IT Security Products for Corporate Users

Review of IT Security Suites for Corporate Users, 2010

Language: English

October 2010

Last revision date: 11th November 2010

www.av-comparatives.org

Contents

Product Section

The Dangers of Malware

Most organizations are aware of the risks threatening their IT environment. Viruses, trojans, worms, exploits and many other threats represent a serious danger for the IT department. A collapse of the IT system could mean grave financial losses right up to insolvency for a company.

The IT departments of companies are conscious of this problem. Getting the best protection against these threats is the only issue. A simple file antivirus solution alone is totally inadequate, as there are too many threats from contaminated e-mails, exploits etc. What is required is a comprehensive suite that provides protection against all of these.

Functional Diversity

Because of the immense functional diversity of various antivirus suites and corporate products, it is becoming increasingly difficult for decision-makers in the IT sector to get a proper overview. Which product should one opt for and for which areas of protection?

During these tests our main focus has not been on malware detection rates, but on the products' handling and user-friendliness, and the scope of functionality. We have compiled the functional scope of various products in a detailed table. For malware detection rates of individual products please refer to the tests of our website: **http://www.av-comparatives.org**

Target Group

This report is aimed primarily at IT administrators in organizations of all sizes. In order to present an overview, we have depicted the installation procedure in detail. This gives administrators an idea of what the program is like to use. However, this only represents the current state, since software products are subject to ongoing development and are updated frequently.

Hardware and Software

Organizations seldom use the latest hardware available in the market. Based on a survey conducted of 50 organizations of various sizes, which we carried out in the run-up to the tests, the hardware that we used is representative of equipment currently deployed.

The selection intentionally included the somewhat older configurations in order to reflect the real status of the IT environment in various organizations.

Server Configuration

CPU:	Dual-Core Xeon
RAM:	8 GB RAM
Hard disk:	2 x 160 GB (Raid 1, Sysvol), SAS
Hard disk:	2 x 500 GB (Raid 1, Datvol), SAS
OS:	Windows Server 2008 64-bit Std. incl. Service Packs and Security Updates current as of July 2010
Server Role:	Domain controller including Exchange 2007 SP1. DNS including forwarders.

Client Configuration

CPU:	Intel Dual Core, 3 GHz
RAM:	4 GB RAM
Hard disk:	80 GB, SATA
OS:	Windows 7 Business, Security Updates current as of July 2010

Management Summary

This year, the participants were AVIRA, BITDEFENDER, ESET, G DATA, KASPERSKY, MCAFEE, SOPHOS and TREND MICRO. Of these, MCAFEE, BITDEFENDER and TREND MICRO are new to the review, having not been covered last year.

Both MCAFEE and SOPHOS impressed us with installers that do everything with a single click. The installation of these products was particularly simple, as was the configuration.

With ESET we noticed the ease of administration of the clients. This works well and enables administrators of extremely large networks to find their way around and configure the systems easily. However, it should be noted that while installing ESET it is necessary to consult the manual. But reading the manual should be done for every installation.

In the case of AVIRA, we observed that the manufacturers have revised the design of the suite and incorporated our suggestions into the product. The configuration and integration of the client PCs are both carried out using wizards. It is good to see a manufacturer responding to the wishes of its customers.

BITDEFENDER, KASPERSKY and G DATA stay with their respective existing proven interfaces.

The TREND MICRO product is new to our corporate reviews. During the tests, an update was delivered that is now generally available. We were particularly impressed with the management console, which manages to make a huge amount of information available to the administrator in a clear and simple manner.

Considering the products reviewed last year, it can be seen that the manufacturers have stayed with proven technology. The plus points of the previous version have been kept, and administrators will immediately find their way around the new software.

You can find the prices in the feature list. However, we take the view that price should be a minor consideration, and security should always be the top priority.

A new trend was observed among the manufacturers this year. The licence models are becoming ever more granular, rather than simpler, and the tendency is towards individual products rather than pre-configured complete packages. We do not understand why the manufacturers are going in this direction, as we believe it would be easier for customers to choose all-in-one packages that give them the protection they need.

For each individual product, it can be difficult to decide exactly which version and which features are needed. Advice from an expert, either a representative of the manufacturers, or an independent IT security consultant, is invaluable.

Unfortunately, none of the manufacturers has made any progress with the development of real-time reporting. In all cases, the software still leaves the administrator in the dark as to the progress of individual actions.

It must be noted that there are still major differences between the suites in terms of functionality, ease of use and installation. It is therefore particularly important when purchasing corporate security suites to consider the particular requirements of one's own network and staff. However, all the products in this review are sufficiently well-designed and effective in protecting the network that they can be recommended without reservation.

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.

AV comparatives APPROVED Corporate Product 2010

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	ESET	G DATA	Kaspersky	McAfee	Sophos	Trend Micro
Ease of Installation	★★★★★	★★★★★	★★★★	★★★★★	★★★★	★★★★★	★★★★★	★★★
Deployment on Client PCs	★★★★	★★★★	★★★	★★★★	★★★★★	★★★★★	★★★★★	★★★★
Usability and Management	★★★★	★★★★★	★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Default Values	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★
Small Business	★★★★★	★★★★	★★★	★★★★★	★★★★	★★★★★	★★★★	★★★★
Medium Business	★★★★★	★★★★	★★★★	★★★★★	★★★★	★★★★★	★★★★★	★★★★
Enterprise	★★★	★★★★	★★★★★	★★★★	★★★★	★★★★★	★★★★★	★★★★★
User Manual	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★	★★★★
MS AD Support	★★★★	★★★	★★★	★★★★	★★★★	★★★★	★★★★★	★★★★
Database Support	★★	★★★	★★★	★★	★★★★★	★★★★★	★★★★	★★
Website	★★★★	★★★★	★★★★★	★★★★	★★★★★	★★	★★★★	★★★
Spam	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Overall Assessment	★★★★	★★★★	★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★
Award	AV APPROVED Corporate Product comparatives 2010	AV APPROVED Corporate Product comparatives 2010	AV APPROVED Corporate Product comparatives 2010	AV APPROVED Corporate Product comparatives 2010	AV APPROVED Corporate Product comparatives 2010	AV APPROVED Corporate Product comparatives 2010	AV APPROVED Corporate Product comparatives 2010	AV APPROVED Corporate Product comparatives 2010

Tested Products

The following vendors participated in the tests and review:

AVIRA	**www.avira.com**
Bitdefender	**www.bitdefender.com**
ESET	**www.eset.com**
G DATA	**www.gdata.de**
Kaspersky	**www.kaspersky.com**
McAfee	**www.mcafee.com**
Sophos	**www.sophos.com**
Trend Micro	**www.trendmicro.com**

Spam Test

Spam is a very annoying issue, which can take up much work time and therefore cost money. Due to this, efficient spam filters are required. On the other hand, spam filters must not filter out any wanted mails (ham), as this could be problematic in business life.

The mails were filtered directly on the Exchange Server 2007 SP1. If there was no Exchange plug-in provided by the product, it was filtered on the client. We used Outlook 2010 (with its junk-mail filter disabled for testing purposes).

All settings on the tested products were left on DEFAULT WITHOUT TRAINING. In real world and by training the spam filters the filtering rates could be increased further.

For this SPAM-test, we took only SPAM mails which had been collected continuously and were not older than 3 weeks (about 3000 emails).

Results Spam Test

	Detected Spam	
AVIRA	➢ 99%	approved
Bitdefender	➢ 99%	approved
ESET	➢ 98%	approved
G DATA	➢ 98%	approved
Kaspersky	➢ 99%[1]	approved
McAfee	➢ 99%	approved
Sophos	➢ 97%	approved
Trend Micro	➢ 99%[2]	approved

Results Ham-Test

Very positive is the fact that **none** of the tested products **classified any wanted mail** (Ham-Mail) of our Ham-test set **as SPAM.**

The spam filters can be set at different levels, the administrator has to find the best selection for his/her own network. Whitelisting and blacklisting are also possible.

[1] Kaspersky: We have been asked to review the Kaspersky Security 8 for Exchange Server (Release Candidate), which will be available end of November 2010

[2] TrendMicro: If you use the MS-Exchange Server direct as an MX you can use Scan Mail for Exchange or Worry Free Business Security, if you use MS Exchange Server with a pop connector you should use Worry Free Business Security, because Scanmail without ip-reputation service would lead to significant lower spam detection.

Product Review Section

The products are reviewed in alphabetical order.

AVIRA

Tested Software:

AVIRA Antivir Server (Windows)	→	File Server Protection
AVIRA Antivir Exchange + Anti-Spam	→	Exchange Server Mail Protection
AVIRA Antivir Security Management Center	→	Centralised Control Console and Deployment
AVIRA AntiVir Professional	→	Client Virus Protection

Product Installation

Download

The layout of the manufacturer's website is simple and logical, and it is easy to find the product you're looking for. If you already have a key, you can download the setup files without further ado.

Registration is necessary to get a test licence. 30 days is long enough to test the product thoroughly. The registration details are forwarded to a certified Avira partner.

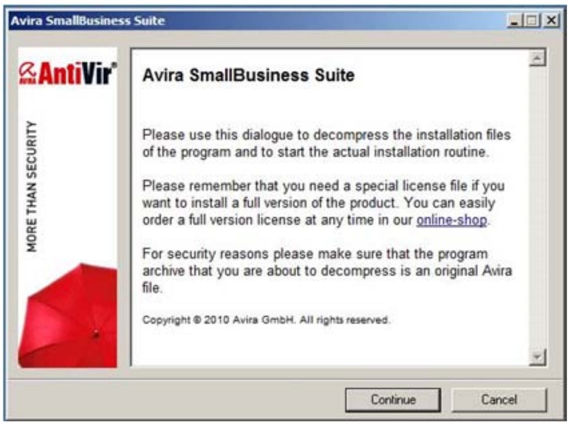
An improvement here is that the individual products of the suite no longer have to be downloaded separately, as there is now a Small Business Suite installer as a single item. This is very much better the previous version.

Another plus point is that the new Avira website provides a very well organized overview on the complete range of Avira business products (the SmallBusiness among them) which makes it very easy to compare the features of the different product offerings.

Installation

Avira has also worked hard on the installation process, and there is no longer any need to consult the SMB product handbook during basic setup.

The installation starts by decompressing the setup files:


Avira SmallBusiness Suite

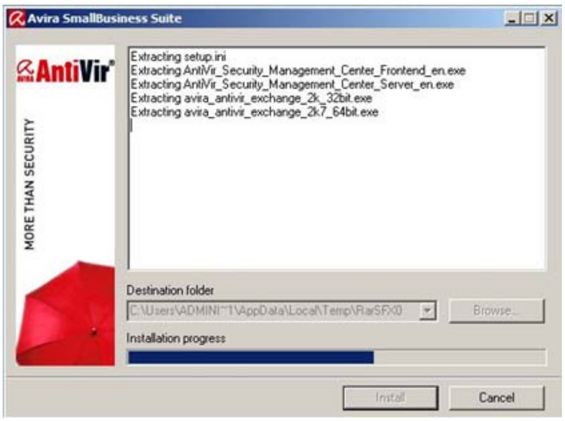
Avira SmallBusiness Suite

Please use this dialogue to decompress the installation files of the program and to start the actual installation routine.

Please remember that you need a special license file if you want to install a full version of the product. You can easily order a full version license at any time in our online-shop.

For security reasons please make sure that the program archive that you are about to decompress is an original Avira file.

Copyright © 2010 Avira GmbH. All rights reserved.

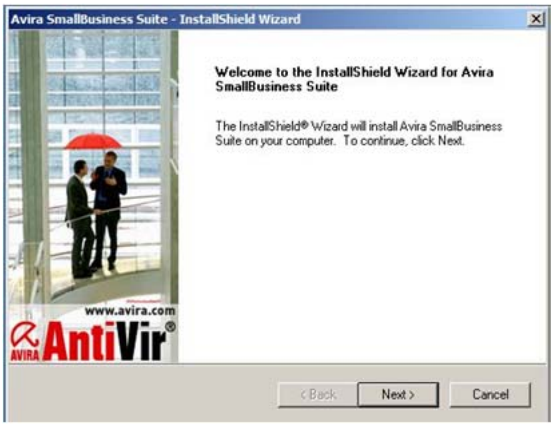

Avira SmallBusiness Suite

```
Extracting setup.ini
Extracting AntiVir_Security_Management_Center_Frontend_en.exe
Extracting AntiVir_Security_Management_Center_Server_en.exe
Extracting avira_antivir_exchange_2k_32bit.exe
Extracting avira_antivir_exchange_2k7_64bit.exe
```

Destination folder: C:\Users\ADMINI~1\AppData\Local\Temp\RarSFX0

Installation progress

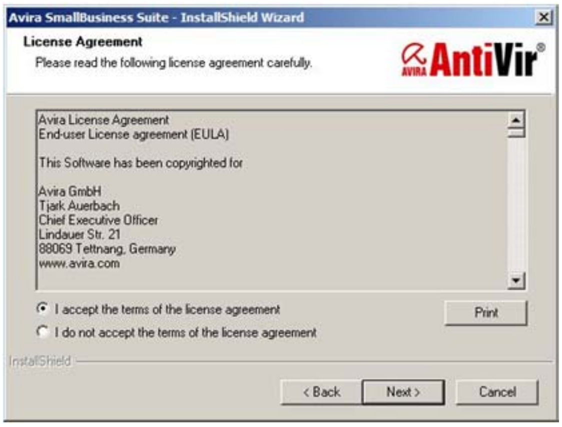
Once the installation files have been unpacked into a temporary folder, we are greeted by the Welcome page of the installer:


Avira SmallBusiness Suite - InstallShield Wizard

Welcome to the InstallShield Wizard for Avira SmallBusiness Suite

The InstallShield® Wizard will install Avira SmallBusiness Suite on your computer. To continue, click Next.

Next comes the obligatory licence agreement:



Avira SmallBusiness Suite - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

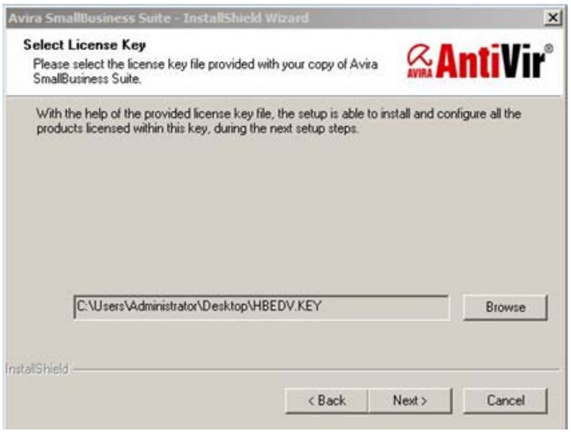
Avira License Agreement
End-user License agreement (EULA)

This Software has been copyrighted for

Avira GmbH
Tjark Auerbach
Chief Executive Officer
Lindauer Str. 21
88069 Tettnang, Germany
www.avira.com

● I accept the terms of the license agreement
○ I do not accept the terms of the license agreement

The licence key file obtained at registration then needs to be located:



Avira SmallBusiness Suite - InstallShield Wizard

Select License Key

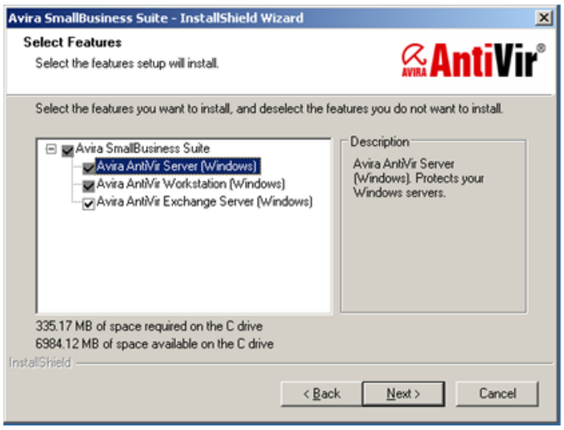
Please select the license key file provided with your copy of Avira SmallBusiness Suite.

With the help of the provided license key file, the setup is able to install and configure all the products licensed within this key, during the next setup steps.

C:\Users\Administrator\Desktop\HBEDV.KEY

The path to the installation folder can now be selected. We chose to install to the standard location:

The first step is the local installation of the products belonging to the Suite, i.e. the AntiVir Workstation, the AntiVir Server and (optionally) AntiVir Exchange:



Avira SmallBusiness Suite - InstallShield Wizard

Select Features

Select the features setup will install.

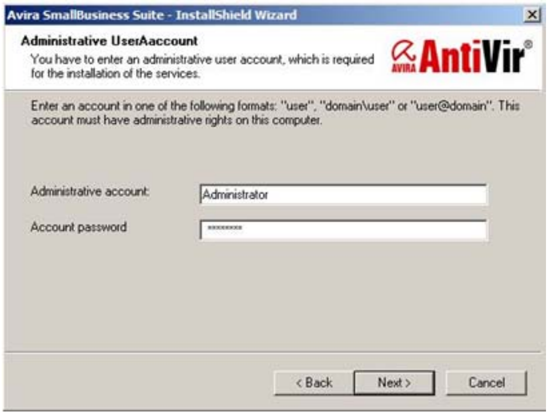
Select the features you want to install, and deselect the features you do not want to install.

☑ Avira SmallBusiness Suite
- ☑ Avira AntiVir Server (Windows)
- ☑ Avira AntiVir Workstation (Windows)
- ☑ Avira AntiVir Exchange Server (Windows)

Description
Avira AntiVir Server (Windows). Protects your Windows servers.

335.17 MB of space required on the C drive
6984.12 MB of space available on the C drive

The next step is to enter the credentials of a Windows user account with administrator privileges:



Avira SmallBusiness Suite - InstallShield Wizard

Administrative UserAaccount

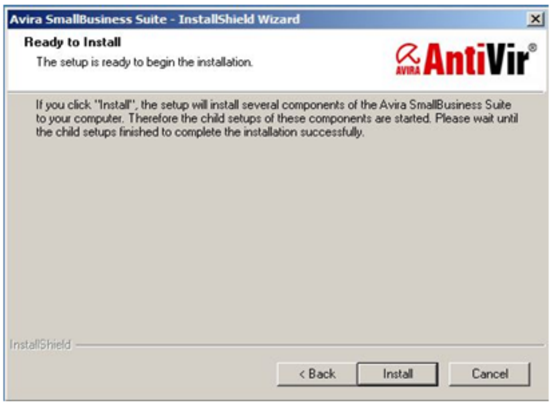
You have to enter an administrative user account, which is required for the installation of the services.

Enter an account in one of the following formats: "user", "domain\user" or "user@domain". This account must have administrative rights on this computer.

Administrative account: Administrator

Account password: ********

The installer now has the information it needs to begin:

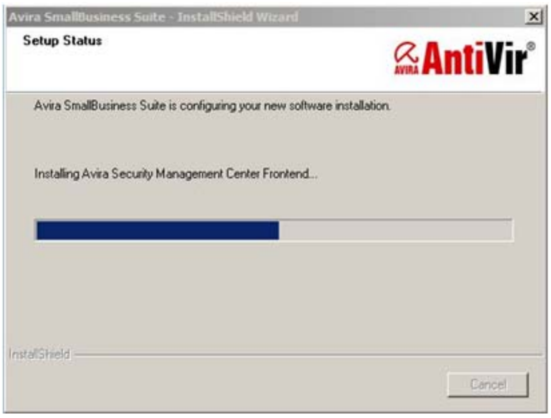


Avira SmallBusiness Suite - InstallShield Wizard

Ready to Install

The setup is ready to begin the installation.

If you click "Install", the setup will install several components of the Avira SmallBusiness Suite to your computer. Therefore the child setups of these components are started. Please wait until the child setups finished to complete the installation successfully.

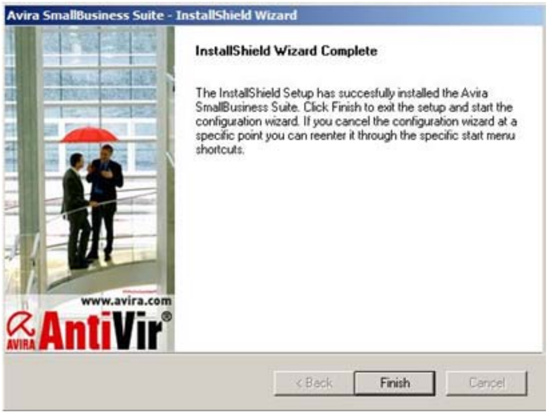


Avira SmallBusiness Suite - InstallShield Wizard

Setup Status

Avira SmallBusiness Suite is configuring your new software installation.

Installing Avira Security Management Center Frontend...

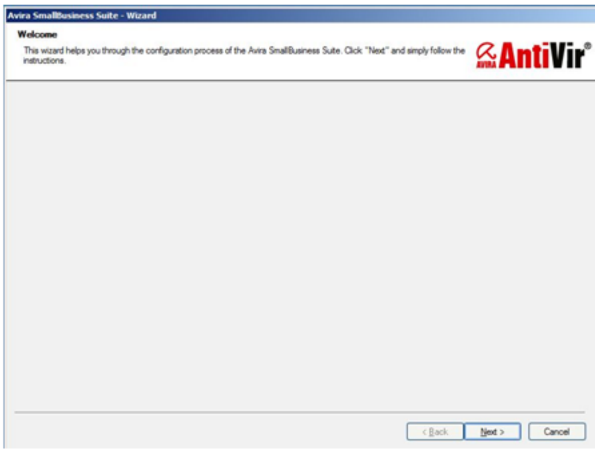


Avira SmallBusiness Suite - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Setup has succesfully installed the Avira SmallBusiness Suite. Click Finish to exit the setup and start the configuration wizard. If you cancel the configuration wizard at a specific point you can reenter it through the specific start menu shortcuts.

After successful installation, the SmallBusiness Suite wizard starts, this takes care of the next step in the setup:

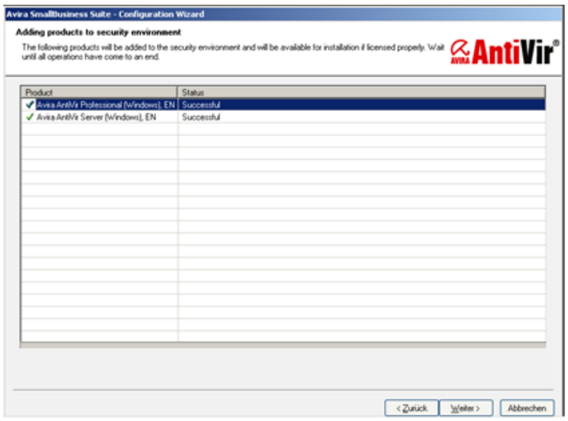


Avira SmallBusiness Suite - Wizard

Welcome

This wizard helps you through the configuration process of the Avira SmallBusiness Suite. Click "Next" and simply follow the instructions.

Here we see that the future security environment database is populated with AntiVir Professional and the AntiVir Server, so that the program can be remotely installed to client PCs.



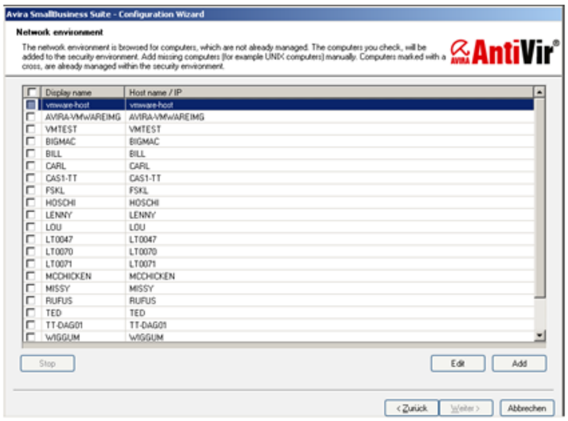
Avira SmallBusiness Suite - Configuration Wizard

Adding products to security environment

The following products will be added to the security environment and will be available for installation if licensed properly. Wait until all operations have come to an end.

Product	Status
✓ Avira AntiVir Professional (Windows), EN	Successful
✓ Avira AntiVir Server (Windows), EN	Successful

The product now searches the network environment for computers that are not already managed. Computers are added to the managed network simply by marking the tick-box



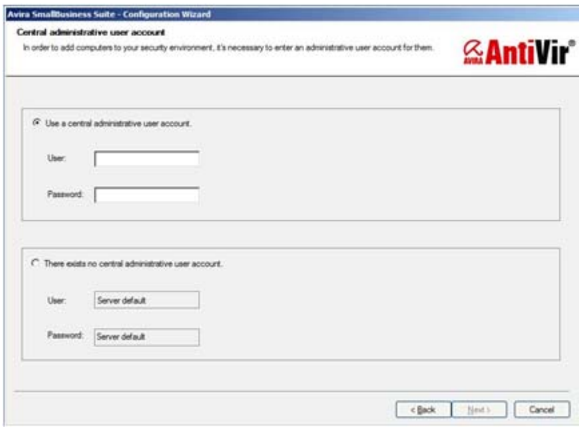
Network environment

The network environment is browsed for computers, which are not already managed. The computers you check, will be added to the security environment. Add missing computers (for example UNIX computers) manually. Computers marked with a cross, are already managed within the security environment.

□	Display name	Host name / IP
■	vmware-host	vmware-host
□	AVIRA-VMWAREIMG	AVIRA-VMWAREIMG
□	VMTEST	VMTEST
□	BIGMAC	BIGMAC
□	BILL	BILL
□	CARL	CARL
□	CAS1-TT	CAS1-TT
□	FSKL	FSKL
□	HOSCHI	HOSCHI
□	LENNY	LENNY
□	LOU	LOU
□	LT0047	LT0047
□	LT0070	LT0070
□	LT0071	LT0071
□	MCCHICKEN	MCCHICKEN
□	MISSY	MISSY
□	RUFUS	RUFUS
□	TED	TED
□	TT-DAG01	TT-DAG01
□	WIGGUM	WIGGUM

There is also a feature which allows additional clients (not found automatically) to be manually added to the list of machines to be installed. The ability to name them individually is particularly useful.

Next, we can choose a user account for adding the marked computers to the managed security environment. This is an ideal solution for larger networks where there is a system administrator who looks after security issues.



Central administrative user account

In order to add computers to your security environment, it's necessary to enter an administrative user account for them.

● Use a central administrative user account.

User:

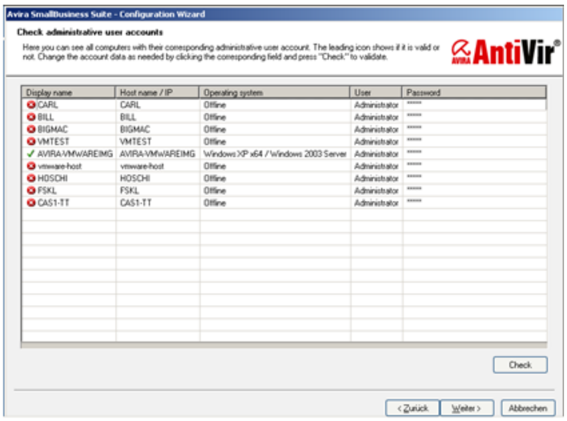
Password:

○ There exists no central administrative user account.

User: Server default

Password: Server default

The product then checks if the administrative account is valid for all marked computers and lists the result:

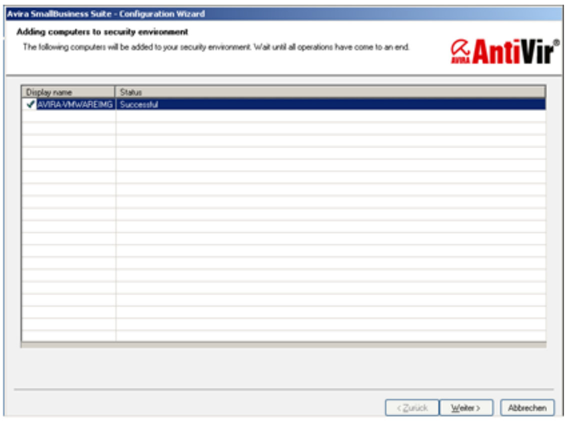


Check administrative user accounts

Here you can see all computers with their corresponding administrative user account. The leading icon shows if it is valid or not. Change the account data as needed by clicking the corresponding field and press "Check" to validate.

Display name	Host name / IP	Operating system	User	Password
⊗ CARL	CARL	Offline	Administrator	******
⊗ BILL	BILL	Offline	Administrator	******
⊗ BIGMAC	BIGMAC	Offline	Administrator	******
⊗ VMTEST	VMTEST	Offline	Administrator	******
✓ AVIRA-VMWAREIMG	AVIRA-VMWAREIMG	Windows XP x64 / Windows 2003 Server	Administrator	******
⊗ vmware-host	vmware-host	Offline	Administrator	******
⊗ HOSCHI	HOSCHI	Offline	Administrator	******
⊗ FSKL	FSKL	Offline	Administrator	******
⊗ CAS1-TT	CAS1-TT	Offline	Administrator	******

If the check was negative for certain computers the account data can be corrected on the spot. Next the marked computers are added to the security environment:



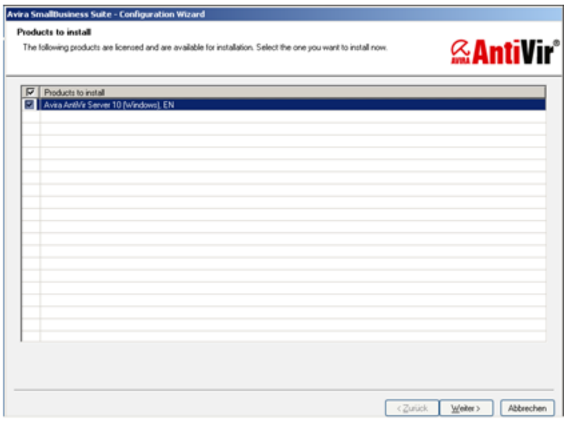
Adding computers to security environment

The following computers will be added to your security environment. Wait until all operations have come to an end.

Display name	Status
✓ AVIRA-VMWAREIMG	Successful

In an up-to-date Windows environment with Windows Server 2008 and Windows 7 clients it is not possible to carry out a remote installation without changing firewall settings. However, with centrally controlled means such as Group Policy, this shouldn't be too much of a hurdle.

The installation then works very smoothly and especially quickly. Products to be installed are chosen from a list:



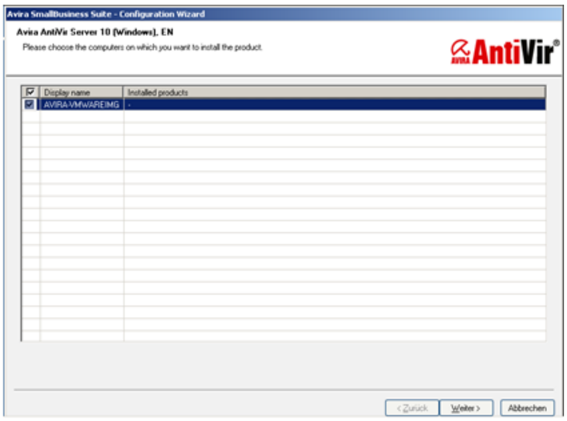
Avira SmallBusiness Suite - Configuration Wizard

Products to install

The following products are licensed and are available for installation. Select the one you want to install now.

☑	Products to install
☑	Avira AntiVir Server 10 (Windows), EN

Then choose the computer(s) that the product is to be installed on.



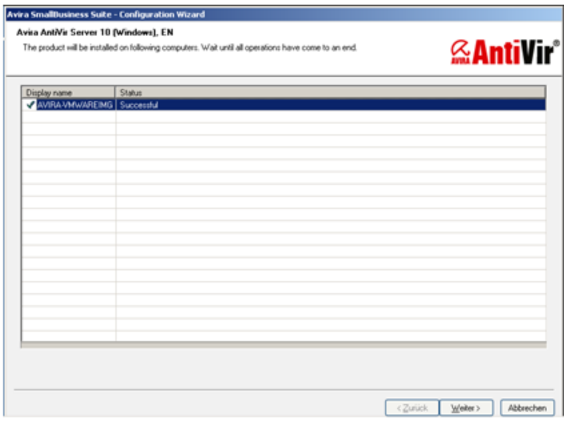
Avira SmallBusiness Suite - Configuration Wizard

Avira AntiVir Server 10 (Windows), EN

Please choose the computers on which you want to install the product.

☑	Display name	Installed products
☑	AVIRA-VMWAREIMG	-

The product is then installed on the marked computer(s). The completion status is also displayed very clearly:



Avira SmallBusiness Suite - Configuration Wizard

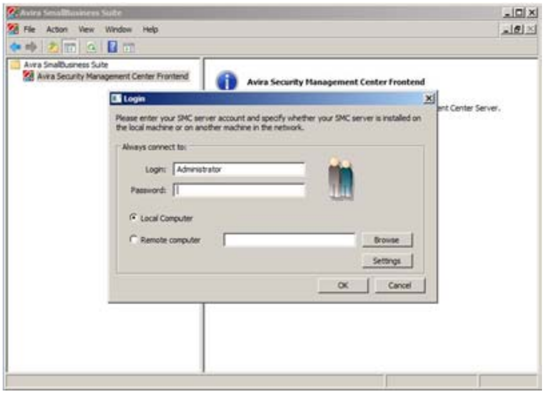
Avira AntiVir Server 10 (Windows), EN

The product will be installed on following computers. Wait until all operations have come to an end.

Display name	Status
✓ AVIRA-VMWAREIMG	Successful

Once the whole installation process is finished we get a final summary listing the computers with their installed products that are now managed within the security environment.

Once the configuration wizard is finished we can start the Security Management Center (SMC) and log on with the credentials used during the server installation:



Login

Please enter your SMC server account and specify whether your SMC server is installed on the local machine or on another machine in the network.

Always connect to:

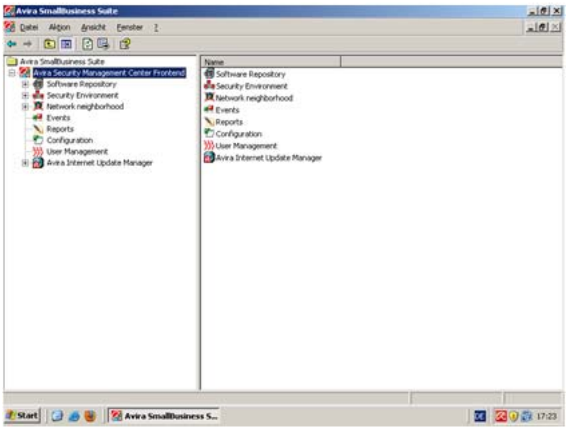
Login: Administrator

Password:

● Local Computer

○ Remote computer

Avira SmallBusiness Suite
File
Action
View
Window
Help
Avira SmallBusiness Suite
Avira Security Management Center Frontend
Avira Security Management Center Frontend
...ent Center Server.
Browse
Settings
OK
Cancel



At first glance, not much has changed from previous versions, so experienced Avira users will feel at home.

Thanks to the new installer, it is no longer necessary to register the licence at this stage, as it has already been done using the setup wizard. Software packets have also been configured with the wizard.

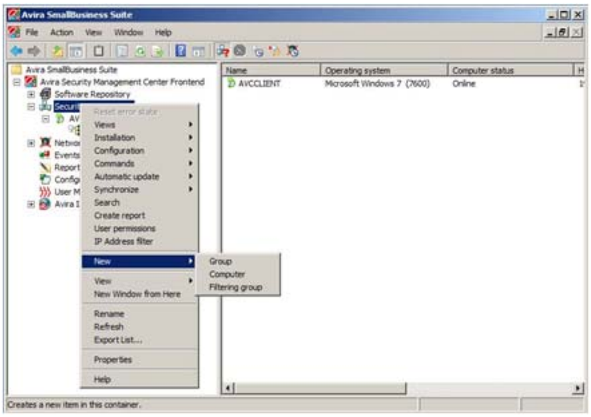
The integration of additional clients or additional products can now be carried out directly from the Security Management Center or by using the configuration wizard again which can be started directly from the Avira/Avira SmallBusiness Suite program group.

Especially the configuration wizard makes the initial configuration of Avira SmallBusiness

Suite child's play. It is very nice to see a manufacturer reacting to customer feedback, and Avira has really succeeded in making the management center much more user-friendly.

The general features have not been significantly changed, and so anyone familiar with Avira will still find their way around the settings very easily.

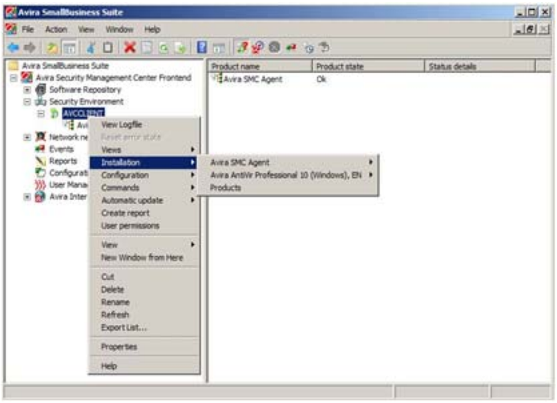
It is of course possible to create an individual structure for complex networks, so that different configurations can be applied as necessary. For example, separate configurations could be assigned for local and remote computers.



Name	Operating system	Computer status
AVCCLIENT	Microsoft Windows 7 (7600)	Online

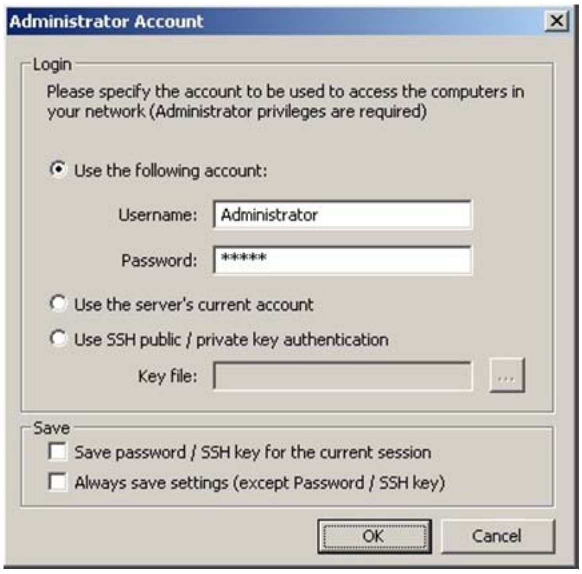
Creates a new item in this container.

Remote Installation remains unchanged. Right-clicking a client machine, then "Installation | Avira SMC Agent" allows installation of the agent. Other software, such as the client antivirus program, can be installed in a similar way if it has not already been installed through the wizard.



Product name	Product state	Status details
Avira SMC Agent	Ok	

The authentication possibilities for a push installation were already exemplary in last year's version:


Administrator Account

Login

Please specify the account to be used to access the computers in your network (Administrator privileges are required)

● Use the following account:

Username: Administrator

Password: *****

○ Use the server's current account

○ Use SSH public / private key authentication

Key file: ...

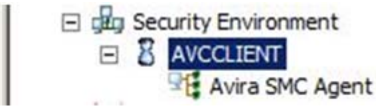
Save

□ Save password / SSH key for the current session

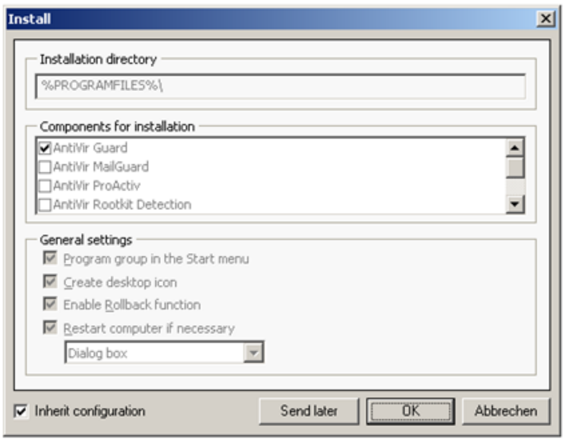
□ Always save settings (except Password / SSH key)

OK Cancel

During the installation, the hour glass symbol is displayed, until the SMC announces that client installation is complete.



The function scope dialog box also remains unchanged.


Install

Installation directory

%PROGRAMFILES%\

Components for installation

☑ AntiVir Guard
☐ AntiVir MailGuard
☐ AntiVir ProActiv
☐ AntiVir Rootkit Detection

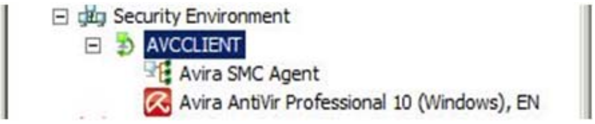
General settings

☑ Program group in the Start menu
☑ Create desktop icon
☑ Enable Rollback function
☑ Restart computer if necessary

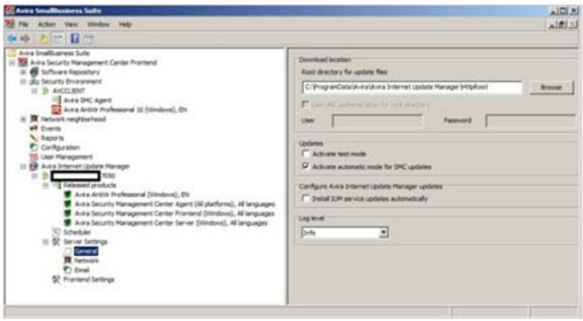
Dialog box

☑ Inherit configuration

On successful completion of the installation, the installed product can be seen under the individual client PC:



The Update Manager is now completely integrated into the Security Management Center which means that it is now possible to have more than one update manager, e.g. you can assign one update manager to one specific security environment group to speed up the distribution of updates. In spite of these changes the update manager remains very user-friendly, and we found our way around it immediately:


Download location

Root directory for update files: C:\ProgramData\Avira\Avira Internet Update Manager\HttpRoot

☐ Use UNC authentication for root directory

User: Password:

Updates

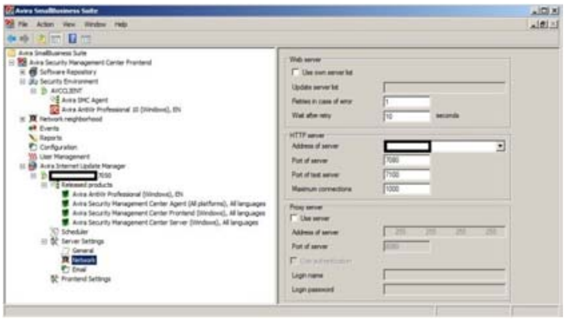
☐ Activate test mode
☑ Activate automatic mode for SMC updates

Configure Avira Internet Update Manager updates

☐ Install IUM service updates automatically

Log level: Info

The update settings are diverse, making the suite very suitable for complex networks.


Web server

☐ Use own server list

Update server list:

Retries in case of error: 1

Wait after retry: 10 seconds

HTTP server

Address of server:

Port of server: 7080

Port of test server: 7100

Maximum connections: 1000

Proxy server

☐ Use server

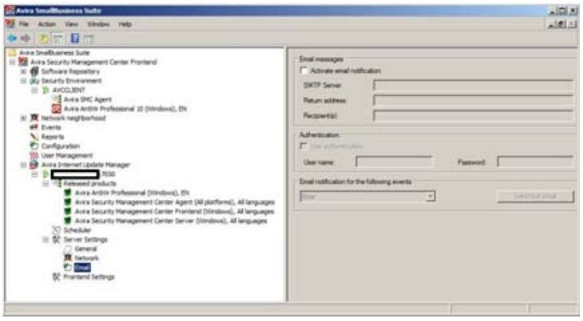
Address of server:

Port of server:

☐ Use authentication

Login name:

Login password:


Email messages

☐ Activate email notification

SMTP Server:

Return address:

Recipient(s):

Authentication

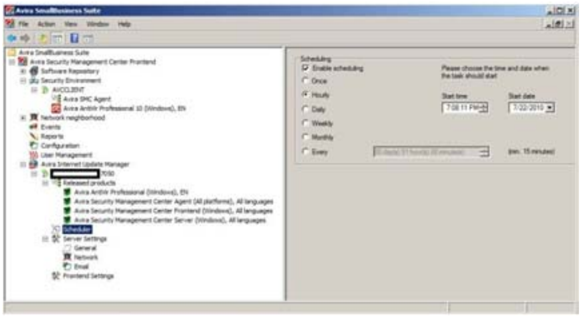
☐ Use authentication

User name: Password:

Email notification for the following events

Error

The Update Manager also provides very detailed scheduling options:


Scheduling

☑ Enable scheduling

○ Once
● Hourly
○ Daily
○ Weekly
○ Monthly
○ Every (min. 15 minutes)

Please choose the time and date when the task should start

Start time: 7:08:11 PM

Start date: 7/22/2010

The user interface is, as in the last version, exemplary, and configuration changes are largely made using convenient drop-down menus.

The installation routine for the Exchange scanner remains unchanged, as do the management console for mail and spam protection.

Manufacturer’s website

The website (www.avira.com) is designed in a suitably clear fashion.

The home page gives an overview of current threats and warnings in the support/virus lab area. You can subscribe to various RSS feeds, in order to keep up to date with the latest events.

There is also a "Virus Lab" area on the Support page where you can find out about viruses and other types of malware.

Avira has consolidated the various products into appropriate suites, and the licence model is, in contrast to the current trend, very simple.

The trial versions of the products run for 30 days without any reduction of functionality.

The installation process

This year, as previously, Avira´s installation process stands out, due to its simplicity and intuitive nature.

The manufacturer has evidently reacted to user feedback, and produced optimal solutions to the small problems that spoiled last year's product.

The installation wizard makes in unnecessary to consult the manual during installation.

The user-friendly nature of the product means that it can be deployed quickly and easily, without having to learn how to use it, and the basic configuration is very simple.

Administrator Console

The Administrator Console is, due to its MMC compatibility, clearly laid out and easy to understand.

It can be said that after the installation, only organisational work remains to be done.

In particular, the opportunity to create one's own security structure is especially impressive. We very much liked the possibility to import inventory lists for large networks; this is very simple to do, and saves a great deal of configuration. If you use an Active Directory you can also import your AD directory directly into the security environment and synchronize it automatically.

We have also noticed that the suite now offers a number of features that simplify its use in larger network environments.

The remote installation of clients is particularly simple. You only need to configure the login account to be used for the installation, and choose a package to install. No other preparation is necessary. Unfortunately, you do need to configure the Windows firewall on the client PCs in order to perform the remote installation. A note from the manufacturers to this effect, giving details of the relevant ports, would be helpful here.

What is particularly helpful for your every day work with the system is that whenever you add a computer to the security environment you can define that it automatically gets an Avira security product installed.

What is also worth mentioning is the active reporting on errors and other security relevant issues by so called filtering groups that show clients that in one way or another need the attention of the administrator.

If you want to use your own SSL certificates you can generate, deploy and use those certificates with Avira´s SmallBusiness Suite.

There is a convenient solution for licence administration, which is easy to configure.

Deployment areas

The Avira suite is ideally suited to small and medium-sized business. There have also been notable improvements for complex networks and enterprise environments. It is possible to live without some other features that would be valuable in an enterprise environment, given the extreme ease of installation and configuration.

In the SMB field, Avira remains a top player.

Antivirus Clients

The message pop-ups are pleasantly discreet. After installation has completed, the initial update must be started manually, unfortunately.

The client software is otherwise clearly laid out and gives a good overview of the state of the system.

Summary

The Avira Small Business Suite is very easy to install and fulfils all essential requirements.

The suite is ideal for small to medium networks, although improvements for larger networks have been implemented.

The client software is light on system resources, and the remote installation runs very quickly and easily.
Unfortunately, Avira is no exception to the general failure of security suites to provide real-time status information.

The noticeable development and improvement of the product is particularly worthy of praise. Even if there are small imperfections in the product now, you can happily use it, as there is every chance that even these will be improved in the future.

Pros:

+ Rapid client installation

+ Clearly structured management console

+ Good configuration wizards

+ Active Directory Support

+ Automatic installation of Avira security products

+ Active error reporting through filtering groups

Cons:

- Only small imperfections that are well compensated by the ease of use and clearly laid out structure.

Deployment areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★★	★★★★★	★★★

Overview:

Installation Wizard	★★★★★
User Navigation	★★★★
Administrator console	★★★★
Default Values	★★★★
MS Active Directory Support	★★★★
Database Support	★★
Remote Installation	★★★★
Website	★★★★
Manual	★★★★

BitDefender

Tested Software:

BitDefender Security for File Servers	→	File Server Protection
BitDefender Security for Exchange	→	Exchange Server Mail Protection
BitDefender Client Security	→	Centralized Control Console and Deployment

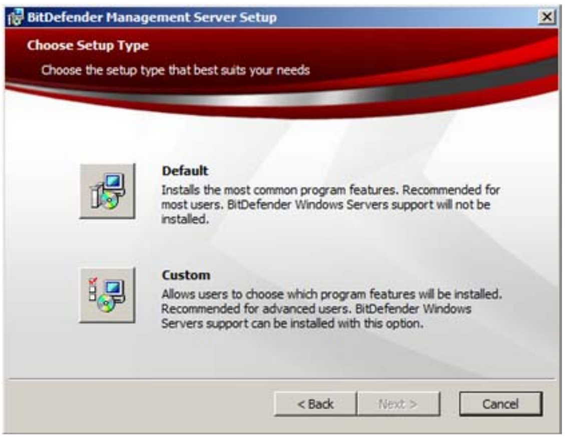
Downloading the product

The website design is simple and logical. There is no difficulty finding the products you want, and they can all be downloaded in fully functioning versions.

You have to register to get a test key for the software. This allows an adequate 30 days in which to test the product.

With BitDefender trial registration you get an email message with downloadinstructions and links, where you are pointed to videoturorials, too.

Two possible installation methods are described in the documentation. The components can be installed individually with their own installers, or by the management console. The latter is significantly simpler, but the individual components method may be useful in special cases.



BitDefender Management Server Setup

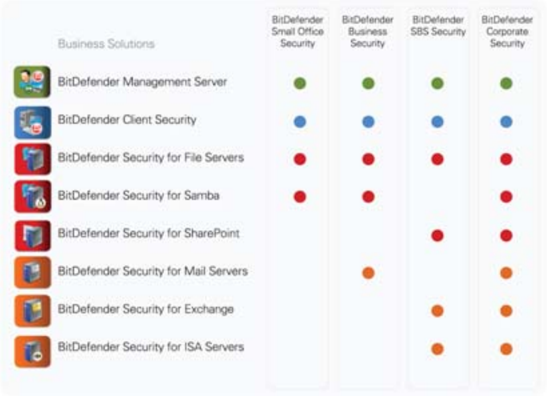
Choose Setup Type

Choose the setup type that best suits your needs

Default
Installs the most common program features. Recommended for most users. BitDefender Windows Servers support will not be installed.

Custom
Allows users to choose which program features will be installed. Recommended for advanced users. BitDefender Windows Servers support can be installed with this option.

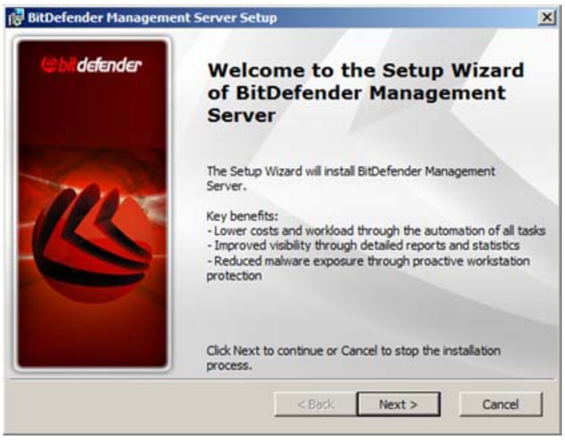
In the business section of the website, there is an overview of the functionality provided by different versions of the suite. This is very simple and practical for the user.



Business Solutions	BitDefender Small Office Security	BitDefender Business Security	BitDefender SBS Security	BitDefender Corporate Security
BitDefender Management Server	●	●	●	●
BitDefender Client Security	●	●	●	●
BitDefender Security for File Servers	●	●	●	●
BitDefender Security for Samba	●	●		●
BitDefender Security for SharePoint			●	●
BitDefender Security for Mail Servers		●		●
BitDefender Security for Exchange			●	●
BitDefender Security for ISA Servers			●	●

Installation

We begin with the installation of the management server, which will then be used to install the other components:



BitDefender Management Server Setup

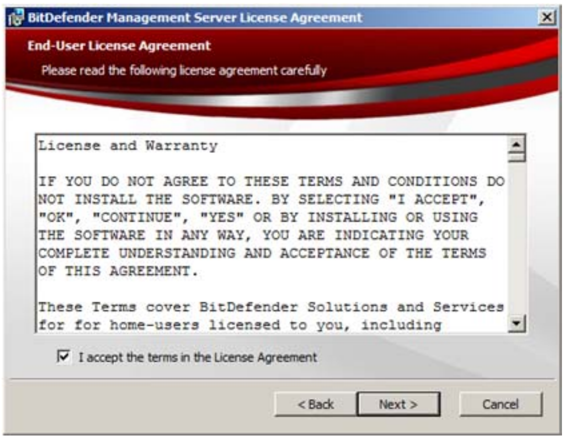
Welcome to the Setup Wizard of BitDefender Management Server

The Setup Wizard will install BitDefender Management Server.

Key benefits:
- Lower costs and workload through the automation of all tasks
- Improved visibility through detailed reports and statistics
- Reduced malware exposure through proactive workstation protection

Click Next to continue or Cancel to stop the installation process.

We then have to agree to the obligatory licence agreement:



BitDefender Management Server License Agreement

End-User License Agreement

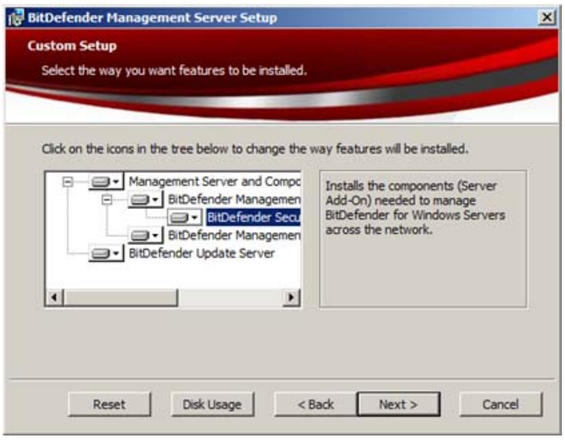
Please read the following license agreement carefully

```
License and Warranty

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO
NOT INSTALL THE SOFTWARE. BY SELECTING "I ACCEPT",
"OK", "CONTINUE", "YES" OR BY INSTALLING OR USING
THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR
COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS
OF THIS AGREEMENT.

These Terms cover BitDefender Solutions and Services
for for home-users licensed to you, including
```

☑ I accept the terms in the License Agreement

After this, we can choose the installation method. For the purposes of our test we chose the Custom Installation, in order to better evaluate the functions of the installer.

The next step is to choose the scope of the installation:



BitDefender Management Server Setup

Custom Setup

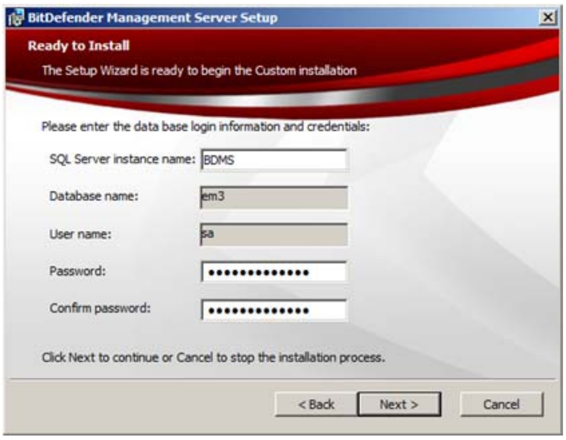
Select the way you want features to be installed.

Click on the icons in the tree below to change the way features will be installed.

- Management Server and Compc
  - BitDefender Managemen
    - BitDefender Secu
  - BitDefender Managemen
- BitDefender Update Server

Installs the components (Server Add-On) needed to manage BitDefender for Windows Servers across the network.

The following point gives us an idea of the scalability of the security system. The Master/Slave variant is ideally suited to large networks, or those with remote sites:



BitDefender Management Server Setup

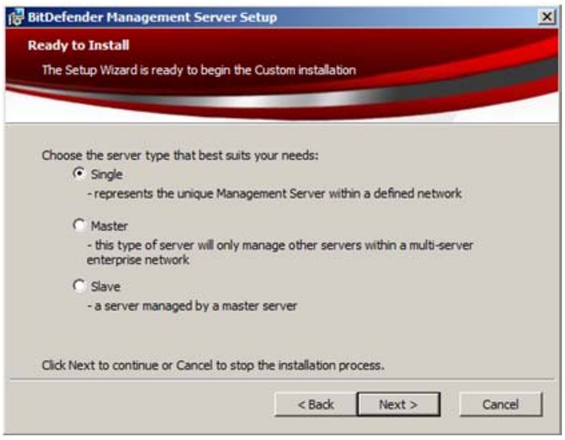
Ready to Install

The Setup Wizard is ready to begin the Custom installation

Please enter the data base login information and credentials:

SQL Server instance name: BDMS
Database name: em3
User name: sa
Password: •••••••••••••
Confirm password: •••••••••••••

Click Next to continue or Cancel to stop the installation process.



BitDefender Management Server Setup

Ready to Install

The Setup Wizard is ready to begin the Custom installation

Choose the server type that best suits your needs:

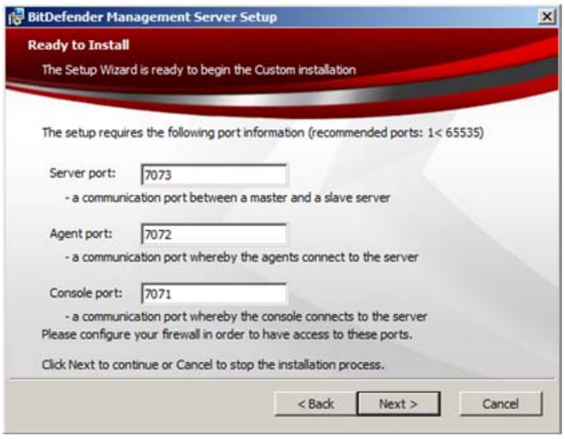
● Single
- represents the unique Management Server within a defined network

○ Master
- this type of server will only manage other servers within a multi-server enterprise network

○ Slave
- a server managed by a master server

Click Next to continue or Cancel to stop the installation process.

The next step is decisive for the communication of the individual components. The ports used by the suite can be configured to suit your own network environment:



BitDefender Management Server Setup

Ready to Install

The Setup Wizard is ready to begin the Custom installation

The setup requires the following port information (recommended ports: 1< 65535)

Server port: 7073

- a communication port between a master and a slave server

Agent port: 7072

- a communication port whereby the agents connect to the server

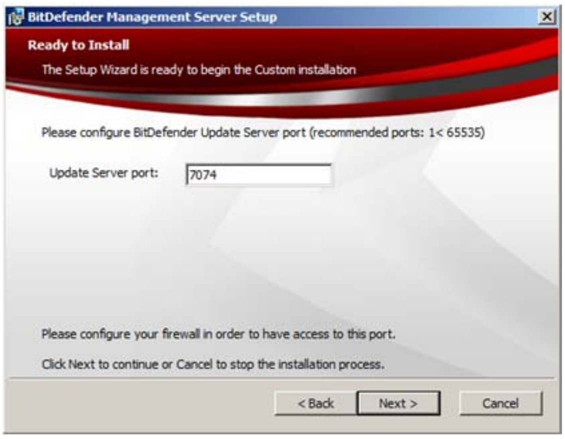
Console port: 7071

- a communication port whereby the console connects to the server

Please configure your firewall in order to have access to these ports.

Click Next to continue or Cancel to stop the installation process.

Even the port used to provide updates can be selected:



BitDefender Management Server Setup

Ready to Install

The Setup Wizard is ready to begin the Custom installation

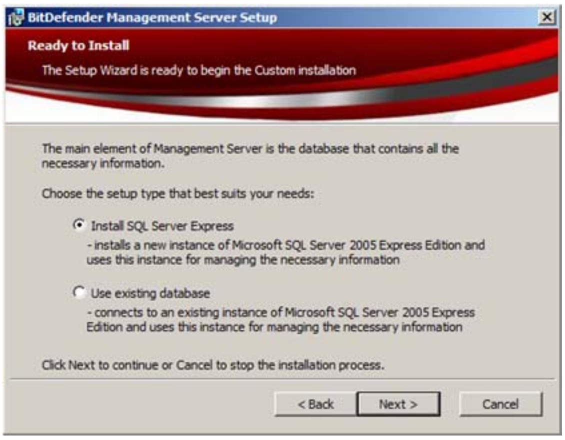
Please configure BitDefender Update Server port (recommended ports: 1< 65535)

Update Server port: 7074

Please configure your firewall in order to have access to this port.

Click Next to continue or Cancel to stop the installation process.

Like many other management products, BitDefender Security Suite needs a database server running in the background. As there is no SQL server in our test network, we select the SQL Express option:



BitDefender Management Server Setup

Ready to Install

The Setup Wizard is ready to begin the Custom installation

The main element of Management Server is the database that contains all the necessary information.

Choose the setup type that best suits your needs:

● Install SQL Server Express

- installs a new instance of Microsoft SQL Server 2005 Express Edition and uses this instance for managing the necessary information

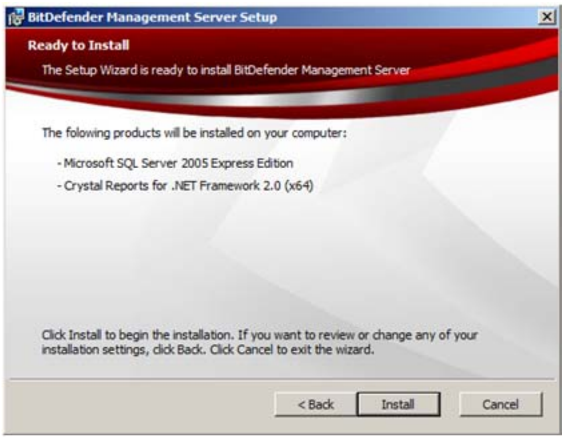
○ Use existing database

- connects to an existing instance of Microsoft SQL Server 2005 Express Edition and uses this instance for managing the necessary information

Click Next to continue or Cancel to stop the installation process.

We leave the database login credentials as the defaults.

The additional software components for SQL Server Express are now shown:



BitDefender Management Server Setup

Ready to Install

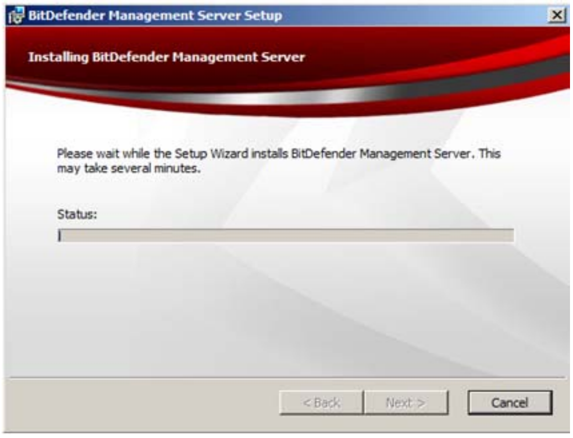
The Setup Wizard is ready to install BitDefender Management Server

The folowing products will be installed on your computer:

- Microsoft SQL Server 2005 Express Edition
- Crystal Reports for .NET Framework 2.0 (x64)

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

After the installation of SQL Server Express and its additional components comes the setup of the management server:



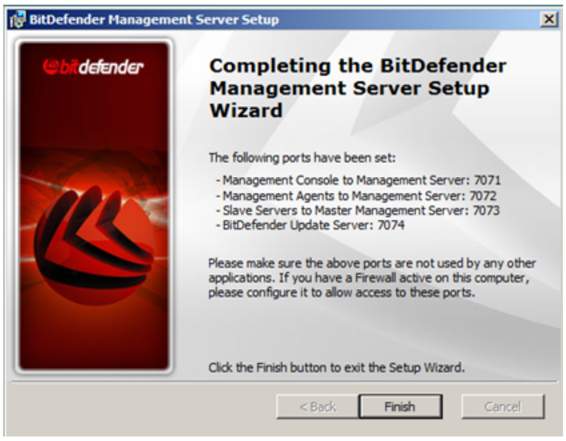
BitDefender Management Server Setup

Installing BitDefender Management Server

Please wait while the Setup Wizard installs BitDefender Management Server. This may take several minutes.

Status:

After the installation, a summary report of the changes made is shown.



BitDefender Management Server Setup

Completing the BitDefender Management Server Setup Wizard

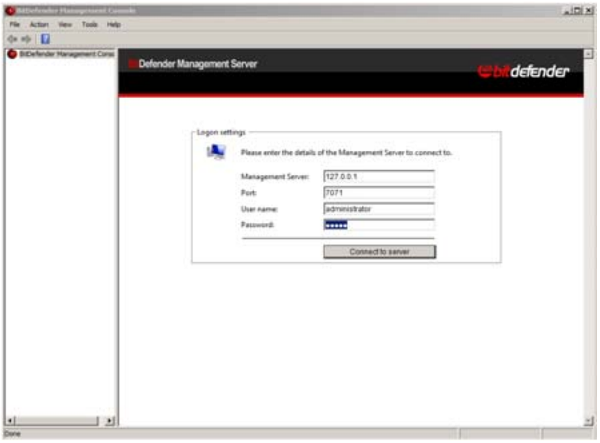
The following ports have been set:

- Management Console to Management Server: 7071
- Management Agents to Management Server: 7072
- Slave Servers to Master Management Server: 7073
- BitDefender Update Server: 7074

Please make sure the above ports are not used by any other applications. If you have a Firewall active on this computer, please configure it to allow access to these ports.

Click the Finish button to exit the Setup Wizard.

The Management Interface


BitDefender Management Console
File Action View Tools Help
BitDefender Management Cons
Defender Management Server
bitdefender
Connect to server
Done

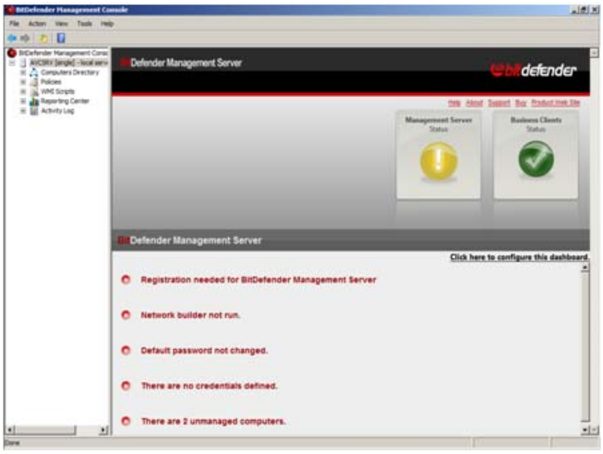
Logon settings

Please enter the details of the Management Server to connect to.

Management Server: 127.0.0.1
Port: 7071
User name: administrator
Password: •••••

The first task is to provide authentication credentials. The standard password has to be used here, which requires delving into the user manual, unfortunately. We confirm the password without change, and log in to the management console for the first time.

We are initially greeted by a very simple, even Spartan, dashboard, which informs us of the next steps.


BitDefender Management Console
File Action View Tools Help
BitDefender Management Cons
AVCSRV [single] - local serv
Computers Directory
Policies
WMI Scripts
Reporting Center
Activity Log
Defender Management Server
bitdefender
Help About Support Buy Product Web Site
Management Server Status
Business Clients Status
BitDefender Management Server
Click here to configure this dashboard.
Done

Registration needed for BitDefender Management Server

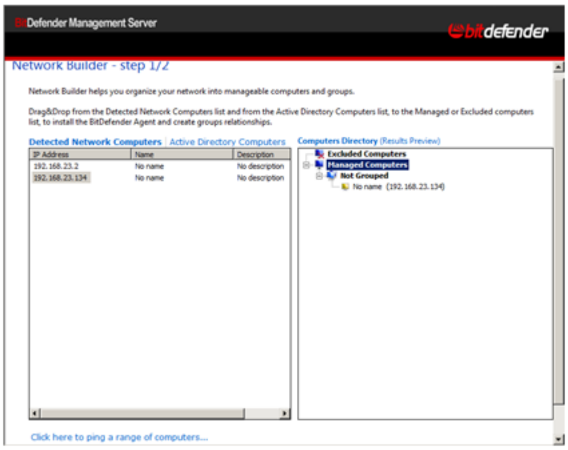
Network builder not run.

Default password not changed.

There are no credentials defined.

There are 2 unmanaged computers.

After successful registration of the management console, we proceed to the next stage of initial configuration. We start the Network Builder in order to define networks:

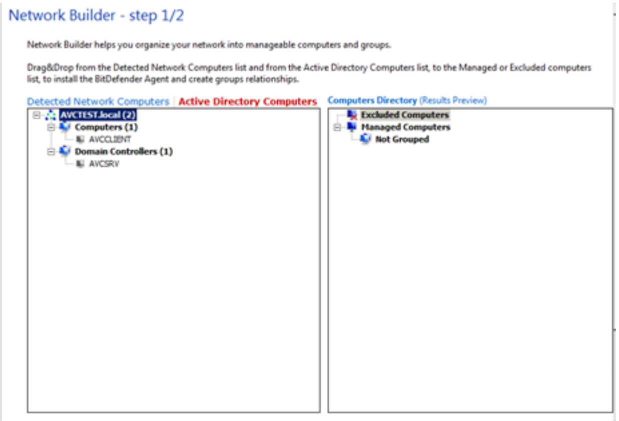

BitDefender Management Server
bitdefender
Network Builder - step 1/2
Detected Network Computers
Active Directory Computers
Computers Directory (Results Preview)
Excluded Computers
Managed Computers
Not Grouped
No name (192.168.23.134)
Click here to ping a range of computers...

Network Builder helps you organize your network into manageable computers and groups.

Drag&Drop from the Detected Network Computers list and from the Active Directory Computers list, to the Managed or Excluded computers list, to install the BitDefender Agent and create groups relationships.

IP Address	Name	Description
192.168.23.2	No name	No description
192.168.23.134	No name	No description

As soon as we start with the Network Builder, the simple handling of the suite is clearly demonstrated, and we can make rapid progress. In order to find the client computers more quickly, and get around any network security barriers, Network Builder enables us to use Active Directory to choose the clients:

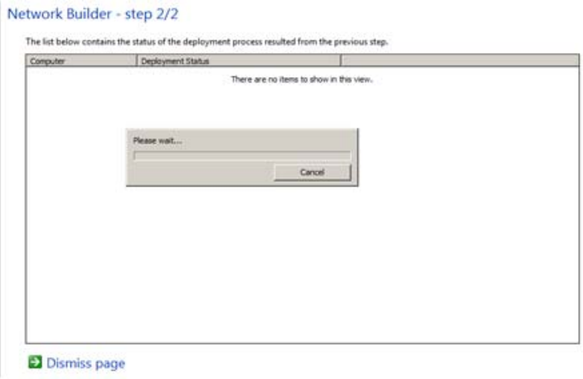

Network Builder - step 1/2
Detected Network Computers
Active Directory Computers
AVCTEST.local (2)
Computers (1)
AVCCLIENT
Domain Controllers (1)
AVCSRV
Computers Directory (Results Preview)
Excluded Computers
Managed Computers
Not Grouped

Network Builder helps you organize your network into manageable computers and groups.

Drag&Drop from the Detected Network Computers list and from the Active Directory Computers list, to the Managed or Excluded computers list, to install the BitDefender Agent and create groups relationships.

Now comes step 2 in the Network Builder wizard. After clicking on "Apply Changes", we immediately see the "Deployment Wizard", which allows us to configure various options for the installation.

After selecting the desired options, we can begin with deployment:



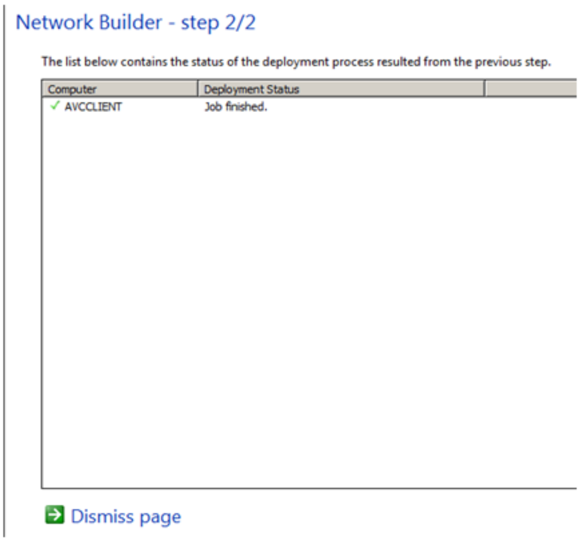
Network Builder - step 2/2

The list below contains the status of the deployment process resulted from the previous step.

Computer	Deployment Status
There are no items to show in this view.	

Please wait...

Configuration continues after successful installation of the clients:

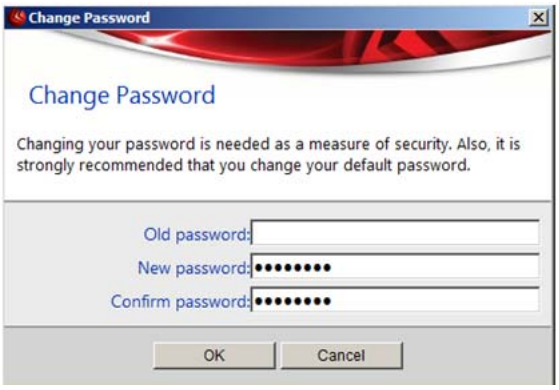


Network Builder - step 2/2

The list below contains the status of the deployment process resulted from the previous step.

Computer	Deployment Status
✓ AVCCLIENT	Job finished.

The next point on our dashboard is quickly dealt with. The standard password needs to be changed:



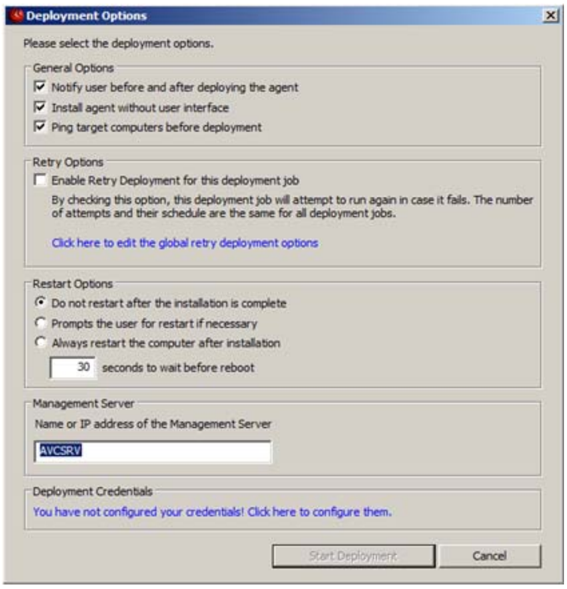
Change Password

Change Password

Changing your password is needed as a measure of security. Also, it is strongly recommended that you change your default password.

Old password:
New password: ●●●●●●●●
Confirm password: ●●●●●●●●

The next job is to bring the clients we have just installed into a group, which we have called simply "Clients". This grouping function is, as in other security suites, the best way to create a security structure which can be modified to fit the individual requirements of the organisation's network.



Deployment Options

Please select the deployment options.

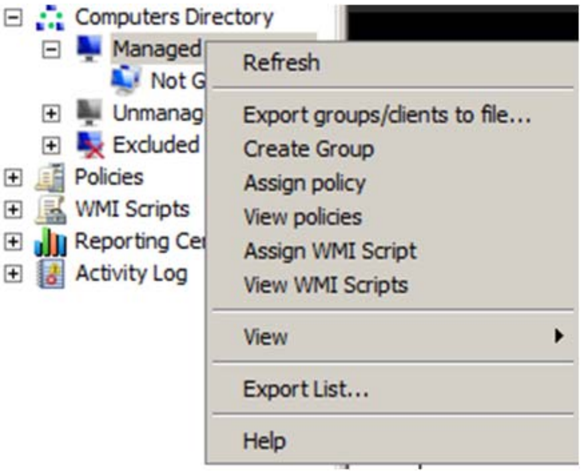
General Options
☑ Notify user before and after deploying the agent
☑ Install agent without user interface
☑ Ping target computers before deployment

Retry Options
☐ Enable Retry Deployment for this deployment job
By checking this option, this deployment job will attempt to run again in case it fails. The number of attempts and their schedule are the same for all deployment jobs.
Click here to edit the global retry deployment options

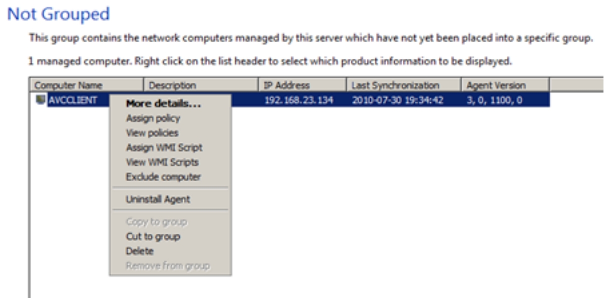
Restart Options
● Do not restart after the installation is complete
○ Prompts the user for restart if necessary
○ Always restart the computer after installation
30 seconds to wait before reboot

Management Server
Name or IP address of the Management Server
AVCSRV

Deployment Credentials
You have not configured your credentials! Click here to configure them.



We remove our client from the "Ungrouped" PCs and add it to our new group:



Not Grouped

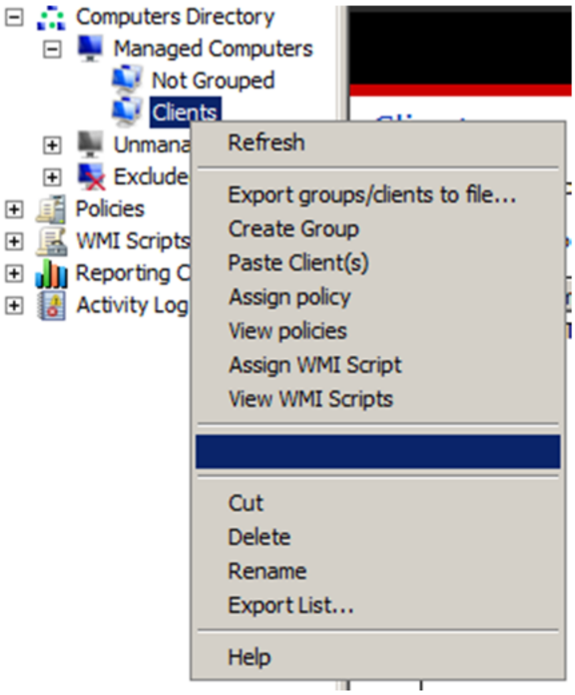
This group contains the network computers managed by this server which have not yet been placed into a specific group.

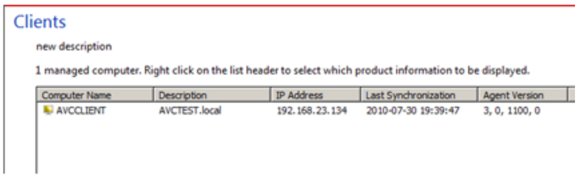
1 managed computer. Right click on the list header to select which product information to be displayed.

Computer Name	Description	IP Address	Last Synchronization	Agent Version
AVCCLIENT		192.168.23.134	2010-07-30 19:34:42	3, 0, 1100, 0

This example shows clearly the way the management console works. In MMC-compatible style, the console shows the available areas to be selected, and individual objects can be conveniently configured by means of a right-click.

After using the "Paste Client(s)" command, we immediately see the client we have just installed appearing in our newly created group:





Clients

new description

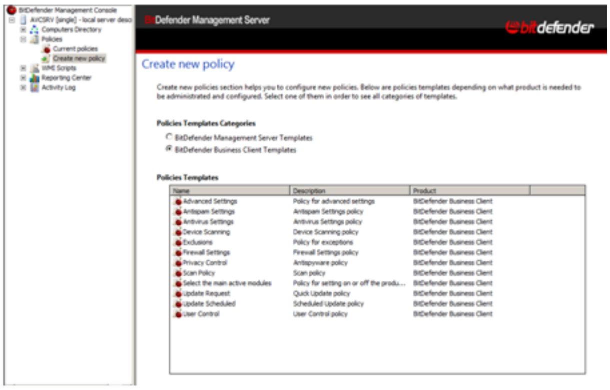
1 managed computer. Right click on the list header to select which product information to be displayed.

Computer Name	Description	IP Address	Last Synchronization	Agent Version
AVCCLIENT	AVCTEST.local	192.168.23.134	2010-07-30 19:39:47	3, 0, 1100, 0

Having completed this step, we have already finished the initial configuration. Now we can take a look at the rest of the management console.

The "Policies" area gives us the opportunity to create various security policies, whereby a number of preconfigured plans are available. It is easy to create one policy for clients and another for the management server. This policy management structure is the best means of realising complex security environments in corporate networks.

The various templates can be used to control the individual functions of the clients, so there are specific templates for the firewall, scan behaviour, and other client functions.



Create new policy

Create new policies section helps you to configure new policies. Below are policies templates depending on what product is needed to be administrated and configured. Select one of them in order to see all categories of templates.

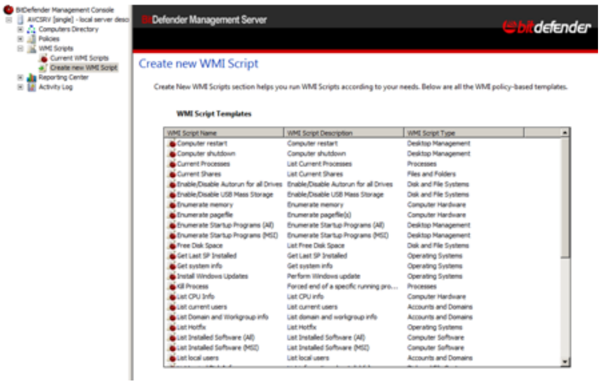
Policies Templates Categories

○ BitDefender Management Server Templates
● BitDefender Business Client Templates

Policies Templates

Name	Description	Product
Advanced Settings	Policy for advanced settings	BitDefender Business Client
Antispam Settings	Antispam Settings policy	BitDefender Business Client
Antivirus Settings	Antivirus Settings policy	BitDefender Business Client
Device Scanning	Device Scanning policy	BitDefender Business Client
Exclusions	Policy for exceptions	BitDefender Business Client
Firewall Settings	Firewall Settings policy	BitDefender Business Client
Privacy Control	Antispyware policy	BitDefender Business Client
Scan Policy	Scan policy	BitDefender Business Client
Select the main active modules	Policy for setting on or off the produ...	BitDefender Business Client
Update Request	Quick Update policy	BitDefender Business Client
Update Scheduled	Scheduled Update policy	BitDefender Business Client
User Control	User Control policy	BitDefender Business Client

The next point, the script manager, is well known in corporate circles, and is an essential component of every good security suite:



Create new WMI Script

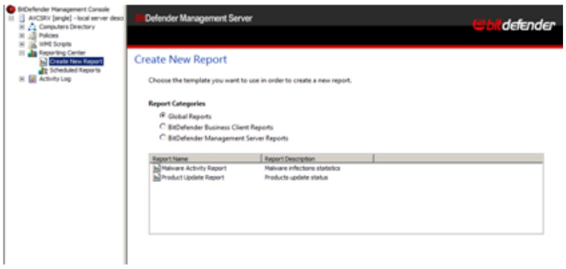
Create New WMI Scripts section helps you run WMI Scripts according to your needs. Below are all the WMI policy-based templates.

WMI Script Templates

WMI Script Name	WMI Script Description	WMI Script Type
Computer restart	Computer restart	Desktop Management
Computer shutdown	Computer shutdown	Desktop Management
Current Processes	List Current Processes	Processes
Current Shares	List Current Shares	Files and Folders
Enable/Disable Autorun for all Drives	Enable/Disable Autorun for all Drives	Disk and File Systems
Enable/Disable USB Mass Storage	Enable/Disable USB Mass Storage	Disk and File Systems
Enumerate memory	Enumerate memory	Computer Hardware
Enumerate pagefile	Enumerate pagefile(s)	Computer Hardware
Enumerate Startup Programs (All)	Enumerate Startup Programs (All)	Desktop Management
Enumerate Startup Programs (MSI)	Enumerate Startup Programs (MSI)	Desktop Management
Free Disk Space	List Free Disk Space	Disk and File Systems
Get Last SP Installed	Get Last SP Installed	Operating Systems
Get system info	Get system info	Operating Systems
Install Windows Updates	Perform Windows update	Operating Systems
Kill Process	Forced end of a specific running pro...	Processes
List CPU Info	List CPU info	Computer Hardware
List current users	List current users	Accounts and Domains
List Domain and Workgroup info	List domain and workgroup info	Accounts and Domains
List Hotfix	List Hotfix	Operating Systems
List Installed Software (All)	List Installed Software (All)	Computer Software
List Installed Software (MSI)	List Installed Software (MSI)	Computer Software
List local users	List local users	Accounts and Domains

As with policies, BitDefender provides a very good choice of pre-configured templates. This makes it very easy to configure the suite according to the requirements of your own network, without needing to consult the manual.

The template-based user interface is also used in the "Report Center". Again, it is an optimal method, and enables you to configure the system as you want in minimal time.



Create New Report

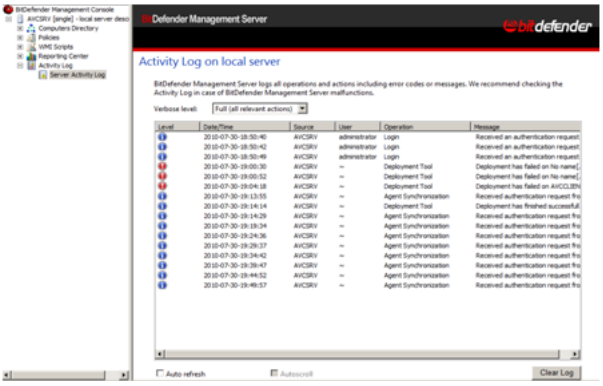
Choose the template you want to use in order to create a new report.

Report Categories

● Global Reports
○ BitDefender Business Client Reports
○ BitDefender Management Server Reports

Report Name	Report Description
Malware Activity Report	Malware infections statistics
Product Update Report	Products update status

The "Activity Log" is the logging centre of the suite, and very simple logs enable the administrator to maintain an overview of the system. The Spartan nature of the information recorded in the logs is ideal for quickly checking the main functions of the suite, but has the downside that it is only of limited use in troubleshooting procedures where detailed information is needed.



Activity Log on local server

BitDefender Management Server logs all operations and actions including error codes or messages. We recommend checking the Activity Log in case of BitDefender Management Server malfunctions.

Verbose level: Full (all relevant actions)

Level	Date/Time	Source	User	Operation	Message
ℹ	2010-07-30-18:50:40	AVCSRV	administrator	Login	Received an authentication request
ℹ	2010-07-30-18:50:42	AVCSRV	administrator	Login	Received an authentication request
ℹ	2010-07-30-18:50:49	AVCSRV	administrator	Login	Received an authentication request
!	2010-07-30-19:00:30	AVCSRV	~	Deployment Tool	Deployment has failed on No name[
!	2010-07-30-19:00:52	AVCSRV	~	Deployment Tool	Deployment has failed on No name[
!	2010-07-30-19:04:18	AVCSRV	~	Deployment Tool	Deployment has failed on AVCCLIEN
ℹ	2010-07-30-19:13:55	AVCSRV	~	Agent Synchronization	Received authentication request fro
ℹ	2010-07-30-19:14:14	AVCSRV	~	Deployment Tool	Deployment has finished successful
ℹ	2010-07-30-19:14:29	AVCSRV	~	Agent Synchronization	Received authentication request fro
ℹ	2010-07-30-19:19:34	AVCSRV	~	Agent Synchronization	Received authentication request fro
ℹ	2010-07-30-19:24:36	AVCSRV	~	Agent Synchronization	Received authentication request fro
ℹ	2010-07-30-19:29:37	AVCSRV	~	Agent Synchronization	Received authentication request fro
ℹ	2010-07-30-19:34:42	AVCSRV	~	Agent Synchronization	Received authentication request fro
ℹ	2010-07-30-19:39:47	AVCSRV	~	Agent Synchronization	Received authentication request fro
ℹ	2010-07-30-19:44:52	AVCSRV	~	Agent Synchronization	Received authentication request fro
ℹ	2010-07-30-19:49:57	AVCSRV	~	Agent Synchronization	Received authentication request fro

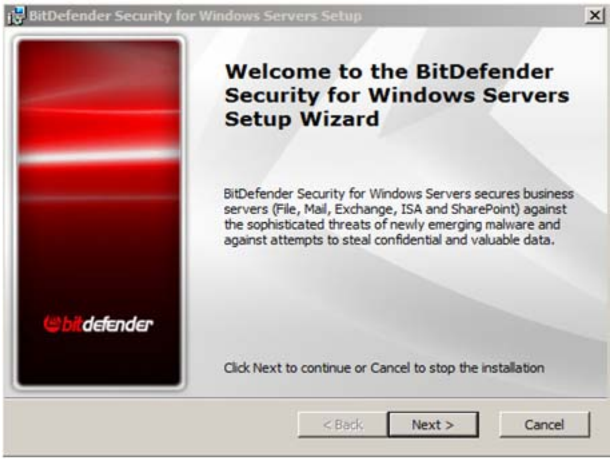
☐ Auto refresh ☐ Autoscroll

All in all, the management console is a very successfully designed tool for the central administration of the suite. The Dashboard in particular gives an excellent overview of the remaining tasks, and little time is needed for the initial configuration.

Exchange 2007 Protection

In order to demonstrate the second means of installation, we also set up the Exchange Protection using the standalone installer.

To begin with, the installer unpacks the installation files into a temporary folder, and then displays the first page of the setup wizard:

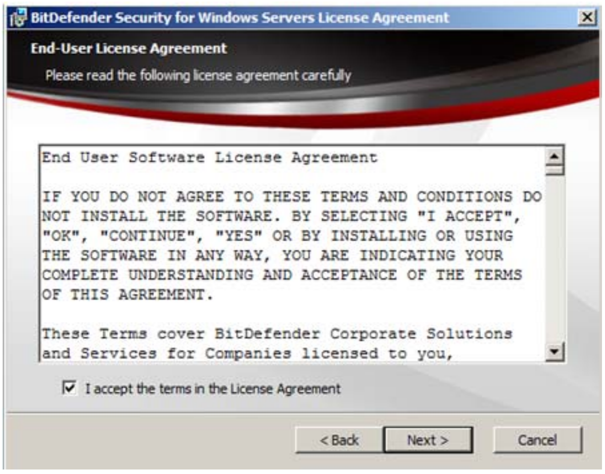


Welcome to the BitDefender Security for Windows Servers Setup Wizard

BitDefender Security for Windows Servers secures business servers (File, Mail, Exchange, ISA and SharePoint) against the sophisticated threats of newly emerging malware and against attempts to steal confidential and valuable data.

Click Next to continue or Cancel to stop the installation

As usual, we have to accept a licence agreement:



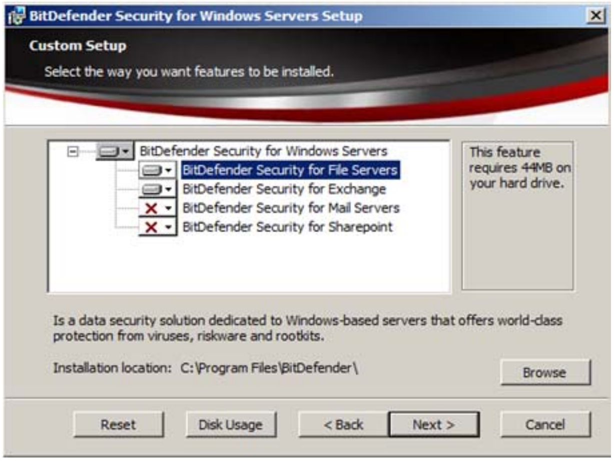
End-User License Agreement

Please read the following license agreement carefully

```
End User Software License Agreement

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO
NOT INSTALL THE SOFTWARE. BY SELECTING "I ACCEPT",
"OK", "CONTINUE", "YES" OR BY INSTALLING OR USING
THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR
COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS
OF THIS AGREEMENT.

These Terms cover BitDefender Corporate Solutions
and Services for Companies licensed to you,
```

☑ I accept the terms in the License Agreement

The screenshot below shows the choice of installation options. As we have already installed the file server protection using the management console, we will deactivate this option in our installation.



BitDefender Security for Windows Servers Setup

Custom Setup

Select the way you want features to be installed.

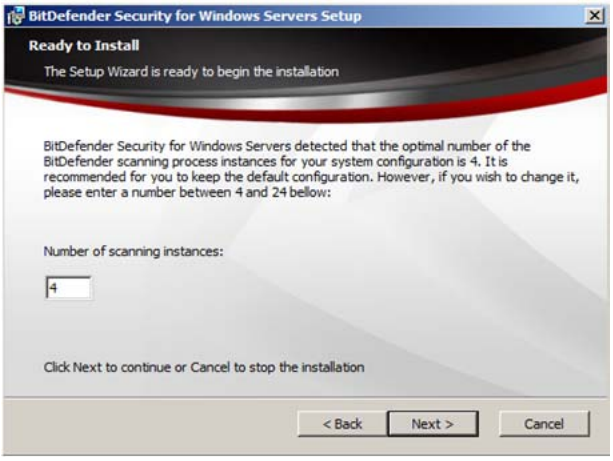
- BitDefender Security for Windows Servers
  - BitDefender Security for File Servers
  - BitDefender Security for Exchange
  - ☒ BitDefender Security for Mail Servers
  - ☒ BitDefender Security for Sharepoint

This feature requires 44MB on your hard drive.

Is a data security solution dedicated to Windows-based servers that offers world-class protection from viruses, riskware and rootkits.

Installation location: C:\Program Files\BitDefender\

The next step is to choose the number of scanning processes. The installer informs us that up to 24 instances can be selected, but recommends 4 (the minimum number) for our own network:



BitDefender Security for Windows Servers Setup

Ready to Install

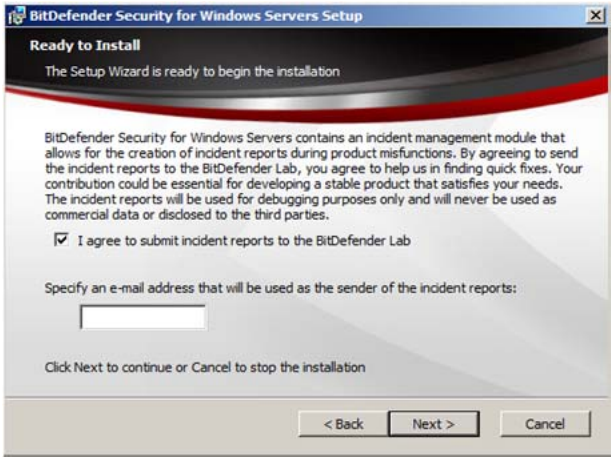
The Setup Wizard is ready to begin the installation

BitDefender Security for Windows Servers detected that the optimal number of the BitDefender scanning process instances for your system configuration is 4. It is recommended for you to keep the default configuration. However, if you wish to change it, please enter a number between 4 and 24 bellow:

Number of scanning instances: 4

Click Next to continue or Cancel to stop the installation

In the next step, you can decide whether to send reports to BitDefender. This option should be deselected for high-security environments.



BitDefender Security for Windows Servers Setup

Ready to Install

The Setup Wizard is ready to begin the installation

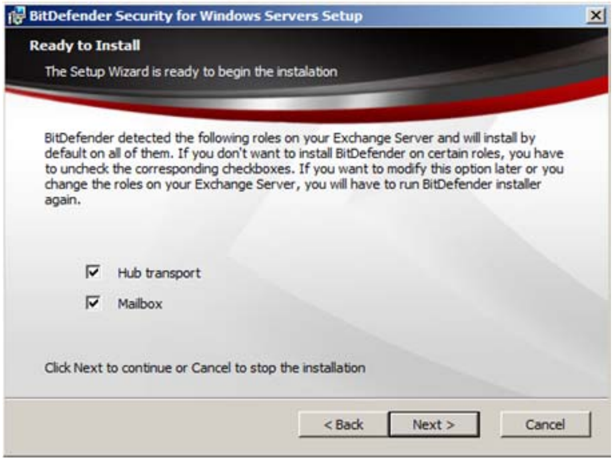
BitDefender Security for Windows Servers contains an incident management module that allows for the creation of incident reports during product misfunctions. By agreeing to send the incident reports to the BitDefender Lab, you agree to help us in finding quick fixes. Your contribution could be essential for developing a stable product that satisfies your needs. The incident reports will be used for debugging purposes only and will never be used as commercial data or disclosed to the third parties.

☑ I agree to submit incident reports to the BitDefender Lab

Specify an e-mail address that will be used as the sender of the incident reports:

Click Next to continue or Cancel to stop the installation

At the start of the process we chose to install the Exchange scanner, so now we are asked about the role of the Exchange Server:



BitDefender Security for Windows Servers Setup

Ready to Install

The Setup Wizard is ready to begin the installation

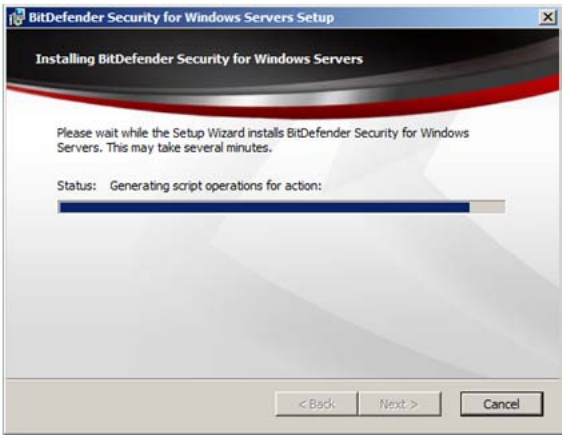
BitDefender detected the following roles on your Exchange Server and will install by default on all of them. If you don't want to install BitDefender on certain roles, you have to uncheck the corresponding checkboxes. If you want to modify this option later or you change the roles on your Exchange Server, you will have to run BitDefender installer again.

☑ Hub transport

☑ Mailbox

Click Next to continue or Cancel to stop the installation

The installer now has enough information to begin the installation process.

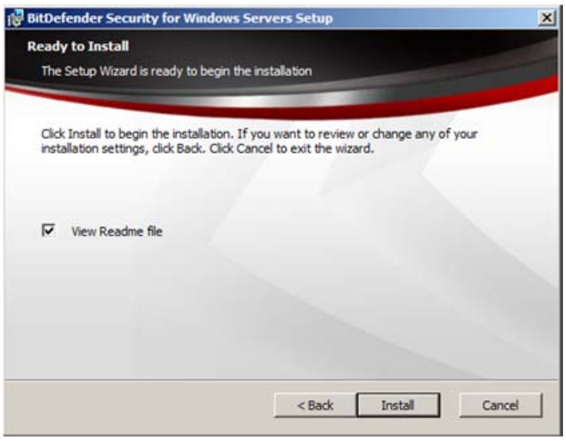


BitDefender Security for Windows Servers Setup

Installing BitDefender Security for Windows Servers

Please wait while the Setup Wizard installs BitDefender Security for Windows Servers. This may take several minutes.

Status: Generating script operations for action:



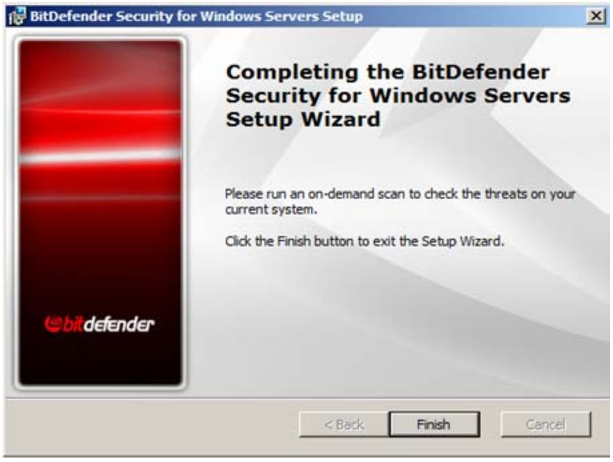
BitDefender Security for Windows Servers Setup

Ready to Install

The Setup Wizard is ready to begin the installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

☑ View Readme file



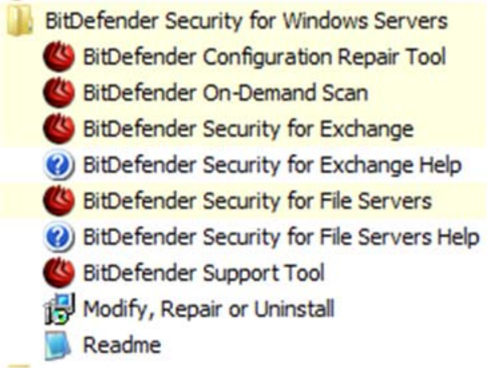
BitDefender Security for Windows Servers Setup

Completing the BitDefender Security for Windows Servers Setup Wizard

Please run an on-demand scan to check the threats on your current system.

Click the Finish button to exit the Setup Wizard.

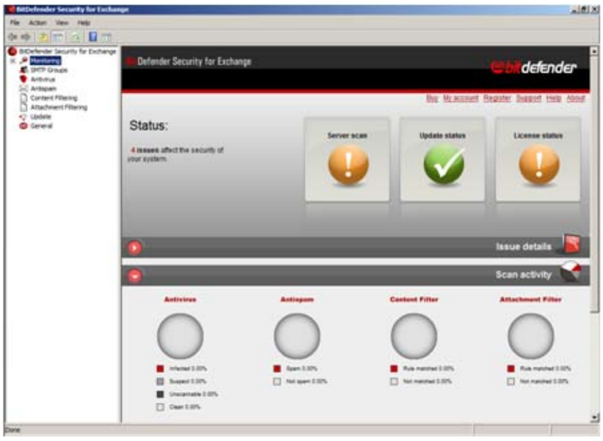
When installation is complete, we find the following program group in the Start Menu:



BitDefender Security for Windows Servers
- BitDefender Configuration Repair Tool
- BitDefender On-Demand Scan
- BitDefender Security for Exchange
- BitDefender Security for Exchange Help
- BitDefender Security for File Servers
- BitDefender Security for File Servers Help
- BitDefender Support Tool
- Modify, Repair or Uninstall
- Readme

Installation of the Exchange Protection component using the standalone installer is thus complete.

The management console for the Exchange 2007 protection

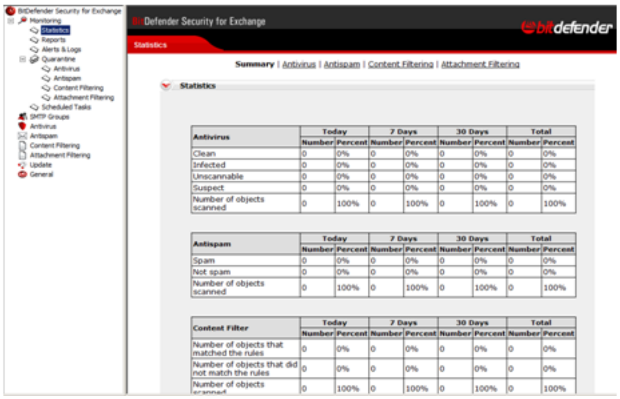


Status:

4 issues affect the security of your system.

The Exchange server protection is also configured using a simple, familiar console like the MMC.

The monitoring section of the Exchange console is exemplary. A very clear overview of the mail system and processed emails is presented, which is very hard to fault.



Statistics

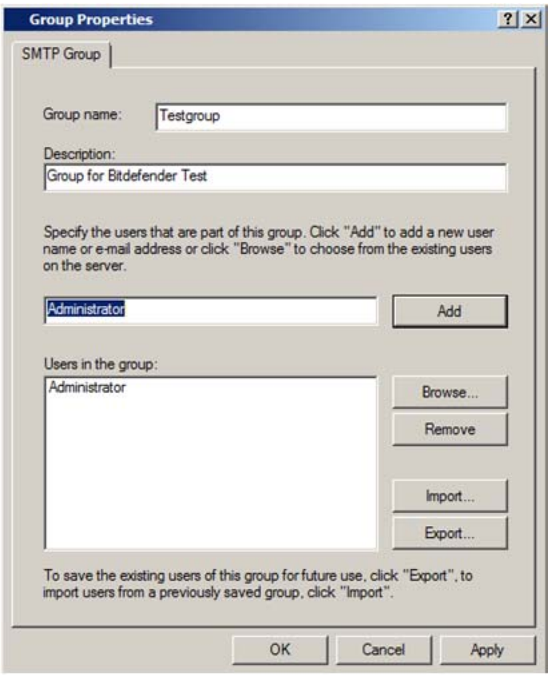
Antivirus	Today		7 Days		30 Days		Total	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Clean	0	0%	0	0%	0	0%	0	0%
Infected	0	0%	0	0%	0	0%	0	0%
Unscannable	0	0%	0	0%	0	0%	0	0%
Suspect	0	0%	0	0%	0	0%	0	0%
Number of objects scanned	0	100%	0	100%	0	100%	0	100%

Antispam	Today		7 Days		30 Days		Total	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Spam	0	0%	0	0%	0	0%	0	0%
Not spam	0	0%	0	0%	0	0%	0	0%
Number of objects scanned	0	100%	0	100%	0	100%	0	100%

Content Filter	Today		7 Days		30 Days		Total	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Number of objects that matched the rules	0	0%	0	0%	0	0%	0	0%
Number of objects that did not match the rules	0	0%	0	0%	0	0%	0	0%
Number of objects scanned	0	100%	0	100%	0	100%	0	100%

You can display detailed information from the various different areas, and so easily track potential problems/threats.

We were particularly pleased to see that BitDefender gives us the opportunity to create our own SMTP groups, a feature that we have very rarely seen elsewhere.



Group name: Testgroup

Description: Group for Bitdefender Test

Specify the users that are part of this group. Click "Add" to add a new user name or e-mail address or click "Browse" to choose from the existing users on the server.

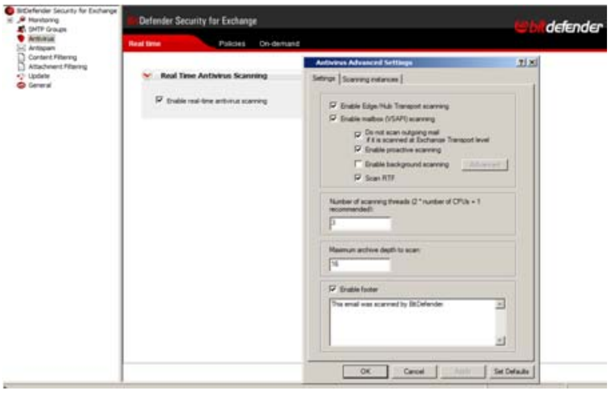
Administrator

Users in the group:

Administrator

To save the existing users of this group for future use, click "Export", to import users from a previously saved group, click "Import".

The configuration options are diverse and comprehensive:



Real Time Antivirus Scanning

☑ Enable real-time antivirus scanning

☑ Enable Edge/Hub Transport scanning

☑ Enable mailbox (VSAPI) scanning

☑ Do not scan outgoing mail if it is scanned at Exchange Transport level

☑ Enable proactive scanning

□ Enable background scanning

☑ Scan RTF

Number of scanning threads (2 * number of CPUs + 1 recommended):

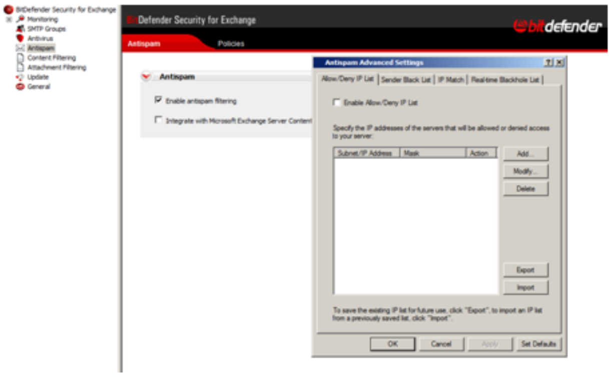
3

Maximum archive depth to scan:

16

☑ Enable footer

This email was scanned by BitDefender



Antispam

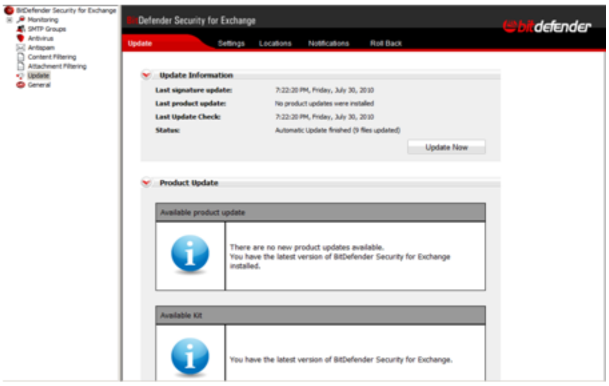
☑ Enable antispam filtering

□ Integrate with Microsoft Exchange Server Content

□ Enable Allow/Deny IP List

Specify the IP addresses of the servers that will be allowed or denied access to your server:

To save the existing IP list for future use, click "Export", to import an IP list from a previously saved list, click "Import".



Update Information

Last signature update: 7:22:20 PM, Friday, July 30, 2010

Last product update: No product updates were installed

Last Update Check: 7:22:20 PM, Friday, July 30, 2010

Status: Automatic Update finished (9 files updated)

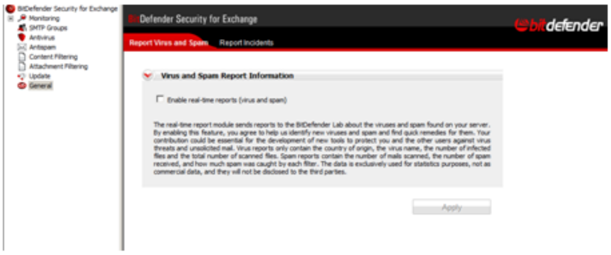
Product Update

Available product update

There are no new product updates available.
You have the latest version of BitDefender Security for Exchange installed.

Available Kit

You have the latest version of BitDefender Security for Exchange.



Virus and Spam Report Information

□ Enable real-time reports (virus and spam)

The real-time report module sends reports to the BitDefender Lab about the viruses and spam found on your server. By enabling this feature, you agree to help us identify new viruses and spam and find quick remedies for them. Your contribution could be essential for the development of new tools to protect you and the other users against virus threats and unsolicited mail. Virus reports only contain the country of origin, the virus name, the number of infected files and the total number of scanned files. Spam reports contain the number of mails scanned, the number of spam received, and how much spam was caught by each filter. The data is exclusively used for statistics purposes, not as commercial data, and they will not be disclosed to the third parties.

Due to the really exemplary choice of configuration options, the Exchange protection module in the BitDefender suite is extremely flexible, and can be adapted perfectly to the needs of your own network.

Manufacturer's Website

The manufacturer's website (**www.bitdefender.com**) is designed in an appropriately clear and simple way, in accordance with current standards.

Additionally, the site offers a security zone, where you can find out about viruses and other malicious programs.

The management console has been very well designed.

The installation process

The installation procedure is very simple if the management server is used, and can easily be performed by any user without resorting to the handbook.

However, we were also pleased that the standalone option is available, as this allows the product to be installed on smaller networks without any need to worry about the many detailed configuration options.

The administration console

The MMC (Microsoft Management Console) compatibility of the administration console makes it clear and easy to use.

Here too it can be said that after the installation, only organisational tasks still need to be completed.

The opportunities to customise a security structure for your own network are excellent.

The available functions and configuration possibilities mean that the suite is intended primarily for up to 3500 endpoints.

The remote installation of the clients is in itself extremely simple. Unfortunately it is necessary to configure the Windows Firewall on all client PCs, to allow the remote installation to work.

The management console for the Exchange protection is extremely powerful but still very straightforward to use.

Deployment areas

The BitDefender suite is suitable for networks of all sizes, including complex environments.

Antivirus clients

The antivirus software for clients is efficient, very user friendly and easy to find your way around. Once installed, clients need virtually no configuration and do not present excessive pop-up warnings.

Summary

The entire suite impresses due to its simple installation routine and very convenient user interface.

Regardless of the size and complexity of your network, the BitDefender suite offers you all the features you need.

The Exchange server protection must be particularly praised, as it is possible to make very detailed configuration changes, without feeling overwhelmed by the possibilities.

The user interface is so simple that a manual is more or less redundant.

In conclusion, the suite can be recommended to everybody.

Pros

+ Rapid client installation
+ Simple and clear management console
+ Easy remote installation
+ Good grouping functionality
+ Quick and simple installation
+ Excellent Exchange protection

Cons

- Limited filtering options
- No real-time status

Deployment areas

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★	★★★★	★★★★

Summary

Installation Wizard	★★★★★
User Navigation	★★★★★
Administrator console	★★★★★
Default Values	★★★★
MS Active Directory Support	★★★
Database Support	★★★
Remote Installation	★★★★
Website	★★★★
Manual	★★★★

ESET

Test Software:

ESET Remote Administrator	→	Management Console
ESET Mail Security	→	Exchange Server Mail Protection
ESET Smart Security 4	→	Client Protection

Installation

Downloading the product

It is easy to find the products you're looking for, as the website is clear and well designed.

ESET is the only manufacturer amongst those in this review to limit the availability of the test version. It is only possible to download a trial of the corporate software after making contact with the company.

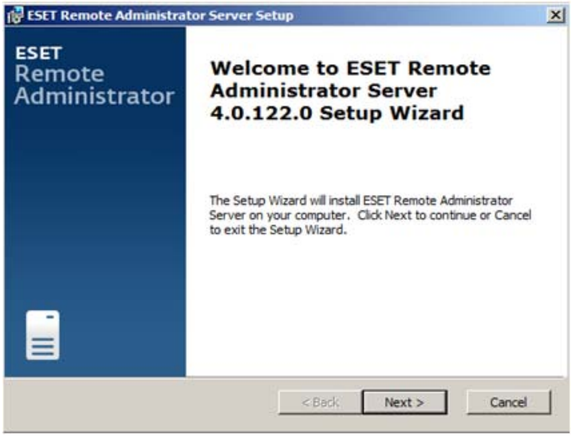
Like many other manufacturers, ESET makes a separate installer for every individual product or tool.

The products can be bought online from the web store. There is all information and user guides about them on the site

ESET offers an online scanner as an additional service free of charge.

Installation of the products

We start with the installation of the Remote Administrator Server:



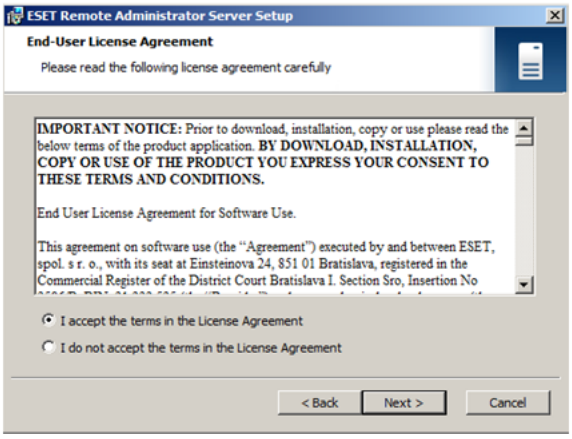
ESET Remote Administrator Server Setup

ESET Remote Administrator

Welcome to ESET Remote Administrator Server 4.0.122.0 Setup Wizard

The Setup Wizard will install ESET Remote Administrator Server on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Next we have to confirm acceptance of the licence agreement:



ESET Remote Administrator Server Setup

End-User License Agreement

Please read the following license agreement carefully

IMPORTANT NOTICE: Prior to download, installation, copy or use please read the below terms of the product application. **BY DOWNLOAD, INSTALLATION, COPY OR USE OF THE PRODUCT YOU EXPRESS YOUR CONSENT TO THESE TERMS AND CONDITIONS.**

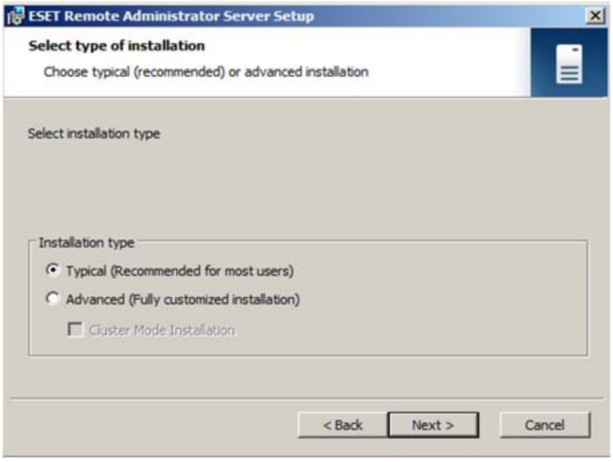
End User License Agreement for Software Use.

This agreement on software use (the "Agreement") executed by and between ESET, spol. s r. o., with its seat at Einsteinova 24, 851 01 Bratislava, registered in the Commercial Register of the District Court Bratislava I. Section Sro, Insertion No

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

After this, we can choose the installation method. The Advanced Installation gives the option of Cluster Mode:



ESET Remote Administrator Server Setup

Select type of installation

Choose typical (recommended) or advanced installation

Select installation type

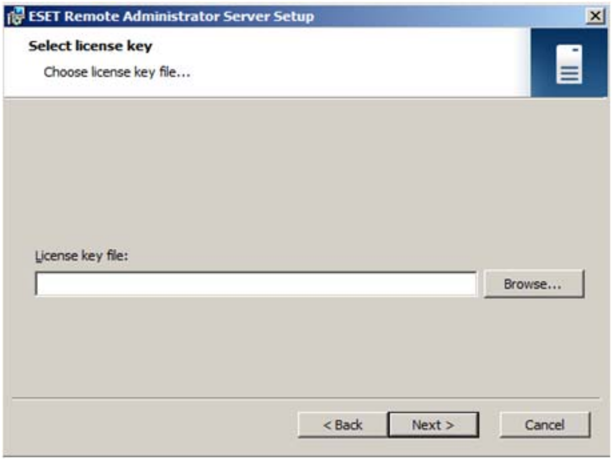
Installation type

● Typical (Recommended for most users)

○ Advanced (Fully customized installation)

□ Cluster Mode Installation

The next step is to locate the licence key file:



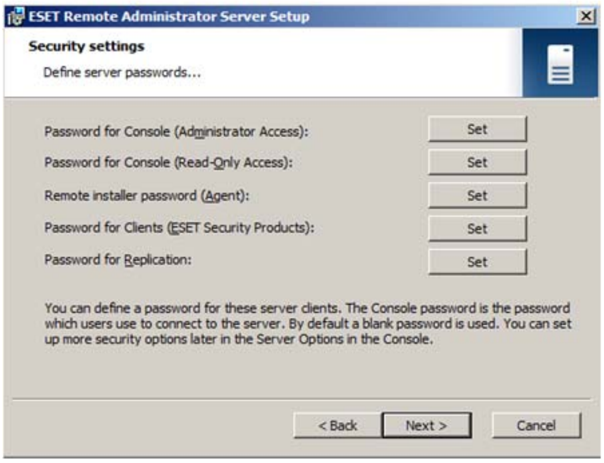
ESET Remote Administrator Server Setup

Select license key

Choose license key file...

License key file:

We now have the opportunity to enter passwords for the individual functions of the software. Using different passwords for different areas of access increases security, although some administrators would surely prefer to use one password for all functions. But, as mentioned before, it is more secure this way!


ESET Remote Administrator Server Setup

Security settings

Define server passwords...

Password for Console (Administrator Access): Set

Password for Console (Read-Only Access): Set

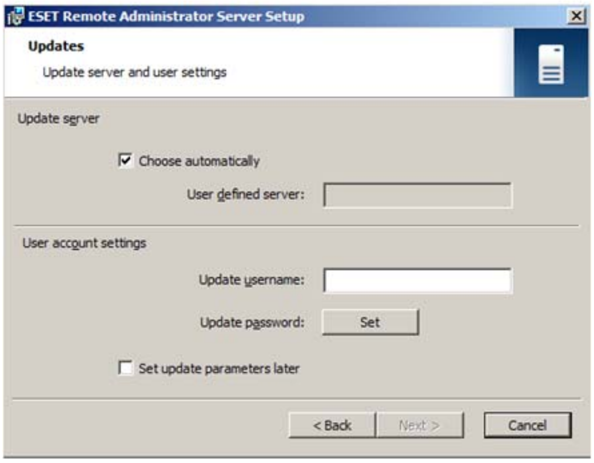
Remote installer password (Agent): Set

Password for Clients (ESET Security Products): Set

Password for Replication: Set

You can define a password for these server clients. The Console password is the password which users use to connect to the server. By default a blank password is used. You can set up more security options later in the Server Options in the Console.

The next point concerns the update settings.


ESET Remote Administrator Server Setup

Updates

Update server and user settings

Update server

☑ Choose automatically

User defined server:

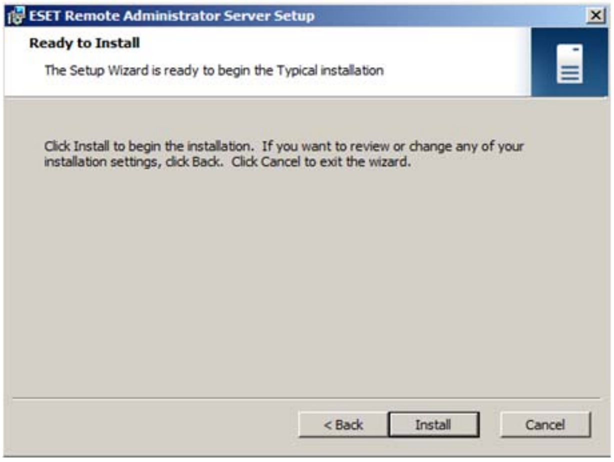
User account settings

Update username:

Update password: Set

☐ Set update parameters later

The installer now has enough information to begin the setup process.

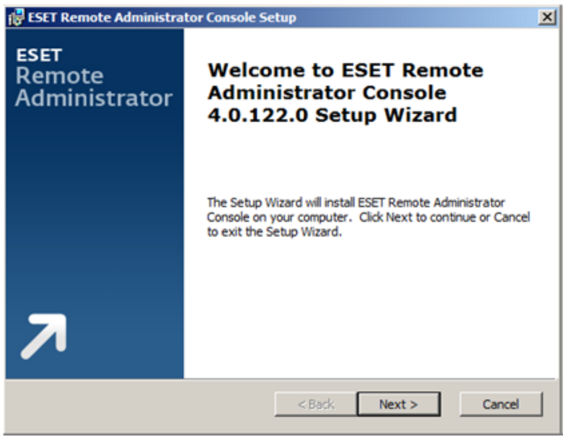

ESET Remote Administrator Server Setup

Ready to Install

The Setup Wizard is ready to begin the Typical installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

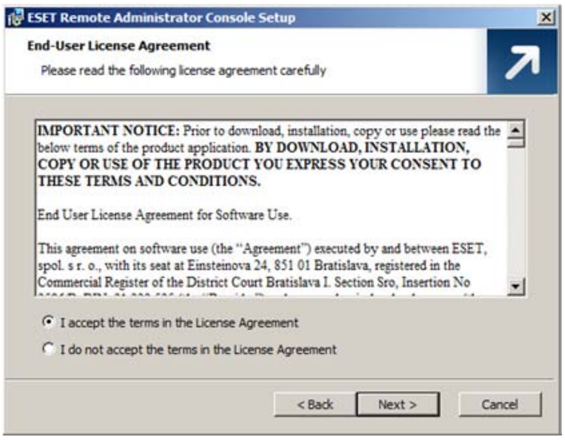
The next step is to install the Remote Administrator Console. This can be installed on any PC on the network, and serves as the interface for the Remote Administrator Server, which we have already installed. This distinction is not very clear to the new user without reading the manual.


ESET Remote Administrator Console Setup

Welcome to ESET Remote Administrator Console 4.0.122.0 Setup Wizard

The Setup Wizard will install ESET Remote Administrator Console on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

There is another licence agreement to accept:



ESET Remote Administrator Console Setup

End-User License Agreement

Please read the following license agreement carefully

IMPORTANT NOTICE: Prior to download, installation, copy or use please read the below terms of the product application. BY DOWNLOAD, INSTALLATION, COPY OR USE OF THE PRODUCT YOU EXPRESS YOUR CONSENT TO THESE TERMS AND CONDITIONS.

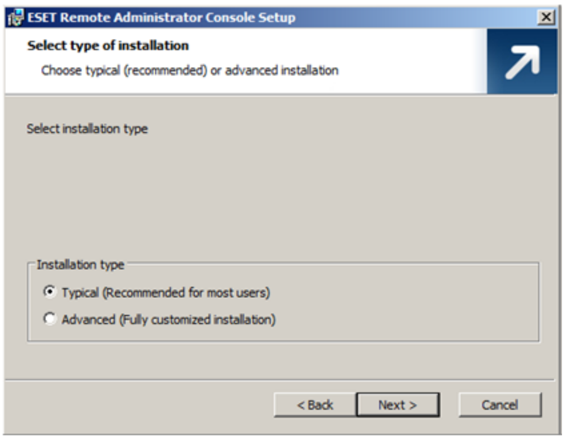
End User License Agreement for Software Use.

This agreement on software use (the "Agreement") executed by and between ESET, spol. s r. o., with its seat at Einsteinova 24, 851 01 Bratislava, registered in the Commercial Register of the District Court Bratislava I. Section Sro, Insertion No

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

Again, there is a choice of "Typical" and "Advanced" installation methods:



ESET Remote Administrator Console Setup

Select type of installation

Choose typical (recommended) or advanced installation

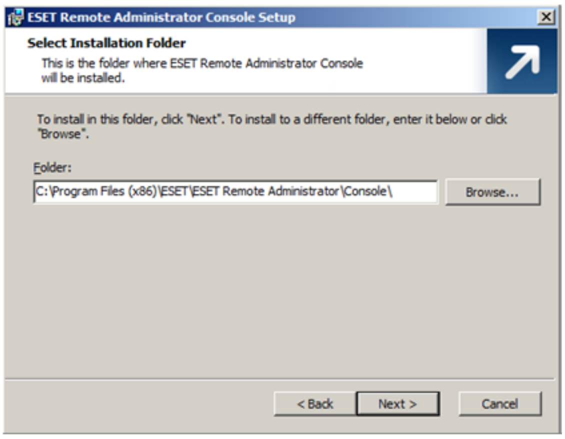
Select installation type

Installation type

● Typical (Recommended for most users)

○ Advanced (Fully customized installation)

We can then choose the installation folder:



ESET Remote Administrator Console Setup

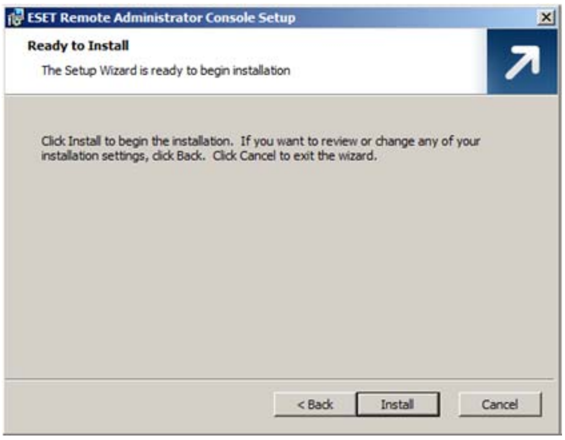
Select Installation Folder

This is the folder where ESET Remote Administrator Console will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files (x86)\ESET\ESET Remote Administrator\Console\

The installer has now collected enough information and can begin the setup process.

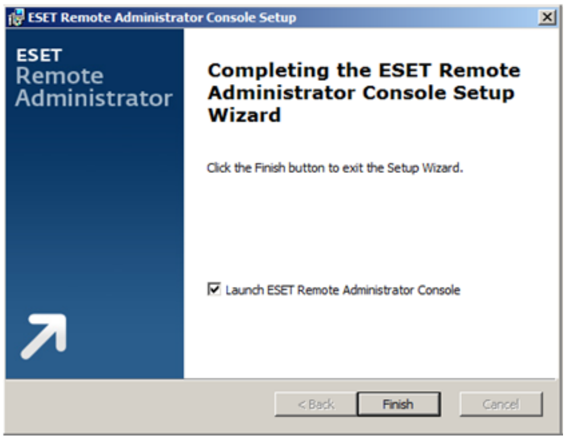


ESET Remote Administrator Console Setup

Ready to Install

The Setup Wizard is ready to begin installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.



ESET Remote Administrator Console Setup

Completing the ESET Remote Administrator Console Setup Wizard

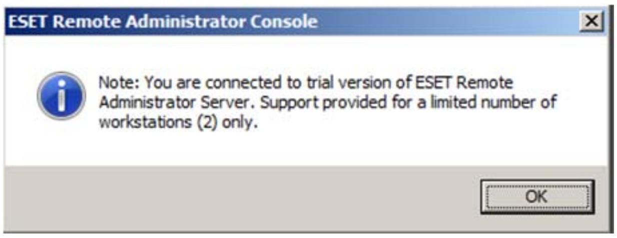
Click the Finish button to exit the Setup Wizard.

☑ Launch ESET Remote Administrator Console

On completion of the installation, we can open the console.

In the case of a Typical Installation, the Microsoft Access Engine (Jet Database) is selected by default as the database. If you want to use an SQL server, this has to be configured manually with the help of the manual.

The management interface

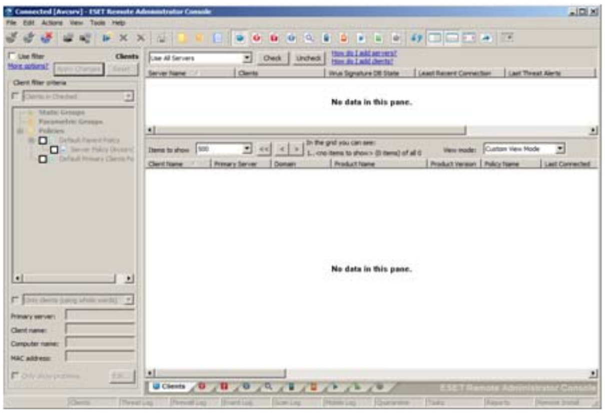


ESET Remote Administrator Console

Note: You are connected to trial version of ESET Remote Administrator Server. Support provided for a limited number of workstations (2) only.

By default, two clients can be managed using ESET Remote Administrator. If you import a test license obtained from ESET, you will be able to manage as many clients as the license permits.

Once we have accepted the message, the ERA console opens:



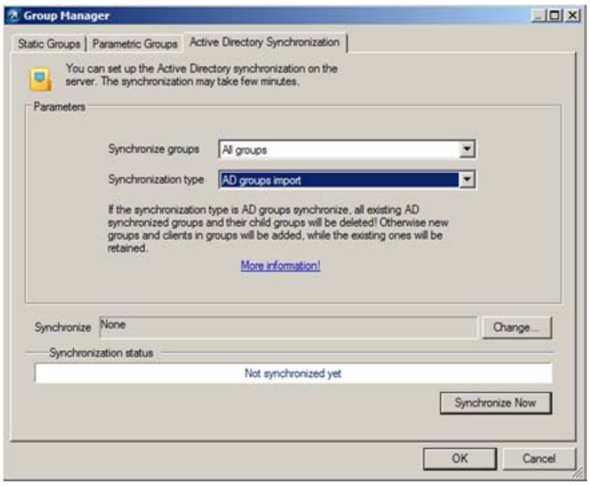
Connected [Avcsrv] - ESET Remote Administrator Console

No data in this pane.

No data in this pane.

The console needs a good deal of getting used to, but offers the users a wide variety of options. Studying the manual is unavoidable. There is a help option within the product, quick start guide and user manual for full feature explanation.

Our first task is to configure the security structure and the clients. To do this, we click on the "Group Manager" button on the taskbar and create the desired group(s). Aside from creating the security structure, dynamic groups can be created – clients become members of these groups based on meeting certain criteria defined at group creation. The Active Directory Import Wizard is very helpful here.



Group Manager

You can set up the Active Directory synchronization on the server. The synchronization may take few minutes.

Parameters

Synchronize groups: All groups

Synchronization type: AD groups import

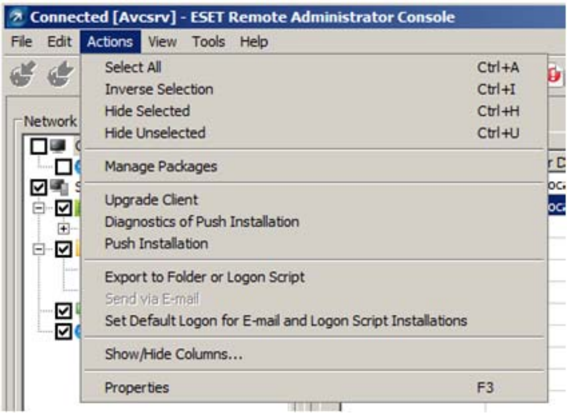
If the synchronization type is AD groups synchronize, all existing AD synchronized groups and their child groups will be deleted! Otherwise new groups and clients in groups will be added, while the existing ones will be retained.

More information!

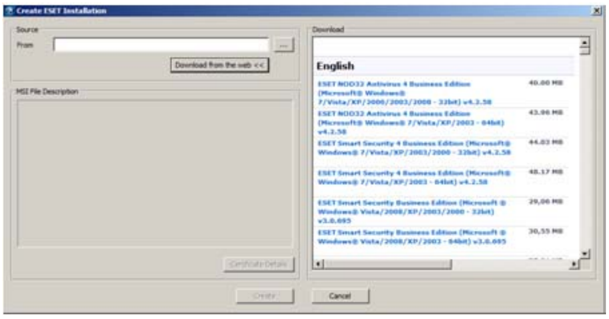
Synchronize: None

Synchronization status: Not synchronized yet

To make the software packets ready for a push installation, we first have to create them, or download them from the manufacturer's website with the help of a wizard.



Connected [Avcsrv] - ESET Remote Administrator Console



Create ESET Installation

Source

From:

MSI File Description

Download

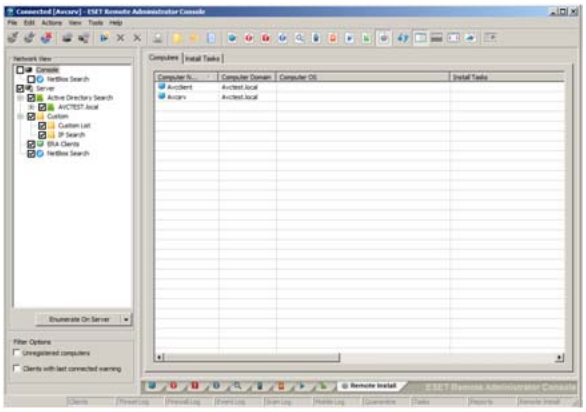
English

ESET NOD32 Antivirus 4 Business Edition (Microsoft® Windows® 7/Vista/XP/2000/2003/2008 - 32bit) v4.2.58	40.00 MB
ESET NOD32 Antivirus 4 Business Edition (Microsoft® Windows® 7/Vista/XP/2003 - 64bit) v4.2.58	43.06 MB
ESET Smart Security 4 Business Edition (Microsoft® Windows® 7/Vista/XP/2003/2000 - 32bit) v4.2.58	44.03 MB
ESET Smart Security 4 Business Edition (Microsoft® Windows® 7/Vista/XP/2003 - 64bit) v4.2.58	48.17 MB
ESET Smart Security Business Edition (Microsoft ® Windows® Vista/2008/XP/2003/2000 - 32bit) v3.0.695	29,06 MB
ESET Smart Security Business Edition (Microsoft ® Windows® Vista/2008/XP/2003 - 64bit) v3.0.695	30,55 MB

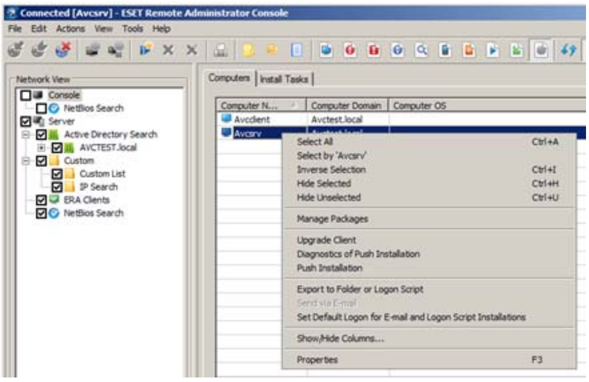
If the relevant MSI files for client installation are already available on the network, these can naturally be used to form the installation packets.

Now we can distribute ESET Smart Security (the client software) to the clients.

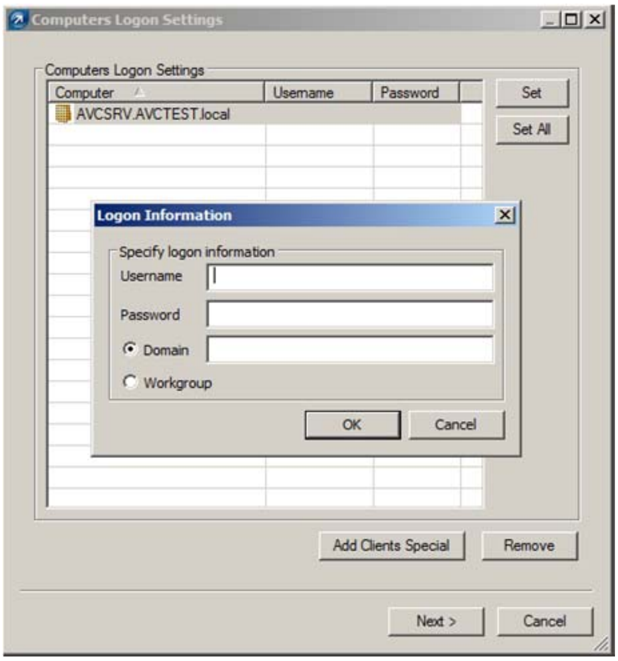
The "Remote Installation" tab allows you to select the client machines to be installed:

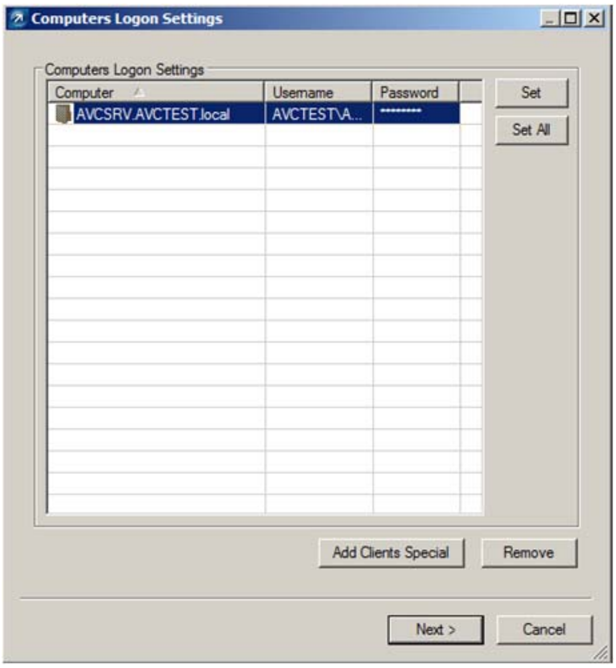


We choose the PCs we want and click on "Push Installation".



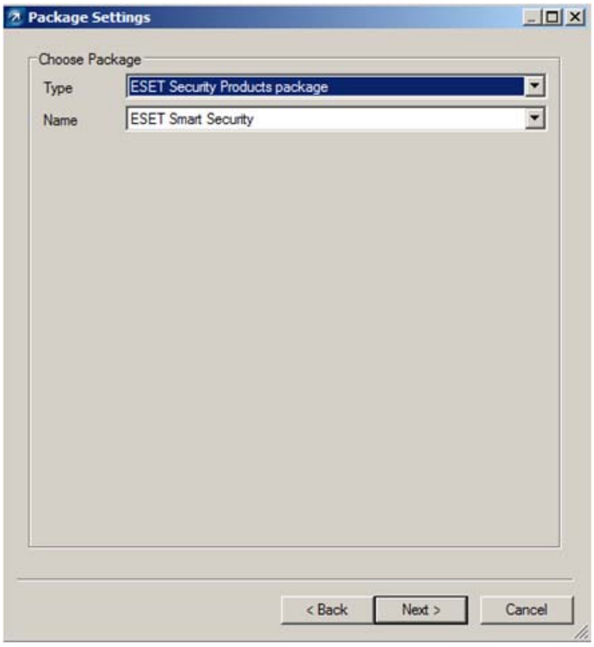
We then need to enter the login details for these machines:





Computer	Username	Password
AVCSRV.AVCTEST.local	AVCTEST\A...	********

The next stage is to choose the package to be installed:



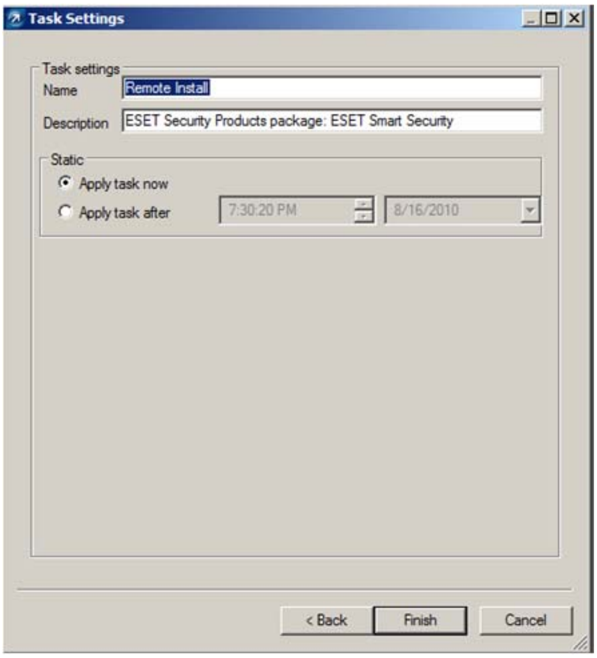
Package Settings

Choose Package

Type: ESET Security Products package

Name: ESET Smart Security

The installation can be carried out immediately, or scheduled for a later time:



Task Settings

Task settings

Name: Remote Install

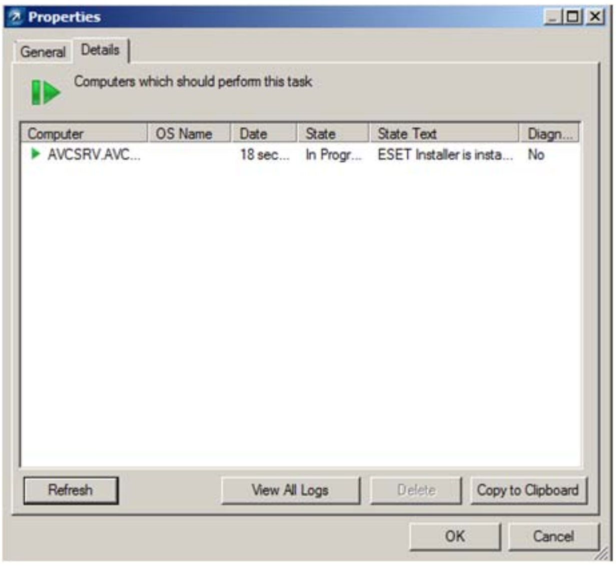
Description: ESET Security Products package: ESET Smart Security

Static

● Apply task now

○ Apply task after 7:30:20 PM 8/16/2010

As with almost all other suites, there is no real-time status, but by clicking on “Task Details” in the context menu, and then “Refresh”, the degree of progress can be seen:



Properties

Computers which should perform this task

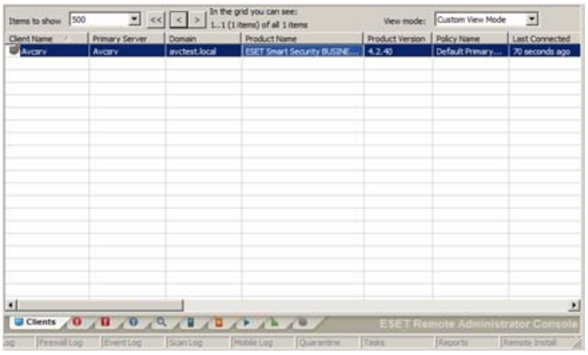
Computer	OS Name	Date	State	State Text	Diagn...
AVCSRV.AVC...		18 sec...	In Progr...	ESET Installer is insta...	No

After a short wait we are informed that installation is complete.

The push installation without interaction improves the user-friendliness of the software.

As in our test last year, we found the filtering and organisational options very comprehensive and good. With ERA 4, ESET has also added a centralized view of the quarantine on the clients; i.e. files that are in quarantine remain on the clients, but the administrator has a centralized view of what has been quarantined and can download the files from the clients for further inspection, delete them or restore them.

The list view with tabs at the bottom of the window for the individual areas is a good solution:

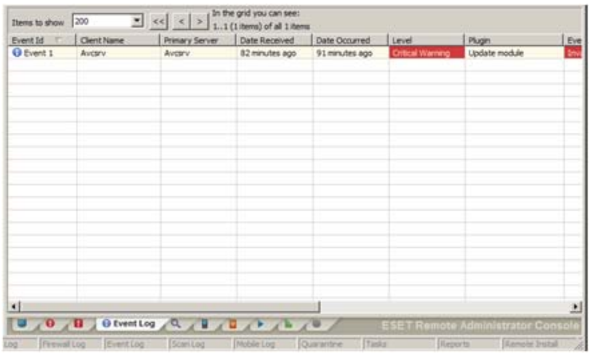


Items to show: 500

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

View mode: Custom View Mode

Client Name	Primary Server	Domain	Product Name	Product Version	Policy Name	Last Connected
Avcsrv	Avcsrv	avctest.local	ESET Smart Security BUSINE...	4.2.40	Default Primary...	70 seconds ago

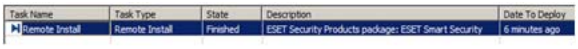


Items to show 200

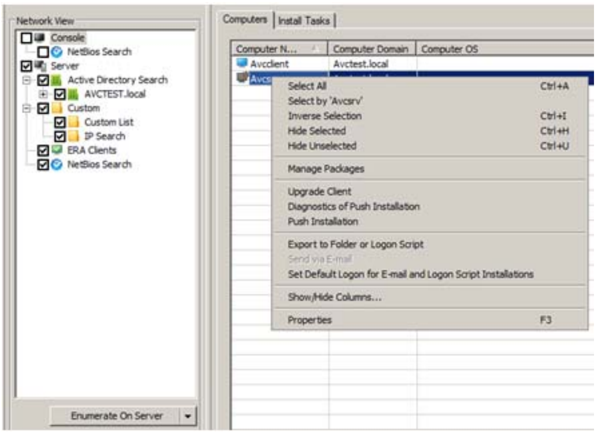
In the grid you can see: 1..1 (1 items) of all 1 items

Event Id	Client Name	Primary Server	Date Received	Date Occurred	Level	Plugin	Eve
Event 1	Avcsrv	Avcsrv	82 minutes ago	91 minutes ago	Critical Warning	Update module	Inv

The variety of functions is strength of the suite. It offers very detailed configuration options, and can thus cope with complex demands. Aside from clients on Windows based systems, the console allows management and configuration of clients running product for Mac OS X, servers running ESET Mail/File/Gateway security solutions, or even mobile clients (ESET Mobile Security for Windows Mobile/Symbian). In other words, it is possible to manage, configure and update all ESET security solutions from a single console.



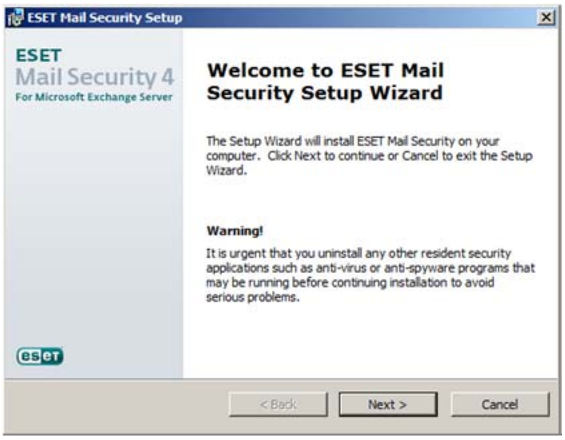
Task Name	Task Type	State	Description	Date To Deploy
Remote Install	Remote Install	Finished	ESET Security Products package: ESET Smart Security	6 minutes ago



Computer N...	Computer Domain	Computer OS
Avcclient	Avctest.local	
Avcs		

Exchange 2007 protection

To start off with, the Exchange protection component has to be installed.



ESET Mail Security Setup

ESET
Mail Security 4
For Microsoft Exchange Server

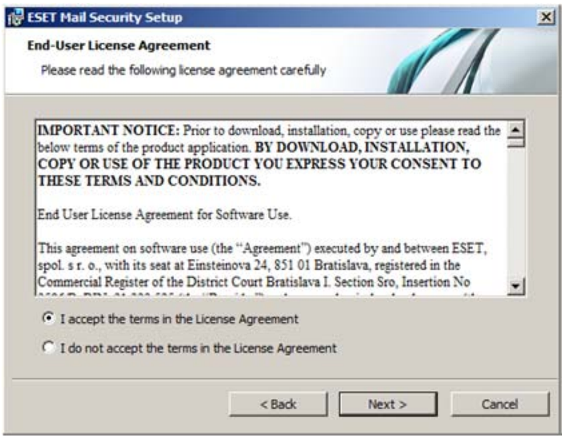
Welcome to ESET Mail Security Setup Wizard

The Setup Wizard will install ESET Mail Security on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Warning!

It is urgent that you uninstall any other resident security applications such as anti-virus or anti-spyware programs that may be running before continuing installation to avoid serious problems.

Once again, there is a licence agreement to accept:



ESET Mail Security Setup

End-User License Agreement

Please read the following license agreement carefully

IMPORTANT NOTICE: Prior to download, installation, copy or use please read the below terms of the product application. BY DOWNLOAD, INSTALLATION, COPY OR USE OF THE PRODUCT YOU EXPRESS YOUR CONSENT TO THESE TERMS AND CONDITIONS.

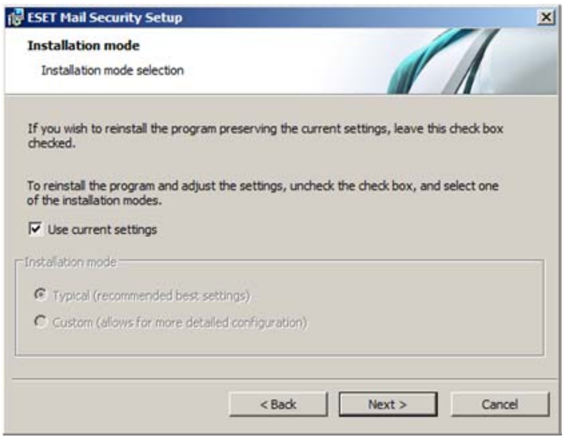
End User License Agreement for Software Use.

This agreement on software use (the "Agreement") executed by and between ESET, spol. s r. o., with its seat at Einsteinova 24, 851 01 Bratislava, registered in the Commercial Register of the District Court Bratislava I. Section Sro, Insertion No

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

There is also a choice of installation options:



ESET Mail Security Setup

Installation mode

Installation mode selection

If you wish to reinstall the program preserving the current settings, leave this check box checked.

To reinstall the program and adjust the settings, uncheck the check box, and select one of the installation modes.

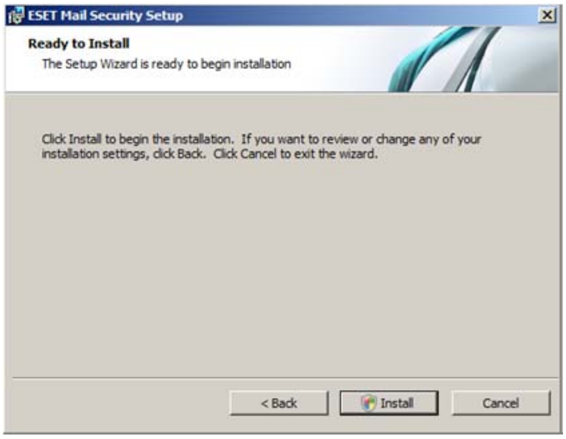
☑ Use current settings

Installation mode

● Typical (recommended best settings)

○ Custom (allows for more detailed configuration)

We have already entered all the information necessary for the installer to begin:

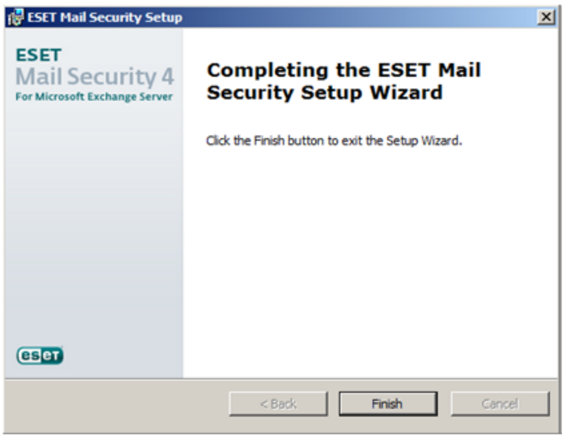


Ready to Install

The Setup Wizard is ready to begin installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Setup is now complete, and we can take a look at the configuration.

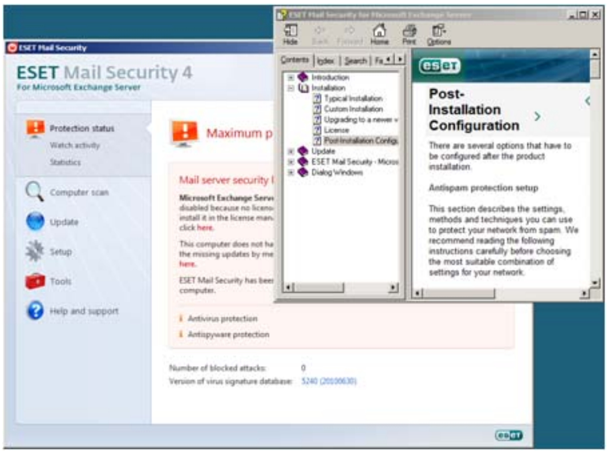


Completing the ESET Mail Security Setup Wizard

Click the Finish button to exit the Setup Wizard.

The Exchange 2007 management interface

Starting the management console also opens the Help window for the initial configuration:



Mail server security l

Microsoft Exchange Serv… disabled because no licens… install it in the license man… click here.

This computer does not ha… the missing updates by me… here.

ESET Mail Security has bee… computer.

Antivirus protection

Antispyware protection

Number of blocked attacks: 0

Version of virus signature database: 5240 (20100630)

Post-Installation Configuration

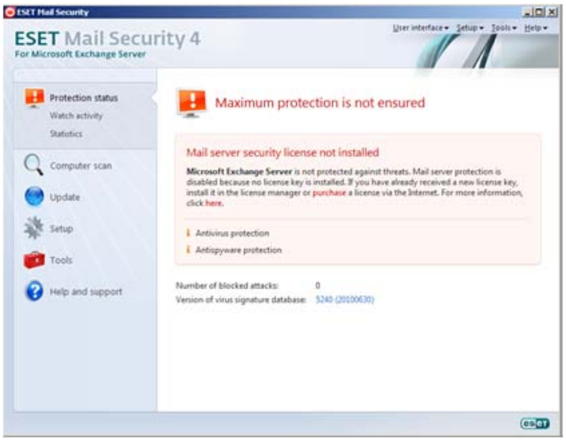
There are several options that have to be configured after the product installation.

Antispam protection setup

This section describes the settings, methods and techniques you can use to protect your network from spam. We recommend reading the following instructions carefully before choosing the most suitable combination of settings for your network.

Mail Security advises a restart, which we carry out.

The management interface is simply and appropriately designed. On the "Protection Status" page we see what needs to be done next. The first step is to enter the licence key.



Maximum protection is not ensured

Mail server security license not installed

Microsoft Exchange Server is not protected against threats. Mail server protection is disabled because no license key is installed. If you have already received a new license key, install it in the license manager or purchase a license via the Internet. For more information, click here.

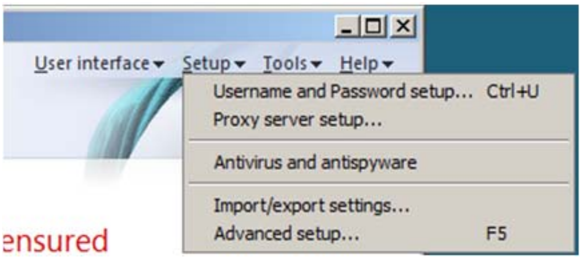
Antivirus protection

Antispyware protection

Number of blocked attacks: 0

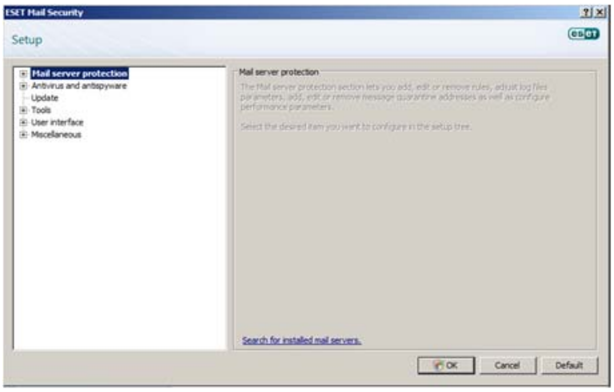
Version of virus signature database: 5240 (20100630)

Extended configuration options can be found by clicking on the "Setup" menu, then "Advanced Setup".


User interface
Setup
Tools
Help
Username and Password setup... Ctrl+U
Proxy server setup...
Antivirus and antispyware
Import/export settings...
Advanced setup... F5
ensured

If the standard options available are insufficient for you, you can use this advanced menu to find all available settings.

The choice of a simple or an advanced interface is very convenient, and makes it easy for less experienced users to configure the Exchange protection.



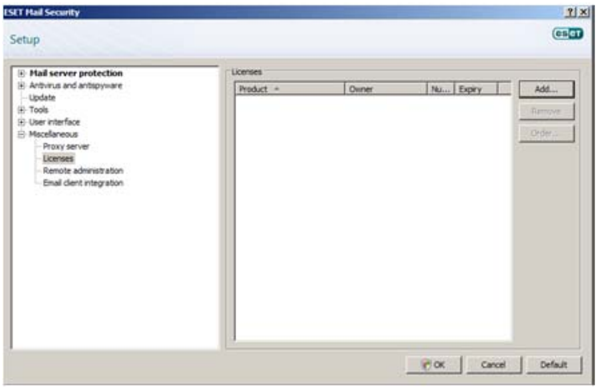
Mail server protection

The Mail server protection section lets you add, edit or remove rules, adjust log files parameters, add, edit or remove message quarantine addresses as well as configure performance parameters.

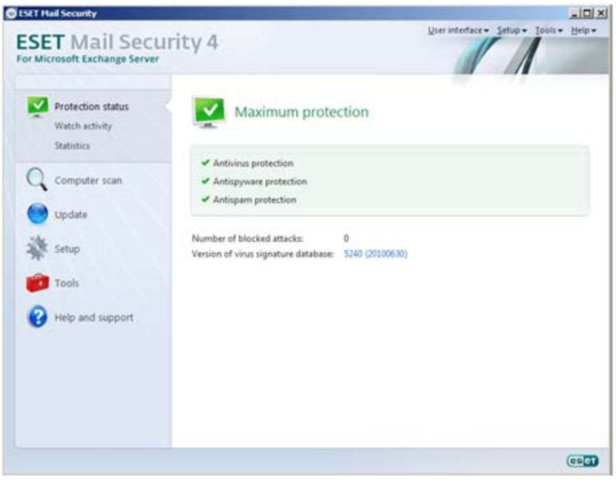
Select the desired item you want to configure in the setup tree.

Search for installed mail servers.

To enter the licence key, we click on "Miscellaneous" and then "License".



As soon as we have entered a valid licence, we can see that the status indicators in the Mail Security window have all turned to green:

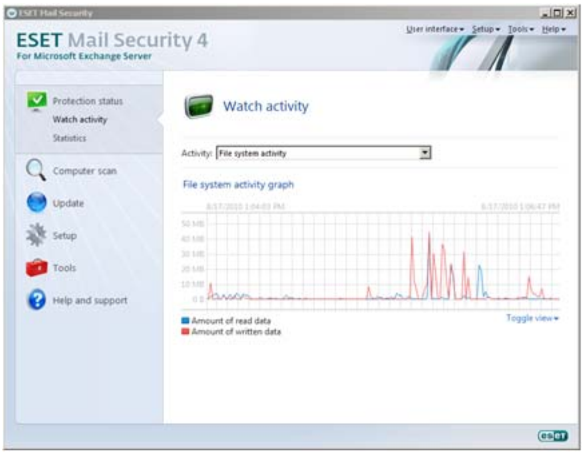


Maximum protection

✓ Antivirus protection
✓ Antispyware protection
✓ Antispam protection

Number of blocked attacks: 0
Version of virus signature database: 5240 (20100630)

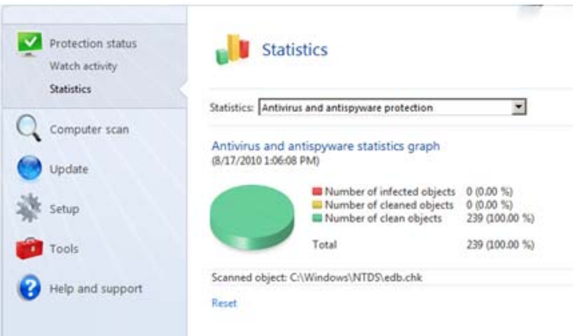
Most users will be happy with the Standard view, although the Advanced view is useful for anyone needing to set up very complex configurations.



Activity: File system activity

File system activity graph

🟦 Amount of read data
🟥 Amount of written data

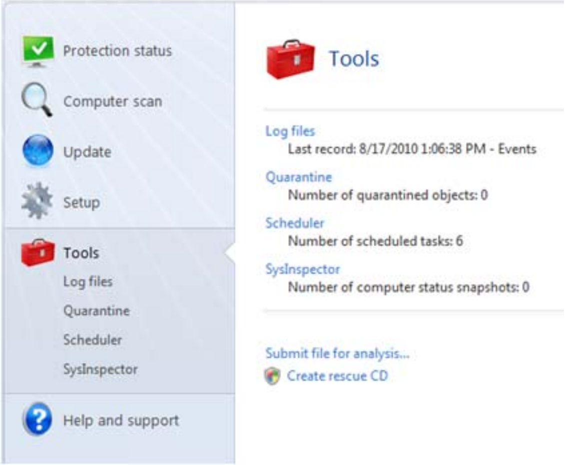


Statistics: Antivirus and antispyware protection

Antivirus and antispyware statistics graph
(8/17/2010 1:06:08 PM)

🟥 Number of infected objects	0 (0.00 %)
🟨 Number of cleaned objects	0 (0.00 %)
🟩 Number of clean objects	239 (100.00 %)
Total	239 (100.00 %)

Scanned object: C:\Windows\NTDS\edb.chk



Log files
Last record: 8/17/2010 1:06:38 PM - Events

Quarantine
Number of quarantined objects: 0

Scheduler
Number of scheduled tasks: 6

SysInspector
Number of computer status snapshots: 0

Anyone who knows their way around the ESET Smart Security Client will feel at home with the interface of Mail Security. Configuration can be carried out quickly and easily.

Manufacturer's website

The website, www.eset.com, is suitably clear and simple, and conforms to current standards.

The site gives basic information about ESET products, and there is an online scanner available to download.

ESET is one of very few manufacturers to limit the functionality of their test software. Additionally, it is only possible to obtain a test licence by contacting a member of their sales team. Some users may regard this as an unnecessary hurdle, although it does mean that users will be properly advised before installing the software.

The installation process

The installation is in itself very straightforward and simple. Hardly any information needs to be entered. Any necessary configuration changes can be made afterwards.

We suggest that ESET should reconsider the Microsoft Jet Engine as the default database.

The administrator console

The management console is very extensive and offers sometimes an too abundant choice of configuration possibilities for maximum customization.

Thorough consultation of the manual is indispensible or has to consult the in-product help.

The icons are arranged so as to enable a good overview. The system is well designed and allows individual systems to be found and configured easily, even in extremely big network environments.

Deployment areas

"The ESET suite can scale for very large networks."

Antivirus clients

There are no complaints about the client software, which is well designed and simple to use.

Summary

The management console takes a lot of time and effort to investigate and understand, but compensates for this with an abundance of configuration possibilities.

The management console shows the status at a glance. The Exchange protection is very simple to configure and cannot be faulted.

All in all, the product is a really well done software for enterprise environments.

Pros

+ Very simple installation
+ Very good organisational features
+ Ideal for very large networks

Cons

- Use of the manual is unavoidable when installing ERA console
- Partially complicated admin interface

Deployment areas

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★	★★★★	★★★★★

Summary

Installation Wizard	★★★★
User Navigation	★★★
Administrator console	★★★★
Default Values	★★★★
MS Active Directory Support	★★★
Database Support	★★★
Remote Installation	★★★
Website	★★★★★
Manual	★★★★

G Data

Test Software:

G Data Endpoint Protection Enterprise

→ Client Protection

→ Mail Server Protection

→ Admin Console & File Server Protection

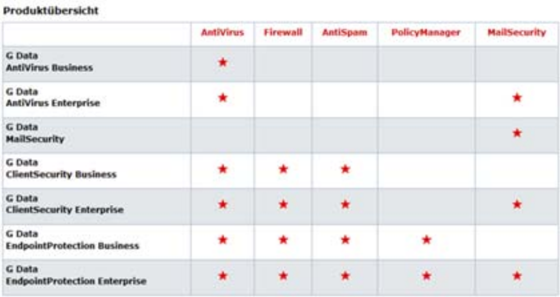
Installation

Downloading the product

It is easy to find your way around the website, which is clear and simple. There is no difficulty finding the products you want, and all software can be downloaded as a fully functional version.

Most modules come as an ISO file, weighing in at 1.3 GB. It's important to allow enough time to download this much. Fortunately, G Data's servers have high-speed connections.

There is of course an overview of the functions contained in the different suites:



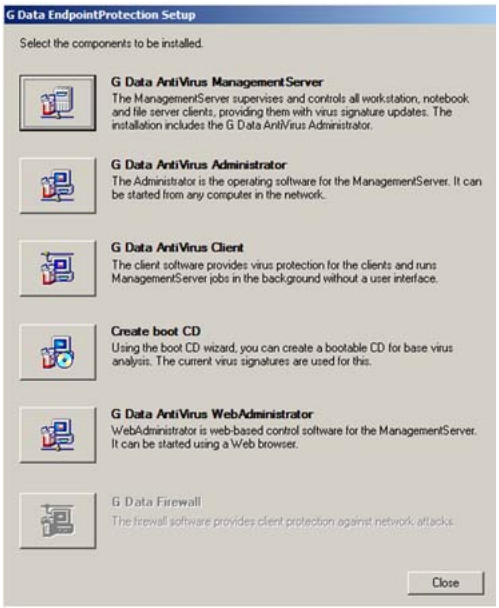
Produktübersicht

	AntiVirus	Firewall	AntiSpam	PolicyManager	MailSecurity
G Data AntiVirus Business	★				
G Data AntiVirus Enterprise	★				★
G Data MailSecurity					★
G Data ClientSecurity Business	★	★	★		
G Data ClientSecurity Enterprise	★	★	★		★
G Data EndpointProtection Business	★	★	★	★	
G Data EndpointProtection Enterprise	★	★	★	★	★

Product installation

We begin with the installation of the management server, which is then used to install the other products.

We were very pleased to see that G Data, as one of very few manufacturers, produces one installer that will install the whole suite. The installation of the management server also includes the AntiVirus Administrator, which will be used later to carry out the remote installation of the clients.



G Data EndpointProtection Setup

Select the components to be installed.

G Data AntiVirus ManagementServer
The ManagementServer supervises and controls all workstation, notebook and file server clients, providing them with virus signature updates. The installation includes the G Data AntiVirus Administrator.

G Data AntiVirus Administrator
The Administrator is the operating software for the ManagementServer. It can be started from any computer in the network.

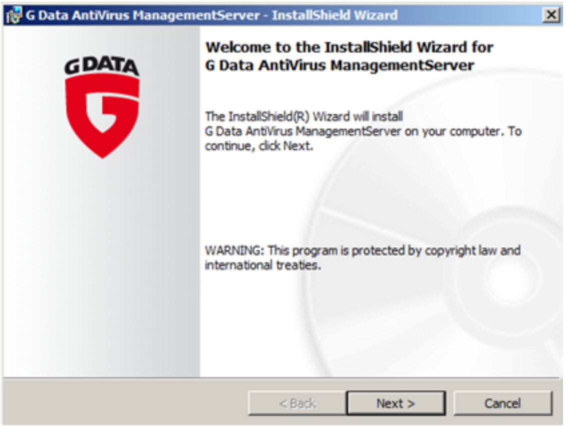
G Data AntiVirus Client
The client software provides virus protection for the clients and runs ManagementServer jobs in the background without a user interface.

Create boot CD
Using the boot CD wizard, you can create a bootable CD for base virus analysis. The current virus signatures are used for this.

G Data AntiVirus WebAdministrator
WebAdministrator is web-based control software for the ManagementServer. It can be started using a Web browser.

G Data Firewall
The firewall software provides client protection against network attacks.

We start at the beginning with the G Data AntiVirus Management Server:



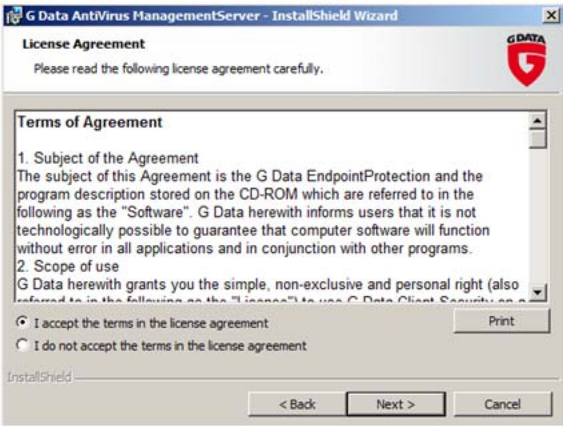
G Data AntiVirus ManagementServer - InstallShield Wizard

Welcome to the InstallShield Wizard for G Data AntiVirus ManagementServer

The InstallShield(R) Wizard will install G Data AntiVirus ManagementServer on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

As usual, there's a licence agreement to accept:



G Data AntiVirus ManagementServer - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

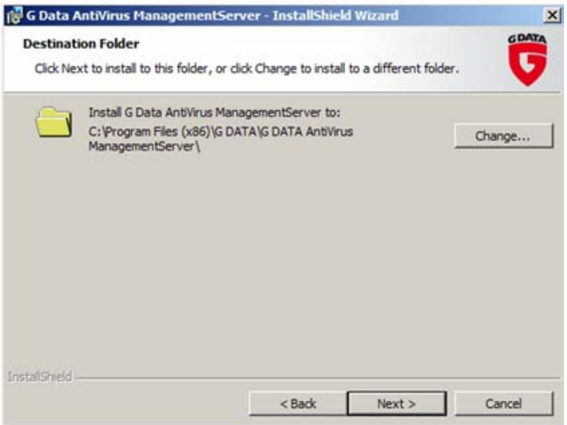
Terms of Agreement

1. Subject of the Agreement
The subject of this Agreement is the G Data EndpointProtection and the program description stored on the CD-ROM which are referred to in the following as the "Software". G Data herewith informs users that it is not technologically possible to guarantee that computer software will function without error in all applications and in conjunction with other programs.
2. Scope of use
G Data herewith grants you the simple, non-exclusive and personal right (also referred to in the following as the "Licence") to use G Data Client Security on a

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Next we choose the installation folder:



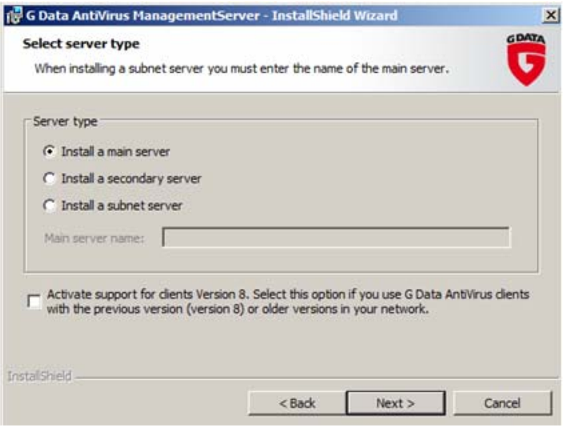
G Data AntiVirus ManagementServer - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install G Data AntiVirus ManagementServer to:
C:\Program Files (x86)\G DATA\G DATA AntiVirus ManagementServer\

Now we can decide on the type of server to be installed. Compatibility mode for earlier client versions can also be selected here. You can see that G Data also allows you to install secondary and local servers, to enable easier distribution in large networks.



G Data AntiVirus ManagementServer - InstallShield Wizard

Select server type

When installing a subnet server you must enter the name of the main server.

Server type

● Install a main server

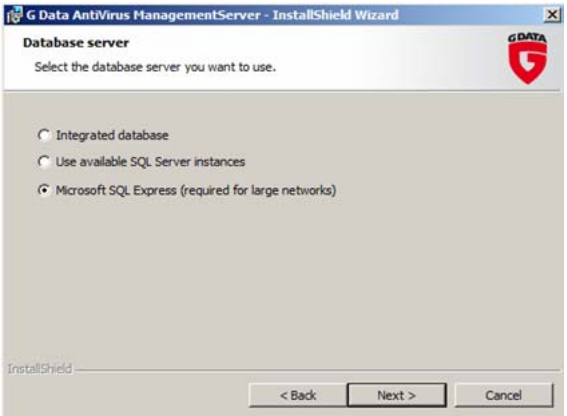
○ Install a secondary server

○ Install a subnet server

Main server name:

□ Activate support for clients Version 8. Select this option if you use G Data AntiVirus clients with the previous version (version 8) or older versions in your network.

The next selection also allows for scalability of the security system. Settings can be stored in an integrated database, an existing SQL server instance, or SQL Express. The SQL Express option states that it is "required for large networks", which gives inexperienced users a completely false impression. If you have a own SQL server, there is no need for the Express version, you can use your SQL server.



G Data AntiVirus ManagementServer - InstallShield Wizard

Database server

Select the database server you want to use.

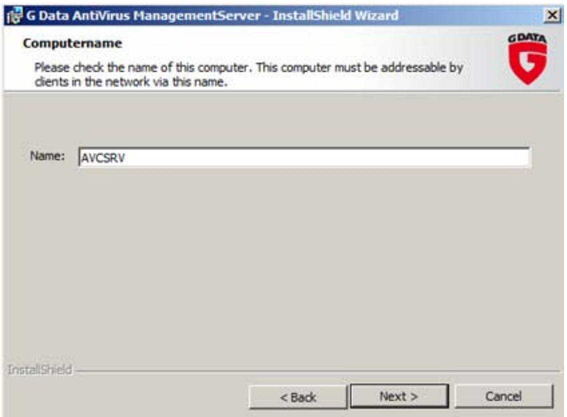
○ Integrated database

○ Use available SQL Server instances

● Microsoft SQL Express (required for large networks)

As we don't have an SQL server in our test environment, we use the integrated database for our test.

The next step is to confirm the hostname of the computer being installed, via which it can be accessed by client PCs:



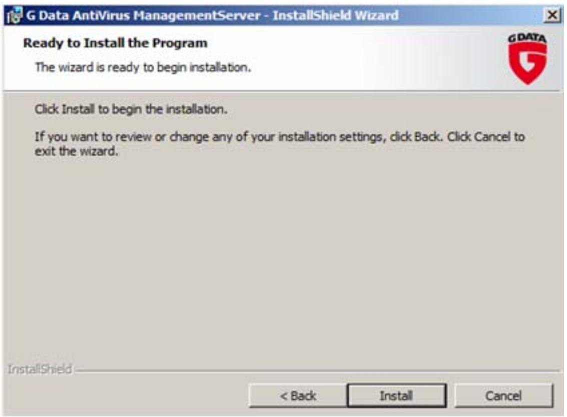
G Data AntiVirus ManagementServer - InstallShield Wizard

Computername

Please check the name of this computer. This computer must be addressable by clients in the network via this name.

Name: AVCSRV

The installer now has all the information it needs to begin the installation process.



G Data AntiVirus ManagementServer - InstallShield Wizard

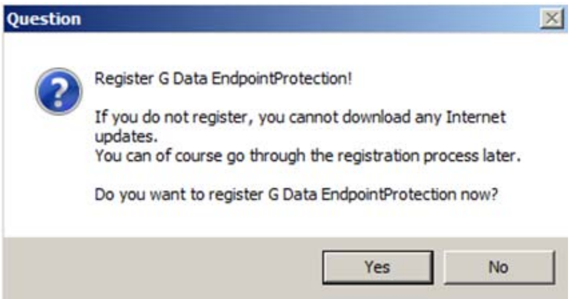
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

When installation has successfully completed, we have to decide whether to register:

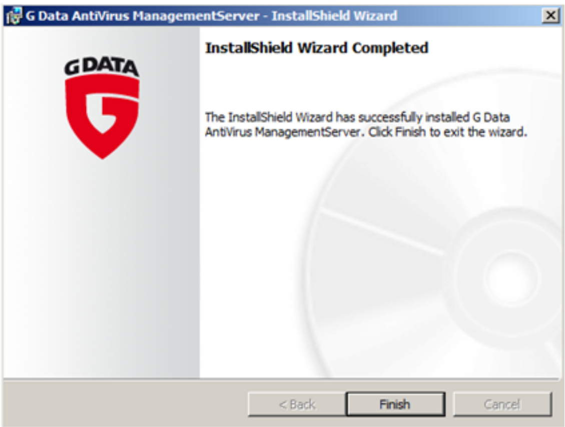


Question

Register G Data EndpointProtection!

If you do not register, you cannot download any Internet updates.
You can of course go through the registration process later.

Do you want to register G Data EndpointProtection now?

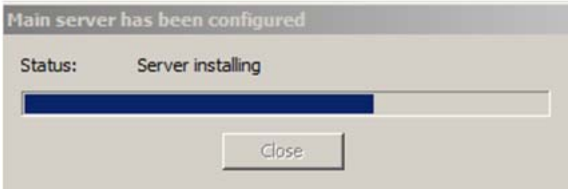


G Data AntiVirus ManagementServer - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed G Data AntiVirus ManagementServer. Click Finish to exit the wizard.

Services and servers are then installed and configured:

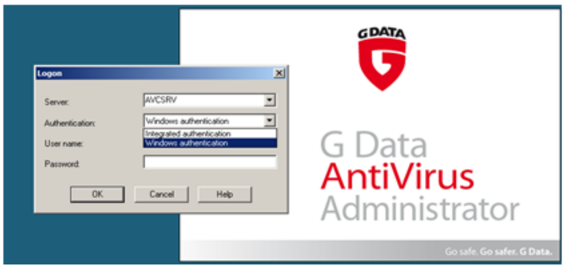


Main server has been configured

Status: Server installing

The management interface

When the administration console first starts, we are asked for logon credentials, and given a choice of integrated or Windows authentication:



Logon

Server: AVCSRV

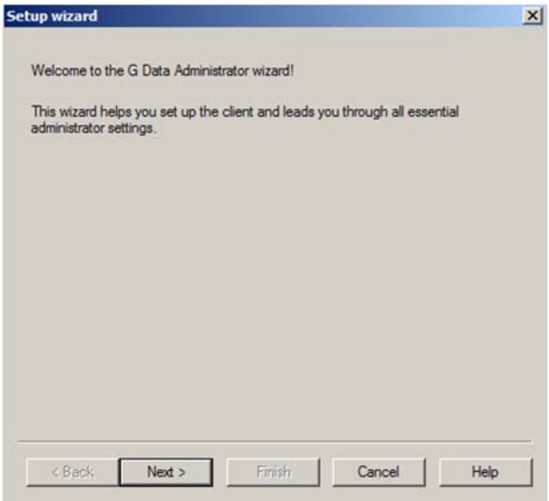
Authentication: Windows authentication

Integrated authentication
Windows authentication

User name:

Password:

Once we have entered the correct logon details, the management console opens and the setup wizard starts:

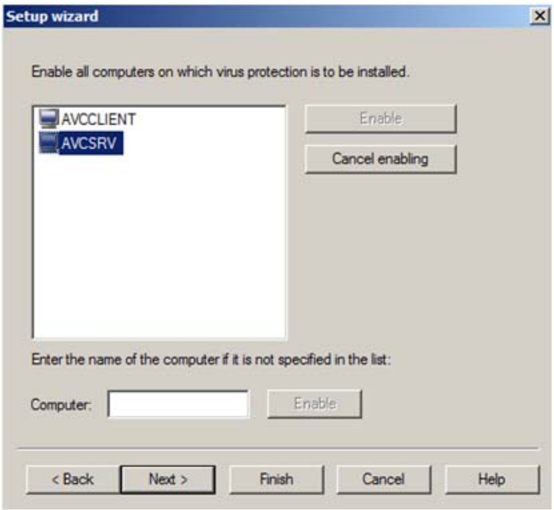


Setup wizard

Welcome to the G Data Administrator wizard!

This wizard helps you set up the client and leads you through all essential administrator settings.

The next step is to select the computers in our network that we need to protect. It is of course possible to manually add any computers that don't appear in the list.



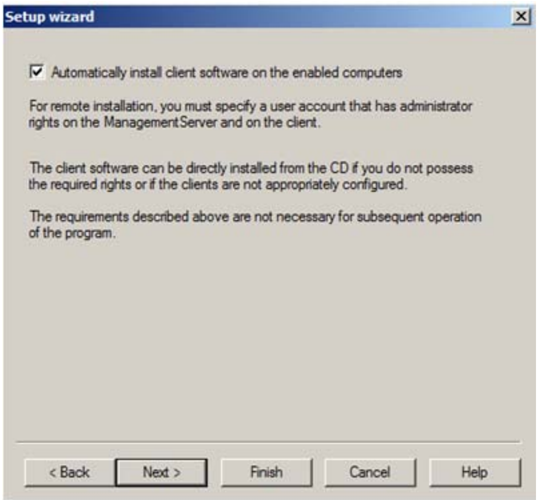
Enable all computers on which virus protection is to be installed.

AVCCLIENT
AVCSRV

Enter the name of the computer if it is not specified in the list:

Computer:

The wizard then asks if we want to install the client protection automatically, which we confirm.



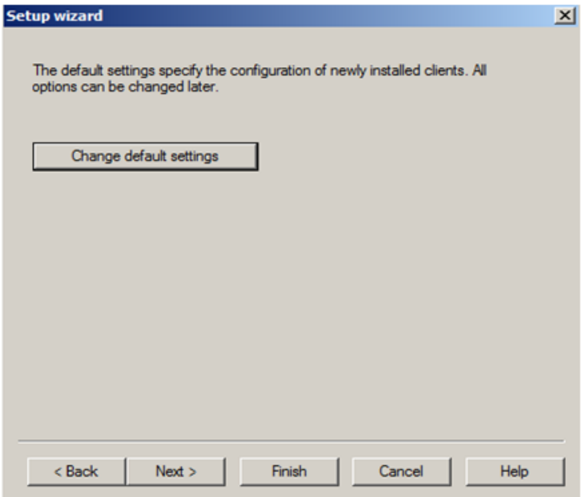
☑ Automatically install client software on the enabled computers

For remote installation, you must specify a user account that has administrator rights on the ManagementServer and on the client.

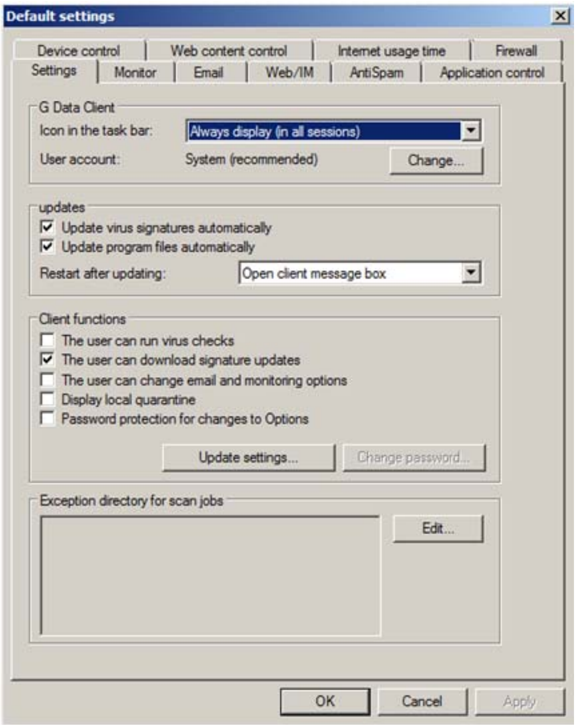
The client software can be directly installed from the CD if you do not possess the required rights or if the clients are not appropriately configured.

The requirements described above are not necessary for subsequent operation of the program.

The next part of setup is the opportunity to change the default settings for the client installation, which can be done very easily.



The default settings specify the configuration of newly installed clients. All options can be changed later.



G Data Client

Icon in the task bar: Always display (in all sessions)

User account: System (recommended)

updates

☑ Update virus signatures automatically

☑ Update program files automatically

Restart after updating: Open client message box

Client functions

☐ The user can run virus checks

☑ The user can download signature updates

☐ The user can change email and monitoring options

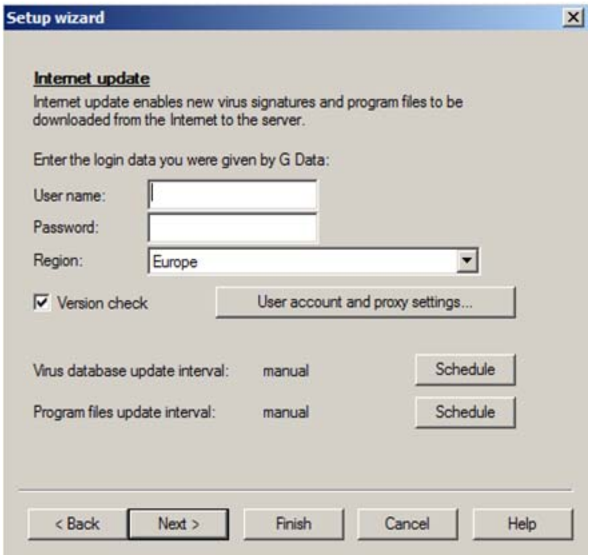
☐ Display local quarantine

☐ Password protection for changes to Options

Exception directory for scan jobs

It is of course possible to change these settings later. In this case we rely on G Data's default settings and don't make any changes.

After this, we can change Internet update settings, to optimise virus updates for the clients. The default configuration is manual, but can easily be changed to one's own requirements.



Setup wizard

Internet update

Internet update enables new virus signatures and program files to be downloaded from the Internet to the server.

Enter the login data you were given by G Data:

User name:

Password:

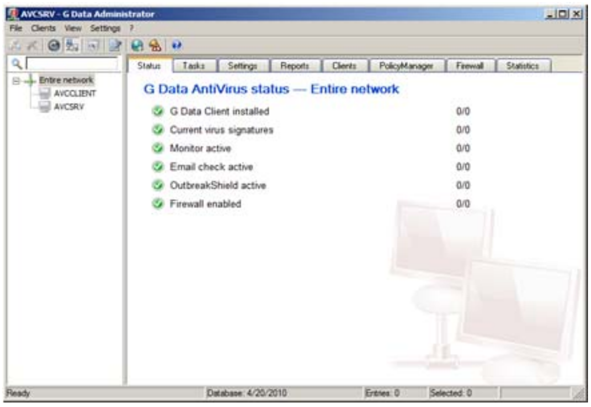
Region: Europe

☑ Version check

Virus database update interval: manual

Program files update interval: manual

When the wizard has finished, we open the G Data Administrator, which shows a status overview:



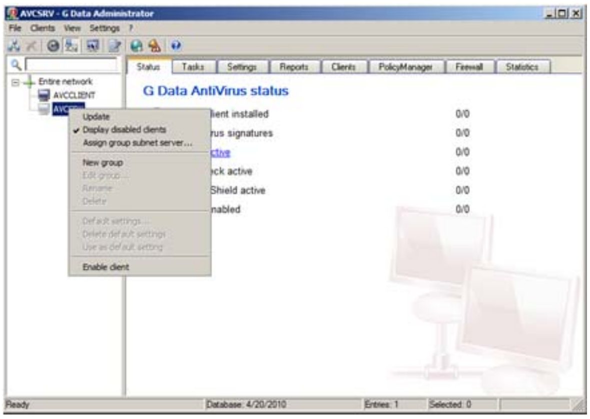
AVCSRV - G Data Administrator

G Data AntiVirus status — Entire network

G Data Client installed	0/0
Current virus signatures	0/0
Monitor active	0/0
Email check active	0/0
OutbreakShield active	0/0
Firewall enabled	0/0

Ready | Database: 4/20/2010 | Entries: 0 | Selected: 0

In the left-hand pane of the window we see a list of all the PCs in the network. You can easily right-click on a machine and activate the G Data client software. There is also the option of forming groups to make larger networks more manageable:

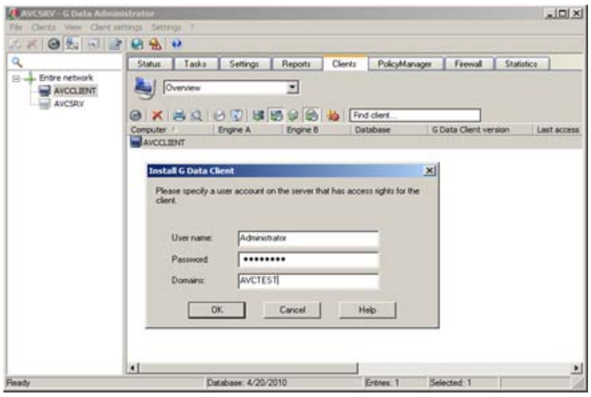


AVCSRV - G Data Administrator

G Data AntiVirus status

Ready | Database: 4/20/2010 | Entries: 1 | Selected: 0

Now we are ready to carry out the remote installation of the clients. To do this, we click on the “Clients” tab and select “Install G Data Client”.



Install G Data Client

Please specify a user account on the server that has access rights for the client.

User name: Administrator

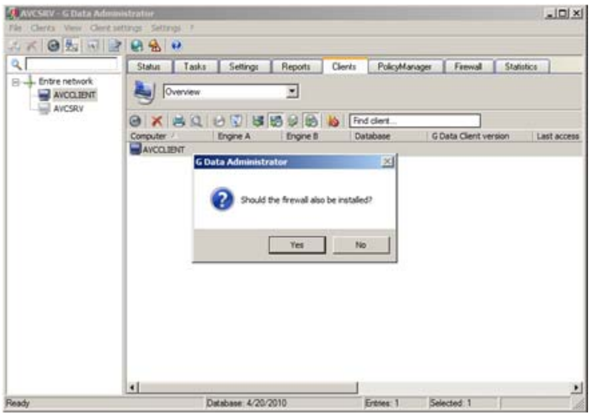
Password: ••••••••

Domain: AVCTEST

Ready | Database: 4/20/2010 | Entries: 1 | Selected: 1

We notice that G Data is a leader with regard to user interface design and intuitive use of the software.

After the access credentials have been entered, we are asked if the G Data client firewall should also be installed:

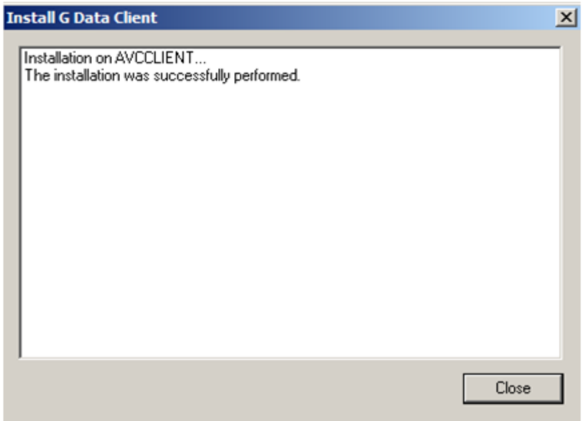


G Data Administrator

Should the firewall also be installed?

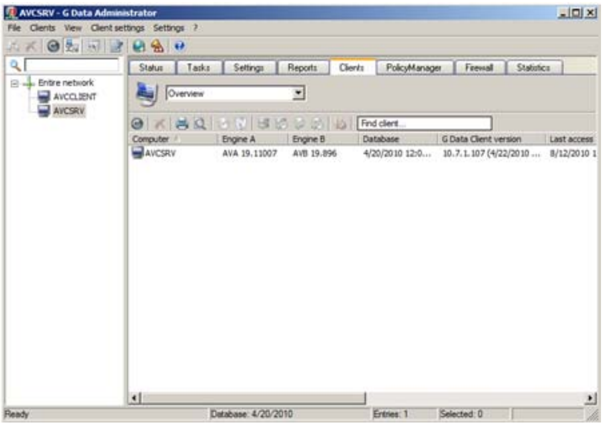
Ready | Database: 4/20/2010 | Entries: 1 | Selected: 1

Unfortunately, there is no real-time progress display, and the messages provided by the status windows can only be described as Spartan:



Installation on AVCCLIENT...
The installation was successfully performed.

However, the client installation completes very quickly and easily, and in just a few moments the remote client is installed.
All further work can be carried out using the G Data Administrator, be it generating reports with various criteria, or changing client settings. An obvious plus point is that there is a preconfigured button for each standard action, so there is no need to go searching through menus.
It is very convenient to be able to install the AV client software on the server itself, using the Administrator. It is exactly the same as installing the software on a client

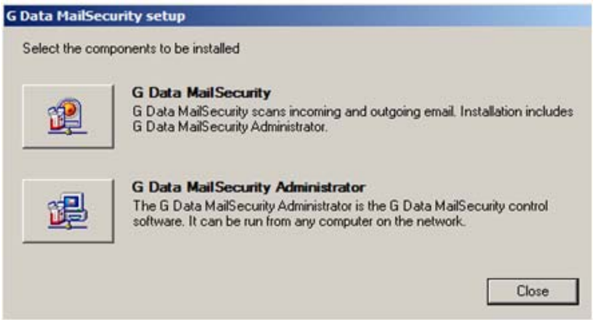


Computer	Engine A	Engine B	Database	G Data Client version	Last access
AVCSRV	AVA 19.11007	AVB 19.896	4/20/2010 12:0...	10.7.1.107 (4/22/2010 ...	8/12/2010 1

Ready | Database: 4/20/2010 | Entries: 1 | Selected: 0

Exchange 2007 protection

We start with the installation of Mail Security. Here again it is pleasing to see one installer for all the mail products. Installing G Data Mail Security also installs the Administrator, although the latter can also be installed separately.



Select the components to be installed

G Data MailSecurity
G Data MailSecurity scans incoming and outgoing email. Installation includes G Data MailSecurity Administrator.

G Data MailSecurity Administrator
The G Data MailSecurity Administrator is the G Data MailSecurity control software. It can be run from any computer on the network.

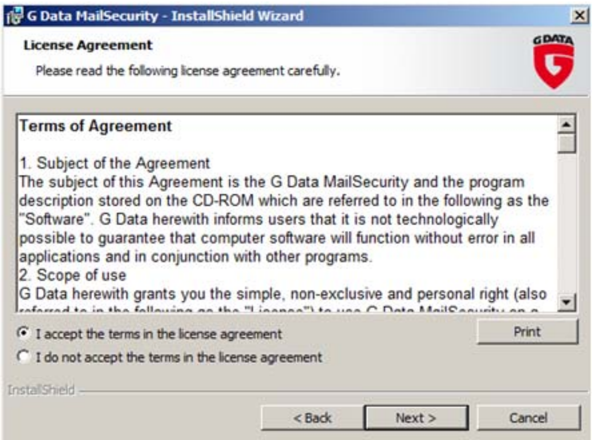
The setup wizard starts after the installation files have been unpacked.

Welcome to the InstallShield Wizard for G Data MailSecurity

The InstallShield(R) Wizard will install G Data MailSecurity on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

First we have to accept the licence agreement.



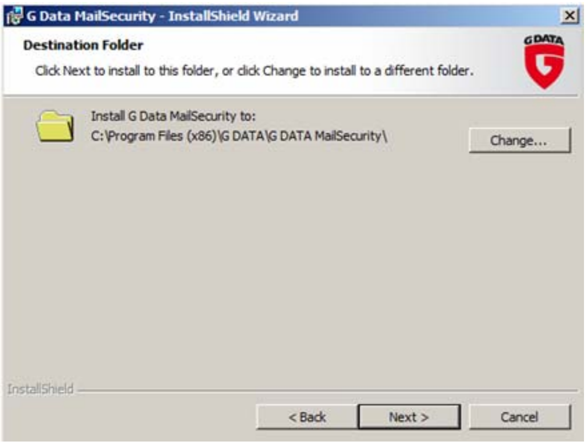
License Agreement
Please read the following license agreement carefully.

Terms of Agreement

1. Subject of the Agreement
The subject of this Agreement is the G Data MailSecurity and the program description stored on the CD-ROM which are referred to in the following as the "Software". G Data herewith informs users that it is not technologically possible to guarantee that computer software will function without error in all applications and in conjunction with other programs.
2. Scope of use
G Data herewith grants you the simple, non-exclusive and personal right (also

● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement

The next step is to choose the installation folder:



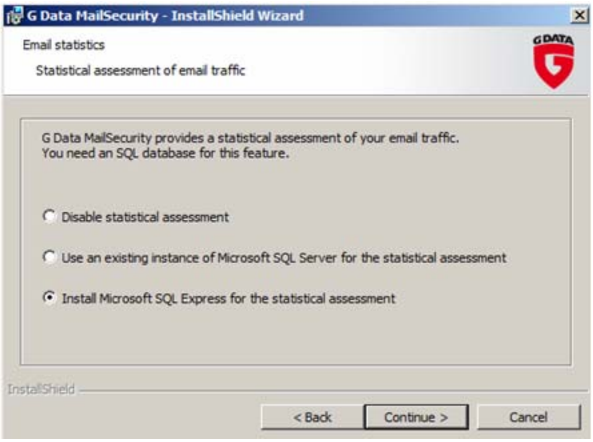
G Data MailSecurity - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install G Data MailSecurity to:
C:\Program Files (x86)\G DATA\G DATA MailSecurity\

Of course, a database will be necessary for statistics and reports in the background. Once again, there is a choice of using an existing SQL Server instance, or installing SQL Express. This time, the misleading message about using SQL Express for large networks has gone:



G Data MailSecurity - InstallShield Wizard

Email statistics

Statistical assessment of email traffic

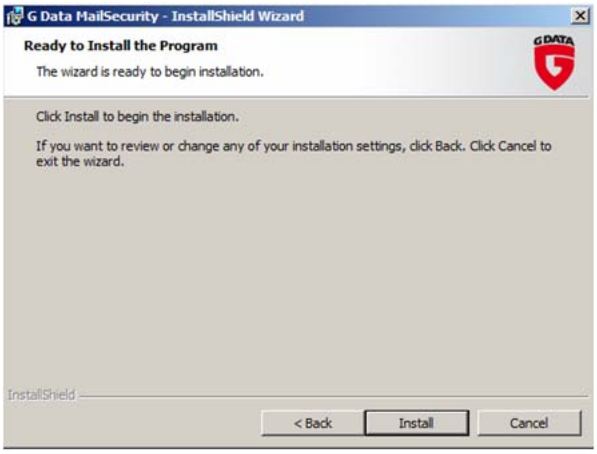
G Data MailSecurity provides a statistical assessment of your email traffic.
You need an SQL database for this feature.

○ Disable statistical assessment

○ Use an existing instance of Microsoft SQL Server for the statistical assessment

● Install Microsoft SQL Express for the statistical assessment

The installer now has all the information it needs to begin.



G Data MailSecurity - InstallShield Wizard

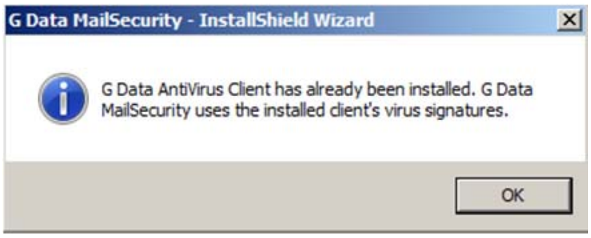
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

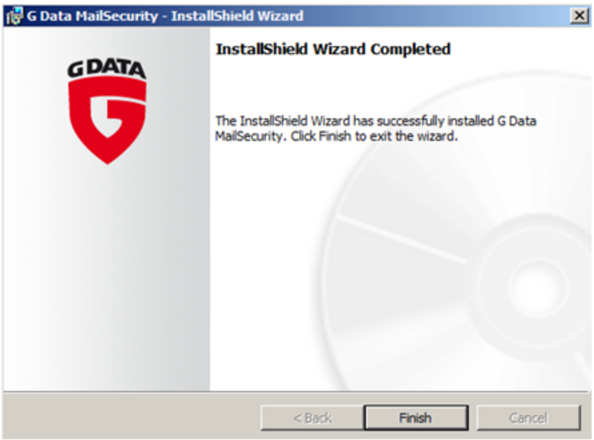
During the installation it will be automatically be recognised that the AV client is installed on the server, and the user is shown a message that its virus database will be used by MailSecurity:



G Data MailSecurity - InstallShield Wizard

G Data AntiVirus Client has already been installed. G Data MailSecurity uses the installed client's virus signatures.

When the installation is complete, we can start the administration console and start configuring.



G Data MailSecurity - InstallShield Wizard

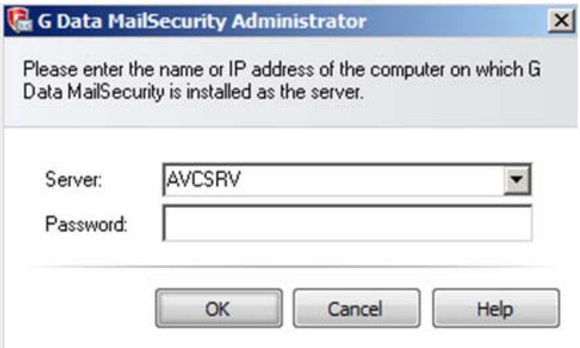
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed G Data MailSecurity. Click Finish to exit the wizard.

The MailSecurity management interface

After the installation, we start the administrator console.

Here too, a password has to be entered:

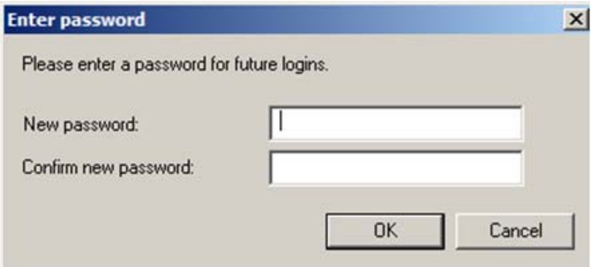


Please enter the name or IP address of the computer on which G Data MailSecurity is installed as the server.

Server: AVCSRV

Password:

As we have not yet set up a password for MailSecurity administration, we have to do this now:



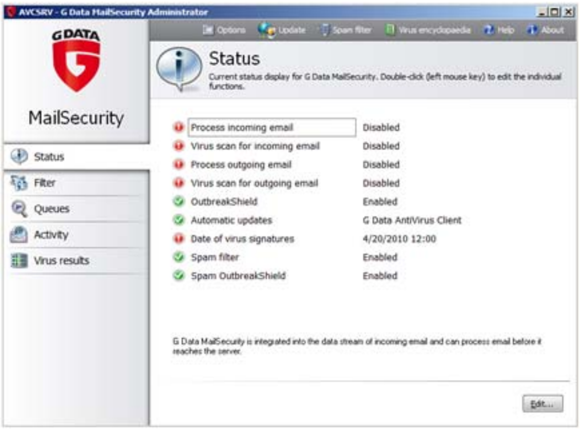
Please enter a password for future logins.

New password:

Confirm new password:

Once again it is clear here that G Data is at the forefront of simple user interface design. All essential information is shown on the first page of the intuitive interface.

The warning indicators show the administrator immediately which areas need immediate attention:



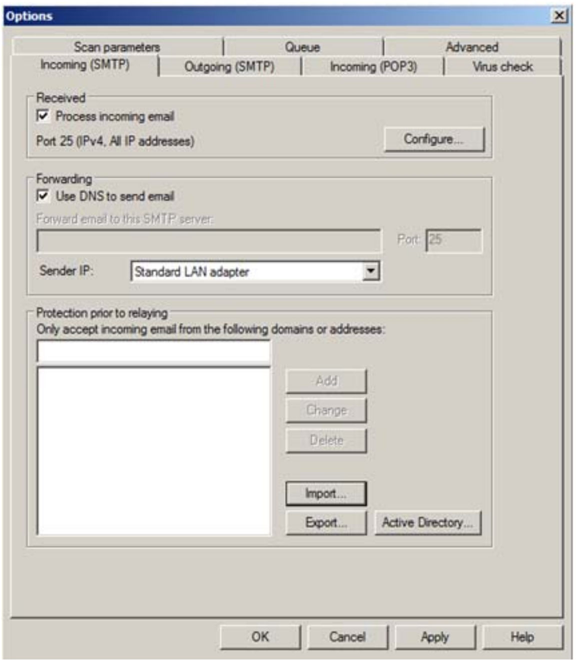
Status

Current status display for G Data MailSecurity. Double-click (left mouse key) to edit the individual functions.

Process incoming email	Disabled
Virus scan for incoming email	Disabled
Process outgoing email	Disabled
Virus scan for outgoing email	Disabled
OutbreakShield	Enabled
Automatic updates	G Data AntiVirus Client
Date of virus signatures	4/20/2010 12:00
Spam filter	Enabled
Spam OutbreakShield	Enabled

G Data MailSecurity is integrated into the data stream of incoming email and can process email before it reaches the server.

To make configuration changes, we click on "Options". The dialog box has tabs to show the different areas, starting by default with incoming security:



Received

☑ Process incoming email

Port 25 (IPv4, All IP addresses)

Forwarding

☑ Use DNS to send email

Forward email to this SMTP server:

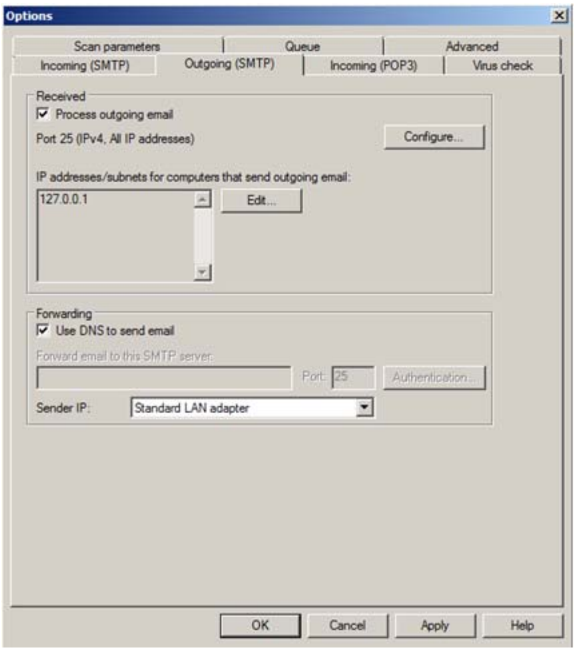
Port: 25

Sender IP: Standard LAN adapter

Protection prior to relaying

Only accept incoming email from the following domains or addresses:

The Incoming tab allows groups etc. to be imported from Active Directory, which is a very useful feature.



Received

☑ Process outgoing email

Port 25 (IPv4, All IP addresses)

IP addresses/subnets for computers that send outgoing email:

127.0.0.1

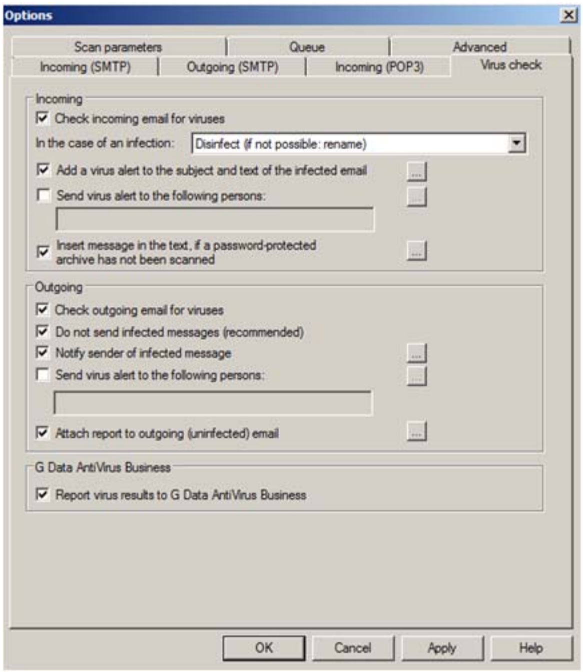
Forwarding

☑ Use DNS to send email

Forward email to this SMTP server:

Port: 25

Sender IP: Standard LAN adapter



Incoming

☑ Check incoming email for viruses

In the case of an infection: Disinfect (if not possible: rename)

☑ Add a virus alert to the subject and text of the infected email

☐ Send virus alert to the following persons:

☑ Insert message in the text, if a password-protected archive has not been scanned

Outgoing

☑ Check outgoing email for viruses

☑ Do not send infected messages (recommended)

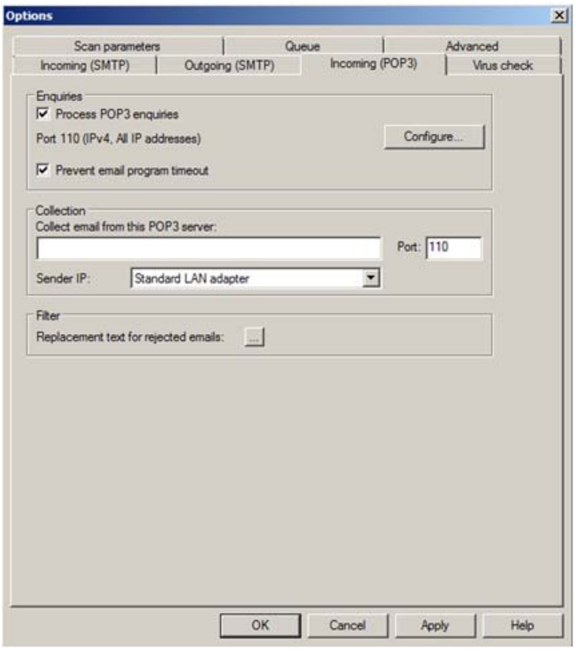
☑ Notify sender of infected message

☐ Send virus alert to the following persons:

☑ Attach report to outgoing (uninfected) email

G Data AntiVirus Business

☑ Report virus results to G Data AntiVirus Business



Enquiries

☑ Process POP3 enquiries

Port 110 (IPv4, All IP addresses)

☑ Prevent email program timeout

Collection

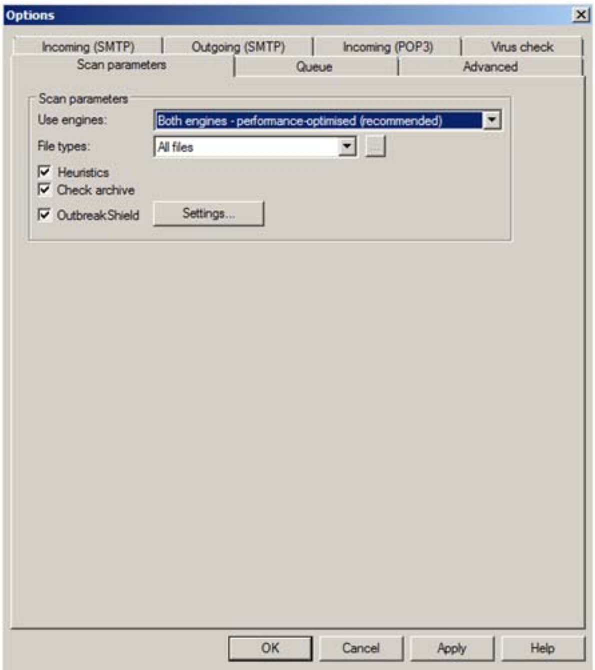
Collect email from this POP3 server:

Port: 110

Sender IP: Standard LAN adapter

Filter

Replacement text for rejected emails:



Scan parameters

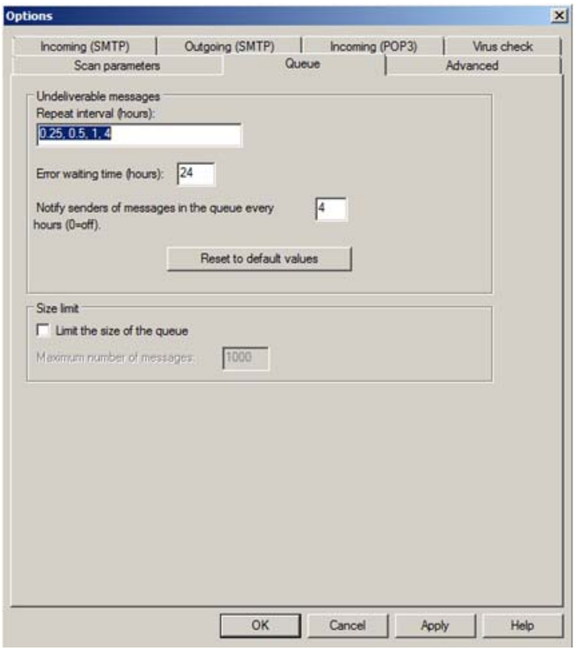
Use engines: Both engines - performance-optimised (recommended)

File types: All files

☑ Heuristics

☑ Check archive

☑ OutbreakShield



Undeliverable messages

Repeat interval (hours): 0.25, 0.5, 1, 4

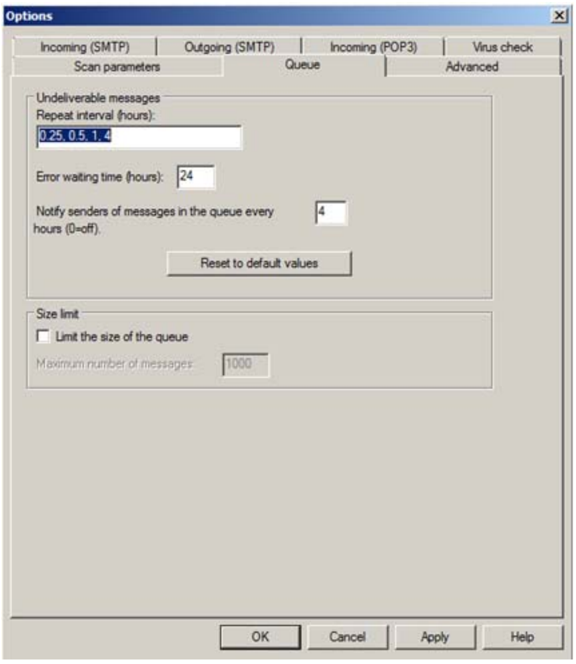
Error waiting time (hours): 24

Notify senders of messages in the queue every hours (0=off). 4

Size limit

☐ Limit the size of the queue

Maximum number of messages: 1000



Undeliverable messages

Repeat interval (hours): 0.25, 0.5, 1, 4

Error waiting time (hours): 24

Notify senders of messages in the queue every hours (0=off). 4

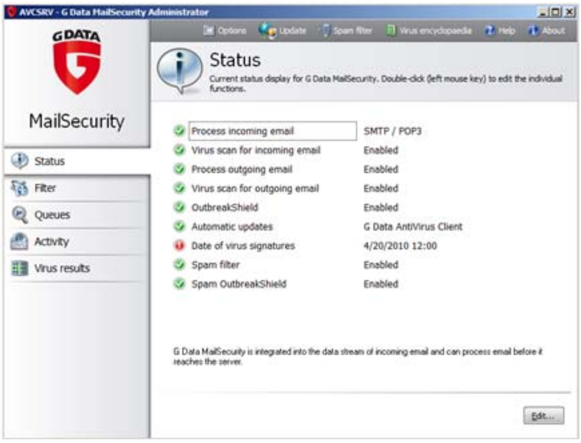
Size limit

☐ Limit the size of the queue

Maximum number of messages: 1000

The tabs have been arranged so as to show all the important options on one page, without overwhelming the user with choices.

Having configured the options, we then see from the overview page of the Administrator window that the system is now well protected:



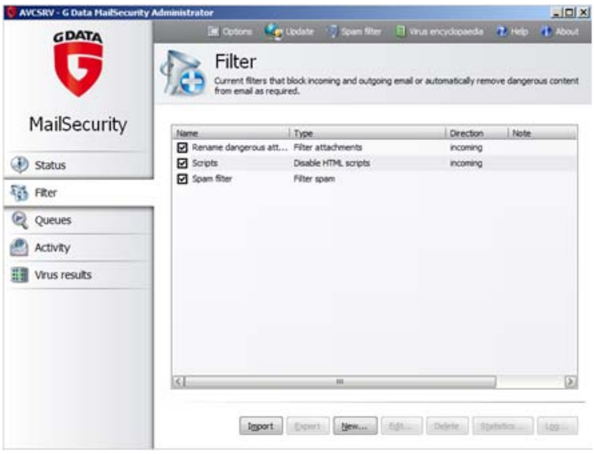
Status

Current status display for G Data MailSecurity. Double-click (left mouse key) to edit the individual functions.

✓ Process incoming email	SMTP / POP3
✓ Virus scan for incoming email	Enabled
✓ Process outgoing email	Enabled
✓ Virus scan for outgoing email	Enabled
✓ OutbreakShield	Enabled
✓ Automatic updates	G Data AntiVirus Client
! Date of virus signatures	4/20/2010 12:00
✓ Spam filter	Enabled
✓ Spam OutbreakShield	Enabled

G Data MailSecurity is integrated into the data stream of incoming email and can process email before it reaches the server.

The "Filter" area allows us to use pre-configured filters, or create our own, to deal with the most diverse requirements:



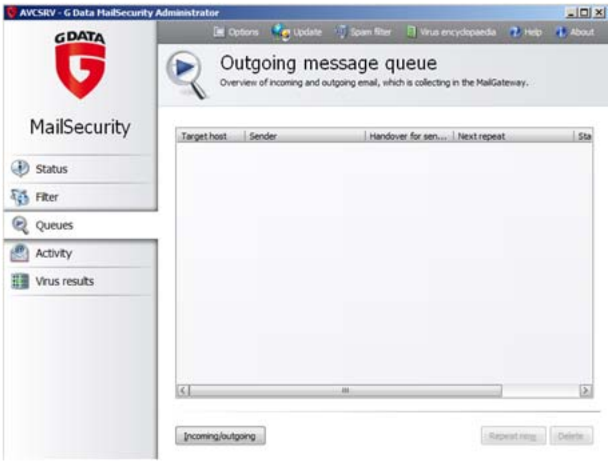
Filter

Current filters that block incoming and outgoing email or automatically remove dangerous content from email as required.

Name	Type	Direction	Note
☑ Rename dangerous att...	Filter attachments	incoming	
☑ Scripts	Disable HTML scripts	incoming	
☑ Spam filter	Filter spam		

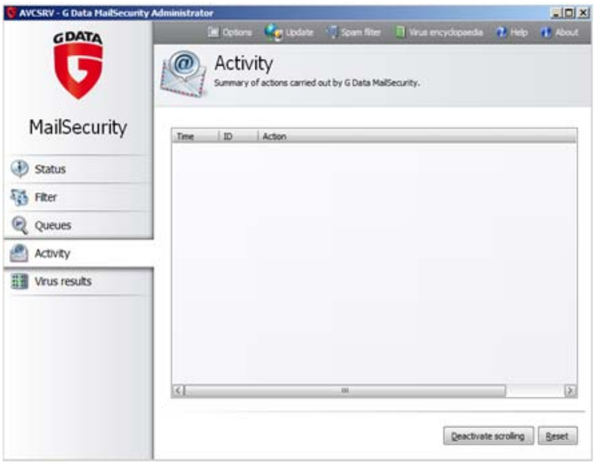
We were also impressed with the various options for viewing the mail protection system, such as the queue, or processed mails.

Any malware found is clearly displayed in the "Virus results" section:



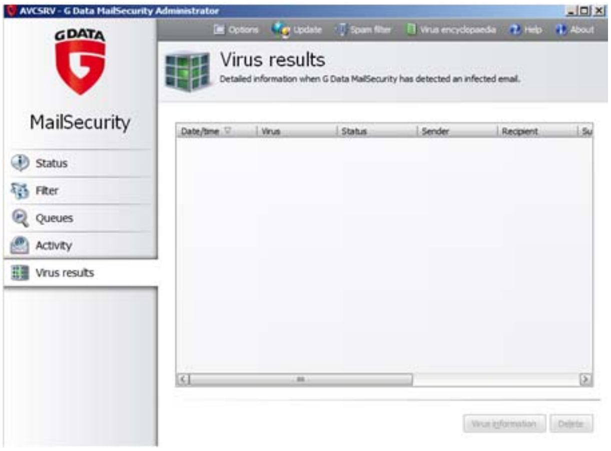
Outgoing message queue

Overview of incoming and outgoing email, which is collecting in the MailGateway.



Activity

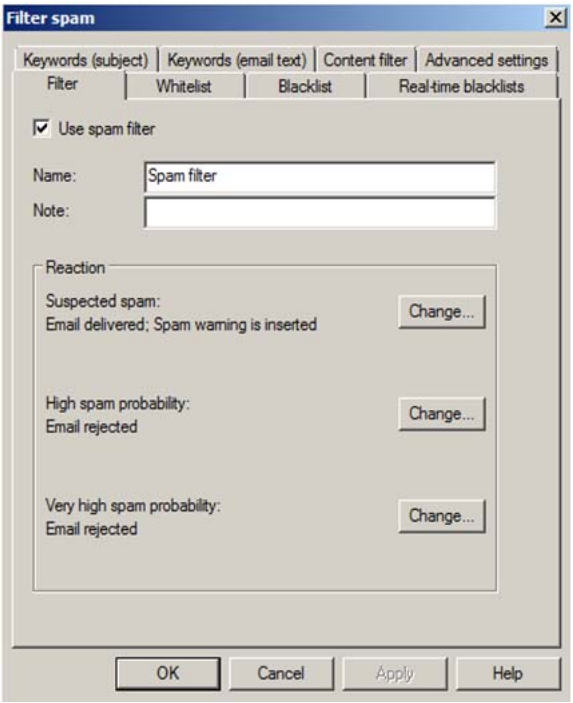
Summary of actions carried out by G Data MailSecurity.



Virus results

Detailed information when G Data MailSecurity has detected an infected email.

The last of the configuration options is found under "Spam Filter". This is structured in the same way as the Options dialog box, which we have already seen. Thus the whole configuration interface of the G Data suite is very much self-explanatory, and the user can immediately find all necessary functions.



☑ Use spam filter

Name: Spam filter

Note:

Suspected spam:
Email delivered; Spam warning is inserted

High spam probability:
Email rejected

Very high spam probability:
Email rejected

All the features one could want are present, and so MailSecurity contributes to our overall very positive impression of the suite.

Summary

Manufacturer's website

The G Data website (**www.gdata.com**) is well-designed and easy to find your way around, being compatible with current standards.

The site offers everything that you would expect from an antivirus manufacturer. There is information about current threats, and a virus encyclopaedia. The business section is appropriate to the needs of business users.

G Data makes it clear on the website that the suite is aimed primarily at medium-sized businesses.

The installation process

As with the version we tested last year, the installation of the G Data suite is made very pleasant by the simple and intuitive user interface, which could be used even by inexperienced users without any need to consult the manual.

The manufacturers have remained true to their philosophy of simple installation, making this one of the best products we have tested.

The administration console

The administration console is certainly one of the simplest we have ever reviewed.

After the installation, only administrative work remains to be done.

The numerous functions and configuration possibilities mean that the suite is lacking nothing in terms of functionality.

Remote installation of clients is very well handled and can be carried out very quickly.

The MailSecurity Administrator is no exception, being very simple to use without lacking anything in the way of functions.

Deployment areas

Although the suite copes with all standard requirements, the manufacturers see it as being appropriate for medium-sized businesses. The simplicity of the administration means that some sorting functions, which would be valuable in larger networks, have to be forfeited.

Antivirus clients

The client software is very user friendly and easy to find your way around. There is effectively no configuration to be done, and warning pop-ups are infrequent. The default settings are ideal, as is the ability to prevent the local user from making configuration changes.

Summary

G Data has, like last year, succeeded in producing a suite that is very easy to use.

There is no lack of functionality, and G Data sets the standard for intuitive user interfaces.

Particularly the Exchange suite and the remote installation are exemplary. The manual is virtually redundant.

Pros

- + Rapid client installation
- + Simple administration console
- + Simple remote installation
- + Quick and easy installation
- + Excellent Exchange protection

Cons

- Few filtering options
- No real-time status
- Misleading annotation in the database set-up section

Deployment areas

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★★	★★★★★	★★★★

Summary

Installation Wizard	★★★★★
User Navigation	★★★★
Administrator console	★★★★★
Default Values	★★★★
MS Active Directory Support	★★★★
Database Support	★★
Remote Installation	★★★★
Website	★★★★
Manual	★★★★

Kaspersky

Test Software:

Kaspersky Antivirus for Windows Workstation	→	Client Protection
Kaspersky Antivirus for Windows Server	→	File Server Protection
Kaspersky Security for Microsoft Exchange Server	→	Exchange Server Mail Protection
Kaspersky Administration Kit	→	Administration

Installation procedure

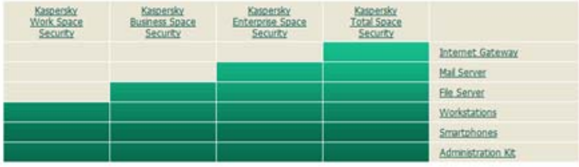
Downloading the product

All the products can be downloaded in fully functioning versions from the manufacturer's website. It is easy to find the products, and the website design is simple and clear.

The trial versions of the software run for 30 days, which is adequate time to carry out comprehensive tests. It is necessary to register to obtain a trial licence.

Unfortunately, Kaspersky conforms to the general rule whereby there is no single installer for the whole suite. This does however give you the opportunity to choose the individual products suitable for your own network. We note that Kaspersky also produce security software for Linux networks.

There is a clear and simple diagram of the different products and their functions:

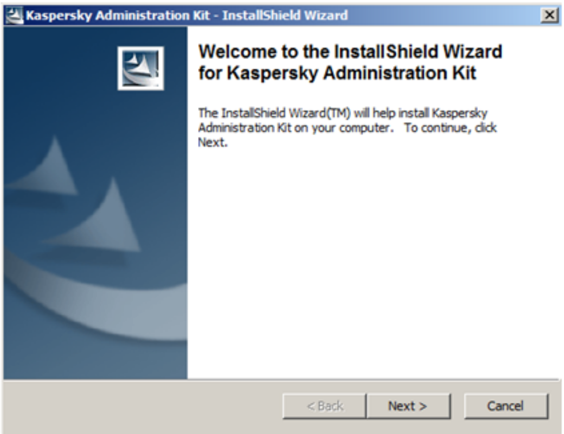


Kaspersky Work Space Security	Kaspersky Business Space Security	Kaspersky Enterprise Space Security	Kaspersky Total Space Security	
			🟩	Internet Gateway
		🟩	🟩	Mail Server
	🟩	🟩	🟩	File Server
🟩	🟩	🟩	🟩	Workstations
🟩	🟩	🟩	🟩	Smartphones
🟩	🟩	🟩	🟩	Administration Kit

By and large we had no complaints about the design of the website.

Product installation

We begin with the installation of the Administrator Kit.

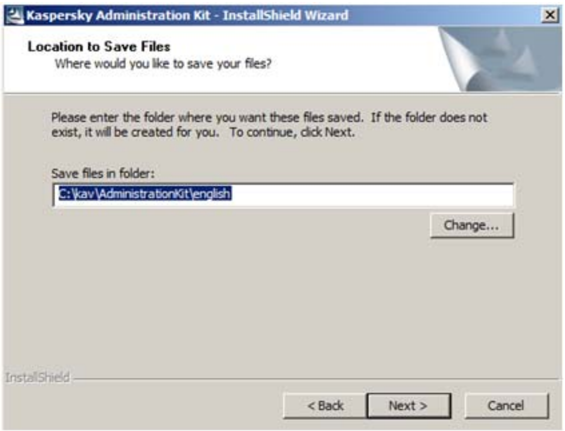


Kaspersky Administration Kit - InstallShield Wizard

Welcome to the InstallShield Wizard for Kaspersky Administration Kit

The InstallShield Wizard(TM) will help install Kaspersky Administration Kit on your computer. To continue, click Next.

The first step is to choose the folder for the setup files:



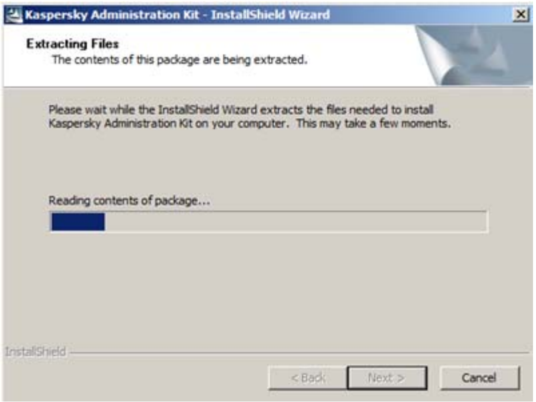
Kaspersky Administration Kit - InstallShield Wizard

Location to Save Files
Where would you like to save your files?

Please enter the folder where you want these files saved. If the folder does not exist, it will be created for you. To continue, click Next.

Save files in folder:
C:\kav\AdministrationKit\english

The installer then unpacks the setup files to this folder:



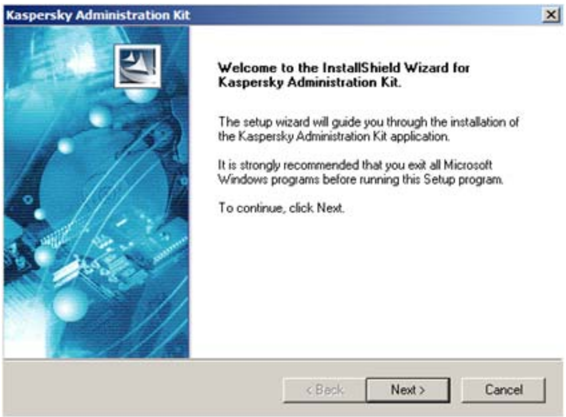
Extracting Files

The contents of this package are being extracted.

Please wait while the InstallShield Wizard extracts the files needed to install Kaspersky Administration Kit on your computer. This may take a few moments.

Reading contents of package...

The setup wizard then starts:



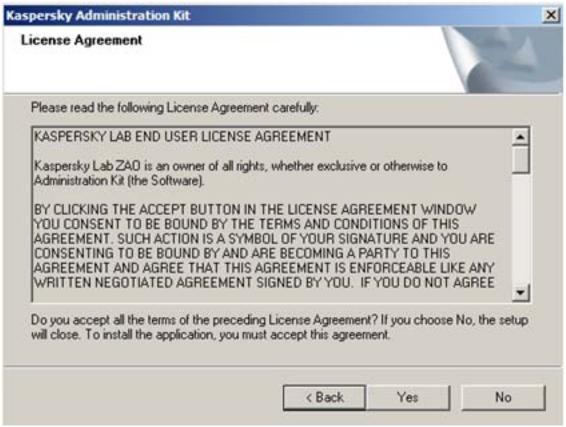
Welcome to the InstallShield Wizard for Kaspersky Administration Kit.

The setup wizard will guide you through the installation of the Kaspersky Administration Kit application.

It is strongly recommended that you exit all Microsoft Windows programs before running this Setup program.

To continue, click Next.

There is the usual licence agreement to accept:



License Agreement

Please read the following License Agreement carefully.

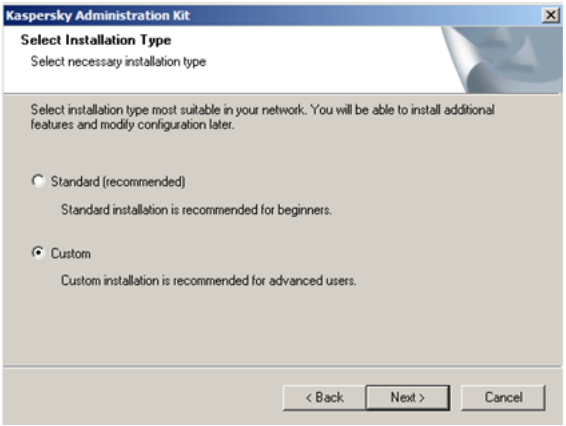
KASPERSKY LAB END USER LICENSE AGREEMENT

Kaspersky Lab ZAO is an owner of all rights, whether exclusive or otherwise to Administration Kit (the Software).

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IF YOU DO NOT AGREE

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install the application, you must accept this agreement.

The next point allows us to choose between "Standard" and "Custom" installation. To get an idea of the options available, we select Custom.



Select Installation Type

Select necessary installation type

Select installation type most suitable in your network. You will be able to install additional features and modify configuration later.

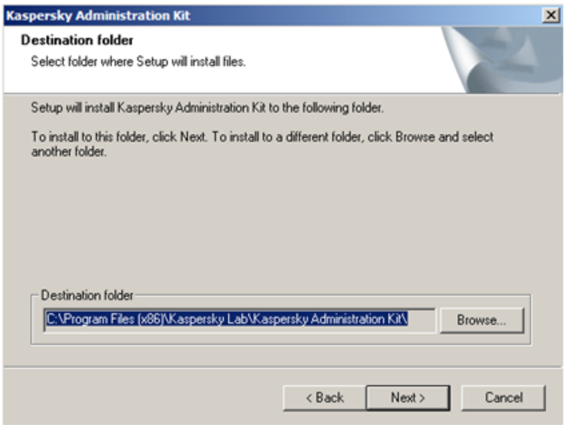
○ Standard (recommended)

Standard installation is recommended for beginners.

● Custom

Custom installation is recommended for advanced users.

Now we have to choose the installation folder:



Destination folder

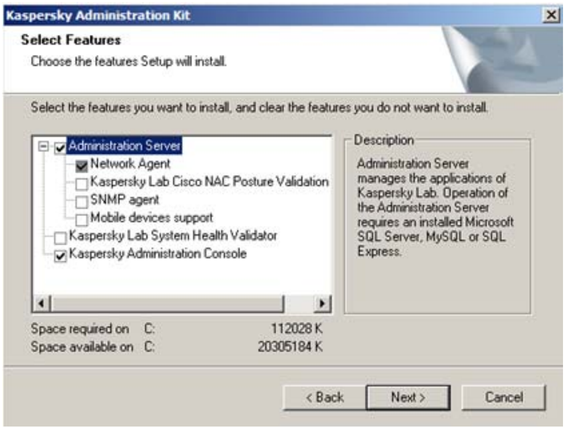
Select folder where Setup will install files.

Setup will install Kaspersky Administration Kit to the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination folder: C:\Program Files (x86)\Kaspersky Lab\Kaspersky Administration Kit\

The next step is to choose the features we want to install:



Select Features

Choose the features Setup will install.

Select the features you want to install, and clear the features you do not want to install.

- ☑ Administration Server
  - ☑ Network Agent
  - □ Kaspersky Lab Cisco NAC Posture Validation
  - □ SNMP agent
  - □ Mobile devices support
- □ Kaspersky Lab System Health Validator
- ☑ Kaspersky Administration Console

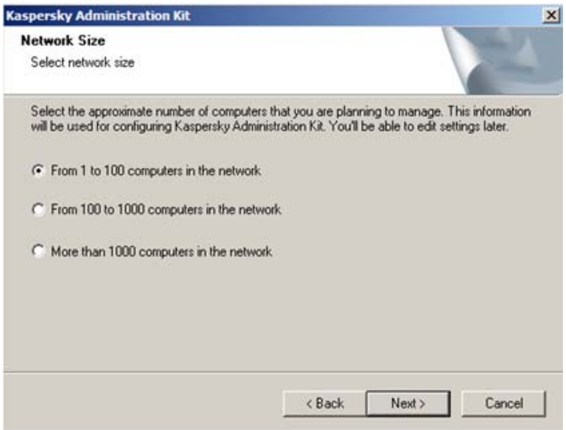
Description

Administration Server manages the applications of Kaspersky Lab. Operation of the Administration Server requires an installed Microsoft SQL Server, MySQL or SQL Express.

Space required on C: 112028 K

Space available on C: 20305184 K

We particularly liked the next step, which asks us to choose the expected size of the network. Unfortunately there is no information as to how each of these options will be configured.



Network Size
Select network size

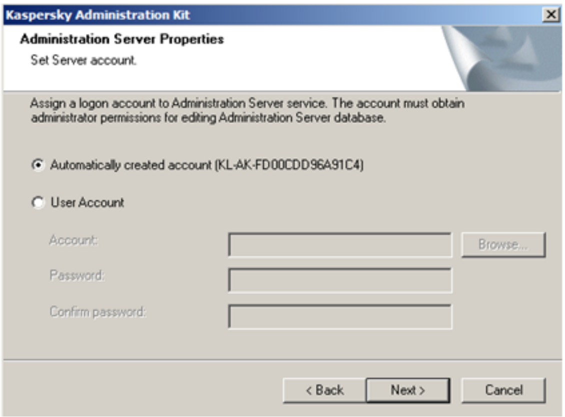
Select the approximate number of computers that you are planning to manage. This information will be used for configuring Kaspersky Administration Kit. You'll be able to edit settings later.

● From 1 to 100 computers in the network

○ From 100 to 1000 computers in the network

○ More than 1000 computers in the network

In the next step we can choose the user account for administering the suite. There is a choice of using an existing account, or creating a new one:



Administration Server Properties
Set Server account.

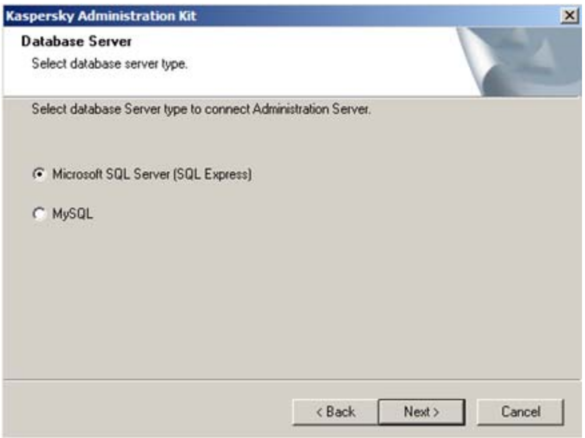
Assign a logon account to Administration Server service. The account must obtain administrator permissions for editing Administration Server database.

● Automatically created account (KL-AK-FD00CDD96A91C4)

○ User Account

Account:
Password:
Confirm password:

We then have to choose a database option from SQL Express or MySQL.



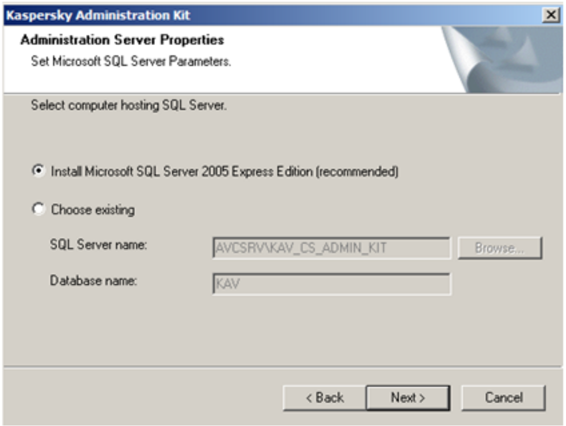
Database Server
Select database server type.

Select database Server type to connect Administration Server.

● Microsoft SQL Server (SQL Express)

○ MySQL

The next point concerns the SQL parameters:



Administration Server Properties
Set Microsoft SQL Server Parameters.

Select computer hosting SQL Server.

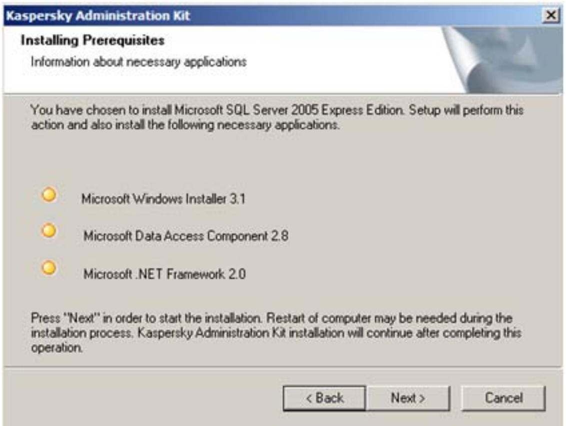
● Install Microsoft SQL Server 2005 Express Edition (recommended)

○ Choose existing

SQL Server name: AVCSRV\KAV_CS_ADMIN_KIT

Database name: KAV

We select SQL Express for our test.



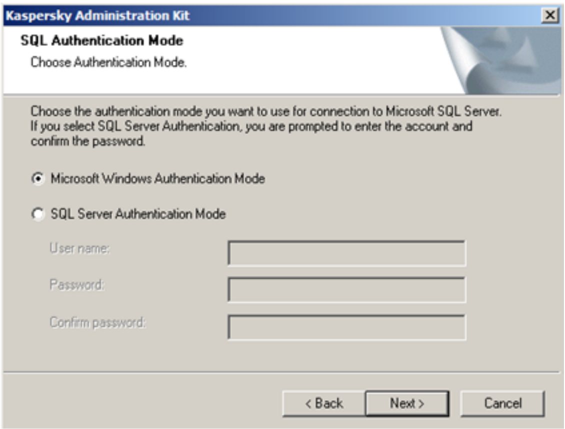
Installing Prerequisites
Information about necessary applications

You have chosen to install Microsoft SQL Server 2005 Express Edition. Setup will perform this action and also install the following necessary applications.

- Microsoft Windows Installer 3.1
- Microsoft Data Access Component 2.8
- Microsoft .NET Framework 2.0

Press "Next" in order to start the installation. Restart of computer may be needed during the installation process. Kaspersky Administration Kit installation will continue after completing this operation.

We now just need to choose the authentication method:



SQL Authentication Mode
Choose Authentication Mode.

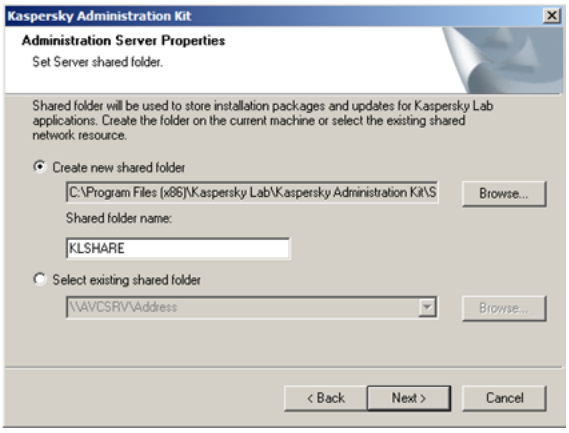
Choose the authentication mode you want to use for connection to Microsoft SQL Server. If you select SQL Server Authentication, you are prompted to enter the account and confirm the password.

● Microsoft Windows Authentication Mode

○ SQL Server Authentication Mode

User name:
Password:
Confirm password:

Kaspersky uses a network share to distribute installation packets and updates. You can choose between using an existing share and creating a new one:


Kaspersky Administration Kit

Administration Server Properties

Set Server shared folder.

Shared folder will be used to store installation packages and updates for Kaspersky Lab applications. Create the folder on the current machine or select the existing shared network resource.

● Create new shared folder

C:\Program Files (x86)\Kaspersky Lab\Kaspersky Administration Kit\S

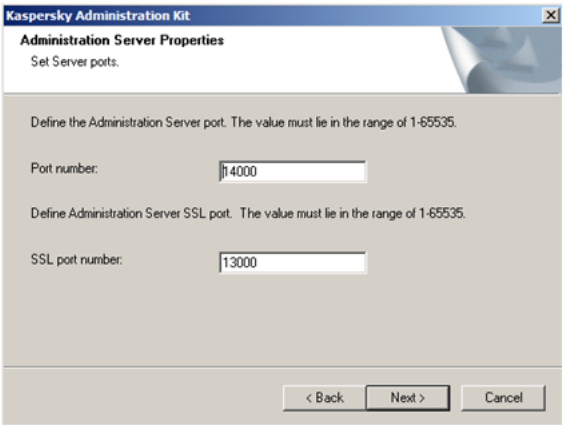
Shared folder name:

KLSHARE

○ Select existing shared folder

\\AVCSRV\Address

An Administration Server port also needs to be defined:


Kaspersky Administration Kit

Administration Server Properties

Set Server ports.

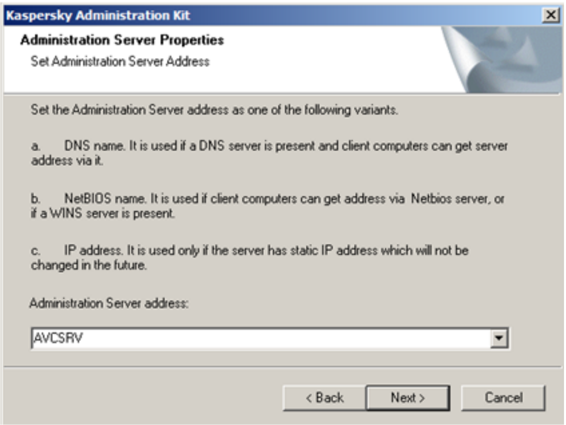
Define the Administration Server port. The value must lie in the range of 1-65535.

Port number: 14000

Define Administration Server SSL port. The value must lie in the range of 1-65535.

SSL port number: 13000

The method of name resolution for the server can also be set:


Kaspersky Administration Kit

Administration Server Properties

Set Administration Server Address

Set the Administration Server address as one of the following variants.

a. DNS name. It is used if a DNS server is present and client computers can get server address via it.

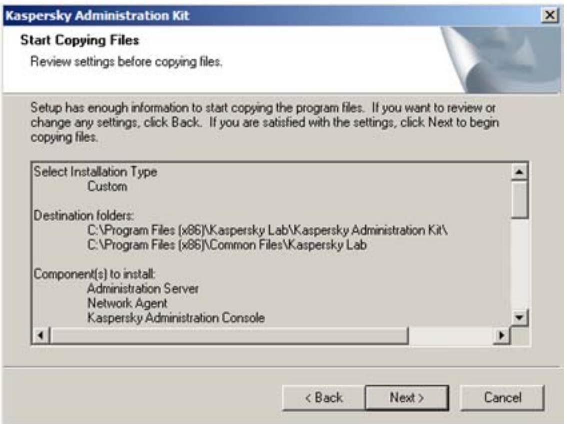
b. NetBIOS name. It is used if client computers can get address via Netbios server, or if a WINS server is present.

c. IP address. It is used only if the server has static IP address which will not be changed in the future.

Administration Server address:

AVCSRV

The installer now has enough information to begin the setup process. It must be noted here that the installation must be carried out using the main Administrator account; any other user account, even with administrator privileges, will not work. We feel that the wizard should notify the user of this at the start.


Kaspersky Administration Kit

Start Copying Files

Review settings before copying files.

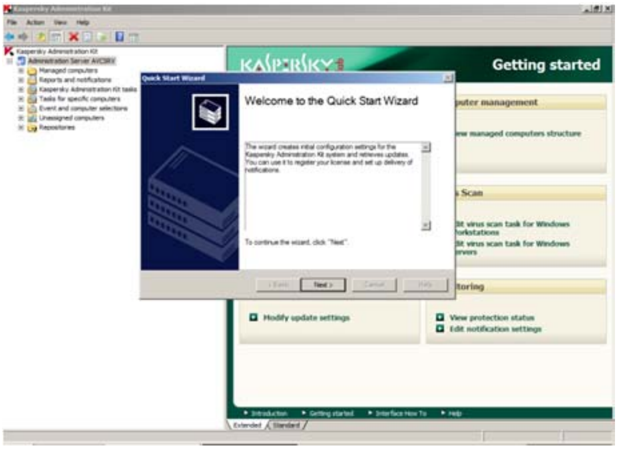
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

```
Select Installation Type
        Custom

Destination folders:
        C:\Program Files (x86)\Kaspersky Lab\Kaspersky Administration Kit\
        C:\Program Files (x86)\Common Files\Kaspersky Lab

Component(s) to install:
        Administration Server
        Network Agent
        Kaspersky Administration Console
```

Once the installation is complete, we can open the administration console:

The management interface

First use of the admin console conveniently starts a configuration wizard:


Quick Start Wizard

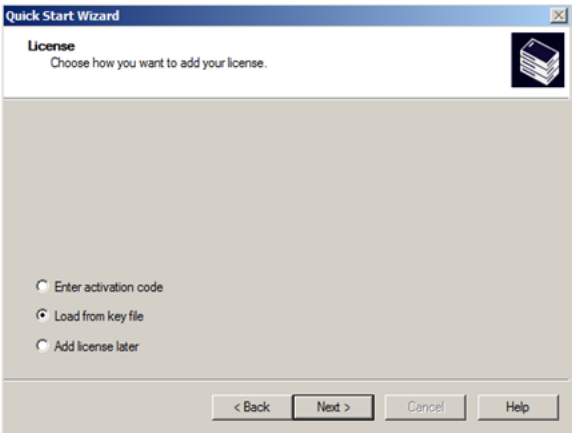
Welcome to the Quick Start Wizard

The wizard creates initial configuration settings for the Kaspersky Administration Kit system and retrieves updates. You can use it to register your license and set up delivery of notifications.

To continue the wizard, click "Next".

Kaspersky Administration Kit
File
Action
View
Help
Kaspersky Administration Kit
Administration Server AVCSRV
Managed computers
Reports and notifications
Kaspersky Administration Kit tasks
Tasks for specific computers
Event and computer selections
Unassigned computers
Repositories
KASPERSKY
Getting started
puter management
ew managed computers structure
Scan
dit virus scan task for Windows orkstations
dit virus scan task for Windows ervers
toring
Modify update settings
View protection status
Edit notification settings
< Back
Next >
Cancel
Help
Introduction
Getting started
Interface How To
Help
Extended
Standard

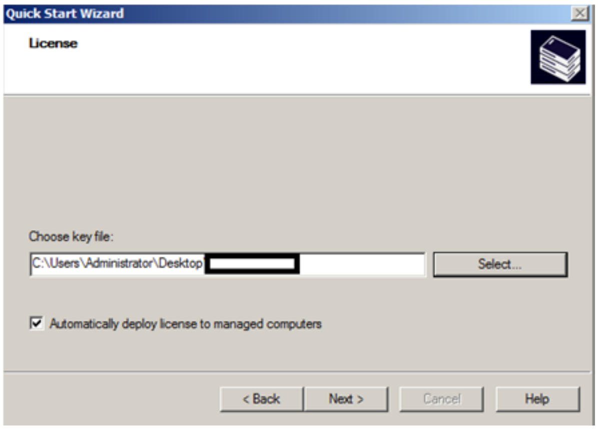
The first step is to select a licence file:



License
Choose how you want to add your license.

○ Enter activation code
● Load from key file
○ Add license later

We choose a locally stored licence key:

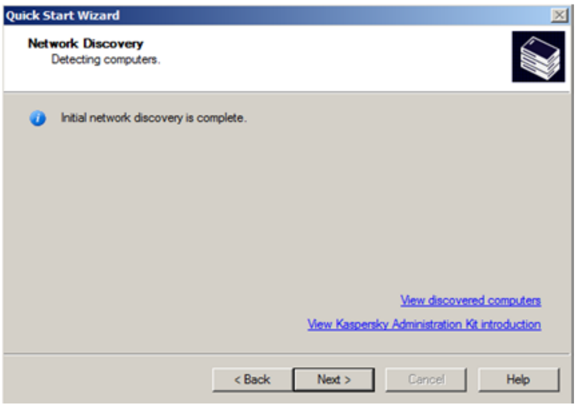


License

Choose key file:
C:\Users\Administrator\Desktop[redacted]

☑ Automatically deploy license to managed computers

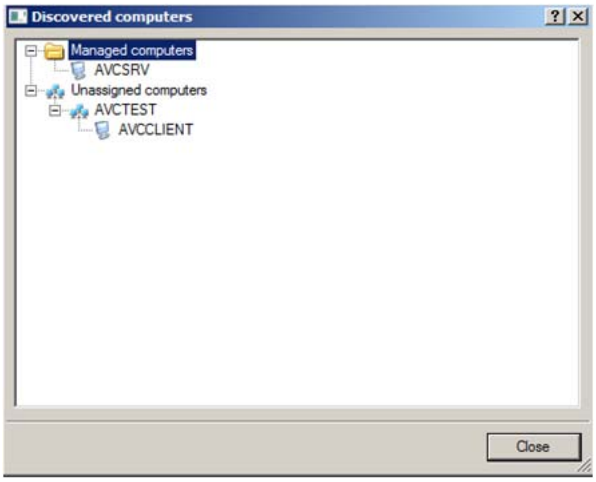
Next, the installer carries out a thorough scan of the network:


Quick Start Wizard
View discovered computers
View Kaspersky Administration Kit introduction
< Back
Next >
Cancel
Help

Network Discovery
Detecting computers.

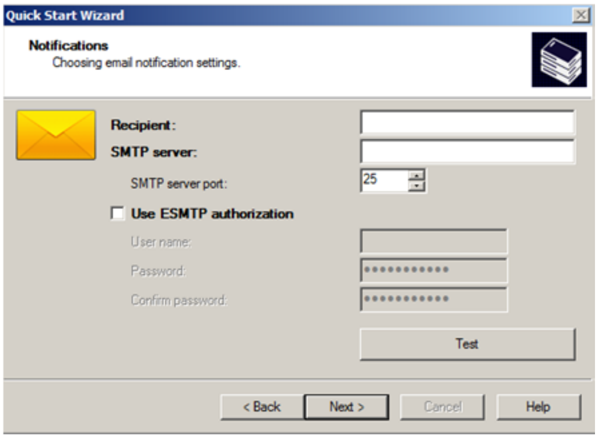
Initial network discovery is complete.

By clicking on "View discovered computers" you can see the client PCs that have been discovered:



```
Managed computers
    AVCSRV
Unassigned computers
    AVCTEST
        AVCCLIENT
```

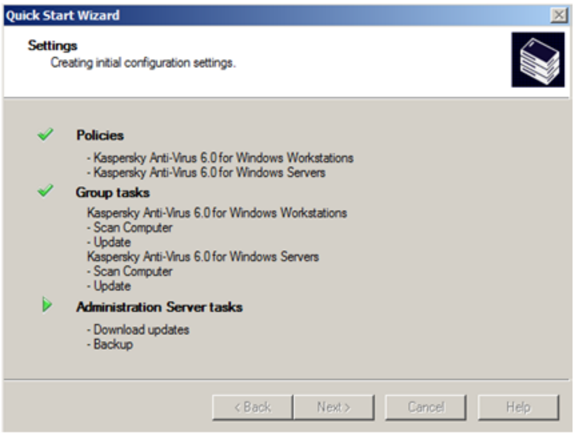
Next, we can configure the notifications for the mail server:



Notifications
Choosing email notification settings.

Recipient:
SMTP server:
SMTP server port: 25
☐ **Use ESMTP authorization**
User name:
Password: •••••••••••
Confirm password: •••••••••••

We then see a summary of the completed tasks:



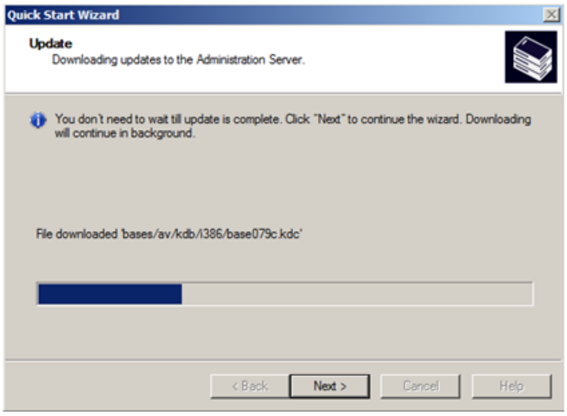
Settings
Creating initial configuration settings.

✓ **Policies**
- Kaspersky Anti-Virus 6.0 for Windows Workstations
- Kaspersky Anti-Virus 6.0 for Windows Servers

✓ **Group tasks**
Kaspersky Anti-Virus 6.0 for Windows Workstations
- Scan Computer
- Update
Kaspersky Anti-Virus 6.0 for Windows Servers
- Scan Computer
- Update

▶ **Administration Server tasks**
- Download updates
- Backup

The configuration wizard then downloads updates to the administration server:

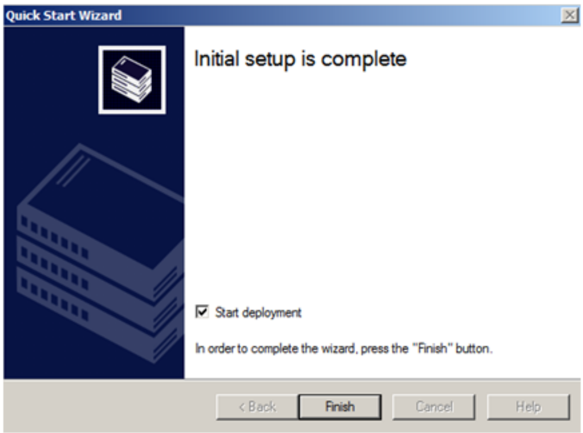


Update
Downloading updates to the Administration Server.

You don't need to wait till update is complete. Click "Next" to continue the wizard. Downloading will continue in background.

File downloaded 'bases/av/kdb/i386/base079c.kdc'

A great number of update files will be downloaded for the various systems, but there is no need to wait for the update process to finish, as it will run unattended in the background. Like last year, Kaspersky's configuration wizard is definitely one of the best we have tested, as finishing one wizard leads to the start of the next, so that no important tasks can be forgotten.

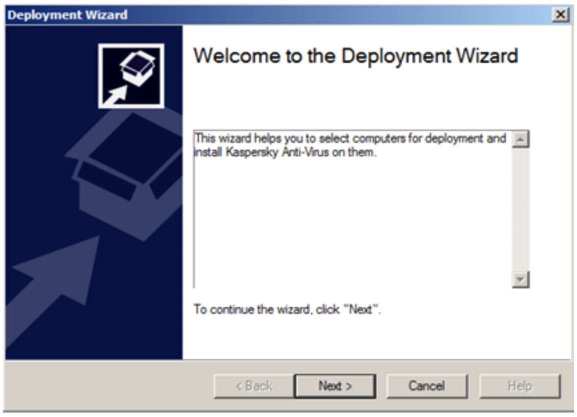


Initial setup is complete

☑ Start deployment

In order to complete the wizard, press the "Finish" button.

Next we start the deployment wizard:

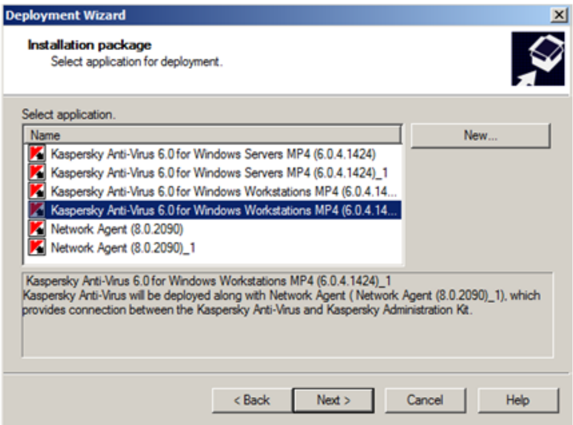


Welcome to the Deployment Wizard

This wizard helps you to select computers for deployment and install Kaspersky Anti-Virus on them.

To continue the wizard, click "Next".

Here we can select the installation packets that we want to distribute to the clients. Any installation packet not in the default list can be added manually:



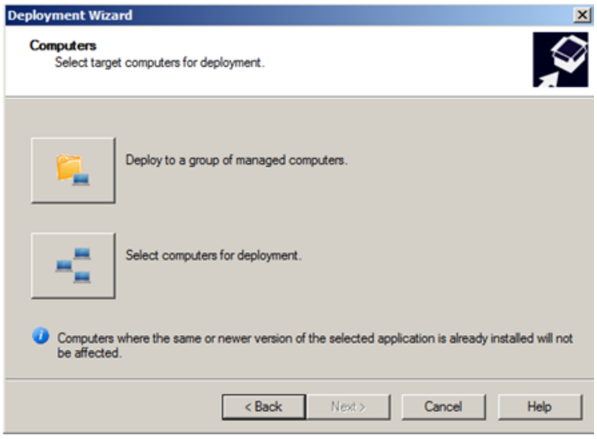
Installation package
Select application for deployment.

Select application.

Name
Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (6.0.4.1424)
Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (6.0.4.1424)_1
Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 (6.0.4.14...
Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 (6.0.4.14...
Network Agent (8.0.2090)
Network Agent (8.0.2090)_1

Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 (6.0.4.1424)_1
Kaspersky Anti-Virus will be deployed along with Network Agent (Network Agent (8.0.2090)_1), which provides connection between the Kaspersky Anti-Virus and Kaspersky Administration Kit.

If the wizard has already been used before, there is a choice of installing software to new clients, or additional packets to existing clients.



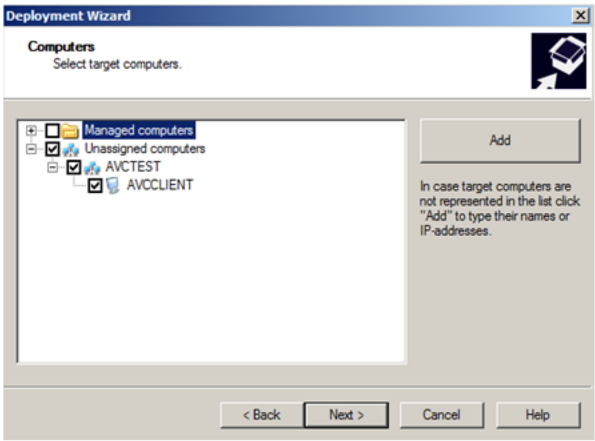
Computers
Select target computers for deployment.

Deploy to a group of managed computers.

Select computers for deployment.

Computers where the same or newer version of the selected application is already installed will not be affected.

As this is the initial configuration, we have to select the client PCs to be installed:



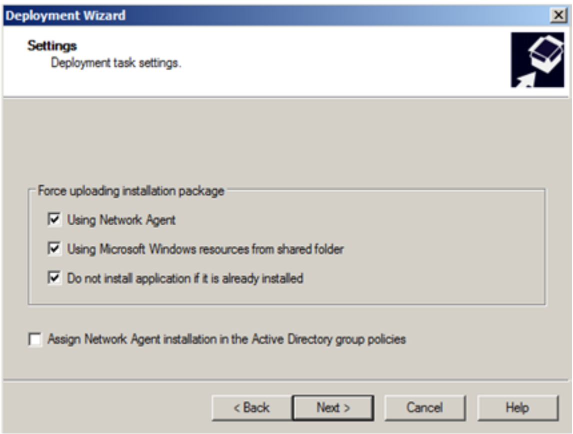
Deployment Wizard

Computers
Select target computers.

- ☐ Managed computers
- ☑ Unassigned computers
  - ☑ AVCTEST
    - ☑ AVCCLIENT

In case target computers are not represented in the list click "Add" to type their names or IP-addresses.

The next point is the selection of options for the client installation. We particularly liked the option for Active Directory integration:



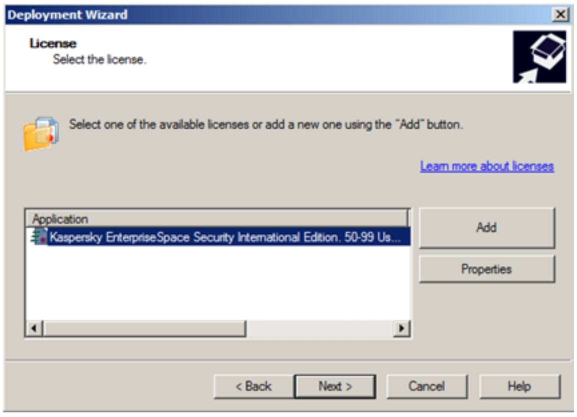
Deployment Wizard

Settings
Deployment task settings.

Force uploading installation package
- ☑ Using Network Agent
- ☑ Using Microsoft Windows resources from shared folder
- ☑ Do not install application if it is already installed

☐ Assign Network Agent installation in the Active Directory group policies

Now we have to select a licence for the client installations:



Deployment Wizard

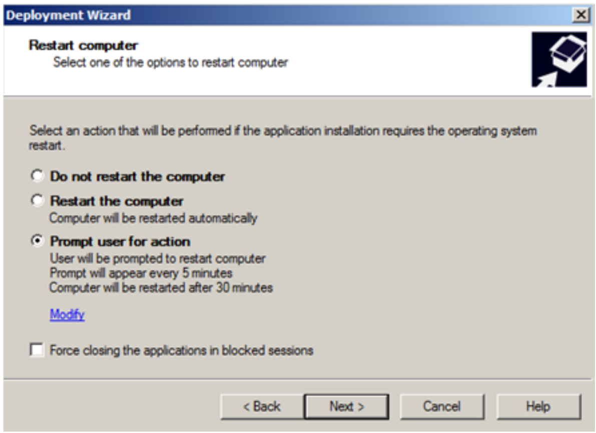
License
Select the license.

Select one of the available licenses or add a new one using the "Add" button.

Learn more about licenses

Application
Kaspersky EnterpriseSpace Security International Edition. 50-99 Us...

Kaspersky provide an exemplary choice of actions to be carried out on client computers when a restart is necessary:



Deployment Wizard

Restart computer
Select one of the options to restart computer

Select an action that will be performed if the application installation requires the operating system restart.

○ **Do not restart the computer**

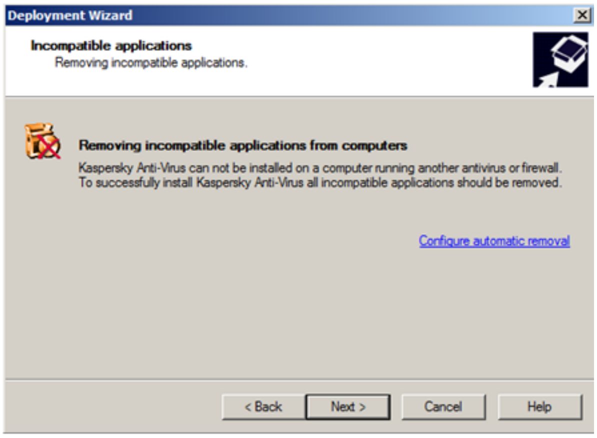
○ **Restart the computer**
Computer will be restarted automatically

● **Prompt user for action**
User will be prompted to restart computer
Prompt will appear every 5 minutes
Computer will be restarted after 30 minutes

Modify

☐ Force closing the applications in blocked sessions

The installer can be configured to remove any incompatible applications, such as other antivirus or firewall programs:



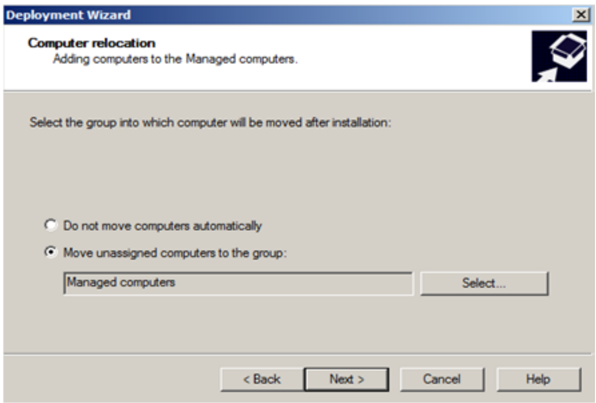
Deployment Wizard

Incompatible applications
Removing incompatible applications.

Removing incompatible applications from computers
Kaspersky Anti-Virus can not be installed on a computer running another antivirus or firewall.
To successfully install Kaspersky Anti-Virus all incompatible applications should be removed.

Configure automatic removal

The next step allows client computers to be assigned to administration groups:



Deployment Wizard

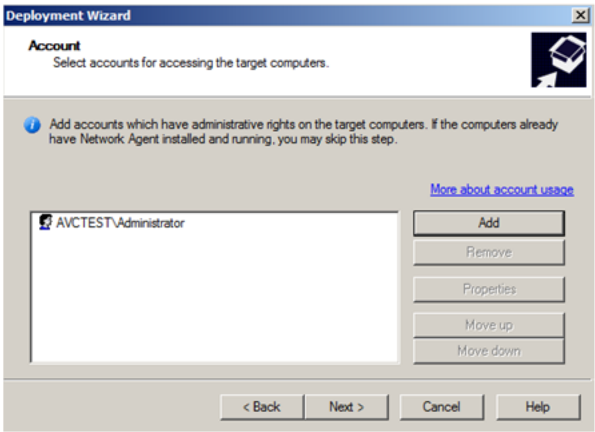
Computer relocation
Adding computers to the Managed computers.

Select the group into which computer will be moved after installation:

○ Do not move computers automatically
● Move unassigned computers to the group:

Managed computers

We then choose the Windows account to be used for the installation:

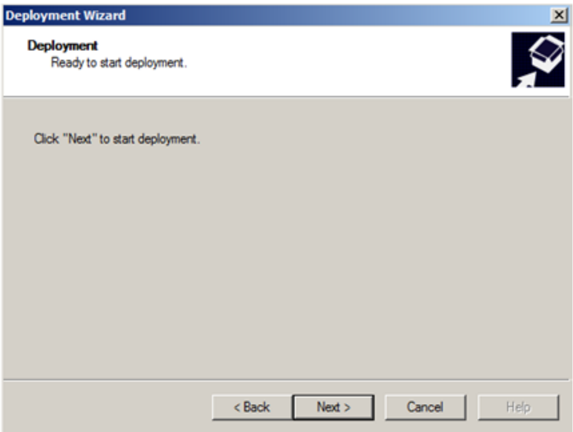


Account

Select accounts for accessing the target computers.

Add accounts which have administrative rights on the target computers. If the computers already have Network Agent installed and running, you may skip this step.

The wizard now has enough information to begin the deployment process:

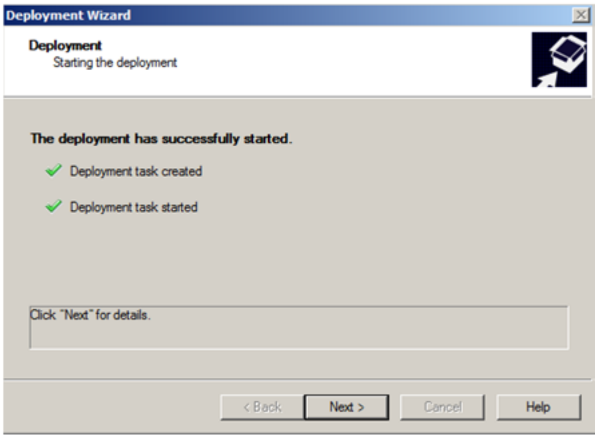


Deployment

Ready to start deployment.

Click "Next" to start deployment.

The wizard then informs us that the deployment task has been created and started:



Deployment

Starting the deployment

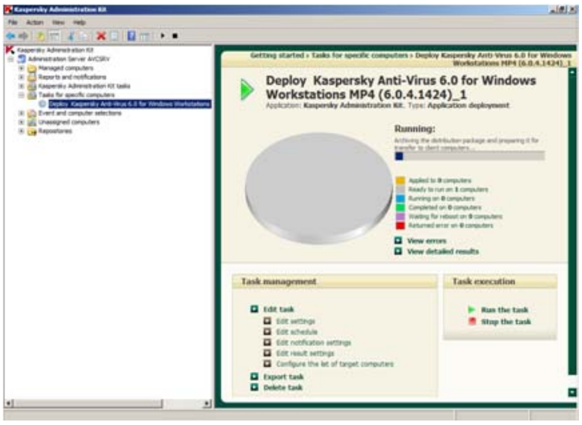
The deployment has successfully started.

✓ Deployment task created

✓ Deployment task started

Click "Next" for details.

It seems impossible, but Kaspersky is the first manufacturer to have created a real-time installation display that informs the user of the current state of client installations:



Getting started › Tasks for specific computers › Deploy Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 (6.0.4.1424)_1

Deploy Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 (6.0.4.1424)_1

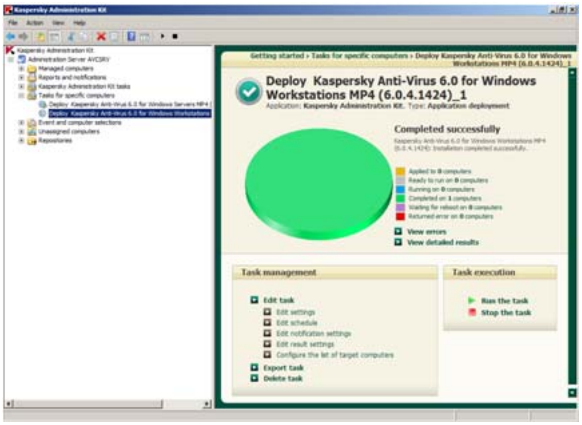
Application: Kaspersky Administration Kit. Type: Application deployment

Running:

Archiving the distribution package and preparing it for transfer to client computers...

- Applied to 0 computers
- Ready to run on 1 computers
- Running on 0 computers
- Completed on 0 computers
- Waiting for reboot on 0 computers
- Returned error on 0 computers

When the installation has been successfully completed, a summary page is presented:



Getting started › Tasks for specific computers › Deploy Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 (6.0.4.1424)_1

Deploy Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 (6.0.4.1424)_1

Application: Kaspersky Administration Kit. Type: Application deployment

Completed successfully

Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 (6.0.4.1424): Installation completed successfully.

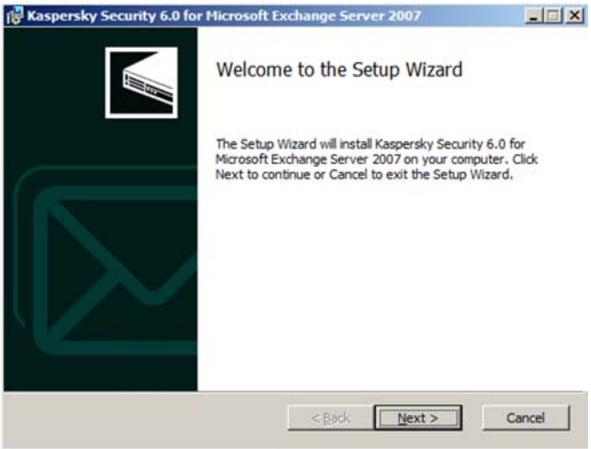
- Applied to 0 computers
- Ready to run on 0 computers
- Running on 0 computers
- Completed on 1 computers
- Waiting for reboot on 0 computers
- Returned error on 0 computers

The only thing to be criticised here is the speed with which the clients are installed.

The console is designed in the accustomed clear and comprehensible manner. All the necessary functions are present and easy to find. This simplicity means that even inexperienced users can find their way around easily, without any need to consult the manual.

Exchange 2007 protection

We begin with the mail security setup:

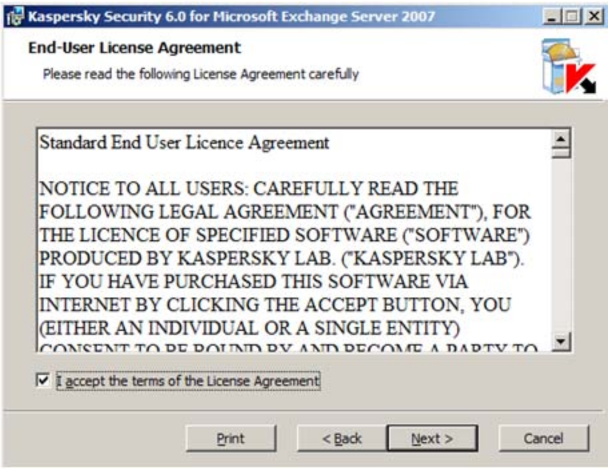


Kaspersky Security 6.0 for Microsoft Exchange Server 2007

Welcome to the Setup Wizard

The Setup Wizard will install Kaspersky Security 6.0 for Microsoft Exchange Server 2007 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

There is the usual licence agreement to accept:



Kaspersky Security 6.0 for Microsoft Exchange Server 2007

End-User License Agreement

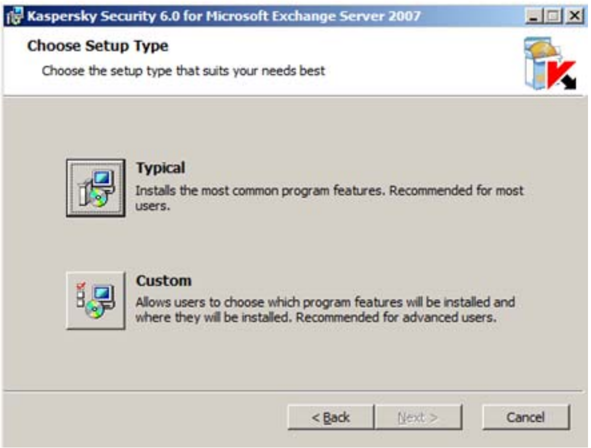
Please read the following License Agreement carefully

Standard End User Licence Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LAB. ("KASPERSKY LAB"). IF YOU HAVE PURCHASED THIS SOFTWARE VIA INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO

☑ I accept the terms of the License Agreement

There is the choice of "Typical" or "Custom" installation:



Kaspersky Security 6.0 for Microsoft Exchange Server 2007

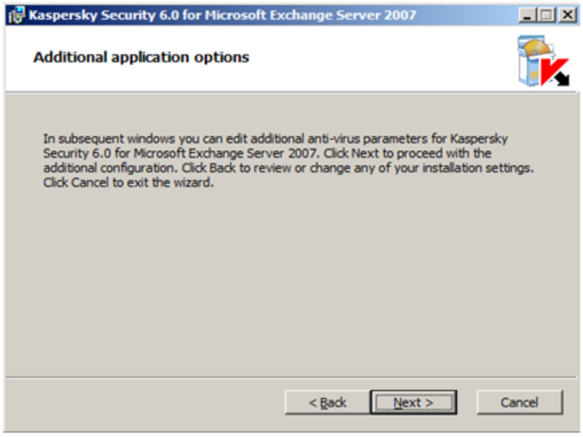
Choose Setup Type

Choose the setup type that suits your needs best

Typical
Installs the most common program features. Recommended for most users.

Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

The installer points out that additional parameters can be configured in the next stages:

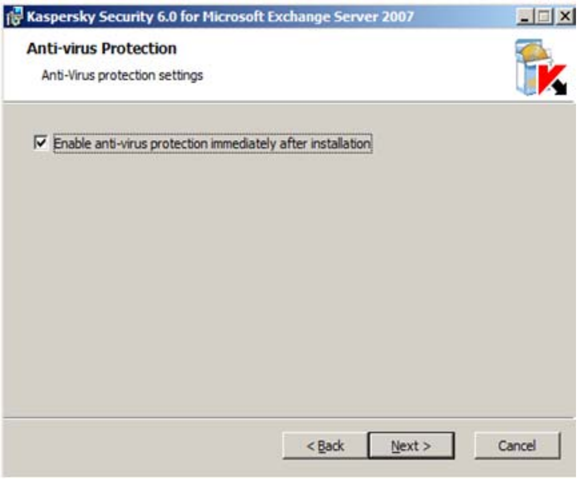


Kaspersky Security 6.0 for Microsoft Exchange Server 2007

Additional application options

In subsequent windows you can edit additional anti-virus parameters for Kaspersky Security 6.0 for Microsoft Exchange Server 2007. Click Next to proceed with the additional configuration. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Here we can choose whether to start protection immediately after setup completes:



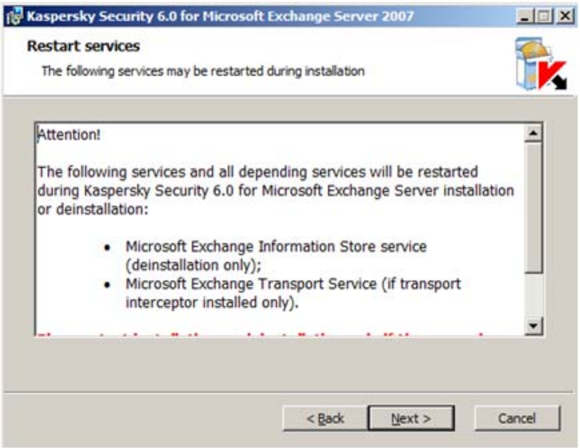
Kaspersky Security 6.0 for Microsoft Exchange Server 2007

Anti-virus Protection

Anti-Virus protection settings

☑ Enable anti-virus protection immediately after installation

We were pleased to note that the installer points out that some Microsoft services need to be restarted after the installation.



Kaspersky Security 6.0 for Microsoft Exchange Server 2007

Restart services

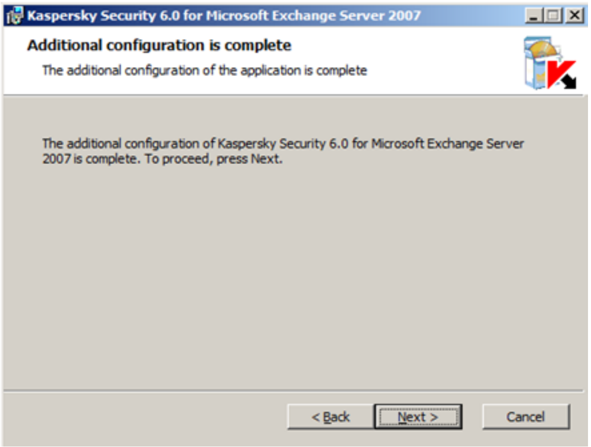
The following services may be restarted during installation

Attention!

The following services and all depending services will be restarted during Kaspersky Security 6.0 for Microsoft Exchange Server installation or deinstallation:

- Microsoft Exchange Information Store service (deinstallation only);
- Microsoft Exchange Transport Service (if transport interceptor installed only).

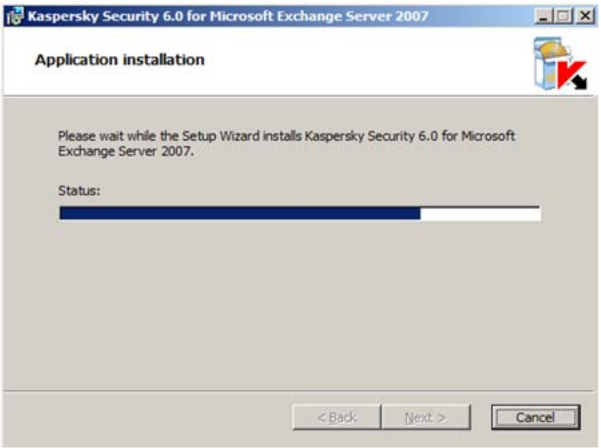
The installer now has enough information to begin:



Additional configuration is complete

The additional configuration of the application is complete

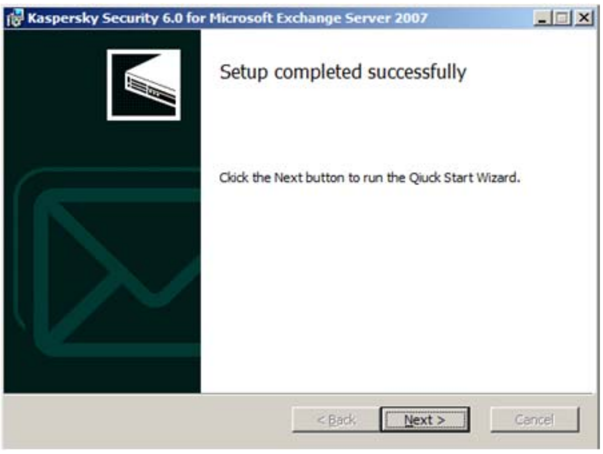
The additional configuration of Kaspersky Security 6.0 for Microsoft Exchange Server 2007 is complete. To proceed, press Next.



Application installation

Please wait while the Setup Wizard installs Kaspersky Security 6.0 for Microsoft Exchange Server 2007.

Status:



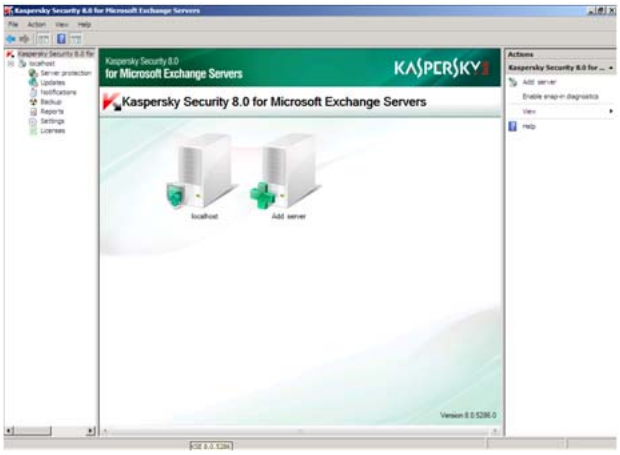
Setup completed successfully

Click the Next button to run the Quick Start Wizard.

The upcoming Kaspersky Security Suite for Microsoft Exchange has fewer steps. We will report in one of our next tests.

The Exchange 2007 interface

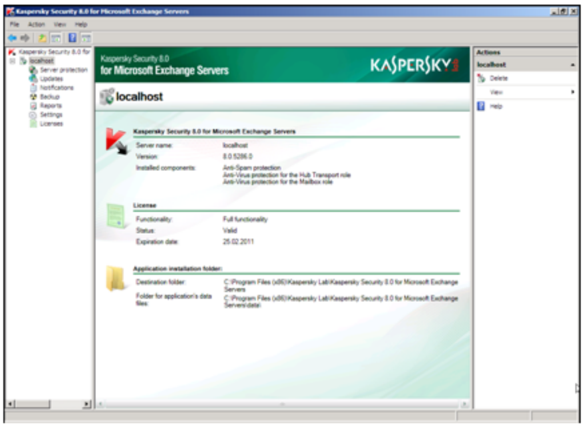
The MMC-compatible management console for the Exchange protection is very clear:


Kaspersky Security 8.0 for Microsoft Exchange Servers
File
Action
View
Help
Kaspersky Security 8.0 for
localhost
Server protection
Updates
Notifications
Backup
Reports
Settings
Licenses
Kaspersky Security 8.0
for Microsoft Exchange Servers
KASPERSKY
Kaspersky Security 8.0 for Microsoft Exchange Servers
localhost
Add server
Version 8.0.5286.0
Actions
Kaspersky Security 8.0 for ...
Add server
Enable snap-in diagnostics
View
Help

An initial screen allows us to define what servers we want to manage with that console. This can be useful for some administrators, who by some reason do not want to use Administration Kit.

If you switch to managed server you can see installed components and basic license overview.

There is a limited range of options here, so it is an easy task to configure the available settings. These are notification, reaction in the event of an infection, backups and reports:



Kaspersky Security 8.0 for Microsoft Exchange Servers

Server name: localhost
Version: 8.0.5286.0
Installed components: Anti-Spam protection
Anti-Virus protection for the Hub Transport role
Anti-Virus protection for the Mailbox role

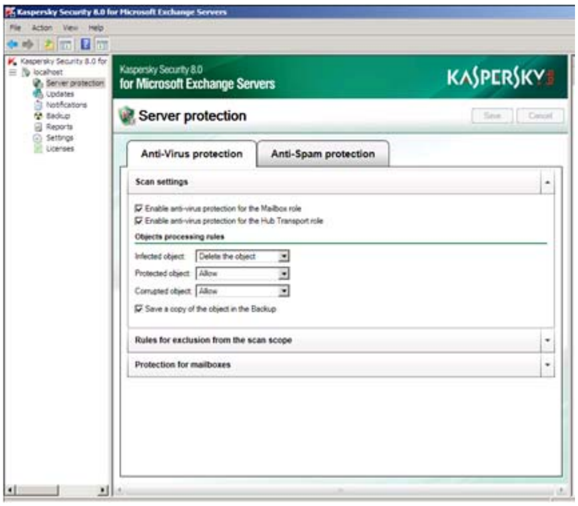
License

Functionality: Full functionality
Status: Valid
Expiration date: 25.02.2011

Application installation folder:

Destination folder: C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security 8.0 for Microsoft Exchange Servers
Folder for application's data files: C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security 8.0 for Microsoft Exchange Servers\data\

Server protection menu have two tabs related to two main tasks the product is charged with – Anti-Virus and Anti-spam protection.



Scan settings

☑ Enable anti-virus protection for the Mailbox role
☑ Enable anti-virus protection for the Hub Transport role

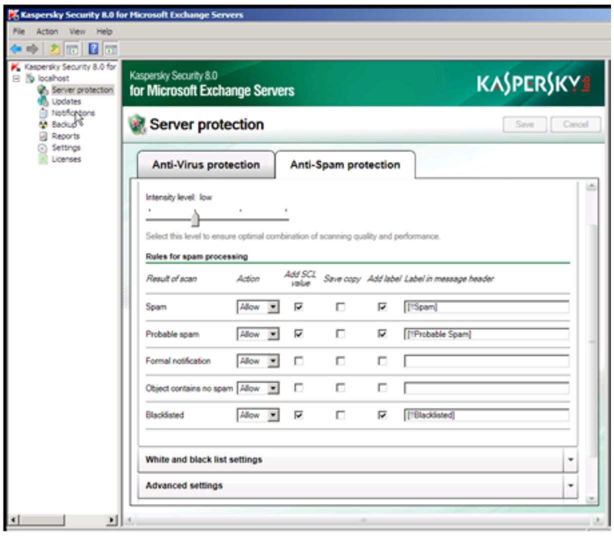
Objects processing rules

Infected object: Delete the object
Protected object: Allow
Corrupted object: Allow
☑ Save a copy of the object in the Backup

Rules for exclusion from the scan scope

Protection for mailboxes

Anti-SPAM protection tab allows us to define rules for spam processing.



Intensity level: low

Select this level to ensure optimal combination of scanning quality and performance.

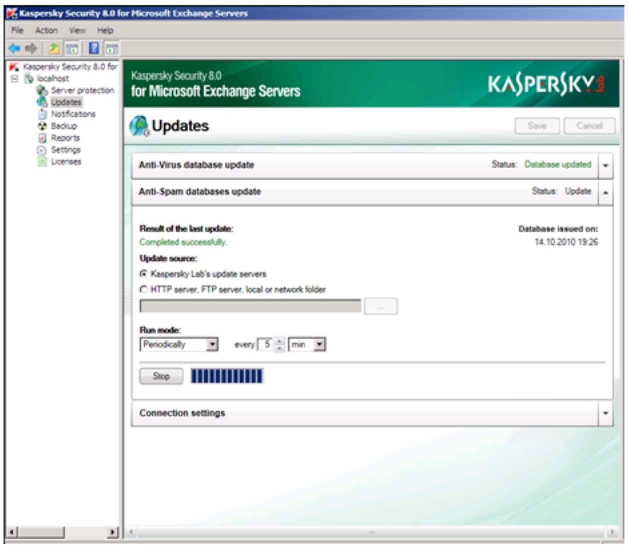
Rules for spam processing

Result of scan	*Action*	*Add SCL value*	*Save copy*	*Add label*	*Label in message header*
Spam	Allow	☑	□	☑	[!!Spam]
Probable spam	Allow	☑	□	☑	[!!Probable Spam]
Formal notification	Allow	□	□	□	
Object contains no spam	Allow	□	□	□	
Blacklisted	Allow	☑	□	☑	[!!Blacklisted]

White and black list settings

Advanced settings

Updates management also allows setting up update source and frequency, again as a separate settings for Anti-spam and Anti-virus protection.



Anti-Virus database update Status: Database updated

Anti-Spam databases update Status: Update

Result of the last update: Completed successfully.

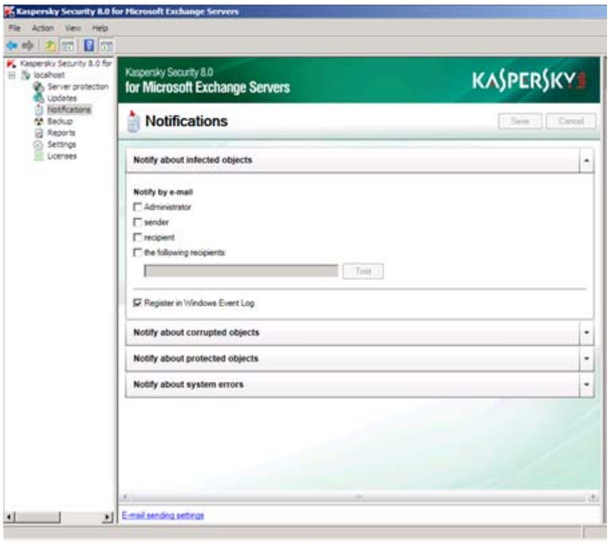
Database issued on: 14.10.2010 19:26

Update source:
● Kaspersky Lab's update servers
○ HTTP server, FTP server, local or network folder

Run mode: Periodically every 5 min

Connection settings

Notification settings allow us to set up notification rules for main predefined event types.



Notify about infected objects

Notify by e-mail
□ Administrator
□ sender
□ recipient
□ the following recipients

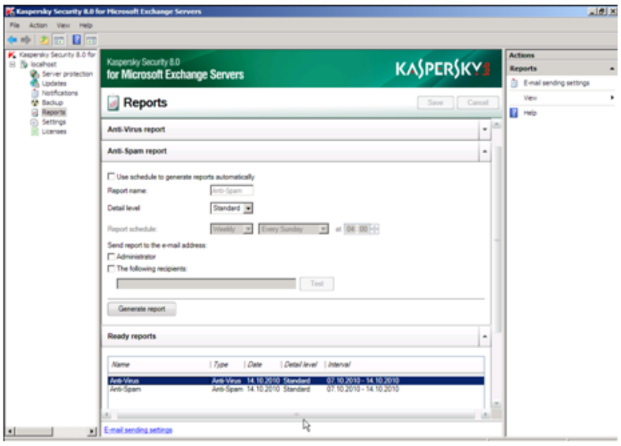
☑ Register in Windows Event Log

Notify about corrupted objects

Notify about protected objects

Notify about system errors

Reports management allows us to create and view reports on virus and spam detection.



Anti-Virus report

Anti-Spam report

☐ Use schedule to generate reports automatically

Report name: Anti-Spam

Detail level: Standard

Report schedule: Weekly Every Sunday at 04 00

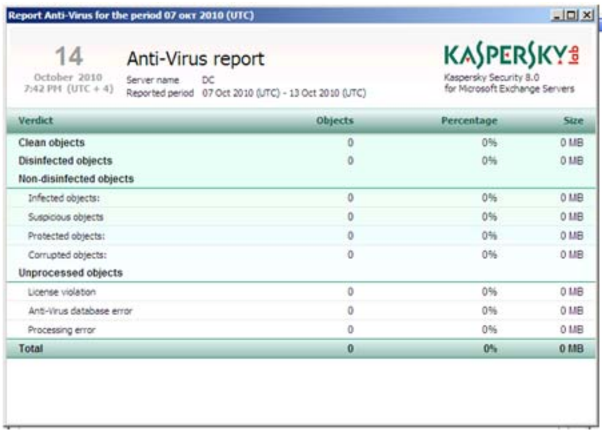
Send report to the e-mail address:

☐ Administrator

☐ The following recipients:

Ready reports

Name	Type	Date	Detail level	Interval
Anti-Virus	Anti-Virus	14.10.2010	Standard	07.10.2010 - 14.10.2010
Anti-Spam	Anti-Spam	14.10.2010	Standard	07.10.2010 - 14.10.2010

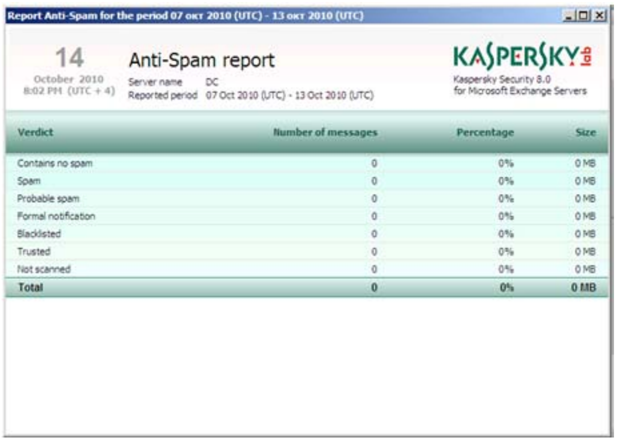

Report Anti-Virus for the period 07 окт 2010 (UTC)

14
October 2010
7:42 PM (UTC + 4)

Anti-Virus report

Server name DC
Reported period 07 Oct 2010 (UTC) - 13 Oct 2010 (UTC)

Verdict	Objects	Percentage	Size
Clean objects	0	0%	0 MB
Disinfected objects	0	0%	0 MB
Non-disinfected objects			
Infected objects:	0	0%	0 MB
Suspicious objects	0	0%	0 MB
Protected objects:	0	0%	0 MB
Corrupted objects:	0	0%	0 MB
Unprocessed objects			
License violation	0	0%	0 MB
Anti-Virus database error	0	0%	0 MB
Processing error	0	0%	0 MB
Total	0	0%	0 MB


Report Anti-Spam for the period 07 окт 2010 (UTC) - 13 окт 2010 (UTC)

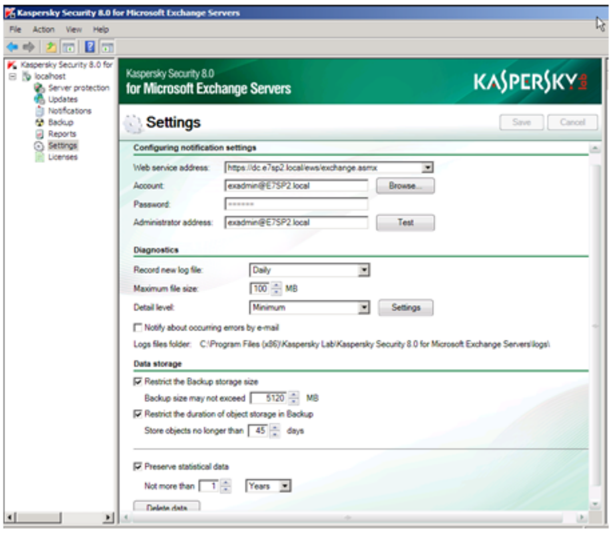
14
October 2010
8:02 PM (UTC + 4)

Anti-Spam report

Server name DC
Reported period 07 Oct 2010 (UTC) - 13 Oct 2010 (UTC)

Verdict	Number of messages	Percentage	Size
Contains no spam	0	0%	0 MB
Spam	0	0%	0 MB
Probable spam	0	0%	0 MB
Formal notification	0	0%	0 MB
Blacklisted	0	0%	0 MB
Trusted	0	0%	0 MB
Not scanned	0	0%	0 MB
Total	0	0%	0 MB

Settings tab used to set up some main system configuration like logging and backup storage capacity.



Configuring notification settings

Web service address: https://dc.e7sp2.local/ews/exchange.asmx

Account: exadmin@E7SP2.local

Password: *******

Administrator address: exadmin@E7SP2.local

Diagnostics

Record new log file: Daily

Maximum file size: 100 MB

Detail level: Minimum

☐ Notify about occurring errors by e-mail

Logs files folder: C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security 8.0 for Microsoft Exchange Servers\logs\

Data storage

☑ Restrict the Backup storage size

Backup size may not exceed 5120 MB

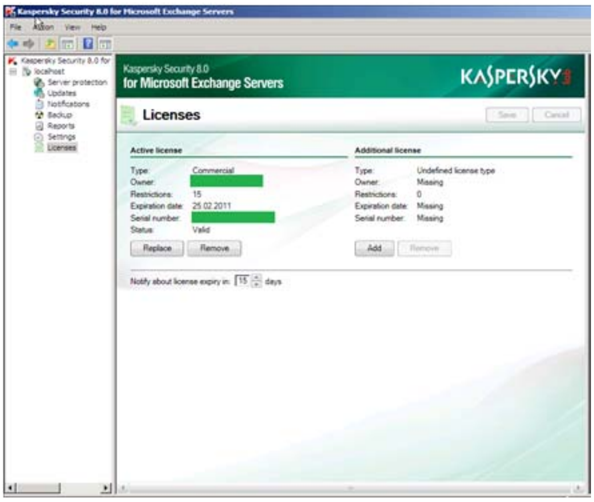
☑ Restrict the duration of object storage in Backup

Store objects no longer than 45 days

☑ Preserve statistical data

Not more than 1 Years

And final License tab used for license management.



Active license		Additional license	
Type:	Commercial	Type:	Undefined license type
Owner:	[redacted]	Owner:	Missing
Restrictions:	15	Restrictions:	0
Expiration date:	25.02.2011	Expiration date:	Missing
Serial number:	[redacted]	Serial number:	Missing
Status:	Valid		

Notify about license expiry in: 15 days

Summary

Manufacturer's website

Kaspersky's website (**www.kaspersky.com**) conforms to normal Internet standards and is easy to find your way around.

There is also a "security zone" where you can find out about viruses and other types of malware.

The installation process

There is a lot of information to be entered during the setup process. However, the cleverly designed setup wizards are a big help, and so even inexperienced users can carry out the installation quickly and easily.

The configuration is also made easy by the wizards.

The entire suite can be installed and configured in minimal time, without having to consult the manual.

The administration console

As with the product we tested last year, Kaspersky knows how to make life easy for the user, and so the entire configuration process is child's play.

The MMC-compatible console, with its graphical presentation in the functions pane is particularly pleasing.

Deployment areas

Kaspersky is at home in networks of all sizes, and the Active Directory integration is a big help. It is only in very large networks that the product might be a little inconvenient.

Antivirus clients

The client software is, as usual for Kaspersky, very professionally produced, and hard to find fault with.

Summary

Kaspersky has, as it did last year, produced a very good corporate suite, which can be recommended to everyone without reservation.

The setup wizards and administrator interface make working with the suite very easy.

It is of particular note that Kaspersky is one of very few manufacturers to produce a real-time display of the status of client deployment.

It is actually mystifying that other software companies don't follow Kaspersky's excellent example and allow the administrator to keep up with the installation status of the clients.

Pros

+ Real-time status of tasks
+ Graphic display in administrator console
+ Simple remote Installation
+ Excellent setup wizards
+ Quick and easy installation

Cons

- Limited Exchange functions

Deployment areas

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★	★★★★	★★★★

Summary

Installation Wizard	★★★★
User Navigation	★★★★★
Administrator Console	★★★★★
Default Values	★★★★
MS Active Directory Support	★★★★
Database Support	★★★★★
Remote Installation	★★★★★
Website	★★★★★
Manual	★★★★

McAfee

Test Software:

McAfee Total Protection for Endpoint ⇨

File Server Protection

Exchange Server Mail Protection

Client Virus Protection

Installation process

Downloading the products

The layout of the McAfee website is simple. It is, however, the least informative of all the manufacturer's websites in this review. You could be forgiven for thinking that it serves rather more as a storage area for developers' documents, and less as a source of information for customers.

Even after searching the website for hours, it is still not clear to the corporate user which products to choose.

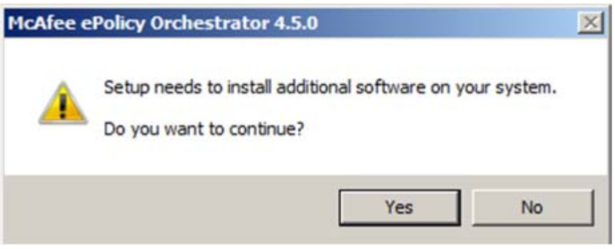
Having eventually reached the download area for the trial versions, you are faced with a huge variety of products. There is a filter function, but the labelling of the filter options is just as mysterious as the naming of the products.

Registration is necessary to obtain a trial key. This is valid for 30 days, which is sufficient time to test the selected product thoroughly.

When we reviewed the beta release of McAfee's ePolicy Orchestrator management server we were pleased to see it bypasses this web site complexity. ePO provides a Software Manager screen that presents the user a list of available evaluation and licensed software for download directly into the management server.

Product installation

We begin the installation of the "Total Protection Suite for Endpoint". The first task is to confirm that additional software packets should be installed:

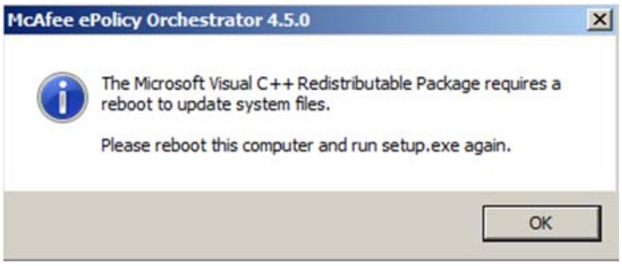


McAfee ePolicy Orchestrator 4.5.0

Setup needs to install additional software on your system.

Do you want to continue?

We confirm this installation. We note that McAfee is one of very few manufacturers to demand a restart of the server after installing the C++ Redistributable Package:

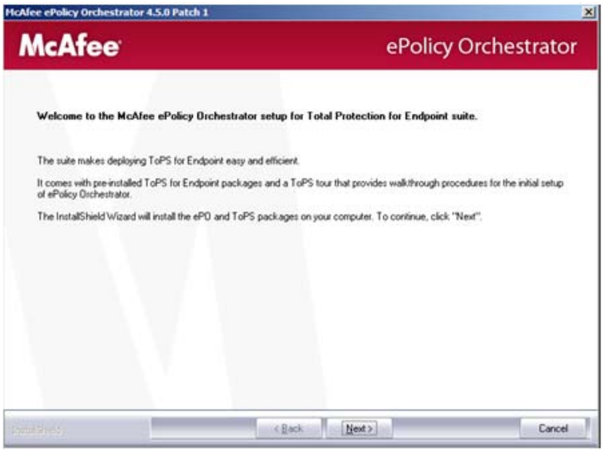


McAfee ePolicy Orchestrator 4.5.0

The Microsoft Visual C++ Redistributable Package requires a reboot to update system files.

Please reboot this computer and run setup.exe again.

Now the installation proper can begin:



McAfee ePolicy Orchestrator 4.5.0 Patch 1

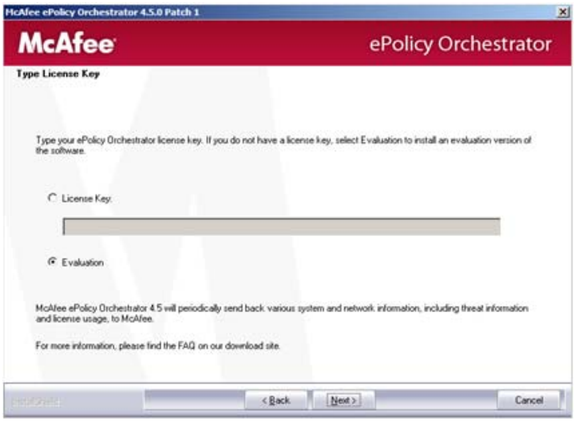
Welcome to the McAfee ePolicy Orchestrator setup for Total Protection for Endpoint suite.

The suite makes deploying ToPS for Endpoint easy and efficient.

It comes with pre-installed ToPS for Endpoint packages and a ToPS tour that provides walkthrough procedures for the initial setup of ePolicy Orchestrator.

The InstallShield Wizard will install the ePO and ToPS packages on your computer. To continue, click "Next".

Next we have the choice of entering a licence key, or using a test version:



McAfee ePolicy Orchestrator 4.5.0 Patch 1

Type License Key

Type your ePolicy Orchestrator license key. If you do not have a license key, select Evaluation to install an evaluation version of the software.

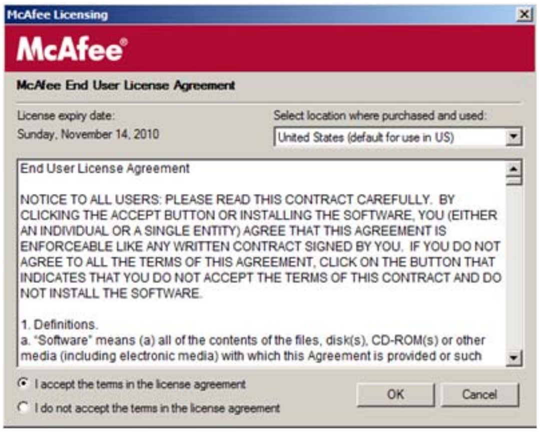
○ License Key:

● Evaluation

McAfee ePolicy Orchestrator 4.5 will periodically send back various system and network information, including threat information and license usage, to McAfee.

For more information, please find the FAQ on our download site.

We accept the licence agreement:



McAfee Licensing

McAfee End User License Agreement

License expiry date: Sunday, November 14, 2010

Select location where purchased and used: United States (default for use in US)

End User License Agreement

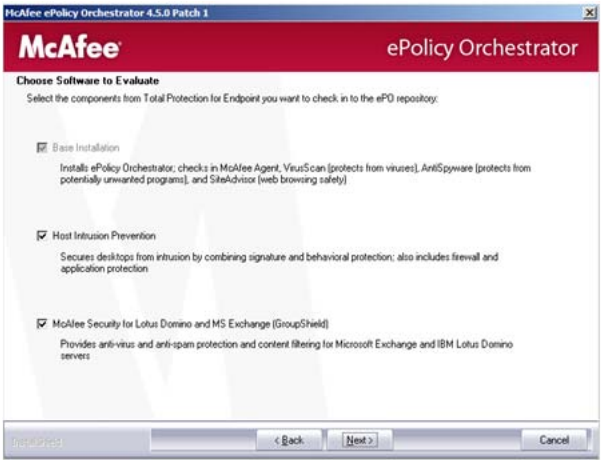
NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT CAREFULLY. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS CONTRACT AND DO NOT INSTALL THE SOFTWARE.

1. Definitions.
a. "Software" means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) with which this Agreement is provided or such

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Following this, we can choose the scope of functionality to be installed:



McAfee ePolicy Orchestrator 4.5.0 Patch 1

Choose Software to Evaluate

Select the components from Total Protection for Endpoint you want to check in to the ePO repository:

☑ Base Installation

Installs ePolicy Orchestrator; checks in McAfee Agent, VirusScan (protects from viruses), AntiSpyware (protects from potentially unwanted programs), and SiteAdvisor (web browsing safety)

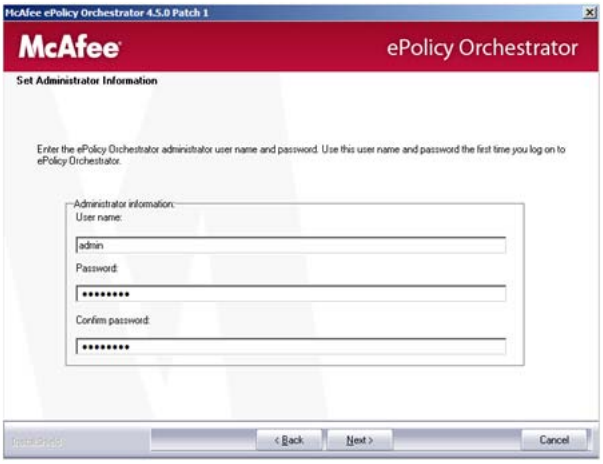
☑ Host Intrusion Prevention

Secures desktops from intrusion by combining signature and behavioral protection; also includes firewall and application protection

☑ McAfee Security for Lotus Domino and MS Exchange (GroupShield)

Provides anti-virus and anti-spam protection and content filtering for Microsoft Exchange and IBM Lotus Domino servers

The next step is to enter the user credentials for the management console:



McAfee ePolicy Orchestrator 4.5.0 Patch 1

Set Administrator Information

Enter the ePolicy Orchestrator administrator user name and password. Use this user name and password the first time you log on to ePolicy Orchestrator.

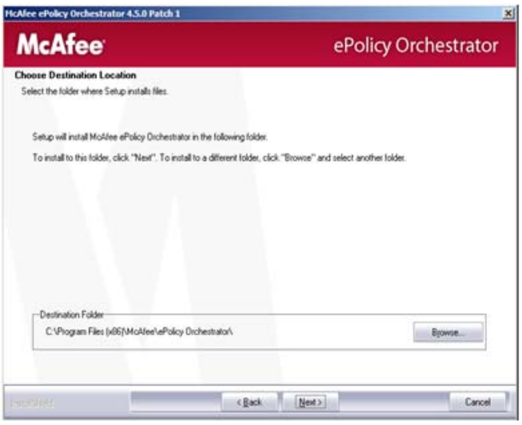
Administrator information:

User name: admin

Password: ••••••••

Confirm password: ••••••••

Here we can select the installation folder:



McAfee ePolicy Orchestrator 4.5.0 Patch 1

Choose Destination Location

Select the folder where Setup installs files.

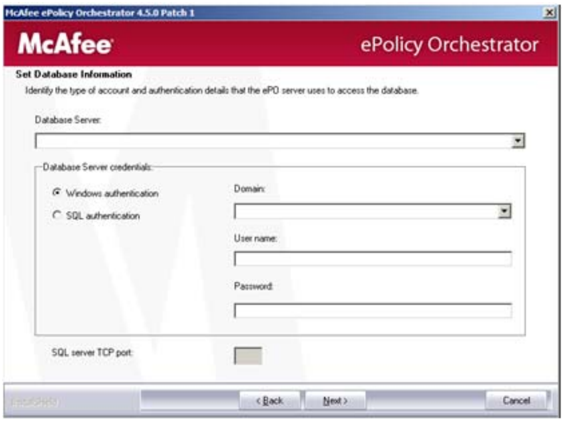
Setup will install McAfee ePolicy Orchestrator in the following folder.

To install to this folder, click "Next". To install to a different folder, click "Browse" and select another folder.

Destination Folder

C:\Program Files (x86)\McAfee\ePolicy Orchestrator\

The access data for the database server is then entered:



McAfee ePolicy Orchestrator 4.5.0 Patch 1

Set Database Information

Identify the type of account and authentication details that the ePO server uses to access the database.

Database Server:

Database Server credentials:

● Windows authentication

○ SQL authentication

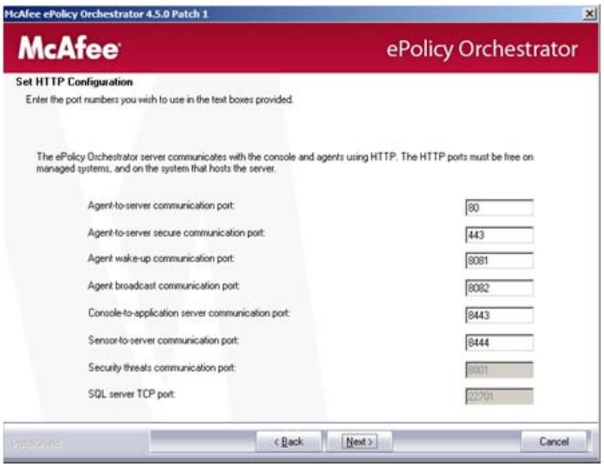
Domain:

User name:

Password:

SQL server TCP port:

This is followed by the choice of ports for communication with the suite:



McAfee ePolicy Orchestrator 4.5.0 Patch 1

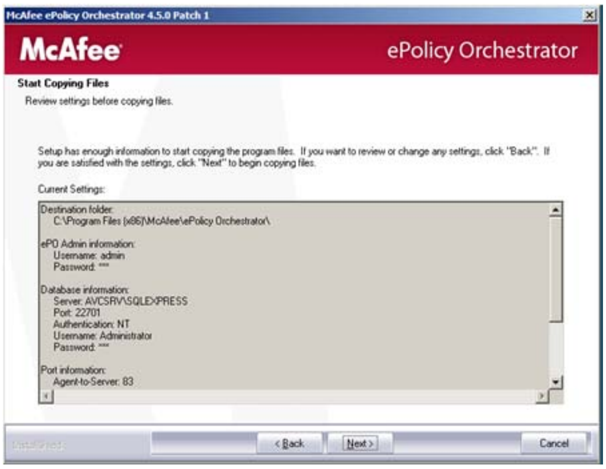
Set HTTP Configuration

Enter the port numbers you wish to use in the text boxes provided.

The ePolicy Orchestrator server communicates with the console and agents using HTTP. The HTTP ports must be free on managed systems, and on the system that hosts the server.

Agent-to-server communication port:	80
Agent-to-server secure communication port:	443
Agent wake-up communication port:	8081
Agent broadcast communication port:	8082
Console-to-application server communication port:	8443
Sensor-to-server communication port:	8444
Security threats communication port:	8801
SQL server TCP port:	22701

The installer now has enough information to complete its task:



McAfee ePolicy Orchestrator 4.5.0 Patch 1

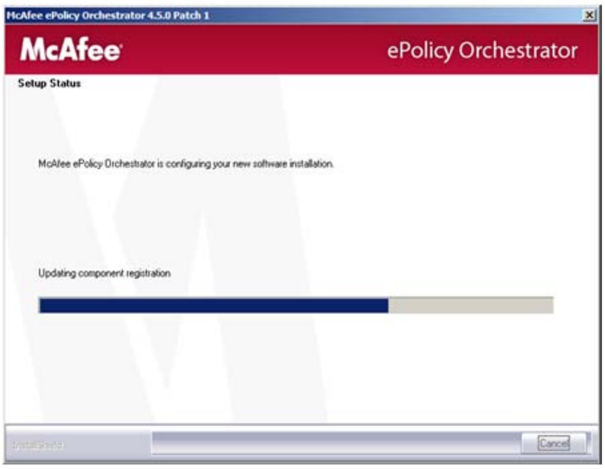
Start Copying Files

Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click "Back". If you are satisfied with the settings, click "Next" to begin copying files.

Current Settings:

```
Destination folder:
    C:\Program Files (x86)\McAfee\ePolicy Orchestrator\

ePO Admin information:
    Username: admin
    Password: ***

Database information:
    Server: AVCSRV\SQLEXPRESS
    Port: 22701
    Authentication: NT
    Username: Administrator
    Password: ***

Port information:
    Agent-to-Server: 83
```



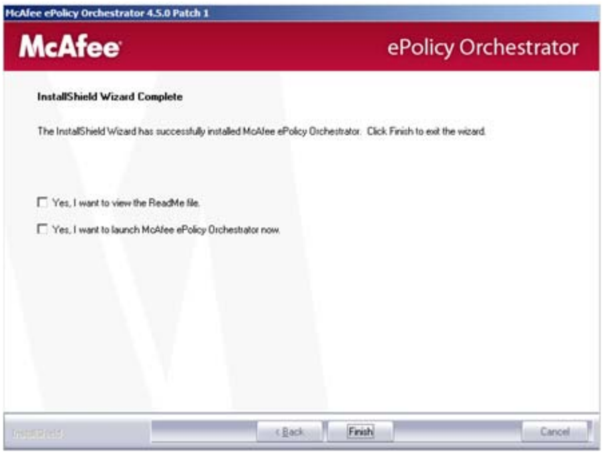
McAfee ePolicy Orchestrator 4.5.0 Patch 1

Setup Status

McAfee ePolicy Orchestrator is configuring your new software installation.

Updating component registration

When installation is complete, we start the “Orchestrator” to carry out the configuration:



McAfee ePolicy Orchestrator 4.5.0 Patch 1

InstallShield Wizard Complete

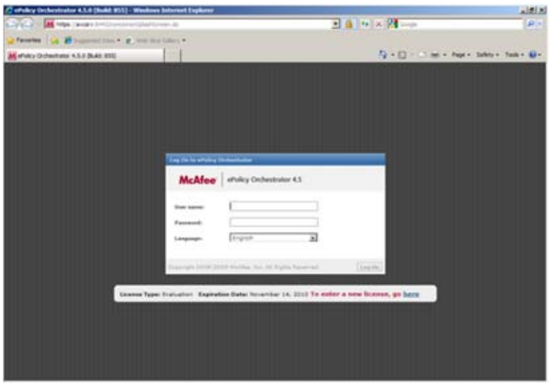
The InstallShield Wizard has successfully installed McAfee ePolicy Orchestrator. Click Finish to exit the wizard.

☐ Yes, I want to view the ReadMe file.

☐ Yes, I want to launch McAfee ePolicy Orchestrator now.

The management interface

After starting the ePolicy Orchestrator, we are greeted by the login site of the web application:

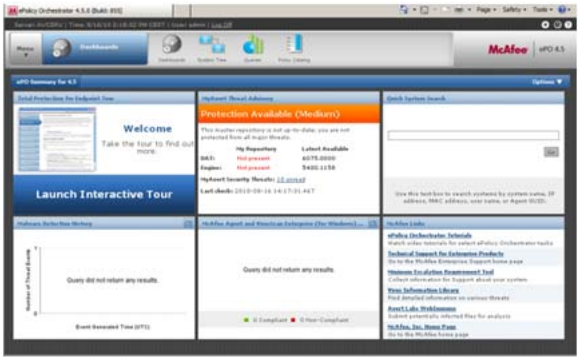

ePolicy Orchestrator 4.5.0 (Build: 855) - Windows Internet Explorer
McAfee
ePolicy Orchestrator 4.5
User name:
Password:
Language:
English
Log On
License Type: Evaluation Expiration Date: November 14, 2010 To enter a new license, go here

The first step is to authenticate yourself.

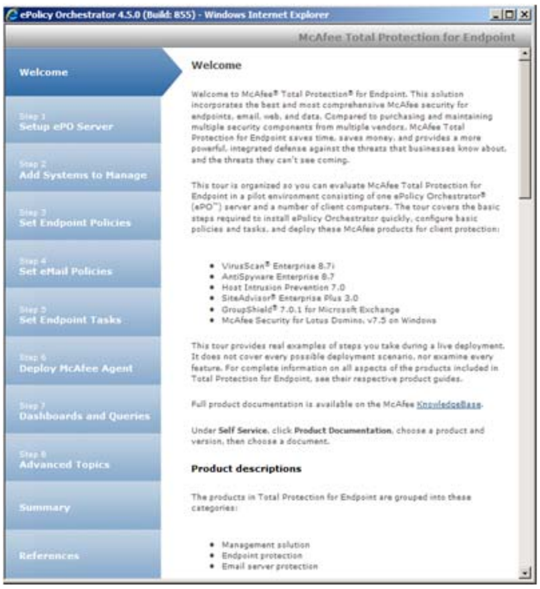
The standard password has to be entered here, which can only be found by reading the handbook.

We confirm without changing the password and log in to the management console for the first time.

The management interface of the Orchestrator has a very pleasing graphic design:


McAfee
Dashboards
Welcome
Take the tour to find out more.
Launch Interactive Tour
Protection Available (Medium)
Query did not return any results.

McAfee is entering new territory here by offering the user an interactive tour of the suite, in order to learn how to use it, and what the next steps will be:



Welcome

Welcome to McAfee® Total Protection® for Endpoint. This solution incorporates the best and most comprehensive McAfee security for endpoints, email, web, and data. Compared to purchasing and maintaining multiple security components from multiple vendors, McAfee Total Protection for Endpoint saves time, saves money, and provides a more powerful, integrated defense against the threats that businesses know about, and the threats they can't see coming.

This tour is organized so you can evaluate McAfee Total Protection for Endpoint in a pilot environment consisting of one ePolicy Orchestrator® (ePO™) server and a number of client computers. The tour covers the basic steps required to install ePolicy Orchestrator quickly, configure basic policies and tasks, and deploy these McAfee products for client protection:

- VirusScan® Enterprise 8.7i
- AntiSpyware Enterprise 8.7
- Host Intrusion Prevention 7.0
- SiteAdvisor® Enterprise Plus 3.0
- GroupShield® 7.0.1 for Microsoft Exchange
- McAfee Security for Lotus Domino, v7.5 on Windows

This tour provides real examples of steps you take during a live deployment. It does not cover every possible deployment scenario, nor examine every feature. For complete information on all aspects of the products included in Total Protection for Endpoint, see their respective product guides.

Full product documentation is available on the McAfee KnowledgeBase.

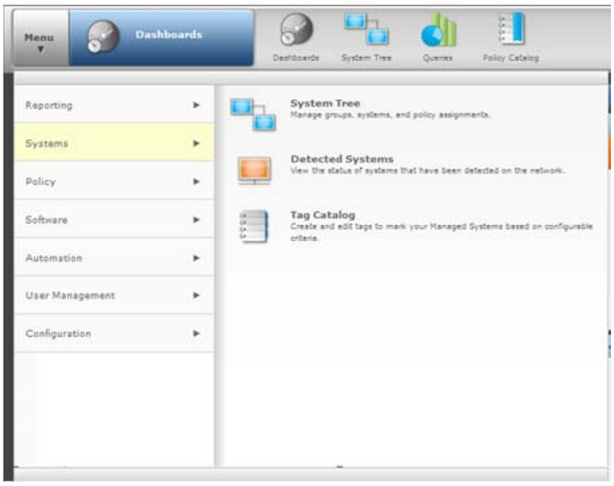
Under **Self Service**, click **Product Documentation**, choose a product and version, then choose a document.

Product descriptions

The products in Total Protection for Endpoint are grouped into these categories:

- Management solution
- Endpoint protection
- Email server protection

The first step is to create groups for network organisation, and assign client PCs to these:

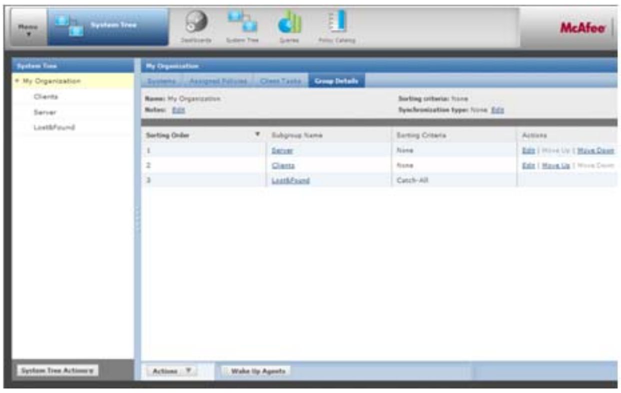


System Tree
Manage groups, systems, and policy assignments.

Detected Systems
View the status of systems that have been detected on the network.

Tag Catalog
Create and edit tags to mark your Managed Systems based on configurable criteria.

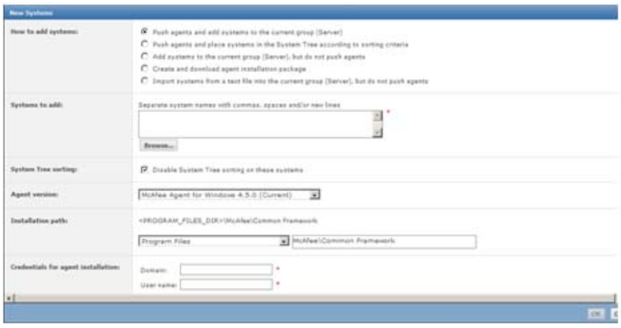
By clicking on System Tree we can begin creating our security structure:



Name: My Organization
Notes: Edit
Sorting criteria: None
Synchronization type: None Edit

Sorting Order	Subgroup Name	Sorting Criteria	Actions
1	Server	None	Edit | Move Up | Move Down
2	Clients	None	Edit | Move Up | Move Down
3	Lost&Found	Catch-All	

Having created two groups, for the server and clients respectively, we add the machines to these:



How to add systems:
● Push agents and add systems to the current group (Server)
○ Push agents and place systems in the System Tree according to sorting criteria
○ Add systems to the current group (Server), but do not push agents
○ Create and download agent installation package
○ Import systems from a text file into the current group (Server), but do not push agents

Systems to add: Separate system names with commas, spaces and/or new lines *

System Tree sorting: ☑ Disable System Tree sorting on these systems

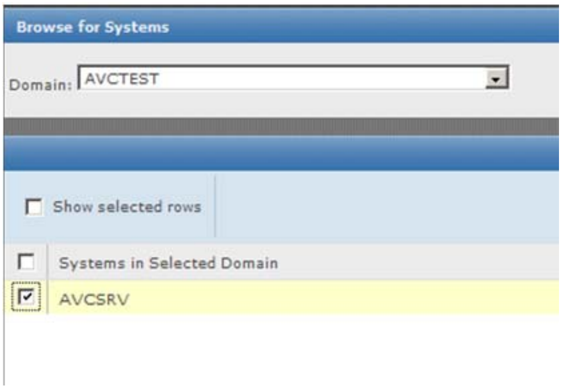
Agent version: McAfee Agent for Windows 4.5.0 (Current)

Installation path: <PROGRAM_FILES_DIR>\McAfee\Common Framework
Program Files | McAfee\Common Framework

Credentials for agent installation:
Domain: *
User name: *

This very extensive form allows the administrator fine control over the process of adding computers, and also enables pre-configuration of some important settings, thus saving a lot of work later.

Having activated the Computer Browser service on the server and entered details of an administrator account, you can select the computers and add them into the security structure:

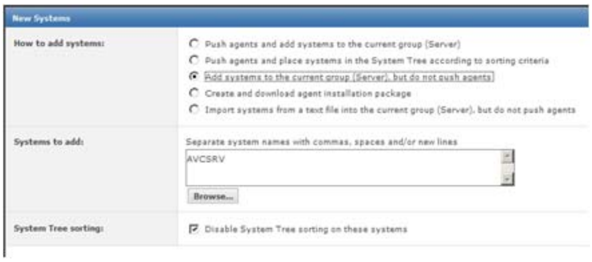


Domain: AVCTEST

□ Show selected rows

□ Systems in Selected Domain
☑ AVCSRV

We import our server with a click on OK:

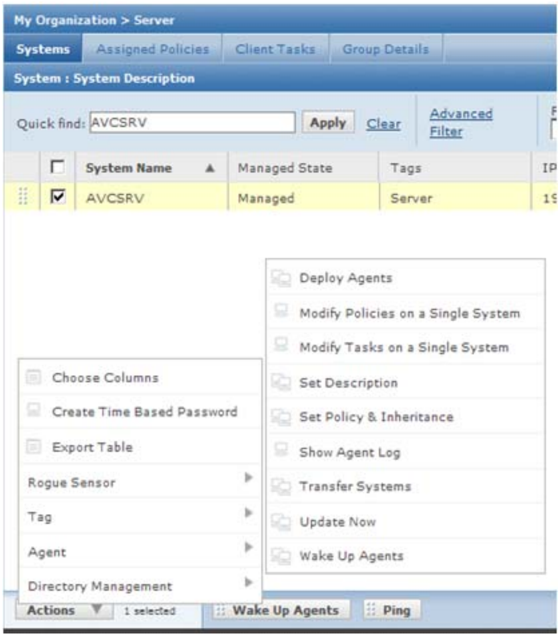


How to add systems:
○ Push agents and add systems to the current group (Server)
○ Push agents and place systems in the System Tree according to sorting criteria
● Add systems to the current group (Server), but do not push agents
○ Create and download agent installation package
○ Import systems from a text file into the current group (Server), but do not push agents

Systems to add: Separate system names with commas, spaces and/or new lines
AVCSRV

System Tree sorting: ☑ Disable System Tree sorting on these systems

When the computer has been added into the group, there is a variety of actions which can be applied to it:

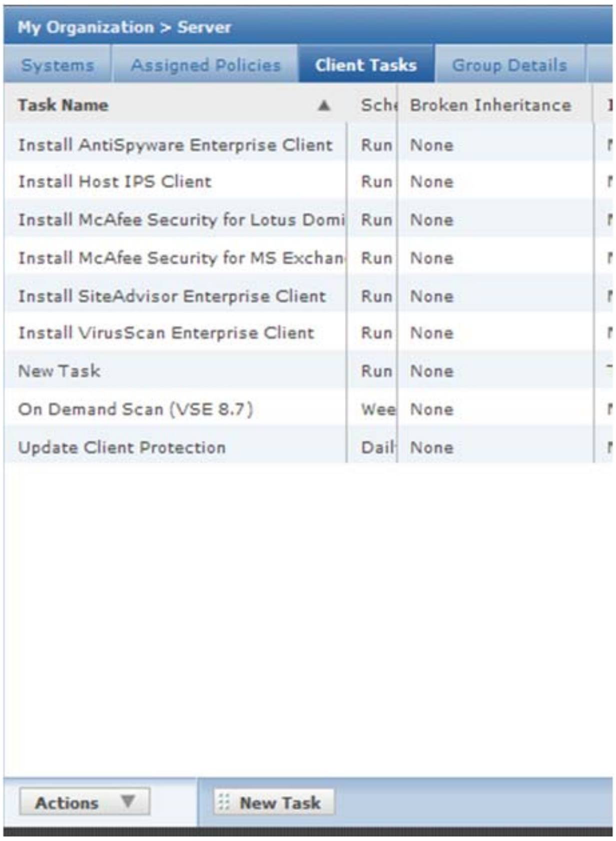


Quick find: AVCSRV

□	System Name	Managed State	Tags	IP
☑	AVCSRV	Managed	Server	19

The scope of the Orchestrator is very wide, and the well-designed web interface makes it very user-friendly. It is very easy to download the necessary software packets and store them in the Repository of the Orchestrator, from where they can be distributed with just a few clicks.

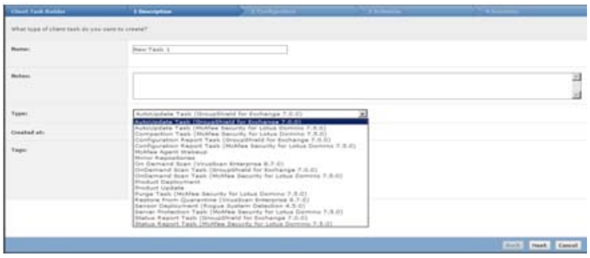
To do this, we go to the Client Tasks area and select “New Task”:



My Organization > Server

Task Name	Sch	Broken Inheritance
Install AntiSpyware Enterprise Client	Run	None
Install Host IPS Client	Run	None
Install McAfee Security for Lotus Domi	Run	None
Install McAfee Security for MS Exchan	Run	None
Install SiteAdvisor Enterprise Client	Run	None
Install VirusScan Enterprise Client	Run	None
New Task	Run	None
On Demand Scan (VSE 8.7)	Wee	None
Update Client Protection	Dail	None

The wizard that then starts has a wide variety of tasks which can be applied to our selected computers.



What type of client task do you want to create?

Name: New Task 1

Notes:

Type: AutoUpdate Task (GroupShield for Exchange 7.0.0)

Created at:

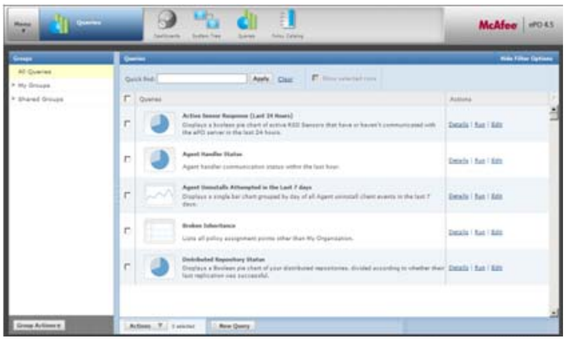
Tags:

AutoUpdate Task (GroupShield for Exchange 7.0.0)
AutoUpdate Task (McAfee Security for Lotus Domino 7.5.0)
Compaction Task (McAfee Security for Lotus Domino 7.5.0)
Configuration Report Task (GroupShield for Exchange 7.0.0)
Configuration Report Task (McAfee Security for Lotus Domino 7.5.0)
McAfee Agent Wakeup
Mirror Repositories
On Demand Scan (VirusScan Enterprise 8.7.0)
OnDemand Scan Task (GroupShield for Exchange 7.0.0)
OnDemand Scan Task (McAfee Security for Lotus Domino 7.5.0)
Product Deployment
Product Update
Purge Task (McAfee Security for Lotus Domino 7.5.0)
Restore From Quarantine (VirusScan Enterprise 8.7.0)
Sensor Deployment (Rogue System Detection 4.5.0)
Server Protection Task (McAfee Security for Lotus Domino 7.5.0)
Status Report Task (GroupShield for Exchange 7.0.0)
Status Report Task (McAfee Security for Lotus Domino 7.5.0)

This type of configuration is found throughout the interface and is very easy to get used to. The individual areas are clear and easy to understand, and laid out in a well-structured manner.

The Interactive Learning Tour is intended to make using the suite easier for less experienced users. However, it must be said that the suite is designed more for very large and complicated networks, which of course requires more in the way of knowledge and experience from the user.

The query area is ideally prepared for analysis of the log files, and offers a huge variety of pre-configured queries, which provide a convenient means of finding out all important information about the system.



Queries	Actions
Active Sensor Response (Last 24 Hours) Displays a boolean pie chart of active RSD Sensors that have or haven't communicated with the ePO server in the last 24 hours.	Details | Run | Edit
Agent Handler Status Agent handler communication status within the last hour.	Details | Run | Edit
Agent Uninstalls Attempted in the Last 7 days Displays a single bar chart grouped by day of all Agent uninstall client events in the last 7 days.	Details | Run | Edit
Broken Inheritance Lists all policy assignment points other than My Organization.	Details | Run | Edit
Distributed Repository Status Displays a Boolean pie chart of your distributed repositories, divided according to whether their last replication was successful.	Details | Run | Edit

It is also very practical that the Exchange protection has been installed at the same time, and everything can be controlled using the Orchestrator. McAfee has definitely created one of the best all-in-one management consoles here.

Summary

Manufacturer's website

The McAfee website (**www.mcafee.com**) conforms to normal Internet design standards.

Unfortunately, it is very easy to get lost on the website, due to the confusing mass of different products. For a corporate user, it is practically impossible to find clear information about the available suites. You are simply overwhelmed with information and cannot get any sort of overview.

This should be improved by McAfee as soon as possible, either by simplifying their product line or finding a way of presenting their products more clearly.

The installation process

When you have eventually managed to find the right suite, you can look forward to a very easy installation.

The fact that the management console, Exchange protection and intrusion prevention system are installed together by one setup program saves a great deal of time and effort.

Other manufacturers should see this as an example and follow suit. Too many "suites" come in the form of separate products with separate installers.

The administrator console

The ePolicy Orchestrator is currently one of the best and most powerful management consoles on the market.

After just a short familiarisation period, the user can carry out the most complex tasks easily.

The enormous functionality and organisational opportunities mean that the Orchestrator is very suitable for large and complex networks.

Deployment areas

In short, all networks!

Antivirus clients

The client software is very user-friendly and easy to find your way around, with no obvious flaws.

Summary

After the initial confusion on the website, you will be very pleasantly surprised by the suite.

Installation is very simple. The management console provides trend-setting solutions in several areas, and the degree of functionality is impressive.

Whether you need to protect a small network or a huge domain, the McAfee suite will be ideally suited for all requirements.

Pros

- + Outstanding administration console
- + Simple configuration
- + Very good grouping functions
- + Quick and easy installation

Cons

- - Very confusing website

Deployment areas

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★★	★★★★★	★★★★★

Summary

Installation Wizard	★★★★★
User Navigation	★★★★★
Administrator Console	★★★★★
Default Values	★★★★
MS Active Directory Support	★★★★
Database Support	★★★★★
Remote Installation	★★★★★
Website	★★
Manual	★★★★

Sophos

Test Software:

SOPHOS Endpoint Security and Control →	File Server Protection / Client Virus Protection / Management Console
SOPHOS PureMessage →	Exchange Server Protection

Installation

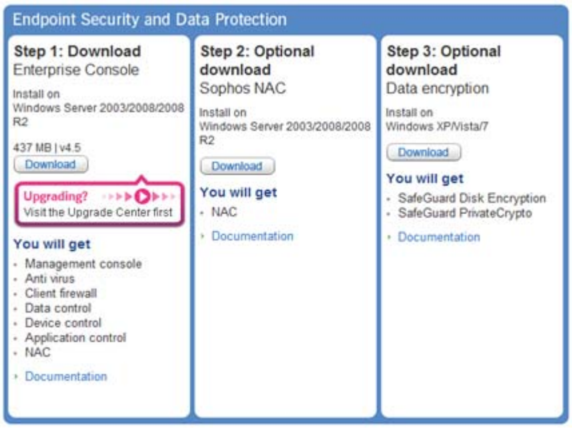
Downloading the product

The website impresses with its pleasant design. It is simple, clear and fast.

Registration is necessary to obtain a free trial key. This gives an adequate 30 days to test the software.

The inexperienced user should take some time to understand NAC; he or she may otherwise waste time trying to find the additional module, which may not be necessary.

By the time you come to download the product, it should be clear which component does what:



Endpoint Security and Data Protection

Step 1: Download
Enterprise Console

Install on
Windows Server 2003/2008/2008 R2

437 MB | v4.5

Upgrading?
Visit the Upgrade Center first

You will get

- Management console
- Anti virus
- Client firewall
- Data control
- Device control
- Application control
- NAC

Step 2: Optional download
Sophos NAC

Install on
Windows Server 2003/2008/2008 R2

You will get

- NAC

Step 3: Optional download
Data encryption

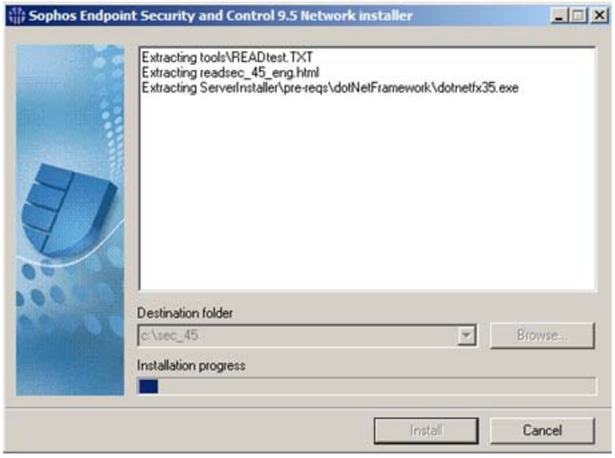
Install on
Windows XP/Vista/7

You will get

- SafeGuard Disk Encryption
- SafeGuard PrivateCrypto

Product installation

The first task is to unpack the installation files to the local hard drive:



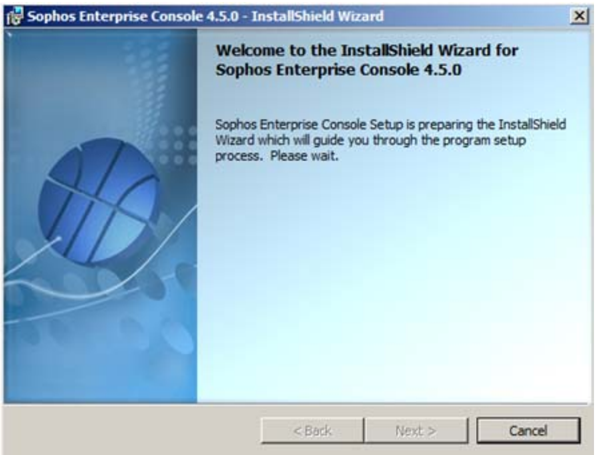
Sophos Endpoint Security and Control 9.5 Network installer

```
Extracting tools\READtest.TXT
Extracting readsec_45_eng.html
Extracting ServerInstaller\pre-reqs\dotNetFramework\dotnetfx35.exe
```

Destination folder: c:\sec_45

Installation progress

We are then greeted by the install wizard:

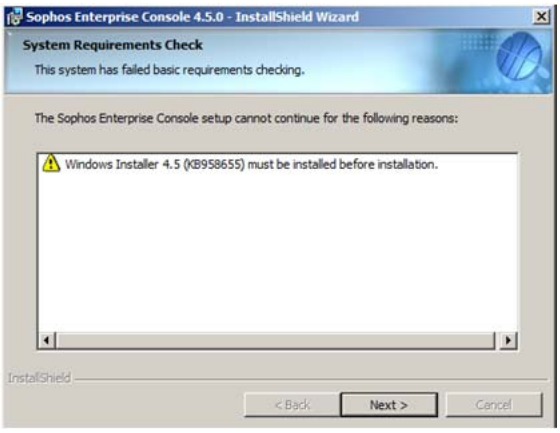


Sophos Enterprise Console 4.5.0 - InstallShield Wizard

Welcome to the InstallShield Wizard for Sophos Enterprise Console 4.5.0

Sophos Enterprise Console Setup is preparing the InstallShield Wizard which will guide you through the program setup process. Please wait.

Next, the setup programs checks that its requirements are met:



Sophos Enterprise Console 4.5.0 - InstallShield Wizard

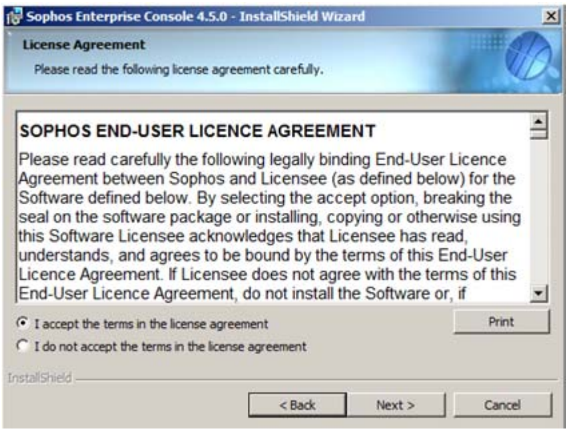
System Requirements Check

This system has failed basic requirements checking.

The Sophos Enterprise Console setup cannot continue for the following reasons:

⚠ Windows Installer 4.5 (KB958655) must be installed before installation.

In this case we have to update to the newest Windows Installer (it is worth checking before installation that this is up to date). Having done this, we can proceed with the installation, and accept the licence agreement:



Sophos Enterprise Console 4.5.0 - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

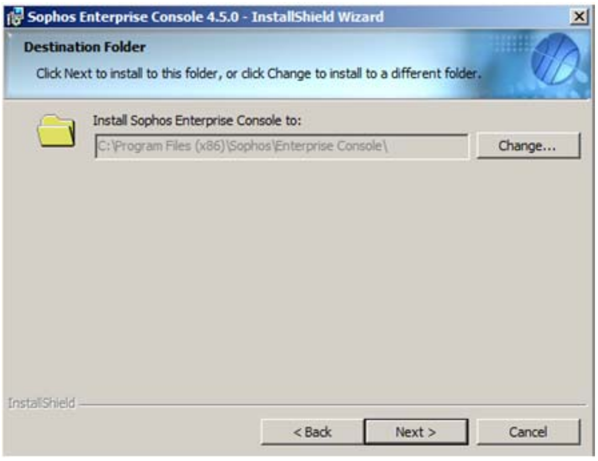
SOPHOS END-USER LICENCE AGREEMENT

Please read carefully the following legally binding End-User Licence Agreement between Sophos and Licensee (as defined below) for the Software defined below. By selecting the accept option, breaking the seal on the software package or installing, copying or otherwise using this Software Licensee acknowledges that Licensee has read, understands, and agrees to be bound by the terms of this End-User Licence Agreement. If Licensee does not agree with the terms of this End-User Licence Agreement, do not install the Software or, if

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Next we can choose the installation folder:



Sophos Enterprise Console 4.5.0 - InstallShield Wizard

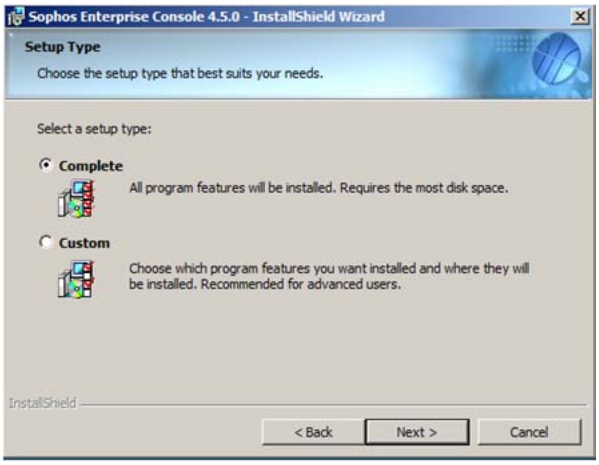
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Sophos Enterprise Console to:

C:\Program Files (x86)\Sophos\Enterprise Console\

Sophos gives us the option of a "Complete" or "Custom" installation:



Sophos Enterprise Console 4.5.0 - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Select a setup type:

● Complete

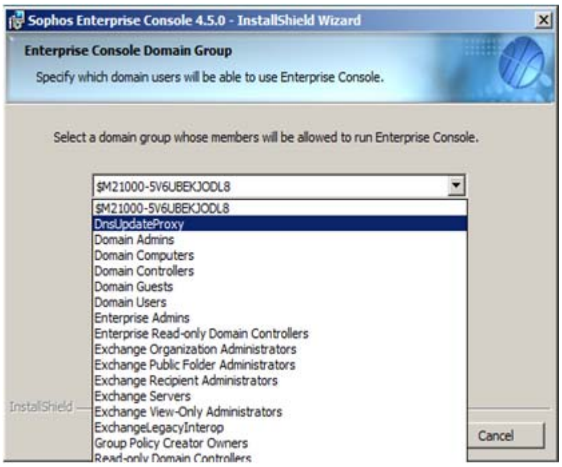
All program features will be installed. Requires the most disk space.

○ Custom

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

We choose the "Complete" option.

As in last year's test, we can only applaud Sophos' optimal Active Directory support. The next step allows us to choose an AD group which will be given administrator access to the suite:



Sophos Enterprise Console 4.5.0 - InstallShield Wizard

Enterprise Console Domain Group

Specify which domain users will be able to use Enterprise Console.

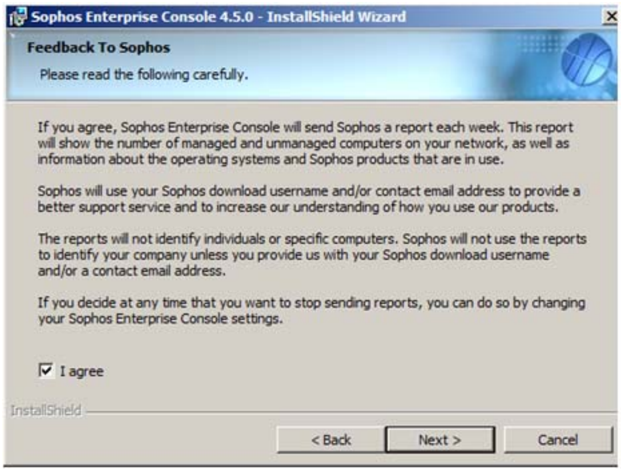
Select a domain group whose members will be allowed to run Enterprise Console.

$M21000-5V6UBEKJODL8

- $M21000-5V6UBEKJODL8
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users
- Enterprise Admins
- Enterprise Read-only Domain Controllers
- Exchange Organization Administrators
- Exchange Public Folder Administrators
- Exchange Recipient Administrators
- Exchange Servers
- Exchange View-Only Administrators
- ExchangeLegacyInterop
- Group Policy Creator Owners
- Read-only Domain Controllers

Sophos offers a service that sends information on installation and operation of the system to them, in order to improve support.

Again, we advise careful consideration as to whether to use this service in high-security environments.



Sophos Enterprise Console 4.5.0 - InstallShield Wizard

Feedback To Sophos

Please read the following carefully.

If you agree, Sophos Enterprise Console will send Sophos a report each week. This report will show the number of managed and unmanaged computers on your network, as well as information about the operating systems and Sophos products that are in use.

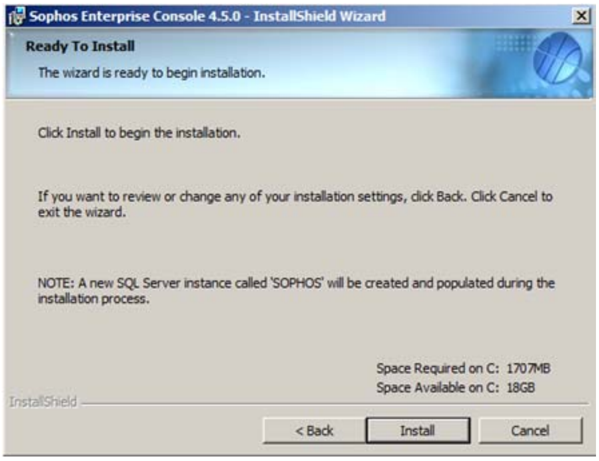
Sophos will use your Sophos download username and/or contact email address to provide a better support service and to increase our understanding of how you use our products.

The reports will not identify individuals or specific computers. Sophos will not use the reports to identify your company unless you provide us with your Sophos download username and/or a contact email address.

If you decide at any time that you want to stop sending reports, you can do so by changing your Sophos Enterprise Console settings.

☑ I agree

The installer has now gathered sufficient information to proceed. With the Complete installation, SQL Server Express is installed:



Sophos Enterprise Console 4.5.0 - InstallShield Wizard

Ready To Install

The wizard is ready to begin installation.

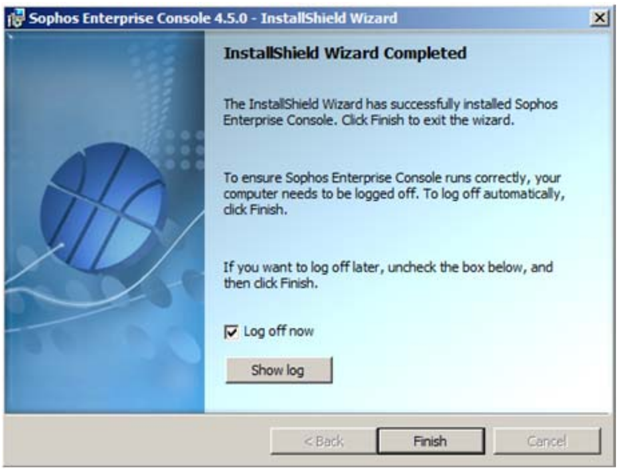
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

NOTE: A new SQL Server instance called 'SOPHOS' will be created and populated during the installation process.

Space Required on C: 1707MB
Space Available on C: 18GB

When installation has finished, the installer informs us that the current user must log out of Windows to complete the installation:



Sophos Enterprise Console 4.5.0 - InstallShield Wizard

InstallShield Wizard Completed

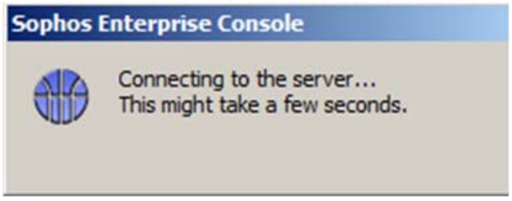
The InstallShield Wizard has successfully installed Sophos Enterprise Console. Click Finish to exit the wizard.

To ensure Sophos Enterprise Console runs correctly, your computer needs to be logged off. To log off automatically, click Finish.

If you want to log off later, uncheck the box below, and then click Finish.

☑ Log off now

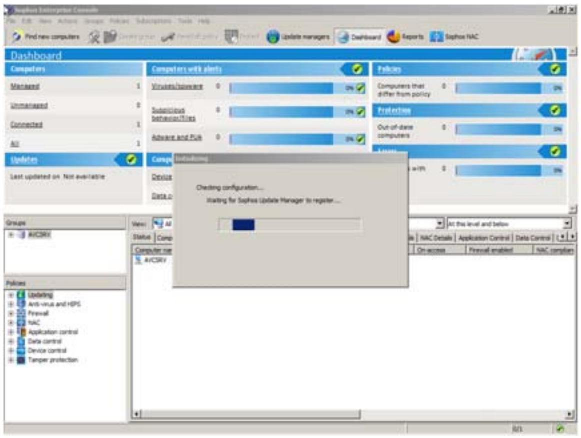
Immediately after the user has logged on again, the Sophos wizard appears and connects to the newly installed management server:



Sophos Enterprise Console

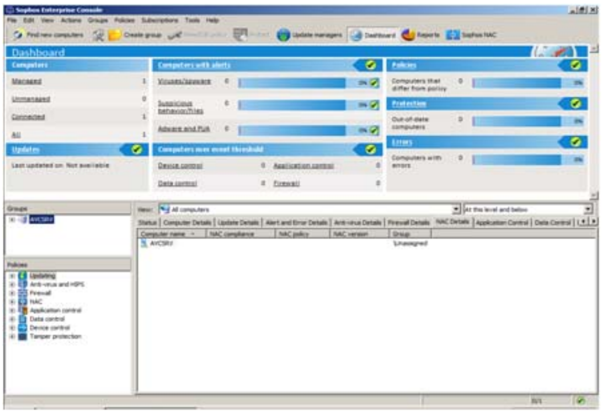
Connecting to the server...
This might take a few seconds.

When the management console has started, the configuration is checked:


Checking configuration...
Waiting for Sophos Update Manager to register...

The management interface

Sophos is one of very few manufacturers to have their own management console design. This is very well thought out and structured:



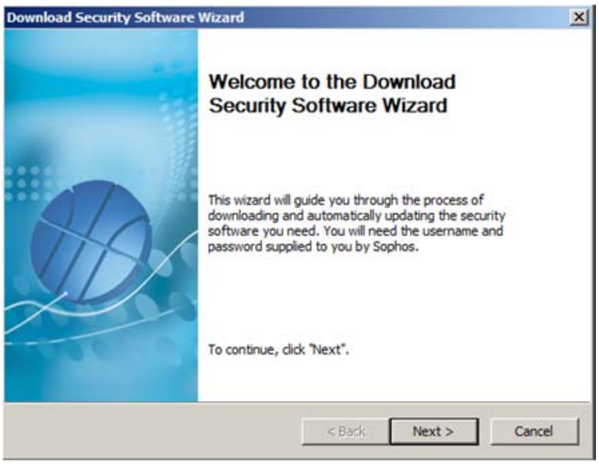
We particularly like the dashboard with its overview of the state of all important security aspects. The experienced user will see the immediate tasks at a glance:

1. Create network organisation groups and add computers to these
2. Configure updates
3. Remote installation of the client software
4. Changes to the central configuration

The most important commands can be found as buttons with appropriate icons on the menu bar.

The second section is the configuration area, where the organisational structures are created and configuration is assigned according to policies. This layout is simple and convenient.

Our first task is to start the download wizard which will obtain the additional software needed to protect the clients:

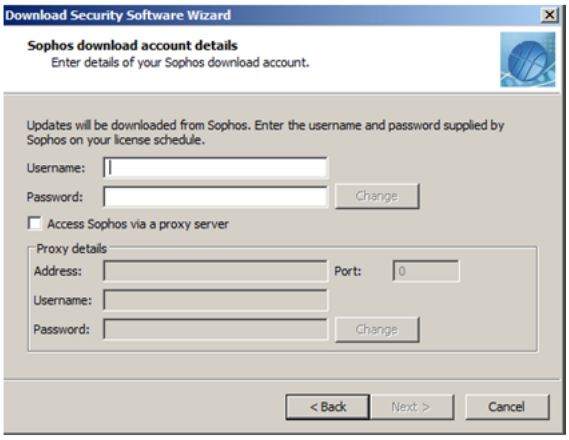

Download Security Software Wizard

Welcome to the Download Security Software Wizard

This wizard will guide you through the process of downloading and automatically updating the security software you need. You will need the username and password supplied to you by Sophos.

To continue, click "Next".

Now we have to enter the username and password for the Sophos download account. In the event that the system connects to the Internet via a proxy server, this information can be added in the same dialog box:


Download Security Software Wizard

Sophos download account details
Enter details of your Sophos download account.

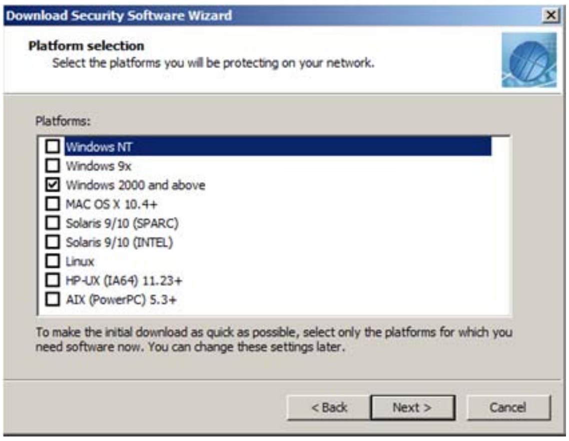
Updates will be downloaded from Sophos. Enter the username and password supplied by Sophos on your license schedule.

Username:
Password:

□ Access Sophos via a proxy server

Proxy details
Address: Port: 0
Username:
Password:

The next page of the wizard allows client software for different operating systems, including Mac and Linux, to be selected:



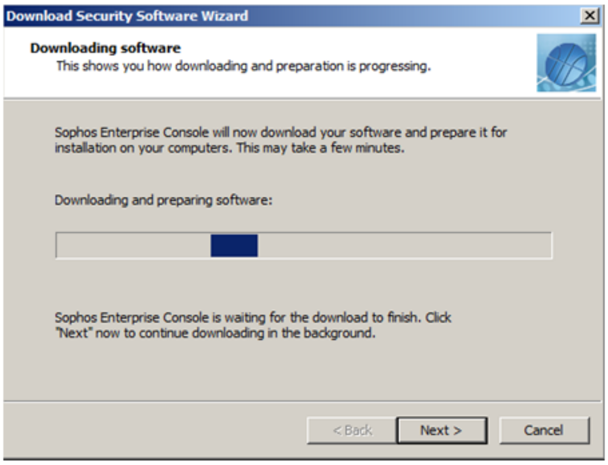
Platform selection
Select the platforms you will be protecting on your network.

Platforms:

- □ Windows NT
- □ Windows 9x
- ☑ Windows 2000 and above
- □ MAC OS X 10.4+
- □ Solaris 9/10 (SPARC)
- □ Solaris 9/10 (INTEL)
- □ Linux
- □ HP-UX (IA64) 11.23+
- □ AIX (PowerPC) 5.3+

To make the initial download as quick as possible, select only the platforms for which you need software now. You can change these settings later.

The necessary files are now downloaded to the hard drive. It is not necessary to wait until the download has completed; you can click on Next to go on to the next page. However, Sophos unfortunately leaves you in the dark as to how fast the download is progressing and when it will finish:



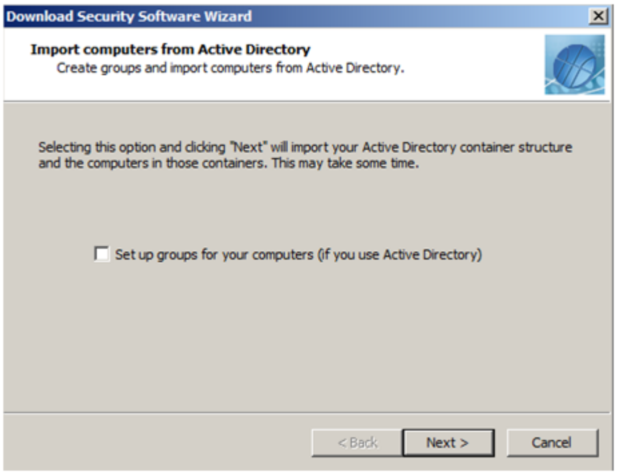
Downloading software
This shows you how downloading and preparation is progressing.

Sophos Enterprise Console will now download your software and prepare it for installation on your computers. This may take a few minutes.

Downloading and preparing software:

Sophos Enterprise Console is waiting for the download to finish. Click "Next" now to continue downloading in the background.

The next stage allows you to use AD to import computers into organisational groups:

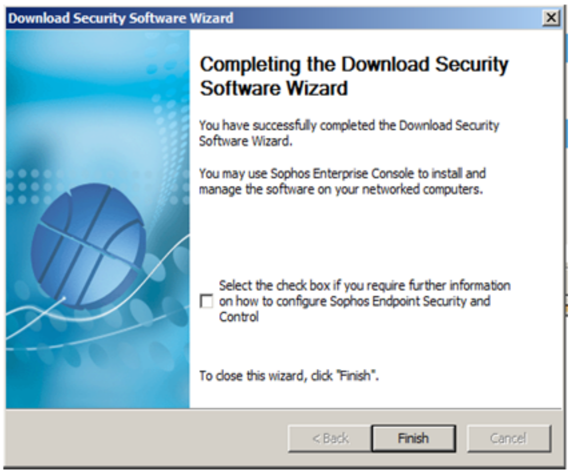


Import computers from Active Directory
Create groups and import computers from Active Directory.

Selecting this option and clicking "Next" will import your Active Directory container structure and the computers in those containers. This may take some time.

□ Set up groups for your computers (if you use Active Directory)

At the end of the wizard, there is the opportunity to view a tutorial on the next stages of the configuration process:



Completing the Download Security Software Wizard

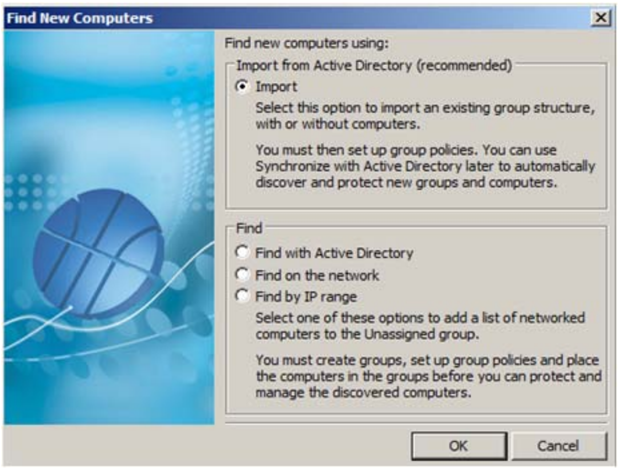
You have successfully completed the Download Security Software Wizard.

You may use Sophos Enterprise Console to install and manage the software on your networked computers.

□ Select the check box if you require further information on how to configure Sophos Endpoint Security and Control

To close this wizard, click "Finish".

As we unfortunately don't know how long we will have to wait before we can start deploying the software to the clients, investigate how easy it is to manually create new security groups.



Find New Computers

Find new computers using:

Import from Active Directory (recommended)

● Import

Select this option to import an existing group structure, with or without computers.

You must then set up group policies. You can use Synchronize with Active Directory later to automatically discover and protect new groups and computers.

Find

○ Find with Active Directory

○ Find on the network

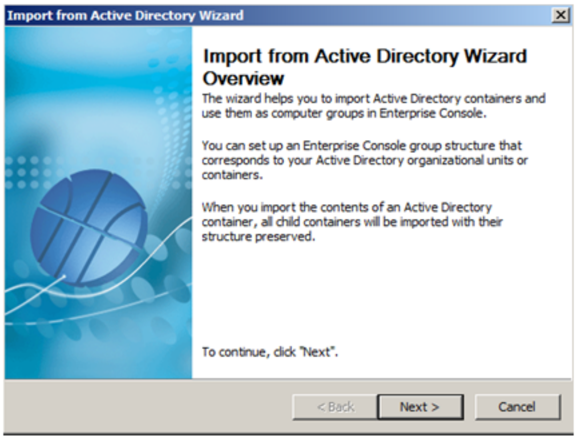
○ Find by IP range

Select one of these options to add a list of networked computers to the Unassigned group.

You must create groups, set up group policies and place the computers in the groups before you can protect and manage the discovered computers.

The wizard above appears after we click on "Find New Computers". Again we see that Sophos has the best Active Directory support of any of the products we have tested here. Even importing complex AD forests is child's play. Of course, it's also possible to add computers that are not part of AD.

For our test, we select "Import from Active Directory":



Import from Active Directory Wizard

Import from Active Directory Wizard Overview

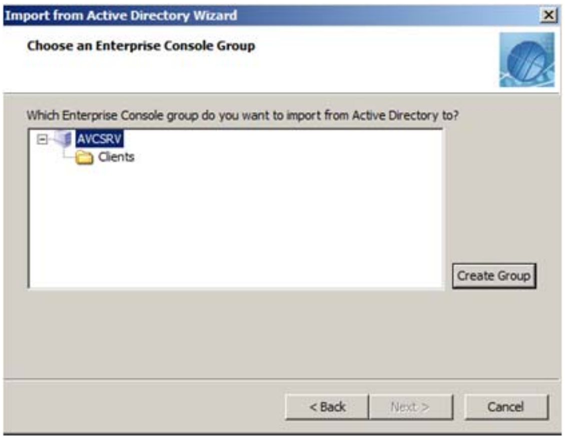
The wizard helps you to import Active Directory containers and use them as computer groups in Enterprise Console.

You can set up an Enterprise Console group structure that corresponds to your Active Directory organizational units or containers.

When you import the contents of an Active Directory container, all child containers will be imported with their structure preserved.

To continue, click "Next".

In the Sophos management console we create a new group called Clients, and use it to import our Client group from AD:

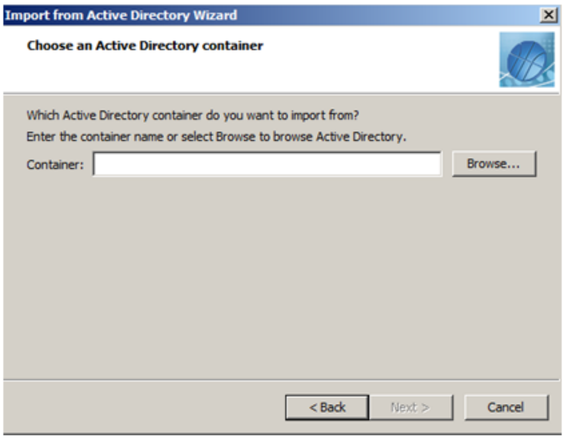


Import from Active Directory Wizard

Choose an Enterprise Console Group

Which Enterprise Console group do you want to import from Active Directory to?

Next we look for the AD container with our client PC in:



Import from Active Directory Wizard

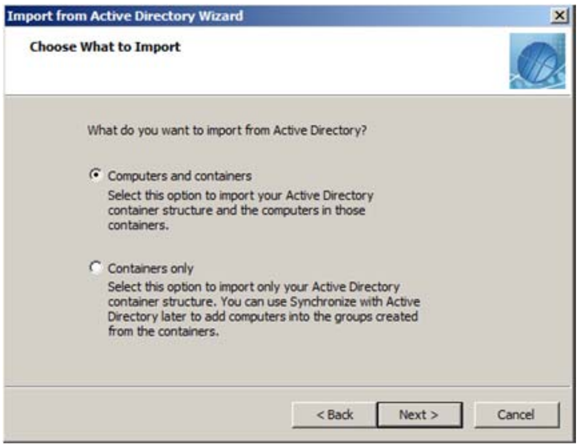
Choose an Active Directory container

Which Active Directory container do you want to import from?

Enter the container name or select Browse to browse Active Directory.

Container:

The container structure can be imported here as well, making it the quickest and most convenient method of importing groups:



Import from Active Directory Wizard

Choose What to Import

What do you want to import from Active Directory?

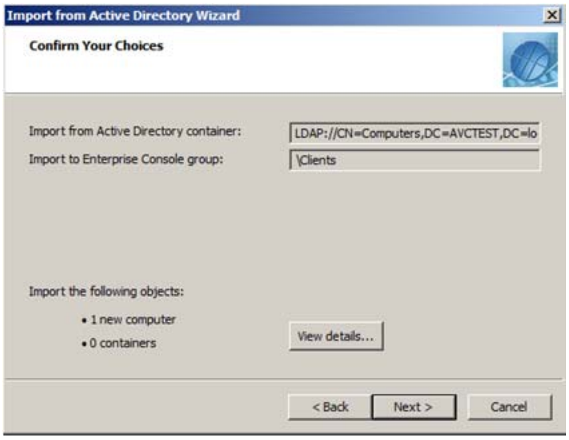
● Computers and containers

Select this option to import your Active Directory container structure and the computers in those containers.

○ Containers only

Select this option to import only your Active Directory container structure. You can use Synchronize with Active Directory later to add computers into the groups created from the containers.

A summary is displayed, and then the import process can proceed:



Import from Active Directory Wizard

Confirm Your Choices

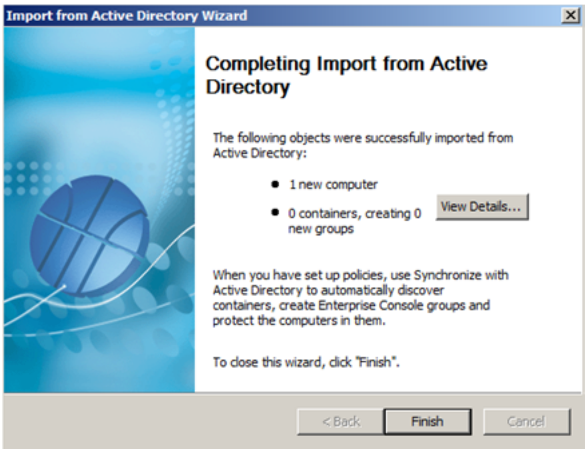
Import from Active Directory container: LDAP://CN=Computers,DC=AVCTEST,DC=lo

Import to Enterprise Console group: \Clients

Import the following objects:

- 1 new computer
- 0 containers

The results of the import wizard are displayed at the end:



Import from Active Directory Wizard

Completing Import from Active Directory

The following objects were successfully imported from Active Directory:

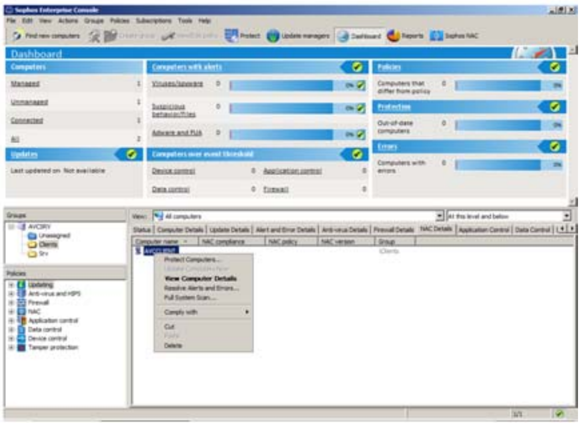
- 1 new computer
- 0 containers, creating 0 new groups

When you have set up policies, use Synchronize with Active Directory to automatically discover containers, create Enterprise Console groups and protect the computers in them.

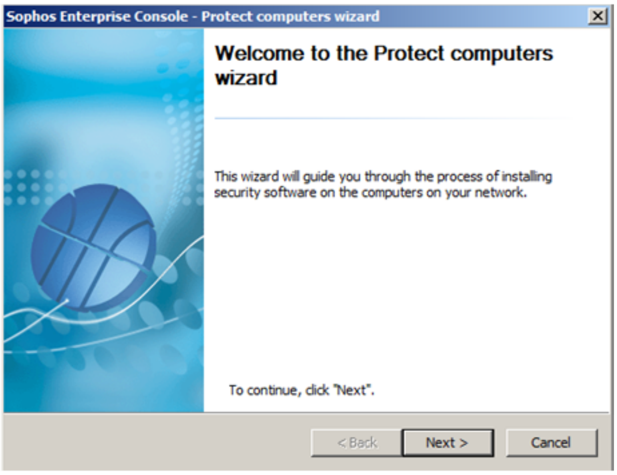
To close this wizard, click "Finish".

At this point we still do not know how far the downloader has progressed with obtaining the client software; we can do little except wait. It is hard to understand why an otherwise highly professional suite gives no information at all as to the status of the download.

Once we have ascertained that the client software is available, we can proceed with the installation of the client PCs. To do this, we right-click on the computer we have just imported and select "Protect Computers":



The Protect Computers wizard starts:



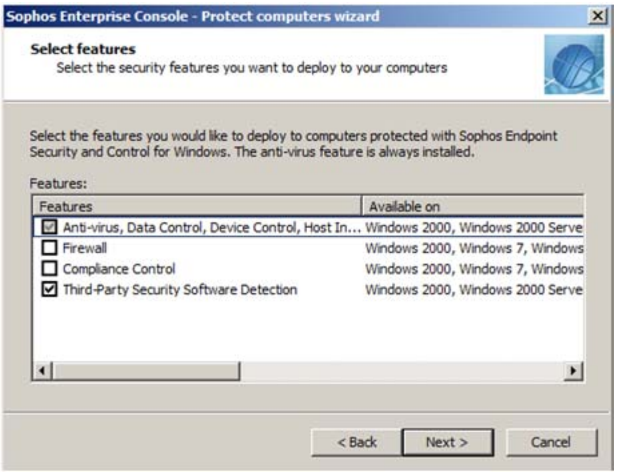
Sophos Enterprise Console - Protect computers wizard

Welcome to the Protect computers wizard

This wizard will guide you through the process of installing security software on the computers on your network.

To continue, click "Next".

Next we can select the features to be installed on the client:



Sophos Enterprise Console - Protect computers wizard

Select features

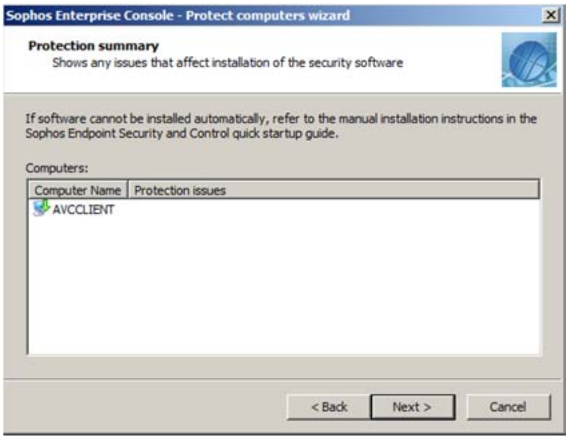
Select the security features you want to deploy to your computers

Select the features you would like to deploy to computers protected with Sophos Endpoint Security and Control for Windows. The anti-virus feature is always installed.

Features:

Features	Available on
☑ Anti-virus, Data Control, Device Control, Host In...	Windows 2000, Windows 2000 Serve
☐ Firewall	Windows 2000, Windows 7, Windows
☐ Compliance Control	Windows 2000, Windows 7, Windows
☑ Third-Party Security Software Detection	Windows 2000, Windows 2000 Serve

Our client is immediately recognised, and the deployment can proceed:



Sophos Enterprise Console - Protect computers wizard

Protection summary

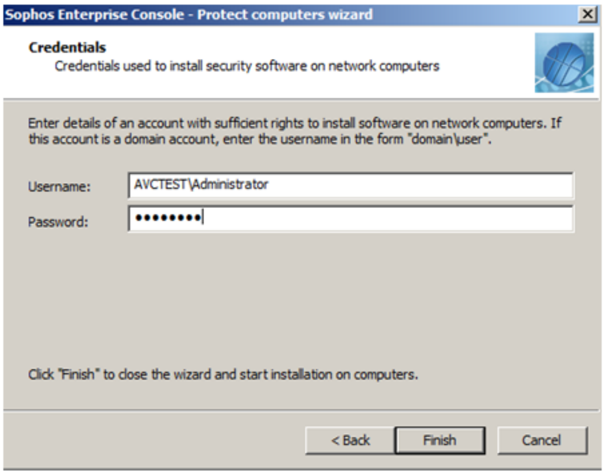
Shows any issues that affect installation of the security software

If software cannot be installed automatically, refer to the manual installation instructions in the Sophos Endpoint Security and Control quick startup guide.

Computers:

Computer Name	Protection issues
AVCCLIENT	

We now enter the credentials of a Windows account with the necessary privileges to carry out the installation:



Sophos Enterprise Console - Protect computers wizard

Credentials

Credentials used to install security software on network computers

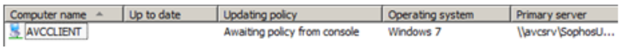
Enter details of an account with sufficient rights to install software on network computers. If this account is a domain account, enter the username in the form "domain\user".

Username: AVCTEST\Administrator

Password: ••••••••

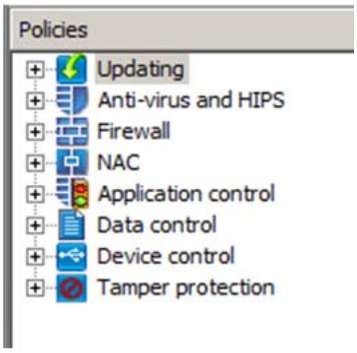
Click "Finish" to close the wizard and start installation on computers.

When installation has finished, we can immediately see that the policies are being pushed out to the client, thus assigning it the configuration settings:



Computer name	Up to date	Updating policy	Operating system	Primary server
AVCCLIENT		Awaiting policy from console	Windows 7	\\avcsrv\SophosU...

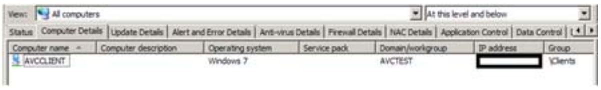
The entire suite follows this principle. Functions are configured using policies, which are distributed to the relevant PCs.



Policies
- Updating
- Anti-virus and HIPS
- Firewall
- NAC
- Application control
- Data control
- Device control
- Tamper protection

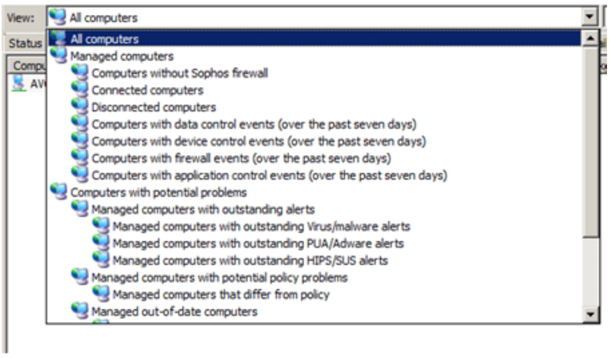
The descriptions of the different policies are self-explanatory, and the default settings appropriate.

The clear ordering, with pre-defined filters, makes administering even large networks very straightforward:



View: All computers | At this level and below

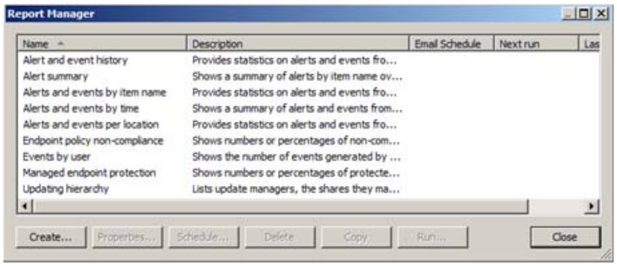
Computer name	Computer description	Operating system	Service pack	Domain/workgroup	IP address	Group
AVCCLIENT		Windows 7		AVCTEST		\Clients



View: All computers

- All computers
- Managed computers
  - Computers without Sophos firewall
  - Connected computers
  - Disconnected computers
  - Computers with data control events (over the past seven days)
  - Computers with device control events (over the past seven days)
  - Computers with firewall events (over the past seven days)
  - Computers with application control events (over the past seven days)
- Computers with potential problems
  - Managed computers with outstanding alerts
    - Managed computers with outstanding Virus/malware alerts
    - Managed computers with outstanding PUA/Adware alerts
    - Managed computers with outstanding HIPS/SUS alerts
  - Managed computers with potential policy problems
    - Managed computers that differ from policy
  - Managed out-of-date computers

The Report Manager, for example, hardly requires any changes to be made to the standard report:

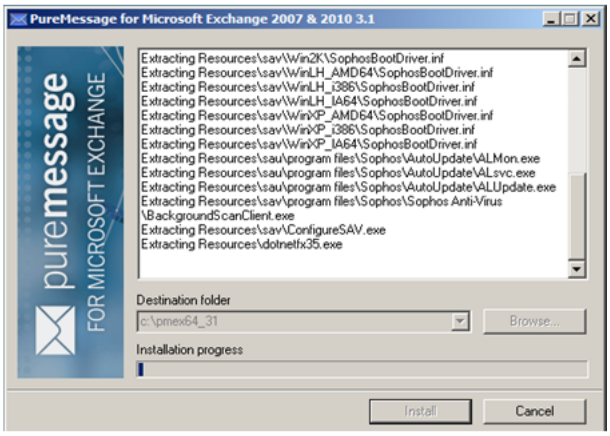


Report Manager

Name	Description	Email Schedule	Next run	Las
Alert and event history	Provides statistics on alerts and events fro...			
Alert summary	Shows a summary of alerts by item name ov...			
Alerts and events by item name	Provides statistics on alerts and events fro...			
Alerts and events by time	Shows a summary of alerts and events from...			
Alerts and events per location	Provides statistics on alerts and events fro...			
Endpoint policy non-compliance	Shows numbers or percentages of non-com...			
Events by user	Shows the number of events generated by ...			
Managed endpoint protection	Shows numbers or percentages of protecte...			
Updating hierarchy	Lists update managers, the shares they ma...			

Exchange 2007 protection

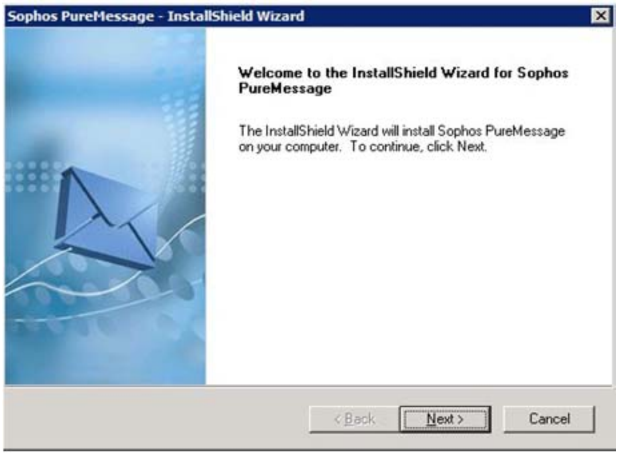
Again, we start by unpacking the installation files onto the local hard disk:



```
Extracting Resources\sav\Win2K\SophosBootDriver.inf
Extracting Resources\sav\WinLH_AMD64\SophosBootDriver.inf
Extracting Resources\sav\WinLH_i386\SophosBootDriver.inf
Extracting Resources\sav\WinLH_IA64\SophosBootDriver.inf
Extracting Resources\sav\WinXP_AMD64\SophosBootDriver.inf
Extracting Resources\sav\WinXP_i386\SophosBootDriver.inf
Extracting Resources\sav\WinXP_IA64\SophosBootDriver.inf
Extracting Resources\sau\program files\Sophos\AutoUpdate\ALMon.exe
Extracting Resources\sau\program files\Sophos\AutoUpdate\ALsvc.exe
Extracting Resources\sau\program files\Sophos\AutoUpdate\ALUpdate.exe
Extracting Resources\sav\program files\Sophos\Sophos Anti-Virus
\BackgroundScanClient.exe
Extracting Resources\sav\ConfigureSAV.exe
Extracting Resources\dotnetfx35.exe
```

Destination folder: c:\pmex64_31

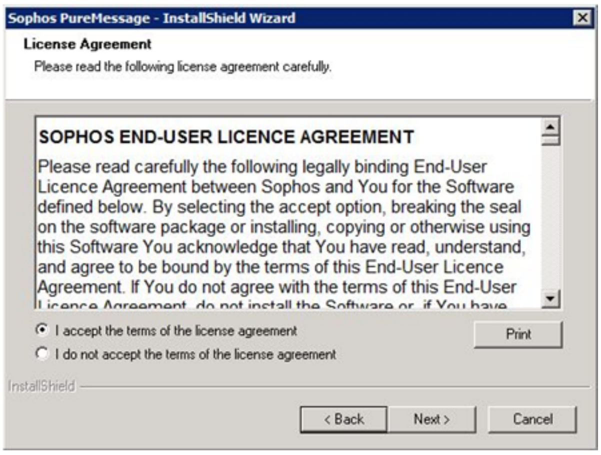
Installation progress



Welcome to the InstallShield Wizard for Sophos PureMessage

The InstallShield Wizard will install Sophos PureMessage on your computer. To continue, click Next.

We accept the licence agreement:



License Agreement

Please read the following license agreement carefully.

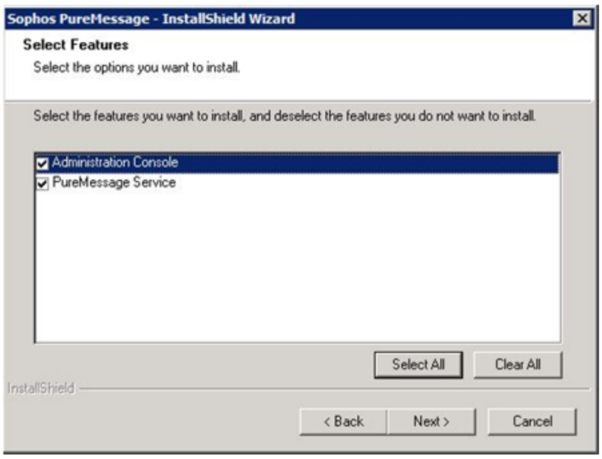
SOPHOS END-USER LICENCE AGREEMENT

Please read carefully the following legally binding End-User Licence Agreement between Sophos and You for the Software defined below. By selecting the accept option, breaking the seal on the software package or installing, copying or otherwise using this Software You acknowledge that You have read, understand, and agree to be bound by the terms of this End-User Licence Agreement. If You do not agree with the terms of this End-User Licence Agreement, do not install the Software or, if You have

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

Here we can select the features to be installed:



Select Features

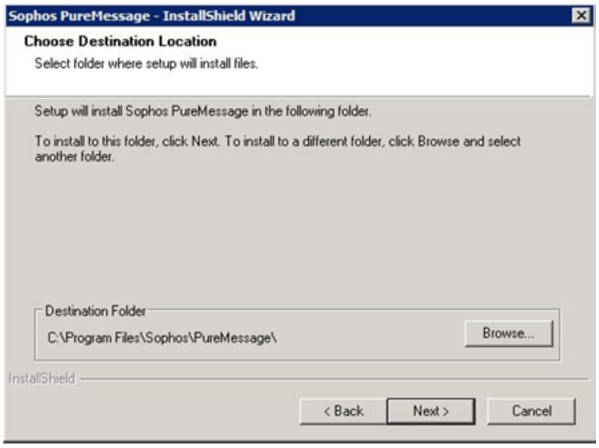
Select the options you want to install.

Select the features you want to install, and deselect the features you do not want to install.

☑ Administration Console

☑ PureMessage Service

Next we define the installation folder:



Choose Destination Location

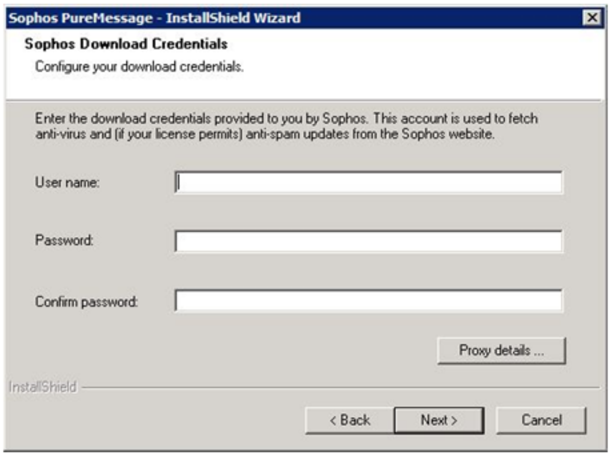
Select folder where setup will install files.

Setup will install Sophos PureMessage in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder: C:\Program Files\Sophos\PureMessage\

Here we have to supply Sophos with the registration information, in order to be able to download updates:



Sophos PureMessage - InstallShield Wizard

Sophos Download Credentials

Configure your download credentials.

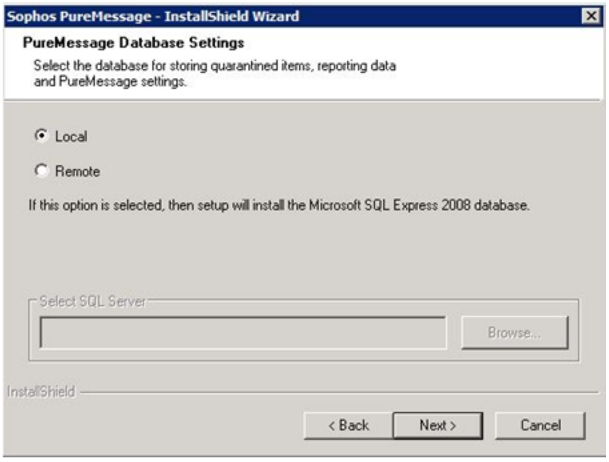
Enter the download credentials provided to you by Sophos. This account is used to fetch anti-virus and (if your license permits) anti-spam updates from the Sophos website.

User name:

Password:

Confirm password:

Now we can choose a database for the storage of quarantined items and other data:



Sophos PureMessage - InstallShield Wizard

PureMessage Database Settings

Select the database for storing quarantined items, reporting data and PureMessage settings.

● Local

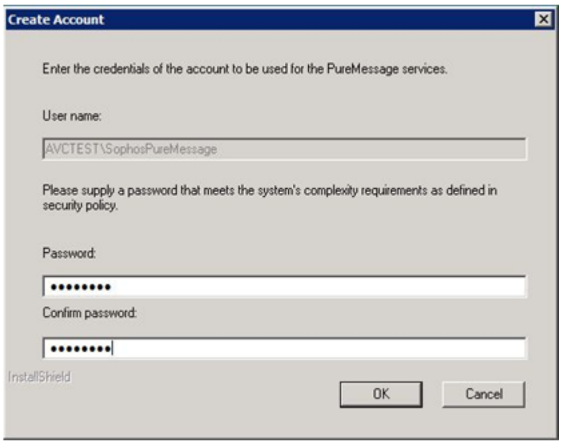
○ Remote

If this option is selected, then setup will install the Microsoft SQL Express 2008 database.

Select SQL Server

If there is no SQL Express server available, this can be automatically installed too. Alternatively, a connection can be made to an existing SQL server.

The next step is to enter details of the service account to be used to run PureMessage:



Create Account

Enter the credentials of the account to be used for the PureMessage services.

User name:

AVCTEST\SophosPureMessage

Please supply a password that meets the system's complexity requirements as defined in security policy.

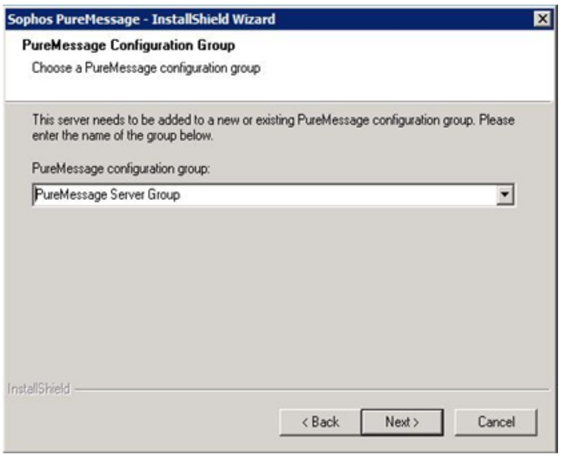
Password:

••••••••

Confirm password:

••••••••

Here we can create a configuration group for PureMessage:



Sophos PureMessage - InstallShield Wizard

PureMessage Configuration Group

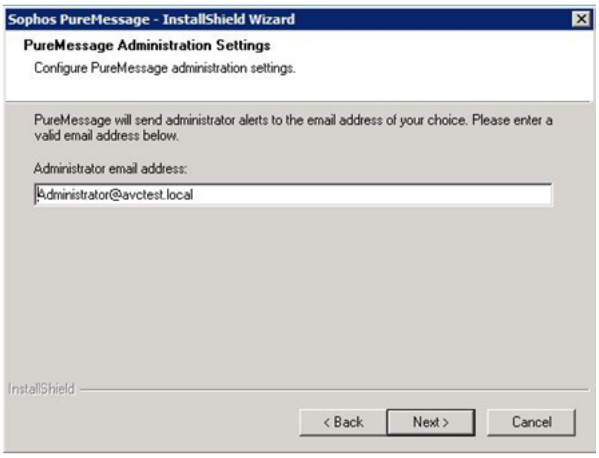
Choose a PureMessage configuration group

This server needs to be added to a new or existing PureMessage configuration group. Please enter the name of the group below.

PureMessage configuration group:

PureMessage Server Group

Then we enter the admin email address:



Sophos PureMessage - InstallShield Wizard

PureMessage Administration Settings

Configure PureMessage administration settings.

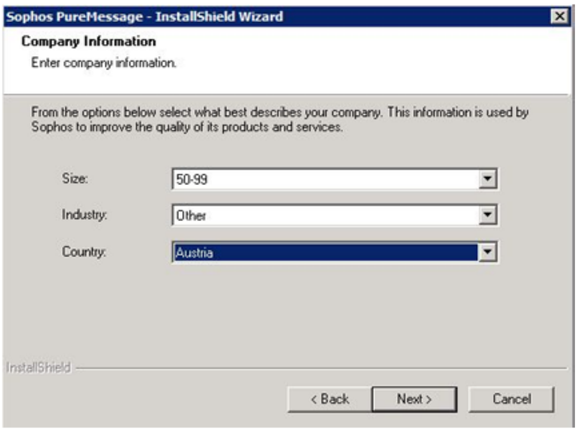
PureMessage will send administrator alerts to the email address of your choice. Please enter a valid email address below.

Administrator email address:

Administrator@avctest.local

At this point it is possible to enter routing information for the email domain, although this can of course be done later.

There are a few details to be entered about the company size and location:



Sophos PureMessage - InstallShield Wizard

Company Information

Enter company information.

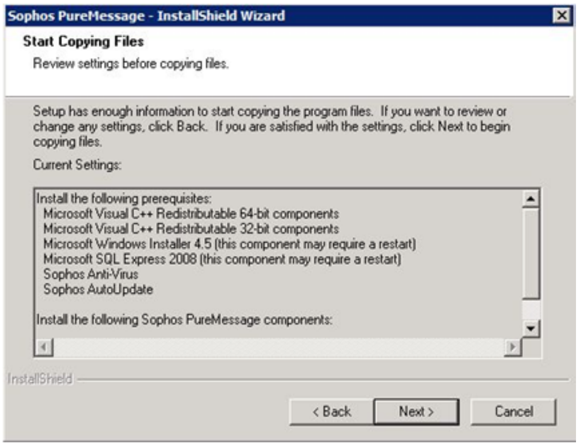
From the options below select what best describes your company. This information is used by Sophos to improve the quality of its products and services.

Size: 50-99

Industry: Other

Country: Austria

Once again, a summary of the installation details is displayed before the installer begins:



Sophos PureMessage - InstallShield Wizard

Start Copying Files

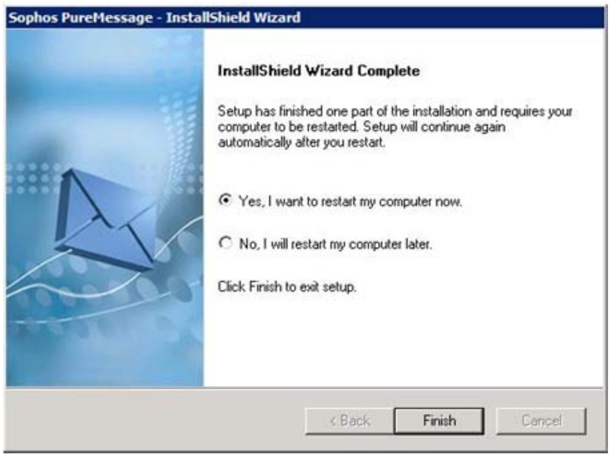
Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
Install the following prerequisites:
  Microsoft Visual C++ Redistributable 64-bit components
  Microsoft Visual C++ Redistributable 32-bit components
  Microsoft Windows Installer 4.5 (this component may require a restart)
  Microsoft SQL Express 2008 (this component may require a restart)
  Sophos Anti-Virus
  Sophos AutoUpdate

Install the following Sophos PureMessage components:
```

When setup is completed, the installer informs us that a restart is required:



Sophos PureMessage - InstallShield Wizard

InstallShield Wizard Complete

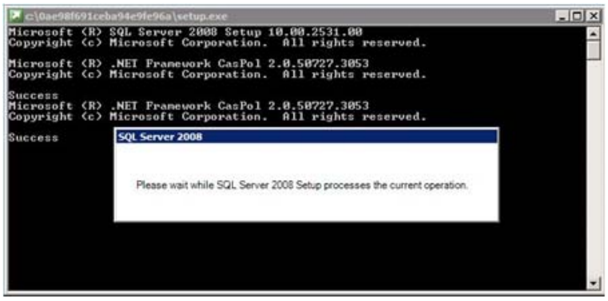
Setup has finished one part of the installation and requires your computer to be restarted. Setup will continue again automatically after you restart.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Click Finish to exit setup.

Immediately after the restart, Sophos begins post-installation tasks. For example, configuration of SQL Server Express, if this is used:

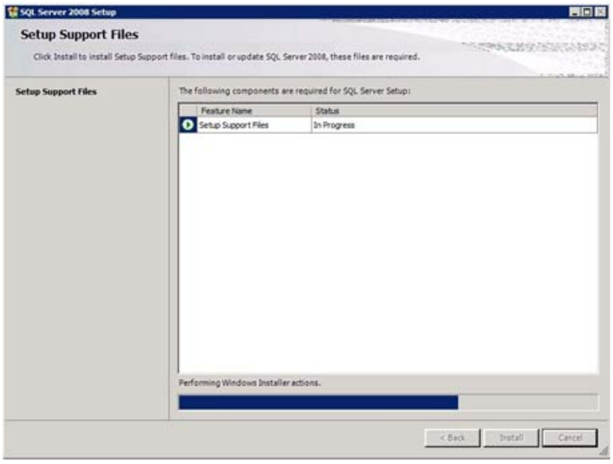


c:\0ae98f691ceba94e9fe96a\setup.exe

```
Microsoft (R) SQL Server 2008 Setup 10.00.2531.00
Copyright (c) Microsoft Corporation.  All rights reserved.

Microsoft (R) .NET Framework CasPol 2.0.50727.3053
Copyright (c) Microsoft Corporation.  All rights reserved.

Success
Microsoft (R) .NET Framework CasPol 2.0.50727.3053
Copyright (c) Microsoft Corporation.  All rights reserved.

Success
```

SQL Server 2008

Please wait while SQL Server 2008 Setup processes the current operation.



SQL Server 2008 Setup

Setup Support Files

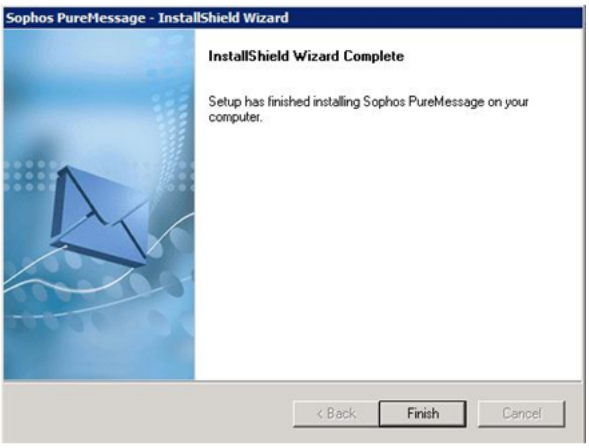
Click Install to install Setup Support files. To install or update SQL Server 2008, these files are required.

The following components are required for SQL Server Setup:

Feature Name	Status
Setup Support Files	In Progress

Performing Windows Installer actions.

As soon as these automatic tasks are completed, we can continue with our own configuration:



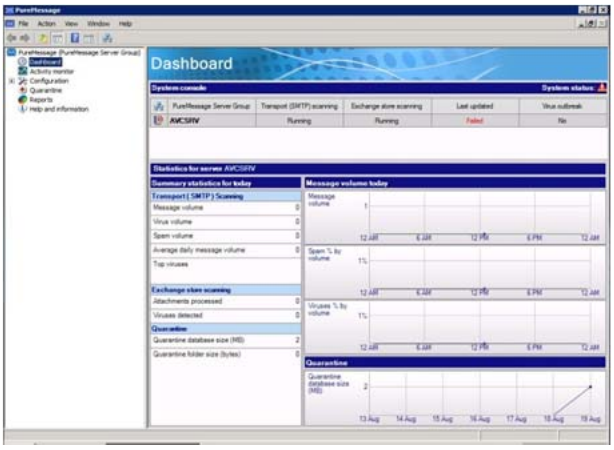
Sophos PureMessage - InstallShield Wizard

InstallShield Wizard Complete

Setup has finished installing Sophos PureMessage on your computer.

The management interface of Pure Message

The management console for Sophos's mail protection is also very well-designed and professional:



System console — System status:

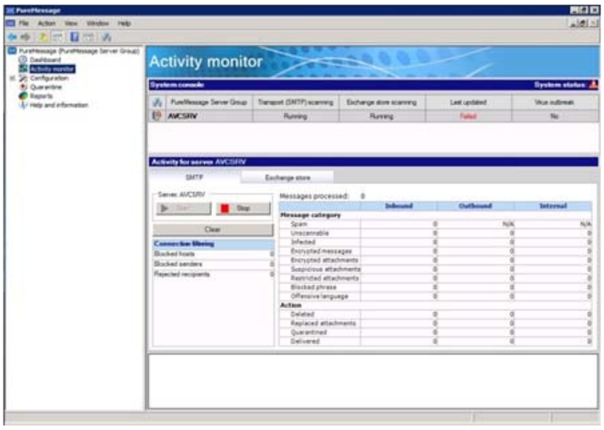
	PureMessage Server Group	Transport (SMTP) scanning	Exchange store scanning	Last updated	Virus outbreak
	AVCSRV	Running	Running	Failed	No

Statistics for server AVCSRV

Summary statistics for today

Transport (SMTP) Scanning	
Message volume	0
Virus volume	0
Spam volume	0
Average daily message volume	0
Top viruses	
Exchange store scanning	
Attachments processed	0
Viruses detected	0
Quarantine	
Quarantine database size (MB)	2
Quarantine folder size (bytes)	0

The MMC-compatible format provides a clear functional structure, with a good summary page. Even the real-time summary display, called "Activity monitor", is a feast for the eyes:



System console — System status:

	PureMessage Server Group	Transport (SMTP) scanning	Exchange store scanning	Last updated	Virus outbreak
	AVCSRV	Running	Running	Failed	No

Activity for server AVCSRV

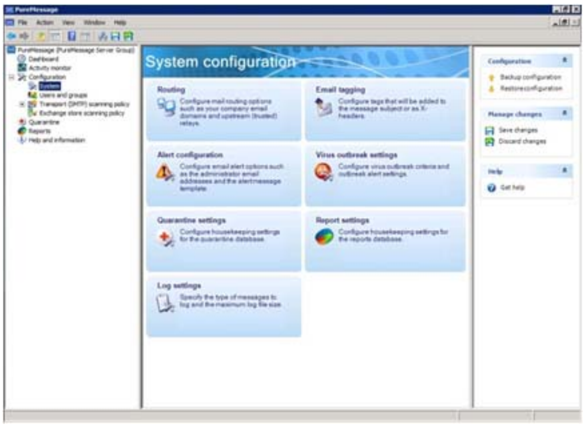
Server: AVCSRV

Connection filtering	
Blocked hosts	0
Blocked senders	0
Rejected recipients	0

Messages processed: 0

	Inbound	Outbound	Internal
Message category			
Spam	0	N/A	N/A
Unscannable	0	0	0
Infected	0	0	0
Encrypted messages	0	0	0
Encrypted attachments	0	0	0
Suspicious attachments	0	0	0
Restricted attachments	0	0	0
Blocked phrase	0	0	0
Offensive language	0	0	0
Action			
Deleted	0	0	0
Replaced attachments	0	0	0
Quarantined	0	0	0
Delivered	0	0	0

It is the clearly ordered and professional design that makes working with the console a pleasure:



Routing: Configure mail routing options such as your company email domains and upstream (trusted) relays.

Email tagging: Configure tags that will be added to the message subject or as X-headers.

Alert configuration: Configure email alert options such as the administrator email addresses and the alert message template.

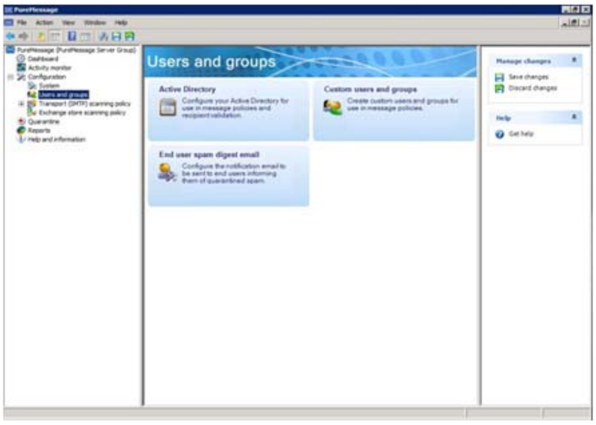
Virus outbreak settings: Configure virus outbreak criteria and outbreak alert settings.

Quarantine settings: Configure housekeeping settings for the quarantine database.

Report settings: Configure housekeeping settings for the reports database.

Log settings: Specify the type of messages to log and the maximum log file size.

The wide variety of functions can be clearly seen, and leaves nothing to be desired:

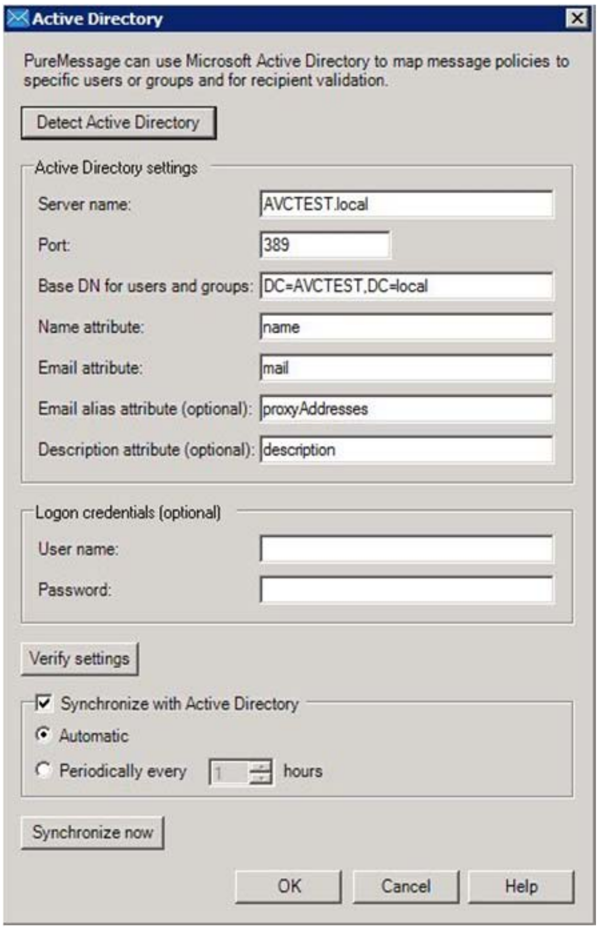


Active Directory: Configure your Active Directory for use in message policies and recipient validation.

Custom users and groups: Create custom users and groups for use in message policies.

End user spam digest email: Configure the notification email to be sent to end users informing them of quarantined spam.

With the Exchange Server protection too, Sophos comes up trumps with outstanding AD support:



PureMessage can use Microsoft Active Directory to map message policies to specific users or groups and for recipient validation.

Active Directory settings

Server name: AVCTEST.local

Port: 389

Base DN for users and groups: DC=AVCTEST,DC=local

Name attribute: name

Email attribute: mail

Email alias attribute (optional): proxyAddresses

Description attribute (optional): description

Logon credentials (optional)

User name:

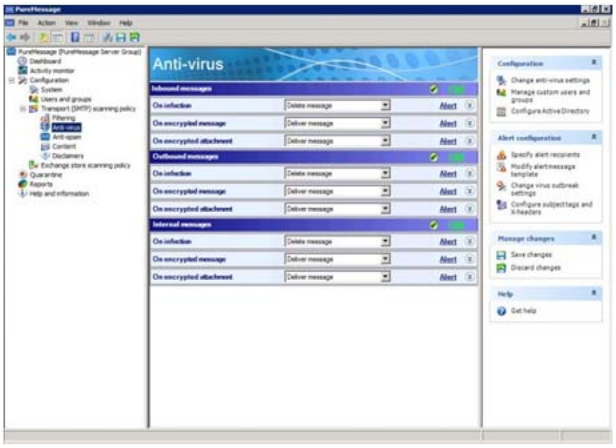
Password:

☑ Synchronize with Active Directory

● Automatic

○ Periodically every 1 hours

The configuration possibilities, with convenient drop-down menus, work very well:


Anti-virus
Configuration
Change anti-virus settings
Manage custom users and groups
Configure Active Directory
Alert configuration
Specify alert recipients
Modify alert message template
Change virus outbreak settings
Configure subject tags and X-headers
Manage changes
Save changes
Discard changes
Help
Get help

Inbound messages

On infection: Delete message — Alert

On encrypted message: Deliver message — Alert

On encrypted attachment: Deliver message — Alert

Outbound messages

On infection: Delete message — Alert

On encrypted message: Deliver message — Alert

On encrypted attachment: Deliver message — Alert

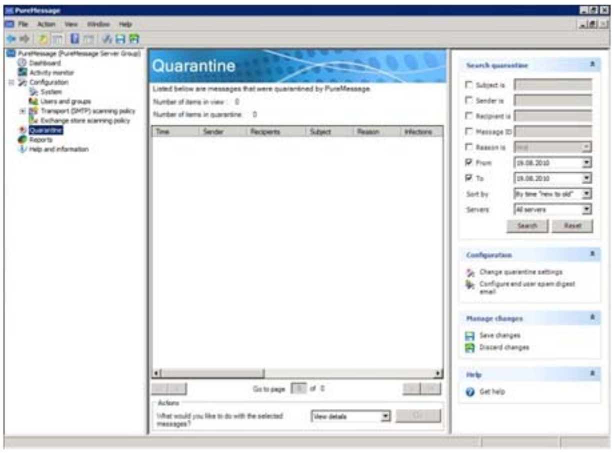
Internal messages

On infection: Delete message — Alert

On encrypted message: Deliver message — Alert

On encrypted attachment: Deliver message — Alert

The Exchange Server protection thus fits very well with the positive impression created by the entire suite.



Listed below are messages that were quarantined by PureMessage.

Number of items in view : 0

Number of items in quarantine: 0

Time	Sender	Recipients	Subject	Reason	Infections

Go to page 0 of 0

Actions

What would you like to do with the selected messages? View details

□ Subject is

□ Sender is

□ Recipient is

□ Message ID

□ Reason is

☑ From 19.08.2010

☑ To 19.08.2010

Sort by: By time "new to old"

Servers: All servers

Summary

Manufacturer's website

The Sophos website (**www.sophos.com**) is pleasantly designed, clear, and conforms to current standards.

If you want to find out more about Network Access Control, the Sophos website is an ideal starting point. There is a lot of well-presented information on the subject, with appropriate references to suitable products.

The installation procedure

The installation is quick and easy, as is to be expected from Sophos. A basic understanding of network security is desirable, but the installer leads you through the process well.

The single installer for the majority of the products is to be commended.

The Active Directory support is also outstanding, and makes child's play of setting up accounts etc.

The management console

As with last year's product, the current Sophos management console is a trend-setting solution.

The clear and simple design with strong reporting functions can cope with the most complex requirements, and the configuration wizards are convincing throughout.

This console should serve as an example for many others.

Deployment areas

The Sophos suite is suitable for all networks, without exception. Its strengths are particularly suited to large and complicated networks.

Antivirus clients

Endpoint Protection is based on the principles of Network Access Control (NAC). This is hardly noticeable to the user, and the remote installation is very simple to carry out.

Summary

This year (as last) Sophos has, along with McAfee, produced the best suite of those we have reviewed.

The consistent design of the product line and its installation is convincing throughout.

Almost no other suite offers the user more functionality with such ease of use and organisational features.

Pros

+ Real-time status of tasks
+ Graphic design of administrator console
+ Simple remote installation
+ Excellent setup wizards
+ Quick and easy installation

Cons

- Few Exchange functions
- No indication of download progress

Deployment areas

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★	★★★★★	★★★★★

Summary

Installation Wizard	★★★★★
User Navigation	★★★★★
Administrator Console	★★★★★
Default Values	★★★★
MS Active Directory Support	★★★★★
Database Support	★★★★
Remote Installation	★★★★★
Website	★★★★
Manual	★★★★

Trend Micro

Test Software:

OfficeScan 10.0	→	Client Protection
ServerProtect for Microsoft Windows	→	File Server Protection
ScanMail for Microsoft Exchange 10	→	Exchange Server Mail Protection
Control Manager 5.5	→	Management Console

Installation process

Downloading the product

The manufacturer's website offers everything you would expect from a commercial website, and it is easy to find what you're looking for. Unfortunately, Trend Micro has adopted the practice of offering suites consisting of individual products, without offering an installer that will install them all in the right order.

Download times:

SPNT58_en_repack1.zip

(234 MB)

05:36min (534kb/sec)

OSCE_10_WIN_ServicePack1_SinglePackage_R4 (en)

(481 MB)

07:17min (489kb/sec)

SMEX10.0_GM_Build1412_R2 (280 MB)

04:4min (544kb/sec)

TMCM50_GM_repack2.zip

(550 MB)

08:10min (772kb/sec)

Product installation

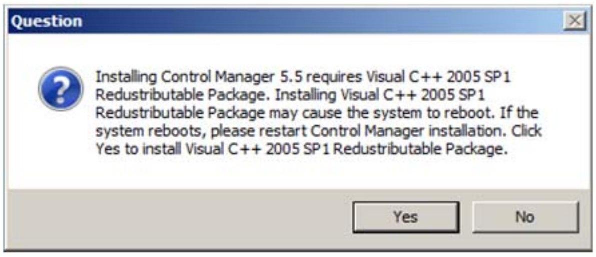
Until recently, only Version 5, Repack 2 was available, which would only work with Windows Server 2003 or earlier.

During our tests, Trend Micro brought out Repack 3, which also supports Windows Server 2008. A few days later, version 5.5 of the Control Manager was released, which we then used for our review.

Even then there was another hurdle to get over. The Control Manager cannot be installed on a server that is acting as a domain controller.

Thus we decided to install the Control Manager on a client PC with Windows 7, in order to simulate an administration computer that is used to manage the Trend Micro security environment.

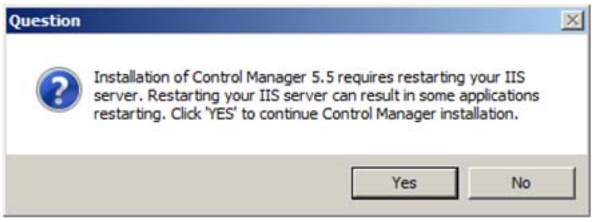
We begin with the installation of the Trend Micro management console.



Installing Control Manager 5.5 requires Visual C++ 2005 SP1 Redustributable Package. Installing Visual C++ 2005 SP1 Redustributable Package may cause the system to reboot. If the system reboots, please restart Control Manager installation. Click Yes to install Visual C++ 2005 SP1 Redustributable Package.

The message above informs us that additional software packets are necessary and will be installed.

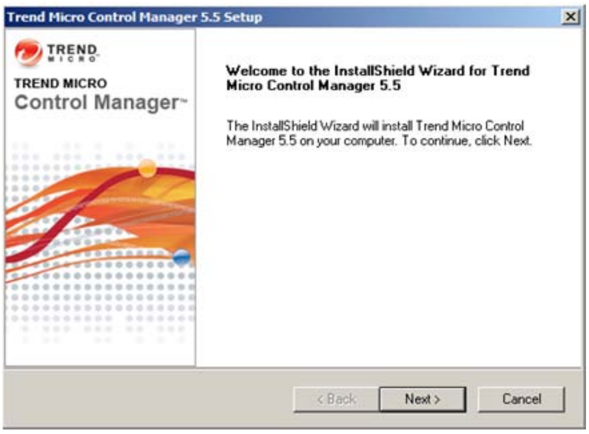
There is also a message to let us know that installation will require Microsoft's IIS service to be restarted:



Question

Installation of Control Manager 5.5 requires restarting your IIS server. Restarting your IIS server can result in some applications restarting. Click 'YES' to continue Control Manager installation.

When we have confirmed that we wish to continue, the Control Manager installer starts:

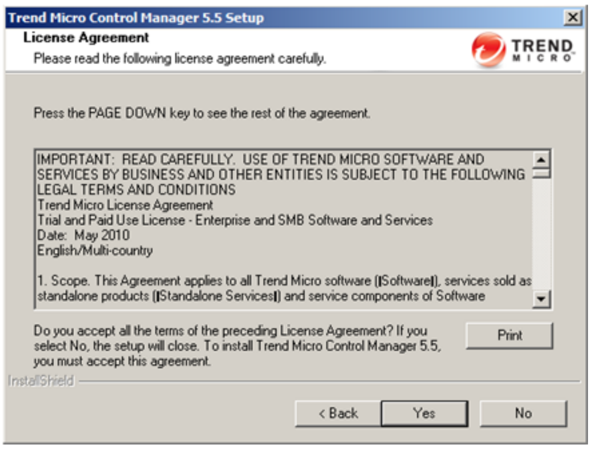


Trend Micro Control Manager 5.5 Setup

Welcome to the InstallShield Wizard for Trend Micro Control Manager 5.5

The InstallShield Wizard will install Trend Micro Control Manager 5.5 on your computer. To continue, click Next.

We accept the licence agreement:



Trend Micro Control Manager 5.5 Setup

License Agreement

Please read the following license agreement carefully.

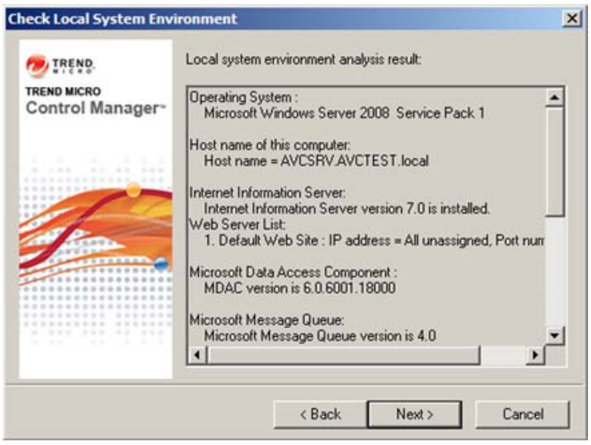
Press the PAGE DOWN key to see the rest of the agreement.

IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS
Trend Micro License Agreement
Trial and Paid Use License - Enterprise and SMB Software and Services
Date: May 2010
English/Multi-country

1. Scope. This Agreement applies to all Trend Micro software (Software), services sold as standalone products (Standalone Services) and service components of Software

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install Trend Micro Control Manager 5.5, you must accept this agreement.

The next step is the investigation of the environment, and a report on this is displayed:



Check Local System Environment

Local system environment analysis result:

Operating System :
Microsoft Windows Server 2008 Service Pack 1

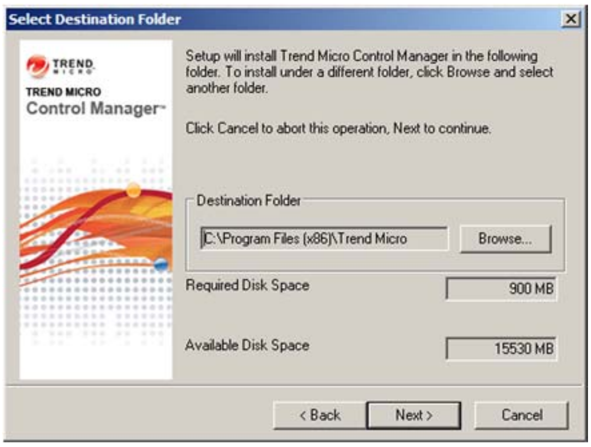
Host name of this computer:
Host name = AVCSRV.AVCTEST.local

Internet Information Server:
Internet Information Server version 7.0 is installed.
Web Server List:
1. Default Web Site : IP address = All unassigned, Port num

Microsoft Data Access Component :
MDAC version is 6.0.6001.18000

Microsoft Message Queue:
Microsoft Message Queue version is 4.0

We can then choose an installation folder:



Select Destination Folder

Setup will install Trend Micro Control Manager in the following folder. To install under a different folder, click Browse and select another folder.

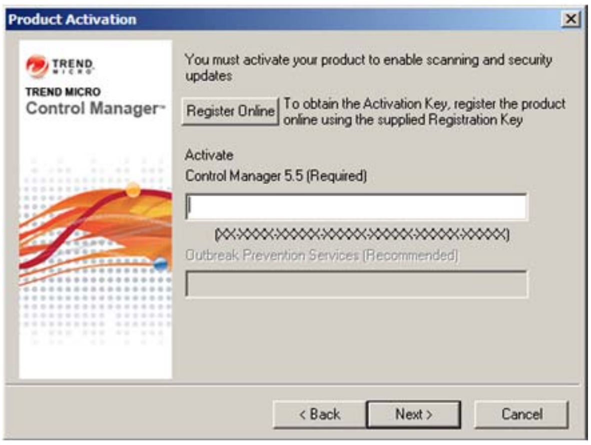
Click Cancel to abort this operation, Next to continue.

Destination Folder: C:\Program Files (x86)\Trend Micro

Required Disk Space: 900 MB

Available Disk Space: 15530 MB

The licence key now needs to be entered:



Product Activation

You must activate your product to enable scanning and security updates

To obtain the Activation Key, register the product online using the supplied Registration Key

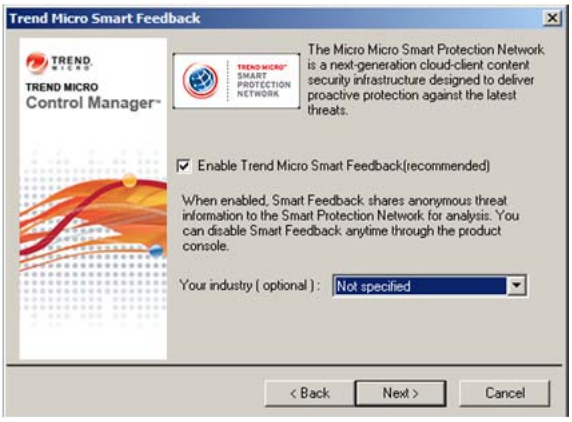
Activate

Control Manager 5.5 (Required)

(XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

Outbreak Prevention Services (Recommended)

Trend Micro also asks whether we wish to join their threat network and send feedback:



Trend Micro Smart Feedback

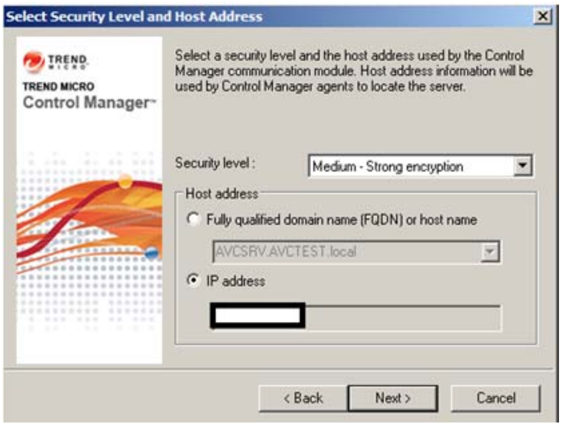
The Micro Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to deliver proactive protection against the latest threats.

☑ Enable Trend Micro Smart Feedback(recommended)

When enabled, Smart Feedback shares anonymous threat information to the Smart Protection Network for analysis. You can disable Smart Feedback anytime through the product console.

Your industry (optional) : Not specified

The next step is to choose the security level and IP or hostname of the Control Manager server:



Select Security Level and Host Address

Select a security level and the host address used by the Control Manager communication module. Host address information will be used by Control Manager agents to locate the server.

Security level : Medium - Strong encryption

Host address

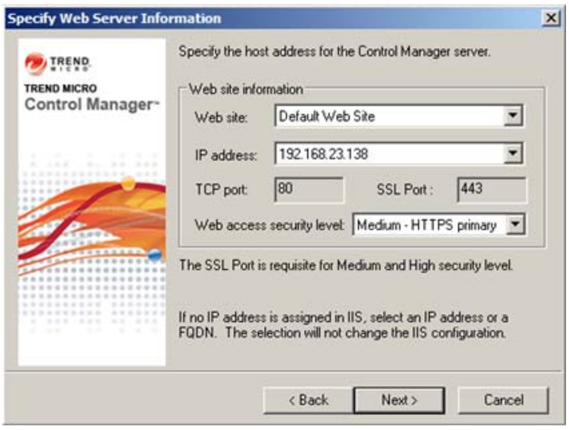
○ Fully qualified domain name (FQDN) or host name

AVCSRV.AVCTEST.local

● IP address

[redacted]

We then enter details of the web server used for Trend Micro administration:



Specify Web Server Information

Specify the host address for the Control Manager server.

Web site information

Web site: Default Web Site

IP address: 192.168.23.138

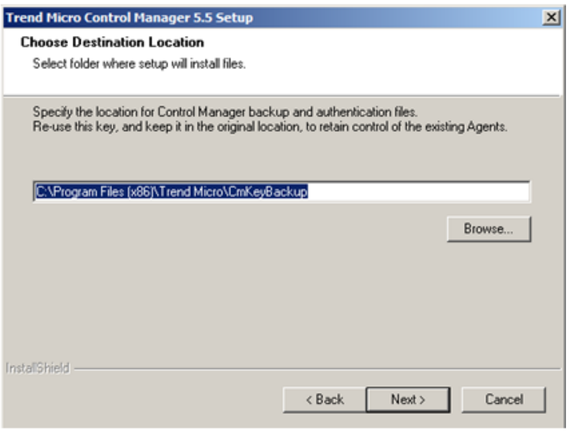
TCP port: 80 SSL Port : 443

Web access security level: Medium - HTTPS primary

The SSL Port is requisite for Medium and High security level.

If no IP address is assigned in IIS, select an IP address or a FQDN. The selection will not change the IIS configuration.

Now we come to choosing a location for updates and backups:



Trend Micro Control Manager 5.5 Setup

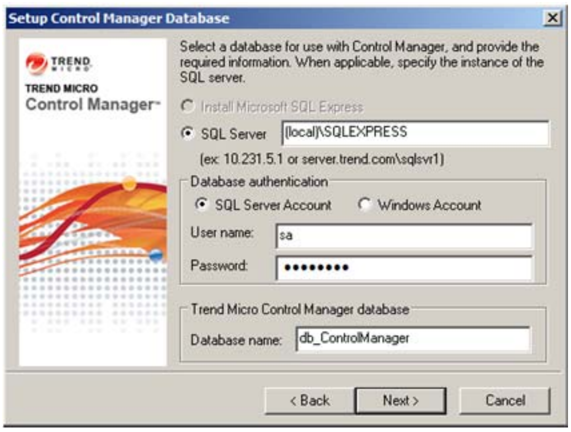
Choose Destination Location

Select folder where setup will install files.

Specify the location for Control Manager backup and authentication files.
Re-use this key, and keep it in the original location, to retain control of the existing Agents.

C:\Program Files (x86)\Trend Micro\CmKeyBackup

The database settings are the next task. If there is no SQL server available in the network, SQL Express can be installed with the Trend Micro suite:



Setup Control Manager Database

Select a database for use with Control Manager, and provide the required information. When applicable, specify the instance of the SQL server.

○ Install Microsoft SQL Express

● SQL Server (local)\SQLEXPRESS

(ex: 10.231.5.1 or server.trend.com\sqlsvr1)

Database authentication

● SQL Server Account ○ Windows Account

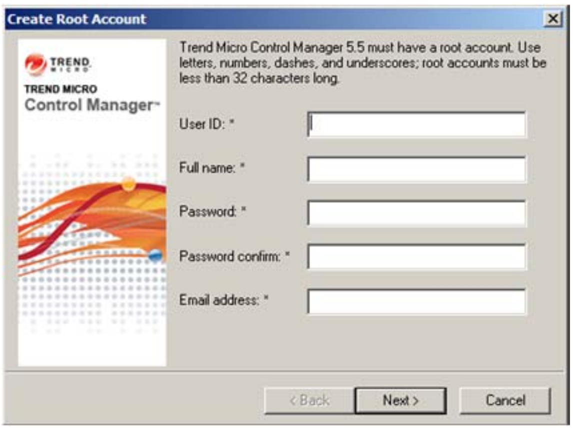
User name: sa

Password: ••••••••

Trend Micro Control Manager database

Database name: db_ControlManager

After verification of the database, we have to create a Root (administrator) Account:



Create Root Account

Trend Micro Control Manager 5.5 must have a root account. Use letters, numbers, dashes, and underscores; root accounts must be less than 32 characters long.

User ID: *

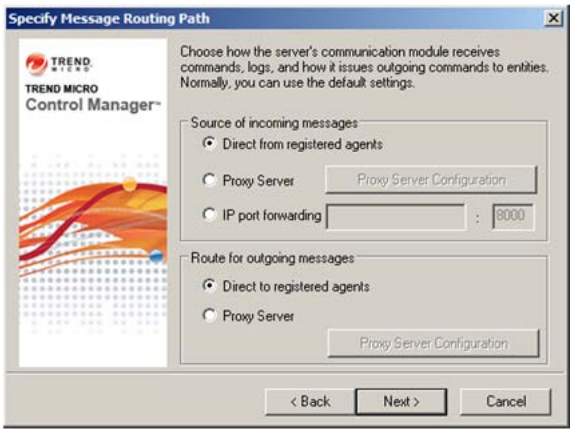
Full name: *

Password: *

Password confirm: *

Email address: *

Now we can configure routing and notification settings, and enter proxy server details if necessary:



Choose how the server's communication module receives commands, logs, and how it issues outgoing commands to entities. Normally, you can use the default settings.

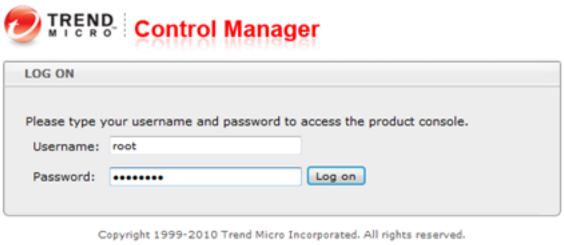
Source of incoming messages
- ● Direct from registered agents
- ○ Proxy Server [Proxy Server Configuration]
- ○ IP port forwarding [ ] : [8000]

Route for outgoing messages
- ● Direct to registered agents
- ○ Proxy Server [Proxy Server Configuration]

When installation is complete, we can begin configuration.

The management interface

The login box appears in a browser window:



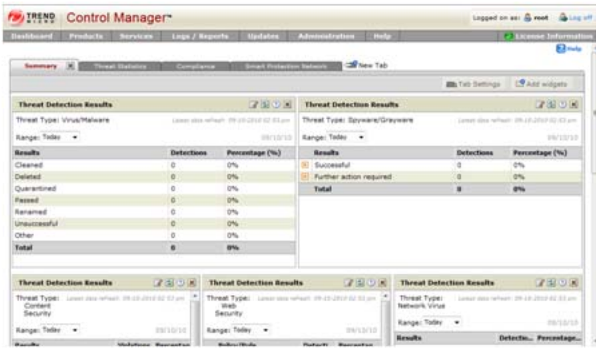
Please type your username and password to access the product console.

Username: root

Password: ••••••••

Copyright 1999-2010 Trend Micro Incorporated. All rights reserved.

Having logged in, we see the dashboard, which gives an overview of the state of the system:



Threat Detection Results

Threat Type: Virus/Malware

Range: Today

Results	Detections	Percentage (%)
Cleaned	0	0%
Deleted	0	0%
Quarantined	0	0%
Passed	0	0%
Renamed	0	0%
Unsuccessful	0	0%
Other	0	0%
Total	0	0%

Threat Detection Results

Threat Type: Spyware/Grayware

Range: Today

Results	Detections	Percentage (%)
Successful	0	0%
Further action required	0	0%
Total	0	0%

Threat Detection Results

Threat Type: Content Security

Range: Today

Threat Detection Results

Threat Type: Web Security

Range: Today

Threat Detection Results

Threat Type: Network Virus

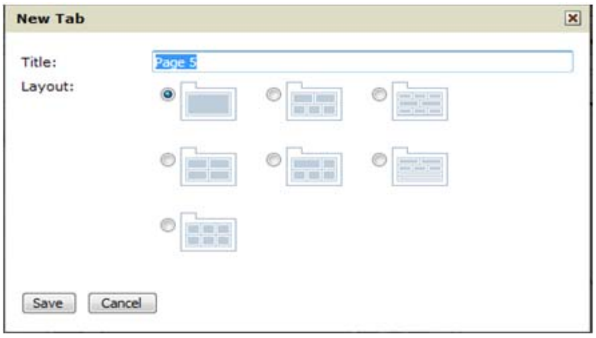
Range: Today

The Control Manager is very well designed, and the clearly structured web interface makes it easy to find your way around.

We are pleased to note that the information is presented in a clear and comprehensible way, allowing the user to keep an overview.

In the "Dashboard" category, under the "Threat Statistics" tab, information about the threats found on the network is displayed. The "Compliance" tab shows relevant system information that can be used to check if the configuration complies with internal IT audit requirements.

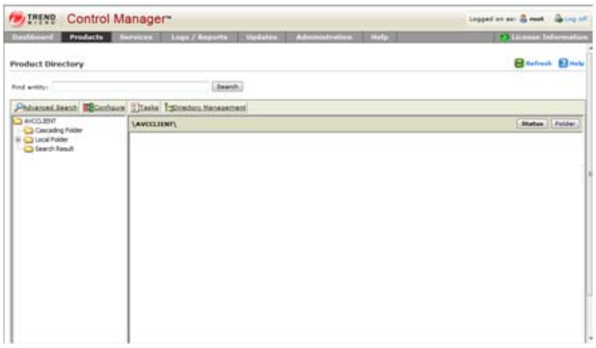
A very convenient feature is the ability to create your own tabs, which can be customised to display the information most important to you:



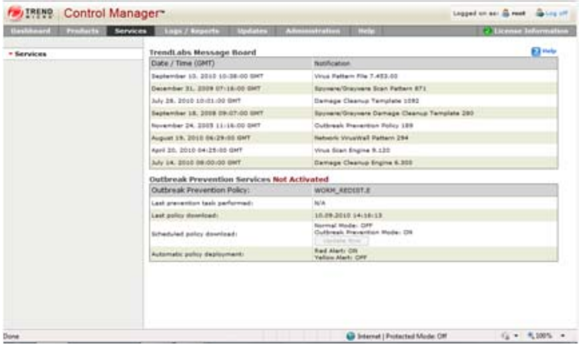
Title: Page 5

Layout:

Such a simple method of customising the tabs would not be out of place on some websites.



Under the "Products" category, you can find installation packets and products which can be installed or distributed around the network.



TrendLabs Message Board

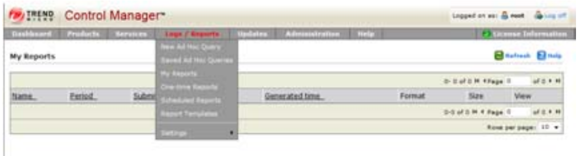
Date / Time (GMT)	Notification
September 13, 2010 10:38:00 GMT	Virus Pattern File 7.453.00
December 31, 2009 07:16:00 GMT	Spyware/Grayware Scan Pattern 871
July 28, 2010 10:01:00 GMT	Damage Cleanup Template 1092
September 18, 2008 09:07:00 GMT	Spyware/Grayware Damage Cleanup Template 280
November 24, 2005 11:16:00 GMT	Outbreak Prevention Policy 189
August 19, 2010 06:29:00 GMT	Network VirusWall Pattern 294
April 20, 2010 04:25:00 GMT	Virus Scan Engine 9.120
July 14, 2010 08:00:00 GMT	Damage Cleanup Engine 6.300

Outbreak Prevention Services Not Activated

Outbreak Prevention Policy:	WORM_REDIST.E
Last prevention task performed:	N/A
Last policy download:	10.09.2010 14:18:13
Scheduled policy download:	Normal Mode: OFF Outbreak Prevention Mode: ON Update Now
Automatic policy deployment:	Red Alert: ON Yellow Alert: OFF

Under "Services" we find components that were selected for installation during the setup process, such as "Outbreak Prevention Services." Additionally, the latest messages from the manufacturer are displayed on the "Trend Labs Message Board".

Next we take a look at the "Logs/Report" area:



My Reports

0-0 of 0 Page 0 of 0

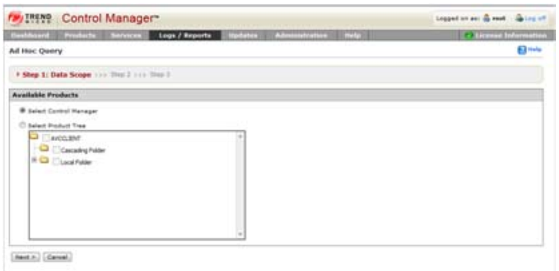
Name	Period	Subm	Generated time	Format	Size	View

0-0 of 0 Page 0 of 0

Rows per page: 10

The enormous experience of Trend Micro is shown here. The logging and reporting system can be precisely customised to suit the administrator's individual needs.

You have the choice of repeating queries which have already been made, or running a so-called "Ad Hoc Query", which runs a wizard that will extract the precise information you want.



Ad Hoc Query

Step 1: Data Scope >>> Step 2 >>> Step 3

Available Products

● Select Control Manager

○ Select Product Tree

□ AVCCLIENT

□ Cascading Folder

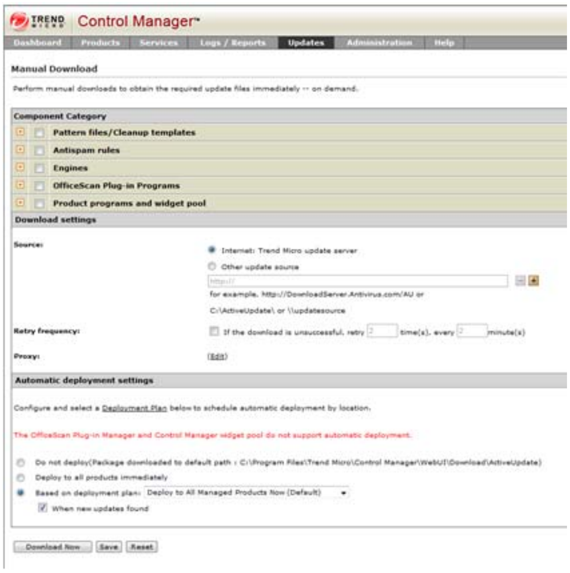
□ Local Folder

Thus it is easy to create the most important queries and run these again when necessary, using just a few clicks.

The other reporting functions are also very well designed. For example, there are 8 default templates for commonly used reports, or more experienced users can create their own templates for customised reports.

In the area of reporting and log options, the Control Manager has everything you could possibly want.

In the "Updates" category, you will also find everything you need:



Manual Download

Perform manual downloads to obtain the required update files immediately -- on demand.

Component Category

□ Pattern files/Cleanup templates

□ Antispam rules

□ Engines

□ OfficeScan Plug-in Programs

□ Product programs and widget pool

Download settings

Source: ● Internet: Trend Micro update server

○ Other update source

http://

for example, http://DownloadServer.Antivirus.com/AU or

C:\ActiveUpdate\ or \\updatesource

Retry frequency: □ If the download is unsuccessful, retry 2 time(s), every 2 minute(s)

Proxy: (Edit)

Automatic deployment settings

Configure and select a Deployment Plan below to schedule automatic deployment by location.

The OfficeScan Plug-in Manager and Control Manager widget pool do not support automatic deployment.

○ Do not deploy(Package downloaded to default path : C:\Program Files\Trend Micro\Control Manager\WebUI\Download\ActiveUpdate)

○ Deploy to all products immediately

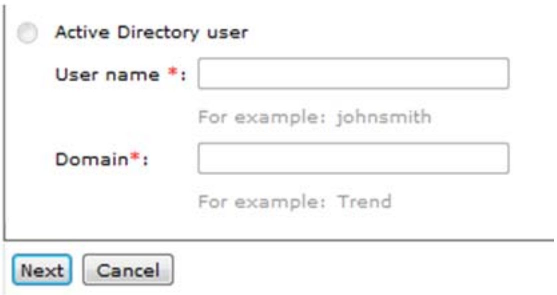
● Based on deployment plan: Deploy to All Managed Products Now (Default)

☑ When new updates found

The update settings can be configured down to the last detail, and the Control Manager is well suited to even complex network environments in this respect.

We were impressed to see that there is an individual control with which you can precisely control how specific updates can be distributed.

The "Administration" area is responsible for the management of the Management Console itself. You can add new Control Manager users, or change settings for existing ones. There is a convenient choice of using Trend Micro's internal user management, or adding a user from Active Directory.



○ Active Directory user

User name *:

For example: johnsmith

Domain*:

For example: Trend

"Command Tracking" can also be found in this area. This gives an overview of which actions were carried out by which user at what time.

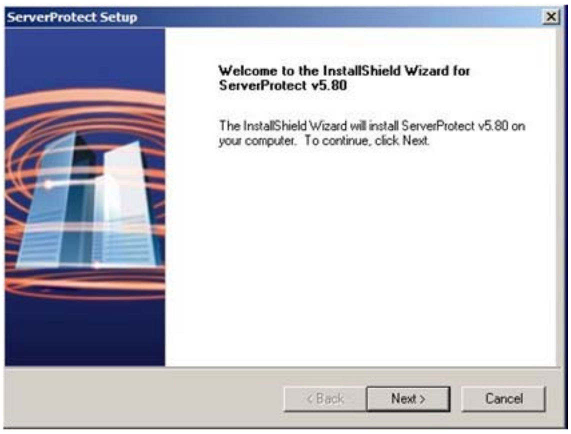
These functions in the Administration area are well thought-out and make the Control Manager suitable for use in large networks which have their own security teams.

The clear and simple web interface and clear structure mean that Control Manager is able to display a huge amount of data in a comprehensible manner.

We now move on to the installation of the server protection software, ServerProtect.

Anyone who has worked with Trend Micro corporate products in recent years will find the installation process of the current version very straightforward, as the layout has remained the same for the last 5 years.

We begin with the installation of ServerProtect:

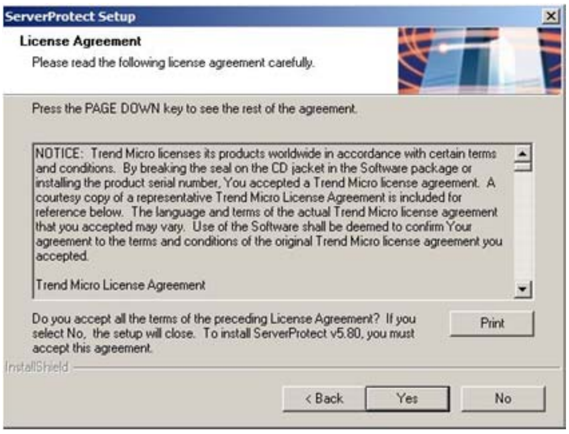


ServerProtect Setup

Welcome to the InstallShield Wizard for ServerProtect v5.80

The InstallShield Wizard will install ServerProtect v5.80 on your computer. To continue, click Next.

There is the usual licence agreement to accept:



ServerProtect Setup

License Agreement

Please read the following license agreement carefully.

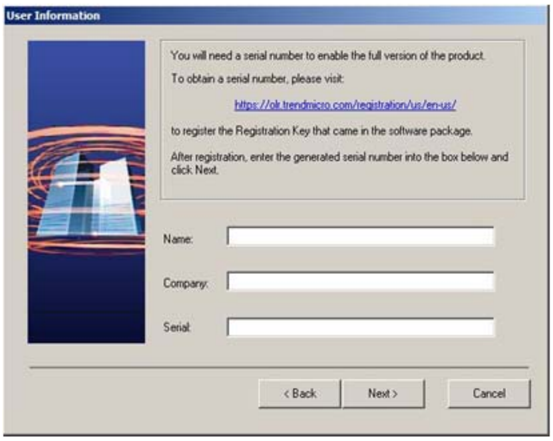
Press the PAGE DOWN key to see the rest of the agreement.

NOTICE: Trend Micro licenses its products worldwide in accordance with certain terms and conditions. By breaking the seal on the CD jacket in the Software package or installing the product serial number, You accepted a Trend Micro license agreement. A courtesy copy of a representative Trend Micro License Agreement is included for reference below. The language and terms of the actual Trend Micro license agreement that you accepted may vary. Use of the Software shall be deemed to confirm Your agreement to the terms and conditions of the original Trend Micro license agreement you accepted.

Trend Micro License Agreement

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install ServerProtect v5.80, you must accept this agreement.

We then enter the registration data.



User Information

You will need a serial number to enable the full version of the product.

To obtain a serial number, please visit:

https://olr.trendmicro.com/registration/us/en-us/

to register the Registration Key that came in the software package.

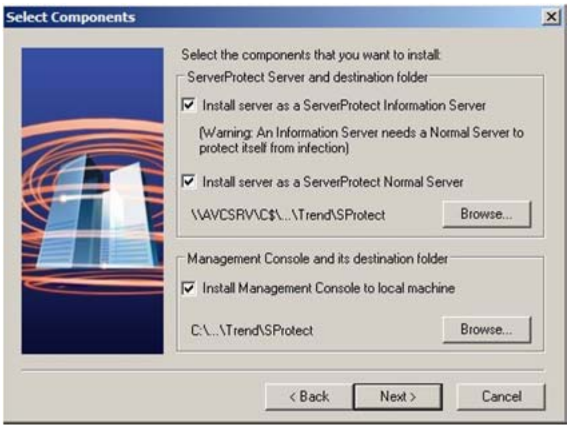
After registration, enter the generated serial number into the box below and click Next.

Name:

Company:

Serial:

After this, we can choose the individual functions of ServerProtect:


Select Components

Select the components that you want to install:

ServerProtect Server and destination folder

☑ Install server as a ServerProtect Information Server

(Warning: An Information Server needs a Normal Server to protect itself from infection)

☑ Install server as a ServerProtect Normal Server

\\AVCSRV\C$\...\Trend\SProtect

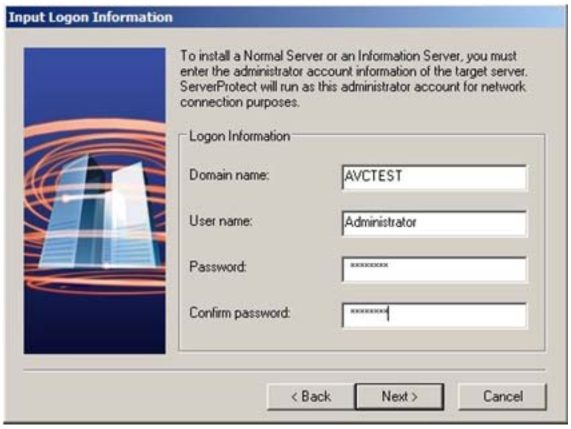
Management Console and its destination folder

☑ Install Management Console to local machine

C:\...\Trend\SProtect

Next, we enter credentials of an administrator account to be used to manage ServerProtect.

Next we enter the "Information Server" password and the domain:


Input Logon Information

To install a Normal Server or an Information Server, you must enter the administrator account information of the target server. ServerProtect will run as this administrator account for network connection purposes.

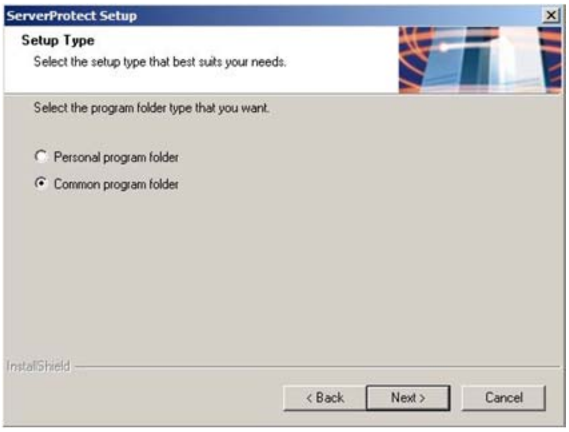
Logon Information

Domain name: AVCTEST

User name: Administrator

Password: ********

Confirm password: ********


ServerProtect Setup

Setup Type

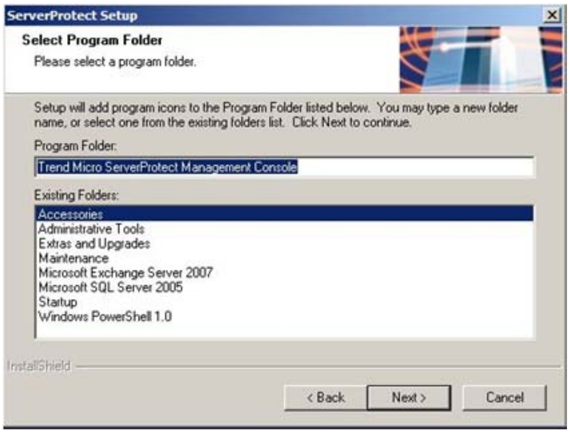
Select the setup type that best suits your needs.

Select the program folder type that you want.

○ Personal program folder

● Common program folder

The next point concerns the creation of a program group in the Windows Start Menu:


ServerProtect Setup

Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

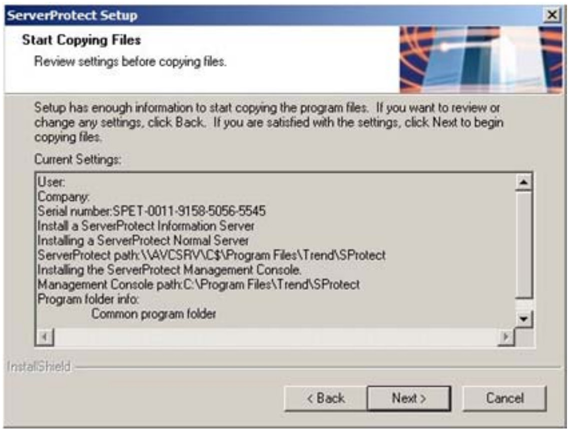
Program Folder:

Trend Micro ServerProtect Management Console

Existing Folders:

Accessories
Administrative Tools
Extras and Upgrades
Maintenance
Microsoft Exchange Server 2007
Microsoft SQL Server 2005
Startup
Windows PowerShell 1.0

The installer now has enough information to begin the setup process:


ServerProtect Setup

Start Copying Files

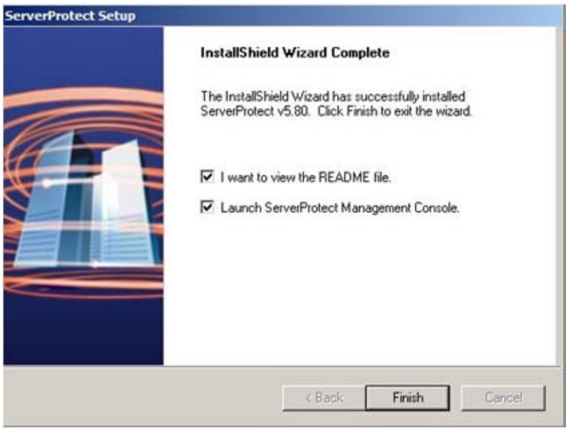
Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
User:
Company:
Serial number:SPET-0011-9158-5056-5545
Install a ServerProtect Information Server
Installing a ServerProtect Normal Server
ServerProtect path:\\AVCSRV\C$\Program Files\Trend\SProtect
Installing the ServerProtect Management Console.
Management Console path:C:\Program Files\Trend\SProtect
Program folder info:
        Common program folder
```

On completion of the installation, we start the ServerProtect Management Interface:


ServerProtect Setup

InstallShield Wizard Complete

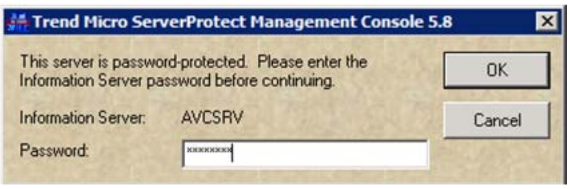
The InstallShield Wizard has successfully installed ServerProtect v5.80. Click Finish to exit the wizard.

☑ I want to view the README file.

☑ Launch ServerProtect Management Console.

The ServerProtect management console

The first step is to enter the password into the familiar logon dialog box:



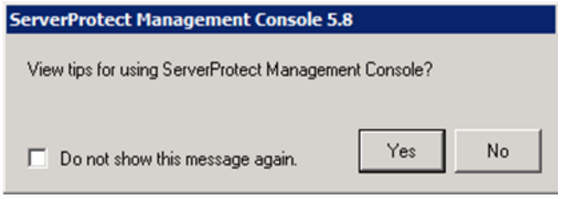
Trend Micro ServerProtect Management Console 5.8

This server is password-protected. Please enter the Information Server password before continuing.

Information Server: AVCSRV

Password: xxxxxxxx

Next we have to decide if we want tips for using the console to be displayed:

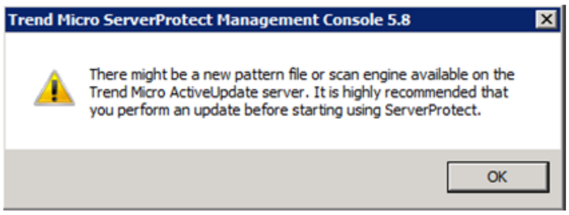


ServerProtect Management Console 5.8

View tips for using ServerProtect Management Console?

□ Do not show this message again.

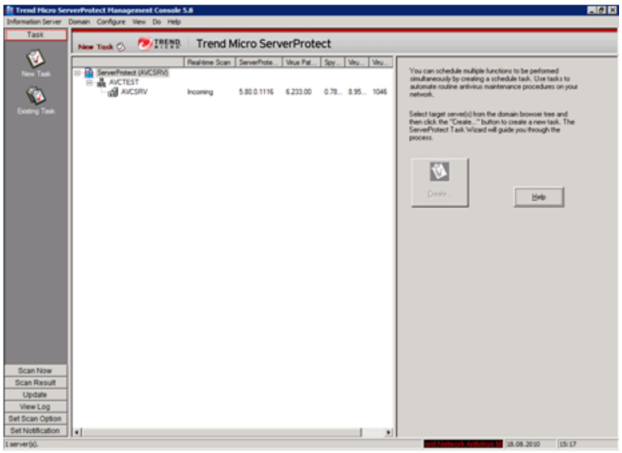
We were pleased to see that an update is immediately recommended:



Trend Micro ServerProtect Management Console 5.8

There might be a new pattern file or scan engine available on the Trend Micro ActiveUpdate server. It is highly recommended that you perform an update before starting using ServerProtect.

It seems that Trend Micro have adopted the motto "*Never change a running system*" as their company philosophy. The ServerProtect management console has not changed at all in the last 5 years



Trend Micro ServerProtect Management Console 5.8

	Real-time Scan	ServerProte...	Virus Pat...	Spy...	Viru...	Viru...
ServerProtect (AVCSRV)						
AVCTEST						
AVCSRV	Incoming	5.80.0.1116	6.233.00	0.78...	8.95...	1046

You can schedule multiple functions to be performed simultaneously by creating a schedule task. Use tasks to automate routine antivirus maintenance procedures on your network.

Select target server(s) from the domain browser tree and then click the "Create..." button to create a new task. The ServerProtect Task Wizard will guide you through the process.

1 server(s). 18.08.2010 15:17

Nonetheless, the console is straightforward and functional. On the left are links to the individual areas that can be configured.

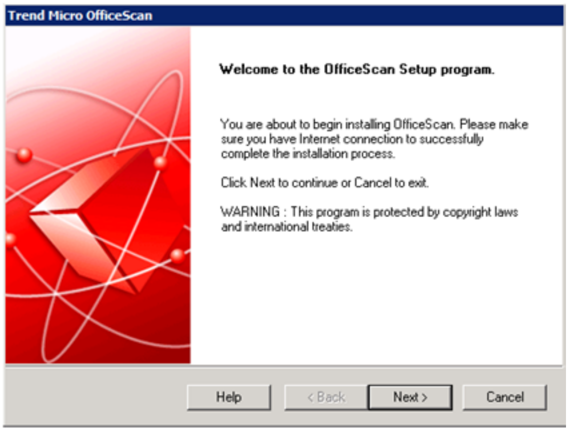
The ServerProtect system is structured simply. There are Information Servers, which are responsible for the updates and administration of ServerProtect branch servers.

This master/slave method ensures that the system can be scaled appropriately.

The console is perfectly functional, but a graphical facelift would definitely not hurt. This would not affect functionality or use, but would fit in better with modern operating systems.

Installation of Trend Micro OfficeScan 10

We begin the installation of OfficeScan:



Trend Micro OfficeScan

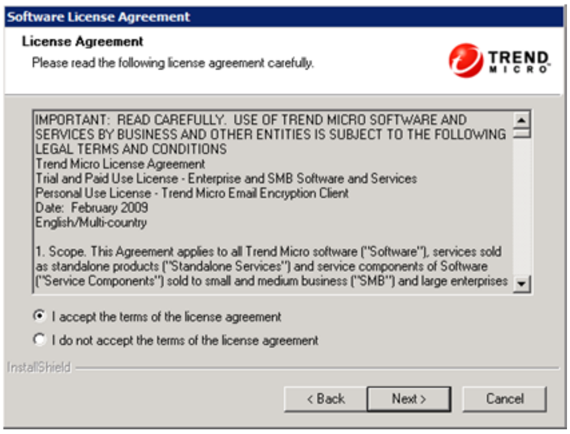
Welcome to the OfficeScan Setup program.

You are about to begin installing OfficeScan. Please make sure you have Internet connection to successfully complete the installation process.

Click Next to continue or Cancel to exit.

WARNING : This program is protected by copyright laws and international treaties.

There's the usual licence agreement to accept:



Software License Agreement

License Agreement

Please read the following license agreement carefully.

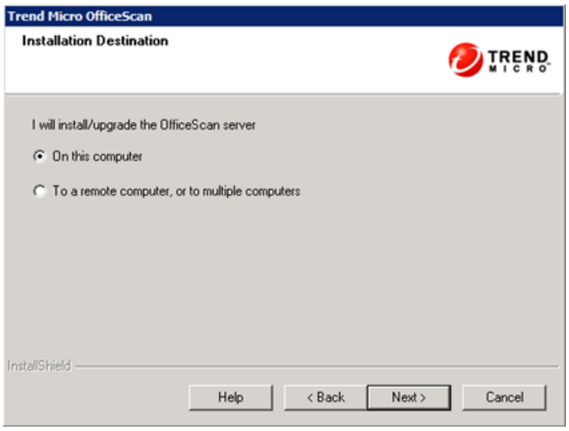
IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS
Trend Micro License Agreement
Trial and Paid Use License - Enterprise and SMB Software and Services
Personal Use License - Trend Micro Email Encryption Client
Date: February 2009
English/Multi-country

1. Scope. This Agreement applies to all Trend Micro software ("Software"), services sold as standalone products ("Standalone Services") and service components of Software ("Service Components") sold to small and medium business ("SMB") and large enterprises

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

Next we can choose between a local installation, and remote installation to one or more different computers:



Trend Micro OfficeScan

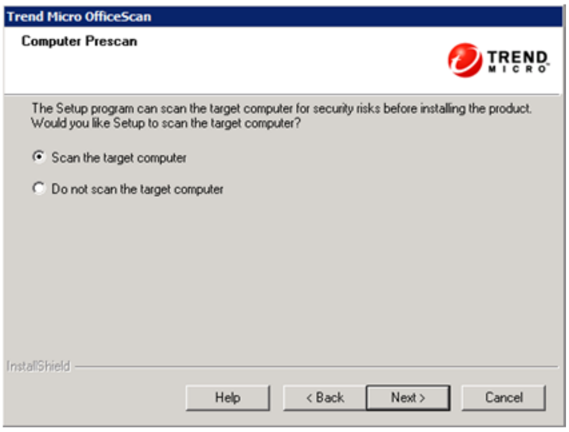
Installation Destination

I will install/upgrade the OfficeScan server

● On this computer

○ To a remote computer, or to multiple computers

The option is provided of scanning the target computer for threats before installation:



Trend Micro OfficeScan

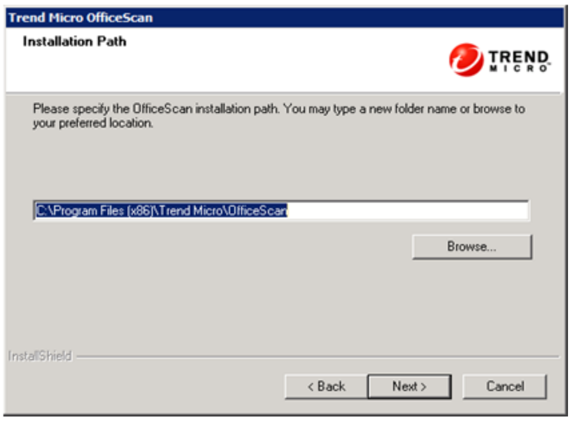
Computer Prescan

The Setup program can scan the target computer for security risks before installing the product. Would you like Setup to scan the target computer?

● Scan the target computer

○ Do not scan the target computer

Next we choose the installation folder:



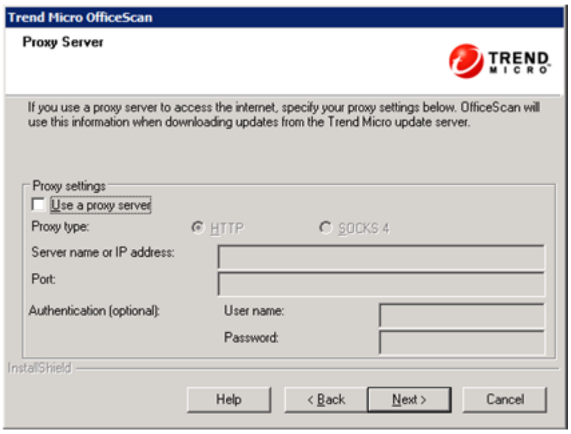
Trend Micro OfficeScan

Installation Path

Please specify the OfficeScan installation path. You may type a new folder name or browse to your preferred location.

C:\Program Files (x86)\Trend Micro\OfficeScan

Now we have the chance to enter any proxy settings necessary:



Trend Micro OfficeScan

Proxy Server

If you use a proxy server to access the internet, specify your proxy settings below. OfficeScan will use this information when downloading updates from the Trend Micro update server.

Proxy settings

□ Use a proxy server

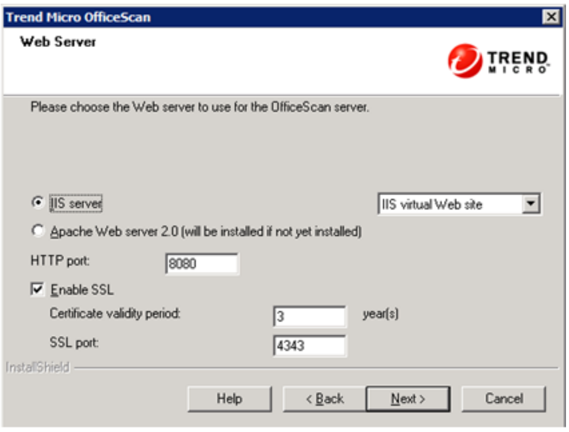
Proxy type: ● HTTP ○ SOCKS 4

Server name or IP address:

Port:

Authentication (optional): User name: Password:

Next we enter the web server that will be responsible for managing OfficeScan on this PC:



Trend Micro OfficeScan

Web Server

Please choose the Web server to use for the OfficeScan server.

● IIS server — IIS virtual Web site

○ Apache Web server 2.0 (will be installed if not yet installed)

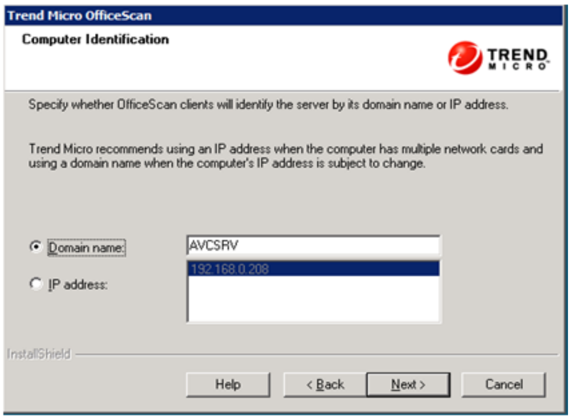
HTTP port: 8080

☑ Enable SSL

Certificate validity period: 3 year(s)

SSL port: 4343

Here we can choose whether the client should be located by its Windows hostname (“domain name”) or IP address:



Trend Micro OfficeScan

Computer Identification

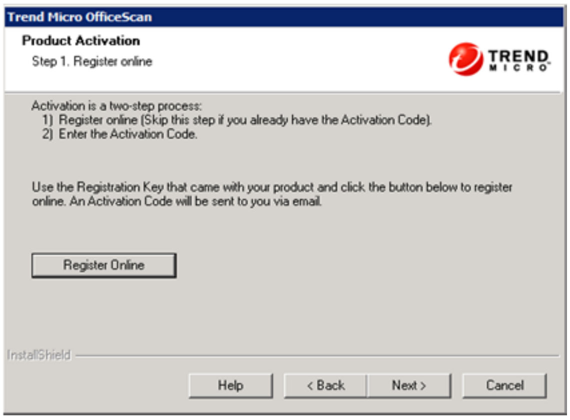
Specify whether OfficeScan clients will identify the server by its domain name or IP address.

Trend Micro recommends using an IP address when the computer has multiple network cards and using a domain name when the computer's IP address is subject to change.

● Domain name: AVCSRV

○ IP address: 192.168.0.208

In the next step, we activate the product:



Trend Micro OfficeScan

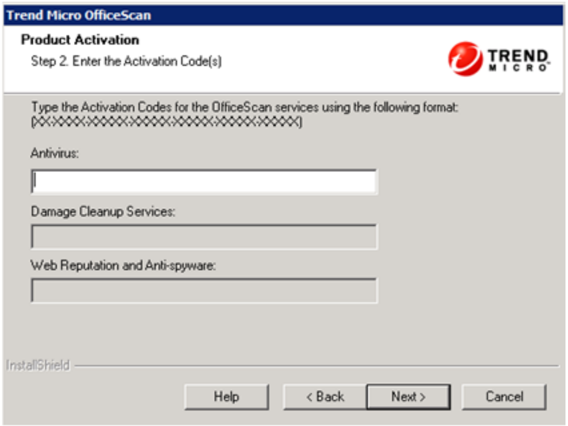
Product Activation

Step 1. Register online

Activation is a two-step process:
1) Register online (Skip this step if you already have the Activation Code).
2) Enter the Activation Code.

Use the Registration Key that came with your product and click the button below to register online. An Activation Code will be sent to you via email.

Next we need to enter activation codes for the various services:



Trend Micro OfficeScan

Product Activation

Step 2. Enter the Activation Code(s)

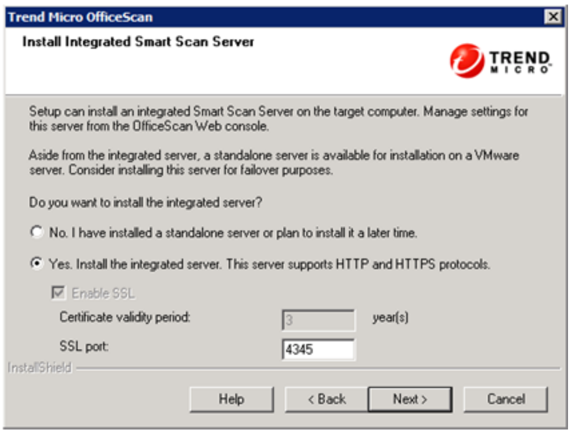
Type the Activation Codes for the OfficeScan services using the following format: (XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX)

Antivirus:

Damage Cleanup Services:

Web Reputation and Anti-spyware:

At this point, we have the chance to install a Smart Scan Server, which runs a fast Cloud-based scanning service:



Trend Micro OfficeScan

Install Integrated Smart Scan Server

Setup can install an integrated Smart Scan Server on the target computer. Manage settings for this server from the OfficeScan Web console.

Aside from the integrated server, a standalone server is available for installation on a VMware server. Consider installing this server for failover purposes.

Do you want to install the integrated server?

○ No. I have installed a standalone server or plan to install it a later time.

● Yes. Install the integrated server. This server supports HTTP and HTTPS protocols.

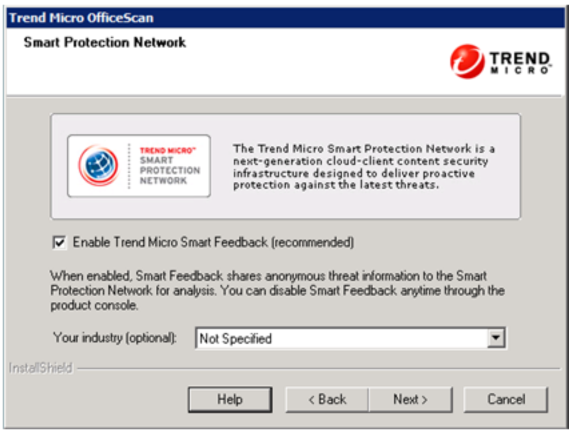
☑ Enable SSL

Certificate validity period: 3 year(s)

SSL port: 4345

We choose to install the Smart Scan Server, and now we can choose additional functions.

There is of course the usual enquiry as to whether to join the manufacturer's feedback mechanism, Smart Protection Network:



Trend Micro OfficeScan

Smart Protection Network

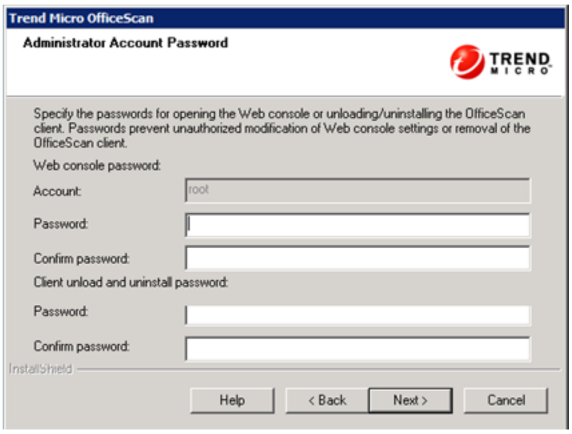
The Trend Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to deliver proactive protection against the latest threats.

☑ Enable Trend Micro Smart Feedback (recommended)

When enabled, Smart Feedback shares anonymous threat information to the Smart Protection Network for analysis. You can disable Smart Feedback anytime through the product console.

Your industry (optional): Not Specified

Now we can enter administrator credentials for the OfficeScan management console:



Trend Micro OfficeScan

Administrator Account Password

Specify the passwords for opening the Web console or unloading/uninstalling the OfficeScan client. Passwords prevent unauthorized modification of Web console settings or removal of the OfficeScan client.

Web console password:

Account: root

Password:

Confirm password:

Client unload and uninstall password:

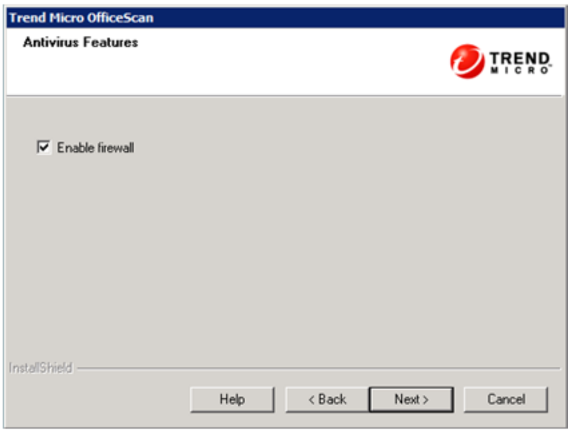
Password:

Confirm password:

Unfortunately there is no option here to use an existing AD account.

Next, we have to state a source folder from which clients will obtain software update packets.

This is followed by the option of installing the Trend Micro client firewall:

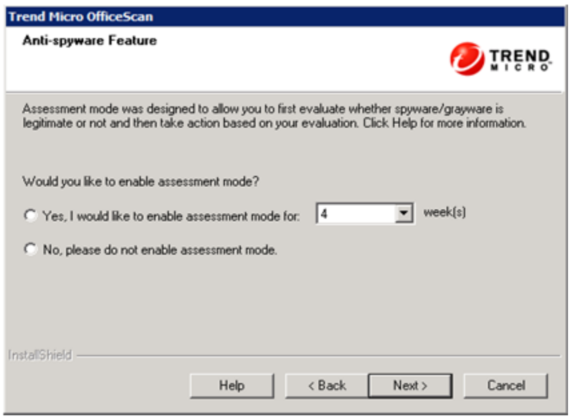


Trend Micro OfficeScan

Antivirus Features

☑ Enable firewall

Next, we can decide whether to use the "assessment mode", which ascertains whether some potentially unwanted applications are legitimate or not:



Trend Micro OfficeScan

Anti-spyware Feature

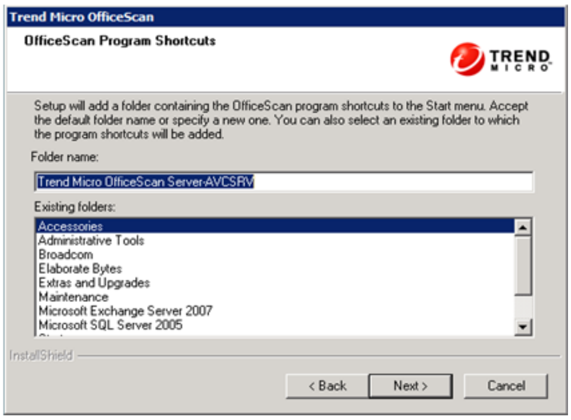
Assessment mode was designed to allow you to first evaluate whether spyware/grayware is legitimate or not and then take action based on your evaluation. Click Help for more information.

Would you like to enable assessment mode?

○ Yes, I would like to enable assessment mode for: 4 week(s)

○ No, please do not enable assessment mode.

Now we come to the next dialog box (it feels like the hundredth), where we can decide on the folder to use for Trend Micro shortcuts in the Windows Start Menu:



Trend Micro OfficeScan

OfficeScan Program Shortcuts

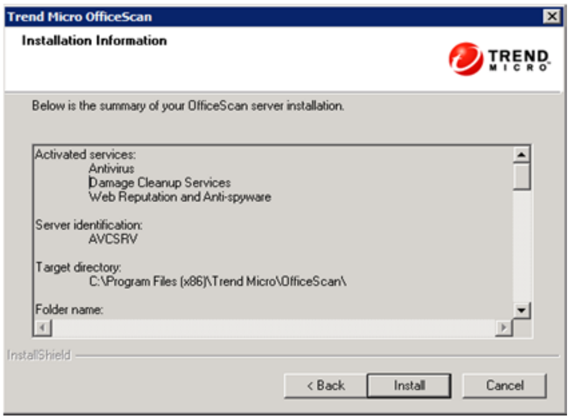
Setup will add a folder containing the OfficeScan program shortcuts to the Start menu. Accept the default folder name or specify a new one. You can also select an existing folder to which the program shortcuts will be added.

Folder name: Trend Micro OfficeScan Server-AVCSRV

Existing folders:

Accessories
Administrative Tools
Broadcom
Elaborate Bytes
Extras and Upgrades
Maintenance
Microsoft Exchange Server 2007
Microsoft SQL Server 2005

At last the installer has enough information to proceed:



Trend Micro OfficeScan

Installation Information

Below is the summary of your OfficeScan server installation.

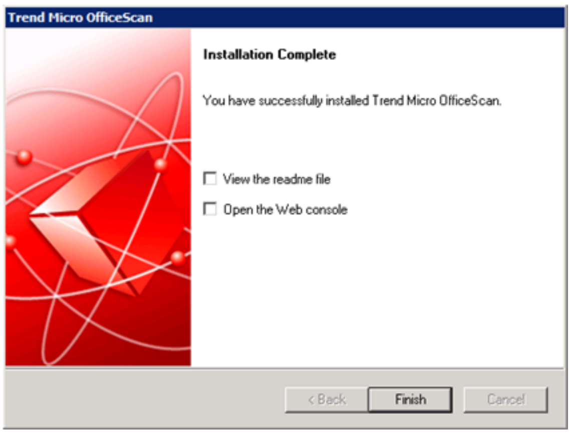
Activated services:
Antivirus
Damage Cleanup Services
Web Reputation and Anti-spyware

Server identification:
AVCSRV

Target directory:
C:\Program Files (x86)\Trend Micro\OfficeScan\

Folder name:

The installation of OfficeScan takes rather longer than that of competing products.



Trend Micro OfficeScan

Installation Complete

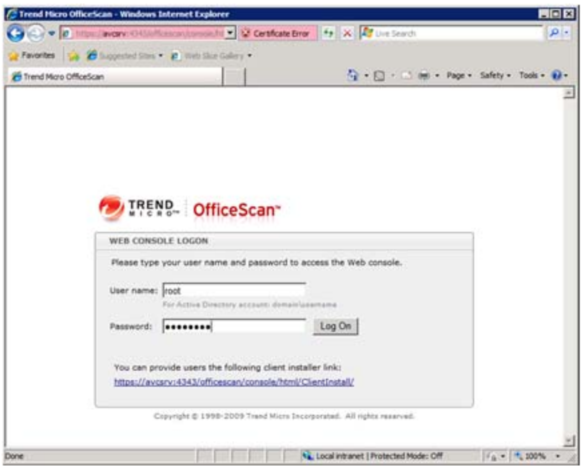
You have successfully installed Trend Micro OfficeScan.

□ View the readme file

□ Open the Web console

The management interface OfficeScan 10

We are greeted by the login dialog of the console:



Trend Micro OfficeScan - Windows Internet Explorer

WEB CONSOLE LOGON

Please type your user name and password to access the Web console.

User name: root

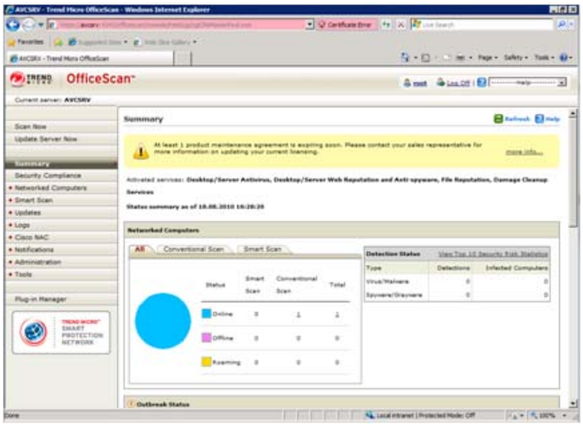
For Active Directory account: domain\username

Password: ●●●●●●●●●

You can provide users the following client installer link:
https://avcsrv:4343/officescan/console/html/ClientInstall/

Copyright © 1998-2009 Trend Micro Incorporated. All rights reserved.

Here again, Trend Micro sticks with a familiar and proven interface:



AVCSRV - Trend Micro OfficeScan - Windows Internet Explorer

Current server: AVCSRV

Summary

At least 1 product maintenance agreement is expiring soon. Please contact your sales representative for more information on updating your current licensing.

Activated services: Desktop/Server Antivirus, Desktop/Server Web Reputation and Anti-spyware, File Reputation, Damage Cleanup Services

Networked Computers

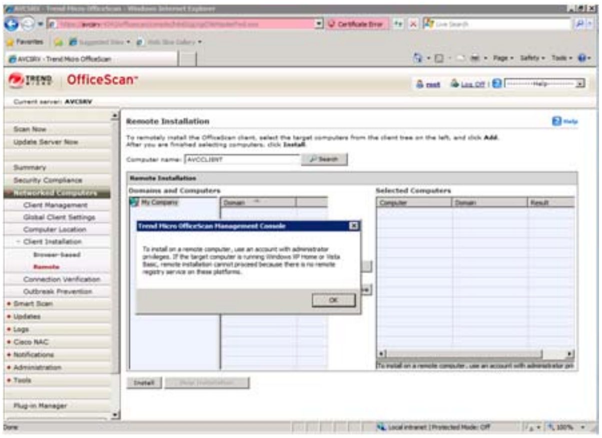
Status	Smart Scan	Conventional Scan	Total
🟦 Online	0	1	1
🟪 Offline	0	0	0
🟨 Roaming	0	0	0

Detection Status

Type	Detections	Infected Computers
Virus/Malware	0	0
Spyware/Grayware	0	0

To protect a computer with OfficeScan, we go to Networked Computers | Client Installation | Remote. To select a client, we have to enter the appropriate login credentials.

Next we are informed that Remote Installation will not work with Windows XP Home or Vista Basic. But, these OS's, lack of an enterprise networking stack prevents deployment using remote deployment. There are other methods to deploy the software - login script, MSI packager, exe, web install, etc.



AVCSRV - Trend Micro OfficeScan - Windows Internet Explorer

Current server: AVCSRV

Remote Installation

To remotely install the OfficeScan client, select the target computers from the client tree on the left, and click **Add**. After you are finished selecting computers, click **Install**.

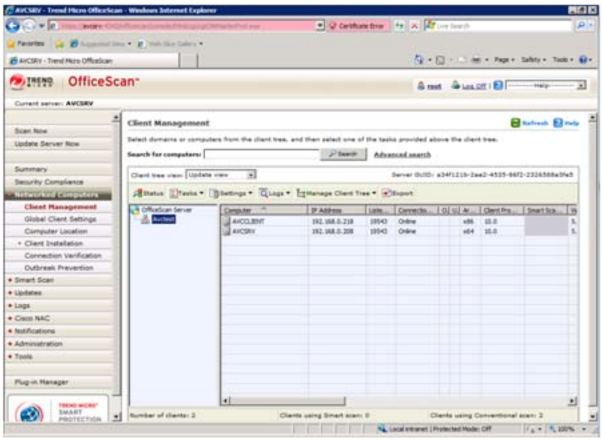
Computer name: AVCCLIENT

Trend Micro OfficeScan Management Console

To install on a remote computer, use an account with administrator privileges. If the target computer is running Windows XP Home or Vista Basic, remote installation cannot proceed because there is no remote registry service on these platforms.

There are various methods of installing the client software. There is the choice of remote installation via the OfficeScan console, sending an email with a link to the installation files, or using a login script.

Once the software has been installed, the client can be managed using the management console:



AVCSRV - Trend Micro OfficeScan - Windows Internet Explorer

Current server: AVCSRV

Client Management

Select domains or computers from the client tree, and then select one of the tasks provided above the client tree.

Search for computers:

Client tree view: Update view

Server GUID: a34f121b-2ae2-4535-86f2-2326588a5fe5

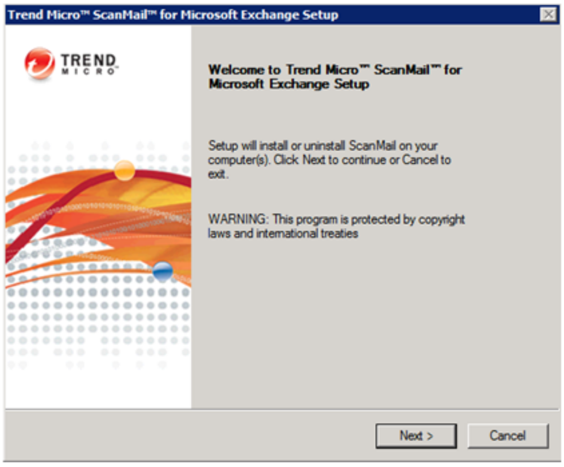
Computer	IP Address	Liste...	Connectio...	O	U	Ar...	Client Pro...	Smart Sca...
AVCCLIENT	192.168.0.218	19543	Online			x86	10.0	
AVCSRV	192.168.0.208	19543	Online			x64	10.0	

Number of clients: 2 Clients using Smart scan: 0 Clients using Conventional scan: 2

The OfficeScan console impressed us with its clear structures and self-explanatory menus.

Exchange 2007 protection

We begin the installation of Trend Micro ScanMail:



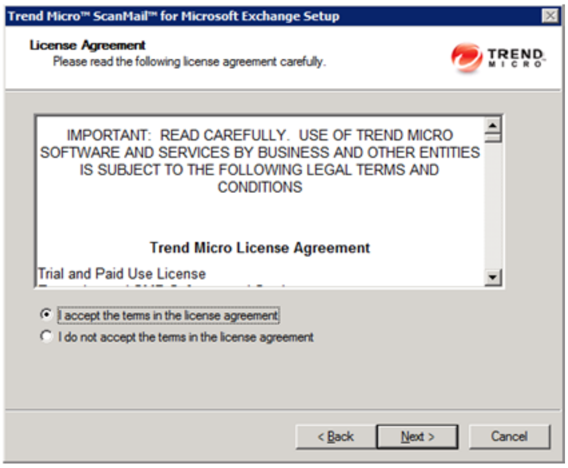
Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Welcome to Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Setup will install or uninstall ScanMail on your computer(s). Click Next to continue or Cancel to exit.

WARNING: This program is protected by copyright laws and international treaties

We accept the licence agreement:



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

License Agreement

Please read the following license agreement carefully.

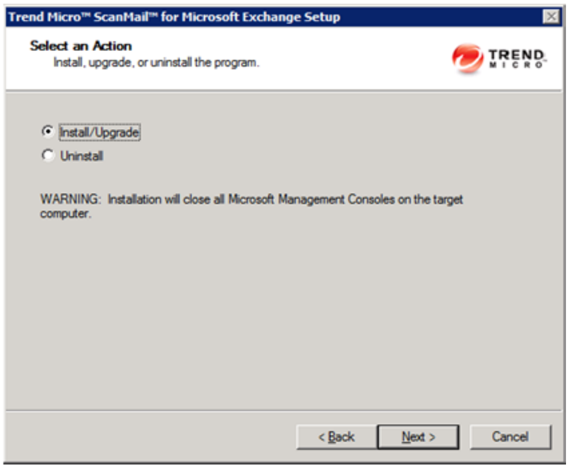
IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement

Trial and Paid Use License

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Select an Action

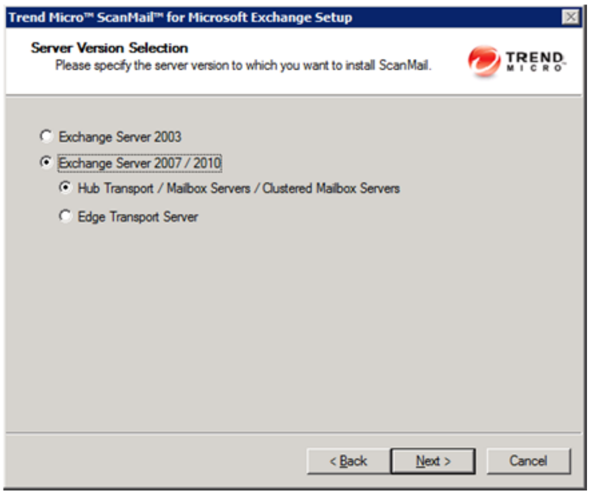
Install, upgrade, or uninstall the program.

● Install/Upgrade

○ Uninstall

WARNING: Installation will close all Microsoft Management Consoles on the target computer.

Somewhat confused, we continue with the installation. The next question is another we haven't seen before; other manufacturers don't find it necessary.



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Server Version Selection

Please specify the server version to which you want to install ScanMail.

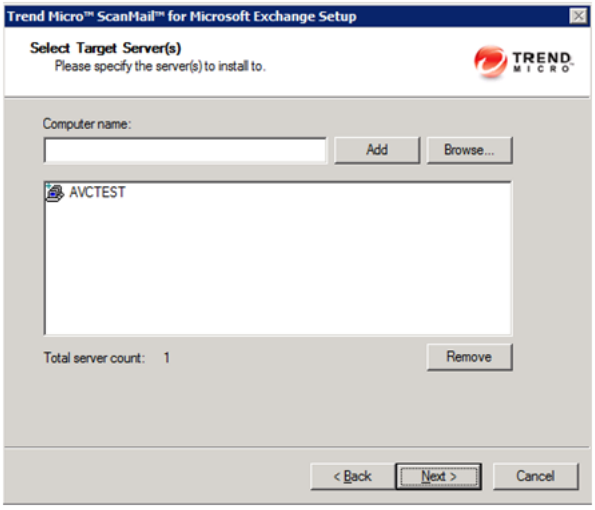
○ Exchange Server 2003

● Exchange Server 2007 / 2010

● Hub Transport / Mailbox Servers / Clustered Mailbox Servers

○ Edge Transport Server

Now we even have to state what the target server for installation:



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Select Target Server(s)

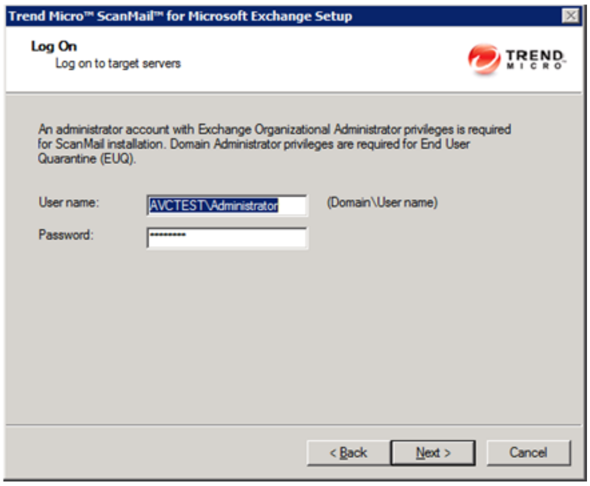
Please specify the server(s) to install to.

Computer name:

AVCTEST

Total server count: 1

The login credentials for the target server have to be entered.



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Log On

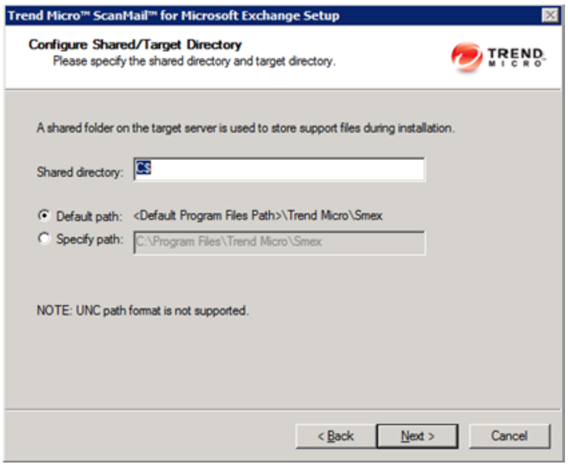
Log on to target servers

An administrator account with Exchange Organizational Administrator privileges is required for ScanMail installation. Domain Administrator privileges are required for End User Quarantine (EUQ).

User name: AVCTEST\Administrator (Domain\User name)

Password: ********

Here too we can state the path to the desired installation folder:



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Configure Shared/Target Directory

Please specify the shared directory and target directory.

A shared folder on the target server is used to store support files during installation.

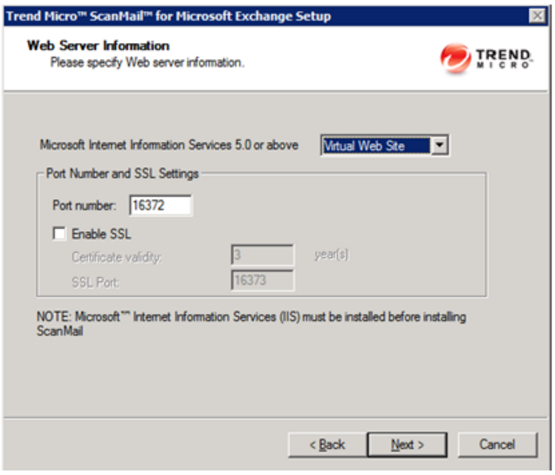
Shared directory: C$

● Default path: <Default Program Files Path>\Trend Micro\Smex

○ Specify path: C:\Program Files\Trend Micro\Smex

NOTE: UNC path format is not supported.

Next we have to enter the web server settings:



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Web Server Information

Please specify Web server information.

Microsoft Internet Information Services 5.0 or above: Virtual Web Site

Port Number and SSL Settings

Port number: 16372

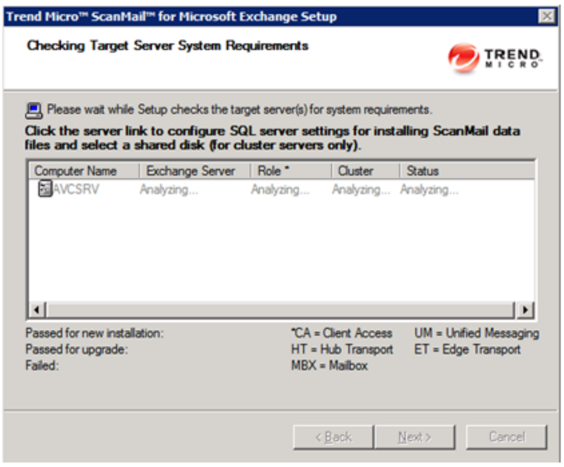
□ Enable SSL

Certificate validity: 3 year(s)

SSL Port: 16373

NOTE: Microsoft™ Internet Information Services (IIS) must be installed before installing ScanMail

As we have so far sorely missed automatic detection in the setup process, we are especially surprised to see the next dialog:



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Checking Target Server System Requirements

Please wait while Setup checks the target server(s) for system requirements.

Click the server link to configure SQL server settings for installing ScanMail data files and select a shared disk (for cluster servers only).

Computer Name	Exchange Server	Role *	Cluster	Status
AVCSRV	Analyzing...	Analyzing...	Analyzing...	Analyzing...

Passed for new installation:

Passed for upgrade:

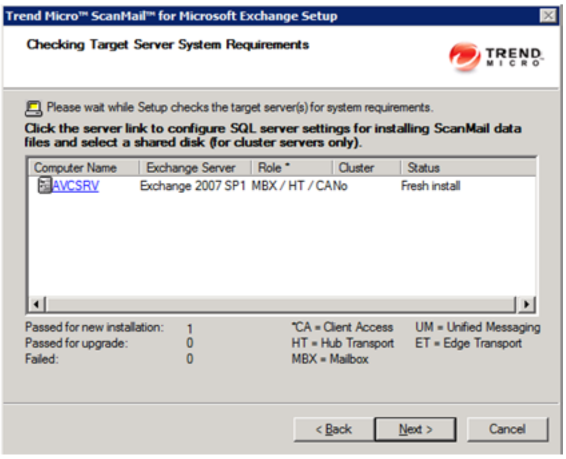
Failed:

*CA = Client Access UM = Unified Messaging

HT = Hub Transport ET = Edge Transport

MBX = Mailbox

Now the installer confirms the information which we have had to enter manually:



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Checking Target Server System Requirements

Please wait while Setup checks the target server(s) for system requirements.

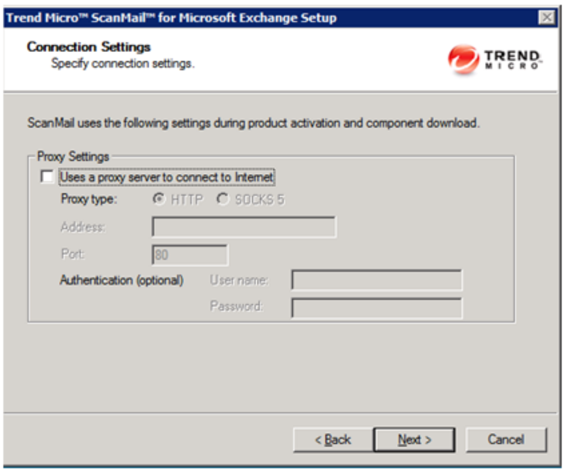
Click the server link to configure SQL server settings for installing ScanMail data files and select a shared disk (for cluster servers only).

Computer Name	Exchange Server	Role *	Cluster	Status
AVCSRV	Exchange 2007 SP1	MBX / HT / CA	No	Fresh install

Passed for new installation: 1
Passed for upgrade: 0
Failed: 0

*CA = Client Access UM = Unified Messaging
HT = Hub Transport ET = Edge Transport
MBX = Mailbox

The installer still needs more input from the user, namely proxy settings:



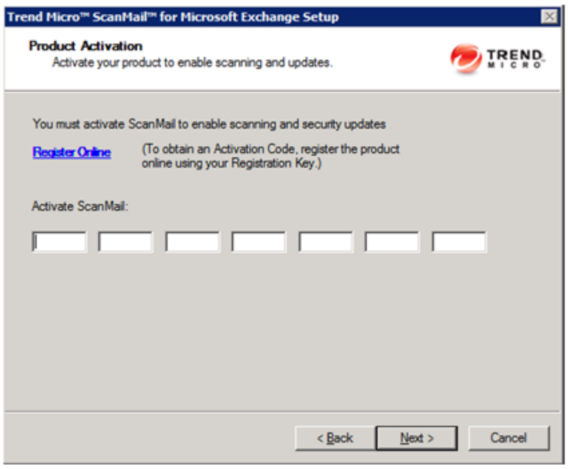
Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Connection Settings
Specify connection settings.

ScanMail uses the following settings during product activation and component download.

Proxy Settings
☐ Uses a proxy server to connect to Internet
Proxy type: ● HTTP ○ SOCKS 5
Address:
Port: 80
Authentication (optional) User name:
Password:

Next we have to enter the activation code:



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

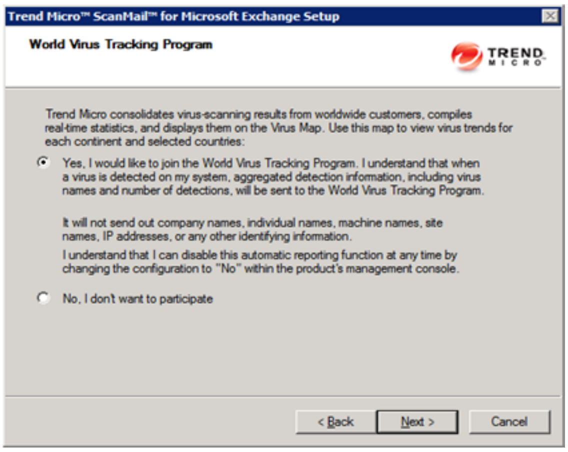
Product Activation
Activate your product to enable scanning and updates.

You must activate ScanMail to enable scanning and security updates

Register Online (To obtain an Activation Code, register the product online using your Registration Key.)

Activate ScanMail:

Again we are asked if we want to take part in the manufacturer's data sharing program, called World Virus Tracking Program:



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

World Virus Tracking Program

Trend Micro consolidates virus-scanning results from worldwide customers, compiles real-time statistics, and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries:

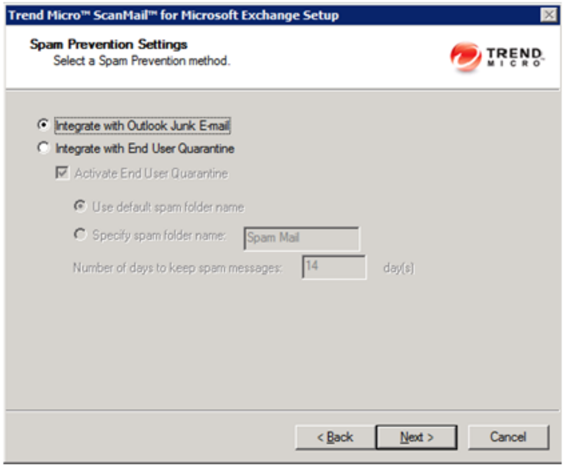
● Yes, I would like to join the World Virus Tracking Program. I understand that when a virus is detected on my system, aggregated detection information, including virus names and number of detections, will be sent to the World Virus Tracking Program.

It will not send out company names, individual names, machine names, site names, IP addresses, or any other identifying information.

I understand that I can disable this automatic reporting function at any time by changing the configuration to "No" within the product's management console.

○ No, I don't want to participate

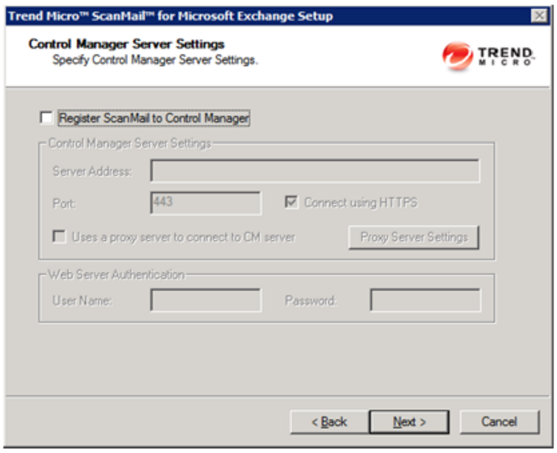
Every detail is asked separately. Now we have to decide what to do with spam mails:



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Spam Prevention Settings
Select a Spam Prevention method.

● Integrate with Outlook Junk E-mail
○ Integrate with End User Quarantine
☑ Activate End User Quarantine
● Use default spam folder name
○ Specify spam folder name: Spam Mail
Number of days to keep spam messages: 14 day(s)



Trend Micro™ ScanMail™ for Microsoft Exchange Setup

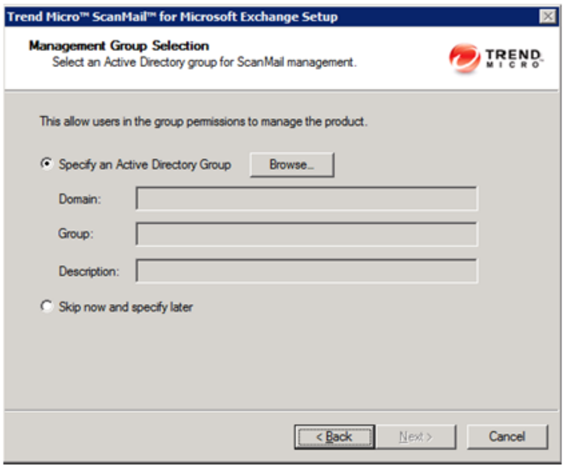
Control Manager Server Settings
Specify Control Manager Server Settings.

☐ Register ScanMail to Control Manager

Control Manager Server Settings
Server Address:
Port: 443 ☑ Connect using HTTPS
☐ Uses a proxy server to connect to CM server

Web Server Authentication
User Name: Password:

In this step, we can use AD to select a group to manage ScanMail:


Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Management Group Selection
Select an Active Directory group for ScanMail management.

This allow users in the group permissions to manage the product.

● Specify an Active Directory Group

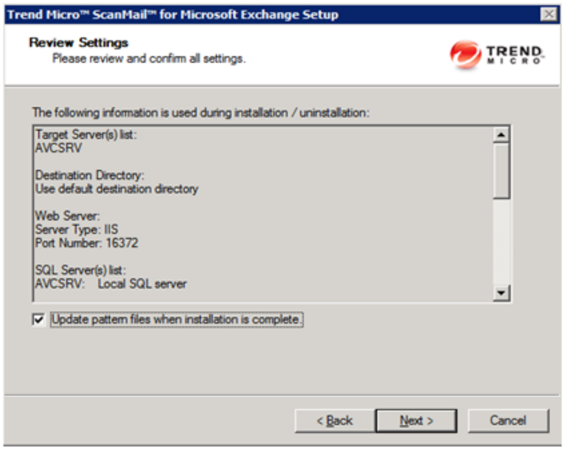
Domain:

Group:

Description:

○ Skip now and specify later

Finally the installer has gathered all the necessary information:


Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Review Settings
Please review and confirm all settings.

The following information is used during installation / uninstallation:

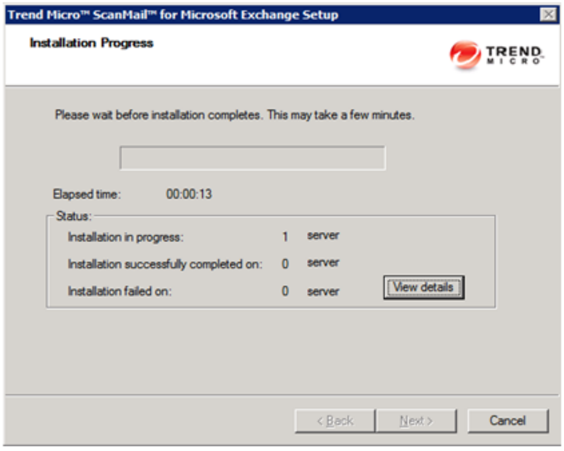
Target Server(s) list:
AVCSRV

Destination Directory:
Use default destination directory

Web Server:
Server Type: IIS
Port Number: 16372

SQL Server(s) list:
AVCSRV: Local SQL server

☑ Update pattern files when installation is complete


Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Installation Progress

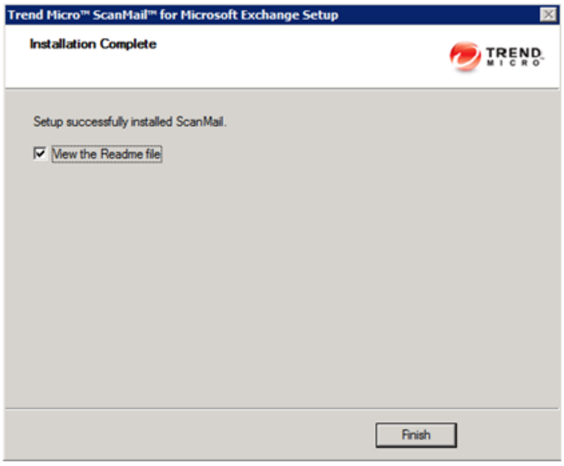
Please wait before installation completes. This may take a few minutes.

Elapsed time: 00:00:13

Status:

Installation in progress:	1	server
Installation successfully completed on:	0	server
Installation failed on:	0	server

Our Exchange server is now protected by ScanMail:

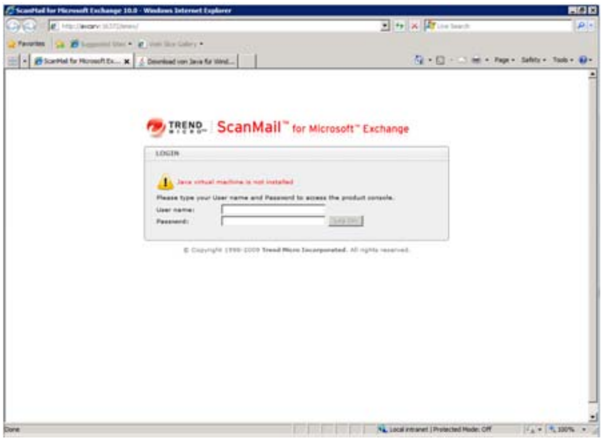

Trend Micro™ ScanMail™ for Microsoft Exchange Setup

Installation Complete

Setup successfully installed ScanMail.

☑ View the Readme file

The ScanMail management interface


ScanMail for Microsoft Exchange 10.0 - Windows Internet Explorer
Favorites
ScanMail for Microsoft Ex...
Download von Java für Wind...
Page
Safety
Tools
TREND MICRO
ScanMail™ for Microsoft™ Exchange
LOGIN
Log On
Done
Local intranet | Protected Mode: Off
100%

Java virtual machine is not installed

Please type your User name and Password to access the product console.

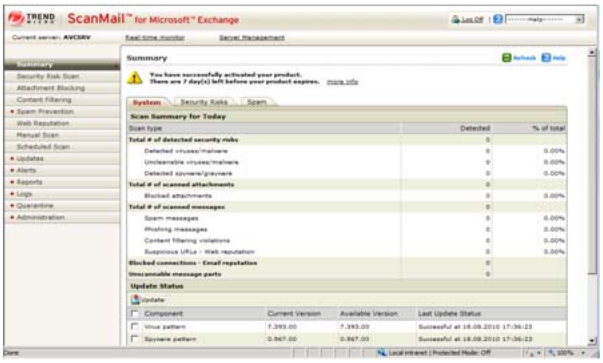
User name:

Password:

© Copyright 1998-2009 Trend Micro Incorporated. All rights reserved.

The ScanMail management console uses the same design as that of OfficeScan, and so anyone familiar with OfficeScan will find their way around easily.

The detailed summary page of the console is particularly good, giving an overview of all important information:



Current server: AVCSRV

Summary

You have successfully activated your product.
There are 7 day(s) left before your product expires. more info

Scan Summary for Today

Scan type	Detected	% of total
Total # of detected security risks	0	
Detected viruses/malware	0	0.00%
Uncleanable viruses/malware	0	0.00%
Detected spyware/grayware	0	0.00%
Total # of scanned attachments	0	
Blocked attachments	0	0.00%
Total # of scanned messages	0	
Spam messages	0	0.00%
Phishing messages	0	0.00%
Content filtering violations	0	0.00%
Suspicious URLs - Web reputation	0	0.00%
Blocked connections - Email reputation	0	
Unscannable message parts	0	

Update Status

□ Component	Current Version	Available Version	Last Update Status
□ Virus pattern	7.393.00	7.393.00	Successful at 18.08.2010 17:36:23
□ Spyware pattern	0.967.00	0.967.00	Successful at 18.08.2010 17:36:23

Here too, the self-explanatory descriptions used are extremely helpful, so it is easy to find and use all the functionality.

The scope of the functions in ScanMail is very good, leaving nothing to be desired.

Thus, apart from the truly poor installer, there is nothing here to criticise.

Summary

Manufacturer's website

The Trend Micro website (**www.trendmicro.com)** is suitably designed and easy to find your way around. It conforms to normal Internet standards.

The site gives information about current threats and contains all the normal antivirus functions.

An online scanner is also available.

The installation process

The installation of the individual products requires a lot of information to be entered manually.

Once you have worked your way through the installers for OfficeScan and ScanMail, you will find a very useable interface which allows easy configuration.

The administrator console

Despite the fact that the administration interface of OfficeScan and ScanMail has hardly changed in recent years, it remains very practical to use. It was a very well-designed interface when it came out, and proves that some designs are so effective that they do not need to be changed.

Deployment areas

The Trend Micro suite is equally suited to both small and large networks.

Antivirus clients

The OfficeScan client is certainly one of the simplest clients on the market. It runs unnoticed on the client PC, and with a well-configured OfficeScan console, no intervention is required.

Summary

Trend Micro is a suite that fits the requirements of both large and small networks. After a somewhat more demanding installation, the administrator can expect a proven interface with a functional design. The Control Manager can be customised easily to your own requirements.

Pros

+ Proven interface for OfficeScan and ScanMail

+ Management console

+ Functional web interface

Cons

- Long, irritating installation

- High degree of manual input required

Deployment areas

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★	★★★★	★★★★★

Summary

Installation Wizard	★★★
User Navigation	★★★★
Administrator Console	★★★★★
Default Values	★★★
MS Active Directory Support	★★★★
Database Support	★★
Remote Installation	★★★★
Website	★★★
Manual	★★★★

Feature List

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Recommended Product for								
up to 5 Clients, 1 Server	Avira AntiVir Professional	BitDefender Internet Security	ESET Smart Security Business Edition	G Data Antivirus Business	Kaspersky Small Office Security	McAfee SaaS and Email Protection	Sophos Computer Security (Small Business Edition)	Trend Micro Worry-Free Business Security
up to 25 Clients and 1 Fileserver	Avira NetWork Bundle	BitDefender Small Office Security	ESET Smart Security Business Edition + ESET File Security for Windows File Server	G Data Antivirus Business	Kaspersky Business Space Security	McAfee SaaS and Email Protection	Sophos Computer Security (Small Business Edition)	Trend Micro Worry-Free Business Security Advanced
up to 25 Clients and Fileserver and Messaging Server	Avira NetWork Bundle	BitDefender Corporate Security	ESET Smart Security Business Edition and Messaging Bundle	G Data Antivirus Enterprise	Kaspersky Enterprise Space Security	McAfee SaaS and Email Protection	Sophos Security Suite (Small Business Edition)	Trend Micro Worry-Free Business Security Advanced
more than 25 Clients, more than 1 Fileserver, more than 1 Messaging server	Avira AntiVir Business Bundle	BitDefender Corporate Security	ESET Smart Security Business Edition and ESET Mail Security	G Data Antivirus Enterprise	Kaspersky Enterprise Space Security	McAfee SaaS and Email Protection	Sophos Endpoint Security and Data Protection	Trend Micro Enterprise Security for Endpoints and Mailservers
Features Management Server								
What is the maximum number of clients overall?	20000	Recommended 1000 per single server. Scales to 10000 if Master/Slave is used (1 Master and 10 Slave Servers).	unlimited	50000	unlimited	unlimited	unlimited	unlimited

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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	20000	1000	10000	1000	50000	Unlimited, Management Server is Web NOC	25000	20000
Required minimum hardware (CPU/Memory/Disc)	Server: 128MB RAM, 512MB HDFrontend: 32MB RAM, 16MB HDAgent: 32MB RAM, 16MB HD	Intel Pentium compatible processor • 800MHz (1 GHz recommended) for Windows 2000/XP • 1GHz (Core2 Duo or equivalent recommended) for Windows Vista/7 • 256MB (512 MB recommended) for Windows 2000 • 512MB (1GB recommended) for Windows XP • 1GB RAM (1.5GB recommended) for Window Vista/7 HDD: 200MB (400MB for installation)	Hardware needs only to be strong enough to support the OS, and only optionally the database	Core 2 Duo 2 GB RAM 1,5 GB	Intel Core 2 Duo E8400, 3GHz, 4GB RAM, HDD SATA 300GB	Intel Pentium Processor or compatible architecture; 512Mb Ram; 500MB Disk space	2GHz Pentium or equivalent/512 MB/300 MB HD	OfficeScan server: 1GHz CPU, min 1 GB RAM , min 3.5 GB free hard disc space

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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?	●	●	configurable	configurable				●
Does the product provide a delta update mechanism?	●	●	●	●	●	●	●	●
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	Password protection, encrypted communication	Administrator account	Authentification username, password	Username/Password requirements	Password protection, encrypted communication, role-based administration	Authentification username, password
Require minimum password length					Depends on Windows Security Policy	●	●	●
Lock administrator account after entering a password multiple times (prevent brute force attack)					Depends on Windows Security Policy		●	●

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Log out administrator if idle for a specified time		•			Depends on Windows Security Policy		•	•
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	5 minutes	5 minutes	15 minutes	4 hours	Real Time	Real Time
Does the product support a push communication mode?	•		•	•	•		•	•
Does the product protect itself from being tampered with by the end-user or malicious software?	•	•	•		•		•	•
Prevent processes from being stopped	•	•	•		•			•
Prevent files and folders from being modified or deleted	•	•	•		•		•	•
Prevent product registry entries from being modified or deleted	•	•	•		•			•
Proxy Server								

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Can a proxy server be specified?	•	•	•	•	•	•	•	•
For HTTP	•	•	•	•	•	•	•	•
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.				Various product versions can be managed within a few clicks	
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?	•	•	•	•	•	•	•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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 sent 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 options can be set for the client installation in the user interface?								

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Does the product allow the administrator to define the installation options (i.e. silent, interactive, installation folder, etc) in the user interface?	•	•	•	•	•	•	•	•
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 chosen 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	Define if user is restricted or power, define what modules to install or enable/disable, restart options, scan before install, set administrative password	Virtually all options of the client can be specified as a parameter of the push installation				Group on bootstrap	

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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?	●		●	●	●	●	●	●

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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?								
Protection technology policies								
Antivirus policies	•			•	•	•		
Firewall policies	•		•	•	•	•	•	•
HIPS & IPS policies	•		•		IPS only	•		IPS only
Device Control policies				•	•			•
Other protection technology policies	Updating			Anti-Spam, Web Content filter, Internet usage control, Application control	Anti-Spam; Proactive Defense; Anti-Banner; Anti-Dialer; Anti-Hacker; Updating	Browser control	Updating	Web Reputation
Client settings	•				•	•		
User interface configuration	•			•	•	•		
Communication settings	•			•	•			•
Content update settings	•		When the client detects the notebook is running on battery, scheduled scans are automatically delayed and updated program components are not downloaded	•	•	•	•	•
Can the customer define an 'unlimited' number of locations?			•	•	•	•		•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Which criteria can the customer use to define locations?								
Client IP Configuration								
By specifying IP addresses / IP address ranges	•		•		•	•	over AD	•
By specifying 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			•		•		over AD	

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
By specifying the type of network connection used or not used by the client (e.g. Ethernet, Wireless, VPN, Dial-up, etc.)	always the adapter that provides the gateway		•				over AD	•
By checking whether a client can or can not resolve a DNS host name							over AD	•
By checking the Registry							over AD	
Can multiple criteria be used to define a location?			•		•		over AD	
When is 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 & Synchronization								
Can computers be imported from a text file?	•	•	•		•		•	
Can computers be imported from Active Directory?	•	•	•	•	•	•	•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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 synchronization schedule be defined?			•		•	•	•	•
Can computers be imported from multiple Active Directory servers?					•		•	•
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 administrator defined lists of extensions	•	•	•		•	•	•	•
By filenames ("file.txt") regardless of folder or location	•	•			•	•		•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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		•	•		•		•	•
Exchange 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 (i.e. which processes to ignore)?		•		•	•	•		•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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	10	100	unlimited	unlimited	10	2
Does the product protect itself against Zip of Death and similar attacks?								
By limiting the recursion depth	●	●	●		●		●	●

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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 files	•				•		•	
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				Removable media	
Does the product provide preconfigured scan locations?	•		•		•		•	
On Demand Scans								
Can the administrator define when scans should take place?	•	•	•	•	•	•	•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Can the system impact vs. scan speed be defined?	•		•	•	•			•
Can the administrator specify which Scan Locations should be included / excluded?	•	•	•	•	•	•	•	•
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	•		•	•	•	•	•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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 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	•	•	•	•	•	•	•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Can the product create a backup of the file before attempting to clean it?	•		•		•	•		•
Quarantine on the local system	•	•	•	•	•	•	•	•
Quarantine in a central location (i.e. management server, quarantine server, etc)			•	•	•		•	•
Delete	•	•	•	•	•	•	•	•
Deny Access (for On Access Scans)	•	•	•	•	•	•	•	
Which processes specific actions can the product perform								
Terminate the process	•	•	•		•	•	•	•
Stop the service		•	•			•	•	•
Registry Access Rules								
Does the product allow monitoring and preventing access to registry keys and values?		•			•		•	•
Does the product allow to define/exclude for which processes (application and services) a registry access rule applies?		•			•		•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
File and Folder Access Rules								
Does the product allow monitoring and preventing 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 Name		•		•			•	•
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)			only if mounted as a removable drive	•			•	•
Any Local Hard Drive		•	only if mounted as a removable drive	•				
Any CD/DVD Drive			only if mounted as a removable drive	•			•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Any Network Drive		●					●	●
Any removable media		●	only if mounted as a removable drive	USB/firewire				●
Process Access Rules								
Does the product allow monitoring and preventing launching processes?				●			●	●
Does the product allow monitoring and preventing 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")	●	●					●	●

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Using wildcards (i.e. *,?)								
Limit by location (i.e. local drive, CD, USB Stick)							●	
Other							By user authorization and by Behavioral Genotype-based whitelisting identities produced by SophosLabs	
HIPS Actions								
Which actions can be taken when a rule is triggered?	Block, allow, allow once, block once, ignore		Block		Block	Block, allow	Block, report only, terminate	
Allow Access to the resource	●		●		●	●	●	
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?								

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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 exists / does not exist							•	
File has specified hash / file fingerprint								
File version							•	
Directory exists							•	
Which conditions can be specified for file (application) versions?								
File version is equal / not equal to specified version							•	
File version is higher / lower 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?								

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Is equal / not equal to specified number					•		•	
Is greater / less than specified number							•	
Conditions for text (String) registry values?								
Is case sensitive equal / not equal to specified text								
Is case in-sensitive equal / not equal to specified text					•		•	
Contains / does not contain specified text (case sensitive)								
Contains / does not contain specified text (case in-sensitive)							•	
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							•	

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Is higher / lower than 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						AntiSpyware	
Remediation								
Does the product provide remediation capabilities?	•	•					•	•
Which remediation action can be defined in the user interface (without resorting to scripts)?								
Registry remediation	•							•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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		•	Alert user when OS is not up-to-date (patched)				•	Virtual Patching provided via the Intrusion Defense Firewall
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	•		•		•		•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Symantec Network Access Control								
Other			OPSWAT				DHCP, 802.1X, VPN	
Does the product have inbuilt enforcement capabilities?								
Host Based Enforcement / Self Enforcement (i.e. leveraging a desktop firewall to prevent network connections)	•	•			•		•	
Other			OPSWAT					
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								

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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	●	●	●	●	●		●	●

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Raw Ethernet		●	●		●		Ability to control network traffic below the IP layer like EAP or PPP and legacy protocols like IPX and Apple Talk	●
Other	128 protocols supported		IPv6-ICMP, IGMP, GRE, ESP, SMP	IGMP, GGP, GUP, IDP, GRE			PPTP	
Which Actions can be taken when a firewall rule is triggered?								
Allow/Block traffic	●	●	●	●	●	●	●	●
Ask the end-user	●	●	●	●	●		●	
Notify 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?		●	●		●			

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Can the number of times an end-user can disable the firewall between reboots be limited?								
Can the end-user easily block all network traffic?		•	•		•			
Can the end-user be allowed to see the network traffic in real time?	•	•	•	•	•			
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,		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		Allowed in last 10 mins, Allowed today, Blocked 10min/today, Processes, System log	
Can the firewall rules be exported and imported?		•	•	•	•		•	
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)	•	•		•	•			•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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		•	Possible using a script		•			
Scan computer	•	•	•	•	•		•	•
Enable On Access Scan	•	•	•	•	•	•	•	•
Enable/Disable Firewall	•	•	•	•	•	•	•	•
Other		All actions available in the client product	Change all aspects of configuration, including handing off a client to another server	mail scan on/off/software update			Comply with policy, Clean up, Initiate scans, Acknowledge alerts, Protect (install/reinstall) etc.	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)	•		•		•		•	partially - outdated clients, firewall rules

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Other		Computers with a specific user logged on (policies per user)			Any set of computers (task for a set of computers) or according to the administration group's hierarchy.		Automatically deploy to discovered machines in AD	
Can the status of the actions be tracked?	●	●	●		●	●	●	●
Is there a web based console?			No. The console is windows based and can run from any computer on the network and access the server from there. The console software is portable and can run from a thumb drive.	●		●	●	●
Administrator Management								
Rights								
Does the product support multiple administrators?	●		One per server (master server, slave servers)	●	●	●	●	●
Does the product support different access levels for administrators?	●		●		●	●	●	●
Access Control								
Can access for administrators be limited?	●		●		●	●	●	●
Authentication mechanism								
Can administrators be authenticated using an integrated authentication mechanism (i.e. username / password)?	●	●	U/P for the administrator console or Windows/Domain authentication can be used	●	●	●	●	●

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Does the product enforce minimum password lengths?		•			Depends on Windows Security Policy	•	•	•
Does the product enforce maximum password age?					Depends on Windows Security Policy		•	•
Can administrators be authenticated using Active Directory?			•		•		•	•
Can administrators be authenticated using RSA Secure ID technology?								
Other				Administrator account			SEC uses AD, NAC and Encryption use separate authentication	
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?					Depends on Windows Security Policy		•	
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	•		•		•		Over AD	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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			•		Block			•
Can you lock								
DVD		•	•	•	•		•	•
Floppy		•	•	•	•		•	•
external media		•	•	•	•		•	•
USB		•	•	•	•		•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
other			All ports and all removable media can be locked, but it's possible to add exceptions for any individual ports or media	webcams			WiFi, IR, Bluetooth, Modems, Firewire, SATA, PCMCIA, Blueray, CD, Unencrypted/Encrypted USB devices, Network bridging	network resources
(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 facing signatures?	●		●		●			●
Does the product include vulnerability facing signatures?	●		●		●			●

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Which actions can be performed?								
Traffic can be allowed / blocked / dropped			●		●		●	●
Incident can be logged	●		●		●		●	●
Failover								
What if the AV Server (local) hang-ups								
automat. switching to a second local server		●	●	●	●		●	●
updates from vendor-server instead of local server	●	●	●	●	●		●	●
other					any other network shared folder			
Quarantine								
Quarantine Folder								
Is there a centralized quarantine-folder			No, but administrator console provides a centralized view of the quarantine on clients	●	●		●	●
Is there a quarantine-folder on the client	●	●	●	●	●	●	●	●
can administrators specify the location of the quarantine folder anywhere	●		●			●	●	●
rechecking quarantine								
after a signature update, is the quarantine folder checked?			●		●			
automatically			●		●			
manually	●	●			●	●	●	

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
undo av-action if false positive is detected	•		•		•		•	
Messaging								
Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange
Feature overview Messaging								
Modules and functional areas			Special module for Exchange. Full integration with MS Exchange, scans the whole Exchange store. Manageable from the central management server. Supports 64-bit Exchange.	Gateway Solution			Complete defense against spam, phishing, malware and data leakage. An upcoming add-on will enable email encryption.	antimalware, antispam, content filtering, attachment blocking, Url filtering
Malware detection								
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled.	•	•	•	•	•		•	•
Information Store scans 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	•	•	•	•			•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Definition of file limitations by a combination of file name, file extension and file size.	•	•	•		only by file extension and by time		•	•
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				•			Optionally possible through integration with email encryption server or as part of upcoming on-box encryption capability.	•
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	•	•		•	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	•	•	•	•	•		•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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	•	•	•		Only for addresses		•	•
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	•	•			•		•	

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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
Modules and functional areas			Integration with most Windows mail servers is possible through the command line scanner	Gateway Solution			Complete defense against spam, phishing, malware, and data leakage	
Malware detection								
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled		•	•	•	•		•	•
Information Store scan on every server					•		•	

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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		•					•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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		•					•	

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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
Modules and functional areas			Special product for Linux mail servers. Includes Anti-Spam, web administration interface. Manageable from the central management console.	Gateway Solution			Complete defense against spam, phishing, malware, and data leakage.	
Malware detection								
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled.			•	•	•		•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Information Store scans 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.			●	●			●	
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		●					●	●

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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							•	

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
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 list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Language:								
In which languages are your corporate products available?	English, German, Spanish, Russian, Italian	English, German, French, Spanish, Chinese Simplified, Japanese, Chinese Traditional, Brazilian Portuguese	Management Server and Console (English, Japanese, Russian, French, Spanish, Polish, Chinese Simplified, Chinese Traditional) Client (Bulgarian, Simplified and Traditional Chinese, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, French Canadian, German, Hungarian, Italian, Japanese, Kazakh, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, Turkish, Ukrainian)	German, English, French, Italian, Spanish, Russian, Brazilian, Turkish, Polish, Japanese	KAV for Windows Workstations & KAV for Windows Servers: 12 languages (English, Russian, Estonian, French, German, Italian, Japanese, Polish, Portuguese, Portuguese (Brazil), Spanish, Turkish). Kaspersky Administration Kit: 7 languages (English, Russian, French, German, Spanish, Polish, Italian).	English, Danish, German, French, Chinese (Simplified or Traditional), Dutch, Hebrew, Italian, Japanese, Korean, Portuguese (Brazilian or Iberian), Spanish, Russian, Finnish, Norwegian, Swedish and Turkish.	English, Spanish, French, Italian, German, Chinese, Japanese	Server Products: English only Desktop Products: all languages in which the products are available
In which languages are your (help) manuals available?	Server: German, English. Client: German, English, Spanish, Russian, Italian	English, German, French, Spanish, Chinese Simplified, Japanese, soon to be released: Chinese Traditional, Brazilian Portuguese	All languages in which the products are available	German, English, French, Italian, Spanish, Russian, Brazilian, Turkish, Polish, Japanese	KAV for Windows Workstations & KAV for Windows Servers: 10 languages (English, Russian, French, German, Italian, Japanese, Polish, Portuguese, Spanish). Kaspersky Administration Kit: 7 languages (English, Russian, French, German, Italian, Japanese, Spanish)	English, Danish, German, French, Chinese (Simplified or Traditional), Dutch, Hebrew, Italian, Japanese, Korean, Portuguese (Brazilian or Iberian), Spanish, Russian, Finnish, Norwegian, Swedish and Turkish.	English, Spanish, French, Italian, German, Chinese, Japanese	Server Products: English only Desktop Products: all languages in which the products are available

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Support								
24/7/365 phone support	for SLA customers	No For Business Products we offer support during business hours in US (EST), UK, DACH, Spain, Romania	for SLA customers	•	for SLA customers	For customers with active support accounts	•	for SLA customers
Dial Rates	Depends on location	Regular (no additional fees)	Toll Free Numbers are available in most countries	Depends on location	Depends on location	Depends on location and support agreement	Depends on location	Regular (no additional fees)
Supported Support Languages	German, English	English, German, Spanish, Romanian, French (our partners offer Tier 1 support in their local languages. They are more than the languages specified above).	ESET has four regional offices (US and Canada, Slovakia, Czech Republic, Argentina); all of the offices provide technical support in their local languages. In addition ESET has exclusive distributors in 50 countries and value added resellers in over 100 additional countries. Support in those countries is provided in local language by the local distributor, who in turn receives support directly from ESET.	German, English, French, Italian, Spanish	Local in countries of presence and English	Local in countries of presence and English	English, Spanish, French, Italian, German, Japanese	Local in countries of presence and English
Remote Desktop Control for support	•	•	•	•	•	•	•	•
Support per Forum	•	•	•		•	•	•	•
Support over Email	•	•	•	•	•	•	•	•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Guaranteed E-Mail response within		Tiered based on the partner or client level: - Platinum 2h - Gold 4h - Silver 6h - Bronze 8h	Guaranteed response for Premium 24/7/365 business support is 1 hour.			Dependent on Support Entitlement		Tiered based on the partner or client level: - Platinum 2h - Gold 4h - Silver 6h - Bronze 8h
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	•	•		•

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Why should users choose your product and not another?	Best detection, fast product, 20 years of experience and continuity, Proven protection	1. BitDefender has very high detection rate awarded the highest possible ADVANCED+ award and also very few false alarms for its anti-virus engine 2. BitDefender provides a more extensive set of Web-based threat protection than any other vendor 3. BitDefender delivers updates more frequently than most of its competitors 4. BitDefender is the only vendor providing Endpoint Auditing and Management scripts 5. BitDefender Client Security has more extensive system and user control features than other vendors	ESET offers the best performance and requires the least resources on workstation. ESET is also the unmatched leader in proactive protection - ESET holds the most AV-Comparatives ADVANCED+ awards in Proactive/Retrospective tests. Centralized management is easy, 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 Security-as-a-Service solutions are designed to provide organizations of all sizes, from small to large enterprises, with a comprehensive set of security products built on a Software-as-a-Service model. This strategy leverages McAfee's core strength in threat prevention, our diverse SaaS portfolio, and our industry-leading global threat intelligence, powered by McAfee Labs.	Sophos and Sophos products are geared towards supporting businesses. Offer Anti-virus, anti-spyware, data loss prevention, device control, application control, network access control and encryption through a single product. Simple-to-use products with low total cost of ownership. Central management of Windows, Mac, Linux, Unix clients. Broadest platform support. Direct support 24/7/365 included in license. Upgrades and updates are included within the license price (no extra charges). Protection provided by global, integrated SophosLabs 24/7/365	

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
Pricing								
Scenario A: 5 clients, server, outlook as mail client								
recommended product	Avira AntiVir Professional	BitDefender Internet Security + BitDefender Security for File Servers for 5 users	ESET Smart Security	G Data AntiVirus MultiUser	Kaspersky Small Office Security	McAfee SaaS and Email Protection (with GOLD support)	Sophos Computer Security (Small Business Edition)	Trend Micro Worry-Free Business Security
1 year Euro	175	167	187	74	208	263	250	270
3 years Euro	350	360	392	195	625	506	500	620
1 year USD	245	205	198	95	209	359	243	370
3 years USD	490	440	396	250	418	754	485	850
Scenario B SMB: 1 SBS 2003 Server, 25 Clients								
recommended product	Avira NetWork Bundle	BitDefender Small Office Security Suite	ESET Smart Security Client + File Server Security	G Data AntiVirus Enterprise	Kaspersky Business Space Security	McAfee SaaS and Email Protection (with GOLD support)	Sophos Security Suite (Small Business Edition)	Trend Micro Worry-Free Business Security Advanced
1 year plan EURO	1015	79	680	1045	716	1104	1606	1652
3 year plan EURO	2030	1578	1428	2122	1610	2126	3212	2589
1 year plan USD	1420	963	930	1340	780	1509	1380	2260
3 year plan USD	2840	1925	1862	2722	1560	3169	2762	3540
Scenario C: 1 Fileserver, 1 Exchange server, 200 Clients								
recommended product	Avira AntiVir Business Bundle	BitDefender SBS Security Suite	ESET NOD32 Antivirus 4 + ESET File Server Security + ESET Mail Server Security	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	McAfee SaaS and Email Protection (with GOLD support)	Sophos Endpoint Security and Data Protection	Trend Micro Worry-Free Business Security Advanced
1 year plan EURO	8600	6880	4910	5575	5166	7407	7550	9700
3 year plan EURO	17200	13760	10311	11878	11622	14261	15100	15520
1 year plan USD	12050	8390	6380	7152	6210	10124	8600	13280

Feature list	AVIRA	Bitdefender	ESET	G Data	Kaspersky	McAfee	Sophos	Trend Micro
3 year plan USD	24100	16780	12760	15238	12400	21260	17200	21260
Scenario D, 2 Fileserver, 1 Exchange server, 1000 Clients								
recommended product	Avira AntiVir Business Bundle	BitDefender SBS Security Suite	ESET NOD32 Antivirus + ESET File Server Security + ESET Mail Server Security	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	McAfee SaaS and Email Protection (with GOLD support)	Sophos Endpoint Security and Data Protection	Trend Micro Enterprise Security for Endpoints and Mail Server
1 year plan EURO	27090	27060	16020	19258	18647	23861	25250	48730
3 year plan EURO	54180	54120	33662	39719	41954	45947	50500	77970
1 year plan USD	37900	33000	20932	24706	25351	32617	28750	66750
3 year plan USD	75800	66000	41864	50955	50601	68505	57500	106800
Scenario E: 10 Fileserver, 10 Exchange server, 10000 Clients								
recommended product	Avira AntiVir Business Bundle	BitDefender SBS Security Suite	ESET NOD32 Antivirus + ESET File Server Security + ESET Mail Server Security	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	McAfee SaaS and Email Protection (with GOLD support)	Sophos Endpoint Security and Data Protection	Trend Micro Enterprise Security for Endpoints and Mail Server
1 year plan EURO	163400	The price for more than 10000 users is negotiated case by case. Please see the reference price for 1000 users	117100	192380	134930	166030	The price for more than 10000 users is negotiated case by case. Please see the reference price for 1000 users	The price for more than 10000 users is negotiated case by case. Please see the reference price for 1000 users
3 year plan EURO	326800	Price is negotiated case by case	245310	396790	303500	319630	Price is negotiated case by case	Price is negotiated case by case
1 year plan USD	228820	Price is negotiated case by case	152120	246800	207200	226850	Price is negotiated case by case	Price is negotiated case by case
3 year plan USD	457650	Price is negotiated case by case	304240	509040	414410	476450	Price is negotiated case by case	Price is negotiated case by case

All prices are Manufactured Suggested Retail Prices of 2010. Actual retail prices may differ considerably esp. for scenarios D and E, as esp. for large projects many factors and savings/discounts may apply. Please contact the vendors for actual project prices. The here listed prices are just a rough estimation. Furthermore, some products may be more expensive as they include e.g. additional Support (or Suites instead of AV clients only).

System Requirements Part 1

System Requirements	AVIRA	AVIRA	AVIRA	ESET	ESET	ESET	G Data	G Data	G Data	Kaspersky	Kaspersky	Kaspersky
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
Apple												
Mac OS												
Mac OS X						●						
Mac OS X Server												
iPhone OS												
iPod OS												
Windows 2000												
Professional		●	●	●	●	●			●	●	●	●
Server	●	●		●	●	●			●	●	●	●
Advanced Server				●	●	●			●	●	●	●
Advanced Server 64 Bit Intel				●	●	●						
Advanced Server 64 Bit Itanium												
Data Center Server				Untested	Untested	Untested			●			
Data Center Server 64 Bit Intel				Untested	Untested	Untested						
Data Center Server 64 Bit Itanium												
Windows XP												
Home		●	●	●	●	●	●	●	●		●	●
Professional		●	●	●	●	●	●	●	●	●	●	●
Professional 64 Bit Intel		●	●	●	●	●	●	●	●	●	●	●
Media Center				●	●	●	●	●	●			
Media Center 2004				●	●	●	●	●	●			
Media Center 2005				●	●	●	●	●	●			
Tablet PC Edition				●	●	●	●	●	●			

System Requirements	AVIRA	AVIRA	AVIRA	ESET	ESET	ESET	G Data	G Data	G Data	Kaspersky	Kaspersky	Kaspersky
Embedded				●	●	●	●	●	●			●
Windows Server 2003												
Standard	●			●	●	●	●	●	●	●	●	●
Enterprise 32 Bit	●			●	●	●	●	●	●	●	●	●
Enterprise 64 Bit	●	●		●	●	●	●	●	●	●	●	●
Data Center 32 Bit	●	●		Untested	Untested	Untested	●	●	●	●	●	●
Data Center 64 Bit	●	●		Untested	Untested	Untested	●	●	●	●	●	●
Small Business Server	●	●		●	●	●	●	●	●	●	●	●
Cluster Server				Untested	Untested	Untested	●	●	●			
Storage Server				●	●	●	●	●	●			
Web Edition				●	●	●	●	●	●	●	●	●
R2 Standard 32 Bit	●	●	●	●	●	●	●	●	●	●	●	●
R2 Enterprise 32 Bit	●	●	●	●	●	●	●	●	●	●	●	●
R2 Standard 64 Bit	●	●	●	●	●	●	●	●	●	●	●	●
R2 Enterprise 64 Bit	●	●	●	●	●	●	●	●	●	●	●	●
Windows Vista												
Home Basic 32 Bit		●	●	●	●	●	●	●	●	●	●	●
Home Basic 64 Bit		●	●	●	●	●	●	●	●	●	●	●
Home Premium 32 Bit		●	●	●	●	●	●	●	●	●	●	●
Home Premium 64 Bit		●	●	●	●	●	●	●	●	●	●	●
Business 32 Bit		●	●	●	●	●	●	●	●	●	●	●
Business 64 Bit		●	●	●	●	●	●	●	●	●	●	●
Enterprise 32 Bit		●	●	●	●	●	●	●	●	●	●	●
Enterprise 64 Bit		●	●	●	●	●	●	●	●	●	●	●
Ultimate 32 Bit		●	●	●	●	●	●	●	●	●	●	●
Ultimate 64 Bit		●	●	●	●	●	●	●	●	●	●	●
Windows 7												
Starter Edition		●	●	●	●	●	●	●	●			
Home Premium 32 Bit		●	●	●	●	●	●	●	●	●	●	●
Home Premium 64 Bit		●	●	●	●	●	●	●	●	●	●	●
Professional 32 Bit		●	●	●	●	●	●	●	●	●	●	●
Professional 64 Bit		●	●	●	●	●	●	●	●	●	●	●
Ultimate / Enterprise 32 Bit		●	●	●	●	●	●	●	●	●	●	●
Ultimate / Enterprise 64 Bit		●	●	●	●	●	●	●	●	●	●	●
Windows Server 2008												
Standard 32 Bit	●	●		●	●	●	●	●	●	●	●	●

System Requirements	AVIRA	AVIRA	AVIRA	ESET	ESET	ESET	G Data	G Data	G Data	Kaspersky	Kaspersky	Kaspersky
Standard 32 Bit - Core Installation	•	•		command line only	command line only	command line only				•		only KAV for WSEE
Standard 64 Bit	•	•		•	•	•	•	•	•	•	•	•
Standard 64 Bit - Core Installation	•	•		command line only	command line only	command line only				•		only KAV for WSEE
Enterprise 32 Bit	•	•		•	•	•	•	•	•	•	•	•
Enterprise 64 Bit	•	•		•	•	•	•	•	•	•	•	•
Server R2 64 Bit (Standard/Enterprise)	•	•		•	•	•	•	•	•	•	•	•
Data Center 32 Bit	•	•		Untested	Untested	Untested	•	•	•	Untested	Untested	only KAV for WSEE
Data Center 64 Bit	•	•		Untested	Untested	Untested	•	•	•	Untested	Untested	only KAV for WSEE
Web Edition 32 Bit	•	•		•	•	•	•	•	•	Untested	Untested	only KAV for WSEE
Web Edition 64 Bit	•	•		•	•	•	•	•	•	Untested	Untested	only KAV for WSEE
Foundation 32 Bit				•	•	•	•	•	•			
Foundation 64 Bit				•	•	•	•	•	•			
HPC 32 Bit				Untested	Untested	Untested	•	•	•			
HPC 64 Bit				Untested	Untested	Untested	•	•	•			
Windows Mobile												
Windows Mobile 5.0 Smart Phone						•						KMS EE
Windows Mobile 5.0 PocketPC						•						KMS EE
Windows Mobile 6.0 Standard						•						KMS EE
Windows Mobile 6.0 Professional						•						KMS EE
Windows Mobile 6.1 Standard						•						KMS EE
Windows Mobile 6.1 Professional						•						KMS EE
Windows Mobile 6.5												
Works for Citrix				Untested	•	•	•	•	•			only KAV for WSEE
Symbian												
OS 9.0												KMS EE
OS 9.1												KMS EE

System Requirements	AVIRA	AVIRA	AVIRA	ESET	ESET	ESET	G Data	G Data	G Data	Kaspersky	Kaspersky	Kaspersky
OS 9.3												KMS EE
Series 60						•						KMS EE
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						•						

System Requirements	AVIRA	AVIRA	AVIRA	ESET	ESET	ESET	G Data	G Data	G Data	Kaspersky	Kaspersky	Kaspersky
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						Novell NetWare, DOS, Solaris, NetBSD, FreeBSD						
Database												
Does the product require a database	•			YES, built-in and supports some others			•	•		•		
For how many users/ clients is the free database recommended							unlimited	unlimited		5000		
Which database is included (i.e. Microsoft SQL, Sybase, MySQL, etc)				Microsoft Access (jet database) engine			SQL Express	SQL Express		Microsoft SQL		
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							•	•				

System Requirements	AVIRA	AVIRA	AVIRA	ESET	ESET	ESET	G Data	G Data	G Data	Kaspersky	Kaspersky	Kaspersky
Other	MS-Access, any ODBC database			MySQL, Oracle			SQL Azure	SQL Azure				
Email Server												
Microsoft Exchange	•					•	•	•			•	•
Domino						•	•	•			•	•
Tobit						Untested	•	•				
Linux	•					•	•	•			•	•
Mac							•	•			•	•
Novell Netware Server						•						•
Dell NAS						•						
Kerio						•						

System Requirements Part 2

System Requirements	Sophos	Sophos	Sophos	McAfee	McAfee	McAfee	Trend Micro	Trend Micro	Trend Micro	Bitdefender	Bitdefender	Bitdefender
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
Apple												
Mac OS												
Mac OS X			•						via plugin			
Mac OS X Server			•						via plugin			
iPhone OS												
iPod OS												
Windows 2000												
Professional	•	•	•							•	•	•
Server	•	•	•							•	•	•
Advanced Server	•	•	•							•	•	•
Advanced Server 64 Bit Intel	•	•	•							•	•	•
Advanced Server 64 Bit Itanium	•	•	•									
Data Center Server	•	•	•							•	•	•
Data Center Server 64 Bit Intel	•	•	•							•	•	•

System Requirements	Sophos	Sophos	Sophos	McAfee	McAfee	McAfee	Trend Micro	Trend Micro	Trend Micro	Bitdefender	Bitdefender	Bitdefender
Data Center Server 64 Bit Itanium	●	●	●									
Windows XP												
Home	●	●	●			●		●	●			●
Professional	●	●	●			●		●	●	●	●	●
Professional 64 Bit Intel	●	●	●			●		●	●	●	●	●
Media Center	●	●	●					●	●			
Media Center 2004	●	●	●					●	●			
Media Center 2005	●	●	●					●	●			
Tablet PC Edition	●	●	●			●		●	●			
Embedded	●	●	●					●	●			
Windows Server 2003												
Standard	●	●	●			●	●	●	●	●	●	●
Enterprise 32 Bit	●	●	●			●	●	●	●	●	●	●
Enterprise 64 Bit	●	●	●			●	●	●	●	●	●	●
Data Center 32 Bit	●	●	●				●	●	●	●	●	●
Data Center 64 Bit	●	●	●				●	●	●	●	●	●
Small Business Server	●	●	●			●		●		●	●	●
Cluster Server	●	●	●				●	●	●	●	●	●
Storage Server	●	●	●				●	●	●	●	●	●
Web Edition	●	●	●					●		●	●	●
R2 Standard 32 Bit	●	●	●							●	●	●
R2 Enterprise 32 Bit	●	●	●							●	●	●
R2 Standard 64 Bit	●	●	●							●	●	●
R2 Enterprise 64 Bit	●	●	●							●	●	●
Windows Vista												
Home Basic 32 Bit	●	●	●			●		●	●			●
Home Basic 64 Bit	●	●	●			●		●	●			●
Home Premium 32 Bit	●	●	●			●		●	●			●
Home Premium 64 Bit	●	●	●			●		●	●			●
Business 32 Bit	●	●	●			●		●	●	●	●	●
Business 64 Bit	●	●	●			●		●	●	●	●	●
Enterprise 32 Bit	●	●	●			●		●	●	●	●	●
Enterprise 64 Bit	●	●	●			●		●	●	●	●	●
Ultimate 32 Bit	●	●	●			●		●	●	●	●	●
Ultimate 64 Bit	●	●	●			●		●	●	●	●	●
Windows 7												
Starter Edition	●	●	●			●						●

System Requirements	Sophos	Sophos	Sophos	McAfee	McAfee	McAfee	Trend Micro	Trend Micro	Trend Micro	Bitdefender	Bitdefender	Bitdefender
Home Premium 32 Bit	●	●	●			●		●	●			●
Home Premium 64 Bit	●	●	●			●		●	●			●
Professional 32 Bit	●	●	●			●		●	●	●	●	●
Professional 64 Bit	●	●	●			●		●	●	●	●	●
Ultimate / Enterprise 32 Bit	●	●	●			●		●	●	●	●	●
Ultimate / Enterprise 64 Bit	●	●	●			●		●	●	●	●	●
Windows Server 2008												
Standard 32 Bit	●	●	●			●	●	●	●	●	●	●
Standard 32 Bit - Core Installation	●	●	●			●						
Standard 64 Bit	●	●	●			●	●	●	●	●	●	●
Standard 64 Bit - Core Installation	●	●	●			●						
Enterprise 32 Bit	●	●	●			●	●	●	●	●	●	●
Enterprise 64 Bit	●	●	●			●	●	●	●	●	●	●
Server R2 64 Bit (Standard/Enterprise)	●	●	●				●	●	●	●	●	●
Data Center 32 Bit	●	●	●				●	●	●	●	●	●
Data Center 64 Bit	●	●	●				●	●	●	●	●	●
Web Edition 32 Bit	●	●	●				●	●	●	●	●	●
Web Edition 64 Bit	●	●	●				●	●	●	●	●	●
Foundation 32 Bit	●	●	●							●	●	●
Foundation 64 Bit	●	●	●							●	●	●
HPC 32 Bit	●	●	●				●	●	●	●	●	●
HPC 64 Bit	●	●	●				●	●	●	●	●	●
Windows Mobile												
Windows Mobile 5.0 Smart Phone			●						via plugin			
Windows Mobile 5.0 PocketPC			●						via plugin			
Windows Mobile 6.0 Standard			●						via plugin			
Windows Mobile 6.0 Professional			●						via plugin			
Windows Mobile 6.1 Standard			●						via plugin			

System Requirements	Sophos	Sophos	Sophos	McAfee	McAfee	McAfee	Trend Micro	Trend Micro	Trend Micro	Bitdefender	Bitdefender	Bitdefender
Windows Mobile 6.1 Professional			•						via plugin			
Windows Mobile 6.5									via plugin			
Works for Citrix			•			•	•	•	•			
Symbian												
OS 9.0									via plugin			
OS 9.1									via plugin			
OS 9.3									via plugin			
Series 60									via plugin			
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			•									•

System Requirements	Sophos	Sophos	Sophos	McAfee	McAfee	McAfee	Trend Micro	Trend Micro	Trend Micro	Bitdefender	Bitdefender	Bitdefender
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.x			•							•	•	•
ESX 4.x			•				•	•	•	•	•	•
Other supported OS			FreeBSD, OpenBSD, TurboLinux, AIX, HPUX, Solaris, OpenVMS, Netware, SCO, Ubuntu, NetApp DataONTAP, vSphere 4.0m Hyper-V 2008									Solaris 10
Database												
Does the product require a database	•						•			•		
For how many users/clients is the free database recommended							20000			1000		

System Requirements	Sophos	Sophos	Sophos	McAfee	McAfee	McAfee	Trend Micro	Trend Micro	Trend Micro	Bitdefender	Bitdefender	Bitdefender
Which database is included (i.e. Microsoft SQL, Sybase, MySQL, etc)	MSDE SQL						DB2			Microsoft SQL Express included free of charge (can support SQL Server, if the customer has a license for the database)		
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			SQL Express 2005 and 2008							SQL Express		
Email Server												
Microsoft Exchange	●					●	●			●	●	●
Domino	●					●	●					
Tobit							●					
Linux	●						●					
Mac							●					
Novell Netware Server							●					
Dell NAS							●					
Kerio							●					

Copyright and Disclaimer

This publication is Copyright © 2010 by AV-Comparatives e.V. ®. Any use of the results, etc., in whole or in part, is ONLY permitted with the explicit written approval of the Management Board of AV-Comparatives e.V., prior to their publication. AV-Comparatives e.V. and its appointed representatives carrying out the tests cannot be held liable for any damage or loss which might occur as a result of, or in connection with, the use of the information provided in this document. We have taken every possible care to ensure the correctness of the basic data, but no liability can be taken for the correctness of the test results by any representative of AV-Comparatives e.V. We do not give any guarantee for the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian non-profit organization.

AV-Comparatives e.V. (October 2010)