push option. The next page of the wizard allows the

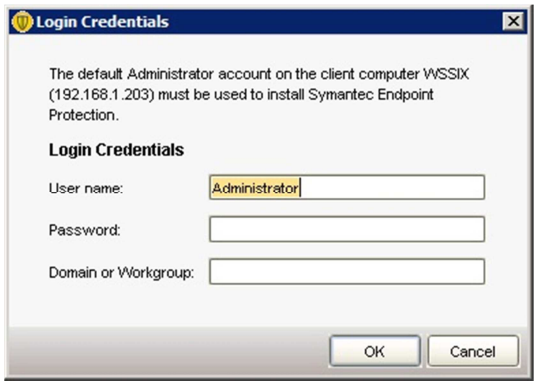
administrator to choose the client PCs to be installed:



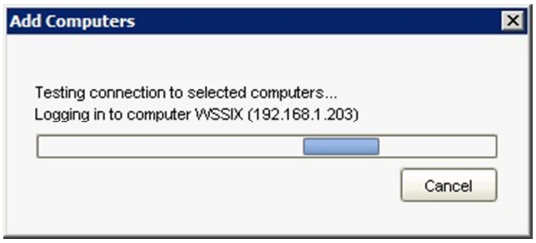
There are two methods of selection, Browse Network (which looks for domains/workgroups found on the network), and Search Network. The latter searches for all computers within a given IP address range, as shown below:



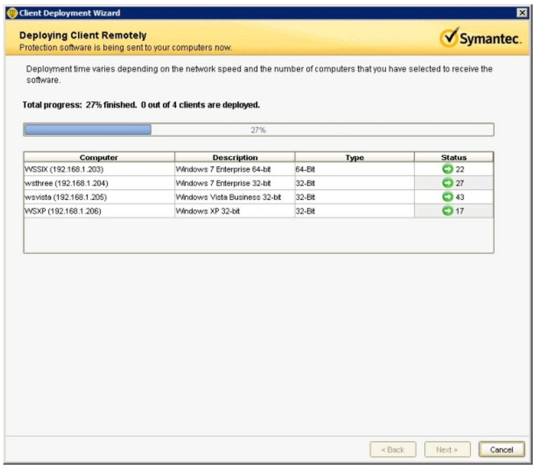
We chose the Search Network option for finding our client PCs. Having selected the PCs from the list in the left-hand pane of the window, clicking on the button to add them to the group to be installed brings up a prompt for administrator credentials to be used:



After this, the deployment wizard attempts to log on to the selected PCs, to test that they can be accessed:



We find this to be a very sensible measure; if any clients are inaccessible (e.g. because file sharing has not been enabled), the administrator can rectify the problem immediately, instead of waiting until the end to find that some installations have failed.
In our test installation, no problems were found, and the process continued. The Symantec wizard displays a very clear and detailed real-time report on the progress of the installation on each individual machine:

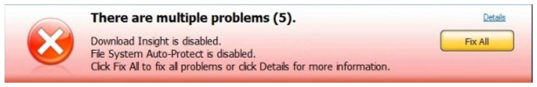


This is ideal, enabling the administrator to see which machines have completed, and how far the installation has progressed on others. The manual notes that a restart is necessary after successful deployment; this can be done remotely for all PCs in one task.

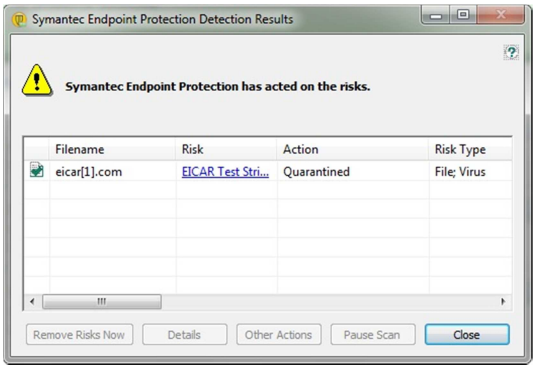
Client software

Symantec Endpoint Protection registers with the Windows 7 Action Center as the firewall, antivirus and antispyware components. The main program window opens on the status page; it is very clear and simple, giving essential information at a glance and easy access to the most important functions, such as updating and scanning, in a menu panel on the left-hand side:

The status strip at the top shows very clearly if optimum protection is functioning, using a large tick (checkmark) on a green background when all is well, and a cross on a red background if there is a problem. In the latter case, a "Fix All" button appears; clicking this automatically tries to resolve any problems without further user intervention.



When we attempted to download the EICAR test virus, Symantec Endpoint Protection blocked the download and displayed the following warning message:



No user interaction is required, and it should be reasonably clear to most users that the "threat" has been eliminated.

When logged on to the PC with administrator rights, it is very easy to temporarily disable the antimalware protection using the Options button in the relevant section of the window. However, this is sensibly disabled when logged on as a standard user without admin privileges:

In summary, the Symantec Endpoint Protection client software can be said to have found an ideal compromise of simplicity with essential functionality. There is a separate manual for the client software included as part of the Endpoint Protection package.

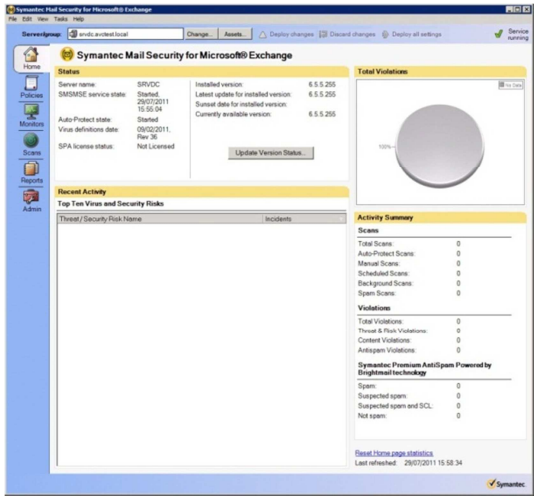
Exchange Server protection

Installation of Symantec Mail Security for Microsoft Exchange is not complicated, but it is important to look at the manual and check that all the system requirements are met before starting the setup program. There are a number of required Windows services and components, such as Internet Information Services and the .net Framework, which must be installed in order for the Mail Security setup to complete successfully; these vary

according to the versions of Windows Server and Exchange Server.

Having ensured that all of the system requirements have been met, the administrator can proceed with the installation. This is a straightforward wizard, which requires accepting a licence agreement; choosing an installation folder and setup type (Complete or Custom, we chose the latter); entering details of the server and port to be used (pre-filled); and entering an email address for notifications.

The Symantec Mail Security Console has a simple design, with a large main pane for information, and a narrow left-hand menu column, with the tabs Home, Policies, Monitors, Scans, Reports and Admin:



The Home page shows program and server information, including a list of recent threats and scan results. The Policies tab has configuration options such as what to do in the event of malware discovery, and how to handle spam. Monitors includes Server Status, Notification Settings, Quarantine, and Event Log. Scans allows settings for Auto-Protect, plus manual and scheduled scans, to be configured. Reports allows detailed activity reports to be created, while Admin includes System Settings and Licensing. We felt that the console provided all the features and settings that the administrator of a small business network could want, easily accessible in a simple program interface.

Conclusion

Symantec's Endpoint Protection software is designed to cope with enterprise networks, and has a wealth of features to enable it to do this. Nonetheless, the design of the software has been kept sufficiently simple that it is very straightforward to use in a small business environment too. Our one suggestion for improvement would be a simplified manual for small businesses, enabling the administrator to find the relevant options more quickly.

Deployment areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)
★★★★	★★★★½

Overview:

Installation/Deployment	★★★★½
Console	★★★★½
Client Software	★★★★★
Manual	★★★★
Overall	★★★★½

Trend Micro

Tested Software:

Trend Micro™ Worry-Free™ Business Security 7.0

Introduction

Trend Micro makes a wide range of products for small, medium and enterprise-sized businesses. Worry-Free Business Security is their small-business product, recommended for networks of 5 to 100 users.

Software version reviewed

Trend Micro™ Worry-Free™ Business Security 7.0

Downloading the software

The software comes in the form of a single .exe file; when run, this unpacks the contents to a single folder, containing the individual installation files.

Using the manual to prepare for installation

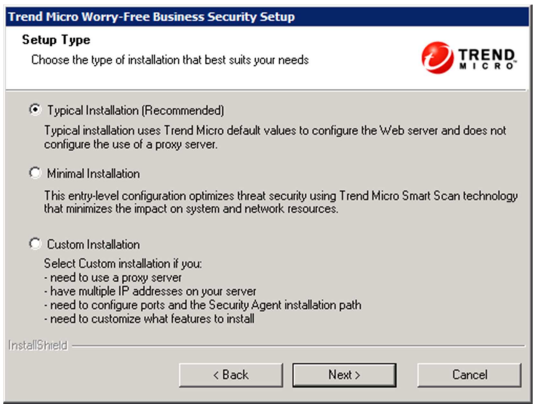
The Administration Guide is the manual provided by Trend Micro for Worry-Free Business Security. It is comprehensive, at 506 pages. It is very well indexed and bookmarked, making it very easy to find specific sections. There is a very detailed table of contents at the beginning, with links to the relevant pages, so that simply clicking on a page number goes directly to that page. The manual can also be navigated very easily using the headings shown in the bookmarks pane of Adobe Reader. Screenshots are few and far between, however, which is a rather a pity, even if the text instructions are very clear.

There is a substantial section at the beginning of the manual describing the product's features, including a subsection on features introduced in the current version. There is a detailed description of the web console and how to use it, along with sections on installing and administering client software.

One thing the manual does not cover is the installation of the management software itself. There is a reference to the WFBS Installation Guide, which is a separate document, not included in the package provided for us by Trend. However, installing the console turned out to be a very straightforward process, so we did not consider the lack of instructions in the main manual to be a problem.

Installation of the administration software

Double-clicking the packaged installation file extracts the necessary files and folders into a folder of the user's choice. In the root of this folder is an .exe file called Setup. Double-clicking this starts the installation wizard. One of the first steps is the normal licence agreement, which is followed by a choice of installation type, with the options Typical, Minimal and Custom. We note that the dialog box very helpfully shows details of the features that can be configured by choosing Custom:



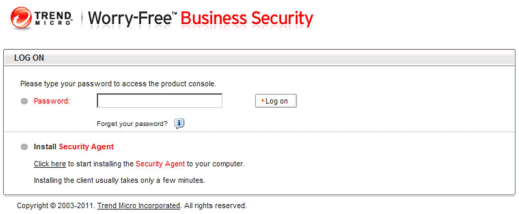
We chose the Typical installation. The next step is entering a licence key. The wizard informs us that leaving the field blank will allow us a 30-day trial of the product, and this is what we selected. We found the following step a little confusing:

The dialog box shows an overview of the major components of the suite, namely Security Server, Security Agent, and Messaging Security Agent. At first we assumed that the pictures shown above were buttons to click on to configure each of the components, but in fact they are just pictures with no functionality. The only possible action is to click on Next to go to the next step, which is whether to install Exchange Server protection (we chose to do this). The next option is choosing the location of the installation folder. After this, we are asked to enter passwords for the web console and security agents (client software), to prevent unauthorised access:

The following step asks for details of the SMTP server for sending reports and notifications; there are fields for server name, port, and recipient's email address. Next comes the option of sending feedback on discovered threats to Trend Micro for analysis. From this point on, no further user input is required, and the remainder of the installation completes in about 10 minutes. We found that the Typical setup option we had chosen was very simple and unproblematic. On completion, we discovered that the Trend Micro Security Agent (standard antivirus software for client PCs/file servers) had been installed on our server, saving us the task of installing it separately.

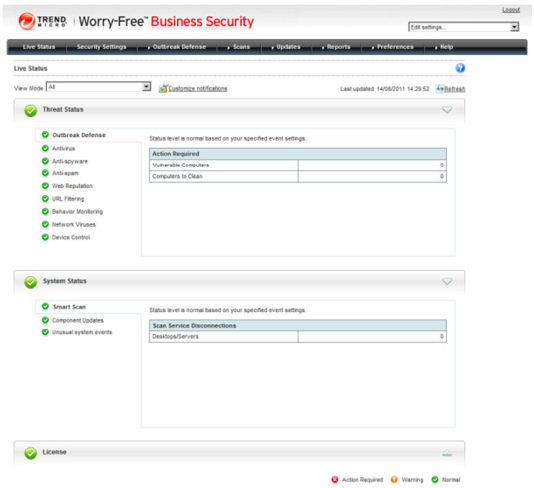
The administration console

The installation process creates Desktop and Start Menu shortcuts to the web-based console. The login page includes a shortcut which can be used to install client software:

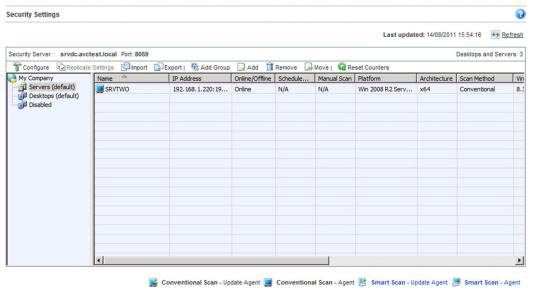


When logging on for the first time, there are two small administrative tasks that need to be carried out. Firstly, Internet Explorer does not recognise the site's certificate, so this needs to be imported to avoid seeing the warning page every time the console is opened. Secondly, the Trend Micro console needs to install an ActiveX component for Internet Explorer. Doing this on a server requires temporarily disabling the Internet Explorer Enhanced Security Configuration, a very quick and simple task for an experienced administrator. We did wonder whether this and the certificate import should be mentioned in the manual, for the benefit of small businesses without dedicated IT staff.

The console opens on the Live Status page, showing an overview of system components and their status:

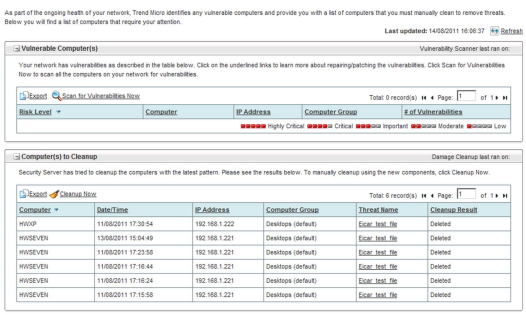


The next tab is Security Settings, which shows all PCs on the network in their respective groups:

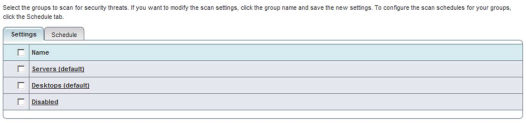


This page can be used to change configuration settings for the groups of PCs. Individual PCs cannot be directly configured, but a new group can be created and the desired configuration settings applied, and a PC is then added to the group. For example, we created a group called Disabled, switched the real-time protection for this group off, and then added a PC to it. We saw that the local protection on that PC was almost instantly disabled. This could be used in practice, e.g. when installing a particular program requires AV protection to be temporarily disabled. Moving the PC out of the Disabled group and back to its original group immediately reactivates the protection.

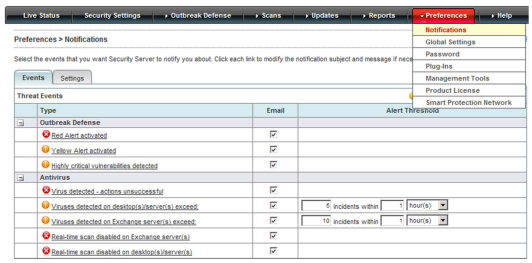
The next tab, Outbreak Defense, is a novel but potentially very valuable means of preventing the spread of self-replicating malware (viruses and worms) around the network. There are three sections: Current Status (shows whether the warning system has been activated), Settings (allows vulnerability scanning and warnings to be set up), and Potential Threat (shows vulnerable computers and recent malware discoveries):



The next tab, Scans, is extremely simple. There is a choice of manual or scheduled scan; the latter includes an additional Schedule tab to set the time, as well as the choice of groups to be scanned:



Updates, the next tab in the console, allows the administrator to choose the components to be updated, a schedule for doing this, and an updates source, i.e. directly from Trend Micro or from an update server on the LAN. The Reports tab allows content and frequency of logs to be configured. The final tab, Preferences, has a menu with numerous configuration areas. The screenshot below shows the menu and a small selection of the Notification settings:



In summary, we found the console to be very simple and straightforward. The idea of configuring and installing groups of computers, rather than individual PCs, is a little unusual, but analogue to the creation of

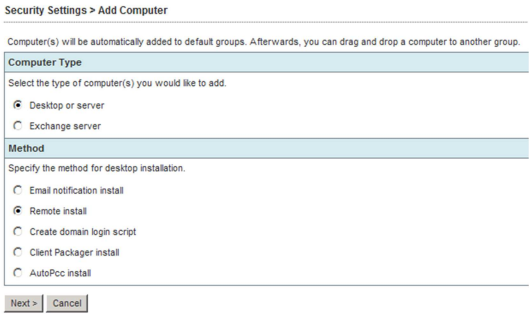
user groups for setting NTFS or share permissions in Windows. Once the administrator has grasped the concept, it works well in practice. Our only actual criticism is the lack of instructions in the manual for installing certificates and disabling ESC for Internet Explorer, as we feel these could be valuable for small business without IT experts.

Using the manual to prepare for deployment

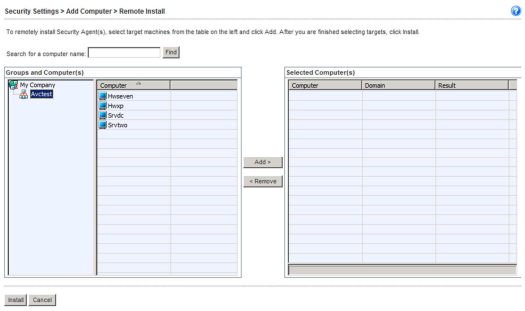
It is very easy to find the instructions for performing a push install in the manual. They are brief, not because they lack any detail, but because the process is extremely simple. There is a short section on preparing Windows Vista/7 clients for preparation, which involves enabling file sharing and starting the Remote Registry service. Again this is very simple and clear; our only tiny criticism is that this section comes rather illogically at the end of the instructions on push installation, rather than at the beginning. Concluding the section on different installation methods is a guide to checking that the client has been installed successfully on each machine (e.g. looking in Programs and Features), and testing its correct function using the EICAR test virus.

Deploying client software using push install

The remote push installation is started by clicking on the Settings tab in the console, then Add. The next step is to choose between desktop/file server installation on the one hand, and Exchange server installation on the other, and select Remote Install as the installation method:



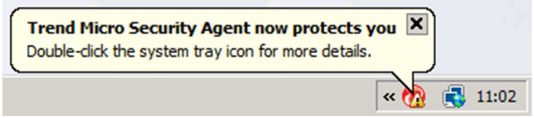
We then need to choose the computers to be installed. The wizard shows the computers within a domain/workgroup; we did not find any means of selecting Active Directory OUs.



Selecting computers from the list uses most normal Windows selection methods, such as Ctrl + Click, although Ctrl + A has no effect. Having selected the computers to be installed, we click on Add. At this point a prompt for the administrator credentials to be used appears, and then clicking on Install starts the installation process. Real-time display of the installation progress is very limited, but the process is so quick that this doesn't matter. In summary, we found installing Trend Micro Worry-Free Business Security clients using remote push to be unbeatably quick and simple.

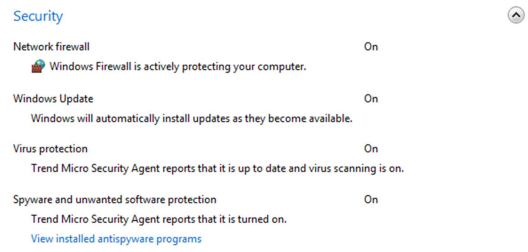
Client Software

When the Trend Micro Security Agent (client software) has been deployed to a PC, a familiar Trend Micro icon appears in the Windows System Tray:

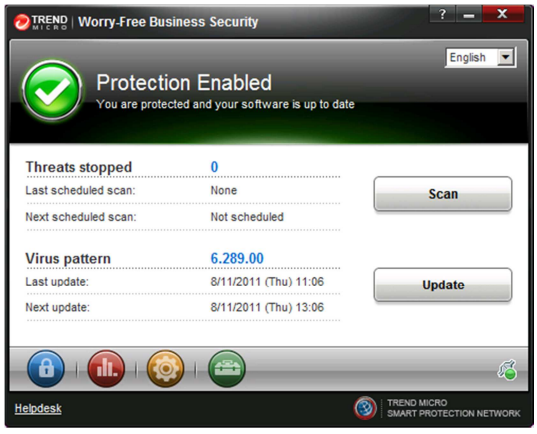


Double-clicking this opens the main program window, and right-clicking it shows a short menu with options such as Update.

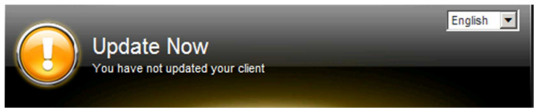
The Trend Micro Security Agent registers itself in the Windows 7 Action Center as the antivirus and antispyware application:

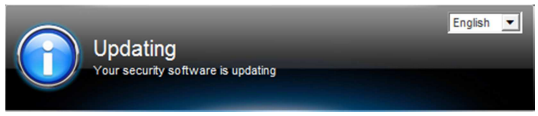


There is a Trend Micro firewall included in the package, although it is not switched on in the default installation (it is one of the additional options in the Custom installation). It can easily be enabled from the console, although this does not automatically turn Windows Firewall off; that has to be done manually.
The main program window has a simple, uncluttered interface, dominated by a big horizontal strip at the top, showing the current security status:



This section changes to show any changes/problems with the security status:

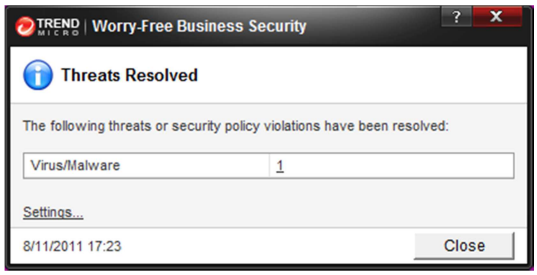




This strip also contains a drop-down menu for changing the interface language, with a choice of 8 major European languages. Selecting a different interface language closes the program window; when re-opened, the new language interface will be displayed:

This very quick and easy method of changing languages would be very valuable in a multi-lingual environment.
The main pane of the program window shows status information on threats found, next scheduled scan, and virus definitions. There are also big, obvious buttons for updating and scanning. The latter uses a very simple folder tree dialog to allow specific drives or folders to be scanned.
There is relatively small strip along the bottom of the window containing buttons for Unlock (enables advanced configuration options, password protected), Logs, Settings, and Tools. A rather obscure-looking button in the bottom right-hand corner shows the status of individual components such as the firewall and behaviour monitoring, plus the status of connectivity to the server, and location (in or out of the office).
We could not find any means of activating/deactivating the firewall or real-time AV protection from the client window, even in the password-protected advanced

mode, although both of these can be done easily from the console.
Notification of malware discovery is disabled by default, so when we tried to download the EICAR test virus, it was blocked silently, without any messages from Trend. However, notification can easily be enabled from the console, in which case the following message appears on discovering a threat:

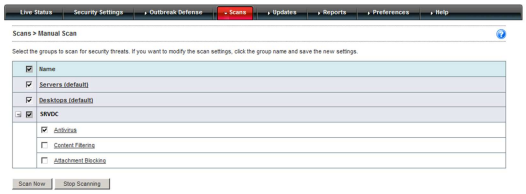


The message clearly states that the threat has been dealt with, and no user interaction is required.

Exchange Server Protection

Exchange Server protection is very much built in to the same framework as the other components. It is installed during the setup of the management software, as described above, requiring only a couple of steps in this process. Protection could be deployed to additional Exchange servers by running the deployment wizard and selecting the Exchange Server option.

Exchange protection management is likewise integrated into the main console. For example, scanning a computer using the Scans tab on the console shows the Exchange server in the list of computer types, with additional relevant options:



All the relevant Exchange server tasks are described in the manual. We feel that Exchange server management is so straightforward and so well integrated into the console, that further description is unnecessary.

Conclusion

Trend Micro Worry-Free Business Security 7.0 is exceptionally easy to install and use. We would suggest that this makes it an excellent choice for small businesses without dedicated IT staff. Our only suggestions for improvement would be to include some additional explanations and screenshots in the manual.

Deployment areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)
★★★★½	★★★★½

Overview:

Installation/Deployment	★★★★½
Console	★★★★½
Client Software	★★★★½
Manual	★★★★½
Overall	★★★★½

Appendix A – Featurelist short

Feature list	AVIRA	Bitdefender	eScan	ESET	G Data	Kaspersky	McAfee	Symantec	Trend Micro
Recommended product for:									
up to 5 Clients, Server	Avira AntiVir Professional	BitDefender Internet Security	eScan ISS SMB	ESET Smart Security Business Edition	G Data Antivirus Business	Kaspersky Small Office Security	McAfee SaaS Endpoint	Symantec Endpoint Protection Cloud	Worry-Free Business Security - Standard
up to 25 Clients and 1 Fileserver	Avira AntiVir NetWork Bundle	BitDefender Small Office Security	eScan ISS SMB	ESET Smart Security Business Edition	G Data Antivirus Business	Kaspersky Business Space Security	McAfee SaaS Endpoint	Symantec Endpoint Protection Small Business Edition	Worry-Free Business Security - Standard
up to 25 Clients and Fileserver and Messaging Server	Avira AntiVir NetWork Bundle	BitDefender Business Security	eScan Enterprise	ESET Small Business Security	G Data Antivirus Enterprise	Kaspersky Enterprise Space Security	McAfee SaaS Total Protection	Symantec Protection Suite Small Business Edition	Worry-Free Business Security - Advanced
more than 25 Clients, more than 1 Fileserver, more than 1 Messaging server	Avira Business Bundle	BitDefender Business Security	eScan Enterprise	ESET Small Business Security	G Data Antivirus Enterprise	Kaspersky Enterprise Space Security	McAfee Endpoint Advanced	Symantec Protection Suite Small Business Edition	Worry-Free Business Security - Advanced
Features Management Server									
What is the maximum number of clients overall?	20000	10000	unlimited	unlimited	50000	unlimited	unlimited	unlimited	unlimited
Master-Slave-Server									
Multiple AV Servers	●	●		●	●	●	●	●	●
Master server controls slave server in different offices	●	●		●	●	●	●	●	●
Slave server for distributing updates	●	●		●	●	●	●	●	●
Client Installation									
Which client deployment methods does the product support?									
Does the product include a mechanism that allows the administrator to push the software to the clients?	●	●	●	●	●	●	●	●	●
Does the product include a mechanism that allows the end user to download and install the software?	●		●	●		●	●	●	●
General Capabilities									
Does the product allow administrators to assign different policies to different groups of computers (regardless of the person logged in)?	●	●	●	●	●	●	●	●	●
Does the product support static groups (i.e. user or computer are assigned manually to a group or are imported from a third party system)?	●	●		●	●	●	●	●	●
Group Import & Synchronisation									
Can changes in Active Directory be synchronized?	●			●		●	●	●	●
Can computers/users be imported from other LDAP server?	●		●	●		●		●	
Can computers be imported by a GUI	●	●	●	●	●	●	●	●	●
Can different actions be defined based on the malware category?				●	●	●	●	●	●
Microsoft Exchange									

Exchange 2003		●	●	●		●	●	●	●
Exchange 2007 / 2010		●	●	●	●	●	●	●	●
Network shares									●
Can a user or administrator scan network shares after entering a password?	●		●	●		●		●	●
Email Messages									
Microsoft Outlook	●	●	●	●	●	●	●	●	●
Lotus Notes	●		●	●	●	●	●	●	
Thunderbird	●		●	●	●			●	
Archives									
ZIP/RAR/ARJ & archived installers	●	●	●	●	●	●	●	●	●
Conditions									
Remediation									
Does the product provide remediation capabilities?	●	●	●	●		●	●	●	●
General capabilities									
Firewall Rules									
Does the product come with default policies?									
For workstations	●	●	●	●	●	●	●	●	●
For server	●		●	●	●	●	●	●	●
Client Management									
Client User Interface									
Can the administrator limit or control configuration changes by the end-user?	●	●	●	●	●	●	●	●	●
Can different policies be applied for different computers?	●	●	●	●	●	●	●	●	●
Depending on the location of the device (i.e. Office, Hotel, Home, etc)	●		●		●	●		●	●
Depending on group membership of the computer	●	●	●	●	●	●	●	●	●
Depending on group membership of the user (i.e. administrator vs. normal user)		●	●			●	●		●
Administrator Management									
Rights / Access Control									
Does the product support multiple administrators and different access levels?	●		●	●	●	●	●	●	●
Device Control									
Does the product allow administrators to limit the use of external devices (USB sticks, printers, etc)?		●	●	●	●	●	●	●	●
Can you lock									

DVD / USB / external media		❁	❁	❁	❁	❁	❁	❁	❁
Floppy		❁		❁	❁	❁	❁	❁	❁
other			Bluetooth/Card Readers	All ports and all removable media can be locked, but it's possible to add exceptions for any	webcams				network ressources
Failover									
What if the AV Server (local) hangs up									
automatic switching to a second local server		❁		❁	❁	❁	●	❁	
updates from vendor-server instead of local server	❁	❁		❁	❁	❁	●	❁	❁
other				Log and notifications		any other network shared folder			

Appendix B – Featurelist detailed

Feature list	AVIRA	Bitdefender	eScan	ESET	G Data	Kaspersky	McAfee	Symantec	Trend Micro
Recommended product for:									
up to 5 Clients, Server	Avira AntiVir Professional	BitDefender Internet Security	eScan ISS SMB	ESET Smart Security Business Edition	G Data Antivirus Business	Kaspersky Small Office Security	McAfee SaaS Endpoint	Symantec Endpoint Protection Cloud	Worry-Free Business Security - Standard
up to 25 Clients and 1 Fileserver	Avira AntiVir NetWork Bundle	BitDefender Small Office Security	eScan ISS SMB	ESET Smart Security Business Edition	G Data Antivirus Business	Kaspersky Business Space Security	McAfee SaaS Endpoint	Symantec Endpoint Protection Small Business Edition	Worry-Free Business Security - Standard
up to 25 Clients and Fileserver and Messaging Server	Avira AntiVir NetWork Bundle	BitDefender Business Security	eScan Enterprise	ESET Small Business Security	G Data Antivirus Enterprise	Kaspersky Enterprise Space Security	McAfee SaaS Total Protection	Symantec Protection Suite Small Business Edition	Worry-Free Business Security - Advanced
more than 25 Clients, more than 1 Fileserver, more than 1 Messaging server	Avira Business Bundle	BitDefender Business Security	eScan Enterprise	ESET Small Business Security	G Data Antivirus Enterprise	Kaspersky Enterprise Space Security	McAfee Endpoint Advanced	Symantec Protection Suite Small Business Edition	Worry-Free Business Security - Advanced
Features Management Server									
What is the maximum number of clients overall?	20000	10000	unlimited	unlimited	50000	unlimited	unlimited	unlimited	unlimited
What is the maximum number of clients that can be managed from a single management server under the following conditions: All necessary components (database, repositories, update mechanisms, reporting, etc.) are installed on this server and the Clients communicate with the server either continuously or at least once per hour	1500	1000	20000	10000	1000	50000	250000	80000	20000
Required minimum hardware (CPU/Mem/Disc)	1 GB RAM, 500 MB free HD	Intel Pentium 1Ghz, 512MB RAM, 1,5GB free HD	Intel Core 2 Duo E8400, 3GHz, 4GB RAM, HDD SATA 300GB	Hardware needs only to be strong enough to support the OS	Core 2 Duo 2 GB RAM 1,5 GB	Intel Core 2 Duo E8400, 3GHz, 4GB RAM, HDD SATA 300GB	1.5 GB free disk space 1 GB RAM Intel Premium 4 Processor or later, 1.3 GHz or faster	Intel Core 2 Duo E8400, 3GHz, 4GB RAM, HDD SATA 300GB	1GHz CPU, 1 GB RAM, 3.5 GB free hard disk space
Does the product provide a mechanism to limit the data transferred over WAN Links when updating clients in remote locations?				●		●	●	●	●
By designating one client as local source for definition updates (Super Agent, Group Update Provider)	●		●	●		●	●	●	●
Does the product provide a mechanism to prevent updates over expensive network connections like UMTS?		●			●	●		●	●
Does the product allow customers to use 3rd party tools for virus signature distribution?				●		●	●	●	
Which options does the product provide to ensure that only authorized administrators can administer the product?	Authentification username, password	Authentification username, password	Authentication username, password/Active Directory integration is possible	Password protection, encrypted communication	Administrator account	Authentification username, password	Authentication username & password / certificate based authentication / AD login	Symantec Authentication, Windows Authentication, and RSA Authentication	Authentification username, password
Require minimum password length								●	●
Lock administrator account after entering a password multiple times (prevent brute force attack)								●	●
Log out administrator if idle for a specified time			●				●	●	●
Client / Server Communication									
Does the client authenticate the server?	●	●	●	●	●	●	●	●	●
Does the server authenticate the client?		●		●	●	●	●	●	●
Is the communication between the client and the server encrypted?	●		●	●	●	●	●	●	
Does the product support a 'pull' communication mode?	●	●	●	●	●	●	●	●	●
Can the communication interval be modified?	●	●	●	●	●	●	●	●	●
What is the recommended communication interval?	60 minutes	5 minutes	120 minutes	10 minutes	5 minutes	15 minutes	60 minutes	60 minutes	Real Time

Does the product support a push communication mode?	●		●		●	●	●	●	●
Does the product protect itself from being tampered (or processes being stopped) by the end-user or malicious software?	●	●	●	●	●	●	●	●	●
Proxy Server									
Can a proxy server be specified for HTTP?	●	●	●	●	●	●	●	●	●
Can a proxy server be specified for FTP?			●			●	●	●	
Does the product support proxy server authentications?	●	●	●	●	●	●	●	●	●
Master-Slave-Server									
Multiple AV Servers	●	●		●	●	●	●	●	●
Master server controls slave server in different offices	●	●		●	●	●	●	●	●
Slave server for distributing updates	●	●		●	●	●	●	●	●
Notes		Update Server is separate from the Slave Server. It is possible to install and configure more Update Servers in cascade		Slave servers can be nested multiple levels, they each have their own credentials for full access and for read-only access. Policies from upper server can be propagated to lower servers.					
Client Installation									
Which client deployment methods does the product support?									
Does the product include a mechanism that allows the administrator to push the software to the clients?	●	●	●	●	●	●	●	●	●
Can the installation of the clients be staggered over time to ensure that the network is not over utilized?	●			●	●	●	●	●	●
Can the administrator see the status of the deployment (i.e. Transfer, Installation in Progress, Installation complete, etc.)?	●	●	●	●	●	●	●	●	●
Does the product include a mechanism that allows the end user to download and install the software?	●		●	●		●	●	●	●
Can the admin send a link which allows the user to download and install the software?	●		●	●		●	●	●	●
Does to product support the creation of MSI packages for deployment with 3rd party tools and Active Directory (GPO)?			●	●		●	●	●	●
Does the product support the creation of single file executable (.exe) installer (i.e. for logon scripts or CD distribution)	●	●	●	●	●	●	●	●	●
Which installation types can be defined in the user interface?									
Silent Installation (no user interface is displayed)	●	●	●	●	●	●	●	●	●
Unattended installation (the end-user sees the progress of the installation but can not modify the settings)	●	●	●	●		●		●	●
Interactive Installation (user chooses the preferences)	●			●	●	●		●	●
Can the installation folder be specified in the user interface?			●	●		●	●	●	●
Can the administrator define whether the program is added to the Start Menu?						●		●	

Other installation options	Modules can be selected	Define if user is restricted or power, define what modules to install or enable/disable, restart options, scan before install, set administrative password		All options of the client can be specified as a parameter of the push installation					A separate tool to probe the local network and deploy the agent accordingly
General Capabilities									
Is the system Multi-tenancy capable (host multiple customers on the same infrastructure but separating the data)?		●			●	●	●	●	
Does the product allow administrators to assign different policies to different groups of computers (regardless of the person logged in)?	●	●	●	●	●	●	●	●	●
Does the product allow administrators to assign policies to users (regardless of the computer they use)?		●					●	●	
Does the product support static groups (i.e. user or computer are assigned manually to a group or are imported from a third party system)?	●	●		●	●	●	●	●	●
Does the product support dynamic group assignment based on criteria like IP addresses?	●			●		●	●		●
Does the product support hierarchical groups with inheritance?	●	●	●	●	●	●	●	●	●
Location Awareness									
Is the product capable of using different policies, settings and rules depending on the location of the computer?	●		●		●	●	●	●	●
Which settings/policies can be changed depending on the location?									
Antivirus policies	●		●		●	●		●	
Firewall policies	●		●	●	●	●	●	●	●
HIPS / IPS policies	●					●	●	●	●
Device Control policies			●		●	●	●	●	●
Other protection technology policies	Updating		●	Update and Network zones	Anti-Spam, Web Content filter, Internet usage control, Application control	Anti-Spam; Proactive Defence; Anti-Banner; Anti-Dialer; Anti-Hacker; Updating		Application Control, System Lockdown, Optional Licensed Host Integrity	Web Reputation
Client settings	●		●			●		●	
User interface configuration	●		●		●	●		●	
Communication settings	●		●	●	●	●		●	●
Content update settings	●		●	●	●	●		●	●
Can the customer define an 'unlimited' number of locations?	●			●	●	●		●	●
Which criteria can the customer use to define locations?									
Client IP Configuration									
By specifying IP addresses / IP address ranges	●		●	●		●		●	●
By specifying the Gateway									
By IP address / range			●	●		●	●	●	●
By MAC address								●	●
The client must have the specified Gateway				●		●	●	●	●

The client must not have the specified Gateway						●		●	
By specifying DHCP server									
By IP address / range			●	●		●	●	●	
By MAC address								●	
The client must have the specified DHCP server				●		●	●	●	
The client must not have the specified DHCP server			●			●		●	
By specifying the DNS Server Address									
The client must have the specified DNS server				●		●	●	●	
The client must not have the specified DNS server						●		●	
By specifying DNS suffixes				●		●	●	●	
By specifying the type of network connection used or not used by the client (e.g. Ethernet, Wireless, VPN, Dial-up, etc.)	●			●				●	●
By checking whether a client can or can not resolve a DNS host name							●	●	●
By checking the Registry							●	●	
Can multiple criteria be used to define a location?				●		●	●	●	
When are location criteria evaluated?									
Periodically					●	●	●	●	
Immediately when a change in the network configuration takes place (i.e. network adapter enabled / disabled)	●			●	●	●	●	●	●
Can the end-user be notified about a location change?				●				●	●
Are location changes logged?	●					●	●	●	
Group Import & Synchronisation									
Can computers be imported from a text file?	●	●		●		●	●		
Can computers be imported from Active Directory?	●	●	●	●	●	●	●	●	●
Keeping the OU structure defined in Active Directory	●	●	●	●	●	●	●	●	●
Using other criteria to assign computers to groups	●	●	●	●	●	●	●		●
Can changes in Active Directory be synchronized?	●			●		●	●	●	●
Can the synchronisation schedule be defined?	●			●	●	●	●	●	●
Can computers be imported from multiple Active Directory server?			●		●	●	●	●	●
Can computers/users be imported from other LDAP server?	●		●	●		●		●	
Can computers be imported by a GUI	●	●	●	●	●	●	●	●	●
Can different actions be defined based on the malware category?				●	●	●	●	●	●
Scan Location									
Can the administrator exclude/include files and folders from being scanned (by file extension)?	●	●	●	●	●	●	●	●	●
By predefined lists of extensions provided by the product	●	●	●	●		●	●	●	●
By filenames ("file.txt") regardless of folder or location	●	●	●			●	●		●

By filenames & specific folder ("c:\Directory\file.txt")	●	●	●	●	●	●	●	●	●
By folder name	●	●	●	●	●	●	●	●	
Standard Windows folder (i.e. %WINDOWS%, %SYSTEM32%) regardless of the operating system language	●	●	●			●	●	●	●
Does the product provide preconfigured exclusions?	●	●	●	●		●		●	●
Microsoft Exchange									
Exchange 5.5				●		●			
Exchange 2000			●	●		●		●	
Exchange 2003		●	●	●		●	●	●	●
Exchange 2007 / 2010		●	●	●	●	●	●	●	●
Network shares									●
Is scanning of network shares disabled by default?	●	●		●	●	●	●	●	●
Can a user or administrator scan network shares after entering a password?	●		●	●		●		●	●
System memory / Processes									
Does the product scan processes in memory for malware?	●	●	●	●	●	●	●	●	●
Can the administrator define exceptions?		●	●		●	●	●		●
Boot sectors	●	●	●	●	●	●	●	●	●
Email Messages									
Does the product scan existing email in the message stores of the following applications?									
Microsoft Outlook	●	●	●	●	●	●	●	●	●
Microsoft Outlook Express	●	●	●	●	●	●	●	●	●
Lotus Notes	●		●	●	●	●	●	●	
Thunderbird	●		●	●	●			●	
Microsoft Windows Live Mail	●		●	●	●			●	
Microsoft Windows Mail	●	●	●	●	●	●		●	
The Bat!	●		●		●	●		●	
Does the product scan incoming and outgoing emails and attachments in the following protocols?									
SMTP / POP3	●	●	●	●	●	●	●	●	●
IMAP	●			●	●	●	●	●	●
Archives									
ZIP/RAR/ARJ & archived installers	●	●	●	●	●	●	●	●	●
how deep at on demand (by default)	20	15	16	10	100	unlimited	unlimited	10	2
Does the product protect itself against Zip of Death and similar attacks?									
By limiting the recursion depth	●	●	●	●		●		●	●
By limiting the number of files unpacked		●							●
By limiting the size of an unpacked archive	●	●	●	●	●	●		●	●
By limiting the processing time for unpacking archives			●	●		●	●		

Offline files and sparse files									
Does the product allow administrators to define how files with the offline bit set should be handled?									
Skip offline and sparse files with a reparse point	●					●		●	
Scan resident portions of offline and sparse files			●			●		●	
Scan all files without forcing demigration			●			●		●	
Scan all files touched within a defined timeframe without forcing demigration			●			●		●	
Other locations				Scan media at computer shutdown				Floppy, well known virus locations	
Does the product provide preconfigured scan locations?	●		●	●		●		●	●
On Demand Scans									
Can the administrator define when scans should take place and which Scan locations should be included / excluded?	●	●	●	●	●	●	●	●	●
Can the system impact vs. scan speed be defined?	●		●	●	●	●	●	●	●
On Access Scan									
Can the administrator define when a scan is triggered?	●	●		●		●		●	●
Can the administrator specify which Scan Locations should be included / excluded?	●	●	●	●	●	●	●	●	●
Files / Directories		●	●	●	●	●	●	●	●
Log									
Which information is logged?									
The Date and time the infection was detected	●	●	●	●	●	●	●	●	●
The name of the infection and the original location where the infection was found (incl. file name)	●	●	●	●	●	●	●	●	●
The malware category (i.e. Virus, Worm, etc)	●		●	●		●	●	●	●
The computer on which the infection was found	●	●	●	●	●	●	●	●	●
The user who was logged on at the time the infection was detected	●		●	●	●	●	●	●	●
The action and current status of the infection (i.e. cleaned, deleted, quarantined, still infected)	●	●	●	●	●	●	●	●	●
The current location of the infected file (i.e. local quarantine)	●	●	●	●	●	●	●	●	●
The scan that detected the infection (i.e. On Access, Manual, Start-up, etc)	●	●	●	●	●	●	●	●	●
End-user Interaction									
Let the end-user choose the action	●	●		●	●	●	●	●	●
Notify the end-user									
By displaying a pop up or balloon	●	●	●	●	●	●	●	●	●
Can the notifications be customized?	●	●		●	●	●	●	●	●
By adding a warning to an infected email body or subject (email)	●	●	●	●	●	●	●	●	●
By replacing an infected attachment	●	●		●	●	●	●	●	●
Can the notification can be customized?	●	●	●	●	●	●	●	●	●
Run a script or application after detection	●			●		●		●	●

Can a second or alternative action be defined (i.e. if the first action fails)?	●	●		●	●	●	●	●	●
Which file specific actions can the product perform?									
Clean / Delete	●	●	●	●	●	●	●	●	●
Can the product create a backup of the file before attempting to clean it?	●		●	●		●	●	●	●
Quarantine on the local system	●	●	●	●	●	●	●	●	●
Quarantine in a central location			●	●	●	●	●	●	●
Deny Access	●	●	●	●	●	●	●	●	
Which processes specific actions can the product perform									
Terminate the process	●	●	●	●	●	●	●	●	●
Stop the service		●		●	●			●	●
Registry Access Rules									
Does the product allow to monitor and prevent access to registry keys and values?	●	●			●	●	●	●	●
Does the product allow to define/exclude for which processes (application and services) a registry access rule applies?		●				●	●	●	●
File and Folder Access Rules									
Does the product allow to monitor and prevent access to specific files and folders?			●	●	●	●	●	●	●
Does the product allow to define/exclude for which process a file/folder access rule applies?			●		●	●	●	●	
Which selection criteria does the product provide to specify files and folders?									
By Filenames ("file.txt") regardless of folder or location		●	●		●		●	●	●
By Filenames & Specific Folder ("c:\Directory\file.txt")		●	●				●	●	●
By Filename and Windows Folder (i.e. %System32%\hosts")		●	●				●	●	●
Using wildcards (i.e. *,?)		●			●		●	●	●
Using regular expressions							●	●	
Limit by Location (i.e. local drive, CD, USB Stick)				●	●	●		●	●
Any Local Hard Drive		●		●	●	●	●	●	
Any CD/DVD Drive				●	●	●	●	●	
Any Network Drive		●				●	●	●	●
Any removable media		●		●	●	●	●	●	●
Process Access Rules									
Does the product allow to monitor and prevent launching processes?		●			●	●	●	●	●
Does the product allow to monitor and prevent terminating processes?	●						●	●	●
Does the product allow to define/exclude for which processes a process access rule applies?		●				●	●	●	●
Does the product provide selection criteria to specify processes, e.g. by name?		●					●	●	●
Process Definition									

How can processes (i.e. applications & services) be specified that are allowed/disallowed to perform actions (i.e. modify files, read registry keys, load dlls)?									
By file fingerprint / hash	●						●	●	●
By filenames & specific folder ("c:\Directory\application.exe")	●	●					●	●	●
Using wildcards (i.e. *,?)							●	●	
Limit by location (i.e. local drive, CD, USB Stick)								●	
HIPS Actions									
Which actions can be taken when a rule is triggered?	repair, rename, quarantine, delete, ignore, block, overwrite and delete	Allow, Ask, Block	Block, Allow Temporary, Allow Permanently	Block		Block	Block, Log, Allow	Block, terminate Process, Log	
Allow / Block Access to the resource	●	●	●	●		●	●	●	
Terminate the process trying to access the resource		●				●		●	
Can the end user be notified when a rule is triggered?		●	●	●		●	●	●	
Can a log entry be created when a rule is triggered?	●	●	●	●		●	●	●	
Conditions									
Which conditions can be checked using the user interface (without using scripts)									
Conditions for files and folder: How can files be specified?									
By filenames ("file.txt") regardless of folder or location	●	●	●			●	●	●	
By filenames & specific folder ("c:\Directory\file.txt")	●	●	●	●		●	●	●	
By filename and windows Folder (i.e. #System32#\hosts")	●		●			●	●	●	
By referencing a value in the registry							●	●	
Which conditions can be specified for file existence									
File or Directory exists / does not exist							●	●	
File has specified hash / file fingerprint							●	●	
File version							●	●	
Which conditions can be specified for file (application) versions?									
File version is equal / not equal to specified version						●	●	●	
Conditions for registry keys and values									
A specified registry key or registry value exists / does not exist							●	●	
Conditions for numeric (DWORD) registry values?									
Is equal / not equal to specified number							●	●	
Conditions for text (String) registry values?									
Is equal / not equal to specified text							●		
Contains / does not contain specified text							●	●	
Conditions for binary registry values?									
Is equal to specified value							●		

Contains specified value							●		
Conditions for processes									
Process or service is running / not running			●			●	●	●	
Conditions relating to the operating system									
Type of operating system						●	●	●	
Language of operating system			●			●	●	●	
Service pack level of the operating system						●	●	●	
Is equal / not equal to specified value							●	●	
How can conditions be combined?									
If .. Then .., Else								●	
Logical (AND, OR)		●					●	●	
Can the checks interact with the end-user?									
Notify end-user (i.e. that an operation will take some time to complete, e.g. by an assessment %)						●		●	
Query end-user		●				●		●	
Does to product provide preconfigured conditions?									
Preconfigured Antivirus Check	●	●	●	●		●	●	●	●
Preconfigured Firewall Check	●		●	●		●	●	●	●
Preconfigured Patch Management Check			●	●			●	●	●
Other	Standard and Expert configuration			Alert user when OS is not up-to-date (patched)		DB update			
Remediation									
Does the product provide remediation capabilities?	●	●	●	●		●	●	●	●
Which remediation action can be defined in the user interface (without resorting to scripts)?									
Registry remediation	●						●	●	●
File remediation									
Delete files / folders	●	●		●		●	●	●	●
Download files						●	●	●	
Process remediation									
Run application in user / system security context	●			●			●	●	●
Start service in user security context	●						●	●	●
Start service in system security context	●			●			●	●	●
Software Remediation									
Download software and patches	●		●	●		●	●	●	
Install / uninstall software and patches in user / system security context						●	●	●	
End-user interaction									
Inform user	●	●	●	●		●	●	●	●
Query user	●	●	●	●		●		●	
Enforcement									

Can the product prevent that a client failing the client health check connects to a network?				●		●	●	●	●
Which enforcement frameworks does the product support?									
Microsoft Network Admission Control	●		●			●	●	●	
Cisco Network Access Control	●		●	●		●		●	●
Other			OPSWAT	OPSWAT			McAfee Network Security Platform	Symantec Network Access Control	
Does the product have inbuilt enforcement capabilities?									
Host Based Enforcement / Self Enforcement (i.e. leveraging a desktop firewall to prevent network connections)	●	●		●		●	●	●	
Behaviour detection									
Behavior detection	●	●	●	●	●	●	●	●	●
Is this technology enabled by default?	●	●	●	●		●	●	●	●
General capabilities									
Is the firewall stateful for TCP and UDP connections?	●	●	●	●	●	●	●	●	●
Can the firewall analyze VPN traffic		●	●	●		●	●	●	●
Firewall Rules									
Does the product come with default policies?									
For workstations	●	●	●	●	●	●	●	●	●
For server	●		●	●	●	●	●	●	●
Which criteria can be used when defining rules?									
Application									
By filenames ("application.exe")		●	●		●	●	●	●	●
By filenames & Specific Folder ("c:\Directory\application.exe")		●	●	●		●	●	●	●
By File Fingerprint / Hash						●	●	●	
By Process	●	●			●		●	●	
Network adapter type									
Ethernet / Wireless / VPN / Dial-up	●	●	●	●	●	●	●	●	●
Direction									
Local / Remote	●	●	●	●		●	●	●	●
Source / Destination	●	●	●	●	●	●	●	●	●
Remote Host									
By IP address / IP range	●	●	●	●	●	●	●	●	●
By MAC address			●				●	●	
By DNS Name						●	●	●	●
By DNS Domain						●	●	●	●
By Technology Type (incl. RDC, VPN, SSH/SCP, Terminal Services and Citrix)	●			●			●	●	●
Protocol									
TCP/UDP/ICMP	●	●	●	●	●	●	●	●	●
Raw Ethernet		●	●	●		●	●	●	●

Other	128 protocols supported			IPv6-ICMP, IGMP, GRE, ESP, SMP	IGMP, GGP, GUP, IDP, GRE	IM, Jabber, HTTPS			
Which Actions can be taken when a firewall rule is triggered?									
Allow / Block traffic	●	●	●	●	●	●	●	●	●
Ask / notify the end-user when traffic is blocked	●	●	●	●	●	●	●	●	
Log									
Log the incident	●		●	●	●	●	●	●	●
Include packet data in log				●			●	●	●
End-user Interaction									
Can end-users be allowed to create firewall rules?		●	●	●	●	●	●	●	●
Can the administrator define rules that can not be overridden by end-user rules?	●	●	●	●	●	●	●	●	●
Can the administrator define rules that can be overridden by end-user rules?		●		●		●	●	●	
Can the end-user be allowed to disable the firewall?		●	●	●	●	●	●	●	●
Can the firewall automatically be enabled after a defined time?		●		●		●	●	●	
Can the end-user easily block all network traffic?		●	●	●		●	●	●	
Can the end-user be allowed to see the network traffic in real time?	●	●	●	●	●	●		●	
Can the firewall rules be exported and imported?		●		●	●	●	●	●	●
Firewall Logs									
Which logs are provided?	App. Blocked and allowed with the reason (automatically because of MD5, publisher, or due game mode), port scan, Service started, stopped, FW enabled, disabled		Application blocked/allowed, Port blocked/allowed, Network blocked/allowed	Critical warnings, Errors, Warnings, Informative records and/or Diagnostic records. For troubleshooting, all blocked connections can be logged.		Network attacks, Banned hosts, Application activity, Packet filtering		Traffic Logs, Packet Logs, Control Logs, Security Logs, System Logs, Tamper Protection Logs, Threat Logs, Scan Log, Risk Log	
Client Management									
Client User Interface									
Can the administrator limit or control configuration changes by the end-user?	●	●	●	●	●	●	●	●	●
Can different policies be applied for different computers?	●	●	●	●	●	●	●	●	●
Depending on the location of the device (i.e. Office, Hotel, Home, etc)	●		●		●	●		●	●
Depending on group membership of the computer	●	●	●	●	●	●	●	●	●
Depending on group membership of the user (i.e. administrator vs. normal user)		●	●			●	●		●
Actions									
Which actions can be initiated in administration console?									
Update signatures	●	●	●	●	●	●	●	●	●
Reboot computer		●		●		●		●	
Scan computer	●	●	●	●	●	●	●	●	●
Enable/Disable On-Access Scan	●	●	●	●	●	●	●	●	●
Enable/Disable Firewall	●	●	●	●	●	●	●	●	●

Other	Activate/Deactivate MailGuard , WebGuard	Change all configuration available in the client, migrate client to another server, modify the communication interval		Change all aspects of configuration, including handing off a client to another server	mail scan on/off/software update				connection verification, uninstallation, outbreak prevention, configuration changes
On which systems can the actions be initiated?									
A single computer / a group of computers	●	●	●	●	●	●	●	●	●
All computers matching certain criteria (i.e. identified by logs or reports)	●			●		●	●	●	●
Other		Computers with a specific user logged on (policies per user)	Any Task can be assigned for a set of computers			Any Task can be assigned for a set of computers			
Can the status of the actions be tracked?	●	●		●		●	●	●	●
Is there a web based console?			●		●	●	●	●	●
Administrator Management									
Rights / Access Control									
Does the product support multiple administrators and different access levels?	●		●	●	●	●	●	●	●
Authentication mechanism									
Can administrators be authenticated using an integrated authentication mechanism (i.e. username / password)?	●	●	●	●	●	●	●	●	●
Does the product enforce minimum password lengths and maximum password age?								●	●
Can administrators be authenticated using Active Directory?			●	●		●	●	●	●
Can administrators be authenticated using RSA Secure ID technology?								●	●
Other					Administrator account, integrated login		certificate		
Account Security									
Does the product lock an administrator account when a wrong password is provided multiple times (prevent brute force attacks) and can it be unlocked automatically after some time or manually by the administrator?								●	
Does the product log an administrator out after being idle for some time?						●	●	●	●
Administrator Auditing									
Does the product keep an audit log?			●	●		●	●	●	●
Which changes are logged?									
Log-in / Log-out	●		●	●		●	●	●	
Changes to policies				●	●	●	●	●	
Changes to system settings				●		●	●	●	●
Changes to groups				●		●	●	●	
Change to administrative accounts						●	●	●	●
Which information is logged									
Time of change	●		●	●	●	●	●	●	●
The administrator who performed the action			●	●		●	●	●	
The action that was performed				●	●	●	●	●	●
Device Control									

Does the product allow administrators to limit the use of external devices (USB sticks, printers, etc)?		●	●	●	●	●	●	●	●
Can the product identify devices by									
Device ID			●	●	●	●	●	●	●
Manufacturer ID / Unique ID					●	●	●	●	
Can you exclude e.g. printer USB Ports from being scanned			●	●		●	●	●	●
Can you lock									
DVD / USB / external media		●	●	●	●	●	●	●	●
Floppy		●		●	●	●	●	●	●
other			Bluetooth/Card Readers	All ports and all removable media can be locked, but it's possible to add exceptions for any individual ports or media	webcams				network ressources
(N)IPS									
Can the product prevent computers from receiving NetBIOS traffic originating from a different subnet?				●			●	●	
Prevent MAC spoofing by allowing incoming and outgoing ARP traffic only if ARP request was made to that specific host							●	●	
Detect ports cans	●			●		●	●	●	
Does the product detect and prevent denial of service attacks?				●		●	●	●	●
Does the product provide a signature based network intrusion prevention systems?	●			●		●	●	●	●
Can a customer create custom IPS signatures?							●	●	
Does the product include attack and vulnerability facing signatures?	●			●		●	●	●	●
Which actions can be performed?									
Traffic can be allowed / blocked / dropped			●	●		●	●	●	●
Incident can be logged	●		●	●		●	●	●	●
Failover									
What if the AV Server (local) hangs up									
automatic switching to a second local server		●		●	●	●	●	●	
updates from vendor-server instead of local server	●	●		●	●	●	●	●	●
other				Log and notifications		any other network shared folder			
Quarantine									
Quarantine Folder									
Is there a centralized quarantine-folder				●	●	●		●	●
Is there a quarantine-folder on the client	●	●	●	●	●	●	●	●	●
can administrators specify the location of the quarantine folder anywhere	●	●	●	●		●	●	●	●
rechecking quarantine									
after an signature update, is the quarantine folder checked?		●		●		●		●	
automatically				●		●		●	

manual	●	●				●	●	●	
undo av-action if false positive is detected	●			●		●	●	●	
Messaging									
Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange
Feature overview Messaging									
Modules and functional areas		Monitoring, SMTP Groups, Antivirus, Anti-Spam, Content filtering, Attachment filtering, Update	The Exchange module is full integrated with MS Exchange server, scans the complete Exchange internal database and can be Managed from the MailScan Management Console. Supports both 32 bit and 64-bit systems.	Product for Exchange. Full integration with MS Exchange, scans the whole Exchange store and Anti-Spam Protection. Manageable from the central management server. Supports 64-bit Exchange.	Exchange Plugin			Integrated option with MS Exchange and Domino. Secure email gateway option (virtual or physical appliance) for Enterprise Edition. Anti-Spam, antivirus, antiphishing, content filtering, and data loss prevention	antimalware, antispam, content filtering, attachment blocking, URL filtering, DLP
Malware detection									
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled	●	●	●	●	●	●		●	●
Information Store scan on every server	●	●	●	●	●	●	●	●	●
Support of automatic virus pattern updates	●	●	●	●	●	●	●	●	●
Scanning of e-mail message text and attachments	●	●	●	●	●	●	●	●	●
Detecting file attachments by means of clear, non-manipulable file patterns or by file type, detects and blocks even manipulated files	●	●	●	●	●		●	●	●
Definition of file limitations by a combination of file name, file extension and file size	●	●		●	●		●	●	●
Application of the restrictions on file archives	●	●	●	●	●		●	●	●
Automatic detection of new mailboxes		●	●	●	●	●	●	●	●
Scanning of existing mailboxes	●	●	●	●	●	●	●	●	●
Anti-Spam									
scan according to the company's policies on prohibited, not desirable or confidential content	●	●		●			●	●	●
Blocking unwanted e-mail senders (spam senders, mailing lists, etc.) as well as to unwanted recipients (e.g. competitors)	●	●	●	●		●	●	●	●
Analysis of images on undesirable content (e.g. pornography)		●	●			●			
Using current spam pattern for the fast detection of new spammer tricks	●	●	●	●		●	●	●	●
User-Specific Management of White- and blacklists on the server solely for effective blocking unwanted e-mails	●	●	●	●		●	●	●	●
Definition of transmitter / receiver channels on a dedicated e-mail communications				●					
Freely editable exclusion list for addresses and content in subject and message text	●	●	●	●		●	●	●	●
Flexible notifications of blocked e-mails (directly or schedule) to administration or transmitter/receiver email	●	●	●	●		●	●	●	●
User-specific access to e-mails in the quarantine	●		●	●			●	●	●
Centralized quarantine management	●	●	●	●	●	●	●	●	●
Formation of company-specific e-mail categories	●			●			●	●	

Automatic classification of e-mails to one or more categories	●	●		●			●	●	
Response Management through defined classifications, for example, the customer support automatic forwarding of e-mails to qualified employees	●	●	●	●			●	●	
Document protection: Following categories may, for example, all outgoing e-mails on company-related content should be examined							●	●	●
A content audit of e-mail attachments is also possible				●			●	●	●
if the same mail is delivered several times, would it be blocked as spam				●					
Feature overview Messaging	General Windows	General Windows	General Windows	General Windows	General Windows	General Windows	General Windows	General Windows	General Windows
Modules and functional areas			Available in more than 32 flavours covering both Linux and Windows based Mail Servers	Integration with most Windows mail servers is possible through the command line scanner	Gateway Solution	Kaspersky Endpoint Security 8 for Windows (POP3/SMTP/NNTP/IMAP traffic check)		Integrated option with MS Exchange and Domino. Secure email gateway option (virtual or physical appliance) for Enterprise Edition. Anti-Spam, antivirus, antiphishing, content filtering, and data loss prevention	
Malware detection									
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled		●	●	●	●	●	●	●	●
Information Store scan on every server	●			●			●	●	●
Support of automatic virus pattern updates	●	●	●	●	●	●	●	●	●
Scanning of e-mail message text and attachments	●	●	●	●	●	●	●	●	●
Detecting file attachments by means of clear, non-manipulable file patterns or by file type, detects and blocks even manipulated files		●			●		●	●	●
Definition of file limitations by a combination of file name, file extension and file size		●		●		●	●	●	●
Application of the restrictions on file archives such as zip, rar		●	●	●	●	●	●	●	●
Automatic detection of new mailboxes				●	●		●	●	
Examination of encrypted e-mails for viruses in combination with Crypt					●				
Scanning of existing mailboxes			●	●			●	●	●
Anti-Spam									
scan according to the company's policies on prohibited, not desirable or confidential content	●	●					●	●	●
Blocking unwanted e-mail senders (spam senders, mailing lists, etc.) as well as to unwanted recipients (e.g. competitors)	●	●	●	●	●		●	●	●
Analysis of images on undesirable content (e.g. pornography)		●	●						●
Using current spam pattern for the fast detection of new spammer tricks.	●	●	●		●			●	●
User-Specific Management of White-and blacklists on the server solely for effective blocking unwanted e-mails.	●	●	●	●	●		●	●	●
Freely editable exclusion list for addresses and content in subject and message text	●	●	●	●				●	●
Flexible notifications of blocked e-mails (directly or schedule) to administration or transmitter/receiver email		●	●		●		●	●	●

User-specific access to e-mails in the quarantine	●		●	●			●	●	●
Centralized quarantine management	●	●		●			●	●	●
Formation of company-specific e-mail categories							●	●	●
Automatic classification of e-mails to one or more categories		●					●	●	
Response Management through defined classifications, for example, the customer support automatic forwarding of e-mails to qualified employees		●						●	●
Document protection: Following categories may, for example, all outgoing e-mails on company-related content should be examined		●						●	●
A content audit of e-mail attachments is also possible		●		●				●	●
if the same mail is delivered several times, would it be blocked as spam				●	●				
Feature overview Messaging	General Linux	General Linux	General Linux	General Linux	General Linux	General Linux	General Linux	General Linux	General Linux
Modules and functional areas		Security for Linux mail servers with web administration interface. Manageable from the central management console.	Products eScan for Linux WorkStation, eScan for Linux File Server (Samba) , MailScan For Linux Mail Servers , WebScan for Linux Proxy Servers	Special product for Linux Mail Servers and Gateways. Includes Anti-Spam, web administration interface. Manageable from the central management console.	Gateway Solution	Special product for Linux mail servers. Includes Antispam, web administration interface. Managable from the central management console.		Integrated option with MS Exchange and Domino. Secure email gateway option (virtual or physical appliance) for Enterprise Edition. Anti-Spam, antivirus, antiphishing, content filtering, and data loss prevention	
Malware detection									
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled.		●	●	●	●	●	●	●	●
Information Store scan on every server.				●		●	●	●	
Support of automatic virus pattern updates.		●	●	●	●	●	●	●	●
Scanning of e-mail message text and attachments.		●	●	●	●	●	●	●	●
Detecting file attachments by means of clear, non-manipulable file patterns ("fingerprints") or by file type, detects and blocks even manipulated files.		●	●	●	●	●	●	●	●
Definition of file limitations by a combination of file name, file extension and file size.		●		●		●	●	●	●
Application of the restrictions on file archives such as zip, rar.		●	●	●	●	●	●	●	●
Automatic detection of new mailboxes.		●		●	●	●	●	●	
Scanning of existing mailboxes		●				●	●	●	●
Anti-Spam									
scan according to the company's policies on prohibited, not desirable or confidential content		●	●				●	●	●
Blocking unwanted e-mail senders (spam senders, mailing lists, etc.) as well as to unwanted recipients (e.g. competitors)		●	●	●	●	YES to blocking unwanted senders, NO to blocking unwanted recipients	●	●	●
Analysis of images on undesirable content (e.g. pornography)		●							●
Using current spam pattern for the fast detection of new spammer tricks		●		●	●	●		●	●
User-Specific Management of White- and blacklists on the server solely for effective blocking unwanted e-mails		●	●	●	●	●	●	●	●

Freely editable exclusion list for addresses and content in subject and message text		●	●	●		●		●	●
Flexible notifications of blocked e-mails (directly or schedule) to administration or transmitter/receiver email		●			●		●	●	●
User-specific access to e-mails in the quarantine.		●					●	●	●
Centralized quarantine management		●	●				●	●	●
Formation of company-specific e-mail categories							●	●	●
Automatic classification of e-mails to one or more categories		●					●	●	
Response Management through defined classifications, for example, the customer support automatic forwarding of e-mails to qualified employees		●						●	●
Document protection: Following categories may, for example, all outgoing e-mails on company-related content should be examined		●						●	●
A content audit of e-mail attachments is also possible		●						●	●
if the same mail is delivered several times, would it be blocked as spam					●				●
Language:									
In which languages are your corporate products available?	German, English, French, Spanish, Portuguese, Italian, Russian, Chinese, Japanese, Korean	English, German, French, Spanish, Polish, Romanian, Russian	English, German, French, Dutch, Italian, Portuguese, Spanish, Turkish, Chinese Simplified, Chinese Traditional, Greek, Korean, Norwegian, Russian, Polish, Latin Spanish, Croatian, Estonian	English, Japanese, German, Russian, French, Spanish, Spanish Latin, Polish, Chinese Simplified, Chinese Traditional, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French Canadian, Hungarian, Italian, Japanese, Kazakh, Korean, Norwegian, Polish, Portuguese Brazilian, Romanian, Serbian Latin, Slovak, Slovenian, Swedish, Thai, Turkish, Ukrainian	German, English, French, Italian, Spanish, Russian, Brazilian, Turkish, Polish, Japanese	English, French, German, Japanese, Russian, Simplified Chinese, Italian, Portuguese, Spanish, Brazilian Portuguese, Latham Spanish, Turkish, Arabic, Kazakh, Lithuanian, Polish, Korean, Thai, Vietnamese, Romanian	English, German, Spanish, French, Italian, Japanese, Korean, Dutch, Polish, Brazilian Portuguese, Russian, Swedish, Chinese Simplified, Chinese Traditional	English, Simplified Chinese, Traditional Chinese, Korean, French, Italian, German, Spanish, Brazilian, Russian, Czech, Polish, Japanese	English, German, French, Italian, Spanish, Polish, Russian, Turkish, Traditional Chinese, Simplified Chinese, Japanese
In which languages are your (help) manuals available?	German, English, French, Spanish, Portuguese, Italian, Russian, Chinese simplified, Chinese traditional, Japanese, Korean	English, German, French, Spanish, Polish, Romanian, Russian	English	English, Japanese, German, Russian, French, Spanish, Spanish Latin, Polish, Chinese Simplified, Chinese Traditional, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French Canadian, Hungarian, Italian, Japanese, Kazakh, Korean, Norwegian, Polish, Portuguese Brazilian, Romanian, Serbian Latin, Slovak, Slovenian, Swedish, Thai, Turkish, Ukrainian	German, English, French, Italian, Spanish, Russian, Brazilian, Turkish, Polish, Japanese	English, Russian, French, German, Italian, Japanese, Polish, Portuguese, Spanish	English, German, Spanish, French, Italian, Japanese, Korean, Dutch, Polish, Brazilian Portuguese, Russian, Swedish, Chinese Simplified, Chinese Traditional	English, Simplified Chinese, Traditional Chinese, Korean, French, Italian, German, Spanish, Brazilian, Russian, Czech, Polish, Japanese	English, German, French, Italian, Spanish, Polish, Russian, Turkish, Traditional Chinese, Simplified Chinese, Japanese
Support									
24/7/365 phone support	only for SLA customers		only for SLA customers	only for SLA customers	●	only for SLA customers	●	●	only for premium service
Dial Rates	Depends on location	Depends on location	Depends on location	Toll Free Numbers are available in most countries	Depends on location	Depends on location	Toll Free Numbers are available in most countries	Toll Free Numbers are available in most countries	Toll Free Numbers are available in most countries

Supported Support Languages	German, English, French, Spanish, Portuguese, Italian, Russian, Chinese, Japanese, Korean	English, German, Spanish, Romanian, French and other languages by local partners	English, German and other languages by local partners	English, Slovak, Czech and other languages by local partners	German, English, French, Italian, Spanish	English and other languages by local partners	English and other languages by local partners	English, French, German, Italian, Spanish, Portuguese Brazil, Czech, Polish, Russian, Chinese Simplified, Chinese Traditional, Korean, Japanese, Taiwanese	English, German, French, Italian, Spanish, Polish, Russian, Turkish, Traditional Chinese, Simplified Chinese, Japanese
Remote Desktop Control for support	●	●	●	●	●	●	●	●	●
Support per Forum	●	●	●	●		●	●	●	●
Support over Email	●	●	●	●	●	●	●	●	●
Guaranteed E-Mail response within	depends on priority	Guaranteed response for Premier business support is within 2 hours	Guaranteed response for Gold Partners is within 1 hour	Guaranteed response for Premium business support is within 1 hour	depends on priority	depends on priority	depends on priority	Response times are only guaranteed for phone support and it depends on priority.	depends on priority
On-Site service?	●	Romania. For other regions the on-site service is based upon issue severity	●	●	●	●	●	●	●
Service									
Managed by Vendor, this means, can the whole management process be done as a service by the vendor?			●	Possible by reseller	Possible by reseller	●	●	●	Possible by reseller
Why should users choose your product and not another?	Best detection, fast product, 20 years of experience and continuity, Proven protection	BitDefender combines antimalware protection with remote audit and system management, allowing network administrators to gain an additional layer of visibility and protection to help them identify and eliminate gaps within their network. BitDefender's very high detection with very few false positives received the highest possible ADVANCED+ award.	eScan offers robust real time scanning of local and network transactions. Strong Endpoint security features.	ESET security solutions offer the best overall performance, while placing minimal demands on system resources. ESET ranked first in an independent review by PassMark Software and was recognized for the "fastest, best overall performance." ESET is also the unmatched leader in proactive protection – the holder of the highest number of ADVANCED+ awards by AV-Comparatives in Proactive/Retrospective tests. Centralized management of ESET security solutions in a networked environment is easy and effective and fits organizations of all sizes.	G Data security solutions offer the highest malware-detection by using the G Data DoubleScan technology. The G Data concept of easy administration saves time and money - long term trainings are not any more necessary.	Our product was designed with large enterprise corporate networks in mind. We do have multiple enterprise customers with 50K+ who have chosen our system due to its flexibility and manageability. We do support server hierarchy with unlimited nesting. The same is also applicable to user groups. We strongly believe that in large corporate networks the only way to eliminate chaos is through properly designed structure of user groups.	McAfee Endpoint Protection provides continuous, updated, and powerful security against the entire spectrum of threats, from zero-day exploits to hacker attacks. As a core component of our Security Connected framework, we provide complete protection for all endpoints, including the latest mobile devices and virtualized environments, ensuring secure, seamless access to business applications and corporate data. We unify endpoint security and management with McAfee ePolicy Orchestrator (ePO), our web-based management console that enhances efficiency, reduces costs, and helps maintain and prove compliance.	Symantec Endpoint Protection is the fastest and most powerful endpoint protection solution in its class.	WFBS is a safer, smarter, and simpler one-stop security solution. Using a strategy of cloud-server-client protection, it provides up-to-the-minute proactive security for your whole network, both PCs and Macs, both stationary and mobile, without overburdening end-user's computers.
Pricing									
Scenario A: 5 clients, server, outlook as mail client									
recommended product	Avira Small Business Suite	BitDefender Internet Security 2010 + BitDefender Security for File Servers for 5 users	eScan ISS SMB	ESET Smart Security	G Data AntiVirus MultiUser	Kaspersky Small Office Security	McAfee SaaS Endpoint (incl. 24x7 Support)	Symantec Endpoint Protection Cloud	Worry-Free Business Security - Service
1 year Euro	353	167	146	187	74	208	196	162	126
3 years Euro	706	360	285	392	195	625	343	389	321

1 year USD	521	205	166	198	95	209	210	175	158
3 years USD	1043	440	324	396	250	418	367	419	402
Scenario B SMB: 1 SBS 2003 Server, 25 Clients									
recommended product	Avira NetWork Bundle	BitDefender Small Office Security Suite	eScan for SBS	ESET Smart Security Client + File Server Security	G Data AntiVirus Enterprise	Kaspersky Business Space Security	McAfee SaaS Endpoint & Email Protection Suite (incl. 24x7 Support)	Symantec Endpoint Protection Small Business Edition	Worry-Free Business Security - Service
1 year plan EURO	1088	789	652	680	1045	716	1610	300	592
3 year plan EURO	1830	1578	1270	1.429	2122	1610	3170	692	1511
1 year plan USD	1607	963	740	931	1340	780	1,509	316	741
3 year plan USD	3214	1925	1444	1.862	2722	1560	3,169	991	1889
Scenario C: 1 Fileserver, 1 Exchange server, 200 Clients									
recommended product	Avira Business Bundle	BitDefender SBS Security Suite	eScan Enterprise	ESET NOD32 Antivirus + ESET File Server Security + ESET Mail Server Security	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	McAfee Endpoint Protection Suite (incl. 24x7 Support)	Symantec Protection Suite Enterprise Edition	Worry-Free Business Security - Advanced
1 year plan EURO	9067	6880	4,882	4.910	5575	5166	6738	7,852	9,600
3 year plan EURO	18135	13760	9,518	10.311	11878	11622	11861	15,704	12,500
1 year plan USD	13390	8390	5,546	6.380	7152	6210	8,005	9,460	11,982
3 year plan USD	26780	16780	10,816	12.760	15238	12400	14,089	20,666	17,341
Scenario D, 2 Fileserver, 1 Exchange server, 1000 Clients									
recommended product	Avira Business Bundle	BitDefender SBS Security Suite	eScan Enterprise	ESET NOD32 Antivirus + ESET File Server Security + ESET Mail Server Security	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	McAfee Endpoint Protection Suite (incl. 24x7 Support)	Symantec Protection Suite Enterprise Edition	Enterprise Security for Endpoints and Mail Servers
1 year plan EURO	32011	27060	15536	16.020	19258	18647	28545	29,950	24,890
3 year plan EURO	64022	54120	30300	33.662	39719	41954	50240	65,440	44,805
1 year plan USD	47280	33000	17662	20.932	24706	25351	32,939	33,460	31,113
3 year plan USD	94560	66000	34432	41.864	50955	50601	57,973	67,620	56,007
Scenario E: 10 Fileserver, 10 Exchange server, 10000 Clients									
recommended product	Avira Business Bundle	BitDefender SBS Security Suite	eScan Enterprise	ESET NOD32 Antivirus + ESET File Server Security + ESET Mail Server Security	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	McAfee Endpoint Protection Suite (incl. 24x7 Support)	Symantec Protection Suite Enterprise Edition	Enterprise Security for Endpoints and Mail Servers
1 year plan EURO	320110	270600	155210	117.100	192384	134930	162224	239,000	191,421
3 year plan EURO	742440	541200	302704	245.310	396792	303500	285470	522,200	344,752
1 year plan USD	470750	330000	176452	152.120	246809	207200	187,174	267,100	239,277
3 year plan USD	1000000	660000	343986	304.240	509044	476450	329,357	583,400	430,659

All prices are MSRP (Manufactured Suggested Retail Price) as of Summer 2011 Actual retail prices may differ considerably esp. for scenarios D and E, as for large projects many factors and savings may apply. Please contact the vendors for actual project prices. The here listed prices are just a rough estimation. We do not take any responsibility for the info provided in the above table, as this information was mainly provided by the vendors.
The information is based on the products which were available at the time of the review.

	AVIRA	AVIRA	AVIRA	Bitdefender	Bitdefender	Bitdefender	eScan	eScan	eScan	ESET	ESET	ESET	G Data	G Data	G Data	Kaspersky	Kaspersky	Kaspersky	McAfee	McAfee	McAfee	Symantec	Symantec	Symantec	Trend Micro	Trend Micro	Trend Micro
Supported Operating Systems	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client
Apple																											
Mac OS																				●	●			●			
Mac OS X												●								●	●			●			●
Mac OS X Server																								●			●
iPhone OS / iPod OS																					●						
Windows 2000																											
Professional / Server / Advanded Server				●	●	●	●	●	●	●	●	●			●	●	●	●		●	●			●			
Advanced Server 64 Bit Intel				●	●	●				●	●	●								●	●			●			
Advanced Server 64 Bit Itanium																				●	●			●			
Data Center Server				●	●	●				●	●	●			●					●	●			●			
Data Center Server 64 Bit Intel				●	●	●				●	●	●								●	●			●			
Data Center Server 64 Bit Itanium																				●	●			●			
Windows XP																											
Home		●	●			●		●	●	●	●	●	●	●	●		●	●		●	●	●	●	●		●	●
Professional		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●		●	●
Media Center / Tablet PC Edition										●	●	●	●	●	●					●	●			●		●	●
Embedded									●	●	●	●	●	●	●			●		●	●			●		●	●
Windows Server 2003																											
Standard / Enterprise / Data Center	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Small Business Server				●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	
Cluster Server / Storage Server				●	●	●				●	●	●	●	●	●				●	●	●	●	●	●	●	●	●
Web Edition				●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	
R2 Standard / Enterprise	●	●					●	●	●	●	●	●				●	●	●	●	●	●	●	●	●	●	●	●
Windows Vista																											
Home Basic / Home Premium		●	●			●	●	●	●	●	●	●	●	●	●	●	●	●		●	●		●	●		●	●
Business / Enterprise / Ultimate		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●		●	●		●	●
Windows 7																											
Starter Edition		●	●			●				●	●	●	●	●	●					●			●	●			
Home Premium		●	●			●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●		●	●
Professional / Ultimate / Enterprise		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●		●	●
Windows Server 2008																											
Standard	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Standard - Core installation	●	●								●	●	●				●		●	●	●	●			●			
Enterprise	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Server R2 (Standard/Enterprise)	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Data Center / Web Edition	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Foundation				●	●	●				●	●	●	●	●	●				●	●	●	●	●	●			
HPC				●	●	●				●	●	●	●	●	●				●	●	●			●	●	●	●
Windows Mobile																											
Windows Mobile 5.0 / 6.0 / 6.1												●						●			●						●
Windows Mobile 6.5												●									●						●
Works for Citrix										●	●	●	●	●	●			●	●	●	●				●	●	●
Symbian																											
OS 9.0 / 9.1 / 9.3																		●									●
Series 60												●						●			●						●
Linux																											
Redhat																											
Redhat Enterprise Linux 3.x 32 Bit						●		●	●			●					●	●						●			
Redhat Enterprise Linux 3.x 64 Bit						●		●	●			●															
Redhat Enterprise Linux 4.x 32 Bit			●			●		●	●			●					●	●			●			●			
Redhat Enterprise Linux 4.x 64 Bit			●			●		●	●			●									●			●			
Redhat Enterprise Linux 5.x 32 Bit			●			●		●	●			●			●		●	●			●			●			
Redhat Enterprise Linux 5.x 64 Bit			●			●		●	●			●			●		●	●			●			●			
SUSE																											
SUSE Linux Enterprise Desktop 9.x 32 Bit			●			●		●	●			●									●						
SUSE Linux Enterprise Server 9.x 32 Bit						●		●	●			●					●	●			●			●			
SUSE Linux Enterprise Desktop 9.x 64 Bit			●			●		●	●			●					●				●						
SUSE Linux Enterprise Server 9.x 64 Bit						●		●	●			●					●	●			●			●			
SUSE Linux Enterprise Desktop 10.x 32 Bit			●			●			●			●			●						●			●			
SUSE Linux Enterprise Server 10.x 32 Bit						●		●	●			●			●		●	●			●			●			
SUSE Linux Enterprise Desktop 10.x 64 Bit			●			●			●			●									●			●			
SUSE Linux Enterprise Server 10.x 64 Bit						●		●	●			●					●	●			●			●			
Novell																											
Open Enterprise Server OES 32 Bit						●						●					●	●			●			●			
Open Enterprise Server OES 64 Bit						●						●									●						
Open Enterprise Server OES2 32 Bit						●						●					●	●			●			●			
Open Enterprise Server OES2 64 Bit						●						●									●			●			
VMware																											
ESX 2.5.x				●	●	●				●	●	●												●			
ESX 3.0.x				●	●	●	●	●	●	●	●	●				●	●	●	●					●			
ESX 4.0.x				●	●	●				●	●	●							●	●	●				●	●	●
Other supported OS						Solaris						DOS, Solaris, NetBSD, FreeBSD												Debian, Fedora, Solaris, Ubuntu			
Database																											
Does the product require a database	●			●			●			●			●	●		●			●			●			●		
For how many users/clients is the free database recommended				1000			5000						unlimited	unlimited		5000			5000			5000			20000		
Which database is included (i.e. Microsoft SQL, Sybase, MySQL, etc)				SQL Express			Microsoft SQL			Microsoft Access (jet database) engine			SQL Express	SQL Express		Microsoft SQL			SQL Express			Microsoft SQL			DB2		
Which additional databases are supported																											
Microsoft SQL Server																											
Microsoft SQL Server 2000							●						●	●		●						●					

Microsoft SQL Server 2005				●			●			●			●	●		●			●			●					
Microsoft SQL Server 2008				●			●						●	●		●			●			●					
Microsoft SQL Server 2008 R2				●									●	●					●			●					
Other	MS-Access, any ODBC database			SQL Express						MySQL, Oracle			SQL Azure	SQL Azure													
Email Server																											
Microsoft Exchange				●	●	●		●	●			●	●	●			●	●			●	●			●		
Domino								●	●			●	●	●			●	●			●	●			●		
Tobit												●	●	●								●			●		
Linux								●	●			●	●	●			●	●				●			●		
Mac													●	●			●	●				●			●		
Novell Netware Server												●						●				●			●		
Dell NAS												●										●			●		
Kerio												●										●			●		

table, as this information was mainly provided by the vendors.

Copyright and Disclaimer

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

AV-Comparatives e.V. (September 2011)