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 Vista (any Edition excl. Starter Edition), latest SP
- Windows 7 (excl. Starter Edition and Home Basic Edition)
- 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://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?

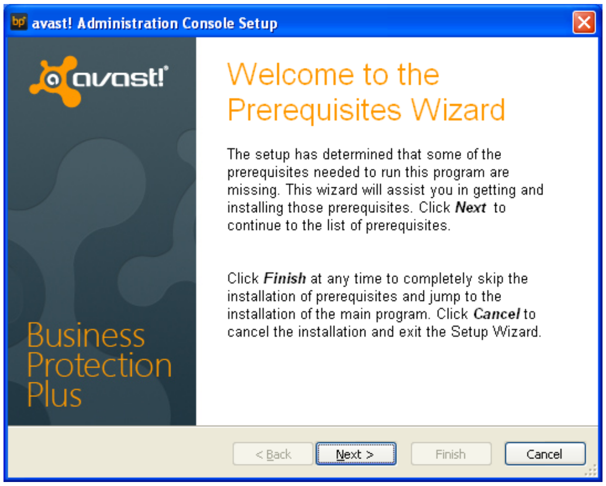
Note: Make sure that you are aware of the minimum system requirements

SQL

- 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 prerequisities are installed. Simply follow the installation wizard which will also help you to find and install any prerequisites which are missing.

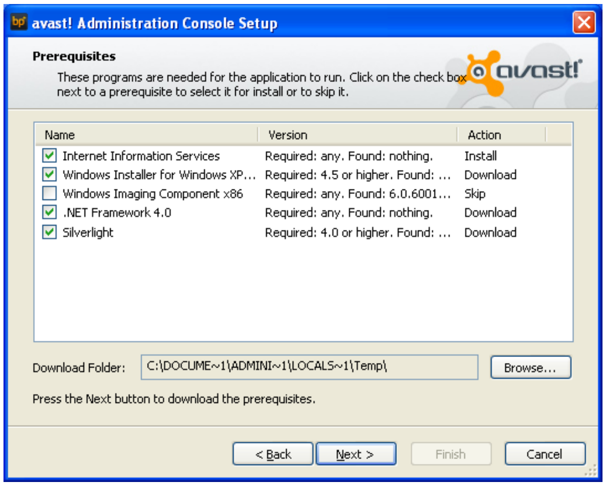


Welcome to the Prerequisites Wizard

The setup has determined that some of the prerequisites needed to run this program are missing. This wizard will assist you in getting and installing those prerequisites. Click ***Next*** to continue to the list of prerequisites.

Click ***Finish*** at any time to completely skip the installation of prerequisites and jump to the installation of the main program. Click ***Cancel*** to cancel the installation and exit the Setup Wizard.

To continue with the installation just click the Next button



Prerequisites

These programs are needed for the application to run. Click on the check box next to a prerequisite to select it for install or to skip it.

Name	Version	Action
☑ Internet Information Services	Required: any. Found: nothing.	Install
☑ Windows Installer for Windows XP...	Required: 4.5 or higher. Found: ...	Download
□ Windows Imaging Component x86	Required: any. Found: 6.0.6001...	Skip
☑ .NET Framework 4.0	Required: any. Found: nothing.	Download
☑ Silverlight	Required: 4.0 or higher. Found: ...	Download

Download Folder: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\

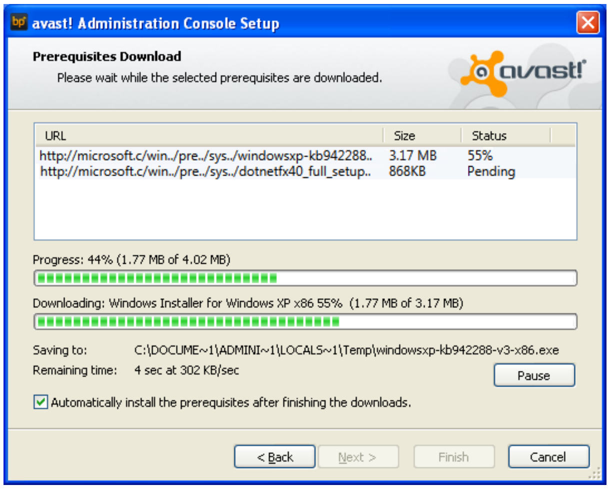
Press the Next button to download the prerequisites.

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

Prior to installing the Administration console all prerequisities 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 prerequisities should be automatically downloaded and installed (an Internet connection is required)



avast! Administration Console Setup

Prerequisites Download

Please wait while the selected prerequisites are downloaded.

URL	Size	Status
http://microsoft.c/win../pre../sys../windowsxp-kb942288..	3.17 MB	55%
http://microsoft.c/win../pre../sys../dotnetfx40_full_setup..	868KB	Pending

Progress: 44% (1.77 MB of 4.02 MB)

Downloading: Windows Installer for Windows XP x86 55% (1.77 MB of 3.17 MB)

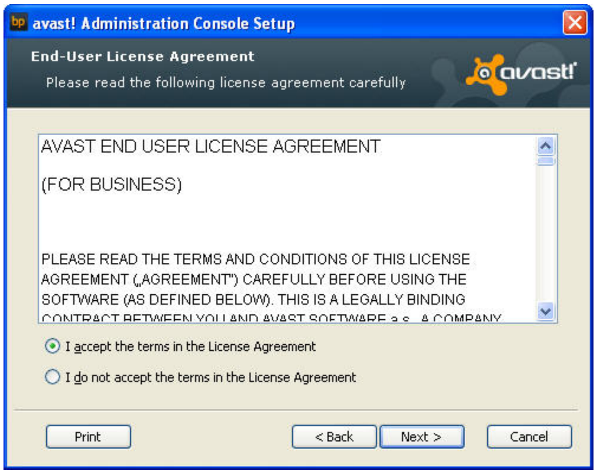
Saving to: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\windowsxp-kb942288-v3-x86.exe

Remaining time: 4 sec at 302 KB/sec

☑ Automatically install the prerequisites after finishing the downloads.

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

To continue with the installation, on the next screen select "I accept the terms in the License Agreement".



avast! Administration Console Setup

End-User License Agreement

Please read the following license agreement carefully

AVAST END USER LICENSE AGREEMENT

(FOR BUSINESS)

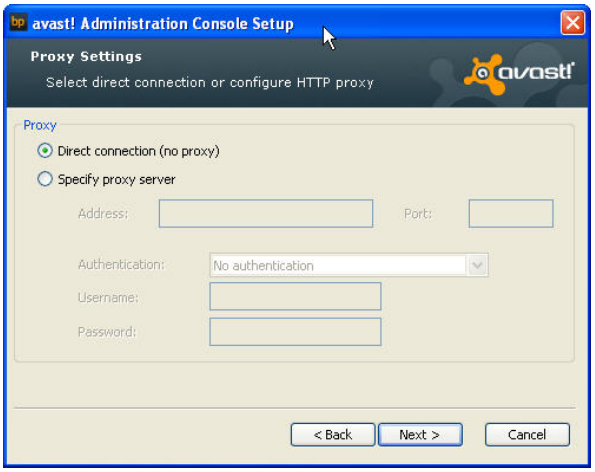
PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT („AGREEMENT") CAREFULLY BEFORE USING THE SOFTWARE (AS DEFINED BELOW). THIS IS A LEGALLY BINDING CONTRACT BETWEEN YOU AND AVAST SOFTWARE a.s., A COMPANY

● I accept the terms in the License Agreement

○ I do not 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.



avast! Administration Console Setup

Proxy Settings

Select direct connection or configure HTTP proxy

Proxy

● Direct connection (no proxy)

○ Specify proxy server

Address:

Port:

Authentication: No authentication

Username:

Password:

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!

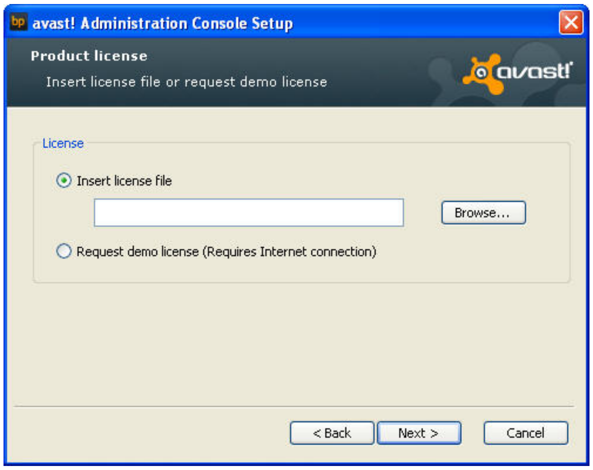
If you connect to the internet through a proxy server and you know the proxy server details, select "Specify proxy server" and enter the proxy details:

- 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:



avast! Administration Console Setup

Product license

Insert license file or request demo license

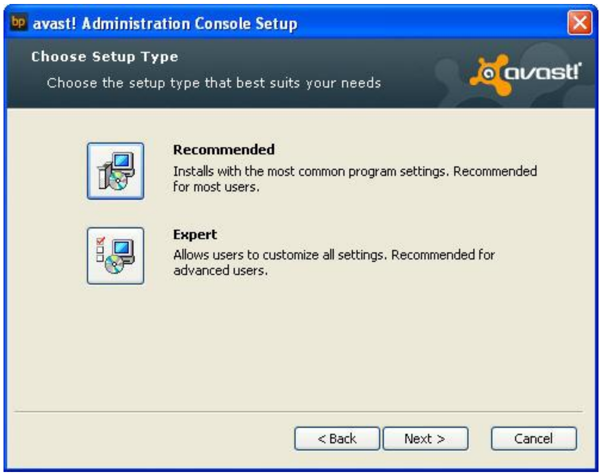
License

● Insert license file

○ Request demo license (Requires Internet connection)

- **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:



Choose Setup Type

Choose the setup type that best suits your needs

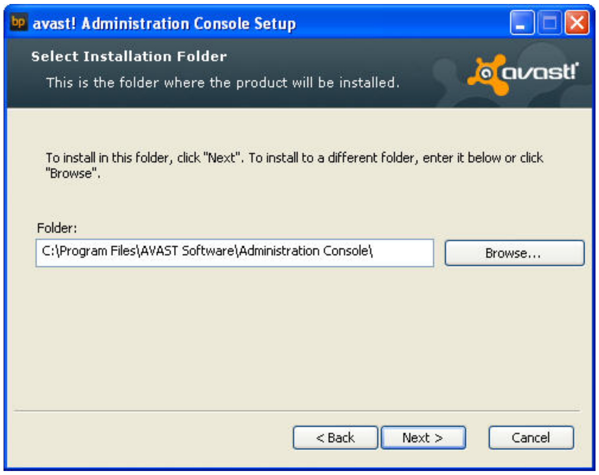
Recommended
Installs with the most common program settings. Recommended for most users.

Expert
Allows users to customize all settings. Recommended for advanced users.

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.



Select Installation Folder

This is the folder where the product will be installed.

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

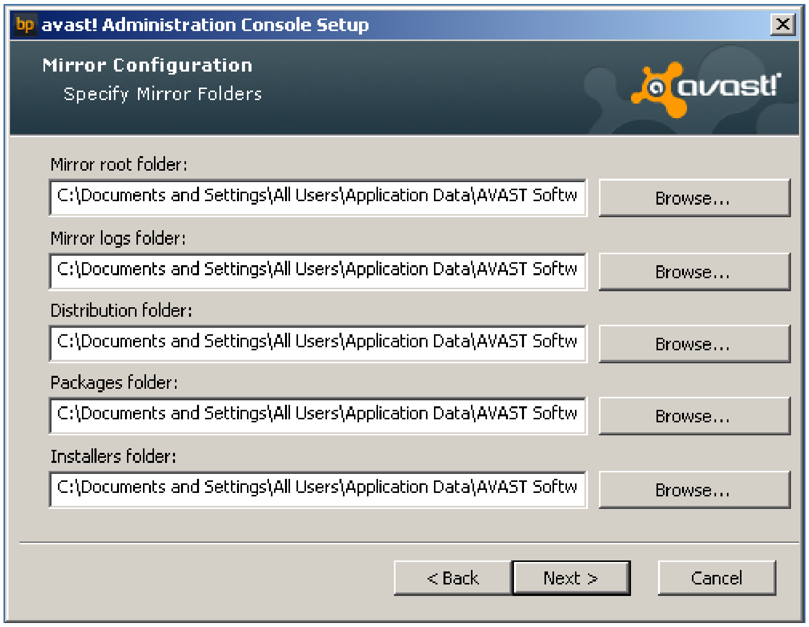
Folder:
C:\Program Files\AVAST Software\Administration Console\

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.



Mirror root folder: C:\Documents and Settings\All Users\Application Data\AVAST Softw

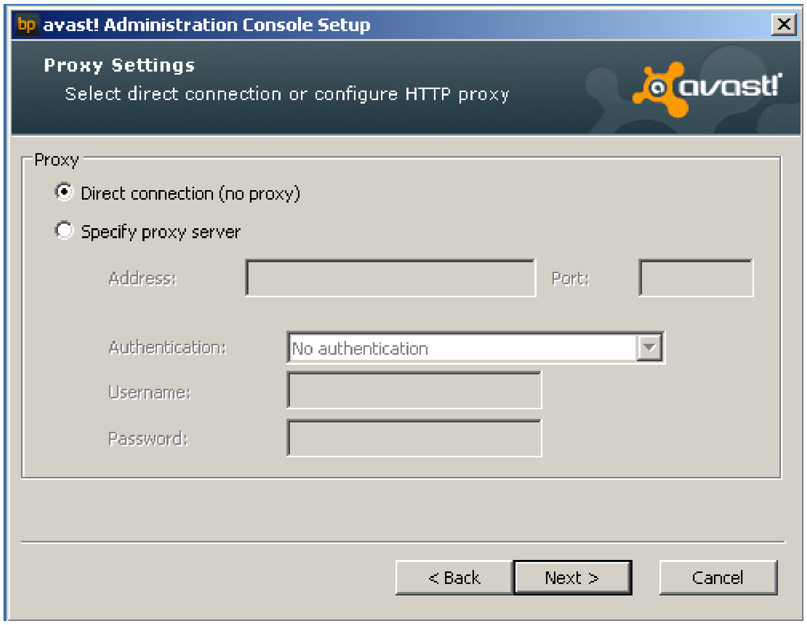
Mirror logs folder: C:\Documents and Settings\All Users\Application Data\AVAST Softw

Distribution folder: C:\Documents and Settings\All Users\Application Data\AVAST Softw

Packages folder: C:\Documents and Settings\All Users\Application Data\AVAST Softw

Installers folder: C:\Documents and Settings\All Users\Application Data\AVAST Softw

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


avast! Administration Console Setup
Proxy Settings
Select direct connection or configure HTTP proxy
avast!

Proxy

● Direct connection (no proxy)

○ Specify proxy server

Address: Port:

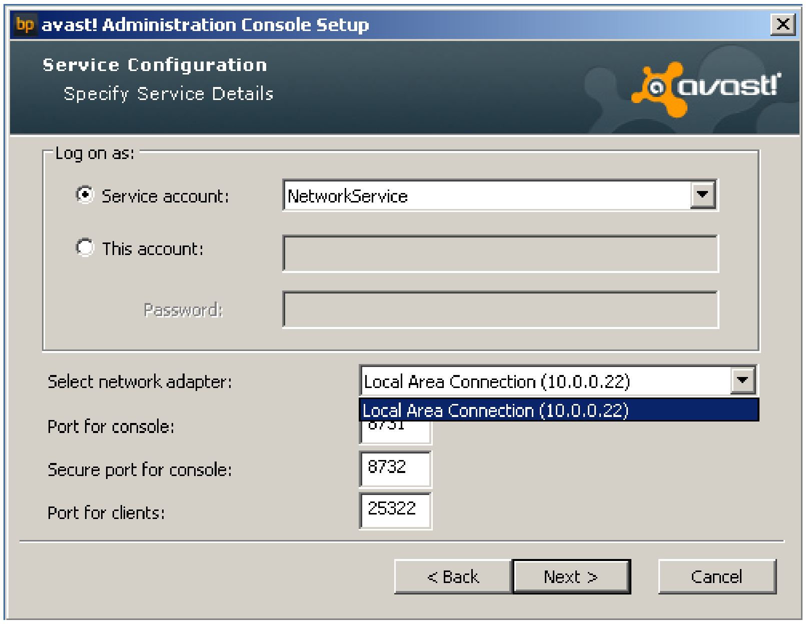
Authentication: No authentication

Username:

Password:

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.

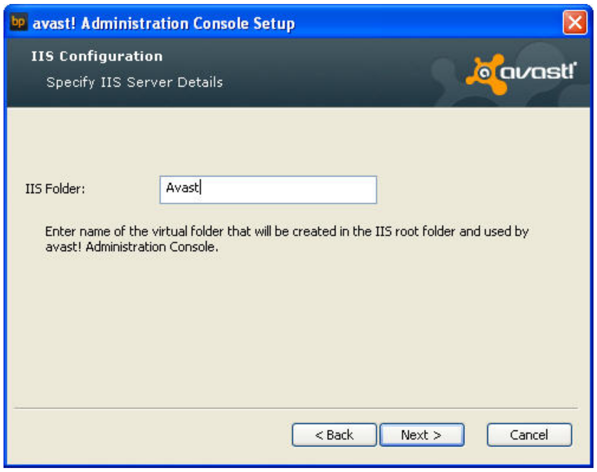


Service Configuration
Specify Service Details

Log on as:
● Service account: NetworkService
○ This account:
Password:

Select network adapter: Local Area Connection (10.0.0.22)
Port for console: 8731
Secure port for console: 8732
Port for clients: 25322

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



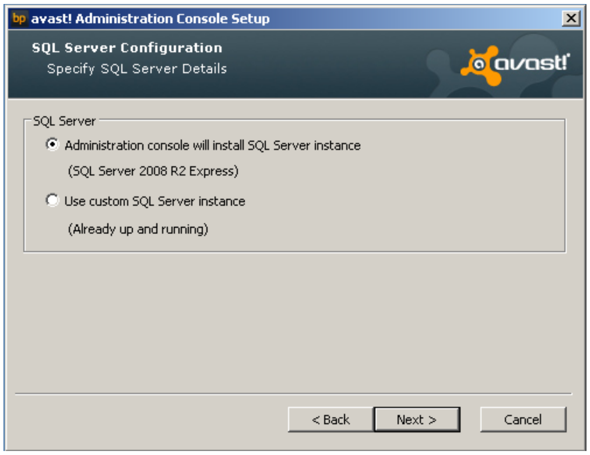
IIS Configuration
Specify IIS Server Details

IIS Folder: Avast

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

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.



avast! Administration Console Setup

SQL Server Configuration

Specify SQL Server Details

SQL Server

● Administration console will install SQL Server instance

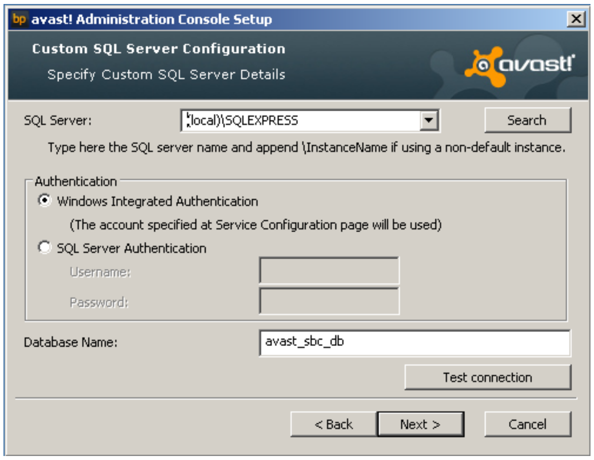
(SQL Server 2008 R2 Express)

○ Use custom SQL Server instance

(Already up and running)

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!



avast! Administration Console Setup

Custom SQL Server Configuration

Specify Custom SQL Server Details

SQL Server: (local)\SQLEXPRESS

Type here the SQL server name and append \InstanceName if using a non-default instance.

Authentication

● Windows Integrated Authentication

(The account specified at Service Configuration page will be used)

○ SQL Server Authentication

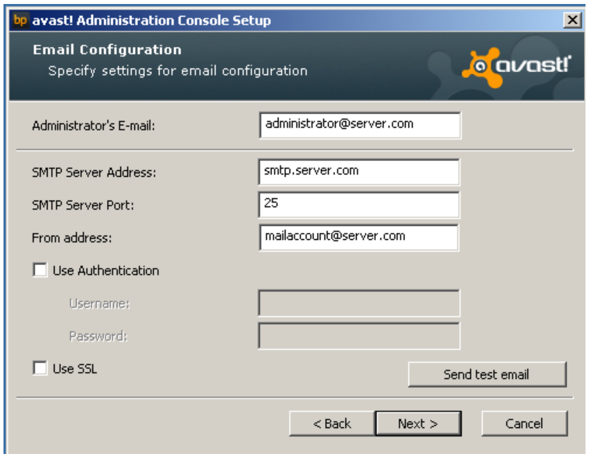
Username:

Password:

Database Name: avast_sbc_db

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.



avast! Administration Console Setup

Email Configuration

Specify settings for email configuration

Administrator's E-mail: administrator@server.com

SMTP Server Address: smtp.server.com

SMTP Server Port: 25

From address: mailaccount@server.com

☐ Use Authentication

Username:

Password:

☐ Use SSL

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

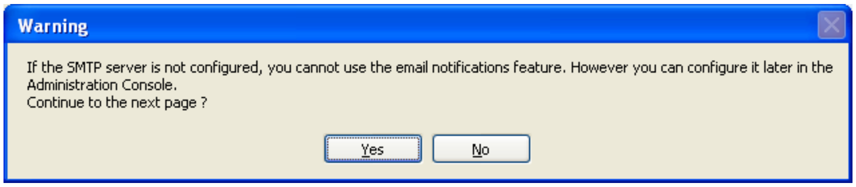
SMTP Server Port - the default is 25

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.

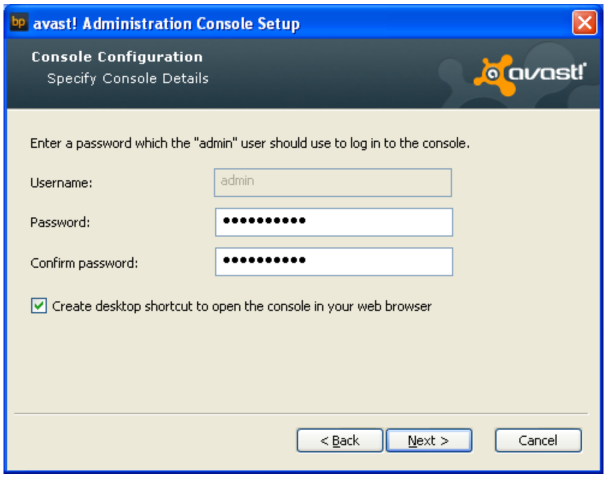
You can proceed without entering these details now, in which case you will see the following message:



Warning

If the SMTP server is not configured, you cannot use the email notifications feature. However you can configure it later in the Administration Console.
Continue to the next page ?

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:



Console Configuration

Specify Console Details

Enter a password which the "admin" user should use to log in to the console.

Username: admin

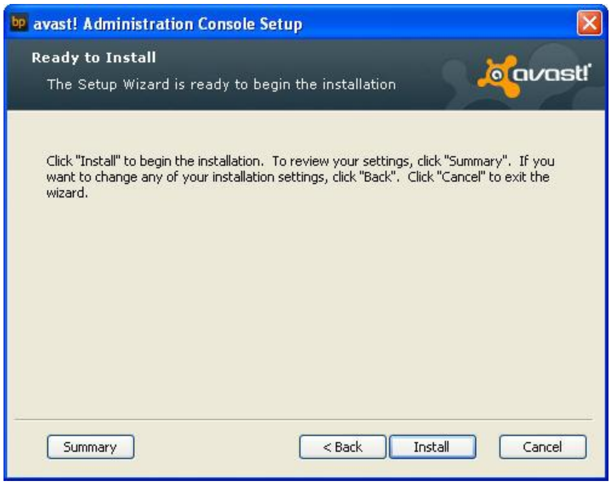
Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

☑ Create desktop shortcut to open the console in your web browser

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

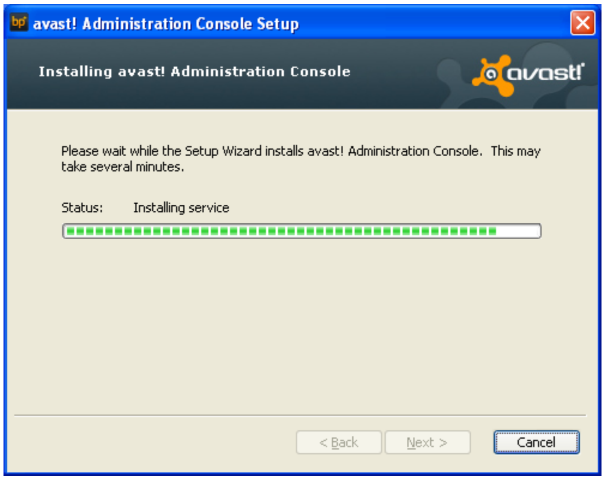
You will now see a final screen before the installation begins. To review all the initial setup details and to check everything is correct, just click on Summary. You can use the “Back” button to go back and make any changes and when you are ready just click “Install”



Ready to Install

The Setup Wizard is ready to begin the installation

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



avast! Administration Console Setup

Installing avast! Administration Console

Please wait while the Setup Wizard installs avast! Administration Console. This may take several minutes.

Status: Installing service

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

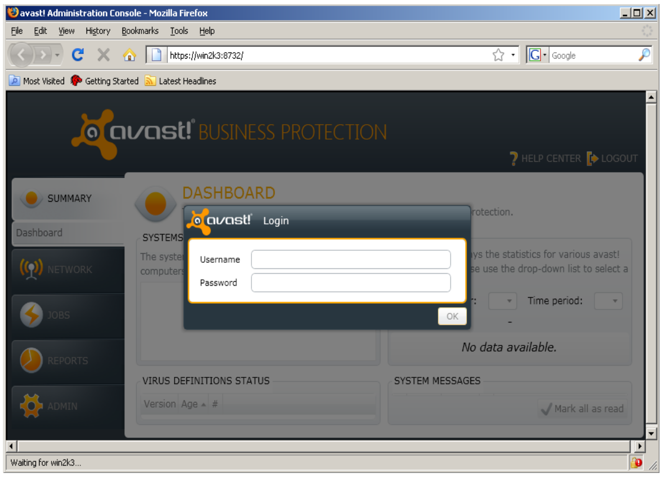
When the installation is complete, a new box will appear with a link, which you can click to open the Administration Console in your computer's web browser.

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

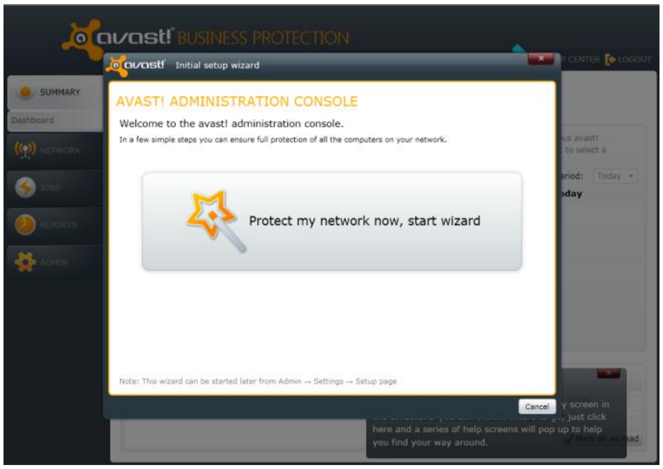
You can open the console via the shortcut installed on your desktop or by clicking the "Start" button in the bottom left corner of your computer screen and selecting "avast Administration Console" from the list of programs installed on your computer. You can also access the console from any other computer 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.



No data available.

When you open the Business Protection Console for the first time, you will first see the system "Dashboard" and the initial setup wizard:


avast! BUSINESS PROTECTION
avast! Initial setup wizard
SUMMARY
Dashboard
NETWORK
JOBS
REPORTS
ADMIN
AVAST! ADMINISTRATION CONSOLE
Protect my network now, start wizard
Cancel

Welcome to the avast! administration console.

In a few simple steps you can ensure full protection of all the computers on your network.

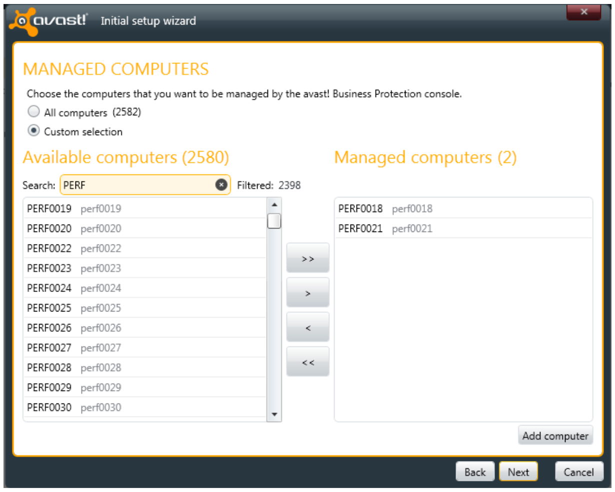
Note: This wizard can be started later from Admin → Settings → Setup page

here and a series of help screens will pop up to help you find your way around.

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.



avast! Initial setup wizard

MANAGED COMPUTERS

Choose the computers that you want to be managed by the avast! Business Protection console.

○ All computers (2582)

● Custom selection

Available computers (2580)

Search: PERF Filtered: 2398

PERF0019	perf0019
PERF0020	perf0020
PERF0022	perf0022
PERF0023	perf0023
PERF0024	perf0024
PERF0025	perf0025
PERF0026	perf0026
PERF0027	perf0027
PERF0028	perf0028
PERF0029	perf0029
PERF0030	perf0030

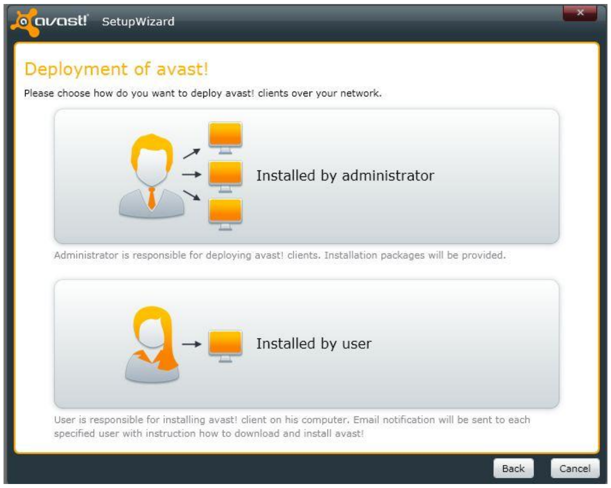
Managed computers (2)

PERF0018	perf0018
PERF0021	perf0021

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



avast! SetupWizard

Deployment of avast!

Please choose how do you want to deploy avast! clients over your network.

Installed by administrator

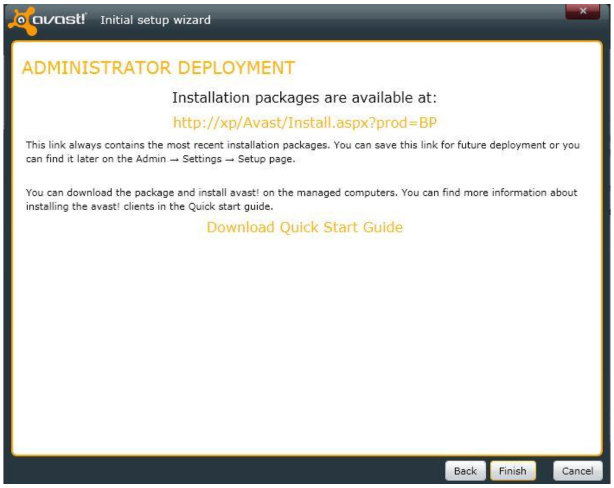
Administrator is responsible for deploying avast! clients. Installation packages will be provided.

Installed by user

User is responsible for installing avast! client on his computer. Email notification will be sent to each specified user with instruction how to download and install avast!

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:



ADMINISTRATOR DEPLOYMENT

Installation packages are available at:

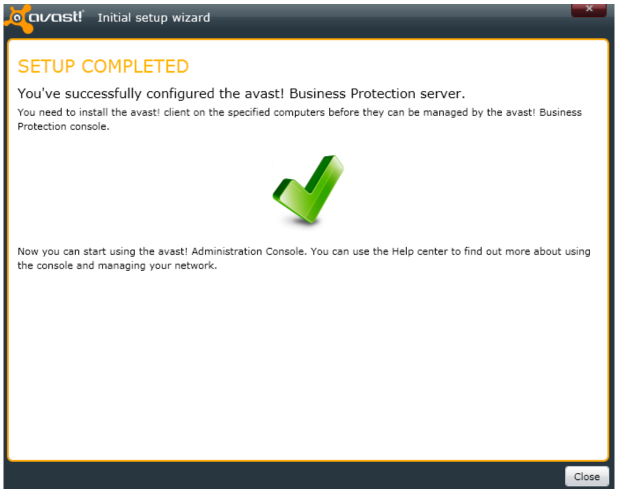
http://xp/Avast/Install.aspx?prod=BP

This link always contains the most recent installation packages. You can save this link for future deployment or you can find it later on the Admin → Settings → Setup page.

You can download the package and install avast! on the managed computers. You can find more information about installing the avast! clients in the Quick start guide.

Download Quick Start Guide

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



SETUP COMPLETED

You've successfully configured the avast! Business Protection server.

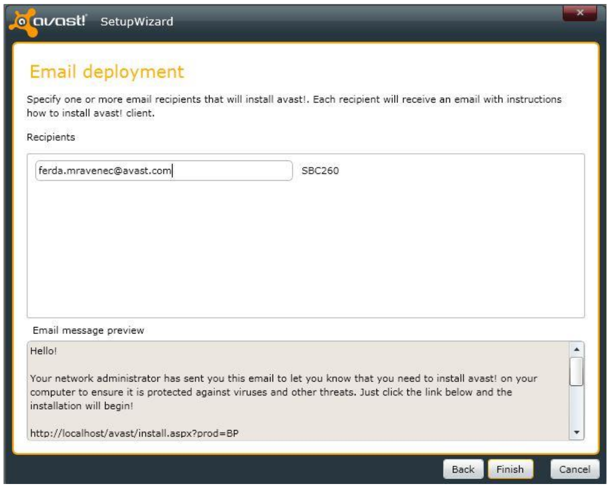
You need to install the avast! client on the specified computers before they can be managed by the avast! Business Protection console.

Now you can start using the avast! Administration Console. You can use the Help center to find out more about using the console and managing your network.

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.



Email deployment

Specify one or more email recipients that will install avast!. Each recipient will receive an email with instructions how to install avast! client.

Recipients

ferda.mravenec@avast.com SBC260

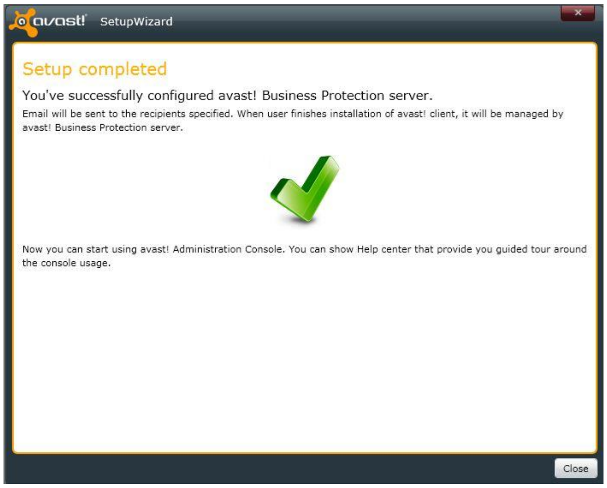
Email message preview

Hello!

Your network administrator has sent you this email to let you know that you need to install avast! on your computer to ensure it is protected against viruses and other threats. Just click the link below and the installation will begin!

http://localhost/avast/install.aspx?prod=BP

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



Setup completed

You've successfully configured avast! Business Protection server.

Email will be sent to the recipients specified. When user finishes installation of avast! client, it will be managed by avast! Business Protection server.

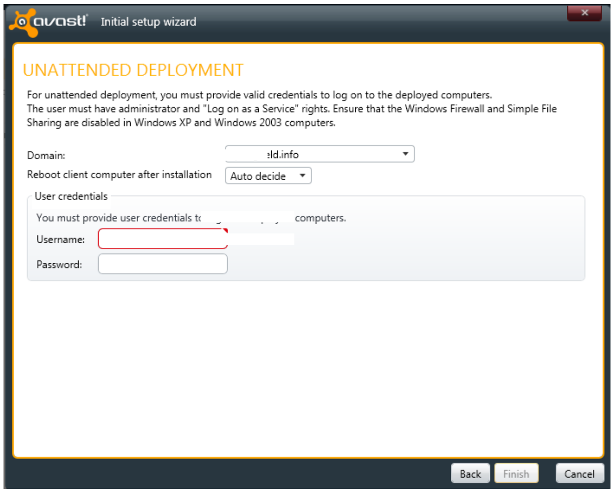
Now you can start using avast! Administration Console. You can show Help center that provide you guided tour around the console usage.

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: ********



UNATTENDED DEPLOYMENT

For unattended deployment, you must provide valid credentials to log on to the deployed computers.
The user must have administrator and "Log on as a Service" rights. Ensure that the Windows Firewall and Simple File Sharing are disabled in Windows XP and Windows 2003 computers.

Domain: ld.info

Reboot client computer after installation: Auto decide

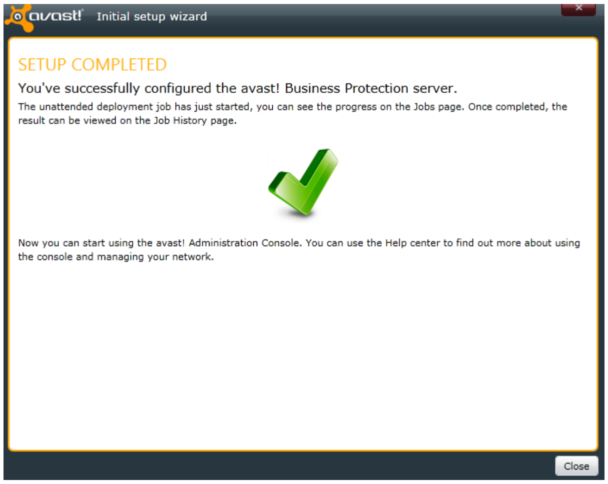
User credentials

You must provide user credentials t computers.

Username:

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:



SETUP COMPLETED

You've successfully configured the avast! Business Protection server.

The unattended deployment job has just started, you can see the progress on the Jobs page. Once completed, the result can be viewed on the Job History page.

Now you can start using the avast! Administration Console. You can use the Help center to find out more about using the console and managing your network.

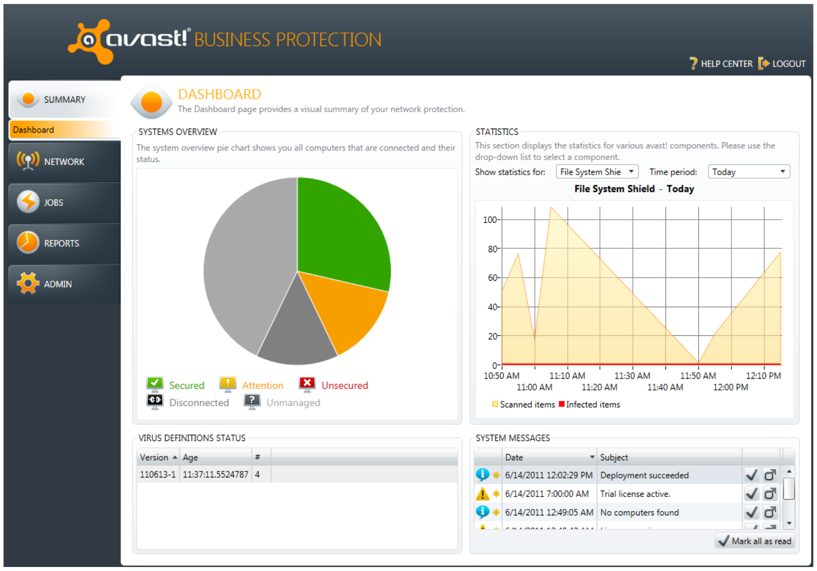
You can check the progress of the installation on the Jobs screen of the Administration Console and once completed, you can see the result on the Job History screen.

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.



The Dashboard page provides a visual summary of your network protection.

The system overview pie chart shows you all computers that are connected and their status.

This section displays the statistics for various avast! components. Please use the drop-down list to select a component.

Show statistics for: File System Shie

Time period: Today

Version	Age	#
110613-1	11:37:11.5524787	4

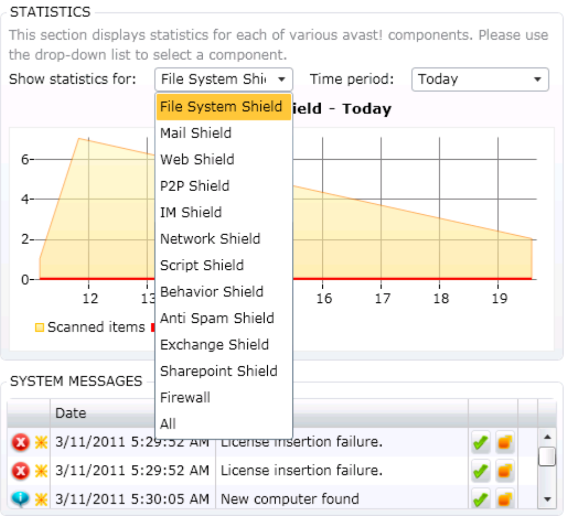
Date	Subject
6/14/2011 12:02:29 PM	Deployment succeeded
6/14/2011 7:00:00 AM	Trial license active.
6/14/2011 12:49:05 AM	No computers found

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.



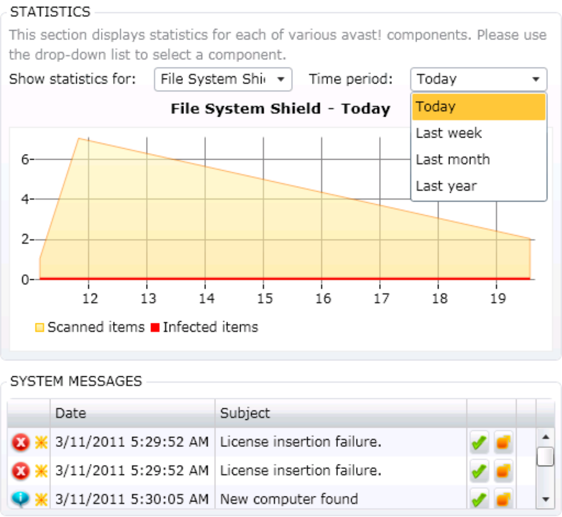
STATISTICS

This section displays statistics for each of various avast! components. Please use the drop-down list to select a component.

Show statistics for: File System Shi Time period: Today

SYSTEM MESSAGES

	Date	
	3/11/2011 5:29:52 AM	License insertion failure.
	3/11/2011 5:29:52 AM	License insertion failure.
	3/11/2011 5:30:05 AM	New computer found



STATISTICS

This section displays statistics for each of various avast! components. Please use the drop-down list to select a component.

Show statistics for: File System Shi Time period: Today

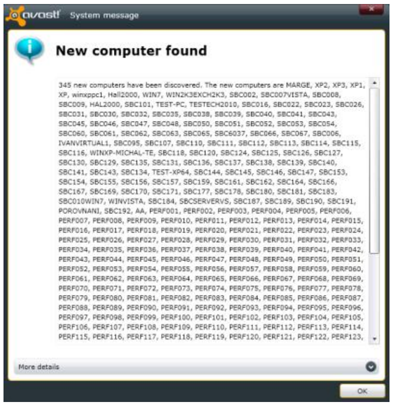
SYSTEM MESSAGES

Date	Subject
3/11/2011 5:29:52 AM	License insertion failure.
3/11/2011 5:29:52 AM	License insertion failure.
3/11/2011 5:30:05 AM	New computer found

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..

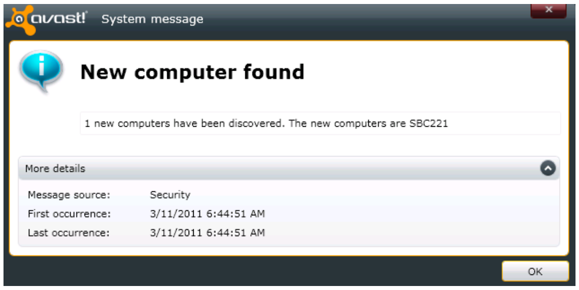
- If you want to see more details about a specific system message, simply double click on it. See the new detailed information window below.



New computer found

345 new computers have been discovered. The new computers are MARGE, XP2, XP3, XP1, XP, winxppc1, Hall2000, WIN7, WIN2K3EXCH2K3, SBC002, SBC007VISTA, SBC008, SBC009, HAL2000, SBC101, TEST-PC, TESTECH2010, SBC016, SBC022, SBC023, SBC026, SBC031, SBC030, SBC032, SBC035, SBC038, SBC039, SBC040, SBC041, SBC043, SBC045, SBC046, SBC047, SBC048, SBC050, SBC051, SBC052, SBC053, SBC054, SBC060, SBC061, SBC062, SBC063, SBC065, SBC6037, SBC066, SBC067, SBC006, IVANVIRTUAL1, SBC095, SBC107, SBC110, SBC111, SBC112, SBC113, SBC114, SBC115, SBC116, WINXP-MICHAL-TE, SBC118, SBC120, SBC124, SBC125, SBC126, SBC127, SBC130, SBC129, SBC135, SBC131, SBC136, SBC137, SBC138, SBC139, SBC140, SBC141, SBC143, SBC134, TEST-XP64, SBC144, SBC145, SBC146, SBC147, SBC153, SBC154, SBC155, SBC156, SBC157, SBC159, SBC161, SBC162, SBC164, SBC166, SBC167, SBC169, SBC170, SBC171, SBC177, SBC178, SBC180, SBC181, SBC183, SBC010WIN7, WINVISTA, SBC184, SBCSERVERVS, SBC187, SBC189, SBC190, SBC191, POROVNANI, SBC192, AA, PERF001, PERF002, PERF003, PERF004, PERF005, PERF006, PERF007, PERF008, PERF009, PERF010, PERF011, PERF012, PERF013, PERF014, PERF015, PERF016, PERF017, PERF018, PERF019, PERF020, PERF021, PERF022, PERF023, PERF024, PERF025, PERF026, PERF027, PERF028, PERF029, PERF030, PERF031, PERF032, PERF033, PERF034, PERF035, PERF036, PERF037, PERF038, PERF039, PERF040, PERF041, PERF042, PERF043, PERF044, PERF045, PERF046, PERF047, PERF048, PERF049, PERF050, PERF051, PERF052, PERF053, PERF054, PERF055, PERF056, PERF057, PERF058, PERF059, PERF060, PERF061, PERF062, PERF063, PERF064, PERF065, PERF066, PERF067, PERF068, PERF069, PERF070, PERF071, PERF072, PERF073, PERF074, PERF075, PERF076, PERF077, PERF078, PERF079, PERF080, PERF081, PERF082, PERF083, PERF084, PERF085, PERF086, PERF087, PERF088, PERF089, PERF090, PERF091, PERF092, PERF093, PERF094, PERF095, PERF096, PERF097, PERF098, PERF099, PERF100, PERF101, PERF102, PERF103, PERF104, PERF105, PERF106, PERF107, PERF108, PERF109, PERF110, PERF111, PERF112, PERF113, PERF114, PERF115, PERF116, PERF117, PERF118, PERF119, PERF120, PERF121, PERF122, PERF123,

- 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.



New computer found

1 new computers have been discovered. The new computers are SBC221

More details

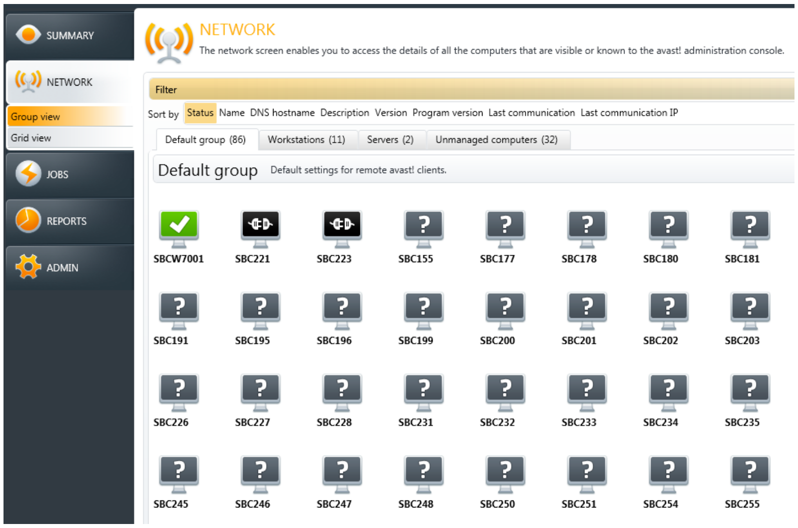
Message source: Security

First occurrence: 3/11/2011 6:44:51 AM

Last occurrence: 3/11/2011 6:44:51 AM

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:



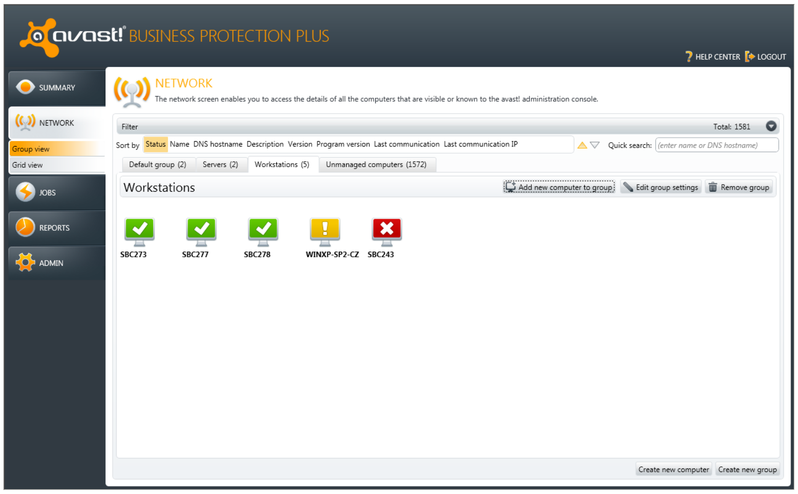
The network screen enables you to access the details of all the computers that are visible or known to the avast! administration console.

Default settings for remote avast! clients.

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):



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

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.

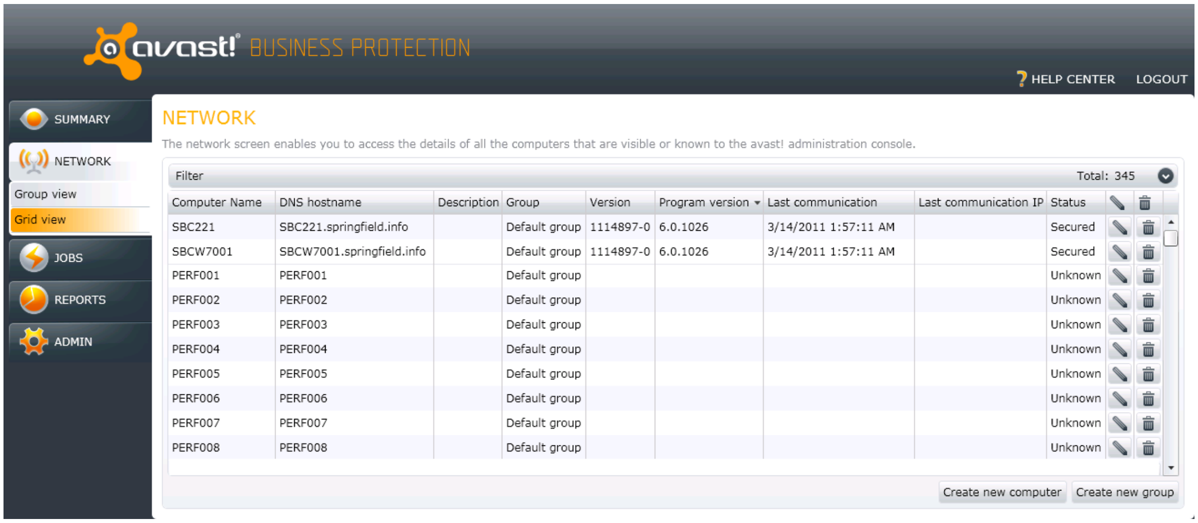
🔌 This icon indicates that the computer hasn't communicated with the Administration console recently (the default value is 30 seconds). This doesn't necessarily mean anything bad. e.g. computers that are turned off will have this icon.

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



NETWORK

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

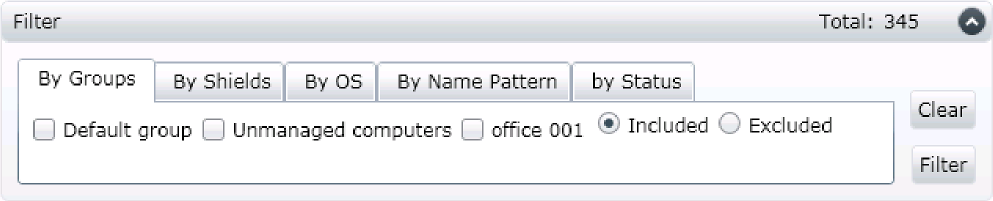
Filter Total: 345

Computer Name	DNS hostname	Description	Group	Version	Program version	Last communication	Last communication IP	Status	✎	🗑
SBC221	SBC221.springfield.info		Default group	1114897-0	6.0.1026	3/14/2011 1:57:11 AM		Secured	✎	🗑
SBCW7001	SBCW7001.springfield.info		Default group	1114897-0	6.0.1026	3/14/2011 1:57:11 AM		Secured	✎	🗑
PERF001	PERF001		Default group					Unknown	✎	🗑
PERF002	PERF002		Default group					Unknown	✎	🗑
PERF003	PERF003		Default group					Unknown	✎	🗑
PERF004	PERF004		Default group					Unknown	✎	🗑
PERF005	PERF005		Default group					Unknown	✎	🗑
PERF006	PERF006		Default group					Unknown	✎	🗑
PERF007	PERF007		Default group					Unknown	✎	🗑
PERF008	PERF008		Default group					Unknown	✎	🗑

- 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

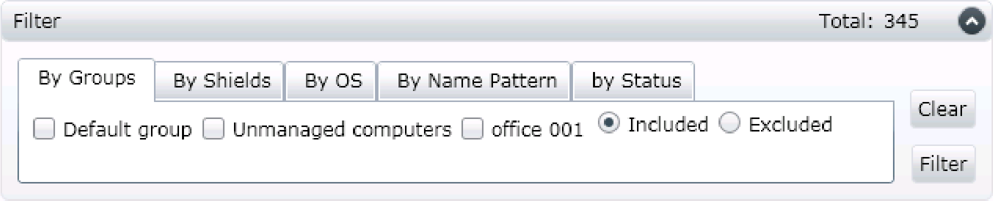
Advanced filtering is possible by Groups, Shields, OS, Name pattern and Status.



Filter Total: 345

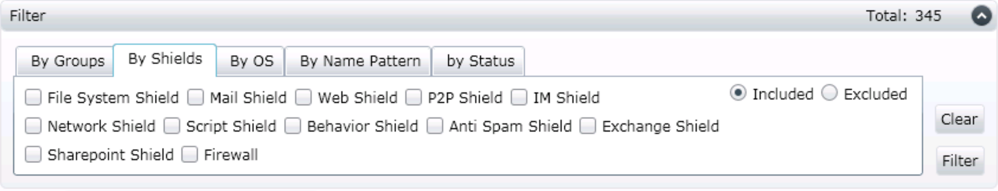
□ Default group □ Unmanaged computers □ office 001 ● Included ○ Excluded

Filtering by Groups



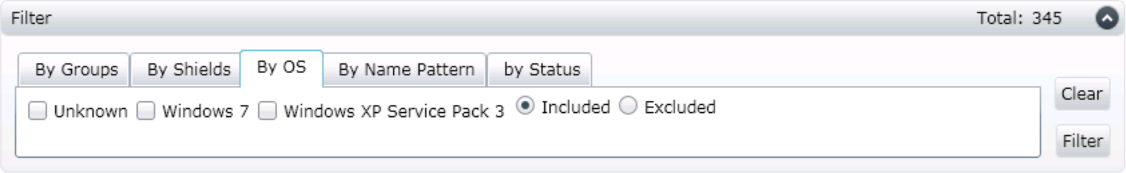
- Contains a list of all default and custom created groups (computer groups)
- Tick or untick required group/s to display your custom Group or Grid view

Filtering by Shields


Filter
Total: 345
By Groups
By Shields
By OS
By Name Pattern
by Status
□ File System Shield □ Mail Shield □ Web Shield □ P2P Shield □ IM Shield
□ Network Shield □ Script Shield □ Behavior Shield □ Anti Spam Shield □ Exchange Shield
□ Sharepoint Shield □ Firewall
● Included ○ Excluded
Clear
Filter

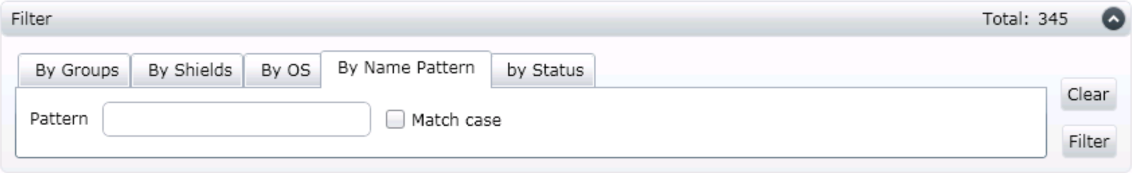
- Contains a list of all avast! components, such as File system shield, Mail shield, Web shield, P2P shield ..
- Tick or untick the required component to display/filter your custom Group or Grid view.

Filtering by Operating System



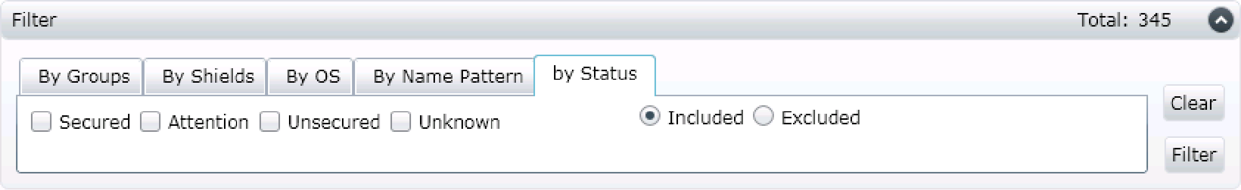
- Contains a list of all found OS's installed on all computers visible to the avast! Administration console
- Tick or untick the required OS to display/filter your custom Group or Grid view

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

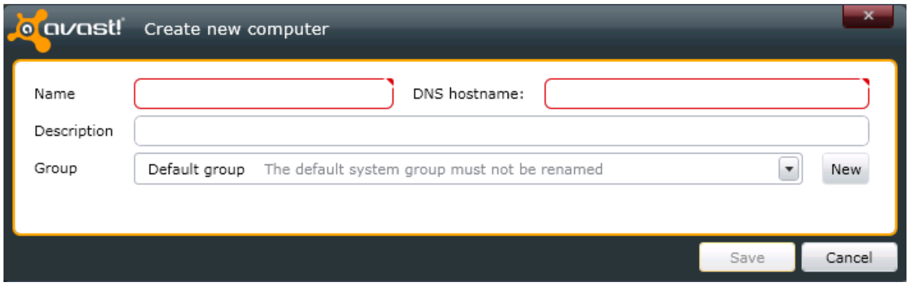


- Contains a list of the statuses of all computers visible to the avast! Administration console, such as Secured, Attention, Unsecured, Unknown.
- Tick or untick the required status to display/filter your custom Group or Grid view

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:



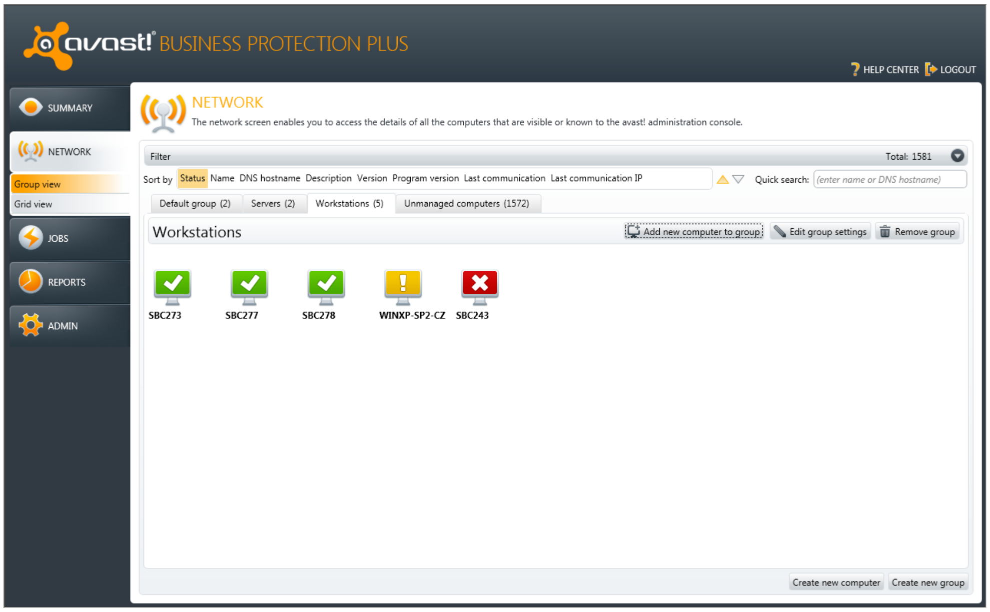
Group: Default group The default system group must not be renamed

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

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

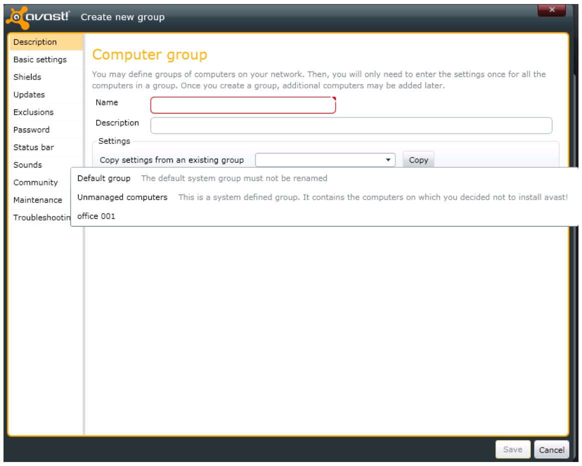
Creating a New Group

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



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

This will open the following new window:



Computer group

You may define groups of computers on your network. Then, you will only need to enter the settings once for all the computers in a group. Once you create a group, additional computers may be added later.

Default group — The default system group must not be renamed

Unmanaged computers — This is a system defined group. It contains the computers on which you decided not to install avast!

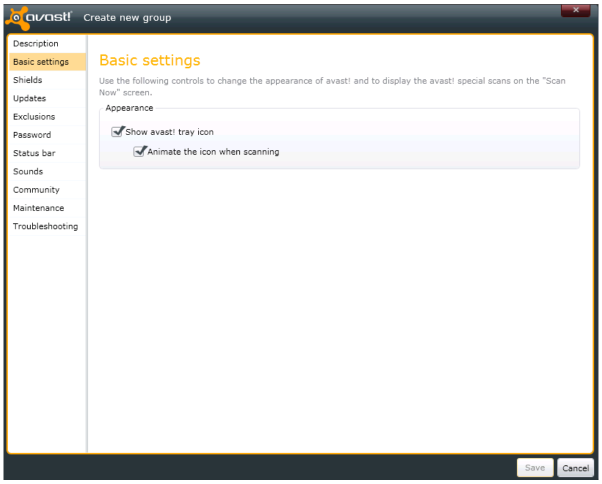
office 001

- 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



Basic settings

Use the following controls to change the appearance of avast! and to display the avast! special scans on the "Scan Now" screen.

Appearance

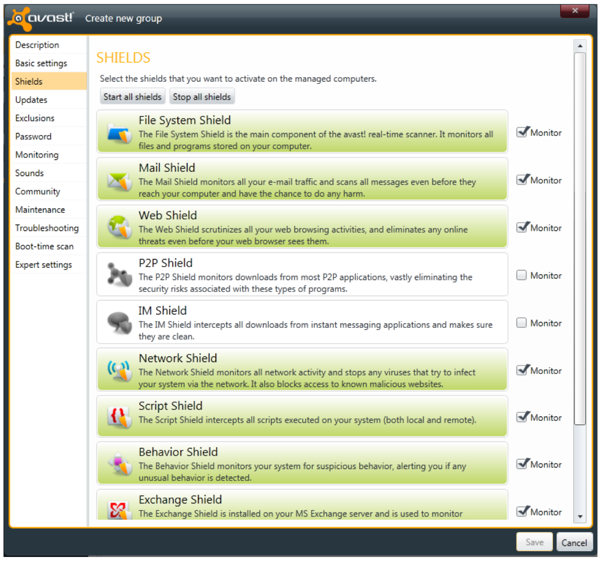
☑ Show avast! tray icon

☑ Animate the icon when scanning

- 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.



SHIELDS

Select the shields that you want to activate on the managed computers.

File System Shield
The File System Shield is the main component of the avast! real-time scanner. It monitors all files and programs stored on your computer. ☑ Monitor

Mail Shield
The Mail Shield monitors all your e-mail traffic and scans all messages even before they reach your computer and have the chance to do any harm. ☑ Monitor

Web Shield
The Web Shield scrutinizes all your web browsing activities, and eliminates any online threats even before your web browser sees them. ☑ Monitor

P2P Shield
The P2P Shield monitors downloads from most P2P applications, vastly eliminating the security risks associated with these types of programs. □ Monitor

IM Shield
The IM Shield intercepts all downloads from instant messaging applications and makes sure they are clean. □ Monitor

Network Shield
The Network Shield monitors all network activity and stops any viruses that try to infect your system via the network. It also blocks access to known malicious websites. ☑ Monitor

Script Shield
The Script Shield intercepts all scripts executed on your system (both local and remote). ☑ Monitor

Behavior Shield
The Behavior Shield monitors your system for suspicious behavior, alerting you if any unusual behavior is detected. ☑ Monitor

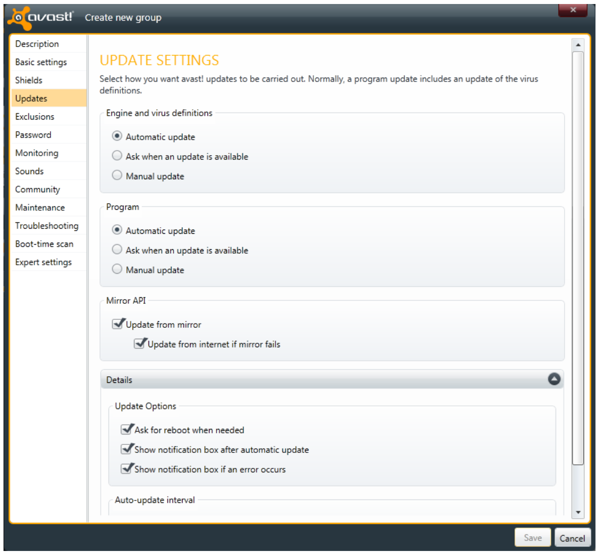
Exchange Shield
The Exchange Shield is installed on your MS Exchange server and is used to monitor ☑ Monitor

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

Select how you want avast! updates to be carried out. Normally, a program update includes an update of the virus definitions.

Engine and virus definitions

● Automatic update
○ Ask when an update is available
○ Manual update

Program

● Automatic update
○ Ask when an update is available
○ Manual update

Mirror API

☑ Update from mirror
☑ Update from internet if mirror fails

Details

Update Options

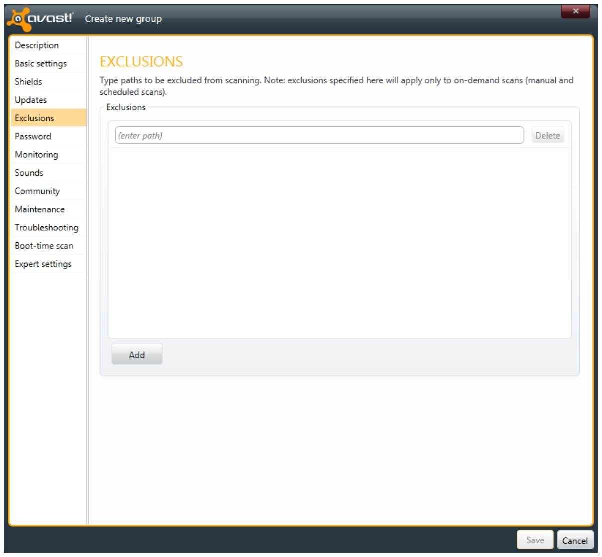
☑ Ask for reboot when needed
☑ Show notification box after automatic update
☑ Show notification box if an error occurs

Auto-update interval

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



EXCLUSIONS

Type paths to be excluded from scanning. Note: exclusions specified here will apply only to on-demand scans (manual and scheduled scans).

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.

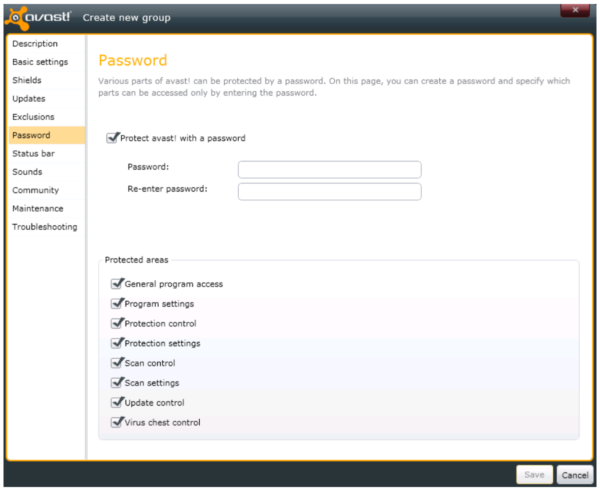
To exclude a location or file, first click the box where it says <enter path> and then type either the location or file to be excluded.

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.



Password

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

☑ Protect avast! with a password

Password:

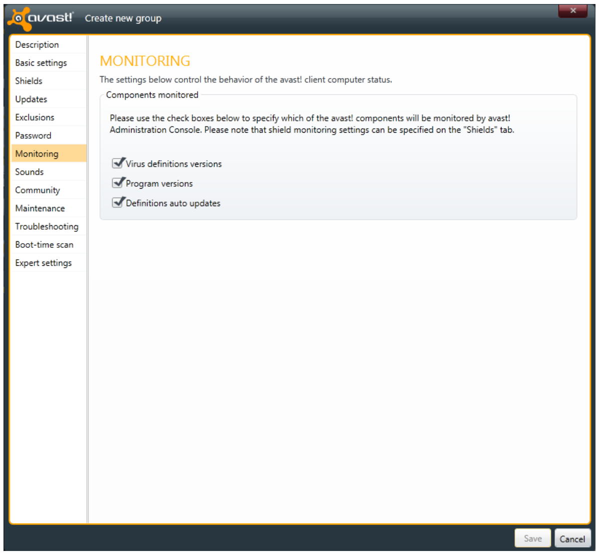
Re-enter password:

Protected areas

☑ General program access
☑ Program settings
☑ Protection control
☑ Protection settings
☑ Scan control
☑ Scan settings
☑ Update control
☑ Virus chest control

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.



MONITORING

The settings below control the behavior of the avast! client computer status.

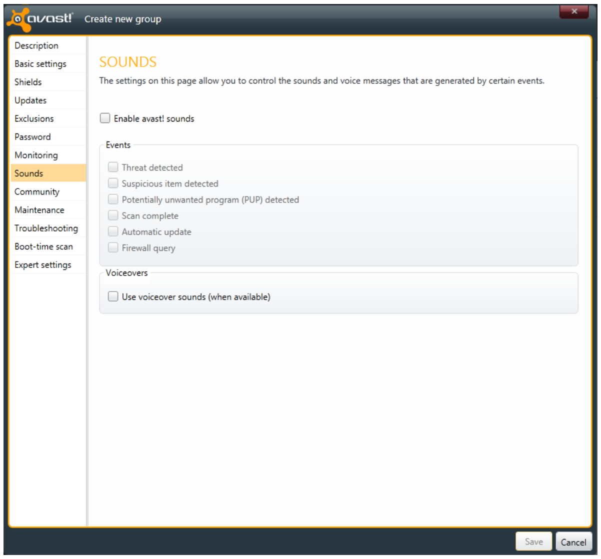
Components monitored

Please use the check boxes below to specify which of the avast! components will be monitored by avast! Administration Console. Please note that shield monitoring settings can be specified on the "Shields" tab.

☑ Virus definitions versions
☑ Program versions
☑ Definitions auto updates

Sounds

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



SOUNDS

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

☐ Enable avast! sounds

Events

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

Voiceovers

☐ Use voiceover sounds (when available)

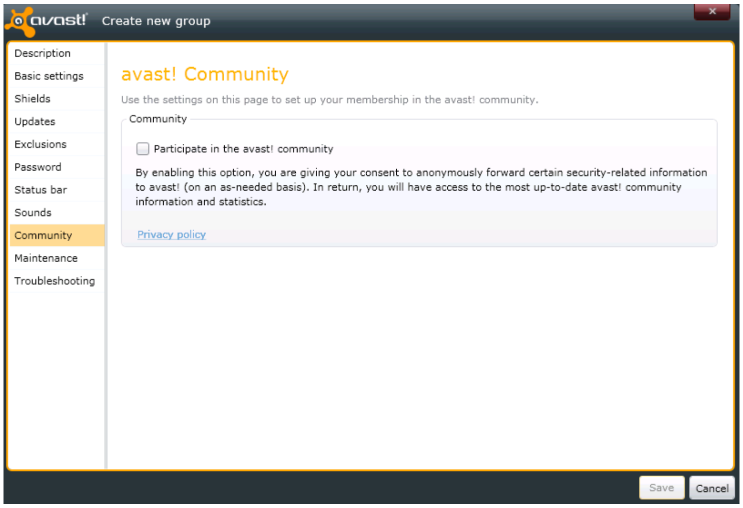
The various events that can trigger an audible sound or voice message are:

- 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.



avast! Community

Use the settings on this page to set up your membership in the avast! community.

Community

□ Participate in the avast! community

By enabling this option, you are giving your consent to anonymously forward certain security-related information to avast! (on an as-needed basis). In return, you will have access to the most up-to-date avast! community information and statistics.

Privacy policy

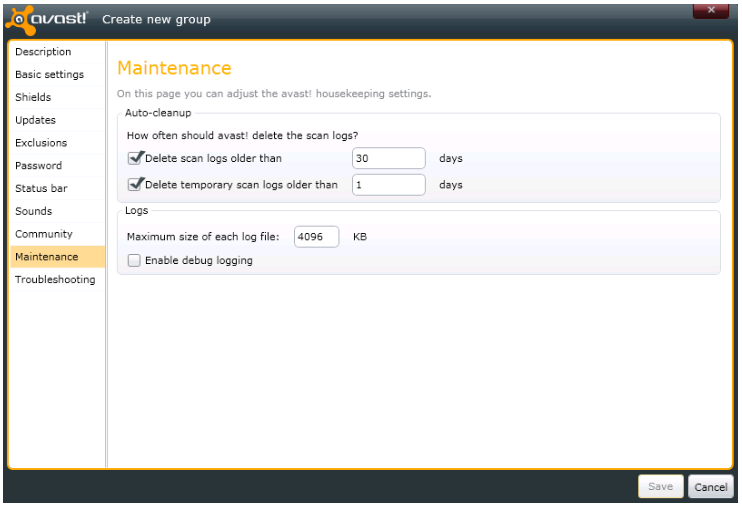
By participating in the avast! community, you will also have access to all the community information and statistics about the latest malware attacks.

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.



Maintenance

On this page you can adjust the avast! housekeeping settings.

Auto-cleanup

How often should avast! delete the scan logs?

☑ Delete scan logs older than 30 days

☑ Delete temporary scan logs older than 1 days

Logs

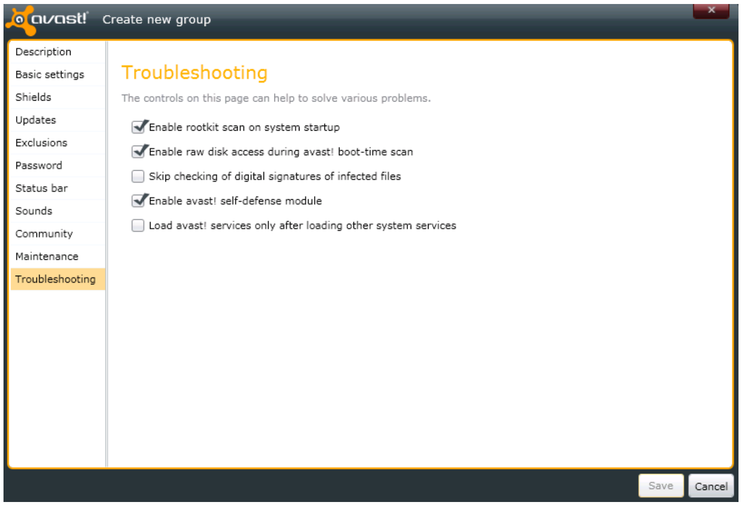
Maximum size of each log file: 4096 KB

☐ Enable debug logging

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



Troubleshooting

The controls on this page can help to solve various problems.

☑ Enable rootkit scan on system startup
☑ Enable raw disk access during avast! boot-time scan
□ Skip checking of digital signatures of infected files
☑ Enable avast! self-defense module
□ Load avast! services only after loading other system services

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.

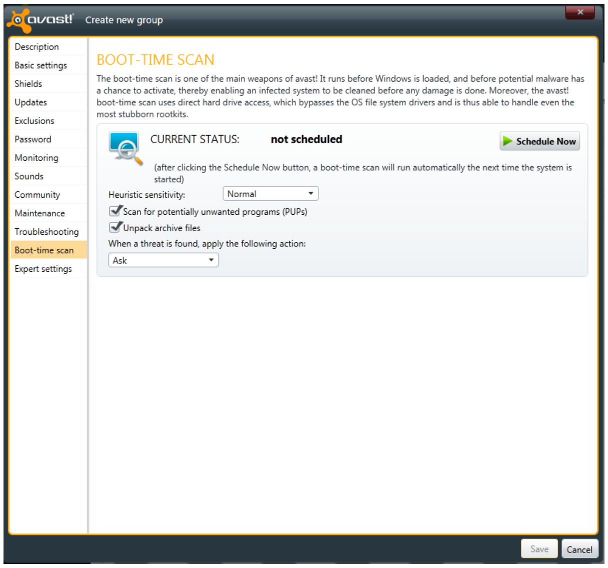
- **Skip checking of digital signatures of infected files**
  To prevent false positive alerts, avast! checks files for digital signatures. If a file is detected as suspicious, but also contains a valid digital signature of a trusted authority, it is likely to be a false positive. In this case the file 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

The boot-time scan is one of the main weapons of avast! It runs before Windows is loaded, and before potential malware has a chance to activate, thereby enabling an infected system to be cleaned before any damage is done. Moreover, the avast! boot-time scan uses direct hard drive access, which bypasses the OS file system drivers and is thus able to handle even the most stubborn rootkits.

CURRENT STATUS: **not scheduled**

(after clicking the Schedule Now button, a boot-time scan will run automatically the next time the system is started)

Heuristic sensitivity: Normal

☑ Scan for potentially unwanted programs (PUPs)

☑ Unpack archive files

When a threat is found, apply the following action: Ask

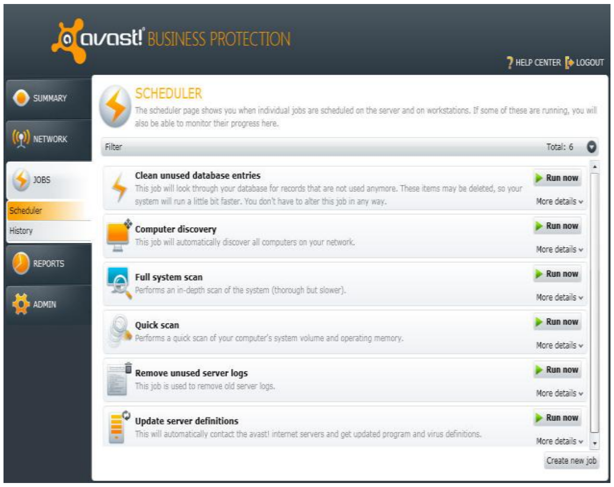
By default, the program automatically scans for potentially unwanted programs and also scans inside archive files, but either of these features can be turned off by unchecking the relevant checkbox.

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 clickling 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.



SCHEDULER

The scheduler page shows you when individual jobs are scheduled on the server and on workstations. If some of these are running, you will also be able to monitor their progress here.

Clean unused database entries
This job will look through your database for records that are not used anymore. These items may be deleted, so your system will run a little bit faster. You don't have to alter this job in any way.

Computer discovery
This job will automatically discover all computers on your network.

Full system scan
Performs an in-depth scan of the system (thorough but slower).

Quick scan
Performs a quick scan of your computer's system volume and operating memory.

Remove unused server logs
This job is used to remove old server logs.

Update server definitions
This will automatically contact the avast! internet servers and get updated program and virus definitions.

Create a new job

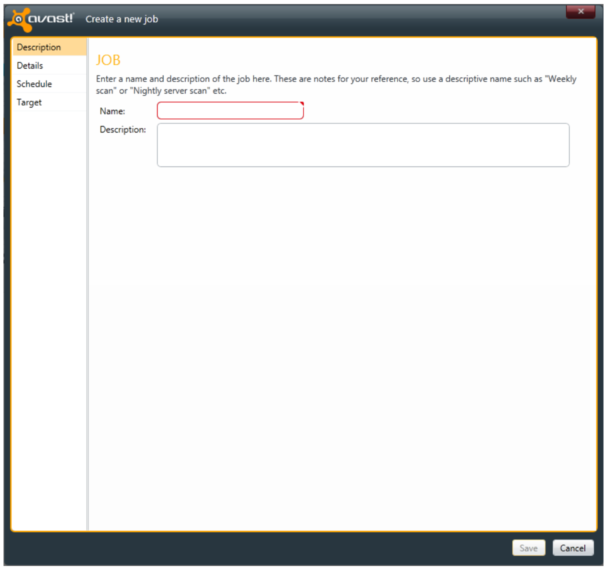
The Console is installed with a number of pre-defined jobs, however, by clicking on the "Create new job" button, you can define a completely new job with its own parameters. Any new job that is created, or any of the pre-defined jobs can be run at any time simply by clicking the “Start” button on the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



JOB

Enter a name and description of the job here. These are notes for your reference, so use a descriptive name such as "Weekly scan" or "Nightly server scan" etc.

Name:

Description:

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

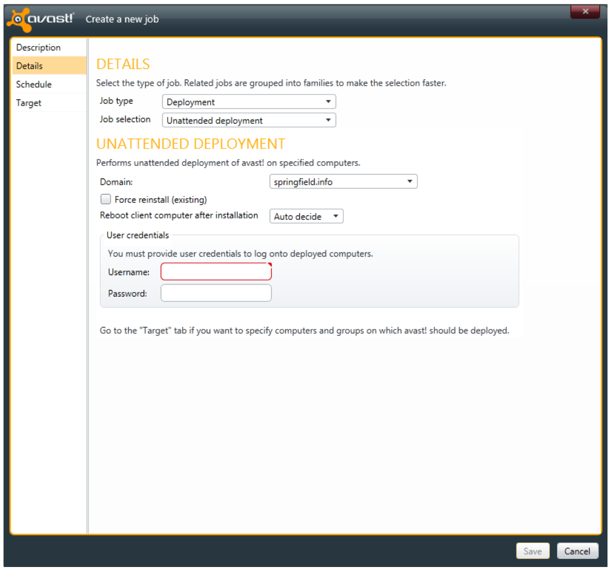
- Discover new computers using Active Directory
- Discover new computers in the network neighborhood

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**”.



DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Deployment

Job selection: Unattended deployment

UNATTENDED DEPLOYMENT

Performs unattended deployment of avast! on specified computers.

Domain: springfield.info

□ Force reinstall (existing)

Reboot client computer after installation: Auto decide

User credentials

You must provide user credentials to log onto deployed computers.

Username:

Password:

Go to the "Target" tab if you want to specify computers and groups on which avast! should be deployed.

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.

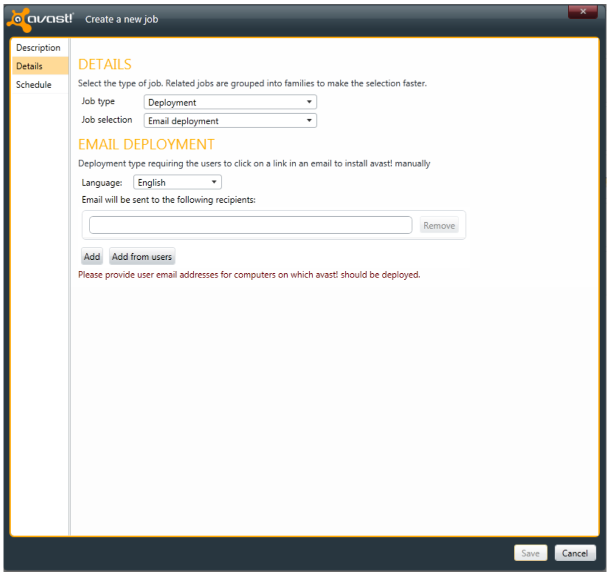
Reboot client computer after installation – if “**Auto-decide**” is selected, each client computer will be automatically restarted only if a reboot is needed to complete the installation, for example in the case of Business Protection, if a previous installation has been replaced or in the case of Business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



DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Deployment

Job selection: Email deployment

EMAIL DEPLOYMENT

Deployment type requiring the users to click on a link in an email to install avast! manually

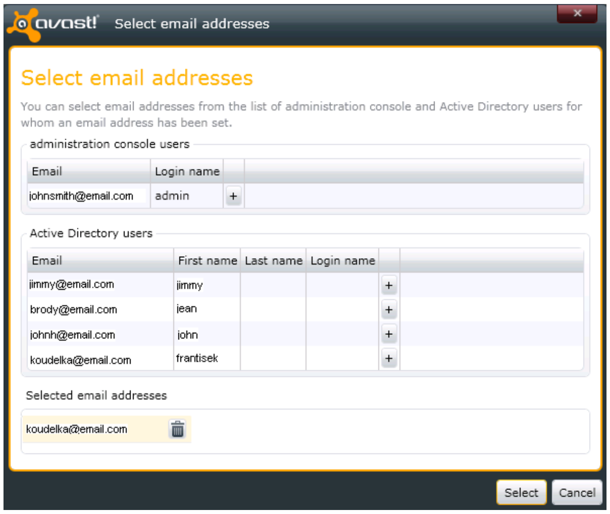
Language: English

Email will be sent to the following recipients:

Please provide user email addresses for computers on which avast! should be deployed.

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.



Select email addresses

You can select email addresses from the list of administration console and Active Directory users for whom an email address has been set.

administration console users

Email	Login name
johnsmith@email.com	admin

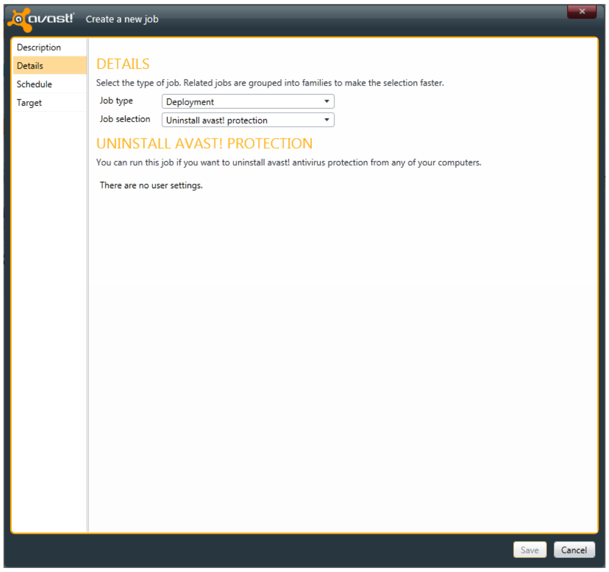
Active Directory users

Email	First name	Last name	Login name
jimmy@email.com	jimmy		
brody@email.com	jean		
johnh@email.com	john		
koudelka@email.com	frantisek		

Selected email addresses

koudelka@email.com

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**".



DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Deployment

Job selection: Uninstall avast! protection

UNINSTALL AVAST! PROTECTION

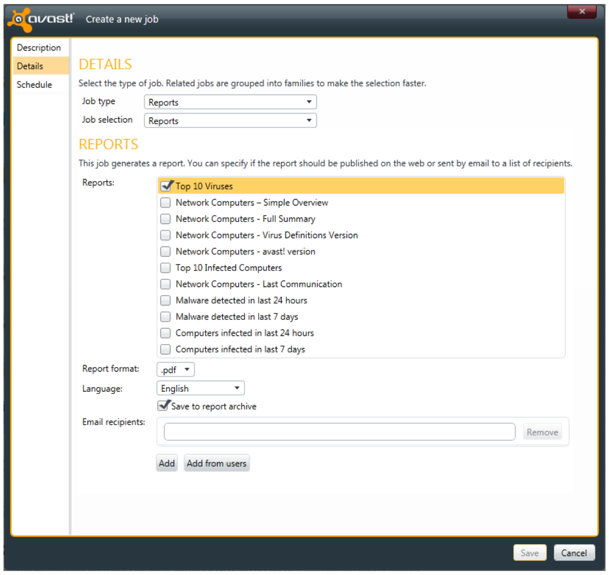
You can run this job if you want to uninstall avast! antivirus protection from any of your computers.

There are no user settings.

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.



DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Reports

Job selection: Reports

REPORTS

This job generates a report. You can specify if the report should be published on the web or sent by email to a list of recipients.

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

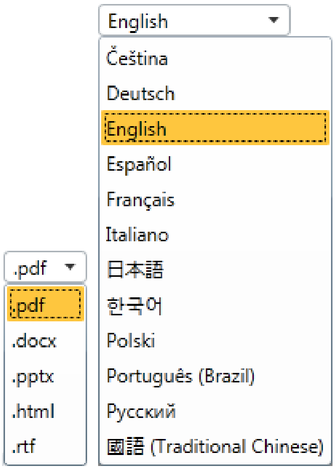
Report format: .pdf

Language: English

☑ Save to report archive

Email recipients:

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

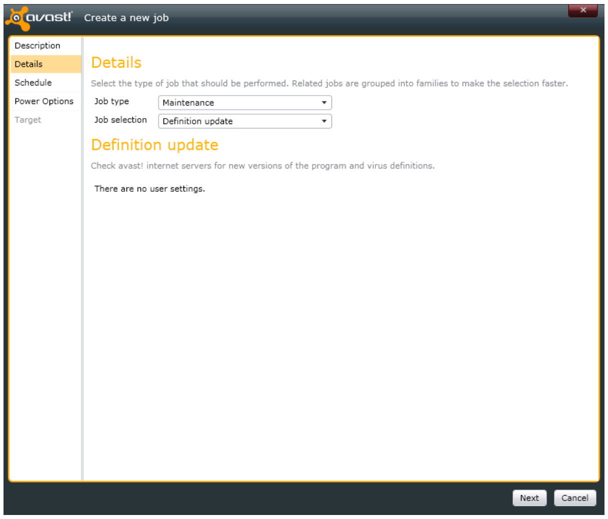


By specifying the recipients' email addresses, you can even have the reports sent to the management team (specific email address) automatically at periodic intervals.

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.



Details

Select the type of job that should be performed. Related jobs are grouped into families to make the selection faster.

Job type: Maintenance

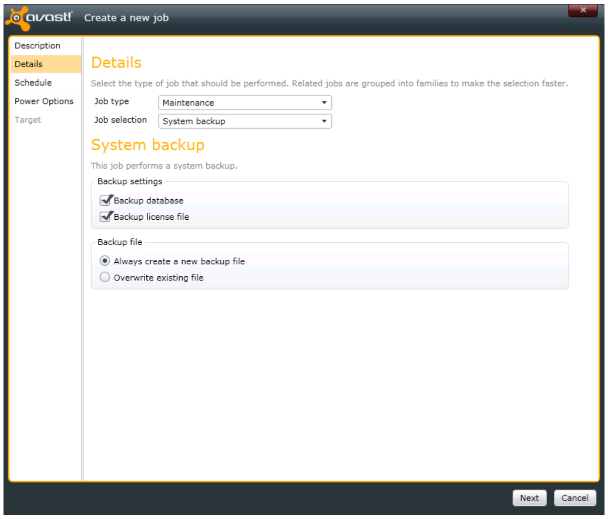
Job selection: Definition update

Definition update

Check avast! internet servers for new versions of the program and virus definitions.

There are no user settings.

3. System Backup



Details

Select the type of job that should be performed. Related jobs are grouped into families to make the selection faster.

Job type: Maintenance

Job selection: System backup

System backup

This job performs a system backup.

Backup settings

☑ Backup database

☑ Backup license file

Backup file

● Always create a new backup file

○ Overwrite existing file

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

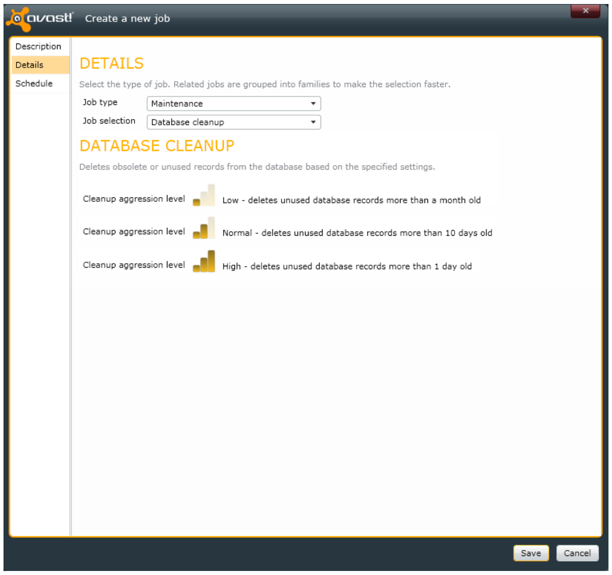
- Backup database
  - Runs DB backup
  - Backup file location - C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Backup
- Backup license file
  - License file is added to the backup

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.



DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Maintenance

Job selection: Database cleanup

DATABASE CLEANUP

Deletes obsolete or unused records from the database based on the specified settings.

Cleanup aggression level — Low - deletes unused database records more than a month old

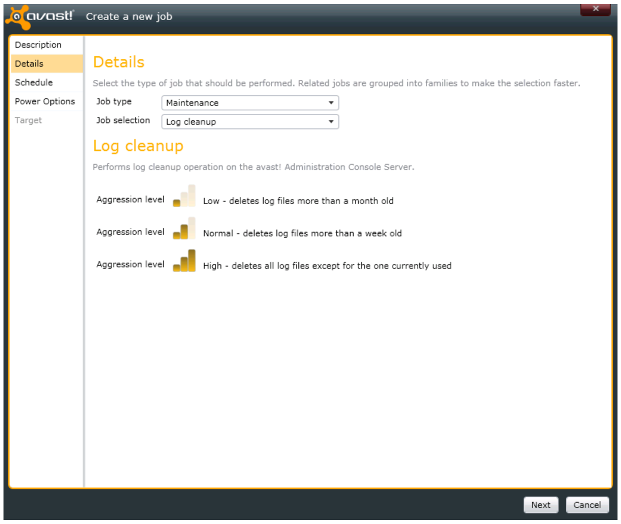
Cleanup aggression level — Normal - deletes unused database records more than 10 days old

Cleanup aggression level — High - deletes unused database records more than 1 day old

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.



Details

Select the type of job that should be performed. Related jobs are grouped into families to make the selection faster.

Job type: Maintenance

Job selection: Log cleanup

Log cleanup

Performs log cleanup operation on the avast! Administration Console Server.

Aggression level — Low - deletes log files more than a month old

Aggression level — Normal - deletes log files more than a week old

Aggression level — High - deletes all log files except for the one currently used

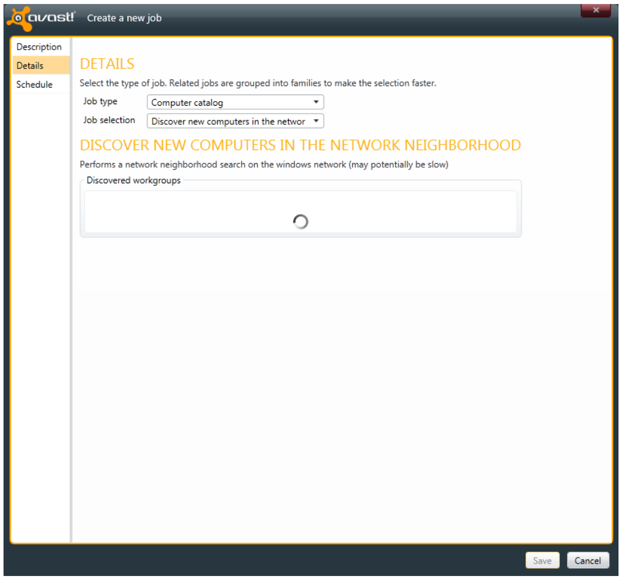
You can specify the following aggression levels:

- 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**



DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Computer catalog

Job selection: Discover new computers in the networ

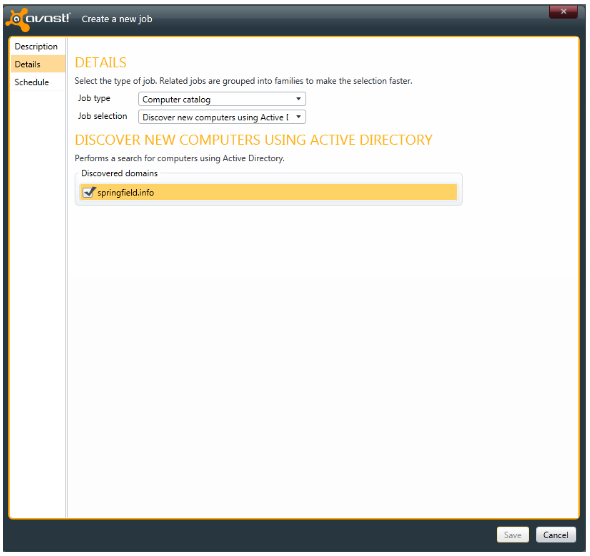
DISCOVER NEW COMPUTERS IN THE NETWORK NEIGHBORHOOD

Performs a network neighborhood search on the windows network (may potentially be slow)

Discovered workgroups

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

2. Discover new computers using Active Directory



Create a new job

DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Computer catalog

Job selection: Discover new computers using Active I

DISCOVER NEW COMPUTERS USING ACTIVE DIRECTORY

Performs a search for computers using Active Directory.

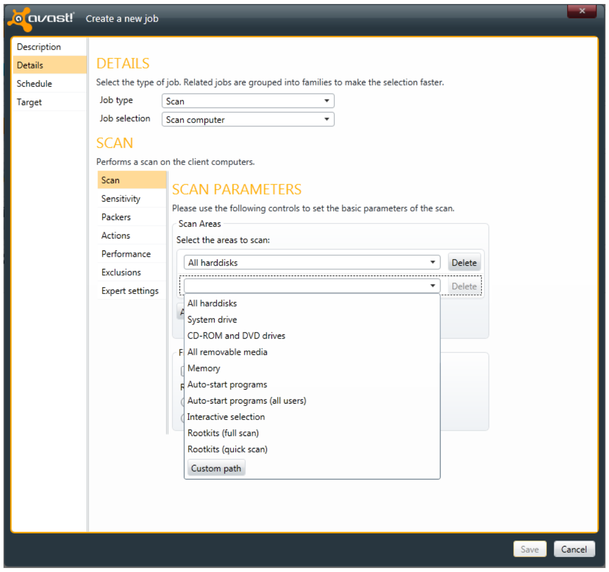
Discovered domains

☑ springfield.info

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.



Create a new job

DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Scan

Job selection: Scan computer

SCAN

Performs a scan on the client computers.

SCAN PARAMETERS

Please use the following controls to set the basic parameters of the scan.

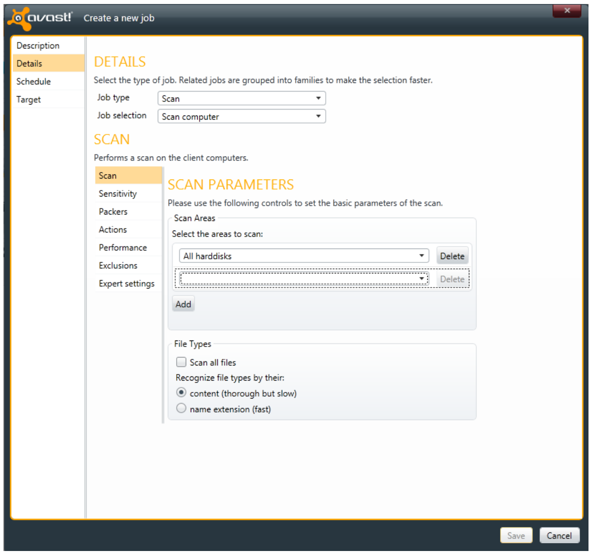
Scan Areas

Select the areas to scan:

All harddisks

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.



DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Scan

Job selection: Scan computer

SCAN

Performs a scan on the client computers.

SCAN PARAMETERS

Please use the following controls to set the basic parameters of the scan.

Scan Areas

Select the areas to scan:

All harddisks

File Types

□ Scan all files

Recognize file types by their:

● content (thorough but slow)

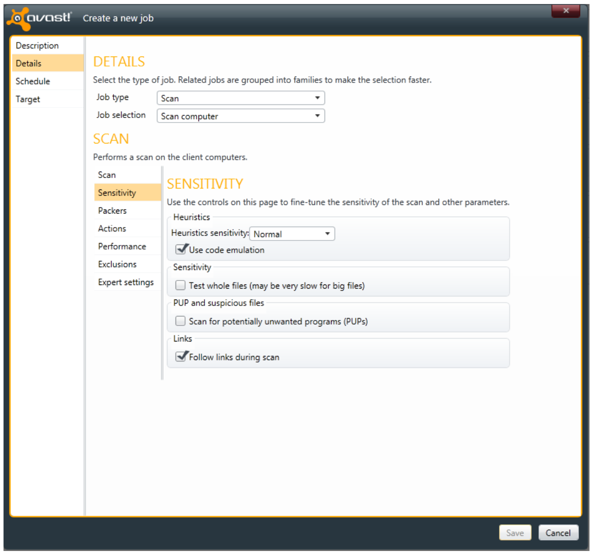
○ name extension (fast)

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.



DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Scan

Job selection: Scan computer

SCAN

Performs a scan on the client computers.

SENSITIVITY

Use the controls on this page to fine-tune the sensitivity of the scan and other parameters.

Heuristics

Heuristics sensitivity: Normal

☑ Use code emulation

Sensitivity

□ Test whole files (may be very slow for big files)

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

Links

☑ Follow links during scan

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".

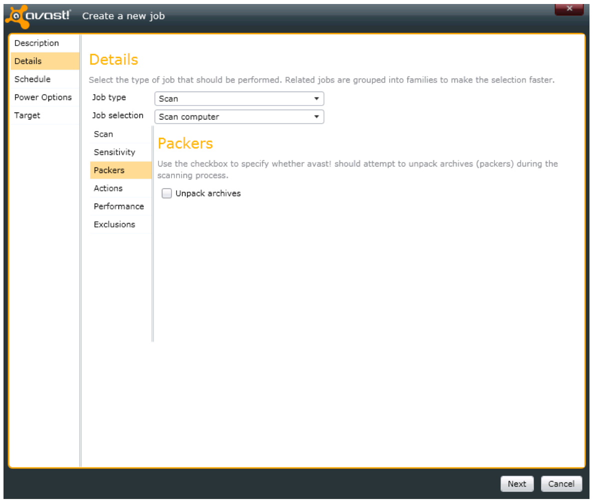
If you find that a large number of clean files are detected by avast! as suspicious ("false positives"), it is possible that the heuristic sensitivity is set too high. Reducing the heuristic sensitivity should result in fewer files being reported as suspicious, however this also reduces the chances of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



Details

Select the type of job that should be performed. Related jobs are grouped into families to make the selection faster.

Job type: Scan

Job selection: Scan computer

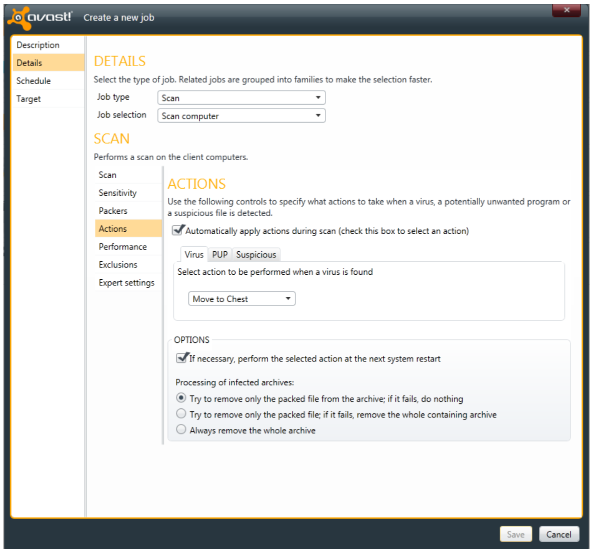
Packers

Use the checkbox to specify whether avast! should attempt to unpack archives (packers) during the scanning process.

☐ Unpack archives

Packers

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



DETAILS

Select the type of job. Related jobs are grouped into families to make the selection faster.

Job type: Scan

Job selection: Scan computer

SCAN

Performs a scan on the client computers.

ACTIONS

Use the following controls to specify what actions to take when a virus, a potentially unwanted program or a suspicious file is detected.

☑ Automatically apply actions during scan (check this box to select an action)

Select action to be performed when a virus is found

Move to Chest

OPTIONS

☑ If necessary, perform the selected action at the next system restart

Processing of infected archives:

● Try to remove only the packed file from the archive; if it fails, do nothing

○ Try to remove only the packed file; if it fails, remove the whole containing archive

○ Always remove the whole archive

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.

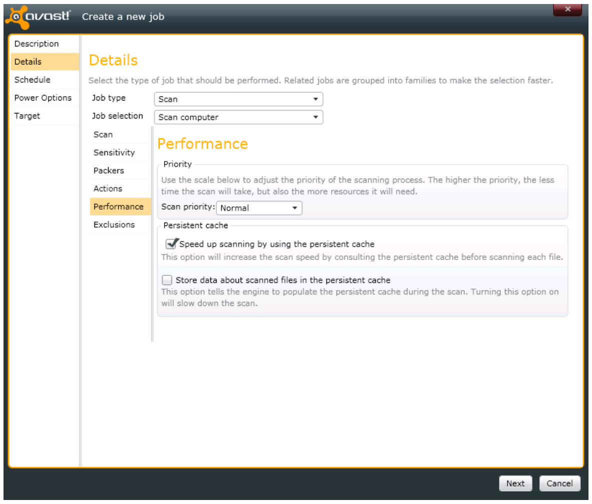
If "Ask" is selected, you will be asked to confirm what action to take at the moment the virus, potentially unwanted program, or suspicious file is detected. You can also specify alternate actions, from the same list of options, which should be taken if the preferred actions cannot be completed.

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.



Details

Select the type of job that should be performed. Related jobs are grouped into families to make the selection faster.

Job type: Scan

Job selection: Scan computer

Performance

Priority

Use the scale below to adjust the priority of the scanning process. The higher the priority, the less time the scan will take, but also the more resources it will need.

Scan priority: Normal

Persistent cache

☑ Speed up scanning by using the persistent cache

This option will increase the scan speed by consulting the persistent cache before scanning each file.

☐ Store data about scanned files in the persistent cache

This option tells the engine to populate the persistent cache during the scan. Turning this option on will slow down the scan.

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.

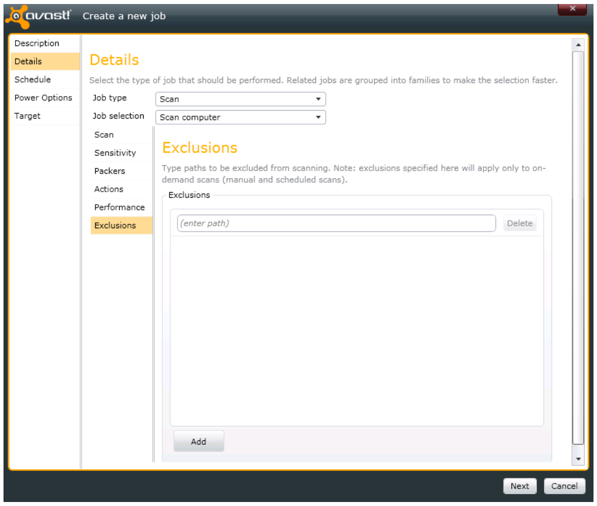
Persistent Cache

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.



Details

Select the type of job that should be performed. Related jobs are grouped into families to make the selection faster.

Job type: Scan

Job selection: Scan computer

Exclusions

Type paths to be excluded from scanning. Note: exclusions specified here will apply only to on-demand scans (manual and scheduled scans).

Exclusions

(enter path)

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.

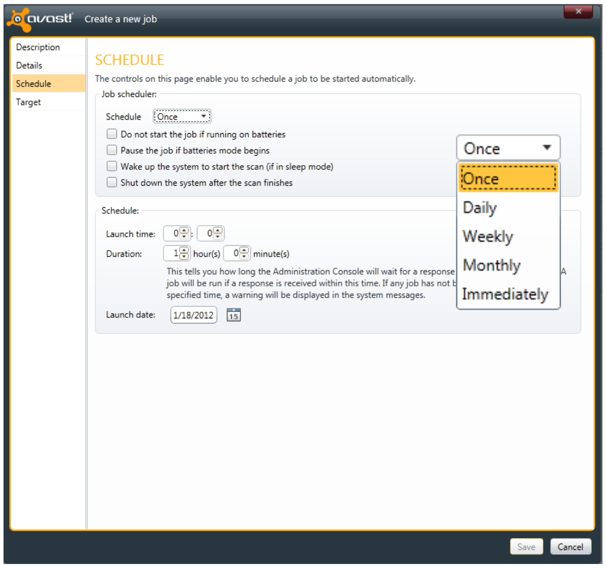
To exclude a location or file, first click the box where it says <enter path> and then either type the location or file to be excluded.

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.



SCHEDULE

The controls on this page enable you to schedule a job to be started automatically.

Job scheduler:

Schedule: Once

□ Do not start the job if running on batteries

□ Pause the job if batteries mode begins

□ Wake up the system to start the scan (if in sleep mode)

□ Shut down the system after the scan finishes

Schedule:

Launch time: 0 : 0

Duration: 1 hour(s) 0 minute(s)

This tells you how long the Administration Console will wait for a response A job will be run if a response is received within this time. If any job has not b specified time, a warning will be displayed in the system messages.

Launch date: 1/18/2012

Job scheduler

Here you can specify when the job will be started.

- Once - simply enter the time and d ate 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

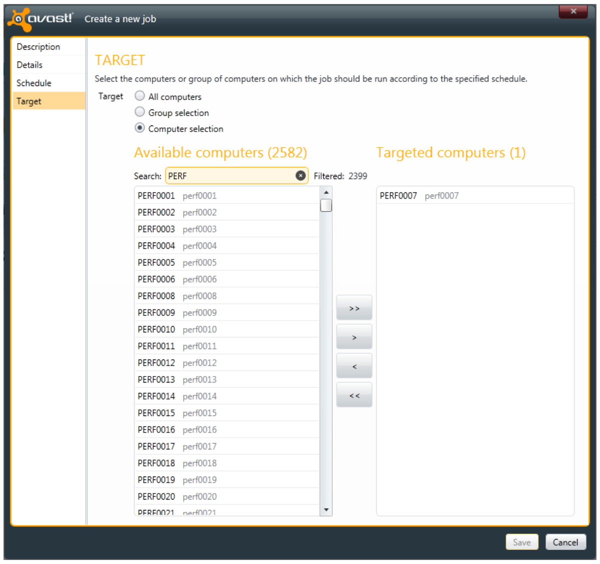
- If the computer is cut off from the electric power supply and switches to batteries while a job is running, the job will be paused. Again, this is useful mainly for notebook owners.

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

Select the computers or group of computers on which the job should be run according to the specified schedule.

Target ○ All computers
○ Group selection
● Computer selection

Available computers (2582)

Search: PERF

Filtered: 2399

PERF0001 perf0001
PERF0002 perf0002
PERF0003 perf0003
PERF0004 perf0004
PERF0005 perf0005
PERF0006 perf0006
PERF0008 perf0008
PERF0009 perf0009
PERF0010 perf0010
PERF0011 perf0011
PERF0012 perf0012
PERF0013 perf0013
PERF0014 perf0014
PERF0015 perf0015
PERF0016 perf0016
PERF0017 perf0017
PERF0018 perf0018
PERF0019 perf0019
PERF0020 perf0020
PERF0021 perf0021

Targeted computers (1)

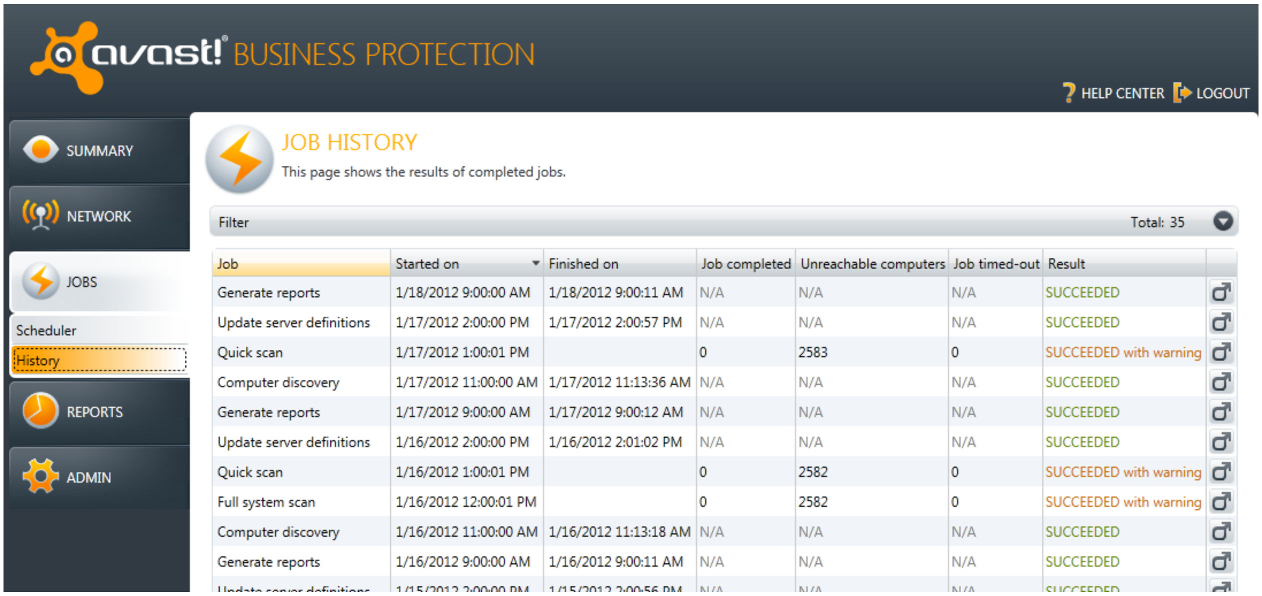
PERF0007 perf0007

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:



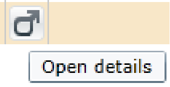
JOB HISTORY

This page shows the results of completed jobs.

Filter Total: 35

Job	Started on	Finished on	Job completed	Unreachable computers	Job timed-out	Result
Generate reports	1/18/2012 9:00:00 AM	1/18/2012 9:00:11 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	1/17/2012 2:00:00 PM	1/17/2012 2:00:57 PM	N/A	N/A	N/A	SUCCEEDED
Quick scan	1/17/2012 1:00:01 PM		0	2583	0	SUCCEEDED with warning
Computer discovery	1/17/2012 11:00:00 AM	1/17/2012 11:13:36 AM	N/A	N/A	N/A	SUCCEEDED
Generate reports	1/17/2012 9:00:00 AM	1/17/2012 9:00:12 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	1/16/2012 2:00:00 PM	1/16/2012 2:01:02 PM	N/A	N/A	N/A	SUCCEEDED
Quick scan	1/16/2012 1:00:01 PM		0	2582	0	SUCCEEDED with warning
Full system scan	1/16/2012 12:00:01 PM		0	2582	0	SUCCEEDED with warning
Computer discovery	1/16/2012 11:00:00 AM	1/16/2012 11:13:18 AM	N/A	N/A	N/A	SUCCEEDED
Generate reports	1/16/2012 9:00:00 AM	1/16/2012 9:00:11 AM	N/A	N/A	N/A	SUCCEEDED
Update server definitions	1/15/2012 2:00:00 PM	1/15/2012 2:00:56 PM	N/A	N/A	N/A	SUCCEEDED

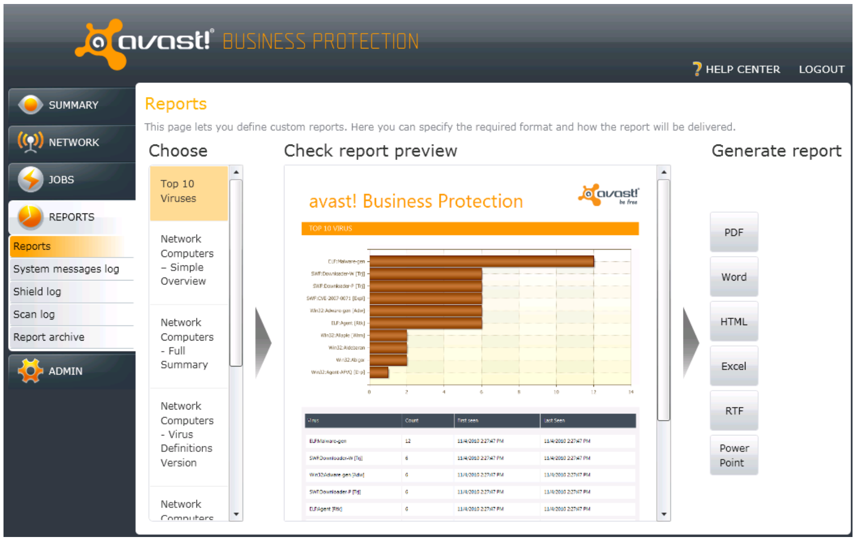
If you would like to see more detailed information, click on the"folder" icon



Open details

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.



Reports

This page lets you define custom reports. Here you can specify the required format and how the report will be delivered.

Virus	Count	First seen	Last Seen
ELF:Malware-gen	12	11/4/2010 2:27:47 PM	11/4/2010 2:27:47 PM
SWF:Downloader-W [Trj]	6	11/4/2010 2:27:47 PM	11/4/2010 2:27:47 PM
Win32:Adware-gen [Adw]	6	11/4/2010 2:27:47 PM	11/4/2010 2:27:47 PM
SWF:Downloader-P [Trj]	6	11/4/2010 2:27:47 PM	11/4/2010 2:27:47 PM
ELF:Agent [Rtk]	6	11/4/2010 2:27:47 PM	11/4/2010 2:27:47 PM

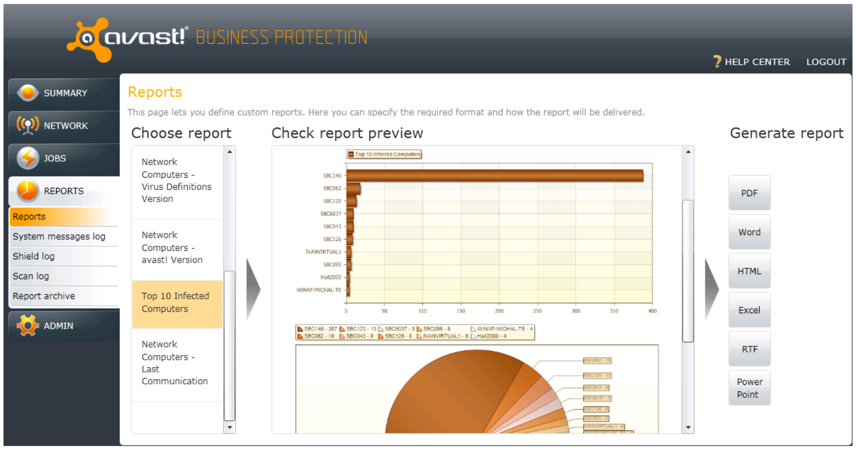
You can export these reports to many popular formats:

- Pdf
- Word
- Html
- Rtf
- Powerpoint

There are 11 pre-defined reports

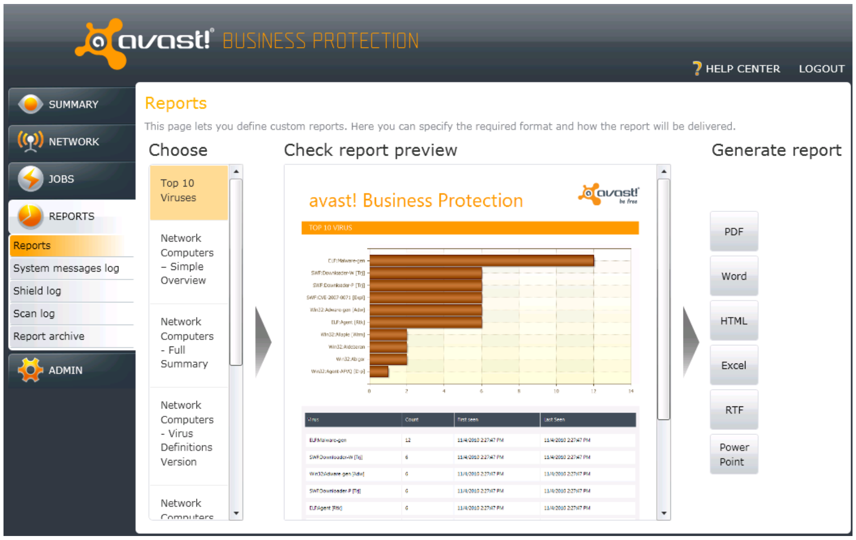
– Top 10 viruses
– Network computers - simple overview
– Network computers - full summary
– Network computers - virus definitions version
– Network computers - avast! version
– Top 10 infected computers
– Network computers - last communicationMalware detected in last 24 hours
– Malware detected in last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

Examples of some of the reports which can be created:



This page lets you define custom reports. Here you can specify the required format and how the report will be delivered.

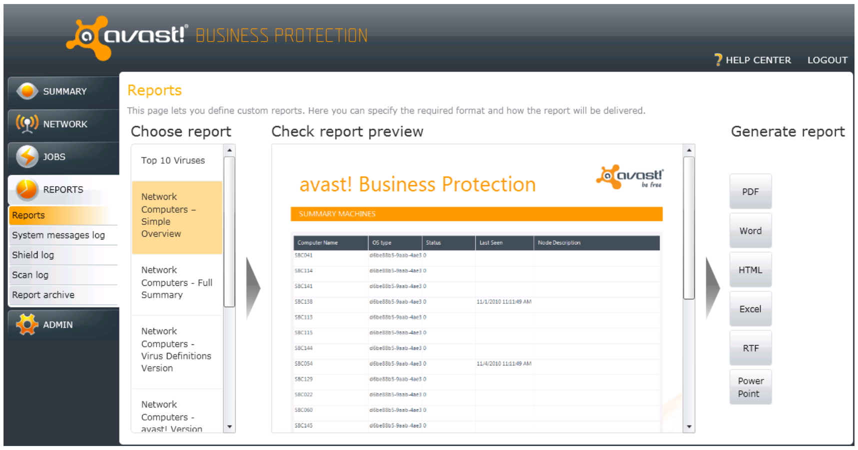
Top 10 infected computers



This page lets you define custom reports. Here you can specify the required format and how the report will be delivered.

Virus	Count	First seen	Last Seen
ELF:Malware-gen	12	11/4/2010 2:27:47 PM	11/4/2010 2:27:47 PM
SWF:Downloader-W [Trj]	6	11/4/2010 2:27:47 PM	11/4/2010 2:27:47 PM
Win32:Adware-gen [Adw]	6	11/4/2010 2:27:47 PM	11/4/2010 2:27:47 PM
SWF:Downloader-P [Trj]	6	11/4/2010 2:27:47 PM	11/4/2010 2:27:47 PM
ELF:Agent [Rtk]	6	11/4/2010 2:27:47 PM	11/4/2010 2:27:47 PM

Top 10 viruses

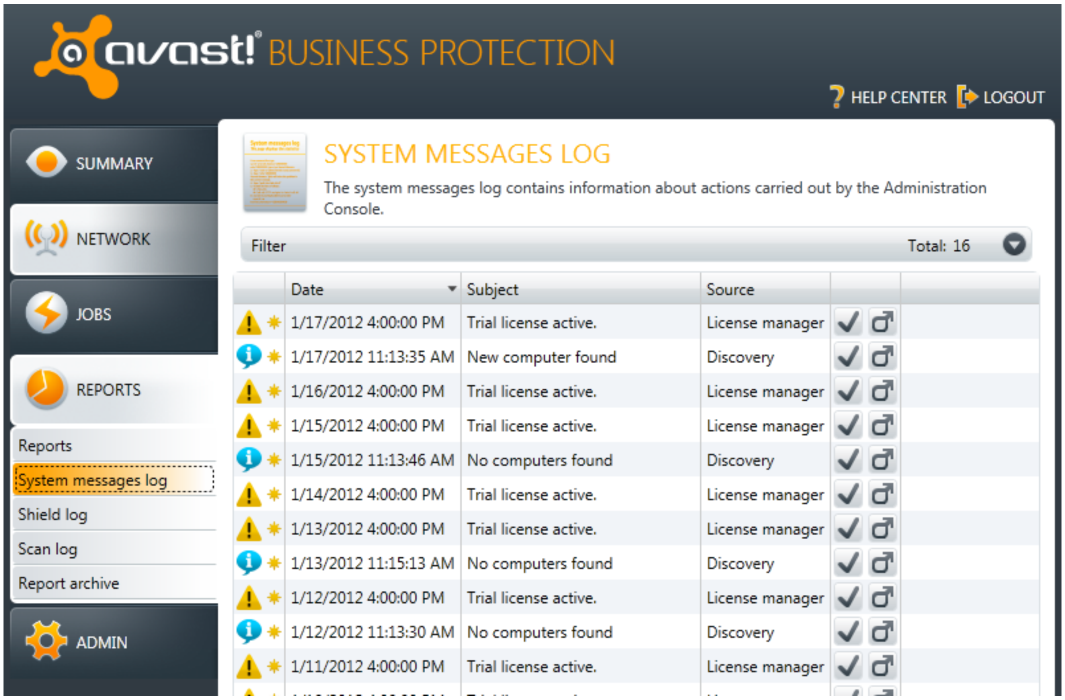


This page lets you define custom reports. Here you can specify the required format and how the report will be delivered.

Network computers – simple overview

System Messages Log

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



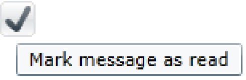
SYSTEM MESSAGES LOG

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

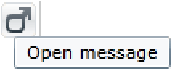
Filter Total: 16

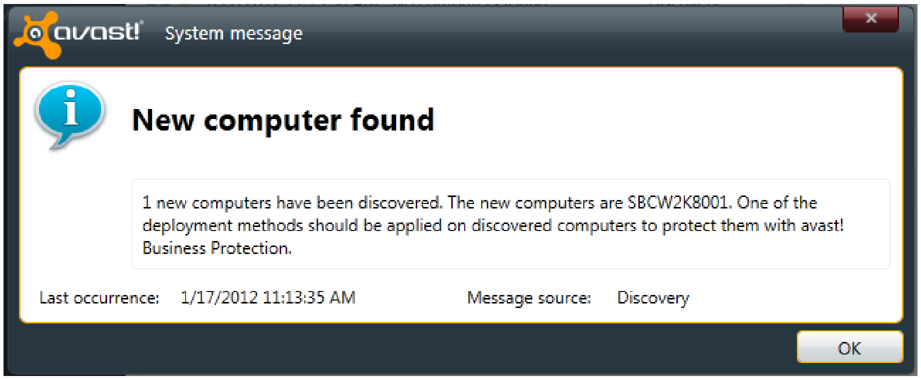
	Date	Subject	Source	
⚠	1/17/2012 4:00:00 PM	Trial license active.	License manager	✓
ℹ	1/17/2012 11:13:35 AM	New computer found	Discovery	✓
⚠	1/16/2012 4:00:00 PM	Trial license active.	License manager	✓
⚠	1/15/2012 4:00:00 PM	Trial license active.	License manager	✓
ℹ	1/15/2012 11:13:46 AM	No computers found	Discovery	✓
⚠	1/14/2012 4:00:00 PM	Trial license active.	License manager	✓
⚠	1/13/2012 4:00:00 PM	Trial license active.	License manager	✓
ℹ	1/13/2012 11:15:13 AM	No computers found	Discovery	✓
⚠	1/12/2012 4:00:00 PM	Trial license active.	License manager	✓
ℹ	1/12/2012 11:13:30 AM	No computers found	Discovery	✓
⚠	1/11/2012 4:00:00 PM	Trial license active.	License manager	✓

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



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





New computer found

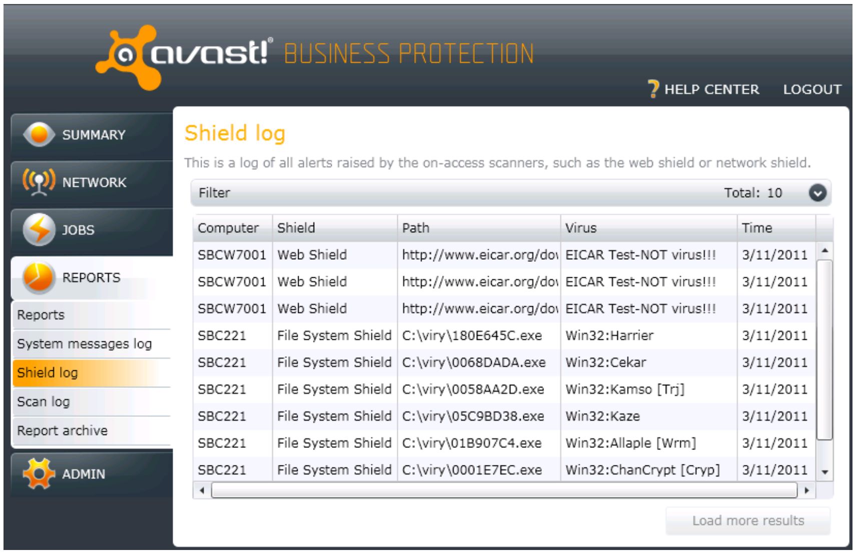
1 new computers have been discovered. The new computers are SBCW2K8001. One of the deployment methods should be applied on discovered computers to protect them with avast! Business Protection.

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.



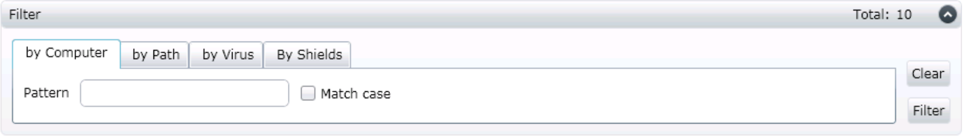
Shield log

This is a log of all alerts raised by the on-access scanners, such as the web shield or network shield.

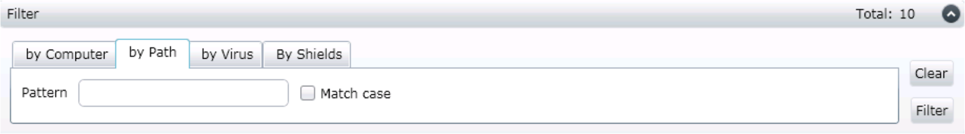
Filter Total: 10

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

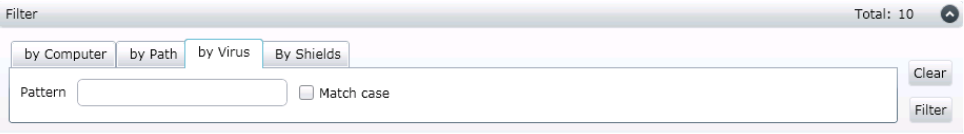
It is possible to filter by Computer name,



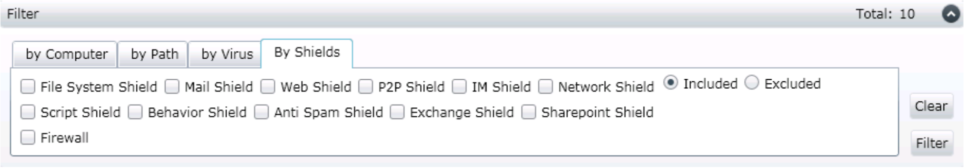
By Path/location,



By Virus name,



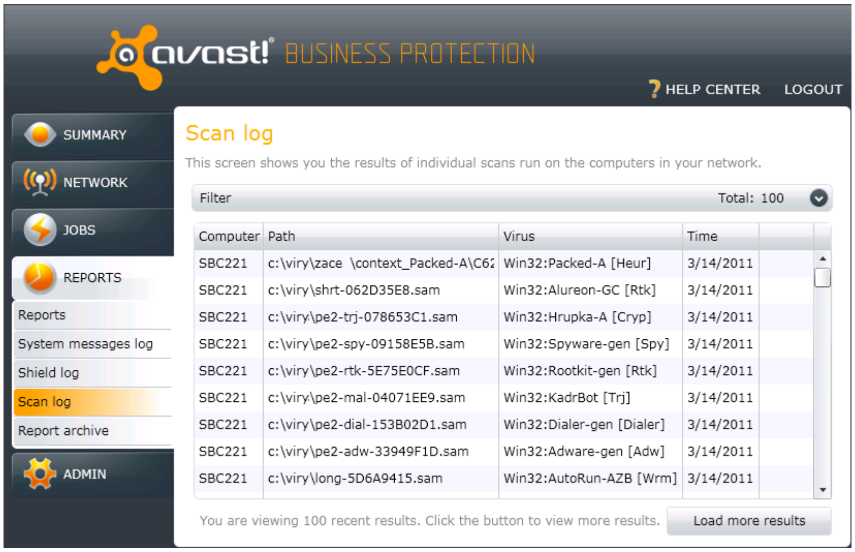
Or by Shields



□ 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

Scan Log

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



Scan log

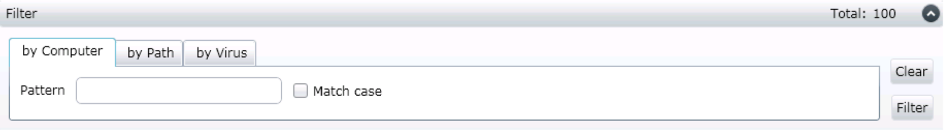
This screen shows you the results of individual scans run on the computers in your network.

Filter Total: 100

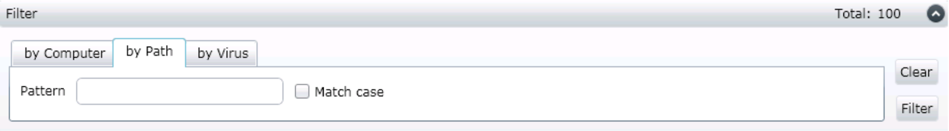
Computer	Path	Virus	Time
SBC221	c:\viry\zace \context_Packed-A\C62	Win32:Packed-A [Heur]	3/14/2011
SBC221	c:\viry\shrt-062D35E8.sam	Win32:Alureon-GC [Rtk]	3/14/2011
SBC221	c:\viry\pe2-trj-078653C1.sam	Win32:Hrupka-A [Cryp]	3/14/2011
SBC221	c:\viry\pe2-spy-09158E5B.sam	Win32:Spyware-gen [Spy]	3/14/2011
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

You are viewing 100 recent results. Click the button to view more results. Load more results

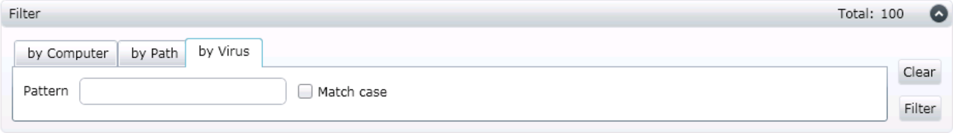
The scan log can be filtered by Computer name,



By Path/location,

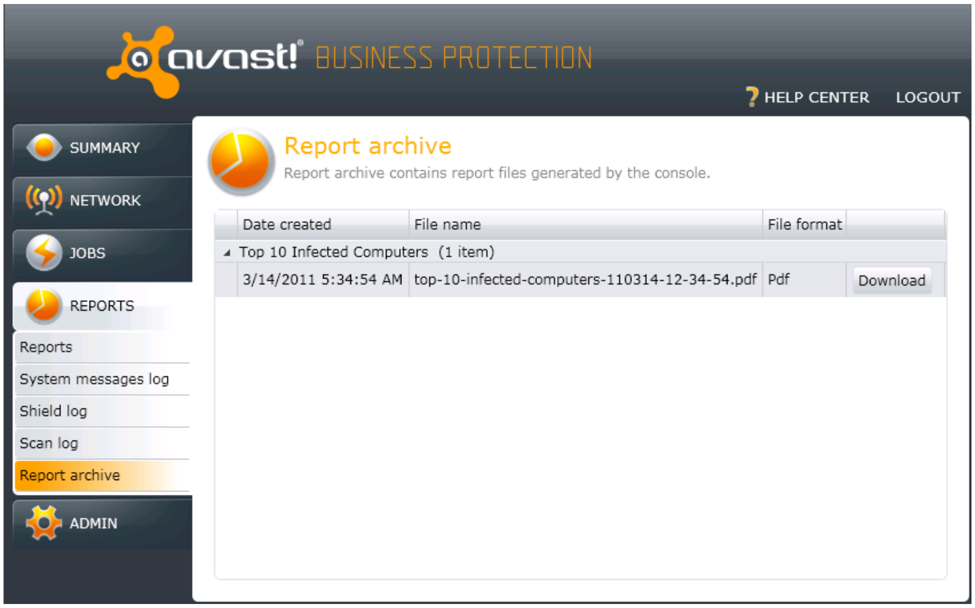


or by Virus name



Report archive

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



Report archive

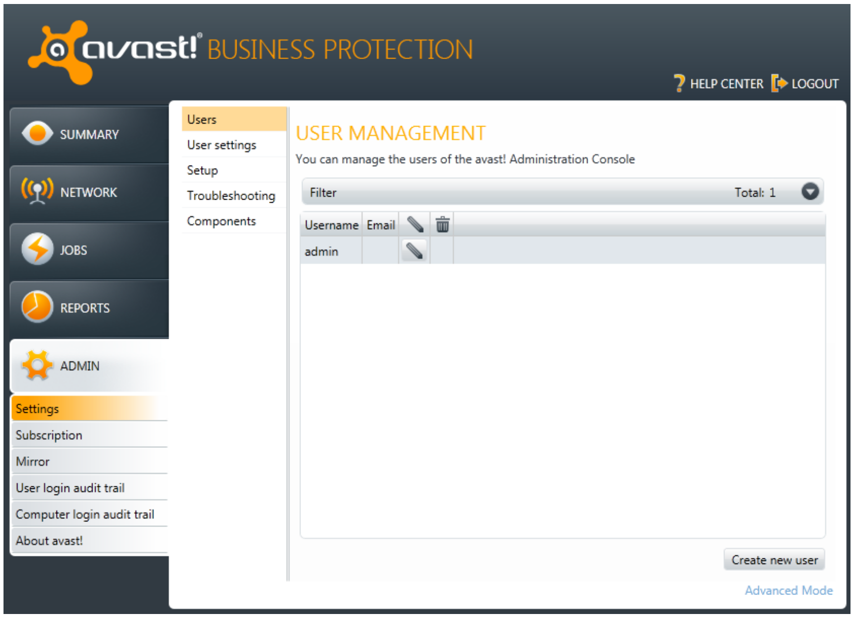
Report archive contains report files generated by the console.

Date created	File name	File format	
Top 10 Infected Computers (1 item)			
3/14/2011 5:34:54 AM	top-10-infected-computers-110314-12-34-54.pdf	Pdf	Download

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

8. Administration

Settings

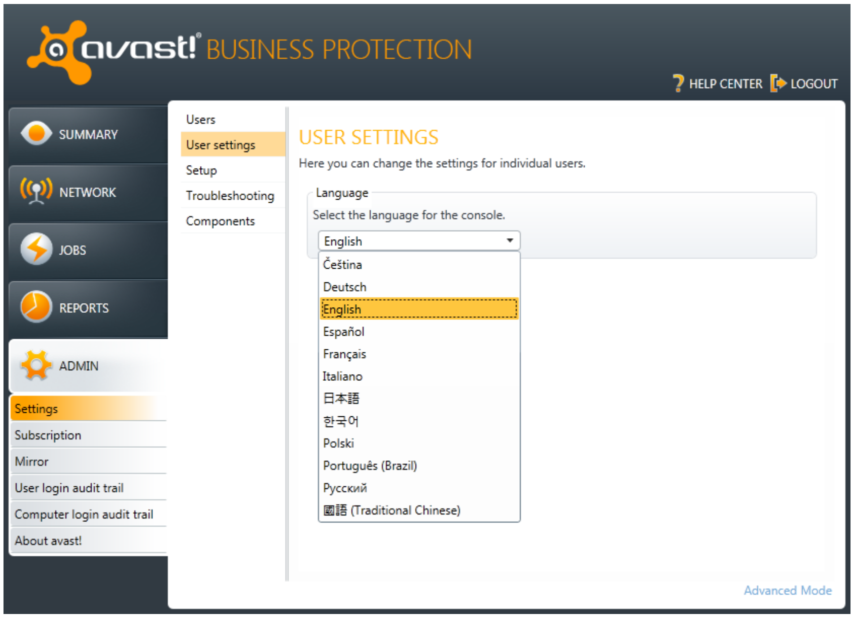


USER MANAGEMENT

You can manage the users of the avast! Administration Console

Users

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



USER SETTINGS

Here you can change the settings for individual users.

Language

Select the language for the console.

English

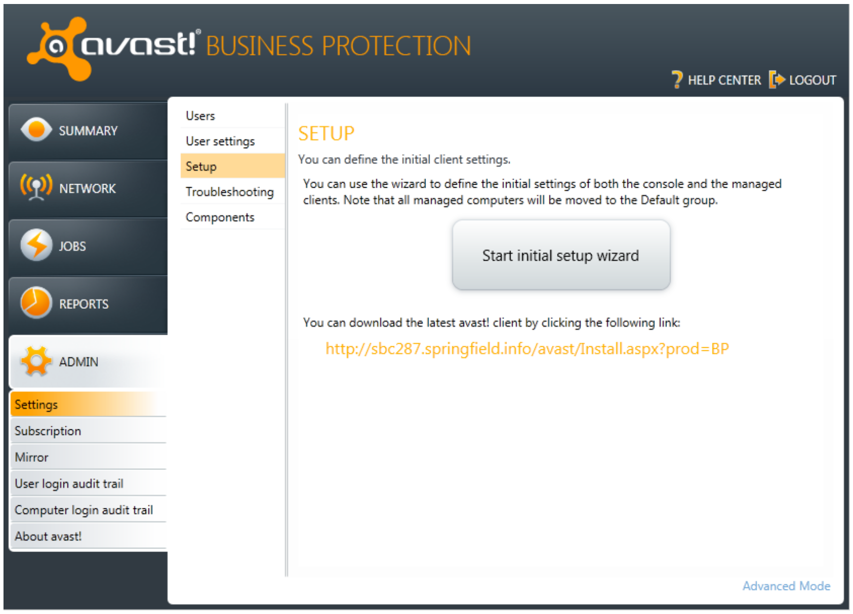
User Settings

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 re-assigned back to their initial default groups.



SETUP

You can define the initial client settings.

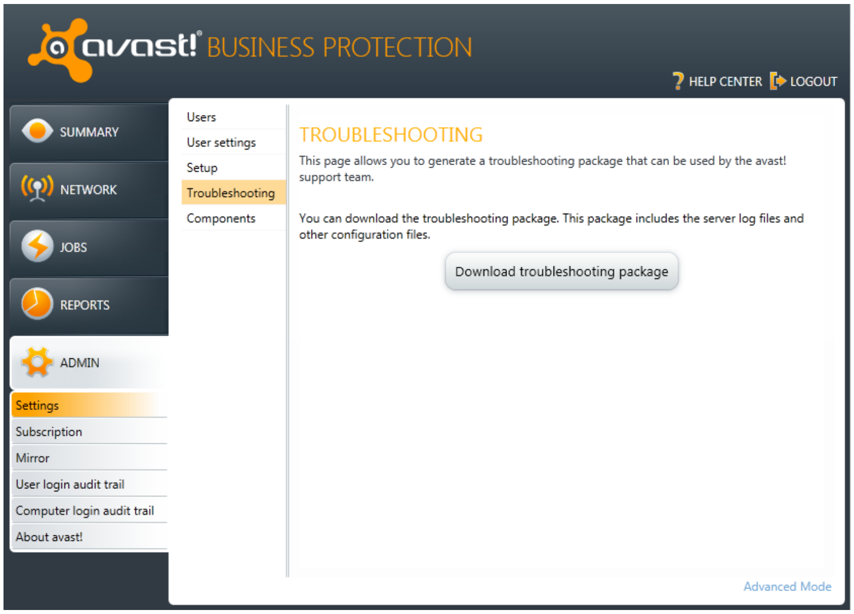
You can use the wizard to define the initial settings of both the console and the managed clients. Note that all managed computers will be moved to the Default group.

You can download the latest avast! client by clicking the following link:

http://sbc287.springfield.info/avast/Install.aspx?prod=BP

Troubleshooting

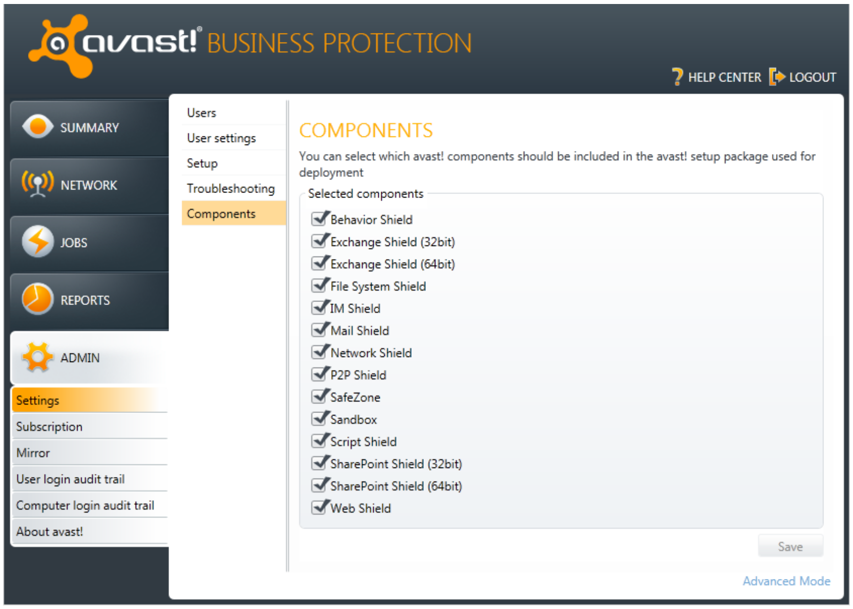
Here you can create a package containing all your system for avast support purposes.



TROUBLESHOOTING

This page allows you to generate a troubleshooting package that can be used by the avast! support team.

You can download the troubleshooting package. This package includes the server log files and other configuration files.



COMPONENTS

You can select which avast! components should be included in the avast! setup package used for deployment

Selected components

- ☑ Behavior Shield
- ☑ Exchange Shield (32bit)
- ☑ Exchange Shield (64bit)
- ☑ File System Shield
- ☑ IM Shield
- ☑ Mail Shield
- ☑ Network Shield
- ☑ P2P Shield
- ☑ SafeZone
- ☑ Sandbox
- ☑ Script Shield
- ☑ SharePoint Shield (32bit)
- ☑ SharePoint Shield (64bit)
- ☑ Web Shield

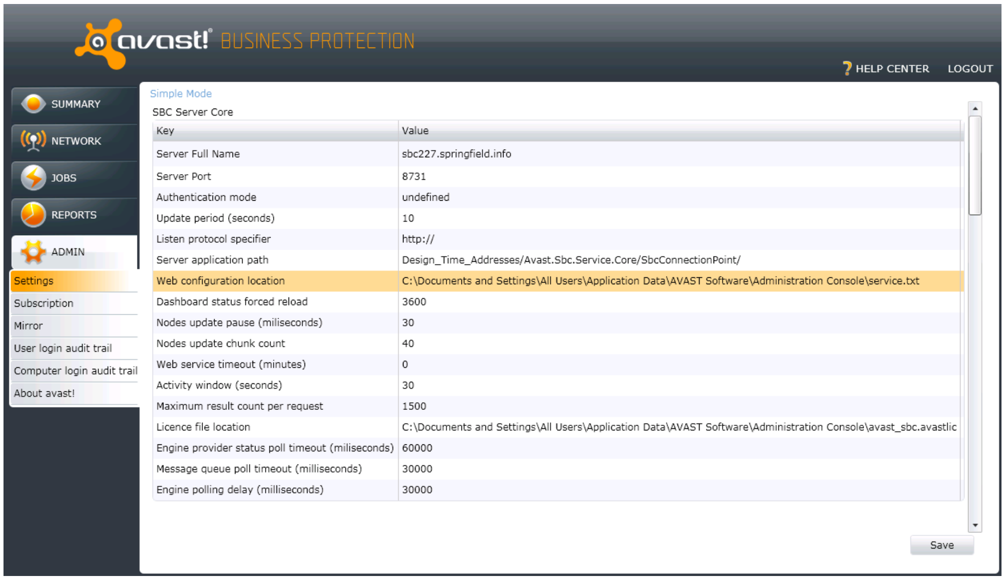
Components

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

Advanced Mode

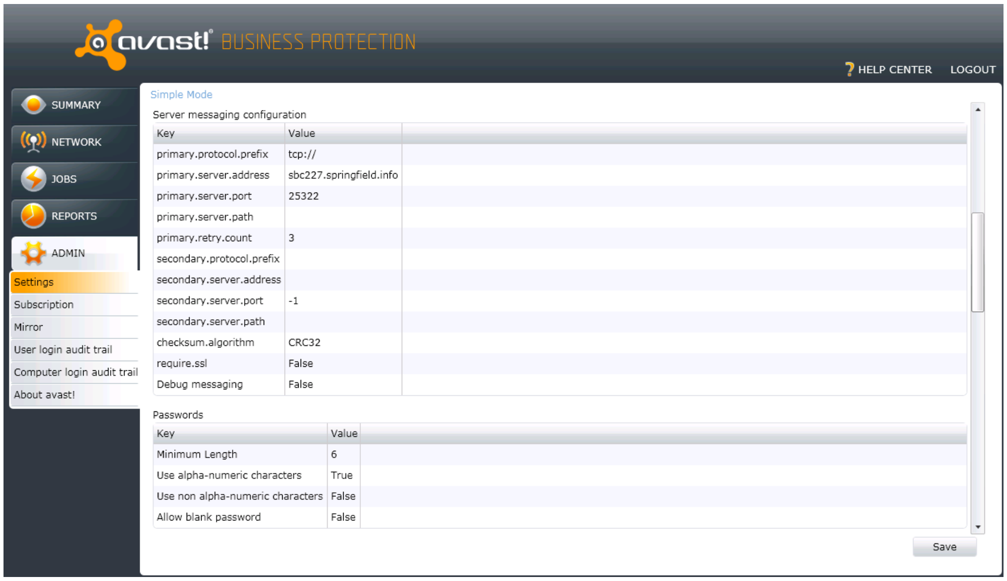
The Advanced mode settinsg are accessed by clicking on “Advanced Mode“ in the bottom right corner of the “Users“ or “User settings“ screen.

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.



SBC Server Core

Key	Value
Server Full Name	sbc227.springfield.info
Server Port	8731
Authentication mode	undefined
Update period (seconds)	10
Listen protocol specifier	http://
Server application path	Design_Time_Addresses/Avast.Sbc.Service.Core/SbcConnectionPoint/
Web configuration location	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\service.txt
Dashboard status forced reload	3600
Nodes update pause (miliseconds)	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\Administration Console\avast_sbc.avastlic
Engine provider status poll timeout (miliseconds)	60000
Message queue poll timeout (milliseconds)	30000
Engine polling delay (milliseconds)	30000

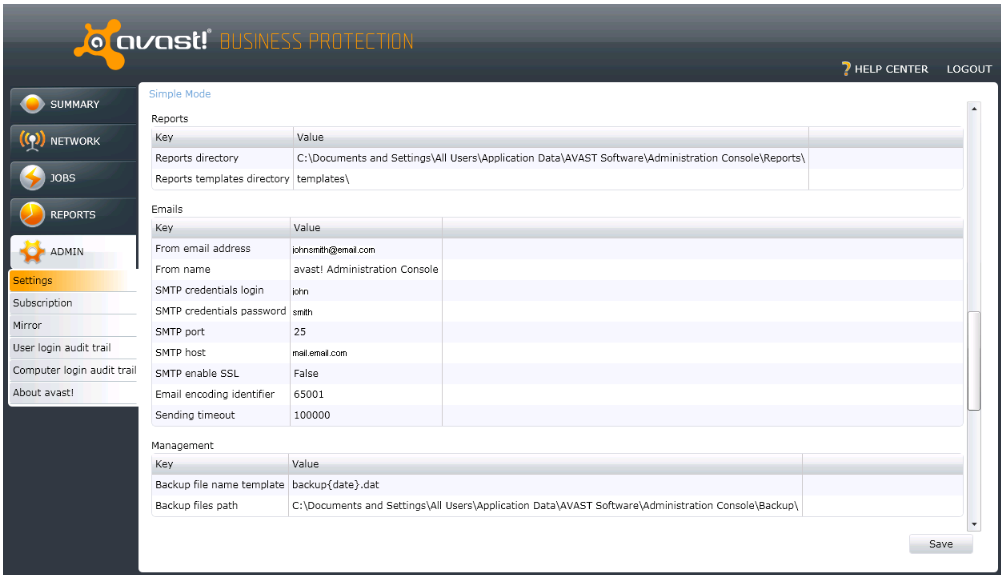


Server messaging configuration

Key	Value
primary.protocol.prefix	tcp://
primary.server.address	sbc227.springfield.info
primary.server.port	25322
primary.server.path	
primary.retry.count	3
secondary.protocol.prefix	
secondary.server.address	
secondary.server.port	-1
secondary.server.path	
checksum.algorithm	CRC32
require.ssl	False
Debug messaging	False

Passwords

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



Reports

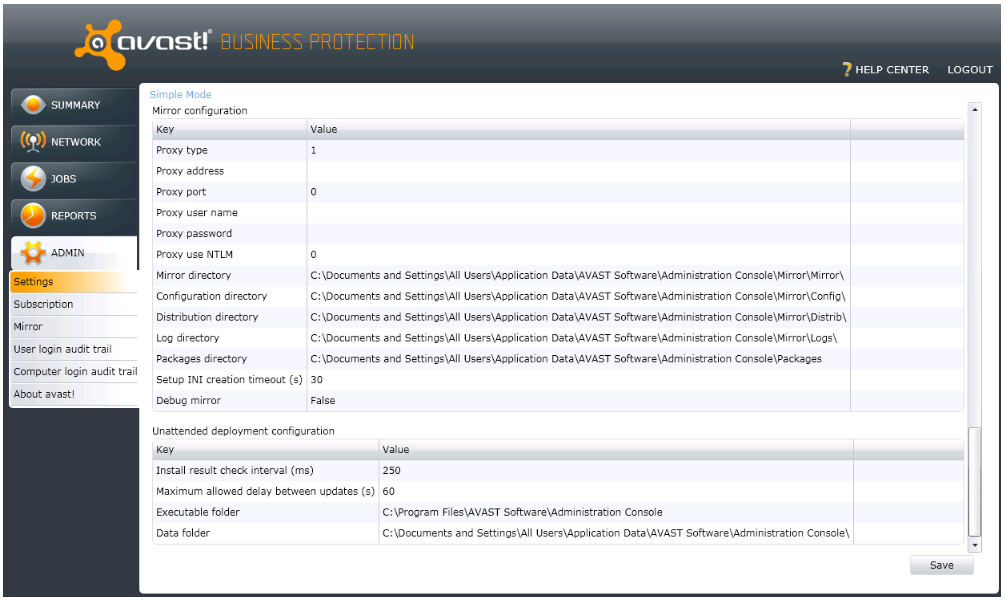
Key	Value
Reports directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Reports\
Reports templates directory	templates\

Emails

Key	Value
From email address	johnsmith@email.com
From name	avast! Administration Console
SMTP credentials login	john
SMTP credentials password	smith
SMTP port	25
SMTP host	mail.email.com
SMTP enable SSL	False
Email encoding identifier	65001
Sending timeout	100000

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\Backup\



Mirror configuration

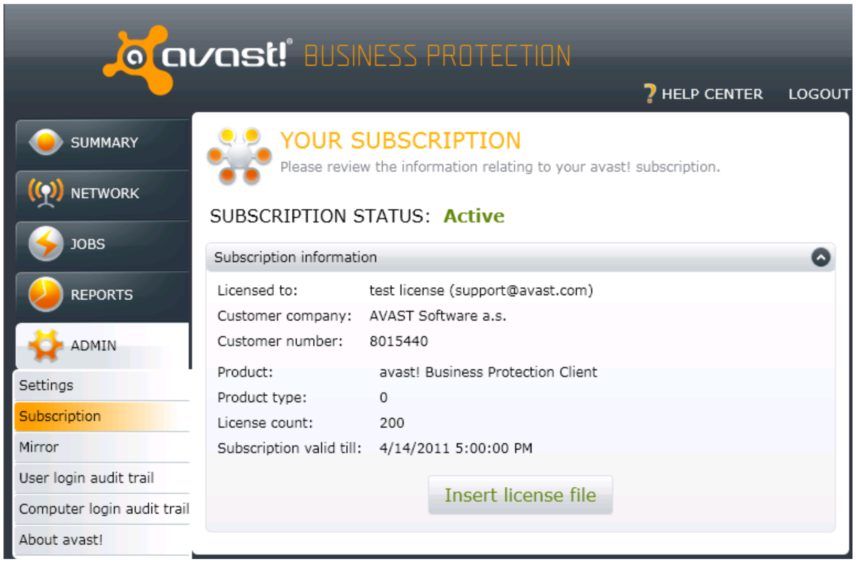
Key	Value
Proxy type	1
Proxy address	
Proxy port	0
Proxy user name	
Proxy password	
Proxy use NTLM	0
Mirror directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Mirror\Mirror\
Configuration directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Mirror\Config\
Distribution directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Mirror\Distrib\
Log directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Mirror\Logs\
Packages directory	C:\Documents and Settings\All Users\Application Data\AVAST Software\Administration Console\Packages
Setup INI creation timeout (s)	30
Debug mirror	False

Unattended deployment configuration

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\Administration Console\

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.



YOUR SUBSCRIPTION

Please review the information relating to your avast! subscription.

SUBSCRIPTION STATUS: Active

Subscription information

Licensed to: test license (support@avast.com)
Customer company: AVAST Software a.s.
Customer number: 8015440

Product: avast! Business Protection Client
Product type: 0
License count: 200
Subscription valid till: 4/14/2011 5:00:00 PM

Insert license file

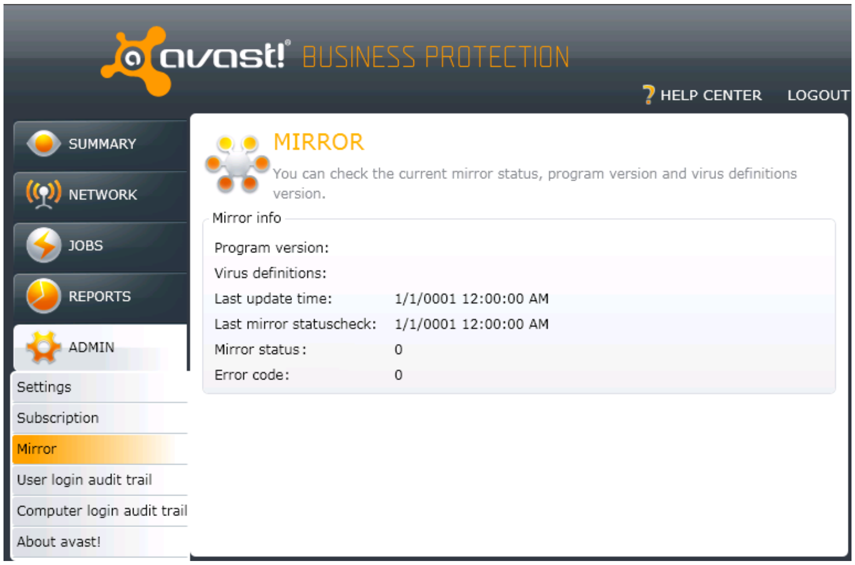
Alternatively, save the license file on your computer, open the avast! interface and click on the Maintenance tab. Next click on "Subscription" and then on "Insert license file". A new window will open where you can browse your computer to locate your license file. Once you have located it, double click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

You can check the current mirror status, program version and virus definitions version.

Mirror info

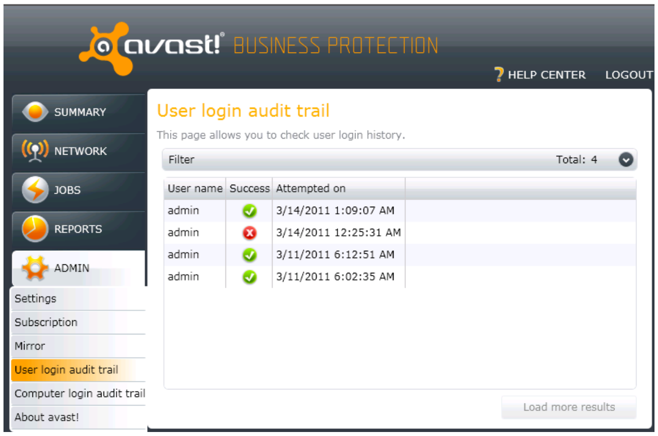
Program version:	
Virus definitions:	
Last update time:	1/1/0001 12:00:00 AM
Last mirror statuscheck:	1/1/0001 12:00:00 AM
Mirror status:	0
Error code:	0

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
- attemps to connect to the avast! Administration console

User login audit trail



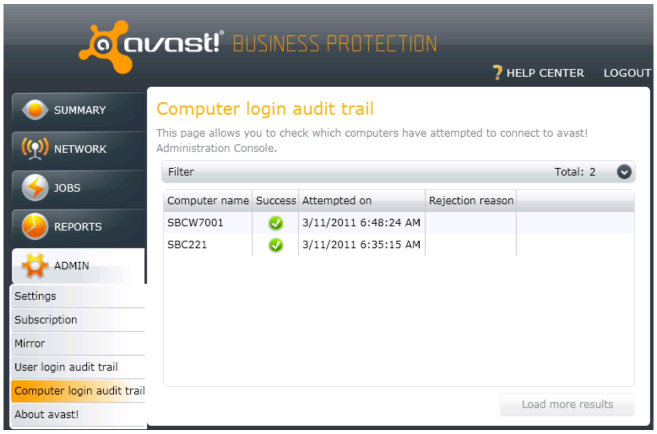
User login audit trail

This page allows you to check user login history.

Total: 4

User name	Success	Attempted on
admin	✓	3/14/2011 1:09:07 AM
admin	✗	3/14/2011 12:25:31 AM
admin	✓	3/11/2011 6:12:51 AM
admin	✓	3/11/2011 6:02:35 AM

Computer login audit trail



Computer login audit trail

This page allows you to check which computers have attempted to connect to avast! Administration Console.

Total: 2

Computer name	Success	Attempted on	Rejection reason
SBCW7001	✓	3/11/2011 6:48:24 AM	
SBC221	✓	3/11/2011 6:35:15 AM	

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