Administration Console

For avast Business Protection (Plus)

Administrator’s Guide
This guide has been written to assist system administrators or anyone who uses the avast! 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
   SBC Administration Console: .............................................................................................................................. 5
   Centrally managed “client” products: .................................................................................................................... 6
3. Installation............................................................................................................................................................. 9
4. Administration Console Setup.......................................................................................................................... 21
   Systems overview .................................................................................................................................................. 26
   Virus definition status ........................................................................................................................................... 26
   Statistics.............................................................................................................................................................. 27
   System messages .................................................................................................................................................. 27
5. Network Screen.................................................................................................................................................... 28
   Group view .......................................................................................................................................................... 28
   Grid view ............................................................................................................................................................ 30
   Filtering .............................................................................................................................................................. 30
   Create (Add) a New Computer ............................................................................................................................ 33
   Creating a New Group ......................................................................................................................................... 34
6. Jobs ..................................................................................................................................................................... 44
   Create a new job ................................................................................................................................................... 44
   Deployment Jobs (3 types) ................................................................................................................................... 47
   Maintenance Jobs (4 types) .................................................................................................................................. 50
   Scanning Jobs ...................................................................................................................................................... 55
   Running a Job .................................................................................................................................................... 61
   Jobs History ....................................................................................................................................................... 62
7. Reports.................................................................................................................................63
   System Messages Log ........................................................................................................65
   Shield Log..........................................................................................................................66
   Scan Log............................................................................................................................67
   Report archive ....................................................................................................................68
8. Administration.....................................................................................................................69
9. Important Files...................................................................................................................77
1. General Information

The avast! Administration Console has been specifically designed to make the administration of your computer network as simple as possible, while providing the maximum protection for all the computers on your network.

The central web based 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 Administration Console is designed primarily for small networks of up to 200 workstations. It’s a simple and easy to use program to help you deploy and manage avast! antivirus on your network, and keep your network free of viruses and other malware.

The Administration Console is a web based system and does not require a server Operating System. Once installed, you can access it from any computer with an internet connection.
2. System Requirements

**SBC Administration Console:**

Supported operating systems:

- Windows XP, SP3 or higher
- Windows 2003 Server (all editions), latest SP
- Windows 2008/R2 Server (all editions, excluding Core Installation), latest SP
- Windows SBS 2011

Note: the latest SP and a fully updated OS is recommended!

Minimum Hardware Requirements:

- Processor Pentium 3
- 1 GB RAM
- A minimum of 900 MB of free hard disk space for the initial installation
- Internet Explorer 6 or higher, or other Silverlight enabled browser

Note: The minimum Windows operating system requirements must also be met.
Centrally managed “client” products:

avast! Business Protection
(for Workstations)

Supported operating systems:

• Windows 7 x32/64bit
• Windows Vista (any Edition excl. Starter Edition) x32/64bit
• Windows XP Service Pack 2 or higher x32/64bit
• Windows 2000 Professional Service Pack 4

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

Minimum Hardware Requirements:

• Processor Pentium 3
• 256 MB RAM
• 300 MB of free hard disk space

avast! Business Protection Plus
(for Workstations)

Supported operating systems:

• Windows 7 x32/64bit
• Windows Vista (any Edition excl. Starter Edition) x32/64bit
• Windows XP Service Pack 2 or higher x32/64bit

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

Minimum Hardware Requirements

• Processor Pentium 3
• 256 MB RAM
• 380 MB of free hard disk space
avast! Business Protection/Plus
(for Server operating systems)

Supported operating systems/hardware requirements:

• Windows 2003 (32 bit/64 bit)
  – Processor Pentium 3
  – 256 MB RAM
  – 200 MB of free hard disk space

• Windows 2008/R2 Server (any edition, 32 bit/64 bit, excluding Core Installation)
  – Processor Pentium 3
  – 512 MB RAM
  – 200 MB of free hard disk space

• Windows SBS 2011
  – Processor Pentium 3
  – 512 MB RAM
  – 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://www.microsoft.com)

SQL full versions vs SQL Free/Express versions


[http://msdn.microsoft.com](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**

- Is DHCP used on the network? Can the Console have a fixed IP address? (It should)
- Is a full MS SQL 2000/2005/2008 database going to be used, or the Free/Express version (MSDE/2005/2008)? If you choose MSDE/Express, will it handle all your management data? (MSDE/Express should only be used on networks of several hundred computers or fewer).

Note: Make sure that you are aware of all limitations of MSDE and SQL Express 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.

To continue with the installation just click the Next button

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:

- IIS – Internet Information Services (has to be installed and running -part of the MS Windows)
- 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.
To continue with the installation, on the next screen select “I accept the terms in the License Agreement”.

Then click Next to continue with the installation

The proxy settings on the next screen are important when avast! needs to access the internet, for example, when carrying out 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

On the next screen, you can insert your license if you have already purchased one and saved it on your computer, or you can request a demo license, valid for 30 days:

- **Insert license file:**
  - If you have already purchased the product, use this option to install the product with your license file.
  - License file locations: C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console
  - License file name: license.avastlic

- **Request demo license (Requires an Internet connection)**
  - Free 30-day trial
On the next screen, you can choose how you want the program to be installed:

Besides the **Recommended** installation with predefined configuration, you can also select **Expert**, which enables you to change/specify the program component settings.

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

Then click **Next** to continue.

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 internet. This will allow the administration console mirror to download virus definition updates.
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“.  

Enter the name of the virtual folder that will be created in the IIS root folder and used by the avast! Administration console.

- This IIS folder specifies the location of the console application – serves as your entry point into the system.
- Our recommendation is to keep the Avast default name.
On the next screen you can choose whether to install SQL server 2008 R2 Express, or to use a custom SQL server which is already installed and in use:

**SQL server 2008 R2 Express:**
The MS “free” SQL database will be automatically downloaded and installed. Make sure that you are aware of all MS SQL Express limitations!

If you selected **Use custom SQL Server Instance** then you’ll have to provide its location, credentials and DB name.
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”
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 Administration Console” 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:

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.

![Managed Computers](image)

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**

![Deployment of avast!](image)

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.

![Dashboard screenshot](image)

**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:

![Network Screen](image)

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

- 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

- 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:

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.

![Update Settings](image)

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.

![Boot-time scan screenshot](image)

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.
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 using Active Directory
- Discover new computers in the network neighborhood

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”
2. 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

![Image of Discover new computers in the network neighborhood job](image)

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.

![Performance Settings](image)

**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.
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:

![Jobs History Image]

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.

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**
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:

![Mark message as read]

To see more detailed information click on the “folder” icon:

![Open message]

**New computer found**

1 new computers have been discovered. The new computers are SBCW2X8001. One of the deployment methods should be applied on discovered computers to protect them with avast! Business Protection.

Last occurrence: 1/17/2012 11:13:35 AM  
Message source: Discovery
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.

![Shield Log Image]

It is possible to filter by Computer name,

![Filter by Computer Image]

By Path/Location,

![Filter by Path Image]

By Virus name,

![Filter by Virus Image]

Or by Shields

![Filter by Shields Image]
Scan Log

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

The scan log can be filtered by Computer name,

By Path/location,

or by Virus name
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 see a list of all the 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 reassigned back to their initial default groups.

**Troubleshooting**

Here you can create a package containing all your system 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.
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:

![Mirror status image]

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

<table>
<thead>
<tr>
<th>User Name</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>3/14/2011 1:09:57 AM</td>
</tr>
<tr>
<td>admin</td>
<td>3/14/2011 12:25:31 AM</td>
</tr>
<tr>
<td>admin</td>
<td>3/12/2011 12:12:51 AM</td>
</tr>
<tr>
<td>admin</td>
<td>3/11/2011 6:02:35 AM</td>
</tr>
</tbody>
</table>

### Computer login audit trail

<table>
<thead>
<tr>
<th>Computer Name</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBC/016</td>
<td>3/12/2011 4:49:24 AM</td>
</tr>
<tr>
<td>SBC/017</td>
<td>3/11/2011 3:26:11 AM</td>
</tr>
</tbody>
</table>
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

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\Logs

Windows XP
• C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Mirror\Logs

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