Avira Management Console 2.7

HowTo

AVIRA

Table of Contents

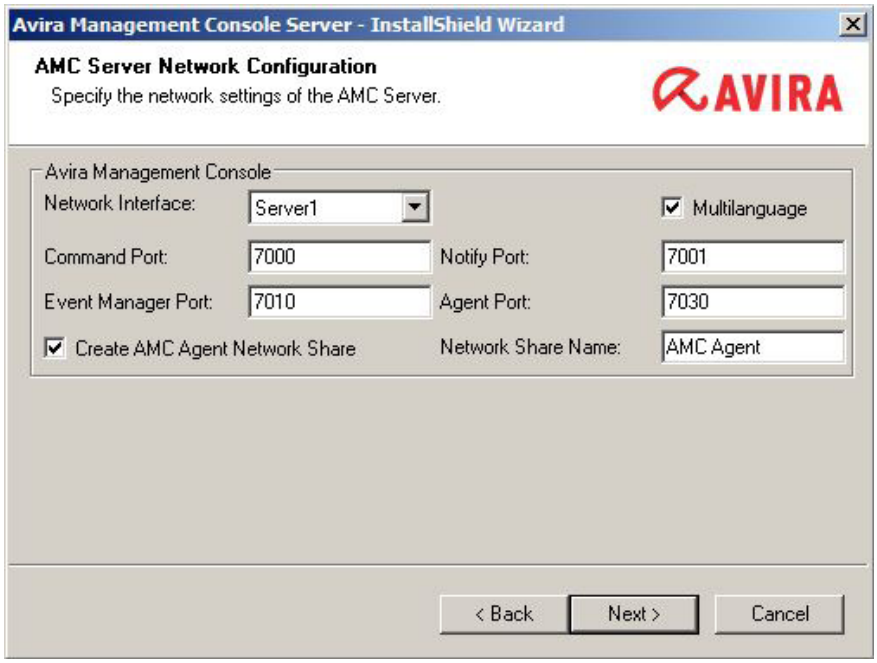
1. Installation of the AMC Server

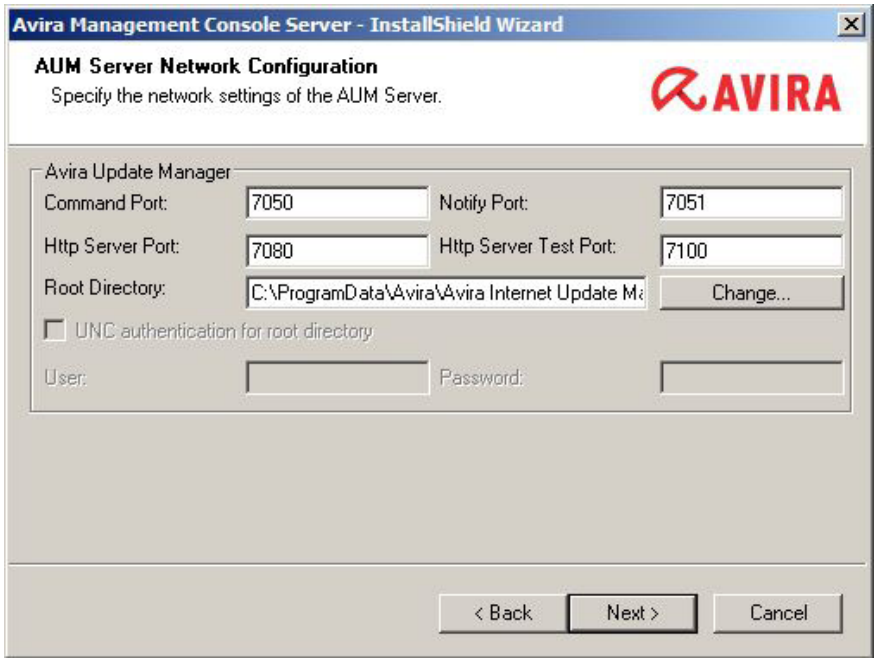
All installation files which are necessary for the installation and the manuals in PDF format can be found on our website for download.

Once you have downloaded the installation file of the AMC and unpacked it on your windows server, you can start the installation of the Avira Management Console Server:

avira_management_console_server_en.exe.

The dialog window below will appear during the installation routine. Here you can change the network configuration of the Avira Management Console Server, if necessary:



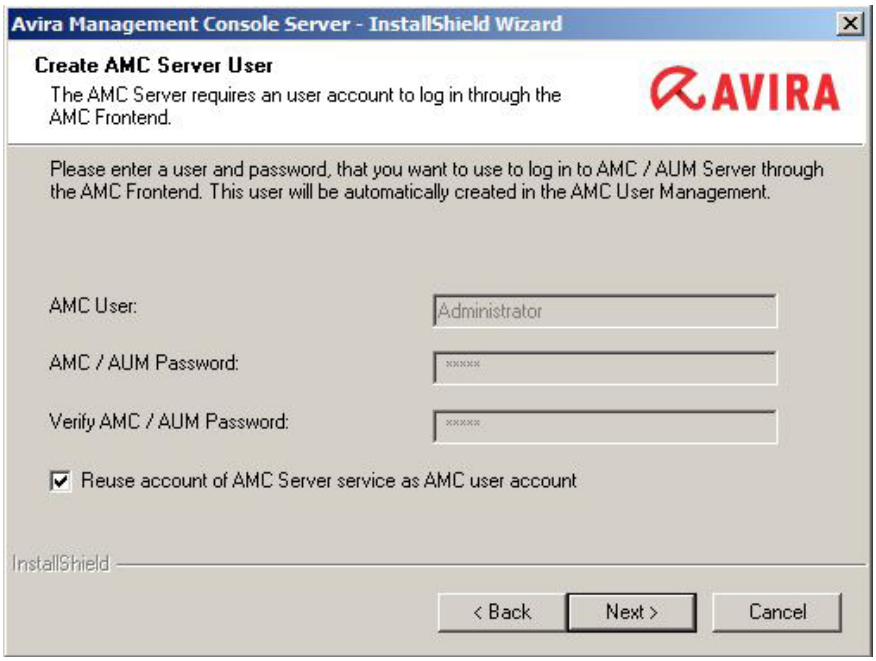


Please make sure that the network ports „7000“, „7001“, „7010“, „7030“, “7050”, 7051”, “7080” and „7100“ are not yet used by any other application installed on the server.

You can check this by using the command `netstat -an`, which can be entered at the command prompt.

The window below will appear during the installation. In order to install the necessary services, you need to log on with an administrator account (or as the case may be, by the domain administrator account) with the corresponding password:

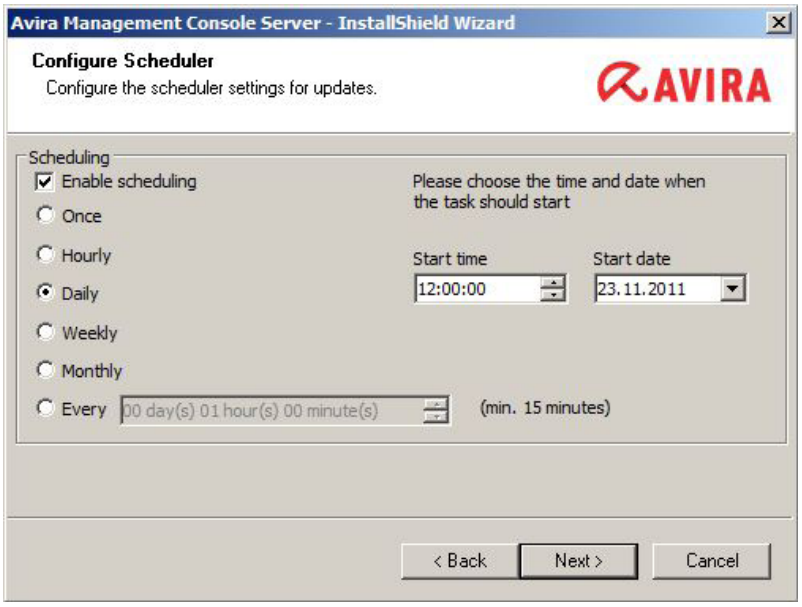
The following window will appear once you have clicked on *Next*:



The activated option “Reuse account of AMC-Server service as AMC user account” means that you can log on the AMC with this user as “administrator” (the same login information as the one earlier used as a windows administrator.)

Alternatively, by deactivating this option, you can also enter a special AMC user who can be used for the login to the AMC.

Then, a window will appear that allows you to configure the scheduler of the Avira Update Manager. Depending on the settings, it will load the product updates, the virus definition file and engine updates.



2. Installation of the AMC Frontend

The AMC Frontend (Graphical User Interface) is necessary in order to configure the AMC and has to be installed separately. This can be done on the windows server and/or on the administrator's workstation PC.

Execute the file *avira_management_console_frontend_en.exe* for the installation of the Avira Management Console Frontend and confirm the next dialog window with **Accept**.

Finish the installation using the installation wizard.

3. Starting the AMC and Logon

The AMC is started via the start menu *Start > All Programs > Avira > Avira Management Console > Avira Management Console Frontend.*
In order to log on to the console of the Avira Management Console Frontend, click on **Avira Management Console Frontend**.

Afterwards, enter the user (default: administrator) and the password you have used during the installation. After that, click on **OK** in order to log on to the AMC.

Please make sure to change the mark from „local computer" to „computer in the network" in case the AMC Frontend should not be installed on the AMC Server.
In such a case enter the IP address/hostname of the server where the AMC Server has been installed. Alternatively, you can select it by clicking on **Browse**.

4. Licensing of the AMC

In case you should already have a valid license file *hbedv.key* for the AMC, you can implement it after the logon as follows:

Click on **Avira Management Console Frontend** with the right mouse button and then on **License**.

You have the possibility to import the AMC license file in the dialog window that appears now.

5. Installing the Software Repositories

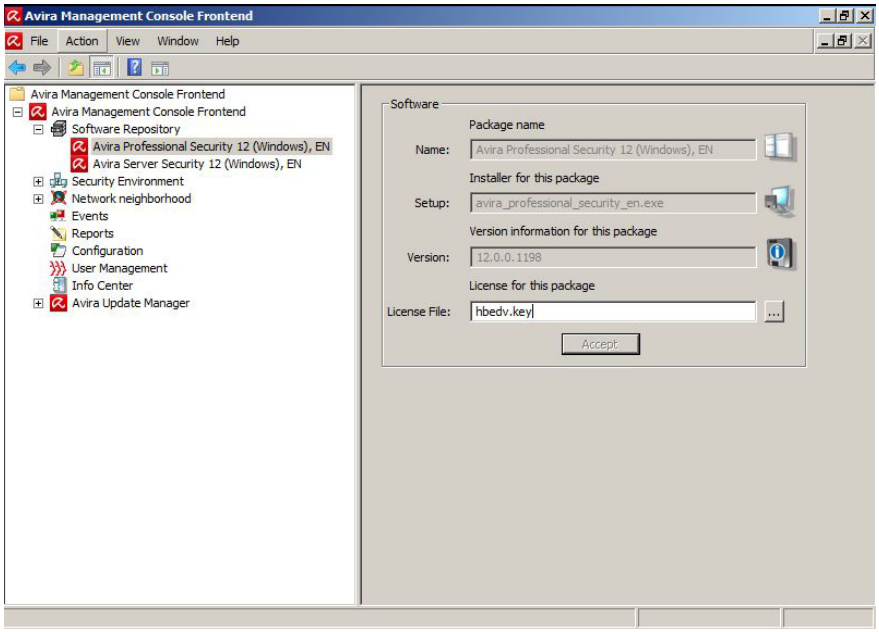
In order to be able to work with the AMC, the Avira products have to be integrated into the AMC. First download the necessary installation file(s) from our website.

In order to add the installation file(s) as software to the AMC, click on **Software Repository** in the AMC Frontend with the right mouse button and then chose *New* > *Software*.

On the dialog window that appears now, you can directly select the already downloaded installation files in the self-unpacking *EXE* format. The formats *ZIP* or for Linux software packages *GZ* and *TGZ* are also possible.

Once the software has been added, it will appear as a faded icon, as a submenu within the AMC software.

After the license file has been integrated into the corresponding software (this is possible in the right half of the window) the icon for the software will appear in bright colours.



Confusing the license or saving an invalid license for the software package is not possible with the new AMC version. Before saving, the license will be checked for validity.

Note
The license on the clients that have already been installed will not be renewed. This needs to be done separately using the copy function in the security environment and the option *Installation* > *Avira Professional Security* > *Copy Files*

The license which is integrated into the software package is only used for the first installation of the software on the clients. In case this license has expired, it has to be renewed for the corresponding software for possible new installations of the Avira products on the clients.

The installation files that have been inserted via the software packages will be added automatically to the Avira Update Manager which has been integrated into the AMC. The Avira Update Manager downloads the necessary updates for the software packages and makes them available for the clients via *http* and the port which was defined in the configuration of the Avira Update Manager (by default: port 7080).

In order to trigger the updates automatically, you should configure the “Scheduler” which is part of the Avira Update Manager. The Scheduler has to be activated via *Avira Update Manager* > *Server name* > *Scheduler*.

If the function “Enable scheduling” is activated in the configuration of the Avira Update Manager, the updates which are downloaded by the Avira Update Manager will be loaded automatically using a command that is sent to the clients. The corresponding update source (e.g. http://10.50.11.91:7080/upd/) will be included automatically.

The clients can also be updated independently from the “automatic updates” of the Avira Update Manager. Please, note chapter 11.4 that describes the planning and proceeding of updates and scans.

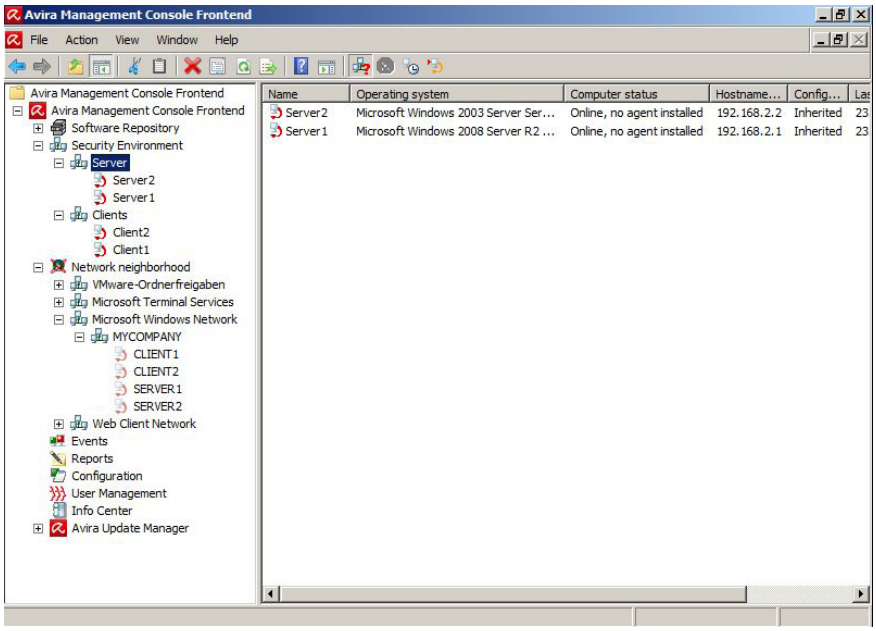
For further information about the “automatic updates” of the Avira Update Manager, please, read the corresponding chapter in the AMC manual.

6. How to Install the Security Environment

The security environment consists of clients that need to be managed using the AMC and can be organized in groups and subgroups.

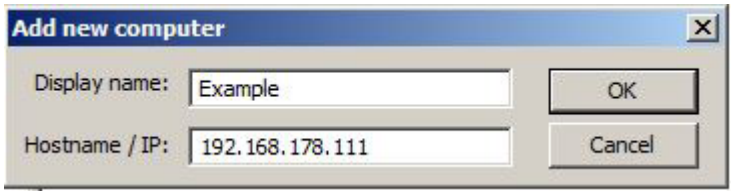
A new group can be a subgroup of the security environment or of an already existing group. A group can be created by clicking on the designated place in the security environment with the right mouse button and choosing *New* > *Group*.

This example shows how the group “Server” and “Clients” are created.
You can drag the computers located in your network from the network environment that is shown underneath the security environment into the security environment or to created groups:



Computers which are not shown in the network, e.g. Linux clients, can be manually added to a group. For this purpose click on the designated group with the right mouse button and select *New* > *Computer*.

Then the following window appears which allows naming the computer via the host name or the IP address. Moreover, a different name can be given with which the computer will be shown in the AMC:



7. Configuration Settings of the AMC

The configuration of the AMC is divided into the following sections:

- General Settings
- Server Settings
- General
- Communication
- Event Settings
- Update

The configuration allows defining general settings of the AMC. If you should use a proxy server it can be entered at *Configuration* > *Server Settings* > *Communication*.

8. Installation of AMC Agents via AMC Frontend

The AMC agent is responsible for the communication between the AMC Server and the clients that have to be managed.

The agent has to be installed on the client in addition to the necessary virus protection. This can be done directly using the AMC, manually or by means of a script. In order to enable the AMC Agent to communicate with the AMC Server, the following conditions have to be fulfilled:

- Firewall: If a firewall is used on the client, the following network ports (TCP) have to be opened:
  Out (TCP): 7000, 7001, 7010, 7020, 7021, 7030, 7050, 7051, 7080, 7100
  In (TCP): 7030
  Moreover, ICMP requests, PING (incoming echo demands) need to be enabled

- Guest account: The user account “Guest“ has to be deactivated

- The simple Filesharing (in the Explorer by selecting *Extras* > *Archive Options* > *View* > *Use simple filesharing (recommended*)) should be deactivated

- The access from the AMC Server to the hidden filesharing “C$“ of the clients has to be possible (\\<*IP address Client*\c$\)

- A network wide, standardized user account is indispensable for a smooth installation via the AMC

The installation of the AMC Agents via the AMC is done by clicking in the security environment on the corresponding client/group with the right mouse button and choosing *Installation* > *AMC Agent* > *Install*.

The computers that have the AMC Agent installed need to be powered on and Windows has to be activated!

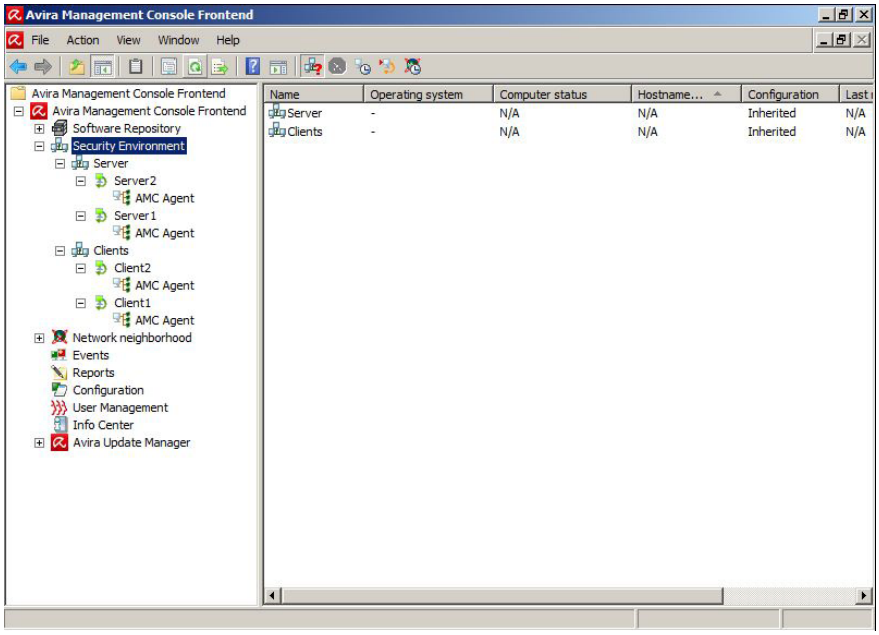
The following authentication window appears:

Enter an existing user with administrative rights on the client into the field “user name” and a corresponding “password”. For linux clients e.g. the user “root”.

In case the account of the AMC server service also exists on the clients (standardized local administrator login, domain administrator …) you can also choose the option “Use the server’s current account”.

For the installation via SSH (Linux clients) you can additionally use the SSH key for the authentication. For this purpose, select the option “Use SSH public/private key authentication” and enter the corresponding key.

After the successful installation of the AMC Agent, the client will be shown with a green icon in the security environment (communication is working):



If you want to uninstall the agent, please click with the right mouse button on the designated client/group and select *Installation* > *AMC Agent* > *Uninstall*. The appearing pop-up window needs to be confirmed with *Yes*.

9. Pull / Push Mode of the AMC Agent

After the installation the AMC applies the “push mode” by default. This means that the AMC Server sends scheduled commands like updates or scans or e.g. changes within the configuration to the AMC Agent, which forwards those to the corresponding client.

For PC’s that are not reachable for the AMC Server at that moment, an “outstanding action” will be generated which will be executed as soon as the installed agent connects to the AMC Server.

In the “push mode” the AMC Server tries to reach all computers. This causes a heavy system load for a short time. For an update command with an interval of one hour the data is sent e.g. to 500 computers and an update of 2 MB is loaded by the Avira Update Manager. This will occur at the same time on 500 clients and cause a system load of (500x2MB) 1 TB in the network.

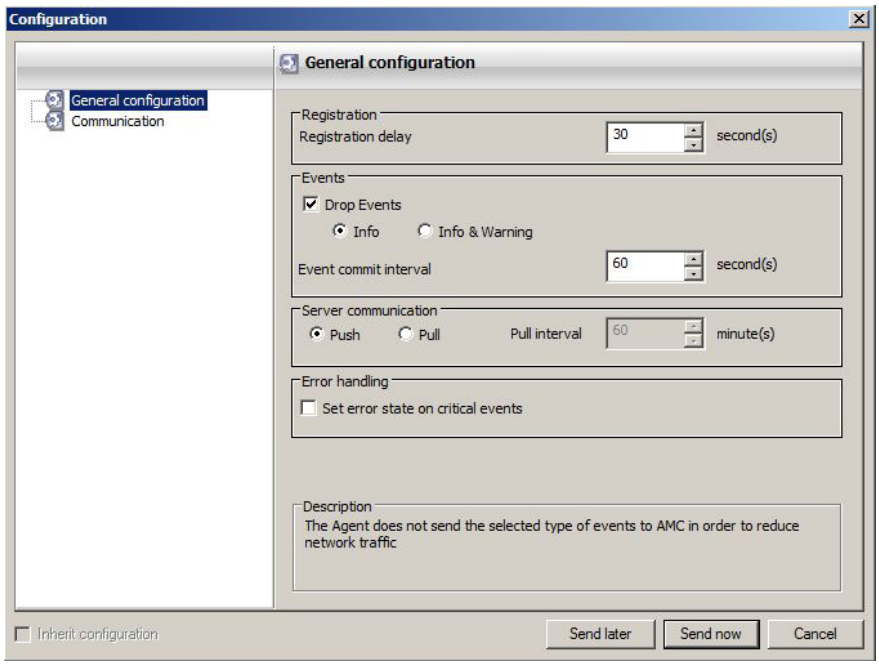
In order to reduce this network load, the AMC can be switched to “pull mode”. This way the AMC Agent will check in predefinable intervals on the AMC Server if there are new “tasks” available and processes those. Since all clients are never started simultaneously, the scheduled update intervals will not take place at the same time. Using the pull mode, the same amount of data is copied for an update but the system load is spread over a longer period of time.

An additional advantage of the pull mode in comparison to the push mode is that the AMC Agent checks for changes in accordance with the configured interval. If it is not supposed to find changes or if it is not supposed to reach the AMC Server, the previous configurations or tasks are maintained. Configured update tasks are processed independently from the AMC Server.

The change from the “push mode“ to the “pull mode“ is done in the configuration of the AMC Agent via the AMC Frontend. It is possible to select pull or push mode separately for individual pc’s or groups.

In order to set the whole security environment on pull mode, click with the right mouse button on the **security environment** and on *Configuration* > *AMC Agent* > *Configure*.

In the configuration of the AMC Agent you will find the “push mode“ in the field “Server communication”. You can change that to “Pull”. The corresponding minute interval for the connection of the AMC Agent to the AMC Server (by default 60 minutes) can be defined via “Pull interval”.



The configuration change of the AMC Agent is sent to the clients with the button **Send now**.

The following functions can be processed with the pull mode:

- Product installation
- Product configuration
- Product commands
- Task management
- Progress bar of the clients

For technical reasons, other functions like recalling the log files of the clients are based on the push mode.

10. Filtering groups

You have the option to filter according to certain criteria to get a quick overview in an AMC that manages a large number of PCs requiring the attention of the administrator. The result is then shown in one or more special virtual groups (filtered groups).

The following filters can be used to create virtual groups:

1. Computers that report an error status

2. Computers that report a product-error status

    2.1. Module outdated
    2.2 General module error

3. Computers that have a certain product installed or not installed.

    3.1. All products that are integrated in „software packages“ can be selected

4. Search using a text filter

    4.1. It can be searched for computers, groups, and host name / IP addresses
    4.2. Last message from the AMC agent to the AMC Server

The following filter options have been added:

1. having a product installed or not installed
   (Previously you could only filter for a not installed product)
2. whose name or hostname matches a wildcard search criteria
3. by agent last registration date

A „filtering group“ provides a particular view of all clients that match the selected filter criterion. This means that the clients will not be permanently moved into this group, but rather remain in their original group. All actions that are performed for that client in the filtered group are actually running on the real client.

Example:
Click with the right button on **Security Environment** to create a „filtering group“. This will filter clients in the „Security Environment“ that have e.g. Avira Professional Security not installed.

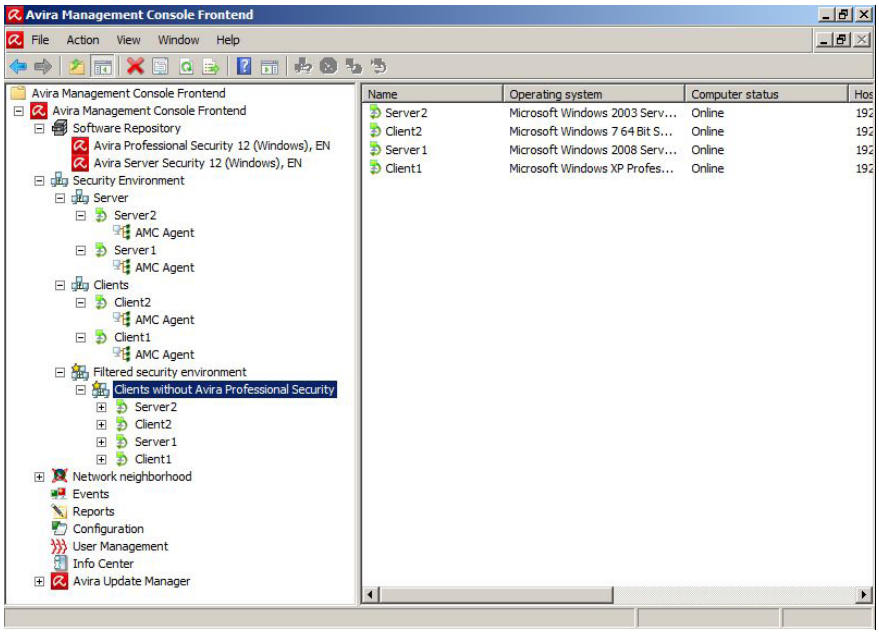
Then, select *New* > *Filtering Group*. The next window opens, allowing you to specify a name for the new „filtering group“:

In this window you can select one of the offered „filtering groups“ (e.g. “having a product installed or not installed”).

Once you clicked on Next, another window will open. Here you will have the choice to select one of the products that have been placed at the „Software Repository“.

In this example, the product „Avira Professional Security (Windows), EN” has been selected. Once you have clicked on Finish the „filtered group“ will be created with the tag „Clients without Avira Professional Security“.

Every computer of the security environment that has „Avira Professional Security (Windows), EN“ not installed, will now appear in this group:



Now, those „filtered“ clients can be targeted for an installation of e.g. Avira Professional Security.

Please see the manual of the AMC for more details about the „filtering groups“.

11. Windows Installation

11.1. “Unattended“ Installation of the AMC Agents

Alternatively, the agent can be installed manually with the setup file or unattended (e.g. integrated into the logon scripts).

On the MaC-Server the following registry has been generated:
C:\Documents and Settings\All Users\Application data\Avira\Avira Management Console Server\Agent

Please enable this registry by enabling Windows with write access. In case of an unattended installation it is not enough to start the file *insallagent.bat* via the registry enabling. (\\<*IP-address-SMC-server*>\<*Enabling(agent)*>*installagent.bat*).

The *installagent.bat* starts the installation (*setup.exe*) of the AMC Agent and uses the AMC Server information which is saved in the file *installsmcagent.iss*.

By generating a corresponding batch file (e.g. *uninstallagent.bat*) for the uninstallation of the AMC Agent the *uninstallsmcagent.iss* can be used.

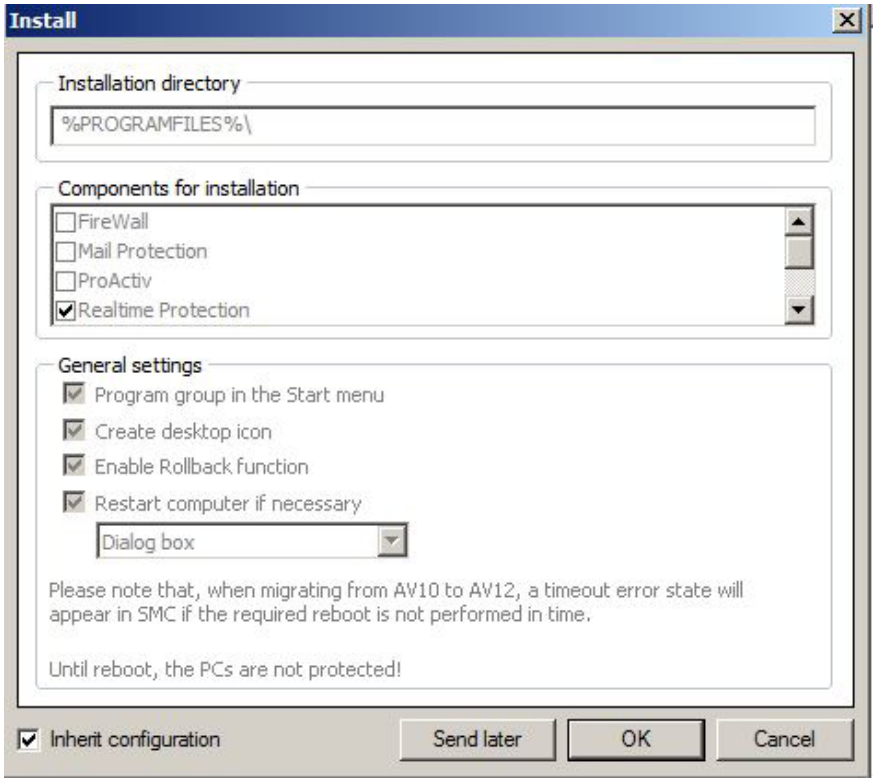
Clients that have not been integrated into the security environment before the unattended AMC Agent installation will be listed in the new group “new computers” and can be moved afterwards via drag & drop.

You have also the possibility to add new computers to existing groups by means of the IP address. Therefore, you can define an IP address or IP address sectors as a property of a group. As soon as an AMC Agent is logging on to the AMC Server for the first time, the AMC will integrate it into the corresponding group according to its IP address.

11.2. Installation of the Avira Professional Security

All Avira products that are integrated into the software repository can be installed via the AMC. This can be done by a click with the right mouse button on the designated group and then by selecting *Installation* > *Avira Professional Security* > *Install*.

Afterwards, the window “Setup Configuration” opens and you can choose the components that need to be installed and the target path:



Here, you can define an installation configuration for the entire security environment or for special computer groups that will be passed on to all computers in that group using the check box. If you uncheck that box, you can add or remove individual components that differ from the standard configuration.

If clients that have already an installed agent, are turned off, an outstanding action will be generated. That means this action will be repeated as soon as the AMC Agent logs on to the AMC Server.

Outstanding actions are shown with a red triangle on the left side of the client:

- If clients are shown with a red exclamation mark (!) (/ /), then something is wrong with the status of the installed product.

- If clients are related to groups that are not shown in extended mode, the possibly appearing red ! will not be recognized. In such a case the red group icon will give a hint:

The error status (the cause of the red !) can be found out by clicking on the client with the right mouse button and choosing *View* > *Product Status*. In such a case you can see that the update status is out of date.

An error status (red !) can also be caused by a not activated “Avira Echtzeit-Scanner” (real time protection), “Avira Email-Schutz” (POP3/SMTP-Scanner), the “Avira Scheduler” or “Avira Browser-Schutz”(WebGuard):

Module name	Module error status	Module status
Realtime Protection	Ok	Activated
Scheduler	Ok	Activated
Mail Protection	Ok	Activated
Web Protection	Ok	Activated
FireWall	Ok	Not installed
Status of update	Ok	Not available

Note
The reset of the status message that is shown by the red “!” can only be carried out by removing the cause of the error message.

In our case it would be automatically reset after an update on the concerned clients (a short waiting time up to a minute is possible).

Note
Module status – “Not available” means that the update process has no module. So “Not available” is correct and not an error.

Decisive is the “Module error status”. Ideally, “OK” should appear here. A red stop sign will appear in case of an error, e.g. during the installation of the Avira AMC Agent or of any other Avira products.

This error message can be seen by a click with the right mouse button on the client and then by selecting *Views* > *Error Messages*.

Please note the color of the the stop icon!

= Error Message
= Warning/Hint

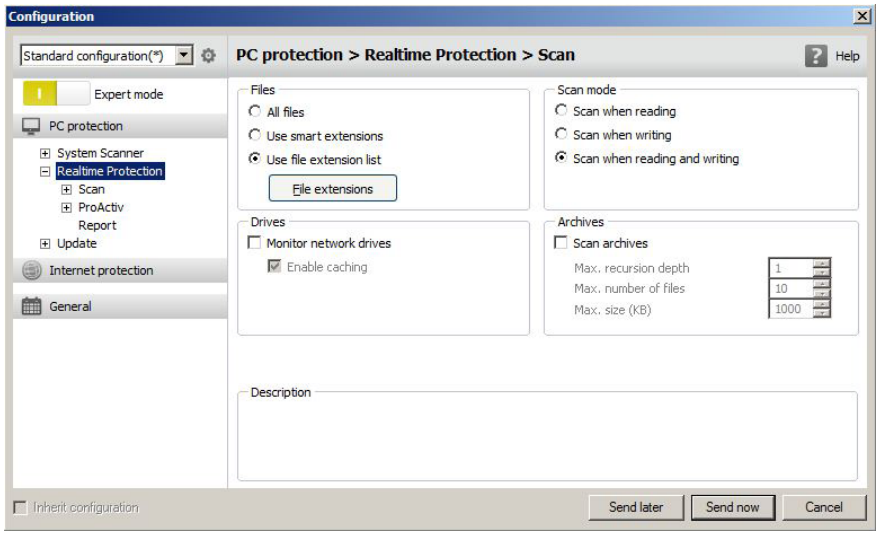
Stop messages are not automatically reset. They remain even if the cause of the stop message has already been removed. Those have to be reset by a mouse click with the right mouse button on **Reset Error Status**.

11.3. Configuration of the Avira Professional Security

All available functions can be adjusted locally at the client using the AMC. In order to get to the configuration of the Avira Professional Security click on the group that has to be configured with the right mouse button and select *Configuration* > *Avira Professional Security* > *Configure*.

The configuration of the Avira Professional Security opens. Here you can make changes similar to the local configuration of the client.

Since Avira Professional Security Version 10 GUI plugins have been integrated that cause the layout of the configuration GUI to be almost identical with the GUI of the clients. This is why you see in Avira Professional Security the same menu as you would find them on the local client:



The Update configuration can be found in each configuration of the clients underneath the point “General” and “Update”.

Change the configuration in order to proceed e.g. central updates.
Choose the update procedure “via internet“ or via fileserver/share.

In case of the update “via webserver” you have to consider that the clients will not inevitably download the updates via the internet. On the contrary the use of the *http* protocol is meant here. The update is done via a webserver which also can be located in a local network (not in the internet).

The AMC offers you an already included Avira Update Manager which also works as a webserver on port 7080. Please, note the detailed information given in the AMC manual.

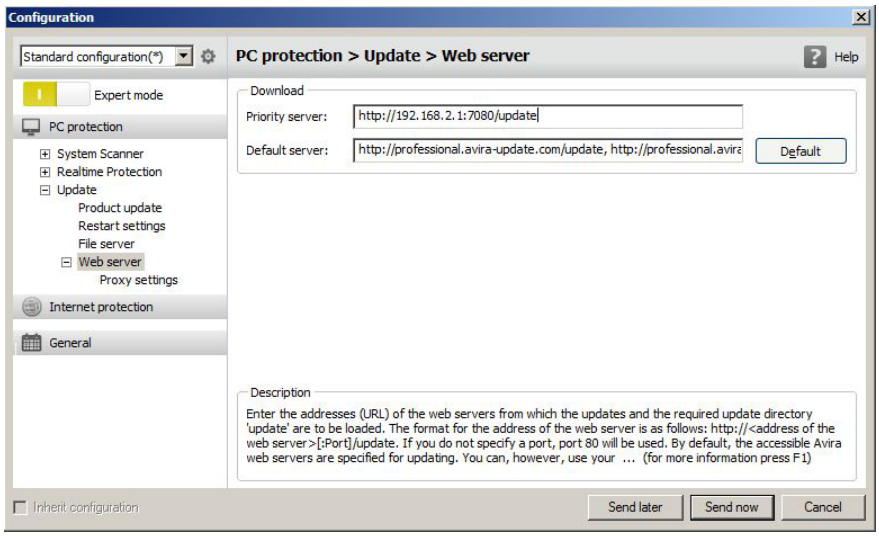
The advantages of using http for the updates are:

- Several update servers can be entered; in case the first one cannot be reached the following registered one will be used.

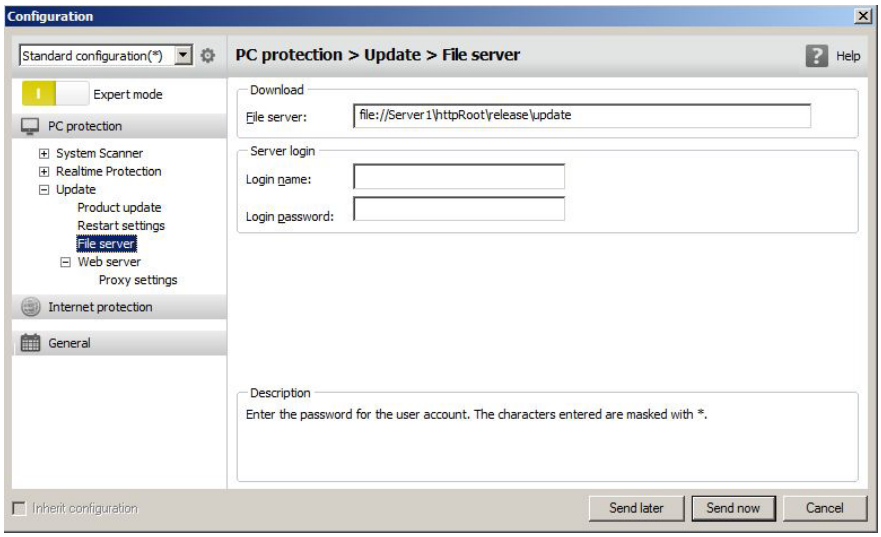
  In case of the configuration of a laptop the internal webserver can be named as the first update server and the Avira Update Manger can be defined as the second update server. If the laptop is used far from the enterprise network the updates will be done via the second update server, the Avira server.

- It is not necessary to care about the authentication of the share which is important for the use of “via filesharing”.

The configuration of the update „via webserver“ can look as follows using Avira Professional Security:



The configuration of the updates „via filesharing“ in Avira Professional Security can look as below:



Using the update option “via filesharing“ you should not forget to enable the destination directory “httproot” (root directory for the updated files) of the Internet Update Manager via the file system (read access is sufficient).

This directory is normally located in:
C:\Documents and settings\All Users\Application data\Avira\Avira Internet Update Manager\HttpRoot

Also, the „Server Login Name“ and the „Server Login Password“ should be configured, so that the updater can load the updates even if the user login on the client has not yet taken place.

Once you have chosen and configured an update possibility, it can be sent by a click on “Send Now” to the clients. For clients that are deactivated when the configurations are transmitted, an outstanding action will be generated. The “outstanding action” will be carried out as soon as the client will be activated and the AMC Agent will have registered with the AMC Server.

11.4. Planning and Executing of Updates and Scans

An update or scan order can be executed by clicking with the right mouse button on the designated group in the AMC. Then click on
Commands > Avira Workstation > Start Update / Scan.

You can now select “Schedule this command” in the dialog that appears now. This command executes updates or scans automatically at particular times and after specified time frames.

If the button “Schedule this command” is not activated, an update or scan is executed at once (depending on the command).

The execution of the commands “Update” or “Scan” are almost the same. The only difference consists in the different possibilities of the execution. This is why a detailed description of the command “Scan” is omitted. Further details can be found in the manual.

11.5. Installation of the Avira Server Security

The Avira Server Security has to be integrated into the “software packages” just like the Avira Professional Security in order to be installed and configured using the AMC.

The installation procedure is similar to the Avira Professional Security and is therefore not described here. For further information of the Avira Server Security installation, please read the manual.

11.6. Configuration of Avira Server Security

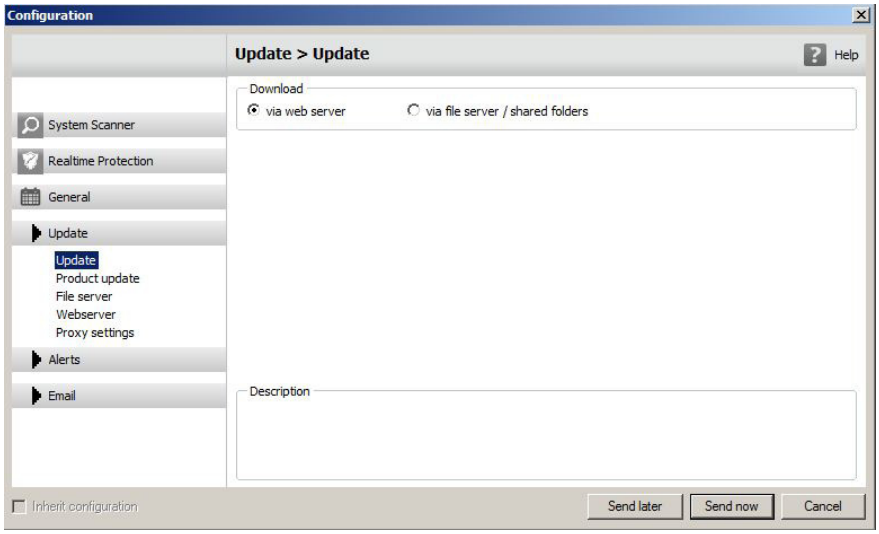
All functions and configurations that can be adjusted locally at the Avira Server Security, are available in the AMC .
You can navigate to the configuration of the Avira Server Security via the AMC with a right mouse click on the group you want to configure.

Select *Configuration* > *Avira Server Security* > *Configure*.

The configuration of Avira Server Security opens. Here you can make changes similar to the local configuration at the Avira Server Security.

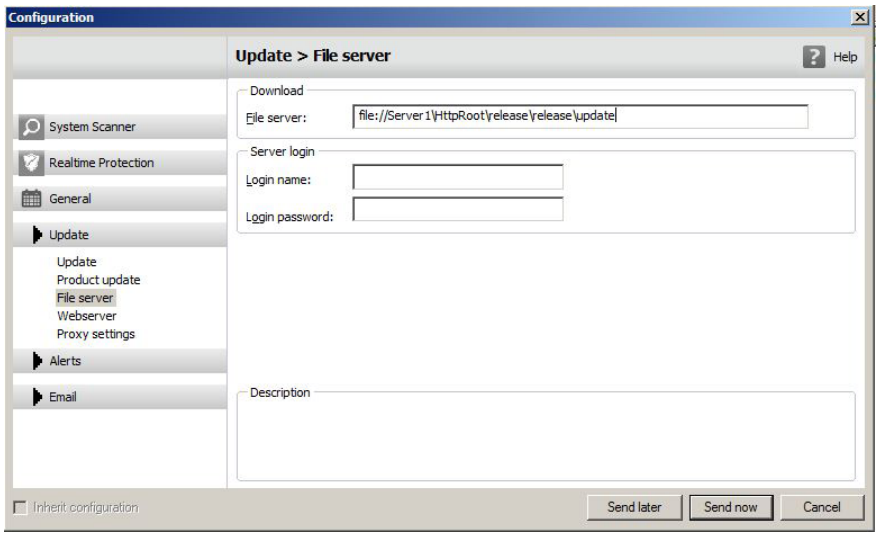
The update configuration is located in the menu of the register „Updates“. Change the configuration here in order to be able to execute e.g. central updates.
You can choose here the update procedure “via a webserver (intranet)” or “via fileserver / share”.

The update path has to be configured, depending on the kind of update you have selected.



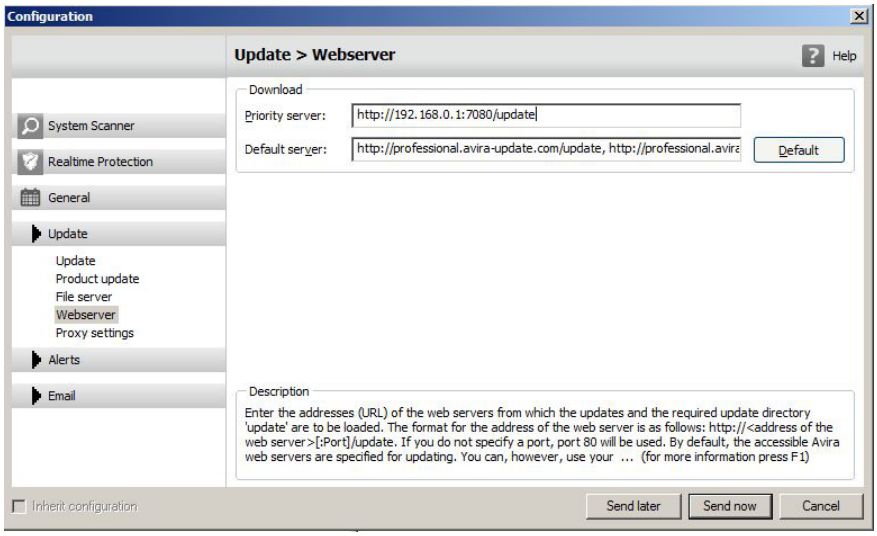
If the update needs to be loaded via “Fileserver/Share”, the target folder of the Internet Update Manager “HttpRoot” has to be enabled via the file system (reading rights are enough). The configuration of the update can be seen in the screenshot above.

It is important to configure “Server Login Name” and “Server Login Password”, so that the Updater can load updates even if the user login to the Windows Server hasn‘t taken place yet or if the user who has logged on, has no access rights to the update registry.



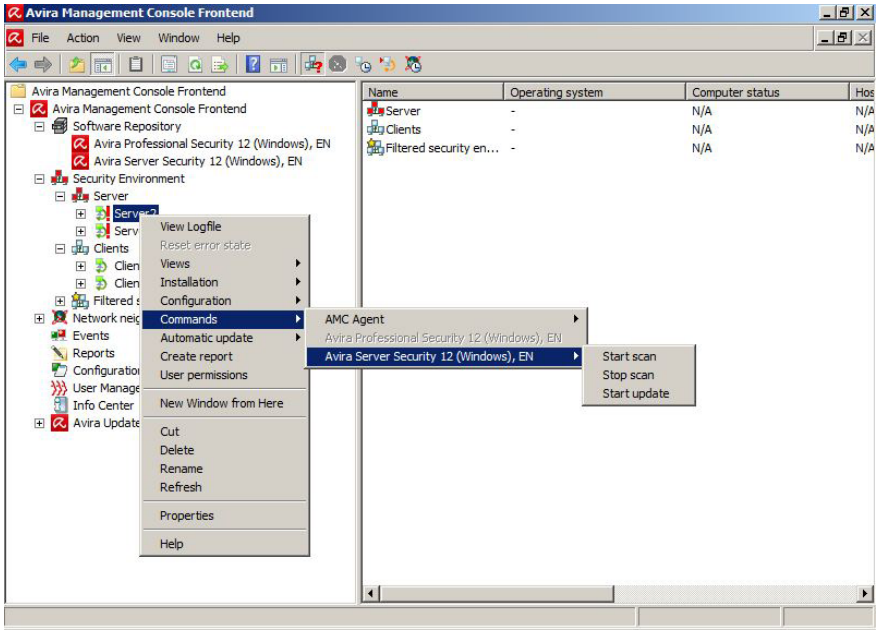
An update via the webserver which is offered by the Internet Update Manager is also possible. The internet update will be changed, so that “dl.antivir.de/update“ isn’t used as the update source but the webserver of the internet updater is called.

The example for the configuration “via webserver (intranet) is shown in the screenshot on the next page.



11.7. Planning and Executing of Updates and Scans

In order to execute an update or a scan command via the AMC you need to click with the right mouse button on the designated group and then on *Commands > Avira Server Security > Start Update/Scan*:



As the planning of the updates or scans is similar to the procedure regarding the Avira Professional Security it will not be described here.

Further information can be found in the manual.

11.8. How to reset or to transfer the configuration

If a configuration concerning the “security environment” has been modified for one product it will be transferred to all pc’s in the “security environment” respectively in the subgroups.

Exception:
In case a subgroup/pc has been configured separately in a particular way by deactivating the option “Transfer configuration”, this group/pc will keep its configuration and will not accept the superior configuration.

In order to make sure that the special configured subgroup/pc accepts the superior configuration, the special configuration of the subgroup/pc needs to be reset (*Configuration* > *Avira Professional Security* > *Reset all*).

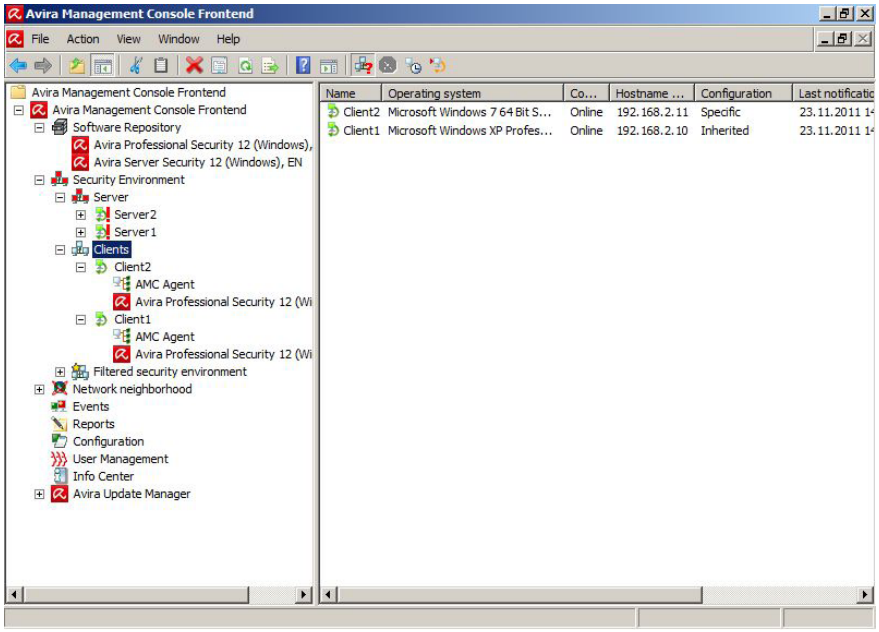
Example:
The function “Transfer configuration” has been deactivated for the subgroup “clients” and it has been configured in a way that the expert mode will not be shown. A configuration has been chosen via the superior group “security environment”, showing the expert mode.

The group “clients” will not accept this configuration that has been made here as a special configuration. If the configuration of the “security environment” needs to be accepted, the configuration of the group “clients” has to be reset.

Click with the right mouse button on the group “clients” and select *Configuration* > *Avira Professional Security* > *Reset all*.

In order to see which groups or pc’s have a transferred or a special configuration, click on the corresponding superior group (f. ex. “security environment”).

In the right half of the Avira Management Console Frontend you can see if the configuration is “specific” or “inherited”.



11.9. Product update from SMC 2.6/AMC 2.6.1 to AMC 2.7

Direct update:

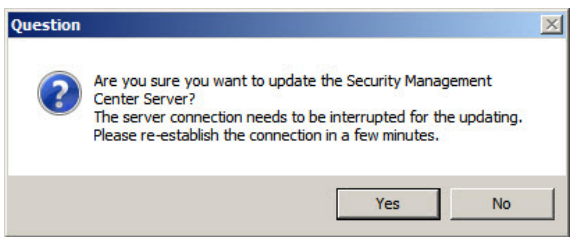
1. Click with the right mouse button on „Security Management Center Frontend“ and select *Update*.

2. Select *Server Start update* to update the server.

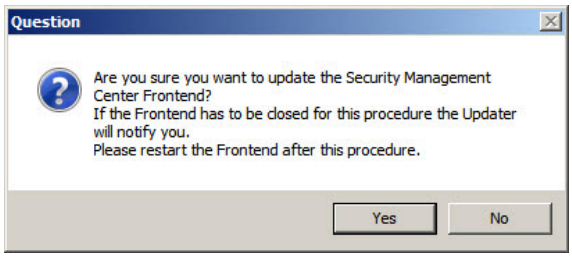
   or

   Select *Frontend* to update the frontend.

The following message appears if you update the SMC-server:



When updating the SMC Frontend:



Click **Yes** to confirm and close the SMC Frontend if necessary.
The connection to the AMC-server will be interrupted.

Avira AMC will connect to the Internet Update Manager, which provides the updates of the product.

Restart the AMC Frontend, and log back on to the AMC Server.

Updating SMC-agents:

It is recommended to update SMC-agents automatically via the Avira Internet Update Manager (Default).

How to update SMC-agents across the network or in a specific group:

Click with the right mouse button on the node **security environment** or on the nodes of the group and select *Commands* > *Avira AMC Agent* > *Start Update*.

How to update SMC-agents on a specific computer:

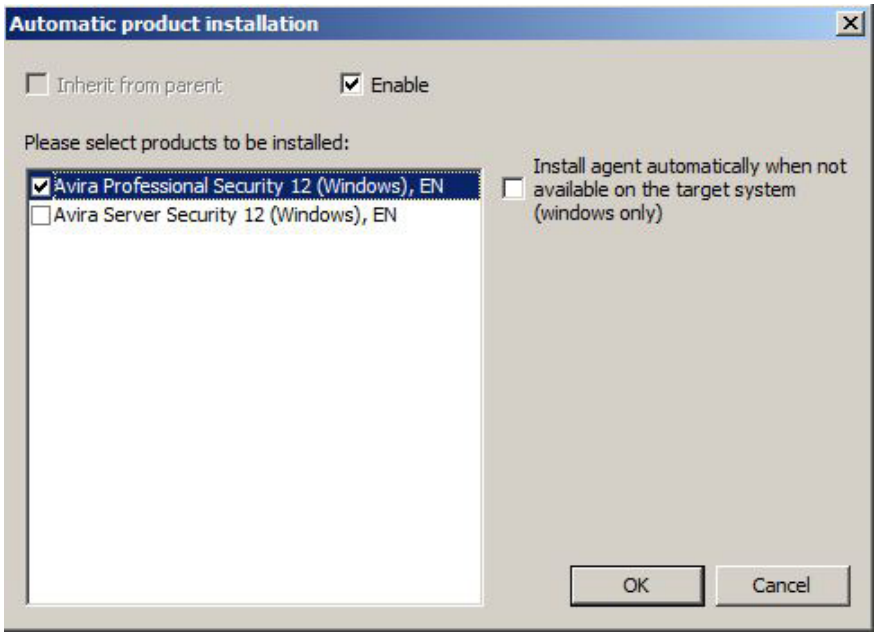
Click with the right mouse button in the **security environment** on the node of the computer at „Avira AMC Agent“ and select *Commands* > *Start Update*.

You can schedule updates of SMC agents also chronologically.
Click within the window „Commands“ on the button **Schedule this command**.

12. Automatic Product Installation

Since SMC Version 2.5 there is the option to define an automatic product installation. This function installs the defined product automatically on all computers that are moved into certain groups.

Click with the right mouse button on a group, then select *Installation* > *Products*. Then, you can select the software packages.



13. Automatic Synchronization with ADS/LDAP

The already existing option to synchronize the AMC Security Environment with ADS or LDAP has been extended. Now you are able to process this with the help of the scheduler.

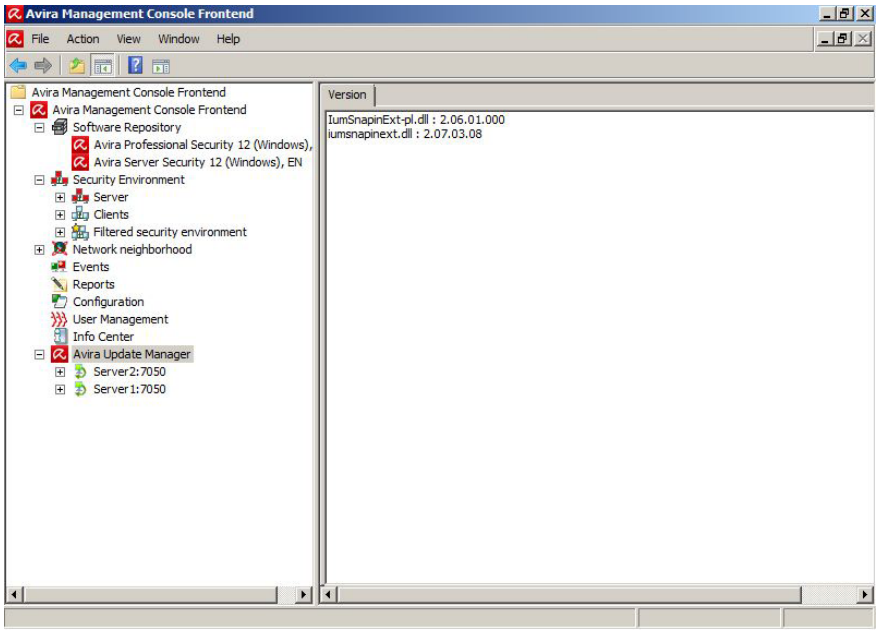
Click with the right mouse button on **Security environment** and select “Plan synchronization”. As usual, you can select how to process the synchronization.

Finally, you can insert a task that automatically processes the synchronization in the future.

14. Administration of several AUMs via the AMC Frontend

In case of several standalone AUMs (e.g. for several subsidiaries), you had to manage those via separate AUM frontends. Since SMC 2.5 you can manage several AUM servers using the AMC frontend.

You can add a new AUM as follows:
Right-click on *Avira Update Manager* > *New* > *Add AUM Server*. After the AUM Server or several AUM servers have been added to the AMC-Frontend, a product synchronization will be performed automatically.



15. AMC Event Levels

15.1 Level Info

Type	Message
Service/Application Startup	Service/Application started. Version: „application version“
Service/Application Stopped	Service/Application stopped.
Service Activated	Service has been activated.
Service Deactivated	Service has been deactivated.
Version Information	Versions: „Module: Version1, Module2: Version2, …“
License Information	License valid until “Expiration date”, user “User”, user count “User count”
License Expires (>30 days)	License expires in „Days until expiration“ days
Update Available	Important new program files are availab-le for download.
Update Successful new files	Update from “Download Server, File1: Version1,…” has been performed suc cessfully.
Update Successful no new files	Update from “Download server” has been performed successfully. No new files available.
Restart Required	Important program files have been downloaded and installed. To complete the installation your system must restart.
Configuration Changed	The configuration has been changed.
Engine VDF Version Info	Engine version: „Engine version“. VDF Version: „VDF version“
Malware Scan Finished	Scan ended “Abort type (Normal, User Abort, …)”. Number of files: “Number of Files scanned”. Number of folders: “Number of folders scanned” Number of malware: “Number of malware found”. Number of errors: “Number of errors”
Rule Added	Added rule: Cause: “Cause”, Access: “Access”, IP-Address: “IP-Address”, Rule Name: “Name”.

Type	Message
Rule Matched	Rule matched: IP-Address: “IP-Address”, Local Port: “Local Port”, Remote Port: “Remote Port”, Rule Name: “Rule Name”.
Proactive activated	Rule matched: IP-Address: “IP-Address”, Local Port: “Local Port”, Remote Port: “Remote Port”, Rule Name: “Rule Name”.
Application silently allowed	Application “Path to file”, running in con text of user “User name” was silently allowed to “Action code”

15.2 Level Error

Type	Message
License Error	The service detected an invalid license.
Update Failed	Update from “Download server“ failed. Error: “Code [Message]”
Error Occured	An error occurred: Code: „Code [Mes-sage]“

15.3 Level Warning

Type	Message
Unauthorized Configuration Change	The configuration has been changed wi-thout authorization. Switching to defaults values.
Proactive deactivated	AntiVir ProActive has been deactivated.
Blacklist Match	AntiVir ProActive has blocked access to the following application: “Path to File”. Start of that application has been denied.
Application allowed (Game Mode)	Avira Firewall automatically allowed (Game mode) communication from and to the following application: “Path to file” Filename: “User name” MD5: “Action code”.
License Expires (>30 days)	License expires in „Days until expiration“ days

15.4 Level Critical

Type	Message
Security Alert	Critical security condition detected: Code: “Code [Message]”

15.5 Level Security

Type	Message
Malware Found	Malware “Malware name [Category (from prefix library]” was found in file “Full qualified file name”. Action taken: “Action taken”
Malware Found (Email)	Malware “Malware name [Category (from prefix library]” was found in email with subject “Subject” from “Sender” to “Receiver”. Action taken: “Action taken “
Malware Found (http)	“Malware name [Category (from prefix library]” was downloaded from “URL”. Action taken: “Action taken”
Spam Detected	Email with subject “Subject” from “Sender” to “Receiver” was classified as “Spam category”‘. Action taken: “Action taken”
Bot Detected (Unauthorized Email Address)	Blocked sending email from the unauthorized email address “Email address”. This can be a hint for a new and hidden malware.
Bot Detected (Unauthorized Mail Server)	Blocked sending email to the unauthorized server “Server name”. This can be a hint for a new and hidden malware.
Application Blocked	Blocked application “Application name”. Local URI: “Local URI”, Remote URI: “Remote URI”, Path: “Application path”, Action taken: “Action ID (EP_OPTION_ACTION_...”
Application Blocked (2)	Avira Firewall blocked communication from and to the following application: “Application name”, Filename: “File name”, MD5: “MD5”.

Type	Message
Port Scan Detected	Port scan detected. Attacker IP: “Attacker IP”
Port Scan Detected (UDP)	UDP Port scan detected. Attacker IP: “Attacker IP”
Enter Flood State	A flooding has started on adapter “Adapter name”
Exit Flood State	A flooding has stopped on adapter “Adapter name”
Harmful Process Found	AntiVir ProActive found a possibly harmful application. Started from file “Path to file”. Action selected by user: “Action description”

16. General Hints / Information

INFO Bubbles:
When you slide over the configuration icons in the AMC with the mouse curser, yellow information windows will appear that will provide you with helpful hints.

ICONS of the AMC:
There are several icons which can appear in the AMC. They are described in the following:

 = Error message

 = Warning/hint

 = The client is activated, agent installed, communication established

 = check produkt status

 = The client is deactivated/cannot be reached; agent is not installed

 = The client is deactivated/cannot be reached; agent is installed

 = The client is deactivated/cannot be reached; agent is installed; outstanding action

 = Client is activated, Agent is not installed

	=	PC is activated; Agent is installed but cannot be reached
	=	Hourglass, the client is connecting to the AMC Server or is busy processing the commands of the AMC
	=	Symbol of the agent that has been installed on the client
	=	Valid software package without integrated license file „hbedv.key“
	=	Valid software package with integrated license file „hbedv.key
	=	Software package is installed on the client

ID of software packages:

In case you get the message “Missing software package with ID XX” the software package is not integrated or it is integrated with an old and faulty version:

Software ID	=	Softwarepaket
3	=	AMC-Agent
51	=	UNIX Server
71	=	UNIX Workstation/Professional
91	=	UNIX MailGate
111	=	UNIX WebGate
121	=	UNIX Updater
500	=	AntiVir Professional 10 German
501	=	AntiVir Professional 10 English
502	=	AntiVir Professional 10 Russian
503	=	AntiVir Professional 10 Spanish
504	=	AntiVir Professional 10 Italian
505	=	AntiVir Professional 10 French
600	=	AntiVir Server 10 German
601	=	AntiVir Server 10 English
602	=	AntiVir Server 10 Russian
603	=	AntiVir Server 10 Spanish
604	=	AntiVir Server 10 Italian
605	=	AntiVir Server 10 French
700	=	Avira Professional Security 12 German

701	=	Avira Professional Security 12 English
702	=	Avira Professional Security 12 Russian
703	=	Avira Professional Security 12 Spanish
704	=	Avira Professional Security 12 Italian
705	=	Avira Professional Security 12 French
706	=	Avira Professional Security 12 Portugese (Brazil)
707	=	Avira Professional Security 12 Chinese (simplified)
708	=	Avira Professional Security 12 Japanese
709	=	Avira Professional Security 12 Korean
710	=	Avira Professional Security 12 Romanian
711	=	Avira Professional Security 12 Chinese (traditional)
712	=	Avira Professional Security 12 Turkish
713	=	Avira Professional Security 12 Dutch
750	=	Avira Server Security 12 German
751	=	Avira Server Security 12 English
752	=	Avira Server Security 12 Russian
753	=	Avira Server Security 12 Spanish
754	=	Avira Server Security 12 Italian
755	=	Avira Server Security 12 French
756	=	Avira Server Security 12 Portugese (Brazil)
757	=	Avira Server Security 12 Chinese (simplified)
758	=	Avira Server Security 12 Japanese
759	=	Avira Server Security 12 Korean
760	=	Avira Server Security 12 Romanian
761	=	Avira Server Security 12 Chinese (traditional)
762	=	Avira Server Security 12 Turkish
763	=	Avira Server Security 12 Dutch
800	=	Avira Professional Security 13 German
801	=	Avira Professional Security 13 English
802	=	Avira Professional Security 13 Russian
803	=	Avira Professional Security 13 Spanish
804	=	Avira Professional Security 13 Italian
805	=	Avira Professional Security 13 French
806	=	Avira Professional Security 13 Portugese (Brasil)
807	=	Avira Professional Security 13 Chinese (simplified)
808	=	Avira Professional Security 13 Japanese
809	=	Avira Professional Security 13 Korean
810	=	Avira Professional Security 13 Romanian
811	=	Avira Professional Security 13 Chinese (traditional)
812	=	Avira Professional Security 13 Turkish
813	=	Avira Professional Security 13 Dutch
850	=	Avira Server Security 13 German
851	=	Avira Server Security 13 English
858	=	Avira Server Security 13 Japanese

16. UNIX

16.1 Manual Installation of the AMC Agents for UNIX

You can also manually install the SMC agent.

The required product package *AntiVir_Security_Management_Center_UNIX_Agent.tgz* is part of Avira Management Console (AMC) installation package and can be downloaded on our homepage.

The installation package can be extracted with the following command:

```
unzip avira_management_console_en.zip
```

Unpack the agent package:

```
tar xzf Avira_Management_Console_Unix_Agent.tgz
```

Change to the installation directory:

```
cd Avira_Management_Console_Unix_Agent
```

Install the AMC agent:

```
./install --server_uri=http://HOST[:PORT] --display-name=<AMC
display name> --update_uri=http://HOST[:PORT]
```

The IP address of the server and the AMC display name have to be issued. The name of the server and update port can be given optionally. This is only necessary if the AMC Server does not use the default ports for the communication with the AMC agent.

16.2 Installation and configuration of Avira AntiVir UNIX Professional/Server

The AV Guard can only be used via the AMC if the dazuko module can be loaded automatically by means of the command modprobe or it has already been loaded. Details about the translation and installation of “dazuko“ can be found in the HowTo on the dazuko website.

Before you can start with the installation the product packages for Avira AntiVir UNIX Professional and Avira AntiVir UNIX server need to be added to the product packages of the AMC and a license needs to be added.
The package is called *antivir-workstation-prof.tar.gz* or *antivir-server-prof.tar.gz.* The packages can also be downloaded from the Avira website.

In order to start the installation of Avira UNIX Professional Security/Server, click on the node „security environment“ and as the case may be, on the group or the computer where the Avira Unix Professional Security/Server should be installed.

Click with the right mouse button on the “group“/the “computer“ and choose „Installation/Avira Professional Security/Server (UNIX)/Install“. The dialog window „Installation“ appears and needs to be confirmed with **OK**.

The AV Guard is started automatically during the boot process but is not started after the installation. This is shown in the AMC with the icons “Check product status”.
In order to start the AV Guard click with the right mouse button on the group/the computer and choose *Avira Professional Security* > *Server (UNIX)* > *Start*.
If the Guard cannot be started and the error status remains, it is possible that dazuko (file access control) is missing on the server or has not yet been loaded.

All directories are monitored by the guard during an installation via the AMC. The choice of directories that should be controlled can be changed in the registry “Basic Settings” of the configuration. Click with the right mouse button on the “group“/the “computer“ and choose *Configuration* > *Avira Professional Security* > *Server (UNIX)* > *configure*.

We recommend supervising only a few important directories (e.g. enable share). Details about the configuration of Avira UNIX Professional Security/Server can be found in the manual for Avira UNIX Server (chapter 4 configurations).

16.3. Installation and Configuration of Avira UNIX WebGate

Before the installation the product package for Avira AntiVir UNIX WebGate needs to be added to the software packages of the AMC and a license has to be entered.
The package is called *antivir-webgate-prof.tar.gz*.
The package can be downloaded from the Avira website.

In order to start the installation of Avira AntiVir UNIX WebGate, click on the node „security environment“ and as the case may be on the “group“/the “computer“ where Avira WebGate should be installed.

Click with the right mouse button on the group/the computer and choose *Installation* > *Avira WebGate (UNIX)* > *Install*. The dialog window installation appears and has to be confirmed by clicking on **OK**.

WebGate is started automatically after the boot process but it will not be started after the installation. This is shown here: *Views* > *Product Status*. In order to start WebGate, click with the right mouse button on the group/the computer and select *commands* > *Avira WebGate (UNIX)* > *Start*.

In order to make changes about the configuration, click with the right mouse button on the “group“/the “computer“ and navigate to *Configuration* > *Avira AntiVir WebGate (UNIX)* > *configure*. You will find all the details about the configuration in the manual Avira AntiVir UNIX WebGate (Chapter 4 Configuration).

16.4. Installation and configuration of Avira UNIX MailGate

Before the installation the product package for Avira AntiVir UNIX MailGate has to be added to the software packages of the AMC and a license needs to be entered. The package is called antivir-mailgate-prof.tar.gz. The package can be downloaded from the Avira website.

In case of an installation via the AMC, only the configuration of MailGate can be done. The configuration of the MTA (e.g. postfix) cannot be processed with the AMC. In order to start the Installation of Avira UNIX MailGate, click on the node „security environment“ and as the case may be on the “group“/the “computer“ where Avira UNIX MailGate should be installed.

Click with the right mouse button on the group/the computer and select *Installation* > *Avira MailGate (UNIX)* > *Install*. The dialog window Installation appears and needs to be confirmed by **OK**.

MailGate and the used MTA need now to be configured. Please note the necessary configuration settings in the manual Avira AntiVir MailGate UNIX (chapter 4.4 Further installation passes dependent on the MTA).

In order to make the described changes in the configuration, click with the right mouse button on the group/the computer and navigate to *Configuration* > *Avira Anti-Vir Mailate (UNIX)* > *configure*. Further Details about the configuration can be found in the manual for Avira AntiVir UNIX MailGate (chapter 6 configuration).

MailGate is started automatically after the boot process but is not started after the installation. In order to start MailGate, click with the right mouse button the “group“/ the “computer“ and choose *Commands* > *AntiVir WebGate (UNIX)* > *Start*.

Issued Q2-2013

AVIRA

live free.™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile +49 7542-500 3000
www.avira.com