avast!

Enterprise Administration

www.avast.com

Contents

- Introduction to Enterprise Administration
- System requirements
- Avast! Enterprise Administration Server (EAS) maintenance tool
- Avast! Enterprise Administration console
  - Overview
  - Tasks
    - Client side tasks
      - On-demand scanning tasks
      - Updating task
      - Deployment task
      - Auxiliary tasks
      - Uninstall managed product(s)
    - Server side tasks
      - Discovery tasks
      - Database management
      - Reporting tasks

Contents (continued)

- Avast! Enterprise Administration console
  - Sessions
  - Computer catalog
  - File system shield
  - Mail shield
  - Web shield
  - P2P shield
  - IM shield
  - Network shield
  - Script shield
  - Browser protection
  - Behavior shield
  - Firewall shield
  - Antispam shield

Contents (continued)

- Avast! Enterprise Administration console
  - Sandbox
  - Exchange shield
  - Sharepoint shield
  - Dynamic computer groups
  - Enterprise Administration servers
  - Users
  - Scheduler
  - Installation packages
  - Events

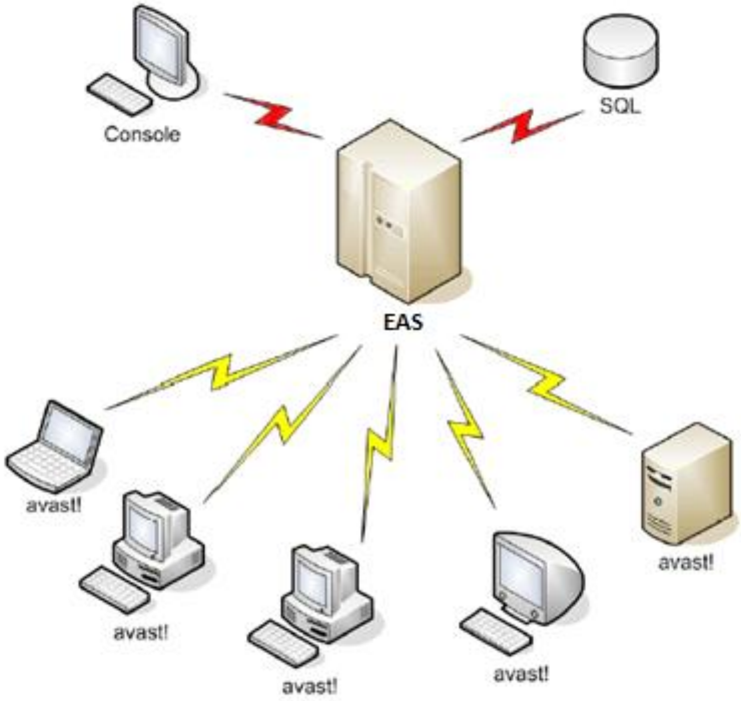
AEA

INTRODUCTION TO AVAST! ENTERPRISE ADMINISTRATION

General information

- avast! Enterprise administration (AEA) is a suite of powerful tools to help network administrators manage the avast! antivirus product line across their whole enterprise.
- The AEA system consists of the following components:
  - avast! Enterprise Server (AES)
    - the heart of AEA that provides the business logic for the whole system
  - SQL Database
    - serves as data storage for all policies, security settings and client information
  - Administration Console
    - the program interface which the administrator uses to manage the whole system
- These three components work together with the avast! antivirus products deployed on individual workstations and servers on the network to provide the best possible protection against malware and to minimize the effort needed to manage and monitor their current status.
- The brain of the whole system is the EAS (avast! Enterprise Server). This is Where all the hard work is done.

General information



- The managed machines connect only to the EAS to download the latest policies and to report their status and scan results.
- The avast! Enterprise Administration Console also connects directly to the EAS.
- The EAS is based on an SQL Database – either a dedicated MS SQL 2008 R2 if available, or for small and medium-size networks, on its lightweight version, SQL Server Express 2008 R2, which is included in the AEA installation package (alternatively, one can use the free version of SQL Server 2005,2008 "SQL Server 2005/2008 Express").
- It is assumed that the EAS machine can connect to the Internet via HTTP protocol.

General information

- For larger networks, the EAS is expected to be installed on a dedicated computer.

- It is also possible to deploy multiple EAS's (each having its own database). These can then be instructed to replicate their databases (requires SQL with full text and replication support) on a regular basis, and also to upload all scanning results to a dedicated EAS on which enterprise-wide reporting can be carried out.

- The administrator can choose from two communication models used by the EAS and the clients: PUSH or POP.
  - The POP model is necessary for larger networks and for networks with roaming users. Each EAS can scale up to tens of thousands of client computers, provided they are all connected by a local area network.

AEA

SYSTEM REQUIREMENTS

System requirements

- **Microsoft Windows XP** (any Edition with the latest Service Pack 3)
- **Microsoft Windows Vista** (any Edition with the latest Service Pack, 32-bit or 64-bit, except Starter Edition)
- **Microsoft Windows 7** (any Edition with the latest Service Pack, 32-bit or 64-bit)
- **Microsoft Windows Server 2003** (any Edition with the latest Service Pack, 32-bit or 64-bit, incl. Small Business Server)
- **Microsoft Windows Server 2003 R2** (any Edition with latest Service Pack, 32-bit or 64-bit, incl. Small Business Server)
- **Microsoft Windows Server 2008** (any Edition with latest Service Pack, 32-bit or 64-bit, incl. Small Business Server, except Server Core)
- **Microsoft Windows Server 2008 R2** (any Edition with latest Service Pack, 32-bit or 64-bit, incl. Small Business Server, except Server Core)
- **Microsoft Windows Small Business Server 2011**

- Free **Microsoft SQL Server 2008 R2 Express** (supplied as an optionally installable component with **avast! Enterprise Administration**) or full **Microsoft SQL Server 2008 R2** (required for the replication service to support multiple **avast! Enterprise Administration Servers** in very complex networks with **more than 1000 computers and/or servers in any combination**).

System requirements

- **Internet Explorer 6.x** or higher.
- **Internet** connection (to download and register the product, and for updates of the **Mirror** from the **AVAST** update server).
- **Domain** network or **Windows workgroup** membership.
- Valid and reachable **SMTP** Server.

- **Intel Pentium III compatible processor** or above (depends on the requirements of the used operating system version and other 3rd party software installed).
- **512 MB RAM** or above (depends on the requirements of the used operating system version and other 3rd party software installed).
- **800 MB** of free hard disk space.
- Optimally standard screen resolution not less than **1024 x 768** pixels.

- **Note:**
  avast! Enterprise Administration is not supported (is not compatible, cannot be installed and won't run) on **DOS**, **Microsoft Windows 3.x**, **Microsoft Windows NT 3.x**, **Microsoft Windows NT 4.0**, **Microsoft Windows 95**, **Microsoft Windows 98**, **Microsoft Windows ME**, **Microsoft Windows 2000**, or any other operating systems which aren't specified as supported.

System requirements

- **Administration Console:**
  - **Microsoft Windows XP** (any Edition with the latest Service Pack 3)
  - **Microsoft Windows Vista** (any Edition with the latest Service Pack, 32-bit or 64-bit, except Starter Edition)
  - **Microsoft Windows 7** (any Edition with the latest Service Pack, 32-bit or 64-bit)
  - **Microsoft Windows Server 2003** (any Edition with the latest Service Pack, 32-bit or 64-bit, incl. Small Business Server)
  - **Microsoft Windows Server 2003 R2** (any Edition with latest Service Pack, 32-bit or 64-bit, incl. Small Business Server)
  - **Microsoft Windows Server 2008** (any Edition with latest Service Pack, 32-bit or 64-bit, incl. Small Business Server, except Server Core)
  - **Microsoft Windows Server 2008 R2** (any Edition with latest Service Pack, 32-bit or 64-bit, incl. Small Business Server, except Server Core)
  - **Microsoft Windows Small Business Server 2011**

  - 128MB recommended
  - 250MB hard disk space
  - Internet Explorer 6 or higher

Note: The Minimum Windows system requirements have to be met!

System requirements

- 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.

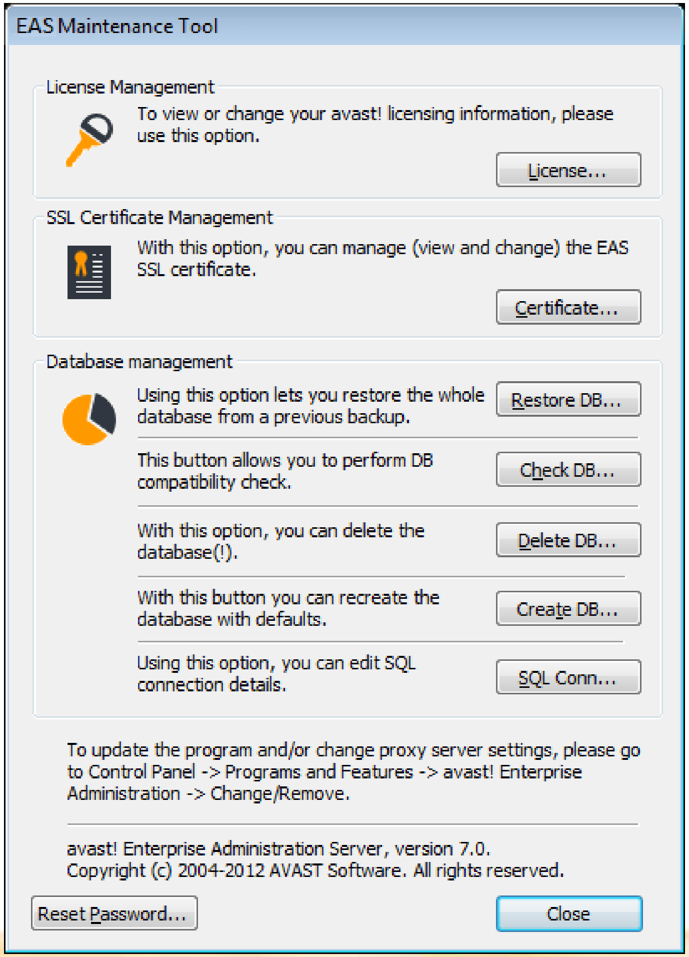
- SQL full versions vs SQL Free/Express versions
    - http://technet.microsoft.com - The TechNet Library contains technical documentation for IT professionals using Microsoft products, tools, and technologies.
    - http://msdn.microsoft.com - MSDN Library, an essential source of information for developers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

- For help with installation, please refer to the Installation Guide for avast! Endpoint Protection (Plus) and avast! Endpoint Protection Suite (Plus).

AEA

EAS MAINTENANCE TOOL

EAS maintenance tool



EAS Maintenance Tool

License Management

To view or change your avast! licensing information, please use this option.

SSL Certificate Management

With this option, you can manage (view and change) the EAS SSL certificate.

Database management

Using this option lets you restore the whole database from a previous backup.

This button allows you to perform DB compatibility check.

With this option, you can delete the database(!).

With this button you can recreate the database with defaults.

Using this option, you can edit SQL connection details.

To update the program and/or change proxy server settings, please go to Control Panel -> Programs and Features -> avast! Enterprise Administration -> Change/Remove.

avast! Enterprise Administration Server, version 7.0.
Copyright (c) 2004-2012 AVAST Software. All rights reserved.

- There are certain maintenance tasks that cannot be performed from the AEA console but instead must be done directly on the server. For most of these tasks, there's a special program called the "EAS Maintenance Tool."

- EAS maintenance tools can be started via the START menu:

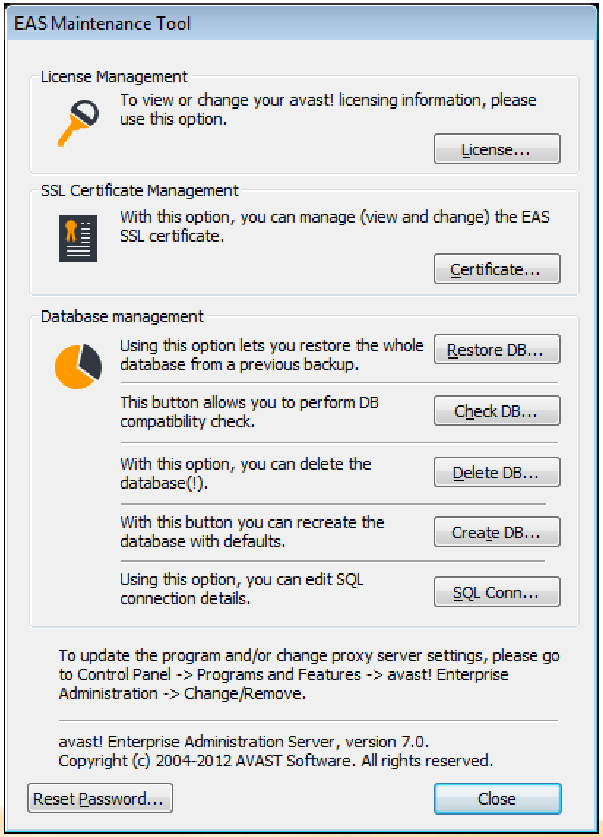
  -> Programs/All programs

  -> avast! Enterprise Administration

  -> EAS Maintenance

EAS maintenance tool

To view or change your avast! license, click the License button.



License Management

To view or change your avast! licensing information, please use this option.

SSL Certificate Management

With this option, you can manage (view and change) the EAS SSL certificate.

Database management

Using this option lets you restore the whole database from a previous backup.

This button allows you to perform DB compatibility check.

With this option, you can delete the database(!).

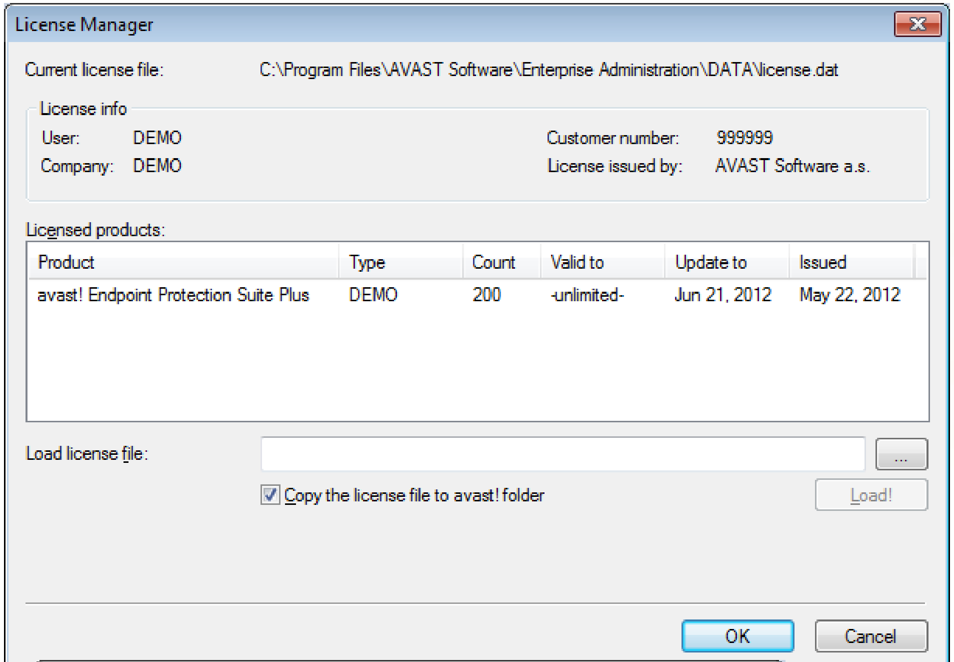
With this button you can recreate the database with defaults.

Using this option, you can edit SQL connection details.

To update the program and/or change proxy server settings, please go to Control Panel -> Programs and Features -> avast! Enterprise Administration -> Change/Remove.

avast! Enterprise Administration Server, version 7.0.
Copyright (c) 2004-2012 AVAST Software. All rights reserved.

After the license file has been successfully uploaded, hit the yes button to restart the avast! Management service.



Current license file: C:\Program Files\AVAST Software\Enterprise Administration\DATA\license.dat

License info

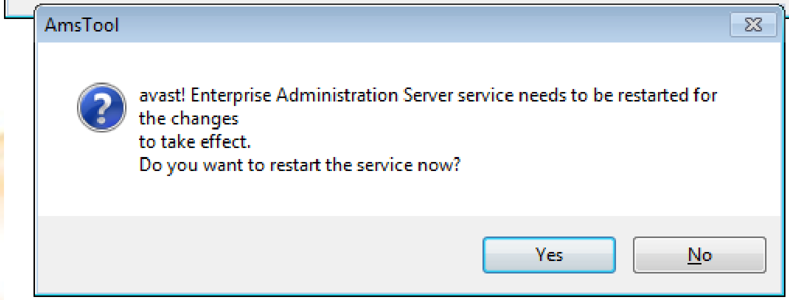
User: DEMO
Company: DEMO
Customer number: 999999
License issued by: AVAST Software a.s.

Licensed products:

Product	Type	Count	Valid to	Update to	Issued
avast! Endpoint Protection Suite Plus	DEMO	200	-unlimited-	Jun 21, 2012	May 22, 2012

Load license file:

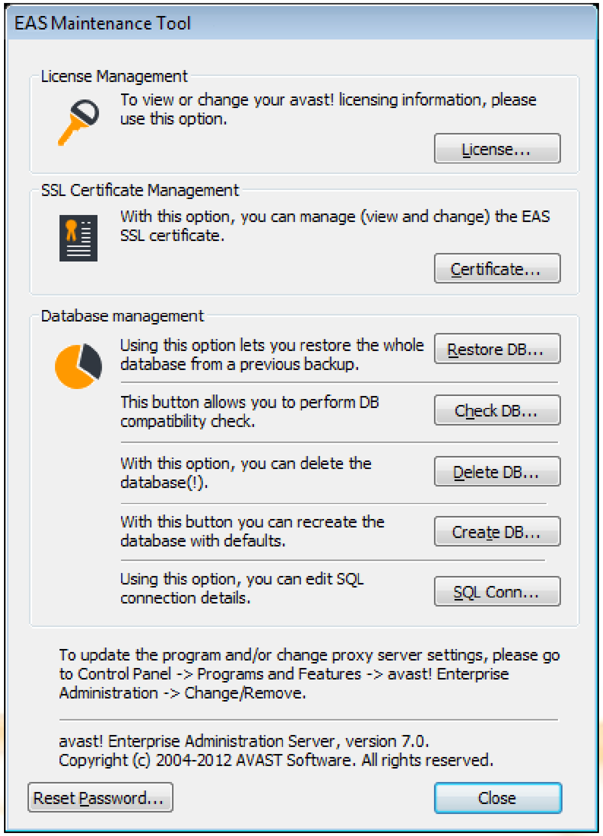
☑ Copy the license file to avast! folder



avast! Enterprise Administration Server service needs to be restarted for the changes
to take effect.
Do you want to restart the service now?

EAS maintenance tool

If the certificate needs to be replaced (corrupted/expired), hit the Certificate button .



EAS Maintenance Tool

License Management

To view or change your avast! licensing information, please use this option.

License...

SSL Certificate Management

With this option, you can manage (view and change) the EAS SSL certificate.

Certificate...

Database management

Using this option lets you restore the whole database from a previous backup.

Restore DB...

This button allows you to perform DB compatibility check.

Check DB...

With this option, you can delete the database(!).

Delete DB...

With this button you can recreate the database with defaults.

Create DB...

Using this option, you can edit SQL connection details.

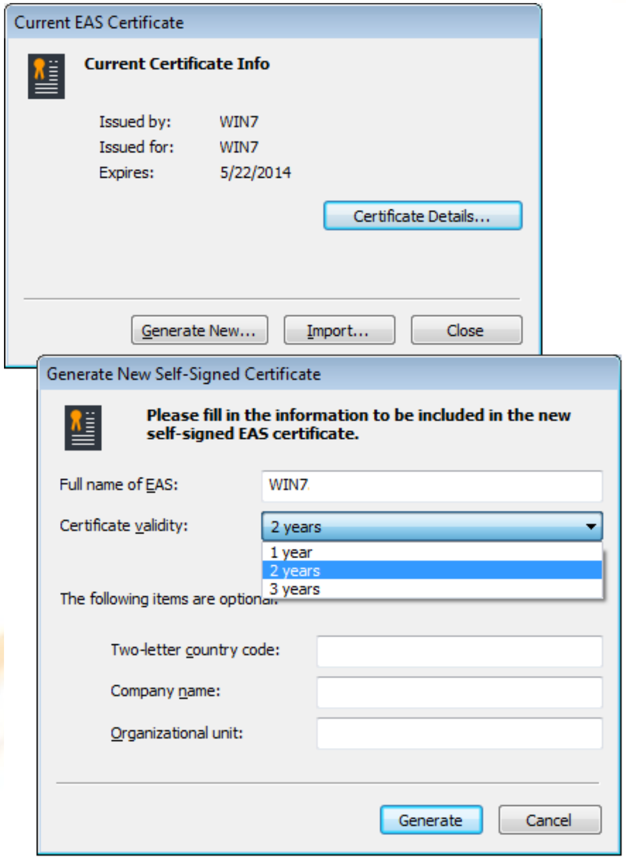
SQL Conn...

To update the program and/or change proxy server settings, please go to Control Panel -> Programs and Features -> avast! Enterprise Administration -> Change/Remove.

avast! Enterprise Administration Server, version 7.0.
Copyright (c) 2004-2012 AVAST Software. All rights reserved.

Reset Password... Close

To change/create the server SSL certificate see the steps below:



Current EAS Certificate

Current Certificate Info

Issued by:	WIN7
Issued for:	WIN7
Expires:	5/22/2014

Certificate Details...

Generate New... Import... Close

Generate New Self-Signed Certificate

Please fill in the information to be included in the new self-signed EAS certificate.

Full name of EAS: WIN7

Certificate validity: 2 years

1 year
2 years
3 years

The following items are optional:

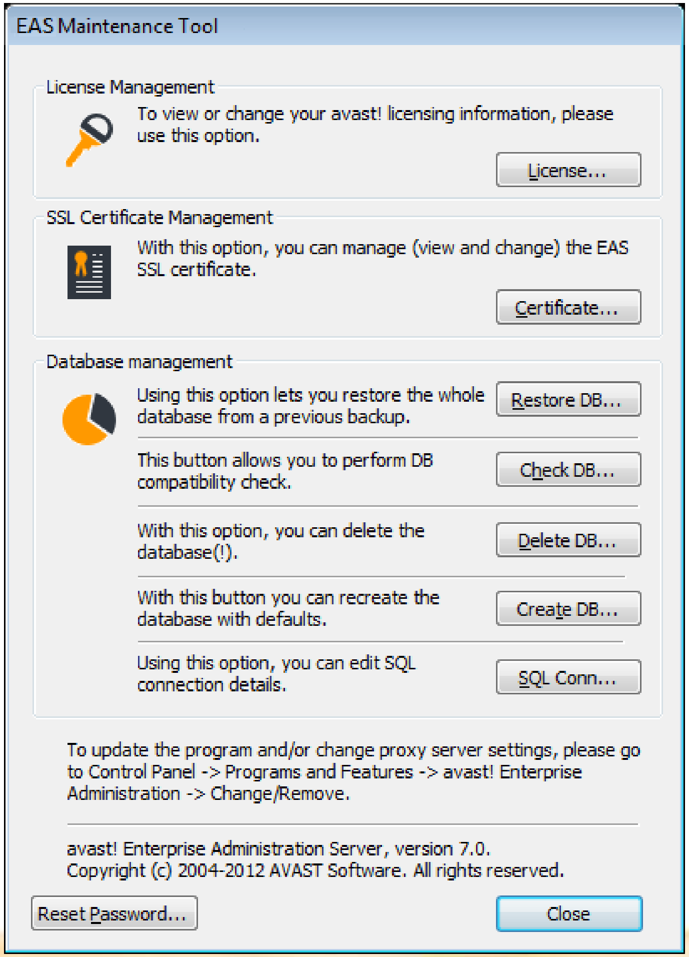
Two-letter country code:

Company name:

Organizational unit:

Generate Cancel

EAS maintenance tool



EAS Maintenance Tool

License Management

To view or change your avast! licensing information, please use this option.

SSL Certificate Management

With this option, you can manage (view and change) the EAS SSL certificate.

Database management

Using this option lets you restore the whole database from a previous backup.

This button allows you to perform DB compatibility check.

With this option, you can delete the database(!).

With this button you can recreate the database with defaults.

Using this option, you can edit SQL connection details.

To update the program and/or change proxy server settings, please go to Control Panel -> Programs and Features -> avast! Enterprise Administration -> Change/Remove.

avast! Enterprise Administration Server, version 7.0.
Copyright (c) 2004-2012 AVAST Software. All rights reserved.

- Restore DB
  - Restores the database from the backup. (Database backups can be done as a Database management task from the administration console, and can even be scheduled to run periodically.)

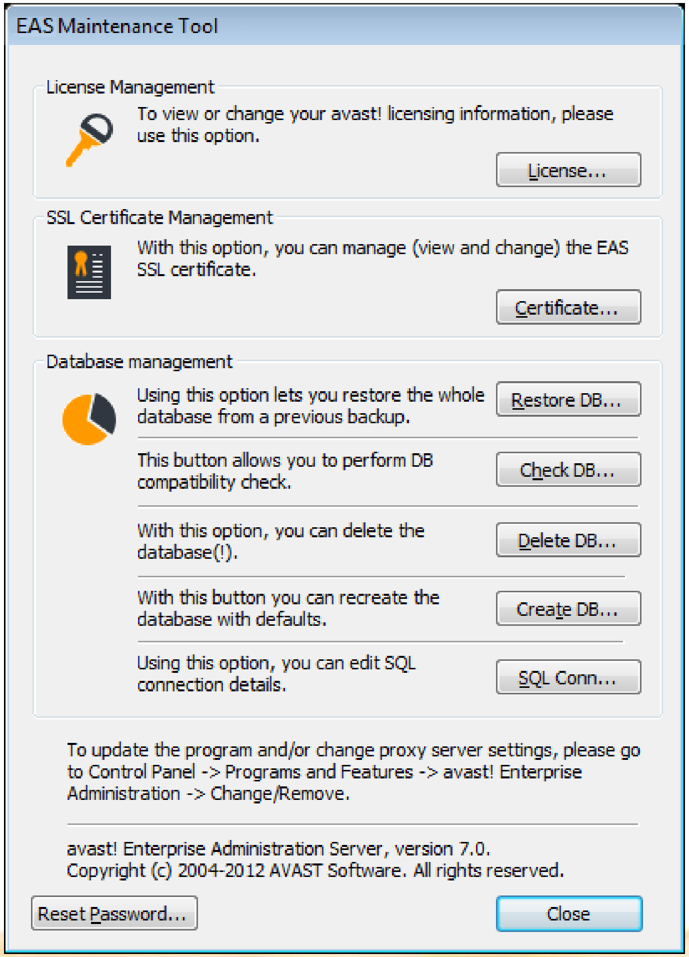
    Note: restoring the database will delete its current contents. It’s therefore a good idea to create a new, separate backup immediately before doing the restore.

- Check DB
  - Checks the validity of the database.

- Delete DB
  - Deletes and reinitializes the database.

    Note: by deleting or recreating the database, all its previous contents will be deleted. Be sure to create a backup before performing these operations.

EAS maintenance tool



EAS Maintenance Tool

License Management

To view or change your avast! licensing information, please use this option.

SSL Certificate Management

With this option, you can manage (view and change) the EAS SSL certificate.

Database management

Using this option lets you restore the whole database from a previous backup.

This button allows you to perform DB compatibility check.

With this option, you can delete the database(!).

With this button you can recreate the database with defaults.

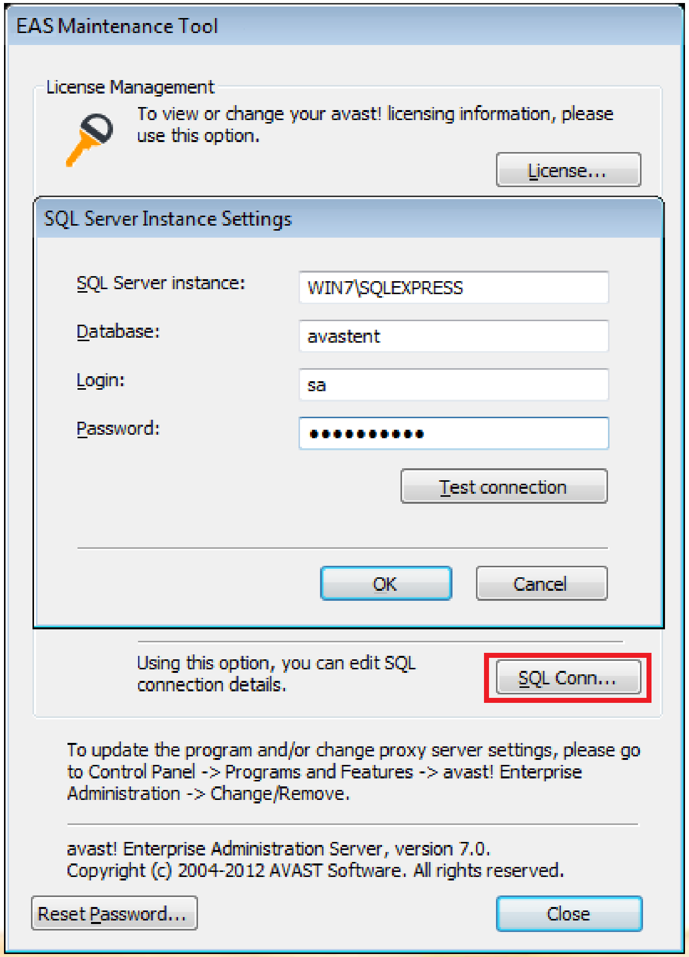
Using this option, you can edit SQL connection details.

To update the program and/or change proxy server settings, please go to Control Panel -> Programs and Features -> avast! Enterprise Administration -> Change/Remove.

avast! Enterprise Administration Server, version 7.0.
Copyright (c) 2004-2012 AVAST Software. All rights reserved.

- Create DB
  - If the previous DB was deleted/corrupted you can create a new DB by clicking on the Create DB button.

EAS maintenance tool



EAS Maintenance Tool

License Management

To view or change your avast! licensing information, please use this option.

SQL Server Instance Settings

SQL Server instance: WIN7\SQLEXPRESS

Database: avastent

Login: sa

Password: ●●●●●●●●●●●

Using this option, you can edit SQL connection details.

To update the program and/or change proxy server settings, please go to Control Panel -> Programs and Features -> avast! Enterprise Administration -> Change/Remove.

avast! Enterprise Administration Server, version 7.0.
Copyright (c) 2004-2012 AVAST Software. All rights reserved.

- SQL Connection
  - here you can change the database connection details. Use this option when you want to move the database to another SQL server.
  - You should create a backup, change the database connection details, and then restore the database from the backup.

- Use a backslash when specifying the SQL instance name
  - For more details see the following article on the avast web site:
    - https://support.avast.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1289

AEA

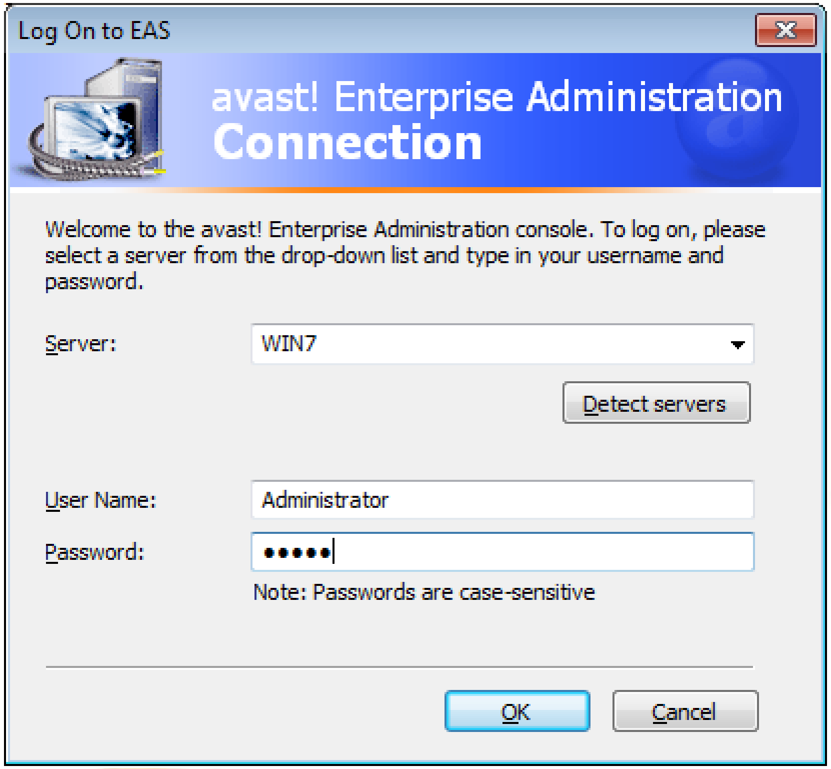
AEA CONSOLE

Log On screen

AEA console

- After the console installation is complete, you can immediately start using the program. Go to the Start menu, and select AEA Console to start the console. The Log On window will open.

- Detect server
  - Type in the name of the machine on which you've installed the EAS, or press the Detect server button to try to discover all available EAS's on the network.
  - If the Detect servers feature does not work you can speficy the server manually:
    - DNS name
    - IP address
    - Localhost



Log On to EAS

avast! Enterprise Administration Connection

Welcome to the avast! Enterprise Administration console. To log on, please select a server from the drop-down list and type in your username and password.

Server: WIN7

User Name: Administrator

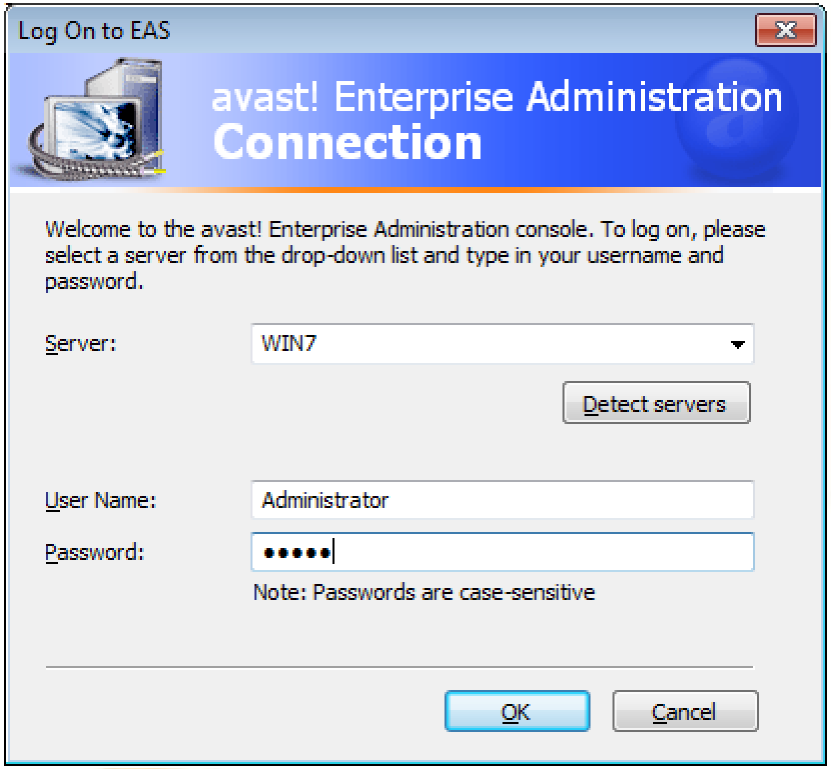
Password: •••••

Note: Passwords are case-sensitive

Log On screen

AEA console

- User name
  - **Do NOT** localize the User name. It should be left as Administrator (not e.g. Administrador.)
- Password
  - Don‘t use Windows logon credentials to log in !
- **Note:**
  - The default username is **Administrator**, and the password is **admin**. We strongly recommend changing the password as soon as possible after logging on to the server, as leaving the password set to its default value may compromise system security.
  - To change the password, open the EAS maintenance tool and click Reset Password



Log On to EAS

avast! Enterprise Administration Connection

Welcome to the avast! Enterprise Administration console. To log on, please select a server from the drop-down list and type in your username and password.

Server: WIN7

User Name: Administrator

Password: •••••

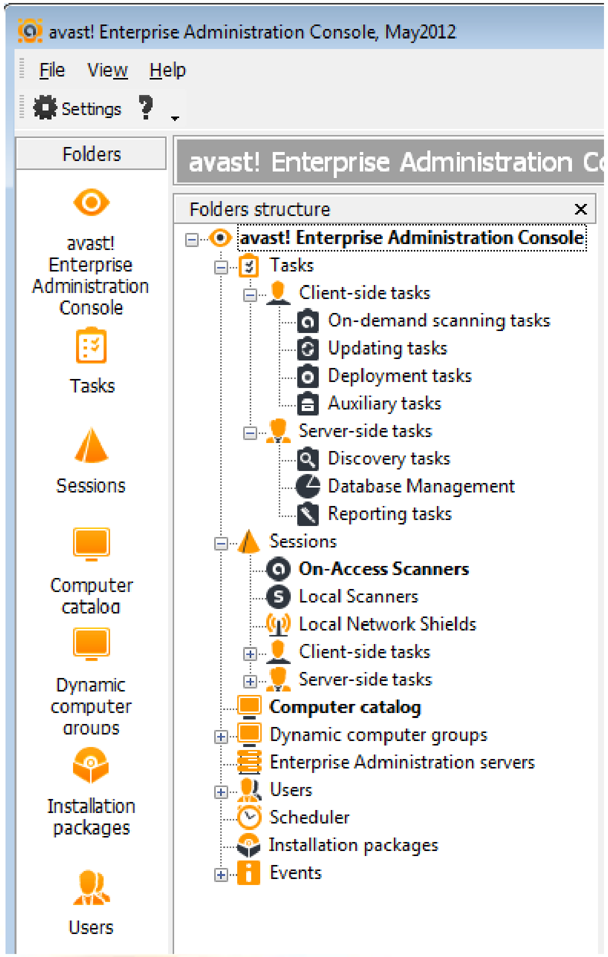
Note: Passwords are case-sensitive

AEA console

OVERVIEW

AEA console

Overview



- The AEA console is organized into folders (besides the main Toolbar) that act as containers for various administration objects. These are the most important AEA console objects:

Main toolbar

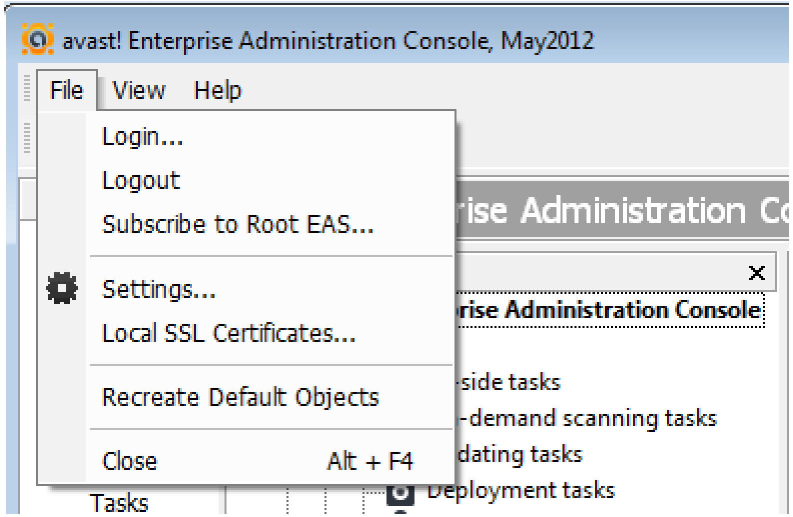
- Program settings
- EAS, mirror status, logs

Folder structure

- Tasks
  - Client-side tasks
  - Server-side tasks
- Sessions
- Computer catalog/groups
  - Computer/computer group settings
- Dynamic groups
- Alerts
- Installation packages
- Events

AEA console

Overview



Main toolbar settings

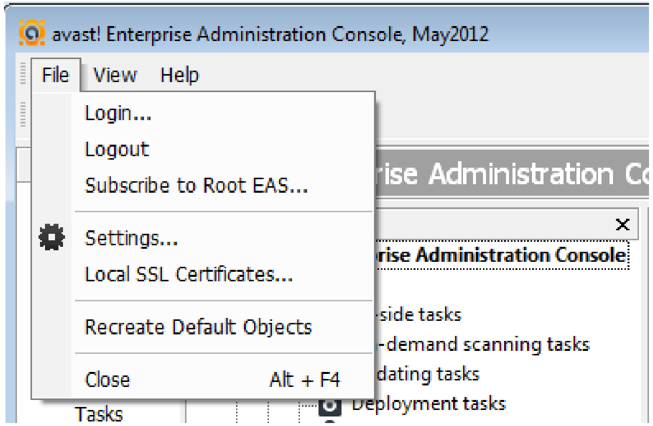
- Login
  - Allows you to log-in as another user (administrator) with different rights
- Logout
  - Current logged user will be automatically logged out.
- Subscribe to Root EAS
  - For more details see the next page
- Settings
  - For more details see the next page
- Local SSL Certificates
  - Opens the certificates management window which allows you to manage trusted EAS certificates
- Recreate default objects
- Close – close the AEA console

AEA console

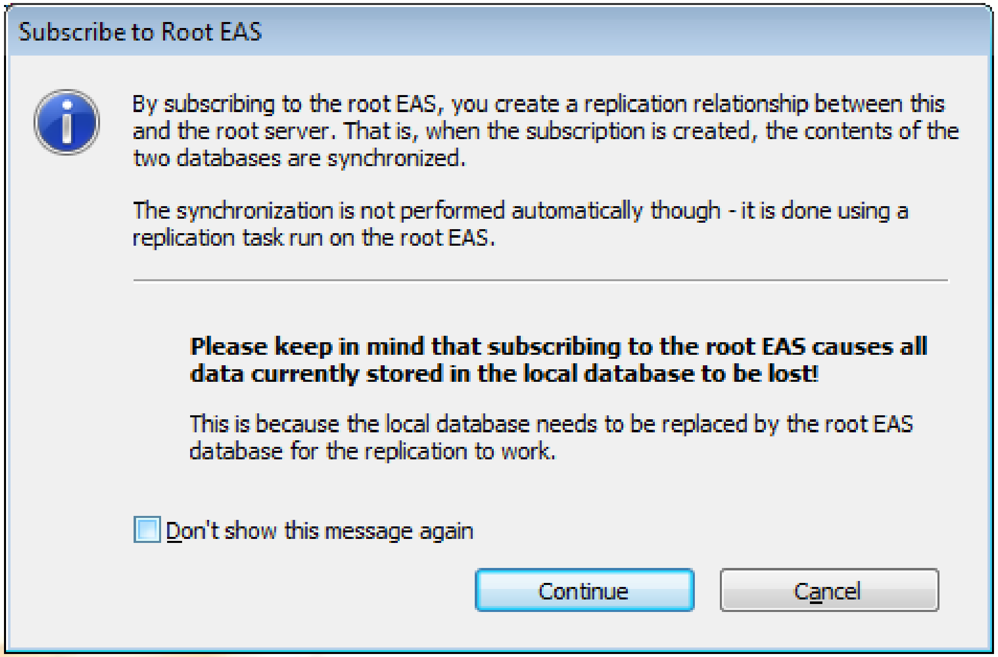
Overview

Main toolbar settings

Subscribe to Root EAS



Connect to each child EAS, i.e., to each EAS except the one you chose as the root, and in the File menu, choose “Subscribe to Root EAS.”



Subscribe to Root EAS

By subscribing to the root EAS, you create a replication relationship between this and the root server. That is, when the subscription is created, the contents of the two databases are synchronized.

The synchronization is not performed automatically though - it is done using a replication task run on the root EAS.

Please keep in mind that subscribing to the root EAS causes all data currently stored in the local database to be lost!

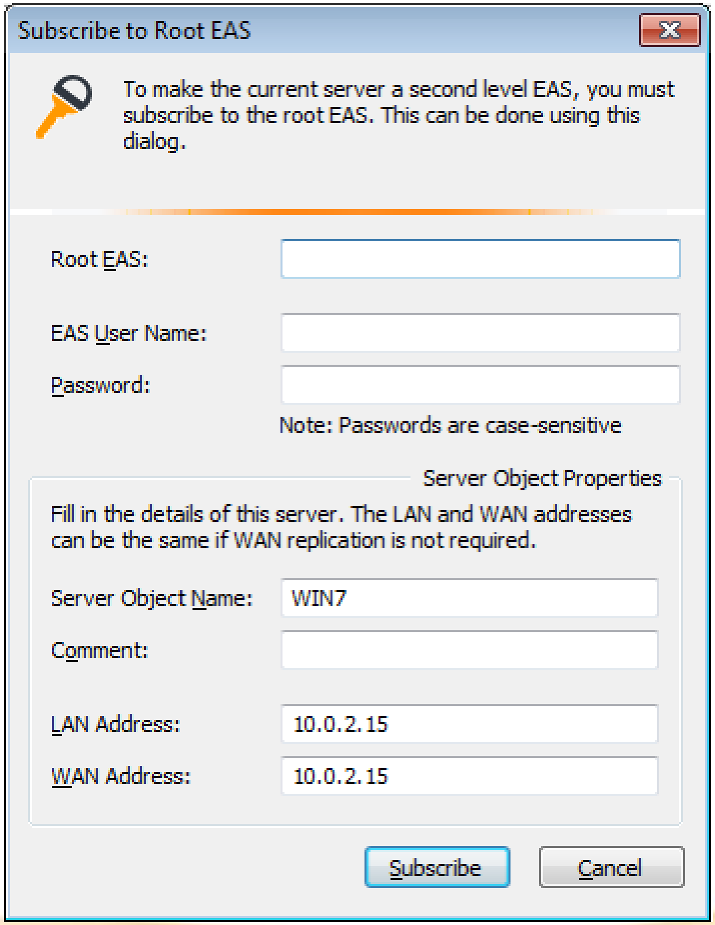
This is because the local database needs to be replaced by the root EAS database for the replication to work.

□ Don't show this message again

AEA console

Overview

Main toolbar settings



Subscribe to Root EAS

To make the current server a second level EAS, you must subscribe to the root EAS. This can be done using this dialog.

Root EAS:

EAS User Name:

Password:

Note: Passwords are case-sensitive

Server Object Properties

Fill in the details of this server. The LAN and WAN addresses can be the same if WAN replication is not required.

Server Object Name: WIN7

Comment:

LAN Address: 10.0.2.15

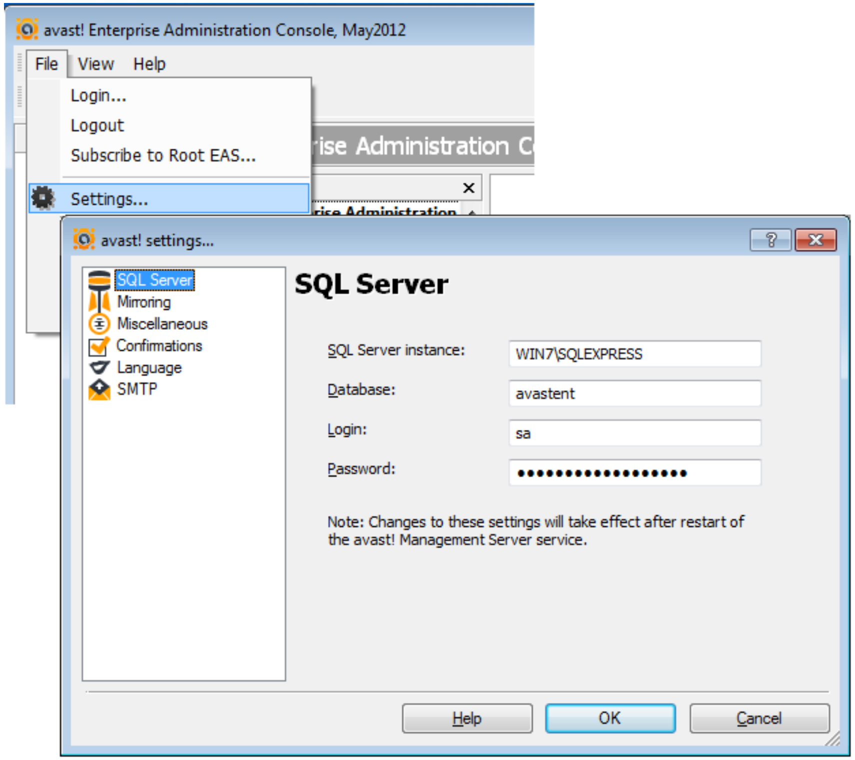
WAN Address: 10.0.2.15

- Root EAS
  - type the address of the root EAS
- EAS User Name and Password
  - fill in the AEA credentials for the root EAS (using the Administrator account is recommended)
- Server Object Name and Comment
  - define how this child server will be presented in the AEA's "Management servers" folder
- LAN Address and WAN Address
  - should contain the IP address of this child EAS
  - the LAN address is typically NATed
  - the WAN address is the outside address

If outside access is not required, use the NATed address in both fields.

AEA console

Overview



SQL Server

SQL Server instance: WIN7\SQLEXPRESS

Database: avastent

Login: sa

Password: ••••••••••••••••••

Note: Changes to these settings will take effect after restart of the avast! Management Server service.

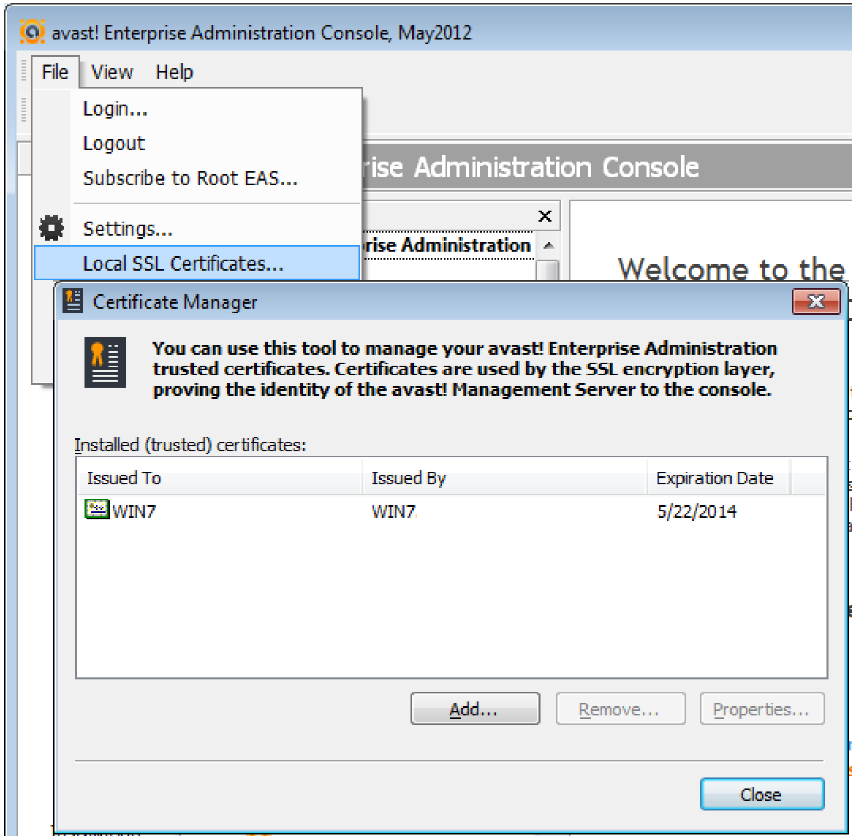
Main toolbar settings

- SQL Server – settings
  - SQL server name and instance
  - DB name
  - Login/Password
- Mirroring – settings
  - Auto sync
  - Mirror http port
  - Second level mirrors
- Miscellaneous
  - Mark engines as offline after..
  - Disconnect inactive user
  - Query limit (e.g. events)
  - Custom logo for reports
- Confirmations
  - Ask before session is deleted..
  - Ask before alert is deleted..
- Language
- SMTP
  - Management server SMTP settings

AEA console

Overview

Main toolbar settings



You can use this tool to manage your avast! Enterprise Administration trusted certificates. Certificates are used by the SSL encryption layer, proving the identity of the avast! Management Server to the console.

Installed (trusted) certificates:

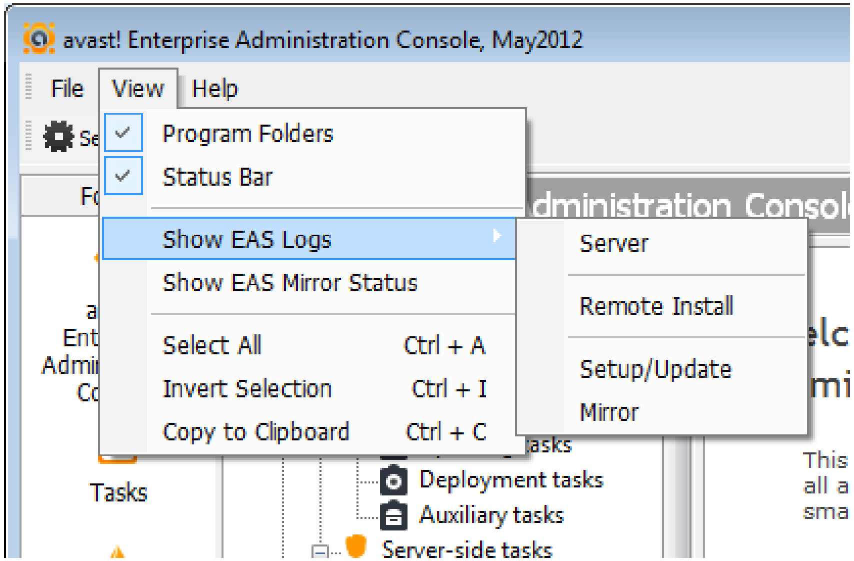
Issued To	Issued By	Expiration Date
WIN7	WIN7	5/22/2014

- Certificate manager
  - Here, AEA trusted certificates can be:
    - added
    - removed
    - modified

- Certificates are used by the SSL encryption layer, proving the identity of the avast! Enterprise Server to the AEA console.

AEA console

Overview


avast! Enterprise Administration Console, May2012

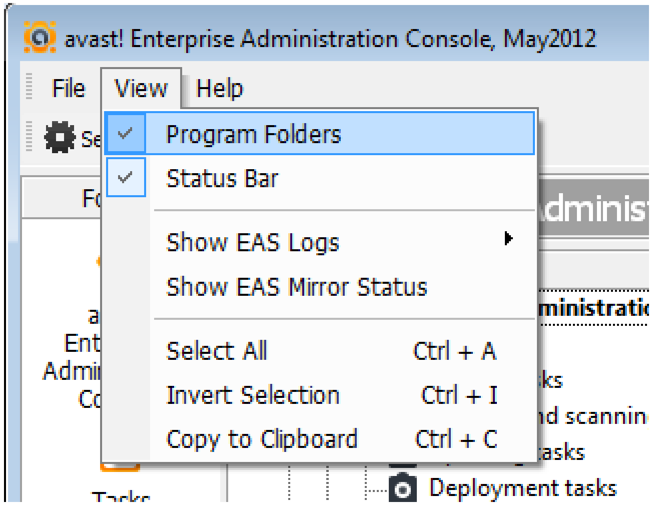
Main toolbar settings

- Program folders
  - Allows you to close/open the Folder structure in the AEA console
- Status bar
  - Allows you to close/open the status bar
- Show EAS logs
  - All EAS logs can be displayed in the Internet browser, without accessing them manually.
- Show EAS Mirror status
- Select all
- Invert selection
- Copy to clipboard

AEA console

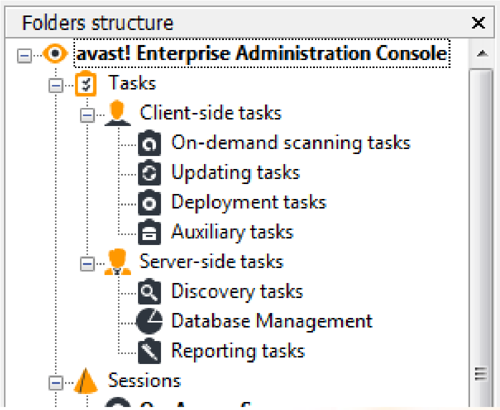
Overview

Main toolbar settings



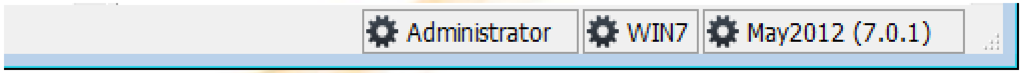
- **Program folders**

  Allows you to close/open the Folder structure in the AEA console



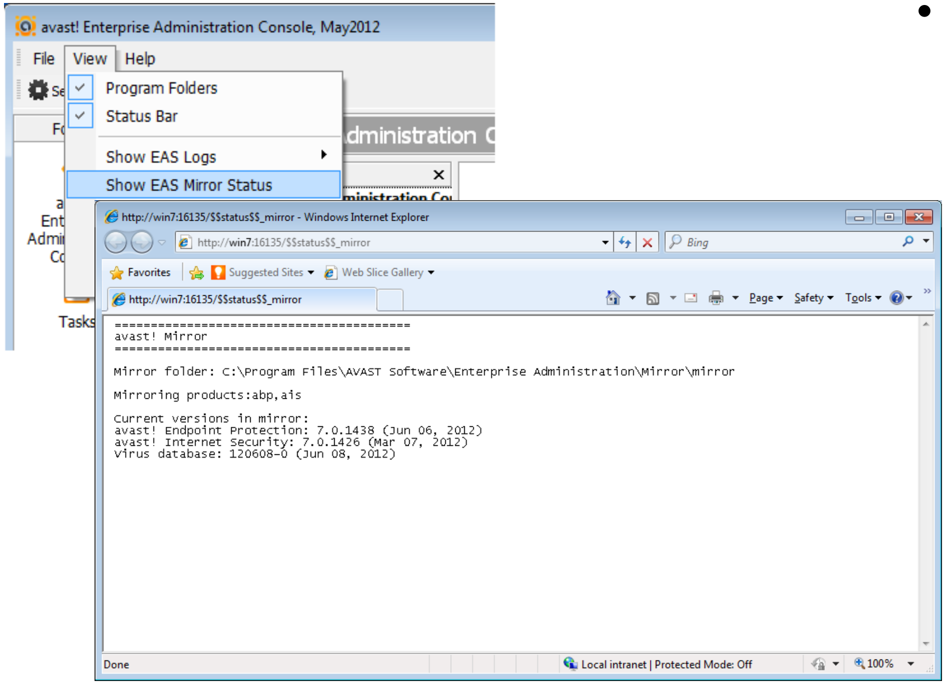
- **Status bar**

  Allows you to close/open the status bar



AEA console

Overview


avast! Enterprise Administration Console, May2012
File
View
Help
Program Folders
Status Bar
Show EAS Logs
Show EAS Mirror Status
http://win7:16135/$$status$$_mirror - Windows Internet Explorer
http://win7:16135/$$status$$_mirror
Bing
Favorites
Suggested Sites
Web Slice Gallery
Page
Safety
Tools
Done
Local intranet | Protected Mode: Off
100%

```
==========================================
avast! Mirror
==========================================

Mirror folder: C:\Program Files\AVAST Software\Enterprise Administration\Mirror\mirror

Mirroring products:abp,ais

Current versions in mirror:
avast! Endpoint Protection: 7.0.1438 (Jun 06, 2012)
avast! Internet Security: 7.0.1426 (Mar 07, 2012)
Virus database: 120608-0 (Jun 08, 2012)
```

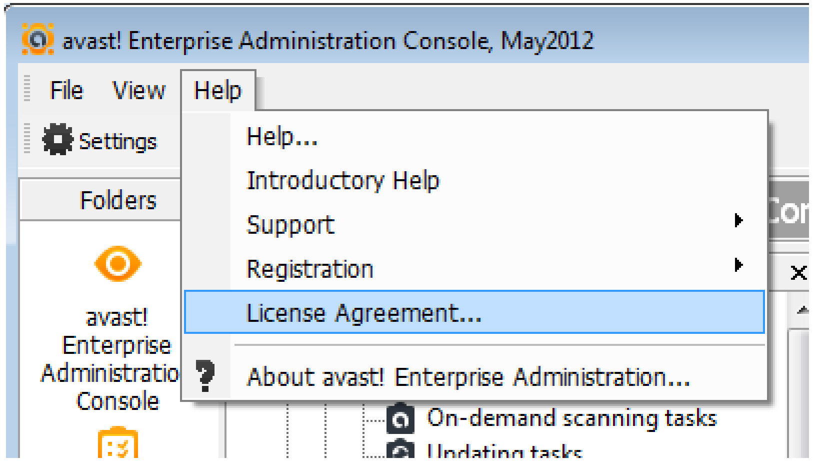
Main toolbar settings

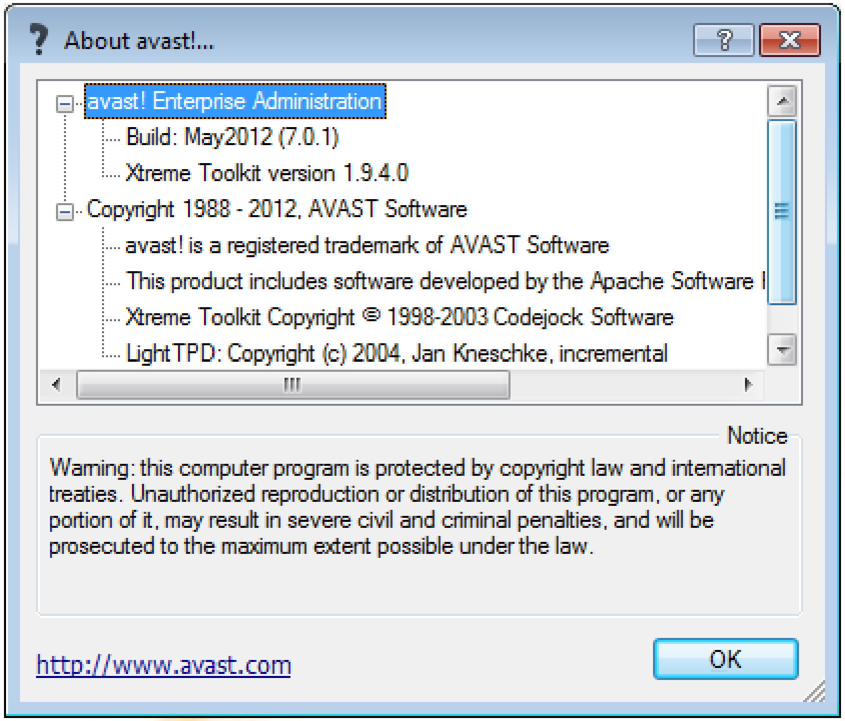
- Show EAS mirror status - displays the following Information:
  - General information
    - Mirror installation folder
    - Mirrored products
  - Current versions of:
    - AEA
    - avast! managed client
    - VPS (virus database)

AEA console

Overview

Main toolbar settings


avast! Enterprise Administration Console, May2012
File
View
Help
Settings
Folders
avast! Enterprise Administratio Console
Help...
Introductory Help
Support
Registration
License Agreement...
About avast! Enterprise Administration...
On-demand scanning tasks
Updating tasks



avast! Enterprise Administration
- Build: May2012 (7.0.1)
- Xtreme Toolkit version 1.9.4.0

Copyright 1988 - 2012, AVAST Software
- avast! is a registered trademark of AVAST Software
- This product includes software developed by the Apache Software I
- Xtreme Toolkit Copyright © 1998-2003 Codejock Software
- LightTPD: Copyright (c) 2004, Jan Kneschke, incremental

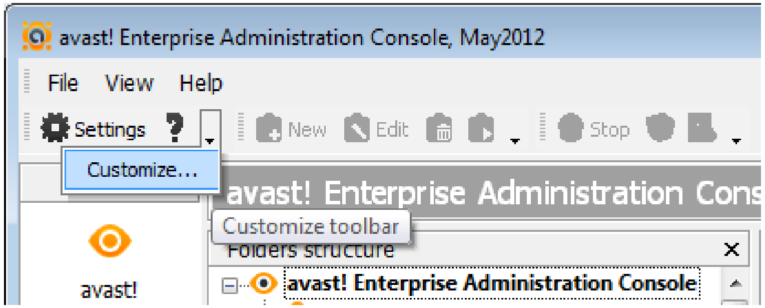
Notice

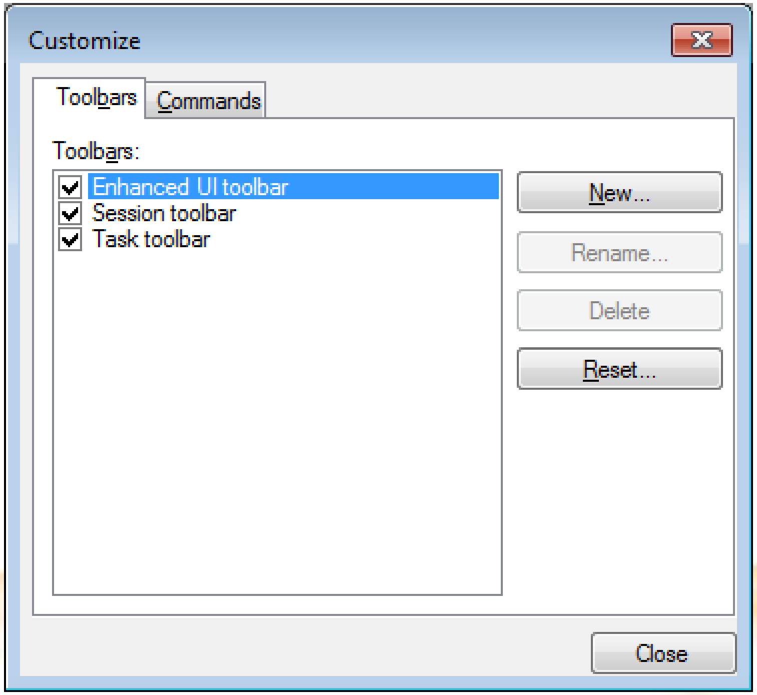
Warning: this computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

http://www.avast.com

AEA console

Overview


avast! Enterprise Administration Console, May2012
File
View
Help
Settings
New
Edit
Stop
Customize…
avast! Enterprise Administration Cons
Customize toolbar
Folders structure
avast!
avast! Enterprise Administration Console



Toolbars:

☑ Enhanced UI toolbar
☑ Session toolbar
☑ Task toolbar

Main toolbar settings

The Settings button will lead you to the avast! Settings.

See page 29.

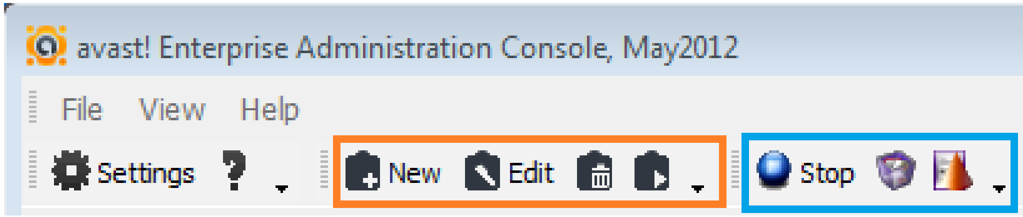
- By default only the Enhanced toolbar is ticked and displayed. Two additional toolbars can be added:

1. Session toolbar
2. Task toolbar

AEA console

Overview

Main toolbar settings



- Session toolbar
  - Allows you to:
    - Create a new task
    - Edit a created task
    - Delete a task
    - Run a selected task

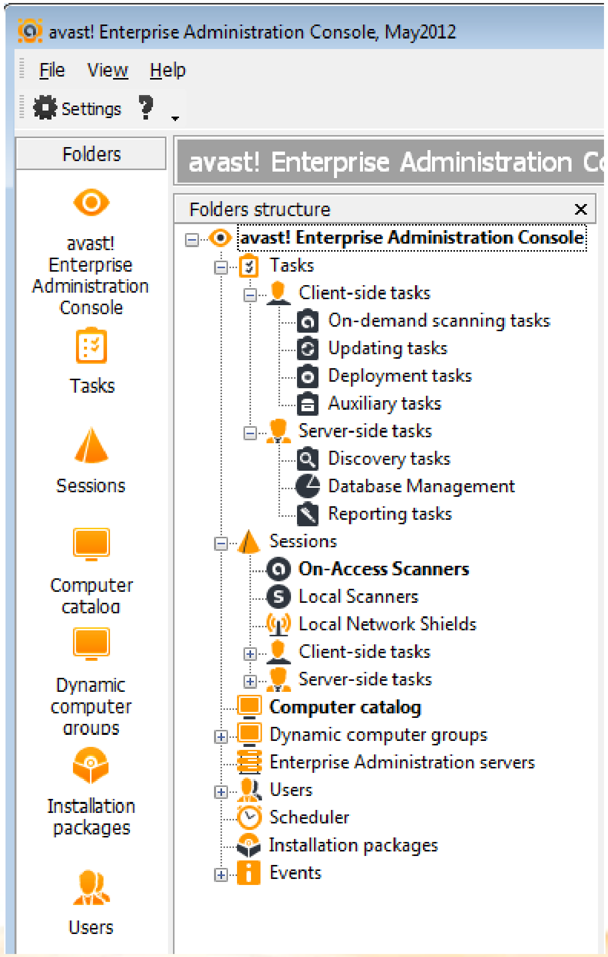
- Task toolbar
  - Allows you to:
    - Stop the current running session
    - Delete a session

AEA console

TASKS

AEA console

Tasks



A task is a definition of a job, i.e., a description of what to do and when. A task also has associated computers on which it should be run. There are many types of tasks in AEA, but the basic distinction is between Client side and Server-side tasks.

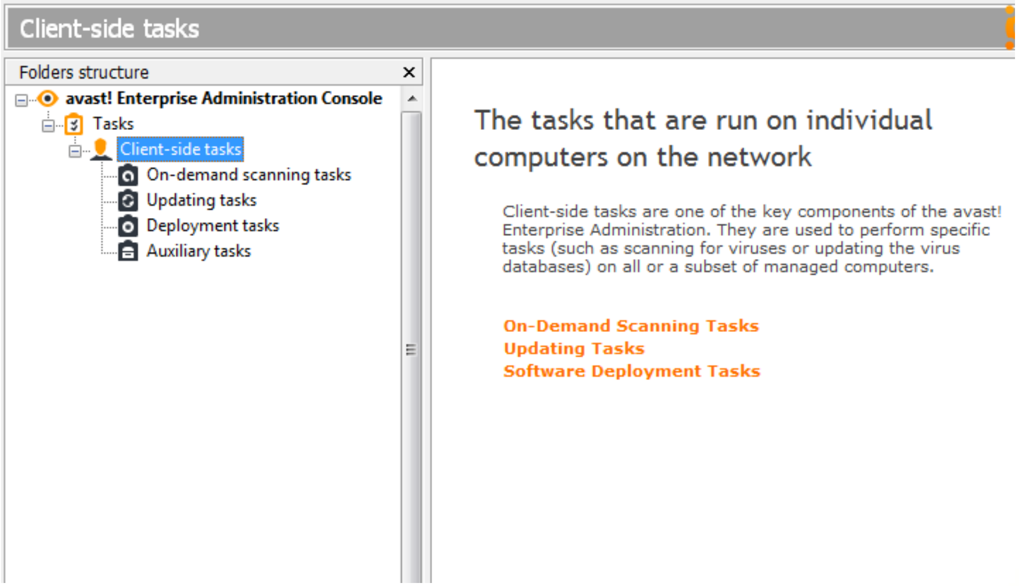
- **Client-Side tasks**
  - can be remotely started/scheduled to run on the client computers (i.e. workstations, servers, etc. – the machines on which the avast! products are deployed).
    - On-demand scanning tasks
    - Updating tasks
    - Deployment tasks
    - Auxiliary tasks
- **Server-side tasks**
  - such as reporting and database maintenance tasks, run on the EAS itself.
    - Discovery tasks
    - Database management
    - Reporting tasks

AEA console

CLIENT-SIDE TASKS

AEA console

Client-side tasks



The tasks that are run on individual computers on the network

Client-side tasks are one of the key components of the avast! Enterprise Administration. They are used to perform specific tasks (such as scanning for viruses or updating the virus databases) on all or a subset of managed computers.

On-Demand Scanning Tasks
Updating Tasks
Software Deployment Tasks

- Client-side tasks are one of the key components of the avast! Enterprise Administration. They are used to perform specific tasks (scanning for viruses, updating the virus database etc..) on all or on a subset of the managed computers.

- The tasks can either be run on-demand, or by creating a schedule. To run an on-demand task on a selected group of computers, you can drag‘n‘drop the task to a group in the Computer Catalog.

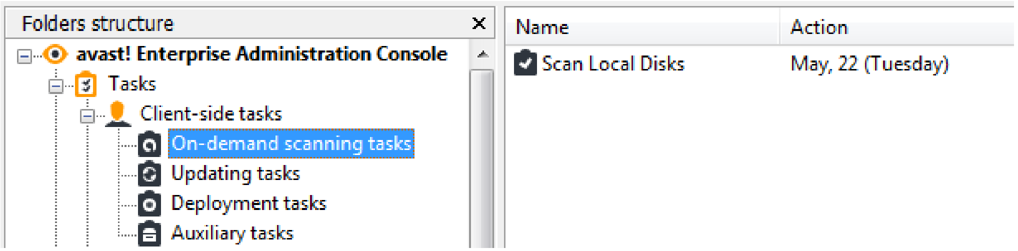
AEA Client-side tasks

ON-DEMAND SCANNING TASKS

AEA console

Client-side tasks

On-demand scanning tasks



Folders structure

- avast! Enterprise Administration Console
  - Tasks
    - Client-side tasks
      - On-demand scanning tasks
      - Updating tasks
      - Deployment tasks
      - Auxiliary tasks

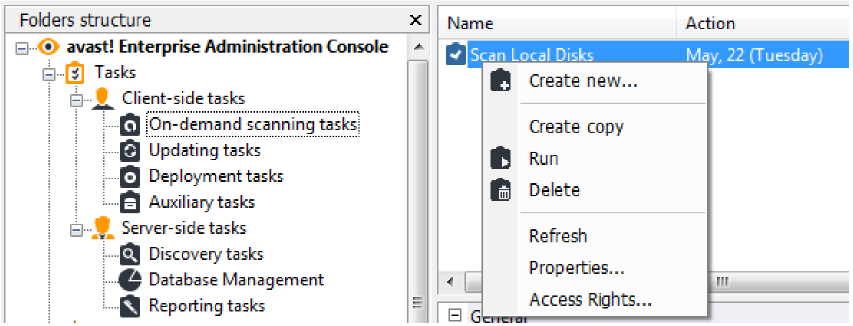
Name	Action
Scan Local Disks	May, 22 (Tuesday)

- AEA makes it easy to do on-demand virus scanning of client machines. The scanning job is defined by creating an On-demand scanning task.
- These tasks can be found in the folder of the same name, under the Client-side tasks folder.

AEA console

Client-side tasks

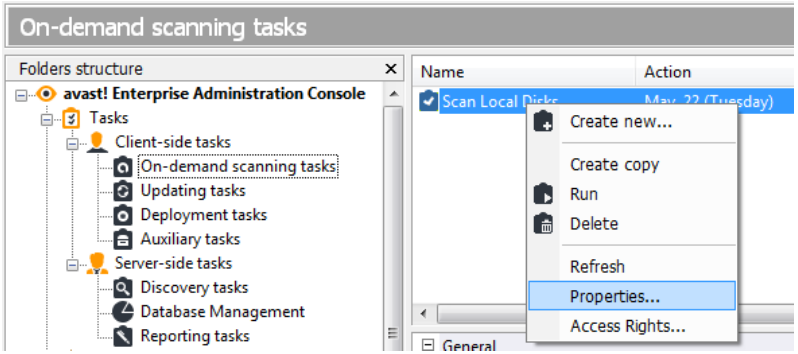
On-demand scanning tasks



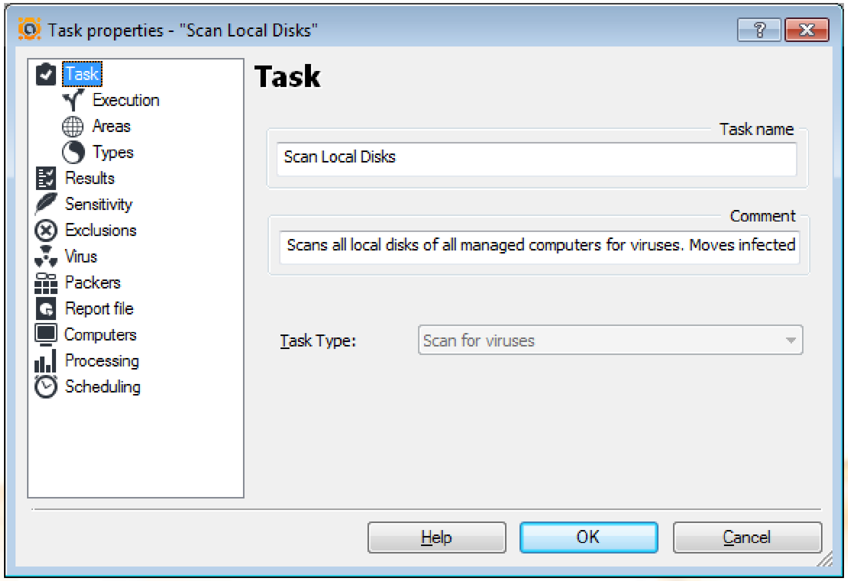
- **Create New**
  - Allows you to create a new task.
- **Delete**
  - Deletes the selected task.
- **Create copy**
  - Creates a new task containing the same settings as the selected task. This new task will be shown in the task list and its name will begin with the word "Copy", e.g. "Copy of Scan: local disks". This option is useful if you want to change the settings of a predefined task (which cannot be changed in the original task).
- **Run**
  - Starts the selected task.
- **Stop**
  - Stops the selected running resident task.
- **Properties**
  - Allows you to edit the selected task.

AEA console

Client-side tasks On-demand scanning tasks



- To edit or define the scan settings, right click on the created scaning task and choose Properties.



Task

Task name: Scan Local Disks

Comment: Scans all local disks of all managed computers for viruses. Moves infected

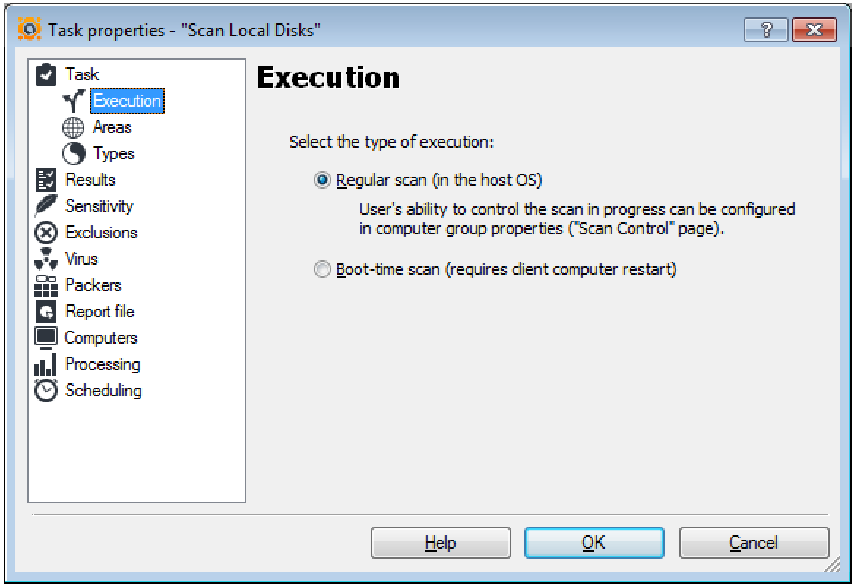
Task Type: Scan for viruses

- The task editor offers a large number of settings, which can be customized e.g.
  - Areas to scan
  - Scan sensitivity
  - Scan results to be posted to the EAS
  - Report file
  - Computer/s on which the task will be run

AEA console

Client-side tasks

On-demand scanning tasks



Task properties - "Scan Local Disks"

Execution

Select the type of execution:

● Regular scan (in the host OS)

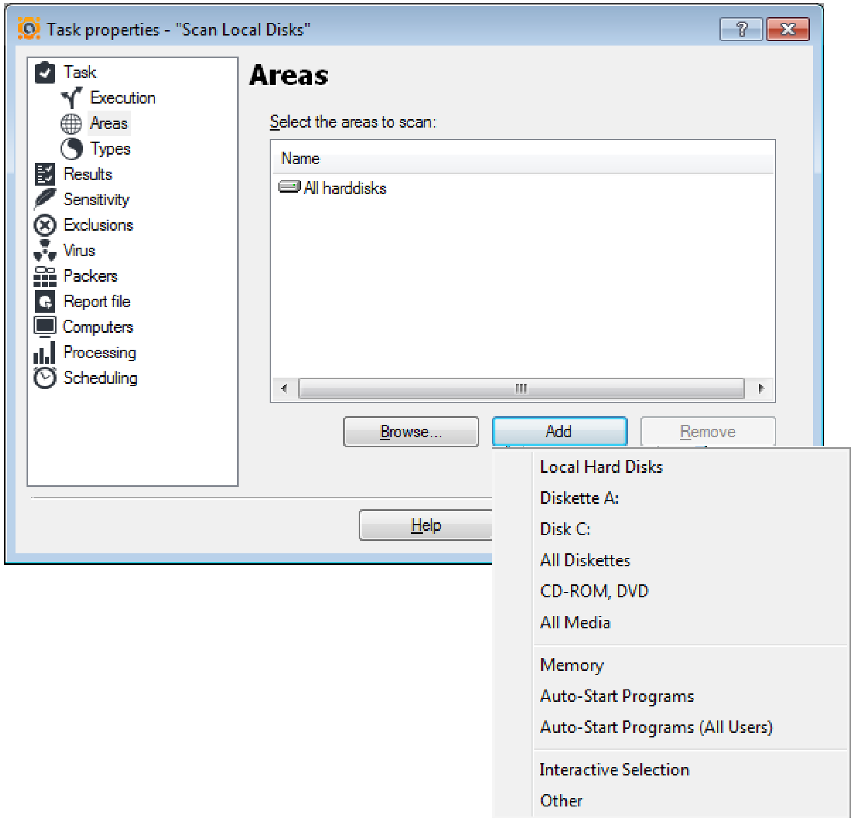
User's ability to control the scan in progress can be configured in computer group properties ("Scan Control" page).

○ Boot-time scan (requires client computer restart)

- Here you can specify the type of scan to be created:
  - Regular scan
    - The user‘s ability to control the scan in progress can be configured in computer group properties (Scan Control page)
  - Boot-time scan (requires client computer restart)
    - The user can abort the scan
    - System files can be skipped

AEA console

Client-side tasks



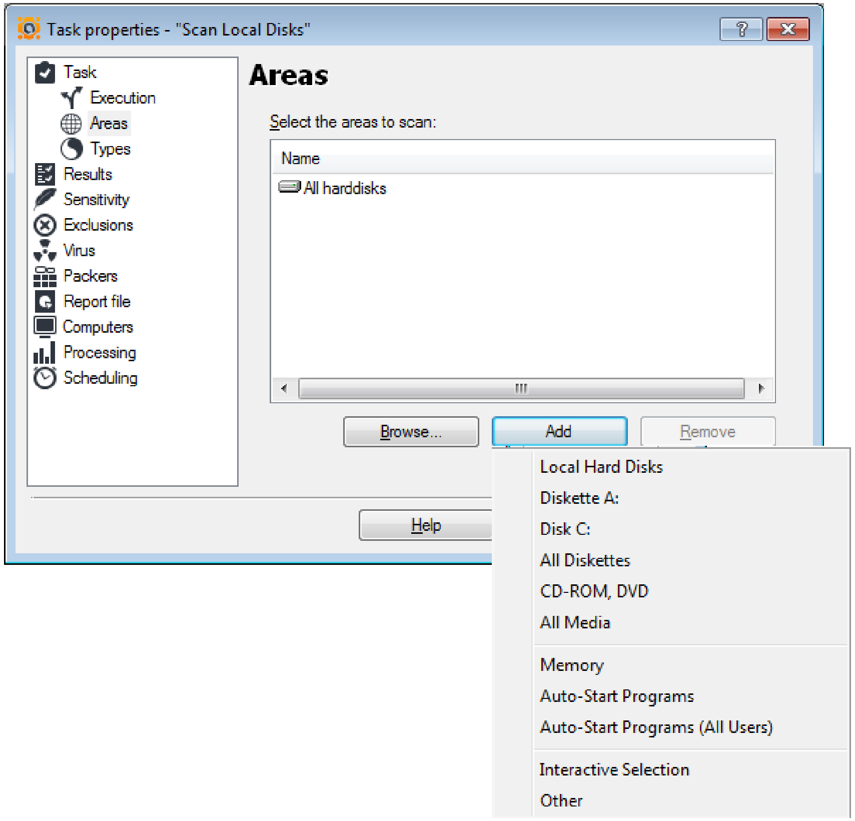
On-demand scanning tasks

- Here you can choose the areas to scan. The default value is "Local hard disks". You can select additional areas, entire folders and/or individual files.
- "**Browse**" button.
  - An Explorer-like window will open; here you can select the areas to scan by checking the particular folders or files.
- "**Add**" button.
  - After clicking this button, a popup menu will appear with the following preset areas:
    - Local hard disks
    - Diskette A:
    - Disk C:
    - All Diskettes
    - CD-ROM and DVD
    - All Media
    - Memory
    - Auto-Start Programs
    - Auto-Start Programs (All Users)
    - Other
    - Interactive Selection
    - Other ..

AEA console

Client-side tasks

On-demand scanning tasks



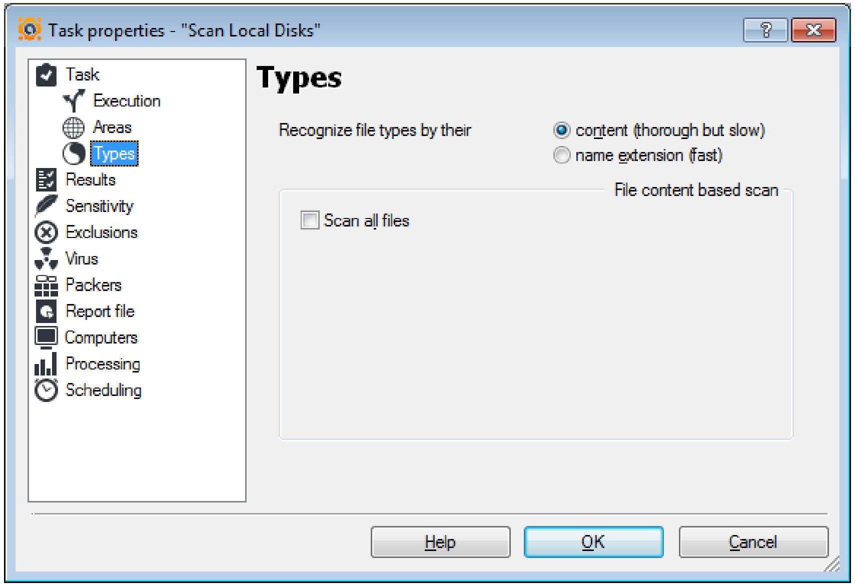
- **Auto-Start Programs** – Checks startup items for the logged user
- **Auto-Start Programs (All Users)** - Checks startup items for all created users

- **Interactive selection**
  - – allows you to select the area to test each time you run the task
- **Other**
  - – In this window, "<type area>“ should be replaced with the actual path (e.g."C:/Windows/System/file.exe").

AEA console

Client-side tasks

On-demand scanning tasks



Task properties - "Scan Local Disks"

Types

Recognize file types by their ● content (thorough but slow) ○ name extension (fast)

File content based scan

□ Scan all files

This page defines the type of files to be scanned by avast!

Recognize file types by their:

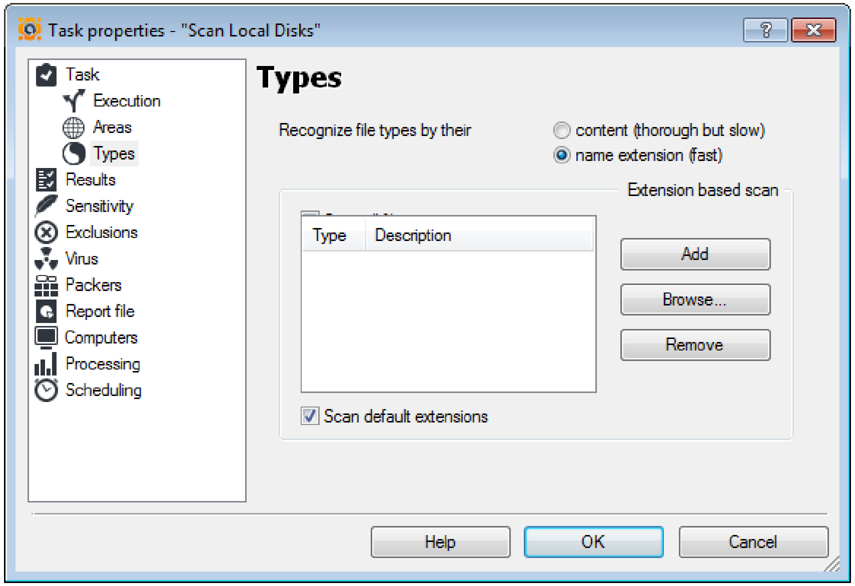
- **content**
  - File extensions will be ignored and the file types will be determined by their code (content). Because of the necessity to open each file and analyze its type, this is slower than recognizing file types by their extensions.
- **name extension**
  - The type of the file is determined by its extension. This choice speeds up the virus scanning process.

If you select the option to determine the file type by its content, you will have only one additional option - Scan all files. It means that even files which usually do not contain viruses, e.g. text files or images, will be scanned.

AEA console

Client-side tasks

On-demand scanning tasks


Task properties - "Scan Local Disks"

Types

Recognize file types by their ○ content (thorough but slow) ● name extension (fast)

Extension based scan

Type	Description

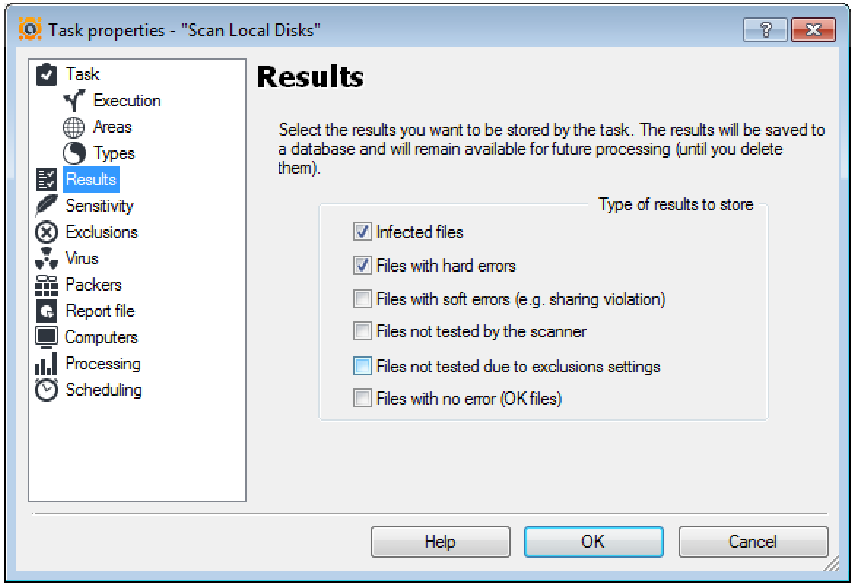
☑ Scan default extensions

- If you select the option to determine the file type by the **name extension**, you will see a list of the extensions (types) to be scanned.
- **Add**
  - Clicking this button enables you to add an extension to the list of those to be scanned. If it is a known extension, its description is shown (e.g. if you enter EXE, the description ("Application") automatically appears).
- **Browse**
  - Displays an alphabetical list of known extensions. You can select one or more of the corresponding file types (for multiple selections, use the CTRL and SHIFT keys).
- **Remove**
  - Removes the selected extension(s) from the list of the types to be scanned.
- The choice “Scan default extensions” adds all the "dangerous" extensions to the list above.

AEA console

Client-side tasks

On-demand scanning tasks



Results

Select the results you want to be stored by the task. The results will be saved to a database and will remain available for future processing (until you delete them).

Type of results to store

- ☑ Infected files
- ☑ Files with hard errors
- □ Files with soft errors (e.g. sharing violation)
- □ Files not tested by the scanner
- □ Files not tested due to exclusions settings
- □ Files with no error (OK files)

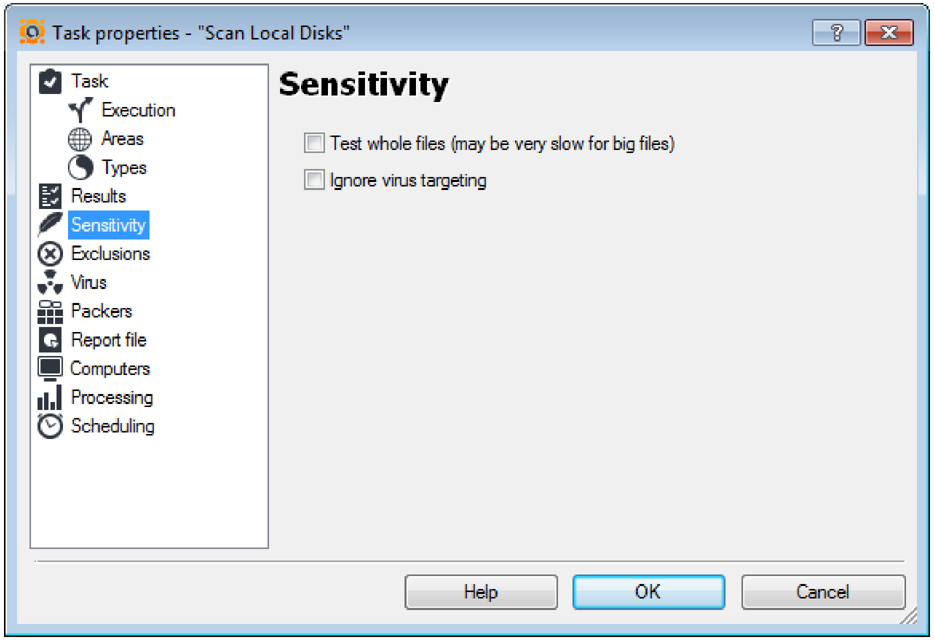
Using various checkboxes, you can select which results are displayed and stored for later usage.

- **Infected files**
  - Information about files containing virus code.
- **Files with hard errors**
  - If a serious, unexpected error occurs during the scanning of the file (e.g. the diskette containing the file to be checked is unreadable), the filename will be displayed.
- **Files with soft errors**
  - Files that were impossible to check will be displayed. It is usually because of a sharing violation (some system files) or because access to the files was denied (e.g. the current user does not have access to the folder they reside in).
- **Files not tested by the scanner**
  - Skipped files (e.g. because of their size) will be displayed. (If the file is too small to contain any virus code, it will be skipped).
- **Files not tested due to exclusion settings**
  - Files skipped because of the current exclusion settings will be displayed.
- **OK files**
  - All files correctly tested (and found uninfected) will be displayed.

AEA console

Client-side tasks

On-demand scanning tasks



Task properties - "Scan Local Disks"

Sensitivity

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

□ Ignore virus targeting

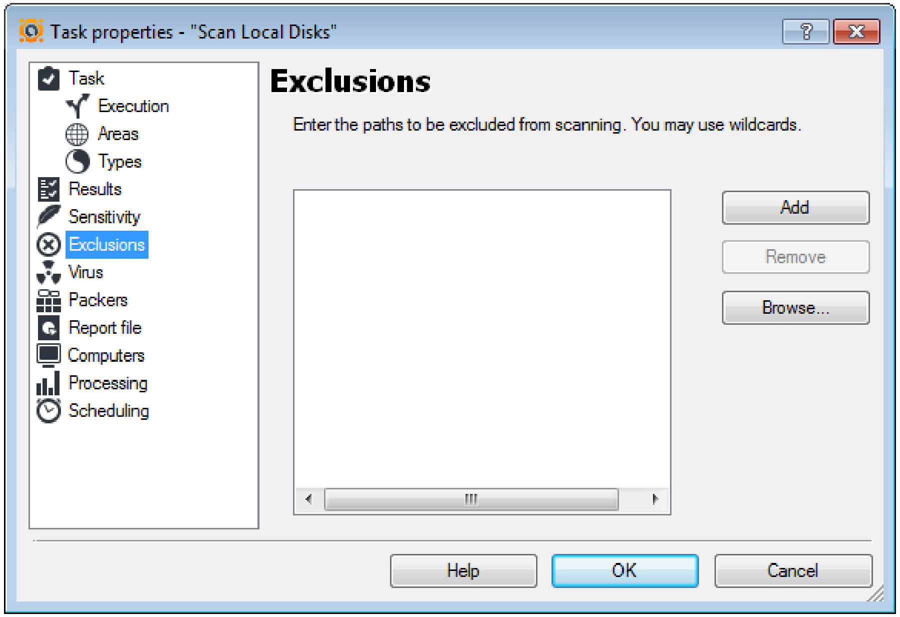
- **Test whole files**
  - Specifies whether whole files will be tested for viruses, or only the parts most frequently affected by viruses. Most viruses appear either at the start of the file, or they are appended to the end. If this option is selected avast! will test the whole file. Naturally, it will slow down the scanning a bit.

- **Ignore virus targeting**
  - If this option is selected avast will check the files against all the viruses in its database. Without this option, the files are tested only against those viruses that affect the given type of file. It means that avast! will not look for viruses only infecting EXE files in a file with a .COM extension.

AEA console

Client-side tasks

On-demand scanning tasks



Exclusions

Enter the paths to be excluded from scanning. You may use wildcards.

avast! makes it possible to exclude some areas, or even single files, from testing; it means that avast! will not search there for viruses. This can be useful in several cases:

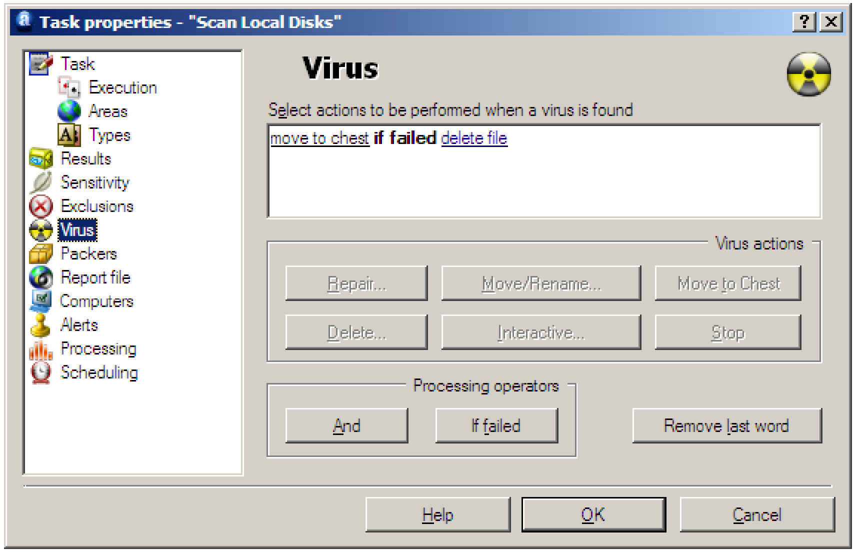
- Avoiding false alarms. If avast! reports a virus infection in a file but you are sure that it is a false alarm, you can exclude the file from testing and avoid further false alarms.
- Speeding up the processing. If you have a directory on your hard disk that contains images only, for example, you can exclude it from testing by adding it to the exclusions list, and thus reduce the time spent on scanning the files.

- **Add**
  - Adds an empty item to the list where you can then enter the folder or file to be excluded. If you want to select a folder including all its subfolders, it is necessary to append "*", e.g. "C:\Windows\*".
- **Remove**
  - Removes the selected folder or file from the exclusions list.
- **Browse**
  - An Explorer-like window will open; here you can select the desired folder or file, without having to type the whole path.

AEA console

Client-side tasks

On-demand scanning tasks



Task properties - "Scan Local Disks"

Virus

Select actions to be perfomed when a virus is found

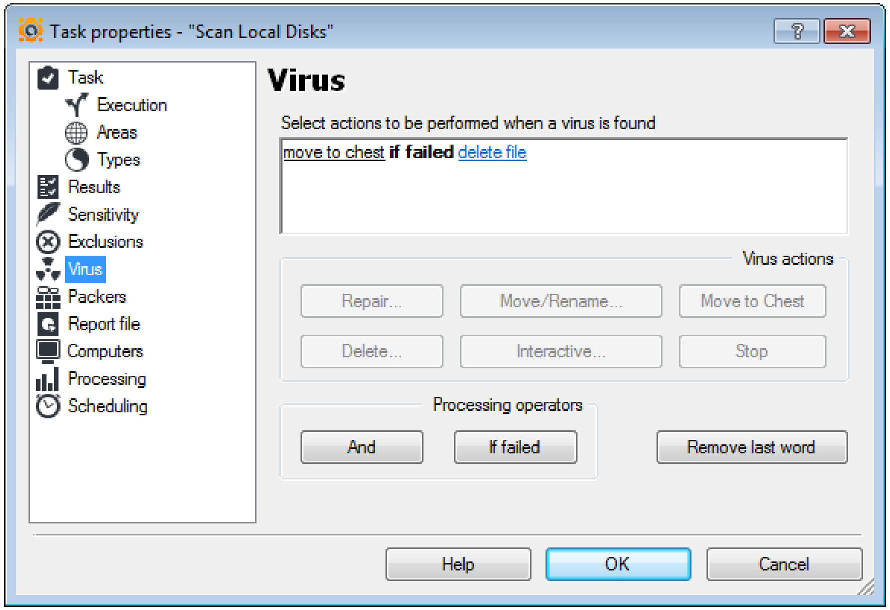
move to chest **if failed** delete file

- On this page, you can specify what actions will be taken if the task finds a virus. The default setting is “choose action”. You can define more than one action, using the operators "...and..." and "...if failed, then...".
- When using "...and...” avast will apply all the selected actions, in the given order (left to right).
- When using "...if failed, then...". avast! will try to take the first action listed; if it is successful, all the others are ignored. However, if the action failed, avast! will try to perform the next action(s).

AEA console

Client-side tasks

On-demand scanning tasks



Select actions to be performed when a virus is found

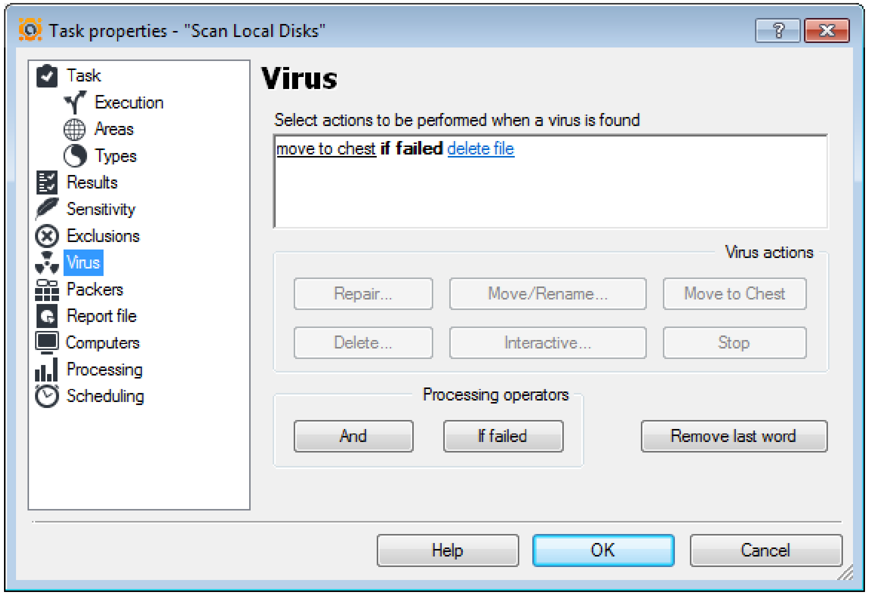
move to chest **if failed** delete file

- **Choose action**
  - When a virus is found, the task is temporarily stopped and a window appears where you can choose the action to take. To select this option, click the “Interactive” button.
- **Repair**
  - avast! will try to repair the infected file. After selecting this option, a window is displayed describing the principle for repairing files. In this window, you can choose whether all macros should be removed from Word 6 documents; macros are removed automatically from Word 6 documents if a virus, or potential virus is identified.
  - Macros will also be automatically removed from Word97, Excel95 and Excel97 documents if a virus or potential virus is detected. In the case of an infected executable file, avast! will try to remove it according to the information stored in the Virus Recovery Database. Files with no records in the Virus Recovery Database cannot be repaired! In the case of a boot virus, avast! will overwrite the diskette boot sector, thus eliminating the virus.

AEA console

Client-side tasks

On-demand scanning tasks



Task properties - "Scan Local Disks"

Virus

Select actions to be performed when a virus is found

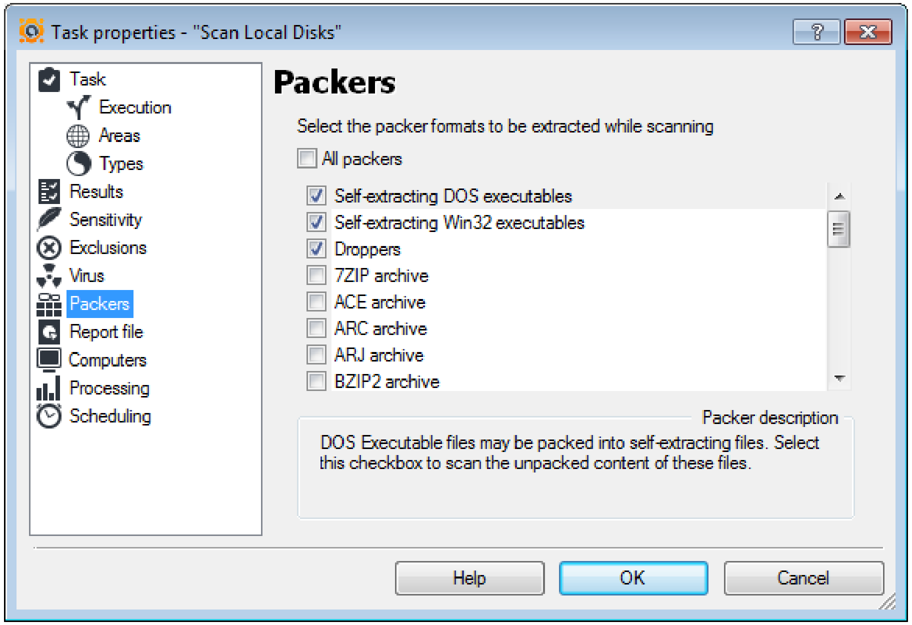
move to chest **if failed** delete file

- **Move/Rename**
  - Moves or renames an infected file. You can specify the folder to move the file to.
- **Move to Chest**
  - An infected file will be moved to the virus Chest.
- **Delete**
  - Deletes the infected file. Additional options can be selected. The default setting is delete file(s) permanently, which means the file will be completely removed from your computer (hard disk, diskette, ...) For this option, you can further specify that the file will be deleted upon OS restart if it is currently locked.
  - This is a very useful setting, as it is impossible to immediately delete the file of a virus that is currently running. So, avast! will "remember" which file the virus is in and delete it as soon as possible, which is normally at the next operating system start (i.e. before the virus is activated again). The option delete file(s) to the recycle bin ensures that the file will not be physically removed, but only moved to the recycle bin.
- **Stop**
  - When the first virus is detected, the task is stopped; no action will be taken with the virus.

AEA console

Client-side tasks

On-demand scanning tasks



Packers

Select the packer formats to be extracted while scanning

□ All packers

☑ Self-extracting DOS executables
☑ Self-extracting Win32 executables
☑ Droppers
□ 7ZIP archive
□ ACE archive
□ ARC archive
□ ARJ archive
□ BZIP2 archive

Packer description

DOS Executable files may be packed into self-extracting files. Select this checkbox to scan the unpacked content of these files.

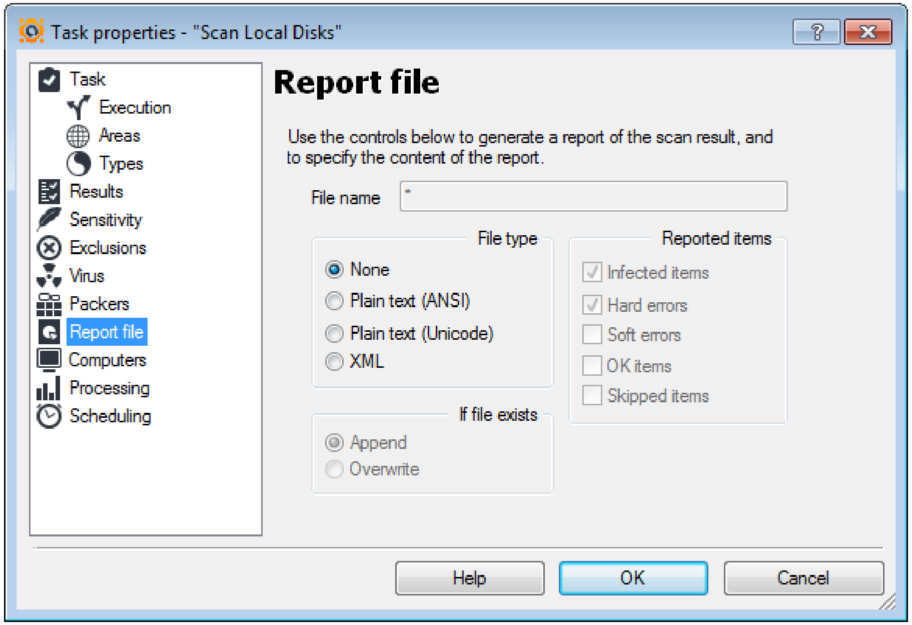
- This page allows you to select which packers (archives) avast! will test during the task processing. The default setting is self-extracting executables only. You can set additional archives to be processed, though it will slow down the test, of course. If “All packers” is checked, avast! will scan all archives that it is able to process.

- avast! is able to process the following archives:

- Self-extracting DOS executables
- Self-extracting Win32 executables (UPX, ASPack, PECompact, ...)
- 7ZIP archive
- ACE archive
- ARC archive
- ARJ archive
- BZIP2 archive
- CAB archive
- CHM archive
- CPIO archive
- DBX archive
- GZIP archive
- Installer archives (Wise, ...)
- ISO archive
- LHA archive
- MAPI files (*.pst)
- MIME
- NTFS streams
- OLE archive (DOC, XLS, MSI, ...)
- RAR archive
- RPM archive
- SIS archive
- TAR archive
- TNEF streams
- ZIP archive
- ZOO archive

AEA console

Client-side tasks



Report file

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name: *

File type

- ● None
- ○ Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

Reported items

- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

If file exists

- ● Append
- ○ Overwrite

On-demand scanning tasks

- avast! can create and save a report file containing information about a past scan. It contains the same information as in the scan results.

- **Report File Folder**
  - Enter the path and name of the report file, e.g. C:\Reports\task_name.rpt. The folder can be selected by clicking the Browse button. The default report file name is the name of the corresponding task.

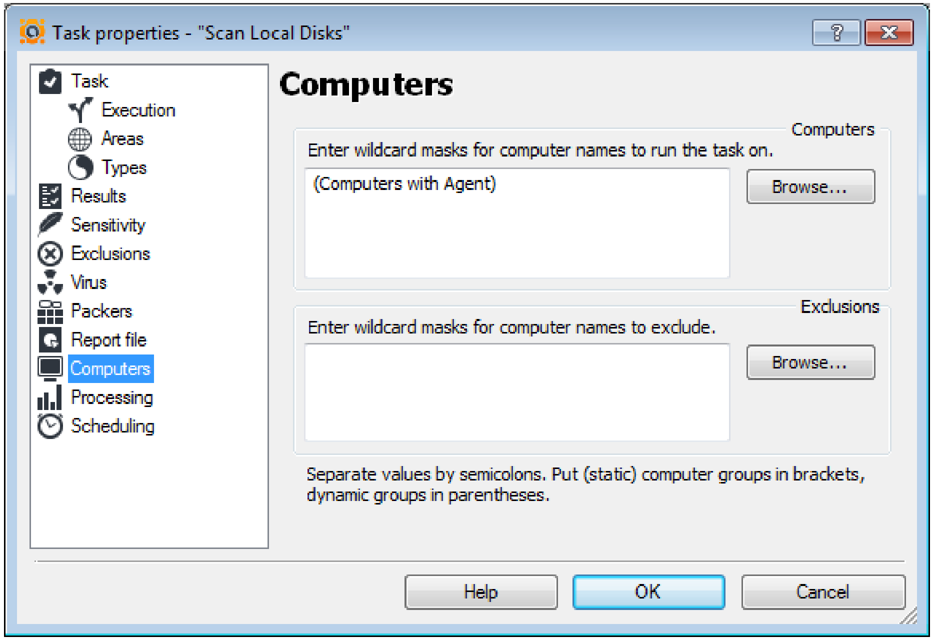
- **Log Record For**
  - Check the items that should be written to the report. **Task start** writes the task start date and time to the report; similarly, task stop writes the task end date and time. The remaining items - **hard errors**, **soft errors**, **skipped files**, **infected files**, and **OK files** are described on the results page.

- **Type of file**
  - Select the format of the report file. You can choose either a simple text file, or the newer XML format.

AEA console

Client-side tasks

On-demand scanning tasks



Computers

Computers

Enter wildcard masks for computer names to run the task on.

(Computers with Agent)

Exclusions

Enter wildcard masks for computer names to exclude.

Separate values by semicolons. Put (static) computer groups in brackets, dynamic groups in parentheses.

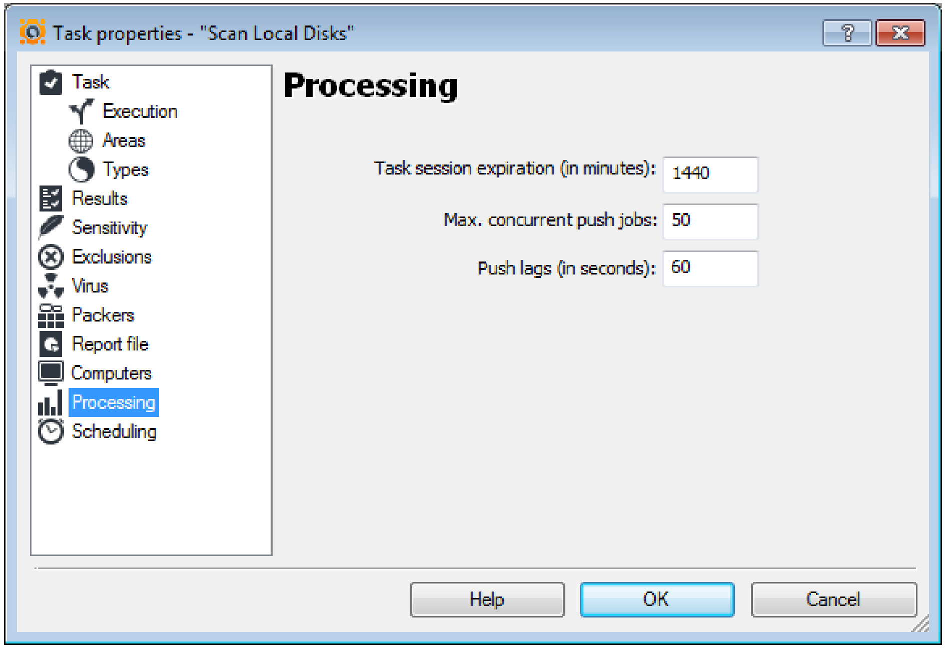
- On this screen you can specify the computers on which the task should be run, or which should be excluded.

- You can also specify computers in groups.
  - Static groups should be enclosed in square brackets
    - e.g., [MyGroupName].
  - Dynamic groups should be enclosed in regular brackets
    - e.g., (Computers with Agent)
    - e.g., (Computers without Agent)

AEA console

Client-side tasks

On-demand scanning tasks



Task properties - "Scan Local Disks"

Processing

Task session expiration (in minutes): 1440

Max. concurrent push jobs: 50

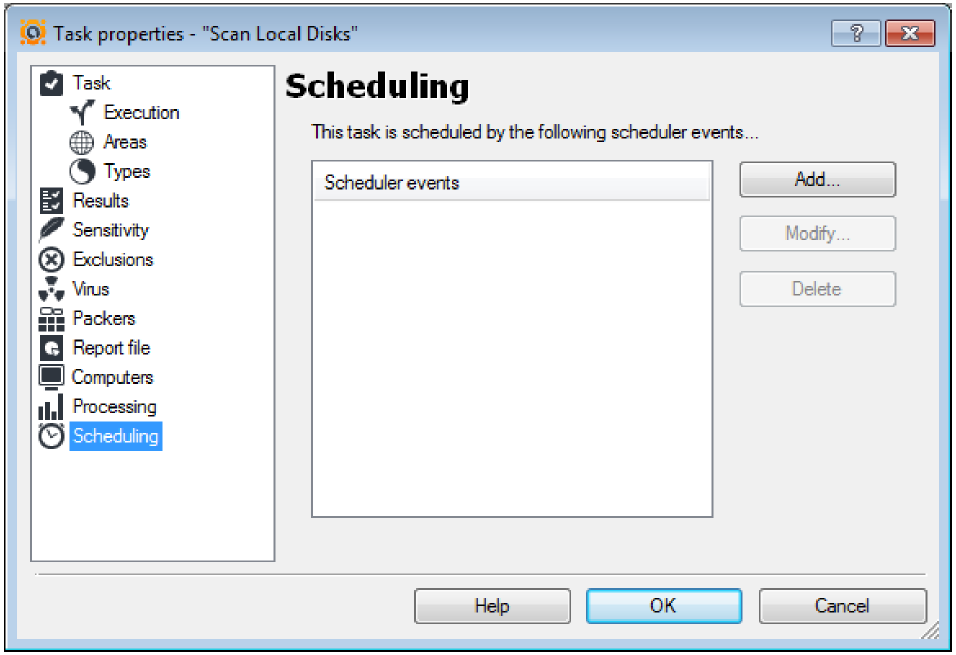
Push lags (in seconds): 60

- Task session expiration
  - The maximum period of time for which AEA will run a specific session (the time from when the task started). When the time limit is reached, the session will be terminated.
  - The default time limit is 1440 minutes
- Max.concurrent push jobs
  - The maximum number of threads which the server creates to contact/establish a connection with computers on the network on which the task should be run.
  - The default maximum number of concurrent jobs is 50
- Push lags
  - The time lag between push jobs to prevent network overload.
  - The default is 60 seconds

AEA console

Client-side tasks

On-demand scanning tasks



Task properties - "Scan Local Disks"

Scheduling

This task is scheduled by the following scheduler events...

Scheduler events

- avast! makes it possible to schedule tasks to start automatically at a given time and on a given date.

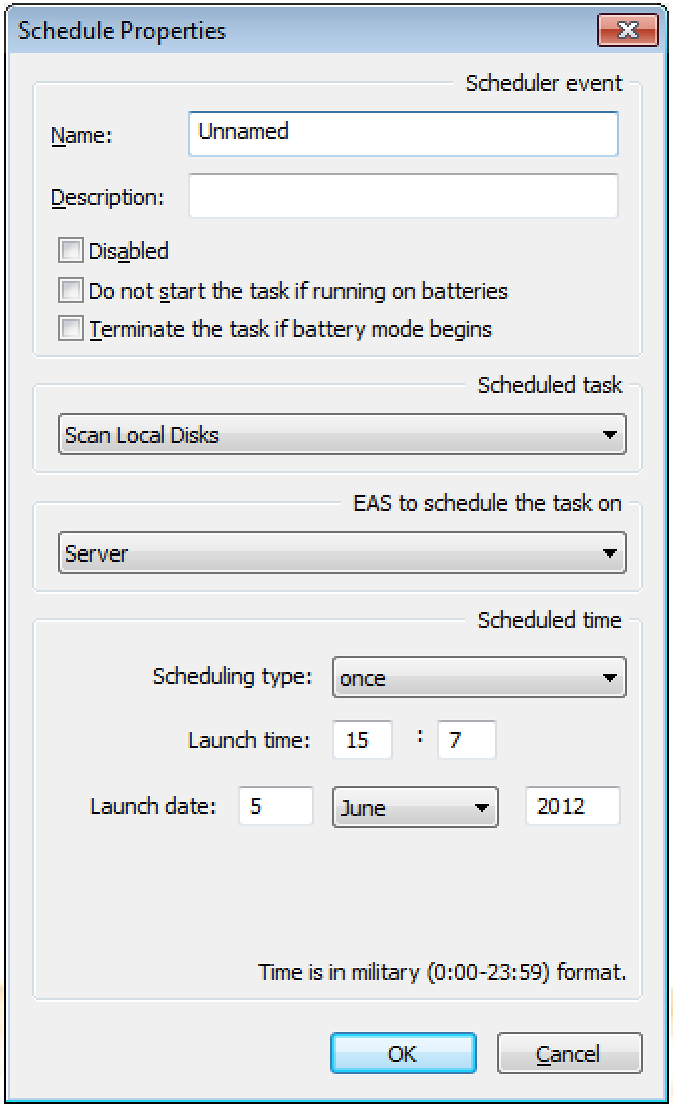
- **Add**
  - Adds a new scheduler event, i.e. it schedules a task startup.
- **Modify**
  - Modifies the selected scheduled event.
- **Delete**
  - Deletes the selected event.

- If you want specify a date/time for a task to be started, select Add. A new window will appear ->

AEA console

Client-side tasks

On-demand scanning tasks



Schedule Properties

Scheduler event

Name: Unnamed

Description:

□ Disabled

□ Do not start the task if running on batteries

□ Terminate the task if battery mode begins

Scheduled task

Scan Local Disks

EAS to schedule the task on

Server

Scheduled time

Scheduling type: once

Launch time: 15 : 7

Launch date: 5 June 2012

Time is in military (0:00-23:59) format.

-> here you should enter the parameters defining the new task

- **Name**
  - Name of the task, e.g. "Weekend scan".
- **Description**
  - Enter a brief description of the task e.g. "Scans all the hard disks every Sunday night".
- **Disabled**
  - This option disables the scheduled task. It is useful when you need to stop the task from running, but you do not want to delete the task completely and have to re-enter it again later.
- **Do not start the task if running on batteries**
  - Useful mainly for notebook owners. The task will not be started if the computer is running on batteries.
- **Terminate the task if battery mode begins**
  - If, while a scheduled task is running, the computer is cut off from the electric power supply and switches to batteries, the task will be terminated. Again, this is useful mainly for notebook owners.
- **Scheduled task**
  - Select the task to be scheduled.
- **Scheduling type**
  - Here you can specify when the task will be started.
    - Once - you simply enter the time and date when the task should be run
    - Daily – enter the time only - the task will be started each day at the given time.
    - Weekly (or monthly)
- **Launch time/launch date**
  - Here you can set the time and the actual day of the week (month) when the scheduled task should be run.

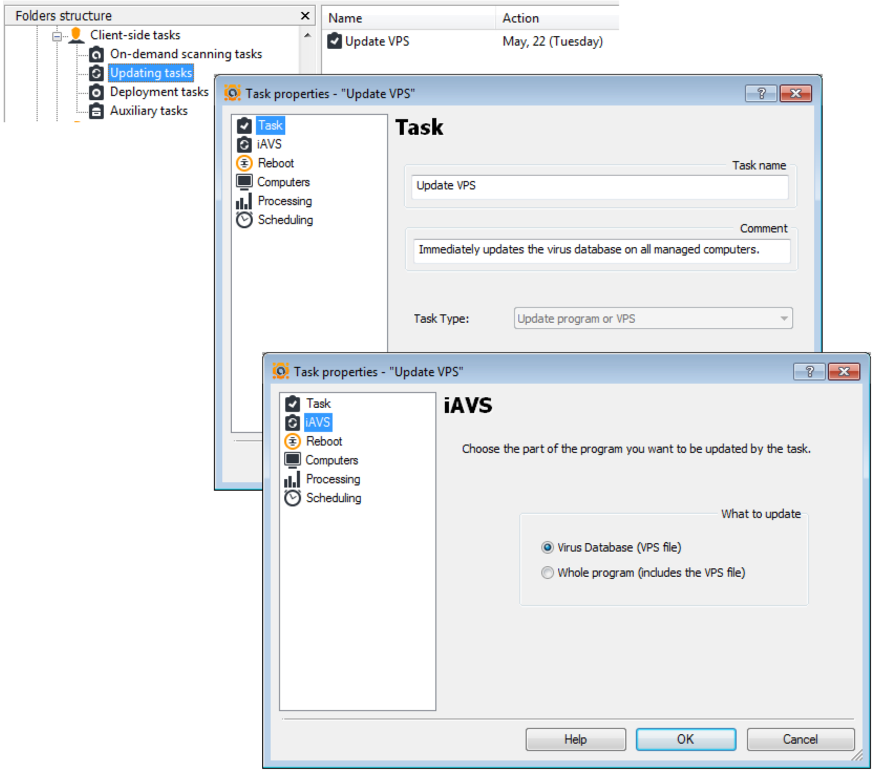
AEA Client-side tasks

UPDATING TASK

AEA console

Client-side tasks

Updating task



Name	Action
Update VPS	May, 22 (Tuesday)

Task properties - "Update VPS"

Task

Task name: Update VPS

Comment: Immediately updates the virus database on all managed computers.

Task Type: Update program or VPS

Task properties - "Update VPS"

iAVS

Choose the part of the program you want to be updated by the task.

What to update

● Virus Database (VPS file)

○ Whole program (includes the VPS file)

- To ensure the maximum possible virus protection, it is necessary to have the most up-to-date virus database (VPS file) and the latest program version.

- The AEA system offers very flexible options for update management, for distributing both virus database and full (program) updates.

- AEA uses “updating mirrors” to provide efficient updating mechanisms to all machines on the network (even those not directly connected to the Internet).

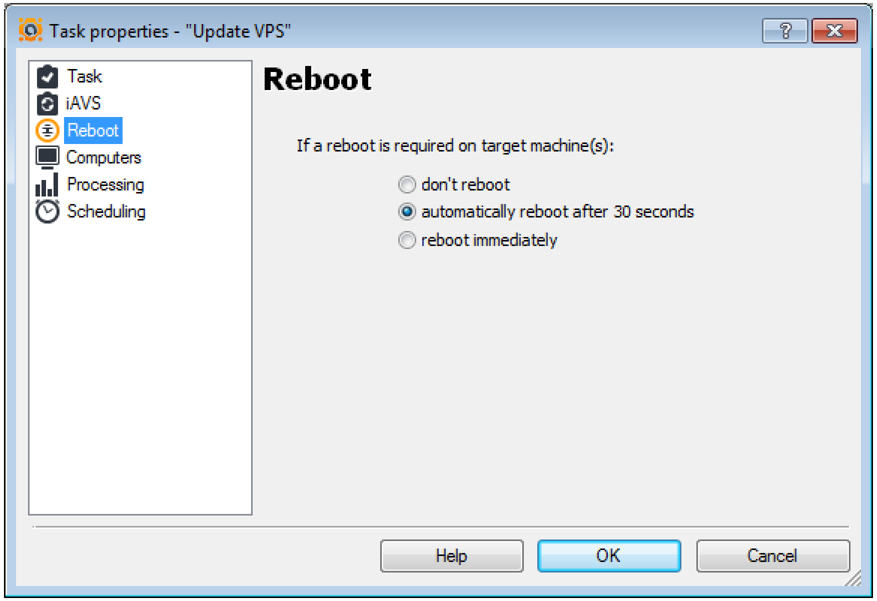
- Mirrors also save greatly on bandwidth requirements, because instead of downloading the updates to each and every machine on the network, AEA downloads the updates only to the mirrors and then distributes the updates locally.

- By default, there is a mirror on the EAS itself, and it is the only mirror on the network. If using multiple EAS’s, there’s a mirror on each EAS by default, and these are the only mirrors on the network. All managed machines download updates from the EAS mirror on the EAS, if a connection to the EAS is available.

AEA console

Client-side tasks

Updating task



Task properties - "Update VPS"

Reboot

If a reboot is required on target machine(s):

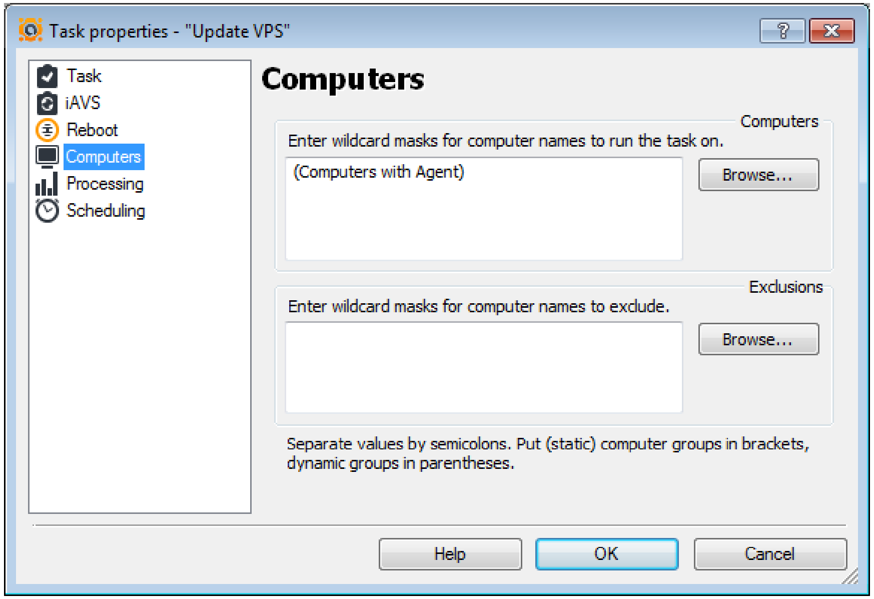
○ don't reboot
● automatically reboot after 30 seconds
○ reboot immediately

- On this screen you can select whether and when the system is restarted, where a re-boot is required to complete the update.
  - Don‘t reboot
  - Automatically reboot after 30 seconds
  - Reboot immediately

AEA console

Client-side tasks

Updating task



Task properties - "Update VPS"

Computers

Computers

Enter wildcard masks for computer names to run the task on.

(Computers with Agent)

Exclusions

Enter wildcard masks for computer names to exclude.

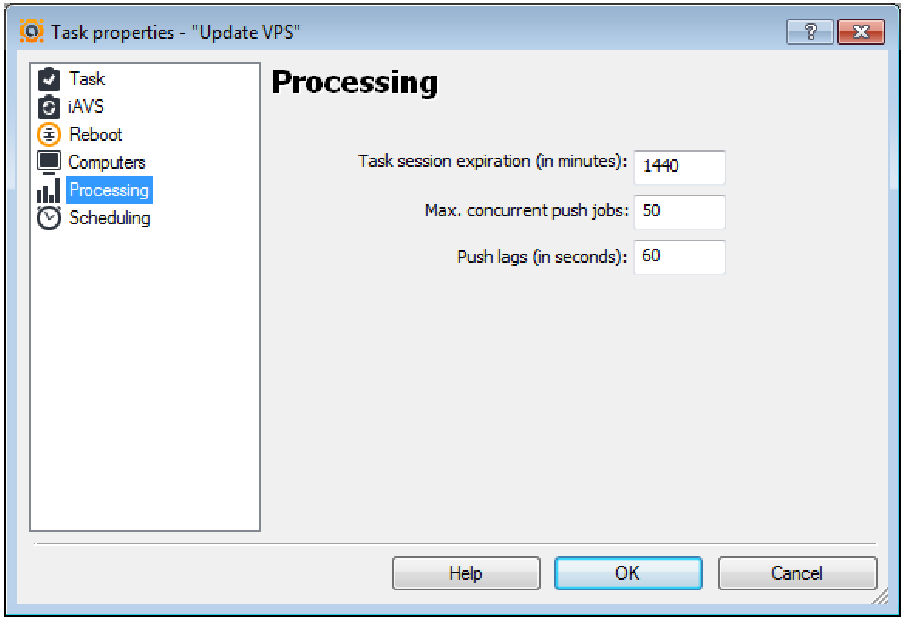
Separate values by semicolons. Put (static) computer groups in brackets, dynamic groups in parentheses.

- On this screen you can specify the computers on which the task should be run, or which should be excluded.
- You can also specify computers in groups.
  - Static groups should be enclosed in square brackets
    - e.g., [MyGroupName].
  - Dynamic groups should be enclosed in regular brackets
    - e.g., (Computers with Agent)
    - e.g., (Computers without Agent)

AEA console

Client-side tasks

Updating task



Task properties - "Update VPS"

Processing

Task session expiration (in minutes): 1440

Max. concurrent push jobs: 50

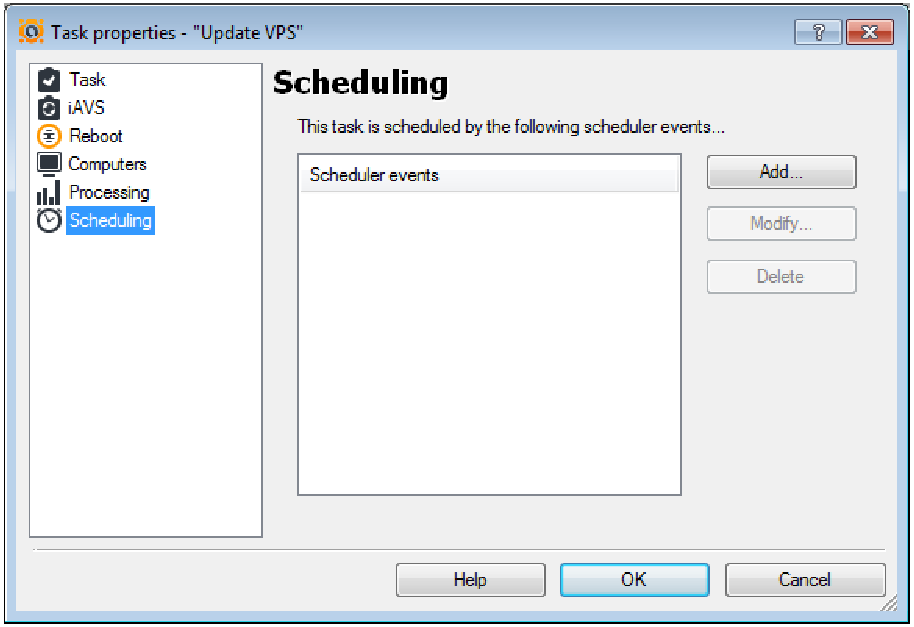
Push lags (in seconds): 60

- Task session expiration
  - The maximum period of time for which AEA will run a specific session (the time from when the task started). When the time limit is reached, the session will be terminated.
  - The default time limit is 1440 minutes
- Max.concurrent push jobs
  - The maximum number of threads which the server creates to contact/establish a connection with computers on the network on which the task should be run.
  - The default maximum number of concurrent jobs is 50
- Push lags
  - The time lag between push jobs to prevent network overload.
  - The default is 60 seconds

AEA console

Client-side tasks

Updating task



Task properties - "Update VPS"

Scheduling

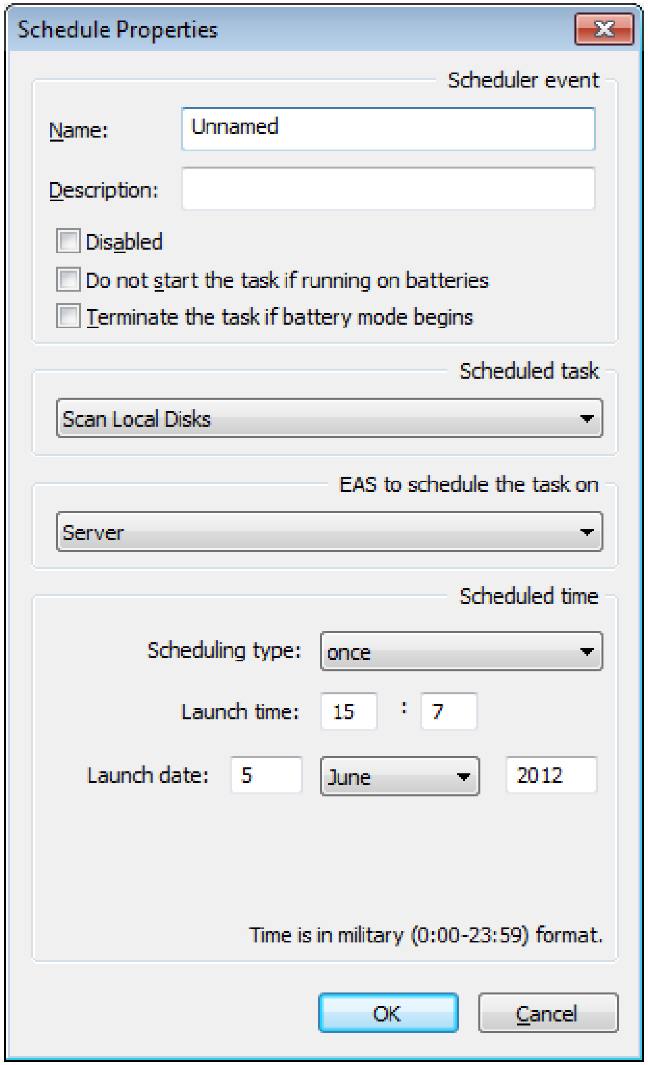
This task is scheduled by the following scheduler events...

Scheduler events

- avast! makes it possible to schedule tasks to start automatically at a given time and on a given date.
- **Add**
  - Adds a new scheduled task, i.e. it schedules when a task will be run.
- **Modify**
  - Modifies the selected scheduled task.
- **Delete**
  - Deletes the selected task.
- If you want a task to be started at a certain time on a given date, select Add. A new window will appear **->**

AEA console

Client-side tasks



Schedule Properties

Scheduler event

Name: Unnamed

Description:

□ Disabled

□ Do not start the task if running on batteries

□ Terminate the task if battery mode begins

Scheduled task

Scan Local Disks

EAS to schedule the task on

Server

Scheduled time

Scheduling type: once

Launch time: 15 : 7

Launch date: 5 June 2012

Time is in military (0:00-23:59) format.

Updating task

-> here you should enter the parameters defining the new task

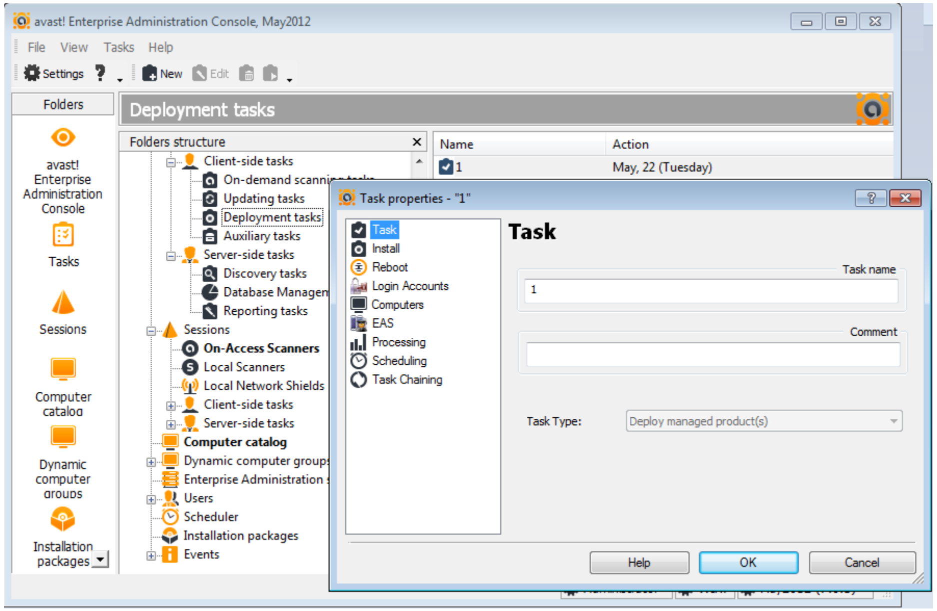
- **Name**
  - Name of the task, e.g. "Weekend scan".
- **Description**
  - Enter a brief description of the task e.g. "Scans all the hard disks every Sunday night".
- **Disabled**
  - This option disables the scheduled task. It is useful when you need to stop the task from running, but you do not want to delete the task completely and have to re-enter it again later.
- **Do not start the task if running on batteries**
  - Useful mainly for notebook owners. The task will not be started if the computer is running on batteries.
- **Terminate the task if battery mode begins**
  - If, while a scheduled task is running, the computer is cut off from the electric power supply and switches to batteries, the task will be terminated. Again, this is useful mainly for notebook owners.
- **Scheduled task**
  - Select the task to be scheduled.
- **Scheduling type**
  - Here you can specify when the task will be started.
    - Once - you simply enter the time and date when the task should be run.
    - Daily - enter the time only - the task will be started each day at the given time.
    - Weekly (or monthly)
- **Launch time/launch date**
  - Here you can set the time and the actual day of the week (month) when the scheduled task should be run.

AEA Client-side tasks

DEPLOYMENT TASK

AEA console

Client-side tasks



Name: 1 — Action: May, 22 (Tuesday)

Task name: 1

Comment:

Task Type: Deploy managed product(s)

Deployment task

- After the installation package is created, you need to create a deployment task and bind the installation package to it.

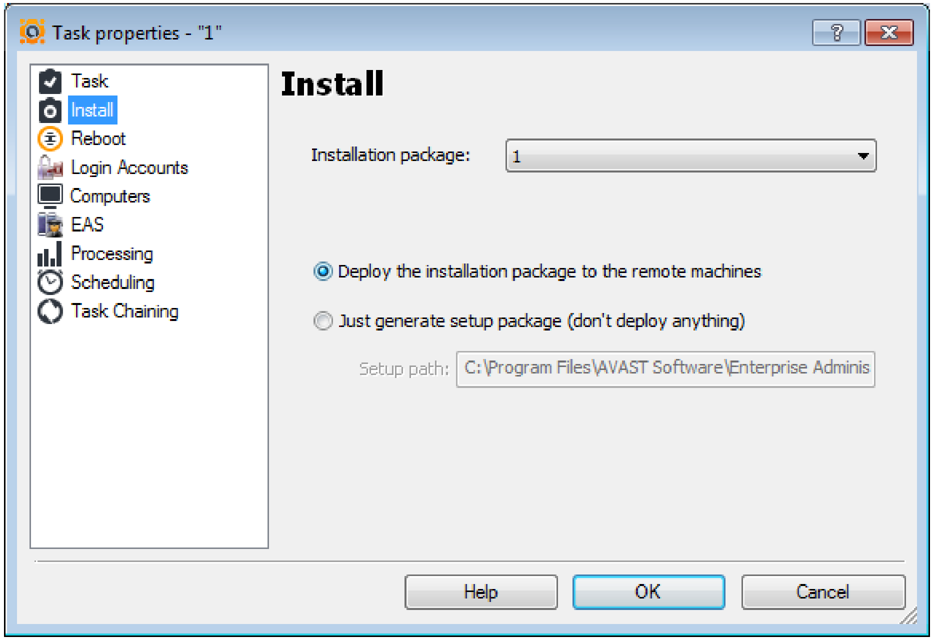
- Make sure to correctly specify valid credentials for all domains/workgroups to ensure the software can be installed on all machines on the network.

- Also make sure that the **Discovery task** to build the **Computer catalog** was successfully created.

- Another source from where you can get a list of client computers on the network is **Dynamic computer group.**

AEA console

Client-side tasks



Task properties - "1"

Install

Installation package: 1

● Deploy the installation package to the remote machines

○ Just generate setup package (don't deploy anything)

Setup path: C:\Program Files\AVAST Software\Enterprise Adminis

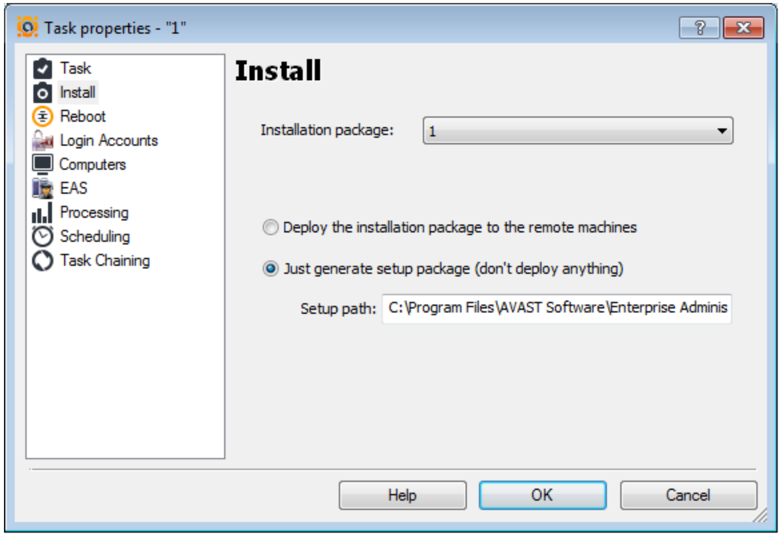
Deployment task

- There are five ways of deploying the avast! product line on the network:
  - By using the AEA Deployment task to push the installation to the clients automatically. Please note that this only works for Windows 2003/2008/XP/Vista/7 machines.
  - By using a log-on script or an alternative approach to execute the (unattended) installation on the target machines.
  - By using setup packages.
  - By disk imaging (cloning) methods.
  - By manually executing the installation program on the target machines and completing the setup wizard.

AEA console

Client-side tasks

Deployment task



Task properties - "1"

Install

Installation package: 1

○ Deploy the installation package to the remote machines

● Just generate setup package (don't deploy anything)

Setup path: C:\Program Files\AVAST Software\Enterprise Adminis

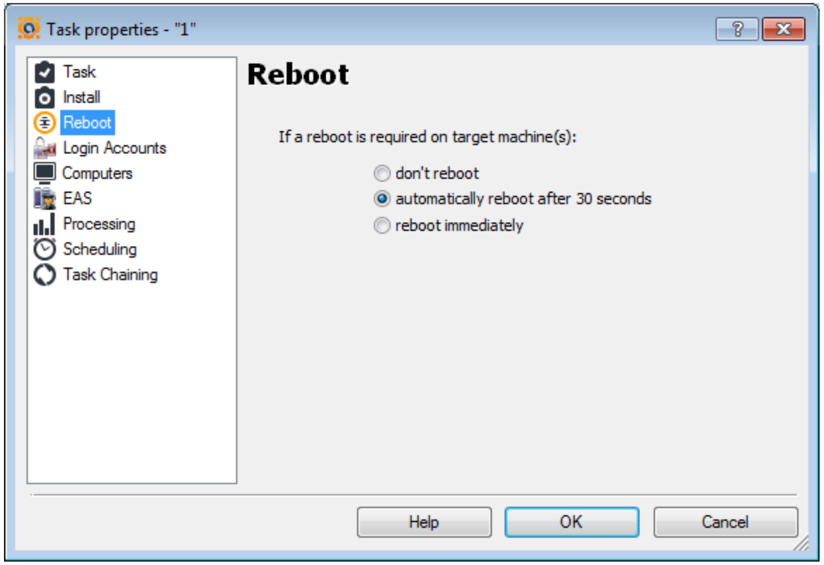
- If you choose to deploy avast! using “setup packages“, you first need to create the package. This is done by creating a deployment task, but choosing the “Just generate setup package..“ option.
- In this mode, the computers specified on the Computers page are ignored, as no deployment is taking place.

- Running the task will create a self-extracting *.exe file only.
  - The default setup package file location is C:\Program Files\AVAST Software\Enterprise Administration\Deploy\Unnamed.exe
  - **Note: if a file name is not specified for the setup package, the installation package will not be created!**

AEA console

Client-side tasks

Deployment task



Task properties - "1"

- Task
- Install
- Reboot
- Login Accounts
- Computers
- EAS
- Processing
- Scheduling
- Task Chaining

Reboot

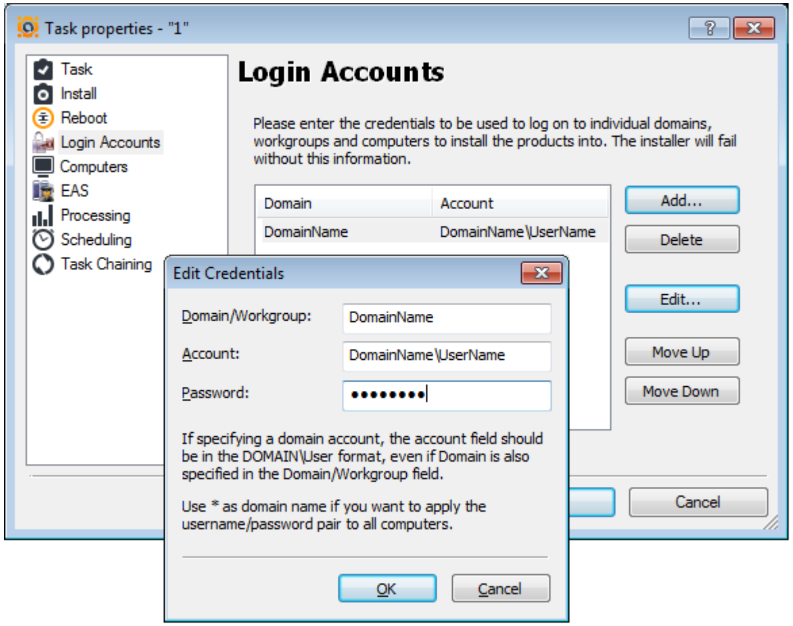
If a reboot is required on target machine(s):

○ don't reboot
● automatically reboot after 30 seconds
○ reboot immediately

- On this page you can customize whether and when a client computer is restarted, where this is required to complete the update.
  - Don‘t reboot
  - Automatically reboot after 30 seconds
  - Reboot immediately

AEA console

Client-side tasks



Task properties - "1"

Login Accounts

Please enter the credentials to be used to log on to individual domains, workgroups and computers to install the products into. The installer will fail without this information.

Domain	Account
DomainName	DomainName\UserName

Edit Credentials

Domain/Workgroup: DomainName

Account: DomainName\UserName

Password: ••••••••

If specifying a domain account, the account field should be in the DOMAIN\User format, even if Domain is also specified in the Domain/Workgroup field.

Use * as domain name if you want to apply the username/password pair to all computers.

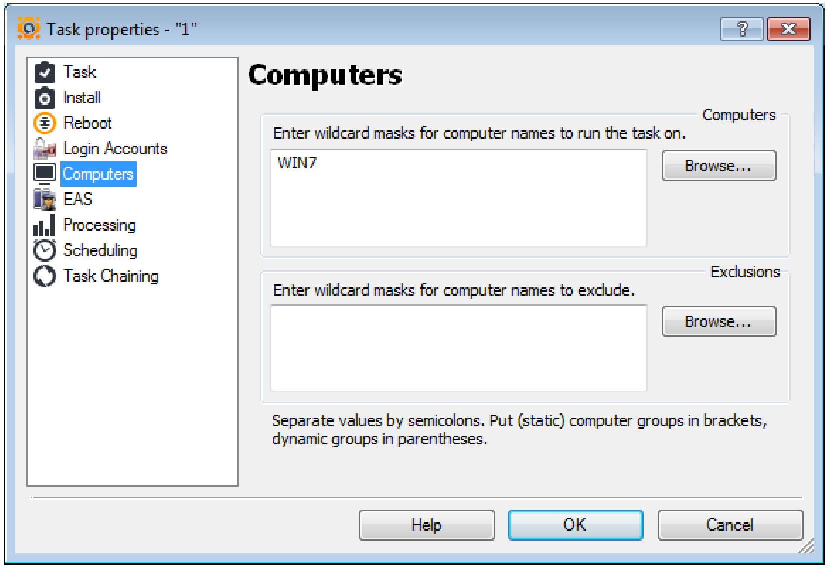
Deployment task

- Here, you should specify all domain/username/password assignments that will be used when logging on to the remote machines and pushing the packages.
- If the machines are not part of a domain, use the domain field to specify the workgroup name.
- **Note:**
  - When specifying the domain account use the format: DomainName\AdministratorAccount
  - If you are not sure about the Domain or Workgroup, or the deployment does not work, you can use the wildcard domain name *

AEA console

Client-side tasks

Deployment task



Computers

Computers

Enter wildcard masks for computer names to run the task on.

WIN7

Exclusions

Enter wildcard masks for computer names to exclude.

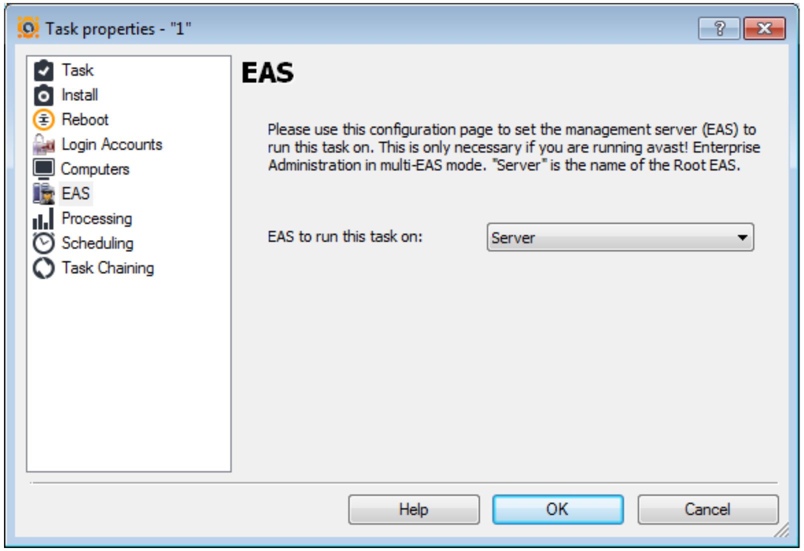
Separate values by semicolons. Put (static) computer groups in brackets, dynamic groups in parentheses.

- On this page you can specify the computers on which this task should be run, or which should be excluded.
- You can also specify computers in groups.
  - Static groups should be closed in square brackets
    - e.g., [MyGroupName].
  - Dynamic groups should be enclosed in regular brackets
    - e.g., (Computers with Agent)
    - e.g., (Computers without Agent)

AEA console

Client-side tasks

Deployment task



EAS

Please use this configuration page to set the management server (EAS) to run this task on. This is only necessary if you are running avast! Enterprise Administration in multi-EAS mode. "Server" is the name of the Root EAS.

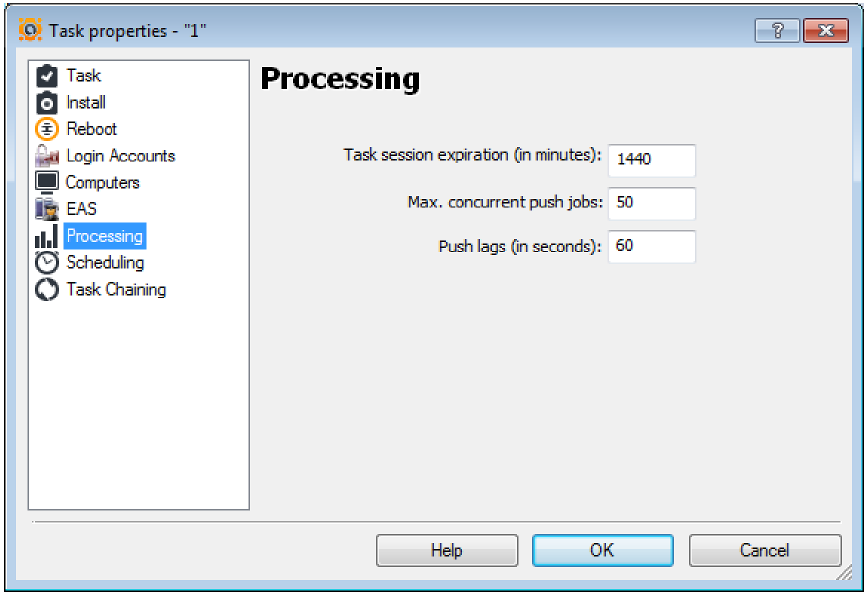
EAS to run this task on: Server

- The following configuration page can be used to select the Enterprise server (EAS) to run this task on. This is only necessary if you are running AEA in multi EAS mode.
- The server is the name of the Root EAS

AEA console

Client-side tasks

Deployment task


Task properties - "1"

Processing

Task session expiration (in minutes): 1440

Max. concurrent push jobs: 50

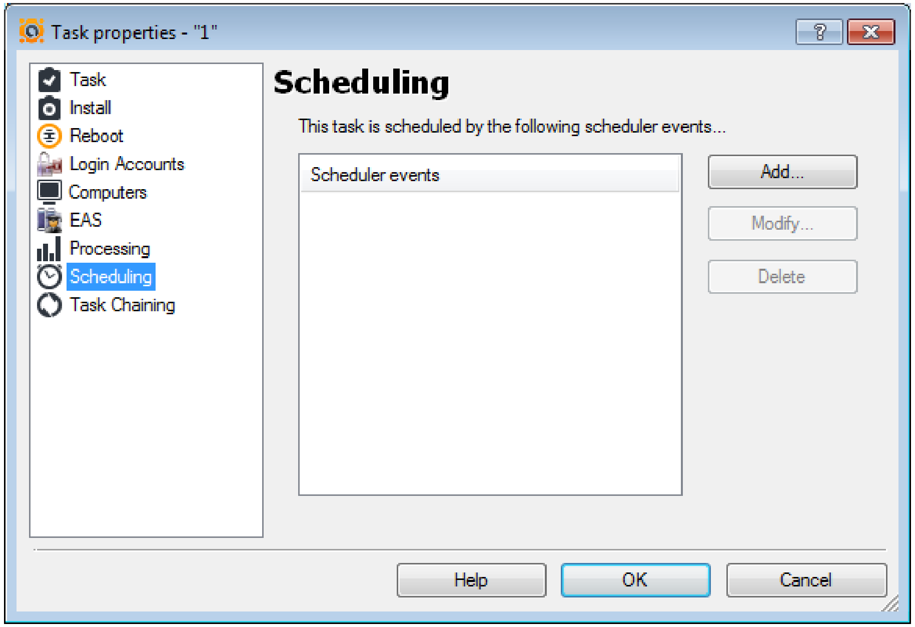
Push lags (in seconds): 60

- Task session expiration
  - The maximum period of time for which AEA will run a specific session (the time from when the task started). When the time limit is reached, the session will be terminated.
  - The default time limit is 1440 minutes
- Max.concurrent push jobs
  - The maximum number of threads which the server creates to contact/establish a connection with computers on the network on which the task should be run.
  - The default maximum number of concurrent jobs is 50
- Push lags
  - The time lag between push jobs to prevent network overload.
  - The default is 60 seconds

AEA console

Client-side tasks

Deployment task



Task properties - "1"

Scheduling

This task is scheduled by the following scheduler events...

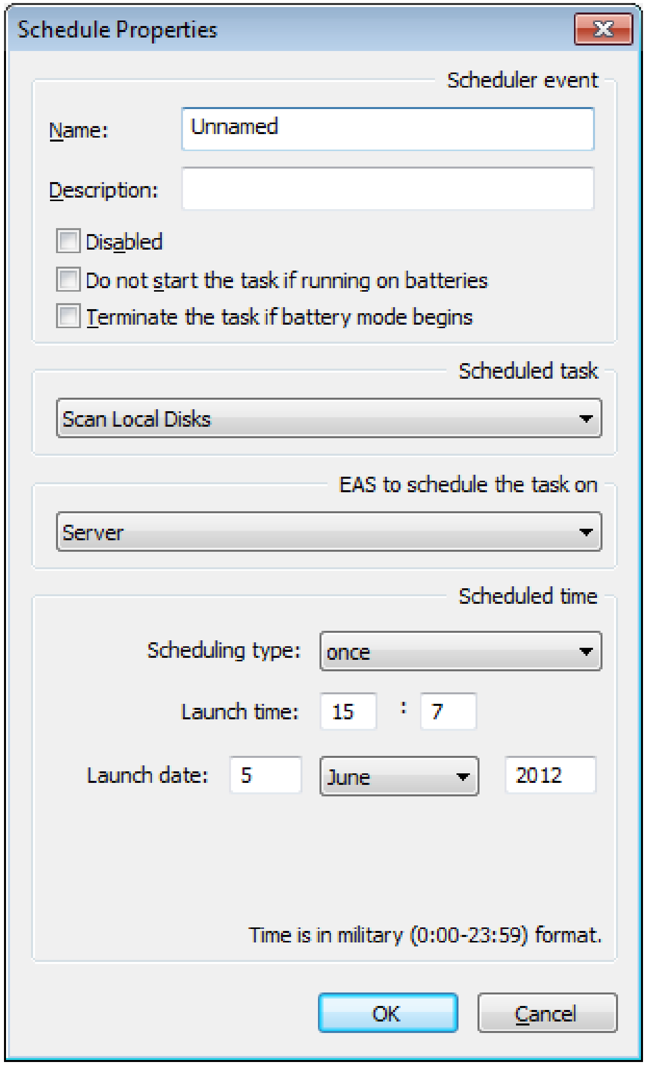
- avast! makes it possible to schedule a task to start automatically on a given date and at a given time.

- **Add**
  - Adds a new scheduled task, i.e. it schedules a task to start automatically.
- **Modify**
  - Modifies the selected scheduled task.
- **Delete**
  - Deletes the selected task.

- If you want a task to be started on a given date and at a given time, select Add. A new window will appear **->**

AEA console

Client-side tasks Deployment task



Schedule Properties

Scheduler event

Name: Unnamed

Description:

□ Disabled

□ Do not start the task if running on batteries

□ Terminate the task if battery mode begins

Scheduled task

Scan Local Disks

EAS to schedule the task on

Server

Scheduled time

Scheduling type: once

Launch time: 15 : 7

Launch date: 5 June 2012

Time is in military (0:00-23:59) format.

-> here you should enter the parameters defining the new task

- **Name**
  - Name of the task, e.g. "Weekend scan".
- **Description**
  - Enter a brief description of the task e.g. "Scans all the hard disks every Sunday night".
- **Disabled**
  - This option disables the scheduled task. It is useful when you need to stop the task from running, but you do not want to delete the task completely and have to re-enter it again later.
- **Do not start the task if running on batteries**
  - Useful mainly for notebook owners. The task will not be started if the computer is running on batteries.
- **Terminate the task if battery mode begins**
  - If, while a scheduled task is running, the computer is cut off from the electric power supply and switches to batteries, the task will be terminated. Again, this is useful mainly for notebook owners.
- **Scheduled task**
  - Select the task to be scheduled.
- **Scheduling type**
  - Here you can specify when the task will be started.
    - Once - you simply enter the time and date when the task should be run.
    - Daily - enter the time only - the task will be started each day at the given time.
    - Weekly (or monthly)
- **Launch time/launch date**
  - Here you can set the time and the actual day of the week (month) when the scheduled task should be run.

AEA console

Client-side tasks

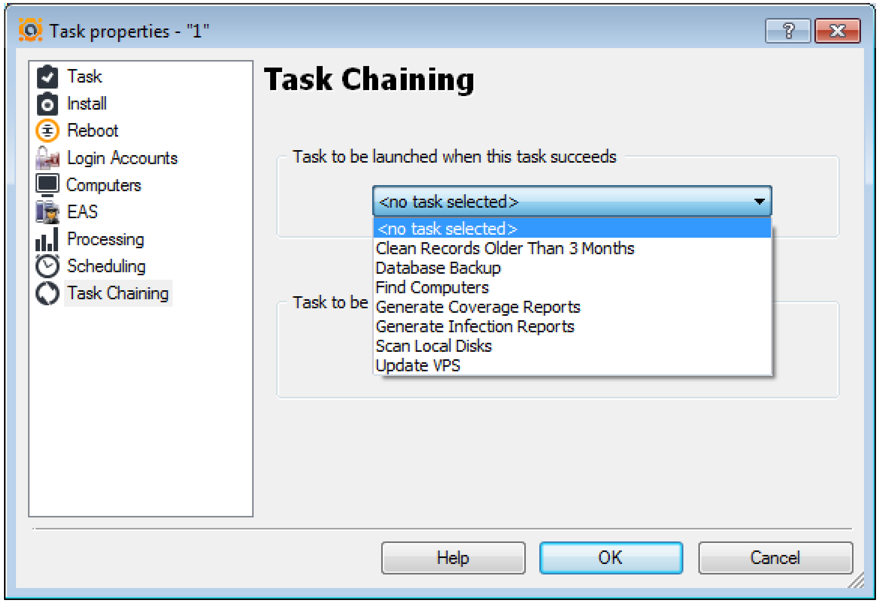
Deployment task

Here you can choose the task which will be launched if the deployment task is successful.

The list of the tasks is displayed below:

Here you can choose the task which will be launched if the deployment task fails.

The list of the tasks is displayed below:



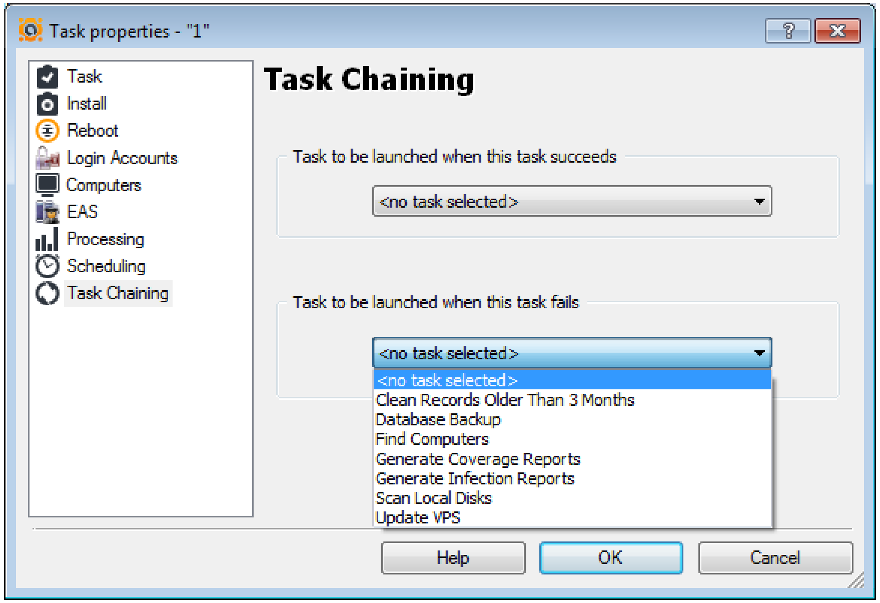
Task properties - "1"

Task Chaining

Task to be launched when this task succeeds

<no task selected>

Task to be



Task properties - "1"

Task Chaining

Task to be launched when this task succeeds

<no task selected>

Task to be launched when this task fails

<no task selected>

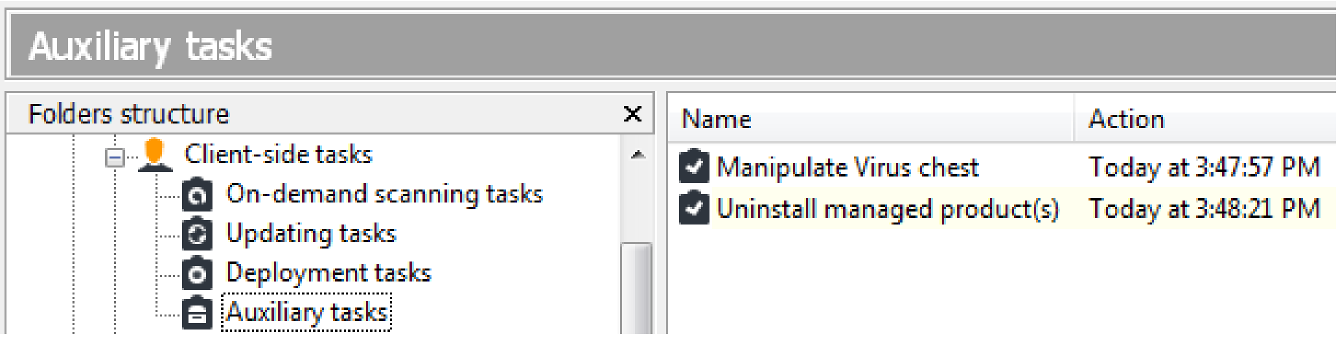
AEA Client-side tasks

AUXILIARY TASKS

AEA console

Client-side tasks

Auxiliary task



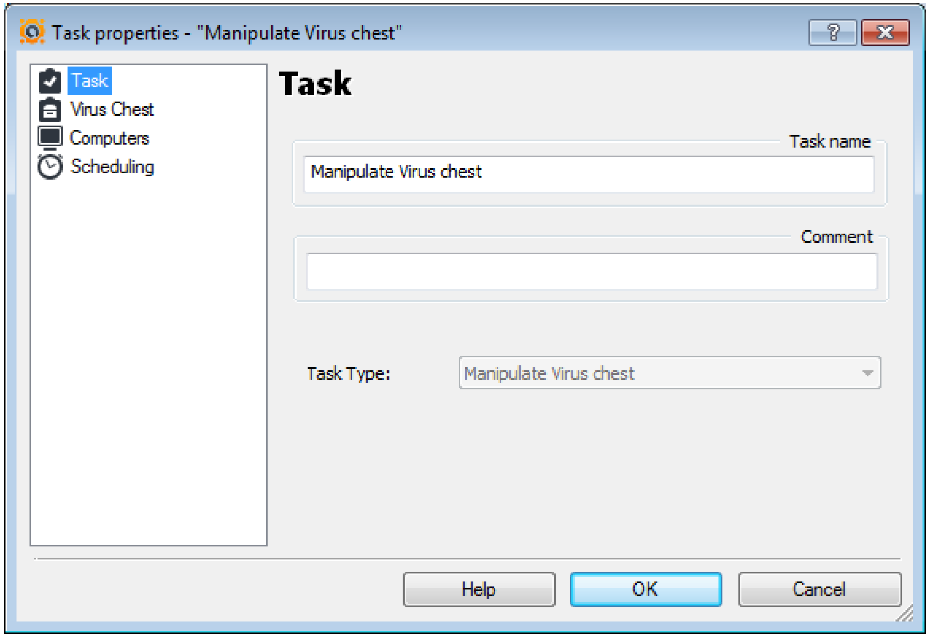
Name	Action
✓ Manipulate Virus chest	Today at 3:47:57 PM
✓ Uninstall managed product(s)	Today at 3:48:21 PM

- Auxiliary tasks can be used to create and manage all available tasks, but mainly they are used to cover:
  - Virus chest tasks
  - Uninstallation tasks

AEA console

Client-side tasks

Auxiliary task



Task properties - "Manipulate Virus chest"

Task

Task name: Manipulate Virus chest

Comment:

Task Type: Manipulate Virus chest

- The “Manipulate virus chest” task allows you (remotely) to :
  - Restore..
  - Remove..
  - Delete..

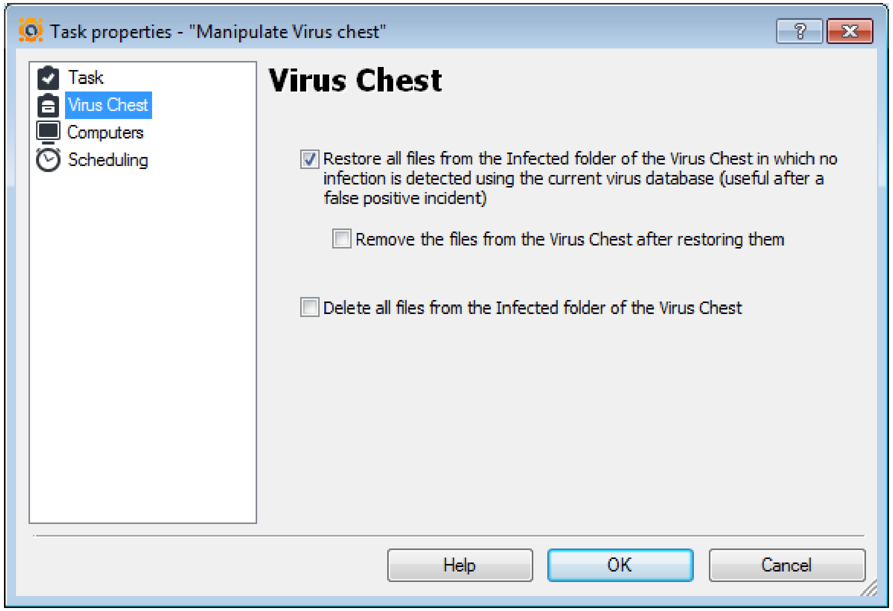
  .. files in the virus chest

- Choose the computer to run the task on
- Schedule one task or task chain

AEA console

Client-side tasks

Auxiliary task



Task properties - "Manipulate Virus chest"

- Task
- Virus Chest
- Computers
- Scheduling

Virus Chest

☑ Restore all files from the Infected folder of the Virus Chest in which no infection is detected using the current virus database (useful after a false positive incident)

□ Remove the files from the Virus Chest after restoring them

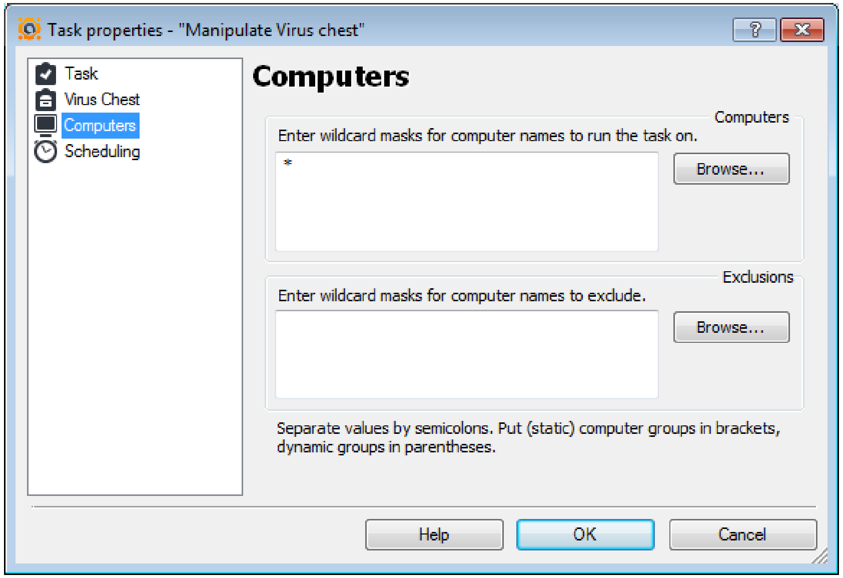
□ Delete all files from the Infected folder of the Virus Chest

- Restore all files from the infected folder of the virus chest, in which no infection is detected using the current VPS (useful after a false positive alert)
  - Remove the files from the virus chest after restoring them
- Delete all files in the infected folder of the virus chest

AEA console

Client-side tasks

Auxiliary task



Task properties - "Manipulate Virus chest"

Computers

Enter wildcard masks for computer names to run the task on.

*

Enter wildcard masks for computer names to exclude.

Separate values by semicolons. Put (static) computer groups in brackets, dynamic groups in parentheses.

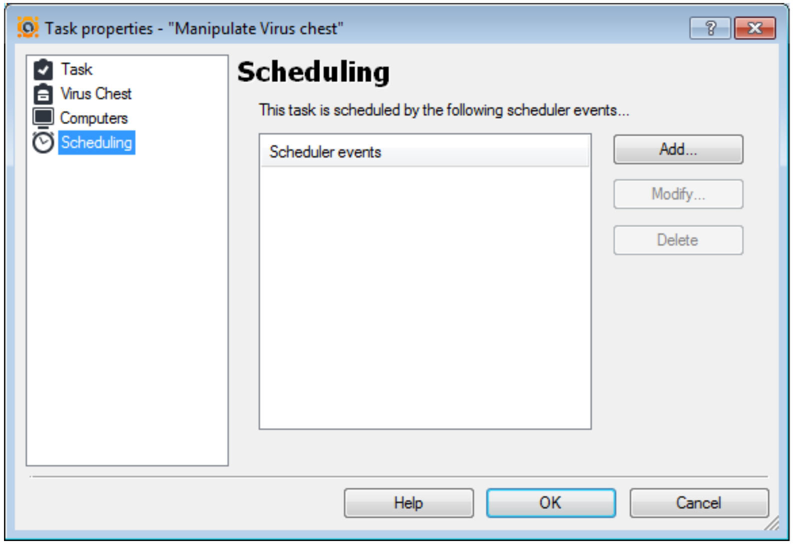
- On this page you can specify the computers on which this task should be run, or which should be excluded.

- You can also specify computers in groups.
  - Static groups should be closed in square brackets
    - e.g., [MyGroupName].
  - Dynamic groups should be enclosed in regular brackets
    - e.g., (Computers with Agent)
    - e.g., (Computers without Agent)

AEA console

Client-side tasks

Auxiliary task



Task properties - "Manipulate Virus chest"

Scheduling

This task is scheduled by the following scheduler events...

Scheduler events

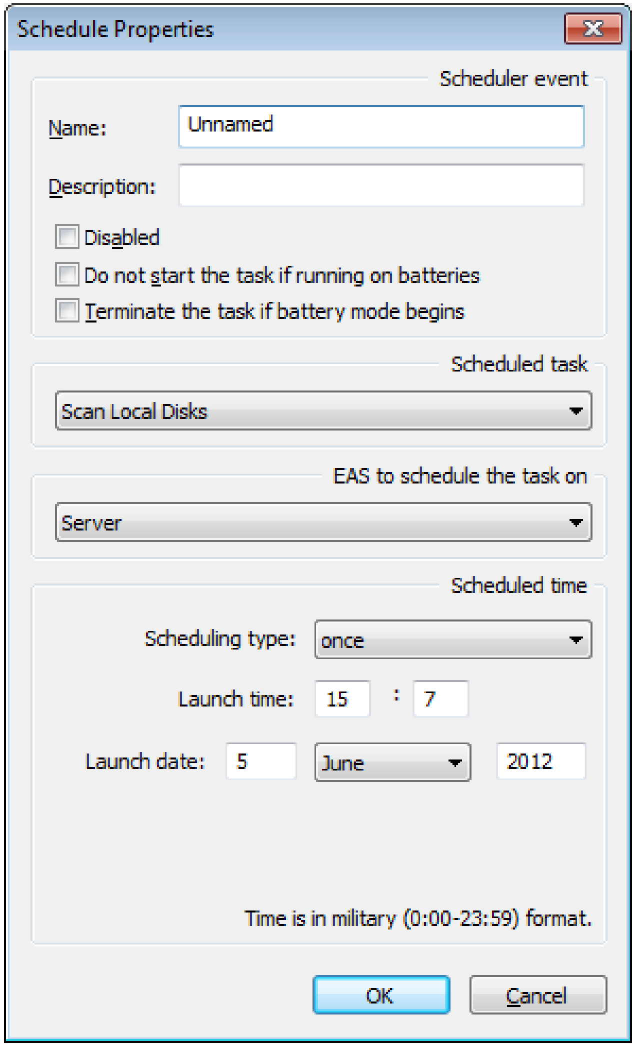
- avast! makes it possible to schedule a task to start automatically on a given date and at a given time.

- **Add**
  - Adds a new scheduled task, i.e. it schedules a task to start automatically.
- **Modify**
  - Modifies the selected scheduled task.
- **Delete**
  - Deletes the selected task.

- If you want a task to be started on a given date and at a given time, select Add. A new window will appear ->

AEA console

Client-side tasks



Schedule Properties

Scheduler event

Name: Unnamed

Description:

□ Disabled

□ Do not start the task if running on batteries

□ Terminate the task if battery mode begins

Scheduled task: Scan Local Disks

EAS to schedule the task on: Server

Scheduled time

Scheduling type: once

Launch time: 15 : 7

Launch date: 5 June 2012

Time is in military (0:00-23:59) format.

Auxiliary task

-> here you should enter the parameters defining the new task

- **Name**
  - Name of the task, e.g. "Weekend scan".
- **Description**
  - Enter a brief description of the task e.g. "Scans all the hard disks every Sunday night".
- **Disabled**
  - This option disables the scheduled task. It is useful when you need to stop the task from running, but you do not want to delete the task completely and have to re-enter it again later.
- **Do not start the task if running on batteries**
  - Useful mainly for notebook owners. The task will not be started if the computer is running on batteries.
- **Terminate the task if battery mode begins**
  - If, while a scheduled task is running, the computer is cut off from the electric power supply and switches to batteries, the task will be terminated. Again, this is useful mainly for notebook owners.
- **Scheduled task**
  - Select the task to be scheduled.
- **Scheduling type**
  - Here you can specify when the task will be started.
    - Once - you simply enter the time and date when the task should be run.
    - Daily - enter the time only - the task will be started each day at the given time.
    - Weekly (or monthly)
- **Launch time/launch date**
  - Here you can set the time and the actual day of the week (month) when the scheduled task should be run.

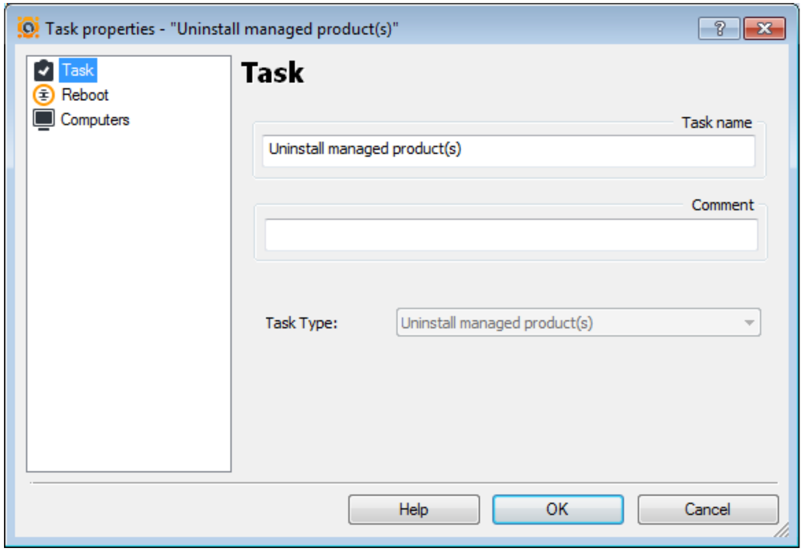
Client-side tasks/Auxiliary task

UNINSTALL MANAGED PRODUCT(s)

AEA console

Client-side tasks

Auxiliary task



Task properties - "Uninstall managed product(s)"

Task

Task name: Uninstall managed product(s)

Comment:

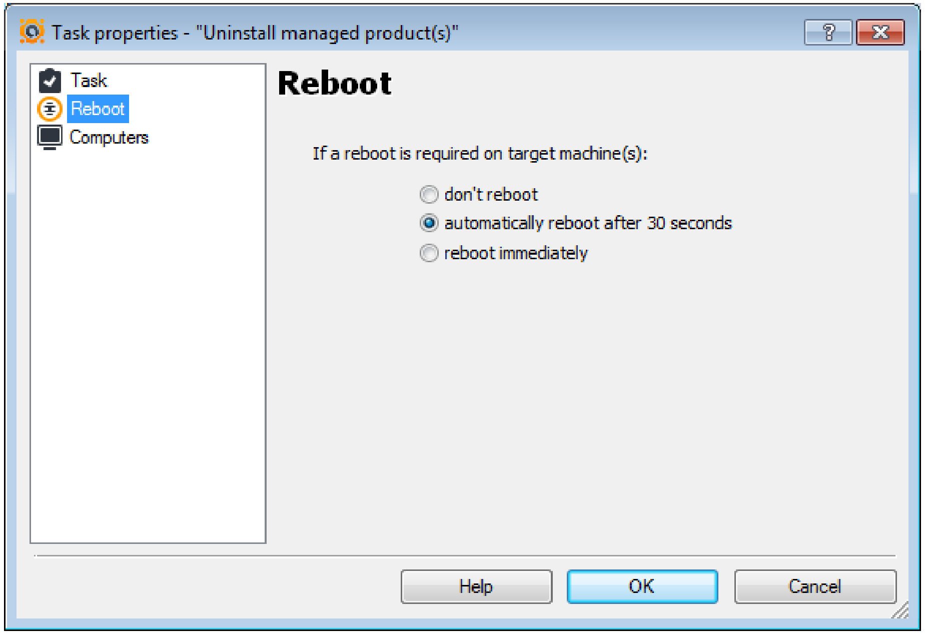
Task Type: Uninstall managed product(s)

- Every good program comes with an uninstallation program, and AEA is no exception.
- The uninstallation task can be also be found in the Deployment Tasks folder, in the console
- The uninstallation task uninstalls all avast! managed products from the selected computers.
- The task can be scheduled to run on all managed computers, or on just some of them.
- **Note:**
  - Sometimes the uninstallation task in the console stays in the “Running” state even if it has already completed, that is, even after the software has been removed from the client machines. This is because the agent is removed as part of the uninstallation process, and therefore it fails to report the final status of the operation to the EAS.

AEA console

Client-side tasks

Auxiliary task



Task properties - "Uninstall managed product(s)"

Reboot

If a reboot is required on target machine(s):

○ don't reboot

● automatically reboot after 30 seconds

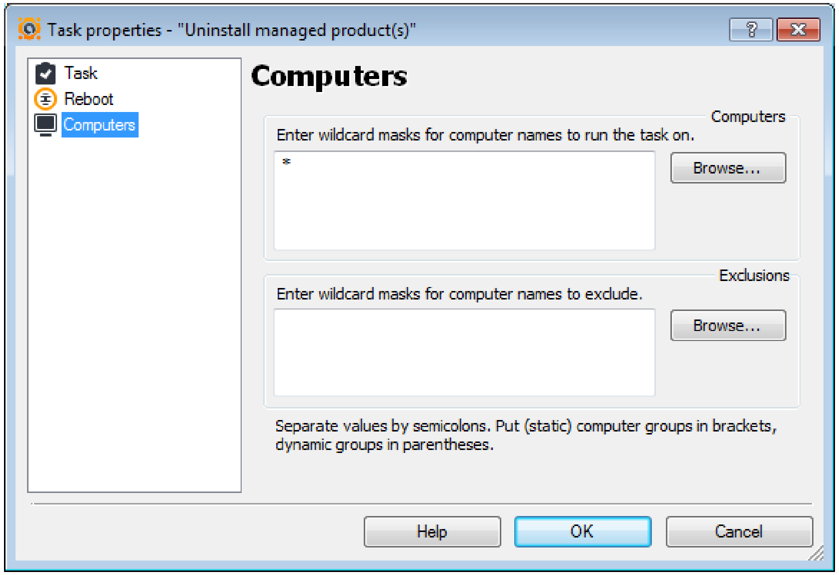
○ reboot immediately

- On this page you can customize the way the program handles the situation where a reboot of a client computer is required to complete the update.
  - Don‘t reboot
  - Automatically reboot after 30 seconds
  - Reboot immediately

AEA console

Client-side tasks

Auxiliary task



Task properties - "Uninstall managed product(s)"

Computers

Computers

Enter wildcard masks for computer names to run the task on.

*

Exclusions

Enter wildcard masks for computer names to exclude.

Separate values by semicolons. Put (static) computer groups in brackets, dynamic groups in parentheses.

- On this page you can specify the computers that this task should run on or should be excluded from.

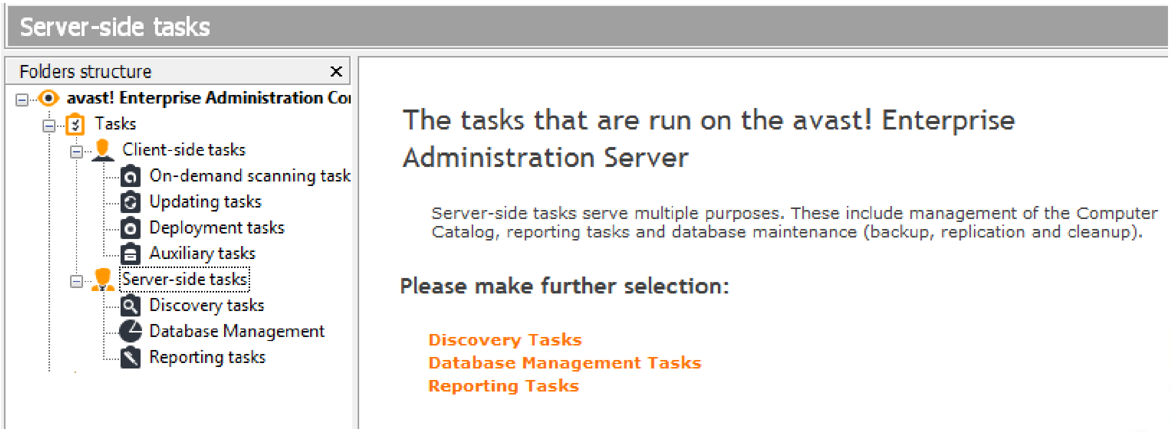
- You can also specify computers in groups.
  - Static groups should be closed in square brackets
    - e.g., [MyGroupName].
  - Dynamic groups should be enclosed in regular brackets
    - e.g., (Computers with Agent)
    - e.g., (Computers without Agent)

AEA console

SERVER-SIDE TASKS

AEA console

Server-side tasks



The tasks that are run on the avast! Enterprise Administration Server

Server-side tasks serve multiple purposes. These include management of the Computer Catalog, reporting tasks and database maintenance (backup, replication and cleanup).

Please make further selection:

Discovery Tasks
Database Management Tasks
Reporting Tasks

- Server-side tasks can be used for multiple purposes. These include management of the Computer Catalog, reporting tasks and database maintenance (backup, replication and cleanup).

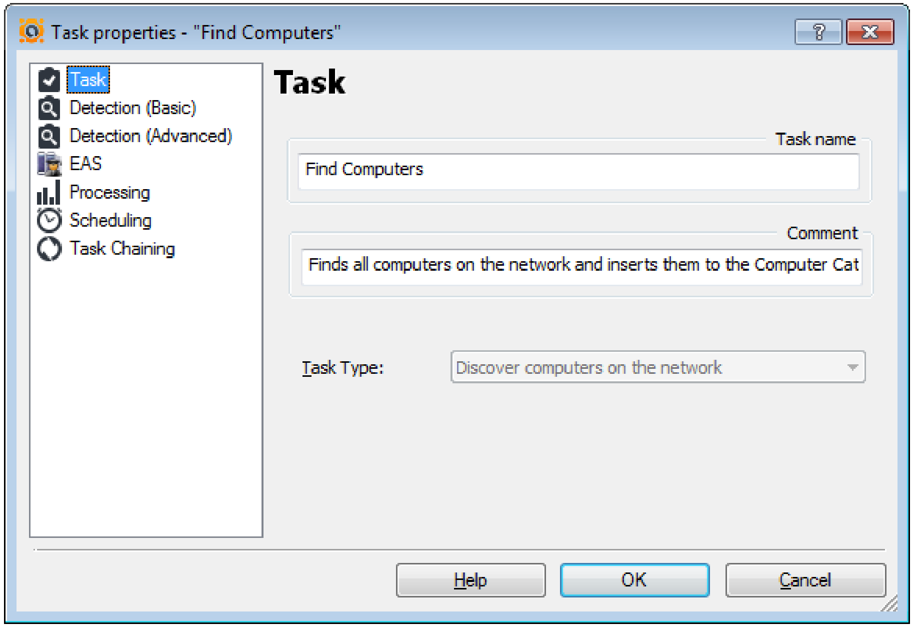
- The tasks can either be run on-demand, or by creating a schedule. It is recommended to create a schedule for the most common tasks, such as reporting and DB backup.

AEA server-side tasks

DISCOVERY TASKS

AEA console

Server-side tasks



Task properties - "Find Computers"

Task

Task name: Find Computers

Comment: Finds all computers on the network and inserts them to the Computer Cat

Task Type: Discover computers on the network

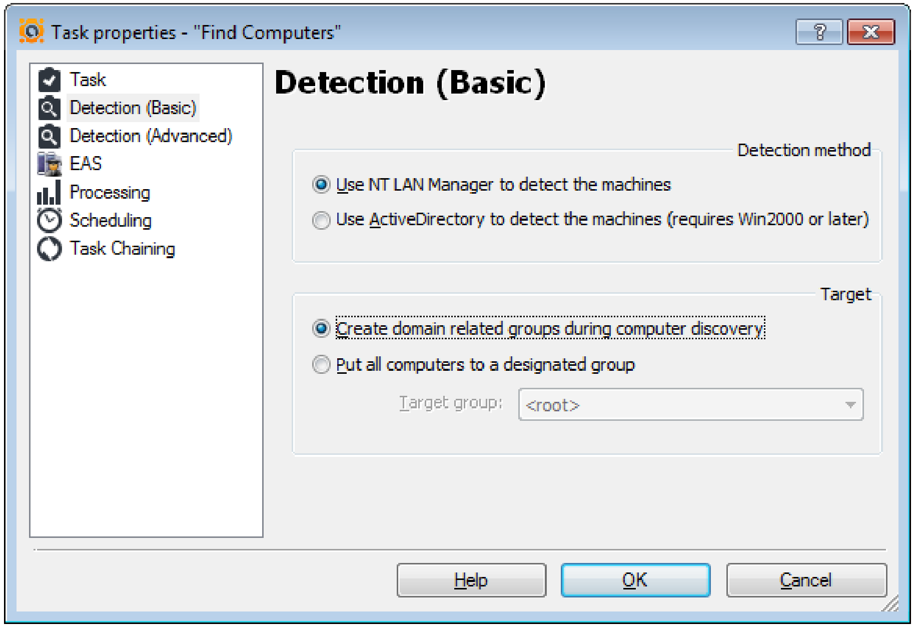
Discovery tasks

- Using a Discovery Task is probably the easiest and most convenient way to build the Computer Catalog. To use it, go to Tasks/Server-side tasks/Discovery tasks and create a new task.
- Normally, you can leave all the boxes set to their default values. Then run the task by double-clicking it. This will create a new session object for that task, as usual.
- The task queries the ActiveDirectory and/or the NT LAN Manager to find all the computers on the network and adds them to the Computer Catalog group, either to the root or to the individual folders created to reflect the organization's domain/workgroup structure.
- Since a discovery task typically runs for quite a while, you'll have to wait for it to complete. You can monitor its current status by looking at the session properties.
- **Note:**
  - **the view is not automatically refreshed. To see the progress, you need to keep refreshing it manually by pressing F5.**
- After the task completes, the Computer Catalog should be populated with all the computers that have been found. Don't forget to refresh the view to see all the new items.
- **Note:**
  - **In some cases you will have to close the AEA console and start it up again to see the GUI refreshed.**

AEA console

Server-side tasks

Discovery tasks



Task properties - "Find Computers"

Detection (Basic)

Detection method

● Use NT LAN Manager to detect the machines

○ Use ActiveDirectory to detect the machines (requires Win2000 or later)

Target

● Create domain related groups during computer discovery

○ Put all computers to a designated group

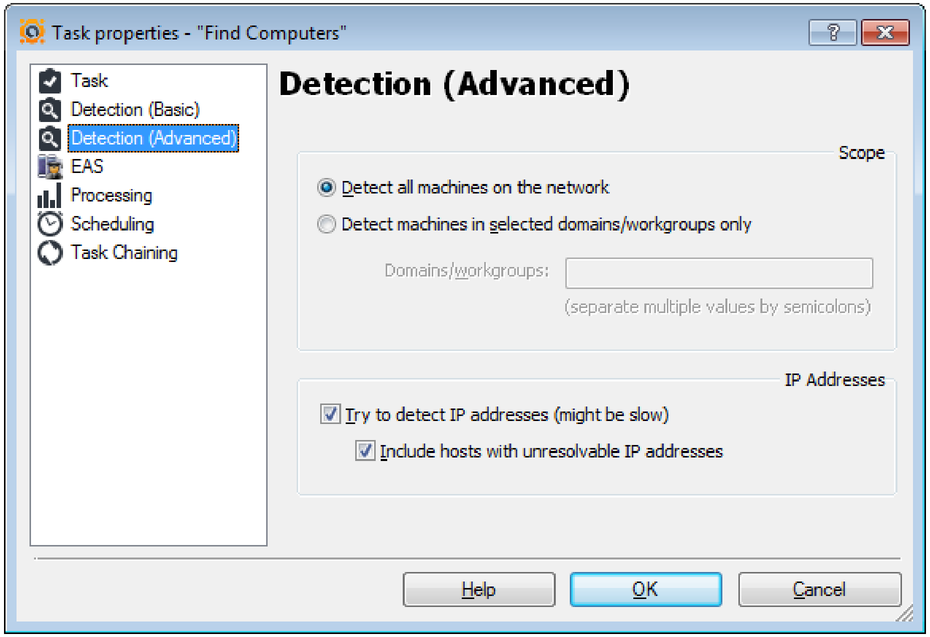
Target group: <root>

- **Detection methods**
  - Use NT LAN manager to detect the machines
  - Use Active directory to detect the machines (requires Win2003 or later)
- **Target groups**
  - Create domain related groups during computer discovery
  - Put all computers into a designed group (custom created groups under Computer catalog)

AEA console

Server-side tasks

Discovery tasks



Task properties - "Find Computers"

Detection (Advanced)

Scope

● Detect all machines on the network

○ Detect machines in selected domains/workgroups only

Domains/workgroups:

(separate multiple values by semicolons)

IP Addresses

☑ Try to detect IP addresses (might be slow)

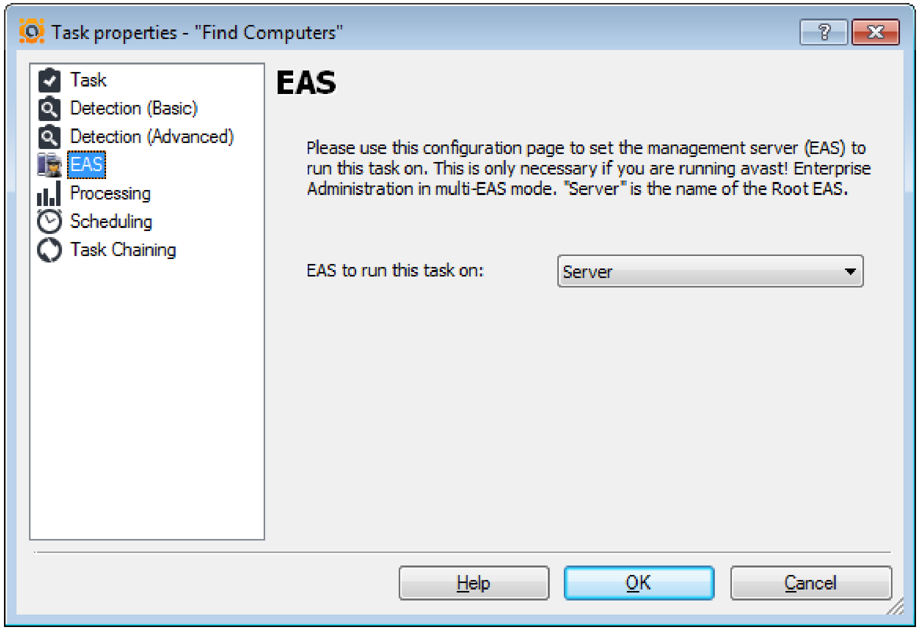
☑ Include hosts with unresolvable IP addresses

- **Scope**
  - – Detect all machines on the network
  - – Detect machines in selected domains/workgroups only
- **IP addresses**
  - – Try to detect IP addresses
    - Include hosts with unresolved IP addresses

AEA console

Server-side tasks

Discovery tasks



EAS

Please use this configuration page to set the management server (EAS) to run this task on. This is only necessary if you are running avast! Enterprise Administration in multi-EAS mode. "Server" is the name of the Root EAS.

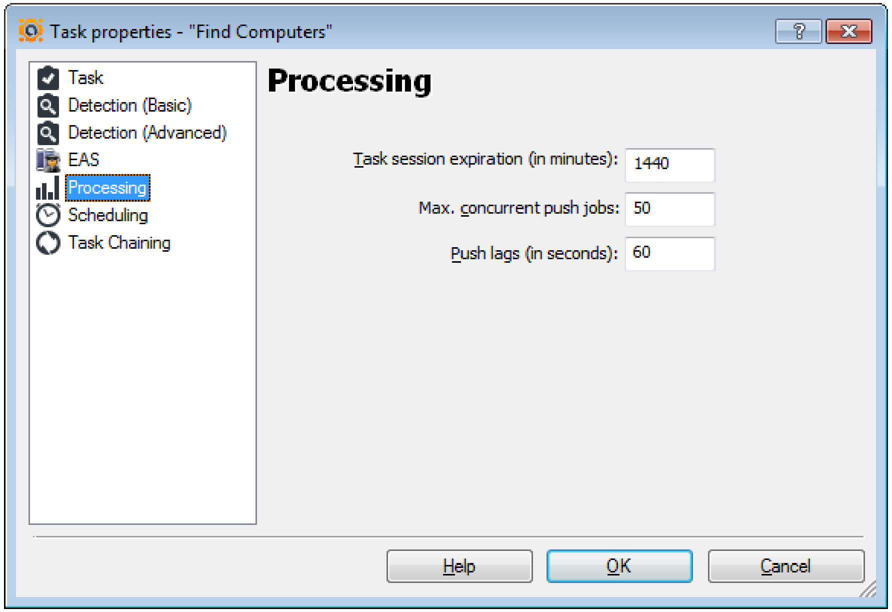
EAS to run this task on: Server

- The following configuration page can be used to select the Enterprise Server (EAS) on which to run this task. This is only necessary if you are running AEA in multi EAS mode.
- The server is the name of the Root EAS

AEA console

Server-side tasks

Discovery tasks


Task properties - "Find Computers"

Processing

Task session expiration (in minutes): 1440

Max. concurrent push jobs: 50

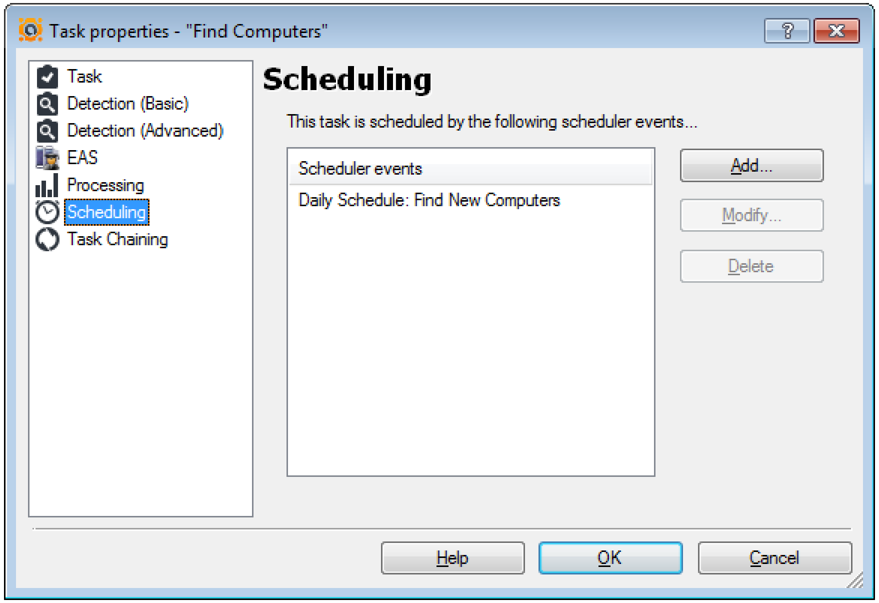
Push lags (in seconds): 60

- Task session expiration
  - The maximum period of time for which AEA will run a specific session (the time from when the task started). When the time limit is reached, the session will be terminated.
  - The default time limit is 1440 minutes
- Max.concurrent push jobs
  - The maximum number of threads which the server creates to contact/establish a connection with computers on the network on which the task should be run.
  - The default maximum number of concurrent jobs is 50
- Push lags
  - The time lag between push jobs to prevent network overload.
  - The default is 60 seconds

AEA console

Server-side tasks

Discovery tasks



Scheduling

This task is scheduled by the following scheduler events...

Scheduler events

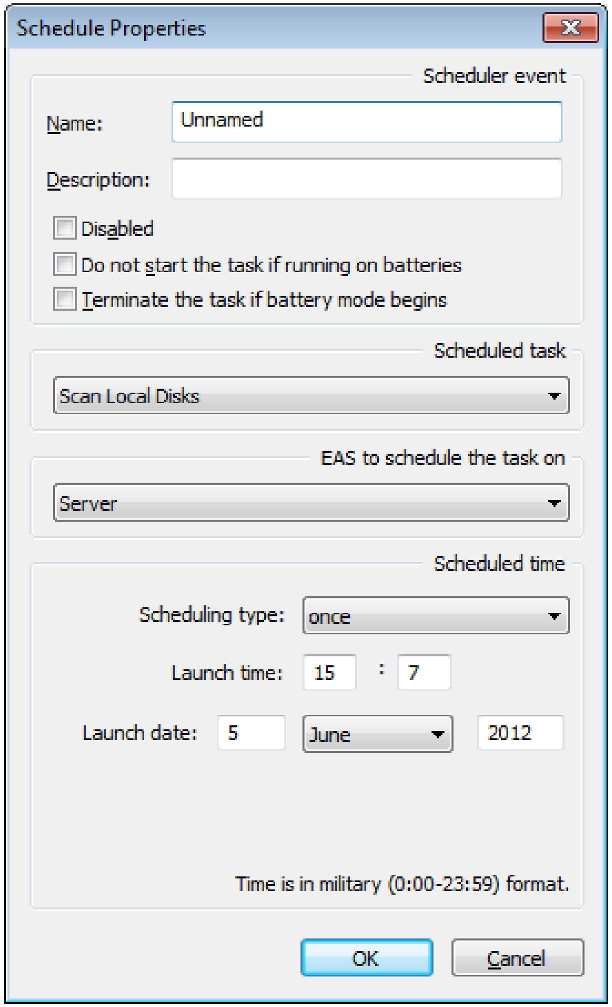
Daily Schedule: Find New Computers

- avast! makes it possible to schedule a task to start automatically on a given date and at a given time.
- **Add**
  - Adds a new scheduled task, i.e. it schedules a task to start automatically.
- **Modify**
  - Modifies the selected scheduled task.
- **Delete**
  - Deletes the selected task.
- If you want a task to be started on a given date and at a given time, select Add. A new window will appear **->**

AEA console

Client-side tasks

Discovery tasks



Schedule Properties

Scheduler event

Name: Unnamed

Description:

□ Disabled

□ Do not start the task if running on batteries

□ Terminate the task if battery mode begins

Scheduled task

Scan Local Disks

EAS to schedule the task on

Server

Scheduled time

Scheduling type: once

Launch time: 15 : 7

Launch date: 5 June 2012

Time is in military (0:00-23:59) format.

-> here you should enter the parameters defining the new task

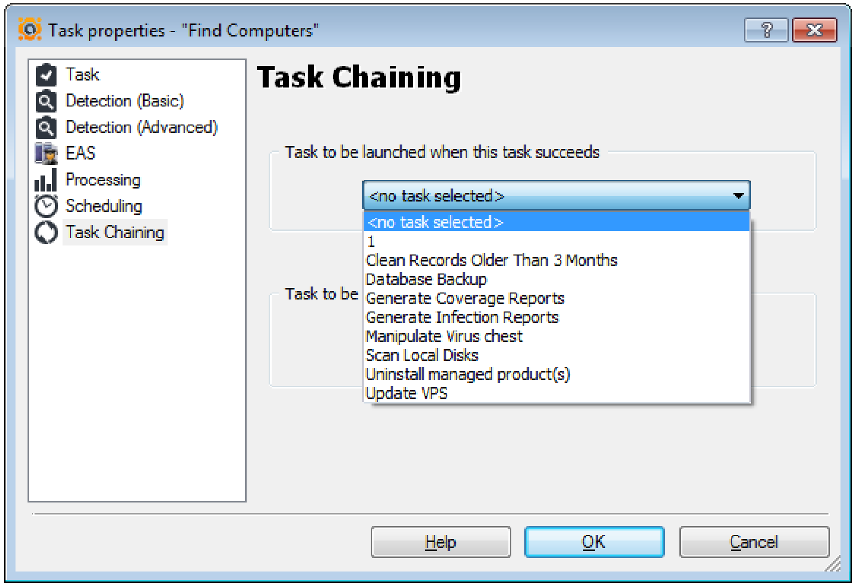
- **Name**
  - Name of the task, e.g. "Weekend scan".
- **Description**
  - Enter a brief description of the task e.g. "Scans all the hard disks every Sunday night".
- **Disabled**
  - This option disables the scheduled task. It is useful when you need to stop the task from running, but you do not want to delete the task completely and have to re-enter it again later.
- **Do not start the task if running on batteries**
  - Useful mainly for notebook owners. The task will not be started if the computer is running on batteries.
- **Terminate the task if battery mode begins**
  - If, while a scheduled task is running, the computer is cut off from the electric power supply and switches to batteries, the task will be terminated. Again, this is useful mainly for notebook owners.
- **Scheduled task**
  - Select the task to be scheduled.
- **Scheduling type**
  - Here you can specify when the task will be started.
    - Once - you simply enter the time and date when the task should be run.
    - Daily - enter the time only - the task will be started each day at the given time.
    - Weekly (or monthly)
- **Launch time/launch date**
  - Here you can set the time and the actual day of the week (month) when the scheduled task should be run.

AEA console

Client-side tasks

Here you can choose the task which will be launched if the deployment task is successful.

The list of the tasks is displayed below:



Task Chaining

Task to be launched when this task succeeds

<no task selected>

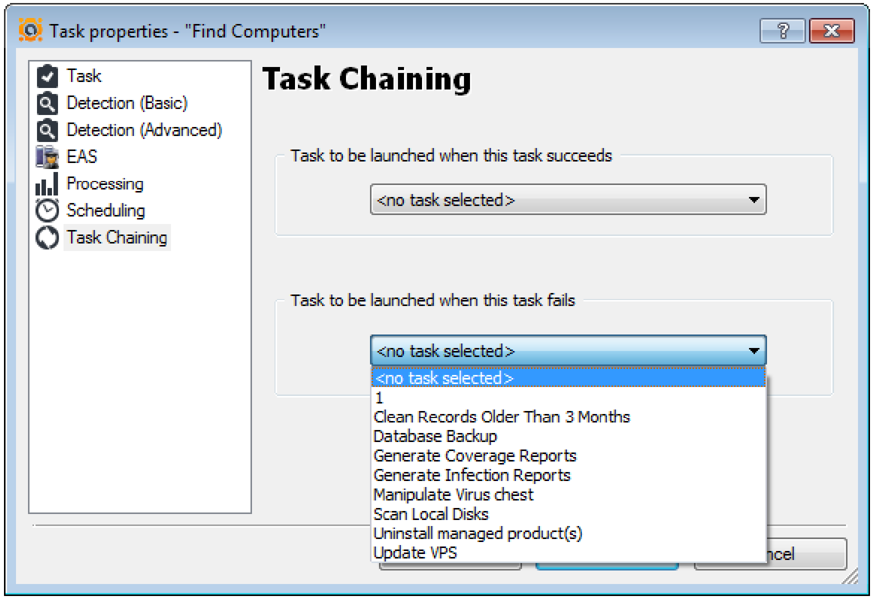
<no task selected>
1
Clean Records Older Than 3 Months
Database Backup
Generate Coverage Reports
Generate Infection Reports
Manipulate Virus chest
Scan Local Disks
Uninstall managed product(s)
Update VPS

Task to be

Discovery tasks

Here you can choose the task which will be launched if the deployment task fails.

The list of the tasks is displayed below:



Task Chaining

Task to be launched when this task succeeds

<no task selected>

Task to be launched when this task fails

<no task selected>

<no task selected>
1
Clean Records Older Than 3 Months
Database Backup
Generate Coverage Reports
Generate Infection Reports
Manipulate Virus chest
Scan Local Disks
Uninstall managed product(s)
Update VPS

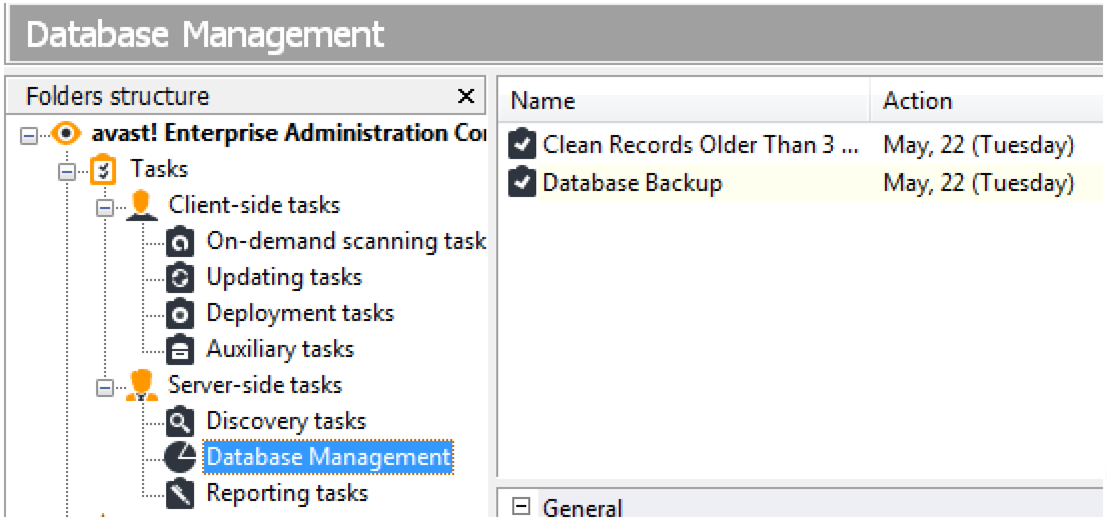
AEA server-side tasks

DATABASE MANAGEMENT

AEA console

Server-side tasks

Database management



Database Management

Folders structure

- avast! Enterprise Administration Co
  - Tasks
    - Client-side tasks
      - On-demand scanning task
      - Updating tasks
      - Deployment tasks
      - Auxiliary tasks
    - Server-side tasks
      - Discovery tasks
      - Database Management
      - Reporting tasks

Name	Action
Clean Records Older Than 3 ...	May, 22 (Tuesday)
Database Backup	May, 22 (Tuesday)

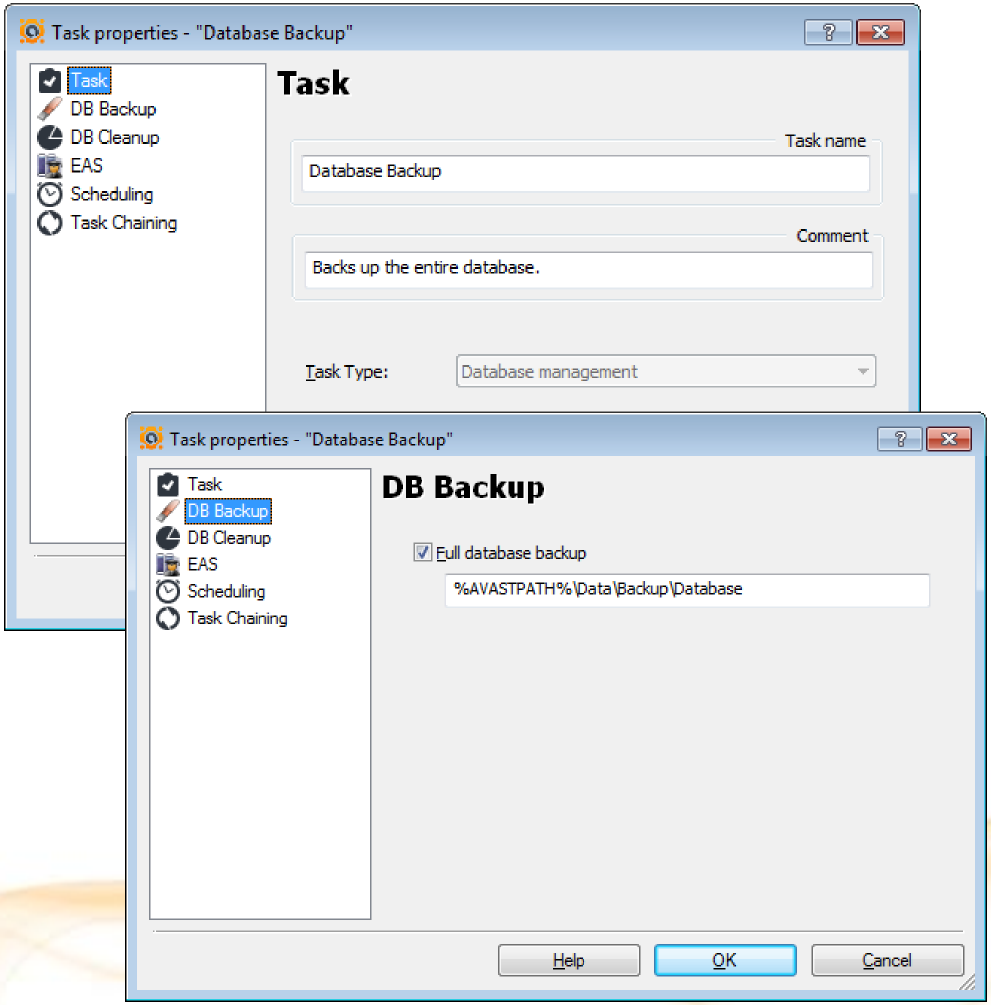
- Database management allows the Administrator to run the most important tasks related to the SQL DB maintenance, such as database cleanup, backup and database replication.

- All neccessarry basic and advanced settings may be modified via task properties, such as full DB backup, delete events, sessions, computers.. Followed by task scheduling or/and task chaining features.

AEA console

Server-side tasks

Database management



Task

Task name: Database Backup

Comment: Backs up the entire database.

Task Type: Database management

DB Backup

☑ Full database backup

%AVASTPATH%\Data\Backup\Database

- As AEA is based on a SQL database, it requires frequent maintenance. For these purposes, there's a special type of server-side task in AEA—the DB maintenance tasks.

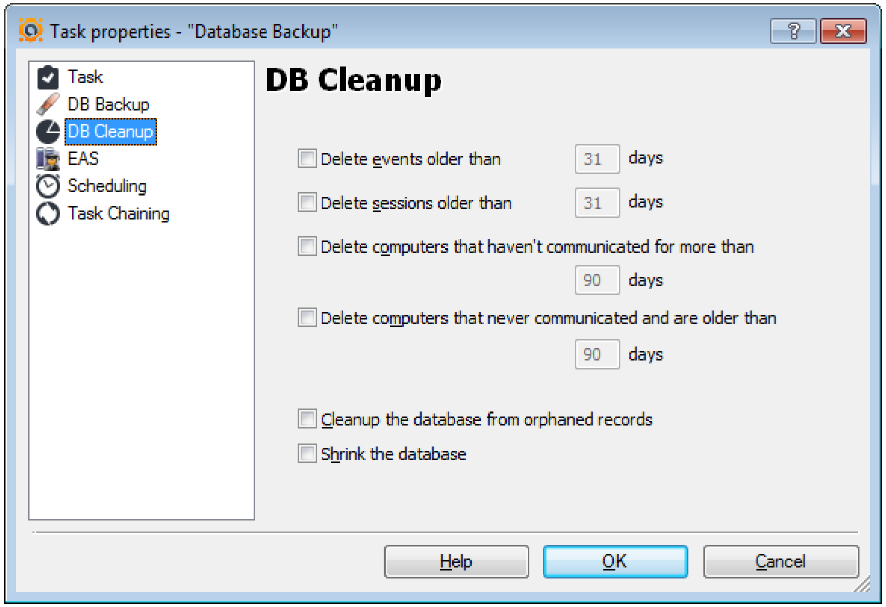
- With a DB Maintenance task, you can do the following:
  - Perform a backup of the database.
  - Perform a database cleanup

- Scheduling regular backups of the whole database is important. You should incorporate backup of the AEA database into your overall network backup strategy. There are two recommended ways:
  - 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 you can use an AEA DB Maintenance task to back up the database to a file and then back up that file using standard methods.

AEA console

Server-side tasks

Database management



Task properties - "Database Backup"

DB Cleanup

□ Delete events older than 31 days

□ Delete sessions older than 31 days

□ Delete computers that haven't communicated for more than 90 days

□ Delete computers that never communicated and are older than 90 days

□ Cleanup the database from orphaned records

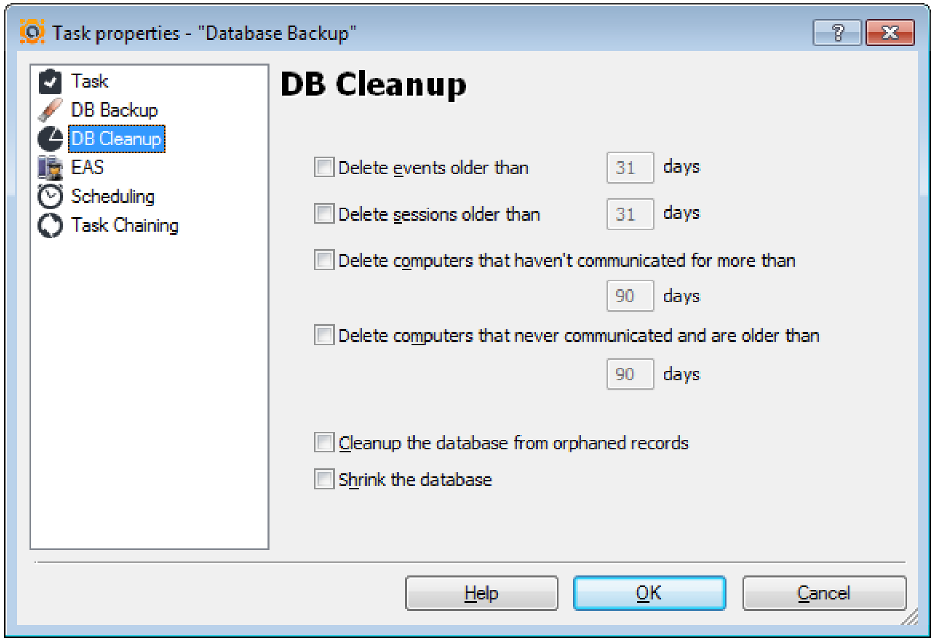
□ Shrink the database

- Database cleanup can be used to remove older records from the database.
- DB cleanup keeps the database from growing indefinitely. The DB Maintenance task also lets you delete “orphaned” records, which will also reduce the size of the database.
- You can specify the oldest records you’d like to keep. Of course, once you delete the old records, you can no longer generate reports from their data, so you must decide in advance how much data you need.

AEA console

Server-side tasks

Database management



DB Cleanup

□ Delete events older than 31 days

□ Delete sessions older than 31 days

□ Delete computers that haven't communicated for more than 90 days

□ Delete computers that never communicated and are older than 90 days

□ Cleanup the database from orphaned records

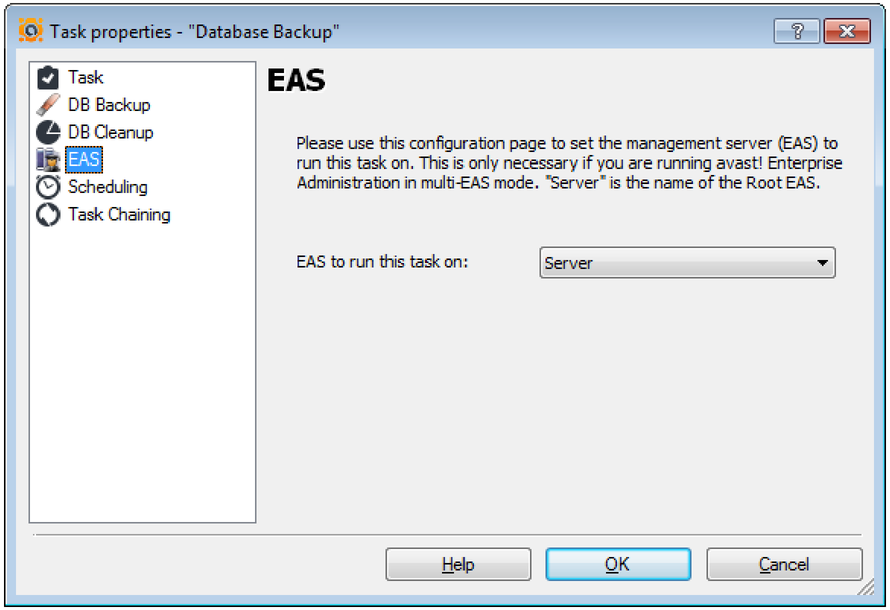
□ Shrink the database

- Delete events older than
  - XX days
- Delete sessions older than
  - XX days
- Delete computers that haven‘t communicated for more than
  - XX days
- Delete computers that have never communicated and are older than
  - XX days
- Cleanup the database from orphaned records

AEA console

Server-side tasks

Database management



Task properties - "Database Backup"

EAS

Please use this configuration page to set the management server (EAS) to run this task on. This is only necessary if you are running avast! Enterprise Administration in multi-EAS mode. "Server" is the name of the Root EAS.

EAS to run this task on: Server

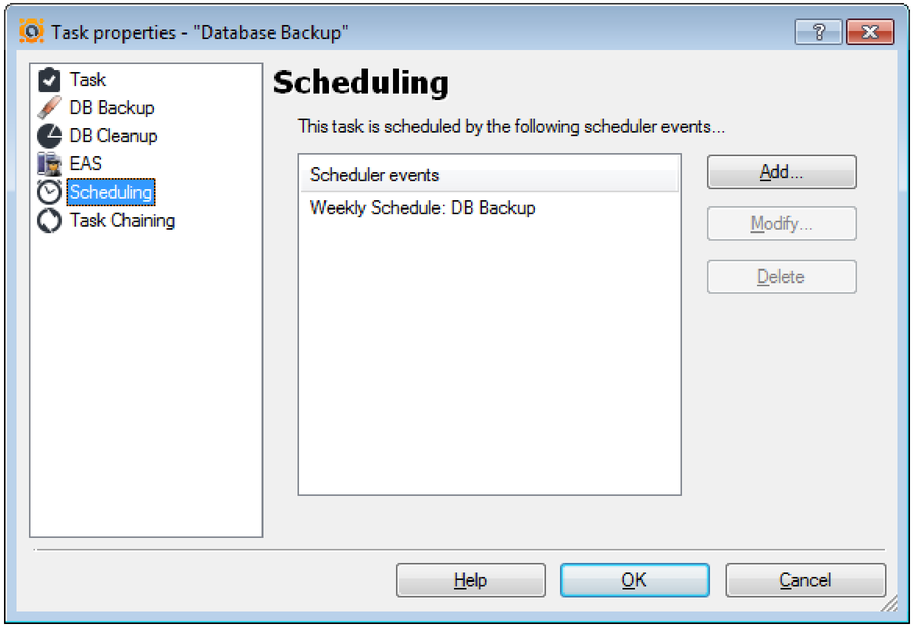
- The following configuration page can be used to select the Enterprise Server (EAS) on which to run this task. This is only necessary if you are running AEA in multi EAS mode.

- The server is the name of the Root EAS

AEA console

Server-side tasks

Database management



Task properties - "Database Backup"

- Task
- DB Backup
- DB Cleanup
- EAS
- Scheduling
- Task Chaining

Scheduling

This task is scheduled by the following scheduler events...

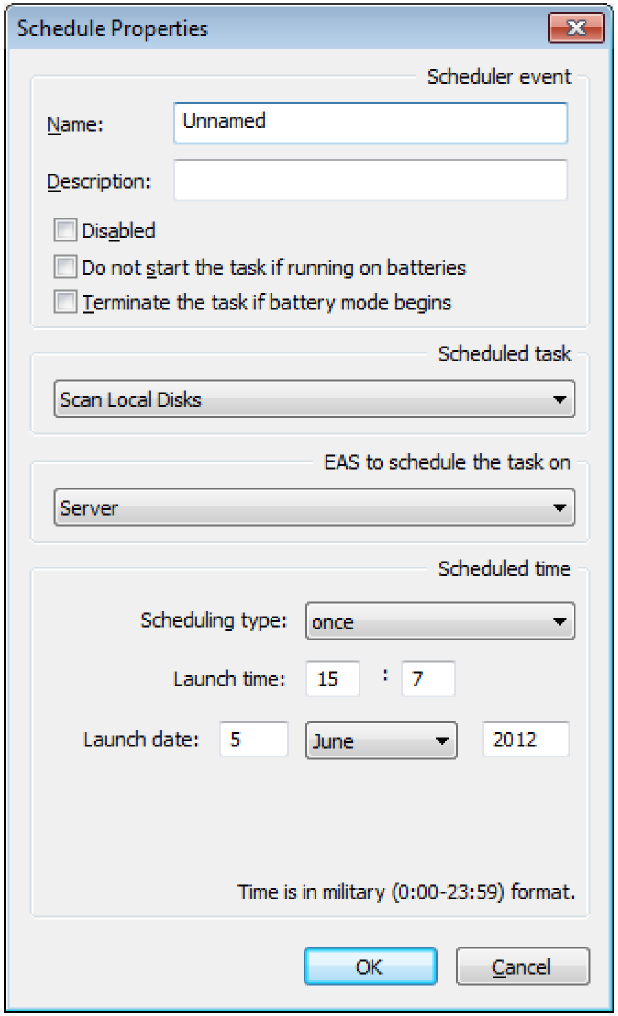
Scheduler events
Weekly Schedule: DB Backup

- avast! makes it possible to schedule a task to start automatically on a given date and at a given time.
- **Add**
  - Adds a new scheduled task, i.e. it schedules a task to start automatically.
- **Modify**
  - Modifies the selected scheduled task.
- **Delete**
  - Deletes the selected task.
- If you want a task to be started on a given date and at a given time, select Add. A new window will appear ->

AEA console

Client-side tasks

Database management



Schedule Properties

Scheduler event

Name: Unnamed

Description:

☐ Disabled

☐ Do not start the task if running on batteries

☐ Terminate the task if battery mode begins

Scheduled task: Scan Local Disks

EAS to schedule the task on: Server

Scheduled time

Scheduling type: once

Launch time: 15 : 7

Launch date: 5 June 2012

Time is in military (0:00-23:59) format.

-> here you should enter the parameters defining the new task

- **Name**
  - Name of the task, e.g. "Weekend scan".
- **Description**
  - Enter a brief description of the task e.g. "Scans all the hard disks every Sunday night".
- **Disabled**
  - This option disables the scheduled task. It is useful when you need to stop the task from running, but you do not want to delete the task completely and have to re-enter it again later.
- **Do not start the task if running on batteries**
  - Useful mainly for notebook owners. The task will not be started if the computer is running on batteries.
- **Terminate the task if battery mode begins**
  - If, while a scheduled task is running, the computer is cut off from the electric power supply and switches to batteries, the task will be terminated. Again, this is useful mainly for notebook owners.
- **Scheduled task**
  - Select the task to be scheduled.
- **Scheduling type**
  - Here you can specify when the task will be started.
    - Once - you simply enter the time and date when the task should be run.
    - Daily - enter the time only - the task will be started each day at the given time.
    - Weekly (or monthly)
- **Launch time/launch date**
  - Here you can set the time and the actual day of the week (month) when the scheduled task should be run.

AEA console

Client-side tasks

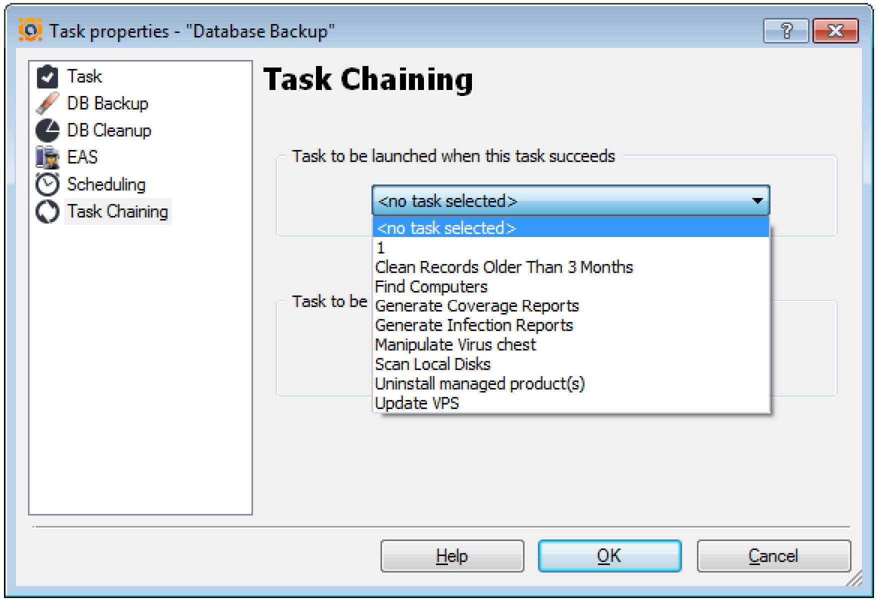
Here you can choose the task which will be launched if the deployment task is successful.

The list of the tasks is displayed below:

Database management

Here you can choose the task which will be launched if the deployment task fails.

The list of the tasks is displayed below:



Task properties - "Database Backup"

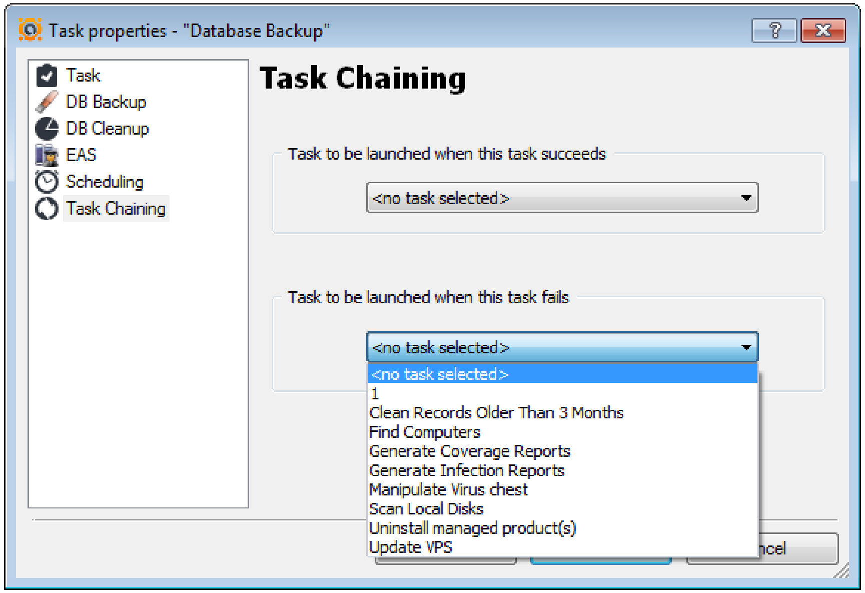
Task Chaining

Task to be launched when this task succeeds

<no task selected>

<no task selected>
1
Clean Records Older Than 3 Months
Find Computers
Generate Coverage Reports
Generate Infection Reports
Manipulate Virus chest
Scan Local Disks
Uninstall managed product(s)
Update VPS

Task to be



Task properties - "Database Backup"

Task Chaining

Task to be launched when this task succeeds

<no task selected>

Task to be launched when this task fails

<no task selected>

<no task selected>
1
Clean Records Older Than 3 Months
Find Computers
Generate Coverage Reports
Generate Infection Reports
Manipulate Virus chest
Scan Local Disks
Uninstall managed product(s)
Update VPS
ncel

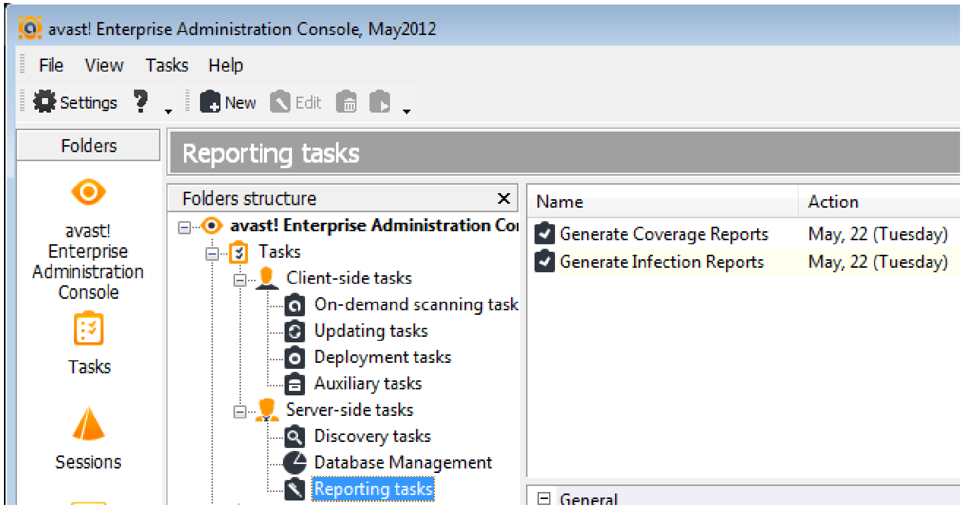
AEA server-side tasks

REPORTING TASKS

AEA console

Server-side tasks

Reporting tasks



Name	Action
☑ Generate Coverage Reports	May, 22 (Tuesday)
☑ Generate Infection Reports	May, 22 (Tuesday)

- AEA features powerful reporting capabilities second to no competing product. You can create a variety of useful reports from information collected by the EAS from the clients.

- You can export these reports in many popular formats. You can even have the reports sent to the management team automatically in periodic intervals.

- Reporting in AEA is generated, as is almost everything else, by certain tasks. Reporting tasks are grouped in a special folder in the console, under the Server-side tasks category.

- AEA comes with about twenty predefined reports

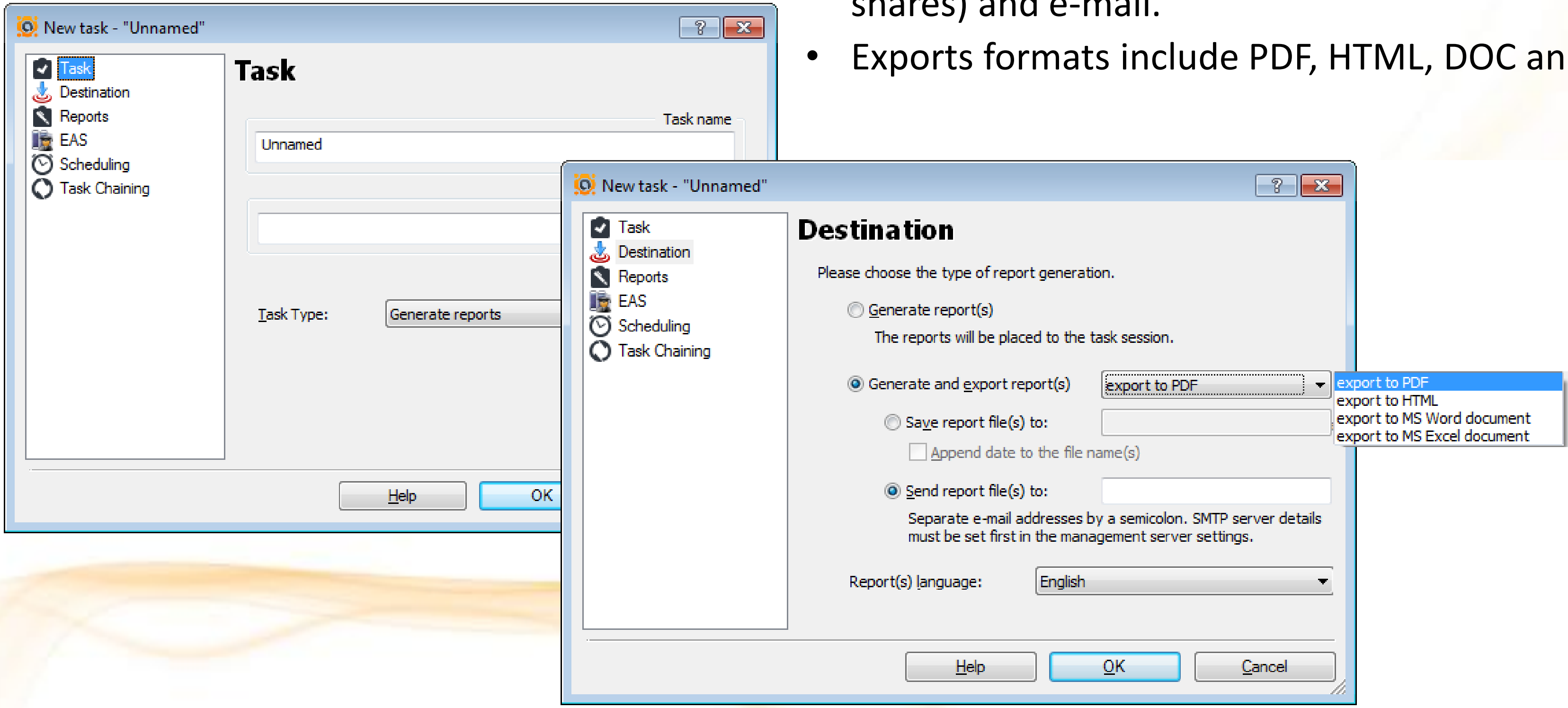
AEA console

Server-side tasks

Reporting tasks

- Reports can be generated directly and saved in the task session, to be viewed and/or printed from the console via the integrated report viewer.

- Or they can be exported outside the database.
  - Export targets include files (possibly on network shares) and e-mail.
  - Exports formats include PDF, HTML, DOC and XLS.



New task - "Unnamed"

Task

Task name: Unnamed

Task Type: Generate reports

New task - "Unnamed"

Destination

Please choose the type of report generation.

○ Generate report(s)

The reports will be placed to the task session.

● Generate and export report(s): export to PDF

○ Save report file(s) to:

□ Append date to the file name(s)

● Send report file(s) to:

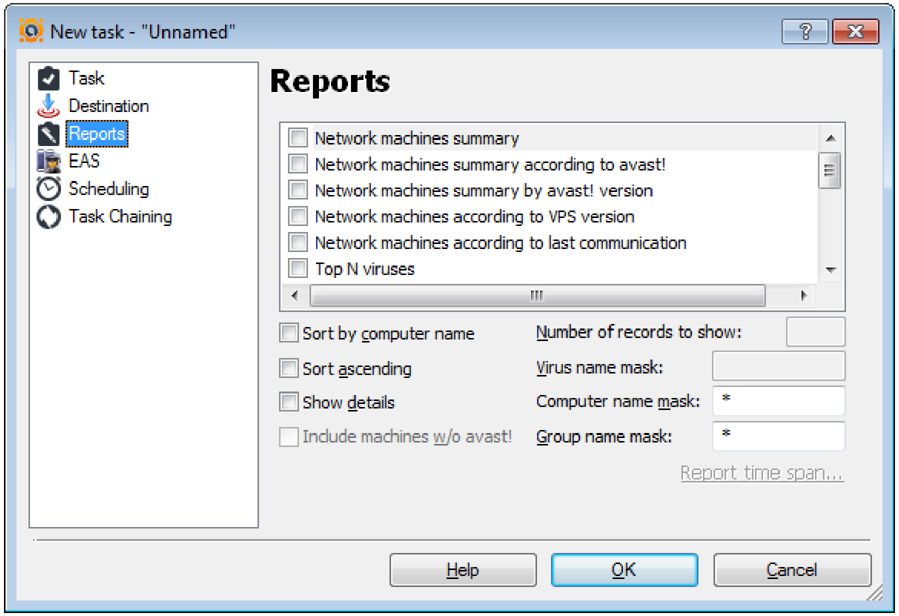
Separate e-mail addresses by a semicolon. SMTP server details must be set first in the management server settings.

Report(s) language: English

AEA console

Server-side tasks

Reporting tasks



New task - "Unnamed"

Reports

- ☐ Network machines summary
- ☐ Network machines summary according to avast!
- ☐ Network machines summary by avast! version
- ☐ Network machines according to VPS version
- ☐ Network machines according to last communication
- ☐ Top N viruses

☐ Sort by computer name — Number of records to show:

☐ Sort ascending — Virus name mask:

☐ Show details — Computer name mask: *

☐ Include machines w/o avast! — Group name mask: *

- Available predefined reports:

- **Network Machines Summary**
  - This report lists all computers on the network.
    - The form gives a summary of each computer—which group it's in, what operating system it runs, and which managed products are installed. It also contains additional, detailed information about every computer on the network.

- Note:
  - this form of the Network Machines Summary can be very large. You'll usually want to reduce its size by applying filters. The filtering options are a group name mask and a computer name mask, sorted in ascending or descending order.

AEA console

Server-side tasks

- **Network Machines Summary by avast! Installations**
  - This report creates a summary of all computers on the network with special regard to whether they have the managed version of avast! installed.
  - This report can also be generated in either a short, summarized form or a complete form that has detailed information about each computer.
  - The settings of this report are the same as for the previous one. It includes a pie chart from which the administrator can easily find out which computers have avast! installed and which do not.

Reporting tasks

- **Network Machines Summary by avast! Version**
  - This creates an easy to read report (with a pie chart and a table view) that shows all versions of avast! installed on the computers on the network.
  - The report can include machines without avast! installed, so it can also be used to check the overall status of antivirus protection on the network.

AEA console

Server-side tasks

- **Network Machines Summary by VPS Version**
  - This report is like the previous one, except that, instead of the avast! version, it provides the version of the virus database (the VPS file) on each computer.
  - It can include computers that do not have avast! installed and can filter machines by computer or domain masks.

Reporting tasks

- **Network Machines Summary by Last Communication**
  - This is a tabular presentation of all network machines sorted by the last time they reported their status to the EAS. It’s useful for discovering communication problems as well as finding zombie computers.
  - Like the other network summary reports, it is fully customizable.

AEA console

Server-side tasks

- **Top N Viruses**
  - Using a pie diagram and a bar chart, this report displays the Top N viruses detected in a given time period, including summary information about their total number and the date of first and last detection of each virus.
  - You can customize the N parameter that specifies the number of viruses to be included in the report, but we suggest that you don't use numbers higher than 20. Otherwise, the report may become less readable.

Reporting tasks

- **Actions on Top N Viruses**
  - This report is like the previous one, except that it shows the actions taken on the Top N viruses, not data on the viruses themselves.
  - The data included in the report can be displayed by time/date period, virus name mask and, as usual, the N parameter. For this report, we recommend setting N to a value no larger than 15.

AEA console

Server-side tasks

- **Top N Infected Files**
  - This report shows the Top N infected files in the form of a pie diagram and a bar chart, accompanied by a comprehensive list of these files, together with their count and time information.
  - The name of an infected file is prefixed by the name of the computer on which the virus was detected.
  - Even though the N parameter is not limited, we suggest that you use numbers no higher than 20, otherwise, the report may become less readable. You can also restrict the date/time span (including custom spans) for which to report infected files.

Reporting tasks

- **Top N Infected Computers**
  - This report shows a summary (as a pie diagram and a table) of the Top N most often infected computers on the network.
  - You can specify whether the report should include detailed information about each of the computers in the table.
  - We suggest that you use numbers no higher than 20 for the N parameter.
  - You can also define a group and domain mask and a date/time period.

AEA console

Server-side tasks

- **Infection Source Summary**
  - This report creates an easy-to-read table showing the relative frequency of various infection vectors—mail, hard disk, removable media, network, and script.
  - You can define the time/date period of the report. The report includes a pie chart for quick assessment.

Reporting tasks

- **Network Infection Summary**
  - The Network Infection Summary report is like the Top N viruses report, except that it shows a list of all viruses that have been found on the network, not only the Top N.
  - If the number of viruses is so large that the report becomes hard to read, you can reduce the virus list by applying a mask or narrowing the date/time period.

AEA console

Server-side tasks

- **Virus Actions Summary**
  - This report gives a tabular and graphical summary of actions taken on infected files—deleted, repaired, moved to Virus Chest, etc.
  - As always, you can set the time/date period of the report.

Reporting tasks

- **Change of Logical Disks Summary**
  - This report is a bit different, because it is not directly related to the antivirus protection.
  - It shows a summary of changes in the logical drive mappings on the managed computers, e.g., attachment of a USB disk, mapping of a network drive, etc.
  - You can specify the time/date period.

AEA console

Server-side tasks

- **Top N Attacked Computers**
  - This report shows the Top N computers that have been attacked (unsuccessfully) by a network worm, as detected by the avast! Network Shield.
  - You can define the parameter N and the time/date period.
  - This report is generated as a pie chart, a bar chart, and a table.

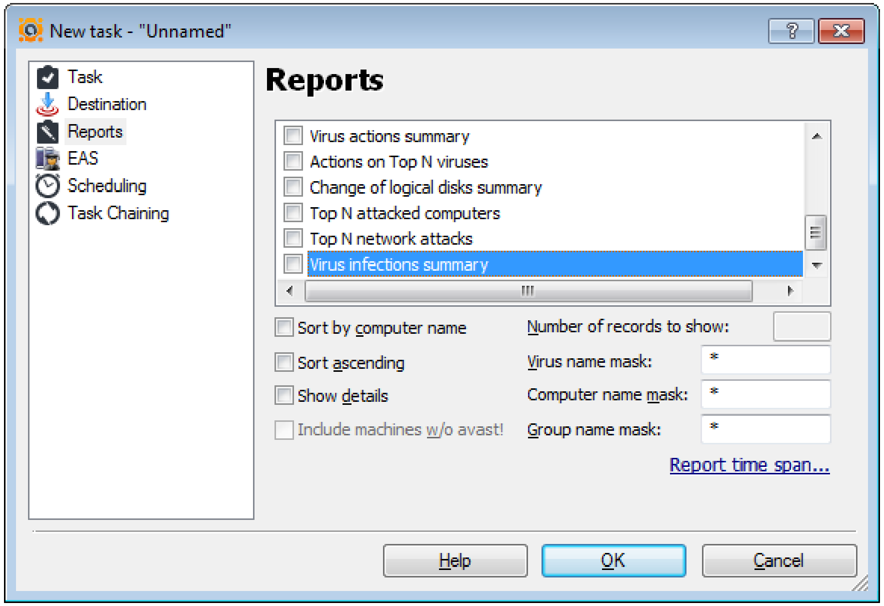
Reporting tasks

- **Top N Network Attacks**
  - The Top N Network Attacks report shows a summary of network attacks detected by the avast! Network Shield.
  - You can define the N parameter and the time/date period.
  - The report provides comprehensive information, including time stamps and the IP address that each attack came from.
  - It includes a pie chart and a bar chart.

AEA console

Server-side tasks

Reporting tasks



New task - "Unnamed"

Reports

- □ Virus actions summary
- □ Actions on Top N viruses
- □ Change of logical disks summary
- □ Top N attacked computers
- □ Top N network attacks
- □ Virus infections summary

- □ Sort by computer name
- □ Sort ascending
- □ Show details
- □ Include machines w/o avast!

Number of records to show:

Virus name mask: *

Computer name mask: *

Group name mask: *

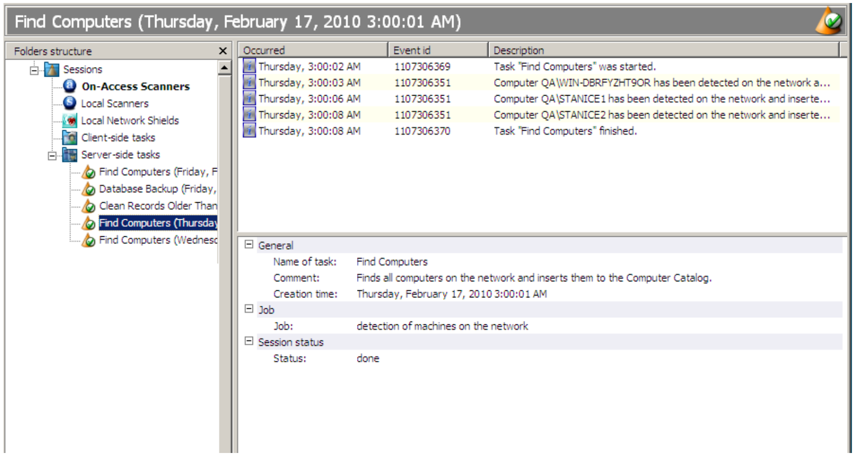
- **Virus Infections Summary**
  - This creates a tabular report that shows all machines on which avast! found a virus during a given time period.
  - This includes information about all viruses, infected files and actions applied to these files, for the computers specified in the reporting task's properties.
  - This report is useful e.g. for finding out which computers are most exposed to viral attacks so that appropriate counter-measures can be taken.

AEA console

SESSIONS

AEA console

Sessions



Find Computers (Thursday, February 17, 2010 3:00:01 AM)

Occurred	Event id	Description
Thursday, 3:00:02 AM	1107306369	Task "Find Computers" was started.
Thursday, 3:00:03 AM	1107306351	Computer QA\WIN-DBRFYZHT9OR has been detected on the network a...
Thursday, 3:00:06 AM	1107306351	Computer QA\STANICE1 has been detected on the network and inserte...
Thursday, 3:00:08 AM	1107306351	Computer QA\STANICE2 has been detected on the network and inserte...
Thursday, 3:00:08 AM	1107306370	Task "Find Computers" finished.

⊟ General

Name of task: Find Computers

Comment: Finds all computers on the network and inserts them to the Computer Catalog.

Creation time: Thursday, February 17, 2010 3:00:01 AM

⊟ Job

Job: detection of machines on the network

⊟ Session status

Status: done

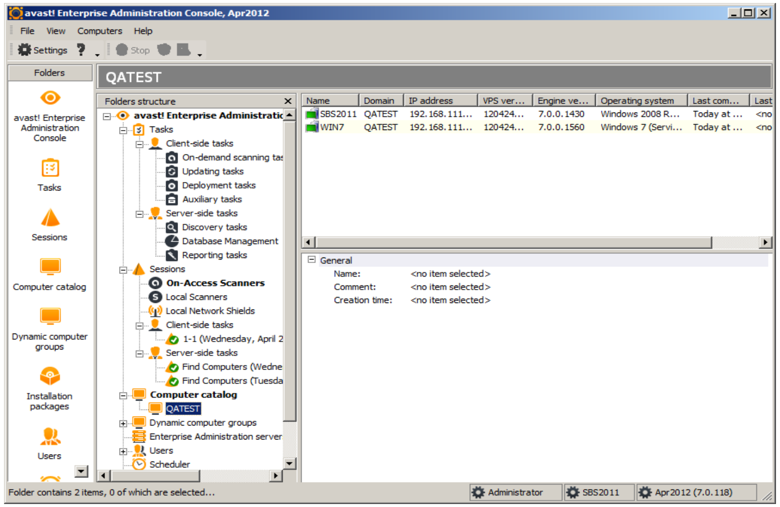
- Each time a task is run, a new session is created by the avast! software.
- A session is an object that defines a particular instance of a run task. For example, if task X is started five times, five different sessions are created, where each contains the results of the specific task.
- For some tasks, the session contains only basic status data; for others, it can hold many results (such as results of on-demand scanning) or even binary data (e.g., reports).
- There are also two special predefined sessions.
  - The “On-Access Scanners” session contains all the results of all on-access scanners on the network.
  - The “Local Scanners” session contains the results of all local on-demand scans, that is, those that were not invoked on behalf of an AEA scanning task.

AEA console

COMPUTER CATALOG

AEA console

Computer catalog



Name	Domain	IP address	VPS ver…	Engine ve…	Operating system	Last com…	Last
SBS2011	QATEST	192.168.111…	120424…	7.0.0.1430	Windows 2008 R…	Today at …	<no
WIN7	QATEST	192.168.111…	120424…	7.0.0.1560	Windows 7 (Servi…	Today at …	<no

General

Name: <no item selected>
Comment: <no item selected>
Creation time: <no item selected>

Folder contains 2 items, 0 of which are selected…

Administrator | SBS2011 | Apr2012 (7.0.118)

- The Computers folder (called “Computer Catalog” in the console) works as a container for all managed machines on the network.

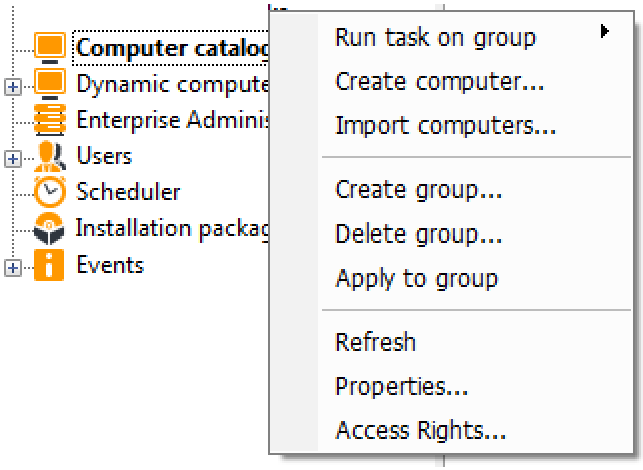
- It has a tree structure, so you can create as many subfolders as you wish, to achieve optimal organization. There can be no duplicates; every computer has its fixed position in the tree.

- To rearrange the computers in the structure, you can use the drag ’n’ drop method.

- The Computer Catalog is where all the security policies are set: Each folder can have a different set of policies. By default, the policies are inherited from the root to the leaves, but they can be overridden at any level. Therefore it is important to pay careful attention when building the tree.

AEA console

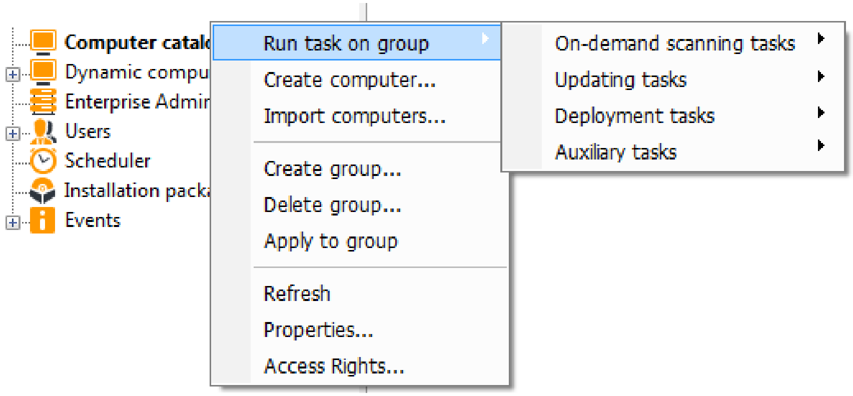
Computer catalog



- Right clicking on a specific computer group allows you to:
  - Run a task on a specific group
  - Create a computer
  - Import computers
  - Create/Delete a group
  - Apply changes to a group
  - Refresh the GUI
  - Change group Properties
  - Change Access rights

AEA console

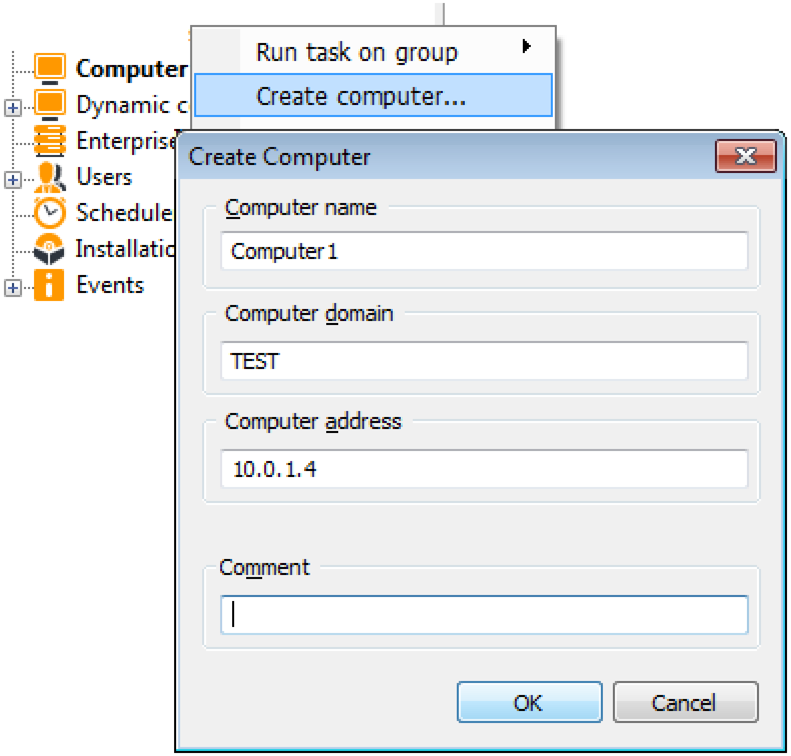
Computer catalog



- The “Run task on group” option allows you to run any of the following:
  - On demand scanning tasks
  - Updating tasks
  - Deployment tasks
  - Auxiliary tasks

AEA console

Computer catalog



Computer name: Computer1

Computer domain: TEST

Computer address: 10.0.1.4

Comment:

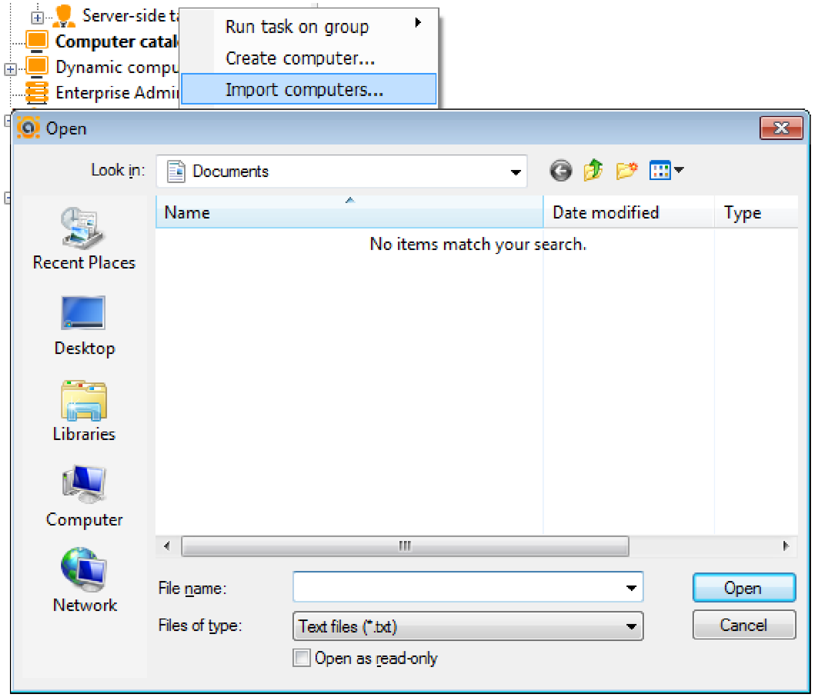
- In some cases, you may not be able to use the Discovery Task (perhaps because your network doesn't run ActiveDirectory or the computer browser does not work).

- Then you should take advantage of AEA's ability to create a computer manually via the right click feature on a specific computer group

- You can create a computer by inserting basic information such as:
  - Computer name
  - Computer domain
  - Computer IP address

AEA console

Computer catalog



No items match your search.

Text files (*.txt)

□ Open as read-only

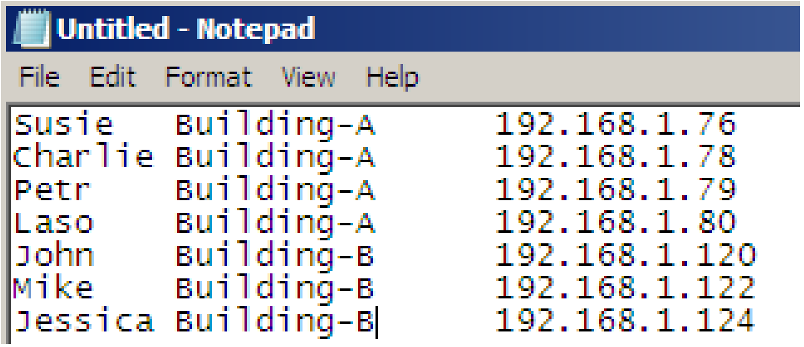
- In some cases, you may not be able to use the Discovery Task (perhaps because your network doesn’t run ActiveDirectory or the computer browser does not work).

- Then you should take advantage of AEA’s ability to import the machine list from an external data source.

- You can import the list of computers to be placed in the Catalog by means of a simple text file. The text file has a very simple structure.
  – see the next page

AEA console

Computer catalog

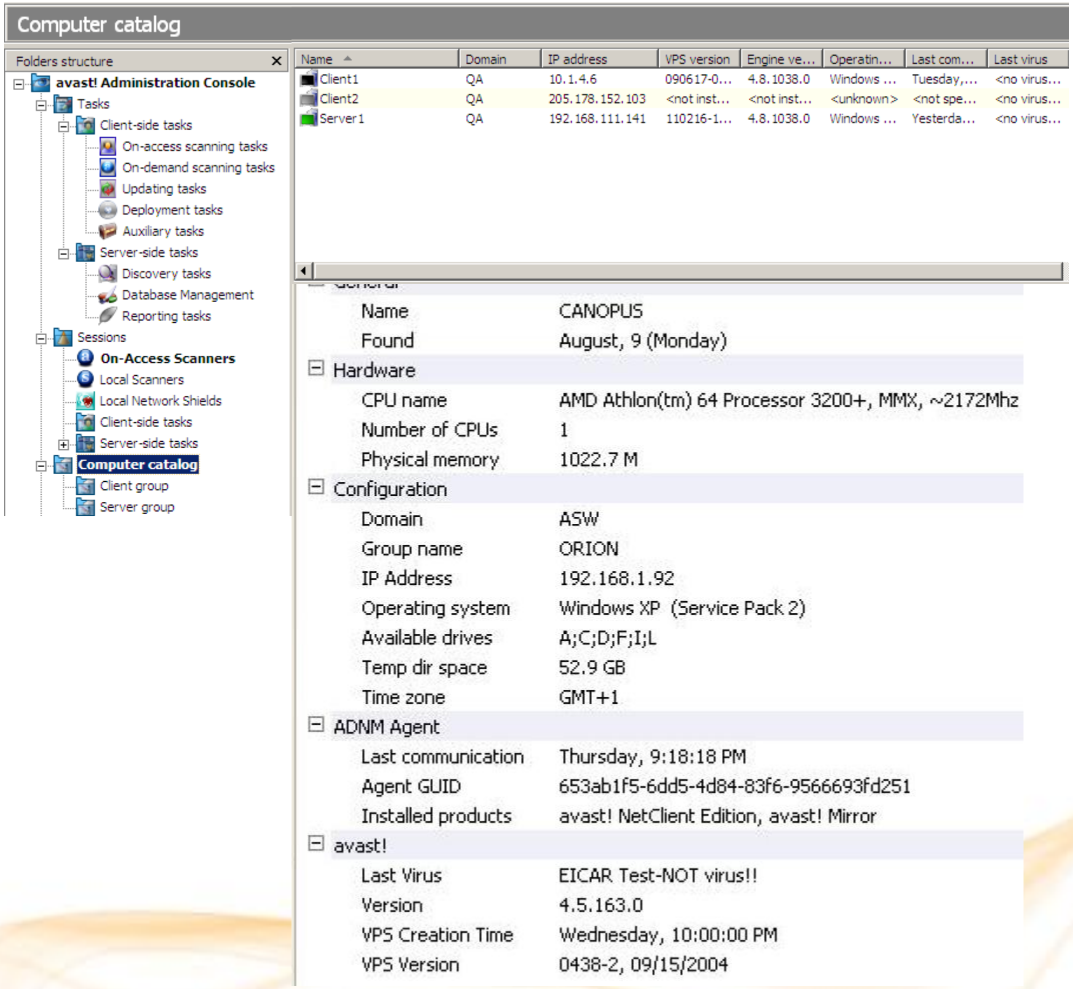


```
Susie	Building-A		192.168.1.76
Charlie	Building-A		192.168.1.78
Petr	Building-A		192.168.1.79
Laso	Building-A		192.168.1.80
John	Building-B		192.168.1.120
Mike	Building-B		192.168.1.122
Jessica	Building-B		192.168.1.124
```

- Each line represents one computer and has three columns. The columns are separated by a single tab character.
  - The first column specifies the name of the computer, as it should appear in the Catalog.
  - The second column represents the name of the domain or workgroup that the computer belongs to.
  - The third row is interpreted as the computer's IP address and should be in the form xx.xx.xx.xx where xx is a number between 0 and 255.
- After the text file is ready (either by compiling it by hand in a text editor or by exporting it from an external application), all you need to do is import it to the AEA.
- To do this, navigate to any folder in the Computer Catalog and select the Import Computers... menu option.

AEA console

Computer catalog



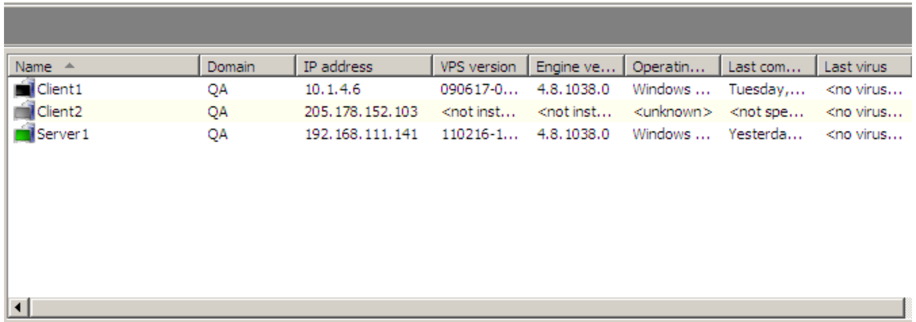
Name	Domain	IP address	VPS version	Engine ve...	Operatin...	Last com...	Last virus
Client1	QA	10.1.4.6	090617-0...	4.8.1038.0	Windows ...	Tuesday,...	<no virus...
Client2	QA	205.178.152.103	<not inst...	<not inst...	<unknown>	<not spe...	<no virus...
Server1	QA	192.168.111.141	110216-1...	4.8.1038.0	Windows ...	Yesterda...	<no virus...

Name	CANOPUS
Found	August, 9 (Monday)
⊟ Hardware	
CPU name	AMD Athlon(tm) 64 Processor 3200+, MMX, ~2172Mhz
Number of CPUs	1
Physical memory	1022.7 M
⊟ Configuration	
Domain	ASW
Group name	ORION
IP Address	192.168.1.92
Operating system	Windows XP (Service Pack 2)
Available drives	A;C;D;F;I;L
Temp dir space	52.9 GB
Time zone	GMT+1
⊟ ADNM Agent	
Last communication	Thursday, 9:18:18 PM
Agent GUID	653ab1f5-6dd5-4d84-83f6-9566693fd251
Installed products	avast! NetClient Edition, avast! Mirror
⊟ avast!	
Last Virus	EICAR Test-NOT virus!!
Version	4.5.163.0
VPS Creation Time	Wednesday, 10:00:00 PM
VPS Version	0438-2, 09/15/2004

- The AEA monitors a number of details about each and every managed machine, related both to avast! and to the system configuration.
- This information can be used by the administrator to analyze problems, and also to get a better idea of the overall network structure.
- The stored information includes the computer name and the domain/workgroup, IP address, CPU type, installed RAM, operating system and service pack level, time zone, disk space in the TEMP directory, and other data.
- It is refreshed upon each contact with the client.

AEA console

Computer catalog



Name	Domain	IP address	VPS version	Engine ve...	Operatin...	Last com...	Last virus
Client1	QA	10.1.4.6	090617-0...	4.8.1038.0	Windows ...	Tuesday,...	<no virus...
Client2	QA	205.178.152.103	<not inst...	<not inst...	<unknown>	<not spe...	<no virus...
Server1	QA	192.168.111.141	110216-1...	4.8.1038.0	Windows ...	Yesterda...	<no virus...

The console also distinguishes individual computers in the Catalog by using icons. Each computer has one of the following icons:

Green computer

– This icon indicates a healthy computer state. The computer has not been recently infected with viruses, and it is switched on and actively communicating with the EAS.

Red computer

– This icon indicates an infection. A virus has been found on the machine recently. The computer keeps the “red” state until it is manually marked as clean by an Administrator (by using the “Mark computer as clean” context menu option).

Gray computer

– This icon indicates that there is no managed product installed on the machine or the machine has not yet communicated with the server. This includes, but is not limited to, newly discovered computers.

Black computer

– This icon indicates that the computer hasn’t communicated with the EAS recently (but still has a managed product installed). The time period after which computers are marked as black can be customized in the global EAS settings; the default value is 20 minutes. The fact that a computer is marked black doesn’t necessarily mean anything bad. E.g. computers that are turned off will have this icon. It is possible to verify the offline status of such computers by right-clicking them and selecting the "Verify offline status„ command.

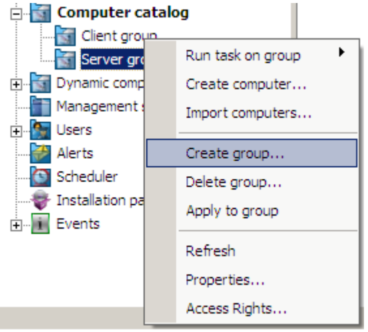
Computer with a key symbol

– This icon indicates that the number of licenses in your license file is not sufficient. That is, the Catalog contains a larger number of computers than the AEA license permits. The EAS chooses the excess machines randomly but prefers those that don't have any managed product installed or have not yet communicated with the server, i.e., those that would be otherwise grayed-out.

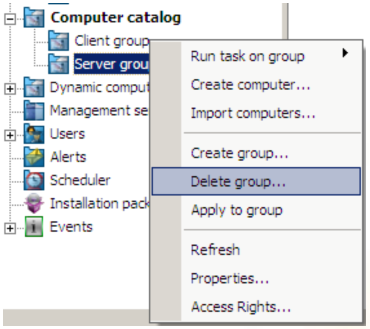
AEA console

Computer catalog

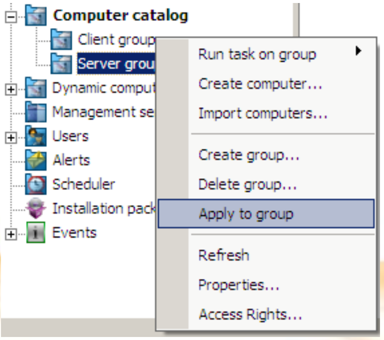
If you want to create a computer group/sub-group just right click on the Computer catalog or on the specific Computer group.



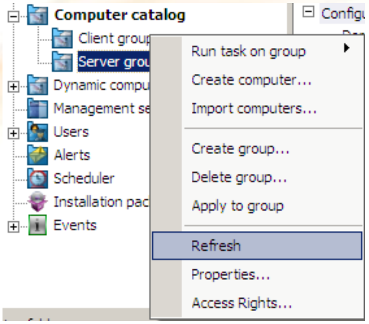
If you need to delete a whole computer group, make sure you didn‘t leave any important computer in the list, otherwise everything will be deleted.



- Whenever you need to apply any changes to a specific computer or computer group you MUST click the “Apply to group” or “Apply to computer” button! Otherwise none of the changes will be applied!

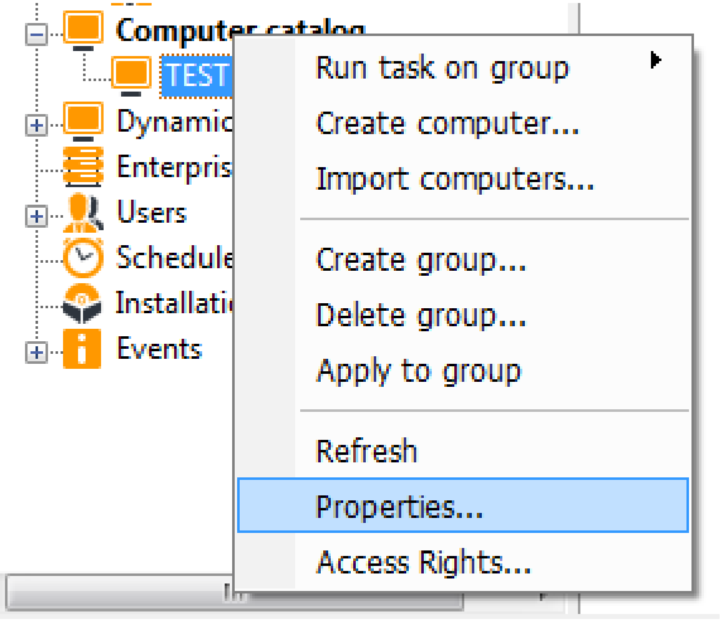


- Refreshing the GUI could help if changes have been made but are not displayed. If the Refresh feature does not help, restart the AEA console.



AEA console

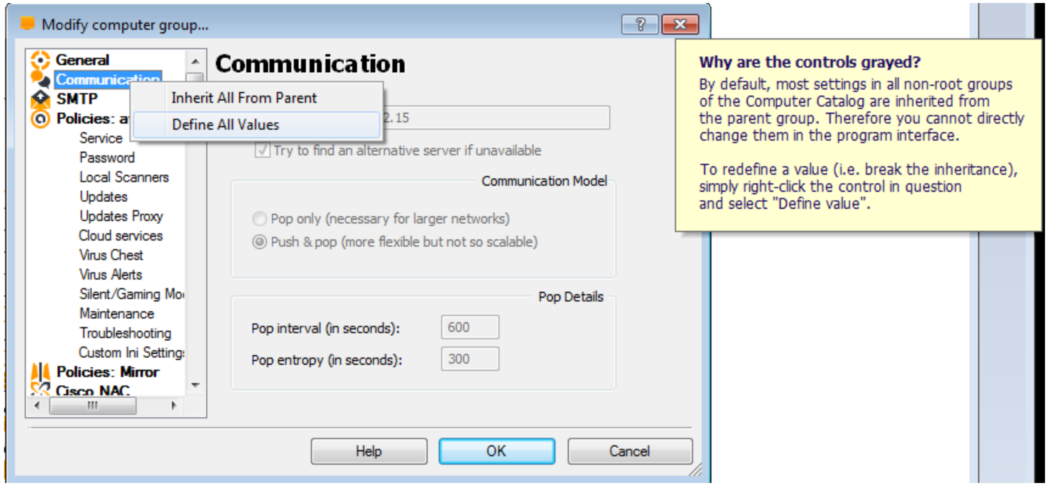
Computer catalog



- The Computer Catalog is where all the security policies are set:
  - Each folder can have a different set of policies.
  - By default, the policies are inherited from the root to the leaves, but they can be overridden at any level.
  - Therefore it is important to pay careful attention when building the tree.

AEA console

Computer catalog



Communication

2.15

☑ Try to find an alternative server if unavailable

Communication Model

○ Pop only (necessary for larger networks)

● Push & pop (more flexible but not so scalable)

Pop Details

Pop interval (in seconds): 600

Pop entropy (in seconds): 300

Why are the controls grayed?

By default, most settings in all non-root groups of the Computer Catalog are inherited from the parent group. Therefore you cannot directly change them in the program interface.

To redefine a value (i.e. break the inheritance), simply right-click the control in question and select "Define value".

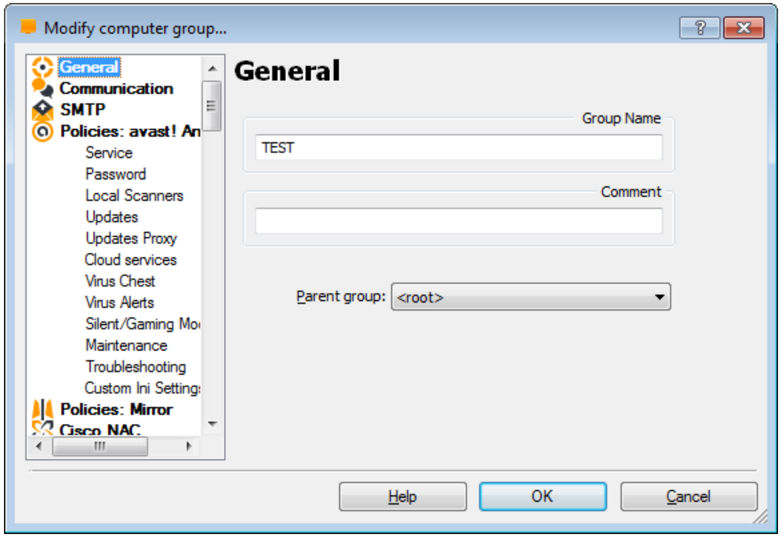
- An undefined policy value is indicated by the appropriate control being greyed (dimmed) in the Group Properties dialog.

- Since no policies are overridden by default, all controls in the properties of all computer groups except the root are greyed.

- To define a policy, right-click the control and choose “Define value.” The control becomes enabled and can be used to specify a value.
- If you later decide to undefine the policy, right-click it again and choose “Inherit from parent.”

AEA console

Computer catalog



General

Group Name: TEST

Comment:

Parent group: <root>

- The Properties dialog contains the policy settings for all supported managed products, whether they are actually installed on the client machines or not.

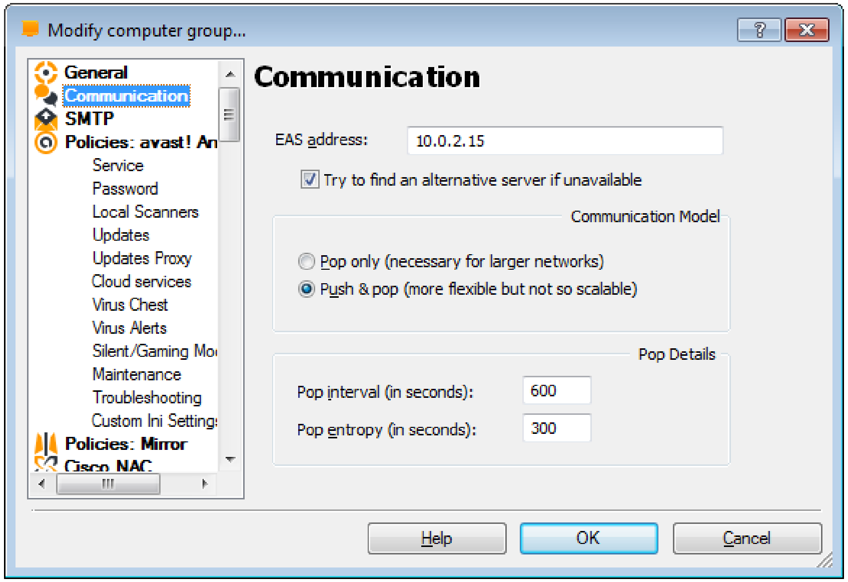
- If a machine has only the Mirror product installed (the Mirror is also considered a managed product), the avast! Antivirus policy settings will not be effective for that machine, but the Mirror policy settings will.

- Most of the policies are set directly as properties of the Computer Group objects.

- Note:
  - An important exception is the case of on-access scanning tasks, i.e., the resident-protection settings. These are only stored in the group properties as a reference to an on-access scanning task object.
  - If you want to redefine the on-access scanning settings for a given machine, you first need to create a new on-access task and then assign it to the proper group. Therefore, individual on-access settings cannot be inherited in the Catalog tree.

AEA console

Computer catalog



Communication

EAS address: 10.0.2.15

☑ Try to find an alternative server if unavailable

Communication Model

○ Pop only (necessary for larger networks)

● Push & pop (more flexible but not so scalable)

Pop Details

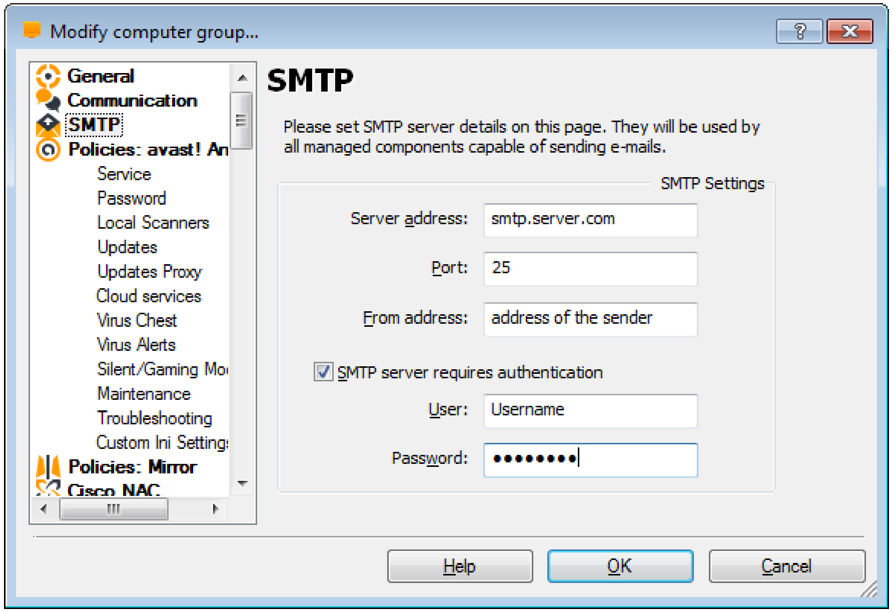
Pop interval (in seconds): 600

Pop entropy (in seconds): 300

- **EAS address**
  - Change the EAS address (when moving to a new/another server) in the Properties window of all relevant groups in the Computer Catalog, and wait for a pop timeout to occur on the client machines (5-15 minutes by default, unless changed in the global EAS settings).
  - Verify that the clients on the network are moving to the new server; you should see that the Last Connected field keeps getting updated.
- **Communication models**
  - Pop only
    - The server never tries to contact the client computer (e.g. for status verification after a task was started)
  - Push and pop
    - The server tries to contact the client computer (task status verification is POP model only)
- **Pop details**
  - Pop interval
    - The average interval between client computers connecting with the server (to spread the client requests over a period of time)
  - Pop entropy
    - A random value which is added to the Pop interval. The actual interval between any two client computers connecting with the server is given by:
    - Pop_interval - pop_entropy ≤ actual interval ≤ pop_interval + pop_entropy >

AEA console

Computer catalog



Modify computer group...

SMTP

Please set SMTP server details on this page. They will be used by all managed components capable of sending e-mails.

SMTP Settings

Server address: smtp.server.com

Port: 25

From address: address of the sender

☑ SMTP server requires authentication

User: Username

Password: ••••••••

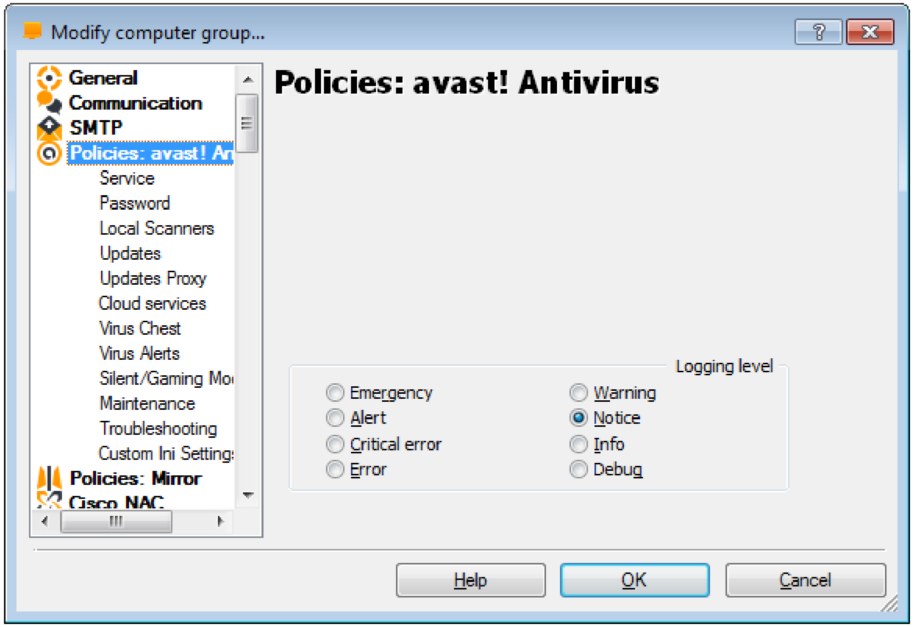
- On this page, you can specify your SMTP server parameters, which avast! uses to send e-mail messages, especially when:
  - Sending warning messages when a virus has been found.
  - Sending files from the Chest to AVAST Software.
  - Sending avast! crash reports to AVAST Software.

- **Server address**
  - the address of the outgoing e-mail server (e.g. smtp.server.com or 192.168.1.25).
- **Port**
  - the port number (the default is 25).
- **From address**
  - address of the sender ("From").

- **Note:**
  - If the **SMTP settings** above (SMTP settings under avast! Program settings or/and SMTP settings under Computer catalog properties) are not specified, NONE of the reported alerts will be sent to the Administrator‘s email!
  - Remember that all settings under Computer catalog must be **Applied** first! They must be “Applied to group” or to a specifiec computer! Otherwise NONE of those settings will be saved on the client computer(s).

AEA console

Computer catalog



Policies: avast! Antivirus

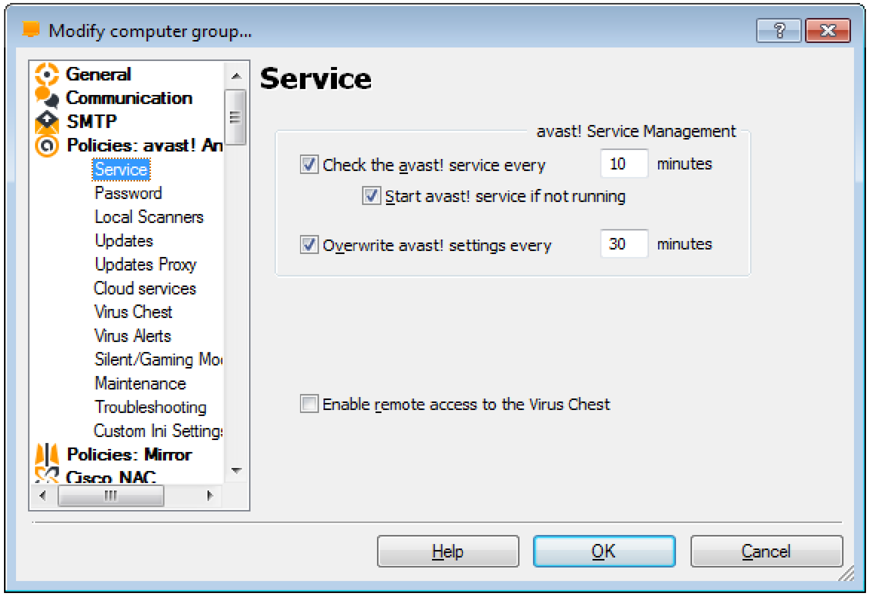
Logging level

○ Emergency	○ Warning
○ Alert	● Notice
○ Critical error	○ Info
○ Error	○ Debug

- **Logging levels**
  - Emergency/Alert/Critical error/Error
  - Warning/Notice/Info/Debug

AEA console

Computer catalog



Service

avast! Service Management

☑ Check the avast! service every 10 minutes

☑ Start avast! service if not running

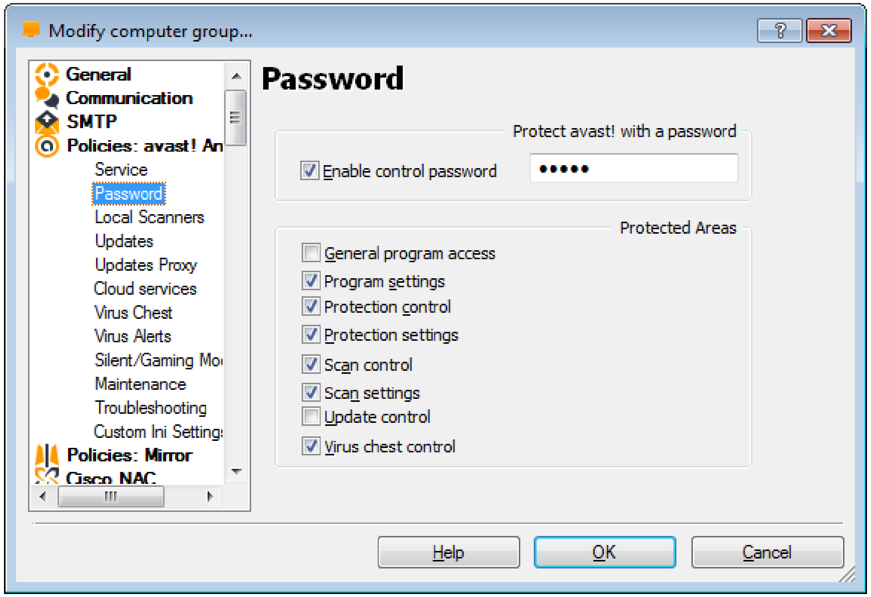
☑ Overwrite avast! settings every 30 minutes

☐ Enable remote access to the Virus Chest

- avast! Service management
  - – Check the avast! service every XX minutes
    - Start avast! service if not running
  - – Overwrite avast! settings every XX minutes
- Enable remote access to the virus chest

AEA console

Computer catalog



Modify computer group...

Password

Protect avast! with a password

☑ Enable control password •••••

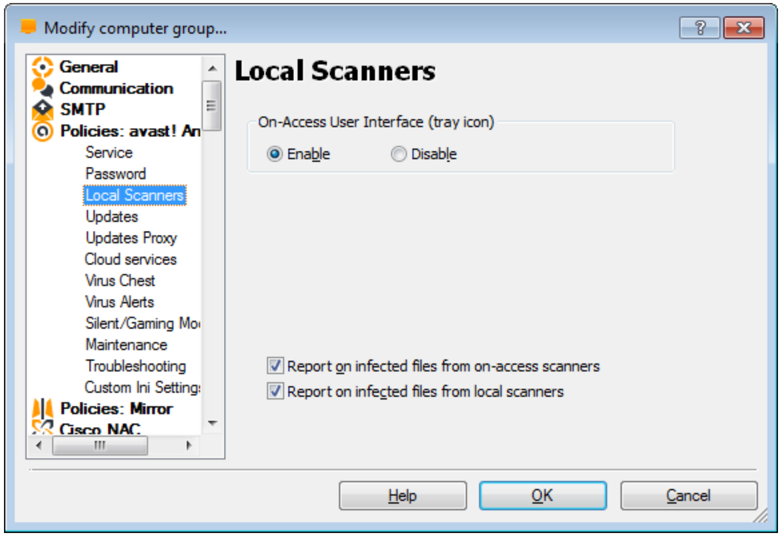
Protected Areas

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

- avast! Password
  - Enable control password
    - Password used to open/modify the avast! GUI on the client machines
    - Specific Protected Areas can be selected from the list

AEA console

Computer catalog


Modify computer group...

Local Scanners

On-Access User Interface (tray icon)

● Enable ○ Disable

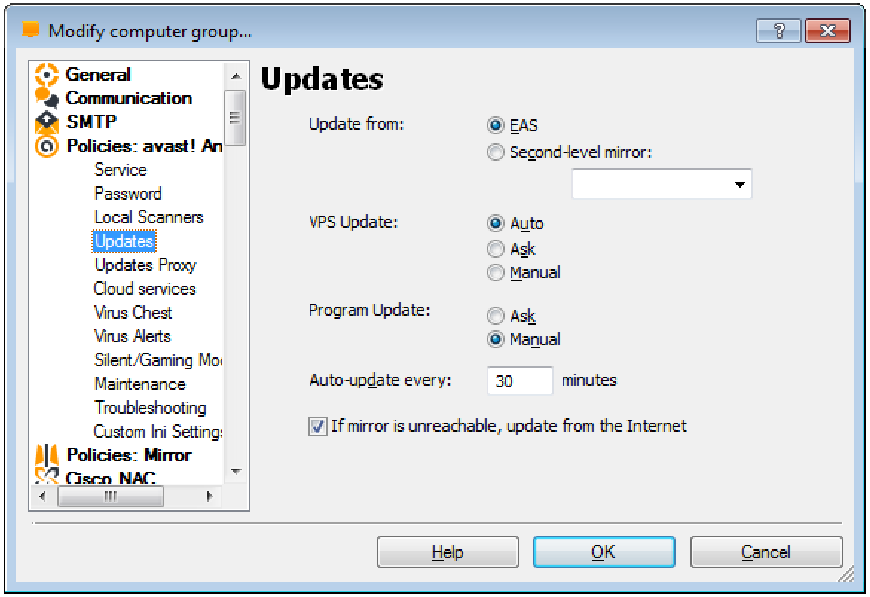
☑ Report on infected files from on-access scanners

☑ Report on infected files from local scanners

- **On-access user interface (tray icon)**
  - Allows the user to interact with the avast! system tray icon (if enabled)
- Report on infected files from on-access scanners
- Report on infected files from local scanners

AEA console

Computer catalog



Modify computer group...

Updates

Update from: ● EAS ○ Second-level mirror:

VPS Update: ● Auto ○ Ask ○ Manual

Program Update: ○ Ask ● Manual

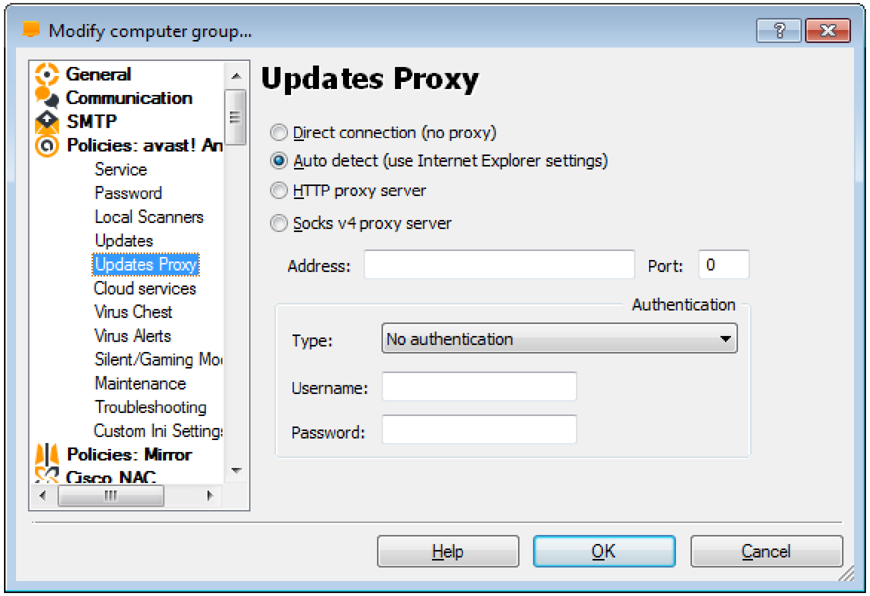
Auto-update every: 30 minutes

☑ If mirror is unreachable, update from the Internet

- **Update from**
  - EAS
  - Second-level mirror
- **VPS update**
  - Auto/Ask/Manual
- **Program update**
  - Ask/Manual
- **Auto update every**
  - XX minutes
- If mirror is unreachable, update from the internet

AEA console

Computer catalog



Updates Proxy

○ Direct connection (no proxy)
● Auto detect (use Internet Explorer settings)
○ HTTP proxy server
○ Socks v4 proxy server

Address: Port: 0

Authentication

Type: No authentication

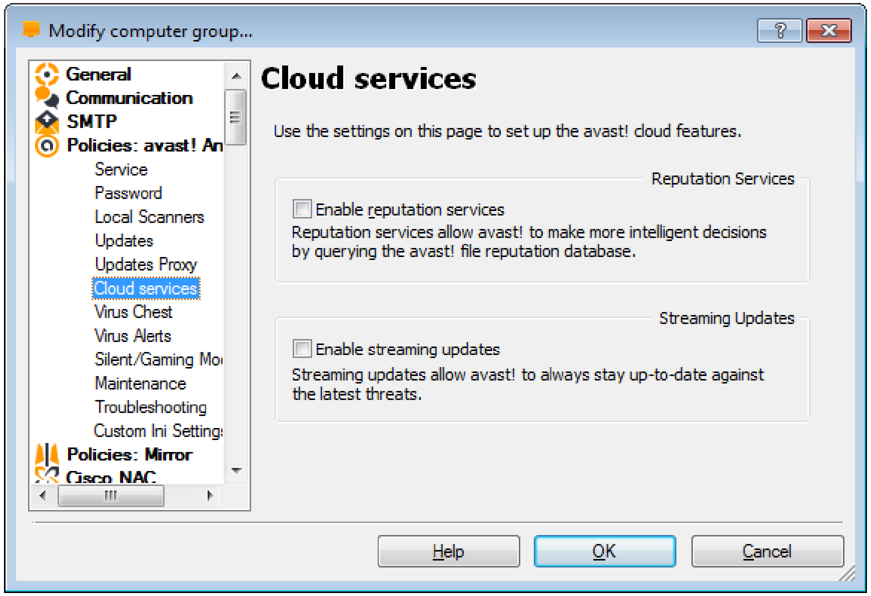
Username:

Password:

- The proxy settings on this page are important when avast! needs to access the internet, for example, when carrying out updates.
- If you connect directly to the internet (i.e. not through a proxy), select "Direct connection (no proxy)". Note: dial-up connections do not use a proxy.
- If you are not sure whether you use a proxy server, or which proxy server you use, select "auto detect" or 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:
  - Type - HTTP or SOCK4
  - Address - Enter the address of your proxy server
  - Port - Enter the port your proxy server uses
- Authentication type - specify here whether the proxy server requires authentication and if so, the type of authentication
  - Username and password -should be entered if required for authentication

AEA console

Computer catalog



Modify computer group...

Cloud services

Use the settings on this page to set up the avast! cloud features.

Reputation Services

□ Enable reputation services

Reputation services allow avast! to make more intelligent decisions by querying the avast! file reputation database.

Streaming Updates

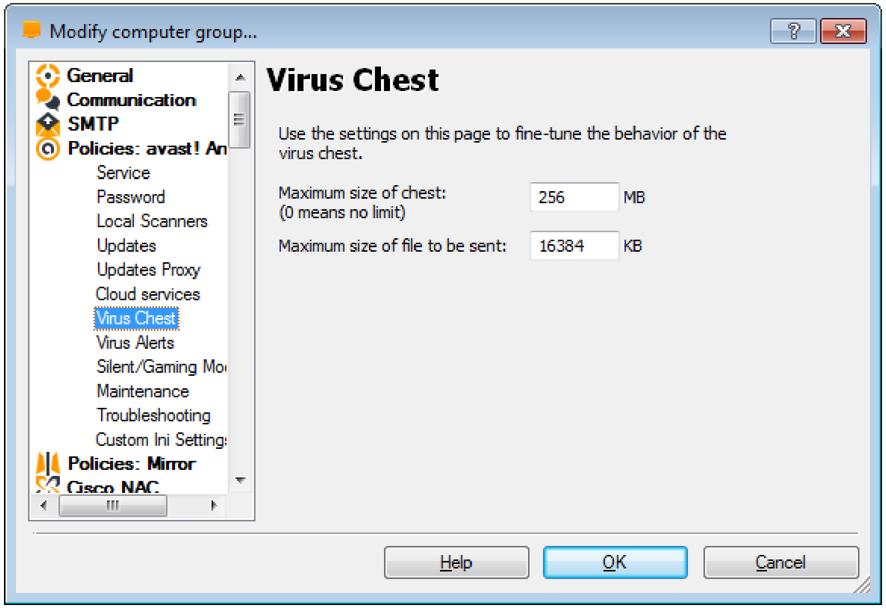
□ Enable streaming updates

Streaming updates allow avast! to always stay up-to-date against the latest threats.

- **Enable reputation services**
  - Reputation services allow avast! to make more intelligent decisions by querying the avast! File reputation database.
- **Enable streaming updates**
  - Streaming updates allow avast! to always stay up-to-date against the latest threats.
- **NOTE:**
  - Internet connection is required!

AEA console

Computer catalog


Modify computer group...

Virus Chest

Use the settings on this page to fine-tune the behavior of the virus chest.

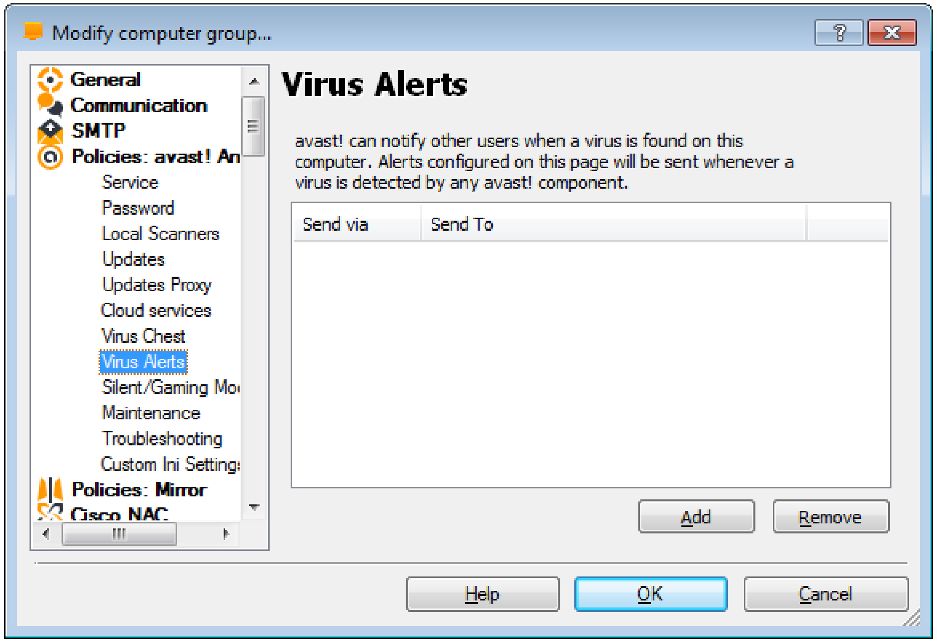
Maximum size of chest: (0 means no limit) 256 MB

Maximum size of file to be sent: 16384 KB

- Here you can specify the maximum permitted size of the virus chest and thus the maximum amount of space it can take up on your computer.
- You can also specify the maximum size of any individual file that is sent to the virus chest.

AEA console

Computer catalog



Virus Alerts

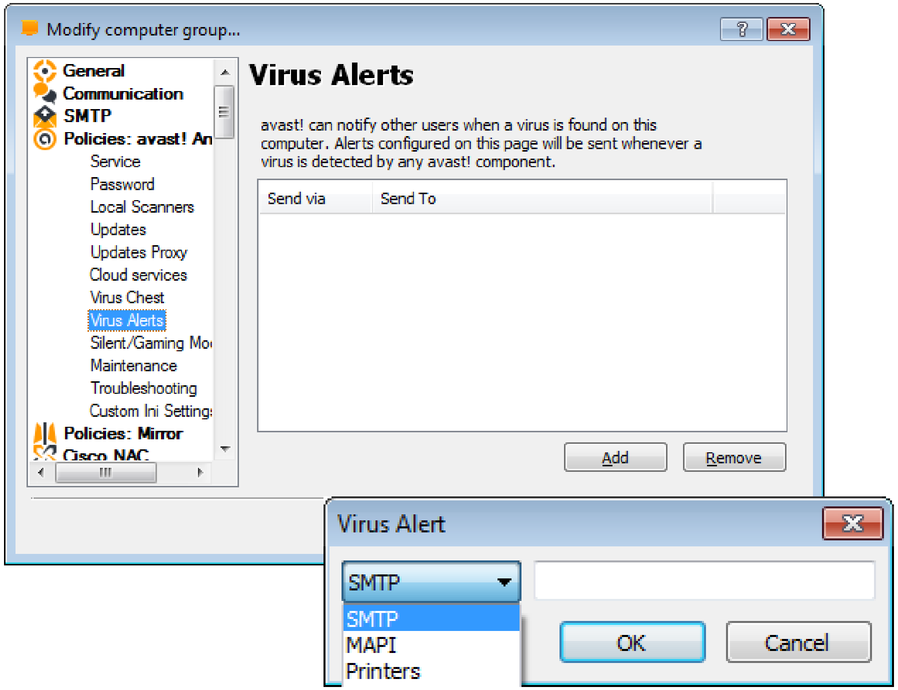
avast! can notify other users when a virus is found on this computer. Alerts configured on this page will be sent whenever a virus is detected by any avast! component.

Send via	Send To

- This is where you can define the alerts (or notifications).
- The alerts can then be assigned to the scanning tasks so that whenever a virus is found, the alert will be used to notify someone about the problem.
- This feature is useful for network administrators who will be notified about the presence of a virus on any computer that they are responsible for, so that they can react quickly.

AEA console

Computer catalog



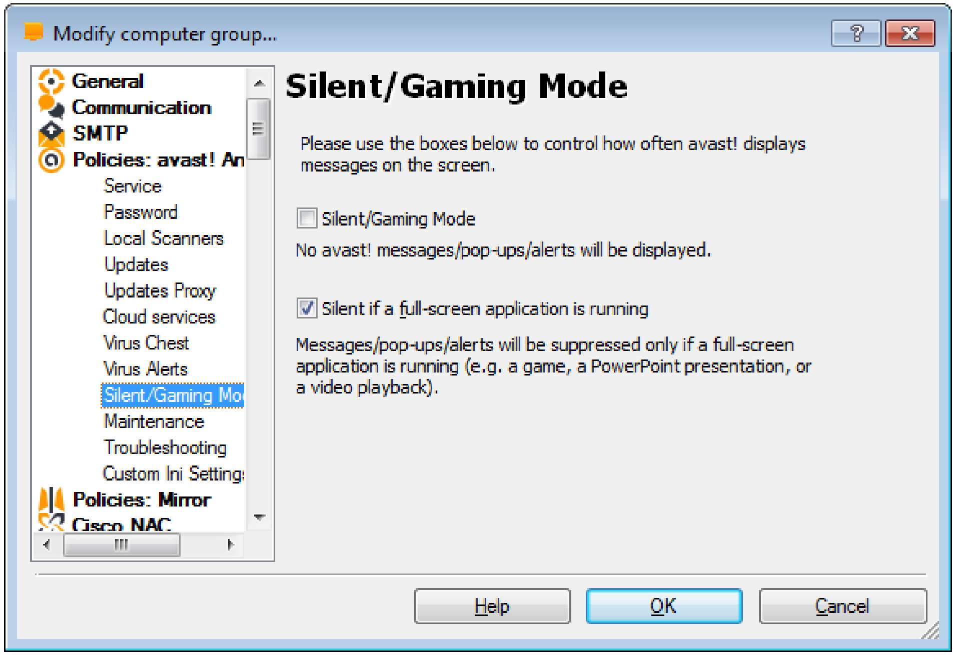
Virus Alerts

avast! can notify other users when a virus is found on this computer. Alerts configured on this page will be sent whenever a virus is detected by any avast! component.

- The alert can be sent in any of the following ways:
- **MAPI**
  - The alert will be sent as an e-mail, using the MAPI protocol. Enter the MAPI profile name, together with the corresponding password to use.
- **WinPopup**
  - The alert will be sent using the net send command. Enter the IP address or the network name of the computer to send the warning to.
- **SMTP**
  - The alert will be sent as an e-mail, using the SMTP protocol. It is necessary to define the SMTP Server, i.e. the mail server the messages will be sent through (e.g. smtp.company.com or 192.168.1.1). Additionally, you have to specify the port that will be used (the standard value is 25). Finally, enter the sender address ("From", i.e. the user address).
- **Note:**
  - Make sure that you also insert the SMTP settings under the Computer catalog properties! If they are not specified, NONE of the reported alerts will be sent to the specified email!

AEA console

Computer catalog



Silent/Gaming Mode

Please use the boxes below to control how often avast! displays messages on the screen.

☐ Silent/Gaming Mode

No avast! messages/pop-ups/alerts will be displayed.

☑ Silent if a full-screen application is running

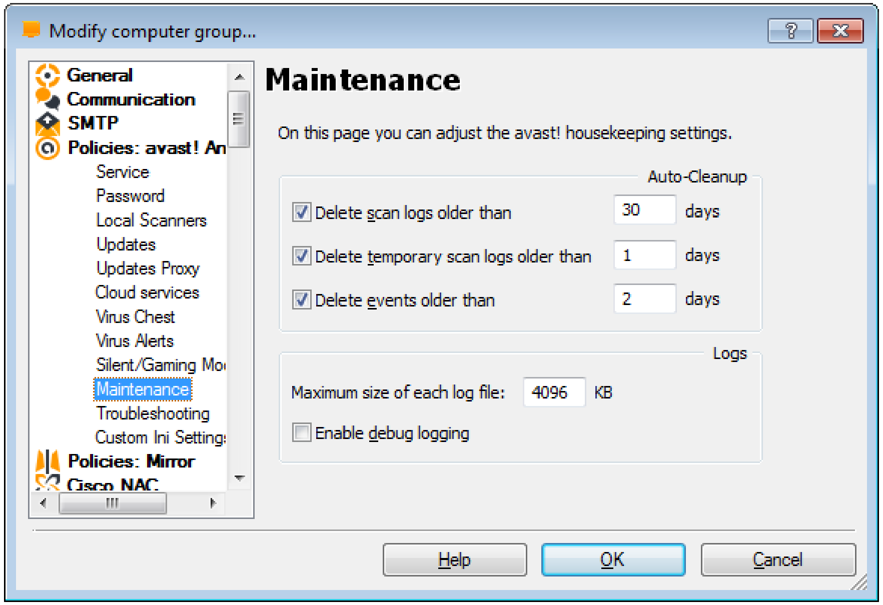
Messages/pop-ups/alerts will be suppressed only if a full-screen application is running (e.g. a game, a PowerPoint presentation, or a video playback).

- At various times while your computer is running, messages may be displayed on your screen e.g. when the virus definitions have been updated, when an incoming email is being scanned etc. This can result in full-screen applications (e.g. games) being interrupted as Windows switches from full-screen mode to normal mode when the message appears.

- On this screen you can specify that messages will never be displayed (**Silent mode**), or will not be displayed if a **full-screen application** is running.

AEA console

Computer catalog



Modify computer group...

Maintenance

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

Auto-Cleanup

☑ Delete scan logs older than 30 days

☑ Delete temporary scan logs older than 1 days

☑ Delete events older than 2 days

Logs

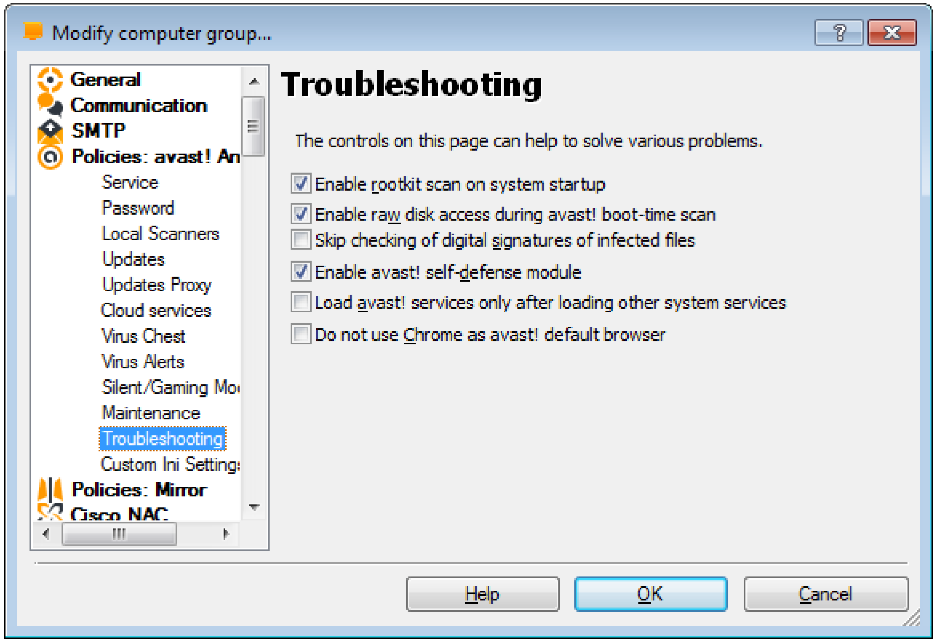
Maximum size of each log file: 4096 KB

☐ Enable debug logging

- On this page you can adjust the avast! Housekeeping settings for Auto-cleanup.
  - Delete scan logs
  - Delete temp. Scan logs older than XX days
  - Delete Events older than XX days
- You can also specify the maximum size of each log
- And select whether you want to enable debug logging

AEA console

Computer catalog



Troubleshooting

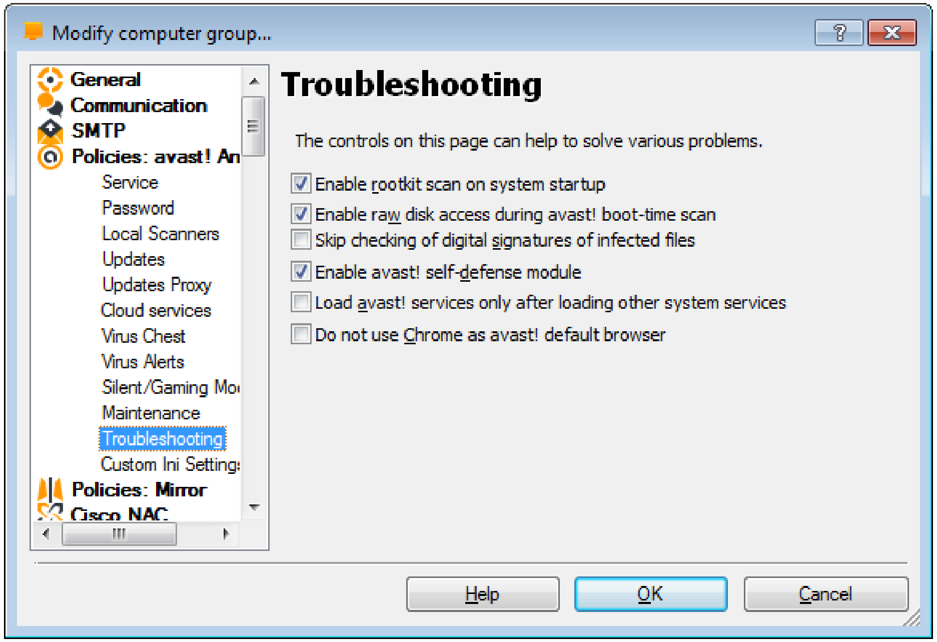
The controls on this page can help to solve various problems.

☑ 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
□ Do not use Chrome as avast! default browser

- 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 whenever your system is restarted.
  - **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.

AEA console

Computer catalog



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
☐ Do not use Chrome as avast! default browser

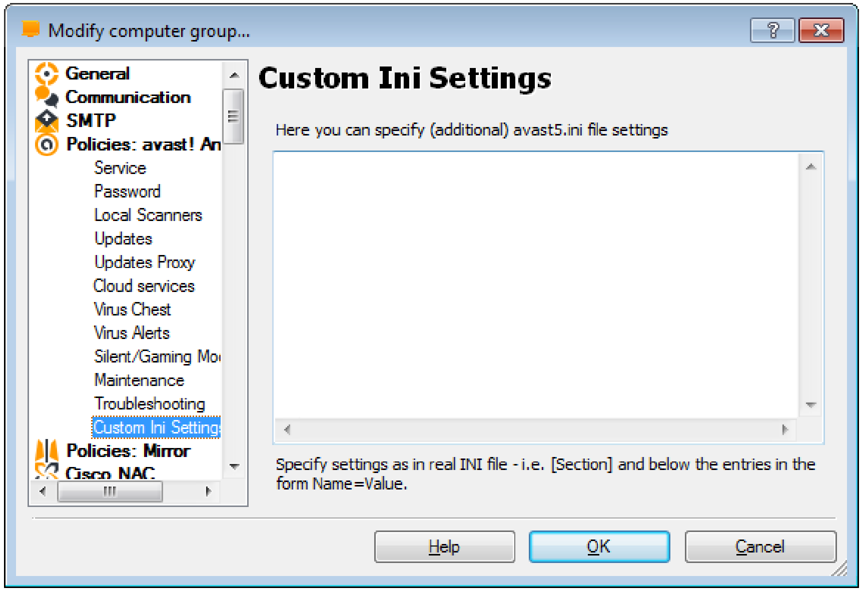
– **Enable avast! self-defense module** - Some viruses deliberately target antivirus software and try to switch it off by deleting or modifying critical files. avast! contains self-defense features that prevent such attacks by blocking the operation.

– **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.

AEA console

Computer catalog



Custom Ini Settings

Here you can specify (additional) avast5.ini file settings

Specify settings as in real INI file - i.e. [Section] and below the entries in the form Name=Value.

- Some settings (policies) of the managed products cannot be directly set through the Computer Group's properties because there are no GUI controls defined for them.

- These mainly include settings that are less important to most users. The majority of these settings are changed by editing the .ini files on the managed client computers.

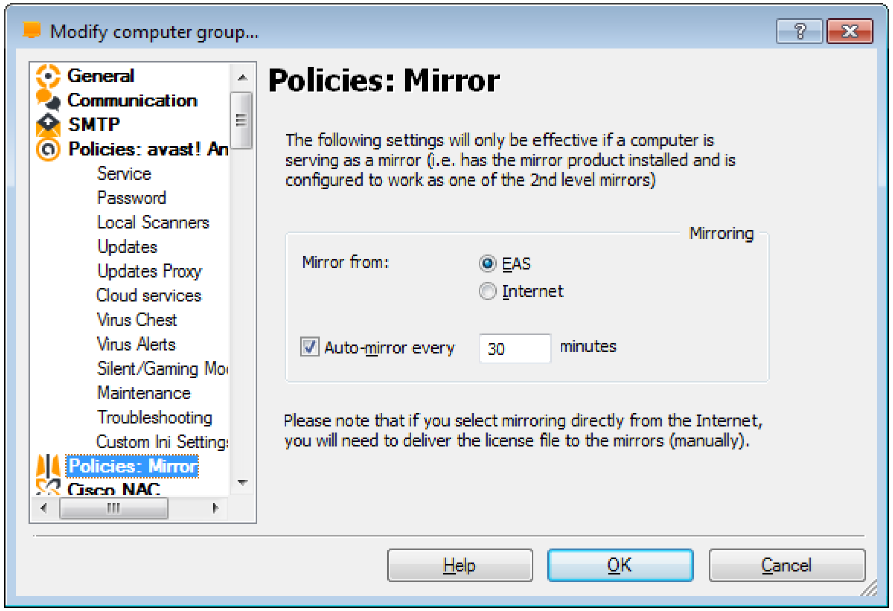
- AEA makes setting these properties much easier with remote batch editing of client .ini files. In fact, the INI file entries become part of the Computer Group properties (and, as such, use features like inheritance).

- The syntax is the same as in the case of real INI files. Section names are included in brackets, and entries are specified in the form entry=value (each entry on a separate line).

- Note:
  - Existing controls such as SMTP settings etc.. can also be changed via Custom.ini features.
  - **Don't forget to use the "Apply to" feature! Otherwise none of the changes/settings will be applied to the selected computer or computer group.**

AEA console

Computer catalog



Policies: Mirror

The following settings will only be effective if a computer is serving as a mirror (i.e. has the mirror product installed and is configured to work as one of the 2nd level mirrors)

Mirroring

Mirror from: ● EAS ○ Internet

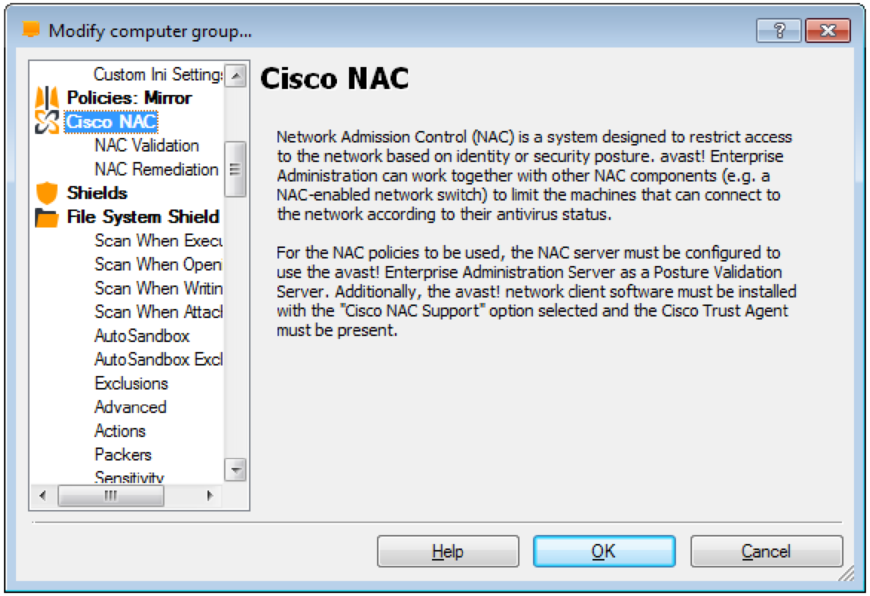
☑ Auto-mirror every 30 minutes

Please note that if you select mirroring directly from the Internet, you will need to deliver the license file to the mirrors (manually).

- The following settings will only be effective if a computer is serving as a mirror (i.e. has the mirror installed and configured to work as one of the 2nd level mirrors).
- **Mirroring**
  - From EMS
  - From Internet
- **Auto-mirror every**
  - XX minutes

AEA console

Computer catalog



Cisco NAC

Network Admission Control (NAC) is a system designed to restrict access to the network based on identity or security posture. avast! Enterprise Administration can work together with other NAC components (e.g. a NAC-enabled network switch) to limit the machines that can connect to the network according to their antivirus status.

For the NAC policies to be used, the NAC server must be configured to use the avast! Enterprise Administration Server as a Posture Validation Server. Additionally, the avast! network client software must be installed with the "Cisco NAC Support" option selected and the Cisco Trust Agent must be present.

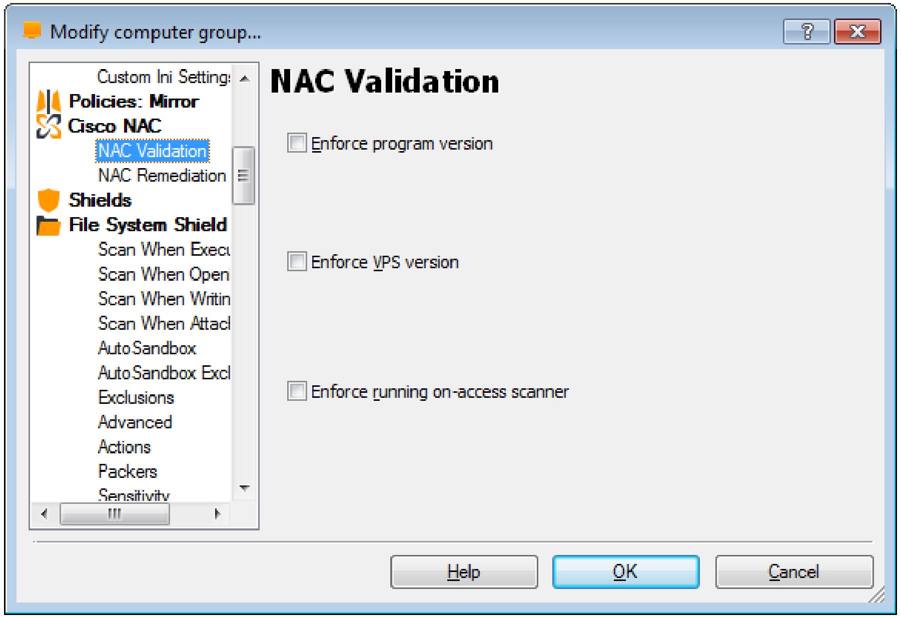
- NAC is a technology developed by Cisco Systems that is designed to enforce security policy compliance on computers connecting to the network. NAC can limit network access when a computer fails to meet certain criteria.
- AEA integrates with NAC to proactively protect against security threats such as viruses and worms before they are introduced into your network.

- Components of a network using Cisco NAC are:
  - NAC-enabled network access device (NAD)
  - the Cisco Secure Access Control Server (ACS)
  - avast! network client with posture plugin (PP) and the Cisco Trust Agent (CTA)
  - avast! Enterprise server (EAS) with posture validation server (PVS)

- When a computer attempts to connect to the network a NAC-enabled NAD detects it and contacts the ACS. The ACS then requests posture credentials from the CTA running on the computer. The CTA asks the avast! PP for the antivirus status (e.g. version) and sends the posture to the ACS. The ACS forwards the credentials to the avast! PVS, which validates them according to the requirements defined by the administrator. The PVS returns the results to the ACS, which maps them to a network authorization in the network access profile. The attributes from the profile are sent to the NAD for enforcement on the computer. The computer can e.g. be granted full access, limited access (quarantined) or denied. If the computer was not fully compliant with the requirements, it can be sent actions that should be performed, to automatically remedy its status (e.g. update). Consult Cisco documentation for more details on the NAC system and its individual components. For configuration of NAC with ACS 4.0, CTA 2.0 and various Cisco NADs, refer to the "NAC Framework Configuration Guide“

AEA console

Computer catalog



Modify computer group...

NAC Validation

□ Enforce program version

□ Enforce VPS version

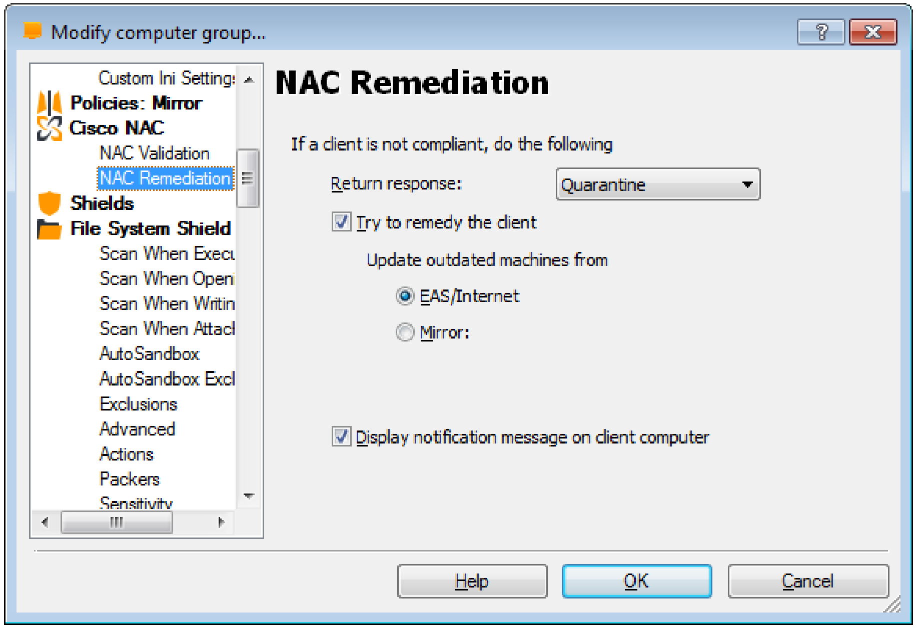
□ Enforce running on-access scanner

- The NAC Validation page defines the requirements for the status of avast! antivirus on computers that are connected to your network.
- You can enforce:
- **Program version**
  - The program version can be specified as an exact version number or you can enforce the latest version that is downloaded to your EAS mirror
- **Virus database (VPS) version**
  - The VPS version can be specified as an exact version number or as the latest available VPS
- **Active on-access protection**

- If the validated computer meets all the specified requirements -> avast! PVS returns status value “Healthy”.
- If any of the requirements are not met -> avast! PVS takes the actions specified on the NAC Remediation page.
  - You can define what status value will be returned (Checkup, Quarantine or Infected) and whether avast! should try to remedy the situation.

AEA console

Computer catalog



Modify computer group...

NAC Remediation

If a client is not compliant, do the following

Return response: Quarantine

☑ Try to remedy the client

Update outdated machines from

● EAS/Internet

○ Mirror:

☑ Display notification message on client computer

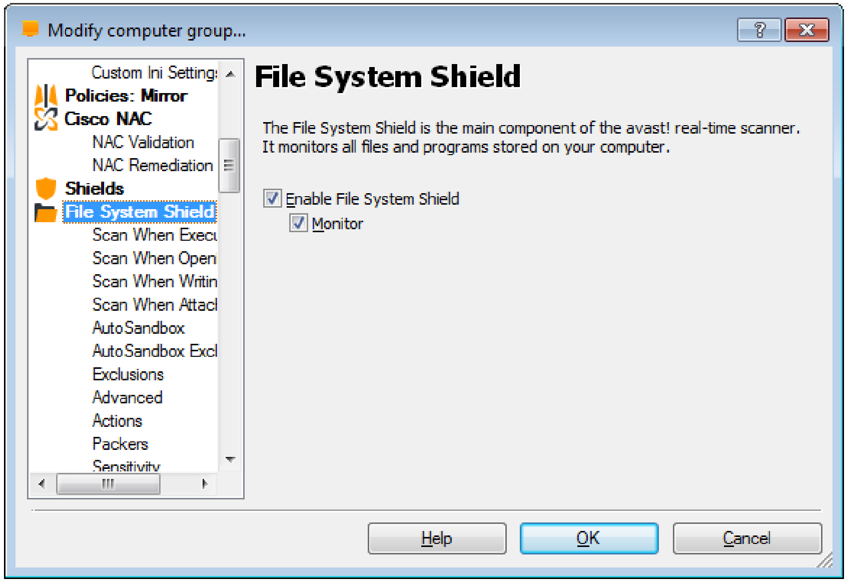
- The remediation action will be delivered to the validated computer where avast! will try to carry it out.
- Remediation means updating, in the case of an outdated avast! program or VPS, or starting the on-access scanner if it was not active.
- You can optionally specify a mirror from which the update will be downloaded. This can be useful if the validated computer was quarantined and cannot access the EAS mirror.
- If you select the option to display a notification message on the client computer, the user will see a pop up message in the bottom right corner of the screen saying that avast! is taking action to satisfy the policies defined by the network administrator and also if the remediation action was successful or not.

FILE SYSTEM SHIELD

AEA console

Computer catalog

File System shield



Modify computer group...

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.

☑ Enable File System Shield

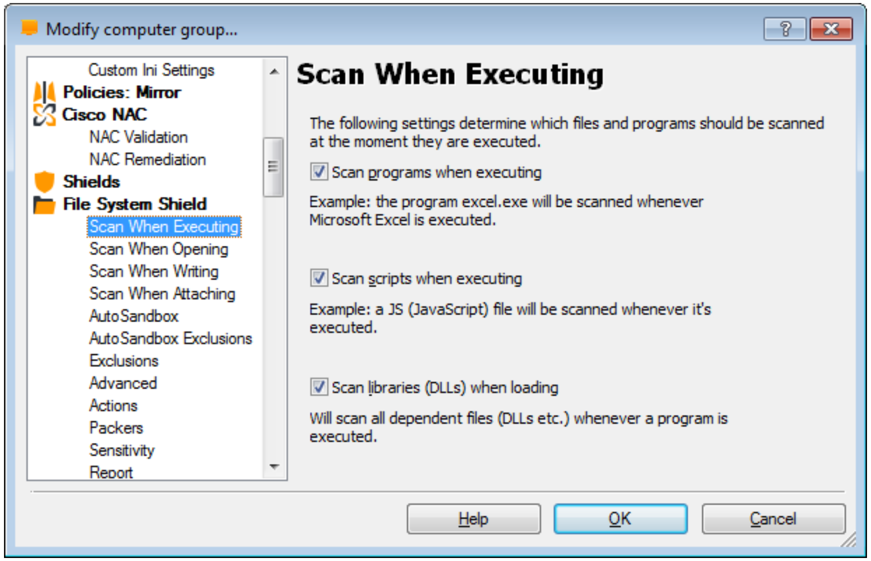
☑ Monitor

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

AEA console

Computer catalog

File System shield



Scan When Executing

The following settings determine which files and programs should be scanned at the moment they are executed.

☑ Scan programs when executing

Example: the program excel.exe will be scanned whenever Microsoft Excel is executed.

☑ Scan scripts when executing

Example: a JS (JavaScript) file will be scanned whenever it's executed.

☑ Scan libraries (DLLs) when loading

Will scan all dependent files (DLLs etc.) whenever a program is executed.

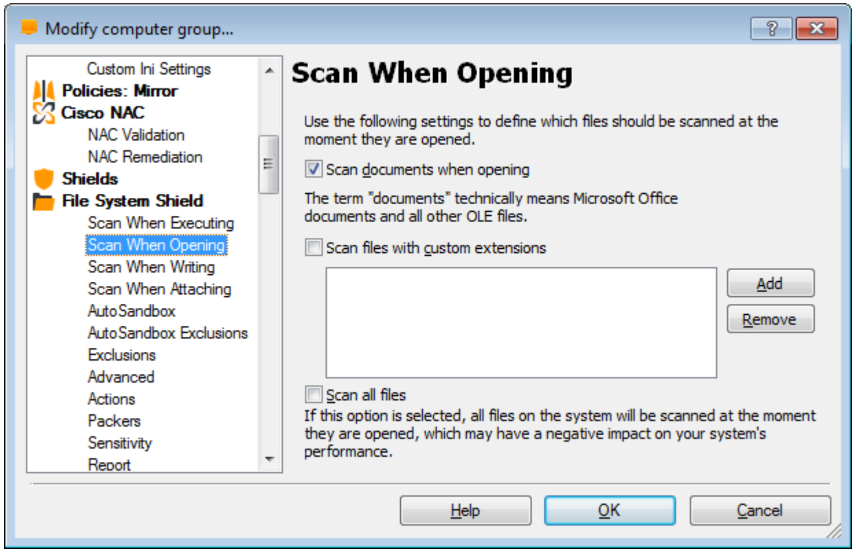
- Here you can specify the types of file that should be scanned at the moment they are run or "executed". It is recommended that all of these boxes are checked.
- Checking the boxes:
  - "**scan programs when executing**"
  - "**scan scripts when executing**"

  will ensure that all programs and scripts will Be scanned at the moment they are run to ensure they are clean and will not cause any damage to your computer or your data.

  - If "**Scan libraries (DLLs) when loading**" is checked, all DLL files will be scanned when they are loaded. This may result in some applications starting more slowly, but will significantly increase the security of your system.

AEA console

Computer catalog



Scan When Opening

Use the following settings to define which files should be scanned at the moment they are opened.

☑ Scan documents when opening

The term "documents" technically means Microsoft Office documents and all other OLE files.

□ Scan files with custom extensions

□ Scan all files

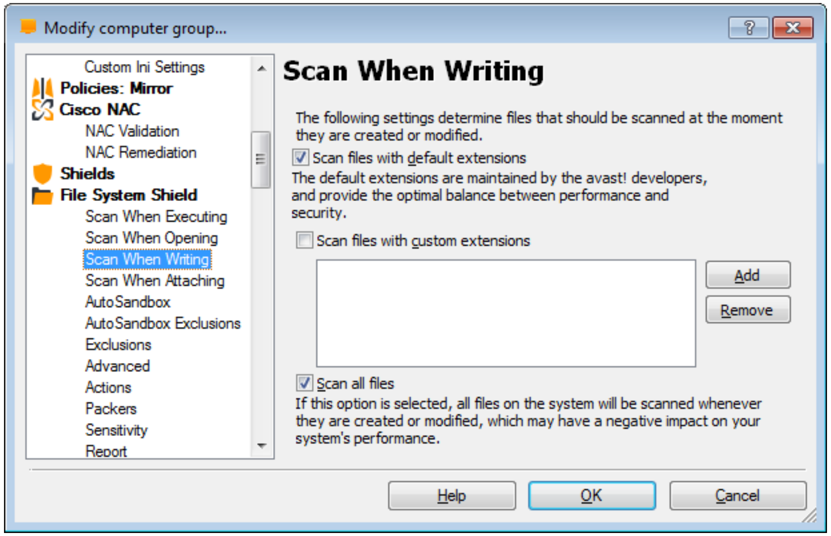
If this option is selected, all files on the system will be scanned at the moment they are opened, which may have a negative impact on your system's performance.

File System shield

- If the box "**Scan documents when opening**" is checked, Microsoft Office documents and other OLE files will be checked at the moment they are opened. To determine which documents and files to check, avast! will check their actual content, not just the file extension.
- You can also specify files that should be scanned based on their extension.
- To scan files with a **specific extension**, check the relevant box and type the extension in the box provided.
  - You can use the **wildcard** "?" for example, if you want all .htm and .html files to be scanned when opening them, you can enter both extensions, or just use the wildcard "ht?". Note however, that this would result in all files with extensions that begin with "ht" being scanned e.g. files with the extension .htt.
- Alternatively, you can specify that all files should be scanned, however this could slow your system down quite significantly while the scan is in progress.

AEA console

Computer catalog



Scan When Writing

The following settings determine files that should be scanned at the moment they are created or modified.

☑ Scan files with default extensions

The default extensions are maintained by the avast! developers, and provide the optimal balance between performance and security.

□ Scan files with custom extensions

☑ Scan all files

If this option is selected, all files on the system will be scanned whenever they are created or modified, which may have a negative impact on your system's performance.

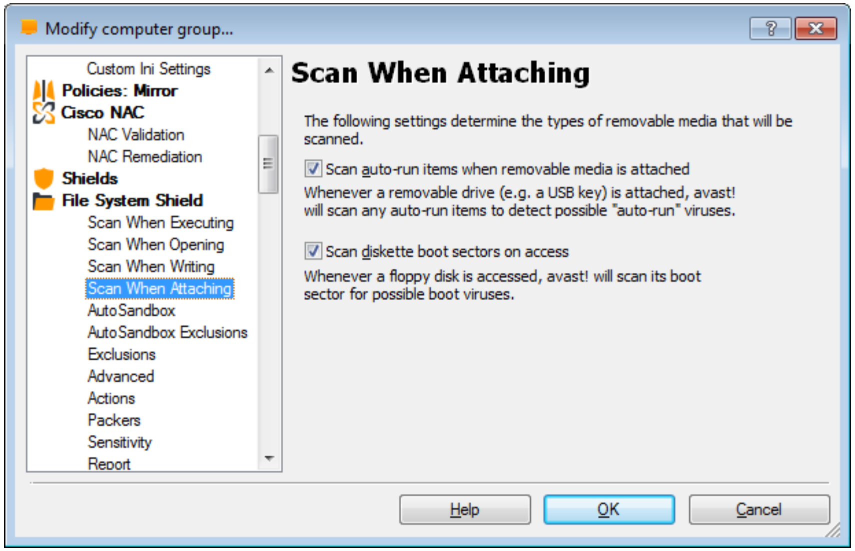
File System shield

- Here you can specify the file types that will be scanned at the moment they are saved. You can specify that all files should be scanned ("**Scan all files**") or just those with particular extensions:
- **Scan files with default extensions** - only those files with extensions that are considered potentially dangerous (e.g. ".exe") will be scanned
- Scan files with **custom extensions** - here you can specify the file types that should be scanned based on their extension. You can use the **wildcard** "?"; for example, if you want all .htm and .html files to be scanned, you can enter both extensions, or just use the wildcard "ht?".
  - Note however, that this would result in all files with extensions that begin with "ht" being scanned e.g. files with the extension .htt.

AEA console

Computer catalog

File System shield



Scan When Attaching

The following settings determine the types of removable media that will be scanned.

☑ Scan auto-run items when removable media is attached

Whenever a removable drive (e.g. a USB key) is attached, avast! will scan any auto-run items to detect possible "auto-run" viruses.

☑ Scan diskette boot sectors on access

Whenever a floppy disk is accessed, avast! will scan its boot sector for possible boot viruses.

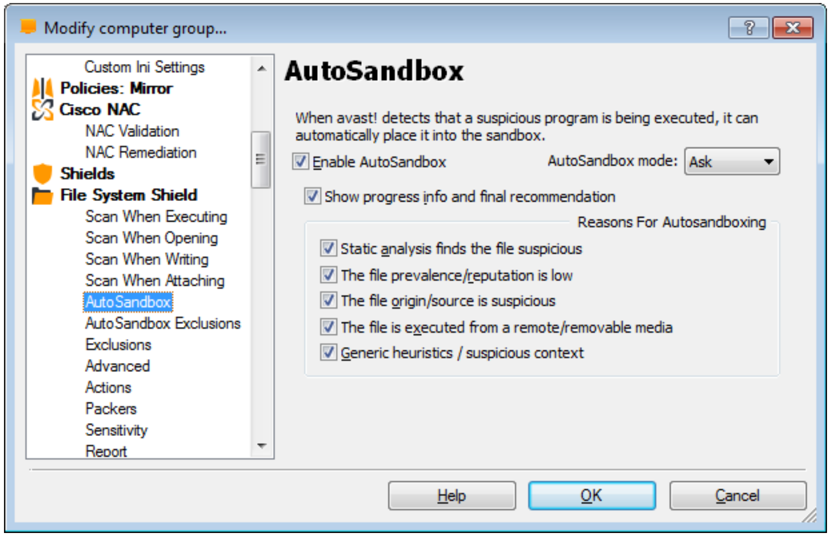
- Here you can specify whether removable media should be scanned when they are connected to your computer to detect potential "**auto-run**" programs that may try to launch when the device is connected.

- You can also specify that the **boot sectors of floppy disks** should be scanned to detect potential boot sector viruses.

AEA console

Computer catalog

File System shield



AutoSandbox

When avast! detects that a suspicious program is being executed, it can automatically place it into the sandbox.

☑ Enable AutoSandbox AutoSandbox mode: Ask

☑ Show progress info and final recommendation

Reasons For Autosandboxing

☑ Static analysis finds the file suspicious

☑ The file prevalence/reputation is low

☑ The file origin/source is suspicious

☑ The file is executed from a remote/removable media

☑ Generic heuristics / suspicious context

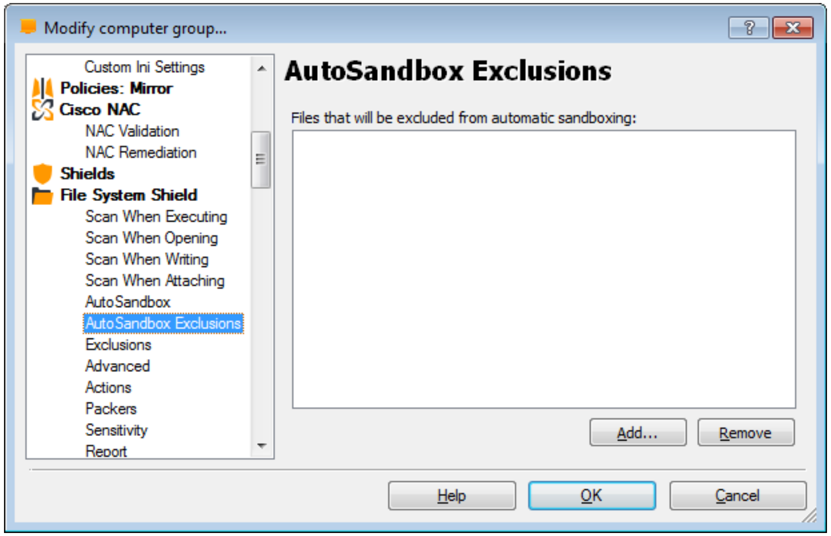
The avast! AutoSandbox is a special security feature which allows potentially suspicious applications to be automatically run in a completely isolated environment.

- By default, if an application is started and avast! detects anything suspicious, it will ask you if you want to run the application in the Sandbox. As the application will be completely contained within the Sandbox, this will prevent any damage being caused to your system by any infected applications.
- Alternatively, the AutoSandbox can be configured to run suspicious applications automatically in the Sandbox. It can also be disabled completely.

AEA console

Computer catalog

File System shield



Modify computer group...

- Custom Ini Settings
- **Policies: Mirror**
- **Cisco NAC**
  - NAC Validation
  - NAC Remediation
- **Shields**
- **File System Shield**
  - Scan When Executing
  - Scan When Opening
  - Scan When Writing
  - Scan When Attaching
  - AutoSandbox
  - AutoSandbox Exclusions
  - Exclusions
  - Advanced
  - Actions
  - Packers
  - Sensitivity
  - Report

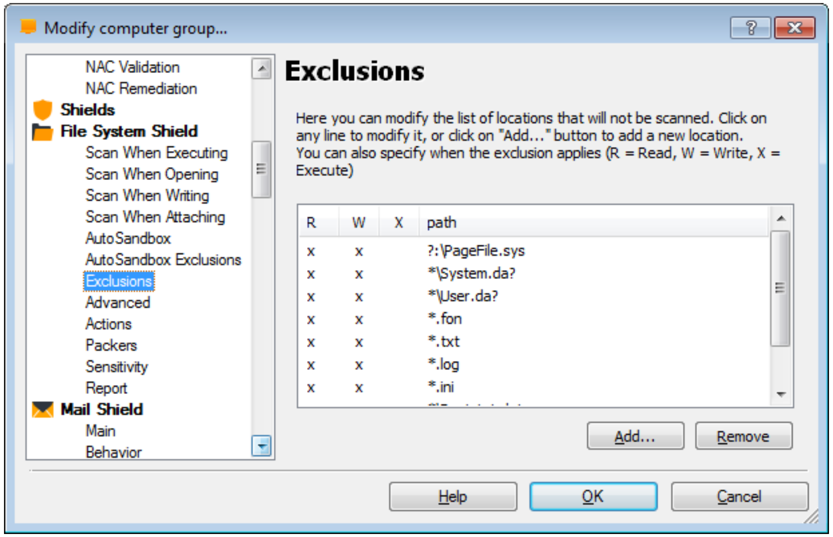
AutoSandbox Exclusions

Files that will be excluded from automatic sandboxing:

- In the AutoSandbox Exclusions, you can specify any files that should be automatically excluded so that they are not run in the Sandbox and are always run on your normal desktop

AEA console

Computer catalog



Exclusions

Here you can modify the list of locations that will not be scanned. Click on any line to modify it, or click on "Add..." button to add a new location. You can also specify when the exclusion applies (R = Read, W = Write, X = Execute)

R	W	X	path
x	x		?:\PageFile.sys
x	x		*\System.da?
x	x		*\User.da?
x	x		*.fon
x	x		*.txt
x	x		*.log
x	x		*.ini

File System shield

- Here you can enter or modify any locations that should not be scanned by the file system shield.
  - Note, that exclusions specified here will only apply to the File System Shield and not to any other scans.

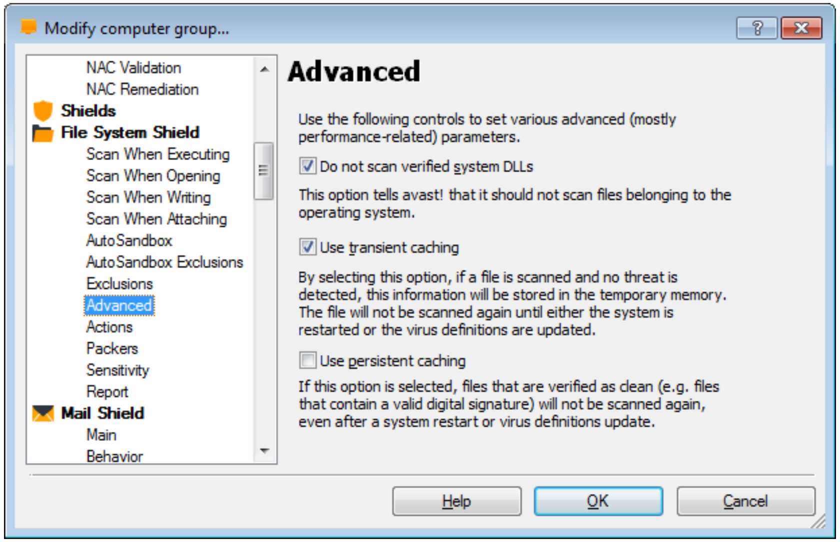
- Certain files are excluded by default at the moment of reading and writing. You can also specify other file types that should be excluded at the moment of
  - reading
  - writing (W)
  - executing (X)

  by clicking on "enter path" and either typing the path to be excluded, or clicking the browse button to select it.

- To exclude files from being scanned by any part of avast!, including manual and scheduled scans, it is necessary to specify the files or areas to be excluded in the general program settings.

AEA console

Computer catalog



Advanced

Use the following controls to set various advanced (mostly performance-related) parameters.

☑ Do not scan verified system DLLs

This option tells avast! that it should not scan files belonging to the operating system.

☑ Use transient caching

By selecting this option, if a file is scanned and no threat is detected, this information will be stored in the temporary memory. The file will not be scanned again until either the system is restarted or the virus definitions are updated.

☐ Use persistent caching

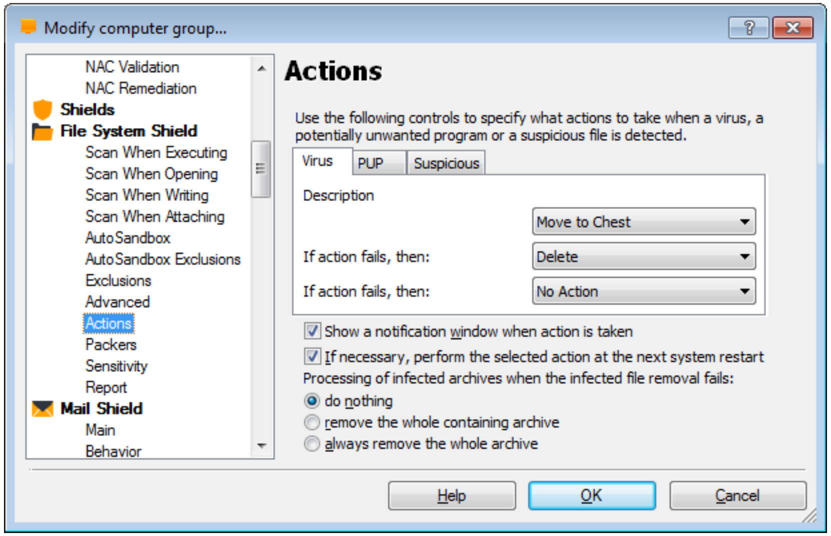
If this option is selected, files that are verified as clean (e.g. files that contain a valid digital signature) will not be scanned again, even after a system restart or virus definitions update.

File System shield

- Scanning time can be potentially reduced by specifying certain types of files that should not be scanned.
- **Do not scan verified system DLLs**
  - if this box is checked, system library files will not be scanned.
- **Use transient caching**
  - if transient caching is used, a file that has been scanned, and in which no infection was detected, will not be scanned again the next time it is accessed. However, this is only valid until the next virus definitions update, as the file may contain an infection that was not previously detected but which may be detected based on the new virus definitions. Also, information that the file is clean will only be stored in the computer's operating (temporary) memory. This means that when the system is restarted the information will be lost, therefore the file will also be scanned again the next time it is accessed after a system restart. This box is checked by default; if you want files to be scanned every time they are accessed, this box should be unchecked.

AEA console

Computer catalog



Actions

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

Description: Move to Chest

If action fails, then: Delete

If action fails, then: No Action

☑ Show a notification window when action is taken

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

Processing of infected archives when the infected file removal fails:

● do nothing

○ remove the whole containing archive

○ always remove the whole archive

File System shield

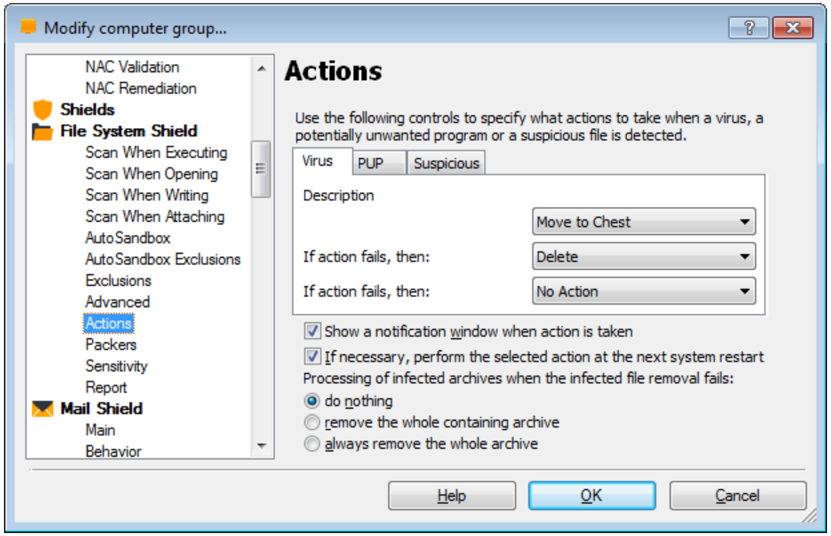
- On this screen, you can specify the action that should be taken automatically whenever a virus, potentially unwanted program (PUP), or suspicious file is detected.
- The default action is "No action" and if this is left unchanged, any suspicious files will be reported at the end of the scan and you will have the opportunity then to deal with them individually:
  - **delete them**
  - **move them to the virus chest**
  - **do nothing**
- Alternatively, you can select an action which avast! will attempt to carry out automatically:
  - **Repair**
  - **Move to Chest**
  - **Delete**

  If any action is selected, you can then specify an alternative action to be taken if the first action fails.

AEA console

Computer catalog

File System shield



Actions

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

Description: Move to Chest

If action fails, then: Delete

If action fails, then: No Action

☑ Show a notification window when action is taken

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

Processing of infected archives when the infected file removal fails:

● do nothing

○ remove the whole containing archive

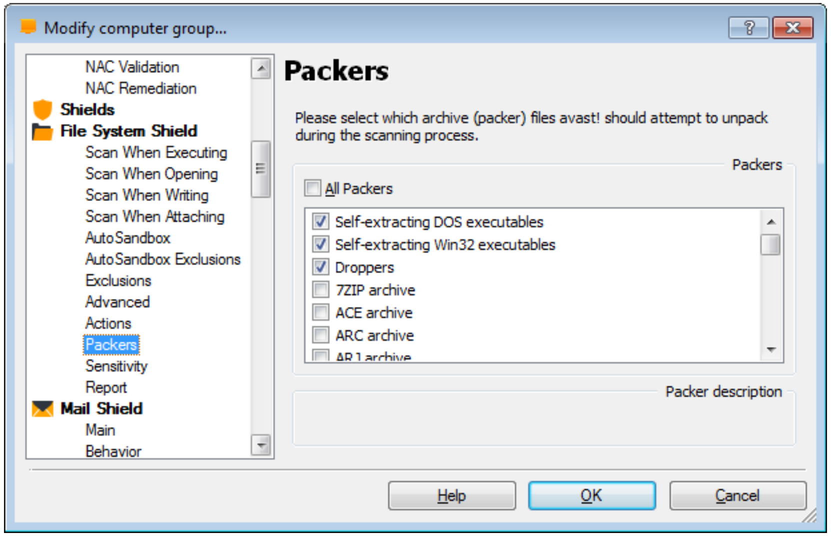
○ always remove the whole archive

- Options:
  - **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.

AEA console

Computer catalog

File System shield



Packers

Please select which archive (packer) files avast! should attempt to unpack during the scanning process.

Packers

□ All Packers

☑ Self-extracting DOS executables
☑ Self-extracting Win32 executables
☑ Droppers
□ 7ZIP archive
□ ACE archive
□ ARC archive
□ ARJ archive

Packer description

- On this page, you can specify which types of archive file are checked when scanning. Certain file types are scanned by default but you can also specify other types that should be scanned by checking the appropriate box.

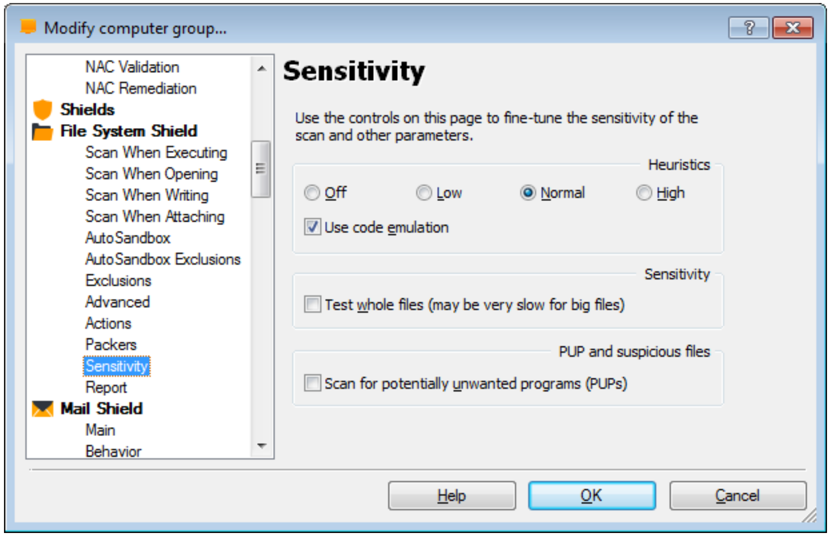
- By clicking once on any of the default file types in the list, you can see a description of that particular type of file at the bottom of the page.

- If you want all archive files to be scanned, check the box "**All packers**", however, this may significantly increase the scanning time.

AEA console

Computer catalog

File System shield



Modify computer group...

Sensitivity

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

Heuristics

○ Off ○ Low ● Normal ○ High

☑ Use code emulation

Sensitivity

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

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

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

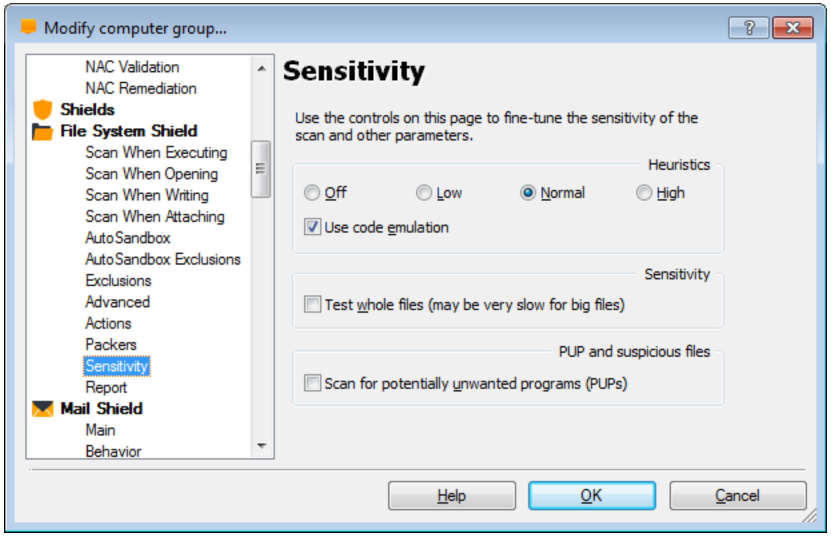
- As well as the standard process of scanning for known malware infections, avast! also performs a heuristic analysis to identify potential, but as yet unknown malware. This is done by looking for certain characteristics that may be a sign of a potential infection. By clicking on the orange bars, you 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 are 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.

AEA console

Computer catalog

File System shield



Modify computer group...

Sensitivity

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

Heuristics

○ Off ○ Low ● Normal ○ High

☑ Use code emulation

Sensitivity

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

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

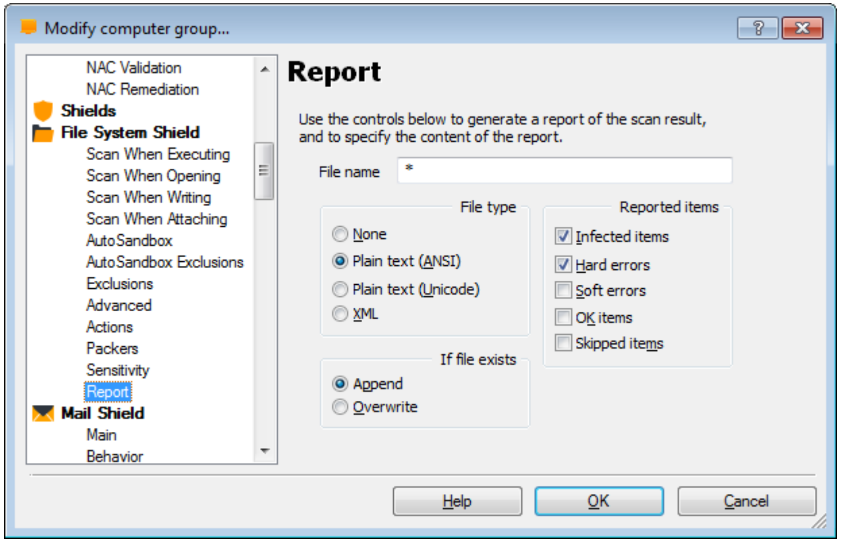
- If the box "**use code emulation**" is checked and avast! detects some suspicious code in a file, it will attempt to run the code in a virtual environment to determine how it behaves. If potential malicious behavior is detected, it will be reported as a virus. Running the code in this virtual environment 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 unchecking 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.

AEA console

Computer catalog

File System shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name: *

File type
- ○ None
- ● Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

Reported items
- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

If file exists
- ● Append
- ○ Overwrite

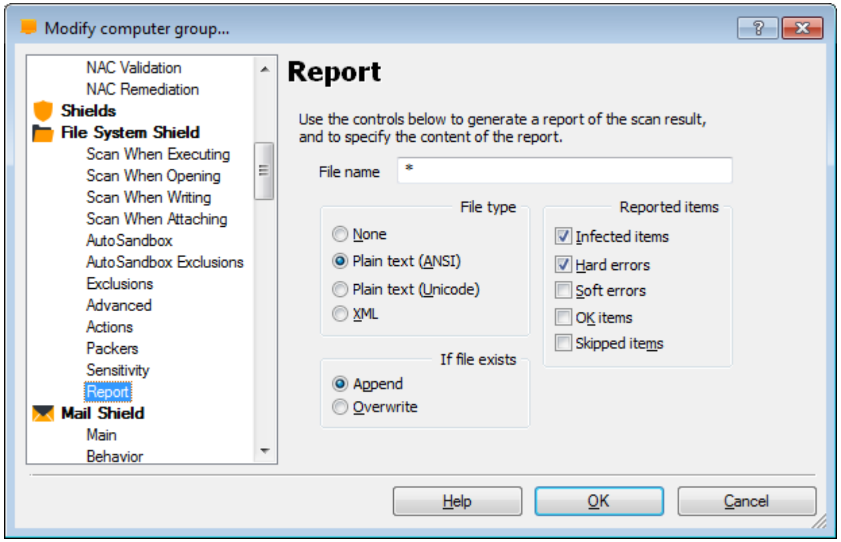
On this page you can create a report of the scan results. You can specify whether you want the report to be created as a plain text file, or in XML format.

- If you want to create a new report after each scan, and you don't want to keep a record of previous scan results, select "overwrite". A new report will then be created after each scan and will replace any previous report.
- If you want to keep the previous scan results, select "Append" and the results of the new scan will be added to the end of the previous report.

AEA console

Computer catalog

File System shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name: *

File type
- ○ None
- ● Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

Reported items
- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

If file exists
- ● Append
- ○ Overwrite

Reported items:

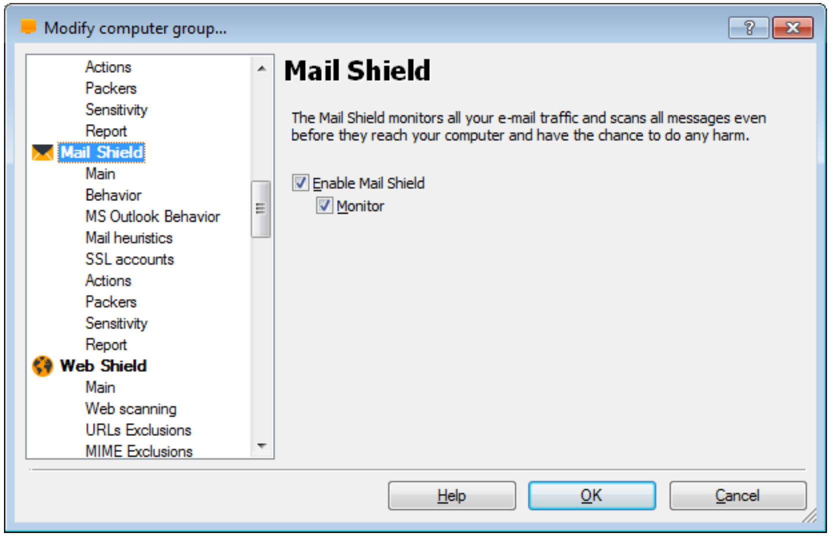
- **Infected items** - files that potentially contain a virus or other malware infection
- **Hard errors** - these arise when the program detects something that would not normally be expected and generally require further investigation.
- **Soft errors** - these are less serious than hard errors and usually concern files that could not be scanned, for example, because they were open and being used by another application.
- **OK items** - these are files that were scanned where nothing suspicious was detected. If all local drives are scanned, checking this box could produce a very long report. It is recommended to check this box only if you intend to carry out a limited scan and only if you really want all clean files to be reported as well as any problematic files.
- **Skipped items** - these are files that were not scanned as a result of the scan settings, for example, if it was specified that only files with specific extension should be scanned or if certain files were specifically excluded from the scan.

MAIL SHIELD

AEA console

Computer catalog

Mail Shield



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.

☑ Enable Mail Shield

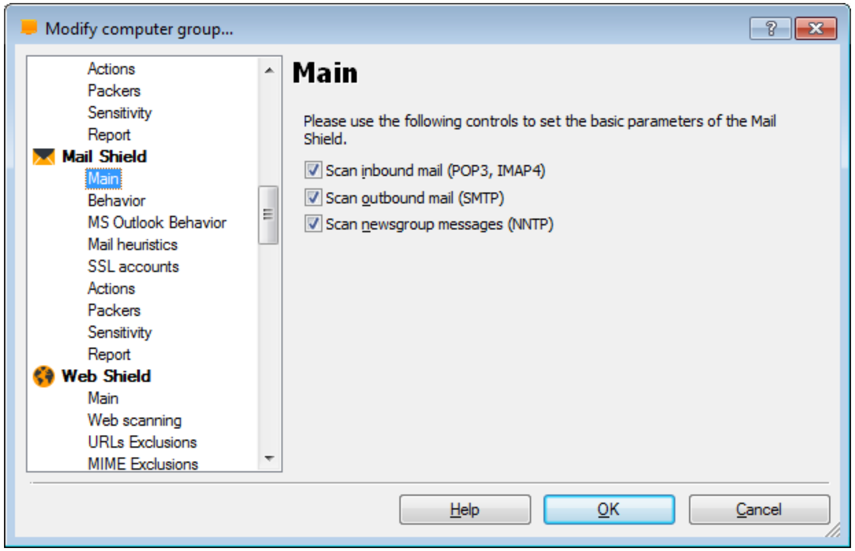
☑ Monitor

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

AEA console

Computer catalog

Mail Shield



Modify computer group...

Main

Please use the following controls to set the basic parameters of the Mail Shield.

☑ Scan inbound mail (POP3, IMAP4)

☑ Scan outbound mail (SMTP)

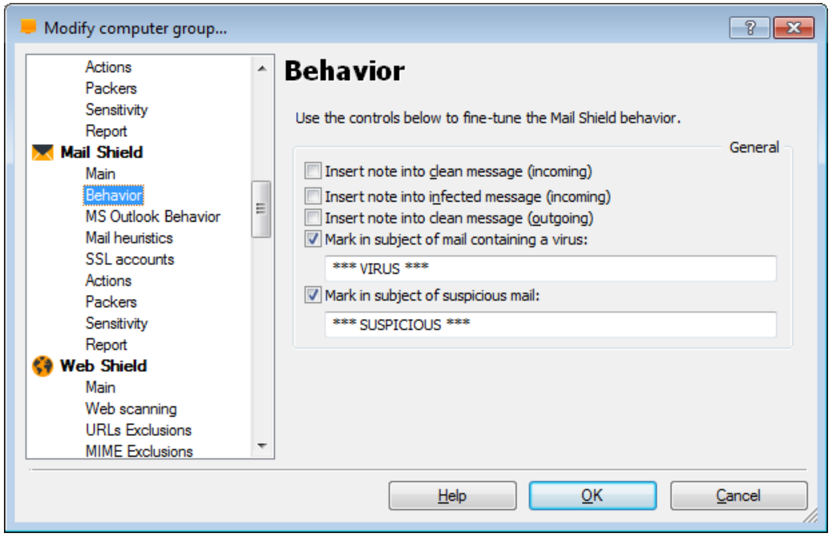
☑ Scan newsgroup messages (NNTP)

- Here you can specify which type of messages are scanned - i.e. messages that are:
  - **received** (inbound POP3,IMAP4)
  - **sent** (outbound SMTP)
  - **newsgroup messages** (NNTP)

AEA console

Computer catalog

Mail Shield



Behavior

Use the controls below to fine-tune the Mail Shield behavior.

General

□ Insert note into clean message (incoming)

□ Insert note into infected message (incoming)

□ Insert note into clean message (outgoing)

☑ Mark in subject of mail containing a virus:

*** VIRUS ***

☑ Mark in subject of suspicious mail:

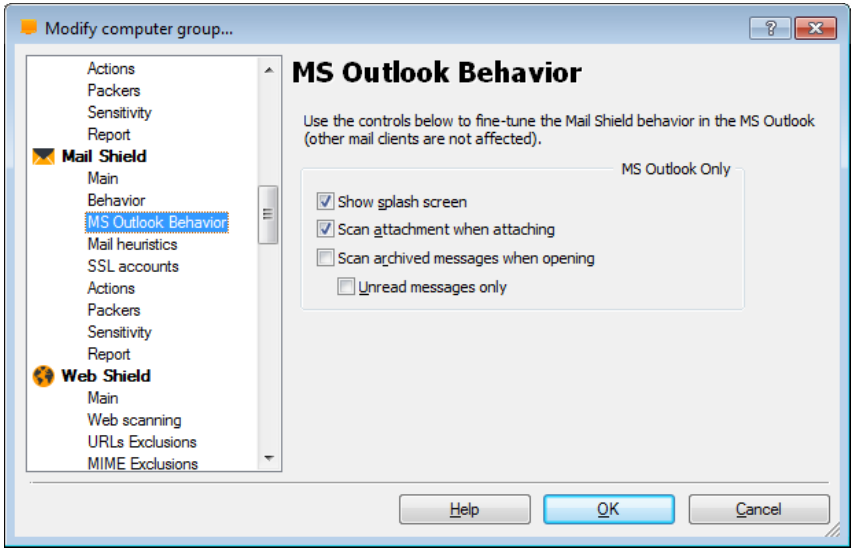
*** SUSPICIOUS ***

- Use the controls below to the fine-tune the Mail Shield behavior
- You can insert a note into
  - Clean messages
  - Infected messages
- You can add a mark into the subject of mail containing a virus
- Or you can add a mark in the subject of suspicious mails

AEA console

Computer catalog

Mail Shield



Modify computer group...

MS Outlook Behavior

Use the controls below to fine-tune the Mail Shield behavior in the MS Outlook (other mail clients are not affected).

MS Outlook Only

☑ Show splash screen

☑ Scan attachment when attaching

□ Scan archived messages when opening

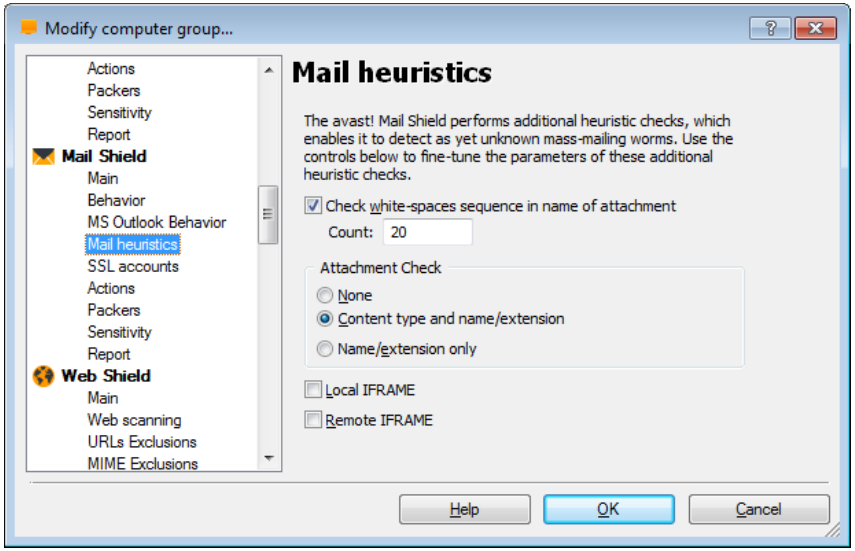
□ Unread messages only

- MS Outlook only
  - **Show splash screen** - if this box is checked, the avast! splash screen will be displayed briefly whenever MS Outlook is launched, to confirm that the Mail Shield is running.
  - **Scan attachment when attaching** - here you can specify that attachments should be scanned at the time they are attached, rather than when they are sent.
  - **Scan archived messages when opening** - by default messages that have been archived are not scanned. By checking this box, you can ensure that even archive messages are scanned.
    - However, you can also specify that this will only apply to unread messages, by checking the "unread messages only" box.

AEA console

Computer catalog

Mail Shield



Mail heuristics

The avast! Mail Shield performs additional heuristic checks, which enables it to detect as yet unknown mass-mailing worms. Use the controls below to fine-tune the parameters of these additional heuristic checks.

☑ Check white-spaces sequence in name of attachment

Count: 20

Attachment Check

○ None

● Content type and name/extension

○ Name/extension only

□ Local IFRAME

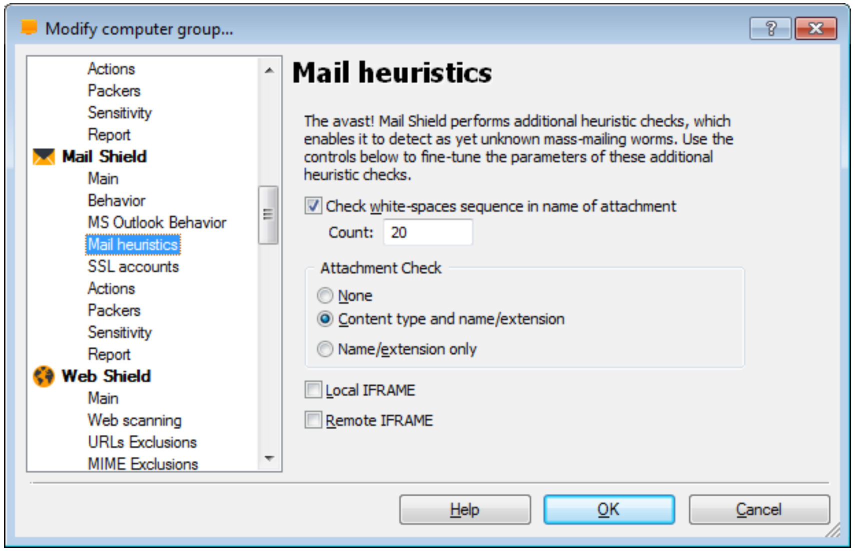
□ Remote IFRAME

- Check white-spaces sequence in name of attachment
  - Some viruses add a number of spaces (or other non-displayable "white" characters) to the end of a file extension, followed by a second real extension, which would normally be recognized as a potentially dangerous extension. However, due to the length of the file name, the person receiving the email might not see the second extension and may open the attachment, believing it to be safe. The heuristic analysis uncovers this trick by looking for white-space sequences in the name of the attachment.
  - The default number of whitespaces is 20 and if the number of white-spaces exceeds this number, a warning will be displayed

AEA console

Computer catalog

Mail Shield



Mail heuristics

The avast! Mail Shield performs additional heuristic checks, which enables it to detect as yet unknown mass-mailing worms. Use the controls below to fine-tune the parameters of these additional heuristic checks.

☑ Check white-spaces sequence in name of attachment

Count: 20

Attachment Check

○ None

● Content type and name/extension

○ Name/extension only

□ Local IFRAME

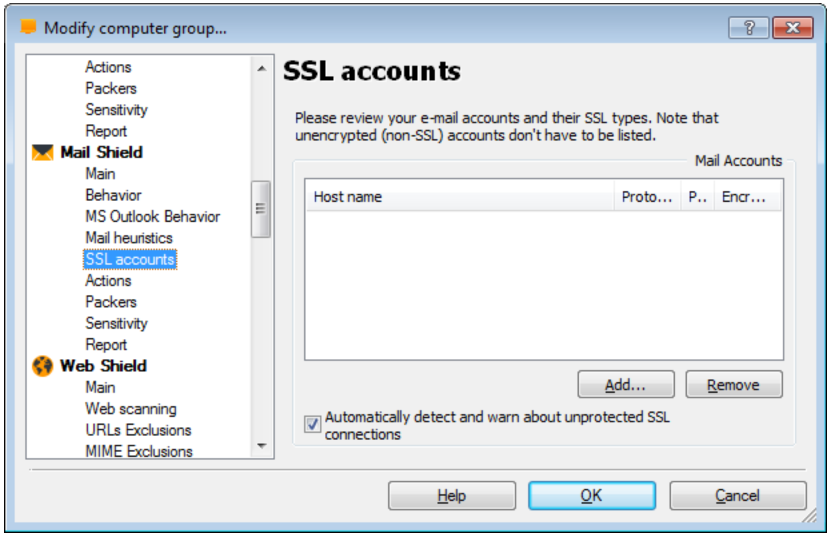
□ Remote IFRAME

- **Attachment check -** if this box is checked, an analysis of the attachment will be performed based its name and extension and, optionally, its content:
  - If "**name/extension only**" is selected, a warning will be displayed, for example, if the attachment has a simple executable extension (EXE, COM, BAT etc). However, not all such files are dangerous and this might result in a higher number of false positive alerts - i.e. clean files identified as potentially suspicious.
  - If "**Content type and name/extension**" is selected, the program will additionally check that the content actually corresponds to the file type e.g. a file ending .jpg actually does contain a picture and is not a renamed COM file.
- **Local iframe/Remote iframe** - Some viruses can exploit bugs in some mail programs that make it possible to start the virus simply be viewing the message in the preview pane. avast! checks whether the HTML code of the message contains a tag which enables it to do this and if such a tag is detected, a warning message is displayed.

AEA console

Computer catalog

Mail Shield



Modify computer group...

SSL accounts

Please review your e-mail accounts and their SSL types. Note that unencrypted (non-SSL) accounts don't have to be listed.

Mail Accounts

Host name	Proto...	P..	Encr...

☑ Automatically detect and warn about unprotected SSL connections

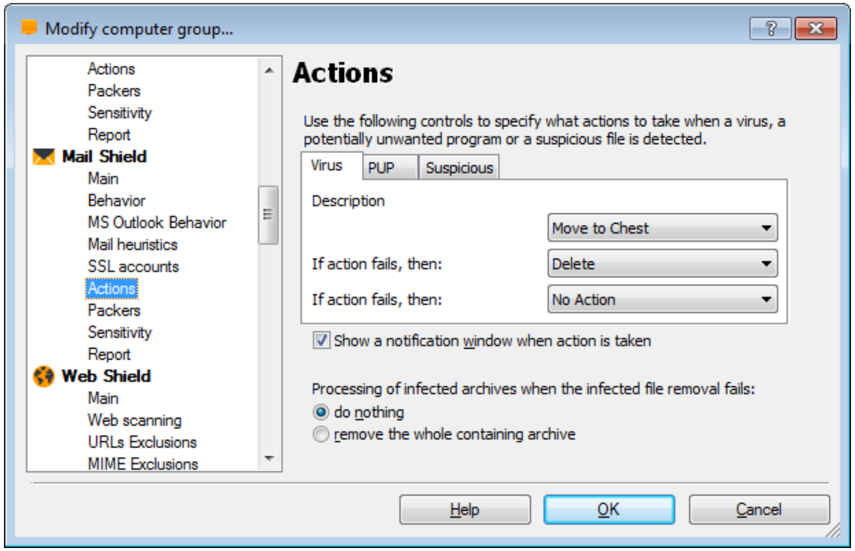
- **Outgoing Mail**
  - The outgoing unencrypted email will first be scanned by the Mail Shield. If the type of encryption is specified on this page, a secure connection will be established and the mail will be sent encrypted to the Mail Server.
  - If the type of encryption has been specified as "None", the mail will be sent unencrypted.
  - If nothing is specified on this page for a particular mail account, the Mail Shield will check whether the Mail Server supports encryption. If it does, a new rule will be created automatically.

A more detailed SSL settings description can be found on the avast website in the knowledge base article: http://support.avast.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=458

AEA console

Computer catalog

Mail Shield


Modify computer group...

Actions
Packers
Sensitivity
Report
Mail Shield
Main
Behavior
MS Outlook Behavior
Mail heuristics
SSL accounts
Actions
Packers
Sensitivity
Report
Web Shield
Main
Web scanning
URLs Exclusions
MIME Exclusions

Actions

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

Description: Move to Chest

If action fails, then: Delete

If action fails, then: No Action

☑ Show a notification window when action is taken

Processing of infected archives when the infected file removal fails:

● do nothing
○ remove the whole containing archive

- On this screen, you can specify the action that should be taken automatically whenever a virus, potentially unwanted program (PUP), or suspicious file is detected.

- The default action is "No action" and if this is left unchanged, any suspicious files will be reported at the end of the scan and you will have the opportunity then to deal with them individually:
  - **delete them**
  - **move them to the virus chest**
  - **do nothing**

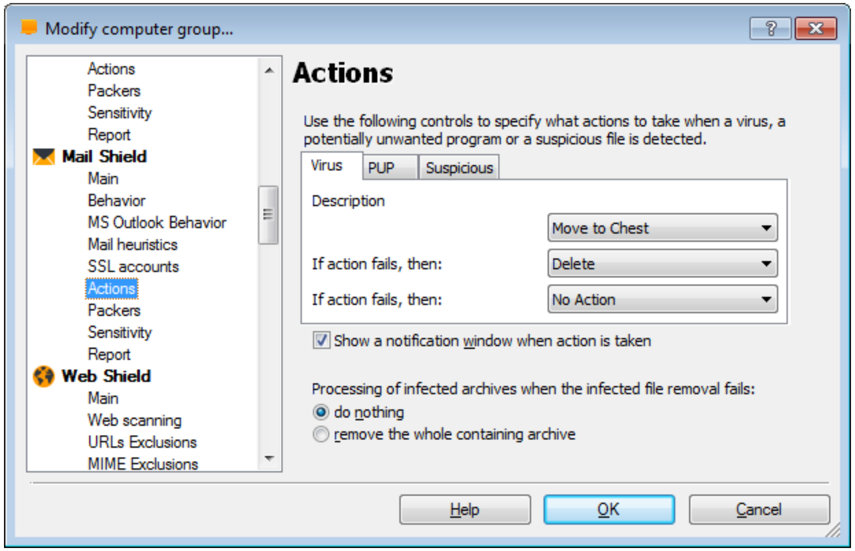
- Alternatively, you can select an action which avast! will attempt to carry out automatically:
  - **Repair**
  - **Move to Chest**
  - **Delete**

  If any action is selected, you can then specify an alternative action to be taken if the first action fails.

AEA console

Computer catalog

Mail Shield



Actions

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

Description: Move to Chest

If action fails, then: Delete

If action fails, then: No Action

☑ Show a notification window when action is taken

Processing of infected archives when the infected file removal fails:

● do nothing

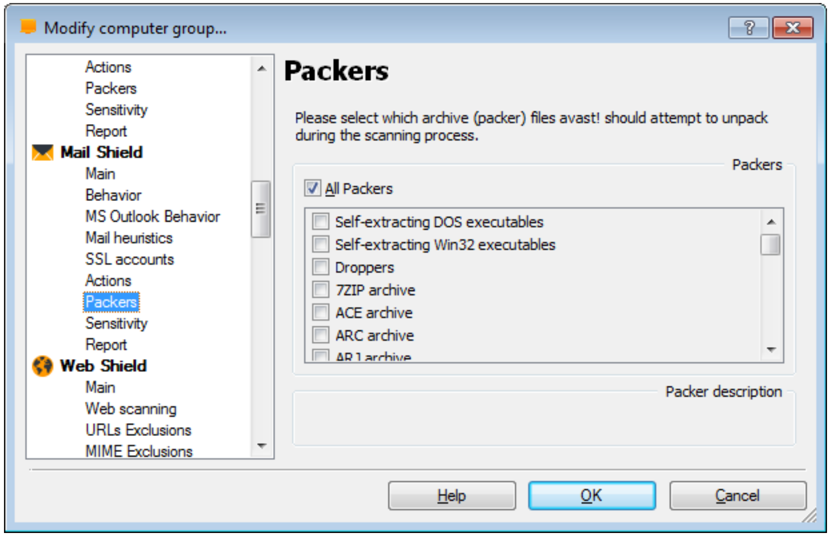
○ remove the whole containing archive

- Options:
  - 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.

AEA console

Computer catalog

Mail Shield



Packers

Please select which archive (packer) files avast! should attempt to unpack during the scanning process.

Packers

☑ All Packers

□ Self-extracting DOS executables
□ Self-extracting Win32 executables
□ Droppers
□ 7ZIP archive
□ ACE archive
□ ARC archive
□ ARJ archive

Packer description

- On this page, you can specify which types of archive file are checked when scanning. Certain file types are scanned by default but you can also specify other types that should be scanned by checking the appropriate box.

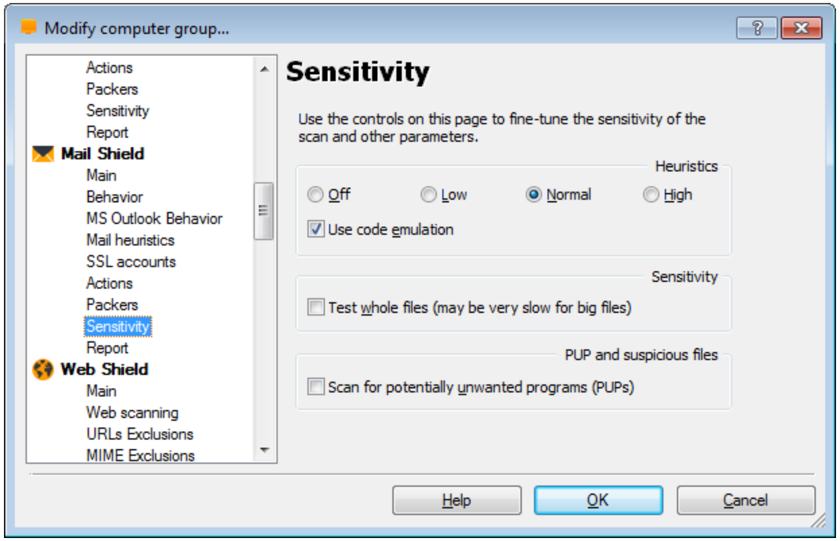
- By clicking once on any of the default file types in the list, you can see a description of that particular type of file at the bottom of the page.

- If you want all archive files to be scanned, check the box "**All packers**", however, this may significantly increase the scanning time.

AEA console

Computer catalog

Mail Shield



Sensitivity

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

Heuristics

○ Off ○ Low ● Normal ○ High

☑ Use code emulation

Sensitivity

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

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

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

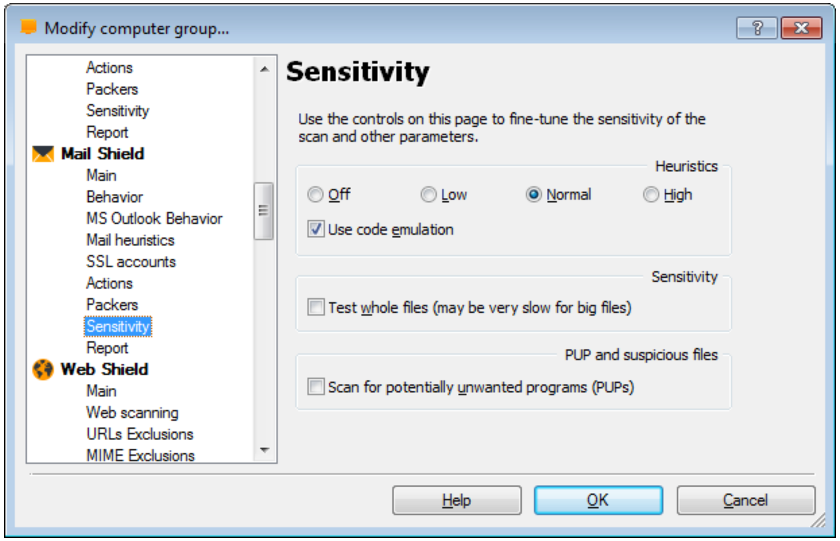
- As well as the standard process of scanning for known malware infections, avast! also performs a heuristic analysis to identify potential, but as yet unknown malware. This is done by looking for certain characteristics that may be a sign of a potential infection. By clicking on the orange bars, you 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 are 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.

AEA console

Computer catalog

Mail Shield



Modify computer group...

Sensitivity

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

Heuristics

○ Off ○ Low ● Normal ○ High

☑ Use code emulation

Sensitivity

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

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

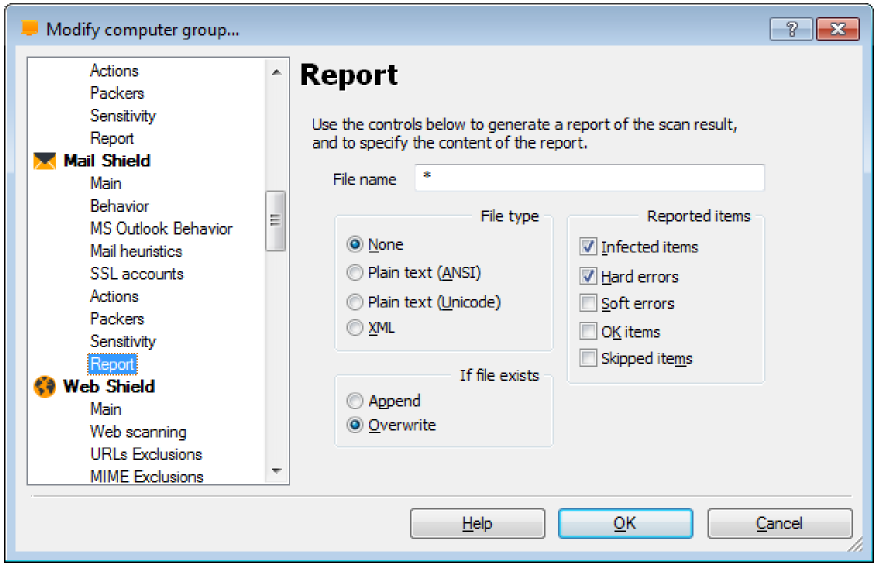
- If the box "use code emulation" is checked and avast! detects some suspicious code in a file, it will attempt to run the code in a virtual environment to determine how it behaves. If potential malicious behavior is detected, it will be reported as a virus. Running the code in this virtual environment 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 unchecking 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.

AEA console

Computer catalog

Mail Shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name *

File type
- ● None
- ○ Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

If file exists
- ○ Append
- ● Overwrite

Reported items
- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

On this page you can create a report of the scan results. You can specify whether you want the report to be created as a plain text file, or in XML format.

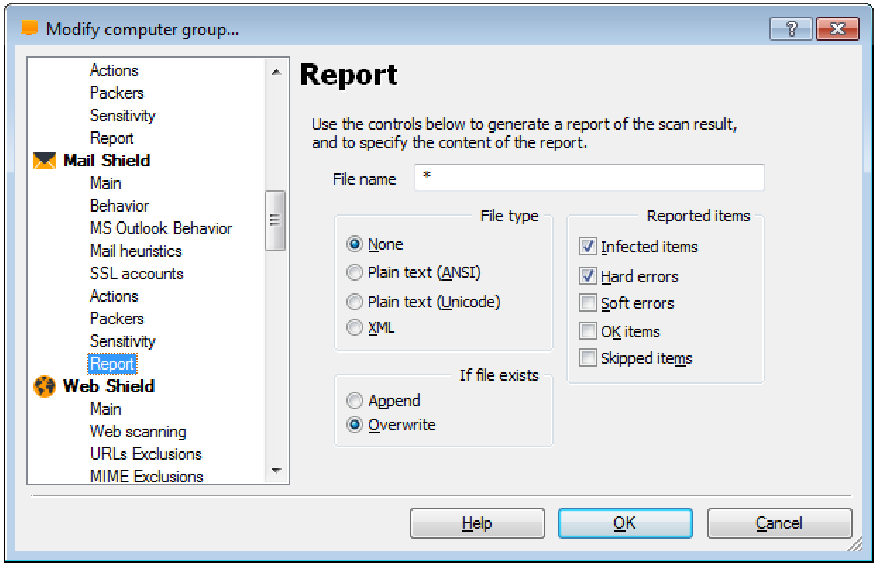
- If you want to create a new report after each scan, and you don't want to keep a record of previous scan results, select "overwrite". A new report will then be created after each scan and will replace any previous report.

- If you want to keep the previous scan results, select "Append" and the results of the new scan will be added to the end of the previous report.

AEA console

Computer catalog

Mail Shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name *

File type

● None
○ Plain text (ANSI)
○ Plain text (Unicode)
○ XML

Reported items

☑ Infected items
☑ Hard errors
☐ Soft errors
☐ OK items
☐ Skipped items

If file exists

○ Append
● Overwrite

Reported items:

- **Infected items** - files that potentially contain a virus or other malware infection

- **Hard errors** - these arise when the program detects something that would not normally be expected and generally require further investigation.

- **Soft errors** - these are less serious than hard errors and usually concern files that could not be scanned, for example, because they were open and being used by another application.

- **OK items** - these are files that were scanned where nothing suspicious was detected. If all local drives are scanned, checking this box could produce a very long report. It is recommended to check this box only if you intend to carry out a limited scan and only if you really want all clean files to be reported as well as any problematic files.

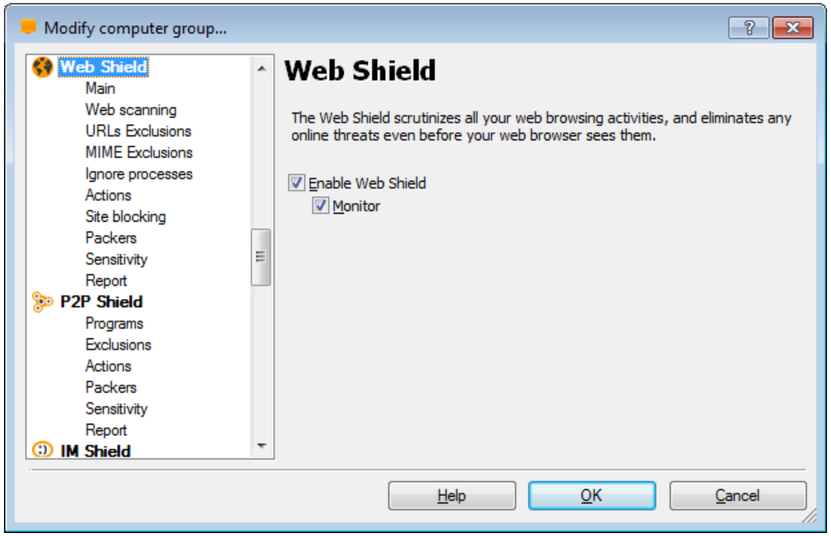
- **Skipped items** - these are files that were not scanned as a result of the scan settings, for example, if it was specified that only files with specific extension should be scanned or if certain files were specifically excluded from the scan.

WEB SHIELD

AEA console

Computer catalog

Web Shield



Modify computer group...

Web Shield

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

☑ Enable Web Shield

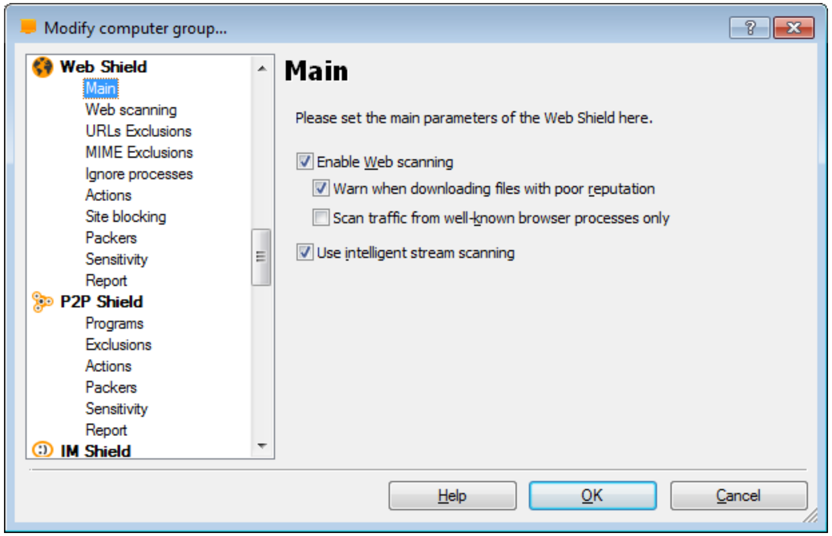
☑ Monitor

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

AEA console

Computer catalog

Web Shield


Modify computer group...

Main

Please set the main parameters of the Web Shield here.

☑ Enable Web scanning

☑ Warn when downloading files with poor reputation

□ Scan traffic from well-known browser processes only

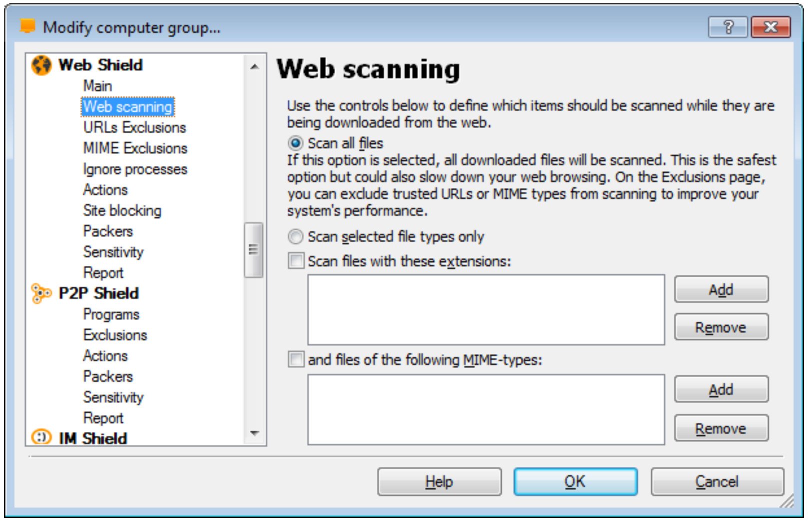
☑ Use intelligent stream scanning

- **Enable Web scanning**
  - this box is checked by default. By unchecking this box, you can turn off the web scanning feature without affecting the URL blocking, which will remain active
- **Use intelligent stream scanning**
  - this is also checked by default. When checked, files that are downloaded are scanned in real-time i.e. during the actual download process. The packets of data are scanned as soon as they arrive - and the next ones are downloaded only when the previous packets have been verified to be infection-free. If this feature is disabled, by unchecking the box, the whole file will be downloaded to a temporary folder first and then scanned

AEA console

Computer catalog

Web Shield



Web scanning

Use the controls below to define which items should be scanned while they are being downloaded from the web.

● Scan all files

If this option is selected, all downloaded files will be scanned. This is the safest option but could also slow down your web browsing. On the Exclusions page, you can exclude trusted URLs or MIME types from scanning to improve your system's performance.

○ Scan selected file types only

□ Scan files with these extensions:

□ and files of the following MIME-types:

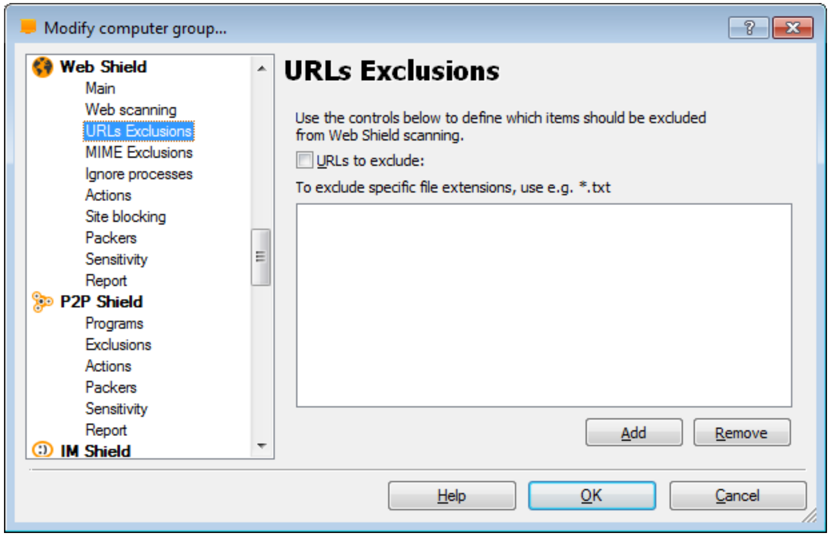
- On this page you can specify which files should be scanned when they are downloaded from the internet. You can specify that all files should be scanned, or just those with particular extensions. For this feature to be active, the "**Enable web scanning**" box should be checked on the Main Settings page.

- You can also enter the **MIME types** of files that should be scanned. In both cases, wildcards can be used.

AEA console

Computer catalog

Web Shield



URLs Exclusions

Use the controls below to define which items should be excluded from Web Shield scanning.

□ URLs to exclude:

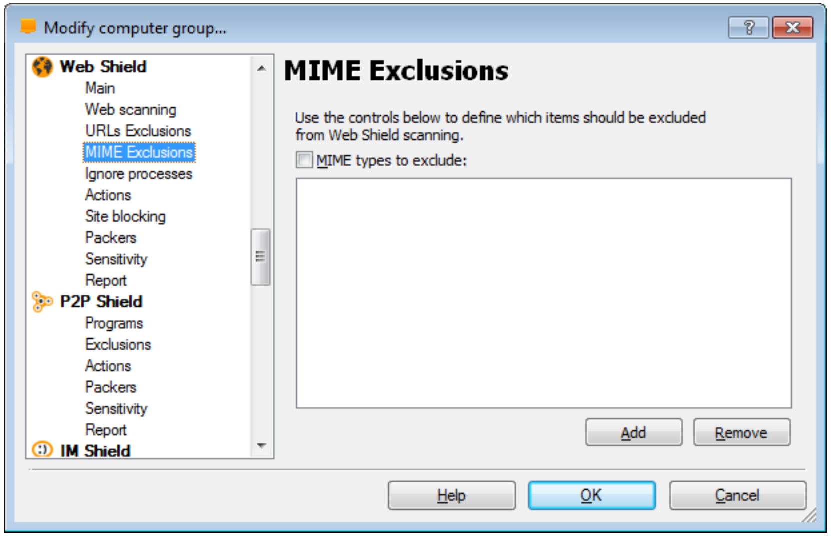
To exclude specific file extensions, use e.g. *.txt

- On this page you can specify URLs that should not be scanned by the Web shield.
- URLs to exclude: Use the “add“ button to enter the URL addresses that should be ignored
  - Single page: http://www.yahoo.com/index.html
  - Whole domain: http://www.yahoo.com/*

AEA console

Computer catalog

Web Shield



MIME Exclusions

Use the controls below to define which items should be excluded from Web Shield scanning.

□ MIME types to exclude:

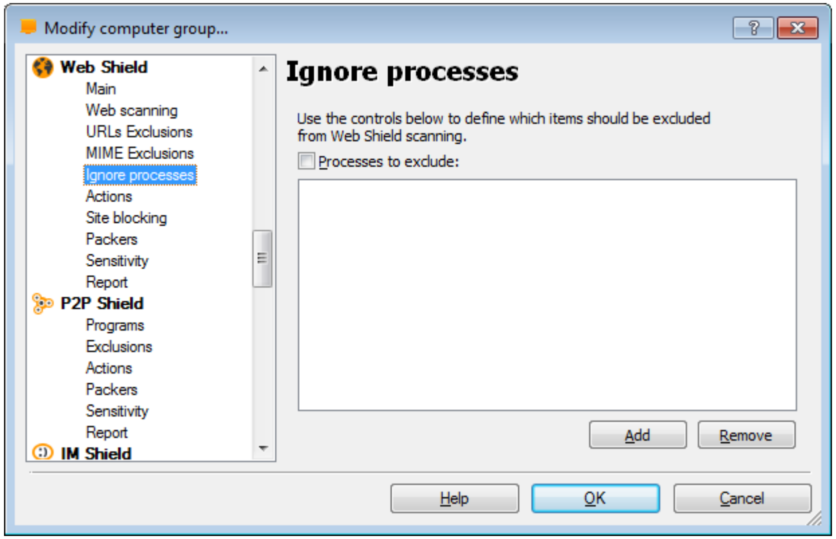
- On this page you can specify MIME types that should not be scanned by the Web shield.

- MIME types to exclude: Here you can specify any MIME types/sub-types that should not be scanned.

AEA console

Computer catalog

Web Shield



Modify computer group...

Ignore processes

Use the controls below to define which items should be excluded from Web Shield scanning.

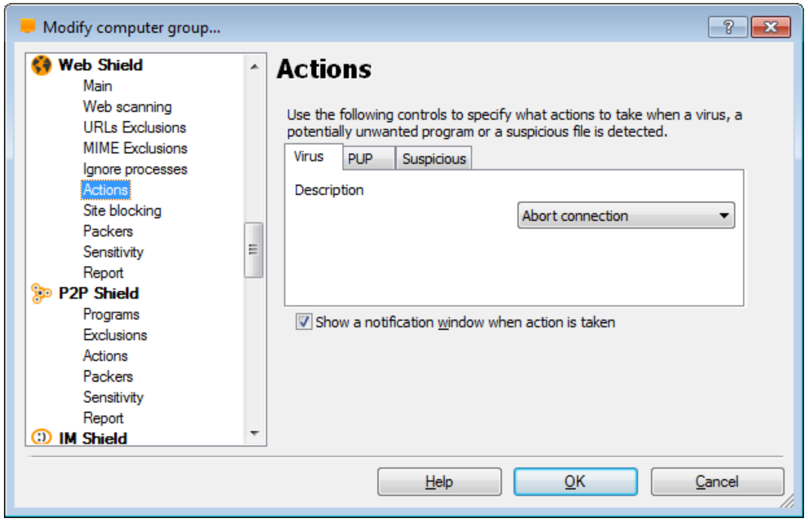
□ Processes to exclude:

- Use the controls below to define which items should be excluded from the web Shield scanning.

AEA console

Computer catalog

Web Shield



Modify computer group...

Actions

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

Description: Abort connection

☑ Show a notification window when action is taken

- On this screen, you can specify the action that should be taken automatically whenever a virus, potentially unwanted program (PUP), or suspicious file is detected.

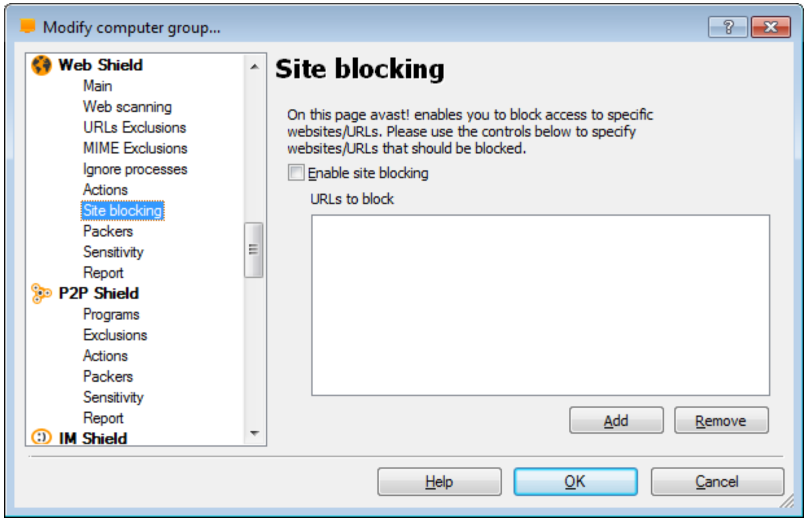
- The default action is „**Abort connection**“ and if this is left unchanged, any suspicious connection will be aborted.

- **Show a notification window when action is taken**
  - If this box is checked, you will see a message on the screen telling you when the specified action has been taken.

AEA console

Computer catalog

Web Shield



Site blocking

On this page avast! enables you to block access to specific websites/URLs. Please use the controls below to specify websites/URLs that should be blocked.

□ Enable site blocking

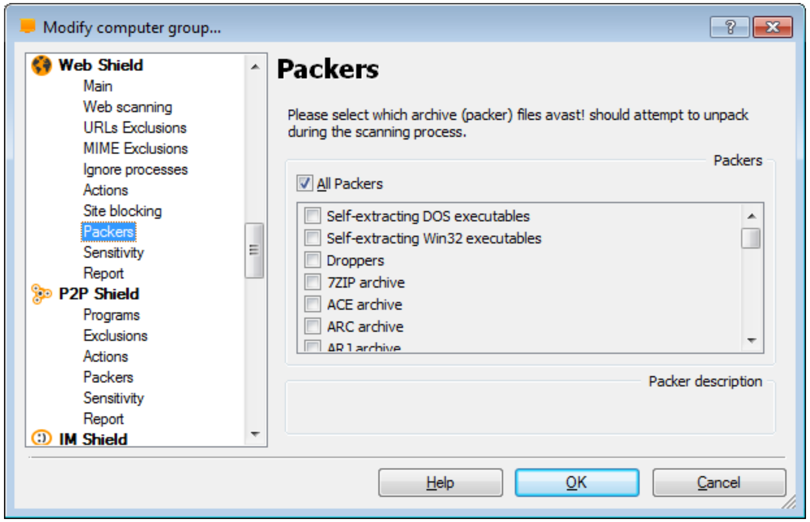
URLs to block

- On this page avast! Enables you to block access to specific websites/URLs. Please use the controls below tospecify websites/URLs that should be blocked.

AEA console

Computer catalog

Web Shield



Packers

Please select which archive (packer) files avast! should attempt to unpack during the scanning process.

Packers

☑ All Packers

□ Self-extracting DOS executables
□ Self-extracting Win32 executables
□ Droppers
□ 7ZIP archive
□ ACE archive
□ ARC archive
□ ARJ archive

Packer description

- On this page, you can specify which types of archive file are checked when scanning. Certain file types are scanned by default but you can also specify other types that should be scanned by checking the appropriate box.

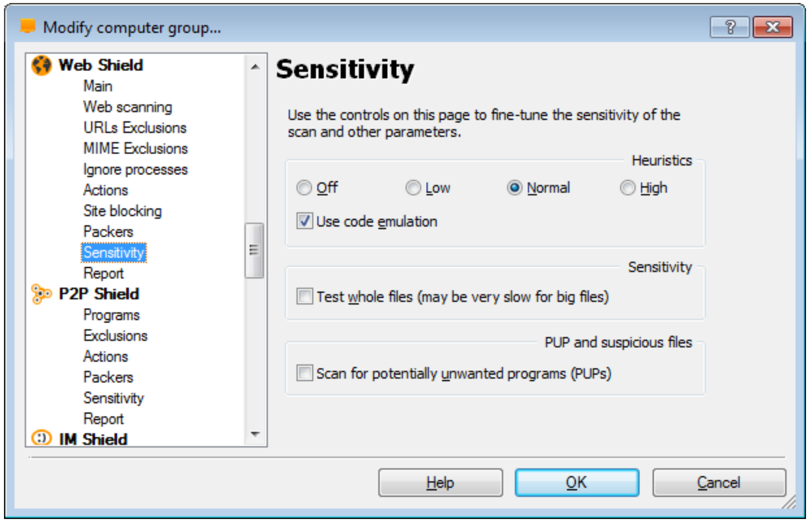
- By clicking once on any of the default file types in the list, you can see a description of that particular type of file at the bottom of the page.

- If you want all archive files to be scanned, check the box "**All packers**", however, this may significantly increase the scanning time.

AEA console

Computer catalog

Web Shield



Sensitivity

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

Heuristics

○ Off ○ Low ● Normal ○ High

☑ Use code emulation

Sensitivity

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

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

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

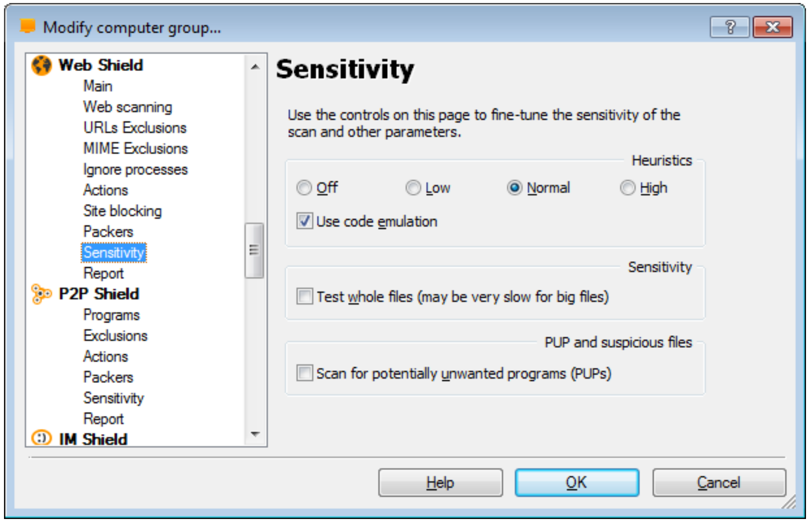
- As well as the standard process of scanning for known malware infections, avast! also performs a heuristic analysis to identify potential, but as yet unknown malware. This is done by looking for certain characteristics that may be a sign of a potential infection. By clicking on the orange bars, you 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 are 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.

AEA console

Computer catalog

Web Shield



Modify computer group...

Sensitivity

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

Heuristics

○ Off ○ Low ● Normal ○ High

☑ Use code emulation

Sensitivity

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

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

- 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 unchecking the following boxes:

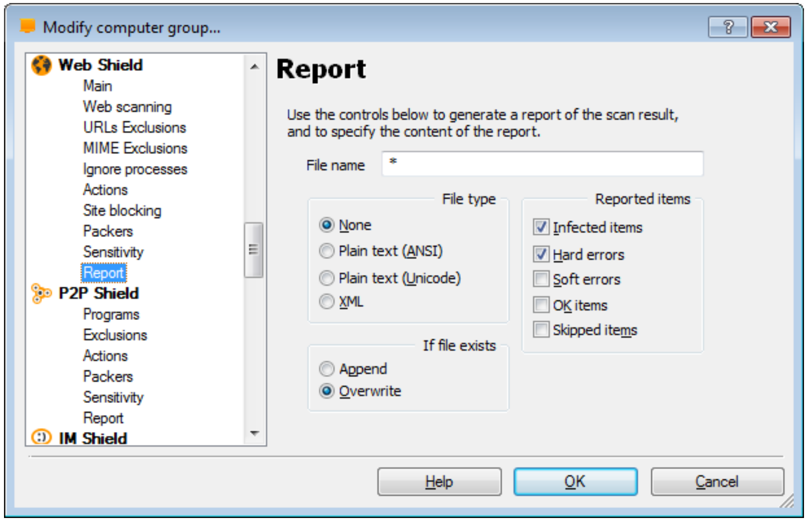
  – **Test whole files (may be very slow for big files)** - checking this box will result in scanned files being tested fully, not just those parts of a file which are normally affected by viruses. Most viruses are normally found either at the beginning of a file, or at the end. Checking this box will 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.

AEA console

Computer catalog

Web Shield



Modify computer group...

Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name: *

File type
- ● None
- ○ Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

Reported items
- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

If file exists
- ○ Append
- ● Overwrite

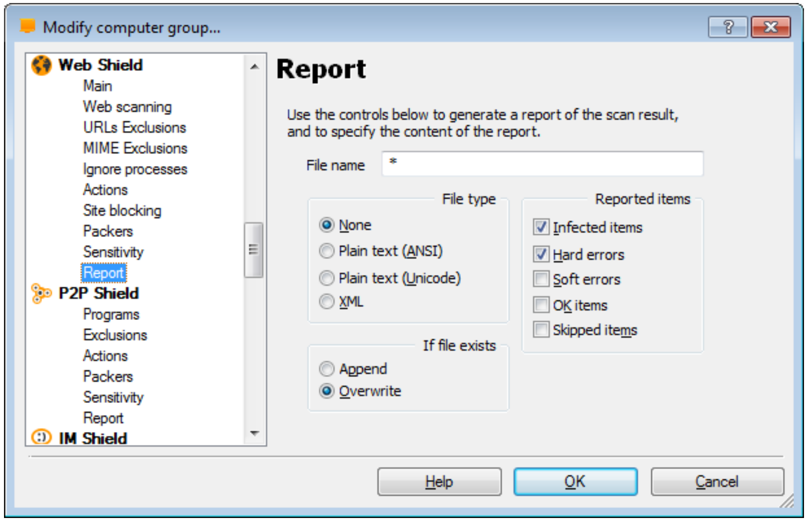
On this page you can create a report of the scan results. You can specify whether you want the report to be created as a plain text file, or in XML format.

- If you want to create a new report after each scan, and you don't want to keep a record of previous scan results, select "overwrite". A new report will then be created after each scan and will replace any previous report.
- If you want to keep the previous scan results, select "Append" and the results of the new scan will be added to the end of the previous report.

AEA console

Computer catalog

Web Shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name: *

File type
- ● None
- ○ Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

Reported items
- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

If file exists
- ○ Append
- ● Overwrite

Reported items:

- **Infected items** - files that potentially contain a virus or other malware infection

- **Hard errors** - these arise when the program detects something that would not normally be expected and generally require further investigation.

- **Soft errors** - these are less serious than hard errors and usually concern files that could not be scanned, for example, because they were open and being used by another application.

- **OK items** - these are files that were scanned where nothing suspicious was detected. If all local drives are scanned, checking this box could produce a very long report. It is recommended to check this box only if you intend to carry out a limited scan and only if you really want all clean files to be reported as well as any problematic files.

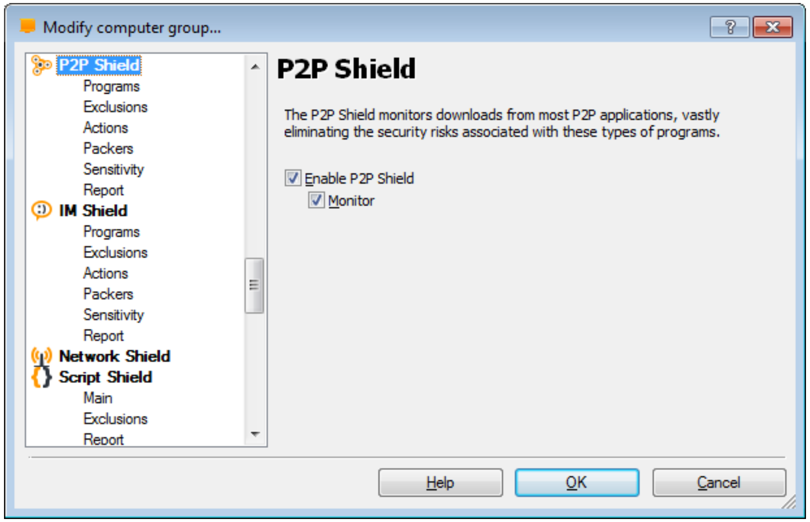
- **Skipped items** - these are files that were not scanned as a result of the scan settings, for example, if it was specified that only files with specific extension should be scanned or if certain files were specifically excluded from the scan.

P2P SHIELD

AEA console

Computer catalog

P2P Shield



Modify computer group...

P2P Shield

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

☑ Enable P2P Shield

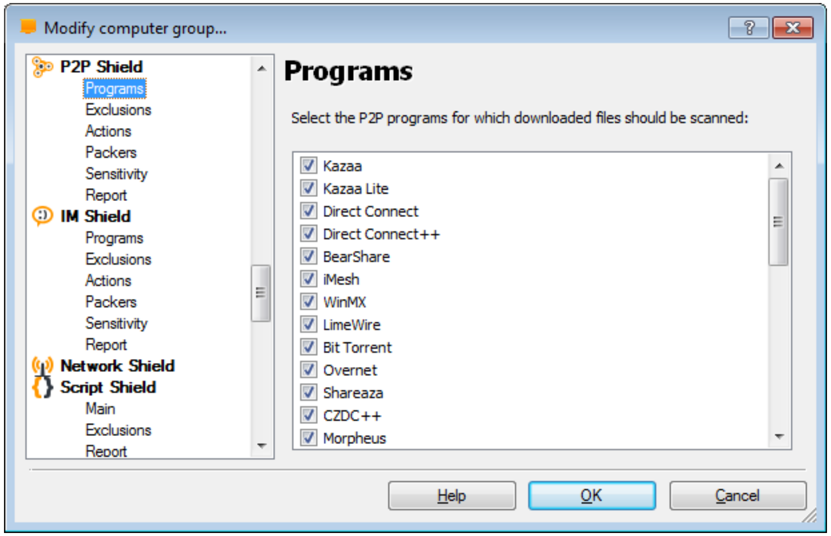
☑ Monitor

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

AEA console

Computer catalog

P2P Shield



Programs

Select the P2P programs for which downloaded files should be scanned:

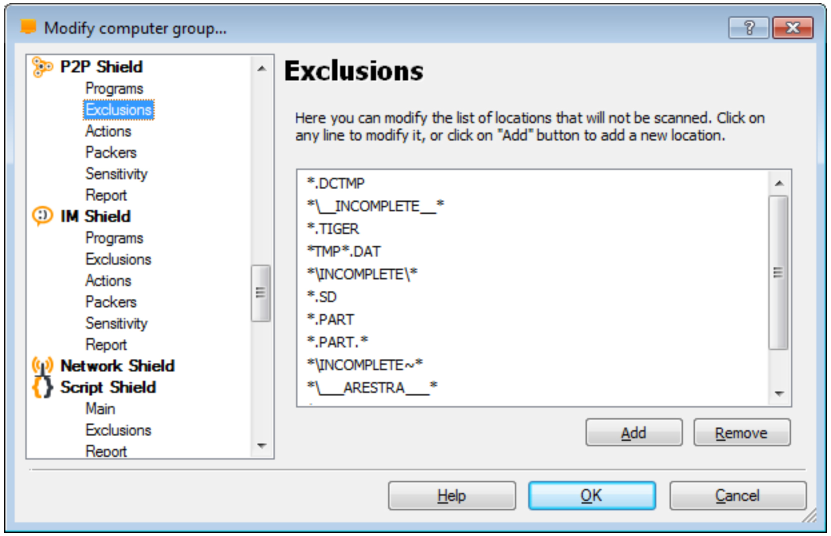
- ☑ Kazaa
- ☑ Kazaa Lite
- ☑ Direct Connect
- ☑ Direct Connect++
- ☑ BearShare
- ☑ iMesh
- ☑ WinMX
- ☑ LimeWire
- ☑ Bit Torrent
- ☑ Overnet
- ☑ Shareaza
- ☑ CZDC++
- ☑ Morpheus

- Select the P2P programs for which downloaded files should be scanned/monitored.
- You can select from a list of 31 programs.

AEA console

Computer catalog

P2P Shield



Exclusions

Here you can modify the list of locations that will not be scanned. Click on any line to modify it, or click on "Add" button to add a new location.

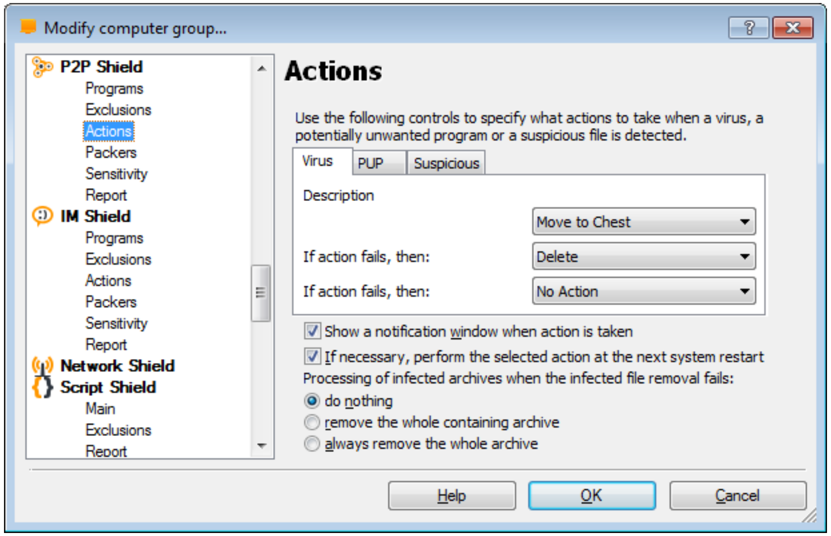
```
*.DCTMP
*\__INCOMPLETE__*
*.TIGER
*TMP*.DAT
*\INCOMPLETE\*
*.SD
*.PART
*.PART.*
*\INCOMPLETE~*
*\___ARESTRA___*
```

- Here you can modify the list of locations that will not be scanned. Click on any line to modify it, or click the “Add“ button to add a new location.

AEA console

Computer catalog

P2P Shield



Actions

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

Description: Move to Chest

If action fails, then: Delete

If action fails, then: No Action

☑ Show a notification window when action is taken

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

Processing of infected archives when the infected file removal fails:

● do nothing

○ remove the whole containing archive

○ always remove the whole archive

- On this screen, you can specify the action that should be taken automatically whenever a virus, potentially unwanted program (PUP), or suspicious file is detected.

- The default action is "No action" and if this is left unchanged, any suspicious files will be reported at the end of the scan and you will have the opportunity then to deal with them individually:
  - **delete them**
  - **move them to the virus chest**
  - **do nothing**

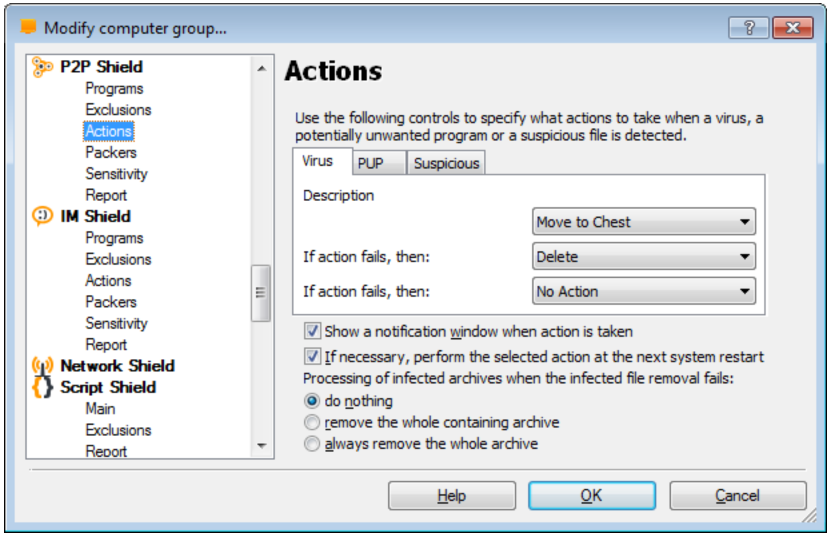
- Alternatively, you can select an action which avast! will attempt to carry out automatically:
  - **Repair**
  - **Move to Chest**
  - **Delete**

  If any action is selected, you can then specify an alternative action to be taken if the first action fails.

AEA console

Computer catalog

P2P Shield



Actions

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

Description: Move to Chest

If action fails, then: Delete

If action fails, then: No Action

☑ Show a notification window when action is taken

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

Processing of infected archives when the infected file removal fails:

● do nothing

○ remove the whole containing archive

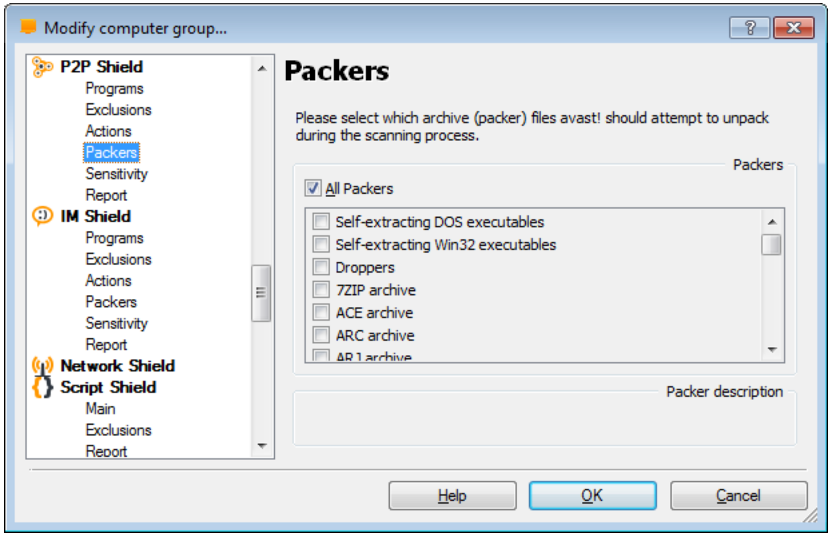
○ always remove the whole archive

- Options:
  - 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.

AEA console

Computer catalog

P2P Shield



Packers

Please select which archive (packer) files avast! should attempt to unpack during the scanning process.

Packers

☑ All Packers

□ Self-extracting DOS executables
□ Self-extracting Win32 executables
□ Droppers
□ 7ZIP archive
□ ACE archive
□ ARC archive
□ ARJ archive

Packer description

- On this page, you can specify which types of archive file are checked when scanning. Certain file types are scanned by default but you can also specify other types that should be scanned by checking the appropriate box.

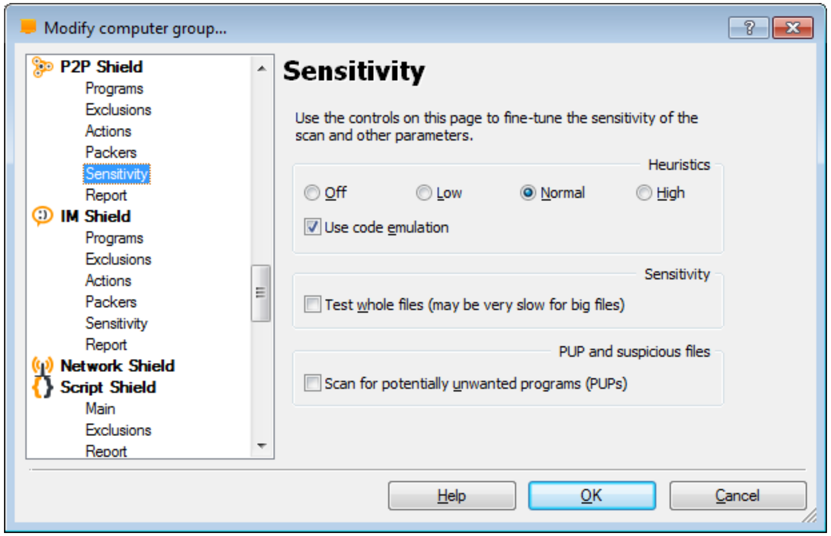
- By clicking once on any of the default file types in the list, you can see a description of that particular type of file at the bottom of the page.

- If you want all archive files to be scanned, check the box "**All packers**", however, this may significantly increase the scanning time.

AEA console

Computer catalog

P2P Shield



Sensitivity

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

Heuristics

○ Off ○ Low ● Normal ○ High

☑ Use code emulation

Sensitivity

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

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

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

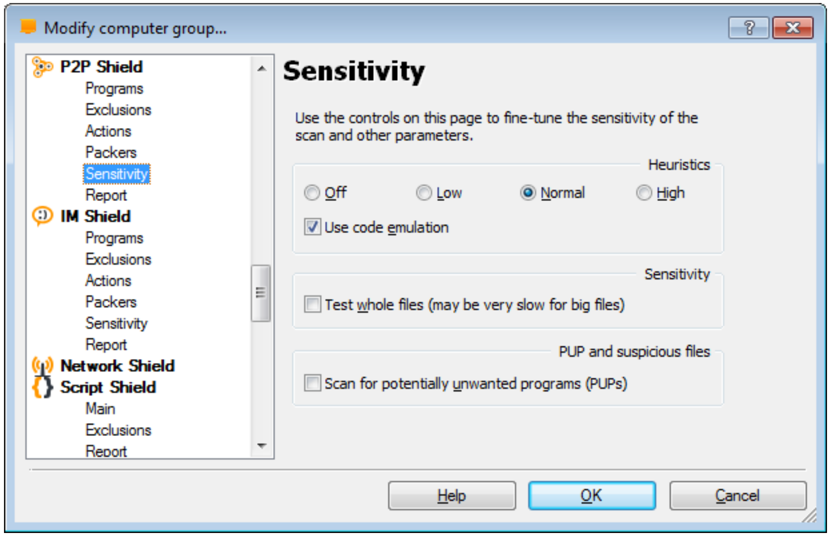
- As well as the standard process of scanning for known malware infections, avast! also performs a heuristic analysis to identify potential, but as yet unknown malware. This is done by looking for certain characteristics that may be a sign of a potential infection. By clicking on the orange bars, you 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 are 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.

AEA console

Computer catalog

P2P Shield



Modify computer group...

Sensitivity

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

Heuristics

○ Off ○ Low ● Normal ○ High

☑ Use code emulation

Sensitivity

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

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

- 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 unchecking the following boxes:

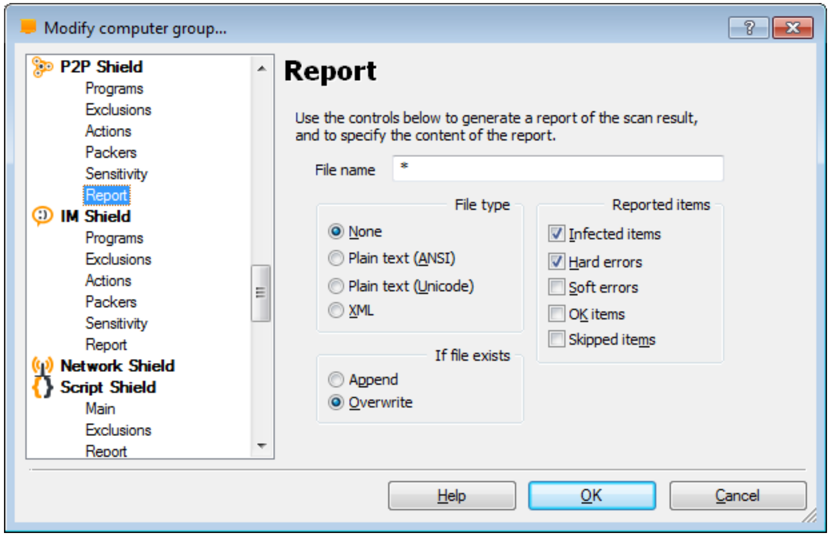
  - **Test whole files (may be very slow for big files)** - checking this box will result in scanned files being tested fully, not just those parts of a file which are normally affected by viruses. Most viruses are normally found either at the beginning of a file, or at the end. Checking this box will 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.

AEA console

Computer catalog

P2P Shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name: *

File type
- ● None
- ○ Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

If file exists
- ○ Append
- ● Overwrite

Reported items
- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

On this page you can create a report of the scan results. You can specify whether you want the report to be created as a plain text file, or in XML format.

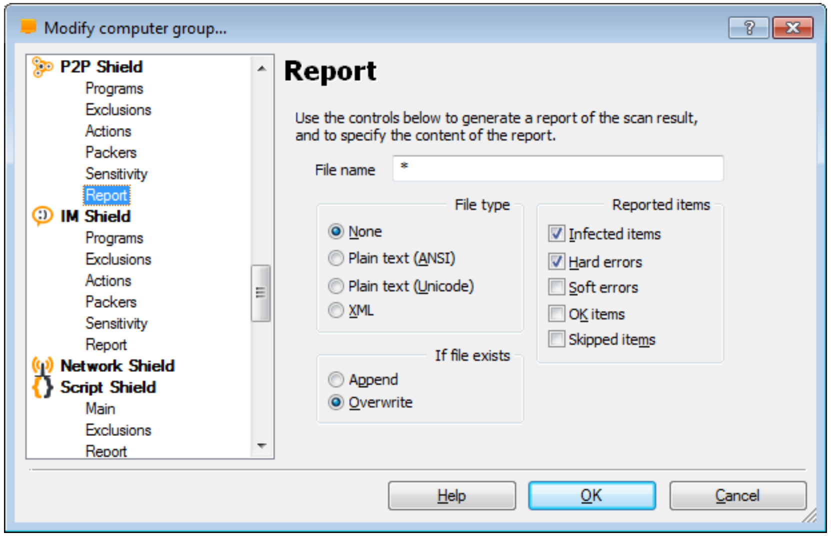
- If you want to create a new report after each scan, and you don't want to keep a record of previous scan results, select "overwrite". A new report will then be created after each scan and will replace any previous report.

- If you want to keep the previous scan results, select "Append" and the results of the new scan will be added to the end of the previous report.

AEA console

Computer catalog

P2P Shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name: *

File type
- ● None
- ○ Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

Reported items
- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

If file exists
- ○ Append
- ● Overwrite

Reported items:

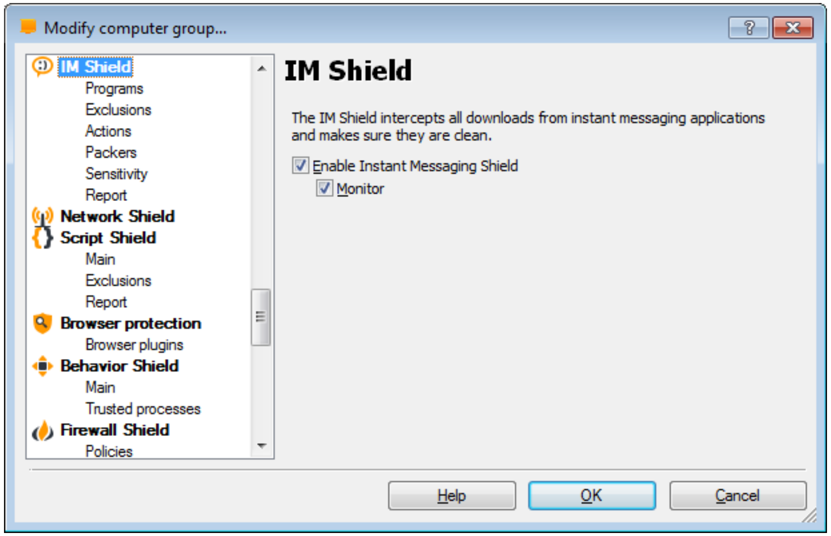
- **Infected items** - files that potentially contain a virus or other malware infection
- **Hard errors** - these arise when the program detects something that would not normally be expected and generally require further investigation.
- **Soft errors** - these are less serious than hard errors and usually concern files that could not be scanned, for example, because they were open and being used by another application.
- **OK items** - these are files that were scanned where nothing suspicious was detected. If all local drives are scanned, checking this box could produce a very long report. It is recommended to check this box only if you intend to carry out a limited scan and only if you really want all clean files to be reported as well as any problematic files.
- **Skipped items** - these are files that were not scanned as a result of the scan settings, for example, if it was specified that only files with specific extension should be scanned or if certain files were specifically excluded from the scan.

IM SHIELD

AEA console

Computer catalog

IM Shield



Modify computer group...

IM Shield

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

☑ Enable Instant Messaging Shield

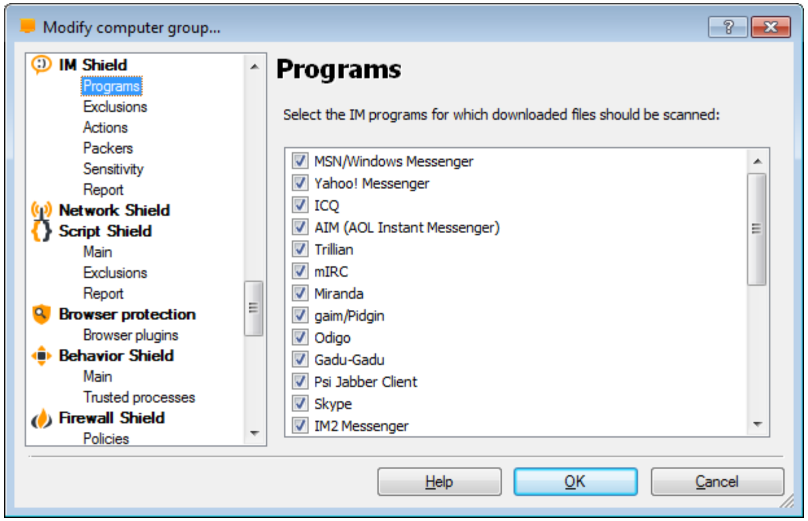
☑ Monitor

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

AEA console

Computer catalog

IM Shield



Programs

Select the IM programs for which downloaded files should be scanned:

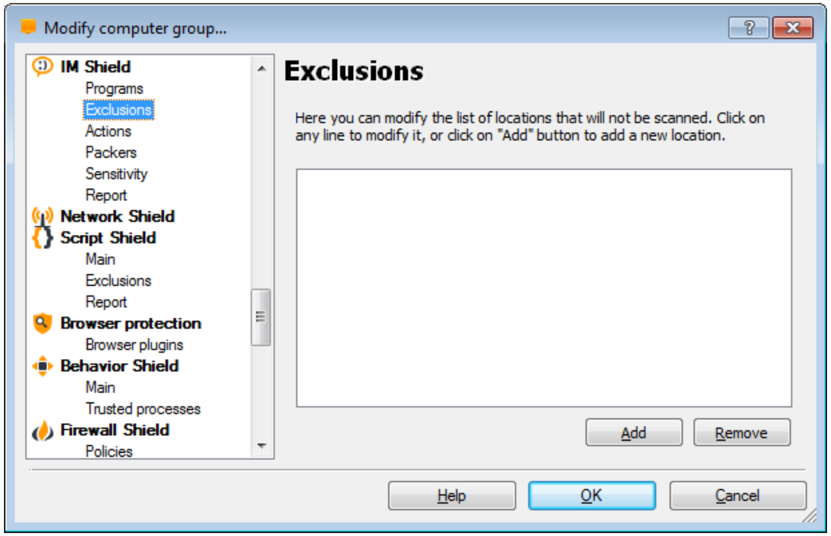
- ☑ MSN/Windows Messenger
- ☑ Yahoo! Messenger
- ☑ ICQ
- ☑ AIM (AOL Instant Messenger)
- ☑ Trillian
- ☑ mIRC
- ☑ Miranda
- ☑ gaim/Pidgin
- ☑ Odigo
- ☑ Gadu-Gadu
- ☑ Psi Jabber Client
- ☑ Skype
- ☑ IM2 Messenger

- Here you can specify which IM programs should be monitored.
- Select the IM programs for which downloaded files should be scanned.

AEA console

Computer catalog

IM Shield



Exclusions

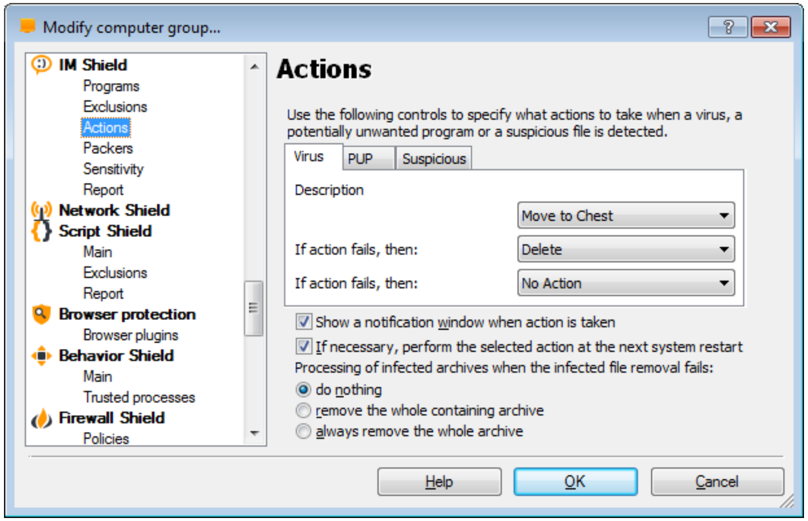
Here you can modify the list of locations that will not be scanned. Click on any line to modify it, or click on "Add" button to add a new location.

- Here you can modify the list of locations that will not be scanned. Click on any line to modify it, or click on the “Add“ button to add a new location.

AEA console

Computer catalog

IM Shield



Actions

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

Description: Move to Chest

If action fails, then: Delete

If action fails, then: No Action

☑ Show a notification window when action is taken

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

Processing of infected archives when the infected file removal fails:

● do nothing

○ remove the whole containing archive

○ always remove the whole archive

- On this screen, you can specify the action that should be taken automatically whenever a virus, potentially unwanted program (PUP), or suspicious file is detected.

- The default action is "No action" and if this is left unchanged, any suspicious files will be reported at the end of the scan and you will have the opportunity then to deal with them individually:
  - **delete them**
  - **move them to the virus chest**
  - **do nothing**

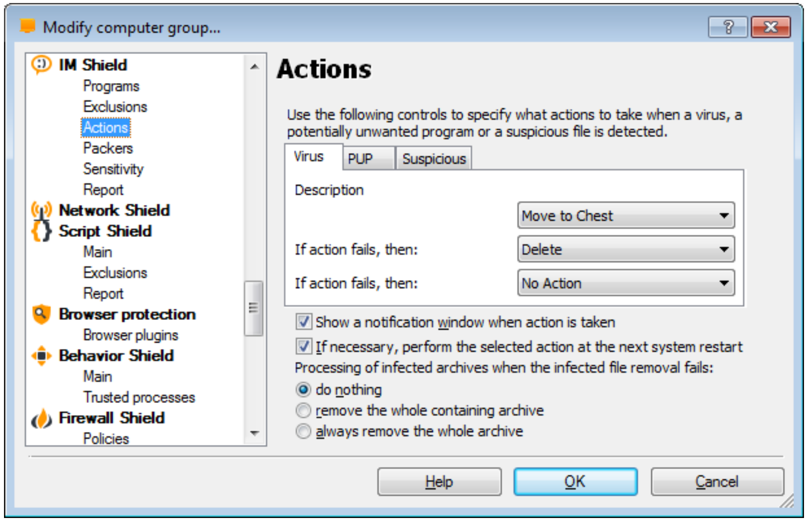
- Alternatively, you can select an action which avast! will attempt to carry out automatically:
  - **Repair**
  - **Move to Chest**
  - **Delete**

  If any action is selected, you can then specify an alternative action to be taken if the first action fails.

AEA console

Computer catalog

IM Shield



Actions

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

Description: Move to Chest

If action fails, then: Delete

If action fails, then: No Action

☑ Show a notification window when action is taken

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

Processing of infected archives when the infected file removal fails:

● do nothing

○ remove the whole containing archive

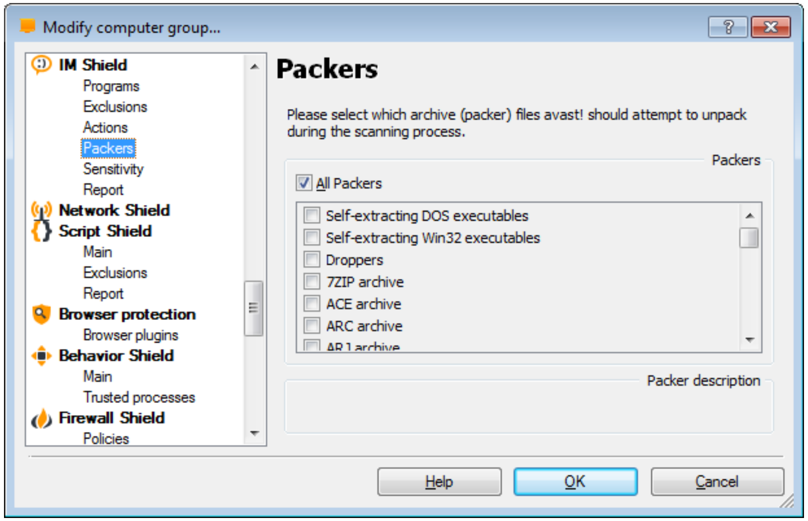
○ always remove the whole archive

- Options:
  - 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.

AEA console

Computer catalog

IM Shield



Packers

Please select which archive (packer) files avast! should attempt to unpack during the scanning process.

Packers

☑ All Packers

□ Self-extracting DOS executables
□ Self-extracting Win32 executables
□ Droppers
□ 7ZIP archive
□ ACE archive
□ ARC archive
□ ARJ archive

Packer description

- On this page, you can specify which types of archive file are checked when scanning. Certain file types are scanned by default but you can also specify other types that should be scanned by checking the appropriate box.

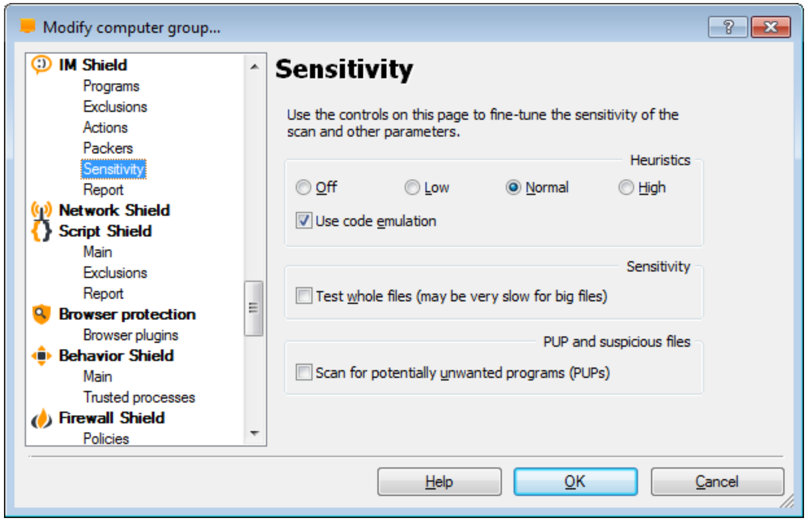
- By clicking once on any of the default file types in the list, you can see a description of that particular type of file at the bottom of the page.

- If you want all archive files to be scanned, check the box "**All packers**", however, this may significantly increase the scanning time.

AEA console

Computer catalog

IM Shield



Modify computer group...

Sensitivity

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

Heuristics

○ Off ○ Low ● Normal ○ High

☑ Use code emulation

Sensitivity

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

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

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

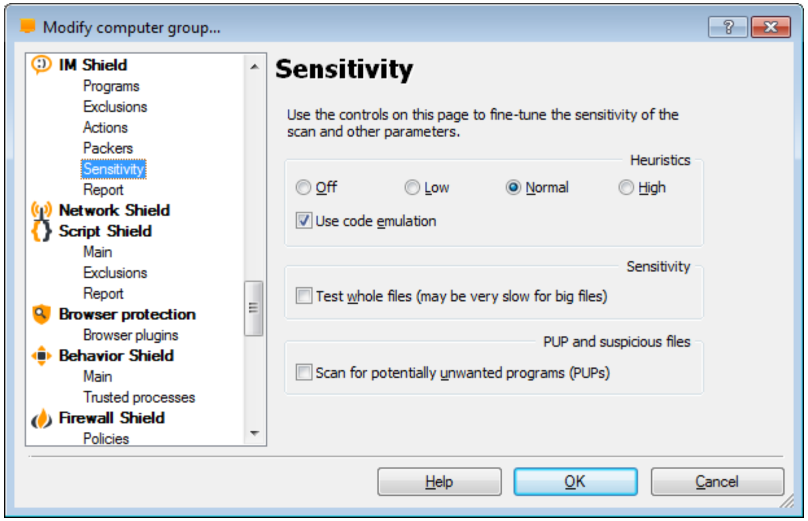
- As well as the standard process of scanning for known malware infections, avast! also performs a heuristic analysis to identify potential, but as yet unknown malware. This is done by looking for certain characteristics that may be a sign of a potential infection. By clicking on the orange bars, you 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 are 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.

AEA console

Computer catalog

IM Shield



Sensitivity

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

Heuristics

○ Off ○ Low ● Normal ○ High

☑ Use code emulation

Sensitivity

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

PUP and suspicious files

□ Scan for potentially unwanted programs (PUPs)

- 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 unchecking the following boxes:

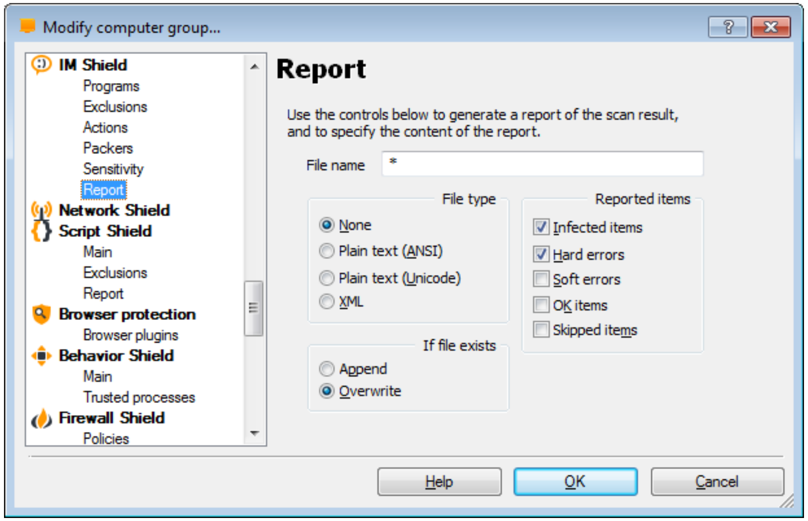
  – **Test whole files (may be very slow for big files)** - checking this box will result in scanned files being tested fully, not just those parts of a file which are normally affected by viruses. Most viruses are normally found either at the beginning of a file, or at the end. Checking this box will 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.

AEA console

Computer catalog

IM Shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name: *

File type
- ● None
- ○ Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

If file exists
- ○ Append
- ● Overwrite

Reported items
- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

On this page you can create a report of the scan results. You can specify whether you want the report to be created as a plain text file, or in XML format.

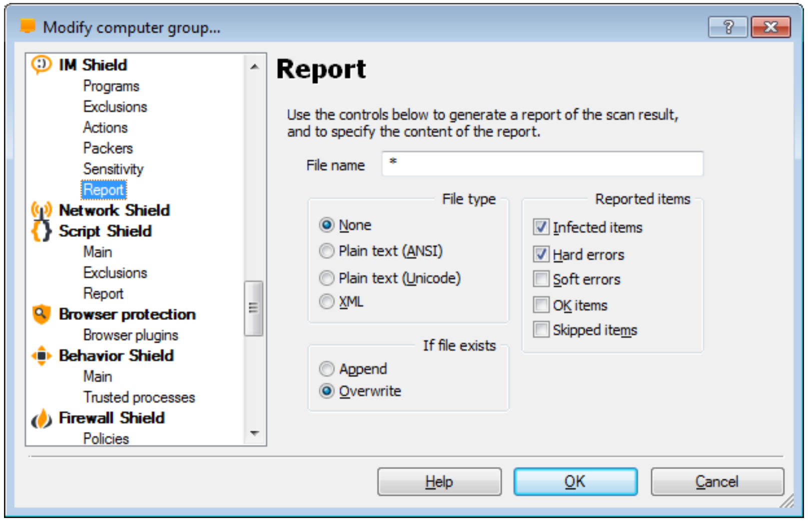
- If you want to create a new report after each scan, and you don't want to keep a record of previous scan results, select "overwrite". A new report will then be created after each scan and will replace any previous report.

- If you want to keep the previous scan results, select "Append" and the results of the new scan will be added to the end of the previous report.

AEA console

Computer catalog

IM Shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name *

File type
- ● None
- ○ Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

If file exists
- ○ Append
- ● Overwrite

Reported items
- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

Reported items:

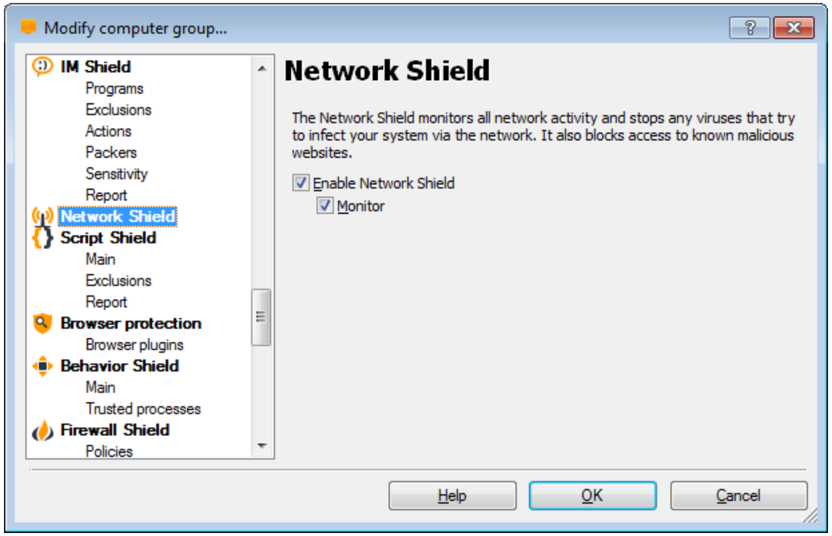
- **Infected items** - files that potentially contain a virus or other malware infection
- **Hard errors** - these arise when the program detects something that would not normally be expected and generally require further investigation.
- **Soft errors** - these are less serious than hard errors and usually concern files that could not be scanned, for example, because they were open and being used by another application.
- **OK items** - these are files that were scanned where nothing suspicious was detected. If all local drives are scanned, checking this box could produce a very long report. It is recommended to check this box only if you intend to carry out a limited scan and only if you really want all clean files to be reported as well as any problematic files.
- **Skipped items** - these are files that were not scanned as a result of the scan settings, for example, if it was specified that only files with specific extension should be scanned or if certain files were specifically excluded from the scan.

NETWORK SHIELD

AEA console

Computer catalog

Network Shield



Modify computer group...

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.

☑ Enable Network Shield

☑ Monitor

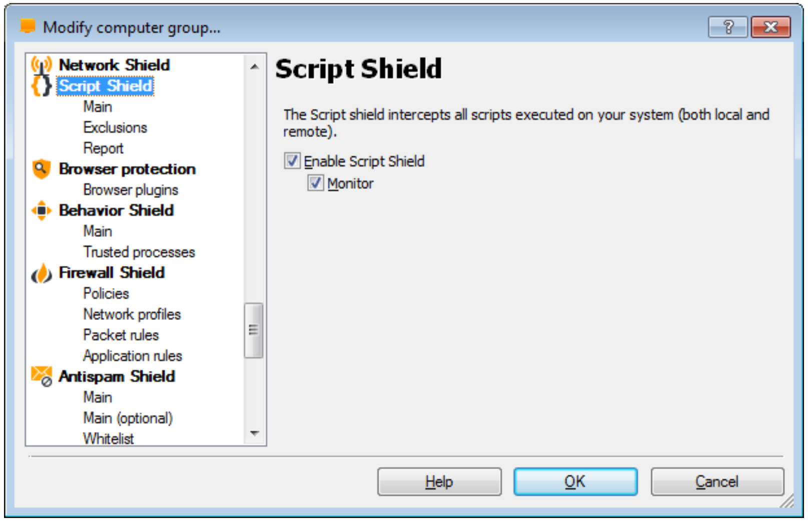
- Provides protection against network-based viruses. This module has two main components: a URL blocker, designed to block malicious URLs (as defined by the Virus Lab), and a lightweight intrusion-detection system.

SCRIPT SHIELD

AEA console

Computer catalog

Script Shield


Modify computer group...

Script Shield

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

☑ Enable Script Shield

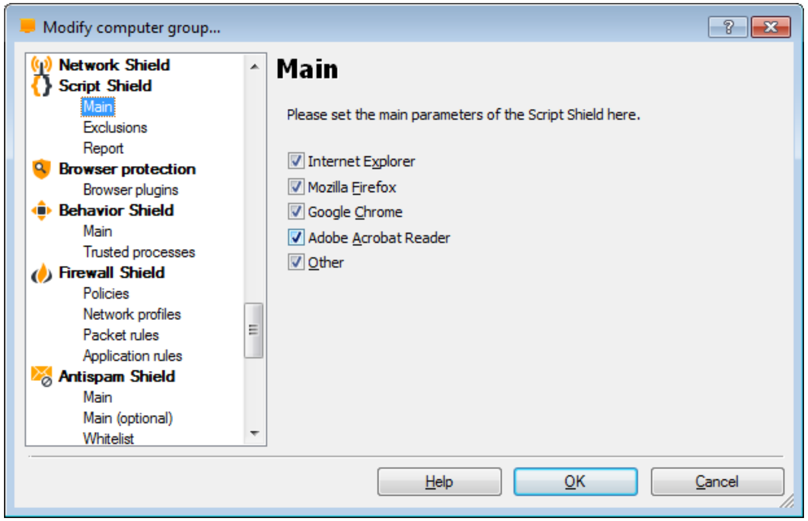
☑ Monitor

- Detects malicious scripts hidden in internet web pages and prevents them from running and hijacking or potentially causing damage to your computer.

AEA console

Computer catalog

Script Shield



Main

Please set the main parameters of the Script Shield here.

☑ Internet Explorer

☑ Mozilla Firefox

☑ Google Chrome

☑ Adobe Acrobat Reader

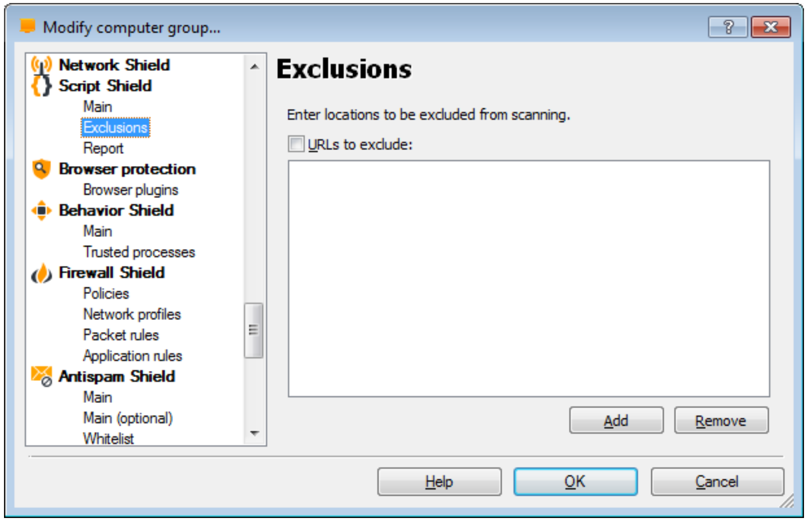
☑ Other

- You can select which browsers should be protected by Script Shield…

AEA console

Computer catalog

Script Shield



Modify computer group...

- Network Shield
- Script Shield
  - Main
  - Exclusions
  - Report
- Browser protection
  - Browser plugins
- Behavior Shield
  - Main
  - Trusted processes
- Firewall Shield
  - Policies
  - Network profiles
  - Packet rules
  - Application rules
- Antispam Shield
  - Main
  - Main (optional)
  - Whitelist

Exclusions

Enter locations to be excluded from scanning.

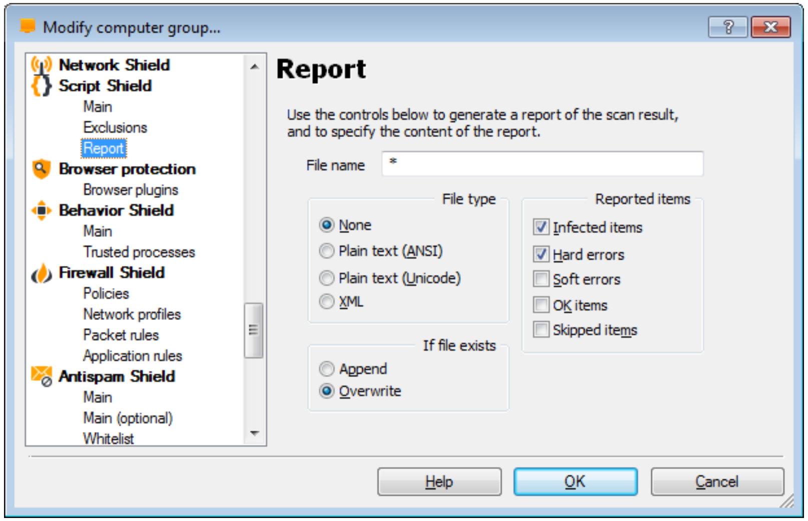
□ URLs to exclude:

- and here you can specify any URLs that should not be scanned.

AEA console

Computer catalog

Script Shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name: *

File type
- ● None
- ○ Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

Reported items
- ☑ Infected items
- ☑ Hard errors
- ☐ Soft errors
- ☐ OK items
- ☐ Skipped items

If file exists
- ○ Append
- ● Overwrite

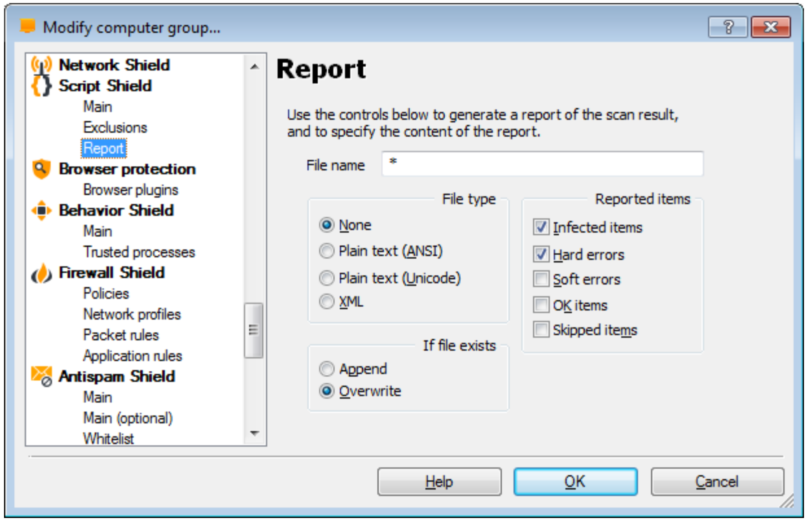
On this page you can create a report of the scan results. You can specify whether you want the report to be created as a plain text file, or in XML format.

- If you want to create a new report after each scan, and you don't want to keep a record of previous scan results, select "overwrite". A new report will then be created after each scan and will replace any previous report.
- If you want to keep the previous scan results, select "Append" and the results of the new scan will be added to the end of the previous report.

AEA console

Computer catalog

Script Shield



Report

Use the controls below to generate a report of the scan result, and to specify the content of the report.

File name: *

File type
- ● None
- ○ Plain text (ANSI)
- ○ Plain text (Unicode)
- ○ XML

Reported items
- ☑ Infected items
- ☑ Hard errors
- □ Soft errors
- □ OK items
- □ Skipped items

If file exists
- ○ Append
- ● Overwrite

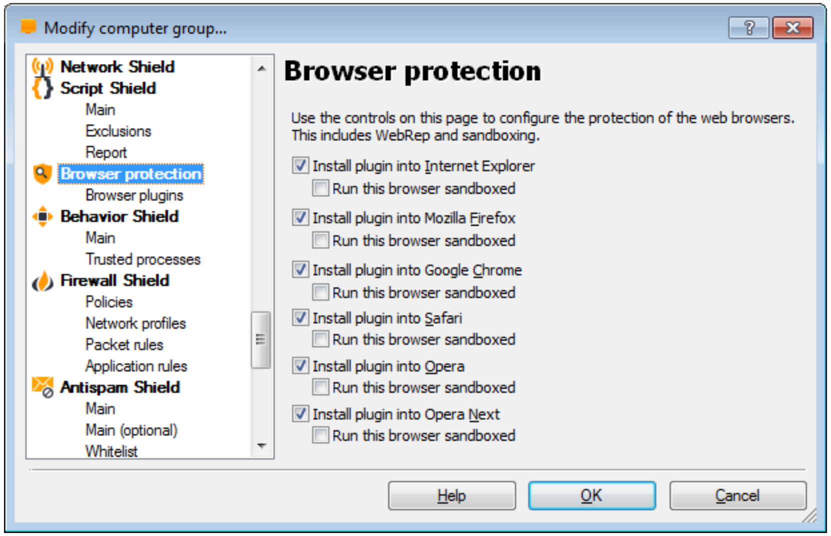
Reported items:

- **Infected items** - files that potentially contain a virus or other malware infection
- **Hard errors** - these arise when the program detects something that would not normally be expected and generally require further investigation.
- **Soft errors** - these are less serious than hard errors and usually concern files that could not be scanned, for example, because they were open and being used by another application.
- **OK items** - these are files that were scanned where nothing suspicious was detected. If all local drives are scanned, checking this box could produce a very long report. It is recommended to check this box only if you intend to carry out a limited scan and only if you really want all clean files to be reported as well as any problematic files.
- **Skipped items** - these are files that were not scanned as a result of the scan settings, for example, if it was specified that only files with specific extension should be scanned or if certain files were specifically excluded from the scan.

BROWSER PROTECTION

AEA console

Computer catalog



Browser protection

Use the controls on this page to configure the protection of the web browsers. This includes WebRep and sandboxing.

☑ Install plugin into Internet Explorer
  □ Run this browser sandboxed
☑ Install plugin into Mozilla Firefox
  □ Run this browser sandboxed
☑ Install plugin into Google Chrome
  □ Run this browser sandboxed
☑ Install plugin into Safari
  □ Run this browser sandboxed
☑ Install plugin into Opera
  □ Run this browser sandboxed
☑ Install plugin into Opera Next
  □ Run this browser sandboxed

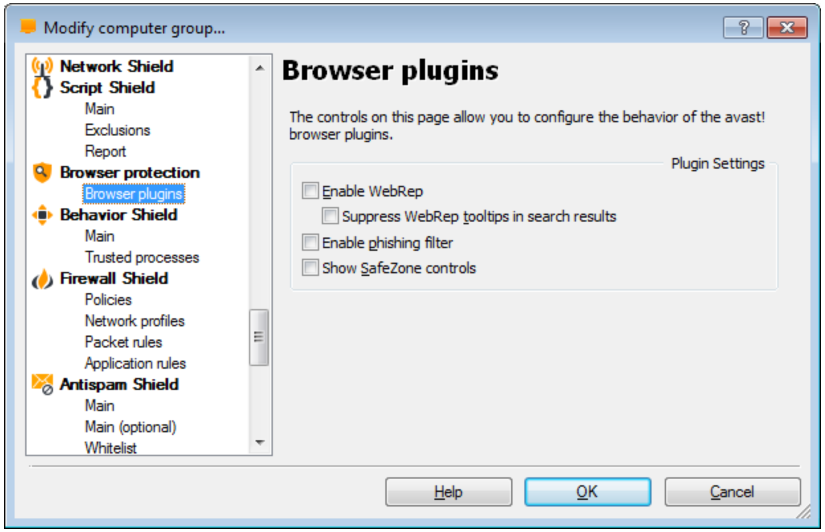
Browser Protection

- Use the controls on this page to configure the additional web browser plug-ins (such as the avast WebRep) and whether they should be run automatically in the Sandbox.

AEA console

Computer catalog

Browser Protection



Browser plugins

The controls on this page allow you to configure the behavior of the avast! browser plugins.

Plugin Settings

- □ Enable WebRep
  - □ Suppress WebRep tooltips in search results
- □ Enable phishing filter
- □ Show SafeZone controls

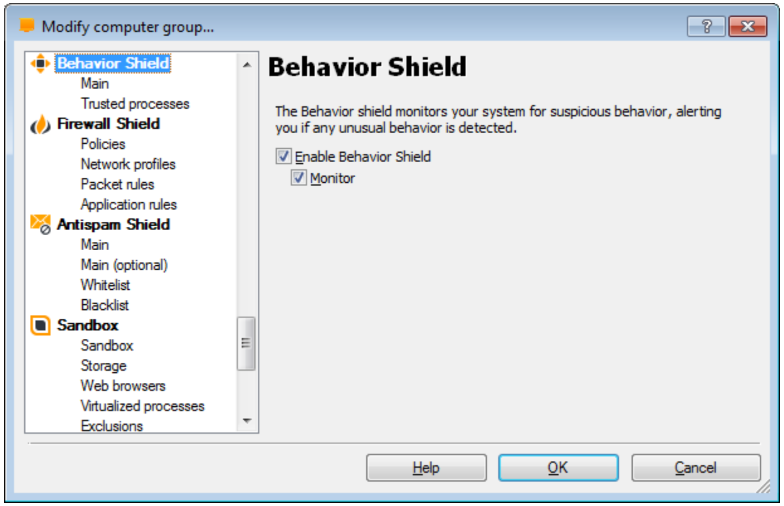
- The controls on this page allow you to configure the behavior of the avast! Browser plugins.
  - WebRep
  - Phishing filter
  - Safezone controls

BEHAVIOR SHIELD

AEA console

Computer catalog

Behavior Shield



Behavior Shield

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

☑ Enable Behavior Shield

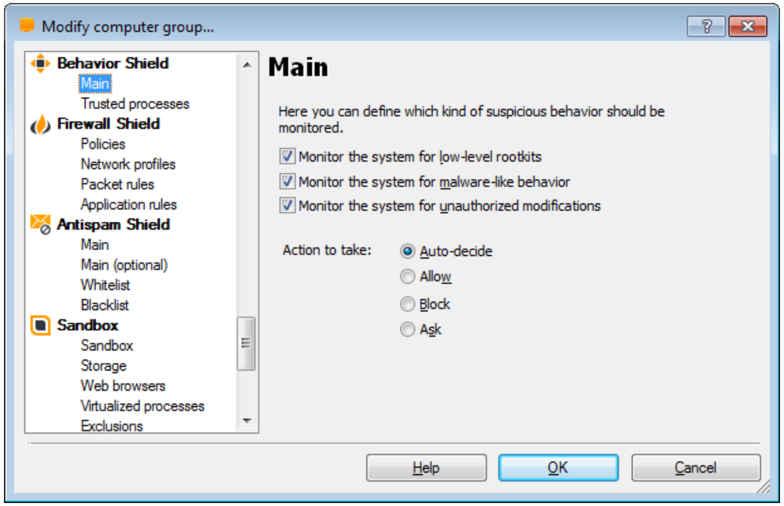
☑ Monitor

- **Behavior shield – real-time shields**
  - Monitors activity on your computer using a number of sensors (file system, registry and network based) and reports/blocks any suspicious behavior.

AEA console

Computer catalog

Behavior Shield



Main

Here you can define which kind of suspicious behavior should be monitored.

☑ Monitor the system for low-level rootkits
☑ Monitor the system for malware-like behavior
☑ Monitor the system for unauthorized modifications

Action to take:
● Auto-decide
○ Allow
○ Block
○ Ask

The Behavior shield can monitor your system for:

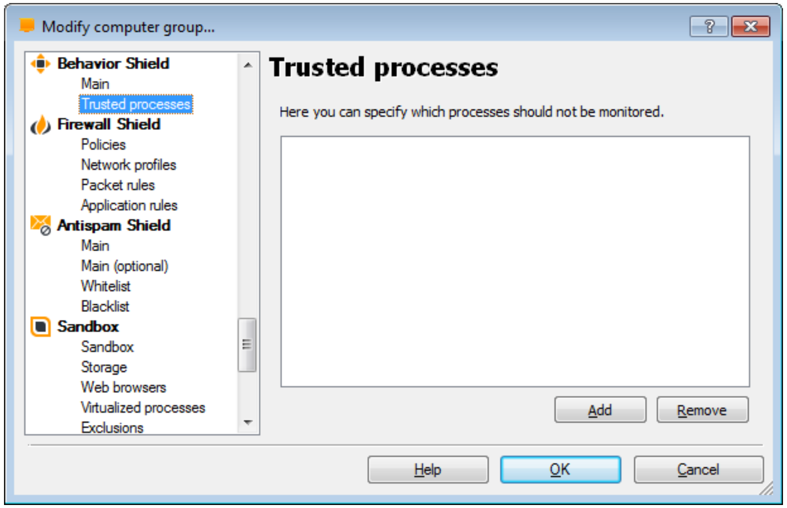
- low-level rootkits
- malware-like behavior
- unauthorized modifications

And you can specify the response if such a potential threat is detected, e.g. whether it is allowed or blocked.

AEA console

Computer catalog

Behavior Shield



Trusted processes

Here you can specify which processes should not be monitored.

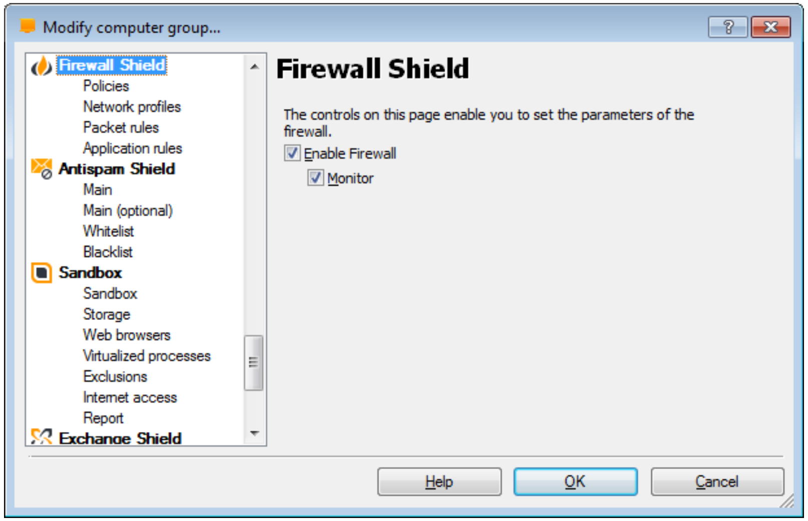
- Here you can specify which processes should not be monitored.
- Browse the harddrive to locate *.exe file/s which is then treated as a trusted application.

FIREWALL SHIELD

AEA console

Computer catalog

Firewall Shield



Firewall Shield

The controls on this page enable you to set the parameters of the firewall.

☑ Enable Firewall

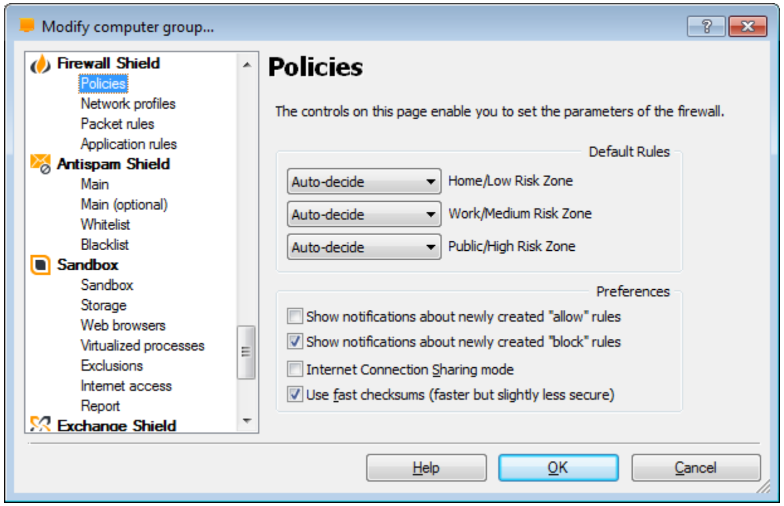
☑ Monitor

- Stops hackers, using heuristic and behavioral analysis and a white list of safe applications.
  - Blocks hacker attacks
  - Secures sensitive data
  - Secures identity information

AEA console

Computer catalog

Firewall Shield



Policies

The controls on this page enable you to set the parameters of the firewall.

Default Rules

Auto-decide Home/Low Risk Zone

Auto-decide Work/Medium Risk Zone

Auto-decide Public/High Risk Zone

Preferences

☐ Show notifications about newly created "allow" rules

☑ Show notifications about newly created "block" rules

☐ Internet Connection Sharing mode

☑ Use fast checksums (faster but slightly less secure)

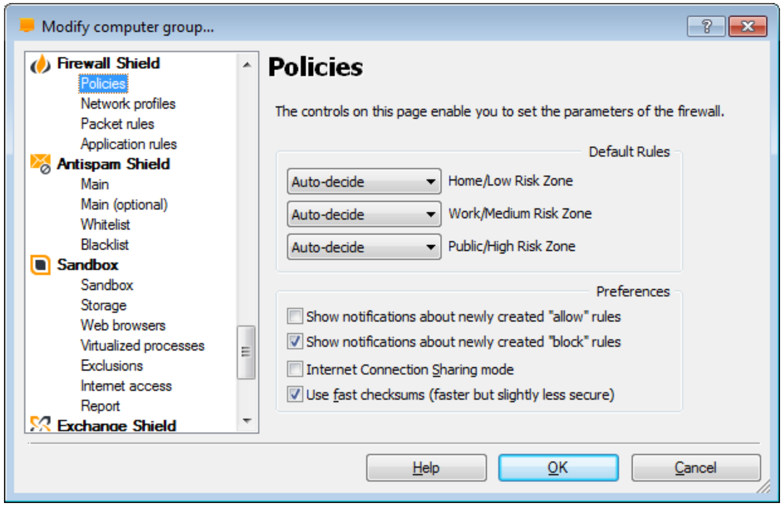
On the Firewall settings page, you can adjust the firewall security settings to limit external connections according to the environment in which the computer is being used.

- Home/low risk zone - suitable when using your computer as part of a home/private network. If this setting is selected, the firewall will allow all communication with the network.
- Work/medium risk zone - suitable for when your computer is connected to a wider public network, including direct connections to the internet. This is the default setting and if selected, the firewall will allow communication in and out only if allowed by the "Application Rules". If no rule has been created, you will be asked to confirm whether or not communication with a particular application should be allowed.
- Public/high risk zone - suitable when using your computer to connect to a public network and where you want to ensure the maximum level of security. This is the most secure setting and if selected, no incoming communication will be allowed, effectively making your computer completely invisible to others.

AEA console

Computer catalog

Firewall Shield



Policies

The controls on this page enable you to set the parameters of the firewall.

Default Rules

- Auto-decide — Home/Low Risk Zone
- Auto-decide — Work/Medium Risk Zone
- Auto-decide — Public/High Risk Zone

Preferences

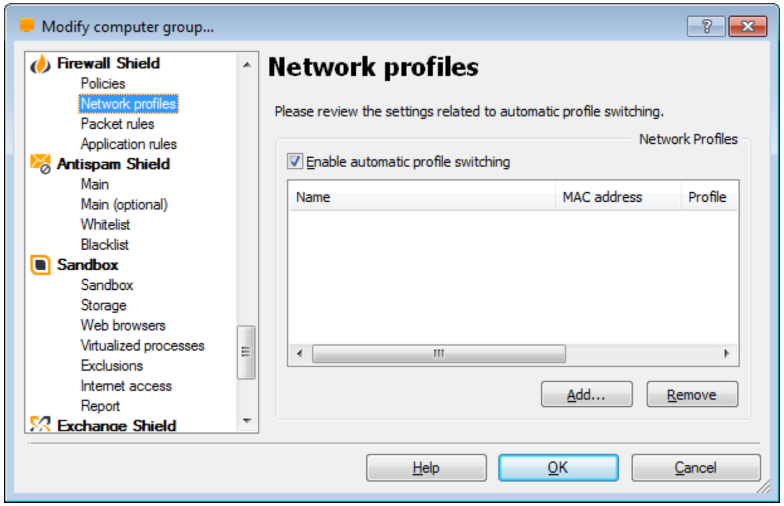
- □ Show notifications about newly created "allow" rules
- ☑ Show notifications about newly created "block" rules
- □ Internet Connection Sharing mode
- ☑ Use fast checksums (faster but slightly less secure)

- **Internet Connection Sharing (ICS) mode**
  - check only if computer acts as gateway between the Internet and other computers
- **Use fast checksums - checksums (or hashes)**
  - are used to identify the applications defined on the Application Rules page.
  - If the calculated checksum does not match the checksum that is stored for an application, it will be treated as a new application.

AEA console

Computer catalog

Firewall Shield



Modify computer group...

Network profiles

Please review the settings related to automatic profile switching.

Network Profiles

☑ Enable automatic profile switching

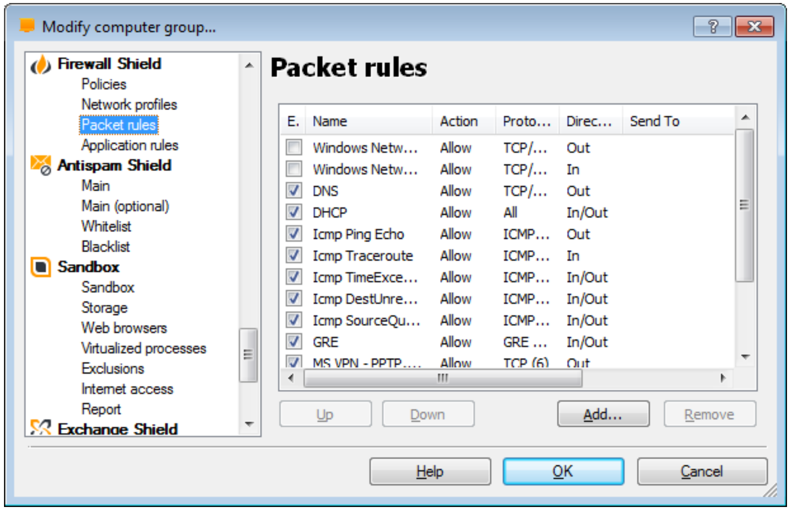
Name	MAC address	Profile

- Profile will be changed automatically when a new network is detected, if the new network corresponds with one of the networks in the table.
- If a profile has been specified for a particular network, the network and its corresponding profile will be listed on this page.
- When a new network is detected, you will be asked to specify the new network profile.

AEA console

Computer catalog

Firewall Shield



Packet rules

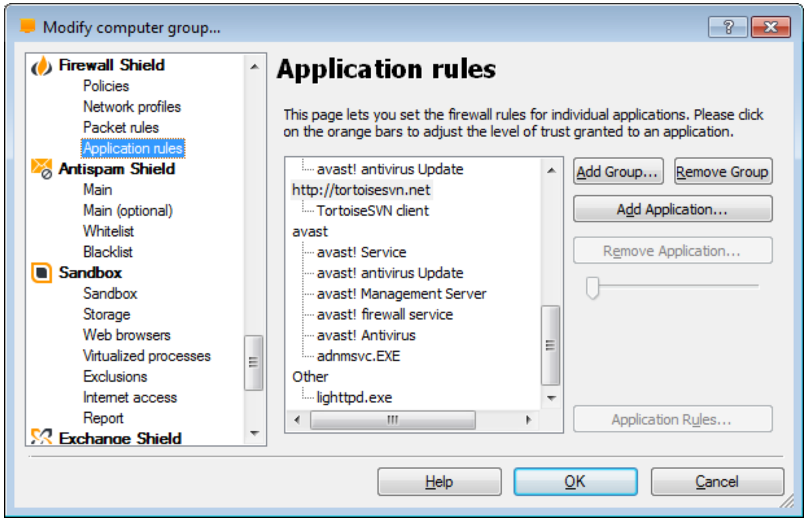
E.	Name	Action	Proto...	Direc...	Send To
☐	Windows Netw...	Allow	TCP/...	Out	
☐	Windows Netw...	Allow	TCP/...	In	
☑	DNS	Allow	TCP/...	Out	
☑	DHCP	Allow	All	In/Out	
☑	Icmp Ping Echo	Allow	ICMP...	Out	
☑	Icmp Traceroute	Allow	ICMP...	In	
☑	Icmp TimeExce...	Allow	ICMP...	In/Out	
☑	Icmp DestUnre...	Allow	ICMP...	In/Out	
☑	Icmp SourceQu...	Allow	ICMP...	In/Out	
☑	GRE	Allow	GRE ...	In/Out	
☑	MS VPN - PPTP....	Allow	TCP (6)	Out	

- Expert users can also review the list of low-level (packet) rules of the firewall.

AEA console

Computer catalog

Firewall Shield



Application rules

This page lets you set the firewall rules for individual applications. Please click on the orange bars to adjust the level of trust granted to an application.

avast! antivirus Update
http://tortoisesvn.net
TortoiseSVN client
avast
avast! Service
avast! antivirus Update
avast! Management Server
avast! firewall service
avast! Antivirus
adnmsvc.EXE
Other
lighttpd.exe

- Default rules are created automatically for software applications from trusted sources when they are started for the first time.

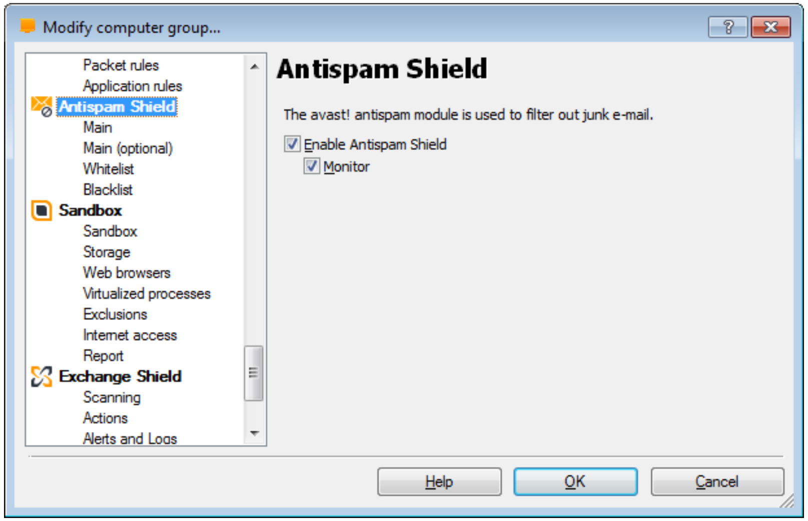
- For detailed information see the following article on the avast! web site: https://support.avast.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=482

ANTISPAM SHIELD

AEA console

Computer catalog

Antispam Shield



Modify computer group...

Antispam Shield

The avast! antispam module is used to filter out junk e-mail.

☑ Enable Antispam Shield

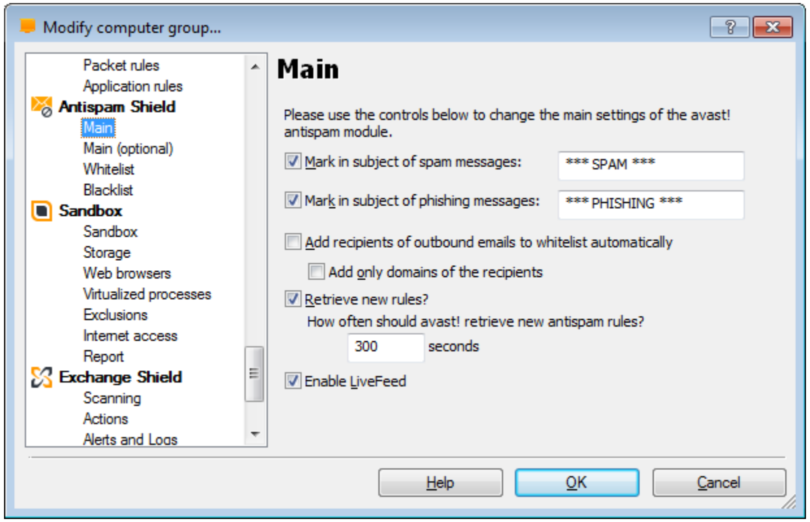
☑ Monitor

- Comprehensive spam and phishing filter, which works as a plug-in to MS Outlook and a generic POP3/IMAP4 proxy for other email clients.

AEA console

Computer catalog

Antispam Shield



Main

Please use the controls below to change the main settings of the avast! antispam module.

☑ Mark in subject of spam messages: *** SPAM ***

☑ Mark in subject of phishing messages: *** PHISHING ***

□ Add recipients of outbound emails to whitelist automatically

□ Add only domains of the recipients

☑ Retrieve new rules?

How often should avast! retrieve new antispam rules? 300 seconds

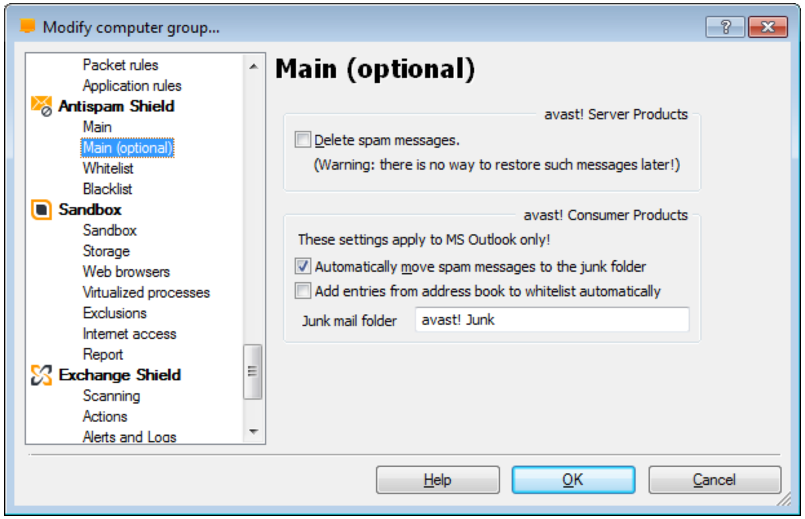
☑ Enable LiveFeed

- You can add a mark in the subject of spam and phishing messages.
- You can also add recipients of outgoing emails, or the recipient’s domain name, to the whitelist of trusted addresses.
- **Retrieve new rules?**
  - Here you can specify how often avast! checks for updates to the rules that are used to identify potential spam.
  - Default timer set to 5 minutes.
- **Enable LiveFeed**
  - All incoming emails are checked against an online database of global spam messages before carrying out the heuristic and other checks.
  - The majority of spam messages are detected this way, so it is recommended to leave this box checked.

AEA console

Computer catalog

Antispam Shield



Main (optional)

avast! Server Products

□ Delete spam messages.
(Warning: there is no way to restore such messages later!)

avast! Consumer Products

These settings apply to MS Outlook only!

☑ Automatically move spam messages to the junk folder

□ Add entries from address book to whitelist automatically

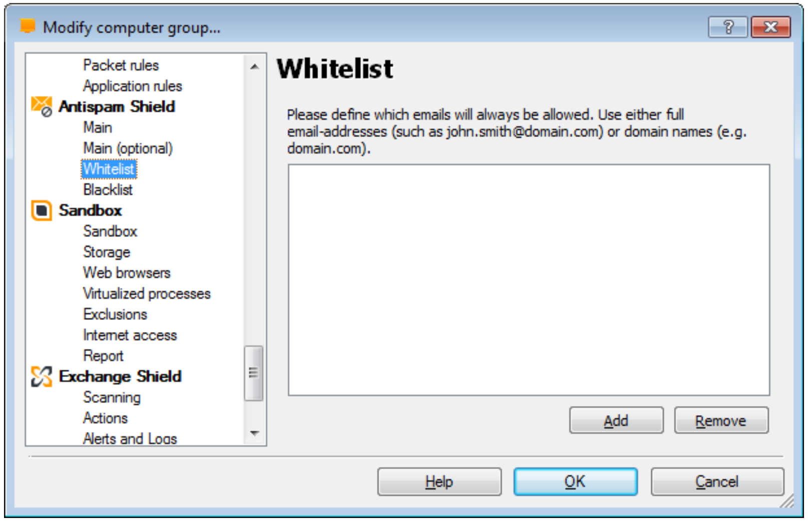
Junk mail folder: avast! Junk

- Use the controls on this page to separately configure the protection for Server products and Consumer (client) products.

AEA console

Computer catalog

Antispam Shield



Whitelist

Please define which emails will always be allowed. Use either full email-addresses (such as john.smith@domain.com) or domain names (e.g. domain.com).

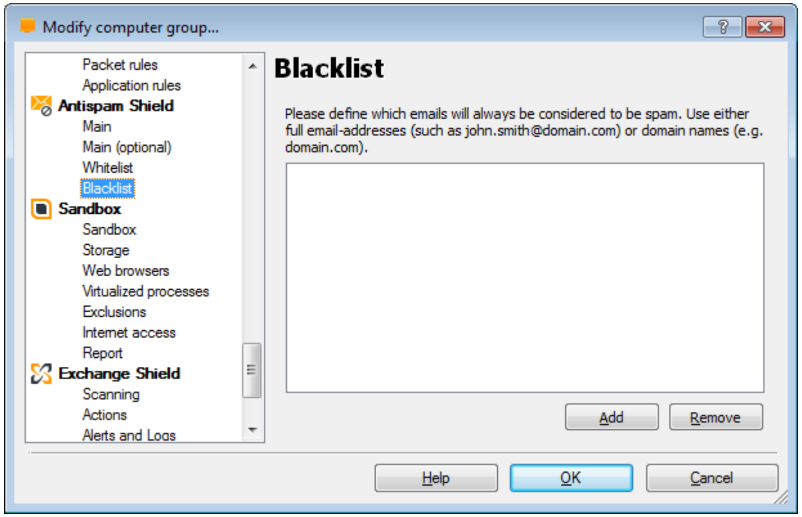
- By clicking on the box provided, you can enter the email addresses of senders from whom email will not be treated as spam and will always be delivered as normal. You can enter the specific email address, e.g. jim.frost@gmail.com , or if you enter the domain name only (e.g. domain.com), all emails from that domain will then be allowed.

- To remove an email address from the whitelist, click on it once and then click "Remove".

AEA console

Computer catalog

Antispam Shield



Modify computer group...

Blacklist

Please define which emails will always be considered to be spam. Use either full email-addresses (such as john.smith@domain.com) or domain names (e.g. domain.com).

- By clicking on the box provided, you can enter the email addresses of senders from whom email will always be treated as spam. You can enter the specific email address, e.g. jim.frost@gmail.com , or if you enter the domain name only (e.g. domain.com), all emails from that domain will be treated as spam.

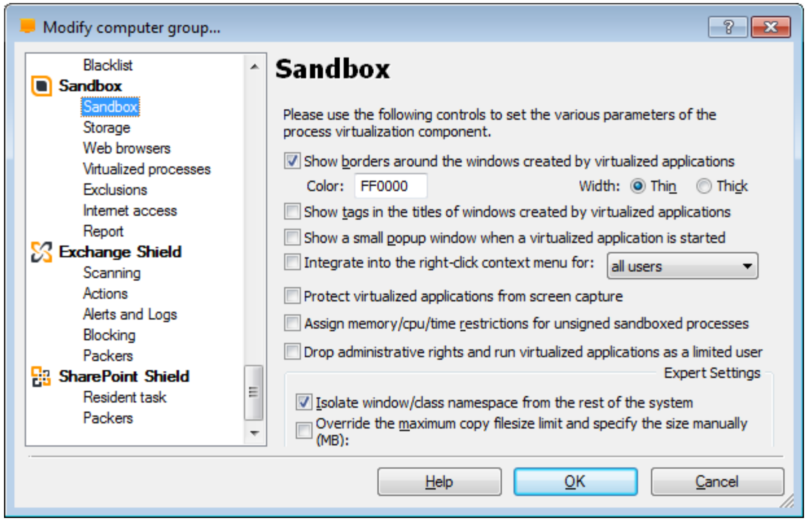
- To remove an email address from the blacklist, click on it once and then click "Remove".

SANDBOX

AEA console

Computer catalog

Sandbox



Sandbox

Please use the following controls to set the various parameters of the process virtualization component.

☑ Show borders around the windows created by virtualized applications

Color: FF0000 Width: ● Thin ○ Thick

□ Show tags in the titles of windows created by virtualized applications

□ Show a small popup window when a virtualized application is started

□ Integrate into the right-click context menu for: all users

□ Protect virtualized applications from screen capture

□ Assign memory/cpu/time restrictions for unsigned sandboxed processes

□ Drop administrative rights and run virtualized applications as a limited user

Expert Settings

☑ Isolate window/class namespace from the rest of the system

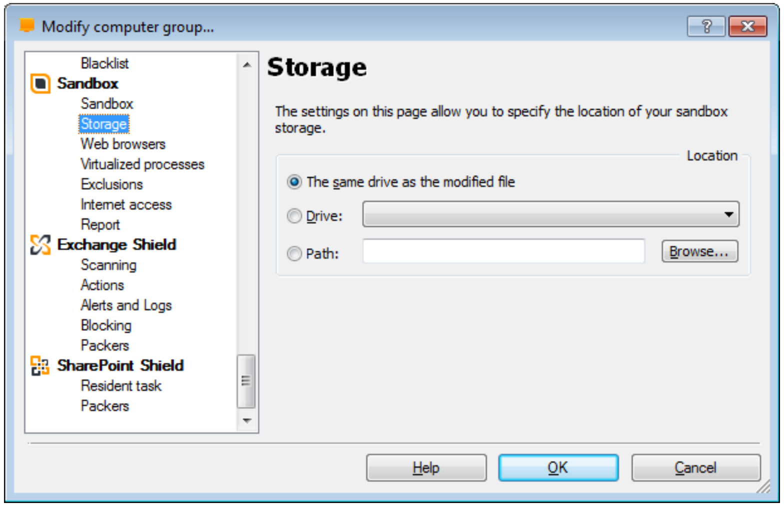
□ Override the maximum copy filesize limit and specify the size manually (MB):

- Here you can set the various parameters of the Sandbox.

AEA console

Computer catalog

Sandbox



Storage

The settings on this page allow you to specify the location of your sandbox storage.

Location

● The same drive as the modified file

○ Drive:

○ Path: Browse...

- **Store files in special storage in the sandbox (contents will not be automatically deleted)**
  - Normally, whenever an application is launched in the sandbox, avast! creates a special sandbox storage area for that application and where virtualized files/folders are saved.

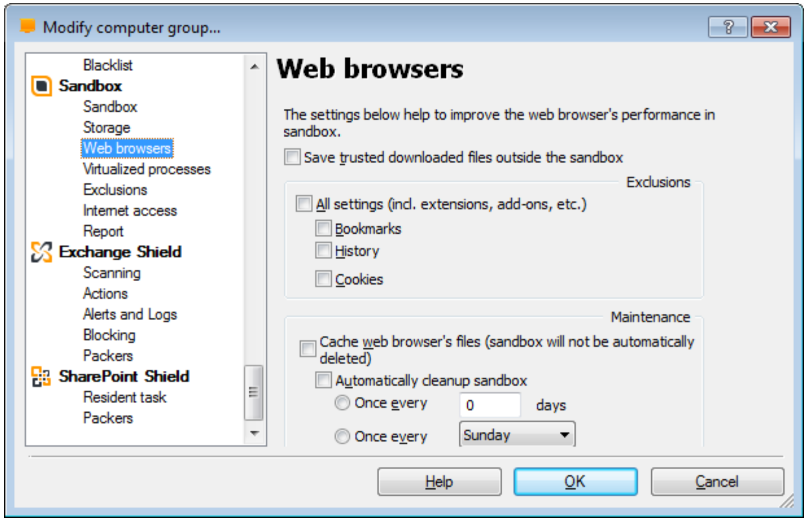
- **Sandbox storage**
  - Hidden folder on the root of drive **C:\## aswSnx private storage**

This sandbox storage is then normally deleted when the application is terminated. If the box "Store files in special storage in the sandbox..." is checked, a completely separate sandbox storage will be used for web browsers and this will not be automatically deleted when the browser is terminated. This means that the next time the browser is launched, it will use the same sandbox storage from the previous browser session, which will therefore improve the browser's performance.

AEA console

Computer catalog

Sandbox



Web browsers

The settings below help to improve the web browser's performance in sandbox.

□ Save trusted downloaded files outside the sandbox

Exclusions

□ All settings (incl. extensions, add-ons, etc.)

□ Bookmarks

□ History

□ Cookies

Maintenance

□ Cache web browser's files (sandbox will not be automatically deleted)

□ Automatically cleanup sandbox

○ Once every 0 days

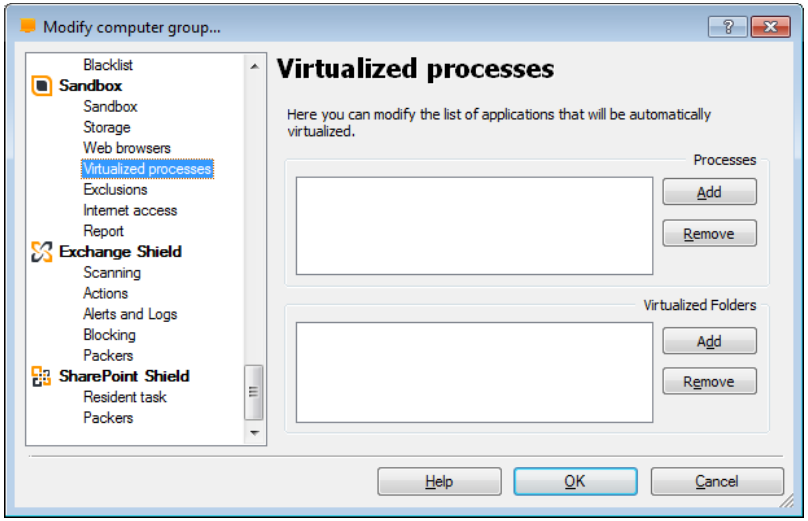
○ Once every Sunday

- **These settings can help to improve the web browser‘s performance in the sandbox.**
  - Under “Exclusions”, you can specify that some options should not be virtualized when running your web browser in the sandbox e.g. bookmarks, browsing history, and cookies
  - these options will not be virtualized and will be available to any other browsing sessions which are open or which are opened later, whether inside the sandbox or outside.

AEA console

Computer catalog

Sandbox



Modify computer group...

Blacklist

Sandbox

Sandbox

Storage

Web browsers

Virtualized processes

Exclusions

Internet access

Report

Exchange Shield

Scanning

Actions

Alerts and Logs

Blocking

Packers

SharePoint Shield

Resident task

Packers

Virtualized processes

Here you can modify the list of applications that will be automatically virtualized.

Processes

Add

Remove

Virtualized Folders

Add

Remove

Help OK Cancel

- List of specific files or/and applications, that will be automatically virtualized.

- Browse to locate and select a file or path that should always be run inside the sandbox.

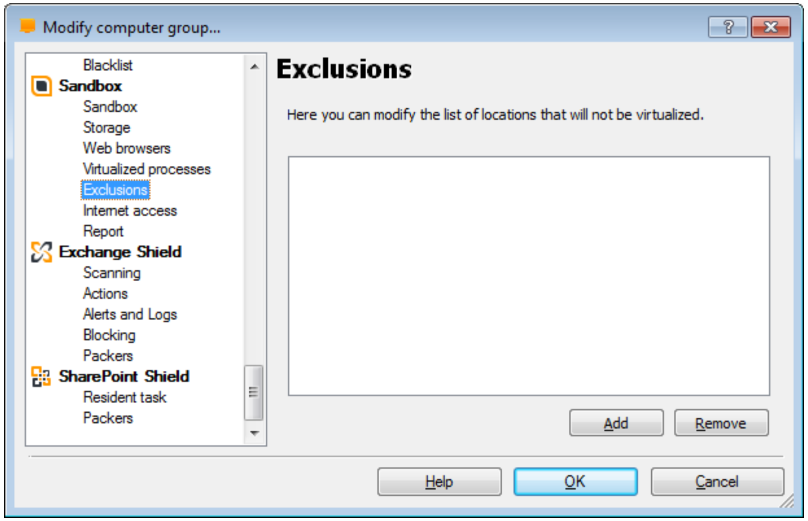
- To remove a file or path from the sandbox, just

click the Remove button.

AEA console

Computer catalog

Sandbox



Modify computer group...

- Blacklist
- Sandbox
  - Sandbox
  - Storage
  - Web browsers
  - Virtualized processes
  - Exclusions
  - Internet access
  - Report
- Exchange Shield
  - Scanning
  - Actions
  - Alerts and Logs
  - Blocking
  - Packers
- SharePoint Shield
  - Resident task
  - Packers

Exclusions

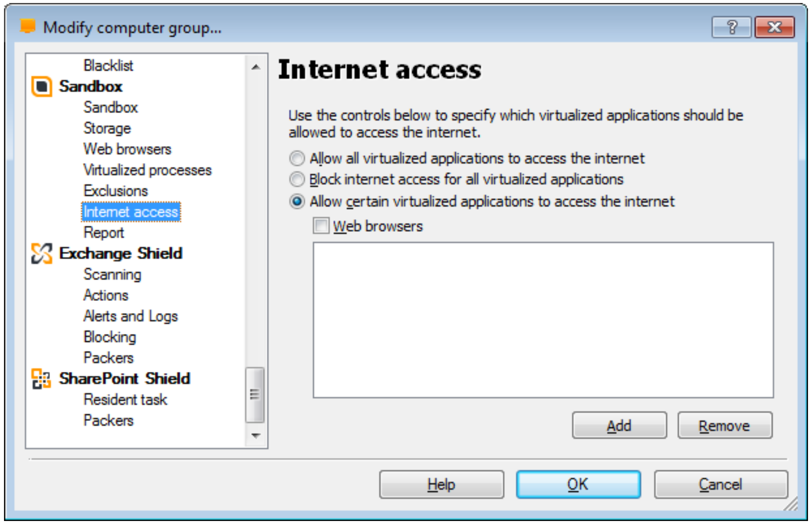
Here you can modify the list of locations that will not be virtualized.

- On this page you can specify files that should never be run virtualized. Just click on the browse button and then locate and select the file or path that should be excluded. To remove a file or path from the list of exclusions, just click the Remove button.

AEA console

Computer catalog

Sandbox



Internet access

Use the controls below to specify which virtualized applications should be allowed to access the internet.

○ Allow all virtualized applications to access the internet
○ Block internet access for all virtualized applications
● Allow certain virtualized applications to access the internet
□ Web browsers

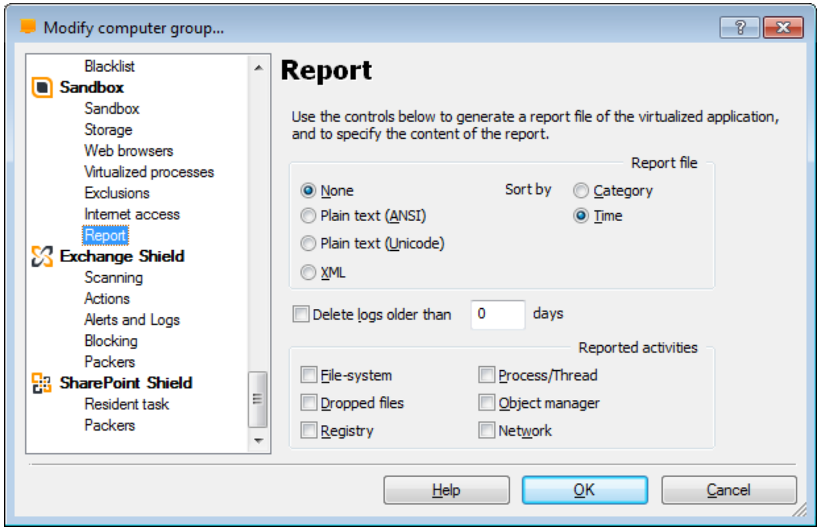
- Here you can define which (or if any) virtualized applications are allowed to access the Internet.

- It is possible to "Allow all" or to "Block all" or you can specify certain applications that will be allowed Internet access and all others will be automatically blocked. For example, you can allow access for all web browsers or you can define other specific applications by clicking in the box "Select additional applications" and using the browse button to locate and select applications that should be allowed Internet access.

AEA console

Computer catalog

Sandbox



Report

Use the controls below to generate a report file of the virtualized application, and to specify the content of the report.

Report file

● None
○ Plain text (ANSI)
○ Plain text (Unicode)
○ XML

Sort by ○ Category ● Time

□ Delete logs older than 0 days

Reported activities

□ File-system
□ Dropped files
□ Registry
□ Process/Thread
□ Object manager
□ Network

- On this screen you can specify that a report should be created after an application is run in virtualization mode. You can specify the type of report file (plain text or xml) and the period for which the report should be retained.

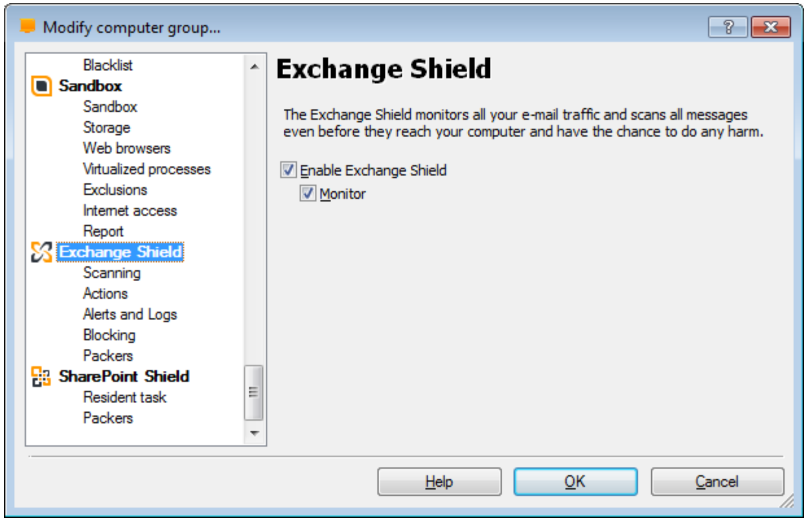
- The report will contain basic information about the application that was run in virtualized mode, the date and time the application was run in virtualized mode and details of what actions were carried out while the program was running in virtualization mode.

EXCHANGE SHIELD

AEA console

Computer catalog

Exchange Shield



Exchange Shield

The Exchange 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.

☑ Enable Exchange Shield

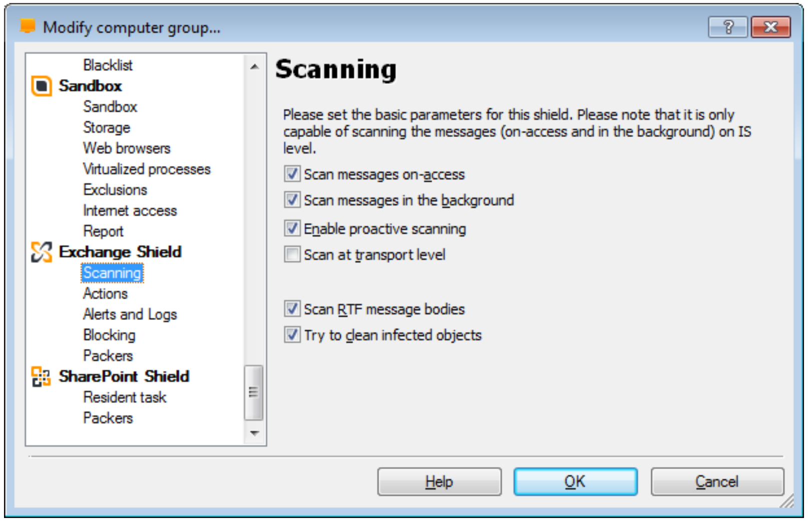
☑ Monitor

- The Exchange 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.
- It provides vital protection for your mailbox servers and ensures your data remains shielded from detrimental loss.

AEA console

Computer catalog

Exchange Shield



Scanning

Please set the basic parameters for this shield. Please note that it is only capable of scanning the messages (on-access and in the background) on IS level.

☑ Scan messages on-access

☑ Scan messages in the background

☑ Enable proactive scanning

☐ Scan at transport level

☑ Scan RTF message bodies

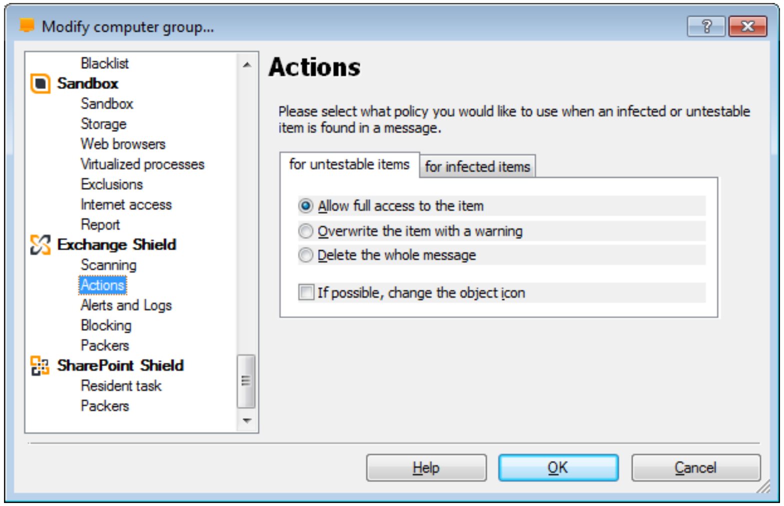
☑ Try to clean infected objects

Here you can set the basic scanning parameters.

AEA console

Computer catalog

Exchange Shield



Actions

Please select what policy you would like to use when an infected or untestable item is found in a message.

for untestable items | for infected items

● Allow full access to the item

○ Overwrite the item with a warning

○ Delete the whole message

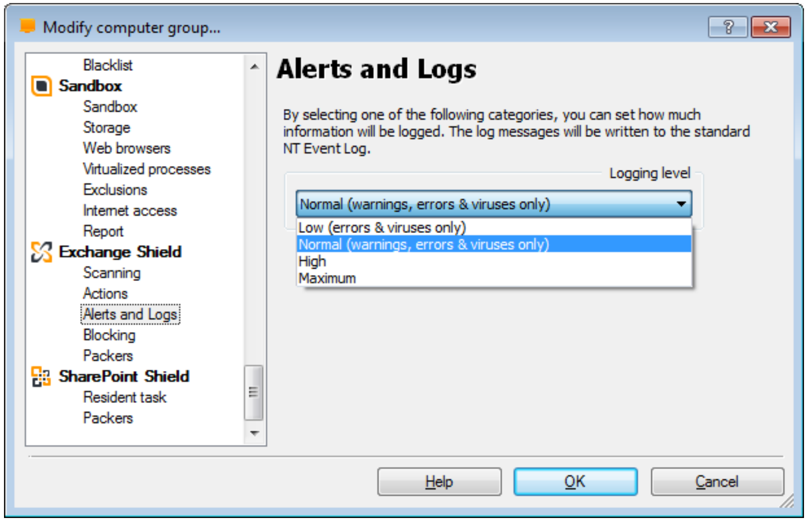
□ If possible, change the object icon

Here you can specify what action should be taken when an infected or untestable object is discovered.

AEA console

Computer catalog

Exchange Shield



Alerts and Logs

By selecting one of the following categories, you can set how much information will be logged. The log messages will be written to the standard NT Event Log.

Logging level: Normal (warnings, errors & viruses only)

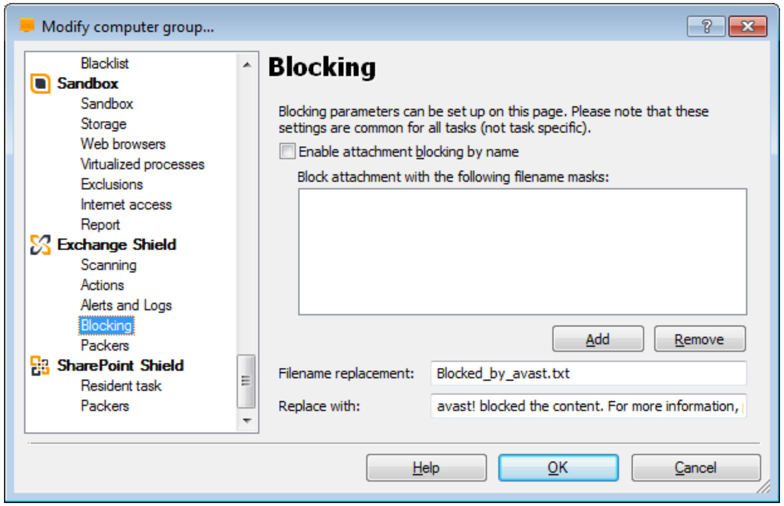
- Low (errors & viruses only)
- Normal (warnings, errors & viruses only)
- High
- Maximum

You can also specify what information will be saved to the log files e.g. only errors and viruses, or other additional less critical information as well.

AEA console

Computer catalog

Exchange Shield



Blocking

Blocking parameters can be set up on this page. Please note that these settings are common for all tasks (not task specific).

□ Enable attachment blocking by name

Block attachment with the following filename masks:

Filename replacement: Blocked_by_avast.txt

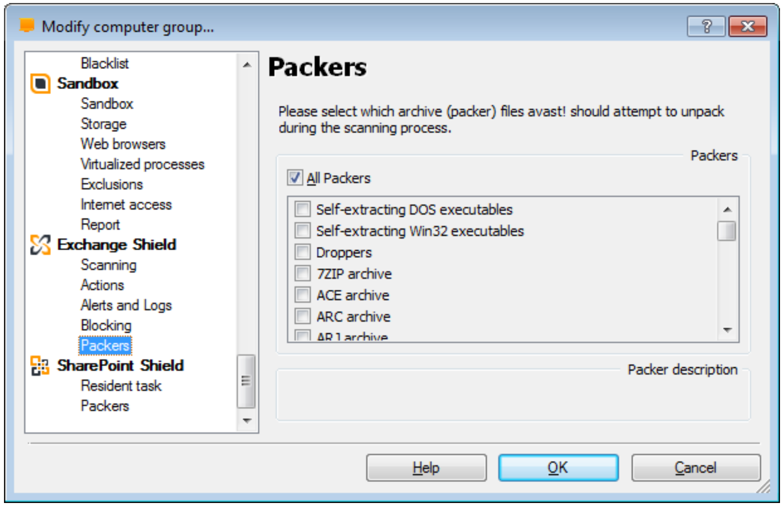
Replace with: avast! blocked the content. For more information,

And you can also block attachments with specific filename masks.

AEA console

Computer catalog

Exchange Shield



Packers

Please select which archive (packer) files avast! should attempt to unpack during the scanning process.

Packers

☑ All Packers

□ Self-extracting DOS executables
□ Self-extracting Win32 executables
□ Droppers
□ 7ZIP archive
□ ACE archive
□ ARC archive
□ ARJ archive

Packer description

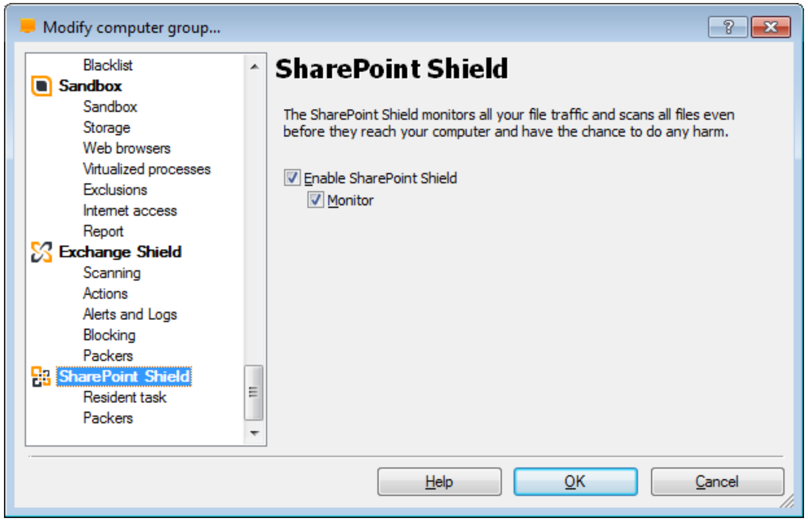
Finally, you can also select which types of archive files avast should attempt to unpack for scanning.

SHAREPOINT SHIELD

AEA console

Computer catalog

SharePoint Shield



Modify computer group...

SharePoint Shield

The SharePoint Shield monitors all your file traffic and scans all files even before they reach your computer and have the chance to do any harm.

☑ Enable SharePoint Shield

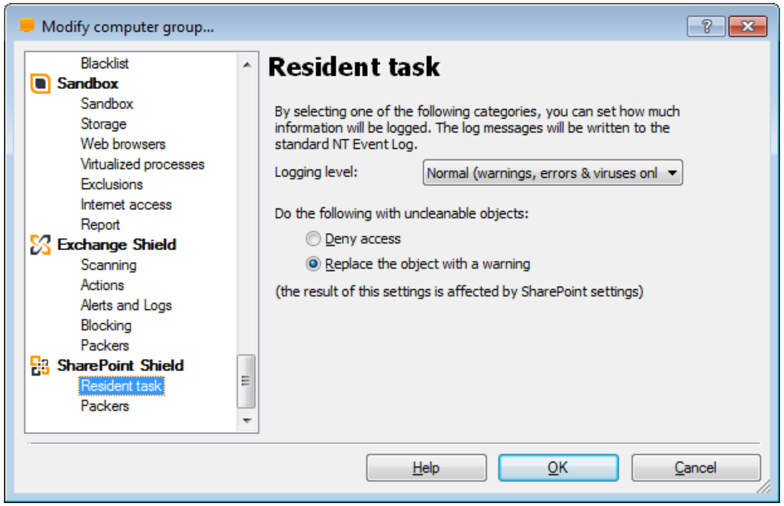
☑ Monitor

- Our SharePoint Server plug-in integrates with SharePoint 2003/2007/2010 Servers via Microsoft's own AV interfaces. It prevents users from uploading or downloading malicious content to SharePoint libraries.

AEA console

Computer catalog

SharePoint Shield



Resident task

By selecting one of the following categories, you can set how much information will be logged. The log messages will be written to the standard NT Event Log.

Logging level: Normal (warnings, errors & viruses onl

Do the following with uncleanable objects:

○ Deny access

● Replace the object with a warning

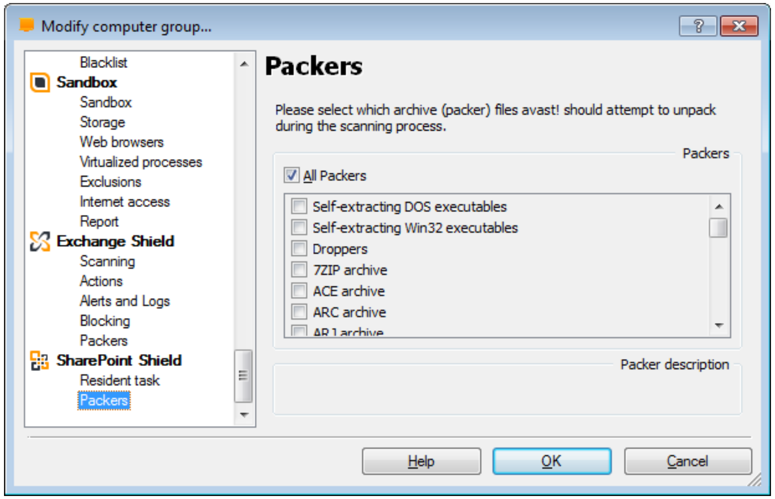
(the result of this settings is affected by SharePoint settings)

- You can specify what information will be saved to the log files e.g. only errors and viruses, or other additional less critical information as well.
- You can also specify what action should be taken with objects that cannotn be cleaned.

AEA console

Computer catalog

SharePoint Shield



Modify computer group...

- Blacklist
- **Sandbox**
  - Sandbox
  - Storage
  - Web browsers
  - Virtualized processes
  - Exclusions
  - Internet access
  - Report
- **Exchange Shield**
  - Scanning
  - Actions
  - Alerts and Logs
  - Blocking
  - Packers
- **SharePoint Shield**
  - Resident task
  - Packers

Packers

Please select which archive (packer) files avast! should attempt to unpack during the scanning process.

Packers

☑ All Packers

□ Self-extracting DOS executables
□ Self-extracting Win32 executables
□ Droppers
□ 7ZIP archive
□ ACE archive
□ ARC archive
□ ARJ archive

Packer description

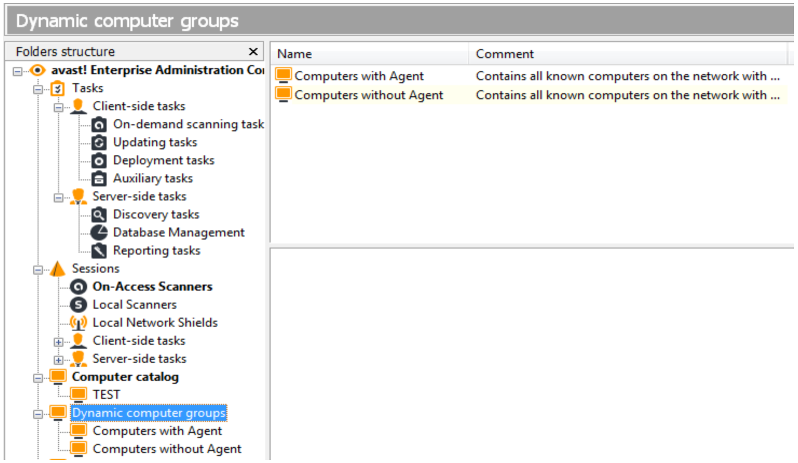
Finally, you can also select which types of archive files avast should attempt to unpack for scanning.

AEA console

DYNAMIC COMPUTER GROUPS

AEA console

Dynamic computer groups



Name	Comment
Computers with Agent	Contains all known computers on the network with ...
Computers without Agent	Contains all known computers on the network with ...

- Dynamic computer groups provide a powerful method to search, manage, and further categorize the Computer Catalog. You can think of it as a high-performance filter for the Computer Catalog, but it’s much more than just a filter.

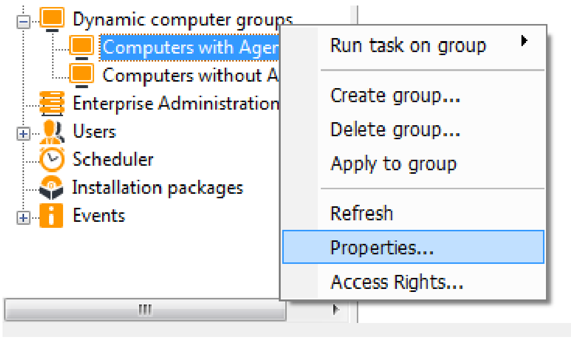
- It can be used anywhere a computer group can be used.

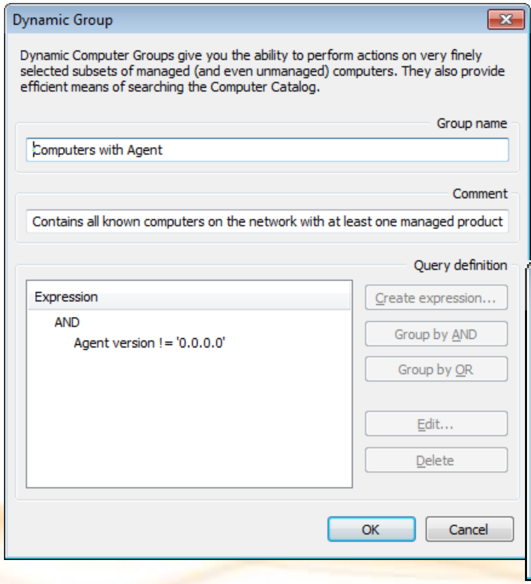
AEA console

Dynamic computer groups

- Each dynamic group is made up of a set of expressions connected by logical operators like AND or OR, for example, “computer_name = NEMESIS.”

- Expressions include operators like equal-to, smaller-than, greater-than, and they can also contain functions, such as MIN, MAX, or AVERAGE. Individual expressions can also be nested together, i.e., they support grouping by parentheses.





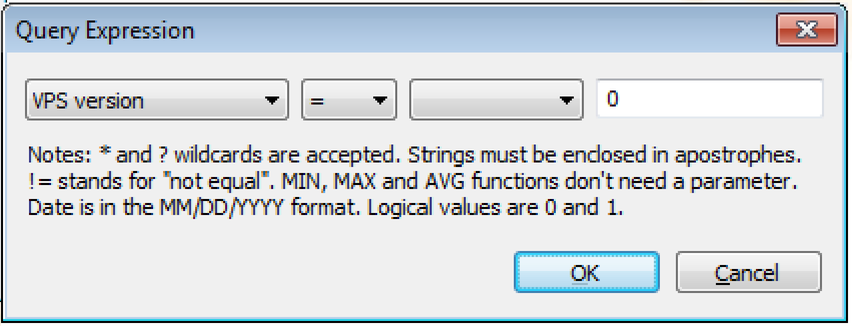
Dynamic Computer Groups give you the ability to perform actions on very finely selected subsets of managed (and even unmanaged) computers. They also provide efficient means of searching the Computer Catalog.

Group name: Computers with Agent

Comment: Contains all known computers on the network with at least one managed product

Query definition

```
Expression
  AND
    Agent version != '0.0.0.0'
```

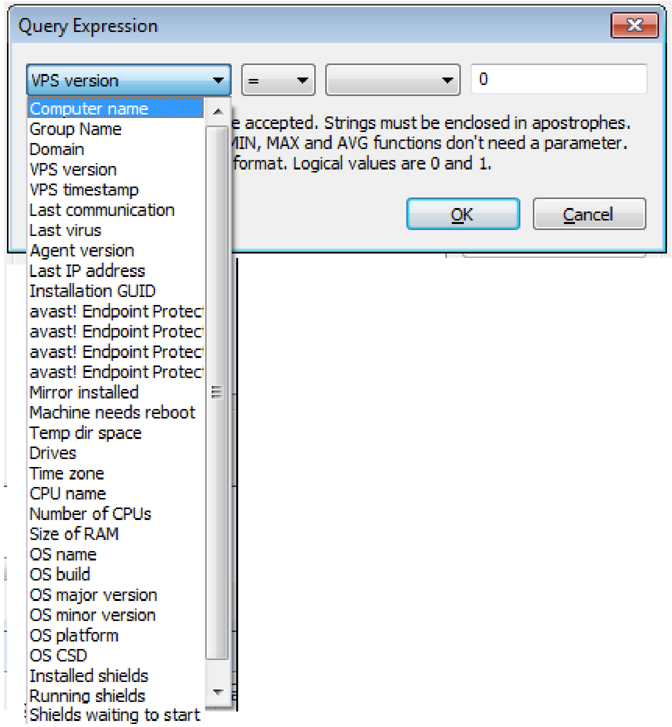


VPS version | = | | 0

Notes: * and ? wildcards are accepted. Strings must be enclosed in apostrophes.
!= stands for "not equal". MIN, MAX and AVG functions don't need a parameter.
Date is in the MM/DD/YYYY format. Logical values are 0 and 1.

AEA console

Dynamic computer groups



Query Expression

VPS version | = | | 0

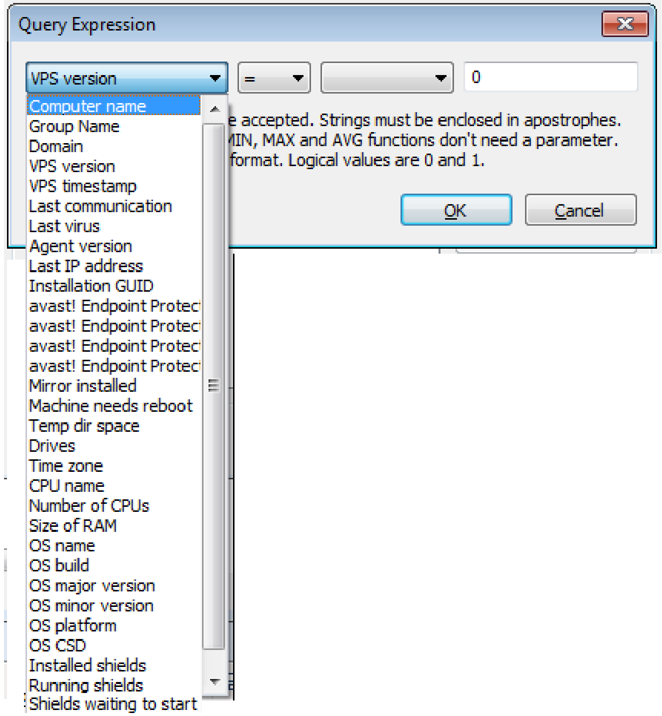
e accepted. Strings must be enclosed in apostrophes.
MIN, MAX and AVG functions don't need a parameter.
format. Logical values are 0 and 1.

- The following parameters are supported for building the expression:

- **Computer name (type: string)**
  - The name of the computer as stored in the Catalog.
- **Group name (type: string)**
  - The name of the (static) group in which the computer is stored in the Catalog.
- **Domain (type: string)**
  - The name of the Windows domain or workgroup in which the computer resides.
- **VPS version (type: tri-dot string)**
  - The version number (in the form x.x.x.x) of the current VPS file (virus database) installed on the machine.
- **VPS timestamp (type: string)**
  - The date of release of the current VPS file (virus database) installed on the machine.
- **Last communication (type: string)**
  - The date and time of last contact with the machine.
- **Last virus (type: string)**
  - The name of the last virus found on the machine.
- **Agent version (type: tri-dot string)**
  - The version of the avast! client installed on the machine (in the form x.x.x.x, e.g., 4.1.102.0).
- **Last IP address (type: tri-dot string)**
  - The last IP address (in the form x.x.x.x) that the machine used to contact the server.
- **Installation GUID (type: string)**
  - The GUID (globally-unique-identifier) of the client installed on the machine.

AEA console

Dynamic computer groups

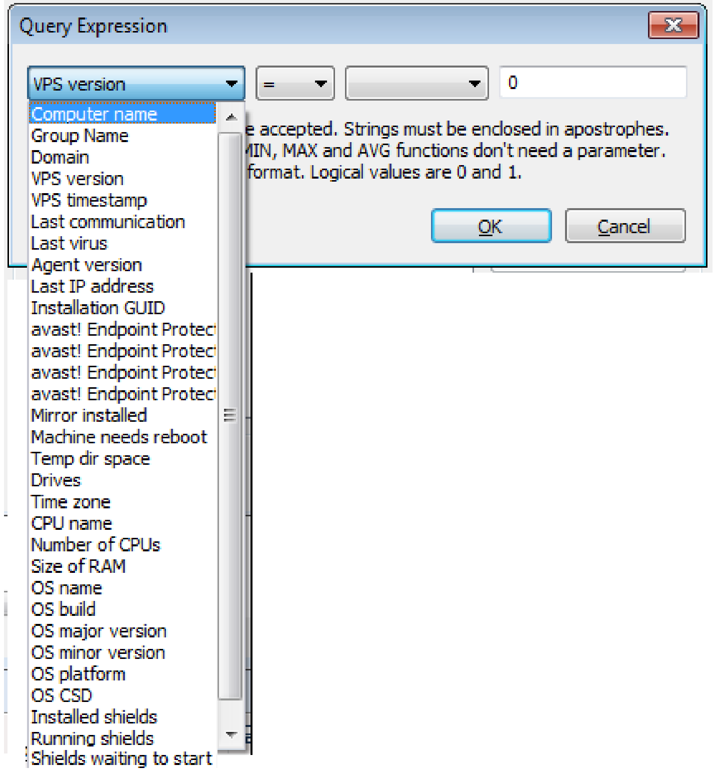


e accepted. Strings must be enclosed in apostrophes.
MIN, MAX and AVG functions don't need a parameter.
format. Logical values are 0 and 1.

- **avast! Endpoint Protection installed (type: logical value, i.e. 0 or 1)**
  - A logical value specifying whether avast! NetClient Edition is installed on the machine.
- **avast! Endpoint Protection Plus installed (type: logical value, i.e. 0 or 1)**
  - A logical value specifying whether avast! NetClient Edition is installed on the machine.
- **avast! Endpoint Protection Suite installed (type: logical value, i.e. 0 or 1)**
  - A logical value specifying whether avast! NetClient Edition is installed on the machine.
- **avast! Endpoint Protection Suite Plus installed (type: logical value, i.e. 0 or 1)**
  - A logical value specifying whether avast! NetClient Edition is installed on the machine.
- **avast! NetServer installed (type: logical value, i.e. 0 or 1)**
  - A logical value specifying whether avast! NetServer Edition is installed on the machine.
- **Mirror installed (type: logical value, i.e. 0 or 1)**
  - A logical value specifying whether the managed product "2nd level mirror" is installed on the machine.
- **Machine needs reboot (type: logical value, i.e. 0 or 1)**
  - A logical value specifying whether the agent on the machine is waiting for a reboot (e.g. because of an incomplete update attempt).
- **Temp dir space (type: integer)**
  - Total free space in the machine's TEMP directory, in megabytes.
- **Drives (type: string)**
  - The list of logical drives on the machine, separated by semicolons without spaces (as A;C;D).
- **Time zone (type: integer)**
  - The time zone of the machine (signed number of minutes shifted from GMT).
- **CPU name (type: string)**
  - The name of the CPU installed on the machine, as presented by the system.
- **Number of CPUs (type: integer)**
  - The number of processors installed on the machine.
- **Size of RAM (type: integer)**
  - The size of operating memory installed on the machine, in megabytes.

AEA console

Dynamic computer groups



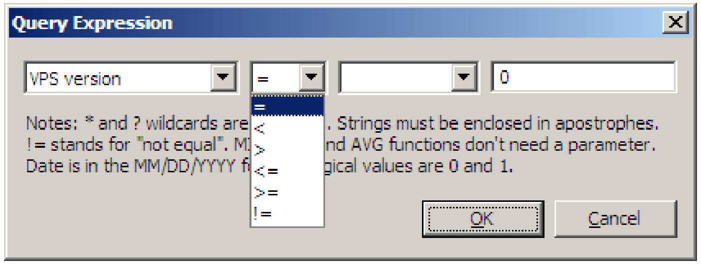
VPS version = 0

e accepted. Strings must be enclosed in apostrophes.
IIN, MAX and AVG functions don't need a parameter.
format. Logical values are 0 and 1.

- **OS name (type: string)**
  - The name of the machine's operating system, such as "Windows XP."
- **OS major version (type: integer)**
  - The major version number of the machine's operating system. For example, the retail version of Windows XP has this value set to 5.
- **OS minor version (type: integer)**
  - The minor version number of the machine's operating system. For example, the retail version of Windows XP has this value set to 1.
- **OS build (type: integer)**
  - The build number of the machine's operating system. For example, the retail version of Windows XP has this value set to 2600.
- **OS platform (type: integer)**
  - The platform ID of the machine's operating system. Value 1 means Windows 9x/ME, value 2 means NT-based platforms.
- **OS CSD (type: string)**
  - The machine operating system's service pack name, for example, "Service Pack 3."
- **Installed shields (type: string)**
  - The list of avast! Real time shields (modules) installed on the machine. Shields are listed by their short names.
- **Running shields (type: string)**
  - The list of avast! Real time shields (modules) running on the machine. By definition, this is a subset of the value "Installed shield."
- **Waiting shields (type: string)**
  - The list of avast! Real time shields (modules) that have the current status "waiting to start" on the machine. By definition, this is a subset of the value "Installed shield"

AEA console

Dynamic computer groups

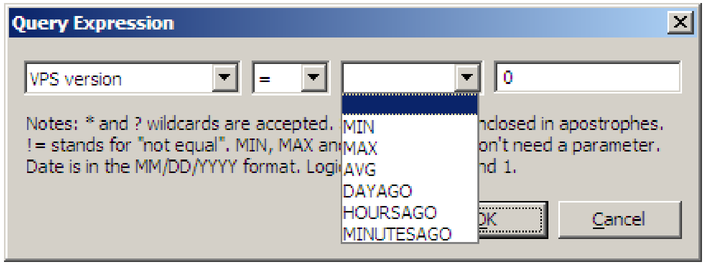


Notes: * and ? wildcards are . Strings must be enclosed in apostrophes.
!= stands for "not equal". M nd AVG functions don't need a parameter.
Date is in the MM/DD/YYYY f gical values are 0 and 1.

- The following operators are supported:
  - Equal-to, **=.**
  - Not-equal-to, **!=.**
  - Smaller-than, **<.**
  - Greater-than, **>.**
  - Smaller-than-or-equal-to, **<=.**
  - Greater-than-or-equal-to, **>=.**

AEA console

Dynamic computer groups



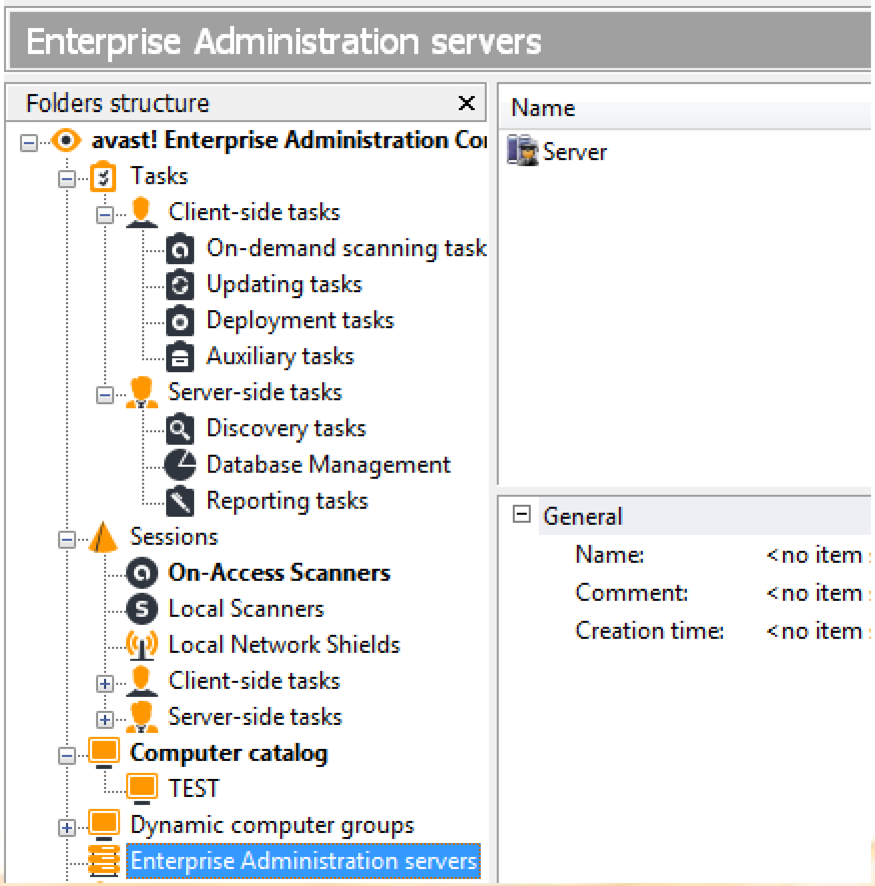
Notes: * and ? wildcards are accepted. nclosed in apostrophes.
!= stands for "not equal". MIN, MAX an on't need a parameter.
Date is in the MM/DD/YYYY format. Logi nd 1.

- The following functions are supported:
- **MIN**
  - This function returns the computer(s) with the minimum value of the parameter. It has no operands.
- **MAX**
  - This function returns the computer(s) with the maximum value of the parameter. It has no operands.
- **AVG**
  - This function returns the computer(s) with the average value of the parameter. It has no operands.
- **DAYSAGO**
  - This function returns the computer(s) for which the parameter, which must be of the timedate type, occurred N days ago at most. The operand specifies the value of N.
- **HOURSAGO**
  - This function returns the computer(s) for which the parameter, which must be of the timedate type, occurred N hours ago at most. The operand specifies the value of N.
- **MINUTESAGO**
  - This function returns the computer(s) for which the parameter, which must be of the timedate type, occurred N minutes ago at most. The operand specifies the value of N.
- There are only two logical operators for connecting multiple expressions: **OR and AND.** The dynamic group definition can be made up of any number of expressions connected by either of these logical operators.

AEA console

ENTERPRISE ADMINISTRATION SERVERS

AEA console



Name: <no item
Comment: <no item
Creation time: <no item

- This is where information about all Enterprise Administration servers is stored.

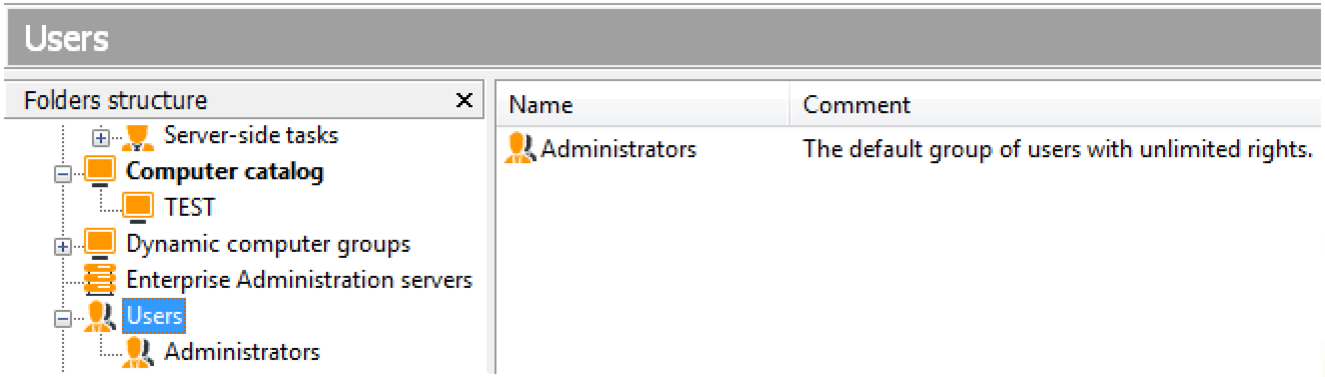
- By default, there's only one – the one you're connected to. But for larger networks, it may be necessary to have several EAS's deployed on the network.

AEA console

USERS

AEA console

Users



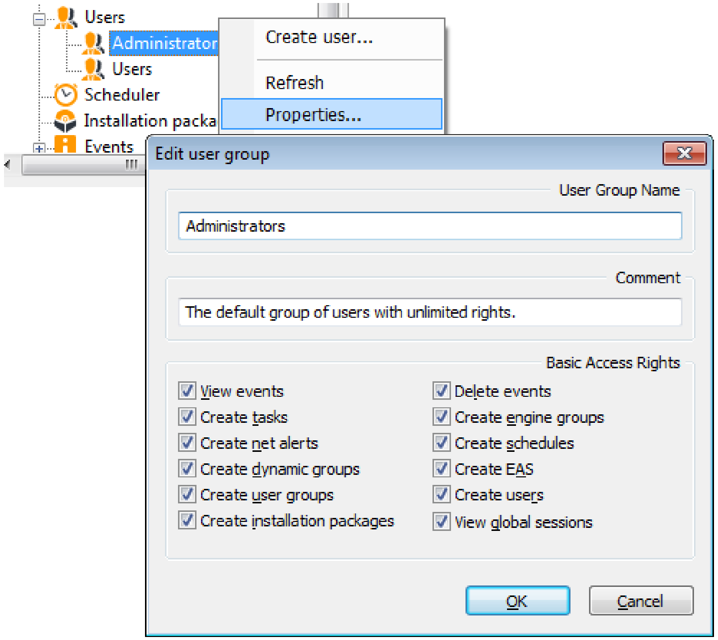
Name	Comment
Administrators	The default group of users with unlimited rights.

- The AEA has a very flexible system for defining users and user rights.

- The Users folder holds the list of all users (administrators\users) who are permitted to access the management capabilities of the EAS, such as:
  - View events
  - Create tasks
  - Create dynamic groups
  - Create EAS
  - etc..

AEA console

Users



Edit user group

User Group Name: Administrators

Comment: The default group of users with unlimited rights.

Basic Access Rights

☑ View events
☑ Create tasks
☑ Create net alerts
☑ Create dynamic groups
☑ Create user groups
☑ Create installation packages
☑ Delete events
☑ Create engine groups
☑ Create schedules
☑ Create EAS
☑ Create users
☑ View global sessions

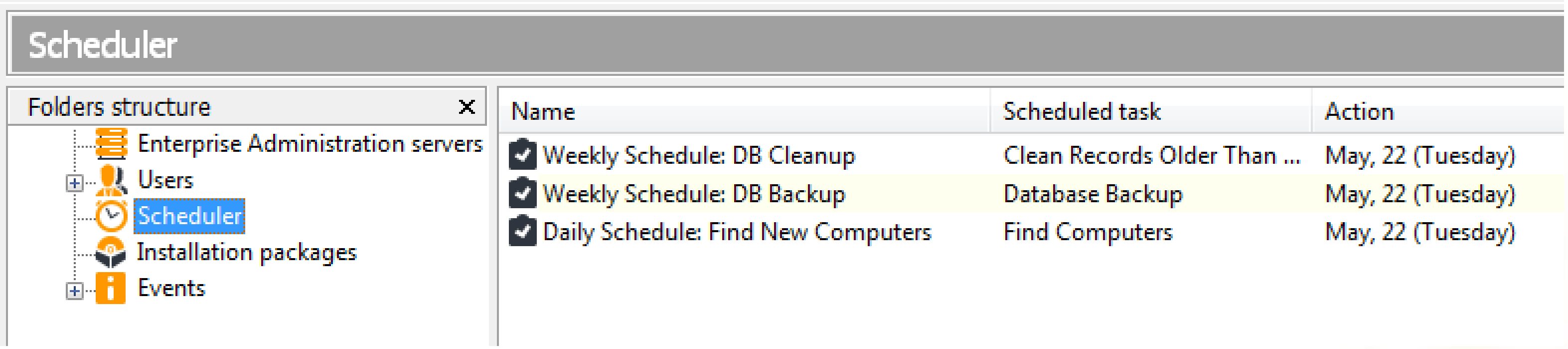
- Different users have different access rights.
- The users can be bunched together in user groups, which are displayed as subfolders of the Users folder.
- Every user has to be in a group, i.e., it is not possible to create individual users in the root of the Users folder.
- The group properties define its basic rights

AEA console

SCHEDULER

AEA console

Scheduler

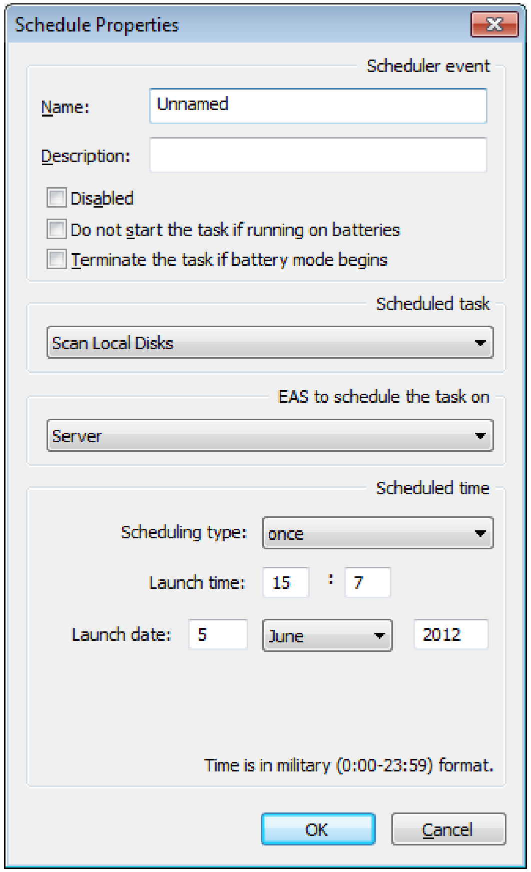


Name	Scheduled task	Action
Weekly Schedule: DB Cleanup	Clean Records Older Than ...	May, 22 (Tuesday)
Weekly Schedule: DB Backup	Database Backup	May, 22 (Tuesday)
Daily Schedule: Find New Computers	Find Computers	May, 22 (Tuesday)

- The scheduler folder holds the scheduler event objects that define when the tasks will run and other important parameters.
- This is one way to edit the schedule. Another is to define the scheduling rules in the task's properties.

AEA console

Scheduler



Schedule Properties

Scheduler event

Name: Unnamed

Description:

□ Disabled

□ Do not start the task if running on batteries

□ Terminate the task if battery mode begins

Scheduled task

Scan Local Disks

EAS to schedule the task on

Server

Scheduled time

Scheduling type: once

Launch time: 15 : 7

Launch date: 5 June 2012

Time is in military (0:00-23:59) format.

Here you should enter the parameters defining the new task

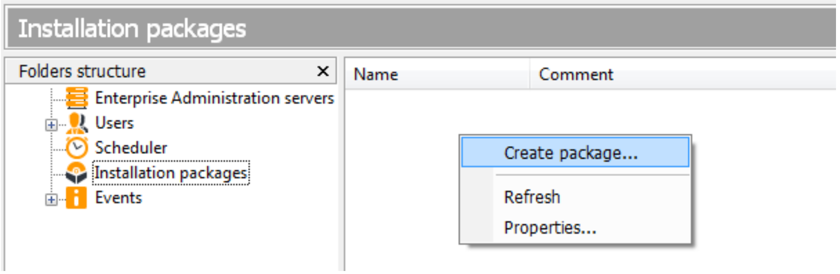
- **Name**
  - Name of the task, e.g. "Weekend scan".
- **Description**
  - Enter a brief description of the task e.g. "Scans all the hard disks every Sunday night".
- **Disabled**
  - This option disables the scheduled task. It is useful when you need to stop the task from running, but you do not want to delete the task completely and have to re-enter it again later.
- **Do not start the task if running on batteries**
  - Useful mainly for notebook owners. The task will not be started if the computer is running on batteries.
- **Terminate the task if battery mode begins**
  - If, while a scheduled task is running, the computer is cut off from the electric power supply and switches to batteries, the task will be terminated. Again, this is useful mainly for notebook owners.
- **Scheduled task**
  - Select the task to be scheduled.
- **Scheduling type**
  - Here you can specify when the task will be started.
    - Once - you simply enter the time and date when the task should be run.
    - Daily - enter the time only - the task will be started each day at the given time.
    - Weekly (or monthly)
- **Launch time/launch date**
  - Here you can set the time and the actual day of the week (month) when the scheduled task should be run.

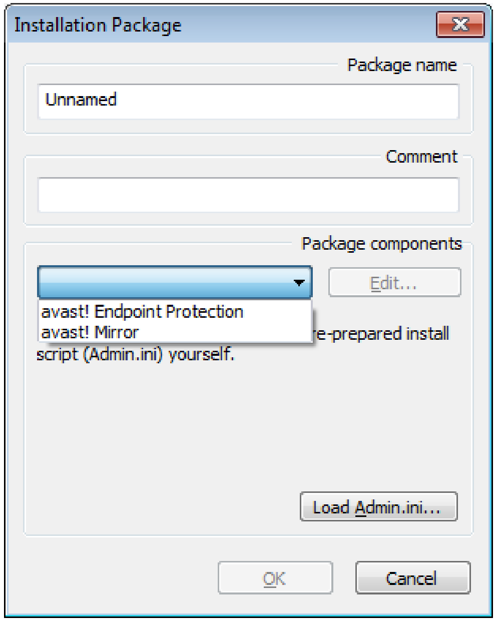
AEA console

INSTALLATION PACKAGES

AEA console

Installation packages




Installation Package

Package name: Unnamed

Comment:

Package components

avast! Endpoint Protection
avast! Mirror

re-prepared install script (Admin.ini) yourself.

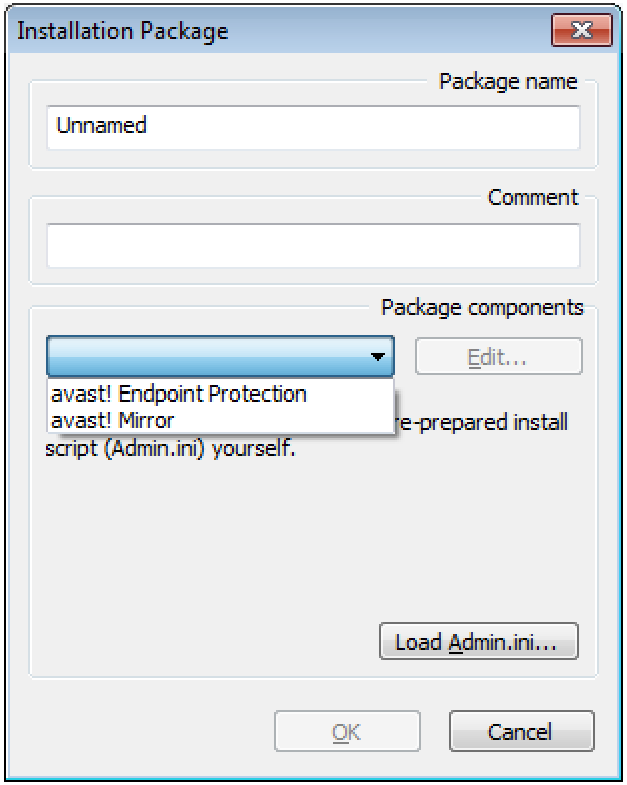
Because the Deployment tasks run silently (without any user intervention), they need to have all the installation options properly preset.

- The installation options are used to define the settings that will be used by the Deployment tasks to push the installations to the clients. Options include: what product to install, destination folder, service accounts, etc.

The **Installation Package** must therefore be created before the deployment task!

AEA console

Installation packages



Installation Package

Package name: Unnamed

Comment:

Package components:

avast! Endpoint Protection
avast! Mirror

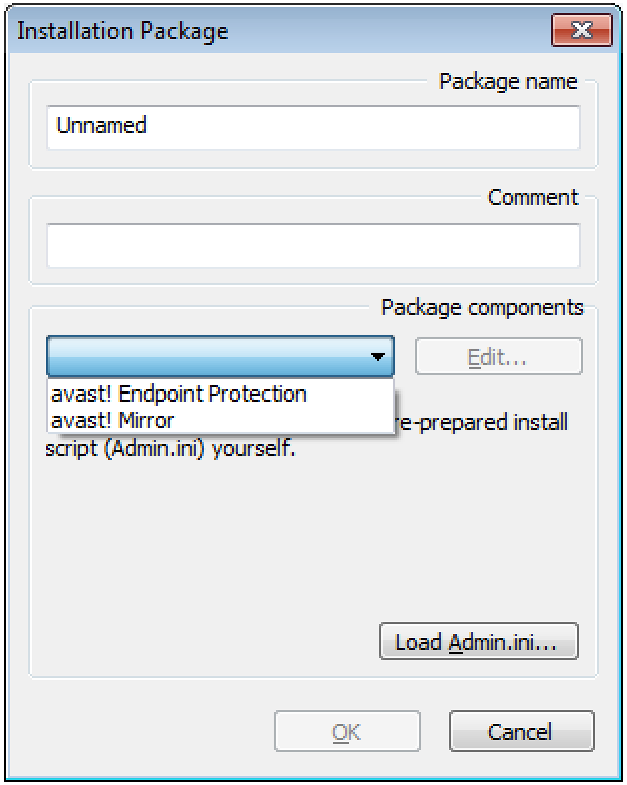
e-prepared install script (Admin.ini) yourself.

- To prepare the installation package, first go to the “Installation packages” folder and select the “Create Package…” option. Select the type of package to be prepared:

- **avast! Endpoint protection**
  - is a managed version of avast! antivirus
- **Mirror**
  - is a second-level mirror agent that can be used to load-balance the updating.

AEA console

Installation packages



Package name: Unnamed

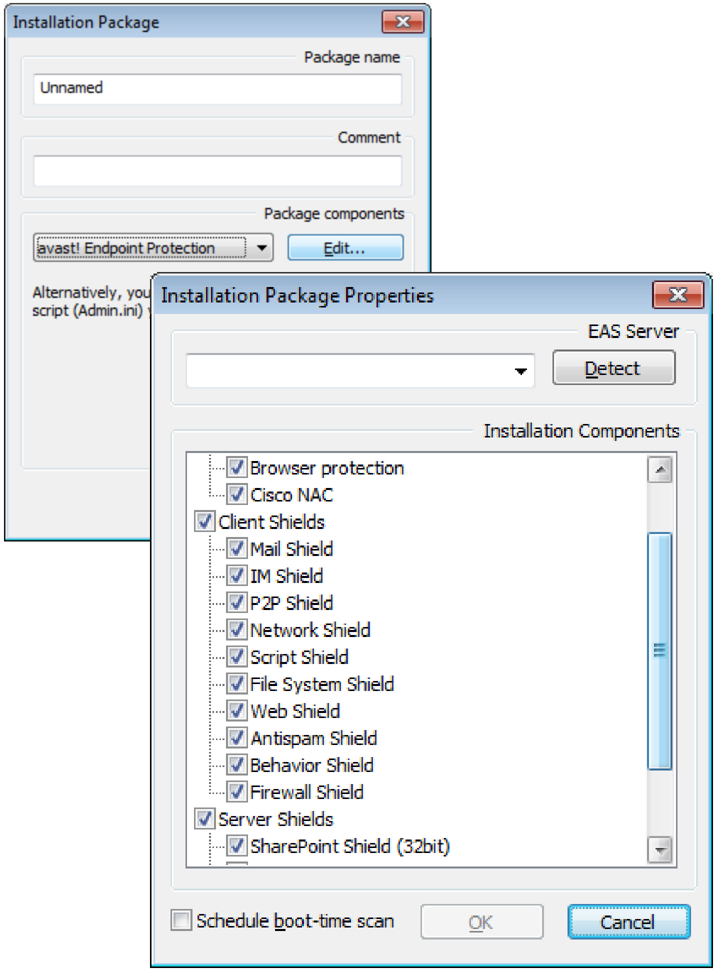
avast! Endpoint Protection
avast! Mirror

e-prepared install script (Admin.ini) yourself.

- Before creating the installation package, you can load the Admin.ini files which contain the pre-defined install settings/scripts.
- This option, intended especially for network administrators, makes it possible (and easy) to install avast! on an arbitrary number of computers. The files may contain predefined settings for both the program and the various tasks.
- **Admin.ini**
  - contains the avast! program settings

AEA console

Installation packages



Installation Package

Package name: Unnamed

Comment:

Package components: avast! Endpoint Protection

Alternatively, you
script (Admin.ini)

Installation Package Properties

EAS Server:

Installation Components
- ☑ Browser protection
- ☑ Cisco NAC
- ☑ Client Shields
  - ☑ Mail Shield
  - ☑ IM Shield
  - ☑ P2P Shield
  - ☑ Network Shield
  - ☑ Script Shield
  - ☑ File System Shield
  - ☑ Web Shield
  - ☑ Antispam Shield
  - ☑ Behavior Shield
  - ☑ Firewall Shield
- ☑ Server Shields
  - ☑ SharePoint Shield (32bit)

☐ Schedule boot-time scan

- Then click the “Edit…” button to set the Installation Components.

- Detect:

- automatically detect available EAS on the network. If the auto detection does not work, you can enter the DNS/IP address of your EAS manually.

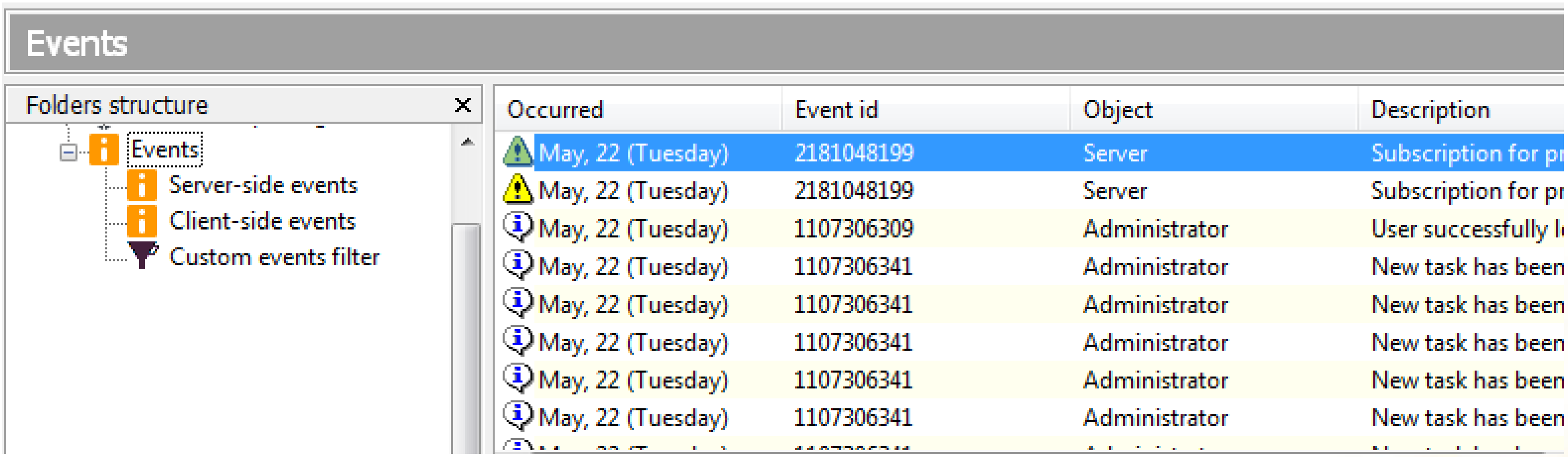
- When the installation package is ready, create the deployment task.

AEA console

EVENTS

AEA console

Events



Events

Folders structure

- Events
  - Server-side events
  - Client-side events
  - Custom events filter

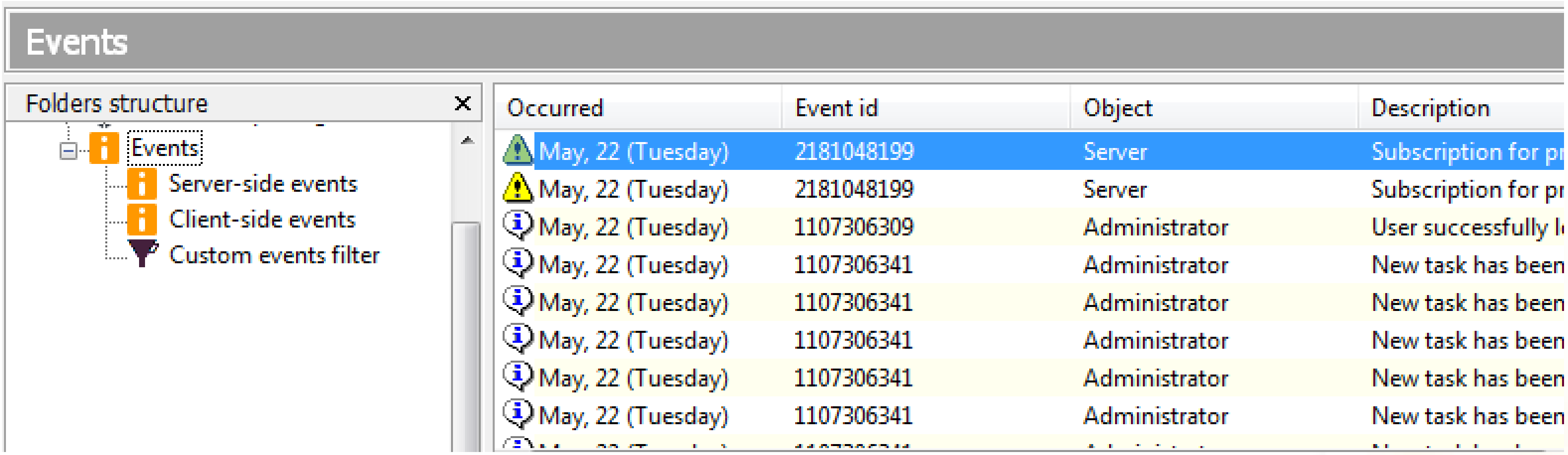
Occurred	Event id	Object	Description
May, 22 (Tuesday)	2181048199	Server	Subscription for pr
May, 22 (Tuesday)	2181048199	Server	Subscription for pr
May, 22 (Tuesday)	1107306309	Administrator	User successfully l
May, 22 (Tuesday)	1107306341	Administrator	New task has been
May, 22 (Tuesday)	1107306341	Administrator	New task has been
May, 22 (Tuesday)	1107306341	Administrator	New task has been
May, 22 (Tuesday)	1107306341	Administrator	New task has been
May, 22 (Tuesday)	1107306341	Administrator	New task has been

- This is the AEA event log. A lot of important information is written to the log from the EAS and from the client computers. The logs are very easy to navigate and include powerful filtering capabilities.

- To ensure the overall health of the network, it is necessary to continuously monitor the log entries that are sent from the clients or written by the EAS itself. In most cases, this is done via the Events folder in the console.

AEA console

Events



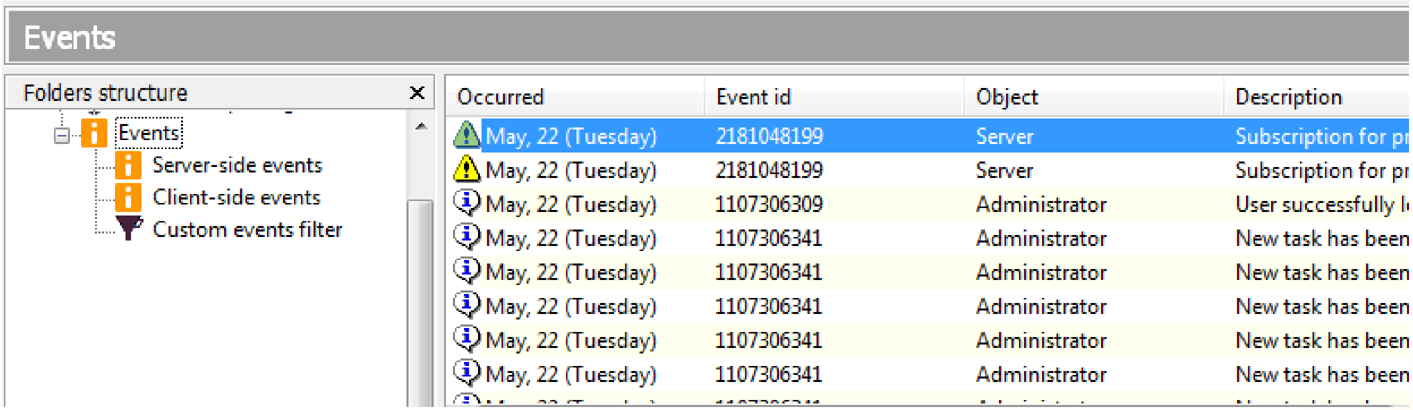
Occurred	Event id	Object	Description
⚠ May, 22 (Tuesday)	2181048199	Server	Subscription for pr
⚠ May, 22 (Tuesday)	2181048199	Server	Subscription for pr
ℹ May, 22 (Tuesday)	1107306309	Administrator	User successfully l
ℹ May, 22 (Tuesday)	1107306341	Administrator	New task has been
ℹ May, 22 (Tuesday)	1107306341	Administrator	New task has been
ℹ May, 22 (Tuesday)	1107306341	Administrator	New task has been
ℹ May, 22 (Tuesday)	1107306341	Administrator	New task has been
ℹ May, 22 (Tuesday)	1107306341	Administrator	New task has been

- Clicking the events folder displays all events stored in the database, unfiltered. There are also three subfolders:

- **Client events**
  - This folder contains all events sent by the managed clients. It contains warnings/critical error entries, so it’s good to monitor this folder on a regular basis.
- **Server events**
  - This folder gathers events generated by the EAS (with the exception of task-specific events, which are filtered out from this view). This includes a simple audit — entries documenting when the server was started/stopped, when a new object was created, etc.

AEA console

Events



Occurred	Event id	Object	Description
May, 22 (Tuesday)	2181048199	Server	Subscription for pr
May, 22 (Tuesday)	2181048199	Server	Subscription for pr
May, 22 (Tuesday)	1107306309	Administrator	User successfully l
May, 22 (Tuesday)	1107306341	Administrator	New task has been
May, 22 (Tuesday)	1107306341	Administrator	New task has been
May, 22 (Tuesday)	1107306341	Administrator	New task has been
May, 22 (Tuesday)	1107306341	Administrator	New task has been
May, 22 (Tuesday)	1107306341	Administrator	New task has been

- **Custom events filter**
  - This folder lets you define your own custom mask to exactly specify the events you’d like to see. Filtering options include: by substring, by type, by category, and by time.

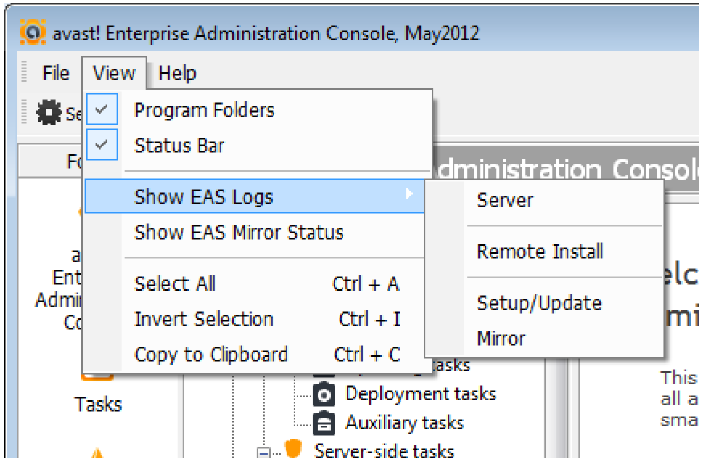
- The event entries cannot be directly deleted from the log. Old entries can be removed using a Database Maintenance task (using the option Delete Events Older Than ... Days).

AEA console

Monitoring the EAS Logs

- Besides the events written directly to the database—shown in client-side and server-side logs, which can be viewed in the Events folder in the administration console—the EAS also logs certain events in separate log files. These logs are usually used for troubleshooting purposes. They're not written to the database because the database connection may not be available. For example, it's impossible to log database connection problems to the database.

- Most of the logs are stored in the ..Program Files\AVAST Software\Enterprise Administration\DATA\log folder. You can use Notepad or any text program to view them.



- The logs can also be viewed directly from the console, by using the menu item View / Show EAS Logs. The console opens the log files in your web browser, so you can even bookmark them if you wish. Of course, the console view only works if you can connect to the EAS, that is, if the EAS service is running properly—not always the case if there's a problem.

- Mirror logs are stored in the folder ..Program Files\AVAST Software\Enterprise Administration\mirror\logs
- AEA installer logs are written to ..Program Files\AVAST Software\Enterprise Administration\Setup.

avast!

Enterprise Administration

www.avast.com