
GFI MailSecurity for Exchange/SMTP 10

Handbuch

GFI Software Ltd.



<http://www.gfisoftware.de>
E-Mail: info@gfisoftware.de

Dieses Handbuch wurde von GFI Software Ltd verfasst und produziert. Die Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden. In den Beispielen verwendete Firmen, Namen und Daten sind, wenn nicht anders angegeben, rein fiktiv. Ohne vorherige ausdrückliche und schriftliche Zustimmung von GFI Software Ltd. darf das Dokument weder ganz noch teilweise in irgendeiner Form, sei es elektronisch oder mechanisch, oder zu irgendeinem Zweck reproduziert bzw. übertragen werden.

GFI MailSecurity wurde von GFI Software Ltd. entwickelt. GFI MailSecurity ist von GFI Software Ltd. urheberrechtlich geschützt. © 2000-2006 GFI Software Ltd. Alle Rechte vorbehalten.

GFI MailSecurity ist eine eingetragene Marke; GFI Software Ltd. und das GFI-Logo sind Marken von GFI Software Ltd. in Europa, den USA und anderen Ländern.

Version 10.0 – Letzte Aktualisierung: 28. Juni 2006

Inhaltsverzeichnis

GFI MailSecurity im Überblick	1
Einleitung	1
Hauptfunktionen von GFI MailSecurity	1
Komponenten von GFI MailSecurity	3
GFI MailSecurity aus Sicht des Anwenders.....	3
Erweitertes E-Mail-Management – GFI MailEssentials	4
Installieren von GFI MailSecurity	5
Einführung.....	5
Auswählen des Installationsmodus.....	9
Systemanforderungen.....	10
Hardware-Anforderungen	10
Vorbereiten der Installation auf einem Mail-Relay-Server	10
Vorbereitungen vor der Installation auf einem E-Mail-Server	19
Installieren von GFI MailSecurity	19
Hinzufügen von GFI MailSecurity zur DEP-Exception-List von Windows XP.....	22
Sichern des Zugriffs auf die Konfigurations-/Quarantäneseiten	23
Sichern des Zugriffs auf RSS-Feeds des Quarantänebereichs.....	28
Zugreifen auf die Konfigurationsseiten und den Quarantänebereich	30
Eingeben des Registrierschlüssels nach der Installation.....	32
Umstieg von GFI MailSecurity Version 8 auf Version 10.....	33
Hinweise zum Umstieg von GFI MailSecurity Version 9 auf 10	35
Allgemeine Einstellungen	37
Einführung.....	37
Angaben der E-Mail-Adresse des Administrators.....	37
Auswählen des Update-Servers	37
Hinzufügen lokaler Domänen.....	39
Bindungen an SMTP-Server	40
Verwalten lokaler Anwender im SMTP-Modus	41
Konfigurieren der Virenprüfung	43
Konfigurieren der Viren-Scan-Engines	43
Konfigurieren der GRISOFT AVG-Engine	44
Konfigurieren der Kaspersky-Engine	46
Konfigurieren der BitDefender-Engine	47
Konfigurieren der McAfee-Engine.....	48
Konfigurieren der Norman-Engine	49
Vorgehensweise bei Virenbefall.....	51
Updates für den Viren-Scanner	52
Festlegen der Scan-Priorität der einzelnen Viren-Scan-Engines	53
Optimieren von Viren-Scan-Aktionen.....	54
Konfigurieren von Informationsspeicher-Scans	54
Konfigurieren der Anhangskontrolle	57
Einführung.....	57

Erstellen einer Regel zur Anhangskontrolle.....	57
Entfernen einer Regel zur Anhangskontrolle	62
Ändern einer Regel zur Anhangskontrolle	63
Aktivieren/Deaktivieren einer Regel zur Anhangskontrolle.....	63
Ändern der Regel-Priorität	63
Konfigurieren der Inhaltskontrolle	65
Einführung.....	65
Erstellen einer Regel zur Inhaltskontrolle	65
Entfernen einer Regel zur Inhaltskontrolle.....	72
Ändern einer Regel zur Inhaltskontrolle.....	72
Aktivieren/Deaktivieren einer Regel.....	72
Ändern der Regel-Priorität	73
Die Dekomprimierungs-Engine	75
Einführung.....	75
Konfigurieren der Filter der Dekomprimierungs-Engine	76
Konfigurieren von Aktionen der Dekomprimierungsfilter	80
Aktivieren/Deaktivieren von Dekomprimierungsfiltern	81
Der Trojan & Executable Scanner	83
Einführung.....	83
Konfigurieren des Trojan & Executable Scanner.....	84
Aktualisieren des Trojan & Executable Scanner.....	86
Die Email Exploit Engine	89
Einführung.....	89
Konfigurieren der Email Exploit Engine	90
Aktualisieren der Email Exploit Engine	92
Der HTML Sanitizer	95
Einführung.....	95
Konfigurieren des HTML Sanitizer	95
Überprüfen auf Produkt-Patches	97
Einführung.....	97
Downloaden und Installieren von Software-Patches	97
Die E-Mail-Quarantäne	99
Einführung.....	99
Suchen nach E-Mails im Quarantänebereich	101
Einordnen von Quarantäne-Mails in Suchordnern.....	102
Ändern der Eigenschaften von Suchordnern.....	106
Löschen von Suchordnern	106
Freigeben von E-Mails im Quarantänebereich	107
Löschen von E-Mails im Quarantänebereich.....	108
Erneute Sicherheitsüberprüfung von E-Mails im Quarantänebereich	108
Freigeben von E-Mails per HTML-Freigabeformular	109
Freigeben oder Löschen von Quarantäne-Mails per E-Mail-Client	110
Versand von Informationen zu Quarantäne-E-Mails an Anwender	111
Aktivieren von RSS-Feeds zum Quarantänebereich	111
Aktivieren des Directory Harvesting-Filters für Quarantäne-Mails.....	114
Die Berichterstellung	117
Einführung.....	117

Konfigurieren der statistischen Datenbank	117
Der Echtzeit-Monitor	123
Einführung.....	123
Überwachen der E-Mail-Verarbeitung.....	123
Ergänzende Optionen	125
Versionsinformationen	125
Zusätzliche urheberrechtliche Informationen.....	125
Weitere Konfigurationsoptionen	127
Anpassen der Benachrichtigungsvorlagen	127
Troubleshooting	131
Einführung.....	131
Wissensdatenbank.....	131
Support-Anfrage per E-Mail	131
Support-Anfrage per Web-Chat	132
Support-Anfrage per Telefon	132
Web-Forum	132
Mitteilungen zu neuen Builds	132

GFI MailSecurity im Überblick

Einleitung

Aufgrund des stetig wachsenden E-Mail-Traffics und der damit verbundenen Gefahren ist es notwendiger denn je, elektronische Post auf sicherheitsgefährdende, anzügliche oder vertrauliche Inhalte zu überprüfen. Zerstörerische Viren, die E-Mail-Systeme und Firmen-Netzwerke binnen Minuten zusammenbrechen lassen, werden weltweit innerhalb nur weniger Stunden per E-Mail verbreitet (z. B. der MyDoom-Wurm). Sicherheitsprodukte, die zur Absicherung nur eine einzige Anti-Viren-Engine einsetzen, gewährleisten keinen zuverlässigen Schutz. Eine weitaus größere Bedrohung stellen jedoch Backdoor-Viren (Trojaner) und andere gefährliche Programme dar, die mit Hilfe von E-Mails eingeschleust werden, um Hackern einen Zugang zum Netzwerk zu verschaffen. Reine Anti-Viren-Produkte bieten keinen ausreichenden Schutz vor E-Mail-Exploits und ähnlichen Angriffen.

Nur durch den Einsatz einer umfassenden Anti-Viren-Lösung mit Inhalts- und Anhangskontrolle für E-Mails können E-Mail-Server und Netzwerke zuverlässig gesichert werden. GFI MailSecurity übernimmt die Rolle einer „E-Mail-Firewall“, um Viren, Exploits und ähnliche E-Mail-basierte Bedrohungen sowie gezielt gegen ein Unternehmen gerichtete E-Mail-Angriffe abzuwehren.

Das Produkt führt seine Kontrollen unbemerkt im Hintergrund durch und erfordert keine zusätzlichen Anwenderschulungen.

Hauptfunktionen von GFI MailSecurity

Virenkontrolle mit mehreren Anti-Viren-Engines

GFI MailSecurity setzt zum Schutz vor digitalen Schädlingen mehrere Anti-Viren-Engines ein. Das Scannen von E-Mails am Gateway und auf Ebene des E-Mail-Servers verhindert, dass Viren ins Netzwerk eindringen können und/oder sich darin verbreiten. Außerdem verhindert die Sicherheitssoftware, dass infizierte E-Mails verschickt werden, da auch für alle ausgehenden Nachrichten eine Virenüberprüfung stattfindet. Im Lieferumfang von GFI MailSecurity sind standardmäßig die leistungsfähigen und bereits mehrfach ausgezeichneten Anti-Viren-Engines von Norman und BitDefender enthalten. Optional können die Anti-Viren-Engines von McAfee, Kaspersky und GRISOFT hinzugefügt werden. Der Einsatz gleich mehrerer Anti-Viren-Engines bietet einen noch höheren Schutz, da sich die Lösungen ergänzen und Viren schneller erkannt und abgewehrt werden. GFI MailSecurity unterstützt zudem automatische Viren-Updates. Die Engines lassen

sich so konfigurieren, dass aktuelle Updates ohne Administrator-Eingriff gesucht und ggf. heruntergeladen werden.

Prüfen und Filtern von E-Mail-Anhängen

GFI MailSecurity überprüft, ob empfangene und zu verschickende E-Mails schädliche Elemente enthalten. E-Mails mit gefährlichen Anhängen können unter Quarantäne gestellt werden, z. B. Dateien der Formate *.exe und *.vbs. Bei Anhängen dieser Art besteht die erhöhte Gefahr, dass sie einen Virus, Wurm oder ähnliche E-Mail-basierte Schadteile enthalten. Da sich E-Mail-Viren sehr schnell verbreiten und Schäden in beträchtlicher Höhe verursachen können, sollten Nachrichten dieser Art vor der Weiterleitung an den Empfänger unter Quarantäne gestellt und überprüft werden. Administratoren haben die Möglichkeit, eine von GFI MailSecurity unter Quarantäne gestellte E-Mail zu analysieren, um sie dann freizugeben oder zu löschen.

Außerdem lassen sich E-Mails mit Anhängen wie mp3- oder mpg-Dateien unter Quarantäne stellen, da diese zuviel Bandbreite belegen und die Speicherkapazität eines E-Mail-Servers unnötig belasten können.

Zudem erlitten Unternehmen, die GFI MailSecurity zum Schutz ihres Netzwerks einsetzen, dank des Moduls zur Anhangskontrolle beispielsweise keinen Schaden durch den Love Letter-Virus.

Der Trojan & Executable Scanner

GFI MailSecurity kann mit Hilfe des Trojan & Executable Scanner per E-Mail empfangene exe-Dateien analysieren und deren Gefährdungspotenzial bestimmen. Hierdurch lassen sich gefährliche und unbekannte Trojaner aufspüren und abwehren, bevor sie ins Netzwerk gelangen können.

Der HTML Sanitizer

Die HTML-Fähigkeit von E-Mails ermöglicht es Hackern und Viren-Programmierern, Befehle in HTML-Mails einzubinden und diese auszulösen, sobald die E-Mail geöffnet wird. Mit Hilfe des HTML Sanitizer überprüft GFI MailSecurity den Textkörper einer E-Mail und angehängte .htm/.html-Dateien auf Skriptcode und bereinigt die gesamte Nachricht samt Anlage. GFI MailSecurity ist das einzige Produkt, das mit Hilfe einer von GFI patentierten Technologie vor potenziell gefährlichen HTML-E-Mails schützt und HTML-Viren und -Angriffe abwehrt.

Der Dekomprimierungsfilter

Der Dekomprimierungsfilter wird zum Entpacken und Analysieren komprimierter Dateien (Archive) eingesetzt, die an E-Mails angehängt sind. Mit Hilfe dieses Filters können passwortgeschützte, fehlerhafte und rekursive Archive überprüft und blockiert werden. Er erlaubt es Ihnen auch zu kontrollieren, wie viele Dateien in einem Archiv enthalten sind und welche Größe sie haben. Archive mit Dateien, deren Anzahl oder Größe einen von Ihnen festgelegten Wert überschreitet, können vom Dekomprimierungsfilter unter Quarantäne gestellt oder gelöscht werden.

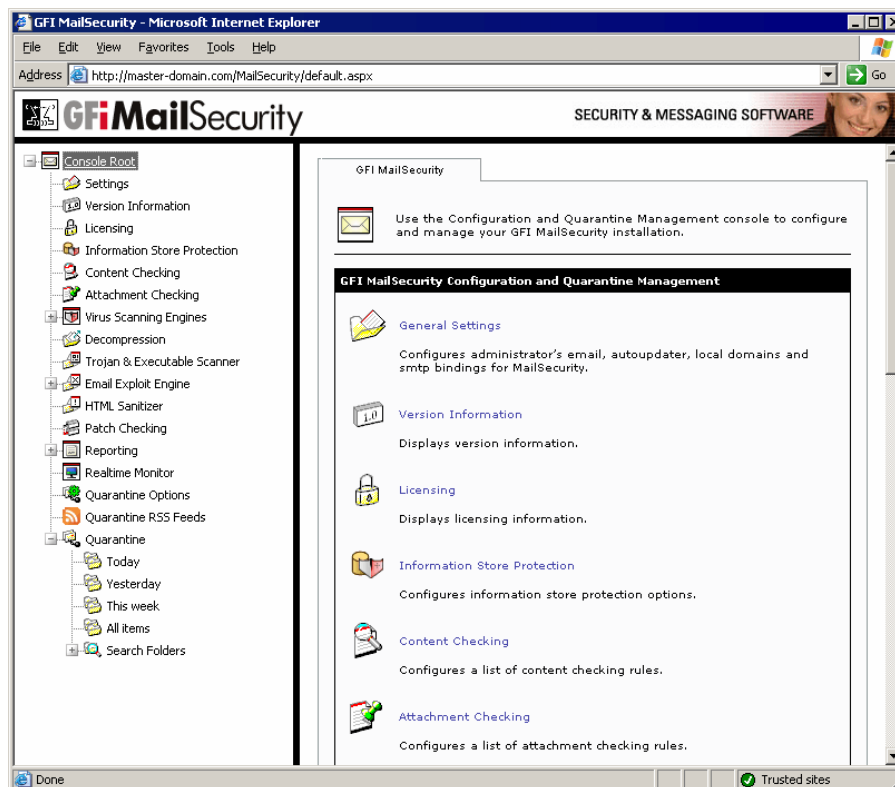
Komponenten von GFI MailSecurity

GFI MailSecurity besteht aus folgenden Bestandteilen:

- **Scan-Engine**

Die Scan-Engine von GFI MailSecurity analysiert den Inhalt sämtlicher ein- und ausgehender E-Mails, darunter auch den Informationsspeicher, wenn das Produkt auf einem Exchange-Server installiert ist. Stellt GFI MailSecurity eine E-Mail unter Quarantäne, wird der zuständige Verantwortliche/Administrator je nach gewählter Option per E-Mail/RSS-Feed darüber informiert.

- **Konfigurationsoberfläche**



Screenshot 1 – GFI MailSecurity Konfigurationsseite

Über die übersichtliche Konfigurationsoberfläche können Sie GFI MailSecurity ganz nach Ihren Bedürfnissen konfigurieren.

GFI MailSecurity aus Sicht des Anwenders

GFI MailSecurity führt seine Scan-Vorgänge vollständig im Hintergrund durch. Anwender bemerken nicht, dass die Software aktiv ist, bis eine Sicherheitsregel durch eine E-Mail verletzt und die Nachricht blockiert wird. Dieser Fall tritt beispielsweise ein, wenn ein Filter festgestellt hat, dass die Mitteilung einen unerlaubten Anhang oder einen Virus enthält.

Verdächtige E-Mails werden von GFI MailSecurity unter Quarantäne gestellt, damit sie vom Administrator kontrolliert werden können. Es ist auch möglich, dem Empfänger eine Nachricht zukommen zu lassen,

dass eine Mitteilung empfangen wurde, diese aber verdächtig ist und daher noch vom Administrator freigegeben werden muss. Nach erfolgter Freigabe wird die Nachricht sofort von GFI MailSecurity an den Empfänger weitergeleitet.

Erweitertes E-Mail-Management – GFI MailEssentials

Als Schwesterprodukt zu GFI MailSecurity ist GFI MailEssentials erhältlich. GFI MailEssentials erweitert die Funktionalität Ihres E-Mail-Servers um wichtige Tools für die geschäftliche E-Mail-Korrespondenz, z. B.:

- Vielseitige Anti-Spam-Filter, unter anderem zur Bayes'schen Analyse
- E-Mail-Management-Tools wie POP3-Downloader, Disclaimer und Server-basierte Auto-Replies

Weitere Informationen erhalten Sie auf der Website von GFI unter <http://www.gfisoftware.de/>.

Hinweis: GFI MailEssentials kann zusammen mit GFI MailSecurity als kostengünstiges Produkt-Bundle erworben werden.

Installieren von GFI MailSecurity

Einführung

In diesem Kapitel erfahren Sie, wie GFI MailSecurity zu installieren und konfigurieren ist. Sie können die Software direkt auf Ihrem E-Mail-Server oder auf einem separaten Server installieren, der als Mail-Relay/Gateway-Server fungiert. Bei Einrichtung auf einem separaten Server ist dieser vor der Installation von GFI MailSecurity so zu konfigurieren, dass er ein- und ausgehende E-Mails an bzw. von Ihrem E-Mail-Server weitergeben kann.

Damit GFI MailSecurity korrekt arbeitet, muss die Software Zugriff auf die E-Mail-Adressen aller Ihrer E-Mail-Anwender haben. Nur so können E-Mail-Überwachungsregeln zur Filterung ein- und ausgehender Mitteilungen erstellt werden. Eine Liste aller E-Mail-Anwender und ihrer Adressen kann von GFI MailSecurity wie folgt bezogen werden: entweder per Active Directory-Abfrage (hierfür muss die Software im **Active Directory-Modus** installiert worden sein) oder durch Importieren der Liste vom SMTP-Server (hierfür muss die Software im **SMTP-Modus** installiert worden sein). Der Installationsmodus ist abhängig von der Beschaffenheit Ihres Netzwerks und des Rechners zu wählen, auf dem die Sicherheitssoftware installiert werden soll. Der erforderliche Modus kann während der Installation von GFI MailSecurity ausgewählt werden.

Installieren von GFI MailSecurity auf einem E-Mail-Server

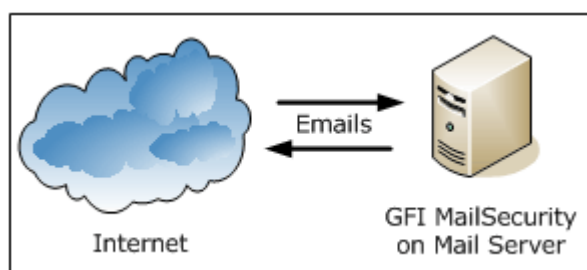


Abbildung 1 – Installation von GFI MailSecurity auf einem E-Mail-Server

GFI MailSecurity kann ohne zusätzliche Konfigurierung direkt auf Ihrem E-Mail-Server installiert werden. Zudem haben Sie die Wahl zwischen zwei Installationsmodi (Active Directory-Modus oder SMTP-Modus). Über diese Auswahl bestimmen Sie, wie GFI MailSecurity die Liste Ihrer E-Mail-Anwender abrufen, da Ihr E-Mail-Server sowohl Zugriff auf Active Directory als auch auf die Liste der SMTP-Anwender nehmen kann, die sich auf dem E-Mail-Server befindet.

Installieren von GFI MailSecurity auf einem Mail-Relay-Server

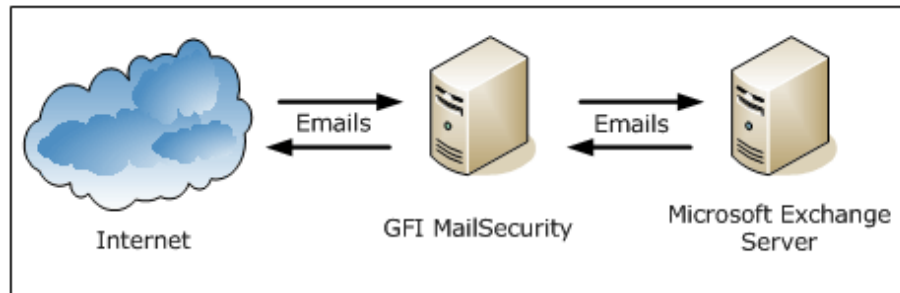


Abbildung 2 – Installation von GFI MailSecurity auf einem E-Mail-Gateway/Relay-Server

Bei der Installation auf einem getrennten Server (d. h. nicht auf Ihrem E-Mail-Server) muss dieser zunächst so konfiguriert werden, dass er als Gateway für alle E-Mails dient (auch „Smart Host“ oder „Mail-Relay“ genannt). Alle eingehenden Nachrichten haben somit zuerst diesen Rechner zur Durchführung der Sicherheitschecks zu passieren, bevor sie an den E-Mail-Server weitergegeben werden. Dieser übernimmt dann die Zustellung an die Empfänger. Sämtliche an Ihren E-Mail-Server geschickten Nachrichten müssen somit immer als Erstes vom Mail-Relay-Server empfangen werden. Gleiches gilt für ausgehende E-Mails: Der E-Mail-Server muss alle zu verschickenden Nachrichten zum Sicherheitscheck an GFI MailSecurity auf dem E-Mail-Relay weitergeben, bevor diese dann per Internet an externe Empfänger versendet werden. Der E-Mail-Relay muss daher die letzte Station für extern über das Internet zu übermittelnde E-Mails sein. Diese Konfiguration gewährleistet, dass GFI MailSecurity sämtliche ein- und ausgehenden E-Mails überprüft, bevor sie den Empfängern zugestellt werden.

Hinweis 1: Wenn Sie Lotus Notes oder einen anderen SMTP/POP3-Server einsetzen, muss GFI MailSecurity im SMTP-Modus installiert werden.

Hinweis 2: Bei Einsatz von Windows NT kann der Server mit GFI MailSecurity von Ihrem NT-Netzwerk getrennt sein – bei einer Installation im SMTP-Modus wird Active Directory von GFI MailSecurity nicht benötigt.

Installieren von GFI MailSecurity vor der Firewall

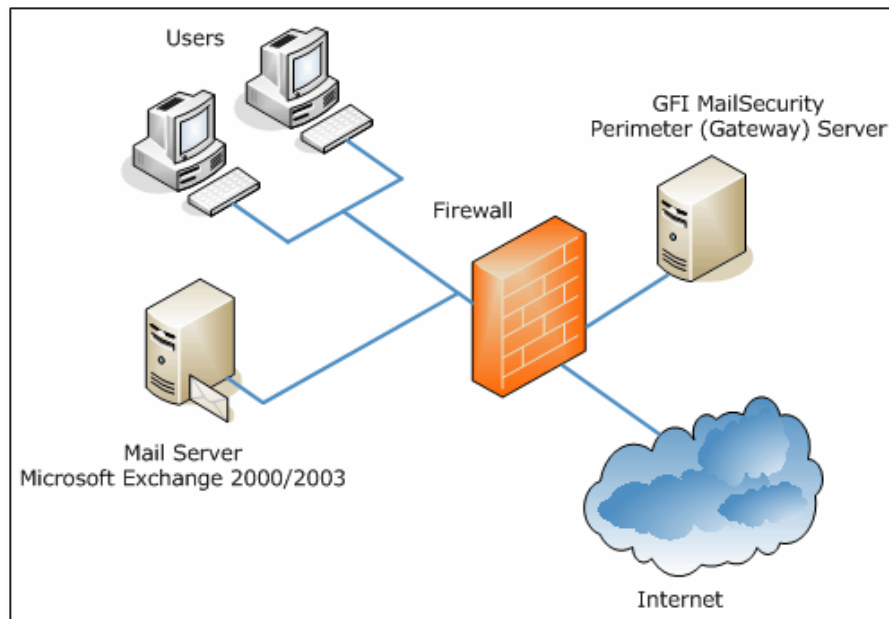


Abbildung 3 – Installation von GFI MailSecurity auf einem separaten Server in einer DMZ

Wenn Sie eine Firewall für Windows 2000/2003 einsetzen, z. B. Microsoft ISA Server, ist zu empfehlen, GFI MailSecurity auf einem eigenen Server vor Ihrer Firewall oder auf dem Firewall-Rechner zu installieren. Hierdurch haben Sie die Möglichkeit, Ihren E-Mail-Server weiterhin hinter der Firewall zu betreiben. GFI MailSecurity fungiert bei der Installation im Netzwerk-Perimeter (DMZ, demilitarisierte Zone) als Smart Host/Mail-Relay-Server.

Folgende Vorteile bestehen, wenn GFI MailSecurity nicht auf Ihrem E-Mail-Server installiert ist:

- Sie können Ihren E-Mail-Server warten und dabei weiterhin E-Mails aus dem Internet empfangen.
- Auf Ihrem E-Mail-Server werden weniger Ressourcen beansprucht.
- Sie profitieren von einer erhöhten Fehlertoleranz – sollte Ihr E-Mail-Server ausfallen, können Sie dennoch weiterhin Mitteilungen empfangen. Diese werden für die Dauer des Ausfalls auf dem GFI MailSecurity-Server in eine Warteschlange gestellt.

Hinweis: GFI MailSecurity erfordert keinen dedizierten Server, falls das Programm nicht auf dem E-Mail-Server installiert ist. Sie können GFI MailSecurity beispielsweise auf Ihrem Firewall-Server (d. h. unter ISA Server) oder auf einem anderen Server einrichten, auf dem Anwendungen wie GFI MailEssentials laufen.

Active/Passive Cluster-Installation von GFI MailSecurity

Bei einer Active/Passive Cluster-Installation von GFI MailSecurity muss die Software auf jedem Knoten installiert werden.

Hinweis: Beachten Sie, dass in diesem Fall jede Installation von GFI MailSecurity einzeln zu konfigurieren und verwalten ist. Es erfolgt kein Abgleich von Konfigurationseinstellungen und Quarantäne-E-Mails zwischen den einzelnen Knoten.

Folgende Installationsschritte sind für jeden Knoten notwendig:

- Installation von GFI MailSecurity auf der lokalen Festplatte des Knotens.
Hinweis: Installieren Sie GFI MailSecurity nicht auf einem freigegebenen Laufwerk.
- Installation des virtuellen WWW-Verzeichnisses von GFI MailSecurity für die **Standardwebsite** des Knotens.
- Bei Installation auf einem IIS-Cluster muss GFI MailSecurity an die **Cluster-Instanz** des virtuellen SMTP-Servers gebunden werden.

Nachfolgend soll die Installation von GFI MailSecurity in einer typischen Active/Passive Cluster-Umgebung exemplarisch beschrieben werden. Für dieses Beispiel soll gelten, dass der Cluster **MAILCLUSTER** heißt und aus den zwei Knoten **Node1** und **Node2** besteht.

1. Aktivieren Sie **Node1** über die **Clusterverwaltung**.
2. Installieren Sie GFI MailSecurity auf der lokalen Festplatte von **Node2** wie in diesem Kapitel unter „Installieren von GFI MailSecurity“ beschrieben. Beim Installationsschritt zum IIS-Setup wählen Sie bitte die **Standardwebsite** zum Hosten des virtuellen WWW-Verzeichnisses von GFI MailSecurity aus.
3. Ist die Installation von GFI MailSecurity auf **Node2** abgeschlossen, ist dessen GFI MailSecurity-Konfiguration über folgende URL aufrufbar: <http://Node2/MailSecurity/>
4. Aktivieren Sie **Node2** über die **Clusterverwaltung**.
5. Installieren Sie GFI MailSecurity auf der lokalen Festplatte von **Node1** wie in diesem Kapitel unter „Installieren von GFI MailSecurity“ beschrieben. Beim Installationsschritt zum IIS-Setup wählen Sie bitte die **Standardwebsite** zum Hosten des virtuellen WWW-Verzeichnisses von GFI MailSecurity aus.
6. Ist die Installation von GFI MailSecurity auf **Knoten1** abgeschlossen, ist dessen GFI MailSecurity-Konfiguration über folgende URL aufrufbar: <http://Node1/MailSecurity/>
7. Über folgende URL lässt sich die Produktkonfiguration des gerade aktiven Knotens aufrufen: <http://MAILCLUSTER/MailSecurity/>.
8. Die Installation von GFI MailSecurity auf einem Active/Passive Cluster ist abgeschlossen.

Hinweis: Fehlt das Service Pack 2 für Microsoft Exchange Server 2003 bei einer Cluster-Installation von Microsoft Exchange Server 2003, erfolgt bei einem Failover eines virtuellen Servers von Exchange Server 2003 zu einem Cluster-Knoten kein automatischer Aufruf der IIS-Websites, die auf dem Cluster gehostet werden. Weitere Informationen hierzu erhalten Sie im [Microsoft Knowledge-Base-Artikel 885440](#).

Aufgrund dieser Einschränkung könnte ein Aufruf der Konfiguration von GFI MailSecurity nach einem Failover oder dem Verschieben eines virtuellen Exchange-Servers von einem Cluster-Knoten auf den anderen nicht möglich sein.

Daher ist die Installation von Service Pack 2 für Microsoft Exchange Server 2003 ist zu empfehlen. Hinweise zur Installation von Service Packs zu Exchange Server 2003 in einer Cluster-Umgebung stehen bereit im [Microsoft Knowledge-Base-Artikel 867624](#).

So deinstallieren Sie GFI MailSecurity aus der oben beschriebenen Cluster-Umgebung **MAILCLUSTER**:

1. Aktivieren Sie **Node1** über die **Clusterverwaltung**.
2. Deinstallieren Sie GFI MailSecurity von **Node2**.
3. Aktivieren Sie **Node2** über die **Clusterverwaltung**.
4. Deinstallieren Sie GFI MailSecurity von **Node1**.
5. Die Deinstallation von GFI MailSecurity auf einem Active/Passive Cluster ist abgeschlossen.

Active/Active Cluster-Installation von GFI MailSecurity

Active/Active Cluster werden derzeit von GFI MailSecurity nicht unterstützt.

Auswählen des Installationsmodus

Active Directory-Modus

Wird GFI MailSecurity im Active Directory-Modus installiert, erstellt das Programm für die im Verzeichnisdienst enthaltenen Benutzer E-Mail-Überwachungsregeln, z. B. zur Anhangs- oder Inhaltskontrolle. Der Server, auf dem GFI MailSecurity läuft, muss sich somit hinter Ihrer Firewall befinden und als Teil der Active Directory-Domäne Zugriff auf das Active Directory mit all Ihren E-Mail-Anwendern haben. GFI MailSecurity kann im Active Directory-Modus direkt auf Ihrem E-Mail-Server oder jedem anderen als Mail-Relay konfigurierten Server der Domäne installiert werden.

SMTP-Modus

Wird GFI MailSecurity im SMTP-Modus installiert, erstellt das Programm unter Berücksichtigung aller auf Ihrem E-Mail-Server verfügbaren E-Mail-Benutzer/Adressen E-Mail-Überwachungsregeln, z. B. zur Anhangs- oder Inhaltskontrolle. Ist kein Zugriff auf Active Directory und die darin verzeichneten E-Mail-Anwender möglich, müssen Sie GFI MailSecurity somit im SMTP-Modus installieren. Dies ist der Fall bei Servern, die nicht Teil Ihrer Active Directory-Domäne sind, oder bei solchen, die sich in einer DMZ befinden. Sie können GFI MailSecurity jedoch auch dann im SMTP-Modus auf Ihrem E-Mail-Server und jedem anderen Server installieren, wenn dieser Zugriff auf Active Directory mit allen (E-Mail-)Anwendern hat.

Hinweis: Beide Installationsmodi bieten dieselben Scan-Funktionen und Leistung. Der einzige Unterschied zwischen dem Active Directory- und SMTP-Installationsmodus besteht in der Art und Weise, wie GFI MailSecurity auf die Liste der E-Mail-Anwender zugreift bzw. diese ermittelt, um seine Überwachungs-/Scan-Regeln und -Benachrichtigungen zu erstellen.

Systemanforderungen

Für die Installation von GFI MailSecurity benötigen Sie:

- Windows 2000 Professional/Server/Advanced Server (mit Service Pack 1 oder höher) oder Windows 2003 Server/Advanced Server oder Windows XP.

Hinweis: Aufgrund von Geschwindigkeitseinschränkungen bei Windows XP sind bei der Installation von GFI MailSecurity auf einem Rechner mit diesem Betriebssystem Leistungseinbußen möglich.

- Microsoft Exchange Server 2000 (mit Service Pack 1), 2003, 4, 5 oder 5.5, Lotus Notes 4.5 und höher oder ein beliebiger SMTP-/POP3-Mail-Server.
- Bei Einsatz von Small Business Server: Service Pack 2 für Exchange Server 2000 und Service Pack 1 für Exchange Server 2003.
- Microsoft .NET Framework 1.1/2.0.
- MSMQ – Microsoft Messaging Queuing Service.
- Internet Information Services (IIS) – SMTP-Service und World Wide Web-Service
- Microsoft Data Access Components (MDAC) 2.8

Wichtig: Konfigurieren Sie Ihre Anti-Viren-Software so, dass die GFI MailSecurity-Verzeichnisse nicht gescannt werden. Anti-Viren-Produkte können die normale Funktionsweise von Software beeinträchtigen und verlangsamen zudem Anwendungen, die auf Dateien zugreifen müssen. Microsoft empfiehlt, keine dateibasierte Anti-Viren-Software auf dem E-Mail-Server einzusetzen. Weitere Informationen erhalten Sie unter:

<http://kbase.gfi.com/showarticle.asp?id=KBID001559>.

Wichtig: Stellen Sie sicher, dass eventuell eingesetzte Backup-Software zu keinem Zeitpunkt eine Sicherheitskopie der GFI MailSecurity-Verzeichnisse anlegt.

Hardware-Anforderungen

Folgende Hardware ist für GFI MailSecurity erforderlich:

- Pentium 4 (oder gleichwertig) mit mindestens 2 GHz.
- Mindestens 512 MB RAM Arbeitsspeicher.
- Mindestens 1,5 GB freier Festplattenspeicher.

Vorbereiten der Installation auf einem Mail-Relay-Server

Damit GFI MailSecurity auf einem Mail-Relay/Gateway-Server installiert werden kann, müssen auf diesem Rechner der IIS SMTP-Dienst und der World Wide Web-Service laufen. Zudem muss der Server als SMTP-Relay für Ihren E-Mail-Server konfiguriert sein. Der MX-Eintrag Ihrer Domäne hat somit auf den Gateway-Server zu verweisen. In diesem Unterkapitel erfahren Sie, wie Sie den Mail-Relay-Server konfigurieren und GFI MailSecurity installieren. Weitergehende Informationen zur Installation von Microsoft Windows 2000

als SMTP-Relay-Server oder Smarthost erhalten Sie unter <http://support.microsoft.com/support/kb/articles/Q293/8/00.ASP>.

Installieren und Konfigurieren des IIS SMTP- und World Wide Web-Diensts

GFI MailSecurity verwendet den IIS SMTP-Dienst von Windows 2000/2003/XP als SMTP-Server. Zuerst müssen Sie diesen Dienst jedoch als Mail-Relay-Server konfigurieren, damit GFI MailSecurity alle ein- und ausgehenden E-Mails scannen kann, bevor diese auf Ihren E-Mail-Server gelangen.

Informationen zum IIS SMTP- und World Wide Web-Service von Windows 2000/2003

Der SMTP-Dienst gehört zu den Internet-Informationendiensten (Internet Information Services, IIS), die Bestandteil von Microsoft Windows 2000/2003/XP sind. Der Dienst wird von Microsoft Exchange Server als Agent für die Nachrichtenübermittlung eingesetzt und kann selbst ein sehr hohes E-Mail-Aufkommen problemlos bewältigen.

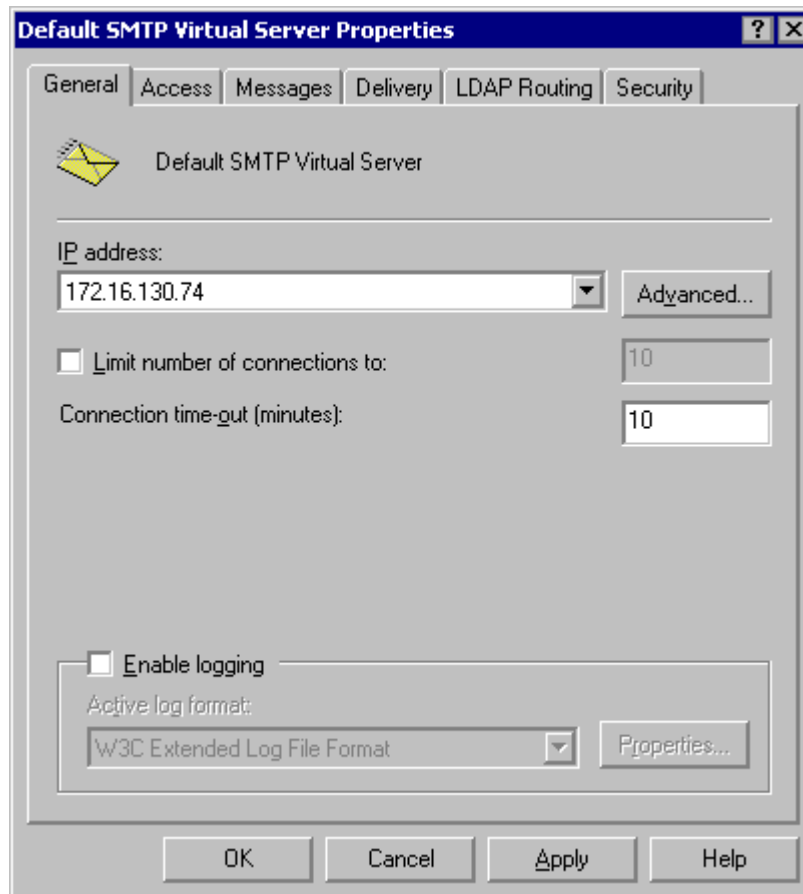
Der World Wide Web-Service ist ebenfalls Bestandteil der IIS. Er verarbeitet Web-Client-Anfragen in einem TCP/IP-Netzwerk per HTTP-Protokoll.

Der IIS SMTP- und World Wide Web-Service ist im Lieferumfang jeder Distribution von Windows 2000/2003/XP enthalten.

Um den IIS SMTP-Dienst als Mail-Relay-Server zu installieren und zu konfigurieren, gehen Sie wie folgt vor:

Schritt 1: Überprüfen der Installation des IIS SMTP- und World Wide Web-Service

1. Gehen Sie auf **Start ▶ Einstellungen ▶ Systemsteuerung**. Klicken Sie auf **Software** und dann auf **Windows-Komponenten hinzufügen/entfernen**.
2. Suchen und markieren Sie im angezeigten Dialogfenster die **Internetinformationsdienste (IIS)**, und klicken Sie dann auf die Schaltfläche **Details**.
3. Überprüfen Sie, ob die Kontrollkästchen **SMTP-Dienst** und **WWW-Dienst** aktiviert sind. Aktivieren Sie sie gegebenenfalls, und klicken Sie auf die Schaltfläche **OK**. Die Installation der ausgewählten Dienste sollte beginnen. Folgen Sie den Bildschirmanweisungen, und warten Sie, bis der Installationsvorgang beendet ist.



Screenshot 2 – Zuweisen einer IP-Adresse für den Mail-Relay-Server

Schritt 2: Benennen des Mail-Relay-Servers und Zuweisen der IP-Adresse

1. Gehen Sie auf **Start ▶ Programme ▶ Verwaltung**, und klicken Sie auf **Internetinformationsdienste-Manager**.
2. Erweitern Sie die Struktur unter dem Server-Namen, und klicken Sie mit der rechten Maustaste auf den Knoten **Virtueller Standardserver für SMTP** (Default SMTP Virtual Server). Wählen Sie im Kontextmenü **Eigenschaften** aus.
3. Weisen Sie dem SMTP-Relay-Server eine IP-Adresse zu, und klicken Sie auf die Schaltfläche **Übernehmen**, um die Änderungen zu übernehmen. Schließen Sie den Dialog.

Schritt 3: Konfigurieren des SMTP-Dienstes zur Weitergabe von Nachrichten an Ihren E-Mail-Server

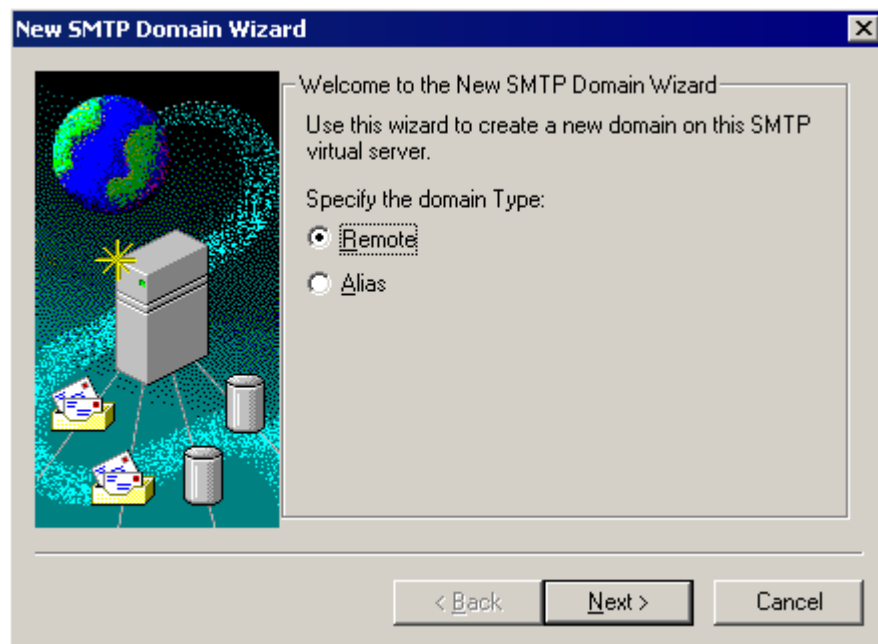
Konfigurieren Sie den SMTP-Dienst so, dass er eingehende Nachrichten an Ihren E-Mail-Server weitergibt.

Erstellen Sie in den IIS zuerst eine lokale Domäne zur Weitergabe von E-Mails:

1. Gehen Sie auf **Start ▶ Programme ▶ Verwaltung**, und klicken Sie auf **Internetinformationsdienste-Manager**.
2. Erweitern Sie zuerst die Struktur unter dem Server-Namen und anschließend den die Struktur unter **Virtueller Standardserver für SMTP** (Default SMTP Virtual Server). Standardmäßig sollte eine

lokale (Standard-)Domäne mit dem voll qualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) des Servers vorgegeben sein.

3. So konfigurieren Sie die Domäne zur Weitergabe eingehender Mitteilungen:

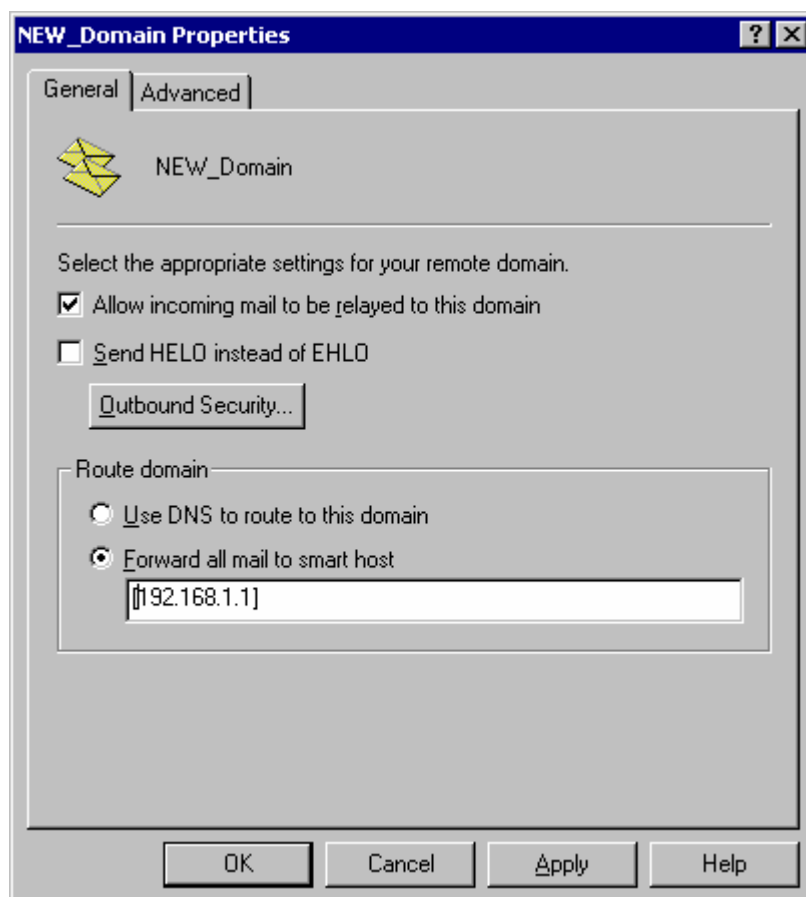


Screenshot 3 – Assistent für SMTP-Domänen; Auswahl des Domänentyps

- a) Klicken Sie mit der rechten Maustaste auf den Knoten **Domänen**, und gehen Sie auf **Neu ▶ Domäne**.
- b) Wählen Sie **Remote**, und klicken Sie auf die Schaltfläche **Weiter**.
- c) Geben Sie im Eingabefeld **Name** den Domännennamen ein, und klicken Sie auf die Schaltfläche **Fertig stellen**.

Wichtiger Hinweis zu lokalen Domänen

Bei der Installation importiert GFI MailSecurity die lokalen Domänen aus dem IIS SMTP-Dienst. Wenn Sie den IIS SMTP-Dienst um weitere lokale Domänen ergänzen, müssen Sie diese auch GFI MailSecurity hinzufügen, da die Software neu hinzugefügte lokale Domänen nicht automatisch erkennt. Weitere/neue lokale Domänen lassen sich über das Konfigurationsprogramm von GFI MailSecurity hinzufügen. Nähere Informationen hierzu erhalten Sie unter im Kapitel „Allgemeine Einstellungen“ unter „Hinzufügen lokaler Domänen“.



Screenshot 4 – Konfigurierung der neuen Domäne

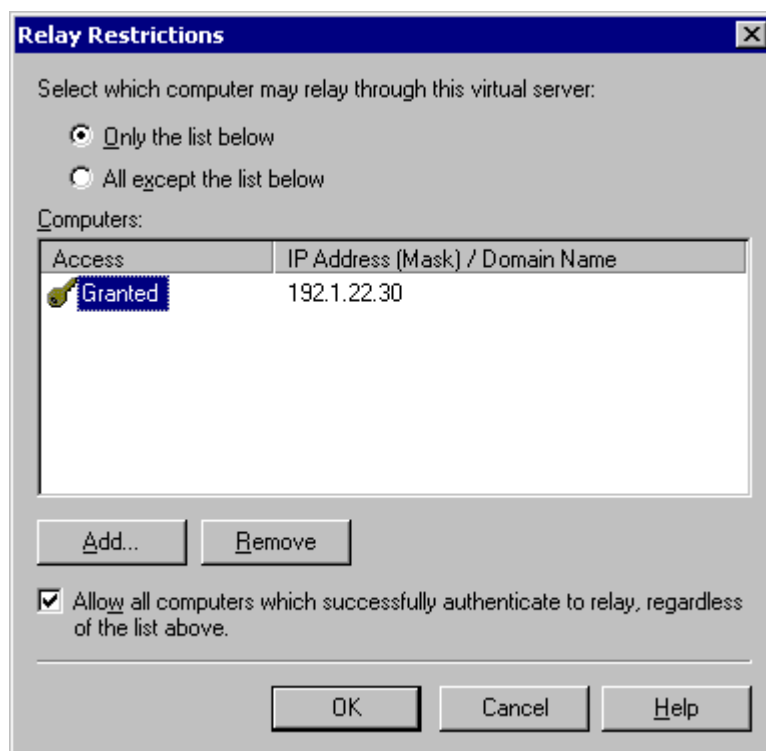
Konfigurieren der Domäne zur Weitergabe von Nachrichten an den E-Mail-Server

1. Klicken Sie mit der rechten Maustaste auf die zuvor erstellte Domäne, und wählen **Eigenschaften** im Kontextmenü. Markieren Sie das Kontrollkästchen **Eingehende Nachrichten können an diese Domäne weitergegeben werden**.

2. Wählen Sie im Bereich **Routingdomäne** die Option **Gesamte Mail an Smarthost weiterleiten**, und geben Sie in eckigen Klammern die IP-Adresse des Servers an, der für die Verarbeitung von E-Mails zuständig ist, die an diese neue Domäne adressiert sind. Beispiel: [123.123.123.123]

Hinweis: Die eckigen Klammern werden verwendet, damit der Server diese Information als IP-Adresse erkennt und sie von einem Host-Namen unterscheiden kann.

3. Klicken Sie auf die Schaltfläche **OK**, um die Eingaben zu speichern und das Dialogfenster zu schließen.

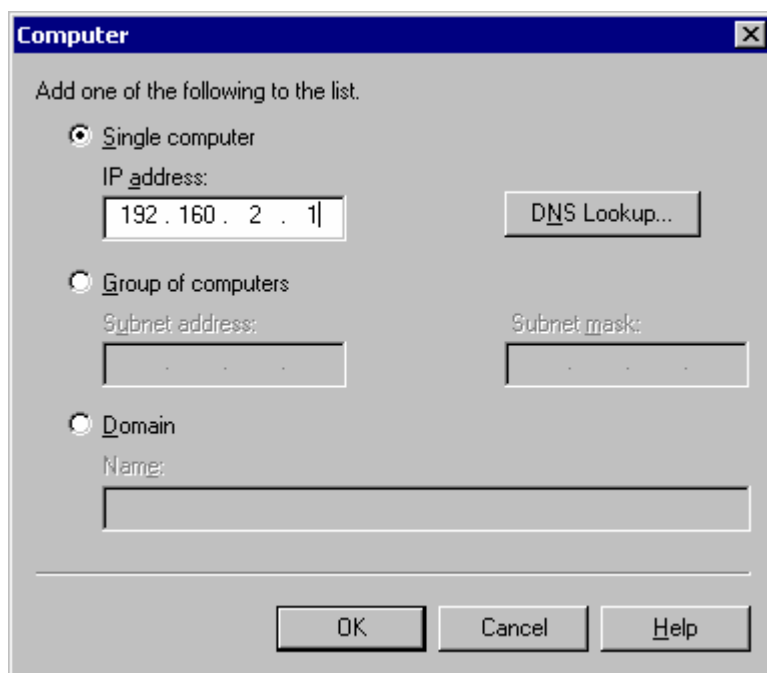


Screenshot 5 – Dialog zu Weiterabeeinschränkungen

Schritt 4: Sichern des Mail-Relay-Servers

Legen Sie nun fest, welche Einschränkungen bei der Weitergabe von Nachrichten über Ihren virtuellen SMTP-Server gelten sollen. Bei diesem Schritt grenzen Sie die Anzahl der Server ein, die E-Mails über diesen virtuellen Server weitergeben dürfen.

1. Klicken Sie mit der rechten Maustaste auf den Knoten **Virtueller Standardserver für SMTP** (Default SMTP Virtual Server), und wählen Sie **Eigenschaften**.
2. Gehen Sie auf den Reiter **Zugriff**, und klicken Sie dann auf die Schaltfläche **Weitergabe**, um das Dialogfenster mit den Weiterabeeinschränkungen zu öffnen.
3. Wählen Sie die Option **Nur den unten angezeigten Computern**, und klicken Sie dann auf die Schaltfläche **Hinzufügen**, um alle zur Weitergabe berechtigten Computer anzugeben.



Screenshot 6 – Computer, die E-Mails über den virtuellen Server weitergeben dürfen

4. Geben Sie im sich öffnenden Dialogfenster die IP-Adresse des E-Mail-Servers an, der Nachrichten an diesen virtuellen Server weiterleiten wird. Klicken Sie auf die Schaltfläche **OK**, um den Eintrag hinzuzufügen.

Hinweis: In diesem Dialogfenster können Sie die IP-Adresse eines einzelnen Computers, einer Gruppe von Computern oder einer Domäne angeben:

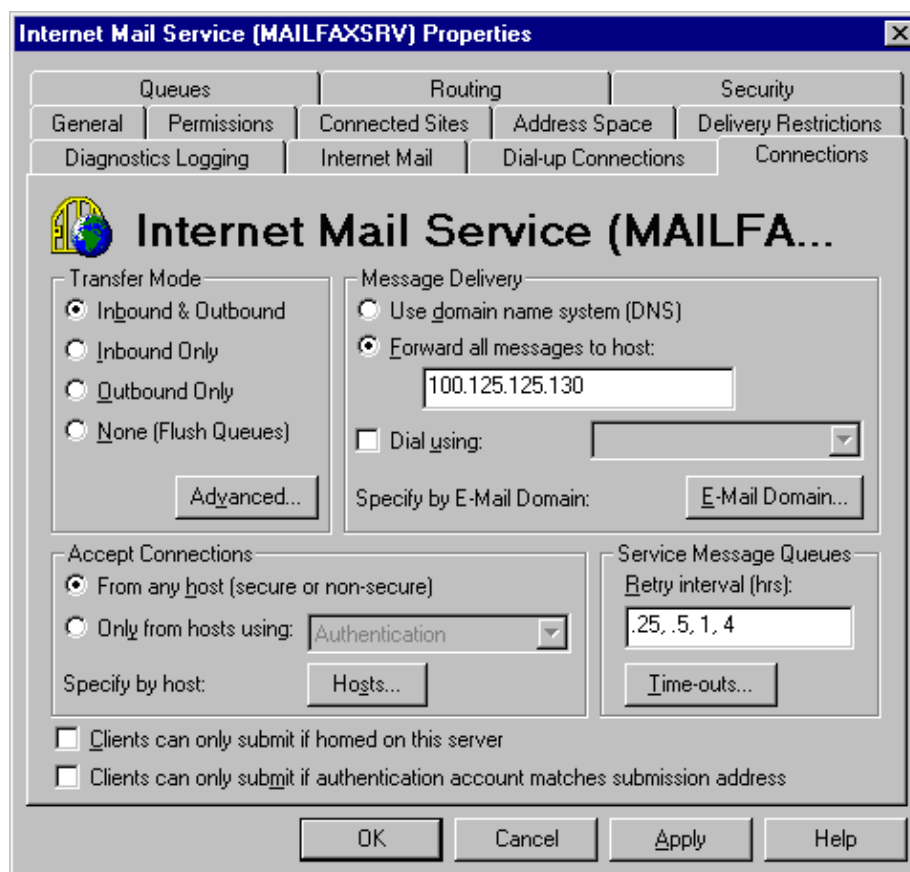
- **Einzelner Computer** – Geben Sie einen einzelnen Host an, der E-Mails über diesen Server weitergeben darf. Um die IP-Adresse eines Hosts abzufragen, klicken Sie auf die Schaltfläche **DNS-Suche**.
- **Gruppe von Computern** – Geben Sie die Basis-IP-Adresse für alle Computer ein, die Nachrichten weitergeben dürfen.
- **Domäne** – Erlauben Sie allen Computer einer angegebenen Domäne die Weitergabe. Der Domänen-Controller gibt hierbei ohne Einschränkung E-Mails über diesen Server weiter. Bei Auswahl dieser Option wird jedoch die Verarbeitungslast erhöht. Die Leistung des SMTP-Diensts kann beeinträchtigt werden, da zur Kontrolle des Domänennamens aller IP-Adressen, über die eine Weitergabe erfolgen soll, eine umgekehrte DNS-Suche erfolgt.

Schritt 5: Konfigurieren des E-Mail-Servers zur Weitergabe von Nachrichten über den Gateway-Server

Nachdem Sie den IIS-SMTP-Dienst für den Versand und Empfang von Nachrichten konfiguriert haben, müssen Sie nun Ihren E-Mail-Server so konfigurieren, dass er diese an den Mail-Relay-Server weitergibt.

Bei Verwendung von Microsoft Exchange Server 4/5/5.5

1. Starten Sie Microsoft Exchange Administrator, und doppelklicken Sie auf **Internet Mail-Dienst**, um dessen Eigenschaften zu konfigurieren.



Screenshot 7 – Microsoft Internet-Mail-Connector

2. Klicken Sie auf den Reiter **Verbindungen**, und wählen Sie dann im Bereich **Nachrichtenübermittlung** die Option **Alle Nachrichten an Host weiterleiten**. Geben Sie den Namen oder die IP-Adresse des Rechners ein, auf dem GFI MailSecurity installiert ist.
3. Klicken Sie auf die Schaltfläche **OK**, und führen Sie über das Dienste-Applet einen Neustart von Microsoft Exchange Server durch.

Bei Verwendung von Microsoft Exchange Server 2000/2003

Sie müssen einen SMTP-Connector einrichten, der alle Nachrichten an GFI MailSecurity weiterleitet:

1. Starten Sie den **Exchange System-Manager**.
2. Klicken Sie mit der rechten Maustaste auf den Knoten **Connectors**, gehen Sie auf **Neu ▶ SMTP-Connector**, und geben Sie den Connector-Namen an.
3. Wählen Sie die Option **Gesamte Mail über diesen Connector an diese Smarthosts weiterleiten**, geben Sie die IP-Adresse des GFI MailSecurity-Servers ein (Mail-Relay/Gateway-Server), und klicken Sie auf die Schaltfläche **OK**.

Hinweis: Geben Sie die IP-Adresse immer in eckigen Klammern [] an. Beispiel: [100.130.130.10].

4. Wählen Sie den SMTP-Server, der diesem SMTP-Connector zugewiesen sein soll. Klicken Sie auf den Reiter **Adressraum**, und klicken Sie auf die Schaltfläche **Hinzufügen**. Wählen Sie **SMTP**, und klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu übernehmen.

5. Klicken Sie abschließend erneut auf die Schaltfläche **OK**. Alle E-Mails werden nun an den GFI MailSecurity-Server weitergeleitet.

Bei Verwendung von Lotus Notes

1. Doppelklicken Sie in Lotus Notes auf die Schaltfläche **Address Book** für das Adressbuch.
2. Klicken Sie auf das Element **Server**, um die Unterelemente aufzurufen.
3. Klicken Sie auf **Domains** und dann auf **Add Domains**, um Domänen hinzuzufügen.
4. Wählen Sie im Bereich **Basics** die Option **Foreign SMTP Domain from the Domain Type**, und geben Sie im Bereich **Messages Addressed to** im Feld **Internet Domain** ein Sternchen ("*") ein.
5. Geben Sie im Feld **Internet Host** des Bereichs **Should be routed to** die IP-Adresse des Servers ein, auf dem GFI MailSecurity läuft.
6. Speichern Sie Ihre Eingaben, und führen Sie einen Neustart des Lotus Notes-Servers durch.

Bei Verwendung eines SMTP/POP3 E-Mail-Servers

1. Starten Sie das Konfigurationsprogramm Ihres E-Mail-Servers.
2. Suchen Sie die Option zum Weiterleiten ausgehender E-Mail über einen anderen E-Mail-Server. Diese Option kann z. B. heißen **Alle Nachrichten an diesen Host weiterleiten**. Geben Sie den Namen oder die IP-Adresse des Servers ein, auf dem GFI MailSecurity installiert ist.
3. Klicken Sie ggf. auf die Schaltfläche **OK**, und starten Sie Ihren E-Mail-Server neu.

Schritt 6: MX-Eintrag der Domäne auf Mail-Relay-Server verweisen lassen

Da der neue Mail-Relay-Server als erster alle eingehenden E-Mails empfangen muss, ist der MX-Eintrag Ihrer Domäne unbedingt zu aktualisieren, damit er auf die IP-Adresse des neuen Mail-Relay/Gateway-Servers verweist. Andernfalls würden die Nachrichten weiterhin direkt an Ihren E-Mail-Server gehen und nicht von GFI MailSecurity gefiltert werden.

Aktualisieren des MX-Eintrags Ihres DNS-Servers

Hinweis: Haben Sie einen ISP mit der Verwaltung Ihres DNS-Servers beauftragt, muss er den Eintrag für Sie aktualisieren.

1. Öffnen Sie die Eingabeaufforderung, und geben Sie „nslookup“ ein.
2. Geben Sie „set type=mx“ ein und dann Ihre E-Mail-Domäne.
3. Der MX-Eintrag sollte in Form einer einzigen IP-Adresse ausgegeben werden und muss mit der Adresse des Servers identisch sein, auf dem GFI MailSecurity läuft.

```
C:\WINNT\System32\cmd.exe - nslookup
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\administrator.GHOST>nslookup
Default Server: server-qa
Address: 192.168.0.1

> set type=mx
> gatest.com
Server: server-qa
Address: 192.168.0.1

gatest.com      MX preference = 10, mail exchanger = gatest.com
gatest.com      internet address = 192.168.0.153
>
```

Screenshot 8 – Prüfen des MX-Eintrags Ihrer Domäne

Schritt 7: Testen des neuen Mail-Relay-Servers

Bevor Sie mit der Installation von GFI MailSecurity beginnen, sollten Sie sicherstellen, dass Ihr neuer Mail Relay-Server korrekt arbeitet.

1. Testen Sie die IIS SMTP-Verbindung für eingehende Nachrichten, indem Sie eine Nachricht von einem externen E-Mail-Konto an einen internen Benutzer verschicken (hierfür können Sie z. B. Hotmail verwenden, wenn Sie kein eigenes externes Konto besitzen). Stellen Sie sicher, dass die Nachricht vom E-Mail-Client empfangen wurde.
2. Testen Sie den IIS SMTP-Ausgang des Mail-Relay-Servers, indem Sie eine Nachricht über einen E-Mail-Client an ein externes E-Mail-Konto senden. Stellen Sie sicher, dass der externe Empfänger die E-Mail erhalten hat.

Hinweis: Anstatt einen E-Mail-Client einzusetzen, können Sie eine Nachricht auch manuell per Telnet versenden. Diese Möglichkeit bietet Ihnen auch mehr Informationen zur Lösung eventuell auftretender Probleme. Weitere Informationen hierzu erhalten Sie im folgenden Knowledge-Base-Artikel von Microsoft:

<http://support.microsoft.com/support/kb/articles/Q153/1/19.asp>

Schritt 8: Installieren von GFI MailSecurity auf dem Mail-Relay-Server

Weitere Informationen zur Installation von GFI MailSecurity erhalten Sie unter „Installieren von GFI MailSecurity“ in diesem Kapitel.

Vorbereitungen vor der Installation auf einem E-Mail-Server

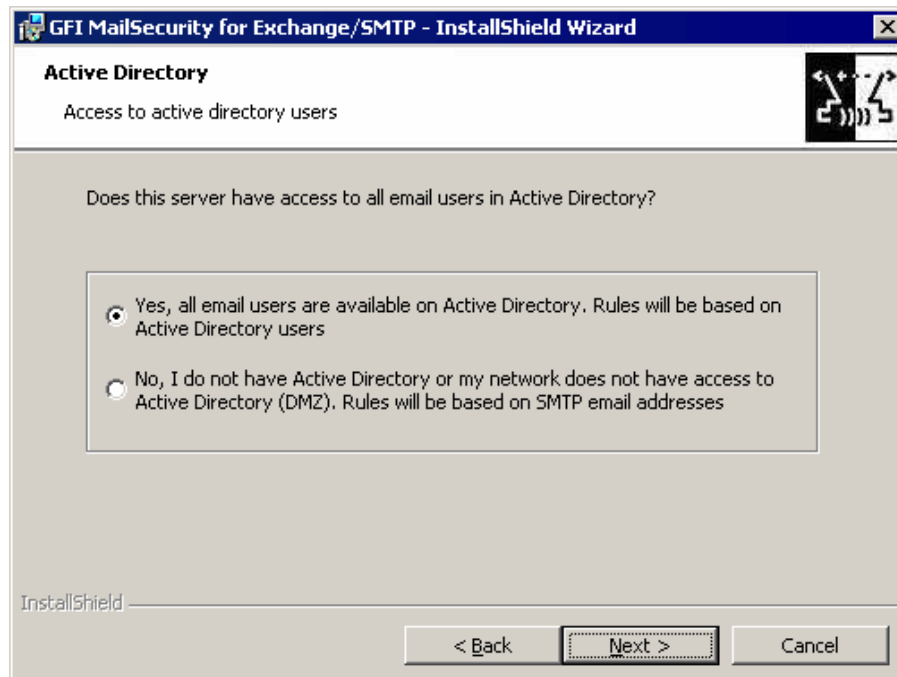
Wenn Sie GFI MailSecurity direkt auf Ihrem E-Mail-Server installieren, sind keine zusätzlichen Konfigurierungsschritte erforderlich. Weitere Informationen zur Installation von GFI MailSecurity erhalten Sie unter „Installieren von GFI MailSecurity“ in diesem Kapitel.

Installieren von GFI MailSecurity

Hinweis: Führen Sie folgende Schritte durch, bevor Sie GFI MailSecurity installieren:

- a) Melden Sie sich als Administrator an, oder verwenden Sie ein Konto mit Administratorrechten.
- b) Schließen Sie alle auf dem Installationsrechner geöffneten Dateien und Anwendungen, bevor Sie die Installation starten.

1. Starten Sie die Installation von GFI MailSecurity per Doppelklick auf „MailSecurityGW.exe“. Klicken Sie im Willkommen-Bildschirm auf die Schaltfläche **Next**.
2. Bestätigen Sie die Lizenzvereinbarung, und klicken Sie auf die Schaltfläche **Next**.
3. Geben Sie Ihren Namen, den Namen Ihrer Firma und den Registrierschlüssel ein. Wenn Sie das Produkt zu Testzwecken einsetzen, ändern Sie den vorgegebenen Eintrag „Evaluation“ bitte nicht. Klicken Sie auf die Schaltfläche **Next**.
4. Geben Sie die E-Mail-Adresse des Administrators oder der Person ein, an die GFI MailSecurity E-Mail-Benachrichtigungen senden soll.

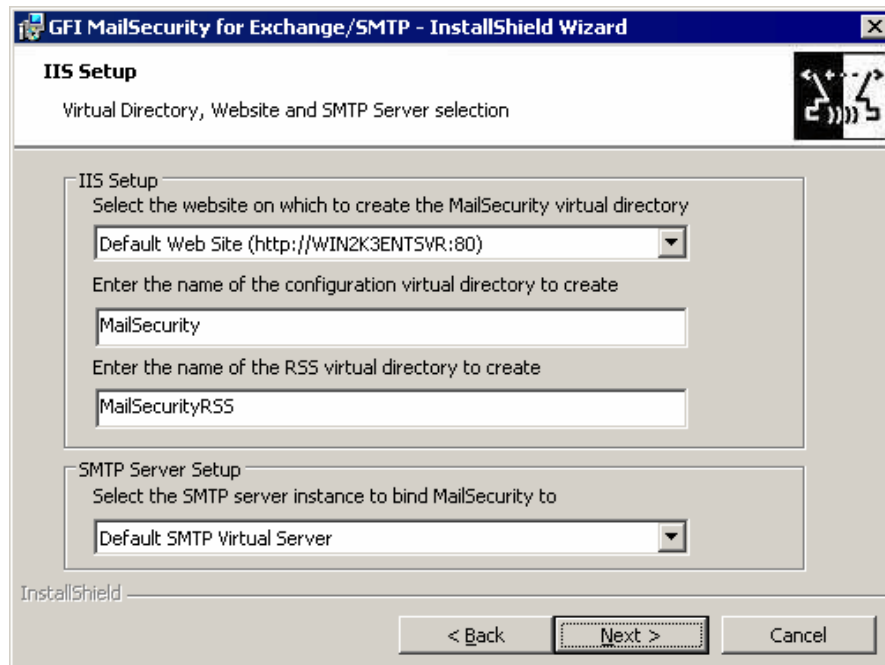


Screenshot 9 – Server-Zugriff auf alle E-Mail-Benutzer in AD

5. Das Installationsprogramm fragt Sie nun nach dem Modus, in dem GFI MailSecurity die Liste Ihrer E-Mail-Anwender abrufen soll. Wählen Sie eine der folgenden Optionen aus:
 - **Yes, all email users are available on Active Directory** – Installiert GFI MailSecurity im Active Directory-Modus. In diesem Modus erstellt das Programm benutzerbasierte E-Mail-Überwachungsregeln für die in Active Directory verzeichneten Anwender. Der Server, auf dem GFI MailSecurity installiert wird, muss sich hinter Ihrer Firewall befinden (z. B. E-Mail-Server) und Zugriff auf Active Directory mit allen Ihren E-Mail-Benutzer haben. Er muss somit Teil der Active Directory-Domäne sein.
 - **No, I do not have Active Directory or my network does not have access to Active Directory (DMZ)** – Installiert GFI MailSecurity im SMTP-Modus. Wird GFI MailSecurity im SMTP-Modus installiert, erstellt das Programm unter Berücksichtigung aller auf Ihrem E-Mail-Server verfügbaren E-Mail-Benutzer/Adressen E-Mail-Überwachungsregeln, z. B. zur Anhangs- oder Inhaltskontrolle. Dieser Modus muss gewählt werden, wenn Sie GFI MailSecurity auf einem Server installieren, der keinen Zugriff auf AD mit allen Ihren E-Mail-Anwendern hat. Hierzu

zählen Computer in einer DMZ oder solche, die nicht Teil einer AD-Domäne sind. Dieser Modus kann auch dann verwendet werden, wenn Sie GFI MailSecurity auf einem Server installieren, der Zugriff auf AD mit all Ihren E-Mail-Anwendern hat.

Klicken Sie auf die Schaltfläche **Next**, um mit der Installation fortzufahren.



Screenshot 10 – SMTP-Server und virtuelles Verzeichnis von GFI MailSecurity

6. Wählen Sie den Server aus, auf dem die Konfigurationsseiten von GFI MailSecurity gehostet werden sollen. Auf diesem Server werden zwei virtuelle Verzeichnisse für die Konfigurationsseiten und die RSS-Feeds des Quarantänebereichs erstellt. Die Standardeinstellungen für die Namen der virtuellen Verzeichnisse können beibehalten oder durch eigene Angaben ersetzt werden.

GFI MailSecurity setzt den IIS SMTP-Dienst für den Versand und Empfang von SMTP-E-Mails ein. Er ist an den standardmäßigen virtuellen SMTP-Server (dem im MX-Eintrag Ihres DNS-Servers angegebenen Server) gebunden. Befinden sich jedoch mehrere virtuelle SMTP-Server in Ihrer Domäne, können Sie GFI MailSecurity an jeden dieser Server binden. Falls Sie die standardmäßige SMTP-Verbindung ändern möchten, wählen Sie den gewünschten Server aus der Liste der verfügbaren virtuellen SMTP-Server aus.

Hinweis 1: Weitere Informationen zu den Einstellungen des IIS SMTP-Diensts erhalten Sie unter „Installieren und Konfigurieren des IIS SMTP- und World Wide Web-Diensts“ in diesem Handbuch.

Hinweis 2: Auch nach der Installation der Software können Sie GFI MailSecurity mit Hilfe der allgemeinen Konfigurationsoptionen an einen anderen virtuellen SMTP-Server binden. Gehen Sie hierfür auf **Console Root** ▶ **Settings** ▶ **Bindings**. Weitere Informationen hierzu erhalten Sie unter „Bindungen an SMTP-Server“ im Kapitel „Allgemeine Einstellungen“.

Klicken Sie auf die Schaltfläche **Weiter** um fortzufahren.

7. Das Setup-Programm durchsucht Ihr Netzwerk und importiert die Liste Ihrer lokalen Domänen vom IIS SMTP-Dienst. GFI MailSecurity ermittelt, ob eine E-Mail ein- oder ausgehend ist, indem die Domäne der Absenderadresse mit der Liste der lokalen Domänen verglichen wird. Ist die Adresse in der Liste verzeichnet, handelt es sich somit um eine ausgehende Nachricht. Kontrollieren Sie, ob sämtliche Ihrer lokalen Domänen in der angezeigten Liste aufgeführt sind. Nicht verzeichnete Domänen sollten nach Abschluss der Installation manuell hinzugefügt werden. Nähere Informationen hierzu erhalten Sie im Kapitel „Allgemeine Einstellungen“ unter „Hinzufügen lokaler Domänen“. Klicken Sie auf die Schaltfläche **Next**.

8. Geben Sie das Installationsverzeichnis von GFI MailSecurity an. GFI MailSecurity benötigt ca. 40 MB freien Festplattenspeicher. Zusätzlich müssen ca. 200 MB für temporäre Dateien verfügbar sein. Klicken Sie auf die Schaltfläche **Change**, um einen neuen Installationspfad anzugeben. Um die bereits vorgegebene Einstellung zu übernehmen, klicken Sie auf die Schaltfläche **Next**.

9. Nachdem die Eingabe der vom Installationsassistenten benötigten Daten beendet ist, kann GFI MailSecurity installiert werden. Zur erneuten Überprüfung oder Änderung von Eingaben klicken Sie auf die Schaltfläche **Back**. Klicken Sie auf die Schaltfläche **Install**, um die Installation von GFI MailSecurity zu starten.

10. Nach Beendigung der Installation werden Sie vom Setup-Programm informiert, dass die SMTP-Dienste neu gestartet werden müssen. Klicken Sie für einen sofortigen Neustart der Dienste und zum Abschluss des gesamten Installationsvorgangs auf die Schaltfläche **Yes**.

Hinzufügen von GFI MailSecurity zur DEP-Exception-List von Windows XP

Die Datenausführungsverhinderung (Data Execution Prevention – DEP) ist eine Sammlung von Hardware- und Software-Technologien, mit denen zusätzliche Prüfungen des Arbeitsspeichers durchgeführt werden, um Schutz vor der unerwünschten, unerwarteten oder böswilligen Ausführung von Code zu bieten.

Die DEP-Technologie steht nur unter Microsoft Windows XP mit Service Pack 2 und unter Microsoft Windows 2003 mit Service Pack 1 zur Verfügung. DEP ist unter Microsoft Windows 2003 mit Service Pack 1 standardmäßig für alle Programme und Dienste aktiviert, vom Administrator bestimmte Programme und Dienste ausgenommen.

Wenn Sie GFI MailSecurity unter Microsoft Windows 2003 mit Service Pack 1 installiert haben, müssen Sie die ausführbare Datei der Scan-Engine von GFI MailSecurity („GFIScanM.exe“) und die ausführbare Datei des Viren-Scanners von Kaspersky („kavss.exe“) der DEP-Ausnahmeliste hinzufügen.

So fügen Sie die beiden ausführbaren Dateien der DEP-Ausnahmeliste hinzu:

1. Gehen Sie auf **Start ▶ Systemsteuerung ▶ System**.
2. Gehen Sie auf den Reiter **Erweitert**, und klicken Sie im Bereich **Systemleistung** auf die Schaltfläche **Einstellungen**.
3. Gehen Sie auf den Reiter **Datenausführungsverhinderung**.

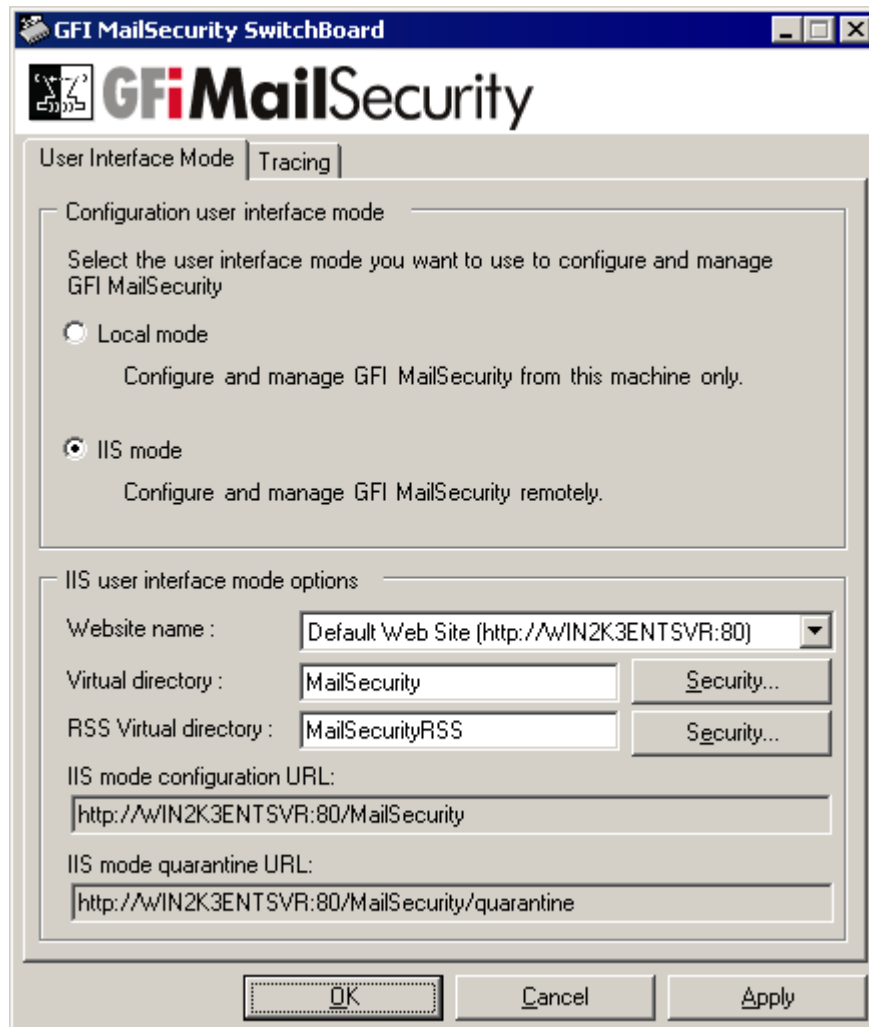
4. Wählen Sie das Optionsfeld **Datenausführungsverhinderung für alle Programme und Dienste mit Ausnahme der ausgewählten aktivieren**.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**, und navigieren Sie im aufgerufenen Dialogfeld zum Installationsverzeichnis von GFI MailSecurity, <GFI\ContentSecurity\MailSecurity>. Wählen Sie dort die Datei „GFIScanM.exe“ aus.
6. Klicken Sie auf die Schaltfläche **Hinzufügen**, und navigieren Sie im aufgerufenen Dialogfeld zum Installationsverzeichnis <GFI\ContentSecurity\AntiVirus\Kaspersky\>. Wählen Sie dort die Datei „kavss.exe“ aus.
7. Klicken Sie auf die Schaltflächen **Übernehmen** und dann auf **OK**, um die Änderungen zu übernehmen.
8. Führen Sie einen Neustart der Dienste „GFI Content Security Auto-Updater Service“ und „GFI MailSecurity Scan Engine“ durch.

Sichern des Zugriffs auf die Konfigurations-/Quarantäneseiten

Die Konfigurationsseiten und der Quarantänebereich von GFI MailSecurity lassen sich über einen Webbrowser aufrufen. Um eine unautorisierte Änderung von Einstellungen der Kontrollmodule und des Quarantänebereichs zu verhindern, muss der Zugriff auf diese Bereiche geschützt werden.

Die Konfigurierung der Zugriffsschutzes erfolgt über das GFI MailSecurity SwitchBoard. So konfigurieren Sie den Zugriffsschutz:

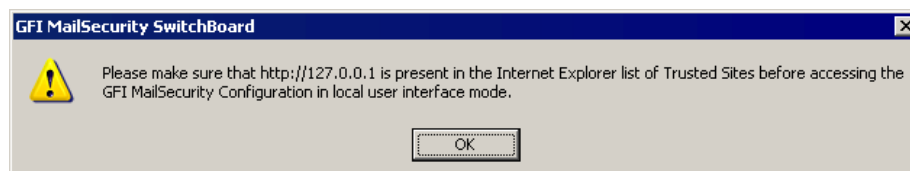
1. Gehen Sie auf **Start ▶ Programme ▶ GFI MailSecurity ▶ GFI MailSecurity SwitchBoard**.
2. Das GFI MailSecurity SwitchBoard wird aufgerufen. Wählen Sie, ob auf die Konfiguration und den Quarantänebereich nur lokal oder sowohl lokal als auch per Fernzugriff zugegriffen werden darf. Für den rein lokalen Zugriff wählen Sie die Option **Local mode**. Hierdurch kann auf die Konfiguration und den Quarantänebereich nur direkt vom Server aus zugegriffen werden, auf dem GFI MailSecurity installiert ist. Sollen autorisierte Benutzer sowohl lokal als auch per Fernzugriff auf die Konfiguration und den Quarantänebereich zugreifen können, wählen Sie die Option **IIS mode**.



Screenshot 11 – GFI MailSecurity SwitchBoard

3. Bei Auswahl der Option **Local mode** sind keine weiteren Einstellungen zu konfigurieren. Bei Auswahl der Option **IIS mode** hingegen sind die Active Directory-Konten oder -Gruppen zu bestimmen, die auf Konfiguration und Quarantänebereich zugreifen dürfen. Zudem kann der Name des virtuellen Verzeichnisses geändert werden, in dem die GFI MailSecurity-Seiten gespeichert sind.

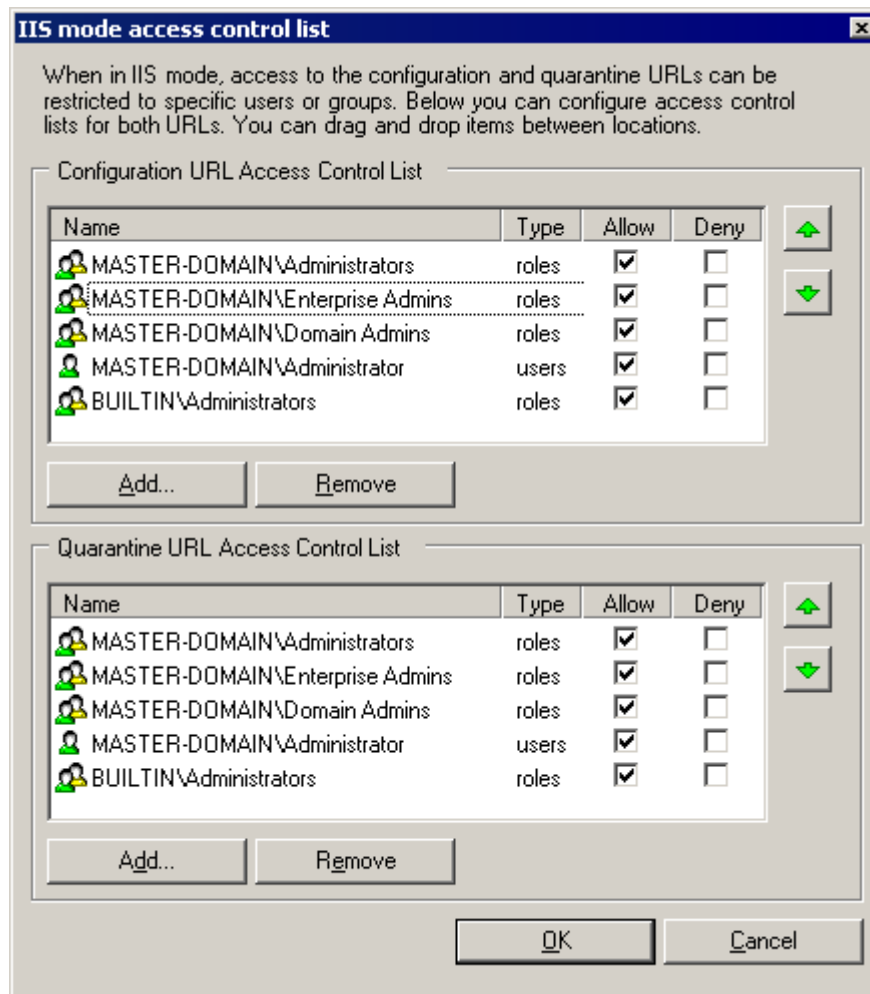
Hinweis: Bei Auswahl von **Local mode** muss im Microsoft Internet Explorer die Adresse „http://127.0.0.1“ der Liste der vertrauenswürdigen Sites hinzugefügt werden. Weitere Informationen hierzu erhalten Sie in diesem Kapitel unter „Hinzufügen des lokalen Hosts zur Liste der vertrauenswürdigen Sites“.



Screenshot 12 – Hinzufügen des lokalen Hosts zur Liste der vertrauenswürdigen Sites

4. Um den Zugriffsschutz zu konfigurieren, klicken Sie auf die Schaltfläche **Security ...** neben dem Eingabefeld **Virtual directory**.

5. Der Dialog **IIS mode access control list** wird angezeigt. Mit seiner Hilfe können Sie anhand verschiedener Zugriffskontrolllisten festlegen, welche Anwender auf die Konfigurationsseiten und den Quarantänebereich zugreifen dürfen.



Screenshot 13 – Zugriffskontrolllisten für Konfigurationsseiten/Quarantänebereich

6. Legen Sie im Bereich **Configuration URL Access Control List** fest, über welche Konten ein Zugriff auf die Konfigurationsseiten möglich sein soll. Mit den zugehörigen Schaltflächen **Add** und **Remove** können Sie Konten hinzufügen bzw. entfernen. Soll einem in der Liste aufgeführten Konto der Zugriff verweigert werden, ohne es aus der Liste zu entfernen, markieren Sie unter der Spalte **Deny** das zugehörige Kontrollkästchen.

7. Legen Sie im Bereich **Quarantine URL Access Control List** fest, über welche Konten ein Zugriff auf den Quarantänebereich möglich sein soll. Mit den zugehörigen Schaltflächen **Add** und **Remove** können Sie Konten hinzufügen bzw. entfernen. Soll einem in der Liste aufgeführten Konto der Zugriff verweigert werden, ohne es aus der Liste zu entfernen, markieren Sie unter der Spalte **Deny** das zugehörige Kontrollkästchen.

Hinweis: Konten und Gruppen lassen sich per Drag-and-Drop zwischen den beiden Listen verschieben.

8. Klicken Sie abschließend auf die Schaltfläche **OK**, um den Dialog zu schließen.

9. Geben Sie, falls notwendig, einen anderen Namen für das virtuelle Verzeichnis im Eingabefeld **Virtual directory** ein.

10. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern. Eine Fortschrittsanzeige informiert über die Verarbeitung der neuen Einstellungen.



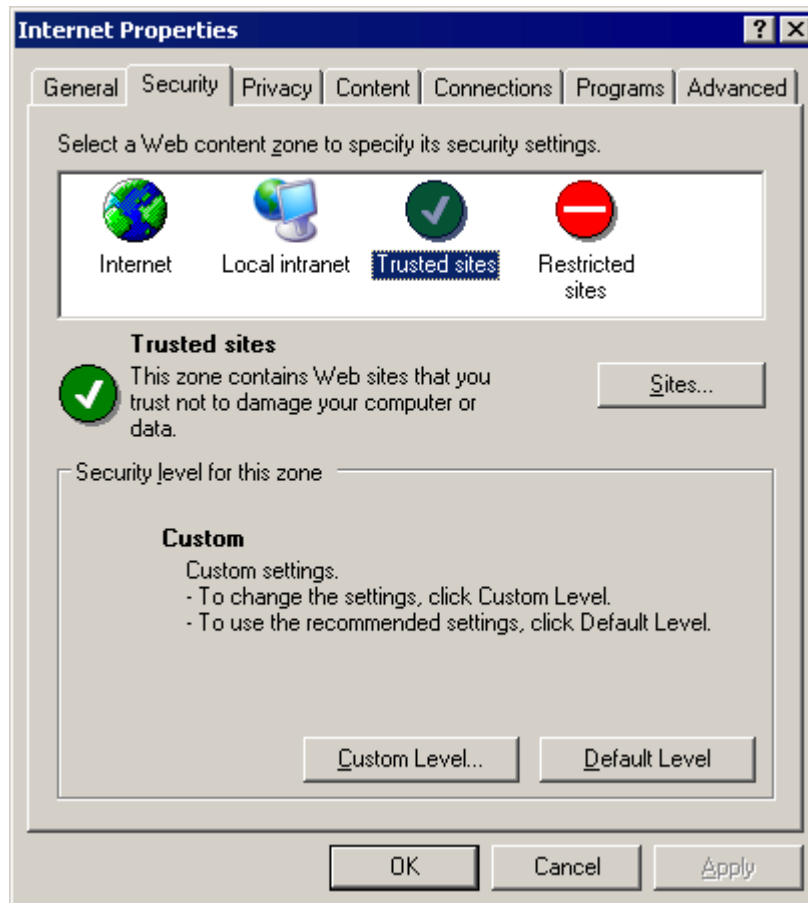
Screenshot 14 – Erfolgreiche Übernahme der SwitchBoard-Einstellungen

11. Klicken Sie nach Abschluss des Vorgangs auf die Schaltfläche **OK**.

Hinzufügen des lokalen Hosts zur Liste der vertrauenswürdigen Sites

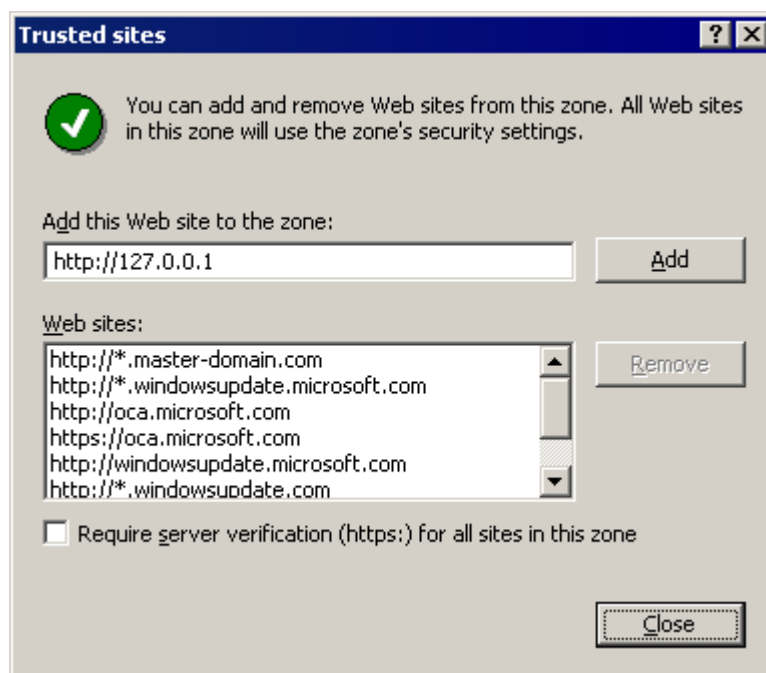
Soll ein Zugriff auf GFI MailSecurity nur lokal möglich sein, müssen Sie die Adresse des lokalen Hosts, „http://127.0.0.1“, im Microsoft Internet Explorer zur Liste der vertrauenswürdigen Sites hinzufügen. So geben Sie den Schlüssel ein:

1. Gehen Sie auf **Start ▶ Einstellungen ▶ Systemsteuerung**.
2. Gehen Sie in der **Systemsteuerung** auf das Applet **Internetoptionen**.
3. Das Dialogfenster **Eigenschaften von Internet** wird aufgerufen. Gehen Sie auf den Reiter **Sicherheit**, und markieren Sie in der Liste der Webinhaltszonen per Mausklick das Symbol **Vertrauenswürdige Sites**.



Screenshot 15 – Dialog „Eigenschaften von Internet“

4. Klicken Sie auf die Schaltfläche **Sites ...**
5. Das Dialogfenster **Vertrauenswürdige Sites** wird aufgerufen. Geben Sie im Eingabefeld zu **Diese Website zur Zone hinzufügen:** die Adresse "http://127.0.0.1" an.
6. Klicken Sie auf die Schaltfläche **Add**. Die Adresse des lokalen Hosts wird der Liste **Websites** hinzugefügt.



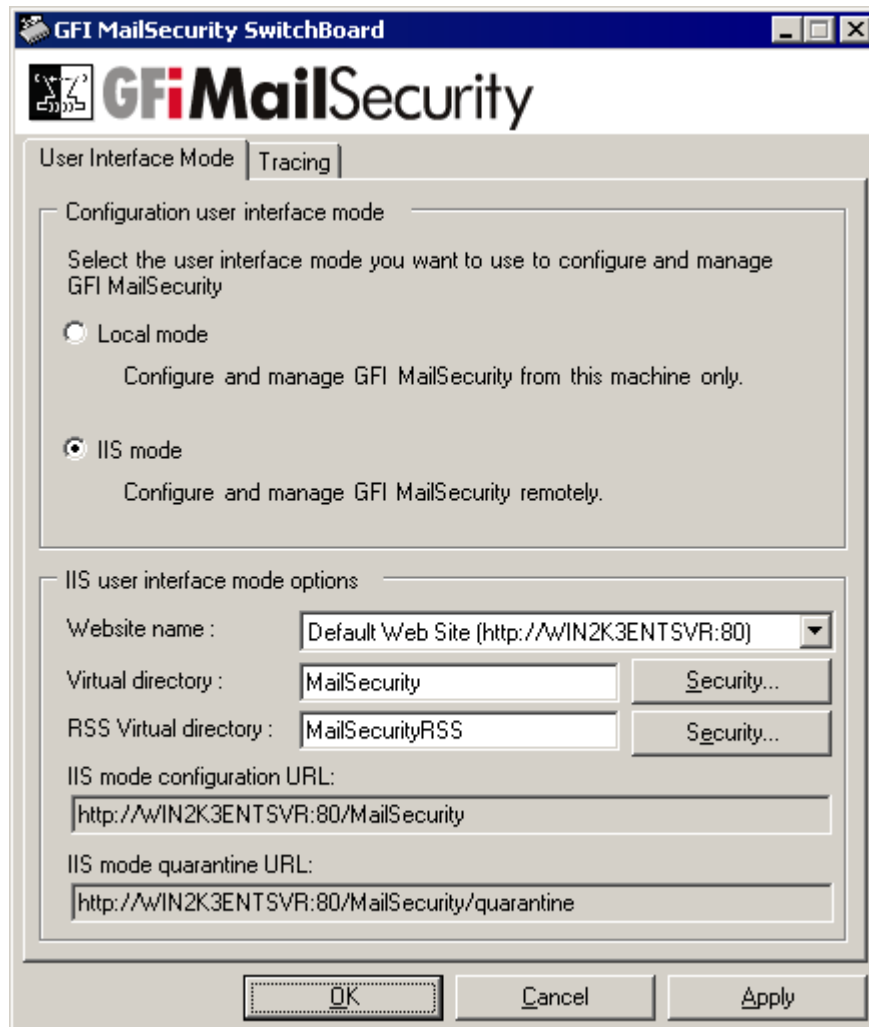
Screenshot 16 – Dialog „Vertrauenswürdige Sites“

7. Klicken Sie auf die Schaltfläche **Schließen**.
8. Klicken Sie im Dialog **Eigenschaften von Internet** auf die Schaltfläche **OK**, um die neue Einstellungen zu speichern und das Fenster zu schließen.

Sichern des Zugriffs auf RSS-Feeds des Quarantänebereichs

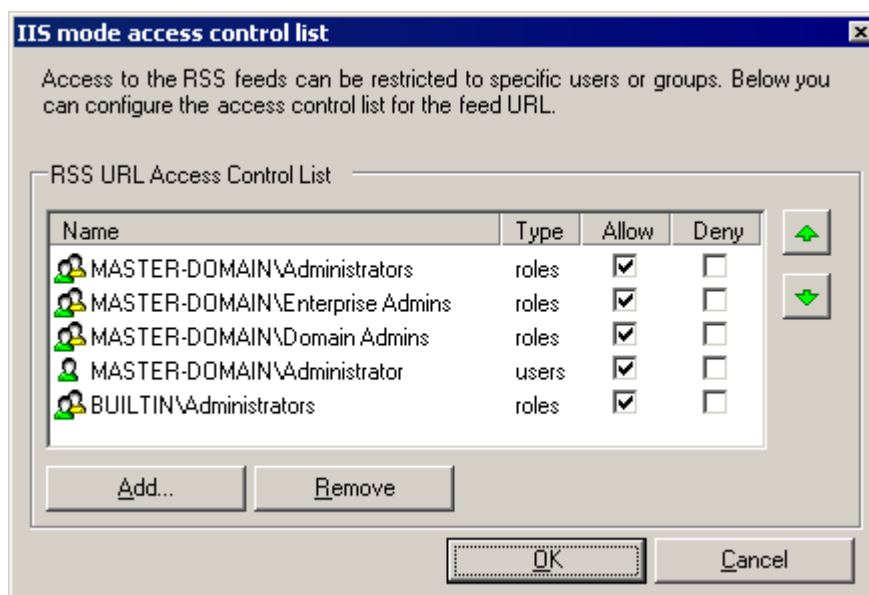
Sie können für einzelne Quarantäneordner RSS-Feeds zu darin abgelegten blockierten E-Mails erstellen lassen. So legen Sie fest, welche Benutzer diese RSS-Feeds abonnieren dürfen:

1. Gehen Sie auf **Start ▶ Programme ▶ GFI MailSecurity ▶ GFI MailSecurity SwitchBoard**.
2. Das GFI MailSecurity SwitchBoard wird aufgerufen.



Screenshot 17 – GFI MailSecurity SwitchBoard

3. Klicken Sie auf die Schaltfläche **Security...** neben dem Eingabefeld **RSS Virtual directory**.
4. Der Dialog **IIS mode access control list** wird angezeigt. Legen Sie fest, welche Benutzer die RSS-Feeds zum Quarantänebereich abonnieren dürfen.



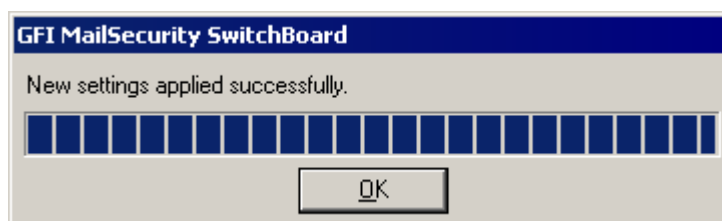
Screenshot 18 – Zugriffskontrollliste für RSS-Feeds

5. Mit den Schaltflächen **Add** und **Remove** können neue Abonnenten hinzugefügt bzw. entfernt werden. Soll einem in der Liste aufgeführten Konto der Zugriff verweigert werden, ohne es aus der Liste zu entfernen, markieren Sie unter der Spalte **Deny** das zugehörige Kontrollkästchen.

6. Klicken Sie abschließend auf die Schaltfläche **OK**, um den Dialog zu schließen.

7. Geben Sie, falls notwendig, im Eingabefeld **RSS Virtual directory** einen anderen Namen für das virtuelle Verzeichnis ein.

8. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern. Eine Fortschrittsanzeige informiert über die Verarbeitung der neuen Einstellungen.



Screenshot 19 – Erfolgreiche Übernahme der SwitchBoard-Einstellungen

9. Klicken Sie nach Abschluss des Vorgangs auf die Schaltfläche **OK**.

Zugreifen auf die Konfigurationsseiten und den Quarantänebereich

Nachfolgend erfahren Sie, wie die Konfigurationsseiten und der Quarantänebereich von GFI MailSecurity lokal oder per Fernzugriff abgerufen werden können.

Lokaler Zugriff über den GFI MailSecurity-Server

So greifen Sie lokal vom Server, auf dem GFI MailSecurity installiert ist, auf die Konfigurationsseiten oder den Quarantänebereich zu:

1. Gehen Sie auf **Start ▶ Programme ▶ GFI MailSecurity ▶ GFI MailSecurity**.

2. Wenn Sie GFI MailSecurity über das SwitchBoard nur für den lokalen Zugriff konfiguriert haben, öffnet sich automatisch ein Viewer, der die Konfigurationsoberfläche und den Quarantänebereich des Programms anzeigt.



Screenshot 20 – Lokaler Zugriff auf GFI MailSecurity

Fernzugriff auf die Konfigurationsseiten von GFI MailSecurity

So greifen Sie per Fernzugriff auf die Konfigurationsseiten oder den Quarantänebereich von GFI MailSecurity zu:

1. Starten Sie den Microsoft Internet Explorer.
2. Geben Sie in der Adressleiste folgende Adresse ein:

„<http://<Rechnername>/<Name des virtuellen Verzeichnisses>>“ für den Zugriff auf die Konfigurationsoberfläche oder „<http://<Rechnername>/<Name des virtuellen Verzeichnisses>/quarantine>“ für den direkten Zugriff auf den Quarantänebereich.

Beispiel:

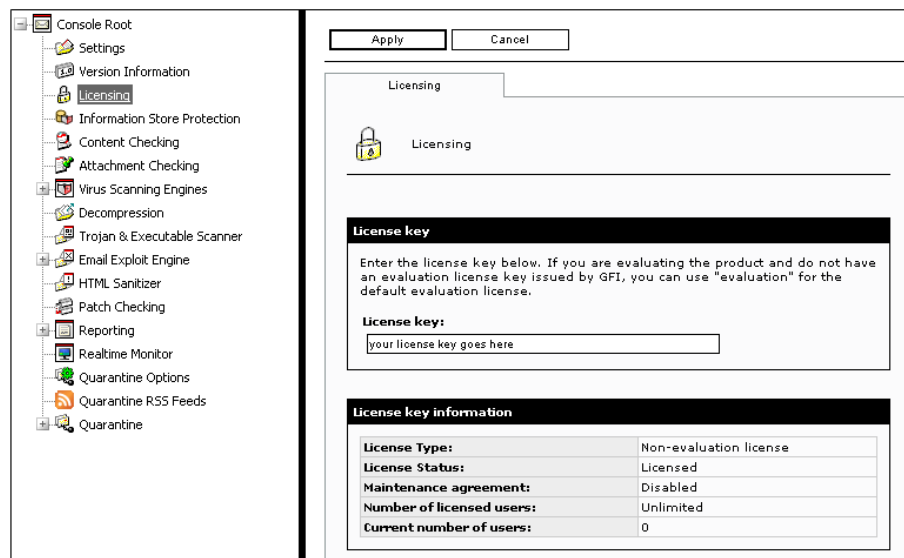
Geben Sie „<http://win2k3entsvr.master-domain.com/mailsecurity>“ für die Konfigurationsoberfläche oder „<http://win2k3entsvr.master-domain.com/mailsecurity/quarantine>“ für den Quarantänebereich ein.

3. Um sicherzustellen, dass Ihnen der Zugriff auf die angeforderte Seite gestattet ist, werden Sie zur Eingabe des entsprechenden Benutzernamens und Passworts aufgefordert. War die Authentifizierung erfolgreich, wird die Konfigurationsoberfläche oder der Quarantänebereich angezeigt.



Screenshot 21 – Fernzugriff auf GFI MailSecurity

Eingeben des Registrierschlüssels nach der Installation



Screenshot 22 – Daten des Registrierschlüssels

Wenn Sie GFI MailSecurity käuflich erworben haben, geben Sie den Registrierschlüssel ein, indem Sie unter **Console Root** auf den Knoten **Licensing** klicken.

Sollten Sie GFI MailSecurity mit einem Evaluierungsschlüssel testen, können Sie das Produkt nur zeitlich begrenzt einsetzen. Möchten Sie GFI MailSecurity nach Ablauf der Testdauer kaufen, brauchen Sie hier nur den endgültigen Registrierschlüssel eingeben, ohne das Produkt erneut installieren zu müssen.

Bitte verwechseln Sie die Eingabe des Registrierschlüssels nicht mit der Online-Registrierung Ihrer Firmendaten auf der GFI-Website. Die Registrierung ist wichtig, um Ihnen bei Problemen schneller helfen und Sie über wichtige Produktmitteilungen informieren zu können. Lassen Sie sich registrieren unter <http://www.gfisoftware.de/de/pages/regfrm.htm>.

Umstieg von GFI MailSecurity Version 8 auf Version 10

Grundlegende konzeptionelle Unterschiede zwischen GFI MailSecurity 8 und GFI MailSecurity 10 erlauben es Ihnen nicht, direkt von einer bereits installierten Version 8 auf die neue Version 10 umzusteigen.

Im Folgenden erfahren Sie, wie Sie

- eine vorhandene Installation von GFI MailSecurity 8 durch die neue Version 10 ersetzen,
- die Konfigurationseinstellungen von GFI MailSecurity 8 in das neue Format der Konfigurationsdatenbank von Version 10 migrieren.

Hinweis: Wurde GFI MailSecurity 8 im SMTP-Modus installiert, und ist für die neue Version 10 nun der Active Directory-Modus vorgesehen, können die Einstellungen aufgrund der anwenderbasierten Regeln nicht migriert werden. Gleiche Einschränkung gilt, wenn Version 8 im Active Directory-Modus installiert war und die neue Version 10 nun im SMTP-Modus eingerichtet werden soll.

So aktualisieren Sie GFI MailSecurity 8 auf GFI MailSecurity 10:

1. Deinstallieren Sie GFI MailSecurity 8.
2. Nach der Deinstallation von GFI MailSecurity 8 bleiben im Installationsverzeichnis dieser Version einige Dateien erhalten. Zu diesen Dateien zählt „avapicfg.rdb“, die sich im Unterverzeichnis „Data“ befindet.

Hinweis: Löschen Sie die Datei „avapicfg.rdb“ bitte nicht, da diese die Konfigurationseinstellungen von GFI MailSecurity 8 enthält. Diese werden für die Migration der Einstellungen von Version 8 auf Version 10 benötigt.

3. Installieren Sie GFI MailSecurity 10 wie in diesem Kapitel unter „Installieren von GFI MailSecurity“ beschrieben.

Hinweis: Für die Installation von GFI MailSecurity 10 sind auf dem Server erforderlich:

- Microsoft .NET Framework 1.1/2.0.
- MSMQ – Microsoft Messaging Queuing Service.
- Internet Information Services (IIS) – SMTP-Service und World Wide Web-Service

Hinweis: Installieren Sie GFI MailSecurity 10 nicht im selben Verzeichnis wie Version 8, um zu verhindern, dass für die Migration benötigte Konfigurationsdateien wie „avapicfg.rdb“ überschrieben werden.

4. Nach Abschluss der Installation von GFI MailSecurity 10 müssen Sie über **Systemsteuerung ▶ Verwaltung ▶ Dienste** alle GFI-bezogenen Dienste und den IIS Admin-Dienst beenden. Erst danach

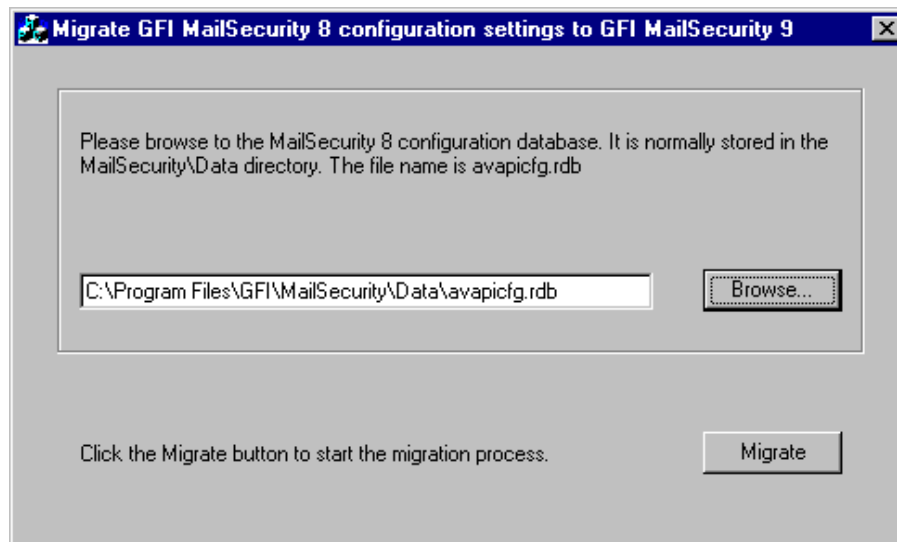
können Sie das Tool für die Migration der Einstellungen von GFI MailSecurity 8 starten.

Hinweis: Folgende Dienste müssen beendet werden, bevor Sie mit dem nächsten Schritt fortfahren:

- GFI Content Security Attendant Service
- GFI Content Security Auto-Updater Service
- GFI MailSecurity Attendant Service
- GFI MailSecurity Scan Engine
- IIS Admin
- Simple Mail Transfer Protocol (SMTP).

5. Um die Einstellungen von GFI MailSecurity 8 in die Konfigurationsdatenbank von GFI MailSecurity 10 zu migrieren, müssen Sie das Tool „msec8upg.exe“ starten. Es befindet sich im Installationsverzeichnis der Version 10, z. B. unter

c:\program files\GFI\ContentSecurity\MailSecurity.



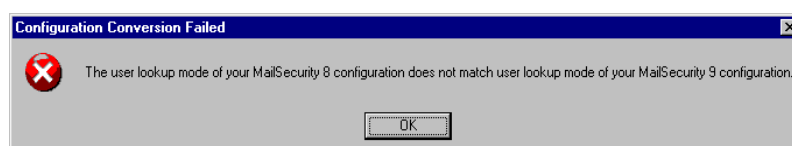
Screenshot 23 – Tool zur Migration von Konfigurationseinstellungen

6. Doppelklicken Sie auf die Datei „msec8upg.exe“.

7. Nachdem das Tool aufgerufen wurde, klicken Sie auf die Schaltfläche **Browse**. Navigieren Sie zum Unterverzeichnis „Data“ im Installationsverzeichnis von GFI MailSecurity 8, und wählen Sie dort die Datei „avapicfg.rdb“ aus.

8. Klicken Sie auf die Schaltfläche **Migrate**.

Hinweis: Stimmen der Anwender-Suchmodus von GFI MailSecurity 8 und GFI MailSecurity 10 nicht überein, z. B., weil Version 8 im SMTP-Modus und Version 10 im Active Directory-Modus installiert wurde oder umgekehrt, erscheint nachfolgende Fehlermeldung. In diesem Fall ist eine Migration der Einstellungen aufgrund der anwenderbasierten Regeln nicht möglich.



Screenshot 24 – Unterschiedlicher Anwender-Suchmodus

9. Ist der Migrationsvorgang abgeschlossen, wird die Meldung **Configuration was successfully converted** angezeigt. Klicken Sie auf die Schaltfläche **OK**, um den Dialog zu schließen. Klicken Sie danach auf das Symbol „Schließen“, um das Migrations-Tool zu schließen.

10. Starten Sie nun über das Applet **Dienste** alle in Schritt 4 beendeten Dienste.

11. Überprüfen Sie in der Konfiguration von GFI MailSecurity 10, ob alle Einstellungen von Version 8 korrekt übernommen wurden.

Hinweise zum Umstieg von GFI MailSecurity Version 9 auf 10

Hinweis: Eine Aktualisierung kann nicht rückgängig gemacht werden. Die Installation von Version 10 von GFI MailSecurity ist somit dauerhaft und kann nicht durch Version 9 ersetzt werden.

Wenn Sie zurzeit GFI MailSecurity 9 einsetzen, ist ein Upgrade auf Version 10 problemlos möglich. Die bereits in Version 9 festgelegten Konfigurationseinstellungen werden beibehalten. Nach Abschluss der Aktualisierung ist der käuflich erworbene Registrierschlüssel einzugeben. Weitere Informationen zum Erhalt des aktualisierten Schlüssels erhalten Sie unter <http://customers.gfi.com>.

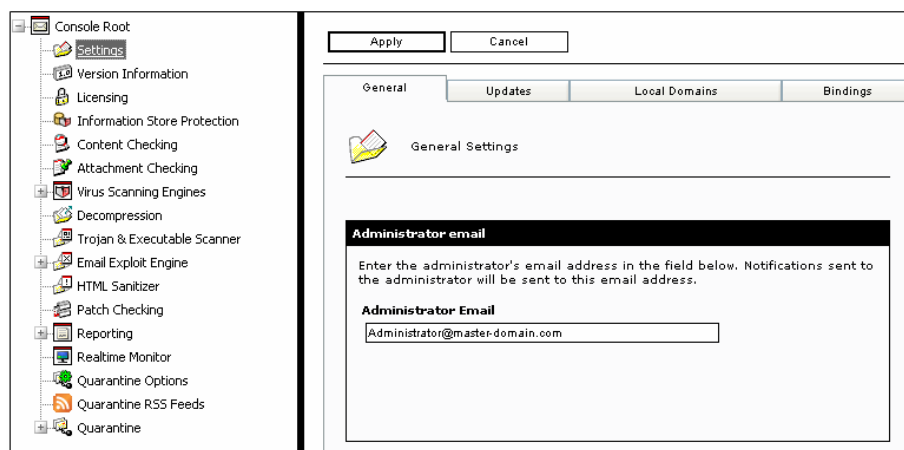
So aktualisieren Sie Ihr Produkt:

1. Rufen Sie das Setup-Programm von GFI MailSecurity 10 auf dem Server auf, auf dem die Software bereits installiert ist. Das Installationsprogramm fragt Sie, ob die aktuell installierte Version von GFI MailSecurity entfernt und die neue Version 10 installiert werden soll. Klicken Sie auf die Schaltfläche „**Yes**“.

2. Nach Ihrer Bestätigung erfolgt der Installationsablauf von GFI MailSecurity 10 wie bei einer neuen Installation der Software (siehe hierzu auch eine detaillierte Beschreibung unter „Installieren von GFI MailSecurity in diesem Kapitel“). Der Zielorder lässt sich jedoch nicht ändern.

Allgemeine Einstellungen

Einführung



Screenshot 25 – Allgemeine Einstellungen

Über den Knoten **Settings** können Sie mehrere allgemeine Einstellungen festlegen, darunter die E-Mail-Adresse des Administrators, die Update-URLs, alle lokale Domänen, die Bindungen zu SMTP-Servern sowie die Verwaltung der Benutzerliste, wenn GFI MailSecurity 10 im SMTP-Modus installiert wurde. Um die allgemeinen Einstellungen festzulegen, klicken Sie unter dem Knoten **Console Root** auf den Knoten **Settings**.

Angeben der E-Mail-Adresse des Administrators

Wird eine E-Mail durch eine Sicherheitsregel der Inhalts- oder Anhangskontrolle blockiert, kann GFI MailSecurity per E-Mail eine Benachrichtigung an den Administrator schicken. So legen Sie die Benachrichtigungsadresse fest:

1. Klicken Sie auf den Knoten **Settings**, um im rechten Fenster die allgemeinen Einstellungen aufzurufen.
2. Der Reiter **General** wird angezeigt. Geben Sie im Eingabefeld **Administrator Email** die E-Mail-Adresse für Benachrichtigungen an den Administrator ein.
3. Klicken Sie auf die Schaltfläche **Apply** links über dem Reiter, um die Einstellungen zu übernehmen.

Auswählen des Update-Servers

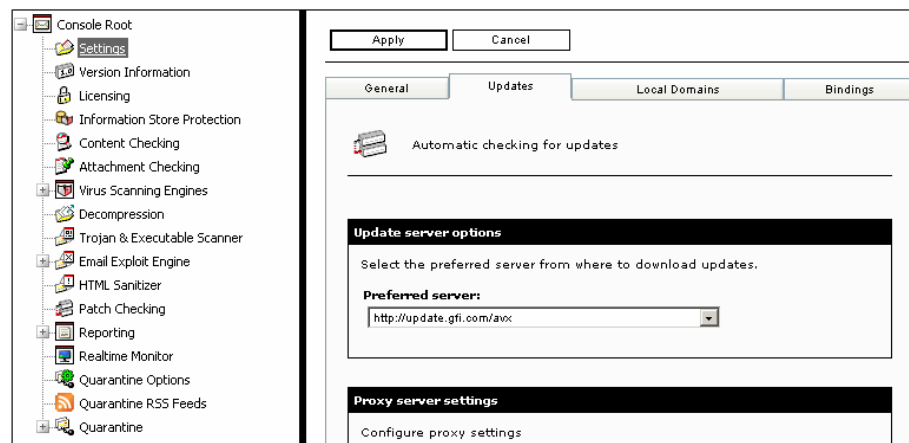
GFI MailSecurity kann automatisch nach sicherheitsrelevanten Updates suchen (z. B. von Virendefinitionen und Definitionsdateien für

den Trojan & Executable Scanner) und diese vom angegebenen GFI-Server herunterladen. So wählen Sie den gewünschten Update-Server aus:

1. Klicken Sie auf den Knoten **Settings**, um die allgemeinen Einstellungen aufzurufen.

2. Klicken Sie auf den Reiter **Updates**, und wählen Sie aus der Liste **Preferred server** den von Ihnen gewünschten GFI Update-Server aus.

- <http://update.gfi.com> – Wählen Sie diesen Server, wenn Sie sich in den USA/Kanada befinden.
- <http://update.gfisoftware.com> – Wählen Sie diesen Server, wenn Sie sich in Europa oder anderen Teilen der Welt befinden.



Screenshot 26 – Angabe allgemeiner Update-Einstellungen

3. Erfolgt die Verbindung über einen Proxy-Server, markieren Sie das Kontrollkästchen **Enabled proxy server**. Geben Sie in den Eingabefeldern **Proxy server** und **Port** den Namen/die IP-Adresse des Proxy-Servers und den Port an. Erfordert der Proxy-Server eine Authentifizierung, markieren Sie das Kontrollkästchen **Enable proxy authentication**, und geben Sie in den Eingabefeldern **Username** und **Password** die entsprechenden Daten ein.

Proxy server settings

Configure proxy settings

Enable proxy server

Proxy server:

Port:

Proxy authentication settings

Configure proxy authentication settings

Enable proxy authentication

Username:

Password:

* For security reasons, the length in the password box above does not necessarily reflect the true password length

Screenshot 27 – Proxy-Einstellungen für Updates

4. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern. Die Änderungen sind sofort gültig.

Hinzufügen lokaler Domänen

- Console Root
- Settings
- Version Information
- Licensing
- Information Store Protection
- Content Checking
- Attachment Checking
- Virus Scanning Engines
- Decompression
- Trojan & Executable Scanner
- Email Exploit Engine
- HTML Sanitizer
- Patch Checking
- Reporting
- Realtime Monitor
- Quarantine Options
- Quarantine RSS Feeds
- Quarantine

General
Updates
Local Domains
Bindings

Local Domains

Configure local domains

Domain:

Local domains list:

master-domain.com	<input type="button" value="Remove"/>
-------------------	---------------------------------------

Screenshot 28 – Liste lokaler Domänen

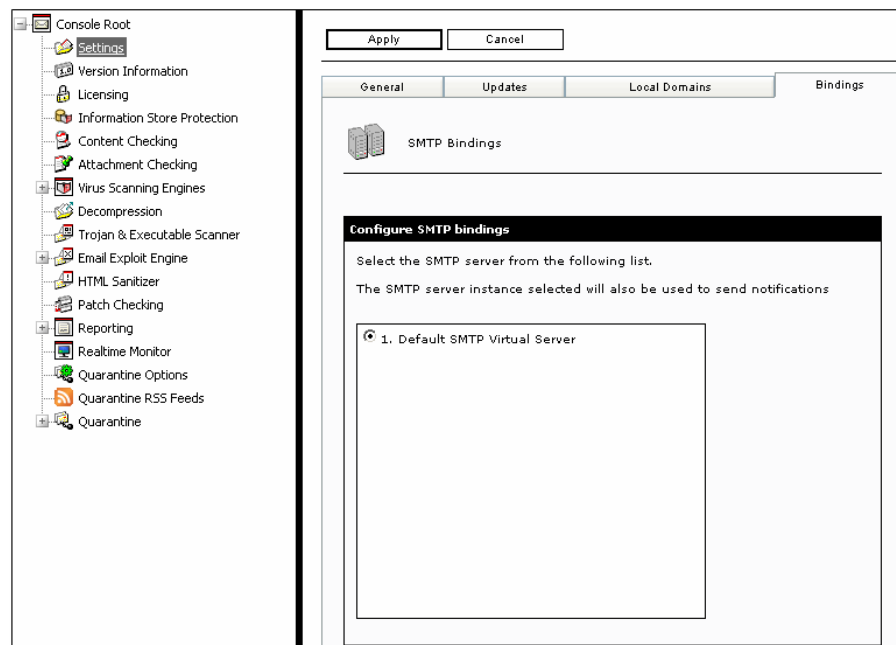
GFI MailSecurity benötigt genaue Angaben zu allen Ihren lokalen Domänen, um zwischen ein- und ausgehender Post unterscheiden zu können. Bei der Installation importiert GFI MailSecurity die lokalen

Domänen aus dem IIS SMTP-Dienst. Wenn Sie jedoch zu einem späteren Zeitpunkt lokale Domänen hinzufügen oder entfernen wollen, gehen Sie wie folgt vor:

1. Klicken Sie auf den Knoten **Settings**, um die allgemeinen Einstellungen aufzurufen.
2. Klicken Sie auf den Reiter **Local Domains**, und geben Sie im Eingabefeld **Domain** den Namen der Domäne an.
3. Klicken Sie auf die Schaltfläche **Add**, um die angegebene Domäne zur Liste der lokalen Domänen hinzuzufügen. Soll eine Domäne hingegen entfernt werden, können Sie diese durch Markierung des Namens in der Liste auswählen und per Mausklick auf **Remove** entfernen.
4. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Änderungen zu bestätigen.

Hinweis: Diese Funktion kann verwendet werden, wenn in den IIS das lokale E-Mail-Routing verändert wird. Dies ist beispielsweise der Fall, wenn Domänen hinzugefügt werden sollen, die für die Weitergabe von E-Mails als lokal gelten, für Ihren E-Mail-Server jedoch nicht.

Bindungen an SMTP-Server



Screenshot 29 – Bindung von GFI MailSecurity an einen anderen SMTP-Server

GFI MailSecurity setzt den SMTP-Dienst der IIS für den Versand und Empfang von SMTP-Mails ein. Als Vorgabe erfolgt die Bindung an Ihren standardmäßigen virtuellen SMTP-Server. Sind jedoch mehrere virtuelle SMTP-Server installiert, können Sie bestimmen, an welchen GFI MailSecurity gebunden werden soll. Der virtuelle SMTP-Server kann während der Installation und zu einem späteren Zeitpunkt über den Reiter **Bindings** geändert werden.

So ändern Sie den aktuellen virtuellen SMTP-Server:

1. Klicken Sie auf den Knoten **Settings**, um im rechten Fenster die allgemeinen Einstellungen zu konfigurieren.

2. Klicken Sie auf den Reiter **Bindings**, und wählen Sie den gewünschten virtuellen SMTP-Server aus der Liste der in Ihrer Domäne verfügbaren Server aus.

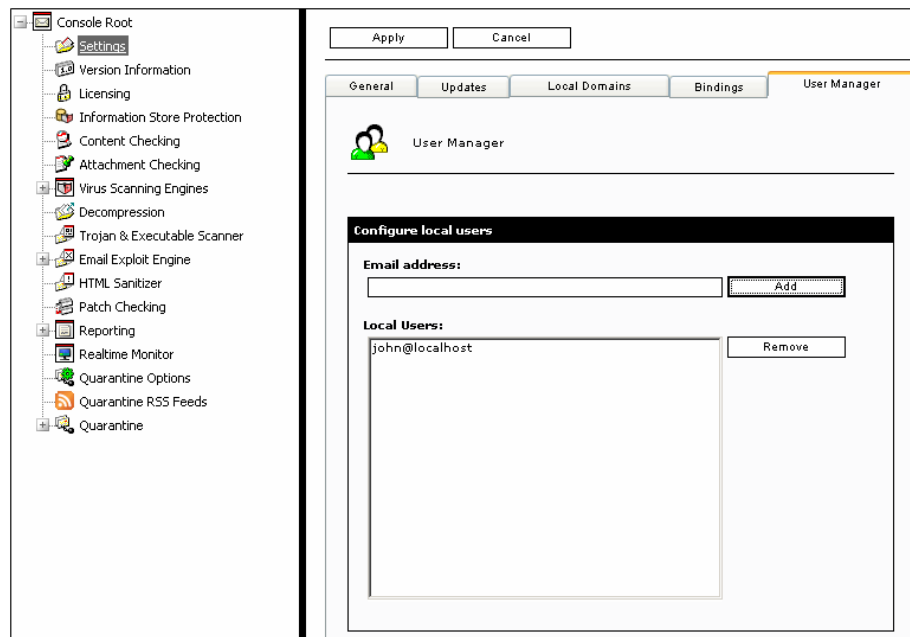
3. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Auswahl zu bestätigen.

Weitere Informationen zu den Einstellungen des SMTP-Diensts erhalten Sie im Kapitel „Installieren und Konfigurieren des IIS SMTP- und World Wide Web-Diensts“ in diesem Handbuch.

Verwalten lokaler Anwender im SMTP-Modus

Bei Installation von GFI MailSecurity im Active Directory-Modus wird die Liste der lokalen Anwender im Active Directory-Speicher gesichert. Bei der Installation von GFI MailSecurity im SMTP-Modus hingegen wird die Liste der lokalen Anwender in einer von GFI MailSecurity verwalteten Datenbank gesichert.

Zur Erweiterung und Verwaltung der Anwenderliste steht im SMTP-Modus von GFI MailSecurity unter dem Knoten **Settings** die Option **User Manager** zur Verfügung.



Screenshot 30 – User Manager

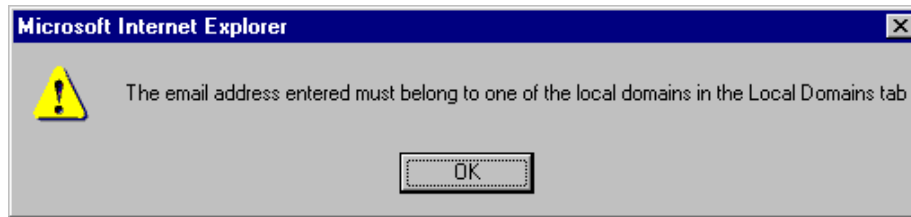
Unter dem Reiter **User Manager** wird eine Liste aller aktuellen lokalen Anwender angezeigt. Sie können Einträge hinzufügen oder löschen. Die Liste der lokalen Anwender wird für die Konfigurierung anwenderbasierter Regeln, z. B. zur Anhangskontrolle oder Inhaltskontrolle, verwendet.

Hinzufügen eines neuen lokalen Anwenders

1. Geben Sie im Eingabefeld **Email address** die E-Mail-Adresse ein.
2. Klicken Sie auf die Schaltfläche **Add**.

Hinweis: GFI MailSecurity bestimmt über die Liste der lokalen Domänen, die über den Reiter **Local Domains** konfiguriert wird, ob eine neue E-Mail-Adresse lokal ist oder nicht. Wird die Adresse eines nicht lokalen Anwenders eingegeben, erscheint folgende Auffor-

derung, in der Sie zur Eingabe von Adressen gebeten werden, die zu einer der lokalen Domänen gehören.



Screenshot 31 – Hinweis bei Eingabe nicht lokaler Anwender

3. Wiederholen Sie Schritte 1 und 2, um mehr als einen lokalen Anwender hinzuzufügen.
4. Klicken Sie auf die Schaltfläche **Apply**, um die Einstellungen zu speichern.

Entfernen eines lokalen Anwenders

1. Wählen Sie den zu entfernenden Anwender aus der Liste **Local Users** aus.
2. Klicken Sie auf die Schaltfläche **Remove**.
3. Wiederholen Sie Schritte 1 und 2, um mehr als einen lokalen Anwender zu entfernen.
4. Klicken Sie auf die Schaltfläche **Apply**, um die Einstellungen zu speichern.

Konfigurieren der Virenprüfung

Konfigurieren der Viren-Scan-Engines

GFI MailSecurity überprüft sämtliche ein- und ausgehenden E-Mails, den gesamten SMTP-Datenverkehr, mit mehreren Viren-Scan-Engines auf Schadteile. Ist GFI MailSecurity auf dem Microsoft Exchange-Server installiert, kann die Sicherheitslösung auch den Informationsspeicher auf Viren kontrollieren. Standardmäßig wird die Software mit den Viren-Scan-Engines von Norman und BitDefender ausgeliefert. Zusätzlich können Sie Lizenzen für die Engines von GRISOFT, Kaspersky und McAfee erwerben und gemeinsam mit den anderen beiden Lösungen einsetzen. Bei allen unterstützten Anti-Viren-Paketen handelt es sich um renommierte und leistungsfähige Engines, die zahlreiche Auszeichnungen und branchenführende Zertifizierungen erhalten haben, darunter auch von der ICSA.

Engine	Status	License	Priority		
AVG Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	0	▲	▼
BitDefender Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	1	▲	▼
Norman Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	2	▲	▼
McAfee Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	3	▲	▼
Kaspersky Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	4	▲	▼

Virus Scanning Optimizations

Stop virus scanning the current item, if viruses are detected by:
virus scanners

Stop scanning even for non-virus related threats.

Screenshot 32 – Statusseite der Viren-Scan-Engines

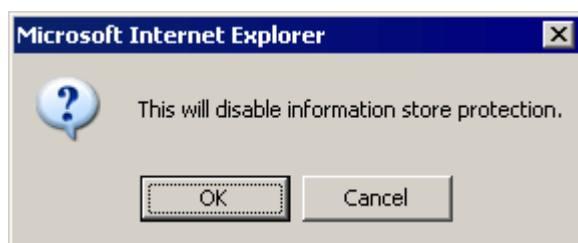
Der Betriebs- und Lizenzstatus jeder Scan-Engine sowie die Kontrollreihenfolge der installierten Scan-Engines können unter **Console Root** über den Knoten **Virus Scanning Engines** abgerufen werden.

Im rechten Fenster wird die Statusseite angezeigt, in der die Engines in der Reihenfolge aufgeführt sind, in der sie von GFI MailSecurity zum Scannen von E-Mails eingesetzt werden (d. h. nach ihrer Priorität, wobei „0“ die höchste Priorität bezeichnet).

Jede Viren-Scan-Engine muss einzeln konfiguriert werden. Klicken Sie hierfür auf der rechten Statusseite auf die entsprechende Engine.

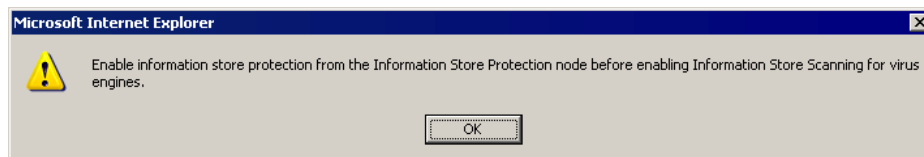
Alternativ können Sie auch den Knoten **Virus Scanning Engines** erweitern und dann nach einem Mausklick auf die jeweilige Engine die Einstellungen vornehmen.

Hinweis: Läuft GFI MailSecurity auf einem Exchange-Server, und wird der Scan-Status von **Information Store Scanning** bei allen Viren-Scan-Engines auf **Disabled**, d. h. deaktiviert, gesetzt, werden die Informationsspeicher-Scans komplett deaktiviert. Es muss somit bei mindestens einer der Scan-Engines das **Information Store Scanning** aktiviert sein, damit der Informationsspeicher kontrolliert wird. Falls Sie auch bei der letzten entsprechend aktivierten Engine das Scannen des Informationsspeichers deaktivieren, weist Sie GFI MailSecurity gesondert darauf hin, dass hierdurch der Informationsspeicher nicht länger überprüft wird. Wenn Sie im eingeblendeten Dialog auf die Schaltfläche **OK** klicken, wird die Scan-Funktion der einzigen für die Informationsspeicher-Kontrolle konfigurierten Scan-Engine deaktiviert und somit die gesamte Kontrolle des Informationsspeichers! Klicken Sie im selben Dialog auf die Schaltfläche **Cancel**, werden keine Änderungen vorgenommen, und die Scan-Funktion für den Informationsspeicher bleibt übergreifend aktiv.



Screenshot 33 – Deaktivierung der Informationsspeicher-Kontrolle

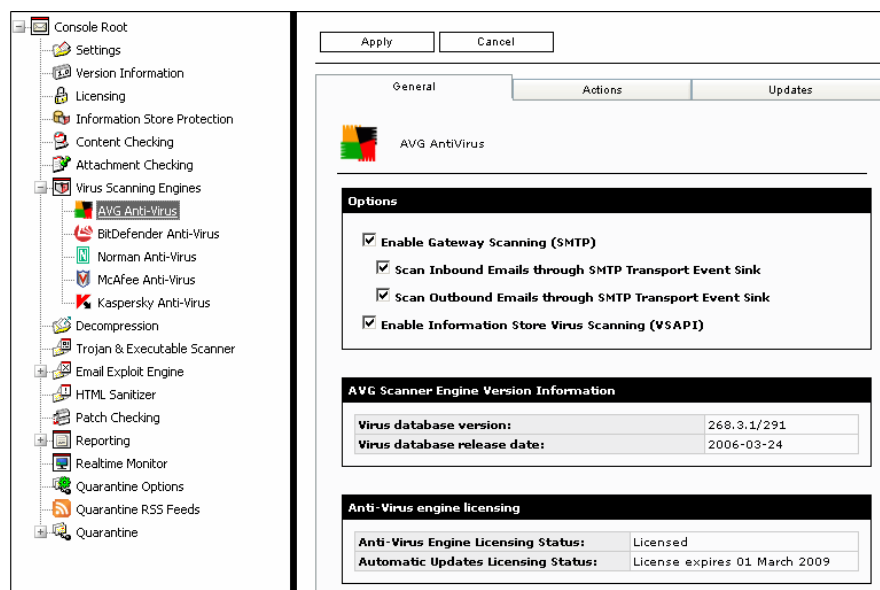
Ist die Funktion **Information Store Scanning** übergreifend deaktiviert, muss sie zuerst über den Knoten **Information Store Protection** aktiviert werden, bevor über die Viren-Scan-Engines die Kontrolle des Informationsspeichers konfiguriert werden kann. Sollten Sie versuchen, über eine Viren-Scan-Engine das Scannen des Informationsspeichers zu aktivieren, wenn diese Funktion über den Knoten **Information Store Protection** deaktiviert wurde, erhalten Sie hierüber folgende Meldung:



Screenshot 34 – Erforderliche vorherige Aktivierung des Informationsspeicher-Schutzes vor Konfigurierung einer Viren-Scan-Engine

Konfigurieren der GRISOFT AVG-Engine

Hinweis: Die Anti-Viren-Engine von GRISOFT muss separat erworben werden. Sie ist nicht im standardmäßigen Lieferumfang von GFI MailSecurity enthalten. Zum standardmäßigen Lieferumfang von GFI MailSecurity zählen nur die Anti-Viren-Engines von Norman und BitDefender. Weitere Informationen und Preisangaben zur GRISOFT-Engine finden Sie auf der GFI-Website unter www.gfisoftware.de.



Screenshot 35 – Viren-Scan-Engines: GRISOFT AVG-Konfigurationsseite (Reiter „General“)

So konfigurieren Sie die GRISOFT AVG-Engine:

1. Erweitern Sie unter **Console Root** den Knoten **Virus Scanning Engines**, und klicken Sie auf **AVG**.

2. Um mit Hilfe dieser Viren-Scan-Engine die SMTP-Kommunikation zu kontrollieren, markieren Sie das Kontrollkästchen **Enable Gateway Scanning (SMTP)**. Wählen Sie nun aus, ob mit dieser Engine ein- und/oder ausgehende E-Mails gescannt werden sollen. Um eingehende Nachrichten scannen zu lassen, markieren Sie das Kontrollkästchen **Scan Inbound Emails through SMTP Transport Event Sink**. Um ausgehende Nachrichten scannen zu lassen, markieren Sie das Kontrollkästchen **Scan Outbound Emails through SMTP Transport Event Sink**.

3. Ist GFI MailSecurity auf dem Exchange-Server installiert, haben Sie zudem die Möglichkeit, mit dieser Viren-Scan-Engine den Exchange-Informationsspeicher kontrollieren zu lassen. Um den Informationsspeicher scannen zu lassen, markieren Sie das Kontrollkästchen **Enable Information Store Virus Scanning (VSAPI)**.

4. Die über die Reiter **Actions** und **Updates** festzulegenden Konfigurationseinstellungen sind für alle installierten Viren-Scan-Engines gleich. Weitere Informationen zur Konfigurierung dieser Parameter erhalten Sie in diesem Kapitel unter „Vorgehensweise bei Virenbefall“ und „Updates für den Viren-Scanner“.

5. Nachdem Sie alle notwendigen Parameter festgelegt haben, klicken Sie auf die Schaltfläche **Apply**, um die Einstellungen zu übernehmen. Alle Änderungen und Einstellungen sind sofort gültig.

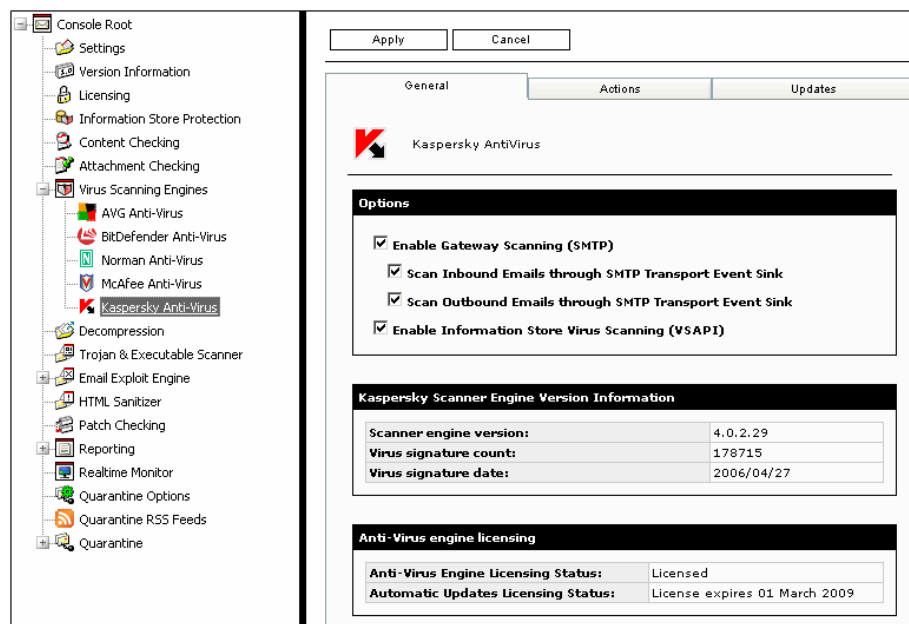
Hinweis: Im unteren Bereich des Reiters **General** erhalten Sie Informationen zur Scan-Engine. Hierzu zählen die Versionsnummer der Virendatenbank und deren Veröffentlichungsdatum. Lizenzangaben zur aktuellen Anti-Viren-Engine werden ebenfalls angezeigt.

Website von GRISOFT

Weitere Informationen zu den Virensignaturen der GRISOFT-Engine finden Sie auf der Website des Unternehmens unter <http://www.grisoft.de/>.

Konfigurieren der Kaspersky-Engine

Hinweis: Die Anti-Viren-Engine von Kaspersky muss separat erworben werden. Sie ist nicht im standardmäßigen Lieferumfang von GFI MailSecurity enthalten. Zum standardmäßigen Lieferumfang von GFI MailSecurity zählen nur die Anti-Viren-Engines von Norman und BitDefender. Weitere Informationen und Preisangaben zur Kaspersky-Engine finden Sie auf der GFI-Website unter www.gfi-software.de.



Screenshot 36 – Viren-Scan-Engines: Kaspersky-Konfigurationsseite (Reiter „General“)

So konfigurieren Sie die Kaspersky-Engine:

1. Erweitern Sie unter **Console Root** den Knoten **Virus Scanning Engines**, und klicken Sie auf **Kaspersky**.
2. Um mit Hilfe dieser Viren-Scan-Engine die SMTP-Kommunikation zu kontrollieren, markieren Sie das Kontrollkästchen **Enable Gateway Scanning (SMTP)**. Wählen Sie nun aus, ob mit dieser Engine ein- und/oder ausgehende E-Mails gescannt werden sollen. Um eingehende Nachrichten scannen zu lassen, markieren Sie das Kontrollkästchen **Scan Inbound Emails through SMTP Transport Event Sink**. Um ausgehende Nachrichten scannen zu lassen, markieren Sie das Kontrollkästchen **Scan Outbound Emails through SMTP Transport Event Sink**.
3. Ist GFI MailSecurity auf dem Exchange-Server installiert, haben Sie zudem die Möglichkeit, mit dieser Viren-Scan-Engine den Exchange-Informationsspeicher kontrollieren zu lassen. Um den Informationsspeicher scannen zu lassen, markieren Sie das Kontrollkästchen **Enable Information Store Virus Scanning (VSAPI)**.
4. Die über die Reiter **Actions** und **Updates** festzulegenden Konfigurationseinstellungen sind für alle installierten Viren-Scan-

Engines gleich. Weitere Informationen zur Konfigurierung dieser Parameter erhalten Sie in diesem Kapitel unter „Vorgehensweise bei Virenbefall“ und „Updates für den Viren-Scanner“.

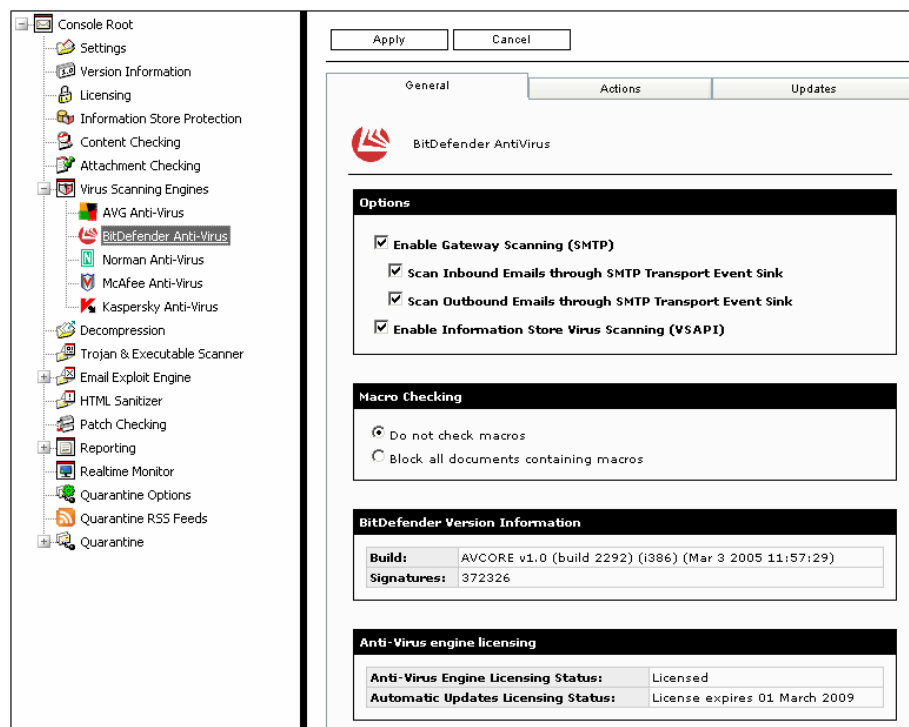
5. Nachdem Sie alle notwendigen Parameter festgelegt haben, klicken Sie auf die Schaltfläche **Apply**, um die Einstellungen zu übernehmen. Alle Änderungen und Einstellungen sind sofort gültig.

Hinweis: Im unteren Bereich des Reiters **General** erhalten Sie Informationen zur Scan-Engine. Hierzu zählen die Versionsnummer der Scan-Engine, die Anzahl der Virensignaturen und das Datum der aktuellen Virendefinitionen. Lizenzangaben zur aktuellen Anti-Viren-Engine werden ebenfalls angezeigt.

Website von Kaspersky

Weitere Informationen zu den Virensignaturen der Kaspersky-Engine finden Sie auf der Website des Unternehmens unter <http://www.kaspersky.com>.

Konfigurieren der BitDefender-Engine



Screenshot 37 – Viren-Scan-Engines: BitDefender-Konfigurationsseite (Reiter „General“)

So konfigurieren Sie die BitDefender-Engine:

1. Erweitern Sie unter **Console Root** den Knoten **Virus Scanning Engines**, und klicken Sie auf **BitDefender**.

2. Um mit Hilfe dieser Viren-Scan-Engine die SMTP-Kommunikation zu kontrollieren, markieren Sie das Kontrollkästchen **Enable Gateway Scanning (SMTP)**. Wählen Sie nun aus, ob mit dieser Engine ein- und/oder ausgehende E-Mails gescannt werden sollen. Um eingehende Nachrichten scannen zu lassen, markieren Sie das Kontrollkästchen **Scan Inbound Emails through SMTP Transport Event Sink**. Um ausgehende Nachrichten scannen zu lassen, markieren Sie

das Kontrollkästchen **Scan Outbound Emails through SMTP Transport Event Sink**.

3. Ist GFI MailSecurity auf dem Exchange-Server installiert, haben Sie zudem die Möglichkeit, mit dieser Viren-Scan-Engine den Exchange-Informationsspeicher kontrollieren zu lassen. Um den Informationsspeicher scannen zu lassen, markieren Sie das Kontrollkästchen **Enable Information Store Virus Scanning (VSAPI)**.

4. Mit BitDefender können Sie zudem E-Mails, die Anhänge mit Makros enthalten, blockieren. Konfigurieren Sie diese Funktion durch Auswahl einer der folgenden Optionen:

- **Do not check macros** – Durch Auswahl dieser Option ignoriert GFI MailSecurity alle Makros und überprüft E-Mails nur auf Viren.
- **Block all documents containing macros** – Durch Auswahl dieser Option werden alle E-Mails mit Makros unter Quarantäne gestellt (selbst wenn es sich um Original-Makros handelt).

Hinweis: Das Unter-Quarantäne-Stellen von E-Mails hängt von den in der Scan-Engine konfigurierten Aktionen ab. Ist die Option **Delete item** über den Reiter **Actions** der Scan-Engine ausgewählt, werden alle E-Mails mit Makros ungeachtet der gewählten Makro-Einstellung GELÖSCHT, d. h. nicht unter Quarantäne gestellt.

5. Die über die Reiter **Actions** und **Updates** festzulegenden Konfigurationseinstellungen sind für alle installierten Viren-Scan-Engines gleich. Weitere Informationen zur Konfigurierung dieser Parameter erhalten Sie in diesem Kapitel unter „Vorgehensweise bei Virenbefall“ und „Updates für den Viren-Scanner“.

6. Nachdem Sie alle notwendigen Parameter festgelegt haben, klicken Sie auf die Schaltfläche **Apply**, um die Einstellungen zu übernehmen. Alle Änderungen und Einstellungen sind sofort gültig.

Hinweis: Im unteren Bereich des Reiters **General** erhalten Sie Informationen zur Scan-Engine. Hierzu zählen die Versionsnummer der Scan-Engine und die Anzahl der Virensignaturen. Lizenzangaben zur aktuellen Anti-Viren-Engine werden ebenfalls angezeigt.

Website von BitDefender

Weitere Informationen zu den Virensignaturen der BitDefender-Engine finden Sie auf der Website des Unternehmens unter <http://www.bitdefender.com>

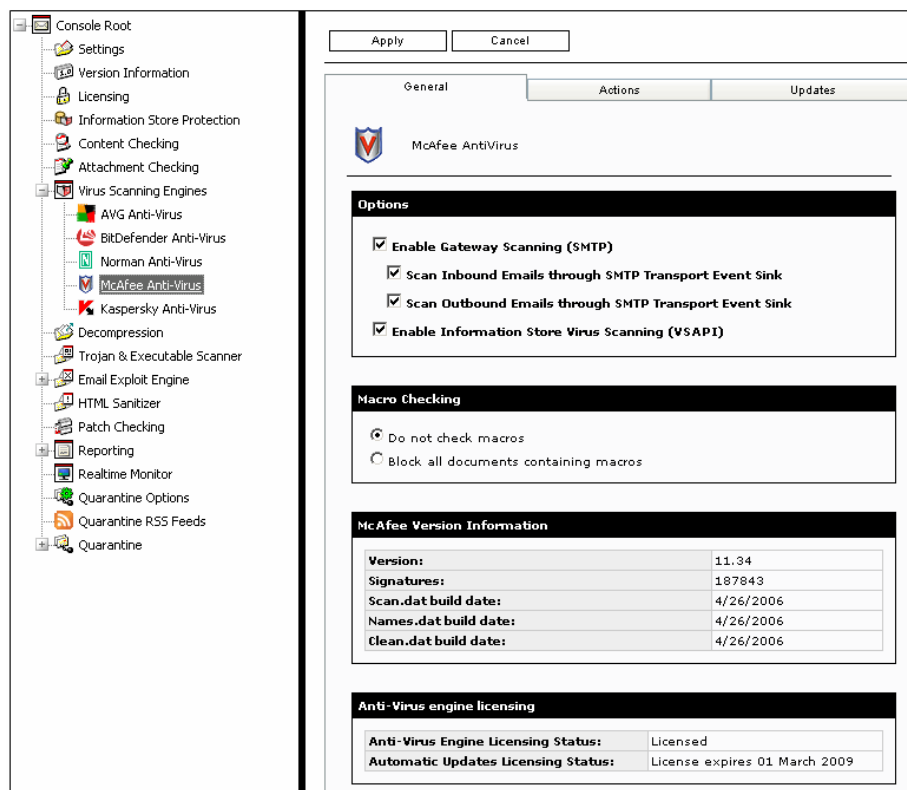
Konfigurieren der McAfee-Engine

Hinweis: Die McAfee-Engine muss gesondert erworben werden, da sie nicht im standardmäßigen Lieferumfang von GFI MailSecurity enthalten ist. GFI MailSecurity wird mit den Anti-Viren-Engines von Norman und BitDefender ausgeliefert. Weitere Informationen und Preisangaben zur McAfee-Engine finden Sie auf der GFI-Website unter www.gfi.com.

Die Konfigurationsoptionen für die Scan-Engine von McAfee gleichen denen von BitDefender. Weitere Informationen zur Konfigurierung dieser Optionen erhalten Sie unter „Konfigurieren der BitDefender-Engine“.

Hinweis: Im unteren Bereich des Reiters **General** erhalten Sie Informationen zur Scan-Engine. Hierzu zählen die Versionsnummer

der Scan-Engine, die Anzahl der Virensignaturen und das Datum der aktuellen Virendefinitionen. Lizenzangaben zur aktuellen Anti-Viren-Engine werden ebenfalls angezeigt.



Screenshot 38 – Viren-Scan-Engines: McAfee-Konfigurationsseite (Reiter „General“)

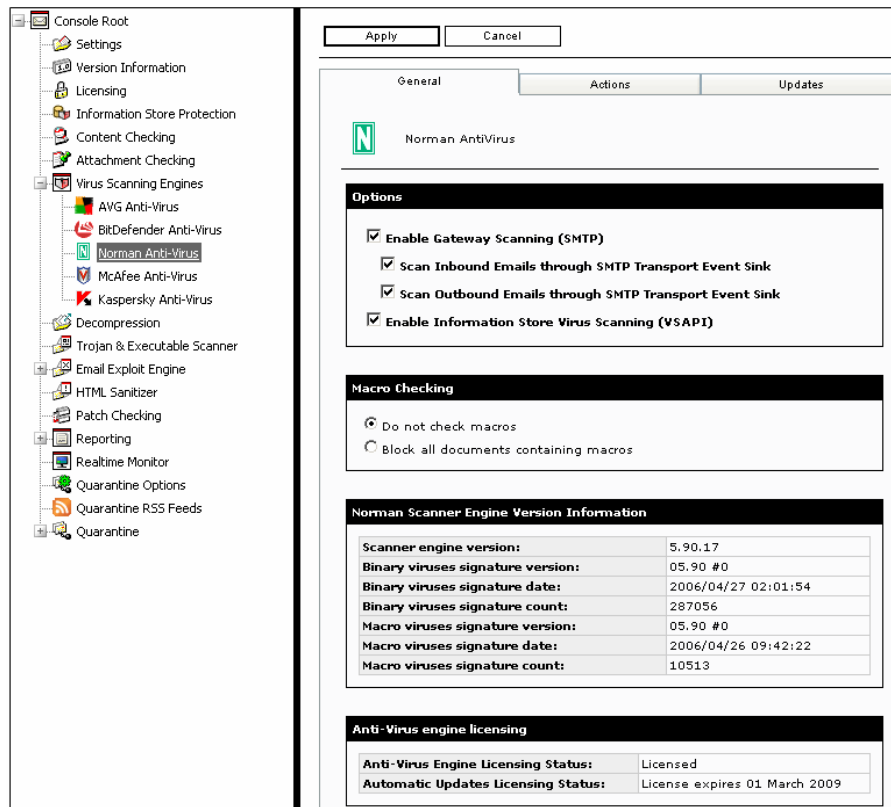
Website von McAfee

Weitere Informationen zu den Virensignaturen der McAfee-Engine finden Sie auf der Website des Unternehmens unter <http://www.mcafee.de>

Konfigurieren der Norman-Engine

Die Konfigurationsoptionen für die Viren-Scan-Engine von Norman gleichen denen von BitDefender. Weitere Informationen zur Konfigurierung dieser Optionen erhalten Sie unter „Konfigurieren der BitDefender-Engine“.

Hinweis: Im unteren Bereich des Reiters **General** erhalten Sie Informationen zur Scan-Engine. Hierzu zählen die Versionsnummer der Scan-Engine, die Anzahl der Virensignaturen und das Datum der aktuellen Virendefinitionen. Lizenzangaben zur aktuellen Anti-Viren-Engine werden ebenfalls angezeigt.

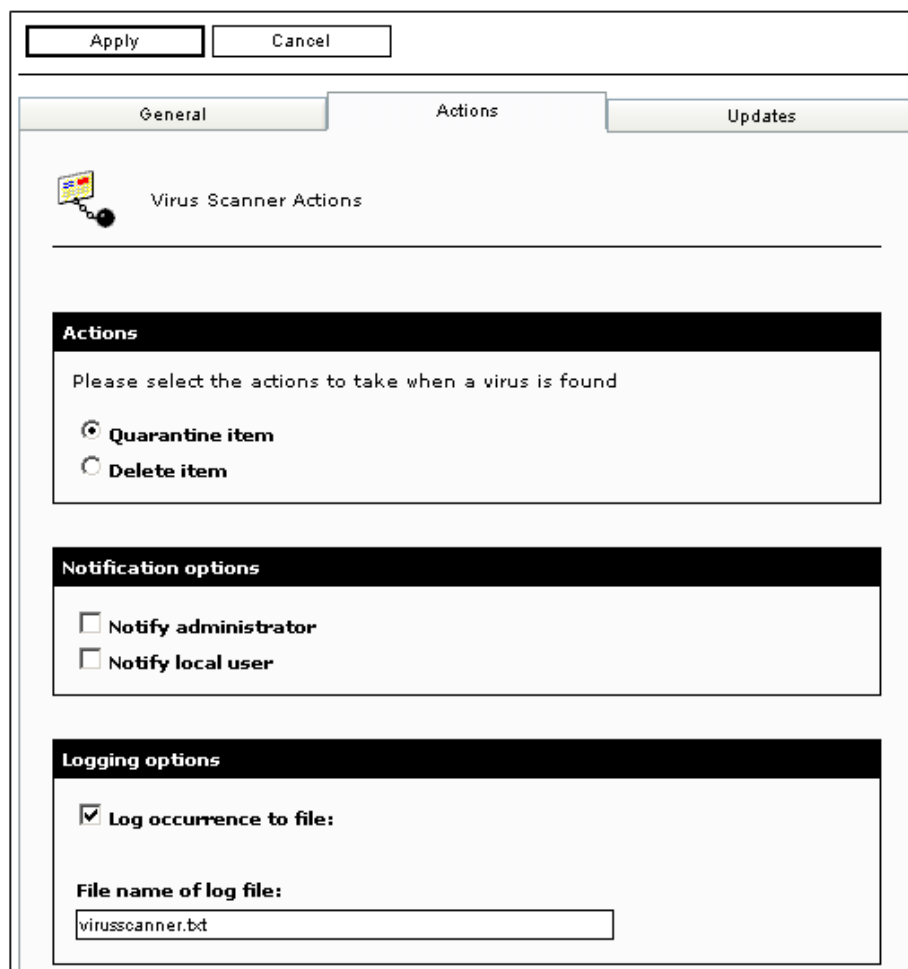


Screenshot 39 – Viren-Scan-Engines: Norman-Konfigurationsseite (Reiter „General“)

Website von Norman

Weitere Informationen zu den Virensignaturen von Norman Virus Control (NVC) finden Sie auf der Website des Unternehmens unter <http://www.norman.com>

Vorgehensweise bei Virenbefall



Screenshot 40 – Viren-Scan-Engine: Konfigurationsseite (Reiter „Actions“)

Legen Sie in GFI MailSecurity fest, wie die einzelnen installierten Scan-Engines vorgehen sollen, wenn eine infizierte E-Mail entdeckt wird. So konfigurieren Sie die Vorgehensweise bei Virenbefall:

1. Wählen Sie den zu konfigurierenden Viren-Scanner aus, und klicken Sie auf den Reiter **Actions**.
2. Wählen Sie eine der folgenden Optionen:
 - **Quarantine item** – Stellt alle von dieser Scan-Engine als infiziert klassifizierten E-Mails unter Quarantäne. Alle Quarantäne-E-Mails können nach der Überprüfung durch den Administrator freigegeben oder gelöscht werden.
 - **Delete item** – Löscht alle von dieser Scan-Engine als infiziert klassifizierten E-Mails.

Hinweis: Diese Option hebt die über den Reiter **General** vorgenommenen Einstellungen auf. Wenn Sie im Reiter **General** die Option **Block all emails containing a macro** ausgewählt haben, jedoch gleichzeitig die Option **Delete item** gewählt wurde, werden ALLE Mitteilungen mit Makros somit gelöscht.

3. Um bei Erkennung einer infizierten Nachricht eine E-Mail-Benachrichtigung zu verschicken, stehen Ihnen folgende Optionen zur Verfügung:

- **Notify local user** – Informiert den Empfänger der Mitteilung, wenn eine an ihn gerichtete (eingehende) Mitteilung vom Viren-Scanner als infiziert erkannt wurde. Soll eine infizierte/blockierte E-Mail verschickt werden, erfolgt ebenfalls eine entsprechende Benachrichtigung über die Infizierung an den Absender.
 - **Notify administrator** – Informiert den Administrator, wenn eine Mitteilung vom Viren-Scanner als infiziert erkannt wurde.
4. Wählen Sie die Option **Log occurrence to file**, wenn die Aktivitäten des Viren-Scanners in einer Protokolldatei gesichert werden sollen. Geben Sie den Namen der Protokolldatei im Eingabefeld **File name of log file** ein.

Updates für den Viren-Scanner

The screenshot displays the 'Updates' configuration tab for the Viren-Scanner. It is divided into two main sections: 'Automatic update options' and 'Update options'. In the 'Automatic update options' section, the 'Automatically check for updates' checkbox is checked. The 'Downloading option' dropdown is set to 'Check for updates and download'. The 'Download/check after the specified number of hours' field contains the value '1'. The 'Last update' status is 'Never'. The 'Update options' section has the 'Enable email notifications upon successful updates' checkbox checked. A 'Download updates' button is visible at the bottom of this section.

Screenshot 41 – Viren-Scan-Engines: Konfigurationsseite (Reiter „Updates“)

Legen Sie in GFI MailSecurity fest, dass Signatur-Updates für den Viren-Scanner automatisch heruntergeladen werden sollen, oder lassen Sie eine Administratornachricht verschicken, sobald neue Updates verfügbar sind. So konfigurieren Sie die Einstellungen für automatische Viren-Scanner-Updates:

1. Wählen Sie den zu konfigurierenden Viren-Scanner aus, und klicken Sie im rechten Fenster auf den Reiter **Updates**.

2. Wählen Sie die Option **Automatically check for updates**, wenn die Aktualisierung der Signatur-Updates automatisch erfolgen soll.

3. Wählen Sie aus der Liste **Downloading options** eine der folgenden Optionen aus:

- **Only check for updates** – GFI MailSecurity überprüft lediglich, ob für den gewählten Viren-Scanner Updates zur Verfügung stehen, um dann den Administrator darüber zu benachrichtigen.

Hinweis: Bei Auswahl dieser Option erfolgt KEIN Download eventuell verfügbarer Updates.

- **Check for updates and download** – GFI MailSecurity überprüft, ob für den gewählten Viren-Scanner neue Updates zur Verfügung stehen, um diese dann automatisch herunterzuladen.

4. Legen Sie fest, wie in welchem zeitlichen Abstand GFI MailSecurity nach Updates für den Viren-Scanner suchen und diese downloaden soll (Angabe in Stunden).






Manueller Abruf von Updates

Um sofort nach Updates für den Viren-Scanner zu suchen und diese herunterzuladen, klicken Sie auf die Schaltfläche **Download updates**.

Festlegen der Scan-Priorität der einzelnen Viren-Scan-Engines

So ändern Sie die Reihenfolge, in der die verschiedenen Viren-Scan-Engines zur Kontrolle von E-Mails eingesetzt werden:

1. Klicken Sie unter **Console Root** auf den Knoten **Virus Scanning Engines**.

Engine	Status	License	Priority		
 AVG Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	0	▲	▼
 BitDefender Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	1	▲	▼
 Norman Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	2	▲	▼
 McAfee Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	3	▲	▼
 Kaspersky Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	4	▲	▼

Screenshot 42 – Viren-Scan-Engines: Übersicht über Engine-Priorität

2. Im rechten Fenster werden die Viren-Scan-Engines ihrer Priorität nach in absteigender Reihenfolge angezeigt.

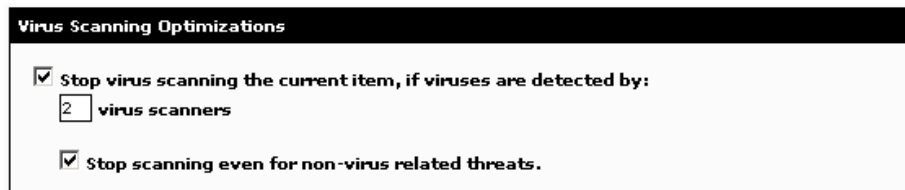
Hinweis: Die Reihenfolge, in der die verschiedenen Scanner zur Kontrolle von E-Mails eingesetzt werden, wird durch die Scanner-Priorität bestimmt, die sich für jeden Scanner einzeln festlegen lässt. E-Mails werden vom Scanner mit der Priorität „0“ als erstes überprüft. Danach erfolgt die Kontrolle mit dem Scanner, der die Priorität „1“ besitzt, usw. Der Scanner an oberster Stelle der Liste kontrolliert E-Mails somit als erstes, sofern er aktiviert wurde.

3. Um die Priorität eines Viren-Scanners zu erhöhen oder zu senken, klicken Sie im rechten Fenster neben dem entsprechenden Scanner auf den Nach-oben-Pfeil oder Nach-unten-Pfeil. Wiederholen Sie diesen Vorgang, bis der Viren-Scanner die gewünschte Priorität in der Liste einnimmt.

Optimieren von Viren-Scan-Aktionen

Unter **Console Root** kann über den Knoten **Virus Scanning Engines** festgelegt werden, dass GFI MailSecurity keinen weiteren Scan einer E-Mail durchführen soll, wenn diese bereits zuvor von mehreren Scannern als infiziert erkannt worden ist.

Aktivieren Sie diese Option, indem Sie das Kontrollkästchen **Stop virus scanning the current item, if viruses are detected by X virus scanners** markieren. Geben Sie die Anzahl der Viren-Scanner an, von denen eine E-Mail als infiziert klassifiziert worden sein muss, bevor Scans dieser Nachricht mit den weiteren Engines eingestellt werden. Klicken Sie auf die Schaltfläche **Apply**.



Screenshot 43 – Optimierung von Viren-Scans

Bei Auswahl dieser Option unter Angabe des Werts „2“ muss beispielsweise eine E-Mail von maximal zwei Engines als infiziert klassifiziert worden sein, bevor eine Kontrolle der Nachricht durch die übrigen Engines eingestellt wird. E-Mails, bei denen kein Virus festgestellt wurde, passieren alle aktivierten Viren-Scanner.

Für E-Mails, die als vireniniziert erkannt wurden, kann zudem der nachfolgende Scan-Ablauf gestrafft werden. Wählen Sie hierfür die Option **Stop scanning even for non-virus related threats**, und klicken Sie auf die Schaltfläche **Apply**. Hierbei stellt GFI MailSecurity die zusätzliche Kontrolle einer E-Mail durch weitere Module wie die Anhangskontrolle ein, wenn die Nachricht bereits von den Viren-Scannern als gefährlich erkannt worden ist.

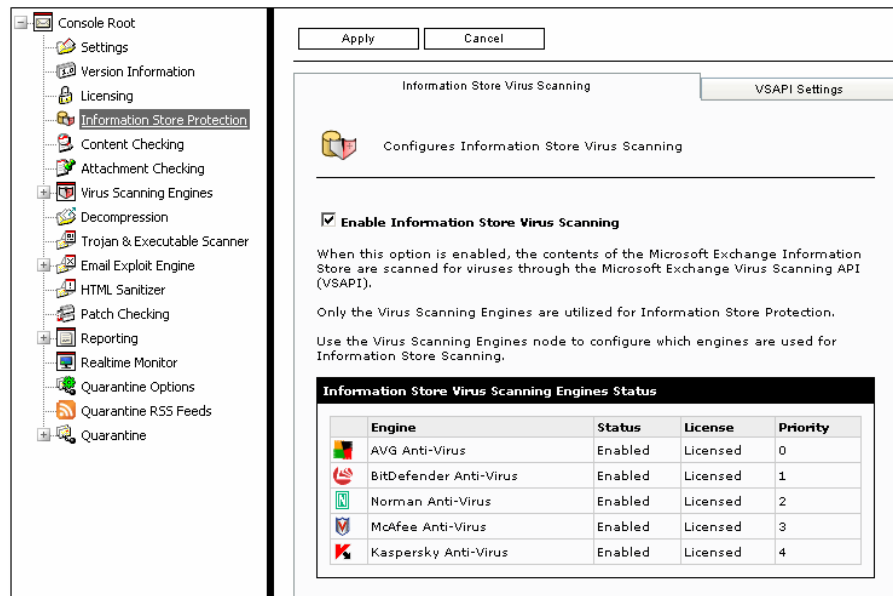
Konfigurieren von Informationsspeicher-Scans

Hinweis: Ein Zugriff auf den Knoten **Information Store Protection** ist nur dann möglich, wenn GFI MailSecurity auf dem Exchange-Server installiert ist.

Im folgenden Unterkapitel erfahren Sie, wie Informationsspeicher-Scans (Information Store Scanning) aktiviert oder deaktiviert werden können und welche Scan-Methoden unter VS API (Virus Scanning API) verfügbar sind.

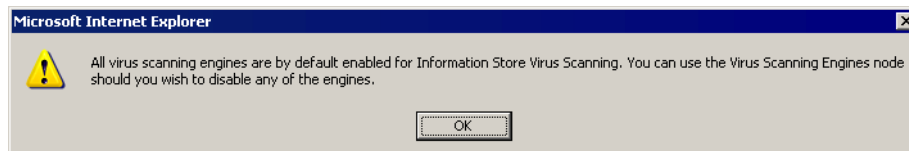
So konfigurieren Sie die Funktion **Information Store Scanning**:

1. Klicken Sie unter **Console Root** auf den Knoten **Information Store Protection**.
2. Im rechten Fenster wird standardmäßig der Reiter **Information Store Virus Scanning** angezeigt. Legen Sie fest, ob das Scannen der Exchange-Informationsspeicher aktiviert werden soll, indem Sie das Kontrollkästchen **Enable Information Store Virus Scanning** markieren. Der Status der einzelnen Viren-Scan-Engines, die zum Scannen des Informationsspeichers verwendet werden können, wird ebenfalls angezeigt.



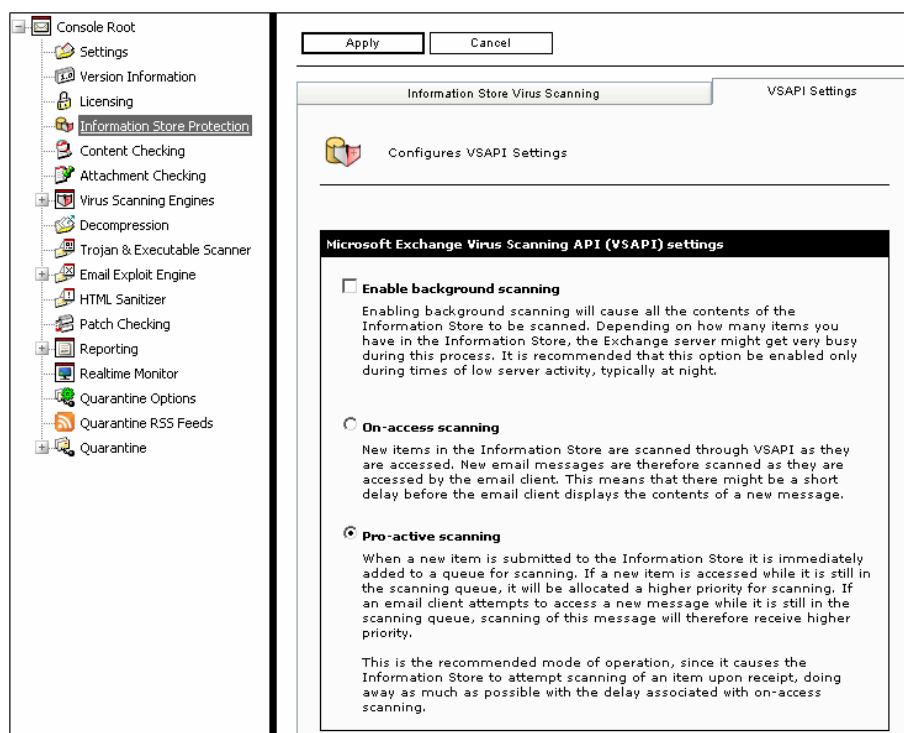
Screenshot 44 – Knoten “Information Store Protection”

Hinweis: Wenn Sie das Scannen des Informationsspeichers deaktivieren, wird diese Option übergreifend automatisch für alle Viren-Scan-Engines außer Funktion gesetzt. Wenn Sie das Scannen des Informationsspeichers aktivieren, wird diese Option ebenso übergreifend automatisch für alle Viren-Scan-Engines aktiviert. GFI MailSecurity informiert Sie über eine übergreifende Aktivierung automatisch mit nachfolgender Nachricht. Informationen, wie die Option zum Scannen des Informationsspeichers für eine einzelne Viren-Scan-Engine aktiviert oder deaktiviert wird, erhalten Sie im Kapitel „Konfigurieren der Viren-Scan-Engines“.



Screenshot 45 – Übergreifende Aktivierung der Option für Informationsspeicher-Scans

3. Legen Sie die im VS API-Modus zu verwendende Scan-Methode fest, indem Sie auf den Reiter **VSAPI Settings** gehen.



Screenshot 46 – VS API Scan-Einstellungen

4. Über den Reiter **VSAPI Settings** können Sie Hintergrund-Scans des Informationsspeichers aktivieren, indem Sie das Kontrollkästchen **Enable background scanning** markieren. Hierdurch werden alle Inhalte des Informationsspeichers gescannt. Bitte beachten Sie, dass diese Kontrolle, je nach Anzahl der im Informationsspeicher vorhandenen Elemente, zu einer hohen Beanspruchung des Exchange-Servers führen kann. Diese Option sollte daher nur dann aktiviert werden, wenn die Auslastung des Servers gering ist, beispielsweise während der Nachtstunden.

5. Wählen Sie eine der folgenden VS API-Scan-Methoden aus:

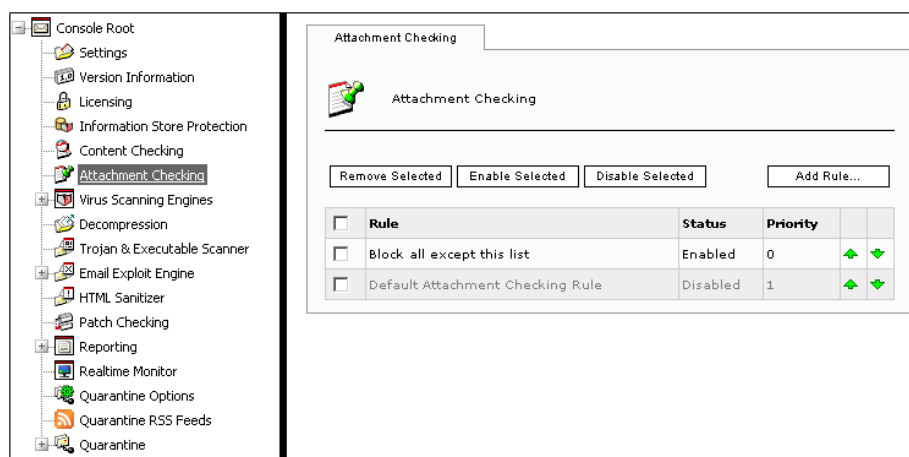
- **On-access scanning** – Neue Elemente im Informationsspeicher werden erst gescannt, wenn sie vom E-Mail-Client abgerufen werden. Bei dieser Scan-Methode besteht vor der Anzeige der neuen Mitteilung aufgrund des Scans eine kurze Verzögerung.
- **Pro-active scanning** – Dem Informationsspeicher neu hinzugefügte Elemente werden in eine Warteschlange gestellt, um gescannt zu werden. Versucht ein E-Mail-Client auf ein Element zuzugreifen, das sich noch in der Warteschlange befindet, wird diesem Element eine höhere Scan-Priorität zugewiesen, damit es schnellstmöglich kontrolliert wird. Dieser voreingestellte Modus sollte beibehalten werden, da hierdurch die beim On-Access-Scanning entstehende Verzögerung in den meisten Fällen vermieden werden kann. Neue Elemente werden sofort der Warteschlange hinzugefügt und sind beim Abruf durch einen E-Mail-Client meistens bereits kontrolliert worden.

6. Klicken Sie auf die Schaltfläche **Apply**, damit GFI MailSecurity die neuen Einstellungen speichert.

Konfigurieren der Anhangskontrolle

Einführung

In diesem Kapitel wird erklärt, wie Sie die Anhangskontrolle zur Überprüfung von Anhängen durch GFI MailSecurity konfigurieren. Die Anhangskontrolle ermöglicht es Ihnen Richtlinien zu erstellen, welche Arten von E-Mail-Anhängen auf Ihren E-Mail-Server gelangen dürfen. Zur Einrichtung einer Richtlinie verwendet GFI MailSecurity Regeln. Mit einer Regel können Sie z. B. festlegen, dass alle Dateianhänge blockiert werden sollen, bei denen es sich um ausführbare Programme handelt. Mit einer Regel zur Anhangskontrolle wiederum können Sie Anhänge eines bestimmten Typs blockieren.



Screenshot 47 – Anhangskontrolle

Die Regeln zur Anhangskontrolle werden über den Knoten **Attachment Checking** konfiguriert. Er bietet Ihnen Optionen, mit denen Sie Regeln erstellen, löschen, aktivieren oder deaktivieren können. Zudem werden alle bereits vorhandenen Kontrollregeln aufgeführt, inklusive ihres Status und der Reihenfolge (Priorität), in der sie auf E-Mails angewandt werden.

Erstellen einer Regel zur Anhangskontrolle

So erstellen Sie eine Regel zur Anhangskontrolle:

1. Klicken Sie unter **Console Root** auf den Knoten **Attachment Checking**.
2. Klicken Sie auf der rechten Seite der Anhangskontrolle auf die Schaltfläche **Add Rule**.

Apply Cancel

General Actions Users/Folders

Attachment Checking

Rule display name

Rule name:
New Attachment Checking Rule

Email checking

Check inbound emails
 Check outbound emails

Attachment blocking

Block all
 Block this list
 Block all except this list

Enter filenames with optional wildcards:
(eg. *.vbs)
(eg. *letter.vbs)
(eg. happy*.exe)
(eg. orders.mdb)

Add

Remove Selected

Options

Block all files greater than the following size in Kb:
2048

Screenshot 48 – Anhangskontrolle: Reiter „General“

3. Geben Sie den Namen der Regel an, und legen Sie fest, ob diese Regel für ein- und/oder ausgehende E-Mails gelten soll. Markieren Sie zur Überprüfung eingehender Nachrichten das Kontrollkästchen **Check inbound emails** und zur Überprüfung ausgehender Nachrichten das Kontrollkästchen **Check outbound emails**.

4. Legen Sie fest, in welchem Umfang Anhänge blockiert werden sollen:

- **Block all** – Blockiert E-Mail-Anhänge jedes Typs.
- **Block this list** – Blockiert NUR die Anhangstypen aus der folgenden Liste.
- **Block all except this list** – Blockiert alle Anhangstypen, die NICHT in der nebenstehenden Liste aufgeführt sind.

Hinweis 1: Um die Liste der Anhangstypen zu erweitern, geben Sie im Eingabefeld neben der Schaltfläche **Add** den vollständigen Dateinamen oder die Dateierweiterung ein. Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf die Schaltfläche **Add**. Zeichen oder Zeichenfolgen in Anhangstyp/Erweiterung lassen sich per Sternchen-Platzhalter „*“ ersetzen. Mit „*Bestellungen*.mdb“ werden z. B. alle Dateien des Formats „.mdb“ blockiert, bei denen die Zeichenfolge „Bestellungen“ im Dateinamen enthalten ist. Bei Eingabe von „*.jpg“ werden alle jpg-Dateien blockiert.

Hinweis 2: Um einen Eintrag aus der Liste zu entfernen, markieren Sie ihn, und klicken Sie auf die Schaltfläche **Remove Selected**.

5. Zusätzlich können Sie als weitere Einschränkung die maximal erlaubte Dateigröße in KB angeben. Hierdurch werden alle Anhänge, die größer sind als von Ihnen erlaubt, blockiert – ungeachtet dessen, ob sie in der Liste der Anhangstypen verzeichnet sind oder nicht. Wählen Sie hierfür die Option **Block all files greater than the following size in Kb**, und geben Sie die maximal erlaubte Dateigröße (in KB an). Anhänge, die größer sind als angegeben, werden blockiert.

The screenshot shows the 'Attachment Checking Actions' configuration window with the 'Actions' tab selected. The window has three tabs: 'General', 'Actions', and 'Users/Folders'. The 'Attachment Checking Actions' title bar is visible. The main content area is divided into three sections:

- Actions:** Contains a checked checkbox for 'Block attachment and perform this action:'. Below it are three radio button options: 'Quarantine email' (selected), 'Delete email', and 'Move to folder:'. A text input field is located below the 'Move to folder:' option.
- Notification options:** Contains two checked checkboxes: 'Notify administrator' and 'Notify local user'.
- Logging options:** Contains an unchecked checkbox for 'Log rule occurrence to this file:'. Below it is a label 'File name of log file:' followed by a text input field.

Screenshot 49 – Anhangskontrolle: Reiter „Actions“

6. Nachdem Sie festgelegt haben, welche Merkmale mit einer Regel zur Anhangskontrolle überprüft werden sollen, müssen Sie bestimmen, wie diese Regel herausgefilterte Anhänge behandeln soll. Klicken Sie auf den Reiter **Actions**, um die Konfigurationsseite für Verfahrensweisen zu öffnen.

7. Wählen Sie die Option **Block attachment and perform this action**, wenn blockierte E-Mails unter Quarantäne gestellt, gelöscht oder in einen Ordner verschoben werden sollen. Wählen Sie hierfür zusätzlich eine der folgenden Optionen aus:

- **Quarantine email** – Stellt die E-Mail mit Anhang bis zur Überprüfung durch den Administrator unter Quarantäne. Weitere Informationen hierzu erhalten Sie im Kapitel „E-Mail-Quarantäne“ in diesem Handbuch.
- **Delete email** – Löscht die E-Mail samt Anhang.
- **Move to folder** – Verschiebt die E-Mail in den angegebenen Ordner. Geben Sie den Namen des Ordners im entsprechenden Eingabefeld ein.

Hinweis: Beachten Sie bitte, dass sich Aktionen nicht allein für den Anhang einer E-Mail konfigurieren lassen. Aktionen gelten immer für die gesamte E-Mail, der der Anhang hinzugefügt wurde.

8. Die Regeln zur Anhangskontrolle können so konfiguriert werden, dass E-Mail-Benachrichtigungen an den Administrator und/oder Anwender verschickt werden, wenn eine E-Mail mit Anhang blockiert wurde. Die Benachrichtigung kann durch Auswahl folgender Optionen eingerichtet werden:

- **Notify local user** – Benachrichtigt den angegebenen Empfänger einer Mitteilung per E-Mail, wenn die Mitteilung samt Anhang blockiert wurde.

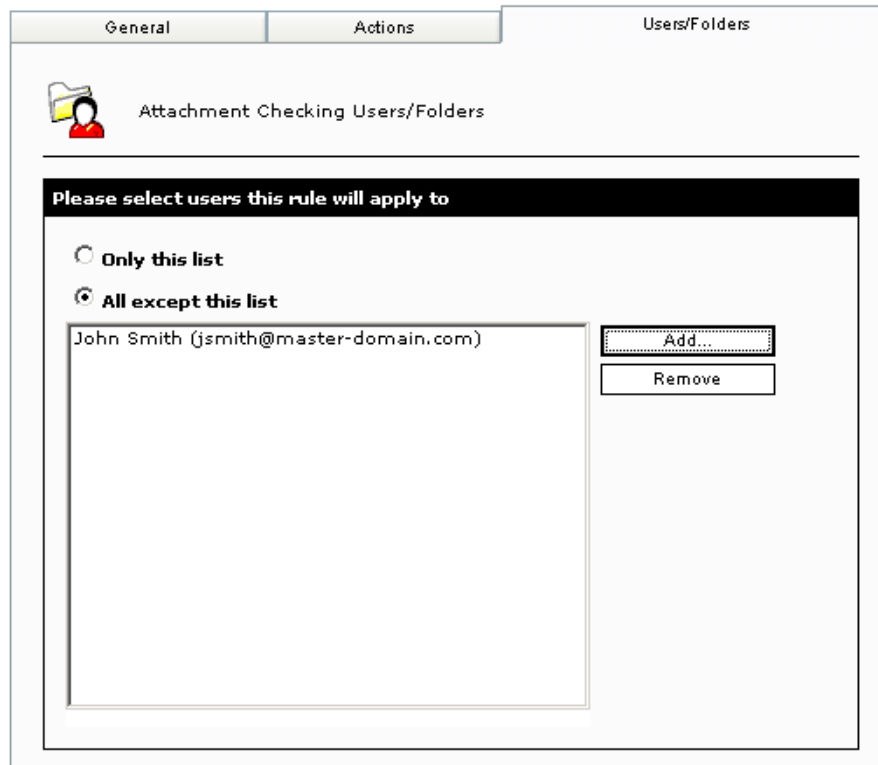
Hinweis: Ist die blockierte E-Mail eingehend, werden mit dieser Option nur die Empfänger der Mitteilung benachrichtigt. Bei ausgehenden E-Mails erfolgt eine entsprechende Benachrichtigung an den Absender.

- **Notify administrator** – Benachrichtigt den Administrator per E-Mail, wenn eine Mitteilung mit Anhang blockiert wurde. Die E-Mail-Adresse des Administrators wird während der Installation von GFI MailSecurity angegeben und kann zu einem späteren Zeitpunkt über das Konfigurationsmenü geändert werden (über **Console Root** ▶ Knoten **Settings** ▶ Reiter **General**). Nähere Informationen hierzu erhalten Sie im Kapitel „Allgemeine Einstellungen“ unter „Angaben der E-Mail-Adresse des Administrators“.

9. Wählen Sie die Option **Log rule occurrence to this file**, wenn sämtliche Aktionen dieser Regel in einer Protokolldatei gesichert werden sollen. Geben Sie den Namen der Protokolldatei im Eingabefeld **File name of log file** ein.

Hinweis: Eine Regel zur Anhangskontrolle kann verschiedene Aktionen/Vorgaben enthalten. Beispielsweise können Sie festlegen, dass E-Mails mit einem Anhang nicht blockiert werden sollen, sondern der Anwender einfach zu benachrichtigen oder der Vorfall in einer Datei zu protokollieren ist.

10. Geben Sie die Anwender an, für die die Regel gelten soll. Standardmäßig werden Regeln auf alle E-Mail-Benutzer angewandt. Wenn eine Regel jedoch nur für bestimmte Anwender gültig sein soll, klicken Sie auf den Reiter **Users/Folders**.

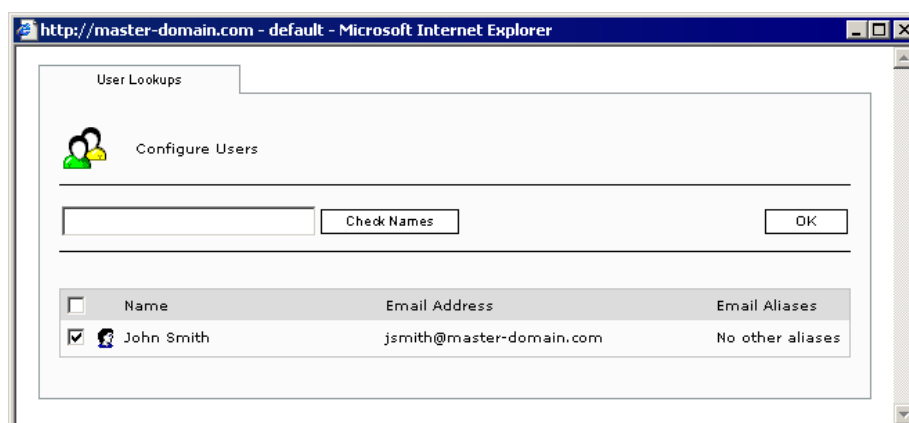


Screenshot 50 – Anhangskontrolle: Seite für Benutzer/Ordner

11. Wählen Sie eine der folgenden Optionen:

- **Only this list** – Wendet die Regel auf alle E-Mail-Anwender/Gruppen oder Öffentlichen Ordner in der angezeigten Liste an.
- **All except this list** – Wendet die Regel auf alle E-Mail-Anwender/Gruppen oder Öffentlichen Ordner an, die NICHT in der angezeigten Liste aufgeführt sind.

12. Um E-Mail-Anwender, Benutzergruppen und/oder Öffentliche Ordner der Liste hinzuzufügen, klicken Sie auf die Schaltfläche **Add**.



Screenshot 51 – Hinzufügen von Anwendern

13. Geben Sie im Dialog zum Hinzufügen von Anwendern den Namen des E-Mail-Anwenders, der Benutzergruppe oder des Öffentlichen Ordners an.

14. Klicken Sie auf die Schaltfläche **Check Names**. GFI MailSecurity überprüft nun per Active Directory oder der importierten Liste der

SMTP-Adressen (je nach Art der Installation von GFI MailSecurity), ob der eingegebene Eintrag vorhanden ist. Nach der Überprüfung wird eine Liste mit übereinstimmenden Ergebnissen angezeigt.

Hinweis: Die Eingabe des vollständigen Namens des Anwenders/der Benutzergruppe oder des Öffentlichen Ordners ist nicht erforderlich. Sie brauchen lediglich mindestens drei Zeichen einzugeben. GFI MailSecurity führt daraufhin alle Namen auf, in denen diese Zeichen enthalten sind. Wenn Sie beispielsweise „ott“ eingeben, findet GFI MailSecurity Namen wie „Scott Adams“ und „Freeman Prescott“, sofern vorhanden.

15. Markieren Sie das Kontrollkästchen vor den aufgeführten Namen für alle Einträge, die der Liste hinzugefügt werden sollen, und klicken Sie auf die Schaltfläche **OK**.

Hinweis 1: Durch Markieren des obersten Kontrollkästchens neben der Spalte **Name** lassen sich alle aufgeführten Namen gleichzeitig auswählen.

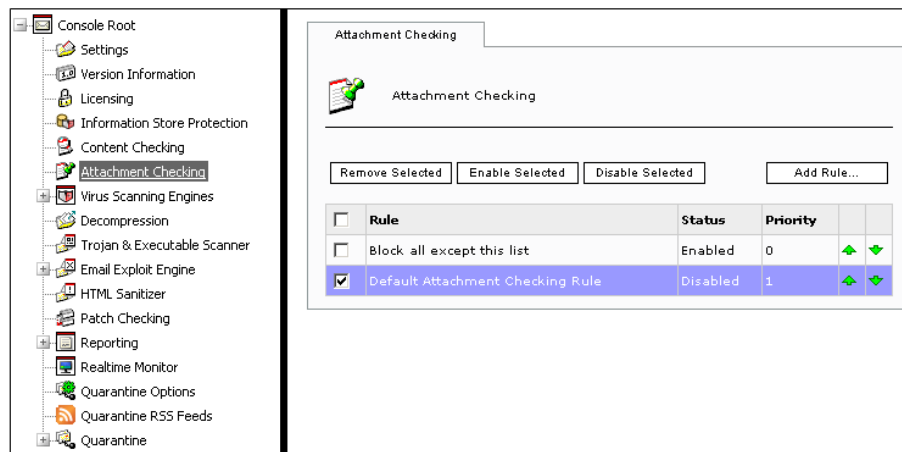
Hinweis 2: Wiederholen Sie die Schritte 12 bis 15, bis alle gewünschten Namen auf der Liste stehen.

Hinweis 3: Um Einträge aus der Liste zu entfernen, wählen Sie den zu löschenden Anwender/die Benutzergruppe/die Öffentlichen Ordner aus, und klicken Sie auf die Schaltfläche **Remove**.

Hinweis 4: Sind in der Liste keine Namen aufgeführt, wendet GFI MailSecurity diese Regel automatisch auf alle in Active Directory/der SMTP-Adressliste enthaltenen E-Mail-Anwender an.

16. Klicken Sie auf die Schaltfläche **Apply** oben auf der Seite, um die Regel zu aktivieren.

Entfernen einer Regel zur Anhangskontrolle



Screenshot 52 – Anhangskontrolle

So entfernen Sie eine Regel zur Anhangskontrolle:

1. Klicken Sie unter **Console Root** auf den Knoten **Attachment Checking**.
2. Wählen Sie im rechten Fenster zur Anhangskontrolle alle Kontrollkästchen der Regeln aus, die Sie entfernen möchten.

Hinweis: Durch Markieren des obersten Kontrollkästchens neben der Spalte **Rule** lassen sich alle Regeln gleichzeitig auswählen.

3. Klicken Sie auf die Schaltfläche **Remove Selected**, um die ausgewählten Regeln zu löschen.

Ändern einer Regel zur Anhangskontrolle

So ändern Sie eine vorhandene Regel:

1. Klicken Sie unter **Console Root** auf den Knoten **Attachment Checking**.
2. Markieren Sie im rechten Fenster zur Anhangskontrolle den Namen der Regel, die sie ändern möchten.
3. Führen Sie die gewünschten Änderungen in den Eigenschaften der Regel durch (z. B. Umbenennung), und klicken Sie auf die Schaltfläche **Apply** oben auf der Seite, um die Änderungen zu übernehmen. Die Änderungen sind sofort gültig.

Aktivieren/Deaktivieren einer Regel zur Anhangskontrolle

Der Status einer Regel (aktiviert/deaktiviert) kann über die Seite zur Anhangskontrolle kontrolliert und geändert werden. So aktivieren oder deaktivieren Sie eine vorhandene Regel:

1. Klicken Sie unter **Console Root** auf den Knoten **Attachment Checking**.
2. Markieren Sie im rechten Fenster zur Anhangskontrolle alle Kontrollkästchen der Regeln, die Sie aktivieren oder deaktivieren möchten.
3. Klicken Sie zur Aktivierung der ausgewählten Regel auf die Schaltfläche **Enable Selected**. Zur Deaktivierung der ausgewählten Regel klicken Sie auf die Schaltfläche **Disable Selected**. Die Änderungen werden sofort in der Status-Spalte der Regel angezeigt.

Ändern der Regel-Priorität

<input type="checkbox"/>	Rule	Status	Priority		
<input type="checkbox"/>	Block all except this list	Enabled	0	▲	▼
<input type="checkbox"/>	Default Attachment Checking Rule	Disabled	1	▲	▼

Screenshot 53 – Anhangskontrolle

Regeln zur Anhangskontrolle werden von oben beginnend in der Reihenfolge angewandt, in der sie auf der Seite zur Anhangskontrolle aufgeführt sind. Die Abfolge/Priorität der Regelkontrolle lässt sich wie folgt ändern:

1. Klicken Sie unter **Console Root** auf den Knoten **Attachment Checking**.

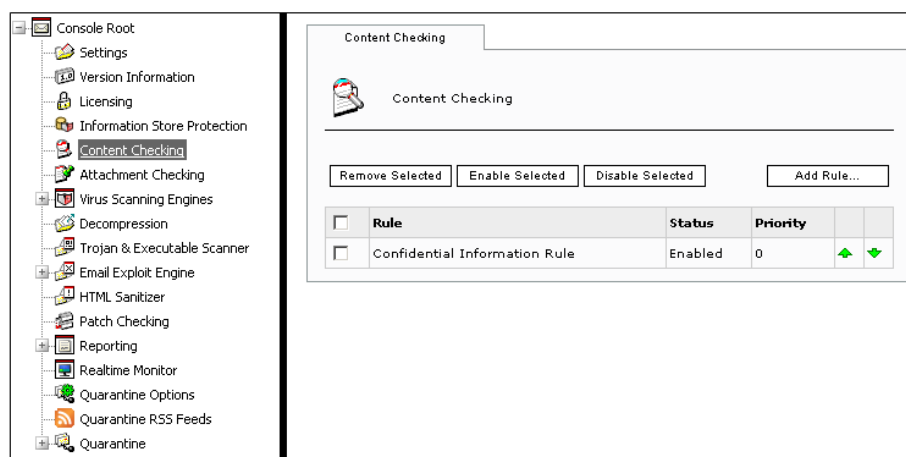
2. Klicken Sie auf der rechten Seite zur Anhangskontrolle auf den Nach-oben-Pfeil oder Nach-unten-Pfeil, um die Priorität einer Regel zu erhöhen oder zu senken. Wiederholen Sie diesen Vorgang, bis der Viren-Scanner die gewünschte Priorität in der Liste einnimmt.

Hinweis: Über die Seite zur Anhangskontrolle lässt sich die Priorität einer Regel jeweils in der Spalte **Priority** kontrollieren.

Konfigurieren der Inhaltskontrolle

Einführung

In diesem Kapitel wird erklärt, wie Sie die Inhaltskontrolle zur Überprüfung von E-Mail-Inhalten durch GFI MailSecurity konfigurieren. Über diese Funktion können Sie Regeln mit Stichwörtern und logischen Operatoren angeben, mit denen sich beispielsweise E-Mails mit vertraulichen Informationen herausfiltern lassen.



Screenshot 54 – Inhaltskontrolle

Die Regeln zur Inhaltskontrolle werden über den Knoten **Content Checking** konfiguriert. Auf der zugehörigen Seite werden alle vorhandenen Regeln zur Inhaltskontrolle aufgeführt, die aktiviert oder deaktiviert werden können. Die Änderung ihrer Kontrollpriorität ist ebenfalls möglich. Zudem können Sie neue Regeln zur Inhaltskontrolle erstellen und bestehende Regeln ändern oder löschen.

Erstellen einer Regel zur Inhaltskontrolle

So erstellen Sie eine Regel zur Kontrolle des Inhalts:

1. Klicken Sie unter **Console Root** auf den Knoten **Content Checking**.
2. Klicken Sie auf der rechten Seite der Inhaltskontrolle auf die Schaltfläche **Add Rule**.
3. Geben Sie unter dem Reiter **General** den Namen der neuen Inhaltskontrollregel ein. Der Name sollte aussagekräftig sein, um verschiedene Regeln leichter voneinander unterscheiden zu können.
4. Legen Sie fest, ob diese Regel für eingehende und/oder ausgehende E-Mails gelten soll, indem Sie die entsprechenden Kontrollkästchen markieren.

General | Body | Subject | Actions | Users/Folders

Content Checking Options

Rule name

Please specify a friendly name for this rule:

Confidential Information Rule

Email checking

This rule can be applied to both inbound and outbound emails. Select below:

Check inbound emails

Check outbound emails

PGP Encryption

This rule can be set to block any PGP encrypted mail. Enable or disable this option below:

Block PGP encrypted emails

Screenshot 55 – Inhaltskontrolle: Reiter „General“

5. Wenn PGP-verschlüsselte E-Mails ebenfalls von dieser Regel blockiert werden sollen, klicken Sie auf das Kontrollkästchen **Block PGP encrypted emails**.

6. Klicken Sie auf den Reiter **Body**, um festzulegen, ob der Textkörper einer E-Mail und seine Anhänge gescannt werden sollen und welche Stichwörter von der Inhaltskontrolle zu berücksichtigen sind.

7. Um mit dieser Regel den Textkörper/Anhang von E-Mails überprüfen und ggf. blockieren zu lassen, markieren Sie das Kontrollkästchen **Block emails if content is found matching these conditions (message body/attachments)**.

8. Geben Sie die Bedingungen an, mit denen der Inhalt von Textkörpern und Anhängen überprüft werden soll. Um eine neue Bedingung festzulegen, geben Sie die benötigten Stichwörter im Textfenster **Edit condition** ein. Klicken Sie auf die Schaltfläche des benötigten logischen Operators, um ihn im Textfenster **Edit condition** an der aktuellen Cursor-Position einzufügen. Haben Sie die Bedingung vollständig eingegeben, klicken Sie auf die Schaltfläche **Add Condition**, um sie der Regel hinzuzufügen. Die neue Bedingung wird dann im Listenfeld **Current conditions** angezeigt.

Um beispielsweise die Bedingung „vertrauliche Informationen UND top secret“ einzugeben, gehen Sie wie folgt vor:

- a) Geben Sie im Textfenster **Edit condition** den Begriff „vertrauliche Informationen“ ein.
- b) Klicken Sie dann auf die Schaltfläche **AND** auf der rechten Seite des Fensters.
- c) Geben Sie „top secret“ ein, und klicken Sie auf die Schaltfläche **Add Condition**.

Hinweis: Um eine Bedingung zu entfernen, wählen Sie diese über das Listenfeld **Current conditions** aus, und klicken Sie auf die Schaltfläche **Remove**. Um eine vorhandene Bedingung zu ändern, wählen Sie diese über das Listenfeld **Current conditions** aus. Die Bedingung wird im Textfenster **Edit condition** angezeigt. Führen Sie die Änderungen wie gewünscht durch. Klicken Sie abschließend auf die Schaltfläche **Update**, um Ihre Änderungen zu speichern.

Screenshot 56 – Inhaltskontrolle: Reiter „Body“

9. Sollen für die in den Bedingungen verwendeten Stichwörter nur ganze Wörter beachtet werden, markieren Sie das Kontrollkästchen **Match whole words only**.

10. Um mit der Regel zur Inhaltskontrolle auch alle E-Mail-Anhänge mit Hilfe der zuvor angegebenen Bedingungen zu überprüfen, markieren Sie das Kontrollkästchen **Apply above conditions to attachments**.

11. Legen Sie fest, welche Arten von Dateinamenerweiterungen kontrolliert werden sollen. Geben Sie hinzuzufügende Dateinamenerweiterungen im Eingabefeld **File extension entry** ein, und klicken Sie auf die Schaltfläche **Add**. Wenn nur die von Ihnen angegebenen Dateinamenerweiterungen kontrolliert werden sollen, klicken Sie auf das Optionsfeld **Check all attachments having file extensions in the list**. Wenn alle Anhangstypen außer den von Ihnen in der Liste angegebenen kontrolliert werden sollen, markieren Sie auf das Optionsfeld **Check all except attachments having file extensions in the list**.

Hinweis: Geben Sie nur die reine Dateinamenerweiterung ein, beispielsweise „txt“ bei Nur-Text-Dateien, nicht jedoch „*.txt“ oder „.txt“.

12. Wenn Sie mit der Regel zur Inhaltskontrolle den Betreff einer E-Mail überprüfen möchten, klicken Sie auf den Reiter **Subject**. Geben Sie die Stichwörter ein, nach denen gesucht werden soll.

13. Markieren Sie unter dem Reiter **Subject** das Kontrollkästchen **Enable subject content checking**.

14. Geben Sie hinzuzufügende Stichwörter im Eingabefeld **Enter phrase** ein, und klicken Sie auf die Schaltfläche **Add**. Das neue Stichwort wird dann im Textfenster **Phrases** angezeigt.

The screenshot shows the 'Subject' tab of the 'Content Checking Actions' dialog. It features a checked checkbox for 'Enable subject content checking'. Below this, a section titled 'Block emails with the following phrases in the 'Subject' field' contains an 'Enter phrase:' input field with an 'Add' button. The 'Phrases:' list contains the text 'personal information' and a 'Remove Selected' button. At the bottom, the 'Options' section has a 'Match whole words only' checkbox which is currently unchecked.

Screenshot 57 – Inhaltskontrolle: Reiter „Subject“

15. Sollen nur ganze Wörter beachtet werden, markieren Sie das Kontrollkästchen **Match whole words only**.

16. Legen Sie über den Reiter **Actions** fest, wie GFI MailSecurity mit E-Mails verfahren soll, die diese Regel verletzen.

17. Wählen Sie die Option **Block email and perform this action**, wenn blockierte E-Mails unter Quarantäne gestellt, gelöscht oder in einen Ordner verschoben werden sollen. Wählen Sie hierfür zusätzlich eine der folgenden Optionen aus:

Quarantine email – Stellt die herausgefilterte E-Mail bis zur Überprüfung durch den Administrator unter Quarantäne. Weitere Informationen hierzu erhalten Sie im Kapitel „E-Mail-Quarantäne“ in diesem Handbuch.

Delete email – Löscht die E-Mail vollständig.

Move to folder – Verschiebt die E-Mail in den angegebenen Ordner. Geben Sie den Namen des Ordners im entsprechenden Eingabefeld ein. Regeln zur Inhaltskontrolle können so konfiguriert werden, dass E-Mail-Benachrichtigungen an den Administrator und/oder Anwender verschickt werden, wenn eine Nachricht eine Regel verletzt.

Die Benachrichtigung kann durch Auswahl folgender Optionen eingerichtet werden:

Notify local user – Informiert den angegebenen Empfänger einer Nachricht per E-Mail, wenn diese Regel verletzt wurde.

Hinweis: Ist die blockierte E-Mail eingehend, werden mit dieser Option nur die Empfänger der Mitteilung informiert. Bei ausgehenden E-Mails erfolgt eine entsprechende Benachrichtigung an den Absender.

Notify administrator – Informiert den Administrator per E-Mail, wenn eine Nachricht diese Regel verletzt hat. Die E-Mail-Adresse des Administrators wird während der Installation von GFI MailSecurity angegeben und kann zu einem späteren Zeitpunkt über das Konfigurationsmenü geändert werden (über **Console Root** ▶ Knoten **Settings** ▶ Reiter **General**). Nähere Informationen hierzu erhalten Sie im Kapitel „Allgemeine Einstellungen“ unter „Angaben der E-Mail-Adresse des Administrators“.

General Body Subject **Actions** Users/Folders

Content Checking Actions

Actions

Block email and perform this action

Quarantine email

Delete email

Move to folder:

Notification options

Notify administrator

Notify local user

Logging options

Log rule occurrence to this file:

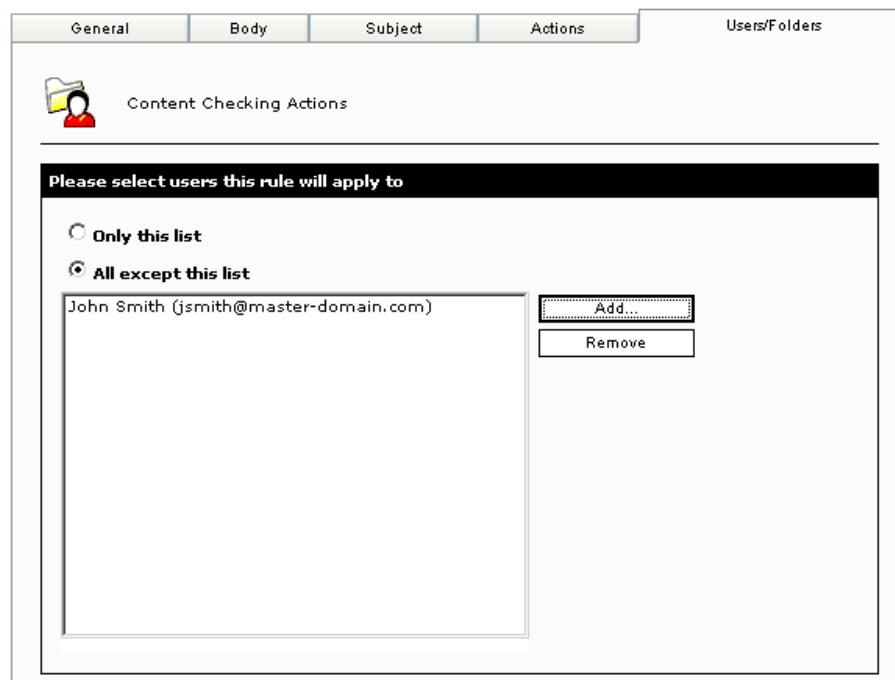
File name of log file:

Screenshot 58 – Inhaltskontrolle: Reiter „Actions“

19. Wählen Sie die Option **Log rule occurrence to this file**, wenn sämtliche Aktionen dieser Regel in einer Protokolldatei gesichert werden sollen. Geben Sie den Namen der Protokolldatei im Eingabefeld **File name of log file** ein.

Hinweis: Für eine Regel zur Inhaltskontrolle können die unterschiedlichsten Aktionen konfiguriert werden. Beispielsweise können Sie festlegen, dass E-Mails, die eine Regel verletzen, nicht blockiert werden sollen, sondern dass nur der Administrator zu benachrichtigen oder der Vorfall in einer Datei zu protokollieren ist.

20. Geben Sie die Anwender an, für die die Regel gelten soll. Standardmäßig werden Regeln auf alle E-Mail-Benutzer angewandt. Wenn eine Regel jedoch nur für bestimmte Anwender gültig sein soll, klicken Sie auf den Reiter **Users/Folders**.



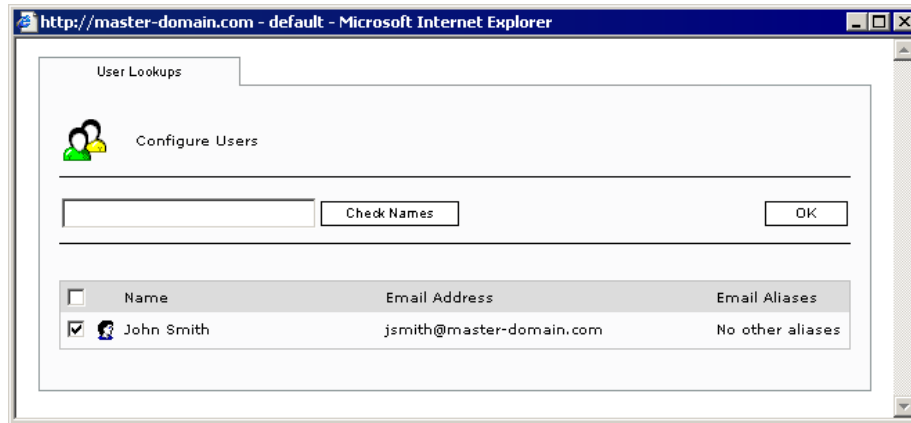
Screenshot 59 – Inhaltskontrolle: Reiter „Users/Folders“

21. Wählen Sie eine der folgenden Optionen:

Only this list – Wendet die Regel auf alle E-Mail-Anwender/Gruppen oder Öffentlichen Ordner in der angezeigten Liste an.

All except this list – Wendet die Regel auf alle E-Mail-Anwender/Gruppen oder Öffentlichen Ordner an, die nicht in der angezeigten Liste aufgeführt sind.

22. Um E-Mail-Anwender, Benutzergruppen und/oder Öffentliche Ordner der Liste hinzuzufügen, klicken Sie auf die Schaltfläche **Add**.



Screenshot 60 – Hinzufügen von Anwendern

23. Geben Sie im Dialog zum Hinzufügen von Anwendern den Namen des E-Mail-Anwenders, der Benutzergruppe oder des Öffentlichen Ordners an.

24. Klicken Sie auf die Schaltfläche **Check Names**. GFI MailSecurity überprüft per Active Directory oder der importierten Liste der SMTP-Adressen (je nach Art der Installation von GFI MailSecurity), ob der eingegebene Eintrag vorhanden ist. Nach der Überprüfung wird eine Liste mit übereinstimmenden Ergebnissen angezeigt.

Hinweis: Die Eingabe des vollständigen Namens des Anwenders/der Benutzergruppe oder des Öffentlichen Ordners ist nicht erforderlich. Sie brauchen lediglich mindestens drei Zeichen einzugeben. GFI MailSecurity führt daraufhin alle Namen auf, in denen diese Zeichen enthalten sind. Wenn Sie beispielsweise „ott“ eingeben, werden Namen wie „Scott Adams“ und „Freeman Prescott“ gefunden, sofern vorhanden.

25. Markieren Sie das Kontrollkästchen vor den aufgeführten Namen für alle Einträge, die der Liste hinzugefügt werden sollen, und klicken Sie auf die Schaltfläche **OK**.

Hinweis 1: Durch Markieren des obersten Kontrollkästchens neben der Spalte **Name** lassen sich alle aufgeführten Namen gleichzeitig auswählen.

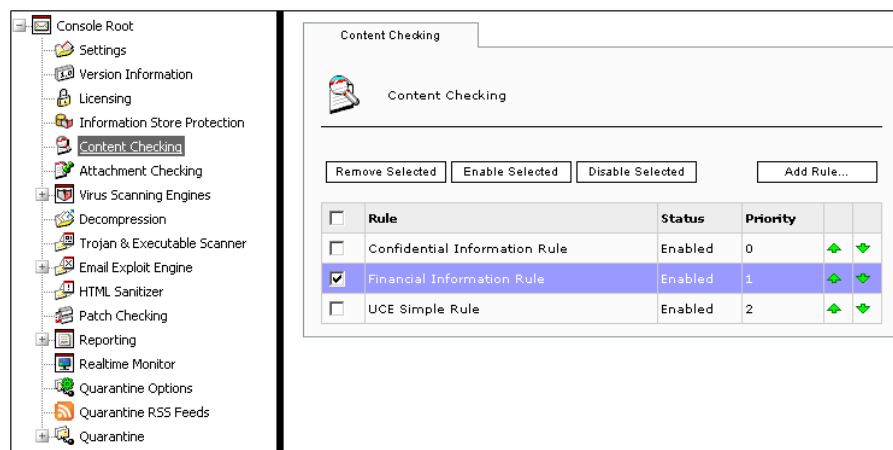
Hinweis 2: Wiederholen Sie die Schritte 22 bis 25, bis alle gewünschten Namen auf der Liste stehen.

Hinweis 3: Um Einträge aus der Liste zu entfernen, wählen Sie den zu löschenden Anwender/die Benutzergruppe/die Öffentlichen Ordner aus, und klicken Sie auf die Schaltfläche **Remove**.

Hinweis 4: Sind in der Liste keine Namen aufgeführt, wendet GFI MailSecurity diese Regel automatisch auf alle in Active Directory/der SMTP-Adressliste enthaltenen E-Mail-Anwender an.

26. Um die neue Regel zur Inhaltskontrolle zu speichern und zu aktivieren, klicken Sie auf die Schaltfläche **Apply** oben auf der Seite.

Entfernen einer Regel zur Inhaltskontrolle



Screenshot 61 – Inhaltskontrolle: Entfernen von Regeln

So entfernen Sie eine Regel zur Inhaltskontrolle:

1. Klicken Sie unter **Console Root** auf den Knoten **Content Checking**.
2. Wählen Sie im rechten Fenster zur Inhaltskontrolle alle Kontrollkästchen der Regeln aus, die Sie entfernen möchten.

Hinweis: Durch Markieren des obersten Kontrollkästchens neben der Spalte **Rule** lassen sich alle Regeln gleichzeitig auswählen.

3. Klicken Sie auf die Schaltfläche **Remove Selected**, um die ausgewählten Regeln zu löschen.

Ändern einer Regel zur Inhaltskontrolle

So ändern Sie eine vorhandene Regel:

1. Klicken Sie unter **Console Root** auf den Knoten **Content Checking**.
2. Markieren Sie im rechten Fenster zur Inhaltskontrolle den Namen der Regel, die sie ändern möchten. Die Regel wird angezeigt.
3. Führen Sie die gewünschten Änderungen in den Eigenschaften der Regel durch (z. B. Umbenennung), und klicken Sie auf die Schaltfläche **Apply** oben auf der Seite, um die Änderungen zu übernehmen. Die Änderungen sind sofort gültig.

Aktivieren/Deaktivieren einer Regel

Der Status einer Regel (aktiviert/deaktiviert) kann über die Seite zur Inhaltskontrolle kontrolliert und geändert werden. So aktivieren oder deaktivieren Sie eine vorhandene Regel:

1. Klicken Sie unter **Console Root** auf den Knoten **Content Checking**.
2. Markieren Sie im rechten Fenster zur Inhaltskontrolle alle Kontrollkästchen der Regeln, die Sie aktivieren oder deaktivieren möchten.
3. Klicken Sie zur Aktivierung der ausgewählten Regel auf die Schaltfläche **Enable Selected**. Zur Deaktivierung der ausgewählten

Regel klicken Sie auf die Schaltfläche **Disable Selected**. Die Änderungen werden sofort in der Status-Spalte der Regel angezeigt.

Ändern der Regel-Priorität

Über die Priorität einer Regel zur Inhaltskontrolle legen Sie fest, mit welcher Regel Mitteilungen zuerst kontrolliert werden sollen.

Auf der Seite zur Inhaltskontrolle werden die zugehörigen Regeln in der Reihenfolge angezeigt, in der die Überprüfung stattfindet. Die Regel mit der höchsten Priorität „0“ steht am Anfang der Liste. Die Priorität einer Regel wird auf der rechten Seite in der Spalte **Priority** angezeigt.

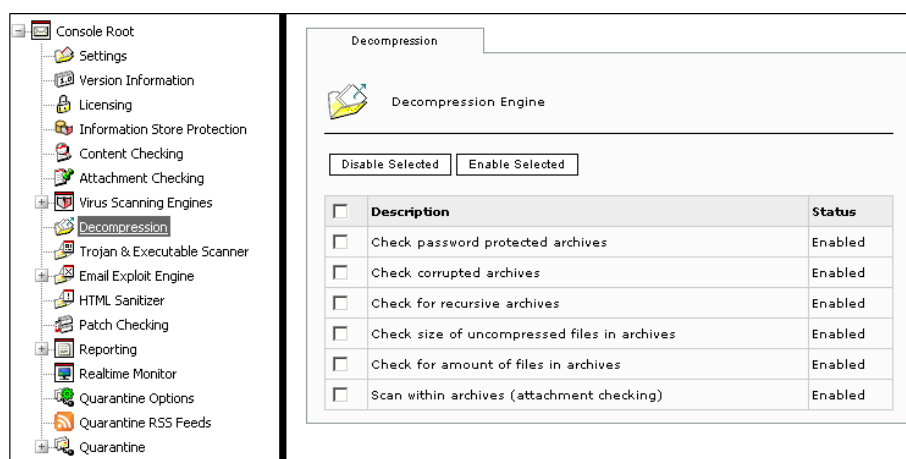
So ändern Sie die Priorität einer Regel auf der Seite zur Inhaltskontrolle:

1. Klicken Sie unter **Console Root** auf den Knoten **Content Checking**.
2. Klicken Sie auf der rechten Seite zur Inhaltskontrolle auf den Nach-oben-Pfeil oder Nach-unten-Pfeil, um die Priorität einer Regel zu erhöhen oder zu senken. Wiederholen Sie diesen Vorgang, bis der Viren-Scanner die gewünschte Priorität in der Liste einnimmt.

Die Dekomprimierungs-Engine

Einführung

Die Dekomprimierungs-Engine entpackt und analysiert Archivdateien, die an E-Mails angehängt sind.



Screenshot 62 – Filterliste der Dekomprimierungs-Engine

Folgende Filter zur Kontrolle von Archivdateien kommen bei der Dekomprimierungs-Engine zum Einsatz:

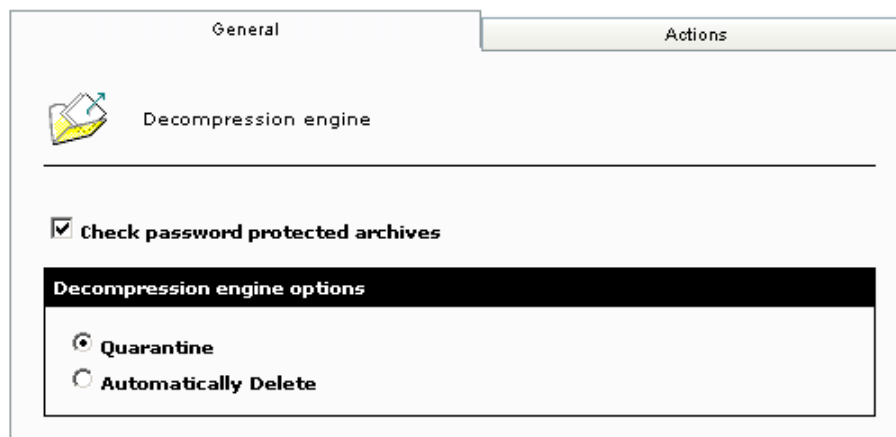
Filter zur

- Kontrolle passwortgeschützter Archivdateien
- Kontrolle fehlerhafter Archivdateien
- Kontrolle nach rekursiven Archivdateien
- Kontrolle der Größe entpackter Dateien in Archivdateien
- Kontrolle der Anzahl von Dateien in einer Archivdatei
- Kontrolle innerhalb von Archivdateien

Jeder dieser Filter ist einzeln zu konfigurieren. Legen Sie dabei fest, wie mit E-Mails, an die bestimmte komprimierte Dateien angehängt sind, zu verfahren ist. Des Weiteren können Sie bestimmen, wie ein Filter mit E-Mails verfahren soll, in denen eine bestimmte Archivdatei gefunden und blockiert wurde (z. B. kann eine entsprechende E-Mail-Benachrichtigung verschickt werden).

Konfigurieren der Filter der Dekomprimierungs-Engine

Kontrollieren passwortgeschützter Archivdateien



Screenshot 63 – Optionen für passwortgeschützte Archivdateien

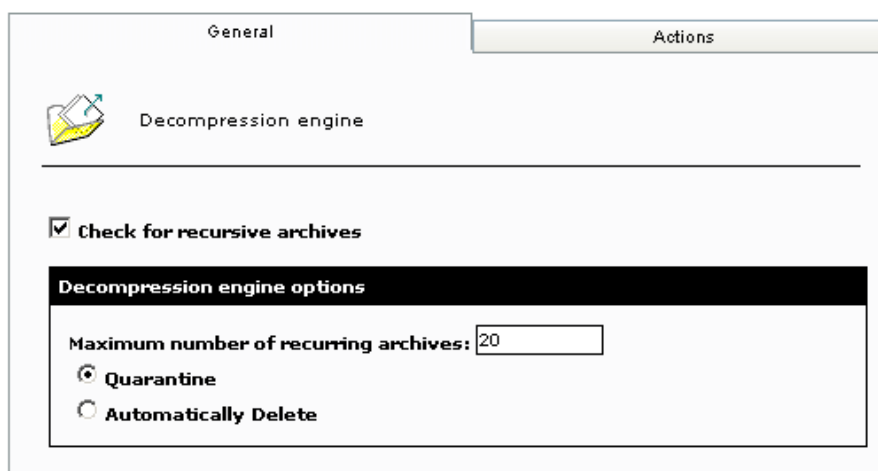
Mit Hilfe dieses Filters können E-Mails, die passwortgeschützte Archivdateien enthalten, unter Quarantäne gestellt oder gelöscht werden. So wird dieser Filter konfiguriert:

1. Klicken Sie unter **Console Root** auf den Knoten **Decompression**.
2. Markieren Sie im rechten Fenster in der Liste der verfügbaren Filter das Kontrollkästchen **Check password protected archives**.
3. Markieren Sie auf der zugehörigen Konfigurationsseite das Kontrollkästchen **Check password protected archives**, um den Filter zu aktivieren.
4. Legen Sie fest, wie mit E-Mails zu verfahren ist, die passwortgeschützte Archive enthalten. Folgende Optionen stehen zur Auswahl:
 - **Quarantine** – Stellt E-Mails mit passwortgeschützten Archivdateien unter Quarantäne. Diese Mitteilungen können zu einem späteren Zeitpunkt vom Administrator analysiert und freigegeben oder gelöscht werden.
 - **Automatically Delete** – Löscht automatisch E-Mails, die passwortgeschützte Archivdateien enthalten.
5. Klicken Sie auf den Reiter **Actions** um festzulegen, wie mit E-Mails mit passwortgeschützten Archivdateien, die herausgefiltert und blockiert wurden, zu verfahren ist. Weitere Informationen zur Konfiguration entsprechender Aktionen erhalten Sie im Kapitel „Konfigurieren von Aktionen der Dekomprimierungsfilter“.
6. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Kontrollieren fehlerhafter Archivdateien

Mit Hilfe dieses Filters können E-Mails, die fehlerhafte Archivdateien enthalten, unter Quarantäne gestellt oder gelöscht werden. Die Konfigurationsoptionen für diesen Filter gleichen denen, die unter „Überprüfen passwortgeschützter Archivdateien“ beschrieben sind. Weitere Informationen hierzu finden Sie weiter oben.

Überprüfen auf rekursive Archivdateien



Screenshot 64 – Optionen für rekursive Archivdateien

Mit Hilfe dieses Filters können E-Mails, die rekursive Archivdateien enthalten, unter Quarantäne gestellt oder gelöscht werden. Rekursive (verschachtelte) Archivdateien sind komprimierte Dateien, die andere/mehrere Ebenen mit Unterarchiven enthalten (d. h. in einer Archivdatei komprimierte Archivdateien). Eine große Anzahl von Archivebenen kann ein Anzeichen für eine böswillige Archivdatei sein: Rekursive Archivdateien lassen sich für DoS-Angriffe („Denial of Service“) einsetzen: Die meisten Content-Scanning- und Anti-Viren-Lösungen lassen sich zum Absturz bringen, wenn sie verschachtelte Archive mit vielen Ebenen scannen sollen.

So konfigurieren Sie diesen Filter:

1. Klicken Sie unter **Console Root** auf den Knoten **Decompression**.
2. Markieren Sie im rechten Fenster in der Liste der verfügbaren Filter das Kontrollkästchen **Check for recursive archives**.
3. Wählen Sie auf der zugehörigen Konfigurationsseite die Option **Check for recursive archives**, um den Filter zu aktivieren. Geben Sie zudem die maximal erlaubte Anzahl der verschachtelten Archivdateien an.

Hinweis: Wenn Sie die Kontrollregel **Check for recursive archives** deaktivieren, werden angehängte rekursive Archive weder gescannt noch unter Quarantäne gestellt und umgehen somit die Viren-Kontrolle.

4. Legen Sie fest, wie mit E-Mails mit rekursiven Archivdateien zu verfahren ist, die die maximal erlaubte Anzahl an verschachtelten Archiven überschreiten:

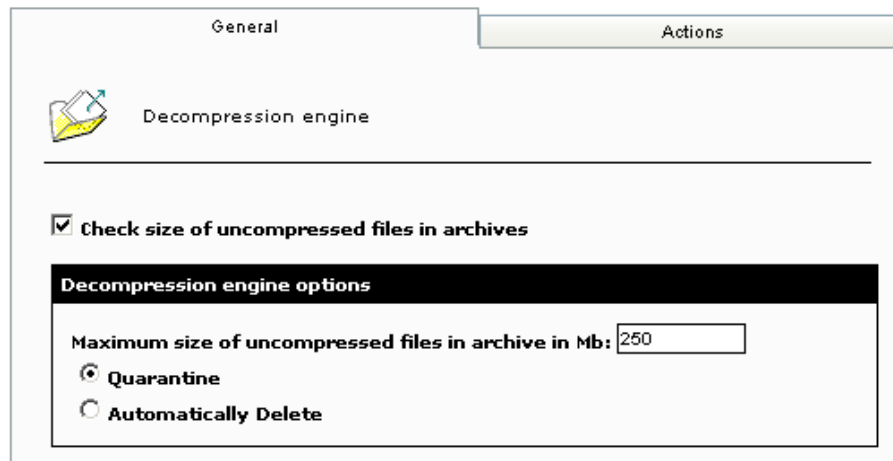
- **Quarantine** – Stellt E-Mails mit rekursiven Archivdateien unter Quarantäne. Diese Mitteilungen können zu einem späteren Zeitpunkt vom Administrator analysiert und freigegeben oder gelöscht werden.
- **Automatically Delete** – Löscht automatisch alle E-Mails mit rekursiven Archivdateien, die die maximal erlaubte Anzahl an Verschachtelungen überschreiten.

5. Klicken Sie auf den Reiter **Actions** um festzulegen, wie mit E-Mails mit rekursiven Archivdateien, die herausgefiltert und blockiert wurden,

zu verfahren ist. Weitere Informationen zur Konfigurierung entsprechender Aktionen erhalten Sie im Kapitel „Konfigurieren von Aktionen der Dekomprimierungsfilter“.

6. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Kontrollieren der Größe entpackter Dateien in Archivdateien



Screenshot 65 – Optionen zur Überprüfung der Größe entpackter Dateien in Archivdateien

Mit Hilfe diese Filters können E-Mails mit Archivdateien, deren physikalische Größe nach dem Entpacken einen bestimmten Wert übersteigt, blockiert oder gelöscht werden. Hacker verwenden diese Methode manchmal für DoS-Angriffe: Indem sie eine Archivdatei verschicken, die nach dem Entpacken sehr groß ist, können sie Content-Security- oder Anti-Viren-Software zum Absturz bringen.

So konfigurieren Sie diesen Filter:

1. Klicken Sie unter **Console Root** auf den Knoten **Decompression**.
2. Markieren Sie im rechten Fenster in der Liste der verfügbaren Filter das Kontrollkästchen **Check size of uncompressed files in archives**.
3. Wählen Sie auf der zugehörigen Konfigurationsseite die Option **Check size of uncompressed files in archives**, um die Funktion zu aktivieren. Geben Sie zudem die maximal erlaubte Größe (in MB) an, die in einer Archivdatei enthaltene Dateien nach dem Entpacken besitzen dürfen.

Hinweis: Wenn Sie die Kontrollregel **Check size of uncompressed files in archives** deaktivieren, werden angehängte Archivdateien weder gescannt noch unter Quarantäne gestellt und umgehen somit die Viren-Kontrolle.

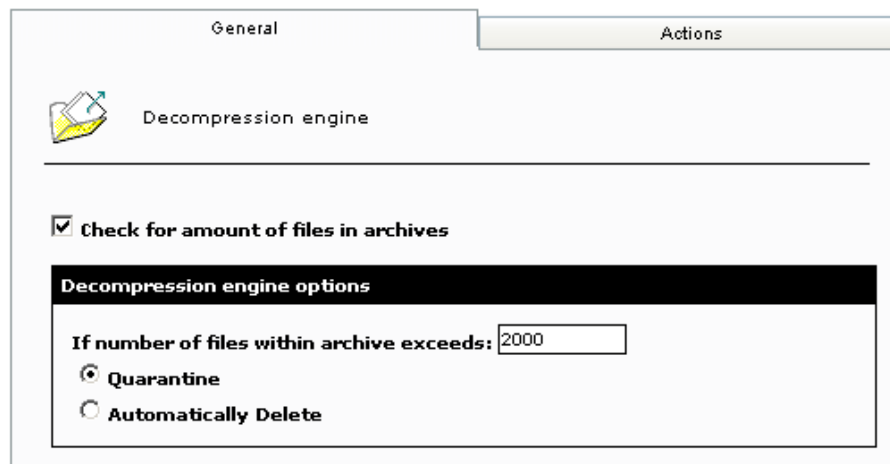
4. Legen Sie fest, wie mit E-Mails mit Archivdateien verfahren werden soll, die nach dem Entpacken eine bestimmte Größe überschreiten.

- **Quarantine** – Stellt E-Mails mit dieser Art von Archivdateien unter Quarantäne. Diese Mitteilungen können zu einem späteren Zeitpunkt vom Administrator analysiert und freigegeben oder gelöscht werden.
- **Automatically Delete** – Löscht automatisch alle E-Mails mit Archivdateien, die nach dem Entpacken die maximal erlaubte Dateigröße überschreiten.

5. Klicken Sie auf den Reiter **Actions** um festzulegen, wie mit E-Mails mit dieser Art von Archivdateien, die herausgefiltert und blockiert wurden, verfahren werden soll. Weitere Informationen zur Konfigurierung entsprechender Aktionen erhalten Sie im Kapitel „Konfigurieren von Aktionen eines Dekomprimierungsfilters“.

6. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Kontrollieren der Anzahl von Dateien in einer Archivdatei



The screenshot shows the 'Actions' tab of a configuration window. At the top, there are two tabs: 'General' and 'Actions'. Below the tabs, there is a section titled 'Decompression engine' with a small icon of a folder and a document. A horizontal line separates this from the next section. In the next section, there is a checkbox labeled 'Check for amount of files in archives' which is checked. Below this is a section titled 'Decompression engine options' with a black header. Inside this section, there is a text box labeled 'If number of files within archive exceeds:' with the value '2000' entered. Below the text box are two radio buttons: 'Quarantine' (which is selected) and 'Automatically Delete'.

Screenshot 66 – Optionen zur Überprüfung der Anzahl von Dateien in Archivdateien

Mit Hilfe dieses Filters lassen sich E-Mails mit Archivdateien, in denen eine übergroße Anzahl an komprimierten Dateien enthalten ist, unter Quarantäne stellen oder löschen. Über diesen Filter können Sie die Anzahl an Dateien eingeben, die in einer angehängten Archivdatei maximal erlaubt sind.

So konfigurieren Sie diesen Filter:

1. Klicken Sie unter **Console Root** auf den Knoten **Decompression**.
2. Markieren Sie im rechten Fenster in der Liste der verfügbaren Filter das Kontrollkästchen **Check for amount of files in archives**.
3. Wählen Sie auf der zugehörigen Konfigurationsseite die Option **Check for amount of files in archives**, um diesen Filter zu aktivieren. Geben Sie dann die maximale Anzahl der Dateien an, die in einer Archivdatei enthalten sein darf.

Hinweis: Wenn Sie die Kontrollregel **Check for amount of files in archives** deaktivieren, werden angehängte Archivdateien weder gescannt noch unter Quarantäne gestellt und umgehen somit die Viren-Kontrolle.

4. Mit Hilfe folgender Optionen legen Sie fest, wie mit E-Mails mit Archivdateien verfahren werden soll, in denen mehr Dateien als erlaubt enthalten sind:

- **Quarantine** – Stellt E-Mails mit dieser Art von Archivdateien unter Quarantäne. Diese Mitteilungen können zu einem späteren Zeitpunkt vom Administrator analysiert und freigegeben oder gelöscht werden.
- **Automatically Delete** – Löscht automatisch alle E-Mails mit Archivdateien, in denen die maximal erlaubte Anzahl an Dateien überschritten wird.

5. Klicken Sie auf den Reiter **Actions** um festzulegen, wie mit E-Mails mit dieser Art von Archivdateien, die herausgefiltert und blockiert wurden, verfahren werden soll. Weitere Informationen zur Konfiguration entsprechender Aktionen erhalten Sie im Kapitel „Konfigurieren von Aktionen der Dekomprimierungsfilter“.

6. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Kontrollieren innerhalb von Archivdateien

Mit Hilfe der Option **Scan within archives** kann die Anhangskontrolle und Inhaltskontrolle von in Archivdateien enthaltenen Dateien deaktiviert werden. Ist diese Option deaktiviert, werden angehängte Archivdateien nicht von den Modulen zur Anhangskontrolle und Inhaltskontrolle gescannt.

So konfigurieren Sie diese Option:

1. Klicken Sie unter **Console Root** auf den Knoten **Decompression**.
2. Markieren Sie im rechten Fenster in der Liste der verfügbaren Filter das Kontrollkästchen **Scan within archives**.
3. Wählen Sie auf der zugehörigen Konfigurationsseite die Option **Scan within archives**, um E-Mails mit angehängten Archivdateien über die Regeln zur Inhalts- und Anhangskontrolle scannen zu lassen.

Konfigurieren von Aktionen der Dekomprimierungsfilter

General Actions

Decompression Engine Actions

Notification options

Select the action to take when this rule is violated

Notify administrator

Notify local user

Logging options

Log occurrence to file

File name of log file:

decompression.log

Screenshot 67 – Aktionen eines Dekomprimierungs-Filters

So legen Sie fest, wie mit E-Mails mit Archivdateien zu verfahren ist, die von einem Filter blockiert wurden:

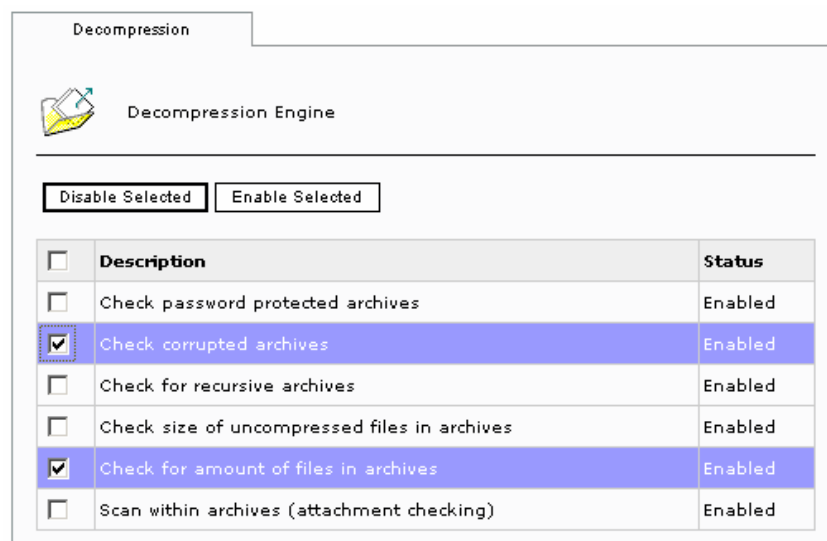
1. Klicken Sie unter dem Knoten **Console Root** auf den Knoten **Decompression**, und wählen Sie im rechten Fenster den jeweiligen Filter aus.

2. Klicken Sie auf den Reiter **Actions**, und wählen Sie alle gewünschten Aktionen:

- **Notify user** – Schickt per E-Mail eine Benachrichtigung an den Empfänger einer Mitteilung, wenn eine an ihn adressierte eingehende E-Mail, die eine Archivdatei enthält, unter Quarantäne gestellt wurde. Wird mit dem gewählten Filter eine ausgehende E-Mail blockiert, erfolgt der Versand einer entsprechenden Mitteilung an den Absender.
- **Notify Administrator** – Schickt per E-Mail eine Benachrichtigung an den Administrator, wenn eine eingehende Mitteilung, die eine Archivdatei enthält, unter Quarantäne gestellt wurde.
- **Log occurrence to file** – Legt bei der Blockierung einer E-Mail durch den gewählten Dekomprimierungsfiler einen Eintrag im Filterprotokoll an. Geben Sie im Eingabefeld **File name of log file** den Namen der Textdatei ein, in der die Protokolldaten gesichert werden sollen, z. B. „PwordArchive.txt“.

3. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Aktivieren/Deaktivieren von Dekomprimierungsfiltren



Screenshot 68 – Liste der Dekomprimierungsfiltren

So aktivieren oder deaktivieren Sie die verfügbaren Dekomprimierungsfiltren:

1. Klicken Sie unter **Console Root** auf den Knoten **Decompression**.
2. Markieren Sie im rechten Fenster die Kontrollkästchen der Filter, die aktiviert oder deaktiviert werden sollen (z. B. **Check for amount of files in archives**).
3. Klicken Sie zur Aktivierung der ausgewählten Regel auf die Schaltfläche **Enable Selected**. Zur Deaktivierung der ausgewählten Regel klicken Sie auf die Schaltfläche **Disable Selected**.

Hinweis: Durch Markieren des obersten Kontrollkästchens neben der Spalte **Description** lassen sich alle Regeln gleichzeitig auswählen.

Der Trojan & Executable Scanner

Einführung

GFI MailSecurity bietet ein fortschrittliches Analyse-Tool für Trojaner und exe-Dateien, den Trojan & Executable Scanner, mit dem die Prozessabläufe einer ausführbaren Datei analysiert und die Auswirkungen ermittelt werden können. Ausführbare Dateien mit verdächtigen Aktionen (z. B. Trojaner) lassen sich unter Quarantäne stellen.

Was ist ein Trojanisches Pferd?

Ein Trojanisches Pferd im Computer-Bereich bezeichnet ein Programm, das auf einem Benutzerrechner unbemerkt installiert wird und seinem Programmierer uneingeschränkten Zugriff auf die auf diesem Rechner gespeicherten Daten verschafft und somit großen Schaden verursachen kann.

Ein Trojaner kann ein einzelnes Programm sein, das ohne Wissen des Anwenders auf seinem Rechner aktiv ist. Ebenso können Trojaner in legitimen Programmen als versteckte Funktion integriert sein.

Unterschied zwischen Trojanern und Viren

Der Unterschied zwischen Trojanern und Viren besteht darin, dass Trojaner oftmals für einen zielgerichteten Einzelangriff verwendet werden, um an bestimmte Daten des Angriffsziels (Anwender/System) zu gelangen. Trojaner werden üblicherweise eingesetzt, um eine Hintertür zu öffnen, durch die ein Angreifer uneingeschränkten Zugriff auf ein System erhält. Auf der Erkennung von Signaturen basierende Anti-Viren-Software kann Trojaner, die für einen Einzelangriff angepasst wurden, nicht aufspüren. Generell gilt, dass Produkte, auch spezielle Anti-Trojaner-Lösungen, die böswillige Software lediglich über Signaturen identifizieren, keinen effektiven Schutz vor diesen Bedrohungen bieten. Solche Lösungen sind nur in der Lage, bereits bekannte Viren und Trojaner zu entdecken. Aus diesem Grund müssen sie häufig aktualisiert werden.

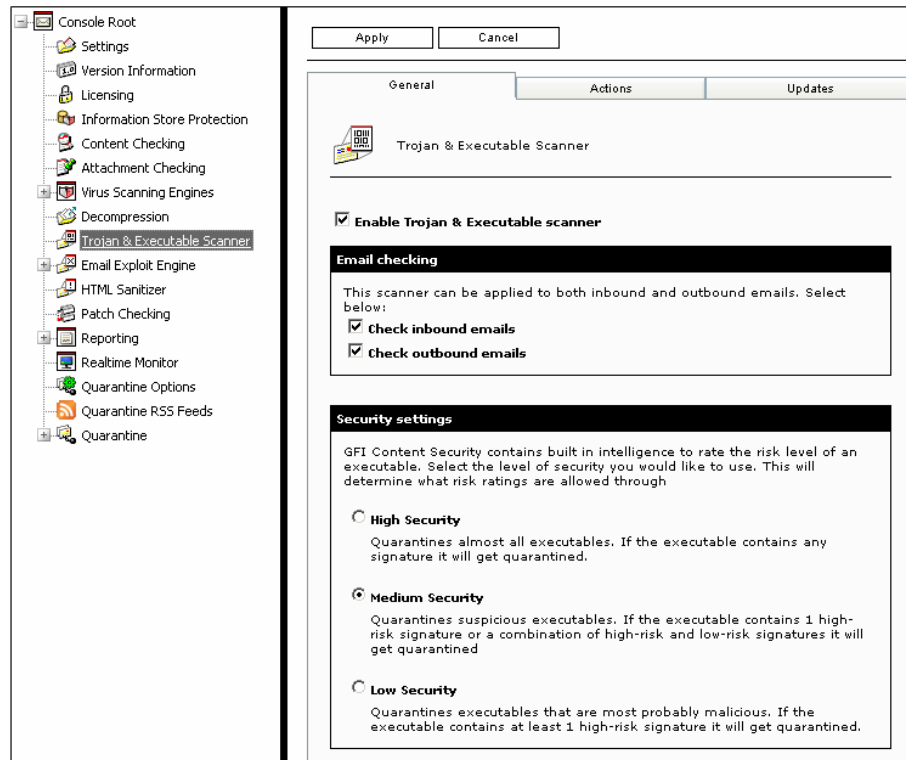
Funktionsweise des Trojan & Executable Scanner

Der Trojan & Executable Scanner von GFI MailSecurity kann den Gefährdungsgrad einer exe-Datei ermitteln, indem die Datei dekompiert und in Echtzeit festgestellt wird, welche Prozessabläufe durch sie gestartet werden könnten. Diese werden dann mit einer Datenbank bekannter böswilliger Aktionen abgeglichen, um den Gefährdungsgrad der exe-Datei zu bestimmen. Dadurch lassen sich potenziell gefährliche, unbekannte Trojaner identifizieren, bevor sie ins Netzwerk gelangen können.

Konfigurieren des Trojan & Executable Scanner

Die Konfiguration des Trojan & Executable Scanner erfolgt über den Knoten **Trojan & Executable Scanner**. Bestimmen Sie, mit welcher Sicherheitsstufe der Scanner Kontrollen vornehmen soll und wie vorzugehen ist, wenn eine E-Mail mit böswilligen exe-Dateien identifiziert wird.

Konfigurieren der Sicherheitsstufe



Screenshot 69 – Trojan & Executable Scanner: Konfigurationsoptionen

So konfigurieren Sie den **Trojan & Executable Scanner**:

1. Klicken Sie unter **Console Root** auf den Knoten **Trojan & Executable Scanner**.
2. Markieren Sie im rechten Fenster der Konfigurationsoptionen das Kontrollkästchen **Enable Trojan & Executable Scanner**, um das Modul zu aktivieren.
3. Legen Sie über folgende Optionen fest, welche E-Mails auf Trojaner und andere böswillige exe-Dateien überprüft werden sollen:
 - **Check inbound emails** – Überprüft eingehende E-Mails auf Trojaner und böswillige exe-Dateien.
 - **Check outbound emails** – Überprüft ausgehende E-Mails auf Trojaner und böswillige exe-Dateien.
4. Legen Sie die gewünschte Sicherheitsstufe über die Auswahl einer der folgenden Optionen fest:
 - **High Security** – Stellt nahezu alle exe-Dateien unter Quarantäne. Die ausführbare Datei wird bei Feststellung einer bekannten böswilligen Signatur sofort unter Quarantäne gestellt.

- **Medium Security** – Stellt verdächtige exe-Dateien unter Quarantäne. Enthält die exe-Datei eine Signatur mit hohem Gefährdungspotenzial oder eine Kombination von Signaturen mit hohem und niedrigem Gefährdungspotenzial, wird sie unter Quarantäne gestellt.
- **Low Security** – Stellt exe-Dateien unter Quarantäne, die als böswillig identifiziert wurden. Enthält die ausführbare Datei mindestens eine Signatur mit hohem Gefährdungsgrad, wird sie sofort unter Quarantäne gestellt.

Festlegen von Vorgehensweisen

The screenshot shows the 'Trojan & Executable Scanner Actions' configuration window with the 'Actions' tab selected. The window has three tabs: 'General', 'Actions', and 'Updates'. Below the title bar, there is a section for 'Notification options' with the instruction 'Please select the action to take when a signature is found'. There are two checkboxes: 'Notify administrator' (checked) and 'Notify local user' (unchecked). Below that is a section for 'Logging options' with a checked checkbox for 'Log occurrence to file:'. Underneath, there is a text input field labeled 'File name of log file:' containing the text 'trojan.txt'.

Screenshot 70 – Trojan & Executable Scanner: Reiter „Actions“

5. Klicken Sie auf den Reiter **Actions** um festzulegen, wie mit E-Mails, in denen eine böswillige exe-Datei entdeckt wurde, verfahren werden soll. Wählen Sie eine der folgenden Optionen:

- **Notify local user** – Schickt per E-Mail eine Benachrichtigung an den Empfänger einer Mitteilung, wenn eine an ihn adressierte eingehende E-Mail, die eine böswillige exe-Datei enthält, unter Quarantäne gestellt wurde. Wird mit dem Scanner eine ausgehende E-Mail blockiert, erfolgt der Versand einer entsprechenden Mitteilung an den Absender.
- **Notify administrator** – Schickt per E-Mail eine Benachrichtigung an den Administrator, wenn eine eingehende Mitteilung, die eine böswillige exe-Datei enthält, unter Quarantäne gestellt wurde.
- **Log occurrence to file** – Legt bei der Identifizierung einer infizierten E-Mail durch den Trojan & Executable Scanner einen Eintrag im Filterprotokoll an. Geben Sie im Eingabefeld **File name of log file** den Namen der Textdatei ein, in der die Protokolldaten gesichert werden sollen, z. B. „Trojan.txt“.

6. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Aktualisieren des Trojan & Executable Scanner

Legen Sie in GFI MailSecurity fest, dass Signatur-Updates für den Trojan & Executable Scanner automatisch heruntergeladen werden. Sie können auch eine Administrator-Mitteilung verschicken lassen, sobald neue Updates verfügbar sind.

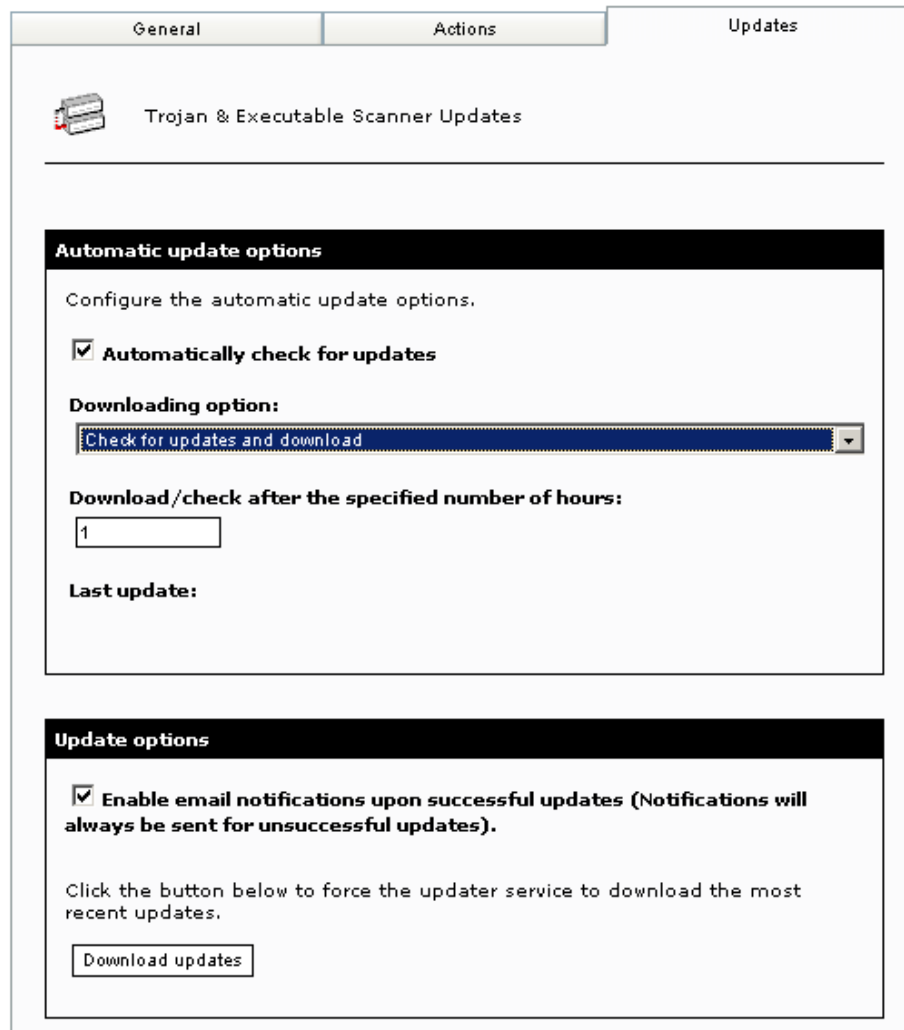
So konfigurieren Sie die automatischen Updates:

1. Klicken Sie unter **Console Root** auf den Knoten **Trojan & Executable Scanner**.
2. Klicken Sie im rechten Fenster des Trojan & Executable Scanner auf den Reiter **Updates**.
3. Wählen Sie die Option **Automatically check for updates**, wenn die Aktualisierung der Signatur-Updates automatisch erfolgen soll.
4. Wählen Sie über die angezeigte Drop-Down-Liste **Downloading options** eine der folgenden Download-Optionen aus:

- **Only check for updates** – GFI MailSecurity überprüft lediglich, ob Updates für den Trojan & Executable Scanner zur Verfügung stehen, um dann den Administrator darüber zu benachrichtigen.

Hinweis: Bei Auswahl dieser Option erfolgt KEIN Download eventuell verfügbarer Updates.

- **Check for updates and download** – GFI MailSecurity überprüft, ob für den Trojan & Executable Scanner neue Updates zur Verfügung stehen, um diese dann ggf. automatisch herunterzuladen.
5. Legen Sie fest, wie in welchem zeitlichen Abstand GFI MailSecurity nach Updates für den Trojan & Executable Scanner suchen und diese downloaden soll (Angabe in Stunden).
 6. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.



Screenshot 71 – Trojan & Executable Scanner: Reiter "Updates"

Manuelles Abrufen von Aktualisierungen

Um sofort nach Updates für den Trojan & Executable Scanner zu suchen und diese herunterzuladen, klicken Sie auf die Schaltfläche **Download updates**.

Die Email Exploit Engine

Einführung

Was ist ein Exploit?

Ein Exploit nutzt bekannte Anfälligkeiten/Sicherheitslücken in Applikationen oder Betriebssystemen aus. Dank dieser Schwachstellen überlistet er die Sicherheitskontrollen des Systems und führt beispielsweise ein Programm oder einen Befehl aus oder richtet eine Hintertür ein. Es nutzt somit eine Programm- oder Betriebssystem-Funktion für seine eigenen Zwecke.

Was ist ein E-Mail-Exploit?

Ein E-Mail-Exploit ist ein Exploit, der per E-Mail übertragen und gestartet wird. Er wird auf dem Rechner des Empfängers ausgeführt, sobald der Anwender die Nachricht öffnet oder empfängt. Dies ermöglicht es Hackern, eine Firewall und Anti-Viren-Produkte zu umgehen.

Unterschied zwischen Anti-Viren-Software und der Email Exploit Engine

Anti-Viren-Software ist so konzipiert, dass bösartiger und schädlicher Programmcode erkannt wird. Die Methode zum Ausführen des Programmcodes muss hierbei nicht zwingend analysiert werden.

Die Email Exploit Engine analysiert E-Mails und durchsucht sie nach Exploits, d. h., sie scannt nach Verfahren, die eingesetzt werden, um ein Programm oder einen Befehl auf dem System des Anwenders auszuführen. Die Engine prüft hierbei nicht, ob das Programm oder der Befehl bösartig ist oder nicht. Bei der Überprüfung wird bereits ein Sicherheitsrisiko angezeigt, sobald eine E-Mail einen Exploit verwendet, um ganz allgemein ein Programm oder einen Befehl auszuführen.

Auf diese Weise arbeitet die Email Exploit Engine wie ein Zugangskontrollsystem (IDS – Intrusion Detection System) für E-Mails. Die Engine kann u. U. eine höhere Anzahl von Fehlalarmen auslösen, bietet gleichzeitig aber auch eine wesentlich höhere Sicherheit gegenüber gängigen Anti-Viren-Lösungen, weil mit ihr ein ganz anderer Ansatz bei der Kontrolle potenziell gefährlicher E-Mails verfolgt wird.

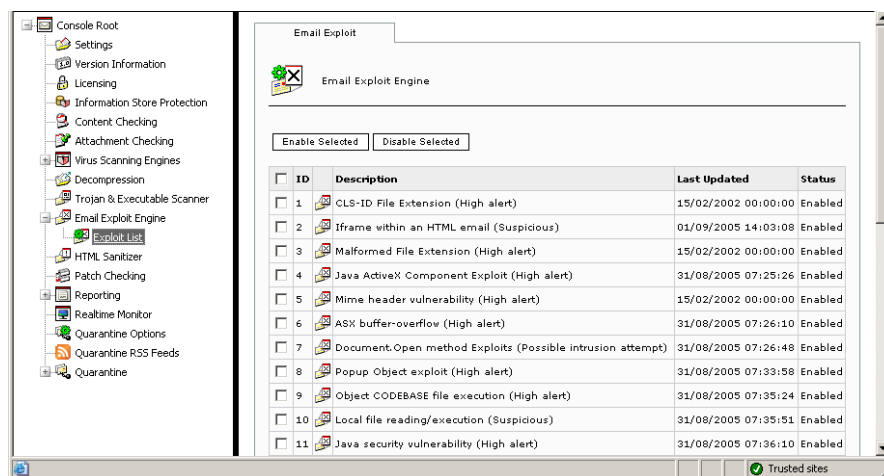
Zudem ist die Email Exploit Engine für das Auffinden von Exploits in E-Mails optimiert und gewährleistet daher eine wesentlich effizientere Überprüfung als herkömmliche Anti-Viren-Engines.

Konfigurieren der Email Exploit Engine

Aktivieren/Deaktivieren von E-Mail-Exploits

So aktivieren/deaktivieren Sie E-Mail-Exploits:

1. Gehen Sie auf **Console Root** ▶ **Email Exploit Engine**, und klicken Sie auf den Unterknoten **Exploit List**.
2. Wählen Sie im rechten Fenster zur Email Exploit Engine alle Kontrollkästchen der Exploits aus, deren Kontrolle Sie aktivieren oder deaktivieren möchten.
3. Klicken Sie zur Aktivierung der ausgewählten Regel auf die Schaltfläche **Enable Selected**. Zur Deaktivierung der ausgewählten Regel klicken Sie auf die Schaltfläche **Disable Selected**. Die Änderungen werden sofort in der Status-Spalte der Exploits angezeigt.

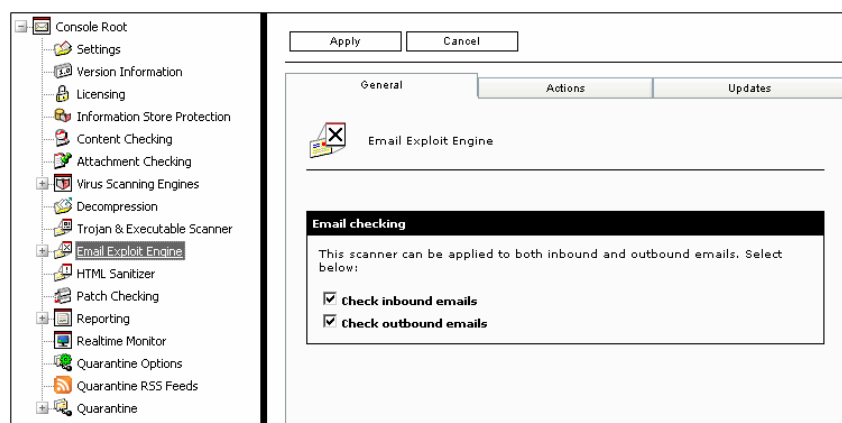


Screenshot 72 – Konfiguration der Email Exploit Engine

Konfigurieren der Eigenschaften der Email Exploit Engine

So konfigurieren Sie die Eigenschaften der Email Exploit Engine:

1. Klicken Sie unter **Console Root** auf den Knoten **Email Exploit Engine**.
2. Wählen Sie über den Reiter **General** aus, ob ein- und/oder ausgehende E-Mails auf Exploits untersucht werden sollen, indem Sie das Kontrollkästchen **Check inbound mails** und/oder **Check outbound mails** markieren.



Screenshot 73 – Email Exploit Engine: Reiter „General“

3. Klicken Sie auf den Reiter **Actions** um festzulegen, wie E-Mails behandelt werden sollen, in denen ein Exploit gefunden wurde.

4. Wählen Sie eine der folgenden Optionen aus:

- **Quarantine email** – Stellt die E-Mail mit dem Exploit bis zur Überprüfung durch den Administrator unter Quarantäne. Weitere Informationen hierzu erhalten Sie im Kapitel „E-Mail-Quarantäne“ in diesem Handbuch.
- **Delete email** – Löscht die E-Mail samt Exploit.

5. Wird ein E-Mail-Exploit identifiziert, kann der Administrator und/oder autorisierte Anwender per E-Mail darüber informiert werden. Die Benachrichtigung kann durch Auswahl folgender Optionen eingerichtet werden:

- **Notify user** – Informiert den angegebenen Empfänger einer Nachricht per E-Mail, wenn die Mitteilung einen Exploit enthält.

Hinweis: Ist die blockierte E-Mail eingehend, werden mit dieser Option nur die Empfänger der Mitteilung benachrichtigt. Bei ausgehenden E-Mails erfolgt eine entsprechende Benachrichtigung an den Absender.

- **Notify administrator** – Informiert den Administrator per E-Mail, wenn eine Nachricht einen Exploit enthält. Die E-Mail-Adresse des Administrators wird während der Installation von GFI MailSecurity angegeben und kann zu einem späteren Zeitpunkt über das Konfigurationsmenü geändert werden (über **Console Root** ▶ Knoten **Settings** ▶ Reiter **General**). Nähere Informationen hierzu erhalten Sie im Kapitel „Allgemeine Einstellungen“ unter „Angabe der E-Mail-Adresse des Administrators“.

General Actions Updates

Email Exploit Actions

Actions

Please select the action to take when one of the listed exploits is detected

Quarantine email

Delete email

Notification options

Notify administrator

Notify local user

Logging options

Log occurrence to file

File name of log file:

EmailExploit.bt

Screenshot 74 – Email Exploit Engine: Reiter „Actions“

6. Wählen Sie die Option **Log occurrence to file**, wenn Informationen zu identifizierten E-Mail-Exploits in einer Protokolldatei gesichert werden sollen. Geben Sie im Eingabefeld **File name of log file** den Namen der Protokolldatei an.

7. Klicken Sie auf die Schaltfläche **Apply**, um die Einstellungen zu speichern.

Aktualisieren der Email Exploit Engine

Legen Sie in GFI MailSecurity fest, dass Updates für die Email Exploit Engine automatisch heruntergeladen werden, oder lassen Sie eine Administrator-Mitteilung verschicken, sobald neue Updates verfügbar sind.

So konfigurieren Sie die automatischen Updates:

1. Klicken Sie unter **Console Root** auf den Knoten **Email Exploit Engine**.

2. Gehen Sie auf den Reiter **Updates**.

3. Wählen Sie die Option **Automatically check for updates**, wenn die Aktualisierung der Signatur-Updates automatisch erfolgen soll.

4. Wählen Sie über die angezeigte Drop-Down-Liste **Downloading options** eine der folgenden Download-Optionen aus:

- **Only check for updates** – Wählen Sie diese Option, wenn GFI MailSecurity nur überprüfen soll, ob für die Email Exploit Engine Updates zur Verfügung stehen, um dann den Administrator darüber zu benachrichtigen.

Hinweis: Bei Auswahl dieser Option erfolgt KEIN Download eventuell verfügbarer Updates.

- **Check for updates and download** – GFI MailSecurity überprüft, ob für die Email Exploit Engine neue Updates zur Verfügung stehen, um diese dann ggf. automatisch herunterzuladen.

5. Legen Sie fest, wie in welchem zeitlichen Abstand GFI MailSecurity nach Updates für die Email Exploit Engine suchen und diese downloaden soll (Angabe in Stunden).

6. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

General
Actions
Updates

Email Exploit Updates

Automatic update options

Configure the automatic update options.

Automatically check for updates

Downloading option:

Check for updates and download
▼

Download/check after the specified number of hours:

1

Last update:

Update options

Enable email notifications upon successful updates (Notifications will always be sent for unsuccessful updates).

Click the button below to force the updater service to download the most recent updates.

Download updates

Screenshot 75 – Email Exploit Engine: Reiter „Updates“

Manuelles Abrufen von Aktualisierungen

Um sofort nach Updates für die Email Exploit Engine zu suchen und diese herunterzuladen, klicken Sie auf die Schaltfläche **Download updates**.

Der HTML Sanitizer

Einführung

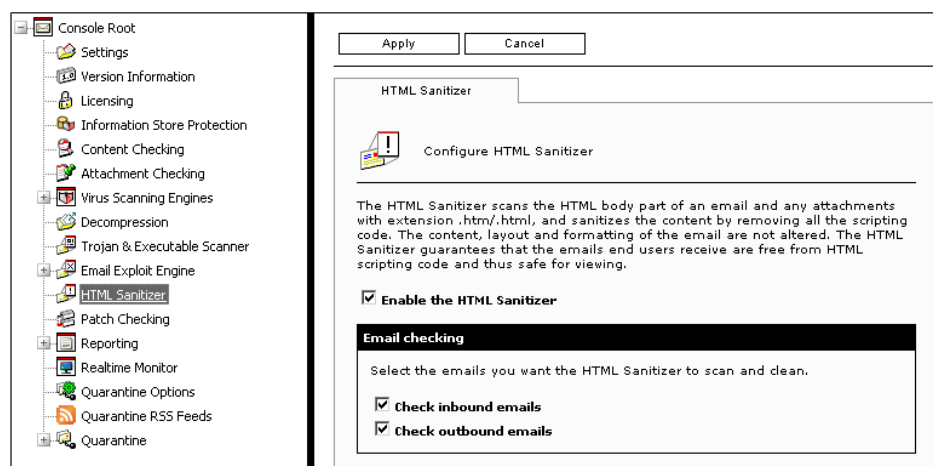
Mit Hilfe des HTML Sanitizer werden die Teile des E-Mail-Textkörpers gescannt und von Skript-Code bereinigt, deren MIME-Typ „text/html“ ist. Gleiches gilt für Anhänge, die die Erweiterung „.htm“ oder „.html“ besitzen. Der HTML-Code wird aus allen Skripten entfernt, sodass er keine Gefahr mehr darstellt. Die Bereinigung von HTML-Code erfolgt vollkommen automatisch und erfordert kein Eingreifen von Seiten des Administrators.

Warum sollten HTML-Skripten entfernt werden?

Dank der HTML-Funktionalität von E-Mails ist es Absendern möglich, elektronische Post mit Skripten zu versehen, die beim Öffnen der Mitteilung automatisch gestartet werden. Zahlreiche Viren machen sich HTML-Skripten zu Nutze und sind dadurch schon häufig zu zweifelhaftem Ruhm gekommen – der KAK-Wurm ist hier nur ein Beispiel von vielen. HTML-Skripten können auch speziell gegen einzelne Anwender und Unternehmen eingesetzt werden. Somit sollte diese Art von Skripten generell aus E-Mails entfernt werden.

Der im Lieferumfang von GFI MailSecurity enthaltene HTML Sanitizer bietet automatisierten Schutz vor Gefahren durch HTML-Skripten.

Konfigurieren des HTML Sanitizer



Screenshot 76 – Eigenschaften des HTML Sanitizer

So konfigurieren Sie den HTML Sanitizer:

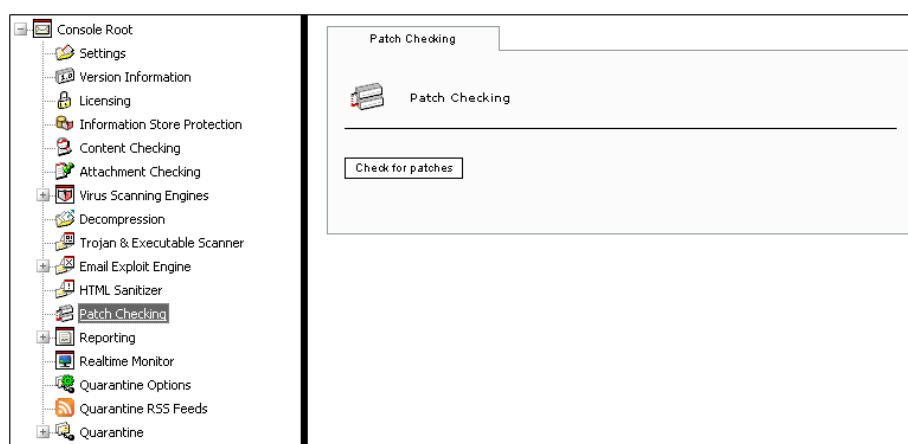
1. Klicken Sie unter **Console Root** auf den Knoten **HTML Sanitizer**.

2. Markieren Sie auf der Konfigurationsseite des HTML Sanitizer das Kontrollkästchen **Enable the HTML Sanitizer**, um das Modul zu aktivieren.
3. Wählen Sie aus, ob ein- und/oder ausgehende E-Mails auf HTML-Skripten überprüft werden und davon bereinigt werden sollen:
 - **Check inbound emails** – Überprüft und bereinigt eingehende E-Mails von HTML-Skripten.
 - **Check outbound emails** – Überprüft und bereinigt ausgehende E-Mails von HTML-Skripten.
4. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Überprüfen auf Produkt-Patches

Einführung

Mit Hilfe der Funktion **Patch Checking** können Sie kontrollieren, ob für Ihre Version von GFI MailSecurity Software-Patches verfügbar sind. Hierfür wird eine direkte Verbindung mit den Update-Servern von GFI hergestellt.



Screenshot 77 – Liste verfügbarer Patches

Sind über die GFI-Server Software-Updates verfügbar, werden sie mit Hilfe dieser Funktion angezeigt und können von Ihnen heruntergeladen werden. Über die Liste der verfügbaren Updates erhalten Sie zudem anhand eines entsprechenden Links Informationen zu jedem Patch sowie zu einem zugehörigen Knowledge-Base-Artikel (falls verfügbar).

Hinweis 1: Um eine effiziente Verwendung von GFI MailSecurity sicherzustellen, ist es zu empfehlen, eine regelmäßige Überprüfung auf Software-Updates durchzuführen. Updates garantieren die optimale Leistungsfähigkeit von GFI MailSecurity und erweitern die Funktionalität des Programms.

Hinweis 2: Weitere Informationen zur Angabe des gewünschten Update-Servers von GFI erhalten Sie im Kapitel „Allgemeine Einstellungen“ unter „Auswählen des Update-Servers“.

Downloaden und Installieren von Software-Patches

So kontrollieren Sie, ob Software-Updates für GFI MailSecurity vorliegen:

1. Klicken Sie unter dem Knoten **Console Root** auf **Patch Checking**. Klicken Sie dann im rechten Fenster auf die Schaltfläche **Check for**

patches, um eine Verbindung mit dem Update-Server von GFI herzustellen und nach verfügbaren Updates zu suchen.

2. Wenn Software-Patches für Ihre Version von GFI MailSecurity vorliegen, werden diese im rechten Fenster angezeigt. Andernfalls erhalten Sie die Mitteilung, dass keine Patches zur Verfügung stehen. Klicken Sie im rechten Fenster in der Liste der verfügbaren Software-Updates neben dem jeweiligen Patch auf den Link **Download**. Die Updates werden heruntergeladen. Wiederholen Sie den Vorgang für alle aufgeführten Patches.

3. Nachdem alle Downloads abgeschlossen sind, können Sie die Updates installieren. Da die Software-Patches in verschiedenen Dateiformaten vorliegen können (z. B. als DLL- oder exe-Dateien), lesen Sie bitte die entsprechenden Hinweise zur Installation eines Patches. Diese Hinweise und andere wichtige Informationen zu einem Patch erhalten Sie durch einen Klick auf **Information** rechts neben dem jeweiligen Patch.

Hinweis 1: Befolgen Sie auf jeden Fall die über „Information“ verfügbaren Installationsanweisungen. Durch eine falsche Patch-Installation kann es zu Fehlfunktionen des Produkts oder Leistungseinbußen kommen.

Hinweis 2: Falls verfügbar, steht ein Link zur Knowledge-Base zur Verfügung, über den ein Artikel mit weiteren Informationen zum entsprechenden Patch abrufbar ist. In einem solchen Fall erscheint der Hinweis **KB Article** unmittelbar neben dem Patch-Datum. Per Klick auf **KB Article** wird der Knowledge-Base-Artikel direkt aufgerufen.

Hinweis 3: GFI MailSecurity verschickt automatisch eine Mitteilung an den Administrator, sobald ein neuer Software-Patch gefunden wird.

Die E-Mail-Quarantäne

Einführung

Sie können GFI MailSecurity so konfigurieren, dass E-Mails, die bei einem Sicherheitscheck (z. B. durch die Anhangskontrolle) herausgefiltert wurden, unter Quarantäne gestellt werden. Unter Quarantäne gestellte E-Mails müssen vor einer möglichen Weiterleitung durch den Administrator oder einen Sicherheitsbeauftragten überprüft (d. h. freigegeben oder gelöscht) werden.

Unter Quarantäne gestellte E-Mails lassen sich auf folgende Weise freigeben oder löschen:

1. Direkt über den Quarantänebereich (empfohlen). Weitere Informationen hierzu erhalten Sie in diesem Kapitel unter „Freigeben von E-Mails über den Quarantänebereich“.
2. Per HTML-Freigabeformular, das an die E-Mail-Adresse des Administrators oder die E-Mail-Adresse einer zur Überprüfung autorisierten Person geschickt wird. Weitere Informationen hierzu erhalten Sie in diesem Kapitel unter „Freigeben von E-Mails per HTML-Freigabeformular“.

Der Quarantäne-Bereich („Quarantine Store“)

The screenshot displays the 'Quarantine' management interface. On the left is a navigation tree with 'Quarantine' highlighted. The main area contains a 'Quick Search' section with three search criteria: 'sender/recipients', 'subject', and 'quarantine reason', each with an input field and a 'Search' button. Below this is a 'Quarantined Items' table showing counts for different time periods.

Folder	Items
Today	0
Yesterday	0
This week	0
All items	1

Below the table is a 'Current search folders' section with a table header: Folder, Items, Auto-purging. A 'New search folder...' button is located at the bottom of the interface.

Screenshot 78 – Statusseite des Quarantänebereichs

GFI MailSecurity speichert blockierte E-Mails in einem Quarantänebereich. Dieser Bereich lässt sich über den Knoten **Console Root ▶ Quarantine** aufrufen. Er erlaubt es Administratoren oder autorisierten Benutzern, E-Mails zu kontrollieren, die unter Quarantäne gestellt wurden, und diese Nachrichten freizugeben oder zu löschen.

Wenn Sie auf den Knoten **Quarantine** klicken, öffnet sich im rechten Fenster die Status-Seite des Quarantänebereichs. Auf dieser Seite erhalten Sie eine Übersicht über die Anzahl der sich aktuell in Quarantäne befindlichen E-Mails sowie eine Aufschlüsselung nach Zeitpunkt der Filterung („heute“, „gestern“ und „diese Woche“). Zudem haben Sie über eine Funktion zur Schnellsuche die Möglichkeit, anhand der Absender-/Empfängeradresse oder über die Angabe von Stichwörtern aus dem E-Mail-Betreff oder aus der Begründung der Blockierung nach bestimmten Quarantäne-Mails zu suchen.

Um alle am heutigen Tag unter Quarantäne gestellten E-Mails anzeigen zu lassen, klicken Sie in der Status-Seite im rechten Fenster auf **Today**. Zur Anzeige aller Quarantäne-Nachrichten bzw. der gestern oder in dieser Woche unter Quarantäne gestellten Nachrichten, klicken Sie auf **All emails, Yesterday** oder **This Week**. Dieselben Übersichten erhalten Sie auch, wenn Sie die Struktur des Knotens **Quarantine** erweitern und auf die Unterknoten **All emails, Today, Yesterday** bzw. **This Week** klicken.

Suchordner

Der Knoten **Quarantine** bietet zudem einen Unterknoten **Search Folders** mit Suchordnern. Über diese Suchordner steht Ihnen ebenfalls das Tool zur Schnellsuche von Nachrichten zur Verfügung. Des Weiteren haben Sie über die Suchordner die Möglichkeit, für jeden Filter einen Ordner zu erstellen, um die blockierten E-Mails nach Filtermethoden zu sortieren. Erstellen Sie beispielsweise für jeden E-Mail-Filter von GFI MailSecurity einen eigenen Suchordner. Das Einsortieren einer Quarantäne-Mitteilung in den Ordner des Filters, von dem sie blockiert wurde, bietet mehr Übersichtlichkeit. Als weitere Möglichkeit können Sie einen Suchordner erstellen, in dem nur solche E-Mails enthalten sind, die von den Viren-Scan-Engines unter Quarantäne gestellt wurden.

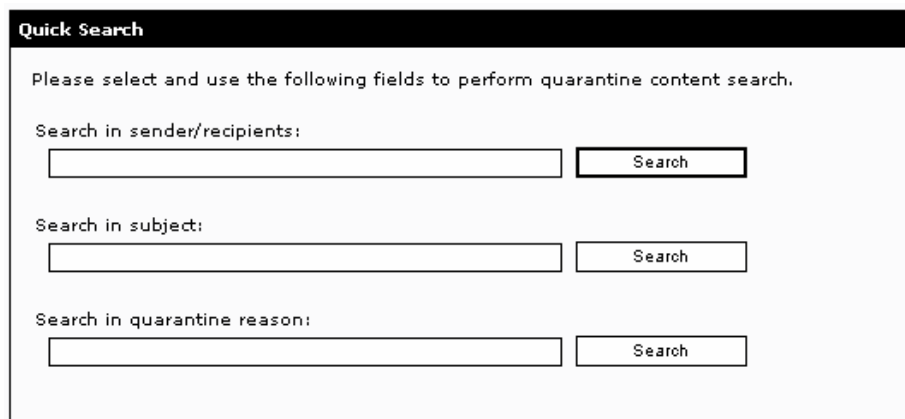
Suchordner dienen somit der gezielten Filterung von E-Mails aus Ihrem Quarantänebereich. Jede Suchordner-Kategorie wird als Unterknoten zum Suchordner eingerichtet. Neue Suchordner lassen sich problemlos einrichten. In jedem Ordner können E-Mails unter anderem nach Datum, Uhrzeit und Stichwort gruppiert werden. Administratoren haben über die Suchordner zudem die Möglichkeit, Quarantäne-Mails direkt freizugeben oder endgültig zu löschen.

Hinweis: Beachten Sie, dass eine E-Mail von mehr als einem Filter unter Quarantäne gestellt werden kann, z. B. weil sie einen bekannten Virus enthält und gleichzeitig einen übergroßen Anhang. In diesem Fall wird eine Kopie der Mitteilung sowohl im Suchordner für die Anti-Viren-Engine als auch im Suchordner für die Anhangskontrolle abgelegt (falls eingerichtet). Das Freigeben oder Löschen dieser Mitteilung durch den Administrator braucht jedoch lediglich über einen der Suchordner zu erfolgen. Soll ein Suchordner nur solche Elemente enthalten, die allein von einem bestimmten E-Mail-Filter unter Quarantäne gestellt wurden, wählen Sie in den Eigenschaften des

Suchordners (**Properties**) neben der Filteroption **Quarantined by** das Kontrollkästchen **only** aus. Weitere Informationen hierzu erhalten Sie in diesem Kapitel unter „Einordnen von Quarantäne-Mails in Suchordnern“.

Suchen nach E-Mails im Quarantänebereich

Mit Hilfe des integrierten Tools zur Schnellsuche können in den Quarantänebereich verschobene E-Mails rasch aufgefunden werden. Nachrichten lassen sich nach der E-Mail-Adresse des Empfängers/Absenders oder nach Stichwörtern im Betreff oder in der Quarantäne-Begründung durchsuchen.

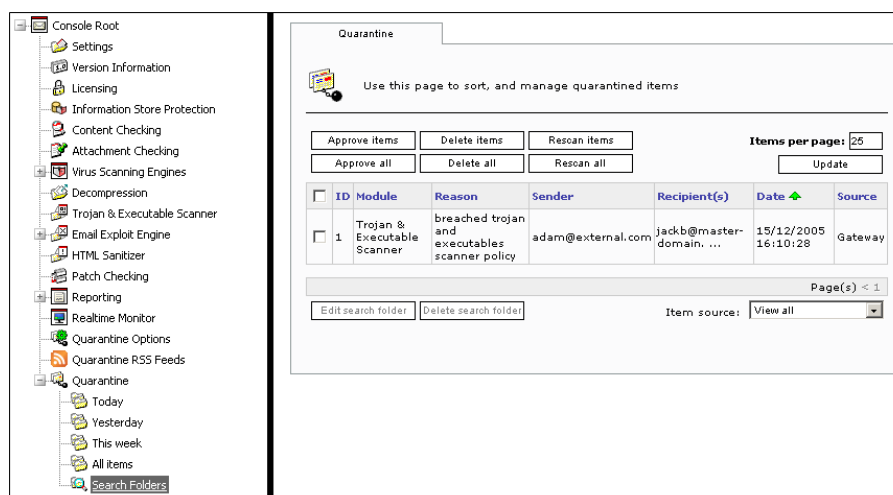


Screenshot 79 – Quarantänebereich Schnellsuche

Schnellsuche

So starten Sie die Schnellsuche von E-Mails im Quarantänebereich:

1. Erweitern Sie unter **Console Root** die Struktur des Knotens **Quarantine**, und klicken Sie auf den Unterknoten **Search Folders**.
2. Auf der Seite **Quick Search** im rechten Fenster stehen folgende Suchmethoden zur Verfügung:
 - **Search in sender/recipients** – Geben Sie im Eingabefeld die E-Mail-Adresse eines Absenders oder Empfängers ein, um dessen blockierte Mitteilungen zu suchen. Klicken Sie zum Starten der Suche auf die Schaltfläche **Search**.
 - **Search in subject** – Geben Sie im Eingabefeld ein Stichwort oder einen Begriff ein um die Betreffzeilen der unter Quarantäne gestellten E-Mails zu durchsuchen. Klicken Sie zum Starten der Suche nach dem Stichwort/Begriff auf die Schaltfläche **Search**.
 - **Search in quarantine reason** – Geben Sie im Eingabefeld ein Stichwort oder einen Begriff ein, um die Quarantäne-Begründung der blockierten E-Mails danach zu durchsuchen. Klicken Sie zum Starten der Suche auf die Schaltfläche **Search**.



Screenshot 80 – Suchergebnisse

Einordnen von Quarantäne-Mails in Suchordnern

Erstellen Sie mit GFI MailSecurity Suchordner, um unter Quarantäne gestellte E-Mails gemäß den von Ihnen angegebenen Suchkriterien sortieren zu lassen. Per Suchordner werden E-Mails aus dem Quarantänebereich somit nach bestimmten dynamischen Suchkriterien gefiltert und in den entsprechenden Ordnern gruppiert. Diese Ordner werden als Unterknoten unter dem Knoten **Search Folders** angelegt.

Für jeden Ordner lassen sich unterschiedliche Suchkriterien festlegen, sodass der Quarantänebereich übersichtlich in einzelne Filtergruppen unterteilt werden kann. Als weitere Möglichkeit können Sie einen Suchordner erstellen, indem nur solche E-Mails enthalten sind, die von den Viren-Scan-Engines unter Quarantäne gestellt wurden.

Der Hauptvorteil von Suchordnern besteht darin, dass sich unter Quarantäne gestellte E-Mails leichter verwalten lassen. Administratoren können blockierte Mitteilungen schneller überprüfen und freigeben bzw. löschen.

So erstellen Sie einen neuen Suchordner:

1. Erweitern Sie unter **Console Root** die Struktur des Knotens **Quarantine**, und klicken Sie auf den Unterknoten **Search Folders**.
2. Klicken Sie auf der rechten Seite zur Schnellsuche auf die Schaltfläche **New search folder**.

New Search Folder

Use this page to create and edit search folders.

Define a new folder

Search folder name:

Item source

Please select item source.

Auto-Purging

With the auto-purge option, you can automate the management of the items stored in this search folder. Items that have been quarantined for at least the number of days you specify will be automatically deleted from the quarantine system.

Enable Auto-purging

Automatically purge items older than:

 days(s)

Keyword search

Quarantine reason:

Item subject:

Sender:

Recipient:

Search options

Quarantined by:

 Attachment Checking only

Item direction:

 Inbound

Date filter

Date:

Day from: **Time from: (hh:mm:ss:am/pm)** 12:00:00:PM

Day to: **Time to: (hh:mm:ss:am/pm)** 12:00:00:PM

Specific date

Screenshot 81 – Eigenschaften eines neuen Suchordners

3. Geben Sie im rechten Fenster in der Eigenschaftenseite im Eingabefeld **Search folder name** den Namen des neuen Ordners ein (z. B. „Blockierung per Anhangscontrollregel“).

4. Ist GFI MailSecurity auf dem Exchange-Rechner installiert, können Sie die jeweilige Quelle des unter Quarantäne gestellten Elements angeben. Wählen Sie aus der Drop-Down-Liste unter **Item source** eine der folgenden Optionen aus:

- **Information store** – Nur unter Quarantäne gestellte Elemente des Informationsspeichers werden angezeigt.
- **Gateway** – Nur unter Quarantäne gestellte ein- oder ausgehende E-Mails (SMTP-Datenverkehr) werden angezeigt.
- **Any** – Alle unter Quarantäne gestellten Elemente werden angezeigt, ungeachtet ihrer Quelle.

Hinweis: Die Gruppe **Item source** wird nur dann angezeigt, wenn GFI MailSecurity auf dem Exchange-Server installiert ist.

5. Legen Sie optional die Einstellungen für das automatische Löschen von Nachrichten aus dem Suchordner fest. Ist die Funktion zum automatischen Löschen aktiviert, werden E-Mails des jeweiligen Suchordners nach einer von Ihnen festgelegten Frist selbsttätig gelöscht.

Aktivieren Sie die Lösch-Funktion, indem Sie das Kontrollkästchen **Enable Auto-purging** markieren und im Eingabefeld **day(s)** einen Wert in Tagen angeben.

Hinweis: Die Funktion zum automatischen Löschen ist mit Vorsicht zu konfigurieren, da hiermit aus dem Quarantänebereich gelöschte E-Mails nicht wiederhergestellt werden können.

6. Geben Sie die Suchkriterien an, nach denen E-Mails in diesen Ordner einsortiert werden sollen. Folgende Optionen stehen zur Auswahl:

- **Quarantine reason** – Berücksichtigt alle E-Mails mit einem bestimmten Stichwort oder Begriff in der Begründung der Quarantäne. Geben Sie das Stichwort/den Begriff im entsprechenden Eingabefeld ein.
- **Item subject** – Berücksichtigt alle E-Mails mit einem bestimmten Stichwort oder Begriff im Betreff der E-Mail. Geben Sie das Stichwort/den Begriff im entsprechenden Eingabefeld ein.
- **Sender** – Sortiert NUR die E-Mails eines bestimmten Absenders ein. Geben Sie die gewünschte E-Mail-Adresse im entsprechenden Eingabefeld ein.
- **Recipient** – Sortiert NUR die E-Mails eines bestimmten Empfängers ein. Geben Sie die gewünschte E-Mail-Adresse im entsprechenden Eingabefeld ein.
- **Quarantined by** – Sortiert alle E-Mails, die von einem bestimmten Filter (jedoch nicht unbedingt ausschließlich von diesem) unter Quarantäne gestellt wurden, in diesem Ordner ein. Wählen Sie den gewünschten Filter (z. B. zur Anhangskontrolle) aus der Drop-Down-Liste neben dieser Option aus.

Hinweis: Eine blockierte E-Mail kann aus mehreren Gründen unter Quarantäne gestellt worden sein. Sie können daher festlegen, dass in diesem Ordner nur solche Nachrichten einzusortieren sind, die von keinem anderen als dem aktuell gewählten Filter blockiert wurden. Wählen Sie hierfür die Option **only** neben der Drop-Down-Liste aus.

- **Item direction** – Legt fest, ob die in diesem Suchordner abzulegenden Elemente eingehend oder ausgehend sein müssen.

Hinweis 1: Um sowohl ein- als auch ausgehende E-Mails in diesen Suchordner einsortieren zu lassen, wählen Sie diese Option bitte nicht aus.

Hinweis 2: Diese Option ist nur dann aktiviert, wenn GFI MailSecurity nicht auf einem Exchange-Server installiert ist oder wenn **Gateway** als **Item source** ausgewählt wurde.

- **Date** – Sortiert E-Mails eines bestimmten Datums ein. Geben Sie das Datum im Eingabefeld ein, oder klicken Sie auf das Kalender-Symbol, um einen Kalender aufzurufen, über den Sie das Datum auswählen können.

Auswählen eines Zeitraums

E-Mails lassen sich auch nach Zeitraum in einem Ordner gruppieren. Geben Sie hierfür im ersten Eingabefeld **Day from** das Anfangsdatum an. Geben Sie im zweiten Eingabefeld **Day to** dann das Enddatum ein.

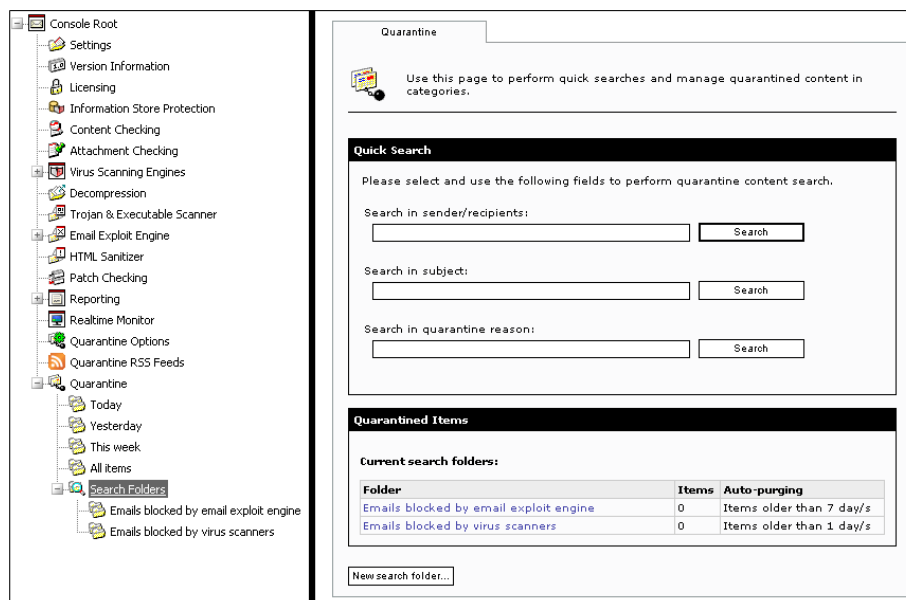
Angabe einer Uhrzeit

Zusätzlich zum Datum können Sie auch eine Uhrzeit (punktuell oder Zeitraum) für die Einsortierung angeben. Markieren Sie hierfür das Kontrollkästchen **Time from**, und geben Sie die Uhrzeit im Eingabefeld ein.

Angabe einer Uhrzeit (Zeitraum)

Um einen Zeitraum an einem bestimmten Tag anzugeben, klicken Sie auf die Schaltfläche **Specific date**. Geben Sie danach im Eingabefeld **Time from** den Beginn und im Eingabefeld **Time to** das Ende des Zeitraums an.

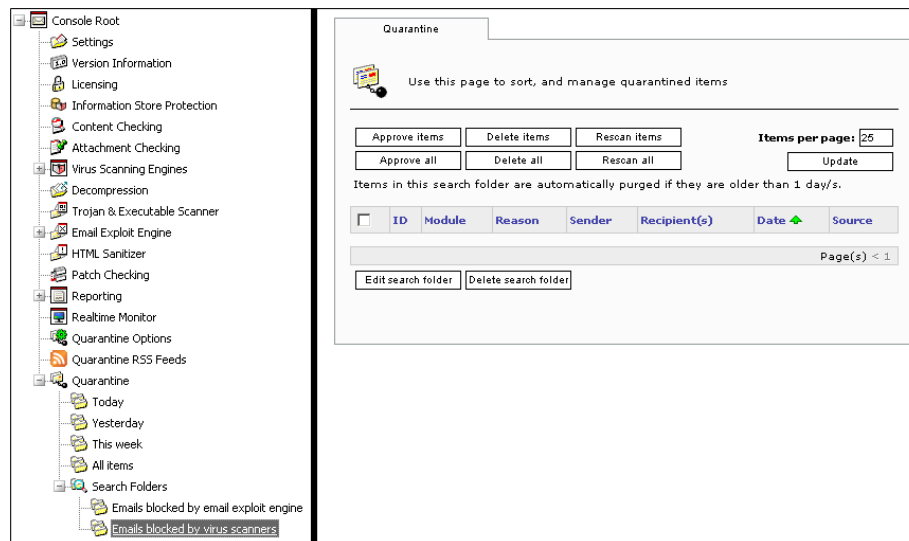
7. Nachdem Sie alle gewünschten Sortierkriterien angegeben haben, klicken Sie auf die Schaltfläche **Save Folder**, um den neuen Suchordner zu erstellen.



Screenshot 82 – Überblick über Suchordner-Inhalte

Hinweis: Klicken Sie auf den Knoten **Search Folder**, um die Anzahl der in jedem Suchordner enthaltenen E-Mails anzeigen zu lassen.

Ändern der Eigenschaften von Suchordnern



Screenshot 83 – Optionen des Suchordners

So ändern Sie die Eigenschaften, Suchkriterien und automatische Lösch-Funktion eines Suchordners:

1. Erweitern Sie die Struktur des Knotens **Quarantine** und dann die des Unterknotens **Search Folders**.
2. Klicken Sie auf den zu ändernden Suchordner und dann im rechten Fenster auf die Schaltfläche **Edit Search Folder**.
3. Ändern Sie die Eigenschaften wie gewünscht. Weitere Informationen zur Konfigurierung der Optionen von Suchordnern erhalten Sie in diesem Kapitel unter „Einordnen von Quarantäne-Mails in Suchordnern“.
4. Klicken Sie auf die Schaltfläche **Save Folder**, um Ihre Änderungen zu bestätigen.

Löschen von Suchordnern

So löschen Sie einen Suchordner:

1. Erweitern Sie die Struktur des Knotens **Quarantine** und dann die des Unterordners **Search Folders**.
2. Wählen Sie den zu löschenden Suchordner im rechten Fenster aus, und klicken Sie auf die Schaltfläche **Delete search folder**.

Hinweis: Beim Löschen eines Suchordners werden KEINE E-Mails gelöscht oder gehen verloren. Wie zuvor beschrieben, handelt es sich bei Suchordnern lediglich um Abfrage-Tools, mit denen sich E-Mails aus dem Quarantänebereich auf verschiedene Art sortieren lassen. Dennoch können E-Mails aus einem Suchordner heraus mit den Schaltflächen **Delete Emails** und **Delete All** freigegeben oder gelöscht werden.

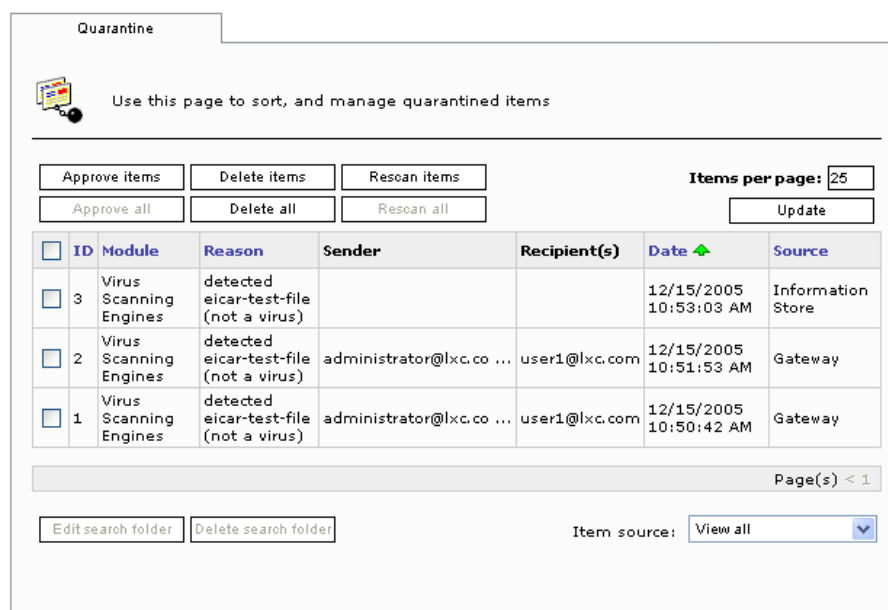
Freigeben von E-Mails im Quarantänebereich

E-Mails lassen sich direkt über jeden Unterknoten des Quarantänebereichs, inklusive der Suchordner, freigeben. Des Weiteren können Sie das Tool zur Schnellsuche verwenden, um nach bestimmten E-Mails zu suchen, die eine Freigabe erfordern.

So geben Sie E-Mails frei:

1. Erweitern Sie unter **Console Root** die Struktur des Knotens **Quarantine**, und wählen Sie den Unterknoten aus, in dem sich die freizugebenden E-Mails befinden. Wählen Sie beispielsweise den Knoten **Today**, wenn E-Mails, die am heutigen Tag unter Quarantäne gestellt wurden, freigegeben werden sollen. Des Weiteren können Sie das Tool zur Schnellsuche verwenden, um nach bestimmten E-Mails zu suchen, die eine Freigabe erfordern.

Hinweis: Eine E-Mail, die am heutigen Tag unter Quarantäne gestellt worden ist, kann über die Knoten **Today**, **This Week**, **All Emails** und über jeden Suchordner, in den die Nachricht einsortiert wurde, freigegeben werden. Der Unterschied zwischen diesen Knoten besteht in der Anzahl der E-Mails, die in den zugehörigen Ordnern enthalten sind.



Quarantine

Use this page to sort, and manage quarantined items

Approve items Delete items Rescan items Items per page: 25

Approve all Delete all Rescan all Update

<input type="checkbox"/>	ID	Module	Reason	Sender	Recipient(s)	Date ▲	Source
<input type="checkbox"/>	3	Virus Scanning Engines	detected eicar-test-file (not a virus)			12/15/2005 10:53:03 AM	Information Store
<input type="checkbox"/>	2	Virus Scanning Engines	detected eicar-test-file (not a virus)	administrator@lxc.co ...	user1@lxc.com	12/15/2005 10:51:53 AM	Gateway
<input type="checkbox"/>	1	Virus Scanning Engines	detected eicar-test-file (not a virus)	administrator@lxc.co ...	user1@lxc.com	12/15/2005 10:50:42 AM	Gateway

Page(s) < 1

Edit search folder Delete search folder Item source: View all ▼

Screenshot 84 – Quarantäne-Mails in einem einzelnen Suchordner

2. Markieren Sie das Kontrollkästchen der E-Mail(s), die Sie freigeben möchten, und klicken Sie auf die Schaltfläche **Approve items**.

Hinweis 1: Wenn alle aufgeführten E-Mails freigegeben werden sollen, klicken Sie auf die Schaltfläche **Approve all**.

Hinweis 2: Um die Liste der angezeigten Nachrichten zu aktualisieren, klicken Sie auf die Schaltfläche **Update**.

Löschen von E-Mails im Quarantänebereich

So löschen Sie E-Mails im Quarantänebereich:

1. Erweitern Sie unter **Console Root** die Struktur des Knotens **Quarantine**, und wählen Sie den Unterknoten aus, in dem sich die zu löschenden E-Mails befinden. Wählen Sie beispielsweise den Knoten **Today**, wenn E-Mails, die am heutigen Tag unter Quarantäne gestellt wurden, gelöscht werden sollen. Des Weiteren können Sie das Tool zur Schnellsuche verwenden, um nach E-Mails zu suchen, die gelöscht werden sollen.

2. Markieren Sie das Kontrollkästchen der E-Mail(s), die Sie löschen möchten, und klicken Sie auf die Schaltfläche **Delete items**.

Hinweis 1: Wenn alle aufgeführten E-Mails gelöscht werden sollen, klicken Sie auf die Schaltfläche **Delete all**.

Hinweis 2: Um die Liste der angezeigten Nachrichten zu aktualisieren, klicken Sie auf die Schaltfläche **Update**.

Erneute Sicherheitsüberprüfung von E-Mails im Quarantänebereich

Der Quarantänebereich erlaubt es Ihnen, eine erneute Sicherheitsüberprüfung von blockierten E-Mails durchzuführen. Diese Option eignet sich vor allem zur schnellen Kontrolle von E-Mails bei neuen Virenausbrüchen.

Beispiel: Eine E-Mail wurde unter Quarantäne gestellt, da sie eine Regel zur Inhaltskontrolle verletzt hat. Die Nachricht enthält zudem einen bisher unbekanntem Virus. Da die Virensignaturen jedoch nicht auf dem neuesten Stand waren, als die E-Mail von GFI MailSecurity kontrolliert wurde, löste keine der Viren-Scan-Regeln Alarm aus.

Kurze Zeit nachdem die Nachricht unter Quarantäne gestellt worden war, erfolgte die Aktualisierung der Virensignaturen. Am darauf folgenden Tag wird die Mitteilung bei der Kontrolle des Quarantänebereichs durch den Administrator geprüft. Ohne die Funktion zur erneuten Sicherheitsüberprüfung hätte der Administrator nur die Möglichkeit, die Mitteilung entweder zu löschen oder sie freizugeben, wodurch jedoch unwissentlich ein Virus im Netzwerk in Umlauf gebracht werden würde.

Dank der Funktion zur erneuten Sicherheitsüberprüfung kann der Administrator veranlassen, dass die E-Mail ein zweites Mal alle Kontrollfilter durchläuft. Aufgrund der aktualisierten Virensignaturen identifizieren jetzt sowohl der Viren-Scanner als auch die Regel zur Inhaltskontrolle die Mitteilung als sicherheitsgefährdend.

Die E-Mail wird somit auch im Viren-Scanner-Ordner des Quarantänebereichs aufzufinden sein, da der Virus nun erkannt wurde.

So führen Sie einen erneuten Scan von E-Mails im Quarantänebereich durch:

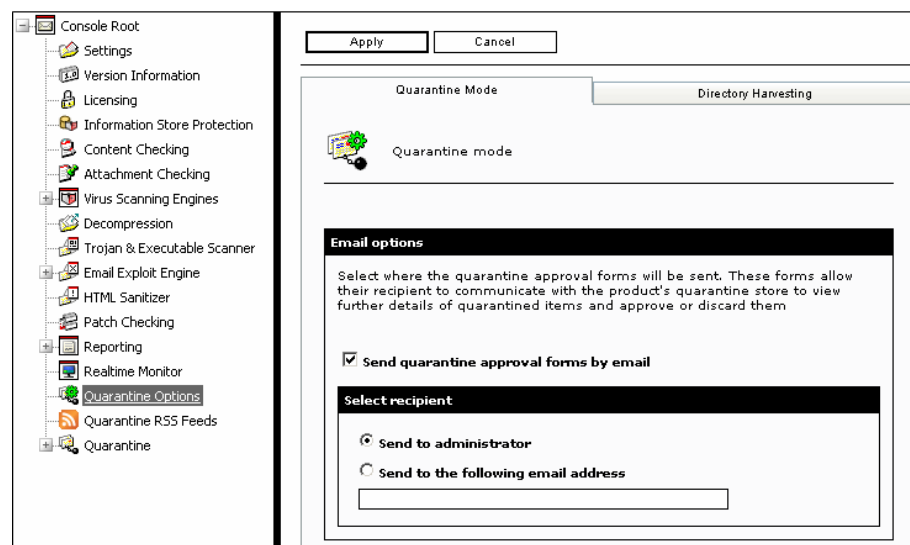
1. Erweitern Sie unter **Console Root** die Struktur des Knotens **Quarantine**, und wählen Sie den Unterknoten aus, in dem sich die neu zu scannenden E-Mails befinden. Wählen Sie beispielsweise den Knoten **Today**, wenn E-Mails, die am heutigen Tag unter Quarantäne gestellt wurden, erneut überprüft werden sollen. Des Weiteren können Sie das Tool zur Schnellsuche verwenden, um nach bestimmten E-Mails zu suchen, die erneut kontrolliert werden sollen.

2. Markieren Sie das Kontrollkästchen der E-Mail(s), die Sie nochmals kontrollieren möchten, und klicken Sie auf die Schaltfläche **Rescan items**.

Hinweis 1: Wenn alle aufgeführten E-Mails erneut gescannt werden sollen, klicken Sie auf die Schaltfläche **Rescan all**.

Hinweis 2: Um die Liste der angezeigten Nachrichten zu aktualisieren, klicken Sie auf die Schaltfläche **Update**.

Freigeben von E-Mails per HTML-Freigabebformular



Screenshot 85 – Konfiguration der Quarantäne-Optionen

Sie können in GFI MailSecurity auch festlegen, dass zur Freigabe von E-Mails ein entsprechendes HTML-Freigabebformular per E-Mail an den Administrator oder eine autorisierte Person geschickt wird. Mit Hilfe dieses Formulars können E-Mails direkt über den E-Mail-Client des Administrators gelöscht oder freigegeben werden, ohne direkt auf den Quarantänebereich zugreifen zu müssen.

So aktivieren Sie den Versand von HTML-Freigabebformularen:

1. Klicken Sie unter **Console Root** auf den Knoten **Quarantine Options**.

2. Wählen Sie auf der rechten Seite zu den Konfigurationseinstellungen die Option **Send quarantine approval forms by email**, um den E-Mail-Versand des HTML-Freigabebformulars zu aktivieren.

3. Geben Sie die Empfängeradresse für das Formular an, d. h. bestimmen Sie, wer Quarantäne-E-Mails überprüfen darf. Wählen Sie hierfür eine der folgenden Optionen aus:

- **Send to administrator** – Schickt HTML-Freigabebformulare an den Administrator. Hierbei wird die E-Mail-Adresse verwendet, die Sie während der Installation oder über den Knoten **Settings**, Reiter **General**, angegeben haben. Nähere Informationen zur Konfiguration der E-Mail-Adresse des Administrators erhalten Sie im Kapitel „Allgemeine Einstellungen“ unter „Angabe der E-Mail-Adresse des Administrators“.

- **Send to the following email address** – Das HTML-Freigabeformular wird an die angegebene E-Mail-Adresse/Benutzergruppe oder einen Öffentlichen Ordner geschickt. Geben Sie die E-Mail-Adresse des Empfängers im entsprechenden Eingabefeld unter dieser Option ein.

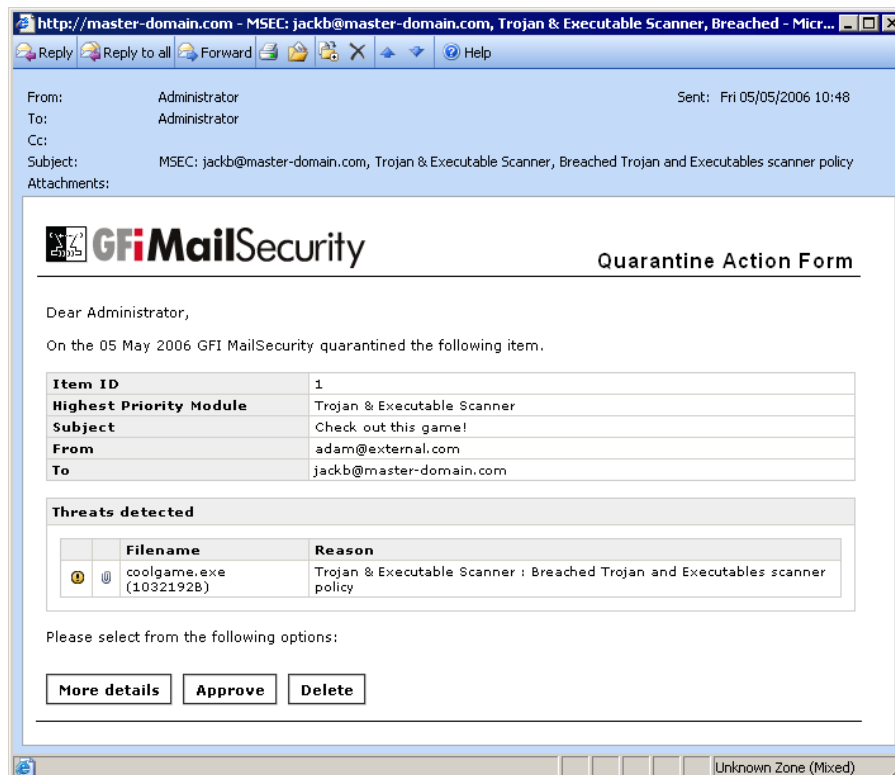
Hinweis: Das HTML-Freigabeformular ermöglicht es dem Empfänger, weitere Details zu den unter Quarantäne gestellten Objekten zu erhalten. Diese Details stammen aus dem Quarantänebereich und können per Mausklick auf die Schaltfläche **More Details** im HTML-Freigabeformular angezeigt werden.

4. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Hinweis: Der Administrator kann Quarantäne-Mails auch direkt über den Knoten **Quarantine** freigeben oder löschen. Der Knoten **Quarantine** ist der zentrale Speicherort für von GFI MailSecurity blockierte E-Mails.

Freigeben oder Löschen von Quarantäne-Mails per E-Mail-Client

Ist eine E-Mail unter Quarantäne gestellt worden, wird der Administrator mit Hilfe des E-Mail verschickten HTML-Freigabeformulars benachrichtigt. Dieses Formular enthält nähere Angaben zur blockierten Mitteilung, u. a. zum Grund der Blockierung und zu ggf. zugehörigen Anhängen.



Screenshot 86 – HTML-Freigabeformular

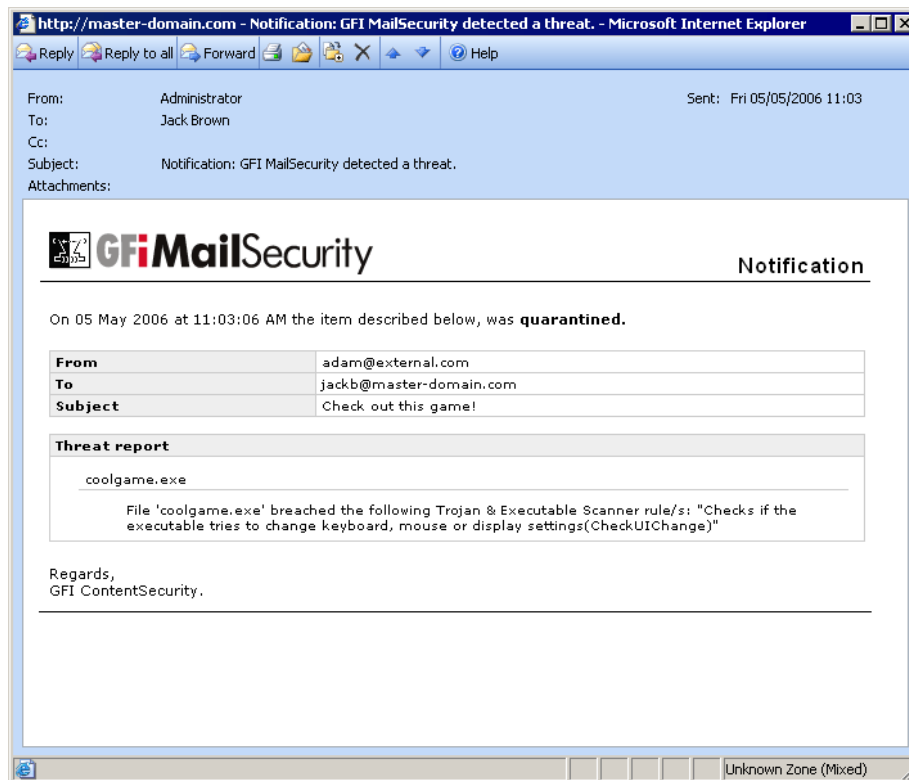
Über das HTML-Freigabeformular hat der Administrator die Möglichkeit, E-Mails, die unter Quarantäne gestellt wurden, per Mausklick auf die Schaltfläche **Approve** oder **Delete** freizugeben bzw. zu löschen. Nach erfolgter Freigabe wird die Nachricht dann sofort an den eigentlichen Empfänger weitergeleitet. Falls es sich bei der

Mitteilung um eine eingehende E-Mail gehandelt hat, erhält der Empfänger zudem eine E-Mail, in der er über die Statusänderung der blockierten Mitteilung informiert wird (d. h. über deren Freigabe oder Löschung). Diese E-Mails ist vor allem wichtig, damit Anwender darüber informiert werden, dass eine an sie adressierte, jedoch infizierte Mitteilung gelöscht wurde.

Versand von Informationen zu Quarantäne-E-Mails an Anwender

Werden E-Mails unter Quarantäne gestellt, verläuft dieser Vorgang für Anwender zum größten Teil unbemerkt. Ein- und ausgehende E-Mails werden sofort nach der Freigabe durch den Administrator weitergeleitet.

Falls Sie über die Benachrichtigungsoptionen festgelegt haben, dass ein lokaler Benutzer bei einer an ihn gerichteten oder von ihm verschickten E-Mail, die unter Quarantäne gestellt wurde, benachrichtigt werden soll, erhält der Benutzer folgenden Hinweis:



Screenshot 87 – Benutzerbenachrichtigung bei empfangener/verschickter Quarantäne-Mail

Aktivieren von RSS-Feeds zum Quarantänebereich

Was ist RSS?

Bei Really Simple Syndication (RSS) handelt es sich um ein Protokoll, das von häufig aktualisierten Websites wie Nachrichten-Sites, Weblogs o. Ä. eingesetzt wird und Anwender über alle neuen oder aktualisierten Site-Inhalte auf dem Laufenden hält.

Die Website veröffentlicht dabei eine XML-Datei, RSS-Feed genannt, die dem RSS-Standard entspricht. Anwender können über eine entsprechende Client-Anwendung, dem Feed-Reader oder Aggregator,

unterschiedliche RSS-Feeds dynamisch abonnieren. Der Feed-Reader lädt die XML-Datei automatisch unter der für das Abonnement angegebenen URL herunter, verarbeitet den Inhalt und zeigt eine Übersicht der aktualisierten Artikel an. Dabei wird üblicherweise eine kurze Zusammenfassung des neuen Artikels und ein Link zum vollständigen Bericht bereitgestellt.

Wie wird RSS von GFI MailSecurity genutzt?

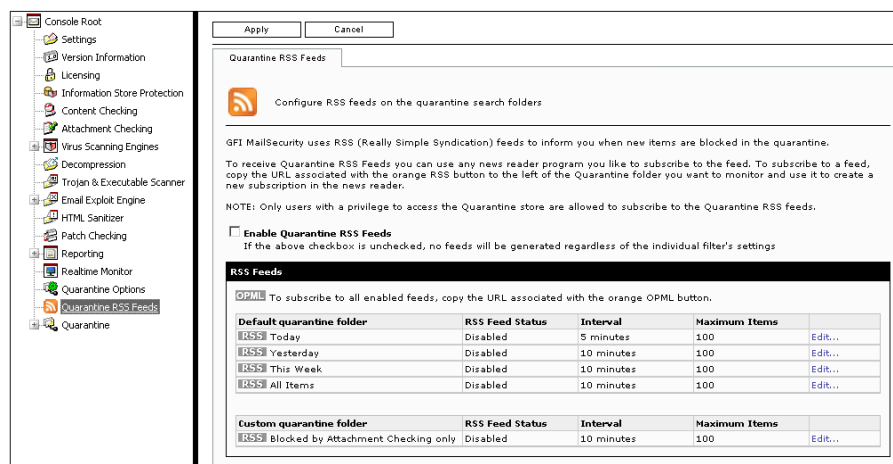
Der Quarantänebereich ähnelt einer Website, die regelmäßig mit neuen blockierten Inhalten aktualisiert wird. Dieser Aufbau lässt sich für RSS-Feeds nutzen, die für Quarantäneordner eingerichtet werden können und Administratoren helfen, sich schnell über Elemente im Quarantänebereich informieren zu lassen.

Wird die Ausgabe von RSS-Feeds für einen Quarantäneordner eingerichtet, kann zu deren Abonnement jeder beliebige Feed-Reader mit Authentifizierungsunterstützung installiert werden, z. B. RSSOwl (www.rssowl.org) oder RSS Bandit (www.rssbandit.org). Administratoren können sich dadurch regelmäßig über blockierte Elemente, die neu in den Quarantänebereich verschoben wurden, informieren lassen.

Einrichten von RSS-Feeds für Quarantäneordner

So richten Sie RSS-Feeds für Quarantäneordner ein:

1. Klicken Sie unter **Console Root** auf den Knoten **Quarantine RSS-Feeds**.



Screenshot 88 – RSS-Feeds für Quarantäneordner

2. Markieren Sie das Kontrollkästchen **Enable Quarantine RSS Feeds**.

3. In der Liste **RSS Feeds** werden alle aktuell konfigurierten standardmäßigen („Default quarantine folder“) und benutzerdefinierten („Custom quarantine folder“) Quarantäneordner angezeigt. Um RSS-Feeds für einen Quarantäneordner zu konfigurieren, klicken Sie auf den Link **Edit...** rechts neben dem jeweiligen Ordner.

RSS Feeds

OPML To subscribe to all enabled feeds, copy the URL associated with the orange OPML button.

Default quarantine folder	RSS Feed Status	Interval	Maximum Items	
Today	Disabled	5 minutes	100	
<input checked="" type="checkbox"/> Enable Quarantine RSS feeds on this folder Interval (minutes) <input type="text" value="5"/> Maximum Items <input type="text" value="100"/> <input checked="" type="checkbox"/> Include Unique ID in RSS feed URL RSS feed URL Unique ID <input type="text" value="088343c3-3922-062c-5822-61baca75383c"/> <input type="button" value="Generate ID"/>				
Yesterday	Disabled	10 minutes	100	Edit...
This Week	Disabled	10 minutes	100	Edit...
All Items	Disabled	10 minutes	100	Edit...
Custom quarantine folder	RSS Feed Status	Interval	Maximum Items	
Blocked by Attachment Checking only	Disabled	10 minutes	100	Edit...

Screenshot 89 – RSS-Feed-Einstellungen eines Quarantäneordners

4. Markieren Sie das Kontrollkästchen **Enable Quarantine RSS Feeds on this folder**, um die Feeds für diesen Ordner zu aktivieren.

5. Geben Sie im Eingabefeld **Interval** das Aktualisierungsintervall in Minuten ein. Der Standardwert beträgt 10 Minuten.

6. Geben Sie im Eingabefeld **Maximum Items** die maximale Anzahl der Elemente ein, die vom RSS-Feed aufgeführt werden sollen.

Hinweis: RSS-Feeds zum Quarantänebereich können nur von autorisierten Benutzern abonniert werden, die über das SwitchBoard von GFI MailSecurity festzulegen sind. Weitere Informationen hierzu erhalten Sie im Kapitel „Installieren von GFI MailSecurity“ unter „Sichern des Zugriffs auf RSS-Feeds des Quarantänebereichs“.

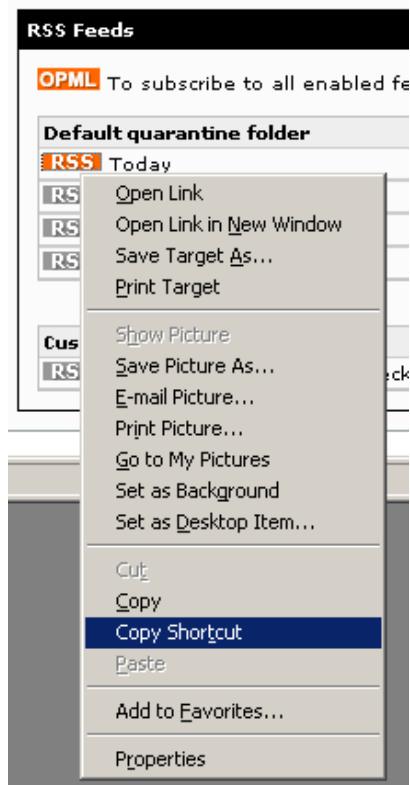
7. Soll dem RSS-Feed eines Quarantäneordners eine eigene eindeutige URL zugewiesen werden, markieren Sie das Kontrollkästchen **Include Unique ID in RSS feed URL**. Hierauf wird die eindeutige ID automatisch erstellt. Möchten Sie eine andere ID erstellen, klicken Sie auf die Schaltfläche **Generate ID**.

8. Klicken Sie auf die Schaltfläche **Apply**, um die Einstellungen zu speichern.

Abonnieren von RSS-Feeds eines Quarantäneordners

So abonnieren Sie die RSS-Feeds eines Quarantäneordners:

1. Klicken Sie mit der rechten Maustaste auf das RSS-Symbol links neben dem Quarantäneordner, dessen RSS-Feeds abonniert werden sollen.



Screenshot 90 – Kopieren der URL des RSS-Feed

2. Wählen Sie aus dem Kontextmenü **Verknüpfung kopieren** aus.
3. Richten Sie in Ihrem Feed-Reader ein neues RSS-Feed-Abonnement ein. Geben Sie dabei die im vorherigen Schritt kopierte Verknüpfung als URL des RSS-Feed an.

Aktivieren des Directory Harvesting-Filters für Quarantäne-Mails

In dem meisten Fällen wird GFI MailSecurity als erste Abwehrmaßnahme gegen E-Mail-basierte Gefahren eingesetzt. Da Serverbasierte Spam-Filter wie GFI MailEssentials normalerweise erst hinter GFI MailSecurity zum Einsatz kommen, befinden sich unter den von der Sicherheitslösung zu kontrollierenden Nachrichten somit auch sehr viele Spam-E-Mails.

Einige dieser Spam-Nachrichten können auch Viren, Trojaner u. v. m. enthalten. Diese Schadteile werden von GFI MailSecurity blockiert und zur Kontrolle in den Quarantänebereich verschoben.

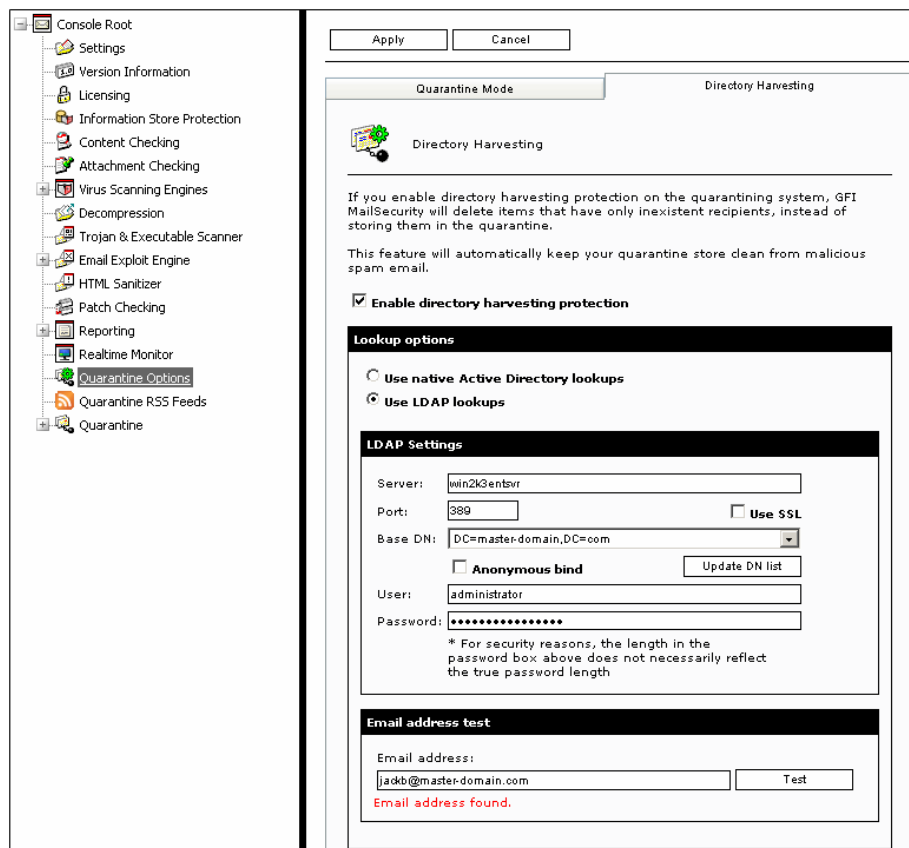
Von GFI MailSecurity abgefangener virenbelasteter Spam kann somit zur unnötigen Füllung des Quarantänebereichs und zu einer Mehrbelastung bei der Kontrolle blockierter Nachrichten führen.

Um mit Viren infizierten Spam vom Quarantänebereich fernzuhalten, kann der Directory-Harvesting-Filter (DHA-Filter) von GFI MailSecurity aktiviert werden. Dieser Filter scannt von GFI MailSecurity blockierte E-Mails, bevor sie in den Quarantänebereich verschoben werden. Ist eine blockierte E-Mail an nicht lokale oder nicht in Active Directory bzw. an auf dem E-Mail-Server eines Unternehmens nicht existierende Empfänger gerichtet, wird die Nachricht gelöscht, anstatt in den Quarantänebereich verschoben zu werden.

Der Directory-Harvesting-Filter ermittelt, ob ein Empfänger real oder lokal ist, indem seine Existenz in Active Directory oder auf dem LDAP-Server überprüft wird.

So aktivieren Sie den Directory-Harvesting-Filter für den Quarantänebereich:

1. Klicken Sie unter **Console Root** auf den Knoten **Quarantine Options**.
2. Gehen Sie auf der rechten Seite in den Konfigurationseinstellungen der Quarantäneoptionen auf den Reiter **Directory Harvesting**.



Screenshot 91 – Directory-Harvesting-Filter

3. Markieren Sie das Kontrollkästchen **Enable directory harvesting protection**.
4. Wurde GFI MailSecurity im AD-Modus installiert, markieren Sie das Kontrollkästchen **Use native Active Directory lookups**, und fahren Sie dann mit Schritt 7 fort. Alternativ können Sie auch die LDAP-Suche verwenden, die im folgenden Schritt erklärt wird.
5. Wurde GFI MailSecurity im SMTP-Modus installiert, markieren Sie das Kontrollkästchen **Use LDAP lookups**.
6. Geben Sie im Eingabefeld **Server** den Namen oder die IP-Adresse des LDAP-Servers und im Eingabefeld **Port** die zugehörige Port-Nummer an (Standard: 389). Erfordert Ihr LDAP-Server eine Authentifizierung, muss das Kontrollkästchen **Anonymous bind** deaktiviert sein. Geben Sie dann zudem die Authentifizierungsdaten in den Eingabefeldern **User** und **Password** ein.

7. Klicken Sie auf die Schaltfläche **Update DN list**, um die Drop-Down-Liste **Base DN** zu füllen. Wählen Sie danach den entsprechenden Eintrag aus der Liste aus.

8. Testen Sie die LDAP-Konfigurationseinstellungen, indem Sie im Eingabefeld **Email address** eine gültige E-Mail-Adresse eingeben und danach auf die Schaltfläche **Test** klicken. Ist die Suche erfolgreich, wird unter dem Eingabefeld **Email address** die Mitteilung „Email address found“ angezeigt.

Hinweis 1: Ist GFI MailSecurity im Active Directory-Modus in einer DMZ installiert, sind in dessen Active Directory üblicherweise nicht alle Netzwerk-Benutzer (d. h. E-Mail-Empfänger) verzeichnet. Dies hat zur Folge, dass viele Fehlalarme ausgegeben werden. In einem solchen Fall sollten Sie die Directory-Harvesting-Kontrollen per LDAP-Suche durchführen lassen und die Option **Use LDAP lookups** unter Angabe der LDAP-Server-Daten auswählen.

Hinweis 2: Wird GFI MailSecurity hinter einer Firewall betrieben, kann die Directory-Harvesting-Funktion keine direkte Verbindung mit dem internen AD herstellen. Damit der Filter durch die Firewall hindurch auf das interne AD Ihres Netzwerks zugreifen kann, müssen Sie in diesem Fall trotz Verfügbarkeit beider Such-Optionen die LDAP-Suche verwenden. Stellen Sie sicher, dass bei Ihrer Firewall Port 389 freigeschaltet ist.

Hinweis 3: Wenn Sie eine Verbindung zum Active Directory per LDAP aufbauen, d. h., wenn GFI MailSecurity in einer DMZ oder hinter einer Firewall installiert ist, müssen Sie die Anmeldedaten in folgender Form angeben: Domäne\Anwender (z. B. „master-domain\administrator“).

Hinweis 4: In einer Active Directory-Umgebung ist der LDAP-Server üblicherweise der Domänen-Controller.

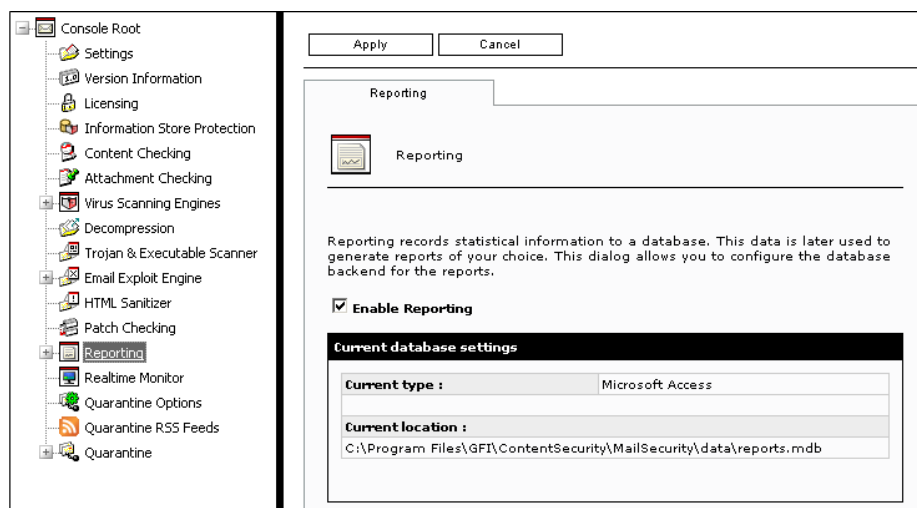
9. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Die Berichterstellung

Einführung

Mit Hilfe der Berichtsfunktion werden von GFI MailSecurity protokollierte statistische Informationen in einer Datenbank gespeichert. Hierzu zählen Angaben zu sämtlichen von GFI MailSecurity kontrollierten E-Mails und solchen Mitteilungen, die aus einem bestimmten Grund unter Quarantäne gestellt wurden. Die in der Datenbank gesammelten Daten können zur Erstellung verschiedener Berichte verwendet werden. GFI MailSecurity unterstützt Microsoft Access und Microsoft SQL Server als Datenbank-Backends.

Konfigurieren der statistischen Datenbank

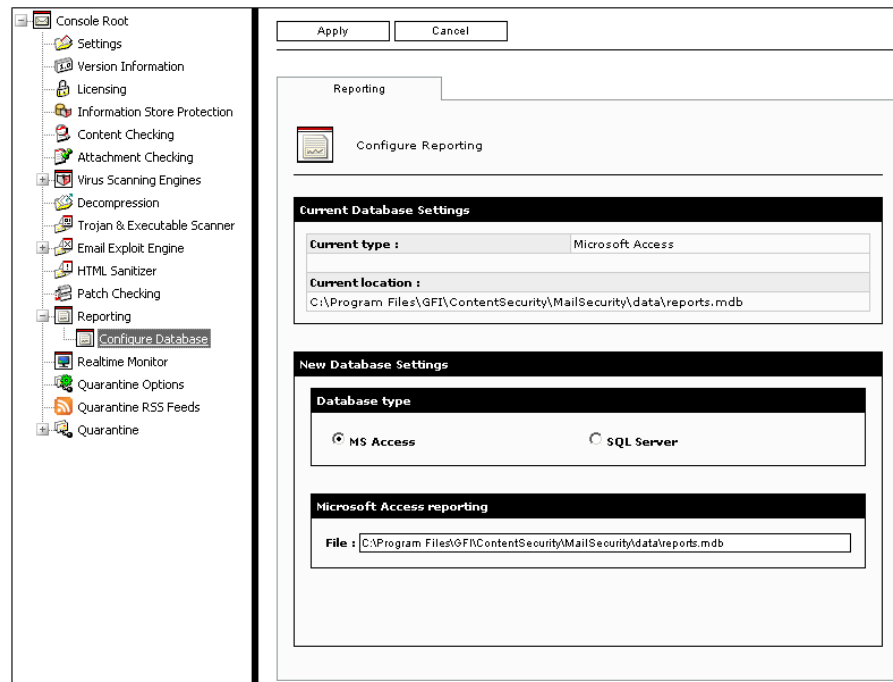


Screenshot 92 – Berichtseite

So konfigurieren Sie die Berichterstellung:

1. Klicken Sie unter **Console Root** auf den Knoten **Reporting**.
2. Markieren Sie das Kontrollkästchen **Enable Reporting**, um die Protokollierung der Scan-Daten zur Berichterstellung zu aktivieren. Bei Deaktivierung dieser Option werden keine Berichtsdaten protokolliert.
3. Die Berichtseite im rechten Fenster informiert über aktuelle Einstellungen zum Datenbank-Backend. Hierzu zählen der Datenbanktyp sowie der Speicherort der verwendeten Datenbankdatei. Um die aktuellen Datenbankeinstellungen zu ändern, erweitern Sie die Struktur des Knotens **Reporting**, und klicken Sie auf den Unterknoten **Configure Reporting**. Die Datenbankeinstellungen lassen sich im rechten Fenster konfigurieren.

Konfigurieren von Microsoft Access als Datenbank-Backend



Screenshot 93 – Konfigurieren von Microsoft Access als Datenbank-Backend

1. Wählen Sie die Option **MS Access**, und geben Sie den vollständigen Pfad und Dateinamen der Datenbankdatei ein, in der die statistischen Informationen gespeichert werden sollen. Wenn Sie nur den Dateinamen angeben, wird die Datenbankdatei unter dem Standardpfad erstellt, d. h.

C:\Program Files\GFI\ContentSecurity\MailSecurity\data\
<filename.mdb>

2. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Konfigurieren von Microsoft SQL Server als Datenbank-Backend

The screenshot shows a 'Reporting' window with a 'Configure Reporting' icon. It is divided into two main sections: 'Current Database Settings' and 'New Database Settings'.

Current Database Settings:

- Current type :** Microsoft Access
- Current location :** C:\Program Files\GFI\ContentSecurity\MailSecurity\data\reports.mdb

New Database Settings:

Database type

- MS Access
- SQL Server

SQL server reporting

- Detected server :** (local) [dropdown]
- Manually specified server :** [input field]
- User :** sa [input field]
- Password :** [password field with dots]
-
- Database :** MailSecurity Reporting Database [dropdown]

Screenshot 94 – Konfigurierung der Microsoft SQL Server-Datenbank

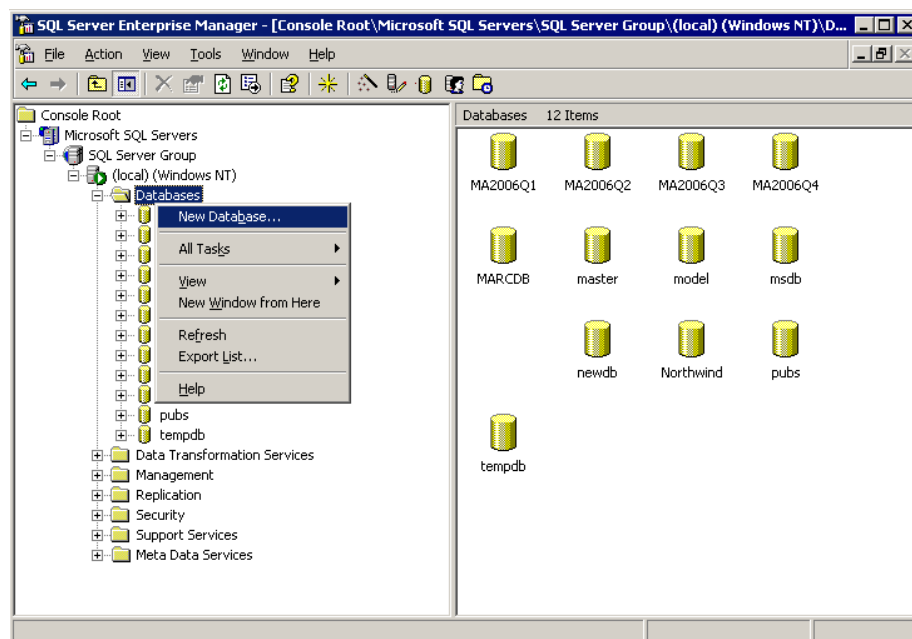
1. Wählen Sie die Option **SQL Server**.
2. Wählen Sie die Option **Detected server** und dann aus der zugehörigen Drop-Down-Liste den gewünschten SQL-Server aus. Alternativ können Sie die Option **Manually specified server** auswählen und im zugehörigen Eingabefeld die IP-Adresse oder den Server-Namen des SQL-Servers angeben.
3. Geben Sie im Eingabefeld **User** den Namen eines Anwenders an, der auf den SQL-Server zugreifen darf.
4. Geben Sie im Eingabefeld **Password** das Passwort für das Konto des zugriffsberechtigten Anwenders ein.
5. Klicken Sie auf die Schaltfläche **Get Database List**, um die Datenbankinformationen von diesem Server zu extrahieren und damit die Drop-Down-Liste **Database** zu füllen.
6. Wählen Sie aus der Drop-Down-Liste **Database** die Datenbank aus, in der die statistischen Informationen gespeichert werden sollen.
7. Klicken Sie auf die Schaltfläche **Apply**, um Ihre Einstellungen zu speichern.

Hinweis 1: Die Datenbank muss bereits vor der Konfigurierung dieser Option erstellt worden sein. Weitere Informationen zum Erstellen einer SQL Server-Datenbank erhalten Sie weiter unten unter „Erstellen einer SQL Server-Datenbank“.

Hinweis 2: Benutzer und Passwort müssen mit den Angaben übereinstimmen, die zuvor als Anmeldeinformationen für Ihre SQL Server-Datenbank gewählt wurden. Weitere Informationen erhalten Sie weiter unten in Schritt 6 des Unterkapitels „Erstellen einer SQL Server-Datenbank“.

Erstellen einer SQL Server-Datenbank

1. Öffnen Sie den SQL Server Enterprise Manager über **Start ▶ Programme ▶ Microsoft SQL Server ▶ Enterprise Manager**, und gehen Sie zum SQL-Server, auf dem die Datenbank erstellt werden soll.

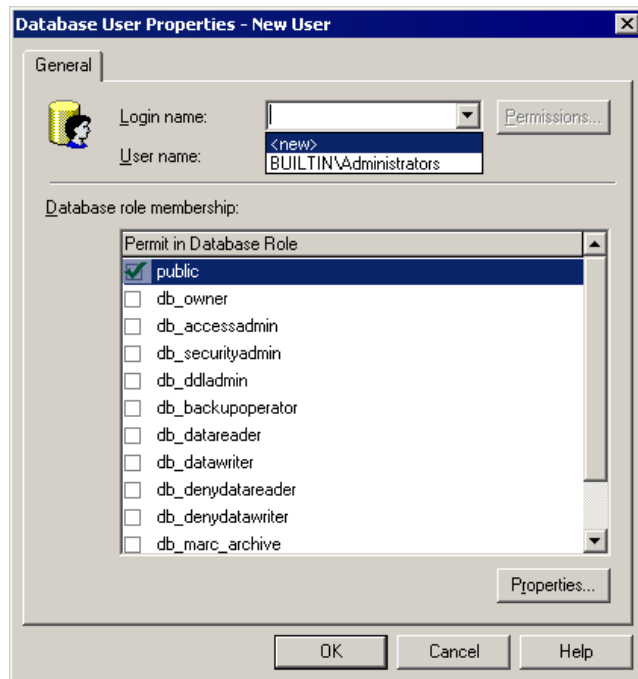


Screenshot 95 – Erstellen einer neuen Datenbank

2. Klicken Sie mit der rechten Maustaste auf den Knoten **Datenbanken**, und wählen Sie die Option **Neue Datenbank....**

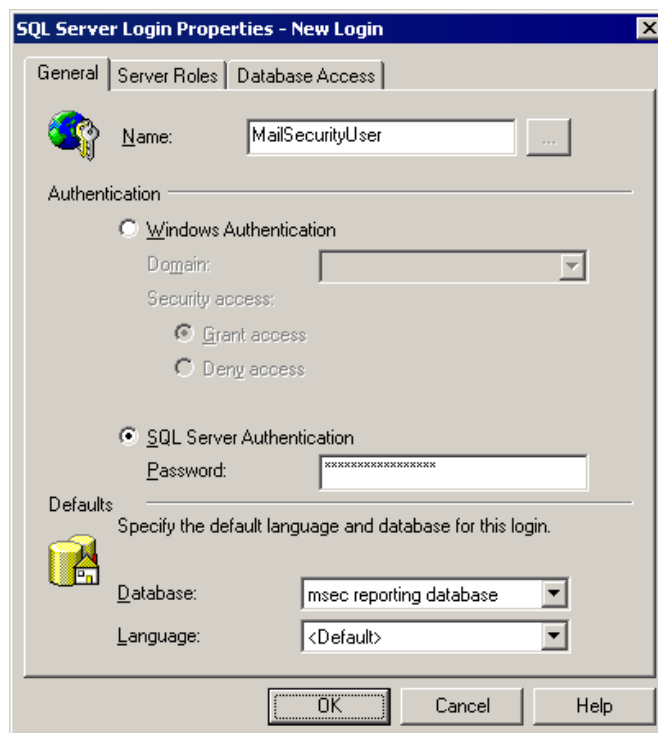
3. Geben Sie in dem angezeigten Dialogfeld den Datenbanknamen an (z. B. „MailSecurityBerichte“), und klicken Sie dann auf die Schaltfläche **OK**.

4. Erweitern Sie die Struktur des neuen Datenbankknotens, klicken Sie mit der rechten Maustaste auf den Unterknoten **Benutzer**, und wählen Sie die Option **Neuer Datenbankbenutzer....**



Screenshot 96 – Festlegung des Benutzernamens

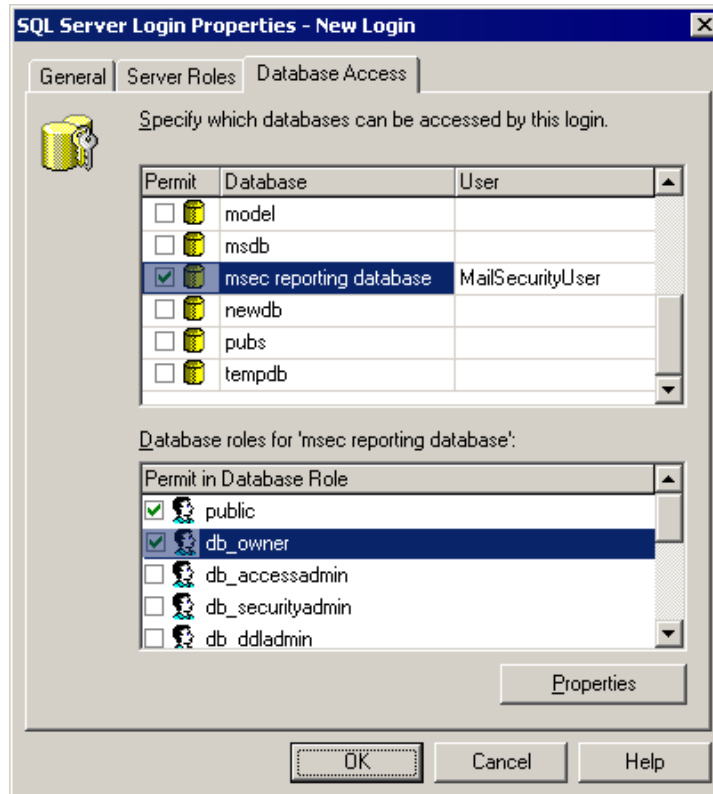
5. Wählen Sie über die Drop-Down-Liste **Benutzername** den Eintrag **<neu>** aus.



Screenshot 97 – Festlegung des Authentifizierungsmodus

6. Ein neues Dialogfenster wird geöffnet. Geben Sie im Eingabefeld **Name** den Benutzernamen ein (z. B. „MailSecurityBenutzer“). Wählen Sie im Bereich **Authentifizierung** die Option **SQL Server-Authentifizierung** aus, und geben Sie dann im zugehörigen Eingabefeld ein Passwort ein.

7. Wählen Sie die gerade erstellte Datenbank aus der Drop-Down-Liste **Datenbank** aus.
8. Gehen Sie auf den Reiter **Datenbankzugriff**.
9. Markieren Sie das Kontrollkästchen neben der gerade erstellten Datenbank.



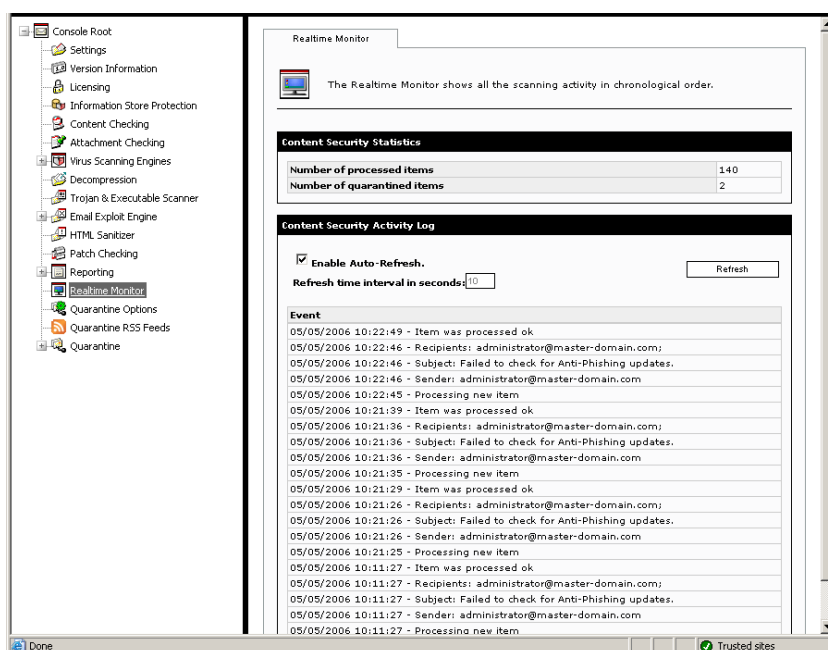
Screenshot 98 – Aktivierung der Datenbankrolle „db_owner“

10. Wählen Sie im Bereich **Datenbankrollen für...**: die Rolle **db_owner** aus. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu speichern und den Dialog zu schließen.

Der Echtzeit-Monitor

Einführung

Mit Hilfe des Echtzeit-Monitors können Sie „live“ kontrollieren, wie GFI MailSecurity E-Mails scannt. Die Funktion unterstützt Sie beim Überprüfen des Kontrollstatus jeder einzelnen E-Mail, und Sie können feststellen, ob eine Mitteilung erfolgreich verarbeitet werden konnte.



Screenshot 99 – Echtzeit-Monitor

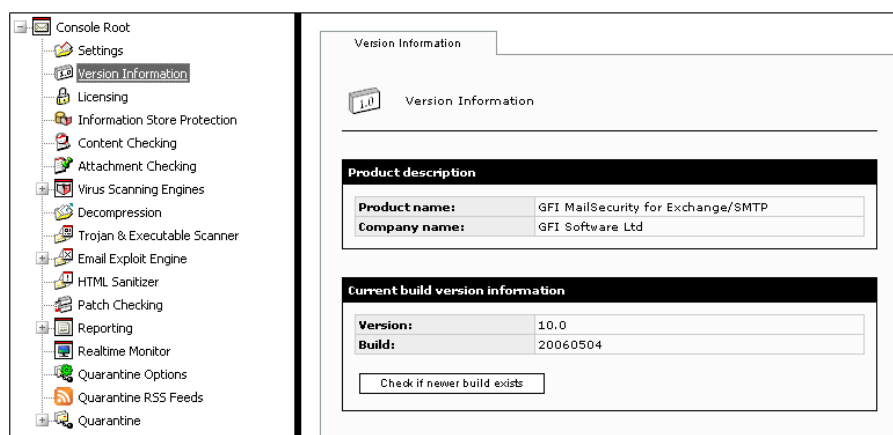
Überwachen der E-Mail-Verarbeitung

1. Klicken Sie unter **Console Root** auf den Knoten **Realtime Monitor**, um den Echtzeit-Monitor zu öffnen. Über den Monitor werden die Anzahl der von GFI MailSecurity verarbeiteten E-Mails sowie die Anzahl der aktuell unter Quarantäne stehenden Mitteilungen angezeigt. Zusätzlich werden Datum und Uhrzeit des Empfangs und der Verarbeitung einer E-Mail angegeben sowie Absender, Empfänger und Betreff jeder kontrollierten Nachricht.

2. Um die angezeigten Informationen automatisch aktualisieren zu lassen, markieren Sie das Kontrollkästchen **Enable Auto-Refresh**. Geben Sie im zugehörigen Eingabefeld das Aktualisierungsintervall in Sekunden an. Das Standardintervall beträgt 10 Millisekunden. Die Überwachungsinformationen lassen sich zudem manuell über die Schaltfläche **Refresh** aktualisieren.

Ergänzende Optionen

Versionsinformationen



Screenshot 100 – Versionsinformationen

Die Versionsinformationen zur von Ihnen eingesetzten Version von GFI MailSecurity erhalten Sie über **Console Root ▶ Version Information**. Auf der rechten Seite des Fensters wird die Versionsnummer des aktuell installierten Produkts sowie die Build-Nummer angezeigt. Per Mausklick auf die Schaltfläche **Check if newer build exists** können Sie feststellen, ob Sie den neuesten Produkt-Build verwenden.

Hinweis: Geben Sie bei Anfragen an den GFI-Support bitte immer die Versions- und Build-Nummer Ihres GFI-Produkts an.

Zusätzliche urheberrechtliche Informationen

Einige Komponenten von GFI MailSecurity wurden unter Verwendung von Drittanbieter-Software entwickelt. Nachfolgend erhalten Sie Informationen zur Software-Lizenz dieser Produkte.

Libxml2: The MIT License

Copyright (C) 1998-2003 Daniel Veillard. Alle Rechte vorbehalten.

Hiermit wird allen Personen, die eine Kopie dieser Software und seiner zugehörigen Dokumentationsdateien (die „Software“) erhalten, sowie Personen, denen die Software bereitgestellt wird, unter nachfolgenden Bedingungen die kostenfreie Genehmigung erteilt, uneingeschränkt mit der Software zu handeln, darin eingeschlossen das freie Recht auf Verwendung, Vervielfältigung, Veränderung, Zusammenführung, Veröffentlichung, Verteilung, Unterlizenzierung und/oder Verkauf von Kopien der Software:

Der oben aufgeführte urheberrechtliche Hinweis und diese Genehmigung sind in allen Kopien oder erheblichen Teilen der Software ausdrücklich zu erwähnen.

DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR „WIE BESEHEN“ ZUR VERFÜGUNG GESTELLT, OHNE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNG, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF GEWÄHRLEISTUNG VON MARKTGÄNGIGKEIT, BRAUCHBARKEIT FÜR BESTIMMTE ZWECKE UND NICHTVERLETZBARKEIT. DANIEL VEILLARD IST NICHT HAFTBAR FÜR SICH MITTELBAR ODER UNMITTELBAR AUS DER SOFTWARE ODER DEREN MITTELBAREN ODER UNMITTELBAREN VERWENDUNG ERGEBENDE ANSPRÜCHE, SCHADENERSATZFORDERUNGEN ODER ANDEREN VERBINDLICHKEITEN, OB AUFGRUND EINER KLAGE AUF VERTRAGSERFÜLLUNG, AUS UNERLAUBTER HANDLUNG ODER ÄHNLICHEM.

Außer im Rahmen dieses Hinweises ist es nicht gestattet, den Namen Daniel Veillard ohne dessen vorherige schriftliche Zustimmung im Zusammenhang mit Werbemaßnahmen oder sonstigen Aktionen zur Förderung des Verkaufs oder der Verwendung dieser Software oder anderen damit verbundenen geschäftlichen Maßnahmen zu verwenden.

Weitere Konfigurationsoptionen

Anpassen der Benachrichtigungsvorlagen

GFI MailSecurity verschickt bei Eintritt eines administrativen oder sicherheitsrelevanten Ereignisses eine Benachrichtigung per E-Mail an den Administrator/autorisierten Benutzer.

Es gibt zwei Arten von Benachrichtigungen:

- **Administrative Benachrichtigungen** – Diese werden z. B. verschickt, wenn eine Lizenz abläuft, ein neuer Patch verfügbar ist oder neue Updates für eine Anti-Viren-Engine bereit stehen.
- **Endanwender-Benachrichtigungen** – Diese werden an den Absender/Empfänger einer E-Mail verschickt, wenn eine E-Mail unter Quarantäne gestellt oder geändert wurde.

Diese E-Mail-Benachrichtigungen werden über Vorlagen erstellt, die sich in Unterordnern des GFI MailSecurity-Verzeichnisses „ContentSecurity\MailSecurity\Templates“ befinden.

Jeder Vorlagen-Unterordner kann jeweils eine Vorlage für den HTML-Textkörper (html.txt), den Textkörper im Nur-Text-Format (text.txt) und den Betreff (subject.txt) enthalten.

Hinweis: Die Namen des Vorlagenordners und der Vorlagendateien sind fest vorgegeben und können nicht geändert werden.

Diese Vorlagen enthalten den Text der Benachrichtigungs-E-Mail sowie Platzhalter, die bei der Erstellung der Nachricht dynamisch mit aktuellen Daten ersetzt werden.

Es stehen zwei Arten von Vorlagen zur Verfügung:

- **Tag-basierte Vorlagen** – Diese Vorlagen setzen zur Kennzeichnung von Feldern, die dynamisch mit aktuellen Daten ausgefüllt werden müssen, Tags ein (dargestellt als "[TAGNAME]").
- **XSL-basierte Vorlagen** – Bei diesen Vorlagen handelt es sich um XSL-Style-Sheets, die die Benachrichtigung mit dynamisch erzeugten XML-Daten erstellen.

Hinweis: Fertigen Sie von allen Vorlagen, die Sie ändern möchten, zuvor eine Sicherheitskopie an. So können Sie stets zu vorherigen Vorlagen zurückkehren, falls eine Modifizierung nicht den gewünschten Effekt erzielt.

Hinweis: Änderungen an XSL-basierten Vorlagen sollten nur von Anwendern mit ausreichenden Kenntnissen in XML und XSL durchgeführt werden. Bei fehlerhaft modifizierten XSL-Vorlagen erfolgt kein ordnungsgemäßer Versand von Benachrichtigungen durch den Benachrichtigungsservice. Um festzustellen, ob eine XSL-basierte

Vorlage korrekt aufgebaut ist, benennen Sie ihre Dateierweiterung in „.xml“ um, und öffnen Sie sie im Microsoft Internet Explorer. Wird die Vorlage korrekt im Browser angezeigt, ist sie korrekt aufgebaut. Bei Fehlern informiert Sie der Browser, in welcher Zeile ein Problem besteht.

Variablen in XSL-basierten Benachrichtigungsvorlagen

Benachrichtigungen für Anwender und Administratoren (aus dem Ordner „notifyuser“ und „notifymanager“)

Knoten	Beschreibung
“itemsenderemailaddress”	E-Mail-Adresse des Absenders
“itemsubject”	Betreff der Quarantäne-E-Mail
“itemdeliverytime”	Datum und Uhrzeit der Zustellung
“itemrecipients/recipient”	Empfänger der Mitteilung; Auflistung per „xsl:for-each“
“action”	Verfahrensweise für herausgefilterte Mitteilung
“shortdate”	Verarbeitungsdatum einer E-Mail; Kurzformat
“longdate”	Verarbeitungsdatum einer E-Mail; Langformat
“time24”	Verarbeitungsuhrzeit einer E-Mail; 24h-Format
“time12”	Verarbeitungsuhrzeit einer E-Mail;
“infringedrules/rule”	Liste verletzter Regeln; Auflistung per „xsl:for-each“
“itemmessageid”	Mitteilungs-ID der verarbeiteten E-Mail
“itemscandirection”	0 – eingehend: 1 – ausgehend: 4 – gemischt

Nachfolgend ist eine HTML-Ausgabe abgebildet, die anhand der im Anschluss dargestellten XSL-Vorlage generiert wurde.

HTML-Ausgabe

```
<HTML>
<BODY>
Am 04. August 2005 wurde eine E-Mail blockiert, die folgende Regeln
verletzt hat: <P></P>
<B>BitDefender Anti-Virus</B><BR/>
<P>
Folgende Maßnahme(n) wurde(n) eingeleitet: <B>Mitteilung unter
Quarantäne gestellt</B>
</P>
Zusätzliche Informationen:
<P>
<table border="1">
<tr>
<td>Betreff</td><td><B>Beispielbetreff</B></td>
</tr>
<tr>
<td>Absender</td><td><B>Beispielabsender@Beispieldomaene.com</B></td>
</tr>
<tr>
<td colspan="2" align="center">Empfänger</td>
</tr>
<tr>
<td colspan="2"><B>Beispielpfänger@lokaledomaene.com</B></td>
</tr>
</table>
</P>
Mit freundlichen Grüßen<BR/>
GFI ContentSecurity.
</BODY>
</HTML>
```

XSL-Vorlage

```
<?xml version="1.0"?>
<xsl:stylesheet
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  version="1.0">
<xsl:output method="html" omit-xml-declaration="yes" standalone="no"/>

<xsl:template match="/properties">
<HTML>
<BODY>

Am <xsl:value-of select="longdate"/> wurde eine E-Mail blockiert, die
folgende Regeln verletzt hat:<P/>
<xsl:for-each select="infringedrules/rule">
<B><xsl:value-of select="."/></B><BR/>
</xsl:for-each>

<P>
Folgende      Maßnahme (n)      wurde (n)      eingeleitet:      <B><xsl:value-of
select="action"/></B>
</P>

Zusätzliche Informationen:

<P>
<table border="1">
<tr>
<td>Betreff</td>
<td><B><xsl:value-of select="itemssubject"/></B></td>
</tr>
<tr>
<td>Absender</td>
<td><B><xsl:value-of select="itemsenderemailaddress"/></B></td>
</tr>
<tr>
<td colspan="2" align="center">Empfänger</td>
</tr>

<xsl:for-each select="itemrecipients/recipient">
<tr>
<td colspan="2"><B><xsl:value-of select="."/></B></td>
</tr>
</xsl:for-each>
</table>
</P>
Mit freundlichen Grüßen<BR/>
GFI ContentSecurity.
</BODY>
</HTML>
</xsl:template>

</xsl:stylesheet>
```

Troubleshooting

Einführung

In diesem Kapitel erfahren Sie, welche Hilfsmöglichkeiten es bei Problemen gibt. Folgende Informationsquellen stehen zur Verfügung:

- Das Handbuch – die meisten Probleme lassen sich mithilfe des Handbuchs lösen.
- Die GFI Knowledge-Base auf der Website von GFI.
- Die Support-Site von GFI.
- E-Mail-Anfrage an den GFI-Support an support@gfisoftware.de
- Kontaktaufnahme mit dem GFI-Support über den englischsprachigen Live-Support unter <http://support.gfi.com/livesupport.asp>.
- Telefonische Kontaktaufnahme mit dem GFI-Support.

Wissensdatenbank

Die Knowledge-Base von GFI hält Antworten zu den am häufigsten gestellten Fragen bereit. Bei Problemen sollten Sie zunächst die Knowledge-Base konsultieren. Die Wissensdatenbank bietet immer die neuesten Informationen zu Support-Fragen und Patches.

Sie kann unter <http://kbase.gfi.com> aufgerufen werden.

Support-Anfrage per E-Mail

Wenn Sie Ihre Probleme mit Hilfe der Wissensdatenbank und dem Handbuch nicht lösen konnten, können Sie sich an den GFI-Support wenden. Sie sollten den Support per E-Mail kontaktieren, da Sie an Ihre Nachricht wichtige Informationen anhängen können, die helfen, Ihre Fragen schneller zu beantworten.

Das Programm Troubleshooter aus der Programmgruppe generiert automatisch eine Reihe von Dateien, die GFI zur Problemanalyse benötigt. Die Dateien beinhalten u. a. Angaben zur Konfiguration. Um diese Dateien zu erzeugen, starten Sie den Troubleshooter, und folgen Sie den Anweisungen des Programms.

Neben dem Sammeln von Informationen stellt Ihnen das Programm einige Fragen. Bitte nehmen Sie sich die Zeit, diese korrekt zu beantworten. Ohne die richtigen Informationen ist es dem Kundendienst nicht möglich, Ihr Problem genauer zu diagnostizieren.

Öffnen Sie danach das Verzeichnis „support“, das sich im Unterverzeichnis des Programmverzeichnisses befindet, **ZIPPEN** Sie die Dateien, und senden Sie diese an support@gfisoftware.de.

Stellen Sie jedoch zuvor bitte sicher, dass Sie Ihr Produkt auf unserer Website unter <http://www.gfisoftware.de/de/pages/regfrm.htm> registriert haben!

Ihre Anfrage wird für gewöhnlich innerhalb von 24 Stunden beantwortet.

Support-Anfrage per Web-Chat

Sie erhalten weiteren Support über unseren Live-Chat im Web. Die Kontaktaufnahme mit dem GFI-Support über den Live-Support erfolgt unter <http://support.gfi.com/livesupport.asp>.

Stellen Sie jedoch zuvor bitte sicher, dass Sie Ihr Produkt auf unserer Website unter <http://www.gfisoftware.de/de/pages/regfrm.htm> registriert haben!

Support-Anfrage per Telefon

Für technische Hilfe können Sie auch telefonischen Kontakt mit dem Support-Team aufnehmen. Die entsprechenden Rufnummern für Ihr Land finden Sie auf der Support-Site von GFI.

Support-Website:

<http://support.gfi.com/?lcode=de>

Stellen Sie jedoch zuvor bitte sicher, dass Sie Ihr Produkt auf unserer Website unter <http://www.gfisoftware.de/de/pages/regfrm.htm> registriert haben!

Web-Forum

Über das Web-Forum steht Ihnen der User-to-User-Support zur Verfügung. Das Forum erreichen Sie unter

<http://forums.gfi.com/>

Mitteilungen zu neuen Builds

Es wird empfohlen, für aktuelle Informationen zu den neuesten Produkt-Builds den entsprechenden GFI-Newsletter zu abonnieren. Um stets über die neuesten Builds auf dem Laufenden zu sein, können Sie die Mitteilungen abonnieren unter: <http://support.gfi.com/?lcode=de>.

