avast! Distributed Network Manager (ADNM)

Quick Start Guide

alwil software

avast! Distributed Network Manager (ADNM): Quick Start Guide

Published September 19, 2004 (Rev. 0.98, ADNM RC-2a)

Table of Contents

1

Basics

Welcome to the avast! Distributed Network Manager, one of the most most powerful tools for network antivirus management.

avast! Distributed Network Manager (ADNM) represents a suite of powerful tools designed to help network administrators manage the avast! antivirus product line across the whole enterprise.

The ADNM system consists of the following components:

- avast! Management Server (AMS) - the heart of ADNM that provides the business logic for the whole system.
- SQL Database - serves as a data storage for all the policies, security settings and client information.
- Administration Console - the program 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 AMS (avast! Management Server). This is where all the hard work is done.

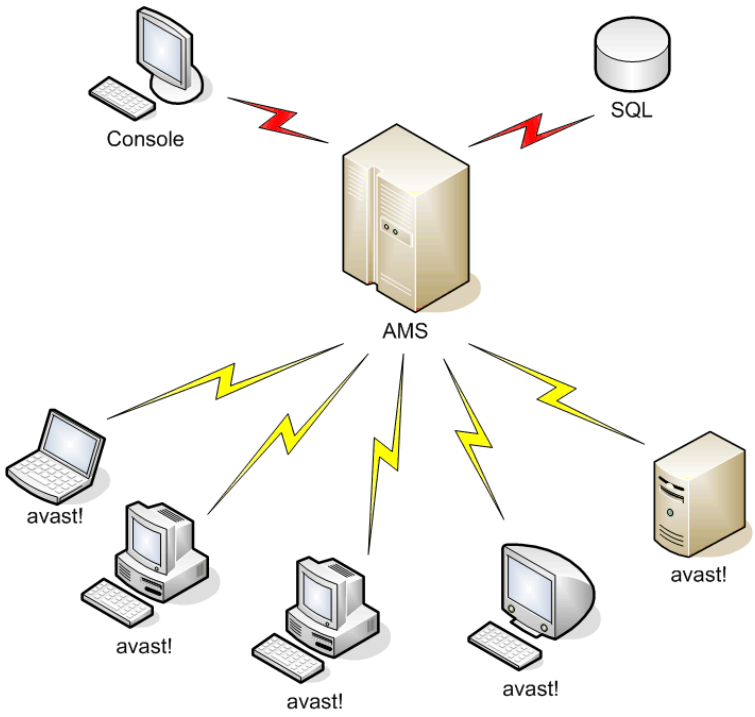

Figure 1.1. Basic ADNM diagram

The managed machines connect only to the AMS to download latest policies and to report their status and scan results. The Administration Console also connects directly to the AMS. The AMS is based on a SQL Database – either a dedicated MS SQL Server 2000, if available, or, for small and medium-size networks, on its lightweight version, MSDE 2000, which is part of the ADNM installation package. It is assumed that the AMS machine can connect to the Internet via HTTP protocol.

For larger networks, the AMS is expected to be installed on a dedicated computer. It is also possible to deploy multiple AMS' (each having its own database). These can then be instructed to replicate their databases on a regular basis, and also upload all scanning results to a dedicated AMS on which enterprise-wide reporting can then be carried out. The administrators can choose from two communication models used by the AMS and the clients: PUSH or POP. The POP model is necessary for larger networks and for networks with roaming users. Each AMS can scale up to tens of thousands of client computers, provided they are all connected by local area network.

2

Installation

2.1 Planning Phase

Before you start installing the product, you should make some considerations about how you'll be deploying the product.

Namely, the following things need to be carefully considered:

AMS

- On which machine to deploy the AMS?
- Is it going to be a dedicated machine? If not, what else will run on the machine? Won't it interfere with the AMS? Will there be enough resources left for the AMS to work properly?
- Is DHCP used on the network? Can the AMS have a fixed IP address? (that should be the case)
- Is a full-blown MS SQL 2000 database going to be used, or rather the lightweight version (MSDE) that's provided as part of the ADNM installation package? If we choose MSDE, will it handle all our management data? (MSDE should only be used on networks with a maximum number of computers in the range of hundreds or less).
- Can we use just one AMS or would it be better to choose the multi-AMS model? Generally, multiple AMS' are advantageous if there is more than one (geographical) site, i.e. multiple LANs connected by slower links.
- Will the AMS machine meet the minimum system requirements? Namely, the following conditions must be met to install the AMS:
    - A Windows NT/2000/XP/2003 -based machine with at least 128MB RAM (256-512MB recommended)
    - CPU power depending on the size of the network – Pentium III or

higher recommended.

- At least 250MB free hard drive space, plus additional ~ 4GB if using MSDE on the same machine
- outbound Internet connection (HTTP protocol)

Console

- Who will be responsible for the management of the ADNM system? Is it just one person or multiple persons?
- On which computers should the administration console(s) be installed?

Management Needs

- How are we going to organize the machines in a tree? Will we do it geographically? Or will we adhere to the network structure (e.g. ActiveDirectory domains)? Or a combination of both?
- How will we import the list of machines to the ADNM? Can we use the discovery task (i.e. does the Network Neighbourhood browser work OK on our network) or will we have to use some alternative method (e.g. import from a text file)?
- Will all administrators have the same rights, or will we have a structure of administrators, each with different responsibilities and access rights?

Deployment of the avast! product line

- How are we going to deploy the avast! products on our network? Do we want to use the ADNM deployment mechanisms (the Deployment tasks), or do we have our own means of software installation?
- Are there any Windows 95/98/ME machines on our network? How will we install the software on those? (the ADNM Deployment tasks only work for NT-based clients)
- Do we use a disk imaging software to prepare new machines? Will we want to include avast! installation in the base image? (If so, please make sure to read the appropriate chapter later on)

2.2 Installation Phase

After completing the Planning Phase, you can actually start installing the software.

AMS

The installation begins with the AMS. To install the AMS, simply load (or extract) the ADNM installation package to the machine that you want to make the AMS, and run the setup program (setup_av_mgm.exe). This will start the setup wizard that will guide you through the installation process. You'll be asked for the following info:

- Destination folder.
- Components to install (either both AMS and console or just the console; leave all components checked to install the AMS).
- License file (you need a license file to use the software; you can either use the attached DEMO file, or supply your own – provided you've already purchased a license for the software). You can change the license file later at any time.
- Database details. If you want to use MSDE, make sure to have the 'Install MSDE' check box ticked. If the check box is dimmed, it means that the setup program did not find the MSDE installation in the current folder. The MSDE installation package folder must be called "MSDE" and must be located in the same folder as the main setup program setup_av_mgm.

After all the files are copied, you're asked if you want to create the updating mirror. It is strongly recommended to answer Yes – otherwise, you'll have to initialize the mirror yourself. Answering Yes will preset all the values for you automatically so you won't have to do anything later. Of course, the mirroring process requires active Internet connection (HTTP only).

After the mirroring is complete, you must initialize the SSL certificate that will be used by the SSL layer when communicating between the AMS and the administration console. You can either supply your own certificate (in PEM, DER, or PKCS#7 format), or have one generated for you by the installer.

Note

The supplied certificate file must contain a private key as it's going to be used to encrypt the communication between the AMS and the consoles.

After the installation completes, you may be prompted by the setup program to restart the machine (depending on the operating system used). After the reboot, the AMS should be ready to function and its services should start automatically.

Administration Console(s)

The next logical step is to install the administration console(s). Sure, you can use the console that was installed as part of the AMS but that's not necessary. Typically, it's much more convenient to install the console directly to the administrator's machine and do all the administration remotely. You can install any number of consoles throughout the network. It's not a very good idea to deploy the consoles to "normal" user's machines, though, as it may result in authorized tampering with the AMS (although this can be very well prevented by using appropriate security measures, such as strong passwords etc.).

To install the console, you basically follow the same procedure as when installing the AMS, with the exception that when asked for the components to install, you uncheck the 'Management Server' box, leaving only the Console option checked.

After the console installation is complete, you can immediately start using the program. Go to the Start menu, and select ADNM Console to start the console. This will result in displaying the Log On window. Type in the name of the machine on which you've installed the AMS, or press the Detect Servers button to try to discover all available AMS' on the network. The default username is *Administrator*, and the password is *admin*. We strongly encourage all users to change the password as soon as possible after logging on to the server as leaving the password set to its default value directly compromises system security.

Figure 2.1. The AMS Log On Dialog

When connecting to the server for the first time, you'll also see a warning that the SSL certificate that the server is using is not known to the client and is therefore suspicious. This is normal and you can safely select the 'Permit and Store' option to permanently allow the certificate. This will prevent any warnings of this kind from appearing on this machine unless the AMS certificate is changed (a rare event).

After the connection to the server completes successfully, you'll have access to all the console features. The following section will get you acquainted with the basic concepts of the console and describe how you can use ADNM to achieve optimal protection of the whole network.

3

The Console – First Steps

3.1 Basic Console Concepts

The console is organized into folders that act as containers for the various administration objects. These are the most important ADNM objects:

- **Tasks.** Tasks are the basic building blocks of ADNM. A task is a definition of a job, i.e. a prescription of what to do. In the ADNM case, a task also has associated computers that it should run on, and associated schedules that govern when it should run. There are many types of tasks in ADNM, but the basic distinction can be done between Client-side and Server-side tasks.

  - Client-Side tasks are those that are run on the client computers (i.e. workstations, servers etc. – the machines on which the avast products are deployed). These include on-demand scanning and updating tasks.

  - Server-side tasks, on the contrary, are run on the AMS itself. Typical representatives are reporting and database maintenance tasks.

- **Sessions.** After a task is run, a session is created for it. A session is an object that defines a particular run of a task. E.g. if there's task A, and it is run five times, five different sessions are created, each holding results of the specific run. For some tasks, the session only contains 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 with special meaning. The "On-Access Scanners" session holds all results of all on-access scanners on the network. The "Local Scanners" session holds results of all local on-demand scans (i.e. those that were not invoked on behalf of an ADNM scanning task).

- **Computers.** The Computers folder (called "Computer Catalog" in the console) works as a container of all managed machines on the network. It has a tree structure, meaning that you can create as many subfolders as you wish to achieve optimal organization. There can be no duplicates, i.e. every computer has its fixed position in the tree (to move 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. The policies are by default inherited from the root to the leaves, but can be overriden at any level. Therefore, it is important to pay careful attention when building the tree.

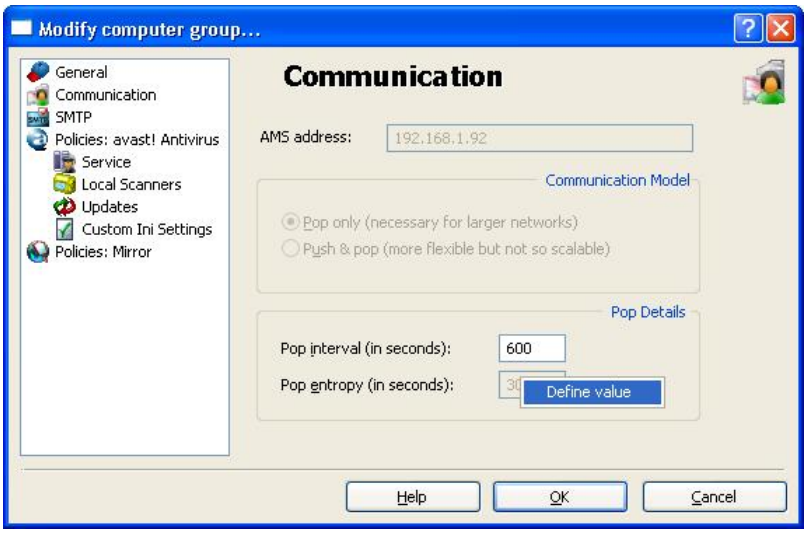

Figure 3.1. Computer Group properties are by default inherited from the parent but can be overriden at any level.

- **Management Servers.** This is where all the management servers are stored. By default, there's only one – the one you're connected to. But for larger networks, it may be necessary to have multiple AMS' deployed on the network. A separate section later on discusses the multi-AMS scenario in detail.

- **Users.** The ADNM has a very fine system of users and user rights. The Users folder holds the list of all users (administrators) that are defined to access the management capabilities of the AMS. Of course, different users have different rights. The users can be bunched to user groups that are displayed as subfolders of the Users folder. In fact, every user has to be in a group, i.e. it is not possible to create User objects in the root of the Users folder. The group only defines its basic rights – a much finer right assignment can be achieved by altering the access control lists (ACL's) on each ADNM administrative object.

- **Alerts.** This is where you can define the alerts (or notifications). The Alerting objects can then be assigned to the scanning tasks so that whenever a virus is found, the object will be used to notify someone about the problem.

- **Scheduler.** The scheduler folder hosts the scheduler event objects that

define when the tasks will run. This is an alternative way of editing the schedule – another way is to define the scheduling rules it in the task's properties.

- **Installation Packages.** Because the Deployment tasks run silently (with no user intervention), they need to have all the install options properly preset. The Installation Packages are used to define the installations (installation settings) that will be then available for the Deployment tasks for pushing to the clients. Options include: what product to install, destionation folder, service accounts etc.

- **Events.** This is the ADNM event log. Many important things are written to the log during the AMS and local agent operation. Powerful filtering capabilities are provided to ease navigation.

Note

Please note that the console view is not automatically refreshed, i.e. to see respective changes in time, you need to keep refreshing it yourself (e.g. by hitting the F5 key or using the apropriate menu item).

3.2 First Steps After Installation

A typical series of steps taken when a new AMS is installed is as follows:

- Change the password of the Administrator account (to do this, go to the Users/Administrators folder, and open the properties of the Administrator object).

- Start creating the Computer Catalog. Refer to the following chapter for details.

- Reorganize the Computer Catalog tree to suit your needs. By default, the Computer Catalog respects the system of workgroups/domains found on the network. However, this is not always the ideal choice to organize the machines for ADNM management. In this step, you generally fine-tune the tree e.g. by creating custom groups of computers that will have special requirements (such as machines of the company executives).

- Start settings the policies in the tree the structure of the Computer Catalog.

- Optionally create new user accounts in the Users folder, and assign appropriate rights to ADNM objects for these accounts in the "Object Rights" dialog (accessible by right-clicking any ADNM object).

- Start deploying the managed avast antivirus products to the clients (see the following chapter).

4

Creating the Computer Catalog

Efficient organization of the Computer Catalog is one of the key aspects of comfortable management. The better you design the Catalog, the better it will be possible to assign the security policies and the better will the whole ADNM perform. It is therefore important to pay special attention to its creation.

There are basically two different methods of creation of the Catalog. These two methods can also be combined. The first method makes use of a special type of server-side tasks, namely the discovery task, to automatically build the catalog. The second method consists of importing the information from an external source (file). You can also create the entries in the catalog by directly using the console's GUI but this is of course a very tedeous task in all cases other than inserting a few machines.

4.1 Using a Discovery Task

Using a Discovery Task is probably the easiest and most convenient way to build the Catalog. To use it, go to the Tasks/Server-side tasks/Discovery tasks and create a new task in this folder (normally, you can leave all the boxes in 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 computers on the network and inserts them to the Catalog, either to the root or to individual folders created to reflect the organization's domain/workgroup structure. Since discovery tasks typically run for quite a while, you'll have to wait for it to complete. You can monitor its current status by looking at the sessions properties, though. Again, please note that the view is not automatically refreshed, i.e. to see the progress, you need to keep refreshing it manually. After the task completes, the Computer Catalog should be filled with all the computers that have been found (again, don't forget to refresh the view to see the new items).

4.2 Importing Computers from an External Source

In some cases, you may not be able to make use of the Discovery Task (e.g. because your network doesn't run ActiveDirectory and/or the computer

browser does not work). Then it is ideal to take advantage of ADNM's ability to import the machine list from an external data source. Namely, 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 fairly simple structure. 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 domain or workgroup of which the computer is part. And finally, the third row is interpreted as the computer's IP address (and therefore should be in the form xx.xx.xx.xx where xx is a number between 0 and 255). This column is optional, meaning that you don't have to specify this value if you don't want to.

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 hand it to the ADNM. To do this, navigate yourself to any folder in the Computer Catalog, and select the Import Computers... menu option.

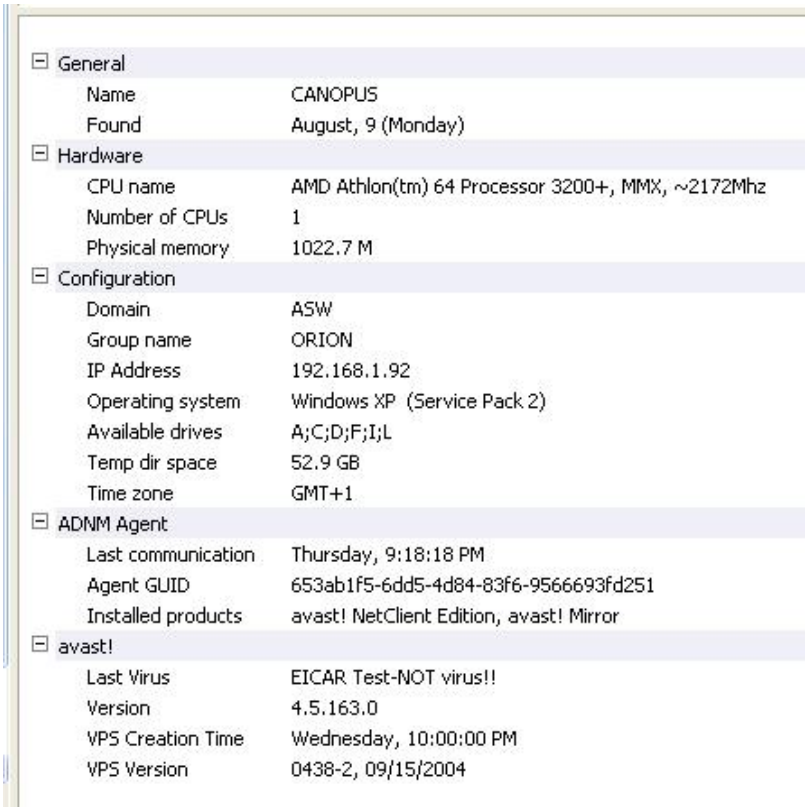

Figure 4.1. Basic info about a managed machine in the Computer Catalog.

5

Deploying the avast! Product Line

There are basically three methods of deploying the avast! product line to the network:

- By using the ADNM Deployment Task to push the installation to the clients automatically. Please note that this only works for Windows NT/2000/XP/2003 based machines.
- By using a log-on script or an alternative approach to execute the (unattended) installation on the target machines.
- By using MSI packages.
- By disk imaging (cloning) methods.
- By manually executing the installation program on the target machines and completing the setup wizard.

Obviously, the first choice is the easiest to use and is the most recommended.

Note

Before installing the clients, make sure that they meet the minimal system requirements. Particularly make sure that the MDAC (ODBC) and Jet drivers are installed and functioning properly. This should be automatically the case for Windows ME, 2000, XP and 2003 machines where stable versions of MDAC are built-in to the system. For older operating systems (such as Windows 98 or Windows NT 4.0), you should ensure that the MDAC/Jet drivers are up-to-date (MDAC version 2.5 or later, Jet 4.0 SP4 or later. Please note that starting with MDAC 2.6, these are two separate downloads (MDAC and Jet)). The latest version of these drivers can be obtained from the Microsoft website http://www.microsoft.com/downloads.

Note

If there is a firewall running on any of the client machines (e.g. the Windows XP SP2 firewall - which is enabled by default), some of the ADNM's features

may not work correctly. For instance, File and Print Sharing must be enabled on the firewall to enable remote installation (otherwise, the installer would have no chance to push the installation packages onto the clients). For more information, please refer to the section *ADNM and Local Firewalls* in the *Advanced Topics* chapter. Fortunately, in the case of the built-in Windows XP firewall, it is possible to set its rules centrally by using the Group Policies.

5.1 Automatic (Push) Installation

To prepare the installation package, first go to the "Installation packages" folder and select the "Create Package…" option. Select the type of package to prepare (avast! Network Client is a version of avast! for workstations (more or less equivalent to avast! Professional Edition); avast! Network Server is a version of avast! for servers (equivalent to avast! Server Edition + its plugins); and avast! Mirror is a second-level mirror agent that can be used to load-balance the updating (described later).

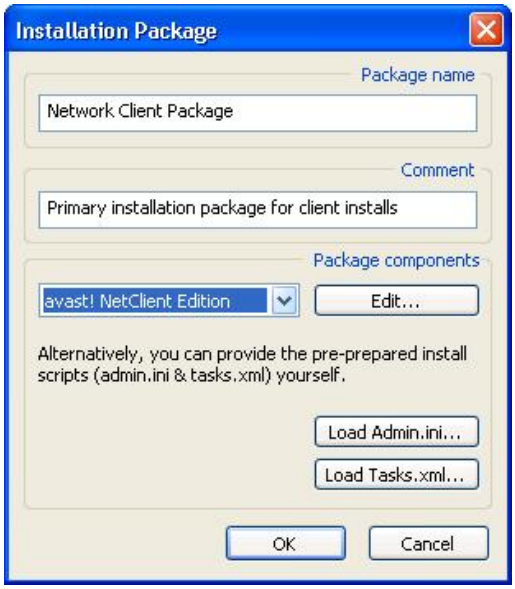

Figure 5.1. The installation package editor

Then click the "Edit…" button to actually set the installation properties. A wizard identical to the one that's shown when doing an interactive installation will be displayed. Set the installation properties, and make sure to save the changes. Pay special attention when entering the account name under which the avast! service will run.

Note

This account must have local administrative rights, and should also have (at least read-only) access to all network resources (to enable network scanning).

Please especially note that:

- the account must be valid on all machines on which you'll be using this installation package
- if you later change the password of this account, you'll have to manage the change of this info for all services on all computers (which may not be an easy task).

Therefore, it's often good idea to mark this account with the 'Password Never Expires' attribute.

After the installation package is ready, proceed to the creation of the deployment task. Navigate yourself to Tasks/Client-side tasks/Deployment tasks, and choose "Create New…". On the Install page, select the package you've just created.

Next proceed to the Login Accounts page. Here create all domain/username/password assignments that will be used while 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. For all workgroups/domains (as last resort), you can use wildcard domain name *.

Note

If the machines are in a domain, and you are using a domain account, make sure to specify the username in the DOMAIN\username format. E.g. if the name of the domain is UKOFFICE and the account you want to use is called "avast", you'd fill in "UKOFFICE" in the domain field, and "UKOFFICE\avast" in the username field (if you failed to specify the domain name as part of the user name field, it would have been interpreted as a local account, not a domain account).

The assignments are read from top to bottom and you can change their order by using the "Move Up" and "Move Down" buttons. For the deployment task to succeed, it's crucial to set this info correctly and completely. Otherwise, some of the machine won't be serviced due to a logon failure.

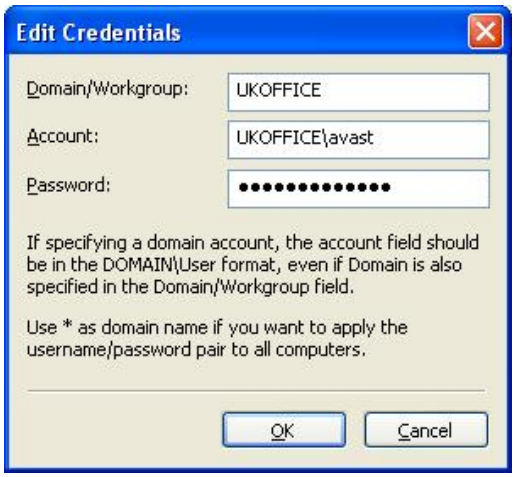

Figure 5.2. Definition of the accounts

Figure 5.3. The Login Accounts page of the ADNM Deployment task editor

On the last configuration page (Computers), you can specify the hosts that this task should run on. You can also specify computer groups – these should be included in brackets (like [Group1]) in case of static groups and parentheses in case of dynamic groups.

When the task is ready, all you need to do is run it and monitor its status (don't forget to refresh the view to keep track of the changes). You can either run it on the set of computers you specified on the Computers page (simply by double-clicking the task), or drag'n'drop it to a specific computer group to run it there (this technique applies to all ADNM tasks, not only Deployment tasks). You can also create a schedule to run the task periodically.

5.2 Manual Installation

If, for any reason, you are unable to use the Automatic Installation procedure described in the previous section, you'll have to deploy the avast! products to the network manually. To ease this process, it is recommended to copy the installation package to a network share so that you won't have to distribute it to every machine separately. This can be done by simply copying the InstPkgs subfolder of the AMS installation folder. This folder contains all files needed to install any supported managed product. The folder also contains the file setup.exe that will be used to start the installation.The program should be run with the following parameters

setup.exe /client /createprogress /sfx /sfxstorage "package-folder"

(in the case of workstation install), or

setup.exe /server /createprogress /sfx /sfxstorage "package-folder"

(in the case of server install), where package-folder stands for the full path name of the folder with the installation packages (and the setup.exe program itself). It may be set to "." if you have the current directory set to that folder.

To prevent the necessity to visit each and every machine on the network and manually run the installation program, you may consider taking advantage of the following methods:

- Placing the installation command to a logon script. This method is quite effective but has one major drawback -- on Windows NT based systems, you may experience installation failures caused by insufficient user rights. This is because the logon script usually runs in the context of a user who's logging on, and in most network scenarios many users don't have local administrative rights on the machine (required by the installer). Fortunately, this is not an issue on Windows 95/98/ME based systems.

- Sending out an e-mail containing a hyperlink to the installation program on the server (in the shared folder), with step-by-step instructions describing to your users how to click on that link and follow the installation wizard. This can be also quite efficient (if your users are sufficiently computer-literate) but unfortunately, the user right problem described previously remains.

- Wrapping the avast! installation files to a MSI package and distributing the MSI package by other means (such as the ActiveDirectory or Microsoft Systems Management Server).

5.3 Installation with MSI Packages

If you choose to deploy the avast! product line with the help of MSI (Microsoft Installer) packages, you first need to prepare (create) the packages. This is done by creating a deployment task, but chosing the "Generate MSI (don't deploy anything)" option on the Install page. In this mode, the targets specified on the Computer page are ignored (as no deployment is taking place). Running the task will create the MSI file.

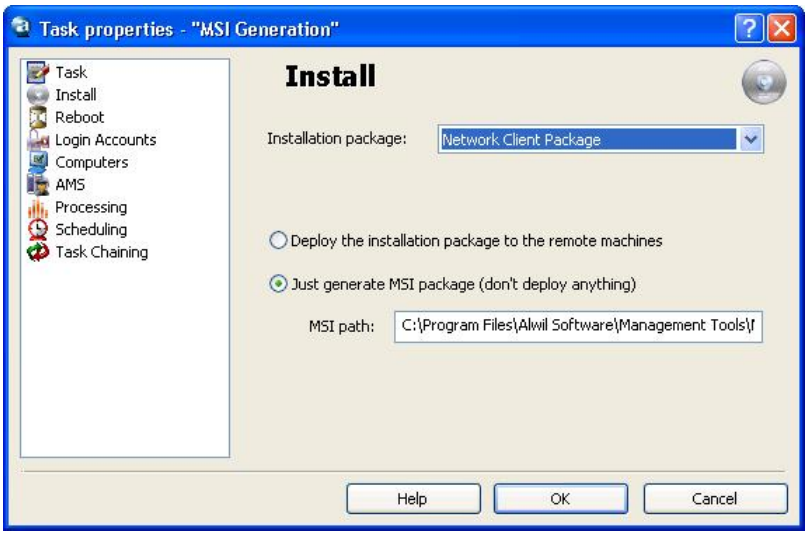

Figure 5.4. Deployment task can also be instructed to create a MSI file instead of doing the real installation.

With the MSI file in hand, you can either use your favourite software deployment tool (such as Microsoft Systems Management Server or even ActiveDirectory Group Policy) to push the installation to the clients or use the procedures described earlier in the Manual Installation section.

5.4 Installation by Disk Imaging

In larger organizations, it is common to install (prepare) new computers by the methods of disk imaging (also known as cloning). This is particularly convenient in cases where there is a big number of machines with the identical hardware configuration. There are specialized tools on the market, such as Symantec Ghost, that make disk imaging simple.

The disk imaging procedure usually consists of preparation of a sample machine - the "master" (i.e. installation of the OS and all application software as well as setting of all their parameters as required), subsequent capturing of machine's disk contents (at sector level) and transfering of the contents to any number of target computers (the actual imaging) .

It is generally possible to clone machines that have the managed avast! products installed. All defined settings will be kept and the communication channel with

the AMS will be maintained. However, some things (such as the agent GUID - i.e. the unique identifier that the agent uses to authorize to the AMS) have to be changed. For this reason, there is a special tool in all avast! managed version installations. The tool is called aswImgPr.exe and is a very simple command-line application which's only purpose is to prepare the avast! installation on the master for imaging. The "preparation" is only temporary - effective before a reboot takes place.

Note

There should be no reboot between running aswImgPr.exe on the master and capturing the image of its disk. If there's a reboot, aswImgPr.exe must be run again.

5.5 Uninstallation

Every decent program comes with an uninstallation program, and ADNM is no exception. If you opt to remove avast! from your network, you can use an Uninstallation task. Uninstallation task is a special type of task (also found in the Deployment Tasks folder in the console) which servers only one purpose: to uninstall all managed products from the selected targets. As usual, you can run the task either on all managed computers or just some of them (e.g. finely selected with the help of a dynamic group).

Note

Sometimes, it is possible that the Uninstallation task in the console stays in the "Running" state even if it has already completed (that is, the software has been removed from the client machines). This is caused by the fact that as part of the uninstallation process, even the agent is removed and therefore fails to report the final status of the operation to the AMS.

6

Using the ADNM

6.1 Managing the Antivirus Policies

ADNM's primary goal is to efficiently manage antivirus installations on the whole network. This chapter will guide you through the most common tasks you'll be facing every day while managing your network security with ADNM.

To be supplied.

6.1.1 Default settings of managed products

By default, the managed avast! versions are installed so that they are secured from computer users. That is, it shouldn't be possible to modify its functionality and/or configuration by a non-administrative user. Of course, if the user has administrative rights on the machine, there's very little that can prevent her/him e.g. from killing the avast! service processes and therefore disabling the protection altogether. This is yet another reason why it's usually not a good idea to grant your users admin rights.

The on-access scanner (the tray icon) is by default locked down so that it doesn't display any context menus or dialogs when clicked. It is expected that normal users shouldn't have the right to change any policies and so the associated GUI is disabled.

All avast! components are also preset in the way that they work in "silent mode", i.e. don't ask the user for actions but rather take actions automatically. The default action is "move to chest, and if that fails, delete". The only exception is the local scanners (the Explorer context menu scanner, the avast! Simple User Interface (if enabled) etc.) that are always interactive -- because it is assumed that the user is trying to run these programs to get an immediate, interactive result (e.g. manually verifying that files on a floppy drive are clean). And since the scanning is invoked solely by the user, it is not considered as part of the corporate policy and it's therefore left at user's discretion to decide what action to take if an infected file is detected.

6.2 Updating in ADNM

The ADNM uses so-called updating mirrors to provide efficient updating mechanisms to all machines on the network (even those that are not directly connected to the Internet). Mirrors also considerably save bandwidth requirements, because instead of downloading the updates to each and every machine on the network, they are downloaded only to the mirrors.

By default, there is a mirror on the AMS itself and it is the only mirror in the network (or in case of multiple AMS', there's a mirror on each of the AMS' and these are the only mirrors on the network).

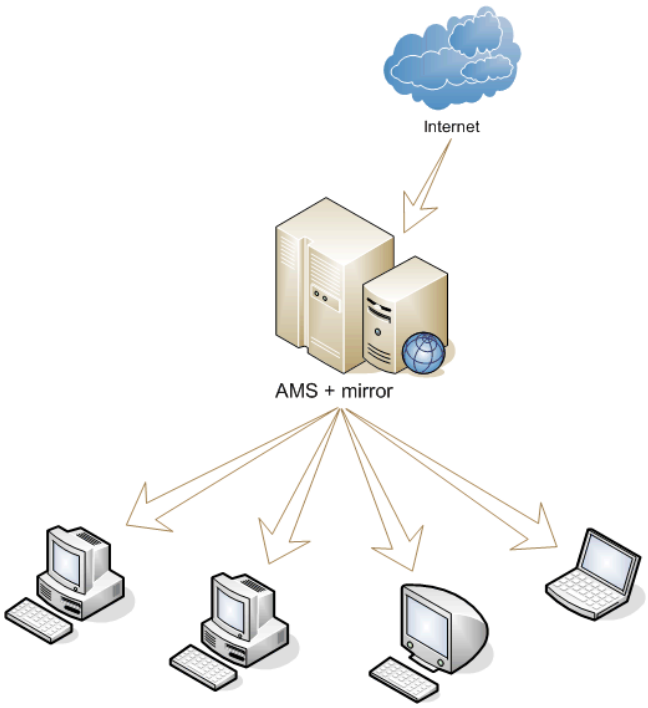

Figure 6.1. The easiest updating mirror scenario. The only mirror on the network is on the AMS iself.

Basic updating parameters for a machine can be set via the group's properties in Computer Catalog. This includes the auto-update interval.

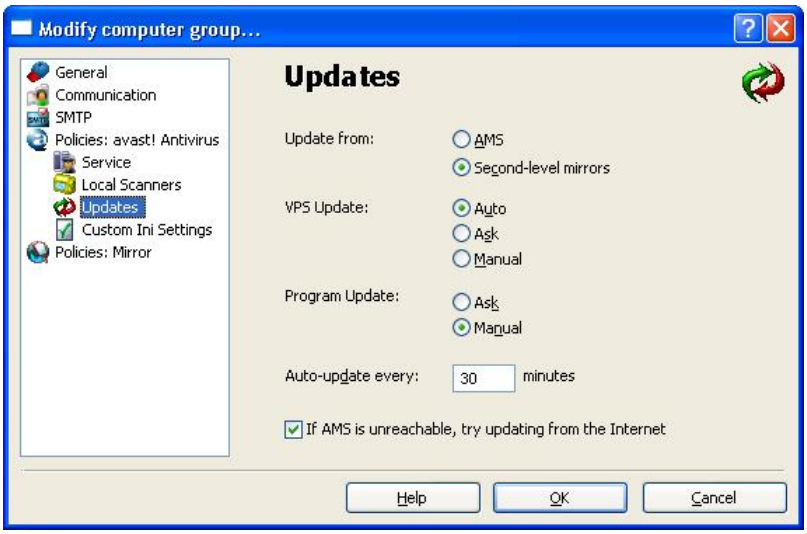

Figure 6.2. Computer group's Updating configuration page.

6.2.1 Deploying second level mirrors

In some cases, it may be necessary to have more than one mirror per AMS. For these purposes, it is possible to deploy any number of 2nd level mirrors. These mirrors are all equivalent (i.e. the client machines randomly choose from which to update at run-time) and their primary goal is to balance the server load (because in case of many machines managed by the same AMS, the AMS mirror may have problems serving all the clients on time). Each mirror should be able to serve hundreds of clients.

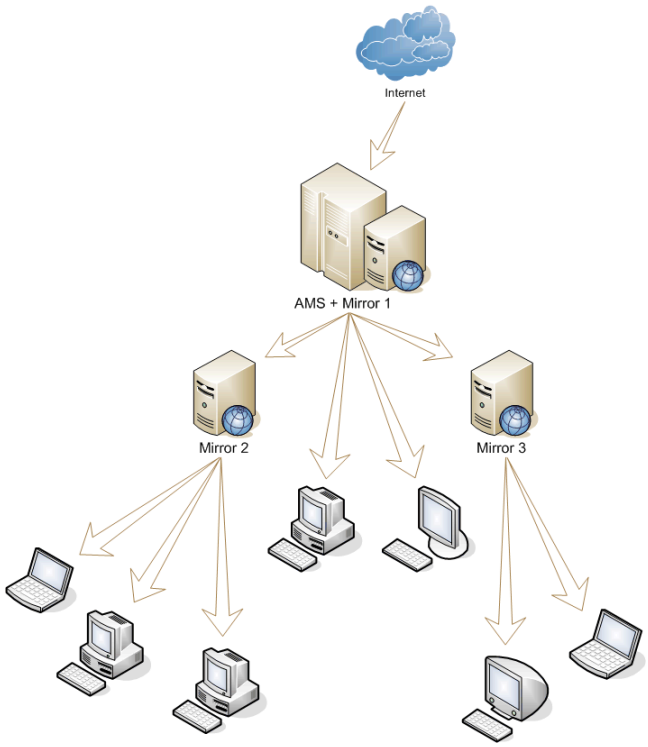

Figure 6.3. Configuration with 2nd level mirrors in place

To be supplied.

6.3 Monitoring the logs

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 AMS itself. This is, in most cases, done via the Events folder in the console (some of the entries are not logged to this folder. Please see the Monitoring AMS Logs section in the Advanced Topics chapter for more info).

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 agents. It may also contain some warning/error entries so it is useful to monitor this folder on a regular basis.

- Server events. This folder gathers events generated by the AMS (with the exception of task-specific events that are filtered out from this view). This includes a simple audit - entries documenting when the server was started/stoped, when a new object has been created etc.

- Custom events filter. This folder lets you define your own custom mask to exactly specify the events which 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 by using a Database Maintenance task (using the option Delete Events Older Than ... Days). For more info about the DB Maintenance taks, please refer to the AMS Maintenance chapter later on.

6.4 Licensing in ADNM

The ADNM provides very flexible licensing model. Basically, all license checking is done on the server. That is, as far as the managed machines are in touch with the server they use (inherit) its license. There is no need to manually distribute the license file to the clients (in fact, the license file is not even present on the individual machines - this prevents potential theft of the file). If the license on the server expires, so it does automatically on all the clients.

This basic behaviour works correctly in most cases. However, there're some situations where it cannot be used, e.g. when some of the machines are not permanently connected to the server (imagine laptops). There's a special

mechanism in ADNM for handling of such situations. Namely, the notebooks are only required to connect to the server at least once every 21 days (3 weeks; this value is hard-coded to the program and cannot be overriden). After this period, the managed products on the client machine will stop functioning (including virus database update) until a connection to the server is established and the server provides a valid license.

Note

If there's a requirement to take a machine out of the reach of the AMS for a period longer than 21 days, a separate license file copy must be locally provided to the machine (manually).

6.5 User Management in ADNM

The ADNM features a comprehensive system of users and user rights. There can be any number of user accounts created on the AMS. Please note that these are not in any way related to the Windows domain/workgroup accounts.

Users are stored in special containers - User Groups. By default, there are two users and two user groups: the Administrator account (located in the Administrators group) and the Guest account, located in the Guests group. These two accounts have special meaning and shouldn't be changed (the only thing that should be changed is the password of the Administrator account). The Administrator account has unlimited access to all objects in ADNM. The Guest account has very limited access rights and more or less cannot change (or even read/list) any objects. The password of the Guest account is empty and cannot be changed.

Figure 6.4. The user group editor

Each object in ADNM (task, schedule, alert, installation package etc.) has an Access Control List (ACL). The ACL specifies access rights to the object. There are four levels of access - read, write, delete and execute. There's also a special access type - 'Full Control' that combines all those four access types. Any account or group can be included in the ACL of an object, with any access level (the only exceptions are the members of the Administrators group that always have Full Control access to all objects).

Such a robust access-level system makes administration easier especially in larger corporations where there are multiple branch offices, each with its own set of administrators. In such a scenario, a typical way of setting up users would be to create an account for each administrator who will be working with ADNM, but limit his/her competency only to computers/objects that are under his/her administration. I.e. if an admin is e.g. responsible for management of LAN_A, you'd typically create a special computer group for LAN_A in the Computer Catalog, and assign full access rights for that group to the account. You'd also create special tasks for that group (that is, tasks that will run specifically on that group) and restrict access of that account to any other tasks. This way, you can have as many branch offices / local admins as you need, each being able to work only inside his/her own scope (part of the Computer Catalog).

6.6 Using the Dynamic Computer Groups

The dynamic computer groups provide a very powerful method to search, manage and further categorize the Computer Catalog. You can imagine it as a high-performance filter of the Computer Catalog, but in fact it can do much more. Namely, it can be used everywhere where a computer group is expected.

Each dynamic group is made of a set of expressions and logical operators. An example of an expression is "computer_name = NEMESIS" and an example of a logical operator is AND or OR. Expressions include operators like equals-to, smaller-than, greater-than and can also contain functions, such as MIN, MAX or AVERAGE. Individual expressions can also be nested together (support parentheses grouping).

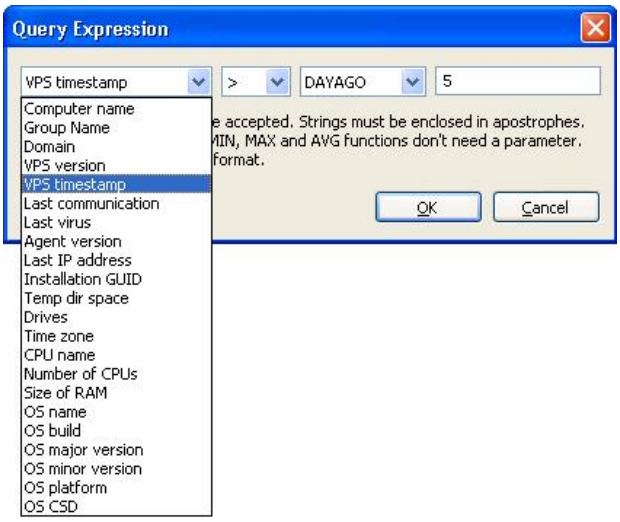

Figure 6.5. Dynamic group expression editor. Expressions can be conncted by AND and OR and grouped by paranthesis.

The following parameters are supported for building the expression:

- **Computer name** (type: string). Name of the computer as stored in the Catalog.
- **Group name** (type: string). Name of the (static) group in which the computer is stored in the Catalog.
- **Domain** (type: string). The name of Windows domain or workgroup in which the computer resides.
- **VPS version** (type: tri-dot string). The version 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! agent 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 that the machine used to contact the server.
- **Installation GUID** (type: string). The GUID (globally-unique-identifier) of the agent installed on the machine.

- **Drives** (type: string). The list of logical drives on the machine, separated by semicolon (such 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 bytes.

- **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. E.g., 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. E.g., 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. E.g., 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. E.g. "Service Pack 3".

The "tri-dot string" means a string in the form "a.b.c.d". It is used for some version numbers as well as IP addresses. All string values are allowed to use the * wildcard, e.g. the mask NEM* satisfies strings NEMO and NEMESIS but not NEON. The Last communication and VPS timestamp fields use date values in the form MM/DD/YYYY.

The following operators are supported:

- Equals-to, **=**.

- Not-equals-to, **!=**.
- Smaller-than, **<**.
- Greater-than, **>**.
- Smaller-than-or-equals-to, **<=**.
- Greater-than-or-equals-to, **>=**.

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 timedate type) occured at most N days ago. The operand specifies the value of N.
- **HOURSAGO**. This function returns the computer(s) for which the parameter (which must be of timedate type) occured at most N hours ago. The operand specifies the value of N.
- **MINUTESAGO**. This function returns the computer(s) for which the parameter (which must be of timedate type) occured at most N minutes ago. The operand specifies the value of N.

Logical operators for connecting of multiple expressions are only two: **OR** and **AND**. The dynamic group definition can be made up of any number of expressions connected by either of these of logical operators.

6.7 Other Good Practices

6.7.1 Scheduling Regular Scans

For extra security, it may be a good idea to schedule regular scans of all hard drives of all managed computers. Of course, the on-access scanner is the most important line of defense but there's nothing like being sure that there's really nothing that got through it.

Usually, it's more than enough to schedule on-demand scanning once a week. Consider scheduling the scans when the computers are idle as the scanning process may considerably slow down the machines and there's no way for the users to stop the scan. A typical choice is to run it at lunch time, on weekends or at night (if your policy is to leave the machines running overnight). The expiration property of the task governs how much time the job will stay in the work queue to be picked up by the target (this applies to all client-side tasks, not only on-demand scanning tasks). E.g. if it's set to 6 hours and the scan is scheduled to run at 2 am, a computer will either be turned on before 8 am and the task will be started, or it will be turned on after 8 am and the task will not be started on it at all (a time out error will be indicated in the task session). This is a convenient way to prevent the scheduled scans designed to run e.g. at night from running in the working hours, decreasing the productivity of your users.

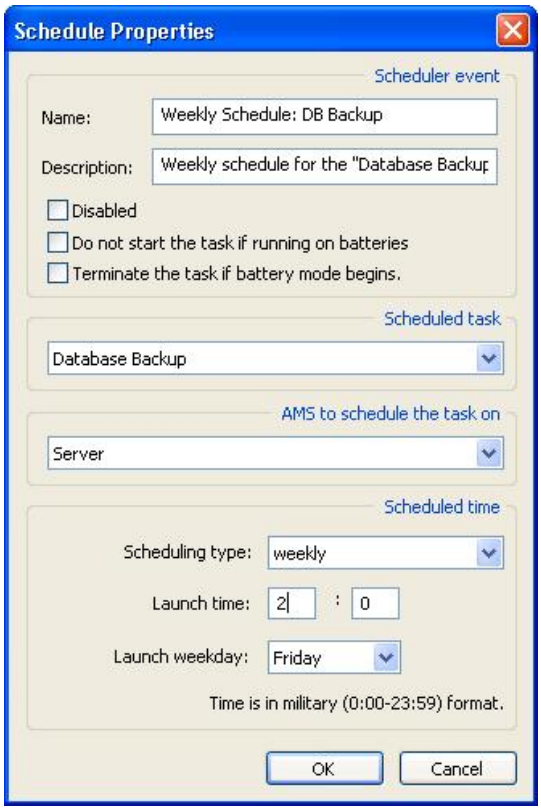

Figure 6.6. The task schedule editor

6.7.2 Covering New Computers

In most networks, computers come and go. Efficient managment of a network which changes often can be a nightmare. Fortunately, the ADNM contains mechanisms that can help administrators easily cover new machines (i.e. automatically push avast to newly created machines).

Achieving this goal requires some work but is an interesting example of how a

number of ADNM features can be used together to provide some advanced functionality. Namely, we'll use the following components:

- Discovery tasks
- Deployment tasks and installation packages bound to them
- Dynamic computer groups
- Task chaining
- Task scheduling

We'll start by preparing an installation package for the avast! NetClient product (if we haven't done so yet). Next we create a deployment task and bind the installation package to it. Make sure to correctly specify valid credentials for all domains/workgroups to be really able to install the software on all machines on the network. Next, we create a dynamic computer group for all machines without the agent installed. This can be done in multiple ways but one of the most straightforward options is to use the simple expression "Agent Version not equal to zero". We use this dynamic group as a target for the deployment task. It remains to create a discovery task, and use the Task chaining feature to indicate that after the task successfully finishes, the deployment task we created in the previous step is to be run. Last, we create a schedule for the discovery task (e.g. daily) to automate the whole procedure.

7

Reporting in ADNM

ADNM features very powerful reporting capabilities that are second to no other competitive product on the market. You can use a variety of useful reports from the information that is collected by the AMS from the clients and exports these to many popular formats. You can even have the reports sent to the management team automatically in periodic intervals.

Reporting in ADNM is realized, as almost anything other, by certain tasks. Reporting tasks are grouped in a special folder in the console, under the Server-side tasks category.

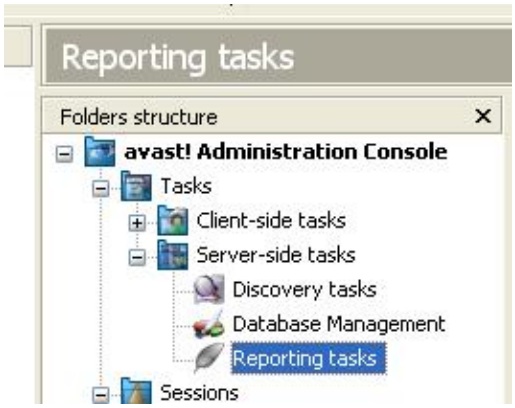

Figure 7.1. Reporting tasks in the console tree

7.1 ADNM Reports

ADNM comes with about twenty pre-prepared reports, as described below.

7.1.1 Network machines summary

This report lists all computers on the network. It exists in two basic versions. The first type gives only a summary of computers with information to which group they belong, what operating system they run and what managed products they have installed. Second possible type of report contains all the above information plus detailed information about the computers on the network. Please note that this report can be very large and in it's usually worth trying to reduce its size by applying additional filters.The filtering options include group

name mask and computer name mask. You can also specify sorting of the data by computer group/name in ascending or descending order.

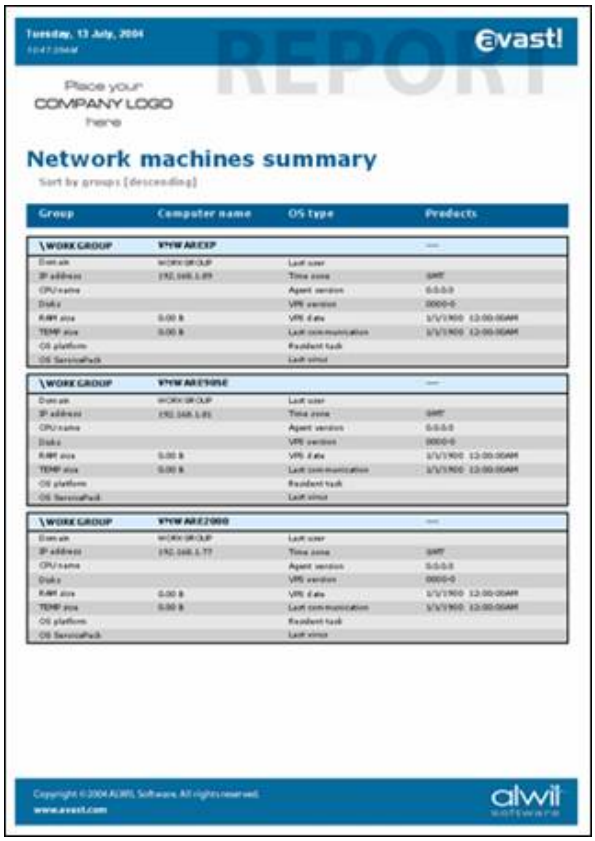

Figure 7.2. The Network machines summary report

7.1.2 Network machines summary according to avast!

This report creates a summary of all computers on the network with special respect to the computers have the managed avast! installed. Again, this report can be generated both in a summarized and complete variants with detailed information of each computer. The settings of this report are the same as the previous report. It also consists of a pie diagram from which the administrator can easily find out which computers do have avast! installed and which do not.

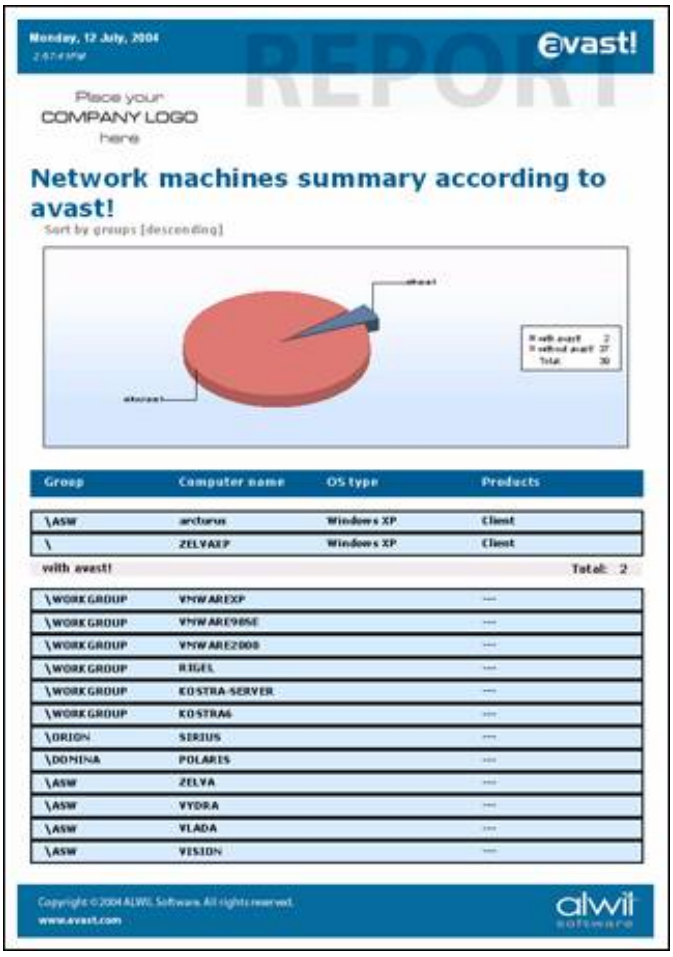

Figure 7.3. The Network machines summary according to avast! report

7.1.3 Network machines summary by avast! version

This creates an easy to read report (with pie diagram and a table view) that shows all versions of avast! that are installed on computers on the network. The report can also include machines without avast! installed so it can also be used to check the overall status of antivirus protection on the network.

7.1.4 Network machines according to VPS version

This report is also similar to the previous one with the exception that instead of avast version, the key here is the version of the virus database (the VPS file). Again, it can be set to include computers that do not have avast! installed, filter machines by computer or domain masks etc.

7.1.5 Network machines summary according to last communication

This is a tabular presentation of all network machines sorted by the last time they reported their status to the AMS. Useful for discovering communication problems as well as finding zombie computers. As with the other network

summary reports, offers a reasonable level of customization.

7.1.6 Top N viruses

Taking advantage of 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 the virus. You can customize the N parameter that specifies the number of entries to be included in the report (e.g. Top 5, Top 10 etc.). Although this parameter is not limited, we suggest not to use numbers higher than 20 as otherwise, the report may become less readable.

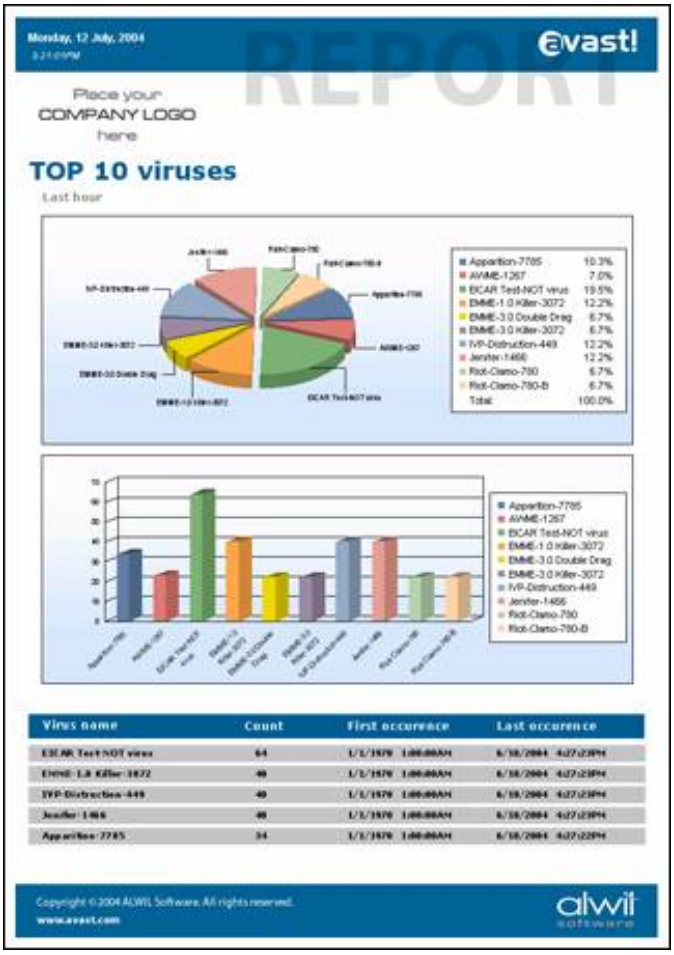

Figure 7.4. The Top N viruses report

7.1.7 Actions on Top N viruses

This report is very similar to the previous one with the exception that it shows the actions taken on Top N viruses, not the viruses themselves. The selection of data included in the report can be done by time/date period, virus name mask and, as usual, the N parameter. Again, we don't recommend setting N to

a larger value than 15.

7.1.8 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 names of the infected files are prefixed by the name of the computer where the virus has been detected. You can customize the N parameter that specifies the number of entries to be included in the report. Although this parameter is not limited, we suggest not to use numbers higher than 15 - 20 as otherwise, the report may become less readable. Another configuration parameter is the date/time span (including custom spans) for which to include the infected files.

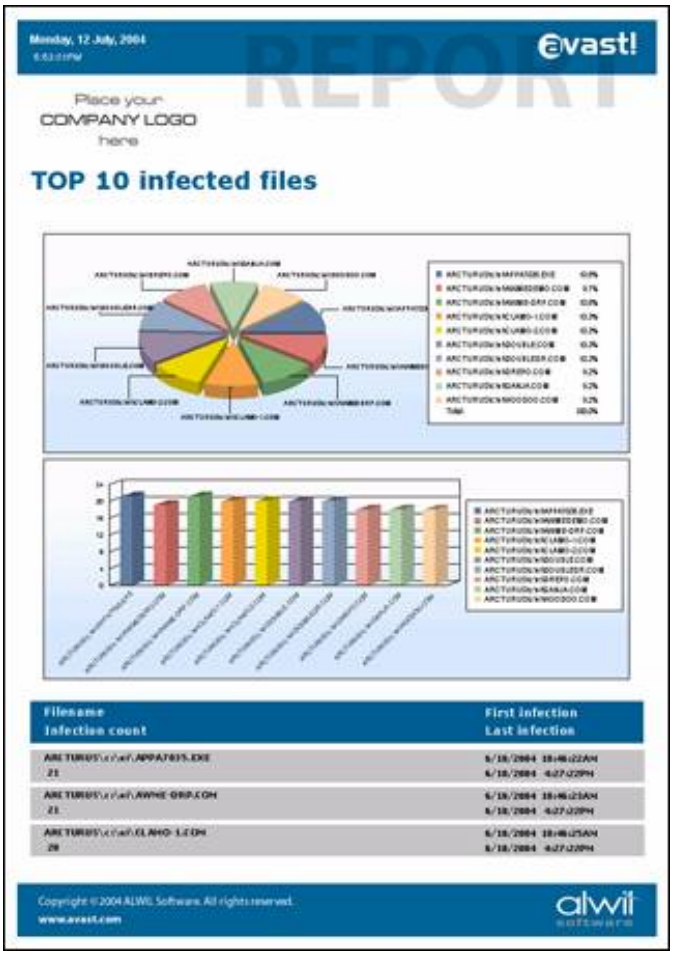

Figure 7.5. The Top N infected files report

7.1.9 Top N infected computers

This report shows a summary (pie diagram and a table) of Top N most infected computers on the network. You can specify if the report should also include

detailed information about the computers in the table. It is possible to customize the N parameter that specifies the number of entries to be included in the report. Again, we suggest not to use higher a number than 15 - 20. As usual, you can also define a group and domain mask and a date/time period.

7.1.10 Infection source summary

This report creates an easy to read table which will show the ratio of different infection vectors (mail, hard disk, removable media, network, script). You can define the time/date value for which the report will be generated. The report also contains a pie diagram for easier comprehension.

7.1.11 Network infection summary

The Network Infection Summary report is similar to the Top N viruses report - with the difference that it shows a list of all viruses that have been found on the network (not only Top N). If the number of viruses is too large so that the report becomes not so easily readable, it is suggested to reduce the virus list by applying a mask or narrowing the date/time period to be included in the report.

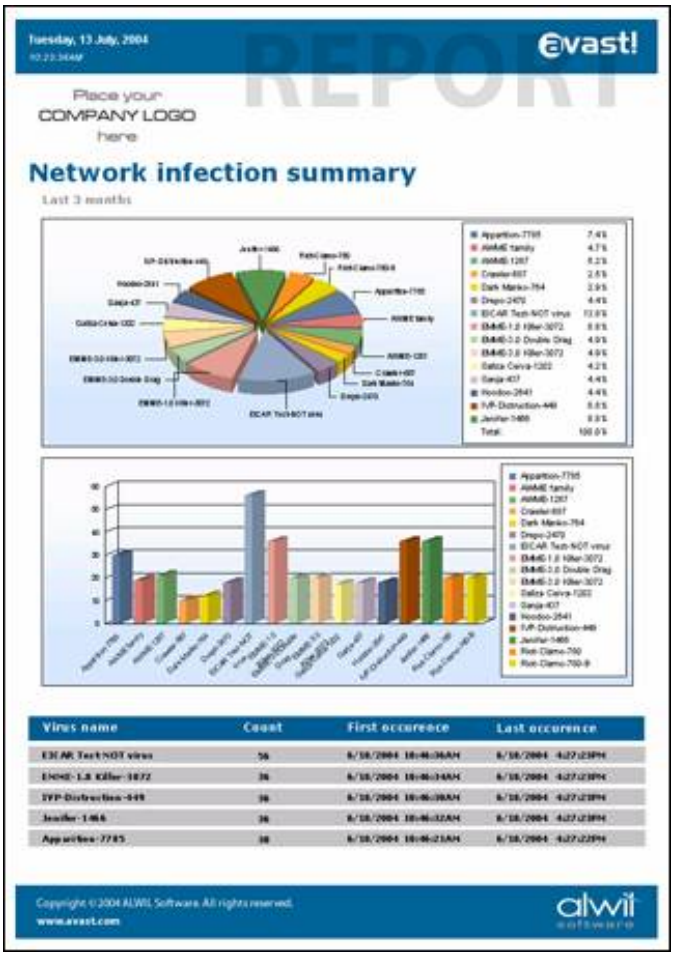

Figure 7.6. The Network machines summary report

7.1.12 Virus actions summary

This report gives a tabular and graphical presentation of actions taken on the infected files (deleted, repaired, moved to Virus Chest etc.). Again, you can set the time/date period for which the report will be generated.

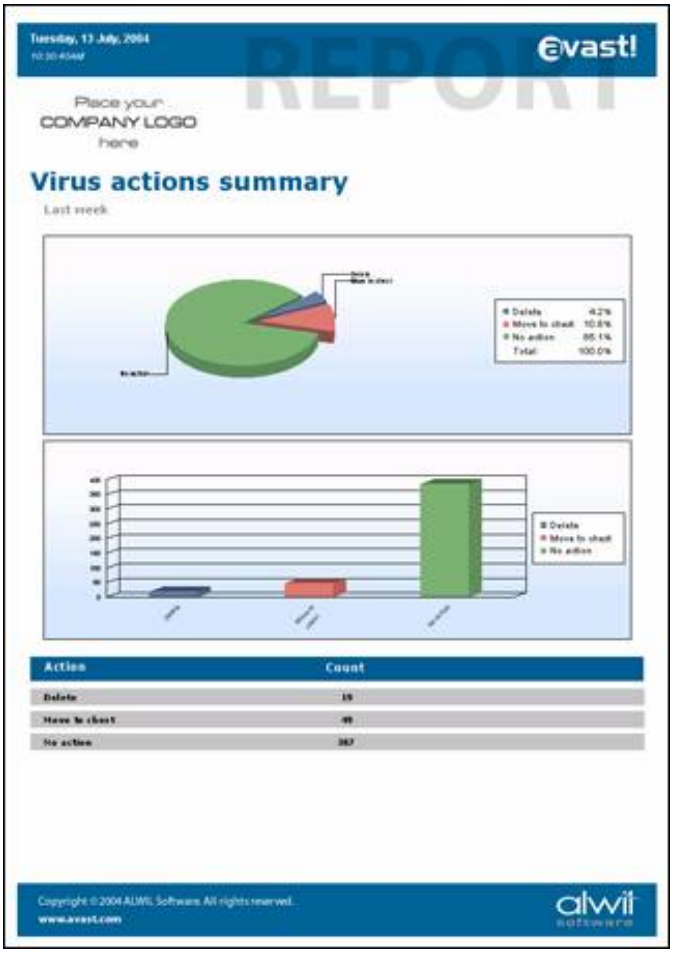

Figure 7.7. The Virus actions summary report

7.1.13 Change of logical disks summary

This report is a bit different because it is not directly related to the antivirus protection. Instead, it shows the summary of changes of logical drive mappings on the managed computers (e.g. attachment of a USB disk, mapping of a network drive etc.). You can customize the report by specifying the time/date period in which the drive mapping change should have occurred.

7.1.14 Top N attacked computers

This report shows the list of Top N computers which have been attacked (unsuccessfully) by a network worm, as detected by the Network Shield provider of avast!. Again, you can define the parameter N as well as the the time/date period for which the data are to be included. For better readability, the report is generated in the form of a pie chart, a bar chart and a table.

7.1.15 Top N network attacks

The Top N Network Attacks report shows a summary of network attacks as detected by the Network shield provider of avast!. Again, you can define the N parameter that will determine how many attacks will be included, as well as time/date period in which the attacks have been detected. The report also includes comprehensive information about the attacks, including the IP address they came from and time stamps. For enhanced readability, the report also includes a pie chart and a bar chart.

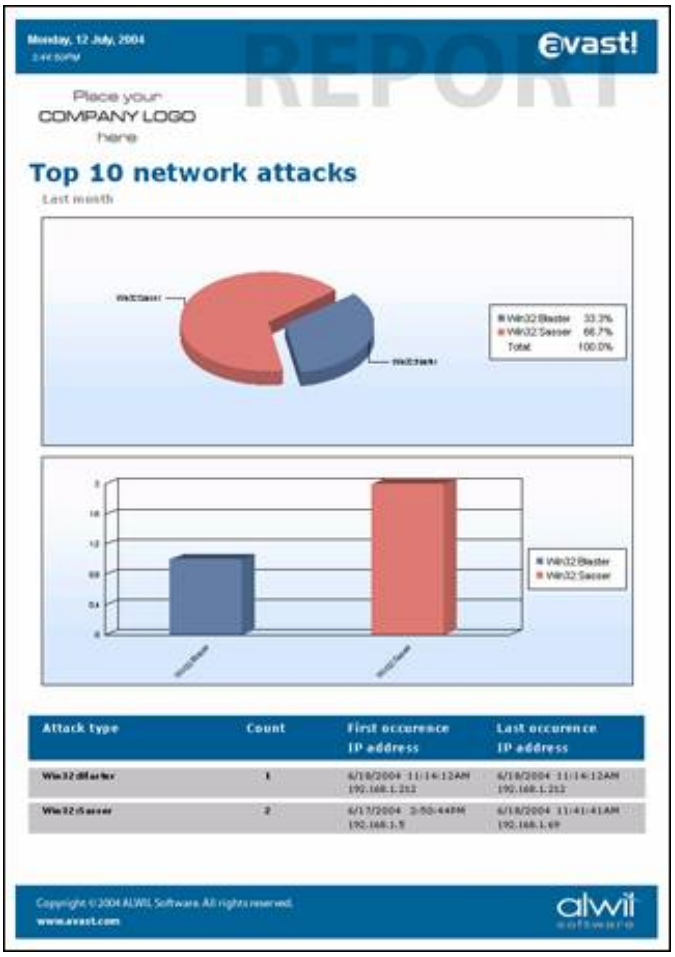

Figure 7.8. The Top N network attacks report

7.2 Report Targets

The reports can either be generated directly to the task session (to be viewed and/or printed from the console via the integrated report viewer), or exported outside the database. Export targets include files (possibly on network shares) and e-mail. Exports formats include PDF, HTML, DOC and XLS. All these parameters can be set in the reporting task properties.

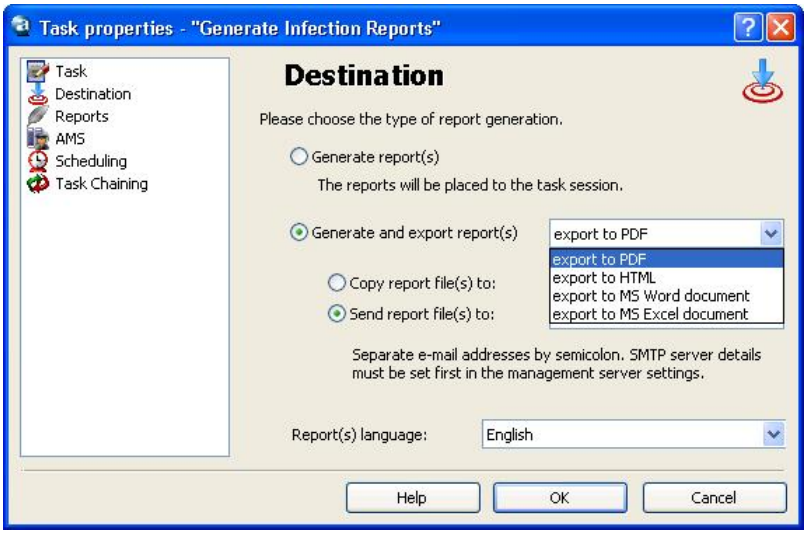

Figure 7.9. Properties of a reporting task

7.3 Using a Custom Company Logo

As can be seen on the report screenshots above, the ADNM lets you place a custom logo to all reports it generates. Such a customization can help maintain corporate identity (especially in the print outs) as well as help administrators who manage more than one network to quickly distinguish reports generated for particular AMS.

To define a custom logo, use the Miscellaneous page of the global settings dialog. Supported image formats are png, jpg and bmp. The picture can be of any size but it is recommended to maintain the aspect ratio of 5:14; otherwise, stretching will occur. It is also recommended not to use large image files as the picture will be part of every report generated and if large, can waste space in the database.

8

AMS Maintenance

8.1 Database Maintenance

As ADNM is based on a SQL database, it requires frequent maintenance. For these purposes there's a special type of server-side tasks in ADNM - 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 periodical backup of the whole database is highly recommended. You should incorporate the backup of the ADNM database to your overall network backup strategy. The recommended way is to either use your backup software to directly back up the SQL server (if it supports it - please consult your backup software documentation for details), or use an ADNM DB Maintenance task to back up the database to a file and then back up that file using standard methods.

Database cleanup can be used to remove older records from the database. You can decide how old records you'd like to keep. Of course, once you delete the old records it won't be e.g. possible to generate reports from older data so it's important to decide how much data you need. DB cleanup is important to prevent the database from growing indefinitely. The DB Maintentance task also offers the ability of deleting of so-called orphaned records that can reduce the size of the database.

8.2 AMS Maintenance Tool

In ADNM, there is also a couple of things that cannot be done via the console but instead must be performed directly on the server. For these purposes, there's a special program called " AMS Maintenance Tool" that provides means to achieve most of these tasks.

Specifically, the AMS Maintenance Tool can be used to perform the following tasks:

- Change the product license file.
- Change the server SSL certificate
- Perform a restore operation of the database (database backups, on the contrary, can be executed by using the Database management tasks from the administration console (or even scheduled to run periodically). **Note:** restoring of the database will destroy its previous contents. It's a good idea to create a backup immediately before doing the restore.
- Check the validity of the database
- Delete and reinitialize the database - this is useful if you want to start from scratch. **Note:** deleting or recreating of the database will destroy its previous contents. Make sure to create a backup before performing these operations.
- Change database connection details. Use this option e.g. when you want to move the database to another SQL server or upgrade from MSDE to a full SQL server (create a backup, change database connection details and finally perform restore of the backup).

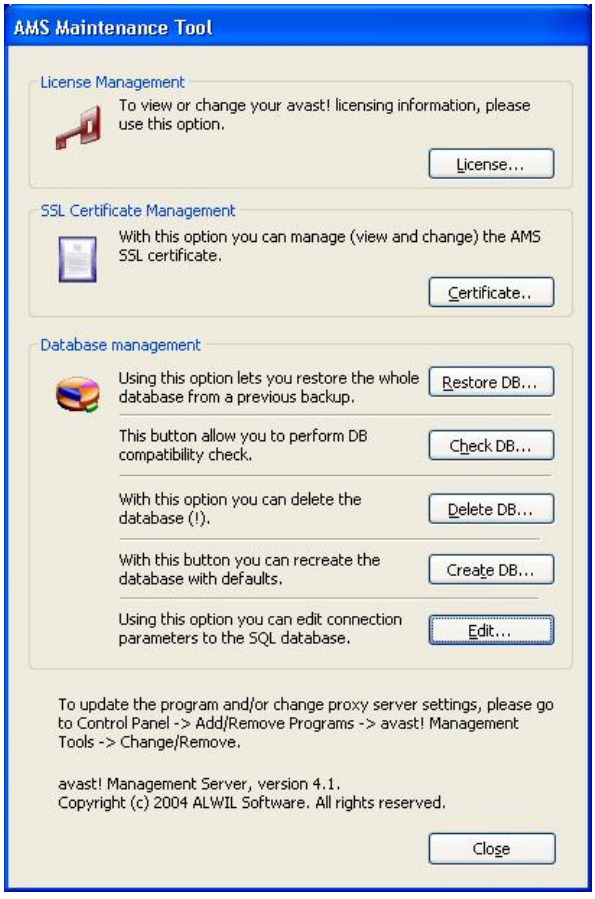

Figure 8.1. The AMS Maintenance Tool's main window.

The AMS Maintenance Tool can be found in the ADNM group in Start menu. As already said, it cannot be run remotely but should work correctly inside remote desktop / terminal server connections.

8.3 Proxy Settings Change

Since the AMS provides mirroring of the updates, it is important to have the proxy server details set correctly. These details are initially set when the AMS is installed but it may be sometimes to necessary to change them. To change the AMS proxy server settings, you'd do the following: open Control Panel, Add/Remove Programs, and go to the "avast! Management Tools" entry. Click the Change/Remove button next to it. A dialog will be shown. One of the options in the dialog is the change of the proxy server.

8.4 AMS/Console Updates

While maintaining regular updates is most important for the case of local clients (i.e. the antivirus agents), it is also a good idea to keep the AMS and the console(s) up-to-date. AMS and console updates (which are in fact always released at the same time and hence share the same version number) are released every couple of months. This section will guide you through the AMS/console updating procedure.

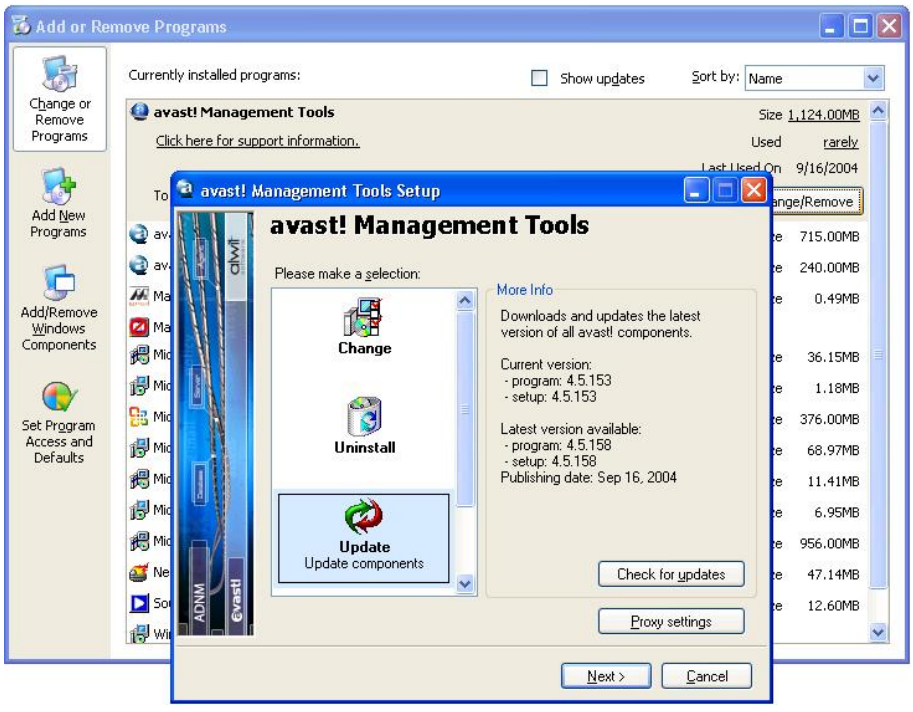

Figure 8.2. Updating the AMS and/or the console.

Warning

Update of the AMS is quite a difficult task because it also involves updating of the SQL server database (data transformation to the new format, if the format of the database (tables, stored procedures etc.) has changed) and typically results in some downtime and may also require a reboot of the server. Therefore, it is wise to plan the update to off-peak time (non-business hours, weekends etc.).

Use the following steps to update the AMS and the console:

1. Shut down all the consoles that are running.

2. Perform update of the AMS. To do that, open Control Panel (directly on the AMS), Add/Remove Programs, and go to the "avast! Management Tools" entry. Click the Change/Remove button next to it. A dialog will be shown. One of the options in the dialog is Update. Click Next to start the update. You can also first try the Check Updates button that will provide you with information on the version numbers (current version and the latest version available for download). After the update completes, you may be requested to reboot the server. Confirm with OK and let the server reboot.

3. Update all the consoles. Follows the same procedure as described for the case of AMS update, but this time on the machine(s) to which the consoles have been installed.

Note

Please make sure not to run any of the consoles before the update is complete (that is, between updating the AMS and the consoles) - otherwise, there will be a version discrepancy and the program may not work correctly.

4. (Optionally) perform a program update of all the network agents using an Updating task. This will ensure that all components of the system are up-to-date.

9

Advanced Topics

9.1 Monitoring of the AMS Logs

Besides the events written directly to the database (both client side and server side logs that can be viewed in the Events folder in the administration console), the AMS also logs certain entries to separate log files. These logs are usually used for troubleshooting purposes. The reason why they're not written to the database is that the database connection may not be available (e.g. it's impossible to log database connection problems to the database).

Most of the logs are stored in the adnm\data\log folder so you can use e.g. Notepad to view them (Error.log and Warning.log are usually the most important). The logs can be also viewed directly from the console, by using the menu item View / Show AMS 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 are able to connect to the AMS, that is, if the AMS service is running and functionable (not always the case if there's a need to troubleshoot something).

Mirror logs are stored in the folder adnm\mirror\logs, and the log entries of the AMS installer/updater are written to adnm\setup\setup.log. Both of these can also be opened by using the View / Show AMS Logs command in the console.

9.2 How the clients look for the AMS

The ADNM was designed to work correctly even on networks with unreliable links, constantly changing hardware and other anomalies that make administration hard. One of the key elements of this design is that the agents deployed on the managed machines do their best to find a suitable AMS (even though it is true that the clients are able to protect the machine even in the case of longer lapses of communication with the AMS)

This is the algorithm that an agents uses to find the AMS:

1. Uses the predefined server. If that fails,

2. tries to use the last known good server address. If that fails,

3. tries to find a server on the network by sending a broadcast packet and waiting for an answer. If that fails,

4. tries to connect to a machine with hardcoded name avastms.

9.3 Moving AMS to another machine

Thanks to the fact that the clients use many different methods to find an active AMS (as described in the previous section), it's quite easy to move the AMS to a different machine (especially if you're using a full SQL server and don't want to move the database, just the AMS itself). The same procedure also applies in the case where there's e.g. a hardware failure of the AMS, or you just simply want to replace the hardware by a more powerful one.

To move the AMS (just the AMS, not the database) to a different machine, follow these steps:

1. Install AMS on the new machine. When asked for SQL Server details, supply the connection info that the old server is currently using.

2. When the installation is complete, stop the AMS service on the old machine (Control Panel / Administrative Tools / Services, avast! Management Server).

3. Using a console, connect to the new server, and

   - change the AMS address in the Properties window of all relevant groups in the Computer Catalog

   - wait for a pop timeout to occur on the client machines (5-15 minutes by default, unless it has been changed in the global AMS settings).

   - verify that the clients on the network are moving to the new server (that is, that the Last Connected field keeps getting updated)

4. If everything is working fine with the new server, optionally uninstall the AMS software from the old machine.

To move the AMS, including the database, to a different machine, follow these steps:

1. Perform a database backup on the old server.

2. Install AMS on the new machine. When asked for SQL Server details, either use MSDE or supply connection info for the new database.

3. When the installation is complete, start the AMS Maintenance Tool (from the ADNM group in Start menu), and restore the database from the backup you've made in step 1.

4. Stop the AMS service on the old machine (Control Panel / Administrative Tools / Services, avast! Management Server).

5. Using a console, connect to the new server, and

   - change the AMS address in the Properties window of all relevant groups in the Computer Catalog

   - wait for a pop timeout to occur on the client machines (5-15 minutes by default, unless it has been changed in the global AMS settings).

   - verify that the clients on the network are moving to the new server (that is, that the Last Connected field keeps getting updated)

6. If everything is working fine with the new server, optionally uninstall the AMS software from the old machine.

If the clients don't seem to be connecting to the new server, here are some troubleshooting options:

- Try giving the AMS machine DNS name avastms. The clients should recognize this special name and start connecting to the machine.

- Try manually changing the AMS name on the clients. To do this, log on as an administrator, open the file avast\data\avast4.ini, and change the entry ServerAddress= to indicate the address of the new AMS. Delete the line with the entry LastServerAddress=xxx. Then start the Registry Editor, navigate to HKLM\Software\ALWIL Software\avast\4.0\SS, and delete the values ServerAddress and LastServerAddress. Finally, restart the "avast! NetAgent" service.

9.4 The Multi-AMS Model

To be supplied

Checklist:

- Enable network protocols on all SQL servers (svrnetconn.exe). Security warning
- Subscribe to root, description of all fields
- Create and schedule replication task
- Run reporting, discovery etc. on root only (discovery can be run if there's no intersection)

9.5 Accessing the AMS From Outside

To be supplied (roaming users; description of ports that need to be allowed on the firewall; security warning)