G DATA
SECURITY SOFTWARE

Inhaltsverzeichnis

1. Einführung

In Zeiten der weltweiten Vernetzung und den daraus resultierenden massiven Sicherheitsrisiken, ist das Thema Virenschutz nicht länger nur für IT-Fachleute von Interesse. Es muss vielmehr im Rahmen eines umfassenden, unternehmensweiten Risikomanagements auf höchster Managementebene betrachtet werden. Ein durch Viren verursachter Ausfall des Computernetzwerks 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-Lösungen wird seit Jahren in zahlreichen Tests mit Traumnoten prämiert. Die G DATA Business-Software 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 ab. Automatische Internet-Updates sorgen im Ernstfall einer Virenattacke für extrem kurze Reaktionszeiten. Die zentrale Steuerung mit dem G DATA ManagementServer ermöglicht Installation, Einstellungen, Updates, Fernsteuerung und Automatik für das gesamte Netzwerk. Das entlastet den Systemadministrator, spart Zeit und Kosten.

Wir wünschen Ihnen erfolgreiches und sicheres Arbeiten mit Ihrer G DATA Business-Software.

Ihr G DATA-Team

1.1. Dokumentation

Ausführliche Informationen zur Verwendung der G DATA-Lösungen finden Sie in der Programmhilfe, die Sie jederzeit über die Taste F1 kontextsensitiv öffnen können. Außerdem haben Sie die Möglichkeit, eine ausführliche PDF-Dokumentation im Downloadbereich der **G DATA Webseite** herunterzuladen.

1.2. Support

Der Support für G DATA Netzwerklizenzen steht allen registrierten Business-Kunden jederzeit zur Verfügung.

> Telefon: +49 234 9762 901
> Nutzen Sie eine Flatrate, so ist das Supportgespräch nach den Tarifbedingungen ohne zusätzliche Kosten.
>
> E-Mail: **business-support@gdata.de**
>
> Viele Fragen und Sachverhalte sind auch schon im Supportbereich der G DATA Webseite beantwortet worden. Besuchen Sie uns unter:
>
> **www.gdata.de**

Überprüfen Sie vor Gesprächen mit den Support-Mitarbeitern, wie Ihr Computer/Netzwerk ausgestattet ist. Wichtig sind dabei vor allem folgende Informationen:

- Die Versionsnummer des G DATA Administrators (diese finden Sie im Hilfe-Menü)
- Die Registrierungsnummer oder den Benutzernamen für das Internet-Update. Die Registriernummer finden Sie in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor.

- Die genaue Version des Betriebssystems (Client/Server)
- Zusätzlich installierte Hard- und Softwarekomponenten (Client/Server)
- Eventuell auftretende Fehlermeldungen (inkl. Fehlercodes, sofern vorhanden) im genauen Wortlaut

Mit diesen Angaben wird das Gespräch mit den Support-Mitarbeitern kürzer, effektiver und erfolgreicher verlaufen. Wenn möglich, platzieren Sie das Telefon in der Nähe eines Rechners, auf dem der G DATA Administrator installiert ist.

1.3. G DATA Security Labs

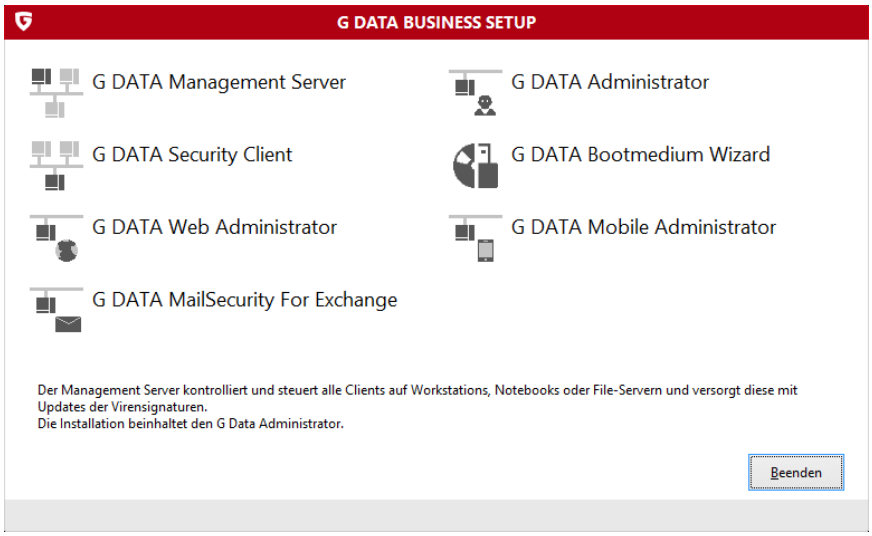
Sollten Sie einen neuen Virus oder ein unbekanntes Phänomen feststellen, senden Sie uns in jedem Fall diese Datei über die Quarantäne-Funktion. Klicken Sie dazu im Bereich **Sicherheitsereignisse** mit der rechten Maustaste auf einen Virusfund und wählen dort die Option **Quarantäne: An G DATA Security Labs senden**. Selbstverständlich behandeln wir Ihre eingesandten Daten höchst vertraulich und diskret.

1.4. G DATA Business-Lösungen

In dieser Dokumentation ist die Funktionalität aller G DATA Business-Module beschrieben. Sollten Sie bei Ihrer installierten Software-Version ein Feature vermissen, können Sie über unsere **Webseite** bequem Informationen zum Upgrade Ihrer Software erhalten.

2. Installation

Starten Sie Windows und legen Sie das G DATA-Installationsmedium ein. Es öffnet sich automatisch ein Installationsfenster, in dem Sie auswählen können, welche der G DATA Software-Komponenten Sie installieren wollen. Wenn Sie eine Download-Version der Software erhalten haben, extrahieren Sie alle Dateien und starten Sie Setup.exe. Um die Installation auf anderen Geräten zu erleichtern, können die extrahierten Dateien auf DVD gebrannt oder auf einen USB-Stick kopiert werden. Schließen Sie 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. Folgende Installationsmöglichkeiten stehen zur Verfügung:



- **G DATA ManagementServer**: Als erstes sollte der G DATA ManagementServer auf dem Computer installiert werden, der alle G DATA-relevanten Einstellungen und Updates verwalten soll. Der G DATA ManagementServer ist das Herzstück der G DATA Architektur: Er verwaltet die Clients, fordert neueste Software- und Virensignaturupdates automatisch von den G DATA Update-Servern an und steuert den Virenschutz im Netzwerk. Mit der Installation des G DATA ManagementServers wird automatisch auch der G DATA Administrator installiert, mit dem der G DATA ManagementServer konfiguriert wird.
- **G DATA Administrator**: Der G DATA Administrator ist die Steuerungssoftware für den G DATA ManagementServer, die die Verwaltung von Einstellungen und Updates für alle im Netzwerk installierten G DATA-Clients ermöglicht. Der G DATA Administrator ist passwortgeschützt und kann auf jedem Windows-Rechner installiert und gestartet werden, der übers Netzwerk mit dem G DATA ManagementServer verbunden ist.
- **G DATA Security Client**: Die Client-Software stellt den Virenschutz für die Clients bereit und führt die ihm vom G DATA ManagementServer zugewiesenen Jobs im Hintergrund aus. Die Installation der Client-Software erfolgt in der Regel zentral für alle Clients über den G DATA Administrator.
- **G DATA Bootmedium Wizard**: Mit Hilfe des G DATA Bootmedium Wizards können Sie eine bootfähige CD, DVD oder einen USB-Stick zur grundlegenden Überprüfung Ihres Rechners erstellen. Diese Überprüfung findet noch vor dem Start des installierten Betriebssystems statt. Dazu werden die aktuellen Virensignaturen verwendet.
- **G DATA WebAdministrator**: Der G DATA WebAdministrator ist eine webbasierte Steuerungssoftware für den G DATA ManagementServer. Mit ihm können Einstellungen für den G DATA ManagementServer über ein Webinterface in einem Browser vorgenommen werden. Er

kann auf diese Weise eine Alternative für die Installation des G DATA Administrators sein.

- **G DATA MobileAdministrator**: Der MobileAdministrator ist eine Web-basierende Steuerungssoftware für den ManagementServer. Er kann mit Hilfe eines Mobile-Web-Browsers gestartet werden und bietet Ihnen grundlegende Administrationsfunktionen des G DATA Administrators.
- **G DATA MailSecurity für Exchange**: Die G DATA MailSecurity für Exchange sichert - vom Systemadministrator zentral gesteuert - den gesamten Exchange-basierten E-Mailverkehr. Die G DATA MailSecurity für Exchange ist als **optionales Modul** verfügbar.
- **G DATA MailSecurity MailGateway**: Das G DATA MailSecurity MailGateway sichert - vom Systemadministrator zentral gesteuert - den gesamten SMTP- und POP3 basierten E-Mailverkehr. Das G DATA MailSecurity MailGateway ist als **optionales Modul** verfügbar und steht auf einem eigenen Installationsmedium zur Verfügung.

2.1. Erste Schritte

Führen Sie bei akutem Virenverdacht auf den betroffenen Rechnern erst einen **Bootscan** durch.

1. Installieren Sie den **G DATA ManagementServer** auf Ihrem Server. Um den optimalen Schutz zu gewährleisten, sollte der Rechner immer erreichbar (eingeschaltet) sein und für das automatische Laden der Virensignaturen über einen Internetzugang verfügen. Die Installation des G DATA ManagementServers muss nicht auf einem Serverbetriebssystem erfolgen (siehe **Systemvoraussetzungen**). Bei der Installation des G DATA ManagementServers wird automatisch der **G DATA Administrator** auf dem Server installiert. Mit diesem Programm kann der G DATA ManagementServer gesteuert werden.
2. Führen Sie nun die Online-Registrierung durch. Ohne eine Online-Registrierung können keine Aktualisierungen der Software und der Virensignaturen erfolgen.
3. Beim ersten Start des G DATA Administrators auf dem Server startet der **Einrichtungsassistent**. Mit diesem kann die **Client-Software** auf den gewünschten Clients in Ihrem Netzwerk auch über eine Remote-Installation verteilt und eingespielt werden. Alle Einstellungen, die mit dem Einrichtungsassistenten vorgenommen werden, lassen sich auch nachträglich ändern.

   Sollten sich Probleme bei der **Remote-Installation** der Clients ergeben, kann die Client-Software auch über eine **Active Directory-Synchronisierung** eingespielt werden oder lokal auf dem jeweiligen Client mit Hilfe des **G DATA-Installationsmediums** oder einem selbst erstellten **Client-Installationspaket** installiert werden. Damit der Server selbst vor Virenbefall geschützt ist, empfiehlt sich auch für den Server die Installation der Client-Software.
4. Nach erfolgter Einrichtung und Installation der Client-Software auf den angeschlossenen Maschinen kann der Virenschutz sowie die Internet-Updates der G DATA Client- und Serversoftware zentral gesteuert werden. Der G DATA Administrator bietet unter anderem Einstellungsmöglichkeiten für den Echtzeitschutz durch den G DATA Wächter sowie die Möglichkeit, Scanaufträge zu definieren, die das Netzwerk regelmäßig auf Virenbefall untersuchen.

   Sollte es notwendig werden, ein Einstellungsproblem an einem Client vor Ort zu lösen, kann der G DATA Administrator auf jedem Client innerhalb des Netzwerks installiert werden. Damit entfällt die Notwendigkeit, alle Einstellungen lokal am Server vorzunehmen. Sollte es notwendig sein, eine kritische Situation innerhalb Ihres Netzwerks, jedoch außerhalb Ihres Unternehmens zu lösen, so kann dafür der G DATA WebAdministrator über jeden Desktop-Web-

Browser verwendet werden. Mit dem G DATA MobileAdministrator können Sie die Administration sogar unterwegs von Ihrem Mobile-Web-Browser aus durchführen.

2.1.1. Systemvoraussetzungen

Folgende Mindestanforderungen gelten für die G DATA-Lösungen:

G DATA ManagementServer

- Betriebssystem: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 oder Windows Server 2003
- Arbeitsspeicher: 1 GB

G DATA Administrator/G DATA WebAdministrator/G DATA MailSecurity Administrator

- Betriebssystem: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-Bits), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 oder Windows Server 2003

G DATA MobileAdministrator

- Betriebssystem: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 oder Windows Server 2008 R2

G DATA Security Client

- Betriebssystem: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista SP1, Windows XP SP3 (32-Bits), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 oder Windows Server 2003
- Arbeitsspeicher: 1 GB

G DATA Security Client für Linux

- Betriebssystem: 32- und 64-Bits-Versionen von Debian 7, 8 und 9, OpenSUSE Leap 42.1 (64-Bits) und Leap 42.2 (64-Bits), Suse Linux Enterprise Server 11 SP4 und 12 (64-Bits), Red Hat Enterprise Linux 5.11, 6.6 und 7.0 (64-Bits), Ubuntu 14.04.1 LTS und 16.04, CentOS 5.11, 6.6 und 7.0 (64-Bits), Fedora 24 und 25

G DATA Security Client für Mac

- Betriebssystem: Mac OS X 10.7 oder höher

G DATA Mobile Device Management für Android

- Betriebssystem: Android 4.0 oder höher

G DATA Mobile Device Management für iOS

- Betriebssystem: iOS 7 oder höher

G DATA MailSecurity MailGateway

- Betriebssystem: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-Bits), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 oder Windows Server 2003
- Arbeitsspeicher: 1 GB

G DATA MailSecurity für Exchange (64-Bits Exchange-Plugin)

- Mail-Server: Microsoft Exchange Server 2016, Microsoft Exchange Server 2013, Microsoft Exchange Server 2010 oder Microsoft Exchange Server 2007 SP1

G DATA-Lösungen nutzen das TCP/IP-Protokoll zur Kommunikation von Client- und Server-Rechnern untereinander.

Bei der Verwendung von G DATA ManagementServer/G DATA MailSecurity MailGateway mit einer lokalen SQL-Datenbank oder anderen anspruchsvollen Anwendungen auf dem gleichen Rechner, gelten die folgenden empfohlenen Systemvoraussetzungen:

- Arbeitsspeicher: 4 GB
- CPU: multicore

2.1.2. Firewall-Konfiguration

Wenn Sie eine Software-Firewall oder Firewall auf Netzwerkebene verwenden, müssen Sie möglicherweise Änderungen an der Firewall-Konfiguration vornehmen. Konfigurieren Sie Ihre Firewall direkt nach der Installation von G DATA-Software, um sicherzustellen, dass alle Funktionen zur Verfügung stehen.

2.1.2.1. Ports

Die G DATA-Lösungen nutzen unterschiedliche TCP-Ports zur sicheren Kommunikation innerhalb Ihres Netzwerks. Bitte stellen Sie sicher, dass diese Ports in Ihrer Firewall entsprechend freigegeben sind:

Haupt- und Secondary-ManagementServer

- Port 80 (TCP)
- Port 443 (TCP)
- Port 7161 (TCP)
- Port 7182 (TCP)
- Port 7183 (TCP)

Subnet-Server

- Port 80 (TCP)
- Port 443 (TCP)
- Port 7161 (TCP)

Clients

- Port 7169 (TCP)

MailSecurity MailGateway Server

- Port 7182 (TCP)

MailSecurity Exchange-Plugin

- Port 7171 (TCP)
- Port 7185...7195 (TCP)

Die Portnummern wurden für die G DATA Software so ausgewählt, um Konflikte mit bestehenden

Standardanwendungen zu vermeiden. Sollte es dennoch zu Port-Konflikten kommen, können Sie die Ports des G DATA ManagementServers natürlich entsprechend ändern. Öffnen Sie dazu zuerst den Dienste-Manager (**Start**, **Ausführen**, *services.msc*) mit Administrator-Rechten und stoppen Sie den G DATA ManagementServer Hintergrund-Task. Öffnen Sie nun im Installationsordner des G DATA ManagementServers (typischerweise C:\Program Files\G Data\G DATA AntiVirus ManagementServer) die Datei Config.xml in einem Text-Editor (z. B. Notepad). Hinterlegen Sie nun - falls notwendig - für die folgenden Einträge geänderte Portnummern:

- **AdminPort**: Geben Sie hier die gewünschte Portnummer ein. Der Standardwert ist hier "0" (d.h. der Port bliebe dann voreingestellt auf 7182).
- **ClientHttpsPort**: Der Standardwert ist hier "0" (d.h. der Port bliebe dann voreingestellt auf 443). In der Regel sollte der ClientHttpsPort-Wert nicht geändert werden, da Android-Clients keinen alternativen Port akzeptieren.
- **ClientHttpPort**: Geben Sie hier die gewünschte Proxy-Nummer ein. Der Standardwert ist hier "0" (d.h. der Port bliebe dann voreingestellt auf 80).

Wenn Sie die Werte für den ClientHttpPort oder den ClientHttpsPort ändern, müssen Sie die HTTP-Sicherheitskonfiguration für den jeweiligen Port neu initialisieren. Öffnen Sie dazu die Kommandozeile mit Administrator-Rechten und starten Sie *C:\Program Files\G Data\G DATA AntiVirus ManagementServer\gdmmsconfig.exe /installcert*.

Führen Sie einen Neustart des G DATA ManagementServers durch, nachdem Sie die Ports geändert haben. Bitte beachten Sie: Falls Sie den AdminPort geändert haben, müssen Sie bei jedem Einloggen beim G DATA Administrator den geänderten Port angeben. Dies erfolgt in folgendem Format: *Servername:Port*.

2.1.2.2. URLs

Beim Einsatz des **PatchManager**-Moduls lädt G DATA ManagementServer Patch-Konfigurationsdateien und Patches herunter. Wenn Sie eine Firewall verwenden, muss der Datenverkehr zwischen G DATA ManagementServer und den folgenden URLs deswegen immer erlaubt sein:

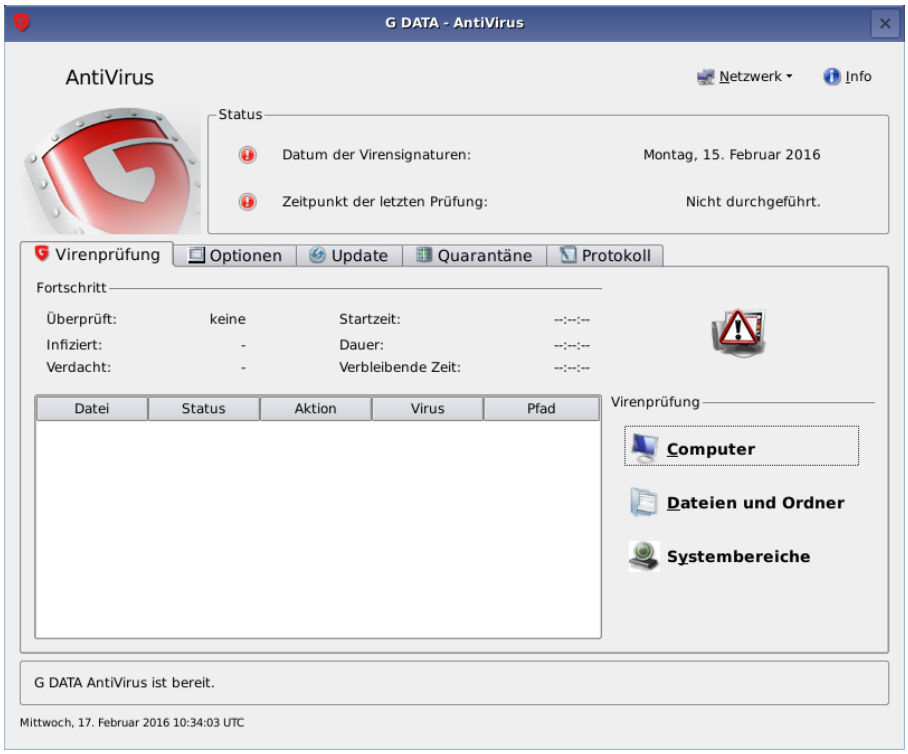
- *gdata.cdn.heatsoftware.com*

Abhängig von der Software, für die Sie Patches verteilen, muss darüber hinaus der Datenverkehr zwischen G DATA ManagementServer und den folgenden URLs erlaubt sein:

- 7-Zip: *http://downloads.sourceforge.net*
- Adobe: *ardownload.adobe.com*, *armdl.adobe.com*, *download.adobe.com*, *swupdl.adobe.com*, *www.adobe.com*
- Microsoft: *go.microsoft.com*, *download.windowsupdate.com*, *www.download.windowsupdate.com*, *download.skype.com*, *download.microsoft.com*
- Mozilla: *http://ftp.mozilla.org*
- UltraVNC: *http://support1.uvnc.com*
- VideoLAN: *http://download.videolan.org*

2.1.3. G DATA Bootmedium

Das G DATA Bootmedium erlaubt eine Bekämpfung von Viren, die sich vor der Installation der Antivirensoftware auf einem Rechner eingenistet haben und möglicherweise die Installation der G DATA-Lösung unterbinden möchten. Dazu gibt es eine spezielle Programmversion von G DATA AntiVirus, die schon vor dem Systemstart ausgeführt werden kann.



1. **Mit dem Installationsmedium**: Legen Sie das G DATA-Installationsmedium ein. Klicken Sie auf dem sich öffnenden Startfenster auf **Beenden** und schalten Sie den Computer aus.
   Mit selbst erstelltem G DATA Bootmedium: Hierzu muss zunächst das Erstellungsprogramm für das G DATA Bootmedium installiert werden. Dies muss auf einem System erfolgen, auf dem G DATA Security Client mit aktuellen Signaturen installiert ist. Folgen Sie bitte nach der Installation den Anweisungen des **G DATA Bootmedium Wizards**, um ein Bootmedium zu erzeugen.
2. Starten Sie den Computer neu. Es erscheint das Startmenü des G DATA Bootmediums.
3. Wählen Sie mit den Pfeiltasten ihre Sprache und danach die Option **G DATA AntiVirus**. Es wird nun ein Linux-Betriebssystem gestartet und es erscheint eine Spezialversion von G DATA AntiVirus.

   Falls Sie Probleme mit der Ansicht der Programmoberfläche haben, starten Sie den Rechner erneut und wählen bitte die Option **G DATA AntiVirus – Alternativ** aus.
4. Wenn Sie selbst ein G DATA Bootmedium erstellt haben, sind die Virensignaturen auf dem Updatestand, den der G DATA Security Client zum Zeitpunkt der Erstellung des Bootmediums geladen hat. Falls nötig, schlägt das Programm vor, die Virensignaturen zu aktualisieren. Klicken Sie hier auf **Ja** und führen Sie das Update durch. Stellen Sie sicher, dass Sie Ihre Registriernummer oder, falls Sie Ihre G DATA-Lösung bereits registriert haben, Ihre Zugangsdaten eingegeben haben, damit das Update durchgeführt werden kann.
5. Nun sehen Sie die Programmoberfläche. Klicken Sie auf den Eintrag **Computer** und Ihr Computer wird auf Viren und Schadsoftware untersucht. Dieser Vorgang kann je nach Rechnertyp und Festplattengröße eine Stunde oder länger dauern.
6. Sollte die G DATA Software Viren finden, entfernen Sie diese mit Hilfe der im Programm

vorgeschlagenen Option. Nach einer erfolgreichen Entfernung des Virus steht Ihnen die Originaldatei weiter zur Verfügung.

7. Nach Abschluss der Virenüberprüfung klicken Sie auf die Schließen-Schaltfläche (oben rechts in der Linux-Programmoberfläche) und wählen anschließend **Beenden** > **Herunterfahren** aus.
8. Entfernen Sie das G DATA Bootmedium aus dem Laufwerk bzw. dem USB-Port.
9. Schalten Sie ihren Computer wieder aus und starten Sie ihn erneut. Nun startet Ihr Computer wieder mit Ihrem Standard-Betriebssystem. Die G DATA Software kann jetzt auf einem virenfreien System installiert werden.

2.1.3.1. G DATA Bootmedium Wizard

Um ein G DATA Bootmedium zu erstellen, müssen Sie zunächst G DATA Bootmedium Wizard installieren. Dies sollte auf einem System erfolgen, auf dem ein G DATA Security Client mit aktuellen Virensignaturen läuft. Legen Sie das G DATA-Installationsmedium ein und wählen Sie **G DATA Bootmedium Wizard** aus.

Nach Abschluss der Installation können Sie unter **Start** > **(Alle) Programme** > **G DATA BOOTMEDIUM** mit einem Klick auf **G Data BootMediumWizard** assistentengestützt ein Bootmedium erzeugen, indem Sie dieses auf CD/DVD brennen, auf einem USB-Stick speichern oder als ISO-Image speichern. Das ISO-Image kann dann ggf. über das Netzwerk an die Clients distribuiert werden.

2.1.3.2. Boot-Option im BIOS einstellen

Sollte das System nicht von CD/DVD-ROM oder USB-Stick booten, kann es sein, dass diese Option erst eingestellt werden muss. Dies erfolgt im BIOS, einem System, das noch vor Ihrem Betriebssystem gestartet wird. Um hier Änderungen vorzunehmen, führen Sie folgende Schritte durch:

1. Schalten Sie den 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**-Taste) drücken. Die Dokumentation des Rechnerherstellers liefert hierzu weitere Hinweise.
3. Wie Sie die Einstellungen in Ihrem BIOS-Setup im Einzelnen ändern, entnehmen Sie der Dokumentation Ihres Mainboard-Herstellers. Im Ergebnis sollte die Bootreihenfolge **USB, CD/DVD-ROM, C:** lauten, d.h. USB-Sticks werden zum 1. Boot-Device, das CD/DVD-ROM-Laufwerk zum 2. Boot-Device und die Festplatten-Partition mit Ihrem Windows-Betriebssystem zum 3. Boot-Device.

4. Speichern Sie die Änderungen und starten Sie Ihren Computer neu. Jetzt ist Ihr Computer bereit für einen Scan vor dem Systemstart.

2.2. Installation des G DATA ManagementServers

Legen Sie das G DATA-Installationsmedium ein und wählen Sie anschließend **G DATA ManagementServer** aus. Schließen Sie spätestens jetzt alle offenen Anwendungen in Ihrem Windows-System, da diese sonst zu Problemen bei der Installation führen können. Wählen Sie Ihre Sprache und Klicken Sie auf **Installation** um den Installationsassistenten zu starten. Lesen Sie sich nun die Lizenzvereinbarung zur Nutzung dieser Software durch. Wählen Sie **Ich akzeptiere die Lizenzvereinbarung** und klicken Sie dann auf **Weiter**, wenn Sie den Vereinbarungen in dieser Form zustimmen.

Nach der Auswahl eines Installationsordners, kann der Server-Typ gewählt werden. Sie haben folgende Möglichkeiten:

- **Haupt-Server**: Bei einer Erstinstallation muss der G DATA ManagementServer immer als Haupt-Server (Haupt-MMS) installiert werden. Der Haupt-Server stellt die zentrale Konfigurations- und Verwaltungsinstanz der netzwerkbasierten G DATA-Architektur dar. Die zu schützenden Rechner werden über den G DATA ManagementServer mit den jeweils aktuellsten Virensignatur- und Programmupdates versorgt. Darüber hinaus werden sämtliche Client-Einstellungen zentral am G DATA ManagementServer vorgenommen.
- **Secondary-Server**: Bei Verwendung einer selbständigen SQL-Instanz ist es möglich, einen zweiten Server (Secondary-MMS) zu betreiben, der auf die gleiche Datenbank wie der Haupt-Server zugreift. Falls der Haupt-Server eine Stunde oder länger nicht erreichbar ist, werden die Clients sich automatisch mit dem Secondary-Server verbinden und von diesem Signaturupdates laden. Der Wechsel zurück zum Haupt-Server erfolgt, sobald dieser wieder verfügbar ist. Beide Server laden die Signaturupdates unabhängig voneinander und stellen so eine Ausfallsicherheit her.
- **Subnet-Server**: Bei großen Netzwerken (z. B. Firmenzentrale mit angeschlossenen Zweigstellen) kann es sinnvoll sein, einen G DATA ManagementServer als Subnet-Server zu betreiben. Subnet-Server dienen der Entlastung des Netzwerks zwischen Clients und dem Haupt-MMS und verwalten nur die ihnen zugeordneten Clients. Die Subnet-Server bleiben funktionsfähig, auch wenn Haupt- oder Secondary-Server nicht erreichbar sind. Diese laden allerdings selbständig keine Virensignaturupdates. Geben Sie im Feld **Hostname oder IP** den Servernamen ein, auf dem der Haupt-Server läuft.

  Eine Alternative zur Benutzung eines Subnet-Servers ist die **Peer to Peer Updateverteilung**. Durch die Aktivierung dieser Option wird die Netzauslastung zwischen Server und Client während der Updateverteilung stark reduziert. Bei einigen Netzwerken kann auf diese Weise die Installation eines Subnet-Servers überflüssig sein.

Nach der Auswahl des Server-Typs wählen Sie den Datenbank-Server aus, den der G DATA ManagementServer verwenden soll:

- **Microsoft SQL Server 2014 Express installieren**: Wählen Sie die Express-Variante, wenn Sie G DATA ManagementServer in einem Netzwerk mit weniger als 1000 Clients installieren. Der Microsoft SQL Server 2014 Express bietet keine Unterstützung für Windows Vista und Windows Server 2008/2003. Installieren Sie auf solchen Systemen manuell den Microsoft SQL Server 2008 R2 Express, bevor Sie G DATA ManagementServer installieren, oder verwenden Sie eine bereits existierende Datenbankinstanz auf einem anderen Server. Mehr Informationen finden Sie im

Reference Guide.

- **Bereits existierende Datenbankinstanz verwenden**: Die SQL-Server-Instanz-Variante bietet sich vor allem in größeren Netzwerken mit einer Client-Anzahl ab 1000 an. Falls Sie G DATA ManagementServer auf einem Server installieren, auf dem sich schon eine SQL-Server-Express-Installation und eine ManagementServer-Datenbank befinden, wählen Sie die Instanz-Variante. Nach der Installation können Sie dann die Verbindung zum SQL Server (Express) konfigurieren.

Die Installation wird gestartet, sobald Sie die in der Installationsübersicht stehenden Einstellungen mit einem Klick auf **Weiter** bestätigen. Nach der Installation des G DATA ManagementServers soll die G DATA-Lösung aktiviert werden. Dies ermöglicht das Laden von Updates nach Beendigung der Installation:

- **Eine neue Registriernummer eingeben**: Wenn Sie die G DATA-Lösung das erste Mal installieren, wählen Sie diese Option aus und geben anschließend die Registriernummer ein. Sie finden diese in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren G DATA Händler bzw. Distributor. Durch die Eingabe der Registrierungsnummer wird Ihre Software-Lösung aktiviert. Die erstellten Zugangsdaten werden Ihnen nach erfolgreicher Registrierung angezeigt. **Notieren Sie sich unbedingt diese Zugangsdaten!** Nach erfolgter Registrierung ist eine erneute Eingabe des Lizenzschlüssels nicht mehr möglich.

  Sollten Sie bei der Eingabe der Registriernummer Probleme haben, überprüfen Sie die Registriernummer auf die korrekte Eingabe. Je nach verwendeten Schriftsatz wird ein großes "I" (wie Ida) oft als Ziffer "1", bzw. Buchstabe "l" (wie Ludwig) fehlinterpretiert. Das Gleiche gilt für: "B" und "8", "G" und 6, "Z" und "2".

- **Zugangsdaten eingeben**: Wenn die G DATA Software schon einmal installiert wurde, haben Sie Zugangsdaten (Benutzername und Passwort) erhalten. Um die G DATA Software erneut zu installieren, geben Sie hier die Zugangsdaten an.
- **Später aktivieren**: Wenn Sie sich zunächst nur einen Überblick über die Software verschaffen möchten oder die Zugangsdaten für den Moment nicht greifbar sind, kann die Installation auch ohne Angabe von Daten installiert werden. Da auf diese Weise allerdings vom Programm keine Aktualisierungen aus dem Internet geladen werden, ist kein echter Schutz vor Schadsoftware gegeben. Nur mit tagesaktuellen Updates kann die G DATA Software Ihren Computer effektiv schützen. Eine Nutzung der Software ohne Aktivierung schützt Sie nur unzureichend. Sie können Ihre Registrierungsnummer oder Ihre Zugangsdaten jederzeit nachträglich eingeben. Lesen Sie hierzu auch die **Hinweise zur nachträglichen Aktivierung der G DATA Software**.

  Beachten Sie: wird die Software installiert, ohne sie zu aktivieren, sind nur die G DATA AntiVirus Business-Komponenten verfügbar, selbst wenn Sie eine G DATA Client Security Business, eine G DATA Endpoint Protection Business oder andere Module erworben haben. Die zusätzlichen Komponenten werden aktiviert und sind verfügbar, sobald die Software registriert wird.

Falls Sie sich für die Verwendung einer bereits existierenden Datenbankinstanz entschieden haben, können Sie die Konfiguration des Datenbanktyps vornehmen, sobald die Installation abgeschlossen ist. Weitere Informationen hierzu finden Sie im Reference Guide.

Nach der Installation des G DATA ManagementServers ist dieser einsatzbereit. Ein Neustart des Servers könnte erforderlich sein. Der G DATA ManagementServer wird bei jedem System(neu)start automatisch mitgestartet.

Um den G DATA ManagementServer zu verwalten, können Sie unter **Start** > **(Alle) Programme** > **G DATA Administrator** den Eintrag **G DATA Administrator** auswählen und auf diese Weise das

Administrationstool für den G DATA ManagementServer starten.

2.3. Installation des G DATA Administrators

Bei einer Installation des **G DATA ManagementServers** wird automatisch auf demselben Rechner der G DATA Administrator mitinstalliert. Eine nachträgliche Installation der Administratorsoftware auf dem G DATA ManagementServer ist nicht erforderlich. Die Installation des G DATA Administrators kann unabhängig von der Installation auf dem Server auch auf jedem Client-Rechner erfolgen. Auf diese Weise kann der G DATA ManagementServer auch dezentral betreut werden.

Zur Installation des G DATA Administrators auf einem Client-Rechner legen Sie das G DATA-Installationsmedium ein und wählen Sie anschließend **G DATA Administrator** aus.

Schließen Sie spätestens jetzt alle offenen Anwendungen im Windows-System, da diese sonst zu Problemen bei der Installation führen können. Folgen Sie den Installationsschritten, bei denen der Installationsassistent Sie unterstützt. Nach der Installation ist unter **Start** > **(Alle) Programme** > **G DATA** > **G DATA Administrator** der Eintrag **G DATA Administrator** anwählbar.

2.4. Installation des G DATA WebAdministrators

Legen Sie das G DATA-Installationsmedium ein und wählen Sie anschließend **G DATA WebAdministrator** durch einen Klick aus.

Die Installation des G DATA WebAdministrators ist einfach und unkompliziert. Nachdem Sie den Lizenzbedingungen zugestimmt haben, wählen Sie den Installationsordner aus, in dem der WebAdministrator installiert werden soll. Empfohlen wird, diesen im HTTP-Verzeichnis des Webservers zu installieren (z. B. \inetpub\wwwroot).

Während der Installation muss möglicherweise - abhängig von den Systemvoraussetzungen - zusätzliche Software installiert werden:

- **Microsoft Internet Information Services (IIS)**: Da der WebAdministrator ein webbasiertes Produkt ist, muss der Server, auf dem es installiert wird, auch als Webserver nutzbar sein. Der WebAdministrator unterstützt Microsoft Internet Information Services (IIS). Bitte stellen Sie sicher, das IIS auf Ihrem Server läuft, bevor Sie den WebAdministrator installieren.
- **Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration**: Vor der Installation des G DATA WebAdministrators ist die Aktivierung der Windows-Funktion Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration erforderlich. Sollte diese Funktion nicht zur Verfügung stehen, wird die Installation des G DATA 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** > **Kompatibilität mit der IIS 6-Verwaltung** > **Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration** an- oder ausschalten. Außerdem müssen - soweit nicht schon geschehen - die WWW-Dienste aktiviert sein. Hierzu setzen Sie das Häkchen unter **Internetinformationsdienste** > **WWW-Dienste**. In Serverbetriebssystemen finden sich die entsprechenden Optionen im **Servermanager** bei **Rollen**.
- **Microsoft .NET Framework**: Der WebAdministrator basiert auf dem .NET Framework von Microsoft. Sollte auf dem Server kein Microsoft .NET Framework installiert sein, fordert Sie der Installationsassistent des WebAdministrators dazu auf, dieses zu installieren. Nach der Installation ist ein Neustart erforderlich.

- **Microsoft Silverlight**: Der G DATA WebAdministrator benötigt Microsoft Silverlight. Falls dies bei der Installation nicht vorhanden ist, werden Sie beim ersten Start des G DATA WebAdministrators darauf aufmerksam gemacht.

Nach der Installation steht Ihnen auf dem Desktop Ihres Computers das Symbol für den **G DATA WebAdministrator** zur Verfügung. Darüber hinaus erhalten Sie einen Link, mit dem Sie den WebAdministrator über Ihren Browser aufrufen können.

Die Verwendung des WebAdministrators übers Internet ohne eine sichere Verbindung ist ein potentielles Sicherheitsrisiko. Optimalerweise verwenden Sie bitte ein **SSL Server Zertifikat in IIS**.

2.5. Installation des G DATA MobileAdministrators

Legen Sie das G DATA-Installationsmedium ein und wählen Sie anschließend **G DATA MobileAdministrator** durch einen Klick aus.

Die Installation des G DATA MobileAdministrators ist mit der des **WebAdministrators** vergleichbar. Nachdem Sie den Lizenzbedingungen zugestimmt haben, wählen Sie den Installationsordner aus, in dem der MobileAdministrator installiert werden soll. Empfohlen wird, diesen im HTTP-Verzeichnis des Webservers zu installieren (z. B. \inetpub\wwwroot).

Während der Installation muss möglicherweise - abhängig von den Systemvoraussetzungen - zusätzliche Software installiert werden:

- **Microsoft Internet Information Services (IIS)**: Da der MobileAdministrator ein webbasiertes Produkt ist, muss der Server, auf dem es installiert wird, auch als Webserver nutzbar sein. Der MobileAdministrator unterstützt Microsoft Internet Information Services (IIS). Bitte stellen Sie sicher, das IIS auf Ihrem Server läuft, bevor Sie den MobileAdministrator installieren.
- **Microsoft .NET Framework**: Der MobileAdministrator basiert auf dem .NET Framework von Microsoft. Sollte auf dem Server kein Microsoft .NET Framework installiert sein, fordert Sie der Installationsassistent des MobileAdministrators dazu auf, dieses zu installieren. Nach der Installation ist ein Neustart erforderlich.

Nach Beendigung der Installation erhalten Sie einen Link, mit dem Sie den MobileAdministrator mit Ihrem Smartphone über einen Mobile Browser aufrufen können.

Die Verwendung des MobileAdministrators übers Internet ohne eine sichere Verbindung ist ein potentielles Sicherheitsrisiko. Optimalerweise verwenden Sie bitte ein **SSL Server Zertifikat in IIS**.

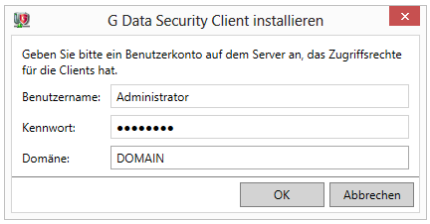
2.6. Installation des G DATA Security Clients

G DATA Security Client schützt und verwaltet Windows-Netzwerkclients und sollte auf jedem Windows-Rechner im Netzwerk installiert sein. Je nach Einsatz-Szenario können Sie die Installation der Client-Software über eine **Remote-Installation** (über den G DATA Administrator) oder über eine **lokale Installation** (per G DATA-Installationsmedium oder ein Client-Installationspaket) durchführen. Darüber hinaus ist es auch empfehlenswert, den G DATA Security Client auch auf dem Server zu installieren.

> Wenn Sie G DATA Security Client auf einem Server installieren, sollten Sie sicherstellen, dass keine Konflikte mit bestehenden Workflows entstehen. Zum Beispiel sollten Sie auf Database-Servern und E-Mail-Servern für manche Ordner und Dateien Scan- und Wächterausnahmen definieren. Weitere Informationen hierzu finden Sie im Reference Guide.

2.6.1. Remote-Installation

Der bequemste Weg, um die Client-Software auf den Clients zu installieren, ist die Remote-Installation über den G DATA Administrator. Über den **Server-Einrichtungsassistent** oder das **Clients**-Modul können Sie automatisch den G DATA Security Client auf allen im Netzwerk angeschlossenen Rechnern installieren.



Abgesehen von den erforderlichen **Port-Konfigurationen** sind folgende Voraussetzungen nötig, um eine Remote-Installation durchzuführen:

- Es muss ein Benutzerkonto mit Administrator-Berechtigungen auf dem Client eingegeben werden. Das Konto muss nicht unbedingt ein Kennwort haben. Allerdings muss der Zielrechner dann umkonfiguriert werden, um Netzwerkanmeldungen für Konten ohne Kennwort zu erlauben. Weitere Informationen hierzu finden Sie im Reference Guide. Für die Remote-Subnet-Server-Installation muss ein Kennwort gesetzt sein: ein leeres Kennwort-Feld ist nicht gestattet.
- Der Service Control Manager auf dem Client muss mit dem angegebenen Benutzerkonto per Remote-Zugriff zugänglich sein.
- Das angegebene Benutzerkonto muss für mindestens eine Netzwerkfreigabe auf dem Client, wie z. B. C$, Admin$ oder eine benutzerdefinierte Freigabe, Schreibrechte haben. Den erforderlichen Zugriff können Sie aktivieren, indem Sie das **Netzwerk- und Freigabecenter** öffnen und unter **Erweiterte Freigabeeinstellungen** die Option **Datei- und Druckerfreigabe aktivieren** einschalten (ab Windows Vista). Auf Windows XP schalten Sie im Windows Firewall unter **Ausnahmen** die **Datei- und Druckerfreigabe** ein.
- Wenn der Client nicht in einer Domäne ist, müssen folgende zusätzlichen Einstellungen konfiguriert werden:
  - Die Option **Einfache Dateifreigabe** (Windows XP) oder **Freigabe-Assistent verwenden** (ab Windows Vista/Windows Server 2008) muss deaktiviert werden. Diese ist standardmäßig in allen Windows-Installationen aktiviert und kann folgendermaßen deaktiviert werden: Öffnen Sie einen beliebigen Ordner im Windows-Explorer, klicken Sie dort auf **Extras** > **Ordneroptionen** > **Ansicht**, und deaktivieren Sie nun die jeweilige Option.
  - Wenn der Client Windows Vista oder höher verwendet: Starten Sie den Registrierungs-Editor auf dem Client und öffnen Sie den Schlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Fügen Sie einen DWORD-Wert mit dem Wertnamen *LocalAccountTokenFilterPolicy* und Wert *1* zum Schlüssel hinzu.

Über den **Server-Einrichtungsassistenten**, der automatisch beim ersten Start des G DATA Administrators aufgerufen wird, erhalten Sie einen Überblick über alle in Ihrem Netzwerk angemeldeten Computer. Darüber hinaus können Sie manuell weitere Computer per Namenseingabe hinzufügen und aktivieren. Alternativ können Sie den G DATA Security Client installieren, indem Sie unter **Clients** > **Übersicht** einen oder mehrere Clients auswählen und in dem erscheinenden Kontextmenü **G DATA Security Client installieren** wählen. Egal ob über den **Server-Einrichtungsassistenten** oder das **Clients**-Modul: Anschließend erscheint ein Eingabefenster, in dem Sie **Benutzername**, **Kennwort** und **Domäne** mit Zugriffsrechten auf den Clients eingeben

können. Nach Auswahl der Anzeigesprache öffnet sich automatisch die **Installationsübersicht**. Nach einer erfolgreichen Installation der Software muss der Client-Rechner meistens neu gestartet werden. Ein entsprechender Bericht wird zu den **Sicherheitsereignissen** hinzugefügt.

> Wenn Sie die **Active Directory Integration** nutzen, können Sie den G DATA Security Client auch automatisch auf neu im Netzwerk eingebundene Rechner installieren.

Die Remote-Installation kann auf zwei verschiedene Arten erfolgen. Wenn der Client die notwendigen Voraussetzungen erfüllt, können die Installationsdaten direkt vom Server aus überspielt und entsprechende Änderungen in der Registry vorgenommen werden. Wenn der Server nur Zugriff auf die Festplatte des Client-Rechners und nicht auf die Registry hat oder andere Systemvoraussetzungen nicht erfüllt sind, dann wird das Setup-Programm auf den Client kopiert und die Installation wird automatisch beim nächsten Neustart des Computers gestartet.

2.6.2. Lokale Installation

Wenn eine **Remote-Installation** nicht möglich ist, können Sie den G DATA Security Client auch direkt manuell auf den Clients installieren. Sie können entweder das G DATA-Installationsmedium dazu verwenden, die Client-Software direkt auf dem Client zu installieren, oder ein Installationspaket erzeugen, welches die Installation im Hintergrund durchführen kann (ideal für die Distribution der Software über Login-Skripts).

2.6.2.1. G DATA Installationsmedium

Zur lokalen Installation des Clients auf einem Client-Rechner legen Sie das G DATA-Installationsmedium ein und wählen Sie anschließend **G DATA Security Client** aus.

Geben Sie im Verlauf der Installation den Servernamen oder die IP-Adresse des Servers ein, auf dem der G DATA ManagementServer installiert ist. Die Angabe des Servernamens ist notwendig, damit der Client über das Netzwerk mit dem Server in Kontakt treten kann. Wenn Sie zusätzlich einen Gruppennamen eingeben, wird der Client zur entsprechenden Gruppe hinzugefügt, sobald er sich am ManagementServer meldet. Lesen Sie das Kapitel **Installationspaket**, um mehr Informationen über die Regeln für die Eingabe von Gruppennamen zu erhalten.

Um unberechtigten Zugriff auf den ManagementServer zu vermeiden, müssen Sie Clients, die mit Hilfe des Installationsmediums installiert werden, im G DATA Administrator autorisieren, bevor sie vollständig verwaltet werden können (siehe **Clients** > **Übersicht**).

2.6.2.2. Installationspaket

Das Paket ist eine einzelne ausführbare Datei (GDClientPck.exe), mit der ein neuer Client 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 oder direkt lokal zu installieren. Das Paket enthält immer die auf dem Server aktuelle Client-Version.

Um ein Installationspaket zu erstellen, starten Sie den G DATA Administrator. Im Menü **Organisation** wählen Sie die Option **Installationspaket für Windows-Clients erstellen**. Nun werden Sie zur Eingabe der folgenden Einstellungen aufgefordert:

- **ManagementServer**: Der ManagementServer, zu dem sich die Clients verbinden sollen.
- **Sprache**: Die installierte Sprache.
- **Gruppe**: Die Gruppe, zu der der Client nach der Installation hinzugefügt wird.

Verwenden Sie einen Schrägstrich "/", um Gruppennamen in einer Hierarchie zu trennen. Sonderzeichen in Gruppennamen müssen markiert werden: Jedes Anführungszeichen muss verdoppelt werden und wenn ein Gruppenname ein "/" enthält, dann muss der Gruppenname in Anführungszeichen eingeschlossen werden.

- **Gültigkeit begrenzen**: Begrenzt die Gültigkeit des Installationspakets. Wenn das Paket nach dem Ablauf der Gültigkeit installiert wird, wird der Client als unautorisiert betrachtet und muss im G DATA Administrator unter **Clients** > **Übersicht** manuell autorisiert werden.

Klicken Sie auf **OK** um einen Speicherort auszuwählen. G DATA Administrator ertstellt das Installationspaket nun im Hintergrund. Es ist unbedingt erforderlich, das Installationspaket auf den Zielrechner zu kopieren und dort mit Administrator-Rechten zu starten. G DATA Security Client wird dann installiert. Falls die Installation ohne Benutzerinterface ausgeführt werden soll, starten Sie das Installationspaket mit dem Parameter /@_QuietInstallation="true": *GDClientPck.exe /@_QuietInstallation="true"*.

2.7. Installation des G DATA Security Clients für Linux

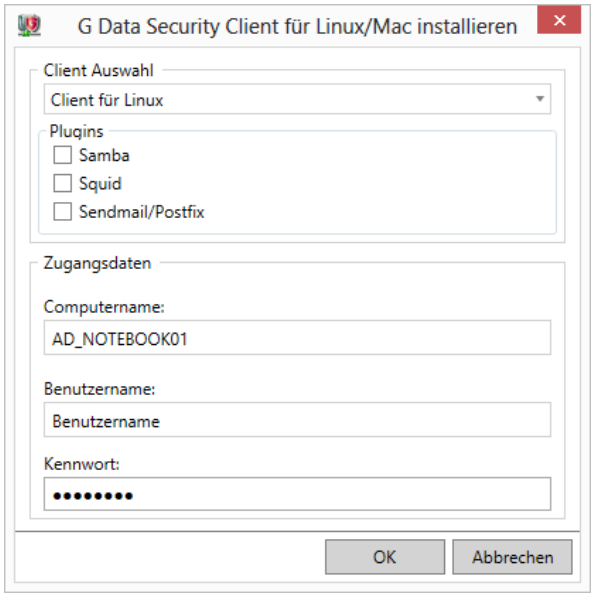
Linux-Clients werden (ebenso wie Windows-Clients) vom G DATA ManagementServer verwaltet, über G DATA Administrator gesteuert und mit automatischen Virensignaturupdates versorgt. Die Standard-Version enthält Funktionen für On-Demand-Virenscans. Darüber hinaus können **zusätzliche Sicherheitsmodule** für Linux-Server installiert werden.

Analog zu Windows-Clients können Sie die Installation der Client-Software über eine **Remote-Installation** (über den G DATA Administrator) oder über eine **lokale Installation** (per Installationsskript) durchführen.

2.7.1. Remote-Installation

Die bequemste Installationsmethode für G DATA Security Client für Linux ist die Remote-Installation. Die Voraussetzungen sind wie folgt:

- Der Linux-Client muss über einen installierten, laufenden SSH-Server verfügen.
- Dem installierenden Benutzer muss die Anmeldung per SSH mit Passwort erlaubt sein.
- Im Netzwerk muss die DNS-Namensauflösung für den ManagementServer und die zu installierenden Clients vorhanden sein.



Die Installationsschritte sind wie folgt:

1. Wählen Sie im Aufgabenbereich **Clients** einen Linux-Client aus und klicken Sie im Menü **Clients** auf **G DATA Security Client für Linux/Mac installieren**.
2. Wählen Sie den Clienttyp (**Client für Linux**) aus.
3. Wählen Sie optional ein oder mehrere **Plugins** aus (**Samba**, **Squid** oder **Sendmail/Postfix**). Beachten Sie hierbei die in den jeweiligen Kapiteln beschriebenen Voraussetzungen.
4. Geben Sie einen **Benutzernamen** und ein **Kennwort** ein. Das Konto muss über Root-Berechtigungen verfügen.
5. Drücken Sie nun auf die **OK**-Schaltfläche. Der Installationsvorgang wird in der **Installationsübersicht** gezeigt.

2.7.2. Lokale Installation

Wenn eine **Remote-Installation** nicht möglich ist, können Sie den G DATA Security Client für Linux auch direkt auf dem Client installieren.

1. Wählen Sie im G DATA Administrator den **Clients**-Bereich aus und klicken Sie im Menü **Organisation** auf **Installationsskript für Linux/Mac-Clients erstellen**.
2. Nachdem Sie einen Speicherort ausgewählt haben, wird das Installationsskript im Hintergrund erstellt.
3. Kopieren Sie das Installationsskript in einen beliebigen Ordner auf dem Client und fügen Sie zu dem Skript die Ausführberechtigung hinzu (Terminal: *chmod +x install-client.sh*).
4. Öffnen Sie ein Terminal-Fenster und aktivieren Sie die Root-Rechte, indem Sie das Kommando *su* und danach das Root-Kennwort eingeben. Alternativ führen Sie das Kommando in Schritt 5 über *sudo* aus.
5. Öffnen Sie den Ordner, in dem sich die kopierte Datei befindet, und starten Sie den Installer mit dem Kommando *./install-client.sh -t <Produkt[,Produkt]>*. Als Produkt geben Sie eine oder mehrere der folgenden Werten ein:
   - *ALL*: G DATA Security Client für Linux und alle Zusatzmodule
   - *WS*: G DATA Security Client für Linux
   - *SMB*: Samba-Modul
   - *AMAVIS*: Sendmail/Postfix-Modul
   - *WEB*: Squid-Modul
6. Um unberechtigten Zugriff auf den ManagementServer zu vermeiden, müssen Sie Clients, die mit Hilfe des Installationsskripts installiert werden, im G DATA Administrator autorisieren, bevor sie vollständig verwaltet werden können (siehe **Clients** > **Übersicht**).

2.7.3. Zusatzmodule

G DATA Security Client für Linux verfügt über Zusatzmodule für den Schutz verschiedener Linux-Komponenten. Wenn Sie während einer Remote- oder Lokalinstallation Zusatzmodule auswählen, werden sie automatisch installiert. Teilweise setzen sie aber zusätzliche Konfigurationsschritte voraus.

2.7.3.1. Samba

Nachdem Sie G DATA Security Client für Linux installiert haben, können Sie den Samba-Schutz einschalten, indem Sie die Zeile *vfs objects = gdvfs* zu der Samba-Konfigurationsdatei (üblicherweise /etc/samba/smb.conf) hinzufügen. Um alle Netzwerkfreigaben zu schützen, fügen Sie die Zeile zu dem Abschnitt *[global]* hinzu. Wenn Sie die Zeile zu einem anderen Abschnitt hinzufügen, wird nur die entsprechende Netzwerkfreigabe geschützt. Nachdem Sie die Konfigurationsdatei gespeichert haben, muss der Samba-Dienst neugestartet werden.

2.7.3.2. Linux Mail Security Gateway

Das Linux Mail Security Gateway ist als **optionales Modul** verfügbar.

Das Modul Linux Mail Security Gateway (Sendmail/Postfix) wurde als Plugin für das Amavis-Plugin-Framework entwickelt. Das Linux Mail Security Gateway benötigt Amavis 2.8.0 oder neuer und altermime. Wenn Amavis auf dem System nicht vorhanden ist, wird es automatisch mitinstalliert. Folgende Konfigurationsschritte sind erforderlich:

1. Ein funktionsfähiger Sendmail/Postfix-Mail-Server wird vorausgesetzt.
2. Stellen Sie sicher, dass der jeweilige Mail-Server die E-Mail-Nachrichten an Amavis weiterleitet. Mehr Informationen hierzu finden Sie in der Dokumentation von Amavis bzw. vom Mail-Server.
3. Vergewissern Sie sich, dass das Überprüfen von Nachrichten auf Spam und Viren in der Amavis-Konfiguration aktiviert wurde. Mehr Informationen hierzu finden Sie in der Amavis-Dokumentation.
4. Öffnen Sie die Konfigurationsdatei /etc/gdata/amavis/mms.cfg und stellen Sie sicher, dass unter *localDomains* die (Sub-)Domäne des Mail-Servers eingetragen ist (z. B. *mail.domain.de*).

Die Verwendung einer schon vorhandenen Amavis-Installation wird nicht empfohlen, da dies unmittelbar nach der Installation vom Linux Mail Security Gateway einen erheblichen manuellen Konfigurationsaufwand erfordert.

Nach der erfolgreichen Konfiguration überprüft das Linux Mail Security Gateway den E-Mail-Verkehr automatisch und benachrichtigt beim Virenfund den ManagementServer. Die Einstellungen können im G DATA Administrator im **Sendmail/Postfix**-Modul konfiguriert werden.

> Achtung: Wenn Sie eine Amavis-Version älter als 2.10.0 verwenden, ist die Funktionalität des Sendmail/Postfix-Moduls nur eingeschränkt verfügbar. Aktualisieren Sie Amavis auf Version 2.10.0 oder neuer, bevor Sie das Sendmail/Postfix-Modul installieren.

2.7.3.3. Linux Web Security Gateway

Das Linux Web Security Gateway ist als **optionales Modul** verfügbar.

Wenn Sie das Zusatzmodul Linux Web Security Gateway (Squid) auswählen, wird auch Squid selbst automatisch mit G DATA Security Client für Linux installiert. Wenn Squid schon auf dem Client vorhanden ist, wird die alte Version vorab automatisch deinstalliert.

Nach der Installation müssen Sie auf den Clients, für die der Verkehr von Squid gefiltert werden soll, die IP-Adresse oder den Hostnamen des Squid-Servers als Proxy-Server konfigurieren (Port 3128). Um die Prüfung von HTTPS-Verkehr zu ermöglichen, definieren Sie zusätzlich einen HTTPS-Proxy-Server mit der Squid-IP-Adresse oder dem Squid-Hostnamen und dem Port 6789. Die dafür notwendigen SSL-Zertifikate liegen auf dem Squid-Server unter /etc/gdata/ssl und müssen auf den Clients importiert

werden. Wenn Sie eigene SSL-Zertifikate verwenden, müssen Sie diese auf dem Server unter /etc/gdata/ssl hinterlegen.

> Achtung: Bei der Installation des Squid-Servers wird das von der jeweiligen Linux-Distribution bereitgestellten Squid-Paket installiert. Wenn diese Squid-Version älter als 3.3.8 ist, ist keine HTTPS-Prüfung verfügbar.

Nach der erfolgreichen Konfiguration vergleicht das Linux Web Security Gateway den Verkehr automatisch mit einer Blacklist und benachrichtigt beim Virenfund den ManagementServer. Die Einstellungen können im G DATA Administrator im **Squid**-Modul konfiguriert werden.

2.8. Installation des G DATA Security Clients für Mac

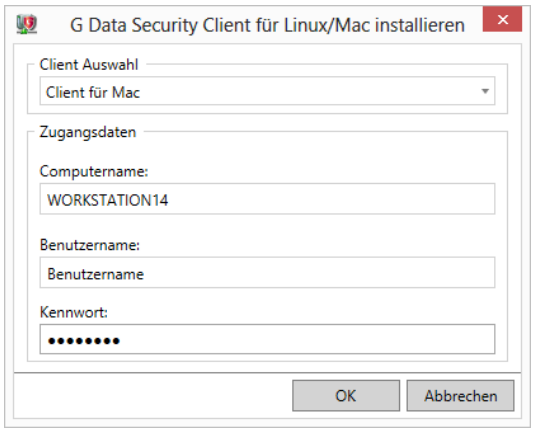
G DATA Security Client für Mac ermöglicht zentral verwalteten Malware-Schutz und wird vom G DATA ManagementServer gesteuert und automatisch mit Virensignaturupdates versorgt. Die Konfiguration erfolgt über G DATA Administrator.

Analog zu Windows- und Linux-Clients können Sie die Installation der Client-Software über eine **Remote-Installation** (über den G DATA Administrator) oder über eine **lokale Installation** (per Installationsskript) durchführen.

2.8.1. Remote-Installation

Die bequemste Installationsmethode für G DATA Security Client für Mac ist die Remote-Installation über G DATA Administrator. Die **Voraussetzungen** und Vorgehensweise sind nahezu identisch zu den für den Linux-Client:

1. Wählen Sie im Aufgabenbereich **Clients** einen Mac-Client aus und klicken Sie im Menü **Clients** auf **G DATA Security Client für Linux/Mac installieren**.
2. Wählen Sie den Clienttyp **Client für Mac** aus.
3. Geben Sie einen **Benutzernamen** und ein **Kennwort** ein. Das Konto muss über Root-Berechtigungen verfügen.
4. Drücken Sie nun auf die **OK**-Schaltfläche. Der Installationsvorgang wird in der **Installationsübersicht** gezeigt.



2.8.2. Lokale Installation

Wenn eine **Remote-Installation** nicht möglich ist, können Sie G DATA Security Client für Mac auch direkt auf dem Client installieren.

1. Wählen Sie im G DATA Administrator den **Clients**-Bereich aus und klicken Sie im Menü

Organisation auf **Installationsskript für Linux/Mac-Clients erstellen**.

2. Nachdem Sie einen Speicherort ausgewählt haben, wird das Installationsskript im Hintergrund erstellt.
3. Kopieren Sie das Installationsskript in einen beliebigen Ordner auf dem Client.
4. Öffnen Sie ein Terminal-Fenster und aktivieren Sie die Root-Rechte, indem Sie das Kommando *su* und danach das Root-Kennwort eingeben. Alternativ führen Sie das Kommando in Schritt 5 über *sudo* aus.
5. Öffnen Sie den Ordner, in dem sich die kopierte Datei befindet, und starten Sie den Installer mit dem Kommando *./install-client.sh -t WS*.
6. Um unberechtigten Zugriff auf den ManagementServer zu vermeiden, müssen Sie Clients, die mit Hilfe des Installationsskripts installiert werden, im G DATA Administrator autorisieren, bevor sie vollständig verwaltet werden können (siehe **Clients** > **Übersicht**).

2.9. Installation der G DATA Exchange Mail Security/MailSecurity MailGateway

Die Konfigurationsart der MailSecurity ist abhängig von dem Mail-Server, der im Netzwerk verwendet wird. In Netzwerken, in denen ein Microsoft Exchange Server 2007 SP1/2010/2013/2016 benutzt wird, kann MailSecurity als Exchange-Plugin installiert werden. Die Exchange Mail Security meldet sich dann bei einem ManagementServer an und kann vom G DATA Administrator verwaltet werden. Die selbständige Gateway-Lösung MailSecurity MailGateway kann mit allen Mail-Servern kombiniert werden. Diese wird vom G DATA MailSecurity Administrator verwaltet.

2.9.1. Exchange Mail Security

Der Installations-Assistent der Exchange Mail Security fügt Microsoft Exchange Server 2007 SP1/2010/2013/2016 ein Plugin hinzu. Das Plugin sollte auf allen Exchange-Servern, die die Mailbox-Rolle oder Hub Transport-Rolle ausführen, installiert werden.

Zur Installation der G DATA Exchange Mail Security legen Sie das G DATA-Installationsmedium ein, wählen Sie **G DATA MailSecurity für Exchange** aus und folgen Sie den Hinweisen des Installations-Assistenten. Das Plugin wird über den G DATA ManagementServer gesteuert. Installieren Sie deswegen zuerst den ManagementServer, bevor Sie G DATA Exchange Mail Security installieren. Die Einstellungen für Exchange Mail Security finden Sie nach der Installation des Plugins im G DATA Administrator auf der Registerkarte **Exchange-Einstellungen**.

Um unberechtigten Zugriff auf den ManagementServer zu vermeiden, müssen Sie Exchange-Clients, die mit Hilfe des Installationsmediums installiert werden, im G DATA Administrator autorisieren, bevor sie vollständig verwaltet werden können (siehe **Clients** > **Übersicht**).

2.9.2. MailSecurity MailGateway

G DATA MailSecurity MailGateway kann auf einem dedizierten Server oder auf dem bestehenden Mail-Server installiert werden. Bei der Installation sind verschiedene Konfigurationen möglich - je nachdem, wo im Netzwerk die Installation erfolgt. Generell sollte sich das MailGateway am besten direkt hinter Ihrer Netzwerk-Firewall befinden (soweit vorhanden), d.h. dass der SMTP/POP3-Datenstrom aus dem Internet über die Firewall direkt zum MailGateway geleitet und von dort weiter verteilt wird.

Zur Installation des MailGateways legen Sie das MailSecurity-Installationsmedium ein und drücken Sie

die Schaltfläche **Installieren**. Wählen Sie anschließend unter **Mail Gateway** die Komponente **MailSecurity** aus und folgen Sie den Hinweisen des Installations-Assistenten.

Wenn Sie die Komponenten für die statistische Auswertung installieren, bekommt der G DATA MailSecurity Administrator im **Status**-Bereich eine **Statistik**-Schaltfläche hinzugefügt. Hierüber können Sie sich statistische Informationen über den Mailserver anzeigen lassen. Die Anzeige dieser Statistik kann über **Optionen** > **Logging** konfiguriert werden.

In allen Fällen sollten direkt nach der Installation mehrere Optionen (IP-Adressen, Ports) konfiguriert werden, sowohl auf dem Rechner, auf dem MailGateway installiert wurde, als auch auf dem Mail-Server. Beispielhafte Port-Konfigurationen für verschiedene Einsatzszenarien finden Sie im Reference Guide.

Je nachdem, wie Ihr Netzwerk aufgebaut ist, kann MailGateway an verschiedenen Knotenpunkten zugreifen, um Mails auf Virenbefall und Spam zu überprüfen:

- Wenn Sie Ihre Mails über einen externen Server als POP3-Mails bekommen, kann MailGateway eingreifen, um die POP3-Mails vor dem Öffnen durch den Empfänger auf Virenbefall zu überprüfen. Hierzu steht Ihnen die Funktion **Optionen** > **Eingehend (POP3)** zur Verfügung.
- Wenn Sie im Netzwerk einen SMTP-Server verwenden, kann MailGateway eingehende Mails schon überprüfen, bevor sie den Mail-Server erreichen. Hierzu steht Ihnen die Funktion **Optionen** > **Eingehend (SMTP)** zur Verfügung.
- MailGateway kann auch all Ihre ausgehenden Mails vor dem Versand auf Virenbefall überprüfen. Hier steht Ihnen die Funktion **Optionen** > **Ausgehend (SMTP)** zur Verfügung.

2.10. Installation der G DATA Internet Security für Android

Um von den Möglichkeiten des G DATA Mobile Device Management Gebrauch zu machen, können Sie eine auf Business-Belange ausgelegte Spezialversion der G DATA Internet Security auf Ihren Android-Geräten installieren. Der G DATA Administrator bietet dabei Installationsmöglichkeiten für Android-Clients im **Clients**-Bereich. Wählen Sie einen oder mehrere Android-Clients und klicken Sie auf die Schaltfläche **Installationslink an mobile Clients senden**, um eine Mail an die jeweiligen Android-Geräte zu versenden. In dieser Mail befindet sich ein Download-Link für die Internet Security App.

Nach dem Versand können Sie oder Ihre Mitarbeiter die Mail auf dem mobilen Gerät öffnen und durch Antippen des Download-Links die APK-Datei installieren. Bitte beachten Sie, dass die Option **Unbekannte Herkunft (Installation von Nicht-Market-Apps zulassen)** aktiviert sein muss, damit die Datei installiert werden kann. Diese Option finden Sie normalerweise im Android-System-Menü unter **Einstellungen** > **Sicherheit** > **Geräteverwaltung**. Nach dem Öffnen der APK-Datei und dem Bestätigen der benötigten Berechtigungen wird die G DATA Internet Security installiert und kann aus dem Android-App-Menü heraus gestartet werden.

Um die Installation abzuschließen, muss die Fernadministration erlaubt werden. Die Mail enthält einen Link, über den Sie die Einstellungen automatisch konfigurieren lassen können. Alternativ können Sie die Einstellungen manuell konfigurieren. Wählen Sie hierzu unter **Einstellungen** > **Allgemein** den Eintrag **Fernadministration gestatten** aus und geben Sie den Namen oder die IP-Adresse des ManagementServers unter **Serveradresse** ein. Unter **Gerätename** können Sie nun für das Android-Gerät einen Namen zuweisen, unter dem dieses im G DATA Administrator ermittelt werden kann. Bei **Passwort** sollten Sie das Passwort eintragen, welches Sie auch beim G DATA Administrator eingetragen haben (dieses Passwort ist auch in der Mail angegeben, die Ihnen mit dem Download-Link ans Android-Gerät geschickt wurde).

Das Gerät wird nun neben den anderen Clients im **Clients**-Bereich des G DATA Administrators angezeigt und kann von dort aus administriert werden. Sollte das Gerät nicht automatisch in dieser Liste erscheinen, rebooten Sie bitte das Gerät, um das Einchecken beim G DATA ManagementServer zu forcieren.

3. G DATA ManagementServer

Der G DATA ManagementServer ist das Herzstück der G DATA-Architektur: Er verwaltet die Clients, fordert neueste Software- und Virensignaturupdates automatisch von den G DATA Update-Servern an und steuert den Virenschutz im Netzwerk. Zur Kommunikation mit den Clients nutzt der G DATA ManagementServer das TCP/IP-Protokoll. Für Clients, die vorrübergehend keine Verbindung zum G DATA ManagementServer haben, werden die Jobs automatisch gesammelt und beim nächsten Kontakt zwischen G DATA Security Client und G DATA ManagementServer synchronisiert. Der G DATA ManagementServer verfügt über einen zentralen Quarantäne-Ordner. In diesem können verdächtige Dateien verschlüsselt sichergestellt, gelöscht, desinfiziert oder gegebenenfalls an die G DATA SecurityLabs weitergeleitet werden. Der G DATA ManagementServer wird über den **G DATA Administrator** gesteuert.

> Wenn Sie den G DATA Administrator beenden, bleibt der G DATA ManagementServer weiterhin im Hintergrund aktiv und steuert die Prozesse, die von Ihnen für die Clients konfiguriert wurden.

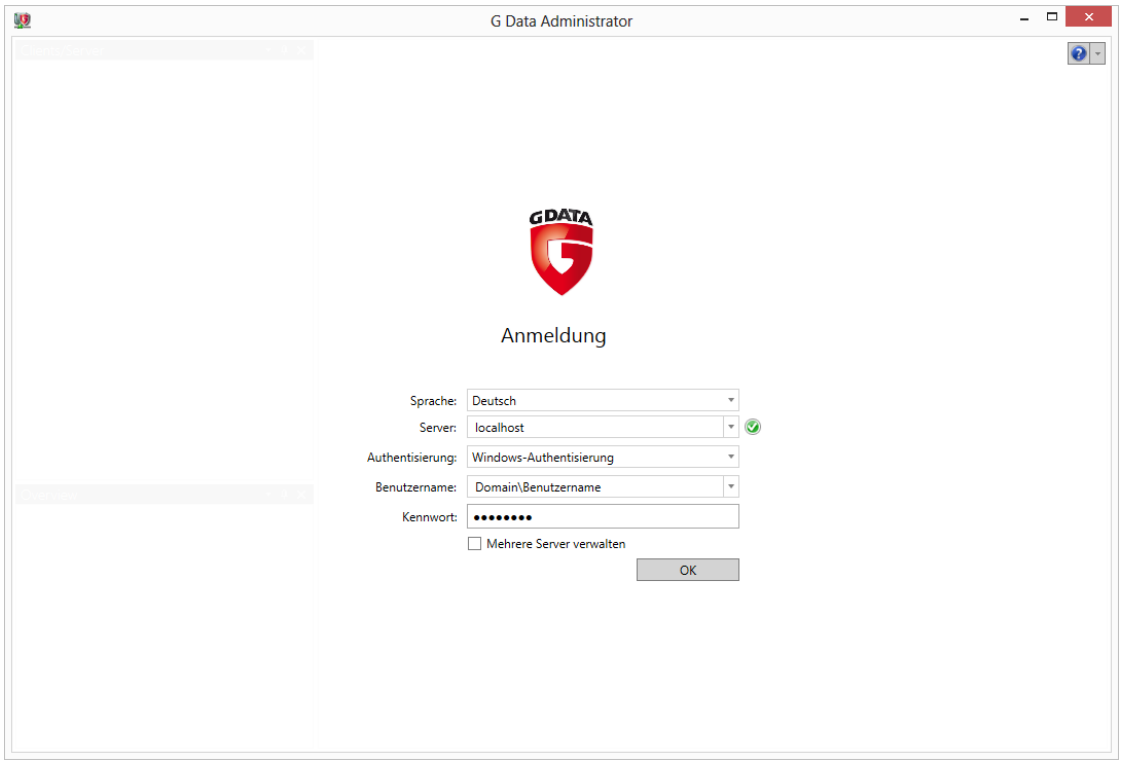
4. G DATA Administrator

Der G DATA Administrator ist die Steuerungssoftware für den G DATA ManagementServer, die die Verwaltung von Einstellungen und Updates für alle G DATA-Clients und -Server im Netzwerk ermöglicht. Der G DATA Administrator ist passwortgeschützt und kann auf jedem Windows-Rechner innerhalb des Netzwerkes installiert und gestartet werden.

Nachdem Sie den G DATA Administrator zum ersten Mal gestartet haben, ist es empfehlenswert, den **Server-Einrichtungsassistenten** auszuführen. So können Sie bequem die wichtigsten Einstellungen des Administrators und ManagementServers für Ihr Netzwerk optimieren.

4.1. Starten des G DATA Administrators

G DATA Administrator wird mit einem Klick auf den Eintrag **G DATA Administrator** in der Programmgruppe **Start** > **(Alle) Programme** > **G DATA** > **G DATA Administrator** des Startmenüs aufgerufen. Geben Sie im Anmeldungsfenster Ihre Zugangsdaten ein:



- **Sprache**: Wählen Sie die Anzeigesprache.
- **Server**: Geben Sie den Namen des Computers ein, auf dem der ManagementServer installiert wurde. Die Anzeige rechts vom Eingabefeld zeigt, ob der angegebene ManagementServer bereit ist. Falls ein Fehler auftritt, können Sie auf die Anzeige klicken um so das Protokoll aufzurufen.
- **Authentisierung**
  - **Windows-Authentisierung**: Wenn Sie diese Authentisierungsvariante wählen, können Sie sich mit dem Benutzernamen und Passwort Ihres Windows-Administrator-Zugangs auf dem G DATA ManagementServer einloggen.
  - **Integrierte Authentisierung**: Sie können sich über ein im G DATA ManagementServer integriertes Authentisierungssystem einloggen. Integrierte Accounts können über die Funktion **Benutzerverwaltung** angelegt werden.
- **Benutzername**: Geben Sie Ihren Windows-Administrator-Benutzernamen oder Ihren Benutzernamen der integrierten Authentisierung ein.

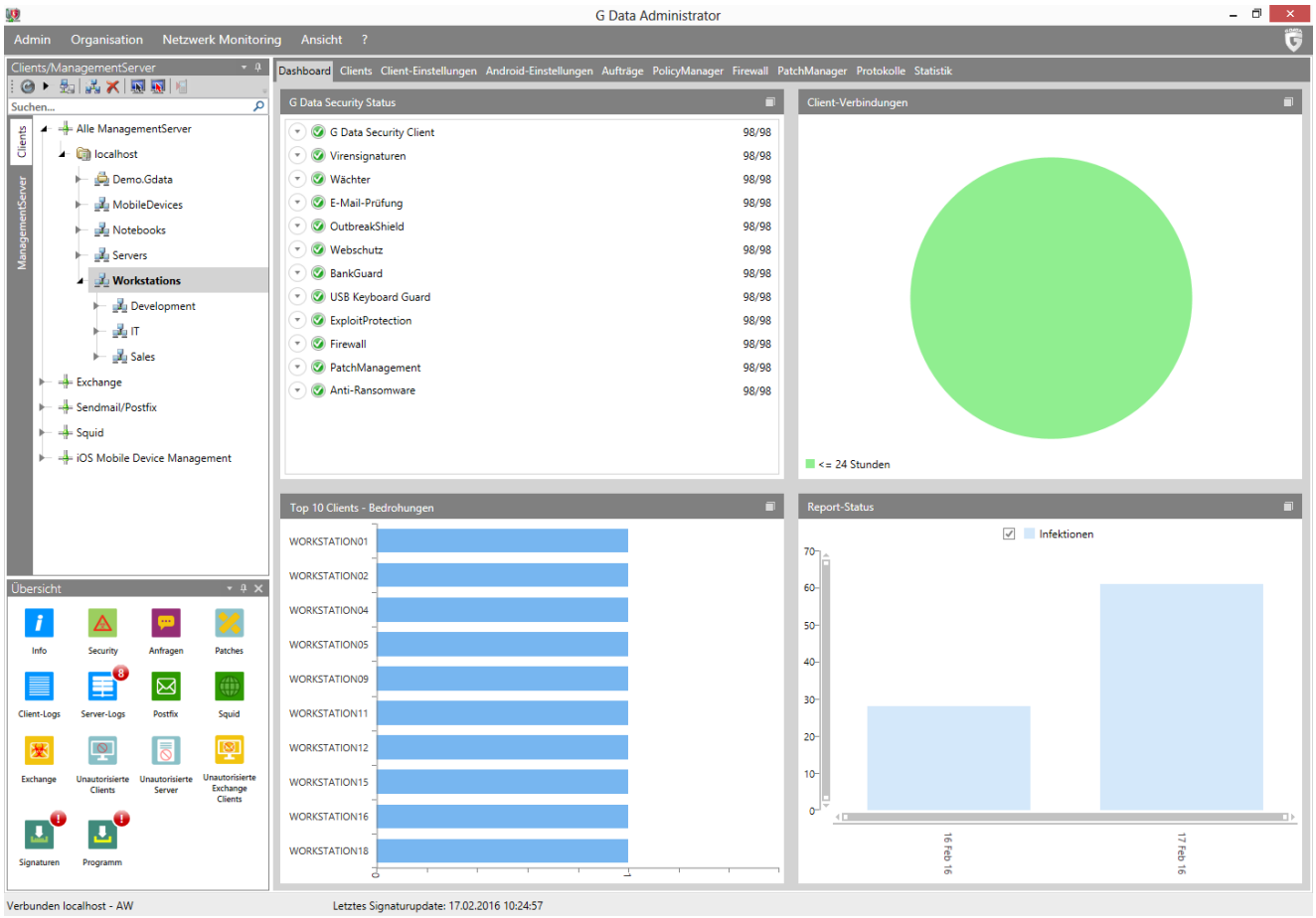
- **Kennwort**: Geben Sie Ihr Windows-Administrator-Kennwort oder Ihr Kennwort der integrierten Authentisierung ein.

Klicken Sie auf **OK**, um sich anzumelden.

Klicken Sie auf den Pfeil neben dem Fragezeichen, um ein Menü mit weiteren Optionen zu öffnen. Die Funktion **Über G DATA Administrator** zeigt die Versionsinformationen. **Einstellungen zurücksetzen** ermöglicht es Ihnen, die Ansichtseinstellungen des G DATA Administrators zurück zu setzen (z. B. Fenstergröße).

4.2. Verwendung des G DATA Administrators

Die Oberfläche des G DATA Administrators ist in vier Bereiche untergliedert.

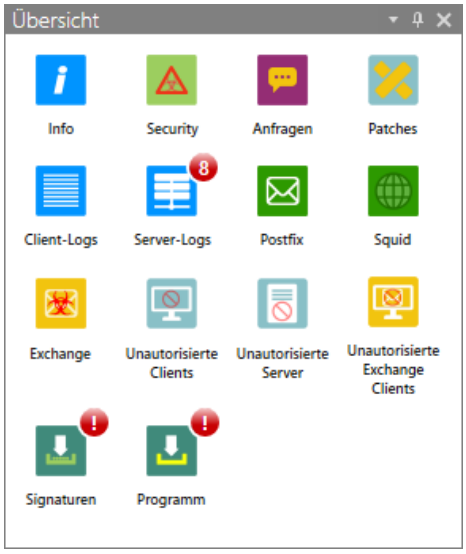


- Der Bereich **Übersicht** zeigt allgemeine Statusinformationen und Verknüpfungen zu Bereichen wie Berichten, Protokollen und Updates.
- Der **Clients/ManagementServer**-Bereich zeigt alle Clients und ManagementServer, die vom G DATA Administrator verwaltet werden.
- Auf der rechten Seite kann über Karteireiter in die jeweiligen **Module** gewechselt werden. Welche Module angezeigt werden, hängt von den von Ihnen selektierten **Clients/ManagementServern** sowie von der gewählten **Lösung** ab.
- Die Menüleiste zeigt globale Funktionen, die in allen Modulen verwendet werden können, sowie Sonderfunktionen für ausgewählte Module:
  - **Admin**: **Server-Einrichtungsassistent** starten oder G DATA Administrator beenden.
  - **Organisation** (siehe **Clients/ManagementServer** > **Clients** > **Organisation**)
  - **Clients** (siehe **Clients** > **Übersicht**)
  - **Aufträge** (siehe **Aufträge**)

- **Firewall** (siehe **Firewall** > **Übersicht**)
- **Sicherheitsereignisse** (siehe **Protokolle** > **Sicherheitsereignisse**)
- **Netzwerk Monitoring**: Öffnet das **G DATA ActionCenter**, um das optionale **Modul** Netzwerk Monitoring zu verwenden.
- **Ansicht**: **Übersicht** ein- oder ausblenden.
- **?**: Hilfe-Datei oder Versionsinformationen anzeigen.

4.2.1. Übersicht

Der Bereich Übersicht zeigt auf einen Blick ungelesene Berichte, Protokolle und andere Status-Informationen. Wenn Sie auf eins der Symbole klicken, öffnet sich das jeweilige Modul mit voreingestellten Filtern, damit nur die gewünschten Informationen angezeigt werden. Die Verfügbarkeit der Symbole hängt von Ihrer **Lösung** ab.



- **Info**: Allgemeine Informationen und Fehlerberichte.
- **Security**: Infektionsberichte.
- **Anfragen**: Anfragen von den Modulen PolicyManager, PatchManager und Firewall sowie von der Android-App-Kontrolle.
- **Patches**: Patches mit hoher Priorität, die noch nicht verteilt wurden.
- **Client-Logs**: Client-Protokolle, wie z. B. geänderte Einstellungen und Statusinformationen für Scanaufträge.
- **Server-Logs**: ManagementServer-Protokolle und Fehlerberichte.
- **Postfix**: Berichte des Sendmail/Postfix-Moduls.
- **Squid**: Berichte des Squid-Moduls.
- **Exchange**: Berichte der MailSecurity für Exchange.
- **Unautorisierte Clients**: Clients, die sich mit dem ManagementServer verbunden haben, aber noch nicht vom Administrator autorisiert wurden.
- **Unautorisierte Server**: Subnet-Server, die sich mit dem ManagementServer verbunden haben, aber noch nicht vom Administrator autorisiert wurden.
- **Unautorisierte Exchange Clients**: Exchange-Clients, die sich mit dem ManagementServer verbunden haben, aber noch nicht vom Administrator autorisiert wurden.
- **Signaturen**: Versionsinformationen für die Virensignaturen auf dem ManagementServer.

- **Programm**: Versionsinformationen für den ManagementServer.

4.2.2. Clients/ManagementServer

Im Clients/ManagementServer-Bereich werden alle Clients und ManagementServer, die vom G DATA Administrator verwaltet werden, angezeigt. Wählen Sie die Registerkarte **Clients**, um Clients anzuzeigen oder die Registerkarte **ManagementServer**, um ManagementServer (Haupt-, Secondary- und Subnet-Server) anzuzeigen.

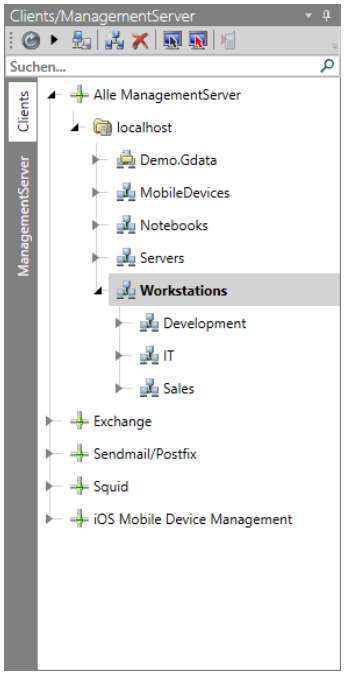
Clients und ManagementServer werden in einer gegliederten Liste angezeigt. Wie im Windows Explorer erscheinen Knoten, in denen sich Untergliederungen befinden, mit einem kleinen Plus-Symbol. Wenn Sie dieses anklicken, öffnet sich die Verzeichnisstruktur an dieser Stelle und ermöglicht die Ansicht der darunter befindlichen Knoten. Ein Klick auf das Minus-Symbol schließt diese Untergliederung wieder.

In der Symbolleiste sehen Sie die wichtigsten Client- und Server-Management-Befehle, von denen einige auch im Menü **Organisation** angezeigt werden. Die Verfügbarkeit der Befehle hängt von den ausgewählten Clients/ManagementServern ab:

- **Aktualisieren**
- **Alle erweitern/reduzieren**: Erweitern oder reduzieren Sie alle Knoten in der Liste.
- **Deaktivierte Clients anzeigen**
- **Neue Gruppe anlegen**
- **Löschen**
- **Client aktivieren**: Hiermit fügen Sie der Clients-Registerkarte einen Windows- oder Linux-Client hinzu, indem Sie den Namen oder die IP-Adresse des Clients eingeben.
- **Installationsübersicht**
- **Installationslink an mobile Clients senden**: Hiermit senden Sie Android- und iOS-Clients einen Installationslink.

4.2.2.1. Clients

Die Clients-Ansicht zeigt die verschiedenen Client-Typen unter fünf Hauptknoten.



- **Alle ManagementServer**: Windows-, Linux-, Mac- und Android-Clients.
- **Exchange**: MailSecurity für Exchange-Clients.
- **Sendmail/Postfix**: Linux-Clients mit dem Sendmail/Postfix-Modul.
- **Squid**: Linux-Clients mit dem Squid-Modul.
- **iOS Mobile Device Management**: iOS-Clients.

Bevor Clients verwaltet werden können, müssen diese zum Clients-Bereich hinzugefügt und installiert werden. Es gibt mehrere Möglichkeiten zum Hinzufügen, abhängig von Client-Typ und Größe bzw. Konfiguration des Netzwerks:

- Windows: Benutzen Sie den **Server-Einrichtungsassistenten**, das **Computer suchen**-Fenster, die **Client aktivieren**-Option in der Symbolleiste oder die **Active Directory**-Unterstützung um Windows-Clients hinzuzufügen. Starten Sie danach die **Installation des G DATA Security Clients**.
- Linux: Benutzen Sie die **Client aktivieren**-Option in der Symbolleiste um Linux-Clients hinzuzufügen. Starten Sie danach die **Installation des G DATA Security Clients für Linux**.
- Mac: Benutzen Sie die **Client aktivieren**-Option in der Symbolleiste um Mac-Clients hinzuzufügen. Starten Sie danach die **Installation des G DATA Security Clients für Mac**.
- MailSecurity für Exchange: Starten Sie die **Installation der G DATA MailSecurity für Exchange**. Der Exchange-Client wird im Anschluss automatisch hinzugefügt.
- Android: Benutzen Sie die Option **Installationslink an mobile Clients senden** in der Symbolleiste um dem Client oder den Clients eine E-Mail zu schicken. Dies startet die **Installation der G DATA Internet Security für Android**. Der Android-Client wird unmittelbar danach automatisch hinzugefügt.
- iOS: Geben Sie Ihre Zugangsdaten für G DATA ActionCenter im Modul **ActionCenter** ein. Benutzen Sie danach die Option **Installationslink an mobile Clients senden** in der Symbolleiste um dem Client oder den Clients eine E-Mail zu schicken. Nachdem der Benutzer die Geräteverwaltung bestätigt hat, wird der iOS-Client automatisch hinzugefügt.

Im Clients-Bereich werden die folgenden Symbole angezeigt:

 Hauptknoten
 ManagementServer
 Gruppe
 Gruppe (Active Directory)
 Client
 Client (deaktiviert)
 Laptop-Client
 Mobile-Client
 Linux-Server
 Linux-Client
 MailSecurity für Exchange-Client
 Nicht auswählbare Geräte: Hierunter fallen z. B. Netzwerkdrucker

Wenn Sie einen Client, eine Gruppe oder einen ManagementServer ausgewählt haben, werden die

relevanten **Client-Module** im **Modulbereich** angezeigt. Abhängig vom ausgewählten Knoten, ändert sich die Auswahl der Module. Zum Beispiel können Sie für PCs den Eintrag **Client-Einstellungen** aufrufen. Bei Android-Clients können Sie hingegen die **Android-Einstellungen** aufrufen.

Im Clients-Bereich können Sie bequem Einstellungen importieren und exportieren. Klicken Sie mit der rechten Maustaste auf einen Client und wählen Sie **Einstellungen exportieren**, um die Client- und PolicyManager-Einstellungen in einer .dbdat-Datei zu speichern. Um Einstellungen zu importieren, klicken Sie mit der rechten Maustaste auf einen Client oder eine Gruppe, wählen Sie **Einstellungen importieren** und selektieren Sie die gewünschten Einstellungsgruppen und die .dbdat-Datei.

Organisation

Wenn Sie die Registerkarte Clients gewählt haben, wird das Menü Organisation in der Menüleiste eingeblendet. Das Menü bietet schnellen Zugriff auf Einstellungen der Client-Organisation.

Aktualisieren

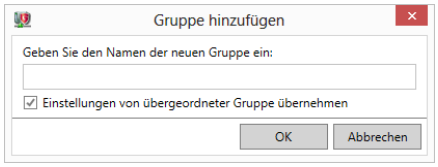
Die Option Aktualisieren aktualisiert die Liste im Bereich Clients/ManagementServer.

Deaktivierte Clients anzeigen

Clients, die nicht aktiviert sind, können über diese Funktion sichtbar gemacht werden. Deaktivierte Clients werden dabei als durchscheinende Symbole dargestellt.

Gruppe hinzufügen

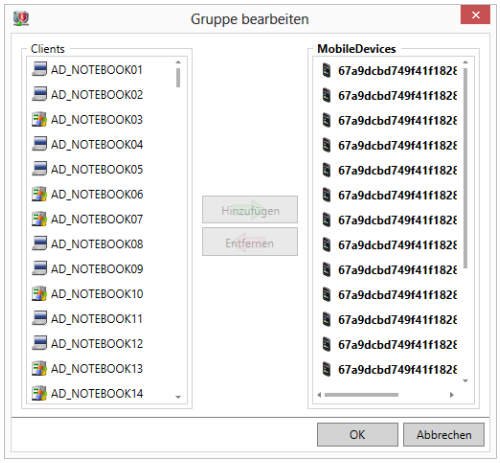
Über diesen Befehl lässt sich eine Gruppe anlegen. Damit lassen sich leicht unterschiedliche Sicherheitszonen definieren, da alle Einstellungen sowohl für einzelne Clients als auch für komplette Gruppen durchgeführt werden können. Wählen Sie einen ManagementServer oder eine Gruppe und klicken Sie auf **Gruppe hinzufügen**. Nach der Vergabe eines Gruppennamens können Clients der neuen Gruppe zugeordnet werden, indem man in der Clientliste den gewünschten Client mit der Maus per Drag&Drop auf die entsprechende Gruppe zieht.



Um eine große Anzahl von Clients in einer Gruppe zu bewegen, verwenden Sie das Modul **Clients** > **Übersicht**. Wählen Sie die Clients, die verschoben werden sollen, drücken Sie die rechte Maustaste und wählen Sie **Clients verschieben**.

Gruppe bearbeiten

Diese Option öffnet eine Dialogbox, in der sich über die Tasten **Hinzufügen** und **Entfernen** Clients zur Gruppe hinzufügen oder aus der Gruppe entfernen lassen. Nur verfügbar, wenn im Clients-Bereich eine Gruppe angewählt ist.



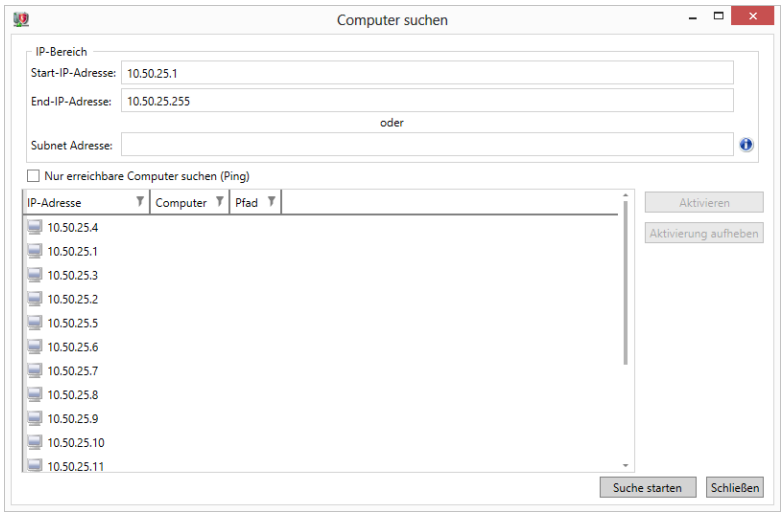
Entfernen

Einzelne Clients lassen sich mit dem Befehl Löschen aus der Clientliste entfernen. Durch das Entfernen des Clients aus der Liste wird der G DATA Security Client nicht deinstalliert.

> Um eine Gruppe zu löschen, müssen alle in ihr enthaltenen Clients nach Bedarf entweder deaktiviert oder in andere Gruppen verschoben werden. Nur leere Gruppen können gelöscht werden.

Computer suchen

Das Computer suchen-Fenster kann dazu verwendet werden, Clients zum Clients-Bereich hinzuzufügen und zu aktivieren. Clients können direkt aus dem Dialogfenster heraus über die IP-Adresse gefunden und aktiviert werden.



Über das Computer suchen-Fenster können alle Computer in einem bestimmten IP-Bereich kontaktiert werden. Der Bereich kann über eine **Start-IP-Adresse** und eine **End-IP-Adresse** (z. B. 192.168.0.1 und 192.168.0.255) oder die **Subnet-Adresse** (CIDR-Notation, z. B. 192.168.0.0/24) definiert werden. Um sicherzustellen, dass nur verfügbare Clients aufgelistet werden, wählen Sie die Option **Nur erreichbare Computer suchen (Ping)**. Klicken Sie auf **Suche starten**, um die Suche im Netzwerk zu beginnen. Computer werden nun aufgelistet, sobald sie gefunden werden. Wenn der Suchvorgang zu lange dauert, können Sie die Suche abbrechen durch Anklicken von **Suche abbrechen**.

Alle Computer, die auf den IP-Check antworten, werden nun aufgelistet, einschließlich ihrer IP-Adresse und dem Namen des Computers. Mit der Schaltfläche **Aktivieren** können die jeweiligen Clients dem Clients-Bereich hinzugefügt werden. Im Suchergebnis können aktivierte Clients durch Anklicken von **Aktivierung aufheben** auch deaktiviert werden.

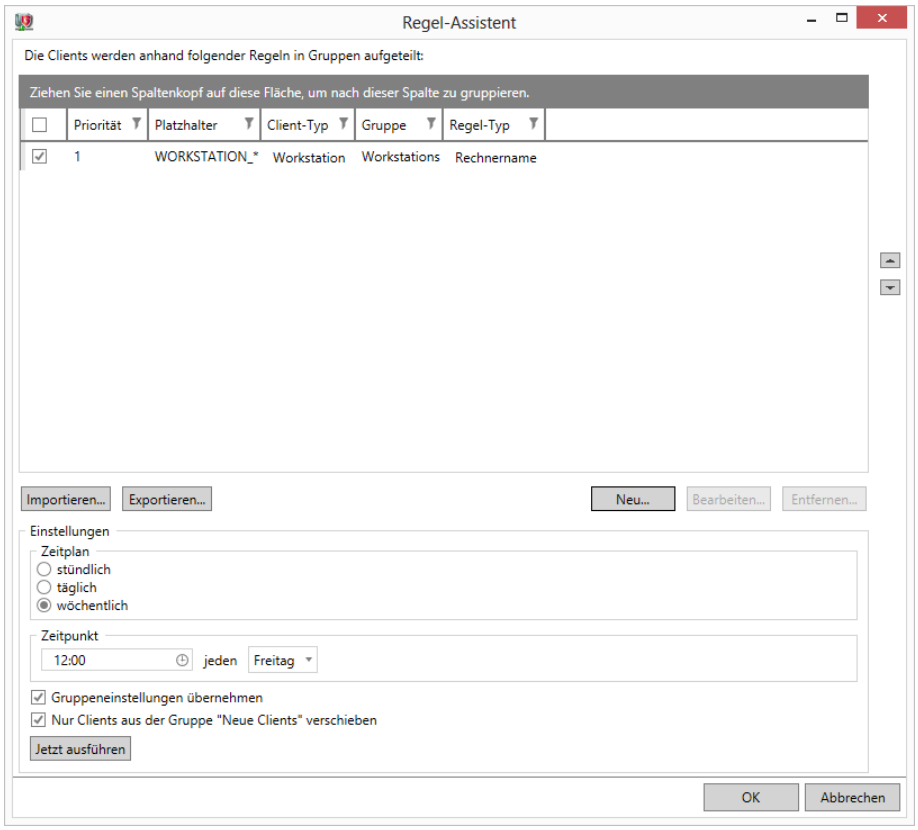
Regel-Assistent

Wenn Clients sich zum ersten Mal mit dem ManagementServer verbinden, werden sie automatisch der Gruppe **Neue Clients** zugeordnet, falls beim Aktivieren des Clients oder beim Anlegen des Installationspakets keine Gruppe definiert wurde. Mit dem Regel-Assistenten können Regeln angelegt werden, die die neuen Clients regelmäßig in voreingestellte Gruppen verschieben.

Die Regeln können mit Hilfe der Schaltflächen **Neu**, **Bearbeiten** und **Entfernen** sowie mit den Pfeilen auf der rechten Seite verwaltet werden. Über die Schaltflächen **Importieren** und **Exportieren** können Sie die Regeln als .json-Datei importieren und exportieren.

Unter Einstellungen definieren Sie die allgemeinen Einstellungen für das Ausführen der Regeln:

- **Zeitplan**: Die Regeln werden **Stündlich**, **Täglich** oder **Wöchentlich** ausgeführt.
- **Zeitpunkt**: Legen Sie den genauen Zeitpunkt der Ausführung fest.
- **Gruppeneinstellungen übernehmen**: Nachdem sie verschoben werden, bekommen Clients automatisch die Gruppeneinstellungen der Gruppe, in die sie verschoben wurden.
- **Nur Clients aus der Gruppe "Neue Clients" verschieben**: Die Regeln werden nur auf Clients in der Gruppe **Neue Clients** angewendet. Wenn diese Option abgewählt wird, werden die Regeln auf alle Clients angewendet. Dies kann dafür sorgen, dass Clients mehrere Male verschoben werden und sollte deshalb aktiviert bleiben.
- **Jetzt ausführen**: Die Regeln werden sofort ausgeführt.

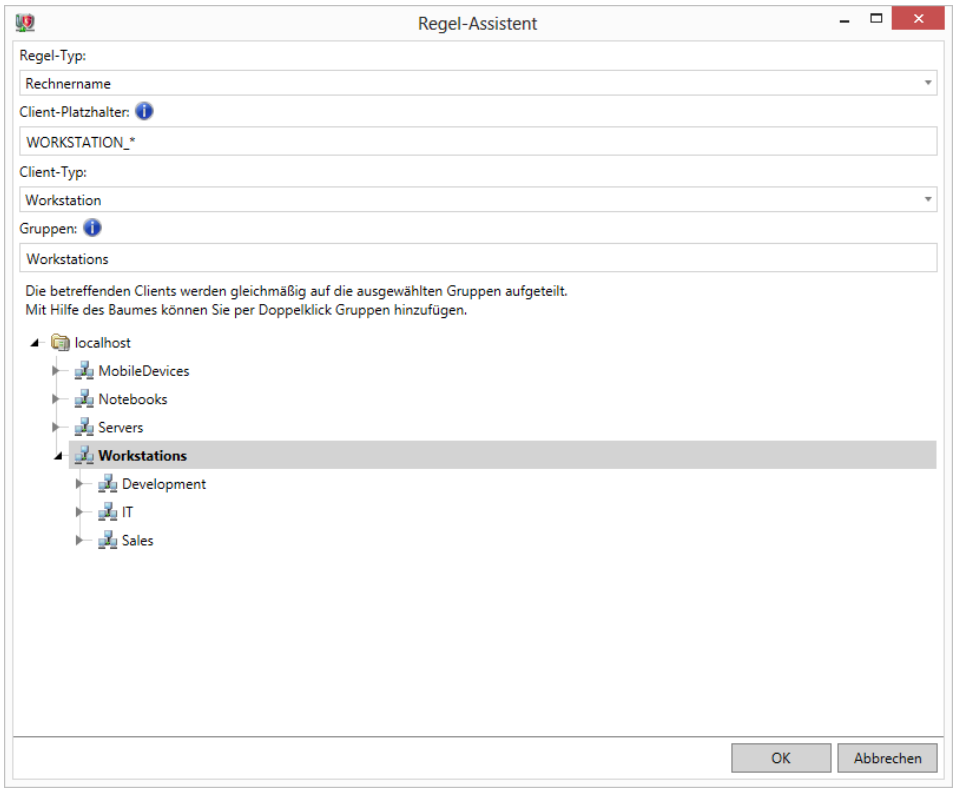


Mit den folgenden Einstellungen können Sie Regeln definieren, um Clients automatisch zu verschieben:

- **Regel-Typ**: Legen Sie fest, ob Clients nach **Rechnername**, **IP-Adresse**, **Domäne** oder **Standardgateway** selektiert werden.
- **Client-Platzhalter**: Geben Sie das Suchmuster ein, mit dem Clients selektiert werden. Sie können Platzhalter verwenden. Zum Beispiel: Geben Sie *Vertrieb_** ein, um alle Clients mit dem

Präfix Vertrieb_ auszuwählen (wenn Sie den Regel-Typ **Rechnername** verwenden) oder *192.168.0.[1-100]*, um alle Clients mit IP-Adressen zwischen 192.168.0.1 und 192.168.0.100 auszuwählen (wenn Sie den Regel-Typ **IP-Adresse** verwenden).

- **Client-Typ**: Legen Sie fest, welche Client-Typen verschoben werden sollen (**Alle**, **Workstation**, **Server**, **Android-Gerät** oder **Laptop**).
- **Gruppen**: Geben Sie einen oder mehrere Gruppen-Namen ein oder wählen Sie in der Baumansicht eine oder mehrere Gruppen per Doppelklick. Wenn Sie mehrere Gruppen auswählen, werden die Clients gleichmäßig auf die ausgewählten Gruppen verteilt.



Installationspaket für Windows-Clients erstellen

Über diese Funktion ist es möglich, ein Installationspaket für den G DATA Security Client zu erstellen. Mit diesem Installationspaket können Sie den G DATA Security Client lokal installieren. Lesen Sie das Kapitel **Installationspaket** für weitere Informationen.

Installationsskript für Linux/Mac-Clients erstellen

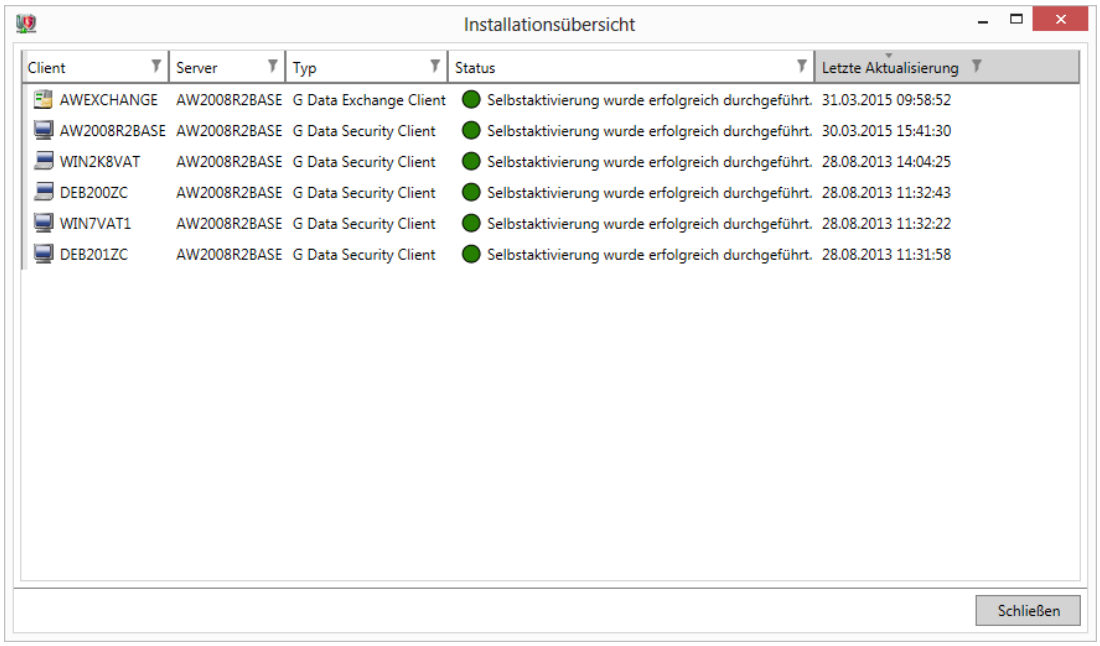
Über diese Funktion ist es möglich, ein Installationsskript für den G DATA Security Client für Linux und den G DATA Security Client für Mac zu erstellen. Mit diesem Installationsskript können Sie den G DATA Security Client lokal installieren. Lesen Sie die Kapitel **Lokale Installation (Linux)** und **Lokale Installation (Mac)** für weitere Informationen.

Installationsübersicht

Um einen Überblick über den Installationsfortschritt zu erhalten, können Sie das Installationsübersichts-Fenster verwenden. Es wird automatisch geöffnet, wenn ein Remote-Installationsauftrag hinzugefügt wird, aber es kann auch über die Installationsübersicht-Schaltfläche in der Menüleiste des Clients/ManagementServer-Bereichs geöffnet werden.

Die Installationsübersicht zeigt alle erledigten und unerledigten Remote-Installationsaufträge an. Die Spalte **Typ** zeigt den Typ der Installation (z. B. G DATA Security Client, G DATA Internet Security für Android oder Subnet-Server). Sobald die Remote-Installation abgeschlossen ist, wird die **Status**-Spalte aktualisiert. Für Clients, die über die **Active Directory-Synchronisation** hinzugefügt wurden,

zeigt die Spalte **Nächster Installationsversuch** den Zeitpunkt, an dem die Remote-Installation gestartet wird.



Weitere Optionen sind verfügbar über das Kontextmenü:

- **Aktualisieren**: Aktualisiert die Liste.
- **Eintrag entfernen**: Löscht den ausgewählten Eintrag.
- **Installationsbericht anzeigen**: Zeigt den Installationsbericht für den ausgewählten Eintrag.
- **Erneut versuchen**: Wiederholt einen fehlgeschlagenen Installationsversuch.

Installationslink an mobile Clients senden

Mit Hilfe von **Installationslink an mobile Clients senden** können Sie mobilen Clients einen Installationslink senden. Abhängig von den Clients, die Sie im Clients-Bereich ausgewählt haben, zeigt das Fenster Optionen für **Android**- oder **iOS**-Geräte.

Wenn der Benutzer die E-Mail-Nachricht auf dem Gerät öffnet, kann er **G DATA Internet Security für Android installieren** (Android) bzw. die Geräteverwaltung aktivieren (iOS). Sobald der jeweilige Ablauf erfolgreich abgeschlossen wird, wird das Gerät im Clients-Bereich angezeigt.

> Stellen Sie sicher, dass G DATA ManagementServer E-Mails verschicken kann, indem Sie unter **Allgemeine Einstellungen** > **E-Mail** > **E-Mail Einstellungen** Ihre Zugangsdaten für einen SMTP-Server eingeben.

Android-Clients

Um Android-Clients einen Installationslink zu senden, geben Sie die folgenden Informationen ein:

- **Kennwort**: Falls Sie unter **Allgemeine Einstellungen** > **Android** > **Authentifizierung für mobile Clients** noch kein Kennwort für die mobile Authentifizierung eingegeben haben, so legen Sie das hier fest.
- **Empfänger**: Geben Sie eine oder mehrere E-Mail-Adressen (getrennt durch Zeilenumbrüche oder Kommata) ein.
- **Betreff**: Geben Sie den Betreff der Installations-E-Mail ein.
- **Inhalt**: Geben Sie den Inhalt der Installations-E-Mail ein. Der Inhalt muss die vordefinierten

Platzhalter für die Download-Links enthalten.

Klicken Sie auf **OK**, um den Installationslink zu senden.

iOS-Clients
Sie können über einige Einstellungen selbst bestimmen, wie die Geräteverwaltungsanfrage an den iOS-Benutzer dargestellt wird:

- **Name**: Geben Sie hier den Geräteverwaltungsnamen ein.
- **Beschreibung**: Geben Sie hier die Geräteverwaltungsbeschreibung ein.
- **Organisation**: Geben Sie den Namen Ihrer Organisation ein.
- **End User License Agreement**: Geben Sie eine End User License Agreement ein.
- **Empfänger**: Geben Sie eine oder mehrere Mail-Adressen (getrennt durch Zeilenumbrüche oder Kommata) ein.

Klicken Sie auf **OK**, um den Link zu senden.

> Bevor Sie einem iOS-Client einen Installationslink senden, sollten Sie sich vergewissern, dass Sie in dem Modul **ActionCenter** Ihre Zugangsdaten für das ActionCenter eingegeben haben.

Active Directory
Über die Active Directory-Integration können alle Computerobjekte der Organisationseinheiten der Domäne importiert werden. Dazu muss eine eigene Gruppe im G DATA Administrator angelegt werden. Nach einem Rechtsklick auf die neu erstellte Gruppe wird der Menüpunkt **Active Directory Eintrag der Gruppe zuordnen** sichtbar. Im Dialogfenster, das sich öffnet, wählen Sie den Punkt **Einer Gruppe im Active Directory zuweisen** aus und geben den LDAP-Server an. Die **Auswahl**-Schaltfläche stellt eine Auswahl verfügbarer Server zur Verfügung. Auch das Verbinden mit einer anderen Domäne ist möglich. Die Option **G DATA Security Client automatisch auf neu hinzugefügten Rechnern installieren** bewirkt dass auf jedem Rechner, der zur Active Directory-Domäne zugefügt wird, sofort der Client installiert wird, sofern er die **Mindestvoraussetzungen** erfüllt. Geben Sie dazu einen Domänen-**Benutzernamen** ein, der über ausreichende Berechtigungen auf den Clients verfügt, sowie das dazugehörige **Kennwort** und die Installations-**Sprache**.

Standardmäßig synchronisiert der G DATA ManagementServer seine Daten alle sechs Stunden mit dem Active-Directory-Server. Dieser Wert kann unter **Allgemeine Einstellungen** > **Synchronisation** geändert werden.

> Änderungen in dem Active Directory werden automatisch mit dem ManagementServer synchronisiert. Wenn Clients allerdings zwischen Domänen verschoben werden, muss die Active-Directory-Verknüpfung zwischen der ManagementServer-Gruppe und der alten Domäne zunächst manuell aufgehoben werden. Nachdem Sie einer ManagementServer-Gruppe eine Active-Directory-Einheit aus der neuen Domäne zugewiesen haben, werden die Clients dann automatisch mit dem richtigen Knoten im **Clients**-Bereich synchronisiert.

4.2.2.2. ManagementServer

Im ManagementServer-Bereich werden die folgenden Server-Symbole angezeigt:

- Hauptknoten
- Haupt-Server
- Secondary-Server

Subnet-Server

Wenn Sie einen Server ausgewählt haben, werden die relevanten **Server-Module** im **Modulbereich** angezeigt.

4.2.3. Module

Abhängig von dem Auswahl im **Clients/ManagementServer**-Bereich werden auf der rechten Seite entweder die **Client**- oder die **Server-Module** als Karteireiter angezeigt. Klicken Sie auf eine Registerkarte um das jeweilige Modul zu öffnen.

Die meisten Module verfügen über eine Symbolleiste. Zusätzlich zu den modulspezifischen Funktionen, stehen meistens die folgenden Schaltflächen zur Verfügung:

- **Aktualisieren**: Aktualisiert die Liste oder Ansicht.
- **Löschen**: Löscht die ausgewählten Einträge.
- **Drucken**: Druckt die ausgewählten Einträge.
- **Seitenansicht**: Zeigt eine Vorschau der zu druckenden Seiten.
- **Zeitraum**: Beschränkt die Ansicht auf einen bestimmten Zeitraum.

Für die meisten Module gibt es darüber hinaus allgemeine Optionen, um das Layout und den Inhalt der Listen im Infobereich zu editieren:

- Klicken Sie zum Sortieren einer Liste auf eine der Spaltenüberschriften.
- Mit einem rechten Mausklick auf die Spaltenüberschriften können Sie weitergehende Informationsspalten zu- oder abwählen.
- Um die Anzahl der Einträge pro Seite zu reduzieren, wählen Sie die maximale **Anzahl pro Seite** am unteren rechten Rand der Programmoberfläche aus.
- Für die Eingabe von Freitext-Filtern klicken Sie auf eine der Filter-Schaltflächen in den Spaltenüberschriften und geben Sie dort Ihre Filterkriterien ein.
- Ziehen Sie eine oder mehrere Spaltenüberschriften auf die Leiste oberhalb der Spaltenüberschriften, um eine Gruppe aus dieser Spalte zu erstellen. Gruppen können in unterschiedlicher Weise und in unterschiedlichen Ansichten erzeugt und verschachtelt werden.

Die Einstellungen in den jeweiligen Modulen beziehen sich immer auf die Clients, Server oder Gruppen, die im **Clients/ManagementServer**-Bereich markiert wurden. Sollten Clients innerhalb einer Gruppe unterschiedliche Einstellungen haben, bekommen einzelne Parameter, die unterschiedlich eingestellt sind, einen undefinierten Status. Wenn Sie die Einstellungen übernehmen, behält jeder Client für die undefinierten Parameter seine eigenen Einstellungen. Nur wenn die jeweiligen Parameter geändert werden, werden sie für alle Clients übernommen. Untergeordnete Clients oder Gruppen, die abweichende Einstellungen haben, werden unter **Clients/Gruppen mit abweichenden Einstellungen** angezeigt. Wählen Sie einen Client aus und klicken Sie auf **Einstellungen anzeigen**, um den Client im **Clients/ManagementServer**-Bereich auszuwählen und die jeweiligen Einstellungen zu sehen. Um den Client auf die Gruppeneinstellungen zurückzusetzen, wählen Sie **Auf Gruppeneinstellungen zurücksetzen**.

Bei der Administration von Gruppen mit sowohl Windows- als auch Linux- oder Mac-Clients werden Funktionen, die für Linux- und Mac-Clients nicht einstellbar sind, durch grünen Text markiert.

Geänderte Einstellungen werden erst nach Betätigung der **Übernehmen**-Schaltfläche gespeichert und zu den ausgewählten Clients/Servern übertragen. In den meisten Modulen wird Ihnen unter **Information** angezeigt, ob die durchgeführten Änderungen schon übernommen wurden. Drücken Sie die **Verwerfen**-Schaltfläche, um die Änderungen zu verwerfen.

4.3. Client-Module

Mit den Client-Modulen können Sie die Clients und Client-Gruppen, die Sie im **Clients**-Bereich ausgewählt haben, verwalten.

4.3.1. Dashboard

Im Dashboard-Bereich erhalten Sie Informationen zum aktuellen Zustand der Clients im Netzwerk. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.

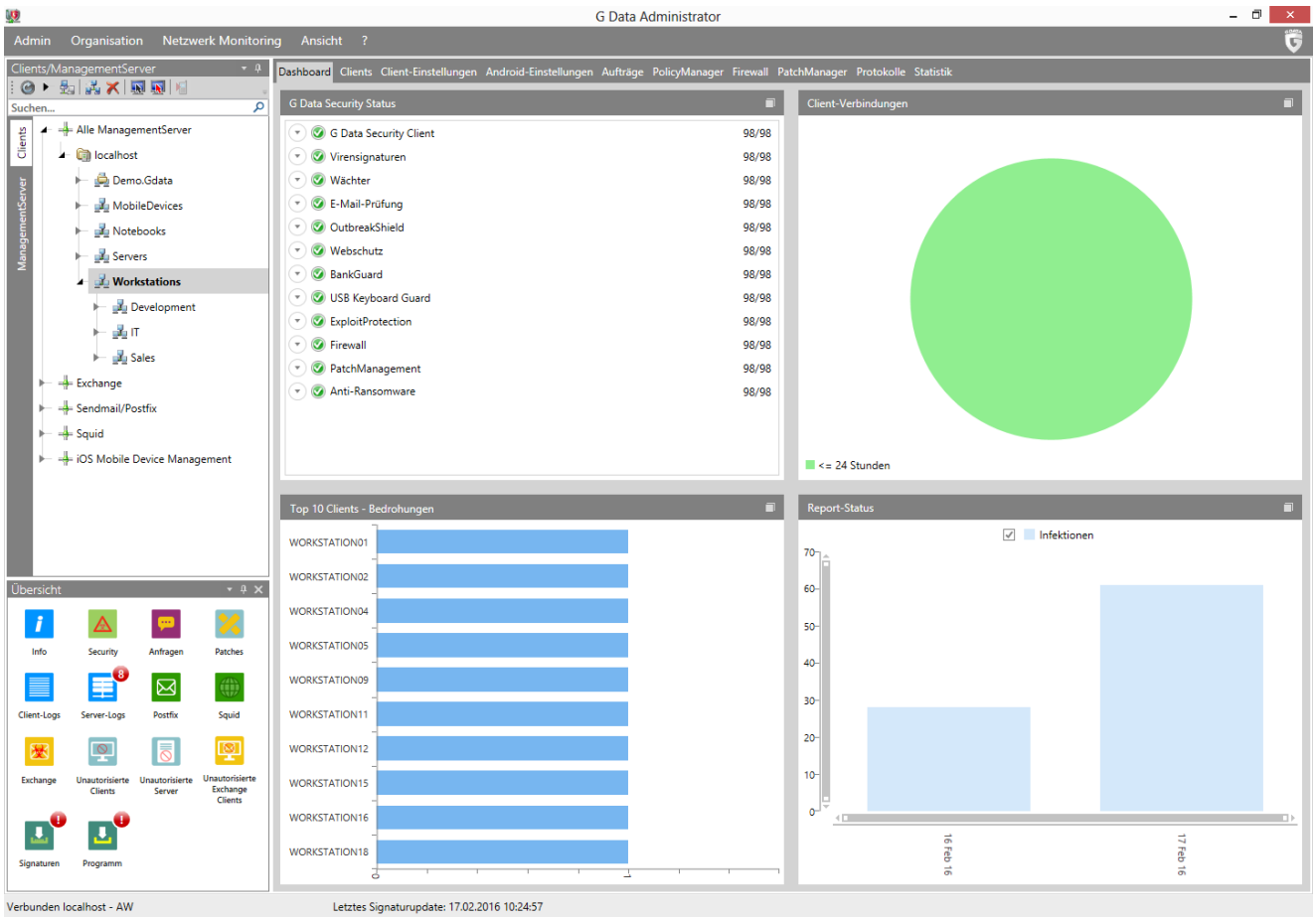
Unter **G DATA Security Status** können Sie alle grundlegenden Sicherheitseinstellungen für die Clients oder Gruppen einstellen, die Sie im **Clients**-Bereich markiert haben.

- Solange das Netzwerk optimal für den Schutz vor Computerviren konfiguriert ist, finden Sie links vor den hier aufgeführten Einträgen ein grünes Symbol.
- Sollte mindestens eine Komponente (Sicherheits-)Probleme vorweisen (z. B. abgeschalteter Wächter oder veraltete Virensignaturen), weist ein Achtung-Symbol darauf hin.
- Wenn sich die G DATA-Programmoberfläche öffnet, sind in einigen Fällen für kurze Zeit die meisten Symbole im Info-Modus. Das heißt nicht, dass das Netzwerk in diesem Moment ungeschützt ist. In diesem Moment wird die Datenbank des G DATA ManagementServers vom G DATA Administrator abgefragt.

Durch 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 Symbol.

Der Bereich **Client-Verbindungen** bietet eine zeitliche Übersicht über die Verbindungen, die die jeweiligen Clients mit dem G DATA ManagementServer hatten. Es sollte darauf geachtet werden, dass sich alle Clients regelmäßig mit dem G DATA ManagementServer verbinden. Die Clients die z. B. aufgrund des Nutzerverhaltens oder technischer Umstände in die Liste **Top 10 Clients - Bedrohungen** erscheinen, sollten besonders beobachtet werden. Ein Auftauchen eines oder mehrerer Clients in diesem Bereich ist unter Umständen eine Indikation dafür, dass der Client-Anwender auf

eventuelle Probleme aufmerksam gemacht werden oder technische Maßnahmen ergriffen werden sollten. Wenn die Infektionen auf Grund des Nutzerverhaltens stattfinden, wäre z. B. eine Nutzung des **PolicyManagers** (als Teil der Lösung **G DATA Endpoint Protection Business** verfügbar) ratsam. Der **Report-Status** bietet eine übersichtliche Darstellung über die Menge der Infektionen, Anfragen und Fehler in Ihrem Netzwerk.



4.3.2. Clients

Unter Clients lässt sich überprüfen, ob die Clients ordnungsgemäß laufen und ob die Virensignaturen und Programmdateien auf dem neuesten Stand sind.

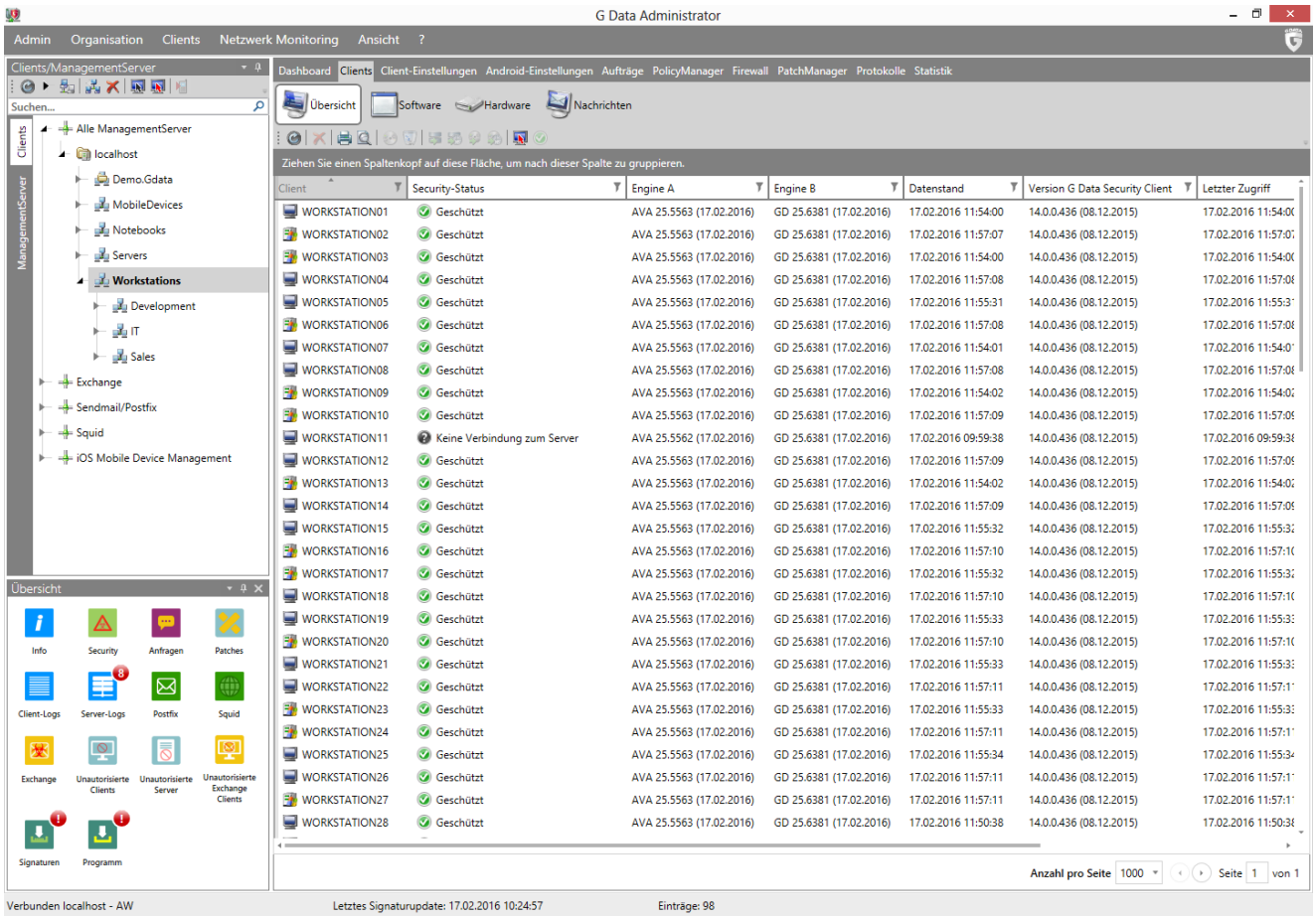
4.3.2.1. Übersicht

Hier erhalten Sie eine Übersicht über alle verwalteten Clients und können diese gleichzeitig auch administrieren. Mit Hilfe der Spalte **Security-Status** behalten Sie den Sicherheitsstatus jedes Clients im Blick.

Zur Administration der Clients und Gruppen stehen Ihnen folgende Schaltflächen zur Verfügung:

- **Aktualisieren**
- **Löschen**: Hiermit entfernen Sie einen Client aus der Clientübersicht. Da diese Funktion die Client-Software nicht vom Client entfernt, sollte sie nur für Clients, die bereits außer Betrieb genommen oder vom Netzwerk entfernt worden sind, benutzt werden. Wenn ein aktiver Client aus Versehen gelöscht wurde, wird er bei der nächsten ManagementServer-Synchronisation wieder zur Liste hinzugefügt (jedoch ohne spezifische Gruppeneinstellungen).
- **Drucken**
- **Seitenansicht**
- **G DATA Security Client installieren**

- **G DATA Security Client deinstallieren**
- **Virendatenbank jetzt aktualisieren**: Aktualisiert die Virendatenbank auf dem Client mit den Dateien vom G DATA ManagementServer.
- **Virendatenbank automatisch aktualisieren**: Aktiviert die automatische Aktualisierung der Virendatenbank. Die Clients prüfen periodisch, ob aktualisierte Virensignaturen auf dem G DATA ManagementServer vorhanden sind und führen die Aktualisierung automatisch durch.
- **Programmdateien jetzt aktualisieren**: Aktualisiert die Programmdateien auf dem Client. Es werden die Client-Programmdateien verwendet, die der G DATA ManagementServer bereit hält. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gestartet werden muss.
- **Programmdateien automatisch aktualisieren**: Aktiviert die automatische Aktualisierung der Programmdateien. Die Clients prüfen periodisch, ob eine neue Version auf dem G DATA ManagementServer existiert und führen die Aktualisierung automatisch durch.
- **Installationsübersicht**



Wenn Sie die Option Übersicht ausgewählt haben, erscheint in der Menüleiste ein zusätzliches Menü namens **Clients**. Im **Clients**-Menü und dem Kontextmenü stehen die folgenden Optionen zur Verfügung:

- **G DATA Security Client installieren**
- **G DATA Security Client für Linux installieren**
- **G DATA Security Client deinstallieren**
- **Installationsübersicht**
- **Auf Gruppeneinstellungen zurücksetzen**: Setzt den Client/die Clients auf die Gruppeneinstellungen zurück.

- **Clients verschieben**: Diese Funktion ermöglicht es Ihnen, ausgewählte Clients in eine existierende Gruppe zu verschieben. Wenn Sie diese Option auswählen, werden alle existierenden Gruppen in einem neuen Fenster angezeigt. Um nun den Client in eine Gruppe zu verschieben, wählen Sie die in Frage kommende Gruppe aus und klicken Sie auf **OK**.
- **Zugewiesene Eula ändern**: Weist eine zuvor definierte Eula dem ausgewählten Client zu (nur für Android-Clients).
- **Zugewiesene Eula löschen**: Entfernt eine zugewiesene Eula von den ausgewählten Clients (nur für Android-Clients).
- **Eulaverwaltung**
- **G DATA Server zuordnen**: Sie können Clients speziellen Subnet-Servern zuweisen mit Hilfe der Funktion im Kontextmenü oder auch über die Funktion **Server** > **Übersicht**.
- **Virendatenbank jetzt aktualisieren**
- **Virendatenbank automatisch aktualisieren**
- **Programmdateien jetzt aktualisieren**
- **Programmdateien automatisch aktualisieren**
- **Neustart nach Aktualisierung der Programmdateien**: Legen Sie hier fest, wie der Client reagieren soll, nachdem die Programmdateien aktualisiert wurden:
  - **Hinweisfenster auf dem Client anzeigen**: Informiert den Anwender darüber, dass er bei nächster Gelegenheit seinen Rechner neu starten sollte, damit das Programm-Update durchgeführt werden kann.
  - **Bericht erzeugen**: Sie erhalten im Sicherheitsereignisse-Bereich Infos darüber, welche Clients aktualisiert wurden.
  - **Neustart ohne Abfrage durchführen**: Zwingt den Client zu einem Neustart.
- **Entfernen** (nur im Kontextmenü)
- **Autorisation erteilen** (nur im Kontextmenü): Autorisiert die ausgewählten Clients. Um unberechtigten Zugriff auf den ManagementServer zu vermeiden, müssen Clients, die mit Hilfe des Installationsmediums installiert werden, im G DATA Administrator autorisiert werden, bevor sie vollständig verwaltet werden können.
- **Eigenschaften** (nur im Kontextmenü): Zeigt Eigenschaften für den ausgewählten Client an (**Allgemein**, **Netzwerkinfo**, **Sicherheitsrisiken** und **Hardware**).

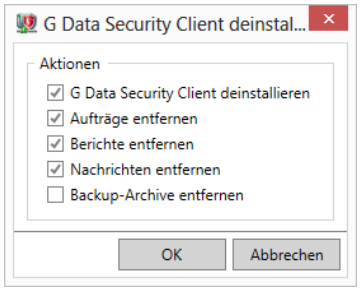
G DATA Security Client installieren
Wählen Sie die Option G DATA Security Client installieren, um die **Remote-Installation** des G DATA Security Clients auf allen ausgewählten Rechnern durchzuführen.

> Um auf deaktivierte Clients zugreifen zu können, müssen diese in der Clientübersicht als aktiv angezeigt werden. Bei Verwendung der Funktion **G DATA Security Client installieren** weist Sie das Programm gegebenenfalls darauf hin und ermöglicht eine Darstellung der deaktivierten Clients.

Sollte die Software nicht über die Remote-Installation auf den Clients aufgespielt werden können, können Sie auch direkt am Clientrechner eine **lokale Installation** mit dem G DATA-Installationsmedium oder einem Client-Installationspaket durchführen.

G DATA Security Client deinstallieren

Diese Funktion erteilt dem G DATA Security Client (für Windows und Linux) den Auftrag, sich selbst zu deinstallieren. Bevor die Deinstallation gestartet wird, können Sie die Komponenten auswählen, die behalten werden sollen. Es ist möglich, die Client-Software zu deinstallieren, während die Aufträge, Berichte, Nachrichten oder Backup-Archive, die diesem Client zugeordnet sind, weiterhin auf dem Server gespeichert bleiben. Wählen Sie die zu entfernenden Komponenten aus und klicken Sie auf **OK**, um die Deinstallation zu starten. Zum vollständigen Entfernen muss der Client neu gestartet werden.



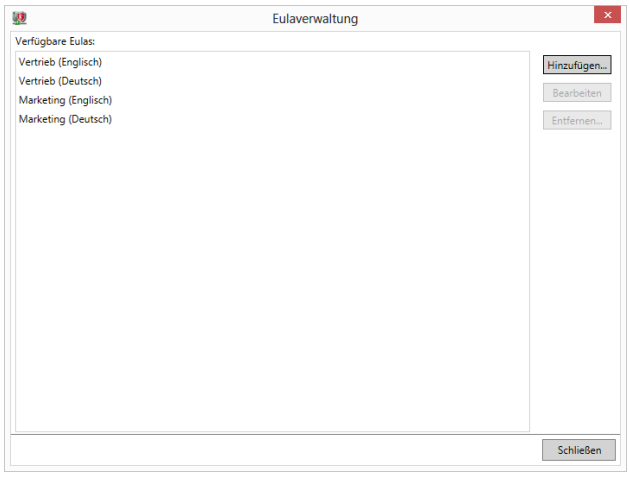
Alternativ ist es auch möglich, den Client lokal zu deinstallieren. Hierzu sind Administratorberechtigungen erforderlich. Starten Sie die Anwendung setup.exe, die sich im Ordner %ProgramData%\G Data\client befindet. Gegebenenfalls wird ein Neustart verlangt. Benutzen Sie für Linux-Clients das Skript gdata_uninstall.sh (meistens unter /usr/sbin/gdata_uninstall.sh).

Eulas verwalten

Im Eulas verwalten-Fenster können Sie End User License Agreements (Eula) für Android-Geräte hinzufügen, bearbeiten und entfernen. Über die entsprechende Option im Clients-Menü kann die jeweilige Eula dann auf jedem Android-Gerät zugewiesen werden, um sicherzustellen, dass die Endnutzer informiert und mit dem Einsatz der G DATA Internet Security für Android-Lösung einverstanden sind.

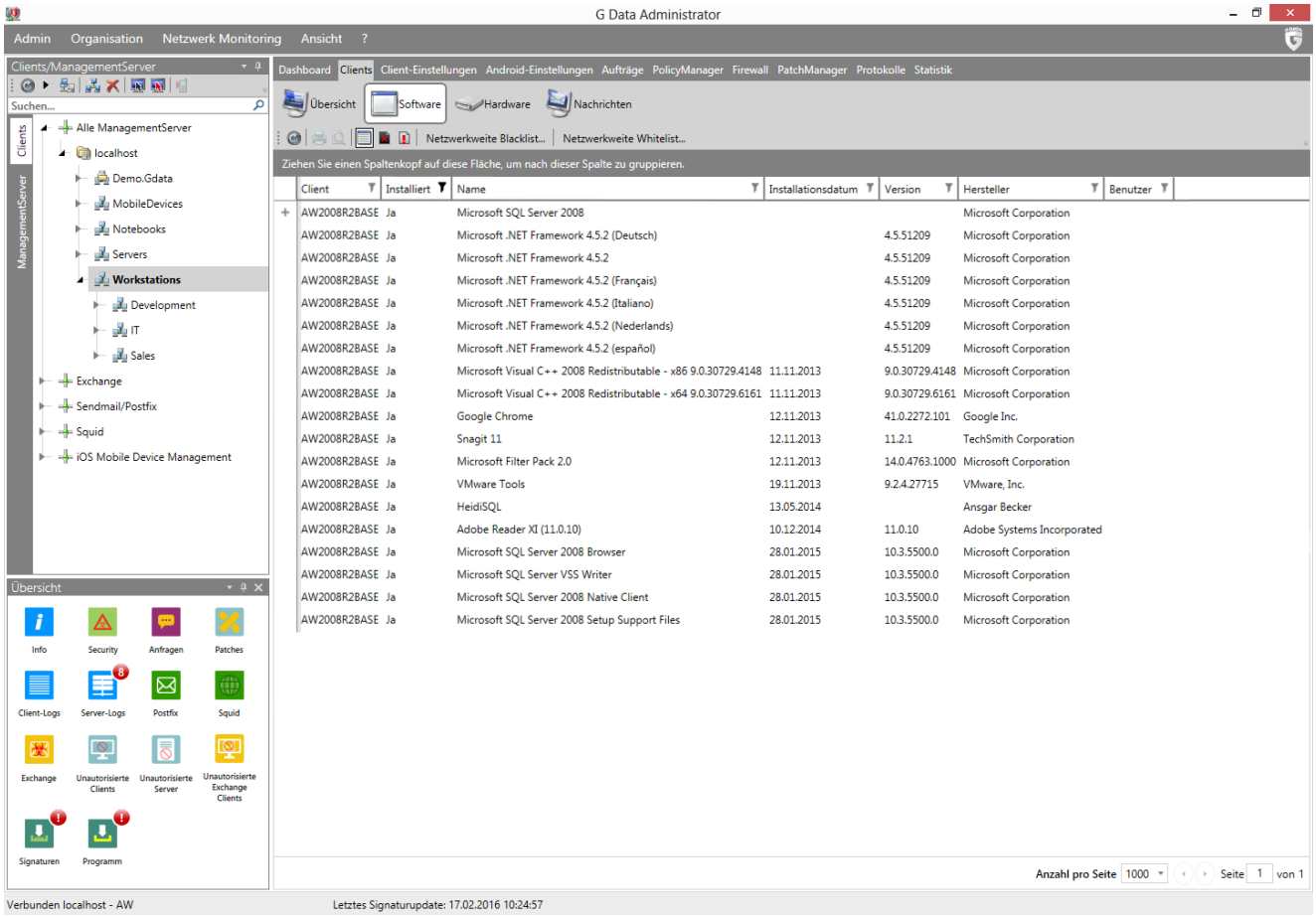
Im Eulas verwalten-Fenster werden alle verfügbaren Eulas aufgelistet. Um eine Eula hinzuzufügen, klicken Sie auf **Hinzufügen**. Im Eula erstellen-Fenster können Sie **Name**, **Sprache** und **Inhalt** der Vereinbarung definieren. Ein Klick auf **OK** fügt die Eula der Liste hinzu.

Um eine vorhandene Eula zu bearbeiten, wählen Sie diese in der Liste aus und klicken dann bitte auf **Ändern**. Um eine Eula zu entfernen, wählen Sie diese aus und klicken auf **Löschen**.



4.3.2.2. Software

Das Software-Inventar erlaubt Ihnen, die Software-Nutzung im gesamten Netzwerk zu überwachen. Software kann dabei auf Blacklists oder Whitelists hinzugefügt werden, um Software-Management im Netzwerk zu unterstützen.



Die Übersicht können Sie mit folgenden Schaltflächen beeinflussen:

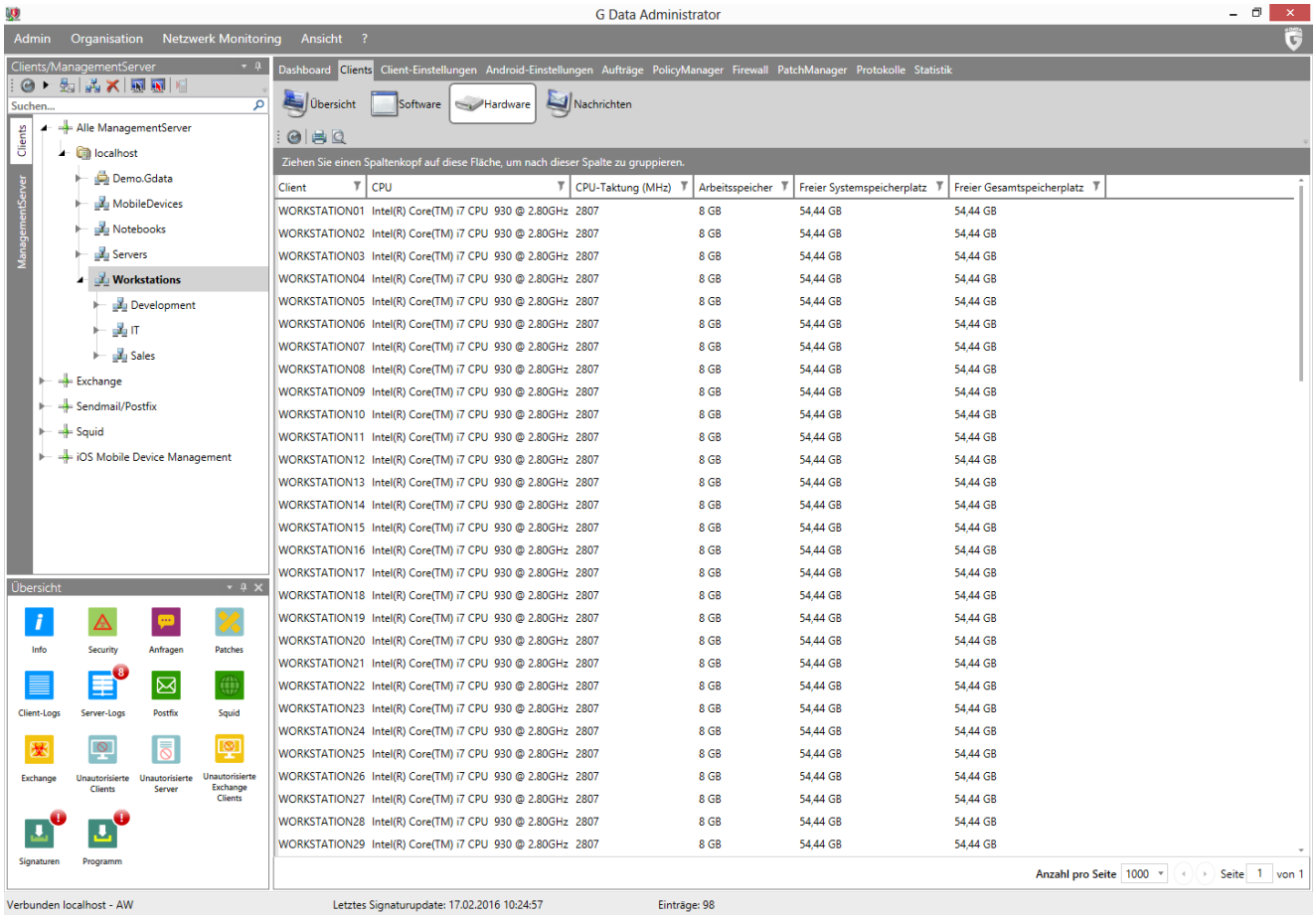
- **Aktualisieren**
- **Drucken**
- **Seitenansicht**
- **Alle anzeigen**: Hiermit wird Ihnen sämtliche im Netzwerk auf den Clients installierte Software angezeigt.
- **Nur Software auf der Blacklist anzeigen**: Über diese Einstellung können Sie sich die Software anzeigen lassen, die Sie zur Blacklist hinzugefügt haben.
- **Nur Software anzeigen, die nicht auf der Whitelist ist**: Hiermit erhalten Sie einen Überblick über installierte Software auf den Netzwerk-Clients, die vom Netzwerkadministrator noch nicht überprüft und kategorisiert wurde. Mit Hilfe dieser Ansicht können Sie gefundene Software mit einem Rechtsklick auf die Whitelist oder Blacklist setzen.

In der Listenansicht wird installierte Software für alle im **Clients**-Bereich selektierten Clients aufgelistet. Um die Whitelist bzw. Blacklist zu füllen, klicken Sie bitte auf die Schaltfläche **Netzwerkweite Blacklist** bzw. **Netzwerkweite Whitelist** und in dem nun erscheinenden Fenster auf die Schaltfläche **Hinzufügen**. Über die Option **Merkmale ermitteln** können Sie Programme auswählen, die Sie auf eine Blacklist oder Whitelist setzen möchten und die zugehörigen Attribute eingeben, mit denen das jeweilige Programm ermittelt werden kann. Um ein Attribut als Regel zu nutzen, setzen Sie einfach das Häkchen an das entsprechende Kästchen. Auf diese Weise können Sie z. B. Software bestimmter Hersteller oder auch nur spezielle Programmversionen black- oder whitelisten. Wenn Ihnen die erforderlichen Daten zur Verfügung stehen, können Sie Software auch durch Direkteingabe der Merkmale (ohne Umweg über Merkmale ermitteln) auf die Black- oder Whitelist setzen.

Standardmäßig zeigt das Software-Inventar nur derzeit installierte Programme. Wählen Sie **Alle Filter zurücksetzen** um auch Programme zu zeigen, die zuvor installiert wurden, jetzt aber nicht mehr vorhanden sind.

4.3.2.3. Hardware

Über diese Ansicht erhalten Sie Informationen zu der von den Clients verwendeten Hardware.

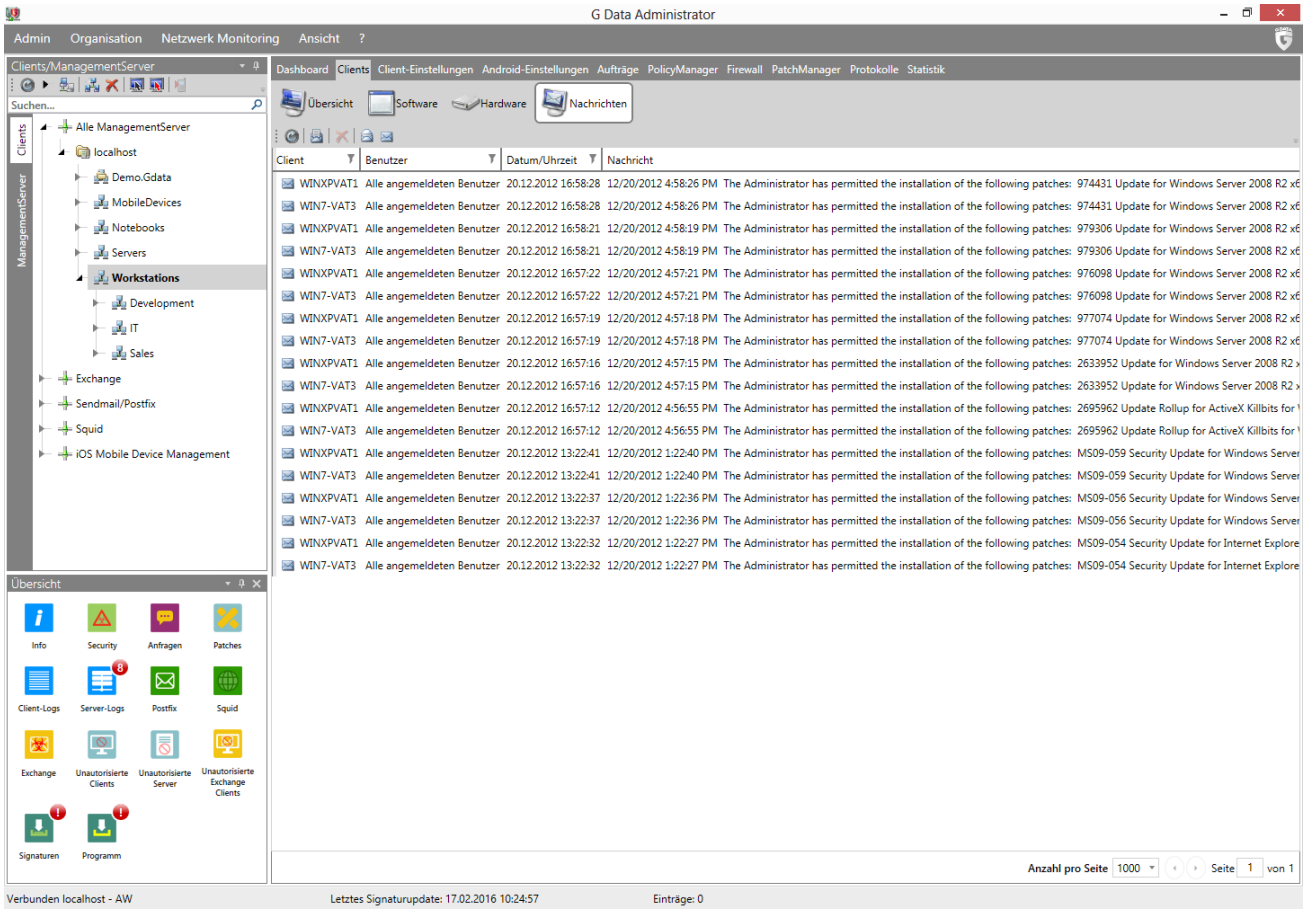


Die Übersicht können Sie mit folgenden Schaltflächen beeinflussen.

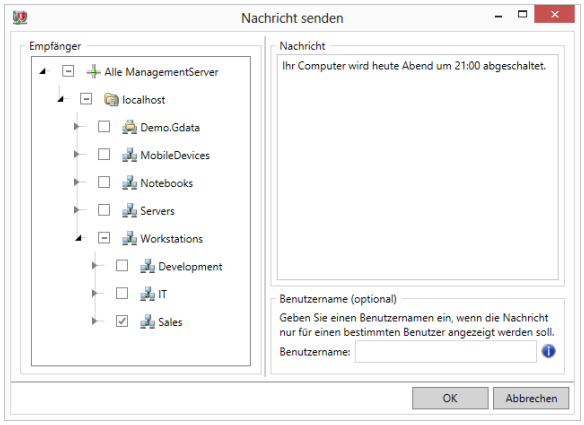
- **Aktualisieren**
- **Drucken**
- **Seitenansicht**

4.3.2.4. Nachrichten

Sie können an einzelne Clients oder Client-Gruppen Nachrichten versenden. Mit dem Versand dieser Nachrichten können Sie Anwender schnell und unkompliziert informieren. Die Nachrichten werden dabei als Info unten rechts auf dem Desktop des Client-Rechners angezeigt.



Um eine neue Nachricht zu erzeugen, wählen Sie **Nachricht senden**. In dem nun erscheinenden Fenster können Sie die Clients, denen Sie die Nachricht senden möchten, per Häkchen zu- oder abwählen.



Wenn Sie eine Nachricht nur an einen bestimmten Benutzer senden möchten, geben Sie dessen Anmeldenamen unter **Benutzername** ein. Tippen Sie nun in dem Feld **Nachricht** Ihre Hinweise ein und drücken Sie dann auf die Schaltfläche **OK**.

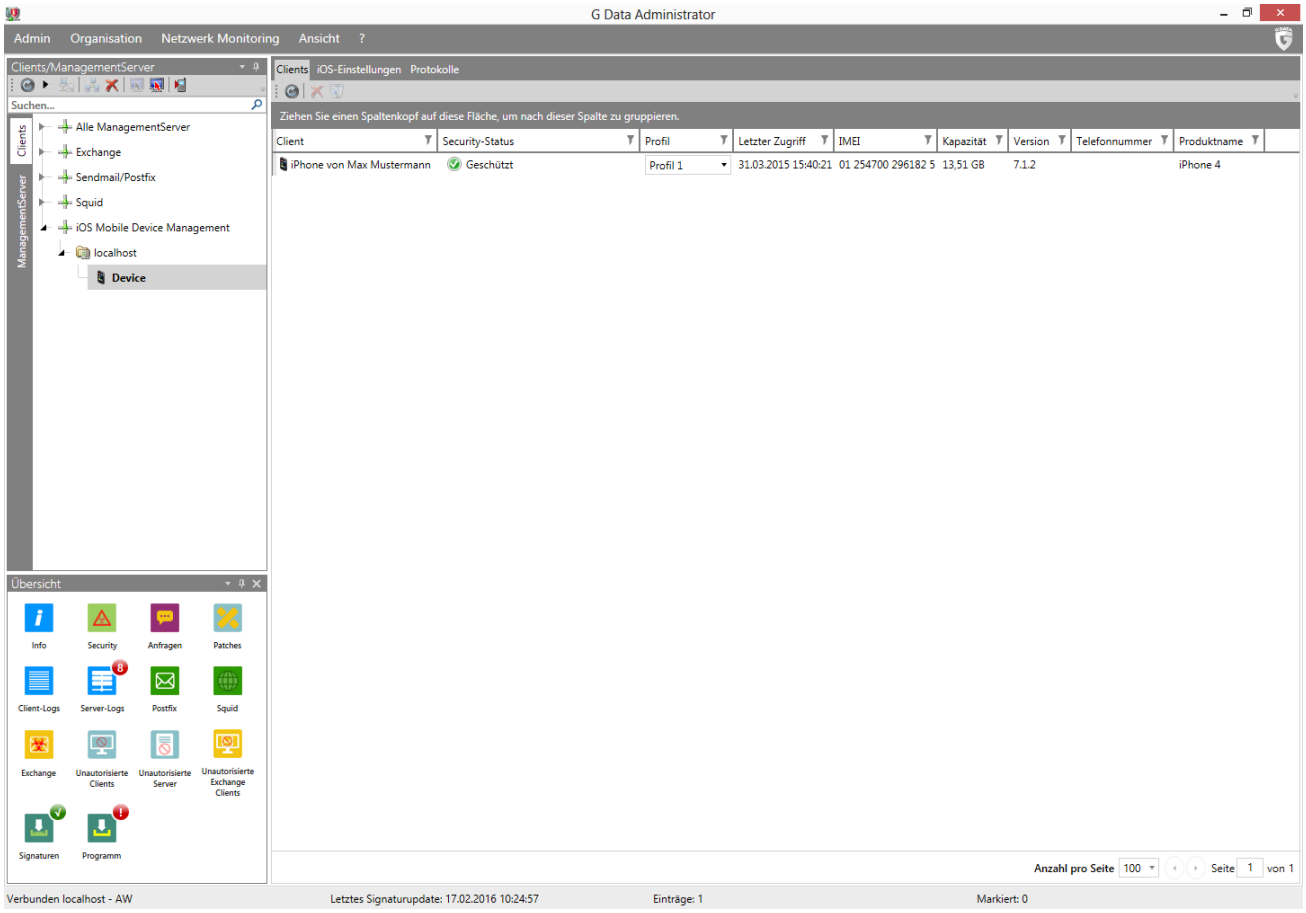
4.3.3. Clients (iOS)

Wenn Sie im **Clients**-Bereich einen oder mehrere iOS-Clients ausgewählt haben, werden im Clients-Modul nur Informationen, die auf die ausgewählten iOS-Clients zutreffen, angezeigt:

- **Client**: Gerätename.
- **Security-Status**: Der aktuelle Security-Status. Es wird eine Warnung angezeigt, wenn kein **Profil** zugewiesen wurde oder wenn das Profil noch nicht übernommen wurde.
- **Profil**: Das aktuell zugewiesene **Profil**. Wählen Sie ein Profil aus der Liste, um das Profil zu

ändern oder wählen Sie **- Kein Profil -**, um das aktuelle Profil zu löschen.

- **Letzter Zugriff**: Zeitpunkt, zu dem sich das iOS-Gerät zuletzt bei G DATA ActionCenter gemeldet hat.
- **IMEI**: Die IMEI-Nummer des Gerätes.
- **Kapazität**: Die Speicherkapazität des Gerätes (in GB).
- **Version**: Die iOS-Versionsnummer.
- **Telefonnummer**: Die Telefonnummer des Gerätes.
- **E-Mail**: Die E-Mail-Adresse, an die der Installationslink gesendet wurde.
- **Produktname**: Der Produktname des Gerätes.



Klicken Sie mit der rechten Maustaste auf einen Client, um eine der folgenden Optionen im Kontextmenü zu wählen:

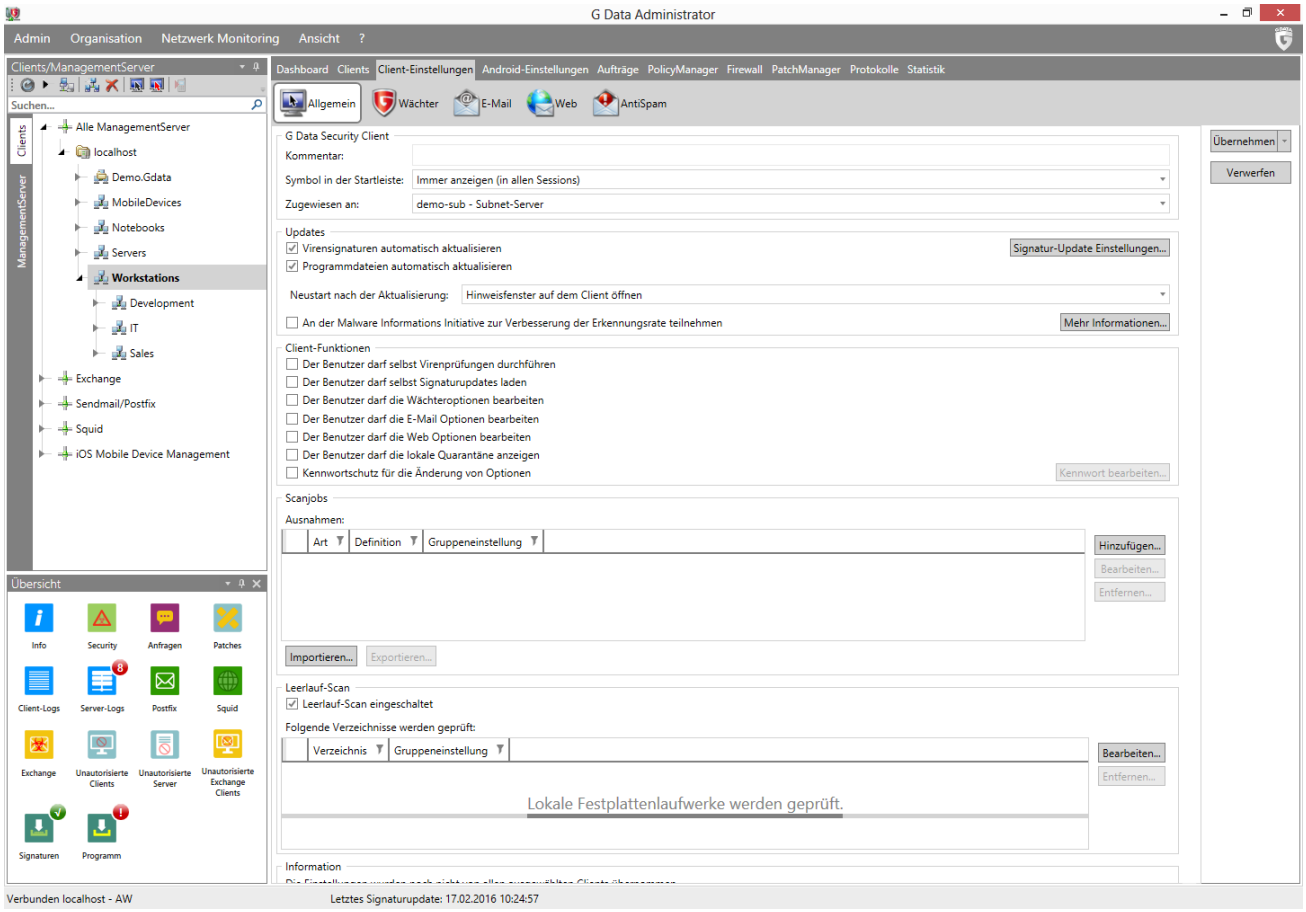
- **Verwaltung entfernen**: Deaktiviert Geräteverwaltung auf dem Gerät.
- **Entfernen**: Entfernt das Gerät aus der Liste. Bevor Sie ein Gerät entfernen, muss zuerst die Geräteverwaltung mit Hilfe der Option **Verwaltung entfernen** deaktiviert werden.
- **E-Mail zur Aktivierung erneut senden**: Sendet den Installationslink erneut zu Clients mit inaktiver oder anstehender Geräteverwaltung.

4.3.4. Client-Einstellungen

In diesem Modul können Sie die Parameter für jeden einzelnen Client bzw. jede Gruppe von Clients managen. In dem Sie die Karteireiter Allgemein, Wächter, E-Mail, Web und AntiSpam nutzen, können Sie Ihre Clients ganz individuell auf die Bedürfnisse Ihres Netzwerks und dessen Benutzer optimieren.

4.3.4.1. Allgemein

In diesem Bereich können Sie die grundlegenden Einstellungen der ausgewählten Clients bearbeiten.



G DATA Security Client

Der G DATA Security Client-Abschnitt behandelt die grundsätzliche Client-Funktionalität.

- **Kommentar**: Geben Sie hier ggf. ergänzende Informationen zum Client ein.
- **Symbol in der Startleiste**: Wählen Sie, in welchen Sessions ein Client-Symbol in der Taskleiste angezeigt werden soll: **Nie anzeigen**, **Nur in der ersten Session anzeigen** (für Terminal-Server und Windows mit schneller Benutzerumschaltung) oder **Immer anzeigen (in allen Sessions)**. Wenn das Client-Symbol nicht angezeigt wird, wird der Funktionsumfang des Security Clients stark eingeschränkt (der Administrator kann z. B. keinen **Leerlauf-Scan** einstellen und der Benutzer hat keinen Zugriff auf die **Client-Funktionen**).
- **Zugewiesen an**: Standardmäßig werden Clients dem Haupt-ManagementServer zugewiesen. Die Liste zeigt den Haupt-ManagementServer und alle Subnet-Server an. Mit Hilfe dieser Option können Sie einen Client bequem einem spezifischen (Subnet-)Server zuweisen.

Updates

Im Bereich Updates können Sie die Update-Einstellungen für Virensignaturen und Programmdateien vornehmen.

- **Virensignaturen automatisch aktualisieren**: Aktiviert die automatische Aktualisierung der Virendatenbank. Die Clients prüfen bei jedem **Synchronisationsintervall**, ob aktualisierte Virensignaturen auf dem ManagementServer vorhanden sind. Liegen aktualisierte Virensignaturen vor, werden diese automatisch auf dem Client installiert.
- **Programmdateien automatisch aktualisieren**: Aktiviert die automatische Aktualisierung der Client-Programmdateien. Die Clients prüfen bei jedem **Synchronisationsintervall**, ob

aktualisierte Programmdateien auf dem ManagementServer vorhanden sind. Liegen aktualisierte Programmdateien vor, werden diese automatisch auf dem Client installiert. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gestartet werden muss. Je nach Einstellung unter **Neustart nach der Aktualisierung** hat der Anwender auf dem Client die Möglichkeit, den Abschluss der Aktualisierung auf einen späteren Zeitpunkt zu verschieben.

- **Neustart nach der Aktualisierung**: Wählen Sie **Hinweisfenster auf dem Client öffnen** um den Anwender darüber zu unterrichten, dass er seinen Client-Rechner in nächster Zeit neu starten sollte, damit das Update eingespielt werden kann. **Bericht erzeugen** erzeugt einen Bericht im Bereich **Sicherheitsereignisse**. Über die Funktion **Neustart ohne Abfrage durchführen** wird auf dem Client-Rechner ungefragt automatisch ein Neustart durchgeführt.
- **An der Malware Information Initiative zur Verbesserung der Erkennungsrate teilnehmen**: Aktiviert die Teilnahme an der Malware Information Initiative. Die G DATA SecurityLabs erforschen ständig Verfahren, um unsere Kunden vor Malware (Viren, Würmern und Schadprogrammen) zu schützen. Je mehr Informationen dazu vorliegen, desto effektiver können Schutzmechanismen entwickelt werden. Viele Informationen sind aber nur auf attackierten oder infizierten Systemen vorhanden. Um auch solche Informationen in die Analyse einschließen zu können, wurde die G DATA Malware Information Initiative gegründet. In diesem Rahmen werden Malware-bezogene Informationen an die G DATA SecurityLabs geschickt.
- **Signatur-Update Einstellungen**: Hier wird festgelegt, woher die Clients ihre Virensignaturupdates beziehen.
  - **Signatur-Updates vom ManagementServer laden**: Clients laden die Virensignaturen vom ManagementServer herunter. Dazu prüfen sie bei jedem **Synchronisationsintervall**, ob neue Signaturen vorliegen.
  - **Online Signatur-Updates selbst laden**: Clients laden die Virensignaturen von den G DATA UpdateServern herunter. Das Update kann unter **Einstellungen und Zeitplanung** konfiguriert werden.
  - **Online Signatur-Updates selbst laden, wenn keine Verbindung zum ManagementServer hergestellt werden kann**: Diese Option empfiehlt sich für mobile Arbeitsplätze, wie z. B. Laptops. Solange der Client eine Verbindung zum ManagementServer hat, bezieht er die Aktualisierungen von dort. Besteht hingegen keine Verbindung zum ManagementServer, werden die Virensignaturen automatisch von den G DATA UpdateServern heruntergeladen. Das Update kann unter **Einstellungen und Zeitplanung** konfiguriert werden.

Client-Funktionen

Im Folgenden werden die Berechtigungen vergeben, die der Benutzer lokal für einzelne Clientfunktionen hat. So können dem Anwender umfangreiche oder auch nur stark eingeschränkte Rechte zur Änderung von Einstellungen eingeräumt werden.

- **Der Benutzer darf selbst Virenprüfungen durchführen**: Im akuten Verdachtsfall kann der Anwender wie bei einer lokal installierten Antivirenlösung auf seinem Rechner unabhängig vom ManagementServer eine Virenprüfung durchführen. Ergebnisse dieser Virenprüfung werden beim nächsten Kontakt mit dem ManagementServer an diesen übermittelt. Diese Funktion erlaubt auch Änderungen im Bereich Virenprüfung (lokale Einstellungen).
- **Der Benutzer darf selbst Signaturupdates laden**: Wenn Sie diese Funktion aktivieren, darf der Nutzer des Client-Rechners aus dem Kontextmenü heraus Virensignaturen auch ohne Verbindung zum ManagementServer direkt aus dem Internet laden.

- **Der Benutzer darf die Wächteroptionen bearbeiten**: Wenn diese Funktion aktiviert ist, hat der Benutzer des Client-Rechners die Möglichkeit, Einstellungen im Bereich **Wächter** zu ändern.
- **Der Benutzer darf die E-Mail Optionen bearbeiten**: Wenn diese Funktion aktiviert ist, hat der Benutzer des Client-Rechners die Möglichkeit, Einstellungen in den Bereichen **Email** und **AntiSpam** zu ändern.
- **Der Benutzer darf die Web Optionen bearbeiten**: Wenn diese Funktion aktiviert ist, hat der Benutzer des Client-Rechners die Möglichkeit, Einstellungen im Bereich **Web** zu ändern.
- **Der Benutzer darf die lokale Quarantäne anzeigen**: Wenn das Anzeigen der lokalen Quarantäne erlaubt wird, kann der Anwender Daten, die wegen Virenbefall oder -verdacht in Quarantäne verschoben wurden ggf. desinfizieren, löschen oder zurückbewegen. Beachten Sie dabei, dass bei einem Zurückbewegen einer Datei aus der Quarantäne ein Virus nicht entfernt wird. Diese Option sollte deshalb nur versierten Anwendern auf den Clients zugänglich gemacht werden.
- **Kennwortschutz für die Änderung von Optionen**: Um einer missbräuchlichen Manipulation von lokalen Einstellungen vorzubeugen, gibt es die Möglichkeit, die Änderung von Optionen nur dann zuzulassen, wenn ein Passwort eingegeben wird. So lässt sich beispielsweise verhindern, dass ein User die Einstellungen ändert. Das Passwort kann individuell für den jeweiligen Client oder die jeweilige Gruppe vergeben werden und muss nur den autorisierten Nutzern mitgeteilt werden.

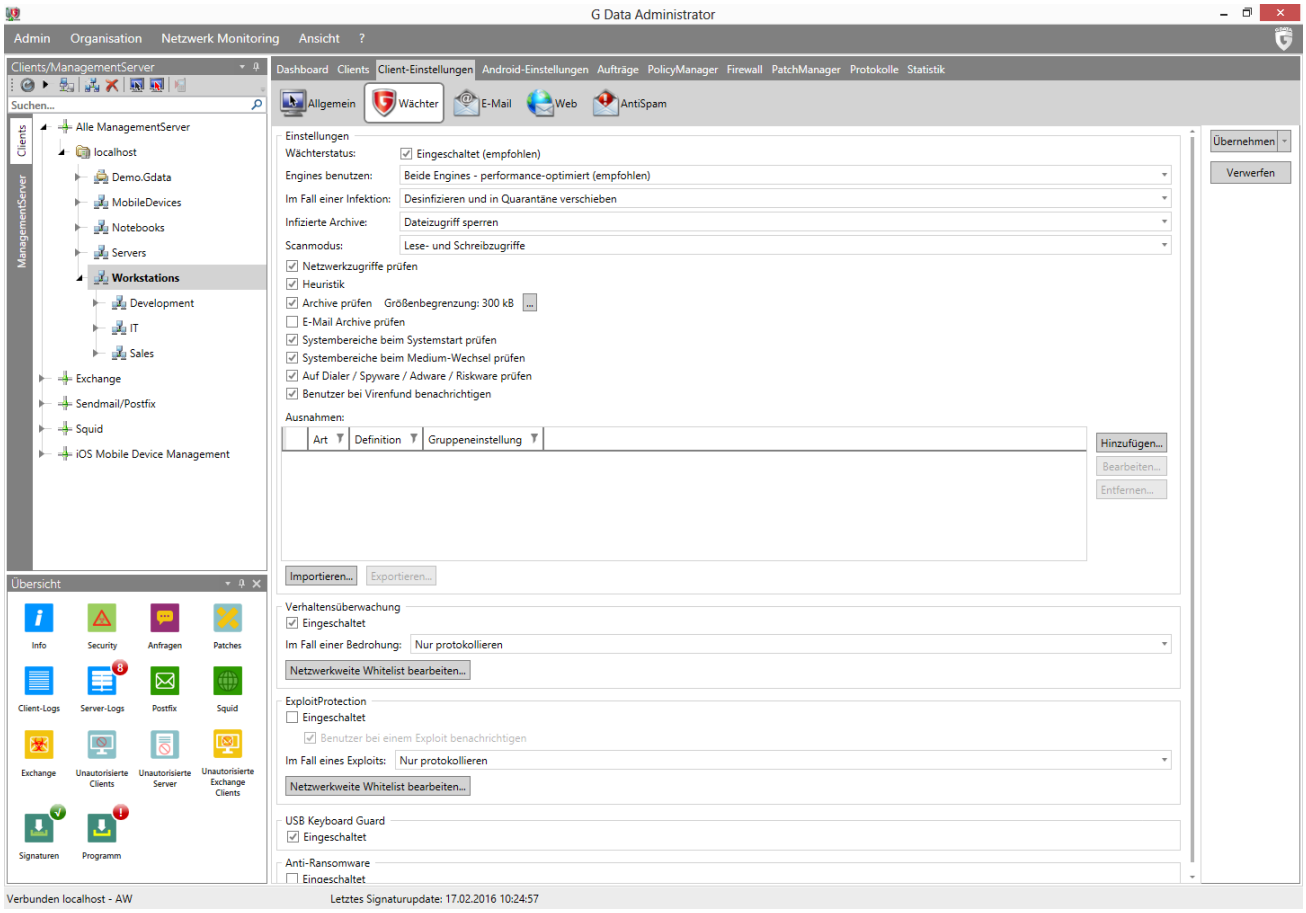
Scanjobs
Sie können hier Ausnahmen definieren, die nicht während der Ausführung der Scan-Aufträge überprüft werden. Zum Beispiel können Archiv- und Backup-Bereiche einer Festplatte oder Partition als Ausnahmen definiert werden, auch bestimmte Ordner oder sogar Dateierweiterungen können von den Scanjobs ausgeschlossen werden. Diese Ausnahmen können auch 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.

Leerlauf-Scan
Wenn Sie möchten, dass der Client einen Virenscan durchführen soll, wenn sich der Computer im Leerlauf befindet, wählen Sie die Option **Leerlauf-Scan eingeschaltet**. Durch Anklicken der **Bearbeiten**-Schaltfläche können Sie den Scan-Bereich festlegen. Standardmäßig sind hier alle lokalen Festplattenlaufwerke eingestellt.

4.3.4.2. Wächter

Hier können die Wächtereinstellungen vorgenommen werden. Der Wächter sollte grundsätzlich nicht deaktiviert werden, da dieser für den Echtzeitschutz vor Schädlingen sorgt. Wird der Wächter deaktiviert, besteht dieser Schutz nicht mehr. Es wird daher empfohlen, den Wächter nur dann auszuschalten, wenn ein wichtiger Grund besteht, zum Beispiel Fehlersuche oder Diagnose.

Die Definition von Ausnahmen für den Wächter ist möglich. Sollte eine Anwendung durch den Einsatz des Wächters von Performanceeinbußen betroffen sein, können für die entsprechenden Programmdateien, Prozesse oder Dateien Ausnahmen hinzugefügt werden; ausgenommene Dateien werden dann nicht mehr vom Wächter geprüft. Beachten Sie, dass das Hinzufügen von Wächterausnahmen unter Umständen ein Sicherheitsrisiko darstellen kann.



Einstellungen

Wächter-Einstellungen können dazu genutzt werden, um den Wächter zu konfigurieren und Ausnahmen zu definieren.

- **Wächterstatus**: Hier können Sie den Wächter an- 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 und in Quarantäne verschieben**: Die Datei wird in die Quarantäne verschoben und es wird versucht, den Virus zu entfernen.
  - **Datei in Quarantäne verschieben**: Die Datei wird in die Quarantäne verschoben. Eine mögliche Desinfektion der Datei kann dann manuell durch den Systemadministrator durchgeführt werden.
  - **Infizierte Datei entfernen**: Als rigorose Maßnahme hilft diese Funktion dabei, den Virus wirkungsvoll einzudämmen. Allerdings kann es dabei im seltenen Fall einer falsch-positiven Virenmeldung zu Datenverlust kommen.
- **Infizierte Archive**: Legen Sie hier fest, wie infizierte Archive behandelt werden sollen. Beachten

Sie beim Festlegen dieser Einstellungen, dass ein Virus innerhalb eines Archives erst dann Schaden anrichtet, wenn das Archiv entpackt wird.

- **Scanmodus**: Legen Sie hier fest, wie Dateien gescannt werden sollen. **Lesezugriffe** scannt jede Datei sofort, wenn Sie gelesen wird. **Lese- und Schreibzugriffe** überprüft Dateien nicht nur bei Lese- sondern auch bei Schreibzugriffen. Dies dient als Schutz vor Viren, die möglicherweise von einem anderen ungeschützten Client oder aus dem Internet kopiert werden. **Bei Ausführung** führt einen Scan durch, sobald eine Datei ausgeführt wird.
- **Netzwerkzugriffe prüfen**: Hier können Sie die Vorgehensweise des Wächters im Zusammenhang mit Netzwerkzugriffen festlegen.
- **Heuristik**: In der heuristischen Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken ermittelt, sondern auch anhand bestimmter virentypischer Merkmale erkannt. 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 Überprüfen großer Archivdateien, 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 E-Mail ein Postfach – abhängig von den Einstellungen des Virenscans – in die Quarantäne verschoben oder gelöscht wird. Alle E-Mails innerhalb des E-Mail-Archivs wären in einem solchen Fall nicht mehr verfügbar. 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 E-Mails zusätzlich durch ein integriertes Plugin geprüft.
- **Systembereiche beim Systemstart prüfen/Systembereiche bei Medium-Wechsel prüfen**: Systembereiche (z. B. Bootsektoren) Ihres Computers sollten nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim Medium-Wechsel (neue DVD 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 unerwünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in Nichts nachstehen. Spyware kann z. B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch Ihre Passwörter) unbemerkt speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.
- **Benutzer bei Virenfund benachrichtigen**: Wird diese Option aktiviert, öffnet sich bei einem Virenfund durch den Wächter auf dem betroffenen Client ein Hinweisfenster, das den Benutzer davon in Kenntnis setzt, dass auf seinem System ein Virus gefunden wurde. Die gefundene Datei sowie der Pfad und die Bezeichnung des gefundenen Schädlings werden dort angezeigt.

Unter **Ausnahmen** können Sie beim Client bestimmte Verzeichnisse von der Virenprüfung ausschließen. Auf diese Weise können Sie z. B. Ordner mit selten benötigten Archiven aussparen, um diese in einem gesonderten Scanauftrag zu prüfen. Des Weiteren lassen sich bestimmte Dateien und Dateitypen von der Virenprüfung ausschließen. Folgende Ausnahmen sind möglich:

- **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.
- **Laufwerk**: Wählen Sie hier mit Anklicken der Verzeichnis-Schaltfläche ein Laufwerk (Partition, Festplatte) aus, welches Sie vom Wächter nicht kontrollieren lassen möchten.
- **Datei**: Hier können Sie den Namen der Datei eingeben, die Sie von der Wächterkontrolle ausnehmen möchten. Sie können hier mit Platzhaltern arbeiten.

  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. xls, xlsx), geben Sie einfach *.xls? ein. Um z. B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu schützen, geben Sie beispielsweise text*.* ein. Dies würde die Dateien text1.txt, text2.txt, text3.txt usw. betreffen.
- **Prozess**: Soll ein bestimmter Prozess nicht vom Wächter überwacht werden, sind der Verzeichnispfad und der Name des betreffenden Prozesses hier einzutragen.

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

Verhaltensüberwachung

Die Verhaltensüberwachung stellt einen weiteren Schutz vor schädlichen Dateien und Prozessen dar, der im Unterschied zum Wächter, nicht signaturbasiert arbeitet, sondern das tatsächliche Verhalten eines Prozesses analysiert. Um eine Einordnung vorzunehmen, legt die Verhaltensüberwachung verschiedene Kriterien zugrunde, unter anderem Schreibzugriffe auf die Registry und das eventuelle Anlegen von Autostarteinträgen. Sind genügend Merkmale vorhanden, die den Schluss zulassen, dass ein Programm zumindest verdächtiges Verhalten an den Tag legt, wird die unter **Im Fall einer Bedrohung** eingestellte Aktion durchgeführt. Hierbei stehen die Optionen **Nur protokollieren**, **Programm anhalten** sowie **Programm anhalten und in Quarantäne verschieben** zur Verfügung.

Wenn die Verhaltensüberwachung eine Aktion durchführt, wird immer ein Bericht zu den **Sicherheitsereignissen** hinzugefügt. Falls ein Programm fälschlicherweise als Bedrohung identifiziert wurde, kann der jeweilige Bericht benutzt werden, um einen Whitelist-Eintrag zu erstellen. Whitelist-Einträge können über die Schaltfläche **Netzwerkweite Whitelist bearbeiten** angesehen und gelöscht werden.

ExploitProtection

Exploits missbrauchen Schwachstellen in Software von Drittanbietern. ExploitProtection überprüft das Verhalten der installierten Software ständig auf Auffälligkeiten. Wenn ungewöhnliche Ereignisse in einem Softwareprozess auftreten, wird die unter **Im Fall eines Exploits** festgelegte Aktion ausgeführt: **Nur protokollieren** oder **Ausführung verhindern**. Wenn **Benutzer bei einem Exploit benachrichtigen** aktiviert ist, erhält der Benutzer zusätzlich eine Nachricht.

Wenn ExploitProtection eine Aktion durchführt, wird immer ein Bericht zu den **Sicherheitsereignissen** hinzugefügt. Falls ein Programm fälschlicherweise als Bedrohung identifiziert wurde, kann der jeweilige Bericht benutzt werden, um einen Whitelist-Eintrag zu erstellen. Whitelist-Einträge können über die Schaltfläche **Netzwerkweite Whitelist bearbeiten** angesehen und gelöscht werden.

USB Keyboard Guard

USB Keyboard Guard schützt Clients gegen BadUSB-Angriffe. Manipulierte USB-Geräte – wie z. B. Kameras, Speichersticks oder Drucker – können sich als Tastatur am Windows-System anmelden. Um den Client vor unbefugten, automatisch durchgeführten Befehlen zu schützen, blockiert USB Keyboard Guard zuerst alle neu angeschlossenen Geräte, die sich als Tastatur anmelden. Falls der Benutzer in der Tat eine Tastatur angeschlossen hat, kann er sie genehmigen. Wenn das Gerät sich als Tastatur anmeldet, der Benutzer aber ein anderes Gerät angeschlossen hat, sollte es nicht genehmigt werden, da es sich um einen Betrugsversuch handeln könnte.

Unabhängig von der Entscheidung des Benutzers wird ein Bericht zu den **Sicherheitsereignissen** hinzugefügt. Wenn ein Gerät genehmigt wurde, kann der Administrator es durch einen Widerruf der Genehmigung dennoch blockieren.

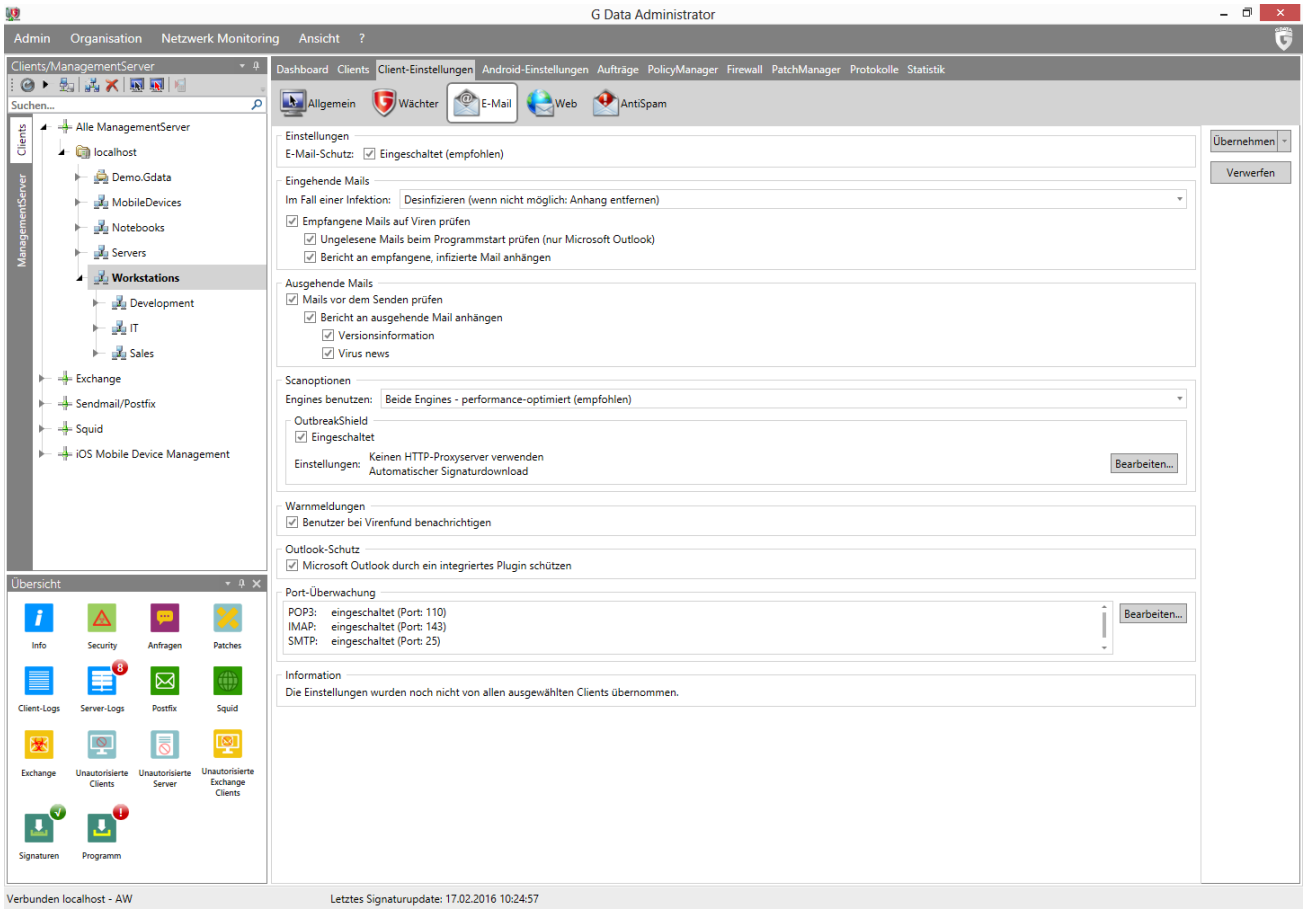
Anti-Ransomware

Während reguläre Malware Geräte infiziert, um sie z. B. als Teil eines Botnets zu verwenden oder Kreditkarteninformationen zu stehlen, versuchen die Entwickler von Ransomware, den Benutzer direkt zu erpressen, um an Geld zu kommen. Für den Erhalt eines Lösegeldes (engl. „ransom“) sperrt die Ransomware das Gerät oder verschlüsselt sogar die Daten, bis das Opfer zahlt. Zusätzlich zur signatur- und verhaltensbasierten Erkennung erkennt die Anti-Ransomware-Funktion bestimmte Ransomware-Aktionen wie Dateiverschlüsselung und blockiert sie, bevor sie Schaden anrichten können. Wenn Ransomware-Aktionen erkannt werden, wird die unter **Im Fall einer Bedrohung** festgelegte Aktion ausgeführt: **Nur protokollieren** oder **In Quarantäne verschieben**. Wenn **Benutzer bei einer Bedrohung benachrichtigen** aktiviert ist, erhält der Benutzer zusätzlich eine Nachricht.

Wenn Anti-Ransomware eine Aktion durchführt, wird immer ein Bericht zu den **Sicherheitsereignissen** hinzugefügt. Falls ein Programm fälschlicherweise als Bedrohung identifiziert wurde, kann der jeweilige Bericht benutzt werden, um einen Whitelist-Eintrag zu erstellen. Whitelist-Einträge können über die Schaltfläche **Netzwerkweite Whitelist bearbeiten** angesehen und gelöscht werden.

4.3.4.3. E-Mail

Auf jedem G DATA Security Client kann ein gesonderter Virenschutz für E-Mails eingerichtet werden. Hierbei werden Standardports für die Protokolle POP3, IMAP und SMTP überwacht. 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.



Eingehende Mails

Der Bereich Eingehende Mails definiert Optionen für das Scannen eingehender E-Mails.

- **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

Der Bereich Ausgehende Mails definiert Optionen für das Scannen ausgehender E-Mails.

- **Mails vor dem Senden prüfen**: Damit aus Ihrem Netzwerk keine Viren per Mail 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 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 DATA AntiVirus*, so lange Sie die Option **Mails vor dem Senden prüfen** aktiviert haben. Zusätzlich können Sie hier das Versionsdatum (**Versionsinformation**) angeben.

Scanoptionen

Der Bereich Scanoptionen konfiguriert die Scan-Parameter für eingehende und ausgehende E-Mails.

- **Engines benutzen**: Die G DATA Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten, den so genannten Engines. 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 eine Analyse schneller durchgeführt werden.
- **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 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. Außerdem können Sie hier Zugangsdaten für die Internetverbindung oder einen Proxyserver eingeben, die dem OutbreakShield automatische Signaturdownloads aus dem Internet ermöglichen.

Warnmeldungen

Der Bereich Warnmeldungen konfiguriert Warnmeldungen für die Empfänger infizierter E-Mails.

- **Benutzer bei Virenfund benachrichtigen**: Sie können den Empfänger einer infizierten Nachricht automatisch informieren. Auf seinem Desktop wird dann eine Virenmeldung angezeigt.

Outlook-Schutz

Outlook-Schutz ermöglicht E-Mail-Scans in Outlook mit Hilfe eines integrierten Plugins.

- **Microsoft Outlook durch ein integriertes Plug-In schützen**: Mit Aktivierung dieser Funktion wird in das Outlook des Clients im Menü **Extras** eine neue Funktion namens **Ordner auf Viren prüfen** eingefügt. Unabhängig von den G DATA 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 prüfen** eine Virenprüfung 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.

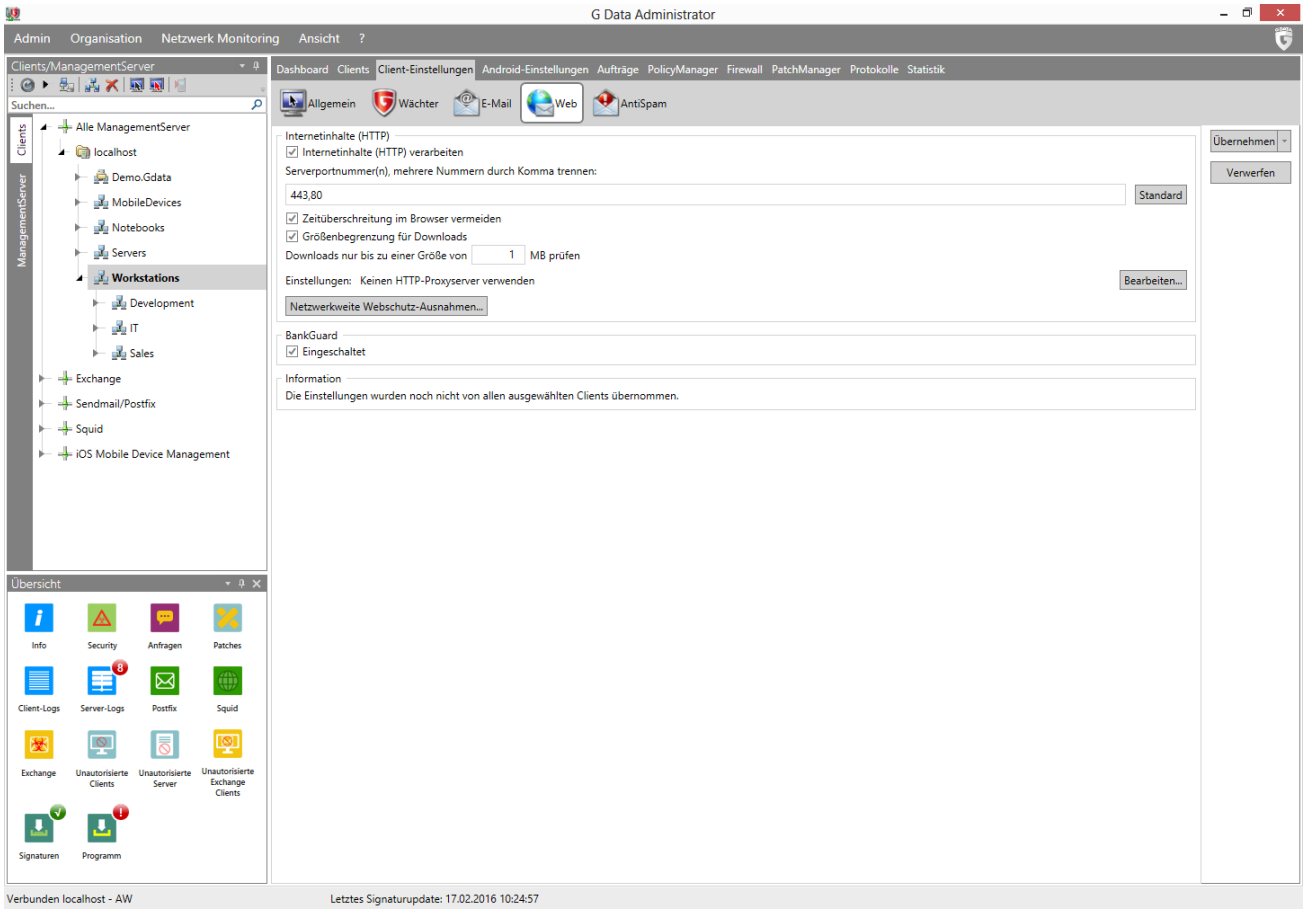
Port-Überwachung

Generell werden die Standardports für POP3 (110), IMAP (143) und SMTP (25) überwacht. Sollten die Porteinstellungen in Ihrem System davon abweichen, können Sie dies entsprechend anpassen.

4.3.4.4. Web

In diesem Bereich können Sie Scan-Einstellungen für Internet und Online-Banking definieren. Wenn Sie die Internetinhalte nicht prüfen lassen wollen, greift der **Virenwächter** ein, wenn auf

heruntergeladene, infizierte Dateien zugegriffen wird. Das System auf dem jeweiligen Client ist also auch ohne die Überprüfung von Internetinhalten geschützt, solange der Virenwächter aktiviert ist.



Internetinhalte (HTTP)

Der Bereich Internetinhalte (HTTP) behandelt Scan-Einstellungen für den HTTP-Datenverkehr.

- **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. Wird im Netzwerk ein Proxy für den Zugang zum Internet genutzt, muss der Serverport eingetragen werden, den der Proxy nutzt. Sonst ist eine Überprüfung des Internetverkehrs nicht möglich. Auch die **Web-Inhaltskontrolle** (verfügbar in der G DATA Endpoint Protection Business) benutzt diese Einstellungen.
- **Zeitüberschreitung im Browser vermeiden**: Da die G DATA Software die Webinhalte 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 angeforderten Daten erhält, da diese zunächst von der Antivirensoftware auf Schadroutinen überprüft werden. Mit Setzen des Häkchens bei **Zeitüberschreitung im Browser vermeiden** wird diese Fehlermeldung unterdrückt. Sobald sämtliche Browserdaten auf Viren überprüft wurden, werden diese dann an den Internet Browser weitergereicht.
- **Größenbegrenzung für Downloads**: Hiermit können Sie die HTTP-Überprüfung für zu große Webinhalte aussetzen. Die Inhalte werden dann vom Virenwächter überprüft, sobald etwaige Schadroutinen aktiv werden. Der Vorteil bei dieser Größenbegrenzung liegt darin, dass es beim Download größerer Dateien nicht zu Verzögerungen durch die Virenkontrolle kommt.
- **Netzwerkweite Webschutz-Ausnahmen**: Diese Funktion erlaubt es Ihnen, bestimmte Webseiten generell von der Überprüfung durch den Webschutz auszunehmen.

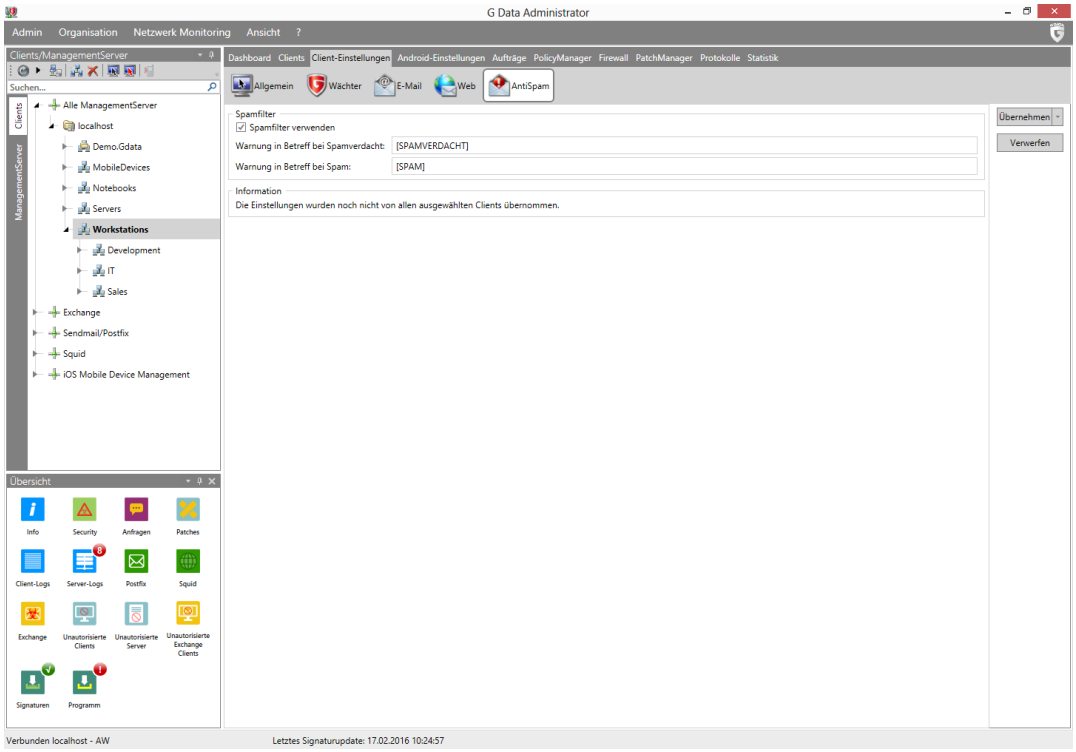
BankGuard
Banking-Trojaner werden zu einer immer größeren Bedrohung. Die wegweisende Technologie von G DATA BankGuard sichert Bankgeschäfte von Anfang an und schützt sofort dort, wo der Angriff stattfindet. Durch eine Prüfung der Echtheit der benutzten Netzwerkbibliotheken stellt G DATA BankGuard sicher, dass Internet-Browser nicht von einem Banking-Trojaner manipuliert werden. Durch diesen proaktiven Sofortschutz von mehr als 99 % sind Online-Bankgeschäfte bestmöglich geschützt – selbst vor bisher unbekannten Trojanern. BankGuard sollte für alle Clients aktiviert werden, die den Internet Explorer, Firefox und/oder Chrome nutzen.

4.3.4.5. AntiSpam

Das AntiSpam-Modul ist als Teil der Client Security Business-, Endpoint Protection Business- und Managed Endpoint Security-**Lösungen** verfügbar.

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 festlegen, die dann im Betreff der Mail angezeigt wird.

> Falls das **Microsoft Outlook-Plugin** aktiv ist, werden eingehende Spam-Berichte in den AntiSpam-Ordner verschoben. Bei anderen E-Mail-Clients können Spam-Berichte automatisch in einen Ordner verschoben werden, indem Sie einen mit der Warnung im Betreff übereinstimmende Filter definieren. AntiSpam-Einstellungen für Microsoft Exchange konfigurieren Sie unter **Exchange-Einstellungen** > **AntiSpam**.



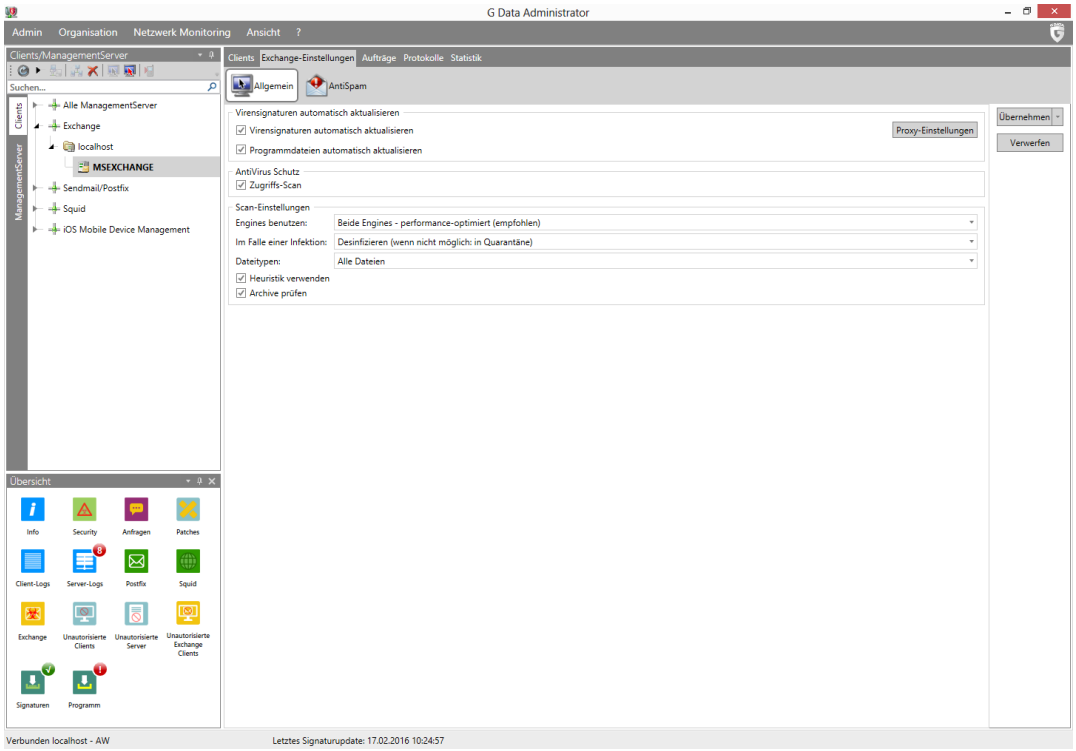
4.3.5. Exchange-Einstellungen

G DATA Exchange Mail Security ist als **optionales Modul** verfügbar.

Das G DATA MailSecurity Exchange-Plugin kann über den Aufgabenbereich Exchange-Einstellungen konfiguriert werden. Der Bereich wird aktiviert sobald das Plugin auf einem Exchange Server 2007 SP1, 2010 oder 2013 installiert worden ist.

4.3.5.1. Allgemein

Der Bereich Allgemein beinhaltet Funktionen für automatische Updates, Malware-Schutz und Scan-Einstellungen.



Virensignaturen automatisch aktualisieren

Ebenso wie Windows- und Linux-Clients können Exchange-Clients Aktualisierungen automatisch herunterladen.

- **Virensignaturen automatisch aktualisieren**: Aktiviert die automatische Aktualisierung der Virendatenbank. Die Clients prüfen bei jedem **Synchronisationsintervall**, ob aktualisierte Virensignaturen auf dem ManagementServer vorhanden sind. Liegen aktualisierte Virensignaturen vor, werden diese automatisch auf dem Client installiert.
- **Programmdateien automatisch aktualisieren**: Aktiviert die automatische Aktualisierung der Client-Programmdateien. Die Clients prüfen bei jedem **Synchronisationsintervall**, ob aktualisierte Programmdateien auf dem ManagementServer vorhanden sind. Liegen aktualisierte Programmdateien vor, werden diese automatisch auf dem Client installiert.

AntiVirus Schutz

Setzen Sie das Häkchen bei **Zugriffs-Scan** um die Virenprüfung zu aktivieren. Der **Zugriffs-Scan** prüft alle Mails, Anhänge und Objekte auf Malware, unmittelbar bevor sie verschickt oder empfangen werden. Im Fall einer Malware-Infektion werden die unter **Scan-Einstellungen** definierten Maßnahmen ausgeführt.

Scan-Einstellungen

Die Scan-Einstellungen ähneln den **Wächter**- und **Scanauftrag**-Einstellungen.

- **Engines benutzen**: Die Scans benutzen entweder einen oder beide Engines. Es wird empfohlen, beide Engines zu benutzen.
- **Im Falle einer Infektion**: Das Exchange-Plugin kann infizierte Dateien auf mehrere Arten behandeln, ähnlich wie beim **Wächter**.
- **Dateitypen**: Um Scans zu beschleunigen, können sie auf Programmdateien und Dokumente

beschränkt werden. Es wird jedoch empfohlen, alle Dateien zu überprüfen.

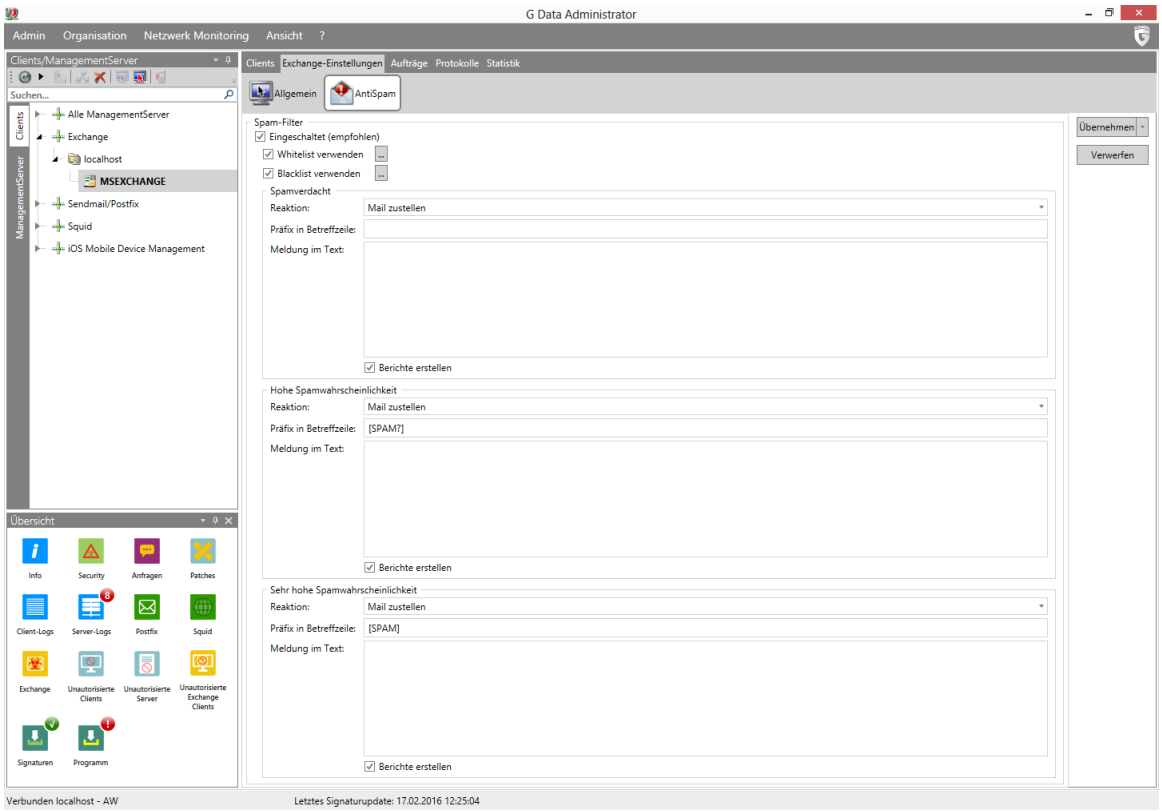
- **Heuristik verwenden**: Mithilfe von Heuristik kann Malware auf Basis von Verhalten erkannt werden.
- **Archive prüfen**: Archive können Malware beinhalten. Wenn eine oder mehrere Dateien innerhalb eines Archives infiziert sind, wird das Archiv als Ganzes desinfiziert oder entfernt, ggf. einschließlich sauberer Dateien. Wenn Sie Quarantäne-Maßnahmen konfiguriert haben, wird die ganze E-Mail-Nachricht (inklusive Archive) in die Quarantäne verschoben.

4.3.5.2. AntiSpam

Mit Hilfe der AntiSpam-Einstellungen können Sie Spam-Berichte noch bevor sie den Empfänger erreichen herausfiltern lassen. AntiSpam ist nur verfügbar auf Exchange-Servern, die die Hub Transport-Rolle ausführen.

Spam-Berichte werden in drei verschiedene Kategorien eingeteilt: **Spamverdacht**, **Hohe Spamwahrscheinlichkeit** und **Sehr hohe Spamwahrscheinlichkeit**. Für jede Kategorie können Sie festlegen, wie das Exchange-Plugin reagiert:

- **Reaktion**:
  - **Mail zustellen**: Die E-Mail-Nachricht wird zugestellt.
  - **Mail in Quarantäne verschieben**: Die E-Mail-Nachricht wird in den Quarantäne-Ordner verschoben.
  - **Mail zurückweisen**: Die E-Mail-Nachricht wird zurückgewiesen.
  - **Mail in Spamordner verschieben**: Die E-Mail-Nachricht wird in den Spamordner verschoben.
- **Präfix in Betreffzeile**: Es wird ein Präfix zu der Betreffzeile hinzugefügt (wie z. B. *[SPAM?]*).
- **Meldung im Text**: Es wird eine Meldung zum E-Mail-Text hinzugefügt.
- **Berichte erstellen**: Es wird ein Bericht zu den **Sicherheitsereignissen** hinzugefügt.



Zusätzlich zu den drei Spam-Kategorien können Sie eine Whitelist und eine Blacklist konfigurieren. E-Mail-Nachrichten von Adressen oder Domänen auf der Whitelist werden nie auf Spam untersucht; Adressen und Domänen auf der Blacklist werden immer als **Sehr hohe Spamwahrscheinlichkeit** behandelt. Die White- und Blacklist können als .json-Datei importiert und exportiert werden.

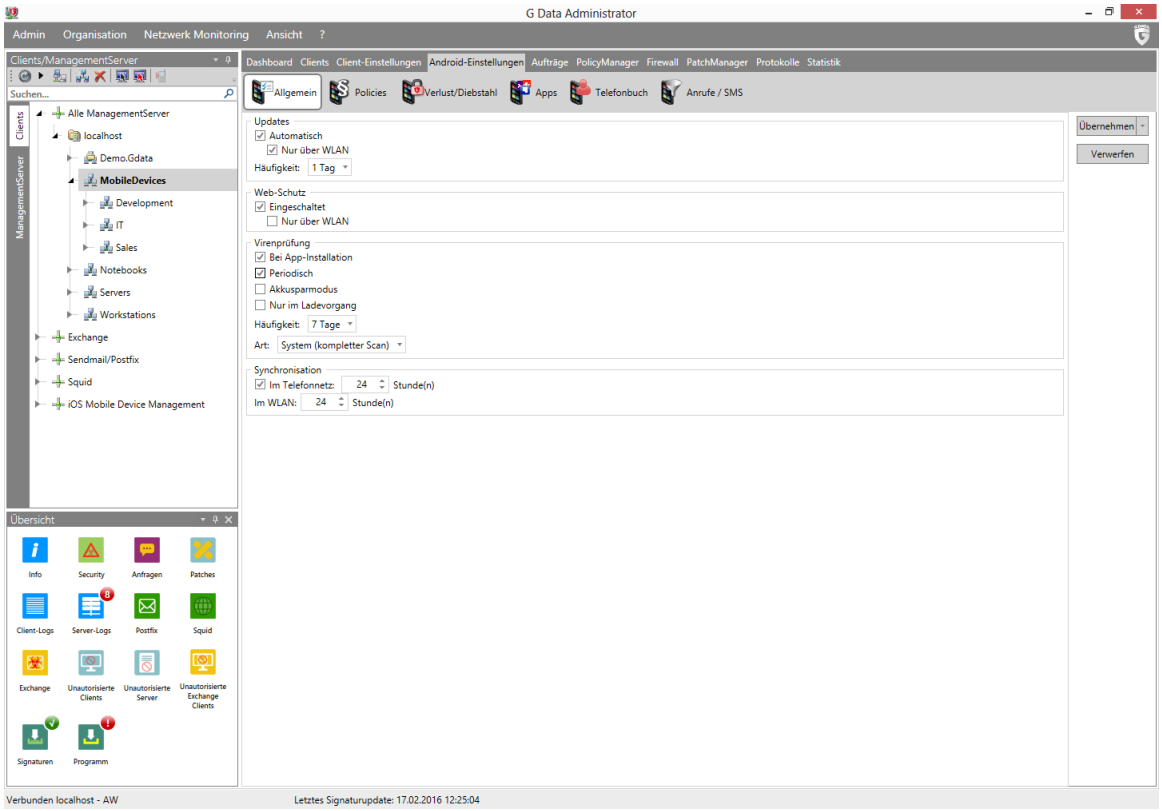
4.3.6. Android-Einstellungen

Das Modul Android-Einstellungen bietet einfachen Zugang zu den Möglichkeiten des G DATA Administrators, Android-Geräte zu administrieren.

4.3.6.1. Allgemein

Die Registerkarte Allgemein bietet Einstellungen für automatische Updates, Web-Schutz, Virenprüfung und Synchronisation sowie zwei allgemeine Geräte-Management-Optionen.

- **Beschreibung**: Geben Sie hier ggf. ergänzende Informationen zum Client ein.
- **Gerätename**: Geben Sie hier einen Gerätenamen ein.



Updates

Der Abschnitt Updates deckt Einstellungen in Bezug auf Updates ab.

- **Automatisch**: Hier können Sie festlegen, ob der Android-Client automatisch nach Software- und Virensignaturen suchen soll. Wenn Updates nicht automatisch heruntergeladen werden sollen, kann der Benutzer diese trotzdem noch manuell aktualisieren. Falls Sie sich für eine automatische Aktualisierung entscheiden, können Sie des Weiteren festlegen, wie oft dies zu erfolgen hat (**Häufigkeit**) und ob eine Aktualisierung **Nur über WLAN** erfolgen soll oder auch über das Mobilfunknetz.

Web-Schutz

Der Web-Schutz blockt Phishing-Webseiten, so dass diese im Android-Browser und Chrome nicht geöffnet werden können. Da der Web-Schutz immer auch ein gewisses Datenvolumen nach sich zieht,

kann er so eingestellt werden, dass er nur dann aktiv ist, wenn das Smartphone WLAN nutzt. Der Web-Schutz-Abschnitt umfasst deswegen auch die Möglichkeit, den Web-Schutz auf WLAN-Netze zu begrenzen.

- **Eingeschaltet**: Legen Sie hier fest, ob Android-Geräte beim Zugriff aufs Internet vom Web-Schutz geschützt werden sollen. Dies kann wahlweise als genereller Schutz eingestellt werden oder nur wenn der Internetzugriff über WLAN erfolgt.

Virenprüfung

Der Bereich Virenprüfung ermöglicht Ihnen, Parameter für On-Demand-und On-Access-Virenscans zu definieren.

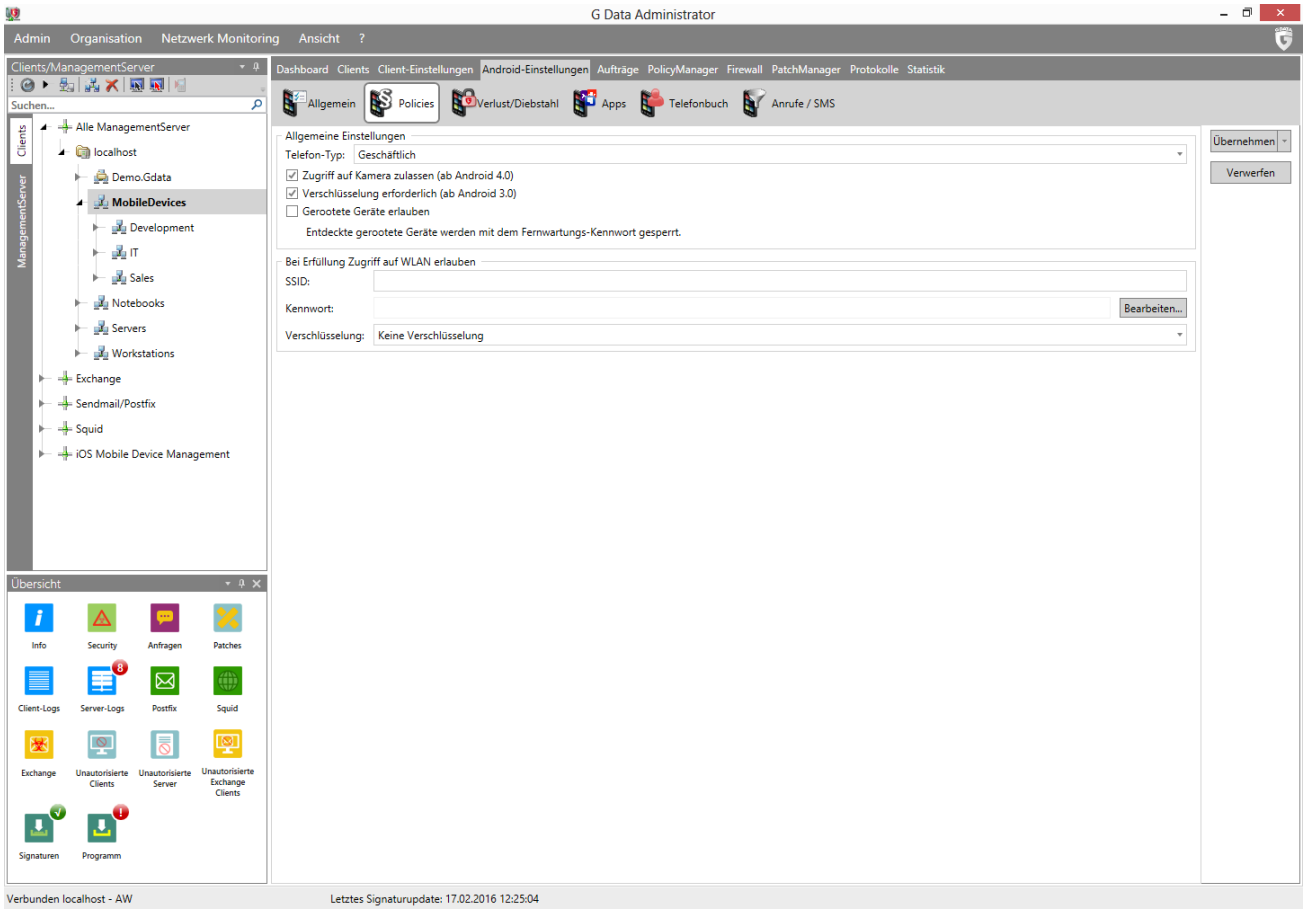
- **Bei App-Installation**: Hier können Sie festlegen, dass neu installierte Applikationen automatisch überprüft werden.
- **Periodisch**: Hier können Sie einen periodischen Scan definieren. Aktivieren Sie dazu das Kontrollkästchen Periodisch und legen Sie dann die **Häufigkeit** fest.
- **Akkusparmodus**: Setzen Sie den periodischen Scan aus, solange Ihr Smartphone im Akkusparmodus läuft.
- **Nur im Ladevorgang**: Hier können Sie festlegen, dass der periodische Scan nur dann durchgeführt wird, wenn sich das Mobilgerät im Ladezustand befindet.
- **Art**: Hier können Sie festlegen, ob nur **Installierte Anwendungen** gescannt werden sollten oder das **System (kompletter scan)**.

Synchronisation

Die Option Synchronisation legt fest, wie oft der Android-Client seine Daten mit dem ManagementServer synchronisiert. Geben Sie hier den Aktualisierungszyklus in Stunden an und entscheiden Sie, ob eine Synchronisation nur über WLAN oder auch über das Telefonnetz erfolgen soll.

4.3.6.2. Policies

Sie haben die Möglichkeit, Policies für verschiedene Handy-Typen zu definieren und damit Ihr Unternehmensnetzwerk zu schützen.



Allgemeine Einstellungen

Unter Allgemeine Einstellungen, wählen Sie den **Telefon-Typ** aus, zu dem das ausgewählte Gerät gehört. Dies entscheidet über das Profil, das von G DATA Internet Security für Android verwendet wird:

- **Geschäftlich**: G DATA Internet Security für Android wird die Einstellungen aus dem geschäftlichen Profil, welches regelmäßig mit dem ManagementServer synchronisiert wird, verwenden. Der Benutzer erhält keinen Zugriff auf die Einstellungen. Diese Einstellung ist die empfohlene Einstellung für Geräte, die von Ihrem Unternehmen ausgegeben werden.
- **Privat**: G DATA Internet Security für Android wird die Einstellungen aus dem privaten Profil, der nicht mit dem ManagementServer synchronisiert wird, verwenden. Der Benutzer erhält Zugriff auf alle Einstellungen in G DATA Internet Security für Android.
- **Gemischt**: Der Benutzer kann frei zwischen dem geschäftlichen und den privaten Profil wechseln.

  Vorsicht: Wenn Sie den Typ **Privat** oder **Gemischt** auswählen, hat der Benutzer des Geräts Zugriff auf Funktionalität, die nicht zentral verwaltet werden kann. Für zentral verwaltete Geräte wird die Benutzung des Typs **Geschäftlich** empfohlen.

Ganz unabhängig vom Telefontyp können folgende Funktionen verwaltet werden:

- **Zugriff auf Kamera zulassen** (ab Android 4.0): Ermöglicht den Zugriff auf die Handykamera (Android 4.0 und höher) zu deaktivieren.
- **Verschlüsselung erforderlich** (ab Android 3.0): Hier muss die volle Geräteverschlüsselung aktiviert sein (Android 3.0 und höher).
- **Gerootete Geräte erlauben**: Erlauben oder verbieten Sie hier gerootete Geräte. Wenn die Funktion deaktiviert ist, werden gerootete Geräte mit dem Passwort blockiert, welches Sie unter **Verlust/Diebstahl** definiert haben. Außerdem wird gerooteten Geräten Zugriff auf das WLAN

verweigert, welches Sie unter **Bei Erfüllung Zugriff auf WLAN erlauben** definiert haben.

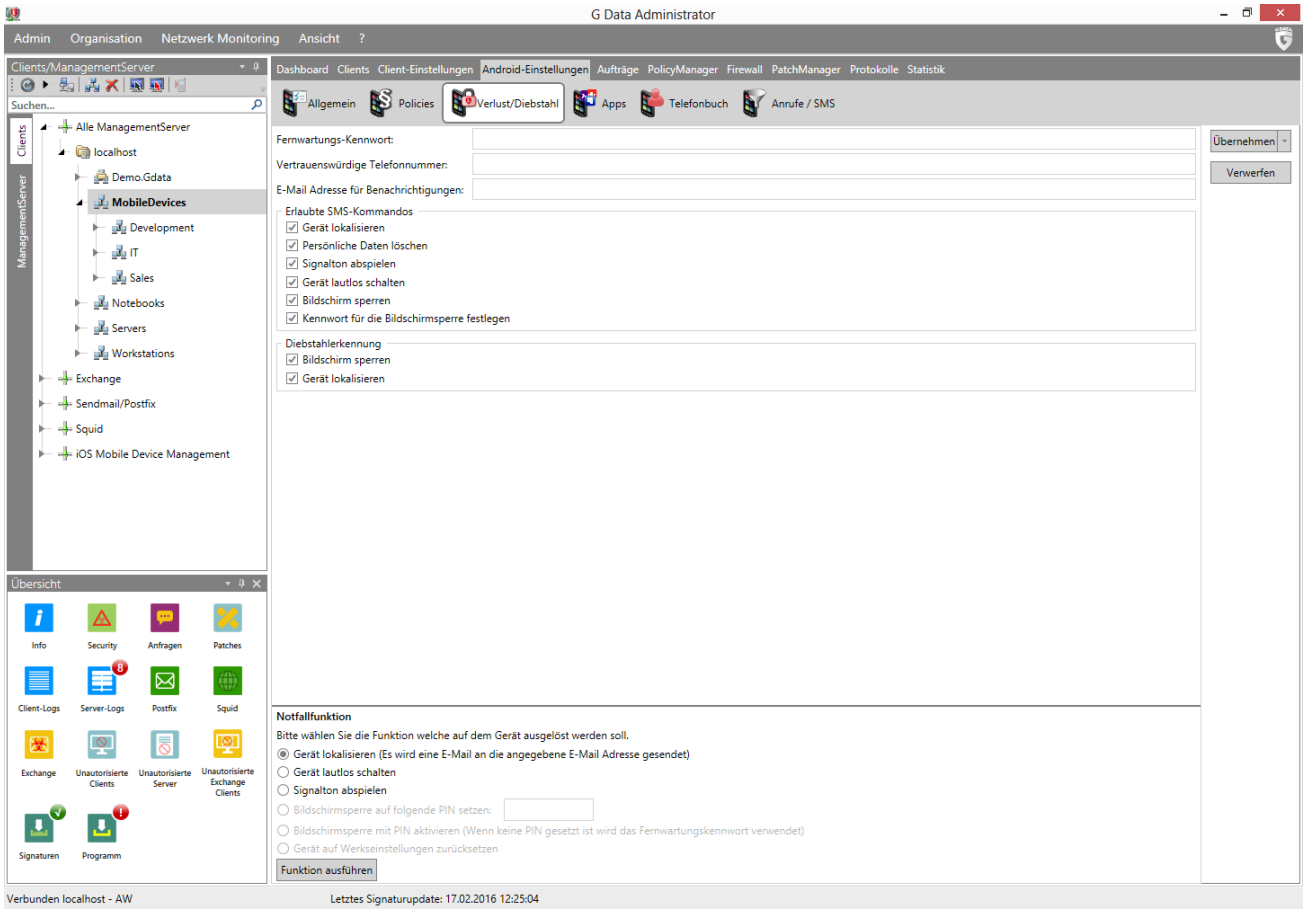
Bei Erfüllung Zugriff auf WLAN erlauben
Der Zugang zu einem bestimmten WLAN-Netzwerk kann gerooteten Geräten untersagt werden. Dies ermöglicht es Ihnen den Zugriff auf das Unternehmens-WLAN-Netzwerk nur für diejenigen Geräte zu erlauben, die die Unternehmensrichtlinien erfüllen.

Geben Sie die **SSID** für das Firmennetzwerk ein, für das der Zugang aktiviert werden soll. Wählen Sie die **Verschlüsselung** und vergeben Sie das **Kennwort** (wenn das Netzwerk verschlüsselt ist).

4.3.6.3. Verlust/Diebstahl

Um verlorene oder gestohlene Mobilgeräte zu schützen, bietet die Internet Security-App verschiedene Maßnahmen an, die ferngesteuert über SMS aktiviert werden können. Geräte, die gestohlen oder verloren werden, können aus der Ferne gesperrt, gelöscht oder lokalisiert werden. Diese Funktion aktivieren Sie durch das Senden einer SMS mit entsprechenden Befehlen an das verlorene Gerät. Über die Firebase Cloud Messaging-Funktion können diese Anti-Diebstahl-Funktionen auch jederzeit manuell ausgelöst werden.

Vor der Eingabe von Diebstahlschutz-Maßnahmen, sollten einige allgemeine Einstellungen vorgenommen werden. Das **Fernwartungs-Kennwort** (ein Zahlen-PIN-Code) ist notwendig, damit Sie sich per SMS gegenüber Ihrem Smartphone identifizieren können. Auf diese Weise wird verhindert, dass andere Personen unautorisiert Sperrbefehle oder dergleichen an Ihr Gerät senden. Ein weiteres Sicherheitsfeature ist eine **Vertrauenswürdige Telefonnummer**. Sie können das Fernwartungs-Kennwort ferngesteuert ändern, aber nur über die Telefonnummer, welche Sie hier vorher eingegeben haben. Antworten und Informationen, die durch die **Erlaubte SMS-Kommandos** ausgelöst werden, werden per SMS an das Gerät geschickt, von dem das Kommando geschickt wurde. Optional können sie auch an eine **E-Mail Adresse für Benachrichtigungen** geschickt werden. Falls Sie eine oder mehrere Optionen der **Diebstahlerkennung** aktiviert haben, werden ggf. Standortinformationen per E-Mail an diese Adresse geschickt.



Erlaubte SMS-Kommandos

Hier können Sie festlegen, welche Aktionen mit Ihrem Smartphone ausgeführt werden dürfen, sobald Sie diesem ein SMS-Kommando zuschicken. Setzen Sie hierzu Häkchen bei den Funktionen, die Sie aktivieren möchten:

- **Gerät lokalisieren**: Hiermit können Sie sich die Position des gestohlenen/verlorenen Gerätes per SMS senden lassen. Wenn unter **Verlust/Diebstahl** eine E-Mail-Adresse eingegeben wurde, wird die Position auch an diese Adresse gesendet. Zum Aktivieren dieses Kommandos senden Sie eine SMS mit dem Textinhalt: *Kennwort***locate**.
- **Persönliche Daten löschen**: Hiermit können Sie Ihr gestohlenes/verlorenes Handy auf den Werkszustand zurücksetzen. Alle persönlichen Daten werden dabei gelöscht. Zum Aktivieren dieses Kommandos senden Sie eine SMS mit dem Textinhalt: *Kennwort***wipe**.
- **Signalton abspielen**: Über diese Funktion kann ein akustisches Signal abgespielt werden, bis Internet Security für Android gestartet wird. Dies erleichtert das Auffinden eines verlorenen Handys. Zum Aktivieren dieses Kommandos senden Sie eine SMS mit dem Textinhalt: *Kennwort* **ring**.
- **Gerät lautlos schalten**: Wenn Sie nicht möchten, dass Ihr gestohlenes/verlorenes Smartphone durch Klingel- oder Systemtöne auf sich aufmerksam macht, können Sie es hiermit lautlos stellen. Die Funktionalität des Signaltons zum Wiederfinden des Geräts wird dabei natürlich nicht beeinträchtigt. Zum Aktivieren dieses Kommandos senden Sie eine SMS mit dem Textinhalt: *Kennwort***mute**.
- **Bildschirm sperren**: Hiermit können Sie den Bildschirm Ihres gestohlenen/verlorenen Smartphones sperren. Eine Nutzung des Smartphones ist so nicht mehr möglich. Zum Aktivieren dieses Kommandos senden Sie eine SMS mit dem Textinhalt: *Kennwort***lock**. Sollte kein Passwort vergeben worden sein, wird hier das Passwort verwendet, welches Sie im Bereich Einstellungen vergeben haben.

- **Kennwort für die Bildschirmsperre festlegen**: Damit Sie selber wieder Zugang zu Ihrem Smartphone erhalten, können Sie mit dieser Funktion ggf. das Kennwort für die Bildschirmsperre neu vergeben, wenn Sie das alte Passwort nicht mehr kennen. Zum Aktivieren dieses Kommandos senden Sie eine SMS mit dem Textinhalt: Kennwort **set device password:** *Gerätekennwort*.

Um das Fernwartungs-Kennwort ferngesteuert zu ändern, senden Sie eine SMS an Ihr Handy mit dem Gerät, dessen Nummer Sie unter **Vertrauenswürdige Telefonnummer** eingegeben haben. Das Kommando hierzu lautet: **remote password reset:** *NeuesKennwort*.

Diebstahlerkennung
Bei der Installation der Internet Security-App merkt sich diese, welche SIM-Karte bei der Installation in dem Mobilgerät vorhanden war. Wenn diese Karte gewechselt wird, weil das Gerät z. B. gestohlen und weiterverkauft wurde, können automatisch bestimmte Aktionen erfolgen:

- **Bildschirm sperren**: Gleiche Funktionalität wie die Optionen unter **Erlaubte SMS-Kommandos**.
- **Gerät lokalisieren**: Gleiche Funktionalität wie die Optionen unter **Erlaubte SMS-Kommandos**.

Notfallfunktion
Mit dem Internet-basierten Firebase Cloud Messaging Framework können Notfallmaßnahmen auf Android-Mobilgeräten ausgelöst werden. Diese funktionieren selbst dann, wenn ein Mobilgerät ohne SIM-Karte genutzt wird. Vorher muss das Firebase Cloud Messaging allerdings unter **Allgemeine Einstellungen** > **Android** konfiguriert werden.

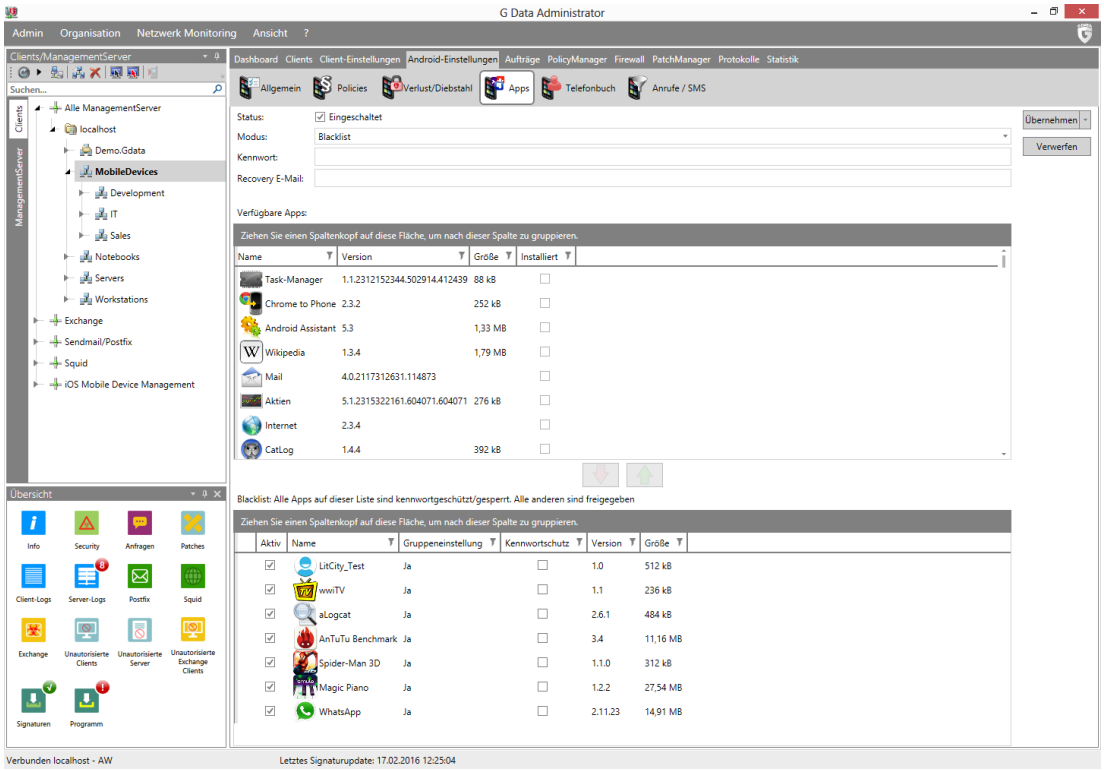
Wählen Sie die gewünschten Aktionen aus und klicken Sie auf **Funktion ausführen**, um den jeweiligen Befehl für die Aktion an das Mobilgerät zu senden:

- **Gerät lokalisieren**: Gleiche Funktionalität wie die Optionen unter **Erlaubte SMS-Kommandos**.
- **Gerät lautlos schalten**: Gleiche Funktionalität wie die Optionen unter **Erlaubte SMS-Kommandos**.
- **Signalton abspielen**: Gleiche Funktionalität wie die Optionen unter **Erlaubte SMS-Kommandos**.
- **Bildschirmsperre auf folgende PIN setzen**: Gleiche Funktionalität wie die Optionen unter **Erlaubte SMS-Kommandos**.
- **Bildschirmsperre mit PIN aktivieren**: Gleiche Funktionalität wie die Optionen unter **Erlaubte SMS-Kommandos**.
- **Gerät auf Werkseinstellungen zurücksetzen**: Gleiche Funktionalität wie die Optionen unter **Erlaubte SMS-Kommandos**.

4.3.6.4. Apps

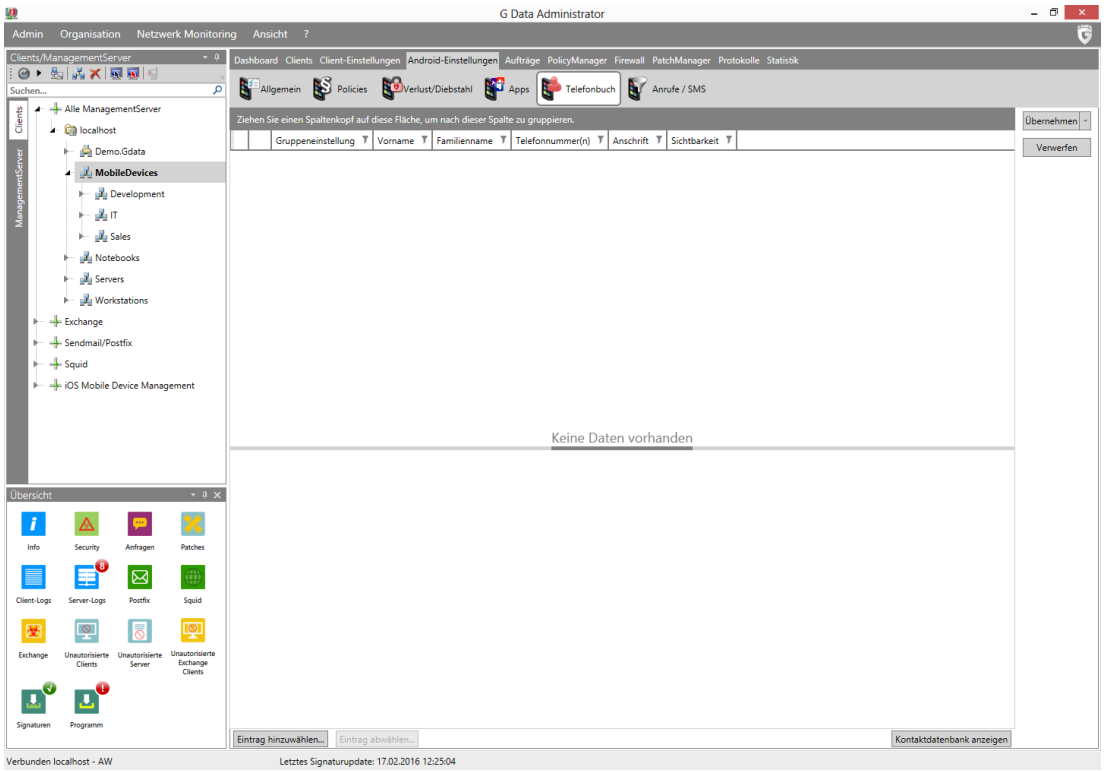
Das Apps-Panel ermöglicht Ihnen den Zugriff auf die App-Verwaltung Ihrer Mobilgeräte. Um Apps zu blockieren oder zu erlauben, müssen Sie zuerst entscheiden, ob der Filter für Apps im **Blacklist**- oder **Whitelist**-Modus verwendet werden soll. Im Blacklist-Modus werden nur die bestimmte Apps, die auf einer Blacklist gelistet sind, blockiert oder ihr Zugriff wird über ein Passwort eingeschränkt. Beliebige andere Apps können verwendet werden. Im Whitelist-Modus werden nur die Apps zugelassen, die sich auch auf dieser Whitelist befinden. Das **Kennwort** (ein PIN-Code) wird dazu verwendet, auf gesperrte Apps zugreifen zu können. Außerdem können Sie eine **Recovery E-Mail** angeben, an die Sie sich das Kennwort zuschicken lassen können, falls Sie es einmal vergessen sollten.

Über **Verfügbare Apps** werden alle Apps aufgelistet, die auf dem jeweiligen Mobilgerät installiert wurden. Bei jeder App sehen Sie den **Namen** der App, die **Version** und die **Größe**. Über die Pfeiltasten können Sie Apps von der White- auf die Blacklist verschieben und andersherum. Hier können Sie auch den **Kennwortschutz** für entsprechend gelistete Apps vergeben.



4.3.6.5. Telefonbuch

Das Telefonbuch-Panel ermöglicht die erweiterte Verwaltung von Kontakten. Kontakte können in der Internet Security App einem Adressbuch hinzugefügt werden und sowohl die Kontakte, als auch ihre Kommunikation können im Mobilgerät so versteckt werden, dass diese nicht im normalen Adress- und Telefonbuch zu sehen sind. In Kombination mit diesen Funktionen kann das Telefonbuch der Internet Security-App das offizielle Android-Telefonbuch vollständig ersetzen.

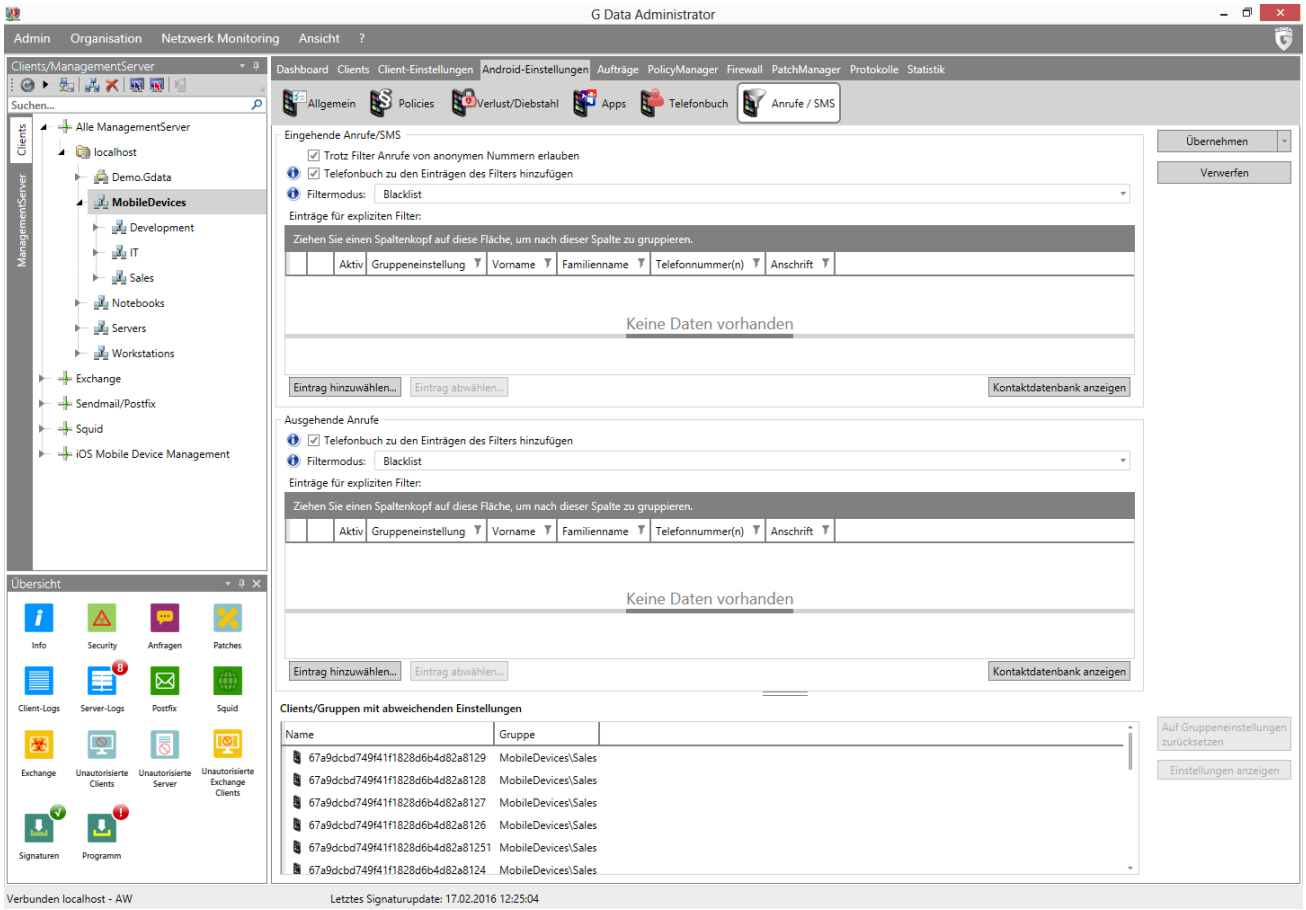


Die Hauptliste zeigt alle Kontakte, die dem Internet Security-Telefonbuch hinzugefügt wurden. Für jeden Kontakt sind die Felder **Vorname**, **Familienname**, **Telefonnummer(n)** und **Anschrift** aufgeführt. Über das Dropdown-Menü **Sichtbarkeit** können Sie festlegen, ob der jeweilige Kontakt im normalen Android-Telefonbuch angezeigt (**Sichtbar**) oder nicht angezeigt (**Versteckt**) wird. Darüber hinaus können Sie alle Anrufe und SMS-Nachrichten der betreffenden Kontakte über **Kommunikation versteckt** verstecken. Um einen Kontakt zum Telefonbuch hinzuzufügen, klicken Sie auf **Eintrag hinzuwählen**. Im **Kontaktdatenbank**-Fenster werden alle Kontakte angezeigt, welche definiert wurden. Wählen Sie einen oder mehrere Kontakte aus und klicken Sie auf **Auswählen**, um die Kontakte dem Telefonbuch hinzuzufügen. Um einen Kontakt aus dem Telefonbuch zu entfernen, klicken Sie bitte **Eintrag abwählen**.

Um einen Kontakt in der Kontakt-Datenbank hinzuzufügen, klicken Sie auf die Schaltfläche **Kontakt erstellen** in der Symbolleiste oder **Kontakte importieren**, um Kontakte aus der Active Directory Organizational Unit (OU) heraus zu importieren. Beim Erstellen eines Kontakts, sollten Sie mindestens **Vorname** oder **Familienname** angeben. Darüber hinaus können Sie eine oder mehrere Postanschriften hinzufügen, sowie E-Mail-Adressen, Telefonnummern, Faxnummern und Organisationen. Um einen Kontakt aus der Kontakt-Datenbank zu entfernen, wählen Sie diesen aus und klicken Sie auf das **Löschen**-Symbol in der Symbolleiste oder wählen die Option **Löschen** im Kontextmenü.

4.3.6.6. Anrufe / SMS

Der Anruf-Filter ermöglicht Ihnen, eingehende Anrufe und SMS-Nachrichten sowie ausgehende Anrufe zu filtern. Mit der gleichen Datenbank, die im **Telefonbuch**-Panel verwendet wird, können Sie ganz einfach Kontakte zu einer Blacklist oder Whitelist hinzufügen, sowie generelle Filter definieren.



Eingehende Anrufe/SMS

Unter Eingehende Anrufe/SMS können Sie definieren, wie Internet Security mit eingehender Kommunikation umgehen soll. Deaktivieren Sie **Trotz Filter Anrufe von anonymen Nummern erlauben**, um alle anonymen Anrufe zu blockieren. Wenn Sie die zusätzliche Option **Telefonbuch zu den Einträgen des Filters hinzufügen** wählen, wird zusätzlich zur Kommunikation mit Kontakten auf der Whitelist auch die Kommunikation mit Nummern aus den Android- und Internet Security-Telefonbüchern erlaubt.

Über die Funktion **Filtermodus** können Sie bestimmte Maßnahmen für eingehende Anrufe und SMS-Nachrichten definieren. Wählen Sie **Blacklist**, um die Kommunikation mit allen Kontakten zu erlauben, bis auf die, welche sich auf der Blacklist befinden oder wählen Sie **Whitelist**, um den Kontakt nur mit Kontakten zu erlauben, die auf der Whitelist gelistet sind. Durch das Anklicken von **Eintrag hinzuwählen**, können Sie jeden Kontakt aus der Kontakt-Datenbank zur jeweiligen Liste hinzufügen und über **Eintrag abwählen** aus der Liste entfernen.

Ausgehende Anrufe

Unter Ausgehende Anrufe können Sie definieren, wie Internet Security ausgehende Anrufe behandeln soll. Wenn Sie den zusätzlichen Filter **Telefonbuch zu den Einträgen des Filters hinzufügen** wählen, können zusätzlich zu den Kontakten auf der Whitelist auch Kontakte aus den Android- und Internet Security-Telefonbüchern kontaktiert werden.

Über die Funktion **Filtermodus** können Sie bestimmte Maßnahmen für eingehende Anrufe und SMS-Nachrichten definieren. Wählen Sie **Blacklist**, um die Kommunikation mit allen Kontakten zu erlauben, bis auf die, welche sich auf der Blacklist befinden oder wählen Sie **Whitelist**, um den Kontakt nur mit Kontakten zu erlauben, die auf der Whitelist gelistet sind. Durch das Anklicken von **Eintrag hinzuwählen**, können Sie jeden Kontakt aus der Kontakt-Datenbank zur jeweiligen Liste hinzufügen und über **Eintrag abwählen** aus der Liste entfernen.

Falls ein Benutzer versucht, eine gesperrte Nummer anzurufen, wird er über die Sperrung informiert und ihm wird die Möglichkeit angeboten, die Freigabe der Nummer anzufordern. Dieser Vorgang fügt einen Bericht im **Sicherheitsereignisse**-Modul hinzu, über den der Administrator dann direkt einen Blacklist- oder Whitelist-Eintrag erstellen kann.

4.3.7. iOS-Einstellungen

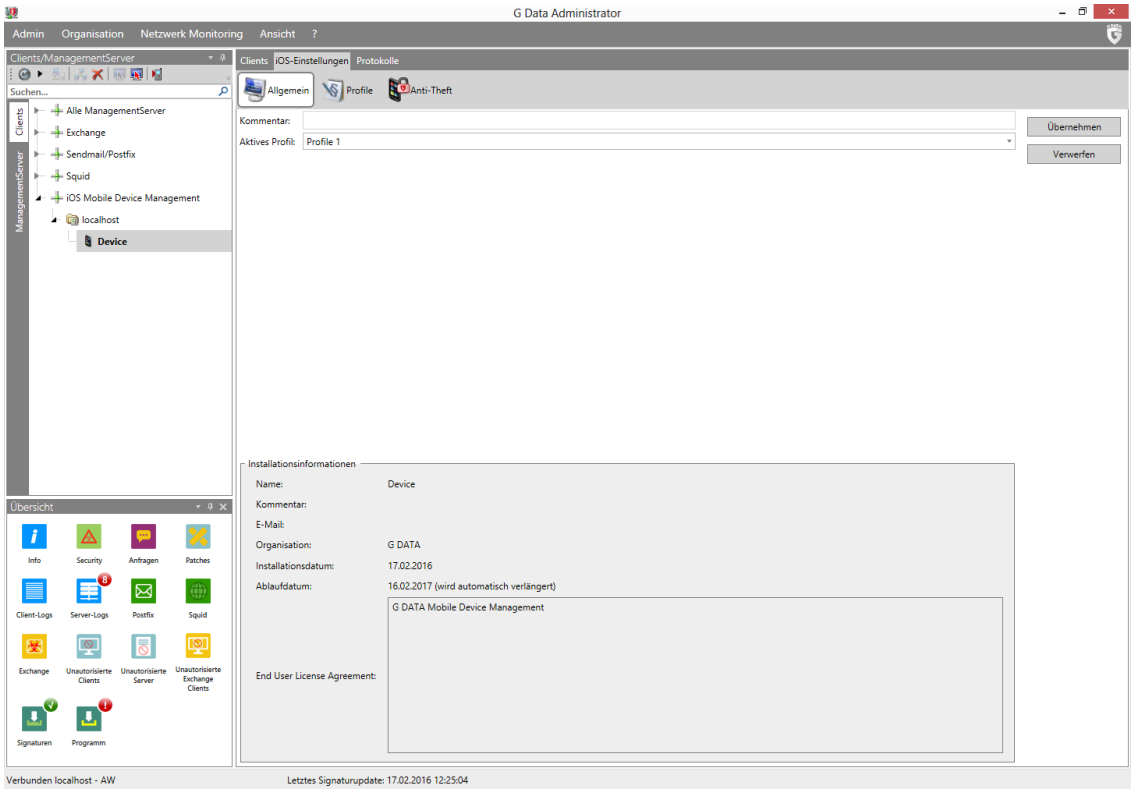
Das Modul iOS-Einstellungen bietet einfachen Zugang zu den Möglichkeiten des G DATA Administrators, iOS-Geräte zu administrieren.

4.3.7.1. Allgemein

Mit Hilfe der Allgemein-Registerkarte können Sie eine Beschreibung eingeben und ein Profil zuweisen.

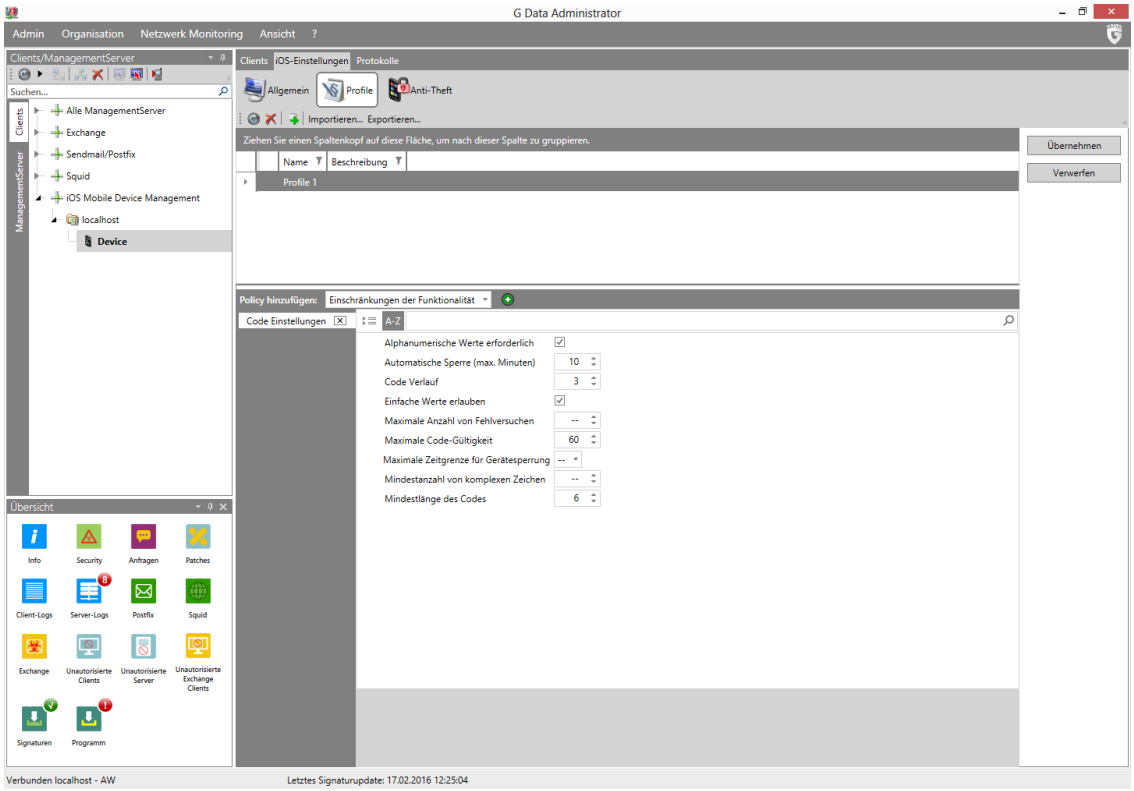
- **Beschreibung**: Geben Sie eine Beschreibung ein, z. B. Informationen über das Gerät oder seine Konfiguration. Die Beschreibung wird nur in G DATA Administrator angezeigt.
- **Aktives Profil**: Das aktuell zugewiesene **Profil**. Wählen Sie ein Profil aus der Liste um das Profil zu ändern oder wählen Sie **- Kein Profil -** um das aktuelle Profil zu löschen.

Zusätzlich zu der Beschreibung und dem Profil zeigt die Allgemein-Registerkarte auch einige Einstellungen an, die konfiguriert wurden als die Geräteverwaltung auf dem Gerät aktiviert wurde. Dazu gehören der Geräteverwaltungsnamen, die Beschreibung, die Organisation sowie die End User License Agreement.



4.3.7.2. Profile

Mit Hilfe von Profilen können Sie iOS-Geräten oder -Gerätegruppen Sicherheitspolicies zuweisen. Klicken Sie auf die **Profil hinzufügen**-Schaltfläche, um ein neues Profil zu definieren, indem Sie den **Namen** und eine **Beschreibung** (optional) eingeben. Jedes Profil kann bis zu fünf Policies beinhalten. Jede Policy ist spezialisiert auf eine bestimmte Kategorie mit Einstellungen. Unter **Policy hinzufügen** wählen Sie eine der fünf Policies und klicken Sie das Plus-Symbol, um die Policy zum Profil hinzuzufügen:



- **Einschränkungen der Funktionalität**: Spezifische Funktionen des iOS-Gerätes werden gesperrt (wie z. B. die Camera-Benutzung, Siri oder iCloud).

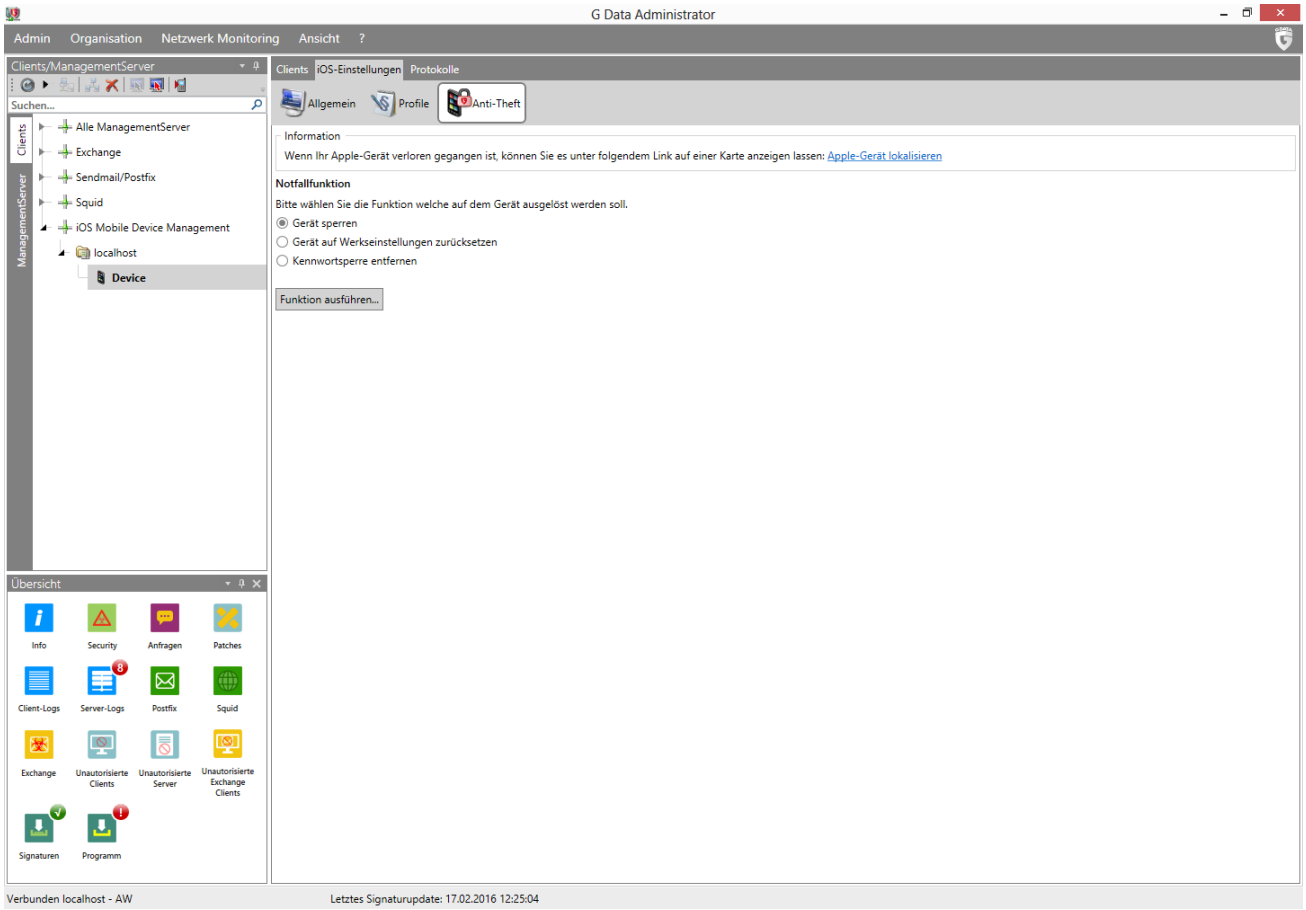
- **App-Einschränkungen**: Spezifische Apps oder App-Funktionen werden gesperrt (wie z. B. YouTube, iTunes Store oder Safari).
- **Einschränkungen für mediale Inhalte**: Spezifische mediale Inhalte werden gesperrt, auf Basis von Altersfreigaberegionen.
- **Code-Einstellungen**: Erzwinge Standards für die iOS-Passcode (wie z. B. die Mindestlänge, Mindestanzahl von komplexen Zeichen oder maximale Anzahl von Fehlversuchen).
- **WLAN**: Das iOS-Gerät darf sich mit dem definierten WLAN-Netzwerk verbinden.

Wählen Sie eine Policy aus, um die jeweiligen Einstellungen zu bearbeiten. Klicken Sie auf **Übernehmen**, um das Profil und alle Policies zu speichern. Wenn Sie ein Profil, das schon einem Gerät zugewiesen wurde, bearbeiten, wird das aktualisierte Profil mit dem Gerät synchronisiert. Sobald das Gerät das Profil übernommen hat, wird dem **Protokolle (iOS)**-Modul ein Bericht hinzugefügt.

Profile können im- und exportiert werden, indem Sie auf die jeweilige Schaltfläche klicken. Die Einstellungen werden als JSON-Datei gespeichert.

4.3.7.3. Anti-Theft

Über die Anti-Theft-Registerkarte können Sie auf dem ausgewählten iOS-Gerät Antidiebstahlmaßnahmen ausführen:



- **Gerät sperren**: Der Sperrbildschirm des Gerätes wird eingeschaltet (inklusive Passcode-Sperrung, falls gesetzt).
- **Gerät auf Werkseinstellungen zurücksetzen**: Das Gerät wird auf Werkseinstellungen zurückgesetzt. Warnung: Diese Funktion entfernt alle Daten und deaktiviert auch die Geräteverwaltung.
- **Passcode entfernen**: Der Passcode des Gerätes wird entfernt.

Klicken Sie auf **Funktion ausführen**, um die ausgewählte Antidiebstahlfunktion auszuführen. Der Status wird unter **Protokolle (iOS)** angezeigt.

4.3.8. Sendmail/Postfix

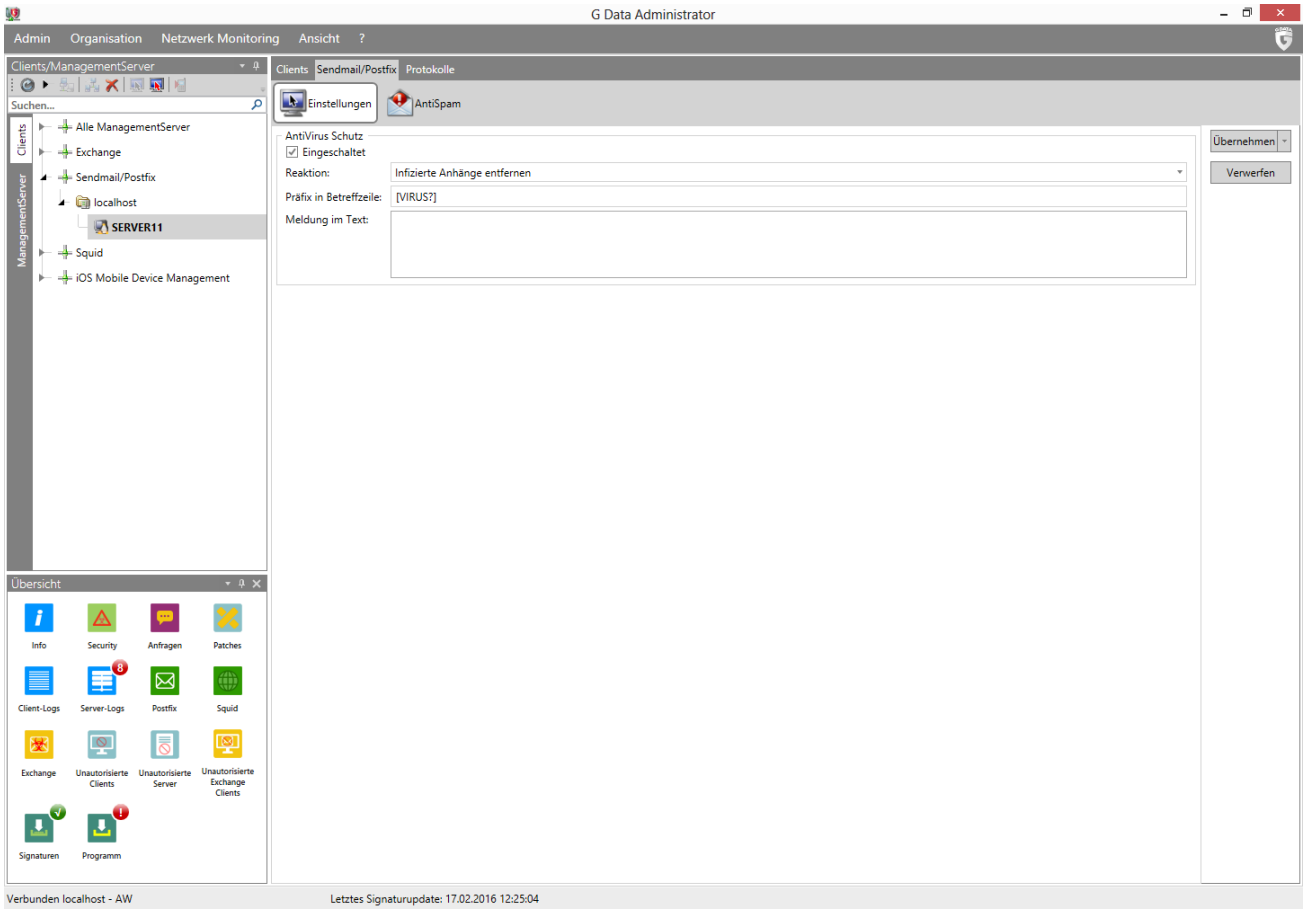
Das Linux Mail Security Gateway ist als **optionales Modul** verfügbar.

Mit dem Modul Sendmail/Postfix können Sie die Einstellungen des Linux Mail Security Gateways konfigurieren.

4.3.8.1. Einstellungen

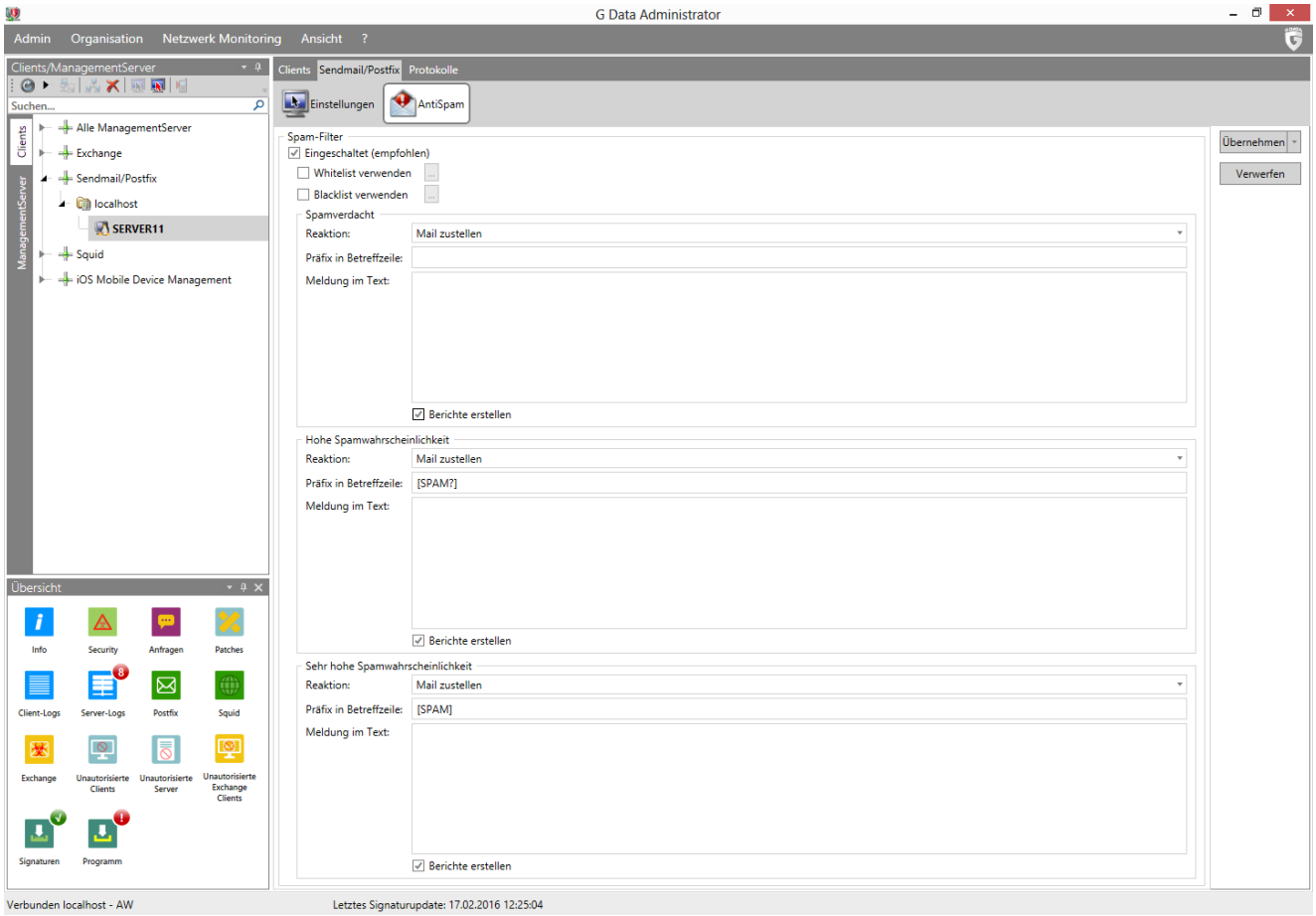
Unter Einstellungen sind die folgenden Funktionen des Virenschutzes verfügbar:

- **Reaktion**: Legen Sie die Reaktion auf infizierte E-Mails fest (**Infizierte Anhänge entfernen** oder **Nachricht in Quarantäne verschieben**).
- **Präfix in Betreffzeile**: Es wird ein Präfix zu der Betreffzeile hinzugefügt (z. B. *[VIRUS]*).
- **Meldung im Text**: Es wird eine Meldung zum E-Mail-Text hinzugefügt (z. B. *Diese E-Mail ist infiziert*).



4.3.8.2. AntiSpam

Das Linux Mail Security Gateway prüft automatisch alle eingehenden Nachrichten auf Spam. Den Schutz können Sie unter AntiSpam konfigurieren.



Spam-Berichte werden in drei verschiedene Kategorien eingeteilt: **Spamverdacht**, **Hohe Spamwahrscheinlichkeit** und **Sehr hohe Spamwahrscheinlichkeit**. Für jede Kategorie können Sie festlegen, wie das Plugin reagiert:

- **Reaktion**:
  - **Mail zustellen**: Die E-Mail-Nachricht wird zugestellt.
  - **Nachricht entfernen**: Die E-Mail-Nachricht wird entfernt.
- **Präfix in Betreffzeile**: Es wird ein Präfix zu der Betreffzeile hinzugefügt (wie z. B. *[SPAM?]*).
- **Meldung im Text**: Es wird eine Meldung zum E-Mail-Text hinzugefügt.
- **Berichte erstellen**: Es wird ein Bericht zu den **Sicherheitsereignissen** hinzugefügt.

Zusätzlich zu den drei Spam-Kategorien können Sie eine Whitelist und eine Blacklist konfigurieren. E-Mail-Nachrichten von Adressen oder Domänen auf der Whitelist werden nie auf Spam untersucht; Adressen und Domänen auf der Blacklist werden immer als **Sehr hohe Spamwahrscheinlichkeit** behandelt. Die White- und Blacklist können als .json-Datei importiert und exportiert werden.

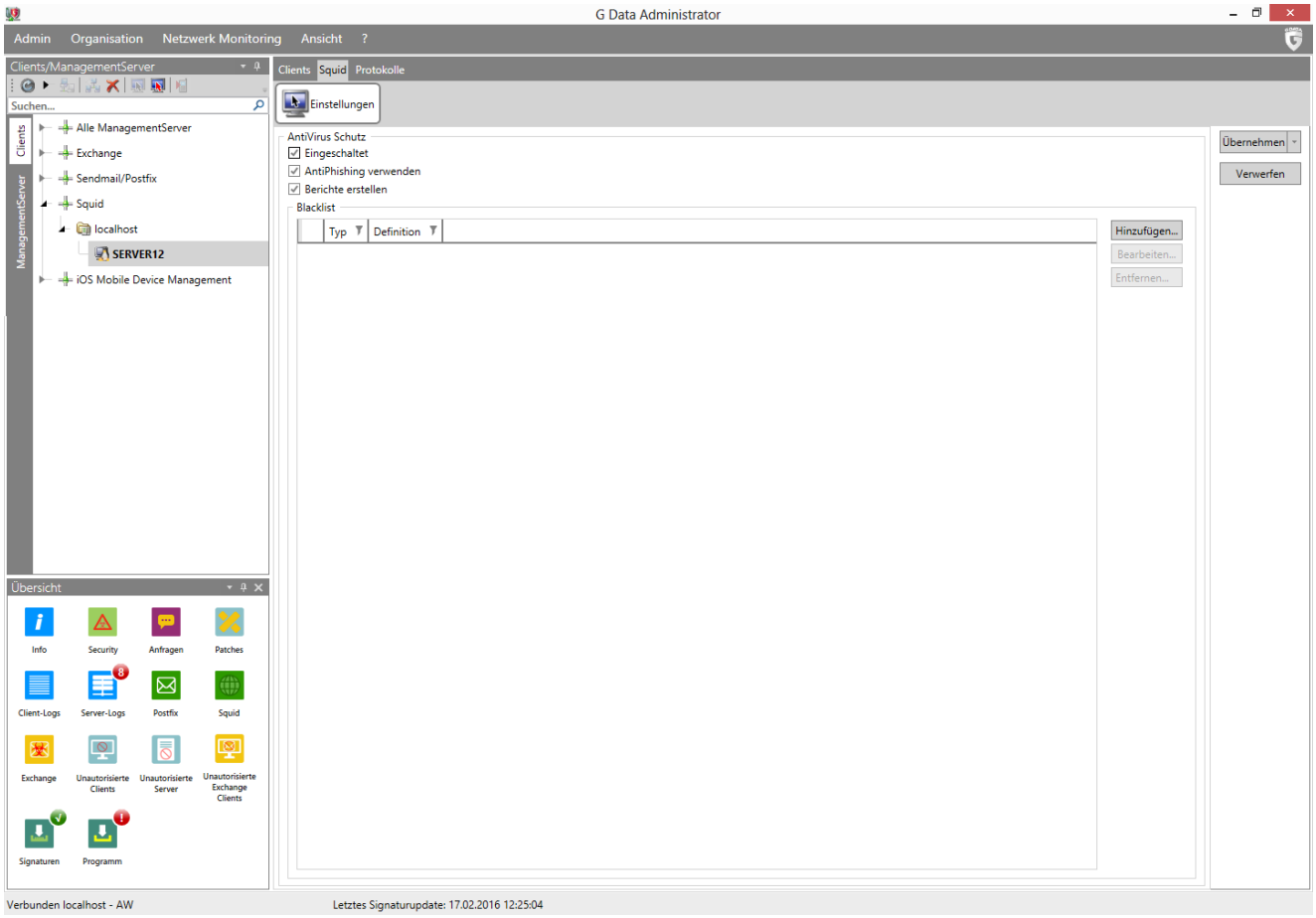
4.3.9. Squid

Das Linux Web Security Gateway ist als **optionales Modul** verfügbar.

Mit dem Modul **Squid** können Sie die Einstellungen des Linux Web Security Gateways konfigurieren. Unter **AntiVirus Schutz** lassen sich folgende Einstellungen setzen:

- **Eingeschaltet**: Der Virenschutz für Squid ist eingeschaltet.
- **AntiPhishing verwenden**: Aktiviert Cloud-Abfragen um den Schutz zu verbessern.
- **Berichte erstellen**: Beim Virenfund wird ein Bericht zu den **Sicherheitsereignissen**

hinzugefügt.



Klicken Sie unter **Blacklist** auf **Hinzufügen** um eine **Domäne** oder **IP-Adresse des Proxy-Clients** oder einen **MIME-Typ** zur Blacklist hinzuzufügen. Blacklist-Einträge werden immer blockiert.

4.3.10. Aufträge

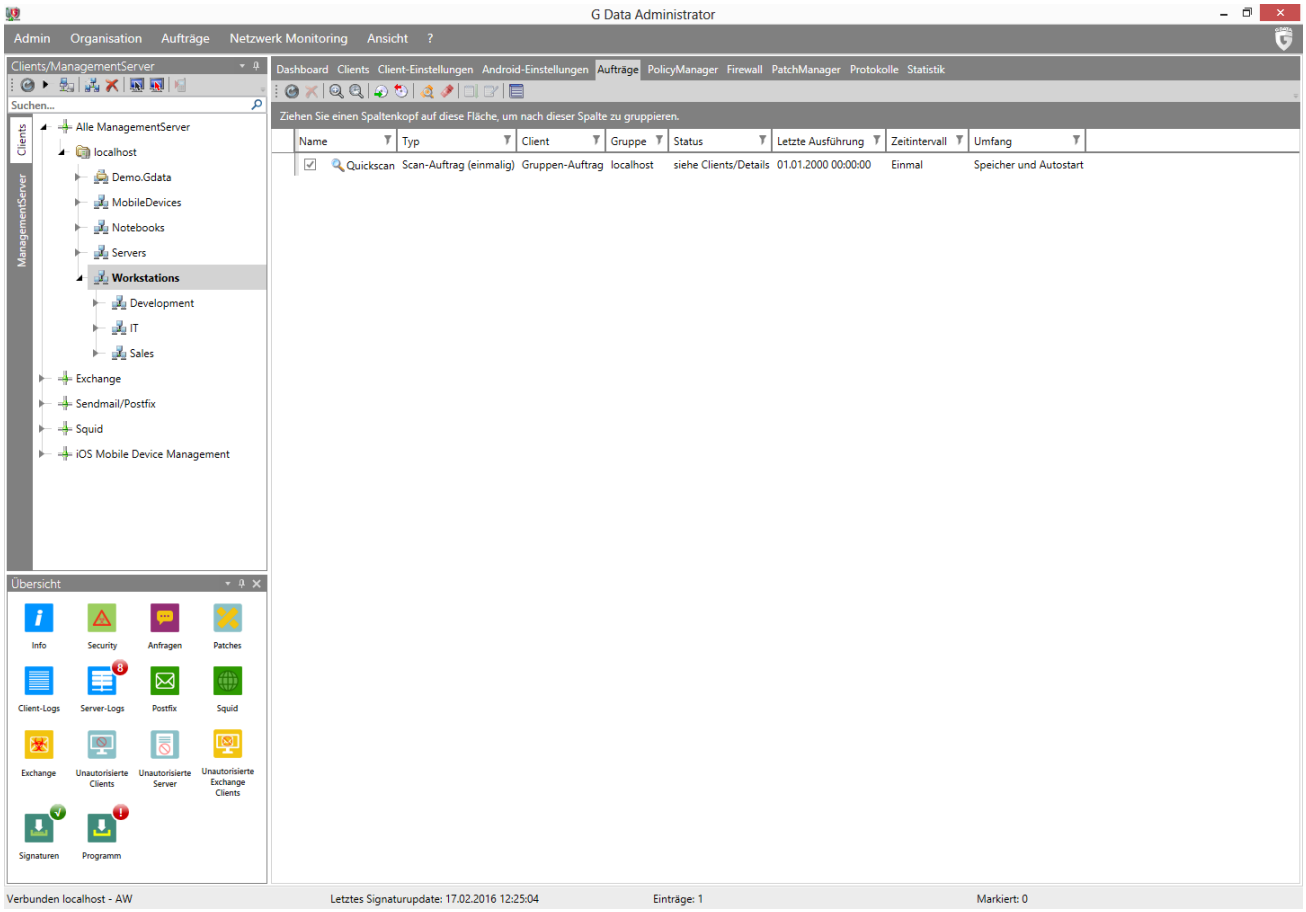
In diesem Bereich werden Aufträge für Clients und Gruppen definiert. Es gibt zwei unterschiedliche Auftragsarten: Einmalige Aufträge und periodische Aufträge. Die einmaligen Jobs werden einmal zum festgelegten Zeitpunkt ausgeführt, für die periodischen wird ein Zeitplan definiert, nach dem sie ausgeführt werden sollen. Sie können beliebig viele unterschiedliche Aufträge definieren. Generell ist es aus Gründen der Performance allerdings sinnvoll, dass sich die Zeitplanungen der Aufträge nicht überschneiden.

Im Bereich Aufträge werden für alle Aufträge die folgenden Daten angezeigt:

- **Name**: Der von Ihnen vorgegebene Name für den Job. Sie können hier beliebig lange Namen eingeben und auf diese Weise Ihren Job genau beschreiben, um bei vielen verschiedenen Jobs den Überblick zu behalten.
- **Typ**: Der Typ des Auftrags, z. B. Scan-Auftrag oder Softwareerkennungsauftrag.
- **Client**: Der Name des jeweiligen Clients. Sie können Jobs nur für aktivierte Clients definieren.
- **Gruppe**: Wenn Sie einen Auftrag für eine Gruppe definieren, erscheinen in der Übersichtsliste nicht die einzelnen Clients, sondern der Gruppenname.
- **Status**: Der Status oder das Ergebnis eines Jobs. 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

Job das letzte Mal durchgeführt wurde.

- **Zeitintervall**: Gemäß der Zeitplanung, die Sie für jeden Job definieren können, steht hier, in welchem Turnus der Job wiederholt wird.
- **Umfang**: Hier erfahren Sie, auf welche Datenträger (z. B. lokale Festplatten) sich der Auftrag erstreckt.



Um Aufgaben zu bearbeiten, wählen Sie im Kontextmenü (über Anklicken mit der rechten Maustaste) den Befehl **Eigenschaften**.

Die Symbolleiste oberhalb der Aufgabenliste bietet die folgenden Funktionen:

Aktualisieren

Löschen

Einmaliger Scan-Auftrag: Mit dieser Funktion lassen sich Scanaufträge für einzelne Clients oder Clientgruppen definieren. Im Konfigurationsdialog lassen sich auf den jeweiligen Karteireitern Zeitplanung, Analyseumfang und weitere Scaneinstellungen festlegen.

Periodischer Scan-Auftrag: Mit dieser Funktion lassen sich periodische Scanaufträge definieren.

Backup-Auftrag: Definieren Sie hier, wann und in welchem Umfang die Daten auf Clients gebackupt werden sollen (optionales Backup-**Modul**).

Wiederherstellungs-Auftrag: Mit dieser Funktion lassen sich auf Clients oder Gruppen zentral Backups zurückspielen (optionales Backup-**Modul**).

Softwareerkennungsauftrag: Mit dieser Funktion lässt sich auf Clients installierte Software ermitteln (optionales PatchManager-**Modul**).

Softwareverteilungsauftrag: Mit dieser Funktion lässt sich Software auf Clients verteilen (optionales PatchManager-**Modul**).

- **Sofort (erneut) ausführen**: Wählen Sie diese Funktion, um einmalige Scanaufträge, die bereits durchgeführt oder abgebrochen wurden, erneut auszuführen. Bei periodischen Scanaufträgen 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.
- **Gruppen-Aufträge ausführlich anzeigen**: Zeigt bei Gruppenjobs alle zugehörigen Einträge an. Die Option ist nur verfügbar, wenn in der Computerliste eine Gruppe selektiert ist.

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

- **Gruppen-Aufträge ausführlich anzeigen**
- **Sofort (erneut) ausführen**: Hiermit können Sie ausgewählte Jobs unabhängig von eingestellten zeitlichen Vorgaben direkt ausführen.
- **Abbrechen**: Über diese Funktion können Sie einen laufenden Job abbrechen.
- **Entfernen**: Ausgewählte Jobs können mit dieser Funktion gelöscht werden.
- **Backup wiederherstellen**: Hiermit können Sie übers Netzwerk Backups auf den Clients einspielen (optionales Backup-**Modul**).
- **Hinzufügen**: Hier können Sie Aufträge planen.

4.3.10.1. Scanaufträge

Im **Neuer Scan-Auftrag**-Fenster können Administratoren einmalige oder regelmäßig wiederkehrende Scan-Aufträge definieren. Eine komplette Job-Konfiguration besteht aus drei Bereichen: **Jobplanung**, **Scanner**-Einstellungen und **Analyseumfang**, jede von diesen ist durch einen eigenen Karteireiter gezielt einstellbar.

Welche Funktionen auf den Registerkarten verfügbar sind, ist abhängig vom ausgewählten Client. Zum Beispiel: Funktionen, die mit Desktop-spezifischen Bedrohungen zu tun haben, sind, wenn Sie einen Auftrag für einen Exchange-Server planen, nicht verfügbar.

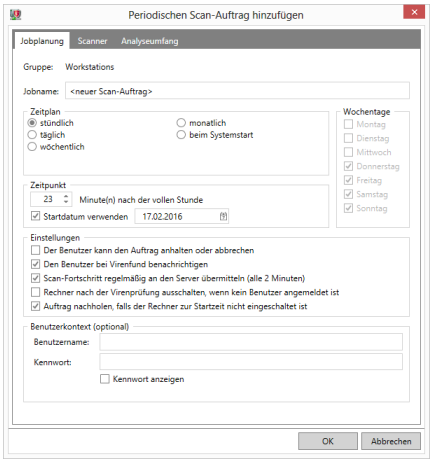
Jobplanung

Über die Registerkarte **Jobplanung** können Sie den Scanauftrag einplanen:

- **Jobname**: Hier kann festgelegt werden, welchen Namen der Scanauftrag haben soll. Hier sollten aussagekräftige Namen, wie *Archivprüfung* oder *Monatliche Prüfung* Verwendung finden, um den gewünschten Job eindeutig zu charakterisieren und in der tabellarischen Übersicht wiederzufinden.
- **Zeitplan** (Periodischer Scan-Auftrag): Bei periodischen Scanaufträgen können Sie festlegen, wann und in welchem Rhythmus die Virenprüfung erfolgen soll. Wird **Beim Systemstart** ausgewählt, fallen die Vorgaben der Zeitplanung weg und die G DATA Software führt die Prüfung aus, wenn der Rechner neu gestartet wird. Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass der Rechner nur an Werktagen eine Virenprüfung durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.
- **Zeitpunkt**: Hier können Sie eine genaue Startzeit definieren. Bei einem einmaligen Scanauftrag ohne Angabe einer Startzeit wird der Auftrag sofort nach dem Anlegen gestartet.
- **Einstellungen**

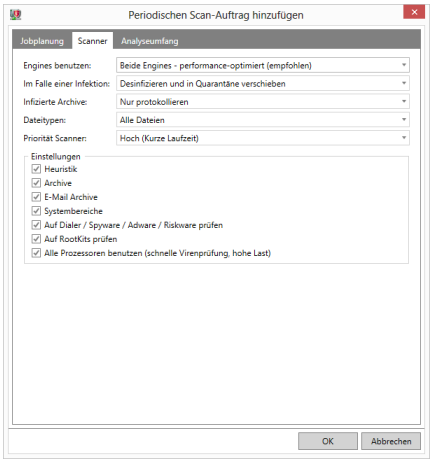
- **Der Benutzer kann den Auftrag anhalten oder abbrechen**: Es können den Anwendern Berechtigungen zum Anhalten oder Abbrechen des Jobs über das Kontextmenü des Trays eingeräumt werden.
- **Den Benutzer bei Virenfund benachrichtigen**: Sie können dem Benutzer eine Benachrichtigung anzeigen lassen, falls ein Virus gefunden wird.
- **Scan-Fortschritt regelmäßig an den Server übermitteln (alle 2 Minuten)**: Über diese Option können Sie sich im G DATA Administrator den Fortschritt eines laufenden Scanauftrags auf einem Client in Prozent anzeigen lassen.
- **Rechner nach der Virenprüfung ausschalten, wenn kein Benutzer angemeldet ist**: Nach der Virenprüfung können Sie den Rechner automatisch ausschalten lassen.
- **Auftrag nachholen, falls der Rechner zur Startzeit nicht eingeschaltet ist**: Sollte ein Rechner zum festgelegten Zeitpunkt eines Scanauftrags nicht eingeschaltet sein, kann der Scanauftrag über diese Option gestartet werden, wenn der Rechner nach diesem Zeitpunkt hochgefahren wird.

- **Benutzerkontext (optional)**: Falls der Scanauftrag Netzwerkfreigaben prüfen soll, müssen diese als UNC-Pfad statt als eingebundenes Netzlaufwerk eingegeben werden. Falls das jeweilige Maschinenkonto (z. B. *Client001$*) keine entsprechenden Berechtigungen besitzt, können Sie hier ein Konto mit geeigneten Berechtigungen eingeben.



Scanner

In dem Scanner-Menü lassen sich die Einstellungen vornehmen, mit denen der Scanauftrag ausgeführt werden soll.

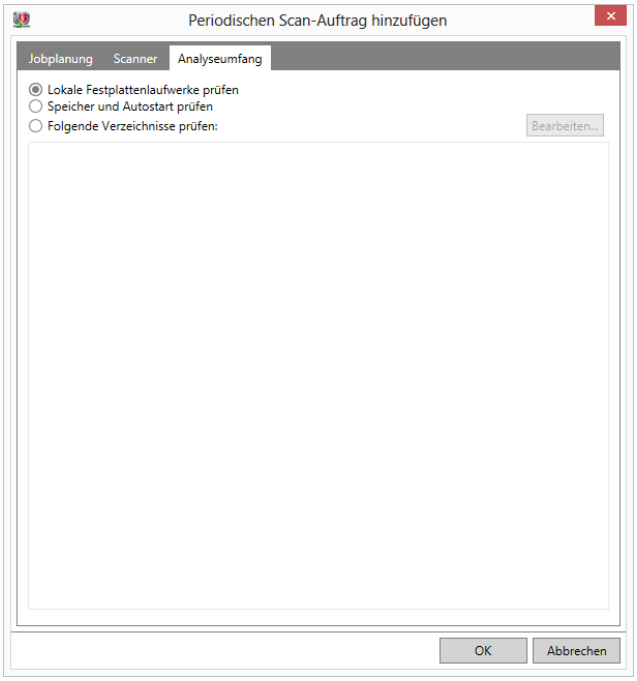


- **Engines benutzen**: Die G DATA Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten (siehe **Client-Einstellungen** > **Wächter**).

- **Im Fall einer Infektion**: Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll (siehe **Client-Einstellungen** > **Wächter**).
- **Infizierte Archive**: Legen Sie hier fest, wie infizierte Archive behandelt werden sollen (siehe **Client-Einstellungen** > **Wächter**).
- **Dateitypen**: Hier können Sie festlegen, welche Dateitypen von G DATA auf Viren untersucht werden sollen. Beachten Sie, dass eine Überprüfung aller Dateien eines Computers 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 schneller, allerdings sind Performanceeinbußen bei anderen Anwendungen möglich) oder niedrige Priorität (die Analyse benötigt mehr Zeit, dafür werden andere Anwendungen nicht beeinträchtigt). 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. Die meisten Einstellungen sind identisch mit denen, die Sie auf dem Karteireiter **Client-Einstellungen** > **Wächter** finden. Darüber hinaus gibt es aber auch Einstellungen, die speziell für Scanaufträge Verwendung finden:
  - **Auf RootKits prüfen**: Ein Rootkit versucht, 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 Prozessoren benutzen**: Mit dieser Option können Sie die Virenprüfung bei Systemen mit mehreren Prozessorkernen auf alle Prozessoren verteilen und auf diese Weise die Virenprüfung deutlich schneller durchführen. Nachteil dieser Option ist, dass so weniger Rechenleistung für andere Anwendungen verfügbar ist. Diese Option sollte nur dann genutzt werden, wenn der Scanauftrag zu Zeiten durchgeführt werden, zu denen das System nicht regulär genutzt wird (z. B. nachts).

Analyseumfang

Über die Registerkarte Analyseumfang lässt sich der Scan-Auftrag auf bestimmte Verzeichnisse (beim Client-Scan) oder Mailboxen (beim Exchange-Scan) begrenzen. Das Verzeichnisauswahl-Fenster erlaubt Ihnen Ordner auf dem Rechner, auf dem der G DATA Administrator ausgeführt wird, und auf Netzwerk-Clients auszuwählen. Falls Sie Netzwerkfreigaben auswählen, müssen diese als UNC-Pfad statt als eingebundenes Netzlaufwerk eingegeben werden. Auf diese Weise können z. B. Ordner mit selten benötigten Archiven ausgenommen und in einem separaten Scanauftrag geprüft werden.



4.3.10.2. Backupaufträge

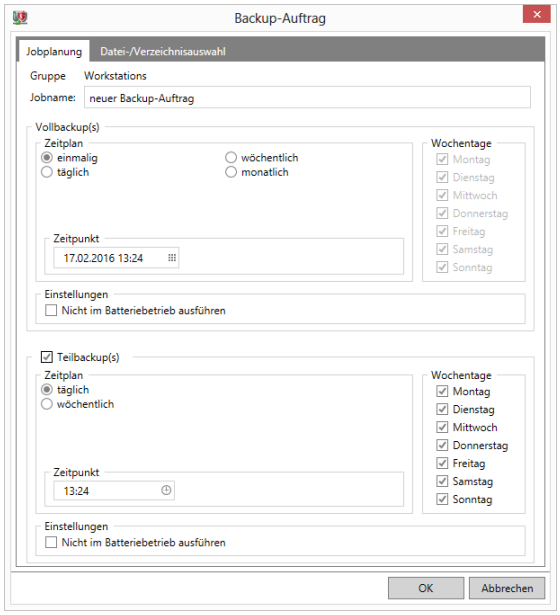
Das Backup-Modul ist als **optionales Modul** verfügbar.

Mit Hilfe von Backupaufträgen können Administratoren wichtige Client-Dateien zentral sichern.

Jobplanung
Hier kann festgelegt werden, welchen **Jobnamen** der Backupauftrag haben soll. Hier sollten aussagekräftige Namen, wie z. B. **Monatsbackup** oder **Teilbackup Außendienst** Verwendung finden, um den gewünschten Job eindeutig zu charakterisieren und in der tabellarischen Übersicht wiederzufinden. Sie können hier festlegen, wann und in welchem Rhythmus das Backup erfolgen soll und ob es sich dabei um ein **Teilbackup** oder **Vollbackup** handelt. Beim Teilbackup werden nur die Daten gebackupt, die sich seit dem letzten Teil- oder Vollbackup geändert haben. Dies spart Zeit bei der Erstellung des Backups. Die Wiederherstellung ist im Fall eines Zurückspielens von Daten allerdings langwieriger, da aus den verschiedenen Teilbackupdatenbeständen das letzte Systemabbild rekonstruiert werden muss.

Um Probleme zu vermeiden, die sich beim Abschalten eines nicht ans Stromnetz angeschlossenen Notebooks ergeben, können Sie die Einstellung **Nicht im Batteriebetrieb ausführen** auswählen. Backups von mobilen Geräten erfolgen dann nur, wenn diese auch ans Stromnetz angeschlossen sind. Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass der Rechner nur an Werktagen ein Backup durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

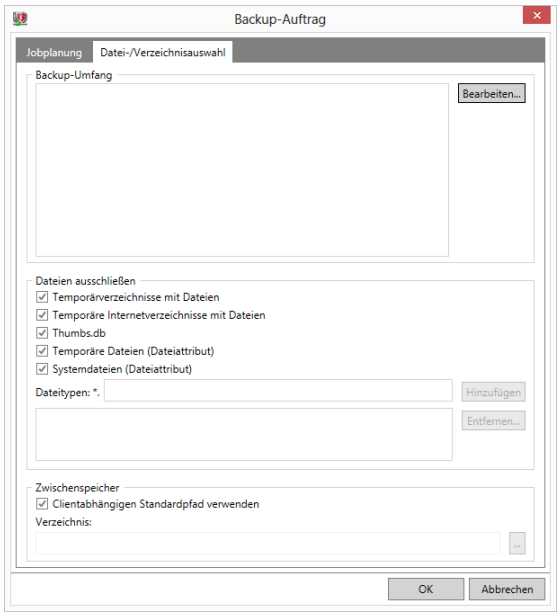
Serverseitige Backupverzeichnisse sowie Warnberichte über Backupspeicherplatz können unter **Allgemeine Einstellungen** > **Backup** konfiguriert werden.



Datei-/Verzeichnisauswahl

Über die Registerkarte Datei-/Verzeichnisauswahl können Sie festlegen, welche Daten genau bei den einzelnen Clients/Gruppen vom Backup erfasst werden sollen. Im Bereich **Backup-Umfang** können Sie dazu direkt im Verzeichnisbaum des jeweiligen Clients die Ordner festlegen, die gesichert werden sollen. Über die Häkchen unter **Dateien ausschließen** können Sie generell Dateien und Ordner mit bestimmten Attributen (z. B. **Temporäre Dateien**, **Systemdateien**) vom Backup ausschließen. Darüber hinaus können Sie auch individuelle Ausnahmen definieren, indem Sie die Endung bestimmter Dateitypen auf die Ausnahmeliste setzen.

Wenn die erstellte Sicherung in einem bestimmten Verzeichnis gespeichert werden soll, bevor Sie an den ManagementServer übermittelt wird, können Sie dies unter **Zwischenspeicher** explizit angeben. Wenn die Option **Clientabhängigen Standardpfad verwenden** nicht aktiv ist und ein absoluter Pfad angegeben ist, wird die Sicherung in dem angegebenen Verzeichnis zwischengespeichert. Wenn Sie die Option auswählen, wird der G DATA Security Client das Backup immer auf der Partition zwischenspeichern, auf der der meiste freie Speicherplatz vorhanden ist. Das Verzeichnis G DATA \Backup wird dann im Root-Verzeichnis dieser Partition angelegt.



4.3.10.3. Wiederherstellungsaufträge

Das Backup-Modul ist als **optionales Modul** verfügbar.

Wiederherstellungsaufträge können auf unterschiedliche Weise geplant werden. Klicken Sie im Menu **Aufträge** auf **Neu** > **Wiederherstellungsauftrag** oder in der Symbolleiste auf die Schaltfläche **Wiederherstellungsauftrag**. Das Fenster **Backup wiederherstellen** öffnet sich und Sie können ein Backup zum Wiederherstellen auswählen. Alternativ können Sie das Backup in der Auftragsliste suchen. Klicken Sie mit der rechten Maustaste auf den Auftrag und wählen Sie **Backup wiederherstellen**.

Das Fenster Backup wiederherstellen zeigt einige grundlegende Informationen über den ausgewählten Backup-Auftrag. Es enthält ein oder mehrere Backups, je nachdem, wie oft der Auftrag ausgeführt wurde. Die Liste zeigt pro Backup den **Zeitpunkt des Backups**, den **Client**, die **Art des Backups**, die **Anzahl der Dateien** und die **Größe (in MB)**. In der Liste **Wiederherstellen auf Client** können Sie den Client wählen, auf dem die Dateien wiederhergestellt werden sollen (dies muss nicht unbedingt der Client sein, auf dem das Backup erstellt wurde). Klicken Sie auf **OK**, um das Fenster Wiederherstellungseinstellungen zu öffnen.

Die Einstellungen für die Wiederherstellung können auf zwei Registerkarten konfiguriert werden. **Auswahl Dateien** ermöglicht es Ihnen, das Backup zu durchsuchen. Klicken Sie auf **Nur ausgewählte Dateien des Archivs wiederherstellen**, um eine Ordnerstruktur zu aktivieren, in der Sie die Dateien, die wiederhergestellt werden sollen, auswählen können. Klicken Sie auf **Alle Dateien des Archivs wiederherstellen**, um die Ordnerstruktur zu deaktivieren und alle Dateien wiederherzustellen. Auf der Registerkarte **Optionen** können Sie die Job-Einstellungen konfigurieren. Sie können unter **Jobname** einen aussagekräftigen Titel eingeben. Wenn Sie die Dateien in ihren ursprünglichen Verzeichnissen wiederherstellen möchten, aktivieren Sie **Dateien in ursprüngliche Verzeichnisse wiederherstellen**. Alternativ wählen Sie ein anderes **Zielverzeichnis**. Schließlich können Sie entscheiden was passieren soll, wenn es Versionskonflikte mit bestehenden Dateien gibt. Nach Bestätigung der Einstellungen wird ein Wiederherstellungsauftrag im Aufträge-Modul hinzugefügt und sofort durchgeführt.

4.3.10.4. Softwareerkennungsaufträge

PatchManager ist als **optionales Modul** verfügbar.

Mit dieser Funktion lässt sich auf Clients oder Gruppen die Anwendbarkeit von verfügbaren Patches ermitteln. Die folgenden Optionen stehen zur Verfügung:

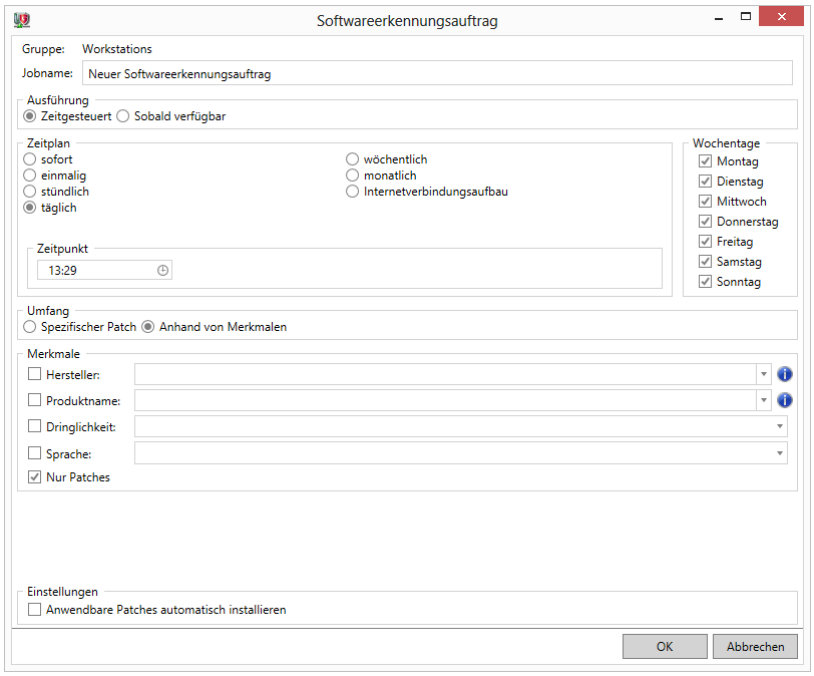
- **Ausführung**: Definieren Sie, wann der Softwareerkennungsauftrag ausgeführt werden soll:
  - **Zeitgesteuert**: Der Auftrag wird nach einem **Zeitplan** ausgeführt. Der Zeitplan kann über die folgenden Parameter konfiguriert werden: **Sofort**, **Einmalig**, **Stündlich**, **Täglich**, **Wöchentlich**, **Monatlich** oder bei **Internetverbindungsaufbau**.
  - **Sobald verfügbar**: Der Auftrag wird jedes Mal, wenn ein neuer Patch verfügbar ist, ausgeführt.

Um zu bestimmen, für welche Patches die Anwendbarkeit ermittelt wird, wählen Sie den **Umfang** der Suche aus:

- **Spezifischer Patch**: Wählen Sie einen oder mehrere Patches aus einer Liste aus.
- **Anhand von Merkmalen**: Um bestimmte Merkmale (**Hersteller**, **Produktname**,

Dringlichkeit, **Sprache**) als Auswahlkriterium zuzulassen, setzen Sie bitte das Häkchen beim jeweiligen Merkmal. So können Sie z. B. Patches für Software nur von bestimmten Herstellern ermitteln oder für konkrete Programmversionen einer Software. Wildcards wie ?und *zur Filterung sind dabei zulässig. Wählen Sie **Nur Patches** falls die Softwareerkennung keine vollständigen Software-Pakete und Upgrades auf Anwendbarkeit prüfen soll.

Aktivieren Sie **Anwendbare Patches automatisch installieren** um die Patches, für die der Softwareerkennungsauftrag die Anwendbarkeit bestätigt, automatisch zu installieren.



Falls Sie den Softwareerkennungsauftrag über die **Status-Übersicht** des PatchManagers planen, gilt der Auftrag für den Patch und die Client(s), die dort gewählt wurden. Falls Sie den Auftrag über das **Patch-Konfiguration**-Modul planen, wählen Sie im Auftragsfenster die Clients, für die die Anwendbarkeit geprüft werden soll. Falls Sie den Auftrag über das **Aufträge**-Modul planen, wählen Sie im Auftragsfenster die Patches, deren Anwendbarkeit geprüft werden soll - der Job wird auf dem aktuell ausgewählten Client oder der aktuell ausgewählten Gruppe ausgeführt.

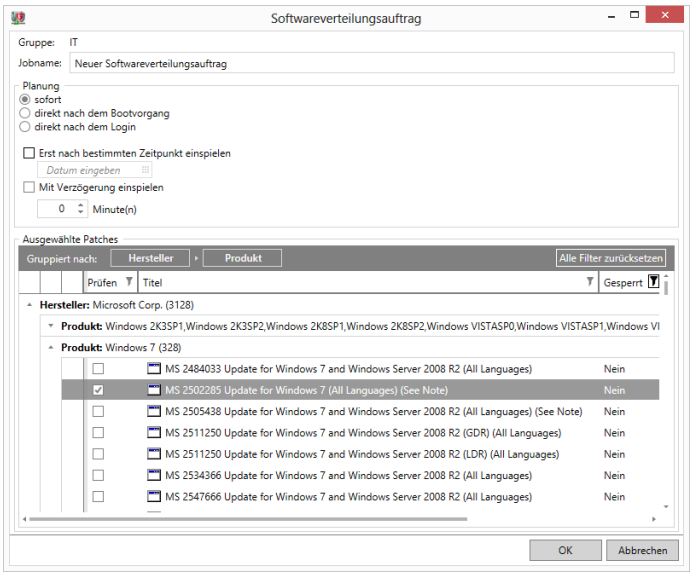
4.3.10.5. Softwareverteilungsaufträge

PatchManager ist als **optionales Modul** verfügbar.

Um **anwendbare Patches** auf Clients und Gruppen zu installieren, definieren Sie einen Softwareverteilungsauftrag. Die folgenden Planungsoptionen stehen zur Verfügung:

- **Sofort**: Der Auftrag wird sofort ausgeführt.
- **Direkt nach dem Bootvorgang**: Der Auftrag wird unmittelbar nach dem nächsten Bootvorgang ausgeführt.
- **Direkt nach dem Login**: Der Auftrag wird ausgeführt, sobald sich der Benutzer das nächste Mal einloggt.
- **Erst nach bestimmten Zeitpunkt einspielen**: Der Auftrag wird erst nach einem bestimmten Zeitpunkt ausgeführt. Die anderen Planungsoptionen treten erst in Kraft nachdem dieser Zeitpunkt erreicht ist.
- **Mit Verzögerung einspielen**: Eine Verzögerung sorgt dafür, dass Bootvorgang und Patch-Einspielung nicht beide gleichzeitig die Performance des Clients beeinträchtigen.

Falls Sie den Softwareverteilungsauftrag über die **Status-Übersicht** des PatchManagers planen, gilt der Auftrag für den Patch und die Client(s), die dort gewählt wurden. Falls Sie den Auftrag über das **Patch-Konfiguration**-Modul planen, wählen Sie im Auftragsfenster die Clients, auf denen der Patch installiert werden soll. Falls Sie den Auftrag über das **Aufträge**-Modul planen, wählen Sie im Auftragsfenster die Patches, die installiert werden sollen - der Job wird auf dem aktuell ausgewählten Client oder der aktuell ausgewählten Gruppe ausgeführt.



4.3.10.6. Rollbackauftrag

PatchManager ist als **optionales Modul** verfügbar.

Ein Rollbackauftrag deinstalliert bereits eingespielte Patches. Wählen Sie den jeweiligen Softwareverteilungsauftrag in dem **Aufträge**-Bereich aus und wählen Sie per Rechtsklick **Rollback**. Auch über die **Status-Übersicht** können Sie einen Rollbackauftrag planen, indem Sie den jeweiligen Client und Patch auswählen und dann per Rechtsklick einen Rollbackauftrag planen.

Im Fenster **Update-Rollback** können Sie einen Jobnamen eingeben, damit Sie den Auftrag nachher einfach identifizieren können. Nachdem Sie den Namen eingegeben haben, klicken Sie auf **OK**, um den Auftrag zu den **Aufträgen** hinzuzufügen. Der Auftrag wird sofort ausgeführt.

4.3.11. PolicyManager

Das PolicyManager-Modul ist als Teil der Endpoint Protection Business- und Managed Endpoint Security-**Lösungen** verfügbar.

Der PolicyManager enthält eine Anwendungs-, Geräte-, Web-Inhaltskontrolle sowie eine Überwachung der Internetnutzungszeit. Diese Funktionen erlauben eine flächendeckende Umsetzung der Unternehmensrichtlinien zur Nutzung der firmeneigenen PCs. So kann über den PolicyManager bestimmt werden, ob und in welchem Umfang externe Massenspeicher- oder optische Medien genutzt werden können. Ebenso lässt sich definieren, welche Webseiten besucht und welche Programme auf den Firmen-PCs genutzt werden dürfen.

4.3.11.1. Anwendungskontrolle

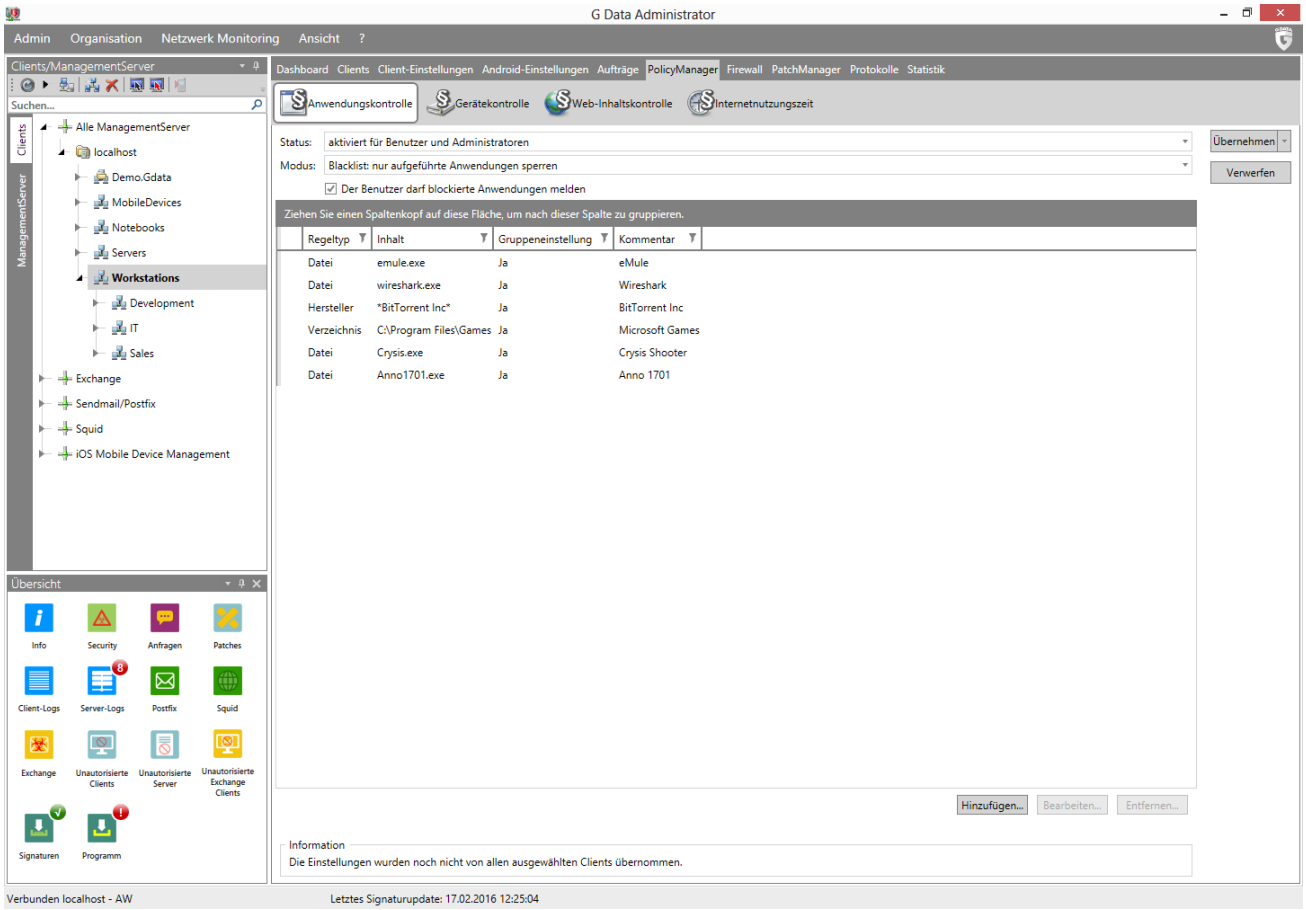
Mit der Anwendungskontrolle lassen sich bestimmte Programme für die Nutzung durch ausgewählte Clients sperren. Legen Sie dazu unter **Status** fest, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen. Unter Modus bestimmen Sie nun, ob es sich bei der Anwendungskontrollliste

um eine Whitelist oder Blacklist handeln soll.

- **Whitelist**: Nur die hier aufgeführten Anwendungen können vom Client-Rechner aus verwendet werden.
- **Blacklist**: Hier aufgeführte Anwendungen können auf dem Client-Rechner nicht verwendet werden.

Über die **Neu**-Schaltfläche, kann eine neue Regel erstellt werden. Zur Auswahl stehen die Regeltypen **Hersteller**, **Datei** und **Verzeichnis**:

- **Hersteller**: Hier werden die Herstellerinformationen in Programmdateien dazu verwendet, eine Nutzung dieser Anwendungen zu erlauben oder zu verbieten. Sie können den Namen des Herstellers hier entweder selbst eintragen oder über die **...**-Schaltfläche gezielt eine Datei auswählen, aus der die Herstellerinformation ausgelesen und übernommen wird.
- **Datei**: Hier können Sie bestimmte Programmdateien für den jeweiligen Client sperren oder erlauben. Dabei können Sie entweder den Dateinamen eingeben, um den Zugriff auf Dateien dieses Namens generell zu verbieten/zu erlauben oder Sie klicken auf die Schaltfläche **Merkmale einer Datei ermitteln**, um ganz speziell eine bestimmte Datei anhand ihrer Merkmale zu definieren. Bei Bedarf können Sie als Platzhalter für beliebige Inhalte einen Stern (*) am Anfang und/oder Ende der Merkmale **Dateiname**, **Produktname** und **Copyright** verwenden.
- **Verzeichnis**: Über diese Funktion können Sie komplette Verzeichnisse (auf Wunsch inklusive der jeweiligen Unterverzeichnisse) für Clients freigeben oder sperren.



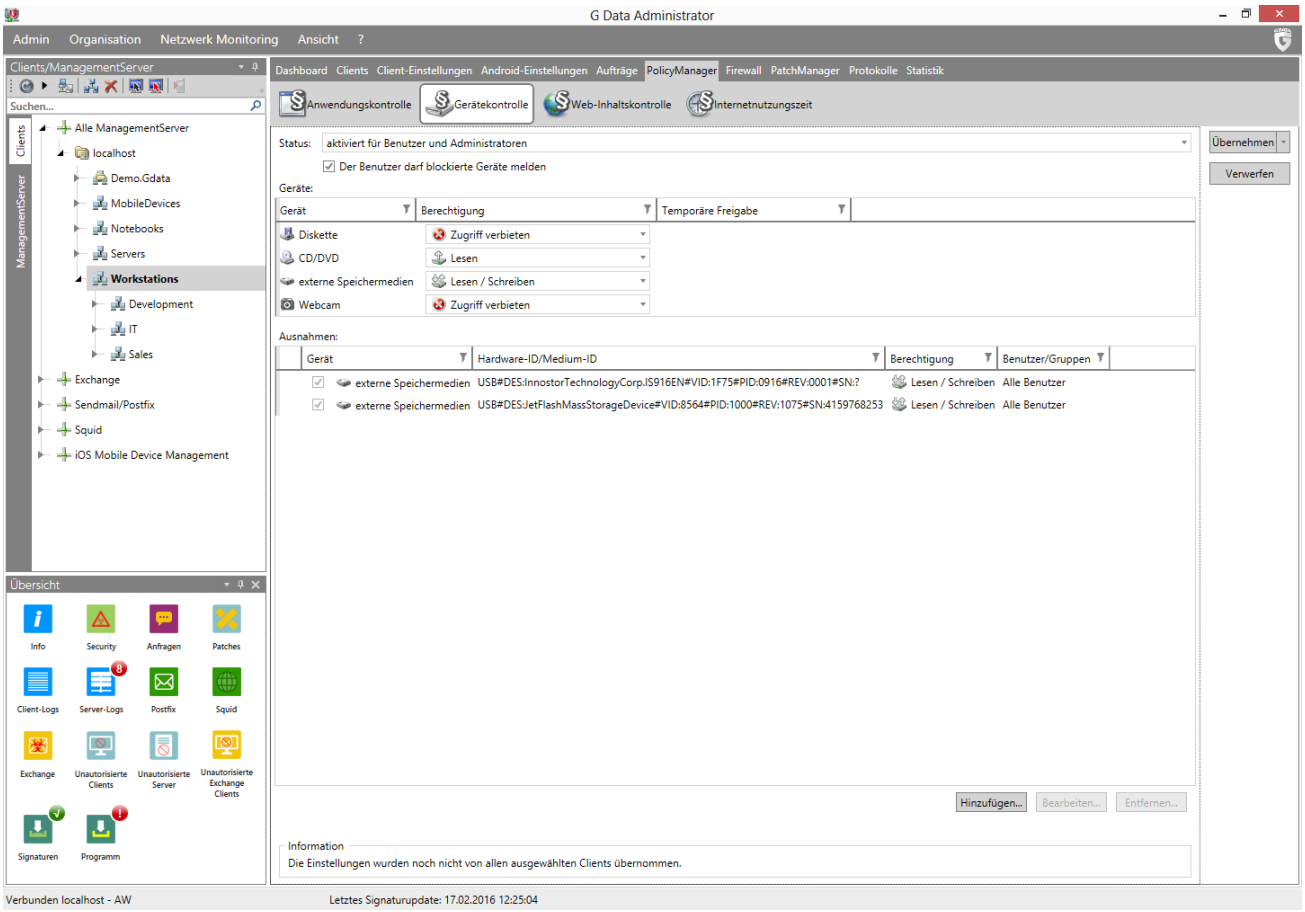
4.3.11.2. Gerätekontrolle

Mit Hilfe der Gerätekontrolle lässt sich der Zugriff auf externe Speichermedien begrenzen. So können USB-Sticks von der Nutzung ausgeschlossen, CD/DVD-Laufwerke mit Schreib- oder Leserechten ausgestattet und auch die Verwendung von Kameras eingeschränkt werden.

Unter **Status** können Sie festlegen, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen.

Unter **Geräte** können Sie die Nutzung verschiedener Gerätetypen mit Hilfe der folgenden Einstellungen einschränken:

- **Berechtigung**
  - **Lesen / Schreiben**: Es besteht voller Zugriff auf das Gerät.
  - **Lesen**: Medien können nur gelesen werden, ein Abspeichern von Daten ist nicht erlaubt.
  - **Zugriff verbieten**: Sowohl Lese- als auch Schreibzugriffe auf das Gerät sind nicht erlaubt. Das Gerät kann vom Anwender nicht verwendet werden.
- **Temporäre Freigabe**: Falls ein Gerät auf Grund einer Anfrage im Modul **Sicherheitsereignisse** temporär freigegeben wurde, wird der Zeitraum hier angezeigt. Klicken Sie auf das X-Symbol um die temporäre Freigabe sofort zu deaktivieren.



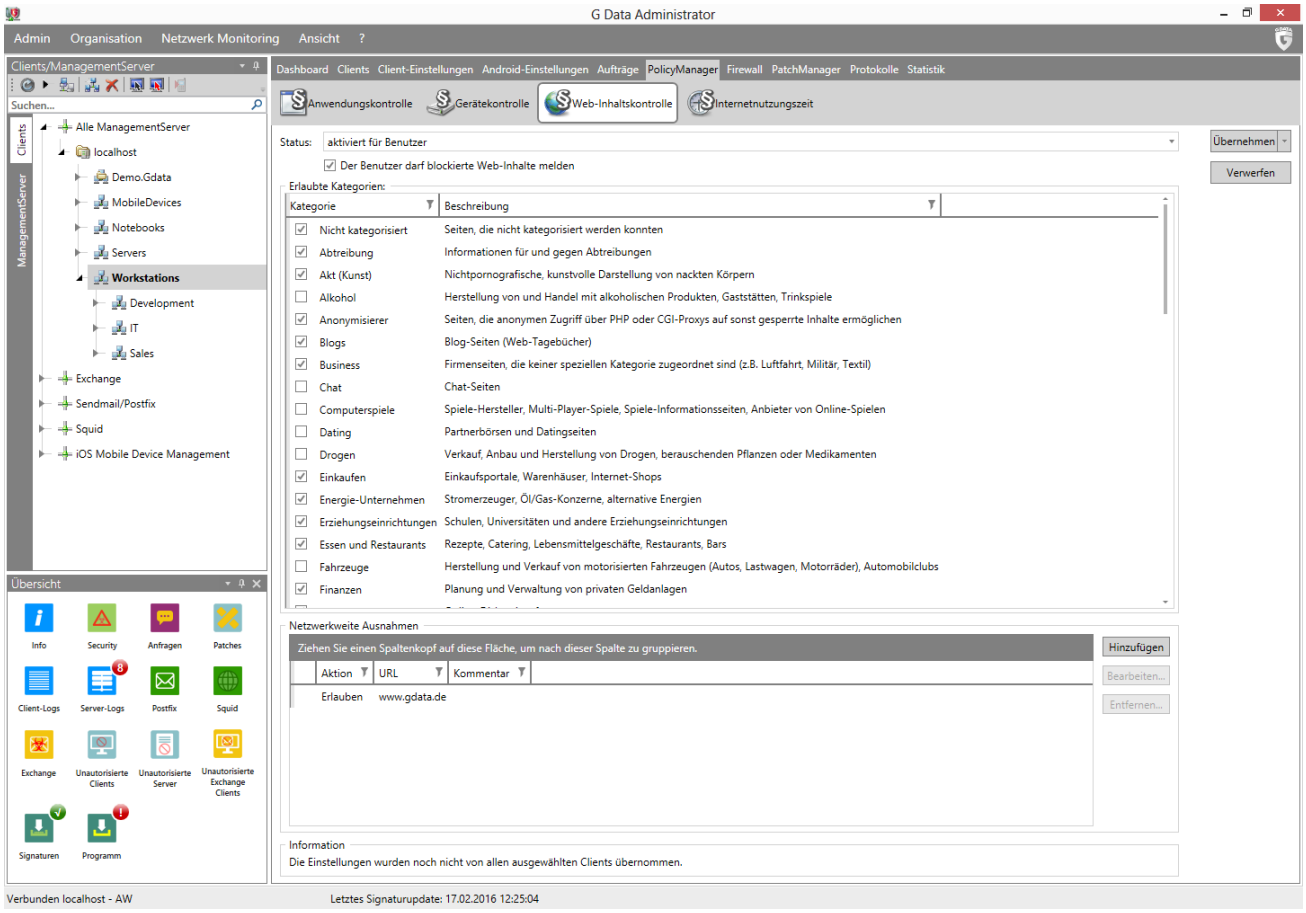
Über die **Ausnahmen**-Einstellungen können Sie die Gerätenutzung, die Sie vorher in irgendeiner Weise eingeschränkt hatten (**Lesen / Zugriff verbieten**) mit bestimmten Ausnahmen wieder erlauben. Wenn Sie auf die **Hinzufügen**-Schaltfläche klicken, öffnet sich ein Dialogfenster, in dem Sie eine Ausnahme hinzufügen können:

- **Geräte**: Wählen Sie den Gerätetyp, für den Sie eine Ausnahme anlegen möchten.

- **Regel aktiv**: Die Ausnahme ist nur aktiv, wenn dieses Häkchen gesetzt ist.
- **Typ**
  - **Gerätetyp-basierte Ausnahme**: Die Ausnahme wird für den **Geräte**-Typ als Ganzes angelegt.
  - **Hardware-ID/Medium-ID basierte Ausnahme**: Die Ausnahme wird nur für die spezifische Geräteinstanz (z. B. eine bestimmte DVD oder einen bestimmten USB-Stick), die Sie unter **Hardware-ID/Medium-ID** festlegen, angelegt.
- **Berechtigung**: Wählen Sie die Art der Berechtigung, die erlaubt werden soll.
- **Hardware-ID/Medium-ID**: Wenn Sie eine **Hardware-ID/Medium-ID basierte Ausnahme** anlegen, geben Sie hier die jeweilige ID ein. Klicken Sie auf die Schaltfläche **...**, um eine spezifische Hardware- oder Medium-ID zu ermitteln:
  - **Quelle auswählen**: Wählen Sie hier **(Lokale Suche...)**, um die Suche nach Hardware- und Medium-IDs auf dem Rechner, auf dem G DATA Administrator installiert wurde, auszuführen. Alternativ wählen Sie einen Client aus der Liste, um auf dem jeweiligen Rechner nach IDs zu suchen.
  - **Geräte**: Wählen Sie **Medium-ID verwenden** um Medium-IDs (z. B. CD/DVD) oder **Hardware-ID verwenden** um Hardware-IDs anzeigen zu lassen.
- **Windows Benutzer/Gruppe definieren**: Falls die Ausnahme auf bestimmte Windows-Benutzer oder -Gruppen beschränkt werden soll, so geben Sie diese hier ein. Falls Sie mehrere Benutzer oder Gruppen eingeben möchten, sollten diese mit einem Zeilenumbruch oder Komma getrennt werden.
- **Kommentar**: Hier können Sie eine Kommentar zur Ausnahme hinzufügen (z. B. um ähnliche Ausnahmen nachher unterscheiden zu können).

4.3.11.3. Web-Inhaltskontrolle

Die Web-Inhaltskontrolle dient dazu, Anwendern zwar den dienstlichen Zugang zum Internet zu erlauben, aber das Surfen auf nicht erwünschten Webseiten oder in bestimmten Themenbereichen zu unterbinden. Sie können hier gezielt Bereiche durch Setzen eines Häkchens für den jeweiligen Client erlauben oder durch Entfernen des Häkchens verbieten. Die Kategorien decken dabei eine große Anzahl thematischer Bereiche ab und werden von G DATA laufend aktualisiert. Somit entfällt für den Netzwerkadministrator der mit der Pflege von White- und Blacklists verbundene Aufwand.



Unter **Status** können Sie festlegen, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorenrechte auf dem Client-Rechner besitzen.

Mit Hilfe der **Netzwerkweiten Ausnahmen** können Sie sicherstellen, dass bestimmte Webseiten unternehmensweit für das gesamte Netzwerk freigegeben oder blockiert werden, unabhängig von den Einstellungen, die unter **Erlaubte Kategorien** vorgenommen wurden. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**, wählen Sie **Erlauben** oder **Sperren**, geben Sie die **Adresse** (ohne Protokoll) ein und klicken Sie auf **OK** um die Ausnahme zu erstellen. Wählen Sie **Bearbeiten** um eine bestehende Ausnahme zu bearbeiten oder **Löschen** um Ausnahmen zu löschen.

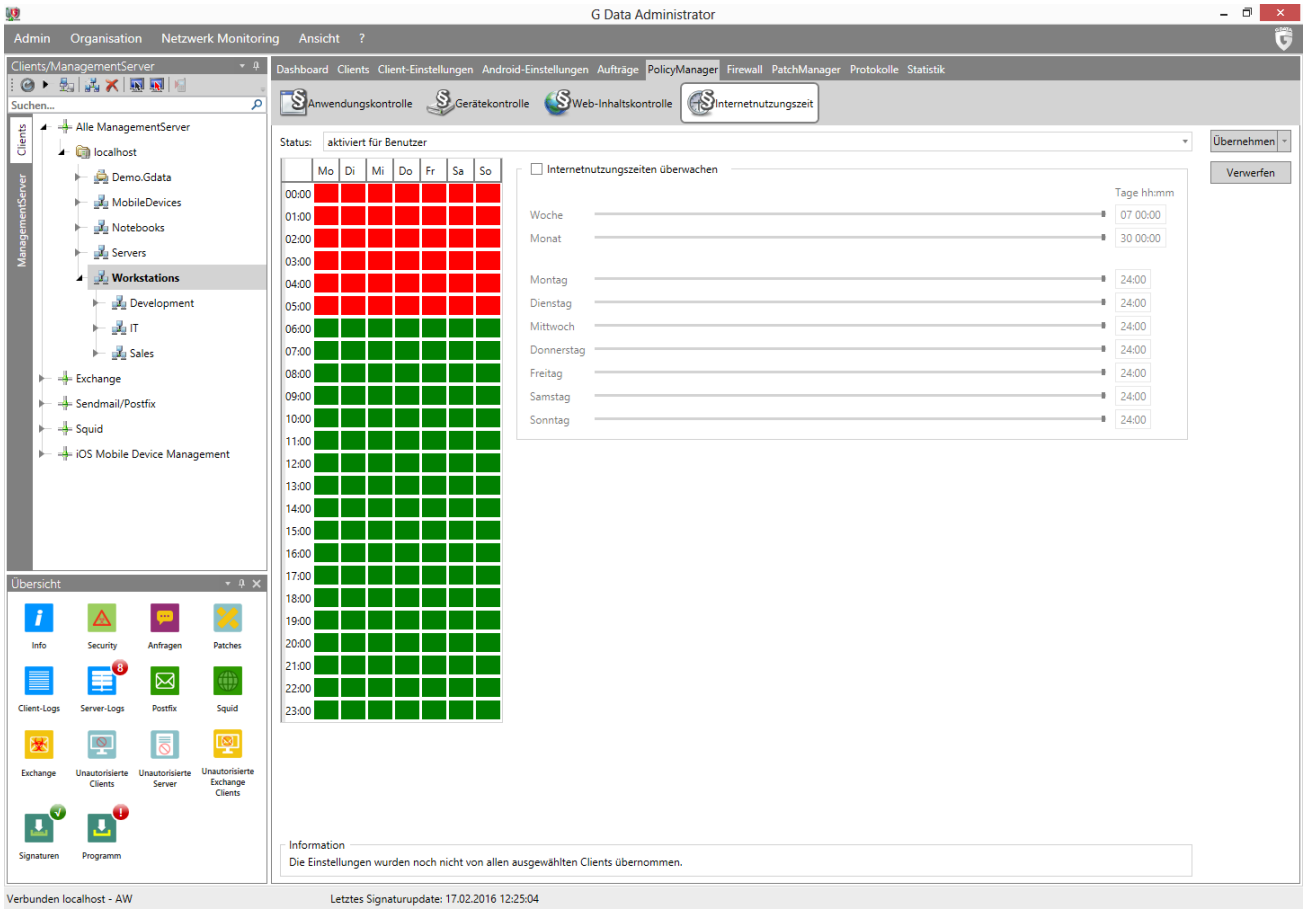
4.3.11.4. Internetnutzungszeit

Im Bereich Internetnutzungszeit kann die generelle Nutzung des Internets auf bestimmte Zeiten beschränkt werden. Zudem ist auch die Einrichtung eines Zeitkontingents für die Internetnutzung möglich. Unter **Status** wird festgelegt, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen.

Auf der rechten Seite kann über die dort vorhandenen Schieberegler das Kontingent festgelegt werden, dass auf dem jeweiligen Clientrechner für die Nutzung des Internets zur Verfügung steht. Es können tägliche, wöchentliche oder monatliche Kontingente vergeben werden; beispielsweise entspricht die Angabe *04 20:05* einer Internetnutzungszeit von 4 Tagen, 20 Stunden und 5 Minuten. Wenn der jeweilige Benutzer versucht, über das erlaubte Zeitkontingent hinaus auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er sein Zeitkontingent überschritten hat.

> Im Zusammenspiel der Angaben zur Internetnutzung zählt immer der jeweils kleinste Wert. Wenn Sie also für den Monat eine zeitliche Beschränkung von vier Tagen festlegen, in der

Woche aber z. B. fünf Tage erlauben, deckelt die Software die Internetnutzung für den Benutzer automatisch auf vier Tage.



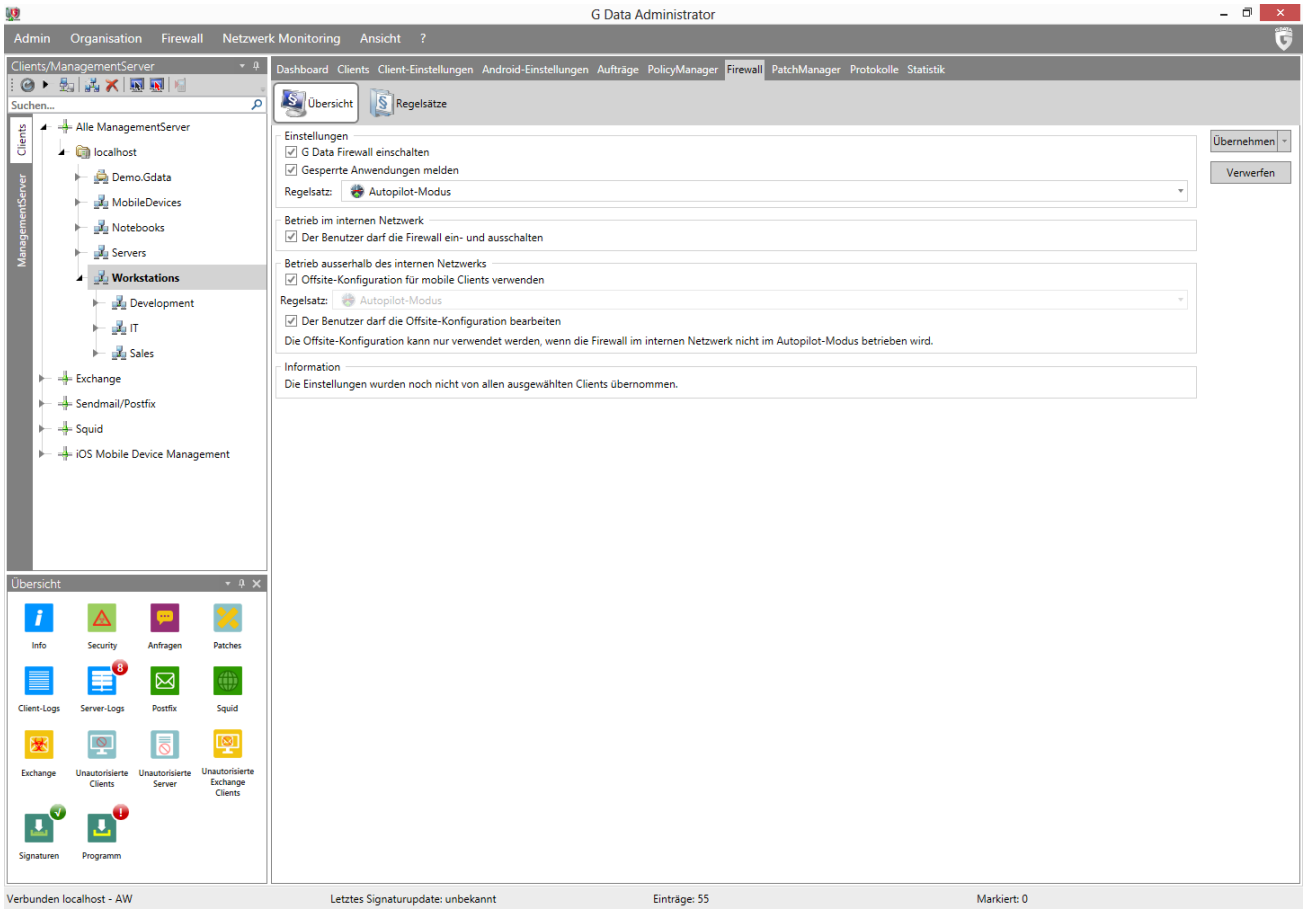
Im Sperrzeiten-Bereich können Sie – zusätzlich zur zeitlichen Eingrenzung der Internetnutzung – bestimmte Zeiträume sperren. Gesperrte Zeiträume sind dabei rot dargestellt, freigegebene Zeiträume in grün. Um einen Zeitraum freizugeben oder zu sperren, markieren Sie diesen mit der Maus. Dann erscheint neben dem Mauszeiger ein Kontextmenü, in dem Sie zwei Möglichkeiten haben: **Zeit freigeben** und **Zeit sperren**. Wenn der jeweilige Benutzer versucht, während der gesperrten Zeiten auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er zu diesem Zeitpunkt keinen Zugriff auf das Internet hat.

4.3.12. Firewall

Das Firewall-Modul ist als Teil der Client Security Business-, Endpoint Protection Business- und Managed Endpoint Security-**Lösungen** verfügbar.

4.3.12.1. Übersicht

In dem Bereich Übersicht können Sie die Firewall-Einstellungen für die ausgewählten Clients festlegen.



Einstellungen

Unter Einstellungen legen Sie die allgemeinen Firewall-Einstellungen fest:

- **G DATA Firewall einschalten**: Firewall aktivieren/deaktivieren.

  Achtung: Ab Version 14 müssen Clients, auf denen die Firewall noch nicht installiert wurde, zuerst auf die neue Version aktualisiert werden, bevor die Firewall aktiviert werden kann.

- **Gesperrte Anwendungen melden**: Wenn der Client-Rechner mit dem G DATA ManagementServer verbunden ist, erhält der Systemadministrator im Bereich **Sicherheitsereignisse** Informationen über Anwendungen, die durch die Firewall geblockt wurden.

- **Regelsatz**: Wählen Sie den Regelsatz, der vom Client verwendet werden soll:
  - **Autopilot-Modus**: Die Regeln werden von G DATA automatisch konfiguriert und die Firewall erfüllt ihre Aufgabe im Hintergrund und stört den Anwender nicht mit Rückfragen. Im Autopilot-Modus optimiert die Firewall ihren Regelsatz mit der Zeit selbstständig.
  - Ein beliebiger Regelsatz, den Sie im Bereich **Regelsätze** definiert haben.

Betrieb im internen Netzwerk

Unter Betrieb im internen Netzwerk finden Sie die Einstellungen, die zutreffen, wenn der Client innerhalb des ManagementServer-Netzwerks verwendet wird:

- **Der Benutzer darf die Firewall ein- und ausschalten**: Hier können Sie als Netzwerkadministrator 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.

Betrieb ausserhalb des internen Netzwerkes
Unter Betrieb ausserhalb des internen Netzwerkes finden Sie die Einstellungen, die zutreffen, wenn der Client ausserhalb des ManagementServer-Netzwerks verwendet wird:

- **Offsite-Konfiguration für mobile Clients verwenden**: Um mobile Rechner, die sich nicht im Netzwerk des G DATA ManagementServers befinden, optimal zu schützen, können die Firewall-Regelsätze des Client-Rechners automatisch durch einen Offsite-Regelsatz ersetzt werden. Sobald der mobile Rechner wieder mit dem Netzwerk des G DATA ManagementServers verbunden wird, wird der ursprüngliche Regelsatz automatisch wiederhergestellt.

  Hinweis: 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 internen Netzwerk verbunden ist.
- **Regelsatz**: Wählen Sie den Offsite-Regelsatz, der vom Client verwendet werden soll:
  - **Autopilot-Modus** (siehe **Firewall** > **Übersicht** > **Einstellungen**).
  - Ein beliebiger Regelsatz, den Sie im Bereich **Regelsätze** definiert haben.
- **Der Benutzer darf die 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 G DATA ManagementServer-Netzwerk verbunden wird, werden die durchgeführten Änderungen wieder durch die vom Netzwerkadministrator vorgegebenen Regeln für diesen Client ersetzt.

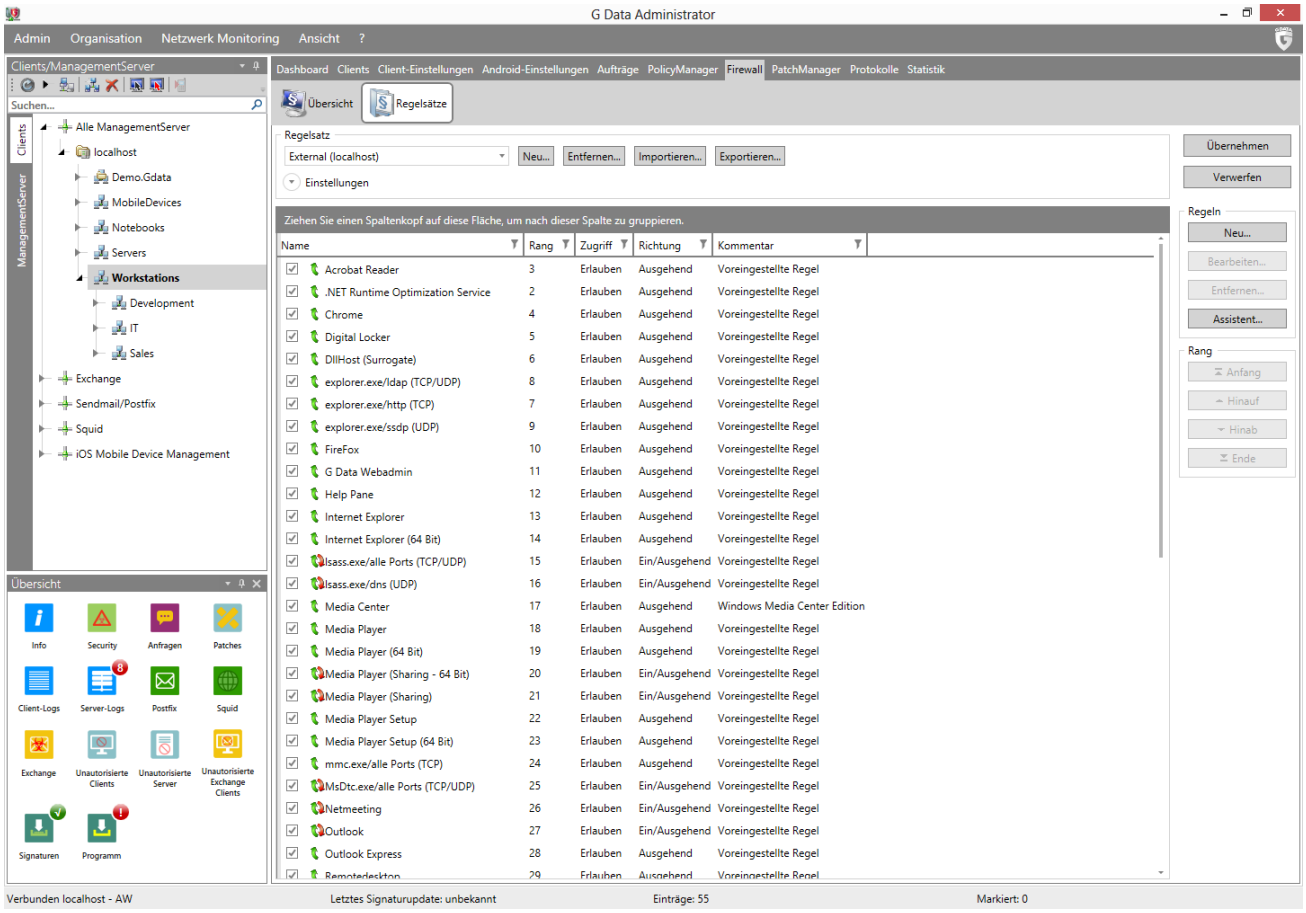
4.3.12.2. Regelsätze

Auf der Registerkarte Regelsätze können Sie Regelsätze für unterschiedliche Netzwerkbereiche erstellen. Jeder Regelsatz kann eine beliebige Anzahl von Firewall-Regeln beinhalten.

Der aktuelle Regelsatz wird unter **Regelsatz** angezeigt. Regelsätze können mit Hilfe der Schaltflächen **Neu**, **Entfernen**, **Importieren** und **Exportieren** verwaltet werden. Unter **Einstellungen** können Sie folgende Einstellungen bearbeiten:

- **Name**: Der Name des Regelsatzes.
- **Kommentar**: Eine Beschreibung des Regelsatzes.
- **Stealth-Modus aktiviert**: Wählen Sie Stealth-Modus aktiviert um Anfragen an den Computer, die dazu dienen, die Erreichbarkeit von Ports zu überprüfen, nicht zu beantworten. Dies erschwert es Angreifern, auf diese Weise Informationen über das System zu erhalten.

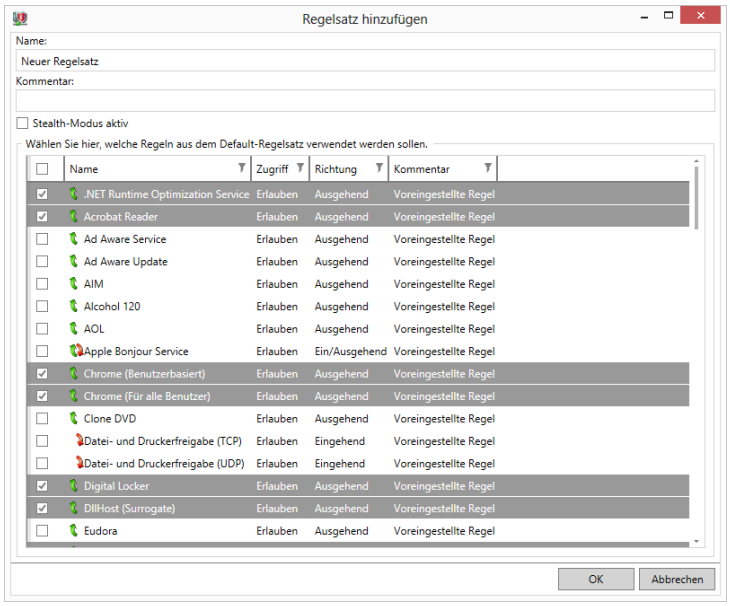
Die Regeln des ausgewählten Regelsatzes werden im unteren Teil des Bereichs angezeigt. Unter **Regeln** können Sie **Regeln erstellen und berarbeiten**, Regeln entfernen oder den **Regel-Assistenten** öffnen. Firewall-Regeln werden der Reihenfolge nach ausgeführt. Um die Reihenfolge zu ändern, wählen Sie einen Regel und klicken Sie unter **Rang** auf **Anfang**, **Hinauf**, **Hinab** oder **Ende**.



Regelsatz hinzufügen

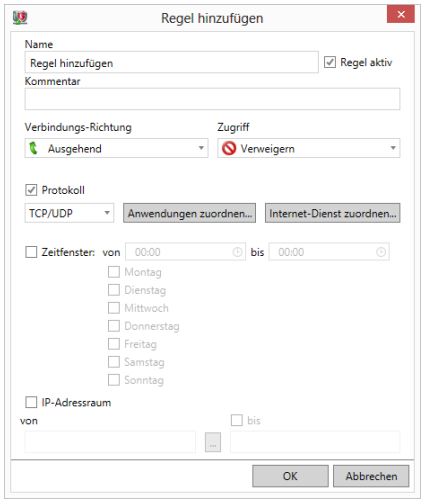
Geben Sie einen **Namen** für den Regelsatz und ggf. **Kommentar** ein. Wählen Sie **Stealth-Modus aktiv** um Anfragen an den Computer, die dazu dienen, die Erreichbarkeit von Ports zu überprüfen, nicht zu beantworten.

Sie können einen oder mehrere vordefinierten Regeln zum Regelsatz hinzufügen. Nachdem Sie **OK** wählen, wird der Regelsatz in der **Regelsätze**-Übersicht gezeigt.



Regel erstellen/Regel bearbeiten

Verwenden Sie unter **Regeln** die Schaltflächen **Neu** und **Bearbeiten**, um neue Regeln hinzuzufügen oder bestehende zu verändern.



- **Name**: Hier findet sich bei voreingestellten und automatisch generierten Regeln der Programmname, für den die jeweilige Regel zutrifft.
- **Regel aktiv**: Sie können eine Regel durch Entfernen des Häkchens aktivieren/deaktivieren, 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 verbinden (**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 Angriffs deutlich.

Regelassistent

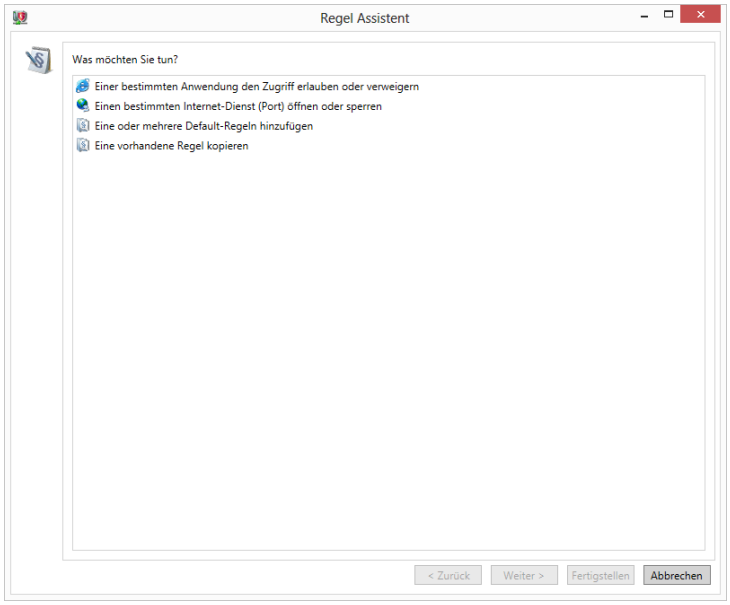
Mit dem Regelassistenten können Sie auf einfache Weise zusätzliche Regeln für den jeweiligen Regelsatz definieren oder bestehende Regeln verändern.

Der Regelassistent stellt folgende Aktionen zur Verfügung:

- **Einer bestimmten Anwendung den Zugriff erlauben oder verweigern**: Hiermit können Sie gezielt eine Anwendung auswählen und ihr im Rahmen des gewählten Regelsatzes den Zugriff auf das Netzwerk erlauben oder verbieten. Wählen Sie im Assistenten dazu einfach das gewünschte Programm aus (Programmpfad) und geben Sie dann unter **Verbindungs-Richtung** 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**: Im Assistenten haben Sie die Möglichkeit, Ports komplett zu sperren oder aber auch nur für eine bestimmte Anwendung (z. B. CRM-Software) freizugeben.
- **Eine oder mehrere Default-Regeln hinzufügen**: Mit dieser Funktion können Sie eine oder mehrere Default-Regeln zu dem gewählten Regelsatz hinzufügen.
- **Eine vorhandene Regel kopieren**: Mit dieser Funktion können Sie zum weiteren Editieren eine Kopie einer bestehenden Regel anfertigen.



4.3.13. PatchManager

PatchManager ist als **optionales Modul** verfügbar.

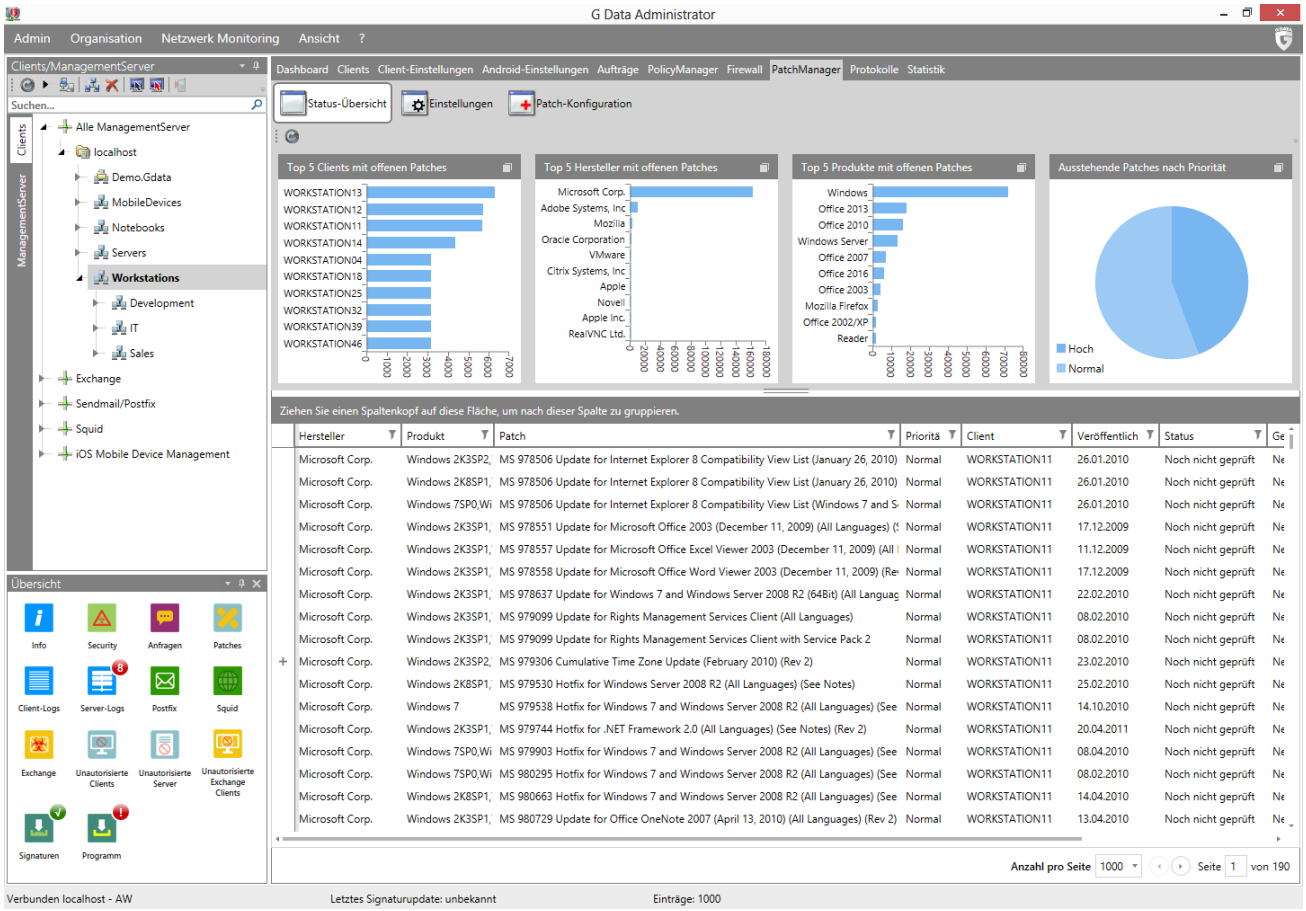
Mit Hilfe des PatchManagers können Sie die Patch-Implementierung für alle verwalteten Clients über eine einzige Schnittstelle steuern. Sie können den PatchManager sowohl für Updates von Microsoft-Software, als auch anderen Anbietern nutzen. Jeder Patch kann auf Anwendbarkeit überprüft, gesperrt, distribuiert oder übers Rollback zurückgenommen werden. Dies funktioniert sowohl für einzelne Clients, als auch für Client-Gruppen.

4.3.13.1. Status-Übersicht

Der Status-Übersichtsbereich bietet Ihnen eine detaillierte Übersicht über Patches und deren Status innerhalb des Netzwerks. Der Bereich listet alle Patches in alphabetischer Reihenfolge und einmal für jeden Client auf. Die umfangreiche Liste kann gefiltert werden um z. B. zu zeigen ob alle Clients mit allen relevanten Patches aktualisiert wurden. Hier können Sie auch direkt die Patch-Bereitstellung planen. Eine Reihe von Grafiken zeigt Informationen über ausstehende Patches, z. B. ob es kritische Patches gibt, die noch installiert werden müssen.

Standardmäßig ist die Status-Übersicht nach **Status**, **Priorität**, **Hersteller** und **Produkt** gruppiert, um schnell feststellen zu können, ob wesentliche Patches schon installiert sind oder nicht. Darüber hinaus sind standardmäßig Filter aktiv, die vollständige Software-Pakete sowie gesperrte Patches ausblenden. Wählen Sie **Alle Filter zurücksetzen**, um alle Listeneinträge anzeigen zu lassen.

Patches, die einen vorherigen Patch ersetzen, können ausgeklappt werden: Klicken Sie auf das jeweilige Pluszeichen, um alle ersetzten Patches anzuzeigen.



Pro Patch und Client können Sie verschiedene Aufträge planen. Wählen Sie einen oder mehrere Patches mit der rechten Maustaste und klicken Sie eine der folgenden Optionen an:

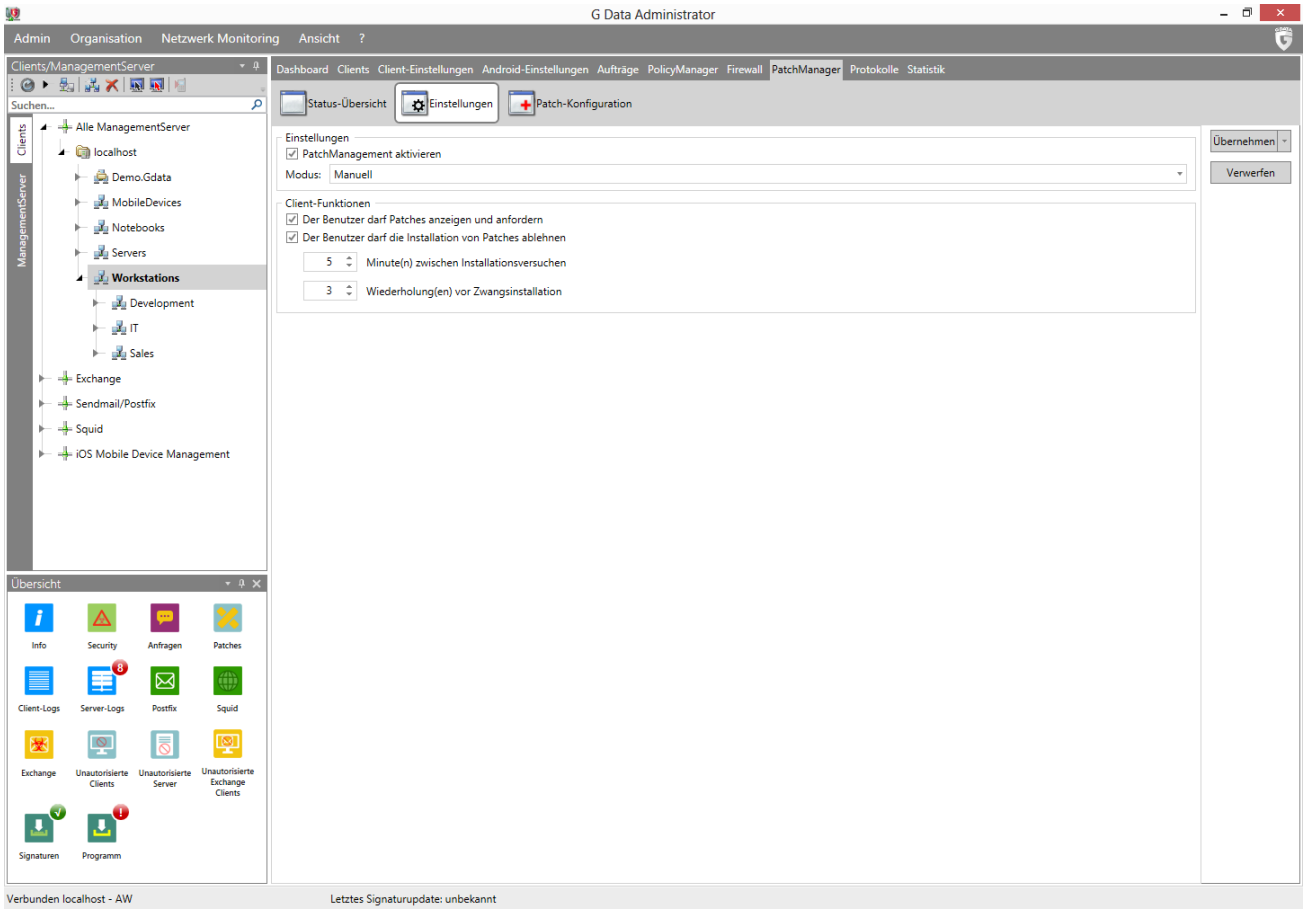
- **Patches auf Anwendbarkeit prüfen**: Planen Sie mit Hilfe vom **Softwareerkennungs**-Fenster einen Auftrag, der die selektierten Patches auf Anwendbarkeit auf dem selektierten Client prüft.
- **Patches installieren**: Planen Sie mit Hilfe vom **Softwareverteilungs**-Fenster einen Auftrag, der die selektierten Patches auf dem selektierten Client installiert.
- **Rollback**: Planen Sie einen **Rollback**-Job für Patches, die bereits installiert worden sind.
- **Patches sperren**: Sperrt einen oder mehrere Patches, die nicht verteilt werden sollen. Gesperrte Patches werden von automatischen Softwareerkennungsaufträgen und Softwareverteilungsaufträgen ignoriert. Wenn Sie einen manuellen Softwareerkennungs- oder Softwareverteilungsauftrag planen, werden gesperrte Patches standardmäßig ausgeblendet.
- **Patches entsperren**: Entsperrt einen oder mehrere Patches.
- **Eigenschaften**: Zeigt weitere Informationen an, wie z. B. eine komplette Beschreibung und den Lizenztext.

Die **Status**-Spalte zeigt den Status jedes Patches und seine geplanten oder laufenden Patch-Jobs (z. B. *Wird geprüft*während ein Auftrag ausgeführt wird oder *Nicht anwendbar*falls der Patch nicht anwendbar ist).

4.3.13.2. Einstellungen

Hier können Sie bestimmen, wie Patches und Updates auf dem Client und den Gruppen eingespielt werden sollen.

- **PatchManagement aktivieren**: PatchManager ein- oder ausschalten.
- **Modus**: Legen Sie fest, ob PatchManager automatische Softwareerkennungsaufträge und/oder Softwareverteilungsaufträge ausführen soll:
  - **Manuell**: PatchManager führt keine automatischen Softwareerkennungsaufträge oder Softwareverteilungsaufträge aus.
  - **Patches mit hoher Priorität automatisch auf Anwendbarkeit prüfen**: Sobald ein Patch mit hoher Priorität freigegeben wird, wird PatchManager die Anwendbarkeit automatisch für alle Clients überprüfen. Für kritische Patches brauchen Sie dann keine separaten Patchanwendbarkeitsjobs mehr definieren.
  - **Patches mit hoher Priorität automatisch installieren**: Sobald ein Patch mit hoher Priorität freigegeben wird, wird PatchManager den Patch automatisch auf allen Clients installieren (falls er anwendbar ist). Dies könnte zu Kompatibilitätsproblemen auf den Clients führen. Die Kompatibilität sollte vorher auf einer Auswahl von Testclients überprüft werden.
- **Der Benutzer darf Patches anzeigen und anfordern**: Der Benutzer darf verfügbare Patches anzeigen und die Bereitstellung anfordern.
- **Der Benutzer darf die Installation von Patches ablehnen**: Der Benutzer darf eine Patch-Installation zumindest zeitweise verweigern. Sie können hierbei festlegen, wie oft der Anwender die Installation ablehnen kann, bis die Installation zwangsweise durchgeführt wird und bestimmen, wie oft eine Patch-Installation vom System versucht werden soll.



4.3.13.3. Patch-Konfiguration

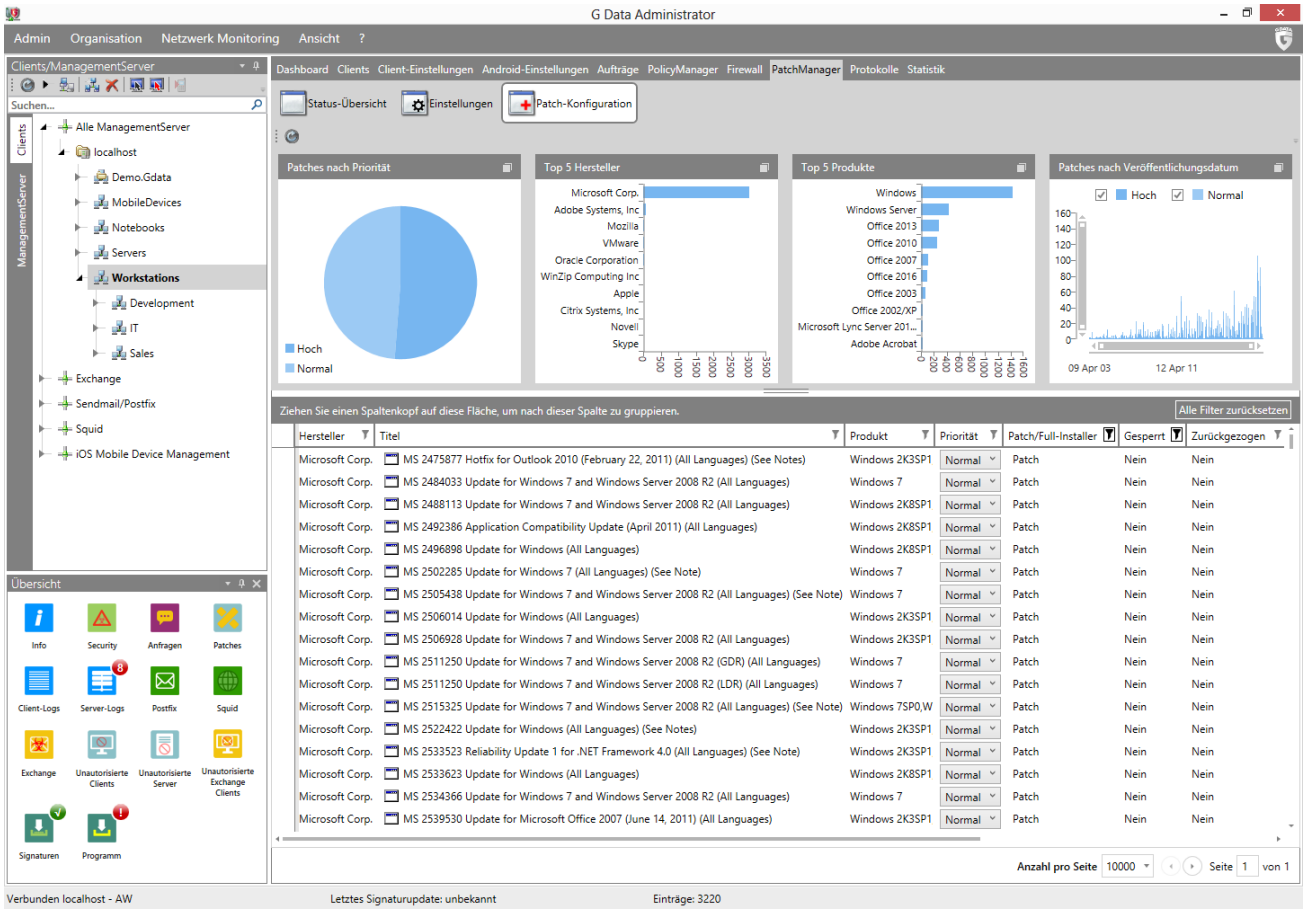
Im Bereich Patch-Konfiguration können Sie alle bekannten systemweiten Patches zentral verwalten. Eine Reihe von Grafiken zeigt Statistiken über Patches, Produkte und Hersteller.

Standardmäßig sind Patches nach **Hersteller**, **Produkt** und **Priorität** gruppiert, so dass Sie schnell

Patches für das jeweilige Produkt finden. Darüber hinaus sind standardmäßig Filter aktiv, die vollständige Software-Pakete sowie gesperrte Patches ausblenden. Wählen Sie **Alle Filter zurücksetzen**, um alle Listeneinträge anzeigen zu lassen. Patches, die einen vorherigen Patch ersetzen, können ausgeklappt werden: Klicken Sie auf das jeweilige Pluszeichen, um alle ersetzten Patches anzuzeigen.

Pro Patch können Sie verschiedene Aufträge planen. Wählen Sie einen oder mehrere Patches mit der rechten Maustaste und klicken Sie eine der folgenden Optionen an:

- **Patches auf Anwendbarkeit prüfen**: Planen Sie mit Hilfe vom **Softwareerkennungs**-Fenster einen Auftrag, der die selektierten Patches auf Anwendbarkeit auf dem selektierten Client prüft.
- **Patches installieren**: Planen Sie mit Hilfe vom **Softwareverteilungs**-Fenster einen Auftrag, der die selektierten Patches auf dem selektierten Client installiert.
- **Patches sperren**: Sperrt einen oder mehrere Patches, die nicht verteilt werden sollen. Gesperrte Patches werden von automatischen Softwareerkennungsaufträgen und Softwareverteilungsaufträgen ignoriert. Wenn Sie einen manuellen Softwareerkennungs- oder Softwareverteilungsauftrag planen, werden gesperrte Patches standardmäßig ausgeblendet.
- **Patches entsperren**: Entsperrt einen oder mehrere Patches.
- **Eigenschaften**: Zeigt weitere Informationen an, wie z. B. eine komplette Beschreibung und den Lizenztext.



Die **Priorität**-Spalte zeigt die Priorität von jedem Patch an. Die hier vorgegebenen Standardprioritäten, die auf den Vorgaben der internen PatchManager-Datenbank basieren, können auch von Ihnen geändert werden.

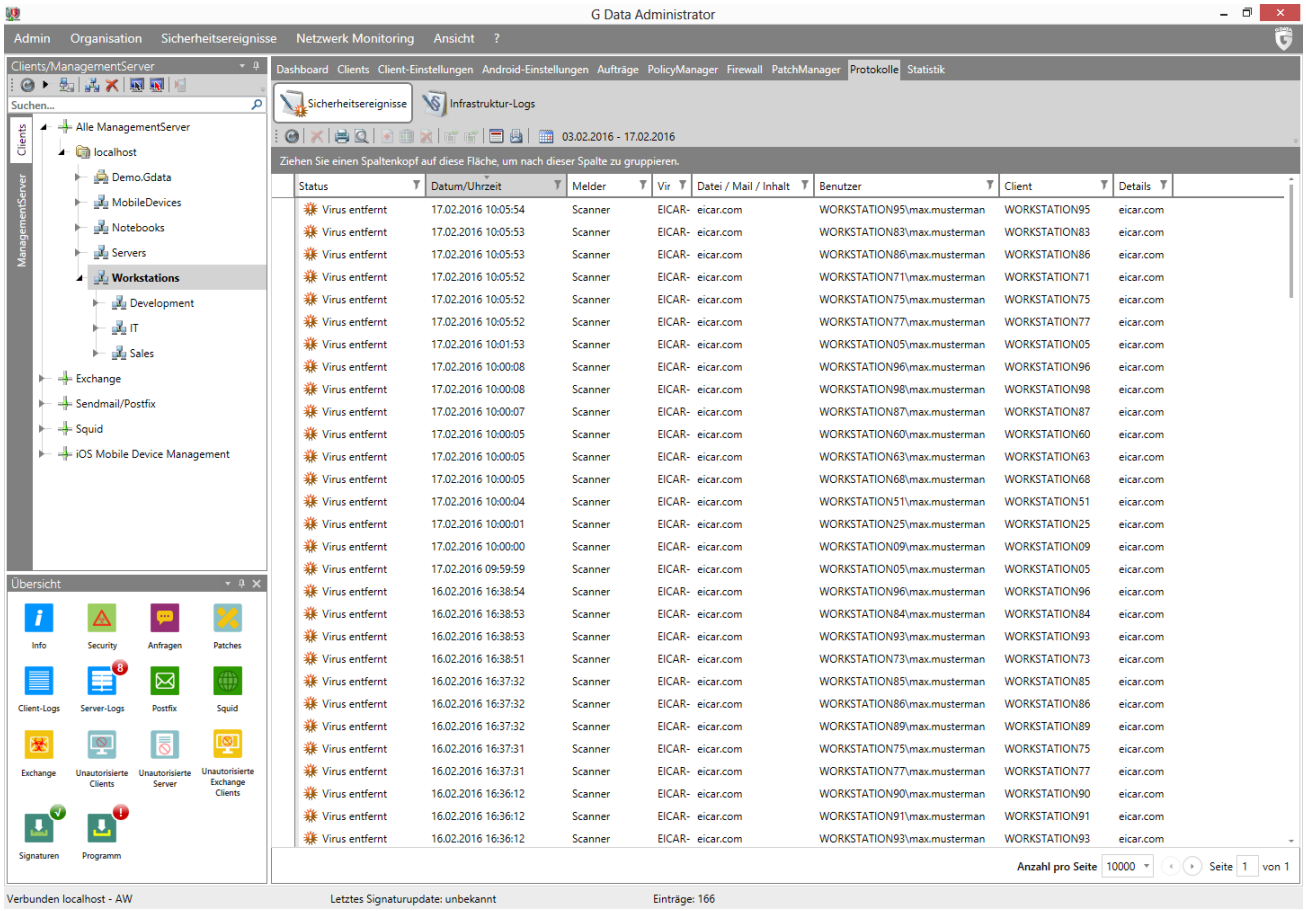
4.3.14. Protokolle

Das Modul Protokolle zeigt clientseitige **Sicherheitsereignisse**, wie z. B. Virenberichte und PolicyManager-Anfragen, und **Infrastruktur-Logs**, wie z. B. geänderte Einstellungen und Statusinformationen für Scanaufträge.

4.3.14.1. Sicherheitsereignisse

Im Bereich Sicherheitsereignisse werden Meldungen wie zum Beispiel Virenfunde, Meldungen des PolicyManagers, PatchManager-Berichte sowie Firewall-Meldungen angezeigt. Darüber hinaus werden zusätzlich systemrelevante Meldungen über Installationen, Berichte, Aufforderungen zum Neustart von Clients usw. hier aufgelistet. In der **Status**-Spalte wird der Berichtstyp angezeigt (z. B. **Virus gefunden** oder **Quarantäne: Datei in Quarantäne verschoben**).

Wenn Sie die Scanaufträge auf Ihrem System so eingestellt haben, dass diese den Virenbefall lediglich protokollieren, können Sie die Virenbekämpfung auch manuell durchführen. Wählen Sie eine oder mehrere protokollierten Dateien und anschließend einen Befehl im Kontextmenü (rechte Maustaste), im Menü **Sicherheitsereignisse** oder in der Symbolleiste. So lassen sich beispielsweise infizierte Dateien löschen oder in den Quarantäne-Ordner verschieben.



Über das Sicherheitsereignisse-Menü und Kontextmenü sind die folgenden Optionen verfügbar:

- **Ansicht**: Hier können Sie festlegen, ob Sie alle Berichte sehen möchten oder nur eine bestimmte Art von Berichten.
  - **Abhängige Berichte ausblenden**: Wenn identische Berichte vorhanden sind (basiert auf die Felder **Client**, **Melder** und **Datei / Mail / Inhalt**), können Sie hiermit die Duplikate ausblenden. Nur der aktuellste Eintrag wird dann angezeigt.
  - **Gelesene Berichte ausblenden**: Hier können Sie die Berichte ausblenden, die Sie schon gelesen haben.

- **Virus aus der Datei entfernen** (nur bei Virenfunden): Versucht den Virus aus der Originaldatei zu entfernen.
- **Datei in die Quarantäne verschieben** (nur bei Virenfunden): Diese Funktion verschiebt die ausgewählten Dateien in den Quarantäne-Ordner. Die Dateien werden verschlüsselt im Quarantäne-Ordner auf dem G DATA ManagementServer gespeichert. Die Originaldateien werden gelöscht. Durch die Verschlüsselung ist sichergestellt, dass der Virus keinen Schaden anrichten kann. Beachten Sie, 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 die **G DATA Security Labs** senden. Öffnen Sie dazu das Kontextmenü eines Quarantäne-Berichts mit einem Rechtsklick. In dem Berichtdialog klicken Sie dann nach Wahl des Einsendegrunds die Schaltfläche OK.
- **Datei entfernen** (nur bei Virenfunden): Löscht die Originaldatei auf dem Client.
- **Als Wächterausnahme definieren** (nur bei Virenfunden; nur im Kontextmenü): Definiert eine Wächterausnahme für die betroffene Datei (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**).
- **Als ExploitProtection-Ausnahme definieren** (nur für ExploitProtection-Berichte; nur im Kontextmenü): Definiert eine ExploitProtection-Ausnahme für das betroffene Programm (siehe **Client-Einstellungen** > **Wächter** > **ExploitProtection**).
- **Tastatur-Freigabe zurücknehmen**: Nimmt die Freigabe zurück für Tastaturen, die vom USB Keyboard Guard blockiert und anschließend vom Benutzer freigegeben wurden.
- **Quarantäne: Säubern und zurückbewegen** (nur bei Quarantäne-Berichte): 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** (nur bei Quarantäne-Berichte): Verschiebt die Datei aus dem Quarantäne-Ordner zurück auf den Client. **Achtung**: Die Datei wird in ihrem Originalzustand wiederhergestellt und ist weiterhin infiziert.
- **Quarantäne: An G DATA Security Labs senden** (nur bei Quarantäne-Berichte): Sollten Sie einen neuen Virus oder ein unbekanntes Phänomen feststellen, senden Sie uns in jedem Fall diese Datei über die Quarantäne-Funktion der G DATA Software. Selbstverständlich behandeln wir Ihre eingesandten Daten höchst vertraulich und diskret.
- **Quarantäne: Datei und Bericht löschen** (nur bei Quarantäne-Berichte): Löscht die gewählten Berichte und Quarantäne-Dateien.
- **Url auf die Whitelist setzen** (nur bei Berichten der **Web-Inhaltskontrolle**): Fügt die jeweilige URL zur Whitelist hinzu.
- **Url auf die Blacklist setzen** (nur bei Berichten der **Web-Inhaltskontrolle**): Fügt die jeweilige URL zur Blacklist hinzu.
- **Bericht entfernen**: Hiermit löschen Sie die ausgewählten 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.
- **Berichte aufräumen**: Wenn identische Berichte vorhanden sind (basiert auf die Felder **Client**, **Melder** und **Datei / Mail / Inhalt**), können Sie hiermit die Duplikate entfernen.

  Die Funktion Berichte aufräumen betrachtet nur Berichte, die in der aktuellen Anzeige enthalten sind. Wenn ein Filter aktiv ist, werden ausgefilterte Berichte nicht aufgeräumt. Wenn die Berichteliste sich über mehrere Seiten erstreckt, werden nur die auf der aktuellen Seite

angezeigten Berichte aufgeräumt.

- **Berichte exportieren** (nur im Kontextmenü): Ausgewählte oder alle Berichte als XML-Datei exportieren.
- **Als gelesen markieren** (nur im Kontextmenü): Ausgewählte Berichte als gelesen markieren.
- **Als ungelesen markieren** (nur im Kontextmenü): Ausgewählte Berichte als ungelesen markieren.
- **Details/Aktionen** (nur im Kontextmenü): Über einige Berichte können Sie direkt einen Auftrag einplanen. Zum Beispiel: Falls ein Client einen Patch-Rollback angefordert hat, können Sie über **Details/Aktionen** das **Softwareverteilungs**-Fenster öffnen. Sie können dann direkt einen Rollback-Auftrag einplanen, ohne das PatchManager-Modul öffnen zu müssen.

Die Symbolleiste des Sicherheitsereignisse-Moduls bietet eine breite Palette von Optionen und Filter-Einstellungen:

- **Aktualisieren**
- **Löschen**
- **Drucken**
- **Seitenansicht**
- **Virus entfernen**
- **In Quarantäne verschieben**
- **Datei löschen**
- **Datei aus der Quarantäne zurückbewegen**
- **Datei säubern und aus der Quarantäne zurückbewegen**
- **Abhängige Berichte ausblenden**
- **Gelesene Berichte ausblenden**
- **Zeitraum**

4.3.14.2. Infrastruktur-Logs

Der Bereich Infrastruktur-Logs zeigt Client-Informationen an, wie zum Beispiel Statusinformationen für Scanaufträge, Aktualisierungen der Virensignaturen und geänderte Einstellungen.

Klicken Sie mit der rechten Maustaste auf einen beliebigen Eintrag, um folgendes Kontextmenü zu öffnen:

- **Aktualisieren**
- **Löschen**
- **Als gelesen markieren**: Ausgewählte Berichte als gelesen markieren.
- **Als ungelesen markieren**: Ausgewählte Berichte als ungelesen markieren.
- **Exportieren**: Ausgewählte oder alle Berichte als XML-Datei exportieren.

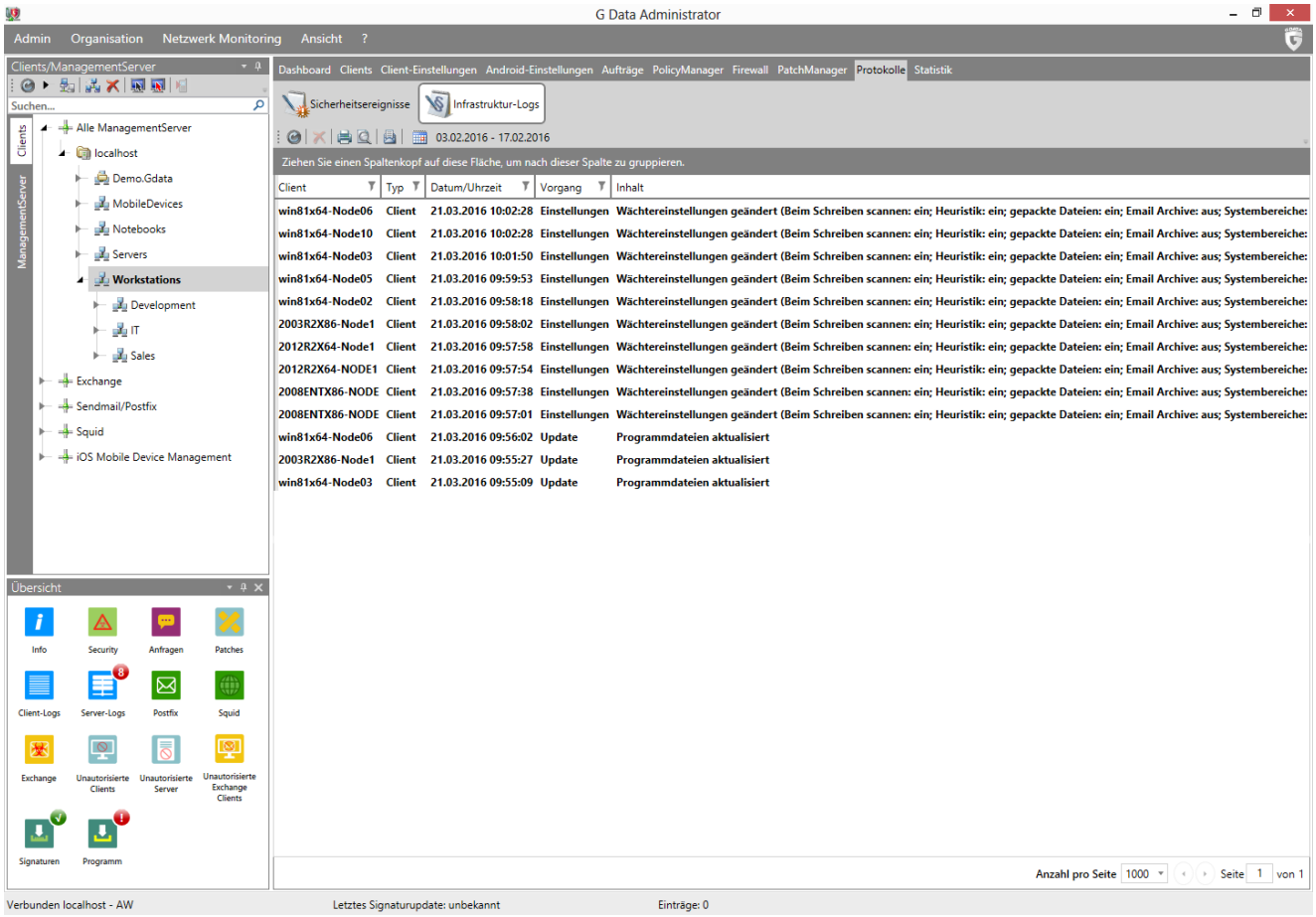
Die Symbolleiste bietet die folgenden Einstellungen:

- **Aktualisieren**
- **Löschen**
- **Drucken**

Seitenansicht

Gelesene Berichte ausblenden

Zeitraum

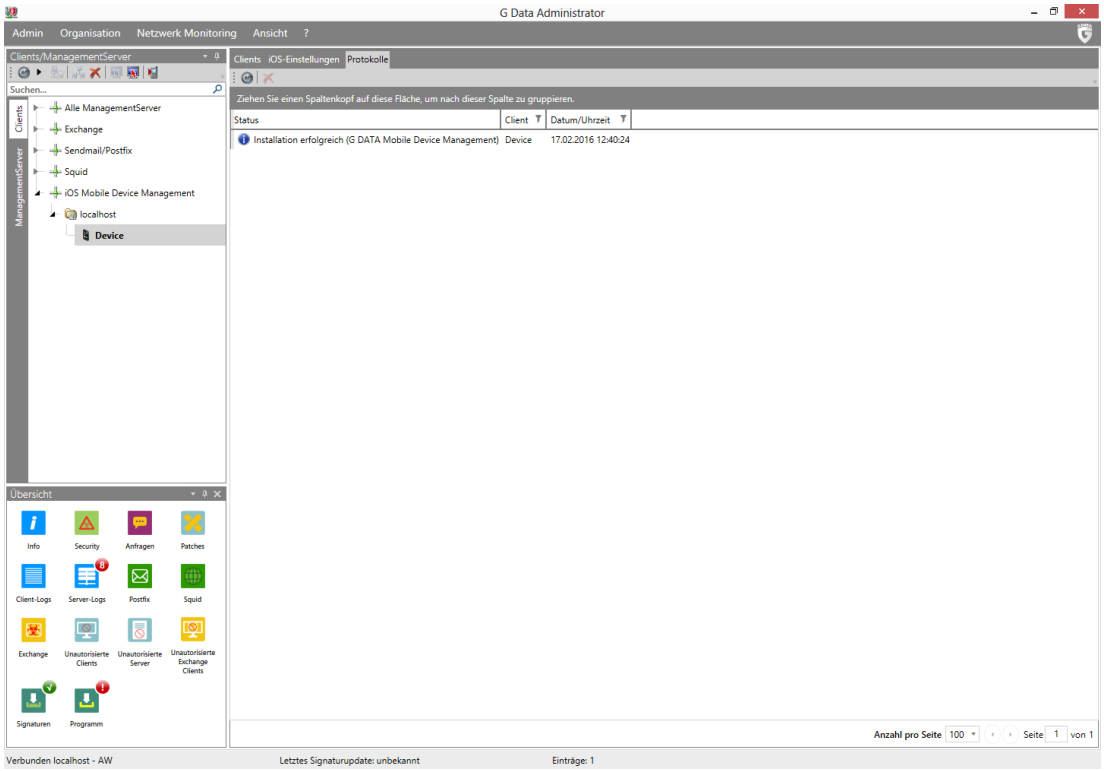


4.3.15. Protokolle (iOS)

Wenn Sie im **Clients**-Bereich einen oder mehrere iOS-Clients ausgewählt haben, werden im Protokolle-Modul nur Berichte, die auf die ausgewählten iOS-Clients zutreffen, angezeigt. Berichte enthalten z. B. Statusinformationen über die Profilverwaltung sowie Antidiebstahlaktionen.

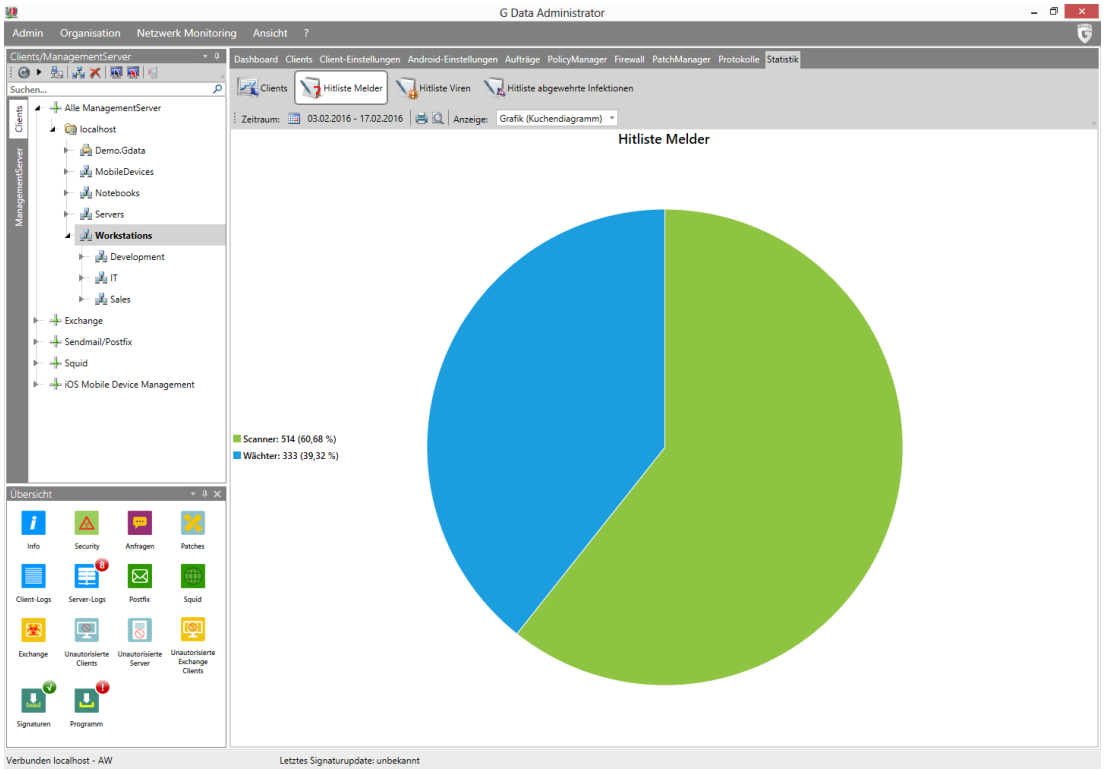
- **Status**: Der Bericht-Status.
- **Client**: Der Client-Name.
- **Datum/Uhrzeit**: Datum und Uhrzeit des Berichts.

Klicken Sie mit der rechten Maustaste auf einen Bericht und wählen Sie **Löschen**, um den Bericht aus der Liste zu löschen.



4.3.16. Statistik

In diesem Aufgabenbereich können Sie sich statistische Informationen zum Virenaufkommen und zu Infektionen auf den Clients bzw. Exchange-Server anzeigen lassen, sowie den Sicherheitsstatus des verwalteten Netzwerks.



Es stehen verschiedene Ansichten zur Verfügung: so kann die Darstellung der Informationen in Textform erfolgen oder auch grafisch aufbereitet werden (Säulen- oder Kuchendiagramm). Die entsprechende Ansicht lässt sich unter **Anzeige** auswählen. Es stehen Informationen bereit über die **Clients** (nicht verfügbar falls ein Exchange-Client selektiert wurde), über die **Hitliste Melder**, die **Hitliste Viren** und über die **Hitliste abgewehrte Infektionen**.

4.4. Server-Module

Mit den Server-Modulen können Sie den Server, den Sie im **ManagementServer**-Bereich ausgewählt haben, verwalten.

4.4.1. Server

Das Modul Server bietet Server-Verwaltungsfunktionen, wie zum Beispiel Versions- und Statusinformationen, Subnet-Serververwaltung, Benutzerverwaltung und Protokolle.

4.4.1.1. Übersicht

Mit Hilfe des Server-Bereichs können Sie Server-Statusinformationen kontrollieren und Subnet-Server installieren und verwalten. Die folgenden Servereigenschaften werden angezeigt:

- **Name**: Der Servername.
- **Typ**: Der Servertyp (**Haupt-Server**, **Subnet-Server**, **Secondary-Server**).
- **Server**: Der Name des übergeordneten ManagementServers (nur für Subnet- und Secondary-Server).
- **Anzahl Clients**: Die Anzahl der Clients, die dem ausgewählten Server zugeordnet sind.
- **Letzter Zugriff**: Datum und Zeit der letzten Synchronisation mit dem ManagementServer (nur für Subnet-Server).
- **Datenstand**: Datum und Zeit der letzten Aktualisierung der Virensignaturen.
- **Version**: Die Versionsnummer und das Datum.
- **Status**: Server-Statusinformationen, z. B. Update-Status.
- **Programmaktualisierung**: Wenn ein Update für einen Subnet-Server vorliegt, wird der Status hier angezeigt.

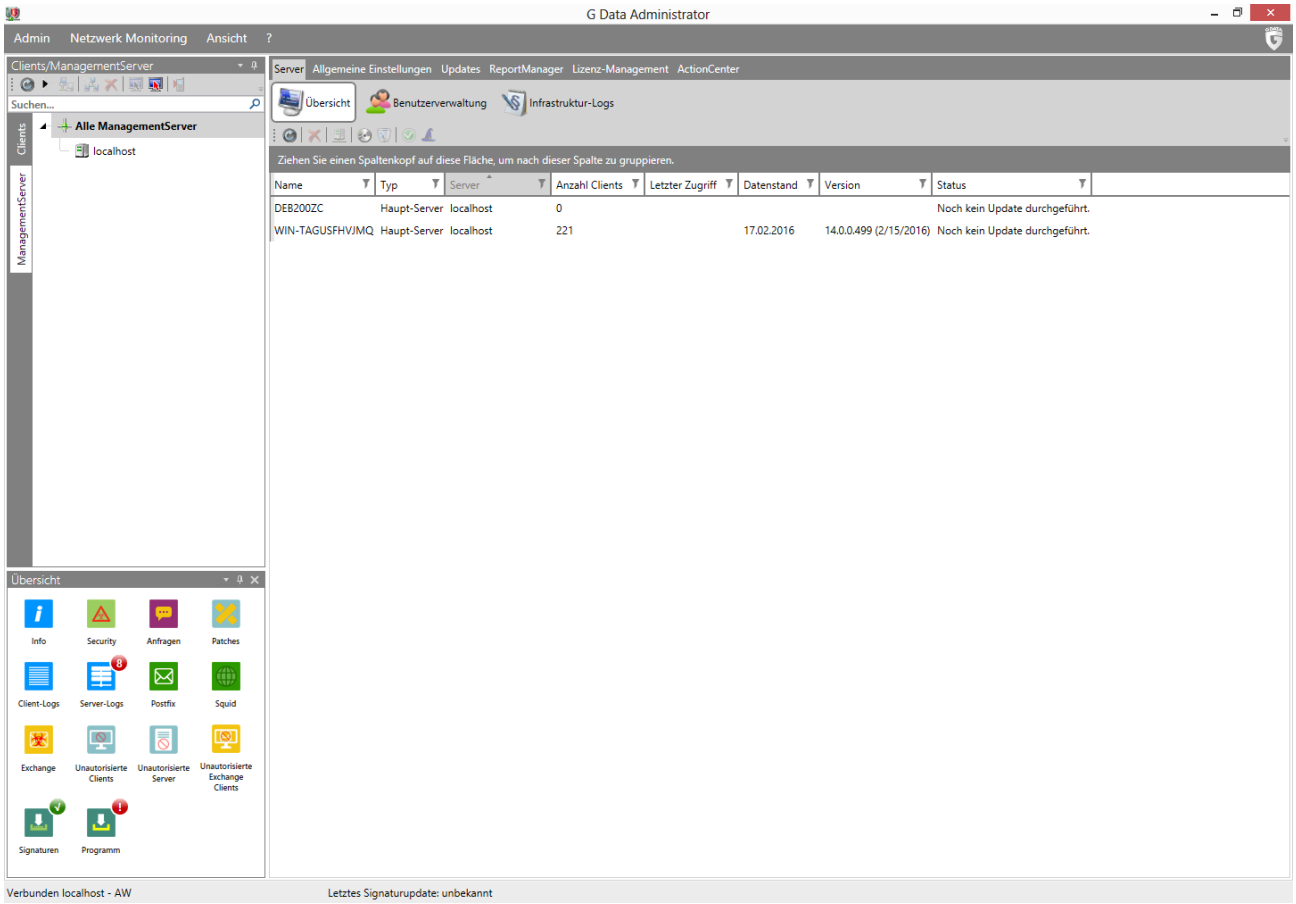
Über die Symbolleiste und das Kontextmenü sind die folgenden Optionen verfügbar:

- **Aktualisieren**
- **Server-Einrichtungsassistent**
- **Entfernen**: Entfernt einen oder mehrere Subnet-Server aus der Liste. Die eigentliche Software auf dem Subnet-Server wird nicht entfernt.
- **Synchronisieren** (nur im Kontextmenü): Um eventuelle Änderungen auch außerhalb des regulären Kommunikationsintervalls von Server und Subnet-Server zu ermöglichen, kann die Subnet-Server-Synchronisation auch manuell angestoßen werden.
- **Clients zuordnen**: Sie können die Clients einzelnen Subnet-Servern zuordnen, die dann die Kommunikation dieser Clients mit dem Haupt-Server bündeln und auf diese Weise die Netzwerknutzung optimieren. Die Zuordnung der Clients zu Subnet-Servern ist unabhängig von der Gruppierung von Clients im Bereich **Clients/ManagementServer**. Daher können Clients, die unterschiedlichen Subnet-Servern zugeordnet sind, dennoch in Gruppen unterteilt werden.
- **Subnet-Server installieren**: Klicken Sie auf Subnet-Server installieren, um einen neuen Subnet-Server zu konfigurieren. Geben Sie den **Computernamen** des Subnet-Servers, sowie ein **Benutzerkonto** mit Administrator-Berechtigungen auf dem neuen Subnet-Server ein. Bestätigen Sie die Eingaben mit **OK**, um eine Remote-Installation zu starten. Das Fenster **Installationsübersicht** ermöglicht es Ihnen, den Installationstatus zu beobachten. Die Remote-Installation für Subnet-Server hat die gleichen Voraussetzungen wie eine **Client-**

Remote-Installation. Der vom Subnet-Server verwendete Microsoft SQL Server 2014 Express bietet keine Unterstützung für Windows Vista und Windows Server 2008/2003. Führen Sie auf solchen Systemen die Subnet-Server-Variante der **lokalen Installation** des G DATA ManagementServers durch.

- **Server deinstallieren**: Initialisiert eine Remote-Deinstallation der gewählten Subnet-Server. Den Installationsstatus können Sie im Fenster **Installationsübersicht** beobachten. Eine Remote-Deinstallation kann nur für autorisierte Subnet-Server vorgenommen werden.
- **Autorisation erteilen**: Um unberechtigten Zugriff auf Server-Daten zu verhindern, müssen lokal installierte Subnet-Server autorisiert werden. Erst nach der Autorisation wird der Managementserver Daten mit dem Subnet-Server synchronisieren.

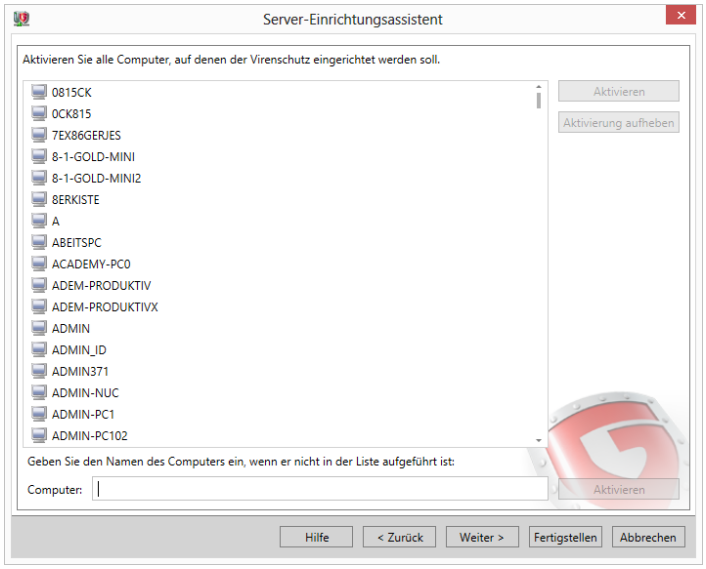
  Subnet-Server, die über eine Remote-Installation hinzugefügt werden, werden automatisch autorisiert. Nur lokal installierte Subnet-Server und Subnet-Server, die über Version 12 oder älter verfügten und aktualisiert wurden, müssen manuell autorisiert werden.
- **Programmaktualisierung freigeben** (nur im Kontextmenü): Subnet-Server mit Version 12 des ManagementServers erfordern eine manuelle Installation eines Datenbankservers, bevor sie auf Version 14 aktualisiert werden können. Installieren Sie auf solchen Systemen zuerst manuell den Microsoft SQL Server 2014 Express (Windows Server 2008 R2/Windows 7 und höher) bzw. Microsoft SQL Server 2008 R2 Express (Windows Server 2003/2008/Windows Vista). Geben Sie dann die Programmaktualisierung frei. Unmittelbar nach der Aktualisierung konfigurieren Sie auf dem Subnet-Server die Verbindung zur Datenbank mit Hilfe von GdmmsConfig.exe. Mehr Informationen hierzu finden Sie im Reference Guide.
- **Eigenschaften** (nur im Kontextmenü): Eigenschaften für den ausgewählten Server, wie zum Beispiel die Version des ManagementServers, der Virensignaturen und der Client-Programmdateien.



Server-Einrichtungsassistent

Mit dem Einrichtungsassistenten lassen sich die wichtigsten Einstellungen des G DATA ManagementServers konfigurieren. Der Einrichtungsassistent wird automatisch beim ersten Starten des G DATA Administrators ausgeführt, kann aber auch nachträglich jederzeit über das **Admin**-Menü erneut durchgeführt werden.

Zunächst müssen alle Clients, die von der G DATA Software verwaltet werden sollen, aktiviert werden. Die zu aktivierenden Clients müssen zunächst markiert und mit einem Klick auf **Aktivieren** aktiviert werden. Eventuell sind einige Computer nicht in der Liste enthalten (z. B. weil die betreffenden Rechner lange nicht eingeschaltet waren oder keine Datei- bzw. Druckerfreigabe eingerichtet haben). Zum Aktivieren dieser Clients wird im Eingabefeld **Computer** der Name des Rechners eingegeben. Nach einem Klick auf **Aktivieren** wird der zu aktivierende Rechner in die Clientliste aufgenommen. Wenn alle zu schützenden Rechner aktiviert wurden, folgt nach einem Klick auf **Weiter** der nächste Schritt. Wenn Sie Clients aktiviert haben, ist das Häkchen bei **Client-Software automatisch auf den aktivierten Computern installieren** voreingestellt. Wenn die Verteilung der Software auf den Client-Rechnern zu einem späteren Zeitpunkt erfolgen soll, muss diese Option durch Entfernen des Häkchens deaktiviert werden.



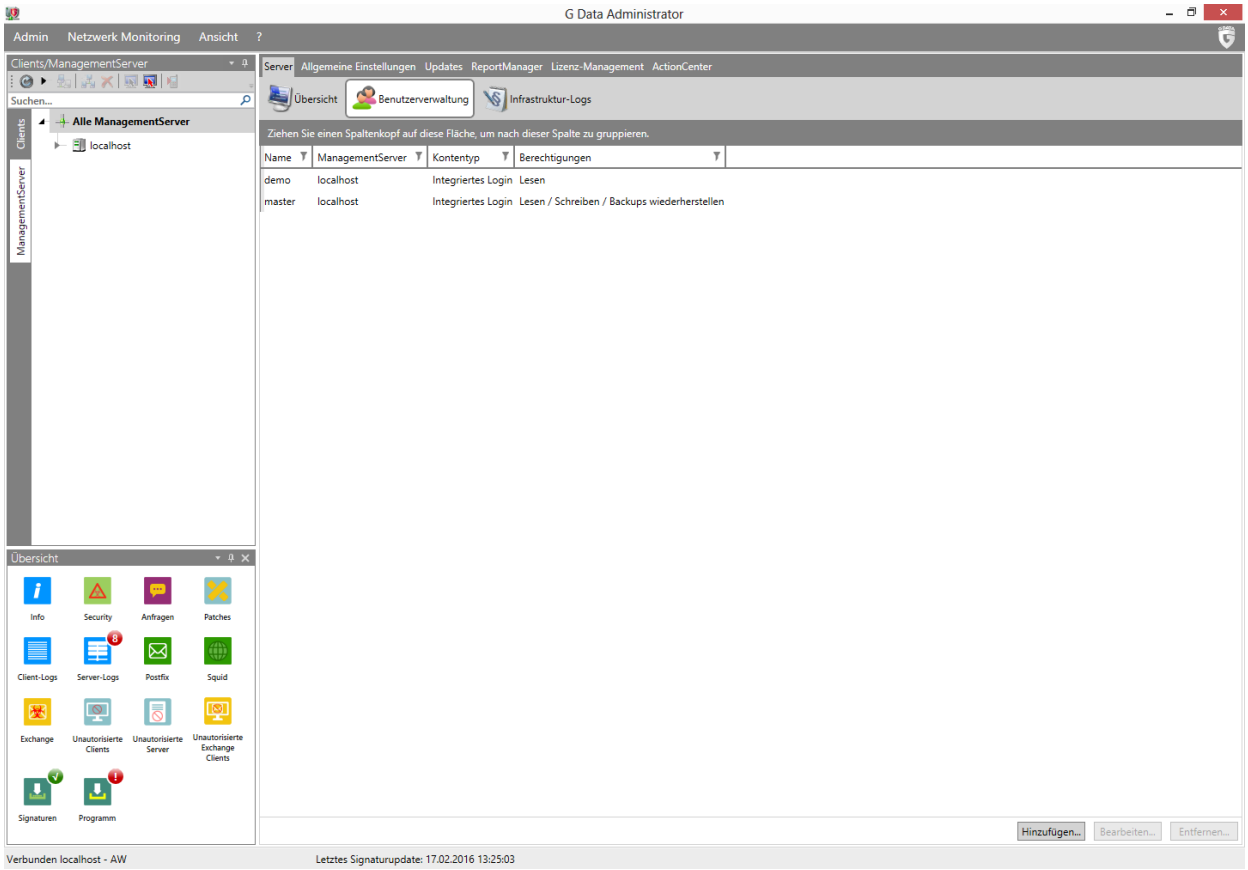
Mit den darauf folgenden Schritten können Sie die wichtigsten Einstellungen konfigurieren:

- **Internet-Update**: Einstellungen für die Aktualisierung der Virensignaturen und Programmdateien. Mehr Informationen finden Sie unter **Updates**.
- **E-Mail-Benachrichtigung**: Einstellungen für den Mail-Server, die E-Mail-Gruppen und Alarmmeldungen. Mehr Informationen finden Sie unter **Allgemeine Einstellungen** > **E-Mail**.
- **Einstellungen für mobile Geräte**: Einstellungen für das Android Mobile Device Management. Mehr Informationen finden Sie unter **Allgemeine Einstellungen** > **Android**.
- **Einstellung für den Zugang zum G DATA ActionCenter**: Zugangsdaten für G DATA ActionCenter müssen eingegeben werden, wenn Sie das iOS Mobile Device Management oder Netzwerk Monitoring verwenden möchten. Mehr Informationen finden Sie unter **ActionCenter**.

Mit **Fertigstellen** wird der Assistent beendet. Wenn Sie die Option **Client-Software automatisch auf den aktivierten Computern installieren** ausgewählt haben, führt der Einrichtungsassistent eine **Remote-Installation** des G DATA Security Clients auf allen ausgewählten Netzwerk-Geräten durch.

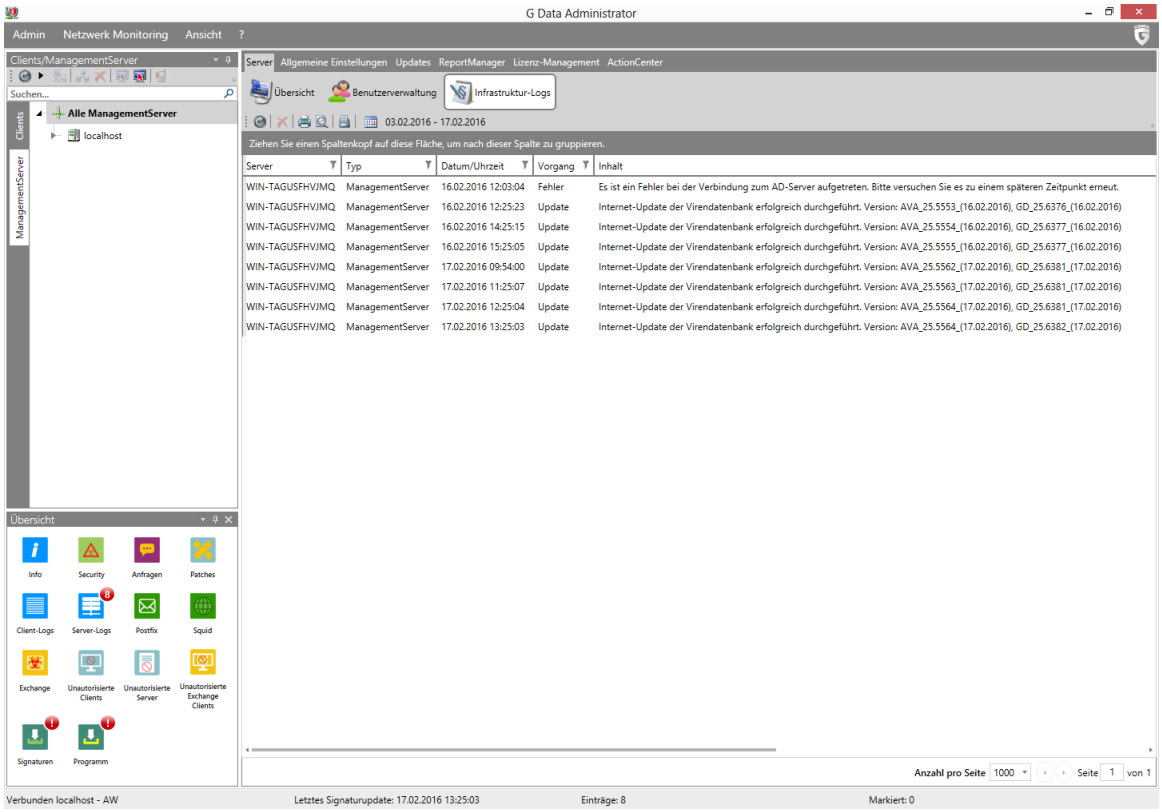
4.4.1.2. Benutzerverwaltung

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



4.4.1.3. Infrastruktur-Logs

Der Bereich Infrastruktur-Logs zeigt Server-Statusinformationen an, wie zum Beispiel für die Aktualisierung der Virensignaturen und Programmdateien. Die Optionen in der Symbolleiste und im Kontextmenü sind identisch zu den Optionen im Client-Modul **Protokolle** > **Infrastruktur-Logs**.

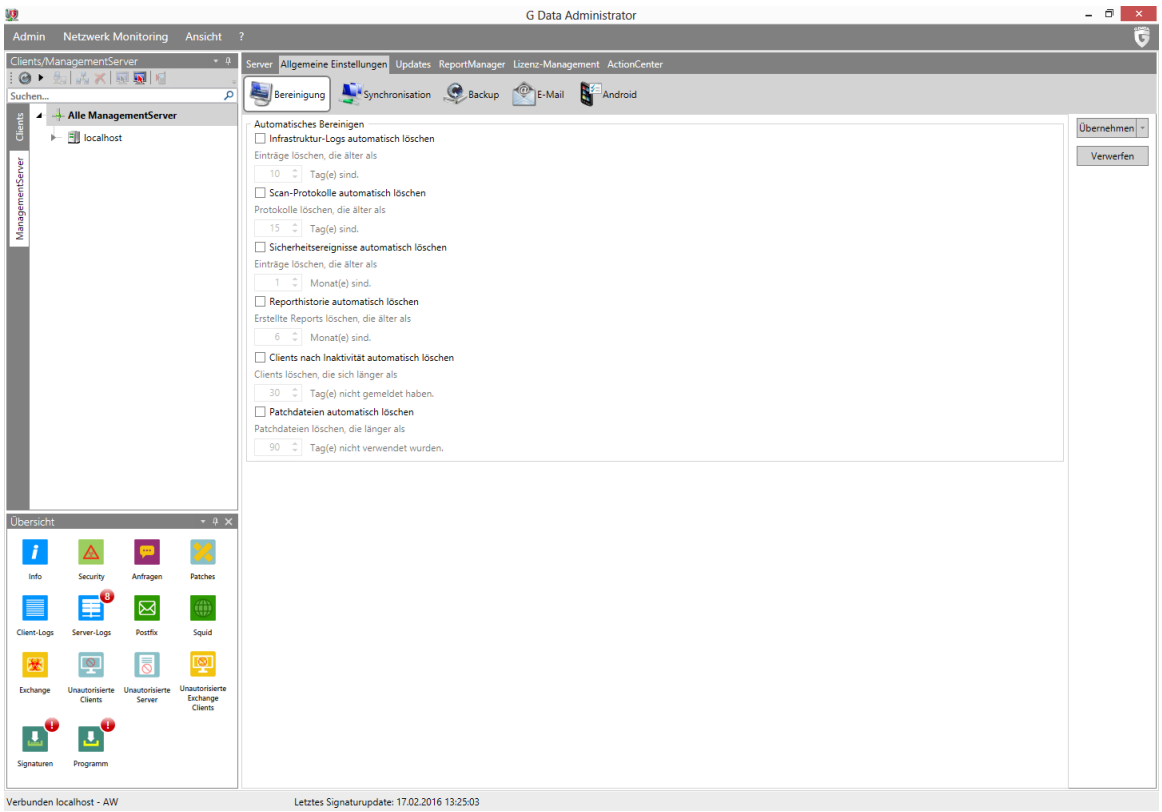


4.4.2. Allgemeine Einstellungen

Über die Allgemeine Einstellungen können Sie unter anderem die Subnet-Server- und Client-Synchronisation verwalten, sowie Backup-Pfade, E-Mail-Server-Einstellungen und das Android Mobile Device Management.

4.4.2.1. Bereinigung

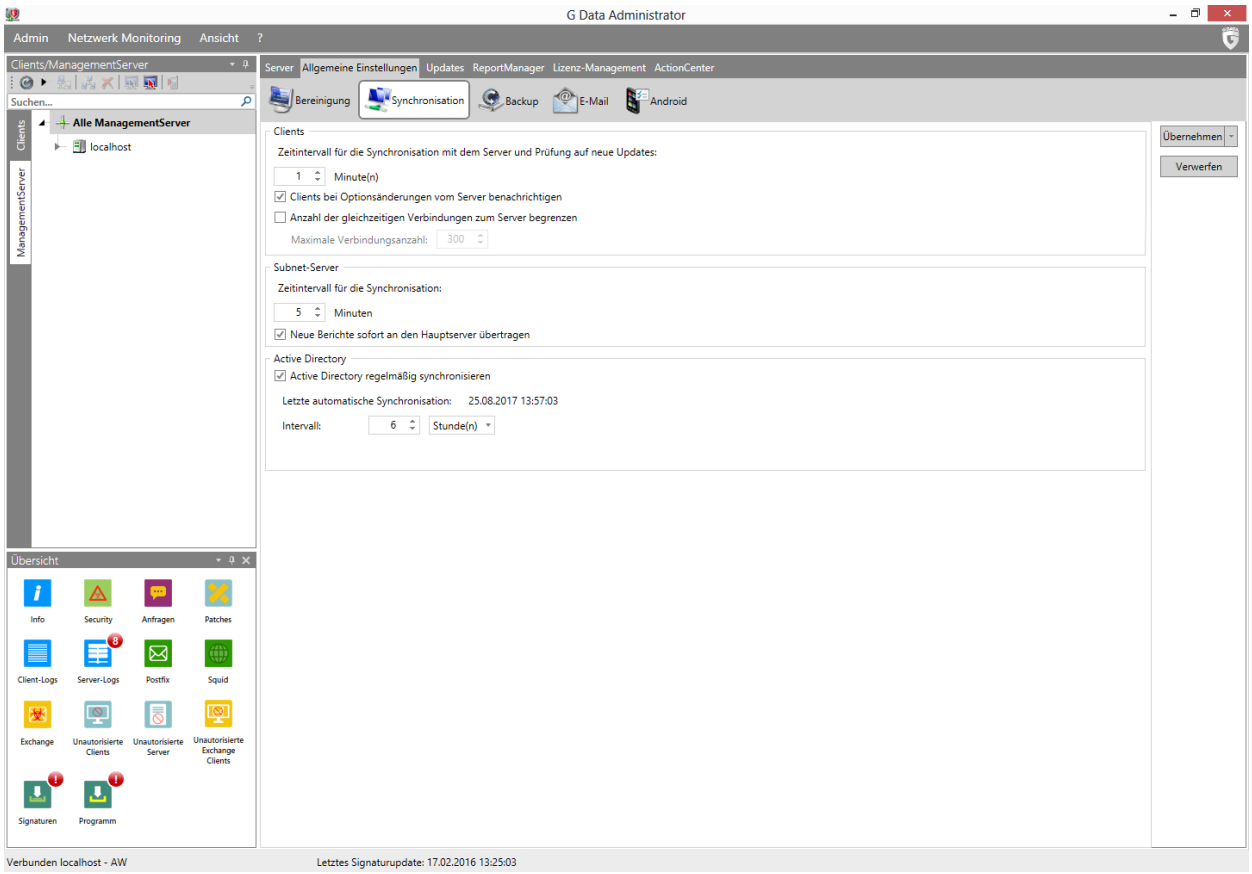
Legen Sie unter **Automatisches Bereinigen** fest, ob alte Updates automatisch nach einer gewissen Zeit gelöscht werden sollen:



- **Infrastruktur-Logs automatisch löschen**: Infrastruktur-Logs, die älter als eine gewisse Anzahl von Tagen sind, können automatisch gelöscht werden.
- **Scan-Protokolle automatisch löschen**: Scan-Protokolle, die älter als eine gewisse Anzahl von Tagen sind, können automatisch gelöscht werden.
- **Sicherheitsereignisse automatisch löschen**: Sicherheitsereignisse, die älter als eine gewisse Anzahl von Monaten sind, können automatisch gelöscht werden.
- **Reporthistorie automatisch löschen**: ReportManager-Berichte, die älter als eine gewisse Anzahl von Monaten sind, können automatisch gelöscht werden.
- **Clients nach Inaktivität automatisch löschen**: Clients, die sich länger als eine gewisse Anzahl von Tagen nicht beim ManagementServer gemeldet haben, können automatisch gelöscht werden.
- **Patchdateien automatisch löschen**: Patchdateien, die länger als eine gewisse Anzahl von Tagen nicht verwendet wurden, können automatisch gelöscht werden.

4.4.2.2. Synchronisation

Im Synchronisation-Bereich können Sie das Synchronisationsintervall zwischen dem ManagementServer und den Clients, Subnet-Servern und dem Active Directory definieren.



- **Clients**
  - **Zeitintervall für die Synchronisation mit dem Server und Prüfung auf neue Updates**: Geben Sie hier das Zeitintervall an, in dem sich die Clients mit dem Server verbinden sollen, um zu prüfen, ob neue Updates und Einstellungen vorliegen. Als Standardwert sind fünf Minuten festgelegt.
  - **Clients bei Optionsänderungen vom Server benachrichtigen**: Wenn Sie dieses Häkchen setzen, werden die Client-Rechner bei Optionsänderungen direkt mit dem Server synchronisiert, unabhängig von vorgegebenen Synchronisationsintervallen.

- **Anzahl der gleichzeitigen Verbindungen zum Server begrenzen**: Legen Sie fest, wie viele Clients sich gleichzeitig mit dem ManagementServer verbinden dürfen. Die Anzahl hängt von den Spezifikationen des Servers und der Netzwerkinfrastruktur ab. Falls Performanceprobleme auftreten, kann das Verringern dieser Anzahl die Server-Performanz verbessern.

- **Subnet-Server**
  - **Zeitintervall für die Synchronisation**: Über diesen Bereich können Sie das Zeitintervall für die Synchronisation zwischen Haupt-ManagementServer und Subnet-Server definieren.
  - **Neue Berichte sofort an den Hauptserver übertragen**: Wenn Sie dieses Häkchen setzen, dann werden Berichte unabhängig von den hier vorgenommenen Einstellungen sofort an den Hauptserver übertragen.
- **Active Directory**
  - **Active Directory regelmäßig synchronisieren**: Aktiviert die regelmäßige Synchronisation zwischen dem Active Directory und dem ManagementServer. Die Synchronisation erfolgt nur, wenn mindestens eine Gruppe einem Active Directory-Eintrag **zugewiesen** wurde.
  - **Intervall**: Legen Sie hier das Intervall fest, indem der G DATA ManagementServer das Active Directory synchronisieren soll. Wenn Sie eine tägliche Synchronisation einstellen, können Sie die Active Directory-Synchronisation für einen bestimmten Zeitpunkt planen.

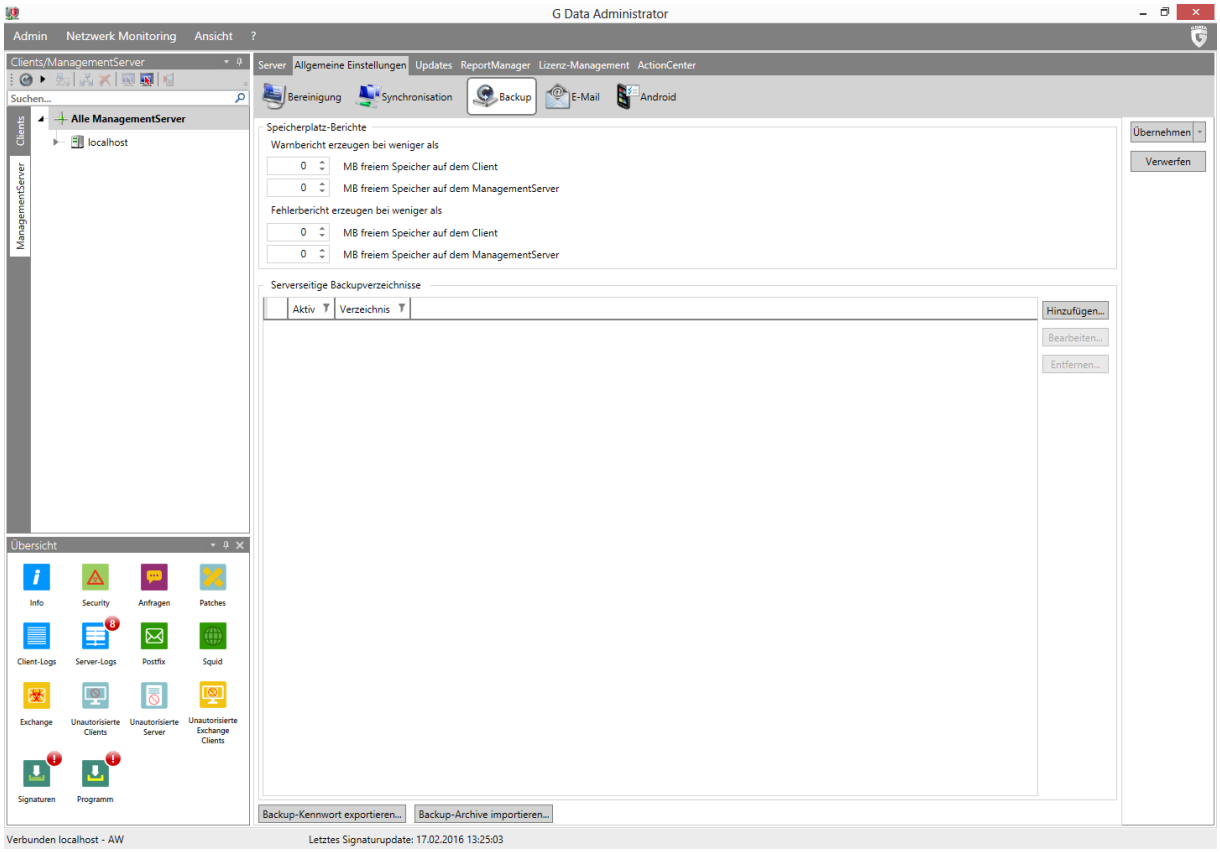
4.4.2.3. Backup

Das Backup-Modul ist als **optionales Modul** verfügbar.

Um sicherzustellen, dass Backupaufträge erfolgreich ausgeführt werden können, sollte sowohl auf dem Server (Backup-Speicher), als auch auf dem Client (Backup-Cache) ausreichend Speicherplatz verfügbar sein. Wenn der Speicherplatz auf dem Client oder Server den Schwellenwert für Warnberichte unterschreitet, wird unter **Sicherheitsereignisse** ein Warnbericht erzeugt und der Client-Cache automatisch gereinigt. Alle Backup-Archive, außer dem neuesten, werden gelöscht (nur wenn sie schon zum ManagementServer hochgeladen worden sind). Wenn der Speicherplatz auf dem Client oder Server den Schwellenwert für Fehlerberichte unterschreitet, wird unter **Sicherheitsereignisse** ein Fehlerbericht erzeugt. Der Backup-Speicher und der Client-Cache werden gereinigt. Falls danach immer noch nicht genügend Speicherplatz auf dem Server verfügbar ist, werden Backups nicht mehr durchgeführt.

Unter **Serverseitige Backupverzeichnisse** kann ein Pfad angegeben werden, auf dem alle auflaufenden Backups gespeichert werden sollen. Wird hier kein Verzeichnis angegeben, werden alle Backups unter C:\ProgramData\G Data\AntiVirus ManagementServer\Backup bzw. C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\G Data\AntiVirus ManagementServer\Backup gespeichert.

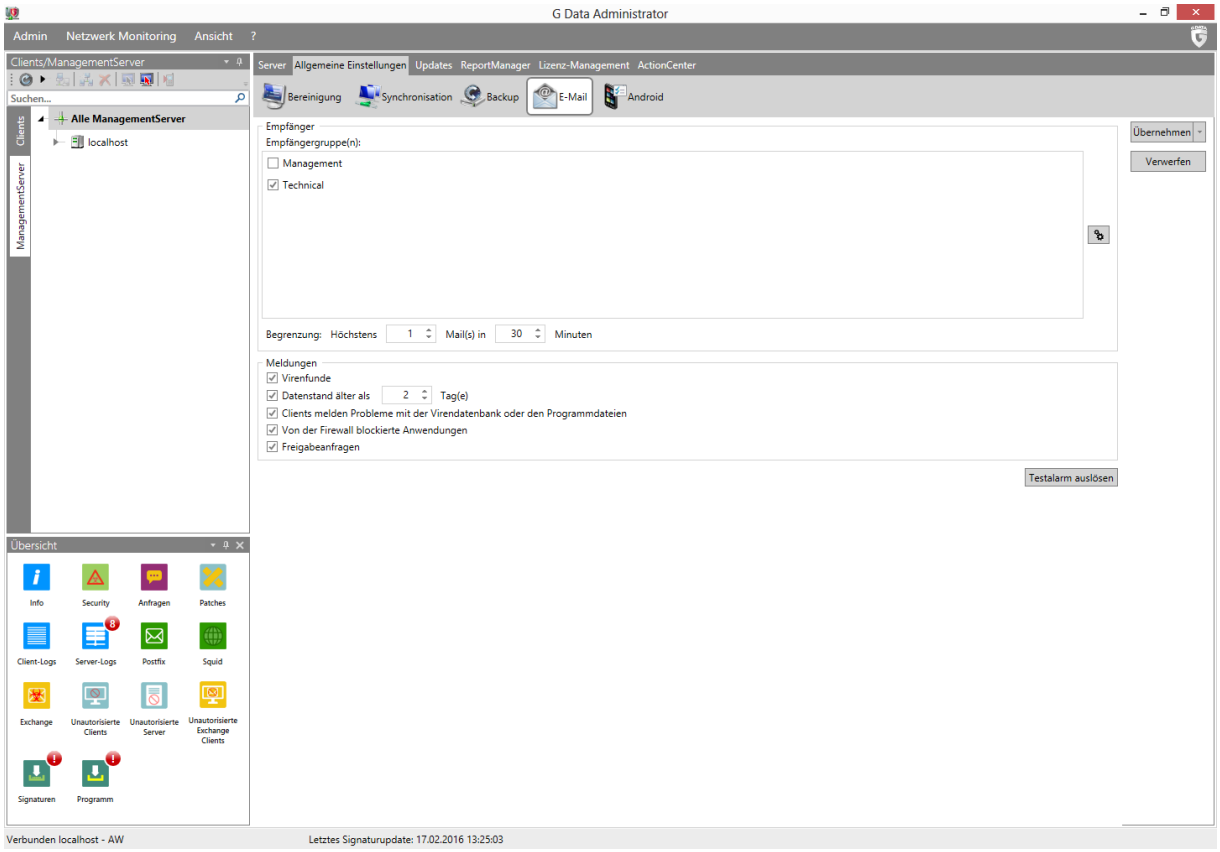
Da sämtliche mit der G DATA-Software erstellten Backups verschlüsselt sind, besteht auch die Möglichkeit, die Passwörter für die Backups zu exportieren und für eine spätere Verwendung zu speichern. Die Schaltfläche **Backup-Archive importieren** ermöglicht den Zugriff auf Backups, die in anderen Ordnern gespeichert sind.



4.4.2.4. E-Mail

G DATA ManagementServer kann bei bestimmten Ereignissen automatisch Alarmmeldungen per E-Mail versenden. Die dazu benötigten Einstellungen werden in diesem Bereich vorgenommen. Aktivieren Sie die E-Mail-Benachrichtigung, indem Sie unter **Meldungen** das Häkchen bei den jeweils meldbaren Ereignissen setzen. Über die **Begrenzung** kann ein übermäßiges Mailaufkommen im Fall eines massiven Virenbefalls verhindert werden. Klicken Sie auf **Testalarm auslösen**, um der Empfängergruppe einen Testalarm zu schicken.

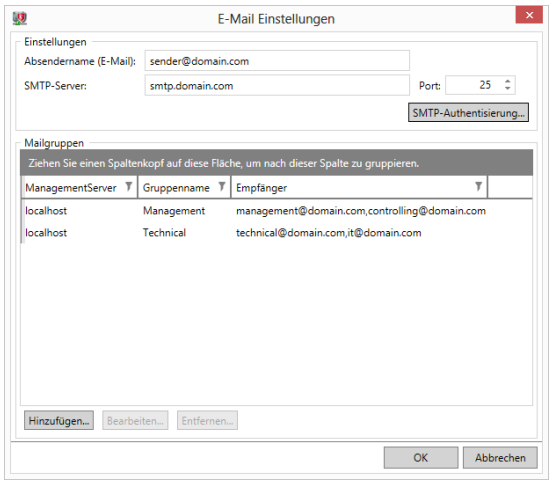
Um den Mail-Server und die Mail-Gruppen zu konfigurieren, klicken Sie bitte auf die Schaltfläche für erweiterte Einstellungen ( ) um das Fenster **E-Mail-Einstellungen** zu öffnen.



E-Mail Einstellungen

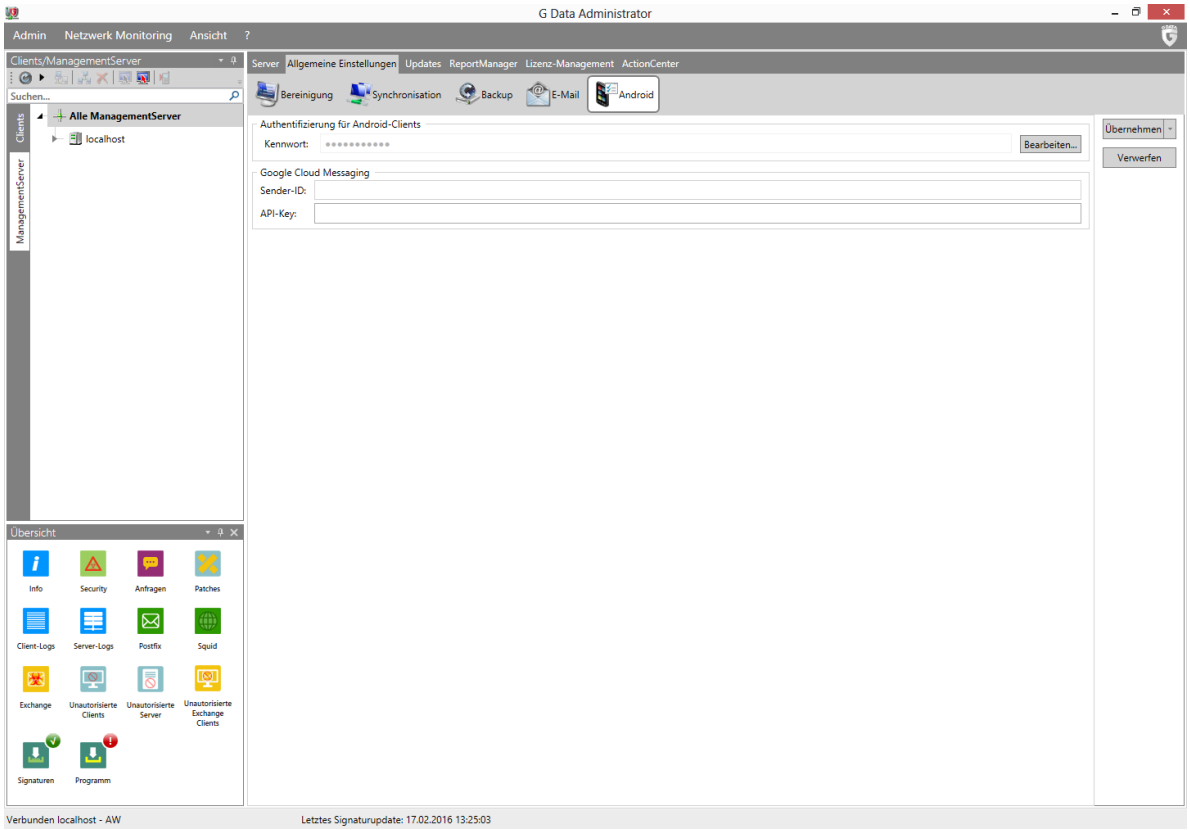
Geben Sie hier den **SMTP-Server** und den **Port** (Standard 25) an, den der G DATA ManagementServer zum Versenden von E-Mails nutzen soll. Weiterhin wird eine (gültige) Absenderadresse benötigt, damit die E-Mails verschickt werden können. Falls Ihr SMTP-Server eine Authentisierung erfordert, klicken Sie auf **SMTP-Authentisierung**. Sie können das Verfahren für **SMTP AUTH** konfigurieren (direkte Anmeldung am SMTP-Server) oder für **SMTP after POP3**.

Unter **Mailgruppen** können Sie Listen verschiedener Empfänger verwalten, z. B. das Management-Team, Techniker usw.



4.4.2.5. Android

Der Bereich Android verfügt über Einstellungen zur Authentisierung mobiler Android-Geräte sowie für das Firebase Cloud Messaging.



Geben Sie bitte unter **Authentifizierung für Android-Clients** ein **Kennwort** ein, mit dem sich das Android-Mobilgerät beim ManagementServer authentifizieren kann. Um **Notfallfunktionen** serverseitig über das Mobilgerät durchführen zu können, müssen Sie die **Sender-ID** und den **API-Key** (Server-Key) Ihres Firebase Cloud Messaging-Kontos eingeben. Kostenlose Konten für diese Push-Benachrichtigung können bei **firebase.google.com** eingerichtet werden. Weitere Informationen hierzu finden Sie im Reference Guide.

4.4.3. Updates

Alle Clients haben eine eigene, lokale Kopie der Virendatenbank, damit der Virenschutz auch gewährleistet ist, wenn sie offline sind (d.h. keine Verbindung mit dem G DATA ManagementServer bzw. dem Internet besteht). Die Aktualisierung der Virensignaturen (sowie der Programmdateien) auf den Clients erfolgt in zwei Schritten, die beide automatisiert werden können. Im ersten Schritt werden die aktuellen Dateien vom G DATA Update-Server in einen Ordner auf dem G DATA ManagementServer kopiert. Diesen Vorgang konfigurieren Sie im Updates-Modul. Im zweiten Schritt werden die neuen Dateien an die Clients verteilt (siehe Aufgabebereich **Client-Einstellungen** > **Allgemein** > **Updates**).

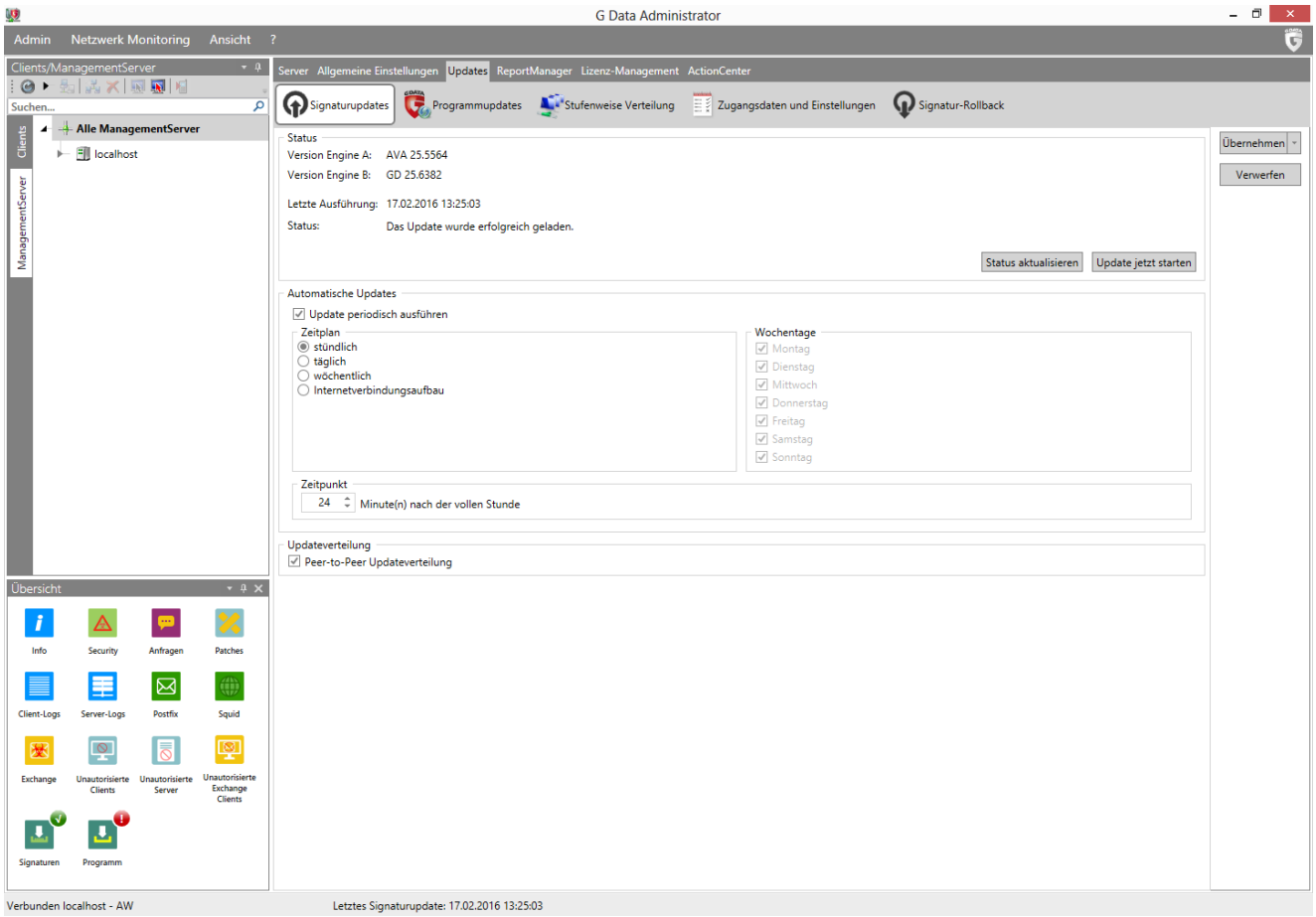
4.4.3.1. Signaturupdates

Im Bereich Signaturupdates konfigurieren Sie das Herunterladen der Virensignaturen vom G DATA Update-Server zum ManagementServer.

Unter **Status** werden die folgenden Informationen und Einstellungen angezeigt:

- **Version Engine A**: Die aktuelle Version der auf dem ManagementServer hinterlegten Virensignaturen für Engine A.
- **Version Engine B**: Die aktuelle Version der auf dem ManagementServer hinterlegten Virensignaturen für Engine B.
- **Letzte Ausführung**: Die letzte Ausführung des Aktualisierungsprozesses.
- **Status**: Der Status des Aktualisierungsprozesses.

- **Status aktualisieren**: Aktualisiert den Status.
- **Update jetzt starten**: Startet eine sofortige Aktualisierung der Virensignaturendatenbank auf dem G DATA ManagementServer.



Im Bereich **Automatische Updates** können Sie die Aktualisierung der Virensignaturen einplanen. Aktivieren Sie dazu das Häkchen bei **Update periodisch ausführen** und legen Sie fest, wann bzw. in welchem Turnus das Update zu erfolgen hat. Damit das Update automatisch erfolgen kann, muss Ihr G DATA ManagementServer mit dem Internet verbunden sein und Sie müssen Ihre Zugangsdaten, die Sie nach der Registrierung erhalten haben, unter **Updates** > **Zugangsdaten und Einstellungen** eingeben. Falls der ManagementServer sich über einen Proxy-Server mit dem Internet verbindet, geben Sie die Proxy-Einstellungen dort ebenfalls ein.

Die Update-Verteilung kann zentral (vom ManagementServer oder Subnet-Server zu den Clients) oder auch dezentral (von bereits aktuellen Clients zu den restlichen Clients) erfolgen. Aktivieren Sie dazu die Option **Peer-to-Peer Updateverteilung**. Bitte achten Sie darauf, dass für die Updateverteilung ggf. die **Port-Konfiguration** angepasst werden muss.

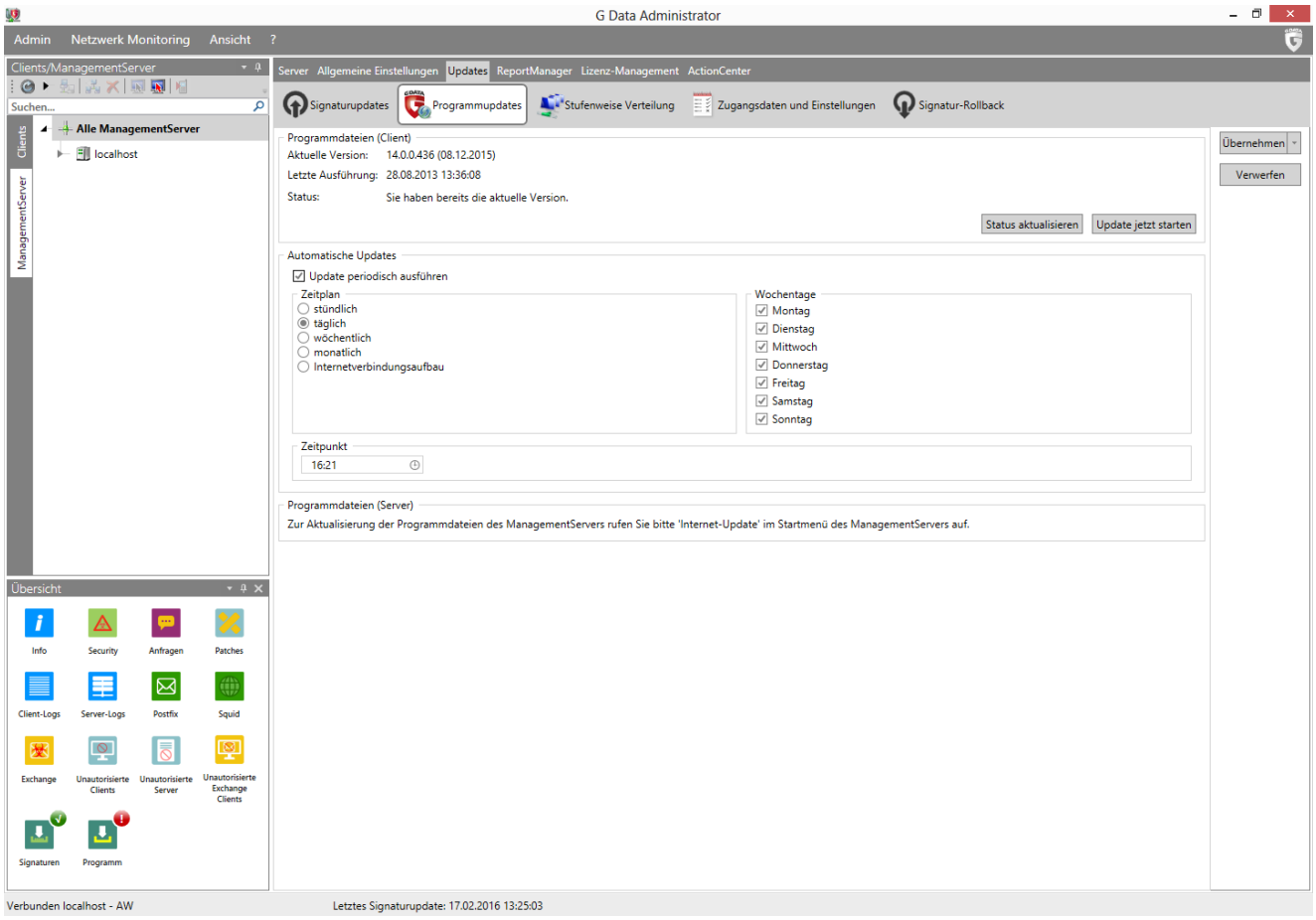
4.4.3.2. Programmupdates

Im Bereich Programmupdates konfigurieren Sie das Herunterladen der Client-Programmdateien vom G DATA Update-Server zum ManagementServer.

Unter **Programmdateien (Client)** werden die folgenden Informationen und Einstellungen angezeigt:

- **Aktuelle Version**: Die aktuelle Version der auf dem ManagementServer hinterlegten Client-Programmdateien.
- **Letzte Ausführung**: Die letzte Ausführung des Aktualisierungsprozesses.

- **Status**: Der Status des Aktualisierungsprozesses.
- **Status aktualisieren**: Aktualisiert den Status.
- **Update jetzt starten**: Startet eine sofortige Aktualisierung der Client-Programmdateien auf dem G DATA ManagementServer.

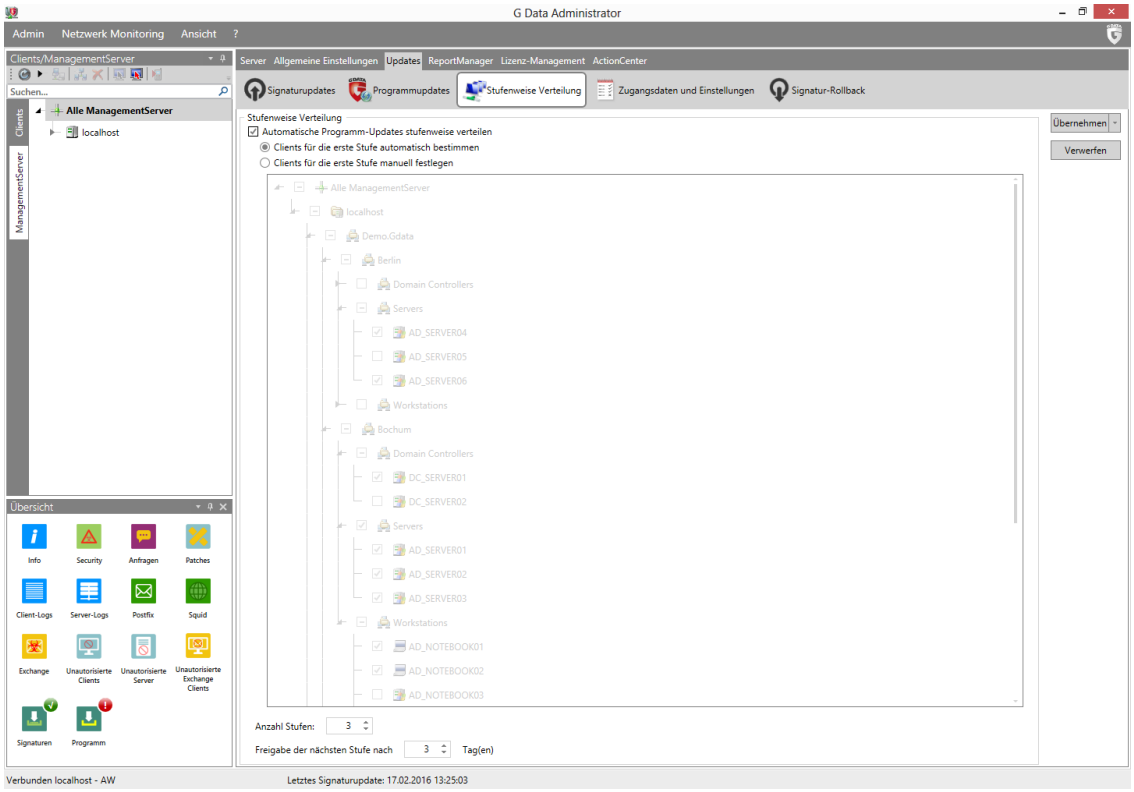


Im Bereich **Automatische Updates** können Sie die Aktualisierung der Client-Programmdateien einplanen. Die Einstellungen sind identisch zu denen unter **Signaturupdates**.

> Der G DATA ManagementServer selbst kann ausschließlich über einen Start-Menü-Eintrag aktualisiert werden. Rufen Sie dazu in der Programmgruppe G DATA ManagementServer im Startmenü den Eintrag **Internet-Update** auf.

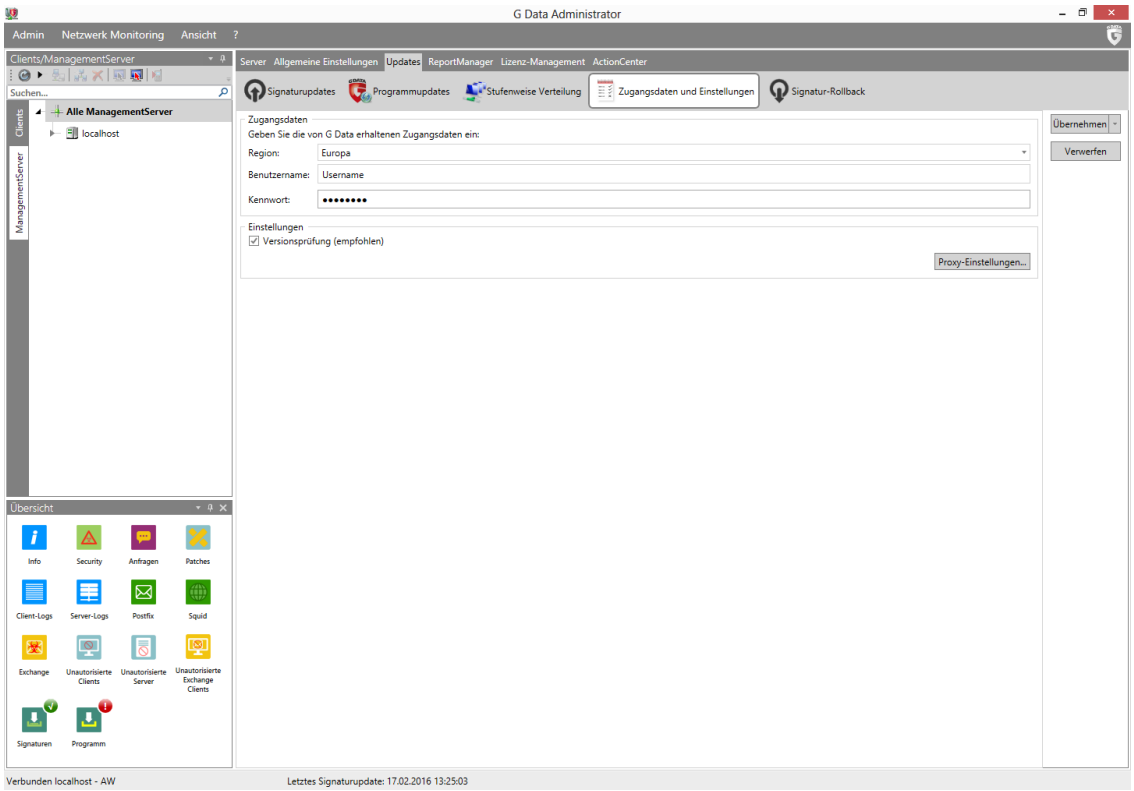
4.4.3.3. Stufenweise Verteilung

Im Bereich **Stufenweise Verteilung** können Sie festlegen, ob Sie Programmupdates zeitgleich auf allen Clients einspielen oder stufenweise. Eine stufenweise Verteilung verringert die bei einem Programmupdate auftretende Server- und Netzwerkbelastung. Wenn Sie sich für eine stufenweise Verteilung entscheiden, können Sie festlegen, ob die Verteilung automatisch erfolgt oder selber festlegen, welche Clients zuerst mit Programm-Updates versehen werden sollen, welche Clients danach kommen und wie weit die Untergliederung in verschiedene Verteilungsstufen untergliedert ist.



4.4.3.4. Zugangsdaten und Einstellungen

Mit der Online-Registrierung erhalten Sie von G DATA die Zugangsdaten für das Update der Virendatenbanken und Programmdateien. Geben Sie diese unter **Benutzername** und **Kennwort** ein. Wählen Sie unter **Region** den nächsten Update-Server aus, um beim Herunterladen von Updates eine optimale Geschwindigkeit zu gewährleisten. Die standardmäßig aktivierte **Versionsprüfung** sollte im Regelfall immer eingeschaltet sein, da sie so die optimale Update-Geschwindigkeit gewährleistet. Sollten jedoch Probleme mit den lokalen Virendatenbankdateien auftreten, dann schalten Sie die Versionsprüfung aus. Auf diese Weise wird beim nächsten Internet-Update die Integrität aller Virendatenbankdateien überprüft und die fehlerhaften Dateien werden neu heruntergeladen.

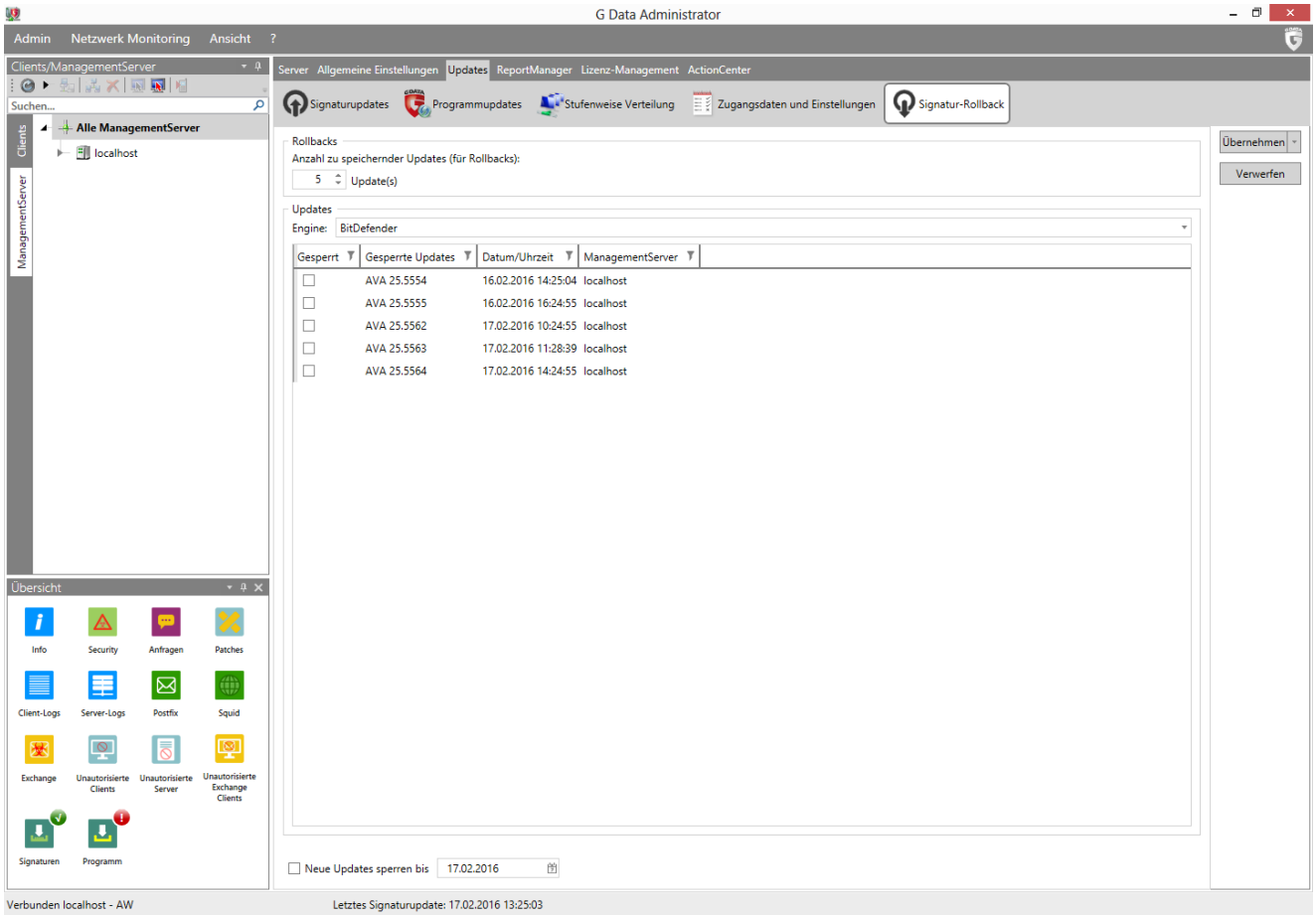


Mit der Schaltfläche **Proxy-Einstellungen** öffnen Sie ein Fenster, in dem Sie Zugangsdaten für Internet & Netzwerk eingeben können. Sie sollten hier nur Eingaben tätigen, wenn sich mit den Standardeinstellungen der G DATA Software Probleme ergeben sollten (z. B. wegen der Verwendung eines Proxyservers) und ein Internet-Update nicht durchführbar ist.

> 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 das Sie den Internet Explorer konfiguriert haben (also das Konto, mit dem Sie sich an Ihrem Rechner angemeldet haben).

4.4.3.5. Signatur-Rollback

Es kann im seltenen Fall von Fehlalarmen oder ähnlichen Problemen sinnvoll sein, das aktuelle Update der Virensignaturen zu sperren und stattdessen eines der vorhergehenden Signaturupdates zu verwenden. Geben Sie unter **Rollbacks** an, wie viele der aktualisierten Virensignaturupdates Sie für **Rollbacks** als Reserve vorhalten möchten. Als Standardwert gelten hier jeweils die letzten fünf Signatur-Updates der jeweiligen Engine.



Sollte es mit dem aktuellen Update der Engine A oder B Probleme geben, kann der Netzwerkadministrator das aktuelle Update für einen bestimmten Zeitraum sperren und stattdessen automatisch das zeitlich davorliegende Signaturupdate an die Clients und Subnet-Server verteilen.

> Auf Clients, die nicht mit dem G DATA ManagementServer verbunden sind (z. B. Notebooks auf Dienstreisen) können keine Rollbacks durchgeführt werden. Eine vom Server an den Client übertragene Sperrung neuer Updates kann dort ohne Kontakt zum G DATA ManagementSever nicht rückgängig gemacht werden.

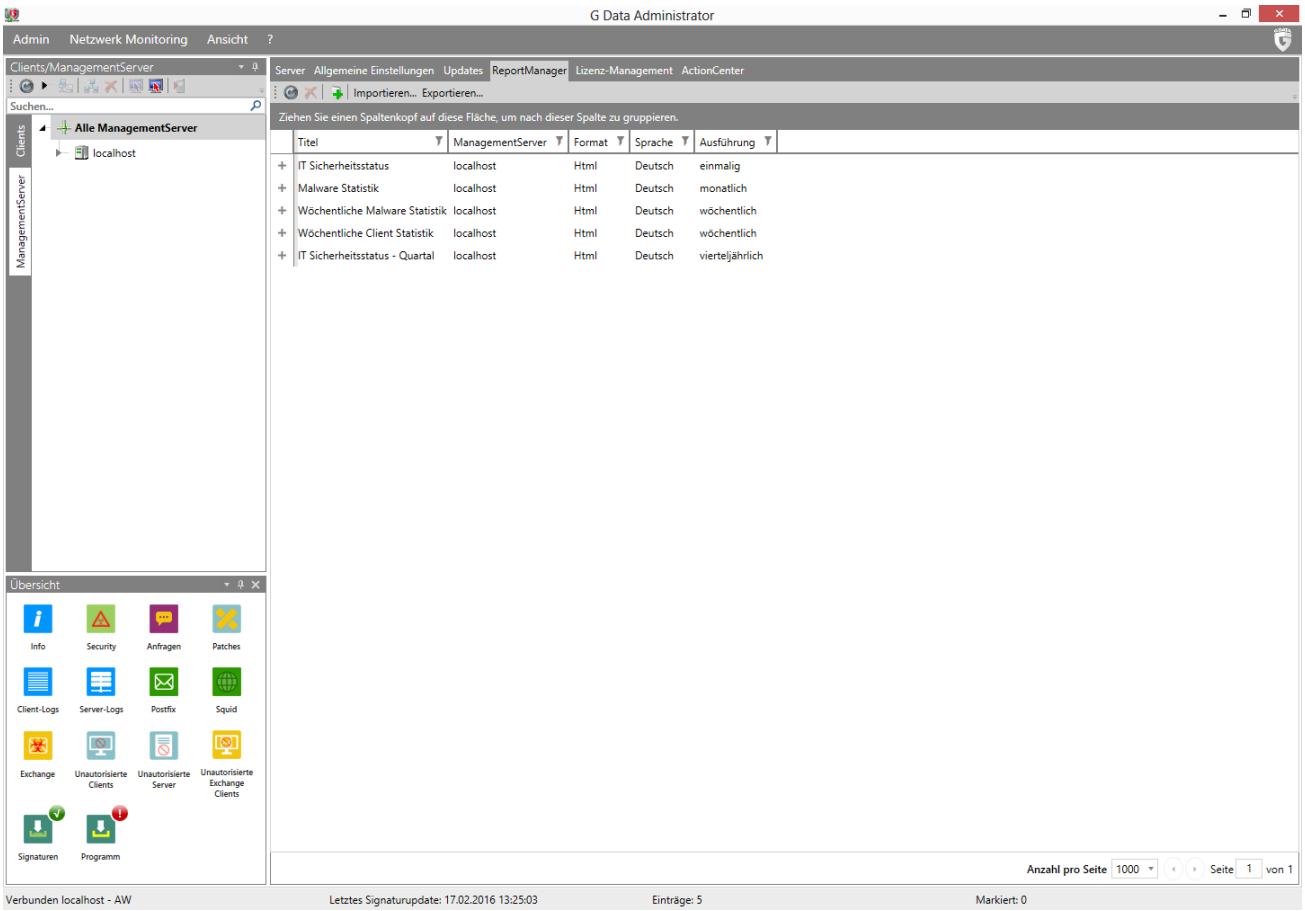
Für die ausgewählte **Engine** werden die jüngsten Engine-Updates unter **Gesperrte Updates** aufgelistet. Wählen Sie das oder die Updates, die blockiert werden sollen, und klicken Sie auf **OK**. Diese Updates werden dann nicht mehr verteilt, und Clients, die sie vorher erhalten haben, werden wieder zurückgesetzt auf das jüngste nicht gesperrte Update. Dies geschieht, sobald diese sich mit dem ManagementServer verbinden. Optional können Sie automatisch neue Updates bis zu einem bestimmten auswählbaren Datum sperren. Erst dann werden die Updates auf den Clients eingespielt. Nutzen Sie hierzu die Funktion **Neue Updates sperren bis**.

4.4.4. ReportManager

Über den ReportManager können Sie zeitplangesteuert Berichte über den Status Ihrer Systemsicherheit konfigurieren und an ausgewählte Empfänger verteilen.

- **Aktualisieren**
- **Löschen**
- **Neue Reportplanung hinzufügen**: Die Funktionen werden Ihnen im Kapitel **Reportdefinition** erläutert.

Über die Schaltfläche **Importieren** / **Exportieren** können Sie Einstellungen für den Report importieren und/oder exportieren. Mit einem Rechtsklick auf einen oder mehrere Berichte können Sie diese löschen oder - mit Auswahl von **Sofort ausführen** - auch direkt noch mal durchführen lassen. Um einen Bericht zu bearbeiten, klicken Sie auf **Eigenschaften**.



4.4.4.1. Reportdefinition

Hier kann festgelegt werden, welchen Namen der Report haben soll und in welcher Sprache er verfasst werden soll. Unter **Empfängergruppe(n)** können Sie festlegen, welche Liste von Empfängern diesen Report erhalten soll. Sie können dafür Gruppen verwenden, die Sie unter

Allgemeine Einstellungen > **E-Mail** > **E-Mail Einstellungen** angelegt haben oder hier auch direkt neue Empfängergruppen definieren, darüber hinaus können Sie über das Eingabefeld **Zusätzliche Empfänger** auch weitere E-Mail-Adressen für den jeweiligen Report hinzufügen (Adressaten werden dabei durch Kommata getrennt).

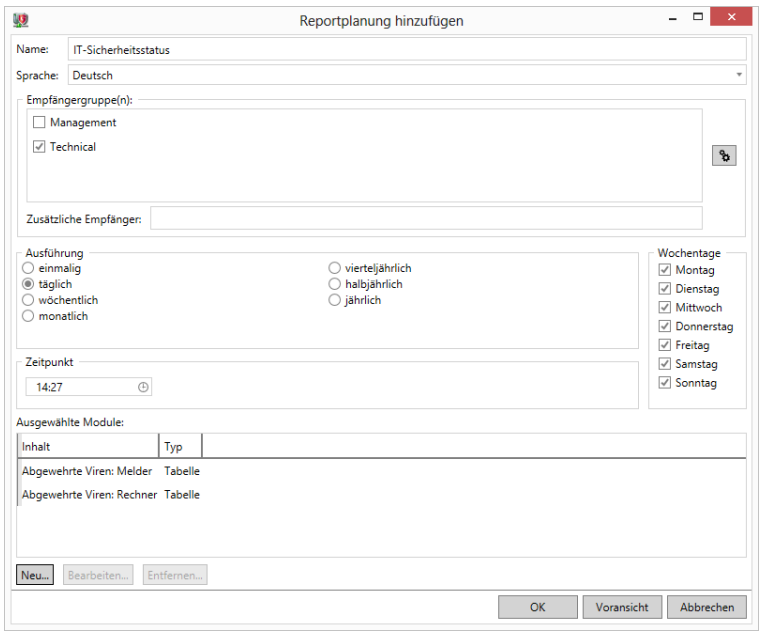
Bei einmaligen Reports können Sie eine Startzeit definieren, bei periodischen Reports können Sie festlegen, wann die Benachrichtigung erfolgen soll.

> Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass ein Report nur an Werktagen durchgeführt wird oder nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

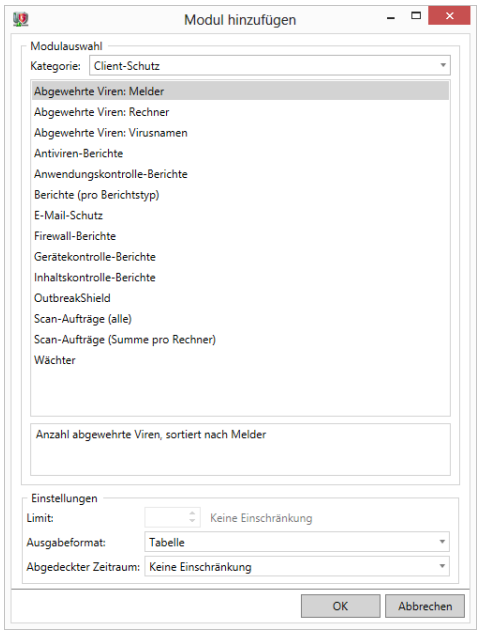
Den Inhalt des jeweiligen Reports definieren Sie, indem Sie unter **Ausgewählte Module** auf die Schaltfläche **Neu** klicken und dort eins der auswählbaren Reportmodule aktivieren. Die Verfügbarkeit der Module ist abhängig von der **G DATA-Lösung**, die Sie verwenden. Die Module für die Reportplanung sind in drei Kategorien untergliedert: **Client-Allgemein**, **Client-Schutz** und **PatchManager**. Wählen Sie das entsprechende Modul und konfigurieren Sie die Einstellungen im unteren Bereich des Fensters:

- **Limit**: Für manche Module können Sie ein Limit definieren, um die Menge der dargestellten Daten zu beschränken.
- **Client-Typ**: Optional können Sie den **Client-Typ**, der für den Bericht berücksichtigt werden soll, auf **Windows**, **Linux** oder **Mac** einschränken.
- **Ausgabeformat**: Für jedes Modul kann ein spezielles Ausgabeformat gewählt werden. Sie haben dabei die Auswahl aus **Tabelle**, **Liniendiagramm**, **Säulendiagramm (3D)** oder **Kuchendiagramm (3D)**. Bitte beachten Sie, dass nicht jedes Modul jedes Ausgabeformat unterstützt.
- **Abgedeckter Zeitraum**: Legen Sie einen absoluten oder relativen Zeitraum fest, der für den Bericht berücksichtigt werden soll.

Klicken Sie auf **OK**, um die ausgewählten Module dem jeweiligen Bericht hinzuzufügen. Um Module zu bearbeiten oder zu löschen, stehen Ihnen die entsprechenden Schaltflächen zur Verfügung. Wenn Sie die Auswahl und Einstellung der Module abgeschlossen haben, können Sie unter **Voransicht** einen Beispielreport mit den getroffenen Einstellungen durchführen.



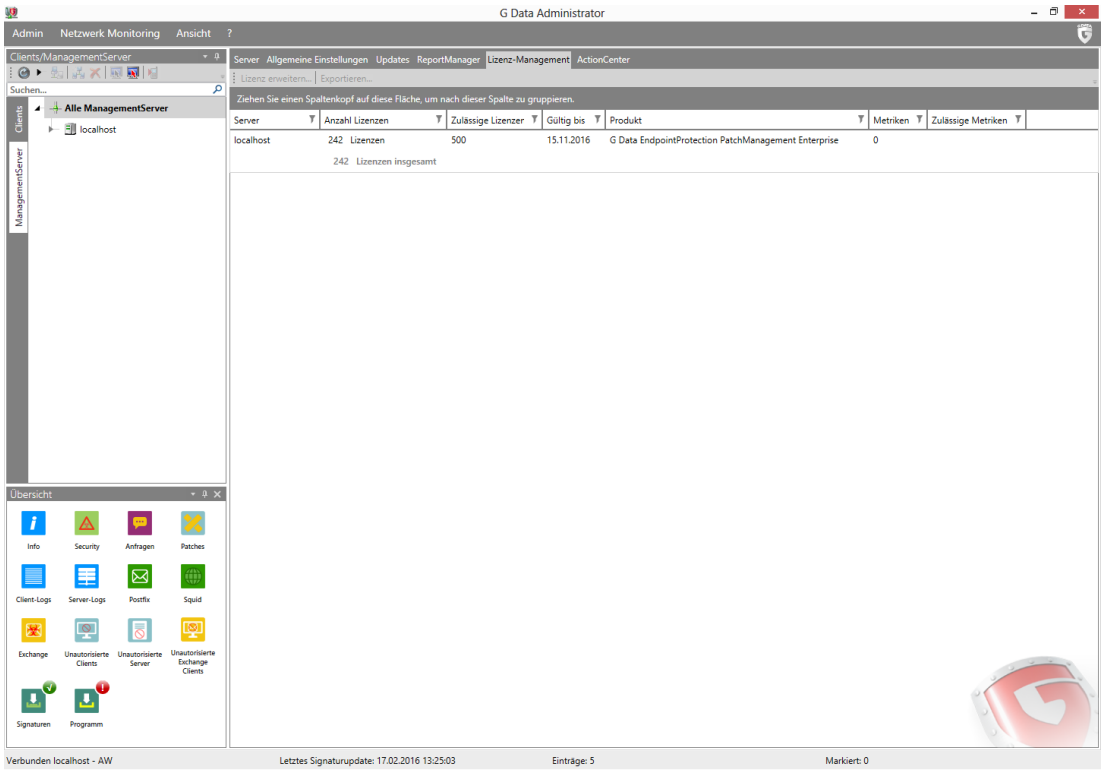
Wenn ein Report-Job durchgeführt wurde, erscheint der erstellte Report in der Übersicht des ReportManagers und wird an die ausgewählten Empfänger versendet. Alle Instanzen eines Reports sehen Sie durch einen Doppelklick auf den entsprechenden Report.



Der Computer, auf dem G DATA Administrator ausgeführt wird, muss über Internet Explorer 8 oder höher verfügen, um die Report-Voransicht und die Reportinstanzen-Ansicht anzeigen zu können.

4.4.5. Lizenz-Management

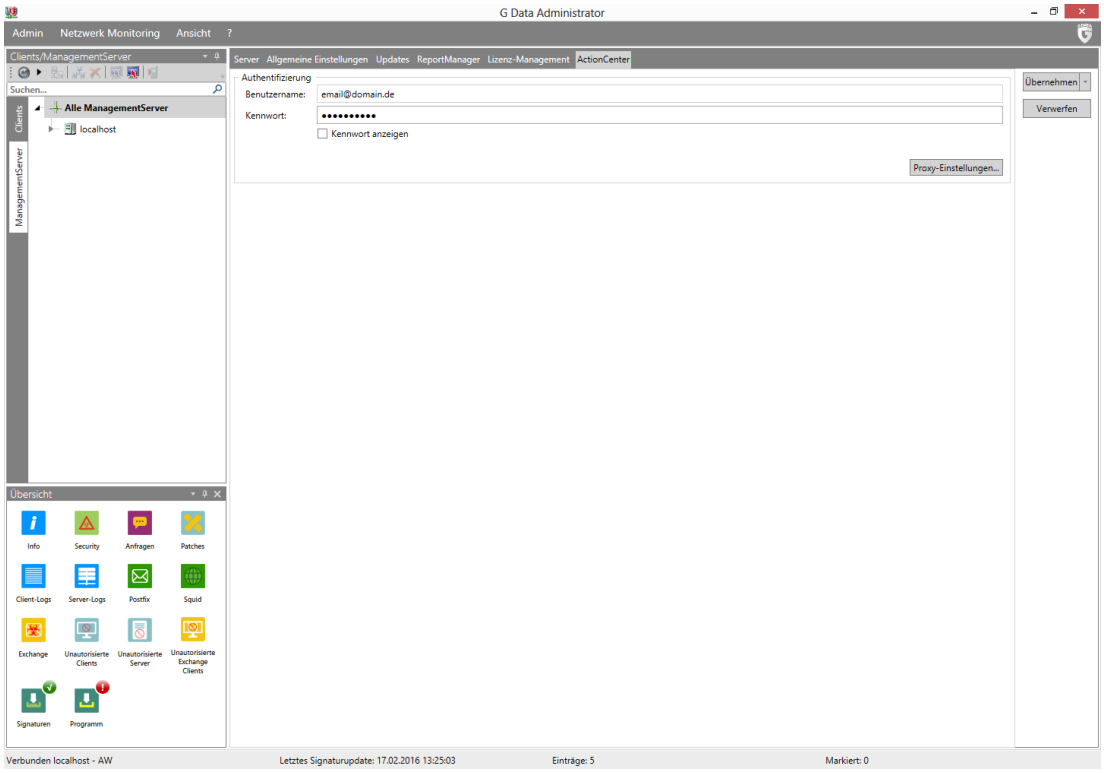
Mit Hilfe des Bereichs Lizenz-Management haben Sie jederzeit Überblick darüber, wie viele Lizenzen Ihrer G DATA Software in Ihrem Netzwerk installiert sind. Wenn Sie weitere Lizenzen benötigen, können Sie direkt über die Schaltfläche **Lizenzen erweitern** mit dem G DATA Upgrade-Center Kontakt aufnehmen. Über die Schaltfläche **Exportieren** haben Sie die Möglichkeit, sich eine Übersicht Ihrer verwendeten Lizenzen als Textdatei ausgeben zu lassen.



4.4.6. ActionCenter

Für die iOS-Geräteverwaltung und das Netzwerk Monitoring ist eine Verbindung zwischen G DATA Administrator und G DATA ActionCenter erforderlich. **Erstellen Sie ein Konto** und geben Sie hier Ihren **Benutzernamen** und Ihr **Kennwort** ein.

Die Verwendung des G DATA ActionCenters ist nur möglich, wenn Sie über eine gültige G DATA Lizenz verfügen. Stellen Sie sicher, dass Sie Ihren Internet-Update-**Benutzernamen** und Ihr Internet-Update-**Kennwort** unter **Updates** > **Zugangsdaten und Einstellungen** eingegeben haben.



Die Kommunikation mit dem G DATA ActionCenter setzt Sicherheitsfunktionen voraus, die nur in Windows Vista und höher verfügbar sind. Die iOS-Geräteverwaltung und das Netzwerk Monitoring sind nicht verfügbar auf G DATA ManagementServer- und G DATA Administrator-Geräte, die Windows XP oder Windows Server 2003 verwenden.

5. G DATA WebAdministrator

Der G DATA WebAdministrator ist eine webbasierte Steuerungssoftware für den G DATA ManagementServer. Mit ihm können Einstellungen für den G DATA ManagementServer über ein Webinterface in einem Browser vorgenommen werden.

5.1. Starten des G DATA WebAdministrators

Um den G DATA WebAdministrator zu nutzen, klicken Sie auf das Desktop-Symbol des G DATA WebAdministrators. Alternativ können Sie auch Ihren Internetbrowser starten und die URL besuchen, die Ihnen beim Abschluss des Installationsprozesses mitgeteilt wurde. Die URL besteht aus der IP-Adresse oder dem Computernamen des Rechners, auf dem IIS ausgeführt wird und der WebAdministrator installiert wurde, sowie dem Ordner-Suffix (z. B. *http://10.0.2.150/GDAdmin/*). Wenn Sie bis jetzt das Microsoft Silverlight Browser Plugin noch nicht installiert haben, werden Sie nun dazu aufgefordert, es herunterzuladen.

Nun öffnet sich automatisch eine Anmeldeseite für den Zugang zum G DATA WebAdministrator. Geben Sie hier nun wie beim regulären G DATA Administrator Ihre Zugangsdaten ein und klicken Sie dann auf die Schaltfläche **OK**.

5.2. Verwendung des G DATA WebAdministrators

Die Programmoberfläche des G DATA WebAdministrators ist sehr ähnlich zur Oberfläche des G DATA Administrators. Nach dem Einloggen sehen Sie das zentrale Dashboard, welches Ihnen einen Überblick über Ihr Netzwerk, die Clients und den Zustand des G DATA ManagementServers bietet.

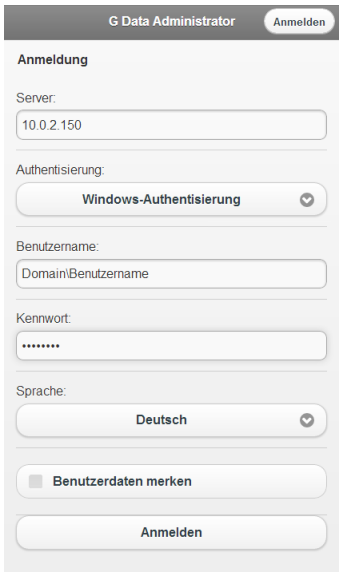
Die Funktionen des WebAdministrators sind identisch zu denen des G DATA Administrators. Diese werden im Kapitel **G DATA Administrator** umfangreich beschrieben.

6. G DATA MobileAdministrator

Der G DATA MobileAdministrator ist die über Smartphones bedienbare Programmoberfläche des G DATA ManagementServers. Es kann zum schnellen Bearbeiten und Updaten von Einstelllungen verwendet werden und ist für die Nutzung mit mobilen Geräten optimiert. Dazu sind die wichtigsten und am häufigsten benutzten Funktionen des G DATA Administrators so zusammengestellt worden, dass Sie auf einer breiten Palette unterschiedlichster Smartphone-Umgebungen genutzt werden können.

6.1. Starten des G DATA MobileAdministrators

Nach Abschluss der Installation des G DATA MobileAdministrators können Sie diesen von jedem Browser aus aufrufen. Starten Sie dazu Ihren Browser und wählen die URL aus, die Ihnen am Ende des Installationsprozesses mitgeteilt wird. Die URL besteht aus der IP-Adresse oder dem Computernamen des Rechners, auf dem IIS ausgeführt wird und der MobileAdministrator installiert wurde, sowie dem Ordner-Suffix (z. B. *http://10.0.2.150/GDMobileAdmin/*).



Die Anmeldeseite des MobileAdministrators ist genauso aufgebaut wie die Anmeldeseite des **G DATA Administrators** und des **G DATA WebAdministrators**. Geben Sie hier bitte den **Server**, den **Benutzernamen**, Ihr **Kennwort** und Ihre **Benutzersprache** an. Wählen Sie die **Windows-Authentisierung**, wenn Sie sich mit Ihren Windows-(Domain-)Zugangsdaten anmelden möchten oder die **Integrierte Authentisierung**, wenn Sie Ihre Zugangsdaten direkt über den Administrator verwalten lassen. Sollten Sie wünschen, dass Ihre Zugangsdaten (bis auf das Kennwort) beim nächsten Öffnen der Anmeldeseite wieder zur Verfügung stehen, wählen Sie bitte **Benutzerdaten merken**.

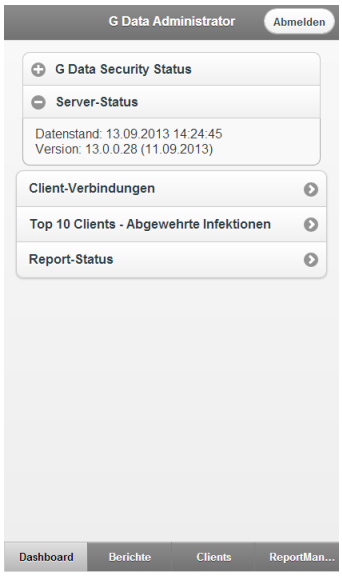
6.2. Verwendung des G DATA MobileAdministrators

Nach dem Einloggen am G DATA MobileAdministrator wird das Hauptmenü angezeigt. Hier stehen Ihnen vier Optionen zur Verfügung: **Dashboard**, **Berichte**, **Clients**, und **ReportManager**. Um das Programm zu beenden, tippen Sie auf die Schaltfläche **Abmelden** oben rechts.

6.2.1. Dashboard

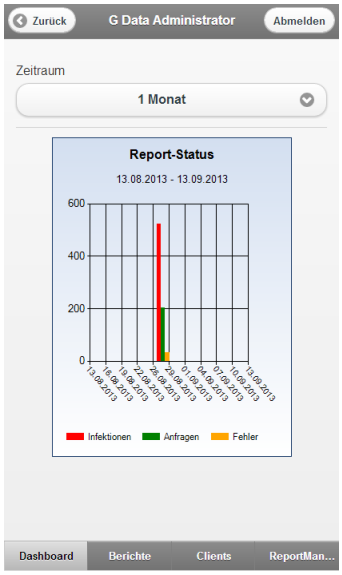
Im Dashboard des G DATA MobileAdministrators können Sie die wichtigsten Statistiken über Ihr Netzwerk auf einen Blick einsehen. Vergleichbar mit der Dashboard-Ansicht im G DATA Administrator haben Sie hier einen Überblick über den G DATA ManagementServer und dessen Clients. Zusätzlich

können Sie sich hier Statistiken über Client-Verbindungen und verhinderte Infektionen anzeigen lassen.



Wählen Sie die Ansicht **G DATA Security Status** um eine genauere Übersicht über den Status von Server und Clients zu erhalten. Der MobileAdministrator zeigt Ihnen, wie viele Clients mit dem G DATA Security Client ausgestattet sind und bietet Ihnen Informationen über den Aktualisierungsstatus der Virensignaturen und anderer Programmkomponenten (z. B. OutbreakShield, Firewall und Wächter). Sie können über das Öffnen des Virus-Signatur-Unterbereichs auch direkt Engine-Rollbacks durchführen. Der Zustand des ManagementServers an sich kann unter **Server-Status** genauer betrachtet werden.

Weitere Statistiken erhalten Sie unter **Client-Verbindungen** und **Top 10 Clients - Abgewehrte Infektionen**. Tippen Sie auf **Report-Status**, um sich Informationen über Infektionen, Anfragen und Fehlerberichte anzeigen zu lassen.

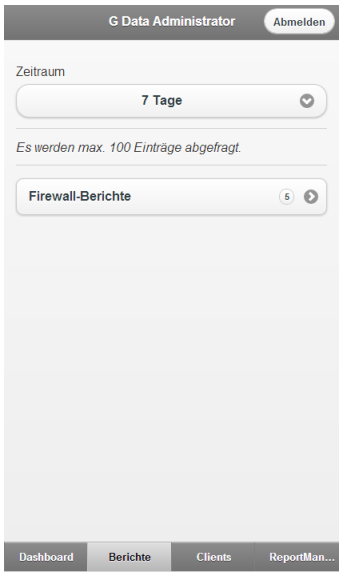


6.2.2. Berichte

In der Berichte-Ansicht finden Sie Reports über Viren, Firewall-Ereignisse und Meldungen des PolicyManagers. Hierbei handelt es sich um eine für mobile Geräte optimierte Darstellung derselben Informationen, die Sie auch im G DATA Administrator im **Sicherheitsereignisse**-Bereich finden.

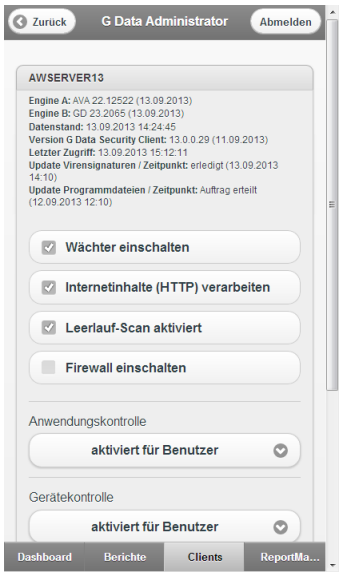
Wählen Sie unter **Zeitraum** aus, ob Sie die Reports des letzten Tages, der letzten sieben Tage oder des

letzten Monats angezeigt bekommen möchten. Der MobileAdministrator zeigt Ihnen dann an, für welche Kategorie Berichte vorliegen. Wenn Sie eine dieser Kategorien antippen, erhalten Sie eine Übersicht über die aufgezeichneten Ereignisse. Berichte können nach Namen gefiltert werden.



6.2.3. Clients

Der MobileAdministrator bietet Ihnen einen genauen Überblick über alle Clients, die vom G DATA ManagementServer verwaltet werden. Für jeden Client sind Detailinformationen abrufbar und wichtige Sicherheitseinstellungen können direkt über den MobileAdministrator verändert werden.

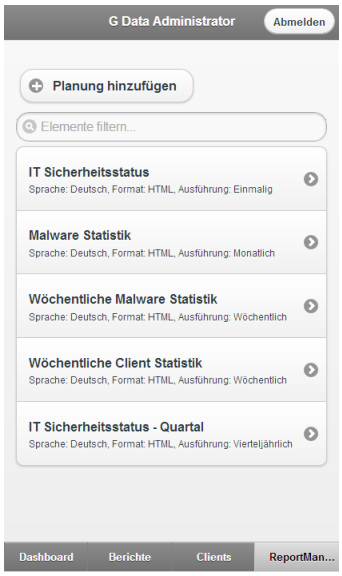


In der Übersichtsanzeige können Sie sich eine Liste aller Rechner anzeigen lassen, welche durch den G DATA ManagementServer verwaltet werden. Diese Liste kann auch nach Namen gefiltert werden. Wenn Sie einen Client gezielt auswählen, können Sie gezielt für diesen Statistiken über Versionen und Updates einsehen. Darüber hinaus können wichtige Sicherheitseinstellungen direkt verändert werden. So können Sie den **Wächter** ein- oder ausschalten, bestimmen ob **Internetinhalte (HTTP)** verarbeitet werden sollen oder nicht, den **Leerlauf-Scan** aktivieren oder deaktivieren und die **Firewall** ein- oder ausschalten.

Über den Bereich Clients können darüber hinaus **Anwendungskontrolle**, **Gerätekontrolle**, **Web-Inhaltskontrolle**, und **Internetnutzungszeit** kontrolliert und editiert werden.

6.2.4. ReportManager

Beim ReportManager handelt es sich um die mobile Version des **ReportManager**-Bereichs im G DATA Administrator. Hier haben Sie die Möglichkeit, Berichte zu konfigurieren, zu timen und in einer Vorschau zu betrachten.



Um eine neuen Report-Auftrag hinzuzufügen, tippen Sie auf **Planung hinzufügen**. Schon vorhandene Reports können Sie durch einfaches Antippen zum Editieren auswählen. Dabei stehen Ihnen alle Einstellungsmöglichkeiten zur Verfügung, die auch im ReportManager der Desktopversion möglich sind.

7. G DATA Security Client

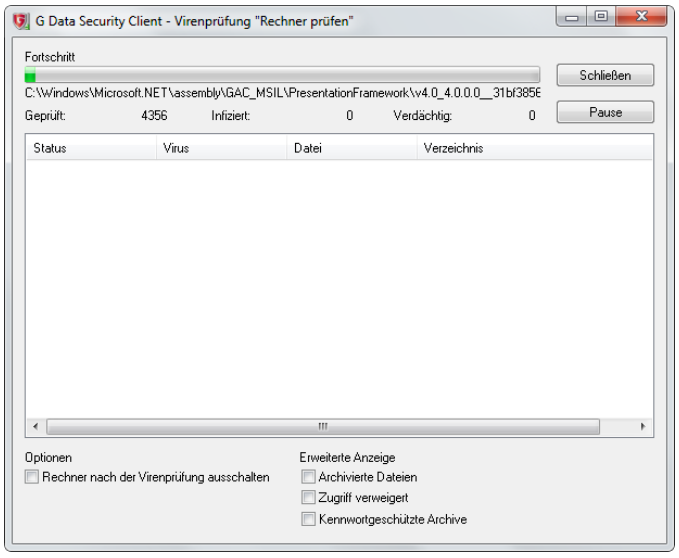
G DATA Security Client stellt den Schutz für die Windows-Clients bereit und führt die ihm vom G DATA ManagementServer zugewiesenen Jobs ohne eigene Bedienoberfläche im Hintergrund aus. Die Clients verfügen über eigene Virensignaturen und einen eigenen Scheduler, damit auch im Offline-Betrieb (z. B. bei Notebooks, die keine ständige Verbindung zum G DATA ManagementServer haben) Aufträge durchgeführt werden können.

Nach der Installation der Client-Software steht dem Benutzer des Clients ein Symbol in der Startleiste zur Verfügung, über welches er unabhängig von den Zeitplänen des Administrators auch selber auf Virenschutz-Funktionen zugreifen kann. Welche Funktionen dem Nutzer zur Verfügung stehen, definieren Sie als Administrator im Bereich **Client-Einstellungen** des G DATA Administrators.

Über die rechte Maustaste kann der Benutzer auf diesem G DATA Security Client-Symbol ein Kontextmenü öffnen, das Zugriff auf alle Funktionen anbietet.

7.1. Virenprüfung

Über diese Option kann der Anwender gezielt mit dem G DATA Security Client seinen Rechner auch außerhalb der im G DATA Administrator vorgegebenen Prüfzeiträume auf Viren überprüfen.



Der Anwender kann zusätzlich Disketten, CDs/DVDs, den Speicher und Autostart-Bereich, sowie einzelne Dateien oder Verzeichnisse prüfen. Auf diese Weise können auch Notebook-Nutzer, die ihren Rechner nur selten mit dem Firmennetzwerk verbinden, gezielt einen Virenbefall des Systems unterbinden. Über das **Optionen**-Fenster können Client-User so festlegen, welche Aktionen bei einem Virenfund durchgeführt werden sollen (z. B. Verschieben der Datei in den Quarantäne-Bereich).

Der Anwender kann auch aus dem Windows-Explorer heraus Dateien oder Verzeichnisse überprüfen, indem er diese markiert und dann in dem Kontextmenü mit der rechten Maustaste die Funktion **Auf Viren prüfen (G DATA AntiVirus)** auswählt.

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 sich das Arbeiten mit anderen Programmen an diesem Rechner deutlich verlangsamen. Bei der Einstellung **Niedrig** dauert die Virenprüfung hingegen vergleichsweise lange, dafür kann währenddessen, ohne

größere Einschränkungen, am Client-Rechner weitergearbeitet werden. Diese Option ist nur verfügbar, wenn eine Virenprüfung lokal gestartet wurde.

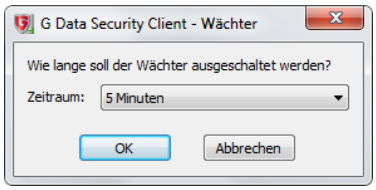
- **Virenprüfung anhalten**: Diese Option erlaubt es dem Anwender, eine lokal gestartete Virenprüfung eigenständig anzuhalten. Scanaufträge, die vom G DATA ManagementServer festgelegt werden, können nur dann angehalten werden, wenn der Administrator beim Anlegen des Jobs die Option **Anwender kann den Job anhalten oder abbrechen** aktiviert hat.
- **Virenprüfung abbrechen**: Diese Option erlaubt es dem Anwender, eine lokal gestartete Virenprüfung eigenständig abzubrechen. Scanaufträge, die vom G DATA ManagementServer festgelegt werden, können nur dann abgebrochen werden, wenn der Administrator beim Anlegen des Jobs die Option **Anwender kann den Job anhalten oder abbrechen** aktiviert hat.
- **Scanfenster anzeigen**: Hiermit kann sich der Anwender das Info-Fenster anzeigen lassen, in dem Verlauf und Fortschritt der Virenprüfung angezeigt werden. Diese Option ist nur verfügbar, wenn eine Virenprüfung lokal gestartet wurde.

Die Option **Virenprüfung** kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

7.2. 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. Das zeitweilige Ausschalten kann bei umfangreichen Dateikopiervorgängen sinnvoll sein, da auf diese Weise der Kopiervorgang beschleunigt wird. Der Echtzeit-Virenschutz ist in diesem Zeitraum allerdings ausgeschaltet.

Die Option **Wächter ausschalten** kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.



7.3. Optionen

Der Benutzer des Client-Rechners hat unter **Optionen** die Möglichkeit, selber Einstellungen in folgenden Bereichen für seinen Client zu ändern: **Wächter**, **Email**, **Virenprüfung** (lokal), **Web** und **AntiSpam**. Auf diese Weise können sämtliche Schutzmechanismen der G DATA Software auf dem Client ausgeschaltet werden. Diese Option sollte nur fachlich versierten Anwendern zugänglich sein. Die einzelnen Einstellungsmöglichkeiten werden ausführlich im Bereich **Client-Einstellungen** erläutert.

Die verschiedenen Karteikarten können im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

7.4. Quarantäne

Jeder Client hat einen lokalen Quarantäneordner, in den infizierte Dateien verschoben werden können (abhängig von den Einstellungen für Wächter/Scanauftrag). Eine Datei, die in Quarantäne verschoben wurde, kann, sofern sie einen Virus enthält, keine Schadroutinen ausführen. Infizierte Dateien werden beim Verschieben in die Quarantäne automatisch gepackt und verschlüsselt. Für die Quarantäne bestimmte Dateien, die größer sind als 1 MB werden automatisch immer in der lokalen

Quarantäne des Clients abgelegt, um bei einem massiven Virenbefall das Netzwerk nicht unnötig zu belasten. Alle Dateien, die kleiner als 1 MB sind, werden an den Quarantäneordner des G DATA ManagementServers übertragen. Diese Einstellungen sind nicht veränderbar. Mehr Informationen über die Quarantäne-Ordner finden Sie im Kapitel **Standardspeicherorte und Pfade**.

Sollte auf einem mobilen Client ohne Verbindung zum G DATA ManagementServer eine infizierte Datei gefunden werden, die kleiner ist als 1 MB, wird sie in der lokalen Quarantäne gespeichert und erst beim nächsten Kontakt zum G DATA ManagementServer in die dortige Quarantäne übertragen. Im Quarantäne-Ordner können befallene Dateien desinfiziert werden. Wenn dies nicht funktioniert, lassen sich die Dateien von dort auch löschen und ggf. aus der Quarantäne an ihren Ursprungsort zurückbewegen.

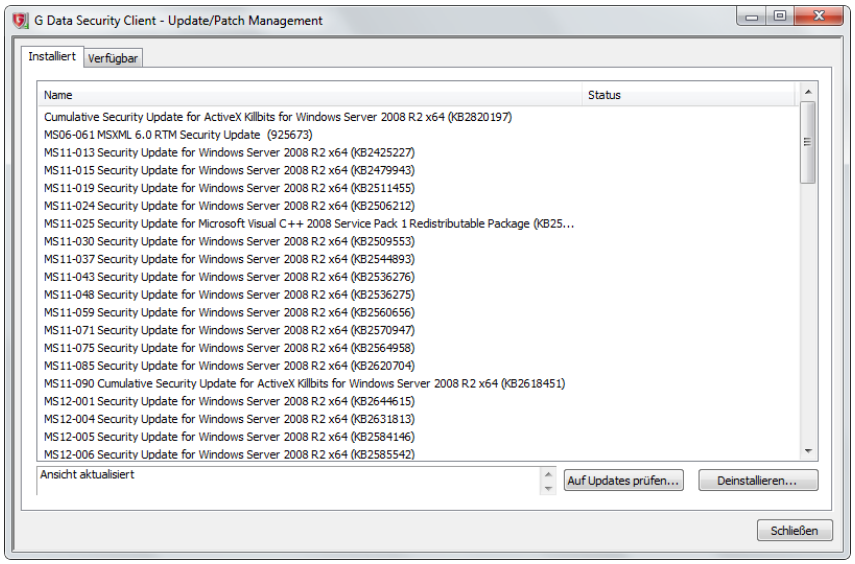
> **Achtung**: Beim Zurückbewegen wird ein Virus nicht entfernt. Sie sollten diese Option nur wählen, wenn das Programm ohne die befallene Datei nicht lauffähig ist und Sie diese trotzdem zur Datenrettung benötigen.

Die Option **Quarantäne** kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

7.5. Updates/Patches

PatchManager ist als **optionales Modul** verfügbar.

Hinter der Option **Updates/Patches** findet sich eine Übersicht der Updates und Patches für den Client-PC.



Auf der Registerkarte **Installiert** sehen Sie alle Patches und Updates, welche auf dem System installiert worden sind. Mit einem Doppelklick auf den jeweiligen Eintrag erhalten Sie ausführliche Informationen zum jeweiligen Patch oder Update. Sollte ein Patch oder Update Probleme machen, kann der Anwender es über die Schaltfläche **Deinstallieren** markieren und automatisch dem Administrator zur Deinstallation vorschlagen. Der **Status** des Patches/Updates wird dann entsprechend aktualisiert und der Administrator erhält einen Report mit einer Rollback-Anfrage. Unabhängig von eventuellen zeit- oder ferngesteuerten Softwareerkennungs-Jobs kann der Anwender über die Schaltfläche **Auf Updates prüfen** auch selber nach aktuellen Patches für sein System suchen.

Auf der Registerkarte **Verfügbar** werden alle Software-Pakete, Patches und Upgrades angezeigt, die für den Client verfügbar sind. Mit einem Doppelklick auf den jeweiligen Eintrag erhalten Sie

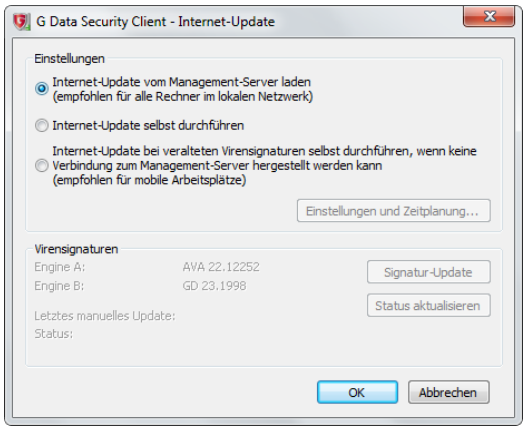
ausführliche Informationen zum jeweiligen Patch oder Update. Um als Client-Nutzer die Installation aktualisierter Programmdaten zu initiieren, kann dieser hier auf **Installieren** klicken. Der **Status** des Patches/Updates wird dann entsprechend aktualisiert und der Administrator erhält einen Report mit einer Distributionsanfrage.

Die Option **Updates/Patches** kann im G DATA Administrator unter **PatchManager** > **Einstellungen** ein- und ausgeschaltet werden.

7.6. Internet-Update

Über den G DATA Security Client können auch vom Client-Rechner aus selbstständig Internet-Updates der Virensignaturen durchgeführt werden, falls keine Verbindung zum G DATA ManagementServer besteht (siehe **Client-Einstellungen** > **Allgemein** > **Updates**).

Die Option **Internet-Update** kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.



7.7. Firewall ausschalten

Das Firewall-Modul ist als Teil der Client Security Business-, Endpoint Protection Business- und Managed Endpoint Security-**Lösungen** verfügbar.

Über **Firewall ausschalten** kann die Firewall ausgeschaltet werden, auch wenn der Client sich noch im ManagementServer-Netzwerk befindet. Wenn die Firewall ausgeschaltet ist, kann sie über die Option **Firewall einschalten** wieder eingeschaltet werden.

Die Option **Firewall ausschalten** kann im G DATA Administrator unter **Firewall** > **Übersicht** > **Betrieb im internen Netzwerk** ein- und ausgeschaltet werden (**Der Benutzer darf die Firewall ein- und ausschalten**).

7.8. Firewall

Das Firewall-Modul ist als Teil der Client Security Business-, Endpoint Protection Business- und Managed Endpoint Security-**Lösungen** verfügbar.

Der Menüeintrag **Firewall** öffnet das Interface der Firewall. Solange sich der Client im Netzwerk des G DATA ManagementServers befindet, wird die Firewall zentral vom Server aus administriert. Sobald der Client sich mit einem anderen Netzwerk verbindet, z. B. wenn ein Firmenlaptop zu Hause verwendet wird, kann das Firewall-Interface genutzt werden, um die Offsite-Konfiguration zu ändern.

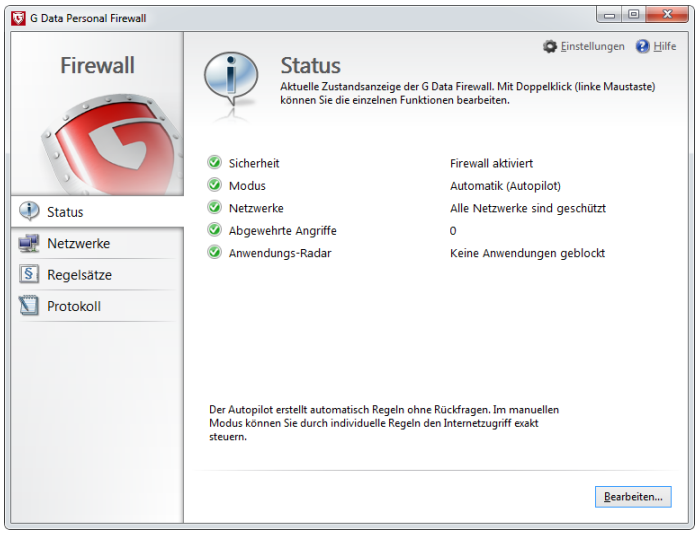
Der Menüeintrag **Firewall** kann im G DATA Administrator unter **Firewall** > **Übersicht** > **Betrieb ausserhalb des internen Netzwerks** ein- und ausgeschaltet werden (**Der Benutzer darf die**

Offsite-Konfiguration ändern).

7.8.1. Status

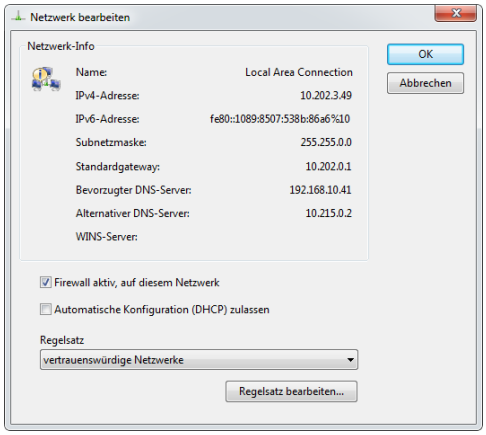
Im Status-Bereich erhalten Sie grundlegende Informationen zum aktuellen Zustand der Firewall. Durch doppeltes Anklicken des jeweiligen Eintrags können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln.

- **Sicherheit**: Firewall aktivieren oder deaktivieren. Diese Funktion ist nur verfügbar, falls der Administrator diese im G DATA Administrator erlaubt hat (**Firewall** > **Übersicht** > **Betrieb im internen Netzwerk** > **Der Benutzer darf die Firewall ein- und ausschalten**).
- **Modus**: Die Firewall kann mit automatischer (Autopilot) oder manueller Regelerstellung betrieben werden. Diese Funktion kann clientseitig nur geändert werden, falls der Client außerhalb des ManagementServer-Netzwerks verwendet wird und der Administrator das Einstellen dieser Funktion im G DATA Administrator erlaubt hat (**Firewall** > **Übersicht** > **Betrieb ausserhalb des internen Netzwerks** > **Der Benutzer darf die Offsite-Konfiguration ändern**).
- **Netzwerke**: Öffnet den **Netzwerke**-Bereich. Hier können Sie sich die Netzwerke, in denen sich Ihr Computer befindet, sowie die verwendeten Regelsätze anzeigen lassen.
- **Abgewehrte Angriffe**: Sobald die Firewall einen Angriff auf Ihren Computer registriert, wird dieser verhindert und hier protokolliert.
- **Anwendungs-Radar**: Dieses Dialogfeld zeigt Ihnen, welche Programme momentan von der Firewall blockiert werden. Sollten Sie einer der blockierten Anwendungen doch die Erlaubnis für die Nutzung des betreffenden Netzwerkes erteilen wollen, wählen Sie diese hier einfach aus und klicken Sie dann die Schaltfläche **Erlauben** an.



7.8.2. Netzwerke

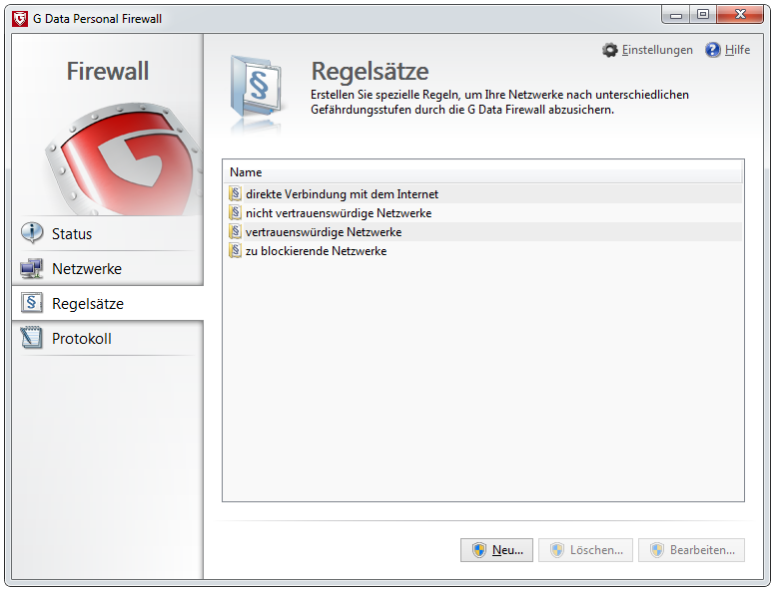
Im Netzwerke-Bereich werden alle Netzwerke (z. B. LAN, DFÜ etc.) aufgelistet, mit denen der Rechner verbunden ist. Hier wird auch aufgezeigt, mit welchem Regelsatz das jeweilige Netzwerk geschützt wird. Wenn Sie ein Netzwerk mit der Maus markieren und die **Bearbeiten**-Schaltfläche anklicken, können Sie die Firewall-Einstellungen für dieses Netzwerk einsehen, bzw. verändern. Einstellungen können nur geändert werden, falls der Administrator dies erlaubt hat (**Firewall** > **Übersicht** > **Betrieb im internen Netzwerk** > **Der Benutzer darf die Firewall ein- und ausschalten**) oder der Client im Offsite-Modus verwendet wird (**Firewall** > **Übersicht** > **Betrieb ausserhalb des internen Netzwerks** > **Der Benutzer darf die Offsite-Konfiguration ändern**).



- **Netzwerk-Info**: Zeigt Netzwerk-Informationen wie IP-Adresse, Subnetzmaske, Standardgateway, DNS- und WINS-Server.
- **Firewall aktiv, auf diesem Netzwerk**: Firewall aktivieren oder deaktivieren.
- **Gemeinsame Nutzung der Internet Verbindung**: Internetverbindungsfreigabe (ICS) erlauben oder sperren.
- **Automatische Konfiguration (DHCP) zulassen**: Automatische IP-Konfiguration (DHCP) erlauben oder sperren.
- **Regelsatz**: Wählen Sie den **Regelsatz**, der für dieses Netzwerk verwendet werden sollte. Wählen Sie **Regelsatz bearbeiten**, um den **Regelassistenten** zu öffnen.

7.8.3. Regelsätze

In diesem Bereich können Sie Regelsätze anlegen und bearbeiten. Regelsätze enthalten Firewall-Regeln und können einem oder mehreren Netzwerken zugewiesen werden.



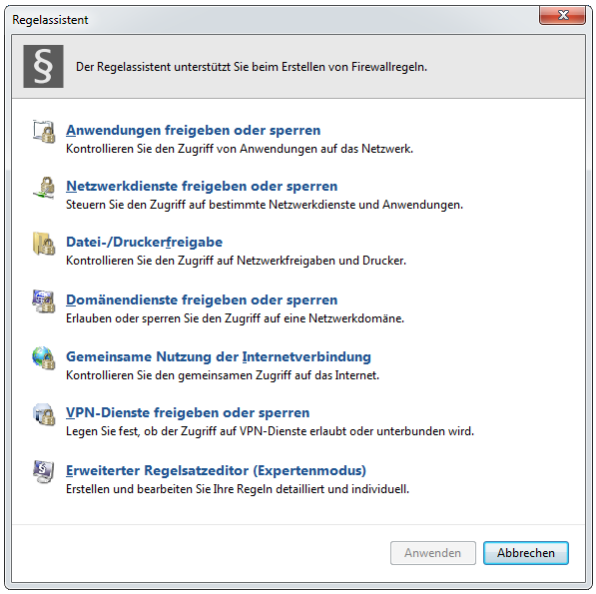
- **Neu**: Einen neuen Regelsatz hinzufügen. Legen Sie in dem erscheinenden Dialogfenster den **Regelsatz Name** fest und entscheiden Sie sich, ob grundlegende Regeln für nicht vertrauenswürdige, vertrauenswürdige oder zu blockierende Netzwerke vordefiniert werden sollen.
- **Löschen**: Regelsatz löschen. Die vorgegebenen Regelsätze für direkte Verbindung mit dem Internet, vertrauenswürdige Netzwerke, nicht vertrauenswürdige Netzwerke und zu blockierende Netzwerke können nicht gelöscht werden.
- **Bearbeiten**: Regelsatz bearbeiten mit dem **Regelassistenten**.

Der Bereich Regelsätze beinhaltet voreingestellte Regelsätze für folgende Netzwerktypen:

- **Direkte Verbindung mit dem Internet**: Hierunter fallen Regeln, die den direkten Internetzugriff behandeln.
- **Nicht vertrauenswürdige Netzwerke**: Hierunter fallen vor allem offene Netzwerke, wie z. B. DFÜ-Netzwerke, die auf das Internet Zugriff haben.
- **Vertrauenswürdige Netzwerke**: Vertrauenswürdig sind in der Regel Heim- und Firmennetzwerke.
- **Zu blockierende Netzwerke**: Wenn zeitweise oder dauerhaft der Kontakt des Rechners zu einem Netzwerk blockiert werden soll, kann dieser Regelsatz verwendet werden.

7.8.3.1. Regelassistent

Mit dem Regelassistenten können Sie Regeln für den jeweiligen Regelsatz definieren oder bestehende Regeln ändern. Der Regelassistent ist besonders geeignet für Anwender, die sich nicht gut mit der Firewall-Technologie auskennen. Für eine genauere Kontrolle über individuelle Regeln verwenden Sie den **Erweiterten Regelsatzeditor**.



Der Regelassistent bietet verschiedene Regeln, mit denen Sie schnell und unkompliziert einen bestimmten Verbindungstyp erlauben oder sperren können. Für die meisten Regeln können Sie eine **Richtung** definieren, die bestimmt, ob eine Regel eingehende und/oder ausgehende Verbindungen blockieren soll.

- **Anwendungen freigeben oder sperren**: Erlauben oder Sperren des Zugriffs einer Anwendung auf das Netzwerk, für das der Regelsatz definiert wurde.
- **Netzwerkdienste freigeben oder sperren**: Über das Sperren eines oder mehrerer Ports können schnell Lücken geschlossen werden, die sonst von Hackern für Angriffe genutzt werden könnten. Im Assistenten haben Sie die Möglichkeit, Ports komplett oder nur für eine bestimme Anwendung zu sperren.
- **Datei-/Druckerfreigabe**: Ordner- und Druckerfreigabe erlauben oder sperren.
- **Domänendienste freigeben oder sperren**: Netzwerkdomänendienste erlauben oder sperren.
- **Gemeinsame Nutzung der Internetverbindung**: Internetverbindungsfreigabe (ICS) erlauben oder sperren.
- **VPN-Dienste freigeben oder sperren**: Virtual Private Network (VPN)-Dienste erlauben oder

sperren.

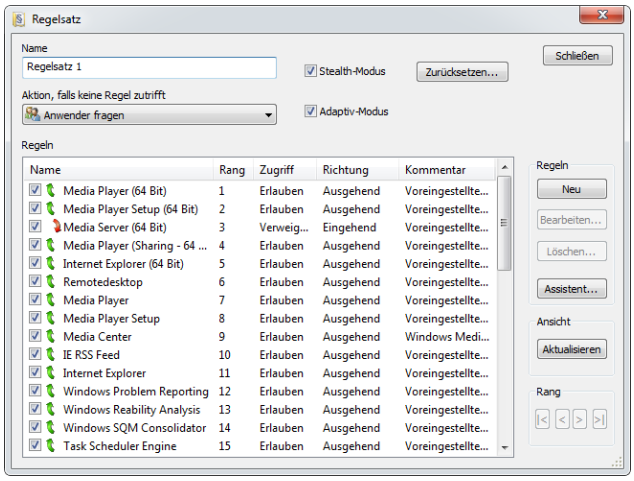
- **Erweiterter Regelsatzeditor (Expertenmodus)**: Öffnet den **Erweiterten Regelsatzeditor**.

7.8.3.2. Erweiterter Regelsatzeditor

Mit dem erweiterten Regelsatzeditor können Sie sehr individuelle Regeln für das jeweilige Netzwerk definieren. Dabei können sämtliche Regeln erzeugt werden, die Sie auch über den Regelassistenten erzeugen können. Es können aber auch weitergehende Einstellungen vorgenommen werden.

Der erweiterte Regelsatzeditor ähnelt dem **Regelsätze**-Bereich des G DATA Administrator **Firewall**-Moduls. Sie können den Editor verwenden, um Regeln zu erstellen, zu bearbeiten und zu löschen, sowie um Regeln nach Rang einzuteilen. Neben den auch im G DATA Administrator verfügbaren Möglichkeiten bietet der erweiterte Regelsatzeditor die folgenden Funktionen:

- **Aktion, falls keine Regel zutrifft**: Hier können Sie festlegen, ob der Zugriff im Netzwerk generell erlaubt, verweigert oder auf Nachfrage geregelt werden soll.
- **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 entfernte Rechner mit Ihrer Anwendung zurückverbindet. Ist der Adaptiv-Modus aktiv, so erkennt die Firewall diesen Rückkanal und lässt ihn zu, ohne gesondert nachzufragen.
- **Zurücksetzen**: Löscht alle Änderungen sowie erlernte Regeln.



Einzelne Regeln können bearbeitet werden, indem Sie die Regel wählen und die **Bearbeiten**-Taste drücken. Das Regelbearbeitungsfenster ist identisch mit dem Fenster **Regel bearbeiten** im G DATA Administrator.

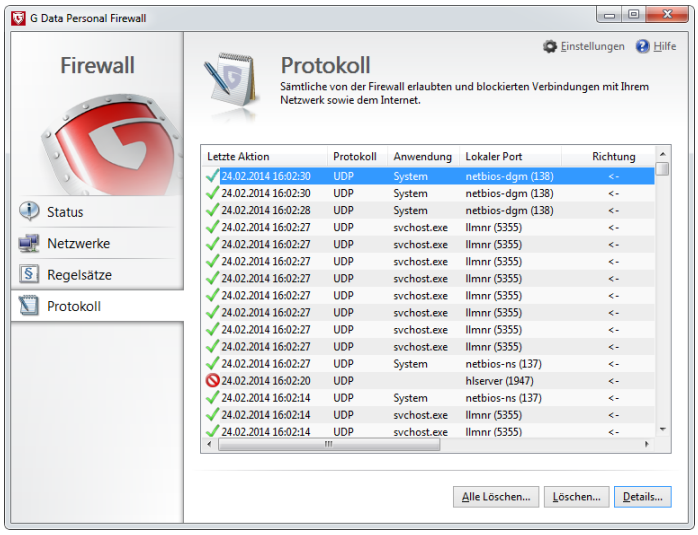
7.8.4. Protokoll

Der Bereich Protokoll zeigt eine detaillierte Übersicht mit allen eingehenden und ausgehenden Verbindungen. Sie können diesen Bereich verwenden für die Dokumentation zur: Überprüfung von Verbindungsprotokollen, Anwendung, Richtung, lokalem Port, entferntem Host, entferntem Port und dem Grund für die Entscheidung, die Verbindung zu blockieren oder zu erlauben.

Wählen Sie **Löschen**, um einen einzelnen Protokolleintrag zu löschen oder **Alle Löschen**, um alle Einträge zu löschen. Die Schaltfläche **Details** zeigt Ihnen weitere Informationen über den ausgewählten Eintrag.

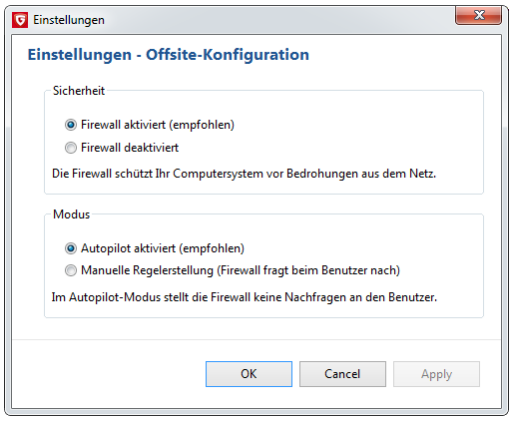
Klicken Sie mit der rechten Maustaste auf einen Eintrag, um Zugriff auf weitere Optionen zu erhalten.

Neben dem **Details**-Fenster, können Sie auch neue Regeln erstellen, bestehende Regeln bearbeiten und einen Filter für die Protokollansicht definieren.



7.8.5. Einstellungen

Das Fenster Einstellungen kann nur dann benutzt werden, wenn der Administrator die entsprechenden Berechtigungen eingestellt hat (**Firewall** > **Übersicht** > **Betrieb im internen Netzwerk** > **Der Benutzer darf die Firewall ein- und ausschalten** und **Firewall** > **Übersicht** > **Betrieb ausserhalb des internen Netzwerks** > **Der Benutzer darf die Offsite-Konfiguration ändern**).



- **Sicherheit**: Firewall aktivieren oder deaktivieren.
- **Modus**: Die Firewall kann mit automatischer (Autopilot) oder manueller Regelerstellung betrieben werden.

8. G DATA Security Client für Linux

G DATA Security Client für Linux wird als Hintergrundservice ausgeführt und bietet Virenprüfungsfunktionen. Auf Linux-Rechner, die als Server eingesetzt werden, können zusätzliche Module für Samba, Sendmail/Postfix und Squid installiert werden (siehe **Installation des G DATA Security Clients für Linux**).

G DATA Security Client für Linux besteht aus einer **grafischen Benutzeroberfläche** und einem **Kommandozeilen-Interface**.

8.1. Grafische Benutzeroberfläche

Eine Verknüpfung zur grafischen Benutzeroberfläche des G DATA Security Clients für Linux finden Sie, abhängig von der verwendeten Linux-Distribution, unter Anwendungen oder in einem ähnlichen Menü. Alternativ starten Sie den Client mit dem Kommando */opt/gdata/bin/gdavclient-qt*.

Nachdem Sie die Benutzeroberfläche gestartet haben, öffnen Sie das Interface mit einem Klick auf das Client-Icon. Welche Optionen verfügbar sind, ist abhängig von den Einstellungen im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen**.

Mit einem Rechtsklick auf dem G DATA Security Client-Symbol können Sie ein Kontextmenü öffnen, das Zugriff auf folgende Funktionen anbietet:

- **Virenprüfung**
- **Quarantäne**
- **Aktualisierung**
- **Hilfe**
- **G DATA Security Client öffnen**: Öffnet das Interface des G DATA Security Clients für Linux und zeigt den **Status**-Bereich an.
- **Über G DATA Security Client**

Alle Module können gegen Änderungen geschützt werden (siehe **Client-Einstellungen** > **Allgemein** > **Client-Funktionen**). Falls der Passwort-Schutz aktiviert wurde, klicken Sie auf das Schloss links unten im Fenster und geben Sie das Passwort ein, um Einstellungen ändern zu können.

8.1.1. Status

Das Status-Modul zeigt Ihnen auf einen Blick den aktuellen Sicherheitsstatus des Clients. Mit Hilfe der Status-Symbole können Sie sehen, ob der Client komplett gesichert ist oder ob ein Sicherheitsrisiko vorliegt.

- **Letzte Prüfung**: Datum und Zeit der letzten **Virenprüfung**. Klicken Sie auf die Schaltfläche **Rechner jetzt prüfen**, um eine Virenprüfung des gesamten Rechners zu starten.
- **Letzte Aktualisierung**: Datum und Zeit der letzten **Aktualisierung** der Virensignaturen. Klicken Sie auf die Schaltfläche **Jetzt aktualisieren**, um die Virensignaturen sofort zu aktualisieren.

8.1.2. Virenprüfung

Die Virenprüfung kann den ganzen Rechner oder auch bestimmte Dateien und Ordner auf Viren prüfen. Wenn ein Virus gefunden wird, wird automatisch die Aktion, die unter **Einstellungen** definiert

wurde, ausgeführt. Darüber hinaus wird auch der ManagementServer benachrichtigt und ein Bericht zu dem Modul **Sicherheitsereignissen** im G DATA Administrator hinzugefügt.

Wählen Sie eine der folgenden Optionen aus und klicken Sie dann auf **Virenprüfung starten**:

- **Gesamten Rechner prüfen**: Alle Dateien und Ordner auf dem Rechner werden geprüft.
- **Systembereiche prüfen**: Der Bootsektor wird geprüft.
- **Dateien und Ordner prüfen**: Spezifische Dateien und Ordner werden geprüft. Den Scanumfang legen Sie unter **Scanumfang** fest.

Unter Einstellungen können Sie die Scan-Parameter festlegen:

- **Reaktion auf infizierte Dateien**: Legen Sie fest, was passieren soll, wenn die Virenprüfung eine infizierte Datei findet:
  - **Nur protokollieren** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
  - **Desinfizieren** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
  - **Löschen** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
  - **In die Quarantäne verschieben** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
  - **Benutzer fragen**: Dem Benutzer wird eine Benachrichtigung angezeigt und gefragt, wie das Virus behandelt werden soll.
- **Falls Desinfektion fehlschlägt**: Wenn Sie die Option Desinfizieren ausgewählt haben, die Datei aber nicht desinfiziert werden kann, wird eine alternative Aktion ausgeführt.
- **Reaktion auf infizierte Archive**: Legen Sie fest, was passieren soll, wenn die Virenprüfung eine infizierte Archive findet.
- **Dateitypen** (siehe **Aufträge** > **Scan-Aufträge** > **Scanner**).

Unter **Erweitert** können Sie die folgenden erweiterten Einstellungen konfigurieren:

- **Heuristik** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
- **Systembereiche prüfen** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
- **Archive prüfen** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
- **Maximale Größe für Archive** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
- **Maximale Größe für Dateien**: Legen Sie die maximale Dateigröße fest. Dateien, die größer sind, werden nicht geprüft.

Unter **Ausnahmen** können Sie mit Hilfe einer Datei- und Verzeichnisliste einzelne Dateien und Verzeichnisse als Scan-Ausnahmen definieren.

Das Modul Virenprüfung kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

8.1.3. Aktualisieren

Das Aktualisieren-Modul sorgt dafür, dass der G DATA Security Client für Linux immer über die aktuellsten Virensignaturen verfügt, um den Rechner optimal zu schützen.

Unter **Letzte Aktualisierung** werden Datum und Zeit der letzten Aktualisierung angezeigt. Die Signaturversion der beiden Engines wird unter **Engine A** bzw. **Engine B** angezeigt. Klicken Sie auf **Virensignaturen aktualisieren** um sofort Updates zu laden.

Die Aktualisierung der Virensignaturen kann unter **Einstellungen** konfiguriert werden:

- **Update-Quelle**: Entscheiden Sie, ob der Client die Virensignaturen vom ManagementServer oder direkt von den G DATA Update-Servern beziehen soll (siehe **Client-Einstellungen** > **Allgemein** > **Updates**).
- **Planung**: Definieren Sie die Zeitplanung der Aktualisierung (**Manuell**, **Stündlich** oder **Täglich**).
- **Proxy-Server**: Wenn ein Proxy-Server verwendet werden soll, um Virensignaturen herunterzuladen, so geben Sie die Zugangsdaten für den Proxy-Server hier ein.
- **Zugangsdaten**: Geben Sie die Zugangsdaten für die G DATA Update-Server hier ein.

Die Einstellungen unter **Planung**, **Proxy-Server** und **Zugangsdaten** treffen nur zu, wenn unter **Update-Quelle** eine andere Einstellung als **Virensignaturenupdates von ManagementServer herunterladen** gewählt wurde. Mehr Informationen finden Sie unter **Client-Einstellungen** > **Allgemein** > **Updates**.

Das Modul Aktualisieren kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

8.1.4. Quarantäne

Das Modul Quarantäne zeigt eine Liste mit Dateien, die von einer Virenprüfung in die Quarantäne verschoben wurden.

Pro Datei werden die folgenden Eigenschaften angezeigt:

- **Dateiname**: Der Name und Pfad der infizierten Datei.
- **Virenname**: Der Name des Virus, das die Datei infiziert hat.
- **Dateigröße**: Die Größe der Datei.

Wählen Sie eine oder mehrere Dateien aus und klicken Sie auf eine der unter der Liste angezeigten Schaltflächen:

- **Desinfizieren und zurückbewegen**: Das Virus wird entfernt und die Datei wird zurück an ihren Ursprungsort bewegt.
- **Zurückbewegen**: Die Datei wird zurück an ihren Ursprungsort bewegt. Achtung: Wenn die Datei vorher nicht desinfiziert wird, kann sie das System infizieren!
- **Löschen**: Die Datei wird aus der Quarantäne gelöscht.

Das Modul Quarantäne kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

8.1.5. Über

Das Fenster Über G DATA Security Client enthält Statusinformationen über den Security Client und kann nur über das Tray-Icon geöffnet werden. Folgende Informationen werden angezeigt:

- **Version**: Die installierte Client-Version.
- **ManagementServer**: Der aktuelle Status der Verbindung zum ManagementServer.
- **Status der Sicherheitssoftware**: Der aktuelle Status der Hintergrundprozessen.

8.2. Kommandozeilen-Interface

Als Alternative zur grafischen Benutzeroberfläche können Sie das Kommandozeilen-Interface des G DATA Security Clients für Linux verwenden. **Gdavclient-cli** ist das empfohlene Tool, um per Kommandozeile Virenscans auszuführen und Aktualisierungen herunterzuladen. Alternativ können Sie mit dem Tool **gdavclientc** Virenprüfungen konfigurieren und ausführen, Versionsinformationen anzeigen, Virensignaturen aktualisieren und den Scan-Server-Hintergrunddienst verwalten. Beide Tools müssen als Root ausgeführt werden um sicherzustellen, dass sie kompletten Zugriff auf das System haben.

8.2.1. gdavclient-cli

Standardmäßig finden Sie gdavclient-cli im Verzeichnis /usr/bin. Die Syntax für gdavclient-cli sieht folgendermaßen aus: *gdavclient-cli [<Optionen>] <Dateien/Pfad>*. Sie können die folgenden Optionen verwenden:

- **--status**: Der Status der Hintergrunddienste gdavclientc und gdavserver wird angezeigt.
- **--version**: Die Versionsinformationen werden angezeigt.
- **--mmsconnection**: Information zur Verbindung mit dem ManagementServer wird angezeigt.
- **--lastscan**: Das letzte Scan-Protokoll wird angezeigt.
- **--lastupdate**: Information zur letzten Aktualisierung der Virensignaturen wird angezeigt.
- **--update**: Startet ein Update der Virensignaturen.
- **--sysinfo**: Erstellt die Datei gdatahwinfo-<Datum>.tar.gz, in der Debugdateien wie z. B. Protokolle und Konfigurationsdateien enthalten sind.

Wenn Sie Dateien oder Pfade spezifizieren, startet gdavclient-cli eine Virenprüfung.

8.2.2. gdavclientc

Standardmäßig finden Sie gdavclientc im Verzeichnis /usr/bin. Das Tool ist unabhängig vom G DATA ManagementServer und lädt die Konfiguration von /etc/gdata/gdav.ini. Die Syntax für gdavclientc sieht folgendermaßen aus: *gdavclientc [<Optionen>] <Kommando>*. Sie können die folgenden Kommandos verwenden:

scan:<Pfad>: Startet eine Virenprüfung für die Datei(en) unter *<Pfad>*. *<Pfad>*kann absolut oder relativ sein und eine Datei oder ein Verzeichnis beinhalten. Verzeichnisse werden rekursiv geprüft. Platzhalter (*, ?*) sind erlaubt.

scanboot: Startet einen Bootsektor-Scan. Die Start-Sektoren aller nicht-optischen Datenträger, die unter /proc/partitions aufgeführt sind, werden untersucht.

abort: Der laufende Scan wird abgebrochen.

start: Startet gdavserver.

stop: Stoppt gdavserver.

restart: Stoppt und startet gdavserver.

updateVDB<:engine>: Startet ein Virensignaturenupdate für *EngineA* oder *EngineB*. Nachdem das Update abgeschlossen wurde, muss der Scan-Server mit dem Kommando *restart* neugestartet werden.

dump: Zeigt die aktuelle Konfiguration von gdavserver.

set:<Schlüssel>=<Wert>: Fügt der Konfiguration von gdavserver eine Einstellung hinzu oder ändert

eine vorhandene. Diese Einstellungen sind nur zur Laufzeit aktiv. Um Einstellungen dauerhaft vorzunehmen, müssen diese vor dem Start des Servers in der Konfigurationsdatei /etc/gdata/gdav.ini gespeichert werden.

get:<Schlüssel>: Gibt den Wert des Schlüssels *<Schlüssel>*zurück.

reload: Lädt die Konfiguration von /etc/gdata/gdav.ini.

engines: Zeigt eine Liste der durch gdavserver geladenen Engines.

baseinfo: Zeigt Versionsinformationen.

coreinfo: Zeigt Engine-Versionsinformationen.

pid: Zeigt die PID des gdavserver-Dienstes.

Wenn Sie mit Hilfe des Kommandos *scan:*eine Virenprüfung ausführen lassen, können Sie zusätzlich die folgenden Optionen verwenden:

-s: Zusätzlich zu dem normalen Scan-Output wird eine Zusammenfassung der Scan-Ergebnisse angezeigt.

-x: Zusätzlich zu dem normalen Scan-Output wird eine Zusammenfassung der Scan-Ergebnisse angezeigt (XML-Format).

9. G DATA Security Client für Mac

G DATA Security Client für Mac bietet Virenschutz für Clients mit Mac OS X. Der Client führt geplante und lokale Virenprüfungen aus und bietet On-Access-Schutz mit Hilfe des Wächter-Moduls.

Nach der Installation der Client-Software steht dem Benutzer des Clients ein Symbol in der Startleiste zur Verfügung. Welche Funktionen dem Nutzer zur Verfügung stehen, definieren Sie als Administrator im Bereich **Client-Einstellungen** des G DATA Administrators.

Der Benutzer kann auf diesem G DATA Security Client-Symbol ein Kontextmenü öffnen, das Zugriff auf folgende Funktionen anbietet:

- **Wächter aktivieren/deaktivieren**
- **Virenprüfung**
- **Quarantäne**
- **Aktualisierung**
- **Hilfe**
- **G DATA Security Client öffnen**: Öffnet das Interface des G DATA Security Clients für Mac und zeigt den **Status**-Bereich an.
- **Über G DATA Security Client**

Alle Module werden gegen unbeabsichtigte Änderungen geschützt. Klicken Sie auf das Schloss links unten im Fenster, um das Ändern der Einstellungen zu erlauben. Wenn Root-Berechtigungen benötigt sind, müssen Zugangsdaten für ein Root-Konto eingegeben werden.

9.1. Status

Das Status-Modul zeigt Ihnen auf einen Blick den aktuellen Sicherheitsstatus des Clients. Mit Hilfe der Status-Symbole können Sie sehen, ob der Client komplett gesichert ist oder ob ein Sicherheitsrisiko vorliegt.

- **Wächter**: Der aktuelle Status des **Wächters**. Durch das Auswählen einer entsprechenden Option im Menü kann der Wächter (temporär) deaktiviert werden.
- **Letzte Prüfung**: Datum und Zeit der letzten **Virenprüfung**. Klicken Sie auf die Schaltfläche **Rechner jetzt prüfen**, um eine Virenprüfung des gesamten Rechners zu starten.
- **Letzte Aktualisierung**: Datum und Zeit der letzten **Aktualisierung** der Virensignaturen. Klicken Sie auf die Schaltfläche **Jetzt aktualisieren**, um die Virensignaturen sofort zu aktualisieren.

9.2. Wächter

Der Wächter prüft im Hintergrund alle Dateien, auf die das System und der Benutzer zugreifen, und reagiert sofort, wenn ein Virus gefunden wird. Die folgenden Einstellungen stehen zur Verfügung:

- **Status**
  - **Aktiviert**: Der Wächter ist aktiviert (empfohlen).
  - **Deaktiviert**: Der Wächter ist permanent deaktiviert. Dies ist ein Sicherheitsrisiko.
  - **Deaktiviert bis zum nächsten Systemstart**: Der Wächter ist deaktiviert. Nach dem nächsten Systemstart wird der Wächter automatisch aktiviert.

  - **Deaktiviert für ... Minuten**: Der Wächter ist für eine bestimmte Zeitspanne deaktiviert. Danach wird der Wächter automatisch aktiviert.
- **Reaktion auf infizierte Dateien**: Legen Sie fest, was passieren soll, wenn der Wächter eine infizierte Datei findet:
  - **Nur protokollieren** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
  - **Desinfizieren** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
  - **Löschen** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
  - **In die Quarantäne verschieben** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
  - **Benutzer fragen**: Dem Benutzer wird eine Benachrichtigung angezeigt und gefragt, wie das Virus behandelt werden soll.
- **Falls Desinfektion fehlschlägt**: Wenn Sie die Option Desinfizieren ausgewählt haben, die Datei aber nicht desinfiziert werden kann, wird eine alternative Aktion ausgeführt.
- **Reaktion auf infizierte Archive**: Legen Sie fest, was passieren soll, wenn der Wächter eine infizierte Archive findet.
- **Dateitypen** (siehe **Aufträge** > **Scan-Aufträge** > **Scanner**).

Unter **Erweitert** können Sie die folgenden erweiterten Einstellungen konfigurieren:

- **Heuristik** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
- **Systembereiche prüfen** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
- **Archive prüfen** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
- **Maximale Größe für Archive** (siehe **Client-Einstellungen** > **Wächter** > **Einstellungen**)
- **Maximale Größe für Dateien**: Legen Sie die maximale Dateigröße fest. Dateien, die größer sind, werden nicht geprüft.

Unter **Ausnahmen** können Sie mit Hilfe einer Datei- und Verzeichnisliste einzelne Dateien und Verzeichnisse als Scan-Ausnahmen definieren.

Das Modul Wächter kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

9.3. Virenprüfung

Die Virenprüfung kann den ganzen Rechner oder auch bestimmte Dateien und Ordner auf Viren prüfen. Wenn ein Virus gefunden wird, wird automatisch die Aktion, die unter **Einstellungen** definiert wurde, ausgeführt. Darüber hinaus wird auch der ManagementServer benachrichtigt und ein Bericht zu dem Modul **Sicherheitsereignisse** im G DATA Administrator hinzugefügt.

Wählen Sie eine der folgenden Optionen aus und klicken Sie dann auf **Virenprüfung starten**:

- **Gesamten Rechner prüfen**: Alle Dateien und Ordner auf dem Rechner werden geprüft.
- **Systembereiche prüfen**: Der Bootsektor wird geprüft.
- **Dateien und Ordner prüfen**: Spezifische Dateien und Ordner werden geprüft. Den Scanumfang legen Sie unter **Scanumfang** fest.

Unter Einstellungen können Sie die Scan-Parameter festlegen (siehe **Wächter**).

Das Modul Virenprüfung kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** >

Client-Funktionen ein- und ausgeschaltet werden.

9.4. Update

Das Update-Modul sorgt dafür, dass der G DATA Security Client für Mac immer über die aktuellsten Virensignaturen verfügt, um den Rechner optimal zu schützen.

Unter **Letztes Update** werden Datum und Zeit der letzten Aktualisierung angezeigt. Die Signaturversion der beiden Engines wird unter **Engine A** bzw. **Engine B** angezeigt. Klicken Sie auf **Virensignaturen aktualisieren** um sofort Updates zu laden.

Die Aktualisierung der Virensignaturen kann unter **Einstellungen** konfiguriert werden:

- **Virensignaturen-Update**: Entscheiden Sie, ob der Client die Virensignaturen vom ManagementServer oder direkt von den G DATA Update-Servern beziehen soll (siehe **Client-Einstellungen** > **Allgemein** > **Updates**).
- **Planung**: Definieren Sie die Zeitplanung des Updates (**Manuell**, **Stündlich** oder **Täglich**).
- **Proxy-Server**: Wenn ein Proxy-Server verwendet werden soll, um Virensignaturen herunterzuladen, so geben Sie die Zugangsdaten für den Proxy-Server hier ein.
- **Zugangsdaten**: Geben Sie die Zugangsdaten für die G DATA Update-Server hier ein.

Die Einstellungen unter **Planung**, **Proxy-Server** und **Zugangsdaten** treffen nur zu, wenn unter **Virensignaturen-Update** eine andere Einstellung als **Virensignaturenupdates von ManagementServer herunterladen** gewählt wurde. Mehr Informationen finden Sie unter **Client-Einstellungen** > **Allgemein** > **Updates**.

Das Modul Update kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

9.5. Quarantäne

Das Modul Quarantäne zeigt eine Liste mit Dateien, die vom Wächter oder von einer Virenprüfung in die Quarantäne verschoben wurden.

Pro Datei werden die folgenden Eigenschaften angezeigt:

- **Dateiname**: Der Name und Pfad der infizierten Datei.
- **Virenname**: Der Name des Virus, das die Datei infiziert hat.
- **Dateigröße**: Die Größe der Datei.

Wählen Sie eine oder mehrere Dateien aus und klicken Sie auf eine der unter der Liste angezeigten Schaltflächen:

- **Desinfizieren und zurückbewegen**: Das Virus wird entfernt und die Datei wird zurück an ihren Ursprungsort bewegt.
- **Zurückbewegen**: Die Datei wird zurück an ihren Ursprungsort bewegt. Achtung: Wenn die Datei vorher nicht desinfiziert wird, kann sie das System infizieren!
- **Löschen**: Die Datei wird aus der Quarantäne gelöscht.

Das Modul Quarantäne kann im G DATA Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

9.6. Über G DATA Security Client

Das Fenster Über G DATA Security Client enthält Statusinformationen über den Security Client:

- **Version**: Die installierte Client-Version.
- **ManagementServer**: Der Name des ManagementServers, mit dem der Client verbunden ist.
- **Status der Sicherheitssoftware**: Der aktuelle Status der Hintergrundprozesse.

10. G DATA ActionCenter

G DATA ActionCenter bietet cloud-fähige G DATA Dienste an. Die Funktionalität ist in verschiedenen Modulen unterteilt. Nachdem Sie ein Konto erstellt und sich auf der Homepage **https://ac.gdata.de** eingeloggt haben, können Sie im Hauptbereich unter **Module** oder im Menü ein Modul auswählen:

- **Mobile Geräte**: Mobile Device Management für G DATA Lösungen für Endkunden.
- **Netzwerk Monitoring**: Überwachen Sie Ihre Netzwerkinfrastruktur, um Ausfälle zu verhindern.

Unter **Einstellungen** finden Sie folgende Verknüpfungen:

- **Berechtigungen**: Verwalten Sie hier die Berechtigungen für andere ActionCenter-Konten, wie z. B. die Nur-Lesen-Berechtigungen für das **Netzwerk Monitoring**.
- **E-Mail-Gruppen**: Mit Hilfe von E-Mail-Gruppen kann das ActionCenter Berichte und Alarmmeldungen verschicken, z. B. die Alarmmeldungen für das **Netzwerk Monitoring**.

Außerdem ermöglicht das ActionCenter das iOS Mobile Device Management, indem es die Kommunikation zwischen iOS-Geräten und dem G DATA ManagementServer verwaltet. Die Konfiguration des iOS Mobile Device Managements wird über den Knoten **iOS Mobile Device Management** im **Clients**-Bereich des G DATA Administrators vorgenommen.

10.1. Konto erstellen und verknüpfen

Klicken Sie auf der Loginseite vom ActionCenter auf **Registrieren** um ein Konto zu erstellen. Geben Sie dazu eine E-Mail-Adresse und ein Passwort ein und stimmen Sie den AGB zu. Sobald Sie auf Registrieren klicken, erhalten Sie eine E-Mail-Nachricht mit einem Bestätigungslink. Klicken Sie auf den Link um Ihr Konto zu bestätigen.

Nachdem Sie Ihr Konto bestätigt haben, öffnen Sie den G DATA Administrator und geben Sie Ihren Benutzernamen und Ihr Kennwort im Modul **ActionCenter** ein, um den G DATA ManagementServer mit dem ActionCenter zu verknüpfen.

10.2. Module

Die Funktionalität des G DATA ActionCenters ist in verschiedenen Modulen unterteilt. Für Business-Lösungen bietet das ActionCenter das Modul Netzwerk Monitoring an.

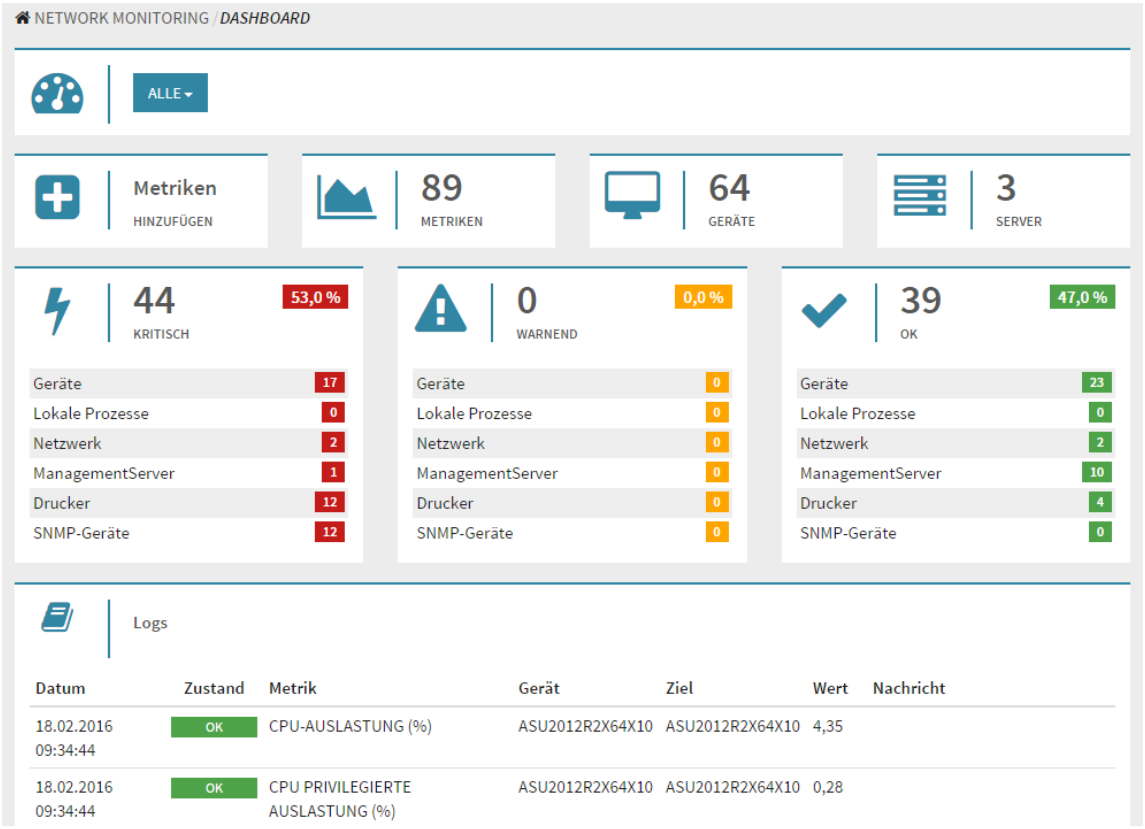
10.2.1. Netzwerk Monitoring

Das Netzwerk Monitoring ist als **optionales Modul** verfügbar.

Mit Hilfe vom Netzwerk Monitoring können Administratoren den Status der Netzwerkinfrastruktur im Auge behalten. Durch das Festlegen von **Metriken** kann eine breite Palette von Client-Statistiken gesammelt und im Dashboard angezeigt werden.

10.2.1.1. Dashboard

Das Dashboard bietet aktuelle Statistiken für alle **Metriken**, sowie eine Übersicht aller verwalteten **Servern** und **Geräten**. Wenn Sie eine Metrik zu Ihren Favoriten hinzufügen, wird im Dashboard ein Widget mit einer Zusammenfassung der Daten (Name, letzter Wert und Trenddiagramm) angezeigt.



In der Mitte des Dashboards wird der aktuelle Zustand aller Metriken angezeigt. Unter **OK** finden Sie eine Liste mit allen Metriken, die im Moment keine Schwellenwerte über- oder unterschreiten. Wenn eine Metrik einen Wert über oder unter einem zuvor festgelegten Schwellenwert meldet, wird der Zustand zu **Warnend** geändert. Nach zwei weiteren Verletzungen des Schwellenwertes wird der Zustand letztlich zu **Kritisch** geändert. Pro Zustand werden die Metriken nach Kategorie aufgelistet. Dies erlaubt eine detaillierte Übersicht, welche Gerätekategorie am meisten betroffen ist.

Der Bereich **Logs** zeigt Protokolleinträge aller Metriken an. Protokolleinträge werden erstellt, wenn eine Metrik zum ersten Mal einen Wert meldet, wenn ein Fehler gemeldet wird und wenn die Metrik eine Zustandsänderung hat (z. B. von **OK** zu **Kritisch**). Klicken Sie auf einen Protokolleintrag um die jeweilige **Metrik**-Seite zu öffnen.

Wenn mehrere Server verwaltet werden, können Sie mehrere Dashboard-Ansichten erstellen. Mit der Liste im oberen Bereich des Dashboards können Sie Ansichten erstellen und auswählen. Klicken Sie auf **Dashboard erstellen**, geben Sie einen **Namen** ein und wählen Sie einen oder mehrere ManagementServer, um eine Dashboard-Ansicht anzulegen.

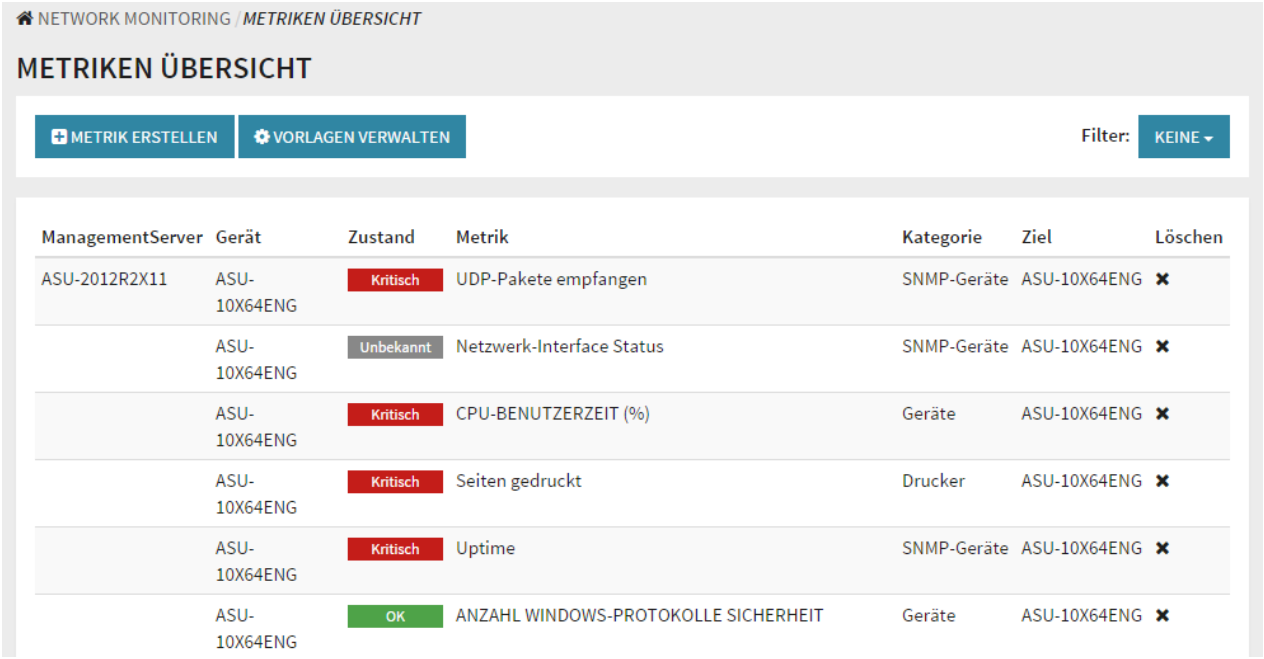
10.2.1.2. Metriken Übersicht

Sie können Metriken erstellen, indem Sie einem oder mehreren Geräten eine **Metrik-Vorlage** zuweisen. Auf Basis von den in der Vorlage spezifizierten Parametern meldet die Metrik dem ActionCenter regelmäßig die Statistiken der ausgewählten Geräte. Klicken Sie auf **Metrik erstellen** um eine neue Metrik anzulegen.

Die Seite **Metriken Übersicht** zeigt alle erstellten Metriken an. Wenn Sie auf eine Metrik klicken, wird die jeweilige **Metrik**-Seite geöffnet. Die Metrik-Liste kann nach Status oder Kategorie gefiltert werden. Für jeden Eintrag werden die folgenden Informationen angezeigt:

- **ManagementServer**: Der ManagementServer, dem das Gerät untergeordnet ist.
- **Gerät**: Das Gerät, dem die Metrikvorlage zugewiesen wurde.

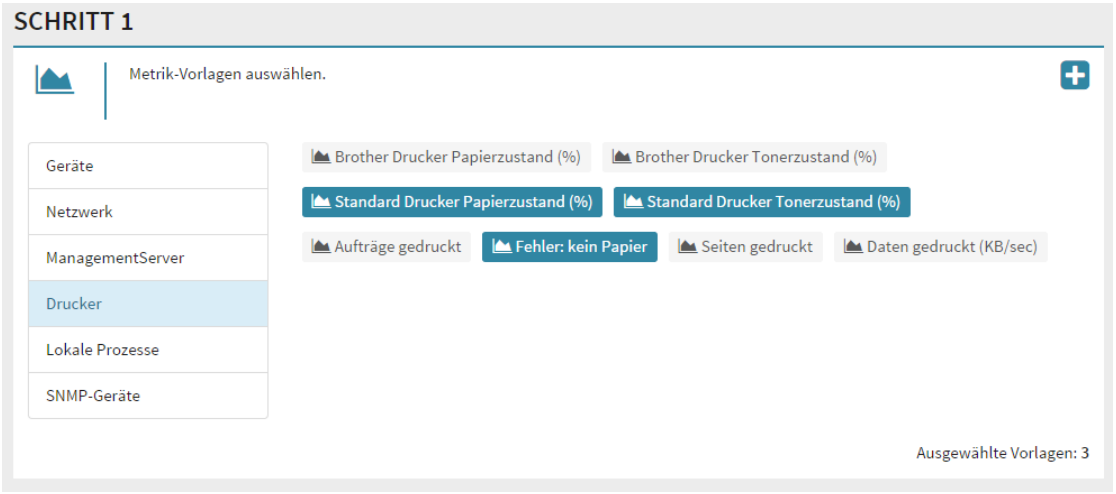
- **Zustand**: Der aktuelle Zustand der Metrik (**OK**, **Warnend**, **Kritisch** oder **Unbekannt**).
- **Metrik**: Der Name der Metrikvorlage, auf die sich die Metrik basiert.
- **Kategorie**: Die Kategorie der Metrikvorlage, auf die sich die Metrik basiert.
- **Ziel**: Das Zielgerät der Metrikvorlage, auf die sich die Metrik basiert.



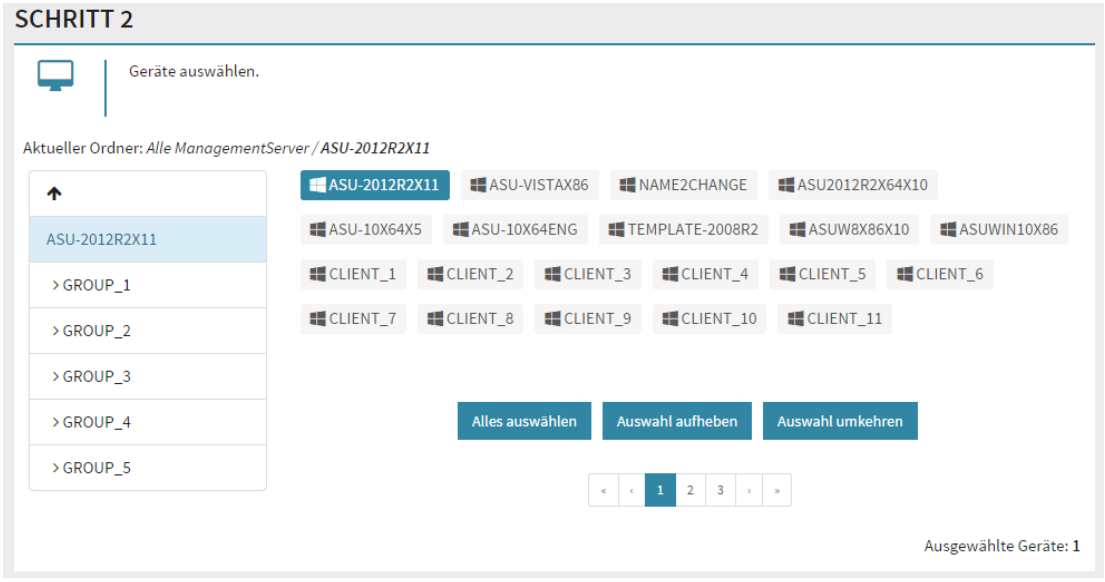
Metriken hinzufügen

Das Erstellen einer Metrik umfasst das Zuweisen von einer oder mehreren Vorlagen zu einem oder mehreren Geräten. Dies können Sie auf der Seite Metriken hinzufügen in vier Schritten erledigen:

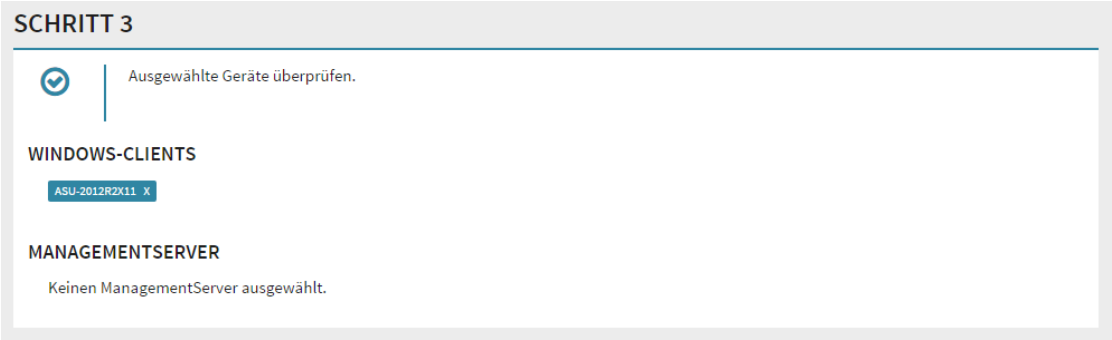
1. **Metrik-Vorlagen auswählen**. Wählen Sie eine oder mehrere Metrik-Vorlagen aus. Die Vorlagen werden pro Kategorie angezeigt.



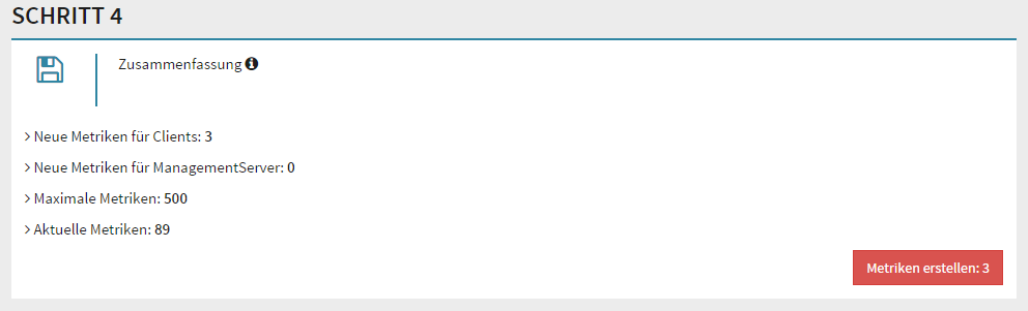
2. **Geräte auswählen**. Wählen Sie ein oder mehrere Geräte aus. Die Geräte werden in einer Ordnerstruktur angezeigt und sind pro ManagementServer gruppiert. Auf der oberen Ebene der Struktur können Sie die ManagementServer selbst auswählen (falls Sie im ersten Schritt eine Vorlage der Kategorie **ManagementServer** ausgewählt haben).



3. **Ausgewählte Geräte überprüfen**. Stellen Sie sicher, dass alle Geräte, zu denen eine Vorlage zugewiesen werden sollte, ausgewählt wurden.



4. **Zusammenfassung**. Klicken Sie auf **Metrik(en) erstellen**, um die gewählten Metriken zu erstellen und die **Metriken Übersicht** zu öffnen.



Metrik

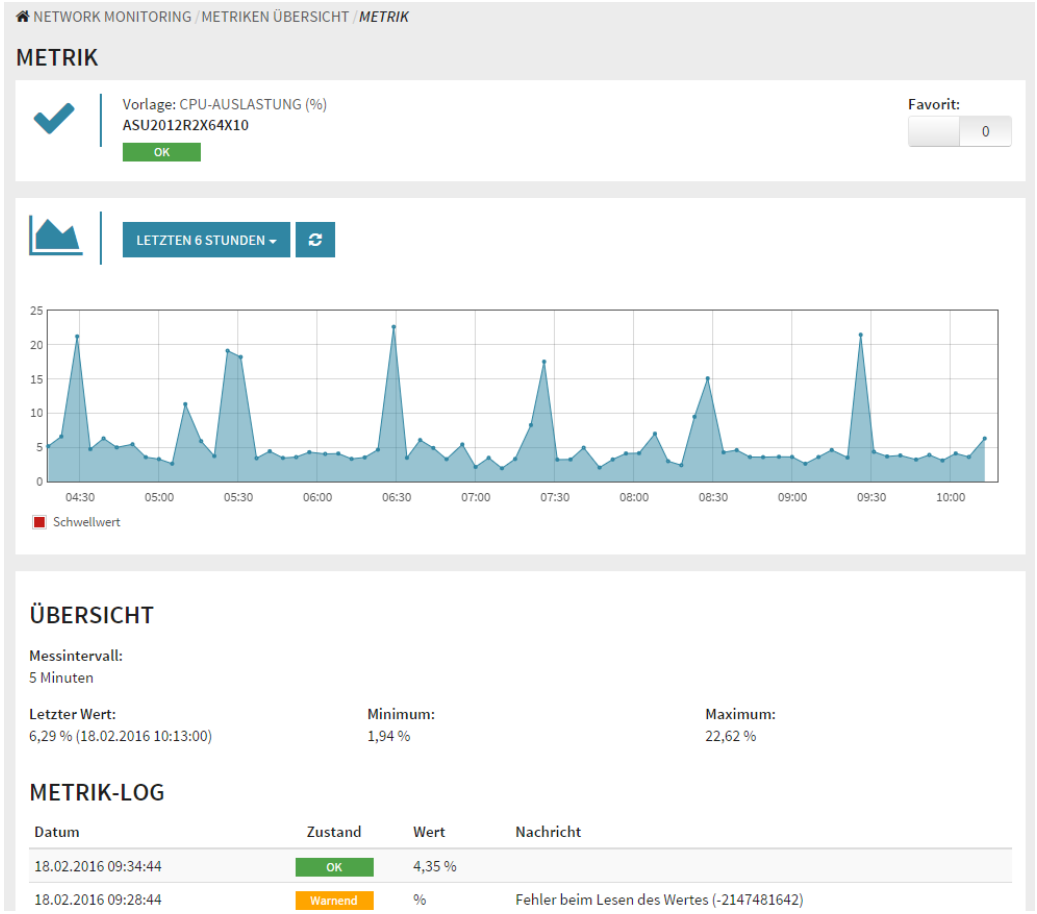
Auf der Seite Metrik können Sie die Details der ausgewählten Metrik überprüfen. Ganz oben werden der **Name**, das **Gerät** und der **ManagementServer** angezeigt, sowie der aktuelle Zustand. Klicken Sie auf **Favorit**, um die Metrik als Widget auf dem **Dashboard** anzuzeigen.

Die Diagramm-Anzeige kann angepasst werden, um Werte für einen bestimmten Zeitraum anzuzeigen. Die Standardeinstellung zeigt die Werte der letzten sechs Stunden an. Der Zeitraum kann im Auswahlmenü festgelegt werden.

Unter **Übersicht** finden Sie die folgenden Parameter:

- **Messintervall**: Das Intervall, in dem die Metrik neue Werte zum ActionCenter sendet.
- **Letzter Wert**: Der aktuellste Wert und Datum/Zeit.
- **Minimum**: Der bis jetzt niedrigste Messwert.

- **Maximum**: Der bis jetzt höchste Messwert.
- **Schwellwert** (nur wenn ein Schwellwert konfiguriert wurde): Der aktuelle Schwellwert.
- **Über dem Schwellwert** (nur wenn ein Schwellwert konfiguriert wurde): Prozentsatz der Messwerten, die über dem Schwellwert lagen.
- **Unter dem Schwellwert** (nur wenn ein Schwellwert konfiguriert wurde): Prozentsatz der Messwerten, die unter dem Schwellwert lagen.



Im Bereich **Metrik-Log** werden alle Protokolleinträge der Metrik angezeigt. Protokolleinträge werden erstellt, wenn eine Metrik zum ersten Mal einen Wert meldet, wenn ein Fehler gemeldet wird und wenn die Metrik eine Zustandsänderung hat (z. B. von **OK** zu **Kritisch**).

Metrik-Vorlagen verwalten

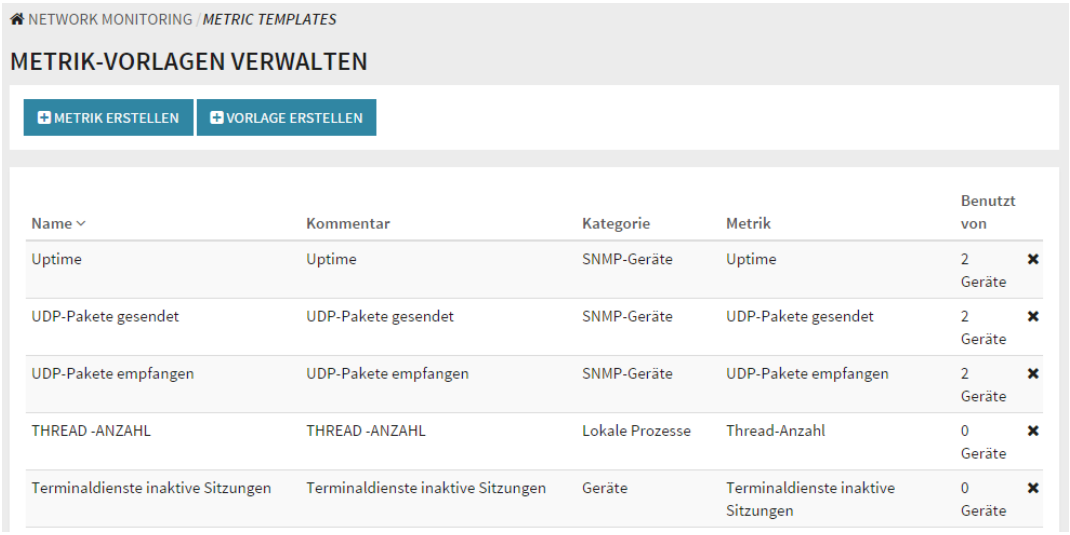
Metrik-Vorlagen enthalten die Parameter für spezifische Einsatzszenarien des Netzwerk Monitorings. Mit Hilfe von Vorlagen werden **Metriken** erstellt, indem eine Vorlage einem oder mehreren Geräten zugewiesen wird. Klicken Sie auf **Vorlage erstellen**, um eine Metrik-Vorlage anzulegen.

Die Seite Metrik-Vorlagen verwalten zeigt alle Metrik-Vorlagen an. Wenn Sie auf eine Metrik klicken, wird die Seite **Vorlage bearbeiten** geöffnet. Für jeden Eintrag in der Liste werden folgende Informationen angezeigt:

- **Name**: Der Name der Vorlage.
- **Kommentar**: Information, mit der Sie die Vorlagen einfacher von einander unterscheiden können.
- **Kategorie**: Die Kategorie der Vorlage (**Geräte**, **Lokale Prozesse**, **Netzwerk**, **ManagementServer**, **Drucker** oder **SNMP-Geräte**).
- **Metrik**: Beschreibt die Statistiken, die überwacht werden, abhängig von der ausgewählten

Kategorie.

- **Benutzt von**: Die Anzahl der Geräte, zu denen eine Metrik auf Basis dieser Vorlage zugewiesen wurde.



Vorlage erstellen

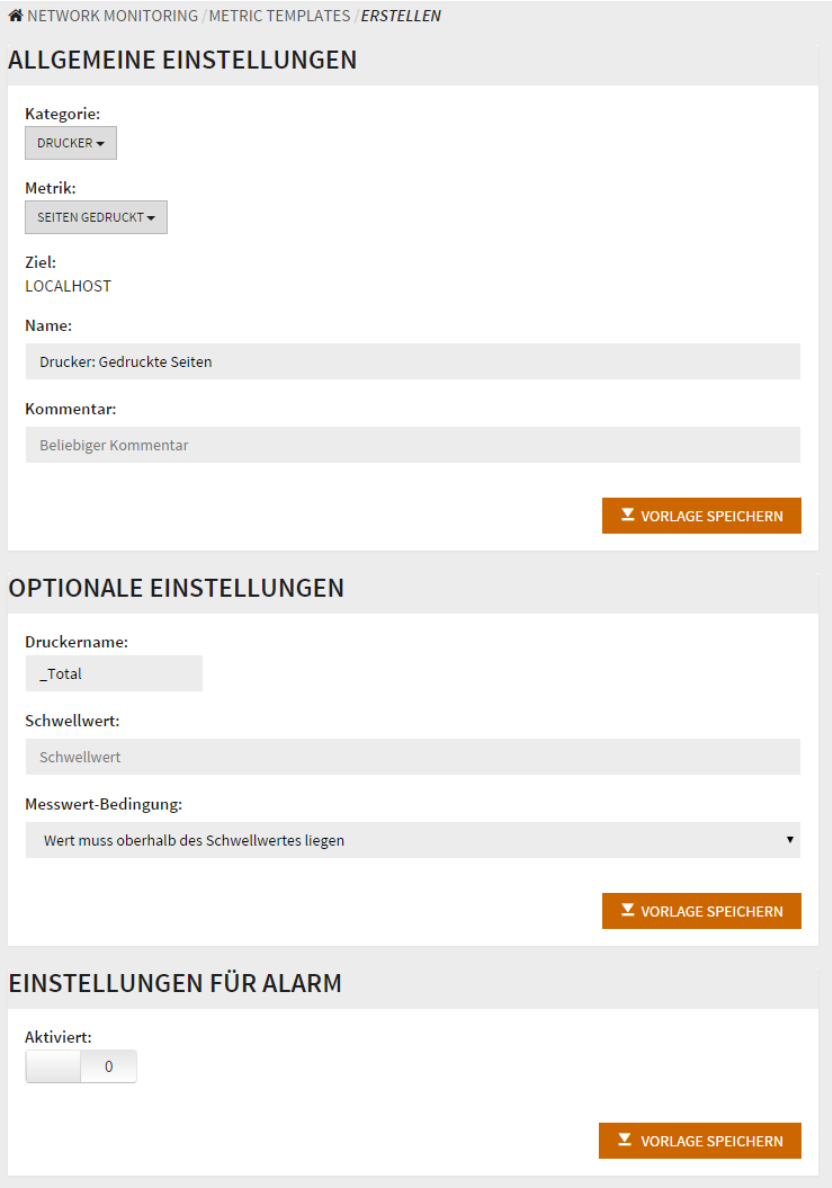
Um eine Metrik-Vorlage zu erstellen, müssen Sie eine Anzahl an erforderlichen und optionalen Parametern eingeben:

- **Kategorie**: Wählen Sie die Vorlage-Kategorie (**Geräte**, **Lokale Prozesse**, **Netzwerk**, **ManagementServer**, **Drucker** oder **SNMP-Geräte**).
- **Metrik**: Wählen Sie die Statistiken, die überwacht werden sollen, abhängig von der ausgewählten Kategorie.
- **Name**: Der Name der Vorlage.
- **Kommentar**: Information, mit der Sie die Vorlagen einfacher von einander unterscheiden können.

Abhängig von der ausgewählten **Kategorie** und **Metrik** werden eine oder mehrere der folgenden Einstellungen angezeigt:

- **Ziel**: Das Zielgerät, auf dem die ausgewählten Statistiken gesammelt werden. Dieser Wert kann nicht geändert werden und ist standardmäßig auf localhost vorkonfiguriert. Dies bedeutet, dass die Statistiken auf dem Gerät, dem die Vorlage zugewiesen wird, gesammelt werden.
- **Hostname**: Der Hostname des Geräts, auf dem die Statistiken überwacht werden. Der Hostname muss nicht unbedingt das Gerät sein, dem die Vorlage zugewiesen wird. Sie können mehrere Hostnamen eingeben; wenn die Vorlage einem Gerät zugewiesen wird, werden dann mehrere Metriken erstellt.
- **URL**: Die URL, für die die ausgewählten Statistiken überwacht werden. Sie können mehrere URLs eingeben; wenn die Vorlage einem Gerät zugewiesen wird, werden dann mehrere Metriken erstellt.
- **SQL Server Instanz**: Der SQL-Server-Instanz, auf dem die Statistiken überwacht werden. Klicken Sie auf die Lupe, um eine Liste von verfügbaren SQL-Servern pro ManagementServer zu öffnen.

Die optionalen Einstellungen sind auch von der **Kategorie** und **Metrik** abhängig und beinhalten eine oder mehreren der folgenden Einstellungen:



- **Schwellwert**: Definieren Sie einen Schwellwert.
- **Messwert-Bedingung**: Legen Sie fest, wie der Schwellwert interpretiert wird. Der Metrik-Zustand wird von **OK** zu **Warnend** und dann zu **Kritisch** geändert, wenn der Messwert über oder unter dem Schwellwert liegt.
- **CPU-Index**: Legen Sie fest, für welche CPU die Statistiken überwacht werden sollen, oder geben Sie _Total ein, um alle CPUs zu überwachen.
- **Laufwerk**: Legen Sie fest, für welches Laufwerk die Statistiken überwacht werden sollen, oder geben Sie _Total ein, um alle Laufwerke zu überwachen.
- **Prozessname**: Legen Sie fest, für welchen Prozess die Statistiken überwacht werden sollen, oder geben Sie _Total ein, um alle Prozesse zu überwachen.
- **Netzwerkadapter**: Legen Sie fest, für welchen Netzwerkadapter die Statistiken überwacht werden sollen, oder geben Sie * ein, um alle Netzwerkadapter zu überwachen.
- **SQL Server Datenbank**: Legen Sie fest, für welche Datenbank die Statistiken überwacht werden sollen, oder geben Sie _Total ein, um alle Datenbanken zu überwachen.
- **Zeitüberschreitung der Anfrage**: Geben Sie die Zeitüberschreitung für Ping-Anfragen ein.
- **Erwarteter HTTP-Status-Code**: Wenn die Metrik einen anderen HTTP-Status-Code als den hier definierten meldet, wird der Wert als Schwellwertverletzung interpretiert und der Zustand der Metrik entsprechend geändert.

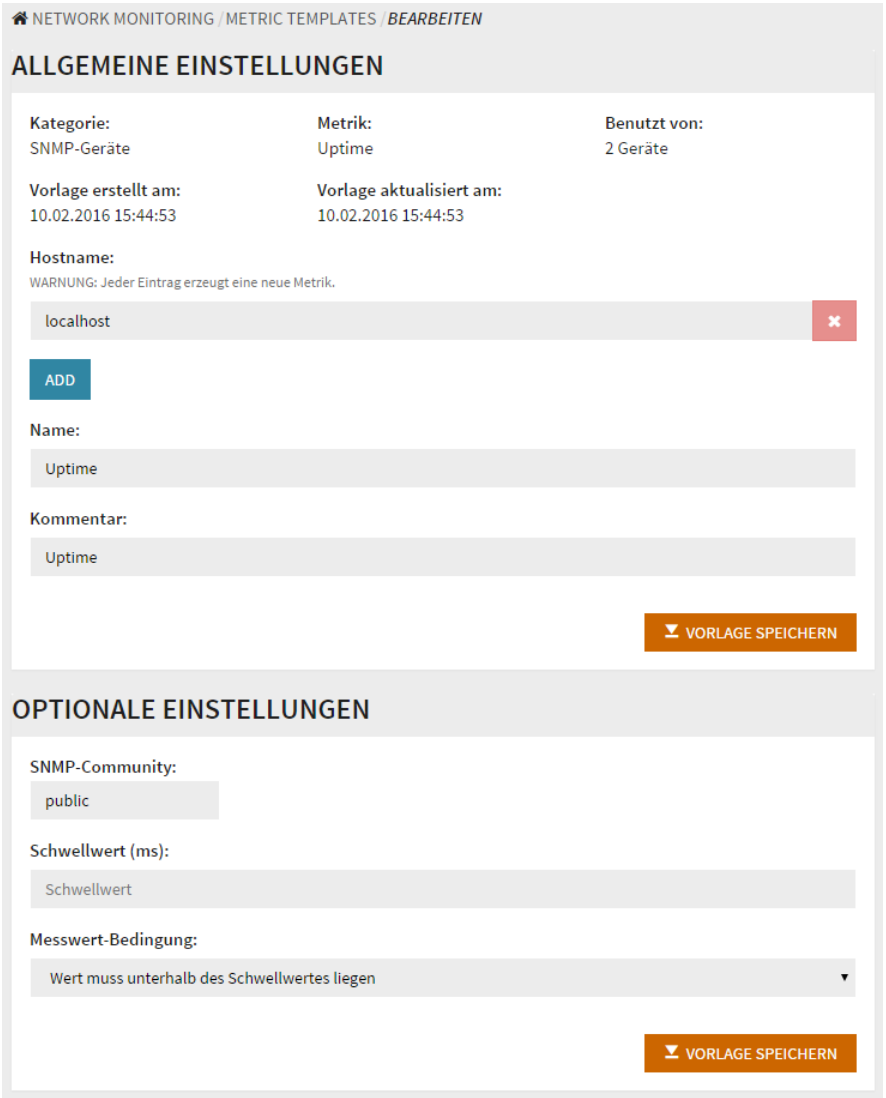
- **SNMP-Community**: Geben Sie den für das SNMP-Gerät erforderlichen SNMP-Community-Wert ein. Der Community-Wert wird vom Hersteller festgelegt und ist meistens in der Dokumentation einzusehen.

Unter **Einstellungen für Alarm** können Sie die E-Mail-Benachrichtigungen konfigurieren:

- **Alarmbedingung**: Eine Alarmnachricht wird gesendet, wenn der Zustand sich zu **Kritisch** ändert, oder wenn der Zustand sich zu **Kritisch** oder **Warnend** ändert.
- **Benachrichtigen Sie nur ausgewählte E-Mail-Gruppen**: Die Alarmnachricht wird an die ausgewählten E-Mail-Gruppen gesendet. E-Mail-Gruppen können unter **E-Mail-Gruppen** festgelegt werden.

Vorlage bearbeiten

Über die Seite Vorlage bearbeiten können Sie bestehende Metrik-Vorlagen anpassen. Alle Einstellungen werden genau so angezeigt, wie zu dem Zeitpunkt, als Sie die Vorlage angelegt haben. Manche können nachträglich nicht geändert werden:



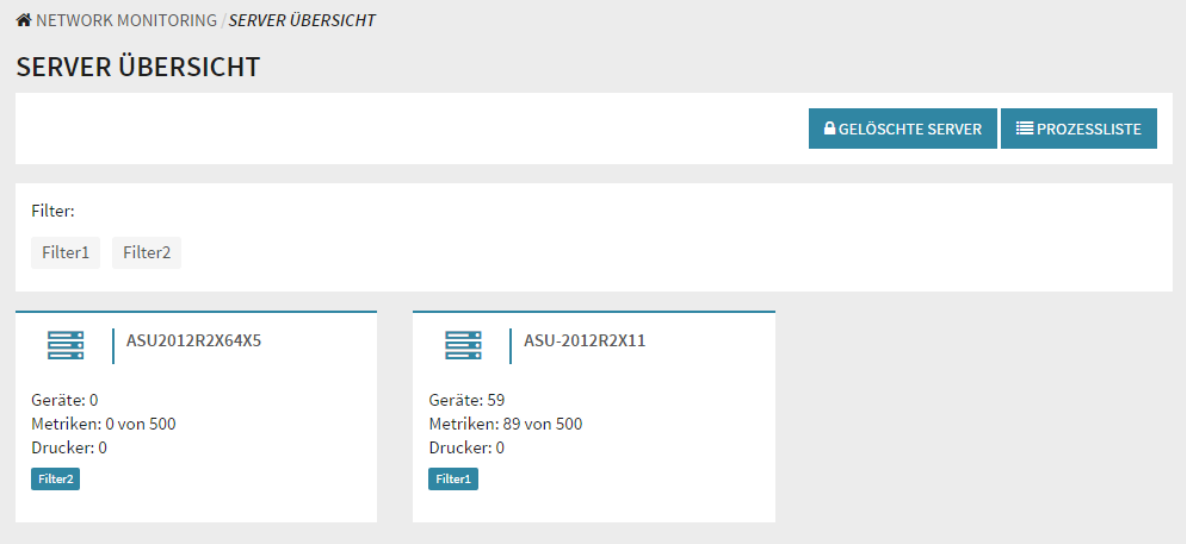
- **Kategorie**
- **Metrik**
- **Benutzt von**
- **Ziel**
- **Hostname**

- **URL**

Alle anderen Einstellungen können bearbeitet werden. Klicken Sie auf **Vorlage speichern** um Ihre Änderungen zu speichern. Änderungen an einer bestehenden Vorlage werden für alle auf der Vorlage basierenden Metriken übernommen.

10.2.1.3. Server Übersicht

In der Server-Übersicht werden alle mit dem ActionCenter-Konto verknüpften ManagementServer aufgelistet. Pro Server werden die jeweiligen Geräte, Metriken und Drucker angezeigt. Mit Hilfe der Kennzeichnungen unter **Filter** können Sie die Liste nach Ihrem Wunsch anpassen.



Klicken Sie auf einen Server um die Seite **Server Info** zu öffnen, welche die folgenden Informationen und Einstellungen anzeigt:

- **Hostname**: Der Hostname des Servers.
- **Version**: Die Versionsnummer des ManagementServers.
- **Letzter Zugriff**: Die letzte Synchronisierung zwischen diesem Server und dem ActionCenter.
- **Metriken**: Die Anzahl der mit diesem Server verwandten Metriken.
- **Geräte**: Die Anzahl der mit diesem Server verwandten Geräten.
- **Drucker**: Die Anzahl der mit diesem Server verwandten Druckern.
- **Kommentar**: Information, mit der Sie die Server einfacher von einander unterscheiden können.
- **API-Zugriff**: Standardmäßig aktiviert. Wenn Sie den API-Zugriff deaktivieren, wird der Server nicht aus dem ActionCenter entfernt, aber er kann dann keine Messwerte mehr melden.
- **Kennzeichnungen**: Fügen Sie eine oder mehrere Kennzeichnungen (Tags) hinzu, die Sie in der Server-Übersicht zum Filtern verwenden können.

Klicken Sie auf **Berechtigungen festlegen**, um einem anderen ActionCenter-Konto Berechtigungen für diesen Server zu erteilen. Geben Sie die E-Mail-Adresse des Kontos unter **E-Mail-Adresse** ein und klicken Sie auf **Einladung senden** um eine Einladung zu verschicken. Nachdem der Empfänger über den Einladungslink beim ActionCenter eingeloggt und die Einladung angenommen hat, bekommt er automatisch Nur-Lesen-Zugriff auf alle Netzwerk-Monitoring-Funktionalität dieses Servers. Sie können die Berechtigungen mit Hilfe des Bereichs **Berechtigungen** verwalten.

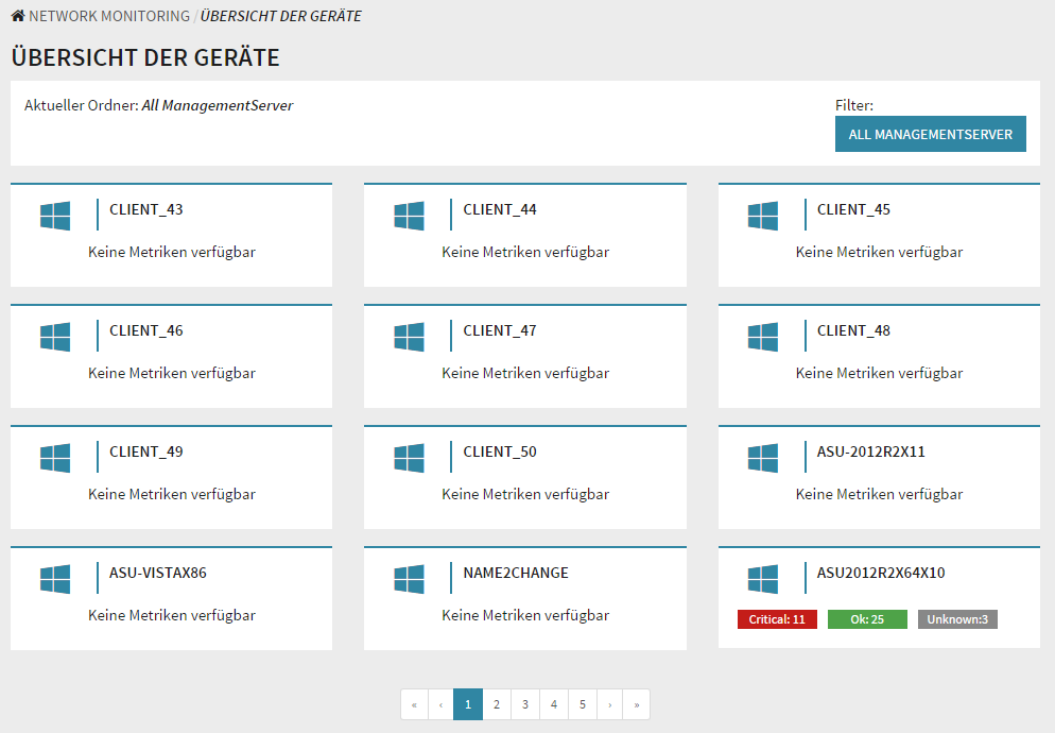
Falls es zu der angegebenen E-Mail-Adresse noch kein ActionCenter-Konto gibt, wird der

Empfänger aufgefordert, zuerst ein ActionCenter-Konto anzulegen. Unmittelbar danach kann er dann die Einladung annehmen.

Über **Server löschen** können Sie den Server aus dem ActionCenter entfernen. Dieser Vorgang entfernt auch alle assoziierten **Geräte**, **Metriken** und Protokolle.

10.2.1.4. Geräte Übersicht

Die Geräte-Übersicht zeigt alle Geräte, die von den mit dem ActionCenter-Konto verknüpften ManagementServern verwaltet werden. Sie können die Anzeige filtern, indem Sie unter **Filter** einen spezifischen ManagementServer auswählen.



Jedes Gerät wird samt Namen und zugewiesenen Metriken aufgelistet. Klicken Sie auf eine Metrik, um die jeweilige **Metrik**-Seite zu öffnen.

10.3. Einstellungen

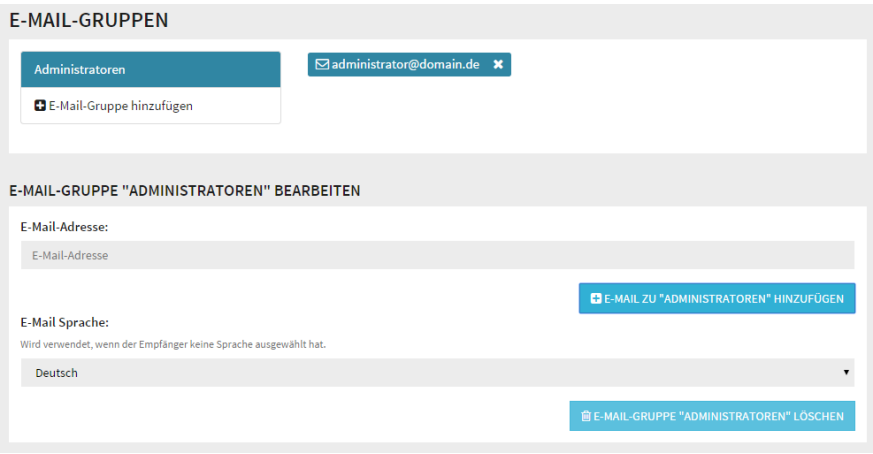
Der Bereich Einstellungen enthält Einstellungen, die in anderen ActionCenter-Modulen verwendet werden können.

10.3.1. Berechtigungen

Der Bereich Berechtigungen wird verwendet, um die unter **Netzwerk Monitoring** > **Server Übersicht** verteilten Berechtigungen zu verwalten. ActionCenter-Konten, die Berechtigungen erhalten haben, werden unter den jeweiligen ManagementServern aufgelistet. Klicken Sie auf **Entfernen**, um dem ausgewählten Konto die Berechtigungen zu entziehen.

10.3.2. E-Mail-Gruppen

E-Mail-Gruppen umfassen eine oder mehrere E-Mail-Adressen und werden für Berichte und Alarmnachrichten verwendet, wie zum Beispiel die Schwellwertbenachrichtigung des Moduls **Netzwerk Monitoring**. Die Seite E-Mail-Gruppen zeigt alle E-Mail-Gruppen und die enthaltenen E-Mail-Adressen.



Klicken Sie auf **E-Mail-Gruppe hinzufügen** um eine neue E-Mail-Gruppe zu erstellen. Geben Sie einen **Namen** ein, wählen Sie eine **Sprache** aus und klicken Sie dann auf **Hinzufügen**. Um der Gruppe eine E-Mail-Adresse hinzuzufügen, klicken Sie auf die Gruppe und geben dann unter **E-Mail-Gruppe bearbeiten** eine **E-Mail-Adresse** ein. Wiederholen Sie diesen Schritt um mehrere E-Mail-Adressen zur gleichen Gruppe hinzuzufügen.

11. G DATA MailSecurity MailGateway

G DATA MailSecurity ist als **optionales Modul** verfügbar.

G DATA MailSecurity MailGateway ist das Softwarepaket zum Komplettschutz Ihrer E-Mail-Kommunikation. Neben der eigentlichen Software, die im Hintergrund läuft, wird automatisch der **MailSecurity Administrator** installiert, über den Sie vollen Zugriff auf die Funktionen und Optionen des MailGateways haben. Diesen Administrator finden Sie bei einer Standardinstallation unter **Start** > **Programme** > **G DATA MailSecurity** > **G DATA MailSecurity**. Wenn Sie die Administrator-Software beenden, schließen Sie damit nicht das MailGateway. Dieses bleibt weiterhin im Hintergrund aktiv und steuert die Prozesse, die von Ihnen eingestellt wurden.

Sie können das MailGateway auch über jeden anderen Rechner warten, der die Systemvoraussetzungen für das G DATA MailSecurity Administrator-Tool erfüllt. Wenn Sie das MailGateway also über einen anderen Rechner im Netzwerk ansteuern möchten, installieren Sie dort einfach den Administrator ohne die eigentliche MailGateway-Software. Starten Sie dazu einfach erneut das Setup und wählen die Schaltfläche **G DATA MailSecurity Administrator** aus.

12. G DATA MailSecurity Administrator

G DATA MailSecurity ist als **optionales Modul** verfügbar.

Der G DATA MailSecurity Administrator ist die Steuerungssoftware für das G DATA MailSecurity MailGateway, das - vom Systemadministrator zentral gesteuert - den gesamten SMTP- und POP3 basierten E-Mailverkehr in Ihrem gesamten Netzwerk sichert. Der Administrator kann passwortgeschützt von jedem Rechner unter Windows gestartet werden. Als ferngesteuerte Jobs sind alle denkbaren Einstellungsänderungen am Virenscanner und Virensignatur-Updates möglich.

12.1. Starten des G DATA MailSecurity Administrators

Sie können den MailSecurity Administrator zur Steuerung des MailGateways mit einem Klick auf den Eintrag **G DATA MailSecurity** in der Programmgruppe **Start** > **(Alle) Programme** > **G DATA MailSecurity** des Startmenüs aufrufen. Beim Starten des Administrators werden Sie nach dem **Server** und dem **Kennwort** gefragt. Geben Sie in dem Feld **Server**, den Computernamen oder die IP-Adresse des Computers ein, auf dem das MailGateway installiert wurde.

Beim ersten Login haben Sie noch kein Kennwort vergeben. Klicken Sie ohne Eingabe eines Kennworts auf die **OK**-Schaltfläche. Es öffnet sich ein Kennworteingabefenster, in dem Sie unter **Neues Kennwort** ein neues Kennwort für den G DATA MailSecurity Administrator vergeben können. Sie bestätigen das eingegebenen Kennwort durch erneutes Eintippen im Feld **Neues Kennwort bestätigen** und klicken dann auf **OK**. Sie können das Kennwort jederzeit im Bereich **Optionen** in der Karteikarte **Erweitert** mit einem Klick auf die Schaltfläche **Kennwort ändern** neu vergeben.

12.2. G DATA MailSecurity Administrator konfigurieren

Die Menüleiste des G DATA MailSecurity Administrators bietet Ihnen folgende Optionen:

- **Optionen**: Hier können Sie grundlegende Einstellungen zum Betrieb Ihrer G DATA MailSecurity verändern und an Ihre individuellen Bedürfnisse anpassen.
- **Update**: Im Internet Update-Bereich können Sie grundlegende Einstellungen zum automatischen Download von aktuellen Virensignaturen aus dem Internet vornehmen. Sie können die Zeitplanungen für diese Downloads individuellen Bedürfnissen anpassen und außerdem Updates der Programmdateien von G DATA MailSecurity durchführen.
- **Spam-Filter**: Die Schaltfläche Spam-Filter ist eine Verknüpfung zu den Spam-Filter-

Einstellungen im **Filter**-Modul.

Hilfe: Hier rufen Sie die Online-Hilfe zum Produkt auf.

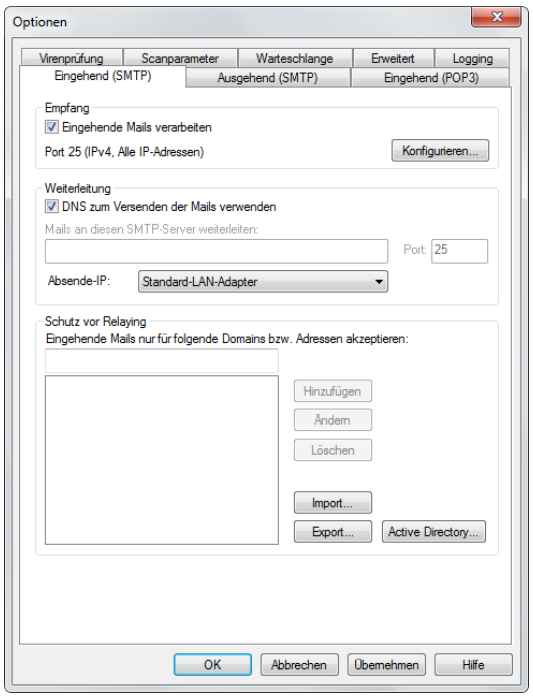
Info: Hier erhalten Sie Informationen zur Programmversion.

12.2.1. Optionen

Im Optionen-Bereich können Sie umfangreiche Einstellungen vornehmen, um G DATA MailSecurity optimal an die Gegebenheiten in Ihrem Netzwerk anzupassen. Dazu stehen Ihnen verschiedene thematisch untergliederte Einstellungsbereiche in verschiedenen Karteikarten zur Verfügung, die Sie durch Anklicken des jeweiligen Karteireiters in den Vordergrund holen.

12.2.1.1. Eingehend (SMTP)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle eingehender SMTP-Mails auf Ihrem Mail-Server vorzunehmen.



Empfang

Hier können Sie festlegen, ob eingehende Mails verarbeitet werden sollen. Generell ist hier Port 25 voreingestellt. Sollte auf Grund besonderer Umstände dieser Standard-Port nicht verwendet werden, können Sie über die Schaltfläche **Konfigurieren** auch andere Port-Einstellungen und Protokoll-Einstellungen für eingehende Mails definieren.

Weiterleitung

Zur Weiterleitung der eingehenden E-Mails an Ihren Mail-Server deaktivieren Sie bitte die Option **DNS zum Versenden der Mails verwenden** und geben Sie unter **Mails an diesen SMTP-Server weiterleiten** den gewünschten Server an. Geben Sie bitte auch den **Port** an, über den die E-Mails an den SMTP-Server weitergeleitet werden sollen. Sollten mehrere Netzwerkkarten zur Verfügung stehen, können Sie über die Auswahl unter **Absende-IP** festlegen, welche dieser Karten Sie verwenden möchten.

Schutz vor Relaying

Um einen Missbrauch Ihres Mail-Servers zu unterbinden, können und sollten Sie unter **Eingehende Mails nur für folgende Domains bzw. Adressen akzeptieren** die Domains festlegen, an die SMTP-Mails versendet werden dürfen. Auf diese Weise kann Ihr Server nicht zur Weiterleitung von SPAM-Mails

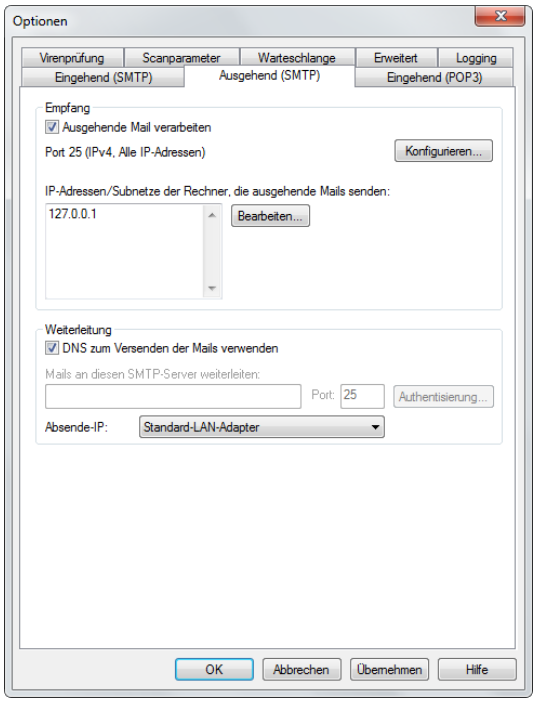
an andere Domains missbraucht werden.

> **Achtung**: Wenn Sie hier keine Domains eintragen, werden auch keine E-Mails angenommen. Sollen alle E-Mails von allen Domains angenommen werden, muss hier ein *.* (Sternchen Punkt Sternchen) hinzugefügt werden.

Der Relay-Schutz kann wahlweise auch über eine Liste von gültigen E-Mail-Adressen realisiert werden. E-Mails für Empfänger, die nicht auf der Liste stehen, werden nicht angenommen. Um die Pflege dieser E-Mailadressen zu automatisieren, können diese automatisch und periodisch aus dem **Active Directory** gelesen werden. Für die Active Directory-Anbindung wird mindestens das .NET Framework 1.1 benötigt.

12.2.1.2. Ausgehend (SMTP)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenprüfung ausgehender SMTP-Mails auf Ihrem Mail-Server vorzunehmen.



Empfang

Über das Häkchenfeld **Ausgehende Mail verarbeiten** legen Sie fest, ob Sie ausgehende SMTP-Mails auf Virenbefall kontrollieren möchten oder nicht. Unter **IP-Adressen/Subnetze der Rechner, die ausgehende Mails senden** können Sie bestimmen, von welchen IP-Adressen die zu überprüfenden E-Mails kommen. Wenn mehrere IP-Adressen dafür in Frage kommen, trennen Sie bitte die einzelnen IP-Adressen durch Kommata voneinander ab. Diese Eingabe ist nötig, damit das MailGateway eingehende und ausgehende E-Mails voneinander unterscheiden kann. Generell ist der Port 25 für den Empfang ausgehender E-Mails voreingestellt. Sollte auf Grund besonderer Umstände dieser Standardport nicht verwendet werden, können Sie über die Schaltfläche **Konfigurieren** auch andere Einstellungen für ausgehende E-Mails definieren.

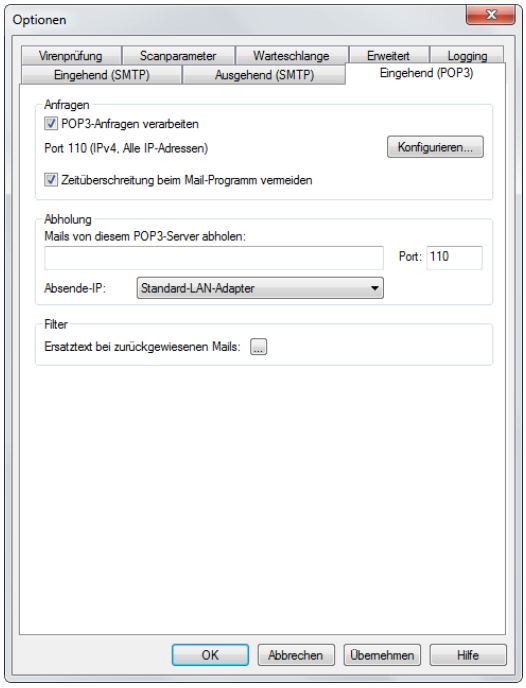
Weiterleitung

Aktivieren Sie den Eintrag **DNS zum Versenden der Mails verwenden**, damit die E-Mails direkt an den für die Zieldomäne zuständigen Mail-Server geschickt werden. Wenn Sie die E-Mails indirekt über ein Relay (z. B. einen Provider) versenden möchten, deaktivieren Sie **DNS zum Versenden der Mails verwenden** und geben Sie unter **Mails an diesen SMTP-Server weiterleiten** das Relay an. Sollten mehrere Netzwerkkarten zur Verfügung stehen, können Sie über die Auswahl unter **Absende-IP**

festlegen, welche dieser Karten Sie verwenden möchten.

12.2.1.3. Eingehend (POP3)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenprüfung eingehender POP3-Mails auf Ihrem Mail-Server vorzunehmen.



Anfragen

Unter **POP3-Anfragen verarbeiten** aktivieren Sie die Möglichkeit, über G DATA MailSecurity Ihre POP3-Mails vom entsprechenden POP3-Server abzuholen, auf Viren zu überprüfen und über Ihren Mail-Server an die Empfänger weiterzuleiten. Sie müssen dazu gegebenenfalls den **Port** angeben, den Ihr Mailprogramm für POP3-Anfragen verwendet (in der Regel Port 110). Mit der Funktion **Zeitüberschreitung beim Mail-Programm vermeiden** überbrücken Sie die Zeit, die G DATA MailSecurity zum Überprüfen der E-Mails benötigt und verhindern so, dass der Empfänger beim Abruf seiner POP3-Mails möglicherweise vom Mail-Programm einen Timeout-Fehler erhält, weil die Daten nicht sofort zur Verfügung stehen (sondern je nach Mail-Aufkommen erst ein paar Sekunden verzögert).

POP3-basierte Mailprogramme können manuell konfiguriert werden. Verwenden Sie dabei in Ihrem Mail-Programm 127.0.0.1 bzw. den Server Ihres MailGateways als eingehenden POP3-Server und schreiben Sie den Namen des externen Mail-Servers, mit einem Doppelpunkt getrennt, vor den Benutzernamen. Also z. B. statt *POP3-Server:mail.xxx.de/Benutzername:Erika Musterfrau* schreiben Sie *POP3-Server:127.0.0.1/Benutzername:mail.xxx.de:Erika Musterfrau*. Um eine manuelle Konfiguration durchzuführen, informieren Sie sich bitte auch in der Bedienungsanleitung Ihres Mail-Programms über die notwendigen Schritte für eine manuelle Konfiguration.

Abholung

Unter **Mails von diesem POP3-Server abholen** müssen Sie gegebenenfalls den POP3-Server angeben, von dem Sie die Mails abholen (z. B. *pop3.maildienstanbieter.de*).

Filter

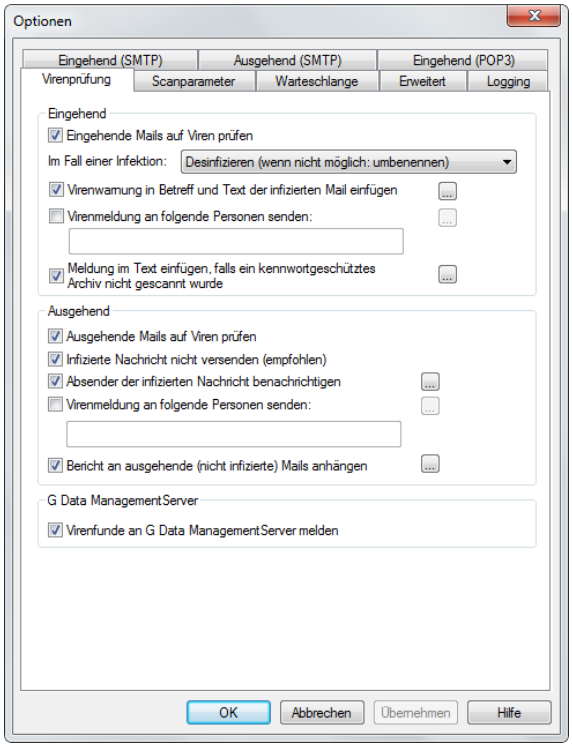
Wenn POP3-Mails auf Grund einer Content-Prüfung oder auf Grund eines Virenbefalls zurückgewiesen werden, kann der Absender dieser Nachricht automatisch darüber informiert werden. Der Ersatztext bei zurückgewiesenen Mails lautet dabei: *Die Nachricht wurde vom Systemadministrator*

zurückgewiesen. Sie können den Text für diese Benachrichtigungsfunktionen aber auch individuell gestalten. Dabei können Sie auch Platzhalter verwenden, die die entsprechenden Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen. Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

- %v > Virus
- %s > Absender
- %r > Empfänger
- %c > Cc
- %d > Datum
- %u > Betreff
- %h > Header
- %i > Absender-IP

12.2.1.4. Virenprüfung

Bei der Virenprüfung haben Sie die Möglichkeit, Virenprüfungsoptionen für ein- und ausgehende E-Mails einzustellen.



Eingehend

Grundsätzlich sollten Sie natürlich die Funktion **Eingehende Mails auf Viren prüfen** aktiviert haben und auch darauf achten, welche Option Sie **Im Fall einer Infektion** nutzen möchten.

- **Nur protokollieren**
- **Desinfizieren (wenn nicht möglich: nur protokollieren)**
- **Desinfizieren (wenn nicht möglich: umbenennen)**
- **Desinfizieren (wenn nicht möglich: löschen)**
- **Infizierte Anhänge umbenennen**

- **Infizierte Anhänge löschen**
- **Nachricht löschen**

Optionen, in denen nur ein Protokollieren eingehender Viren stattfindet, sollten Sie nur dann verwenden, wenn Sie Ihr System auf andere Weise permanent vor Virenbefall geschützt haben (z. B. mit dem Client/Server-basierten Virenschutz G DATA AntiVirus Business).

Bei Virenfunden haben Sie eine große Anzahl von Benachrichtigungsoptionen. So können Sie eine Virenwarnung in den Betreff und den Text der infizierten Mail einfügen, um den Empfänger einer solchen E-Mail zu informieren. Auch können Sie eine Meldung über den Virenfund an bestimmte Personen senden. sie können z. B. den Systemadministrator oder zuständige Mitarbeiter davon in Kenntnis setzen, dass ein Virus an eine E-Mail-Adresse in ihrem Netzwerk verschickt wurde. Mehrere Empfängeradressen trennen Sie bitte mit Semikolons voneinander ab.

Sie können den Text für die Benachrichtigungsfunktionen individuell gestalten. Hierbei handelt es sich um die gleichen Platzhalter, wie diejenigen, die unter **Eingehend (POP3)** > **Filter** verwendet werden.

Ausgehend

Grundsätzlich sollten Sie die Funktion **Ausgehende Mails auf Viren prüfen** aktiviert haben und die Funktion **Infizierte Nachricht nicht versenden** standardmäßig eingeschaltet haben. Auf diese Weise verlässt kein Virus Ihr Netzwerk und richtet möglicherweise bei Geschäftspartnern Schaden an. Bei Virenfunden haben Sie eine große Anzahl von Benachrichtigungsoptionen. So können Sie den **Absender der infizierten Nachricht benachrichtigen** und unter **Virenmeldung an folgende Personen senden** z. B. Systemverwalter oder zuständige Mitarbeiter davon in Kenntnis setzen, dass aus Ihrem Netzwerk ein Virus verschickt werden sollte. Mehrere Empfängeradressen trennen Sie bitte mit Semikolons voneinander ab.

Sie können den Text für die Benachrichtigungsfunktionen individuell gestalten. Klicken Sie dazu einfach auf die **...**-Schaltfläche rechts. Hierbei handelt es sich um die gleichen Platzhalter, wie diejenigen, die unter **Eingehend (POP3)** > **Filter** verwendet werden.

Zusätzlich haben Sie unter **Bericht an ausgehende (nicht infizierte) Mails anhängen** die Möglichkeit, von G DATA MailSecurity geprüfte E-Mails mit einem Bericht am Ende des E-Mailtextes zu versehen, in dem explizit darauf hingewiesen wird, dass diese E-Mail von G DATA MailSecurity geprüft wurde. Selbstverständlich können Sie diesen Bericht aber auch individuell verändern oder ganz weglassen.

G DATA ManagementServer

Wenn Sie eine Client/Server-basierte G DATA Business-Lösung installiert haben, können Sie über das Setzen des Häkchens bei **Virenfunde an G DATA ManagementServer melden** dafür sorgen, dass der G DATA ManagementServer über Virenfunde des MailGateways benachrichtigt wird und Ihnen auf diese Weise einen umfassenden Überblick über die Virenbelastung bzw. -gefährdung Ihres Netzwerkes liefert.

12.2.1.5. Scanparameter

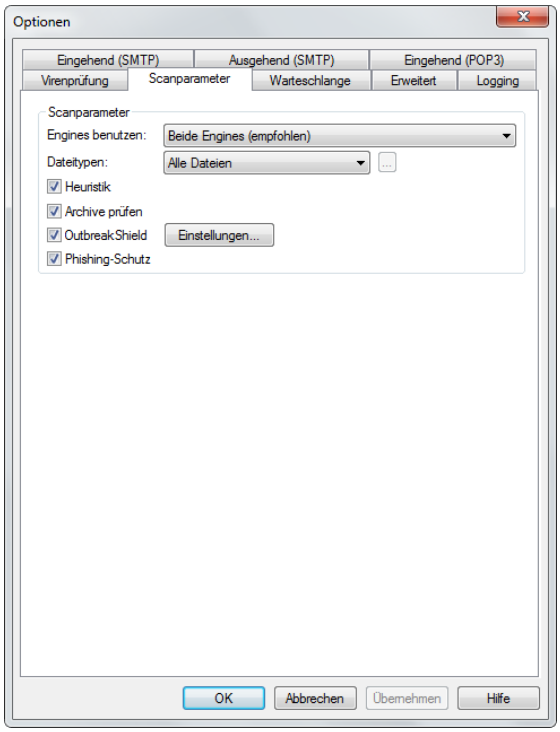
In diesem Bereich können Sie die Virenerkennungsleistung von G DATA MailSecurity optimieren und an persönliche Erfordernisse anpassen. Generell gilt, dass durch eine Verringerung der Virenerkennungsleistung die Performance des Gesamtsystems steigt, während eine Erhöhung der Virenerkennungsleistung möglicherweise leichte Einbußen in der Performance mit sich bringen kann.

Hier ist von Fall zu Fall abzuwägen.

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Engines benutzen**: G DATA MailSecurity arbeitet mit zwei unabhängig voneinander operierenden Antiviren-Engines. Unter Engines benutzen stellen Sie ein, wie diese miteinander kooperieren. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenerkennung. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich, d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen.
- **Dateitypen**: Unter Dateitypen können Sie festlegen, welche Dateitypen von G DATA MailSecurity auf Viren untersucht werden sollen. Wir empfehlen hier die automatische Typ-Erkennung über die automatisch nur die Dateien geprüft werden, die theoretisch auch einen Virus enthalten können. Wenn Sie selber die Dateitypen definieren möchten, für die eine Virenprüfung erfolgen soll, verwenden Sie die Funktion **Benutzerdefiniert**. Durch Anklicken der **...**-Schaltfläche können Sie dann eine Dialogbox öffnen, in der Sie die gewünschten Dateitypen ins obere Eingabefeld eintragen und dann über die **Hinzufügen**-Schaltfläche in die Liste der benutzerdefinierten Dateitypen übernehmen. Sie können dabei auch mit Platzhaltern arbeiten.

  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 prüfen zu lassen, geben Sie also **.exe*ein. Um z. B. Dateien unterschiedlicher Tabellenkalkulationsformate zu überprüfen (z. B. xlr, xls), geben Sie einfach **.xl?*ein. Um z. B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu prüfen, geben Sie beispielsweise *text*.**ein.
- **Heuristik**: In der Heuristik-Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist einerseits ein weiteres Sicherheitsplus, andererseits kann sie in seltenen Fällen auch einen Fehlalarm erzeugen.



- **Archive prüfen**: Das Überprüfen gepackter Dateien in Archiven sollte generell aktiviert sein.
- **OutbreakShield**: Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt

und bekämpft werden, bevor aktualisierte Signaturen 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 Signaturen besteht. Wenn Sie das **OutbreakShield** verwenden möchten, geben Sie über die Schaltfläche **Einstellungen** an, ob Sie einen Proxyserver verwenden und gegebenenfalls - um OutbreakShield jederzeit Zugang zum Internet zu ermöglichen - die **Zugangsdaten für die Internetverbindung** ein. Auf der Registerkarte OutbreakShield können Sie den Text der E-Mail definieren, den ein E-Mailempfänger erhält, wenn eine an ihn gerichtete Massenmail zurückgewiesen wurde.

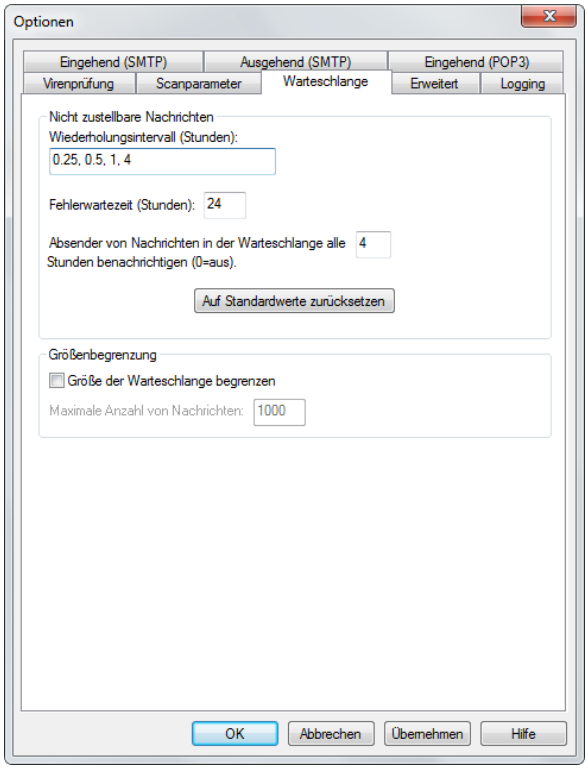
Da das OutbreakShield auf Grund seiner eigenständigen Architektur infizierte E-Mailanhänge nicht desinfizieren, umbenennen oder in die Quarantäne verschieben kann, informiert der Ersatztext den Anwender darüber, dass ihm die verdächtige bzw. infizierte E-Mail nicht zugestellt wurde. Eine Meldung über vom OutbreakShield zurückgewiesene E-Mails entfällt, wenn Sie auf der Karteikarte **Virenprüfung** > **Eingehend** unter **Im Falle einer Infektion** den Punkt **Nachricht löschen** auswählen. In diesem Fall werden alle infizierten E-Mails, inklusive derer, die ausschließlich vom OutbreakShield erkannt werden, direkt gelöscht.

- **Phishing-Schutz**: Aktivieren Sie den Phishing-Schutz, um E-Mails von vermeintlich seriösen Institutionen zu blockieren. Diese sogenannten Phishing-Mails werden versendet, um Benutzerdaten wie z. B. Kennwörter, Kreditkarteninformationen oder andere persönlichen Daten von Ihrem Rechner zu sammeln.

12.2.1.6. Warteschlange

In diesem Bereich können Sie festlegen, wie oft und in welchen Abständen der erneute Versand von E-Mails erfolgen soll, die vom MailGateway nicht an den entsprechenden Mail-Server weitergeleitet werden können.

Generell gelangen E-Mails erst nach der Virenüberprüfung durch die G DATA MailSecurity in die Warteschlange. E-Mails können sich dabei aus verschiedenen Gründen in der Warteschlange befinden. So kann z. B. der Mail-Server, an den Sie nach der Virenprüfung weitergeleitet werden sollen, überlastet oder ausgefallen sein.



Nicht zustellbare Nachrichten

Geben Sie unter **Wiederholungsintervall** an, in welchen Abständen G DATA MailSecurity einen neuen Versendeversuch unternehmen soll. So bedeutet z. B. die Angabe *1, 1, 1, 4*, dass G DATA MailSecurity die ersten drei Stunden stündlich versucht, die E-Mail zu verschicken und von da an regelmäßig im Abstand von 4 Stunden. Unter **Fehlerwartezeit** legen Sie fest, wann die Versendung der E-Mail endgültig abgebrochen und die E-Mail gelöscht wird.

Sie können **Absender von Nachrichten in der Warteschlange alle ... Stunden benachrichtigen**, wobei **...** ein ganzzahliger Stundenwert sein muss. Wenn Sie die Absender einer nicht zustellbaren Nachricht nicht regelmäßig informieren möchten, geben Sie hier einfach eine *0* ein. Auch wenn Sie die regelmäßige Benachrichtigung von Absendern nicht weitergeleiteter E-Mails abschalten, wird der Absender natürlich dennoch informiert, wenn seine E-Mail endgültig nicht zugestellt und vom Server gelöscht wurde.

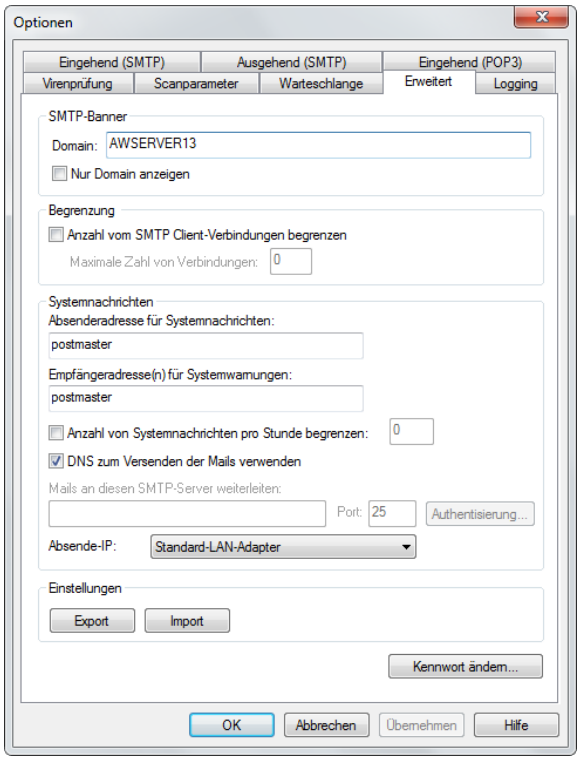
Über die Schaltfläche **Auf Standardwerte zurücksetzen** können Sie die Standardeinstellungen im Bereich Warteschlange wiederherstellen. Diese Einstellungen haben sich in der Praxis bewährt.

Größenbegrenzung

Die Größe der Warteschlange kann auf Wunsch begrenzt werden. Dies dient dem Schutz vor Denial of Service-Attacken. Sollte die Größenbeschränkung überschritten werden, werden keine weiteren E-Mails mehr in die Warteschlange aufgenommen.

12.2.1.7. Erweitert

Im Erweitert-Bereich können Sie die globalen Einstellungen von G DATA MailSecurity verändern.



SMTP-Banner

Standardmäßig beinhalt das Feld **Domain** den Computernamen. Beim Senden von ausgehenden E-Mails über DNS sollte der Fully Qualified Domain Name (FQDN) hier eingetragen werden, um Reverse-Lookups zu ermöglichen. Aktivieren Sie **Nur Domain anzeigen**, um die Anzeige der Server-Version in der Kommunikation mit anderen Servern zu unterdrücken.

Begrenzung

Um die Anzahl der SMTP-Verbindungen zu begrenzen, die G DATA MailSecurity gleichzeitig verarbeitet, setzen Sie bitte das Häkchen vor **Anzahl von SMTP Client-Verbindungen begrenzen**. G DATA MailSecurity lässt dann nur die maximale Zahl von Verbindungen zu, die Sie vorgeben. Auf diese Weise können Sie die Mailfilterung an die Leistung der Hardware anpassen, die Sie für das MailGateway verwenden.

Systemnachrichten

Die **Absenderadresse für Systemnachrichten** ist die E-Mail-Adresse, die z. B. dazu verwendet wird, Absender und Empfänger vireninfizierter E-Mails zu informieren oder darüber zu informieren, dass sich ihre E-Mails in der Warteschlange befinden. G DATA MailSecurity Systemwarnungen sind unabhängig von den allgemeinen Mitteilungen bei Virenfunden. Bei einer Systemwarnung handelt es sich in der Regel um eher globale Informationen, die nicht mit einer einzelnen, möglicherweise infizierten E-Mail in Zusammenhang stehen. So würde G DATA MailSecurity z. B. eine Systemwarnung verschicken, wenn die Virenprüfung aus irgendwelchen Gründen nicht mehr gewährleistet ist.

Einstellungen

Über die Schaltflächen **Import** und **Export** können Sie die Einstellungen der Programm-Optionen auch als XML-Datei speichern und so ggf. erneut einspielen, wenn der Bedarf gegeben ist.

Kennwort ändern

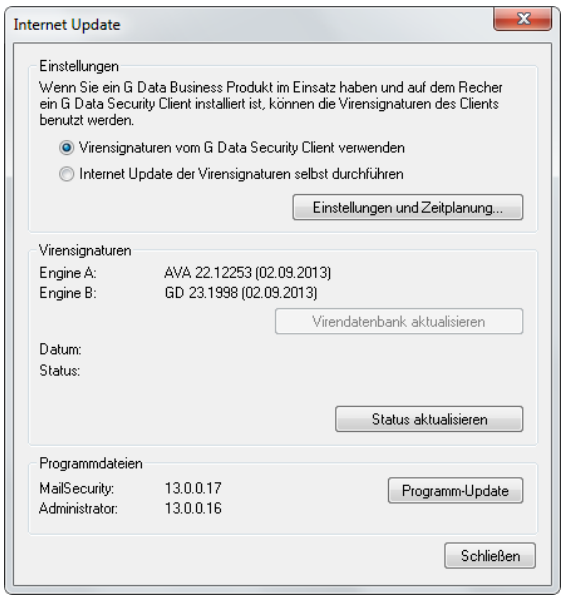
Hier können Sie das Administrator-Passwort ändern, dass Sie beim ersten Start von G DATA MailSecurity vergeben haben. Geben Sie dazu einfach das momentan aktuelle Passwort unter **Altes Kennwort** ein und dann unter **Neues Kennwort** und **Neues Kennwort bestätigen** das neue Kennwort. Mit dem Anklicken der **OK**-Schaltfläche wird die Kennwortänderung durchgeführt.

12.2.1.8. Logging

Im Logging-Bereich können Sie den E-Mailverkehr auf Ihrem Server statistisch auswerten. Die Ergebnisse dieser Statistikfunktion können Sie im Statistik-Bereich der Programmoberfläche aufrufen, den Sie durch das Anklicken der Schaltfläche **Statistik** im Programmbereich **Status** finden. Alternativ können Sie die ermittelten Daten auch in einer externen Log-Datei abspeichern (maillog.txt, gespeichert im MailSecurity-Installationsverzeichnis). Über die Funktionen **Nur Junk-Mails** und **Anzahl von E-Mails begrenzen** können Sie die Größe dieser Log-Datei gegebenenfalls begrenzen.

12.2.2. Update

Im Update-Bereich können Sie umfangreiche Einstellungen vornehmen, um G DATA MailSecurity optimal auf die Gegebenheiten anzupassen, die in Ihrem Netzwerk existieren. Hier können Sie die Virensignaturen und Programmdateien von G DATA MailSecurity manuell oder automatisiert auf den neuesten Stand bringen.

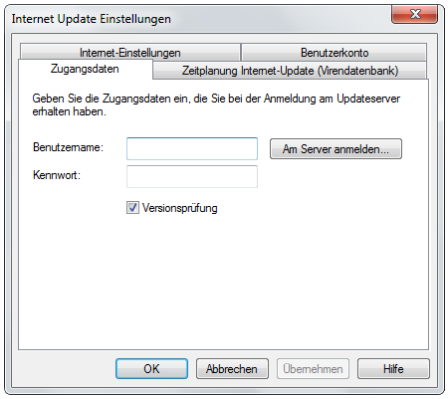


12.2.2.1. Einstellungen

Hier können Sie grundlegende Einstellungen für das Internet Update vorgeben. Wenn Sie (z. B. im Rahmen einer G DATA Business-Lösung) parallel zu G DATA MailSecurity den G DATA Security Client installiert haben, können Sie sich über **Virensignaturen vom G DATA Security Client verwenden** den doppelten Download der Virensignaturen sparen und diese direkt vom installierten G DATA Security Client aus erhalten. Über **Internet Update der Virensignaturen selbst durchführen** führt G DATA MailSecurity diesen Vorgang selbstständig durch. Über die Schaltfläche **Einstellungen und Zeitplanung** gelangen Sie in einen Bereich, in dem Sie sämtliche notwendigen Einstellungen für manuelle und automatische Internet Updates eingeben können.

Zugangsdaten

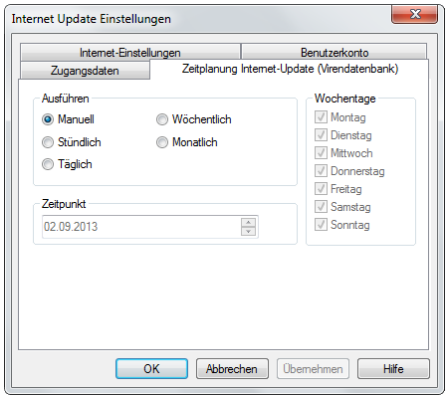
Geben Sie unter Zugangsdaten den **Benutzernamen** und das **Kennwort** ein, das Sie bei der Anmeldung von G DATA MailSecurity erhalten haben. Mit Hilfe dieser Daten werden Sie vom G DATA-Server erkannt und das Update der Virensignaturen kann vollautomatisch erfolgen. Klicken Sie auf die Schaltfläche **Am Server anmelden**, wenn Sie sich noch nicht am G DATA-Server angemeldet haben. Geben Sie einfach die Registriernummer ein (Sie finden diese auf der Rückseite des Benutzerhandbuches), Ihre Kundendaten und klicken Sie auf **Anmelden**. Sofort werden Ihnen die Zugangsdaten (Benutzername und Passwort) angezeigt. Sie sollten sich diese Daten aufschreiben und sicher verwahren. Für die Anmeldung am Server ist natürlich (wie auch für das Internet Update der Virensignaturen) eine Internetverbindung notwendig.



Zeitplanung Internet-Update (Virendatenbank)

Über die Karteikarte Zeitplanung Internet-Update (Virendatenbank) 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** spezifizieren.

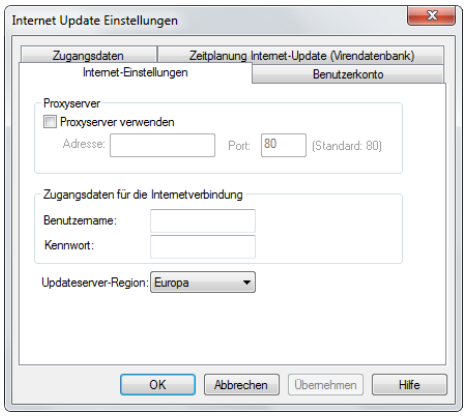


Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** z. B. bestimmen, dass Ihr Rechner nur an Werktagen das Update durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird. Um unter **Zeitpunkt** Daten- und Zeiteinträge zu ändern, markieren Sie einfach das Element, das Sie ändern möchten (z. B. Tag, Stunde, Monat, Jahr) mit der Maus und nutzen dann die Pfeiltasten oder die kleinen Pfeilsymbole rechts vom Eingabefeld, um sich im jeweiligen Element chronologisch zu bewegen.

Internet-Einstellungen

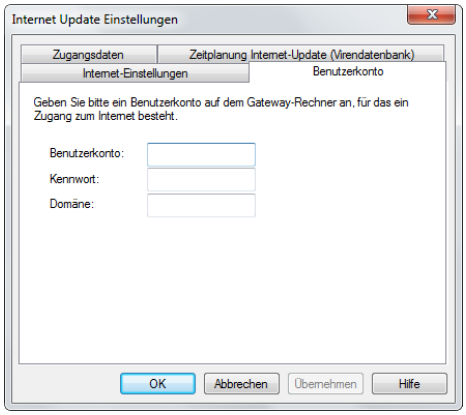
Falls Sie einen Rechner hinter einer Firewall verwenden oder andere besondere Einstellungen bezüglich Ihres Internetzugangs haben, verwenden Sie bitte einen **Proxyserver**. Sie sollten diese Einstellung nur ändern, wenn das Internet Update nicht funktioniert. Wenden Sie sich wegen der Proxy-Adresse gegebenenfalls an Ihren Internetanbieter.

Die Zugangsdaten für die Internetverbindung (Benutzername und Passwort) sind gerade beim automatischen Internet Update per Zeitplan sehr wichtig. Ohne diese Angaben kann keine automatische Verbindung mit dem Internet erfolgen. Achten Sie bitte auch darauf, dass Sie in Ihren allgemeinen Interneteinstellungen (z. B. für Ihr Mailprogramm oder Ihren Internetbrowser) die automatische Einwahl ermöglichen. Ohne die automatische Einwahl startet G DATA MailSecurity zwar den Internet Update-Vorgang, muss dann aber darauf warten, dass Sie den Aufbau der Internetverbindung mit **OK** bestätigen. Über die Auswahl unter **Updateserver-Region** können Sie einen Updateserver in Ihrer Region auswählen, um ggf. die Datenübermittlung zu optimieren.



Benutzerkonto

Geben Sie bitte unter **Benutzerkonto** ein Benutzerkonto auf dem MailGateway-Rechner an, für das ein Zugang zum Internet besteht.



Achtung: Bitte verwechseln Sie nicht die Angaben, die Sie in den Karteikarten **Zugangsdaten** und **Benutzerkonto** tätigen.

12.2.2.2. Virensignaturen

Über die Schaltflächen **Virendatenbank aktualisieren** und **Status aktualisieren** können Sie auch unabhängig von den Vorgaben, die Sie unter Zeitplanung vorgenommen haben, ein aktuelles Virensignaturupdate starten.

12.2.2.3. Programmdateien

Über die Schaltfläche **Programm-Update** können Sie auch die Programmdateien von G DATA MailSecurity aktualisieren, sobald sich hier Änderungen und Verbesserungen ergeben.

12.3. Programmbereiche

Die Bedienung von G DATA MailSecurity ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten, die Sie über die im G DATA MailSecurity Administrator angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Vorgänge überprüfen.

12.3.1. Status

Im Status-Bereich des Administrators erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und des MailGateways. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.

- Solange Ihre G DATA MailSecurity 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. veraltete Virensignaturen, abgeschaltete Virenprüfung), weist Sie ein Achtung-Symbol darauf hin.

Durch doppeltes Anklicken des jeweiligen Eintrags (oder durch Auswählen des Eintrags und das Anklicken der **Bearbeiten**-Schaltfläche) können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit einem Achtung-Symbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Ampelsymbol. Folgende Einträge stehen Ihnen zur Verfügung:

- **Verarbeitung eingehender Mail**: Die Verarbeitung eingehender E-Mails sorgt dafür, dass E-Mails vor der Weitergabe an den Empfänger durch das MailGateway überprüft werden. Mit einem Doppelklick gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Eingehend (SMTP)** und **Optionen** > **Eingehend (POP3)**) und können die Verarbeitung eingehender E-Mails an individuelle Bedürfnisse anpassen.
- **Virenprüfung eingehender Mail**: Die Prüfung eingehender E-Mails verhindert, dass infizierte E-Mails in Ihr Netz gelangen. Mit einem Doppelklick gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Virenprüfung**) und können die Prüfung eingehender E-Mails an individuelle Bedürfnisse anpassen.
- **Verarbeitung ausgehender Mail**: Die Verarbeitung ausgehender E-Mails sorgt dafür, dass E-Mails vor der Weitergabe an den Empfänger durch das MailGateway überprüft werden. Mit einem Doppelklick gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Ausgehend (SMTP)**) und können die Verarbeitung eingehender E-Mails an Ihre individuellen Bedürfnisse anpassen.
- **Virenprüfung ausgehender Mail**: Die Prüfung ausgehender E-Mails verhindert, dass aus Ihrem Netz infizierte Dateien verschickt werden. Mit einem Doppelklick gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Virenprüfung**) und können die Prüfung ausgehender E-Mails an individuelle Bedürfnisse anpassen.
- **OutbreakShield**: Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Signaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen E-Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Signaturen besteht.
- **Automatische Updates**: Die Virensignaturen können selbstständig aktualisiert werden. Sie sollten die Option für automatische Updates generell aktiviert haben. Mit einem Doppelklick gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Update**) und können die Updatefrequenz an individuelle Bedürfnisse anpassen.
- **Datum der Virensignaturen**: Je aktueller die Virensignaturen, desto sicherer ist Ihr Virenschutz. Sie sollten die Virensignaturen so oft wie möglich updaten und diesen Prozess

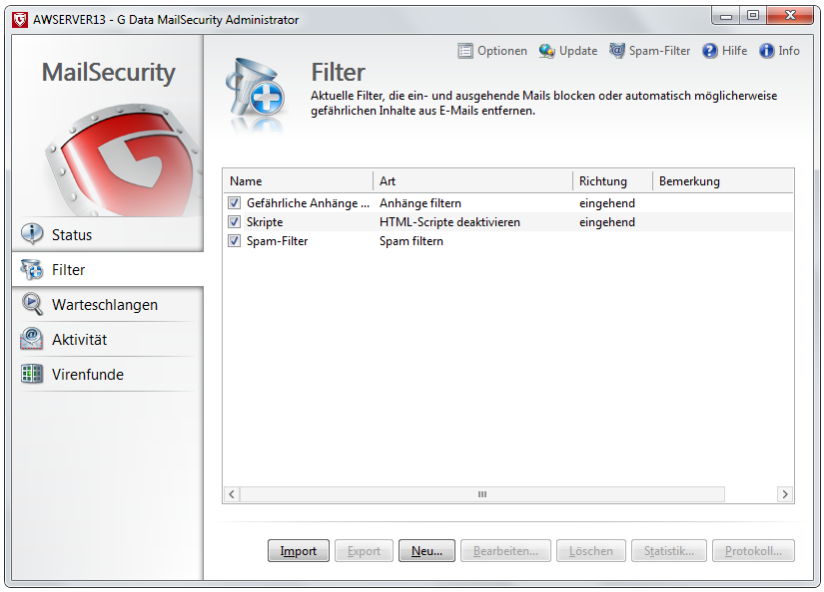
möglichst automatisieren. Mit einem Doppelklick gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Update**) und können auch direkt ein Internet Update durchführen (unabhängig von etwaigen Zeitplänen).

- **Spam-Filter**: Über den **Spam-Filter** haben Sie umfangreiche Einstellungsmöglichkeiten, um E-Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z. B. Massenmailversendern) wirkungsvoll zu blockieren.
- **Spam-OutbreakShield**: Mit dem Spam-OutbreakShield können Massenmails schnell und sicher erkannt und bekämpft werden. Das Spam-OutbreakShield erfragt dabei vor dem Abruf von E-Mails über das Internet besondere Häufungen von verdächtigen E-Mails ab und lässt diese gar nicht erst in das Postfach des Empfängers gelangen.

Wenn Sie bei der Installation die Option E-Mail-Statistik aktiviert haben, können Sie über die Schaltfläche **Statistik** Zugriff auf die statistische Auswertung Ihres Mailverkehrs bzw. Spamaufkommens nehmen. Das Konfigurieren der Statistik erfolgt dabei im **Optionen**-Menü des Administrators auf der Registerkarte **Logging**.

12.3.2. Filter

Im Filter-Bereich können Sie auf komfortable Weise Filter nutzen, die ein- und ausgehende E-Mails blocken oder automatisch möglicherweise gefährliche Inhalte aus E-Mails entfernen. Die jeweiligen Filter werden in der Liste im Filter-Bereich angezeigt und können über die Häkchenfelder links vom jeweiligen Eintrag beliebig an- bzw. abgeschaltet werden.



- **Import**: Sie können einzelne Filter mit ihren speziellen Einstellungen aus XML-Dateien importieren.
- **Export**: Sie können einzelne Filter mit ihren speziellen Einstellungen als XML-Datei speichern und ggf. erneut oder auf anderen Rechnern nutzen. Um mehrere Filter zu exportieren, wählen Sie diese bitte mit der Maus aus und halten dabei die Strg-Taste gedrückt.
- **Neu**: Über die Neu-Schaltfläche können Sie neue Filterregeln anlegen. Wenn Sie einen neuen Filter anlegen, öffnet sich ein Auswahlfenster, in dem Sie den grundlegenden Filtertyp festlegen können. Alle weiteren Angaben zum zu erstellenden Filter können Sie dann in einem dem Filtertyp angepassten Assistentenfenster angeben. Auf diese Weise erstellen Sie auf sehr komfortable Weise Filter gegen jede erdenkliche Gefährdung.
- **Bearbeiten**: Über die Bearbeiten-Schaltfläche können Sie vorhandene Filter bearbeiten.

- **Löschen**: Um einen Filter endgültig zu löschen, markieren Sie diesen bitte mit einem einfachen Mausklick und verwenden dann die Löschen-Schaltfläche.
- **Statistik**: Zu jedem Filter können Sie statistische Informationen aufrufen.
- **Protokoll**: Für den **Spam-Filter** gibt es ein Protokoll mit einer Liste, in der die als Spam eingestuften E-Mails aufgelistet sind. Dem Protokoll kann man auch entnehmen, welche Kriterien für die Einstufung als Spam verantwortlich waren (Spam-Index-Werte). Hier können Sie ggf. bei einer fälschlichen Einstufung einer E-Mail als Spam den OutbreakShield-Server online darüber informieren, dass hier eine Fehlerkennung (False Positive) vorliegt. Die E-Mail wird dann vom OutbreakShield erneut geprüft und - falls sie tatsächlich fälschlicherweise als Spam erkannt wurde - des Weiteren als unbedenklich eingestuft. Hierbei wird lediglich eine Prüfsumme übermittelt und nicht der Inhalt dieser Mail.

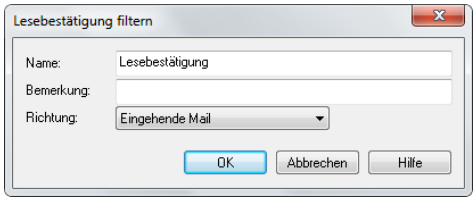
  Selbstverständlich ist Ihr Netzwerk auch unabhängig von individuellen Filterregeln vor Virenbefall geschützt, da G DATA MailSecurity ständig im Hintergrund eingehende und ausgehende E-Mails überprüft. Filterregeln dienen eher dazu, Ihre E-Mail-Accounts vor unerwünschten E-Mails, Spam und unsicheren Skripten zu bewahren und potentielle Virenherde schon vor der eigentlichen Virenerkennung durch G DATA MailSecurity zu minimieren.

Generell können Sie bei allen Filtertypen unter **Name** einen aussagekräftigen Namen für den jeweiligen Filter angeben, mit dem dieser Filter dann in der Liste des Filter-Bereichs angezeigt wird und Sie können unter **Bemerkung** interne Bemerkungen und Notizen zu dem betreffenden Filter angeben. Unter **Richtung** können Sie generell bestimmen, ob eine Filterregel nur für **Eingehende Mails**, nur für **Ausgehende Mails** oder **Beide Richtungen** gelten soll.

Im Abschnitt **Reaktion** können Sie festlegen, wie mit Mails verfahren werden soll, sobald sie die Filterkriterien erfüllen, also als Spam-Mails definiert wurden. Sie können dabei den Text für die Funktionen **Absender der Nachricht benachrichtigen** und **Meldung an folgende Personen senden** individuell gestalten. Klicken Sie dazu einfach auf die Schaltfläche rechts von der jeweiligen Reaktion. Wildcards können verwendet werden, um Informationen in den **Betreff**- und **Mailtext**-Feldern einzufügen. Hierbei handelt es sich um die gleichen Platzhalter, wie diejenigen, die unter **Eingehend (POP3)** > **Filter** verwendet werden.

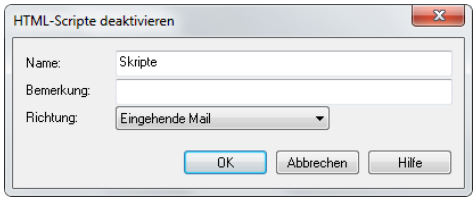
12.3.2.1. Lesebestätigung filtern

Dieser Filter löscht Lesebestätigungs-Anfragen für eingehende oder ausgehende E-Mails.



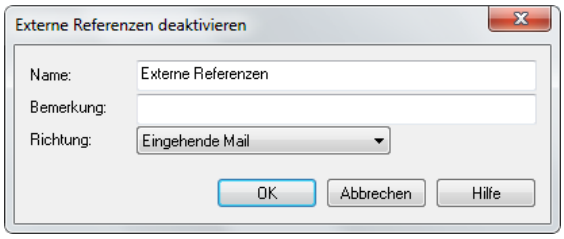
12.3.2.2. HTML-Scripte deaktivieren

Dieser Filter deaktiviert Skripte im HTML-Teil einer E-Mail. Skripte, die in einer Webseite durchaus einen Sinn haben mögen, sind - wenn sie in eine HTML-E-Mail eingebunden sind - eher störend. In manchen Fällen werden HTML-Skripte auch aktiv dazu verwendet, Rechner zu infizieren, wobei Skripte die Möglichkeit haben, sich nicht erst durch das Öffnen einer infizierten Anlage weiterzuverbreiten, sondern alleine schon in der Vorschauansicht einer E-Mail wirksam werden können.



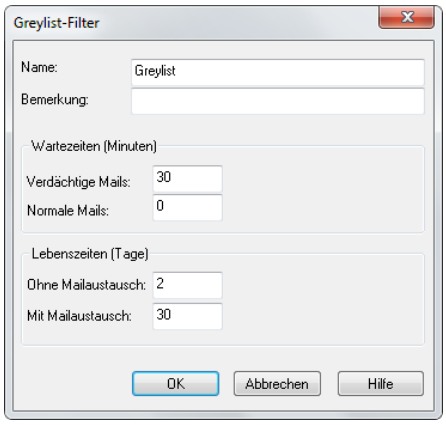
12.3.2.3. Externe Referenzen deaktivieren

Viele Newsletter und Produktinformationen im HTML-E-Mailformat beinhalten Links, die erst dann ausgeführt und angezeigt werden, wenn die E-Mail geöffnet wird. Dies können z. B. Grafiken sein, die nicht mit der E-Mail versandt wurden, sondern erst über einen Hyperlink automatisch nachgeladen werden. Da es sich hierbei nicht nur um harmlose Grafiken handeln kann, sondern durchaus auch um Schadroutinen, ist es sinnvoll, diese Referenzen zu deaktivieren. Der eigentliche E-Mail-Text ist von dieser Deaktivierung nicht betroffen.



12.3.2.4. Greylist-Filter

Greylist-Filter sind eine effektive Methode, um das Spam-Aufkommen zu reduzieren. Hierbei werden E-Mails von unbekannten Absendern nicht sofort beim ersten Zustellversuch über den SMTP-Server an den E-Mail-Empfänger übermittelt. Da Spam-Versender in der Regel keine Queue-Verwaltung nutzen und ihre E-Mails selten ein zweites Mal an denselben SMTP-Server schicken, kann die Anzahl an übermittelten Spam-Mails erheblich sinken.

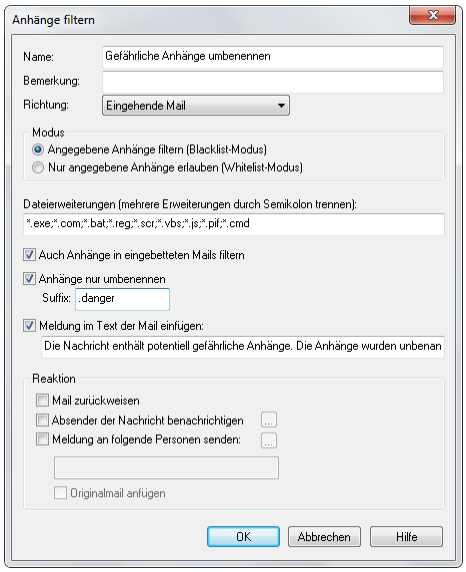


- **Wartezeiten (Minuten)**: Über diese Einstellungen können Sie festlegen, wie lange die Übermittlung verdächtiger E-Mails blockiert werden soll. Nach Ablauf dieser Zeitspanne wird die E-Mail bei einem erneuten Sendeversuch dann übermittelt. Wenn der Adressat auf diesen Absender reagiert, wird dieser aus dem Greylist-Filter herausgenommen und in eine Whitelist eingetragen. Nun wird die Zustellung dieser E-Mails nicht mehr blockiert bzw. verzögert.
- **Lebenszeiten (Tage)**: Damit die Whitelist der erwünschten Absender aktuell bleibt, verbleibt eine Absenderadresse nur eine bestimmte Zeit auf der Whitelist, bevor sie wieder auf Greylist-Status gesetzt wird. Der Timer wird für den jeweiligen Absender bei jedem neuen Mailversand wieder zurückgesetzt. Wenn Sie hier z. B. einen Wert über 30 Tage eintragen, können Sie auch erwünschte monatliche Newsletter permanent auf der Whitelist führen.

Der Greylist-Filter kann nur dann ausgewählt werden, wenn auch der **Spam-Filter** von G DATA MailSecurity aktiviert ist. Außerdem muss eine SQL-Datenbank auf dem Server installiert sein.

12.3.2.5. Anhänge filtern

Beim Filtern von Anhängen haben Sie eine große Auswahl von Möglichkeiten, um E-Mail-Anhänge (Attachments) und Anlagen zu filtern. Die meisten E-Mail-Viren verbreiten sich über solche Attachments, die in den meisten Fällen mehr oder minder gut verborgene ausführbare Dateien enthalten. Dabei kann es sich um eine klassische EXE-Datei handeln, die ein Schadprogramm enthält, aber auch um VB-Skripte, die sich unter bestimmten Voraussetzungen sogar hinter vermeintlich sicheren Grafik-, Film- oder Musikdateien verbergen. Generell sollte jeder Anwender bei der Ausführung von E-Mail-Anhängen große Vorsicht walten lassen und im Zweifelsfall lieber noch einmal eine Rückfrage beim Absender einer E-Mail durchführen, bevor er eine Datei ausführt, die er nicht ausdrücklich angefordert hat.



Unter **Dateierweiterungen** können Sie die Dateiendungen aufzählen, auf die Sie den jeweiligen Filter anwenden möchten. Dabei können Sie z. B. alle ausführbaren Dateien (z. B. EXE und COM-Dateien) in einem Filter zusammenfassen, aber auch andere Formate (z. B. MPEG, AVI, MP3, JPEG, JPG, GIF etc.) filtern, wenn diese aufgrund Ihrer Größe eine Belastung für den Mail-Server darstellen. Selbstverständlich können Sie auch beliebige Archivdateien (z. B. ZIP, RAR oder CAB) filtern. Trennen Sie bitte alle Dateierweiterungen einer Filtergruppe durch Semikolon, z. B. **.exe; *.dll*. Geben Sie unter **Modus** an, ob Sie die unter Dateierweiterungen aufgelisteten Dateiendungen erlauben möchten (**Nur angegebene Anhänge erlauben**) oder verbieten (**Angegebene Anhänge filtern**).

Über die Funktion **Auch Anhänge in eingebetteten Mails filtern** sorgen Sie dafür, dass die Filterung der unter Dateierweiterungen ausgewählten Anlagentypen auch in E-Mails stattfindet, die selber eine Anlage einer E-Mail darstellen. Diese Option sollte generell aktiviert sein. Über **Anhänge nur umbenennen** werden die zu filternden Anlagen nicht automatisch gelöscht, sondern nur umbenannt. Dies ist z. B. bei ausführbaren Dateien (wie z. B. EXE und COM) durchaus sinnvoll, aber auch bei Microsoft Office-Dateien, die möglicherweise ausführbare Skripte und Makros enthalten könnten. Durch das Umbenennen einer Anlage kann Sie nicht unbedacht durch einen einfachen Mausklick geöffnet werden, sondern muss vom Empfänger erst abgespeichert und ggf. wieder umbenannt werden, bevor er sie verwenden kann. Wenn das Häkchen bei **Anhänge nur umbenennen** nicht gesetzt ist, werden die entsprechenden Anhänge direkt gelöscht.

Unter **Suffix** geben Sie die Zeichenfolge ein, mit der Sie die eigentliche Dateiendung erweitern

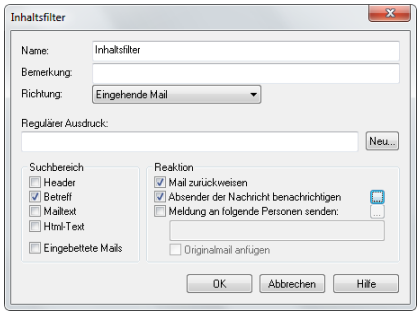
möchten, auf diese Weise wird die Ausführbarkeit einer Datei durch einfaches Anklicken verhindert (z. B. **.exe_danger*). Unter **Meldung im Text der Mail einfügen** können Sie den Empfänger der gefilterten E-Mail darüber informieren, dass ein Anhang aufgrund einer Filterregel gelöscht oder umbenannt wurde.

12.3.2.6. Inhaltsfilter

Über den Inhaltsfilter können Sie E-Mails, die bestimmte Themen oder Texte enthalten auf bequeme Weise blocken. Geben Sie dazu unter **Regulärer Ausdruck** einfach die Schlüsselwörter und Ausdrücke ein, auf die G DATA MailSecurity reagieren soll und geben Sie unter **Suchbereich** an, in welchen Bereichen einer E-Mail nach diesen Ausdrücken gesucht werden soll. Über die **Neu**-Schaltfläche rechts vom Eingabefeld für **Regulärer Ausdruck** können Sie bequem einen Text eingeben, der eine Filteraktion hervorruft. Dabei können Sie mehrere Texte auf beliebige Weise mit den logischen Operatoren UND und ODER verknüpfen.

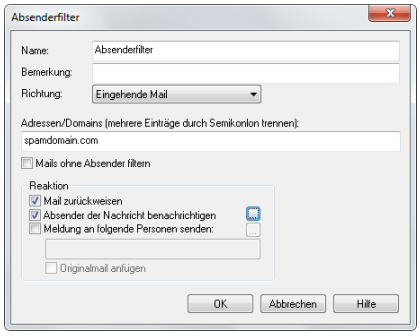
> Wenn Sie z. B. *Alkohol UND Drogen* eingeben, würde der Filter bei einer E-Mail, die z. B. die Begriffe *Alkohol* und *Drogen* enthält, aktiviert werden, nicht aber bei einer E-Mail, die nur den Begriff *Alkohol* oder nur den Begriff *Drogen* enthält. Der logische Operator UND setzt also voraus, dass alle mit UND verknüpften Elemente vorhanden sind. Der logische Operator ODER setzt lediglich voraus, dass eines der Elemente vorhanden ist.

Sie können auch ohne die Eingabehilfe unter **Regulärer Ausdruck** beliebige Suchbegriffe miteinander kombinieren. Geben Sie dazu einfach die Suchbegriffe ein und verknüpfen diese mit den logischen Operatoren. "Oder" entspricht dem Trennstrich "|" (AltGr + <). "Und" entspricht dem Kaufmanns-Und "&" (Shift + 6).



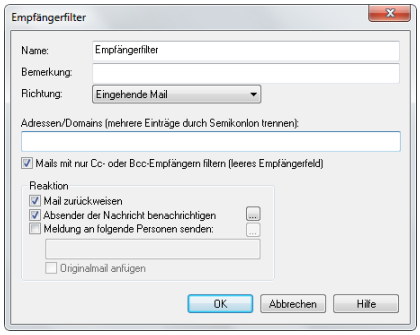
12.3.2.7. Absenderfilter

Über den Absenderfilter können Sie E-Mails, die von bestimmten Absendern kommen, auf bequeme Weise blocken. Geben Sie dazu unter **Adressen/Domains** einfach die E-Mail-Adressen oder Domain-Namen ein, auf die G DATA MailSecurity reagieren soll. Mehrere Einträge können Sie durch Semikolons voneinander trennen. Sie können auch E-Mails ohne Absenderangabe automatisch ausfiltern.



12.3.2.8. Empfängerfilter

Über den Empfängerfilter können Sie E-Mails für bestimmte Empfänger auf bequeme Weise blocken. Geben Sie dazu unter **Adressen/Domains** einfach die E-Mail-Adressen oder Domain-Namen ein, auf die G DATA MailSecurity reagieren soll. Mehrere Einträge können Sie durch Semikolon voneinander trennen. Sie können auch E-Mails mit leerem Empfängerfeld (also E-Mails, die nur Bcc- und/oder Cc-Empfänger enthalten) automatisch ausfiltern.



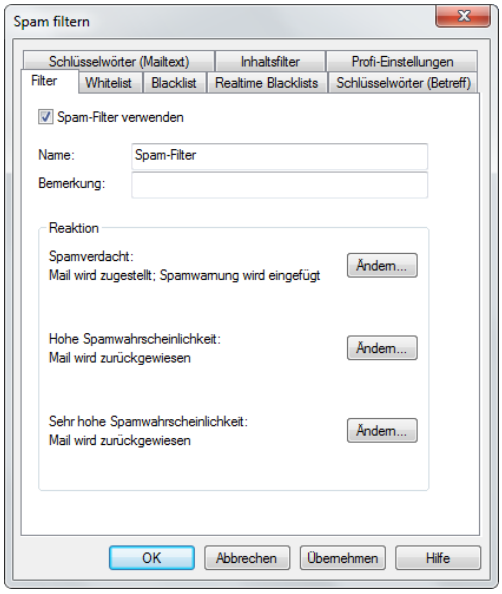
12.3.2.9. Spam filtern

Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um E-Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z. B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der E-Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Dazu stehen Ihnen mehrere Karteikarten zur Verfügung, in denen Ihnen alle relevanten Einstellungsmöglichkeiten thematisch gegliedert zur Verfügung stehen.

Filter

Geben Sie unter **Name** und **Bemerkung** an, wie Sie den Filter nennen möchten und welche zusätzlichen Informationen hierzu vielleicht nötig sind. Unter **Reaktion** können Sie bestimmen, wie der Spam-Filter mit E-Mails umgehen soll, die möglicherweise Spam enthalten. Dabei können Sie drei Abstufungen vornehmen, die davon beeinflusst werden, wie hoch G DATA MailSecurity die Wahrscheinlichkeit dafür ansetzt, dass es sich bei der betreffenden E-Mail um Spam handelt.

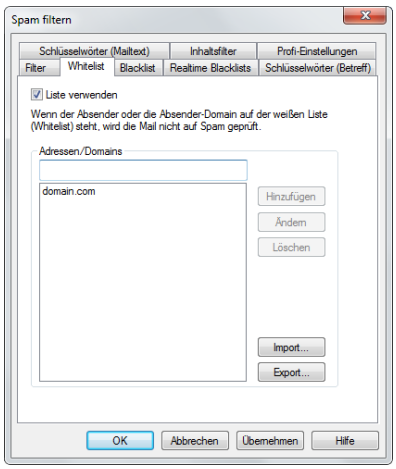
Unter **Spamverdacht** wird der Umgang mit den E-Mails geregelt, in denen G DATA MailSecurity einzelne Spam-Elemente findet. Dabei muss es sich nicht generell um Spam handeln, sondern in seltenen Fällen möglicherweise auch um Newsletter-E-Mails oder Sammelmailings, die vom Empfänger durchaus erwünscht sind. Hier empfiehlt es sich, den Empfänger auf den Spam-Verdacht hinzuweisen. Unter **Hohe Spamwahrscheinlichkeit** werden die E-Mails zusammengefasst, die viele Merkmale für Spam in sich vereinen und nur in sehr seltenen Fällen vom Empfänger wirklich erwünscht sind. Unter **Sehr hohe Spamwahrscheinlichkeit** finden sich die E-Mails, die alle Kriterien einer Spam-Mail erfüllen. Hier handelt es sich so gut wie nie um erwünschte E-Mails und das Zurückweisen von derart gestalteten E-Mails ist in den meisten Fällen empfehlenswert. Jede dieser drei abgestuften Reaktionen können Sie individuell gestalten.



So haben Sie über **Mail zurückweisen** die Möglichkeit, die E-Mail gar nicht erst auf Ihren Mail-Server gelangen zu lassen. Der Empfänger erhält diese E-Mail dann erst gar nicht. Über **Spamwarnung in Betreff und Text der Mail einfügen** können Sie einen Empfänger einer als Spam identifizierten E-Mail davon in Kenntnis setzen, dass es sich um Spam handelt. Über die Option **Absender der Nachricht benachrichtigen** können Sie eine automatische Antwort-E-Mail an den Absender der als Spam erkannten E-Mail verschicken, in der Sie diesen darauf hinweisen können, dass seine E-Mail als Spam erkannt wurde. Da gerade bei Spam viele E-Mailadressen aber nur einmal verwendet werden, sollten Sie sich überlegen, ob Sie diese Funktion aktivieren. Über die Option **An folgende Personen weiterleiten** können Sie als Spam verdächtige E-Mails auch automatisch weiterleiten, z. B. an den Systemadministrator.

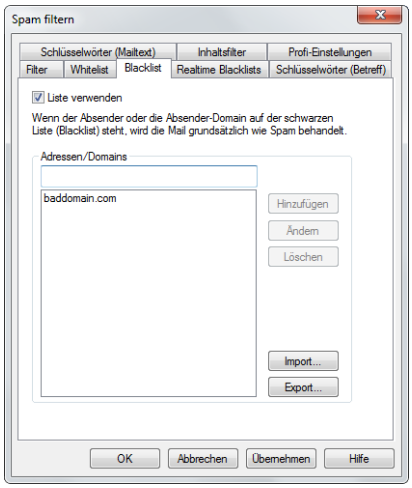
Whitelist

Über die Whitelist können Sie bestimmte Absender-Adressen oder Domains explizit vom Spamverdacht ausnehmen. Geben Sie dazu in das Feld **Adressen/Domains** die gewünschte E-Mail-Adresse (z. B. *newsletter@gdata.de*) oder Domain (z. B. *gdata.de*) ein, die Sie vom Spamverdacht ausnehmen möchten und G DATA MailSecurity behandelt E-Mails von diesem Absender bzw. dieser Absenderdomain nicht als Spam. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Whitelist einfügen. Die Adressen und Domains müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache .txt-Datei verwendet, wie sie z. B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Whitelist auch als Textdatei exportieren.



Blacklist

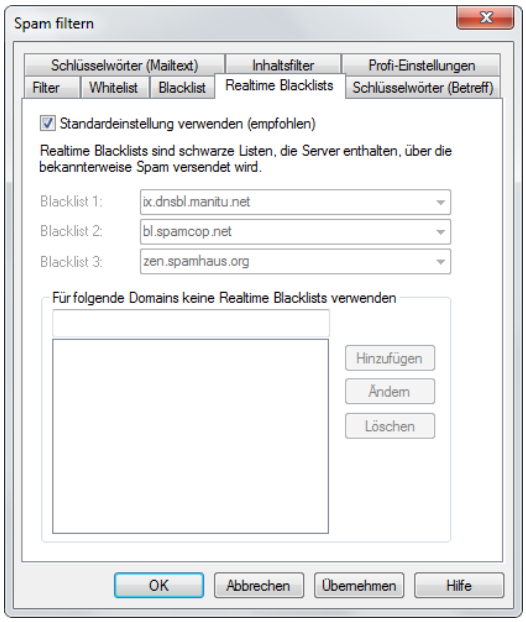
Über die Blacklist können Sie bestimmte Absender-Adressen oder Domains explizit unter Spamverdacht setzen.



Geben Sie dazu in das Feld **Adressen/Domains** die gewünschte E-Mail-Adresse (z. B. *newsletter@megaspam.de.vu*) oder Domain (z. B. *megaspam.de.vu*) ein, die Sie unter Spamverdacht setzen möchten und G DATA MailSecurity behandelt E-Mails von diesem Absender bzw. dieser Absenderdomain generell als E-Mails mit sehr hoher Spamwahrscheinlichkeit. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Blacklist einfügen. Die Adressen und Domains müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache .txt-Datei verwendet, wie sie z. B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Blacklist auch als Textdatei exportieren.

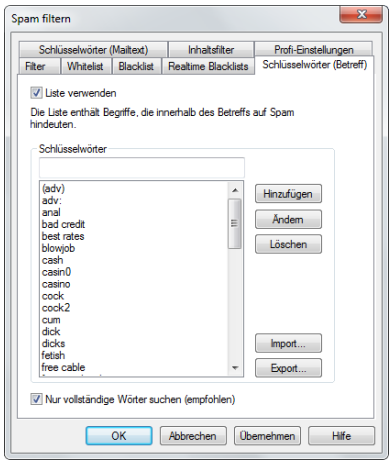
Realtime Blacklists

Im Internet finden sich schwarze Listen, die IP-Adressen von Servern enthalten, über die bekanntermaßen Spam verschickt wird. G DATA MailSecurity ermittelt durch DNS-Anfragen an die RBLs (Realtime Blacklists), ob der sendende Server gelistet ist. Falls ja, erhöht sich die Spamwahrscheinlichkeit. Generell sollten Sie hier die Standardeinstellung verwenden, können allerdings auch unter **Blacklist 1**, **2** und **3** eigene Adressen für Blacklists aus dem Internet vergeben.



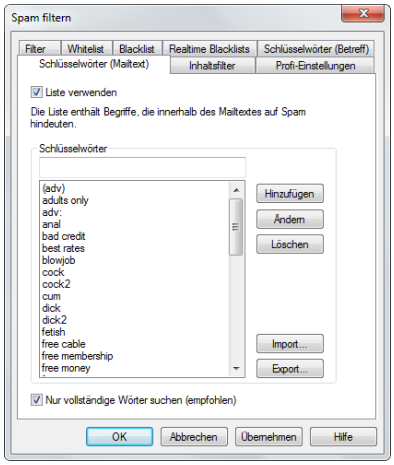
Schlüsselwörter (Betreff)

Über die Liste der Schlüsselwörter können Sie E-Mails anhand der in der Betreffzeile verwendeten Wörter unter Spamverdacht stellen. Wenn mindestens einer der Begriffe in der Betreffzeile vorkommt, erhöht sich die Spamwahrscheinlichkeit. Diese Liste können Sie über die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von Schlüsselwörtern in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache .txt-Datei verwendet, wie sie z. B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. Über das Häkchen vor **Nur vollständige Wörter suchen** können Sie festlegen, dass G DATA MailSecurity die Betreffzeile einer E-Mail nur nach ganzen Wörtern durchsucht, so würde z. B. ein Begriff wie *cash* unter Spamverdacht fallen, während z. B. die gemeinen *Cashew-Kerne*weiterhin unbeanstandet bleiben.



Schlüsselwörter (Mailtext)

Über die Liste der Schlüsselwörter können Sie E-Mails anhand der im E-Mailtext verwendeten Wörter unter Spamverdacht stellen. Wenn mindestens einer der Begriffe im E-Mailtext vorkommt, erhöht sich die Spamwahrscheinlichkeit. Diese Liste können Sie über die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern.

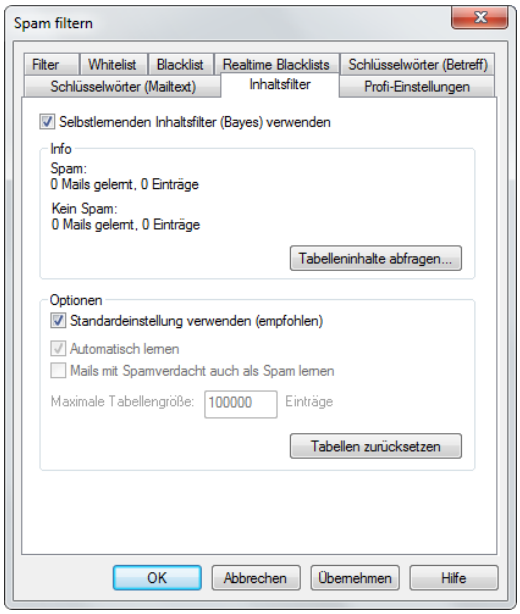


Über die **Import**-Schaltfläche können Sie vorgefertigte Listen von Schlüsselwörtern in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache .txt-Datei verwendet, wie sie z. B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. Über das Häkchen vor **Nur vollständige Wörter suchen** können Sie festlegen, dass G DATA MailSecurity die Betreffzeile einer E-Mail nur nach ganzen Wörtern durchsucht,

so würde z. B. ein Begriff wie *cash* unter Spamverdacht fallen, während z. B. die gemeinen *Cashew-Kerne* weiterhin unbeanstandet bleiben.

Inhaltsfilter

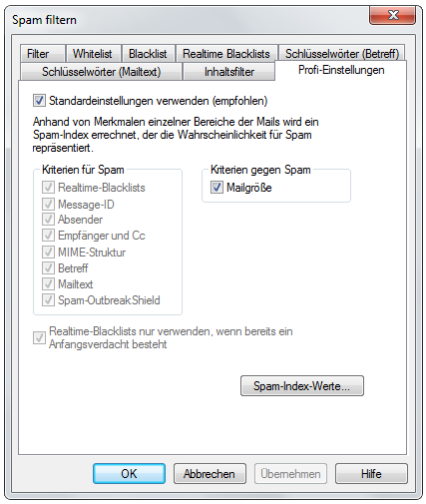
Beim Inhaltsfilter handelt es sich um einen selbstlernenden Filter auf Basis der Bayes-Methode, der auf Grund der im E-Mailtext verwendeten Worte eine Spamwahrscheinlichkeit berechnet. Dabei arbeitet dieser Filter nicht allein auf Basis feststehender Wortlisten, sondern lernt bei jeder neu empfangenen E-Mail weiter dazu. Über die Schaltfläche **Tabelleninhalte abfragen** können Sie sich die Wortlisten anzeigen lassen, die der Inhaltsfilter zur Einordnung einer E-Mail als Spam verwendet. Über die Schaltfläche **Tabellen zurücksetzen** löschen Sie alle gelernten Tabelleninhalte und der selbstlernende Inhaltsfilter startet den Lernvorgang erneut.



Profi-Einstellungen

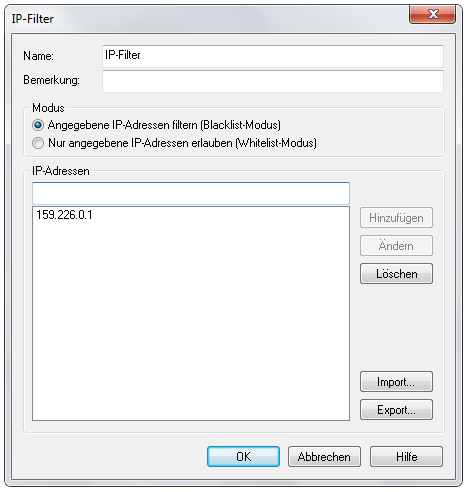
In diesem Bereich können Sie die Spamerkennung von G DATA MailSecurity sehr detailliert verändern und an die Gegebenheiten Ihres Mail-Servers anpassen. Generell empfiehlt es sich hier jedoch, die Standardeinstellungen zu verwenden. In den Profi-Einstellungen sollten Sie nur dann Veränderungen vornehmen, wenn Sie sich in der Thematik auskennen und genau wissen, was Sie tun.

Wählen Sie **Spam-Index-Werte** um die einzelnen Werte zu bearbeiten, die benutzt werden, um die Spam-Wahrscheinlichkeit von E-Mails zu klassifizieren. Wir empfehlen hier die Standardwerte.



12.3.2.10. IP-Filter

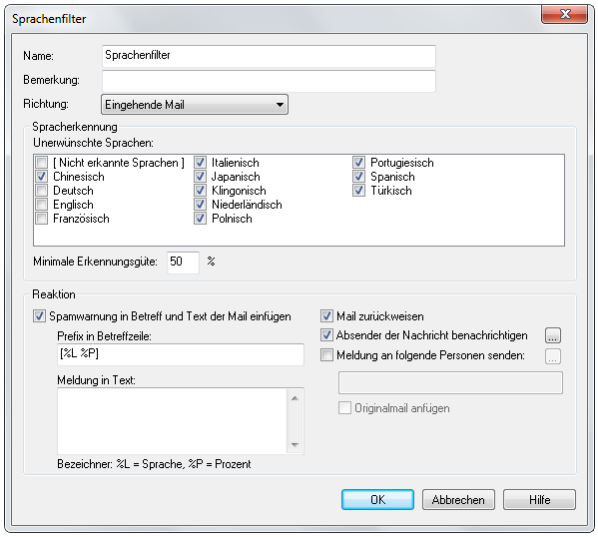
Der IP-Filter unterbindet den Empfang von E-Mails, die von bestimmten Servern abgesendet werden.



Der Filter kann sowohl im Blacklist- als auch im Whitelist-Modus verwendet werden. Geben Sie unter **Name** und **Bemerkung** Informationen dazu ein, wieso Sie die jeweiligen IP-Adressen sperren oder erlauben möchten und dann jede einzelne IP-Adresse unter **IP-Adressen** ein. Klicken Sie auf **Hinzufügen** und die aktuell eingetragene IP-Adresse wird in die Liste der gesperrten IP-Adressen übernommen. Unter Modus können Sie dabei festlegen, ob der IP-Filter im Whitelist-Modus nur bestimmte IP-Adressräume erlauben soll oder im Blacklist-Modus nur bestimmte IP-Adressräume sperren soll. Sie können die Liste der IP-Adressen auch als txt-Datei exportieren oder eine entsprechende Liste mit IP-Adressen importieren.

12.3.2.11. Sprachenfilter

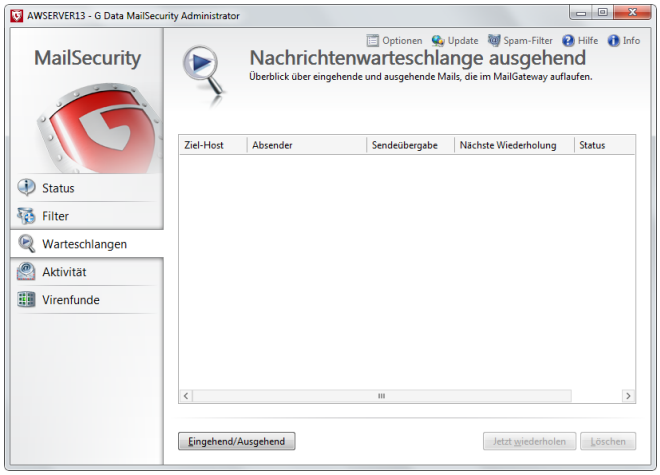
Mit dem Sprachenfilter können Sie automatisch E-Mails bestimmter Landessprachen als Spam definieren. Wenn Sie also in der Regel z. B. keinen E-Mailkontakt zu englischsprachigen Personen haben, können Sie über die Definition von Englisch als Spam-Sprache sehr viel Spam ausfiltern. Wählen Sie hier einfach die Sprachen aus, bei denen Sie davon ausgehen, dass Sie in eben diesen Sprachen keine regulären E-Mails erhalten und G DATA MailSecurity erhöht damit die Spameinschätzung für diese E-Mails erheblich.



12.3.3. Warteschlangen

Im Warteschlangen-Bereich haben Sie jederzeit Überblick über eingehende und ausgehende E-Mails, die im MailGateway auflaufen und auf Viren und/oder Content überprüft werden. Die E-Mails werden in der Regel sofort weitergeleitet, durch das MailGateway nur minimal verzögert und dann auch sofort wieder aus der Warteschlangenliste gelöscht. Sobald eine E-Mail nicht zustellbar ist oder sich Verzögerungen in der Zustellung ergeben (weil der jeweilige Server z. B. momentan nicht erreichbar ist), erfolgt in der Warteschlangenliste ein entsprechender Eintrag. G DATA MailSecurity versucht dann in einstellbaren Abständen (unter **Optionen** > **Warteschlange**) die E-Mail erneut zu verschicken.

Eine nicht erfolgte oder verzögerte E-Mailzustellung wird auf diese Weise jederzeit dokumentiert. Über die Schaltfläche **Eingehend/Ausgehend** wechseln Sie von der Listenansicht für eingehende E-Mails zur Listenansicht für ausgehende E-Mails. Über die Schaltfläche **Jetzt wiederholen** können Sie eine markierte E-Mail, die nicht zugestellt werden konnte - unabhängig von den Zeitvorgaben, die Sie für eine erneute Zustellung unter **Optionen** > **Warteschlange** definiert haben - erneut zustellen. Mit der **Löschen**-Schaltfläche entfernen Sie eine nicht zustellbare E-Mail endgültig aus der Queue.

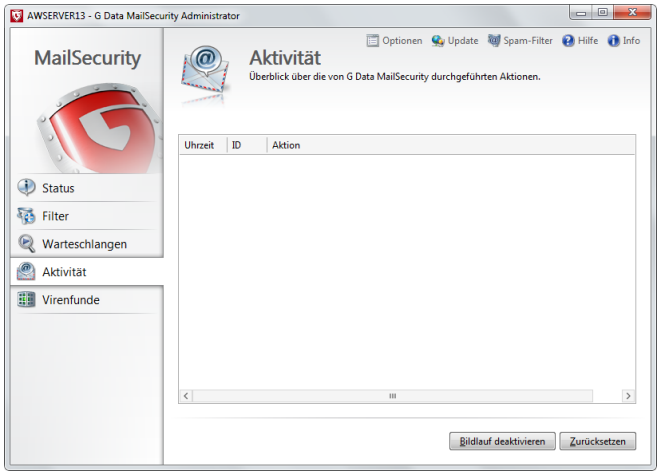


12.3.4. Aktivität

Im Aktivität-Bereich haben Sie jederzeit Überblick über die von G DATA MailSecurity durchgeführten Aktionen.

Aktionen werden mit **Uhrzeit**, **ID** und **Aktion** in der Aktivität-Liste aufgelistet. Mit dem Scroll-Balken rechts können Sie in dem Protokoll hoch- und runterscrollen. Über die **Zurücksetzen**-Schaltfläche löschen Sie das bis dahin erzeugte Protokoll und G DATA MailSecurity beginnt die Aufzeichnung der Aktivitäten erneut. Mit der Funktion **Bildlauf deaktivieren** wird die Liste weiterhin aktualisiert, aber die neuesten Aktivitäten werden nicht direkt an erster Stelle eingeblendet. Sie können dann ohne Ablenkung in der Liste scrollen.

> Über die ID können Sie die protokollierten Aktionen eindeutig einzelnen E-Mails zuordnen. So gehören Vorgänge mit gleicher ID immer zusammen (z. B. 12345 Lade E-Mail, 12345 Verarbeite E-Mail, 12345 Sende E-Mail).



12.3.5. Virenfunde

Im Virenfunde-Bereich werden sie detailliert darüber informiert, wann G DATA MailSecurity eine infizierte E-Mail ermittelt hat, welche Maßnahmen dahingehend erfolgten, um welche Art von Virus es sich handelt und wer die eigentlichen Sender und Empfänger dieser betreffenden E-Mail sind. Über **Löschen** entfernen Sie die jeweils ausgewählte Virenmeldung aus der Virenfunde-Liste.

13. FAQ

13.1. Installation

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

Der Wächter überwacht im Hintergrund alle Dateizugriffe und prüft im Zugriff befindliche 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 dies zu umgehen, deaktivieren Sie den Wächter zunächst temporär, um herauszufinden, ob die Verzögerungen durch ihn hervorgerufen werden. Wenn der betroffene Rechner auf Dateien eines Servers zugreift, muss auch der Wächter auf dem Server temporär deaktiviert werden. 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 diese Daten ermittelt werden. Wenden Sie sich hierzu ggf. an unseren **Support**.

> Selbstverständlich können Sie auch die Performance dadurch steigern, indem Sie nicht beide Engines zur Virenüberprüfung verwenden, sondern nur eine Engine. Dies bietet sich in erster Linie auf älteren Systemen an und kann im **Wächter**-Bereich eingestellt werden.

13.1.2. Ich habe die G DATA Software ohne Registrierung installiert. Wie kann ich die Software registrieren?

Um die Software nachträglich zu registrieren, öffnen Sie unter **Start** > **Alle Programme** > **G DATA** > **G DATA ManagementServer** das **Internet-Update**. Dort steht die Option **Online-Registrierung** zur Verfügung. Nach einem Klick auf diese Schaltfläche öffnet sich das Registrierungsformular. Geben Sie dort die Registriernummer ein, die der Software-Lösung beiliegt. Sie finden diese in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor.

Durch die Eingabe der Registrierungsnummer wird Ihre G DATA-Lösung aktiviert. Die erstellten Zugangsdaten werden Ihnen nach erfolgter Registrierung angezeigt. **Notieren Sie sich unbedingt diese Zugangsdaten!** Nach erfolgter Registrierung ist eine erneute Eingabe des Lizenzschlüssels nicht mehr möglich. Sollten Sie bei der Eingabe der Registriernummer Probleme haben, überprüfen Sie die Registriernummer auf die korrekte Eingabe. Je nach verwendetem Schriftsatz wird ein großes "I" (wie Ida) oft als die Ziffer "1", bzw. der Buchstabe "l" (wie Ludwig) fehlinterpretiert. Das Gleiche gilt für: "B" und "8", "G" und 6, "Z" und "2".

> Sollten Sie eine G DATA Client Security Business, eine G DATA Endpoint Protection Business oder als Zusatzmodul einen G DATA PatchManager erworben und bei der Installation nicht aktiviert haben, werden die Karteireiter Firewall, PatchManager und PolicyManager erst nach einer erfolgreichen Aktivierung freigeschaltet. Bis dahin stehen nur die Funktionen von G DATA AntiVirus Business zur Verfügung.

13.1.3. MailSecurity für Exchange

13.1.3.1. MailSecurity und Exchange Server 2007

Wenn Sie die MailSecurity für Exchange auf einem Microsoft Exchange Server 2007 aktualisieren, muss das Microsoft .NET Framework 3.5 oder höher vorhanden sein. Wenn Microsoft .NET Framework 3.5 oder höher nicht vorhanden ist, wird der Dienst GDVSService nach dem Upgrade nicht starten

können. Installieren Sie deswegen das Microsoft .NET Framework 3.5 oder höher, bevor Sie die MailSecurity für Exchange aktualisieren.

13.1.3.2. Aktualisierung der Version 12

Auf Grund von Änderungen im Installationsvorgang kann die Version 12 des Exchange-Plugins nicht auf die Version 14 aktualisiert werden, selbst wenn es vorher bereits auf die Version 13.0 oder 13.1 aktualisiert wurde. In diesem Fall müssen Sie die MailSecurity für Exchange deinstallieren, bevor Sie die Version 14 installieren. Dabei sollten Sie sicherstellen, dass das Plugin auf allen Exchange-Servern, die die Mailbox- oder Hub Transport-Rolle ausführen, installiert wird.

13.1.3.3. MailSecurity, Exchange Server 2000 und AVM Ken!

Wenn Sie AVM Ken! nutzen und die G DATA MailSecurity auf demselben Computer wie den Ken!-server installieren möchten, wenden Sie sich bitte für detaillierte Informationen an unser **Support-Team**.

Wenn Sie den Exchange Server 2000 nutzen und die G DATA MailSecurity auf demselben Computer wie den Exchange Server installieren möchten oder wenn Sie die Ports für ein- und ausgehende E-Mails auf dem Exchange Server ändern möchten, wenden Sie sich bitte für detaillierte Informationen an unser **Support-Team**.

13.1.3.4. Installation in einem Netzwerk mit mehreren Domain-Controllern

Wenn Sie die MailSecurity für Exchange in einem Netzwerk, in dem sich mehrere Domain-Controller befinden, installieren möchten, muss das Tool Repadmin.exe auf dem Rechner vorhanden sein. Repadmin.exe ist als Teil der Rollen Active Directory Domain Services und Active Directory Lightweight Directory Services sowie als Teil der Active Directory Domain Services Tools (Remote Server Administration Tools) verfügbar. Stellen Sie sicher, dass mindestens eine dieser Komponenten vorhanden ist, bevor Sie die Installation der MailSecurity für Exchange starten.

13.2. Fehlermeldungen

13.2.1. Client: "Programmdateien wurden verändert oder sind beschädigt"

Um einen optimalen Virenschutz zu gewährleisten, werden die Programmdateien regelmäßig auf Ihre Integrität 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 unseren **Support**, wenn der Fehlerbericht erneut eingefügt wird.

13.2.2. Client: "Die Virendatenbank ist beschädigt."

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 unseren **Support**, wenn der Fehlerbericht erneut eingefügt wird.

13.2.3. "Sie benötigen mindestens Microsoft Exchange Server 2007 SP1"

Sollten Sie die Fehlermeldung "Sie benötigen mindestens Microsoft Exchange Server 2007 SP1" erhalten, sind die Mindestvoraussetzungen für die Installation des G DATA MailSecurity Exchange-

Plugins nicht erfüllt. Für eine Installation wird mindestens Microsoft Exchange 2007 mit Service Pack 1 benötigt. Dieser muss vor der G DATA MailSecurity installiert werden. Siehe hierzu auch **Installation** und **Systemvoraussetzungen**.

13.3. Linux

13.3.1. Installation

Der Installationsvorgang des G DATA Security Clients für Linux/Mac verwendet ein ManagementServer-basiertes Repository. Wenn Sie einen Linux- oder Mac-Client installieren, werden die jeweiligen ausführbaren Dateien vom ManagementServer-Repository zum Client kopiert. Wenn die Dateien noch nicht im Repository verfügbar sind, werden sie zuerst von den G DATA Update-Servern heruntergeladen, dann dem Repository hinzugefügt und unmittelbar danach zum Client kopiert.

13.3.2. Hintergrundprozesse

Zum Prüfen der beiden Prozesse des G DATA Security Clients für Linux geben Sie im Terminal das folgende Kommando ein:

linux:~# *ps ax|grep av*

Sie sollten die folgenden Ausgaben erhalten:

/usr/local/sbin/gdavserver
/usr/local/sbin/gdavclientd

Sie können die Prozesse mit den folgenden Kommandos starten:

linux:~# */etc/init.d/gdavserver start*
linux:~# */etc/init.d/gdavclient start*

Sie können die Prozesse mit den folgenden Kommandos anhalten:

linux:~# */etc/init.d/gdavserver stop*
linux:~# */etc/init.d/gdavclient stop*

Hierzu müssen Sie die Root-Rechte haben.

13.3.3. Protokolle

Die Remote-Installation des G DATA Security Clients für Linux wird in der Datei /var/log/gdata_install.log protokolliert. Der gdavclientd-Prozess protokolliert Informationen und Fehler in /var/log/gdata/avclient.log. Der gdavserver-Prozess protokolliert Informationen und Fehler in /var/log/gdata/gdavserver.log. Diese Datei kann beim Troubleshooting der Verbindung mit G DATA ManagementServer hilfreich sein.

> 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 (Fügen Sie die Einträge hinzu, wenn es sie noch nicht gibt). Vorsicht: Hohe LogLevel erzeugen viele Meldungen und lassen die Log-Dateien schnell anwachsen. Setzen Sie die LogLevel im Normalbetrieb immer auf niedrige Werte.

13.3.4. Scan-Server-Test

Mit **gdavclientc** können Sie prüfen, ob der Scan-Server-Dienst gdavserver läuft. Sie können Versionsinformationen mit den Kommandos *baseinfo* und *coreinfo* anfordern. Starten Sie einen Test-Scan mit dem Kommando *scan:<Pfad>*. Mehr Informationen finden Sie in dem Kapitel **gdavclientc**.

13.3.5. Verbindung mit G DATA ManagementServer

Die Kommunikation mit G DATA ManagementServer wird unter /etc/gdata/avclient.cfg konfiguriert. Kontrollieren Sie, ob die IP-Adresse des ManagementServers korrekt eingetragen ist. Falls nicht, löschen Sie den falschen Eintrag und tragen Sie die Adresse des G DATA ManagementServers direkt ein oder melden Sie den Linux-Client über den G DATA Administrator erneut an.

13.4. Sonstiges

13.4.1. Wie kann ich überprüfen, ob die Clients eine Verbindung zum G DATA ManagementServer haben?

Die Spalte **Letzter Zugriff** im Aufgabenbereich **Clients** enthält den Zeitpunkt, an dem sich der Client zum letzten Mal beim G DATA ManagementServer gemeldet hat. In der Standardeinstellung melden sich die Clients alle fünf Minuten beim G DATA ManagementServer (wenn gerade keine Scanaufträge ausgeführt werden). Folgende Ursachen können für eine fehlgeschlagene Verbindung verantwortlich sein:

- Der Client ist ausgeschaltet oder vom Netzwerk getrennt.
- Es kann keine TCP/IP-Verbindung zwischen dem Client und dem G DATA ManagementServer aufgebaut werden. Prüfen Sie die Netzwerkeinstellungen bzw. Portfreigaben.
- Der Client kann die IP-Adresse des Servers nicht ermitteln, d.h. die DNS Namensauflösung funktioniert nicht. Die Verbindung kann mit dem Befehl **telnet** über die Eingabeaufforderung überprüft werden. Am Server muss der TCP-Port 7161 erreichbar sein, am Client muss der TCP-Port 7167 bzw. 7169 erreichbar sein. Prüfen Sie die Verbindung mit dem Befehl *telnet <SERVERNAME> <PORTNUMMER>*

  Beachten Sie, dass unter Windows Vista, Windows 7 sowie Server 2008 (R2) der telnet-Befehl standardmäßig nicht verfügbar ist. Aktivieren Sie daher die entsprechende Windows-Funktion bzw. fügen Sie sie als neues Feature zum Server hinzu. Ist die Verbindung vom Client zum Server intakt, erscheint in der Eingabeaufforderung eine Sammlung kryptischer Zeichen. Wenn die Verbindung vom Server zum Client intakt ist, erscheint ein leeres Eingabefenster.

13.4.2. Mein Postfach wurde in die Quarantäne geschoben

Dies passiert, wenn sich in dem Postfach eine infizierte E-Mail befindet. Zurückbewegen der Datei: Schließen Sie das Mailprogramm auf dem betroffenen Client und löschen Sie eine evt. neu angelegte Archivdatei. Öffnen Sie anschließend im G DATA Administrator den zugehörigen Bericht und klicken Sie auf **Quarantäne: Zurückbewegen**. Kontaktieren Sie bitte unseren **Support**, wenn das Zurückbewegen fehlschlägt.

13.4.3. Mit dem ManagementServer über IP verbinden

Bei der Installation wird nach dem Servernamen gefragt. Der Name kann durch die IP-Adresse ersetzt werden, wenn Sie sich statt mit dem Namen, über die IP-Adresse mit dem ManagementServer verbinden möchten. Sie können den Servernamen auch nachträglich durch die IP-Adresse ersetzen, wenn der G DATA ManagementServer bereits installiert ist. Öffnen Sie hierzu die Datei Config.xml

(befindet sich im Installationsordner des G DATA ManagementServers) und ändern Sie den Wert der Einstellung *MainMms* auf die IP-Adresse. Mehr Informationen zum Thema Config.xml finden Sie in dem Reference Guide.

Damit die Verbindung vom Server zu den Clients auch über die IP-Adresse hergestellt werden kann, müssen die Clients im G DATA Administrator mit Ihrer IP-Adresse aktiviert werden. Das geht entweder von Hand oder durch **Active Directory Synchronization**. Wenn die Clients direkt von dem Installationsmedium installiert werden, fragt das Installationsprogramm sowohl nach dem Servernamen als auch nach dem Computernamen. Geben Sie hier jeweils die IP-Adresse ein.

13.4.4. Standardspeicherorte und Pfade

Virensignaturen G DATA Security Client

- Windows XP/Server 2003/Server 2003 R2: C:\Programme\Gemeinsame Dateien\G DATA \AVKScanP\BD bzw. G DATA
- Windows Vista/Server 2008 und neuer: C:\Programme (x86)\Common Files\G DATA\AVKScanP \BD bzw. G DATA

Virensignaturen G DATA ManagementServer

- Windows Server 2003/Server 2003 R2: C:\Dokumente und Einstellungen\All Users \Anwendungsdaten\G DATA\AntiVirus ManagementServer\Updates
- Windows Vista/Server 2008 und neuer: C:\ProgramData\G DATA\AntiVirus ManagementServer \Updates

G DATA Security Client-Quarantäne

- Windows XP/Server 2003/Server 2003 R2: C:\Dokumente und Einstellungen\All Users \Anwendungsdaten\G DATA\AntiVirusKit Client\Quarantine
- Windows Vista/Server 2008 und neuer: C:\ProgramData\G DATA\AntiVirusKit Client\Quarantine

G DATA ManagementServer-Quarantäne

- Windows Server 2003/Server 2003 R2: C:\Dokumente und Einstellungen\All Users \Anwendungsdaten\G DATA\AntiVirus ManagementServer\Quarantine
- Windows Vista/Server 2008 und neuer: C:\ProgramData\G DATA\AntiVirus ManagementServer \Quarantine

G DATA ManagementServer-Datenbanken

Windows Vista/Server 2003 und neuer:

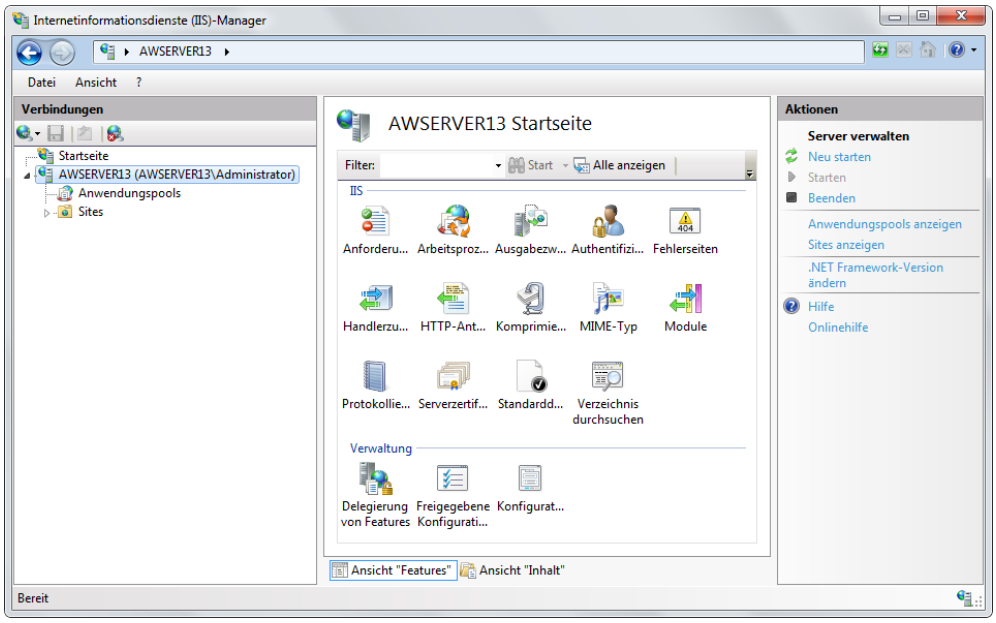
- C:\Programme (x86)\Microsoft SQL Server\MSSQL12.GDATA2014\MSSQL\Data \GDATA_AntiVirus_ManagementServer_*.mdf
- C:\Programme (x86)\Microsoft SQL Server\MSSQL12.GDATA2014\MSSQL\Data \GDATA_AntiVirus_ManagementServer_log_*.ldf

13.4.5. Wie aktiviere ich ein SSL-Server-Zertifikat in IIS 7 und neuer?

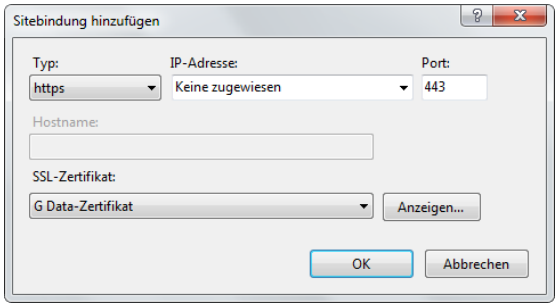
Um eine sichere Kommunikation zwischen Clients und WebAdministrator / MobileAdministrator zu erleichtern, empfiehlt es sich, ein SSL-Server-Zertifikat in Internet Information Services (IIS) zu ermöglichen.

Um ein SSL-Server-Zertifikat in IIS 7 oder neuer zu aktivieren, öffnen Sie bitte

Internetinformationsdienste (IIS)-Manager. Wenn Sie Windows Server 2008 nutzen, können Sie den IIS Manager unter **Start** > **Alle Programme** > **Verwaltung** finden. Alternativ klicken Sie auf **Start** > **Ausführen** und geben Sie das Kommando **inetmgr** ein.



Wählen Sie Ihren Server unter **Verbindungen** aus. Wählen Sie dann die **IIS** Kategorie aus und doppelklicken auf **Serverzertifikate**. Klicken Sie nun auf **Selbstsigniertes Zertifikat erstellen**. Nach der Eingabe eines Namens für das Zertifikat wird dieses erzeugt und in der Serverzertifikat-Übersicht angezeigt. Bitte beachten Sie, dass das Standard-Ablaufdatum für das Zertifikat tagesgenau ein Jahr beträgt.

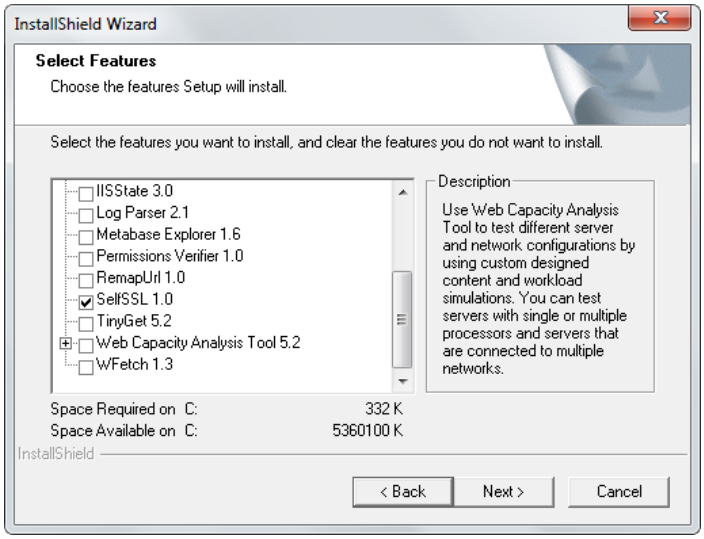


Um das Zertifkat für die Kommunikation zu verwenden wählen Sie die entsprechende Seite im Bereich **Verbindungen** aus. Im Bereich **Aktionen** auf der rechten Seite können Sie nun **Bindungen** auswählen. Klicken Sie nun auf **Hinzufügen**, um eine neue Bindung zu etablieren. Als **Typ** wählen Sie bitte **https** im DropDown-Menü aus und unter **SSL-Zertifikat** das Zertifikat, welches Sie zuvor definiert haben. Klicken Sie auf **OK**, um die Bindung zu bestätigen.

Der Zugriff auf den WebAdministrator und den MobileAdministrator über eine sichere Verbindung ist nun dadurch möglich, dass Sie das Präfix *http://* in Ihrem Browser durch *https://* ersetzen, z. B. *https://servername/gdadmin*. Da Sie Ihr Zertifikat selber erstellt haben, kann es sein, dass der Browser hier eine Warnung ausgibt, bevor er Ihnen erlaubt, den WebAdministrator oder MobileAdministrator zu öffnen. Trotzdem ist die Kommunikation mit dem Server vollständig verschlüsselt.

13.4.6. Wie aktiviere ich ein SSL-Server-Zertifikat in IIS 5 oder 6?

Um eine sichere Kommunikation zwischen Clients und WebAdministrator / MobileAdministrator zu erleichtern, empfiehlt es sich, ein SSL-Server-Zertifikat in Internet Information Services (IIS) zu ermöglichen.



Um ein SSL-Server-Zertifikat in IIS 5 (Windows XP) oder IIS 6 (Windows Server 2003) zu aktivieren, verwenden Sie bitte das Microsoft-Tool SelfSSL, welches Sie bei den IIS 6.0 Resource Kit Tools (ein kostenloser Download von der **Microsoft-Internetseite**) finden. Wenn Sie hier den Setup-Typ **Custom** durchführen, können Sie die Tools auswählen, die Sie installieren möchten. Wählen Sie hier bitte **SelfSSL 1.0** aus. Nach der Installation öffnen Sie die SelfSSL Kommandozeile über **Start** > **Programme** > **IIS Resources** > **SelfSSL**.

Mit Hilfe einer einzigen Eingabe können Sie nun ein selbst signiertes Zertifikat für Ihre Webseite erzeugen. Geben Sie bitte *selfssl /N:CN=localhost /K:2048 /V:365 /S:1 /T* ein und drücken Sie dann **Enter**. Bestätigen Sie die Erzeugung des Zertifikats durch Drücken der **Y**-Taste. Nun wird ein Zertifikat für die Standard-IIS Seite auf Ihrem lokalen Server erzeugt und der localhost wird auf die Liste der vertrauenswürdigen Zertifikate hinzugefügt. Die Schlüssellänge beträgt 2048 Zeichen und ist für genau 365 Tage gültig. Wenn Ihre Seite nicht die Standard-ISS Seite auf Ihrem lokalen Server ist, können Sie unter **Start** > **Programme** > **Verwaltung** > **Internetinformationsdienste (IIS)-Manager** die entsprechende Seite auf Ihrem Server ermitteln und den Parameter */S:1* entsprechend modifizieren.

Der Zugriff auf den WebAdministrator und den MobileAdministrator über eine sichere Verbindung ist nun dadurch möglich, dass Sie das Präfix *http://* in Ihrem Browser durch *https://* ersetzen, z. B. *https://servername/gdadmin*. Da Sie Ihr Zertifikat selber erstellt haben, kann es sein, dass der Browser hier eine Warnung ausgibt, bevor er Ihnen erlaubt, den WebAdministrator oder MobileAdministrator zu öffnen. Trotzdem ist die Kommunikation mit dem Server vollständig verschlüsselt.

14. Lizenzen

SharpSerializer

SharpSerializer is distributed under the New BSD License (BSD). Copyright © 2011, Pawel Idzikowski. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Polenter - Software Solutions nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Json.NET

Json.NET is distributed under The MIT License (MIT). Copyright © 2007 James Newton-King.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DotNetZip

DotNetZip is distributed under the Microsoft Public License (Ms-PL).

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

PhoneNumbers.dll / PushSharp

PhoneNumbers.dll and PushSharp are distributed under the Apache License 2.0 (www.apache.org/licenses).

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Index