avast! Distributed Network Manager (ADNM)

Administrator's Guide

alwil
software

avast! Distributed Network Manager (ADNM): Administrator's Guide

Published October 3, 2007 (Rev. 1.2.0)

Table of Contents

1

Basics

Welcome to the avast! Distributed Network Manager, the solution for network antivirus management.

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

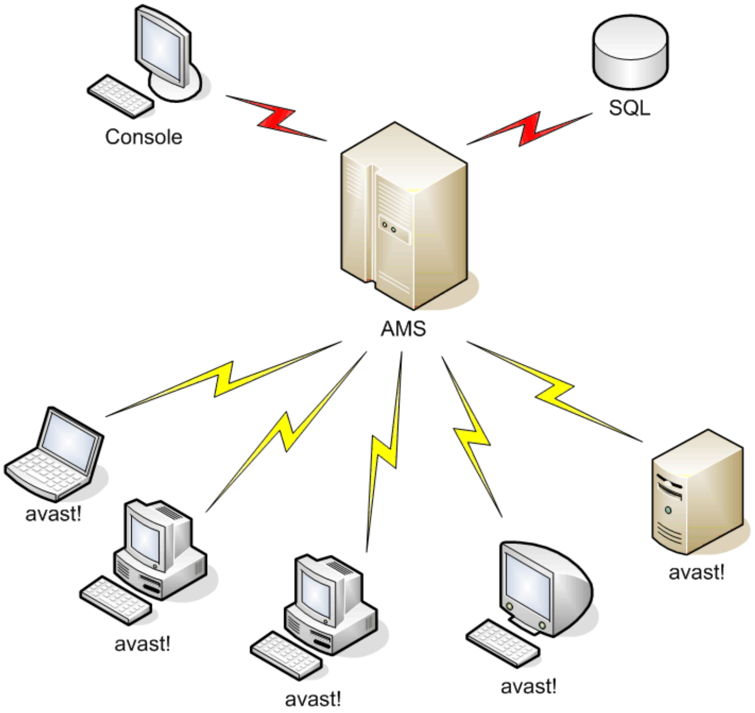


Figure 1.1. Basic ADNM diagram

The managed machines connect only to the AMS to download the latest policies and to report their status and scan results. The Administration Console also connects directly to the AMS. The AMS is based on an SQL Database – either a dedicated MS SQL Server 2000/2005, if available, or, for small and medium-size networks, on its lightweight version, MSDE 2000, which is part of the ADNM installation package (alternatively, one can use the free version of SQL Server 2005, "SQL 2005 Express"). 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's (each having its own database). These can then be instructed to replicate their databases on a regular basis, and also to upload all scanning results to a dedicated AMS on which enterprise-wide reporting can 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 think about how you'll be deploying it.

The following things need to be carefully considered:

AMS

- On which machine will you deploy the AMS?
- Is it going to be a dedicated machine? If not, what else will run on the machine? Will the other software 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? (It should.)
- Is a full-blown MS SQL 2000/2005 database going to be used, or 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 of several hundred computers or fewer).
- Can we use just one AMS or would it be better to choose the multi-AMS model? Generally, multiple AMS's 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? The following conditions must be met to install the AMS:
    - A Windows NT/2000/XP/2003/Vista-based machine with at least 128MB RAM (512-1024MB recommended); please note that Windows Vista and

Windows x64 Editions do not support MSDE.

- CPU power depending on the size of the network – Pentium III or higher recommended.
- At least 500MB 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 several people?
- 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 Neighborhood 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 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 you've chosen to hold the AMS, and run the setup program (setup_adnm.exe). This will start the setup wizard, which will guide you through the installation process. You'll be asked for the following information:

- Destination folder.

- Components to install (either 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 use the attached DEMO file, or supply your own if you've 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 you're using does not contain the MSDE packages (i.e. you're using setup_adnm_no_msde.exe) and the MSDE installation could not be found 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_adnm_no_msde.

- Options for updating mirror creation and synchronization. We strongly recommended that you let the setup program generate the mirror – otherwise, you'll have to initialize the mirror yourself. Letting the setup do it will preset all the values for you automatically, so you won't have to do anything later. Of course, the mirroring process requires an active Internet connection (HTTP only) - unless you configure it to use another updating mirror as a source.

After all the files are copied and 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 consoles to "normal" user's machines, though, as that may result in unauthorized tampering with the AMS (although this can be prevented very well by using appropriate security measures, such as strong passwords, etc.).

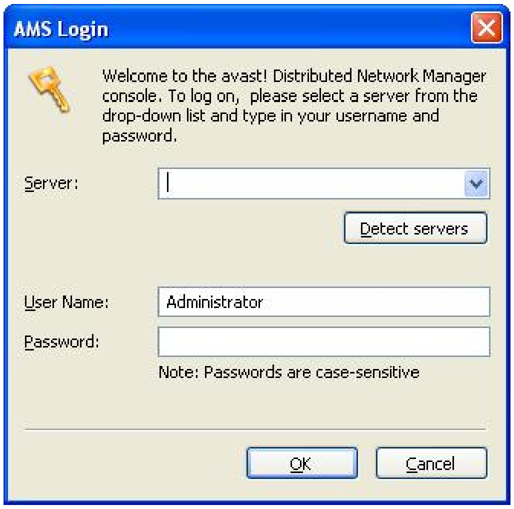
To install the console, you follow the same procedure as when installing the AMS, except that when asked for the components to install, you uncheck the 'Management Server' box, leaving only the Console option checked.

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. The Log On window will display. 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's on the network.

Note

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, because leaving the password set to its default value directly compromises system security.



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

Server:

User Name: Administrator

Password:

Note: Passwords are case-sensitive

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 used by the server 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 such warnings from appearing on this machine unless the AMS certificate is changed (a rare event).

When the connection to the server succeeds, 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.

Note

Please note that the AMS works as a traditional server (network listener). That means that if there is a firewall installed on the AMS machine, it must be configured to allow the AMS service (AvEngine.exe) to listen on selected ports. Also, the ADNM mirror listener service (httpd.exe) should be enabled for both inbound and outbound access. No action is required in case of Windows XP SP2 / Vista firewall as the program takes care of defining appropriate rules automatically.

3

The Console – First Steps

3.1 Basic Console Concepts

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

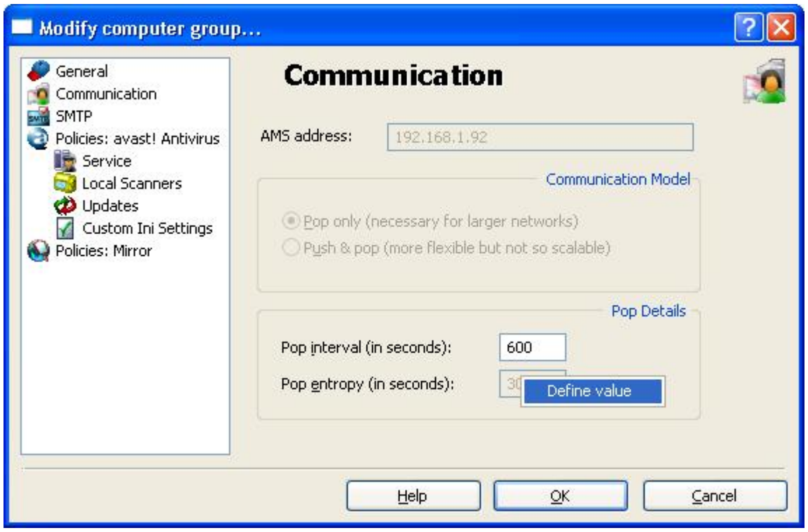
- **Tasks.** Tasks are the basic building blocks of ADNM. A task is a definition of a job, i.e., a prescription of what to do. A task also has associated computers that it should run on, and associated schedules that govern when it should run. There are many types of tasks in ADNM, but the basic distinction is 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 such as reporting and database maintenance tasks, run on the AMS itself.

- **Sessions.** Each time a task is run, the avast! software creates a session for it. A session is an object that defines a particular run of a task. For example, if task A is run five times, five different sessions are created, each holding results of the specific run. 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 predefined sessions with special meaning. The "On-Access Scanners" session holds all the results of all on-access scanners on the network. The "Local Scanners" session holds the results of all local on-demand scans, that is, 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, 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.



Modify computer group...

Communication

AMS address: 192.168.1.92

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): 30

Figure 3.1. By default, Computer Group properties are inherited from the parent but can be overridden at any level.

- **Management Servers.** This is where information about all management 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 AMS's 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) who are permitted to access the management capabilities of the AMS. Of course, different users have different rights. The users can be bunched into 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 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 holds the scheduler event objects that define when the tasks will run. This is one way to edit the schedule. Another is to define the scheduling rules in the task's properties.

- **Installation Packages.** Because the Deployment tasks run silently (without any user intervention), they need to have all the installation options properly preset. The Installation Packages are used to define the settings that will be used by the Deployment tasks to push installations to the clients. Options include: what product to install, destination 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 ease navigation within it.

Note

Please note that the console view is not automatically refreshed. To see the respective changes, you need to keep refreshing the view yourself by hitting the F5 key or using the appropriate menu item.

3.2 First Steps After Installation

Here is a typical series of steps taken when a new AMS is installed:

- 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 setting the policies in the tree the structure of the Computer Catalog (by modifying the properties of individual computer groups).

- 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 easier it will be to assign the security policies and the better the whole ADNM will perform. It is therefore important to pay special attention to its creation.

There are basically two different ways to create the Catalog. These two methods can be combined. The first method makes use of a special type of server-side task, the discovery task, to build the catalog automatically. The second method consists of importing the information from an external source file. You can also create entries in the catalog directly by using the console's GUI, but this is tedious for more than a few machines.

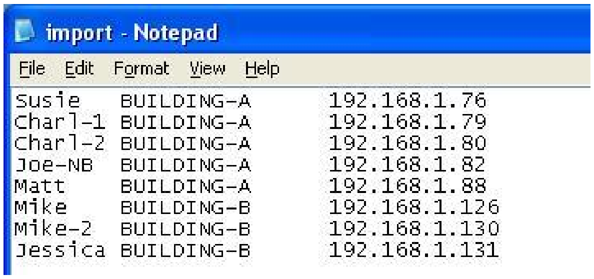
4.1 Using a Discovery Task

Using a Discovery Task is probably the easiest and most convenient way to build the Catalog. To use it, go to 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 inserts them to the Catalog, either to the root or to 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, though. Again, please note that the view is not automatically refreshed; 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. Don't forget to refresh the view to see all the new items.

4.2 Importing Computers from an External Source

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 ADNM'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 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 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. This column is optional; you don't have to specify this value if you don't want to.



```
Susie   BUILDING-A      192.168.1.76
Charl-1 BUILDING-A      192.168.1.79
Charl-2 BUILDING-A      192.168.1.80
Joe-NB  BUILDING-A      192.168.1.82
Matt    BUILDING-A      192.168.1.88
Mike    BUILDING-B      192.168.1.126
Mike-2  BUILDING-B      192.168.1.130
Jessica BUILDING-B      192.168.1.131
```

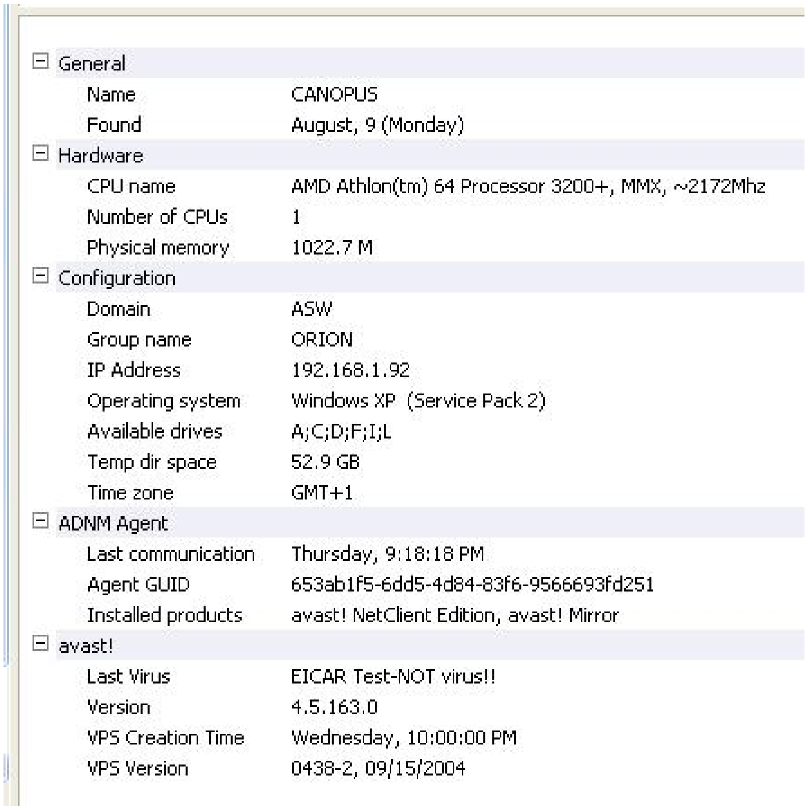
Figure 4.1. Importing Computers to the Catalog from a Text File.

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 to any folder in the Computer Catalog and select the Import Computers... menu option.

4.3 Viewing the Cataloged Computers

The ADNM monitors a number of interesting details about each and every managed machine, related both to avast! and to system configuration. This information can be used by the administrators to analyze problems and also to get a better idea of the overall network structure.

The stored information includes the computer name and 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.



⊟ General	
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

Figure 4.2. Basic information about a managed machine in the Computer Catalog.

The console also distinguishes Individual computers in the Catalog by icon. 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 AMS.

Red computer. This icon indicates 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).

Black computer. This icon indicates that the computer hasn't communicated with the AMS recently (but still has a managed product installed). The time period after which computers are marked as black can be customized in the global AMS 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.

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.

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 larger number of computers than the ADNM license permits. The AMS 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.

5

Deploying the avast! Product Line

There are five 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/Vista-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.

The first choice is the easiest and usually the best.

Note

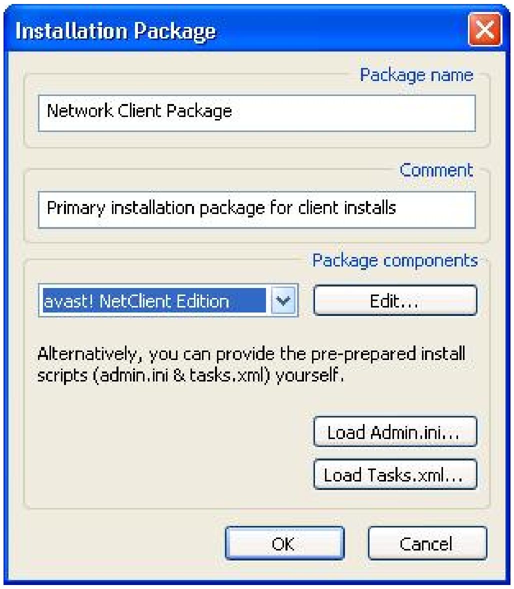
Before installing to the clients, make sure that they meet the minimal system requirements.

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 remote installation, File and Print Sharing must be enabled on the firewall. Otherwise, the installer will be unable 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, by using the Group Policies, you can set rules centrally for the built-in Windows XP firewall.

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).



Installation Package

Package name: Network Client Package

Comment: Primary installation package for client installs

Package components: avast! NetClient Edition

Alternatively, you can provide the pre-prepared install scripts (admin.ini & tasks.xml) yourself.

Figure 5.1. The installation package editor

Then click the “Edit…” button to set the installation properties. A wizard identical to the one shown during an interactive installation will be displayed. Set the installation properties, and make sure to save the changes.

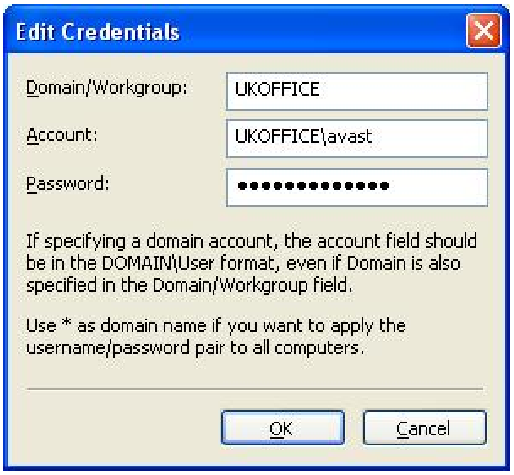
After the installation package is ready, create the deployment task. Navigate to Tasks/Client-side tasks/Deployment tasks, and choose “Create New….” On the Install page, select the package you’ve just created.

Next, proceed to the Login Accounts page. Here, you can 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 a last resort, you can use wildcard domain name *.

Note

If the machines are in a domain, and you are using a domain account, be sure to specify the username in the DOMAIN\username format. For example, 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 fail to specify the domain name as part of the user name field, it will be interpreted as a local account, not a domain account.

The assignments are read from top to bottom. 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 machines won’t be serviced due to a logon failure.



Domain/Workgroup: UKOFFICE

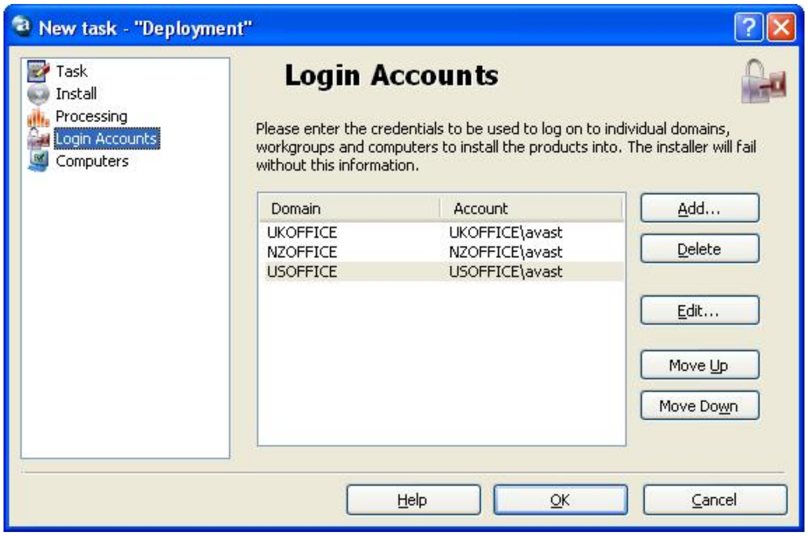
Account: UKOFFICE\avast

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.

Figure 5.2. Definition of the accounts



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
UKOFFICE	UKOFFICE\avast
NZOFFICE	NZOFFICE\avast
USOFFICE	USOFFICE\avast

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 computers in groups. Static groups should be enclosed in brackets — e.g., [Group1]. Dynamic groups should be enclosed in parentheses — e.g., (Group 2).

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 run it on the set of computers you specified on the Computers page, simply by double-clicking the task, or your can drag 'n' drop it onto a specific computer group to run it on those machines. 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 make this process easier, copy the installation package to a network share so that you won't have to distribute it to every machine separately. You can do this can be done by 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 avoid visiting each and every machine on the network and to run the installation program manually, you may consider the following methods:

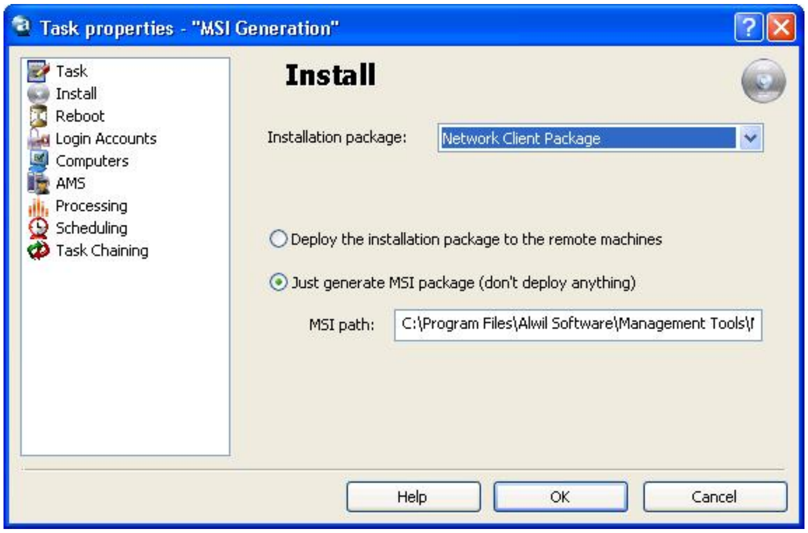
- Placing the installation command in a logon script. This method is quite effective but has one major drawback — on Windows NT-based systems, you may experience installation failures caused by insufficient user rights. This is because the logon script usually runs in the context of a user who's logging on, and in most network scenarios many users don't have local administrative rights on the machine, which are 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 in the shared folder on the server, with instructions to your users 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 rights problem remains.

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

5.3 Installation with MSI Packages

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



Install

Installation package: Network Client Package

○ Deploy the installation package to the remote machines

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

MSI path: C:\Program Files\Alwil Software\Management Tools\

Figure 5.4. A deployment task can also be instructed to create an MSI file instead of doing the real installation.

With the MSI file in hand, you can either use your favorite 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 means of disk imaging, also known as cloning. This is particularly convenient when there is a large number of machines with 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 preparing a sample machine — the "master" — by installing the operating system and all application software, and setting all their parameters as required, then copying the master machine's disk contents at the sector level and transferring it 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 have to be changed, such as the agent GUID, the unique identifier that the agent uses to authorize to the AMS. 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 with one purpose: to prepare the avast! installation on the master for imaging. The preparation is only temporary, effective until 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 good 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. Also found in the Deployment Tasks folder, in the console, the Uninstallation task uninstalls all avast! managed products from the selected targets. You can run the task on all managed computers, or only on some of them — for example, on selections made with the help of a dynamic group.

Note

Sometimes 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 because even the agent is removed as part of the uninstallation process, and therefore it fails to report the final status of the operation to the AMS.

6

Using the ADNM

6.1 Managing the Antivirus Policies

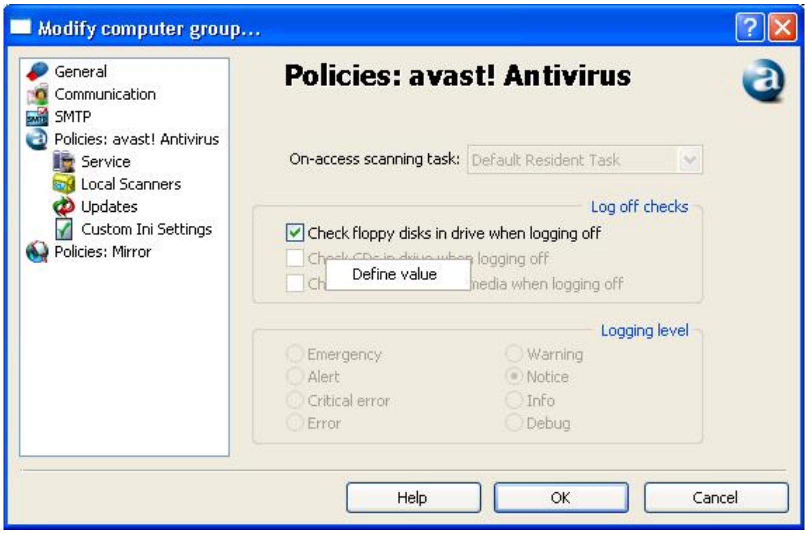
ADNM's primary goal is to efficiently manage antivirus installations on the whole network. This chapter will guide you through the most common tasks you'll face every day while managing your network security with ADNM.

6.1.1 Computer Catalog Management Basics

Most management-related settings are specified in the properties of the Computer Catalog groups. That is, in ADNM, policies are not applied to specific machines, but rather to groups of machines. If you have a machine with individual management needs, you should create a separate group for it first, typically a subgroup of the group the machine currently resides in.

Each group has its own set of policies. By default, the policies are inherited from the parent group, hence the hierarchical structure. However, they can be overridden at any level.

An undefined policy value is indicated by the appropriate control being grayed (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 grayed. 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."



Policies: avast! Antivirus

On-access scanning task: Default Resident Task

Log off checks

☑ Check floppy disks in drive when logging off
□ Check CDs in drive when logging off
□ Ch... media when logging off

Logging level

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

Figure 6.1. Overriding parent group policies. The "Define value" menu is brought up by using the right mouse button.

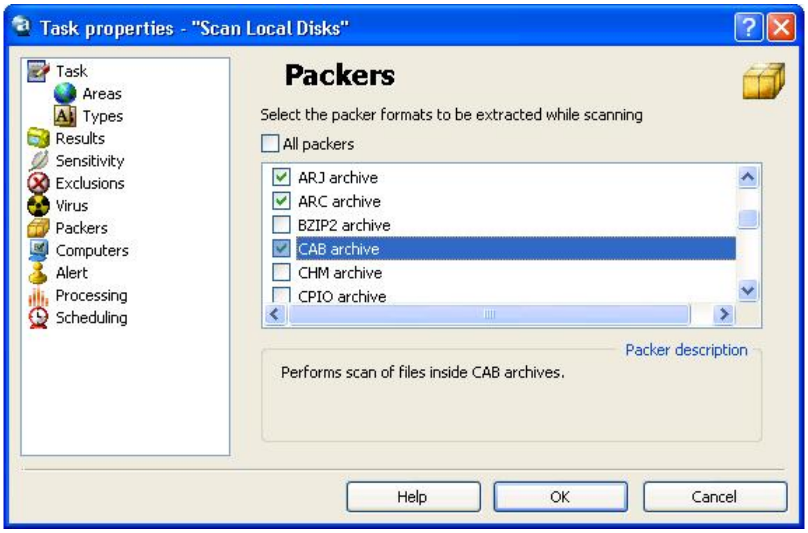
The Properties dialog contains policy settings for all supported managed products, whether they are actually installed on the client machines or not. If a machine has only the Mirror product installed (the Mirror is also considered a managed product), the avast! Antivirus policy settings will not be effective for that machine, but the Mirror policy settings will.

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

6.1.2 Using On-Demand Scans

ADNM 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 a folder of the same name, under the Client-side tasks folder.

The task editor offers a large number of settings, which can be customized. These include areas to scan, thoroughness of the scan, results to be posted to the AMS, and the archives the scanner should unpack during its execution. Of course, the task also defines default computers it will run on.



Packers

Select the packer formats to be extracted while scanning

☐ All packers

☑ ARJ archive
☑ ARC archive
☐ BZIP2 archive
☑ CAB archive
☐ CHM archive
☐ CPIO archive

Packer description

Performs scan of files inside CAB archives.

Figure 6.2. Properties of an on-demand scanning task.

When the task is ready, you can either run it immediately or schedule it to run periodically. If you run the task immediately by using the "Run Task" menu option, it will run on the computers predefined in the task's properties. If you use the drag 'n' drop method to drop the task on a group in the Computer Catalog, it will be run on that group, and the default computers setting will be ignored.

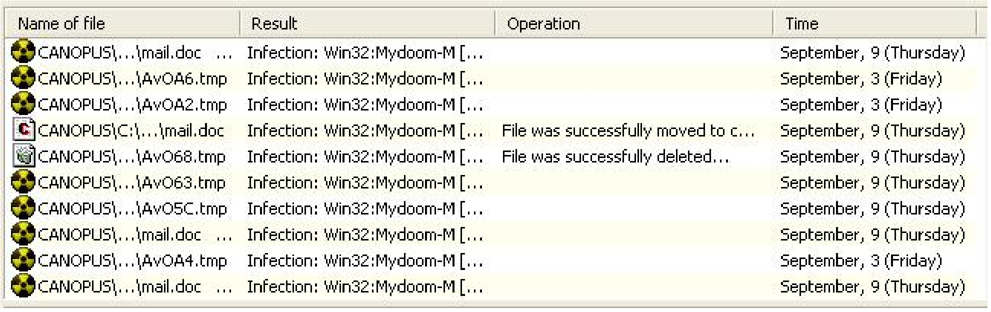
More information about scheduling on-demand scan tasks can be found in the section "Scheduling Regular Scans" later in this chapter.

6.1.3 Monitoring Scan Results

All scanning tasks (both on-access and on-demand) can generate infection-related results. These results are stored in the database for future reference, report generation, or direct viewing.

The task results are stored in task's session. A session is a representation of any given instance or run of a task, complete with its results. Sessions can be found in the Client-side Sessions and Server-side Sessions folders.

The console presents session results in a table. Each result (file) is stated on a single line, including the full file name and the name of the machine on which the file resides, the name of the virus (if the file is infected), and any action performed by avast! on the file.



Name of file	Result	Operation	Time
CANOPUS\...\mail.doc ...	Infection: Win32:Mydoom-M [...		September, 9 (Thursday)
CANOPUS\...\AvOA6.tmp	Infection: Win32:Mydoom-M [...		September, 3 (Friday)
CANOPUS\...\AvOA2.tmp	Infection: Win32:Mydoom-M [...		September, 3 (Friday)
CANOPUS\C:\...\mail.doc	Infection: Win32:Mydoom-M [...	File was successfully moved to c...	September, 9 (Thursday)
CANOPUS\...\AvO68.tmp	Infection: Win32:Mydoom-M [...	File was successfully deleted...	September, 9 (Thursday)
CANOPUS\...\AvO63.tmp	Infection: Win32:Mydoom-M [...		September, 9 (Thursday)
CANOPUS\...\AvO5C.tmp	Infection: Win32:Mydoom-M [...		September, 9 (Thursday)
CANOPUS\...\mail.doc ...	Infection: Win32:Mydoom-M [...		September, 9 (Thursday)
CANOPUS\...\AvOA4.tmp	Infection: Win32:Mydoom-M [...		September, 3 (Friday)
CANOPUS\...\mail.doc ...	Infection: Win32:Mydoom-M [...		September, 9 (Thursday)

Figure 6.3. Scanning task results

6.1.4 Default Settings of Managed Products

By default, the managed avast! versions are installed so that they are secured from computer users. That is, a non-administrative user shouldn't be able to modify the software's functionality or configuration. If the user has administrative rights on the machine, there's little to prevent her/him from, for example, killing the avast! service processes and disabling the protection altogether. This is one reason why it's usually a bad idea to grant your users admin rights.

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

All avast! components are preset to work in "silent mode," i.e., to take actions automatically without asking for user input. The default action is "move to chest, and if that fails, delete." The only exception is in the local scanners, such as the Explorer context menu scanner and the avast! Simple User Interface (if enabled), which are always interactive because it is assumed that the user is running these programs to get an immediate result, for example, verifying that files on a floppy drive are clean. Since the scanning is invoked by the user, it is not considered part of corporate policy, so it's left up to the user to decide what action to take if an infected file is detected.

6.1.5 Custom INI Settings

Some settings (policies) of the managed products cannot be directly set by using 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 avast4.ini on the managed clients.

ADNM makes setting these properties much easier with remote batch editing of client avast4.ini files. In fact, the INI file entries become part of the Computer Group properties (and, as such, use features like inheritance). The INI file settings can be entered on the "Custom INI Settings" page of the group properties dialog. 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).

6.2 Updating in ADNM

The ADNM system offers very flexible options for update management, for distribution of both virus database and full (program) updates.

ADNM 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, ADNM downloads only to the mirrors and then distributes the updates locally.

By default, there is a mirror on the AMS itself, and it is the only mirror on the network. If using multiple AMS's, there's a mirror on each AMS by default, and these are the only mirrors on the network. All managed machines download updates from the AMS mirror on the AMS if a connection to the AMS is available. That need not be the case, for example, for notebook users. See the end of this chapter for more information on roaming users.

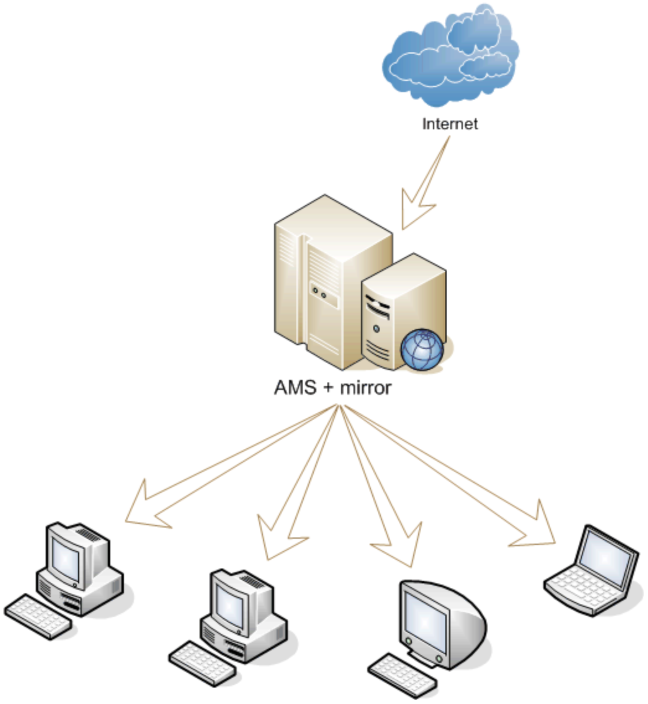
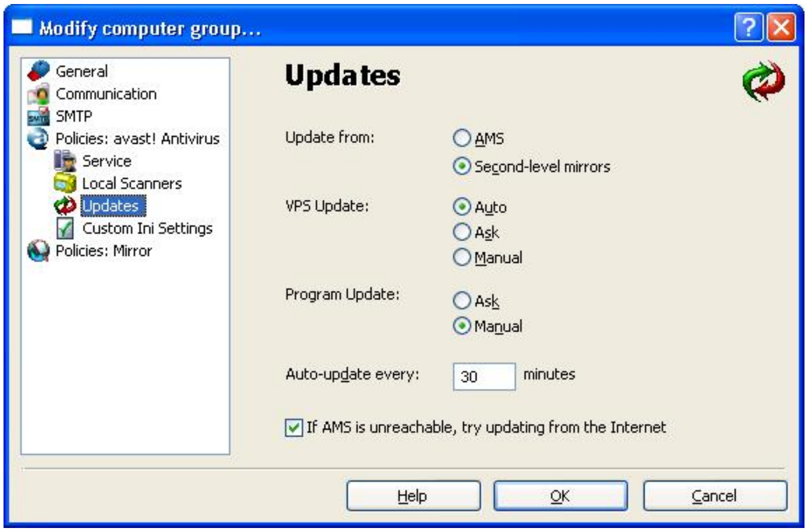


Figure 6.4. The easiest updating mirror scenario. The only mirror on the network is on the AMS itself.

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



Updates

Update from: ○ AMS ● Second-level mirrors

VPS Update: ● Auto ○ Ask ○ Manual

Program Update: ○ Ask ● Manual

Auto-update every: 30 minutes

☑ If AMS is unreachable, try updating from the Internet

Figure 6.5. Computer group's Updating configuration page.

Updating tasks

For on-demand updating, there's a special task type: the updating task. To create an updating task, navigate to the Updating tasks folder, and select New Task. Choose Updating in the Task type field, and specify the target machines for this task on the Computers page. You can also customize the way the program handle the situation where a reboot of a client computer is required to complete the update.

Special Updating Needs

The single-mirror model should accommodate most types of networks. It offers reasonable scalability for networks of hundreds of machines and is by far the easiest to administer. However, it may not be sufficient if

- this is a large network with thousands of computers, or
- the AMS machine does not have access to the Internet (not recommended), or
- there is a requirement to test each and every update on a set of test machines before releasing it to the network.

6.2.1 Deploying Second-Level Mirrors

If the single-mirror scenario doesn't meet the needs of your network, you can deploy any number of second-level mirrors. These mirrors are all equivalent, i.e., the client machines randomly choose at run-time which one to update from. Their primary goal is to balance the server load. When many machines are 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.

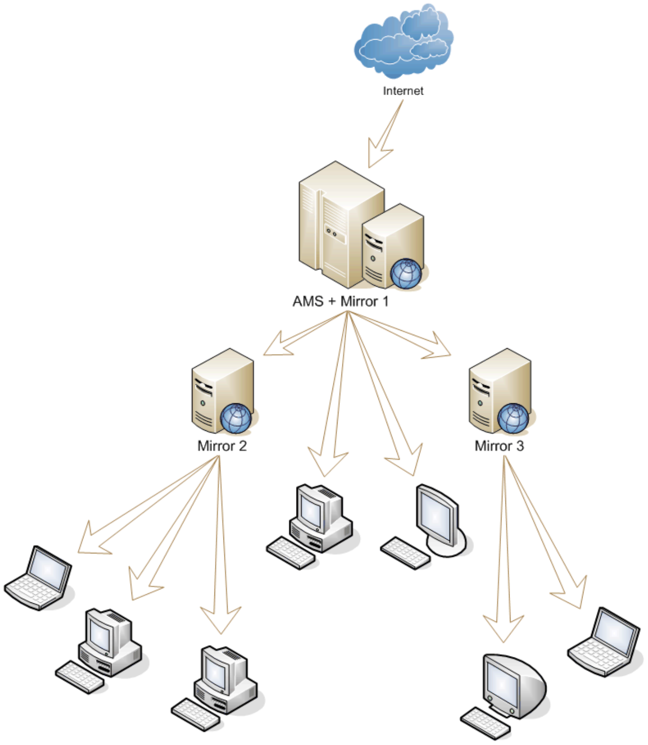
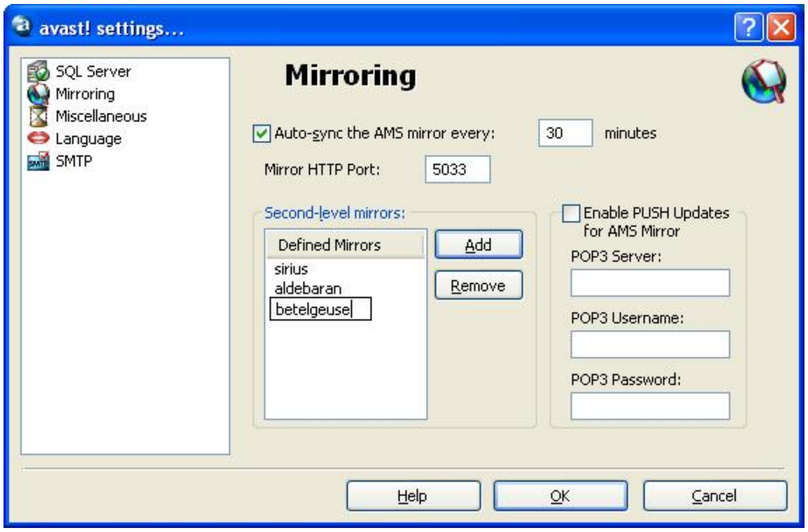


Figure 6.6. Configuration with second-level mirrors in place

To use second-level mirror(s), they first need to be installed on the target machines. Mirrors are handled like any other managed product in ADNM. That is, their roll out is accomplished the same way as deployment of avast! antivirus clients: by creating an installation package and then using one of the methods discussed in the previous chapter, usually a deployment task.

The mirror software can be used as soon as it's installed. The second-level mirrors must be registered in the AMS. Do this by using the "Mirroring page" of the global Settings dialog in the console. Here you must list all second-level mirrors currently in use. You can use IP addresses (if they are fixed) or DNS names, as shown on the following screenshot.



Mirroring

☑ Auto-sync the AMS mirror every: 30 minutes

Mirror HTTP Port: 5033

Second-level mirrors:

Defined Mirrors
sirius
aldebaran
betelgeuse

☐ Enable PUSH Updates for AMS Mirror

POP3 Server:

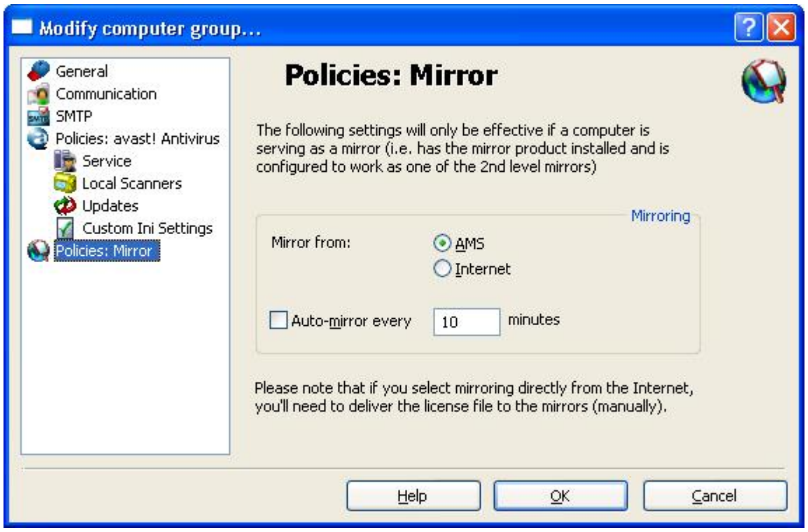
POP3 Username:

POP3 Password:

Figure 6.7. Configuration with second-level mirrors in place

It remains to tell the clients to use the second-level mirrors instead of the AMS mirror. This is done by altering the policies for a group. Mirror options can be set differently for different computer groups. Some clients can be told to update from second-level mirrors and others to continue updating from the AMS itself. The relevant setting is on the “Updates” page under “Policies: avast! Antivirus.”

Second-level mirrors also have a couple of configuration options, including the time interval in which the mirror is to be synchronized. These options can be found on the “Policies: Mirror” page of a Computer Group’s properties (of course, they are also inherited from the parent group(s).



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: ● AMS ○ Internet

☐ Auto-mirror every 10 minutes

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

Figure 6.8. Properties of the Mirror product (the second-level mirrors)

Mirroring tasks

There's a special task type just for synchronizing second-level mirrors: the mirroring task. Mirroring tasks are stored in the Updating tasks folder. To create a mirroring task, navigate to the Updating tasks folder, and select New Task. Choose Mirroring in the Task type field and specify the second-level mirror machines for this task on the Computers page. The task will have no effect on any machines that don't have the Mirror product installed.

Using two-phase updates

In some organizations (especially in those where security is the number-one issue), all updates distributed to the machines on the network must first be verified on a number of test machines. If the test results are OK, the updates are authorized to be pushed onto the production machines. This requirement can be quite easily implemented by using the ADNM second-level mirrors feature:

- The second-level mirrors have auto-sync turned off, and
- the AMS mirror is used exclusively by the test machines.

In this case, if there's an update released on our Internet servers, the following steps are taken:

1. The AMS mirror synchronizes with our Internet server, downloading the new packages and publishing them to the clients.
2. The set of test machines (that are set to update directly from the AMS mirror) downloads the new version. However, no other machines update at this point, as there is nothing new on the second-level mirrors yet.
3. Testers verify that the new update works as expected.
4. If everything is OK, the mirroring task is executed on the second-level mirror machines, and it copies the new files to the second-level mirrors.
5. All computers on the network start downloading and installing the new, verified update.

6.2.2 To Update Roaming Users

ADNM is designed to handle updating needs for mobile/roaming users quite simply: If the AMS (or second-level mirror) is available, use it to fetch the updates. Otherwise, update from the Internet.

While this may sound almost trivial, it is actually very effective. Roaming users who are partly connected to the corporate network (either directly or remotely via VPN) and partly not (but most likely still with Internet access) always download the updates from the best available source anyway. The only situation where no updates take place is when the machine has access neither to corporate network, nor the Internet – but this is probably not a big surprise.

6.2.3 Using the PUSH Updates

The AMS mirror can also be instructed to use push-style synchronization (not to be confused with automatic push updating of clients). Push-style updates in ADNM work exactly the same way as in avast! Professional Edition: by using e-mails.

Traditionally, every installed program checks now and then whether a new version is available. Push updates, however, are initiated by our server — immediately after an update is published. In response, the AMS mirror quickly performs the necessary synchronization. The system is based on the SMTP protocol, i.e., on usual e-mail messages.

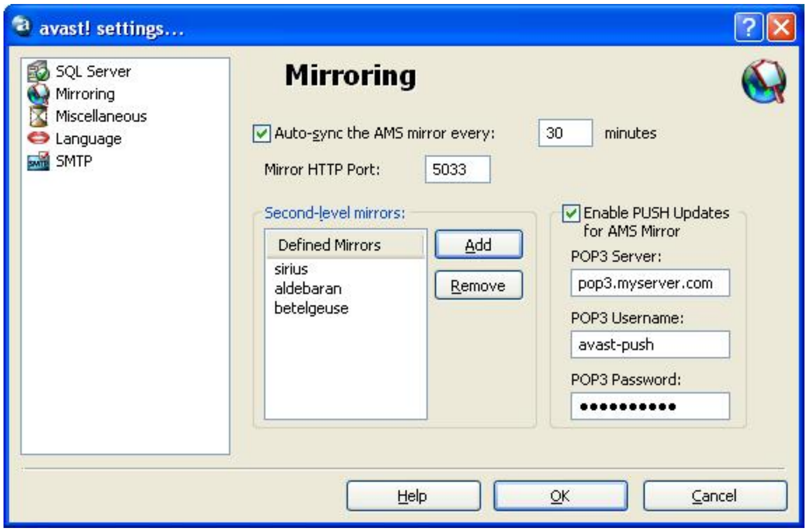
The whole Push update system is protected by asymmetric ciphers and is resistant to unauthorized misuse.

6.2.3.1 Setting Up Push Updating for AMS Mirror

To set up Push-style synchronization for the AMS mirror, first register to receive the update notification e-mails. This is done by filling in the target e-mail address at http://www.avast.com/i_idt_112.html. For corporate customers with their own mail server, we recommend setting up a separate e-mail account for this purpose.

After registering the address to receive the notifications, open the global AMS Settings dialog, go to the Mirroring page and fill in the account details. The configuration page only supports changing the most basic parameters (POP3 Server name, username and password). To fine tune the settings, you'll have to change certain entries in the [InetWDMirror] section of the file <ADMM>\DATA\avast4.ini on the AMS. For example, the PushDaemonInterval value specifies the interval, in minutes, in which to POP the e-mails (the default is 3; you can set the interval to as low as 1 minute to maximize the efficiency of the

PUSH updater). Another important value is the PushDaemonDeleteMessages entry, a boolean (0 or 1) value that governs whether the program should delete the messages after they are downloaded from the server or instead leave them on the server. The default value is 0 (leave the messages on the server). If you use the default value, it may be useful to delete the messages manually from the mailbox at least once a year (more often if you're getting lots of spam).



☑ Auto-sync the AMS mirror every: 30 minutes

Mirror HTTP Port: 5033

Second-level mirrors:

Defined Mirrors
sirius
aldebaran
betelgeuse

☑ Enable PUSH Updates for AMS Mirror

POP3 Server: pop3.myserver.com

POP3 Username: avast-push

POP3 Password: ••••••••••

Figure 6.9. Specifying POP3 server details for the PUSH updater.

6.3 Monitoring the ADNM 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. In most cases, this is done via the Events folder in the console, but entries are not logged to this folder. Please see the Monitoring AMS Logs section in the Advanced Topics chapter for more information.

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's good 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, 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.

- 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 by using a Database Maintenance task (using the option Delete Events Older Than ... Days). For more information about the DB Maintenance tasks, please refer to the AMS Maintenance chapter later on.

6.4 Licensing in ADNM

The ADNM provides a very flexible licensing model. All license checking is done on the server. That is, as long 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 theft of the file. If the license on the server expires, it automatically expires on all the clients, too.

This works in most cases, but not for laptops, which are not permanently connected to the server. The ADNM handles such situations by requiring the notebooks to connect to the server at least once every 21 days. This value is hard-coded into the program and cannot be overridden. After three weeks, all the managed products on the client machine will stop functioning until a connection to the server is established and the server provides a valid license. This includes virus database update.

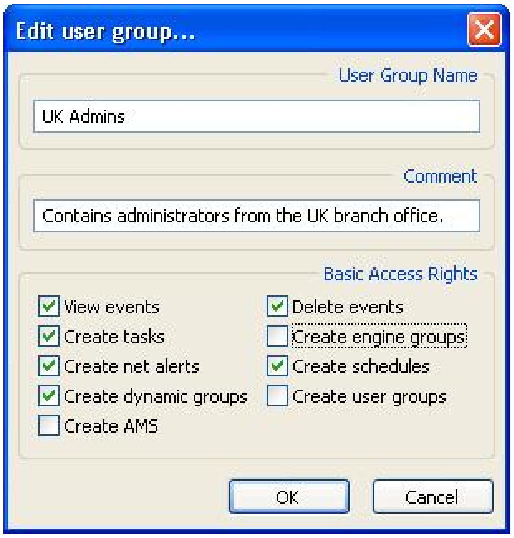
Note

If someone needs to take a machine out of reach of the AMS for longer than 21 days, a separate license file copy must be locally provided to the machine by hand.

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, in the Administrators group, and the Guest account, in the Guests group. These two accounts have special meaning and shouldn't be changed. The only thing that should be changed (immediately) is the default 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 cannot change (or even read/list) any objects. The password of the Guest account is empty and cannot be changed.



User Group Name: UK Admins

Comment: Contains administrators from the UK branch office.

Basic Access Rights

☑ View events	☑ Delete events
☑ Create tasks	□ Create engine groups
☑ Create net alerts	☑ Create schedules
☑ Create dynamic groups	□ Create user groups
□ Create AMS	

Figure 6.10. The user group editor

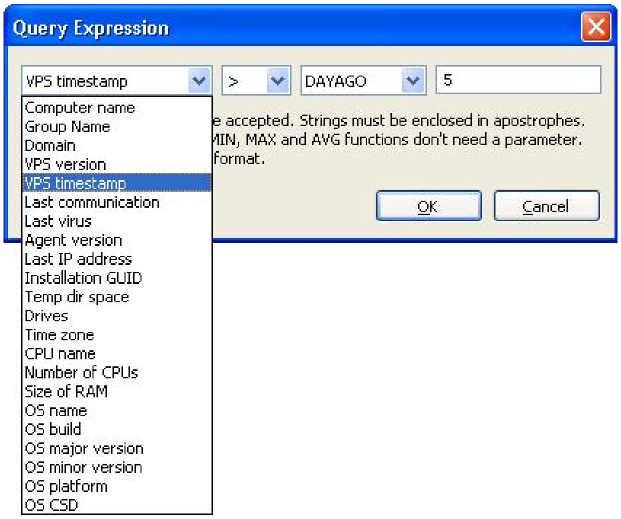
Each object in ADNM (task, schedule, alert, installation package, etc.) has an Access Control List (ACL). The ACL specifies access rights to the object. There are four levels of access—read, write, delete and execute. There's also a special access type, Full Control, which combines all four access types.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

Such a robust access-level system makes administration easier, especially in larger corporations having many 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 to computers and objects that are under his/her administration. So if an administrator is responsible for managing LAN_A, you'd create a computer group for LAN_A in the Computer Catalog and assign the administrator's account full access rights for that group only. You'd also create tasks specifically for that group and restrict that account from accessing any tasks for other groups. This way, you can have as many branch offices and local administrators as you need, each able to work only within the scope of his/her own part of the Computer Catalog.

6.6 Using Dynamic Computer Groups

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

Each dynamic group is made 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.


Query Expression

VPS timestamp > DAYAGO 5

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

Figure 6.11. Dynamic group expression editor. Expressions can be connected by AND or OR and grouped by parentheses.

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 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! 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 (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 agent installed on the machine.

- **avast! NetClient 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.

- **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 providers** (type: string). The list of avast! resident providers (modules) installed on the machine. Providers are listed by their short names, e.g., STANDARD for Standard Shield, MAIL for Internet Mail, and OUTLOOK for Outlook/Exchange. They are separated by commas.

- **Running providers** (type: string). The list of avast! resident providers (modules) running on the machine. By definition, this is a subset of the value "Installed providers."

- **Waiting providers** (type: string). The list of avast! resident providers (modules) that have the current status "waiting to start" on the machine. By definition, this is a subset of the value "Installed providers."

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 may use the * wildcard. For example, the mask NEM* covers the 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:

- Equal-to, **=**.
- Not-equal-to, **!=**.
- Smaller-than, **<**.
- Greater-than, **>**.
- Smaller-than-or-equal-to, **<=**.
- Greater-than-or-equal-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, 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 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 timedate type, occurred N minutes ago at most. The operand specifies the value of N.

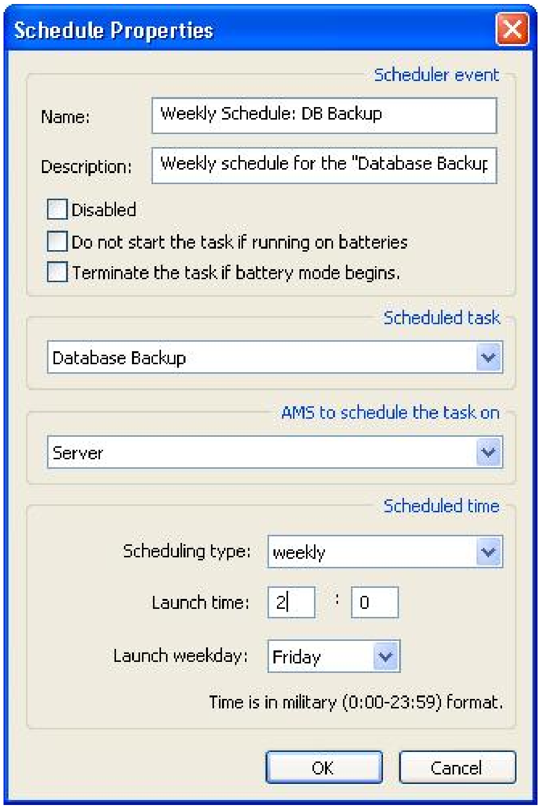
There are only two logical operators for connecting multiple expressions: **OR** and **AND**. The dynamic group definition can be made up of any number of expressions connected by either of these logical operators.

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 in all managed computers. Of course, the on-access scanner is the most important line of defense, but nice to know 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 users to stop the scan. Typical choices are 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). For example, if the expiration property is 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 keep scans scheduled to run at night from running during the workday and decreasing the productivity of your users.


Schedule Properties

Scheduler event

Name: Weekly Schedule: DB Backup

Description: Weekly schedule for the "Database Backup

□ Disabled
□ Do not start the task if running on batteries
□ Terminate the task if battery mode begins.

Scheduled task

Database Backup

AMS to schedule the task on

Server

Scheduled time

Scheduling type: weekly

Launch time: 2 : 0

Launch weekday: Friday

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

Figure 6.12. The task schedule editor

6.7.2 Covering New Computers

In most networks, computers come and go. Efficient management of a network that changes often can be a nightmare. Fortunately, the ADNM contains mechanisms that can help administrators easily cover new machines by automatically pushing avast! to newly created machines.

Achieving this goal requires some work, but it illustrates how a number of ADNM features can be used together to provide some advanced functionality. We'll use the following components:

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

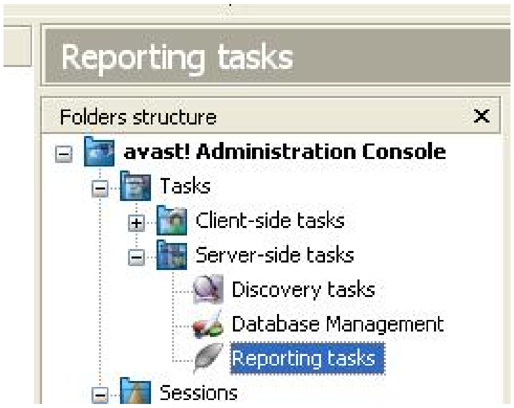
We'll start by preparing an installation package for the avast! NetClient product (if we haven't done so yet). Next we create a deployment task and bind the installation package to it. Make sure to correctly specify valid credentials for all domains/workgroups to be really able to install the software 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 several ways, but one of the most straightforward is to use the simple expression "Agent Version 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 powerful reporting capabilities second to no competing product. You can create a variety of useful reports from information collected by the AMS from the clients. You can export these reports 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 is almost everything else, by certain tasks. Reporting tasks are grouped in a special folder in the console, under the Server-side tasks category.



Reporting tasks

Folders structure

- avast! Administration Console
  - Tasks
    - Client-side tasks
    - Server-side tasks
      - Discovery tasks
      - Database Management
      - Reporting tasks
  - Sessions

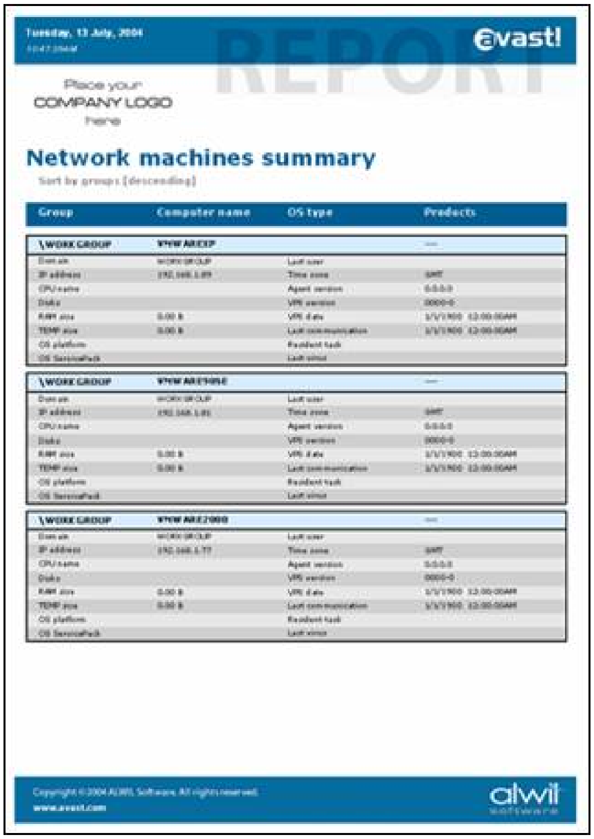
Figure 7.1. Reporting tasks in the console tree

7.1 ADNM Reports

ADNM comes with about twenty predefined reports, as described below.

7.1.1 Network Machines Summary

This report lists all computers on the network. It can be generated in two forms. The first form gives a summary of each computer—which group it's in, what operating system it runs, and what managed products it has installed. The second form contains much additional, detailed information about every computer on the network. Please note that 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.



Tuesday, 13 July, 2004
[illegible]

Network machines summary

Sort by groups (descending)

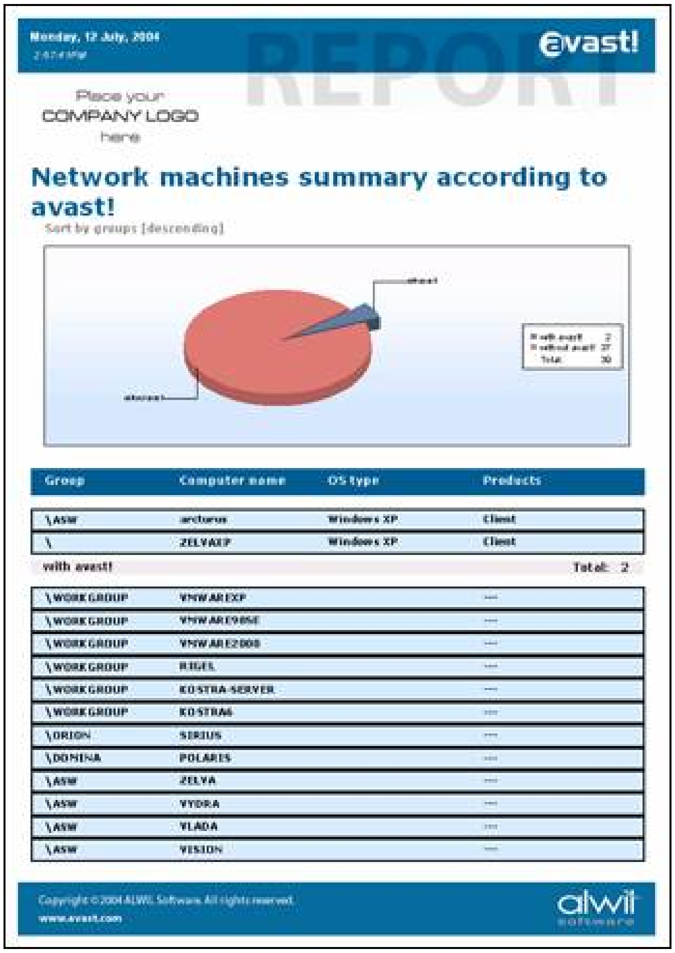
Group	Computer name	OS type	Products
\WORKGROUP	[illegible]		—
Domain	WORKGROUP	Last user	
IP address	192.168.1.89	Time zone	GMT
CPU name		Agent version	0.0.0.0
Disks		VPS version	0000-0
RAM size	0.00 B	VPS date	1/1/1900 12:00:00AM
TEMP size	0.00 B	Last communication	1/1/1900 12:00:00AM
OS platform		Resident task	
OS ServicePack		Last virus	
\WORKGROUP	[illegible]		—
Domain	WORKGROUP	Last user	
IP address	192.168.1.81	Time zone	GMT
CPU name		Agent version	0.0.0.0
Disks		VPS version	0000-0
RAM size	0.00 B	VPS date	1/1/1900 12:00:00AM
TEMP size	0.00 B	Last communication	1/1/1900 12:00:00AM
OS platform		Resident task	
OS ServicePack		Last virus	
\WORKGROUP	[illegible]		—
Domain	WORKGROUP	Last user	
IP address	192.168.1.77	Time zone	GMT
CPU name		Agent version	0.0.0.0
Disks		VPS version	0000-0
RAM size	0.00 B	VPS date	1/1/1900 12:00:00AM
TEMP size	0.00 B	Last communication	1/1/1900 12:00:00AM
OS platform		Resident task	
OS ServicePack		Last virus	

Copyright © 2004 ALWIL Software. All rights reserved.
www.avast.com

Figure 7.2. The Network machines summary report

7.1.2 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 avast! installed. This report also can be generated in either a short, summarized form or a complete form that has detailed information on 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.



Monday, 12 July, 2004
2:57:4[illegible] PM

Network machines summary according to avast!

Sort by groups [descending]

Group	Computer name	OS type	Products
\ASW	arcturus	Windows XP	Client
\	ZELVAXP	Windows XP	Client
with avast!			Total: 2
\WORKGROUP	VMWAREXP		---
\WORKGROUP	VMWARE98SE		---
\WORKGROUP	VMWARE2000		---
\WORKGROUP	RIGEL		---
\WORKGROUP	KOSTRA-SERVER		---
\WORKGROUP	KOSTRA6		---
\ORION	SIRIUS		---
\DOMINA	POLARIS		---
\ASW	ZELVA		---
\ASW	VYDRA		---
\ASW	VLADA		---
\ASW	VISION		---

Copyright © 2004 ALWIL Software. All rights reserved.
www.avast.com

Figure 7.3. The Network machines summary by avast! installations report

7.1.3 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 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.

7.1.4 Network Machines Summary by VPS Version

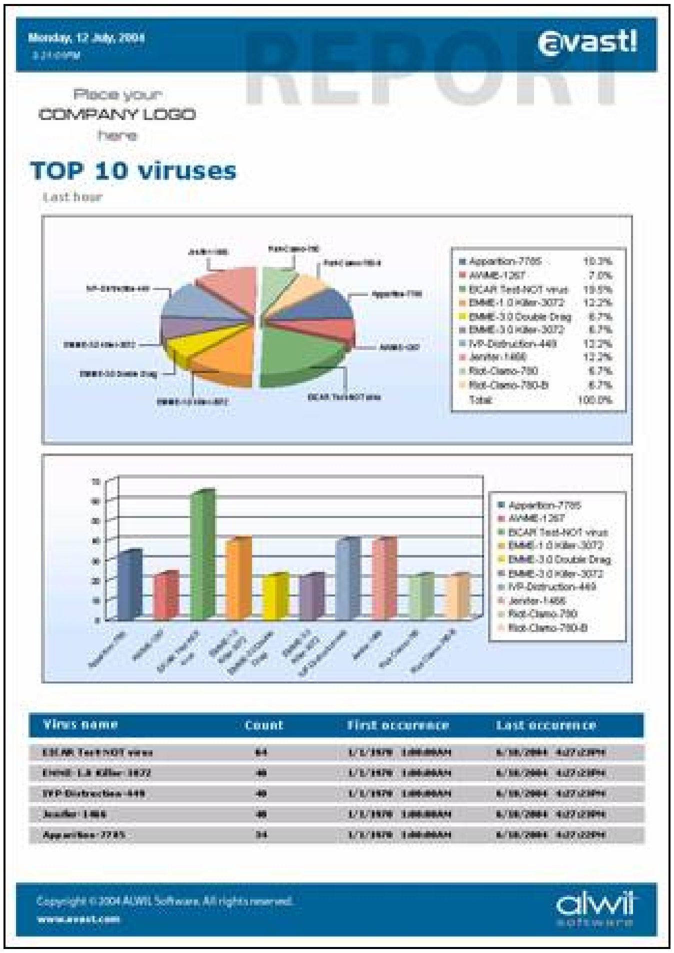
This report is like the previous one, except that, instead of the avast! version, it provides the version of the virus database (the VPS file) on each computer. It can include computers that do not have avast! installed and filter machines by computer or domain masks.

7.1.5 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 AMS. It's useful for discovering communication problems as well as finding zombie computers. Like the other network summary reports, it is customizable.

7.1.6 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.



Monday, 12 July, 2004
3:21:09PM

TOP 10 viruses

Last hour

Virus name	Count	First occurence	Last occurence
EICAR Test-NOT virus	64	1/1/1970 1:00:00AM	6/18/2004 4:27:23PM
EMME-1.0 Killer-3072	40	1/1/1970 1:00:00AM	6/18/2004 4:27:23PM
IVP-Distruction-449	40	1/1/1970 1:00:00AM	6/18/2004 4:27:23PM
Jenifer-1466	40	1/1/1970 1:00:00AM	6/18/2004 4:27:23PM
Apparition-7785	34	1/1/1970 1:00:00AM	6/18/2004 4:27:22PM

Copyright © 2004 ALWIL Software. All rights reserved.
www.avast.com

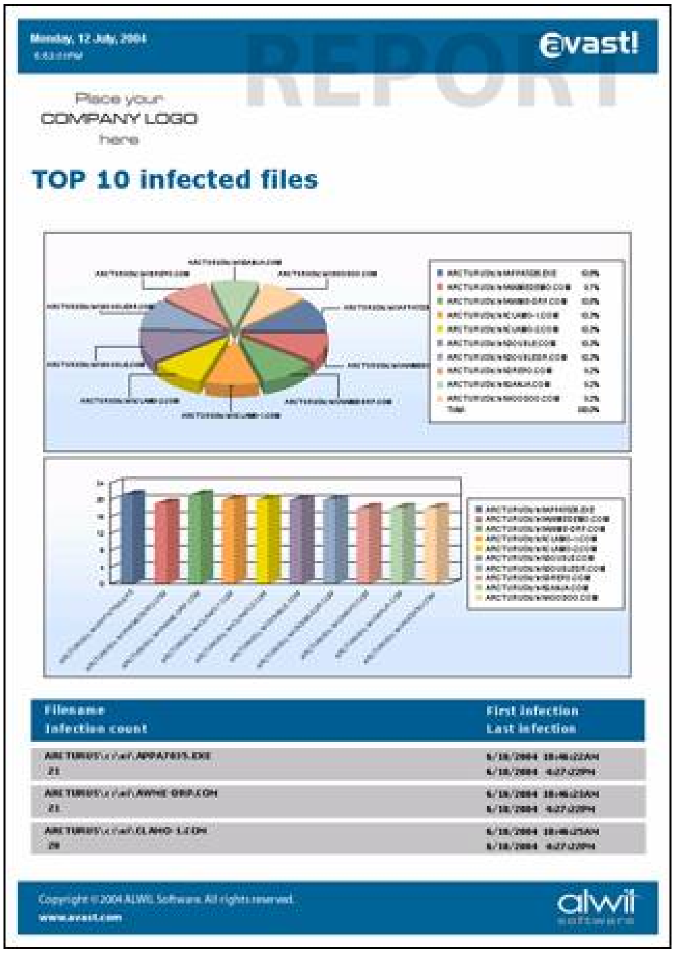
Figure 7.4. The Top N viruses report

7.1.7 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 selection of data included in the report can be done 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.

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 name of an infected file is prefixed by the name of the computer where the virus was detected. Even though the N parameter is not limited, we suggest that you use numbers no higher than 15-20. Otherwise, the report may become less readable. You can also restrict the date/time span (including custom spans) for which to report infected files.



Monday, 12 July, 2004

Place your COMPANY LOGO here

TOP 10 infected files

Filename Infection count	First infection Last infection
ARCTURUS\c:\a\APPA7015.EXE 21	6/18/2004 10:46:22AM 6/18/2004 4:27:22PM
ARCTURUS\c:\a\AWHE-D89.COM 21	6/18/2004 10:46:21AM 6/18/2004 4:27:22PM
ARCTURUS\c:\a\CLAHO-1.COM 20	6/18/2004 10:46:25AM 6/18/2004 4:27:22PM

Copyright © 2004 ALWIL Software. All rights reserved.
www.avast.com

Figure 7.5. The Top N infected files report

7.1.9 Top N Infected Computers

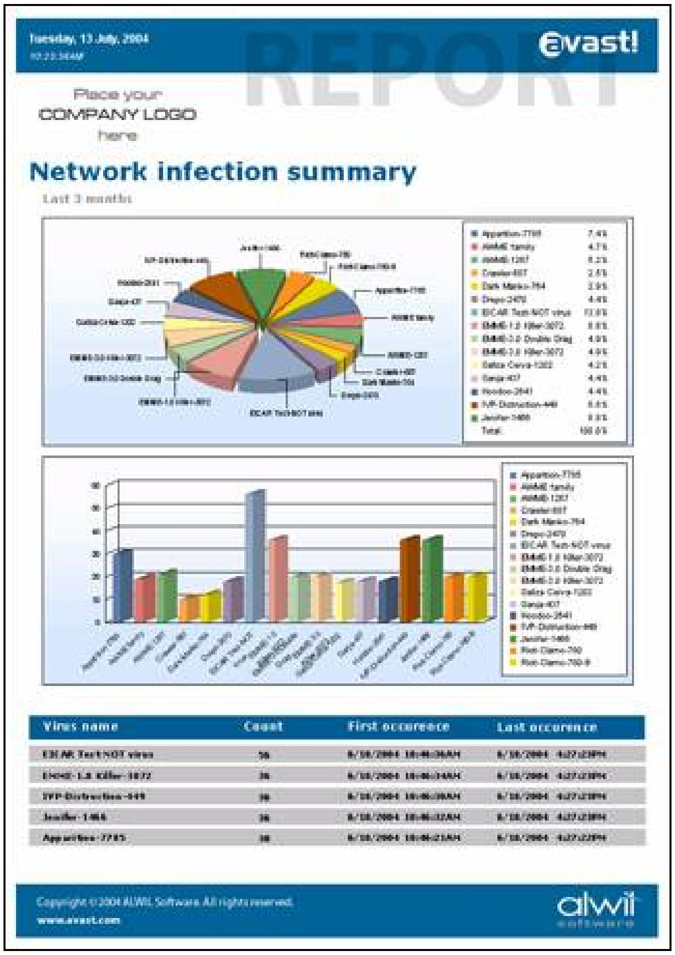
This report shows a summary (as a pie diagram and a table) of the Top N most often infected computers on the network. You can specify whether the report should include detailed information about each of the computers in the table. We suggest that you use numbers no higher than 15-20 for the N parameter. 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 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.

7.1.11 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 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.



Tuesday, 13 July, 2004
10:23:36AM

REPORT

Place your
COMPANY LOGO
here

Network infection summary

Last 3 months

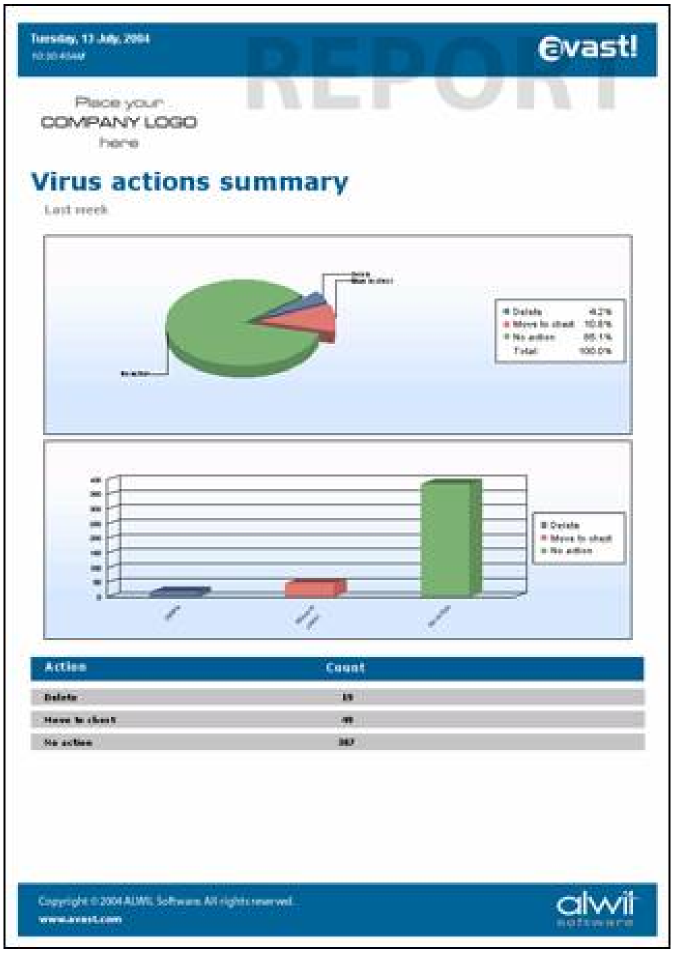
Virus name	Count	First occurence	Last occurence
EICAR Test-NOT virus	56	6/18/2004 10:46:36AM	6/18/2004 4:27:23PM
EMME-1.0 Killer-3072	36	6/18/2004 10:46:34AM	6/18/2004 4:27:23PM
IVP-Distruction-449	36	6/18/2004 10:46:30AM	6/18/2004 4:27:23PM
Jenifer-1466	36	6/18/2004 10:46:32AM	6/18/2004 4:27:23PM
Apparition-7785	30	6/18/2004 10:46:21AM	6/18/2004 4:27:22PM

Copyright © 2004 ALWIL Software. All rights reserved.
www.avast.com

Figure 7.6. The Network infection summary report

7.1.12 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.



Tuesday, 13 July, 2004
10:30:45AM

avast!

REPORT

Place your
COMPANY LOGO
here

Virus actions summary

Last week

Action	Count
Delete	19
Move to chest	49
No action	387

Copyright © 2004 ALWIL Software. All rights reserved.
www.avast.com

alwil software

Figure 7.7. The Virus actions summary report

7.1.13 Change of Logical Disks Summary

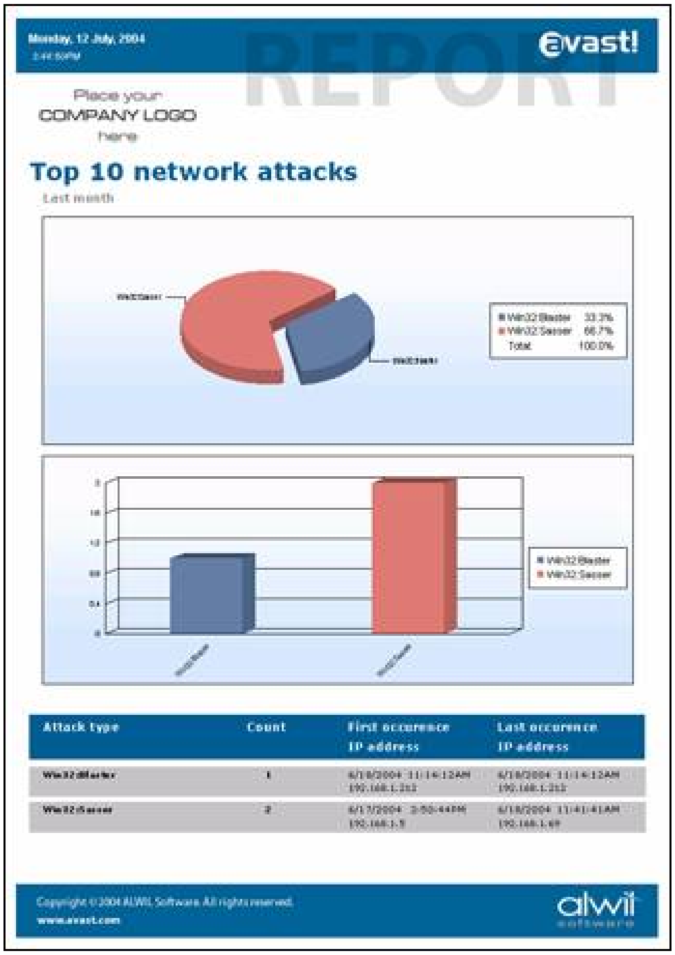
This report is a bit different, because it is not directly related to the antivirus protection. Instead, it shows a summary of changes in logical drive mappings on the managed computers, e.g., attachment of a USB disk, mapping of a network drive, etc. You can specify the time/date period.

7.1.14 Top N Attacked Computers

This report shows the Top N computers that have been attacked (unsuccessfully) by a network worm, as detected by avast!'s Network Shield provider. You can define the parameter N the time/date period. This report is generated as 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 detected by avast!'s Network Shield provider. You can define the N parameter and the time/date period. The report provides comprehensive information, including time stamps and the IP address each attack came from. It includes a pie chart and a bar chart.



Monday, 12 July, 2004
2:44:50PM

Top 10 network attacks
Last month

Attack type	Count	First occurence IP address	Last occurence IP address
Win32:Blaster	1	6/18/2004 11:14:12AM 192.168.1.212	6/18/2004 11:14:12AM 192.168.1.212
Win32:Sasser	2	6/17/2004 2:50:44PM 192.168.1.5	6/18/2004 11:41:41AM 192.168.1.69

Copyright © 2004 ALWIL Software. All rights reserved.
www.avast.com

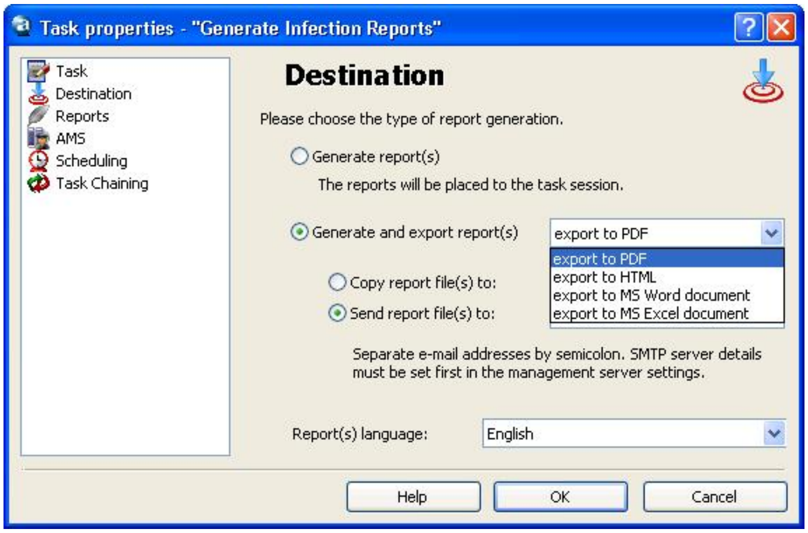
Figure 7.8. The Top N network attacks report

7.1.16 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 on these files on a set of computers specified in the reporting task's properties. The report is useful e.g. for finding out which computers are most exposed to viral attacks so that appropriate countermeasures can be taken.

7.2 Report Targets

Reports can be generated directly to 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. These parameters can be set in the reporting task properties.



Task properties - "Generate Infection Reports"

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

- export to PDF
- export to HTML
- export to MS Word document
- export to MS Excel document

○ Copy report file(s) to:

● Send report file(s) to:

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

Report(s) language: English

Figure 7.9. Properties of a reporting task

7.3 Using a Custom Company Logo

As seen in the report screenshots above, the ADNM lets you place a custom logo on all reports it generates. Such customization can help maintain corporate identity, especially in the printouts. It can also 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 you should maintain the aspect ratio of 5:14; otherwise, stretching will occur. We also recommended that you do not use large image files. Since the picture will be part of every report generated, a large image 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 task 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 regular backup of the whole database is important. You should incorporate backup of the ADNM 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 ADNM DB Maintenance task to back up the database to a file and then back up that file using standard methods.

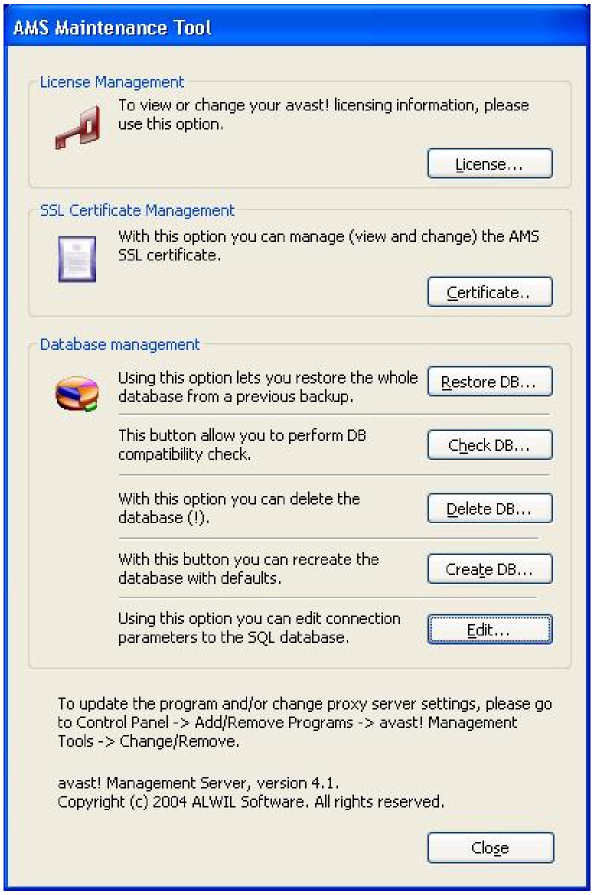
Database cleanup can be used to remove older records from the database. DB cleanup keeps the database from growing indefinitely. The DB Maintenance task also lets you delete "orphaned" records, and that can also reduce the size of the database. You specify the oldest records you'd like to keep. Of course, 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.

8.2 AMS Maintenance Tool

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

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

- Change the product license file.
- Change the server SSL certificate.
- Restore the database from a backup. (Database backups can be done as a Database management task from the administration console, even scheduled to run periodically.) **Note:** restoring the database will destroy its current contents. It's a good idea to create a new, separate backup immediately before doing the restore.
- Check the validity of the database.
- Delete and reinitialize the database. Do this if you want to start from scratch. **Note:** deleting or recreating the database will destroy its previous contents. Be sure to create a backup before performing these operations.
- Change database connection details. Use this option when you want to move the database to another SQL server or upgrade from MSDE to a full SQL server. You should create a backup, change the database connection details, and then restore the database from the backup.



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

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

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

This button allow 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 connection parameters to the SQL database.

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

avast! Management Server, version 4.1.
Copyright (c) 2004 ALWIL Software. All rights reserved.

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

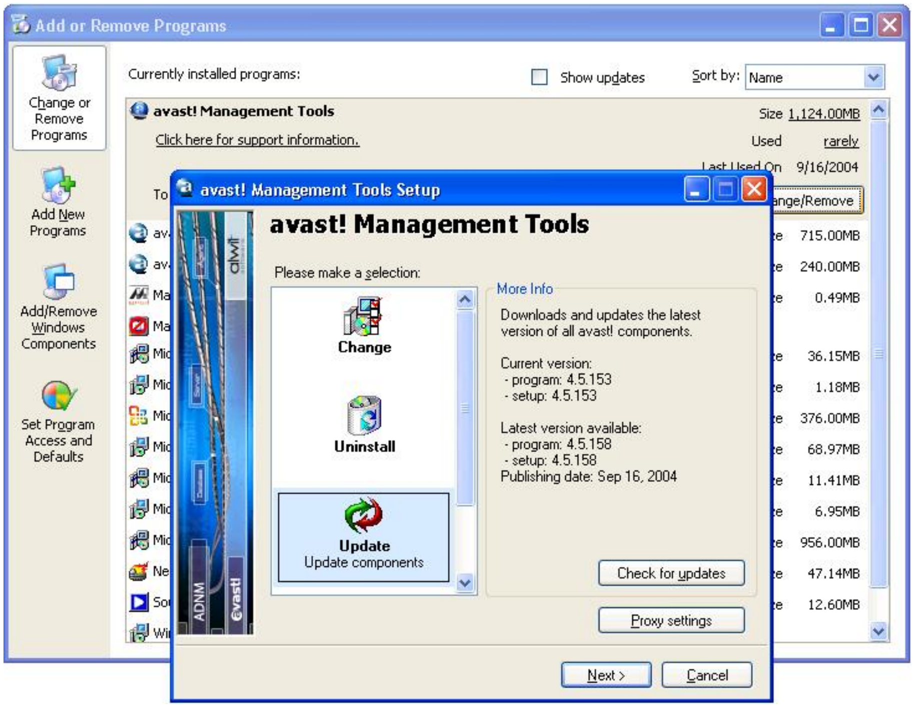
The AMS Maintenance Tool can be found in the ADNM group in the Start menu. It cannot be run remotely, but it should work correctly inside remote desktop or terminal server connections.

8.3 Proxy Settings Change

Since the AMS provides mirroring of updates, it's important to have the proxy server details set correctly. These details are set when the AMS is installed, but sometimes you may need to change them. To change the AMS proxy server settings, 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 change of the proxy server.

8.4 AMS/Console Updates

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



avast! Management Tools — Size 1,124.00MB — Used rarely — Last Used On 9/16/2004

Click here for support information.

avast! Management Tools

Downloads and updates the latest version of all avast! components.

Current version:
- program: 4.5.153
- setup: 4.5.153

Latest version available:
- program: 4.5.158
- setup: 4.5.158

Publishing date: Sep 16, 2004

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

Warning

Updating the AMS is difficult because it involves updating the SQL server database. If the database format (tables, stored procedures, etc.) has changed, this requires transforming the data to the new format. Updating typically results in some downtime and may require a reboot of the server. Therefore, it is wise to schedule the update for 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. Update the AMS. 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 first try the Check Updates button, which will give you 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. Follow the same procedure as for the AMS update, but this time on the machine(s) to which the consoles have been installed.

Note

Please be sure not to run any of the consoles before the update is complete, that is, between updating the AMS and updating 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

Cisco NAC Support

9.1 Overview

NAC is a technology developed by Cisco Systems that is designed to enforce security policy compliance on computers connecting to network. NAC can limit network access when a computer fails to meet certain criteria. ADNM 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

- a 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! Management Server (AMS) with posture validation server (PVS)

We shortly describe how NAC works and how avast! is involved in the validation procedure. When a computer attempts to connect to the network a NAC-enabled NAD detects it and contacts the ACS. ACS then requests the CTA running on the computer for posture credentials. CTA asks avast! PP for antivirus status (e.g. version) and sends the posture to ACS. ACS forwards the credentials to avast! PVS, which validates them according to requirements defined by administrator. PVS returns results to 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" (http:// www.cisco.com/ application/ pdf/ en/ us/ guest/ netsol/ ns617/ c649/ cdccont_0900aecd8040bbd8.pdf) Here we describe only portions specific to avast.

9.2 Cisco Secure ACS setup

NACS configuration is a lengthy procedure explained e.g. in the "NAC Framework Configuration Guide". We describe two of the steps that are specific to avast.

1. *Importing attribute definition file.* You need to import a NAC attribute definition file that defines attributes provided by avast! posture plugin. You can find this file on the AMS machine in <ADNM>\ CiscoNAC\ aswAVP.adf. Use the CSUtil.exe utility on the ACS machine to import the attributes.

2. *Creating posture validation policy.* In the Posture validation section you will create an External policy that defines a connection to avast! posture validation server. It will be set up this way:

   - URL: Type avast! posture validation server URL in the following format: *https://<host>:<port>/pvs*, where <host> is the name or address of the computer with AMS and <port> is 16103 by default

   - Username, Password: Leave them empty, they are not required.

   - Trusted Root CA: Select the certificate authority that issued the AMS certificate. If the particular CA is not in the list you must first add the CA certificate to ACS in the System configuration section. If you use a self-signed certificate for AMS, you can use the AMS Maintenance Tool to export the certificate to a file and then add the certificate from the file to ACS.

   - Forwarding Credential Types: Move attributes of type ALWIL-Software:avast-Antivirus (that were imported from aswAVP.adf) to the Selected credentials section.

9.3 AMS setup

Avast! posture validation server is a part of the avast! Management Server, you don't need to install any third party web server. Configuration of avast! PVS is performed through AMS console. You set up the NAC options as properties of a computer group, separately for each group of the computer catalog.

NAC configuration consists of two pages: NAC Validation and NAC Remediation. The NAC Validation page defines requirements for the status of avast! on computers that are connected to your network. You can enforce program version, virus database (VPS) version and/or active on-access protection. The program version can be specified by an exact version number or you can enforce the latest version that is downloaded to your AMS mirror. The VPS version can be specified by an exact version number or by a maximum admissible VPS age. If the validated computer meets all the specified requirements, avast! PVS returns status value Healthy.

If some of the requirements is broken, avast! PVS takes actions specified at the NAC Remediation page. You can define what status value will be returned (Checkup, Quarantine or Infected) and if avast! should try to remedy the situation. The remediation action will be delivered to the validated computer where avast! software will try to accomplish it. Remediation means updating in the case of outdated avast! program or VPS, and 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 AMS mirror. If you select the option to display notification message on client computer, a user will see a pop up message at the right bottom of the screen saying that avast! is taking actions to satisfy policies defined by the network administrator and also if the remediation action was successful or not.

9.4 Workstation setup

On the workstations, the Cisco Trust Agent and the avast! posture plugin for CTA must be present. To install the posture plugin as part of the avast! network client software, select the option "Cisco NAC Support" when you create the installation package. The Cisco Trust Agent is not installed as part of the avast! network client, it must be installed separately.

10

Advanced Topics

10.1 Monitoring the AMS 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 AMS also logs certain events to 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 adnm\data\log folder. You can use Notepad or any text program to view them. Error.log and Warning.log are usually the most important. The logs can also be 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 can connect to the AMS, that is, if the AMS service is running properly—not always the case if there's a problem.

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.

10.2 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 problems 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, though the clients can protect the machine even during long lapses of communication with the AMS.

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

1. The agent uses the predefined server. If that fails,

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

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

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

10.3 Moving AMS to Another Machine

Since 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 applies when there's a hardware failure of the AMS, or you just want to replace the hardware with a more powerful machine.

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 information that the old server is currently using.

2. When 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,

   - change the AMS address 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 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 on 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 information for the new database.

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

   - change the AMS address 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 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 the 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.

10.4 The Multi-AMS Model

In some cases, a single AMS may not be sufficient. ADNM handles such cases by letting you install multiple AMS's on the same network. This is distinct from the obvious case where your network segments are totally disconnected from each other, and you simply install a separate AMS on each of them. The multiple AMS's are organized in a parent-child structure. Each AMS is responsible for its own subset of client machines. All policies are stored (replicated) on all AMS's, but each AMS holds task results only from its own clients—except for the root AMS, which eventually stores all results from all clients. This enables enterprise-wide reporting on the root AMS.

Please follow this procedure when installing ADNM in the multi-AMS model:

1. Install all AMS's separately, typically one for each LAN, and decide which of them will be the root AMS (the "parent"). That is usually, but not necessarily, the one at the corporate headquarters.

Note
No computers should be in direct reach of more than one AMS at a time. By "direct reach," we mean the reach of UDP broadcast packets. Typically, this means a single network segment. Otherwise, the AMS's may "steal" clients from each other.

Each AMS must use its own SQL server. It makes sense to use a full SQL Server on the root AMS and MSDE on the children, as the child AMS's usually will hold less data.

2. On each MSDE server in use, enable the network listener. By default, MSDE's are installed in a special mode that disables all network communication. This is because of security risks inherently associated with network listeners. The notorious "SQL Slammer" worm exploited a vulnerability in SQL/MSDE that caused great damage on thousands of servers worldwide in 2002. However, in the case of multiple AMS's, the individual database servers need to be able to communicate with each other, because the data is transferred between them by means of SQL DB replication. To enable the network listeners, please follow these steps for each AMS with MSDE:

   - Run the following program: %ProgramFiles%\Microsoft SQL Server\80\Tools\Binn\svrnetconn.exe

- A dialog window is shown. Move "Named Pipes" and "TCP/IP" from the "Disabled Protocols" box to the "Enabled Protocols" box.

- Save the changes by pressing OK, stop the "MSSQL$AVAST" and "avast! Management Server" services, and then start them again. Both must be stopped before restarting.

3. Connect to each child AMS, i.e., to each AMS except the one you chose to be the root, and in the File menu, choose "Subscribe to Root AMS." In the "Root AMS" field, type the address of the root AMS. In the AMS User Name and Password fields, fill in the ADNM credentials for the root AMS (using the Administrator account is recommended). The Server Name and Comment fields define how this child server object will be presented in the ADNM's "Management servers" folder. LAN Address and WAN Address fields should contain the IP addresses of this child AMS. 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. Finally, the SQL Server field should contain the full name of the local SQL Server, including instance, e.g., NEMESIS\AVAST.

4. Connect to the root AMS, and create a replication task. Replication tasks are stored in the Database Management tasks folder. Add a schedule for it, e.g., nightly. Please note that there must be a valid connection between the AMS SQL DB's for the replication task to work. Initial replication can also be run immediately (on-demand) by directly starting the replication task. Note that it makes no sense to run a replication task on any server other than the root.

Reporting and discovery tasks are typically run only on the root AMS. This is because reports are created enterprise-wide (taking into account data from all managed machines from all AMS's), and discovery tasks shouldn't create unwanted duplicates. Discovery tasks should be run on a child AMS only if there is no Network Neighborhood / Active Directory intersection, i.e., no duplicate machines would be discovered.

It is also worth noting that the replication task provides very limited error reporting. To thoroughly check the status of the replication process, you should use the SQL Enterprise Manager tool. Look for this on the root AMS SQL Server, which is usually not MSDE but rather a full SQL with the Enterprise Manager.

10.5 Accessing the AMS From Outside

Sometimes you may want to enable access to the AMS from outside the network. This may be useful for roaming users without VPN access, i.e., without direct access to the AMS, or for outsourced administration, such as a management console running outside the LAN. To make this work, certain changes have to be done on the network perimeter (firewall); namely, the following must be enabled:

For accessing the AMS by a remote console

- Open the ports tcp/16102 and udp/6000 on the firewall (gateway), and have them redirected to the AMS itself.
- In the console, use the public (WAN) IP address of the gateway as the AMS address.

For accessing the AMS by remote agents

- Open the ports tcp/16111 and udp/6000 on the firewall (gateway), and have them redirected to the AMS itself. (Updates will be downloaded directly from the Internet, as it is not possible to create gateway routing for the mirror http listener.)
- Set the agent(s) to use the public (WAN) IP address of the gateway as the AMS address. One way to set this is by using the aswChAms.exe utility, which is part of the managed avast! installation.

Please note that the Apply Now command will not work for clients outside the LAN. These machines are not addressable by the AMS, and therefore there's no way to force a policy update on them. The same applies to the situation where there's a firewall active on the agents. To make the Apply Now feature work even with the firewall installed, you'd have to enable traffic on port tcp/16109 on each of the clients. An exception to this is the case of Windows XP SP2 / Vista firewall as the program takes care of defining appropriate rules for it automatically.

Warning

Creating a hole in your firewall can indeed be dangerous, as it may compromise the system security. Please use this option carefully.

10.6 What Is Where

- The default AMS/console installation path is

%ProgramFiles%\ALWIL Software\Management Tools

- The default avast! installation path is

%ProgramFiles%\ALWIL Software\Avast

- The AMS is hosted in the "avast! Management Server" system service, which is implemented by the executable file avEngine.exe. Most of the work is done in the aswNeser.dll that loads in it, though.

- The management console process is called asaAdmin.exe. The AMS Maintenance Tool is contained in AmsTool.exe.

- If running under Windows NT/2000/XP/2003/Vista, the agent is hosted in the "avast! NetAgent" system service, contained in the file AvAgent.exe. All on-demand scans scheduled from the AMS also run in the context of this process. Most of the agent's work is done in the aswComun.dll and avClient.dll that load into the AvAgent process.

- If running under Windows NT/2000/XP/2003/Vista, the on-access scanner and VRDB generator is hosted in the "avast! Antivirus" system service contained in the file aswServ.exe.

- The mail scanner (Internet Mail resident provider) is implemented by aswMaiSv.exe. MS Outlook scanning is realized by aswOutXt.dll which loads directly to the Outlook process.

- The web scanner (Web Shield resident provider) is implemented by aswWebSv.exe.

- The virus database is contained in the file <avast>\data\400.vps.

- The main global configuration file is <avast>\data\avast4.ini. Please note that the managed settings are first read from the *avast! Secure Storage* — an encrypted data storage area in the registry key HKLM\ Software\ALWIL Software\avast\4.0\SS. If you want to change a managed key in avast4.ini and have administrative rights allowing you to make the change, you must delete the associated entry from Secure Storage before changing the INI value. Otherwise, the key value will be read directly from Secure Storage, and the updated INI value will be ignored.

- The installation files for the managed products are in the <ADNM>\InstPkgs folder on the AMS. This folder is populated after the Management Server service starts and then after each successful mirror operation.

10.7 ADNM and Local Firewalls

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.

A quote from Microsoft about Win XP SP2 firewall and program deployment:

Fortunately, by using the Group Policies, you can set rules centrally for the built-in Windows XP firewall: http://download.microsoft.com/ download/ 6/8/a/ 68a81446-cd73-4a61-8665-8a67781ac4e8/ wf_xpsp2.doc

Configuring Windows Firewall Group Policy.

Windows Firewall Group Policy settings are located in the following Group Policy Object Editor snap-in paths:

- Computer Configuration / Administrative Templates / Network / Network Connections / Windows Firewall

- Computer Configuration / Administrative Templates / Network / Network Connections / Windows Firewall / Domain Profile

- Computer Configuration / Administrative Templates / Network / Network Connections / Windows Firewall / Standard Profile

From these locations, you can configure the following Group Policy settings: http://technet.microsoft.com/ en-us/ library/ 2b2b3681- bfb7- 2c4a- a671- ea1664a738e9.aspx

ADNM

There are a number of services in use by ADNM, and these communicate using different ports.

The following table summarizes most:

AMS

- **tcp/16111**- basic communication client -> AMS. Without this, nothing will work .
- **tcp/5033**- update mirror access. Necessary to get VPS and program updates from the local mirror .
- **tcp/16102**- console access. No need to open this from DMZ.
- **udp/6000**- AMS discovery. Used only if currently selected AMS is unreachable.

Managed machines

- **tcp/16109**- "Apply to..." feature. This port is used to push new policies from AMS to the client when an Admin uses the "Apply to computer" or "Apply to group" feature in the console.
- **tcp/16108**- remote Virus chest access.
- **tcp/135, tcp/139, tcp/445, udp/137, udp/138**- these are standard RPC and NETBIOS ports necessary for remote deployment of the agents. For more info, please refer to Microsoft website: http://www.microsoft.com/ technet/ security/ smallbusiness/ topics/ ServerSecurity/ ref_net_ports_ms_prod.mspx

Remote installation

For remote installation "File and Printer sharing" must be enabled on the firewall, and in the network preferences. Otherwise, the installer will be unable to push the installation packages onto the clients. http://technet2.microsoft.com/ WindowsServer/en/library/ d3cbd31c- 6e01- 415f- 9d7a-d0cbc73baabd1033.mspx?mfr=true

10.8 Simple file sharing

Deployment of avast! netclient

One of the important/basic MS Windows XP settings is "simple file sharing". Be sure that you check this on all client machines (SFS is the default setting for this operating system, unless the machine is part of a domain). SFS can prevent the push installation from working.

The problems can go like this:

- Creating the discovery task => works
- Creating the installation package => works
- Creating a deployment task => error "access denied"

If you turn "simple file sharing" off (computer needs to be restarted after making this change!), the push client installation will then work. Beware of MS Windows XP Home, where you cannot take this action!

Also check the Firewall settings to ensure the needed ports are open : *see summary table in 10.7 - ADNM and Local Firewalls.*

There is not only one remote installation option, you can also install the netclients manually (same as with e.g. avast! Professional Edition). For example, you can use the option under deployment task's properties to create a MSI package and then run it on client computers. For further information see *chapter 5. Deploying the avast! Product line.* You can use this type of installation especially when you are using a client with MS Windows XP Home Edition.

When you are using MS Windows Vista, you should also pay special attention during deployment, especially regarding the UAC settings. More details can be found directly on the Microsoft web page, which deals with similar situations:

UAC and Remote logon

http://blogs.msdn.com/vistacompatteam/archive/2006/09/22/766945.aspx

UAC

http://blogs.msdn.com/vistacompatteam/archive/2006/09/22/766945.aspx