



Small Office Administration Console

**For Endpoint Protection (Plus) and
Endpoint Protection Suite (Plus)**

Administrator's Guide

This guide has been written to assist system administrators or anyone who uses the avast! Small Office Administration Console to manage their network. The information contained in this guide is divided into the following key areas:

- 1. General Information 4
- 2. System Requirements 5
 - Small Office Administration Console:..... 5
 - Centrally managed "client" products: 6
- 3. Installation 9
- 4. Administration Console Setup 22
 - Systems overview 27
 - Virus definition status..... 27
 - Statistics 28
 - System messages 28
- 5. Network Screen 29
 - Group view 29
 - Grid view 31
 - Filtering..... 31
 - Create (Add) a New Computer 34
 - Creating a New Group 35
- 6. Jobs 46
 - Create a new job 46
 - Deployment Jobs (3 types) 48
 - Maintenance Jobs (4 types)..... 51
 - Scanning Jobs 56
 - Running a Job 63
 - Jobs History 64

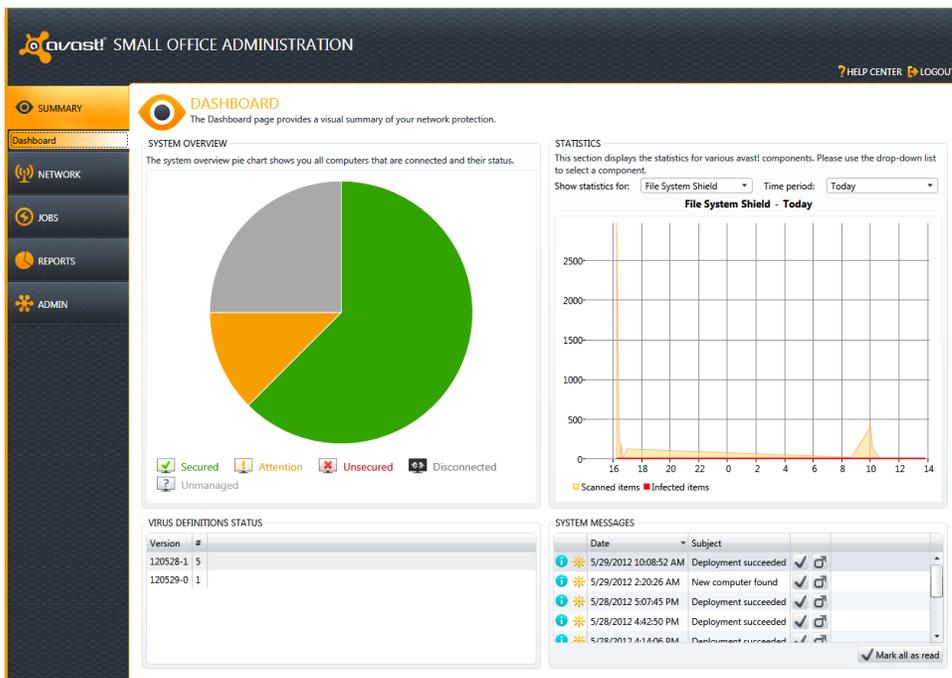
7.	Reports.....	65
	System Messages Log.....	67
	Shield Log.....	68
	Scan Log.....	69
	Report archive.....	70
8.	Administration.....	71
9.	Important Files.....	80

1. General Information

The Small Office Administration Console provides central management capability for your installation of avast! Endpoint Protection or avast! Endpoint Protection Plus and is designed to make the administration of your computer network as simple as possible. As well as providing protection for all the computers on your network, the Small Office Administration Console allows you to install avast! antivirus on all your computers remotely, enabling you to:

- Centrally manage updates
- Create and schedule scans to be run on selected computers
- Receive real-time security alerts
- Create reports
- Receive automatic notifications whenever a new computer is connected to the network

The Small Office Administration Console is a web-based management console designed primarily for small networks of up to 200 workstations. It's a simple and easy to use program to help you both deploy and manage avast! antivirus on your network and so keep your network free of viruses and other malware. It does not require a server Operating System and, once installed, you can access it from any computer with an internet connection.



2. System Requirements

Small Office Administration Console:

- Microsoft Windows XP (any edition except Home Edition) with latest Service Pack 3, 32-bit only
Windows Vista (any edition, excluding Starter Edition and Home Edition) with latest Service Pack, 32-bit or 64-bit
Windows 7 (any edition except Starter Edition and Home Edition) with latest Service Pack, 32-bit or 64-bit
Windows Server 2003 (all editions with latest Service Pack), 32-bit or 64-bit
Windows Server 2003 R2 (all editions with latest Service Pack), 32-bit or 64-bit
Windows Server 2008 (all editions with latest Service Pack, excluding Server Core), 32-bit or 64-bit
Windows SBS 2011.
- 1 GB RAM or above, depending on requirements of operating system and other 3rd party software installed
- A minimum of 900 MB free hard disk space for the initial installation
- Internet connection (to download and register the product, for automatic updates of the Mirror)
- Valid SMTP Server within reach of the server
- Windows workgroup or active directory network
- Internet connection with Silverlight 5 enabled browser e.g. Internet Explorer 7 or above.

Centrally managed “client” products:

avast! Endpoint Protection/Suite (for Workstations)

- Windows 2000 Professional Service Pack 4, Windows XP Service Pack 2 or higher (any edition, 32 or 64 bit)/Windows Vista (any edition, 32 or 64 bit)/Windows 7 (32/64 bit)
- 256 MB RAM
- 300 MB free hard disk space

Older Windows operating systems (Windows 95/98/ME/NT) are not supported.

avast! Endpoint Protection Plus/Suite Plus (for Workstations)

- Windows XP Service Pack 2 or higher (any edition, 32 or 64 bit)/Windows Vista (any edition, 32 or 64 bit)/Windows 7 (32/64 bit)
- 256 MB RAM
- 380 MB free hard disk space

Older Windows operating systems (Windows 95/98/ME/NT/2000) are not supported.

**avast! Endpoint Protection Suite/Suite Plus
(for Server operating systems)**

- Windows Server 2003 (x32bit/64 bit), Windows Server 2008/R2 (any edition, excluding Core Installation), Windows SBS 2011
- 256 MB RAM (512MB if running Windows server 2008)
- 200 MB of free hard disk space

Microsoft Sharepoint

- MSP 2003
- MSP 2007
- MSP 2010

Microsoft Exchange

- MSE 2003
- MSE 2007
- MSE 2010

Windows OS vs SQL compatibility

- www.microsoft.com
- <http://technet.microsoft.com> - The TechNet Library contains technical documentation for IT professionals using Microsoft products, tools, and technologies.

SQL full versions vs SQL Free/Express versions

- <http://technet.microsoft.com> - The TechNet Library contains technical documentation for IT professionals using Microsoft products, tools, and technologies.
- <http://msdn.microsoft.com> - MSDN Library, an essential source of information for developers using Microsoft® tools, products, technologies and services. The MSDN Library includes how-to and reference documentation, sample code, technical articles, and more.

3. Installation

Before you start installing the product, you should think about how you'll be deploying it. The following things need to be carefully considered:

Administration Console

- On which machine will you deploy the Console?
- Is it going to be a dedicated machine? If not, what else will run on the machine?
- Will other software interfere with the Console?
- Will there be enough resources left for the Console to work properly?
- Will you use just one Console, or would it be better to use more than one?

Note: Make sure that you are aware of the minimum system requirements

SQL

During the installation, an embedded SQL Server Compact 4.0 database is installed by default, however you can optionally select to use another database. In the expert installation, you can choose to use a MS SQL database, but note that only MS SQL 2008 R2 is supported, either the Full or the Express version.

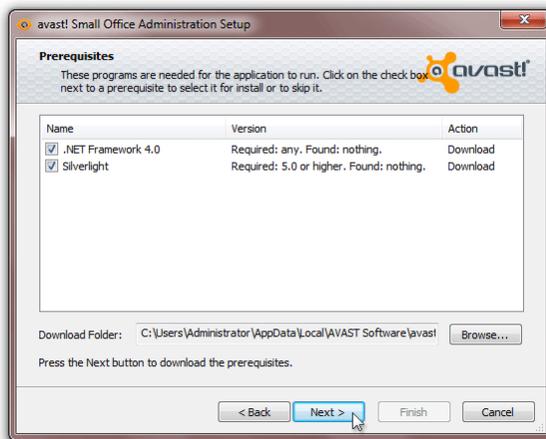
- Is DHCP used on the network? Can the Console have a fixed IP address? (It should)
- Is a full MS SQL 2008 R2 database going to be used, Express version 2008 R2, or the default embedded SQL Server Compact 4.0 database? If you choose Compact/Express, will it handle all your management data? (Express/Compact should only be used on networks of several hundred computers or fewer).

Note: Make sure that you are aware of all limitations of SQL Express and the SQL Server Compact 4.0 versions!

The installation begins with the automatic detection of whether all prerequisites are installed. Simply follow the installation wizard which will also help you to find and install any prerequisites which are missing.



Just click "Next" to proceed and you will then see a list of the pre-requisites which need to be satisfied before the program can be installed.

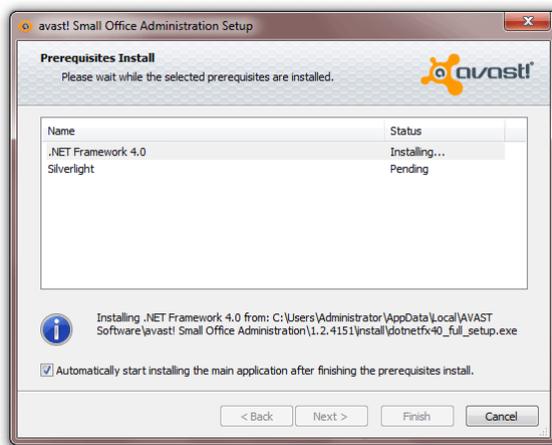


Note: Silverlight can be installed separately after successful installation of the avast! Administration Console.

Prior to installing the Administration console all prerequisites have to be met:

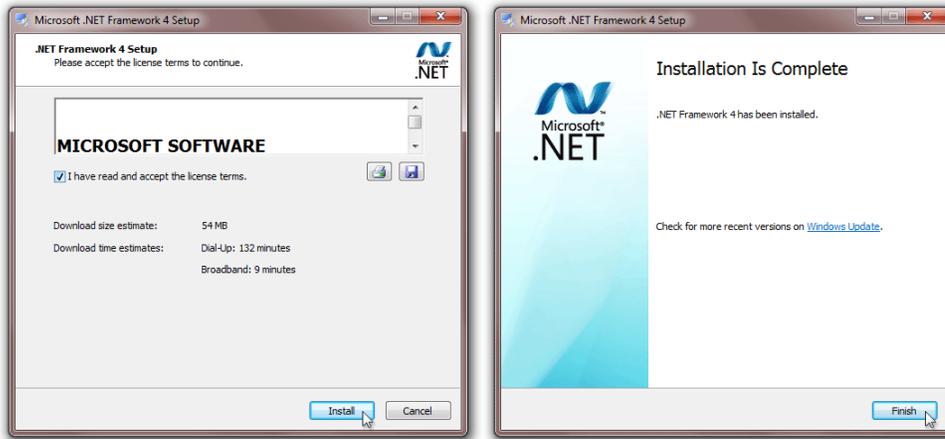
- Windows Installer – if the package cannot be downloaded automatically see www.microsoft.com
- .NET Framework – if the package cannot be downloaded automatically see www.microsoft.com
- Silverlight – can be installed separately, after the successful avast! Administration console installation

All prerequisites should be automatically downloaded and installed (an Internet connection is required)



If the download does not start automatically, visit www.microsoft.com to download the necessary prerequisites.

You may be asked to confirm the installation of the individual prerequisites, for example .NET Framework:



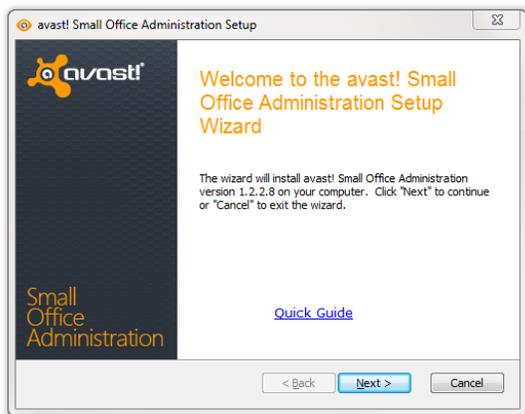
And Silverlight:



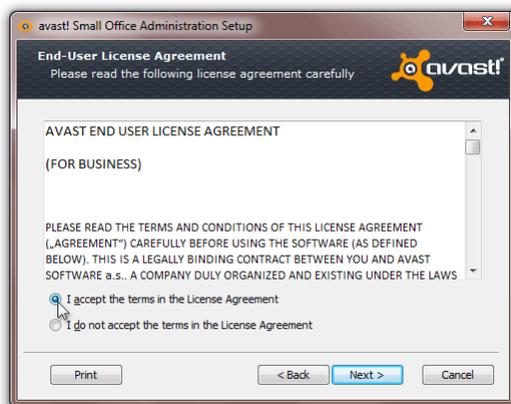
If you are prompted to re-start your computer, click "Restart Now" to prevent the installation from being terminated unexpectedly.



When the machine is restarted, the **avast! Small Office Administration Setup Wizard** will start automatically:



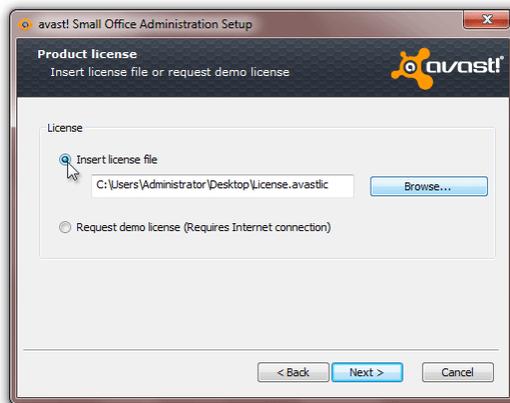
You now need to confirm that you have read and accept the terms of the license agreement by clicking the appropriate button and then click "Next" to proceed.



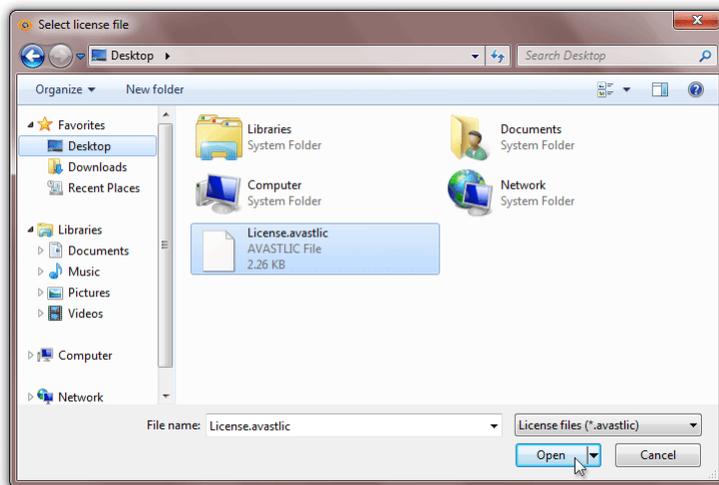
You will now be invited to insert a valid license file. Unless you want to use the program first in demo mode, it is recommended to provide a license file immediately.

Alternatively, you can request a demo license, which will allow you to use the program in demo mode for 30 days. To request a demo license, you will need to be connected to the internet as the demo license will be automatically downloaded from the avast server during the installation.

During the 30 day demo period you will need to purchase and insert a valid license file to continue to use the product, otherwise the avast! Small Office Administration Console will not be able to communicate with any connected machines and you will not be able to deploy the avast! Managed Client onto your network after the demo period expires.

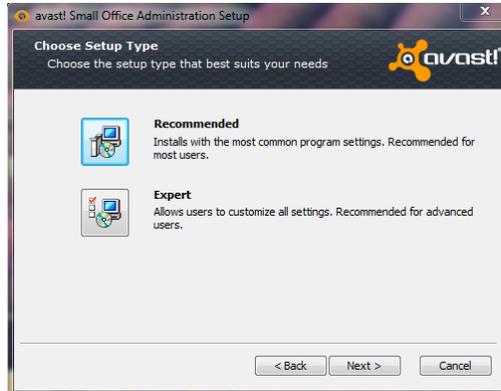


In order to insert a license now, the license must first have been saved on your computer. To locate your license on your computer, click the “Browse” button, then click “Open” and the path to our license will be inserted automatically.

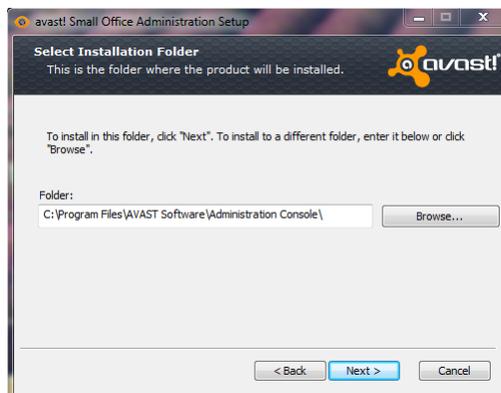


After the installation is completed, you can continue to use the product for **12, 24, or 36 months** from the date of purchase, depending on the purchased license period.

You can now select the type of installation. The recommended installation type is “Recommended” unless you are an experienced system administrator and want to e.g. specify a folder other than the default folder for storing the installation files or use your own MS SQL Database.



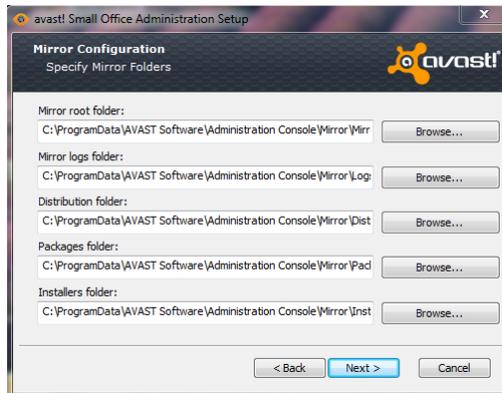
The following screens show all the steps if you select “Expert” installation.



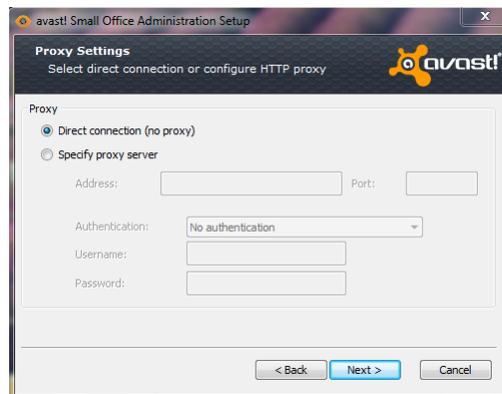
To install the program in the default folder, just click “Next”

To install in a different folder, enter the required path or click “Browse” to select the custom location. By default the recommended destination drive is C:\.

To install the avast! Mirror in the default folder, just click "Next". To install it in a different folder, enter the required path or click "Browse" to select the custom location.



You can set up a proxy for connecting to the internet. This will allow the administration console mirror to download virus definition updates.



If you connect directly to the internet (i.e. not through a proxy), select "Direct connection (no proxy)".
Note: dial-up connections do not use a proxy.

If you are not sure whether you use a proxy server, or which proxy server you use, ask your internet provider or network administrator!

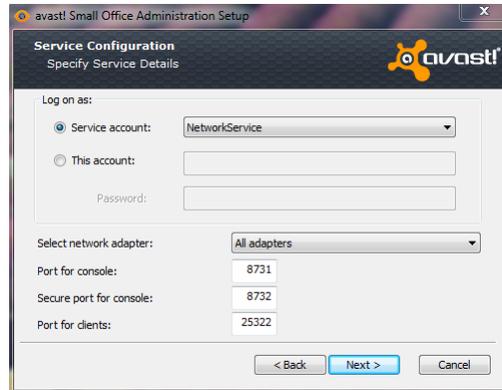
If you connect to the internet through a proxy server and you know the proxy server details, select "Specify proxy server" and enter the proxy details:

- Address - Enter the address of your proxy server
- Port - Enter the port your proxy server uses

Authentication type – specify whether the proxy server requires authentication and if so, the type of authentication. A username and password must be entered if required for authentication.

You will now have the option to use NetworkService or LocalService, or a custom specified account.

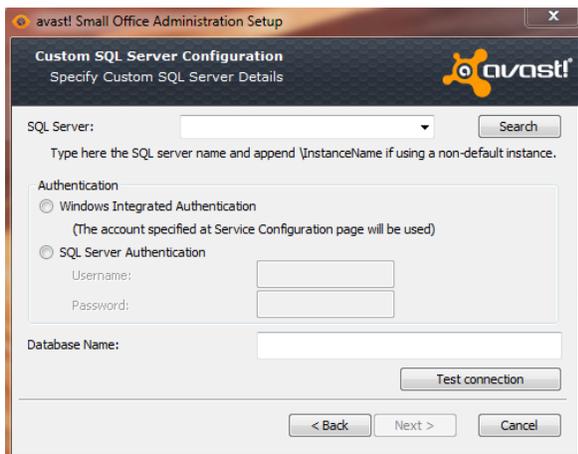
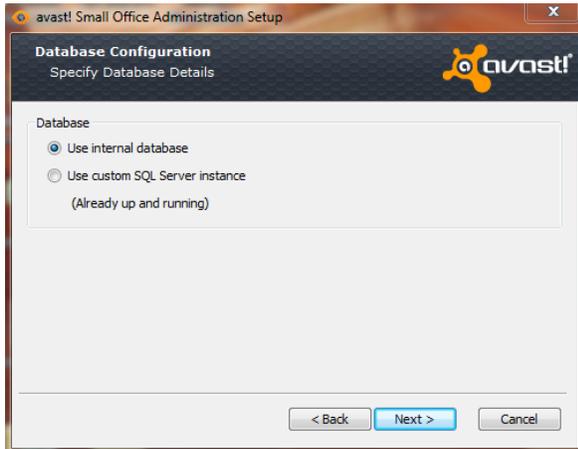
Our recommendation is to choose the Network service account.



Now specify a user/admin account, with sufficient system rights to install/run the avast! Administration console and its components. Then click „Next“.

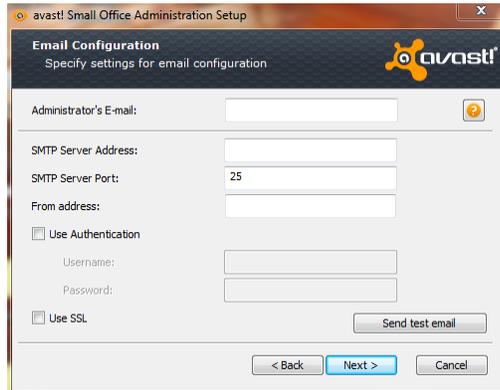
avast! Endpoint Protection – Installation Guide

On the next screen you can choose whether to install the provided internal database, or to use a custom SQL server which is already installed and in use. Note however that only MS SQL 2008 R2 is supported, either the Full or the Express version.



If you selected **Use custom SQL Server Instance** then you'll have to provide its location, credentials and DB name. The DB has to be already up and running. The installer will not create the database for you!

On the next screen, you should enter the SMTP server details.



Administrator's E-mail – this will be used to send the welcome email with the Administration Console login information.

SMTP Server Address - the address of the outgoing email server e.g. smtp.server.com

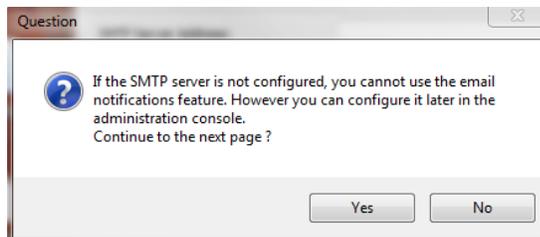
SMTP Server Port - the default is 25

From Address – the address which will be used to send alerts/reports

- **Use Authentication**
 - If the SMTP server requires authentication you must enter the username and password.
- **Use SSL**
 - Don't forget to tick Use SSL if SSL encryption is used

The "**Send test email**" button allows you to send a test email using the details that you entered.

You can proceed without entering these details now, in which case you will see the following message:

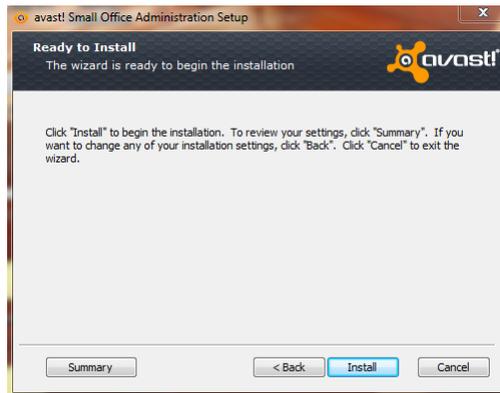


On the next screen you should enter the password you wish to use to log on to the console – note the password must contain alpha-numeric characters:



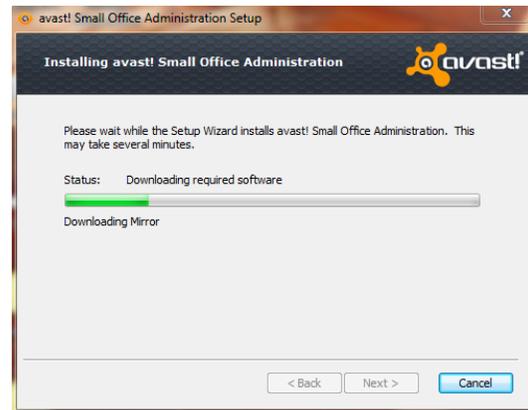
You can also create a desktop shortcut to open the console in your browser

You will now see a final screen before the installation begins. To review all the initial setup details and to check everything is correct, just click on Summary. You can use the “Back” button to go back and make any changes and when you are ready just click “Install”

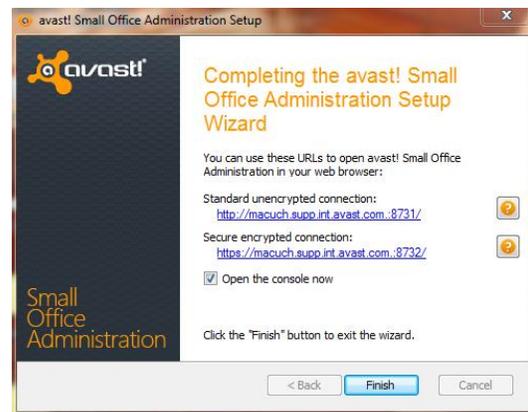


avast! Endpoint Protection – Installation Guide

You will see the progress of the installation as shown opposite.



When the installation is complete, a new box will appear with a link, which you can click to open the Administration Console in your computer's web browser.

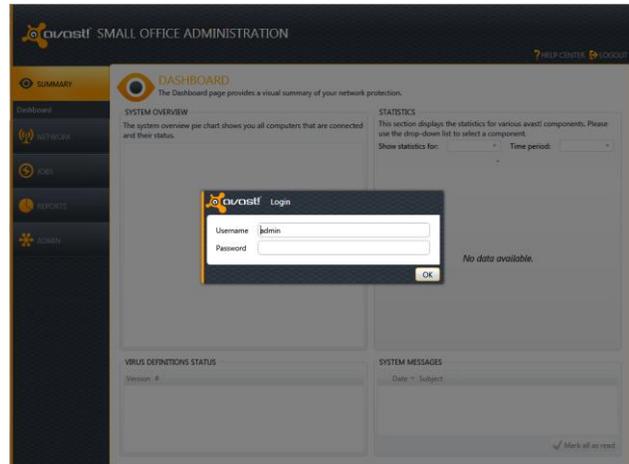


A shortcut will also be installed on your desktop which you can use in future to launch the console on the same computer.

4. Administration Console Setup

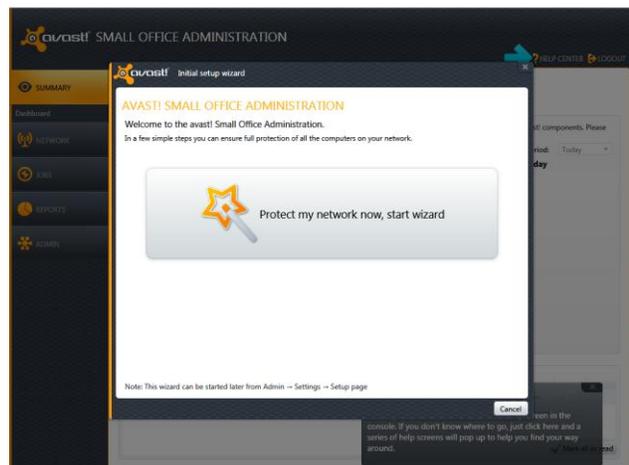
You can open the console via the shortcut installed on your desktop or by clicking the “Start” button in the bottom left corner of your computer screen and selecting “avast Small Office Administration” from the list of programs installed on your computer. You can also access the console from any other computer with an internet connection by simply copying or typing the location into the computer’s web browser.

Then, just enter the user name “Admin” and the password which you provided during the installation process.



When you open the Business Protection Console for the first time, you will first see the system “Dashboard” and the initial setup wizard.

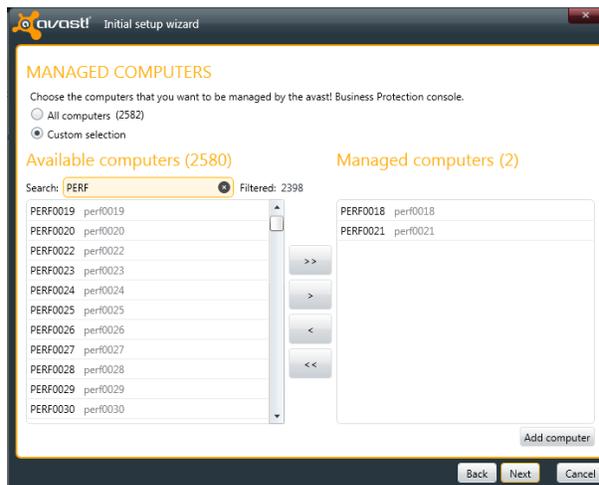
You can access this again later at any time by opening the “Admin” tab and selecting “Setup”. Then just click “Start initial setup wizard”.



The Initial setup wizard will help you to deploy the avast! client on the computers in your network. The wizard works in a network with a windows domain controller, as well as in a network with computers in a workgroup.

Click on “Protect my network now, start wizard” to start the wizard or “Cancel” if you want to deploy the clients manually.

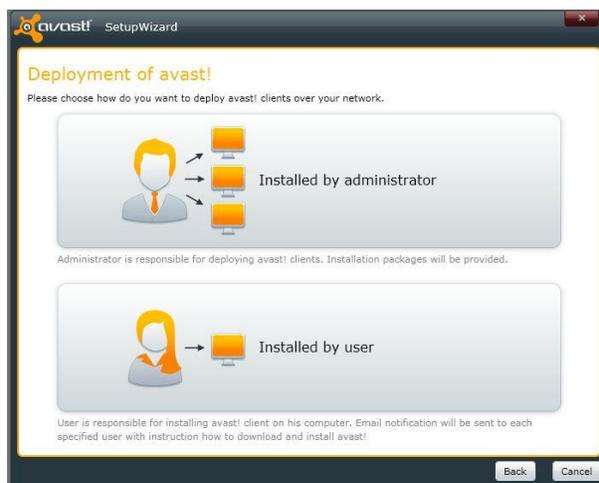
You can now see any computers that have automatically been detected. Select those that you want to be managed by the avast! Administration Console.



Note: If any of your network computers are not listed, they can be added by clicking on “Add computer”. The avast! client will not be deployed on any computers that are not listed on this screen.

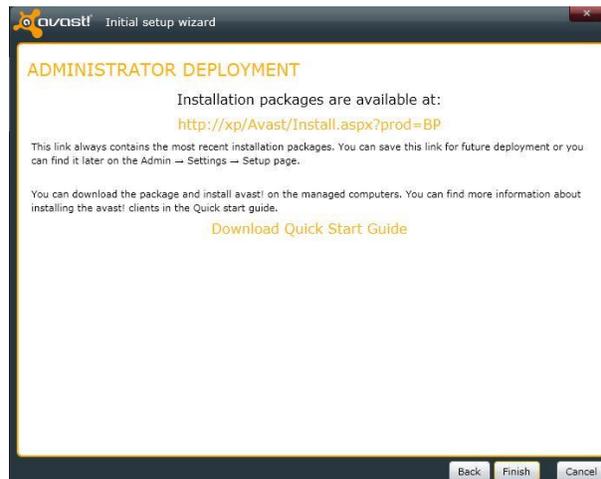
When you click “Next” the next steps will be depend on whether your computers are networked as a workgroup or a domain.

Initial setup wizard for workgroups

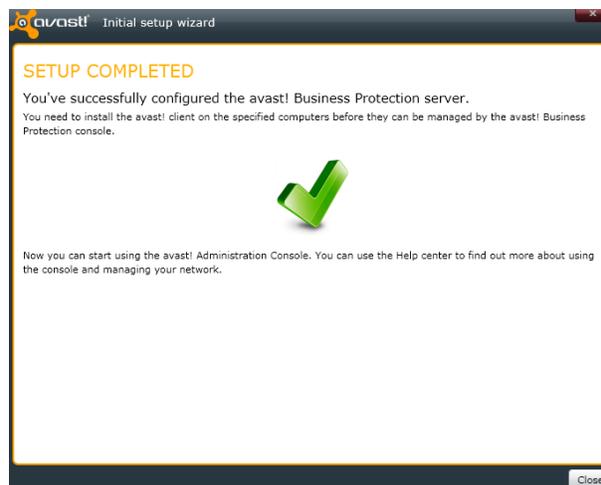


In a workgroup you can choose whether the avast clients will be installed manually on all computers by one person (the administrator) or whether the individual computer users will receive an email with a link to the installation package. In both cases running the installation package will install the avast! client which will then connect to the avast! Administration Console automatically.

If you select the option to have the clients “Installed by administrator” you will see the following screen:



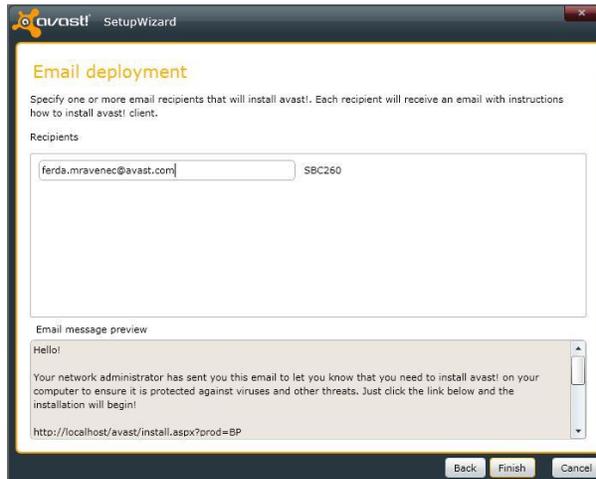
You can download the installation package by clicking on the link.



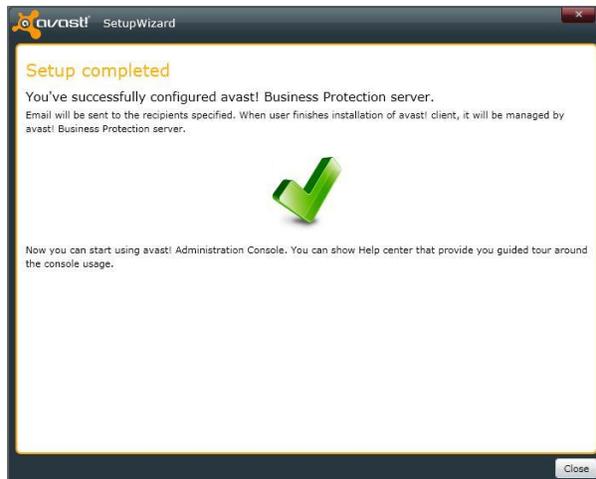
The installation file then needs to be run on each computer in the workgroup to install the client. You can either save the file on an external medium e.g. a flash drive and run it on each computer from there, or download the file on each computer by copying the link into its web browser.

As soon as the avast! client is installed on a networked computer, it will start to communicate immediately with the console.

Alternatively, you can create an email to the individual computer users on the network, which will include a link to the installation package.



Each user will then need to download the installation package and run it on their computer to install the avast! client.



As soon as the avast! client is installed on a networked computer, it will start to communicate immediately with the console.

Initial setup wizard for domains

You need to enter a valid domain administrator username and password.

Example: username: domainname\adminaccount, password: *****

Then click on Finish to proceed with the installation. The deployment of the avast! clients will then start automatically and you will see the following screen confirming that the deployment is in progress:

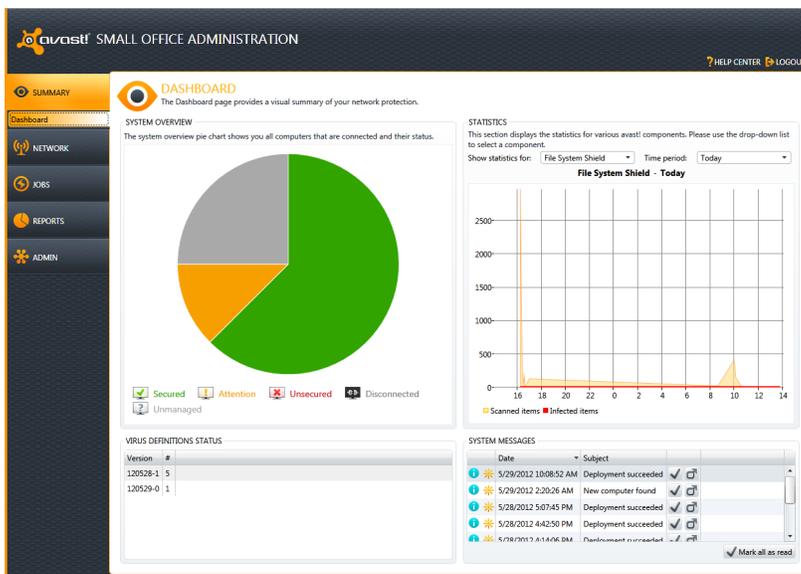
You can check the progress of the installation on the Jobs screen of the Administration Console and once completed, you can see the result on the Job History screen.

Once the initial setup is complete, the main summary page and Dashboard will appear.

The dashboard shows information about the current status of the network and is divided into four main parts:

Systems overview

When you open the Dashboard of the avast! Administration console, in the **Systems Overview** you can see a circular chart, which may be divided into different colored segments representing the current status of all the computers that the Console has detected. Initially, until avast! is deployed on the network, this will be completely grey.

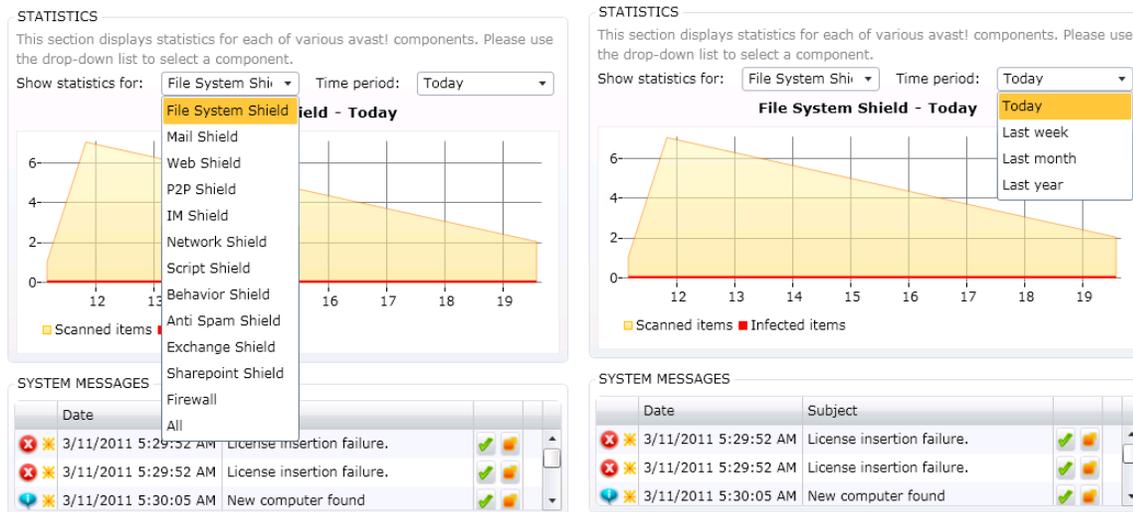


Virus definition status

This information helps you to maintain the maximum possible virus protection, by showing you the virus database version, date and number of computers that have this VPS installed. This will help you to ensure that you always have the most up to date virus definition and that you are protected from the latest threats.

Statistics

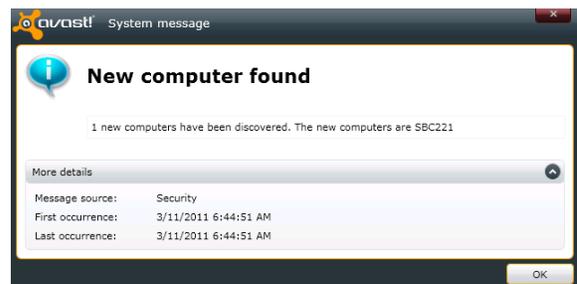
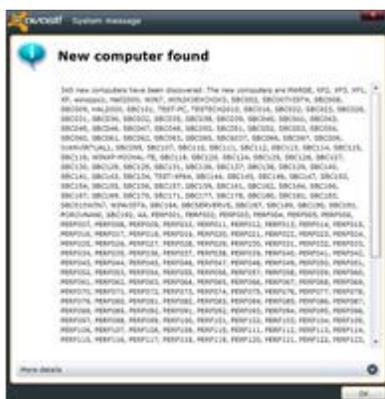
This section displays statistics for each of various avast! components. By clicking on the drop-down menu, you can select the required component. Statistics can be displayed for a single component and a specific period of time. Currently the statistics chart allows you to view the number of scanned items and the number of infected items.



System messages

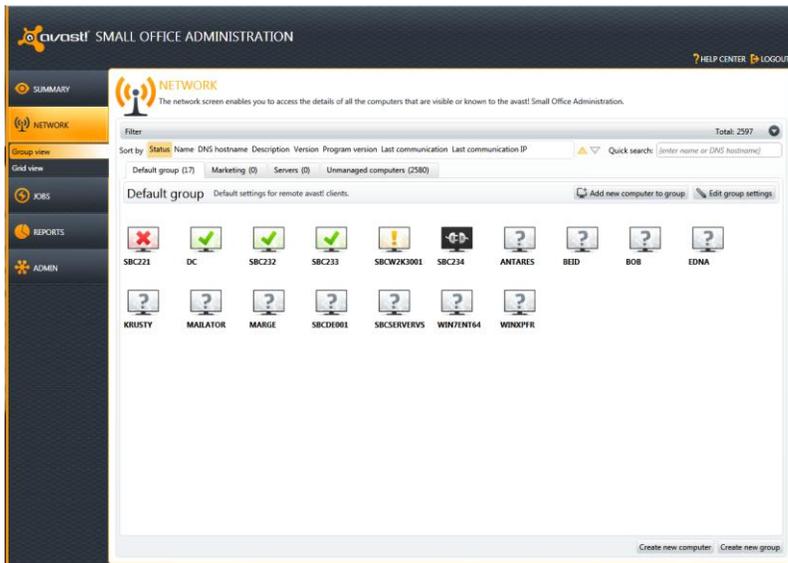
This section shows all important system messages related to the Administration console and clients e.g. Your license will expire soon, License insertion failure, Deployment job failed, New computer found etc..

- If you want to see more details about a specific system message, simply double click on it. See the new detailed information window below.
- If you would like to remove the message from the list, click on the green "tick" icon.
- If you would like to see more detailed information, click on the orange "folder" icon.



5. Network Screen

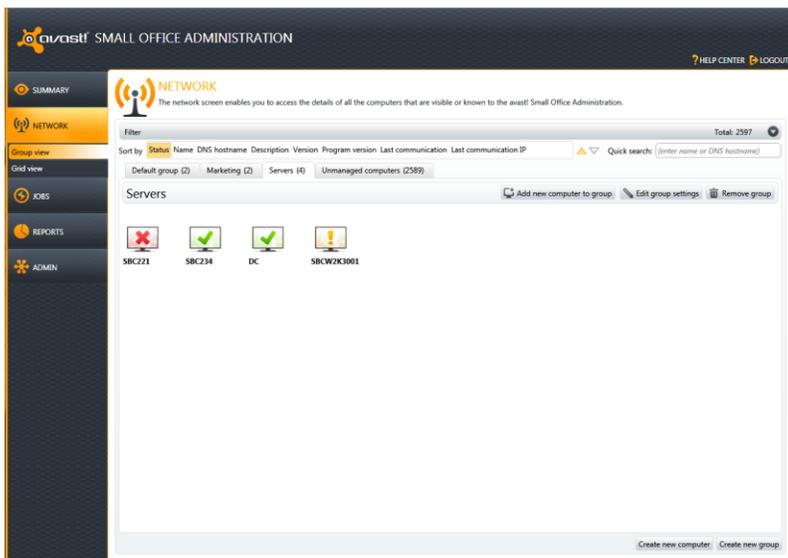
The network screen enables you to access the details of all the computers that are visible or known to the avast! Administration console:



You can select to display the networked computers in either “Group view” or “Grid view”.

Group view

The Group view is a list of all visible computers in a graphic mode (icon view):



Initially, any detected computers will be displayed as grey icons, meaning that they have been detected but have not yet communicated with the console. Connected computers will only be able to communicate with the console after the managed client has been deployed on them.



A green icon means everything is up to date and running as it should be.



A yellow icon means you are not fully protected, for example, if the program or your virus definitions are not up to date, or if one or more of your shields is currently turned off.



A red icon indicates you are currently not protected at all, most likely because all of the shields have been turned off.



This icon indicates that the computer has been detected but has never communicated with the Administration console, for example, if the avast client has not been installed.



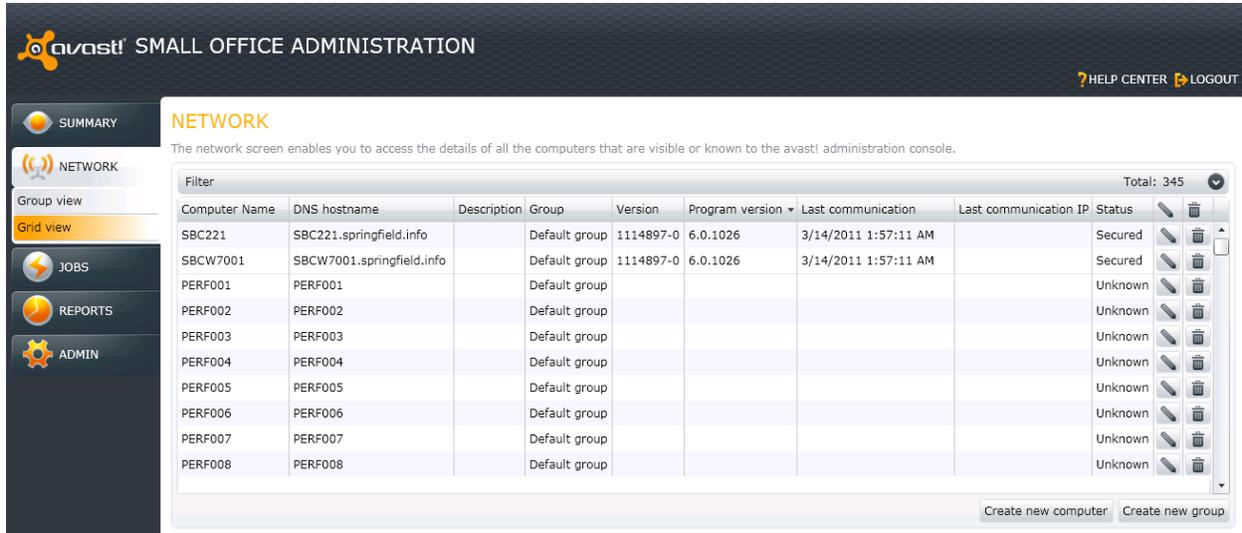
This icon indicates that the computer hasn't communicated with the Administration console recently (the default value is 30 seconds). This doesn't necessarily mean anything bad. e.g. computers that are turned off will have this icon.

All computers that have been discovered automatically are initially allocated to the same default "group". New groups can be created for the purpose of creating special group settings and group jobs. For example, separate groups can be created for servers, or different groups of workstations with different security levels e.g. different combinations of active/inactive shields.

- You can create as many groups as you wish in order to achieve optimal organization
- There can be no duplicates. Every computer has its fixed position in a specific group
- The security policies are set for each specific Group
- Each Group can have a different set of policies
- To access the Group settings simply click the  icon
- To remove a Group from the list simply click the  icon

Grid view

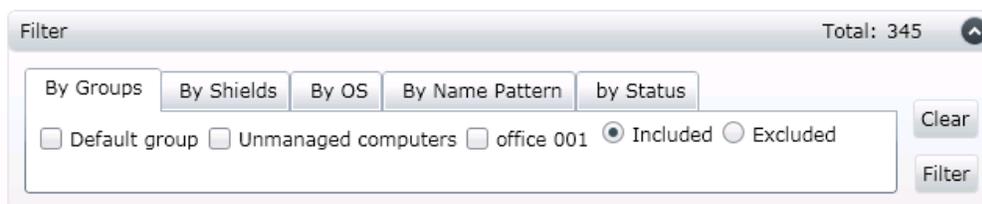
The Grid view is a list of all visible computers in a more detailed text mode



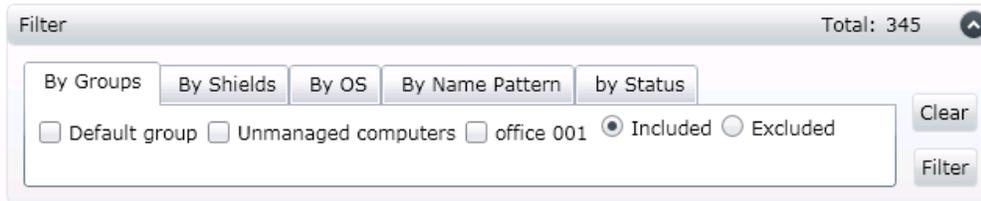
- This allows you to see more detailed information about specific computers, without the need to open the computer information
- The Grid view list contains general information such as Computer name, DNS name, Description, Group in which the computer is located, VPS and program version, Last communication, Status
- To access the computer information click the  icon
- To remove a computer from the list click the  icon

Filtering

Advanced filtering is possible by Groups, Shields, OS, Name pattern and Status.

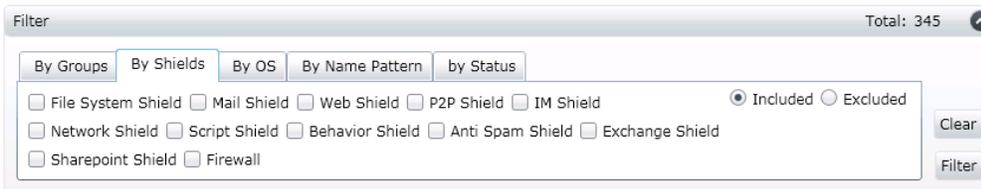


Filtering by Groups



- Contains a list of all default and custom created groups (computer groups)
- Tick or untick required group/s to display your custom Group or Grid view

Filtering by Shields



- Contains a list of all avast! components, such as File system shield, Mail shield, Web shield, P2P shield ..
- Tick or untick the required component to display/filter your custom Group or Grid view.

Filtering by Operating System



- Contains a list of all found OS's installed on all computers visible to the avast! Administration console
- Tick or untick the required OS to display/filter your custom Group or Grid view

Filtering by Name Pattern

The screenshot shows a 'Filter' window with a total count of 345. It features five tabs: 'By Groups', 'By Shields', 'By OS', 'By Name Pattern', and 'by Status'. The 'By Name Pattern' tab is selected. Below the tabs is a text input field labeled 'Pattern' and a checkbox for 'Match case'. To the right of the input field are 'Clear' and 'Filter' buttons.

- Insert the full or partial computer name of the computer as stored in the Group to display/filter your custom Group or Grid view

Filtering by Status

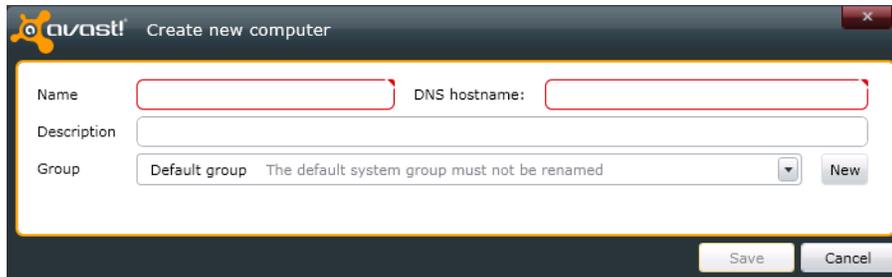
The screenshot shows the same 'Filter' window with a total count of 345. The 'by Status' tab is selected. Below the tabs are four checkboxes: 'Secured', 'Attention', 'Unsecured', and 'Unknown'. To the right of these checkboxes are two radio buttons: 'Included' (which is selected) and 'Excluded'. To the far right are 'Clear' and 'Filter' buttons.

- Contains a list of the statuses of all computers visible to the avast! Administration console, such as Secured, Attention, Unsecured, Unknown.
- Tick or untick the required status to display/filter your custom Group or Grid view

Create (Add) a New Computer

In some cases, you may not be able to use the Discovery Task (perhaps because your network doesn't run ActiveDirectory or the computer browser does not work).

In that case you can create a computer manually via the "Create new computer" feature:



The screenshot shows a dialog box titled "Create new computer" with the Avast! logo. It contains the following fields and controls:

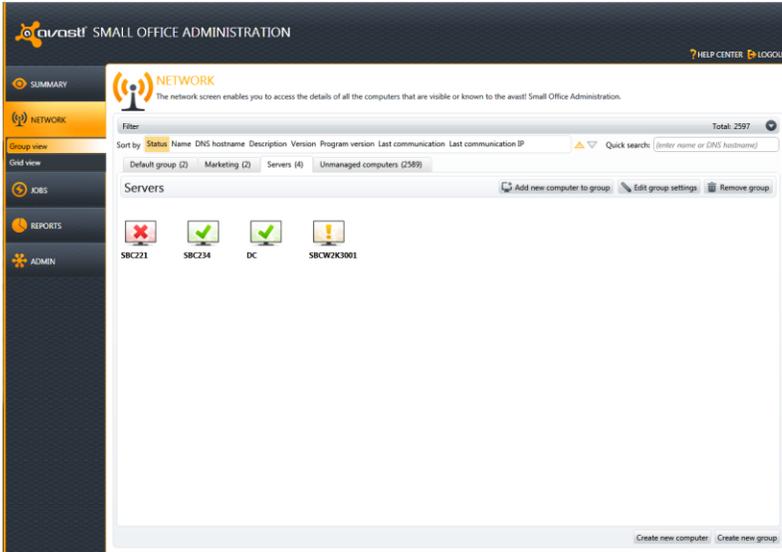
- Name:** A text input field with a red dashed box around it.
- DNS hostname:** A text input field with a red dashed box around it.
- Description:** A text input field.
- Group:** A dropdown menu showing "Default group" with a "New" button to its right. Below the dropdown is the text "The default system group must not be renamed".
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

You can create a computer by inserting the required basic information:

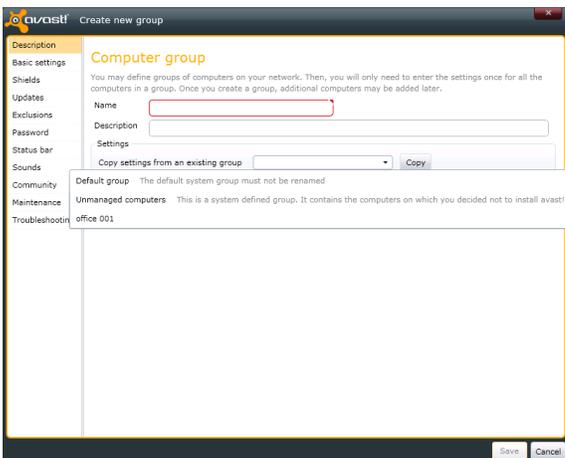
- Computer name
- DNS Hostname
- Description
- Group in which the computer will be located

Creating a New Group

If you want to create a new computer group just click on “Create new group”.



This will open the following new window:

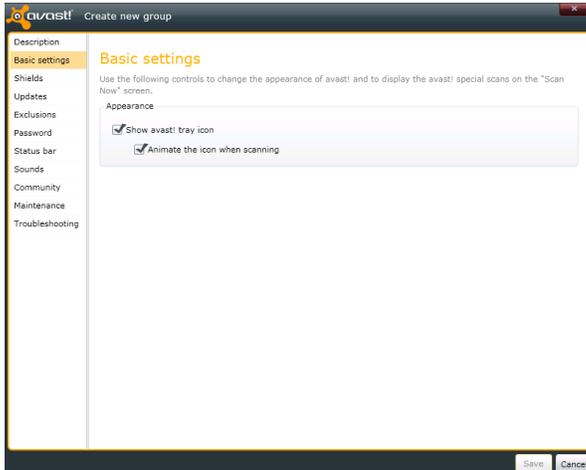


- Enter the name of the new group and a short description.
- You need to enter the settings just once for all computers in the group,
- Or you can copy the settings from an existing computer group.
- Once the computer group is created, additional computers may be added later.

When an avast client is deployed, it will be deployed with all the settings according to the group to which it is allocated in the Administration Console.

Computers can be moved from one group to another and if a computer is moved to a new group, the avast settings for that computer will be updated immediately based on the settings for the new group.

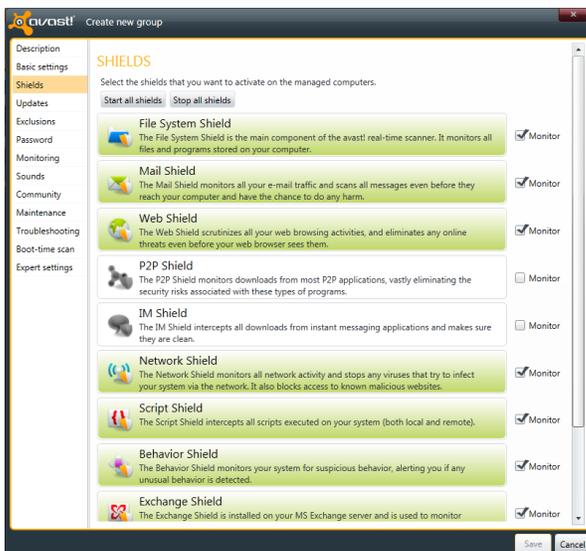
Basic Settings



- Show avast! tray icon - allows the user to interact with avast!
- Animate the icon when scanning - the avast! icon located in the system tray will start rotating whenever a scan is in progress

Shields

Real-time shields - avast! real-time protection is based on so-called shields - special modules protecting various parts of your computer, e.g. file system, e-mail etc.

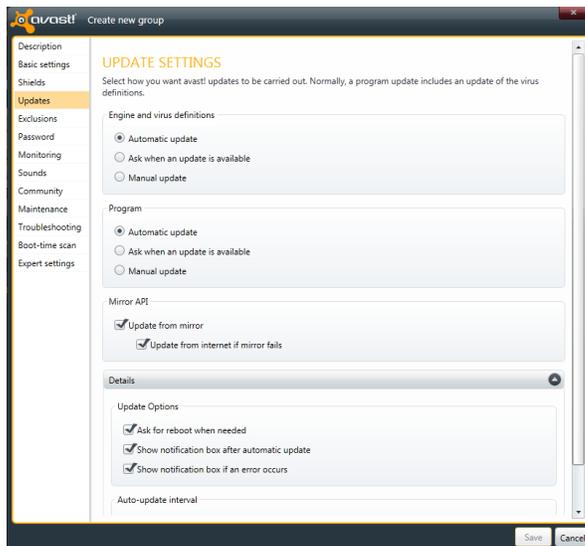


Click the shield/s you want to use or remove - the selected shields will be automatically started on the chosen computers on which the avast! managed client is installed

The Monitor checkbox identifies if the status of this shield should influence the status of this computer

Updates

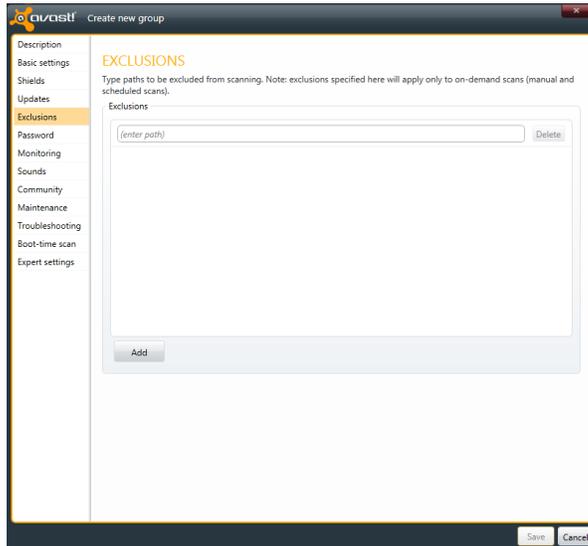
You can choose whether the program and virus definitions are updated automatically or manually, or only on request following notification that an update is available.



By default, updates are applied from the mirror and only from the Internet if the mirror is unreachable.

- Update options
 - Ask for reboot when needed
 - Show notification box after an automatic update - to notify the user of the update
 - Show notification box if an error occurs
- Auto-update interval
 - Default set to 240 minutes

Exclusions



Keep in mind that any exclusions specified here apply to all on-demand scans (manual and scheduled).

- If you want to exclude files only from a specific manual or scheduled scan, use the Exclusions page in the scan settings.
- To exclude files only from being scanned by the real-time shields, use the Exclusions page in the real-time shield expert settings on the client computer.

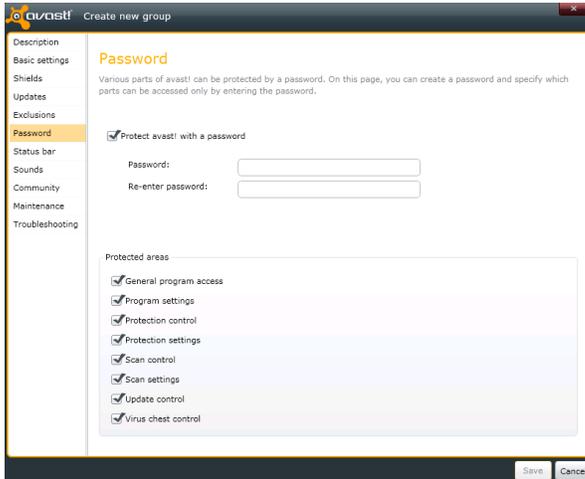
To exclude a location or file, first click the box where it says <enter path> and then type either the location or file to be excluded.

If you want to exclude a folder, including all of its sub-folders, it is necessary to add "*" to the end of the folder name e.g. C:\Windows*.

To remove a location or a file from the exclusions list, click on it once to select it, then click the "delete" button.

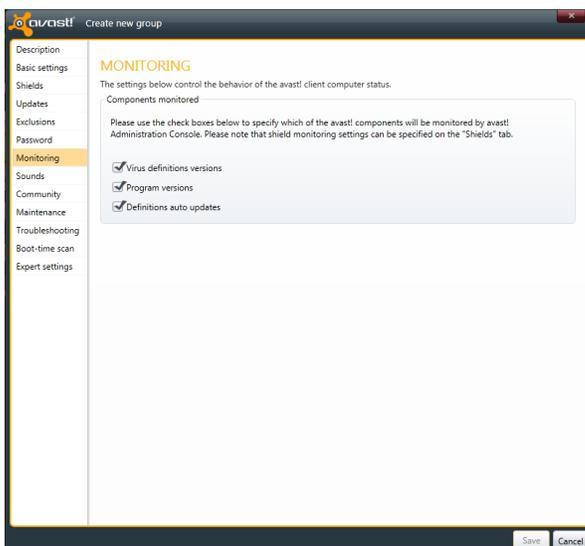
Password

Various parts of avast! can be protected by a password. On this page, you can create a password and specify which parts can only be accessed by entering the password.



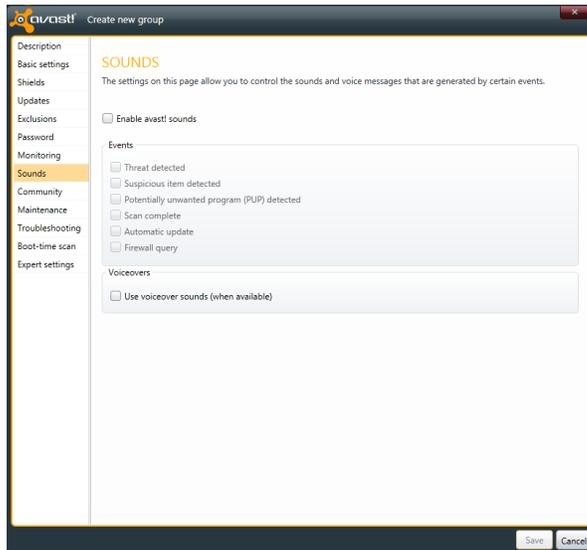
Monitoring

The settings on this screen control the behavior of the avast! status bar which is displayed when the program is opened on the client machine. By checking the various boxes, you can specify which avast components will be monitored and will therefore influence the displayed status, and which will not.



Sounds

The settings on this page allow you to control the sounds and voice messages that are generated by different events.



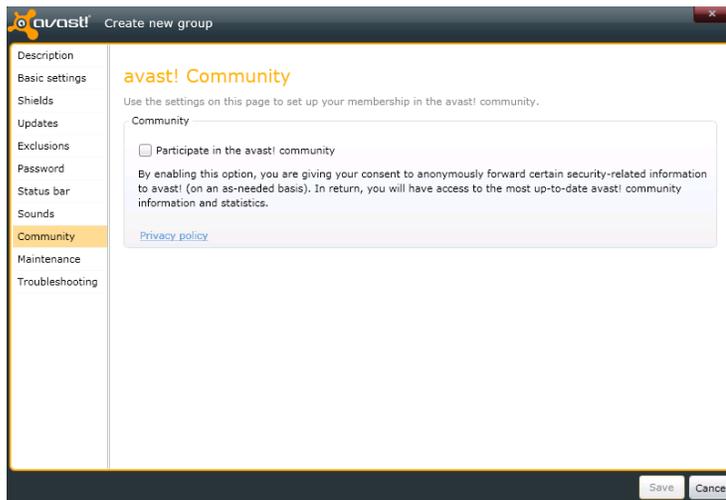
The various events that can trigger an audible sound or voice message are:

- Threat detected
- Suspicious item detected
- Potentially unwanted program (PUP)detected
- Scan complete
- Automatic update
- Firewall query

Community

By checking the box on this page, you can **participate in the avast! community** and share information of a technical nature on a need-to-know basis. This does not concern personal information of any sort and is strictly security-related information concerning, for example, malware that avast! has detected while running on your computer, actions that have been blocked etc.

This information will be used by avast! to improve its detection ability and technical support for the benefit of the whole avast! community.



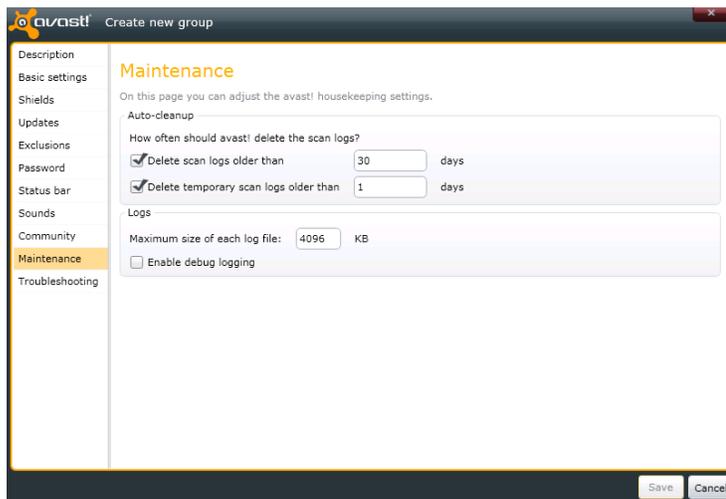
By participating in the avast! community, you will also have access to all the community information and statistics about the latest malware attacks.

Maintenance

On this screen you can specify:

- how long the scan logs are kept before they are deleted
- the maximum size of the scan logs.

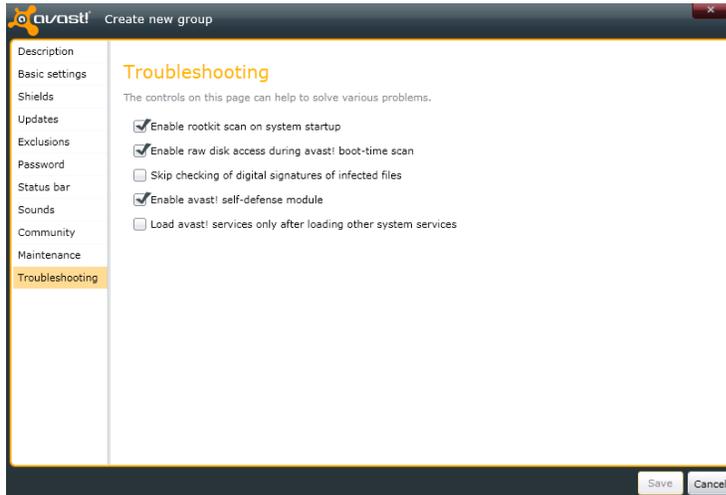
This ensures that the space on your hard-disk is optimized by limiting the size of the logs, and removing logs which are no longer needed.



If the box "**Enable debug logging**" is checked, a special log file will be created if an error occurs while the program is running.

If the error persists, this log can then be sent to avast! technical support and may help to identify the cause of the error.

Troubleshooting



Changing the settings on this page may help to resolve certain specific problems. However, these settings should not be changed without good reason. If in doubt, please contact AVAST Software first.

- Enable rootkit scan on system startup**

Normally avast! scans for rootkits whenever the operating system is restarted. Uncheck this box if you do not want this scan to be carried out automatically.
- Enable raw disk access during avast! boot-time scan**

During a boot-time scan, avast! uses a special method to access the raw data on the hard disk, to check for any viruses that may be hidden there.
- Skip checking of digital signatures of infected files**

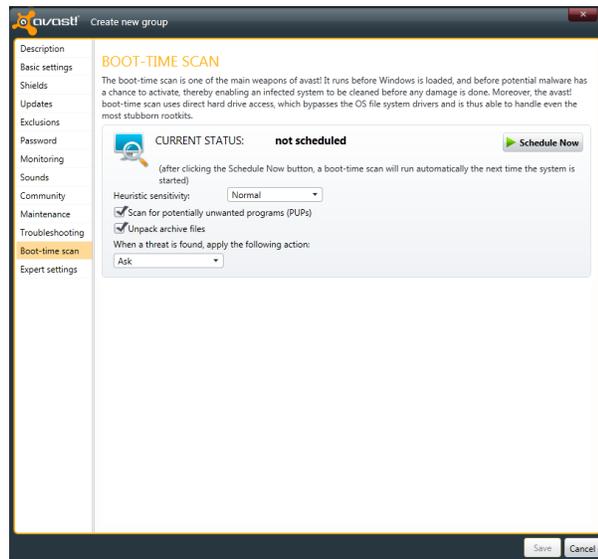
To prevent false positive alerts, avast! checks files for digital signatures. If a file is detected as suspicious, but also contains a valid digital signature of a trusted authority, it is likely to be a false positive. In this case the file will not be reported as suspicious. If this box is checked, all suspicious files will be reported, including those with valid digital signatures.
- Enable avast! self-defense module**

Some viruses deliberately target antivirus software and try to switch it off by deleting or modifying critical files. avast! contains self-defense features that prevent such attacks by blocking the operation.
- Load avast! services only after loading other system services**

The avast! service is normally loaded quite early in the boot process. Sometimes this can cause problems when loading other system services e.g. the system may appear to "freeze" temporarily after starting. Checking this box will delay the loading of avast! services until after the other system services are loaded.

Boot-time scan

It is possible to schedule a scan to be carried out automatically when the system restarts i.e. when it "boots", before the operating system is active. This is useful if you suspect that a virus may have been installed on your computer, as it will enable the virus to be detected before it is activated and before it can do any damage to your computer.



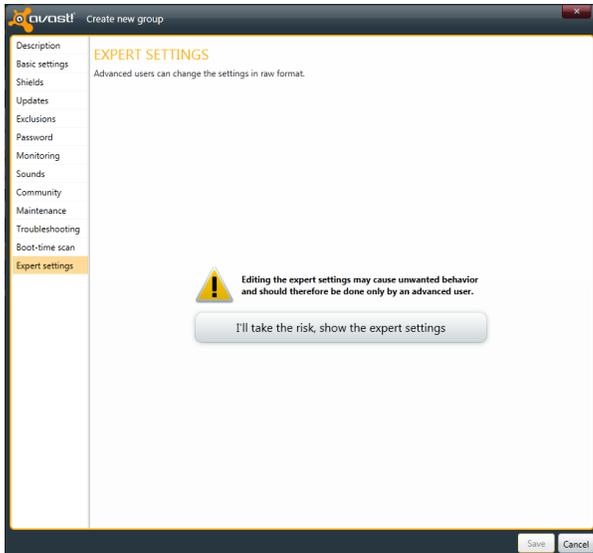
By default, the program automatically scans for potentially unwanted programs and also scans inside archive files, but either of these features can be turned off by unchecking the relevant checkbox.

You can also specify what action should be taken if a threat is detected. avast! can automatically attempt to repair the file, move it to the virus chest, or delete it. Alternatively, you can specify that you should be asked what action to take for each detected threat, or you can specify that no action should be taken.

Finally, click on "Schedule Now" and the scan will start automatically as soon as the system is restarted.

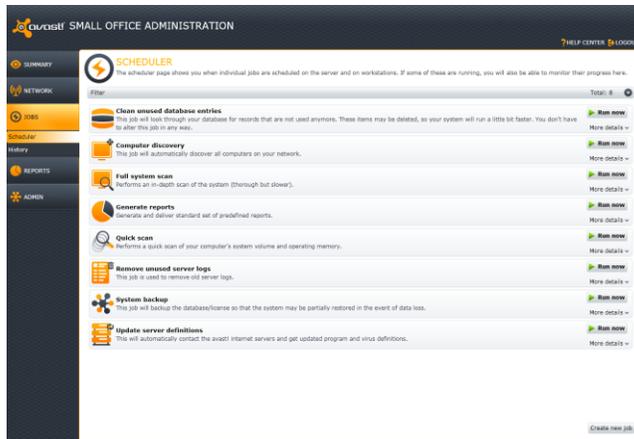
Expert Settings

In the expert settings, you have direct access to the raw data values related to the various settings. As any accidental or erroneous changes could adversely affect the behavior of avast you should only access the expert setting if you are an advanced user and you are used to working directly with the raw data settings.



6. Jobs

After clicking on the Jobs tab, the main scheduler page contains a list of all created jobs on the server and on the individual workstations, with basic information about them (click "More details" button). If any of these jobs are running, you will also be able to monitor their progress here.



Create a new job

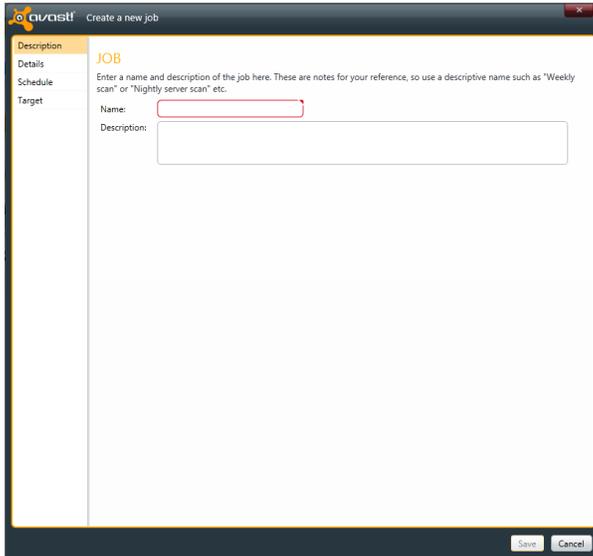
The Console is installed with a number of pre-defined jobs, however, by clicking on the "Create new job" button, you can define a completely new job with its own parameters. Any new job that is created, or any of the pre-defined jobs can be run at any time simply by clicking the "Start" button on the above scheduler screen.

Description

Enter a name and description of the job you are defining here. The description section is just a note to remind you later what the specific job was created for.

Details

On this screen you should select the type of job to be performed. Related jobs are grouped into “families” to make the selection faster.



You can select from the following jobs :

Job Type : Deployment

- Unattended deployment
- Email deployment
- Uninstall avast! protection

Job Type : Reports

- Reports

Job Type : Maintenance

- Definitions update
- System backup
- Database cleanup
- Log cleanup

Job Type : Computer catalog

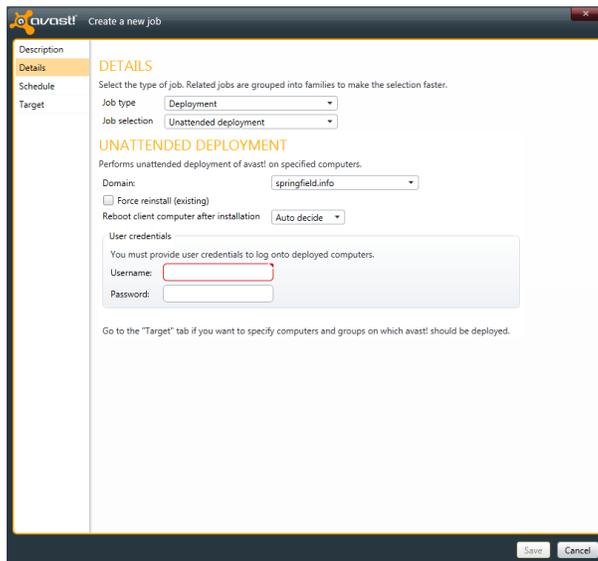
- Discover new computers

Job Type : Scan

- Scan Computer

Deployment Jobs (3 types)

1. to install avast! remotely on your network, select Job type "**Deployment** " and Job selection "**Unattended Deployment**".



Unattended deployment runs silently (without any user intervention). That's why it's important that all the installation options are properly preset.

Force reinstall (existing) - if this box is checked, any current installation of avast! on a client computer will be automatically uninstalled before the new version is installed.

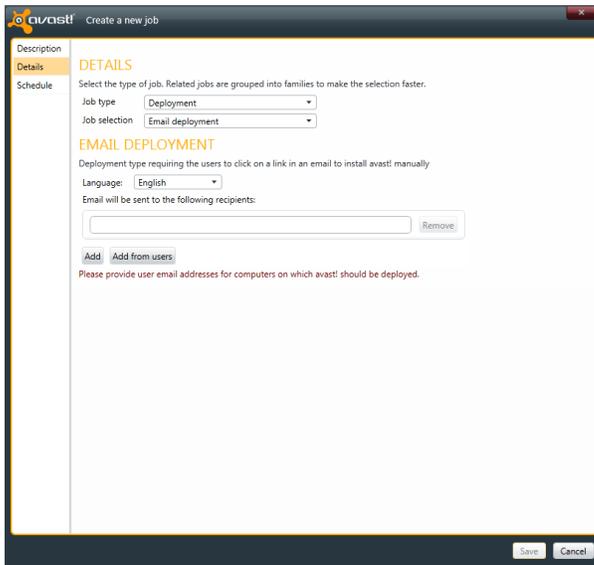
Reboot client computer after installation – if "**Auto-decide**" is selected, each client computer will be automatically restarted only if a reboot is needed to complete the installation, for example in the case of Business Protection, if a previous installation has been replaced or in the case of Business Protection Plus, to complete the installation of the Firewall.

On this screen, you need to specify the user credentials to log on to the target computers

- Username (Usually Administrator with full admin rights)
- Password

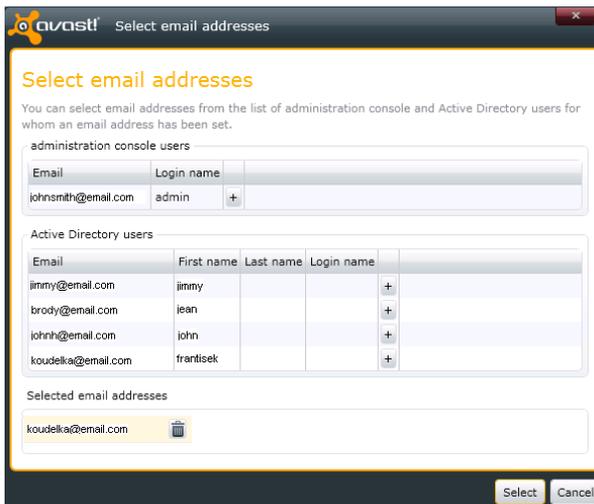
On the "**Schedule**", "**Power Options**" and "**Target**" screens, you can specify a future date and time for the job to be run, any actions that should be carried out before or after running the job, and the actual computers on which the managed avast client should be deployed. These options are described later in the section "**Running a Job**"

- To create a new job to enable users to install avast on their own computers, select Job type “Deployment” and Job Selection “Email Deployment”.

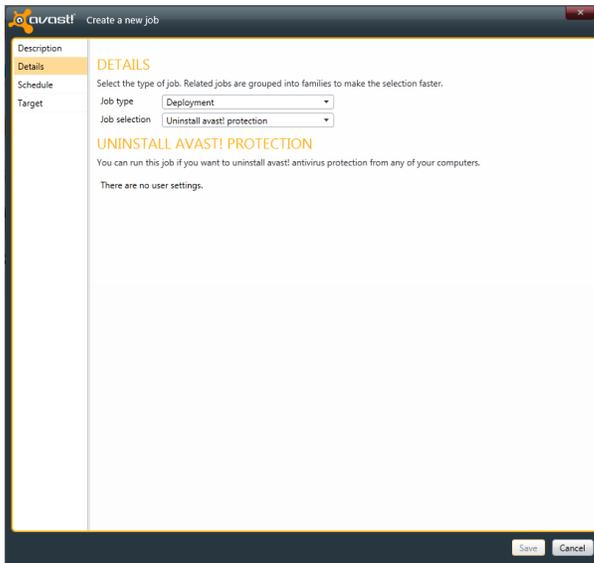


Running this job will result in the user(s) receiving an email with a link which they will need to click to install avast! on their computer manually. Use the language selector to define the language in which the email should be sent.

Email addresses can be inserted manually or by using Active Directory.



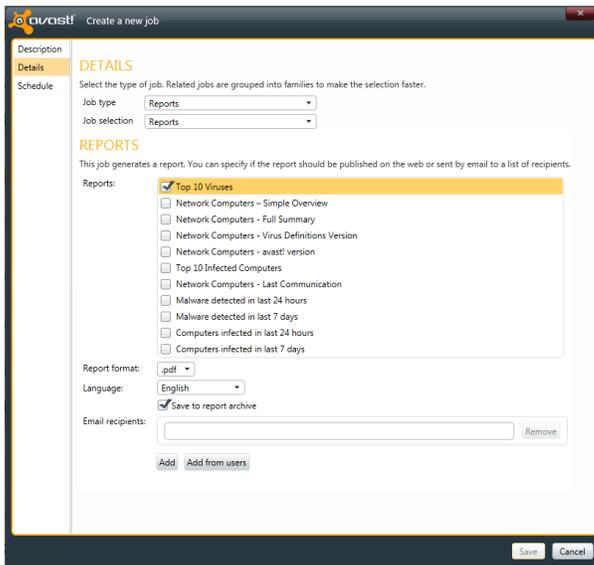
3. If you need to uninstall avast on any or all of the networked computers. select Job type “**Deployment**” and Job selection “**Uninstall avast! protection**”.



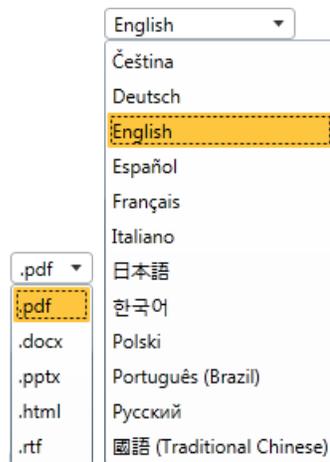
The job can be scheduled to run on all managed computers, or only on some of them. When the job is run, it will uninstall all avast! managed products from the selected computers.

Maintenance Jobs (4 types)

1. Reports.



The Administration Console enables you to create a variety of useful reports, in different formats and languages:

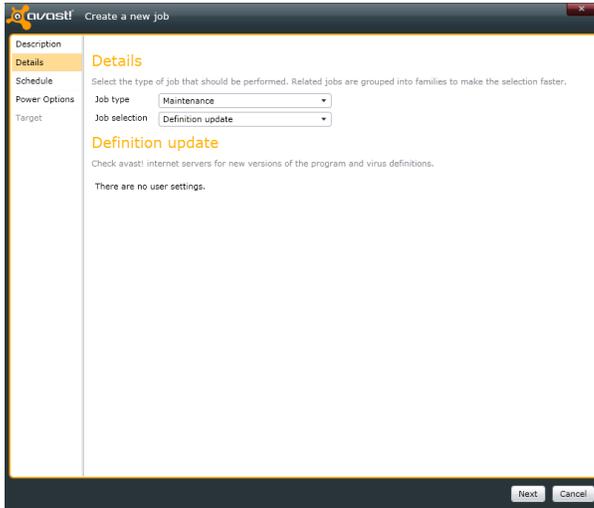


By specifying the recipients' email addresses, you can even have the reports sent to the management team (specific email address) automatically at periodic intervals.

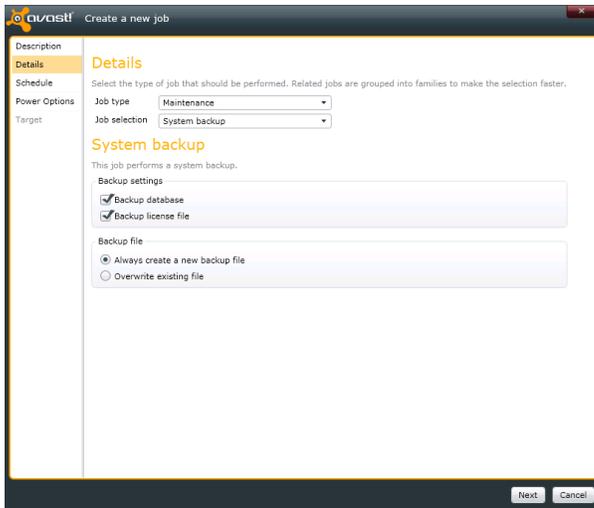
More about reports can be found later in this guide.

2. Definitions Update

It is vital to always keep your security software up-to-date. While avast! is pre-set to update automatically, you can also control the update manually.



3. System Backup



Scheduling regular backups of the whole database is important. You should incorporate a backup of the Administration console database into your overall network backup strategy.

There are two recommended ways:

- a. you can use your backup software to back up the SQL server directly (if the program can do so; consult your backup software documentation for details), or
- b. you can use an Administration console System backup to back up the database.

Backup settings

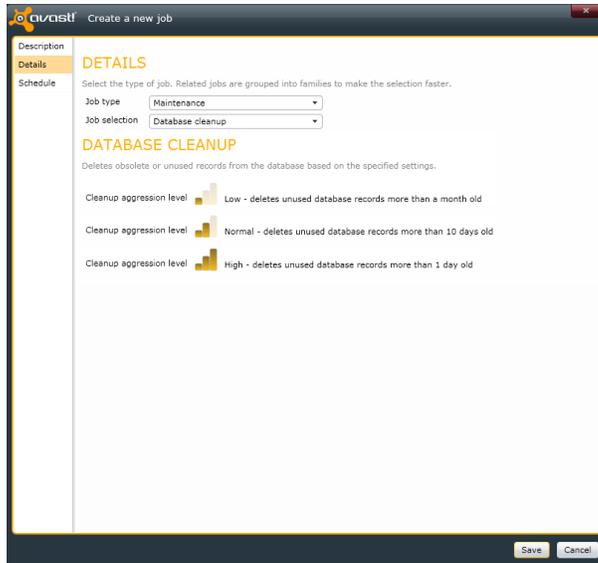
- Backup database
 - Runs DB backup
 - Backup file location - C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Backup
- Backup license file
 - License file is added to the backup

Backup file

- Always create a new backup file
 - Default location is C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Backup
- Overwrite existing file

4. Database Cleanup

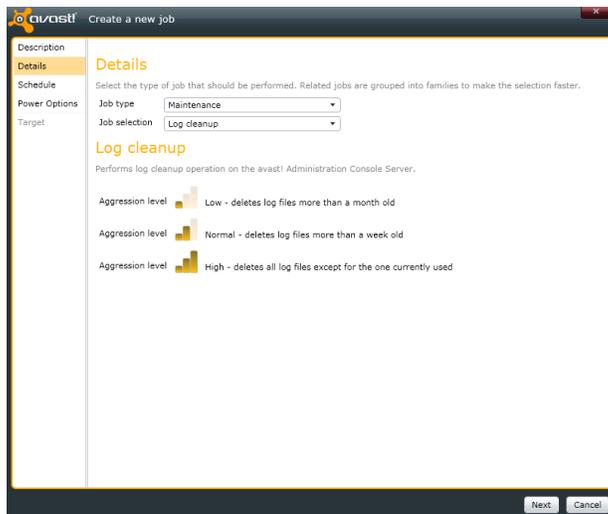
The Database Cleanup job can be used to remove older records from the database.



This helps you to keep the database from growing indefinitely. It also lets you delete “orphaned” records to further reduce the size of the database.

5. Log Cleanup

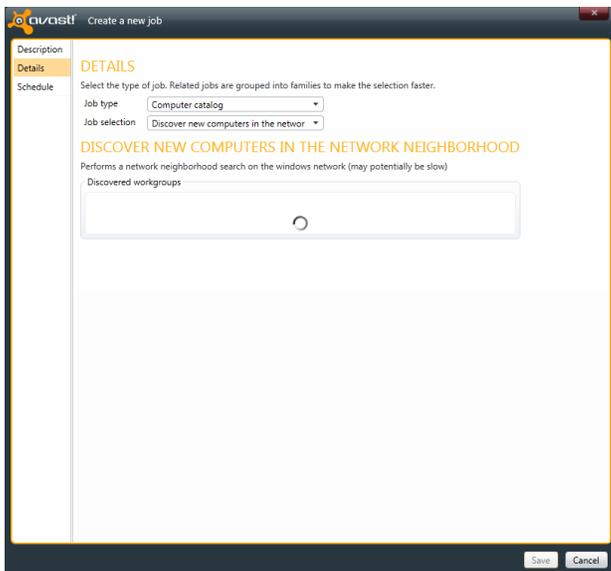
This job can be run to remove old log files.



You can specify the following aggression levels:

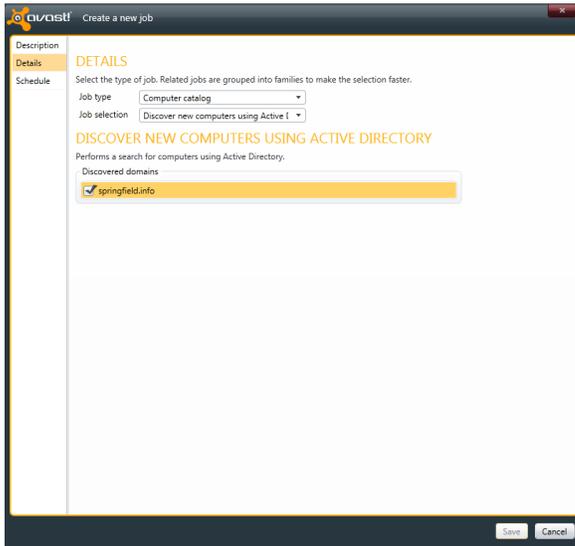
- Low aggression level means only the oldest database records will be deleted. Only records more than a month old will be deleted. Any less than a month old will not be deleted.
- Medium aggression level means more records will be deleted – all records more than 10 days old
- High aggression level means all but the very latest database records will be deleted - all that are more than 1 day old. Computer Catalog Jobs (2 types)

1. Discover new computers in the network neighborhood



This job can be used to discover all new computers where Windows Workgroups are used.

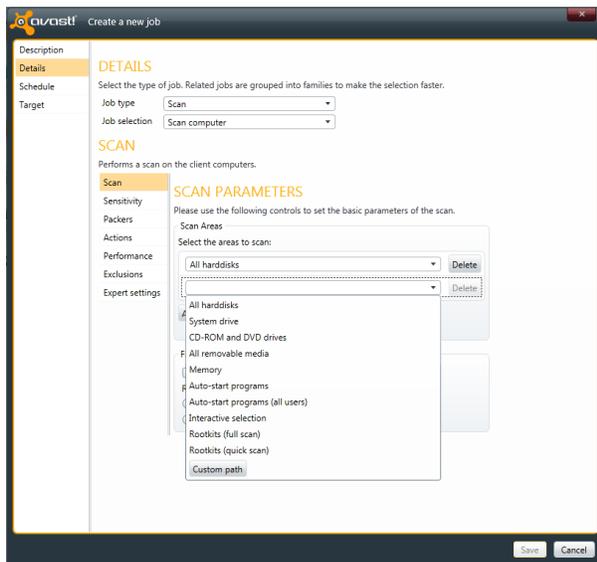
2. Discover new computers using Active Directory



This job can be used to discover all new computers listed in Active Directory.

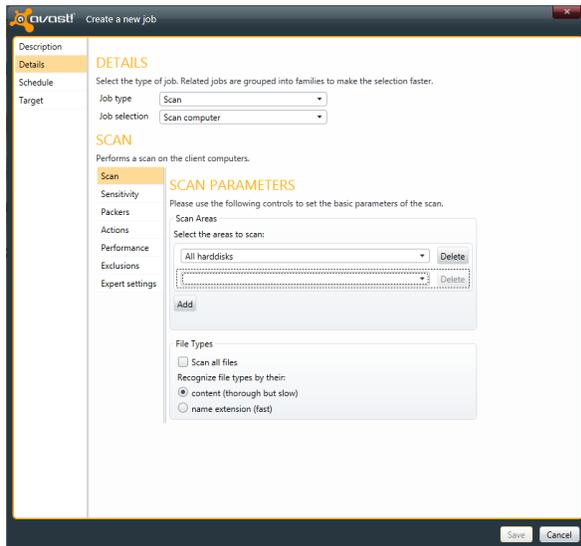
Scanning Jobs

By choosing "Scan computer" you can define a completely new scan with its own scan parameters.



By default, the area to be scanned is set as "All hard-disks". To select a new area to be scanned, just open the drop-down menu and select the additional area to be scanned. To remove an area, click on it once and then click "delete".

If "Interactive selection" is chosen, a new window will open whenever the custom scan is started, in which the actual area to be scanned can be selected/ Once the area is selected, the scan will start.

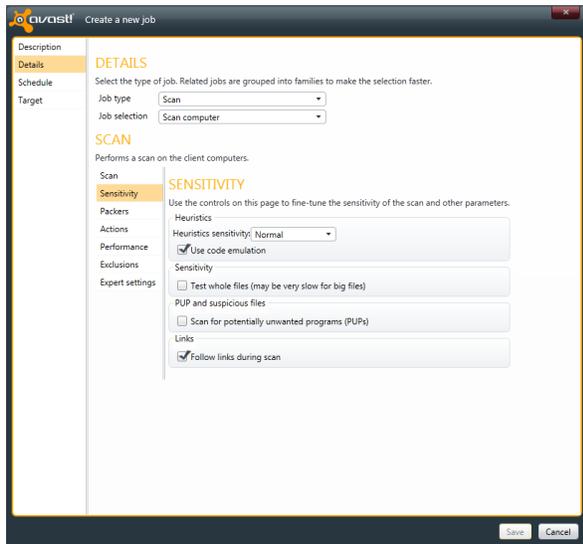


You can also specify how avast! should recognize potentially suspicious files that should be scanned, either by checking the file extension or by checking the actual content.

If "**content**" is selected, avast! will look inside every file to determine what type of file it is and whether it should be scanned.

If "**name extension**" is selected, then by default, only files with extensions such as "exe", "com", "bat" etc. will be scanned. You can add other file extensions by clicking on "select additional areas" and typing the required file extension in the box. Then click OK. To remove a file extension, click on it once and then click "delete".

On the "Sensitivity" screen, you can adjust the basic sensitivity, which determines how thoroughly files are scanned, and also the heuristic sensitivity.



As well as the standard process of scanning for known malware infections, avast! also performs a heuristic analysis to identify potential, but as yet unknown malware. This is done by looking for certain characteristics that may be a sign of a potential infection. By You can adjust the level of heuristics sensitivity to Low, Normal or High, or you can turn it off completely. Increasing the sensitivity increases the chances of detecting a virus but also the likelihood of "false positives".

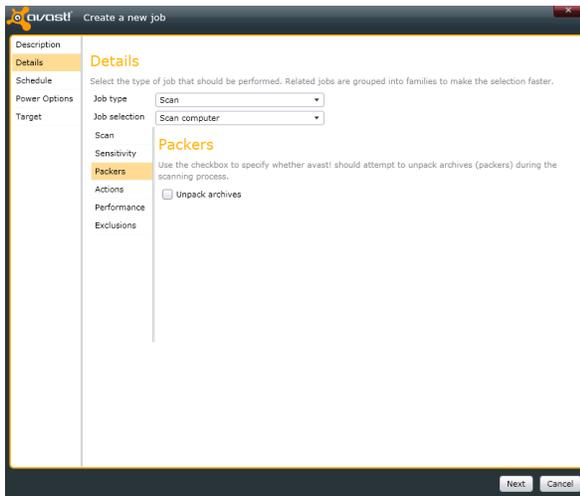
If you find that a large number of clean files are detected by avast! as suspicious ("false positives"), it is possible that the heuristic sensitivity is set too high. Reducing the heuristic sensitivity should result in fewer files being reported as suspicious, however this also reduces the chances of a real virus being detected.

If the box "use code emulation" is checked and avast! detects some suspicious code in a file, it will attempt to run the code in a virtual environment to determine how it behaves. If potential malicious behavior is detected, it will be reported as a virus. Running the code in this virtual environment means that if the code is malicious it will not be able to cause damage to your computer.

You can adjust the basic scan sensitivity by checking or un-checking the following boxes:

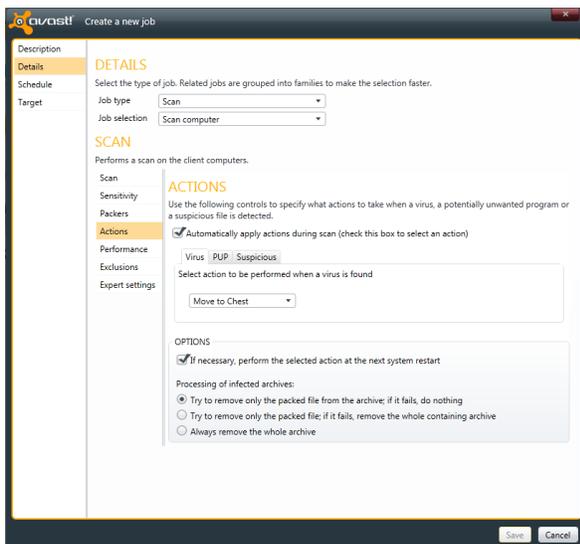
- Test whole files (may be very slow for big files) - checking this box will result in scanned files being tested fully, not just those parts of a file which are normally affected by viruses. Most viruses are normally found either at the beginning of a file, or at the end. Checking this box will therefore result in a more thorough scan, but will also slow the scan down.
- By checking the box "Scan for potentially unwanted programs (PUPs)", you can also scan for programs which you may have downloaded unknowingly, typically programs that are used for advertising, or collecting information about your computer or internet use.

By checking the box "Follow links during scan" you can ensure that the targets of any file system links are also scanned for potentially harmful content. If this box is checked, the content of any folder to which you would be redirected from a folder which is being scanned, will also be scanned.



Packers

On this screen, use the checkbox to specify whether avast! should attempt to unpack archives (packers) during the scanning process



Actions

On this screen, you can specify what actions to take when a virus, PUP, or suspicious file is detected.

The default action is "Move to Chest". If this is left as the selected action, any suspicious files will be automatically moved to the virus chest.

Alternatively, you can select a different action, which avast! will attempt to carry out automatically - Repair, Delete, No Action, or Ask.

If "Ask" is selected, you will be asked to confirm what action to take at the moment the virus, potentially unwanted program, or suspicious file is detected. You can also specify alternate actions, from the same list of options, which should be taken if the preferred actions cannot be completed.

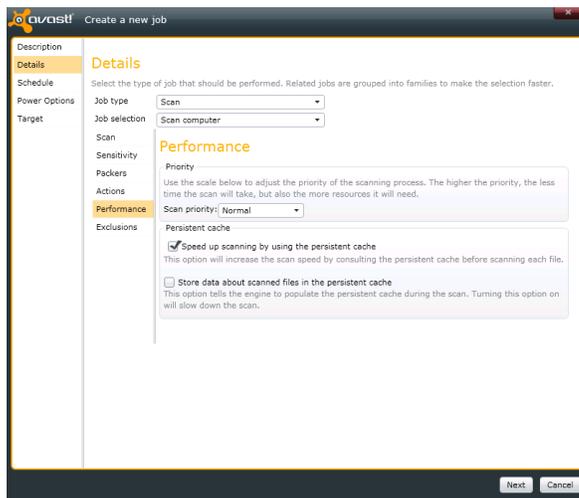
Under "Options", you can select If necessary, perform the selected action at the next system restart. If this box is checked and the action could not be completed, avast! will attempt to carry out the action again the next time the computer is restarted. This could happen, for example where a file was in use and could not be deleted or moved.

Finally there are additional options for dealing with infected archives:

By default, if an infected file is discovered in an archive file, avast! will attempt to remove it.

You can further specify that if the infected file cannot be removed, avast! should remove the archive (the parent archive) within which the infected file is located. Alternatively, you can specify that whenever an infected file is detected inside an archive, the entire archive should always be removed.

On the next screen, you can find the **“Performance”** settings which affect the speed of scanning.



Scan Priority

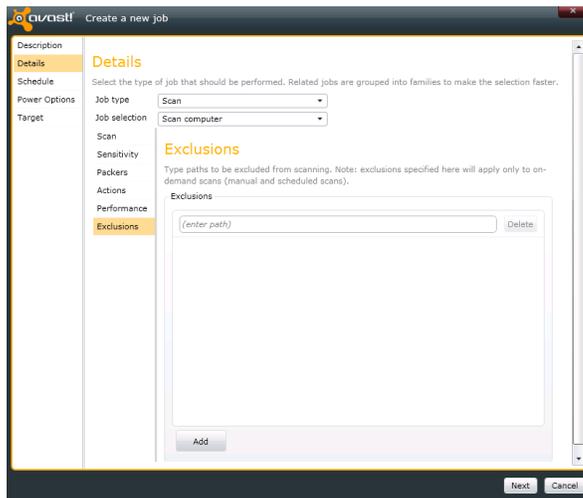
The scan priority can be set to “Low”, “Normal” or “High”. The higher the priority, the faster the scan will be, but the more system resources it will use up.

Persistent Cache

On this screen, you can configure the persistent cache settings. avast! can store information about files that are verified as clean (e.g. they contain a valid digital signature), and this information can then be used to speed up future scans. This information is stored in the "persistent cache".

- Speed up scanning by using the persistent cache - If this is checked, avast! will check the persistent cache for information about files which have been verified as clean and these files will not be scanned again.
- Store data about scanned files in the persistent cache - If this box is checked, information about any new verified clean files detected by avast! during the scan will be added to the persistent cache. This will slow down the current scan, but may increase the speed of future scans, if the first checkbox is checked.

Finally, on the “**Exclusions**” screen, you can specify any files or folders that should not be scanned.



Bear in mind that any exclusions specified on this screen will apply to **all** on-demand scans (manual and scheduled).

- If you want to exclude files only from a specific manual or scheduled scan, use the Exclusions page in the scan settings.
- To exclude files only from being scanned by any of the real-time shields, use the Exclusions page in the real-time shield expert settings on the clients computer.

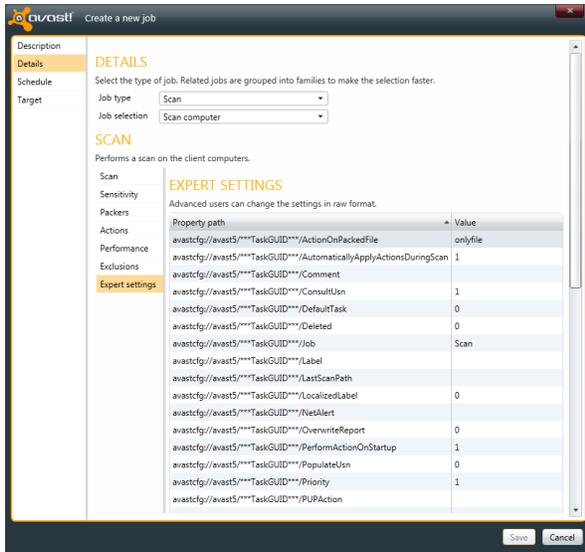
To exclude a location or file, first click the box where it says <enter path> and then either type the location or file to be excluded.

If you want to exclude a folder, including all of its sub-folders, it is necessary to add "*" to the end of the folder name e.g. C:\Windows*.

To remove a location or a file from the exclusions list, click on it once to select it, then click the "delete" button.

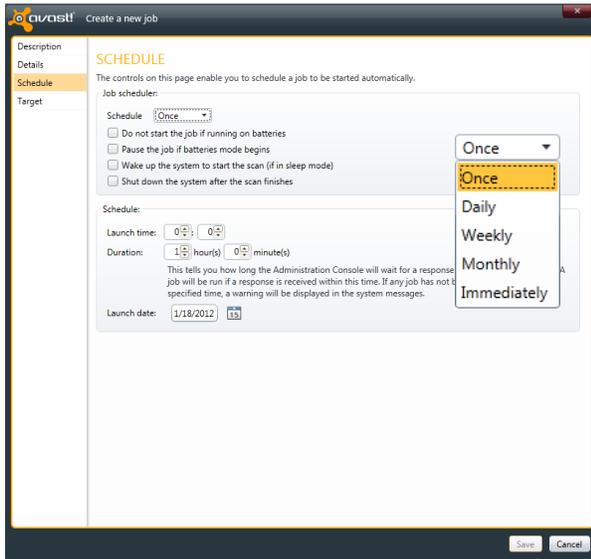
Expert Settings

In the expert settings, you have direct access to the raw data values related to the various settings. As any accidental or erroneous changes could adversely affect the behavior of avast you should only access the expert setting if you are an advanced user and you are used to working directly with the raw data settings.



Running a Job

On the “**Schedule**” screen, you can specify when the job will be run, either once on a given date and at a given time, or regularly on a specific day of the week or month.



Job scheduler

Here you can specify when the job will be started.

- Once - simply enter the time and date when the job should be run
- Daily - enter the time only - the job will be started each day at the given time.
- Weekly (or monthly)
- Immediately

Do not start the job if running on batteries

- Useful mainly for notebook owners. The job will not be started if the computer is running on batteries.

Pause the job if battery mode begins

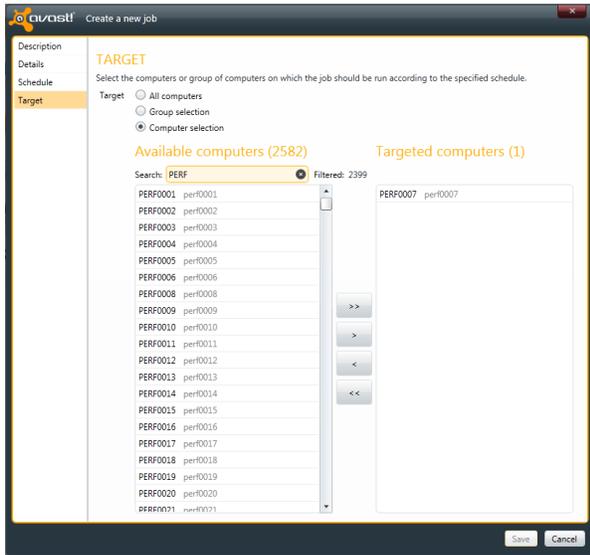
- If the computer is cut off from the electric power supply and switches to batteries while a job is running, the job will be paused. Again, this is useful mainly for notebook owners.

Schedule

- Select a launch time and launch date for jobs that are to be run automatically at a future time.

Duration

- Specify how long the Administration Console will wait for a response from the target computer. A job will be run if a response is received within this time.



Target

This is where you can specify the computer, or group of computers, on which the job should be run. You can select just a single computer, or a computer group, or you can “select all” to run the job on all networked machines.

Jobs History

The History page displays the results of completed jobs:

Job	Started on	Finished on	Job completed	Unreachable computers	Job timed-out	Result
Update server definitions	6/5/2012 5:31:42 AM	6/5/2012 5:35:47 AM	N/A	N/A	N/A	SUCCEEDED
Quick scan	6/5/2012 5:23:50 AM	6/5/2012 5:23:51 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	6/5/2012 5:23:50 AM	6/5/2012 5:31:41 AM	N/A	N/A	N/A	SUCCEEDED
Clean unused database entries	6/5/2012 5:23:50 AM	6/5/2012 5:23:52 AM	N/A	N/A	N/A	SUCCEEDED
Computer discovery	6/5/2012 4:09:57 AM	6/5/2012 4:11:31 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	5/29/2012 7:25:54 AM	5/29/2012 7:28:58 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	5/29/2012 5:25:54 AM	5/29/2012 5:30:21 AM	N/A	N/A	N/A	SUCCEEDED
Quick scan	5/29/2012 4:00:02 AM	5/29/2012 4:00:03 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	5/29/2012 3:25:54 AM	5/29/2012 3:28:57 AM	N/A	N/A	N/A	SUCCEEDED
Computer discovery	5/29/2012 2:00:01 AM	5/29/2012 2:01:08 AM	N/A	N/A	N/A	SUCCEEDED
Clean unused database entries	5/29/2012 2:00:00 AM	5/29/2012 2:00:04 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	5/29/2012 1:25:54 AM	5/29/2012 1:32:43 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	5/28/2012 8:25:54 AM	5/28/2012 8:30:17 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	5/28/2012 6:25:54 AM	5/28/2012 6:28:40 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	5/28/2012 4:27:20 AM	5/28/2012 4:32:04 AM	N/A	N/A	N/A	SUCCEEDED
Quick scan	5/28/2012 4:18:01 AM	5/28/2012 4:18:02 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	5/28/2012 4:18:01 AM	5/28/2012 4:27:19 AM	N/A	N/A	N/A	SUCCEEDED
Clean unused database entries	5/28/2012 4:18:01 AM	5/28/2012 4:18:03 AM	N/A	N/A	N/A	SUCCEEDED
Computer discovery	5/28/2012 3:24:57 AM	5/28/2012 3:26:16 AM	N/A	N/A	N/A	SUCCEEDED



If you would like to see more detailed information, click on the “folder” icon

7. Reports

The Administration Console also offers wide reporting capabilities. You can create a variety of useful reports by simply clicking on the selected file format. See the section “Running a job” for a description of how to create and send reports automatically to specific users.

The screenshot shows the 'REPORTS' page in the avast! Small Office Administration console. The page is titled 'REPORTS' and includes a sub-header: 'This page lets you define custom reports. Here you can specify the required format and how the report will be delivered.' The page is divided into three main sections: 'CHOOSE REPORT', 'CHECK REPORT PREVIEW', and 'GENERATE REPORT'.

CHOOSE REPORT: This section lists various report types, including 'Top 10 Viruses', 'Network Computers - Simple Overview', 'Network Computers - Full Summary', 'Network Computers - Virus Definitions Version', 'Network Computers - avast! version', 'Top 10 Infected Computers', 'Malware detected in last 24 hours', 'Malware detected in last 7 days', 'Computers infected in last 24 hours', and 'Computers infected in last 7 days'.

CHECK REPORT PREVIEW: This section shows a preview of the 'TOP 10 VIRUSES' report. The preview includes a horizontal bar chart and a table. The table data is as follows:

Report	Count	First seen	Last Communication
Win32:Packed-A [Heur]	3	5/11/2012 1:39:37 PM	5/11/2012 1:39:41 PM
JS:Pdfka-gen [Exp]	3	5/11/2012 1:39:39 PM	5/11/2012 1:39:39 PM
WV:AutoRun-AR [Wvm]	3	5/11/2012 1:39:39 PM	5/11/2012 1:39:39 PM
Other:Malware-gen [Trj]	2	5/11/2012 1:39:38 PM	5/11/2012 1:39:38 PM
Win32:Adware-gen [Adv]	2	5/11/2012 1:39:37 PM	5/11/2012 1:39:40 PM
Win32:AutoRun-A2B [Wvm]	2	5/11/2012 1:39:37 PM	5/11/2012 1:39:40 PM
LNK:Runner	2	5/11/2012 1:39:37 PM	5/11/2012 1:39:41 PM

GENERATE REPORT: This section offers buttons for PDF, Word, HTML, RTF, and PowerPoint.

You can export these reports to many popular formats – Pdf, Word, Html, Rtf, Powerpoint.

There are 11 pre-defined reports:

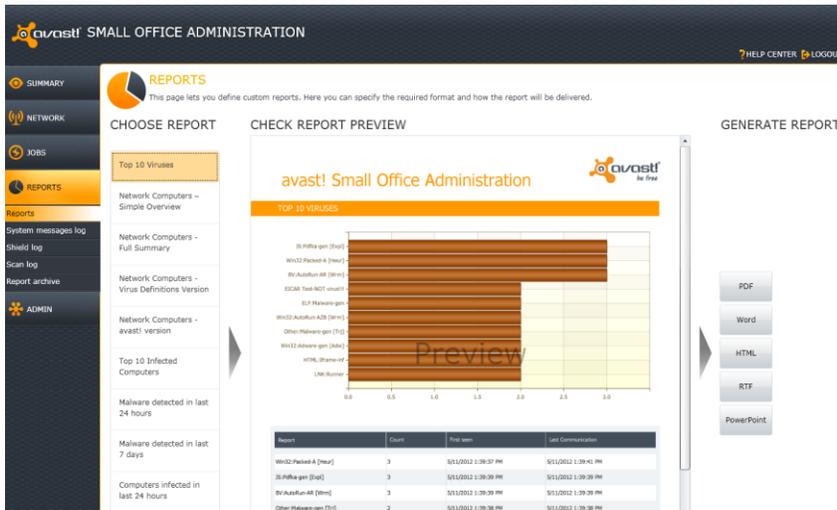
- Top 10 viruses
- Network computers - simple overview
- Network computers - full summary
- Network computers - virus definitions version
- Network computers - avast! version
- Top 10 infected computers
- Network computers - last communication
- Malware detected in last 24 hours
- Malware detected in last 7 days
- Computers infected in last 24 hours
- Computers infected in last 7 days

Examples of some of the reports which can be created:

Top 10 infected computers



Top 10 viruses

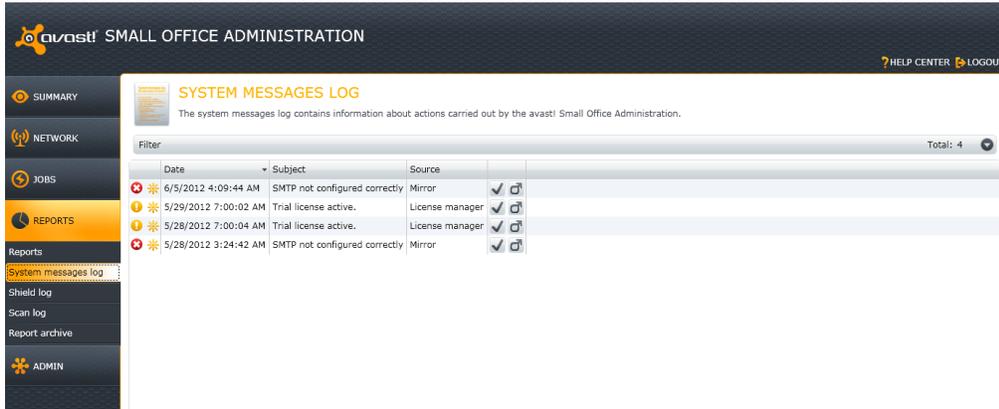


Network computers – simple overview

Computer Name	OS type	Status	Last Communication	Computer Description
AVI5413	Unknown	Unmanaged		
Bob	Unknown	Unmanaged		
Carl	Windows XP Service Pack 3	Secured	5/1/2012 8:29:47 PM	
Carl Notebook	Windows XP Service Pack 3	Secured	5/1/2012 8:29:48 PM	
EDNA	Unknown	Unmanaged		
Jane	Windows XP Service Pack 3	Secured	5/1/2012 8:29:51 PM	
John	Windows XP Service Pack 3	Secured	5/1/2012 8:29:51 PM	
MILEY	Unknown	Unmanaged		
PER0001	Unknown	Unmanaged		
PER0002	Unknown	Unmanaged		
PER0003	Unknown	Unmanaged		
PER0004	Unknown	Unmanaged		
PER0005	Unknown	Unmanaged		
PER0006	Unknown	Unmanaged		
PER0007	Unknown	Unmanaged		
PER0008	Unknown	Unmanaged		
PER0009	Unknown	Unmanaged		

System Messages Log

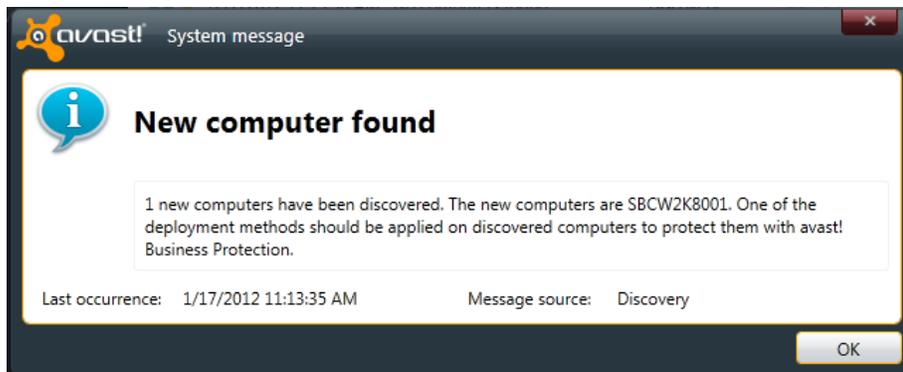
The system messages log contains all information about actions carried out by the Administration console.



To remove a message from the list click on the "tick" icon:



To see more detailed information click on the "folder" icon:



Shield Log

The shield log contains all alerts raised by the on-access scanners, such as the Web shield, Network shield, File system shield etc.

avast! SMALL OFFICE ADMINISTRATION

SHIELD LOG
This is a log of all alerts raised by the on-access scanners, such as the Web Shield or Network Shield.

Filter Total: 10

Computer	Shield	Path	Virus	Time
SBCW7001	Web Shield	http://www.eicar.org/do	EICAR Test-NOT virus!!!	3/11/2011
SBCW7001	Web Shield	http://www.eicar.org/do	EICAR Test-NOT virus!!!	3/11/2011
SBCW7001	Web Shield	http://www.eicar.org/do	EICAR Test-NOT virus!!!	3/11/2011
SBC221	File System Shield	C:\viry\180E645C.exe	Win32:Harrier	3/11/2011
SBC221	File System Shield	C:\viry\0068DADA.exe	Win32:Cekar	3/11/2011
SBC221	File System Shield	C:\viry\0058AA2D.exe	Win32:Kamso [Trj]	3/11/2011
SBC221	File System Shield	C:\viry\05C9BD38.exe	Win32:Kaze	3/11/2011
SBC221	File System Shield	C:\viry\01B907C4.exe	Win32:Allaple [Wrm]	3/11/2011
SBC221	File System Shield	C:\viry\0001E7EC.exe	Win32:ChanCrypt [Cryp]	3/11/2011

It is possible to filter by Computer name,

Filter Total: 10

by Computer by Path by Virus By Shields

Pattern Match case

Clear Filter

by Path/location,

Filter Total: 10

by Computer by Path by Virus By Shields

Pattern Match case

Clear Filter

by Virus name,

Filter Total: 10

by Computer by Path by Virus By Shields

Pattern Match case

Clear Filter

or by Shield

Filter Total: 10

by Computer by Path by Virus By Shields

File System Shield Mail Shield Web Shield P2P Shield IM Shield Network Shield Included Excluded

Script Shield Behavior Shield Anti Spam Shield Exchange Shield Sharepoint Shield

Firewall

Clear Filter

Scan Log

The scan log screen shows you the results of individual scans run on the computers in your network:

SCAN LOG
This screen shows you the results of individual scans run on the computers in your network.

Filter Total: 0

Computer	Path	Virus	Time
SBC221	c:\viry\zace \context_Packed-A\C6z	Win32:Packed-A [Heur]	3/14/2011
SBC221	c:\viry\shrt-062D35E8.sam	Win32:Alureon-GC [Rtk]	3/14/2011
SBC221	c:\viry\pe2-trj-078653C1.sam	Win32:Hrupka-A [Cryp]	3/14/2011
SBC221	c:\viry\pe2-spy-09158E5B.sam	Win32:Spyware-gen [Spy]	3/14/2011
SBC221	c:\viry\pe2-rtk-5E75E0CF.sam	Win32:Rootkit-gen [Rtk]	3/14/2011
SBC221	c:\viry\pe2-mal-04071EE9.sam	Win32:KadrBot [Trj]	3/14/2011
SBC221	c:\viry\pe2-dial-153B02D1.sam	Win32:Dialer-gen [Dialer]	3/14/2011
SBC221	c:\viry\pe2-adw-33949F1D.sam	Win32:Adware-gen [Adw]	3/14/2011
SBC221	c:\viry\long-5D6A9415.sam	Win32:AutoRun-AZB [Wrm]	3/14/2011

Page 1 of 1

The scan log can be filtered by Computer name,

Filter Total: 100

by Computer | by Path | by Virus

Pattern Match case Clear Filter

by Path/location,

Filter Total: 100

by Computer | by Path | by Virus

Pattern Match case Clear Filter

or by Virus name

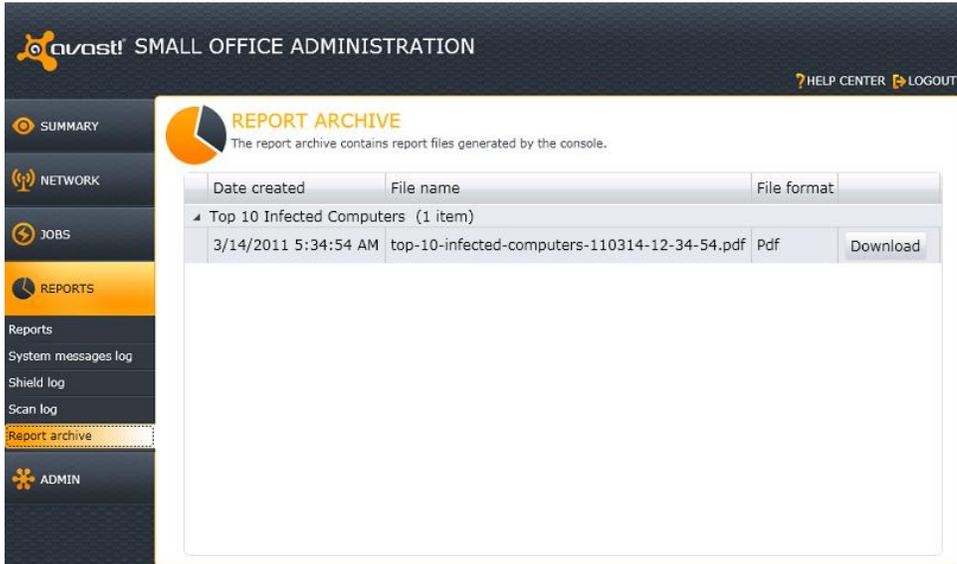
Filter Total: 100

by Computer | by Path | by Virus

Pattern Match case Clear Filter

Report archive

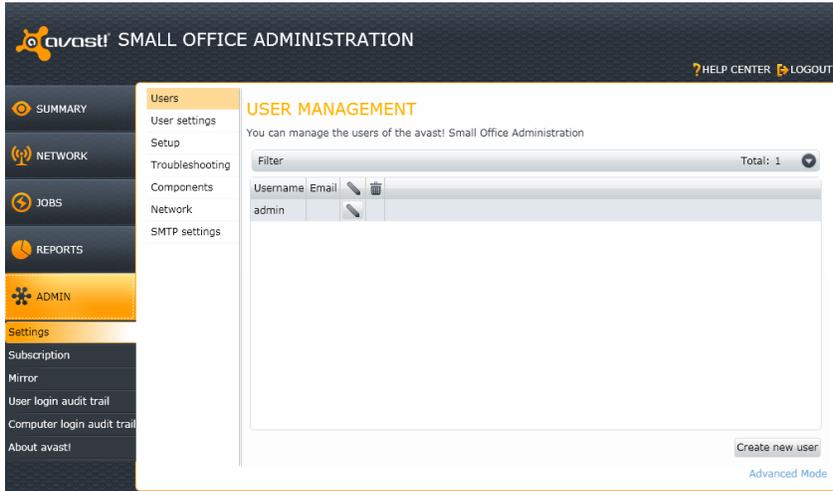
For future use, the Administration console stores every generated report, which can be downloaded by clicking the Download button.



To make it easy to locate specific reports, you can categorize reports by Creation date, File name, or File format.

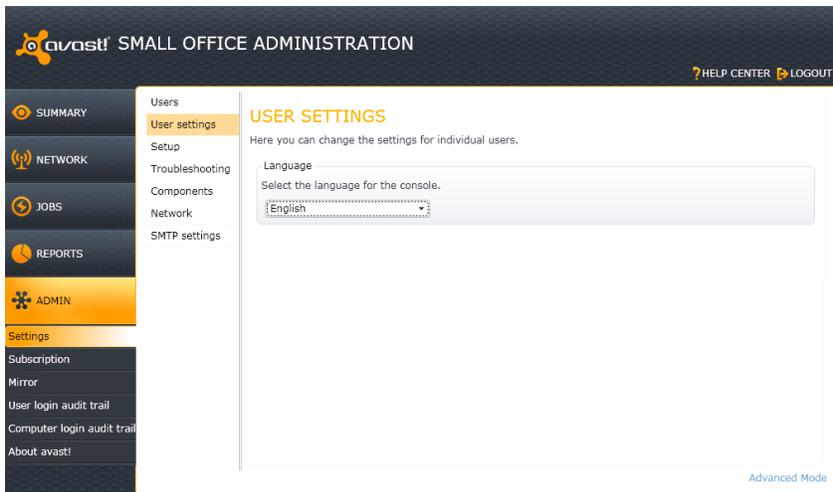
8. Administration

Settings



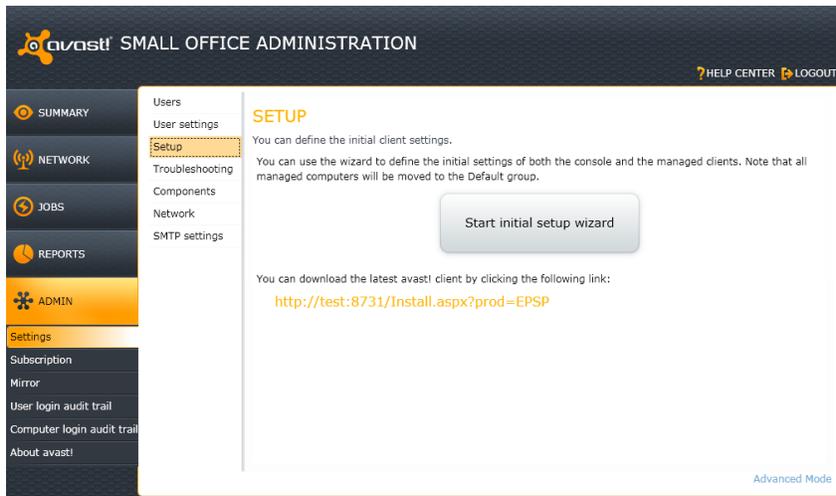
Users

The Users folder holds a list of all users who are permitted to access the Administration console.



User Settings

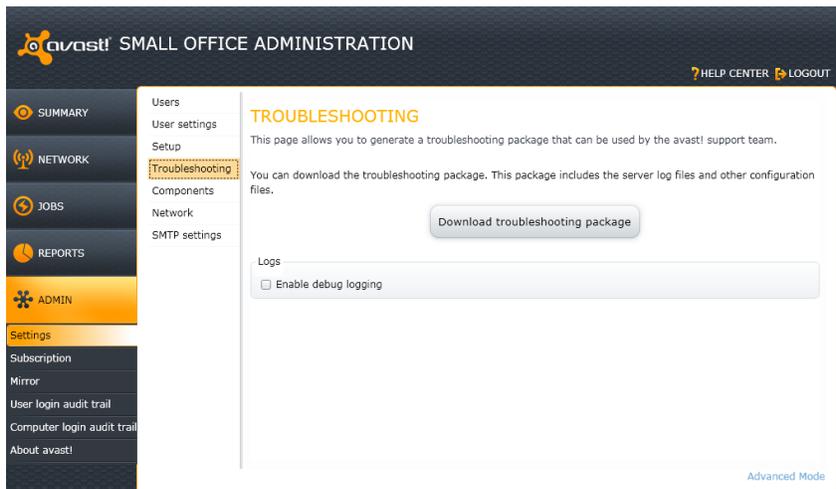
Here you can select the language for the interface from the list of available Administration console languages.



Setup

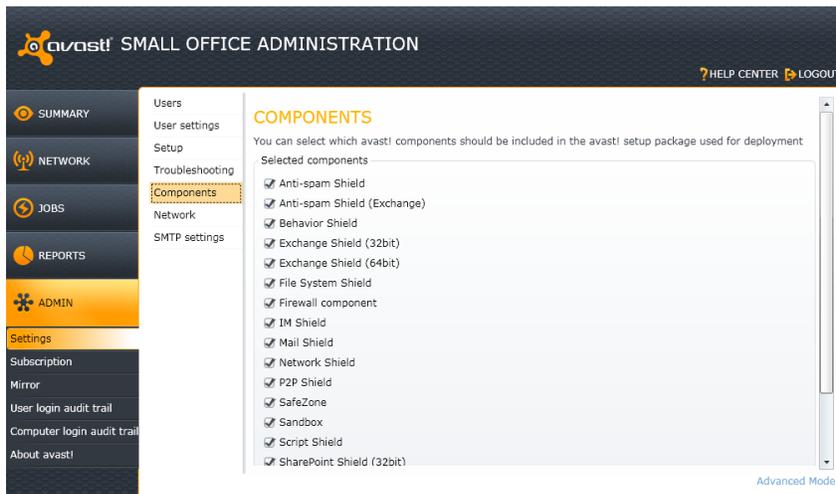
You can define the initial client settings.

Note that running the initial setup wizard again, after you have allocated your computers to groups will result in all computers being re-assigned back to their initial default groups.



Troubleshooting

Here you can create a package containing all your key system information for avast support purposes.



Components

Here you can select which avast! components should be used in the avast! setup packages used for deployment.

Advanced Mode

The Advanced mode settings are accessed by clicking on “Advanced Mode” in the bottom right corner of the “Users” or “User settings” screen.

Changes to the Advanced Mode settings should be made only if specifically requested by avast! technical support and all changes are logged for internal use. Unauthorized changes may seriously impair the performance of your system. Avast Software cannot be held responsible for any problems caused by any unauthorized changes to the Advanced Mode settings.



avast! SMALL OFFICE ADMINISTRATION HELP CENTER LOGOUT

SUMMARY | **NETWORK** | **JOBS** | **REPORTS** | **ADMIN**

Settings

Subscription

Mirror

User login audit trail

Computer login audit trail

About avast!

Simple Mode

Management

Key	Value
Backup file name template	backup(date).dat
Backup files path	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\B...
Message queue validity	1209600
Troubleshooting dump validity	1209600
Max age of VPS versions	1825
Max age of program versions	1825

Mirror configuration

Key	Value
Proxy address	
Proxy type	0
Proxy port	0
Proxy user name	
Proxy password	

Save

avast! SMALL OFFICE ADMINISTRATION HELP CENTER LOGOUT

SUMMARY | **NETWORK** | **JOBS** | **REPORTS** | **ADMIN**

Settings

Subscription

Mirror

User login audit trail

Computer login audit trail

About avast!

Simple Mode

Proxy use NTLM	0
Mirror directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\M...
Distribution directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\M...
Log directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\M...
Configuration directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\M...
Packages directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\M...
MSI packages directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\M...
Setup INI creation timeout (s)	30
Debug mirror	False
Polling interval	10000

Passwords

Key	Value
Minimum Length	6
Use alpha-numeric characters	True
Use non alpha-numeric characters	False

Save

avast! SMALL OFFICE ADMINISTRATION HELP CENTER LOGOUT

SUMMARY | **NETWORK** | **JOBS** | **REPORTS** | **ADMIN**

Settings

Subscription

Mirror

User login audit trail

Computer login audit trail

About avast!

Simple Mode

Allow blank password False

Provider status aggregate

Key	Value
Five minute records age (days)	1
Half hour records age (days)	1
Two hour records age (days)	3
One day records age (days)	7

Reports

Key	Value
Reports directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\R...
Reports templates directory	templates\
Reports thumbs directory	thumbs\
Enable thumbnail regeneration	False

Server core

Save

avast! SMALL OFFICE ADMINISTRATION HELP CENTER LOGOUT

ADMIN

Settings

Subscription

Mirror

User login audit trail

Computer login audit trail

About avast!

Simple Mode

Key	Value
Authentication mode	undefined
Update period (seconds)	10
Listen protocol specifier	http
Secure listen protocol specifier	https
Server application path	Design_Time_Addresses/Avast.Sbc.Service.Core/SbcConnectionPoint/
Dashboard status forced reload	3600
Nodes update pause (milliseconds)	30
Nodes update chunk count	40
Web service timeout (minutes)	0
Activity window (seconds)	30
Maximum result count per request	1500
Licence file location	C:\Documents and Settings\All Users\Application Data\AVAST Software\Admin
Engine provider status poll timeout (milliseconds)	60000
Message queue poll timeout (milliseconds)	30000

Save

avast! SMALL OFFICE ADMINISTRATION HELP CENTER LOGOUT

ADMIN

Settings

Subscription

Mirror

User login audit trail

Computer login audit trail

About avast!

Simple Mode

Message queue resend threshold (milliseconds)	10000
Engine polling delay (milliseconds)	30000
System monitor polling delay (milliseconds)	500
Entity names for troubleshooting	Configuration,NativeProperty,Node,NodeGroup,Job,ScheduleItem
Managed network type	All
Network adapter name	
Network IP address	
Network MAC address	
System language name	en-US
Node cache validity (milliseconds)	30000
Activity check interval (milliseconds)	5000
Last known version file location	C:\Documents and Settings\All Users\Application Data\AVAST Software\Admin
Program update check interval (minutes)	60
Provider status cleanup interval (minutes)	60
Common aggregation delay (secs)	300
Aggregation interval for monthly results (minutes)	30

Save

avast! SMALL OFFICE ADMINISTRATION HELP CENTER LOGOUT

ADMIN

Settings

Subscription

Mirror

User login audit trail

Computer login audit trail

About avast!

Simple Mode

Aggregation interval for daily results (minutes)	2
Aggregation interval for week results (minutes)	10
Aggregation interval for year results (minutes)	90
Program update manifest URL	http://files.avast.com/iavs5x/{edition}_console.info.ver
Track unknown node login requests	True
Health monitor trigger interval (minutes)	60
Service controller timeout (milliseconds)	60000
Service controller attempts	3

Server messaging configuration

Key	Value
Primary protocol prefix	tcp://
Primary server port	25322
Primary server path	
Primary retry count	3
Secondary protocol prefix	

Save

avast! Endpoint Protection – Installation Guide

The screenshot shows the 'Simple Mode' configuration page for the 'NETWORK' section. The left sidebar contains navigation options: SUMMARY, NETWORK, JOBS, REPORTS, ADMIN (highlighted), Settings, Subscription, Mirror, User login audit trail, Computer login audit trail, and About avast!. The main content area displays a list of network-related settings:

Key	Value
Secondary server address	
Secondary server port	-1
Secondary server path	
Checksum algorithm	CRC32
Require SSL	False
Debug messaging	False
Activity processor thread count	10
Process messages on separate threads	True
Min worker thread count	5
Max worker thread count	20
APIP check	True
APIP check timeout (ms)	10000

Below this list is a 'Server scheduler' section with a table:

Key	Value
Scheduler thread wait	250

A 'Save' button is located at the bottom right of the configuration area.

The screenshot shows the 'Simple Mode' configuration page for the 'ADMIN' section. The left sidebar is identical to the previous screenshot. The main content area displays settings for 'APIP check', 'Server scheduler', and 'Unattended deployment configuration':

Key	Value
APIP check	True
APIP check timeout (ms)	10000

Below this is the 'Server scheduler' section:

Key	Value
Scheduler thread wait	250
Scheduler maximum workers	5
Scheduler cache flush interval (ms)	10000
Scheduler rebuild cache interval (ms)	600000

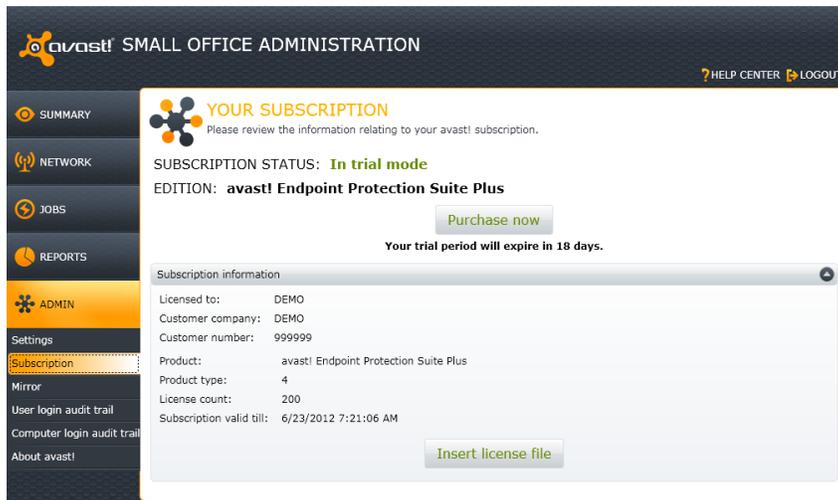
Finally, the 'Unattended deployment configuration' section includes:

Key	Value
Install result check interval (ms)	250
Maximum allowed delay between updates (s)	60
Executable folder	C:\Program Files\AVAST Software\Administration Console
Data folder	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administra

A 'Save' button is located at the bottom right of the configuration area.

Subscription

After receiving your license file, you just need to double-click to open it and your license will be inserted into your program automatically. You can now continue to use your avast! antivirus for the duration of your license and you will continue to receive automatic updates to both the program and your virus definitions.



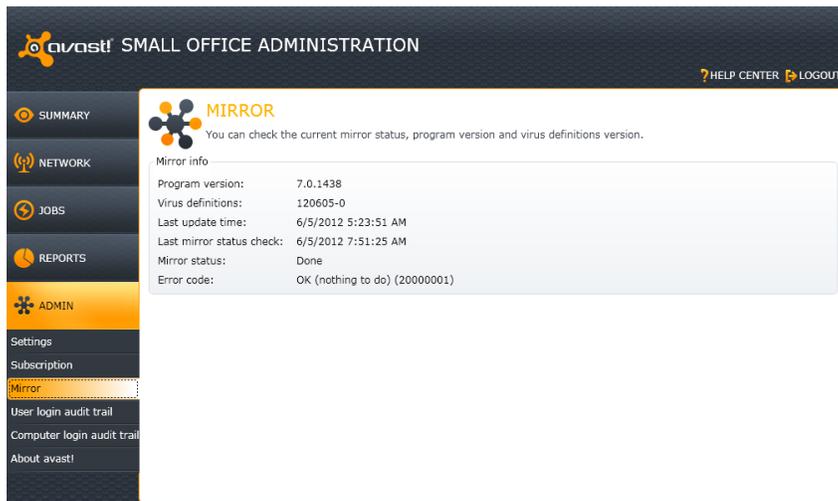
Alternatively, save the license file on your computer, open the avast! interface and click on the Maintenance tab. Next click on "Subscription" and then on "Insert license file". A new window will open where you can browse your computer to locate your license file. Once you have located it, double click on it and it will be automatically inserted into the program.

Mirror

The Mirror, which was installed automatically during the installation, automatically receives updates from the avast! server and distributes them automatically to all the managed clients on your network to ensure they are always completely up to date.

The great advantage of using the Mirror to distribute updates in this way is that the updates need to be downloaded only once from the avast Update server, thus saving you valuable bandwidth.

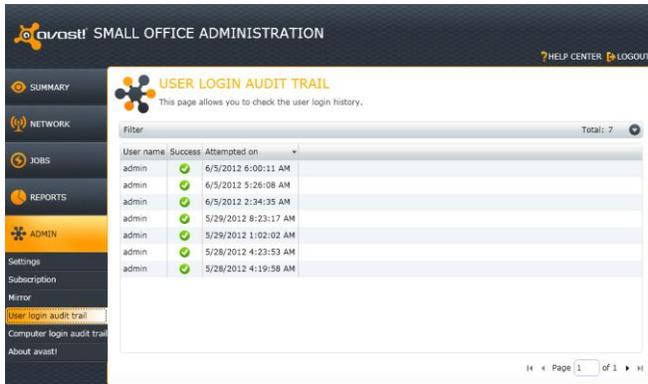
This screen shows you certain summary information about the status of the mirror:



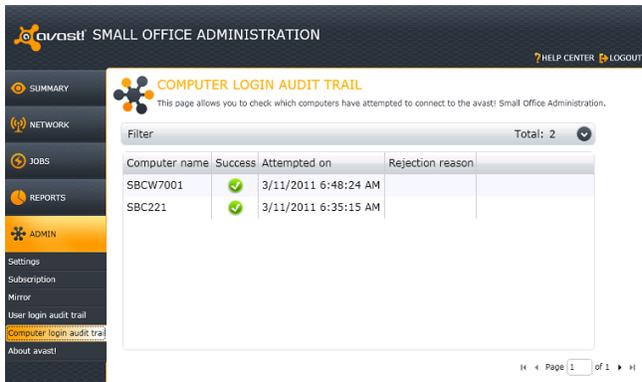
Although the mirror is updated automatically, you can also manually update it to make sure that you have the very latest copy of the update server at any given moment. To ensure you have the very latest updates and virus definitions, just run the job "Update Server Definitions" on the "Jobs" screen.

For security reasons, the Administration console provides you with both a User login audit trail and a Computer login audit trail. This allows you to check the history of:

- users/administrators logins
- attempts to connect to the avast! Administration console



User login audit trail



Computer login audit trail

9. Important Files

Default installation path:

Windows Vista/7

- C:\Program Files\AVAST Software\Administration Console
- C:\Users\All Users\AVAST Software\Administration Console

Windows XP

- C:\Program Files\AVAST Software\Administration Console
- C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console

Administration console log files:

Windows Vista/7

- C:\Users\All Users\AVAST Software\Administration Console\Logs

Windows XP

- C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Logs

License files:

Windows Vista/7

- C:\Users\All Users\AVAST Software\Administration Console

Windows XP

- C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console

Important Mirror files:

Mirror root folder

Windows Vista/7

- C:\Users\All Users\AVAST Software\Administration Console\Mirror\Mirror

Windows XP

- C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Mirror\Mirror

Distribution folder

Windows Vista/7

- C:\Users\All Users\AVAST Software\Administration Console\Mirror\Distrib

Windows XP

- C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Mirror\Distrib

Packages folder

Windows Vista/7

- C:\Users\All Users\AVAST Software\Administration Console\Mirror\Packages

Windows XP

- C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Mirror\Packages

Installers folder

Windows Vista/7

- C:\Users\All Users\AVAST Software\Administration Console\Mirror\Install

Windows XP

- C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Mirror\Install