

Avira Management Console 2.7

Kurzanleitung

Inhaltsverzeichnis

1. Installation AMC-Server	4
2. Installation AMC-Frontend	7
3. Aufruf und Anmeldung an der AMC	7
4. Lizenzierung der AMC	7
5. Softwarepakete einrichten	8
6. Sicherheitsumgebung einrichten	10
7. Konfigurationseinstellungen der AMC	11
8. Installation des AMC-Agents über das AMC-Frontend	11
9. Pull / Push Modus des AMC Agents.....	13
10. Filternde Gruppen.....	15
11. Windows Installation	18
11.1. Installation des AMC-Agents „unattended“	18
11.2. Installation der Avira Professional Security	19
11.3. Konfiguration von Avira Professional Security.....	21
11.4. Planen- bzw. Ausführen von Updates / Suchläufen.....	24
11.5. Installation der Avira Server Security	24
11.6. Konfiguration des Avira Server Security.....	24
11.7. Planen- bzw. Ausführen von Update u. Suchläufen.....	26
11.8. Konfiguration rücksetzen/vererben:.....	27
11.9. Produktupdate der SMC 2.6/AMC 2.6.1 auf AMC 2.7.....	28
12. Automatische Produktinstallation.....	30

13. Automatische Synchronisierung mit ADS/ LDAP...	30
14. Mehrere Avira Update Manager (AUM) über AMC-Frontend verwalten	31
15. AMC Event Levels	31
15.1 Level Info	31
15.2 Level Error	33
15.3 Level Warning	33
15.4 Level Critical	33
15.5 Level Security	33
16. Generelle Hinweise/Informationen	35
16. UNIX	37
16.1. Manuelle Installation des AMC-Agents für UNIX	37
16.2. Installation und Konfiguration von Avira AntiVir UNIX Professional/Server	38
16.3. Installation und Konfiguration von Avira AntiVir UNIX WebGate	39
16.4. Installation und Konfiguration von Avira AntiVir UNIX MailGate	40

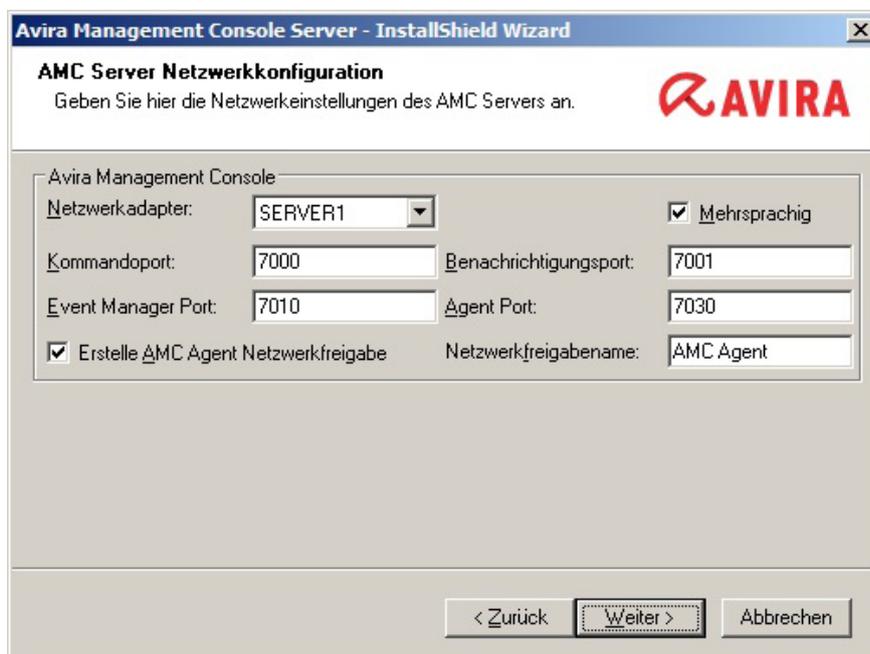
1. Installation AMC-Server

Sämtliche für die Installation benötigten Installationsdateien sowie die Produkthandbücher im PDF-Format, finden Sie zum Download auf unserer [Internetseite](#).

Nachdem Sie die Installationsdatei der AMC heruntergeladen und auf Ihrem Windowsserver entpackt haben, starten Sie zunächst die Installation des Avira Management Console Server:

avira_management_console_server_de.exe.

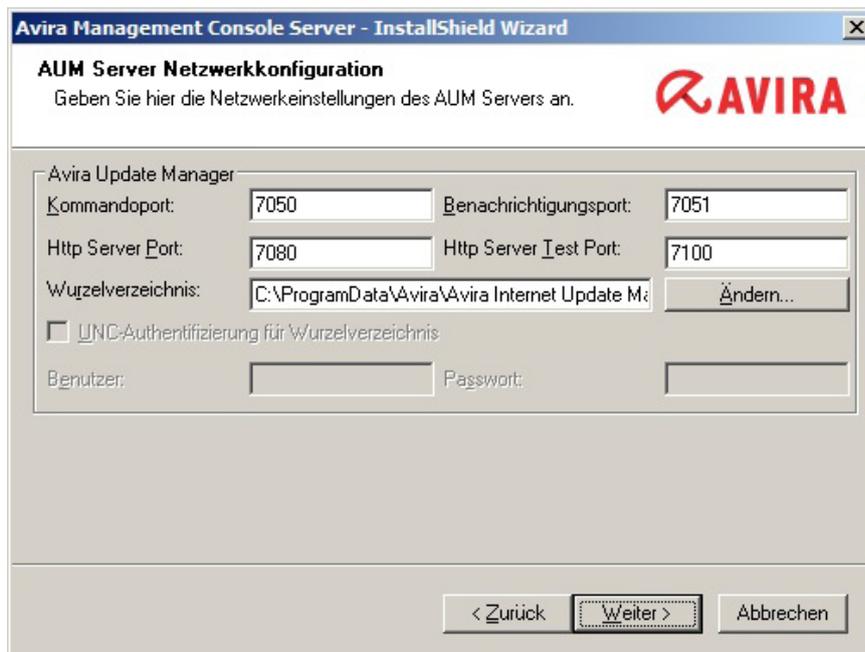
Während der Installationsroutine erscheint folgendes Fenster, in dem Sie die Netzwerkkonfiguration des Avira Management Console Servers, falls notwendig, abändern können:



The screenshot shows a window titled "Avira Management Console Server - InstallShield Wizard". The main heading is "AMC Server Netzwerkkonfiguration" with the instruction "Geben Sie hier die Netzwerkeinstellungen des AMC Servers an." and the Avira logo. The configuration area is titled "Avira Management Console" and contains the following fields and options:

Netzwerkadapter:	SERVER1	<input checked="" type="checkbox"/> Mehrsprachig	
Kommandoport:	7000	Benachrichtigungsport:	7001
Event Manager Port:	7010	Agent Port:	7030
<input checked="" type="checkbox"/> Erstelle AMC Agent Netzwerkfreigabe	Netzwerkfreigabename: AMC Agent		

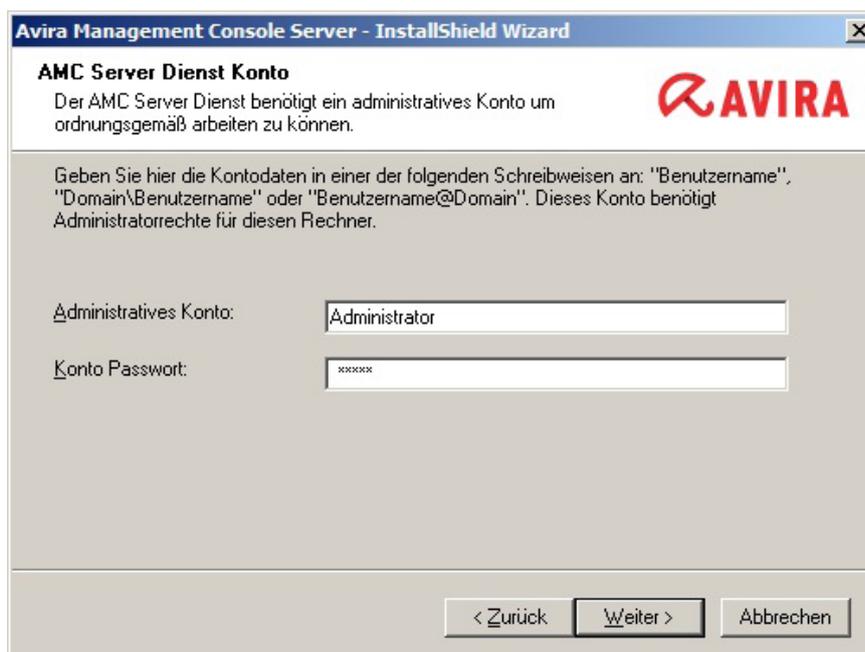
At the bottom, there are three buttons: "< Zurück", "Weiter >" (highlighted with a dashed border), and "Abbrechen".



Achten Sie darauf, dass die hier standardmäßig vorgegebenen Ports „7000“, „7001“, „7010“, „7030“, „7050“, „7051“, „7080“ und „7100“ von keiner anderen auf dem Server installierten Anwendung bereits verwendet werden.

Dies können Sie mit Hilfe des Befehls `netstat -an`, welchen Sie über die Eingabeaufforderung absetzen können, überprüfen.

Während der Installation erscheint folgendes Fenster. Um die benötigten Dienste installieren zu können, müssen Sie das Administratorkonto (bzw. Domänen-Administratorkonto) mit entsprechendem Kennwort hinterlegen:



Nachdem Sie auf **Weiter** geklickt haben, erscheint folgendes Fenster:

Avira Management Console Server - InstallShield Wizard

AMC Benutzer Anlegen

Der AMC Server benötigt ein Benutzerkonto mit Hilfe dessen Sie sich über das AMC Frontend anmelden können.

Bitte geben Sie hier einen Benutzernamen und Passwort an, mit dem Sie sich über das AMC Frontend am AMC / AUM Server anmelden möchten. Dieser Benutzer wird automatisch in der Benutzerverwaltung des AMC Servers angelegt.

AMC Benutzer: Administrator

AMC / AUM Passwort: [REDACTED]

AMC / AUM Passwort wiederholen: [REDACTED]

Konto des AMC Server Dienstes als AMC Benutzerkonto verwenden

InstallShield

< Zurück Weiter > Abbrechen

Die aktivierte Option „Konto des AMC-Server Dienstes als AMC Benutzerkonto verwenden, bedeutet, dass Sie sich mit dem soeben angegebenen Benutzer später ebenfalls an der AMC als „Administrator“ anmelden können (die selben Login-Daten wie der zuvor angegebene Windows-Administrator).

Alternativ können Sie, indem das Häkchen deaktiviert wird, an dieser Stelle einen eigenen AMC-Benutzer angeben, welcher zur Anmeldung an der AMC verwendet werden soll. Im anschließend erscheinenden Fenster haben Sie die Möglichkeit den Planer des Avira Update Managers zu konfigurieren. Je nach Einstellung lädt dieser später die Produktupdates, sowie die neusten Virendefinitions- und Engine Updates herunter:

Avira Management Console Server - InstallShield Wizard

Zeitplaner Konfigurieren

Legen Sie hier fest in welchen Intervallen nach Aktualisierungen gesucht werden soll.

Zeitplanung

Zeitplaner aktivieren: Bitte wählen Sie Uhrzeit und Datum zu dem die Aktualisierung starten soll

Einmalig

Stündlich

Täglich

Wöchentlich

Monatlich

Alle: 00 Tag(e) 01 Stunde(n) 00 Minute(n) (min. 15 Minuten)

Startzeit: 10:00:00

Startdatum: 15.12.2011

< Zurück Weiter > Abbrechen

2. Installation AMC-Frontend

Das AMC-Frontend (Programmverwaltungsoberfläche) wird benötigt, um den AMC-Server zu konfigurieren und muss separat installiert werden. Dies kann ebenfalls auf dem Windowsserver und/oder auf einem Administrator-Arbeitsplatz-PC geschehen.

Führen Sie für die Installation des Avira Management Console Center Frontends die Datei „avira_management_console_frontend_de.exe“ aus und bestätigen Sie das erscheinende Fenster mit „Annehmen“.

Führen Sie die Installation über den Installationsassistenten zu Ende.

3. Aufruf und Anmeldung an der AMC

Die AMC wird über den Startmenüeintrag *Start > Programme > AVIRA > Avira Management Console > Avira Management Console Frontend* aufgerufen.

Um sich an AVIRA Management Console anzumelden, klicken Sie auf **AVIRA Management Console Frontend**.

Geben Sie nun Ihren während der Installation angegebenen Benutzer (Standard: Administrator) und das zugehörige Kennwort an. Klicken Sie anschließend auf die Schaltfläche **OK** um sich an der AMC anzumelden.

Achten Sie bei der Anmeldung ebenfalls darauf, sollte das AMC-Frontend nicht auf dem AMC-Server installiert sein, die Markierung von „Lokaler Computer“ auf „Computer im Netzwerk“ umzustellen.

Geben Sie in diesem Fall die IP-Adresse/Hostnamen des Servers ein, auf dem der AMC-Server installiert ist. Alternativ können Sie diesen über **Durchsuchen** auswählen.

4. Lizenzierung der AMC

Sollten Sie bereits in Besitz einer gültigen Lizenzdatei „hbedv.key“ für die AMC sein, so können Sie diese nach der Anmeldung an der AMC wie folgt einspielen:

Klicken Sie mit der rechten Maustaste auf **Avira Management Console Frontend** und anschließend auf **Lizenz**.

Über das sich anschließend erscheinende Fenster haben Sie die Möglichkeit, Ihre AMC-Lizenz einzuspielen.

Wird keine Lizenz für die AMC eingespielt, läuft diese 30 Tage im Testmodus.

5. Softwarepakete einrichten

Um mit der AMC arbeiten zu können, müssen zunächst die zu verwaltenden AVIRA-Produkte, für die eine entsprechende Lizenz *hbedv.key* vorhanden ist, als Softwarepaket in der AMC eingebunden werden.

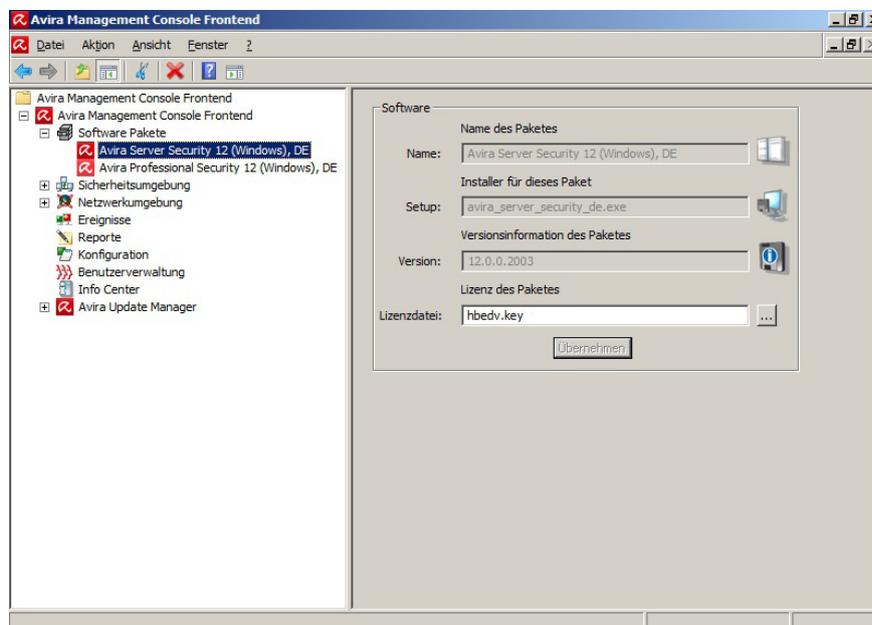
Laden Sie sich hierzu zunächst die benötigte(n) Installationsdatei(en) von unserer [Internetseite](#) herunter.

Um die Installationsdatei(en) als Softwarepaket in der AMC hinzuzufügen, klicken Sie mit der rechten Maustaste im AMC-Frontend auf **Softwarepakete** und wählen *Neu > Software* aus.

Über das sich anschließend öffnende Fenster können Sie die zuvor heruntergeladenen Installationsdateien direkt im selbstentpackenden *EXE*-Format angeben. Ebenso sind die Formate *ZIP* oder für Linux-Softwarepakete *GZ* und *TGZ* möglich.

Nachdem das Softwarepaket eingebunden wurde, erscheint dies mit einem verblassten Symbol als Unterpunkt der Softwarepakete der AMC.

Nachdem die Lizenzdatei für das entsprechende Softwarepaket ebenfalls hinterlegt wurde (dies geschieht im rechten Bereich des Fensters), wird das Symbol des Softwarepaketes farblich kräftig dargestellt:



Ein Verwechseln der Lizenz oder das Einspielen einer für das jeweilige Softwarepaket ungültigen Lizenz ist mit der aktuellen Version der AMC nicht möglich. Beim Einspielen der Lizenz wird diese auf die Gültigkeit für dieses Softwarepaket überprüft.

Die den Softwarepaketen hinterlegte Lizenz wird ausschließlich für die Erstinstallation der Software auf den Clients verwendet. Ist diese Lizenz abgelaufen, muss sie für evtl. Neuinstallationen der AVIRA-Produkte auf den Clients in den entsprechenden Softwarepaketen neu hinterlegt werden.

Hinweis

Die Lizenz auf den bereits installierten Clients wird hiermit nicht ausgetauscht. Dies muss über die „Kopierfunktion“ separat durchgeführt werden über die Sicherheitsumgebung und den Punkt *Installation > Avira Professional Security > Dateien Kopieren*.

Der Avira Update Manager lädt für die hinterlegten Produkte die benötigten Updates herunter und stellt sie per http über den in der Konfiguration des Avira Update Managers definierten Port (Standardport 7080) für die Updates der Clients zur Verfügung. Um die Updates automatisiert durchzuführen, konfigurieren Sie den im Avira Update Manager integrierten „Planer“ (Klicken Sie hierzu auf den „Avira Update Manager“ und wählen dann im entsprechenden Server den „Planer“).

Achten Sie in jedem Fall vor dem ersten Update der Clients darauf, dass der Avira Update Manager bereits das erste Update durchgeführt hat. Dies können Sie durch einen Klick mit der rechten Maustaste auf *Freigegebene Produkte > Aktualisiere gespiegelte Produkte* tun.

Ist der Haken bei der Funktion „Automatischen Modus für AMC Aktualisierungen aktivieren“ in der Konfiguration des Avira Update Managers unter Server Einstellungen gesetzt, werden Updates, welche vom Avira Update Manager geladen wurden, automatisch über ein an die Clients gesendetes Updatekommando geladen. Die entsprechende Updatequelle (z.B. <http://10.50.11.91:7080/update/>) wird hierbei automatisch temporär übergeben.

Damit sich Clients auch unabhängig von „automatischen Updates“ des Avira Update Managers aktualisieren lassen, beachten Sie bitte den Punkt „11.4. Planen-bzw. Ausführen von Updates / Suchläufen“.

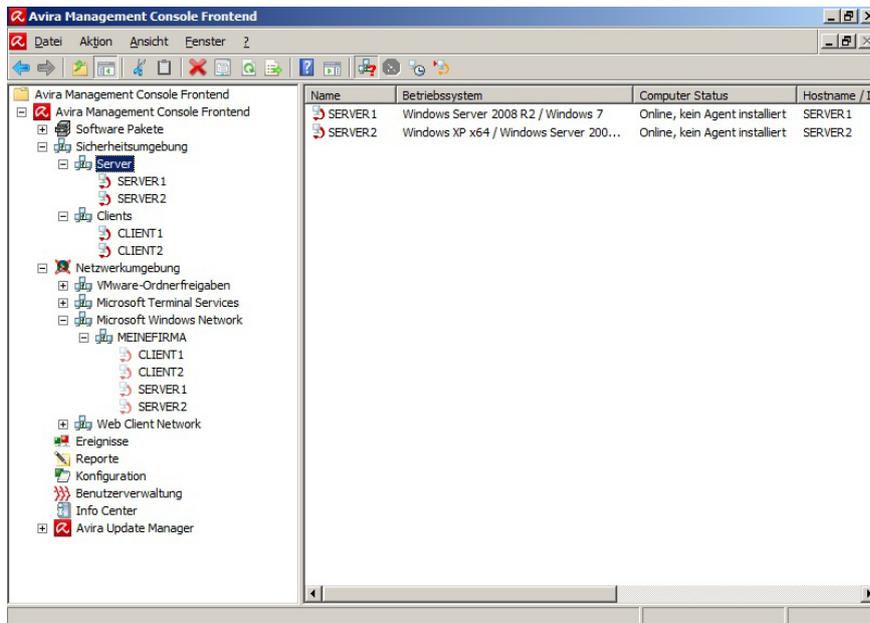
Für weitere Informationen über die „automatischen Updates“ des Internet Update Managers schlagen Sie bitte das entsprechende Kapitel im AMC-Handbuch nach.

6. Sicherheitsumgebung einrichten

Die Sicherheitsumgebung besteht aus den Clients, die über die AMC verwaltet werden sollen und können in angelegten Untergruppen zugeordnet werden.

Eine neue Gruppe kann eine Untergruppe der „Sicherheitsumgebung“ sein oder eine bereits selbst angelegte Gruppe. Gruppen werden angelegt, indem auf der gewünschten Stelle innerhalb oder auf der Sicherheitsumgebung mit einem Rechtsklick *Neu > Gruppe* ausgewählt.

Im Beispiel hier werden unterhalb der Sicherheitsumgebung die beiden Gruppen „Server“ und „Clients“ angelegt. Die Rechner, die momentan in Ihrem Netzwerk vorhanden sind, können Sie aus der „Netzwerkumgebung“, die direkt unterhalb der „Sicherheitsumgebung“ angezeigt wird, per Drag&Drop in die Sicherheitsumgebung, bzw. selbstangelegte Gruppen ziehen:



Rechner, die nicht im Netzwerk angezeigt werden, z.B. Linux, können manuell einer Gruppe zugeordnet werden. Hierzu wird auf der gewünschten Gruppe ebenfalls ein Klick mit der rechten Maustaste durchgeführt und *Neu > Computer* ausgewählt.

Anschließend öffnet sich folgendes Fenster, in dem der Rechner über den Hostnamen bzw. die IP-Adresse angegeben werden kann. Außerdem kann ein abweichender Anzeigenamen angegeben werden, unter dem dieser Rechner anschließend in der AMC angezeigt wird:



7. Konfigurationseinstellungen der AMC

Die Konfiguration der AMC selbst ist unter „Konfigurationen“ in folgende Abschnitte unterteilt:

- Allgemein
- Server
- Internet Update Manager
- Alert Manager

In der Konfiguration können allgemeine Einstellungen der AMC vorgenommen werden. Sollten Sie einen Proxyserver im Einsatz haben, kann dieser beispielsweise unter Konfigurationen > Server Einstellungen > Kommunikation angegeben werden.

Weitere Konfigurationseinstellungen wie z.B. die Konfiguration des „Alert Managers“ bitten wir Sie im aktuellen Handbuch der AMC nachzuschlagen.

8. Installation des AMC-Agents über das AMC-Frontend

Für die Kommunikation zwischen dem AMC-Server und den zu verwaltenden Clients ist der AMC-Agent zuständig.

Dieser muss zusätzlich zum auf dem Client notwendigen Virenschutz installiert werden. Dies kann direkt über die AMC oder manuell bzw. über ein Script erfolgen. Damit der AMC-Agent mit dem AMC Server kommunizieren kann, müssen folgende Bedingungen erfüllt sein:

- Firewall: Wird auf dem Client eine Firewall eingesetzt, müssen folgende Ports (TCP) freigeschaltet sein:
Out (TCP): 7000, 7001, 7010, 7020, 7021, 7030, 7050, 7051, 7080, 7100.
In (TCP): 7030. Außerdem müssen ICMP-Anfragen, PING (eingehende Echoanforderungen zulassen) zugelassen werden.
- Gastkonto: Das Benutzerkonto „Gast“ muss deaktiviert sein.
- Die „einfache Dateifreigabe“ (*Explorer > Extras > Ordneroptionen > Ansicht > Freigabe-Assistent verwenden (empfohlen)*) sollte deaktiviert sein.
- Zugriff vom AMC-Server auf die versteckte Freigabe „C\$“ des Clients muss möglich sein (\\<IP-Adresse Client\c\$).
- Zur Erleichterung der Installation über die AMC sollte es ein netzwerkweites, einheitliches administratives Benutzerkonto geben.

Die Installation des AMC-Agents über die AMC wird durchgeführt, indem Sie in der „Sicherheitsumgebung“ auf die entsprechenden Clients/Gruppen einen Rechtsklick machen und *Installation > AMC Agent > Installieren* anklicken.

Die Rechner, auf denen der AMC-Agent installiert wird, müssen zu diesem Zeitpunkt eingeschaltet und Windows hochgefahren sein!

Folgendes Authentifizierungsfenster erscheint:



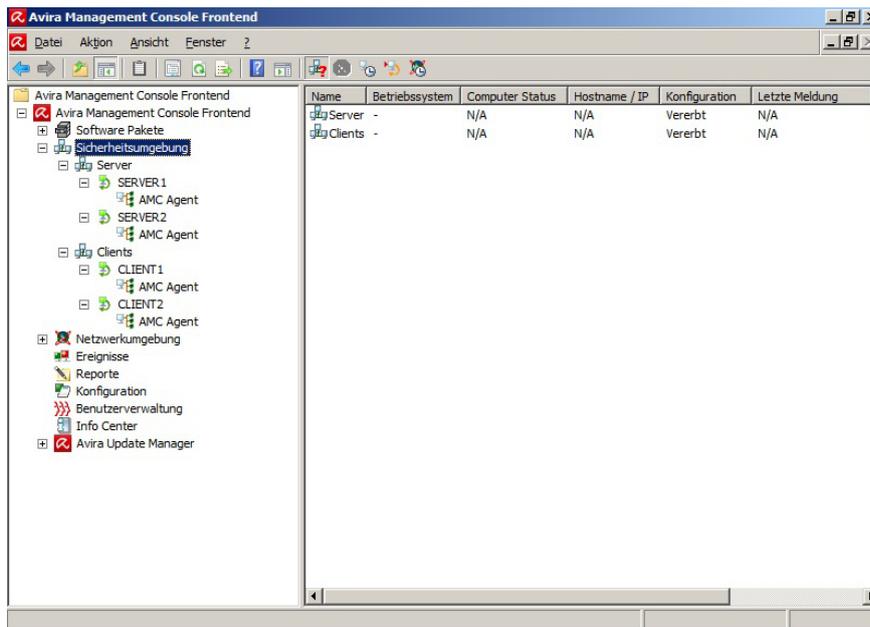
Tragen Sie entsprechend in den Feldern „Benutzername“ und „Kennwort“ einen auf dem Client existierenden Benutzer ein, der administrative Rechte besitzt. Für Linux-Clients z.B. den Benutzer „root“.

Sollte das Konto, mit dem der AMC-Server gestartet wurde, auf den jeweiligen Clients ebenfalls existieren (einheitliches lokales Administratorlogin, Domänenadministrator, ...), so kann auch die Option „Den aktuellen Account des Servers verwenden“ ausgewählt werden.

Für die Installation per SSH (Linux Clients) können Sie, falls vorhanden, einen SSH-KEY verwenden, um sich am Client zu authentifizieren.

Wählen Sie hierzu die Option „SSH public/private key Authentifizierung verwenden“ und geben den entsprechenden Schlüssel an.

Nach der erfolgreichen Installation des AMC-Agents wird der Client mit einem „grünen“ Symbol in der Sicherheitsumgebung angezeigt (Kommunikation funktioniert):



Eine evtl. notwendige Deinstallation funktioniert, ähnlich wie die Installation über einen Rechtsklick auf dem gewünschten Client/Gruppe und der Auswahl von *Installation > AMC Agent > Deinstallieren*. Die Hinweismeldung muss mit *Ja* bestätigt werden.

9. Pull / Push Modus des AMC Agents

Die AMC arbeitet nach der Installation standardmäßig im „Push-Modus“.

Dies bedeutet, dass der AMC Server geplante Kommandos wie Updates oder Suchläufe sowie beispielsweise Konfigurationsänderungen an den AMC Agent sendet, der diese auf dem entsprechenden Clients umsetzt.

Für PCs, welche zu diesem Zeitpunkt nicht vom AMC Server erreichbar sind, wird in diesem Fall eine „ausstehende Aktion“ generiert, die abgearbeitet wird, sobald sich der auf dem Client installierte Agent erneut mit dem AMC Server verbindet.

Im „Push-Modus“ versucht der AMC Server die Zielrechner gleichzeitig zu erreichen, was in einem größeren Netzwerk mit mehreren Clients zu einer kurzzeitig hohen Auslastung führt. So wird beispielsweise zu jeder Stunde ein Updatekommando an 500 PCs gesendet, bei welchem z.B. ein Update von 2 MB vom Avira Update Manager geladen wird. Dies geschieht zeitgleich auf allen 500 Clients, was bedeutet, dass (500x2MB) 1TB im Netzwerk kopiert wird.

Um diese Netzlast zu verteilen, kann die AMC auf den „Pull-Modus“ umgestellt werden. Dies hat in großen Netzwerken den Vorteil, dass der AMC Agent im konfigurierbaren Intervall beim AMC Server nachschaut, ob hier neue „Tasks“ vorhanden sind und diese abarbeitet. Das konfigurierte Intervall beginnt auf jedem Client jeweils nach dem Start des AMC Agents. Da niemals alle Clients zeitgleich eingeschaltet werden, sind beispielsweise die geplanten Update-intervalle ebenfalls unterschiedlich.

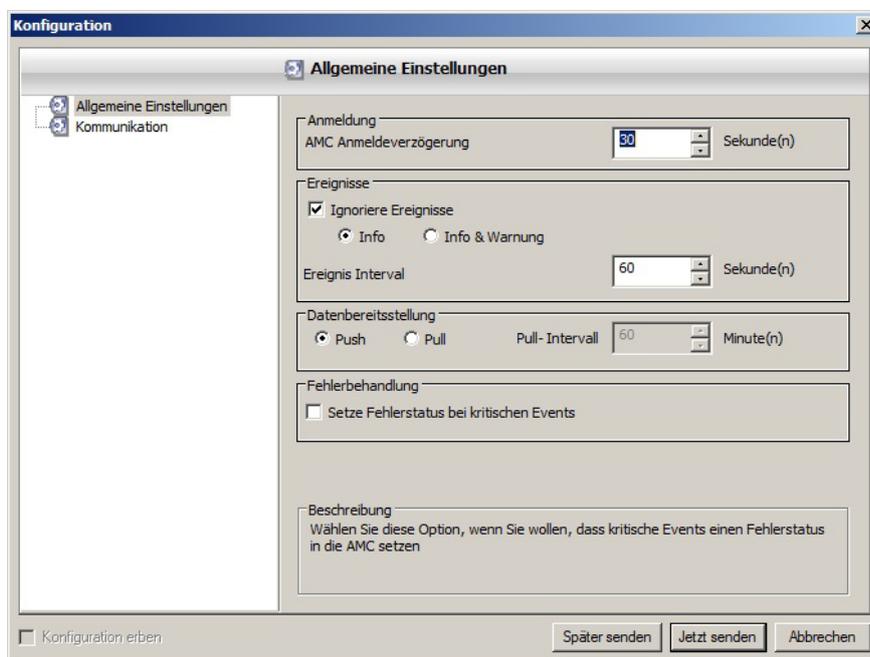
Über diese Variante wird zwar im Fall eines Updates die gleiche Datenmenge wie im „Push-Modus“ kopiert, jedoch verteilt über einen längeren Zeitraum (es entstehen keine „Stoßzeiten“).

Ein weiterer Vorteil des „Pull-Modus“ im Vergleich zum „Push-Modus“ ist, dass der AMC Agent im konfigurierten Intervall beim AMC Server nach Änderungen schaut. Sollte er keine Änderungen finden oder den AMC Server nicht erreichen, wird an der ursprünglichen Konfiguration bzw. den ursprünglichen Tasks festgehalten. Konfigurierte Update-Tasks werden beispielsweise auch unabhängig vom AMC Server durchgeführt.

Die Umstellung zwischen dem „Push-Modus“ und „Pull-Modus“ erfolgt in der Konfiguration des AMC Agent über das AMC Frontend und kann auf einzelnen PCs oder Gruppen innerhalb der „Sicherheitsumgebung“ unterschiedlich konfiguriert werden.

Um beispielsweise die komplette „Sicherheitsumgebung“ auf den „Pull-Modus“ umzustellen, müssen Sie mit der rechten Maustaste auf die „Sicherheitsumgebung“ klicken und *Konfiguration > AMC Agent > Konfigurieren* auswählen.

In der Konfiguration des AMC Agents ist unter dem Punkt „Datenbereitstellung“ standardmäßig „Push“ eingestellt, welches auf „Pull“ umkonfiguriert werden kann. Den entsprechenden Minuten-Intervall (Standardmäßig 60 Minuten), in dem sich der SMC Agent mit dem SMC Server abgleicht, lässt sich über „Pull-Intervall“ festlegen:



Die Konfigurationsänderung des AMC Agent wird über **Jetzt senden** auf den Clients übernommen.

Folgende Funktionen werden über den „Pull-Modus“ unterstützt:

- Produktinstallation /-deinstallation (Ausnahme AMC Agent)
- Produkt-Konfiguration
- Produkt-Kommandos
- Task Management
- Statusanzeige der Clients

Aus technischen Gründen basieren die weiteren Funktionen, wie das Abrufen und Anzeigen der Logdateien der Clients auf dem „Push-Modus“.

10. Filternde Gruppen

Um in einer AMC, in der eine große Anzahl von PCs verwaltet werden, einen schnellen Überblick über Rechner, die in irgendeiner Form die Aufmerksamkeit des Administrators erfordern, anzeigen zu lassen, besteht die Möglichkeit, diese nach bestimmten Kriterien zu filtern und das Ergebnis in einer oder mehreren speziellen virtuellen Gruppen (gefilterten Gruppen) darzustellen.

Folgende Filter können zur Erzeugung virtueller Gruppen verwendet werden:

1. Rechner, die einen Fehlerstatus melden
2. Rechner, die einen Produkt-Fehler-Status melden
 - 2.1. Modul veraltet
 - 2.2. Allgemeiner Modulfehler
3. Rechner, auf denen ein bestimmtes Produkt installiert bzw. nicht installiert ist
 - 3.1. Alle Produkte, die unter „Software Pakete“ eingebunden sind können ausgewählt werden
4. Suchen anhand eines Textfilters
 - 4.1. Es kann nach Computer, Gruppen und Hostname / IP Adressen gesucht werden
 - 4.2. Letzte Meldung des AMC Agent am AMC Server



Die folgenden Filteroptionen sind neu hinzugekommen:

1. die ein Produkt installiert oder nicht installiert haben (bisher konnte nur nach einem nicht installierten Produkt gefiltert werden)
2. deren Name oder Hostname einem gewählten Text entspricht
3. anhand der letzten Meldung

Eine „filternde Gruppe“ liefert eine bestimmte Sicht auf alle Clients, die dem eingestellten Filterkriterium entsprechen. Das heißt die Clients werden nicht permanent in diese Gruppe verschoben, sondern bleiben in ihrer ursprünglichen Gruppe.

Alle Aktionen, die für diesen Client in der filternden Gruppe ausgeführt werden, werden jedoch tatsächlich auf dem realen Client ausgeführt.

Beispiel:

Um eine „filternde Gruppe“, welche auf der „Sicherheitsumgebung“ Clients filtert, die beispielsweise keine Avira Professional Security installiert hat anzulegen, klicken Sie mit der rechten Maustaste auf „Sicherheitsumgebung“. Wählen Sie *Neu > Filternde Gruppe* aus.

Das folgende Fenster öffnet sich, in der Sie einen Namen für die neue „filternde Gruppe“ angeben können:



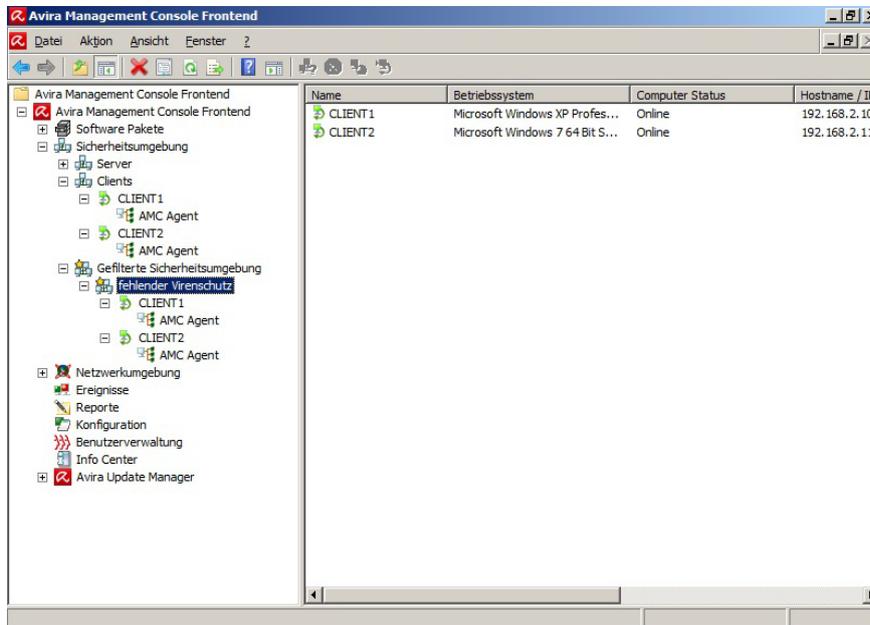
In diesem Fenster können Sie sich auch für eine der angebotenen „filternden Gruppen“ entscheiden (beispielsweise „Computer filtern die ein Produkt nicht installiert haben“).

Nachdem Sie auf **Weiter** geklickt haben öffnet sich das folgende Fenster. Hier haben Sie nun die Auswahl eines der unter „Software Pakete“ hinterlegten Produkte auszuwählen.



Im Beispielfall wurde das Produkt „Avira Professional Security (Windows), DE“ ausgewählt. Nachdem auf *Fertig stellen* geklickt wurde, wird innerhalb der „Sicherheitsumgebung“ die „filternde Gruppe“ mit der Bezeichnung „fehlender Virenschutz“ angelegt.

In dieser Gruppe taucht nun jeder Rechner der Sicherheitsumgebung auf, auf dem das Produkt „Avira Professional Security (Windows), DE“ nicht installiert ist:



Gezielt auf diese „gefilterten“ Clients kann nun beispielsweise die Avira Professional Security installiert werden.

Für weitere Details der „filternden Gruppen“ empfehlen wir Ihnen im Handbuch der AMC nachzuschlagen.

11. Windows Installation

11.1. Installation des AMC-Agents „unattended“

Alternativ kann die Installation des AMC-Agents natürlich manuell über den Aufruf der Installationsdatei oder unattended (z.B. im Anmeldeskript eingebunden) ausgeführt werden.

Auf dem AMC Server wurde folgendes Verzeichnis erstellt:

C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Avira\Avira Security Management Center Server\Agent

Geben Sie dieses Verzeichnis, falls nicht während der Installation der AMC geschehen, über die Windowsfreigabe mit Schreibrechten frei. Für eine „unattended“ Installation reicht es aus, die Datei „installagent.bat“ über die bestehende Verzeichnisfreigabe aufzurufen (`\\<IP-Adresse-SMC-Server>\<Freigabe(Agent)>\installagent.bat`).

Die *installagent.bat* ruft die eigentliche Installation (*setup.exe*) des AMC-Agents auf und verwendet die in der Datei „*installsmcagent.iss*“ hinterlegten AMC-Server-Informationen. Durch Anlegen einer entsprechenden Batchdatei (z.B. *uninstallagent.bat*) für die Deinstallation des AMC-Agents kann entsprechend die *uninstallsmcagent.iss* verwendet werden.

Clients, die vor der unattended AMC-Agent Installation noch nicht in der Sicherheitsumgebung eingebunden waren, werden in einer neuerscheinenden Gruppe „Neue Computer“ aufgelistet und können nachträglich per „Drag&Drop“ verschoben werden.

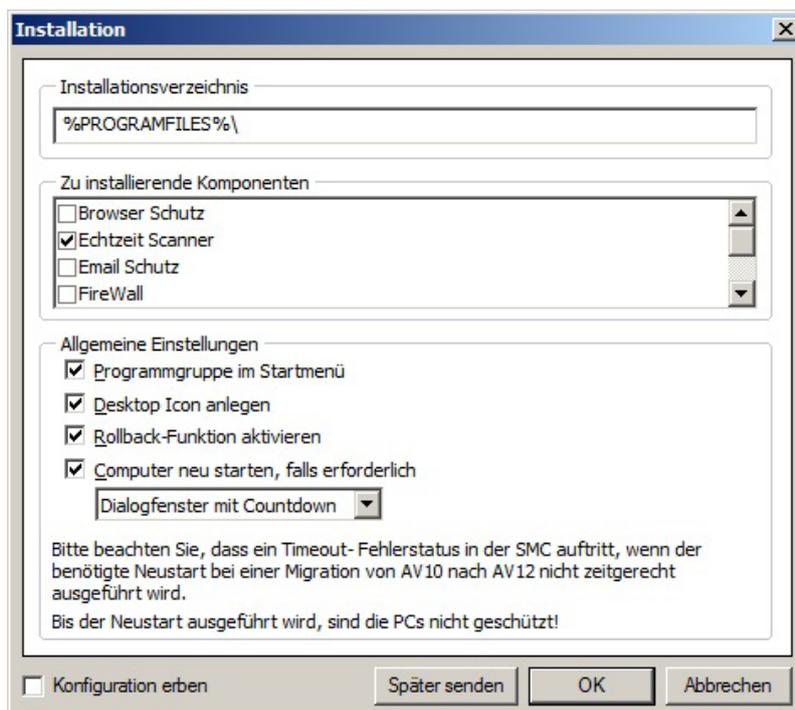
Es besteht ebenfalls die Möglichkeit, neue Rechner mithilfe ihrer IP-Adresse automatisch in bestehende Gruppen einzufügen. Dazu lassen sich als Eigenschaft einer Gruppe eine IP-Adresse oder IP-Adressbereiche festlegen. Sobald sich ein AMC-Agent zum ersten Mal am AMC-Server anmeldet, wird die AMC diesen Rechner automatisch in die Computergruppe einordnen in die er auf Grund seiner IP-Adresse gehört.

11.2. Installation der Avira Professional Security

Sämtliche in der AMC unter „Softwarepakete“ eingebundenen Avira Produkte können nun über die AMC auf den Clients installiert werden.

Dies geschieht, ähnlich wie bei der Installation des AMC-Agents, über einen Rechtsklick auf der gewünschten Gruppe und der Auswahl von *Installation > Avira Professional Security > Installieren*.

Das Fenster „Installation“ öffnet sich danach wie folgt und Sie können die zu installierenden Komponenten sowie den Zielpfad wählen:



Hierbei können Sie für die komplette Sicherheitsumgebung oder für einzelne Computergruppen eine Installationskonfiguration definieren, welche über den Haken bei „Konfiguration erben“ dann an alle Computer unterhalb dieser Gruppe vererbt wird. Entfernt man diesen Haken, können individuell Komponenten hinzugefügt oder entfernt werden, abweichend der Standardkonfiguration.

Sind Clients mit bereits installiertem AMC-Agent während des Installations-kommandos ausgeschaltet, wird eine ausstehende Aktion angelegt. Das heißt, dass diese Aktion (in diesem Fall die Installation) nachgeholt wird, sobald sich der AMC-Agent am AMC-Server anmeldet.

Ausstehende Aktionen werden mit einem roten Dreieck, rechts neben dem Client angezeigt, dargestellt: 

- Werden Clients mit einem „roten Ausrufezeichen (!)“ ( /  / ) dargestellt, bedeutet dies, dass mit dem Status des installierten Produktes etwas nicht in Ordnung ist.
- Sind Clients Gruppen zugeordnet, die nicht erweitert angezeigt werden, wird das evtl. angezeigte „rote Ausrufezeichen (!)“ nicht erkannt. In diesem Fall zeigt das „roteingefärbte Gruppensymbol“ darauf hin: 

Der Fehlerstatus (Ursache der „roten Ausrufezeichen (!)“) lässt sich ermitteln, indem mit einem Rechtsklick auf den Client geklickt wird und *Ansicht > Produktstatus* ausgewählt wird.

In diesem Fall ist zu erkennen, dass der „Update Status“ veraltet ist. Ebenfalls hätte ein nicht gestarteter „Avira Echtzeit-Scanner“, „Avira Wmail-Schutz“ (POP3/SMTP-Scanner), der „Avira Planer“ oder der „Avira Browser-Schutz“ einen Fehlerstatus („rotes Ausrufezeichen !“) hervorrufen können:

Modulname	Modul Fehlerstatus	Modul Status
 Echtzeit Scanner	Ok	Aktiviert
 Planer	Ok	Aktiviert
 Email Schutz	Ok	Aktiviert
 Browser Schutz	Ok	Aktiviert
 FireWall	Ok	Aktiviert
 Update Status	Ok	Nicht verfügbar

Hinweis

Das Zurücksetzen der Statusmeldungen, die über das „rote Ausrufezeichen!“ dargestellt werden, kann nur dadurch erfolgen, dass die Ursache der Fehlermeldung behoben wird.

In unserem Fall würde dies, nachdem ein Update auf den betroffenen Clients durchgeführt wurde, automatisch zurückgesetzt werden (kurze Zeitdifferenz von bis 1 Minute möglich).

Hinweis

Modul Status – „Nicht verfügbar“, bedeutet, dass der Updateprozess kein Modul hat. „Nicht verfügbar“ ist also zutreffend, somit kein Fehler.

Ausschlaggebend ist der „Modul Fehlerstatus“. Hier sollte im Idealfall „OK“ stehen. Im Fall eines Fehlers, z.B. bei der Installation des Avira AMC-Agents oder eines anderen Avira Produktes, kann es sein, dass ein rotes Stoppsymbol erscheint.

Die aufgetretene Fehlermeldung kann, wie die Statusmeldung („rotes Ausrufezeichen“) über einen Rechtsklick auf den Client und die Auswahl von *Ansichten > Fehlermeldungen* angezeigt werden.

Achten Sie bei „Stoppsymbolen“ darauf, mit welcher Farbe dies dargestellt wird!



= Fehlermeldung
= Warnung/Hinweis

Stoppmeldungen werden nicht automatisch zurückgesetzt, sondern bleiben, selbst wenn die Ursache der Stoppmeldung bereits beseitigt wurde, bestehen und müssen über einen Rechtsklick auf „Fehlerstatus rücksetzen“ zurückgesetzt werden.

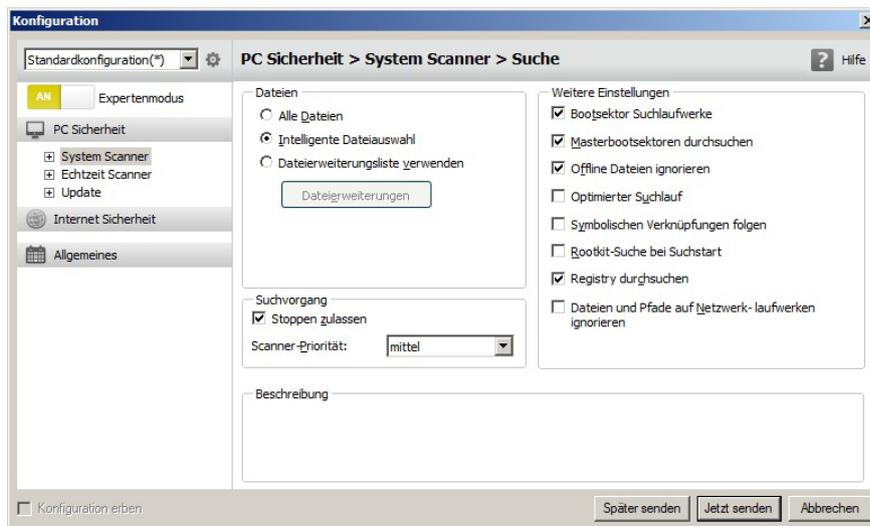
11.3. Konfiguration von Avira Professional Security

Über die AMC sind nahezu alle Funktionen der Konfiguration verfügbar, die Sie auch lokal am Client einstellen können.

Um in die Konfiguration von Avira Professional Security zu kommen, führen Sie einen Rechtsklick auf die zu konfigurierende Gruppe und wählen Konfiguration > AVIRA Professional Security (Windows).DE“ > „Konfigurieren“ aus.

Die Konfiguration von Avira Professional Security öffnet sich, in der Sie Änderungen, ähnlich der lokalen Konfiguration am Client, vornehmen können.

Seit der Version 10 von AntiVir Professional wurden nun Gui-Plugins integriert, welche das Design der Konfigurationsoberfläche innerhalb der AMC nahezu identisch mit jener des Clients erscheinen lassen. Sie sehen also mit Avira Professional Security dieselben Menüpunkte, wie Sie sie auch auf dem lokalen Client vorfinden:



Die Updatekonfiguration finden Sie in der jeweiligen Konfiguration der Clients unter dem Reiter „Allgemeines“ und dem Unterpunkt „Update“.

Ändern Sie hier die Konfiguration, um zum Beispiel zentrale Updates durchführen zu können.

Wählen Sie je nach Wunsch das Updateverfahren „über Webserver“ oder „über Dateiserver/Freigegebene Verzeichnisse“ aus.

Bei der Auswahl von „über Webserver“ ist zu beachten, dass die Clients nicht zwangsläufig die Updates über das Internet laden. Vielmehr sollte hier die Verwendung des http-Protokolls verstanden werden. Also ein Update generell über einen Webserver, der aber selbstverständlich auch im lokalen Netzwerk (kein Internet) stehen kann.

Ab der AMC Version 2.0 ist der Internet Update Manager integriert und beinhaltet einen Webserver, welcher auf Port 7080 läuft. Beachten Sie hierbei spezielle Einzelheiten aus dem Handbuch der aktuellen AMC.

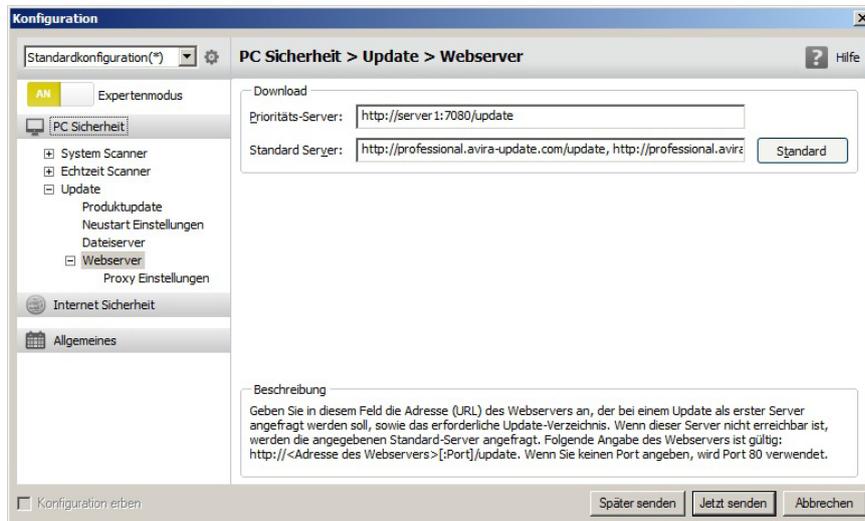
Folgende Vorteile haben Sie, wenn das Update über http durchgeführt wird:

- Es können mehrere Updateserver angegeben werden, sollte der primäre Updateserver nicht erreichbar sein, wird auf den konfigurierten Standardserver ausgewichen.

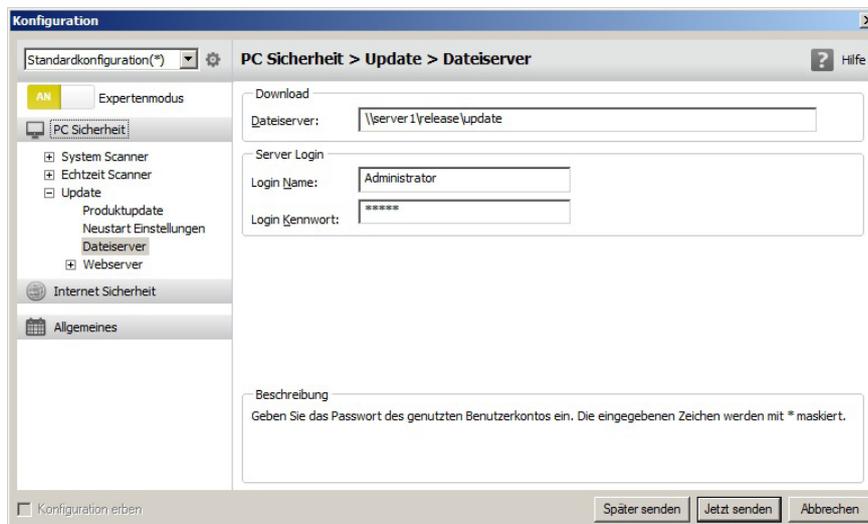
So kann für die Konfiguration eines Laptops z.B. als erster Updateserver der netzinterne Webserver festgelegt und als zweiter der Internetupdateserver von AVIRA definiert werden. Wird der Laptop einmal nicht im Firmennetz betrieben (zu Hause, Hotel, Außendienst, ...), kann somit trotzdem sichergestellt werden, dass Updates durchgeführt werden können.

- Es ist nicht notwendig, sich um die Authentifizierung der Freigabe zu kümmern, bzw. diese zu pflegen. Sie wird bei der Verwendung von „via Freigabe/Share“ benötigt.

Die Konfiguration des Updates „über Webserver“ könnte bei der Verwendung von Avira Professional Security wie folgt aussehen:



Die Konfiguration des Updates „über Dateiserver/Freigegebene Verzeichnisse“ als Alternative wie folgt:



Bei der Updatevariante „über Dateiserver/Freigegebene Verzeichnisse“ darf nicht vergessen werden, das Zielverzeichnis „HttpRoot“ (Wurzelverzeichnis für aktualisierte Dateien) des Internet Update Managers über das Dateisystem freizugeben (Lese-rechte sind hierbei ausreichend).

Dieses Verzeichnis liegt standardmäßig unter:

C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Avira\Avira Internet Update Manager\HttpRoot

Ebenso sollten die Felder „Server Login Name“ und „Server Login Kennwort“ konfiguriert werden, damit der Updater auch dann Updates laden kann, wenn die Benutzeranmeldung am Client selbst noch nicht stattgefunden hat.

Nachdem Sie sich für eine Updatevariante entschieden und diese konfiguriert haben, wird sie über einen Klick auf „Jetzt senden“ an die Clients geschickt.

Für Clients, die zum Zeitpunkt der Konfigurationsübermittlung über die AMC ausgeschaltet sind, wird eine „ausstehende Aktion“ angelegt.

Die „ausstehende Aktion“ wird nachgeholt, sobald der Client eingeschaltet ist und der AMC-Agent sich am AMC-Server registriert hat.

11.4. Planen- bzw. Ausführen von Updates / Suchläufen

Um über die AMC ein Update- bzw. Suchlaufkommando durchzuführen, muss in der AMC mit einem Rechtsklick auf die gewünschte Gruppe und anschließend auf *Kommandos > Avira Professional Security > Update starten / Suche* geklickt werden.

Im sich öffnenden Fenster und der Auswahl von „Kommando periodisch ausführen“ lassen sich Updates oder Suchläufe automatisiert zu geplanten Zeitpunkten oder Intervallen ausführen.

Wird die Schaltfläche „Kommando periodisch ausführen“ nicht angeklickt, sondern sofort auf **OK** geklickt, wird ein Update oder Suchlauf (je nach Kommandotyp) sofort ausgeführt.

Die beiden Kommandos „Update“ oder „Suchlauf“ unterscheiden sich von der Ausführung nur unwesentlich. Der Unterschied besteht in den unterschiedlichen Ausführungsmöglichkeiten. Daher wird auf eine detaillierte Ausführung des Kommandos „Suche“ verzichtet. Weitere Details hierzu sind im Handbuch zu finden.

11.5. Installation der Avira Server Security

Der Avira Server Security muss wie Avira Professional Security unter „Softwarepakete“ eingebunden sein, um über die AMC installiert bzw. konfiguriert zu werden.

Der Installationsvorgang ist ähnlich wie bei Avira Professional Security und wird daher nicht detaillierter erklärt. Für weitere Informationen der Avira Server Security Installation schlagen Sie bitte im Handbuch nach.

11.6. Konfiguration des Avira Server Security

Über die AMC sind nahezu alle Funktionen der Konfiguration verfügbar, die Sie auch lokal am Avira Server Security einstellen können.

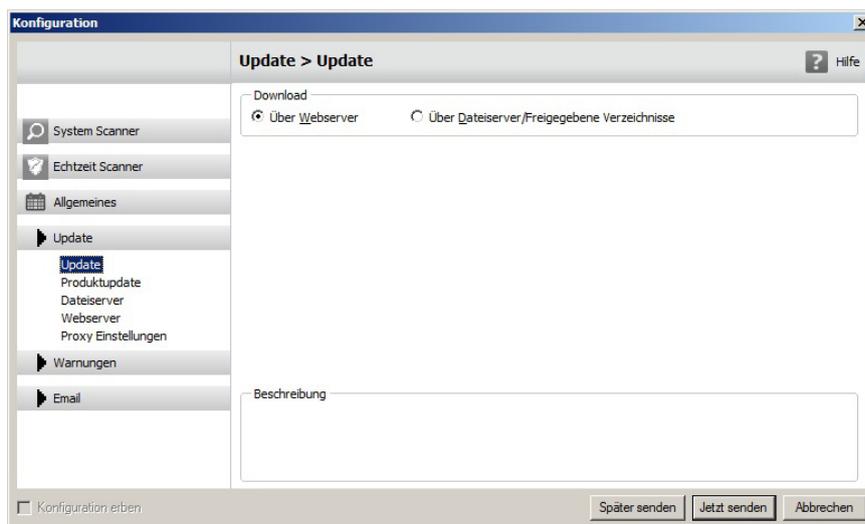
In die Konfiguration des Avira Server Security gelangen Sie über die AMC, über einen Rechtsklick auf die zu konfigurierende Gruppe wählen Sie *Konfiguration > Avira Server Security > Konfigurieren* aus.

Die Konfiguration des Avira Server Security öffnet sich. Hier können Sie Änderungen, ähnlich der lokalen Konfiguration am Avira Server Security selbst, vornehmen.

Die Updatekonfiguration finden Sie unter dem Reiter „Update“.

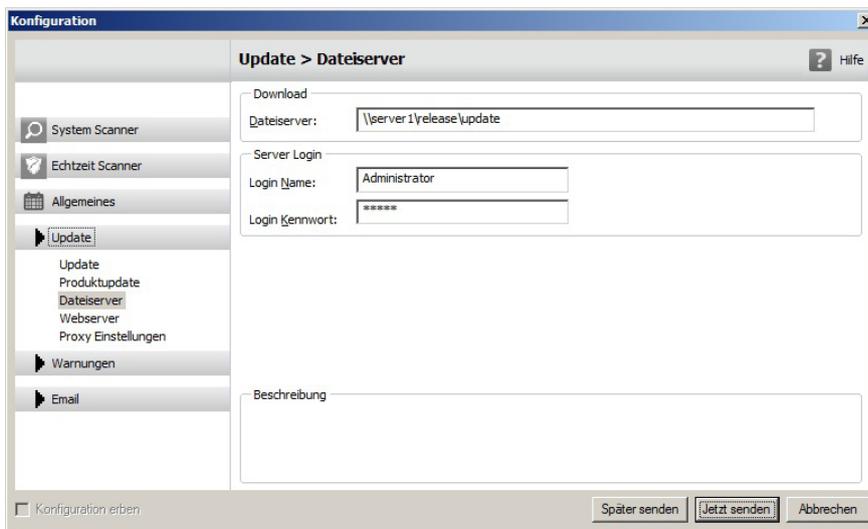
Ändern Sie hier die Konfiguration, um zum Beispiel zentrale Updates durchführen zu können. Wählen Sie je nach Wunsch das Updateverfahren „über Webserver“ oder „über Dateiserver/Freigegebene Verzeichnisse“ aus.

Je nachdem, für welche Art Update Sie sich entschieden haben, muss der Updatepfad entsprechend angepasst werden:

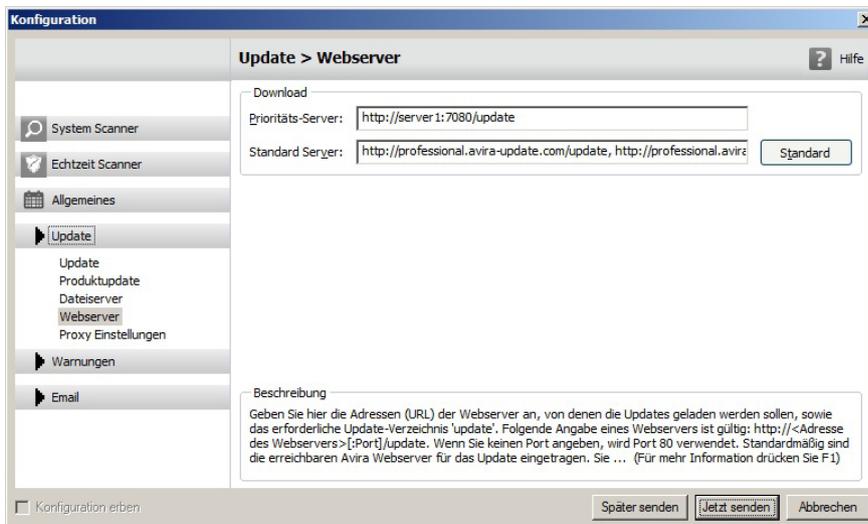


Im Fall, dass das Update „über Dateiserver/Freigegebene Verzeichnisse“ geladen werden soll, darf man ebenfalls nicht vergessen, das Zielverzeichnis „HttpRoot“ des Internet Update Managers über das Dateisystem freizugeben (Leserechte sind hierbei ausreichend).

Ebenfalls sollten die Felder „Server Login Name“ und „Server Login Kennwort“ konfiguriert werden, damit der Updater auch dann Updates laden kann, wenn die Benutzeranmeldung am Windows Server selbst noch nicht stattgefunden hat, bzw. der angemeldete Windowsbenutzer keine Zugriffsrechte auf das Updateverzeichnis hat.

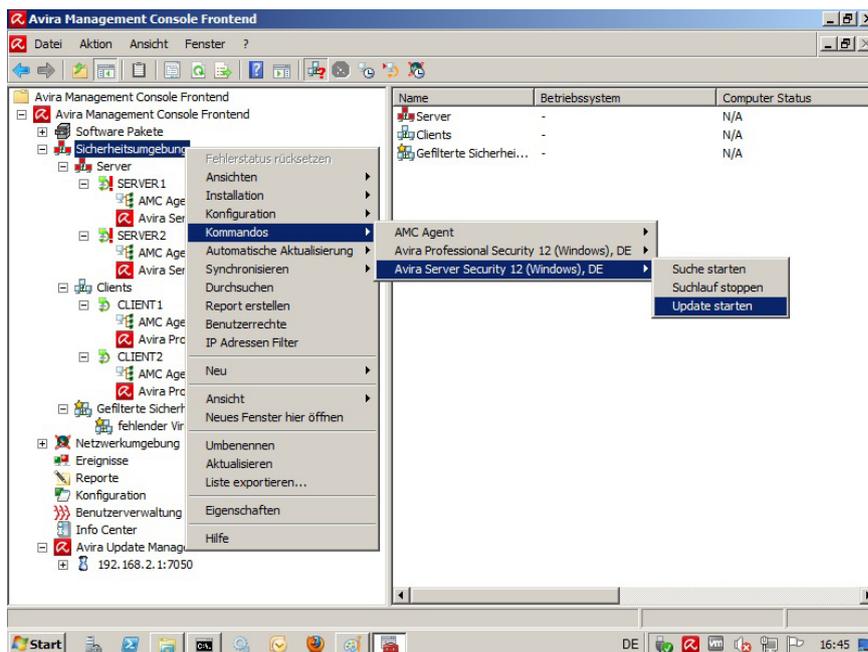


Ein Update über den im Avira Update Manager bereitgestellten Webserver ist selbstverständlich ebenfalls möglich. Hierbei wird das standardmäßig konfigurierte Internetupdate so geändert, dass nicht *http://dl.antivir.de/update* als Updatequelle verwendet wird, sondern entsprechend der Webserver des Avira Update Managers angesprochen wird.



11.7. Planen- bzw. Ausführen von Update u. Suchläufen

Um über die AMC ein Update- bzw. Suchlaufkommando durchzuführen, muss in der AMC mit einem Rechtsklick auf die gewünschte Gruppe und anschließend auf *Kommandos > Avira Server Security > Update starten / Suche starten* geklickt werden:



Da das Planen der Updates bzw. Suchläufe denen von Avira Professional Security ähnelt und dies bereits beschrieben wurden, wird an dieser Stelle auf die Beschreibung verzichtet.

Weitere Details hierzu sind im Handbuch zu finden.

11.8. Konfiguration rücksetzen/vererben:

Wird eine Konfiguration auf der „Sicherheitsumgebung“ für ein Produkt geändert, wird diese auf alle PCs in der „Sicherheitsumgebung“ bzw. in den angelegten Untergruppen vererbt.

Ausnahme:

Wurde bereits eine Untergruppe/PC separat in einer speziellen Form einzeln konfiguriert, indem die Option „Konfiguration erben“ deaktiviert wurde, behält diese Gruppe/PC ihre Konfiguration und nimmt die übergeordnete Konfiguration nicht an.

Um zu erreichen, dass Untergruppen bzw. PCs die jeweils übergeordnete Konfiguration vererbt bekommen, muss die spezifisch eingerichtete Konfiguration einer Untergruppe/PC zurückgesetzt werden (*Konfiguration > Avira Professional Security > Alles zurücksetzen*).

Beispiel:

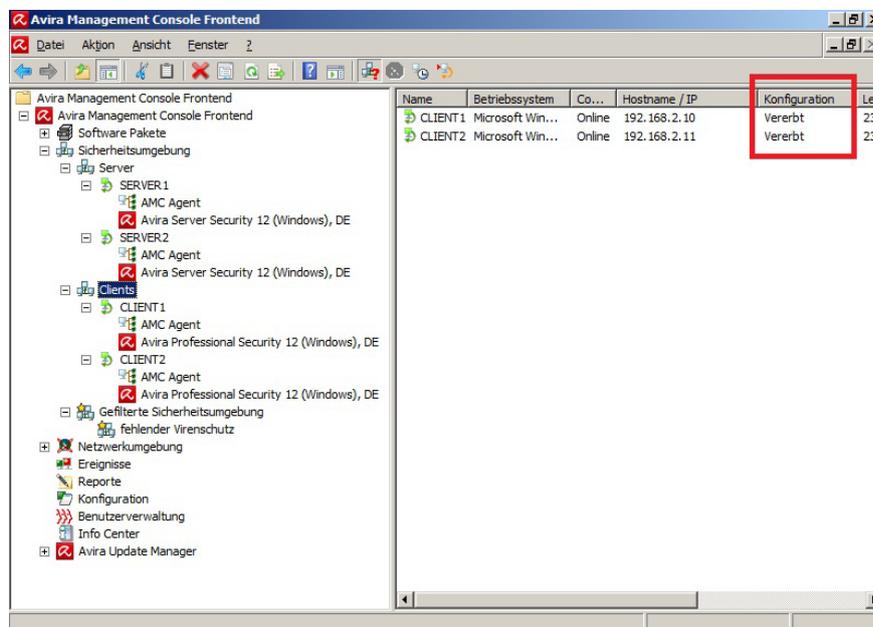
Bei der Untergruppe „Clients“ wurde der Haken bei „Konfiguration erben“ deaktiviert und sie wurde so konfiguriert, dass der „Expertenmodus“ nicht angezeigt wird. Über die übergeordnete Gruppe „Sicherheitsumgebung“ wurde anschließend konfiguriert, dass der „Expertenmodus“ angezeigt werden soll.

Die Gruppe „Clients“ übernimmt diese Konfigurationsänderung nicht, da hier eine spezifische Konfiguration erfolgt ist.

Damit die Konfiguration der „Sicherheitsumgebung“ vererbt (übernommen) wird, muss die Konfiguration der Gruppe „Clients“ zurückgesetzt werden. Dies erfolgt über einen Klick mit der rechten Maustaste auf die Gruppe „Clients“ und der Auswahl *Konfiguration > Avira Professional Security > Alles zurücksetzen*.

Um zu erkennen, welche Gruppen bzw. PCs eine vererbte oder spezifische Konfiguration haben, klicken Sie je die übergeordnete Gruppe (z.B. die „Sicherheitsumgebung“) an.

In der rechten Hälfte des Security Management Center Frontends lässt sich ablesen, ob die Konfiguration „Spezifisch“ oder „Vererbt“ ist:



11.9. Produktupdate der SMC 2.6/AMC 2.6.1 auf AMC 2.7

Direkte Aktualisierung:

1. Klicken Sie mit der rechten Maustaste auf „Security Management Center Frontend“, und wählen Sie *Update*.
2. Wählen Sie *Server/Update starten*, um den Server zu aktualisieren.

oder

Wählen Sie *Frontend*, um das Frontend zu aktualisieren.

Die folgende Meldung wird angezeigt bei einer Aktualisierung des SMC-Servers:



Bei einer Aktualisierung des SMC-Frontend:



Klicken Sie zur Bestätigung auf **Ja**, und schließen Sie ggf. das SMC-Frontend. Die Verbindung zum AMC-Server wird unterbrochen.

Avira AMC stellt eine Verbindung zum Avira Update Manager her, welcher die Aktualisierungen des Produktes zur Verfügung stellt.

Starten Sie das AMC-Frontend neu, und melden Sie sich wieder beim AMC Server an.

Aktualisieren von SMC-Agents:

Es wird empfohlen, SMC-Agents automatisch über den Avira Update Manager zu aktualisieren (Standardeinstellung).

So aktualisieren Sie SMC-Agents im gesamten Netzwerk oder in einer bestimmten Gruppe:

Klicken Sie mit der rechten Maustaste auf den Knoten „Sicherheitsumgebung“ oder auf den Knoten der Gruppe, und wählen Sie *Kommandos > Avira AMC Agent > Aktualisierung Starten*.

So aktualisieren Sie SMC-Agents auf einem bestimmten Computer:

Klicken Sie mit der rechten Maustaste in der Sicherheitsumgebung unter dem Knoten des Computers auf „Avira AMC Agent“, und wählen Sie *Kommandos > Aktualisierung Starten*.

Sie können die Aktualisierung von SMC-Agents auch zeitlich planen. Klicken Sie im Fenster „Kommandos“ auf die Schaltfläche *Kommando periodisch ausführen*.

12. Automatische Produktinstallation

Seit der SMC 2.5 gibt es die Möglichkeit, eine automatische Produktinstallation zu definieren. Somit wird auf Rechnern, die in eine bestimmte Gruppe verschoben werden, automatisch das definierte Produkt installiert bzw. deinstalliert.

Klicken Sie dafür mit der rechten Maustaste auf eine Gruppe, Menüpunkt *Installation* > *Produkte*. Anschließend können Sie die Softwarepakete auswählen:



13. Automatische Synchronisierung mit ADS/LDAP

Die bisherige Möglichkeit, die AMC-Sicherheitsumgebung mit dem ADS bzw. LDAP zu synchronisieren, wurde erweitert. Nun kann man diesen Vorgang via Planer erledigen lassen.

Klicken Sie mit der rechten Maustaste auf die Sicherheitsumgebung und wählen „Synchronisierung planen“. Hier werden Sie wie gewohnt gefragt, wie die Synchronisierung ablaufen soll.

Abschließend legen Sie einen Task an, der die Synchronisierung in Zukunft automatisch erledigt.

14. Mehrere Avira Update Manager (AUM) über AMC-Frontend verwalten

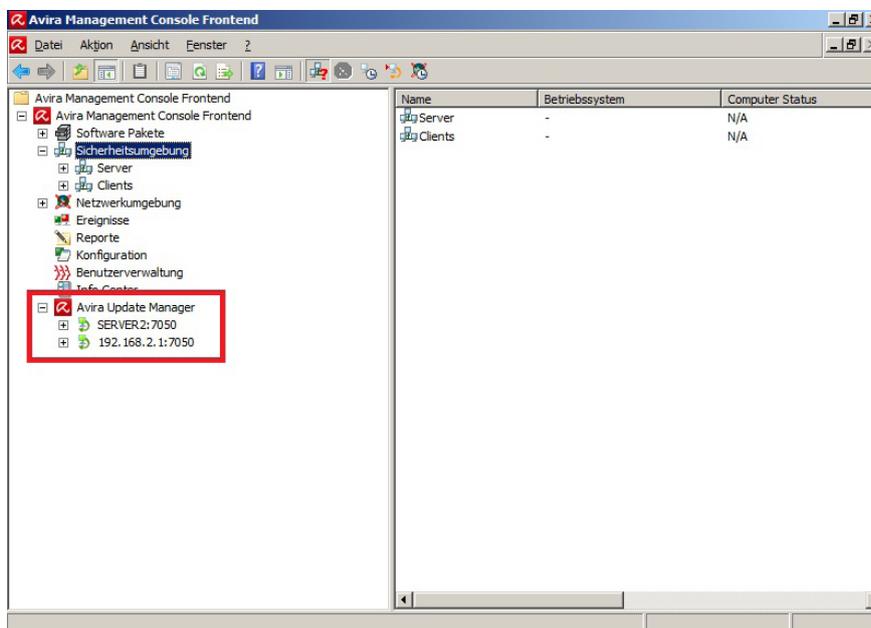
Haben Sie mehrere Standalone-AUMs (z.B. pro Standort), musste man diese bisher mit einem separaten AUM-Frontend administrieren.

Das hat sich seit SMC 2.5 geändert. Hier können Sie mehrere AUM-Server im AMC-Frontend verwalten.

Einen neuen AUM fügen Sie wie folgt ein:

Rechte Maustaste auf *Avira Update Manager > Neu > AUM Server* hinzufügen.

Nachdem der bzw. die AUM Server im AMC-Frontend hinzugefügt worden sind, wird automatisch eine Produktsynchronisation durchgeführt.



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, ...“

Type	Message
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 available for download.
Update Successful new files	Update from "Download Server, File1: Version1,..." has been performed successfully.
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".
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 context 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 [Message]"

15.3 Level Warning

Type	Message
Unauthorized Configuration Change	The configuration has been changed without 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"

Type	Message
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".
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. Generelle Hinweise/Informationen

INFO-Bubbles:

Beim Überfahren von Konfigurationsflächen in der AMC mit dem Mauszeiger erscheinen gelbe Kurzinformatioensfenster, in denen hilfreiche Tipps angezeigt werden.

Symbole der AMC:

In der AMC können verschiedene Symbole erscheinen, die im Folgenden in Kurzform aufgelistet und erklärt werden:

	=	Fehlermeldung
	=	Warnung/Hinweis
	=	Client ist eingeschalten, Agent installiert, Kommunikation hergestellt
	=	Produkt Status prüfen
	=	Client ist ausgeschaltet/nicht erreichbar, Agent ist nicht installiert
	=	Client ist ausgeschaltet/nicht erreichbar, Agent ist installiert
	=	Client ist ausgeschaltet, Agent ist installiert, Ausstehende Aktion
	=	Client ist eingeschaltet, kein Agent installiert
	=	PC eingeschaltet, Agent installiert aber nicht erreichbar
	=	Sanduhr, Client stellt Verbindung zum AMC-Server her oder ist mit Kommandos der AMC beschäftigt
	=	Symbol des auf dem Client installierten Agents
	=	gültiges Softwarepaket ohne hinterlegter Lizenzdatei „hbedv.key“
	=	gültiges Softwarepaket mit hinterlegter Lizenzdatei „hbedv.key“
	=	Softwarepaket auf dem Client installiert

ID DER SOFTWAREPAKETE:

Sollte Ihnen die Meldung „Fehlendes Softwarepaket mit ID XX“ angezeigt werden, so ist dies nicht oder in einer veralteten bzw. fehlerhaften Version unter „Software Pakete“ eingebunden:

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 deutsch
501	=	AntiVir Professional 10 englisch
502	=	AntiVir Professional 10 russisch
503	=	AntiVir Professional 10 spanisch
504	=	AntiVir Professional 10 italienisch
505	=	AntiVir Professional 10 französisch
600	=	AntiVir Server 10 deutsch
601	=	AntiVir Server 10 englisch
602	=	AntiVir Server 10 russisch
603	=	AntiVir Server 10 spanisch
604	=	AntiVir Server 10 italienisch
605	=	AntiVir Server 10 französisch
700	=	Avira Professional Security 12 deutsch
701	=	Avira Professional Security 12 englisch
702	=	Avira Professional Security 12 russisch
703	=	Avira Professional Security 12 spanisch
704	=	Avira Professional Security 12 italienisch
705	=	Avira Professional Security 12 französisch
706	=	Avira Professional Security 12 portugiesisch (Brasilien)
707	=	Avira Professional Security 12 chinesisch (vereinfacht)
708	=	Avira Professional Security 12 japanisch
709	=	Avira Professional Security 12 koreanisch
710	=	Avira Professional Security 12 rumänisch
711	=	Avira Professional Security 12 chinesisch (traditionell)
712	=	Avira Professional Security 12 türkisch
713	=	Avira Professional Security 12 niederländisch
750	=	Avira Server Security 12 deutsch
751	=	Avira Server Security 12 englisch
752	=	Avira Server Security 12 russisch
753	=	Avira Server Security 12 spanisch

754	=	Avira Server Security 12 italienisch
755	=	Avira Server Security 12 französisch
756	=	Avira Server Security 12 portugiesisch (Brasilien)
757	=	Avira Server Security 12 chinesisch (vereinfacht)
758	=	Avira Server Security 12 japanisch
759	=	Avira Server Security 12 koreanisch
760	=	Avira Server Security 12 rumänisch
761	=	Avira Server Security 12 chinesisch (traditionell)
762	=	Avira Server Security 12 türkisch
763	=	Avira Server Security 12 niederländisch
800	=	Avira Professional Security 13 deutsch
801	=	Avira Professional Security 13 englisch
802	=	Avira Professional Security 13 russisch
803	=	Avira Professional Security 13 spanisch
804	=	Avira Professional Security 13 italienisch
805	=	Avira Professional Security 13 französisch
806	=	Avira Professional Security 13 portugiesisch (Brasilien)
807	=	Avira Professional Security 13 chinesisch (vereinfacht)
808	=	Avira Professional Security 13 japanisch
809	=	Avira Professional Security 13 koreanisch
810	=	Avira Professional Security 13 rumänisch
811	=	Avira Professional Security 13 chinesisch (traditionell)
812	=	Avira Professional Security 13 türkisch
813	=	Avira Professional Security 13 niederländisch
850	=	Avira Server Security 13 deutsch
851	=	Avira Server Security 13 englisch
858	=	Avira Server Security 13 japanisch

16. UNIX

16.1. Manuelle Installation des AMC-Agents für UNIX

Sie können den AMC-Agent bei Bedarf auch manuell installieren.

Das dafür benötigte Produktpaket

AntiVir_Security_Management_Center_UNIX_Agent.tgz

ist im Installationspaket der Avira Management Console (AMC) enthalten und kann über unsere [Avira](#) Webseite bezogen werden.

Das Installationspaket kann wie folgt extrahiert werden:

```
unzip avira_management_console_de.zip
```

Entpacken Sie das Agent-Paket:

```
tar xzf Avira_Management_Console_Unix_Agent.tgz
```

Wechseln Sie in das Installationsverzeichnis:

```
cd Avira_Management_Console_Unix_Agent
```

Installieren Sie den AMC-Agent:

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

Die IP-Adresse und des Servers und der AMC Anzeigename müssen zwingend angegeben werden. Die Angabe des Server Ports ist optional und muss nur vorgenommen werden, wenn der AMC Server nicht die Default Ports für die Kommunikation mit dem AMC Agent verwendet.

16.2. Installation und Konfiguration von Avira AntiVir UNIX Professional/Server

Der AvGuard kann über die AMC nur dann benutzt werden, wenn das Dazuko Modul bzw. DazukoFS mit Hilfe des Befehls `modprobe` automatisch geladen werden kann oder bereits geladen ist. Details zum Übersetzen und Installieren von Dazuko finden Sie in der HowTo auf der [dazuko](#) Webseite.

Sofern kein Dazuko / DazuoFS verwendet wird, muss das OnAccess Management ausgeschaltet werden. Um dies zu deaktivieren, muss der Parameter `OnAccessManagement` von „auto“ auf „no“ umgestellt werden. Damit wird auch die Warnung im AMC gelöscht.

Bevor mit der Installation begonnen werden kann, muss das Produktpaket für Avira AntiVir UNIX Professional bzw. Avira AntiVir UNIX Server zu den Software Paketen der AMC hinzugefügt werden und eine Lizenz hinterlegt werden.

Das Paket heißt „`antivir-workstation-prof.tar.gz`“ bzw. `antivir-server-prof.tar.gz`. Die Pakete können von der [Avira](#) Webseite heruntergeladen werden.

Um die Installation von Avira AntiVir UNIX Professional/Server zu starten, klicken Sie im Navigationsbereich auf den Knoten „Sicherheitsumgebung“ und ggf. darunter auf die Gruppe/den Rechner, in der/auf dem die AntiVir UNIX Professional/Server installiert werden soll.

Klicken Sie mit der rechten Maustaste auf die Gruppe bzw. den Rechner und wählen dann „Installation/Avira AntiVir Workstation/Server (UNIX)/Installieren“. Das Dialogfenster „Installation“ erscheint und muss mit **OK** bestätigt werden.

Der AvGuard wird automatisch beim Booten gestartet, ist nach der Installation jedoch nicht gestartet. Dies wird an der AMC mit den „Produkt Status prüfen“ Symbolen dargestellt.

Zum Starten des AvGuard klicken Sie mit der rechten Maustaste auf die Gruppe bzw. den Rechner und wählen dann *Kommandos > Avira AntiVir Professional > Server (UNIX) > Start*.

Kann der Guard nicht gestartet werden und der Fehlerstatus bleibt dauerhaft erhalten, fehlt eventuell Dazuko auf dem System oder ist noch nicht geladen worden.

Standardmäßig wird bei einer Installation über die AMC das Verzeichnis */home* vom AvGuard überwacht. Welche Verzeichnisse überwacht werden sollen, können Sie in dem Reiter „Basic Settings“ der Konfiguration ändern. Dazu klicken Sie mit der rechten Maustaste auf die Gruppe bzw. den Rechner und wählen daraufhin „Konfiguration/Avira AntiVir Professional/Server (UNIX)/konfigurieren“. Wir empfehlen nur einzelne, wichtige Verzeichnisse (in der Regel Freigaben) zu überwachen.

Details zur Konfiguration für Avira AntiVir UNIX Professional/Server finden Sie in dem Benutzerhandbuch für Avira AntiVir UNIX Server (Kapitel 4 Konfiguration).

16.3. Installation und Konfiguration von Avira AntiVir UNIX Web-Gate

Bevor mit der Installation begonnen werden kann, muss das Produktpaket für Avira AntiVir UNIX WebGate zu den Software Paketen der AMC hinzugefügt werden und eine Lizenz hinterlegt werden. Das Paket heißt *antivir-webgate-prof.tar.gz*. Das Paket kann von der [Avira](#) Webseite heruntergeladen werden.

Um die Installation von Avira AntiVir UNIX WebGate zu starten, klicken Sie im Navigationsbereich auf den Knoten „Sicherheitsumgebung“ und gegebenenfalls darunter auf die Gruppe bzw. den Rechner wo Avira AntiVir UNIX WebGate installiert werden soll.

Klicken Sie mit der rechten Maustaste auf die Gruppe bzw. den Rechner und wählen dann *Installation > Avira AntiVir WebGate (UNIX) > Installieren*. Das Dialogfenster Installation erscheint und muss mit **OK** bestätigt werden.

WebGate wird automatisch beim Booten gestartet, ist nach der Installation jedoch nicht gestartet. Dies wird an der AMC mit den „Produkt Status prüfen“ Symbolen dargestellt. Zum Starten von WebGate klicken Sie mit der rechten Maustaste auf die Gruppe/den Rechner und wählen *Kommandos > Avira AntiVir WebGate (UNIX) > Start*.

Um Änderungen in der Konfiguration vorzunehmen, klicken Sie mit der rechten Maustaste auf die Gruppe bzw. den Rechner und wählen *Konfiguration > Avira AntiVir Webgate (UNIX) > konfigurieren*.

Details zur Konfiguration entnehmen Sie bitte dem Benutzerhandbuch für Avira AntiVir UNIX WebGate (Kapitel 4 Konfiguration).

16.4. Installation und Konfiguration von Avira AntiVir UNIX MailGate

Bevor mit der Installation begonnen werden kann, muss das Produktpaket für Avira AntiVir UNIX MailGate zu den Software Paketen der SMC hinzugefügt werden und eine Lizenz hinterlegt werden. Das Paket heißt `antivir-mailgate-prof.tar.gz`. Das Paket kann von der [Avira](#) Webseite heruntergeladen werden.

Bei einer Installation über die AMC kann nur die Konfiguration von MailGate vorgenommen werden. Die Konfiguration des MTA (z.B. Postfix) kann nicht über die SMC erfolgen.

Um die Installation von Avira AntiVir UNIX MailGate zu starten, klicken Sie im Navigationsbereich auf den Knoten Sicherheitsumgebung und ggf. darunter auf die Gruppe/den Rechner, in der/auf dem Avira AntiVir UNIX MailGate installiert werden soll. Klicken Sie mit der rechten Maustaste auf die Gruppe/den Rechner und wählen Sie Installation/Avira AntiVir MailGate (UNIX)/Installieren. Das Dialogfenster Installation erscheint und muss mit **OK** bestätigt werden.

MailGate und der verwendete MTA müssen nun konfiguriert werden. Bitte entnehmen Sie die notwendigen Konfigurationseinstellungen dem Benutzerhandbuch Avira AntiVir MailGate UNIX (Kapitel 4.4 Weiter Installationschritte in Abhängigkeit vom MTA).

Um die beschriebenen Änderungen in der Konfiguration vorzunehmen, klicken Sie mit der rechten Maustaste auf die Gruppe/den Rechner und wählen Sie Konfiguration/Avira AntiVir MailGate (UNIX)/konfigurieren.

Weitere Details zur Konfiguration entnehmen Sie bitte dem Benutzerhandbuch für Avira AntiVir UNIX MailGate (Kapitel 6 Konfiguration).

MailGate wird automatisch beim Booten gestartet, ist nach der Installation jedoch nicht gestartet. Dies wird an der AMC mit den „Produkt Status prüfen“ Symbolen dargestellt. Zum Starten von MailGate klicken Sie mit der rechten Maustaste auf die Gruppe/den Rechner und wählen sie Kommandos/AntiVir WebGate (UNIX)/Start.

Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. Die Vervielfältigung dieser Publikation oder von Teilen dieser Publikation in jeglicher Form ist ohne vorherige schriftliche Genehmigung durch die Avira Operations GmbH & Co. KG nicht gestattet. Irrtümer und technische Änderungen vorbehalten.

Ausgabe Q2-2013

AntiVir® ist ein registriertes Warenzeichen der Avira Holding GmbH. Alle anderen Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer. Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.



live free.™