

Inhalt

Allgemeines	2
Vor der Installation	7
Installation	11
G Data ManagementServer	13
G Data Administrator	18
G Data Client	81
G Data WebAdministrator	87
Firewall	89
Anhang	107

Allgemeines

In Zeiten der weltweiten Vernetzung und der daraus resultierenden massiven Sicherheitsrisiken, geht das Thema *Virenschutz* nicht länger nur IT-Fachleute an. Es muss vielmehr im Rahmen eines umfassenden, unternehmensweiten Risikomanagements auf höchster Managementebene betrachtet werden. Ein durch Viren verursachter Ausfall des Computernetzwerkes trifft ein Unternehmen an seiner empfindlichsten Stelle. Die Folgen: Stillstand lebenswichtiger Systeme, Verlust erfolgsrelevanter Daten, Ausfall wichtiger Kommunikationskanäle. Computerviren können einem Unternehmen Schäden zufügen, von denen es sich nie mehr erholt! *G Data* bietet Ihnen High-End Virenschutz für Ihr gesamtes Netzwerk. Die führende Sicherheitsleistung der *G Data*-Produkte wird seit Jahren in zahlreichen Tests mit Traumnoten prämiert. *G DATA ClientSecurity* setzt konsequent auf zentrale Konfiguration und Verwaltung sowie größtmögliche Automatisierung. Alle Clients, ob Workstation, Notebook oder Fileserver, werden zentral gesteuert. Sämtliche Client-Prozesse laufen transparent im Hintergrund. Automatische Internet Updates sorgen im Ernstfall einer Virenattacke für extrem kurze Reaktionszeiten und die preisgekrönte Client-Firewall rundet den Komplettschutz ab. Die zentrale Steuerung mit dem *G Data ManagementServer* ermöglicht Installation, Einstellungen, Updates, Fernsteuerung und Automatik für das gesamte Netzwerk. Das entlastet den Systemadministrator und spart Zeit und Kosten.

G Data PremiumHotline

Die **PremiumHotline** für *G Data Mehrfach- und Netzwerklicenzen* steht allen registrierten Business-Kunden jederzeit zur Verfügung. .

Telefon: 0180 11 55 190

(3,9 Cent/Minute a. d. deutschen Festnetz. Anrufe aus dem Mobilfunknetz können bis zu 60 Cent pro Minute kosten.)

Telefax: 0234 9762 162

E-Mail: business-support@gdata.de

Die **Registriernummer** finden Sie auf der Rückseite des Benutzerhandbuchs. Wenn Sie die Software online gekauft haben, erhalten Sie die Registriernummer in einer gesonderten E-Mail. Über das **Online-Registrierungsformular** können Sie diese eingeben und erhalten auf diese Weise sofort online ein Kennwort, mit dem Sie Ihre persönlichen Internet Updates downloaden können. Viele Fragen sind auch schon in der **Online-Datenbank für häufig gestellte Fragen (FAQ)** beantwortet worden:

www.gdata.de

Überprüfen Sie vor dem Gespräch mit der **Hotline** bitte, wie Ihr Computer/ Netzwerk ausgestattet ist. Wichtig sind dabei vor allem folgende Informationen:

- die **Versionsnummern** des Administrators und des ManagementServers (diese finden Sie im **Hilfe**-Menü der Administrator-Software)
- die **Registrierungsnummer** oder den **Benutzernamen** für das **Internet Update**. Die Registriernummer befindet sich auf der Rückseite des Benutzerhandbuchs. Der Benutzername wird Ihnen bei der **Online-Registrierung** übermittelt.
- genaue Windows-Version (Client/Server)
- zusätzlich installierte Hard- und Softwarekomponenten (Client/Server)

Mit diesen Angaben wird das Gespräch mit den Hotline-Mitarbeitern kürzer, effektiver und erfolgreicher verlaufen. Bitte richten Sie es für die Beratung möglichst so ein, dass Telefon in der Nähe eines Rechners zu haben, auf dem Sie die Administratorsoftware für den Managementserver installiert haben.

PremiumSupport-Verlängerungen

Mit dem **PremiumSupport** erhalten Sie mit Durchführung der Online-Registrierung für ein Jahr lang stündlich aktualisierte Virendaten per Internet Update zur Virenbekämpfung. Auf Wunsch erhalten Sie weitergehende Informationen (z.B. über Upgrades der ManagementServer-Software und aktuelle Virenwarnungen) per E-Mail. Der PremiumSupport kann befristet oder unbefristet abgeschlossen oder verlängert werden. Kontaktieren Sie uns einfach unter

Telefon: 0234 / 9762-170 (Mo. bis Fr. von 9 bis 18 Uhr)

Telefax: 0234 9762 299

E-Mail: b-vertrieb@gdata.de

- ?** Selbstverständlich wird unser **Business-Vertrieb** Ihre Anfragen bestmöglich bearbeiten und Sie individuell beraten. Haben Sie bitte Verständnis dafür, dass technische Fragen zur vorliegenden Software nur über unser **ServiceCenter** bearbeitet werden können.

Emergency-AntiViren Service

Sollten Sie einen neuen Virus oder ein unbekanntes Phänomen feststellen, senden Sie uns bitte in jedem Fall diese Datei über die Quarantäne-Funktion der *G Data Software*. Wir analysieren den Virus und werden Ihnen möglichst schnell ein Gegenmittel zur Verfügung stellen. Selbstverständlich behandeln wir Ihre eingesandten Daten höchst vertraulich und diskret.

- ?** Die Rücksende-Adresse für Dateien, die vom Emergency-AntiViren Service repariert wurden, können Sie im Bereich **E-Mail-Einstellungen** definieren.

Lizenzvereinbarung

Nachfolgend sind die Vertragsbedingungen für die Benutzung der Software **G DATA ClientSecurity** durch den Endverbraucher (im Folgenden auch: Lizenznehmer), aufgeführt.

1. Gegenstand des Vertrages: Gegenstand des Vertrages ist die auf einem Datenträger aufgezeichnete oder aus dem Internet geladene *G Data Software* und die Programmbeschreibung. Sie werden im Folgenden auch als Software bezeichnet. *G Data* macht darauf aufmerksam, dass es nach dem Stand der Technik nicht möglich ist, Software so zu erstellen, dass sie in allen Anwendungen und Kombinationen fehlerfrei arbeitet.
2. Umfang der Benutzung: *G Data* gewährt Ihnen für die Dauer dieses Vertrages das einfache, nicht ausschließliche und persönliche Recht (im Folgenden auch als Lizenz bezeichnet), die Software auf einer vertraglich vereinbarten Anzahl von Computern zu benutzen. Die Nutzung der Software kann sowohl in Form einer Installation auf einer physikalischen Einheit (CPU), einer virtuellen / emulierten Maschine (wie z.B. VMWare) oder einer Instanz einer Terminal Session erfolgen. Ist dieser Computer ein Mehrbenutzersystem, so gilt dieses Benutzungsrecht für alle Benutzer dieses einen Systems. Als Lizenznehmer dürfen Sie Software in körperlicher Form (d.h. auf einem Datenträger abgespeichert) von einem Computer auf einen anderen Computer übertragen, vorausgesetzt, dass sie zu irgendeinem Zeitpunkt immer nur auf der vertraglich vereinbarten Anzahl von Computern genutzt wird. Eine weitergehende Nutzung ist nicht zulässig.

3. Besondere Beschränkungen: Dem Lizenznehmer ist untersagt, ohne vorherige schriftliche Einwilligung von *G Data* die Software abzuändern.

4. Inhaberschaft an Rechten: Sie erhalten mit dem Erwerb des Produktes nur Eigentum an dem körperlichen Datenträger, auf dem die Software aufgezeichnet ist und auf die mittels Supportrahmen vereinbarten Updates. Ein Erwerb von Rechten an der Software selbst ist nicht damit verbunden. *G Data* behält sich insbesondere alle Veröffentlichungs-, Vervielfältigungs-, Bearbeitungs- und Verwertungsrechte an der Software vor.

5. Vervielfältigung: Die Software und das zugehörige Schriftmaterial sind urheberrechtlich geschützt. Das Anfertigen einer Sicherheitskopie, die jedoch nicht an Dritte weitergegeben werden darf, ist erlaubt.

6. Dauer des Vertrages: Der Vertrag läuft auf unbestimmte Zeit. Diese Laufzeit umfasst nicht den Bezug von Updates. Das Recht des Lizenznehmers zur Benutzung der Software erlischt automatisch und ohne Kündigung, wenn er eine Bedingung dieses Vertrages verletzt. Bei Beendigung des Nutzungsrechtes ist er verpflichtet, die Original CD-ROM einschließlich etwaiger UPDATES/UPGRADES sowie das schriftliche Material zu vernichten.

7. Schadensersatz bei Vertragsverletzung: *G Data* macht darauf aufmerksam, dass Sie für alle Schäden aufgrund von Urheberrechtsverletzungen haften, die *G Data* aus einer Verletzung dieser Vertragsbestimmungen durch Sie entstehen.

8. Änderungen und Aktualisierungen: Es haben jeweils unsere neuesten Servicebedingungen Gültigkeit. Die Servicebedingungen können jederzeit, ohne Ankündigung und ohne Angabe von Gründen geändert werden.

9. Gewährleistung & Haftung von *G Data*:

a) *G Data* gewährleistet gegenüber dem ursprünglichen Lizenznehmer, dass zum Zeitpunkt der Übergabe der Software der eventuell vorhandene Datenträger (CD-ROM), auf dem die Software aufgezeichnet ist, unter normalen Betriebsbedingungen und bei normaler Instandhaltung in Materialausführung fehlerfrei ist.

b) Sollte der Datenträger oder der Download aus dem Internet fehlerhaft sein, so kann der Erwerber Ersatzlieferung während der Gewährleistungszeit von 6 Monaten ab Lieferung verlangen. Er muss dazu den Erwerb der Software belegen.

c) Aus den vorstehend unter 1. genannten Gründen übernimmt *G Data* keine Haftung für die Fehlerfreiheit der Software. Insbesondere übernimmt *G Data* keine Gewähr dafür, dass die Software den Anforderungen und Zwecken des Erwerbers genügt oder mit anderen von ihm ausgewählten Programmen zusammenarbeitet. Die Verantwortung für die richtige Auswahl und die Folgen der Benutzung der Software sowie der damit beabsichtigten oder erzielten Ergebnisse trägt der Erwerber. Das gleiche gilt für das die Software begleitende, schriftliche Material. Ist die Software nicht im Sinne von 1. grundsätzlich brauchbar, so hat der Erwerber das Recht, den Vertrag rückgängig zu machen. Das gleiche Recht hat *G Data*, wenn die Herstellung von im Sinne von 1. brauchbarer Software mit angemessenem Aufwand nicht möglich ist.

d) *G Data* haftet nicht für Schäden, es sei denn, dass ein Schaden durch Vorsatz oder grobe Fahrlässigkeit seitens *G Data* verursacht worden ist. Gegenüber Kaufleuten wird auch die Haftung für grobe Fahrlässigkeit ausgeschlossen. Die maximale Entschädigungsleistung beträgt den Kaufpreis der Software.

10. Gerichtsstand: Alleiniger Gerichtsstand bei allen aus dem Vertragsverhältnis mittelbar oder unmittelbar sich ergebenden Streitigkeiten ist der Firmensitz von *G Data*.

11. Schlussbestimmungen: Sind einzelne Bestimmungen dieser Lizenzvereinbarung ungültig, so bleiben die übrigen Bestimmungen wirksam. Anstelle der ungültigen Bestimmung gilt eine ihrem wirtschaftlichen Zweck möglichst nahekommende, wirksame Bestimmung als vereinbart.



Copyright © 2009 G Data Software AG

Engine A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2009 BitDefender SRL.

Engine B: © 2009 Alwil Software

OutbreakShield: © 2009 Commtouch Software Ltd.

[G DATA ClientSecurity - 12.11.2009, 14:02]

Vor der Installation

Bitte führen Sie bei akutem Virenverdacht auf den betroffenen Rechnern erst einen **BootScan** durch.

- Installieren Sie dann den **ManagementServer** auf Ihrem Server. Bei der Installation des ManagementServers wird automatisch der **Administrator** auf dem Server installiert. Mit diesem Programm können Sie den Managementserver vom Server-Rechner aus steuern. Um den optimalen Schutz zu gewährleisten sollte der Rechner immer erreichbar (eingeschaltet) sein und für das automatische Laden der Virensignaturen über einen Internetzugang verfügen. Sie müssen den Managementserver also nicht unbedingt auf Ihrem zentralen Fileserver installieren.
- Führen Sie nun bitte die **Online-Registrierung** durch. Ohne eine Online-Registrierung können Sie die Aktualisierung der Virendatenbanken via Internet nicht durchführen.
- Beim ersten Start des Administrators auf dem Server startet der **Einrichtungsassistent**. Hiermit können Sie die **Client-Software** auf den gewünschten Clients in Ihrem Netzwerk direkt installieren, ohne diese Installation auf allen Clients einzeln auszuführen.
- Sollten sich Probleme bei der **Remote-Installation** der Clients ergeben, können Sie die Client-Software natürlich auch von Hand oder halbautomatisch auf den Clients installieren. Damit auch Ihr Server vor Virenbefall geschützt ist, sollten Sie die Client-Software natürlich auch auf Ihrem Server installieren.
- Nun können Sie Virenprophylaxe und -bekämpfung, sowie Internet Updates der **G Data Client- und Serversoftware** einfach über den Administrator zentral durchführen, in dem Sie z.B. den **G Data Wächter** für die fortlaufende Kontrolle verwenden oder Scanjobs definieren, die Ihr Netzwerk regelmäßig auf Virenbefall durchleuchten.
- Sollten Sie einmal ein Problem *vor Ort* lösen müssen, können Sie die Administrator-Software einfach und schnell auf jedem Client installieren und haben auch von dort aus vollen Zugriff auf den ManagementServer.

Systemvoraussetzungen

Das *G Data-System* setzt auf das **TCP/IP-Protokoll** auf und nutzt dies sowohl zur Kommunikation von Client- und Server-Rechnern untereinander, als auch für die Online-Verbindung zum *G Data UpdateServer*. Folgende Mindestanforderungen werden an die Clients- bzw. Server gestellt:

- **G Data ManagementServer**: PC mit mind. 128 MB RAM, Internetzugang. Mögliche Betriebssysteme: Windows 7, Windows Vista, Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 (vorzugsweise die Serverversionen, auch x64 Edition),
- **G Data Clients**: PC mit mind. 256 MB RAM. Mögliche Betriebssysteme: Windows 7, Windows Vista, Windows XP, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 (auch x64 Edition),

? Für **Linux-Rechner**, die als Fileserver arbeiten und verschiedenen Clients Windows-Freigaben (über das **SMB-Protokoll**) zur Verfügung stellen, kann manuell ein Modul installiert werden, das den Zugriff auf die Freigaben kontrolliert und bei jedem Zugriff einen Scan auf die Datei ausführt, so dass keine Malware vom **Samba-Server** auf die Windows-Clients (und umgekehrt) gelangen kann.

BootScan

Der **BootScan** hilft Ihnen dabei, Viren zu bekämpfen, die sich vor der Installation der Antivirensoftware auf Ihrem Rechner eingenistet haben und möglicherweise die Installation der **G Data Software** unterbinden möchten. Dazu gibt es eine spezielle Programmversion der **G Data Software**, die schon vor dem Start von Windows ausgeführt werden kann.

? **Was mache ich, wenn mein Computer nicht von CD-ROM bootet?** Sollte Ihr Computer nicht von CD/DVD-ROM booten, kann es sein, dass Sie diese Option erst einstellen müssen. Dies erfolgt im sogenannten **BIOS**, einem System, das noch vor Ihrem Windows-Betriebssystem automatisch gestartet wird. Um im BIOS Änderungen vorzunehmen, führen Sie bitte folgende Schritte durch:

1. Schalten Sie Ihren Computer aus.
2. Starten Sie Ihren Computer wieder. Üblicherweise gelangen Sie zum BIOS-Setup, indem Sie beim Hochfahren (= Booten) des Rechners die **Entf**-Taste (manchmal auch die Taste **F2** oder **F10**) drücken.

3. Wie Sie die Einstellungen in Ihrem BIOS-Setup im Einzelnen ändern, ist von Computer zu Computer unterschiedlich. Lesen Sie bitte in der Dokumentation Ihres Computers. Im Ergebnis sollte die Bootreihenfolge **CD/DVD-ROM; C:** lauten, d.h. das CD/DVD-ROM-Laufwerk wird zum ***1st Boot Device*** und die Festplatten-Partition mit Ihrem Windows-Betriebssystem zum ***2nd Boot Device***.
4. Speichern Sie die Änderungen und starten Sie Ihren Computer neu. Jetzt ist Ihr Computer bereit für einen BootScan.

Beim **BootScan** gehen Sie bitte folgendermaßen vor:

- 1a** **BootScan mit der Programm-CD:** Sie verwenden die **G Data Programm-CD** und booten mit dieser Ihren Rechner. - Legen Sie die **G Data Software CD** in das Laufwerk. Klicken Sie auf dem sich öffnenden Startfenster auf **Abbrechen** und schalten Sie den Computer aus.
- 1b** **BootScan mit G Data Software, die Sie aus dem Internet heruntergeladen haben:** Sie brennen sich über den Eintrag **G Data BootCD erstellen** in der **G Data Software-Programmgruppe** eine neue BootCD. - Legen Sie Ihre selbstgebrannte BootCD in das Laufwerk. Klicken Sie auf dem sich öffnenden Startfenster auf **Abbrechen** und schalten Sie den Computer aus.

Nach dem ersten Schritt verläuft der BootScan für alle drei Varianten identisch:

- 2** Starten Sie den Computer neu. Es erscheint das Startmenü des **G Data BootScans**.



- 3** Wählen Sie mit den Pfeiltasten die Option **G Data BootCD** und bestätigen die Auswahl mit **Enter**. Es wird nun ein Linux-Betriebssystem von der CD gestartet und es erscheint eine **G Data Spezialversion** für BootScans.

? Falls Sie Probleme mit der Ansicht der Programmoberfläche haben, starten Sie den Rechner erneut und wählen bitte die Option **G Data BootCD – Alternativ** aus.

4 Das Programm schlägt nun vor, die Virensteckbriefe (auch **Virensignaturen** genannt) zu aktualisieren.

5 Klicken Sie hier auf **Ja** und führen Sie das Update durch. Sobald die Daten über das Internet aktualisiert wurden, erscheint die Meldung **Update erledigt**. Verlassen Sie nun den Update-Bildschirm mit Anklicken der **Schließen**-Schaltfläche.

? Das automatische **Internet Update** steht Ihnen dann zur Verfügung, wenn Sie einen **Router** verwenden, der IP-Adressen automatisch vergibt (**DHCP**). Sollte das Internet Update nicht möglich sein, können Sie den **BootScan** auch mit alten Virensteckbriefen durchführen. Dann sollten Sie allerdings nach der Installation der **G Data Software** möglichst bald einen neuen BootScan mit aktualisierten Daten durchführen.

6 Nun sehen Sie die Programmoberfläche. Klicken Sie auf den Eintrag **Überprüfe Computer** und Ihr Computer wird nun auf Viren und Schadsoftware untersucht. Dieser Vorgang kann je nach Rechnerart und Festplattengröße eine Stunde oder länger dauern.

7 Sollte die **G Data Software** Viren finden, entfernen Sie die bitte mit Hilfe der im Programm vorgeschlagenen Option. Nach einer erfolgreichen Entfernung des Virus steht Ihnen die Originaldatei weiter zur Verfügung.

8 Nach Abschluss der Virenüberprüfung verlassen Sie nun bitte das System, in dem Sie auf die **Beenden**-Schaltfläche klicken und anschließend **Neu Starten** auswählen.



Die **Beenden**-Schaltfläche befindet sich unten rechts in der Linux-Programmieroberfläche.

9 Entfernen Sie die **G Data Software CD** aus dem Laufwerk, sobald sich die Lade Ihres Laufwerks öffnet.

10 Schalten Sie ihren Computer wieder aus und starten Sie ihn erneut. Nun startet Ihr Computer wieder mit Ihrem Standard-Windows-Betriebssystem und sie haben die Gewähr, die reguläre **G Data Software** auf einem virenfreien System installieren zu können.

Installation

Die Installation der *G Data Windows-Version* ist ausgesprochen unkompliziert. Starten Sie einfach Ihr Windows und legen die *G Data CD-ROM* in Ihr CD-ROM-Laufwerk ein. Es öffnet sich automatisch ein Installationsfenster.

? Sollten Sie die **Autostart-Funktion Ihres CD-ROM-Laufwerks** nicht aktiviert haben, kann die *G Data Software* den Installationsvorgang nicht automatisch starten. Klicken Sie dann im **Start-Menü** von Windows auf **Ausführen**, tippen in dem erscheinenden Fenster **e:** **setup.exe** ein und klicken auf **OK**. Auf diese Weise öffnet sich ebenfalls der Einstiegsbildschirm für die *G Data Software-Installation*. Der Eintrag **e:** bezeichnet den Laufwerksbuchstaben Ihres CD-ROM-Laufwerks. Sollten Sie Ihr CD-ROM-Laufwerk auf einem anderen Laufwerksbuchstaben angemeldet haben, geben Sie statt **e:** bitte den entsprechenden Laufwerksbuchstaben an.

Schließen Sie bitte alle anderen Programme, bevor Sie mit der Installation der *G Data Software* beginnen. Es kann zu Fehlfunktionen oder einem Abbruch kommen, falls z.B. Programme geöffnet sind, die auf Daten zugreifen, die die *G Data Software* zur Installation benötigt.

- **Installieren:** Mit Klick auf diese Schaltfläche starten Sie die Installation der *G Data Software* auf Ihrem Computer,
- **Durchsuchen:** Über den Windows-Explorer können Sie hier die Verzeichnisse der CD-ROM sichten.
- **Abbrechen:** Über diesen Eintrag können Sie die den Autostart-Bildschirm schließen, ohne eine Aktion durchzuführen.

Nachdem Sie die Schaltfläche **Installieren** gedrückt haben, erscheint ein Bildschirm, in dem Sie auswählen können, welche der *G Data Software-Komponenten* Sie installieren wollen. Folgende Installationsmöglichkeiten stehen Ihnen zur Verfügung:

- **G Data ManagementServer:** Als erstes sollten Sie den **Managementserver** auf dem Computer installieren, den Sie als Antiviren-Server verwenden möchten. Der Managementserver ist das Herzstück der *G Data Architektur*. Er verwaltet die Clients, fordert neueste Software- und Virensignaturupdates automatisch vom *G Data UpdateServer* an und steuert die Antiviren-Technologie im Netzwerk. Mit der Installation des ManagementServers wird automatisch auch auf dem Server die **Administrator-Software** aufgerufen, mit der Sie den ManagementServer steuern können.
- **G Data Administrator:** Der **Administrator** ist die Steuerungssoftware für den Managementserver; die - vom Systemverwalter zentral gesteuert - das gesamte Netz sichert. Der Administrator kann passwortgeschützt von jedem Rechner unter Windows gestartet werden.
- **G Data Client:** Die **Client-Software** stellt den Virenschutz für die Clients her und führt die Jobs vom Managementserver ohne Bedienungsfläche im Hintergrund aus. Die Installation der Client-Software erfolgt in der Regel zentral für alle Clients über den Administrator.
- **Boot-CD-Erstellung:** Mit Hilfe des Boot-CD Wizards können Sie eine bootfähige CD zur grundlegenden Überprüfung Ihres Rechners noch vor dem Start des Windows-Betriebssystems erstellen. Dazu werden die aktuellen Virensignaturen verwendet. Mit einer erstellten Boot-CD können Sie einen **BootScan** auch ohne die Original *G Data-Software-CD* durchführen. Lesen Sie hierzu bitte auch das Kapitel **BootScan**.
- **G Data WebAdministrator:** Der **Webadministrator** ist eine Web basierte Steuerungssoftware für den Managementserver. Er kann mit Hilfe eines Web-Browsers gestartet werden.
- **G Data Firewall:** Mit der **Firewall** können Sie Clients zusätzlich mit einer Firewall schützen. Wenn Sie die Firewall manuell auf dem jeweiligen Client installieren, muss vorher die *G Data Client-Software* auf diesen Client eingespielt worden sein, da diese die Kommunikation der Firewall mit dem Managementserver regelt.



Hinweise und Informationen darüber, was Sie bei der Installation der jeweiligen Modul beachten sollten, erhalten Sie in den Kapiteln zum jeweiligen Softwarekomponente.

G Data ManagementServer

Der **Managementserver** ist das Herzstück der *G Data Architektur*. Er verwaltet die Clients, fordert neueste Software- und Virensignaturupdates automatisch vom *G Data UpdateServer* an und steuert die Virentechnologie im Netzwerk. Zur Kommunikation mit den Clients setzt der Managementserver auf **TCP/IP** auf. Für **Clients**, die offline sind, werden die Jobs automatisch gesammelt und bei der nächsten Online-Sitzung synchronisiert. Der Managementserver verfügt über einen zentralen **Quarantäne**-Ordner, in dem Sie optional verdächtige Dateien verschlüsselt sicherstellen lassen, löschen, desinfizieren oder gegebenenfalls an den **Emergency-AntiViren Service** weiterleiten können. Der Managementserver wird über die **Administrator-Software** gesteuert.



Wenn Sie die Administrator-Software beenden, schließen Sie damit nicht den Managementserver. Dieser bleibt weiterhin im Hintergrund aktiv und steuert die Prozesse, die von Ihnen für die Clients eingestellt wurden.

Installation des Managementservers



Legen Sie die *G Data-CD-ROM* ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data ManagementServer** durch einen Klick auf die nebenstehende Schaltfläche.

Begrüßungsbildschirm

Im folgenden Begrüßungsbildschirm werden Sie darüber informiert, dass Sie im Begriff sind den Managementserver auf Ihrem System zu installieren. Bitte schließen Sie spätestens jetzt alle offenen Anwendungen in Ihrem Windows-System, da diese sonst zu Problemen bei der Installation führen könnten. Klicken Sie auf **Weiter** um mit der Installation fortzufahren.

Lizenzvereinbarung

Lesen Sie sich nun bitte die Lizenzvereinbarung zur Nutzung dieser Software durch, wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** und klicken dann auf **Weiter**, wenn Sie den Vereinbarungen in dieser Form zustimmen.

Zielordner

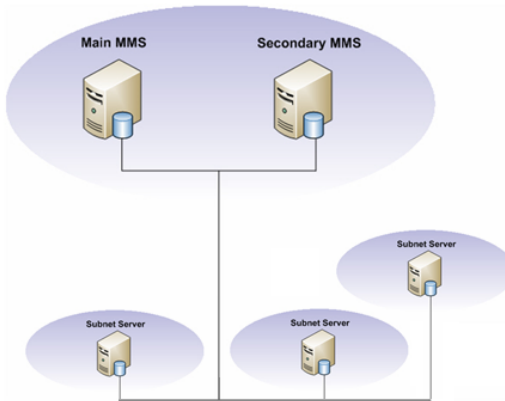
Der nächste Bildschirm ermöglicht Ihnen die Auswahl des Ortes, an dem die Daten des Managementserver abgespeichert werden sollen. Sollten Sie einen individuellen Zielordner auswählen wollen, haben Sie die Möglichkeit über die Schaltfläche **Ändern** eine Verzeichnisansicht zu öffnen, in der Sie ein anderes Verzeichnis auswählen oder auch neu anlegen können.

Server-Typ auswählen

Sie haben bei der Auswahl der Server-Typen folgende Optionen:

- **Einen Main-Server installieren:** Grundlegend muss der *G Data ManagementServer* als **Main-Server (Main-MMS)** angelegt werden. Der Main-Server stellt die zentrale Konfigurations- und Verwaltungsinstanz der netzwerkbasieren Virenschutz-Architektur dar. Die zu schützenden Rechner werden über den Managementserver mit den jeweils aktuellsten Virensignatur- und Programmupdates versorgt. Darüber hinaus werden sämtliche spezifischen Client-Einstellungen zentral am Managementserver vorgenommen.
- **Einen Secondary-Server installieren:** Bei Verwendung einer **SQL-Datenbank** ist es möglich einen **zweiten Server (Secondary MMS)** zu betreiben, der die gleiche Datenbank wie der Hauptserver benutzt. Falls der **Hauptserver** eine Stunde oder länger nicht erreichbar ist, werden die Clients sich automatisch mit dem Secondary MMS verbinden und von diesem Signaturupdates laden. Der Wechsel zurück zum Hauptserver erfolgt sobald dieser wieder verfügbar ist. Beide Server laden die Signaturupdates unabhängig voneinander.
- **Einen Subnet-Server installieren:** Bei großen Netzwerken ist es sinnvoll, den *G Data ManagementServer* auch als **Subnet-Server** zu betreiben. Subnet-Server dienen der Entlastung des Netzwerktraffics zwischen Clients und dem Main-MMS. Sie können in Subnetzwerken verwendet werden und verwalten dort die ihnen zugeordneten Clients. Die Subnet Server sind voll funktionsfähig, auch wenn Main- oder Secondary-Managementserver nicht erreichbar sind.

Schematisch sähe ein **Aufbau der Server-Typen** also in großen Netzwerken folgendermaßen aus: Subnet-Server bündeln einzelne Clients oder Client-Gruppen und geben Sie an den Main-Server weiter. Dieser wird von einem Secondary-Server unterstützt, der im Fall eines Ausfalls des Main-Servers als Backup fungiert.



Datenbank-Server

Wählen Sie nun bitte einen Datenbank-Server aus, den Sie installieren. Sie haben dabei die Möglichkeit, vorhandene **SQL-Server** zu verwenden, **Microsoft SQL-Express** oder eine **integrierte Datenbank** (z.B. für kleinere Netzwerke).

? Ein Server-Betriebssystem ist nicht zwingend notwendig. Die SQL-Variante bietet sich vor allem in größeren Netzwerken mit einer Client-Anzahl von > 50 an.

Computername

Überprüfen Sie nun den **Namen Ihres Computers**, auf dem Sie den Managementserver installieren. Dieser Rechner muss über den hier angegebenen Namen von den Clients im Netzwerk angesprochen werden können. Sollte hier nicht der korrekte Name angezeigt werden, ändern Sie die Angabe unter **Name** bitte entsprechend.

Installationsbeginn

Nun erfolgt die Installation des Managementserver. Die Installation wird mit einem Abschlussbildschirm gestartet. Klicken Sie auf **Installieren**.

Online-Registrierung

Spätestens vor der Durchführung eines **Internet Updates** müssen Sie sich beim *G Data UpdateServer* registrieren, um Ihre Zugangsdaten zu erhalten. Sie können dazu die Registrierung direkt während der Installation durchführen oder später durch Aufrufen der Funktion **Internet Update** unter **Start > Programme > G Data ManagementServer** durchführen. Betätigen Sie hier die Schaltfläche **Online-Registrierung**. Anschließend werden Sie nach Ihren Kundendaten und der Registriernummer gefragt.

? Sie finden die **Registriernummer** auf der Rückseite des Bedienungshandbuches. Sollten Sie die Software online erstanden haben, erhalten Sie die Registriernummer nach der Bestellung in einer gesonderten E-Mail.

? Bitte beachten Sie auch, dass natürlich eine **Internetverbindung** per Standleitung oder automatischem Einwahlverfahren bestehen oder erzeugt werden muss.

Geben Sie die Registriernummer einfach fortlaufend ohne Bindestriche in die entsprechenden fünf Eingabefelder ein. Bitte füllen Sie auch alle anderen Eingabefelder korrekt aus, da die Online-Registrierung nur mit sämtlichen hier abgefragten Angaben erfolgen kann. Unmittelbar nach der Online-Registrierung erhalten Sie in einer Infobox Ihren Benutzernamen und Ihr Passwort übermittelt.

? **Achtung:** Schreiben Sie Sich **Benutzernamen** und **Passwort** auf alle Fälle an einem sicheren Ort auf, damit sie Ihnen auch nach einer möglichen Neukonfiguration Ihres Computers zur Verfügung stehen. Sie können im Programmablauf erst fortfahren, nachdem Sie das Häkchenfeld mit der entsprechenden Aufforderung abgehakt haben.

? Die *G Data Software* übernimmt diese Angaben automatisch in das Internet Update-Formular. Nun haben Sie die Möglichkeit, Internet Updates durchzuführen.

? Die **Internet Updates** können Sie direkt aus der Administrator-Oberfläche heraus durchführen und sogar nach frei variierbaren Zeitschemata automatisieren.

Konfiguration Datenbanktyp

Dieser Installationsschritt erfolgt nur dann, wenn Sie den Managementserver reinstallieren oder auf dem Rechner noch eine **SQL-Datenbank** vorinstalliert ist. In der Regel reicht es, diese Info-Box durch Anklicken der **Schließen**-Schaltfläche zu schließen.

Installationsabschluss

Nach der Installation und nach jedem Neustart des Computers wird der Managementserver nun automatisch gestartet. Um Änderungen am Managementserver vorzunehmen können Sie unter **Start > (Alle) Programme > G Data ManagementServer** den Eintrag **G Data Administrator** auswählen und auf diese Weise das Administrationstool für den Managementserver starten.

G Data Administrator

Der **Administrator** ist die Steuerungssoftware für den Managementserver; die - vom Systemadministrator zentral gesteuert - das gesamte Netzwerk sichert. Der Administrator kann passwortgeschützt von jedem Rechner unter Windows gestartet werden. Als ferngesteuerte Jobs sind alle denkbaren Bedienungen von Virenscannern wie automatische Installationen, Software- und Virensignaturupdates, Virenanalysen (sofort oder periodisch), Wächterfunktionen und Änderungen von Einstellungen unternehmensweit möglich. Sie können das Administrator-Tool zur Steuerung des Managementsservers mit einem Klick auf den Eintrag **G Data Administrator** in der Programmgruppe **Start > (Alle) Programme > G Data ManagementServer** des Startmenüs aufrufen.

Installation des Administrators

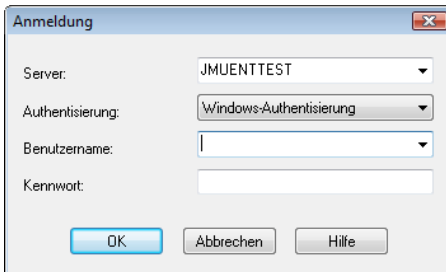


Bei einer Installation des **Managementservers** wird automatisch auf dem selben Rechner (nämlich dem Rechner, den Sie als **Server** verwenden möchten) der **Administrator** mitinstalliert. Sie müssen also die Installation des Administrators nicht zusätzlich durchführen. Die Installation des Administrators kann jedoch (unabhängig von der Installation auf dem Server) auch auf jedem Client-Rechner erfolgen. Auf diese Weise können Sie den Managementserver auch dezentral betreuen. Zur Installation des Administrators auf einem Client-Rechner legen Sie bitte die **G Data-CD-ROM** in das CD-ROM-Laufwerk des Client-Rechners und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data Administrator** durch einen Klick auf die nebenstehende Schaltfläche.

Im folgenden Begrüßungsbildschirm werden Sie darüber informiert, dass Sie im Begriff sind den Administrator auf Ihrem System zu installieren. Bitte schließen Sie spätestens jetzt alle offenen Anwendungen in Ihrem Windows-System, da diese sonst zu Problemen bei der Installation führen könnten. Klicken Sie auf **Weiter** um mit der Installation fortzufahren und folgen Sie dann den Installationsschritten, bei denen der Installationsassistent Sie unterstützt. Nach der Installation können Sie unter **Start > (Alle) Programme > G Data ManagementServer** den Eintrag **G Data Administrator** auswählen und auf diese Weise das Administrationstool für den Managementserver starten.

Anmeldung

Beim Starten des Administrators werden Sie nach dem **Server**, **Authentisierung**, **Benutzername** und **Kennwort** gefragt.



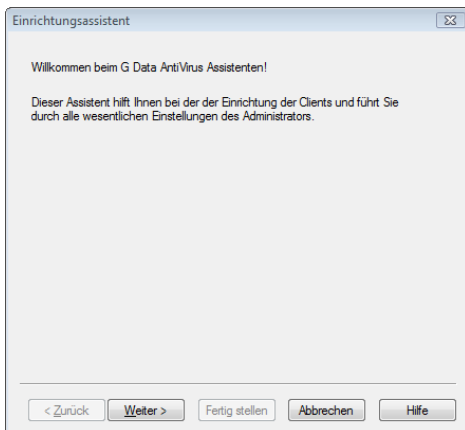
Geben Sie in dem Feld **Server**, den Namen des Computers ein, auf dem der Managementserver installiert wurde.

Wählen Sie nun Ihre **Authentisierung** aus.

- **Windows-Authentisierung:** Wenn Sie diese Authentisierungsvariante wählen, können Sie sich mit dem Benutzernamen und Passwort Ihres Administrator-Zugangs auf diesem Rechner anmelden, also dem **Windows-Benutzerkonto**.
- **Integrierte Authentisierung:** Mit der integrierten Authentisierung können Sie als Systemadministrator auch anderen Personen Zugriff auf den *G Data Administrator* geben. So können Sie z.B. ein spezielles Konto anlegen, dass nur Lese-Rechte beinhaltet. Diese zusätzlichen Konten können Sie über den die Funktion **Benutzerverwaltung** anlegen und verwalten.

Erster Programmstart (Einrichtungsassistent)

Beim ersten Start des Administrators wird automatisch der **Einrichtungsassistent** geöffnet. Er hilft bei der Einrichtung der Clients und führt Sie durch alle wesentlichen Einstellungen. Der Assistent kann auch nach der Erstinstallation über den Befehl **Einrichtungsassistent** im **Datei**-Menü jederzeit gestartet werden.



Aktivieren

Zunächst müssen alle Clients, die von der *G Data Software* überwacht werden sollen, aktiviert werden. Markieren Sie in der Liste die Computer und drücken Sie anschließend die Schaltfläche **Aktivieren**. Eventuell sind einige Computer nicht in der Liste enthalten (z. B. weil Sie lange nicht eingeschaltet waren oder keine Datei- bzw. Druckerfreigabe eingerichtet haben). Zum Aktivieren dieser Clients können Sie im Eingabefeld **Computer** den Namen eingeben und die Schaltfläche **Aktivieren** neben dem Eingabefeld drücken. Der Computer wird dann in die Liste aufgenommen. Drücken Sie auf **Weiter**, wenn Sie alle Clients aktiviert haben.

Installieren

Im folgenden Dialog ist das Häkchen bei **Client-Software automatisch auf den aktivierten Computern installieren** voreingestellt. Wenn Sie die Software auf den Client-Rechnern lieber manuell installieren möchten, entfernen Sie bitte hier das Häkchen.

Defaulteinstellungen

Im folgenden Dialog können Sie die Defaulteinstellungen für Wächter, Virenschutz und Client-Einstellungen ändern. Die Defaulteinstellungen sind so gewählt, dass Sie auch ohne Änderung direkt für die meisten Netzwerke verwendet werden können. Sollten diese Einstellungen letztendlich nicht optimal für Ihr Netzwerk sein, können Sie diese natürlich jederzeit nachträglich über die jeweiligen Arbeitsbereiche des Administrators ändern. Ausführliche Erläuterungen zu den einstellbaren Optionen finden Sie in den Erläuterungen zum Aufgabenbereich **Einstellungen**.

Internet Update

Der Managementserver kann über das Internet neue Virensignaturen und Programmdateien laden. Damit dieser Vorgang automatisch erfolgen kann, müssen Anmeldung und ggf. Einwahl automatisiert werden. Geben Sie zunächst hier die **Zugangsdaten** ein, die Sie bei der Online-Registrierung erhalten haben. Eine detaillierte Beschreibung zur Planung von Updateintervallen und der Durchführung grundlegender Einstellungen finden Sie im Kapitel **Internet Update**. Selbstverständlich können Sie das Internet Update auch jederzeit nachträglich über die Administrator-Programmoberfläche automatisieren.

E-Mail-Einstellungen

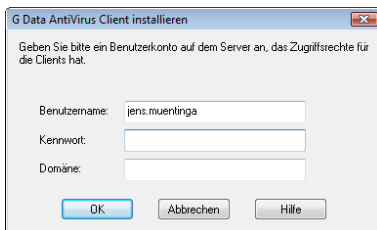
Der Managementserver kann potentiell infizierte Dateien zur Untersuchung an den **Emergency-AntiViren Service** schicken. Damit dies auf Knopfdruck erfolgen kann, müssen Sie dazu den Namen des **Mail-Servers**, die **Port-Nummer (SMTP)** und die **Absender-Adresse** angeben. Antworten des **Emergency-AntiViren Service** werden an diese E-Mail-Adresse zurückgesendet.

E-Mail-Benachrichtigung

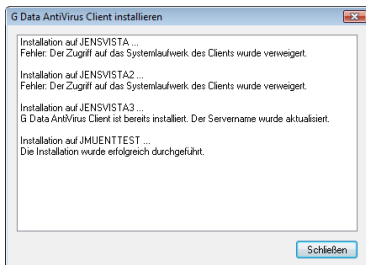
Der Managementserver kann den Administrator des Netzwerkes per E-Mail benachrichtigen, wenn auf einem der Clients ein Virus gefunden wird. Geben Sie dazu die E-Mail-Adresse des Empfängers der Warnmeldungen an. Über die **Mengenbegrenzung** können Sie verhindern, dass bei einem massiven Virenbefall Ihr E-Mail-Postfach von Benachrichtigungen *überschwemmt* wird. Drücken Sie auf **Fertig stellen**, um den Assistenten zu beenden.

Automatische Installation der Client-Software

Wenn Sie angegeben haben, dass die Client-Software automatisch installiert werden soll, werden Sie aufgefordert, ein Benutzerkonto auf dem Server anzugeben, das Zugriffsrechte für die Clients hat.



Nach der Bestätigung des Dialogs versucht der Managementserver die Client-Software auf allen aktivierten Computern zu installieren. Ein Info-Bildschirm informiert Sie dabei über den Fortschritt der Installation und eventuelle Probleme.

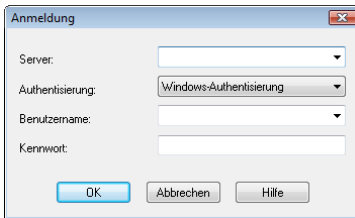


? Sollte es Probleme bei der **Remote-Installation** der **G Data Clients** über den Administrator geben, gibt es auch die Möglichkeit, die Client-Software manuell oder halbautomatisch auf den Clientrechnern zu installieren. Lesen Sie hierzu bitte auch die Kapitel **G Data Client installieren**.

? Sie können auch eine spezielle Client-Software auf **Linux-Clients** im Netzwerk installieren. Lesen Sie hierzu bitte das Kapitel **Installation der Client-Software auf Linux-Rechnern** im Anhang dieser Dokumentation.

Weitere Programmstarts (Zugangskennwort)

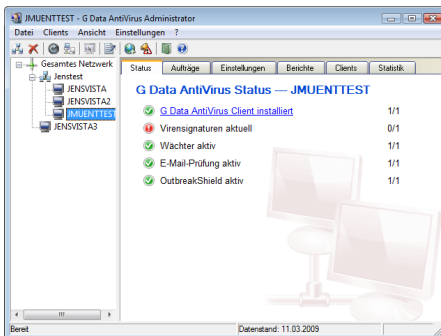
Sie können das Administrator-Tool zur Steuerung des Managementservers mit einem Klick auf den Eintrag **G Data Administrator** in der Programmgruppe **Start > Programme > G Data ManagementServer** des Startmenüs aufrufen. Beim Starten des Administrators werden Sie nach dem Server und dem Kennwort gefragt. Geben Sie in dem Feld **Server**, den Namen des Computers ein, auf dem der Managementserver installiert wurde.



Nun öffnet sich die Programmoberfläche des Administrators. Ihre Funktionen werden in den folgenden Kapiteln erläutert.

Programmaufbau des Administrators

Die Oberfläche des Administrators ist folgendermaßen untergliedert:



Der links befindliche **Clientauswahlbereich** zeigt die hierarchische Struktur der überwachten Computer. Rechts davon kann über Karteireiter in die jeweiligen **Aufgabenbereiche** umgeschaltet werden. Der Inhalt des Aufgabenbereiches bezieht sich normalerweise auf den im Clientauswahlbereich markierten Computer bzw. auf die markierte Gruppe von Clients. Oberhalb dieser Spalten finden Sie eine **Menüleiste** und **Symbolleiste** für globale Funktionen, die in allen Aufgabenbereichen verwendet werden können.

? Bei der Administration von **Linux-Clients**, die als **Samba-Server** fungieren, sind Funktionen, die z.B. den Umgang mit E-Mails beinhalten gesperrt, da diese im Kontext eines Fileservers nicht notwendig sind. Funktionen, die für Linux-Clients nicht einstellbar sind, werden durch einen roten Punkt vor der jeweiligen Funktion markiert.

Menüleiste

Die Menüleiste beinhaltet globale Funktionen, die in allen Aufgabenbereichen verwendet werden können. Sie haben dabei eine Untergliederung in folgende Bereiche:

- Datei
- Clients
- Ansicht
- Aufträge (nur im Aufgabenbereich **Aufträge**)
- Berichte (nur im Aufgabenbereich **Berichte**)
- Client-Einstellungen (nur im Aufgabenbereich **Clients**)
- Einstellungen
- ? (Hilfe)

Datei

Im Datei-Menü stehen Ihnen grundlegende Benutzerverwaltungs- und Druckfunktionen sowie der **Einrichtungsassistent** zur Verfügung.

Einrichtungsassistent

Mit dem Einrichtungsassistenten können Sie in einem anwenderunterstützenden Prozess aus Ihrem Netzwerk die Clients auswählen und aktivieren, für die Sie eine Kontrolle durch die *G Data Software* wünschen. Der Einrichtungsassistent wird im Kapitel **Erster Programmstart (Einrichtungsassistent)** ausführlich erläutert.

Protokoll anzeigen

Über die **Protokolldatei** haben Sie einen schnellen globalen Überblick über die letzten Aktionen Ihrer *G Data Software*. Hier werden sämtliche relevanten Informationen angezeigt. Sie können die Anzeige des Protokolls über folgende Einstellungsbereiche filtern:

- **Protokollansicht:** Legen Sie hier fest, ob Sie ein Protokoll von den Client- oder Servervorgängen einsehen möchten.
- **Rechner/Gruppe:** Hier können Sie festlegen, ob Sie sich ein Protokoll aller Clients bzw. Gruppen oder nur einzelner Bereichen anschauen möchten.
- **Vorgang:** Definieren Sie hier, ob Sie alle protokollrelevanten Informationen einsehen möchten oder nur Meldungen zu bestimmten Themen.
- **Zeitraum:** Hier können Sie den von/bis Zeitraum definieren, für den Protokollinformationen verfügbar sein sollen.

Das Feld **Aktualisieren** dient dazu Vorgänge mitaufzulisten, die sich ereignen, während die Protokolldateiansicht geöffnet ist. Über **Schließen** wird das Fenster der Protokolldatei geschlossen, außerdem können Sie das Protokoll oder einen markierten Bereich des Protokolls **drucken** und **exportieren** (im XML-Format). Sämtliche Vorgänge erscheinen erst einmal in chronologischer Reihenfolge und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach bestimmten Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet.

Benutzerverwaltung

Als Systemadministrator können Sie weitere Benutzerzugängen für das Administrator-Interface vergeben. Klicken Sie dazu auf die **Neu**-Schaltfläche und geben anschließend den Benutzernamen, die **Berechtigungen** dieses Nutzers (**Lesen/Schreiben** bzw. **nur Lesen**) ein, definieren Sie den **Kontentyp** (**integriertes Login**, **Windows-Benutzer**, **Windows-Benutzergruppe**) und vergeben Sie ein **Kennwort** für diesen Benutzer.

Server verwalten

Über die Server-Verwaltung können Sie **Clients** einzelnen **Subnet-Servern** zuordnen, die dann die Kommunikation dieser Clients mit dem **Mainserver** bündeln und auf diese Weise die Netzwerknutzung optimieren. Über dieses Menü können Sie Subnet-Server installieren. Über die Schaltfläche **Clients zuordnen** können Sie vorhandene Clients den definierten Subnet-Servern zuordnen.

? Die Zuordnung der Clients zu Subnet-Servern ist unabhängig von der Gruppierung von Clients im Hinblick auf Virenüberprüfungen. Clients unterschiedlicher Subnet-Server können natürlich in einer Gruppe für **Virenkontrollen** und Scanjobs zusammengefasst werden.

Subnet-Server-Synchronisation

Um eventuelle Änderungen auch außerhalb des regulären Kommunikationsintervalls von Server und Subnet-Server zu ermöglichen, können Sie die Subnet-Server-Synchronisation auch manuell durchführen.

Druckvorlagen

Hier können Sie umfangreiche Einstellungen für den Ausdruck von Protokoll- und Statistikfunktionen vornehmen und in unabhängig voneinander nutzbaren Vorlagen speichern.

? Je nach gewähltem **Aufgabenbereich** haben Sie unterschiedliche Auswahldialoge und Einstellungsmöglichkeiten. Nicht bei jedem Aufgabenbereich sind Druckoptionen verfügbar.

Seitenansicht

In diesem Menü können Sie festlegen, welche Details und Angaben Sie ausdrucken möchten. In dem erscheinenden Auswahlfenster können Sie die gewünschten Elemente für den Ausdruck markieren und gelangen über **OK** in die Seitenansicht, die Ihnen eine Bildschirmvorschau des Ausdrucks anzeigt.



Je nach gewähltem **Aufgabenbereich** haben Sie unterschiedliche Auswahldialoge und Einstellungsmöglichkeiten. Nicht bei jedem Aufgabenbereich sind Druckoptionen verfügbar.

Drucken

Hiermit starten Sie den Druckvorgang für die Client-Einstellungen oder Berichte. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details und Bereiche der Client-Einstellungen Sie ausdrucken lassen möchten.



Je nach gewähltem **Aufgabenbereich** haben Sie unterschiedliche Auswahldialoge und Einstellungsmöglichkeiten. Nicht bei jedem Aufgabenbereich sind Druckoptionen verfügbar.

Beenden

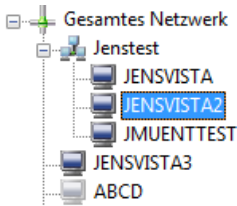
Über diese Funktion beenden Sie den Administrator. Selbstverständlich läuft die Überwachung Ihres Netzwerks gemäß der Vorgaben, die Sie dem Managementserver übermittelt haben, auch dann ungestört weiter, wenn der Administrator nicht geöffnet ist.

Clients

Im Clients-Menü können Sie grundlegende Einstellungen für die Arbeit mit den zu verwaltenden Clients und Gruppen vornehmen.

Neue Gruppe

Über diesen Befehl können Sie eine **Gruppe** erzeugen. Dies ist im Prinzip ein Ordner auf Netzwerkebene, in dem Sie verschiedene Clients zusammenfassen und gemeinsam bearbeiten können. Mit Aktivierung dieses Befehls erscheint unterhalb des Ordners, in dem Sie sich in dem Clientauswahlbereich befinden ein neues Ordnersymbol, in dem Sie direkt einen neuen Namen für diese Gruppe vergeben können.



Um auf unkomplizierte Weise einzelne Clients diesen Gruppen zuzuordnen, können Sie diese einfach mit der Maus auf den jeweiligen Gruppeneintrag ziehen. Dadurch werden diese Clients zu Unterelementen der jeweiligen Gruppe.

Gruppe bearbeiten

Hiermit öffnen Sie eine Dialogbox, in der Sie über die Tasten **Hinzufügen** und **Entfernen** Clients miteinander gruppieren können. Sollten Sie in dem Clientauswahlbereich keine Gruppe ausgewählt haben, kann diese Funktion nicht angewählt werden.

Löschen

Sie können einen Computer aus der Liste der zu überwachenden Clients entfernen (**deaktivieren**), indem Sie ihn markieren und dann den Befehl **Löschen** aus dem Clients-Menü wählen. Beachten Sie, dass das Deaktivieren eines Computers nicht dazu führt, dass die Client-Software deinstalliert wird.

Gruppen können Sie erst löschen, wenn die Gruppe leer ist. Sie müssen also entweder alle darin enthaltenen Clients deaktivieren oder in andere Gruppen verschieben. Gelöschte Clients können Sie über die Funktion **Deaktivierte Clients anzeigen** wieder sichtbar machen.

Defaulteinstellungen

Sie können für den Schutz des gesamten Netzwerks oder ausgewählter Gruppen Defaulteinstellungen erzeugen und damit schnell einheitliche Vorgaben für den Virenschutz vergeben. So können Sie z.B. einfach neue Clients in eine Gruppe hineinverschieben und automatisch für diese Clients die Einstellungen der Gruppe übernehmen.

? Die Defaulteinstellungen stehen Ihnen in dem Clientauswahlbereich nur dann zur Verfügung, wenn Sie eine Gruppe oder den Eintrag **Gesamtes Netzwerk** markiert haben. Neue Clients, die in die Gruppe integriert werden, übernehmen die Defaulteinstellungen und können dann ggf. nachträglich spezifiziert werden.

? Welche Bedeutung die einzelnen Einstellungsbereiche und Funktionen bei den Defaulteinstellungen haben, lesen Sie im Kapitel **Einstellungen**

Defaulteinstellungen löschen

Die Defaulteinstellungen einer Gruppe können Sie über diese Funktion löschen. Auf diese Weise werden dann automatisch die Defaulteinstellungen für das gesamte Netzwerk auf die jeweilige Gruppe übertragen.

Ansicht aktualisieren

Um Änderungen im Netzwerk zu verfolgen, die sich zu der Zeit ergeben, in der Sie den Administrator nutzen, können Sie die **Aktualisieren**-Funktion verwenden.

Deaktivierte Clients anzeigen



Clients, die Sie nicht **aktiviert** haben oder über die Funktion **Löschen** aus der Liste der aktiven Clients entfernt haben, können Sie über diese Funktion wieder sichtbar machen. **Deaktivierte Clients** werden dabei als durchscheinende Symbole dargestellt.



Im Gegensatz dazu sind **aktivierte Clients** durch vollfarbige Symbole definiert.

Client aktivieren



Wenn Sie einen deaktivierten *G Data Client* (dargestellt durch ein durchscheinendes Symbol) auswählen und **Clients aktivieren** betätigen, wird dieser aktiv geschaltet.



Das heißt, dass er Ihnen sozusagen zur Beobachtung zur Verfügung steht. Damit ist noch keine Virenkontrolle verbunden. Sie müssen dazu Vorgaben im Aufgabenbereich **Wächter** oder **Aufträge** erstellen oder den Client einer Gruppe zuordnen, für die solche Vorgaben schon bestehen. Sobald Sie den *G Data Client* auf dem *beobachteten* Client-Rechner installieren, steht Ihnen der Virenschutz zur Verfügung.

Client aktivieren (Dialog)

Über diese Funktion können Sie auch **Clients aktivieren**, ohne Sie in dem Clientauswahlbereich zu markieren. Bei Betätigung dieser Funktion erscheint ein Dialogfeld, in dem Sie einfach den Namen des Clients eingeben, der aktiviert werden soll.

Computer suchen

Mittels dieser Funktion können Sie Computer innerhalb einer definierten Bereichs von **IP-Adressen** Ihres Netzwerks suchen lassen. Geben Sie einfach die **Start-IP Adresse** ein und die **End-IP-Adresse**. Die *G Data Software* durchsucht nun automatisch Ihre **Host-IDs** nach angeschlossenen Computern. Sie haben dann die Möglichkeit, die gefundenen Rechner zu aktivieren. Dabei steht Ihnen einerseits die Möglichkeit zur Verfügung, diese über Ihren Rechnernamen zu aktivieren oder aber direkt über die IP-Adresse anzusprechen. Der jeweilige Client erscheint dann mit seiner IP-Adresse im Clientauswahlbereich.

G Data Client Installationspaket erstellen

Über diese Funktion ist es möglich, ein Installationspaket für den *G Data Client* erstellen zu lassen. Das Paket ist eine einzelne ausführbare Datei (***AvkClientSetupPck.exe***) mit der ein neuer Client ohne weitere Benutzerinteraktion auf einem zu schützenden Rechner installiert werden kann. Das Installationspaket eignet sich beispielsweise dazu, den Client via Login-Script auf allen Rechnern einer Domäne zu verteilen.

? Das Paket enthält immer die auf dem Server aktuelle Client-Version. Bei der Installation der Client-Software werden Sie gefragt, ob auf dem Client-Rechner auch die **G Data Firewall** mitinstalliert werden soll. Weitere Informationen zur **Firewall** erhalten Sie im gleichnamigen Kapitel dieser Dokumentation.

Ansicht

Über dieses Menü können Sie die verschiedenen Auswahlbereiche der Software anwählen. Angezeigte Bereiche werden durch ein Häkchen markiert. Über den Menüpunkt **Aktualisieren** können Sie die Ansicht der Programmoberfläche jederzeit aktualisieren, um z.B. auch aktuelle Änderungen bei der Ansicht zu berücksichtigen. Sie finden Informationen zu den Bereichen in den jeweiligen Kapiteln der **Aufgabenbereiche**.

Einstellungen

Im Einstellungen-Menü haben Sie Zugriff auf grundlegende Programmeinstellungen.

Internet Update

Hier führen Sie die Internet Updates der Virendatenbanken und der Programmdateien der *G Data Software* durch. Geben Sie zunächst in der Karteikarte **Zugangsdaten und Einstellungen** die Zugangsdaten ein, die Sie bei der **Online-Registrierung** erhalten haben. Beim Internet Update werden die aktuellen Dateien vom *G Data UpdateServer* geladen und auf dem Managementserver gespeichert. Die Verteilung der neuen Dateien an die Clients wird vom Aufgabenbereich **Clients** gesteuert. Mit dem Internet Update stellen Sie sicher, dass Sie immer die aktuellsten Virensignaturdatenbanken haben und über die neuesten Programmdateien verfügen.

Virendatenbank

Alle Clients haben eine Kopie der Virendatenbank, damit der Virenschutz auch gewährleistet ist, wenn sie offline sind (d.h. keine Verbindung mit dem Managementserver haben). Dies ist z.B. wichtig bei **Notebooks**, die nur in unregelmäßigen Abständen mit dem Netzwerk Ihres Unternehmens verbunden sind. Die **Aktualisierung** der Dateien auf den Clients erfolgt in zwei Schritten, die natürlich beide automatisiert werden können. Im ersten Schritt werden die aktuellen Dateien vom *G Data UpdateServer* in einen Ordner auf dem Managementserver kopiert. Im zweiten Schritt werden die neuen Dateien an die Clients verteilt (siehe Aufgabenbereich "Clients").

- **Status aktualisieren:** Über diese Schaltfläche können Sie die Statusanzeige der Virensignaturen auf dem Client gegebenenfalls aktualisieren, falls Änderungen in der Anzeige noch nicht übernommen worden sind.
- **Update jetzt starten:** Über die Schaltfläche **Update jetzt starten** können Sie eine Aktualisierung der Virendatenbanken direkt durchführen.
- **Automatische Updates:** Wie die Virenprüfungen können Sie auch die Internet Updates automatisch durchführen lassen. Aktivieren Sie dazu das Häkchen bei **Update periodisch ausführen** und legen Sie fest, wann und in welchem Turnus das Update zu erfolgen hat.



Damit das Update automatisch erfolgen kann, muss Ihr Managementserver natürlich mit dem Internet verbunden sein oder der *G Data Software* eine automatische Einwahl ermöglichen. Geben Sie hierzu unter **Zugangsdaten und Einstellungen** gegebenenfalls **Benutzerkonto** und **Proxy-Einstellungen** vor.

Programmdateien

Wenn die **Client-Software** von **G Data** aktualisiert wird, können Sie die Aktualisierung über den Managementserver automatisch erledigen lassen. Die **Aktualisierung** der Dateien auf den Clients erfolgt in zwei Schritten, die natürlich beide automatisiert werden können. Im ersten Schritt werden die aktuellen Dateien vom **G Data UpdateServer** in einen Ordner auf dem Managementserver kopiert. Im zweiten Schritt werden die neuen Dateien an die Clients verteilt und damit wird der dortige Client aktualisiert (siehe **Aufgabenbereich Clients**).

- **Aktualisieren:** Über die Schaltfläche **Aktualisieren** können Sie die Statusanzeige der Softwareversion auf dem Client gegebenenfalls aktualisieren, falls Änderungen in der Anzeige noch nicht übernommen worden sind.
- **Update jetzt durchführen:** Über die Schaltfläche **Update jetzt durchführen** können Sie eine Aktualisierung der Client-Software direkt durchführen.
- **Automatische Updates:** Wie die Virenprüfungen können Sie auch die Internet Updates der Client-Software automatisch durchführen lassen. Aktivieren Sie dazu das Häkchen bei **Update periodisch ausführen** und legen Sie fest, wann und in welchem Turnus das Update zu erfolgen hat.

? Damit das Update automatisch erfolgen kann, muss Ihr Managementserver natürlich mit dem Internet verbunden sein oder der **G Data Software** eine automatische Einwahl ermöglichen. Geben Sie hierzu unter **Zugangsdaten und Einstellungen** gegebenenfalls **Benutzerkonto** und **Proxy-Einstellungen** vor.

? **Achtung:** Um die Programmdateien des Managementservers zu aktualisieren rufen Sie bitte in der Programmgruppe **G Data ManagementServer** im Startmenü den Eintrag **Internet Update** auf. Der Managementserver kann ausschließlich über diesen Eintrag aktualisiert werden. Im Gegensatz zur **G Data Client-Software**, die auch über den Administrator aktualisiert werden kann.

Zugangsdaten und Einstellungen

Mit der **Online-Registrierung** erhalten Sie von **G Data** direkt online die Zugangsdaten für das Update Ihrer Virendatenbanken und Programmdateien. Geben Sie diese bitte unter **Benutzername** und **Kennwort** Ihre notwendigen Daten ein. Über die Schaltfläche **Versionsprüfung** können Sie beim nächsten Update der Virendatenbank feststellen, ob Sie die aktuellsten Programmdateien verwenden. Im Regelfall sollte die Versionsprüfung immer eingeschaltet sein, da sie unnötige Updates verhindert. Sollten sich jedoch Probleme beim Arbeiten mit Virendatenbanken ergeben, dann schalten Sie bitte das Feld **Versionsprüfung** aus. Auf diese Weise wird beim nächsten Internet Update automatisch eine aktuelle Version der Virendatenbank auf Ihren Server überspielt. Mit der Schaltfläche **Benutzerkonto und Proxy-Einstellungen** öffnen Sie ein Fenster, in dem Sie grundlegende Zugangsdaten für Internet & Netzwerk eingeben können.

? **Achtung:** Sie sollten hier nur Eingaben tätigen, wenn sich mit den Standardeinstellungen der *G Data Software* Probleme ergeben sollten (z.B. wegen der Verwendung eines **Proxyservers**) und ein Internet Update nicht durchführbar ist.

Internet Einstellungen

So benötigen Sie für Ihr Benutzerkonto die Informationen **Benutzername**, **Kennwort** und **Domäne**. Für die Anmeldung beim **Proxyserver** ist zusätzlich der Port (im Regelfall: 80) und - falls vom Benutzerkonto abweichend - eine Eingabe von Benutzername und Kennwort für den Proxyserver notwendig.

? **Benutzerkonto** ist ein Konto für den Rechner, auf dem sich der Managementserver befindet.

? Die *G Data Software* kann die **Verbindungsdaten des Internet Explorer** (ab Version 4) verwenden. Konfigurieren Sie zunächst den **Internet Explorer** und prüfen Sie, ob die Testseite unseres Update-Servers erreichbar ist: <http://ieupdate.gdata.de/test.htm>. Schalten Sie anschließend die Option **Proxyserver verwenden** aus. Geben Sie unter **Benutzerkonto** das Konto ein, für den Sie den Internet Explorer konfiguriert haben (als das Konto, mit dem Sie sich an Ihrem Rechner angemeldet haben).

Alarmmeldungen

Bei neuen Virenfunden kann der Managementserver automatisch Alarmmeldungen per **E-Mail** versenden. Die dazu benötigten Einstellungen werden in diesem Bereich vorgenommen.

E-Mail-Einstellungen

Geben Sie den Namen des Mailservers in Ihrem Netzwerk, den **SMTP-Server** und den **Port** an (normalerweise 25). Weiterhin wird eine (gültige) Absenderadresse benötigt, damit die Mails verschickt werden können.



An diese E-Mail-Adresse werden auch die Antworten des **Emergency-AntiViren Service** geschickt.

E-Mail-Benachrichtigung

Aktivieren Sie die E-Mail-Benachrichtigung, indem Sie das Häkchen bei **Alarm-Meldungen per E-Mail verschicken** setzen und geben Sie unter **Empfänger** die Mail-Adresse des Empfängers der Benachrichtigungen an. Sie sollten auf jeden Fall unter **Begrenzung** eine Mengenbegrenzung definieren, damit das Postfach bei akuten Verseuchungen nicht überquillt.

Telefon-Benachrichtigung

Sie können sich auch per Telefon automatisch von der *G Data Software* über einen Virenbefall informieren lassen. Unter **Status** können Sie diesen Service ein- oder ausschalten. Geben Sie einfach unter **Ansage** den Text ein, der Ihnen bei einer Virenwarnung vorgelesen werden soll und unter **Rufnummer** die Telefonnummer unter der Sie erreichbar sind. Unter **Zeitfenster** können Sie außerdem festlegen, dass die *G Data Software* Sie nur während bestimmter Zeiten warnt. Um die Grundeinstellungen für den telefonische Benachrichtigungen einzustellen, rufen Sie bitte in der Programmgruppe "*G Data ManagementServer*" im Startmenü den Eintrag **Telefon-Benachrichtigung (Einstellungen)** auf. Hier können Sie weitergehende Vorgaben für das Anwahlverfahren vornehmen.



Bitte achten Sie darauf, eine Amtsvorwahl (in der Regel die **0**) zu verwenden, wenn der Telefonanruf über eine firmeninterne Telefonanlage nach außen geleitet wird.

Update-Rollback Engine A / B

Es kann im Fall von Fehlalarmen oder ähnlichen Problemen in seltenen Fällen sinnvoll sein, dass aktuelle **Update der Virensignaturen** zu sperren und statt dessen eines der vorhergehenden Signaturupdates zu verwenden. Der Managementserver speichert von jeder AntiViren-Engine die letzten Updates. Sollte es also mit dem aktuellen Update der Engine A oder B Probleme geben, kann der Administrator das aktuelle Update für einen bestimmten Zeitraum sperren und statt dessen automatisch das zeitlich davorliegende Signaturupdate an die Clients und Subnet-Server verteilen.

? Auf Clients, die nicht mit dem Managementserver verbunden sind (z. B. Notebooks auf Dienstreisen) können keine **Rollbacks** durchgeführt werden. Eine vom Server an den Client übertragene Sperrung kann dort nicht rückgängig gemacht werden.

? Die Anzahl der zu speichernden Rollbacks können Sie im Bereich **Server-Einstellungen** vornehmen.

Server-Einstellungen

Hier können Sie grundlegende Einstellungen für Synchronisierungen und automatische Löschoptionen vornehmen.

Einstellungen

Im Einstellungen-Bereich finden Sie folgende Optionen:

- **Rollbacks:** Geben Sie hier an, wie viele der aktualisierten Virensignaturupdates Sie für **Rollbacks** als Reserve vorhalten möchten. Als Standardwert gelten hier jeweils die letzten zehn Signaturupdates der jeweiligen Engine.
- **Automatisches Bereinigen:** Hier können Sie festlegen, dass **Protokolleinträge**, **Scan-Protokolle** und **Berichte** nach einem eingegebenen Zeitraum automatisch gelöscht werden.

Synchronisation

Im Synchronisation-Bereich können Sie die Kommunikation zwischen Clients, Subnet-Servern und Servern zeitlich definieren:

- **Clients:** Geben Sie hier das Zeitintervall an, in dem die Clients mit dem Server synchronisiert werden. Wenn Sie das Häkchen bei **Clients bei Optionsänderungen vom Server benachrichtigen** setzen, erhält der Anwender auf dem Client-Rechner eine Meldung darüber, dass Änderungen vollzogen wurden.
- **Subnet-Server:** Über diesen Bereich können Sie die Intervalle für die Kommunikation zwischen Server und Subnet-Server definieren. Wenn Sie das Häkchen bei **Neue Berichte sofort an den Hauptserver übertragen** setzen, dann werden Berichte unabhängig von den hier getätigten Einstellungen sofort an den Hauptserver übertragen.

Hilfe

Hier erhalten Sie Informationen zum Programm und haben außerdem die Möglichkeit, auf die Online-Hilfe der *G Data Software* zurückzugreifen.

Symbolleiste

In der Symbolleiste finden Sie die wichtigsten Befehle der **Menüleiste** als anklickbare Symbole.



Neue Gruppe: Die aktivierten Computer können zu **Gruppen** zusammengefasst werden. Damit lassen sich leicht unterschiedliche Sicherheitszonen definieren, da alle Einstellungen sowohl für einzelne Clients als auch für komplette Gruppen durchgeführt werden können. Zum Anlegen einer neuen Gruppe markieren Sie zunächst die übergeordnete Gruppe und klicken Sie dann auf das abgebildete Symbol.



Löschen: Sie können einen Computer aus der Liste entfernen (**deaktivieren**), indem Sie ihn markieren und dann die Schaltfläche **Löschen** anklicken. Beachten Sie, dass das Deaktivieren eines Computers nicht dazu führt, dass die Client-Software deinstalliert wird.



Ansicht aktualisieren: Über **Aktualisieren** oder die Taste **F5** können Sie die Ansicht der Administratoroberfläche jederzeit aktualisieren, um z.B. auch aktuelle Änderungen bei der Ansicht zu berücksichtigen.



Deaktivierte Clients anzeigen: Wählen Sie diese Schaltfläche um auch die nicht aktivierten Computer anzuzeigen. Sie erkennen die deaktivierten Computer an den grau durchscheinenden Icons. Computer ohne Dateifreigabe bzw. Druckerfreigabe werden normalerweise nicht angezeigt.



Client aktivieren: Zum Aktivieren eines Computers markieren Sie ihn in der Liste und wählen dann die abgebildete Schaltfläche. Sie können auch Computer aktivieren, die nicht in der Liste aufgeführt sind. Wählen Sie dazu im Clients-Menü den Befehl **Client aktivieren (Dialog)** und geben Sie den Namen des Computers ein.



Protokoll anzeigen: Über die Protokolldatei haben Sie einen schnellen globalen Überblick über die letzten Aktionen Ihrer *G Data Software*. Hier werden sämtliche relevanten Informationen angezeigt.



Internet Update: Über den Bereich **Internet Update** führen Sie die Internet Updates der Virendatenbanken und der Programmdateien der Clients durch.



Alarmmeldungen: Bei neuen Virenfunden kann der Managementserver automatisch Alarmmeldungen per E-Mail versenden. Die dazu benötigten Einstellungen werden in dem Bereich **Alarmmeldungen** im Menü **Einstellungen** vorgenommen.



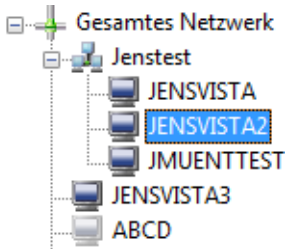
Online-Virenlexikon: Über die Funktion **Online-Virenlexikon** rufen Sie das *G Data-Virenlexikon* auf. Dieses liefert Ihnen einen interessanten Einblick in die weitverzweigte Welt der Viren und Schadprogramme. Da das **Virenlexikon** ständig aktualisiert wird, finden Sie dieses als Online-Lexikon im Internet.



Hilfe: Über diese Schaltfläche haben Sie die Möglichkeit, auf die Online-Hilfe von *G Data* zurückzugreifen.

Clientauswahlbereich

Hier finden Sie sämtliche Clients und Server sowie definierte Gruppen in Ihrem Netzwerk hierarchisch aufgelistet und untergliedert. Wie im Windows Explorer erscheinen Gruppen, in denen sich Untergliederungen befinden mit einem kleinen Plus-Symbol. Wenn Sie dieses anklicken, öffnet sich die Verzeichnisstruktur an dieser Stelle und ermöglicht die Ansicht der dahinter befindlichen Struktur.



Ein Klick auf das Minus-Symbol schließt diese Untergliederung wieder. Folgende Symbole sind in der Verzeichnisauswahl sichtbar:



Netzwerksymbol



Gruppe



Server (aktiviert)



Server (deaktiviert)



Client (aktiviert)



Client (deaktiviert)



Nicht auswählbare Geräte: Hierunter fallen z.B. Netzwerkdrucker

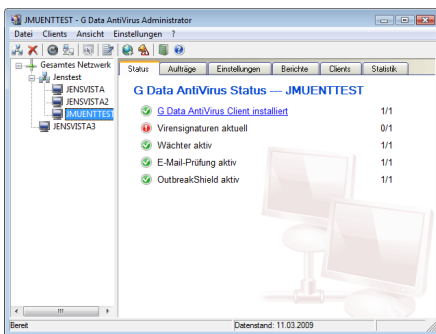
Aufgabenbereiche

In den verschiedenen Aufgabenbereichen, die Sie über die jeweiligen Karteireiter anwählen können, haben Sie die Möglichkeit, die Absicherung Ihrer Clients komfortabel zu administrieren. Die Einstellungen, die Sie dabei vornehmen, beziehen sich immer auf die Clients oder Gruppen, die Sie in dem **Clientauswahlbereich** markiert oder ausgewählt haben. Die einzelnen Themenfelder werden in den folgenden Abschnitten eingehend erläutert.

- **Status**
- **Aufträge**
- **Einstellungen**
- **Berichte**
- **Clients**
- **Firewall**
- **Statistik**

Status

Im Status-Bereich der *G Data Software* erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.



Solange Ihr System optimal für den Schutz vor Computerviren konfiguriert ist, finden Sie links vor den hier aufgeführten Einträgen ein grünes Ampelsymbol.



Sollte eine Komponente nicht optimal eingestellt sein (z.B. abgeschalteter Wächter oder veraltete Virensignaturen), weist Sie ein Achtung-Symbol darauf hin.



Wenn sich die *G Data-Programmoberfläche* öffnet, sind für kurze Zeit die meisten Symbole im Achtung-Modus. Das heißt nicht, dass die *G Data Software* Ihren Computer in diesem Moment nicht schützt. Hier handelt es sich ganz im Gegenteil um eine interne Überprüfung des Virenschutz-Status, die Ihnen anzeigt, dass hier ein automatischer Check der Funktionen erfolgt.

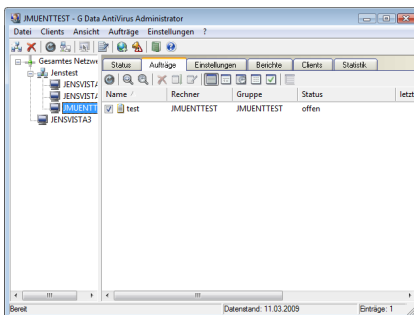
Durch doppeltes Anklicken des jeweiligen Eintrags können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Aufgabenbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit Achtung-Symbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Ampelsymbol.

Aufträge

In diesem Aufgabenbereich können Sie Aufträge für Virenprüfungen auf den *G Data Clients* definieren. Es gibt zwei unterschiedliche Auftragsarten: **Einmalige Scanjobs** und **periodische Scanjobs**. Die einmaligen Jobs werden direkt nach dem Anlegen ausgeführt, für die periodischen wird ein **Zeitplan** definiert, nach dem sie ausgeführt werden sollen.



Scanjobs bzw. **Jobs** sind die jeweiligen Aufträge, die Sie im gleichnamigen Aufgabenbereich zur Virenkontrolle, -entfernung oder -prophylaxe erstellen.



Im Aufgabenbereich **Aufträge** erscheinen alle Jobs unter dem von Ihnen vorgegebenen Namen und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach folgenden Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet:

- **Name:** Der von Ihnen vorgegebene Name für den Scanjob. Sie können hier beliebig lange Namen eingeben und auf diese Weise Ihren Scanjob genau beschreiben, um bei vielen verschiedenen Jobs den Überblick zu behalten.
- **Rechner:** Hier finden Sie den Namen des jeweiligen Clients. Sie können Scanjobs nur für aktivierte Clients definieren.
- **Gruppe:** Sie können einzelne Clients zu Gruppen zusammenfassen, die dann dieselben Scanjobs nutzen. Wenn Sie einer Gruppe einen Scanjob zuordnen, erscheinen in der Übersichtsliste nicht die einzelnen Rechner, sondern der Gruppenname.
- **Status:** Hier erhalten Sie den Status oder das Ergebnis eines Scanjobs in Klartext angezeigt. So erfahren Sie z.B. ob der Job gerade durchgeführt oder abgeschlossen wurde und werden auch darüber informiert, ob Viren gefunden wurden oder nicht.
- **letzte Ausführung:** Über diese Spalte erhalten Sie Informationen darüber, wann der jeweilige Scanjob das letzte Mal durchgeführt wurde.
- **Zeitintervall:** Gemäß der **Zeitplanung**, die Sie für jeden Scanjob definieren können, steht hier, in welchem Turnus der Job wiederholt wird.
- **Analyse-Umfang:** Hier erfahren Sie auf welche **Datenträger** (z.B. lokale Festplatten) sich die Analyse erstreckt.



In der Menüleiste steht Ihnen für den Aufgabenbereich **Aufträge** ein zusätzlicher Menüeintrag mit folgenden Funktionen zur Verfügung:

- **Ansicht:** Wählen Sie hier aus, ob Sie sich alle **Scanjobs**, nur einmalige Scanjobs, nur periodische Scanjobs oder nur offene Scanjobs oder nur erledigte Scanjobs anzeigen lassen möchten. Für Scanjobs, die für eine **Gruppe** von Clients definiert wurden, können Sie festlegen, ob detaillierte Infos zu allen Clients oder nur gruppenübergreifende Zusammenfassungen angezeigt werden sollen. Setzen Sie hier zu das Häkchen bei **Gruppenjobs ausführlich anzeigen**.
- **Erneut (sofort) ausführen:** Hiermit können Sie ausgewählte Scanjobs unabhängig von eingestellten zeitlichen Vorgaben direkt ausführen.

- **Abbrechen:** Über diese Funktion können Sie einen laufenden Scanjob abbrechen.
- **Löschen:** Ausgewählte Scanjobs können mit dieser Funktion gelöscht werden.
- **Neu:** Wählen Sie hier aus, ob Sie einen *einmaligen Scanjob* (einmaliges Prüfen) oder einen *regelmäßigen Scanjob* (periodisches Prüfen) erstellen wollen.

Sie können beliebig viele unterschiedliche Scanjobs definieren. Generell ist es aus Gründen der Performance allerdings sinnvoll, dass sich Scanjobs zeitlich nicht überschneiden.

Aktualisieren



Dieser Funktion aktualisiert die Ansicht. Lädt die aktuelle Jobliste vom Managementserver.

Neuer Scanjob (einmalig)



Mit dieser Funktion erstellen Sie einen neuen Job zum einmaligen Prüfen. Es öffnet sich ein Dialog zum Einstellen der Job- und Scanparameter. Hier können Sie die gewünschten Vorgaben eingeben. Wechseln Sie dabei zwischen den Einstellungsbereichen, in dem Sie einfach die jeweilige Registerkarte auswählen. Diese Registerkarten werden im Kapitel **Neuer Scanjob (periodisch)** ausführlich erläutert.



Über die Funktion **Neuer Scanjob (periodisch)** haben Sie die Möglichkeit, zeitgesteuerte Scanjobs zu definieren, die Ihr System automatisch in regelmäßigen Abständen überprüfen.



Doppelklicken Sie zum Ändern der Parameter eines vorhandenen Jobs auf den Eintrag, oder wählen Sie im Kontextmenü (über Anklicken mit der rechten Maustaste) den Befehl **Eigenschaften**. Nun können Sie die Einstellungen des Scanjobs beliebig verändern.

Neuer Scanjob (periodisch)



Mit dieser Funktion erstellen Sie einen neuen Job zum periodischen Prüfen. Es öffnet sich ein Dialog zum Einstellen der Job- und Scanparameter. Hier können Sie die gewünschten Vorgaben eingeben. Wechseln Sie dabei zwischen den Einstellungsbereichen, in dem Sie einfach die jeweilige Registerkarte auswählen:



Doppelklicken Sie zum Ändern der Parameter eines vorhandenen Jobs auf den Eintrag oder wählen Sie im Kontextmenü (über Anklicken mit der rechten Maustaste) den Befehl **Eigenschaften**. Nun können Sie die Einstellungen des Scanjobs beliebig verändern.

Job

Legen Sie in den Jobparametern fest welchen Namen der Scanjob haben soll. Sie können hier z.B. aussagekräftige Namen, wie **Archivprüfung** oder **Monatliche Prüfung** verwenden, um den gewünschten Job eindeutig zu charakterisieren und in der tabellarischen Übersicht wiederzufinden. Darüber hinaus können Sie angeben, ob der Anwender den Job über das Kontextmenü des Clients abbrechen kann. Sollten Sie Ihr Netzwerk permanent mit dem Wächter überwachen, ist es vertretbar, den Scanjob vom Anwender abbrechen zu lassen, da dieser ihn leicht in seinem Arbeitstempo beeinträchtigen kann. Sollten Sie den Wächter jedoch nicht verwenden, sind gerade die periodischen Scanvorgänge unverzichtbar und sollten nicht abschaltbar sein. Über die Option **Scan-Fortschritt regelmäßig an den Server übermitteln** können Sie sich im Administrator den Status eines laufenden Scan-Vorgangs auf einem Client anhand einer Prozentangabe anzeigen lassen. Mit der Funktion **Rechner nach der Virenprüfung ausschalten, wenn kein Benutzer angemeldet ist** haben Sie eine weitere Option, die Ihnen den administrativen Aufwand zu verringern hilft.

Zeitpunkt / Zeitplanung

Über diese Karteikarte können Sie festlegen, wann und in welchem Rhythmus das automatische Update erfolgen soll. Unter **Ausführen** geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter **Zeitpunkt** und **Wochentage** spezifizieren. Wenn Sie **Beim Systemstart** auswählen, fallen die Vorgaben der Zeitplanung natürlich fort und die *G Data Software* führt das Update immer aus, wenn der Rechner neu gestartet wird.

? Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** z.B. bestimmen, dass der Rechner nur an Werktagen das Update durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

Scanner

In dem Scanner-Menü können Sie festlegen, wie die Virenprüfung durch die *G Data Software* zu erfolgen hat. Da eine Virenprüfung auf Basis eines Zeitplans oder eines manuellen Analysebeginns meist zu Zeiten erfolgt, in der der Computer nicht völlig mit anderen Aufgaben ausgelastet ist, können hier in der Regel mehr Systemressourcen für die Virenanalyse verwendet werden, als beim **Virenwächter**.

- **Engines benutzen:** Die *G Data Software* arbeitet mit zwei Antiviren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich; d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen. Wir empfehlen die Einstellung **Beide Engines - performance-optimiert**. Hierbei sind beide Virens Scanner so miteinander verwoben, dass sie optimale Erkennung mit minimierter Scandauer ermöglichen.

- **Im Fall einer Infektion:** Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Client verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll. Bei der Einstellung **Datei in Quarantäne verschieben** handelt es sich um ein spezielles Verzeichnis, welches der Managementserver anlegt, in dem infizierte Dateien verschlüsselt und damit ohne fortlaufende Schadfunktion abgelegt werden. Dateien in der **Quarantäne** können vom Administrator desinfiziert, gelöscht, an den Ursprungsort zurückbewegt oder gegebenenfalls an den **Emergency-AntiViren Service** von **G Data** versendet werden.
- **Infizierte Archive:** Legen Sie hier fest, ob die Behandlung von Virenfunden für **Archive** gesondert erfolgen soll. Dabei sollten Sie bedenken, dass ein Virus innerhalb eines Archives erst dann Schaden anrichtet, wenn das Archiv entpackt wird.
- **Dateitypen:** Hier können Sie festlegen, welche Dateitypen von **G Data** auf Viren untersucht werden sollen. In der Regel ist es nicht nötig, Dateien, die keinen ausführbaren Programmcode enthalten zu überprüfen; zumal eine Überprüfung aller Dateien eines Computers durchaus eine gewisse Zeit in Anspruch nehmen kann.
- **Priorität Scanner:** Über die Stufen **hoch**, **mittel** und **niedrig** können Sie festlegen, ob eine Virenprüfung durch **G Data** auf Ihrem System hohe Priorität haben soll (in diesem Fall erfolgt die Analyse relativ schnell, andere Anwendungen werden während der Analyse aber möglicherweise langsamer) oder niedrige Priorität (die Analyse erfolgt relativ langsam, dafür laufen andere Anwendungen während dieser Zeit quasi ungestört ab). Je nach der Zeit, zu der Sie die Virenanalyse durchführen, sind hier unterschiedliche Einstellungen sinnvoll.
- **Einstellungen:** Legen Sie hier fest, welche zusätzlichen Virenanalysen die **G Data Software** durchführen soll. Die hier gewählten Optionen sind für sich gesehen durchaus sinnvoll, je nach Anwendungsart kann der Vorteil der Zeitersparnis durch Weglassen dieser Überprüfungen das etwas geringere Maß an Sicherheit aufwiegen. Folgende Einstellungsmöglichkeiten stehen Ihnen hier zur Verfügung:

Heuristik: In der Heuristik werden Viren nicht nur anhand der Virendatenbanken, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Die Heuristik kann in sehr seltenen Fällen einen Fehlalarm erzeugen.

Archive: Das Überprüfen gepackter Daten in Archiven ist sehr zeitintensiv und kann in der Regel unterbleiben, wenn der **G Data Wächter** auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung. Dennoch sollten bei regelmäßigen Kontrollen außerhalb der eigentlichen Nutzungszeit des Computers auch eine Kontrolle der Archive erfolgen.

E-Mail Archive: Das Überprüfen gepackter Daten in E-Mail Archiven ist sehr zeitintensiv und kann in der Regel unterbleiben, wenn der **G Data Wächter** auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung. Dennoch sollten bei regelmäßigen Kontrollen außerhalb der eigentlichen Nutzungszeit des Computers auch eine Kontrolle der Archive erfolgen.

Systembereiche: Die Systembereiche Ihres Computers (**Bootsektoren, Master Boot Records** etc.) die eine grundlegende Basis für das Betriebssystem bieten, sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden.

Auf Dialer / Spyware / Adware / Riskware prüfen: Mit der **G Data Software** können Sie Ihr System auch auf **Dialer** und andere Schadprogramme (**Spyware, Adware, Riskware**) überprüfen. Hierbei handelt es sich z.B. um Programme, die von ihnen ungewünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen, die z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch ihre Passwörter) heimlich speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.

Auf RootKits prüfen: **Rootkits** versuchen sich herkömmlichen Virenerkennungsmethoden zu entziehen. Sie können mit dieser Funktion gezielt nach Rootkits suchen, ohne eine komplette Überprüfung der Festplatten und gespeicherten Daten vorzunehmen.

Alle verfügbaren Prozessoren benutzen: Mit dieser Option können Sie die Virenkontrolle bei Systemen mit mehreren **Prozessoren** (z.B. DualCore) auf alle Prozessoren verteilen und diese Weise die Virenprüfung deutlich schneller durchführen. Nachteil dieser Option ist es, dass die Arbeitsgeschwindigkeit des Systems für andere Anwendungen ausgebremst wird. Sie sollten diese Option also nur dann benutzen, wenn Sie Ihren Scanjob zu Zeiten durchführen, wo das System nicht regulär genutzt wird (z.B. nachts).

Analyse-Umfang

Über das Register **Analyse-Umfang** können Sie beim Client die Virenkontrolle auch auf bestimmte Verzeichnisse begrenzen. Auf diese Weise können Sie z.B. Ordner mit selten benötigten Archiven aussparen oder in ein spezielles Scanschema integrieren. Die Verzeichnisauswahl bezieht sich dabei auf den aktuell ausgewählten Rechner und nicht auf den gewählten Client.



Besonderheit bei Scanjobs auf einem Linux-Fileserver: Bei der Verzeichnisauswahl werden das Root-Laufwerk (/) und alle Freigaben zurück geliefert. So können Scanjobs gezielt auf ausgewählten Freigaben oder beliebig gewählten Verzeichnissen des Dateiservers durchgeführt werden.

Scanjobs löschen



Die Funktion **Scanjobs löschen** löscht alle markierten Jobs.

Scanjobs erneut (sofort) ausführen



Wählen Sie diese Funktion, um einmalige Scanjobs, die bereits durchgeführt oder abgebrochen wurden, erneut auszuführen. Bei periodischen Scanjobs bewirkt diese Funktion, dass sie unabhängig vom Zeitplan sofort ausgeführt werden.

Protokolle



Rufen Sie mit dieser Funktion die Protokolle zu den Aufträgen des jeweiligen Clients auf.

Anzeigeoptionen

Bei einer großen Anzahl unterschiedlicher Scanjobs ist es sinnvoll, diese sich nach bestimmten Kriterien anzeigen und auflisten zu lassen. Folgende Möglichkeiten stehen Ihnen hier zur Verfügung:



Alle Jobs anzeigen



Nur einmalige Scanjobs anzeigen



Nur periodische Scanjobs anzeigen



Nur offene Scanjobs anzeigen



Nur erledigte Scanjobs anzeigen

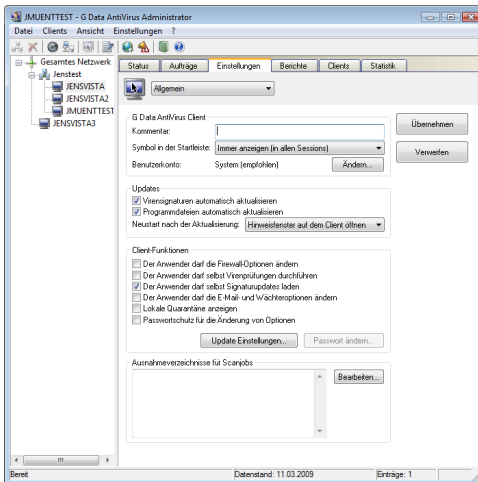


Gruppenjobs ausführlich anzeigen: Zeigt bei Gruppenjobs alle zugehörigen Einträge an. Die Option ist nur verfügbar, wenn in der Computerliste eine Gruppe selektiert ist.

Einstellungen

In diesem Aufgabenbereich können Optionen für alle Clients, einzelne Clients oder eine Gruppe von Clients eingestellt werden (z.B. ob Updates automatisch durchgeführt werden sollen, ob eigene Internet Updates über die Clients erlaubt sind, ob Ausnahmeverzeichnisse dort individuell definiert werden dürfen etc.).

Über die oben befindliche Auswahlbox können Sie entscheiden, welche Art von Optionen Sie hierbei bearbeiten möchten. Wählen Sie dazu im **Clientauswahlbereich** den gewünschten Client oder die Gruppe von Clients aus, die Sie konfigurieren möchten, tätigen dann die gewünschten Eingaben und schließen den Vorgang durch Anklicken der **Übernehmen**-Schaltfläche ab.



Allgemein

Hier haben Sie folgende Einstellungsmöglichkeiten:

G Data Client

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Kommentar**: Geben Sie hier einen aussagekräftigen Namen für den jeweiligen Client an
- **Symbol in der Startleiste**: Für Terminal-Server und Windows mit schneller Benutzerumschaltung kann gewählt werden, in welchen Sessions ein Client-Symbol in der Taskleiste angezeigt werden soll.: ***nie***, ***nur in der ersten Session*** oder ***immer***. Bei *normalen* Clients kann mit der Option das Anzeigen des Client-Symbols wahlweise unterbunden werden. Damit der Anwender Zugriff auf erweiterte Client-Funktionen hat, muss das Symbol angezeigt werden, da auf diese Weise per Mausklick auf das entsprechende ***Kontextmenü*** zugegriffen werden kann.
- **Benutzerkonto**: Die Client-Software läuft normalerweise im Systemkontext. Sie können hier ein anderes Konto angeben, um die Prüfung von Netzwerkverzeichnissen zu ermöglichen. Das Konto muss dazu Administratorrechte auf dem Client haben.

Updates

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Virensignaturen automatisch aktualisieren**: Schaltet die automatische Aktualisierung der Virendatenbank ein. Die Clients prüfen periodisch, ob eine neue Version auf dem Managementserver existiert und führen die Aktualisierung automatisch durch.
- **Programmdateien automatisch aktualisieren**: Aktualisiert die Programmdateien auf dem Client mit den Dateien vom Managementserver. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gebootet werden muss. Je nach Einstellung unter **Neustart nach der Aktualisierung** hat der Anwender auf dem Client die Möglichkeit, die Aktualisierung der Daten auf einen späteren Zeitpunkt zu verschieben

- **Neustart nach der Aktualisierung**: Hier können Sie festlegen, ob der Client bei einer Aktualisierung der Programmdateien automatisch neu gestartet wird (**Neustart ohne Abfrage**), ob dem Anwender die Möglichkeit geboten wird, den Neustart sofort oder später durchzuführen (**Hinweisfenster auf dem Client**) oder ob die Aktualisierung der Programmdateien erst dann erfolgt, wenn der Client von sich aus neu gebootet wird (**Bericht erzeugen**).

Client-Funktionen

Mit den folgenden Funktionen definieren Sie Aussehen, Verhalten und Funktionsumfang des jeweiligen Clients. Je nach Vorgabe hat der Anwender auf diese Weise umfangreiche oder auch nur stark eingeschränkte Rechte im Hinblick auf Virenprophylaxe und -bekämpfung:

- **Der Anwender darf selbst Virenprüfungen durchführen**: Im akuten Verdachtsfall kann der Anwender wie bei einer lokal installierten Antivirenlösung auf seinem Rechner unabhängig vom Managmentserver eine ***Virenprüfung*** durchführen. Ergebnisse dieser Virenprüfung werden beim nächsten Kontakt mit dem Managementserver an diesen übermittelt.
- **Der Anwender darf selbst Signaturupdates laden**: Wenn Sie diese Funktion aktivieren, darf der jeweilige Client Virensignaturen auch ohne Verbindung zum Firmenserver direkt aus dem Internet laden. Dies erhöht gerade bei im Außendienst eingesetzten Notebooks die Sicherheit erheblich.
- **Der Anwender darf die E-Mail- und Wächteroptionen ändern**: Bei Aktivierung dieser Funktion hat der Client-Anwender gezielt die Möglichkeit, neben den ***Wächteroptionen*** auch die Einstellungen zum Thema ***E-Mail-Sicherheit*** für seinen Client zu beeinflussen.
- **Lokale Quarantäne anzeigen**: Wenn Sie das Anzeigen der lokalen ***Quarantäne*** erlauben, kann der Anwender Daten, die vom Wächter wegen Virenbefall oder -verdacht in diesen Quarantäne-Ordner geschoben wurden ggf. desinfizieren, löschen oder zurückbewegen. Beachten Sie dabei, dass bei einem Zurückbewegen der Virus nicht entfernt wurde. Diese Option sollten Sie deshalb nur versierten Anwendern auf den Clients ermöglichen.

- **Passwortschutz für die Änderung von Optionen:** Wenn dem Anwender auf den Clients das Recht zum Ändern der Wächteroptionen verliehen wird, besteht natürlich immer die Möglichkeit, dass andere Leute auf diesem Rechner die Wächterfunktionen missbräuchlich abschalten. Um dem vorzubeugen, können Sie die Einstellungen der Wächteroptionen auf dem Client mit einem Passwort schützen. Vergeben Sie das Passwort hier individuell für den jeweiligen Client oder die jeweilige Gruppe und teilen Sie es den autorisierten Nutzern der Client-Rechner mit.
- **Update-Einstellungen:** Hier können Sie festlegen, ob das Internet Update von Virensignaturen generell zentral über den Server, individuell für jeden Client oder kombiniert erfolgen soll. Gerade bei mobilen Arbeitsplätzen, die nur gelegentlich mit dem Firmennetzwerk verbunden werden, empfiehlt sich eine Kombination der Varianten. Über die Schaltfläche **Einstellungen und Zeitplanung** können Sie des Weiteren für den jeweiligen Client individuelle Bezugseinstellungen für die Virensignaturen definieren.

Ein mit vollen Anwenderrechten freigeschalteter Client würde auf dem Client-Rechner also das folgende Kontextmenü zur Verfügung stellen:



Ausnahmeverzeichnisse für Scanjobs

Hier können Sie Ausnahmeverzeichnisse auf den Clients definieren, die bei der Durchführung von Scanjobs nicht geprüft werden sollen. Archiv- und Backup-Bereiche einer Festplatte oder Partition können z.B. gegebenenfalls als Ausnahmeverzeichnisse definiert werden.

? Ausnahmeverzeichnisse können für komplette **Gruppen** definiert werden. Falls die Clients in einer Gruppe unterschiedliche Ausnahmeverzeichnisse definiert haben, können neue Verzeichnisse hinzugefügt oder vorhandene gelöscht werden. Die speziell für einzelne Clients definierten Verzeichnisse bleiben dabei erhalten. Das gleiche Verfahren wird auch bei den Wächterausnahmen angewendet.

? **Besonderheit auf einem Linux-Fileserver**
Bei der Auswahl von Ausnahmeverzeichnissen werden das Root-Laufwerk (/) und alle Freigaben zurück geliefert. Dabei können Laufwerksausnahmen, Verzeichnisausnahmen und Dateimasken angelegt werden.

Wächter

Hier können die Wächtereinstellungen für den im **Clientauswahlbereich** selektierten Client vorgenommen werden. Selektieren Sie eine Gruppe, um die Wächtereinstellungen alle Clients der Gruppe zu ändern. Im **Wächter**-Bereich können Sie für jeden Client/Gruppe individuelle Einstellungen vornehmen. Die geänderten Einstellungen werden erst nach Betätigung der **Übernehmen**-Schaltfläche gespeichert und von den Clients gesetzt. Drücken Sie die **Verwerfen**-Schaltfläche, um die aktuellen Einstellungen vom Managementserver zu laden ohne die Änderungen zu übernehmen.

? Wenn Sie die Wächtereinstellung einer **Gruppe** bearbeiten, können die einzelnen Parameter einen undefinierten Status einnehmen. Die Clients der Gruppe haben in diesem Fall unterschiedliche Einstellungen für den Parameter. Undefinierte Parameter werden beim Übernehmen nicht gespeichert.

Zunächst einmal sollten Sie ohne triftigen Grund den Wächter auf den Clients niemals ausschalten, da er erheblich zur Datensicherheit Ihres Netzwerks beiträgt. Sobald Sie den Wächter auf einem Client aktiviert haben, bleibt dieser automatisch immer im Hintergrund aktiv.

? Es kann bei der Verwendung bestimmter Programme oder Komponenten zu erheblichen Verzögerungen kommen (z.B. **T-Online**, **Microsoft Office** mit bestimmten **HP-Druckern**). Um dies zu umgehen, können Sie die INI-Dateien dieser Produkte als Ausnahmen definieren. Dies kürzt den Prüfprozess erheblich ab, stellt aber auch ein gewisses Sicherheitsrisiko dar. Hier gilt es abzuwägen.

Einstellungen

Folgende Funktionen stehen Ihnen im Einstellungen-Bereich zur Verfügung:

- **Wächterstatus:** Hier können Sie den Wächter anschalten bzw. ausschalten. Generell sollten Sie den Wächter eingeschaltet lassen. Er ist die Grundlage für einen permanenten und lückenlosen Virenschutz.
- **Engines benutzen:** Die *G Data Software* arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich.
- **Im Fall einer Infektion:** Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Client verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll.

Dateizugriff sperren: Auf eine infizierte Datei können weder Schreib- noch Lesezugriffe ausgeführt werden.

Desinfizieren (wenn nicht möglich: Zugriff sperren): Hier wird versucht, den Virus zu entfernen, falls das nicht möglich ist, dann wird der Dateizugriff gesperrt.

Desinfizieren (wenn nicht möglich: in Quarantäne): Hier wird versucht, den Virus zu entfernen, falls das nicht möglich ist, dann wird die Datei in die **Quarantäne** verschoben.

Desinfizieren (wenn nicht möglich: Datei löschen): Hier wird versucht, den Virus zu entfernen, falls das nicht möglich ist, dann wird die Datei gelöscht.

Datei in Quarantäne verschieben: Hier wird die infizierte Datei in die Quarantäne verschoben. Eine mögliche Desinfektion der Datei kann dann manuell durch den Systemadministrator durchgeführt werden.

Infizierte Datei löschen: Als rigorose Maßnahme hilft diese Funktion dabei, den Virus wirkungsvoll einzudämmen. Allerdings kann es dabei - je nach Virus - zu erheblichen Datenverlusten kommen.

- **Infizierte Archive:** Legen Sie hier fest, ob die Behandlung von Virenfunden für Archive anders erfolgen soll. Dabei sollten Sie bedenken, dass ein Virus innerhalb eines Archives erst dann Schaden anrichtet, wenn das Archiv entpackt wird.
- **Dateitypen:** Hier können Sie festlegen, welche Dateitypen von der *G Data Software* auf Viren untersucht werden sollen. In der Regel ist es nicht nötig, Dateien, die keinen ausführbaren Programmcode enthalten zu überprüfen; zumal eine Überprüfung aller Dateien eines Computers durchaus eine gewisse Zeit in Anspruch nehmen kann.
- **Beim Schreiben prüfen:** Normalerweise erzeugt ein virenfreies System beim Schreiben von Dateien natürlich keine vireninfizierten Dateien, um jedoch alle Eventualitäten auszuschließen, besonders bei Systemen, bei denen kein **BootScan** durchgeführt wurde, können Sie hier für einen Scanvorgang beim Schreiben von Dateien sorgen. Der immense Vorteil liegt hier darin, dass so auch Viren erkannt werden, die von einem anderen möglicherweise ungeschützten Client auf ein freigegebenes Verzeichnis des durch den Wächter geschützten Clients kopiert werden und dass aus dem Internet geladene Dateien schon beim Ladevorgang und nicht erst beim Ausführen als virenbehaftet erkannt werden.
- **Netzwerkzugriffe prüfen:** Hier können Sie die Vorgehensweise des Wächters im Zusammenhang mit Netzwerkzugriffen festlegen. Wenn Sie ihr gesamtes Netzwerk generell mit der *G Data Software* überwachen, kann eine Überprüfung der Netzwerkzugriffe entfallen.
- **Heuristik:** In der heuristischen Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken ermittelt, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist einerseits ein weiteres Sicherheitsplus, andererseits kann in seltenen Fällen auch ein **Fehlalarm** erzeugt werden.

- **Archive prüfen**: Das Überprüfen gepackter Daten in Archiven ist sehr zeitintensiv und kann in der Regel dann unterbleiben, wenn der *G Data Virenwächter* auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung. Um die Performance durch das unnötige Überprüfung großer Archiv-Dateien, die selten verwendet werden, nicht zu belasten, können Sie die Größe der Archivdateien, die durchsucht werden, auf einen bestimmten Wert in Kilobyte begrenzen.
- **E-Mail Archive prüfen**: Diese Option sollte in der Regel ausgeschaltet werden, da die Prüfung von E-Mail-Archiven in der Regel sehr lange dauert und im Falle einer infizierten Mail überhaupt keine Mails mehr gelesen werden können. Da der Wächter die Ausführung von infizierten E-Mail-Anhängen blockiert, wird durch das Ausschalten dieser Option kein Sicherheitsloch geschaffen. Bei der Verwendung von **Outlook** werden die ein- und ausgehenden Mails zusätzlich durch ein integriertes PlugIn geprüft.
- **Systembereiche beim Systemstart prüfen**: Systembereiche (z.B. **Bootsektoren**) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim Medium-Wechsel (neue CD-ROM o.ä.). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Systembereiche beim Medium-Wechsel prüfen**: Systembereiche (z.B. **Bootsektoren**) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim **Medium-Wechsel** (neue CD-ROM o.ä.). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Auf Dialer / Spyware / Adware / Riskware prüfen**: Mit der *G Data Software* können Sie Ihr System auch auf **Dialer** und andere Schadprogramme (**Spyware**, **Adware**, **Riskware**) überprüfen. Hierbei handelt es sich z.B. um Programme, die von ihnen ungewünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen, die z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch ihre Passwörter) heimlich speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.

Ausnahmen

Hier können Sie beim Client die Virenkontrolle auch auf bestimmte Verzeichnisse begrenzen. Auf diese Weise können Sie z.B. Ordner mit selten benötigten Archiven aussparen oder in ein spezielles Scanschema integrieren. Des Weiteren lassen sich bestimmte Dateien und Dateitypen von der Virenprüfung ausschließen. Folgende Ausnahmen sind möglich:

- **Laufwerk:** Wählen Sie hier mit Anklicken der Verzeichnis-Schaltfläche ein Laufwerk (**Partition**, **Festplatte**) aus, welches Sie vom Wächter nicht kontrollieren lassen möchten.
- **Verzeichnis:** Wählen Sie hier mit dem Anklicken der Verzeichnis-Schaltfläche einen **Ordner** (gegebenenfalls inkl. seiner darin befindlichen **Unterordner**) aus, der nicht vom Wächter kontrolliert werden soll.
- **Datei:** Hier können Sie den Namen der Datei eingeben, die Sie von der Wächterkontrolle ausnehmen möchten. Sie können hier auch mit Platzhaltern arbeiten (z.B. das Fragezeichen (?) für ein beliebiges Zeichen oder das Sternchen (*) für eine beliebige Zeichenfolge).

Sie können diesen Vorgang bei Bedarf beliebig oft wiederholen und im **Wächter Ausnahmen**-Fenster vorhandene Ausnahmen auch wieder löschen oder modifizieren.



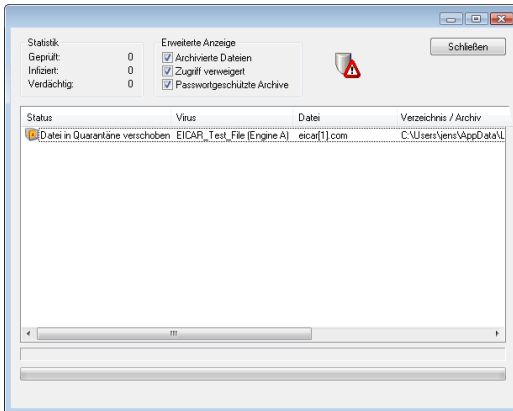
Die Funktionsweise von **Platzhaltern** ist folgendermaßen:

- Das **Fragezeichen-Symbol** (?) ist Stellvertreter für einzelne Zeichen.
- Das **Sternchen-Symbol** (*) ist Stellvertreter für ganze Zeichenfolgen.

Um z.B. sämtliche Dateien mit der Dateiendung **exe** schützen zu lassen, geben Sie also ***.exe** ein. Um z.B. Dateien unterschiedlicher Tabellenkalkulationsformate zu schützen (z.B. **xlr**, **xls**), geben Sie einfach ***.xl?** ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu schützen, geben Sie beispielsweise **text*. *** ein.

Warnmeldungen

Hier können Sie festlegen, ob der Anwender auf dem Client-Rechner über einen Virenfund benachrichtigt wird. Wenn das Häkchen hier gesetzt ist, erscheint beim Anwender ein Info-Fenster, welches ihn über den Virenfund in Kenntnis setzt.



Status

Hier wird Ihnen angezeigt, ob Sie die am Wächter durchgeführten Änderungen schon für den Client oder die Gruppe übernommen haben oder Sie die **Übernehmen**-Schaltfläche noch nicht gedrückt haben.

E-Mail

Auf jedem *G Data Client* kann ein gesonderter Virenschutz für E-Mails eingerichtet werden. Hierbei werden die Protokolle **POP3**, **IMAP** und **SMTP** auf **TCP/IP-Ebene** überprüft. Für **Microsoft Outlook** findet darüber hinaus ein spezielles **PlugIn** Verwendung. Das PlugIn überprüft automatisch alle eingehenden Mails auf Viren und verhindert, dass infizierte Mails versendet werden. Mit der Schaltfläche **Übernehmen** akzeptieren Sie dabei durchgeführte Änderungen, mit **Abbrechen** verlassen Sie den Dialog ohne die durchgeführten Änderungen zu übernehmen. Über den Administrator können Sie für jeden Client oder für Benutzergruppen individuelle Konfigurationen für den Umgang mit Mails erstellen. Sie haben dabei die Auswahl aus folgenden Optionen:

Eingehende Mails

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Im Fall einer Infektion**: Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Client verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll.
- **Empfangene Mails auf Viren prüfen**: Mit Aktivierung dieser Option werden sämtliche E-Mails auf Viren überprüft, die den Client online erreichen.
- **Ungelesene Mails beim Programmstart prüfen (nur für Microsoft Outlook)**: Diese Option dient dazu, E-Mails auf Virenbefall zu kontrollieren, die den Client erreichen, während dieser nicht mit dem Internet verbunden ist. Sobald **Outlook** geöffnet wird, werden deshalb sämtliche ungelesenen Mails im Posteingang-Ordner und den darin enthaltenen Unterordnern kontrolliert.
- **Bericht an empfangene, infizierte Mails anhängen**: Sobald eine an den Client geschickte E-Mail einen Virus enthält, erhalten Sie im Body dieser Mail unter dem eigentlichen Mailtext die Meldung **ACHTUNG! Diese Mail enthält folgenden Virus** gefolgt vom Namen des Virus. Außerdem finden Sie vor dem eigentlichen Betreff die Mitteilung **VIRUS**. Sollten Sie die Option **Anhang/Text löschen** aktiviert haben, wird Ihnen außerdem mitgeteilt, dass der infizierte Teil der E-Mail gelöscht wurde.

Ausgehende Mails

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Mails vor dem Senden prüfen**: Damit aus Ihrem Netzwerk nicht versehentlich selbst Viren verschickt werden, bietet die *G Data Software* auch die Möglichkeit, Mails vor dem Versenden auf Virenbefall zu überprüfen. Sollte tatsächlich ein Virus versendet werden, erscheint die Meldung **Die Mail [Betreffzeile] enthält folgenden Virus: [Virusname]**. Die Mail kann nicht verschickt werden und die entsprechende E-Mail wird nicht versandt.

- **Bericht an ausgehende Mails anhängen:** Ein Prüfbericht wird im Body jeder ausgehenden E-Mail unter dem eigentlichen Mailtext angezeigt. Dieser lautet Virengeprüft von G DataAntiVirus, so lange Sie die Option **Mails vor dem Senden prüfen** aktiviert haben. Zusätzlich können Sie hier das Versionsdatum von *G Data AntiVirus* (**Versionsinformation**) sowie einen Link zum **G Data Virenlexikon** angeben (**Virus News**).

Scanoptionen

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Engines benutzen:** Die *G Data Software* arbeitet mit zwei AntiViren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich; d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen.
- **OutbreakShield:** Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Virensignaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Virensignaturen besteht. Unter **Ändern** können Sie festlegen, ob das OutbreakShield zur Steigerung der Erkennungsleistung zusätzliche Signaturen verwendet. Das Laden der Signaturen kann zu einem automatischen Aufbau einer Internetverbindung führen. Außerdem können Sie hier die Zugangsdaten für die Internetverbindung eingeben, die dem OutbreakShield ein automatisches Signaturndownload aus dem Internet ermöglichen.

Warnmeldungen

Anwender bei Virenfund benachrichtigen: Sie können den Empfänger einer infizierten Nachricht automatisch über diesen Tatbestand informieren. Dazu wird diesem eine Warnmeldung auf seinem Desktop angezeigt.

Outlook-Schutz

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Microsoft Outlook durch ein integriertes Plugin schützen**: Mit Aktivierung dieser Funktion wird in das **Outlook** des Clients im Menü **Extras** eine neue Funktion namens **Ordner auf Viren überprüfen** eingefügt. Unabhängig von den Administrator-Einstellungen kann der Nutzer des einzelnen Clients den jeweils momentan ausgewählten Mailordner nach Viren durchsuchen. Im Ansichtsfenster einer E-Mail können Sie im Menü **Extras** über **Mail auf Viren überprüfen** eine Virenkontrolle der Dateianlagen durchführen. Nach Abschluss des Vorgangs erscheint ein Info-Bildschirm, in dem das Ergebnis der Virenprüfung zusammengefasst wird. Hier erfahren Sie, ob die Virenanalyse vollständig erfolgte, erhalten Infos über die Anzahl der untersuchten Mails und Dateianhänge, etwaige Lesefehler sowie über gefundene Viren und wie damit verfahren wurde. Beide Fenster können Sie mit einem Klick auf die Schaltfläche **Schließen** ausblenden.
- **Ports-Überwachung**: Generell werden die **Standardports** für **POP3**, **IMAP** und **SMTP** überwacht. Sollten die Porteeinstellungen in Ihrem System davon abweichen, können Sie dies entsprechend anpassen.

Web/IM

Folgende Einstellungen können Sie hier vornehmen.

Internetinhalte (HTTP)

- **Internetinhalte (HTTP) verarbeiten**: In den Web-Optionen können Sie bestimmen, dass sämtliche **HTTP-Webinhalte** schon beim Browsen auf Viren überprüft werden. Infizierte Webinhalte werden dann gar nicht erst ausgeführt und die entsprechenden Seiten nicht angezeigt. Setzen Sie hierzu bitte das Häkchen bei **Internetinhalte (HTTP) verarbeiten**.
- **Zeitüberschreitung im Browser vermeiden**: Da die *G Data Software* die Web-Inhalte vor Ihrer Darstellung im Internet Browser bearbeitet und dafür je nach Datenaufkommen eine gewisse Zeit benötigt, kann es vorkommen, dass eine Fehlermeldung im Internet Browser erscheint, weil dieser nicht sofort die Daten zugestellt bekommt, da diese ja von der Antivirensoftware auf Schadroutinen überprüft werden. Mit Setzen des Häkchens bei **Zeitüberschreitung im Browser vermeiden** wird eine solche Fehlermeldung unterdrückt und sobald sämtliche Browserdaten auf Viren überprüft wurden, werden diese dann ganz normal an den Internetbrowser überreicht.
- **Größenbegrenzung für Downloads**: Hiermit können Sie die HTTP-Überprüfung für zu große Webinhalte unterbrechen. Die Inhalte werden dann vom Virenwächter überprüft, sobald etwaige Schadroutinen aktiv werden. Der Vorteil bei dieser Größenbegrenzung liegt darin, dass es beim Surfen im Web nicht zu Verzögerungen durch die Virenkontrolle kommt.

Instant Messaging

- **IM-Inhalte verarbeiten**: Da auch über Instant Messaging-Tools Viren und andere Schadprogramme verbreitet werden können, kann die *G Data Software* auch hier die Anzeige und den Download infizierter Daten im Vorfeld unterbinden. Sollten Ihre Instant Messaging-Anwendungen nicht über die Standardportnummern ablaufen, geben Sie bitte unter Serverportnummer(n), die entsprechenden **Port-Adressen** ein.
- **Instant Messaging (Integration in der IM-Anwendung)**: Sollten Sie den **Microsoft Messenger (ab Version 4.7)** oder **Trillian (ab Version 3.0)** verwenden, können Sie durch Setzen des Häkchens für das jeweilige Programm ein Kontextmenü definieren, in dem Sie verdächtige Dateien direkt auf Viren überprüfen können.

- ?** Wenn Sie die Internetinhalte nicht prüfen lassen wollen, greift natürlich der **Virenwächter** dann ein, wenn infizierte Dateien gestartet werden. Das System auf dem jeweiligen Client ist also auch ohne die Überprüfung von Internetinhalten geschützt, solange der Virenwächter aktiviert ist.

AntiSpam

Folgende Einstellungen können Sie hier vornehmen.

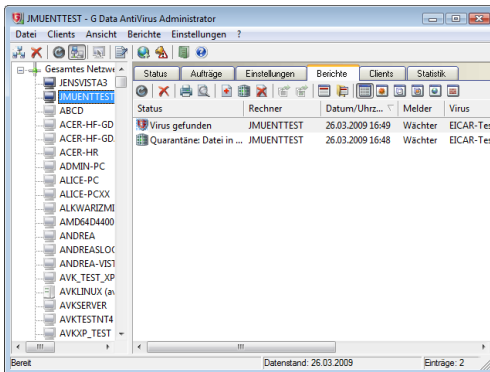
Spamfilter

Wenn Sie das Häkchen bei **Spamfilter verwenden** setzen, wird der E-Mail-Verkehr des Clients auf eventuelle Spam-Mails überprüft. Sobald eine E-Mail als Spam erkannt wird oder unter Spamverdacht fällt, können Sie eine Warnung definieren, die dann im Betreff der Mail angezeigt wird.

- ?** Über die Warnung können Sie - oder der Anwender - auf dem Client im Mailprogramm eine Regel definieren, nach der z.B. Mails, die die Meldung **[Spam]** in der Betreffzeile haben, automatisch in den Papierkorb oder einen speziellen Ordner für Spam- und Junk-Mail verschoben werden.

Berichte

Alle Virenfunde werden in diesem Aufgabenbereich angezeigt. In der ersten Spalte der Liste wird der Status des Berichtes angezeigt (z.B. **Virus gefunden** oder **Datei in Quarantäne verschoben**). Sie können auf Virenfunde reagieren, indem Sie die Einträge in der Liste selektieren und anschließend im Kontextmenü (rechte Maustaste) oder in der Symbolleiste einen Befehl wählen. So lassen sich beispielsweise infizierte Dateien löschen oder in den **Quarantäne-Ordner** verschieben.



Im Aufgabenbereich **Berichte** erscheinen alle Berichte unter dem von Ihnen vorgegebenen Namen und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach unterschiedliche Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet.

Folgende Kriterien stehen Ihnen dabei zur Auswahl:

- **Status:** Hier erhalten Sie den Inhalt des jeweiligen Berichts kurz und prägnant angezeigt. Aussagekräftige Symbole unterstreichen die Wichtigkeit und Art der jeweiligen Meldung.
- **Rechner:** Der Computer, von dem der jeweilige Bericht erfolgte, wird hier aufgezeigt. Bei Benutzergruppen werden alle Rechner einzeln aufgelistet.
- **Datum/Uhrzeit:** Das Datum, an dem der Bericht entweder auf Grund eines akuten Virenfundes durch den *G Data Wächter* oder auf Basis eines Scanjobs angelegt wurde.
- **Melder:** Über diesen Eintrag erfahren Sie, ob der Bericht vom **Virens Scanner** auf Basis eines Scanjobs erfolgte, automatisch über den **Wächter** gemeldet wurde oder über das *G Data-Mail PlugIn*.
- **Virus:** Soweit bekannt, wird hier der Name des gefundenen Virus angezeigt.

- **Datei/Mail:** Hier wird die Datei aufgelistet, in der ein Virus gefunden wurde oder bei der ein Virenverdacht besteht. Bei ***E-Mails*** finden Sie zusätzlich die Mail-Adresse des Absenders hier aufgelistet.
- **Ordner:** Die Verzeichnisinformationen der jeweiligen Datei sind wichtig für den Fall, dass eine Datei in die Quarantäne verschoben und nachträglich wieder zurückbewegt werden soll.



In der Menüleiste steht Ihnen für den Aufgabenbereich **Berichte** ein zusätzlicher Menüeintrag zur Verfügung. Für die Funktionen, die mit Dateien operieren (löschen, zurückbewegen etc.) müssen Sie in der Berichtsübersicht die jeweilige Datei bzw. Dateien markieren. Folgende Funktionen können Sie hier auswählen.

- **Ansicht:** Geben Sie hier an, ob Sie sich alle Berichte, nur Berichte mit nicht entfernten Viren oder nur Quarantäneberichte anzeigen lassen wollen. Sie können sich auch den Inhalt der Quarantäne anzeigen lassen.
- **Abhängige Berichte ausblenden:** Wenn auf Grund verschiedener Aufträge oder mehrfach durchgeführter Aufträge eine Virenmeldung oder ein Bericht doppelt oder mehrfach angezeigt wird, können Sie hiermit die Duplikate ausblenden. Nur der aktuellste Eintrag wird dann angezeigt und kann bearbeitet werden.
- **Archivierte Dateien ausblenden:** Hier können Sie Meldungen über Berichte aus Archivprüfungen aus- oder einblenden. Bei einem Virenfund in einem Archiv erstellt die **G Data Software** generell zwei Meldungen, wobei die erste Meldung darauf hinweist, dass ein Archiv infiziert ist und die zweite Meldung darauf hinweist, welche Datei genau in DIESEM Archiv befallen ist. Wenn Sie die Funktion **Archivierte Dateien ausblenden** nutzen, werden diese beiden Meldungen zusammengefasst.

Wenn Sie die **Scanjobs** auf Ihrem System so eingestellt haben, dass diese den Virenbefall lediglich protokollieren, können Sie die Virenbekämpfung auch manuell durchführen. Wählen Sie dazu im Bericht eine oder mehrere protokollierte Datei/en aus und führen Sie dann die gewünschte Operation durch:

- **Virus aus der Datei entfernen:** Versucht den Virus aus der Originaldatei zu entfernen.
- **Datei in die Quarantäne verschieben:** Verschiebt die Datei in den **Quarantäne**-Ordner.

- **Datei löschen**: Löscht die Originaldatei auf dem Client.
- **Quarantäne: Säubern und zurückbewegen**: Es wird versucht, den Virus aus der Datei zu entfernen. Wenn dies gelingt, wird die gesäuberte Datei zurück an Ihren Ursprungsort auf dem jeweiligen Client bewegt. Wenn der Virus nicht entfernt werden kann, wird die Datei auch nicht zurückbewegt.
- **Quarantäne: Zurückbewegen**: Verschiebt die Datei aus dem Quarantäne-Ordner zurück auf den Client. **Achtung**: Die Datei wird in ihrem Originalzustand wiederhergestellt und ist weiterhin infiziert.
- **Quarantäne: Zur Internet-Ambulanz senden**: Sollten Sie einen neuen Virus oder ein unbekanntes Phänomen feststellen, senden Sie uns bitte in jedem Fall diese Datei über die Quarantäne-Funktion der *G Data Software*. Wir analysieren den Virus und werden Ihnen möglichst schnell ein Gegenmittel zur Verfügung stellen. Selbstverständlich behandelt unser ***Emergency-AntiViren Service*** Ihre eingesandten Daten höchst vertraulich und diskret.
- **Löschen**: Löscht die selektieren Berichte. Wenn Berichte gelöscht werden sollen, zu denen eine Quarantäne-Datei gehört, müssen Sie das Löschen noch einmal bestätigen. In diesem Fall werden auch die in Quarantäne befindlichen Dateien gelöscht.
- **Abhängige Berichte löschen**: Wenn auf Grund verschiedener Aufträge oder mehrfach durchgeführter Aufträge eine Virenmeldung oder ein Bericht doppelt oder mehrfach angezeigt wird, können Sie hiermit die doppelten Einträge in der Protokolldatei löschen.

Aktualisieren



Diese Funktion aktualisiert die Ansicht. Lädt die aktuellen **Berichte** vom Managementserver.

Berichte löschen



Hiermit löschen Sie die selektierten Berichte. Wenn Berichte gelöscht werden sollen, zu denen eine **Quarantäne**-Datei gehört, müssen Sie das Löschen noch einmal bestätigen. In diesem Fall werden auch die in Quarantäne befindlichen Dateien gelöscht.

Drucken



Hiermit starten Sie den Druckvorgang für die Berichte. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details und Bereiche Sie ausdrucken lassen möchten.

Seitenansicht



Über die Seitenansicht-Funktion können Sie sich vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben lassen.

Virus entfernen

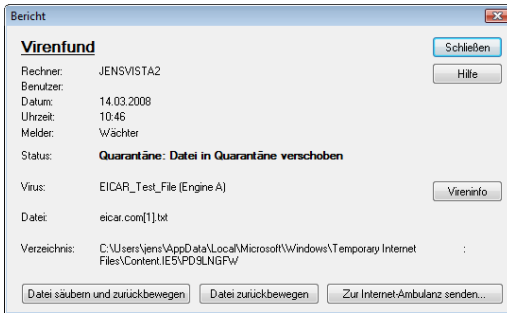


Mit dieser Funktion können Sie versuchen, den Virus manuell aus der Originaldatei zu entfernen. Ob dieser Versuch erfolgreich war, wird Ihnen in der Übersicht angezeigt.

In Quarantäne verschieben



Diese Funktion verschiebt die ausgewählten Dateien in den Quarantäne-Ordner. Die Dateien werden verschlüsselt im **Quarantäne**-Ordner auf dem Managementserver gespeichert. Die Originaldateien werden gelöscht. Durch die Verschlüsselung ist sichergestellt, dass der Virus keinen Schaden anrichten kann. Beachten Sie bitte, dass zu jeder Datei in der Quarantäne ein Bericht gehört. Wenn Sie den Bericht löschen wird auch die Datei im Quarantäne-Ordner gelöscht. Sie können eine Datei aus dem Quarantäne-Ordner zur Untersuchung an den **Emergency-AntiViren Service** senden. Doppelklicken Sie dazu auf den Quarantäne-Bericht.



In dem Berichtdialog klicken Sie dann nach Eingabe des Einsendegrunds die Schaltfläche **Zur Internet Ambulanz senden**.

Datei löschen



Mit der Funktion **Datei löschen** löschen Sie die Originaldatei auf dem Client.

Datei aus Quarantäne zurückbewegen



Hiermit verschieben Sie eine Datei aus dem **Quarantäne**-Ordner zurück auf den Client.



Achtung: Die Datei wird in ihrem Originalzustand wiederhergestellt und ist weiterhin infiziert.

Datei säubern und aus Quarantäne zurückbewegen



Der Virus wird mit dieser Funktion aus der Datei entfernt und die gesäuberte Datei wird auf den Client zurückbewegt. Wenn der Virus nicht entfernt werden kann, verbleibt die Datei im **Quarantäne**-Ordner.

Anzeigeoptionen

Bei einer großen Anzahl unterschiedlicher Berichte ist es sinnvoll, diese sich nach bestimmten Kriterien anzeigen und auflisten zu lassen. Folgende Möglichkeiten stehen Ihnen hier zur Verfügung:



Abhängige Berichte ausblenden: Wenn auf Grund verschiedener Aufträge oder mehrfach durchgeführter Aufträge eine Virenmeldung oder ein Bericht doppelt oder mehrfach angezeigt wird, können Sie hiermit die Duplikate ausblenden. Nur der aktuellste Eintrag wird dann angezeigt und kann bearbeitet werden.



Archivierte Dateien ausblenden



Alle Berichte anzeigen



Alle Berichte mit nicht entfernten Viren anzeigen



Alle Quarantäne-Berichte anzeigen



Inhalt der Quarantäne anzeigen



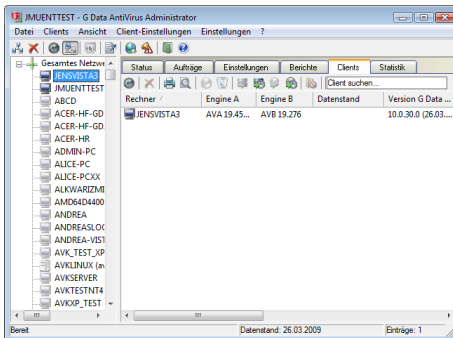
Alle HTTP-Berichte anzeigen



Alle Firewall-Berichte anzeigen

Clients

Selektieren Sie im **Clientauswahlbereich** eine Gruppe, um eine Übersicht über alle Clients der Gruppe zu erhalten. Für jeden Client wird angezeigt, welche Versionen die installierten Komponenten haben und wann der Client sich zum letzten Mal beim Managementserver gemeldet hat. Hier lässt sich leicht überprüfen, ob die Clients ordnungsgemäß laufen und ob die Internet Updates durchgeführt wurden.



Im Aufgabenbereich **Clients** stehen Ihnen folgende Informationen in einer Liste zur Verfügung. Sie lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach diversen Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet. Folgende Kriterien stehen Ihnen zur Verfügung:

- **Rechner:** Hier wird der Name des betreffenden Client angezeigt.
- **Engine:** Die Versionsnummer der Virendatenbanken und das Datum Ihrer letzten Aktualisierung per Internet Update werden hier angezeigt.
- **Datenstand:** Das Datum, an dem der Status der Virendatenbank auf dem Client aktualisiert wurde. Dieses Datum ist nicht identisch mit dem Aktualisierungsdatum der Virendatenbank.
- **Version G Data Client:** Hier finden Sie Versionsnummer und das Erstellungsdatum der verwendeten *G Data Client-Software*.
- **Letzter Zugriff:** Über diesen Eintrag erfahren Sie, zu welchem Zeitpunkt der *G Data Client* das letzte Mal aktiv war.
- **Update Virendatenbank:** Hier erfahren Sie, ob das Update der aktuellsten Virendatenbank *erledigt* ist, ob ein Auftrag dazu erteilt wurde oder ob es zu Irregularitäten oder Fehlern kam.
- **Update Programmdateien:** Wenn neue Updates der Client-Software erfolgen, erhalten Sie hier die entsprechende Statusinformation.

- **Zeitpunkt:** Das Datum, an dem der Status der Programmdateien auf dem Client aktualisiert wurden.
- **Ausnahmeverzeichnisse:** Soweit Sie für den jeweiligen Client Ausnahmeverzeichnisse angelegt haben, die nicht in die Virenkontrolle miteinbezogen werden sollen, werden die entsprechenden **Ausnahmetatbestände** hier angezeigt.



In der Menüleiste steht Ihnen für den Aufgabenbereich **Clients** ein zusätzlicher Menüeintrag namens **Client-Einstellungen** mit folgenden Funktionen zur Verfügung:

- **G Data Client installieren:** Installiert die Client-Software. Die Installation ist nur möglich, wenn die Clients bestimmte Voraussetzungen erfüllen.
- **G Data Client deinstallieren:** Erteilt dem *G Data Client* den Auftrag, sich selbst zu deinstallieren. Zum vollständigen Entfernen muss der Client-Rechner neu gestartet werden. Der Anwender wird durch eine Meldung dazu aufgefordert.
- **G Data Client für Linux installieren:** Sie können auch eine spezielle Client-Software auf Linux-Clients im Netzwerk installieren. Lesen Sie hierzu bitte das Kapitel ***Installation der Client-Software auf Linux-Rechnern*** im Anhang dieser Dokumentation.
- **G Data Subnet-Server zuordnen:** Während Sie mit der Funktion **Server verwalten** die Möglichkeit haben, Clients bestimmten **Subnet-Servern** zuzuordnen, können Sie über die Funktion **G Data Subnet-Server zuordnen** auch gezielt für den jeweiligen Client einen Subnet-Server auswählen.
- **Auf Defaulteinstellungen zurücksetzen:** Sie können für den Schutz des gesamten Netzwerks oder ausgewählter Gruppen **Defaulteinstellungen** erzeugen und damit schnell einheitliche Vorgaben für den Virenschutz vergeben. Um individuelle Regeln für einzelne Gruppen wieder auf den allgemeinen Stand zu bringen, können Sie die Defaulteinstellungen mit dieser Funktion auf die global definierten Standardwerte zurücksetzen.
- **Virendatenbank jetzt aktualisieren:** Aktualisiert die Virendatenbanken auf den Clients mit den Dateien vom Managementserver.

- **Virendatenbank automatisch aktualisieren**: Schaltet die automatische Aktualisierung der Virendatenbank ein. Die Clients prüfen periodisch, ob eine neue Version auf dem Managementserver existiert und führen die Aktualisierung automatisch durch.
- **Programmdateien jetzt aktualisieren**: Aktualisiert die Programmdateien auf den Clients mit den Dateien vom Managementserver. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gebootet werden muss.
- **Programmdateien automatisch aktualisieren**: Schaltet die automatische Aktualisierung der Programmdateien ein. Die Clients prüfen periodisch, ob eine neue Version auf dem Managementserver existiert und führen die Aktualisierung automatisch durch.
- **Neustart nach Aktualisierung Programmdateien**: Hier können Sie als Administrator festlegen, welche Priorität eine Aktualisierung der Programmdateien auf den Clients hat. So können Sie über **Hinweisfenster auf dem Client öffnen** einen Anwender darüber informieren, dass er seinen Client-Rechner zu einem geeigneten Zeitpunkt neustarten soll, über **Bericht erzeugen** an Hand der Protokolldateien im Bereich **Berichte** selbst tätig werden oder den **Neustart ohne Abfrage durchführen**.

Aktualisieren



Diese Funktion aktualisiert die Ansicht und lädt die aktuellen Clienteinstellungen vom Managementserver.

Löschen



Hiermit entfernen Sie einen Client aus einer **Gruppe**.

Drucken



Hiermit starten Sie den Druckvorgang für die Client-Einstellungen. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details und Bereiche der Client-Einstellungen Sie ausdrucken lassen möchten.

Seitenansicht



Hier können Sie vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben.

G Data Client installieren



Installiert die *G Data Client-Software*. Die Installation ist nur möglich, wenn die Clients bestimmte Voraussetzungen erfüllen.

Sie können die Clients auch vom **Managementserver** aus mit der *G Data Client-Software* ausstatten, soweit diese gewisse Grundvoraussetzungen erfüllen. Mit Aktivierung dieser Funktion öffnet sich ein Menü, in dem Sie die Zugriffsdaten für den Server eingeben, über den die Installation der *G Data Clients* erfolgen soll.

Nach Eingabe der entsprechenden Daten (die vom Programm gespeichert werden und deshalb nicht jedesmal eingegeben werden müssen), bestätigen Sie bitte mit **OK**. Nun öffnet sich eine Dialogbox, in der sämtliche verfügbaren Clients angezeigt werden. Wählen Sie hier einen oder mehrere deaktivierte Clients aus und klicken dann auf **Installieren**. Die *G Data Software* installiert dann automatisch die Client-Software auf die entsprechenden Rechner. Sollte die Installation der Software über die hier beschriebene **Remote-Installation** nicht möglich sein, können Sie diese auch manuell oder halbautomatisch auf den Clients installieren.

? Um auf **deaktivierte Clients** zugreifen zu können, müssen diese in der Verzeichnisansicht natürlich auch angezeigt werden. Bei Verwendung der Funktion **G Data Client installieren** weist Sie das Programm gegebenenfalls darauf hin und ermöglicht eine Darstellung der deaktivierten Clients.

? Sie können auch eine spezielle Client-Software auf **Linux-Clients** im Netzwerk installieren. Lesen Sie hierzu bitte das Kapitel **Installation der Client-Software auf Linux-Rechnern** im Anhang dieser Dokumentation.

? Bei der Installation der Client-Software werden Sie gefragt, ob auf dem Client-Rechner auch die **G Data Firewall** mitinstalliert werden soll. Weitere Informationen zur **Firewall** erhalten Sie im gleichnamigen Kapitel dieser Dokumentation.

G Data Client deinstallieren



Erteilt dem *G Data Client* den Auftrag, sich selbst zu deinstallieren. Zum vollständigen Entfernen muss der Client neu gestartet werden. Der Anwender wird durch eine Meldung dazu aufgefordert.

Virendatenbank aktualisieren



Aktualisiert die Virendatenbank auf dem Client mit den Dateien vom Managementserver.

Virendatenbank automatisch aktualisieren



Schaltet die **automatische Aktualisierung der Virendatenbank** ein. Die Clients prüfen periodisch, ob eine neue Version auf dem Managementserver existiert und führen die Aktualisierung automatisch durch.

Programmdateien aktualisieren



Aktualisiert die Programmdateien auf dem Client mit den Dateien vom Managementserver. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gebootet werden muss.

Programmdateien automatisch aktualisieren



Schaltet die automatische Aktualisierung der Programmdateien ein. Die Clients prüfen periodisch, ob eine neue Version auf dem Managementserver existiert und führen die Aktualisierung automatisch durch.

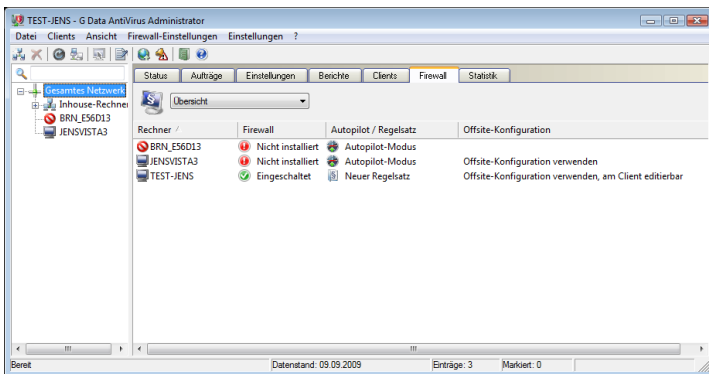
Ausnahmeverzeichnisse bearbeiten



Hier können Sie Ausnahmeverzeichnisse auf den Clients definieren, die bei der Durchführung von Scanjobs nicht geprüft werden sollen.

Firewall

Über diesen Bereich können Sie die Firewall auf den jeweiligen Clients oder Gruppen zentral administrieren. Über die oben befindliche Auswahlbox können Sie entscheiden, ob Sie eine Übersicht über den Firewallstatus der jeweiligen Client-Rechner administrieren möchten oder Regelsätze definieren.



Übersicht

In der Übersicht werden alle Client-Rechner oder die Clients einer ausgewählten Gruppe angezeigt. Hier sehen Sie auf einen Blick, welche Einstellungen die jeweilige Client-Firewall hat und können durch Anklicken des jeweiligen Clients direkt Änderungen vornehmen.

? **Regelsatz oder Autopilot?**

Es gibt zwei grundsätzlich verschiedene Möglichkeiten, eine Firewall zu betreiben.

- **Autopilot:** Wenn die Firewall auf "Autopilot" betrieben wird, ist sie schon standardmäßig von **G Data** vorkonfiguriert, erfüllt Ihre Aufgabe im Hintergrund und stört den Anwender nicht mit Rückfragen, mit denen sie sich selbstlernend zunehmend optimiert.
- **Regelsatz:** Als Administrator können Sie auch spezielle Firewallregeln für unterschiedliche Rechnerumgebungen definieren, so lassen sich z.B. Regelsätze für die direkte Verbindung mit dem Internet, vertrauenswürdige und nicht vertrauenswürdige Netzwerke oder auch andere Umgebungen definieren.

Folgende Informationen hält die Übersichtsliste für Sie bereit:

- **Rechner:** Der Name des Client-Rechners. Anhand des abgebildeten Symbols können Sie hier erkennen, ob die Client-Software auf diesem Client installiert ist.
- **Firewall:** Hier erfahren Sie, ob die Firewall auf dem Client eingeschaltet, ausgeschaltet oder ggf. gar nicht installiert ist.
- **Autopilot / Regelsatz:** Sie können verschiedenen Clients verschiedene Firewall-Funktionalitäten zuordnen. Vom anwenderfreundlichen Autopilot-Modus bis zu individuell definierten Regelsätzen.
- **Offsite-Konfiguration:** Wenn Sie für einen Client die Offsite-Konfiguration auswählen, kann der Anwender auf diesem Client seine Firewall-Einstellungen individuell verwalten und einstellen, solange er nicht mit dem Netzwerk des ManagementServers verbunden ist. Die Offsite-Konfiguration kann nur verwendet werden, wenn die Firewall im Firmennetz nicht im Autopilot-Modus betrieben wird.

Um die Firewall-Einstellungen für die in der Liste ausgewählten Clients zu ändern, klicken Sie den Eintrag einfach mit der rechten Maustaste an. Es öffnet sich ein Auswahlménü mit folgenden Optionen:

- **Einstellungen**: Über dieses Dialogfenster können Sie grundlegende Einstellungen an der jeweiligen Client-Firewall vornehmen. Lesen Sie hierzu bitte das Kapitel **Firewall-Einstellungen**.
- **Regelsatz erstellen**: Hiermit wechseln Sie in den Bereich **Regelsätze** und können individuelle Regeln für ihre Client-Firewalls definieren.
- **Regelsatz bearbeiten**: Hiermit wechseln Sie in den Bereich **Regelsätze** und können bestehende Regeln für ihre Client-Firewalls ändern.
- **Regelsatz auswählen**: Hier öffnet sich ein Dialog, in dem Sie aus schon definierten **Regelsätzen** auswählen können oder aber den **Autopilot**-Modus für die jeweilige Client-Firewall aktivieren.
- **Firewall installieren**: Über diese Funktion können Sie auf aktivierten Client-Rechnern zentral eine Firewall installieren und im Anschluss daran auch administrieren.
- **Firewall deinstallieren**: Mit dieser Funktion wird die bestehende Client-Firewall deinstalliert.

Firewall-Einstellungen

In dem Dialogfenster für die Firewall-Einstellungen können Sie grundlegende Vorgaben für die Funktionalität der jeweiligen Client-Firewall definieren:

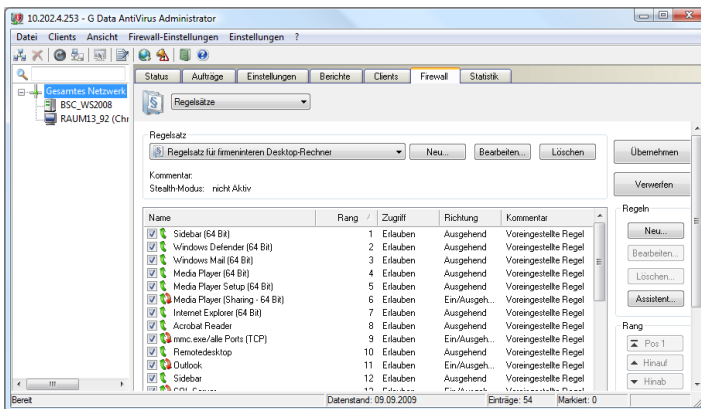
- **Firewall eingeschaltet**: Durch Setzen des Häkchens wird die Firewall auf dem jeweiligen Client aktiviert. Wenn Sie das Häkchen entfernen, ist die Firewall inaktiv.
- **Gesperrte Anwendungen melden**: Wenn dieses Häkchen gesetzt ist und der Client-Rechner mit dem Mangementsserver verbunden ist, erhält der Administrator im Bereich **Berichte** Informationen über Anwendungen, die durch die jeweilige Client-Firewall geblockt wurden.
- **Der Anwender darf die Firewall ein- und ausschalten**: Hier können Sie als Administrator dem Nutzer des Client-Rechners erlauben, die Firewall zwischenzeitlich auszuschalten. Diese Möglichkeit ist nur dann gegeben, solange sich der Client innerhalb des Firmennetzwerks befindet und sollte natürlich nur versierten Anwendern ermöglicht werden.

- **Offsite-Konfiguration für mobile Clients verwenden:** In der **Offsite-Konfiguration** werden die Firewall-Regelsätze des Client-Rechners, die in Ihrem Firmennetzwerk gelten, durch Standardregelsätze ersetzt, die automatisch den Umgang mit dem Internet, sicheren-, unsicheren und zu blockierenden Netzen regeln. Auf diese Weise ist der mobile Rechner optimal geschützt, solange er sich nicht im Netzwerk des Managementsservers befindet. Sobald der mobile Rechner wieder mit dem Netzwerk des Managementsservers verbunden wird, werden diese Standardregelsätze automatisch wieder durch die Regelsätze ersetzt, wie Sie für diesen jeweiligen Client in Ihrem Netzwerk gelten.
- **Der Anwender darf Offsite-Konfiguration ändern:** Diese Option soll es versierten Anwendern erlauben, Ihre Firewall außerhalb des Netzwerks individuell zu konfigurieren. Sobald der mobile Rechner wieder mit dem Managementserver verbunden wird, werden die durchgeführten Änderungen wieder durch die vom Administrator vorgegebenen Regeln für diesen Client ersetzt.

? Die **Offsite-Konfiguration** kann nur verwendet werden, wenn die Firewall im Firmennetz nicht im **Autopilot-Modus** betrieben wird. Wenn der jeweilige Client im Firmennetzwerk die Autopilot-Einstellungen für die Firewall verwendet, werden die Autopilot-Einstellungen auch dann verwendet, wenn der Client nicht mit dem Netzwerk verbunden ist.

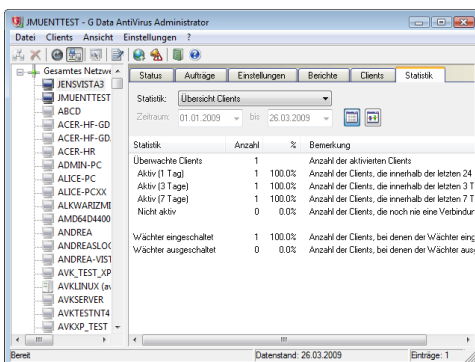
Regelsätze

Im Bereich **Regelsätze** können Sie individuelle Firewallregeln für alle Belange und Bereiche Ihres Netzwerks aufstellen. Ausführliche Informationen dazu, wie Sie Regeln erstellen, administrieren und nutzen können, finden Sie in der Dokumentation zur Nutzung der Firewall.



Statistik

In diesem Aufgabenbereich können Sie sich statistische Informationen zum Virenaufkommen und zu Infektionen auf Ihren Clients anzeigen lassen können. Wählen Sie dazu unter **Statistik** einfach aus, ob Sie eine allgemeine Übersicht über die Clients und ihre Interaktion mit dem Managementserver haben möchten (**Übersicht Clients**), eine Übersicht über die bekämpften Viren (**Hitliste Viren**) oder eine Auflistung der infizierten Clients (**Hitliste infizierte Clients**).



G Data Client

Die **Client-Software** stellt den Virenschutz für die Clients her und führt die Jobs vom Managementserver ohne Bedienungs Oberfläche im Hintergrund aus. Die Clients verfügen über eigene Virensignaturen und einen eigenen Scheduler, damit auch im offline-Betrieb (z.B. bei Notebooks) Virenanalysen durchgeführt werden können.

Installation der Clients



Die **Client-Software** stellt den Virenschutz für die Clients her und führt die Jobs vom Managementserver ohne Bedienungs Oberfläche im Hintergrund aus. Die Installation der Client-Software erfolgt in der Regel zentral für alle Clients über den Administrator aus. Hierbei werden Sie im Administratortool durch einen Einrichtungsassistenten unterstützt.

Sollte die Installation der Clients über das Netzwerk fehlschlagen, können Sie die Client-Software auch direkt auf den Client-Rechnern installieren. Zur Installation des Clients auf einem Client-Rechner legen Sie bitte die **G Data-CD-ROM** in das CD-ROM-Laufwerk des Client-Rechners ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data Client** durch einen Klick auf die nebenstehende Schaltfläche. Geben Sie bitte im Verlauf der Installation den **Servernamen** oder die **IP-Adresse des Servers** ein, auf dem der Managementserver installiert ist. Der Servername ist notwendig, damit der Client über das Netzwerk mit dem Server in Kontakt treten kann. Außerdem müssen Sie den **Computernamen** dieses Rechners eingeben, soweit dieser nicht automatisch angezeigt wird.



Zur Installation von Clients für Samba-Fileserver lesen Sie bitte im Anhang dieser Dokumentation das Kapitel: **Installation von Client für Samba-Fileserver**

Security-Symbol



Nach der Installation der Client-Software steht dem Benutzer des Client ein Symbol in der Startleiste zur Verfügung, über den dieser unabhängig von administrativen Vorgaben auch eigenständig sein System auf Virenbefall überprüfen kann.

Über die **rechte Maustaste** kann er dabei auf diesem *G Data Client-Symbol* ein **Kontextmenü** öffnen, das ihm folgende Funktionalitäten ermöglicht:

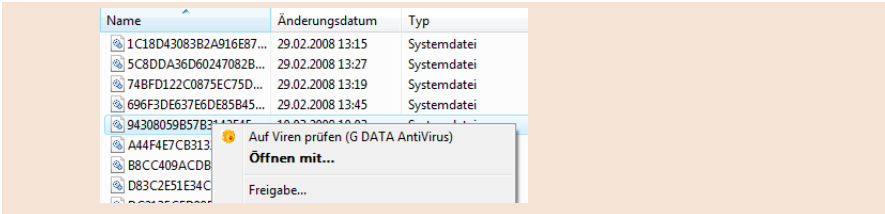


Virenprüfung

Über diese Funktionalität kann der Anwender gezielt mit dem *G Data Client* seinen Rechner auch außerhalb der vom Administrator vorgegebenen Prüfzeiträume auf Viren überprüfen. Ebenfalls kann der Anwender hier Disketten, CD-ROMs, den Speicher und Autostart-Bereich, sowie gezielt einzelne Dateien oder Verzeichnisse (Ordner) kontrollieren. Auf diese Weise können auch Notebook-Nutzer, die ihren Rechner nur selten mit dem Firmennetzwerk verbinden, gezielt Virenbefall unterbinden. Außerdem hat er nun die Möglichkeit, virenbefallene Dateien lokal in einen Quarantäne-Ordner zu schieben, so unschädlich zu machen und zur weiteren Begutachtung dem Netzwerkadministrator bei nächster Gelegenheit verfügbar zu machen.

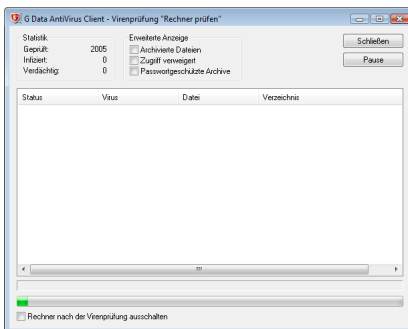


Der Anwender kann auch aus dem Explorer heraus Dateien oder Verzeichnisse einfach überprüfen, indem er die Dateien oder Verzeichnisse markiert und dann in dem **Kontextmenü** der rechten Maustaste die Funktion **Auf Viren prüfen (G Data AntiVirus)** verwendet.



Während einer laufenden Virenprüfung wird das Kontextmenü um folgende Einträge erweitert:

- **Priorität Virenprüfung:** Der Anwender hat hier die Möglichkeit, die Priorität der Virenprüfung festzulegen. Bei **Hoch** erfolgt die Virenprüfung schnell, allerdings kann sie das Arbeiten mit anderen Programmen an diesem Rechner deutlich verlangsamen. Bei der Einstellung **Niedrig** dauert die Virenprüfung hingegen vergleichsweise lang, dafür kann währenddessen aber ohne größere Einschränkungen am Client-Rechner weitergearbeitet werden.
- **Virenprüfung anhalten:** Hiermit kann der Anwender die Virenprüfung unterbrechen und zu einem späteren Zeitpunkt wieder aufnehmen.
- **Virenprüfung abbrechen:** Soweit der Administrator die Option **Der Anwender darf Wächteroptionen ändern** aktiviert hat, kann ein Anwender auf dem Client die Virenkontrolle auf seinem Client auch abbrechen, auch, wenn die Prüfung manuell auf dem Client gestartet wurde.
- **Scanfenster anzeigen:** Hiermit kann sich der Anwender das Info-Fenster anzeigen lassen, in dem Verlauf und Fortschritt der Virenprüfung angezeigt werden.



Wächter ausschalten

Über diesen Befehl kann der *G Data Wächter* vom Anwender für einen gewissen Zeitraum (von **5 Minuten** bis **zum nächsten Neustart des Rechners**) ausgeschaltet werden. Dies ist natürlich nur dann möglich, wenn er vom Administrator die entsprechenden Rechte erhalten hat. Das zeitweilige Ausschalten des Wächters kann z.B. bei umfangreichen Dateikopiervorgängen sinnvoll sein, da auf diese Weise der Kopiervorgang beschleunigt wird. Die Virenkontrolle ist in diesem Zeitraum allerdings ausgeschaltet. Hier gilt es also abzuwägen.

Optionen

Soweit der Administrator die Option **Der Anwender darf Wächteroptionen ändern** aktiviert hat, kann der Anwender auf dem Client die Optionen für die Virenprüfung auf seinem Rechner sowie die Optionen für den im Hintergrund laufenden Wächter auch an eigene Bedürfnisse anpassen.

? **Achtung:** Auf diese Weise können natürlich sämtliche Virenkontrollmechanismen auf dem Client quasi ausgeschaltet werden. Sie sollten als Administrator diese Option nur fachlich versierten Anwendern zur Verfügung stellen.

? Die sicherheitsrelevanten Einstellungen unter **Optionen** können auch für den Client-Rechner passwortgeschützt werden. Dazu vergibt der Administrator für den jeweiligen Client ein individuelles Passwort, mit dem der Anwender die Virenkontrollfunktionen auf dem Client verändern kann. Dieses Passwort wird über den Arbeitsbereich **Einstellungen** im Administrator unter **Passwortschutz für die Änderung von Optionen** vergeben.

Die einzelnen Einstellungsmöglichkeiten, die dem Anwender über den Bereich **Optionen** zur Verfügung stehen, werden ausführlich im Bereich **Programmaufbau des Administrators > Aufgabenbereiche > Einstellungen** in den folgenden Kapiteln erläutert:

- **Wächter**
- **E-Mail**
- **Virenprüfung**
- **Web-/IM-Filter**
- **Spamfilter**

- ? Wenn Sie dem Anwender auf seinem Client die Option **Der Anwender darf selbst Virenprüfungen durchführen** aktivieren, kann dieser unabhängig von den automatischen Virenkontrollen des Wächters seinen Clientrechner auf Viren überprüfen. Die Einstellungen, die für den Anwender auf dem Client hier möglich sind, entsprechen weitestgehend denen, wie Sie auch im **Wächter** Verwendung finden.

Quarantäne

Auch für Rechner, die momentan nicht mit dem von *G Data* überwachten Netzwerk verbunden sind, steht ein lokaler Quarantäne-Ordner zur Verfügung. Auf diese Weise können Anwender auch außer Haus (z.B. während einer Geschäftsreise) auf ihrem Notebook verdächtige Dateien in Quarantäne schieben und diese bei nächstbesten Gelegenheit im Firmennetzwerk begutachten lassen. Im Quarantäne-Ordner können Sie befallene Dateien desinfizieren, wenn dies nicht funktioniert löschen und ggf. auch aus der Quarantäne an ihren Ursprungsort zurückbewegen.

- ? **Achtung:** Beim Zurückbewegen wurde der Virus nicht entfernt. Sie sollten diese Option nur wählen, wenn das Programm ohne die befallene Datei nicht lauffähig ist und sie diese trotzdem zur Datenrettung benötigen.

Internet Update

Über den *G Data Client* können auch vom Client-Rechner aus selbstständig Internet Updates der Virensignaturen durchgeführt werden. Dies ist z.B. sinnvoll bei Notebooks, die zeitweise keinen Zugang zum Firmennetzwerk haben. Auch diese Funktionalität kann vom Administrator explizit für einzelne Clients freigeschaltet werden.

- ? Über die Schaltfläche **Einstellungen und Zeitplanung** kann auch die Aktualisierung der Virensignaturen auf dem Client zeitgesteuert ablaufen.

Firewall

Über den Firewallbereich können Anwender umfangreiche Einstellungen zur Firewall Ihres Client vornehmen, wenn diese Option für den jeweiligen Client serverseitig freigeschaltet wurde. So lange sich der Client im Netzwerk des ManagementServers befindet, wird die Firewall zentral vom Server aus administriert. Ausführliche Informationen über die Funktionalität dieser Firewall erhalten Sie in dem Kapitel **G Data Firewall**.

Info

Über **Info** kann die Version und Aktualität der Virendatenbank erfragt werden.

G Data WebAdministrator



Der *G Data WebAdministrator* ist eine Web basierte Steuerungssoftware für den Managementserver. Er kann mit Hilfe eines **Web-Browsers** gestartet werden.

Installation des WebAdministrators



Der **WebAdministrator** ist eine Web basierte Steuerungssoftware für den Managementserver. Er kann mit Hilfe eines **Webrowsers** gestartet werden. Bei der Installation des WebAdministrators werden Sie ggf. dazu aufgefordert, **Microsoft .NET Framework-Komponenten** zu installieren. Diese sind zum Betrieb des WebAdministrators unerlässlich. Nach der Installation ist ein Neustart erforderlich.



Achtung: VOR der Installation des WebAdministrators ist die Aktivierung der Windows-Funktion **Kompabilität mit IIS-Metabasis und IIS 6-Konfiguration** erforderlich. Sollte diese Funktion nicht zur Verfügung stehen, wird die Installation des WebAdministrators abgebrochen. Sie finden diesen Eintrag z.B. bei Windows Vista unter **Start > Systemsteuerung > Programme > Programme und Funktionen > Windows-Funktionen ein- oder ausschalten**. Hier können Sie den Eintrag unter **Internetinformationsdienste > Webverwaltungstools > Kompabilität mit der IIS 6-Verwaltung > Kompabilität mit IIS-Metabasis und IIS 6-Konfiguration** an- oder ausschalten. Außerdem müssen - soweit nicht schon geschehen - die **WWW-Dienste** aktiviert sein. Hierzu setzen Sie bitte das Häkchen unter **Internetinformationsdienste > WWW-Dienste**.

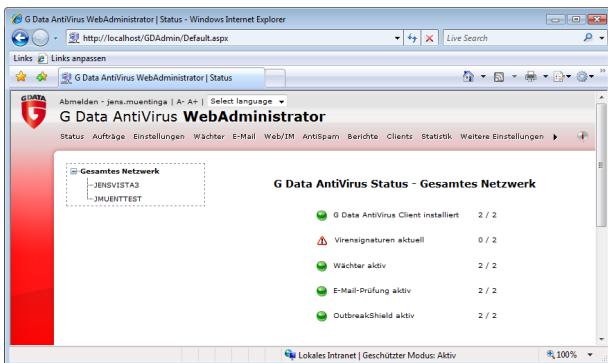
Nun können Sie den WebAdministrator installieren.



Nach der Installation steht Ihnen auf dem Desktop Ihres Computers das Symbol für den **G Data WebAdministrator** zur Verfügung.

Programmaufbau des WebAdministrators

Um den **WebAdministrator** zu nutzen, klicken Sie einfach auf das Desktop-Symbol des WebAdministrators. Nun öffnet sich automatisch Ihr Webbrowser mit einer Anmeldeseite für den Zugang zum WebAdministrator. Geben Sie hier nun wie beim regulären **Administrator** Ihre **Zugangsdaten** ein und klicken Sie dann auf die Schaltfläche **Anmelden**. Die Funktionalität des WebAdministrators entspricht sowohl inhaltlich, als auch in der Bedienung weitestgehend der des regulären **G Data Administrators**.



Firewall

Eine Firewall schützt Ihren Computer davor, ausgespäht zu werden. Sie überprüft, welche Daten und Programme aus dem Internet oder Netzwerk auf Ihren Rechner gelangen und welche Daten von Ihrem Computer gesendet werden. Sobald etwas darauf hindeutet, dass Daten auf Ihrem Rechner unberechtigt aufgespielt oder heruntergeladen werden sollen, schlägt die Firewall Alarm und blockt den unberechtigten Datenaustausch. In der Regel ist es sinnvoll, die Firewall im **Autopilot-Modus** zu verwenden. Sie läuft dann quasi im Hintergrund und schützt Sie, ohne dass Sie große Einstellungen vornehmen müssen.

? Wenn Sie die Firewall im **Autopilot-Modus** verwenden, bleibt Sie vollständig im Hintergrund und funktioniert selbstständig. Wenn Sie die Firewall **benutzerdefiniert** verwenden, erscheint in Zweifelsfällen ein Dialogfenster, in dem Sie die Firewall nach und nach auf Ihre Systemgegebenheiten hin optimieren. Der Autopilot-Modus ist bei der Installation der Firewall als Standard vorgegeben.



Sobald die Firewall installiert ist, verfolgt sie sämtliche Netzwerkaktivitäten Ihres Computers. Wenn Sie mit Ihrem Computer lokal arbeiten, fällt die Firewall nur durch das **Security-Symbol** in der Start-Leiste von Windows auf. Welche Funktionen Sie im Einzelnen über das Security-Symbol aufrufen können, erfahren Sie in dem Kapitel **Security-Symbol**.

Über die Schaltflächen **Konfigurieren** und **Erweitert** können Sie die Firewall individuell einstellen, wenn Sie den Autopilot-Modus nicht verwenden möchten.

Konfigurieren

Generell läuft die Firewall im Autopilot-Modus. Nur bei ausreichenden Kenntnissen im Umgang mit Netzwerken, Internetzugängen und Datentransfer an sich ist es ratsam, die Firewall-Einstellungen zu verändern. Wenn Sie die Firewall-Einstellungen individuell anpassen möchten, können Sie dies über die Firewall-Programmoberfläche. Anhand unterschiedlicher Karteikarten, die Sie über die links in der Firewall angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Verbindungsdetails überprüfen.

Status

Im Status-Bereich der Firewall erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und der Firewall. Diese finden sich rechts vom jeweiligen Eintrag als Text- oder Zahlenangabe. Darüber hinaus wird der Status der Komponenten auch grafisch dargestellt. Durch doppeltes Anklicken des jeweiligen Eintrags (oder durch Auswählen des Eintrags und Anklicken der **Bearbeiten**-Schaltfläche) können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit Warnsymbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Häkchensymbol.

- **Sicherheit:** Während Sie den Computer für ihre tägliche Arbeit nutzen, lernt die Firewall nach und nach, welche Programme Sie für den Zugang zum Internet nutzen, welche nicht und welche Programme ein Sicherheitsrisiko sind. Je nach dem, wie sehr sie sich in der Materie der Firewall-Technologie auskennen, können Sie die Firewall so konfigurieren, dass Sie Ihnen entweder einen sehr guten Basis-Schutz bietet, ohne viele Nachfragen zu stellen oder aber einen professionellen Schutz, der sich sehr genau an ihrem Computernutzungsverhalten ausrichtet, aber auch gewisse Kenntnisse von Ihnen als Anwender verlangt. Wenn Sie einen Doppelklick mit der Maus auf den Eintrag **Sicherheit** ausführen, haben Sie eine Auswahl aus folgenden Sicherheitsvarianten:

Autopilot-Modus (empfohlen): Hier arbeitet die Firewall vollkommen autonom und hält Gefahren automatisch vom heimischen PC ab. Diese Einstellung bietet einen praktischen Rundumschutz und ist in den meisten Fällen empfehlenswert.

Manuelle Regelerstellung: Wenn Sie Ihre Firewall individuell konfigurieren möchten oder bestimmte Anwendungen nicht mit dem Autopilot-Modus zusammenarbeiten wollen, können Sie über die manuelle Regelerstellung Ihren Firewallschutz ganz auf Ihre Bedürfnisse einrichten.

- **Modus:** Hier werden Sie darüber informiert, mit welcher Grundeinstellung Ihre Firewall gerade betrieben wird. Möglich wären hier entweder die manuelle Regelerstellung oder die Automatik (**Autopilot**).

- **Netzwerke:** Die Firewall überwacht natürlich sämtliche Netzwerkaktivitäten, wie z.B. ein **DFÜ-Netzwerk** und eine **LAN-Verbindung**. Sollten ein oder mehrere Netzwerke nicht geschützt werden, weil sie z.B. manuell von der Firewallüberwachung ausgenommen wurden, weist Sie ein Warnsymbol darauf hin. Ein Doppelklick auf den jeweiligen Eintrag öffnet ein Dialogfenster, über den Sie die Regeln und Einstellungen zum gewählten Netzwerk individuell konfigurieren können. Wählen Sie hier unter **Regelsatz** einfach aus, ob das jeweilige Netzwerk zu den **vertrauenswürdigen Netzwerken**, den **nicht vertrauenswürdigen Netzwerken** oder den **zu blockierenden Netzwerken** gehören soll.

? Die Einstellung **direkte Verbindung mit dem Internet** orientiert sich weitestgehend an den Einstellungen, die auch für **vertrauenswürdige Netzwerke** gelten.

? Jedem **Netzwerk** kann ein spezieller **Regelsatz** zugeordnet werden. Während Sie im Bereich **Netzwerke** sehen, welche Netzwerke auf Ihrem Computer vorhanden sind, sehen Sie im Bereich **Regelsätze**, welche automatischen oder selbst erstellten Regelsätze Ihnen in der Firewall zur Verfügung stehen.

- **Registrierte Angriffe:** Sobald die Firewall einen Angriff auf Ihren Computer registriert, wird dieser hier protokolliert und Sie können durch Anklicken des Menüpunktes weitergehende Informationen erhalten.
- **Anwendungs-Radar:** Der Anwendungs-Radar zeigt Ihnen, welche Programme momentan von der Firewall blockiert werden. Sollten Sie eine der blockierten Anwendungen doch die Erlaubnis für die Nutzung des Netzwerkes erteilen wollen, wählen Sie diese hier einfach aus und klicken dann die **Erlauben**-Schaltfläche an.

Netzwerke

Im Netzwerke-Bereich werden die Netzwerke (z.B. **LAN**, **DFÜ** etc.) aufgelistet, mit denen ihr Rechner verbunden ist. Hier wird auch aufgezeigt, nach welchem **Regelsatz** (siehe Kapitel **Regelsätze**) das jeweilige Netzwerk geschützt wird. Wenn Sie das Häkchen vor dem jeweiligen Netzwerk entfernen, wird dieses vom Firewall-Schutz ausgenommen. Sie sollten den Schutz allerdings nur in begründeten Einzelfällen abschalten. Wenn Sie ein Netzwerk mit der Maus markieren und die **Bearbeiten**-Schaltfläche anklicken, können Sie die Firewall-Einstellungen für dieses Netzwerk einsehen bzw. verändern.

Netzwerk bearbeiten

Beim Bearbeiten von Netzwerk-Einstellungen haben Sie die Auswahl, den **Regel-Assistenten** oder den **Profi-Dialog** zu verwenden. Generell ist der Regel-Assistent zu empfehlen, da er den Anwender beim Erstellen von Regeln und Einstellungen unterstützt.

- **Netzwerk-Info:** Hier erhalten Sie Informationen zum Netzwerk, als - soweit vorhanden - Angaben zu **IP-Adresse**, **Subnetzmaske**, **Standardgateway**, **DNS**- und **WINS**-Server.
- **Firewall aktiv, auf diesem Netzwerk:** Sie können die Firewall für das Netzwerk hier deaktivieren, sollten dies allerdings nur in begründeten Einzelfällen tun.
- **Gemeinsame Nutzung der Internet-Verbindung:** Bei direkten Verbindungen mit dem Internet können Sie festlegen, ob alle über ein **TCP/IP-Netzwerk** verbundenen Rechner Zugriff aufs Internet haben sollen oder nicht. Diese **Internetverbindungsfreigabe (ICS)** kann für ein Heimnetzwerk in der Regel aktiviert werden.
- **Automatische Konfiguration (DHCP) zulassen:** Bei der Verbindung Ihres Computers mit dem Netzwerk wird eine **dynamische IP-Adresse** (über das **DHCP = Dynamic Host Configuration Protocol**) vergeben. Wenn Sie über diese Standardkonfiguration mit dem Netzwerk verbunden sind, sollten Sie das Häkchen hier gesetzt lassen.
- **Regelsatz:** Sie können hier sehr schnell zwischen vorstrukturierten Regelsätzen wählen und auf diese Weise festlegen, ob es sich bezüglich der Überwachungskriterien der Firewall z.B. um ein vertrauenswürdigen, nicht vertrauenswürdigen oder zu blockierendes Netzwerk handelt. Mit der Schaltfläche **Regelsatz bearbeiten** haben Sie auch die Möglichkeit, die Regelsätze individuell zu konfigurieren. Lesen Sie hierzu bitte auch das Kapitel **Regelsätze**.

Regelsätze

In diesem Bereich können Sie für verschiedene Netzwerke spezielle Regeln erstellen. Diese Regeln werden dann jeweils zu einem Regelsatz zusammengefasst. Voreingestellt sind Regelsätze für ***direkte Verbindung mit dem Internet, nicht vertrauenswürdige Netzwerke, vertrauenswürdige Netzwerke*** und ***zu blockierende Netzwerke***. In der Übersicht wird der jeweilige Regelsatz mit Namen und Stealth-Modus-Status angezeigt. Mit Hilfe der Schaltflächen **Neu**, **Löschen** und **Bearbeiten** können Sie bestehende Regelsätze verändern, bzw. weitere Regelsätze hinzufügen.

? Mit dem **Stealth-Modus** (engl.: verborgen, heimlich) werden Anfragen an den Computer, die dazu dienen, die Erreichbarkeit der jeweiligen Ports zu überprüfen nicht beantwortet. Dies erschwert Hackern, auf diese Weise Informationen über das System zu erhalten.

? Die vorgegebenen Regelsätze für ***direkte Verbindung mit dem Internet, vertrauenswürdige Netzwerke, nicht vertrauenswürdige Netzwerke*** und ***zu blockierende Netzwerke*** können nicht gelöscht werden. Zusätzliche Regelsätze, die Sie selber erstellt haben, können Sie natürlich jederzeit löschen.

Regelsätze erstellen

Sie können jedem Netzwerk einen eigenen **Regelsatz** (also eine Sammlung speziell darauf abgestimmter Regeln) zuweisen. Auf diese Weise können Sie Netzwerke mit unterschiedlichen Gefährdungstufen unterschiedlich mit der Firewall absichern. So benötigt ein privates Heimnetzwerk sicherlich weniger Schutz (und damit auch Administrationsaufwand), als ein DFÜ-Netzwerk, das im direkten Kontakt mit dem Internet steht. Die Firewall beinhaltet drei voreingestellte Regelsätze für folgende Netzwerktypen:

- **Regelsatz für ein nicht vertrauenswürdiges Netzwerk**: Hierunter fallen in der Regel offene Netzwerke, wie z.B. **DFÜ-Netzwerke**, die auf das **Internet** Zugriff haben.
- **Regelsatz für ein vertrauenswürdiges Netzwerk**: Vertrauenswürdig sind in der Regel **Heim- und Firmennetzwerke**.

- **Regelsatz für ein zu blockierendes Netzwerk:** Wenn zeitweise oder dauerhaft der Kontakt des Rechners zu einem Netzwerk blockiert werden soll, kann diese Einstellung verwendet werden. Dies macht z.B. Sinn bei der Verbindung mit **fremden Netzwerken**, über deren Sicherheitsstandard man sich nicht ganz im Klaren ist (z.B. auf **LAN-Partys**, fremden Firmennetzwerken, öffentlichen Arbeitsplätzen für Notebooks etc.)

Sie können neu etablierten Netzwerken auf Ihrem Computer einen entsprechend ausgewählten Regelsatz zuordnen. Darüber hinaus können Sie über die **Neu**-Schaltfläche auch eigene Regelsätze für Netzwerke erstellen. Klicken Sie dazu im **Regelsätze**-Bereich auf die **Neu**-Schaltfläche und legen in dem erscheinenden Dialogfenster folgendes fest:

- **Regelsatzname:** Geben Sie hier einen aussagekräftigen Namen für den Regelsatz ein.
- **Einen leeren Regelsatz erzeugen:** Hier können Sie einen vollkommen leeren Regelsatz erzeugen und diesen ausschließlich mit selbstdefinierten Regeln bestücken.
- **Einen Regelsatz erzeugen, der einige sinnvolle Regeln enthält:** Bei dieser Auswahl können Sie entscheiden, ob beim neuen Regelsatz grundlegende Regeln für nichtvertrauenswürdige, vertrauenswürdige oder zu blockierende Netzwerke vordefiniert werden sollen. Auf Basis dieser Voreinstellungen können Sie dann individuelle Änderungen vornehmen.

Der neue Regelsatz erscheint nun im **Regelsätze**-Bereich unter dem jeweiligen Regelsatznamen (z.B. **Neuer Regelsatz**) in der Liste. Wenn Sie nun auf **Bearbeiten** klicken, öffnet sich - je nach Einstellung, die Sie unter **Sonstiges** (siehe gleichnamiges Kapitel) getroffen haben - der **Regel Assistent** oder der **Profi-Dialog** zum Bearbeiten der einzelnen Regeln dieses Regelsatzes.

Wie Sie in den Regelsätzen neue Regeln vergeben, lesen Sie in den Kapiteln **Regel Assistent verwenden** bzw. **Profi-Dialog verwenden**.

? Neben der direkten Eingabe von Regeln haben Sie natürlich noch die Möglichkeit über die Info-Box des Firewall-Alarms Regeln zu erstellen. Dieser Lernprozess der Firewall wird Ihnen im Kapitel **Firewall-Alarm** erläutert.

Regel Assistenten verwenden

Mit dem Regel Assistenten können Sie bestimmte zusätzliche Regeln für den jeweiligen Regelsatz definieren oder bestehende Regeln ändern. Gerade für Anwender, die sich nicht gut mit der Firewalltechnologie auskennen, ist der **Regel Assistent** dem **Profi-Dialog** vorzuziehen.

? Mit dem Regel Assistenten verändern Sie eine oder mehrere Regeln in dem jeweils ausgewählten Regelsatz. Sie erstellen also immer eine Regel innerhalb eines Regelsatzes, der verschiedene Regeln beinhaltet.

? Abhängig davon, welchen Regelsatz Sie für das jeweilige Netzwerk definiert haben, kann eine Anwendung in dem einen Regelsatz (z.B. für nicht vertrauenswürdige Netze) gesperrt sein, in dem anderen Regelsatz (z.B. für vertrauenswürdige Netze) vollen Netzzugriff haben. So könnten Sie z.B. einen Browser mit entsprechend unterschiedlichen Regeln so beschränken, dass er wohl auf Seiten zugreifen kann, die in ihrem Heimnetzwerk bereitstehen, aber keine Möglichkeit hat, auf Inhalte aus dem DFÜ-Netzwerk zuzugreifen.

Der Regel Assistent stellt Ihnen folgende Basisregeln zur Verfügung:

- **Einer bestimmten Anwendung den Zugriff erlauben oder verweigern:** Hiermit können Sie gezielt eine Anwendung (ein Programm) auf Ihrer Festplatte auswählen und ihm explizit den Zugriff auf das über den Regelsatz definierte Netzwerk erlauben oder verbieten. Wählen Sie im Assistenten dazu einfach das gewünschte Programm aus (**Programmpfad**) und geben Sie dann unter **Verbindungsrichtung** an, ob das Programm für eingehende Verbindungen, ausgehende Verbindungen oder sowohl ein-, als auch ausgehende Verbindungen gesperrt werden soll. Auf diese Weise können Sie z.B. ihre MP3-Playersoftware ggf. daran hindern, Daten über Ihre Hörgewohnheiten weiterzugeben (ausgehende Verbindungen) oder dafür sorgen, dass nicht automatisch Programmupdates aufgespielt werden (eingehende Verbindungen).

- **Einen bestimmten Internet-Dienst (Port) öffnen oder sperren:** Als **Port** werden spezielle Adressbereiche bezeichnet, die über ein Netzwerk übermittelte Daten automatisch an ein bestimmtes Protokoll und darüber an bestimmte Software weiterleiten. So wird z.B. die Übermittlung von regulären Webseiten über den Port 80 abgewickelt, E-Mail-Versand über den Port 25, E-Mail-Abholung über Port 110 usw. Ohne Firewall stehen an Ihrem Computer generell alle Ports offen, obwohl die meisten von normalen Anwendern gar nicht benötigt werden. Über das Sperren eines oder mehrerer Ports können deshalb schnell Lücken geschlossen werden, die sonst von Hackern für Angriffe genutzt werden könnten. Im Assistenten haben Sie die Möglichkeit Ports komplett zu sperren oder aber auch nur für eine bestimmte Anwendung (z.B. Ihre MP3-Abspielsoftware).
- **Datei- und Druckerfreigabe (NetBIOS) erlauben oder verweigern:** Das **NetBIOS** ist eine spezielle Schnittstelle in Netzwerken und kann dazu genutzt werden z.B. Datei- oder Druckerfreigaben direkt von Rechner zu Rechner durchzuführen, ohne dabei z.B. das TCP/IP-Protokoll zu nutzen. Da dies in Heimnetzwerken meistens unnötig ist und das NetBIOS von Hackern dazu genutzt werden kann, einen Rechner lahmzulegen, ist es in vielen Fällen ratsam, diese Freigabe für nicht vertrauenswürdige Netze zu verweigern.
- **Domänen-Dienste erlauben oder verweigern:** Eine **Domäne** ist eine Art Gliederungsverzeichnis für Computer in einem Netzwerk und ermöglicht damit eine zentralisierte Verwaltung der im Netzwerk eingebunden Rechner. Freigaben für Domänen-Dienste in nicht vertrauenswürdigen Netzen sollten in der Regel verweigert werden.
- **Gemeinsame Nutzung der Internet-Verbindung erlauben:** Bei direkten Verbindungen mit dem Internet können Sie festlegen, ob alle über ein **TCP/IP-Netzwerk** verbundenen Rechner Zugriff aufs Internet haben sollen oder nicht. Diese **Internetverbindungsfreigabe (ICS)** kann für ein Heimnetzwerk in der Regel aktiviert werden.
- **In den erweiterten Bearbeitungsmodus (Profi-Dialog) wechseln:** Hiermit können Sie vom Regel Assistenten zum **Profi-Dialog** wechseln. Informationen zum Profi-Dialog erhalten Sie im Kapitel **Profi-Dialog verwenden**.



Wenn Sie das Häkchen bei **Auch in Zukunft den Regel Assistenten starten** entfernen, öffnet die Firewall für neue Regeln automatisch den Profi-Dialog.

Profi-Dialog verwenden

Im Profi-Dialog können Sie - gewisse Kenntnisse in Netzwerksicherheit vorausgesetzt - sehr individuelle Regeln für das jeweilige Netzwerk definieren. Dabei können natürlich sämtliche Regeln erzeugt werden, die Sie auch über den Regel Assistenten erzeugen können, aber auch darüber hinaus weitergehende Einstellungen vorgenommen werden. Folgende Einstellungsmöglichkeiten stehen Ihnen hier zur Verfügung:

- **Name:** Hier können Sie den Namen für den aktuellen Regelsatz gegebenenfalls verändern. Unter diesem Namen wird der Regelsatz dann in der Liste im **Regelsätze**-Bereich angezeigt und kann mit den dort von der Firewall identifizierten Netzwerken kombiniert werden.
- **Stealth-Modus:** Mit dem Stealth-Modus (engl.: verborgen, heimlich) werden Anfragen an den Computer, die dazu dienen, die Erreichbarkeit der jeweiligen Ports zu überprüfen nicht beantwortet. Dies erschwert Hackern, auf diese Weise Informationen über das System zu erhalten.
- **Aktion, falls keine Regel zutrifft:** Hier können Sie festlegen, ob der Zugriff im Netzwerk generell erlaubt, verweigert oder auf Nachfrage geregelt werden soll. Sollten durch die **Lernfunktion** der Firewall für einzelne Programme Sonderregeln definiert sein, werden diese natürlich berücksichtigt.
- **Adaptiv-Modus:** Der Adaptiv-Modus unterstützt Sie bei Anwendungen, die die sogenannte **Rückkanal-Technik** verwenden (z.B. **FTP** und viele **Online-Spiele**). Solche Anwendungen verbinden sich mit einem entfernten Rechner und handeln mit ihm einen Rückkanal aus auf dem sich der entfernten Rechner mit Ihrer Anwendung "zurückverbindet". Ist der Adaptiv-Modus aktiv, so erkennt die Firewall diesen Rückkanal und lässt ihn zu ohne gesondert deshalb nachzufragen.

Regeln

In der Liste der Regeln finden Sie sämtliche Regeln, die als Ausnahmetatbestände für diesen Regelsatz definiert wurden. So können hier z.B. ausgewählten Programmen umfangreiche Netzzugriffe gestattet werden, obgleich das Netzwerk an sich als nicht vertrauenswürdig definiert wird. Die Regeln, die hier einfließen, können auf verschiedene Weise erzeugt worden sein:

- Über den **Regel Assistenten**
- Direkt über den **Profi-Dialog** über die **Neu**-Schaltfläche
- Über den Dialog in der Info-Bfox, die bei einem Firewall-Alarm erscheint.

Jeder Regelsatz hat natürlich eine eigene Liste mit Regeln.



Da die Firewall-Regeln teilweise hierarchisch verschachtelt sind, ist es in manchen Fällen wichtig, die **Rangfolge** bei den Regeln zu beachten. So kann es sein, dass eine Freigabe für einen Port durch die Verweigerung eines Protokollzugriffs wieder blockiert werden kann. Sie können den Rang einer Regel in der Abfolge ändern, indem Sie diese mit der Maus markieren und dann über die Pfeiltasten unter **Rang** in der Liste hinauf- oder hinab bewegen.

Wenn Sie eine neue Regel über den **Profi-Dialog** erstellen oder eine bestehende Regel über den **Bearbeiten-Dialog** verändern, erscheint der **Regel bearbeiten** Dialog mit folgenden Einstellungsmöglichkeiten:

- **Name:** Hier findet sich bei voreingestellten und automatisch generierten Regeln der **Programmname** für den die jeweilige Regel zutrifft. Sie können den Namen über die **Bearbeiten**-Schaltfläche auch jederzeit verändern oder um zusätzliche Informationen ergänzen.
- **Regel aktiv:** Sie können eine Regel durch Entfernen des Häkchens inaktiv setzen, ohne sie gleich zu löschen.
- **Kommentar:** Hier erfahren Sie, auf welche Weise die Regel erzeugt wurde. Bei für den Regelsatz voreingestellten Regeln steht **Voreingestellte Regel**, bei Regeln, die sich aus dem Dialog aus dem Firewall-Alarm ergeben steht **per Nachfrage generiert** und für Regeln, die Sie selber über den Profi-Dialog generieren, können Sie einen eigenen Kommentar einfügen.

- **Verbindungs-Richtung**: Mit der **Richtung** wird definiert, ob es sich bei dieser Regel um eine Regel für eingehende, ausgehende oder ein- und ausgehende Verbindungen handelt.
- **Zugriff**: Hier wird eingestellt, ob für das jeweilige Programm innerhalb dieses Regelsatzes der Zugriff erlaubt oder verweigert werden soll.
- **Protokoll**: Hier können Sie auswählen, welchen **Verbindungsprotokollen** Sie einen Zugriff erlauben oder verwehren wollen. Dabei haben Sie die Möglichkeit, Protokolle generell zu sperren oder freizugeben oder die Verwendung des Protokolls mit der Nutzung einer bestimmten Anwendung oder mehrerer Anwendungen zu koppeln (**Anwendungen zuordnen**). Genauso können Sie die unerwünschten bzw. erwünschten Ports über die Schaltfläche **Internet-Dienst zuordnen** genau definieren.
- **Zeitfenster**: Sie können den Zugriff auf Netzwerkressourcen auch zeitabhängig gestalten und so z.B. dafür sorgen, dass ein Zugriff nur zu Ihren Arbeitszeiten und nicht außerhalb dieser Zeiten erfolgt.
- **IP-Adressraum**: Gerade für Netzwerke mit fest vergebenen IP-Adressen macht es Sinn, deren Nutzung über eine Beschränkung des IP-Adressraumes zu reglementieren. Ein klar definierter IP-Adressraum verringert die Gefahr eines Hackerangriffs deutlich.

Firewall-Alarm

Generell fragt die Firewall im Modus **manuelle Regelerstellung** bei unbekannten Programmen und Prozessen, die mit dem Netzwerk in Verbindung treten wollen, nach, ob dies erlaubt oder verweigert werden soll. Dazu öffnet sich eine Info-Box, in der Ihnen Details zur jeweiligen Anwendung geliefert werden. Hier haben Sie auch die Möglichkeit, der Anwendung einen Zugriff auf das Netzwerk einmal oder auch dauerhaft zu erlauben oder zu verweigern. Sobald Sie einem Programm den Zugriff dauerhaft erlauben oder verweigern, wird dies als **Regel** in den **Regelsatz** des jeweiligen Netzwerkes aufgenommen und von nun an nicht mehr nachgefragt.



Hier stehen Ihnen folgende Schaltflächen zur Verfügung:

- **Immer erlauben**: Über diese Schaltfläche erstellen Sie für die oben aufgeführte Anwendung (z.B. ***Opera.exe*** oder ***Explorer.exe*** oder ***iTunes.exe***) eine Regel, die in dem genannten Netzwerk der Anwendung einen dauerhaften Zugriff aufs Netzwerk bzw. Internet erlaubt. Diese Regel finden Sie dann auch als auf Nachfrage erzeugte Regel im Bereich **Regelsätze**.
- **Temporär erlauben**: Über diese Schaltfläche erlauben Sie der jeweiligen Anwendung nur ein einziges Mal Zugriff aufs Netzwerk. Beim nächsten Versuch eines Netzwerkzugriffs durch dieses Programm fragt die Firewall erneut nach.
- **Immer verweigern**: Über diese Schaltfläche erstellen Sie für die oben aufgeführte Anwendung (z.B. ***dialer.exe*** oder ***spam.exe*** oder ***trojan.exe***) eine Regel, die in dem genannten Netzwerk der Anwendung einen dauerhaften Zugriff aufs Netzwerk bzw. Internet verweigert. Diese Regel finden Sie dann auch als auf Nachfrage erzeugte Regel im Bereich **Regelsätze**.
- **Temporär verweigern**: Über diese Schaltfläche verbieten Sie der jeweiligen Anwendung nur ein einziges Mal den Zugriff aufs Netzwerk. Beim nächsten Versuch eines Netzwerkzugriffs durch dieses Programm fragt die Firewall erneut nach.

Des Weiteren erhalten Sie Informationen zu ***Protokoll***, ***Port*** und ***IP-Adresse*** mit der die jeweilige Anwendung interagieren möchte.

Protokoll

Im Protokoll-Bereich werden alle von der Firewall erlaubten und blockierten Verbindungen mit Netzwerk und Internet protokolliert. Sie können diese Liste durch Anklicken der jeweiligen Spaltenüberschriften beliebig sortieren und mit Anklicken der **Details**-Schaltfläche zu einzelnen Verbindungen weitergehende Informationen erhalten.

Optionen - Firewall

In der oberen Menüleiste der Programmoberfläche finden Sie durch Anklicken der Schaltfläche **Optionen** übergreifende Funktionen und Einstellungsmöglichkeiten.

Automatik

Der Vorteil bei der Nutzung der vordefinierten **Sicherheitsstufen** liegt darin, ohne administrativen Aufwand und Fachkenntnisse im Bereich der Netzwerksicherheit die Firewall trotzdem auf individuelle Bedürfnisse anpassen zu können. Stellen Sie einfach mit dem Schieberegler die Sicherheitsstufe ein, die Sie benötigen. Folgende Sicherheitsstufen stehen dabei zur Auswahl:

- **Höchste Sicherheit:** Die Firewall-Regeln werden mit sehr feinkörnigen Richtlinien erstellt. Dazu sollten Sie sich mit netzwerkspezifischen Fachbegriffen auskennen (**TCP**, **UDP**, **Ports** etc.). Die Firewall bemerkt kleinste Ungereimtheiten und wird während der Lernphase sehr häufig nachfragen.
- **Hohe Sicherheit:** Die Firewall-Regeln werden mit sehr feinkörnigen Richtlinien erstellt. Dazu sollten Sie sich mit netzwerkspezifischen Fachbegriffen auskennen (TCP, UDP, Ports etc.). Die Firewall wird während der Lernphase unter Umständen häufig nachfragen.
- **Normale Sicherheit:** Die Firewall-Regeln werden nur auf Anwendungsebene erstellt. Assistenten halten netzwerkspezifische Details von Ihnen fern. Sie werden während der Lernphase möglichst wenig gefragt.

- **Niedrige Sicherheit:** Die Firewall-Regeln werden nur auf Anwendungsebene erstellt. Assistenten halten netzwerkspezifische Details von Ihnen fern und Sie werden während der Lernphase selten gefragt. Höchst sicherer Schutz vor ankommenden Verbindungsanforderungen besteht auch in dieser Sicherheitsstufe.
- **Firewall deaktiviert:** Sie können die Firewall bei Bedarf auch abschalten. Ihr Computer ist dann weiterhin mit dem Internet und anderen Netzwerken verbunden, wird von der Firewall aber nicht mehr vor Angriffen oder Spionage-Attacken geschützt.

? Wenn Sie die Firewall spezifischer einstellen möchten, setzen Sie bitte das Häkchen bei **Benutzerdefinierte Einstellung**. Beachten Sie aber, dass für diese Einstellungen zumindest ein Grundwissen zum Thema Netzwerksicherheit nötig ist.

Nachfrage

Hier legen Sie fest, wann, wie und ob die Firewall beim Anwender nachfragen soll, sobald Programme einen Verbindungsaufbau mit dem Internet oder Netzwerk anfragen.

- **Regel erstellen:** Wenn die Firewall eine Verbindungsaufnahme mit dem Netzwerk feststellt, erscheint eine Infobox, in der Sie festlegen, wie mit der jeweiligen Anwendung weiter zu verfahren ist. Hier können Sie festlegen, was genau Sie mit dem Erlauben oder Verbießen eines Netzwerkzugriffs bestimmen möchten:

pro Protokoll/Port/Anwendung. Pro Anwendung, falls min. ____
Nachfragen anstehen: Es gibt Anwendungen (z.B. **Microsoft Outlook**), die bei einer Netzwerkanfrage gleich mehrere **Ports** anfragen bzw. gleichzeitig unterschiedliche **Protokolle** nutzen. Da dieses z.B. in der Einstellung pro Protokoll/Port/Anwendung mehrere Abfragen über Info-Boxen mit sich brächte, kann hier auch festgelegt werden, dass Anwendungen eine generelle Freigabe bzw. Absage für die Netzwerknutzung erhalten, sobald Ihnen die Verbindung vom Anwender erlaubt oder untersagt wird.

pro Anwendung: Hier wird der Netzwerkzugriff für die aktuell angezeigte Anwendung generell auf jedem Port und mit jedem Übertragungsprotokoll (z.B. **TCP** oder **UDP**) erlaubt oder verweigert.

pro Protokoll/Port/Anwendung: Die Anwendung, die einen Netzwerkzugriff erfragt, erhält die Erlaubnis nur mit dem erfragten Übertragungsprotokoll und ausschließlich mit dem angefragten Port online zu gehen. Sollte dieselbe Anwendung einen weiteren Netzwerkzugriff auf einem anderen Port oder mit einem anderen Protokoll erfragen, erscheint die Info-Box erneut und es kann eine weitere Regel diesbezüglich erstellt werden.

- **Cache:** Sie können erneut wiederkehrende Verbindungsanfragen einer Anwendung bündeln. Auf diese Weise erscheint bei Verbindungsversuchen, die sie noch nicht über eine Regel spezifiziert haben, nicht ständig eine Infobox, sondern z.B. nur in 20-Sekunden-Abständen oder einem anderen von Ihnen definierbaren Zeitraum.
- **Unbekannte Server Anwendungen:** Anwendungen, die noch nicht über eine Regel in der Firewall verwaltet werden, können unterschiedlich behandelt werden. Der Zeitpunkt der Nachfrage steht dabei in einem gewissen Ermessensspielraum. Wenn die **Serveranwendung** auf Empfang geht, heißt das, dass sie quasi auf Standby eine Verbindungsanforderung erwartet. Bei der Einstellung **Verbindungsanforderung** erfolgt eben diese Verbindungsanforderung.

? Generell sollten Sie das Häkchen bei **Beim Programmstart auf unbekannte Serveranwendungen prüfen** gesetzt lassen, da sonst z.B. Trojaner, die vor dem Starten der Firewall auf dem Rechner waren, weiterhin aktiv bleiben können, ohne entdeckt zu werden.

- **Ungeschützte Netzwerke:** Natürlich kann eine Firewall nur dann problemlos funktionieren, wenn alle Netzwerke, auf die der zu schützende Rechner zugreift, von ihr auch erkannt und überwacht werden. Sie sollten deshalb die Häkchen bei **Neue Netzwerke sofort melden, falls ungeschützt** und **Beim Programmstart auf ungeschützte Netzwerke prüfen** gesetzt lassen.

Angriffe

Generell sollten Sie die Häkchen für das Erkennen der unterschiedlichsten Hacker-Angriffe gesetzt lassen. Der geringe Performance-Vorteil, der sich dadurch ergibt, dass die Firewall diese Möglichkeiten der Einflussnahme nicht überprüft, steht in keinem Verhältnis zum Schaden, der durch einen geglückten Angriff entstehen kann. Folgende Angriffsarten werden von der Firewall erkannt:

- **Port Scans:** Dabei werden die offenen **TCP**- und **UDP**-Ports auf einem angegriffenen Computer ermittelt. Ein solcher Angriff dient der Suche nach Schwachstellen im Computersystem und geht meist gefährlicheren Angriffen voraus.
- **Ping of Death:** Bei diesem Angriff wird ein **ICMP**-Paket gesendet, dessen Größe den zulässigen Wert von 64 KB überschreitet. Der Angriff kann zum Absturz bestimmter Betriebssysteme führen.
- **Land:** Bei diesem Angriff wird an einen offenen **Port** des angegriffenen Computers eine Anfrage auf Verbindungsherstellung mit sich selbst gesendet. Dies führt zu einer Endlosschleife im angegriffenen Computer, was eine stark erhöhte Prozessorbeltastung zur Folge hat und zum Absturz des Betriebssystems führen kann.
- **SYN Flood:** Bei diesem Angriff werden große Mengen falscher Verbindungsanfragen an den angegriffenen Computer gesendet. Das System reserviert für jede dieser Verbindungen bestimmte Ressourcen, wodurch es seine gesamten Ressourcen verbraucht und nicht auf Verbindungsanfragen anderer Quellen reagiert.
- **UDP Flood:** Bei diesem Angriff wird ein UDP-Paket gesendet, das auf Grund seiner Struktur endlos zwischen dem angegriffenen Computer und einer dem angegriffenen Computer frei zugänglichen Adresse hin- und hergeschickt wird. Dies führt auf beiden Computern zum Verlust von Ressourcen und erhöht die Belastung des Verbindungskanals.
- **ICMP Flood:** Bei diesem Angriff werden große Mengen von ICMP-Paketen an den angegriffenen Computer gesendet. Dies führt zu einer stark erhöhten Prozessorbeltastung, da der Computer auf jedes Paket reagiert.
- **Helkern:** Bei diesem Angriff werden spezielle UDP-Pakete mit ausführbarem schädlichem Code an den angegriffenen Computer gesendet. Der Angriff führt zur Verlangsamung der Internetfunktionen.

- **SMB Die:** Bei diesem Angriff wird versucht, eine Verbindung nach SMB-Protokoll aufzubauen; bei erfolgreicher Verbindung wird an den angegriffenen Computer ein spezielles Paket gesendet, das versucht, den Puffer zu überfüllen. Als Folge wird der Computer neu gestartet.
- **Lovesan:** Bei einem Angriff durch Lovesan wird versucht, auf Ihrem Computer Sicherheitslücken im Service **DCOM RPC** der Betriebssysteme Windows NT 4.0/NT 4.0 Terminal Services Edition/2000/XP/Server(tm) 2003 zu ermitteln. Sind solche Schwachstellen auf dem Computer vorhanden, dann wird ein Programm mit schädlichen Funktionen gesendet, das es erlaubt, auf Ihrem Computer beliebige Manipulationen vorzunehmen.

? Wenn Sie die Angaben in der Spalte **Modus** anklicken, können Sie festlegen, ob Hacker-Angriffe per Dialogbox sofort gemeldet oder nur protokolliert werden sollen.

Sonstiges

Hier stehen Ihnen weitere Einstellungsmöglichkeiten zur Verfügung.

- **Referenzprüfung für Anwendungen:** Bei der Referenzprüfung wird für **Anwendungen**, denen von der Firewall schon der Zugriff aufs Netzwerk erlaubt wurde, eine Prüfsumme auf Basis der Dateigröße und anderer Kriterien ermittelt. Wenn diese Prüfsumme des Programms plötzlich abweicht, kann es daran liegen, dass das Programm durch ein Schadprogramm verändert wurde. In diesem Fall schlägt die Firewall Alarm. Die **Referenzprüfung für Anwendungen** sollte in der Regel eingeschaltet bleiben. Die **Referenzprüfung für geladene Module** beobachtet auf gleiche Weise die **Module**, die die Anwendungen verwenden (z.B. **DLLs**). Da diese sich häufig ändern oder auch neue Module nachgeladen werden, kann eine konsequente Prüfung auf modifizierte und unbekannte Referenzen bei Modulen zu einem erheblichen Administrationsaufwand bei der Nutzung der Firewall führen. Jedes geänderte Modul würde dann nämlich eine Sicherheitsabfrage der Firewall nach sich ziehen. Die Modulprüfung sollte deshalb nur bei sehr hohen Ansprüchen an die Sicherheit in dieser Weise genutzt werden.

- **Modifizierte Referenzen:** Modifizierte Referenzen können in der Referenzprüfung (z.B. bei einem **Windows-Update**) kann weitestgehend automatisiert werden, wenn die Module über ein **G Data AntiVirus Modul** geprüft und für unbedenklich gefunden wurden. Sollte das AntiVirus Modul nicht installiert sein, kann die Bestätigung für modifizierte Referenzen auch manuell durch den Anwender erfolgen.
- **Regelsätze:** Hier können Sie festlegen, ob Sie das Erstellen neuer Regeln generell über den **Regel Assistenten** oder mit dem **Profi-Dialog** durchführen möchten. Für Anwender, die sich in der Materie der Netzwerksicherheit nicht auskennen, empfehlen wir den **Regel Assistenten**.

? Natürlich kann man vom **Regel Assistenten** auch jederzeit direkt zum **Profi-Dialog** wechseln und auch ein Wechsel in die andere Richtung ist jederzeit möglich. Wählen Sie dazu beim **Regel Assistenten** einfach unter **Was möchten Sie tun?** den Eintrag **In den erweiterten Bearbeitungsmodus wechseln** aus oder klicken Sie im **Profi-Dialog** auf die **Assistent**-Schaltfläche.

- **Verbindungs-Protokoll:** Hier können Sie festlegen, wie lange die Firewall Verbindungsdaten aufbewahren soll. Sie können die Daten von einer Stunde bis zu 56 Stunden nachhalten und im Programmbereich **Protokoll** einsehen.
- **Autopilot:** Gerade bei **Computerspielen** (und anderen **Full-Screen Anwendungen**) kann es störend sein, wenn die Firewall mit Nachfragefenstern den Spielfluss oder einfach nur die Darstellung stört. Um einen ungestörten Spielgenuss ohne Sicherheitseinbußen zu gewährleisten, ist der Autopilot eine sinnvolle Einstellung, da er Nachfragen der Firewall unterdrückt. Sollten Sie den Autopiloten nicht als Standardeinstellung verwenden, können Sie über die Funktion **Autopilot automatisch anbieten** dafür sorgen, dass er immer nur dann automatisch aktiviert wird, wenn Sie ein Programm nutzen, welches im **Vollbildmodus** läuft.

Anhang

Problemlösungen (FAQ)

In diesem Bereich finden Sie Antworten zu Fragestellungen, die bei der Arbeit mit der *G Data Software* möglicherweise auftreten könnten.

Ich möchte die Installation der Clients zentral vom Server aus über den Administrator durchführen

Am komfortabelsten ist die ***Installation über den Administrator***. Dazu müssen die Clients aber bestimmte Voraussetzungen erfüllen. Die ***Remote-Installation*** kann in zwei Varianten durchgeführt werden. Wenn der Client die Voraussetzungen dafür erfüllt, werden die Dateien direkt kopiert und die Einträge in der Registry vorgenommen. Kann der Server nur auf die Festplatte aber nicht auf die Registry zugreifen oder sind andere Systemvoraussetzungen nicht erfüllt, wird das komplette Setup-Programm auf den Client kopiert und beim nächsten Hochfahren des Computers automatisch gestartet. Zur Installation begeben Sie sich einfach in der Menüleiste des Administrators und rufen dort die Funktion **Clients > G Data Client installieren** auf. Es erscheint ein Eingabefenster, in dem Sie Benutzername, Passwort und Domäne des Managementsservers angeben. Nach Eingabe dieser Daten erscheint ein Fenster mit allen verfügbaren Netzwerkrechnern. Aktivierte Clients sind dabei mit einem Symbol gekennzeichnet, deaktivierte Clients werden durch ein schattiertes Symbol dargestellt. Wählen Sie zur Installation einen Netzwerkrechner aus und klicken dann auf die Schaltfläche **Installieren**. Auf diese Weise wird der *G Data Client* auf diesem Rechner installiert. Sollte Ihr System nicht die Voraussetzungen für eine Remote-Installation der *G Data Client-Software* erfüllen, haben Sie natürlich auch die Möglichkeit, die Clients manuell oder halbautomatisch mit der *G Data Client-Software* zu versehen.

Ich möchte den Administrator auf einem Client-Rechner installieren

Sie können den **Administrator** natürlich auch von jedem anderen Computer im Netzwerk starten.

? Für einen reibungslosen Ablauf der *G Data Software* ist es nicht zwingend nötig, den Administrator auf den Clients zu installieren. Eine Installation des Administrators auf einem Client-Rechner empfiehlt sich eigentlich nur im Bedarfsfall für eine Problemlösung *vor Ort*.

Wir empfehlen dazu, das Verzeichnis **Admin** freizugeben und dann die Datei **Admin.exe** von dem anderen Computer aufzurufen. Natürlich können Sie die Datei auch auf andere Computer kopieren und von dort starten. Die Freigabe hat den Vorteil, dass Sie immer die neueste Version starten, da die Datei durch ein Internet Update aktualisiert werden kann. Wahlweise können Sie deshalb auch die *G Data*-CD-ROM in das CD-ROM-Laufwerk des Client-Rechners einlegen, die Schaltfläche **Installieren** drücken und anschließend die Komponente *G Data Administrator* durch einen Klick auf die entsprechende Schaltfläche auswählen. Im folgenden Begrüßungsbildschirm werden Sie darüber informiert, dass Sie im Begriff sind den Administrator auf Ihrem System zu installieren. Bitte schließen Sie spätestens jetzt alle offenen Anwendungen in Ihrem Windows-System, da diese sonst zu Problemen bei der Installation führen könnten. Klicken Sie auf **Weiter** um mit der Installation fortzufahren. Der nächste Bildschirm ermöglicht Ihnen die Auswahl des Ortes, an dem die Daten des Administrators abgespeichert werden sollen. Standardmäßig wird der Managementserver unter **C: > Programme > G Data > G Data Administrator** abgelegt. Sollten Sie einen anderen Speicherort auswählen wollen, haben Sie die Möglichkeit über die Schaltfläche **Durchsuchen** eine Verzeichnisansicht zu öffnen, in der Sie ein anderes Verzeichnis auswählen oder auch neu anlegen können. Mit **Weiter** gelangen Sie zum nächsten Installationsschritt. Nun haben Sie die Möglichkeit, eine Programmgruppe auszuwählen. Wenn Sie auf **Weiter** klicken, finden Sie das Programm standardmäßig in der Programmgruppe **G Data Administrator** in der Programmauswahl des Windows-Startmenüs. Die Installation wird mit einem Abschlussbildschirm beendet. Klicken Sie auf **Beenden**. Der Administrator steht Ihnen nun zur Verfügung. Sie können das Administrator-Tool zur Steuerung des Managementsservers mit einem Klick auf den Eintrag **G Data Administrator** in der Programmgruppe **Start > Programme > G Data Administrator** des Startmenüs aufrufen.

Ich möchte die Clients mit Hilfe der G Data-CD-ROM mit der Client-Software ausstatten

Sie können die Client-Software auch direkt auf den einzelnen Clients von der mitgelieferten CD installieren. Legen Sie dazu die **CD-ROM** in das CD-ROM-Laufwerk des Client-Rechners, wählen dann die Komponente **G Data Client** mit einem Klick auf die nebenstehende Schaltfläche aus. Bei der Installation werden Sie dann nach dem Namen des Computers gefragt, auf dem der Managementserver installiert ist. Geben Sie den entsprechenden Namen (z. B. **avk_server**) ein. Mit Betätigung der **Weiter**-Schaltfläche schließen Sie die Installation ab. Sollte das Setup-Programm auf dem Abschlussbildschirm einen Neustart des Computers vorschlagen, führen Sie diesen bitte durch, da der Client in diesem Fall erst nach einem Neustart funktionsfähig ist.

Einige Clients melden "Die Virendatenbank ist beschädigt.". Was ist zu tun?

Um einen optimalen Virenschutz zu gewährleisten wird die Virendatenbank regelmäßig auf Ihre Unversehrtheit geprüft. Bei einem Fehler wird der Bericht **Die Virendatenbank ist beschädigt** eingefügt. Löschen Sie den Bericht und laden Sie das aktuelle Update der Virendatenbank von unserem Server. Führen Sie anschließend auf den betroffenen Clients eine Aktualisierung der Virendatenbank durch. Kontaktieren Sie bitte unsere telefonische Hotline, wenn der Fehlerbericht erneut eingefügt wird.

Die Clients sollen nicht über ihre Namen sondern über ihre IP-Adresse angesprochen werden

Installation des Managementserver: Bei der Installation wird nach dem Servernamen gefragt. Der Name muss durch die **IP-Adresse** ersetzt werden. Sie können den Servernamen auch nachträglich durch die IP-Adresse ersetzen, wenn der Managementserver bereits installiert ist. Passen Sie dazu den Registry-Eintrag

HKEY_LOCAL_MACHINE\Software\G Data\G Data ManagementServer\ComputerName und die Datei **\Programme\G Data\G Data**

ManagementServer\AvkClientSetup\RegServer.txt an. **Aktivierung der Clients im Administrator:** Damit die Verbindung vom Server zu den Clients auch über die IP-Adresse hergestellt werden kann, müssen die Clients im Administrator mit Ihrer IP-Adresse aktiviert werden. Das geht entweder von Hand (**Clients/Client aktivieren (Dialog)**) oder durch Absuchen eines IP-Adressbereiches (**Client/Computer suchen**). **G Data Client-Setup von der CD:** Wenn die Clients direkt von der **CD** installiert werden, fragt das Installationsprogramm sowohl nach dem Servernamen als auch nach dem Computernamen. Geben Sie hier jeweils die IP-Adresse ein.

Mein Postfach wurde in die Quarantäne geschoben

Das kann passieren, wenn sich in dem Postfach eine infizierte Mail befindet. **Zurückbewegen der Datei:** Schließen Sie das Mailprogramm auf dem betroffenen Client und löschen Sie eine evt. neu angelegte Archivdatei. Öffnen Sie anschließend mit dem Administrator den zugehörigen Bericht und klicken Sie auf **Datei zurückbewegen**. Kontaktieren Sie bitte unsere telefonische Hotline, wenn das Zurückbewegen fehlschlägt.

Wie kann ich überprüfen, ob die Clients eine Verbindung zum ManagementServer haben?

Die Spalte **Letzter Zugriff** im Aufgabenbereich **Clients** enthält den Zeitpunkt, an dem sich der Client zum letzten Mal beim Managementserver gemeldet hat. Normalerweise melden sich die Clients alle paar Minuten beim Managementserver (wenn gerade keine Scanjobs ausgeführt werden). Folgende mögliche Ursachen können für eine fehlgeschlagene Verbindung ursächlich sein:

- Der Client ist ausgeschaltet oder vom Netzwerk getrennt.
- Es kann keine TCP/IP-Verbindung zwischen dem Client und dem Managementserver aufgebaut werden. Prüfen Sie die Netzwerkeinstellungen.
- Der Client kann die IP-Adresse des Servers nicht ermitteln, d.h. die Namensauflösung funktioniert nicht. Die Verbindung kann mit dem Befehl **ping** überprüft werden. Geben Sie dazu in der Eingabeaufforderung den Befehl **ping <Servername>** ein, wobei **<Servername>** der Name des Computers im Netzwerk ist, auf dem der Managementserver installiert ist.

Einige Clients melden "Programmdateien wurden verändert oder sind beschädigt". Was ist zu tun?

Um einen optimalen Virenschutz zu gewährleisten werden die Programmdateien regelmäßig auf Ihre Unversehrtheit geprüft. Bei einem Fehler wird der Bericht **Programmdateien wurden verändert oder sind beschädigt** eingefügt. Löschen Sie den Bericht und laden Sie das aktuelle Update der Programmdateien (*G Data Client*) von unserem Server. Führen Sie anschließend auf den betroffenen Clients eine Aktualisierung der Programmdateien durch. Kontaktieren Sie bitte unsere telefonische Hotline, wenn der Fehlerbericht erneut eingefügt wird.

Nach der Installation des Clients laufen einige Anwendungen erheblich langsamer als vorher

Der Wächter überwacht im Hintergrund alle Dateizugriffe und prüft die geöffneten und gespeicherten Dateien auf Viren. Dieses führt normalerweise zu einer kaum spürbaren **Verzögerung**. Falls eine Anwendung sehr viele Dateien oder einige Dateien sehr oft öffnet, kann eine erhebliche Verzögerung auftreten. Um dieses Problem zu umgehen, deaktivieren Sie den Wächter zunächst temporär, um herauszufinden, ob er wirklich die Verzögerungen hervorruft. Wenn der betroffene Rechner auf Dateien eines Servers zugreift, müssen Sie natürlich auch den Wächter auf dem Server deaktivieren. Falls der Wächter die Ursache ist, kann das Problem i.d.R. durch die Definition einer **Ausnahme** (= Dateien, die nicht geprüft werden sollen) behoben werden. Dazu müssen zunächst die Dateien ermittelt werden, auf die häufig zugegriffen wird. Mit einem Programm wie z.B. **MonActivity** können Sie diese Daten ermitteln. Wenden Sie sich hierzu ggf. an unser **ServiceCenter**. Bekannte Verzögerungen:

- Bei der Verwendung einiger **HP-Drucker** mit **Microsoft Office** sollten die Dateien **HP*.INI** als Ausnahme definiert werden.
- Bei der Verwendung der Mailsoftware **Eudora** sollten die Dateien **EUDORA.INI** und **DEUDORA.INI** als Ausnahmen definiert werden.

? Selbstverständlich können Sie auch die Performance dadurch steigern, in dem Sie nicht beide Engines zur Virenüberprüfung verwenden, sondern nur eine Engine.

Installation der Client-Software auf Linux-Rechnern

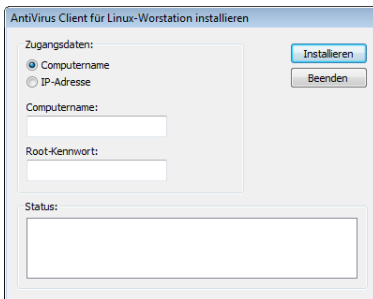
Das Produkt ermöglicht es, den **G Data Virenschutz** auf **Linux-Workstations** verschiedener Distributionen einzusetzen. Der **Linux-Client** kann dabei (ebenso wie die **Windows-Clients**) in die Infrastruktur des **G Data ManagementServers** eingebunden und zentral über die **G Data Administratorsoftware** gesteuert und mit Signaturupdates versorgt werden. Analog zu den Windows-Clients wird auch bei Linux-Clients ein Dateisystemwächter mit einer grafischen Benutzeroberfläche eingerichtet, die sich in der Funktionalität an der Windows-Version orientiert. Für Linux-Rechner, die als **Fileserver** arbeiten und verschiedenen Clients Windows-Freigaben (über das **SMB-Protokoll**) zur Verfügung stellen, kann hierzu ein Modul installiert werden, das den Zugriff auf die Freigaben kontrolliert und bei jedem Zugriff einen Scan auf die Datei ausführt, so dass keine Malware vom Samba-Server auf die Windows-Clients (und umgekehrt) gelangen kann.

- ?** Für den **Workstation-Client** ist eine Kernel-Version größer gleich 2.6.25 erforderlich, dies ist z.B. bei Ubuntu 8.10, Debian 5.0, Suse Linux Enterprise Desktop 11 und anderen aktuellen Distributionen der Fall. Bei anderen Distributionen ist im Einzelfall eine Anpassung erforderlich. Der **Fileserver-Client** lässt sich auf allen gängigen Distributionen verwenden.

Um die Software auf dem Linux-Client zu installieren, gehen Sie bitte folgendermaßen vor:

1 Remote-Installation der Client-Software übers Netzwerk

Wählen Sie im Aufgabenbereich **Clients** im Menü **Client-Einstellungen** den Befehl **G Data Client für Linux installieren** aus. Nun erscheint ein Dialogfenster über das Sie den Client definieren können, auf den die Client-Software kopiert werden soll. Der Rechner muss dazu im Netzwerk bekannt sein.



- 2 Verwenden Sie die Auswahl **Computername**, wenn auf dem Client-Rechner ein **Samba-Dienst** installiert ist oder wenn der Rechner im **Nameserver** des Netzwerkes registriert ist. Sollte der Name des Rechners nicht bekannt sein, verwenden Sie bitte die **IP-Adresse** des Rechners.
- 3 Geben Sie nun das **Root-Kennwort** des Rechners ein. Für eine Remote-Installation muss ein Root-Kennwort vergeben sein. Standardmäßig ist dies unter einigen Distributionen (z.B.) Ubuntu nicht der Fall.
- 4 Drücken Sie nun auf die **Installieren**-Schaltfläche. Im Bereich **Status** sehen Sie, ob die Installation der Client-Software erfolgreich war.

? Manuelle Installation der Client-Software

In einem speziellen Verzeichnis auf der Programm-CD finden Sie die folgenden Dateien

- **installersmb.bin** = Installer für Samba Fileserver
- **installerws.bin** = Installer für Workstation

Sie können diese Dateien auf den Client-Rechner kopieren und zur Installation der Client-Software die entsprechende Datei starten.

Zusätzlich finden Sie hier noch eine Datei mit den **Virensignaturen**. Da die Software nach der Installation aber automatisch die neuesten Virensignaturen vom Server bezieht, ist die Installation dieser Datei fakultativ.

- **signatures.tar** = Archiv mit Virensignaturen

Linux-Fileserver Clients: Es wird keine Verbindung zum ManagementServer aufgebaut / Signaturen werden nicht aktualisiert

- 1 Prüfen Sie ob die beiden Prozesse des *G Data Clients* laufen:
Geben Sie auf der Kommandozeile

```
linux:~# ps ax|grep av
```

ein. Sie sollte die Ausgaben

```
... Ssl 0:07 /usr/sbin/avkserver --daemon
```

```
... Ssl 0:05 /usr/sbin/avguard --daemon
```

erhalten. Die können die Prozessen unabhängig von der eingesetzten Distribution mit

```
linux:~# /etc/init.d/avkserver start
```

```
linux:~# /etc/init.d/avclient start
```

starten und mit

```
linux:~# /etc/init.d/avkserver stop
```

```
linux:~# /etc/init.d/avclient stop
```

anhalten. Hierzu müssen Sie als Administrator (=“root“) auf dem Linux-Rechner eingeloggt sein.

- 2** Sehen Sie sich die Log-Dateien an: Unter */var/log/avk* befinden sich die Log-Dateien *avk.log* und *remote.log*. In der Datei *avk.log* werden die Scan-Ergebnisse des Scanners *avkserver* protokolliert, in der Datei *remote.log* befinden sich die Ausgaben des Prozesses *avclient*, der die Verbindung zum *G Data ManagementServer* herstellt. Schauen Sie sich die Dateien an und suchen Sie nach Fehlermeldungen. Wenn Sie mehr Meldungen sehen möchten, können Sie in den Konfigurationsdateien */etc/gdata/gdav.ini* und *etc/gdata/avclient.cfg* die Einträge für *LogLevel* auf den Wert *7* setzen.

Vorsicht: Hohe LogLevel erzeugen viele Meldungen und lassen die Log-Dateien schnell anwachsen. Setzen Sie die LogLevel im Normalbetrieb immer auf niedrige Werte!

- 3** Testen Sie den Scanner: Mit dem Kommandozeilen-Tool *avkclient* können sie die Funktion des Scanservers *avkserver* testen. Folgende Kommando lassen sich ausführen:

linux:~\$ avkclient avkversion - gibt Version und Updatedatum der Virensignaturen aus

linux:~\$ avkclient version - gibt Version in Kurzform aus

linux:~\$ avkclient scan:<file> - scannt die Datei *<file>* und gibt das Ergebnis aus

- 4** Sehen Sie sich die Konfigurationsdatei an: Unter *etc/gdata/avclient.cfg* finden Sie die Konfigurationsdatei des Remoteclients *avclient*. Kontrollieren Sie, ob die Adresse des Haupt-Management-Servers (MainMMS) korrekt eingetragen ist. Falls nicht, löschen Sie den falschen Eintrag und melden den Linux-Client über den *G Data Administrator* erneut an oder tragen Sie die Adresse des *G Data ManagementServers* direkt ein.

- 5** Testen Sie Ihre Freigaben: Der Virenschutz für die Samba-Freigaben wird durch den Eintrag

vfs objects = gdvfs

in der Samba-Konfigurationsdatei /etc/samba/smb.conf aktiviert. Steht der Eintrag in der Sektion [global] so ist der Schutz für alle Freigaben aktiviert, steht die Zeile in eine einer anderen Sektion, so gilt der Schutz nur für die entsprechende Freigabe. Sie können die Zeile testweise auskommentieren (eine Raute (#) voranstellen), um zu festzustellen, ob der Zugriff ohne den Virenschutz funktioniert. Falls nicht, suchen Sie bitte zunächst den Fehler in Ihrer Samba-Konfiguration.

6 *Linux Workstation Wächter*

Prüfen Sie ob, der Wächter-Prozess avguard läuft:

ps ax|grep avguard

Der Wächter benötigt die Kernel-Module redirfs und avflt. Sie können mit lsmod prüfen, ob die Module geladen sind: lsmod|grep redirfs und lsmod|grep avflt....

Die Module müssten für den von Ihnen verwendeten Kernel kompiliert sein. Dies erledigt das Dynamic Kernel Module System (DKMS), welches zusammen mit den passenden Kernel-Header-Pakete Ihren Distribution installiert sein muss. Wenn das der Fall ist kompiliert und installiert DKMS die Module automatisch. Sie finden die Logdatei des Wächters unter /var/log/gdata/avguard.log.

Index

A

- Abhängige Berichte ausblenden 65, 70
- Abhängige Berichte löschen 65
- Absender-Adresse 21
- Adaptiv-Modus 97
- Admin 108
- Admin.exe 108
- Administrator 7, 11, 17, 18, 19, 23, 108, 112
- Administratorsoftware 112
- Administrator-Software 11, 13
- Adminstrator 88
- Adware 45, 55
- Aktion, falls keine Regel zutrifft 97
- Aktivieren 20
- aktiviert 29
- aktivierte Clients 29
- Aktivierung der Clients im Administrator 110
- Aktualisieren 25, 29, 31, 33, 37, 43, 67, 73
- Aktualisierung 32, 33
- Alarmmeldungen 35, 37
- Alarm-Meldungen per E-Mail verschicken 35
- Alle Berichte anzeigen 70
- Alle Berichte mit nicht entfernten Viren anzeigen 70
- Alle Firewall-Berichte anzeigen 70
- Alle HTTP-Berichte anzeigen 70
- Alle Jobs anzeigen 49
- Alle Quarantäne-Berichte anzeigen 70
- Alle verfügbaren Prozessoren benutzen 45
- Allgemein 50
- allgemeine Regel für Anwendung erstellen (TCP/UDP alle Ports) 99
- Allgemeines 2
- Analyse-Umfang 41, 48
- Angriffe 104
- Anhang 107
- Anhang/Text löschen 60
- Anmelden 88
- Anmeldung 19
- Ansage 35
- Ansicht 24, 31, 41, 65
- Ansicht aktualisieren 29, 37
- AntiSpam 64
- AntiVirus Client Installationspaket erstellen 31
- Anwender bei Virenfund benachrichtigen 61
- Anwendung auf Viren und Schadfunktionen überprüfen 99
- Anwendungen 105
- Anwendungen zuordnen 98
- Anwendungsdetails 99
- Anwendungs-Radar 90
- Anzeigeoptionen 49, 70
- Archive 45
- Archive prüfen 55
- Archivierte Dateien ausblenden 65, 70
- Archivprüfung 44
- Assistent 105
- Auch in Zukunft den Regel Assistenten starten 95
- Auf Defaulteinstellungen zurücksetzen 71
- Auf Dialer / Spyware / Adware / Riskware prüfen 45, 55
- Auf RootKits prüfen 45
- Auf Viren prüfen (G Data AntiVirus) 82
- Aufbau der Server-Typen 14

- Aufgabenbereich Clients 33
- Aufgabenbereiche 23, 31, 40
- Aufträge 24, 30, 40, 41
- Ausführen 11, 45
- Ausgehende Mails 60
- Ausnahme 112
- Ausnahmen 58
- Ausnahmetatbestände 71
- Ausnahmeverzeichnisse 71
- Ausnahmeverzeichnisse bearbeiten 76
- Ausnahmeverzeichnisse für Scanjobs 54
- Authentisierung 19
- Automatik 101
- automatische Aktualisierung der Virendatenbank 75
- Automatische Installation der Client-Software 22
- Automatische Konfiguration (DHCP) zulassen 92
- automatische Typ-Erkennung 45, 55
- Automatische Updates 32, 33
- Automatisches Bereinigen 36
- Autopilot 77, 90, 105
- Autopilot / Regelsatz 77
- Autopilot automatisch anbieten 105
- Autopilot-Modus 78, 89
- Autopilot-Modus (empfohlen) 90
- Autostart-Funktion Ihres CD-ROM-Laufwerks 11
- avk.log 114
- avk_server 109
- avkclient 114
- AvkClientSetupPck.exe 31
- avkremote 114
- avkremote-Pakets 112
- avkserver 114
- avkvfs-Moduls 112
- avkvfs-Paket 112
- B**
- Beenden 27
- Begrenzung 35
- Begrüßungsbildschirm 13
- Beide Engines - performance-optimiert 45
- Beim Programmstart auf unbekannte Serveranwendungen prüfen 102
- Beim Programmstart auf ungeschützte Netzwerke prüfen 102
- Beim Schreiben prüfen 55
- Beim Systemstart 45
- Benutzerdefinierte Einstellung 101
- Benutzerkonto 32, 33, 51
- Benutzerkonto und Proxy-Einstellungen 34
- Benutzername 2, 19, 34
- Benutzernamen 16
- Benutzerverwaltung 19, 25
- Berechtigungen 25
- Bericht an ausgehende Mails anhängen 60
- Bericht an empfangene, infizierte Mails anhängen 60
- Bericht erzeugen 51, 71
- Berichte 24, 36, 40, 65, 67, 71
- Berichte löschen 68
- Besonderheit auf einem Linux-Fileserver 54
- Besonderheit bei Scanjobs auf einem Linux-Fileserver 48
- BIOS 8
- Boot-CD-Erstellung 11
- BootScan 7, 8, 11, 55
- BootScan mit der Programm-CD 8

BootScan mit G Data Software, die Sie aus dem Internet heruntergeladen haben 8

Bootsektoren 45, 55

Business-Vertrieb 3

C

Cache 102

CentOS 112

Client 11, 30, 31, 51, 59, 75, 81, 82, 85, 107, 109, 111

Client (aktiviert) 39

Client (deaktiviert) 39

Client aktivieren 30, 37

Client aktivieren (Dialog) 30, 37

Client deinstallieren 71, 75

Client für Samba-Fileserver 112

Client Installationspaket erstellen 22

Client installieren 22, 71, 74

Client- und Serversoftware 7

Client/Computer suchen 110

Clientauswahlbereich 23, 39, 40, 49, 54, 71

Client-Einstellungen 24, 71

Client-Funktionen 52

Clients 13, 22, 24, 26, 27, 31, 40, 41, 71, 74, 111

Clients bei Optionsänderungen vom Server benachrichtigen 37

Clients zuordnen 26

Clients/Client aktivieren (Dialog) 110

Client-Setup von der CD 110

Client-Software 7, 11, 33, 71, 74, 81, 107

Client-Software automatisch auf den aktivierten Computern installieren 20

Client-Symbol 82

Computer 20

Computer suchen 30

Computernamen 15, 81, 112

Computerspielen 105

D

Datei 20, 24, 58

Datei aus Quarantäne zurückbewegen 69

Datei in die Quarantäne verschieben 65

Datei in Quarantäne verschieben 45, 55

Datei in Quarantäne verschoben 65

Datei löschen 65, 69

Datei säubern und aus Quarantäne zurückbewegen 69

Datei- und Druckerfreigabe (NetBIOS) erlauben oder verweigern 95

Datei zurückbewegen 110

Datei/Mail 65

Dateitypen 45, 55

Datenbank-Server 15

Datenstand 71

Datenträger 41

Datum/Uhrzeit 65

DCOM RPC 104

deaktivieren 28, 37

deaktivierte Clients 29, 74

Deaktivierte Clients anzeigen 28, 29, 37

Debian 112

Defaulteinstellungen 21, 29, 71

Defaulteinstellungen löschen 29

Der Anwender darf die E-Mail- und Wächteroptionen ändern 52

Der Anwender darf die Firewall ein- und ausschalten 78

Der Anwender darf die Firewall-Optionen ändern 52

Der Anwender darf Offsite-Konfiguration ändern	78	Einen leeren Regelsatz erzeugen	93
Der Anwender darf selbst Signaturupdates laden	52	Einen Main-Server installieren	14
Der Anwender darf selbst Virenprüfungen durchführen	52, 84	Einen Regelsatz erzeugen, der einige sinnvolle Regeln enthält	93
Der Anwender darf Wächteroptionen ändern	82, 84	Einen Secondary-Server installieren	14
Desinfizieren (wenn nicht möglich: Datei löschen)	55	Einen Subnet-Server installieren	14
Details	99, 101	Einer bestimmten Anwendung den Zugriff erlauben oder verweigern	95
DEUDORA.INI	112	Eingehende Mails	60
DFÜ	91	Einige Clients melden "Die Virendatenbank ist beschädigt". Was ist zu tun?	109
DFÜ-Netzwerk	90	Einige Clients melden "Programmdateien wurden verändert oder sind beschädigt". Was ist zu tun?	111
DFÜ-Netzwerke	93	Einmalige Scanjobs	41
DHCP	8, 92	einmaliger Scanjob	41
Dialer	45, 55	Einrichtungsassistent	7, 20, 24
Die Clients sollen nicht über ihre Namen sondern über ihre IP-Adresse angesprochen werden	110	Einstellungen	21, 24, 29, 31, 36, 37, 40, 45, 49, 55, 77, 84
Die Virendatenbank ist beschädigt	109	Einstellungen und Zeitplanung	52, 85
direkte Verbindung mit dem Internet	90, 93	E-Mail	21, 35, 59, 84
DLLs	105	E-Mail Archive	45
DNS	92	E-Mail Archive prüfen	55
Domäne	34, 95	E-Mail-Benachrichtigung	21, 35
Domänen-Dienste erlauben oder verweigern	95	E-Mail-Einstellungen	4, 21, 35
Drucken	25, 27, 68, 74	E-Mails	65
Druckvorlagen	26	E-Mail-Schutz	62
Durchsuchen	108	E-Mail-Sicherheit	52
Dynamic Host Configuration Protocol	92	Emergency-AntiViren Service	4, 13, 21, 35, 45, 65, 68
dynamische IP-Adresse	92	Empfangene Mails auf Viren prüfen	60
E		Empfänger	35
Eigenschaften	43, 44	End-IP-Adresse	30
Einen bestimmten Internet-Dienst (Port) öffnen oder sperren	95	Engine	71
		Engines benutzen	45, 55, 61
		Entfernen	28

Erneut (sofort) ausführen 41
Erster Programmstart
(Einrichtungsassistent) 20, 24
Eudora 112
EUDORA.INI 112
exportieren 25
Extras 62

F

Fedora 112
Fehlalarm 55
Festplatte 58
Fileserver 112
Fileserver-Client 112
Firewall 11, 31, 52, 74, 77, 86, 89, 101
Firewall aktiv, auf diesem Netzwerk 92
Firewall deaktiviert 101
Firewall deinstallieren 77
Firewall eingeschaltet 78
Firewall installieren 77
Firewall-Alarm 93, 99
Firewall-Berichte 70
Fragezeichen-Symbol 58
fremden Netzwerken 93
FTP 97
Full-Screen Anwendungen 105

G

G DATA AntiVirus 107
G Data AntiVirus Client für Linux
installieren 112
G Data Subnet-Server zuordnen 71
G Data UpdateServer 32
G Data Virenschutz 112
G Data AntiVirus Client für Linux
installieren 71
Gemeinsame Nutzung der
Internet-Verbindung 92

Gemeinsame Nutzung der
Internet-Verbindung erlauben 95
Gesamtes Netzwerk 29
Gesperrte Anwendungen melden 78
Größenbegrenzung für Downloads 63
Gruppe 28, 39, 41, 54
Gruppe bearbeiten 28
Gruppen 37, 54
Gruppenjobs ausführlich anzeigen 41,
49

H

Hauptserver 14
Heim- und Firmennetzwerke 93
Helkern 104
Heuristik 45, 55
Hilfe 2, 37
Hinweisfenster auf dem Client 51
Hinweisfenster auf dem Client öffnen
71
Hinzufügen 28
Hitliste infizierte Clients 80
Hitliste Viren 80
Höchste Sicherheit 101
Hohe Sicherheit 101
Host-IDs 30
Hotline 2
HP*.INI 112
HP-Drucker 112
HP-Druckern 54
HTTP-Berichte 70
HTTP-Webinhalte 63

I

Ich akzeptiere die Bedingungen der
Lizenzvereinbarung 13
Ich möchte den Administrator auf einem
Client-Rechner installieren 108

Ich möchte die Clients mit Hilfe der CD-ROM mit der Client-Software ausstatten 109

Ich möchte die Installation der Clients zentral vom Server aus über den Administrator durchführen 107

ICMP 104

ICMP Flood 104

ICS 92, 95

Im Fall einer Infektion 45, 60

IMAP 59, 62

IM-Inhalte verarbeiten 63

Immer erlauben 99

Immer verweigern 99

In den erweiterten Bearbeitungsmodus (Profi-Dialog) wechseln 95

In den erweiterten Bearbeitungsmodus wechseln 105

In Quarantäne verschieben 68

Infizierte Archive 45, 55

Infizierte Datei löschen 55

Info 86

Inhalt des Quarantäne-Ordners anzeigen 70

Installation 11

Installation der Clients 81

Installation des Administrators 18

Installation des Managementservers 13, 110

Installation des WebAdministrators 87

Installation über den Administrator 107

Installation von Client für Samba-Fileserver 81, 112

Installationsabschluss 17

Installationsbeginn 16

Installieren 11, 13, 16, 20, 74, 81, 107, 108, 112

Instant Messaging 63

Instant Messaging (Integration in der IM-Anwendung) 63

Integrierte Authentisierung 19

integrierte Datenbank 15

integriertes Login 25

Internet 93

Internet Explorer 34

Internet Update 2, 8, 16, 21, 31, 33, 37, 85

Internet-Dienst zuordnen 98

Internetinhalte (HTTP) 63

Internetinhalte (HTTP) verarbeiten 63

Internetverbindung 16

Internetverbindungsfreigabe 92, 95

IP-Adresse 92, 99, 110, 112

IP-Adresse des Servers 81

IP-Adressen 30

IP-Adressraum 98

J

Job 44

Jobs 41

K

Kennwort 19, 25, 34

Kommandozeile 112

Kommentar 51

Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration 87

Komponenten 11

Konfiguration Datenbanktyp 17

Konfigurieren 89

Kontentyp 25

Kontextmenü 51, 81, 82

L

LAN 91

Land 104

LAN-Partys 93
LAN-Verbindung 90
Laufwerk 58
Lernfunktion 97
Lesen/Schreiben 25
letzte Ausführung 41
Letzter Zugrif 111
Letzter Zugriff 71
Linux Workstation Wächter 114
Linux-Client 112
Linux-Clients 23, 74
Linux-Rechner 8
Linux-Rechnern 112
Linux-Workstations 112
Lizenzvereinbarung 4, 13
LogLevel 114
Lokale Quarantäne anzeigen 52
Löschen 28, 73
Lovesan 104

M

Mail auf Viren überprüfen 62
Mail PlugIn 65
Mails vor dem Senden prüfen 60
Mail-Server 21
Main-MMS 14
Mainserver 26
Main-Server 14
ManagementServer 2, 7, 8, 11, 13, 14, 18, 33, 35, 74, 112
ManagementServer auch als Subnet-Server 14
ManagementServers 13, 112
manuelle Regelerstellung 90, 99
Master Boot Records 45
Medium-Wechsel 55
Mehrfach- und Netzwerklizenzen 2

Mein Postfach wurde in die Quarantäne geschoben 110
Melder 65
Mengenbegrenzung 21
Menüleiste 23, 24, 37
Microsoft .NET Framework-Komponenten 87
Microsoft Messenger (ab Version 4.7) 63
Microsoft Office 54, 112
Microsoft Outlook 59, 102
Microsoft Outlook durch ein integriertes Plugin schützen 62
Microsoft SQL-Express 15
Modifizierte Referenzen 105
Module 105
Modus 90, 104
MonActivity 112
Monatliche Prüfung 44

N

Nach der Installation des Clients laufen einige Anwendungen erheblich langsamer als vorher 112
Nachfrage 102
Name 15, 41
Namen Ihres Computers 15
Nameserver 112
NetBIOS 95
Netzwerk 90
Netzwerk bearbeiten 92
Netzwerke 90, 91
Netzwerk-Info 92
Netzwerksymbol 39
Netzwerkzugriffe prüfen 55
Neue Berichte sofort an den Hauptserver übertragen 37
Neue Gruppe 28, 37

Neue Netzwerke sofort melden, falls ungeschützt 102

Neuer Regelsatz 93

Neuer Scanjob (einmalig) 43

Neuer Scanjob (periodisch) 43, 44

Neustart nach Aktualisierung

Programmdateien 71

Neustart nach der Aktualisierung 51

Neustart ohne Abfrage 51

Neustart ohne Abfrage durchführen 71

Nicht auswählbare Geräte 39

nicht vertrauenswürdige Netzwerke
90, 93

Niedrige Sicherheit 101

Normale Sicherheit 101

Notebooks 32

Nur einmalige Scanjobs anzeigen 49

Nur erledigte Scanjobs anzeigen 49

nur in der ersten Session 51

nur Lesen 25

Nur offene Scanjobs anzeigen 49

Nur periodische Scanjobs anzeigen 49

O

Offsite-Konfiguration 77, 78

Offsite-Konfiguration für mobile Clients
verwenden 78

Online-Datenbank für häufig gestellte
Fragen (FAQ) 2

Online-Registrierung 2, 7, 16, 31, 34

Online-Registrierungsformular 2

Online-Spiele 97

Online-Virenlexikon 37

openSUSE 112

Optionen 84, 89, 101

Ordner 58, 65

Ordner auf Viren überprüfen 62

OutbreakShield 61

Outlook 55, 60, 62

Outlook-Schutz 62

P

Partition 58

Passwort 16

Passwortschutz für die Änderung von
Optionen 52, 84

per Nachfrage generiert 98

periodische Scanjobs 41

ping 111

Ping of Death 104

Platzhaltern 58

PlugIn 59

POP3 59, 62

Port 35, 95, 99, 104

Port Scans 104

Port-Adressen 63

Port-Nummer 21

Ports 101, 102

Ports überwachen 62

Ports-Überwachung 62

PremiumHotline 2

PremiumSupport 3

PremiumSupport-Verlängerungen 3

Priorität Scanner 45

Priorität Virenprüfung 82

pro Anwendung 102

pro Protokoll/Port/Anwendung 102

Problemlösungen (FAQ) 107

Profi-Dialog 92, 93, 95, 98, 105

Profi-Dialog verwenden 93, 95, 97

Programmaufbau des Administrators
23

Programmaufbau des
WebAdministrators 88

Programmdateien 33

Programmdateien aktualisieren 76

Programmdateien automatisch
aktualisieren 51, 71, 76
Programmdateien jetzt aktualisieren
71
Programmdateien wurden verändert
oder sind beschädigt 111
Programmname 98
Programmoberfläche 40
Programmpfad 95
Protokoll 98, 99, 101, 105
Protokoll anzeigen 25, 37
Protokollansicht 25
Protokolldatei 25
Protokolle 49, 102
Protokolleinträge 36
Proxy-Einstellungen 32, 33
Proxyserver 34
Proxyserver verwenden 34
Prozessoren 45

Q

Quarantäne 13, 45, 52, 55, 65, 68, 69,
85
Quarantäne: Säubern und
zurückbewegen 65
Quarantäne: Zur Internet-Ambulanz
senden 65
Quarantäne: Zurückbewegen 65
Quarantäne-Ordner 65

R

Rang 98
Rangfolge 98
Rechner 41, 65, 71, 77
Rechner nach der Virenprüfung
ausschalten, wenn kein Benutzer
angemeldet ist 44
Rechner/Gruppe 25
rechte Maustaste 82

Referenzprüfung für Anwendungen
105
Referenzprüfung für geladene Module
105
Regel 99
Regel aktiv 98
Regel Assistent 95, 98, 105
Regel Assistent verwenden 93
Regel erstellen 99, 102
Regel-Assistenten 92
regelmäßiger Scanjob 41
Regelsatz 77, 90, 91, 99
Regelsatz auswählen 77
Regelsatz bearbeiten 77, 92
Regelsatz erstellen 77
Regelsatz für ein nicht
vertrauenswürdiges Netzwerk 93
Regelsatz für ein vertrauenswürdiges
Netzwerk 93
Regelsatz für ein zu blockierendes
Netzwerk 93
Regelsätze 80, 93, 97, 105
Regelsätze erstellen 93
Regelsatzname 93
Registriernummer 16
Registrierte Angriffe 90
Registrierungsnummer 2
remote.log 114
Remote-Installation 7, 22, 74, 107
Remote-Installation der Client-Software
übers Netzwerk 112
Remote-Installation der Linux-Software
112
Richtung 98
Riskware 45, 55
Rollbacks 36
Root-Kennwort 112
Rootkits 45

Router 8

Rückkanal-Technik 97

Rufnummer 35

S

Samba-Dienst 112

Samba-Server 8, 23, 112

Scanfenster anzeigen 82

Scan-Fortschritt regelmäßig an den
Server übermitteln 44

Scanjobs 41, 65

Scanjobs erneut (sofort) ausführen 48

Scanjobs löschen 48

Scannen 99

Scanner 45

Scanoptionen 61

Scan-Protokolle 36

Secondary MMS 14

Security-Symbol 82, 89, 99

Seitenansicht 27, 68, 74

Server 18, 19, 23

Server (aktiviert) 39

Server (deaktiviert) 39

Server verwalten 26, 71

Serveranwendung 102

Server-Einstellungen 36

Servernamen 81

Server-Typ auswählen 14

ServiceCenter 3, 112

Setup/LinuxClient/Debian 112

Setup/LinuxClient/Fedora 112

Setup/LinuxClient/Suse 112

Sicherheit 90

Sicherheitsstufen 101

SLE 112

SMB Die 104

SMB-Protokoll 8, 112

SMTP 21, 59, 62

SMTP-Server 35

Software-CD 11

Sonstiges 105

Spamfilter 64, 84

Spamfilter verwenden 64

spezielle Regel für dieses
Protokoll/Port/Anwendung erstellen
99

Spyware 45, 55

SQL-Datenbank 14, 17

SQL-Server 15

Standardgateway 92

Standardports 62

Start-IP Adresse 30

Start-Menü 11

Statistik 40, 80

Status 35, 40, 41, 59, 65, 90, 112

Status aktualisieren 32

Stealth-Modus 93, 97

Sternchen-Symbol 58

Subnet-Server 37

Subnet-Servern 26, 71

Subnet-Server-Synchronisation 26

Subnetzmaske 92

Symbol in der Startleiste 51, 81

Symbolleiste 23, 37

SYN Flood 104

Synchronisation 37

System 8

Systembereiche 45

Systembereiche beim Medium-Wechsel
prüfen 55

Systembereiche beim Systemstart
prüfen 55

Systemvoraussetzungen 8

T

Täglich 45
TCP 99, 101, 102, 104
TCP/IP 13
TCP/IP-Ebene 59
TCP/IP-Netzwerk 92, 95
TCP/IP-Protokoll 8
Telefon-Benachrichtigung 35
Temporär erlauben 99
Temporär verweigern 99
T-Online 54
Trillian (ab Version 3.0) 63

U

Ubuntu 112
UDP 99, 101, 102, 104
UDP Flood 104
Übersicht Clients 80
Unbekannte Server Anwendungen 102
Ungelesene Mails beim Programmstart
prüfen (nur für Microsoft Outlook) 60
Ungeschützte Netzwerke 102
Unterordner 58
Update der Virensignaturen 36
Update erledigt 8
Update jetzt durchführen 33
Update jetzt starten 32
Update periodisch ausführen 32, 33
Update Programmdateien 71
Update Virendatenbank 71
Update-Einstellungen 52
Update-Rollback Engine A / B 36
Updates 51
UpdateServer 8, 11, 13, 16, 31, 33

V

Verbindungsanforderung 102

Verbindungsdaten des Internet Explorer
34
Verbindungs-Protokoll 105
Verbindungsprotokolle 98
Verbindungsrichtung 95
Verbindungs-Richtung 98
Version Client 71
Versionsinformation 60
Versionsnummer 2
Versionsprüfung 34
vertrauenswürdige Netzwerke 90, 93
Verwerfen 54
Verzeichnis 58
Verzögerung 112
Virendatenbank 32
Virendatenbank aktualisieren 75
Virendatenbank automatisch
aktualisieren 71, 75
Virendatenbank jetzt aktualisieren 71
Virengeprüft von G Data AntiVirus 60
Virenkontrollen 26
Virenlexikon 37, 60
Virenprüfung 52, 82, 84
Virenprüfung abbrechen 82
Virenprüfung anhalten 82
Virens Scanner 65
Virenschutz 2
Virensignaturen 8, 112
Virensignaturen automatisch
aktualisieren 51
Virenwächter 45, 55, 63
Virus 65
Virus aus der Datei entfernen 65
Virus entfernen 68
Virus gefunden 65
Virus News 60
Vollbildmodus 105

Vor der Installation 7

Voreingestellte Regel 98

Vorgang 25

Vorsicht 114

W

Wächter 7, 21, 30, 45, 54, 65, 84, 114

Wächter Ausnahmen 58

Wächter ausschalten 84

Wächteroptionen 52

Wächterstatus 55

Warnmeldungen 59, 61

Was mache ich, wenn mein Computer
nicht von CD-ROM bootet? 8

Was möchten Sie tun? 105

Web/IM 62

Web-/IM-Filter 84

WebAdministrator 11, 87, 88

Webbrowser 87

Web-Browsers 87

Weitere Programmstarts
(Zugangskennwort) 23

Wie kann ich überprüfen, ob die Clients
eine Verbindung zum
ManagementServer haben? 111

Windows-Authentisierung 19

Windows-Benutzer 25

Windows-Benutzergruppe 25

Windows-Benutzerkonto 19

Windows-Clients 112

Windows-Update 105

Windows-Version 11

WINS 92

Wochentage 45

Wollen sie das erlauben? 99

Workstation-Client 112

WWW-Dienste 87

Z

Zeitfenster 35, 98

Zeitintervall 41

Zeitplan 41

Zeitplanung 41

Zeitpunkt 45, 71

Zeitpunkt / Zeitplanung 45

Zeitraum 25

Zeitüberschreitung im Browser
vermeiden 63

Zielordner 14

zu blockierende Netzwerke 90, 93

Zugangsdaten 21, 88

Zugangsdaten und Einstellungen 31,
32, 33, 34

Zugriff 98

zum nächsten Neustart des Rechners
84

Zur Internet Ambulanz senden 68

Zurückbewegen der Datei 110

zweiter Server 14