

# VirusScan® ASaP



## COPYRIGHT

© 2003 Networks Associates Technology, Inc. Alle Rechte vorbehalten. Diese Veröffentlichung darf in keiner Weise und in keiner Form ohne die schriftliche Genehmigung von Networks Associates Technology, Inc. oder ihren Lieferanten und angeschlossenen Unternehmen vollständig oder teilweise vervielfältigt, übertragen, kopiert, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden. Diese Genehmigung können Sie schriftlich bei der Rechtsabteilung von Network Associates unter der folgenden Adresse beantragen: 5000 Headquarters Drive, Plano, Texas 75024. Oder rufen Sie uns an unter: +1-972-963-8000.

## MARKENHINWEISE

*Active Firewall, Active Security, Active Security (in Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware und das Logo, AVERT, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert und das Logo, Covert, Design (stilisiertes N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon's, die Dr Solomon's-Marke, Enterprise SecureCast, Enterprise SecureCast (in Katakana), ePolicy Orchestrator, Event Orchestrator (in Katakana), EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (in Katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, LANGuru, LANGuru (in Katakana), M und das Logo, Magic Solutions, Magic Solutions (in Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (in Katakana), McAfee und das Logo, McAfee.com, MultiMedia Cloaking, Net Tools, Net Tools (in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, NetStalker, Network Associates, Network Policy Orchestrator, NetXray, NotesGuard, nPO, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PortalShield, Powered by SpamAssassin, PrimeSupport, Recoverkey, Recoverkey – International, Registry Wizard, Remote Desktop, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (in Hangul), SpamKiller, SpamAssassin, Stalker, SupportMagic, ThreatScan, TIS, TMEG, Total Network Security, Total Network Visibility, Total Network Visibility (in Katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (in Katakana), WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000 und Zip Manager* sind eingetragene Marken von Network Associates, Inc. bzw. der angeschlossenen Tochterunternehmen in den USA und/oder anderen Ländern. Sniffer<sup>®</sup>-Markenprodukte werden ausschließlich von Network Associates, Inc. hergestellt. Alle weiteren geschützten und ungeschützten Marken in diesem Dokument sind das alleinige Eigentum ihrer jeweiligen Inhaber.

Dieses Produkt enthält möglicherweise vom OpenSSL-Projekt für die Verwendung im OpenSSL Toolkit entwickelte Software (<http://www.openssl.org/>).

Dieses Produkt enthält möglicherweise von Eric Young geschriebene Kryptografie-Software ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

Dieses Produkt enthält möglicherweise Softwareprogramme, die der GNU General Public License (GPL) oder ähnlichen Free Software-Lizenzen unterliegen, die den Benutzer u. a. dazu berechtigen, bestimmte Programme vollständig oder teilweise zu kopieren, zu ändern und weiterzugeben und auf den Quellcode zuzugreifen. Nach der GPL muss bei jeglicher ihr unterliegenden Software, die in einer ausführbaren binären Form verteilt wird, auch der Quellcode zur Verfügung gestellt werden. Für solche Software, die der GPL unterliegt, wird der Quellcode auf dieser CD zur Verfügung gestellt. Falls eine Free Software-Lizenz es erfordert, dass Network Associates Rechte zum Verwenden, Kopieren oder Ändern eines Softwareprogramms gewährt, die weiter gehen als die Rechte in diesem Vertrag, dann haben jene Rechte Vorrang vor den hierin genannten Rechten und Einschränkungen.

## LIZENZVERTRAG

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DIE RECHTSVEREINBARUNG, DIE FÜR DIE ERWORBENE LIZENZ GILT, AUFMERKSAM DURCH. SIE ENTHÄLT ALLGEMEINE BESTIMMUNGEN ZUR VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE SICH NICHT SICHER SIND, WELCHE ART VON LIZENZ SIE ERWORBEN HABEN, SEHEN SIE BITTE DIE VERKAUFUNTERLAGEN AUF GEWÄHRTE LIZENZVEREINBARUNGEN DURCH SOWIE DIE VERKAUFSGEBEGLEITENDEN PAPIERE, DIE IN IHREM SOFTWARE-PAKET ENTHALTEN SIND ODER SEPARAT AN SIE AUSGEHÄNDIGT WURDEN (IN FORM EINES HEFTS, EINER DATEI, EINER PRODUKT-CD ODER EINER DATEI AUF DER WEBSEITE, VON DER SIE IHR SOFTWARE-PAKET HERUNTERGELADEN HABEN). WENN SIE NICHT ALLEN BESTIMMUNGEN DER VEREINBARUNG ZUSTIMMEN, INSTALLIEREN SIE DIE SOFTWARE NICHT. GEGEBENENFALLS KÖNNEN SIE DAS PRODUKT ZURÜCKGEBEN, WOBEI IHNEN DER VOLLE KAUFPREIS ZURÜCKERSTATTET WIRD.

# Inhalt

<b>Vorwort</b> .....	<b>7</b>
Zielgruppe .....	7
Konventionen .....	8
Weitere Informationen .....	9
Kontaktaufnahme mit McAfee Security und Network Associates .....	10
<b>1 Einführung in VirusScan ASaP</b> .....	<b>13</b>
Was genau ist VirusScan ASaP? .....	13
Funktionsweise von VirusScan ASaP .....	14
Aktualisierungen .....	14
Abrufen von Updates .....	15
Hochladen von Berichten .....	15
Internet Independent Updating (IIU) .....	15
Rumor-Technologie .....	16
Neues in dieser Version .....	17
<b>2 Installieren von VirusScan ASaP</b> .....	<b>19</b>
Systemanforderungen .....	19
Vor der Installation .....	20
Deinstallieren vorhandener Antivirusanwendungen .....	20
Konfigurieren des Browsers .....	21
Überblick über ActiveX .....	21
Internet Explorer 5.5 .....	22
Internet Explorer 6.x .....	22
Netscape Communicator .....	23
Installieren von VirusScan ASaP .....	23
Internet-URL-Installation .....	24
Anforderungen .....	24
Installation .....	24
Hintergrundinstallation .....	26
Anforderungen .....	26
Installation .....	27

VSSETUP-Parameter .....	28
Beispiele .....	29
Push-Installation .....	29
Anforderungen .....	29
Installation .....	30
Wenn Sie eine Firewall oder einen Proxy-Server verwenden .....	31
Aktivieren von Relay-Servern .....	31
Verwenden des Push Install-Dienstprogramms .....	32
Mit VSSETUP .....	32
Erste Installation .....	32
Ändern einer vorhandenen Konfiguration .....	32
Testen von VirusScan ASaP .....	33
<b>3 Verwenden von VirusScan ASaP .....</b>	<b>35</b>
Customer Home-Website .....	35
Anmelden .....	35
Aktualisieren Ihres Benutzerprofils .....	36
Hinzufügen neuer Dienste .....	36
Zugriffs- und Hilfsprogramme .....	37
Aufrufen Ihrer Berichte .....	37
Scannen .....	37
Automatisches Scannen .....	37
Excluded Items Viewer .....	38
Die Funktion "Jetzt scannen" .....	39
Nach Ausführung der Funktion "Jetzt scannen" erzeugte Berichte .....	39
Aktualisierungen .....	40
Automatische Updates .....	40
Updates auf Anforderung .....	41
Berichtsübersicht .....	41
Erstmaliges Erstellen von Gruppen .....	42
Lesen Ihrer Berichte .....	44
Seite Alle Gruppen verwalten .....	44
Seite Gruppenliste .....	47
Verschieben von Arbeitsstationen in eine andere Gruppe .....	48
Löschen von Arbeitsstationen aus einer Gruppe .....	48
Mehr Details über ein System erhalten .....	49
Seite Gruppenüberblick .....	50
Seite DAT-Überblick .....	51

---

Blockieren von Systemen .....	52
Aufheben der Blockierung eines Systems .....	53
<b>4 Fehlerbehebung .....</b>	<b>55</b>
Häufig gestellte Fragen (FAQ) .....	55
Fragen zur Installation .....	55
Fragen zum Scannen .....	57
Fragen zu Berichten .....	58
Fragen zum Aktualisieren .....	59
Allgemeine Fragen .....	59
Fehlermeldungen .....	61
Freigegebenes Remote-Verzeichnis nicht gefunden .....	62
Die Installation kann nicht fortgesetzt werden, da Sie keine zentrale Agentenkomponente akzeptiert haben... .....	63
Invalid Entitlement Error .....	64
Ihre aktuellen Sicherheitseinstellungen verhindern die Ausführung von ActiveX-Steuerelementen auf dieser Seite .....	64
MyASUtil.SecureObjectFactory .....	64
Cab Installer-Objekt kann nicht erstellt werden .....	65
Es konnte keine Verbindung zum McAfee ASaP-Aktualisierungsserver hergestellt werden .....	66
URL-Download in Datei fehlgeschlagen .....	67
Kontaktaufnahme mit dem technischen Support .....	68



# Vorwort

Dieses Produkthandbuch ist eine Einführung in McAfee® VirusScan® ASaP Managed Service und enthält folgende Informationen:

- Detaillierte Anweisungen zur Installation der Software.
- Übersicht über das Produkt.
- Beschreibungen der Produktfunktionen.
- Beschreibung aller neuen Funktionen in dieser Version der Software.
- Detaillierte Anweisungen zum Konfigurieren und Ausbringen der Software.
- Verfahren zum Ausführen von Tasks.
- Informationen zur Fehlerbehebung.

## Zielgruppe

Dieses Handbuch wurde für System- und Netzwerkadministratoren geschrieben, die für die Betreuung des Antiviren- und Sicherheitsprogramms in ihren Unternehmen verantwortlich sind.

# Konventionen

Für diese Handbuch gelten die folgenden Konventionen:

**Fett** Alle Begriffe der Benutzeroberfläche, darunter die Bezeichnungen von Optionen, Menüs, Schaltflächen und Dialogfeldern.

**Beispiel**

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

**Courier** Text, den der Benutzer exakt so eingeben muss, zum Beispiel ein Befehl an der Eingabeaufforderung.

**Beispiel**

Führen Sie zum Aktivieren des Agenten die folgende Befehlszeile auf dem Client-Computer aus:

```
FRMINST.EXE /INSTALL=AGENT /SITEINFO=C:\TEMP\SITELIST.XML
```

**Kursiv** Titel von Produkthandbüchern und Themen (Überschriften) in den Handbüchern; Betonung; Einführung eines neuen Begriffs.

**Beispiel**

Weitere Informationen finden Sie im *VirusScan Enterprise-Produkthandbuch*.

<BEGRIFF> Eckige Klammern umschließen einen allgemeinen Begriff.

**Beispiel**

Klicken Sie in der Konsolenstruktur unter **ePolicy Orchestrator** mit der rechten Maustaste auf <SERVER>.

**HINWEIS** Zusatzinformationen, zum Beispiel eine alternative Möglichkeit zur Ausführung eines Befehls.

**WARNUNG** Wichtiger Ratschlag zum Schutz des Benutzers, des Computersystems, des Unternehmens, der Softwareinstallation oder der Daten.



## Weitere Informationen

<b>Produkt<span>hand</span>buch *</b>	Produktvorstellung und -funktionen, ausführliche Anweisungen für die Konfiguration der Software, Informationen zur Ausbringung, zu wiederkehrenden Tasks und zu Vorgehensweisen. <i>VirusScan ASaP Managed Service-Produkt<span>hand</span>buch</i>
<b>Hilfe §</b>	Allgemeine und detaillierte Informationen zur Konfiguration und Verwendung der Software.
<b>Einführung<span>hand</span>buch *</b>	Verfahren zum Installieren und Verwenden des McAfee Security-Produkts.
<b>Versions<span>in</span>formationen ‡</b>	<i>ReadMe</i> (LiesMich). Produktinformationen, behobene Fehler, bekannte Probleme, in letzter Minute am Produkt oder der zugehörigen Dokumentation vorgenommene Ergänzungen und Änderungen.
<b>Kontakt<span>in</span>formationen ‡</b>	Kontaktinformationen für Dienstleistungen und Ressourcen von McAfee Security und Network Associates: technischer Support, Kundendienst, AVERT (Anti-Virus Emergency Response Team), Betaprogramm und Schulungen. Diese Datei enthält außerdem eine Liste mit Telefonnummern, Anschriften, Webadressen und Faxnummern für Network Associates-Niederlassungen in den USA und weltweit.

\* Eine PDF-Datei (Adobe Acrobat) auf der Produkt-CD oder auf der Download-Site von McAfee Security.

† Ein gedrucktes Handbuch, das mit der Produkt-CD mitgeliefert wird.

‡ Textdateien, die auf der Produkt-CD mit der Softwareanwendung mitgeliefert werden.

§ Hilfe, die in der Softwareanwendung aufgerufen werden kann: Menü "Hilfe" und/oder Schaltfläche "Hilfe" für Hilfe auf Seitenebene; *Kontexthilfe* über die rechte Maustaste.

# Kontaktaufnahme mit McAfee Security und Network Associates

---

## Technischer Support

Homepage	<a href="http://www.nai.com/naicommon/services/technical-support/intro.asp">http://www.nai.com/naicommon/services/technical-support/intro.asp</a>
KnowledgeBase-Suche	<a href="https://knowledgemap.nai.com/phpclient/Homepage.aspx">https://knowledgemap.nai.com/phpclient/Homepage.aspx</a>
PrimeSupport Service-Portal *	<a href="http://mysupport.nai.com">http://mysupport.nai.com</a>

---

## McAfee-Betaprogramm

<http://www.mcafeesecurity.com/beta/>

---

## AVERT Anti-Virus Emergency Response Team

Homepage	<a href="http://www.mcafeesecurity.com/naicommon/avert/default.asp">http://www.mcafeesecurity.com/naicommon/avert/default.asp</a>
Bibliothek mit Virusinformationen	<a href="http://vil.nai.com">http://vil.nai.com</a>
Einreichen eines Beispiels	<a href="https://www.webimmune.net/default.asp">https://www.webimmune.net/default.asp</a>

---

## Download-Site

Homepage	<a href="http://www.mcafeesecurity.com/naicommon/download/">http://www.mcafeesecurity.com/naicommon/download/</a>
DAT-Datei- und Modulaktualisierungen	<a href="http://www.mcafeesecurity.com/naicommon/download/dats/find.asp">http://www.mcafeesecurity.com/naicommon/download/dats/find.asp</a>
	<a href="ftp://ftp.nai.com/pub/antivirus/datfiles/4.x">ftp://ftp.nai.com/pub/antivirus/datfiles/4.x</a>
Produkt-Upgrades *	<a href="http://www.mcafeesecurity.com/naicommon/download/upgrade/login.asp">http://www.mcafeesecurity.com/naicommon/download/upgrade/login.asp</a>

---

## Schulungen

Schulungen vor Ort	<a href="http://www.mcafeesecurity.com/services/mcafee-training/default.asp">http://www.mcafeesecurity.com/services/mcafee-training/default.asp</a>
McAfee Security University	<a href="http://www.mcafeesecurity.com/services/mcafeesecurityu.asp">http://www.mcafeesecurity.com/services/mcafeesecurityu.asp</a>

---

## Network Associates-Kundendienst

E-Mail	<a href="mailto:services_corporate_division@nai.com">services_corporate_division@nai.com</a>
Web	<a href="http://www.nai.com">http://www.nai.com</a> <a href="http://www.mcafeesecurity.com">http://www.mcafeesecurity.com</a>
USA, Kanada und Lateinamerika (gebührenfrei):	
Telefon	<b>+1-888-VIRUS-NR</b> oder <b>+1-888-847-8766</b> Montag bis Freitag, 08.00-20.00 Uhr (US-Central Time)

---

## Network Associates-Partner und -Vertragshändler

Channel-Programm	<a href="http://www.nai.com/partners/default.asp">http://www.nai.com/partners/default.asp</a>
McAfee-Entwicklungsprogramm	<a href="http://www.mcafeesecurity.com/partners/oem/default.asp">http://www.mcafeesecurity.com/partners/oem/default.asp</a>
McAfee Managed Services (ASaP)	<a href="http://www.mcafeesap.com/content/find_sp/default.asp">http://www.mcafeesap.com/content/find_sp/default.asp</a>
McAfee Service Provider (MSP)	<a href="http://www.mcafeesecurity.com/partners/msp/default.asp">http://www.mcafeesecurity.com/partners/msp/default.asp</a>

---

McAfee hat sich zum Ziel gesetzt, Produkte anzubieten, die auf dem Feedback der Kunden basieren. Wenn Sie sprachliche oder andere Anmerkungen machen wollen, senden Sie uns bitte eine E-Mail an die Adresse: [B2BLoc\\_DE@nai.com](mailto:B2BLoc_DE@nai.com)

---

Weitere Informationen zur Kontaktaufnahme mit Network Associates und McAfee Security (einschließlich gebührenfreier Nummern für andere Länder) finden Sie in der Kontaktdatei, die mit dieser Produktversion mitgeliefert wurde.

---

\* Anmeldeinformationen erforderlich.



In diesem Abschnitt erhalten Sie einen Überblick über die Funktionen von VirusScan® ASaP Managed Service sowie die Technologie, die sich hinter diesem Produkt verbirgt.

## Was genau ist VirusScan ASaP?

VirusScan ASaP-Dienst ist ein webbasierter Dienst, der die Computer in Ihrem Unternehmen schützt und verwaltet, indem automatisch nach Viren gesucht wird und Berichte erstellt werden. Die Installation kann von einem Administrator auf mehreren Arbeitsstationen oder von einem einfachen Benutzer auf einem Einzelplatzrechner mit Verbindung zum VirusScan ASaP-Server (über eine angegebene URL-Adresse) vorgenommen werden.

Nach Abschluss der ersten Installation wird der VirusScan ASaP-Dienst im Hintergrund ausgeführt und aktualisiert sich dabei automatisch selbst mit den neuesten Virusdefinitionsdateien (DAT), mit denen die Dateien auf Ihrem Computer auf Viren geprüft werden. Anschließend werden Berichte auf den Server geladen, auf dem der aktuelle Status aller Computer in Ihrem Unternehmen sowie Informationen zu verhinderten Infektionen und Ausbrüchen angezeigt werden.

VirusScan ASaP bietet Ihnen beständigen Schutz vor Viren, die von Disketten oder aus dem Netzwerk übertragen werden. Der Dienst wird zusammen mit Ihrem Computer gestartet und bleibt so lange aktiv, bis das System heruntergefahren wird.

Der VirusScan ASaP-Dienst bietet Folgendes:

- **Ständigen Schutz:** VirusScan ASaP überwacht im Hintergrund alle Dateieingänge und -ausgänge, Downloads, ausgeführten Programme sowie andere systembezogene Aktivitäten.
- **Sofortige Erkennung:** Wenn VirusScan ASaP einen Virus entdeckt, wird versucht, die infizierte Datei zu bereinigen, bevor weiterer Schaden verursacht werden kann.
- **Automatische Aktualisierungen:** VirusScan ASaP überwacht Ihr System den ganzen Tag über in regelmäßigen Abständen und vergleicht dabei die Virusdefinitionsdateien (DAT) mit der neuesten Version. Wenn eine Aktualisierung erforderlich ist, ruft VirusScan ASaP die entsprechenden Daten automatisch ab.

- **AVERT-Frühwarnsystem:** VirusScan ASaP verwendet die neuesten Informationen über Virusbedrohungen und -ausbrüche, sobald diese von AVERT Labs, einer Abteilung von Network Associates, entdeckt werden.

## Funktionsweise von VirusScan ASaP

Der VirusScan ASaP-Dienst basiert auf der Technologie, die auch im McAfee Security VirusScan-Desktop-Produkt zum Einsatz kommt. Bei jedem Dateizugriff auf Ihrem Computer scannt VirusScan ASaP die Datei und prüft so, ob diese virenfrei ist. Entdeckt der Dienst Viren und säubert oder sperrt er die entsprechenden Dateien, werden diese Informationen gespeichert und zur Protokollierung auf den Server geladen.

## Aktualisierungen

Garant für die Wirksamkeit des VirusScan ASaP-Dienstes sind regelmäßige Aktualisierungen. In einem einfachen Szenario hat jede Arbeitsstation über das Internet eine direkte Verbindung zum Network Operations Center (NOC) und sucht nach neuen Updates der Virusdefinitionsdateien (DAT) und des Scan-Moduls. Wenn eine Arbeitsstation jedoch nicht über Internet-Zugriff verfügt, ist keine direkte Verbindung möglich. Selbst wenn alle Arbeitsstationen im Netzwerk über eine direkte Verbindung zum Internet verfügen, kann das Ausführen von mehreren Downloads vom NOC zu unnötigem Internetverkehr führen. Aus diesem Grund unterstützen die beiden folgenden Funktionen VirusScan ASaP dabei, die Netzwerkressourcen effizient zu nutzen:

- **Internet Independent Updating (IIU):** Alle Computer im Netzwerk können vom NOC Informationen beziehen, auch wenn der Computer selbst keine Verbindung zum Internet hat.
- **Rumor-Technologie:** Alle Computer in einer Arbeitsgruppe können heruntergeladene Dateien gemeinsam nutzen. Dadurch muss nicht jeder Computer ein Download vom NOC auszuführen, wenn er eine aktualisierte Datei benötigt.

## Abrufen von Updates

Fünf Minuten, nachdem der Computer hochgefahren wurde, und anschließend in regelmäßigen Abständen während des Tages VirusScan ASaP eine Verbindung zum NOC her und überprüft, ob Updates vorliegen. Wenn Updates vorhanden sind, zieht Ihr Computer diese entweder von einem anderen Computer im Netzwerk (über [Rumor-Technologie](#)) oder lädt diese direkt vom NOC herunter.

McAfee aktualisiert die Virusdefinitionsdateien (DAT) im NOC regelmäßig. Wenn VirusScan ASaP eine Verbindung mit dem NOC herstellt, wird Folgendes abgerufen:

- Alle neuen DAT-Dateien.
- Upgrades der Software, wenn eine neuere Version vorhanden ist.

### HINWEIS

Bei einer Virusbedrohung oder einem Virusausbruch stellt das NOC häufiger neue Updates zur Verfügung.

Der Benutzer kann jederzeit eine Aktualisierung manuell ausführen, indem er mit der rechten Maustaste auf das VirusScan ASaP-Symbol in der Symbolleiste klickt und die Option **Jetzt aktualisieren** auswählt.

## Hochladen von Berichten

Arbeitsstationen laden Daten nach jeder Aktualisierung hoch und prüfen stündlich, ob Virensan-Vorgänge ausgeführt werden. Diese Informationen stehen in den Berichten, die auf dem NOC-Partner-Server gespeichert werden.

## Internet Independent Updating (IIU)

Mit dem internetunabhängigen Aktualisieren (IIU, Internet Independent Updating) können Sie den VirusScan ASaP-Dienst mit Computern verwenden, die nicht über eine Internet-Verbindung verfügen. Um diese Funktion zu nutzen, muss mindestens eine Arbeitsstation im Subnet über eine Internetverbindung verfügen, um mit dem NOC kommunizieren zu können. Diese Arbeitsstation wird als Relay-Server konfiguriert, und die anderen Computer kommunizieren dann über diesen Computer mit dem NOC.

- Der Relay-Server lädt einen Katalog der Updates vom NOC herunter, wenn dieser von einer anderen Arbeitsstation dazu aufgefordert wird, die keine direkte Verbindung zum NOC herstellen konnte.
- Die Arbeitsstation, die nicht über eine direkte Internet-Verbindung verfügt, lädt die erforderlichen Updates über den Relay-Server vom NOC herunter.

Weitere Informationen zum Konfigurieren von Computern als Relay-Server finden Sie unter [Aktivieren von Relay-Servern auf Seite 31](#).

## Rumor-Technologie

Rumor ist ein Vorgang, bei dem eine Arbeitsstation Updates mit anderen Computern im lokalen Netzwerk (LAN) gemeinsam verwendet, anstatt dass alle Computer die Updates einzeln vom NOC abrufen. Diese Funktion reduziert den Internetverkehr im Netzwerk.

- Alle Arbeitsstationen rufen vom NOC Versionsinformationen zu der neuesten Katalogdatei ab. Diese Katalogdatei enthält Informationen zur aktuellen Version aller Komponenten in VirusScan ASaP und wird digital im CAB-Dateiformat gespeichert.
  - ◆ Wenn diese Version mit der Version der Arbeitsstation übereinstimmt, wird der Vorgang an dieser Stelle angehalten.
  - ◆ Wenn diese Version nicht mit der auf der Arbeitsstation vorhandenen Version übereinstimmt, wird versucht, die neueste Version der Katalogdatei von den Peers abzurufen, indem angefragt wird, ob andere Computer im LAN das neue Update bereits heruntergeladen haben.
- Die Arbeitsstation ruft die erforderliche Katalogdatei ab (entweder direkt vom NOC oder von einem Peer). Anhand dieser Katalogdatei wird ermittelt, ob neue VirusScan ASaP-Komponenten zur Verfügung stehen.
- Wenn neue Komponenten zur Verfügung stehen, versucht die Arbeitsstation diese von den Peers abzurufen, indem sie anfragt, ob andere Computer im LAN die neue VirusScan ASaP-Komponente bereits heruntergeladen haben.
  - ◆ Ist dies der Fall, ruft die Arbeitsstation das Update von einem lokalen Computer ab (die digitalen Signaturen werden überprüft, um sicherzustellen, dass es sich bei der Arbeitsstation um einen gültigen Benutzer handelt).
  - ◆ Ist dies nicht der Fall, ruft die Arbeitsstation das Update direkt vom NOC ab.
- Nachdem die Arbeitsstation das Update abgerufen hat, wird die CAB-Datei extrahiert und alle neuen Komponenten werden installiert.



## Neues in dieser Version

- **Server-Unterstützung:** Diese Version von VirusScan ASaP unterstützt zusätzlich zu den aktuell unterstützten Betriebssystemen auf Arbeitsstationen Installationen auf Server-Betriebssystemen. Weitere Informationen finden Sie unter [Systemanforderungen auf Seite 19](#).
- **Automatische Deinstallation von Anwendungen:** Während des Installationsvorgangs deinstalliert VirusScan ASaP automatisch viele bestehende Anti-Virus-Softwareprodukte. In dieser Version wurden der Liste der zu deinstallierenden Anwendungen weitere Produkte hinzugefügt. Die vollständige Liste der Produkte, die automatisch deinstalliert werden, erhalten Sie unter [Deinstallieren vorhandener Antivirusanwendungen auf Seite 20](#).
- **Zusätzliche Berichtsfunktionen:** Ihre personalisierten Berichten stehen mit dieser Version zusätzliche Funktionen zur Verfügung. Beim Verwalten Ihrer Gruppen und individuellen Arbeitsstationen können Sie eine oder mehrere Arbeitsstationen für das Erhalten von Aktualisierungen sperren. Sie können auf allen Arbeitsstationen eine Systemsuche durchführen und dabei als Suchkriterium den Systemnamen oder die E-Mail-Adresse verwenden. Weitere Informationen finden Sie unter [Lesen Ihrer Berichte auf Seite 44](#).



Dieser Abschnitt enthält Informationen zum Installieren von VirusScan ASaP.

- *Systemanforderungen*
- *Vor der Installation*
- *Installieren von VirusScan ASaP*
- *Testen von VirusScan ASaP*

## Systemanforderungen

Der VirusScan ASaP-Dienst wurde für Microsoft Windows-Betriebssysteme auf PC-Plattformen entwickelt. VirusScan ASaP kann auf Servern und Arbeitsstationen installiert und ausgeführt werden, die mit Folgendem ausgestattet sind:

- Einem Intel Pentium-Prozessor oder einer kompatiblen Architektur.
- Eines der nachstehenden Betriebssysteme:
  - ◆ **Arbeitsstationen:** Windows 95, Windows 98, Windows 98 SE, Windows Me, Windows NT 4.0 Arbeitsstation mit Service Pack 6a oder höher, Windows 2000 Professional mit Service Pack 2 oder höher, Windows XP Home oder Professional.
  - ◆ **Server:** Windows NT 4.0 Server mit Service Pack 6a oder höher, Windows NT 4.0 Server Enterprise Edition, Windows 2000 mit Service Pack 2 oder höher, Windows 2000 Advanced Server mit Service Pack 2 oder höher, Windows 2003 Standard Server, Windows 2003 Enterprise Server, Windows 2003 Web Edition.
- RAM-Anforderungen:
  - ◆ **Windows 95 und Windows 98**  
Mindestens 32 MB  
Empfohlen 128 MB
  - ◆ **Andere Betriebssysteme**  
Mindestens 64 MB  
Empfohlen 128 MB  
Empfohlen bei Servern 256 MB
- Eine Microsoft-Maus oder ein kompatibles Zeigegerät.

- VGA-Monitor mit 256 oder mehr Farben.
- Microsoft Internet Explorer 5.5 SP2 oder höher, oder Netscape Communicator 4.6x oder 4.7x (für Netscape ist Internet Explorer 5.5 SP2 oder höher erforderlich).
- Microsoft Internet Explorer 5.5 SP2 oder höher ist für das internetunabhängige Aktualisieren (IIU) erforderlich.

### **HINWEIS**

Das VirusScan ASaP Activator-Plug-In ermöglicht zwar die Kompatibilität mit Netscape Communicator, Sie müssen jedoch vor der Installation des Plug-Ins Internet Explorer oder höher installieren. Weitere Informationen erhalten Sie unter [Konfigurieren des Browsers auf Seite 21](#).

## Vor der Installation

Vergewissern Sie sich vor der Installation von VirusScan ASaP, dass das System bereit ist. Führen Sie vor der Installation die folgenden Prozeduren aus:

- [Deinstallieren vorhandener Antivirusanwendungen](#)
- [Konfigurieren des Browsers](#)

## Deinstallieren vorhandener Antivirusanwendungen

Der VirusScan ASaP-Dienst enthält die neueste Antivirustechnologie von McAfee Security. Andere Antivirusanwendungen beeinträchtigen jedoch die erweiterten Funktionen von VirusScan ASaP. Wenn mehrere Virusscan-Module versuchen, auf einem Computer auf dieselbe Datei zuzugreifen, können sich diese gegenseitig behindern.

Wenn Sie während der Installation darauf hingewiesen werden, dass Antivirusanwendungen vorhanden sind, führen Sie die angezeigten Anweisungen aus, um vorhandene Antivirusprogramme zu entfernen. In der folgenden Liste sind alle Produkte aufgeführt, die von VirusScan ASaP automatisch deinstalliert werden. Wenn auf Ihrem Computer nicht in der Liste aufgeführte Antivirussoftware installiert ist, müssen Sie diese vor der Installation manuell deinstallieren VirusScan ASaP.

- ♦ Dr. Ahn V3 2002 Deluxe
- ♦ McAfee ActiveShield
- ♦ McAfee VirusScan 4.03 Verkaufsversion
- ♦ McAfee NetShield 4.03 für NT
- ♦ McAfee VirusScan 4.03 für NT
- ♦ McAfee VirusScan 4.03 für 9x
- ♦ McAfee VirusScan 4.5 für 9x
- ♦ McAfee NetShield 4.5 für NT
- ♦ McAfee VirusScan 4.5 für NT
- ♦ McAfee VirusScan 5.0 Verkaufsversion
- ♦ McAfee VirusScan 5.1 Verkaufsversion
- ♦ McAfee VirusScan TC 6.1
- ♦ McAfee VirusScan 6.0 Verkaufsversion
- ♦ McAfee VirusScan 7.0 Verkaufsversion
- ♦ McAfee VirusScan 6.0 Pro
- ♦ McAfee VirusScan 7.0 Pro
- ♦ McAfee VirusScan Enterprise 7.0
- ♦ McAfee VirusScan ePO Agent
- ♦ McAfee VirusScan TC
- ♦ myCIO EarlyVersion
- ♦ Symantec Norton AntiVirus
- ♦ Symantec Norton AntiVirus Corporate Edition
- ♦ PC-Cillin 2002
- ♦ Trendmicro Housecall
- ♦ F-Prot für Windows

## Konfigurieren des Browsers

VirusScan ASaP verwendet das ActiveX-Softwaremodul, um eine Arbeitsstation aus einem Webbrowser heraus einzuschalten. Wenn Sie Internet Explorer verwenden, ist die ActiveX-Technologie in den Browser integriert. Wenn Netscape als primärer Browser verwendet wird, muss Internet Explorer ebenfalls installiert sein.

## Überblick über ActiveX

Ein ActiveX-Steuerelement ist ein Softwaremodul, das auf der COM-Architektur (Component Object Model) von Microsoft basiert. Mit diesem Steuerelement kann ein Programm Funktionen hinzufügen, indem vorgefertigte Komponenten aufgerufen werden, die sich einfügen und als integrierte Teile des Programms dargestellt werden.

Gegenwärtig werden ActiveX-Steuerelemente von Netscape Communicator nicht unterstützt. Wenn Sie Netscape als primären Browser verwenden, werden Sie vom Installationsprogramm aufgefordert, das für die Verwendung von ActiveX erforderliche Plug-In zu installieren.

### Internet Explorer 5.5

VirusScan ASaP funktioniert mit den Standardeinstellungen von Internet Explorer. Dadurch wird ein Maximum an Sicherheit gewährleistet und gleichzeitig das Herunterladen und Installieren der ActiveX-Komponenten ermöglicht.

Wenn Sie sich nicht sicher sind, ob die Einstellungen richtig sind, führen Sie die folgenden Schritte aus, um die Sicherheitseinstellungen in Internet Explorer zu ändern:

- 1 Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start**, und wählen Sie anschließend **Einstellungen | Systemsteuerung**.
- 2 Doppelklicken Sie auf das Symbol **Internetoptionen**.
- 3 Öffnen Sie die Registerkarte **Sicherheit**.
- 4 Wählen Sie die Zone **Internet**.
- 5 Klicken Sie auf **Standardstufe**. Eine Bildlaufleiste wird angezeigt.
- 6 Ziehen Sie die Bildlaufleiste auf **Mittel**. So können signierte ActiveX-Steuerelemente heruntergeladen werden.
- 7 Klicken Sie auf **OK**.

### Internet Explorer 6.x

VirusScan ASaP funktioniert mit den Standardeinstellungen von Internet Explorer. Dadurch wird ein Maximum an Sicherheit gewährleistet und gleichzeitig das Herunterladen und Installieren der ActiveX-Komponenten ermöglicht.

Wenn Sie sich nicht sicher sind, ob die Einstellungen richtig sind, führen Sie die folgenden Schritte aus, um die Sicherheitseinstellungen in Internet Explorer zu ändern:

- 1 Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start**, und wählen Sie anschließend **Einstellungen | Systemsteuerung**.
- 2 Doppelklicken Sie auf das Symbol **Internetoptionen**.
- 3 Öffnen Sie die Registerkarte **Sicherheit**.
- 4 Klicken Sie auf **Stufe anpassen**.
- 5 Klicken Sie im Menü **Zurücksetzen** auf **Mittel**. Klicken Sie auf **Zurücksetzen**.

- 6 Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern.
- 7 Klicken Sie auf **OK**, um das Fenster **Interneteigenschaften** zu schließen.

## Netscape Communicator

Wenn Sie Netscape Communicator als Standardbrowser verwenden, müssen Sie auf dem Computer auch Internet Explorer 5.5 SP2 oder höher sowie das VirusScan ASaP Activator-Plug-In installieren. Öffnen Sie zum Installieren der VirusScan ASaP-Komponenten Internet Explorer, und führen Sie die Schritte für die Konfiguration aus. Dies müssen Sie auch tun, wenn Sie zum Browsen im Web eigentlich Netscape verwenden.

### Installieren des Netscape-Plug-Ins

Wenn Sie zum Zugreifen auf die VirusScan ASaP-Installationswebseite Netscape verwenden, werden Sie automatisch zu dem erforderlichen Plug-In geführt. Führen Sie die Schritte zum Herunterladen der Plug-In-Datei PLGSETUP.EXE aus, und doppelklicken Sie auf die Datei, um sie zu installieren. Ein Installationsassistent führt Sie durch diesen Prozess.

Das VirusScan ASaP-Plug-in für Netscape funktioniert nur mit den Browser-Versionen 4.x. Wenn Sie eine höhere Version von Netscape als Standardbrowser verwenden, müssen Sie die Installation von VirusScan ASaP mit Internet Explorer durchführen.

# Installieren von VirusScan ASaP

Die Installation des VirusScan ASaP-Dienstes auf einer Arbeitsstation können Sie auf drei Arten vornehmen:

### *Internet-URL-Installation*

Das ist das am häufigsten verwendete Installationsverfahren. Jeder Benutzer einer Arbeitsstation gibt eine vorgegebene URL-Adresse ein. Daraufhin wird der Dienst automatisch auf dem Computer installiert.

### *Hintergrundinstallation*

Bei diesem Verfahren kann ein LAN-Administrator mit dem Programm VSSETUP.EXE VirusScan ASaP über die Befehlszeile auf dem Computer eines Benutzers installieren, ohne dass der Benutzer eingreifen muss.

### *Push-Installation*

Dieses Installationsverfahren ähnelt im Wesentlichen der Hintergrundinstallation, wird aber statt lokal an den einzelnen Computern aus der Ferne für einen oder mehrere Computer durchgeführt.

## Internet-URL-Installation

Bei diesem Verfahren kann ein Benutzer VirusScan ASaP einzeln auf der Arbeitsstation installieren, indem er das Programm von dem URL herunterlädt, der für Ihr Unternehmen eingerichtet wurde.

### Anforderungen

Voraussetzungen für die Internet-URL-Installation:

- Der Benutzer der Arbeitsstation muss über lokale Administratorrechte verfügen. Beachten Sie, dass dies nicht die Standardvorgabe für Windows NT-, Windows 2000- und Windows XP-Betriebssysteme ist.
- Der Benutzer der Arbeitsstation muss über ausreichend Rechte zum Installieren eines ActiveX-Steuerelements und eines Produkts auf dem System verfügen.

### Installation

Nachdem Sie sich für den VirusScan ASaP-Dienst angemeldet haben, erhalten Sie eine E-Mail, die den URL enthält, der für Ihr Unternehmen eingerichtet wurde. In den meisten Fällen können Sie diese URL-Adresse per E-Mail an die Benutzer weiterleiten.

#### **HINWEIS**

Die Internet-URL-Installation funktioniert nicht bei Arbeitsstationen ohne Verbindung zum Internet bzw. Arbeitsstationen, bei denen die Benutzer nicht über Administratorrechte verfügen.

- 1 Zum Installieren des VirusScan ASaP-Dienstes auf einer Arbeitsstation öffnet der Benutzer die E-Mail und klickt auf den URL.





Abbildung 2-1. Internet-URL-Installation

- 2 Der VirusScan ASaP-Dienst wird automatisch installiert. Während der Installation wird der Benutzer dazu aufgefordert, eine oder mehrere der folgenden Aktionen auszuführen:

- ◆ Eine E-Mail-Adresse einzugeben, die zum Erkennen des Computers verwendet wird, auf dem die Installation erfolgt.

**HINWEIS**

Die vom Benutzer hier eingegebene Adresse dient der Identifizierung des Computers in Berichten auf der **Customer Home-Website**.

- ◆ ActiveX-Steuerelemente werden akzeptiert. Das ist Voraussetzung für die Ausführung des VirusScan ASaP-Dienstes.

Dies ist nicht erforderlich, wenn der Benutzer vorher zugestimmt hat, alle ActiveX-Steuerelemente von Network Associates zu akzeptieren oder wenn die Sicherheitseinstellungen in Internet Explorer auf eine Stufe gesetzt sind, bei der ActiveX-Steuerelemente heruntergeladen werden können, ohne dass der Benutzer diesen Vorgang bestätigen muss.

- ◆ Wenn der Benutzer über Netscape eine Verbindung zur Installations-URL-Adresse hergestellt hat, erkennt VirusScan ASaP den Browser bei der Installation und fordert den Benutzer zum Herunterladen des Netscape-Plug-Ins auf. Der Benutzer wird anschließend dazu aufgefordert, das System neu zu starten.

## Hintergrundinstallation

McAfee stellt eine ausführbare Datei zur Verfügung, die Optionen für die Massenbereitstellung enthält. Mit dem Dienstprogramm VSSETUP können Sie das gesamte VirusScan ASaP-Paket auf einem Computer im Hintergrund installieren, ohne dass der Benutzer aktiv werden muss. Die Hintergrundinstallation ist nicht netzwerkspezifisch und erfordert keinen Eingriff seitens des Benutzers. Mit VSSETUP können Sie VirusScan ASaP-Dienste auf jedem Windows-Betriebssystem im Hintergrund installieren.

## Anforderungen

Voraussetzungen für die Hintergrundinstallation:

- Auf den Netzwerkarbeitsstationen muss eine Methode zum Installieren von ausführbaren Dateien vorhanden sein. Beispiel:
  - ◆ Ein Drittanbieterbereitstellungstool wie Novell NAL, ZenWorks, das SMS-Installationsprogramm (Systems Management Server) von Microsoft, Tivoli IT Director oder ein anderes Tool.
  - ◆ Ein Anmeldeskript.
  - ◆ Eine Verknüpfung zu einer Datei in einer E-Mail.
  - ◆ Entfernte Ausführungsrechte.
  - ◆ Imaging oder Klonen von Systemen, um Daten von einem Computer zu einem anderen zu kopieren.
- Der Administrator sollte diesen Prozess ausführen, indem er ein Konto mit ausreichend Rechten zum Installieren des Produkts verwendet. Das bedeutet in der Regel, dass er über lokale Administratorrechte verfügen muss.

## Installation

Führen Sie für die Hintergrundinstallation von VirusScan ASaP-Dienst die folgenden Schritte aus:

- 1 Gehen Sie auf Ihre **Customer Home**-Website und klicken Sie auf **Tools und Hilfsprogramme**. Klicken Sie unter **VirusScan ASaP-Hintergrundinstallation** auf **Download**.
- 2 Laden Sie die Datei mit dem Namen VSSETUP.EXE auf Ihre Festplatte herunter. Bei dieser Datei handelt es sich um das Programm VSSETUP.
- 3 Stellen Sie das Programm für Arbeitsstationen mit einem Bereitstellungstool bereit, wie beispielsweise diejenigen, die unter [Systemanforderungen auf Seite 19](#) aufgelistet sind.
- 4 Am einfachsten ist es, wenn Sie den folgenden Befehl ausführen, um VirusScan ASaP-Dienst zu installieren.

```
VSSETUP.EXE /CK=<Schlüssel des Unternehmens>
```

Wie in diesem Beispiel dargestellt, müssen Sie den Unternehmensschlüssel (CK, Company Key) als Parameter des Installationsbefehls angeben.

- 5 Verwenden Sie die folgende Befehlszeile sowie alle Parameter, die für die Hintergrundinstallation verwendet werden sollen:

```
VSSETUP.EXE /<Parameter>
```

Unter [VSSETUP-Parameter auf Seite 28](#) befindet sich eine Liste der verfügbaren Parameter mit deren Bedeutung.

## Unternehmensschlüssel

Der Unternehmensschlüssel ist dem URL angehängt, den Sie nach der Anmeldung bei VirusScan ASaP erhalten haben. Der Schlüssel ist der hexadezimale Wert, der nach den Zeichen `ck=` am Ende der URL-Adresse steht.

### VSSETUP-Parameter

Die Parameter lauten wie folgt:

<code>/CK=XYZ</code>	Startet das Setup unter Verwendung des Unternehmensschlüssels.
<code>/Email=x@y.com</code>	<p>Kennzeichnet die E-Mail-Adresse des Benutzers in Aktivitätsberichten. Für diesen Parameter ist der Befehlsschalter <code>/CK</code> erforderlich.</p> <p><b>HINWEIS</b> Bei der E-Mail-Variable kann es sich trotz des Namens auch um eine beliebige Beschreibung handeln. Es muss sich nicht um eine E-Mail-Adresse handeln. Wenn die hier eingegebene Zeichenkette Zeichen enthält, die vom Standard abweichen, werden diese möglicherweise nicht richtig auf der Berichts-Website angezeigt.</p>
<code>/InstallService</code>	Installiert den VirusScan ASaP-Dienst.
<code>/Uninstall</code>	Deinstalliert den VirusScan ASaP-Dienst.
<code>/SetRelayServerEnable=1</code>	In einer vorhandenen Installation legt dieser Parameter fest, dass ein Computer mit einer Verbindung zum Internet ein Relay-Server ist. Wenn dieser Computer nicht als Relay-Server verwendet wird, wird dieser Parameter auf 0 gesetzt.

## Beispiele

```
VSSETUP.EXE /CK=abcd /Email=joe@xyz.com
```

Installiert VirusScan ASaP auf der Grundlage des Unternehmensschlüssels `abcd` mit der E-Mail-Adresse des Benutzers `joe@xyz.com` für Berichtszwecke.

```
VSSETUP.EXE /InstallService /CK=abcd /Email=joe@example.com
```

Registriert einen Dienst, der die Installation startet, wenn der Dienst gestartet wird, auf der Grundlage des Unternehmensschlüssels `abcd` mit der E-Mail-Adresse des Benutzers `joe@xyz.com` für Berichtszwecke.

## Push-Installation

Bei dieser Methode wird die Administratorarbeitsstation verwendet, um die Installation direkt vom Network Operations Center (NOC) auf die Arbeitsstationen zu übertragen. Für die Push-Installation ist weder Bereitstellungssoftware von Drittanbietern noch ein Eingriff seitens des Benutzers erforderlich.

Bestimmen Sie für diese Methode einen Computer als die Administratorarbeitsstation, auf der Sie das Push Install-Dienstprogramm installieren, und legen Sie die Zielarbeitsstationen im Netzwerk fest. Das Push Install-Dienstprogramm, bei dem es sich im wesentlichen um ein ActiveX-Steuerelement handelt, stellt VirusScan ASaP bereit und installiert das Programm auf allen Zielcomputern, die zum Zeitpunkt der Übertragung online sind.

Mit dem Push Install-Dienstprogramm können Sie einen oder mehrere Rechner im Netzwerk angeben, der/die als Relay-Server dient/dienen (diese müssen über Zugriff auf das Internet verfügen). Sie müssen Relay-Server in einem separaten Push-Vorgang angeben.

### HINWEIS

Da Microsoft Windows XP Home Edition nicht auf eine Windows NT- oder Active Directory-Domäne zugreifen kann, wird die Push-Installation unter Microsoft Windows XP Home Edition nicht unterstützt.

## Anforderungen

Voraussetzungen für die Push-Installation:

- Auf der Administratorarbeitsstation muss das Betriebssystem Windows NT mit Service Pack 6a oder höher, Windows 2000 oder Windows XP Professional installiert sein.
- Auf der Administratorarbeitsstation muss Internet Explorer 5.5 SP2 oder höher installiert sein.

- Alle Arbeitsstationen müssen in der selben Windows-Domäne wie die Administratorarbeitsstation angemeldet sein.
- Der Benutzer, der sich bei der Administratorarbeitsstation anmeldet, muss sich mit Domänenadministratorrechten für die installierte Domäne anmelden.
- Um den Installationsvorgang auf Arbeitsstationen mit Windows 95, Windows 98 oder Windows Millennium Edition durchzuführen, muss Folgendes aktiviert sein:
  - ◆ Datei- und Druckerfreigabe
  - ◆ Reigabe auf Benutzerebene, wobei im Feld **Benutzer- und Gruppenliste beziehen von**: die gleiche Windows NT-Domäne wie bei der Administratorarbeitsstation eingestellt wurde.
  - ◆ Fähigkeit, sich auf dieselbe Windows NT-Domäne wie die Administratorarbeitsstation anmelden zu können.

### Installation

Führen Sie für die Push-Installation von VirusScan ASaP-Dienst die folgenden Schritte aus:

- 1 Vergewissern Sie sich, dass auf Arbeitsstationen mit Windows 95, Windows 98 und Windows Millennium Edition die Remoteverwaltung aktiviert ist. Gehen Sie dazu folgendermaßen vor:
  - a Aktivieren Sie die Datei- und Druckerfreigabe.
  - b Aktivieren Sie Zugriffsrechte auf Benutzerebene für die Domäne.
- 2 Stellen Sie von der Website Ihres Anbieters eine Verbindung zu der **Customer Home**-Website her. Weitere Informationen finden Sie unter *Customer Home-Website auf Seite 35*.
- 3 Klicken Sie auf die Verknüpfung **VirusScan ASaP**. Daraufhin wird eine Webseite mit Installationsoptionen für VirusScan ASaP aufgerufen.
- 4 Wählen Sie **VirusScan ASaP-Remote-Installation**, um auf das Push-Installationsprogramm zuzugreifen.
- 5 Wählen Sie in der Domäne die Arbeitsstationen, auf denen VirusScan ASaP-Dienst installiert werden soll. Klicken Sie auf die Schaltfläche **VirusScan ASaP installieren**. Nach Abschluss der Installation wird eine Meldung angezeigt.

### Angeben von Relay-Server

Wenn sich in dem Netzwerk Arbeitsstationen befinden, die nicht über eine Internet-Verbindung verfügen, müssen Sie mindestens einen Relay-Server angeben.

- 1 Befolgen Sie [Schritt 1](#) bis [Schritt 5](#) des Abschnitts *Installation auf Seite 30*.
- 2 Geben Sie an, welche Arbeitsstationen als Relay-Server fungieren sollen. Aktivieren Sie das Kontrollkästchen **Als Relay-Server einstellen**. Relay-Server müssen über eine Internet-Verbindung verfügen.
- 3 Klicken Sie auf die Schaltfläche **VirusScan ASaP installieren**. Nach Abschluss der Installation wird eine Meldung angezeigt.

#### HINWEIS

Nach der Push-Installation unter Windows 95 oder Windows 98 muss nach dem Abschluss der Installation das System neu gestartet werden.

## Wenn Sie eine Firewall oder einen Proxy-Server verwenden

VirusScan ASaP wurde so konzipiert, dass Komponenten direkt von McAfee Security-Servern auf Ihren Computer heruntergeladen werden. Wenn sich Ihr Rechner hinter einer Firewall befindet oder die Verbindung ins Internet über einen Proxy-Server erfolgt, benötigen Sie möglicherweise zusätzliche Angaben, damit VirusScan ASaP richtig funktioniert.

- Als Authentifizierungsverfahren werden lediglich die anonyme und die Windows Domänen-Abfrage-/Rückmeldungsauthentifizierung unterstützt. Die Basisauthentifizierung wird nicht unterstützt.
- Wenn beim Installieren oder Aktualisieren von VirusScan ASaP weitere Fragen zu Proxys auftauchen, wenden Sie sich an den technischen Support.

## Aktivieren von Relay-Servern

Wenn ein Computer im Netzwerk nicht über eine direkte Verbindung zum Internet verfügt, ermöglicht die VirusScan ASaP-Funktion internetunabhängiges Aktualisieren, dass diese den Dienst verwenden können. In diesem Fall müssen Sie mindestens einen Computer im LAN als Relay-Server angeben.

#### HINWEIS

Wenn alle Computer im Netzwerk über eine Verbindung zum Internet verfügen, müssen keine Relay-Server eingerichtet werden.

Sie haben zwei Möglichkeiten, einen oder mehrere Computer als Relay-Server anzugeben:

- *Verwenden des Push Install-Dienstprogramms*
- *Mit VSSETUP*

### Verwenden des Push Install-Dienstprogramms

Um das Push Install-Dienstprogramm verwenden zu können, müssen Sie sich wie in [Schritt 2](#) bis [Schritt 4](#) des Abschnitts [Installation auf Seite 30](#) beschrieben, bei der Website anmelden. Sie geben die Computer an, die als Relay-Server verwendet werden sollen, indem Sie das Kontrollkästchen **Als Relay-Server einstellen** und dann auf **VirusScan ASaP installieren** klicken.

### Mit VSSETUP

Während der Hintergrundinstallation oder nach der Installation von VirusScan ASaP auf einem Computer kann der Administrator den Befehl `vssetup` mit der Variablen ausführen, die angibt, ob ein Computer ein Relay-Server ist. Die `vssetup`-Syntax unterscheidet sich in Abhängigkeit davon, ob es sich hierbei um die erste ASaP-Installation oder um Änderungen an einer vorhandenen Installation handelt.

#### Erste Installation

Während der Installation von VirusScan ASaP-Dienst verwendet `vssetup` die folgende Syntax, um einen Computer als Relay-Server einzurichten:

```
VSSETUP.EXE /RelayServer = 1
```

#### HINWEIS

Wenn Sie den Computer während der Installation nicht als Relay-Server angeben, lautet der Wert standardmäßig 0 (aus), und der Computer wird nicht als Relay-Server eingerichtet.

#### Ändern einer vorhandenen Konfiguration

Verwenden Sie zum Bearbeiten einer vorhandenen Installation von VirusScan ASaP `vssetup` mit der folgenden Syntax:

- Angeben eines Computers als Relay-Server:

```
VSSETUP.EXE /SetRelayServerEnable = 1
```

- Einrichten eines Relay-Server-Computers, so dass dieser nicht mehr als Relay-Server fungiert:

```
VSSETUP.EXE /SetRelayServerEnable = 0
```



## Testen von VirusScan ASaP

Sie können die Installation von VirusScan ASaP testen, indem Sie die EICAR Standard-Antivirustestdatei von [eicar.org](http://www.eicar.org) herunterladen. Wurde die Installation erfolgreich durchgeführt, entdeckt VirusScan ASaP die Testdatei und gibt eine Virenwarnmeldung aus. Beachten Sie, dass die EICAR-Testdatei kein Virus ist.

So testen Sie Ihre VirusScan ASaP-Installation:

- 1 Laden Sie die EICAR-Datei von folgender Site herunter:

<http://www.eicar.org/download/eicar.com>

Bei richtiger Installation unterbricht VirusScan ASaP das Herunterladen und zeigt ein Dialogfeld mit einer Viruswarnung an.

- 2 Klicken Sie in diesem Dialogfeld auf **OK**.
- 3 Klicken Sie im Dialogfeld für das Herunterladen der Datei auf **Abbrechen**.

Bei falscher Installation erkennt VirusScan ASaP **keinen** Virus und unterbricht das Herunterladen auch nicht. Wenn das Herunterladen nicht unterbrochen wird, löschen Sie über Windows Explorer die EICAR-Testdatei von der Arbeitsstation. Dann installieren Sie VirusScan ASaP-Dienst neu.



Dieser Abschnitt beschreibt, wie Sie Zugriff auf die **Customer Home**-Site erhalten und den VirusScan ASaP-Dienst verwalten können. Des Weiteren enthält der Abschnitt Informationen zum Virenschannen, Aktualisieren der Software und Lesen der Berichte.

- [Customer Home-Website](#)
- [Scannen](#)
- [Aktualisierungen](#)
- [Berichtsübersicht](#)
- [Lesen Ihrer Berichte](#)

## Customer Home-Website

Die **Customer Home**-Website enthält Verknüpfungen zu den Verwaltungsfunktionen Ihres VirusScan ASaP-Dienstes. Auf dieser Site können Sie Folgendes durchführen:

- [Anmelden](#)
- [Aktualisieren Ihres Benutzerprofils](#)
- [Hinzufügen neuer Dienste](#)
- [Aufrufen Ihrer Berichte](#)
- [Scannen](#)

## Anmelden

- 1 Öffnen Sie in Ihrem Browser die Webseite von McAfee VirusScan ASaP oder Ihrem Anbieter, und klicken Sie dann auf die Verknüpfung für **VirusScan ASaP**. Auf der Hauptseite befindet sich die Verknüpfung zur Anmeldung immer in der linken oberen Ecke unter dem McAfee Security-Logo.

### HINWEIS

Lassen Sie sich von Ihrem Vertreter oder Händler die exakte URL-Adresse für Ihre **Customer Home**-Website mitteilen.

- 2 Geben Sie zur Anmeldung bei der **Customer Home**-Website Ihren Benutzernamen und Ihr Kennwort ein:
  - ♦ **Benutzername:** Die E-Mail-Adresse, die Sie bei der Anmeldung für den Dienst angegeben haben (in der Regel die Adresse, unter der Sie die Begrüßungs-E-Mail-Nachricht erhalten haben).
  - ♦ **Kennwort:** In den meisten Fällen das Kennwort, das Sie bei der Anmeldung eingegeben haben.

Wenn Sie Ihr Kennwort vergessen haben, klicken Sie auf **Kennwort vergessen?**. Ihr Kennwort wird dann an Ihre E-Mail-Adresse geschickt.

Ihr Kennwort können Sie nach dem Anmelden jederzeit ändern, indem Sie Ihr Benutzerprofil aktualisieren. Beachten Sie dabei, dass das Kennwort aus mindestens 6 Zeichen bestehen muss.

#### **HINWEIS**

Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden. Beachten Sie dies bei der Eingabe Ihres Kennwortes.

## **Aktualisieren Ihres Benutzerprofils**

Zum Ändern von Einstellungen in Ihrem Benutzerprofil klicken Sie auf der **Customer Home**-Hauptseite auf die Verknüpfung **Profil aktualisieren**. Nehmen Sie an Ihrem Namen, Ihrer Adresse oder Ihrem Kennwort die gewünschten Änderungen vor. Speichern Sie die Änderungen, indem Sie auf **Profil aktualisieren** am unteren Rand der Seite klicken.

#### **HINWEIS**

Möglicherweise möchten Sie die E-Mail-Adresse ändern, unter der Sie auf die **Customer Home**-Website zugreifen. Viele Kunden legen für diesen Zweck eine spezielle E-Mail-Adresse an (z. B. `asap_admin@beispiel.com`), damit die E-Mail-Adresse problemlos auf einen neuen Administrator übertragen werden kann, wenn der alte VirusScan ASaP-Administrator die Firma verlässt.

## **Hinzufügen neuer Dienste**

Zum Hinzufügen neuer VirusScan ASaP-Dienste klicken Sie auf die Verknüpfung **Abonnement** am oberen Rand der **Customer Home**-Seite. Folgen Sie hier dem Anmeldeprozess, um Ihrem VirusScan ASaP-Dienst weitere Computer hinzuzufügen.

## Zugriffs- und Hilfsprogramme

Klicken Sie auf die Verknüpfung **Tools und Hilfsprogramme** am oberen Rand der **Customer Home**-Hauptseite, um die Verbindung mit einer Seite aufzubauen, die regelmäßig mit den neuesten Tools und Hilfsprogrammen zur Verwendung mit VirusScan ASaP aktualisiert wird.

## Aufrufen Ihrer Berichte

Auf Ihre Berichte können Sie auf drei verschiedene Arten von der **Customer Home**-Website zugreifen:

- Klicken Sie auf das Wort **Berichte**.
- Klicken Sie auf den Namen **VirusScan ASaP**, um eine Website mit einer Liste mit Optionen anzuzeigen. Klicken Sie auf **Berichte anzeigen**.
- Klicken Sie im nachfolgenden Satz auf das Wort **Berichten**:

Behalten Sie den Überblick über Ihr Netzwerk mit den VirusScan ASaP-**Berichten**. Aufgelistet werden u.a. die Anzahl und Typen von Viren, die gefunden und beseitigt wurden, Status des Systems usw.

Weitere Informationen zum Lesen Ihrer Berichte finden Sie unter [Berichtsübersicht auf Seite 41](#).

## Scannen

Der VirusScan ASaP-Dienst schützt Ihren Computer durch Virenschans. Das Scannen erfolgt automatisch. Sie können VirusScan ASaP jedoch auch dazu auffordern, indem Sie auf **Jetzt scannen** klicken.

- *Automatisches Scannen*
- *Die Funktion "Jetzt scannen"*
- *Nach Ausführung der Funktion "Jetzt scannen" erzeugte Berichte*

## Automatisches Scannen

In der Standardkonfiguration für den VirusScan ASaP-Dienst werden alle Dateien und Ordner, mit den Dateierweiterungen, die in den DAT-Dateien angegeben wurden, auf Ihrem Computer beim Zugriff auf diese gescannt.

E-Mail-Nachrichten werden beim Empfang nicht gescannt, aber wenn Sie eine E-Mail-Nachricht, die über eine in der DAT-Datei angegebenen Dateierweiterung verfügt, auf der Festplatte speichern, wird die Nachricht sofort gescannt.

Die Standardrichtlinie für das Scannen, die *Bei-Zugriff-Scanrichtlinie* ist:

- Alle Dateien, die den aktuellen Kriterien der Liste mit den Dateierweiterungen entsprechen, werden zunächst beim Öffnen und anschließend beim Schließen (sofern sie geändert wurden) gescannt.
- Die Dateierweiterungskriterien sind in den Virusdefinitionsdateien (DAT) definiert.
- Dem Administrator steht ein **Excluded Items Viewer** zur Verfügung. Damit kann er bestimmte Ordner oder Laufwerke vom Scannen bei Zugriff ausschließen.
- Alle E-Mail-Anhänge werden beim Zugriff gescannt. Damit wird die Arbeitsstation vor einem Virenbefall durch E-Mail-Anhänge geschützt.

## Excluded Items Viewer

Mit diesem Viewer können Sie festlegen, dass bestimmte Dateien oder Ordner nicht gescannt werden: Mit dem **Excluded Items Viewer** können Sie festlegen, welche Dateien und Ordner auf einer Arbeitsstation nicht gescannt werden sollen. Gehen Sie dazu folgendermaßen vor:

- 1 Zum Zugriff auf den **Excluded Items Viewer** geben Sie in Ihren Browser den folgenden URL ein:

`http://<ihr-provider.com>/vs2/exclude/exclude.htm`

### HINWEIS

Tragen Sie in den oben genannten URL die Adresse Ihres Providers ein.

- 2 Zum Hinzufügen eines Ordners oder einer Datei zu der Liste der Elemente, die *nicht* gescannt werden sollen, klicken Sie auf **Hinzufügen**. Verwenden Sie die Option **Durchsuchen**, um eine Datei oder einen Ordner auszuwählen. Klicken Sie auf **OK**.

### WARNUNG

Alle Elemente, die Sie dem **Excluded Items Viewer** hinzugefügt haben, werden von VirusScan ASaP während des automatischen Scannens nicht gescannt und deshalb auch nicht auf Viren überprüft. Wählen Sie nur Dateien aus, die sicher nicht infiziert sind.

- 3 Mit den Schaltflächen am unteren Rand des Viewers können Sie Ihrer Liste Elemente hinzufügen, Elemente in der Liste wählen und Elemente aus der Liste löschen.

- 4 Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

#### HINWEIS

Sie müssen auf den **Excluded Items Viewer** von derselben Arbeitsstation aus zugreifen, auf der Sie die Ausschlüsse konfigurieren möchten. Dieses Tool arbeitet nur local.

## Die Funktion "Jetzt scannen"

Ihr VirusScan ASaP-Dienst scannt automatisch die meisten Dateien, wenn auf diese zugegriffen wird. Möglicherweise möchten Sie aber ein bestimmtes Laufwerk oder einen bestimmten Ordner zu einem beliebigen Zeitpunkt scannen. Die Funktion **Jetzt scannen** gibt Ihnen dafür die Möglichkeit. So starten Sie unverzüglich einen Scan:

- 1 Klicken Sie mit der rechten Maustaste auf das **VirusScan ASaP**-Symbol im Symbolfeld, und wählen Sie **Jetzt scannen**
- 2 Geben Sie an, ob **Arbeitsplatz**, **Eigene Dateien** oder das **Diskettenlaufwerk** durchsucht bzw. durch Wahl von **Durchsuchen** nach einem Laufwerk oder Ordner gesucht werden soll. Klicken Sie auf den gewünschten Befehl.
- 3 Das Dialogfeld **Scan abgeschlossen** wird mit einer Zusammenfassung der Scanergebnisse angezeigt. Schließen Sie das Dialogfeld oder klicken Sie auf **Bericht**, um weitere Informationen anzuzeigen.

Alternativ können Sie mit der rechten Maustaste auf jede Datei oder jeden Ordner im Windows Explorer klicken und im angezeigten Menü auf **Jetzt scannen** wählen.

## Nach Ausführung der Funktion "Jetzt scannen" erzeugte Berichte

Nach Ausführung der Funktion **Jetzt scannen** für einen Ordner oder ein Laufwerk können Sie den Scan-Bericht anzeigen. Dazu klicken Sie auf **Bericht**.

Der Bericht wird in Ihrem Standardbrowserfenster geöffnet. Er enthält folgende Angaben:

- Scan-Statistik.
- Datum und Uhrzeit des Starts des Scanvorgangs.
- Verstrichene Zeit für den Scanvorgang.
- Version des Scan-Moduls und Virusdefinitionsdateien (DAT).
- Zeitpunkt der letzten Aktualisierung.
- Gescannte(s) Element(e) und Anzahl der gefundenen Infektionen.

- Eine Liste aller infizierten Dateien (sofern vorhanden) sowie deren Status und Virustyp. Folgende Statusangaben sind möglich:
  - ◆ **Infiziert:** Die Datei ist noch infiziert und befindet sich noch im System. Wahrscheinlich befindet sie sich in einem komprimierten Archiv (z. B. einem ZIP-Archiv) oder auf einem schreibgeschützten Datenträger.
  - ◆ **Gesäubert:** Die Datei wurde von der Virusinfektion gesäubert.
  - ◆ **Säubern fehlgeschlagen:** Die Datei konnte nicht gesäubert werden und wurde deshalb gelöscht.

Wenn der aktive Scanner eine infizierte Datei entdeckt, versucht er, die Datei zu säubern. Wenn sie gesäubert werden kann, wird die Arbeit des Benutzers nicht mit Virenalarmen unterbrochen. Wenn sie nicht gesäubert werden kann, wird jedoch ein Virusalarm mit der Meldung **Säubern fehlgeschlagen** angezeigt. Die infizierte Datei wird gelöscht. Alle Aktivitäten werden dem NOC (Network Operation Center) mitgeteilt.

## Aktualisierungen

Der VirusScan ASaP-Dienst wird von der AutoUpdate-Funktion automatisch aktualisiert. Der Benutzer kann die Aktualisierung des VirusScan ASaP-Dienstes mit der Funktion **Jetzt aktualisieren** aber auch selbst anfordern.

## Automatische Updates

Die automatische Aktualisierung von VirusScan ASaP erfolgt über eine Verbindung zum NOC-Server. Der Dienst ist so konfiguriert, dass er fünf Minuten nach dem Herstellen der Verbindung über das Netzwerk und dann in regelmäßigen Abständen während des Tages eine Prüfung auf neue Updates vornimmt.

Beispiel:

- Wenn ein Benutzer üblicherweise eine ständige Verbindung zum Internet hat, fragt der Computer des Benutzers beim Server in regelmäßigen Abständen während des Tages nach Updates nach.
- Wenn ein Benutzer jeden Morgen eine Verbindung zum Internet herstellt, prüft der Computer den Server jeden Tag fünf Minuten nach dem Anmelden und danach in regelmäßigen Abständen während des Tages auf Updates.

### HINWEIS

Wenn der Benutzer eine DFÜ-Verbindung ins Internet verwendet, nimmt der Computer eine Überprüfung nach neuen Updates fünf Minuten nach dem Einwählen vor. Am nächsten Tag wird die Überprüfung in regelmäßigen Abständen vorgenommen.



## Updates auf Anforderung

VirusScan ASaP aktualisiert sich zwar automatisch selbst, möglicherweise möchten Sie die Prüfung auf neue Updates auf dem NOC-Server dennoch manuell starten. So starten Sie eine Aktualisierung auf Anforderung:

- 1 Doppelklicken Sie auf das **VirusScan ASaP**-Symbol in der Symbolablage (oder klicken Sie mit der rechten Maustaste auf **Jetzt aktualisieren**).

Es wird ein Dialogfeld angezeigt, in dem der Fortschritt des Aktualisierungsvorgangs veranschaulicht wird. Weitere Informationen erhalten Sie, wenn Sie auf **Hilfe** klicken.

- 2 Wenn die Aktualisierung abgeschlossen ist, wird im Dialogfeld **Letzte Aktualisierung** und das betreffende Datum angezeigt. Ferner wird eine Liste der heruntergeladenen Dateien angezeigt.
- 3 15 Sekunden nach Abschluss der Aktualisierung wird das Dialogfeld automatisch geschlossen.

## Berichtsübersicht

Jede Arbeitsstation meldet den Verlauf der Virenskans, den Aktualisierungsstatus und das Erkennen von Viren durch Hochladen der Daten über eine Internet-Verbindung an das NOC (entweder direkt oder über einen Relay-Server). Die entsprechenden Berichte werden dann auf dem Server fortlaufend aktualisiert. In den Berichten werden alle installierten Computer für denselben Unternehmensschlüssel angezeigt.

Im VirusScan ASaP-Berichtswesen haben Sie folgende Möglichkeiten:

- Definieren und Anzeigen von Berichten nach logischen Gruppen
- Suchen von Arbeitsstationen nach Name oder E-Mail-Adresse.
- Hinzufügen und Löschen von Arbeitsstationen zu und von einer Gruppe
- Anzeigen von Standardberichten
- Sperren und Aufheben der Sperre des Empfangs von Aktualisierungen auf ausgewählten Arbeitsstationen.

- Ermitteln der Anzahl der Arbeitsstationen, auf denen sich infizierte Dateien befinden, und ihre Behandlung Der Status einer Datei kann der folgende sein:

<b>Gesäubert</b>	Es wurde ein Virus entdeckt und entfernt. Die Datei ist deshalb <i>gesäubert</i> und kann vom Benutzer sicher verwendet werden.
<b>Gelöscht</b>	Es wurde ein Virus entdeckt, die Datei konnte aber nicht gesäubert werden. Deshalb wurde die Datei <i>gelöscht</i> .
<b>Isoliert</b>	Ein Virus wurde gefunden und die Datei wurde in einen <i>Quarantäneordner</i> verschoben. Dort kann nur mit einem <b>Quarantine Viewer</b> auf sie zugegriffen werden.

### HINWEIS

Um auf den **Quarantine Viewer** zuzugreifen, halten Sie die **Strg-** und die **Umschalttaste** auf der Tastatur gedrückt und klicken Sie mit der rechten Maustaste auf das VirusScan ASaP-Symbol im Symbolfeld. Wählen Sie **Jetzt scannen | Quarantine Viewer**.

Um auf den **Quarantine Viewer** zugreifen zu können, müssen Sie über Administratorrechte auf dem Computer verfügen.

## Erstmaliges Erstellen von Gruppen

Mit VirusScan ASaP kann der Administrator für die Berichtsanalyse Gruppen mit Arbeitsstationen erstellen. Die Einteilung kann auf der Basis des Standorts, der Abteilung, des Computertyps oder eines anderen, für Ihr Unternehmen relevanten Kriteriums erfolgen.

Für jede Gruppe werden detaillierte Statistiken angezeigt. Zusätzlich werden alle statistischen Angaben am unteren Rand der Berichtstabelle in der Zeile **Alle Rechner** zusammengefasst. So verwenden Sie die Gruppenberichtsaktionen:

- **Systeme in einer Gruppe auflisten:** Klicken Sie auf die Verknüpfung **Liste** neben dem Gruppentitel oder auf den Gruppennamen.
- **Zusammenfassende Gruppeninformationen anzeigen:** Klicken Sie auf die Verknüpfung **Übersicht** neben dem Gruppentitel.
- **Alle DAT-Versionen innerhalb einer Gruppe anzeigen:** Klicken Sie auf die Verknüpfung **DAT** neben dem Gruppentitel.

- **Gruppen hinzufügen:** Durch Eingeben des Namens der zu erstellenden Gruppe im Feld **Gruppe hinzufügen** und anschließendes Klicken auf die Schaltfläche **Gruppe hinzufügen**.

#### HINWEIS

Gruppennamen dürfen höchstens 25 Zeichen groß sein.

- **Gruppen bearbeiten:** Klicken Sie in der Zeile für die betreffende Gruppe auf die Verknüpfung **Bearbeiten**.
- **Gruppen entfernen:** Klicken Sie in der Zeile für die betreffende Gruppe auf die Verknüpfung **Löschen**.

#### HINWEIS

Die Option **Löschen** ist nur für leere Gruppen verfügbar (es befinden sich keine Arbeitsstationen in dieser Gruppe).

### So fügen Sie einer Gruppe Arbeitsstationen hinzu:

- 1 Klicken Sie auf der Seite **Alle Gruppen verwalten** auf **Nicht zugewiesen**. Daraufhin wird eine Liste mit allen Arbeitsstationen angezeigt, die derzeit keiner Gruppe zugewiesen sind.
- 2 Wählen Sie eine oder mehrere Arbeitsstationen, indem Sie die Kontrollkästchen neben den betreffenden Namen aktivieren.
- 3 Wählen Sie im Menü neben der Verknüpfung **Verschieben nach**, um eine Gruppe auszuwählen.
- 4 Klicken Sie nach dem Wählen einer Gruppe auf **Verschieben nach**.
- 5 Wenn ein Bestätigungsdialogfeld angezeigt wird, klicken Sie auf **OK**.
- 6 Zur Rückkehr auf die Hauptseite und zum Anzeigen aller Gruppen klicken Sie auf **Alle Gruppen verwalten** am oberen rechten Seitenrand.

Um eine Arbeitsstation von einer Gruppe in eine andere zu verschieben, befolgen Sie dieselben Schritte. Weitere Informationen finden Sie unter [Mehr Details über ein System erhalten auf Seite 49](#).

## Lesen Ihrer Berichte

VirusScan ASaP-Berichte werden in Schichten präsentiert. Wenn Sie auf Ihrer **Customer Home-Site** auf die Verknüpfung **Berichte** klicken, werden Sie mit der Seite **Alle Gruppen verwalten** verbunden, die allgemeine Informationen und Details enthält, auf die Sie mit Hilfe von Verknüpfungen zugreifen können.

Klicken Sie auf der Seite **Alle Gruppen verwalten** auf einen Gruppennamen, um die Gruppenstatusseite anzuzeigen. Klicken Sie dort auf **Liste**, **Übersicht** oder **DAT**, um die Details einer Gruppe anzuzeigen.

## Seite Alle Gruppen verwalten

Auf der Seite **Alle Gruppen verwalten** werden alle Gruppen und deren Status angezeigt. Am oberen Tabellenrand befindet sich ein Pulldown-Menü mit der Bezeichnung **Berichtszeitraum**. Wählen Sie in diesem Menü aus, welcher Zeitraum angezeigt werden soll. Der größte Zeitraum beträgt ein Jahr, da Berichte auf dem Server nur ein Jahr gespeichert werden.

**Alle Gruppen verwalten**

Neue Gruppe hinzufügen:   Systemsuche  Systeme blockieren

Berichtszeitraum: Letzte 7 Tage Berichte werden für die Dauer von einem Jahr auf dem Server archiviert.

Gruppentitel	Kumuliert			Letzte 7 Tage			Verwaltung	
	Verwaltete Desktops	Veraltet	Gesäubert	Gelöscht	Isoliert	Gruppennamen bearbeiten	Gruppe löschen	
<b>Nicht zugewiesen</b>	27	27	0	0	0			
IT	2	2	0	0	0	<a href="#">Namen bearbeiten</a>		
Marketing	4	4	0	0	0	<a href="#">Namen bearbeiten</a>		
Purchasing	6	6	2	0	2	<a href="#">Namen bearbeiten</a>		
Sales	5	5	0	0	0	<a href="#">Namen bearbeiten</a>		
<b>Alle Rechner</b>	<b>44</b>	<b>44</b>	<b>2</b>	<b>0</b>	<b>2</b>			

**Alle Rechner** **Alle Rechner** zeigt die Summe aller Rechner in allen Gruppen, einschließlich aller nicht zugeordneten Rechner an. **Nicht zugewiesen** **Nicht zugewiesen** enthält immer alle neu hinzugefügten Rechner oder Rechner, die keiner Gruppe zugeordnet sind. Keine dieser Gruppen kann bearbeitet oder gelöscht werden.

---

**Kurzhilfe:**

**Gruppe anzeigen:**  
Klicken Sie auf den gewünschten "Gruppennamen". Wenn eine Gruppe keine verwalteten Desktops enthält, sind keine Berichte verfügbar.

**Hinzufügen einer neuen Gruppe:**  
Wenn Sie eine weitere "Gruppe" benötigen, die im aktuellen Profil nicht vorhanden ist, geben Sie den neuen Gruppennamen in das Textfeld ein, und klicken Sie auf die Schaltfläche "Gruppe hinzufügen".

**Gruppe löschen:**  
Klicken Sie auf "Löschen". Diese Funktion ist nur verfügbar, wenn alle dieser Gruppe zugeordneten Rechner verschoben oder gelöscht wurden. *Es lassen sich nur leere Gruppen löschen.*

Abbildung 3-2. Seite Alle Gruppen verwalten

Nach Auswahl eines Berichtszeitraums wird die Seite automatisch aktualisiert und zeigt dann an, wie viele Dateien im gewählten Zeitraum gesäubert, gelöscht und isoliert wurden. Die Spalten auf dieser Seite sind:

<b>Liste</b>	Eine Verknüpfung auf die Seite <b>Gruppenliste</b> .
<b>Übersicht</b>	Eine Verknüpfung auf die Seite <b>Gruppenüberblick</b> .
<b>DAT</b>	Eine Verknüpfung auf die Seite <b>DAT-Überblick</b> der Gruppe.
<b>Verwaltete Desktops</b>	Die Anzahl der zur Gruppe gehörenden Arbeitsstationen. Am unteren Rand der Tabelle ist unter <b>Alle Rechner</b> die Gesamtanzahl aufgeführt.
<b>Veraltet</b>	Die Anzahl der Systeme in der Gruppe, die über DAT-Dateien, die älter als 7 Tage sind, verfügen. <b>HINWEIS:</b> Die betreffenden Arbeitsstationen sind in den nachfolgenden Detailseiten mit einem blinkenden roten Symbol markiert.
<b>Gesäubert</b>	Die Anzahl der Dateien in der Gruppe, die während dem angegebenen Berichtszeitraum gesäubert wurden.
<b>Gelöscht</b>	Die Anzahl der Dateien in der Gruppe, die während dem angegebenen Berichtszeitraum gelöscht wurden.
<b>Isoliert</b>	Die Anzahl der Dateien in der Gruppe, die während dem angegebenen Berichtszeitraum isoliert wurden.
<b>Gruppennamen bearbeiten</b>	Damit können Sie den Namen der Gruppe ändern.
<b>Gruppe löschen</b>	Damit können Sie diese Gruppe aus Ihren Berichten löschen. <b>HINWEIS:</b> Es lassen sich nur leere Gruppen löschen.

Von dieser Seite aus können Sie auch:

- **Eine neue Gruppe hinzufügen:** Erstellen Sie eine neue Gruppe, indem Sie in das vorhandene Feld einen Namen eingeben und auf **Hinzufügen** klicken.
- **Eine Systemsuche durchführen:** Klicken Sie auf die Verknüpfung **Systemsuche**, um eine bestimmte Arbeitsstation in Ihren Berichten zu finden. Geben Sie einen vollständigen oder einen Teil eines Namens oder eine E-Mail-Adresse ein, nach der Sie Suchen möchten.
- **Eine Kopie Ihres Berichts herunterladen:** Berichte können in Microsoft Excel-, Microsoft Word- oder Standard-Text-Formaten heruntergeladen werden, indem Sie auf das entsprechende Symbol klicken.
- **Systeme blockieren:** Klicken Sie auf die Verknüpfung **Systeme blockieren** und wählen Sie ein oder mehrere System(e), die keine Aktualisierungen empfangen sollen.

### Mehr Details über eine Gruppe erhalten

Klicken Sie auf der Seite **Alle Gruppen verwalten** auf **Liste**, **Übersicht** oder **DAT**, um die Details einer Gruppe anzuzeigen. Auf diesen Seiten werden mehr Informationen über die Gruppe angezeigt.

- **Seite Gruppenliste:** Diese Seite enthält eine Liste aller Computer in dieser Gruppe, einschließlich Informationen über deren aktuelle DAT-Version, der E-Mail-Adresse, die mit dem Computer in Verbindung gebracht wird und mehr.
- **Seite Gruppenüberblick:** Diese Seite enthält ein Tortendiagramm und Diagramme, die die zusammenfassenden Informationen über die Gruppe in grafischer Form anzeigen.
- **Seite DAT-Überblick:** Diese Seite enthält ein Tortendiagramm und eine Tabelle, die aufschlüsselt, wie viele Computer über bestimmte DAT-Versionen verfügen.

Klicken Sie auf **Nicht zugewiesen**, um Details über alle Computer ohne Zuordnung anzuzeigen.

## Seite Gruppenliste

Wenn Sie auf die Verknüpfung **Liste** neben einem Gruppentitel klicken, werden Details über diese Gruppe in Listenform angezeigt. Die Gruppendetailangaben sind in Tabellenform aufgelistet. Sie umfassen Informationen zu den einzelnen Arbeitsstationen.

**Gruppenliste:Purchasing**

Hinzufügen einer neuen Gruppe:

Anzeigen: 10 | 25 | 50 | 100 | Alle Datensätze pro Seite Seite 1/1 (6 records)

Markierte Elemente in diese Gruppe verschieben: IT

Alle markieren <input type="checkbox"/>	Systemname	DAT-Version	DAT-Veröffentlichungsdatum	E-Mail-Adresse	Infizierte Dateien	Zuletzt infiziert
<input type="checkbox"/>	LAURA	4.0.4251	6/15/2003	Laura@sample-nai.com	6	9/4/2003 4:14:48 PM
<input type="checkbox"/>	NATHAN	4.0.4251	6/15/2003	Nathan@sample-nai.com	0	
<input type="checkbox"/>	PURCH6	4.0.4251	6/15/2003	Purch6@sample-nai.com	0	
<input type="checkbox"/>	PURCH7	4.0.4251	6/20/2003	Purch7@sample-nai.com	0	
<input type="checkbox"/>	PURCH8	4.0.4251	6/15/2003	Purch8@sample-nai.com	0	
<input type="checkbox"/>	PURCH9	4.0.4251	6/15/2003	Purch9@sample-nai.com	0	

Markierte Elemente in diese Gruppe verschieben: IT   Seite 1/1 (6 records)

---

**Kurzhilfe:**

**Sortieren von Tabellen:**  
Sie können die Tabelle sortieren, indem Sie auf eine Kopfzeile klicken.

**Hinzufügen einer neuen Gruppe:**  
Wenn Sie eine weitere Gruppe benötigen, die im aktuellen Profil nicht vorhanden ist, geben Sie den neuen Gruppennamen in das Textfeld ein, und klicken Sie auf die Schaltfläche 'Hinzufügen'.

**Symbole:**

- System auf dem neuesten Stand
- Veraltetes System
- Relay-Server auf dem neuesten Stand
- Veralteter Relay-Server

Ein System gilt als veraltet, wenn es eine DAT-Datei umfasst, die älter als 7 Tage ist.

Abbildung 3-3. Seite Gruppenliste

Wenn Sie auf den Spaltenkopf klicken, wird die Sortierreihenfolge zwischen absteigend und aufsteigend hin- und hergeschaltet. Die Tabelle enthält folgende Spalten:

<b>Systemname</b>	Der Name der Arbeitsstation aus den Windows-Netzwerkeinstellungen.
<b>DAT-Version</b>	Die Version der DAT-Datei (Virendefinitionsdatei) auf der Arbeitsstation.
<b>DAT-Veröffentlichungsdatum</b>	Das Datum, an dem die DAT-Version von McAfee Security veröffentlicht wurde.

<b>E-Mail-Adresse</b>	Die vom Benutzer bei der Installation des Dienstes in das Feld <b>E-Mail-Adresse</b> eingegebene Adresse. Dabei kann es sich um die E-Mail-Adresse des jeweiligen Benutzers, aber auch um eine andere beschreibende Angabe handeln, je nachdem was der Benutzer bei der Installation eingegeben hat (das Feld kann sogar leer sein).
<b>Infizierte Dateien</b>	Die Anzahl der auf der Arbeitsstation seit der Ausstellung der ersten Lizenz gefundenen infizierten Dateien.
<b>Zuletzt infiziert</b>	Datum und Uhrzeit der letzten Infektion der Arbeitsstation.

### Verschieben von Arbeitsstationen in eine andere Gruppe

Auf der Seite **Gruppenliste** können Sie Arbeitsstationen von einer Gruppe in eine andere verschieben. Gehen Sie dazu folgendermaßen vor:

- 1 Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Arbeitsstationen.
- 2 Wählen Sie in dem Pulldown-Menü neben **Markierte Elemente verschieben nach**, um eine neue Gruppe für die gewählten Arbeitsstationen auszuwählen.
- 3 Klicken Sie nach dem Wählen einer Gruppe auf **OK**.
- 4 Wenn das Bestätigungsdialogfeld angezeigt wird, klicken Sie auf **OK**.
- 5 Zur Rückkehr auf die Zusammenfassungsseite und zum Anzeigen aller Gruppen klicken Sie auf **Alle Gruppen verwalten** am oberen rechten Seitenrand.

### Löschen von Arbeitsstationen aus einer Gruppe

Auf der Seite **Gruppenliste** können Sie Arbeitsstationen löschen. Gehen Sie dazu folgendermaßen vor:

- 1 Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Arbeitsstationen.
- 2 Klicken Sie auf **Markierte löschen**, um die gewählten Arbeitsstationen zu löschen.

#### **HINWEIS**




Wenn Sie einen Computer löschen, wird er von den Berichtsseiten entfernt. Wenn Sie den VirusScan ASaP-Dienst wieder auf diesem Computer installieren, wird er bei der ersten Verbindung mit dem NOC jedoch wieder in den Berichten angezeigt.

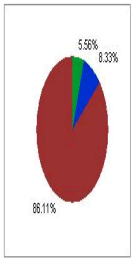


## Mehr Details über ein System erhalten

Wenn sie auf der Seite **Gruppenliste** auf einen Arbeitsstationsnamen klicken, wird die Seite **Detaillierter Systembericht** für dieses System angezeigt.

Systemdetails: SK101 [Verknüpfungen zu Berichten](#) | [All Machines Gruppenüberblick](#) | [All Machines Gruppenliste](#) | [Alle Gruppen verwalten](#) | [All Machines DAT-Überblick](#)

Systemname:	SK101	<b>Gefundene Viren</b>	<b>31</b>
Gruppe:	All Machines	 <b>Gesäubert</b>	2
Systemstatus:	Auf dem neuesten Stand	 <b>Gelöscht</b>	3
System-E-Mail-Adresse:	<a href="mailto:SK101@sample-nai.com">SK101@sample-nai.com</a>	 <b>Isoliert</b>	31
Letzte Server-Verbindung:	4/8/2003		
DAT-Version:	4.0.4251		
DAT-Veröffentlichungsdatum:	4/8/2003		
Systemsprache:	Unbekannt		
Modulversion:	4.1.60		
Relay-Server:	Nein		
Build-Nummer des Agenten:	2.6.2.1		
Build-Nummer des Scanners:	2.5.2.1		
Version des Betriebssystems:	Win2000		
Browser-Version:	IE6.1		



Anzeigen [10](#) | [25](#) | [100](#) | [Alle Datensätze pro Seite](#) Seite 1 von 1 (31 Datensätze)

Infizierte Datei	Virennamen	Gefunden am	Status
C:\Meine Dokumente\Brian\SULFNK.exe	<a href="#">W32/Nimda.gen@MM</a>	8/30/2002 11:09:24 AM	Isoliert
C:\Meine Dokumente\Brian\TECGG.exe	<a href="#">W32/Nimda.gen@MM</a>	9/10/2002 1:09:24 AM	Isoliert
C:\WINDOWS\SYSTEM\EDIL.DLL	<a href="#">JS/Kak</a>	9/10/2002 11:09:24 AM	Gesäubert
C:\WINDOWS\SYSTEM\EDIL.AA.DLL	<a href="#">W32/Nimda.gen@MM</a>	12/12/2002 7:09:24 AM	Isoliert

Abbildung 3-4. Seite Detaillierter Systembericht

Die Seite **Detaillierter Systembericht** enthält detaillierte Informationen über das jeweilige System. Von dieser Seite aus können Sie zu anderen Berichtsseiten zurückkehren, indem Sie den **Links zu Berichten** folgen.

## Seite Gruppenüberblick

Wenn Sie auf die Verknüpfung **Übersicht** neben einem Gruppentitel klicken, ein Überblick über diese Gruppe in Diagramm- und Tabellenform angezeigt.



Abbildung 3-5. Seite Gruppenüberblick

Auf der Seite **Gruppenüberblick** zeigen Tortendiagramme Virusinformationen für die betreffende Gruppe an. Über diesen Diagrammen ist jeder Virennamen und jeder Computernamen eine Verknüpfung.

- Wenn Sie auf einen Virennamen klicken, gelangen Sie zur AVERT-Virusinformationsbibliothek.
- Wenn Sie auf einen Computernamen klicken, wird die Seite **Detaillierter Systembericht** aufgerufen. Sie enthält vollständige Angaben zum System.

In einem Balkendiagramm wird der zeitliche Verlauf der Virenausbrüche nach Monaten aufgeschlüsselt angezeigt. Dieses Diagramm wird fortlaufend aktualisiert. Es umfasst immer die vergangenen zwölf Monate.

## Seite DAT-Überblick

Wenn Sie auf die Verknüpfung **DAT** neben einem Gruppentitel klicken, wird die Seite **DAT-Überblick** angezeigt. Diese Seite enthält eine Zusammenfassung der DAT-Versionen und der Softwaremodul-Versionen, die von den Systemen der Gruppe verwendet werden.

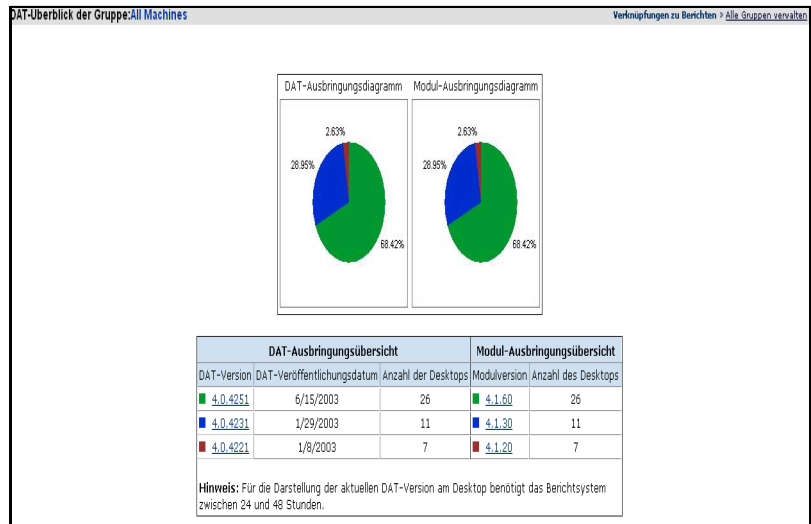


Abbildung 3-6. Seite DAT-Überblick

Tortendiagramme zeigen eine Aufschlüsselung, welche DAT- und Modulversionen aktuell auf allen Systemen in der Gruppe verwendet werden. Unterhalb der Diagramme befindet sich eine Tabelle mit genaueren DAT- und Scan-Modul-Ausbringungstatistiken.

- Die Zahlen in der Spalte **DAT-Version** sind Verknüpfungen auf eine Seite **Gruppenliste**, in der alle Systeme in der Gruppe angezeigt werden, die die gewählte DAT-Version verwenden.
- Die Zahlen in der Spalte **Modulversion** sind Verknüpfungen auf eine Seite **Gruppenliste** in der alle Systeme in der Gruppe angezeigt werden, die die gewählte Scan-Modul-Version verwenden.

## Blockieren von Systemen

Möglicherweise möchten Sie eine Arbeitsstation blockieren, so dass sie keine Aktualisierungen empfängt. Beispielsweise möchten Sie verhindern, dass ein Mitarbeiter, der seinen Computer zuhause oder ein Laptop für den Zugriff auf VirusScan ASaP verwendete, zukünftig Zugriff auf Aktualisierungen erhält, nachdem er die Firma verlassen hat.

Suchen und blockieren Sie mit Hilfe der nachfolgenden Funktionen nicht identifizierte Desktops in Ihrem Managed Service. Verwenden Sie die Suchfunktion, geben Sie mindestens ein Zeichen ein, und suchen Sie nach "Systemname" oder nach "E-Mail-Adresse". Alternativ können Sie die Liste "Zusammenfassung aller Rechner" durchblättern und die nicht identifizierten Desktops zum Blockieren markieren.

Suche nach blockierten Systemen

Systeme durchsuchen Systemname Übereinstimmende Search

**Systemblockierung:** Markieren Sie das Kontrollkästchen, um für die folgenden Systeme das Erhalten von Aktualisierungen zu blockieren. Klicken Sie hier, [um die Blockierung von Systemen aufzuheben](#).

Anzeigen: Datensätze pro Seite 10 | 25 | 50 | 100 | alle Seite 1 / 1 (6 records)

Alle markieren	Systemname	DAT-Version	DAT-Veröffentlichungsdatum	E-Mail-Adresse
<input type="checkbox"/>	LAURA	4.0.4251	6/15/2003	Laura@sample-nai.com
<input type="checkbox"/>	NATHAN	4.0.4251	6/15/2003	Nathan@sample-nai.com
<input type="checkbox"/>	PURCH6	4.0.4251	6/15/2003	Purch6@sample-nai.com
<input type="checkbox"/>	PURCH7	4.0.4251	6/15/2003	Purch7@sample-nai.com
<input type="checkbox"/>	PURCH8	4.0.4251	6/15/2003	Purch8@sample-nai.com
<input type="checkbox"/>	PURCH9	4.0.4251	6/15/2003	Purch9_@sample-nai.com

Seite 1 / 1 (6 records)

Abbildung 3-7. Seite Systeme blockieren

So blockieren Sie eine oder mehrere Arbeitsstationen:

- 1 Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Arbeitsstationen.
- 2 Klicken Sie entweder am oberen oder unteren Ende der Tabelle auf **Markierte blockieren**.
- 3 Wenn das Bestätigungsdialogfeld angezeigt wird, klicken Sie auf **OK**.
- 4 Zur Rückkehr auf die Zusammenfassungsseite und zum Anzeigen aller Gruppen klicken Sie auf **Alle Gruppen verwalten** am oberen rechten Seitenrand.

## Aufheben der Blockierung eines Systems

So heben Sie die Blockierung einer oder mehrerer Arbeitsstationen auf, diese können nun wieder Aktualisierungen empfangen:

- 1 Klicken Sie auf die Verknüpfung **Klicken Sie hier, um die Blockierung von Systemen aufzuheben** oder klicken Sie auf die Verknüpfung **Liste der blockierten Systeme** am oberen rechten Seitenrand. Eine **Liste der blockierten Systeme** wird eingeblendet und zeigt alle blockierten Systeme an.
- 2 Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Arbeitsstationen.
- 3 Klicken Sie entweder am oberen oder unteren Ende der Tabelle auf **Blockierung für Markierte aufheben**.
- 4 Wenn das Bestätigungsdiaologfeld angezeigt wird, klicken Sie auf **OK**.
- 5 Zur Rückkehr auf die Zusammenfassungsseite und zum Anzeigen aller Gruppen klicken Sie auf **Alle Gruppen verwalten** am oberen rechten Seitenrand.



Dieses Kapitel enthält eine Liste von häufig gestellten Fragen sowie bestimmte Fehlermeldungen und deren Lösungen.

- [Häufig gestellte Fragen \(FAQ\)](#)
- [Fehlermeldungen](#)
- [Kontaktaufnahme mit dem technischen Support](#)

## Häufig gestellte Fragen (FAQ)

- [Fragen zur Installation](#)
- [Fragen zum Scannen](#)
- [Fragen zu Berichten](#)
- [Fragen zum Aktualisieren](#)
- [Allgemeine Fragen](#)

### Fragen zur Installation

#### **Wie ermögliche ich es Benutzern ohne Administratorrechte, das URL-Verfahren der Installation zu nutzen?**

Bei Arbeitsstationen mit den Betriebssystemen Windows NT, Windows 2000 und Windows XP müssen bestimmte Voraussetzungen erfüllt sein, wenn der VirusScan ASaP-Dienst installiert wird. Diese Betriebssysteme verfügen über Sicherheitseinrichtungen, die verhindern, dass Benutzer ohne die Rechte eines lokalen Administrators Programme auf ihren Computern installieren.

Um diesen Benutzern die Installation von VirusScan ASaP zu ermöglichen, müssen Sie vorher einen Standalone-Installationsagenten auf der Arbeitsstation installieren.

Führen Sie für die Bereitstellung des Installationsagenten die folgenden Schritte aus:

- 1 Laden Sie den Standalone-Installationsagenten von der Seite **Tools und Hilfsprogramme** der **Customer Home**-Site herunter. Weitere Informationen finden Sie unter [Customer Home-Website auf Seite 35](#).

- 2 Stellen Sie die Datei unter Verwendung der von Ihnen dazu üblicherweise verwendeten Tools (z. B. Systems Management Server Installer von Microsoft, Windows NT-Login-Skripts oder Tivoli IT Director) auf den Arbeitsstationen bereit, und führen Sie sie aus. Die Ausführung dieser Datei setzt ein Account mit lokalen Administratorrechten voraus.
- 3 Wenn der Agent auf einer Arbeitsstation installiert wurde, kann jeder Benutzer den VirusScan ASaP-Dienst installieren.

### **Spielt es eine Rolle, welche E-Mail-Adresse beim Installieren von VirusScan ASaP eingegeben wird?**

Anhand dieser E-Mail-Adresse wird in Ihren Online-Verwaltungsberichten die Arbeitsstation identifiziert. Die Verwendung einer E-Mail-Adresse bildet eine Verknüpfung zum jeweiligen Benutzer. Es kann aber auch eine Beschreibung oder gar nichts in das Feld eingegeben werden.

### **Wo erhalte ich eine Kopie meines Installations-URL?**

Wenn Sie den Installations-URL, der verwendet wird, um den VirusScan ASaP-Dienst herunterzuladen, verlegt haben, können Sie eine per E-Mail-Nachricht-Nachricht gesendete Kopie dieses URLs anfordern. Gehen Sie dazu folgendermaßen vor:

- 1 Klicken Sie auf der **Customer Home**-Site auf **Eigene Dienste**. Daraufhin wird eine Liste mit allen Diensten angezeigt, die Sie zurzeit abonniert haben.
- 2 Klicken Sie auf die Verknüpfung **Haben Sie die VirusScan ASaP-Download-URL vergessen?**
- 3 Eine E-Mail-Nachricht mit der Installations-URL-Adresse wird an Ihre E-Mail-Adresse gesandt.

In Ihrem Installations-URL ist der Firmenschlüssel enthalten. Der Firmenschlüssel besteht aus der Zahl hinter den Zeichen **cx=** im URL.

### **Beim Versuch, VirusScan ASaP zu installieren, wird die Meldung "Ungültige Berechtigung" angezeigt, d. h., Sie sind nicht berechtigt, auf die betreffende Seite zuzugreifen.**

In den meisten Fällen wurde der URL in Ihrer E-Mail-Nachricht abgeschnitten oder falsch formatiert. Sie müssen den vollständigen URL *ohne Leerzeichen* verwenden. Wenn das Klicken auf die Verknüpfung in Ihrer E-Mail-Nachricht nicht den gewünschten Effekt hat, müssen Sie den URL möglicherweise in Ihren Webbrowser kopieren.



### Die Installation wird unter Verwendung von Netscape durchgeführt und das Plug-In funktioniert nicht.

Das VirusScan ASaP-Plug-in für Netscape funktioniert nur mit den Browser-Versionen 4.x. Wenn Sie eine höhere Version von Netscape als Standardbrowser verwenden, müssen Sie die Installation von VirusScan ASaP mit Internet Explorer durchführen.

Um die Installation unter Verwendung des Internet Explorers durchzuführen, kopieren Sie die Verknüpfung in Internet Explorer, anstelle die Installations-URL-Adresse anzuklicken (der automatisch in Netscape geladen wird), und der Installationsvorgang wird weiter ausgeführt.

#### HINWEIS

Sobald VirusScan ASaP installiert wurde, können Sie Netscape als Standardbrowser verwenden.

### Beim Versuch, VirusScan ASaP zu installieren, erhalte ich die Meldung "MyINX Error".

Das bedeutet, dass sich auf Ihrem Computer noch eine andere Virussoftware befindet. Möglicherweise war auf Ihrem Computer schon ein Virenschutzprogramm vorinstalliert, als Sie ihn gekauft haben. So beheben Sie dieses Problem:

- 1 Öffnen Sie in der Systemsteuerung das Modul **Software**.
- 2 Deinstallieren Sie alle hier angezeigten Virenschutzprogramme, auch VirusScan ASaP.
- 3 Führen Sie die **VirusScan ASaP Cleanup Utility** aus (verfügbar auf Ihrer **Customer Home**-Website).
- 4 Starten Sie den Installationsvorgang von VirusScan ASaP neu.

## Fragen zum Scannen

### Wie gehe ich vor, wenn ich bestimmte Dateien oder Verzeichnisse vom Scannen auf Viren ausschließen möchte?

Beim **Excluded Items Viewer** handelt es sich um ein Online-Dienstprogramm für VirusScan ASaP, die Administratoren die Verwaltung des Ausschlusses von Dateien und Verzeichnissen für VirusScan ASaP ermöglicht, ohne dass dazu die Registrierung direkt bearbeitet werden muss. Administratoren können Ausschlüsse anzeigen, hinzufügen und löschen. Weitere Informationen dazu finden Sie unter [Excluded Items Viewer auf Seite 38](#).

Zur Verwendung des **Excluded Items Viewers** geben Sie in Ihren Browser den folgenden URL ein:

`http://virusscanasap.mcafeesasap.com/vs2/exclude/exclude.htm`

VirusScan ASaP muss bereits auf dem Computer installiert sein, über den Sie auf den **Excluded Items Viewer** zugreifen.

### **HINWEIS**

Der URL zum Ausschlusstool kann von Anbieter zu Anbieter variieren. Wenden Sie sich an Ihren Vertreter oder Händler, wenn Sie nicht das McAfee Security VirusScan ASaP NOC nutzen.

## Fragen zu Berichten

### **Wie finde ich meine Berichte?**

Ihre Berichte können Sie über Verknüpfungen auf der **Customer Home**-Website aufrufen. Klicken Sie auf der Hauptseite auf die Verknüpfung **Berichte starten**.

### **In meinem Bericht tauchen einige meiner Computer nicht auf.**

Wenn Ihre Firma weitere Knoten erstellt hat oder ein Upgrade von der Testversion zur Vollversion durchgeführt hat, haben Sie unter Umständen, wenn Sie sich mit einer neuen E-Mail-Adresse angemeldet haben, einen neuen Kundenschlüssel und URL für die Installation erhalten.

Wenn Sie zwei verschiedene Kundenschlüssel (CK, Customer Keys) haben, werden die Berichte an zwei verschiedenen Stellen angezeigt. Deshalb müssen die Benutzer, die noch mit der Testversion arbeiten, unter Verwendung der mit dem neuen Schlüssel verknüpften Installations-URL-Adresse eine Neuinstallation vornehmen.

### **Meine geklonten Systeme sind in Berichten als ein Computer aufgeführt.**

VirusScanASaP erzeugt nach seiner Installation eine eindeutige System-ID. Wenn ein Laufwerk nach der Installation von VirusScanASaP gespiegelt wird, haben alle geklonten Systeme dieselbe ID. Dieses Problem umgehen Sie, indem Sie VirusScan ASaP nach dem Neustart der neuen Systeme installieren. Das können Sie im Rahmen des Hintergrundinstallationsverfahrens automatisch durchführen lassen.

### **Wie lange werden Berichtsdaten auf dem Server gespeichert?**

Zurzeit werden Ihre Daten für den gesamten Lizenzzeitraum gespeichert. Bei Verlängerung der Lizenz wird die Speicherung fortgesetzt.

## Fragen zum Aktualisieren

### Wann nimmt VirusScan ASaP eine Prüfung auf Updates vor?

Die automatische Aktualisierung von VirusScan ASaP erfolgt über eine Verbindung zum NOC-Server. Der Dienst ist so konfiguriert, dass er fünf Minuten nach dem Herstellen der Verbindung über das Netzwerk und dann in regelmäßigen Abständen während des Tages eine Prüfung auf neue Updates vornimmt.

Eine Aktualisierung kann auch von Hand ausgelöst werden. Dazu klicken Sie mit der rechten Maustaste auf das VirusScan ASaP-Symbol in der Systemablage. Dann wählen Sie die Option **Jetzt aktualisieren**.

## Allgemeine Fragen

### Kann ich eine Lizenz von einer Arbeitsstation auf eine andere übertragen?

Ja, Sie können VirusScan ASaP auf einer Arbeitsstation deinstallieren und auf einer anderen wieder installieren, ohne dass sich dadurch die Anzahl Ihrer Lizenzen verändert. Die alte Arbeitsstation wird auf dem VirusScan ASaP-Buchhaltungssystem automatisch von der Gesamtanzahl an Lizenzen abgezogen. Die Anzahl Ihrer Lizenzen bleibt deshalb gleich. Führen Sie dazu folgende Schritte aus:

- 1 Deinstallieren Sie VirusScan ASaP von der alten Arbeitsstation. Weitere Informationen finden Sie unter [Deinstallieren vorhandener Antivirusanwendungen auf Seite 20](#).
- 2 Rufen Sie die Seite **Berichte** auf, und löschen Sie die Arbeitsstation dort, damit Arbeitsstationen nicht doppelt aufgeführt sind. Weitere Informationen finden Sie unter [Löschen von Arbeitsstationen aus einer Gruppe auf Seite 48](#).
- 3 Installieren Sie VirusScan ASaP auf der neuen Arbeitsstation.
- 4 Die neue Arbeitsstation wird bei der ersten Verbindung zum NOC automatisch auf der Seite **Berichte** angezeigt.

### Mein Computer ist abgestürzt, und ich musste das Betriebssystem neu installieren. Hat dies Einfluss auf die Anzahl meiner Lizenzen?

Nein, die Anzahl Ihrer Lizenzen verändert sich dadurch nicht. Die alte Arbeitsstation wird auf dem VirusScan ASaP-Buchhaltungssystem automatisch von der Gesamtanzahl an Lizenzen abgezogen, wenn Sie sie von der Seite **Berichte** löschen. Die Anzahl Ihrer Lizenzen bleibt deshalb konstant.

- 1 Rufen Sie Ihre Seite **Berichte** auf, und löschen Sie den ursprünglichen Eintrag für die Arbeitsstation. Weitere Informationen finden Sie unter [Löschen von Arbeitsstationen aus einer Gruppe auf Seite 48](#).
- 2 Installieren Sie VirusScan ASaP auf der neu eingerichteten Arbeitsstation.
- 3 Die Arbeitsstation mit dem neuen Betriebssystem wird bei der ersten Verbindung zum NOC automatisch auf der Seite **Berichte** angezeigt.

### Ist mein PC vor E-Mail-Viren geschützt?

Ja. VirusScan ASaP scannt Dateien beim Zugriff auf diese. Wenn auf Dateien oder E-Mail-Anhänge zugegriffen wird bzw. diese geöffnet werden, findet ein Virens캔 statt. VirusScanASaP säubert infizierte E-Mail-Nachrichten nicht, solange sie ungelesen sind, sondern stoppt den Virus beim Zugriff.

### Ist es sinnvoll, gemeinsam mit VirusScan ASaP einen E-Mail-Scanner einzusetzen?

Ein E-Mail-Scanner wie GroupShield<sup>®</sup> oder ein Gateway-SMTP-Scanner wie Webshield<sup>®</sup> kann gemeinsam mit VirusScan ASaP eingesetzt werden. Sie sind dann auf mehreren Ebenen gegen Viren geschützt. Ein E-Mail-Scanner entdeckt Viren auf dem Server, bevor die infizierte Nachricht auf Ihren PC gelangt.

### Ich habe einen Virus auf meinen PC kopiert, es scheint aber nichts zu passieren. Warum hat VirusScan ASaP den Virus nicht entdeckt?

VirusScan ASaP ist so konzipiert, dass es Viren im Hintergrund entdeckt und beseitigt. Ein Eingriff durch den Benutzer ist dabei nicht erforderlich. Die meisten Virenarten werden gelöscht, ohne dass der Benutzer davon in Kenntnis gesetzt wird. Grund dafür ist, dass der Benutzer nicht abgelenkt werden und sich nicht unnötig oft an den Support wenden soll. Die Entdeckung von Viren wird immer in den Administratorberichten vermerkt. Ob der Virus gefunden wurde, können Sie in den Online-Berichten auf Ihrer **Customer Home**-Site prüfen.

### Woher bekomme ich die Cleanup Utility?

Die **Cleanup Utility**, die alle Spuren des VirusScan ASaP-Dienstes entfernt, können Sie von folgender Site herunterladen:

<http://virusscanasap.mcafeesasap.com/vs2/bin/myciocleanup.exe>

#### **HINWEIS**

Der URL zur **Cleanup Utility** kann von Anbieter zu Anbieter variieren. Wenden Sie sich an Ihren Vertreter oder Händler, wenn Sie nicht das McAfee Security VirusScan ASaP NOC nutzen.

**Wenn ich den Mauszeiger über das VirusScan ASaP-Symbol im Systemfeld bewege, wird die Nachricht "Ihr Abonnement ist abgelaufen" angezeigt.**

Entweder ist das VirusScan ASaP-Konto abgelaufen oder es liegt ein anderes Problem mit dem Konto vor. Sie können eine Kopie Ihres Unternehmensschlüssels per E-Mail erhalten und versuchen, VirusScan ASaP erneut zu installieren. Gehen Sie dazu folgendermaßen vor:

- 1 Stellen Sie eine Verbindung zu Ihrer **Customer Home**-Site her.
- 2 Klicken Sie auf die Registerkarte **Eigene Dienste**.
- 3 Am unteren Rand der Seite wird der Text **Haben Sie die VirusScan ASaP-Download-URL vergessen?** Klicken Sie auf die Verknüpfung **Hier klicken**.
- 4 Die Download-URL-Adresse, der Ihren Unternehmensschlüssel beinhaltet wird zu der E-Mail-Adresse verschickt, die Sie bei der Registrierung angegeben haben.
- 5 Folgen Sie den nachstehenden zur [Internet-URL-Installation auf Seite 24](#).

Wenn die Meldung über ein abgelaufenes Abonnement nach der erneuten Installation weiterhin angezeigt wird, wenden Sie sich an Ihre Support-Niederlassung.

**Wenn ich den Mauszeiger über das VirusScan ASaP-Symbol im Systemfeld bewege, wird die Nachricht "VirusScan ASaP ist veraltet" angezeigt.**

Diese Meldung bedeutet, dass Ihre Software seit über zwei Wochen nicht aktualisiert wurde. Melden Sie sich auf der **Customer Home**-Site an und überprüfen Sie Ihre Berichte nach weiteren Informationen zum Aktualisierungsverlauf dieser bestimmten Arbeitsstation. Weitere Informationen zur Verständlichkeit der Berichte finden Sie unter [Seite DAT-Überblick auf Seite 51](#).

## Fehlermeldungen

Dieser Abschnitt enthält einige geläufige Fehlermeldungen und deren Lösungen.

- [Freigegebenes Remote-Verzeichnis nicht gefunden](#)
- [Die Installation kann nicht fortgesetzt werden, da Sie keine zentrale Agentenkomponente akzeptiert haben...](#)
- [Invalid Entitlement Error](#)
- [Ihre aktuellen Sicherheitseinstellungen verhindern die Ausführung von ActiveX-Steuerelementen auf dieser Seite](#)
- [MyASUtil.SecureObjectFactory](#)

- *Es konnte keine Verbindung zum McAfee ASaP-Aktualisierungsserver hergestellt werden*
- *Cab Installer-Objekt kann nicht erstellt werden*
- *URL-Download in Datei fehlgeschlagen*

## Freigegebenes Remote-Verzeichnis nicht gefunden

Diese Fehlermeldung wird bei einer fehlgeschlagenen Push-Installation angezeigt. Die Arbeitsstationen, auf denen VirusScan ASaP installiert wurde, erfüllen eine oder mehrere der folgenden Voraussetzungen nicht:

- Auf der Arbeitsstation müssen die Datei- und die Druckfreigabe aktiviert sein.
- Auf der Arbeitsstation muss die Zugangssteuerung auf Benutzerebene aktiviert sein.
- Der als Administrator fungierende Benutzer, der die Push-Installation einleitet, muss auf der Arbeitsstation Administratorrechte für die Domäne haben.
- Auf der Arbeitsstation darf nicht Microsoft Windows XP Home Edition installiert sein, da dieses Betriebssystem keine Windows NT-Domänenanmeldungen unterstützt.

Prüfen Sie, ob auf der betreffenden Arbeitsstation die entsprechenden Freigaben aktiviert sind, und ob Sie über Administratorrechte zur Durchführung der Push-Installation auf der Arbeitsstation verfügen. Gehen Sie dazu folgendermaßen vor:

- 1 Klicken Sie auf Ihrem Computer auf **Start**, und wählen Sie die Option **Ausführen**.
- 2 Geben Sie in das Textfeld **Öffnen:** die Zeichenfolge `\\CPUNAME\ADMIN$` ein (CPUNAME ist der Name des Computers, auf dem die Push-Installation erfolgen soll). Klicken Sie dann auf **OK**.

### **HINWEIS**

Das funktioniert nicht unter Microsoft Windows XP Home Edition, da dieses Betriebssystem keine Windows NT-Domänenanmeldungen unterstützt.

- 3 Als Ergebnis der Ausführung dieses Befehls wird das `\WINDOWS`-Verzeichnis des Computers angezeigt, auf dem die Installation erfolgen soll. Wenn Sie für diesen Computer nicht über die erforderlichen Administratorrechte verfügen oder wenn bei diesem Computer nicht die entsprechenden Zugangsrechte auf Benutzerebene und Freigaben aktiviert sind, wird ein Fehlermeldungsfeld angezeigt, das besagt, dass der Netzwerkpfad nicht gefunden wurde.
- 4 Informationen zum Korrigieren der Netzwerkeinstellungen finden Sie in der entsprechenden Windows-Dokumentation.

## Die Installation kann nicht fortgesetzt werden, da Sie keine zentrale Agentenkomponente akzeptiert haben...

Der vollständige Text der Fehlermeldung ist **Die Installation kann nicht fortgesetzt werden, da Sie keine zentrale Agentenkomponente akzeptiert haben, Sie über keine Administratorrechte auf dem Rechner verfügen oder andere Probleme aufgetreten sind**. Diese lange Fehlermeldung kann mehrere Ursachen haben.

### Lösung 1

Meistens lässt sich dieses Problem durch Leeren des Internet Explorer-Caches und Anpassen der Sicherheitsstufeneinstellungen beheben.

So leeren Sie den Internet Explorer-Cache:

- 1 Öffnen Sie auf eine der folgenden Arten das Dialogfeld **Eigenschaften**:
  - ◆ Klicken Sie mit der rechten Maustaste auf das **Internet Explorer**-Symbol auf dem Desktop, und wählen Sie die Option **Eigenschaften**.
  - ◆ Öffnen Sie das **Internet**-Modul in der **Systemsteuerung**.
- 2 Klicken Sie auf **Dateien Löschen**.
- 3 Wählen Sie die Option **Alle Offlineinhalte löschen**. Während des Löschvorgangs wird eine Sanduhr angezeigt. Nach Abschluss des Vorgangs verschwindet die Sanduhr.
- 4 Klicken Sie auf **OK**.
- 5 Klicken Sie auf **Einstellungen**.
- 6 Klicken Sie auf **Dateien anzeigen**.
- 7 Klicken Sie auf **Bearbeiten | Alles markieren**.
- 8 Klicken Sie auf **Datei | Löschen**. Es kann eine Weile dauern, bis alle Dateien gelöscht sind. Nach Abschluss des Löschvorgangs kehren Sie zum Dialogfeld **Eigenschaften** zurück.
- 9 Klicken Sie auf **OK**.

So passen Sie die Sicherheitseinstellungen an:

- 1 Öffnen Sie auf eine der folgenden Arten das Dialogfeld **Eigenschaften**:
  - ◆ Klicken Sie mit der rechten Maustaste auf das **Internet Explorer**-Symbol auf dem Desktop, und wählen Sie die Option **Eigenschaften**.
  - ◆ Öffnen Sie das **Internet**-Modul in der **Systemsteuerung**.
- 2 Öffnen Sie die Registerkarte **Sicherheit**.
- 3 Klicken Sie auf **Standardstufe**.

- 4 Klicken Sie auf **Übernehmen**.
- 5 Klicken Sie auf **Stufe anpassen**.
- 6 Wählen Sie unter den Überschriften **ActiveX-Steuerelemente** und **Scripting** für jede Option **Aktivieren**.
- 7 Klicken Sie auf **OK**.
- 8 Öffnen Sie die Registerkarte **Erweitert**.
- 9 Klicken Sie auf **Wiederherstellen**.
- 10 Klicken Sie auf **OK**.

### Lösung 2

Wenn sich das Problem durch die in Lösung 1 beschriebenen Fehlerbehebungsmaßnahmen für den Cache und die Sicherheitseinstellungen nicht beheben lässt, ist möglicherweise eine fehlende Systemdatei REGEDIT.EXE Ursache des Problems. Suchen Sie im Verzeichnis \WINDOWS der Arbeitsstation nach der Datei.

Wenn die Datei fehlt, kann VirusScan ASaP nicht die erforderlichen Einträge in die Registrierung schreiben. Kopieren Sie die Datei zur Behebung des Problems von einem anderen Computer mit demselben Betriebssystem.

## Invalid Entitlement Error

Die häufigste Ursache für diesen Fehler besteht darin, dass der URL in Ihrer E-Mail-Nachricht abgeschnitten wurde oder falsch formatiert ist. Sie müssen den vollständigen URL ohne Leerzeichen verwenden. (Wenn das Klicken auf die Verknüpfung in Ihrer E-Mail-Nachricht nicht den gewünschten Effekt hat, müssen Sie den URL möglicherweise kopieren und im Webbrowser einfügen.)

## Ihre aktuellen Sicherheitseinstellungen verhindern die Ausführung von ActiveX-Steuerelementen auf dieser Seite

Siehe [Die Installation kann nicht fortgesetzt werden, da Sie keine zentrale Agentenkomponente akzeptiert haben....](#) Führen Sie die dort vorgeschlagenen Schritte aus.

## MyASUtil.SecureObjectFactory

Diese Fehlermeldung bedeutet, dass das SecureObjectFactory Class-Programm beschädigt ist. Um dies zu überprüfen, ermitteln Sie den Status der SecureObjectFactory Class-Programmdatei. Dazu gehen Sie wie folgt vor:

- 1 Starten Sie Internet Explorer.
- 2 Wählen Sie im Menü **Extras Internetoptionen**.



- 3 Klicken Sie im Bereich **Temporäre Internetdateien** des Dialogfelds auf die Schaltfläche **Einstellungen**. Das Dialogfeld **Einstellungen** wird geöffnet.
- 4 Klicken Sie auf **Objekte anzeigen**. Damit öffnen Sie den Ordner **Downloaded Program Files**.
- 5 Suchen Sie den Eintrag für **SecureObjectFactory Class**. Beachten Sie die Angaben in den Spalten **Status** und **Erstellungsdatum** an:
  - ◆ Wenn unter Status und Erstellungsdatum **Unbekannt** angegeben ist, löschen Sie die SecureObjectFactory Class-Programmdatei. Nehmen Sie eine Deinstallation und Neuinstallation von VirusScan ASaP vor, um die Datei neu zu laden.
  - ◆ Wenn als Status **Installiert** angegeben ist und die Datumsangabe richtig ist, liegt an der Datei keine Beschädigung vor.
  - ◆ Wenn die Spalte **Status** eine andere Angabe enthält, wenden Sie sich mit dieser Information an den technischen Support.

**HINWEIS**

Wenn keine Spalte **Status** angezeigt wird, stellen Sie die Anzeigoptionen auf **Details**.

## Cab Installer-Objekt kann nicht erstellt werden

Eine mögliche Ursache dafür ist, dass der Dienst MYAGTSVC.EXE nicht mehr auf dem Computer ausgeführt wird. Um MYAGTSVC.EXE manuell zu starten, führen Sie folgende Schritte aus:

- 1 Klicken Sie im Menü **Start** auf **Ausführen**.
- 2 Geben Sie den Pfad zu MYAGTSVC.EXE an (Sie können die Funktion **Durchsuchen** verwenden, um die Datei zu finden) und fügen Sie die Option `-start` hinzu. Beispiel:

```
C:\winnt\mycio\agent\myagtsvc.exe -start
```

- 3 Klicken Sie auf **OK**.

Wenn dadurch das Problem nicht gelöst werden kann, wenden Sie sich an den technischen Support.

**HINWEIS**

Dabei handelt es sich um einen Fehler von Microsoft Internet Explorer. Zu seiner Behebung muss möglicherweise ein Microsoft-Patch installiert werden.

## Es konnte keine Verbindung zum McAfee ASaP-Aktualisierungsserver hergestellt werden

Dieser Fehler kann mehrere Ursachen haben, meistens lässt er sich jedoch durch Leeren des Internet Explorer-Cache und Einstellen der Sicherheitsstufe auf **Mittel** beheben.

So leeren Sie den Internet Explorer-Cache:

- 1 Öffnen Sie auf eine der folgenden Arten das Dialogfeld **Eigenschaften**:
  - ◆ Klicken Sie mit der rechten Maustaste auf das **Internet Explorer**-Symbol auf dem Desktop, und wählen Sie die Option **Eigenschaften**.
  - ◆ Öffnen Sie das **Internet**-Modul in der **Systemsteuerung**.
- 2 Klicken Sie auf die Schaltfläche **Dateien löschen** (Registerkarte **Allgemein**).
- 3 Wählen Sie die Option **Alle Offlineinhalte löschen**. Während des Löschvorgangs wird eine Sanduhr angezeigt. Nach Abschluss des Vorgangs verschwindet die Sanduhr.
- 4 Klicken Sie auf **OK**.
- 5 Klicken Sie auf **Einstellungen**.
- 6 Klicken Sie auf **Dateien anzeigen**.
- 7 Klicken Sie auf **Bearbeiten | Alles markieren**.
- 8 Klicken Sie auf **Datei | Löschen**. Es kann eine Weile dauern, bis alle Dateien gelöscht sind. Nach Abschluss des Löschvorgangs kehren Sie zum Dialogfeld **Eigenschaften** zurück.
- 9 Klicken Sie auf **OK**.

So passen Sie die Sicherheitseinstellungen an:

- 1 Öffnen Sie auf eine der folgenden Arten das Dialogfeld **Eigenschaften**:
  - ◆ Klicken Sie mit der rechten Maustaste auf das **Internet Explorer**-Symbol auf dem Desktop, und wählen Sie die Option **Eigenschaften**.
  - ◆ Öffnen Sie das **Internet**-Modul in der **Systemsteuerung**.
- 2 Öffnen Sie die Registerkarte **Sicherheit**.
- 3 Klicken Sie auf **Standardstufe**.
- 4 Klicken Sie auf **Übernehmen**.
- 5 Klicken Sie auf **Stufe anpassen**.
- 6 Wählen Sie unter den Überschriften **ActiveX-Steuerelemente** und **Scripting** für jede Option **Aktivieren**.

- 7 Klicken Sie auf **OK**.
- 8 Öffnen Sie die Registerkarte **Erweitert**.
- 9 Klicken Sie auf **Wiederherstellen**.
- 10 Klicken Sie auf **OK**.

Wenn sich das Problem durch die hier beschriebenen Fehlerbehebungsmaßnahmen für den Cache und die Sicherheitseinstellungen nicht beheben lässt, sind möglicherweise Ihre Proxy- oder Firewall-Einstellungen Ursache des Problems. Siehe [Wenn Sie eine Firewall oder einen Proxy-Server verwenden auf Seite 31](#).

## URL-Download in Datei fehlgeschlagen

Diese Fehlermeldung wird nur bei Windows 98-Systemen angezeigt. Für den hier vorgeschlagenen Lösungsansatz muss im Menü **Start** der Eintrag **Microsoft Plus! 98** angezeigt werden. Wenn das nicht der Fall ist, wenden Sie sich an den technischen Support. Andernfalls gehen Sie folgendermaßen vor:

- 1 Wählen Sie im Menü **Start** die Option **Einstellungen | Systemsteuerung**.
- 2 Doppelklicken Sie auf **Software**.
- 3 Wählen Sie **Microsoft Plus! 98**.
- 4 Klicken Sie auf **Hinzufügen/Entfernen**. Damit öffnen Sie das Dialogfeld **Microsoft Plus!-Setup**.
- 5 Wählen Sie **Hinzufügen/Entfernen**, und klicken Sie dann auf **Weiter**.
- 6 Gehen Sie ans Ende der Liste mit den Komponenten, und deaktivieren Sie **VirusScan**.
- 7 Klicken Sie zweimal auf **Weiter** und dann auf **Fertig stellen**.
- 8 Starten Sie den Computer neu. Schließen Sie nach dem Hochfahren das Modul **Software** und die **Systemsteuerung**.

VirusScan ASaP müsste sich jetzt ohne diesen Fehler installieren lassen.

### HINWEIS

Wenn Sie bereits versucht haben, VirusScan ASaP von Hand zu deinstallieren, müssen Sie VirusScan ASaP mit der Option **Microsoft Plus!-Setup** neu installieren und diesen Fehler noch einmal erzeugen. Danach führen Sie die oben angegebenen Schritte zur Behebung des Problems aus.

## Kontaktaufnahme mit dem technischen Support

Sie können sich auf drei Arten an den technischen Support wenden:

### Per E-Mail

Die E-Mail-Adresse für die Kontaktaufnahme mit dem technischen Support finden Sie in Ihrer Begrüßungs-E-Mail.

### Per Telefon

Um eine Liste mit aktuellen Telefonnummern zu erhalten, gehen Sie auf:

<http://www.mcafee2b.com/naicommon/aboutnai/contact/intro.asp#software-support>

### Über das Web

- 1 Melden Sie sich bei der **Customer Home**-Website mit Ihrem Benutzernamen und Ihrem Kennwort an.
- 2 Klicken Sie auf die Verknüpfung **E-Care** am oberen Rand der Seite.

#### **HINWEIS**

Bei anderen Dienst Anbietern kann die Verknüpfung auch die Bezeichnung **Support** statt **E-Care** haben.

- 3 Geben Sie in das angezeigte Feld eine Beschreibung Ihres Problems ein, und klicken Sie auf **Anfrage starten**.

# Index

## A

- Abrufen von Updates, [15](#)
- ActiveX, Überblick, [21](#)
- Aktualisieren Ihres Benutzerprofils, [36](#)
- Aktualisieren von VirusScan ASaP, [14, 40](#)
  - abrufen, [15](#)
  - auf Anforderung, [41](#)
  - automatisch, [13, 40](#)
  - Fragen, [59](#)
- Allgemeine Fragen, Fehlerbehebung, [59](#)
- Anforderungen
  - Hintergrundinstallation, [26](#)
  - Installation, [20](#)
  - Internet-URL-Installation, [24](#)
  - Push-Installation, [29](#)
- Anmelden bei VirusScan ASaP, [35](#)
- Anzeigen von Gruppen, [42](#)
- Ausschließen von Dateien oder Verzeichnissen, [57](#)
- Automatische Updates, [14](#)
- Automatisches Scannen, [37](#)
- AVERT Anti-Virus Emergency Research Team, Kontakt, [10](#)

## B

- Bearbeiten von Gruppen, [43](#)
- Benutzerprofil aktualisieren, [36](#)
- Berichte, [41](#)
  - hochladen, [15](#)
  - nach "Jetzt scannen", [39](#)
  - zugreifen, [37](#)
- Betaprogramm, Kontakt, [10](#)
- Bibliothek mit Virusinformationen, [10](#)
- Browser
  - für die Installation konfigurieren, [21](#)
  - Internet Explorer 5.x, [22](#)
  - Internet Explorer 6.x, [22](#)
  - Netscape Communicator, [23](#)

## C

- Cleanup Utility herunterladen, [60](#)
- Customer Home-Website, [35](#)

## D

- DAT-Dateiaktualisierungen, Website, [10](#)
- DAT-Dateien, [13 bis 14](#)
- Deinstallieren anderer Virenschutzprogramme, [57](#)
- Die Funktion "Jetzt aktualisieren", [41](#)
- Dienste, neue hinzufügen, [36](#)
- Dokumentation zum Produkt, [9](#)
- Download-Website, [10](#)

## E

- E-Care-Verknüpfung, technischer Support, [68](#)
- EICAR-Testvirus, [33](#)
- Einreichen eines Beispielvirus, [10](#)
- Excluded Items Viewer, die Utility verwenden, [57](#)

## F

- Fehlerbehebung, [55](#)
  - Aktualisieren, [59](#)
  - allgemein, [59](#)
  - Berichterstellung, [58](#)
  - Installation, [55](#)
  - Push-Installation, [62](#)
  - REGEDIT.EXE, fehlende Systemdatei, [64](#)
  - Scannen, [57](#)
  - Testvirus, [60](#)
  - vorhandene Antivirusanwendungen deinstallieren, [57](#)
- Fehlermeldungen, [61](#)
  - Cab Installer-Objekt kann nicht erstellt werden, [65](#)
  - Es konnte keine Verbindung zum Aktualisierungsserver hergestellt werden, [66](#)

---

Freigegebenes Remote-Verzeichnis nicht gefunden, [62](#)

Ihre aktuellen Sicherheitseinstellungen verhindern die Ausführung von ActiveX-Steurelementen auf dieser Seite, [64](#)

Installation fehlgeschlagen. Sie haben eine wichtige Komponente nicht akzeptiert bzw. verfügen nicht über Administratorrechte, [63](#)

Invalid Entitlement, [56](#), [64](#)

MyASUtil.SecureObjectFactory, [64](#)

MyINX, [57](#)

URL-Download in Datei fehlgeschlagen, [67](#)

Firewall oder Proxy-Server, Installationsfragen, [31](#)

Firewall-Server, Installation mit, [31](#)

Fragen zum Berichtswesen, [58](#)

## G

Gruppe

- Arbeitsstationen löschen, [48](#)
- Arbeitsstationen verschieben, [48](#)
- eine neue Gruppe hinzufügen, [46](#)

## H

Handbücher, [9](#)

Häufig gestellte Fragen (FAQ), [55](#)

Hintergrundinstallation, [26](#)

- Unternehmensschlüssel, [27](#)
- Verfahren, [27](#)

Hinzufügen neuer Dienste, [36](#)

Hinzufügen von Gruppen, [43](#)

Hochladen von Berichten, [15](#)

## I

Installation von VirusScan ASaP

- Firewall oder Proxy-Server, [31](#)
- Fragen, [55](#)
- Ihre Installation testen, [33](#)
- Push-Installation, [29](#)

  - Verfahren, [30](#)

- Relay-Server aktivieren, [31](#)

Installationsagent bereitstellen, [55](#)

Installieren von VirusScan ASaP, [19](#)

Hintergrundinstallation, [26](#)

- Verfahren, [27](#)

Internet-URL, [24](#)

- Verfahren, [24](#)

Systemanforderungen, [20](#)

Internet Explorer

- Cache leeren, [66](#)
- Installationsanforderungen

  - Version 5.x, [22](#)
  - Version 6.x, [22](#)

- Sicherheitseinstellungen anpassen, [66](#)

Internet Independent Updating (IIU), [15](#)

Internet-URL-Installation, [24](#)

Invalid Entitlement-Fehler, [56](#)

Isoliert, Definition, [42](#)

## J

Jetzt scannen, Funktion, [39](#)

## K

KnowledgeBase-Suche, [10](#)

Konfigurieren des Browsers, [21](#)

Kontaktaufnahme mit dem technischen Support, [68](#)

Kontaktaufnahme mit McAfee Security, [10](#)

Konventionen dieses Handbuchs, [8](#)

Kundendienst, Kontakt, [10](#)

## L

Local Area Network (LAN), [16](#)

Löschen von Arbeitsstationen aus einer Gruppe, [48](#)

Löschen von Gruppen, [43](#)

## M

McAfee Security University, Kontakt, [10](#)

MyINX Error, [57](#)

## N

Netscape Communicator

- Installationsanforderungen, [23](#)

Network Operations Center (NOC), [14](#)

## P

PrimeSupport, [10](#)

---

Produktdokumentation, 9  
Produktschulungen, Kontakt, 10  
Proxy-Server, Installation mit, 31  
Push Install-Diensprogramm, 29  
Push-Installation, 29  
    Anforderungen, 29  
    Fehlerbehebung, 62  
    Verfahren, 30

## Q

Quarantine Viewer, 42

## R

RAM-Anforderungen für die Installation, 19  
REGEDIT.EXE, Systemdatei, 64  
Relay-Server aktivieren, 31  
Relay-Servern aktivieren, 31  
Rumor, 16

## S

Scan-Modul aktualisieren, 14  
Scannen  
    auf Anforderung, 39  
    automatisch, 37  
    Fragen, 57  
Scannen bei Zugriff, 38  
Schulungs-Website, 10  
SecureObjectFactory Class-Programmdatei, 64  
Service-Portal, PrimeSupport, 10  
Software, andere Virenschutzprogramme  
    deinstallieren, 57

## T

Technischer Support, 10  
Technischer Support, Kontaktaufnahme zu, 68  
Testen von VirusScan ASaP, 33

## U

Übersicht, 13  
Unternehmensschlüssel, 27  
Updates auf Anforderung, 41  
Upgrade-Website, 10  
URL-Verfahren der Installation

Fehlerbehebung, 55  
Verfahren, 24

## V

Verschieben von Arbeitsstationen in andere  
    Gruppen, 48  
Virendefinitionsdateien (DAT) aktualisieren, 14  
Virenschutzprogramme, Deinstallieren, 57  
Virus, Einreichen eines Beispiels, 10  
VirusScan ASaP  
    Aktualisieren, 14, 40  
    Einführung, 13  
    installieren, 19  
    verwenden, 35  
VirusScan ASaP Cleanup Utility verwenden, 57  
vorhandene Antivirusanwendungen deinstallieren  
    bevor Sie beginnen, 20  
    Fehlerbehebung, 57  
VSSETUP-Dienstprogramm  
    Befehlsparameter, 28  
    für die Hintergrundinstallation, 26  
    Relay-Servern aktivieren, 32

## W

Weitere Informationen, 9

## Z

Zielgruppe dieses Handbuchs, 7

