Benutzerhandbuch
Revision 1.0

VirusScan® for Mac

Version 8.6

McAfee®
Systemschutz

Bewährte Sicherheit

McAfee®

Inhalt

1 Einführung zu VirusScan for Mac

Welche Informationen enthält dieses Handbuch?

Dieses Handbuch bietet eine Einführung in VirusScan for Mac 8.6 und enthält folgende Themen, in denen Sie erfahren, wie Sie Ihren Rechner virenfrei halten:

- Produktüberblick
- Beschreibungen der Produktfunktionen
- Beschreibungen aller neuen Funktionen in dieser Softwareversion
- Detaillierte Anweisungen für die Installation der Software
- Detaillierte Anweisungen für die Konfiguration und die Ausbringung der Software
- Vorgehensweisen zum Durchführen von Tasks
- Informationen zur Fehlerbehebung
- Integration mit ePolicy Orchestrator 3.6 (Patch 2), 3.6.1 und 4.0

Was ist VirusScan?

VirusScan for Mac ist eine Antivirensoftware, mit der Sie Ihren Macintosh-Rechner frei von Viren, Trojanern oder sonstiger Malware halten können. VirusScan bietet Scannen auf Anforderung, Apple-Mail-Scannen, eUpdate-Planung, Online-Hilfe, Scannen bei Zugriff und Drag-and-Drop-Scannen. Darüber hinaus können Sie mit nur einem Mausklick online auf die umfassende Virusinformationsbibliothek zugreifen, sodass Sie stets über alle neuen Bedrohungen informiert sind.

VirusScan schützt Ihr System vor Viren, die von anderen Rechnern, z. B. Macintosh-, Windows- oder UNIX-Rechnern und extern aktivierten Volumes, wie USB-Geräten, Firewall-Geräten und CDs/DVDs, auf Ihr System übertragen werden können.

Diese Version von VirusScan bietet auch Antivirenschutz für das Betriebssystem Mac OS X 10.5 (Leopard).

Was können Sie mit VirusScan machen?

VirusScan erkennt und entfernt Programmviren, Makroviren und Trojaner in allen Macintosh-, Windows- und UNIX-Dateien, einschließlich komprimierter Dateien und OLE-Verbunddokumenten.

Mit VirusScan können Sie einzelne Dateien, Verzeichnisse, Laufwerke oder aktivierte Volumes, wie CDs, DMG-Dateien, auf dem Netzwerk aktivierte Dateien, Apple-Mail-Nachrichten und USB-Geräte, wie Pen Drives, iPods und Kameras, auf Viren scannen. Unbekannte Makro- und Programmviren werden durch eine verbesserte heuristische Analyse erkannt.

Neue Funktionen dieser Version

- Support für Mac OS X Leopard (10.5)
- Leistungsoptimierung von Scannen bei Zugriff
- Leistungsoptimierung von Scannen auf Anforderung
- Support für ePolicy Orchestrator 4.0
- Inkrementelle DAT-Aktualisierungen
- Support für Scanmodul 5200

VirusScan-Funktionen

VirusScan verbindet seine früheren leistungsstarken Funktionen mit neuen Sicherheitsfunktionen und Tools, mit denen Sie Ihr System noch besser schützen können. In der Online-Hilfe finden Sie Informationen zur Fehlerbehebung und zu Tasks.

VirusScan-Konsole

Die VirusScan-Konsole ermöglicht die Konfiguration von VirusScan über eine einfach zu bedienende Benutzeroberfläche.

Mithilfe der Konsole können Sie den Scanner auf Anforderung konfigurieren und über das Drag-and-Drop-Fenster (ein Bereich der VirusScan-Konsole, in dem Sie mithilfe von Drag-and-Drop zu scannende Dateien einfügen können) Scans auf Anforderung durchführen. Sie können auch auf die **Drop-Elemente oder hier klicken**, um das Dialogfeld **Datei oder Ordner zum Scannen & Säubern auswählen** zu öffnen und die Dateien bzw. Ordner auszuwählen, für die das Scannen auf Anforderung und die Säuberung durchgeführt werden sollen.

Außerdem können Sie den Scanner bei Zugriff über die VirusScan-Konsole konfigurieren und aktivieren sowie die automatische Aktualisierung Ihrer Virusdefinitionen mithilfe von eUpdate aktivieren.

Um auf die VirusScan-Konsole zuzugreifen, doppelklicken Sie im Ordner **Programme** Ihres Computers auf das **VirusScan**-Symbol.

Scanner auf Anforderung

Mit dem Scanner auf Anforderung können Sie jederzeit einen Scan initiieren, indem Sie die ausgewählten Dateien durch Drag-and-Drop in der Konsole ablegen. Sie können auch auf die **Drop-Elemente oder hier klicken**, um das Dialogfeld **Datei oder Ordner zum Scannen & Säubern auswählen** zu öffnen und die Dateien bzw. Ordner auszuwählen, die Sie scannen und säubern möchten.

Mithilfe des Scanners auf Anforderung können Sie mehrere Dateien, Verzeichnisse oder Volumes auswählen. Die Scanergebnisse werden in einem Bericht angezeigt, der gesichert oder gedruckt werden kann. Sie können festlegen, wonach der Scanner sucht und wie er auf infizierte Dateien reagiert. Der Scanner benachrichtigt Sie, wenn er einen Virus findet, und generiert ein Protokoll, in dem die durchgeführten Aktionen aufgezeichnet werden.

Um auf den Scanner auf Anforderung zuzugreifen, ziehen Sie die zu scannenden Dateien auf das **VirusScan**-Symbol oder in das Drag-and-Drop-Fenster der Konsole.

Scanner bei Zugriff

Der Scanner bei Zugriff ermöglicht die ständige Überwachung aller verwendeten Dateien, um zu ermitteln, ob ein Virus oder ein sonstiger potenziell unerwünschter Code vorhanden ist. Ein Scan wird automatisch jedes Mal durchgeführt, wenn eine Datei vom Datenträger gelesen und/oder auf den Datenträger geschrieben wird, sei es durch den Benutzer oder durch Systemprozesse.

Mit dem Scanner bei Zugriff wird eine ständige Richtlinienumsetzung für mehrere Dateien, Verzeichnisse oder Volumes gewährleistet, einschließlich Volumes auf Remote-Rechnern, die über das Netzwerk verbunden sind. Sie können festlegen, wonach der Scanner sucht und wie er auf infizierte Dateien reagiert. Der Scanner meldet im Popup-Fenster **Reporter**, wenn er einen Virus oder andere Malware findet.

Der Scanner bei Zugriff wird über die VirusScan-Konsole aktiviert.

VirusScan Schedule Editor

Mit VirusScan Schedule Editor können Sie automatisierte Scans und Aktualisierungen für die Antivirusdefinitionen (DAT-Dateien) planen, die online verfügbar sind. Sie können Scans und Aktualisierungen über die **VirusScan Schedule Editor**-Konsole planen. Sie können festlegen, dass automatische Scans und Aktualisierungen täglich, wöchentlich oder monatlich durchgeführt werden. Um auf den VirusScan Schedule Editor zuzugreifen, führen Sie einen der folgenden Tasks aus:

- Klicken Sie in der VirusScan-Konsole auf **Scheduler**  .
- Wählen Sie im Hauptmenü im Menü **Darstellung** die Option **Geplanter Task**.
- Rufen Sie VirusScan Schedule Editor direkt aus dem Ordner `/Programme/Dienstprogramme` auf.

eUpdate

Mit eUpdate können Sie DAT-Dateien und das Antivirenmodul aktualisieren. eUpdate aktualisiert Ihre Antivirensoftware ständig mit neuen Informationen zu Viren und Scanfunktionen und sucht automatisch nach neuen Aktualisierungen, wenn eine Internetverbindung besteht, und aktualisiert die Virusdefinitionen, wenn neue verfügbar sind. Mit VirusScan Schedule Editor können Sie eUpdate zudem so konfigurieren, dass nach Ihrem eigenen Zeitplan nach Aktualisierungen gesucht wird.

Um ein eUpdate manuell zu starten, klicken Sie auf die Registerkarte **eUpdate** der VirusScan-Konsole und dann auf die Schaltfläche **Starten**. Die Unterstützung für eUpdate erfolgt über das FTP-Protokoll.

Verwaltung über ePolicy Orchestrator

VirusScan kann zusammen mit McAfee ePolicy Orchestrator Version 3.6 (Patch 2), 3.6.1 und 4.0 verwendet werden, sodass Sie dieses Programm in einer verwalteten Umgebung nutzen können. Die ePolicy Orchestrator-Software bietet einen zentralen Hub für die McAfee System Protection Solutions. Administratoren können das Risiko nicht autorisierter, nicht kompatibler Systeme reduzieren, den Schutz auf dem neuesten Stand halten, Schutzrichtlinien konfigurieren und umsetzen und den Sicherheitsstatus über eine zentralisierte, je nach Unternehmensgröße skalierbare Konsole überwachen. In ePolicy Orchestrator können Sie VirusScan for Mac für alle Zielsysteme im gesamten Netzwerk konfigurieren. So müssen diese Rechner nicht mehr einzeln im Fenster **Voreinstellungen** konfiguriert werden.

Die Verwendung von ePolicy Orchestrator ist optional. Alle Funktionen von VirusScan stehen auch in der Standalone-Version zur Verfügung.

Sie können die auf ePolicy Orchestrator bezogenen Funktionen nur verwenden, wenn Sie ePolicy Orchestrator und den Nicht-Windows-Agenten installiert und für die Verwaltung von VirusScan in einer Unternehmensumgebung konfiguriert haben.

Zielgruppe

Dieses Handbuch ist für Netzwerkadministratoren vorgesehen, die für das Antiviren- und Sicherheitsprogramm Ihres Unternehmens verantwortlich sind.

Konventionen

In diesem Handbuch gelten die folgenden Konventionen:

Bold Condensed	Alle Begriffe der Benutzeroberfläche, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder. **Beispiel:** Geben Sie den **Benutzer**namen und das **Kennwort** des entsprechenden Kontos ein.

`Courier`	Der Pfad eines Ordners oder Programms oder Eingaben, die der Benutzer genau so machen muss (z. B. ein Befehl bei der Eingabeaufforderung).
	Beispiele:
	Der Standardspeicherort für das Programm ist:
	`/Programme/Dienstprogramme`
	Führen Sie folgenden Befehl auf dem Clientrechner aus:
	`scan --help`

Kursiv	Wird zur Hervorhebung oder bei Einführung eines neuen Begriffs sowie für Namen von Produktdokumentation und Themen (Überschriften) des Handbuches verwendet. **Beispiel:** Weitere Informationen finden Sie im *VirusScan Enterprise-Produkthandbuch*.
Blau	Eine Webadresse (URL) und/oder ein aktiver Link. **Beispiel:** Besuchen Sie die McAfee-Site unter: `http://www.mcafee.com`
<BEGRIFF>	Generische Begriffe werden in spitze Klammern gesetzt. **Beispiel:** Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf <SERVER>.
	**Hinweis:** Zusätzliche Informationen, z. B. eine andere Möglichkeit zum Ausführen desselben Befehls.
	**Tipp:** Vorschläge für optimale Methoden sowie Empfehlungen von McAfee zur Vorbeugung von Bedrohungen und zu Leistung und Effizienz.
	**Achtung:** Wichtiger Hinweis, der Informationen zum Schutz Ihres Computersystems, des Unternehmens, der Software oder von Daten enthält.
	**Warnung:** Wichtiger Hinweis, der Informationen zum Schutz des Benutzers beim Umgang mit Hardware enthält.

Produktinformationen

Wenn nicht anders angegeben, steht die Produktdokumentation in Form von Adobe Acrobat PDF-Dateien auf der Produkt-CD oder auf der McAfee-Download-Site zur Verfügung.

Standarddokumentation

Benutzerhandbuch: Dieses Handbuch bietet eine Einführung in das Produkt, beschreibt seine Funktionen und liefert detaillierte Informationen zur Installation und Konfiguration der Software sowie zum laufenden Betrieb und zur Wartung. Darüber hinaus beschreibt es die in Verbindung mit ePolicy Orchestrator verfügbaren Verwaltungsfunktionen für VirusScan und enthält ausführliche Anweisungen zum Installieren, Konfigurieren und Verwalten der Software in einer Unternehmensumgebung. Dieses Handbuch (*VirusScan-Benutzerhandbuch*) finden Sie als PDF-Datei im Ordner **Documentation** des Produktpakets.

Hilfe: Die Hilfe enthält ausführliche Informationen, die in der Softwareanwendung selbst aufgerufen werden können.

Versionshinweise zu VirusScan for Mac: Die Datei enthält Informationen zu den Produktfunktionen, zu aktuellen Zusätzen oder Änderungen an der Dokumentation, zu bekannten Problemen der Produktversion und zur Installation. Diese Datei finden Sie im Ordner **Documentation** des Produktpakets.

Lizenz: Die McAfee-Lizenzvereinbarungsbroschüre (PDF-Datei) enthält alle Lizenzarten, die Sie für Ihr Produkt erwerben können. Die Lizenzvereinbarung enthält die allgemeinen Bedingungen für die Verwendung des lizenzierten Produkts. Lesen Sie diese Bestimmungen sorgfältig durch. Wenn Sie das Produkt installieren, akzeptieren Sie die Bedingungen der Lizenzvereinbarung. Diese McAfee-Lizenzvereinbarung finden Sie im Ordner **Documentation** des Produktpakets.

Links innerhalb des Produkts

Das Hilfemenü im Produkt bietet Links zu einigen nützlichen Ressourcen:

- VirusScan-Hilfe
- Beispiel weiterleiten
- Technischer Support
- Virusinformationsbibliothek

VirusScan-Hilfe

Verwenden Sie diesen Link, um auf die Themen der Online-Hilfe des Produkts zuzugreifen.

Beispiel weiterleiten

Verwenden Sie diesen Link, um potenziell infizierte Dateien zur Analyse an McAfee zu senden. Sie erhalten Informationen zu Ihren Dateien, einschließlich Lösungen und Echtzeitkorrekturen, falls erforderlich.

Technischer Support

Mit diesem Link können Sie auf die Site des technischen Supports von McAfee zugreifen, um Produktinformationen, FAQs oder Hinweise und Tipps zur Fehlerbehebung abzurufen.

Virusinformationsbibliothek

Verwenden Sie den Link „Virusinformationsbibliothek“, um auf die Virusinformationsbibliothek von McAfee Avert Labs zuzugreifen. Diese Website bietet detaillierte Informationen über die Herkunft von Viren sowie über die Art und Weise, wie sie Ihr System infizieren und wie sie entfernt werden können.

Neben Informationen über echte Viren bietet die Virusinformationsbibliothek auch nützliche Information zu Virus-Hoaxes, wie beispielsweise die Viruswarnungen, die Sie per E-Mail erhalten. Die Hoaxes „Virtual Card For You“ und „SULFNBK“ sind wohl die bekanntesten Hoaxes, aber es gibt noch zahlreiche weitere Falschmeldungen dieser Art. Wenn Sie die nächste gut gemeinte Viruswarnung erhalten, sollten Sie zunächst einen Blick auf unsere Hoax-Seite werfen, bevor Sie die Nachricht an Ihre Freunde oder Kollegen weiterleiten.

So greifen Sie auf die Virusinformationsbibliothek zu:

1 Öffnen Sie VirusScan.

2 Wählen Sie im Menü **Hilfe** die Option **Virusinformationsbibliothek**.

Kontaktinformationen

Threat Center: McAfee Avert Labs http://www.mcafee.com/us/threat_center/default.asp

Avert Labs Threat Library
http://vil.nai.com

Avert Labs WebImmune & Beispiel weiterleiten *(Anmeldeinformationen erforderlich)*
https://www.webimmune.net/default.asp

Avert Labs DAT Notification Service
http://vil.nai.com/vil/signup_DAT_notification.aspx

Download-Site http://www.mcafee.com/us/downloads/

Produktaktualisierungen *(gültige Registrierungsnummer erforderlich)*

Sicherheitsaktualisierungen (DAT-Dateien, Modul)

HotFix- und Patch-Versionen

- **Für Sicherheitschwachstellen** *(öffentlich verfügbar)*
- **Für Produkte** *(ServicePortal-Konto und gültige Registrierungsnummer erforderlich)*

Produkttest

McAfee-Beta-Programm

Technischer Support http://www.mcafee.com/us/support/

Suche in der KnowledgeBase
http://knowledge.mcafee.com/

McAfee Technischer Support ServicePortal *(Anmeldeinformationen erforderlich)*
https://mysupport.mcafee.com/eservice_enu/start.swe

Kundendienst

Web
http://www.mcafee.com/us/support/index.html
http://www.mcafee.com/us/about/contact/index.html

Telefon – USA, Kanada und Lateinamerika gebührenfrei:
+1-888-VIRUS NO oder **+1-888-847-8766** Montag-Freitag, 8:00-20:00 Uhr (Central Time)

Professional Services

Großunternehmen: http://www.mcafee.com/us/enterprise/services/index.html

Kleine und mittlere Unternehmen: http://www.mcafee.com/us/small/services/index.html

2 Installieren von VirusScan for Mac

Dieser Abschnitt enthält Informationen zur Installation der VirusScan-Software sowie Einzelheiten zu folgenden Themen:

Systemanforderungen

Für die Installation von VirusScan for Mac ist ein PowerPC oder ein Intel-basierter Mac-Computer mit Mac OS X Tiger 10.4.6 (oder höher) oder Mac OS X Leopard 10.5, mindestens 512 MB RAM und 45 MB freiem Festplattenspeicher erforderlich.

Anforderungen für ePolicy Orchestrator

VirusScan kann zusammen mit ePolicy Orchestrator 3.6 (Patch 2), 3.6.1 und 4.0 verwendet werden. Die Verwendung von ePolicy Orchestrator ist optional. VirusScan for Mac kann auch als Standalone-Version verwendet werden.

Sie können die auf ePolicy Orchestrator bezogenen Funktionen nur verwenden, wenn Sie ePolicy Orchestrator und den Nicht-Windows-Agenten installiert und für die Verwaltung von VirusScan in einer Unternehmensumgebung konfiguriert haben.

Installieren von VirusScan

VirusScan for Mac kann entweder über eine Standardinstallation (mit grafischer Benutzeroberfläche) oder eine Befehlszeileninstallation (Hintergrundinstallation) installiert werden. Nach der Installation des Produkts steht die zugehörige ReadMe-Datei im Ordner **Documentation** des Produktpakets zur Verfügung. In dieser Datei finden Sie Informationen zu bekannten Problemen, Online-Ressourcen und andere nützliche Informationen.

In VirusScan können Sie mit eUpdate eine Verbindung zu einer Website herstellen und neue DAT-Dateien herunterladen. Weitere Informationen zu eUpdate und anderen VirusScan-Funktionen finden Sie unter *Erste Schritte* auf Seite 17.

Zur Installation dieses Produkts sind Administratorrechte zwingend erforderlich.

Standardinstallation

Sie können VirusScan mithilfe der VirusScan-Installationsdatei installieren, die Sie auf der Produkt-CD oder in der ZIP-Installationsdatei finden, die Sie von der McAfee-Site heruntergeladen und in einem temporären Ordner gespeichert haben.

So installieren Sie VirusScan:

1. Doppelklicken Sie auf die Datei **VirusScan.pkg**, um das Installationsprogramm zu starten.
2. Führen Sie die angezeigten Schritte durch, um die Software zu installieren.
3. Lesen und bestätigen Sie die Lizenzvereinbarung. Wenn Sie der Lizenzvereinbarung nicht zustimmen, können Sie nicht mit der Installation fortfahren.
4. Klicken Sie auf **Installieren**, um die Installation durchzuführen. Das Dialogfeld **Authentifizieren** wird angezeigt.
5. Geben Sie Ihren Benutzernamen und Ihr Administratorkennwort ein, und klicken Sie auf **OK**. Nach Abschluss des Installationsvorgangs wird eine Meldung angezeigt. Klicken Sie auf **Schließen**.

Mit dem Installationsprogramm von VirusScan for Mac wird VirusScan auf Ihrem Computer im Ordner `Programme` und VirusScan Schedule Editor im Ordner `Programme/Dienstprogramme` installiert.

Anders als bei früheren Versionen müssen Sie Ihren Computer nach der Installation von VirusScan for Mac 8.6 nicht neu starten.

Befehlszeileninstallation (Hintergrundinstallation)

1 Suchen Sie die Datei **VirusScan.pkg** auf der Produkt-CD oder in der ZIP-Installationsdatei, die Sie von der McAfee-Site heruntergeladen haben, und speichern Sie die Datei in einem temporären Ordner.

2 Öffnen Sie das **Terminal**-Fenster, und wechseln Sie zu dem Verzeichnis, in dem sich die Datei **VirusScan.pkg** befindet.

3 Führen Sie im **Terminal**-Fenster folgenden Befehl aus:

```
sudo installer -pkg VirusScan.pkg -target /
```

4 Geben Sie auf Aufforderung Ihr Systemkennwort ein.

5 Nach Abschluss des Installationsvorgangs wird eine Meldung angezeigt. Schließen Sie das **Terminal**-Fenster.

Aktualisierungsinstallation

Frühere Versionen von VirusScan (8.0 und 8.5) können auf VirusScan for Mac Version 8.6 aktualisiert werden. Nach der Aktualisierung werden die Voreinstellungen von früheren Versionen in die aktuelle Version (8.6) migriert.

Testen der Installation

Sie können VirusScan mithilfe der Standard-Antiviren-Testdatei des European Institute of Computer Anti-Virus Research (EICAR) testen. Diese Datei wurde in Zusammenarbeit mit Anbietern von Antivirensoftware auf der ganzen Welt entwickelt, um einen Standard bereitzustellen, mit dem Kunden die Funktionsfähigkeit ihrer Antivirensoftware überprüfen können.

So testen Sie das installierte Programm:

1 Öffnen Sie die EICAR.ORG-Website (http://www.eicar.org), und laden Sie die AntiVirus-Testdatei Eicar.zip herunter.

2 Führen Sie den Scanner auf Anforderung für die heruntergeladene ZIP-Datei aus. VirusScan meldet, dass die EICAR-Testdatei gefunden wurde.

Bei dieser Datei handelt es sich *nicht* um einen Virus. Sie ist zum Testen von Antivirensoftware gedacht. Sie können die Datei löschen, wenn der Testvorgang für die Software beendet ist, um andere Benutzer nicht unnötig zu verunsichern.

Wenn der Test erfolgreich war, können Sie jetzt beginnen, die VirusScan-Software zu verwenden.

Deinstallieren von VirusScan

Sie deinstallieren VirusScan mithilfe einer Deinstallationsdatei (**VirusScan Uninstall.command**), die Sie auf der Produkt-CD oder in der ZIP-Installationsdatei finden, die Sie von der McAfee-Site heruntergeladen und in einem temporären Ordner gespeichert haben. Sie können auch einen Deinstallationsbefehl über das Terminal-Fenster ausführen.

So deinstallieren Sie VirusScan:

1 Führen Sie einen der folgenden Schritte aus:

- Doppelklicken Sie auf das Symbol **VirusScan Uninstall.command**.
- Verschieben Sie das Symbol **VirusScan Uninstall.command** per Drag-and-Drop in das **Terminal**-Fenster, und drücken Sie die Eingabetaste.
- Öffnen Sie das **Terminal**-Fenster, wechseln Sie zum Verzeichnis `/usr/local/vscanx/`, und führen Sie **VirusScan Uninstall.command** aus.

Um das **Terminal**-Programm zu öffnen, doppelklicken Sie unter `/Programme/Dienstprogramm` auf das Programm.

Im **Terminal**-Fenster werden Sie aufgefordert, das Administratorkennwort einzugeben.

2 Geben Sie Ihr Administratorkennwort ein, und klicken Sie dann auf **Eingeben**.

Ihr Administratorkennwort wird nicht im **Terminal**-Fenster angezeigt.

Nach erfolgreicher Deinstallation wird im **Terminal**-Fenster eine Meldung angezeigt, die besagt, dass die VirusScan-Software vom Rechner entfernt wurde.

3 Erste Schritte

Dieses Kapitel enthält Informationen zu VirusScan und darüber, wie Sie Ihren Rechner mit diesem Programm vor Viren schützen können. Es beinhaltet folgende Themen:

Verwenden der VirusScan-Konsole

Die VirusScan-Konsole ermöglicht die Verwendung und Konfiguration von Scannen auf Anforderung und bei Zugriff. Die Konsole stellt eine Verbindung zur Virusinformationsbibliothek von McAfee her, führt eUpdates durch und druckt und sichert Scanberichte.

Die VirusScan-Konsole enthält außerdem ein Drag-and-Drop-Fenster für das Scannen auf Anforderung. Sie können einen Scan auf Anforderung jederzeit initiieren, indem Sie Dateien in das mittlere Fenster der Konsole ziehen, im Drag-and-Drop-Fenster ablegen und dann auf die Schaltfläche **Starten** klicken. Wenn Sie nach Beendigung des Scanvorgangs weitere Dateien in das Drag-and-Drop-Fenster ziehen, werden die zuvor gescannten Dateien durch die neuen Dateien ersetzt.

Die VirusScan-Konsole

Die VirusScan-Konsole enthält neben den üblichen Macintosh-Komponenten spezielle Antivirenkomponenten, z. B.:

- Titelleiste mit dem Namen des aktuell ausgeführten Programms.

- Symbolleistenschaltflächen zum Schließen, Ablegen im Dock, Vergrößern oder Ausblenden des Fensters.

Abbildung 3-1 VirusScan-Konsole

Symbolleiste

Auf der Symbolleiste befinden sich die folgenden Schaltflächen:

Sichert den Scanbericht als RTF-Datei (Rich Text Format).

Löscht den Bericht, der aktuell im Statusfenster angezeigt wird.

Druckt den aktuellen Bericht.

Ermöglicht die Planung von Scantasks und eUpdate-Tasks.

Öffnet das Dialogfeld **Voreinstellungen**, in dem Sie die folgenden Aktionen durchführen können:

- Voreinstellungen für den Scanner auf Anforderung festlegen.
- Voreinstellungen für den Scanner bei Zugriff festlegen.
- Voreinstellungen für die Aktion festlegen, die durchgeführt werden soll, wenn ein Virus gefunden wird.
- Ergebnisse in einer Datei protokollieren.
- eUpdate-Servereinstellungen konfigurieren.
- Ausschlussliste konfigurieren.
- Automatisch nach Virusdefinitionsaktualisierungen suchen.

Öffnet Ihren Standard-Browser, und leitet Sie zur Virusinformationsbibliothek von McAfee weiter.

Menüleiste

Auf der Menüleiste befinden sich Standard-Dropdown-Menüs, die in allen Fenstern angezeigt werden: **Ablage**, **Bearbeiten**, **Darstellung**, **Fenster** und **Hilfe**.

Konfigurieren der Scanner

Im Dialogfeld **Voreinstellungen** können Sie die Einstellungen für den Scanner auf Anforderung und den Scanner bei Zugriff konfigurieren. Es sind zwei Versionen dieses Dialogfensters verfügbar: eine zur Konfiguration des Scanners auf Anforderung und eine für den Scanner bei Zugriff. Für beide Scanner gelten die gleichen allgemeinen Voreinstellungen, während die erweiterten Scanoptionen scannerspezifisch sind.

Scanner-Voreinstellungen sind globale Einstellungen, die für alle Benutzer gelten.

Die Voreinstellungen werden bei Ihrer Auswahl automatisch gespeichert.

Zum Ändern der Voreinstellungen benötigen Sie Administratorrechte.

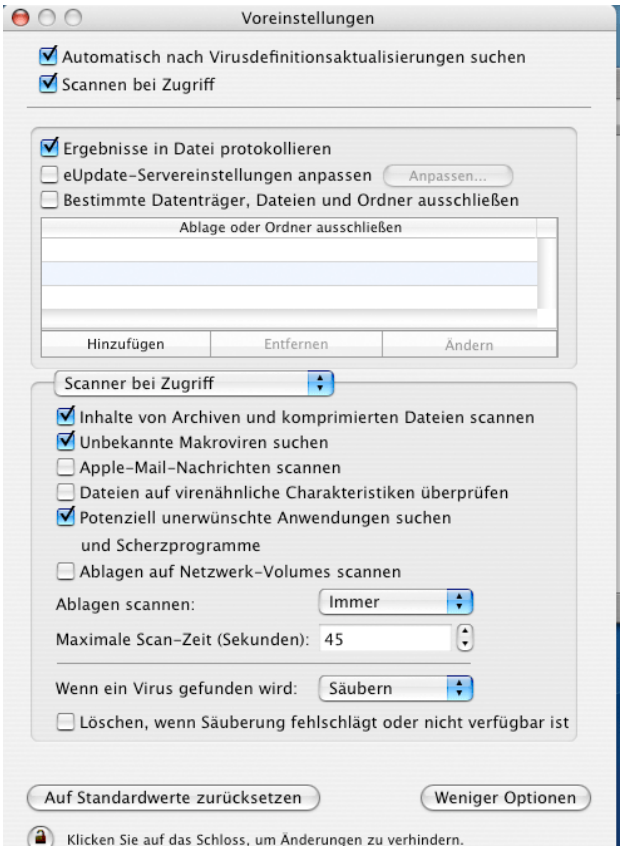
Konfigurieren der allgemeinen Voreinstellungen

Die allgemeinen Voreinstellungen gelten sowohl für den Scanner auf Anforderung als auch für den Scanner bei Zugriff. Sie sind für beide Scanner identisch.

So konfigurieren Sie allgemeine Voreinstellungen:

1 Klicken Sie in der Symbolleiste auf **Voreinstellungen**  , um das Dialogfeld **Voreinstellungen** anzuzeigen. Das obere Fenster in diesem Dialogfeld enthält Optionen für die allgemeinen Voreinstellungen, die sowohl für den Scanner auf Anforderung als auch für den Scanner bei Zugriff gelten.

Abbildung 3-2 Allgemeine Voreinstellungen



2 Wählen Sie Ihre allgemeinen Scanvoreinstellungen für den Scanner auf Anforderungen und den Scanner bei Zugriff aus. Tabelle 3-1 enthält die verfügbaren allgemeinen Voreinstellungen.

Tabelle 3-1 Allgemeine Voreinstellungen für den Scanner auf Anforderungen und den Scanner bei Zugriff

Automatisch nach Virusdefinitions-aktualisierungen suchen	Aktiviert bzw. deaktiviert automatische eUpdates.
Scannen bei Zugriff	Aktiviert/deaktiviert das Scannen bei Zugriff.
Ergebnisse in Datei protokollieren	Aktiviert bzw. deaktiviert die Protokollierung der Ergebnisse in einer Datei.
Meine eUpdate-Servereinstellungen aktualisieren	Mithilfe dieser Option können Sie Ihren Aktualisierungsserver mit Benutzernamen und Kennwort verwalten. Klicken Sie auf **Anpassen**, um die FTP-Einstellungen für eUpdate zu ändern.

Tabelle 3-1 Allgemeine Voreinstellungen für den Scanner auf Anforderungen und den Scanner bei Zugriff

Bestimmte Datenträger, Dateien und Ordner ausschließen	Mithilfe dieser Option können Sie bestimmte Elemente vom Scan ausschließen. Wenn Sie diese Option nicht auswählen, werden keine auszuschließenden Elemente festgelegt. **So fügen Sie einen Ausschluss hinzu:** ■ Klicken Sie in der Liste **Ablage oder Ordner ausschließen** auf **Hinzufügen**. Wählen Sie die gewünschte Datei bzw. den gewünschten Ordner im Dialogfeld **Öffnen** aus. **So entfernen Sie einen Ausschluss:** ■ Wählen Sie die Datei bzw. den Ordner in der Liste **Ablage oder Ordner ausschließen** aus. Klicken Sie auf **Entfernen**. **So ändern Sie einen Ausschluss:** ■ Wählen Sie die Datei bzw. den Ordner in der Liste **Ablage oder Ordner ausschließen** aus. Klicken Sie auf **Ändern**. Das Dialogfeld **Öffnen** wird angezeigt. Wählen Sie die Datei bzw. den Ordner aus, der den bestehenden Ausschluss ersetzen soll.

3 Legen Sie die gewünschten erweiterten Voreinstellungen fest. Diese werden im unteren Fenster des Dialogfelds **Voreinstellungen** angezeigt. Es sind zwei verschiedene Gruppen von Voreinstellungen verfügbar: eine für den Scanner auf Anforderung und eine für den Scanner bei Zugriff. Weitere Informationen hierzu finden Sie unter *Konfigurieren des Scanners auf Anforderung auf Seite 21* und *Konfigurieren des Scanners bei Zugriff auf Seite 23*.

4 Klicken Sie auf das **Schloss**, damit keine Änderungen an den Voreinstellungen vorgenommen werden können.

5 Klicken Sie in der linken oberen Ecke auf **Schließen**, um das Dialogfeld **Voreinstellungen** zu schließen.

Konfigurieren des Scanners auf Anforderung

Mit dem Scanner auf Anforderung können Sie jederzeit einen Scan initiieren. Sie konfigurieren die erweiterten Voreinstellungen des Scanners auf Anforderung mithilfe der im unteren Fenster des Dialogfelds „Voreinstellungen“ verfügbaren Optionen.

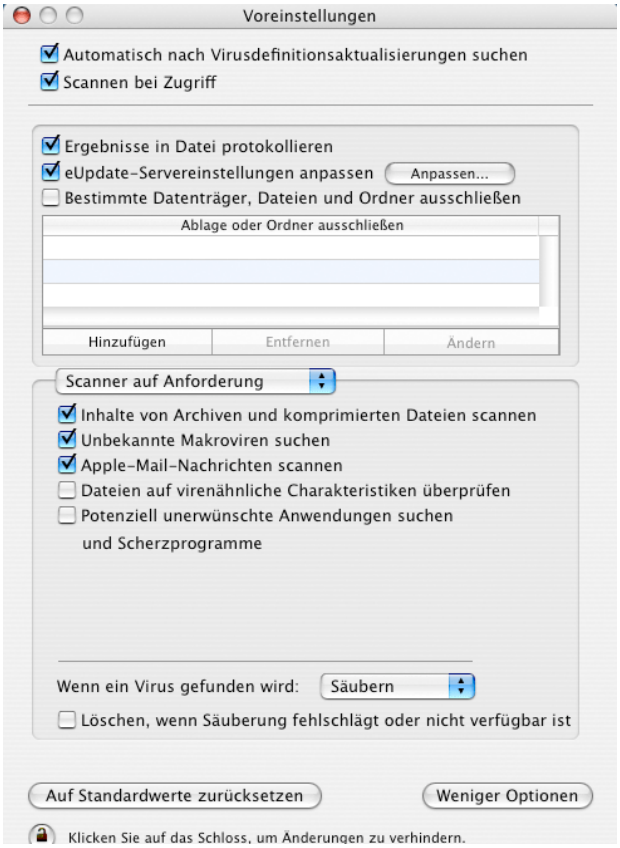
So konfigurieren Sie den Scanner auf Anforderung:

1 Klicken Sie in der Symbolleiste auf **Voreinstellungen**  , um das Dialogfeld **Voreinstellungen** anzuzeigen.

2 Klicken Sie in der unteren rechten Ecke des Dialogfelds auf **Mehr Optionen**, um die erweiterten Voreinstellungen anzuzeigen.

3 Wählen Sie **Scanner auf Anforderung** aus dem Dropdown-Menü aus (wenn nicht bereits ausgewählt), um die Version dieses Dialogfelds für Scannen auf Anforderung anzuzeigen.

Abbildung 3-3 Voreinstellungen für Scanner auf Anforderung



4 Wählen Sie Ihre erweiterten Voreinstellungen für den Scanner auf Anforderung aus. Tabelle 3-2 enthält die verfügbaren Voreinstellungen.

Tabelle 3-2 Erweiterte Einstellungen für Scanner auf Anforderung

Inhalte von Archiven und komprimierten Dateien scannen	Mithilfe dieser Option können Sie festlegen, dass der ausgewählte Scanner Archive und andere komprimierte Dateien scannt. Für den Scanner auf Aufforderung ist sie standardmäßig aktiviert.
Unbekannte Makroviren suchen	Wenn eine Datei ein potenziell infiziertes Makro (unbekannte Infektionen) enthält, wird die Datei im Rahmen der Säuberung gescannt und gesäubert/gelöscht.
Apple-Mail-Nachrichten scannen	Aktiviert/deaktiviert den Scanner auf Anforderung für die Überprüfung von Apple-Mail-Nachrichten auf Infektionen.
Dateien auf virenähnliche Charakteristiken überprüfen	Aktiviert/deaktiviert im Scanner auf Anforderung die Suche nach Dateien, die virus- oder wurmähnliche Eigenschaften aufweisen und unbekannte Infektionen enthalten können.

Tabelle 3-2 Erweiterte Einstellungen für Scanner auf Anforderung

Potenziell unerwünschte Programme und Scherzprogramme suchen	Aktiviert/deaktiviert den Scanner auf Anforderung für die Suche nach unerwünschten Programmen oder Scherzprogrammen.
Wenn ein Virus gefunden wird: ■ Säubern ■ Löschen ■ Benachrichtigen	Mit dieser Option können Sie die primäre Aktion des Scanners auf Anforderung festlegen.
Löschen, wenn Säuberung fehlschlägt oder nicht verfügbar ist	Mit dieser Option können Sie die sekundäre Aktion des Scanners auf Anforderung festlegen. Diese Option ist nur verfügbar, wenn **Säubern** als primäre Aktion festgelegt wurde.

5 Klicken Sie auf das **Schloss**, damit keine Änderungen an den Voreinstellungen vorgenommen werden können.

6 Klicken Sie in der linken oberen Ecke auf **Schließen**, um das Dialogfeld **Voreinstellungen** zu schließen.

Konfigurieren des Scanners bei Zugriff

Der Scanner bei Zugriff überwacht ständig alle verwendeten Dateien, um festzustellen, ob ein Virus oder sonstige Malware vorhanden ist. Der Scan bei Zugriff findet immer dann statt, wenn eine Datei vom Datenträger gelesen wird, wenn eine Datei auf den Datenträger geschrieben wird oder in beiden Fällen, je nach den für diesen Scanner festgelegten Voreinstellungen.

Sie konfigurieren die erweiterten Voreinstellungen des Scanners bei Zugriff mithilfe der im unteren Fenster des Dialogfelds „Voreinstellungen“ verfügbaren Optionen.

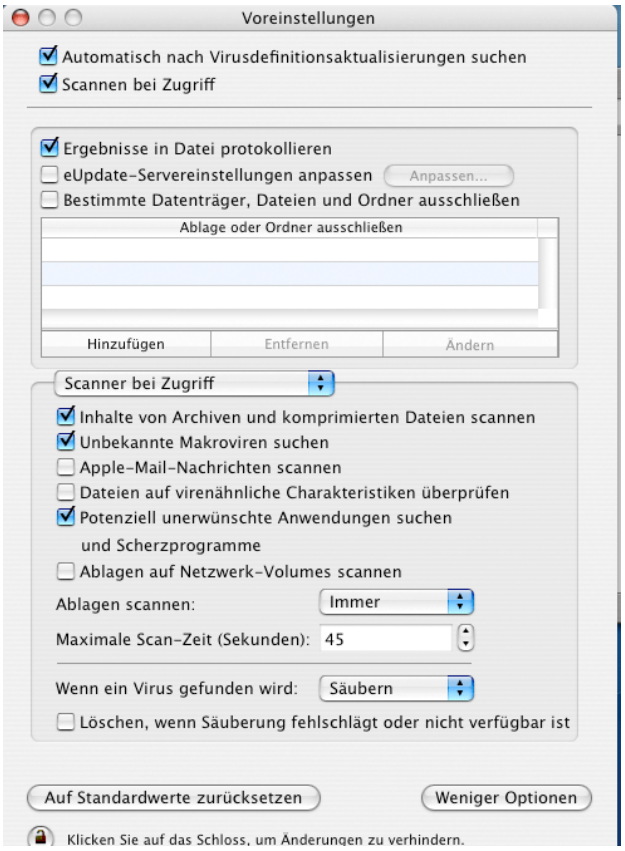
So konfigurieren Sie den Scanner bei Zugriff:

1 Klicken Sie in der Symbolleiste auf **Voreinstellungen**  , um das Dialogfeld **Voreinstellungen** anzuzeigen.

2 Klicken Sie in der unteren rechten Ecke des Dialogfelds auf **Mehr Optionen**, um die erweiterten Voreinstellungen anzuzeigen.

3 Wählen Sie im Dropdown-Menü **Scanner bei Zugriff** aus (wenn nicht bereits ausgewählt), um die Version dieses Dialogfensters für das Scannen bei Zugriff anzuzeigen.

Abbildung 3-4 Voreinstellungen für den Scanner bei Zugriff



4 Wählen Sie Ihre Voreinstellungen für den Scanner bei Zugriff aus. Tabelle 3-3 enthält die verfügbaren Voreinstellungen.

Tabelle 3-3 Erweiterte Einstellungen für das Scannen bei Zugriff

Inhalte von Archiven und komprimierten Dateien scannen	Mithilfe dieser Option können Sie festlegen, dass der ausgewählte Scanner Archive und andere komprimierte Dateien scannt. Standardmäßig ist diese Option für den Scanner bei Zugriff aktiviert. Beachten Sie, dass der Scanner bei Zugriff keine Stuffit-Archive überprüft.
Unbekannte Makroviren suchen	Wenn eine Datei ein potenziell infiziertes Makro (unbekannte Infektionen) enthält, wird die Datei im Rahmen der Säuberung gescannt und gesäubert/gelöscht.
Apple-Mail-Nachrichten scannen	Aktiviert/deaktiviert im Scanner bei Zugriff die Überprüfung von Apple-Mail-Nachrichten auf Infektionen.

Tabelle 3-3 Erweiterte Einstellungen für das Scannen bei Zugriff

Dateien auf virenähnliche Charakteristiken überprüfen	Aktiviert/deaktiviert im Scanner bei Zugriff die Suche nach Dateien, die virus- oder wurmähnliche Eigenschaften aufweisen und unbekannte Infektionen enthalten können.
Potenziell unerwünschte Programme und Scherzprogramme suchen	Aktiviert/deaktiviert im Scanner bei Zugriff die Suche nach unerwünschten Programmen oder Scherzprogrammen.
Ablagen auf Netzwerk-Volumes scannen	Legt fest, dass der Scanner Dateien scannt, auf die über Netzwerk-Volumes zugegriffen wird.
Ablagen scannen: ■ Immer ■ Lesen ■ Schreiben	Legt fest, ob der Scanner bei Zugriff Dateien scannen soll, die vom Datenträger gelesen werden, die auf den Datenträger geschrieben werden oder beides.
Maximale Scan-Zeit	Die maximale Dauer (in Sekunden) für einen Scan einer Datei. (Eine komprimierte Datei wird nicht als eine Datei interpretiert. Diese Zeitspanne gilt für die letzte Einzeldatei und nicht für die letzte Container-Datei der höchsten Ebene.)
Wenn ein Virus gefunden wird: ■ Säubern ■ Löschen ■ Benachrichtigen	Mit dieser Option können Sie die primäre Aktion des Scanners bei Zugriff festlegen.
Löschen, wenn Säuberung fehlschlägt oder nicht verfügbar ist	Wenn diese Option aktiviert ist, wird die für den Scanner festgelegte sekundäre Aktion ausgeführt. Diese Option ist nur verfügbar, wenn **Säubern** als primäre Aktion festgelegt wurde.

5 Klicken Sie auf das **Schloss**, damit keine Änderungen an den Voreinstellungen vorgenommen werden können.

6 Klicken Sie in der linken oberen Ecke auf **Schließen**, um das Dialogfeld **Voreinstellungen** zu schließen.

Verwenden des Scanners auf Anforderung

Mithilfe des Scanners auf Anforderung können Sie Scans jederzeit auf folgende Weise starten:

- Durch Ziehen von Dateien auf das **VirusScan**-Dock-Symbol, das **VirusScan**-Symbol im Finder oder in das Drag-and-Drop-Fenster der Konsole.
- Über das Dialogfeld **Datei oder Ordner zum Scannen & Säubern auswählen**.

Sie können mehrere Dateien oder Verzeichnisse auswählen. Die Gesamtergebnisse werden im Protokollfenster angezeigt.

So initiieren Sie einen Scan auf Anforderung:

1 Öffnen Sie die VirusScan-Konsole.

2 Ziehen Sie die zu scannende Datei, den Ordner oder das Volume in das Drag-and-Drop-Fenster der Hauptkonsole. Gehen Sie folgendermaßen vor, um mehrere Dateien auszuwählen:

- Halten Sie die **Umschalttaste** gedrückt, und wählen Sie die gewünschten Dateien aus.
- Klicken Sie auf das Drag-and-Drop-Fenster. Ein Auswahlfenster wird angezeigt. Wählen Sie die zu scannenden Dateien, Verzeichnisse oder Volumes aus, und klicken Sie auf **Objekt auswählen**.
- Ziehen Sie die Dateien, Ordner oder Volumes auf das **VirusScan**-Dock-Symbol im **Finder**.

3 Klicken Sie in der Konsole auf **Starten**, um das Scannen zu beginnen.

In der **Statuszeile** werden der Name der gescannten Datei und der Status des Scans angezeigt. Der **Pfeil** neben der Statuszeile dient zum Anzeigen oder Ausblenden des **Protokollfensters**. Das **Protokollfenster** ist standardmäßig ausgeblendet.

Im **Protokollfenster** wird ein Scanbericht angezeigt. Der Bericht enthält die Uhrzeit des Scans, die Gesamtzahl der gescannten Dateien und die durchgeführten Aktionen. In der Konsole wird der Status eines Scans zwischen dem Drag-and-Drop-Fenster und dem Protokollfenster angezeigt. Im Statusfenster wird **Leerlauf** angezeigt, wenn kein Scan durchgeführt wird.

Verwenden des Scanners bei Zugriff

Mit dem Scanner bei Zugriff wird eine ständige, automatische Richtlinienumsetzung für mehrere Dateien, Verzeichnisse oder Volumes gewährleistet, einschließlich Volumes auf Remote-Rechnern, die über das Netzwerk verbunden sind. Aktivieren Sie einfach den Scanner bei Zugriff, um ihn auszuführen.

So aktivieren Sie das Scannen bei Zugriff:

1 Öffnen Sie die VirusScan-Konsole.

2 Klicken Sie in der Symbolleiste auf **Voreinstellungen**  , um das Dialogfeld **Voreinstellungen** anzuzeigen.

3 Wählen Sie das Kontrollkästchen **Scannen bei Zugriff** aus, um das Scannen bei Zugriff zu aktivieren.

Der Scanner meldet im Popup-Fenster **Reporter**, wenn er einen Virus oder andere Malware findet.

Aktualisieren der DAT-Dateien

eUpdate stellt standardmäßig jeden Tag über Ihre Internetverbindung eine Verbindung zum eUpdate-Server her und sucht nach neuen DAT-Dateien. Die Aktualisierungen können Proxyserver überschreiten. Über **VirusScan Schedule Editor** können Sie weitere eUpdates planen.

Automatische und geplante eUpdates und Scans auf Anforderung können gleichzeitig ausgeführt werden.

Warum müssen die Aktualisierungen durchgeführt werden?

Damit Sie vor den neuesten Bedrohungen geschützt sind, sollten Sie Ihre Antivirensoftware auf dem neuesten Stand halten, indem Sie die DAT-Dateien und das Modul regelmäßig aktualisieren.

- Es tauchen regelmäßig neue Viren und Würmer auf. McAfee erstellt aktualisierte DAT-Dateien, um sicherzustellen, dass VirusScan solche Viren und Würmer erkennen und entfernen kann.
- Gelegentlich sind Aktualisierungen des Scanmoduls verfügbar. Diese ermöglichen VirusScan, die neuesten Viruserkennungstechniken einzusetzen.

Wie funktioniert eUpdate?

Mithilfe von eUpdate erhalten Sie neue DAT-Dateien oder Aktualisierungen der Antivirensoftware, wenn eine Internetverbindung hergestellt ist. Wenn eine Aktualisierung vorhanden ist, versucht VirusScan automatisch, diese herunterzuladen und zu installieren. Wenn ein Tag ohne Aktualisierung vergeht, lädt VirusScan die Aktualisierung automatisch herunter. Auf diese Weise wird sichergestellt, dass Ihr System immer auf dem neuesten Stand ist.

Konfigurieren von eUpdate-Einstellungen

DAT-Dateien können über einen FTP-Server aktualisiert werden. McAfee stellt einen FTP-Server für eUpdates Ihrer DAT-Dateien bereit.

McAfee-FTP-Server

Standardmäßig ist VirusScan so konfiguriert, dass es zum Herunterladen der neuesten DAT-Dateien auf den McAfee-FTP-Server zugreift. Nach der Installation von VirusScan stellt das Programm bei einer bestehenden Internetverbindung automatisch eine Verbindung zum FTP-Server her, um die DAT-Dateien herunterzuladen und zu aktualisieren.

Konfigurieren des internen FTP-Servers

Zur Verwendung eines internen FTP-eUpdate-Repository für Ihre Macintosh-Rechner im Netzwerk müssen Sie einen internen FTP-eUpdate-Server konfigurieren. In diesem Fall müssen Sie regelmäßig die DAT-Dateien vom McAfee-FTP-Server (`ftp://ftp.mcafee.com/commonupdater`) auf den konfigurierten internen FTP-Server herunterladen.

So konfigurieren Sie den internen FTP-Server:

1. Laden Sie die DAT-Datei von `ftp://ftp.mcafee.com/commonupdater` herunter.
2. Kopieren Sie die DAT-Datei in einen Ordner auf dem FTP-eUpdate-Server.

So können Sie über „Voreinstellungen“ auf den FTP-Server zugreifen:

1. Öffnen Sie die VirusScan-Konsole, um die Einstellungen im Dialogfeld **eUpdate-Servereinstellungen** zu ändern.
2. Klicken Sie in der Symbolleiste auf **Voreinstellungen**. Das Dialogfeld **Voreinstellungen** wird angezeigt. Wählen Sie die Option **eUpdate-Servereinstellungen anpassen** aus.
3. Klicken Sie auf die Schaltfläche **Anpassen**. Das Dialogfeld **eUpdate-Serverereinstellungen** wird angezeigt.
4. Geben Sie unter **Server-URL** die URL des FTP-Servers ein.
5. Geben Sie unter **Verzeichnis** das Verzeichnis ein, in das Sie die DAT-Dateien heruntergeladen haben.
6. Klicken Sie auf **OK**.

Beispiel:

1 Erstellen Sie auf Ihrem FTP-Server auf der obersten Ebene ein Verzeichnis namens "commonupdater".

2 Öffnen Sie `ftp://ftp.mcafee.com/commonupdater`.

3 Laden Sie die folgenden Dateien von `ftp://ftp.mcafee.com/commonupdater/` in das Verzeichnis `<Ihr FTP-Server>/commonupdater/` herunter:

- oem.ini
- alle GEM-Dateien
- gdeltaavv.ini

4 Laden Sie die Datei avvdat-xxxx.zip von `ftp://ftp.mcafee.com/commonupdater/current/VSCANDAT1000/DAT/0000/` in das Verzeichnis `<Ihr FTP-Server>/commonupdater/current/VSCANDAT1000/DAT/0000/` herunter.

5 Virusdefinitionen werden täglich aktualisiert. Daher müssen Sie die Schritte 1 bis 4 täglich wiederholen, wenn Sie Ihr lokales Aktualisierungs-Repository auf dem neuesten Stand halten möchten.

Wie können Sie eUpdate über einen Proxyserver verwenden?

Die Proxyeinstellungen von WebProxy (HTTP) werden unterstützt. Details zur Konfiguration dieser Proxyeinstellungen unter Max OS X finden Sie in der Apple-Dokumentation.

Außerdem müssen Sie sicherstellen, dass der anonyme Zugriff auf den FTP-Server aktiviert ist, damit eUpdate funktionieren kann.

VirusScan unterstützt keine Proxyserverauthentifizierung.

Verwenden von VirusScan Schedule Editor

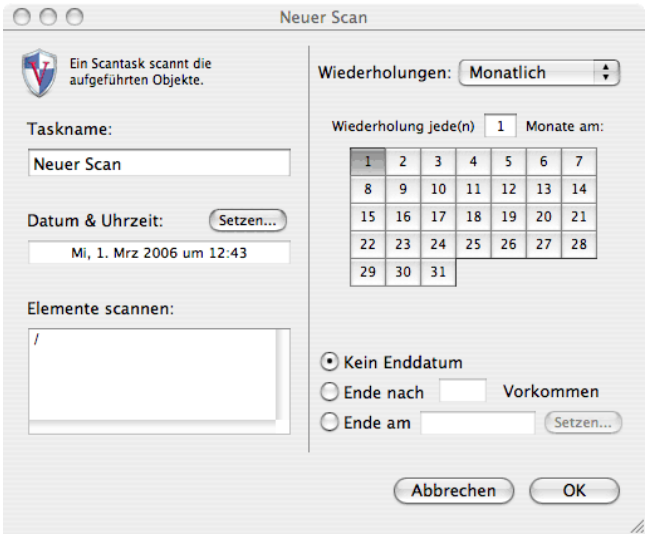
In VirusScan Schedule Editor können Sie festlegen, dass bestimmte Dateien oder Verzeichnisse wiederholt gescannt werden sollen. Sie können festlegen, dass die Scans täglich, wöchentlich oder monatlich durchgeführt werden.

So planen Sie einen Scan:

1 Klicken Sie in der VirusScan-Konsole auf **Scheduler**. Alternativ können Sie **Geplanter Task** im Menü **Darstellung** im Hauptmenü auswählen. Daraufhin wird das Dialogfeld **VirusScan Schedule Editor** angezeigt.

2 Klicken Sie auf **Neuer Scantask**  . Ein Dialogfeld **Ohne Titel** wird angezeigt.

Abbildung 3-5 Dialogfeld „Neuer Scan“



3 Benennen Sie den Task. Verwenden Sie einen beschreibenden Namen für den geplanten Scan.

4 Klicken Sie auf **Setzen**, um **Datum & Uhrzeit** des geplanten Scans anzugeben.

5 Wählen Sie die zu scannenden Elemente aus. Dazu haben Sie die folgenden Möglichkeiten:

- Ziehen und Ablegen der Elemente im Fenster **Scanelemente**.
- Klicken auf das Fenster **Elemente scannen**. Das Dialogfeld **Element wählen** wird angezeigt. Klicken Sie auf **Wählen**, wenn Sie die zu scannende(n) Datei(en) ausgewählt haben.

6 Wählen Sie **Wiederholung**. Folgende Optionen stehen zur Auswahl:

- **Täglich**: Geben Sie das Tagesintervall für den Scan an.
- **Wöchentlich**: Wählen Sie aus, an welchen Tagen der Woche der Scanvorgang durchgeführt werden soll.
- **Monatlich**: Wählen Sie aus, an welchen Tagen des Monats und in welchen Monaten der Scan durchgeführt werden soll.
- **Nie**: Wählen Sie diese Option, wenn keine Wiederholung stattfinden soll.

7 Geben Sie an, wann der geplante Scan endet, und klicken Sie auf **OK**.

Der neue Scantask wird in einer Liste mit allen geplanten Scans und eUpdates in VirusScan Schedule Editor angezeigt. Um geplante Tasks zu aktivieren oder zu deaktivieren, aktivieren Sie das Kontrollkästchen neben dem Task.

Wenn der Computer beim Ausführen eines geplanten Tasks ausgeschaltet wird, überspringt VirusScan den Task, wenn der Computer erneut eingeschaltet wird.

Planen von eUpdates

In VirusScan Schedule Editor können Sie festlegen, dass die DAT-Dateien Ihres Rechners und das Scanmodul in regelmäßigen Abständen aktualisiert werden sollen. Dies wird durch FTP unterstützt.

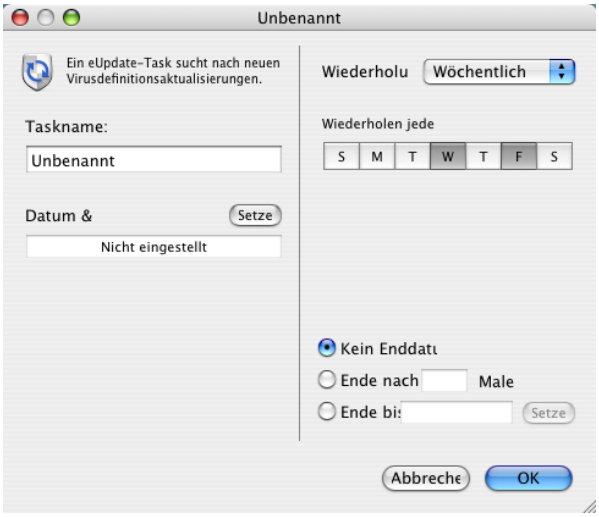
eUpdate ist so eingerichtet, dass es automatisch nach Aktualisierungen sucht. Sie können darüber hinaus eigene eUpdates planen oder die bestehenden Pläne ändern.

So planen Sie ein eUpdate:

1 Wählen Sie im Menü **Darstellung** die Option **Geplante Tasks** aus. Das Dialogfeld **VirusScan Schedule Editor** wird angezeigt.

2 Klicken Sie auf **Neuer eUpdate-Task**. Ein Fenster **Ohne Titel** wird angezeigt.

Abbildung 3-6 Dialogfeld „Neues eUpdate“



3 Geben Sie einen Namen für den Task ein. Es wird empfohlen, einen Namen zu verwenden, der den geplanten Task beschreibt.

4 Klicken Sie auf **Setzen**, um **Datum & Uhrzeit** für die Aktualisierung anzugeben.

5 Wählen Sie **Wiederholung**. Folgende Optionen stehen zur Auswahl:

- **Täglich**: Geben Sie das Tagesintervall für die Ausführung von eUpdate an.
- **Wöchentlich**: Wählen Sie aus, an welchen Tagen der Woche das eUpdate durchgeführt werden soll.
- **Monatlich**: Wählen Sie aus, an welchen Tagen des Monats und an welchen Monaten eine automatische Aktualisierung stattfinden soll.
- **Nie**: Wählen Sie diese Option, wenn keine automatische Aktualisierung stattfinden soll.

6 Wählen Sie ein Enddatum aus, und klicken Sie auf **OK**.

Der neue eUpdate-Task wird in einer Liste mit allen geplanten Scans und eUpdates in VirusScan Schedule Editor angezeigt. Um eUpdate-Tasks zu aktivieren oder zu deaktivieren, aktivieren Sie das Kontrollkästchen neben dem entsprechenden Task. eUpdate startet automatisch, wenn eine Aktualisierung verfügbar ist.

So starten Sie ein nicht geplantes eUpdate:

1. Öffnen Sie die VirusScan-Konsole.
2. Klicken Sie auf die Registerkarte **eUpdate**, um zum eUpdate-Fenster zu wechseln.
3. Klicken Sie auf **Starten**, um zu prüfen, ob neue Virusdefinitionen zum Download bereitstehen.

4 Integration mit ePolicy Orchestrator 3.6

Einführung

In diesem Abschnitt wird die Konfiguration von VirusScan for Mac mithilfe der McAfee ePolicy Orchestrator-Verwaltungssoftware (Version 3.5 bzw. 3.6) erläutert. Um dieses Handbuch effizient verwenden zu können, müssen Sie mit ePolicy Orchestrator vertraut sein. Weitere Informationen finden Sie in den *ePolicy Orchestrator-Produkthandbüchern*. Mit der ePolicy Orchestrator-Software können Sie Ihre McAfee-Antivirenprodukte zentral steuern und so Antivirenrichtlinien verwalten sowie Berichte über Antivirenereignisse und Virusaktivitäten in einer Unternehmensumgebung anzeigen. Mithilfe von ePolicy Orchestrator können Sie VirusScan for Mac auf allen Zielcomputern im gesamten Netzwerk konfigurieren. Sie müssen sie also nicht alle einzeln konfigurieren.

Dieser Abschnitt enthält die folgenden Informationen:

- Hinzufügen der ePolicy Orchestrator-Agentenkonfiguration zum ePolicy Orchestrator-Server
- Festlegen der Antivirenrichtlinien auf den Zielsystemen zum Konfigurieren der folgenden VirusScan for Mac-Funktionen:
  - Allgemeine Richtlinien zum Steuern der allgemeinen VirusScan for Mac-Funktionen
  - eUpdate-Serverrichtlinien
  - Richtlinien für Scanner auf Anforderung
  - Richtlinien für Scanner bei Zugriff
- Konfigurieren der ePolicy Orchestrator-Agentenfunktionen für Macintosh-Computer:
  - Agentenkommunikationsintervall
  - Richtlinienumsetzungsintervall
  - Ereignisweiterleitung
  - Protokollierung.

Dieses Handbuch bietet keine ausführlichen Informationen zum Installieren oder Verwenden der ePolicy Orchestrator-Software. Ziehen Sie die *ePolicy Orchestrator-Produkthandbücher* zurate.

Voraussetzungen für die Verwendung von ePolicy Orchestrator zur Verwaltung von VirusScan for Mac

Erforderliche Schritte vor der Verwendung der ePolicy Orchestrator-Software zur Verwaltung von VirusScan for Mac:

- Checken Sie die entsprechenden Network Associate Package-Dateien (.NAP) für VirusScan for Mac in das ePolicy Orchestrator-Software-Repository ein.
- Checken Sie die Nicht-Windows Agent-Datei (NWA) in das ePolicy Orchestrator-Repository ein.

> Der Nicht-Windows-Agent (NWA) wird auch als ePolicy Orchestrator-Agent für Mac OS X bezeichnet.

- Installieren Sie den ePolicy Orchestrator-Agenten auf dem Macintosh-Computer.

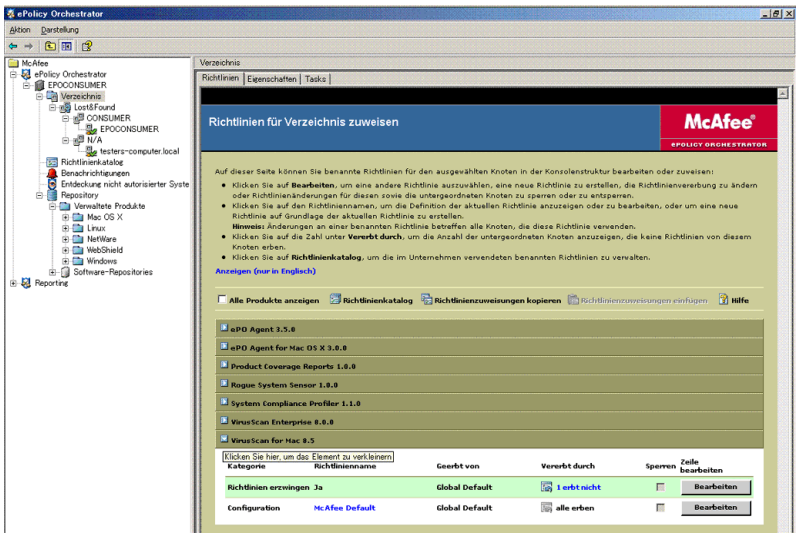
Einführung in die ePolicy Orchestrator-Konsole

Die Microsoft Management Console (MMC) ist Ihre Schnittstelle zum ePolicy Orchestrator-Produkt und seinen Funktionen. Hier registrieren und konfigurieren Sie das VirusScan for Mac-Antivirenprodukt, das über ePolicy Orchestrator verwaltet wird. Die Konsole verwendet MMC-Standardfunktionen.

Die Konsole ist in zwei Bereiche bzw. Fenster unterteilt:

- Die Konsolenstruktur ist das Navigationsfenster der Konsole. Hier werden Server, Arbeitsstationen und Anwendungen angezeigt, die Sie mit ePolicy Orchestrator verwalten können.
- Das Detailfenster befindet sich auf der rechten Seite der Konsole. Je nachdem, welches Element Sie in der Konsolenstruktur ausgewählt haben, verfügt das Detailfenster über ein oberes Detailfenster und ein unteres Detailfenster.

Abbildung 4-1 ePolicy Orchestrator-Konsole



Bei der ersten Anmeldung am Server wird die Konsole mit markiertem **Konsolenstammverzeichnis** im linken Fenster angezeigt.

Je nachdem, welche Elemente Sie in der Konsolenstruktur oder im Detailfenster ausgewählt haben, ändert sich die Anzeige der Konsole.

Ausführliche Informationen zur Verwendung von ePolicy Orchestrator finden Sie in den *ePolicy Orchestrator-Produkthandbüchern*.

Installation

Einführung

Der Nicht-Windows-Agent ist die verteilte Komponente von ePolicy Orchestrator, die auf jedem Macintosh-Computer im Netzwerk installiert werden muss. Der Agent sorgt für die Erfassung und den Austausch von Informationen zwischen dem ePolicy Orchestrator-Server und den Repositories und verwaltet VirusScan-Installationen im gesamten Netzwerk. Von der Konfigurierung des Agenten und seinen Richtlinien hängt es ab, wie er die Kommunikation und Aktualisierung in Ihrer Umgebung unterstützt.

Systemanforderungen

Der Agent kann unter dem Betriebssystem Apple Macintosh OS X (Version 10.4.6 oder höher) sowie auf folgenden Macintosh-Plattformen installiert werden:

- G3
- G4
- G5
- SMP (Dualprozessor)
- Intel-basierter Macintosh-Rechner

Einchecken von NAP-Dateien für die Verwaltung von VirusScan

Um die Verwaltung von VirusScan über ePolicy Orchestrator zu ermöglichen, müssen zunächst die NAP-Dateien des Produkts dem Software-Repository auf dem ePolicy Orchestrator-Server hinzugefügt werden. Die NAP-Dateien enthalten VirusScan-Richtlinienseiten, über die Sie die Produkteinstellungen steuern können, die über den ePolicy Orchestrator-Agenten auf den Clientcomputern ausgebracht werden.

McAfee veröffentlicht NAP-Dateien für alle Antiviren- und Sicherheitsprodukte, die von ePolicy Orchestrator unterstützt werden. Die NAP-Datei eines bestimmten Produkts wird mit den anderen Installationsdateien dieses Produkts zur Verfügung gestellt. Diese Dateien befinden sich entweder auf der Produkt-CD oder in der ZIP-Datei des Produkts, wenn Sie die Installationsdateien von der McAfee-Website heruntergeladen haben. Die NAP-Dateien für VirusScan befinden sich im Unterordner mit den **ePolicy Orchestrator-Serverkomponenten** auf der Produkt-CD bzw. in der ZIP-Datei. Eine NAP-Datei hat immer die Dateierweiterung .NAP und enthält im Namen einen Produktcode und eine Versionsnummer, z. B. NWA-MAC300.NAP.

Richtlinienseiten werden nicht zum Master-Repository hinzugefügt, sondern auf dem ePolicy Orchestrator-Server gespeichert. Aus diesem Grund werden NAP-Dateien nicht auf verteilte Repositories oder aktualisierte Macintosh-Computer repliziert.

Hinzufügen der NAP-Datei (NWA-MAC300.NAP) eines nicht auf Windows basierenden Macintosh-Agenten

So checken Sie die NAP-Datei eines nicht auf Windows basierenden Macintosh-Agenten für den ePolicy Orchestrator-Server ein:

1 Suchen Sie die Datei **NWA-MAC300.NAP** auf der Produkt-CD oder in der ZIP-Installationsdatei, die Sie von der McAfee-Website heruntergeladen haben, und speichern Sie die Datei in einem temporären Ordner, der vom ePolicy Orchestrator-Server aus zugänglich ist.

2 Melden Sie sich als Administrator am ePolicy Orchestrator-Server an.

3 Klicken Sie in der ePolicy Orchestrator-Konsolenstruktur mit der rechten Maustaste auf **Repository**, und wählen Sie **Repository konfigurieren** aus. Der Assistent **Software-Repository konfigurieren** wird angezeigt.

Sie können den Assistenten auch aufrufen, indem Sie in der ePolicy Orchestrator-Konsolenstruktur auf **Repository** doppelklicken und dann im Detailfenster auf **NAP einchecken** klicken.

4 Wählen Sie **Neue zu verwaltende Software hinzufügen** aus, und klicken Sie dann auf **Weiter**.

5 Wählen Sie im Dialogfeld **Ein Softwarepaket wählen** die Datei **NWA-MAC300.NAP** aus, die Sie in Schritt 1 auf Seite 36 in einem temporären Ordner gespeichert haben.

6 Klicken Sie auf **Öffnen**, damit ePolicy Orchestrator die ausgewählte NAP-Datei laden kann.

Hinzufügen einer VirusScan for Mac-NAP-Datei (Virex.nap)

So fügen Sie dem ePolicy Orchestrator-Server die Datei Virex.nap hinzu:

1 Suchen Sie die Datei **Virex.nap** auf der Produkt-CD oder in der ZIP-Installationsdatei, die Sie von der McAfee-Website heruntergeladen haben, und speichern Sie die Datei in einem temporären Ordner, der vom ePolicy Orchestrator-Server aus zugänglich ist.

2 Melden Sie sich als Administrator am ePolicy Orchestrator-Server an.

3 Klicken Sie in der ePolicy Orchestrator-Konsolenstruktur mit der rechten Maustaste auf **Repository**, und wählen Sie **Repository konfigurieren** aus. Der Assistent **Software-Repository konfigurieren** wird angezeigt.

4 Wählen Sie **Neue zu verwaltende Software hinzufügen** aus, und klicken Sie dann auf **Weiter**.

5 Wählen Sie im Dialogfeld **Ein Softwarepaket wählen** die Datei **Virex.nap** aus, die Sie in Schritt 1 auf Seite 36 in einem temporären Ordner gespeichert haben.

6 Klicken Sie auf **Öffnen**, damit ePolicy Orchestrator die ausgewählte NAP-Datei laden kann.

Hinzufügen einer VirusScan for Mac-NAP-Berichtsdatei (virexExt.nap)

So fügen Sie dem ePolicy Orchestrator-Server die Datei virexExt.nap hinzu:

1 Suchen Sie die Datei **virexExt.nap** auf der Produkt-CD oder in der ZIP-Installationsdatei, die Sie von der McAfee-Website heruntergeladen haben, und speichern Sie die Datei in einem temporären Ordner, der vom ePolicy Orchestrator-Server aus zugänglich ist.

2 Melden Sie sich als Administrator am ePolicy Orchestrator-Server an.

3 Klicken Sie in der ePolicy Orchestrator-Konsolenstruktur mit der rechten Maustaste auf **Repository**, und wählen Sie **Repository konfigurieren** aus. Der Assistent **Software-Repository konfigurieren** wird angezeigt.

4 Wählen Sie **Neue Berichte hinzufügen**, und klicken Sie auf **Weiter**.

5 Wählen Sie im Dialogfeld **Ein Softwarepaket wählen** die Datei **virexExt.nap** aus, die Sie in Schritt 1 im Abschnitt *Hinzufügen einer VirusScan for Mac-NAP-Berichtsdatei (virexExt.nap)* in einem temporären Ordner gespeichert haben, und klicken Sie dann auf **Öffnen**, damit ePolicy Orchestrator die NAP-Berichtsdatei in das Repository laden kann.

Nachdem ePolicy Orchestrator sämtliche NAP-Dateien geladen hat, wird der Agent in der Richtlinienliste im Detailfenster angezeigt.

Installieren des ePolicy Orchestrator-Agenten für Macintosh-Computer

Der ePolicy Orchestrator-Agent für Macintosh-Computer kann entweder im Rahmen einer Standardinstallation (grafische Benutzeroberfläche) oder über die Befehlszeile (Hintergrundinstallation) installiert werden. Der Agent wird im Verzeichnis `/Library/NETAepoagt` installiert. Konfigurationsbezogene Daten werden im Verzeichnis `/Library/NETASSOC` gespeichert.

Sie können das Installationsverzeichnis des ePolicy Orchestrator-Agenten nicht ändern.

Standardinstallation

1 Suchen Sie die Datei **nwa.dmg** auf der Produkt-CD oder in der ZIP-Installationsdatei, die Sie von der McAfee-Website heruntergeladen haben, und speichern Sie die Datei in einem temporären Ordner.

Die Datei **nwa.dmg** befindet sich im Ordner **ePO Agent** der Datei **ePO Components.ZIP** auf der Produkt-CD.

2 Doppelklicken Sie auf die Datei **nwa.dmg**. Daraufhin werden folgende Dateien angezeigt:

- NWA.pkg
- cmdinstall

3 Doppelklicken Sie auf die Datei **NWA.pkg**. Daraufhin wird das Fenster **Willkommen beim Installationsprogramm für den ePO-Agenten für Mac OS X** eingeblendet.

4 Klicken Sie auf **Weiter**. Daraufhin wird das Fenster **ReadMe** angezeigt. Die ReadMe-Datei enthält eine Beschreibung aller Funktionen des Agenten sowie aller bekannten Probleme dieser Agentenversion.

5 Klicken Sie auf **Weiter**. Daraufhin wird das Fenster mit der **Software-Lizenzvereinbarung** eingeblendet.

Lesen und bestätigen Sie die Lizenzvereinbarung. Wenn Sie der Lizenzvereinbarung nicht zustimmen, können Sie nicht mit der Installation fortfahren.

6 Klicken Sie auf **Weiter**. Daraufhin wird das Fenster für die **Zielauswahl** eingeblendet. Wählen Sie das Volume aus, auf dem Sie den ePolicy Orchestrator-Agenten installieren möchten, und klicken Sie auf **Weiter**.

7 Das Fenster **Easy Install** wird angezeigt.

Welche der zwei Varianten dieses Fensters angezeigt wird, hängt davon ab, ob Sie eine Installation/Neuinstallation bzw. eine Aktualisierung des Agenten durchführen. Wenn Sie den Agenten zum ersten Mal installieren bzw. ihn nach der Deinstallation der vorherigen ePolicy Orchestrator-Agenteninstallation erneut installieren, enthält dieses Fenster eine Schaltfläche **Installieren**. Bei der Aktualisierung einer älteren Version des ePolicy Orchestrator-Agenten enthält dieses Fenster eine Schaltfläche mit der Bezeichnung **Upgrade**.

8 Klicken Sie zum Fortfahren auf**Installieren/Upgrade**.

9 Sie müssen Ihre Anmeldeinformationen authentifizieren. Geben Sie Ihr Kennwort ein, und klicken Sie dann auf **OK**. Daraufhin wird das Fenster für die **Installation der Software** eingeblendet.

Während dieses Vorgangs werden Sie vom Installationsprogramm aufgefordert, sich bei **ePO Agent Configurator** zu authentifizieren. Geben Sie Ihr Kennwort ein, und klicken Sie dann auf **OK**. Daraufhin wird das Dialogfeld **ePO Agent Configurator** eingeblendet.

10 Geben Sie die **IP-Adresse des ePO-Servers** und die Nummer des **ePO-Server-Ports** ein. Klicken Sie auf **Anwenden**. Daraufhin wird das Fenster für die **Installation der Software** eingeblendet.

11 Klicken Sie auf **Neu starten**, um den Installationsvorgang anzuschließen.

Hintergrundinstallation (Befehlszeile)

1 Suchen Sie die Datei **nwa.dmg** auf der Produkt-CD oder in der ZIP-Installationsdatei, die Sie von der McAfee-Website heruntergeladen haben, und speichern Sie die Datei in einem temporären Ordner.

Die Datei **nwa.dmg** befindet sich im Ordner **ePO Agent** der Datei **ePO Components.ZIP** auf der Produkt-CD.

2 Doppelklicken Sie auf die Datei **nwa.dmg.** Daraufhin werden folgende Dateien angezeigt:

- NWA.pkg
- cmdinstall

3 Öffnen Sie das **Terminal**-Fenster, und wechseln Sie zum Arbeitsverzeichnis `/Volumes/NAINWA`.

Zur Ausführung dieses Befehls sind Administratorrechte erforderlich.

4 Führen Sie im **Terminal**-Fenster folgenden Befehl aus:
`sudo ./cmdinstall <IP-Adresse des ePO-servers>:<Port des ePO-Servers>`

5 Nach Abschluss der Hintergrundinstallation enthält das **Terminal**-Fenster folgende Meldungen:

Abbildung 4-2 Terminal-Fenster – Installation/Upgrade abgeschlossen

```
installer[661]:                      It took 3.385372 seconds to run preupgrade script for ePO Agent for Mac OS X
installer[661]:                      It took 0.445282 seconds to Write files
installer[661]:                      It took 3.174604 seconds to run postupgrade script for ePO Agent for Mac OS X
installer[661]:                      It took 0.098582 seconds to Assembling receipt
installer[661]:
installer[661]: Summary Information
installer[661]: Type           Elapsed time (sec)
installer[661]:          patch          0.000117
installer[661]:           zero          0.010520
installer[661]:         script          6.559976
installer[661]:        extract          0.445282
installer[661]:         config          0.065356
installer[661]:        receipt          0.433727
installer[661]:           disk          1.006918
installer[661]:        install          7.509475
installer[661]:
installer[661]: Starting installation:
installer[661]: Finalizing installation.
#
installer:     Finishing Installation
installer[661]: Registering applications
installer[661]: Registered /Library/NETAepoagt/bin/ePO Agent Configurator.app.
#
installer:
#
installer: The software was successfully installed.....
installer: The upgrade was successful.
installer: The install recommends restarting now.
Cleaning /tmp/NAINWA.mpnlThby
iMac-Mactel-2:/Volumes/NAINWA shreyas$
```

Sie haben Ihren ePolicy Orchestrator-Agenten für Mac OS X erfolgreich installiert/aktualisiert.

Installieren von VirusScan for Mac

Details zum Installieren der Software auf Macintosh-Computern finden unter *Installieren von VirusScan for Mac* auf Seite 13.

Deinstallation

Entfernen von VirusScan for Mac vom ePolicy Orchestrator-Server

Sie können die VirusScan for Mac-NAP-Datei auf dem ePolicy Orchestrator-Server deinstallieren.

So entfernen Sie die VirusScan for Mac-NAP-Datei:

1. Melden Sie sich am ePolicy Orchestrator-Datenbankserver an.
2. Wählen Sie in der Konsolenstruktur unter **Repository** | **Verwaltete Produkte** | **MAC OS X** | den Eintrag **VirusScan for Mac** aus.
3. Klicken Sie mit der rechten Maustaste auf **VirusScan for Mac**, und wählen Sie dann **Entfernen** aus, um die VirusScan-NAP-Datei auf dem ePolicy Orchestrator-Server zu deinstallieren.

Entfernen des ePolicy Orchestrator-Agenten für Mac OS X vom ePolicy Orchestrator-Server

Nach seinem Einchecken kann der **ePolicy Orchestrator-Agent für MAC OS X** nicht mehr vom ePolicy Orchestrator-Server entfernt werden.

Entfernen des ePolicy Orchestrator-Agenten aus VirusScan for Mac

Der ePolicy Orchestrator-Agent kann auf einem Macintosh-Computer deinstalliert werden.

So deinstallieren Sie den ePolicy Orchestrator-Agenten über die Befehlszeile:

1. Melden Sie sich mit Administratorrechten an.
2. Wechseln Sie zum Verzeichnis `/Library/NETAepoagt`.
3. Führen Sie `cmduninst` aus.

Festlegen von Richtlinien in ePolicy Orchestrator

Über die ePolicy Orchestrator-Konsole können Sie Richtlinien für Gruppen von Computern bzw. für einen Einzelrechner umsetzen. Diese Richtlinien setzen die Konfigurationen einzelner Computer außer Kraft.

Wählen Sie vor der Konfiguration von Richtlinien die Gruppe von Computern aus, für die Sie VirusScan for Mac-Richtlinien ändern möchten. Sie können die VirusScan for Mac-Richtlinien über die Seiten und Registerkarten im Detailfenster der ePolicy Orchestrator-Konsole ändern. Diese Seiten unterscheiden sich nur geringfügig von den Seiten, auf die Sie direkt über die VirusScan for Mac-Benutzeroberfläche zugreifen können.

Nachdem Sie die entsprechenden Richtlinien geändert und die Änderungen für den entsprechenden Computer bzw. die Gruppe von Computern gespeichert haben, können Sie die neuen Einstellungen über den ePolicy Orchestrator-Agenten ausbringen.

So ändern Sie Richtlinien für VirusScan for Mac in ePolicy Orchestrator:

1 Melden Sie sich am ePolicy Orchestrator-Server an.

2 Wählen Sie in der Konsolenstruktur unter **ePolicy Orchestrator** | <**SERVER**> | **Verzeichnis** die Site, die Gruppe, den einzelnen Computer oder das gesamte Verzeichnis aus, für das diese Richtlinien gelten sollen. Die Registerkarten **Richtlinien**, **Eigenschaften** und **Tasks** werden im Detailfenster angezeigt.

3 Aktivieren Sie im Detailfenster die Registerkarte **Richtlinien**, und erweitern Sie dann den Eintrag **VirusScan for Mac 8.6**. Unterhalb des Eintrags **VirusScan for Mac 8.6** wird **Umsetzen von Richtlinien** und **VirusScan-Richtlinien** angezeigt.

4 Klicken Sie unterhalb von **Richtlinienname** unter **Kategorie** auf **McAfee-Standard**, um die standardmäßigen Richtlinieneinstellungen anzuzeigen.

Die Konfiguration der Richtlinieneinstellungen **McAfee-Standard** für eine ausgewählte **Kategorie** ist nicht möglich. Wenn Sie eine ausgewählte Kategorie konfigurieren möchten, *müssen* Sie für die ausgewählte **Kategorie** eine neue Richtlinie erstellen.

So erstellen Sie eine neue Richtlinie für eine Kategorie:

1 Klicken Sie im ePolicy Orchestrator-Detailfenster unter **VirusScan for Mac 8.6** für eine **Kategorie** auf die Option **Bearbeiten**.

2 Klicken Sie auf die Dropdown-Liste **Richtlinienname**, und wählen Sie **Neue Richtlinie** aus. Daraufhin wird das Dialogfeld **Neue Richtlinie erstellen** angezeigt.

Neue Richtlinie erstellen – Optionen

Folgende Richtlinie duplizieren	Erstellt ein Richtlinienduplikat für die ausgewählte **Kategorie**. Wählen Sie die Richtlinie in der Dropdown-Liste aus.
Richtlinie erstellen, in der alle Registerkarten übernehmen	Erstellt eine neue Richtlinie, in der sämtliche Einstellungen der Registerkarte „Richtlinie“ übernommen werden.
Neuer Richtlinienname	Geben Sie den neuen Richtlinienamen für die **Kategorie** ein, die Sie erstellen möchten.

3 Konfigurieren Sie die erforderlichen Optionen der ursprünglichen Richtlinie, und klicken Sie dann auf **OK**, um die neue Richtlinie zu erstellen.

4 Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

So bearbeiten Sie eine bestehende Richtlinie:

1 Klicken Sie im ePolicy Orchestrator-Detailfenster unter **VirusScan for Mac 8.6** für die ausgewählte **Kategorie** auf  .

2 Konfigurieren Sie die erforderlichen Optionen, und klicken Sie dann zum Speichern der Richtlinie auf **Anwenden**.

So setzen Sie Richtlinien um:

1 Klicken Sie in ePolicy Orchestrator unterhalb des VirusScan for Mac-Eintrags für **Umsetzen von Richtlinien** auf die Option **Bearbeiten**.

2 Klicken Sie auf die Dropdown-Liste **Richtlinienname**, und wählen Sie **Ja**.

3 Klicken Sie auf **Anwenden**, um die soeben konfigurierten Richtlinien umzusetzen.

Registerkarte „Allgemein“

Über die Registerkarte **Allgemein** können allgemeine Richtlinien umgesetzt werden, mit denen die allgemeine Funktionsweise von VirusScan for Mac gesteuert wird. So können beispielsweise automatisch Aktualisierungen von Virusdefinitionen gesucht, Scans bei Zugriff durchgeführt, Scanergebnisse protokolliert sowie Ausschlusslisten für bestimmte Datenträger, Dateien und Ordner erstellt werden.

Folgende allgemeine Richtlinien können umgesetzt werden:

Automatisch nach Virusdefinitionsaktualisierungen suchen	Aktiviert bzw. deaktiviert automatische eUpdates.
Scan bei Zugriff	Aktiviert/deaktiviert das Scannen bei Zugriff.
Ergebnisse in Datei protokollieren	Aktiviert bzw. deaktiviert die Protokollierung der Ergebnisse in einer Datei.
Bestimmte Datenträger, Dateien und Ordner ausschließen	Schließt die hier aufgeführten Elemente vom Scannen aus. Wenn diese Option nicht aktiviert ist, ignoriert der Scanner die Ausschlussliste. Ausschluss hinzufügen: ■ Klicken Sie auf **Hinzufügen**. Daraufhin wird das Dialogfeld **Scanelement hinzufügen – Webseite** angezeigt. Geben Sie den vollständigen Pfad der Datei, des Verzeichnisses oder des Datenträgers ein, die Sie ausschließen möchten, und klicken Sie auf **OK**. Die Ausnahmen werden in der **Ausschlussliste** aufgeführt. Ausschluss entfernen: ■ Wählen Sie die Ausnahme in der **Ausschlussliste** aus, und klicken Sie auf **Entfernen**. Ausschluss bearbeiten: ■ Wählen Sie die Ausnahme in der **Ausschlussliste** aus, und klicken Sie auf **Bearbeiten**.

Registerkarte „eUpdate“

Mithilfe der Registerkarte **eUpdate** können Sie die Aktualisierungseinstellungen der DAT-Dateien und des Scanmoduls an Ihre Erfordernisse anpassen. eUpdate sorgt dafür, dass Ihre Antivirensoftware ständig mit Informationen zu Viren und mit Scanfunktionen aktualisiert wird. Sie können Ihre DAT- und Moduldateien über FTP (File Transfer Protocol) aktualisieren.

Anpassen von eUpdate-Einstellungen

Beim Aktualisieren Ihrer DAT- und Moduldateien müssen Sie die Details des Servers angeben, von dem die Aktualisierungsdateien übertragen werden sollen.

Server-URL	Der Server-URL zum Herunterladen von DAT- und Modulaktualisierungen.
Port	Die Port-Nummer, die Sie für FTP verwenden möchten.
Benutzername	Ihr Benutzername.
Kennwort	Ihr Kennwort.
Konto	Ihr FTP-Konto.
Verzeichnis	Der Pfad zu Ihren DAT- und Moduldateien.

Registerkarte „Scanner bei Zugriff“

Über die Registerkarte „Scanner bei Zugriff“ können alle derzeit verwendeten Dateien automatisch gescannt werden, um zu ermitteln, ob ein Virus oder eine andere Art von Malware vorliegt. Ein Scan wird immer dann durchgeführt, wenn eine Datei vom Datenträger gelesen und/oder durch einen vom Benutzer oder vom System initiierten Vorgang auf den Datenträger geschrieben wird. Der Scanner bei Zugriff ermöglicht die kontinuierliche Richtlinienumsetzung für mehrere Dateien, Verzeichnisse oder Volumes. Dies beinhaltet auch Volumes auf Remote-Computern, zu denen eine Netzwerkverbindung besteht. Sie können festlegen, wonach der Scanner sucht und wie er auf infizierte Dateien reagiert. Wenn ein Virus oder eine andere Form von Malware gefunden wird, wird auf dem Macintosh-Computer im Popup-Fenster **Reporter** eine Benachrichtigung angezeigt.

Folgende Richtlinien für den Scanner bei Zugriff können umgesetzt werden:

Inhalte von Archiven und komprimierten Dateien scannen	Legt fest, dass der Scanner Archive und andere komprimierte Dateien scannt. Diese Funktion ist für den Scanner bei Zugriff standardmäßig deaktiviert. Beachten Sie, dass der Scanner bei Zugriff keine Stuffit-Archive überprüft.
Unbekannte Makroviren suchen	Wenn eine Datei ein potenziell infiziertes Makro (unbekannte Infektionen) enthält, wird die Datei im Rahmen der Säuberung gescannt und gesäubert/gelöscht.
Apple-Mail-Nachrichten scannen	Legt fest, dass der Scanner Apple-Mail-Nachrichten überprüft.
Dateien auf virenähnliche Charakteristiken überprüfen	Mithilfe dieser Option können Sie heuristische Aktivitäten aktivieren bzw. deaktivieren, die nach Dateien suchen, die virus- oder wurmähnliche Eigenschaften aufweisen und unbekannte Infektionen enthalten können.
Potenziell unerwünschte Anwendungen und Scherzprogramme suchen	Aktiviert/deaktiviert die Suche des Scanners nach unerwünschten Anwendungen oder Scherzprogrammen.
Ablagen auf Netzwerk-Volumes scannen	Legt fest, dass der Scanner Dateien auf Netzwerk-Volumes überprüft.
Ablagen scannen: ■ Immer ■ Lesen ■ Schreiben	Bestimmt, ob der Scanner Dateien überprüfen soll, die vom Datenträger gelesen bzw. auf den Datenträger geschrieben werden bzw. für die beides zutrifft. Die Standardeinstellung lautet **Immer**. Dateien, die auf den Datenträger geschrieben bzw. vom Datenträger gelesen werden, werden also gescannt.
Wenn ein Virus gefunden wird: ■ Säubern ■ Löschen ■ Benachrichtigen	Wählt die primäre Aktion des Scanners bei Zugriff für den Fall aus, dass ein Virus gefunden wird.
Löschen, wenn Säuberung fehlschlägt oder nicht verfügbar ist	Wählt die sekundäre Aktion des Scanners bei Zugriff für den Fall aus, dass ein Virus gefunden wird. Diese Option ist nur verfügbar, wenn **Säubern** als primäre Aktion festgelegt wurde.
Maximale Scan-Zeit	Die maximale Dauer (in Sekunden) für einen Scan einer Datei. (Eine komprimierte Datei wird nicht als eine Datei interpretiert. Dieses Zeitlimit gilt für die letzte Einzeldatei und nicht für die letzte Container-Datei der höchsten Ebene.)

Registerkarte „Scanner auf Anforderung“

Über die Registerkarte „Scanner auf Anforderung“ können Sie jederzeit einen Scanvorgang starten, indem Sie ausgewählte Dateien in die Konsole ziehen und dort ablegen. Sie können hierzu auch auf **Datei** und dann auf **Öffnen** klicken. Mithilfe des Scanners auf Anforderung können Sie mehrere Dateien, Verzeichnisse oder Volumes auswählen. Die Scanergebnisse werden in einem Bericht angezeigt, der gesichert oder gedruckt werden kann. Sie können festlegen, wonach der Scanner sucht und wie er auf infizierte Dateien reagiert. Der Scanner benachrichtigt Sie, wenn er einen Virus findet und generiert ein Protokoll, in dem die durchgeführten Aktionen aufgezeichnet werden.

Sie können folgende Richtlinien für den Scanner auf Anforderung umsetzen:

Inhalte von Archiven und komprimierten Dateien scannen	Legt fest, dass der Scanner Archive und andere komprimierte Dateien scannt. Diese Funktion ist für den Scanner auf Anforderung standardmäßig aktiviert.
Unbekannte Makroviren suchen	Wenn eine Datei ein potenziell infiziertes Makro (unbekannte Infektionen) enthält, wird die Datei im Rahmen der Säuberung gescannt und gesäubert/gelöscht.
Apple-Mail-Nachrichten scannen	Legt fest, dass der Scanner Apple-Mail-Nachrichten überprüft.
Dateien auf virenähnliche Charakteristiken überprüfen	Mithilfe dieser Option können Sie heuristische Aktivitäten aktivieren bzw. deaktivieren, die nach Dateien suchen, die virus- oder wurmähnliche Eigenschaften aufweisen und unbekannte Infektionen enthalten können.
Potenziell unerwünschte Anwendungen und Scherzprogramme suchen	Aktiviert/deaktiviert die Suche des Scanners nach unerwünschten Anwendungen oder Scherzprogrammen.
Wenn ein Virus gefunden wird: ■ Säubern ■ Löschen ■ Benachrichtigen	Wählt die primäre Aktion des Scanners bei Zugriff für den Fall aus, dass ein Virus gefunden wird.
Löschen, wenn Säuberung fehlschlägt oder nicht verfügbar ist	Wählt die sekundäre Aktion des ausgewählten Scanners bei Zugriff für den Fall aus, dass ein Virus gefunden wird. Diese Option ist nur verfügbar, wenn **Säubern** als primäre Aktion festgelegt wurde.

Planen von Scans und eUpdates

Wenn VirusScan for Mac einen Virenscan durchführt, verwendet das Programm Informationen aus den DAT-Dateien, um Viren zu suchen und zu entfernen. Jeden Tag werden viele neue Viren entdeckt, und McAfee erstellt regelmäßig neue DAT-Dateien, um einen Schutz vor diesen Viren bereitzustellen. Um den besten Antivirenschutz zu gewährleisten, können Sie VirusScan for Mac mithilfe von ePolicy Orchestrator darüber informieren, wo die aktuellsten DAT-Dateien zu finden sind. Außerdem können Sie mit ePolicy Orchestrator Pläne für das Ersetzen älterer DAT-Dateien und das Ausführen von Scans auf Anforderung erstellen.

Mit ePolicy Orchestrator können Sie die folgenden geplanten Tasks für die VirusScan for Mac-Software erstellen:

- Scan auf Anforderung
- eUpdate

Geplante Tasks für einen Computer können so festgelegt werden, dass sie in Übereinstimmung mit der Ortszeit oder mit GMT (Greenwich Mean Time) ausgeführt werden. Der Fortschritt eines geplanten Tasks kann jedoch von ePolicy Orchestrator nicht überwacht werden. Daher sollten Sie die Protokolldatei auf dem Server in regelmäßigen Abständen aufrufen, um zu überprüfen, ob der Task erfolgreich ausgeführt wurde.

Scans auf Anforderung

VirusScan for Mac kann Ihre Dateien auf Anforderung scannen. Hierbei werden sämtliche Dateien auf Ihrem Computer auf Viren, Trojaner und andere Arten von Malware geprüft. Sie können beliebig viele Pläne für Scans auf Anforderung erstellen. Die geplanten Scans können so konfiguriert werden, dass sie in bestimmten Intervallen durchgeführt werden und jederzeit vom Benutzer ausgeführt werden können. Sie können zudem Pläne deaktivieren, die nicht automatisch ausgeführt werden sollen.

Erstellen eines neuen Tasks

1. Klicken Sie im oberen Detailfenster auf die Registerkarte **Tasks**. Klicken Sie mit der rechten Maustaste in dieses Fenster, und wählen Sie die Option **Task planen** aus.
2. Geben Sie einen Namen für den Task im Feld **Name des neuen Tasks** ein, und wählen Sie den Task aus, den Sie erstellen möchten.
3. Wählen Sie in der Dropdown-Liste **Task-Typ** die Option für den Scan auf Anforderung (On-Demand Scan, ODS) aus. Klicken Sie auf **OK**.

   Der erstellte Task wird auf der Registerkarte **Tasks** aufgeführt.

Bearbeiten eines Tasks

1 Klicken Sie mit der rechten Maustaste auf den Task, und wählen Sie die Option **Task bearbeiten** aus.

2 Klicken Sie auf **Einstellungen**. Daraufhin wird die Seite **Ort** angezeigt, über die Sie Dateien und Verzeichnisse in den geplanten Scan einbeziehen können.

Diese Dateien und Verzeichnisse in den Scan einbeziehen	Konfigurieren Sie die Elemente, die gescannt werden sollen. Aufnahme hinzufügen: ■ Klicken Sie auf **Hinzufügen**. Daraufhin wird das Dialogfeld **Scanelement hinzufügen – Webseite** angezeigt. Geben Sie den vollständigen Pfad der Datei, des Verzeichnisses oder des Datenträgers ein, die Sie einbeziehen möchten, und klicken Sie auf **OK**. Die Aufnahme wird in der **Aufnahmeliste** aufgeführt. Aufnahme entfernen: ■ Wählen Sie die Aufnahme in der **Ausschlussliste** aus, und klicken Sie auf **Entfernen**. Aufnahme bearbeiten: ■ Wählen Sie die Aufnahme in der **Aufnahmeliste** aus, und klicken Sie auf **Bearbeiten**. Ändern Sie im Dialogfeld **Scanelement hinzufügen – Webseite** den gesamten Pfad der Datei oder des Verzeichnisses, das Sie in den Scan einbeziehen möchten, und klicken Sie dann auf **OK**.

Planungseinstellungen

3 Deaktivieren Sie **Übernehmen**, um die Einstellungen im Fenster **Planungseinstellungen** zu aktivieren.

Aktivieren (der geplante Task wird zur festgelegten Zeit ausgeführt)	Wählen Sie diese Option aus, um einen Task zu einer bestimmten Uhrzeit auszuführen.
Task stoppen nach:	Geben Sie an, wie lange der Task ausgeführt werden kann, bevor er abgebrochen wird (in Stunden und Minuten).

4 Klicken Sie auf die Registerkarte **Plan**, um folgende Optionen aufzurufen:

Task planen	Wählen Sie einen der verfügbaren Task-Typen in der Dropdown-Liste aus: ■ Täglich ■ Wöchentlich ■ Monatlich ■ Einmal ■ Beim Systemstart ■ Sofort ausführen
Anfangszeit ■ UTC-Zeit ■ Ortszeit	Legen Sie die Anfangszeit für den geplanten Task fest. Wählen Sie die Option für die Ortszeit aus, um den Task im geplanten Intervall gemäß der Systemzeit des Clientcomputers auszuführen. Diese Option ist nützlich, um prozessorintensive Tasks (z. B. Scans auf Anforderung) so zu planen, dass sie außerhalb der Geschäftszeiten ausgeführt werden. Wenn Sie die Option „UTC-Zeit“ (Universal Time Conversion) auswählen, wird der Task zu der entsprechenden GMT-Uhrzeit (Greenwich Mean Time) ausgeführt. Diese Option sorgt dafür, dass der Task auf allen Ihren Macintosh-Clients zur selben Zeit ausgeführt wird, unabhängig von der Ortszeit des Macintosh-Systems.

Zufallsausführung aktivieren	Der Task wird nicht genau zur festgelegten Anfangszeit ausgeführt, sondern nach einer beliebigen, festgelegten Zeit. Legen Sie die Stunden und Minuten fest, um die Zufallsausführung zu aktivieren.
Verpassten Task ausführen	Stellt sicher, dass der Task gestartet wird, wenn der Macintosh-Computer heruntergefahren wurde oder aus einem anderen Grund zur geplanten Anfangzeit nicht verfügbar war. Durch Auswahl dieser Option wird sichergestellt, dass der Task ausgeführt wird, wenn der Macintosh-Computer das nächste Mal verfügbar ist.
Verpassten Task verschieben um	Klicken Sie im Dialogfeld **Erweiterte Zeitplanoptionen** auf **Erweitert**. Wenn Sie ausgelassene Tasks ausführen und diese Option auswählen, wird der ausgelassene Task mit Verzögerung ausgeführt, nachdem der Macintosh-Computer wieder verfügbar ist.
Anfangsdatum / Enddatum	Klicken Sie im Dialogfeld **Erweiterte Zeitplanoptionen** auf **Erweitert**. Geben Sie ein Start- und Enddatum ein, wenn der Task nur für einen bestimmten Zeitraum, etwa einige Tage oder Wochen, ausgeführt werden soll.
Task wiederholen	Klicken Sie im Dialogfeld **Erweiterte Zeitplanoptionen** auf **Erweitert**. Verwenden Sie diese Option, um einen Task am selben Tag mehrfach auszuführen. Wählen Sie dazu die Option **Task wiederholen** aus, und legen Sie das entsprechende Wiederholungsintervall fest. Im Normalfall wird diese Option dazu verwendet, um einen Clientaktualisierungstask mehrere Male am Tag auszuführen, insbesondere dann, wenn es zahlreiche neue Viren gibt. Sie können den Task auch so planen, dass er in anderen Intervalle, z. B. wöchentlichen oder monatlichen Intervallen, wiederholt wird.
Task täglich planen	Geben Sie das Intervall für die Ausführung des geplanten Tasks an. Hierbei kann es sich um ein Intervall von einem oder mehreren Tagen handeln. Wenn Sie „1“ auswählen, wird der geplante Task jeden zweiten Tag ausgeführt.

Löschen eines Tasks

- Klicken Sie im Fenster **Tasks** mit der rechten Maustaste auf den Task, und wählen Sie **Löschen** aus.

eUpdate

Ihre Antivirensoftware kann Sie nur dann umfassend schützen, wenn sie laufend mit den aktuellsten DAT-Dateien und Scanmodulen aktualisiert wird. Wir empfehlen, DAT-Dateien täglich zu aktualisieren und auf der McAfee Avert Labs-Website regelmäßig nach neuen DAT-Dateien zu suchen. Wenn Sie in der aktuellen Domäne über mehrere Server verfügen (die alle VirusScan for Mac ausführen), können Sie einen Server zum Herunterladen der aktuellen DAT-Dateien verwenden und anschließend die anderen Server so konfigurieren, dass sie die Dateien von diesem Server kopieren. Ihre Server können Dateien für verschiedene Betriebssysteme herunterladen, unabhängig davon, welches Betriebssystem Sie gerade verwenden.

Angeben des Speicherorts der DAT-Dateien

Sie können die Quelle der DAT-Dateien über die Registerkarte **eUpdate** angeben.

Erstellen eines eUpdate-Tasks

1 Klicken Sie in der Konsolenstruktur unter **ePolicy Orchestrator** mit der rechten Maustaste auf **Verzeichnis** bzw. auf die Site, die Gruppe oder den Host, und wählen Sie anschließend **Task planen** aus. Das Dialogfeld **Task planen** wird geöffnet.

2 Geben Sie im Feld **Name des neuen Tasks** einen Namen ein.

3 Wählen Sie in der Liste **Software/Task-Typ** die Option **VirusScan for Mac 8.6 - Aktualisierung** aus.

4 Klicken Sie auf **OK**, um den Task zu erstellen.

Konfigurieren eines eUpdate-Tasks

Nachdem Sie einen neuen eUpdate-Task erstellt haben, können Sie den Task nach Bedarf konfigurieren.

1 Klicken Sie auf der Registerkarte **Tasks** im oberen Detailfenster mit der rechten Maustaste auf den Task, und wählen Sie anschließend **Task bearbeiten** aus. Das Dialogfeld **ePolicy Orchestrator Scheduler** wird angezeigt.

2 Klicken Sie auf **Einstellungen**, und bearbeiten Sie die erforderlichen Optionen sowohl auf der Registerkarte **Task** als auch auf der Registerkarte **Zeitplan**.

3 Deaktivieren Sie **Übernehmen**.

4 Wählen Sie **eUpdate ausführen** und dann **Übernehmen** aus.

5 Klicken Sie auf **OK**, um zum Dialogfeld **ePolicy Orchestrator Scheduler** zurückzukehren.

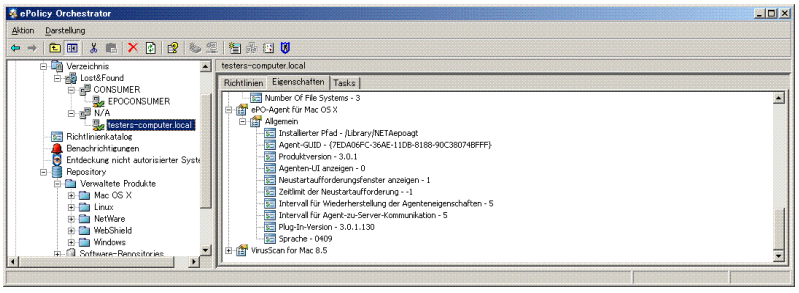
Anzeigender ePolicy Orchestrator-Eigenschaften

Auf dem ePolicy Orchestrator-Server können Sie verschiedene Systemeigenschaften anzeigen.

So zeigen Sie die Eigenschaften an:

1 Wählen Sie in der Konsolenstruktur den Server aus, dessen Einstellungen angezeigt werden sollen.

Abbildung 4-3 Systemeigenschaften



2 Klicken Sie im oberen Detailfenster auf die Registerkarte **Eigenschaften**.

3 Erweitern Sie im Fenster **Eigenschaften** die **VirusScan for Mac**-Strukturansicht, um die verschiedenen Eigenschaften aufzulisten.

4 Klicken Sie auf das **+** neben einer Eigenschaft, um ihre Details anzuzeigen.

Berichte

Über die ePolicy Orchestrator-Konsole können Sie die Konfiguration der Hosts überprüfen und Berichte darüber anzeigen, wie die VirusScan for Mac-Hosts Infektionen bekämpfen. Außerdem können Sie mit den Daten aus der ausgewählten ePolicy Orchestrator-Datenbank, die vom Nicht-Windows-Agenten übermittelt werden, Berichte erstellen. Sie können die Auswahl, die Sie in den Dialogfeldern **Berichtinformationen eingeben** und **Berichtdatenfilter** treffen, für die zukünftige Verwendung speichern.

Sämtliche VirusScan for Mac-Berichte sind unter der Überschrift **Antiviren** zusammengefasst.

Die Berichtfunktion von ePolicy Orchestrator ermöglicht Ihnen Folgendes:

- Legen Sie einen Verzeichnisfilter fest, um nur die Informationen abzurufen, die Sie anzeigen möchten. Beim Festlegen dieses Filters können Sie wählen, welcher Teil der ePolicy Orchestrator-Konsolenstruktur in den Bericht aufgenommen werden soll.
- Legen Sie mithilfe logischer Operatoren einen Datenfilter fest, um exakte Filter für die Daten zu definieren, die im Bericht erfasst werden sollen.
- Erstellen Sie grafische Berichte mit den Informationen in der Datenbank, und filtern Sie die Berichte nach Bedarf. Sie können die Berichte ausdrucken und für die Verwendung in einer anderen Software exportieren.
- Führen Sie Abfragen von Computern, Ereignissen und Installationen durch.

So führen Sie einen Bericht aus:

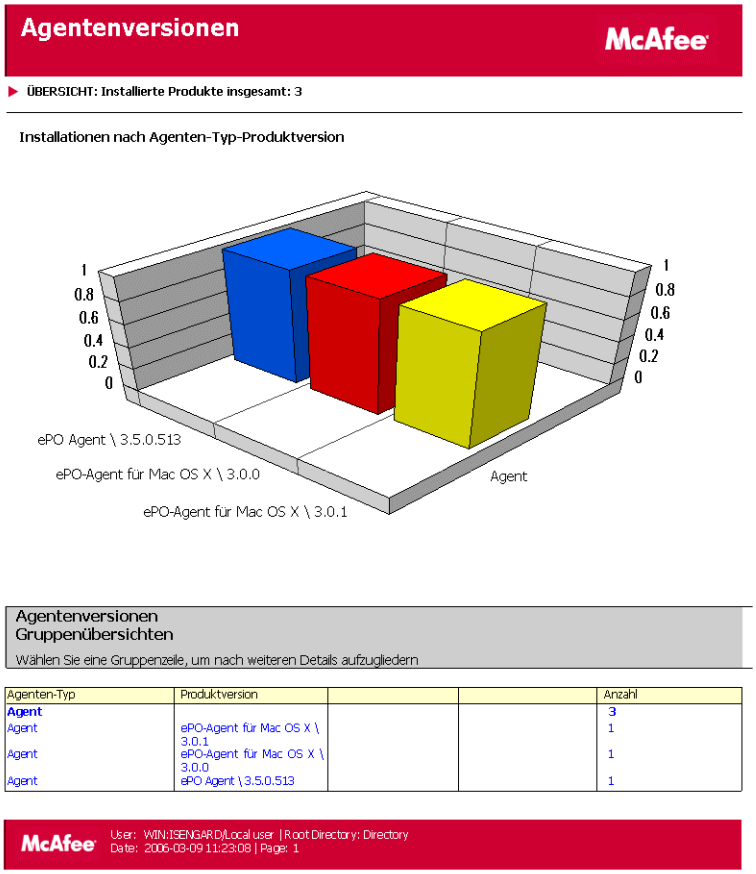
1. Melden Sie sich am ePolicy Orchestrator-Datenbankserver an.
2. Wählen Sie den entsprechenden VirusScan for Mac-Bericht in der Konsolenstruktur unter **Berichterstellung** | **ePO-Datenbanken** | <**Datenbankserver**> | **Berichte** | <**Berichtsgruppe**> aus.
   - Wenn das Dialogfeld **Aktuelle Sicherheitsstandards** angezeigt wird, geben Sie die Version der Virusdefinitionsdateien oder des Scanmoduls ein, für das der Bericht erstellt werden soll.
   - Wenn das Dialogfeld **Berichtinformationen eingeben** angezeigt wird, treffen Sie auf allen angezeigten Registerkarten eine Auswahl: **Regeln, Layout, Datengruppierung, Innerhalb, Gesicherte Einstellungen**.

   In Abhängigkeit vom ausgewählten Bericht können die Registerkarten variieren. Weitere Informationen zu allen verfügbaren Registerkarten mit Einstellungen finden Sie in den *ePolicy Orchestrator-Produkthandbüchern*.

3. Wählen Sie den Bericht (**Agentenversionen**) aus, den Sie generieren möchten, und legen Sie den Datenfilter im Dialogfeld **Berichtdatenfilter** fest. Klicken Sie auf **OK**.

4 Daraufhin wird ein Bericht für **Agentenversionen** generiert.

Abbildung 4-4 Beispielbericht – Agentenversionen



Konfigurieren von Berichten

Sie haben verschiedene Möglichkeiten, festzulegen, welche Daten in einem Bericht erfasst werden sollen. Sie können die Versionsnummer der Virusdefinitionsdateien, der Scanmodule und der unterstützten Produkte definieren, die auf den Macintosh-Clientcomputern installiert werden müssen, damit sie mit dem Antiviren- und Sicherheitsprogramm Ihres Unternehmens kompatibel sind. Außerdem können Sie die Ergebnisse der Berichte durch ausgewählte Produktkriterien einschränken (z. B. Computername, Betriebssystem, Virusname oder für infizierte Dateien ausgeführte Aktion).

Nachdem das Ergebnis eines Berichts angezeigt wird, können Sie verschiedene Tasks ausführen. Sie können Details zu erforderlichen Berichtsdaten anzeigen, um beispielsweise zu ermitteln, auf welchen Macintosh-Clientcomputern keine kompatible Version von VirusScan for Mac installiert ist. Einige Berichte bieten sogar Links zu anderen Berichten. Diese sogenannten Unterberichte enthalten Daten, die mit dem aktuellen Bericht verwandt sind. Außerdem können Sie Berichte und Berichtdaten in verschiedenen Dateiformaten (einschließlich HTML und Microsoft Excel) drucken oder exportieren.

5 Integration mit ePolicy Orchestrator 4.0

Einführung

In diesem Kapitel wird die Konfiguration von VirusScan mit der McAfee-Verwaltungssoftware ePolicy Orchestrator Version 4.0 beschrieben. Um dieses Kapitel effizient verwenden zu können, sollten Sie mit ePolicy Orchestrator 4.0 vertraut sein.

ePolicy Orchestrator 4.0 bietet eine skalierbare Plattform zur zentralen Verwaltung und Umsetzung von Richtlinien für Ihre Sicherheitsprodukte und die Systeme, auf denen sie vorhanden sind. Außerdem bietet es umfassende Berichtsoptionen und Möglichkeiten zur Produktbereitstellung, die alle zentral gesteuert werden können.

Dieses Handbuch bietet keine ausführlichen Informationen zum Installieren oder Verwenden der ePolicy Orchestrator-Software. Diese Informationen finden Sie im *Produkthandbuch zu ePolicy Orchestrator 4.0*.

Erweiterungen

VirusScan-Erweiterungen werden mit ePolicy Orchestrator 4.0 vorinstalliert. Sie können VirusScan-Erweiterungsdateien installieren, entfernen und verwalten. Erweiterungsdateien befinden sich in ZIP-Dateien und müssen installiert werden, bevor das Produkt oder die Komponente über ePolicy Orchestrator 4.0 verwaltet werden kann.

Wenn Sie VirusScan-Erweiterungen deinstallieren, sind die Erweiterungen unter **Programme** | **McAfee** | **ePolicyOrchestrator** | **Erweiterungen** verfügbar.

Für VirusScan sind die folgenden zwei Erweiterungsdateien verfügbar:

- **VSCANMAC8600.ZIP**
- **VIREXREPORTS.ZIP**

So installieren Sie Erweiterungsdateien für VirusScan-Richtlinien:

1. Melden Sie sich über ein Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Konfiguration** | **Erweiterungen** | **Erweiterung installieren**. Das Dialogfeld **Erweiterung installieren** wird angezeigt.
3. Klicken Sie auf **Durchsuchen**, wählen Sie die Erweiterungsdatei **VSCANMAC8600.ZIP** aus, und klicken Sie auf **OK**.

So installieren Sie Erweiterungsdateien für VirusScan-Berichte:

1 Melden Sie sich über ein Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie auf **Konfiguration** | **Erweiterungen** | **Erweiterung installieren**. Das Dialogfeld **Erweiterung installieren** wird angezeigt.

3 Klicken Sie auf **Durchsuchen**, wählen Sie die Erweiterungsdatei **VIREXREPORTS.ZIP** aus, und klicken Sie auf **OK**.

Einführung in ePolicy Orchestrator 4.0 Dashboard

Dashboards sind vorkonfigurierte und/oder vom Benutzer ausgewählte Monitore, die aktuelle Daten zu Ihren Erkennungen bieten.

Das ePolicy Orchestrator-Dashboard besteht aus mehreren benannten Dashboard-Monitoren. Je nach den Ihrem Benutzerkonto zugewiesenen Berechtigungen können Sie ein neues Dashboard erstellen, vorhandene Dashboards verwalten, aktive Dashboards auswählen und Voreinstellungen für Dashboards bearbeiten.

Erstellen neuer Dashboards

1 Melden Sie sich über ein Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie auf **Dashboards** | **Optionen** | **Neues Dashboard**. Die Seite **Neues Dashboard** wird geöffnet.

3 Geben Sie einen **Namen für das Dashboard** ein, und wählen Sie im Dropdown-Menü die gewünschte **Dashboard-Größe** aus.

4 Klicken Sie auf **Neuer Monitor**.

5 Wählen Sie unter **Kategorie** die Option **Abfragen** und im Dropdown-Menü **Monitor** die gewünschte Abfrage zu VirusScan aus.

6 Klicken Sie auf **OK**.

7 Wiederholen Sie Schritt 4 und 5 für die verbleibenden Monitore.

8 Klicken Sie auf **Speichern**. Das Dialogfeld **Aktivieren** wird angezeigt.

9 Klicken Sie auf **Ja**, um das neue Dashboard den aktiven Dashboards hinzuzufügen.

Tabelle 5-1 Dashboard-Optionen

Optionen	Beschreibung
Dashboard-Name	Gibt den Namen des von Ihnen ausgewählten Dashboards an.
Dashboard-Größe	Gibt die Größe (die Anzahl der Dashboard-Monitore) des ausgewählten Dashboards an.
Erstellt von	Gibt den Namen des Benutzers an, der das ausgewählte Dashboard erstellt hat.
Zuletzt geändert von	Gibt den Namen des Benutzers an, der die letzte Änderung vorgenommen hat, sowie das Datum und die Uhrzeit.
Bearbeiten	Sie gelangen zur Seite **Dashboard bearbeiten**, auf der Sie Änderungen an Name und Größe des Dashboards vornehmen können.
Löschen	Löscht das ausgewählte Dashboard.

Tabelle 5-1 Dashboard-Optionen

Optionen	Beschreibung
Duplizieren	Erstellt und speichert eine Kopie des ausgewählten Dashboards. Auf diese Weise können Sie ähnliche Dashboards erstellen und bearbeiten, ohne diese ganz neu erstellen zu müssen.
Veröffentlichen	Fügt das ausgewählte private Dashboard der Liste der öffentlichen Dashboards hinzu, sodass alle Benutzer mit entsprechenden Berechtigungen darauf zugreifen können.
Aktivieren	Fügt das ausgewählte Dashboard der Registerkarte „Dashboards“ hinzu, sodass einfacher darauf zugegriffen werden kann.

Systeme

Alle Systeme im Netzwerk werden über die Registerkarte **Systeme** verwaltet. Die **Systemstruktur** enthält alle Systeme, die von ePolicy Orchestrator verwaltet werden. Dies ist die Hauptoberfläche zum Verwalten von Richtlinien und Tasks auf diesen Systemen. In der **Systemstruktur** können Sie diese Systeme in logischen Gruppen organisieren bzw. sortieren.

Meine Organisation ist das Stammverzeichnis der **Systemstruktur**. Es enthält die Gruppe **Lost&Found**, in der Systeme gespeichert werden, deren Standorte vom Server nicht bestimmt werden können. Je nach den Methoden, mit denen Segmente (Systeme) in der **Systemstruktur** erstellt und verwaltet werden, ordnet der Server die Systeme anhand unterschiedlicher Merkmale in die **Systemstruktur** ein.

Informationen zum Hinzufügen neuer Systeme finden Sie im *Produkthandbuch zu ePolicy Orchestrator 4.0*.

Senden einer Agentenreaktivierung

1. Melden Sie sich über ein Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Systeme**.
3. Wählen Sie in der **Systemstruktur** eine Gruppe aus.
4. Wählen Sie den gewünschten **Computernamen** dieser Gruppe aus.
5. Klicken Sie auf **Weitere Aktionen** | **Agent reaktivieren**. Die Seite **Agenten reaktivieren** wird geöffnet.
6. Wählen Sie einen **Reaktivierungstyp** und einen Zeitraum für die **Zufallsausführung** (0 – 60 Minuten). In diesem Zeitraum können die Systeme auf die vom ePolicy Orchestrator-Server gesendete Reaktivierung antworten.
7. Wählen Sie **Alle Produkteigenschaften abrufen** aus, damit die Agenten alle Eigenschaften und nicht nur die seit der letzten Kommunikation zwischen Agenten und Server geänderten Eigenschaften senden.
8. Klicken Sie auf **OK**.

Rufen Sie das **Servertask-Protokoll** auf, um den Status der Agentenreaktivierung zu prüfen.

Richtlinien

Sie können Richtlinien erstellen, bearbeiten und löschen sowie einer bestimmten Gruppe oder einem bestimmten System in der **Systemstruktur** zuweisen.

Erstellen von neuen Richtlinien

1 Melden Sie sich über ein Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie auf **Systeme** | **Systemstruktur**, und wählen Sie eine Gruppe aus.

3 Wählen Sie unter **Richtlinien** das gewünschte **Produkt** in der Dropdown-Liste aus. Eine Liste der vom ausgewählten Einzelprodukt verwalteten Richtlinien wird im unteren Fenster angezeigt.

4 Suchen Sie die gewünschte Richtlinienkategorie, und klicken Sie dann auf **Zuweisung bearbeiten**. Die Seite **Richtlinienzuweisung für: Meine Organisation** | **Lost&Found** | **(ausgewählte Gruppe)** wird angezeigt.

5 Klicken Sie auf **Neue Richtlinie erstellen**. Das Dialogfeld **Neue Richtlinie erstellen** angezeigt.

6 Wählen Sie **McAfee-Standard** oder **Mein Standard** aus.

Die Richtlinien unter **McAfee-Standard** sind schreibgeschützt und können weder bearbeitet, umbenannt noch gelöscht werden.

7 Geben Sie einen neuen Richtliniennamen ein.

8 Klicken Sie auf **OK** und dann auf **Speichern**.

Umsetzen von Richtlinien

Sie können eine Richtlinie auf mehreren verwalteten Systemen innerhalb einer Gruppe umsetzen.

1 Melden Sie sich über ein Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie auf **Systeme** | **Systemstruktur**, und wählen Sie eine Gruppe aus.

3 Wählen Sie die gewünschten Systeme aus.

4 Klicken Sie auf **Richtlinie zuweisen**. Die Seite **Zuweisen von Richtlinie für <n> System** wird angezeigt.

5 Wählen Sie in der Dropdown-Liste **Produkt**, **Kategorie** und **Richtlinie** aus, und klicken Sie dann auf **Speichern**.

6 Wählen Sie die Systeme erneut aus.

7 Senden Sie eine Agentenreaktivierung.

Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung* auf Seite 53.

Sie können VirusScan-Richtlinien erst erstellen und umsetzen sowie Berichte anzeigen, nachdem die VirusScan-Erweiterungsdateien hinzugefügt wurden.

Client-Tasks

Mit ePolicy Orchestrator können Sie Client-Tasks, die auf den verwalteten Systemen ausgeführt werden, erstellen, planen und verwalten. Sie können Client-Tasks für die gesamte **Systemstruktur**, eine bestimmte Gruppe oder ein einzelnes System definieren.

Mit ePolicy Orchestrator 4.0 können Sie die folgenden geplanten Tasks für die VirusScan-Software erstellen:

- eUpdate-Task
- Task für Scan auf Anforderung

Welche Client-Tasks in der Dropdown-Liste verfügbar sind, hängt von den installierten Erweiterungsdateien ab.

eUpdate-Task

Ihre Software kann nur dann einen umfassenden Schutz gewährleisten, wenn sie laufend mit den neuesten Antivirusdefinitionen (DAT-Dateien) und Scanmodulen aktualisiert wird. Wir empfehlen, DAT-Dateien täglich zu aktualisieren und auf der McAfee AVERT-Website (Anti-Virus Emergency Response Team) regelmäßig nach neuen DAT-Dateien zu suchen.

Erstellen neuer eUpdate-Tasks

1. Melden Sie sich über ein Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Systeme** | **Systemstruktur**, und wählen Sie eine Gruppe aus.
3. Wählen Sie unter **Client-Tasks** in der **Systemstruktur** die Gruppe aus, für die ein eUpdate-Task erstellt werden soll.
4. Klicken Sie auf **Task erstellen**. Die Seite **Clienttask-Generator** wird angezeigt.
5. Geben Sie unter **Beschreibung** einen **Namen** und gegebenenfalls **Notizen** für den eUpdate-Task ein.
6. Wählen Sie unter **Typ** die Option **eUpdate-Task (VirusScan 8.6)** aus, und klicken Sie auf **Weiter**.
7. Planen Sie den Task wie gewünscht, und klicken Sie auf **Weiter**, um die **Zusammenfassung** des eUpdate-Tasks anzuzeigen. Hier werden **Name**, **Notizen**, **Produkt**, **Typ** sowie **Planungsinformationen** des Tasks angezeigt.
8. Klicken Sie auf **Speichern**.
9. Senden Sie eine Agentenreaktivierung.

Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung* auf Seite 53.

Klicken Sie auf **Bearbeiten**, um die Beschreibung/den Zeitplan des eUpdate-Tasks zu ändern, oder auf **Löschen**, um ihn zu entfernen.

Task für Scan auf Anforderung

Sie können beliebig viele Pläne für bedarfsmäßige Scans erstellen. Die geplanten Scans können so konfiguriert werden, dass sie in bestimmten Intervallen oder jederzeit vom Benutzer ausgeführt werden können.

Erstellen eines Tasks für das Scannen auf Anforderung

1 Melden Sie sich über ein Administratorkonto beim ePolicy Orchestrator-Server an.

2 Klicken Sie auf **Systeme** | **Systemstruktur** | **Client-Tasks**.

3 Wählen Sie in der **Systemstruktur** die Gruppe aus, für die ein Task für einen San auf Anforderung erstellt werden soll.

4 Klicken Sie auf **Task erstellen**. Die Seite **Clienttask-Generator** wird angezeigt.

5 Geben Sie unter **Beschreibung** einen **Namen** und gegebenenfalls **Notizen** für den Task für einen Scan auf Anforderung ein.

6 Wählen Sie unter **Typ** die Option **Scan auf Anforderung (VirusScan 8.6)** aus, und klicken Sie auf **Weiter**.

7 Wählen Sie unter **Konfiguration** eine Richtlinie in der Dropdown-Liste aus.

8 Klicken Sie auf **Weiter**, und planen Sie den Task wie gewünscht.

9 Klicken Sie auf **Weiter**, um die **Zusammenfassung** des Tasks für einen Scan auf Anforderung anzuzeigen. Hier werden **Name**, **Notizen**, **Produkt**, **Typ** sowie **Planungsinformationen** des Tasks angezeigt.

10 Klicken Sie auf **Speichern**.

11 Senden Sie eine Agentenreaktivierung.

Informationen zum Senden einer Agentenreaktivierung finden Sie unter *Senden einer Agentenreaktivierung* auf Seite 53.

Klicken Sie auf das **Bearbeiten**, um die Beschreibung/den Zeitplan des Tasks für einen Scan auf Anforderung zu ändern, oder auf **Löschen**, um ihn zu entfernen.

Deinstallation

Entfernen der Produkterweiterung

1. Melden Sie sich über ein Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Konfiguration** | **Erweiterungen**.
3. Wählen Sie die Erweiterungsdatei **VirusScan** aus, und klicken Sie auf **Entfernen**.
4. Wählen Sie die Option **Entfernen erzwingen, alle Überprüfungen oder Fehler umgehen** aus.
5. Klicken Sie auf **OK**.

Entfernen der Berichterweiterung

1. Melden Sie sich über ein Administratorkonto beim ePolicy Orchestrator-Server an.
2. Klicken Sie auf **Konfiguration** | **Erweiterungen**.
3. Wählen Sie die Erweiterungsdatei **VirusScan-Berichte** aus, und klicken Sie auf **Entfernen**.
4. Wählen Sie die Option **Entfernen erzwingen, alle Überprüfungen oder Fehler umgehen** aus.
5. Klicken Sie auf **OK**.

6 Fehlerbehebung

In diesem Kapitel finden Sie Lösungen zu Problemen, die beim Installieren oder Verwenden der VirusScan-Software auftreten können.

Es umfasst die folgenden Themen:

Häufig gestellte Fragen

Installation

Warum funktioniert das Installationsprogramm nicht?
Überprüfen Sie, auf welcher Plattform Sie VirusScan installieren. Hierbei muss es sich um Mac OS X Tiger Version 10.4.6 (oder höher) oder Mac OS X Leopard Version 10.5, PowerPC oder einen Intel-basierten Mac-Computer handeln. Der Computer muss über mindestens 512 MB RAM und 45 MB freien Festplattenspeicher verfügen. Alternativ kann auch ein vorhandenes Antivirenprogramm während der Installation erkannt worden sein, das entfernt werden muss, damit VirusScan erfolgreich installiert werden kann. Damit VirusScan ordnungsgemäß ausgeführt werden kann, muss außerdem das BSD-Subsystem auf Ihrem System installiert sein.

Welche VirusScan-Dateien werden installiert, und wo werden sie installiert?
VirusScan wird unter `/Programme`, VirusScan Schedule Editor unter `/Programme/Dienstprogramme` und VirusScan Reporter unter `/Library/Application Support` installiert. DAT-Dateien, Dynamic Libraries und Daemons finden Sie unter `/usr/local/vscanx`.

Scannen

Warum hat VirusScan einige Dateien beim Scannen übersprungen?
Überprüfen Sie, ob die übersprungenen Dateien vielleicht in der Ausschlussliste aufgeführt werden. Außerdem scannt VirusScan Archive und komprimierte Dateien nur, wenn es dazu konfiguriert wurde.

Während VirusScan eine Datei gescannt hat, habe ich eine andere Datei per Drag-and-Drop zum Scan hinzugefügt. Was ist mit dieser Datei passiert?
Während eines Scans können keine Dateien hinzugefügt werden. Beim Ziehen und Ablegen mehrerer Elemente werden diese in eine Warteschlange gestellt. Wenn Sie beispielsweise drei Ordner oder drei Dateien per Drag-and-Drop hinzufügen, führt der Scanner drei Scanvorgänge durch. Wenn Sie einen Ordner mit mehreren Dateien per Drag-and-Drop hinzufügen, führt der Scanner nur einen Scan durch.

Warum scannt VirusScan meinen Computer nicht in regelmäßigen Abständen?
Überprüfen Sie, ob ein Plan für das Scannen Ihres Systems auf Anforderung erstellt wurde, der aktiviert und für die regelmäßige Ausführung konfiguriert ist.

Viren und Erkennung

Kann VirusScan sowohl Macintosh- als auch Windows-Viren erkennen?
VirusScan erkennt alle bekannten Macintosh- und Windows-Viren und -Würmer.

Warum zeigt VirusScan die gescannten Elemente nicht mehr an?
VirusScan zeigt nur die ersten 200.000 Elemente an, die gescannt wurden und bei denen eine Infektion gefunden wurde.

Warum ist der Inhalt meiner Protokolldatei abgeschnitten?
Die maximale Größe von Protokolldateien beträgt 512 KB. Wenn eine Protokolldatei größer ist als 512 KB, wird sie in **VirusScan.log.0** umbenannt, und eine neue Datei **VirusScan.log** wird erstellt. Maximal zwei Protokolldateien werden gesichert. Wenn Sie eine Kopie der bestehenden Protokolldatei aufbewahren möchten, wird empfohlen, alte Protokolldateien zu sichern, bevor Sie einen neuen Scanvorgang starten. Um die Protokolldatei anzuzeigen, wählen Sie **Ablage** | **Protokoll anzeigen**.

Allgemeine Informationen

Kann ich die Änderungen an den Voreinstellungen rückgängig machen?
Wenn Sie unerwünschte Voreinstellungen gespeichert haben, können Sie diese auf die Vorgaben zurücksetzen, indem Sie in der linken unteren Ecke des Fensters **Voreinstellungen** auf **Auf Standardwerte zurücksetzen** klicken. An den Voreinstellungen vorgenommene Änderungen können nicht rückgängig gemacht werden. Die Einstellungen im Menü für Voreinstellungen werden gesichert, sobald sie vorgenommen werden. Es wird empfohlen, die aktuellen Voreinstellungen zu notieren, bevor Sie Änderungen daran vornehmen.

Unterstützt eUpdate Rollbacks?
eUpdate unterstützt nur bestehende oder neue Aktualisierungen. Rollbacks werden nicht unterstützt.

Umfassen die Aktualisierungen Macintosh-Virusdefinitionen?
eUpdates enthalten sowohl Macintosh- als auch Windows-Virusdefinitionen.

Wie finde ich die Versionsnummer und das Datum der Virusdefinitionsdateien (DAT-Dateien)?

Wählen Sie **Über VirusScan** aus dem VirusScan-Menü in der Menüleiste des Programms. Die Datumsangaben der DAT-Versionen geben nur an, wann die DAT-Dateien erstellt wurden.

Wie oft werden DAT-Dateien automatisch in VirusScan aktualisiert?

eUpdate überprüft automatisch über das Internet, ob neue Aktualisierungen vorhanden sind. Außerdem können Sie tägliche Aktualisierungen manuell über die Virusinformationsbibliothek von McAfee herunterladen.

Warum kann ich keine Verbindung zum eUpdate-Server herstellen, um ein nicht geplantes eUpdate durchzuführen?

Prüfen Sie, ob eine Internetverbindung besteht. Möglicherweise ist der eUpdate-Server gerade ausgelastet.

Erweiterte Fehlerbehebung

Kann ich nach der Installation von VirusScan die ausgeführten Prozesse anzeigen?

Die ausgeführten Prozesse sind VShieldScanManager und VShieldScanner.

Kann ich Virusdefinitionen manuell herunterladen, ohne eUpdate zu verwenden?

Klicken Sie in der Symbolleiste der VirusScan-Konsole auf **Virusinfo**. Hierdurch wird Ihr Standard-Browser gestartet und eine Verbindung mit der Virusinformationsbibliothek von McAfee hergestellt. Klicken Sie auf den Link für **Downloads** links im Bildschirm, um die DAT-Dateien herunterzuladen.

Wie passe ich die eUpdate-Servereinstellungen an?

1. Klicken Sie in der Symbolleiste auf **Voreinstellungen**, um das Dialogfeld **Voreinstellungen** anzuzeigen.
2. Klicken Sie auf **Mehr Optionen**.
3. Wählen Sie die Option **eUpdate-Servereinstellungen anpassen**, und klicken Sie anschließend auf **Anpassen**.
4. Konfigurieren Sie die Servereinstellung für eUpdate FTP-Servereinstellungen, und klicken Sie auf **OK**.
5. Klicken Sie auf **Schließen**.

Wo finde ich die Protokolldateien?

In Tabelle 6-1 sind die Protokolldateien aufgeführt.

Tabelle 6-1 Protokolldateien

Protokolldatei	Beschreibung	Speicherort
VirusScan.log	Enthält Einträge, die sich auf VirusScan beziehen.	Sie können auf diese Protokolldatei über `/var/log/VirusScan.log` zugreifen.
Protokoll	Enthält Einträge in Bezug auf den ePolicy Orchestrator-Agenten.	Sie können auf diese Protokolldatei über `/Library/NETAepoagt/scratch/etc/log` zugreifen.

Fehlermeldungen

In Tabelle 6-2 werden alle möglichen Fehlermeldungen aufgelistet, die während der Ausführung von VirusScan angezeigt werden, sowie die möglichen Gründe für ihr Auftreten.

Tabelle 6-2 Fehlermeldungen – VirusScan

Seriennr.	Meldung	Mögliche Ursache
1	Initialisierung der VirusScan-Engine ist fehlgeschlagen (Fehler x).	Das Modul oder die DAT-Dateien sind beschädigt bzw. wurden verschoben/gelöscht. Installieren Sie erneut.
2	Der Bericht konnte nicht gesichert werden. Möglicherweise ist das Volume voll, oder es sind keine zu schreibenden Daten verfügbar.	Auf Ihrem Volume ist wahrscheinlich nicht genügend freier Speicherplatz verfügbar, um den Bericht zu sichern. Machen Sie Speicherplatz frei, und versuchen Sie es erneut.
3	Die URL-Adresse für die Virusinformationsbibliothek konnte nicht geöffnet werden. Möglicherweise ist Ihr Browser nicht korrekt installiert.	Vergewissern Sie sich, dass Ihr Browser korrekt installiert ist.
4	Bei der Installation der Aktualisierung ist ein Fehler aufgetreten. Das eUpdate wurde nicht abgeschlossen.	Beim Versuch, eine Aktualisierung zu installieren, ist ein Fehler aufgetreten. Starten Sie das eUpdate erneut, und versuchen Sie es noch einmal.
5	Beim Entpacken des Updates ist ein Fehler aufgetreten. Das eUpdate wurde nicht abgeschlossen.	Beim Versuch, die Aktualisierung für die Installation zu entpacken, ist ein Fehler aufgetreten. Starten Sie das eUpdate erneut, und versuchen Sie es noch einmal.
6	Beim Herunterladen der Aktualisierung ist ein Fehler aufgetreten. Das eUpdate wurde nicht abgeschlossen.	Beim Versuch, die Aktualisierung herunterzuladen, ist ein Fehler aufgetreten. Möglicherweise ist der Server gerade beschäftigt. Warten Sie einige Minuten, und starten Sie dann das eUpdate erneut.
7	Dieses Softwareprodukt nähert sich dem Ende seiner Lebensdauer. Um einen vollständigen Antivirenschutz zu gewährleisten, sollte das Produkt möglichst bald aktualisiert werden.	Ihre VirusScan-Version ist veraltet. Sie sollten VirusScan auf die neueste Version aktualisieren, um den bestmöglichen Antivirenschutz zu gewährleisten.
8	Dieses Softwareprodukt nähert sich stark dem Ende seiner Lebensdauer. Seine weitere Verwendung kann nicht länger unterstützt werden. Um einen vollständigen Antivirenschutz zu gewährleisten, ist es wichtig, das Produkt möglichst bald zu aktualisieren.	Ihre VirusScan-Version ist veraltet. Sie sollten VirusScan auf die neueste Version aktualisieren, um den bestmöglichen Antivirenschutz zu gewährleisten.
9	Dieses Softwareprodukt bietet keinen ausreichenden Antivirenschutz mehr. Um einen vollständigen Antivirenschutz zu gewährleisten, muss das Produkt jetzt aktualisiert werden.	Ihre VirusScan-Version ist veraltet. Sie sollten VirusScan auf die neueste Version aktualisieren, um den bestmöglichen Antivirenschutz zu gewährleisten.

Tabelle 6-2 Fehlermeldungen – VirusScan

Seriennr.	Meldung	Mögliche Ursache
10	Das für dieses Produkt installierte Scanmodul bietet keinen ausreichenden Antivirenschutz mehr. Um einen vollständigen Antivirenschutz zu gewährleisten, sollte das Scanmodul möglichst bald aktualisiert werden.	Das in VirusScan enthaltene Modul ist veraltet. Führen Sie so bald wie möglich einen eUpdate-Task aus, um den bestmöglichen Antivirenschutz zu gewährleisten.
11	Das für dieses Produkt installierte Scanmodul nähert sich stark dem Ende seiner Lebensdauer. Seine weitere Verwendung kann nicht länger unterstützt werden. Um einen vollständigen Antivirenschutz zu gewährleisten, ist es wichtig, das Scanmodul möglichst bald zu aktualisieren.	Das in VirusScan enthaltene Modul ist veraltet. Führen Sie so bald wie möglich einen eUpdate-Task aus, um den bestmöglichen Antivirenschutz zu gewährleisten.
12	Das für dieses Produkt installierte Scanmodul bietet keinen ausreichenden Antivirenschutz mehr. Um einen vollständigen Antivirenschutz zu gewährleisten, muss das Scanmodul aktualisiert werden.	Das in VirusScan enthaltene Modul ist veraltet. Führen Sie so bald wie möglich einen eUpdate-Task aus, um den bestmöglichen Antivirenschutz zu gewährleisten.

Glossar

Agenten-AutoUpgrade	Die automatische Aktualisierung des Agenten, sobald eine neuere Version auf dem ePolicy Orchestrator-Server verfügbar ist.
Agenteninstallations-Paket	Das Setup-Programm und alle anderen Dateien, die zum Installieren des Agenten benötigt werden.
Agentenmonitor	Die Benutzeroberfläche des Agenten, die optional auf den verwalteten Computern angezeigt wird. Sie ermöglicht Ihnen das sofortige Ausführen von Tasks, die vom Agenten normalerweise in vordefinierten Intervallen initiiert werden.
Agentenreaktivierung	Bietet eine Möglichkeit, die Kommunikation zwischen Agent und Server vom Server aus zu initiieren.
Agentensprachpakete	Die Dateien, die an die Clientcomputer verteilt werden müssen, damit die Benutzeroberfläche des Agenten in anderen Sprachen als Englisch angezeigt werden kann.
Agent-Server-Kommunikation	Jede Form der Kommunikation zwischen dem ePolicy Orchestrator-Agenten und dem ePolicy Orchestrator-Server, bei der Daten zwischen Agent und Server ausgetauscht werden. Im Normalfall initiiert der Agent die Kommunikation mit dem Server.
Agent-Server-Kommunikationsintervall (ASKI)	Die Zeitspanne zwischen vordefinierten Agent-Server-Kommunikationen.
Ausbringen, Ausbringung	Das Verteilen und Installieren von Setup-Programmen auf Client-Computern von einer zentralen Stelle aus.
Bei-Zugriff-Scanner	Der Scanner bei Zugriff bietet eine ständige Überwachung aller verwendeten Dateien, um zu ermitteln, ob ein Virus oder sonstige potenziell unerwünschte Malware vorhanden ist. Dies geschieht immer dann, wenn eine Datei vom Datenträger gelesen und/oder auf den Datenträger geschrieben wird. Es können mehrere Verzeichnisse und Volumes gescannt werden.
Binärdateien (Setup-Dateien)	Das Setup-Programm und alle anderen Dateien, die zum Installieren der Produkte benötigt werden.
Daemon	Ein Programm, das permanent ausgeführt wird und Dienstanforderungen abarbeitet, die der Rechner erhält. Das Daemon-Programm leitet diese Anforderungen dann an andere Programme zur Verarbeitung weiter.
DAT-Dateien	Virusdefinitionsdateien, anhand derer die Antivirensoftware Viren und zugehörigen, potenziell unerwünschten, in Dateien eingebetteten Programmcode erkennt.

Dienstprogramm zur Meldung von Fehlern	Ein spezielles Dienstprogramm zum Verfolgen und Protokollieren von Fehlern in der McAfee-Software auf Ihrem System. Die so erfassten Informationen können zum Analysieren von Problemen verwendet werden.
EICAR	European Institute of Computer Anti-Virus Research. EICAR hat Dateien entwickelt, mit deren Hilfe getestet werden kann, ob die Antivirensoftware ordnungsgemäß installiert wurde und funktioniert.
Eigenschaften	Daten, die während der Agent-Server-Kommunikation ausgetauscht werden und Informationen über jeden verwalteten Computer (z. B. Hardware und Software) und seine verwalteten Produkte (z. B. bestimmte Richtlinieneinstellungen sowie die Produktversionsnummer) enthalten.
Einchecken	Das Hinzufügen von Dateien zum Master-Repository.
ePolicy Orchestrator-Agent	Ein Programm, das auf verwalteten Computern Hintergrundaufgaben ausführt, alle Anfragen zwischen dem ePolicy Orchestrator-Server und den Antiviren- und Sicherheitsprodukten auf diesen Computern vermittelt und dem Server den Status dieses Tasks zurückmeldet.
ePolicy Orchestrator-Datenbank	Die Datenbank, in der alle Daten gespeichert werden, die der ePolicy Orchestrator-Server vom ePolicy Orchestrator-Agenten erhält, sowie alle Einstellungen, die auf dem Server selbst vorgenommen werden.
ePolicy Orchestrator-Datenbankserver	Der Computer, auf dem sich die ePolicy Orchestrator-Datenbank befindet. Dies kann ein separater Computer sein oder der gleiche Computer, auf dem der ePolicy Orchestrator-Server installiert ist.
ePolicy Orchestrator-Konsole	Die Benutzeroberfläche der ePolicy Orchestrator-Software, mit der verwaltete Computer per Remote-Zugriff gesteuert und überwacht werden.
ePolicy Orchestrator-Remote-Konsole	Die ePolicy Orchestrator-Benutzeroberfläche, wenn sie auf einem separaten Computer und nicht auf dem gleichen Computer wie der ePolicy Orchestrator-Server installiert ist.
ePolicy Orchestrator-Server	Die Back-End-Komponente der ePolicy Orchestrator-Software.
Ereignisse	Daten, die während der Agent-Server-Kommunikation ausgetauscht werden und Informationen über jeden verwalteten Computer (z. B. Hardware und Software) und seine verwalteten Produkte (z. B. bestimmte Richtlinieneinstellungen und Produktversionsnummern) enthalten.
eUpdate	eUpdate ermöglicht Ihnen, Ihre DAT-Dateien und das Scanmodul zu aktualisieren. eUpdate prüft automatisch täglich auf neue Aktualisierungen, falls eine Internetverbindung vorhanden ist.
Firewall	Ein Programm, das als Filter zwischen Ihrem Rechner und dem Netzwerk bzw. dem Internet fungiert. Mithilfe dieses Programms kann der gesamte eingehende Verkehr und der gesamte ausgehende Verkehr bei Ihrem Rechner gescannt werden. Der Verkehr wird auf der Paketebene gescannt und gemäß den von Ihnen eingerichteten Regeln entweder blockiert oder zugelassen.
FTP	File Transfer Protocol. Eine häufig verwendete Methode, um Dateien zwischen zwei Internetsites zu verschieben.
Globaler Administrator	Ein Benutzerkonto mit Lese-, Schreib- und Löschberechtigungen sowie Rechten für alle Vorgänge. Vorgänge, die sich auf die gesamte Installation auswirken, dürfen nur von Benutzerkonten globaler Administratoren durchgeführt werden.

Gruppe Eine logische Gruppierung von Entitäten in der Konsolenstruktur, die zum Zweck einer einfacheren Verwaltung zusammengefasst wurden. Gruppen können andere Gruppen oder Computer enthalten. Ihnen können IP-Adressbereiche oder IP-Subnetzmasken zugewiesen werden, um das Sortieren der Computer nach IP-Adresse zu ermöglichen. Wenn Sie eine Gruppe durch Importieren einer Windows NT-Domäne erstellen, können Sie das Agenteninstallationspaket automatisch an alle importierten Computer in der Domäne senden.

Hintergrundinstallation Eine Installationsmethode, bei der ein Softwarepaket automatisch auf einem Computer installiert wird, ohne dass ein Benutzereingriff erforderlich ist.

HTTP HyperText Transfer Protocol. Ein Protokoll, mit dessen Hilfe Dateien im Internet verschoben werden können. Hierfür ist ein HTTP-Clientprogramm an einem Ende und ein HTTP-Serverprogramm am anderen Ende erforderlich.

Inaktiver Agent Jeder Agent, der nicht innerhalb einer bestimmten Zeitspanne mit dem ePolicy Orchestrator-Server kommuniziert hat.

Konsolenstruktur Der Inhalt der Registerkarte **Struktur** im linken Fenster der ePolicy Orchestrator-Konsole. Hier werden die Elemente angezeigt, die in der Konsole verfügbar sind.

Konsolenstruktur-element Die einzelnen Symbole in der Konsolenstruktur der ePolicy Orchestrator-Konsole.

Lost&Found-Gruppe Eine Gruppe zum temporären Speichern von Computern, deren ordnungsgemäße Position im **Verzeichnis** nicht bestimmt werden kann.

Makro Bei einigen Textverarbeitungsprogrammen sind Makros gespeicherte Befehlsfolgen, die über einen einzelnen Befehl oder einen Tastenanschlag wieder aufgerufen werden können.

Oberes Detailfenster Das obere rechte Fenster der Konsole, das die Registerkarten **Richtlinien**, **Eigenschaften** und **Tasks** enthält.

Protokoll/Protokolldatei Eine Aufzeichnung über die Aktivitäten einer Komponente der McAfee-Antivirensoftware. In Protokolldateien werden die Aktionen aufgezeichnet, die während einer Installation oder im Verlauf von Scan- oder Aktualisierungsaufgaben durchgeführt werden.

Repository Der Ort, an dem die Richtlinienseiten gespeichert sind, die zum Verwalten von Produkten verwendet werden.

Richtlinie Die Konfigurationseinstellungen verwalteter Produkte, die über ePolicy Orchestrator definiert und verwaltet werden.

Richtlinienumsetzungs intervall Die Zeitspanne, während der der Agent die Einstellungen umsetzt, die er vom ePolicy Orchestrator-Server erhalten hat. Da diese Einstellungen lokal umgesetzt werden, benötigt dieses Intervall keine Bandbreite.

Säubern, Säuberung Eine Aktion, die vom Scanner ausgeführt wird, wenn er einen *Virus*, einen *Trojaner* oder einen *Wurm* erkennt. Der Säuberungsprozess kann Folgendes beinhalten: Das Entfernen des Virus aus einer Datei und das Wiederherstellen der Datei, das Entfernen von Verweisen auf den Virus aus Systemdateien, INI-Dateien und der Registrierung, das Beenden des vom Virus eingeleiteten Prozesses, das Löschen eines Makros oder eines Microsoft Visual Basic-Skripts, das eine Datei infiziert, das Löschen einer Datei, wenn die Datei ein Trojaner oder ein Wurm ist sowie das Umbenennen einer Datei, die nicht gelöscht werden kann.

Scan, Scannen
Eine Prüfung von Dateien, die durchgeführt wird, um festzustellen, ob ein Virus oder anderer potenziell unerwünschter Code vorhanden ist.

Scannen auf Anforderung
Eine geplante Prüfung ausgewählter Dateien, die durchgeführt wird, um festzustellen, ob ein Virus oder anderer potenziell unerwünschter Code vorhanden ist. Diese Prüfung kann sofort, zu einem geplanten Zeitpunkt in der Zukunft oder in regelmäßig geplanten Intervallen stattfinden.

Scannen bei Zugriff
Eine laufende Prüfung verwendeter Dateien, die durchgeführt wird, um festzustellen, ob ein Virus oder eine andere Form von Malware vorhanden ist. Sie kann immer dann durchgeführt werden, wenn eine Datei vom Datenträger gelesen und/oder auf den Datenträger geschrieben wird. Es können mehrere Verzeichnisse und Volumes gescannt werden.

Scanner auf Anforderung
Mithilfe des Scanners auf Anforderung können Sie Virenscans jederzeit starten, indem Sie ausgewählte Dateien in die Konsole ziehen und dort ablegen oder sie im Dialogfeld zum Öffnen von Dateien öffnen. Sie können mehrere Dateien, Verzeichnisse und Volumes scannen.

Scantask
Ein einzelnes Scanereignis.

Scherzprogramm
Ein sich nicht replizierendes Programm, das einen Endbenutzer ängstigen oder belästigen könnte, aber keine Malware enthält und tatsächlich Dateien und Daten nicht beschädigt.

Serverereignisse
Aktivitäten auf dem ePolicy Orchestrator-Server, die von der Windows-Ereignisanzeige aufgezeichnet werden. Diese Informationen werden nicht in der ePolicy Orchestrator-Datenbank gespeichert, stehen also nicht für Berichte zur Verfügung.

Site
Eine logische Gruppierung von Entitäten in der Konsolenstruktur, die zum Zweck einer einfacheren Verwaltung zusammengefasst wurden. Sites können Gruppen von Computern enthalten und nach ihren IP-Adressbereichen, ihren IP-Subnetzmasken, ihrem Speicherort, der Abteilung usw. organisiert werden.

Sofortige Ereignisweiterleitung
Das sofortige Senden von Ereignissen eines bestimmten (oder höheren) Schweregrades an den ePolicy Orchestrator-Server, nachdem eine vordefinierte Anzahl von Ereignissen verfügbar ist. Diese Kommunikation findet außerhalb der normalen Agent-Server-Kommunikation statt.

Task
Eine Aktivität (sowohl Einzelaktionen, z. B. *Scannen auf Anforderung*, als auch Routineaktionen, z. B. *Aktualisierungen*), die planmäßig zu einem bestimmten Zeitpunkt oder in bestimmten Intervallen durchgeführt wird. Vergleiche mit *Richtlinie*.

Trojaner
Ein Programm, das entweder vorgibt, eine Reihe nützlicher oder wünschenswerter Funktionen zu besitzen, oder so beschrieben wird, tatsächlich aber schädliche Auswirkungen mit sich bringt. Trojaner sind keine Viren im eigentlichen Sinne, da sie sich nicht fortpflanzen.

Übernehmen, Übernahme
Die Anwendung der Einstellungen eines Elementes auf ein in der Hierarchie weiter unten stehendes Element.

Umsetzen, Umsetzung
Das Anwenden vordefinierter Einstellungen auf einem Client-Computer in vorbestimmten Intervallen.

UTC-Zeit
Coordinated Universal Time (UTC). Bezieht sich auf die Zeitzone auf dem Null- oder Greenwich-Meridian.

Verteilte Software-Repositories	Mehrere Websites oder Computern, die so im Netzwerk angeordnet sind, dass die Clientcomputer die Bandbreite beim Zugriff effizient nutzen. In verteilten Repositories werden die Dateien gespeichert, die von Client-Computern benötigt werden, um unterstützte Produkte und Aktualisierungen dieser Produkte zu installieren.
Verzeichnis	Die Liste aller über ePolicy Orchestrator zu verwaltenden Computer in der Konsolenstruktur; der Link zu den primären Schnittstellen für die Verwaltung dieser Computer.
Virus	Ein Programm mit Malware, die Dateien oder Programme verändern oder vernichten kann, oder Programme, die sich ohne oder nur mit geringer Benutzerintervention replizieren können. Auch die replizierten Programme können sich replizieren.
Virusinformations-bibliothek von McAfee	In der Virusinformationsbibliothek (http://vil.nai.com/vil/default.aspx) finden Sie detaillierte Informationen über die Herkunft der Viren, die Art und Weise, wie sie den Rechner infizieren und darüber, wie Sie sie entfernen. Die Site enthält außerdem Informationen zu Hoaxes.
VirusScan Schedule Editor	Mithilfe dieser Funktion können Sie zusätzliche Aktualisierungen für Virusdefinitionen und Software-Updates einplanen.
VirusScan-Konsole	Die am häufigsten verwendete Benutzeroberfläche für VirusScan. Mit dieser Konsole können Sie den Scanner auf Anforderung und den Scanner bei Zugriff konfigurieren, Scans auf Anforderung durchführen und eUpdates starten.
Warnung	Eine Nachricht oder Benachrichtigung über Computeraktivität, z. B. die Erkennung eines Virus. Diese kann je nach vordefinierter Konfiguration automatisch per E-Mail, Pager oder Telefon an Systemadministratoren und Benutzer gesendet werden.
Warnungspriorität	Der Wert, den Sie jeder Warnung zu Informationszwecken zuweisen. Sie können Warnungen die Priorität **Kritisch**, **Hoch**, **Gering**, **Warnung** oder **Informativ** zuweisen.
Wurm	Ein Virus, der sich durch die Erzeugung von eigenen Duplikaten auf anderen Laufwerken, Systemen oder Netzwerken verbreitet. Ein Wurm hängt sich nicht an weitere Programme an, er kann jedoch Dateien und Programme verändern, installieren oder zerstören.
Zusätzliche DAT-Dateien	Zusätzliche Virusdefinitionsdatei, die als Reaktion auf den Ausbruch eines neuen Virus oder einer neuen Variante eines bereits bestehenden Virus erstellt wird.
Zweig	Verzeichnisse im Master-Repository, die Ihnen ermöglichen, verschiedene Versionen ausgewählter Aktualisierungen zu speichern und zu verteilen.

Index

T

U

V

W

Z

McAfee®

mcafee.com