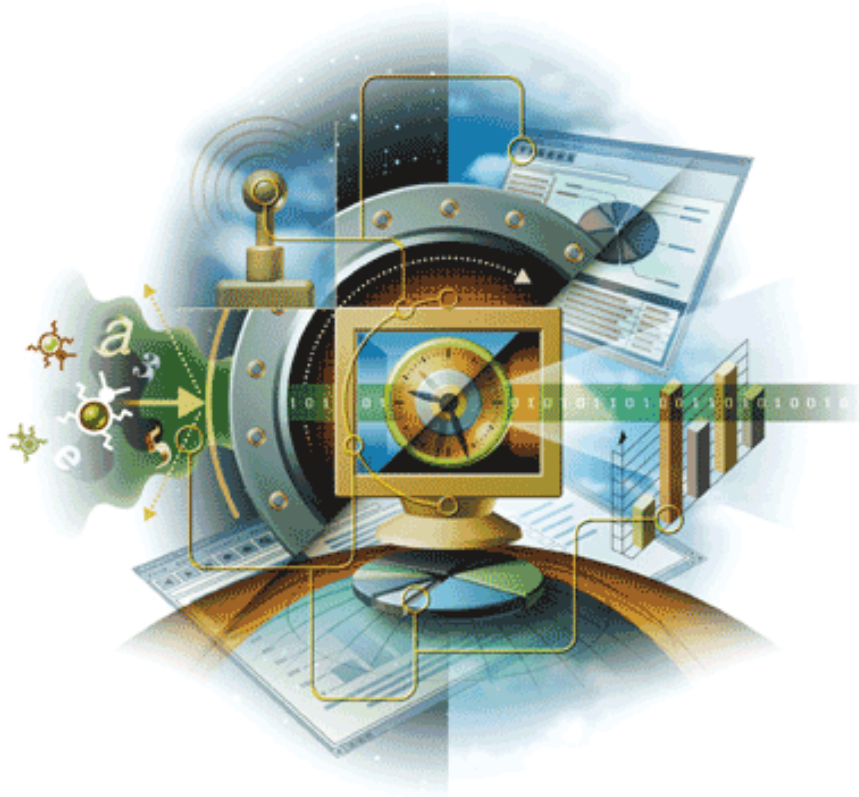


**Virex®**

Version 7.6

zur Verwendung mit ePolicy Orchestrator



**McAfee®**  
System Protection

Marktführende Intrusion-Prevention-Lösungen

## COPYRIGHT

Copyright © 2004-2005 McAfee, Inc., Alle Rechte vorbehalten.

Diese Veröffentlichung darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung durch McAfee Inc., ihrer Zulieferer oder Partnerunternehmen vervielfältigt, übertragen, transkribiert, in einem Retrieval-System gespeichert oder in andere Sprachen übersetzt werden. Um diese Genehmigung zu erhalten, schreiben Sie an die Rechtsabteilung von McAfee unter der Adresse: 5000 Headquarters Drive, Plano, Texas 75024, oder rufen Sie uns unter +1-972-963-8000 an.

## HINWEISE AUF MARKEN

Active Firewall, Active Security, ActiveSecurity (und in Katakana), ActiveShield, AntiVirus Anyware und Design, Clean-Up, Design (Stilisiertes E), Design (Stilisiertes N), Entercept, Enterprise SecureCast, Enterprise SecureCast (und in Katakana), ePolicy Orchestrator, First Aid, ForceField, GMT, GroupShield, GroupShield (und in Katakana), Guard Dog, HomeGuard, Hunter, IntruShield, Intrusion Prevention Through Innovation, M und Design, McAfee, McAfee (und in Katakana), McAfee und Design, McAfee.com, McAfee VirusScan, NA Network Associates, Net Tools, Net Tools (und in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, Network Associates, Network Associates Coliseum, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, RingFence, Router PM, SecureCast, SecureSelect, SpamKiller, Stalker, ThreatScan, TIS, TMEG, Total Virus Defense, Trusted Mail, Uninstaller, Virex, Virus Forum, Virusscan, Virusscan (und in Katakana), Webscan, Webshield, Webshield (und in Katakana), Webstalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, Your E-Business Defender, Your Network. Our Business. sind eingetragene Marken oder Marken von McAfee, Inc., und/oder Partnerunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Erkennungsmerkmal für McAfee®-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken, die in diesem Dokument genannt werden, sind Eigentum der jeweiligen Inhaber.

## LIZENZINFORMATIONEN

### Lizenzvereinbarung

HINWEIS AN ALLE BENUTZER: LESEN SIE DIE ENTSPRECHENDE LIZENZVEREINBARUNG FÜR DIE VON IHNEN ERWORBENE LIZENZ SORGFÄLTIG DURCH. IN DIESER VEREINBARUNG SIND DIE ALLGEMEINEN BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE ENTHALTEN. WENN SIE NICHT WISSEN, WELCHEN LIZENTYP SIE ERWORBEN HABEN, WENDEN SIE SICH BITTE AN DEN VERTRIEB ODER SCHAUEN SIE IN ANDEREN LIZENZBEZOGENEN DOKUMENTEN BZW. BESTELLUNTERLAGEN NACH, DIE MIT IHREM SOFTWAREPAKET GELIEFERT ODER SEPARAT ALS TEIL DES PRODUKTS ZUR VERFÜGUNG GESTELLT WURDEN (ALS BROSCHÜRE, ALS DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSITE ZUR VERFÜGUNG STEHT, VON DER SIE DAS SOFTWAREPAKET HERUNTERGELOADEN HABEN). WENN SIE EINIGEN BEDINGUNGEN DES LIZENZVERTRAGS NICHT ZUSTIMMEN, DÜRFEN SIE DIE SOFTWARE NICHT INSTALLIEREN. IN DIESEM FALL KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES AN MCAFEE ODER AN DIE STELLE ZURÜCKGEBEN, VON DER SIE ES ERWORBEN HABEN.

### Ergänzungen

Dieses Produkt umfasst oder kann umfassen:

- Software, die vom OpenSSL-Projekt zur Verwendung mit dem OpenSSL-Toolkit entwickelt wurde <http://www.openssl.org/>.
- Kryptographie-Software, die von Eric Young entwickelt wurde, und Software, die von Tim J. Hudson entwickelt wurde.
- Einige Softwareprogramme, die gemäß der GNU, General Public License (GPL) oder anderen ähnlichen Lizenzen für kostenlose Software zugelassen werden und es dem Benutzer neben anderen Rechten erlauben, bestimmte Programme oder Teile davon zu kopieren, zu modifizieren und weiterzugeben sowie auf den Quellcode zuzugreifen. GPL-lizenzierte Software, die einem Benutzer in einem ausführbaren binären Format bereitgestellt wird, muss diesem Benutzer auch als Quelltext bereitgestellt werden. Die Quelltexte der mitgelieferten GPL-lizenzierten Softwareanwendungen sind auf der diesem Produkt beigefügten CD enthalten. Falls Lizenzen für kostenlose Software verlangen, dass McAfee Rechte für die Nutzung, das Kopieren oder die Modifikation eines Softwareprogramms gewährt, die über die in diesem Vertrag gewährten Rechte hinausgehen, so haben Rechte dieser Art Vorrang vor den Rechten und Einschränkungen in diesem Vertrag.
- Von Henry Spencer entwickelte Software, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Von Robert Nordier entwickelte Software, Copyright © 1996-7 Robert Nordier.
- Von Douglas W. Sauder entwickelte Software.
- Von der Apache Software Foundation entwickelte Software (<http://www.apache.org>). Eine Kopie des Lizenzvertrags für diese Software erhalten Sie unter [www.apache.org/licenses/LICENSE-2.0.txt](http://www.apache.org/licenses/LICENSE-2.0.txt).
- International Components for Unicode („ICU“), Copyright © 1995-2002 International Business Machines Corporation und andere.
- Von CrystalClear Software, Inc. entwickelte Software, Copyright, © 2000 CrystalClear Software, Inc.
- FEAD® Optimizer®-Technologie, Copyright Netopsystems AG, Berlin, Deutschland.
- Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. und/oder Outside In® HTML Export, © 2001 Stellent Chicago, Inc.
- Software, urheberrechtlich geschützt von Thai Open Source Software Center Ltd. und Clark Cooper, © 1998, 1999, 2000.
- Software, urheberrechtlich geschützt von Expat maintainers.
- Software, urheberrechtlich geschützt von The Regents of the University of California, © 1989-1989.
- Software, urheberrechtlich geschützt von Gunnar Ritter.
- Software, urheberrechtlich geschützt von Sun Microsystems®, Inc., © 2003.
- Software, urheberrechtlich geschützt von Gisle Aas. © 1995-2003.
- Software, urheberrechtlich geschützt von Michael A. Chase, © 1999-2000.
- Software, urheberrechtlich geschützt von Neil Winton, © 1995-1996.
- Software, urheberrechtlich geschützt von RSA Data Security, Inc., © 1990-1992.
- Software, urheberrechtlich geschützt von Sean M. Burke, © 1999, 2000.
- Software, urheberrechtlich geschützt von Martijn Koster, © 1995.
- Software, urheberrechtlich geschützt von Brad Appleton, © 1996-1999.
- Software, urheberrechtlich geschützt von Michael G. Schwern, © 2001.
- Software, urheberrechtlich geschützt von Graham Barr, © 1998.
- Software, urheberrechtlich geschützt von Larry Wall and Clark Cooper, © 1998-2000.
- Software, urheberrechtlich geschützt von Frodo Looijaard, © 1997.
- Software, urheberrechtlich geschützt von Python Software Foundation, Copyright © 2001, 2002, 2003. Eine Kopie des Lizenzvertrags für diese Software erhalten Sie unter [www.python.org](http://www.python.org).
- Software, urheberrechtlich geschützt von Beman Dawes, © 1994-1999, 2002.
- Von Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek entwickelte Software © 1997-2000 University of Notre Dame.
- Software, urheberrechtlich geschützt von Simone Bordet & Marco Cravero, © 2002.
- Software, urheberrechtlich geschützt von Stephen Purcell, © 2001.
- Von der Indiana University Extreme! entwickelte Software. Lab (<http://www.extreme.indiana.edu/>).
- Software, urheberrechtlich geschützt von International Business Machines Corporation und anderen, © 1995-2003.
- Von der University of California, Berkeley und deren Mitwirkenden entwickelte Software.
- Von Ralf S. Engelschall, <[rse@engelschall.com](mailto:rse@engelschall.com)>, entwickelte Software für die Verwendung im mod\_ssl-Projekt (<http://www.modssl.org/>).
- Software, urheberrechtlich geschützt von Kevin Henney, © 2000-2002.
- Software, urheberrechtlich geschützt von Peter Dimov und Multi Media Ltd. © 2001, 2002.
- Software, urheberrechtlich geschützt von David Abrahams, © 2001, 2002. Dokumentation erhalten Sie unter <http://www.boost.org/libs/bind/bind.html>.
- Software, urheberrechtlich geschützt von Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000.
- Software, urheberrechtlich geschützt von Boost.org, © 1999-2002.
- Software, urheberrechtlich geschützt von Nicolai M. Josuttis, © 1999.
- Software, urheberrechtlich geschützt von Jeremy Siek, © 1999-2001.
- Software, urheberrechtlich geschützt von Daryle Walker, © 2001.
- Software, urheberrechtlich geschützt von Chuck Allison und Jeremy Siek, © 2001, 2002.
- Software, urheberrechtlich geschützt von Samuel Kremp, © 2001. Aktualisierungen, Dokumentationen und Versionsverlauf unter <http://www.boost.org>.
- Software, urheberrechtlich geschützt von Doug Gregor ([gregod@cs.rpi.edu](mailto:gregod@cs.rpi.edu)), © 2001, 2002.
- Software, urheberrechtlich geschützt von Cadenza New Zealand Ltd., © 2000.
- Software, urheberrechtlich geschützt von Jens Maurer, © 2000, 2001.
- Software, urheberrechtlich geschützt von Jaakko Järvi ([jaakko.jarvi@cs.utu.fi](mailto:jaakko.jarvi@cs.utu.fi)), © 1999, 2000.
- Software, urheberrechtlich geschützt von Ronald Garcia, © 2002.
- Software, urheberrechtlich geschützt von David Abrahams, Jeremy Siek und Daryle Walker, © 1999-2001.
- Software, urheberrechtlich geschützt von Stephen Cleary ([shammah@voyager.net](mailto:shammah@voyager.net)), © 2000.
- Software, urheberrechtlich geschützt von Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software, urheberrechtlich geschützt von Paul Moore, © 1999.
- Software, urheberrechtlich geschützt von Dr. John Maddock, © 1998-2002.
- Software, urheberrechtlich geschützt von Greg Colvin und Beman Dawes, © 1998, 1999.
- Software, urheberrechtlich geschützt von Peter Dimov, © 2001, 2002.
- Software, urheberrechtlich geschützt von Jeremy Siek und John R. Bandela, © 2001.
- Software, urheberrechtlich geschützt von Joerg Walter and Mathias Koch, © 2000-2002.

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>5</b>
	Welche Informationen enthält dieses Handbuch? . . . . .	5
	Voraussetzungen für die Verwendung von ePolicy Orchestrator zur Verwaltung von Virex . . . . .	6
	Einführung in die ePolicy Orchestrator-Konsole . . . . .	6
	Lesergruppe . . . . .	7
	Konventionen . . . . .	7
	Ressourcen . . . . .	8
	Produktinformationen . . . . .	8
	Links zur Verknüpfung mit externen Ressourcen . . . . .	9
	Produktservice . . . . .	11
	Kontaktinformationen . . . . .	12
<b>2</b>	<b>Installation</b>	<b>13</b>
	Einleitung . . . . .	13
	Systemanforderungen . . . . .	13
	Konfigurieren der ePolicy Orchestrator-Konsole zum Verwalten von Virex 7.6 . . . . .	13
	Hinzufügen der NAP-Dateien zum Verwalten von Virex 7.6 . . . . .	14
	Installieren des Agenten für Macintosh-Systeme . . . . .	17
	Installationsverzeichnis des Agenten . . . . .	17
	Installieren des Agenten . . . . .	18
	Installieren von Virex 7.6 . . . . .	23
	Deinstallation . . . . .	23
	Entfernen von Virex NAP vom ePolicy Orchestrator-Server . . . . .	23
	Entfernen des ePolicy Orchestrator-Agenten vom ePolicy Orchestrator-Server . . . . .	24
	Entfernen des ePolicy Orchestrator-Agenten unter Mac OS X . . . . .	24
<b>3</b>	<b>Festlegen der ePolicy Orchestrator-Richtlinien für Virex 7.6</b>	<b>25</b>
	Festlegen von Richtlinien in ePolicy Orchestrator . . . . .	25
	Allgemein . . . . .	27
	eUpdate . . . . .	28
	Aktiver Scanner . . . . .	29
	Hintergrund-Scanner . . . . .	31
	Scanner für aktivierte Volumes . . . . .	32
	Bedarfsmäßiger Scanner . . . . .	33
	Planen von Scans und eUpdates . . . . .	34
	Informationen über geplante Tasks . . . . .	34
	eUpdate . . . . .	38
	Anzeigender ePolicy Orchestrator-Servereigenschaften . . . . .	40
<b>4</b>	<b>Entferntes Steuern des Agenten</b>	<b>41</b>
	Anzeigen von Agenteneigenschaften . . . . .	41
	Durchsetzen von Richtlinien für den ePolicyOrchestrator-Agenten . . . . .	42
	Agentenoptionen . . . . .	43
	Ereignisse . . . . .	44
	Anzeigen von Serverereignissen . . . . .	47
	Protokollierung . . . . .	48

<b>5</b>	<b>Berichte</b>	<b>49</b>
	Berichte .....	49
	Konfigurieren von Berichten .....	50
	<b>Glossar</b>	<b>51</b>
	<b>Index</b>	<b>55</b>

# 1

## Einleitung

---

### Welche Informationen enthält dieses Handbuch?

Dieses Handbuch beschreibt die Konfiguration von Virex 7.6 mit der Verwaltungssoftware McAfee ePolicy Orchestrator Version 3.0.2 und höher. Um dieses Handbuch effektiv verwenden zu können, sollten Sie mit ePolicy Orchestrator vertraut sein. Weitere Informationen finden Sie im *ePolicy Orchestrator-Produkt Handbuch*. Die ePolicy Orchestrator-Software bietet einen zentralen Kontrollpunkt für Ihre McAfee-Anti-Virus-Produkte, von dem aus Sie Anti-Virus-Richtlinien verwalten und Berichte über Anti-Virus-Ereignisse und Virusaktivitäten in einer Unternehmensumgebung anzeigen können. Mit dem ePolicy Orchestrator können Sie Virex auf den Zielcomputern in Ihrem Netzwerk konfigurieren. Sie müssen sie nicht individuell über das Dialogfeld **Voreinstellungen** von Virex konfigurieren.

Dieses Handbuch enthält die folgenden Informationen:

- Hinzufügen der ePolicy Orchestrator-Agentenkonfiguration zum ePolicy Orchestrator-Server.
- Festlegen der Anti-Virus-Richtlinien auf den Zielsystemen zum Konfigurieren der folgenden Virex-Funktionen:
  - Allgemeine Richtlinien zum Steuern der allgemeinen Virex-Funktionen.
  - eUpdate-Serverrichtlinien.
  - Richtlinien für den aktiven Scanner.
  - Richtlinien für den Hintergrund-Scanner.
  - Richtlinien des Scanners für aktivierte Volumes.
  - Richtlinien des bedarfsmäßigen Scanners.
- Konfigurieren des ePolicy Orchestrator-Agent für Mac OS X.
  - Agent-Kommunikationsintervall.
  - Intervall für die Richtliniendurchsetzung.
  - Ereignisweiterleitung.
  - Protokollierung.



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

## Voraussetzungen für die Verwendung von ePolicy Orchestrator zur Verwaltung von Virex

Damit Sie Virex mit der ePolicy Orchestrator-Software konfigurieren können, müssen Sie zunächst Folgendes tun:

- Fügen Sie die Virex 7.6 NAP-Datei zum Software-Repository von ePolicy Orchestrator hinzu.
- Fügen Sie die Datei<sup>1</sup> des nicht auf Windows basierenden Agenten in ePolicy Orchestrator hinzu.
- Installieren Sie Virex 7.6 auf dem Macintosh-System.
- Installieren Sie den ePolicy Orchestrator Agent auf dem Macintosh-System.

## 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 die Virex-Anti-Virus-Produkte, die über ePolicy Orchestrator verwaltet werden.

Bei der ersten Anmeldung am Server erscheint die Konsole mit markiertem Stammverzeichnis im linken Fenster. Das Erscheinungsbild der Konsole ändert sich, um die Elemente widerzuspiegeln, die Sie in der Konsolenstruktur oder im Detailfenster ausgewählt haben. Die Konsole verwendet MMC-Standardfunktionen.

Unter den Menüs am oberen Fensterrand ist die Konsole in zwei Hälften oder Fenster geteilt.

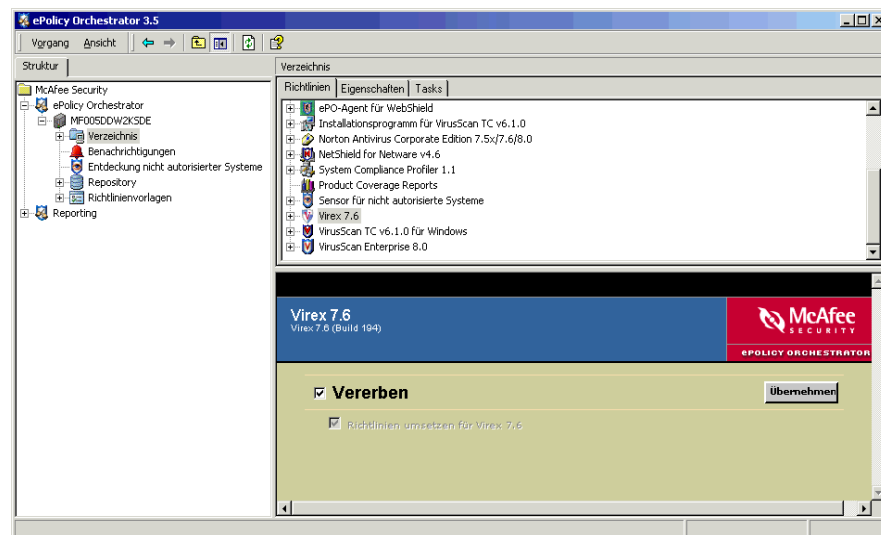


Abbildung 1-1 ePolicy Orchestrator-Konsole

<sup>1</sup> Der nicht auf Windows basierende Agent (Non Windows Agent, NWA) wird auch als ePolicy Orchestrator-Agent für Mac OS X bezeichnet.

- Die **Konsolenstruktur** befindet sich auf der linken Seite der Konsole. Sie zeigt die Server, Arbeitsstationen und Anwendungen an, die Sie 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**.

## Lesergruppe

Dieses Handbuch wurde für System- und Netzwerkadministratoren entwickelt, die für das Anti-Viren-Programm Ihres Unternehmens verantwortlich sind.

## Konventionen

In diesem Handbuch gelten die folgenden Konventionen:

**Bold Serif** Alle Wörter auf der Benutzeroberfläche, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder.

**Beispiel:**

Geben Sie den **Benutzernamen** und das **Kennwort** des gewünschten Kontos ein.

**Courier** Der Pfad eines Ordners oder Programms; eine Webadresse (URL); Text, der etwas darstellt, das der Benutzer genau so eingibt (z. B. ein Befehl bei der Eingabeaufforderung).

**Beispiele:**

Der Standardspeicherort für das Programm ist:

`C:\Programme\McAfee\EPO\3.5.0`

Besuchen Sie die McAfee-Website unter:

`http://www.mcafee.com/de`

Führen Sie diesen Befehl auf dem Clientcomputer aus:

`C:\SETUP.EXE`

**Kursiv** Wird zur Hervorhebung oder bei Einführung eines neuen Begriffs sowie für Namen von Produktdokumentation und Themen (Überschriften) des Handbuchs verwendet.

**Beispiel:**

Weitere Informationen finden Sie im *Virex 7.6-Produkthandbuch*.

**<BEGRIFF>** Generische Begriffe werden in spitze Klammern gesetzt.

**Beispiel:**

Klicken Sie im Konsolenbaum unter **ePolicy Orchestrator** mit der rechten Maustaste auf **<SERVER>**.



**Hinweis:** Zusätzliche Informationen, z. B. eine alternative Methode zum Ausführen eines Befehls.



**Tipp:** Empfehlungen für optimale Methoden und Empfehlungen von McAfee zur Vorbeugung von Bedrohungen, zu Leistung und Effizienz.



**Achtung:** Wichtiger Hinweis, der Informationen zum Schutz Ihres Computer-Systems, des Unternehmens, der Software oder von Daten enthält.



**Warnung:** Wichtiger Hinweis, der Informationen zum Schutz des Benutzers beim Umgang mit einer Hardware enthält.



**Neu:** Neue oder überarbeitete Funktion oder Option in dieser Produktversion.

---

## Ressourcen

McAfee®-Produkte stehen für jahrelange Erfahrung und Engagement für die Zufriedenheit der Kunden. Das McAfee PrimeSupport®-Team aus verantwortungsbewussten, hoch qualifizierten Supportmitarbeitern bietet maßgeschneiderte Lösungen und detaillierte technische Unterstützung für die erfolgreiche Bewältigung von kritischen Projekten – und das alles mit verschiedenen Support-Stufen, die die Ansprüche jedes Kundenunternehmens erfüllen. McAfee Research, ein weltweit führendes Unternehmen im Bereich Informationssysteme und Sicherheitsforschung, ist auch weiterhin der Vorkämpfer für Innovationen bei der Entwicklung und Verbesserung all unserer Technologien.

Weitere Ressourcen finden Sie in den folgenden Abschnitten:

- Produktinformationen.
- Links zur Verknüpfung mit externen Ressourcen.
- Produktservice.
- Kontaktinformationen.

## 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.

**Produkthandbuch** – Produktüberblick und Funktionen, detaillierte Anweisungen zum Konfigurieren der Software, Informationen zur Weitergabe, sich wiederholende Tasks und Vorgehensweisen.

- *Virex 7.6 Handbuch*

**Hilfe** – Qualitativ hochwertige und ausführliche Informationen, die von der Softwareanwendung aus zugänglich sind.

**Konfigurationshandbuch** – Zur Verwendung mit ePolicy Orchestrator®. Prozeduren zum Weitergeben und Verwalten von Virex mit der ePolicy Orchestrator-Verwaltungssoftware.

**Versionshinweise<sup>A</sup>** – ReadMe Produktinformationen, gelöste und bekannte Probleme und Ergänzungen kurz vor Drucklegung oder Änderungen an Produkt oder Dokumentation.



**Kontakte<sup>^</sup>** – Kontaktinformationen für McAfee-Services und -Ressourcen: technischer Support, Kundendienst, Security Headquarters ( AVERT Anti-Virus & Vulnerability Emergency Response Team), Beta-Programm und Schulung. Diese Datei enthält außerdem Telefonnummern, Postadressen, Webadressen und Faxnummern von Unternehmensniederlassungen in den USA und in anderen Ländern.

**Lizenz** – Die McAfee-Lizenzvereinbarungsbroschüre, die alle Lizenzarten enthält, die Sie für Ihr Produkt erwerben können. Die Lizenzvereinbarung enthält die allgemeinen Bedingungen für die Verwendung des lizenzierten Produkts.

\* Ein gedrucktes Handbuch, das der Produkt-CD beigelegt ist. Hinweis: Für einige Sprachen sind die Handbücher evtl. nur als PDF-Datei erhältlich.

<sup>^</sup> In der Softwareanwendung und auf der Produkt-CD enthaltene Textdateien.

## Links zur Verknüpfung mit externen Ressourcen

Das Produkt bietet Links zu einigen nützlichen Ressourcen:

- Online-Hilfe.
- Virus Information Library.
- Technischer Support für ePolicy Orchestrator.
- Minimum Escalation Resource Tool.
- AVERT Web Immune.
- McAfee-Security-Homepage.

### Online-Hilfe

Verwenden Sie diesen Link, um auf die Onlinehilfe-Themen des Produkts zuzugreifen.



Wenn das integrierte Hilfesystem des Produkts (das von der Software aus durch Klicken auf das Menü **Hilfe** zugänglich ist) auf Ihrem System nicht ordnungsgemäß angezeigt wird, funktionieren möglicherweise die ActiveX-Steuerelemente in Ihrer Version des Microsoft® Internet Explorers nicht einwandfrei. Diese Steuerelemente werden zum Anzeigen der Hilfedatei benötigt. Stellen Sie sicher, dass Sie die neueste Version des Internet Explorers installieren.

### Virus Information Library

Verwenden Sie den Link **Virusinformationen**, um auf die Virus Information Library von AVERT (McAfee Anti-Virus & Vulnerability Emergency Response Team) zuzugreifen. Diese Website bietet detaillierte Informationen darüber, wo Viren herkommen, wie sie Ihr System infizieren und wie sie entfernt werden können.

Neben Informationen über echte Viren bietet die Virus Information Library auch nützliche Information über Virus-Hoaxes wie 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. Beim nächsten Mal, wenn Sie eine gutgemeinte Viruswarnung erhalten, werfen Sie zunächst einen Blick auf unsere Hoax-Seite, bevor Sie die Nachricht an Ihre Freunde weiterleiten.

So greifen Sie auf die Virus Information Library zu:

- 1 Öffnen Sie ePolicy Orchestrator.
- 2 Wählen Sie den Link **Virus Information Library** auf der **Startseite** aus.

#### **Technischer Support für ePolicy Orchestrator.**

Verwenden Sie den Link **Technischer Support**, um auf die Website des McAfee PrimeSupport KnowledgeCenter Service Portals zuzugreifen. Durchsuchen Sie diese Website, um häufig gestellte Fragen (FAQs) und Dokumentationen anzuzeigen und eine geführte Wissenssuche durchzuführen.

- 1 Öffnen Sie ePolicy Orchestrator.
- 2 Klicken Sie auf den Link **Technischer Support für ePolicy Orchestrator** auf der **Startseite**.

#### **Minimum Escalation Resource Tool**

Verwenden Sie den Link „Minimum Escalation Resource Tool“, um auf die Website des McAfee PrimeSupport KnowledgeCenter Service Portals zuzugreifen. Melden Sie sich auf der Support-Site für die Registrierung von Eskalationen an.

- 1 Öffnen Sie ePolicy Orchestrator.
- 2 Klicken Sie auf den Link **Minimum Escalation Resource Tool** auf der **Startseite**.

#### **AVERT Web Immune**

Verwenden Sie den Link „AVERT Web Immune“, um auf die Avert Web Immune Portal-Website zuzugreifen.

- 1 Öffnen Sie ePolicy Orchestrator.
- 2 Wählen Sie den Link **AVERT Web Immune** auf der **Startseite** aus.

#### **McAfee Security-Homepage**

Verwenden Sie den Link „McAfee Security-Homepage“, um auf die Website McAfee Security-Homepage zuzugreifen.

- 1 Öffnen Sie ePolicy Orchestrator.
- 2 Wählen Sie den Link **McAfee Security-Homepage** auf der **Startseite** aus.

## Produktservice

Die folgenden Services helfen Ihnen dabei, das Beste aus Ihren McAfee-Produkten herauszuholen:

- Beta-Programm.
- HotFixes und Patches.
- Support für Produkte am „Ende ihrer Lebensdauer“ (End-of-Life-Support).

### Beta-Programm

Mit dem McAfee-Beta-Programm können Sie unsere Produkte vor der Veröffentlichung testen. So können Sie neue Funktionen für bestehende Produkte kennen lernen und ausprobieren sowie vollkommen neue Produkte testen. Dieses Programm hilft Ihnen dabei, aktualisierte und neue Funktionen früher zu implementieren, und zwar in einer sicheren Umgebung. Sie erhalten die Möglichkeit, Vorschläge zu neuen Produktfunktionen zu machen und direkt mit dem Technikpersonal von McAfee zu kommunizieren.

Weitere Informationen finden Sie auf folgender Website:

<http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm>

### HotFixes und Patches

HotFixes und Patches werden mit aktualisierten Dateien, Treibern, ausführbaren Dateien usw. zwischen den Hauptversionen eines Produkts herausgegeben. Die aktuellsten HotFixes und Patches finden Sie auf folgender Website:

<http://www.mcafeesecurity.com/de/downloads/updates/hotfixes.asp>

### Support für Produkte am „Ende ihrer Lebensdauer“ (End-of-Life-Support)

Ihre Anti-Viren-Software muss ständig aktualisiert werden, um im Kampf gegen Viren und andere potentiell gefährliche Software effektiv zu bleiben. Daher ist es wichtig, dass Sie die Virusdefinitionsdateien (DAT) regelmäßig aktualisieren. Um Ihre Software in die Lage zu versetzen, auf die ständige Bedrohung entsprechend reagieren zu können, verändern wir oft die Art und Weise, in der die DAT-Dateien und Scan-Module zusammenarbeiten. Daher ist es wichtig, dass Sie Ihr Scan-Modul aktualisieren, wenn eine neue Version herausgegeben wird. Ein älteres Modul wird viele der neu auftretenden Bedrohungen nicht erkennen.

Wenn wir ein neues Modul herausgeben, kündigen wir das Datum an, ab dem Ihr bestehendes Modul nicht mehr unterstützt werden wird. Informationen zu unserer End-of-Life-Richtlinie und eine umfassende Liste der unterstützten Scan-Module und Produkte finden Sie auf folgender Website:

[http://www.mcafeesecurity.com/de/products/mcafee/end\\_of\\_life.htm](http://www.mcafeesecurity.com/de/products/mcafee/end_of_life.htm)

## Kontaktinformationen

### Technischer Support

Homepage	<a href="http://www.mcafeesecurity.com/de/support/technical_support">http://www.mcafeesecurity.com/de/support/technical_support</a>
Suche in der KnowledgeBase	<a href="https://knowledgemap.nai.com/phpclient/homepage.aspx">https://knowledgemap.nai.com/phpclient/homepage.aspx</a>
PrimeSupport Service Portal *	<a href="https://mysupport.nai.com">https://mysupport.nai.com</a>

### McAfee Beta-Programm

<http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm>

### Sicherheitszentrale – AVERT: Anti-Virus & Vulnerability Emergency Response Team

Homepage	<a href="http://www.mcafeesecurity.com/de/security/home.asp">http://www.mcafeesecurity.com/de/security/home.asp</a>
Virus Information Library	<a href="http://vil.nai.com">http://vil.nai.com</a>
AVERT WebImmune, *	<a href="https://www.webimmune.net/default.asp">https://www.webimmune.net/default.asp</a>
Beispiel weiterleiten	
AVERT DAT Notification Service	<a href="http://vil.mcafeesecurity.com/vil/join-DAT-list.asp">http://vil.mcafeesecurity.com/vil/join-DAT-list.asp</a>

### Download-Site

Homepage	<a href="http://www.mcafeesecurity.com/de/downloads/">http://www.mcafeesecurity.com/de/downloads/</a>
DAT-Datei und Engine-Aktualisierungen	<a href="http://www.mcafeesecurity.com/de/downloads/updates/default.asp">http://www.mcafeesecurity.com/de/downloads/updates/default.asp</a>
	<a href="ftp://ftp.mcafeesecurity.com/pub/antivirus/datfiles/4.x">ftp://ftp.mcafeesecurity.com/pub/antivirus/datfiles/4.x</a>
Produktaktualisierungen *	<a href="https://secure.nai.com/de/forms/downloads/upgrades/login.asp">https://secure.nai.com/de/forms/downloads/upgrades/login.asp</a>

### Schulung

Schulung vor Ort	<a href="http://www.mcafeesecurity.com/de/services/security/home.htm">http://www.mcafeesecurity.com/de/services/security/home.htm</a>
McAfee University	<a href="http://www.networkassociates.com/de/services/education/mcafee/university.htm">http://www.networkassociates.com/de/services/education/mcafee/university.htm</a>

### Kundendienst

E-Mail	<a href="https://secure.nai.com/us/forms/support/request_form.asp">https://secure.nai.com/us/forms/support/request_form.asp</a>
Web	<a href="http://www.mcafeesecurity.com/us/index.asp">http://www.mcafeesecurity.com/us/index.asp</a> <a href="http://www.mcafeesecurity.com/de/support/default.asp">http://www.mcafeesecurity.com/de/support/default.asp</a>

USA, Kanada und Lateinamerika  
gebührenfrei:

**+1-888-VIRUS NO** oder **+1-888-847-8766**

Montag – Freitag, 8.00 – 20.00 Uhr, Central Time

Weitere Informationen zu den Kontaktdaten von McAfee, einschließlich der gebührenfreien Nummern für andere Länder, finden Sie in der Kontaktdatei, die diesem Produkt beigelegt ist.

\* Anmeldedaten erforderlich.

# 2 Installation

---

## Einleitung

Dieser Agent ist die verteilte Programmkomponente von ePolicy Orchestrator, die auf jedem Macintosh-Computer im Netzwerk installiert wird. Der Agent sammelt und sendet Informationen zwischen dem ePolicy Orchestrator-Server, den Repositories und den verwalteten Virex 7.6-Installationen im Netzwerk. Von der Konfigurierung des Agenten und seiner Richtlinien hängt es ab, wie er die Kommunikation und Aktualisierung in Ihrer Umgebung unterstützt.

## Systemanforderungen

Der Agent kann auf Macintosh-Systemen wie:

- MAC OS 10.2.6
- MAC OS 10.2.8
- MAC OS 10.3.x

sowie auf den folgenden Macintosh-Plattformen installiert werden:

- G3
- G4
- G5

---

## Konfigurieren der ePolicy Orchestrator-Konsole zum Verwalten von Virex 7.6

Ein Computer mit komplett installiertem ePolicy Orchestrator-Agenten ermöglicht Ihnen das einfache Bereitstellen der Berichtfunktion. Führen Sie die folgenden Schritte aus, um die Berichtfunktion für Ihre Computer einzurichten:

- Stellen Sie sicher, dass Sie die IP-Adresse und den Port des Policy Orchestrator-Servers über die ePolicy Orchestrator Configurator-Benutzeroberfläche Ihres Clientcomputers konfiguriert haben.

## Hinzufügen der NAP-Dateien zum Verwalten von Virex 7.6

Network Associate Package-Datei (NAP-Datei). Diese Dateierweiterung wird zur Kennzeichnung von McAfee-Software-Programmdateien verwendet, die zu Verwaltungszwecken im Software-Repository von ePolicy Orchestrator installiert sind. Der ePolicy Orchestrator-Server wird mit einer Reihe von Richtlinien für die wichtigsten unterstützten Produkte installiert, die zum Veröffentlichungszeitpunkt Ihre Version von ePolicy Orchestrator verfügbar waren. Um Virex 7.6 verwalten zu können, müssen Sie zunächst die entsprechenden NAP-Dateien des Produkts zum Software-Repository hinzufügen.

### Wo finde ich die \*.NAP-Dateien für Virex 7.6, die ich zum Repository hinzufügen möchte?

McAfee veröffentlicht NAP-Dateien für alle Anti-Virus- und Sicherheitsprodukte, die von ePolicy Orchestrator unterstützt werden. Die NAP-Datei eines bestimmten Produkts ist mit den anderen Installationsdateien dieses Produkts verfügbar. 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 Virex 7.6 befinden sich im Unterordner mit den **ePolicy Orchestrator-Serverkomponenten** auf der Produkt-CD oder in der ZIP-Datei. Die 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 Ressourcen oder aktualisierte Macintosh-Computer repliziert.

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

### So fügen Sie die NAP-Datei eines nicht auf Windows basierenden Macintosh-Agenten zum ePolicy Orchestrator-Server hinzu:

- 1 Suchen Sie die NAP-Datei 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.



**Abbildung 2-1 Software-Repository konfigurieren, Assistent**



Doppelklicken Sie auf **Repository** in der ePolicy Orchestrator-Konsolenstruktur, und klicken Sie anschließend auf den Link **NAP hinzufügen** im rechten Detailfenster, um den Assistenten **Software-Repository konfigurieren** anzuzeigen.

- 4 Wählen Sie im **Software-Repository konfigurieren**-Assistenten die Option **Neue Software zur Verwaltung hinzufügen** aus, und klicken Sie auf **Weiter**.

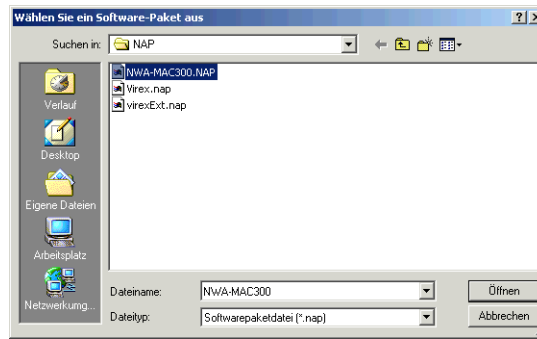


Abbildung 2-2 Das Dialogfeld „Softwarepaket auswählen“

- 5 Gehen Sie im Dialogfeld **Softwarepaket auswählen** zu der Datei **NWA-MAC300.NAP**, die Sie in **Schritt 1** in einem temporären Ordner gespeichert haben, und wählen Sie die Datei aus.
- 6 Klicken Sie auf **Öffnen**, damit ePolicy Orchestrator die NAP-Datei laden kann.

## Hinzufügen der Virex .NAP-Datei

**So fügen Sie eine Virex .NAP-Datei zum ePolicy Orchestrator-Server hinzu:**

- 1 Suchen Sie die NAP-Datei 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.

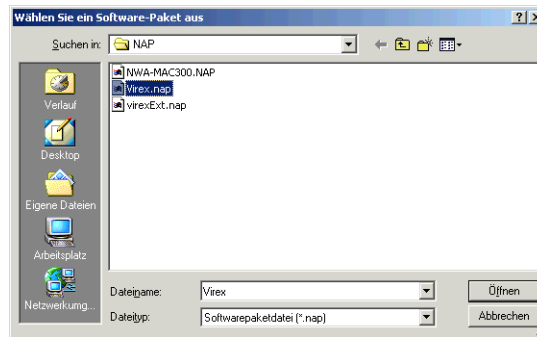


Abbildung 2-3 Software-Repository konfigurieren, Assistent



Doppelklicken Sie auf **Repository** in der ePolicy Orchestrator-Konsolenstruktur, und klicken Sie anschließend auf den Link **NAP hinzufügen** im rechten Detailfenster, um den Assistenten **Software-Repository konfigurieren** anzuzeigen.

- 4 Wählen Sie im **Software-Repository konfigurieren**-Assistenten die Option **Neue Software zur Verwaltung hinzufügen** aus, und klicken Sie auf **Weiter**..



**Abbildung 2-4 Das Dialogfeld „Softwarepaket auswählen“**

- 5 Gehen Sie im Dialogfeld **Softwarepaket auswählen** zu der Datei **Virex.NAP**, die Sie in **Schritt 1** in einem temporären Ordner gespeichert haben, und wählen Sie die Datei aus.
- 6 Klicken Sie auf **Öffnen**, damit ePolicy Orchestrator die NAP-Datei laden kann.

## Hinzufügen der Bericht-.NAP-Datei

**So fügen Sie eine Bericht-NAP-Datei zum ePolicy Orchestrator-Server hinzu:**

- 1 Suchen Sie die NAP-Datei 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.



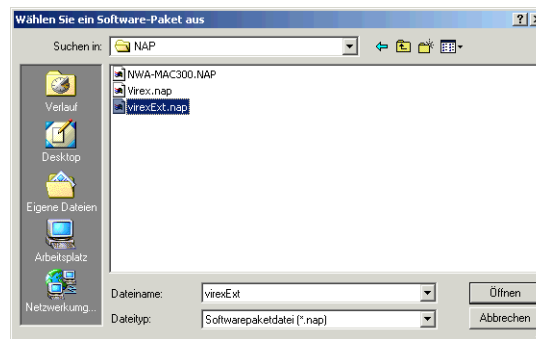
**Abbildung 2-5 Software-Repository konfigurieren, Assistent**



Doppelklicken Sie auf **Repository** in der ePolicy Orchestrator-Konsolenstruktur, und klicken Sie anschließend auf den Link **NAP hinzufügen** im rechten Detailfenster, um den Assistenten **Software-Repository konfigurieren** anzuzeigen.



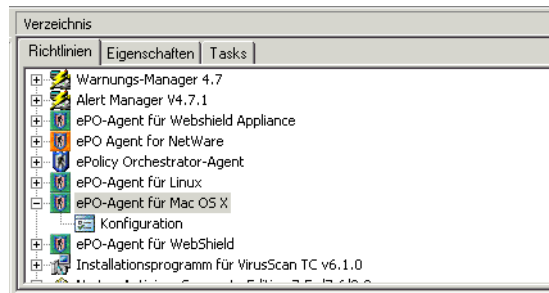
- 4 Wählen Sie im **Software-Repository konfigurieren**-Assistenten die Option **Neue Berichte hinzufügen** aus, und klicken Sie auf **Weiter**.



**Abbildung 2-6 Das Dialogfeld „Softwarepaket auswählen“**

- 5 Gehen Sie im Dialogfeld **Softwarepaket auswählen** zu der Datei **VirexExt.NAP**, die sie in **Schritt 1** in einem temporären Ordner gespeichert haben, und klicken Sie auf **Öffnen**, damit ePolicy Orchestrator die Bericht-NAP-Datei laden kann.

Nachdem der ePolicy Orchestrator die NAP-Dateien geladen hat, wird der Agent in der Richtlinienliste in der oberen Hälfte des Detailfensters angezeigt.



**Abbildung 2-7 Registerkarte „Richtlinien“**

## Installieren des Agenten für Macintosh-Systeme

### Installationsverzeichnis des Agenten

Der Agent ist unter /Library/NETAepoagt installiert und verwendet außerdem das Verzeichnis /Library/NETASSOC für konfigurationsbezogene Daten.



Sie können das Installationsverzeichnis des ePolicy Orchestrator-Agenten auf einem Macintosh OS X-System nicht ändern.

## Installieren des Agenten

Der ePolicy Orchestrator-Agent für Macintosh kann entweder im Rahmen einer Standardinstallation (grafische Benutzeroberfläche) oder über eine Befehlszeile (automatische Installation) installiert werden.

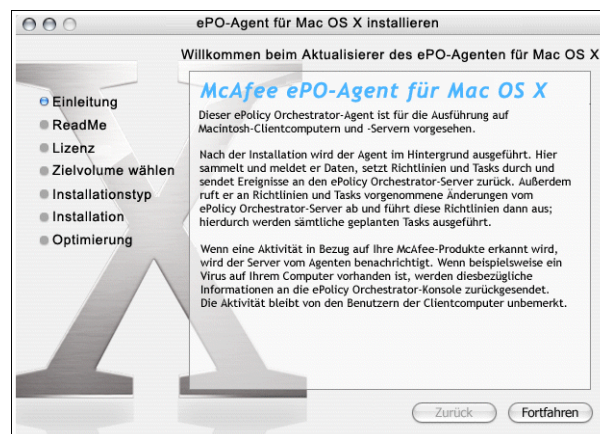
### Standardinstallation

- 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.



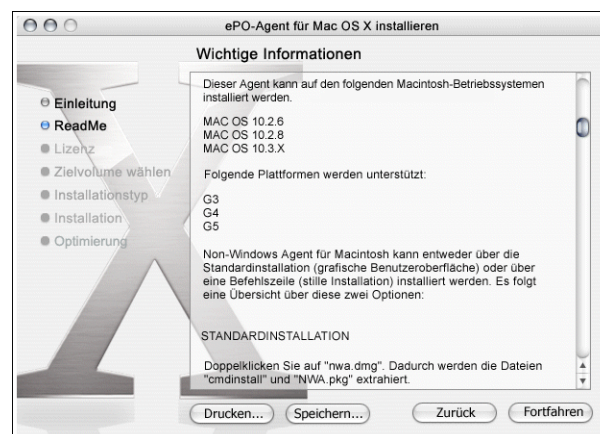
**nwa.dmg** befindet sich im Ordner **ePO Agent** der Datei **ePO Components.ZIP** auf der Produkt-CD.

- 2 Doppelklicken Sie auf **nwa.dmg**. Daraufhin werden folgende Dateien extrahiert:
  - NWA.pkg
  - cmdinstall
- 3 Doppelklicken Sie auf **NWA.pkg**. Daraufhin wird das Fenster mit der **Begrüßung beim ePO-Agenten für den Mac OS X-Aktualisierer** eingeblendet.



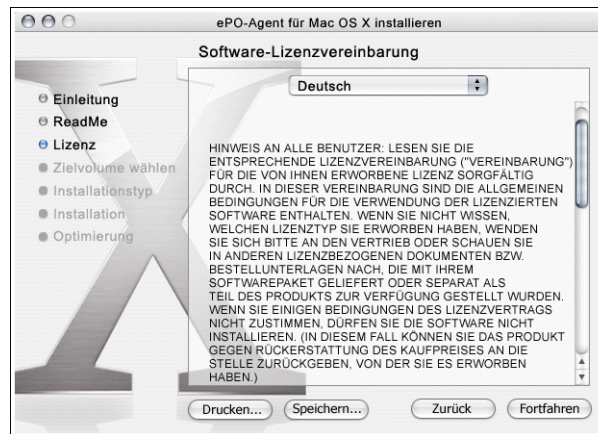
**Abbildung 2-8 ePO-Agenten-Installationsfenster – Einleitung**

- 4 Klicken Sie auf **Weiter**. Daraufhin wird das Fenster **ReadMe** angezeigt. Die ReadMe-Datei beschreibt die Funktionen des Agenten, nennt alle bekannten Verhaltensprobleme oder andere Probleme dieser Agentenversion.



**Abbildung 2-9 ePO-Agenten-Installationsfenster – ReadMe**

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

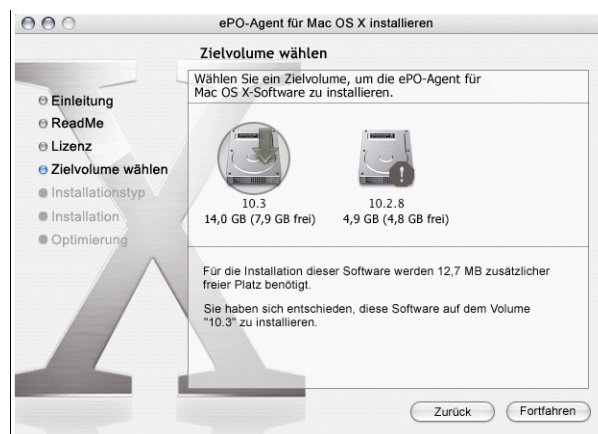


**Abbildung 2-10 ePO-Agenten-Installationsfenster – Lizenz**



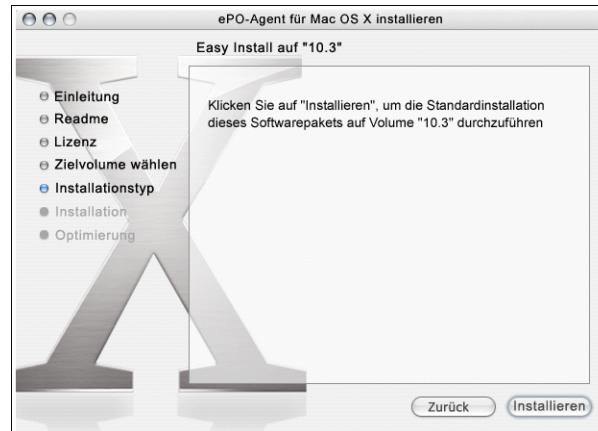
Lesen und bestätigen Sie die Lizenzvereinbarung. Wenn Sie der Lizenzvereinbarung nicht zustimmen, können Sie nicht mit der Installation fortfahren.

- 6 Klicken Sie auf **Weiter**. Daraufhin wird das Fenster für die **Zielauswahl** eingeblendet.



**Abbildung 2-11 ePO-Agenten-Installationsfenster – Zielauswahl**

Wählen Sie das Volume aus, auf dem Sie den ePolicy Orchestrator-Agenten installieren müssen, und klicken Sie auf **Weiter**. Das Fenster des **Easy Install** wird angezeigt.



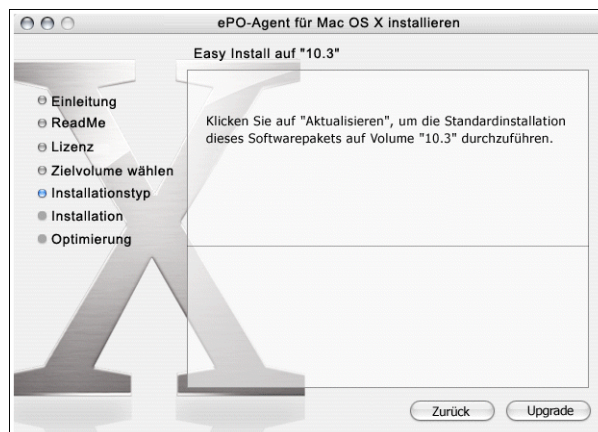
**Abbildung 2-12 ePO-Agenten-Installationsassistent – Neuinstallation**



In folgenden Fällen wird das Fenster **Easy Install** mit der Schaltfläche **Installieren** eingeblendet:

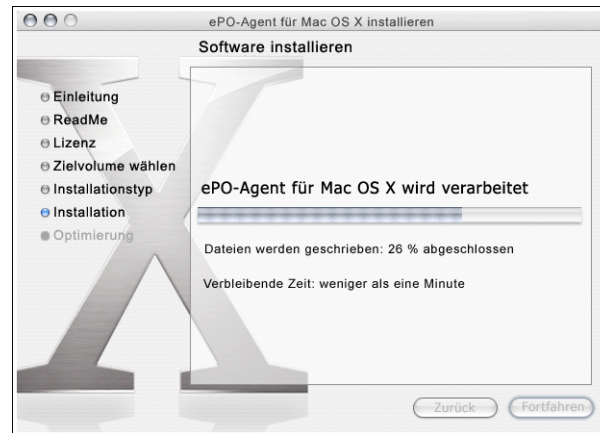
- Sie installieren den Agenten zum ersten Mal.
- Sie installieren den Agenten erneut, nachdem Sie die vorherige ePolicy Orchestrator-Agenteninstallation entfernt haben.

Bei der Aktualisierung des ePolicy Orchestrator-Agenten wird das nachfolgend dargestellte Fenster eingeblendet.



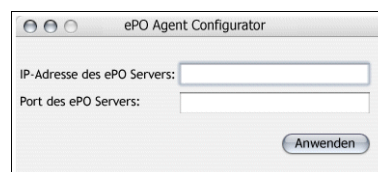
**Abbildung 2-13 ePO-Agenten-Installationsfenster – Aktualisierungsinstallation**

- 7 Wählen Sie zum Fortfahren die Option für das **Installieren/Aktualisieren**. Bevor Sie fortfahren können, werden Sie vom Aktualisierer zur Authentifizierung aufgefordert. Geben Sie Ihr Kennwort ein, und klicken Sie dann auf **OK**. Daraufhin wird das Fenster für die **Installation der Software** eingeblendet.



**Abbildung 2-14 ePO-Agenten-Installationsfenster – Installation der Software**

Während dieses Vorgangs werden Sie vom Aktualisierer 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.



**Abbildung 2-15 Dialogfeld „ePO Agent Configurator“**

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



**Abbildung 2-16 ePO-Agenten-Installationsfenster – Installation der Software**

- 9 Mit **Neu starten** wird der Installationsvorgang abgeschlossen.

## Automatische Installation (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.



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

- 2 Doppelklicken Sie auf **nwa.dmg**. Daraufhin werden folgende Dateien extrahiert:

- NWA.pkg
- cmdinstall

- 3 Öffnen Sie das Fenster **Terminal**, und ändern Sie das Arbeitsverzeichnis in NAINWA.



Zur Ausführung dieses Befehls sind Administratorrechte erforderlich.

- 4 Führen Sie im Fenster **Terminal** `sudo ./cmdinstall` aus, und wählen Sie dann <IP-Adresse des ePO-Servers>:<Port des ePO-Servers>

```
Terminal - bash - 85x41
Manoj-Ts-Computer : /Volumes/NAINWA manoj$ sudo ./cmdinstall 172.16.197.94 79
Kennwort:
Das Arbeitsverzeichnis ist /Volumes/NAINWA
Temporärer Ordner wird erstellt /tmp/NAINWA.rESFqHq3
Server inf.-Datei wird verworfen
172.16.197.94
79
Aktualisierer [2420]: Sprache des Aktualisierers: Englisch
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for root=(none), domain=0
installer [2420]: Requirement: requires "certain file content criteria" PASS for root=(none), domain=0
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for root=/, domain=0
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for installer [2420]: Requirement: requires "certain file content criteria" PASS for root=/, domain=0
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for root=/, domain=0
installer [2420]: == Starting check on volume /
installer [2420]: Requirement: requires "certain file content criteria" PASS for root=/, domain=0
installer: Package name is ePO Agent for Mac OS X
Aktualisierer: Das in / aktivierte Volume wird aktualisiert.
installer: Preparing the Disk....
```

**Abbildung 2-17 Terminal-Fenster – Start**

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

```
Terminal - bash - 85x24
#
Aktualisierer: ePO-Agent für Mac OS X wird verarbeitet
#
Aktualisierer: Installation beenden
###installer[709]: Registered /Library/NETApoagt/bin/ePO Agent Configurator.app.
###
installer:
#
Aktualisierer: Systemleistung optimieren...
#installer[709]: Running task: /usr/bin/update_prebinding
installer[709]: 1970-02-15 10:56:34.539 update_prebinding[829] Start of update_prebinding
installer: Optimizing volume "10.3": 0% complete
installer: Optimizing volume "10.3": 5% complete
installer: Optimizing volume "10.3": 30% complete
installer: Optimizing volume "10.3": 100% complete
installer[709]: 1970-02-15 10:56:41.284 update_prebinding[829] Update_prebinding done
installer[709]: 1970-02-15 10:56:41.293 update_prebinding[829] 1 files successfully prebound, 0 files unsuccessfully prebound.
installer[709]: Finished task: /usr/bin/update_prebinding
Aktualisierer: Das Upgrade war erfolgreich.
Bereinigungsvorgang /tmp/NAINWA.NXT800VY
```

**Abbildung 2-18 Terminal-Fenster – Installation/Aufrüstung abgeschlossen**

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



## Installieren von Virex 7.6



Anweisungen zum Installieren von Virex 7.6 auf Macintosh-Systemen finden Sie im *Virex 7.6-Produkt Handbuch*.

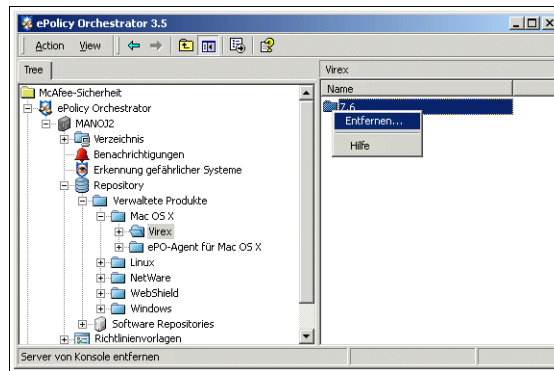
## Deinstallation

### Entfernen von Virex NAP vom ePolicy Orchestrator-Server

Virex NAP kann vom ePolicy Orchestrator-Server entfernt werden.

#### So wird Virex NAP entfernt:

- 1 Melden Sie sich am ePolicy Orchestrator-Datenbankserver an.
- 2 Wählen Sie in der Konsolenstruktur **Virex** unter **Repository** | **Verwaltete Produkte** | **MAC OS X** aus.



**Abbildung 2-19 Virex NAP – Entfernen**

- 3 Klicken Sie mit der rechten Maustaste auf **Virex**, und wählen Sie dann **Entfernen** aus, um die Deinstallation von Virex NAP auf dem ePolicy Orchestrator-Server vorzunehmen.

## Entfernen des ePolicy Orchestrator-Agenten vom ePolicy Orchestrator-Server



Nach dem Hinzufügen ist das Entfernen des **ePolicy Orchestrator-Agenten für MAC OS X** vom ePolicy Orchestrator-Server **nicht** möglich.

## Entfernen des ePolicy Orchestrator-Agenten unter Mac OS X

Sie können den ePolicy Orchestrator-Agenten über die Befehlszeile von einem Macintosh-Computer deinstallieren.

### Über die Befehlszeile

- 1 Melden Sie sich als Root-Benutzer an.



Der Root-Benutzer ist auf einem Macintosh-System standardmäßig deaktiviert. Aktivieren Sie den Root-Benutzer, falls dieser deaktiviert ist. Wenn Sie sich als Benutzer angemeldet haben, öffnen Sie das **Terminal**-Fenster, geben Sie „su“ ein, und geben Sie anschließend das Root-Kennwort ein, um sich als Root-Benutzer anzumelden.

- 2 Gehen Sie zu /Library/NETAepoagt
- 3 Führen Sie cmduninst aus.



# 3

## Festlegen der ePolicy Orchestrator-Richtlinien für Virex 7.6

In diesem Kapitel wird erklärt, wie Sie die Virex-Richtlinien vom ePolicy Orchestrator aus durchsetzen. Dabei gibt es zwei grundlegende Schritte:

- Sie wählen im ePolicy Orchestrator die Namen der Computer und die Virex-Richtlinien aus, die auf diese Computer zutreffen werden. Beispielsweise sollen Computer A und B auf Viren gescannt werden. Sie können viele verschiedene Richtlinien festlegen, die auf viele einzelne Computer oder Gruppen von Computern zutreffen.
- Sie weisen ePolicy Orchestrator an, diese Richtlinien auf Computern durchzusetzen; der Agent kommuniziert mit dem Server, um zu ermitteln, ob neue Richtlinien bereitgestellt wurden. Die Computer befolgen dann Ihre Richtlinie und ignorieren alle Richtlinien, die vorher im Virex-Dialogfeld **Voreinstellungen** konfiguriert waren.

---

### Festlegen von Richtlinien in ePolicy Orchestrator

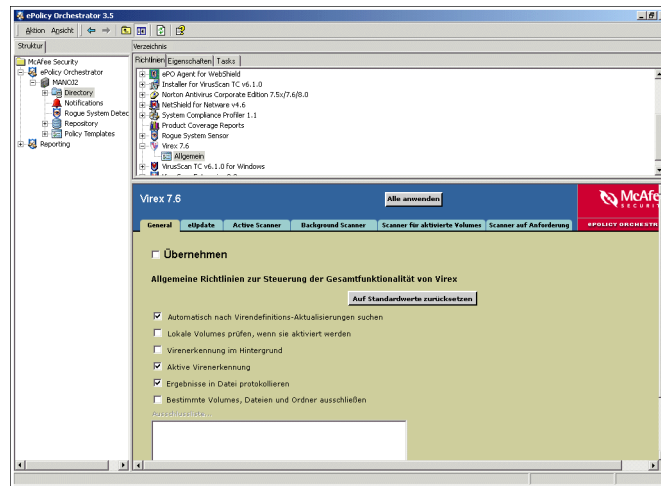
Über die ePolicy Orchestrator-Konsole können Sie Richtlinien für Gruppen von Computern bzw. auf einem einzelnen Computer durchsetzen. Diese Richtlinien setzen die Konfigurationen einzelner Computer außer Kraft. Informationen über Richtlinien und ihre Durchsetzung finden Sie im *ePolicy Orchestrator-Produktthandbuch*.

Wählen Sie vor dem Konfigurieren von Richtlinien eine Gruppe von Computern aus der Konsolenstruktur aus, deren Virex-Richtlinien Sie ändern möchten. Sie können die Virex-Richtlinien über die Virex-Seiten und -Registerkarten im Detailfenster der ePolicy Orchestrator-Konsole ändern. Diese Seiten sind nahezu identisch mit den Seiten und Dialogfeldern, auf die Sie über die Virex-Benutzeroberfläche direkt zugreifen können. Ausführliche Informationen über diese Konfigurationsoptionen in Virex 7.6 finden Sie im *Virex-Produktthandbuch*.

Nachdem Sie die Richtlinie geändert und die Änderungen für den entsprechenden Computer oder die Gruppe von Computern gespeichert haben, können Sie die neuen Einstellungen über den ePolicy Orchestrator-Agenten weitergeben. [Siehe Richtlinien durchsetzen auf Seite 27](#).

**So ändern Sie Richtlinien für Virex im 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. Die Registerkarten **Richtlinien**, **Eigenschaften** und **Tasks** werden in der oberen Hälfte des Detailfensters angezeigt.
- 3 Wählen Sie die Registerkarte **Richtlinien** in der oberen Hälfte des Detailfensters aus, und erweitern Sie Virex. Unter dem Virex-Eintrag wird ein einziger Eintrag angezeigt.

**Abbildung 3-1 ePolicy Orchestrator-Konsole – Virex**

Das untere Fenster zeigt die Konfigurationsoptionen der Virex-Oberfläche an:

- Allgemein
  - eUpdate
  - Aktiver Scanner
  - Hintergrund-Scanner
  - Scanner für aktivierte Volumes
  - Bedarfsmäßiger Scanner
- 4 Wählen im unteren Detailfenster eine Option aus, z. B. **Allgemein**.
  - 5 Deaktivieren Sie auf der Seite **Allgemein** das Kontrollkästchen **Übernehmen**.
  - 6 Konfigurieren Sie die erforderlichen Optionen.



Diese Seiten sind identisch mit den Seiten in Virex. Im *Virex 7.6-Produkt*handbuch erfahren Sie mehr zu diesem Thema.

- 7 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern. Konfigurieren Sie weitere Richtlinien, und klicken Sie anschließend auf **Alle übernehmen**, um alle Richtlinien, die Sie konfiguriert haben zu übernehmen.

## Richtlinien durchsetzen

Nachdem Sie die Richtlinien konfiguriert haben, müssen Sie sie auf den Computern, auf denen Virex installiert ist, durchsetzen.

- 1 Wählen Sie in der Konsolenstruktur unter „Verzeichnis“ die Site, die Gruppe, den einzelnen Computer oder das gesamte Verzeichnis aus.
- 2 Wählen Sie im oberen Detailfenster zunächst die Registerkarte **Richtlinien** und anschließend **Virex** aus. Die **Virex**-Seite wird im unteren Detailfenster angezeigt.
- 3 Deaktivieren Sie **Übernehmen**.
- 4 Wählen Sie **Richtlinien für Virex 7.6 durchsetzen** aus.
- 5 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Die ePolicy Orchestrator-Software macht die Richtlinien, die Sie konfiguriert haben, für den ePolicy Orchestrator-Agenten auf den Virex-Computern verfügbar.



Abbildung 3-2 Richtlinien für Virex 7.6 durchsetzen

## Allgemein

Über die Registerkarte **Allgemein** können Sie allgemeine Richtlinien durchsetzen, die die generelle Funktionsweise von Virex 7.6 steuern, z. B. die automatische Suche nach Virusdefinitions-Aktualisierungen, das Scannen von lokalen Volumes bei deren Aktivierung, die Protokollierung von Scan-Ergebnissen, das Ausführen von Hintergrund-Scans und das Erstellen von Ausschlusslisten für bestimmte Volumes, Dateien und Ordner.

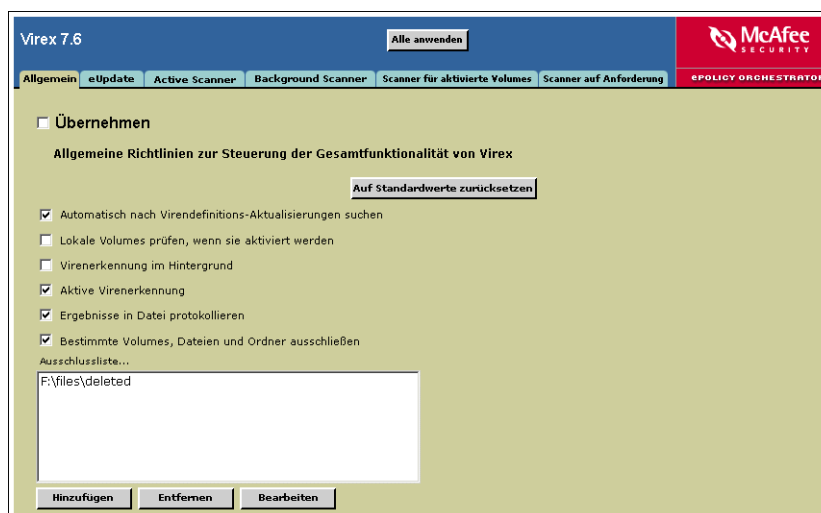


Abbildung 3-3 Registerkarte „Allgemein“

**Sie können die folgenden allgemeinen Richtlinien durchsetzen:**

Automatisch nach Virendefinitions-Aktualisierungen suchen	Aktiviert bzw. deaktiviert automatische eUpdates.
Lokale Volumes prüfen, wenn sie aktiviert werden	Aktiviert bzw. deaktiviert den Scanner für aktivierte Volumes.
Hintergrund-Virusentdeckung	Aktiviert bzw. deaktiviert den Hintergrund-Scanner.
Aktive Virusentdeckung	Aktiviert bzw. deaktiviert den aktiven Scanner.
Ergebnisse in Datei protokollieren	Aktiviert bzw. deaktiviert die Protokollierung der Ergebnisse in einer Datei.
Bestimmte Volumes, Dateien und Ordner ausschließen	<p>Mithilfe dieser Option können Sie Dateien oder Volumes vom Scan ausschließen. Die Ausnahmen werden in der Textdatei VShieldExclude.txt als Liste gespeichert. Wenn diese Option nicht aktiviert ist, wird keine Ausschlussliste verwendet.</p> <p>Ausschluss hinzufügen:</p> <ul style="list-style-type: none"> <li>■ Klicken Sie auf <b>Hinzufügen</b>. Der <b>Webseitendialog -- Scan-Objekt hinzufügen</b> wird angezeigt. Geben Sie den vollständigen Pfad der Datei, des Verzeichnisses oder des Volumes ein, die Sie ausschließen möchten, und klicken Sie auf <b>OK</b>. Die Ausnahmen werden in der <b>Ausschlussliste</b> aufgeführt.</li> </ul> <p>Ausschluss entfernen:</p> <ul style="list-style-type: none"> <li>■ Wählen Sie den Ausschluss aus der <b>Ausschlussliste</b> aus, und klicken Sie auf <b>Entfernen</b>.</li> </ul> <p>Ausschluss bearbeiten:</p> <ul style="list-style-type: none"> <li>■ Wählen Sie den Ausschluss aus der <b>Ausschlussliste</b> aus, und klicken Sie auf <b>Bearbeiten</b>, um den Ausschluss zu bearbeiten.</li> </ul>

## eUpdate

Mithilfe der Registerkarte **eUpdate** können Sie die Aktualisierungseinstellungen der DAT-Dateien und des Scan-Moduls an Ihre Erfordernisse anpassen. eUpdate sorgt dafür, dass Ihre Anti-Virus-Software laufend mit Informationen über Viren und mit Scan-Funktionen aktualisiert wird. Sie können Ihre DAT-Dateien und das Scan-Modul mit FTP oder HTTP aktualisieren.

**Abbildung 3-4 Registerkarte „eUpdate“**

## eUpdate-Einstellungen anpassen

Sie können die folgenden eUpdate-Einstellungen für Virex durchsetzen:

### FTP

FTP (File Transfer Protocol) dient zum Senden und Empfangen von Dateien über das Internet. Sie müssen die Serverdetails des Standortes angeben, von dem Sie Dateien auf Ihren Computer übertragen möchten, um Ihre DAT- und Engine-Dateien zu aktualisieren.

Server-URL	Geben Sie den URL des Servers an, von dem Sie DAT- und Engine-Aktualisierungen herunterladen möchten.
Port	Geben Sie die Portnummer an, die Sie für FTP verwenden möchten.
Benutzername	Geben Sie den Benutzernamen ein.
Kennwort	Geben Sie Ihr Kennwort ein.
Konto	Geben Sie Ihr FTP-Konto ein.
Verzeichnis	Geben Sie den Pfad zu Ihren DAT- und Engine-Dateien an.

### HTTP

HTTP (Hypertext Transfer Protocol) ist ein Satz von Regeln für die Übertragung von Dateien (Text, Graphiken, Sounds, Video und andere Multimediadateien) über das World Wide Web. Sie müssen den Server-URL angeben, von dem Sie Dateien auf Ihren Computer übertragen möchten, um Ihre DAT- und Engine-Dateien zu aktualisieren.

Server-URL	Geben Sie den URL des Servers an, von dem Sie DAT- und Engine-Aktualisierungen herunterladen möchten.
Benutzername	Geben Sie den Benutzernamen ein.
Kennwort	Geben Sie Ihr Kennwort ein.

## Aktiver Scanner

Der „Aktive Scanner“ ist eine Virex-Funktion, die die Festplatte ständig vor Viren aus dem Netzwerk oder dem Internet schützt. Da der aktive Scanner fortwährend arbeitet, besteht für Ihr System kein Infektionsrisiko.

Der aktive Scanner scannt Dateien, wenn sie auf Ihre Festplatte (alle Partitionen) und alle Wechselplattenlaufwerke geschrieben werden. Er wird beim Starten des Computers gestartet und so lange ausgeführt, bis der Computer heruntergefahren wird. Der Scanner wird standardmäßig auf Ihrem Computer ausgeführt. Sie können festlegen, wonach der Scanner sucht und wie er auf infizierte Dateien reagiert.

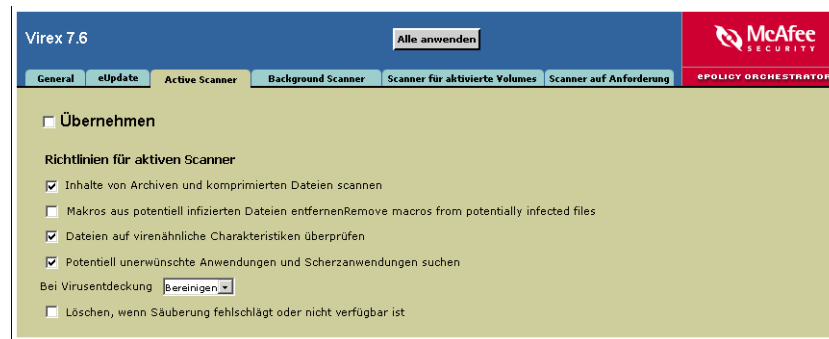


Abbildung 3-5 Registerkarte „Aktiver Scanner“

Sie können die folgenden Richtlinien für den aktiven Scanner durchsetzen:

Inhalte von Archiven und komprimierten Dateien scannen	Mithilfe dieser Option können Sie festlegen, dass der ausgewählte Scanner Archive und andere komprimierte Dateien scannt. Standardmäßig für Hintergrund-Scanner und bedarfsmäßigen Scanner eingeschaltet.
Makros aus potentiell infizierten Dateien entfernen	Wenn eine infizierte Datei gefunden wird, werden im Rahmen ihrer Säuberung alle Makros für diese Datei entfernt.
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. Standardmäßig für Hintergrund-Scanner eingeschaltet.
Potentiell unerwünschte Anwendungen und Scherzprogramme suchen	Mithilfe dieser Option können Sie festlegen, dass der Scanner nach unerwünschten Anwendungen oder Scherzprogrammen sucht.
Wenn ein Virus gefunden wurde:	Legt die primäre Aktion des Scanners fest.
<ul style="list-style-type: none"> <li>■ Bereinigen</li> <li>■ Löschen</li> <li>■ Benachrichtigen</li> </ul>	
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 die Säuberung als primäre Aktion festgelegt wurde.

## Hintergrund-Scanner

Der Hintergrund-Scanner ist eine Funktion, die alle Dateien auf Ihrem System fortwährend scannt. Dieser Scanner schützt Ihr System, indem er es ständig auf infizierte Dateien scannt. Dieser Scan erfordert nur wenige Ressourcen, sodass die Leistung Ihres Computers während des Scannens nicht beeinträchtigt wird. Sie können festlegen, wonach der Scanner sucht und wie er auf infizierte Dateien reagiert.

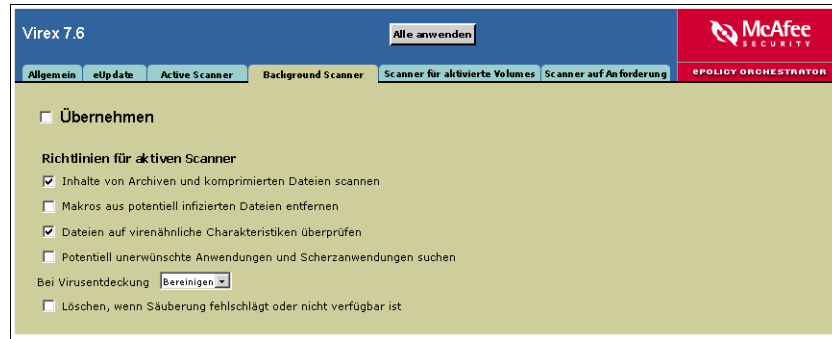


Abbildung 3-6 Registerkarte „Hintergrund-Scanner“

Sie können die folgenden Richtlinien für den Hintergrund-Scanner durchsetzen:

Inhalte von Archiven und komprimierten Dateien scannen	Mithilfe dieser Option können Sie festlegen, dass der ausgewählte Scanner Archive und andere komprimierte Dateien scannt. Standardmäßig für Hintergrund-Scanner und bedarfsmäßigen Scanner eingeschaltet.
Makros aus potentiell infizierten Dateien entfernen	Wenn eine infizierte Datei gefunden wird, werden im Rahmen ihrer Säuberung alle Makros für diese Datei entfernt.
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. Standardmäßig für Hintergrund-Scanner eingeschaltet.
Potentiell unerwünschte Anwendungen und Scherzprogramme suchen	Mithilfe dieser Option können Sie festlegen, dass der Scanner nach unerwünschten Anwendungen oder Scherzprogrammen sucht.
Wenn ein Virus gefunden wurde:	Legt die primäre Aktion des Scanners fest.
<ul style="list-style-type: none"> <li>■ Bereinigen</li> <li>■ Löschen</li> <li>■ Benachrichtigen</li> </ul>	
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 die Säuberung als primäre Aktion festgelegt wurde.

## Scanner für aktivierte Volumes

Der Scanner für aktivierte Volumes initiiert das Scannen von Volumes, z. B. von CDs oder Kameras, wenn sie lokal aktiviert werden. Mithilfe dieses Scanners können Sie ein großes Volume oder Gerät auf Viren scannen, bevor Sie es mit Ihrem System verbinden. Dies schränkt die Anfälligkeit Ihres Systems gegenüber Viren ein. Die Funktion funktioniert nur mit lokal eingelegten Medien oder Wechselmedien wie ZIP-Laufwerken, CDs, DVDs oder OS X .DMG-Dateien. Der Scanner scannt auch USB-Geräte, wie Pen Drives und Kameras, oder Firewire-Geräte, wie iPod. Volumes auf Geräten, die über das Internet verbunden sind, werden nicht gescannt. Der Scanner wird im Hintergrund ausgeführt und interagiert mit dem Benutzer.

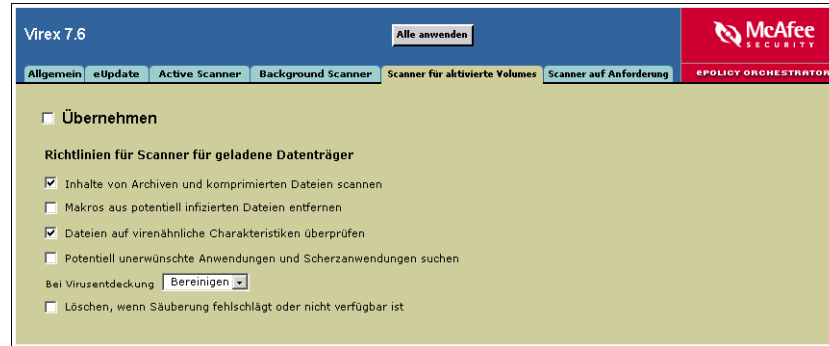


Abbildung 3-7 Scanner für aktivierte Volumes

Sie können die folgenden Richtlinien für den Scanner für aktivierte Volumes durchsetzen:

Inhalte von Archiven und komprimierten Dateien scannen	Mithilfe dieser Option können Sie festlegen, dass der ausgewählte Scanner Archive und andere komprimierte Dateien scannt.
Makros aus potentiell infizierten Dateien entfernen	Wenn eine infizierte Datei gefunden wird, werden im Rahmen ihrer Säuberung alle Makros für diese Datei entfernt.
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.
Potentiell unerwünschte Anwendungen und Scherzprogramme suchen	Mithilfe dieser Option können Sie festlegen, dass der Scanner nach unerwünschten Anwendungen oder Scherzprogrammen sucht.
Wenn ein Virus gefunden wurde:	Legt die primäre Aktion des Scanners fest.
<ul style="list-style-type: none"> <li>■ Bereinigen</li> <li>■ Löschen</li> <li>■ Benachrichtigen</li> </ul>	
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 die Säuberung als primäre Aktion festgelegt wurde.



Der Scanner für aktivierte Volumes läuft nicht standardmäßig auf Ihrem Computer.



## Bedarfsmäßiger Scanner

Mithilfe des bedarfsmäßigen Scanners können Sie Viren-Scans jederzeit starten, indem Sie ausgewählte Dateien in die Konsole ziehen und dort ablegen oder sie im Dialogfeld zum **Öffnen** von Dateien öffnen. Sie können im bedarfsmäßigen Scanner mehrere Dateien, Ordner und Volumes auswählen. Die Scan-Ergebnisse werden in einem Bericht angezeigt, der gespeichert oder gedruckt werden kann. Sie können festlegen, wonach der Scanner sucht und wie er auf infizierte Dateien reagiert. Sie können auch eine Ausschlussliste konfigurieren, die vom aktiven Scanner, dem Hintergrund-Scanner und dem Scanner für aktivierte Volumes verwendet wird. Der Scanner benachrichtigt Sie, wenn er einen Virus findet und generiert ein Protokoll, in dem die durchgeführten Aktionen aufgezeichnet werden.

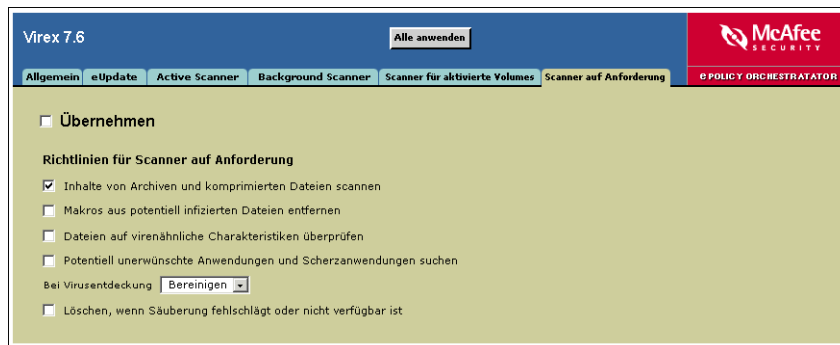


Abbildung 3-8 Registerkarte „Bedarfsmäßiger Scanner“

**Sie können die folgenden Richtlinien für den bedarfsmäßigen Scanner durchsetzen:**

Inhalte von Archiven und komprimierten Dateien scannen	Mithilfe dieser Option können Sie festlegen, dass der ausgewählte Scanner Archive und andere komprimierte Dateien scannt. Standardmäßig für den bedarfsmäßigen Scanner eingeschaltet.
Makros aus potentiell infizierten Dateien entfernen	Wenn eine infizierte Datei gefunden wird, werden im Rahmen ihrer Säuberung alle Makros für diese Datei entfernt.
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.
Potentiell unerwünschte Anwendungen und Scherzprogramme suchen	Mithilfe dieser Option können Sie festlegen, dass der Scanner nach unerwünschten Anwendungen oder Scherzprogrammen sucht.
Wenn ein Virus gefunden wurde:	Legt die primäre Aktion des Scanners fest.
<ul style="list-style-type: none"> <li>■ Bereinigen</li> <li>■ Löschen</li> <li>■ Benachrichtigen</li> </ul>	
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 die Säuberung als primäre Aktion festgelegt wurde.

## Planen von Scans und eUpdates

Wenn Virex nach Viren sucht, verwendet es Informationen aus der „Virusdefinitionsdatei“ (DAT-Datei), um Viren zu finden und zu entfernen. Jeden Tag werden viele neue Viren entdeckt, und wir erstellen regelmäßig neue DAT-Dateien, um vor diesen Viren zu schützen. Um den besten Anti-Virus-Schutz zu gewährleisten, können Sie Virex mithilfe von ePolicy Orchestrator darüber informieren, wo die aktuellsten DAT-Dateien zu finden sind. Außerdem können Sie mit dem ePolicy Orchestrator Pläne für das Ersetzen älterer DAT-Dateien und das Ausführen von Scans auf Anforderung erstellen.

## Informationen über geplante Tasks

Mit dem ePolicy Orchestrator können Sie die folgenden geplanten Tasks für die Virex-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. ePolicy Orchestrator kann jedoch nicht den Fortschritt der Tasks kontrollieren, weshalb wir empfehlen, dass Sie sich von Zeit zu Zeit das Protokoll auf dem Server anschauen.

## Scan auf Anforderung

Virex kann Ihre Dateien auf Anforderung scannen, so dass alle Dateien in der Datenbank auf fragwürdigen Inhalt geprüft werden. Sie können beliebig viele Pläne für bedarfsmäßige Scans erstellen. Die geplanten Scans können so konfiguriert werden, dass sie in bestimmten Intervallen durchgeführt werden und jederzeit vom Benutzer ausgeführt werden können. Sie können Pläne deaktivieren, die nicht automatisch ausgeführt werden sollen.

## Neuen Task erstellen

### So erstellen Sie einen neuen Task:

- 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.

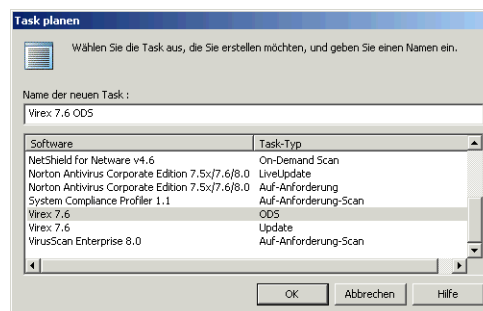


Abbildung 3-9 Geplante Tasks

- Geben Sie einen Namen für den Task im Feld **Neuer Task-Name** ein und wählen Sie den Task aus, den Sie erstellen möchten. Wählen Sie aus der Dropdownliste **Task-Typ** die Option **Scan auf Anforderung** aus. Klicken Sie auf **OK**.

- Die erstellte Task wird im **Tasks**-Fenster angezeigt.

Verzeichnis							
Richtlinien	Eigenschaften	Tasks					
Task-Name	Zuletzt bearbeitet bei	Erstellt bei	Aktiviert	Planungstyp	Anfangsdatum	Startzeit	
Deployment	Verzeichnis	Verzeichnis	Nein	Täglich	02.02.2005	00:00:00 (Ortszeit)	
Update Virex 7.6	Verzeichnis	Verzeichnis	Nein	Täglich	02.02.2005	12:14:00 (Ortszeit)	
Virex 7.6 ODS	Verzeichnis	Verzeichnis	Nein	Täglich	02.02.2005	12:16:00 (Ortszeit)	

Abbildung 3-10 Registerkarte „Tasks“

## Task bearbeiten

### So bearbeiten Sie eine Task:

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

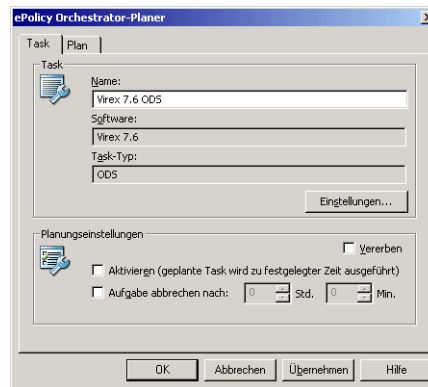


Abbildung 3-11 ePolicy Orchestrator Scheduler – Registerkarte „Task“

- Klicken Sie auf **Einstellungen**, um Dateien und das Verzeichnis in den geplanten Scan einzubeziehen. *Siehe Bedarfsmäßiger Scanner auf Seite 33.*

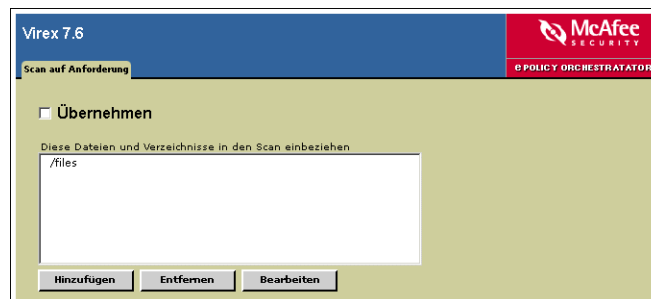


Abbildung 3-12 Scan auf Anforderung – Dateien und Verzeichnisse einbeziehen



Heben Sie die Auswahl von **Übernehmen** aus, und wählen Sie **Aktivieren (der geplante Task wird zur festgelegten Zeit ausgeführt)**, um die Task-Einstellungen im Fenster **Zeitplan-Einstellungen** zu aktivieren.

Beziehen Sie diese Dateien und Verzeichnisse in den Scan ein.	<p>Mithilfe dieser Option können Sie Dateien oder Volumes in den Scan einbeziehen.</p> <p>Aufnahme hinzufügen:</p> <ul style="list-style-type: none"> <li>■ Klicken Sie auf <b>Hinzufügen</b>. Der <b>Webseitendialog -- Scan-Objekt hinzufügen</b> wird angezeigt. Geben Sie den vollständigen Pfad der Datei, des Verzeichnisses oder des Volumes ein, die Sie einbeziehen möchten, und klicken Sie auf <b>OK</b>. Die Aufnahme wird in der <b>Aufnahmeliste</b> angezeigt.</li> </ul> <p>Aufnahme entfernen:</p> <ul style="list-style-type: none"> <li>■ Wählen Sie die Aufnahme aus der <b>Aufnahmeliste</b> aus, und klicken Sie auf <b>Entfernen</b>.</li> </ul> <p>Aufnahme bearbeiten:</p> <ul style="list-style-type: none"> <li>■ Wählen Sie die Aufnahme aus der <b>Aufnahmeliste</b> aus, und klicken Sie auf <b>Bearbeiten</b>. Der <b>Webseitendialog -- Scan-Objekt</b> wird angezeigt. Ändern Sie den gesamten Pfad der Datei oder des Verzeichnisses, das Sie in den Scan einbeziehen möchten, und klicken Sie auf <b>OK</b>.</li> </ul>
---	--

### Zeitplan-Einstellungen

Aktivieren (der geplante Task wird zur festgelegten Zeit ausgeführt)	Wählen Sie diese Option aus, um einen Task zu einer bestimmten Zeit auszuführen.
Task stoppen, wenn er länger läuft als:	Legen Sie die Stunden und Minuten fest, nach deren Überschreitung ein Task abgebrochen werden soll.

### Registerkarte „Zeitplan“

Beim Planen eines Task gibt es viele Optionen.

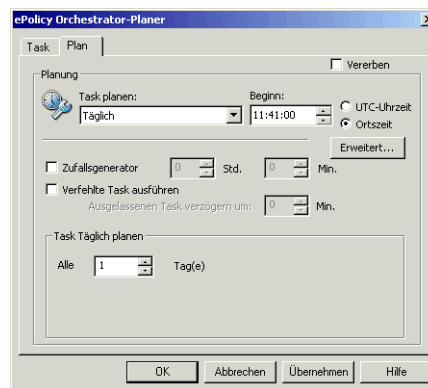


Abbildung 3-13 ePolicy Orchestrator Scheduler – Registerkarte „Zeitplan“

Task planen	<p>Wählen Sie den Task-Typ aus dem Dropdownmenü aus. Sie können eine der folgenden Optionen auswählen:</p> <ul style="list-style-type: none"> <li>■ Täglich</li> <li>■ Wöchentlich</li> <li>■ Monatlich</li> <li>■ Einmal</li> <li>■ Beim Systemstart</li> <li>■ Sofort ausführen</li> </ul>
Anfangszeit ■ UTC-Zeit ■ Ortszeit	<p>Legen Sie die Anfangszeit des Zeitplans fest. Wählen Sie die Ortszeit aus, um den Task mit dem geplanten Intervall zur Systemzeit des Clientcomputers auszuführen. Diese Option ist nützlich, um prozessorintensive Tasks (z. B. bedarfsmäßige Scans) außerhalb der Geschäftszeiten zu planen.</p> <p>Wenn Sie UTC auswählen, wird der Task zur UTC-Zeit (Universal Time Conversion, auch bekannt als GMT oder Greenwich Mean Time) ausgeführt. Mit dieser Option wird der Task auf allen Ihren Macintosh-Clients zur selben Zeit ausgeführt, unabhängig von der Ortszeit des Macintosh-Systems.</p>
Zufallsausführung aktivieren	Der Task wird nicht genau zur festgelegten Anfangszeit ausgeführt, sondern beginnt sie 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 nicht zur geplanten Anfangszeit verfügbar war. Wählen Sie diese Option, um den Task auszuführen, wenn der Macintosh-Computer das nächste Mal verfügbar ist.
Verpassten Task verschieben um	Klicken Sie im Dialogfeld <b>Erweiterte Zeitplanoptionen</b> auf <b>Erweitert</b> . Wenn Sie diese Option auswählen, wird der verpasste Task mit Verzögerung ausgeführt, nachdem der Macintosh-Computer wieder verfügbar ist.
Anfangsdatum / Enddatum	Klicken Sie im Dialogfeld <b>Erweiterte Zeitplanoptionen</b> auf <b>Erweitert</b> . Geben Sie das Anfangs- und Enddatum ein, wenn der Task auf temporärer Basis nur innerhalb eines bestimmten Zeitraumes über mehrere Tage oder Wochen ausgeführt werden soll.
Task wiederholen	<p>Klicken Sie im Dialogfeld <b>Erweiterte Zeitplanoptionen</b> auf <b>Erweitert</b>. Verwenden Sie diese Option, um einen Task am selben Tag mehrfach auszuführen. Wählen Sie dazu die Option Task <b>Wiederholen</b> aus, und legen Sie das entsprechende Wiederholungsintervall fest.</p> <p>Im Normalfall wird diese Option dazu verwendet, um einen Client-Aktualisierungs-Task mehrere Male am Tag auszuführen, insbesondere dann, wenn viele neue Viren aufgetaucht sind. Sie können den Task auch so planen, dass er während anderer Intervalle, z. B. wöchentlichen oder monatlichen Intervallen, wiederholt wird.</p>
Task täglich planen	Legen Sie das Intervall für die Ausführung von geplanten Tasks fest. Dieses Intervall kann 1 oder mehrere Tage sein. Wenn Sie 1 wählen, wird der geplante Task jeden zweiten Tag ausgeführt.

## Task löschen

### So löschen Sie einen Task:

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

## eUpdate

Wenn Virex (entsprechend Ihrer Einstellungen) einen Scan durchführt, verwendet es sein Anti-Virus-Scan-Modul und die aktuellen Virusdefinitionsdateien (DAT-Dateien), um Viren zu finden und zu entfernen. Jeden Tag werden viele neue Viren entdeckt, und wir erstellen regelmäßig neue DAT-Dateien, um vor diesen Viren zu schützen. Ihre Anti-Virus-Software kann Sie nur dann umfassend schützen, wenn Sie laufend mit den aktuellsten DAT-Dateien und Scan-Modulen aktualisiert wird. Wir empfehlen, dass Sie die Virex-DAT-Dateien mindestens einmal wöchentlich aktualisieren und regelmäßig die McAfee AVERT (Anti-Virus Emergency Response Team)-Website nach neuen DAT-Dateien überprüfen. Wenn Sie in der aktuellen Domäne mehrere Server haben (die alle Virex ausführen), können Sie einen Server zum Herunterladen der aktuellsten 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 benutzen.

### Speicherort der DAT-Dateien angeben

Sie können die Quelle der DAT-Dateien mithilfe der eUpdate-Seite angeben. [Siehe eUpdate-Einstellungen anpassen auf Seite 29.](#)

### eUpdate-Task erstellen

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

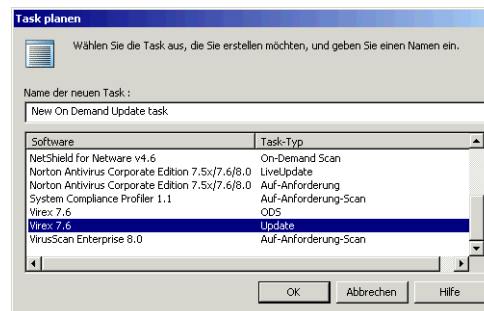


Abbildung 3-14 Neuer Aktualisierungs-Task

- 2 Geben Sie im Dialogfeld **Task planen** einen Namen in das Feld **Neuer Task-Name** ein.
- 3 Wählen Sie **Virex 7.6 – Update** aus der **Software/Task-Typ**-Liste aus.
- 4 Klicken Sie auf **OK**, um den Task zu erstellen.

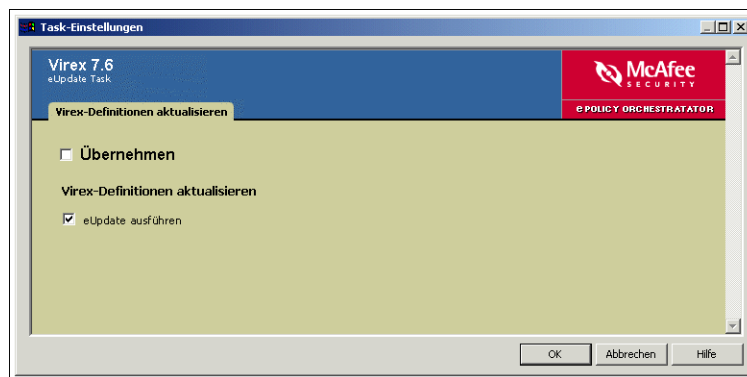
## eUpdate-Task konfigurieren

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 Deaktivieren Sie **Übernehmen**. *Siehe Task bearbeiten auf Seite 35.*
- 3 Klicken Sie auf **OK**, um zum Dialogfeld **ePolicy Orchestrator Scheduler** zurückzukehren.
- 4 Hier finden Sie Informationen zum Löschen von Virex eUpdate-Tasks: *Siehe Task löschen auf Seite 37.*

## eUpdate-Task deaktivieren

- 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**, wenn Sie die Bearbeitung der erforderlichen Optionen – auf den Registerkarten **Task** und **Zeitplan** sowie im Dialogfeld **ePolicy Orchestrator Scheduler** – beendet haben. Die Seite **Virex eUpdate-Task-Einstellungen** wird angezeigt.



**Abbildung 3-15 Virex-Definitionen aktualisieren – eUpdate ausführen**

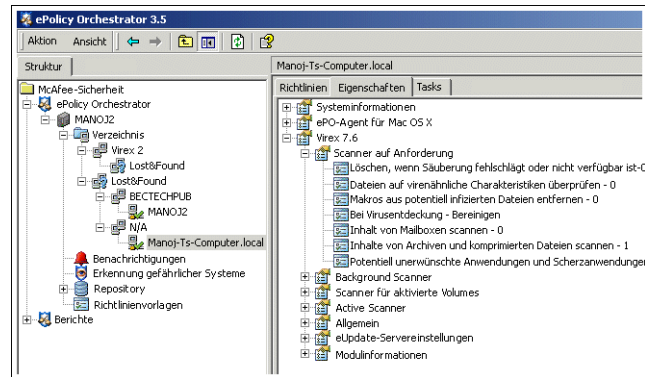
- 3 Deaktivieren Sie **Übernehmen** auf der Seite **Virex eUpdate-Task-Einstellungen**.
- 4 Deaktivieren Sie **eUpdate ausführen**, und wählen Sie anschließend **Übernehmen** aus.
- 5 Klicken Sie auf **OK**, um zum Dialogfeld **ePolicy Orchestrator Scheduler** zurückzukehren.
- 6 Hier finden Sie Informationen zum Löschen von Virex eUpdate-Tasks: *Siehe Task löschen auf Seite 37.*

## Anzeigender ePolicy Orchestrator-Servereigenschaften

Vom ePolicy Orchestrator-Server aus können Sie verschiedene Systemeigenschaften anzeigen.

**So zeigen Sie die Servereigenschaften an:**

- 1 Wählen Sie den Server, dessen Einstellungen Sie anzeigen möchten, aus der Konsolenstruktur aus.



**Abbildung 3-16 Konsolenstrukturverzeichnis**

- 2 Klicken Sie im oberen Fenster auf die Registerkarte **Eigenschaften**.
- 3 Erweitern Sie die **Virex 7.6**-Ordnerstruktur im **Eigenschaften**-Fenster, um ihre verschiedenen Eigenschaften aufzulisten.
- 4 Klicken Sie auf das **+** neben einer Eigenschaft, um ihre Details anzuzeigen.



# 4

## Entferntes Steuern des Agenten

---

### Anzeigen von Agenteneigenschaften

Sie können die aktuellen Eigenschaften eines bestimmten Computers mit Hilfe der ePolicy Orchestrator-Konsole anzeigen. Diese Eigenschaften enthalten grundlegende Systeminformationen, z. B. Betriebssystem, Netzwerk-IP-Adresse, RAM und Prozessorgeschwindigkeit. Sie zeigen außerdem die Eigenschaften des Agenten und der Anti-Virus-Sicherheitsprodukte von McAfee an, die auf diesem Computer installiert sind.

Insbesondere bei der Problemdiagnose ist es angebracht, die Computerrichtlinien zu überprüfen, um sicherzustellen, dass die Änderungen, die Sie in der Konsole vorgenommen haben, auch tatsächlich auf dem Macintosh-Client durchgesetzt werden. Der Agent sendet bei jedem Agent-Server-Kommunikationsintervall (ASCI – Agent-to-Server-Communication Interval) Eigenschaften an den Server und ermöglicht Ihnen so, die Systemeigenschaften der Macintosh-Clientcomputer von der ePolicy Orchestrator-Konsole aus anzuzeigen.

#### **Was ist der Unterschied zwischen Eigenschaften und Richtlinien?**

Richtlinien sind Regeln, die Sie für den Agenten oder für bestimmte Produkte auf den Richtlinienseiten des ePolicy Orchestrator-Servers konfigurieren. Wenn der Agent diese Richtlinien auf dem Macintosh-Clientcomputer durchsetzt, werden sie zu Eigenschaften. Eigenschaften sind die Einstellungen, die tatsächlich auf dem Macintosh-Clientcomputer aktiv sind.

## Agenteneigenschaften anzeigen

So zeigen Sie die Eigenschaften an, die der Agent für ausgewählte Computer im Verzeichnis sammelt:

- 1 Wählen Sie in der Konsolenstruktur den Computer aus, auf dem Virex installiert ist.
- 2 Klicken Sie in der oberen Hälfte des rechten Detailfensters auf die Registerkarte **Eigenschaften**, um die Eigenschaften des ausgewählten Computers anzuzeigen.

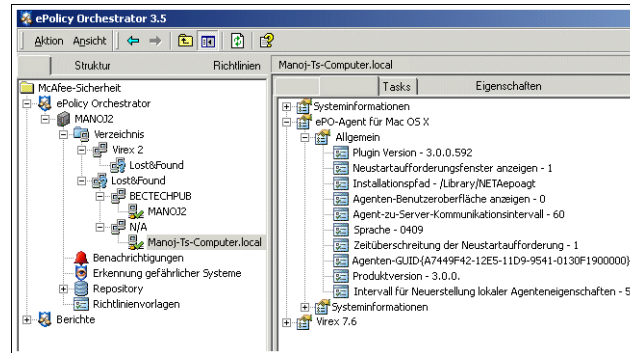


Abbildung 4-1 Agenteneigenschaften anzeigen

- 3 Erweitern Sie die Eigenschaftstypen, um die Details bestimmter Eigenschaften anzuzeigen. Die Eigenschaften des Agenten befinden sich unter dem ePolicy Orchestrator-Agenten.

## Durchsetzen von Richtlinien für den ePolicyOrchestrator-Agenten

Nachdem Sie die Richtlinien konfiguriert haben, müssen Sie sie durchsetzen, um sie für den ePolicy Orchestrator-Agenten auf den Virex-Hosts verfügbar zu machen.

Wählen Sie in der ePolicy Orchestrator-Konsole die Hosts aus, für die Sie Richtlinien durchsetzen möchten.

- 1 Wählen Sie im oberen Detailfenster **ePO-Agent für Mac OS X** aus.

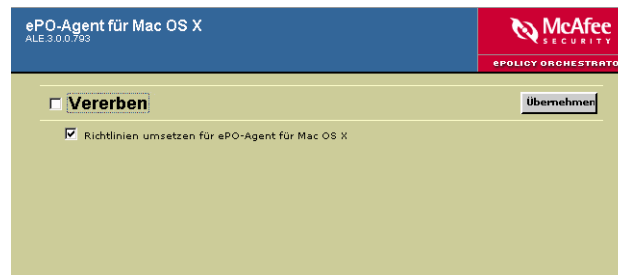


Abbildung 4-2 Durchsetzen von Richtlinien für den ePolicy Orchestrator-Agenten für Mac OS X

- 2 Deaktivieren Sie **Übernehmen**.
- 3 Wählen Sie **Durchsetzen von Richtlinien für den ePolicy Orchestrator-Agenten für Mac OS X** aus.
- 4 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern. Die ePolicy Orchestrator-Software macht die Richtlinien, die Sie konfiguriert haben, für den Agenten auf den Virex-Hosts verfügbar.

## Agentenoptionen

Der Agent ist die verteilte Komponente von ePolicy Orchestrator, die auf jedem Macintosh-Computer in Ihrem Netzwerk installiert ist. Dieser Agent sammelt und sendet Informationen zwischen dem ePolicy Orchestrator-Server, den Repositories und den verwalteten Clientcomputern und -produkten. Von der Konfigurierung des Agenten und seiner Richtlinien hängt es ab, wie er funktioniert und die Kommunikation und Aktualisierung in Ihrer Umgebung unterstützt.

### So konfigurieren Sie die Agentenrichtlinie für einen Computer:

- 1 Wählen Sie in der ePolicy Orchestrator-Konsolenstruktur den Computer aus, den Sie für Virex hinzugefügt haben.
- 2 Wählen Sie auf der Registerkarte **Richtlinien** (im oberen Detailfenster) die Option **Konfiguration** unter dem Eintrag **ePO-Agent für Mac OS X** aus. Die **Richtlinien**-Seite wird im unteren Detailfenster angezeigt.
- 3 Deaktivieren Sie auf der Registerkarte **Agentenoptionen** das Kontrollkästchen **Übernehmen**.



**Abbildung 4-3 ePolicy Orchestrator – Agentenoptionen**

- 4 Wählen Sie für das **Intervall für die Richtlinienumsetzung** ein Intervall (in Minuten) aus, dass den Anforderungen Ihres Unternehmens am besten entspricht. Der Standardwert ist 5 Minuten. Sie können einen Wert zwischen 5 und 10.080 Minuten (1 Woche) verwenden.
- 5 Wählen Sie unter **Agent-Server-Kommunikation (ASCI)** ein Intervall (in Minuten) aus, dass den Anforderungen Ihres Unternehmens am besten entspricht. Der Standardwert ist 60 Minuten. Sie können einen Wert zwischen 5 und 2.880 Minuten (2 Tage) verwenden.
- 6 Wenn Sie den ePolicy Orchestrator-Server dazu befähigen möchten, Wake-up-Calls an den Agenten zu senden, markieren Sie das Kontrollkästchen **Wake-up-Call-Unterstützung für Agenten aktivieren**.

## Ereignisse

Der ePolicy Orchestrator-Server empfängt Benachrichtigungen vom nicht auf Windows basierenden Agenten. Sie müssen die Richtlinienseite konfigurieren, um Ereignisse entweder sofort oder nur in Agent-Server-Kommunikationsintervallen an den ePolicy Orchestrator-Server weiterzuleiten.

Wenn Sie sich dazu entscheiden, Ereignisse sofort zu senden, dann werden alle Ereignisse mit einem Schweregrad, der gleich oder größer als der für den Agenten konfigurierte Wert ist, sofort weitergeleitet.

Wenn Sie sich dazu entscheiden, Ereignisse nicht sofort zu senden, dann leitet der Agent Ereignisse – unabhängig von deren Schweregrad – nur während der Agent-Server-Kommunikation weiter.

### So legen Sie die ePolicy Orchestrator-Agentenrichtlinie fest:

- 1 Melden Sie sich am ePolicy Orchestrator-Server an.
- 2 Wählen Sie das Verzeichnis, die gewünschte Site, Gruppe oder den Computer aus, und wählen Sie anschließend die Registerkarte **Richtlinien** im oberen Detailfenster.
- 3 Wählen Sie **ePolicy Orchestrator-Agent für Mac OS X | Konfiguration** im oberen Detailfenster aus.
- 4 Wählen Sie im unteren Detailfenster die Registerkarte **Ereignisse** aus.

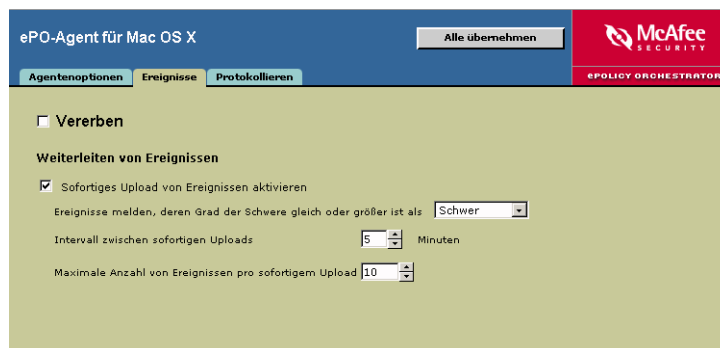


Abbildung 4-4 Registerkarte „Ereignisse“

- 5 Deaktivieren Sie **Übernehmen**.

Konfigurieren Sie die folgenden Richtlinienoptionen:

## Ereignisweiterleitung

Wählen Sie **Sofortigen Upload von Ereignissen aktivieren**, um den Agenten zu befähigen, Ereignisse sofort an den Server weiterzuleiten.

Deaktivieren Sie diese Option, um die Ereignisse erst beim nächsten ASCI weiterzuleiten. Wenn die Option aktiviert ist, müssen Sie Folgendes angeben:

- Den niedrigsten Schweregrad, ab dem Ereignisse an den Server gesendet werden sollen (unter „Melde alle Ereignissen mit einem <Schweregrad> größer oder gleich“). Sie können aus den folgenden Schweregraden auswählen: Kritisch, Hoch, Niedrig, Warnung oder Information. Wenn Sie beispielsweise „Niedrig“ auswählen, dann werden alle Ereignisse mit dem Schweregrad „Niedrig“ oder höher an den Server weitergeleitet.
  - Das Intervall zum Weiterleiten von Ereignissen (unter „Intervall zwischen sofortigen Uploads“). Die Zeitspanne, die Sie hier auswählen, bestimmt die höchste Frequenz, mit der Ereignisse weitergeleitet werden. Wenn Sie beispielsweise 5 Minuten auswählen, dann leitet der Agent Ereignisse höchstens alle fünf Minuten an den Server weiter.
  - Die maximale Zahl von Ereignissen, die gleichzeitig gesendet werden können (unter „Maximale Ereigniszahl pro sofortigem Upload“). Wenn die Zahl der Ereignisse diese Grenze überschreitet, dann werden die übrigen Ereignisse während des nächsten Intervalls zum Weiterleiten von Ereignissen gesendet.
- 6 Klicken Sie auf **Alle übernehmen**, um die Einstellungen zu speichern.  
Die Änderungen werden bei der nächsten Agent-Server-Kommunikation wirksam.

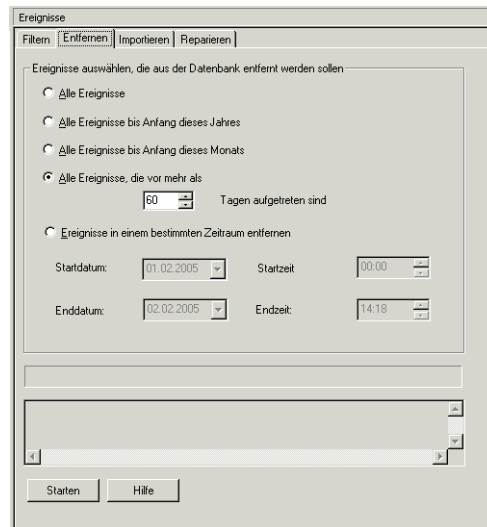
## Alte Ereignisse regelmäßig aus der Datenbank löschen

Sie können Ereignisse regelmäßig aus der Datenbank löschen, um die Größe der Datenbank gering zu halten und die Leistung zu verbessern. Viele Ereignisse sind nach gewisser Zeit weniger nützlich. Dies gilt insbesondere für informatorische Ereignisse und Ereignisse mit niedrigem Schweregrad. Außerdem können und sollten Sie eine Sicherungskopie der Datenbank erstellen, bevor Sie irgendwelche Ereignisse aus der Datenbank löschen. Sie können diese Datenbank archivieren und später, wenn nötig, zum Erstellen von Berichten verwenden.

Verwenden Sie die folgende Prozedur, um Ereignisse permanent aus der ePolicy Orchestrator-Datenbank zu löschen:

- 1 Melden Sie sich am gewünschten ePolicy Orchestrator-Datenbankserver an.

- 2 Wählen Sie in der Konsolenstruktur unter **Berichte | ePO-Datenbanken | <Datenbankserver> Ereignisse** aus. Die Registerkarten **Filter**, **Import**, **Reparatur** und **Entfernen** werden im Detailfenster angezeigt.



**Abbildung 4-5 Ereignisse – Registerkarte „Entfernen“**

- 3 Klicken Sie auf die Registerkarte **Entfernen**.
- 4 Wählen Sie die Ereignisse aus, die Sie aus der Datenbank entfernen möchten.
- **Alle Ereignisse** – Wählen Sie diese Option, um alle Ereignisse aus der Datenbank zu entfernen.
  - **Alle Ereignisse bis zum Jahresbeginn** – Wählen Sie diese Option, um alle Ereignisse vor dem Beginn des aktuellen Kalenderjahrs zu entfernen.
  - **Alle Ereignisse bis zum Monatsbeginn** – Wählen Sie diese Option, um alle Ereignisse vor dem Beginn des aktuellen Monats zu entfernen.
  - **Alle Ereignisse, die länger als X Tage zurückliegen** – Wählen Sie diese Option, um alle Ereignisse zu entfernen, die länger zurückliegen als die von Ihnen angegebene Anzahl von Tagen.
  - **Ereignisse innerhalb eines bestimmten Zeitraumes entfernen** – Wählen Sie diese Option, um eine Zeitspanne festzulegen. Alle Ereignisse, die innerhalb dieser Zeitspanne aufgetreten sind, werden entfernt.
- 5 Klicken Sie auf **Start**, um die ausgewählten Ereignisse aus der Datenbank zu entfernen.

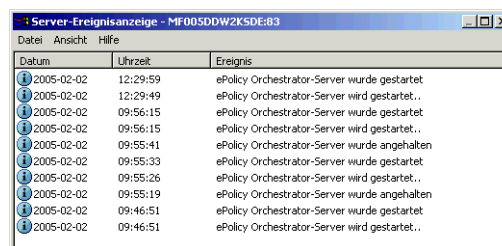
## Anzeigen von Serverereignissen

In der ePolicy Orchestrator-Konsole können Sie alle Informations-, Warnungs- und Fehlerereignisse für jeden ePolicy Orchestrator-Server anzeigen, speichern und drucken. Überprüfen Sie das Serverereignisfenster, um zu sehen, ob Aktionen, die vom Server aus initiiert wurden (z. B. die Verteilung von Agenten oder das Anfordern aktualisierter DAT-Dateien von einem Quell-Repository) erfolgreich waren oder gescheitert sind.

Außerdem können Sie verwalten, welche Ereignisse in der ePolicy Orchestrator-Datenbank gespeichert werden sollen. Siehe *ePolicy Orchestrator-Produkt Handbuch* zum Verwalten von ePolicy Orchestrator-Datenbanken und Ereignissen in Datenbanken.

### So können Sie Serverereignisse von der ePolicy Orchestrator-Konsole aus anzeigen, speichern oder drucken:

- 1 Melden Sie sich am ePolicy Orchestrator-Server an.
- 2 Wählen Sie in der Konsolenstruktur unter ePolicy Orchestrator den Serverknoten aus, und klicken Sie anschließend auf die Registerkarte **Allgemein** im Detailfenster.
- 3 Klicken Sie auf **Serverereignisse**, um das Dialogfeld **Serverereignis-Anzeige** zu öffnen.



Datum	Uhrzeit	Ereignis
2005-02-02	12:29:59	ePolicy Orchestrator-Server wurde gestartet
2005-02-02	12:29:49	ePolicy Orchestrator-Server wird gestartet..
2005-02-02	09:56:15	ePolicy Orchestrator-Server wurde gestartet
2005-02-02	09:56:15	ePolicy Orchestrator-Server wird gestartet..
2005-02-02	09:55:41	ePolicy Orchestrator-Server wurde angehalten
2005-02-02	09:55:33	ePolicy Orchestrator-Server wurde gestartet
2005-02-02	09:55:26	ePolicy Orchestrator-Server wird gestartet..
2005-02-02	09:55:19	ePolicy Orchestrator-Server wurde angehalten
2005-02-02	09:46:51	ePolicy Orchestrator-Server wurde gestartet
2005-02-02	09:46:51	ePolicy Orchestrator-Server wird gestartet..

Abbildung 4-6 Serverereignis-Anzeige

- 4 Wählen Sie **Ansicht | Aktualisieren** aus, um sicherzugehen, dass die Ereignisliste aktuell ist.

### Details eines bestimmten Ereignisses anzeigen

Um eine detaillierte Beschreibung eines Serverereignisses anzuzeigen, wählen Sie das gewünschte Ereignis aus, und öffnen Sie es mit einem doppelten Mausklick. Das Dialogfenster **Serverereignisdetails** wird angezeigt.

### Ereignisse in einer Protokolldatei speichern

Um alle Serverereignisse in einer Serverprotokolldatei (.log) zu speichern, wählen Sie **Datei | Speichern unter** aus. Wenn Sie nur ausgewählte Serverereignisse in einer Serverprotokolldatei speichern möchten, wählen Sie die gewünschten Ereignisse aus, und klicken Sie anschließend auf **Datei | Speichern unter**. Wählen Sie im Dialogfeld **Speichern unter** die Option **Nur ausgewählte Elemente** aus.

### Serverereignisse drucken

Um alle Serverereignisse auf dem Standarddrucker auszudrucken, klicken Sie auf **Drucken** im Menü **Datei**. Um nur ausgewählte Serverereignisse auf dem Standarddrucker auszudrucken, wählen Sie die gewünschten Ereignisse aus, und klicken Sie anschließend auf **Datei | Drucken**.

## Protokollierung

Der Agent auf dem Macintosh-Computer erzeugt während des Normalbetriebs ständig Software-Ereignisse. Dabei handelt es sich beispielsweise um informatorische Ereignisse über den normalen Betrieb, z. B. über das lokale Durchsetzen von Richtlinien oder den Start eines Scans auf Anforderung. Diese Ereignisse werden vom Agent protokolliert und bei jedem ASCII an den Server gesendet und in der Datenbank gespeichert. Ein typischer Einsatz von ePolicy Orchestrator kann in einem großen Netzwerk pro Stunde Tausende dieser Ereignisse erzeugen.

### So legen Sie die ePolicy Orchestrator-Protokollrichtlinie fest:

- 1 Melden Sie sich am ePolicy Orchestrator-Server an.
- 2 Wählen Sie das Verzeichnis, die gewünschte Site, Gruppe oder den Computer aus, und wählen Sie anschließend die Registerkarte **Richtlinien** im oberen Detailfenster.
- 3 Wählen Sie **ePolicy Orchestrator-Agent für Mac OS X | Konfiguration** im oberen Detailfenster aus.
- 4 Wählen Sie im unteren Detailfenster die Registerkarte **Protokollierung** aus.

Mit diesen Optionen können Sie die Richtlinien für die Protokollierung der Agentenaktivität konfigurieren.

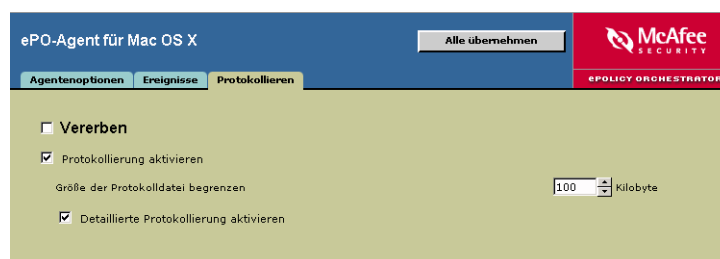


Abbildung 4-7 Registerkarte „Protokollierung“

Agentenrichtlinien protokollieren	Eigenschaftsbeschreibung
Protokollierung aktivieren	Wählen Sie aus, ob Sie die Protokollierung aktivieren möchten. Wenn Sie dieses Kontrollkästchen markieren, wird die Protokollierung unter /Library/NETAepoagt/Scratch/etc/log aktiviert.
Detaillierte Protokollierung aktivieren	Aktivieren Sie das detaillierte Agentenaktivitätsprotokoll agent_<computer>.log. Diese Protokolldatei kann sehr groß werden. Wir empfehlen Ihnen, die detaillierte Protokollierung zu aktivieren, da anderenfalls nur kritische Fehler protokolliert werden, die für die Diagnose spezifischer Kommunikationsprobleme möglicherweise unzureichend sind.



# 5

## Berichte

---

### Berichte

Über die ePolicy Orchestrator-Konsole können Sie die Konfiguration der Hosts überprüfen und Berichte darüber anzeigen, wie die Virex-Hosts Infektionen behandeln. Außerdem können Sie mit den Daten in der ausgewählten ePolicy Orchestrator-Datenbank, die vom nicht auf Windows basierenden Agenten übermittelt werden, Berichte erstellen. Sie können die Auswahl, die Sie in den Dialogfeldern **Berichtsinformationen eingeben** und **Berichtsdatenfilter** treffen, für die zukünftige Verwendung speichern.

#### Die Berichtsfunktion von ePolicy Orchestrator ermöglicht Ihnen Folgendes:

- Legen Sie einen Verzeichnisfilter fest, um nur die Informationen zu sammeln, die Sie anzeigen möchten. Beim Festlegen des 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 erscheinen sollen.
- Erzeugen Sie graphische 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 gewünschten Virex-Bericht unter **Berichte | ePO-Datenbanken | <Datenbankserver> | Berichte | <Berichtsgruppe>** in der Konsolenstruktur aus.
  - Wenn das Dialogfeld **Aktuelle Sicherheitsstandards** angezeigt wird, geben Sie die Versionsnummer der Virusdefinitionsdateien oder des Virus-Scan-Moduls ein, die Sie für die Berichterstellung verwenden möchten.
  - Wenn das Dialogfeld **Berichtsinformationen eingeben** angezeigt wird, treffen Sie eine Auswahl auf den Registerkarten, die angezeigt werden: **Regeln, Layout, Datengruppierung, Innerhalb, Gespeicherte Einstellungen**.



In Abhängigkeit vom ausgewählten Bericht können die Registerkarten variieren. Siehe *ePolicy Orchestrator-Produkthandbuch* für weitere Informationen zu den Registerkarten „Regeln“, „Layout“, „Gruppierung“, „Innerhalb“ und „Gespeicherte Einstellungen“.

- 3 Wählen Sie den Bericht (**Agentenversionen**) aus, den Sie erzeugen möchten, und legen Sie den Datenfilter im Dialogfeld **Berichtsdatenfilter** fest. Klicken Sie auf **OK**.
- 4 Der Bericht für **Agentenversionen** wird erzeugt.

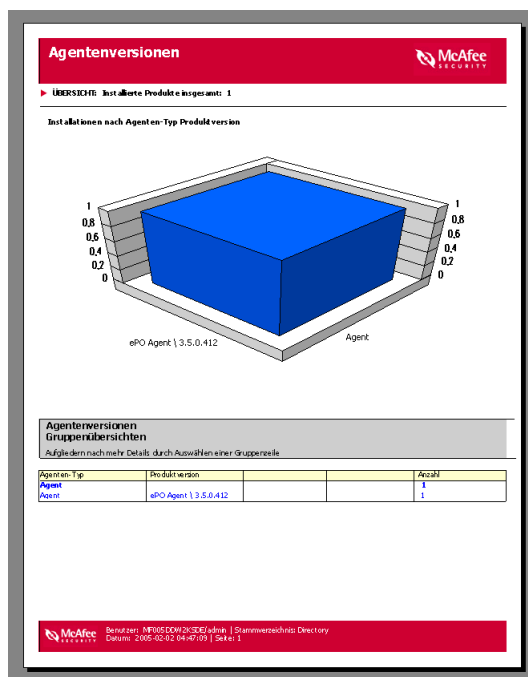


Abbildung 5-1 Beispielbericht – Agentenversionen

## Konfigurieren von Berichten

Es gibt verschiedene Möglichkeiten, um festzulegen, welche Daten in einem Bericht erscheinen sollen. Sie können die Versionsnummer der Virusdefinitionsdateien, des Virus-Scan-Moduls und der unterstützten Produkte definieren, die auf den Macintosh-Clientcomputern installiert werden müssen, damit sie mit den Anti-Virus- und Sicherheitsprogrammen Ihres Unternehmens kompatibel sind. Außerdem können Sie die Ergebnisse der Berichte durch ausgewählte Produktkriterien begrenzen (z. B. Computernamen, Betriebssystem, Virusname oder gegen infizierte Dateien eingeleitete Aktion).

Nachdem das Ergebnis eines Berichts angezeigt wird, können Sie verschiedene Tasks ausführen. Sie können die Details von ausgewählten Berichtsdaten anzeigen (z. B. um festzustellen, auf welchen Macintosh-Clientcomputern keine kompatible Version von Virex 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 Berichtsdaten in verschiedenen Dateiformaten (einschließlich HTML und Microsoft Excel) drucken oder exportieren.



Siehe *ePolicy Orchestrator-Produkthandbuch* für weitere Informationen zum Konfigurieren von Berichten.

# Glossar

## **Agenteninstallationspaket**

Das Setup-Programm und alle anderen Dateien, die zum Installieren des Agenten benötigt werden.

## **Agenten-Monitor**

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.

## **Agentensprachpakete**

Die Gruppe von Dateien, die an die Clientcomputer verteilt werden muss, damit die Benutzeroberfläche des Agenten in anderen Sprachen als Englisch angezeigt werden kann.

## **Agenten-Wake-up-Call**

Die Fähigkeit, die Agent-Server-Kommunikation vom Server aus zu initiieren.

Siehe auch *SuperAgent-Wake-up-Call*.

## **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 ( ASCI )**

Die Zeitspanne zwischen vordefinierten Agent-Server-Kommunikationen.

## **Alarm**

Eine Nachricht oder Benachrichtigung über Computeraktivität, z. B. die Entdeckung eines Virus. Diese kann je nach vordefinierter Konfiguration automatisch per E-Mail, Pager oder Telefon an Systemadministratoren und Benutzer gesendet werden.

Siehe auch *Alert Manager*.

## **ASCI (Agent Server Communication Interval)**

Siehe *Agent-Server-Kommunikationsintervall*.

## **Automatische Agentenaktualisierung**

Die automatische Aktualisierung des Agenten, sobald eine neuere Version auf dem ePolicy Orchestrator-Server verfügbar ist.

## **Automatische Installation**

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

## **Bereinigen**

Eine Maßnahme, die vom Scanner ergriffen wird, wenn er einen *Virus*, einen *Trojaner* oder einen *Wurm* entdeckt. Der Bereinigungsprozess 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; das Umbenennen einer Datei, die nicht gelöscht werden kann.

**Binärdateien (Setup-Dateien)**

Das Setup-Programm und alle anderen Dateien, die zum Installieren der Produkte benötigt werden.

**DAT-Dateien**

Virusdefinitionsdateien, auch Signaturdateien genannt, die der Anti-Virus-Software ermöglichen, Viren und anderen in Dateien eingebetteten, potentiell unerwünschten Code zu entdecken und entsprechend damit umzugehen.

Siehe auch *EXTRA.DAT-Datei*, *Inkrementelle DAT-Dateien* und *SuperDAT*.

**Detailfenster**

Das rechte Fenster der ePolicy Orchestrator-Konsole, das die Details des aktuell ausgewählten Konsolenstrukturelements anzeigt. In Abhängigkeit vom ausgewählten Konsolenstrukturelement kann das Detailfenster in ein oberes und ein unteres Fenster unterteilt sein.

Siehe auch *Oberes Detailfenster* und *Unteres Detailfenster*.

**durchsetzen, Durchsetzung**

Das Anwenden vordefinierter Einstellungen auf einem Clientcomputer in vorbestimmten Intervallen.

**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 und Produktversionsnummern) enthalten.

**ePolicy Orchestrator-Agent**

Ein Programm, das auf verwalteten Computern Hintergrundaufgaben ausführt, alle Anfragen zwischen dem ePolicy Orchestrator-Server und den Anti-Virus- und Sicherheitsprodukten auf diesen Computern vermittelt und dem Server Bericht über den Status dieses Tasks erstattet.

**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.

Siehe auch *ePolicy Orchestrator-Datenbankserver*.

**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, die zum entfernten Steuern und Überwachen verwalteter Computer verwendet wird.

Siehe auch *ePolicy Orchestrator-Remote-Konsole*.

**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.

Siehe auch *ePolicy Orchestrator-Konsole*.

**ePolicy Orchestrator-Server**

Die Back-End-Komponente der ePolicy Orchestrator-Software.

Siehe auch *ePolicy Orchestrator-Agent* und *ePolicy Orchestrator-Konsole*.

**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.

**Fehlerberichtsdiensprogramm**

Ein spezielles Dienstprogramm zum Verfolgen und Protokollieren von Fehlern in der McAfee-Software oder auf Ihrem System. Die so gewonnenen Informationen können zum Analysieren von Problemen verwendet werden.

**Gruppe**

Eine logische Sammlung 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 ihrer 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.

**Hinzufügen**

Das Hinzufügen von Dateien zum Master-Repository.

**Inaktiver Agent**

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

**Intervall für die Richtliniendurchsetzung**

Die Zeitspanne, während derer der Agent die Einstellungen durchsetzt, die er vom ePolicy Orchestrator-Server erhalten hat. Da diese Einstellungen lokal durchgesetzt werden, benötigt dieses Intervall keine Bandbreite.

**Konsolenstruktur**

Der Inhalt der Registerkarte **Struktur** im linken Fenster der ePolicy Orchestrator-Konsole. Sie zeigt die Elemente, die in der Konsole verfügbar sind.

**Konsolenstrukturelement**

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

**Lost&Found-Gruppe**

Eine Gruppe zum temporären Speichern von Computern, deren angemessene Stelle im **Verzeichnis** nicht bestimmt werden kann.

**Oberes Detailfenster**

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

**Protokolldatei**

Eine Aufzeichnung über die Aktivitäten einer Komponente der McAfee-Anti-Virus-Software. Protokolldateien zeichnen die während einer Installation oder des Scannens oder Aktualisierens von Aufgaben durchgeführten Aufgaben auf.

Siehe auch *Ereignisse*.

**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.

**Scan auf Anforderung**

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

Vergleiche mit *Scannen bei Zugriff*.

**Scan, scannen**

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

Siehe *Scannen bei Zugriff* und *Scan auf Anforderung*.

**Scan-Task**

Ein einzelnes Scan-Ereignis.

**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 Sammlung von Entitäten in der Konsolenstruktur, die zum Zweck einer einfacheren Verwaltung zusammengefasst wurden. Sites können Gruppen oder Computer enthalten und können nach ihren IP-Adressbereichen, ihren IP-Subnetzmasken, ihrem Speicherort, der Abteilung usw. organisiert werden.

**Sofortige Ereignisweiterleitung**

Das sofortige Senden von Ereignissen eines bestimmten Schweregrades oder höher 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 einzeln, z. B. *Scans auf Anforderung*, als auch routinemäßig, z. B. *Aktualisierungen*), die planmäßig zu einer bestimmten Zeit oder in bestimmten Intervallen durchgeführt wird.

Vergleiche mit *Richtlinie*.

**übernehmen, Übernahme**

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

**Unteres Detailfenster**

Das untere rechte Fenster der Konsole, in dem die Konfigurationseinstellungen für die Produkte angezeigt werden, die auf der Registerkarte **Richtlinien** im oberen Detailfenster aufgelistet sind.

Siehe auch *Detailfenster* und *Oberes Detailfenster*.

**UTC-Zeit**

Coordinated Universal Time (UTC). Dies bezieht sich auf den Null- oder Greenwichmeridian.

**Verteilte Software-Repositories**

Eine Sammlung von Websites oder Computern, die so in einem Netzwerk angeordnet sind, dass sie einen bandbreiteneffizienten Zugriff für die Clientcomputer bieten. In verteilten Repositories werden die Dateien gespeichert, die von Clientcomputern 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, das in der Lage ist, sich ohne oder nur mit geringer Benutzerintervention zu replizieren. Die replizierten Programme replizieren sich dann zudem weiter.

**Warnungspriorität**

Der Wert, den Sie jeder Warnung zu Informationszwecken zuweisen. Sie können Warnungen die Priorität **Kritisch**, **Hoch**, **Niedrig**, **Warnung** oder **Information** zuweisen.

**weitergeben, Weitergabe**

Das Verteilen und Installieren von Setup-Programmen auf Clientcomputern von einer zentralen Stelle aus.

**Wurm**

Ein Virus, der sich durch die Erzeugung von eigenen Duplikaten auf anderen Laufwerken, Systemen oder Netzwerken verbreitet.

**Zweig**

Verzeichnisse im Master-Repository, die Ihnen ermöglichen, verschiedene Versionen ausgewählter Aktualisierungen zu speichern und zu verteilen.

Siehe auch *Selektives Aktualisieren*.

# Index

## A

- Agent
  - anzeigen, Eigenschaften, [41](#)
  - durchsetzen, Richtlinien, [42](#)
  - installieren, [18](#)
    - automatische Installation, [22](#)
    - Befehlszeile, [22](#)
    - Standardinstallation, [18](#)
  - Optionen, [43](#)
  - Systemanforderungen, [13](#)
  - Verzeichnis, [17](#)
- Aktualisieren von
  - Anti-Virus-Software, [48](#)
- Aktualisierung, Website, [12](#)
- AVERT
  - Anti-Virus & Vulnerability Emergency Response Team, Kontakt, [12](#)
  - DAT Notification Service, [12](#)
  - WebImmune, [12](#)

## B

- Begriffsdefinitionen (*Siehe* Glossar)
- Berichte, [49](#)
  - konfigurieren, [50](#)
- Beta-Programm, Kontakt, [12](#)

## C

- Consulting Services, [12](#)

## D

- DAT-Datei
  - Aktualisierungen über den AVERT Notification Service, [12](#)
  - Aktualisierungen, Website, [12](#)
  - angeben, Speicherort, [38](#)
- Deinstallation
  - ePO-Agent vom ePO-Server entfernen, [24](#)
  - ePO-Agenten unter OS X entfernen, [24](#)
  - Virex NAP vom ePO-Server entfernen, [23](#)
- Dokumentation des Produkts, [8](#)
- Download-Website, [12](#)

## E

- ePolicy Orchestrator
  - Servereigenschaften, [40](#)
- Ereignisse, [44](#)
  - Anzeigen von Serverereignissen, [47](#)
  - löschen, Ereignisse, [45](#)
- eUpdate, [28](#)
  - deaktivieren, [39](#)
  - erstellen, [38](#)
  - FTP, [29](#)
  - HTTP, [29](#)
  - konfigurieren, [39](#)

## F

- Festlegen von Richtlinien
  - aktiver Scanner, [29](#)
  - aktivierte Volumes, Scanner, [32](#)
  - allgemein, [27](#)
  - bedarfsmäßiger Scanner, [33](#)
  - ePolicy Orchestrator, [25](#)
  - Hintergrund-Scanner, [31](#)

## G

- Glossar, [51](#)

## H

- Handbücher, [8](#)

## I

- Informationsquellen, [8](#)
  - im Produkt, [9](#)
  - Kontaktliste, [12](#)
- Informationsressourcen, [8](#)

## K

- Kontakt zu McAfee, [12](#)
- Kundendienst, Kontakt, [12](#)

## L

- Links zu Ressourcen im Produkt, [9](#)

## M

- McAfee University, Kontakt, [12](#)

## N

- NAP-Dateien
  - hinzufügen, [14](#)
  - Hinzufügen eines Nicht-Windows-Agenten, [14](#)
  - hinzufügen, Bericht-NAP-Datei, [16](#)
  - hinzufügen, Virex NAP-Datei, [15](#)
  - wo finde ich die NAP-Dateien, [14](#)
- Notification Service, DAT-Aktualisierungen, [12](#)

## P

- Planen von Scans und eUpdates, [34](#)
- PrimeSupport, [12](#)
- Produktdokumentation, [8](#)
- Produktinformationen, Ressourcen, [8](#)
- Produktschulung, vor Ort, [12](#)
- Protokollierung, [48](#)

## S

- Schulung, vor Ort, [12](#)
- Schulungs-Website, [12](#)
- Serverkomponenten, [14](#)
- Service Portal, PrimeSupport, [12](#)
- Sicherheitszentrale, Kontakt zu AVERT, [12](#)

## T

- Task
  - bearbeiten, [35](#)
  - löschen, [37](#)
- Technischer Support
  - Kontaktinformationen, [12](#)
  - Zugriff vom Produkt aus, [10](#)

## V

- Verwenden dieses Handbuchs
  - Schriftbildkonventionen und Symbole, [7](#)
- Virus Information Library, [9, 12](#)
- Virus, Beispiel weiterleiten
  - Website, [12](#)
- Vor Ort, Schulung, [12](#)

**W**

WebImmune, [12](#)

Weiterleiten, Virusbeispiel, [12](#)

**Z**

Zielgruppe des Handbuchs, [7](#)