



## **Aagon Client Management Platform - AVdetective -**

Aagon Consulting GmbH  
Coesterweg 45  
59494 Soest  
Fon: +49 (0)2921 - 789 200  
Fax: +49 (0)2921 - 789 244  
[www.aagon.com](http://www.aagon.com)  
[info@aagon.com](mailto:info@aagon.com)



# Inhaltsverzeichnis

1. AVdetective	4
1.1. Lizenzbestimmungen	4
1.2. Einleitung	6
1.3. AVdetective	7
1.3.1. Reports	7
1.3.2. FProt	8
1.3.2.1. Reports	8
1.3.2.2. Start/stop application	9
1.3.3. FSecure	11
1.3.3.1. Reports	11
1.3.4. McAfee	12
1.3.4.1. Reports	12
1.3.4.2. Start/stop service	13
1.3.5. Symantec	15
1.3.5.1. Reports	15
1.3.5.2. Send grc.dat	16
1.3.5.3. Send virus definitions	19
1.3.5.4. Start/stop service	22
1.3.6. Trend Micro	24
1.3.6.1. Reports	24
1.3.6.2. Start/stop service	25
1.4. Anhang	27
Index	29

# 1. AVdetective

## 1.1. Lizenzbestimmungen

### Hinweis

Aagon gewährt Ihnen eine Lizenz für die in diesem Paket enthaltene Software ausschließlich unter der Voraussetzung, dass Sie die Bedingungen dieser Lizenzvereinbarung in vollem Umfang anerkennen. Bitte lesen Sie die Bestimmungen sorgfältig, bevor Sie diese Verpackung öffnen. Mit dem Öffnen der Verpackung erklären Sie sich mit den Bestimmungen des Lizenzvertrages einverstanden.

Sollten Sie nicht einverstanden sein, geben Sie bitte die ungeöffnete Packung zusammen mit allen zum Lieferumfang gehörenden Gegenständen unverzüglich gegen Erstattung des Kaufpreises an die Stelle zurück, von der Sie diese bezogen haben.

### Lizenz und Garantie

Die mit dieser Lizenz erworbene Software (im folgenden als "Software" bezeichnet) ist Eigentum der Firma Aagon oder deren Lizenzgeber und ist durch nationale Gesetze urheberrechtlich geschützt. Mit der Annahme der Lizenzbedingungen erhalten Sie das Recht zur Benutzung der Software. Sofern nicht durch eine mit dieser Lizenz ausgelieferte Zusatzvereinbarung andere Regelungen getroffen werden, unterliegt die Nutzung der Software folgenden Bestimmungen:

#### Sie sind berechtigt:

- a) eine Kopie der Software auf einem Einzelcomputer zu benutzen.
- b) eine Kopie der Software zu Archivierungszwecken anzufertigen oder die Software auf die Festplatte Ihres Computers zu kopieren und die Originaldisketten zu archivieren.
- c) die Software in einem Netzwerk einzusetzen, vorausgesetzt, dass Sie über eine lizenzierte Kopie der Software für jeden Computer verfügen, der über das Netzwerk auf die Software zugreifen kann.
- d) nach schriftlicher Benachrichtigung an Aagon die Software dauerhaft einem Dritten zu überlassen, vorausgesetzt, dass Sie alle Kopien der Software und der Begleitdokumentation übergeben und der Empfänger der Software sich mit den Bestimmungen dieser Lizenzvereinbarung einverstanden erklärt.

#### Sie sind nicht berechtigt:

- a) die mit der Software gelieferte Dokumentation zu kopieren.
- b) die Software ganz oder teilweise zu verleihen oder zu vermieten oder Unterlizenzen zu vergeben.
- c) die Software zurück zu entwickeln (reverse engineering), zu dekompile, zu disassemblieren oder auf andere Weise zu versuchen, den Quellcode der Software zugänglich zu machen, die Software zu ändern, zu übersetzen oder davon abgeleitete Produkte zu erstellen.
- d) nach Erhalt eines Austauschdiskettensatzes oder einer Upgrade-Version als Ersatz für eine frühere Version die vorher erhaltene Kopie oder die frühere Version der Software zu benutzen, es sei denn, dass Sie die frühere Version nach einem Upgrade einer gemeinnützigen Organisation Ihrer Wahl zur Verfügung stellen und diese Organisation schriftlich erklärt, das Produkt als alleiniger Endbenutzer einzusetzen und die Bestimmungen dieser Vereinbarung einzuhalten. In allen anderen Fällen müssen nach dem Erwerb einer aktualisierten Version der Software alle Kopien früherer Versionen vernichtet werden.

### Beschränkte Garantie

Aagon gewährleistet für sechzig (60) Tage ab Empfangsdatum, dass das Medium, auf dem die Software ausgeliefert wird, keine Material- und/oder Herstellungsmängel aufweist. Im Falle, dass das gelieferte Produkt dieser Garantie nicht genügt, besteht Ihr alleiniger Anspruch nach Wahl von Aagon entweder im Ersatz der zusammen mit einem Kaufnachweis an Aagon innerhalb der Garantiezeit zurückgegebenen fehlerhaften Erzeugnisse oder in der Erstattung des bezahlten Kaufpreises.

Diese beschränkte Garantie ist ausschließlich und anstelle aller anderen Garantien, sowohl ausdrücklicher als auch implizierter Art, einschließlich der implizierten Garantie der Verkäuflichkeit, der Eignung für einen bestimmten Zweck und der Nichtübertretung. Diese Garantie gibt Ihnen bestimmte gesetzliche Rechte. Sie haben möglicherweise andere Rechte, die von Staat zu Staat unterschiedlich sind.

### Haftungsausschluss

Unabhängig davon, ob eines der hierin dargelegten Rechtsmittel seinen wesentlichen Zweck nicht erfüllt, ist Aagon in keinem Falle ersatzpflichtig für irgendwelche indirekten, Folge- oder ähnlichen Schäden (eingeschlossen sind Schäden aus entgangenem Gewinn oder Verlust von Daten), die aufgrund der Benutzung der Software oder der Unfähigkeit, die Software zu verwenden, entstehen, selbst wenn Aagon von der Möglichkeit solcher Schäden unterrichtet worden ist.

Einige Staaten erlauben die Beschränkung oder den Ausschluss der Haftung für Begleit- und Folgeschäden nicht, so dass die oben angeführte Beschränkung oder der Ausschluss für Sie möglicherweise nicht zutrifft.

In jedem Falle ist die Haftung von Aagon auf den für die Software bezahlten Kaufpreis beschränkt.

Der oben dargelegte Ausschluss und die Beschränkung sind unabhängig von Ihrer Annahme der Software.

### Allgemein

Diese Vereinbarung kann nur durch eine mit dieser Lizenz ausgelieferte Zusatzlizenzvereinbarung oder durch ein anderes, sowohl von Ihnen als auch von Aagon unterzeichnetes, schriftliches Dokument geändert werden. Sollten Sie Fragen zu dieser Vereinbarung haben oder sich aus anderen Gründen mit Aagon in Verbindung setzen wollen, wenden Sie sich bitte an:

Aagon Consulting GmbH

Coesterweg 45

59494 Soest

Tel.: +49 (0) 2921 789 200

Fax: +49 (0) 2921 789 244

© Aagon Consulting GmbH



### **Copyright**

Copyright © 2002 - 2005 Aagon Consulting GmbH

Alle Rechte vorbehalten.

Dieses Handbuch ist urheberrechtlich geschützt. Kein Teil dieser Publikation darf in irgendeiner Form ohne ausdrückliche schriftliche Genehmigung der Aagon Consulting GmbH kopiert, fotokopiert, reproduziert, übersetzt oder unter Verwendung elektronischer Hilfsmittel verarbeitet, vervielfältigt oder verbreitet werden.

### **Warenzeichen**

Aagon, Aagon Consulting, ACK und ACMP sind eingetragene Warenzeichen der Aagon Consulting GmbH.

Windows, Windows 95, Windows 98, Windows 98 SE, Windows ME, Windows NT4.0 Workstation, Windows NT4.0 Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home, Windows XP Professional und Windows 2003 Server sind Warenzeichen der Microsoft Corporation. Andere in diesem Handbuch erwähnte Marken- und Produktnamen sind Warenzeichen der jeweiligen Rechtsinhaber und werden hiermit anerkannt.

## 1.2. Einleitung

Der *AVdetective* ist Bestandteil der *Aagon Client Management Platform*, der Komplettlösung für eine vollständige, zentrale Inventarisierung der Hard- und Software Ihres Netzwerks sowie für eine zuverlässige Kontrolle der Antivirenlösungen. Durch den modularen Aufbau lässt sich ACMP um eine Vielzahl weiterer Lösungen, so genannte *Solutions*, erweitern. Zu diesen *Solutions* gehört der *AVdetective*, den Sie mit *Active Update* nachinstallieren können. Zusätzlich benötigen Sie eine entsprechende Lizenz, um das Modul in vollem Umfang nutzen zu können.

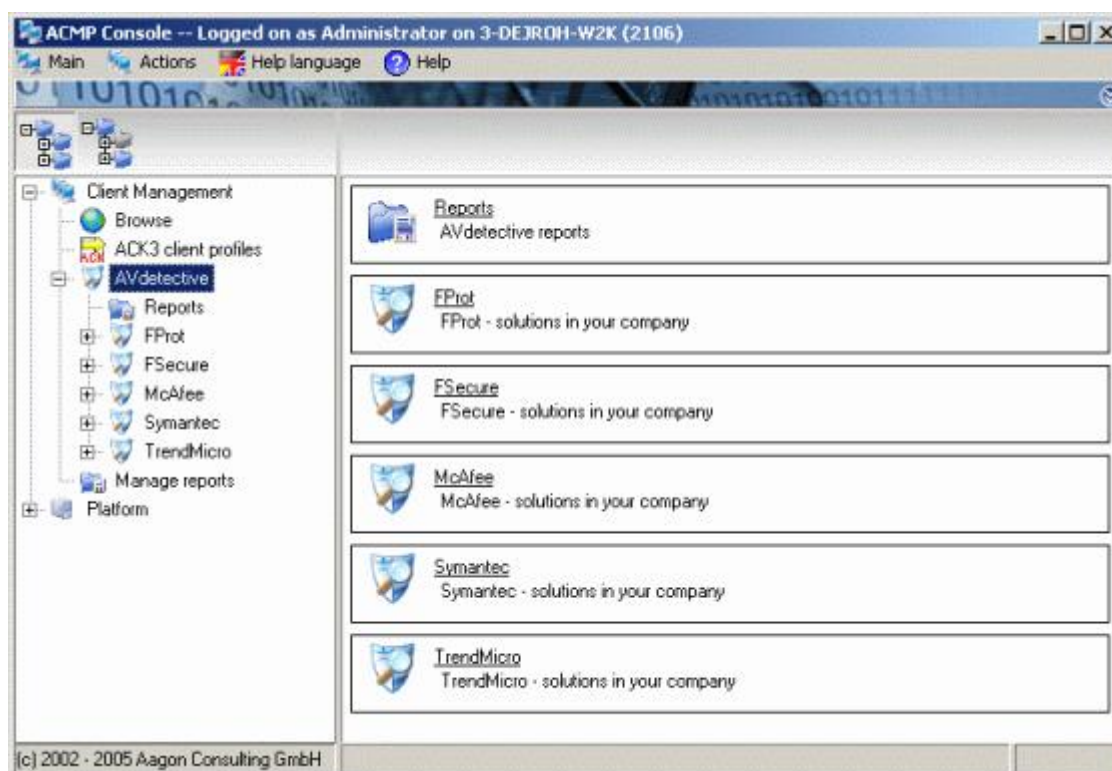
### Was ist der AVdetective?

Der *AVdetective* ist die professionelle Kontrolle der Antivirenlösungen in Ihrem Netzwerk.

Mit dem *AVdetective* können Sie ermitteln,

- ob alle Clients gesichert sind,
- welcher Virenschutz im Einsatz ist,
- welche Antiviren-Definition installiert ist,
- ob die Antiviren-Dienste gestartet sind
- und ob alle Rechner die neusten Virenschutz-Definitionen haben.

Ob Ihre Virenabwehr funktioniert, sagt Ihnen zuverlässig das Antivirenmanagement von ACMP. Der *AVdetective* sorgt für eine zentrale Antivirenprogramm-Inventarisierung und überprüft den Virenschutz im gesamten Netzwerk. So erfahren Sie als Administrator, ob das Netzwerk rundum geschützt ist, ob jeder Client tatsächlich eine Antivirenlösung hat, ob diese aktiv ist und ob die Virendefinitionen aktuell sind.



Nach der Installation finden Sie das Programm im Programmbaum unter *Client Management*. Klicken Sie einfach auf die Schaltfläche, die jetzt neu hinzugekommen ist.



**AVdetective**

AV-solutions in your company

### 1.3. AVdetective

Im Programm *Reports* finden Sie 34 fertige Reports, mit deren Hilfe Sie sich einen ersten Überblick über die in Ihrem Unternehmen eingesetzten Antivirenlösungen verschaffen können.



#### Reports

AVdetective reports

Zur Zeit unterstützt der AVdetective folgende Antivirenlösungen:



#### FProt

FProt - solutions in your company



#### Fsecure

Fsecure - solutions in your company



#### McAfee

McAfee - solutions in your company



#### Symantec

Symantec - solutions in your company




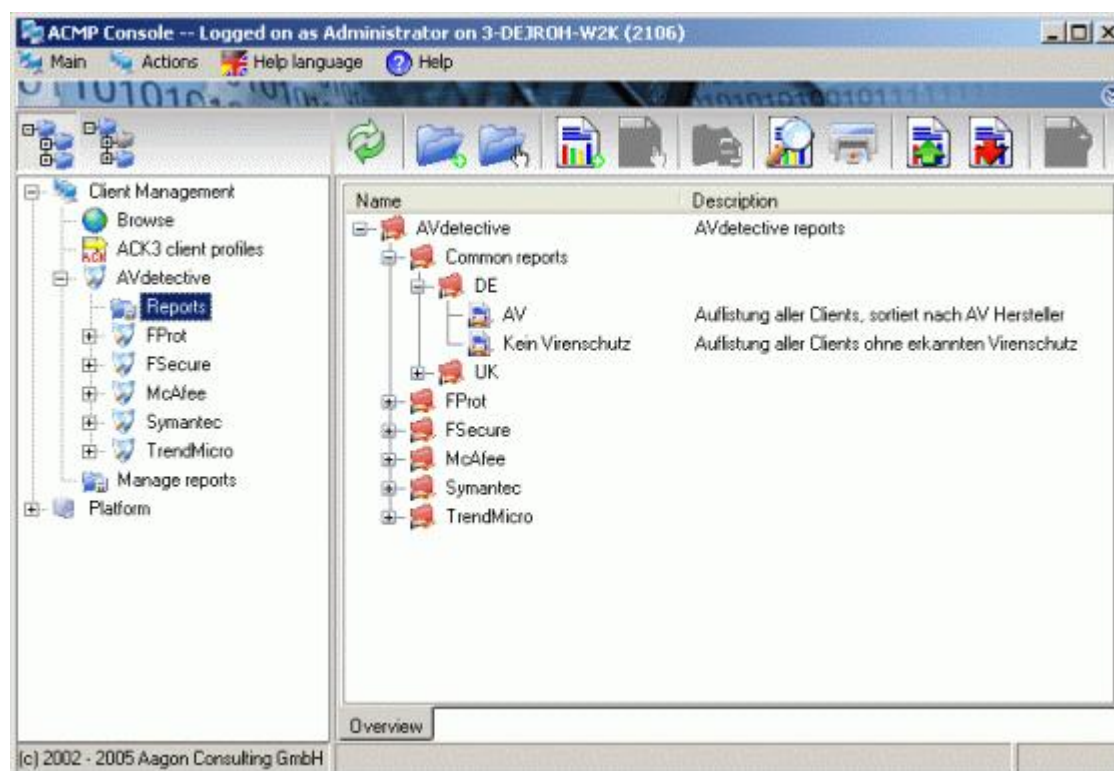
#### Trend Micro

TrendMicro - solutions in your company

Um das gewünschte Programm zu starten, klicken Sie einfach auf die entsprechende Schaltfläche.

#### 1.3.1. Reports

Unter  *AVdetective* stehen Ihnen 34 fertige Reports, je 17 in Deutsch und Englisch, zur Verfügung. Um einen ersten Überblick zu erhalten, wählen Sie unter *Common Reports* den Report *AV* aus und starten ihn mit einem Doppelklick. Dieser Report liefert Ihnen eine Auflistung aller Clients, sortiert nach AV Hersteller, aus der Sie ablesen können, ob Ihr Netzwerk ausreichend geschützt ist. Alle fertigen Reports können Sie ausführen, bearbeiten oder löschen. Die Verzeichnisse, in denen die Reports stehen, können nicht gelöscht werden.



Mit Hilfe dieses Programms können Sie weitere Reports für Ihre AV-Solutions erstellen, bearbeiten



und ausdrucken. Außerdem können Sie diese Reports in einer Verzeichnisstruktur übersichtlich organisieren und verwalten. Eine ausführliche Hilfe, wie Sie Reports erstellen, finden Sie im Handbuch ACMP im Abschnitt **Manage Reports**.

## Hinweis:

Ordner und Reports die Sie hier erstellen, finden Sie anschließend im Programm *Manage Reports* wieder. Sie können dort genauso bearbeitet werden wie in diesem Programm. Ordner und Reports aus dem Programm *Manage Reports* werden hier allerdings nicht angezeigt.

## 1.3.2. FProt

Hier finden Sie die Schaltflächen, die zur Antivirenlösung von FProt gehören.



### Reports


FProt reports

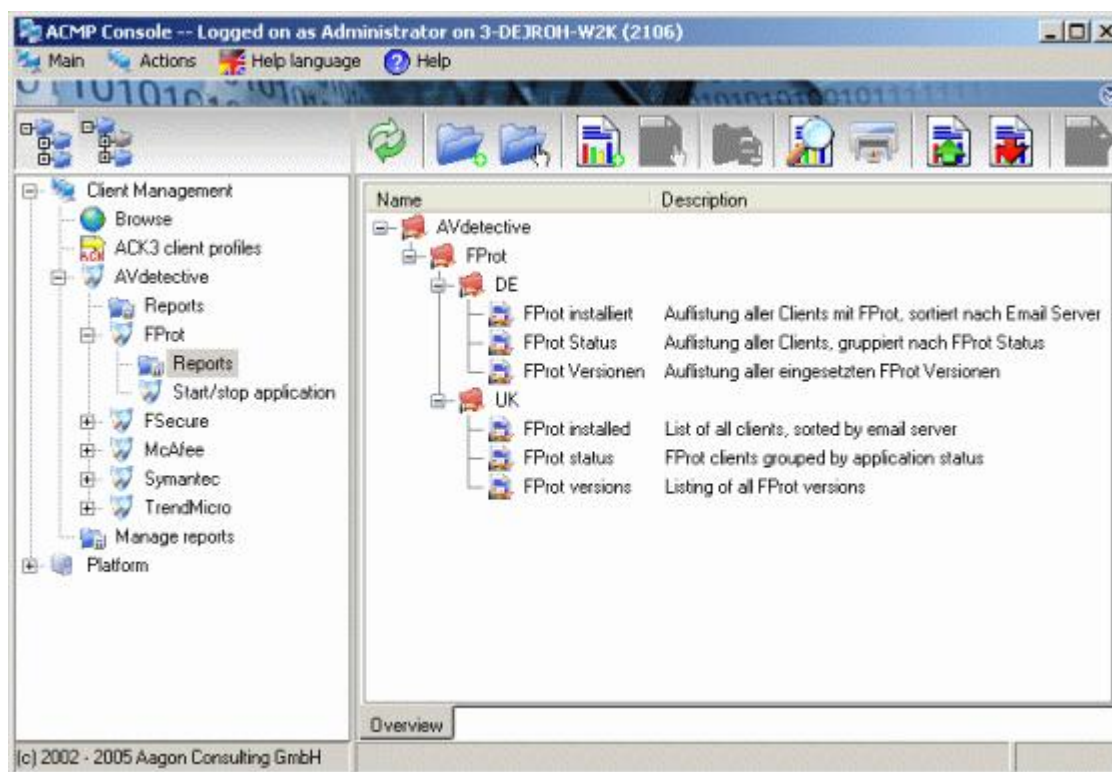
### Start/stop application

Start/stop FPROT-application

Um ein Programm zu starten, klicken Sie einfach auf die entsprechende Schaltfläche.

### 1.3.2.1. Reports

Unter  *FProt* stehen Ihnen sechs fertige Reports, drei in Deutsch und drei in Englisch zur Verfügung, die Sie ausführen, bearbeiten oder löschen können.



Mit Hilfe dieses Programms können Sie weitere Reports für Ihre FProt-Solution erstellen, bearbeiten und ausdrucken. Außerdem können Sie diese Reports in einer Verzeichnisstruktur übersichtlich organisieren und verwalten. Eine ausführliche Hilfe, wie Sie Reports erstellen, finden Sie im Handbuch ACMP im Abschnitt **Manage Reports**.

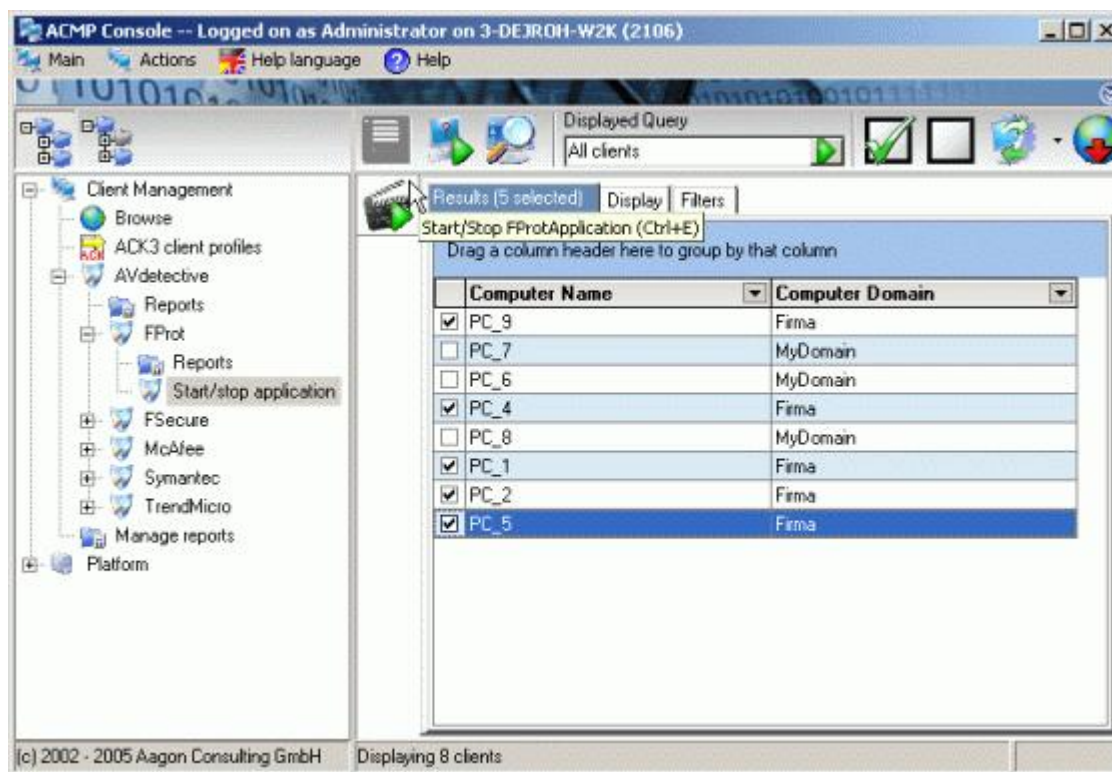
## Hinweis:

Ordner und Reports die Sie hier erstellen, finden Sie anschließend im Programm *Manage Reports* wieder. Sie können dort genauso bearbeitet werden wie in diesem Programm. Ordner und Reports aus dem Programm *Manage Reports* werden hier allerdings nicht angezeigt.



### 1.3.2.2. Start/stop application


Hier können Sie auf beliebigen Clients Anwendungen stoppen oder starten. Dies ist bei FProt der *RealTime Protector*.



Führen Sie als erstes eine Abfrage aus, die Ihnen alle Rechner in Ihrem Netzwerk anzeigt, auf denen FProt installiert ist. Wie das geht, können Sie in den Abschnitten *Browse* oder *Query Management* nachlesen.

Sobald Ihre Abfrage ausgeführt ist, können Sie die gewünschten Clients auswählen. Aktivieren Sie dazu das Auswahlkästchen ☐ in der betreffenden Zeile ☒.

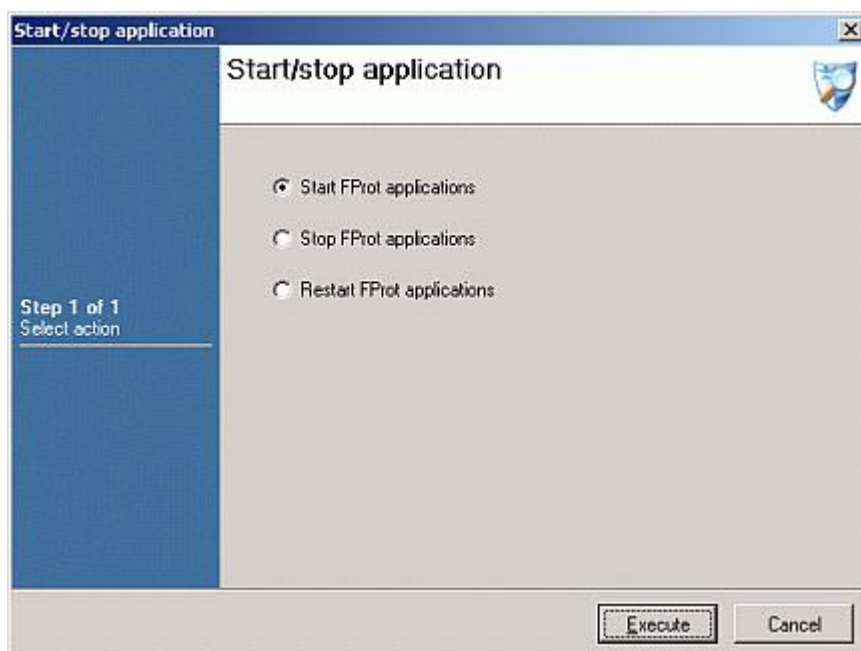
Beachten Sie, dass Sie nur Clients auswählen können, auf denen der ACMP Agent installiert ist.

Wenn Sie alle Clients ausgewählt haben, klicken Sie auf das Symbol  (Start/Stop FProtApplication(Ctrl+E) [Starte/Stoppe die FProt Anwendung]).

Es öffnet sich das Fenster *Start/Stop FProt Applications*.

### Start/Stop FProt Applications

Abhängig von Ihren Rechten (siehe: Handbuch ACMP Kapitel: *User management*) stehen Ihnen bis zu drei so genannte Radio-Schalter zur Auswahl:



- ☒ *Start FProt Applications [Starte die FProt Anwendung]*
- ☐ *Stop FProt Applications [Stoppe die FProt Anwendung]*
- ☐ *Restart FProt Applications [Starte die FProt Anwendung neu]*

Mit *Cancel* verlassen Sie das Fenster, ohne die Aktion auszulösen. Mit *Execute* wird die ausgewählte Aktion gestartet.

Die Anweisungen für jeden Rechner werden nun in eine Warteschlange gestellt und abgearbeitet, sobald der betreffende Rechner wieder Verbindung zum ACMP Server aufnimmt. Im Programm **Queue** können Sie überprüfen, ob Ihre Anweisungen bereits ausgeführt worden sind oder nicht.

### 1.3.3. FSecure

Hier finden Sie die Schaltflächen, die zur Antivirenlösung von FSecure gehören.




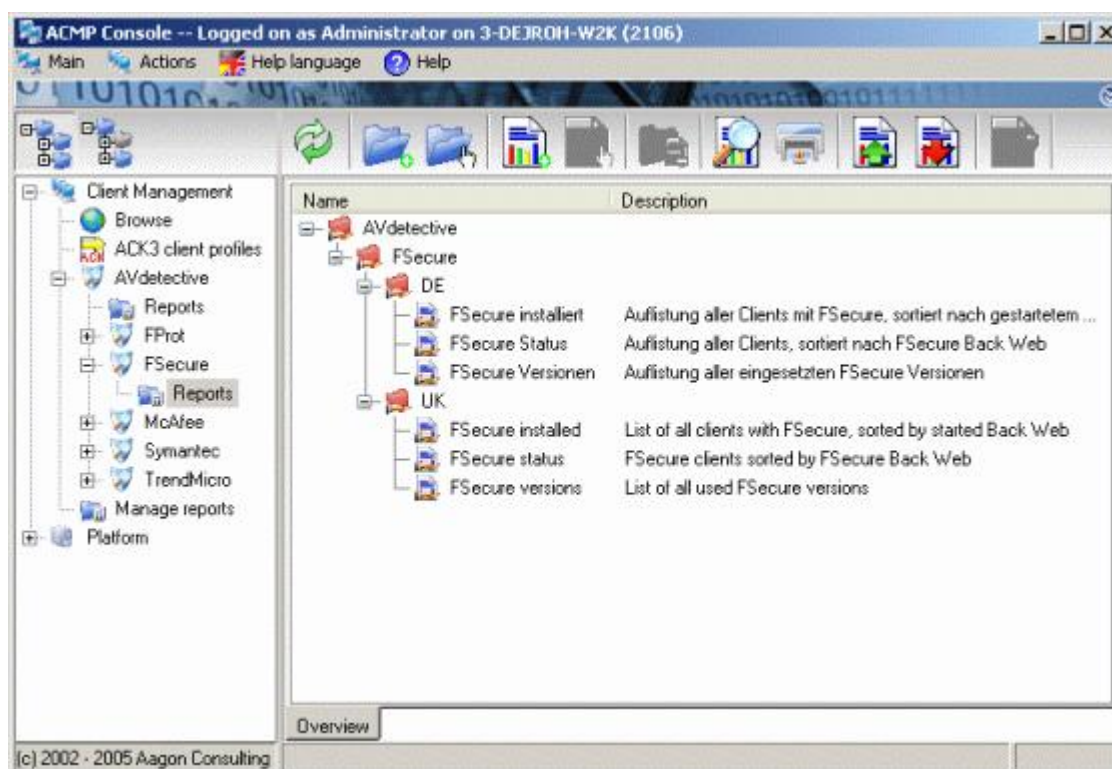
#### Reports

Fsecure reports

Um ein Programm zu starten, klicken Sie einfach auf die entsprechende Schaltfläche.

#### 1.3.3.1. Reports

Unter  **FSecure** stehen Ihnen sechs fertige Reports, drei in Deutsch und drei in Englisch zur Verfügung, die Sie ausführen, bearbeiten oder löschen können.



Mit Hilfe dieses Programms können Sie weitere Reports für Ihre FSecure-Solution erstellen, bearbeiten und ausdrucken. Außerdem können Sie diese Reports in einer Verzeichnisstruktur übersichtlich organisieren und verwalten. Eine ausführliche Hilfe, wie Sie Reports erstellen, finden Sie im Handbuch ACMP im Abschnitt **Manage Reports**.

#### Hinweis:

Ordner und Reports die Sie hier erstellen, finden Sie anschließend im Programm **Manage Reports** wieder. Sie können dort genauso bearbeitet werden wie in diesem Programm. Ordner und Reports aus dem Programm **Manage Reports** werden hier allerdings nicht angezeigt.

## 1.3.4. McAfee

Hier finden Sie die Schaltflächen, die zur Antivirenlösung von McAfee gehören.



[Reports](#)

McAfee reports




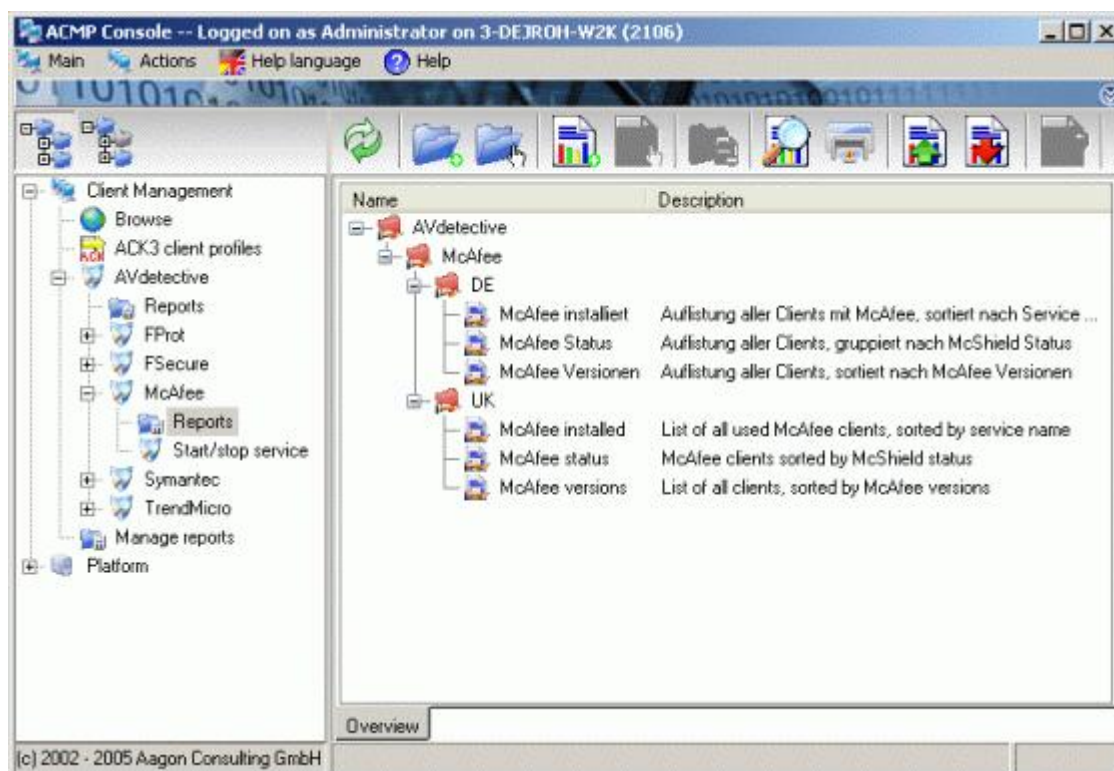
[Start/stop service](#)

Start/stop McAfee-services

Um ein Programm zu starten, klicken Sie einfach auf die entsprechende Schaltfläche.

### 1.3.4.1. Reports

Unter  McAfee stehen Ihnen sechs fertige Reports, drei in Deutsch und drei in Englisch zur Verfügung, die Sie ausführen, bearbeiten oder löschen können.



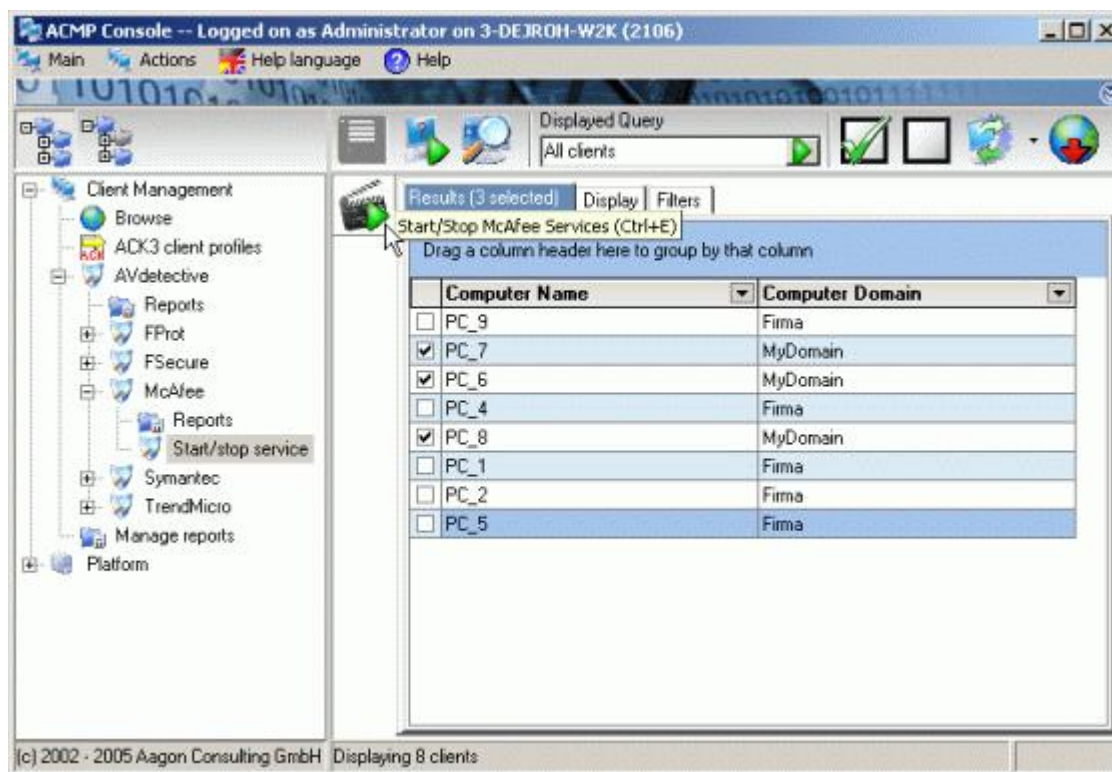
Mit Hilfe dieses Programms können Sie weitere Reports für Ihre McAfee-Solution erstellen, bearbeiten und ausdrucken. Außerdem können Sie diese Reports in einer Verzeichnisstruktur übersichtlich organisieren und verwalten. Eine ausführliche Hilfe, wie Sie Reports erstellen, finden Sie im Handbuch ACMP im Abschnitt **Manage Reports**.

#### Hinweis:

Ordner und Reports die Sie hier erstellen, finden Sie anschließend im Programm *Manage Reports* wieder. Sie können dort genauso bearbeitet werden wie in diesem Programm. Ordner und Reports aus dem Programm *Manage Reports* werden hier allerdings nicht angezeigt.

### 1.3.4.2. Start/stop service

Hier können Sie auf beliebigen Clients die McAfee-Dienste stoppen und starten. Dies sind bei McAfee: *AV Sync. Manager* und *McShield*



Führen Sie als erstes eine Abfrage aus, die Ihnen alle Rechner in Ihrem Netzwerk anzeigt, auf denen McAfee installiert ist. Wie das geht, können Sie in den Abschnitten *Browse* oder *Query Management* nachlesen.

Sobald Ihre Abfrage ausgeführt ist, können Sie die gewünschten Clients auswählen. Aktivieren Sie dazu das Auswahlkästchen ☐ in der betreffenden Zeile ☒.

Beachten Sie, dass Sie nur Clients auswählen können, auf denen der ACMP Agent installiert ist.

Wenn Sie alle Clients ausgewählt haben, klicken Sie auf das Symbol  (*Start/Stop McAfee Services (Ctrl+E)* [*Starte/Stoppe die McAfee-Dienste*]).

Es öffnet sich das Fenster *Start/Stop McAfee Services*.



### Start/Stop McAfee Services

Abhängig von Ihren Rechten (siehe: Handbuch ACMP Kapitel: *User management*) stehen Ihnen drei so genannte Radio-Schalter zur Auswahl:



- ☒ *Start Services [Starte die Dienste]*
- ☐ *Stop Services [Stoppe die Dienste]*
- ☐ *Restart Services [Starte die Dienste neu]*

Mit *Cancel* verlassen Sie das Fenster, ohne die Aktion auszulösen. Mit *Execute* wird die ausgewählte Aktion gestartet.

Die Anweisungen für jeden Rechner werden nun in eine Warteschlange gestellt und abgearbeitet, sobald der betreffende Rechner wieder Verbindung zum ACMP Server aufnimmt. Im Programm **Queue** können Sie überprüfen, ob Ihre Anweisungen bereits ausgeführt worden sind oder nicht.

### 1.3.5. Symantec

Hier finden Sie die Schaltflächen, die zur Antivirenlösung von Symantec gehören.



[Reports](#)

Symantec reports



[Send grc.dat](#)

Send grc.dat



[Send virus definitions](#)

Send virus definitions




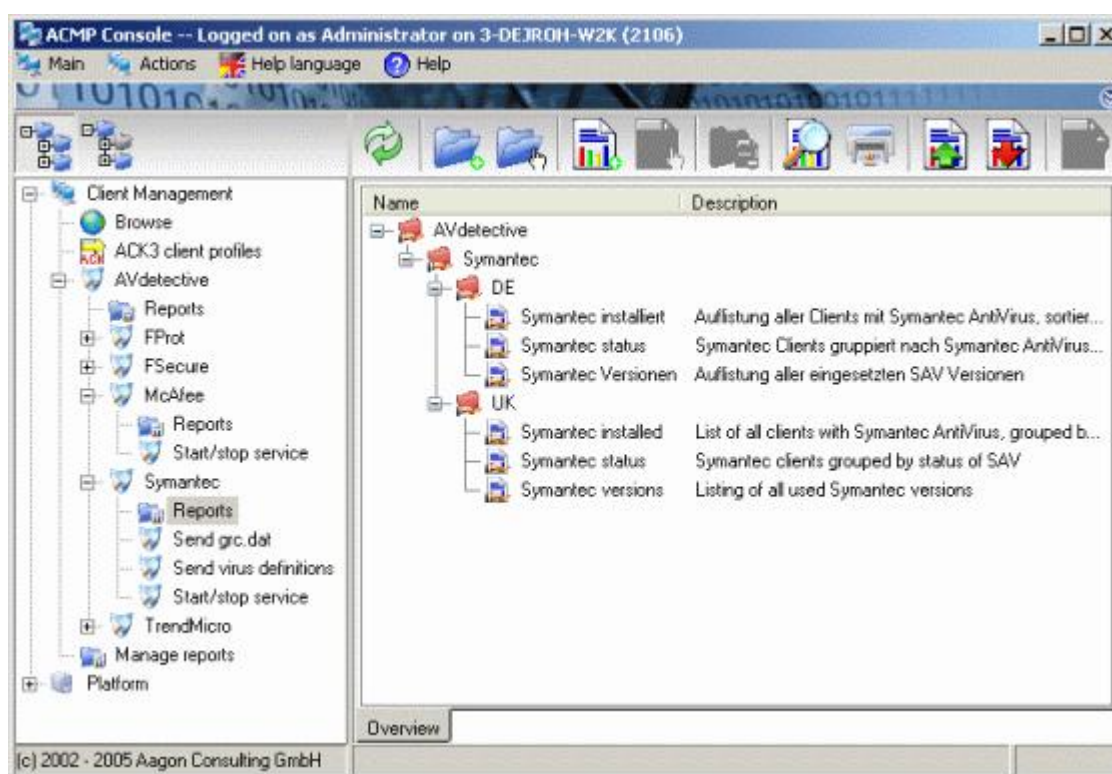
[Start/stop service](#)

Start/stop Symantec-services

Um ein Programm zu starten, klicken Sie einfach auf die entsprechende Schaltfläche.

#### 1.3.5.1. Reports

Unter  *Symantec* stehen Ihnen sechs fertige Reports, drei in Deutsch und drei in Englisch zur Verfügung, die Sie ausführen, bearbeiten oder löschen können.



Mit Hilfe dieses Programms können Sie weitere Reports für Ihre Symantec-Solution erstellen, bearbeiten und ausdrucken. Außerdem können Sie diese Reports in einer Verzeichnisstruktur übersichtlich organisieren und verwalten. Eine ausführliche Hilfe, wie Sie Reports erstellen, finden Sie im Handbuch ACMP im Abschnitt **Manage Reports**.

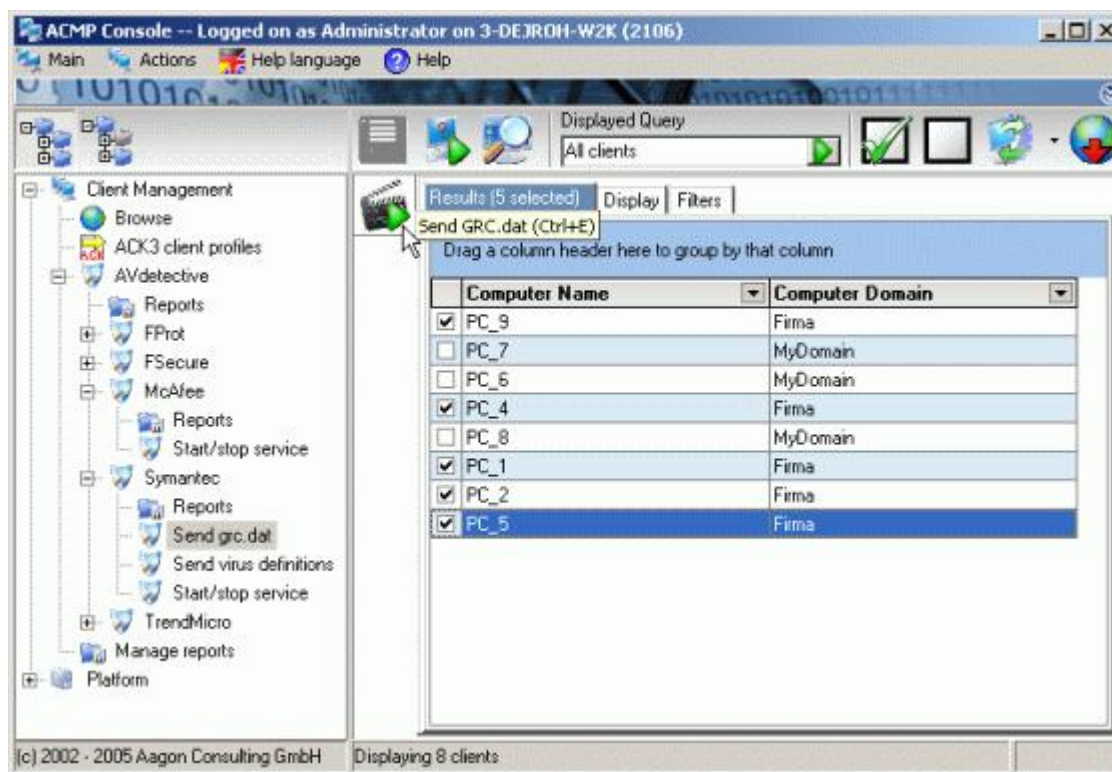
#### Hinweis:

Ordner und Reports die Sie hier erstellen, finden Sie anschließend im Programm *Manage Reports* wieder. Sie können dort genauso bearbeitet werden wie in diesem Programm. Ordner und Reports aus dem Programm *Manage Reports* werden hier allerdings nicht angezeigt.



### 1.3.5.2. Send grc.dat


Hier können Sie beliebigen Clients eine neue **grc.dat** senden, um sie so einem anderen Parent-Server zuzuordnen.



Führen Sie als erstes eine Abfrage aus, die Ihnen alle Rechner in Ihrem Netzwerk anzeigt, auf denen Symantec AntiVirus installiert ist. Wie das geht, können Sie in den Abschnitten *Browse* oder *Query Management* nachlesen.

Sobald Ihre Abfrage ausgeführt ist, können Sie die gewünschten Clients auswählen. Aktivieren Sie dazu das Auswahlkästchen ☐ in der betreffenden Zeile ☒.

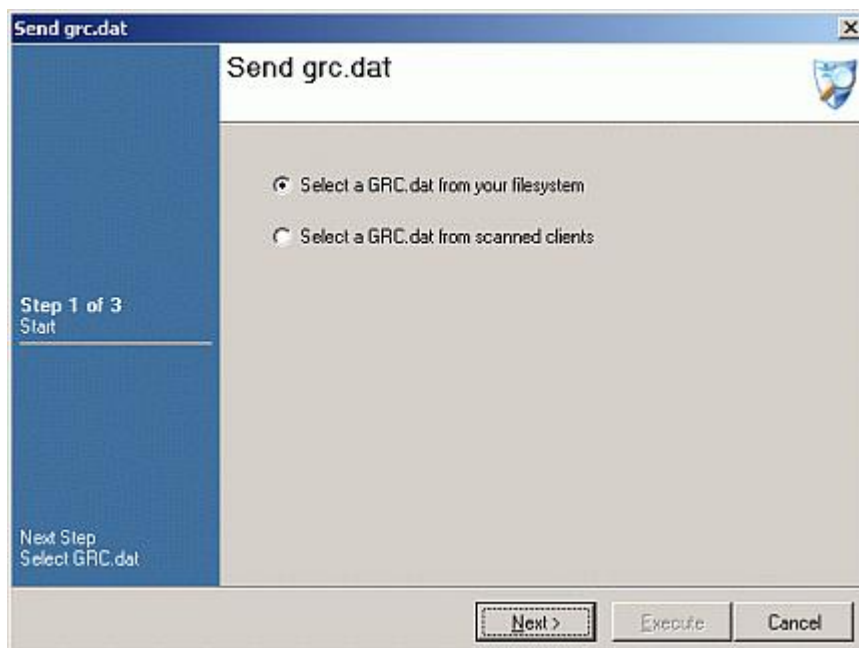
Beachten Sie, dass Sie nur Clients auswählen können, auf denen der ACMP Agent installiert ist.

Wenn Sie alle Clients ausgewählt haben, klicken Sie auf das Symbol  (*Send GRC.Dat(Ctrl.+E)* [*Sende GRC.Dat*]).

Es öffnet sich das Fenster *Send GRC.dat to selected clients* [*Sende GRC.Dat zu den ausgewählten Clients*].

## Send GRC.dat to selected clients


Hier stehen Ihnen zwei so genannte Radio-Schalter zur Auswahl:

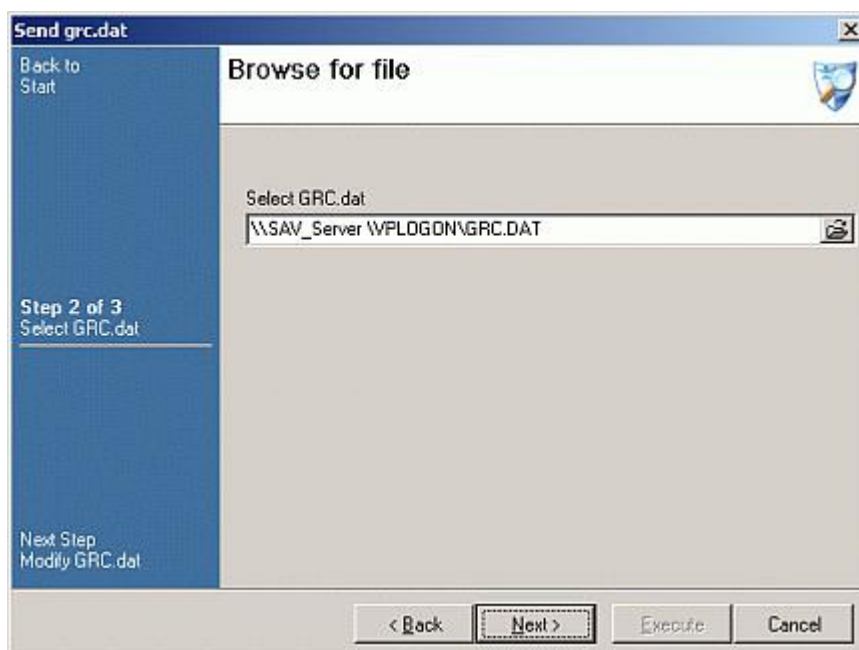



- ⊙ *Select a GRC.DAT from your filesystem [Wählen Sie eine GRC.DAT aus Ihrem Dateisystem]* - verzweigt in den Bildschirm *Browse for file* [Nach der Datei suchen].
- *Select a GRC.DAT from scanned clients* [Wählen Sie eine GRC.DAT von einem der erfassten Clients] - verzweigt in den Bildschirm *Select collected server* [Wähle einen erfassten Server aus].

Wählen Sie eine der beiden Möglichkeiten aus und klicken Sie *Next*, um in den nächsten Bildschirm zu gelangen.

## Browse for file

Es steht Ihnen nun ein Eingabefeld mit dem Symbol  zur Verfügung:

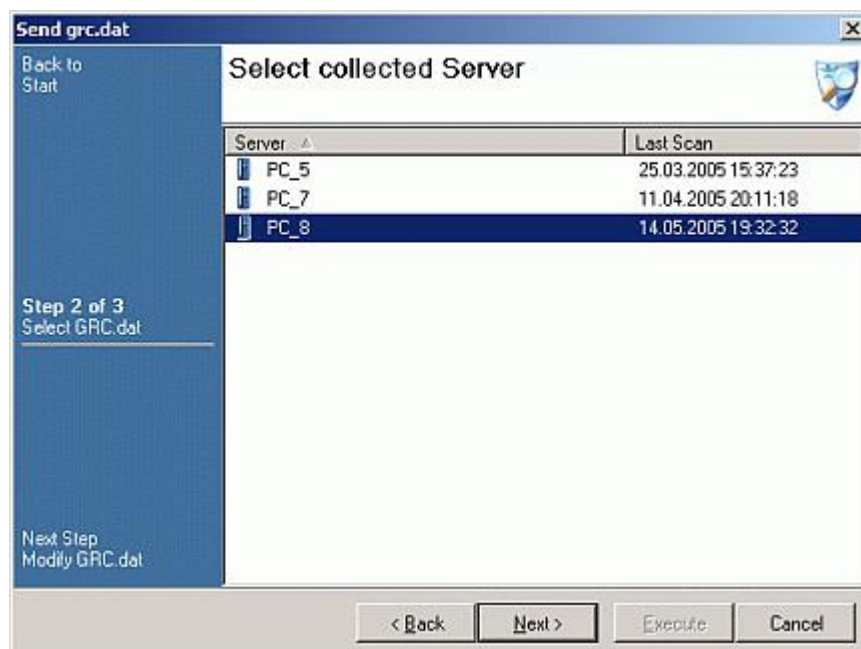


Mit einem Klick auf dieses Symbol  öffnet sich ein Standarddialog. Hier können Sie bequem in

Ihrem Dateisystem nach der gewünschten GRC.DAT suchen. Bestätigen Sie anschließend mit *Öffnen/Open*. Mit *Back* gelangen Sie zum vorherigen Bildschirm mit *Next* in den nächsten.

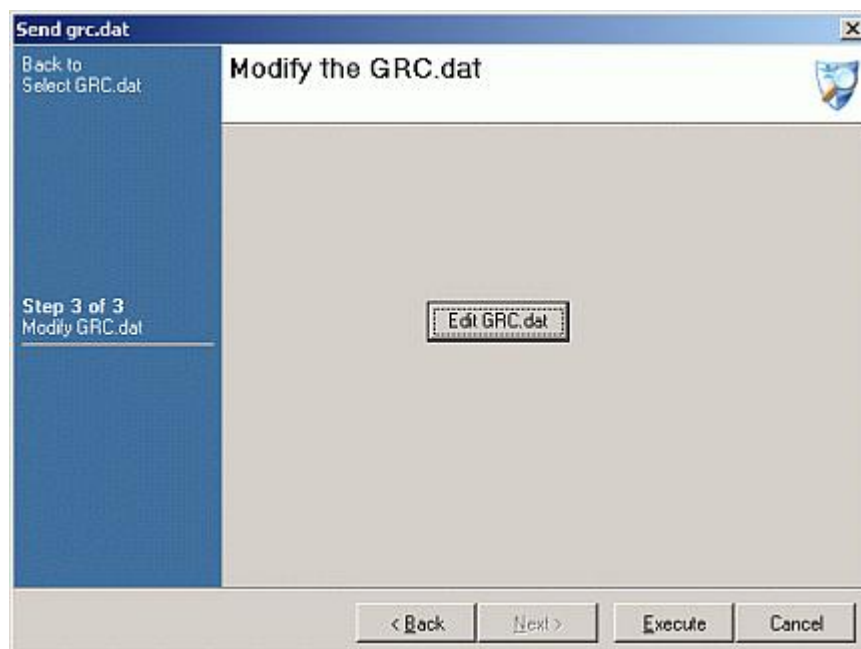
## Select collected server

Hier sehen Sie eine Liste mit Servern, auf denen eine GRC.DAT zur Verfügung steht. Wählen Sie einfach den gewünschten Server mit einem Mausklick aus.



Mit *Back* gelangen Sie zum vorherigen Bildschirm mit *Next* in den nächsten.

## Modify the GRC.dat



Hier finden Sie den Schalter *Edit GRC.dat*. Wenn Sie diesen anklicken wird die ausgewählte GRC.DAT angezeigt und Sie können Änderungen darin vornehmen. Dazu sollten Sie aber über die notwendigen Kenntnisse verfügen. Im Zweifelsfall finden Sie Informationen darüber im Handbuch von Symantec.

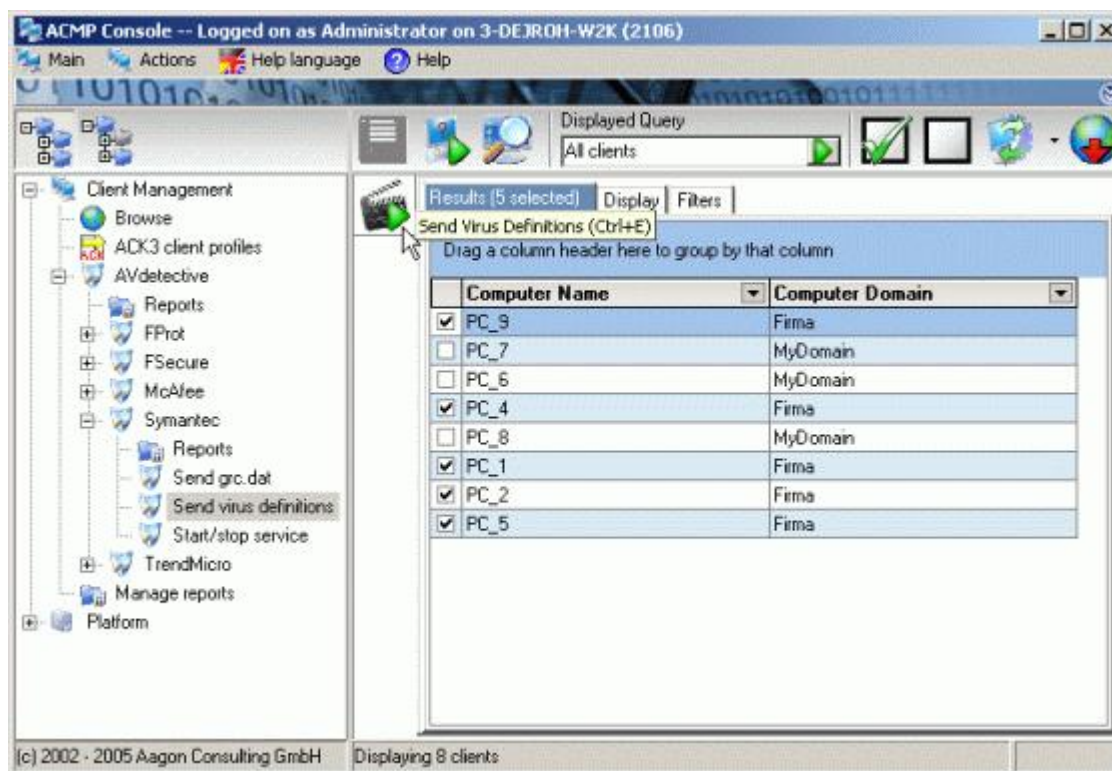
Mit *Back* gelangen Sie zum vorherigen Bildschirm. Mit *Execute* wird die Aktion ausgeführt. Mit

*Cancel* verlassen Sie das Fenster, ohne die Aktion auszulösen.

Die Anweisungen für jeden Rechner werden nun in eine Warteschlange gestellt und abgearbeitet, sobald der betreffende Rechner wieder Verbindung zum ACMP Server aufnimmt. Im Programm **Queue** können Sie überprüfen, ob Ihre Anweisungen bereits ausgeführt worden sind oder nicht.

## 1.3.5.3. Send virus definitions


Hier können Sie beliebigen Clients die aktuellsten Virusdefinitionen senden.



Führen Sie als erstes eine Abfrage aus, die Ihnen alle Rechner in Ihrem Netzwerk anzeigt, auf denen Symantec AntiVirus installiert ist. Wie das geht, können Sie in den Abschnitten *Browse* oder *Query Management* nachlesen.

Sobald Ihre Abfrage ausgeführt ist, können Sie die gewünschten Clients auswählen. Aktivieren Sie dazu das Auswahlkästchen ☐ in der betreffenden Zeile ☒.

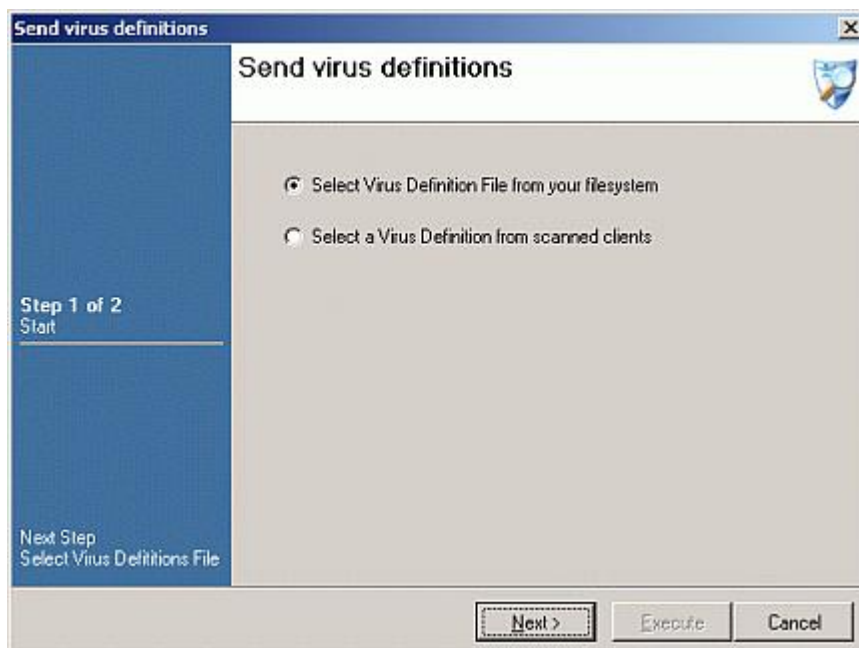
Beachten Sie, dass Sie nur Clients auswählen können, auf denen der ACMP Agent installiert ist.

Wenn Sie alle Clients ausgewählt haben, klicken Sie auf das Symbol  (*Send Virus Definitions(Ctrl+E)* [*Sende Virusdefinitionen*]).

Es öffnet sich das Fenster *Send Virus Definitions to selected clients* [*Sende Virusdefinitionen zu den ausgewählten Clients*].

## Send Virus Definitions to selected clients

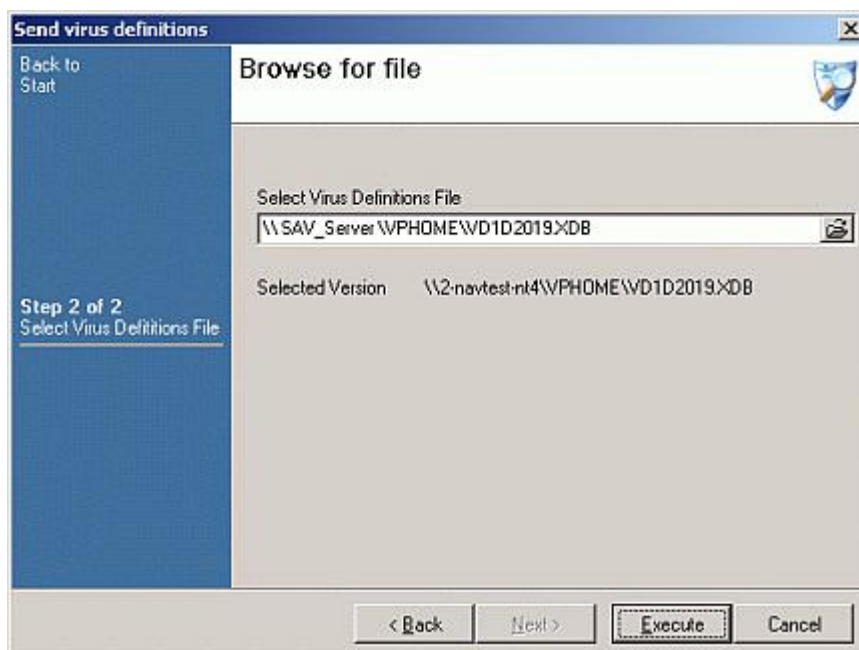
Hier stehen Ihnen zwei so genannte Radio-Schalter zur Auswahl:





- Ⓐ *Select Virus Definition File from your filesystem [Wählen Sie die Viren-Definitions-Datei aus Ihrem Dateisystem]*
- Ⓑ *Select a Virus Definition from scanned clients [Wählen Sie die Viren-Definitions-Datei von einem der erfassten Clients]*

Wählen Sie eine der beiden Möglichkeiten aus und klicken Sie *Next*, um in den nächsten Bildschirm zu gelangen.

## Browse for file



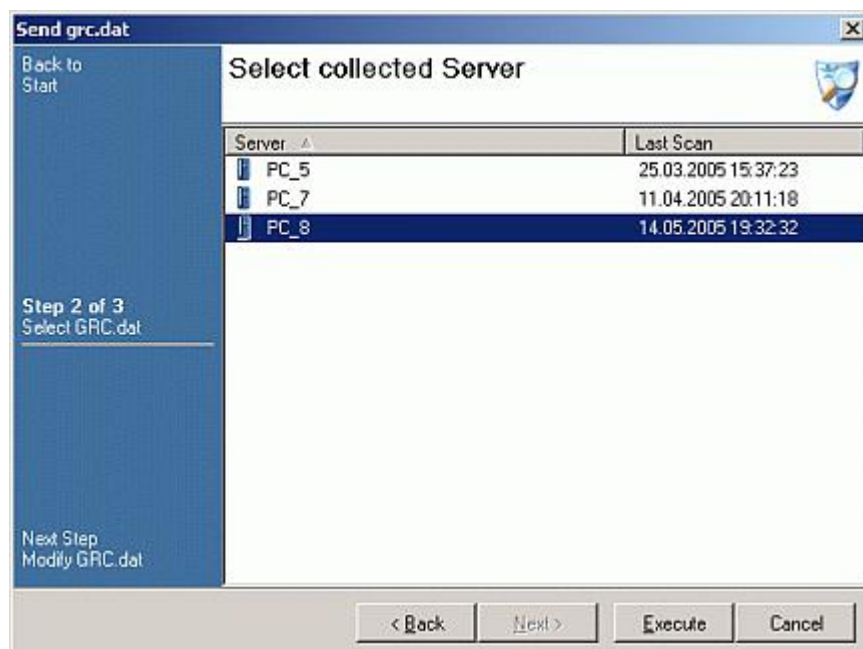
Es steht Ihnen nun ein Eingabefeld mit dem Symbol  zur Verfügung: Mit einem Klick auf dieses Symbol  öffnet sich ein Standarddialog. Hier können Sie bequem in Ihrem Dateisystem nach der gewünschten Virusdefinitionsdatei suchen. Bestätigen Sie abschließend mit *Öffnen/Open*.



Mit *Back* gelangen Sie zum vorherigen Bildschirm. Mit *Execute* wird die Aktion ausgeführt. Mit *Cancel* verlassen Sie das Fenster, ohne die Aktion zu starten.

## Select collected server

Hier Sie sehen eine Liste mit Rechnern, die aktuelle Virendefinitionen haben. Wählen Sie einfach aus der Liste den gewünschten Rechner aus.

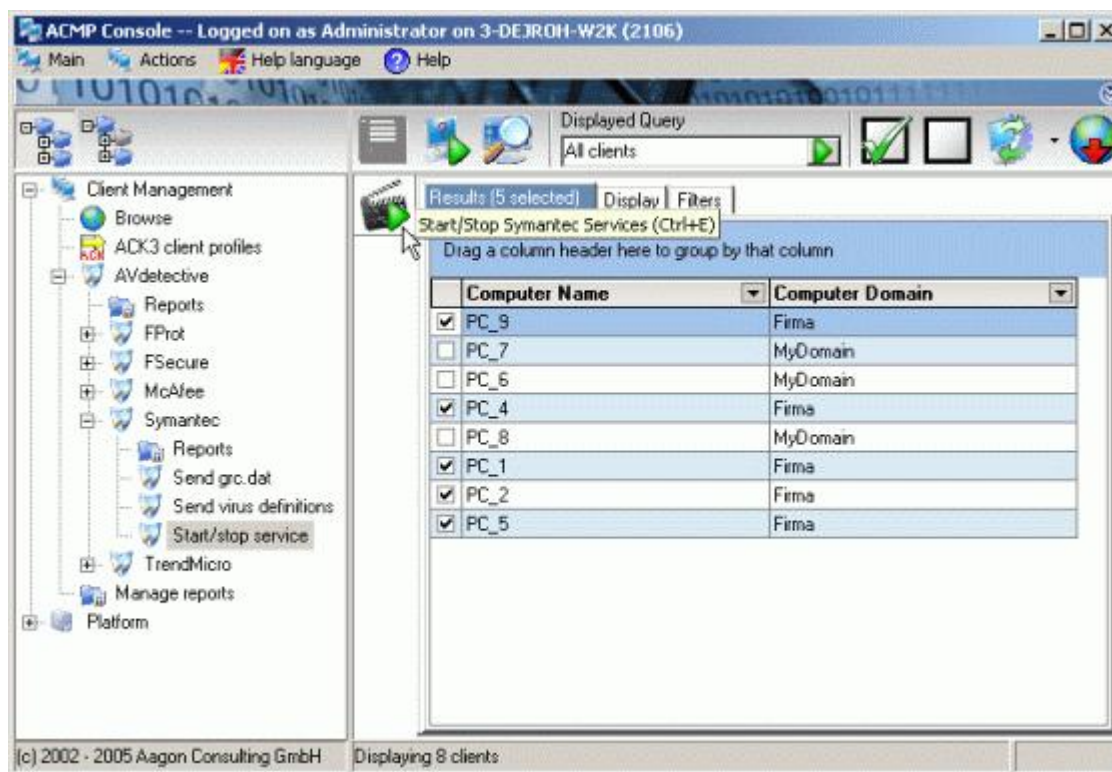


Mit *Back* gelangen Sie zum vorherigen Bildschirm. Mit *Execute* wird die Aktion ausgeführt. Mit *Cancel* verlassen Sie das Fenster, ohne die Aktion zu starten.

Die Anweisungen für jeden Rechner werden nun in eine Warteschlange gestellt und abgearbeitet, sobald der betreffende Rechner wieder Verbindung zum ACMP Server aufnimmt. Im Programm **Queue** können Sie überprüfen, ob Ihre Anweisungen bereits ausgeführt worden sind oder nicht.

#### 1.3.5.4. Start/stop service


Hier können Sie auf beliebigen Clients die Dienste stoppen und starten. Dies ist bei Symantec: *Symantec AntiVirus Dienst*, der u. a. für den Echtzeitschutz sorgt.



Führen Sie als erstes eine Abfrage aus, die Ihnen alle Rechner in Ihrem Netzwerk anzeigt, auf denen Symantec AntiVirus installiert ist. Wie das geht, können Sie in den Abschnitten *Browse* oder *Query Management* nachlesen.

Sobald Ihre Abfrage ausgeführt ist, können Sie die gewünschten Clients auswählen. Aktivieren Sie dazu das Auswahlkästchen ☐ in der betreffenden Zeile ☒.

Beachten Sie, dass Sie nur Clients auswählen können, auf denen der ACMP Agent installiert ist.

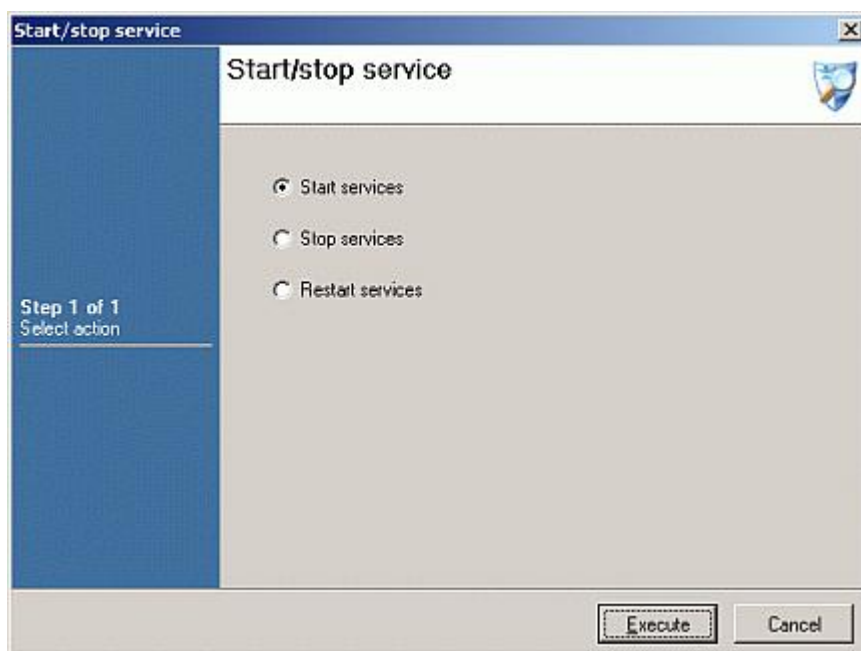
Wenn Sie alle Clients ausgewählt haben, klicken Sie auf das Symbol  (*Start/Stop Symantec Services*) (*Starte/Stoppe die Symantec-Dienste*).

Es öffnet sich das Fenster *Start/Stop Symantec Services*.



### Start/Stop Symantec Services

Abhängig von Ihren Rechten (siehe: Handbuch ACMP Kapitel: *User management*) stehen Ihnen bis zu drei so genannte Radio-Schalter zur Auswahl:



- ☒ *Start Services [Starte die Dienste]*
- ☐ *Stop Services [Stoppe die Dienste]*
- ☐ *Restart Services [Starte die Dienste neu]*

Mit *Cancel* verlassen Sie das Fenster, ohne die Aktion auszulösen. Mit *Execute* wird die ausgewählte Aktion gestartet.

Die Anweisungen für jeden Rechner werden nun in eine Warteschlange gestellt und abgearbeitet, sobald der betreffende Rechner wieder Verbindung zum ACMP Server aufnimmt. Im Programm **Queue** können Sie überprüfen, ob Ihre Anweisungen bereits ausgeführt worden sind oder nicht.

### 1.3.6. Trend Micro

Hier finden Sie die Schaltflächen, die zur Antivirenlösung von Trend Micro gehören.



[Reports](#)

Trend Micro reports



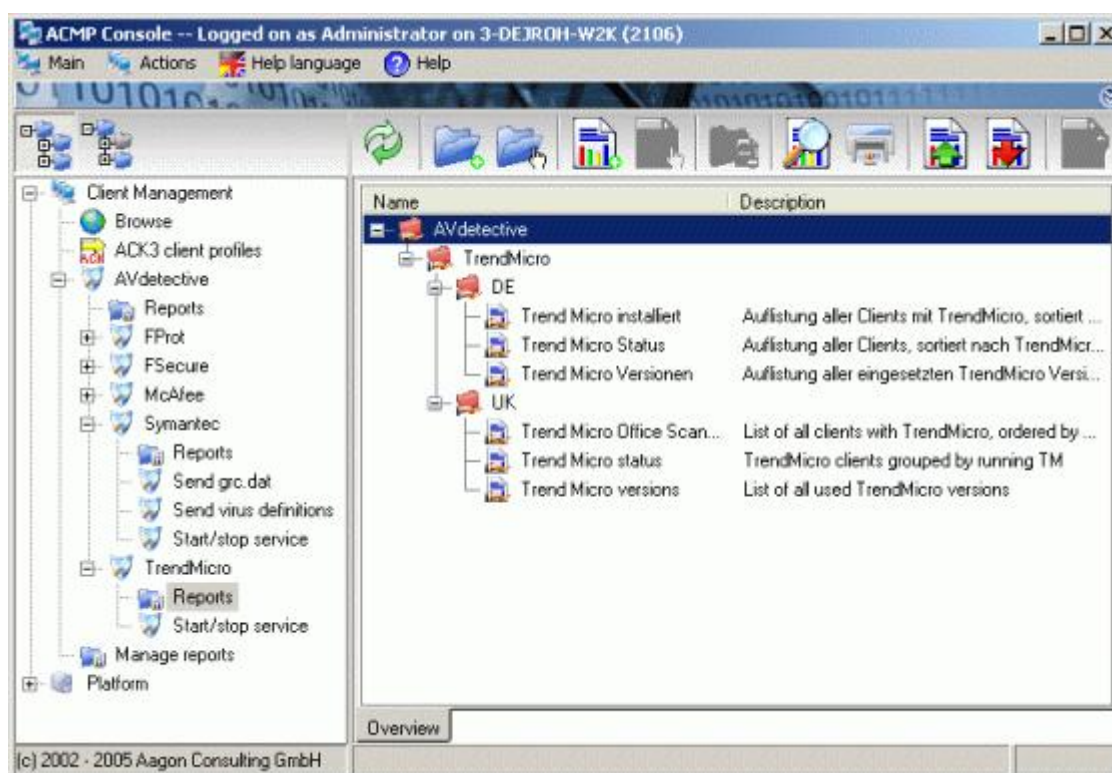
[Start/stop service](#)

Start/stop TrendMicro-services

Um ein Programm zu starten, klicken Sie einfach auf die entsprechende Schaltfläche.

#### 1.3.6.1. Reports

Unter  *Trend Micro* stehen Ihnen sechs fertige Reports, drei in Deutsch und drei in Englisch zur Verfügung, die Sie ausführen, bearbeiten oder löschen können.



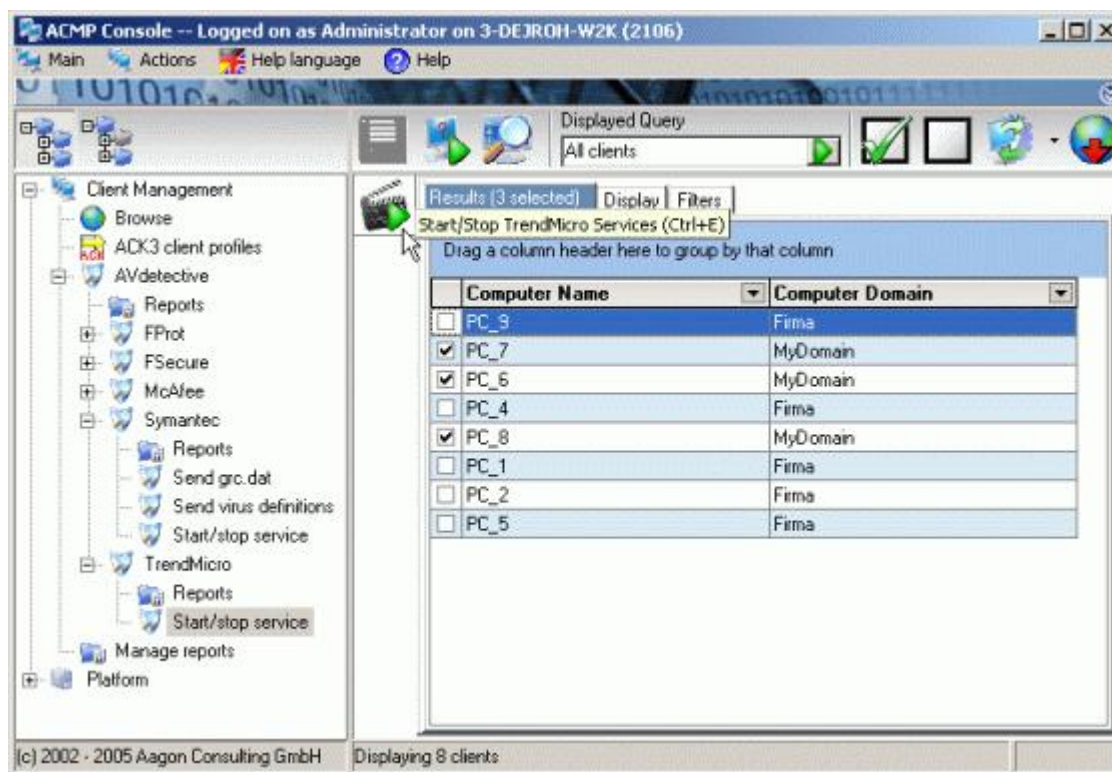
Mit Hilfe dieses Programms können Sie weitere Reports für Ihre Trend Micro-Solution erstellen, bearbeiten und ausdrucken. Außerdem können Sie diese Reports in einer Verzeichnisstruktur übersichtlich organisieren und verwalten. Eine ausführliche Hilfe, wie Sie Reports erstellen, finden Sie im Handbuch ACMP im Abschnitt **Manage Reports**.

#### Hinweis:

Ordner und Reports die Sie hier erstellen, finden Sie anschließend im Programm *Manage Reports* wieder. Sie können dort genauso bearbeitet werden wie in diesem Programm. Ordner und Reports aus dem Programm *Manage Reports* werden hier allerdings nicht angezeigt.

### 1.3.6.2. Start/stop service

Hier können Sie auf beliebigen Clients die Dienste stoppen und starten. Dies sind bei Trend Micro: *tmlisten* und *nrtscan*



Führen Sie als erstes eine Abfrage aus, die Ihnen alle Rechner in Ihrem Netzwerk anzeigt, auf denen Trend Micro installiert ist. Wie das geht, können Sie in den Abschnitten *Browse* oder *Query Management* nachlesen.

Sobald Ihre Abfrage ausgeführt ist, können Sie die gewünschten Clients auswählen. Aktivieren Sie dazu das Auswahlkästchen ☐ in der betreffenden Zeile ☒.

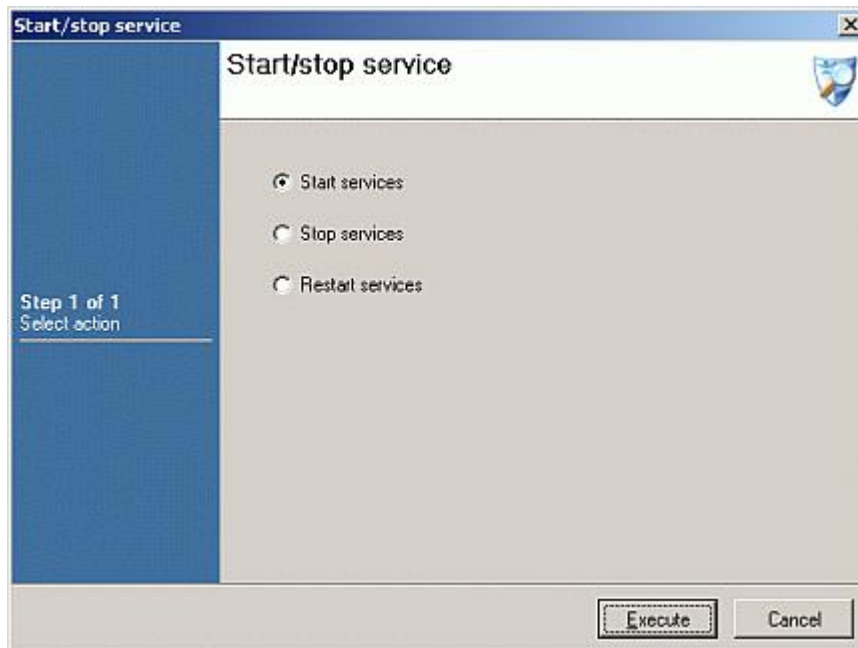
Beachten Sie, dass Sie nur Clients auswählen können, auf denen der ACMP Agent installiert ist.

Wenn Sie alle Clients ausgewählt haben, klicken Sie auf das Symbol  (Start/Stop Trend Micro Services(Ctrl+E) [Starte/Stoppe Trend Micro-Dienste]).

Es öffnet sich das Fenster *Start/stop TrendMicro-services*.

### Start/stop Trend Micro-services

Abhängig von Ihren Rechten (siehe: Handbuch ACMP Kapitel: *User management*) stehen Ihnen bis zu drei so genannte Radio-Schalter zur Auswahl:



- ☒ *Start Services [Starte die Dienste]*
- ☐ *Stop Services [Stoppe die Dienste]*
- ☐ *Restart Services [Starte die Dienste neu]*

Mit *Cancel* verlassen Sie das Fenster, ohne die Aktion auszulösen. Mit *Execute* wird die ausgewählte Aktion gestartet.

Die Anweisungen für jeden Rechner werden nun in eine Warteschlange gestellt und abgearbeitet, sobald der betreffende Rechner wieder Verbindung zum ACMP Server aufnimmt. Im Programm **Queue** können Sie überprüfen, ob Ihre Anweisungen bereits ausgeführt worden sind oder nicht.

## 1.4. Anhang

Diese Liste enthält alle Daten, die vom AVdetective erfasst werden. Der Aufbau der Liste entspricht genau der Struktur, die Sie vom Erstellen von Abfragen her kennen.

### AVDETECTIVE

#### AV-Solution FProt

FProt Language	FProt Sprache
FProt Scanner Path	FProt Scanner Pfad
FProt Installed	FProt installiert
FProt Package Name	FProt Paket Name
FProt Package Version	FProt Paket Version
FProt Application Status	FProt Applikationsstatus
FProt Installation Path	FProt Installtionspfad
FProt Run On Startup	FProt läuft beim Start
FProt Run Expired Tasks	FProt führe abgelaufene Aufgaben aus
FProt Reportfile Path	FProt Pfad der Reportdatei
FProt Show Icon	FProt zeige Symbol
FProt E-Mail Address	FProt E-Mail Adresse
FProt E-Mail Server	FProt E-Mail Server
FProt Scheduler Path	FProt Pfad des Zeitplanungsprogramms

#### AV-Solution FSecure

FSecure Authentication Agent	FSecure Authentifikationsagent
FSecure Back Web	FSecure BackWeb
FSecure Back Web Agent	FSecure BackWeb Agent
FSecure Back Web LAN Access	FSecure BackWeb LAN Zugang
FSecure Gate Keeper Handler	FSecure Gate Keeper Steuerung
FSecure Gate Keeper Start	FSecure Gate Keeper Start
FSecure Installed	FSecure installiert
FSecure Language	FSecure Sprache
FSecure Management Agent	FSecure Management Agent
FSecure Net Request Broker	FSecure Net Request Broker
FSecure Path	FSecure Pfad
FSecure Scan Manager	FSecure Scan Manager
FSecure Settings And Descriptions	FSecure Einstellungen und Beschreibungen
FSecure Standalone	FSecure Standalone
FSecure Version	FSecure Version

#### AV-Solution McAfee

NAI Installed	NAI installiert
NAI Service Name	NAI Name des Dienstes
NAI Service Started	NAI Dienst gestartet
NAI Status Of Service	NAI Status des Dienstes
McAfee Version Of Scanengine	McAfee Version der Scanengine
McAfee Product Name	McAfee Produktname
NAI Product Name	NAI Produktname
McAfee Language	McAfee Sprache
NAI Language	NAI Sprache
McAfee Install Path	McAfee Installationspfad
McAfee Program Version	McAfee Programmversion
NAI Version	NAI Version
AV Solution Name	AV Lösungsname
AV Sync. Manager Started	AV Sync. Manager gestartet

AV Sync. Manager Status	AV Sync. Manager Status
NAI Software ID	NAI Software ID
McAfee Date Of DAT-File	McAfee Datum der DAT-Datei
McAfee DAT Folder	McAfee DAT Ordner
McAfee Version Of DAT-File	McAfee Version der DAT-Datei
McAfee Installed	McAfee installiert
McAfee Service Name	McAfee Name des Dienstes
McShield Started	McShield gestartet
McShield Status	McShield Status
McAfee Serial Number	McAfee Seriennummer
NAI Installation Path	McAfee Installationspfad
McAfee Install Date	McAfee Installationsdatum

## AV-Solution Office Scan

TM Running	TM läuft
TM Real Time Protection Enabled	TM Echtzeitschutz aktiviert
TM Server	TM Server
TM Server Port	TM Server Port
TM Database Path	TM Datenbankpfad
TM Domain	TM Domäne
TM Application Path	TM Applikationspfad
TM Scan Engine Version	TM Version der Scan-Engine
TM Pattern Version	TM (Viren-)Muster Version
TM Real Time Scan Started	TM Echtzeit-Scan gestartet
TM Real Time Scan Status	TM Echtzeit-Scan Status
TM Install Time	TM Installationszeit
TM Install Date	TM Installationsdatum
TM Program Version	TM Programmversion
TM Filter Version	TM Filterversion
TM Installed	TM installiert
TM Listener started	TM Listener gestartet
TM Listener Status	TM Listener Status

## AV-Solution Symantec

SAV Service Status	SAV Status des Dienstes
SAV Version	SAV Version
SAV Quar. Forwarding enabled	SAV Quarantäne-Weiterleitung aktiviert
SAV Used Quar. Server	SAV benutzter Quarantäneserver
SAV Real Time Protection	SAV Echtzeitschutz
SAV Version Number	SAV Versionsnummer
SAV Previous Definitions	SAV bisherige (Viren-)Definitionen
SAV LiveUpdate Enabled	SAV LiveUpdate aktiviert
SAV Update Pattern Manually	SAV (Viren-)Muster manuell updaten
SAV Client Type	SAV Clienttyp
SAV Process GRC	SAV führe GRC(.dat) aus
SAV Connected	SAV verbunden
SAV Is Parent Server	SAV ist Parent Server
SAV Parent Server	SAV Parent Server
SAV Current Definitions	SAV aktuelle (Viren-)Definitionen
SAV Service Name	SAV Name des Dienstes
SAV Servergroup	SAV Servergruppe
SAV Installed	SAV installiert
SAV Service Started	SAV Dienst gestartet



## Index

## - S -

### - A -

Anhang	27
AVdetective	7
FProt	7
Fsecure	7
McAfee	7
Reports	7
Symantec	7
Trend Micro	7

### - E -

Einleitung	6
Was ist der AVdetective?	6

### - F -

FProt	8
Reports	8
Start/stop application	8
FSecure	11
Reports	11

### - L -

Lizenzbestimmungen	4
Copyright	4
Haftungsausschluss	4
Warenzeichen	4

### - M -

McAfee	12
Reports	12
Start/stop service	12

### - R -

Reports	7, 8, 11, 12, 15, 24
Manage Reports	7, 8, 11, 12, 15, 24

Send grc.dat	16
Back	16
Cancel	16
Edit GRC.dat	16
Execute	16
Next	16
Query Management	16
Queue	16
Select from filesystem	16
Select from scanned clients	16
Send virus definitions	19
Back	19
Cancel	19
Execute	19
Next	19
Query Management	19
Queue	19
Select from filesystem	19
Select from scanned clients	19
Start/Stop FProt-application	9
Cancel	9
Execute	9
Query Management	9
Queue	9
RealTime Protector	9
Restart FProt Applications	9
Start FProt Applications	9
Stop FProt Applications	9
Start/stop McAfee-services	13
AV Sync. Manager	13
Cancel	13
Execute	13
McShield	13
Query Management	13



Start/stop McAfee-services	13
Queue	13
Restart Services	13
Start Services	13
Stop Services	13
Start/Stop Symantec-services	22
Cancel	22
Execute	22
Norton AntiVirus Server-Dienst	22
Query Management	22
Queue	22
Restart Services	22
Start Services	22
Stop Services	22
Start/stopTrendMicro-services	25
Cancel	25
Execute	25
ntrtscan	25
Query Management	25
Queue	25
Restart Services	25
Start Services	25
Stop Services	25
tmlisten	25
Symantec	15
Reports	15
Send grc.dat	15
Send virus definitions	15
Start/stop service	15
 <b>- T -</b>	
Trend Micro	24
Reports	24
Start/stop service	24

