

SOPHOS



enterprise console

Benutzerhandbuch

Enterprise Console 1.0

Dokumentversion 1.0



Inhalt

Wie fange ich an?.....	1
Wie fange ich an?.....	1
Was ist eine Gruppe?.....	2
Was ist eine Richtlinie?.....	2
Was ist ein "Nicht zugewiesen"-Ordner?.....	2
Was sind Libraries?.....	2
Wie kann ich Computer zu der Liste hinzufügen?.....	3
Computer suchen.....	3
Computer von einer Datei importieren.....	4
Wie kann ich Gruppen erstellen und nutzen?.....	6
Warum gibt es Gruppen?.....	6
Eine Gruppe erstellen.....	6
Computer zu einer Gruppe hinzufügen.....	7
Computer aus einer Gruppe löschen.....	7
Eine Gruppe ausschneiden und einfügen.....	8
Eine Gruppe löschen.....	8
Eine Gruppe umbenennen.....	8
Wie schütze ich neue Computer vor Viren?.....	9
Neue Computer schützen.....	10
Neue Computertypen schützen.....	12
Computer schützen, die sich bereits in einer Gruppe befinden.....	15
Computer schützen, auf denen eine manuelle Installation erforderlich ist..	17
Computer mit einem Skript schützen.....	18
Woher weiß ich, welche Computer geschützt sind?.....	20
Welche Computer sind geschützt?.....	20
Welche Computer sind up to date?.....	20
Wie kann ich Updates einrichten?.....	22
Einrichten automatischer Updates (Überblick).....	22
Auswählen der Quelle für Updates.....	23
Auswählen einer alternativen Quelle für Updates.....	25
Zeitpläne für Updates.....	27
Updates, wenn sich Computer einwählen.....	28
Updates über einen Proxyserver.....	29
Zu verwendende Bandbreite beschränken.....	30
Computer, die sich für Updates automatisch einwählen.....	31
Auswählen einer anderen Quelle für die Erstinstallation.....	32

Inhalt

Wie kann ich Updates einrichten?	
Update-Protokoll.....	33
Wie richte ich Virenbenachrichtigungen ein?.....	35
Einrichten von E-Mail-Benachrichtigungen.....	35
Konfiguration von Desktop-Benachrichtigungen.....	38
Wie kann ich die Antiviren-Einstellungen ändern?.....	40
Ändern der überprüften Dateitypen.....	40
Dateien von der Überprüfung ausschließen.....	41
Ändern der Bedingungen für die On-Access-Überprüfung.....	43
Archivdateien überprüfen.....	44
Dateien automatisch desinfizieren.....	45
Computer zu festgesetzten Zeiten überprüfen.....	46
Wie stelle ich ein, dass mehrere Computer dieselben Einstellungen verwenden?.....	48
Prüfen, ob mehrere Computer die Gruppeneinstellungen verwenden.....	48
Einstellen, dass mehrere Computer die Gruppeneinstellungen verwenden.....	48
Wie kann ich Computer zu festgesetzten Zeiten überprüfen?.....	49
Zeitgesteuerte Überprüfungen einrichten.....	49
Die Einstellungen für die zeitgesteuerten Überprüfungen ändern.....	50
Wie kann ich Computer mit Problemen finden und die Probleme beheben?.....	52
Computer suchen, auf denen die On-Access-Überprüfung nicht aktiv ist.....	52
Computer mit Alarmen suchen, die eine nähere Untersuchung erfordern.....	53
Veraltete Computer suchen.....	53
Computer suchen, die nicht von der Konsole verwaltet werden.....	54
Computer suchen, die nicht mit dem Netzwerk verbunden sind.....	55
Wie gehe ich mit Alarmen um?.....	56
Umgang mit Alarmen.....	56
Alarme aus der Konsole löschen.....	56
Wie kann ich Computer desinfizieren?.....	57
Computer desinfizieren (Überblick).....	57
Einen Computer mit einer sofortigen Überprüfung desinfizieren.....	57
Computer manuell desinfizieren.....	59
Computer mit einer zeitgesteuerten Überprüfung desinfizieren.....	59
Den Computer nach Nebeneffekten wiederherstellen.....	61

Inhalt

Wie kann ich Computer desinfizieren?	
Einrichten der automatischen Desinfektion.....	61
Wie kann ich Reports erzeugen?.....	63
Einen Report erzeugen.....	63
Einen Report in Form einer Tabelle anzeigen.....	64
Einen Report in Form eines Diagramms anzeigen.....	65
Die Anzahl der Alarme pro Virus anzeigen.....	66
Anzahl der Alarme pro Ort anzeigen.....	68
Die Häufigkeit von Virenalarmen anzeigen.....	69
Details von Virenalarmen anzeigen.....	71
Einen Report ausdrucken.....	73
Einen Report in eine Datei exportieren.....	73
Das Report–Layout ändern.....	74
Fehlersuche.....	75
Einstellungen für den Ordner "Nicht zugewiesen" können nicht geändert werden.....	75
Computer im Ordner "Nicht zugewiesen" können nicht geschützt werden.....	75
Computer werden nicht aktualisiert.....	75
Antiviren–Einstellungen werden von Macs nicht übernommen.....	76
Einstellungen der On–Access–Überprüfung werden nicht übernommen...	76
Neue Überprüfung erscheint unerwartet auf Windows 2000/XP.....	76
Mehr Hilfe.....	77

Wie fange ich an?

Dieser Abschnitt gibt einen schnellen Überblick darüber, wie Sie Ihr Netzwerk mit der Enterprise Console schützen. Er erklärt außerdem die wesentlichen Funktionen des Produkts.

- Wie fange ich an?
- Was ist eine Gruppe?
- Was ist eine Richtlinie?
- Was ist ein "Nicht zugewiesen"-Ordner?
- Was sind Libraries?

Wie fange ich an?

So schützen Sie Ihr Netzwerk mit Enterprise Console: Dies ist lediglich ein Überblick, so dass Sie für nähere Informationen bitte die anderen erwähnten Abschnitte lesen.

1. Klicken Sie auf das **Suchen**-Symbol in der Werkzeugleiste und markieren Sie die Domänen oder Arbeitsgruppen, in denen Sie nach Computern suchen möchten. Die Konsole fügt die Computer zum Ordner **Nicht zugewiesen** hinzu.
2. Klicken Sie auf das Symbol **Gruppe erstellen**. Wenn die neue Gruppe angezeigt wird, benennen Sie sie um.
3. Markieren Sie die Gruppe und klicken Sie auf das Symbol **Update-Richtlinie**. Geben Sie für jeden Computertyp in der Gruppe die Update-Quelle an. Lesen Sie dazu [Wie kann ich Updates einrichten?](#)
4. Wenn Sie Überprüfungen und Virenalarme verändern möchten, klicken Sie auf das Symbol **SAV-Richtlinie**. Lesen Sie dazu [Wie kann ich die Antiviren-Einstellungen ändern?](#)

und [Wie richte ich Virenbenachrichtigungen ein?](#)
5. Klicken Sie auf den Ordner **Nicht zugewiesen**. Markieren Sie die Computer, die Sie in der Gruppe ablegen möchten. Ziehen Sie die Computer mittels "Drag-and-Drop" in die neue Gruppe.
6. Es startet ein Wizard, der Ihnen bei der Installation der Antiviren-Software auf den Computern hilft. Lesen Sie dazu [Wie schütze ich neue Computer vor Viren?](#)

7. Wenn die Installation abgeschlossen ist, sehen Sie sich noch einmal die Computerliste in der neuen Gruppe an. In der Spalte **On-Access** sollten Sie jetzt das Wort "Aktiv" sehen: Dies zeigt an, dass der Computer durch die On-Access-Überprüfung geschützt und von der Enterprise Console verwaltet wird.

Was ist eine Gruppe?

Eine Gruppe ist ein Ordner, der von Ihnen erstellt wird und in dem mehrere Computer enthalten sind.

Jede Gruppe hat ihre eigenen Einstellungen für den Virenschutz und für Updates. Alle Computer in einer Gruppe sollten diese Einstellungen verwenden.

Eine Gruppe kann auch Untergruppen enthalten.

Was ist eine Richtlinie?

Eine Richtlinie ist eine Zusammenstellung von Einstellungen, die für alle Computer in einer Gruppe gelten.

- Die "SAV-Richtlinie" spezifiziert, wie Sophos Anti-Virus Computer auf Viren überprüft und sie desinfiziert.
- Die "Update-Richtlinie" spezifiziert, wie Computer mit neuer Antiviren-Software aktualisiert werden.

Was ist ein "Nicht zugewiesen"-Ordner?

Der Ordner "Nicht zugewiesen" ist ein Ordner, in dem Enterprise Console Computer ablegt, bevor Sie sie in Gruppen einordnen.

Sie können nicht:

- eine Antiviren- oder Update-Richtlinie für den Ordner "Nicht zugewiesen" einrichten
- den Ordner "Nicht zugewiesen" verschieben oder löschen.

Was sind Libraries?

Libraries laden die neueste Software von Sophos herunter und stellen sie auf Ihrem Server zur Verfügung, von wo aus sie auf vernetzten Computern installiert werden kann.

Eine Komponente namens EM Library hält die Libraries up to date. Um EM Library zu verwenden, klicken Sie auf das **Libraries**-Symbol in der Werkzeugleiste.

Wie kann ich Computer zu der Liste hinzufügen?

Dieser Abschnitt erläutert, wie Sie neue Computer im Netzwerk finden und sie in der Enterprise Console auflisten.

- Computer suchen
- Computer von einer Datei importieren

Computer suchen

Mit der Funktion "Computer suchen" können Sie eine Liste mit Ihren Computern im Ordner **Nicht zugewiesen** ablegen.

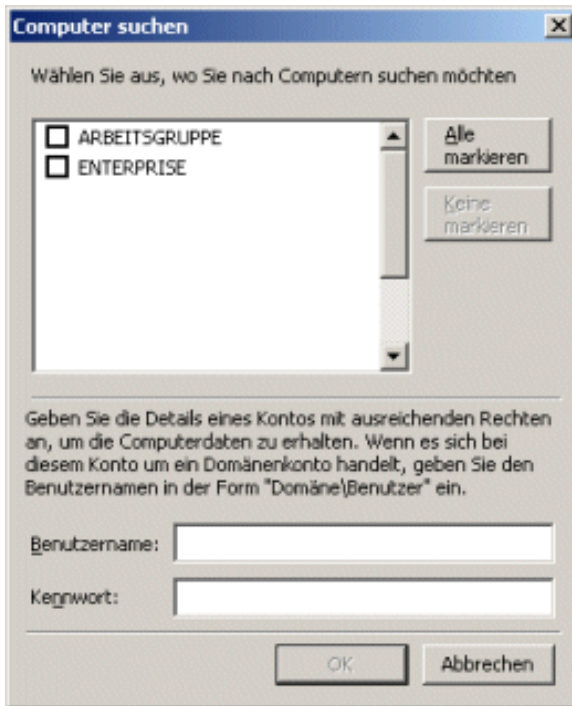


Sie können Computer auch aus einer Datei importieren.



Die Funktion "Computer suchen" sucht nur nach Computern in Windows-Domänen und -Arbeitsgruppen.

1. Klicken Sie auf das Symbol **Suchen** in der Werkzeugleiste.
2. Markieren Sie im Dialogfenster **Computer suchen** die Domänen oder Arbeitsgruppen, die Sie durchsuchen möchten. Sie müssen nur dann einen **Benutzernamen** und ein **Kennwort** eingeben, wenn Sie über Computer verfügen, auf die nur mit Kontodaten zugegriffen werden kann (z. B. Windows XP Service Pack 2). Das Konto benötigt keine Administratorrechte. Klicken Sie auf **OK**.



3. Klicken Sie auf den Ordner **Nicht zugewiesen**, um die aufgefundenen Computer zu sehen.
4. Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

Computer von einer Datei importieren

Damit Enterprise Console Ihre Computer auflistet, können Sie die Computernamen aus einer Datei importieren.

Auf die Datei mit den Computernamen muss eines der Folgenden zutreffen:

- eine Datei, die die nachfolgend aufgeführten Konventionen verwendet
- eine aus SAVAdmin exportierte SGR-Datei.

Sie können eine Datei erstellen, die Einträge wie folgt verwendet:

[GroupName1]

Domain1|Windows2000|ComputerName1

Domain1|Windows2000Server|ComputerName2



Sie haben nicht angegeben, in welche Gruppe die Computer gelegt werden sollen. Wenn Sie als Gruppenname [] eingeben, werden die Computer in die Gruppe 'Nicht zugewiesen' gelegt.



Gültige Betriebssystemnamen sind: Windows95, Windows98, WindowsMe, WindowsNT, WindowsNTServer, Windows2000, Windows2000Server,

WindowsXP, Windows2003, MACOS9, MACOSX, Windows9x.

Der Domänenname und das Betriebssystem sind optional. Ein solcher Eintrag kann so aussehen:

**[GroupName1]
||ComputerName1**

Folgendermaßen importieren Sie Computernamen.

1. Klicken Sie im **Datei**-Menü auf **Computernamen aus Datei importieren**.
2. Markieren Sie im Browser-Fenster die Datei.
3. Klicken Sie auf den Ordner **Nicht zugewiesen**, um die aufgefundenen Computer zu sehen.
4. Um die Computer zu verwalten, ziehen Sie sie in eine Gruppe.

Wie kann ich Gruppen erstellen und nutzen?

Dieser Abschnitt erläutert, wie Computer-Gruppen erstellt und verwaltet werden.

- Warum gibt es Gruppen?
- Eine Gruppe erstellen
- Computer zu einer Gruppe hinzufügen
- Computer aus einer Gruppe löschen
- Eine Gruppe ausschneiden und einfügen
- Eine Gruppe löschen
- Eine Gruppe umbenennen

Warum gibt es Gruppen?

Sie müssen Gruppen erstellen und Computer in ihnen ablegen, bevor Sie den Virenschutz installieren und verwalten können.

Gruppen sind nützlich, da Sie Folgendes tun können:

- Gruppen von verschiedenen Quellen oder über verschiedene Zeitpläne aktualisieren
- verschiedene Antiviren-Einstellungen für verschiedene Gruppen verwenden
- Computer einfacher verwalten



Sie können auch Gruppen innerhalb von Gruppen erstellen.

Eine Gruppe erstellen

Um eine neue Gruppe zu erstellen, tun Sie Folgendes:

1. Markieren Sie im linken Fensterbereich der Konsole, an welcher Stelle Sie die Gruppe erstellen möchten. Klicken Sie auf den Computernamen oben, wenn Sie eine neue Top-Level-Gruppe erstellen möchten. Klicken Sie auf eine bestehende Gruppe, wenn Sie eine Untergruppe erstellen möchten.
2. Klicken Sie auf das Symbol **Gruppe erstellen** in der Werkzeugleiste.
3. Es wird eine "Neue Gruppe" zur Liste hinzugefügt und der Name wird markiert. Geben Sie einen neuen Namen für die Gruppe ein.

Sie können jetzt Antiviren-Einstellungen und Update-Einstellungen für die Gruppe spezifizieren und Computer zu der Gruppe hinzufügen.



Wenn es sich bei der neuen Gruppe um eine Untergruppe handelt, verwendet die Untergruppe anfangs dieselben Einstellungen wie die Gruppe, in der sie sich befindet.

Computer zu einer Gruppe hinzufügen

Um Computer zu einer Gruppe hinzuzufügen, tun Sie Folgendes:

1. Markieren Sie den Computer, den Sie zu einer Gruppe hinzufügen möchten. Klicken Sie z. B. auf den Ordner **Nicht zugewiesen** und markieren Sie dort Computer.
2. Ziehen Sie die Computer mittels "Drag-and-Drop" in die neue Gruppe.



Wenn Sie ungeschützte Computer aus dem Ordner **Nicht zugewiesen** in eine Gruppe verschieben, für die automatische Updates eingerichtet sind, wird ein Wizard gestartet, der Ihnen dabei hilft, diese Computer zu schützen. Wenn Sie Computer von einer Gruppe in eine andere verschieben,



verwenden diese Computer möglicherweise nicht dieselben Antiviren- und Update-Einstellungen wie die Computer der Gruppe, in die sie verschoben werden. Lesen Sie dazu Einstellen, dass mehrere Computer die Gruppeneinstellungen verwenden.

Computer aus einer Gruppe löschen

Sie können Computer aus einer Gruppe löschen, z. B. wenn Sie Einträge für Computer entfernen möchten, die sich nicht mehr im Netzwerk befinden.



Wenn Sie Computer löschen, die sich noch im Netzwerk befinden, werden sie nicht mehr in der Konsole aufgelistet oder von ihr verwaltet. So löschen Sie Computer:

1. Markieren Sie die Computer, die Sie löschen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **Löschen**.



Wenn Sie die Computer erneut sehen möchten, klicken Sie auf das **Suchen**-Symbol in der Werkzeugleiste. Diese Computer werden solange nicht als verwaltet angezeigt, bis sie neu gestartet werden.

Eine Gruppe ausschneiden und einfügen

Um eine Gruppe auszuschneiden und einzufügen, tun Sie Folgendes:

1. Markieren Sie die Gruppe, die Sie ausschneiden und einfügen möchten. Klicken Sie im Menü **Bearbeiten** auf **Ausschneiden**.
2. Markieren Sie die Gruppe, in die Sie die Gruppe einfügen möchten. Klicken Sie im Menü **Bearbeiten** auf **Einfügen**.

Eine Gruppe löschen

Um eine Gruppe zu löschen, tun Sie Folgendes:



Wenn die Gruppe Computer enthält, werden diese Computer dann nirgends mehr in der Konsole aufgelistet. Um sie wieder zu finden, klicken Sie auf das **Suchen**-Symbol in der Werkzeugleiste.

1. Markieren Sie die Gruppe, die Sie löschen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **Löschen**.

Eine Gruppe umbenennen

Um eine Gruppe umzubenennen, tun Sie Folgendes:

1. Markieren Sie die Gruppe, die Sie umbenennen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **Umbenennen**.

Wie schütze ich neue Computer vor Viren?

Dieser Abschnitt erläutert, wie die Antiviren-Software auf vernetzten Computern installiert wird.

- Neue Computer schützen
- Neue Computertypen schützen
- Computer schützen, die sich bereits in einer Gruppe befinden
- Computer schützen, auf denen eine manuelle Installation erforderlich ist
- Computer mittels eines Loginskripts oder einer CD schützen

Neue Computer schützen

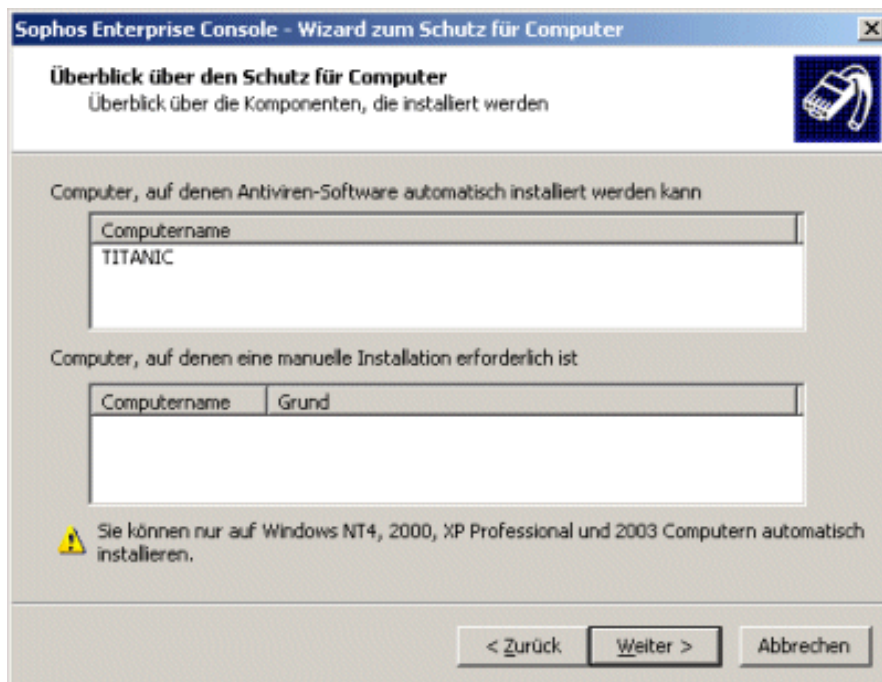
Neue Windows-Computer können automatisch von der Konsole aus geschützt werden.

Diese Anleitung geht davon aus, dass Sie bereits Gruppen erstellt und Update-Einstellungen für diese Gruppen eingerichtet haben.



Auf Windows 95/98/Me-Computern ist die automatische Installation nicht möglich. Verwenden Sie stattdessen die manuelle Installation.

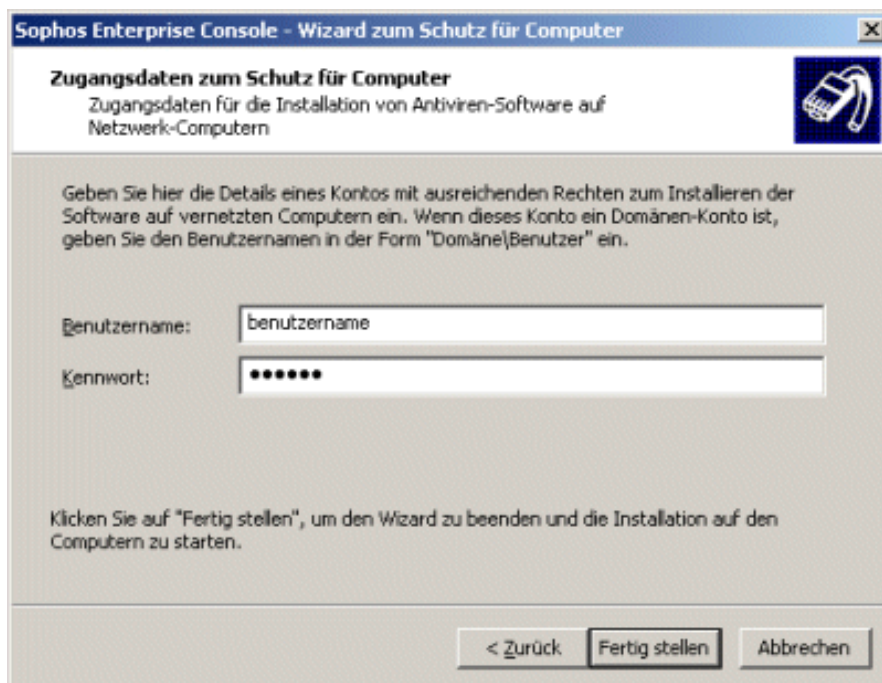
1. Klicken Sie auf das **Suchen**-Symbol in der Werkzeugleiste (sofern Sie dies nicht bereits getan haben). Enterprise Console sucht neue Computer und legt sie im Ordner **Nicht zugewiesen** ab.
2. "Ziehen" Sie die Computer in eine Gruppe. Es startet ein Wizard.
3. Klicken Sie im **Willkommen** Fenster auf **Weiter**.
4. Prüfen Sie im Dialogfenster **Überblick über den Schutz für Computer**, ob sich die Computer in der Liste der "Computer, auf denen Antiviren-Software automatisch installiert werden kann" befinden. Auf Computern, die sich nicht in dieser Liste befinden, ist eine manuelle Installation erforderlich. Klicken Sie auf **Weiter**.



5. Geben Sie im Dialogfenster **Zugangsdaten zum Schutz für Computer** die Zugangsdaten für ein Konto ein, mit dem Software installiert werden kann.

Dieses Konto ist typischerweise ein Domänen-Administratorkonto. Es muss:

- ◆ lokale Administratorrechte auf den Computern haben, die Sie schützen möchten
- ◆ sich an dem Computer anmelden können, auf dem Sie den Management-Server installiert haben
- ◆ Lesezugriff auf den Speicherort des Primary Servers haben, den Sie beim Einrichten der Updates spezifiziert haben.



Sophos Enterprise Console - Wizard zum Schutz für Computer

Zugangsdaten zum Schutz für Computer
Zugangsdaten für die Installation von Antiviren-Software auf Netzwerk-Computern

Geben Sie hier die Details eines Kontos mit ausreichenden Rechten zum Installieren der Software auf vernetzten Computern ein. Wenn dieses Konto ein Domänen-Konto ist, geben Sie den Benutzernamen in der Form "Domäne\Benutzer" ein.

Benutzername:


Kennwort:

Klicken Sie auf "Fertig stellen", um den Wizard zu beenden und die Installation auf den Computern zu starten.


< Zurück Fertig stellen Abbrechen

Neue Computertypen schützen

Wenn Sie Computer zum Netzwerk hinzufügen, die ein Betriebssystem einsetzen, für das Sie zuvor keinen Virenschutz installiert haben, folgen Sie der Anleitung unten.

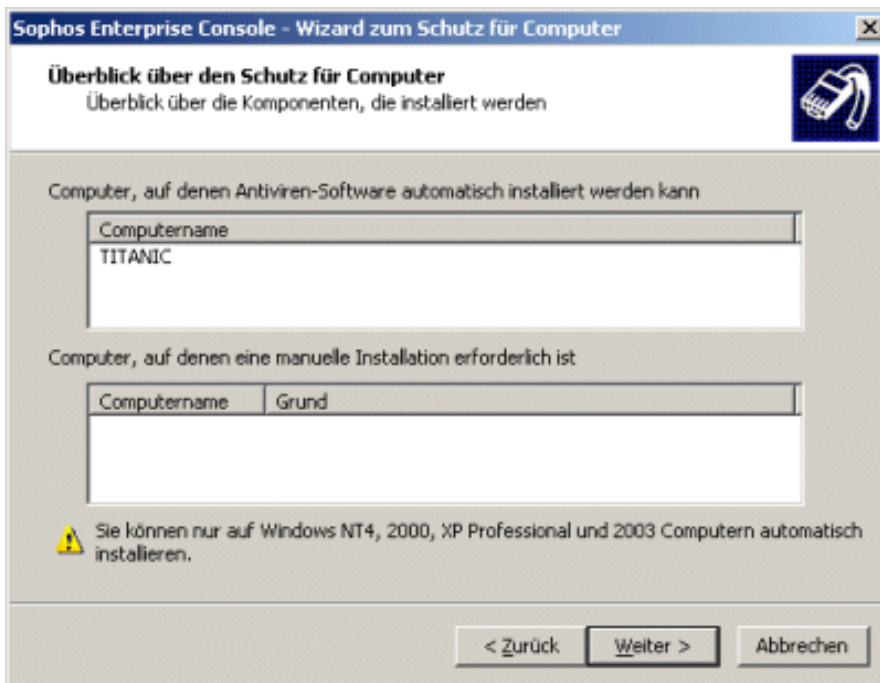
 Sophos behandelt Windows 2000, 2003 und XP als einen Computertyp und Windows 95, 98 und Me ebenfalls als einen Computertyp. Wenn Sie in Ihrem Netzwerk bereits Windows 2000 geschützt haben und dann Windows 2003 Computer hinzufügen, können Sie den normalen Schritten im Abschnitt Neue Computer schützen folgen.

1. Klicken Sie auf das Symbol **Libraries** in der Werkzeugleiste. Es öffnet sich das EM Library Fenster.
2. Klicken Sie auf **Select Packages**. Klicken Sie mit der rechten Maustaste auf das Paket für das neue Betriebssystem, wählen Sie **Subscribe** und folgen Sie den Aufforderungen.

 Um das neue Paket schneller zu erhalten, gehen Sie in das **Library**-Menü und wählen dort **Select Packages**. Dadurch wird das Paket in dem Standard-Speicherort abgelegt.

3. Klicken Sie auf **Download Packages**.
4. Klicken Sie im Meldungsfenster **EM Library** auf **Yes**.
5. Schließen Sie das **EM Library** Fenster, um zur Enterprise Console zurückzukehren.
6. Markieren Sie in der Enterprise Console die Gruppe, in der Sie die neuen Computer ablegen möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.
7. Markieren Sie in der Liste das neue Betriebssystem. Klicken Sie auf **Konfigurieren**.
8. Geben Sie in der Registerkarte **Primary Server** die Daten des Ordners ein, von dem aus die Computer aktualisiert werden. Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie auf **OK**. Klicken Sie nochmals auf **OK**.
9. "Ziehen" Sie die neuen Computer in die neue Gruppe. Es startet ein Wizard, der Ihnen hilft, die Computer zu schützen.
10. Klicken Sie im **Willkommen** Fenster auf **Weiter**.

11. Prüfen Sie im Dialogfenster **Überblick über den Schutz für Computer**, ob sich die Computer in der Liste der "Computer, auf denen Antiviren-Software automatisch installiert werden kann" befinden. Auf Computern, die sich nicht in dieser Liste befinden, ist eine manuelle Installation erforderlich. Klicken Sie auf **Weiter**.



12. Geben Sie im Dialogfenster **Zugangsdaten zum Schutz für Computer** die Zugangsdaten für ein Konto ein, mit dem Software installiert werden kann. Dieses Konto ist typischerweise ein Domänen-Administratorkonto. Es muss:

- ◆ lokale Administratorrechte auf den Computern haben, die Sie schützen möchten
- ◆ sich an dem Computer anmelden können, auf dem Sie den Management-Server installiert haben
- ◆ Lesezugriff auf den Speicherort des Primary Servers haben, den Sie beim Einrichten der Updates spezifiziert haben.

Sophos Enterprise Console - Wizard zum Schutz für Computer

Zugangsdaten zum Schutz für Computer
Zugangsdaten für die Installation von Antiviren-Software auf Netzwerk-Computern

Geben Sie hier die Details eines Kontos mit ausreichenden Rechten zum Installieren der Software auf vernetzten Computern ein. Wenn dieses Konto ein Domänen-Konto ist, geben Sie den Benutzernamen in der Form "Domäne\Benutzer" ein.

Benutzername:

Kennwort:

Klicken Sie auf "Fertig stellen", um den Wizard zu beenden und die Installation auf den Computern zu starten.

< Zurück Fertig stellen Abbrechen

13. Wiederholen Sie die Schritte 6 bis 12 für jede weitere Gruppe, in der Sie neue Computer ablegen möchten.

Computer schützen, die sich bereits in einer Gruppe befinden

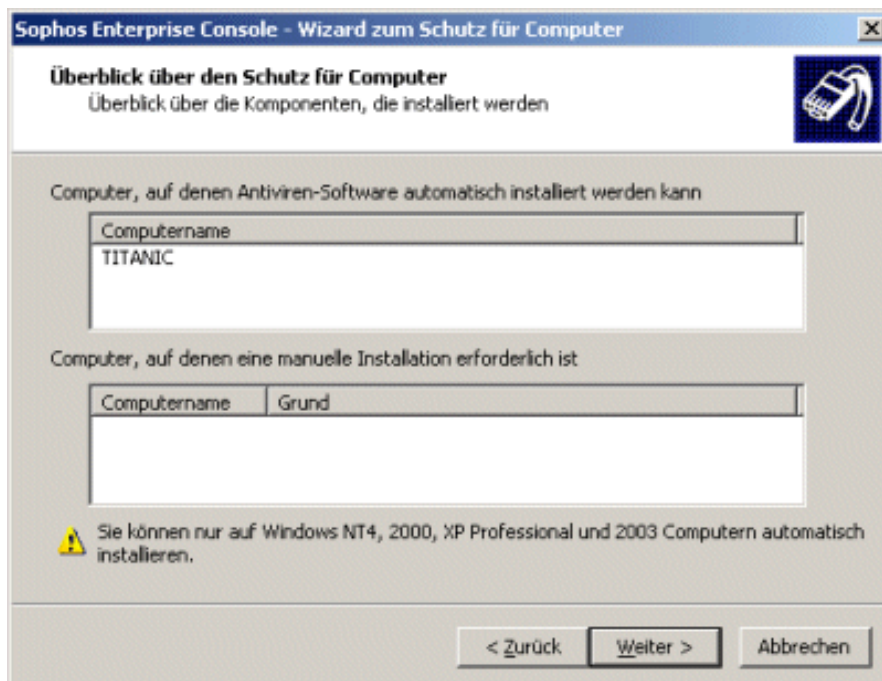
Wenn Sie Computer in einer benutzerdefinierten Gruppe abgelegt, auf ihnen aber noch keinen Schutz installiert haben, schützen Sie die Computer automatisch wie folgt:

Diese Anleitung geht davon aus, dass Sie für die Gruppe bereits Update-Einstellungen festgelegt haben.



Auf Windows 95/98/Me-Computern ist die automatische Installation nicht möglich. Verwenden Sie stattdessen die manuelle Installation.

1. Markieren Sie die Computer. Klicken Sie auf das Symbol **Schützen** in der Werkzeugleiste.
2. Es startet ein Wizard. Klicken Sie im **Willkommen** Fenster auf **Weiter**.
3. Prüfen Sie im Dialogfenster **Überblick über den Schutz für Computer**, ob sich die Computer in der Liste der "Computer, auf denen Antiviren-Software automatisch installiert werden kann" befinden. Bei allen Computern, die in dieser Liste nicht aufgeführt sind, ist eine manuelle Installation erforderlich. Klicken Sie auf **Weiter**.



4. Geben Sie im Dialogfenster **Zugangsdaten zum Schutz für Computer** die Zugangsdaten für ein Konto ein, mit dem Software installiert werden kann.

Dieses Konto ist typischerweise ein Domänen-Administratorkonto. Es muss:

- ◆ lokale Administratorrechte auf den Computern haben, die Sie schützen möchten
- ◆ sich an dem Computer anmelden können, auf dem Sie den Management-Server installiert haben
- ◆ Lesezugriff auf den Speicherort des Primary Servers haben, den Sie beim Einrichten der Updates spezifiziert haben.

Sophos Enterprise Console - Wizard zum Schutz für Computer

Zugangsdaten zum Schutz für Computer
Zugangsdaten für die Installation von Antiviren-Software auf Netzwerk-Computern

Geben Sie hier die Details eines Kontos mit ausreichenden Rechten zum Installieren der Software auf vernetzten Computern ein. Wenn dieses Konto ein Domänen-Konto ist, geben Sie den Benutzernamen in der Form "Domäne\Benutzer" ein.

Benutzername:

Kennwort:

Klicken Sie auf "Fertig stellen", um den Wizard zu beenden und die Installation auf den Computern zu starten.

< Zurück **Fertig stellen** Abbrechen

Computer schützen, auf denen eine manuelle Installation erforderlich ist

Wenn Enterprise Console auf bestimmten Computern die Antiviren-Software nicht automatisch installieren kann, können Sie die Installation manuell durchführen.

Danach jedoch verwaltet und aktualisiert Enterprise Console diese Installationen, vorausgesetzt, Sie haben die Computer in einer Gruppe oder mehreren Gruppen abgelegt.



Sie können die Installation auch automatisch über ein Skript durchführen. Lesen Sie dazu Computer mittels eines Loginskripts oder einer CD schützen.



Wenn Sie eine frühere Version von Sophos Anti-Virus auf Windows 95, 98 oder Me installiert haben, müssen Sie diese deinstallieren, bevor Sie die neueste Version installieren.

1. Prüfen Sie, von wo aus die Antiviren-Software installiert werden soll. Markieren Sie dazu die Gruppe und klicken Sie auf das Symbol **Update-Richtlinie**. Markieren Sie das Betriebssystem des Computers und klicken Sie auf **Konfigurieren**. Notieren Sie sich dann die angezeigte Adresse.
2. Gehen Sie zu dem Computer und gehen Sie auf diese Adresse.

Auf einem Windows-Computer doppelklicken Sie auf setup.exe.

Auf einem Mac OS X-Computer doppelklicken Sie auf Sophos Anti-Virus.mkpg

Computer mit einem Skript schützen

Sie können Computer auch schützen, indem Sie das Installationsprogramm mit einem Skript oder einem Programm wie Microsoft SMS starten.

Das Installationsprogramm befindet sich im zentralen Installationsverzeichnis (CID), dem Verzeichnis, in das EM Library die Sophos-Updates ablegt. Das Standard-CID für jedes Betriebssystem ist:

Windows 2000/XP/2003	\\Servername\InterChk\ESXP
Windows NT	\\Servername\InterChk\ESNT
Windows 95/98/Me	\\Servername\InterChk\ES9X
Mac OS X	\\Servername\InterChk\ESOSX
Mac OS 8/9	\\Servername\InterChk\macinst

Bei Windows 95/98/Me Computern können Sie ein Loginskript verwenden (siehe unten).

Verwenden Sie bei Mac OS X Computern Apple Remote Desktop. Gehen Sie in das zentrale Installationsverzeichnis und kopieren Sie den Installer auf den Computer, auf dem Apple Remote Desktop läuft, bevor Sie ihn verwenden.



Danach jedoch verwaltet und aktualisiert Enterprise Console diese Installationen, vorausgesetzt, Sie haben die Computer in einer Gruppe oder mehreren Gruppen abgelegt.

Windows 95/98/Me Computer mit einem Login-Skript schützen

1. Suchen Sie das Verzeichnis, in dem sich das Installationsprogramm befindet. Als Standard ist dies \\Servername\InterChk\ES9X



Wenn Sie mit Enterprise Console eine Update-Richtlinie eingerichtet haben, wählen Sie die Gruppe der Computer und klicken Sie auf das Symbol **Update-Richtlinie**. Wählen Sie **Windows 95/98/Me** und klicken Sie auf **Konfigurieren**. Notieren Sie sich die angezeigte Adresse.

2. Fügen Sie folgende Zeile zum Login-Skript hinzu:

```
[Pfad]\setup.exe -user [domain\name] -pwd [password] -login -s
```

wobei [Pfad] der Speicherort des zentralen Installationsverzeichnisses ist.



Wenn Sie über Windows 95-Computer verfügen, müssen Sie vor der Installation auf ihnen ein kleines Dienstprogramm starten. Kopieren Sie von der Sophos Anti-Virus CD die Datei Tools/Utils/w95ws2setup.exe

auf Ihren Server. Fügen Sie dann, wie oben erläutert, eine Zeile in das Loginskript ein, um dieses Dienstprogramm zu starten.

Das angegebene Benutzerkonto muss:

- ◆ sich an den Computern, die Sie schützen möchten, anmelden können
- ◆ Lesezugriff auf den Speicherort des Primary Servers haben, den Sie beim Einrichten der Updates spezifiziert haben.



Wenn Sie die Computer nicht mit Enterprise Console verwalten möchten, sollten Sie den Parameter `-mng no` hinzufügen.

Wenn sich der Computer das nächste Mal anmeldet, wird die Antiviren-Software installiert.

Woher weiß ich, welche Computer geschützt sind?

Dieser Abschnitt erläutert, wie Sie sicherstellen, dass Computer korrekt vor Viren geschützt sind.

- Welche Computer sind geschützt?
- Welche Computer sind up to date?

Welche Computer sind geschützt?

Computer sind komplett geschützt, wenn auf ihnen die On-Access-Überprüfung aktiviert ist **und** dass sie up to date sind.



Möglicherweise haben Sie sich entschieden, bei bestimmten Computertypen, z. B. auf Fileservern, die On-Access-Überprüfung nicht einzusetzen. Stellen Sie in diesem Fall sicher, dass auf diesen Computern zeitgesteuerte Überprüfungen laufen und dass sie up to date sind.

So überprüfen Sie, dass die Computer geschützt sind:

1. Markieren Sie die Computer-Gruppe, die Sie prüfen möchten.
2. Wenn Sie Computer in einer Untergruppe der Gruppe prüfen möchten, wählen Sie in der Drop-Down-Liste **Auf dieser Stufe und darunter**.
3. Suchen Sie in der Computerliste die Spalte **On-Access**. Wenn in dieser Spalte für den Computer "Aktiv" angezeigt wird, ist auf dem Computer die On-Access-Überprüfung aktiviert. Wenn Sie ein graues Schild sehen, ist die On-Access-Überprüfung auf diesem Computer nicht aktiviert.
4. Sehen Sie jetzt in die Spalte **Up to date**. Wenn sie für den Computer "Ja" anzeigt, ist der Computer up to date. Wenn sie ein Uhrensymbol und ein Datum anzeigt, ist der Computer nicht up to date.



Sie können sich eine Liste der ungeschützten Computer anzeigen lassen. Gehen Sie in die Drop-Down-Liste **Ansicht** und wählen Sie **Computer, auf denen die On-Access-Überprüfung nicht aktiv ist** oder **Veraltete Computer**.

Welche Computer sind up to date?

Wenn Sie Enterprise Console wie empfohlen eingerichtet haben, sollten die Computer Antiviren-Updates automatisch erhalten.

1. Markieren Sie die Computer-Gruppe, die Sie prüfen möchten.

2. Wenn Sie Computer in einer Untergruppe der Gruppe prüfen möchten, wählen Sie in der Drop-Down-Liste **Auf dieser Stufe und darunter**.
3. Sehen Sie jetzt in die Spalte **Up to date**.

Wenn sie für den Computer "Ja" anzeigt, ist der Computer up to date.

Wenn sie ein Uhrensymbol und ein Datum anzeigt, ist der Computer veraltet. Der Text zeigt an, wie lange der Computer nicht aktualisiert wurde.



Um Computer sofort zu aktualisieren, markieren Sie die Computer. Klicken Sie auf das Symbol **Computer aktualisieren** in der Werkzeugleiste.

Wie kann ich Updates einrichten?

Dieser Abschnitt erläutert, wie Sie automatische Updates für Computer in jeder Gruppe einrichten und konfigurieren.

- Einrichten automatischer Updates (Überblick)
- Auswählen der Quelle für Updates
- Auswählen einer alternativen Quelle für Updates
- Zeitpläne für Updates
- Updates, wenn sich Computer einwählen
- Updates über einen Proxyserver
- Zu verwendende Bandbreite beschränken
- Computer, die sich für Updates automatisch einwählen
- Auswählen einer anderen Quelle für die Erstinstallation
- Update-Protokoll

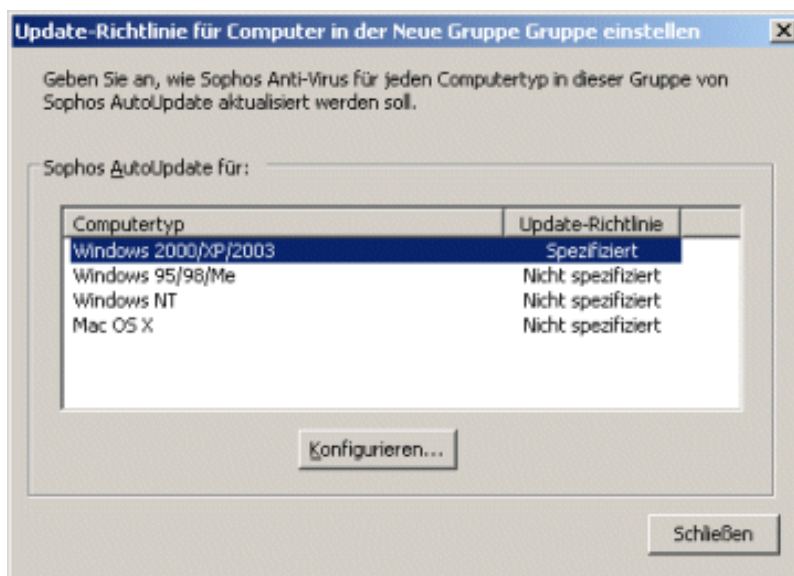
Einrichten automatischer Updates (Überblick)

So richten Sie für jede Computergruppe automatische Updates ein:



Die folgenden Schritte müssen Sie für jeden Computertyp in der Gruppe ausführen (z. B. Windows 2000/XP/2003 oder Mac OS X).

1. Markieren Sie die Gruppe, für die Sie zeitgesteuerte Überprüfungen einrichten möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.
2. Wählen Sie im Dialogfenster **Update-Richtlinie für Computer in der ... Gruppe einstellen** ein Betriebssystem, das von Computern in dieser Gruppe eingesetzt wird. Klicken Sie auf **Konfigurieren**.



3. Klicken Sie auf die Registerkarte **Primary Server** und auf Adresse.

The screenshot shows the 'Update-Richtlinie für Windows XP/2000/2003-Computer in der Neue Gruppe Gruppe einste...' dialog box. The 'Primary Server' tab is selected. The text reads: 'Geben Sie den Speicherort an, von dem Computer dieser Gruppe Updates erhalten.' Below this, there are fields for 'Adresse: (HTTP oder UNC)' with a dropdown menu showing '\\server\InterChk\ESXP' and a 'Durchsuchen...' button. There are also fields for 'Benutzername:' (containing 'Paul'), 'Kennwort:', and 'Kennwort bestätigen:', all with masked input. At the bottom, there are buttons for 'Erweitert...', 'Proxy-Details...', 'OK', and 'Abbrechen'.

4. Klicken Sie auf die Registerkarte **Zeitplan** und auf Zeitplan für Updates.

The screenshot shows the same dialog box, but with the 'Zeitplan' tab selected. A checkbox labeled 'Sophos-Updates für vernetzte Computer automatisch aktivieren:' is checked. Below it, a text box says 'Nach Updates suchen alle 5 Minuten.' with a spinner box set to '5'. A descriptive paragraph follows: 'Mit dieser Option können vernetzte Computer automatisch prüfen, ob Updates von Sophos heruntergeladen wurden, und gegebenenfalls ihre Version von Sophos Anti-Virus aktualisieren.' At the bottom, there is an unchecked checkbox 'Bei Einwahl nach Updates suchen' and 'OK' and 'Abbrechen' buttons.

Auswählen der Quelle für Updates

Wenn sich eine Computergruppe automatisch aktualisieren soll, müssen Sie angeben, von wo aus sich die Computer die Updates herunterladen.



Sie müssen angeben, wo sich jeder Computertyp (z. B. Windows 2000/XP/2003) seine Updates herunterlädt.

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.
2. Wählen Sie im Dialogfenster **Update-Richtlinie für Computer in der ... Gruppe einstellen** ein Betriebssystem, das von Computern in dieser Gruppe eingesetzt wird. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Primary Server** und stellen Sie die Optionen wie nachfolgend erläutert ein.

Update-Richtlinie für Windows XP/2000/2003-Computer in der Neue Gruppe Gruppe einste... X

Primary Server | Secondary Server | Protokoll | Zeitplan | Speicherort der Erstinstallation

Geben Sie den Speicherort an, von dem Computer dieser Gruppe Updates erhalten.

Adresse: (HTTP oder UNC) \\server\InterChk\ESXP Durchsuchen...

Benutzername: Paul

Kennwort:

Kennwort bestätigen:

Erweitert... Proxy-Details...

OK Abbrechen

Adresse

Geben Sie die Adresse (UNC (Netzwerk)–Pfad oder Internetadresse) ein, von der Sophos Anti-Virus Updates herunterlädt.

Benutzername

Wenn erforderlich, geben Sie den **Benutzernamen** für das Konto ein, mit dem auf den Server zugegriffen wird, und geben Sie dann das **Kennwort** ein. Bestätigen Sie das Kennwort. Dieses Konto benötigt Leserechte für das Verzeichnis, das Sie in das Adressfeld eingegeben haben.



Wenn der **Benutzername** die Domäne enthalten muss, verwenden Sie die Form domäne\benutzername.

Erweitert und Proxy-Details

Wenn Sie die verwendete Bandbreite beschränken oder Computer so einrichten möchten, dass sie automatisch eine Einwahlverbindung für Updates aufbauen, klicken Sie auf **Erweitert**.

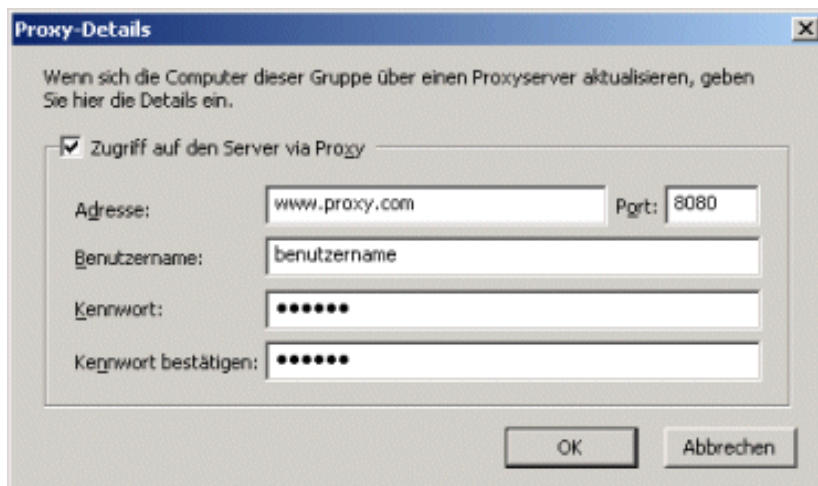
Wenn Sie auf das Internet über einen Proxyserver zugreifen, klicken Sie auf **Proxy Details**. Beachten Sie, dass bei einigen Internet Service Providern Internetanfragen an einen Proxyserver gesendet werden.

Proxy-Details

Wählen Sie im Dialogfenster **Proxy Details** die Option **Auf den Server über Proxy zugreifen**.

Geben Sie dann die **Adresse** und den **Port** des Proxyservers ein. Geben Sie einen **Benutzernamen** und ein **Kennwort** ein, die Zugriff auf den Proxyserver geben.

Wenn der Benutzername die Domäne anzeigen muss, verwenden Sie die Form domäne\benutzername.



Auswählen einer alternativen Quelle für Updates

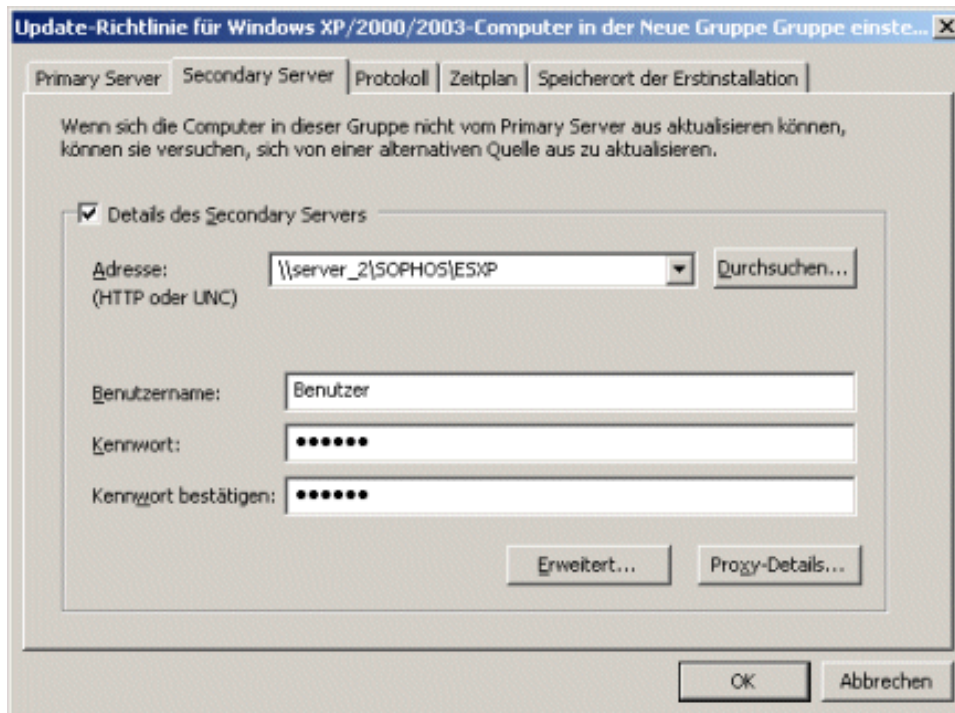
Sie können eine alternative Quelle für Updates angeben. Wenn Computer ihre normale Quelle nicht kontaktieren können, versuchen sie, sich von der alternativen Quelle aus zu aktualisieren.



Sie müssen angeben, wo sich jeder Computertyp (z. B. Windows 2000/XP/2003) seine Updates herunterlädt.

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.

2. Wählen Sie im Dialogfenster **Update-Richtlinie für Computer in der ... Gruppe einstellen** ein Betriebssystem, das von Computern in dieser Gruppe eingesetzt wird. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Secondary Server**. Wählen Sie **Details des Secondary Servers**. Geben Sie dann die Details, wie nachfolgend erläutert, ein.



Adresse

Geben Sie die **Adresse** (UNC (Netzwerk)–Pfad oder Internetadresse) ein, von der Computer Updates heruntergeladen sollen, wenn sie die andere Quelle nicht kontaktieren können. Wenn Sie Sophos wählen, lädt Sophos Anti-Virus Updates direkt von Sophos über das Internet herunter.

Benutzername

Wenn erforderlich, geben Sie den **Benutzernamen** für das Konto ein, mit dem auf den Server zugegriffen wird, und geben Sie dann das **Kennwort** ein. Bestätigen Sie das Kennwort. Dieses Konto benötigt Leserechte für das Verzeichnis, das Sie in das Adressfeld eingegeben haben.



Wenn der **Benutzername** die Domäne enthalten muss, verwenden Sie die Form domäne\benutzername.

Erweitert und Proxy-Details

Wenn Sie die verwendete Bandbreite beschränken oder Computer so einrichten möchten, dass sie automatisch eine Einwahlverbindung für Updates aufbauen, klicken Sie auf **Erweitert**.

Wenn Sie auf die Adresse über einen Proxyserver zugreifen, klicken Sie auf **Proxy Details**. Beachten Sie, dass bei einigen Internet Service Providern Internetanfragen an einen Proxyserver gesendet werden.

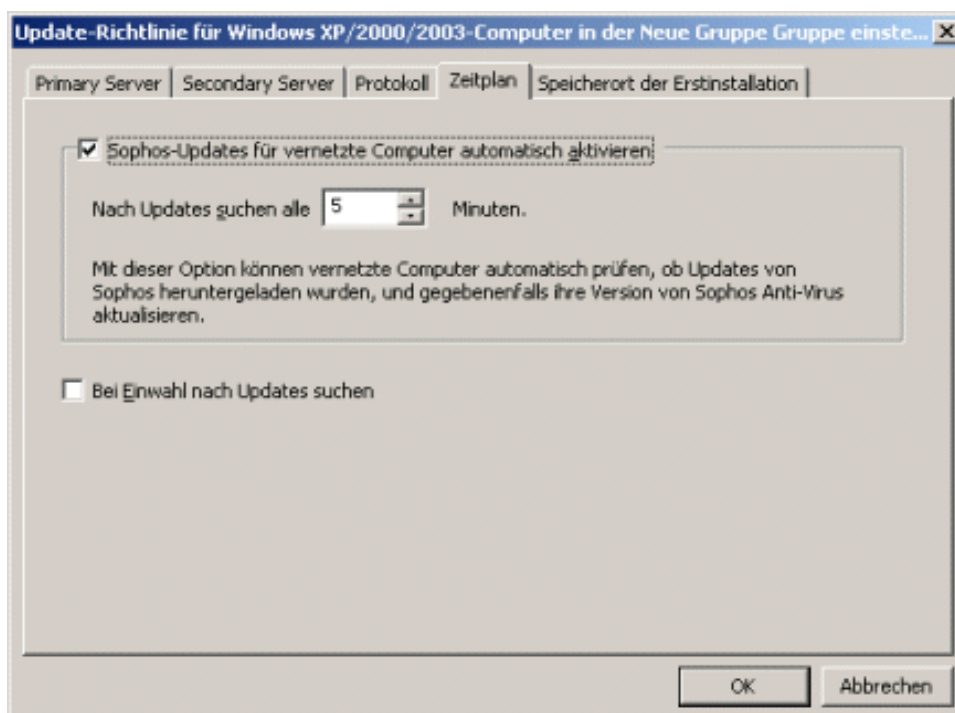
Zeitpläne für Updates

Sie können angeben, wann oder wie häufig die Computer in einer Gruppe aktualisiert werden.



Sie geben diese Einstellungen separat für jeden Computertyp in der Gruppe ein (z. B. Windows 2000/XP/2003 oder Mac OS X).

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.
2. Wählen Sie im Dialogfenster **Update-Richtlinie für Computer in der ... Gruppe einstellen** ein Betriebssystem, das von Computern in dieser Gruppe eingesetzt wird. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Zeitplan**. Geben Sie dann die Details, wie nachfolgend erläutert, ein.



Sophos-Updates für vernetzte Computer automatisch aktivieren

Wählen Sie diese Option, wenn die Computer in regelmäßigen Intervallen aktualisiert werden sollen. Geben Sie dann das Intervall (in Minuten) ein, in dem die Computer nach aktualisierter Software suchen sollen. Die Standardvorgabe ist 5 Minuten.



Wenn die Computer Updates direkt von Sophos herunterladen, haben diese Intervalleinstellungen keine Auswirkung. Die Computer aktualisieren sich alle 60 Minuten.

Bei Einwahl nach Updates suchen

Wählen Sie diese Option, wenn sich die Computer in der Gruppe über eine Einwahlverbindung mit dem Internet verbinden sollen. Die Computer versuchen dann immer sich zu aktualisieren, sobald sie sich mit dem Internet verbinden.

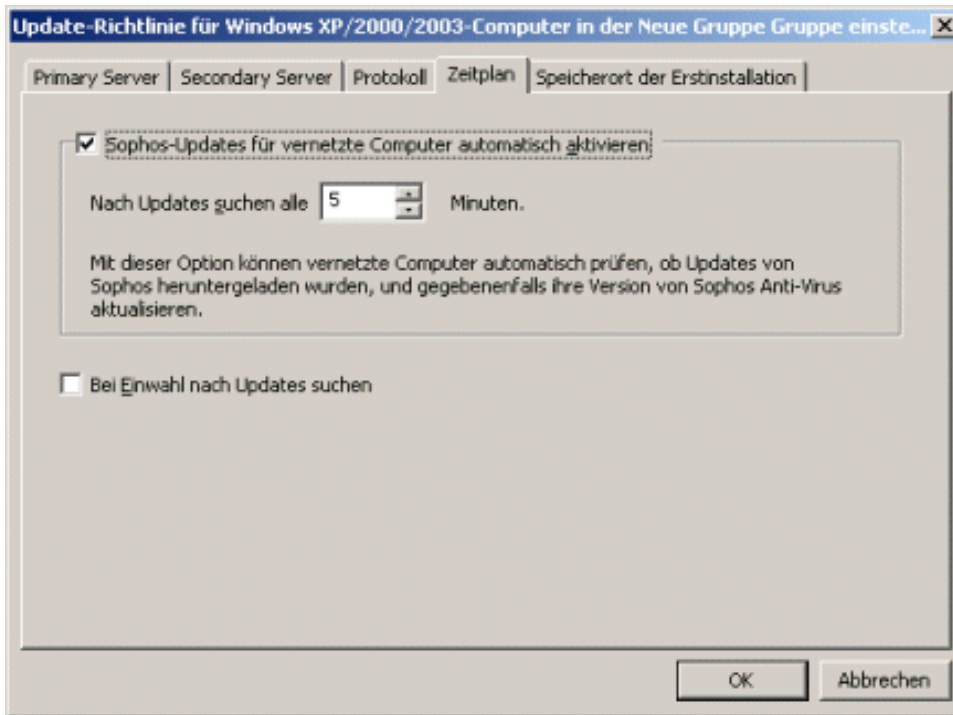
Updates, wenn sich Computer einwählen

Wenn sich eine Computergruppe aktualisieren soll, sobald die Computer eine Einwahlverbindung aufbauen, tun Sie Folgendes:



Sie geben diese Einstellungen separat für jeden Computertyp in der Gruppe ein (z. B. Windows 2000/XP/2003 oder Mac OS X).

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.
2. Wählen Sie im Dialogfenster **Update-Richtlinie für Computer in der ... Gruppe einstellen** ein Betriebssystem, das von Computern in dieser Gruppe eingesetzt wird. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Zeitplan**. Wählen Sie **Bei Einwahl nach Updates suchen**.



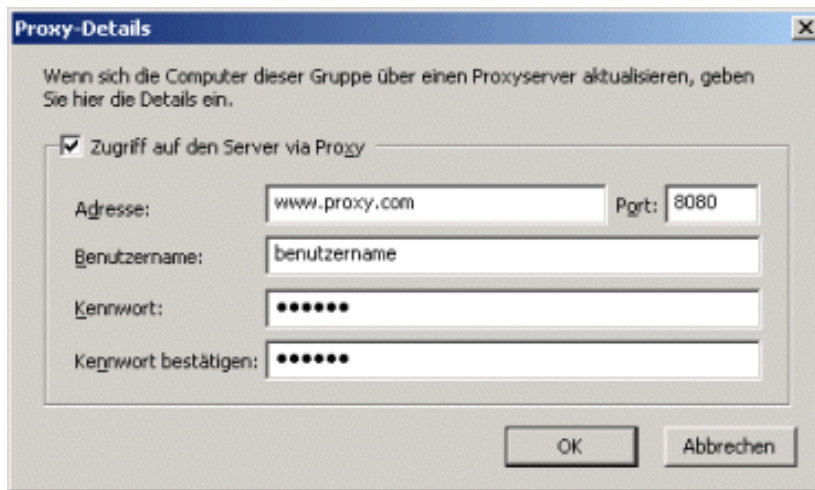
Updates über einen Proxyserver

Wenn sich die Computer in einer Gruppe Updates über das Internet herunterladen, müssen Sie die Details eines Proxyserver eingeben, über den Sie sich mit dem Internet verbinden.



Sie geben diese Einstellungen separat für jeden Computertyp in der Gruppe ein (z. B. Windows 2000/XP/2003 oder Mac OS X).

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.
2. Wählen Sie im Dialogfenster **Update-Richtlinie für Computer in der ... Gruppe einstellen** ein Betriebssystem, das von Computern in dieser Gruppe eingesetzt wird. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie, je nachdem, auf die Registerkarte **Primary Server** oder **Secondary Server**. Vergewissern Sie sich, dass alle eingegebenen Daten korrekt sind. Klicken Sie dann auf **Proxy-Details**.
4. Wählen Sie im Dialogfenster **Proxy-Details** die Option **Zugriff auf den Server via Proxy**. Geben Sie dann die **Adresse** und den **Port** des Proxyserver ein. Geben Sie einen **Benutzernamen** und ein **Kennwort** ein, die Zugriff auf den Proxyserver geben. Wenn der Benutzername die Domäne anzeigen muss, verwenden Sie die Form `domäne\benutzername`.



Zu verwendende Bandbreite beschränken

Sie können die Bandbreite, die für die Updates verwendet wird, beschränken. Dadurch wird verhindert, dass die gesamte Bandbreite verbraucht wird, während ein Computer dies auch für andere Zwecke benötigt, z. B. zum Download von E-Mails.



Sie geben diese Einstellungen separat für jeden Computertyp in der Gruppe ein (z. B. Windows 2000/XP/2003 oder Mac OS X).

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.
2. Wählen Sie im Dialogfenster **Update-Richtlinie für Computer in der ... Gruppe einstellen** ein Betriebssystem, das von Computern in dieser Gruppe eingesetzt wird. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie, je nachdem, auf die Registerkarte **Primary Server** oder **Secondary Server**. Vergewissern Sie sich, dass alle eingegebenen Daten korrekt sind. Klicken Sie dann auf **Erweitert**.
4. Wählen Sie im Dialogfenster **Erweiterte Einstellungen** die Option **Verwendete Bandbreite beschränken** und geben Sie mit Hilfe des Schiebereglers die Bandbreite in Kbits/Sekunde an. Wenn Sie mehr Bandbreite angeben, als dem Computer zur Verfügung steht, wird für die Updates die Bandbreite benutzt, die verfügbar ist.



Computer, die sich für Updates automatisch einwählen

Wenn Computer eine Einwahlverbindung nutzen, können Sie sicherstellen, dass diese Verbindung automatisch aufgebaut wird, wenn sie für Updates erforderlich ist.




Sie geben diese Einstellungen separat für jeden Computertyp in der Gruppe ein (z. B. Windows 2000/XP/2003).


1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.
2. Wählen Sie im Dialogfenster **Update-Richtlinie für Computer in der ... Gruppe einstellen** ein Betriebssystem, das von Computern in dieser Gruppe eingesetzt wird. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie, je nachdem, auf die Registerkarte **Primary Server** oder **Secondary Server**. Vergewissern Sie sich, dass alle eingegebenen Daten korrekt sind. Klicken Sie dann auf **Erweitert**.
4. Wählen Sie im Dialogfenster **Erweiterte Einstellungen** die Option **Einwahlverbindung automatisch aufbauen**.



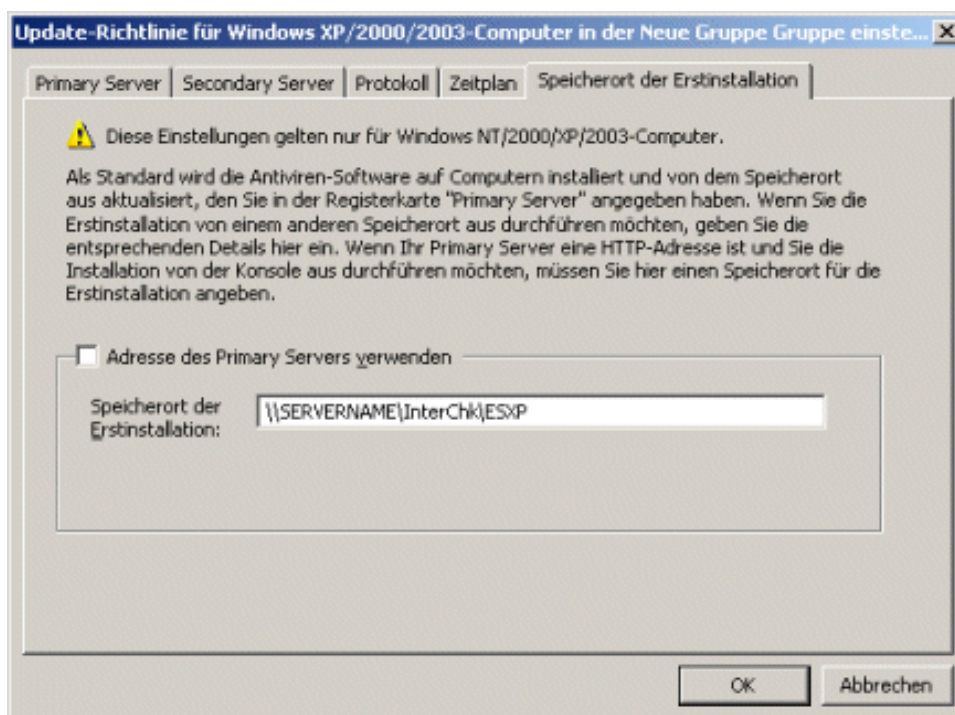
Auswählen einer anderen Quelle für die Erstinstallation

Als Standardvorgabe wird auf den Computern Antiviren-Software installiert und von der Quelle aus aktualisiert (dem "Primary Server"), die Sie angegeben haben, als Sie die Computergruppe eingerichtet haben. Wenn Sie die Erstinstallation von einer anderen Quelle aus durchführen möchten, tun Sie Folgendes:

 Wenn Ihr Primary Server eine HTTP (Internet)-Adresse ist und Sie die Installation auf den Computern von der Konsole aus durchführen möchten, müssen Sie eine Quelle für die Erstinstallation angeben.

 Sie geben diese Einstellungen separat für jeden Computertyp in der Gruppe ein (z. B. Windows 2000/XP/2003 oder Mac OS X).

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.
2. Markieren Sie im Dialogfenster **Update-Richtlinie für Computer in der ... Gruppe einstellen** ein Betriebssystem, das von Computern in dieser Gruppe eingesetzt wird, z. B. Windows 2000, 2003 und XP. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Speicherort der Erstinstallation**. Deaktivieren Sie die Option **Adresse des Primary Servers verwenden**. Geben Sie dann die Adresse der Quelle ein, die Sie verwenden möchten.



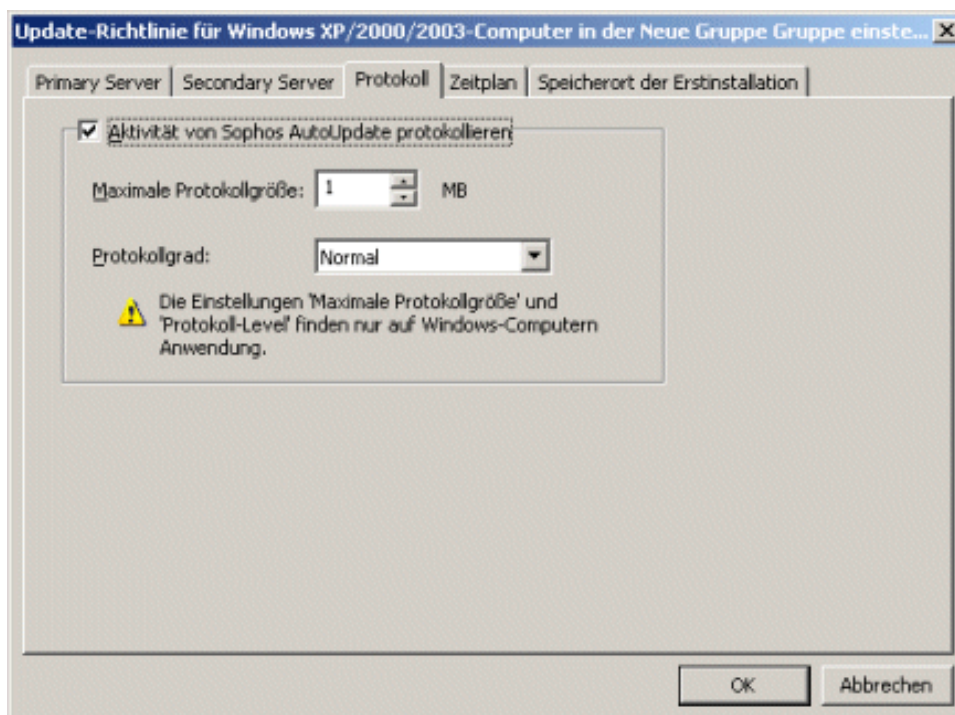
Update-Protokoll

Sie können Computer so konfigurieren, dass ihre Update-Aktivität protokolliert wird.



Sie geben diese Einstellungen separat für jeden Computertyp in der Gruppe ein (z. B. Windows 2000/XP/2003 oder Mac OS X).

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **Update-Richtlinie** in der Werkzeugleiste.
2. Wählen Sie im Dialogfenster **Update-Richtlinie für Computer in der ... Gruppe einstellen** ein Betriebssystem, das von Computern in dieser Gruppe eingesetzt wird. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Protokoll**. Vergewissern Sie sich, dass **Aktivität von Sophos AutoUpdate protokollieren** ausgewählt ist. Setzen Sie dann die anderen Optionen, wie nachfolgend erläutert.



Maximale Protokollgröße

Geben Sie eine maximale Größe für das Protokoll in MB an.

Protokollgrad

Sie können zwischen **Normal** und **Ausführlich** für das Protokoll wählen. Bei einem ausführlichen Protokoll werden Informationen über viel mehr

Aktivitäten protokolliert als normal, so dass das Protokoll schneller wachsen wird. Verwenden Sie diese Einstellung nur, wenn Sie das ausführliche Protokoll für eine Problembeseitigung benötigen.

Wie richte ich Virenbenachrichtigungen ein?

Als Standardvorgabe werden Alarme auf dem Computer–Desktop angezeigt, wenn dort ein Virus gefunden wurde. Sie können auch E–Mail–Benachrichtigungen für Administratoren einrichten.

Dieser Abschnitt erläutert, wie Sie beide Benachrichtigungsarten konfigurieren.

- Einrichten von E–Mail–Benachrichtigungen
- Konfiguration von Desktop–Benachrichtigungen

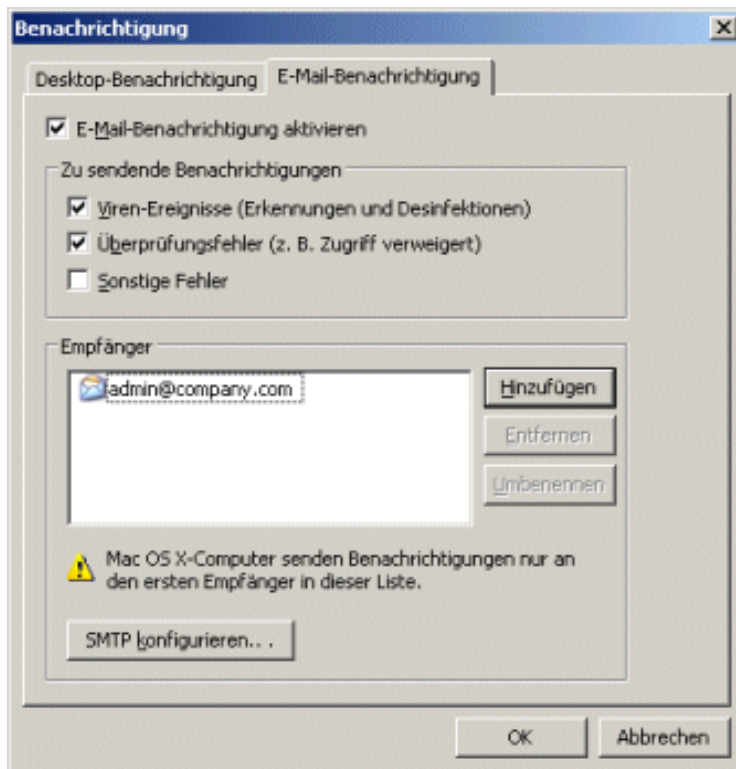
Einrichten von E–Mail–Benachrichtigungen

Sie können E–Mail–Benachrichtigungen an bestimmte Benutzer senden, wenn auf einem der Computer in einer Gruppe ein Virus entdeckt wurde oder ein Fehler aufgetreten ist.



Mac OS X Computer können E–Mail–Benachrichtigungen nur an eine Adresse senden.

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **SAV–Richtlinie** in der Werkzeugleiste.
2. Klicken Sie im Dialogfenster **Antiviren–Richtlinie** im Bereich **Sophos Anti–Virus konfigurieren** auf **Benachrichtigung**.
3. Klicken Sie auf die Registerkarte **E–Mail–Benachrichtigung**. Wählen Sie die Optionen aus wie nachfolgend erläutert.



E-Mail-Benachrichtigung aktivieren

Wählen Sie diese Option, damit Sophos Anti-Virus E-Mail-Benachrichtigungen senden kann.

Zu sendende Benachrichtigungen

Wählen Sie die Ereignisse, bei denen Sophos Anti-Virus E-Mail-Benachrichtigungen senden soll. Ein Überprüfungsfehler liegt beispielsweise auch dann vor, wenn Sophos Anti-Virus der Zugriff auf ein Objekt, das überprüft werden sollte, verwehrt wurde.

Empfänger

Klicken Sie entsprechend auf **Hinzufügen** oder **Entfernen**, um E-Mail-Adressen hinzuzufügen oder zu entfernen, an die die Benachrichtigungen gesendet werden sollen. Klicken Sie auf **Umbenennen**, um die E-Mail-Adresse zu ändern, die Sie hinzugefügt haben.

SMTP konfigurieren

Klicken Sie darauf, um die Einstellungen für den SMTP-Server und die Sprache der E-Mail-Benachrichtigungen zu ändern. (Siehe auch SMTP-Einstellungen konfigurieren.)

SMTP-Einstellungen konfigurieren

Configure SMTP settings

SMTP server
Enter the host name (e.g. mail.sophos.com) or IP address (e.g. 182.83.82.1) of your SMTP server

182.83.82.1

Test

SMTP 'sender' address
Bounces and non-delivery reports will be sent to this address. Leaving this blank will prevent SMTP servers from sending non-delivery reports.

sender@mycompany.com

SMTP 'reply to' address

admin@mycompany.com

This setting applies to Windows XP/2000/2003 computers only.

Language
Which language do you want the email to be sent in?

English

This setting applies to Windows XP/2000/2003 computers only.

OK Cancel

SMTP-Server

Geben Sie in das Textfeld den Hostnamen oder die IP-Adresse des SMTP-Servers ein. Klicken Sie auf **Test**, um eine Test-Benachrichtigungs-E-Mail zu senden.

SMTP 'sender' Adresse

Geben Sie in das Textfeld eine E-Mail-Adresse ein, an die nicht zustellbare Benachrichtigungen und Nicht-Zustellbarkeitsmeldungen gesendet werden können.

SMTP 'antwort an' Adresse

Da E-Mail-Benachrichtigungen von einem Systemkonto gesendet werden, können Sie in das Textfeld eine E-Mail-Adresse eingeben, an die Antworten auf E-Mail-Benachrichtigungen gesendet werden können.

Sprache

Klicken Sie auf den Drop-Down-Pfeil und wählen Sie die Sprache, in der die E-Mail-Benachrichtigungen gesendet werden sollen.

Konfiguration von Desktop-Benachrichtigungen

Als Standardvorgabe werden Alarme auf dem Computer angezeigt, auf dem ein Virus gefunden wurde. Sie können diese Alarme/Benachrichtigungen konfigurieren.

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Klicken Sie im Dialogfenster **Antiviren-Richtlinie** im Bereich **Sophos Anti-Virus konfigurieren** auf **Benachrichtigung**.
3. Klicken Sie auf die Registerkarte **Desktop-Benachrichtigung**. Wählen Sie die Optionen aus wie nachfolgend erläutert.



Desktop-Benachrichtigung aktivieren

Wählen Sie diese Option, damit Sophos Anti-Virus Desktop-Benachrichtigungen anzeigt, wenn ein Virus gefunden wurde.

Benutzerdefinierte Nachricht

In dieses Textfeld können Sie eine Nachricht eingeben, die an das Ende der Standard-Nachricht angefügt wird.

Wie kann ich die Antiviren-Einstellungen ändern?

Dieser Abschnitt erläutert, wie Sie die Einstellungen für die Virenüberprüfung und Desinfektion ändern. Sie können für jede Computer-Gruppe andere Einstellungen verwenden.

- Ändern der überprüften Dateitypen
- Dateien von der Überprüfung ausschließen
- Ändern der Bedingungen für die On-Access-Überprüfung
- Archivdateien überprüfen
- Dateien automatisch desinfizieren
- Computer zu festgesetzten Zeiten überprüfen

Ändern der überprüften Dateitypen

Als Standard überprüft Sophos Anti-Virus Dateitypen, die für Viren anfällig sind. Sie können weitere Dateitypen überprüfen oder bestimmte Dateitypen von der Überprüfung ausnehmen.

Die als Standard überprüften Dateitypen sind vom Betriebssystem abhängig und ändern sich bei Produkt-Updates. Sie können eine Liste der Dateitypen ansehen, wenn Sie zu einem Computer mit dem entsprechenden Betriebssystem gehen, das Sophos Anti-Virus Fenster öffnen und auf die Konfigurationsseite "Erweiterungen" gehen.



Diese Optionen sind nur für Windows-Computer relevant. Auf Macintosh-Computern können Sie Änderungen mit Hilfe des Mac Update Managers vornehmen.



Auf Windows 2000/XP/2003 können Sie diese Einstellungen für die On-Access- und die zeitgesteuerte Überprüfung separat ändern. Auf Windows NT/95/98/Me gelten Änderungen der Einstellungen für die zeitgesteuerte Überprüfung auch für die On-Access-Überprüfung.

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Es erscheint das Dialogfenster **Antiviren-Richtlinie**.

Um die On-Access-Überprüfung zu konfigurieren, klicken Sie im Bereich **Sophos Anti-Virus konfigurieren** auf **On-Access**.

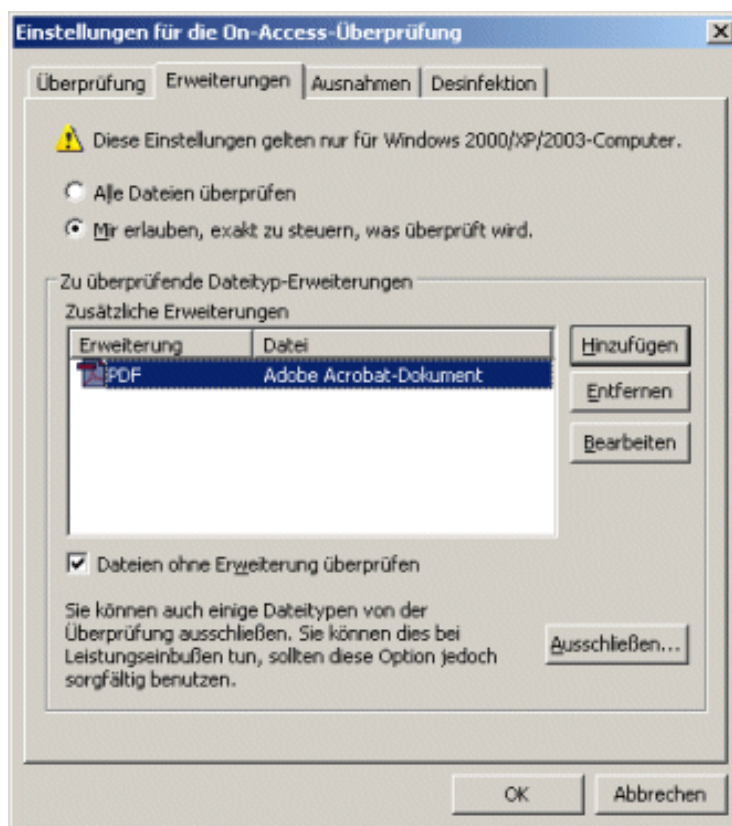
Um zeitgesteuerte Überprüfungen zu konfigurieren, klicken Sie im Bereich **Zeitgesteuerte Überprüfung** auf **Erweiterungen und Ausnahmen**.

3. Klicken Sie auf die Registerkarte **Erweiterungen**. Wählen Sie die Option **Mir erlauben, exakt zu steuern, was überprüft wird**.

Um zusätzliche Dateitypen zu überprüfen, klicken Sie auf **Hinzufügen** und geben im Feld "Erweiterung" die entsprechende Datei-Erweiterung ein, z. B. PDF.

Um Dateitypen auszuschließen, die normalerweise als Standard überprüft werden, klicken Sie auf **Ausschließen**. Es öffnet sich das Dialogfenster **Erweiterungen ausschließen**. Geben Sie die Datei-Erweiterung ein.


Als Standardvorgabe werden Dateien ohne Erweiterung überprüft.



Dateien von der Überprüfung ausschließen

Sie können Objekte von der Virenüberprüfung ausschließen.

 Diese Optionen sind nur für Windows-Computer relevant. Auf Macintosh-Computern können Sie Änderungen mit Hilfe des Mac Update Managers vornehmen.

 Auf Windows 2000/XP/2003 können Sie diese Einstellungen für die On-Access- und die zeitgesteuerte Überprüfung separat ändern. Auf Windows NT/95/98/Me gelten Änderungen der Einstellungen für die zeitgesteuerte Überprüfung auch für die On-Access-Überprüfung.

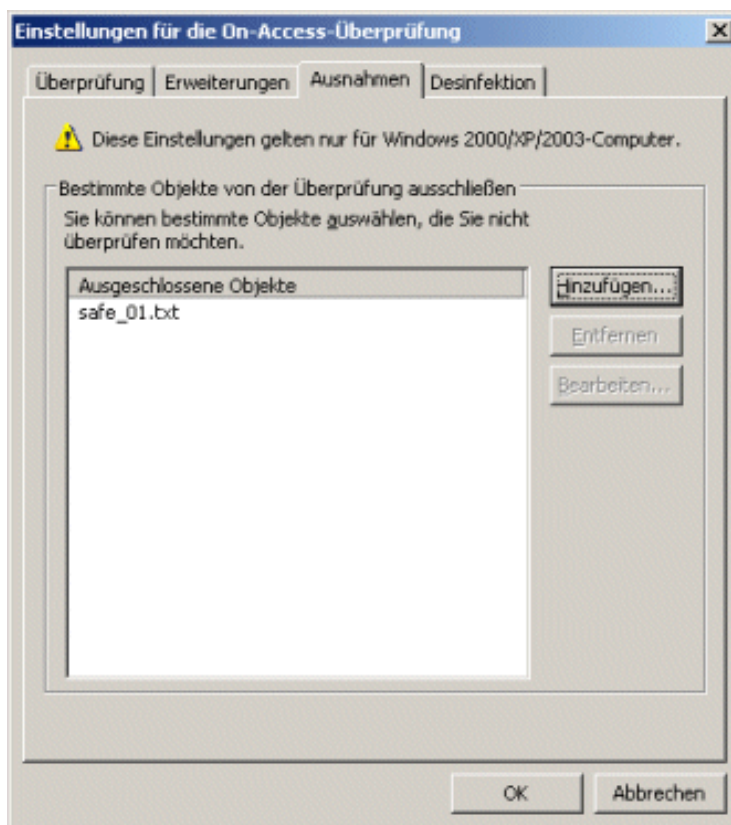
1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Es erscheint das Dialogfenster **Antiviren-Richtlinie**.

Um die On-Access-Überprüfung zu konfigurieren, klicken Sie im Bereich **Sophos Anti-Virus konfigurieren** auf **On-Access**.

Um zeitgesteuerte Überprüfungen zu konfigurieren, klicken Sie im Bereich **Zeitgesteuerte Überprüfung** auf **Erweiterungen und Ausnahmen**.

3. Klicken Sie auf die Registerkarte **Ausnahmen**. Um Objekte zu der Liste hinzuzufügen, klicken Sie auf **Hinzufügen** und geben den vollständigen Pfad in das Textfeld **Objekt** ein.

Die Objekte, die Sie von der Überprüfung ausschließen können, sind auf jedem Computertyp anders. Lesen Sie dazu Objekte, die von der Überprüfung ausgeschlossen werden können.



Objekte, die von der Überprüfung ausgeschlossen werden können

Auf jedem Computertyp gibt es verschiedene Einschränkungen der Objekte, die Sie von der Überprüfung ausschließen können.

Auf **Windows 2000/XP/2003** können Sie Laufwerke, Ordner und Dateien ausschließen. Sie können die Platzhalter * und ? benutzen.

Auf Windows NT können Sie Dateien und Verzeichnisse ausschließen.

Auf Windows 95/98/Me können Sie Dateien, Verzeichnisse (bei zeitgesteuerten Überprüfungen) und Laufwerke ausschließen.

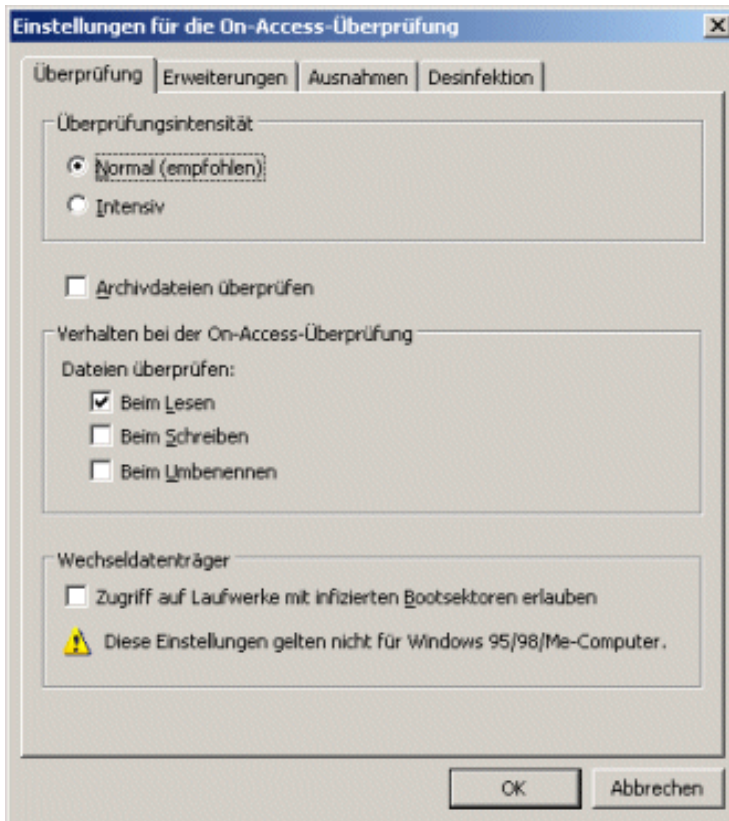
Ändern der Bedingungen für die On-Access-Überprüfung

Sie können angeben, ob Dateien überprüft werden sollen, wenn sie geöffnet ("beim Lesen"), gespeichert ("beim Schreiben") oder umbenannt werden.



Diese Optionen sind nur für Windows-Computer relevant.

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Klicken Sie im Dialogfenster **Antiviren-Richtlinie** im Bereich **Sophos Anti-Virus konfigurieren** auf **On-Access**.
3. Klicken Sie auf die Registerkarte **Überprüfung**. Wählen Sie im Bereich "Verhalten bei der On-Access-Überprüfung" die gewünschten Optionen aus.



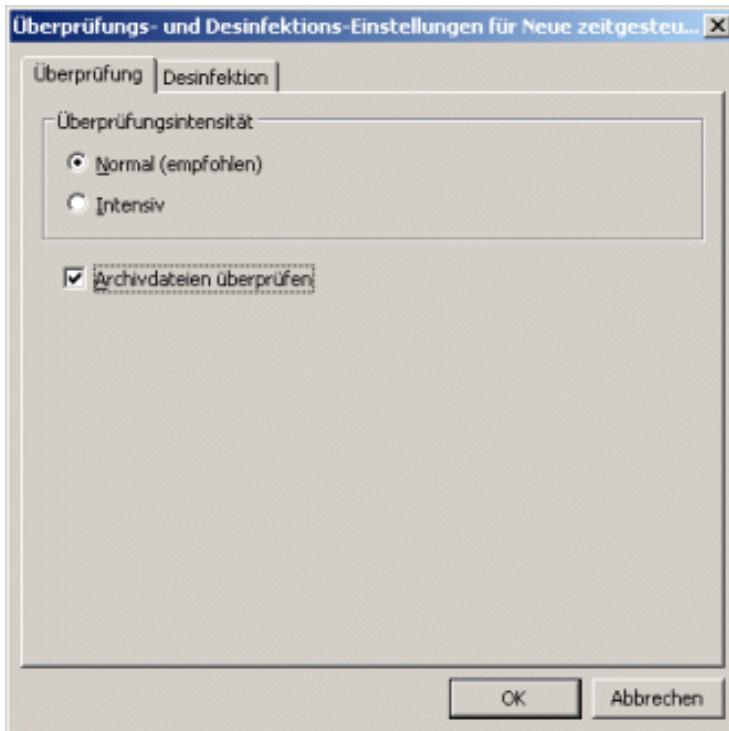
Archivdateien überprüfen

Sie können Archivdateien überprüfen.



Bei der On-Access-Überprüfung werden automatisch alle Dateien in einem Archiv überprüft, wenn Sie auf diese Dateien zugreifen. Die Überprüfung von Archivdateien ist daher optional und wird **nicht für die Verwendung bei der On-Access-Überprüfung empfohlen**.

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Klicken Sie im Dialogfenster **Antiviren-Richtlinie** im Bereich **Zeitgesteuerte Überprüfung** auf **Hinzufügen** (oder markieren Sie eine bestehende Überprüfung und klicken Sie auf **Bearbeiten**).
3. Geben Sie im Dialogfenster **Einstellungen der zeitgesteuerten Überprüfung** Ihre Einstellungen ein und klicken Sie dann auf **Konfigurieren** (unten in diesem Fenster).
4. Klicken Sie auf die Registerkarte **Überprüfung**. Wählen Sie **Archivdateien überprüfen**. Klicken Sie auf **OK**.



Dateien automatisch desinfizieren

Wenn ein Virus gefunden wurde, können diese Dateien automatisch desinfiziert werden.

Dieser Abschnitt erläutert, wie die automatische Desinfektion für die On-Access-Überprüfung eingerichtet wird. Wenn Sie dies tun, versucht Sophos Anti-Virus, infizierte Objekte zu desinfizieren, sobald ein Benutzer versucht, auf sie zuzugreifen.

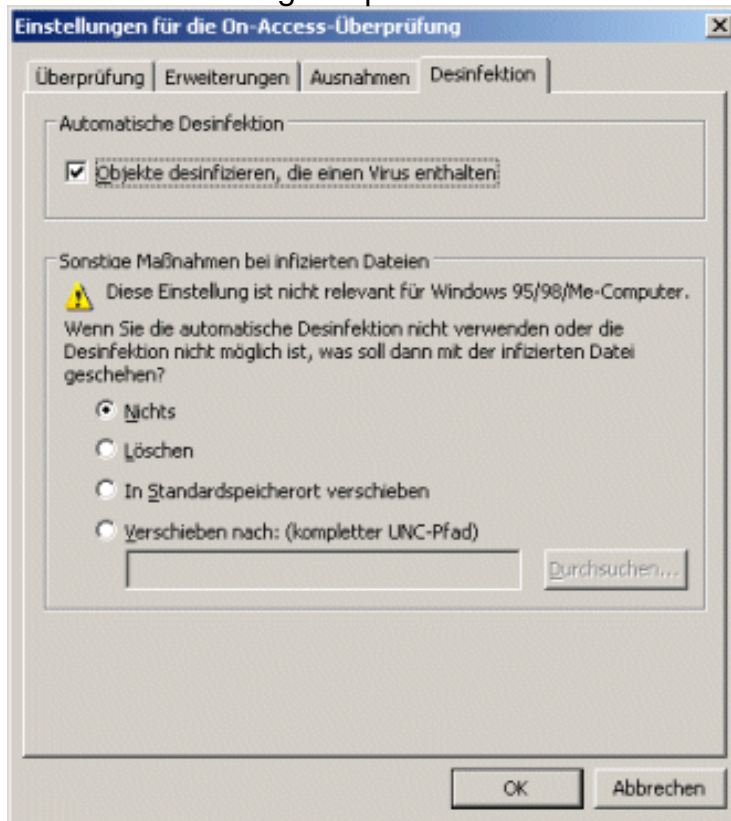
Sie können auch zeitgesteuerte Überprüfungen so konfigurieren, dass sie Desinfektionen automatisch durchführen. Lesen Sie dazu Computer bei einer zeitgesteuerten Überprüfung desinfizieren.

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Klicken Sie im Dialogfenster **Antiviren-Richtlinie** im Bereich **Sophos Anti-Virus konfigurieren** auf **On-Access**.
3. Klicken Sie auf die Registerkarte **Desinfektion**. Wählen Sie die Option **Objekte desinfizieren, die einen Virus enthalten**. Im Bereich **Sonstige Maßnahmen bei infizierten Dateien** können Sie angeben, was getan werden soll, wenn die Desinfektion fehlschlägt.



Wenn Sie wählen **Verschieben nach:** und einen Speicherort angeben, verschieben Mac OS X Computer infizierte Dateien trotzdem in den

standardmäßigen Speicherort.



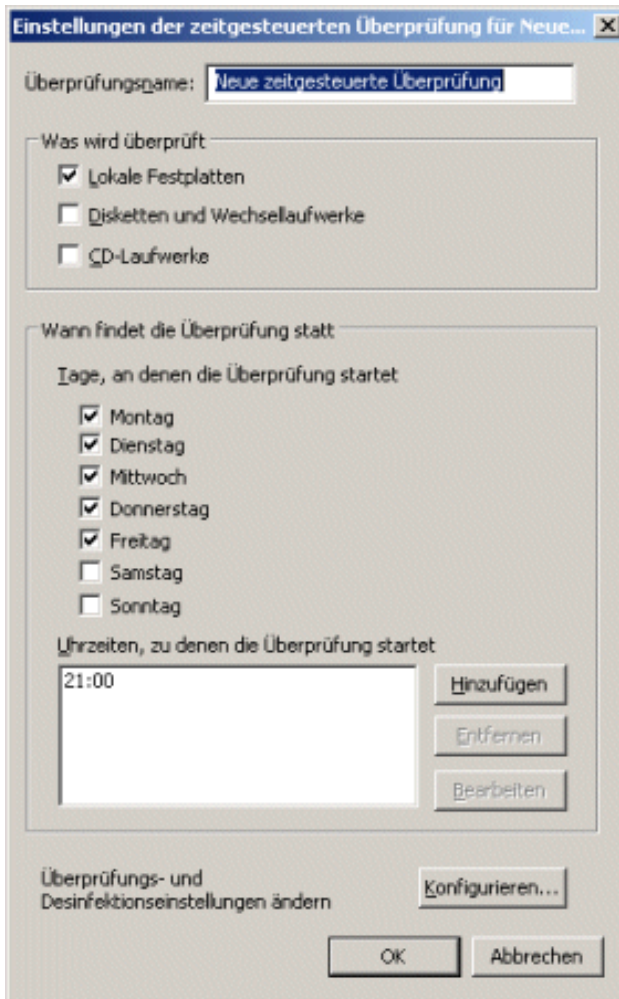
Computer zu festgesetzten Zeiten überprüfen

Computer können zu festgesetzten Zeiten überprüft werden.



Zeitgesteuerte Überprüfungen laufen nur auf Windows-Computern.

1. Markieren Sie die Gruppe, für die Sie zeitgesteuerte Überprüfungen einrichten möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Klicken Sie im Dialogfenster **Antiviren-Richtlinie** im Bereich **Zeitgesteuerte Überprüfung** auf **Hinzufügen**.
3. Geben Sie im Dialogfenster **Einstellungen der zeitgesteuerten Überprüfung** einen Namen für die zeitgesteuerte Überprüfung ein. Wählen Sie die Objekte aus, die überprüft werden sollen (als Standard werden alle lokalen Festplatten überprüft). Wählen Sie die Tage und Uhrzeiten, an denen die Überprüfung stattfinden soll. Wenn Sie andere Überprüfungsoptionen ändern oder die automatische Desinfektion einrichten möchten, klicken Sie auf **Konfigurieren** unten in dem Dialogfenster.



Wie stelle ich ein, dass mehrere Computer dieselben Einstellungen verwenden?

Dieser Abschnitt erläutert, wie Sie sicherstellen, dass alle Computer in einer Gruppe dieselben Antiviren- und Update-Einstellungen verwenden.

Sie können:

- prüfen, ob mehrere Computer die Gruppeneinstellungen verwenden
- einstellen, dass mehrere Computer die Gruppeneinstellungen verwenden

Prüfen, ob mehrere Computer die Gruppeneinstellungen verwenden

Sie können prüfen, ob alle Computer in einer Gruppe die Antiviren- und Update-Einstellungen für diese Gruppe verwenden.



Wenn Sie einen Computer von einer Gruppe in eine andere verschieben, behält der Computer die Einstellungen der ersten Gruppe bei. Diese können von denen der neuen Gruppe abweichen.

1. Markieren Sie die Gruppe, die Sie prüfen möchten.
2. Sehen Sie sich auf der **Status**-Seite die Spalten **SAV-Richtlinie** und **Update-Richtlinie** an. Verwendet der Computer nicht dieselben Einstellungen wie die übrigen Computer der Gruppe, sehen Sie ein rotes Warnsymbol und den Text "Anders als Gruppe".

Einstellen, dass mehrere Computer die Gruppeneinstellungen verwenden

Wenn Sie Computer finden, die nicht mit den Antiviren- und Update-Einstellungen für ihre Gruppe übereinstimmen, können Sie die Gruppeneinstellungen für diesen Computer wirksam machen.

1. Markieren Sie die Computer, die nicht mit den Gruppeneinstellungen übereinstimmen.
2. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **Übereinstimmung mit**. Wählen Sie dann entsprechend **Gruppen-Antiviren-Richtlinie** oder **Gruppen-Update-Richtlinie**.

Wie kann ich Computer zu festgesetzten Zeiten überprüfen?

Dieser Abschnitt erläutert, wie Computer zu bestimmten Zeiten überprüft werden.

Sie können:

- zeitgesteuerte Überprüfungen einrichten
- die Einstellungen für die zeitgesteuerten Überprüfungen ändern

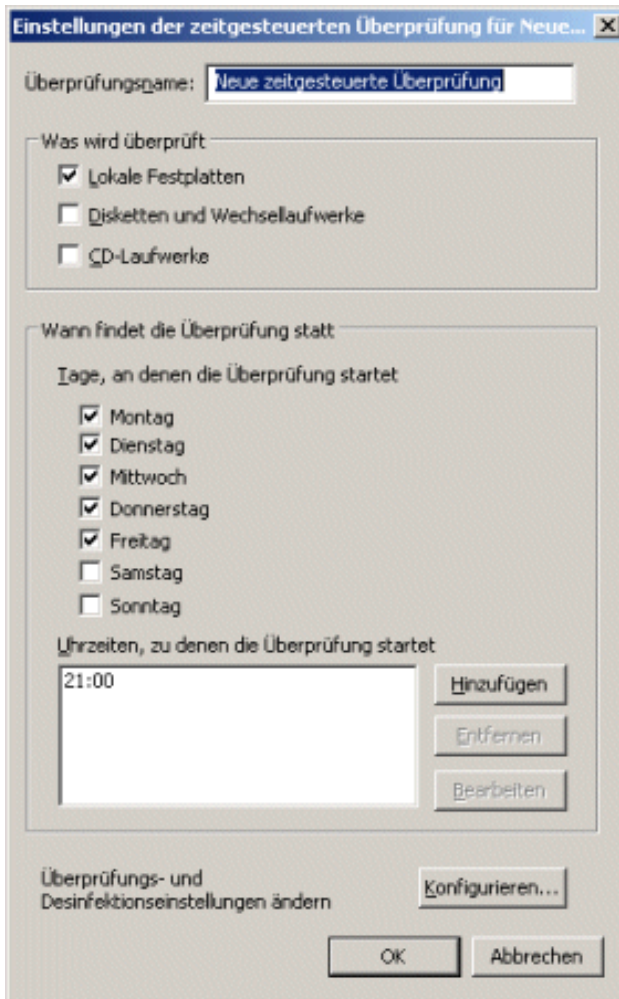
Zeitgesteuerte Überprüfungen einrichten

Computer können zu festgesetzten Zeiten überprüft werden.



Zeitgesteuerte Überprüfungen laufen nur auf Windows-Computern.

1. Markieren Sie die Gruppe, für die Sie zeitgesteuerte Überprüfungen einrichten möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Klicken Sie im Dialogfenster **Antiviren-Richtlinie** im Bereich **Zeitgesteuerte Überprüfung** auf **Hinzufügen**.
3. Geben Sie im Dialogfenster **Einstellungen der zeitgesteuerten Überprüfung** einen Namen für die zeitgesteuerte Überprüfung ein. Wählen Sie die Objekte aus, die überprüft werden sollen (als Standard werden alle lokalen Festplatten überprüft). Wählen Sie die Tage und Uhrzeiten, an denen die Überprüfung stattfinden soll. Wenn Sie andere Überprüfungsoptionen ändern oder die automatische Desinfektion einrichten möchten, klicken Sie auf **Konfigurieren** unten in dem Dialogfenster.



Die Einstellungen für die zeitgesteuerten Überprüfungen ändern

Sie können die Einstellungen für die zeitgesteuerte Überprüfung ändern.

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Im Dialogfenster **Antiviren-Richtlinie**, im Bereich **Zeitgesteuerte Überprüfung** können Sie zwei Arten der Einstellungen ändern:

Um die Dateitypen, die von **allen** zeitgesteuerten Überprüfungen gescannt werden, zu ändern, klicken Sie auf **Erweiterungen und Ausnahmen**.

Um Einstellungen speziell für eine Überprüfung zu ändern (z. B. was überprüft wird, die Überprüfungsoptionen, Desinfektion), markieren Sie die Überprüfung und klicken auf **Bearbeiten**. Klicken Sie dann im Dialogfenster **Einstellungen der zeitgesteuerten Überprüfung** auf **Konfigurieren**.



Ausführliche Hinweise über diese Einstellungen finden Sie im Abschnitt *Wie kann ich die Antiviren-Einstellungen ändern* ?

Wie kann ich Computer mit Problemen finden und die Probleme beheben?

Dieser Abschnitt erläutert, wie Sie Computer, auf denen ein Problem aufgetreten ist, finden und wie Sie das Problem lösen.

Sie können:

- Computer suchen, auf denen die On-Access-Überprüfung nicht aktiv ist
- Computer mit Alarmen suchen, die eine nähere Untersuchung erfordern
- Veraltete Computer suchen
- Computer suchen, die nicht von der Konsole verwaltet werden
- Computer suchen, die nicht mit dem Netzwerk verbunden sind

Computer suchen, auf denen die On-Access-Überprüfung nicht aktiv ist



Möglicherweise haben Sie sich entschieden, bei bestimmten Computertypen, z. B. auf Fileservern, die On-Access-Überprüfung nicht einzusetzen. Stellen Sie in diesem Fall sicher, dass auf diesen Computern zeitgesteuerte Überprüfungen laufen und dass sie up to date sind.

Wenn auf einem Computer die On-Access-Überprüfung nicht aktiv ist, werden auf der **Status-Seite** in der Spalte **On-Access** ein graues Schild und das Wort "Inaktiv" angezeigt.

Um sich alle diese Computer anzeigen zu lassen und das Problem zu beheben, tun Sie Folgendes:

1. Markieren Sie die Gruppe, in der Sie die Gruppe suchen möchten.
2. Wählen Sie in der Werkzeugleiste in der **Ansicht** Drop-Down-Liste **Computer, auf denen die On-Access-Überprüfung nicht aktiv ist**.
3. Wenn die Gruppe auch Untergruppen enthält, wählen Sie, ob Sie Computer **Nur auf dieser Stufe** oder **Auf dieser Stufe und darunter** suchen möchten.
4. Sind dort Computer aufgelistet, überprüfen Sie die Antiviren-Richtlinie. Markieren Sie dazu die Gruppe und klicken Sie auf das Symbol SAV-Richtlinie in der Werkzeugleiste. Überprüfen Sie, dass die Option **On-Access-Überprüfung aktivieren** ausgewählt ist.
5. Markieren Sie die Computer, auf denen keine On-Access-Überprüfung läuft, klicken Sie mit der rechten Maustaste auf sie und wählen Sie

Übereinstimmung mit|Gruppen–Antiviren–Richtlinie.

Computer mit Alarmen suchen, die eine nähere Untersuchung erfordern

Wenn ein Computer einen Alarm gesendet hat, der eine nähere Untersuchung erfordert, erscheint ein Alarmsymbol in der Spalte **Alarme** auf der **Status**–Seite. Ein rotes Warnsymbol zeigt einen Virus an; ein gelbes Dreieck zeigt einen Fehler an.

Um sich Computer mit schwerwiegenden Alarmen anzeigen zu lassen, tun Sie Folgendes:

1. Markieren Sie die Gruppe, in der Sie Computer mit Alarmen suchen möchten.
2. Wählen Sie in der Werkzeugleiste in der **Ansicht** Drop–Down–Liste **Computer, auf denen die On–Access–Überprüfung nicht aktiv ist**.
3. Wenn die Gruppe auch Untergruppen enthält, wählen Sie, ob Sie Computer **Nur auf dieser Stufe** oder **Auf dieser Stufe und darunter** suchen möchten.
4. Sollte es Computer mit einem Virus geben, lesen Sie bitte Computer desinfizieren (Übersicht).

Wenn es veraltete Computer gibt, lesen Sie bitte Veraltete Computer suchen für Hilfe bei der Diagnose und der Behebung des Problems.



Wenn der Alarm nicht mehr angezeigt werden soll, können Sie ihn löschen. Markieren Sie die Computer mit Alarmen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Alarme löschen**.

Veraltete Computer suchen

Wenn ein Computer eine veraltete Antiviren–Software hat, wird ein Uhrensymbol in der Spalte **Up to date** auf der **Status**–Seite angezeigt. Der Text zeigt an, wie lange der Computer nicht aktualisiert wurde.

Ein Computer kann aus einem von zwei Gründen veraltet sein:

- Dieser Computer hat kein Update vom Server erhalten.
- Der Server selbst hat nicht die neueste Sophos Software verfügbar.

Dieser Abschnitt erläutert, wie Sie das Problem diagnostizieren und die Computer aktualisieren.

1. Markieren Sie die Gruppe, in der Sie veraltete Computer suchen möchten.
2. Klicken Sie in der Registerkarte **Status** auf die Spalte **Up to date**, um die Computer nach Aktualität zu sortieren.
3. Klicken Sie auf die Registerkarte **Update–Details** und sehen Sie in der Spalte **Primary Server** nach. Dort wird das Verzeichnis angezeigt, von dem aus sich jeder Computer aktualisiert.
4. Sehen Sie sich jetzt die Computer an, die sich von einem bestimmten Verzeichnis aus aktualisieren.

Wenn einige veraltet sind, andere aber nicht, besteht das Problem auf einzelnen Computern. Markieren Sie diese Computer und klicken Sie auf das Symbol **Computer aktualisieren** in der Werkzeugleiste.

Wenn alle Computer veraltet sind, könnte das Problem im Verzeichnis liegen. Klicken Sie auf das Symbol **Libraries** in der Werkzeugleiste. Klicken Sie in der EM Library Console auf den Library–Namen (im linken Fensterbereich) und klicken Sie dann auf **Central Installations**. Markieren Sie das Verzeichnis, von dem Sie vermuten, dass es veraltet ist. Klicken Sie mit der rechten Maustaste darauf und wählen Sie **Update CID**. Gehen Sie dann wieder zur Enterprise Console, markieren Sie die veralteten Computer und klicken Sie auf das **Computer aktualisieren** Symbol in der Werkzeugleiste.

Computer suchen, die nicht von der Konsole verwaltet werden

Windows– und Macintosh–Computer sollten von Enterprise Console verwaltet werden, so dass sie aktualisiert und überwacht werden können.

Wenn ein Computer nicht verwaltet wird, sind seine **Details** auf der Registerkarte **Status** ausgegraut.

Folgendermaßen finden Sie nicht verwaltete Computer und können dieses Problem beheben.

1. Wählen Sie in der Werkzeugleiste in der Ansicht Drop–Down–Liste Nicht verwaltete Computer.
2. Markieren Sie alle aufgelisteten Computer. Klicken Sie in der Werkzeugleiste auf **Schützen**, um eine verwaltete Version von Sophos Anti–Virus zu installieren.

3. Wenn es Computer gibt, auf denen Enterprise Console Sophos Anti-Virus nicht automatisch installieren kann, führen Sie eine manuelle Installation durch.



Denken Sie daran, dass zum Netzwerk neu hinzugefügte Computer von der Konsole nicht automatisch angezeigt bzw. verwaltet werden. Klicken Sie auf **Suchen** in der Werkzeugleiste, um nach diesen Computern zu suchen und in den Ordner 'Nicht zugewiesen' zu legen.

Computer suchen, die nicht mit dem Netzwerk verbunden sind

Wenn ein Computer nicht mit dem Netzwerk verbunden ist, erscheint ein rotes Kreuz auf dem Symbol neben seinem Namen in der **Status**-Seite.

Um sich eine Liste aller Computer anzeigen zu lassen, die nicht mit dem Netzwerk verbunden sind, tun Sie Folgendes:

1. Markieren Sie die Gruppe, in der Sie nach Computern suchen möchten, die nicht mit dem Netzwerk verbunden sind.
2. Wählen Sie in der Werkzeugleiste in der **Ansicht** Drop-Down-Liste **Nicht verbundene Computer**.
3. Wenn die Gruppe auch Untergruppen enthält, wählen Sie, ob Sie Computer **Nur auf dieser Stufe** oder **Auf dieser Stufe und darunter** suchen möchten.



"Nicht verbundene Computer" meint hier Computer, die normalerweise von Enterprise Console verwaltet werden, aber nicht mit dem Netzwerk verbunden sind. Nicht verwaltete unverbundene Computer werden nicht angezeigt.

Wie gehe ich mit Alarmen um?

Dieser Abschnitt erläutert, wie Sie mit Alarmen umgehen.

Sie können:

- Alarme bearbeiten
- Alarme aus der Konsole löschen

Umgang mit Alarmen

Wenn Sie Alarme von Computern im Netzwerk erhalten oder Alarme bzw. Warnungen für Computer auf der **Status**-Seite sehen, sollten Sie eine Maßnahme ergreifen.

In folgenden Abschnitten finden Sie Informationen über den Umgang mit infizierten oder veralteten Computern:

- Desinfektion von Computern (Überblick)
- Computer jetzt aktualisieren

Alarme aus der Konsole löschen

Wenn Sie bei Alarmen Maßnahmen ergreifen oder überzeugt sind, dass ein Computer sicher ist, können Sie die Alarmsymbole in der Konsole löschen.

1. Markieren Sie die Computer, für die Sie die Alarme löschen möchten. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **Benachrichtigungen löschen**.
2. Klicken Sie im Dialogfenster **Alarme löschen** auf die Registerkarte **Virenbenachrichtigungen** oder **Sophos Anti-Virus Fehler**. Markieren Sie alle Alarme und klicken Sie auf **OK**.

Wie kann ich Computer desinfizieren?

Dieser Abschnitt erläutert, wie Sie Computer desinfizieren, die mit einem Virus infiziert sind.

Sie können Folgendes tun:


- Computer desinfizieren (Überblick)
- einen Computer mit einer sofortigen Überprüfung desinfizieren
- einen Computer manuell desinfizieren
- Computer mit einer zeitgesteuerten Überprüfung desinfizieren
- den Computer nach Nebeneffekten wiederherstellen
- die automatische Desinfektion einrichten

Computer desinfizieren (Überblick)

Wenn Sie Computer haben, die mit einem Virus infiziert sind, sollten Sie diese Computer vom Netzwerk isolieren, um eine weitere Verbreitung des Virus zu verhindern.

Sie sollten dann die Computer desinfizieren.

1. Gehen Sie zu jedem Computer. Löschen Sie entweder die infizierten Objekte oder versuchen Sie, diese mit Hilfe der Optionen in Sophos Anti-Virus zu desinfizieren. Lesen Sie dazu auch einen Computer mit einer sofortigen Überprüfung desinfizieren.
2. Wenn Sophos Anti-Virus den Virus nicht entfernen kann, können Sie sich auf der Sophos Website über die Entfernung des Virus informieren und die Desinfektion selbst durchführen. Lesen Sie dazu auch Computer manuell desinfizieren.
3. Ergreifen Sie nach der Desinfektion Maßnahmen, um den Computer nach Nebeneffekten wiederherzustellen.

 Wenn Sie eine größere Anzahl infizierter Computer haben, können Sie versuchen, sie von der Konsole aus mit einer zeitgesteuerten Überprüfung durch Sophos Anti-Virus zu desinfizieren. Dies ist jedoch nicht der empfohlene Weg. Lesen Sie dazu Computer bei einer zeitgesteuerten Überprüfung desinfizieren.

Einen Computer mit einer sofortigen Überprüfung desinfizieren

Mit Sophos Anti-Virus können Sie infizierte Objekte auf einem Computer

desinfizieren. Nachfolgend werden die dafür erforderlichen Schritte erläutert für:

- Windows 2000/XP/2003
- Windows NT oder Windows 95/98/Me
- Mac OS X

Sollten danach noch infizierte Dateien vorhanden sein, lesen Sie bitte Computer manuell desinfizieren.

Desinfektion auf Windows 2000/XP/2003-Computern

1. Gehen Sie zu dem infizierten Computer, klicken Sie mit der rechten Maustaste auf das Sophos Anti-Virus Symbol im Systemtray und wählen Sie **Sophos Anti-Virus öffnen**.
2. Klicken Sie im **Sophos Anti-Virus** Fenster, im **Konfigurations**-Menü auf **Überprüfung bei Rechtsklick**.
3. Klicken Sie auf die Registerkarte **Desinfektion**. Wählen Sie die Option **Objekte desinfizieren, die einen Virus enthalten**.
4. Öffnen Sie den Windows Explorer. Klicken Sie dazu in der Taskleiste auf Start|**Programme**|**Zubehör**|Windows-Explorer.
5. Markieren Sie die Datei(en), Ordner und/oder Laufwerke, die Sie überprüfen möchten.
6. Klicken Sie mit der rechten Maustaste auf die Auswahl und wählen Sie **Mit Sophos Anti-Virus überprüfen** aus dem Menü.

Desinfektion auf Windows NT- oder Windows 95/98/Me-Computern

1. Gehen Sie zu dem infizierten Computer, klicken Sie mit der rechten Maustaste auf das Sophos Anti-Virus Symbol im Systemtray und wählen Sie **Sophos Anti-Virus öffnen**.
2. Klicken Sie im **Sophos Anti-Virus** Fenster, im **Optionen**-Menü auf **Konfiguration**.
3. Klicken Sie auf die Registerkarte **Maßnahme**. Wählen Sie dann die gewünschten Optionen aus.
4. Klicken Sie dann auf **Go**, um eine Überprüfung mit aktivierter Desinfektion zu starten.

Desinfektion auf Mac OS X-Computern

1. Gehen Sie zu dem infizierten Computer, klicken Sie mit der rechten Maustaste auf das Sophos Anti-Virus Symbol in der Menüleiste und wählen Sie **Sophos Anti-Virus öffnen**.
2. Öffnen Sie im Sophos Anti-Virus Fenster den Dialog **On-Demand-Überprüfung Einstellungen**.
3. Wählen Sie im Menü **On-Demand-Überprüfung** die Option **Desinfektion**. Wählen Sie dann die gewünschten Desinfektionsoptionen aus.
4. Kehren Sie zum Sophos Anti-Virus Fenster zurück und klicken Sie auf den grünen Pfeil, um eine Überprüfung mit aktivierter Desinfektion zu starten.

Computer manuell desinfizieren

Wenn Sie Sophos Anti-Virus nicht so eingerichtet haben, dass infizierte Objekte desinfiziert werden, oder wenn die Desinfektion fehlgeschlagen ist, können Sie sich über die manuelle Desinfektion informieren.

1. Klicken Sie in der Computerliste auf die Registerkarte **Alarm-Details**. Suchen Sie in der Spalte **Virus erkannt** nach dem Namen des Virus.
2. Klicken Sie im **Hilfe**-Menü auf **Vireninformationen**. Dadurch werden Sie mit der Sophos Website verbunden, auf der Sie die Analyse des Virus und Informationen über seine Desinfektion finden.



Auf der Sophos Website sind außerdem spezielle Desinfektions-Tools für bestimmte Viren und Würmer zum Download verfügbar.

Computer mit einer zeitgesteuerten Überprüfung desinfizieren

Wenn Sie auf Ihren Computern noch keine automatische Desinfektion eingerichtet haben, können Sie jetzt eine Desinfektion von der Konsole aus durchführen.

Richten Sie dazu eine zeitgesteuerte Überprüfung auf dem Computer ein und konfigurieren Sie diese so, dass alle entdeckten Viren desinfiziert werden.



Bevor Sie beginnen, sollten Sie alle infizierten Computer vorübergehend in dieselbe Gruppe legen. Dazu müssen Sie die nachfolgenden Schritten nur einmal ausführen.

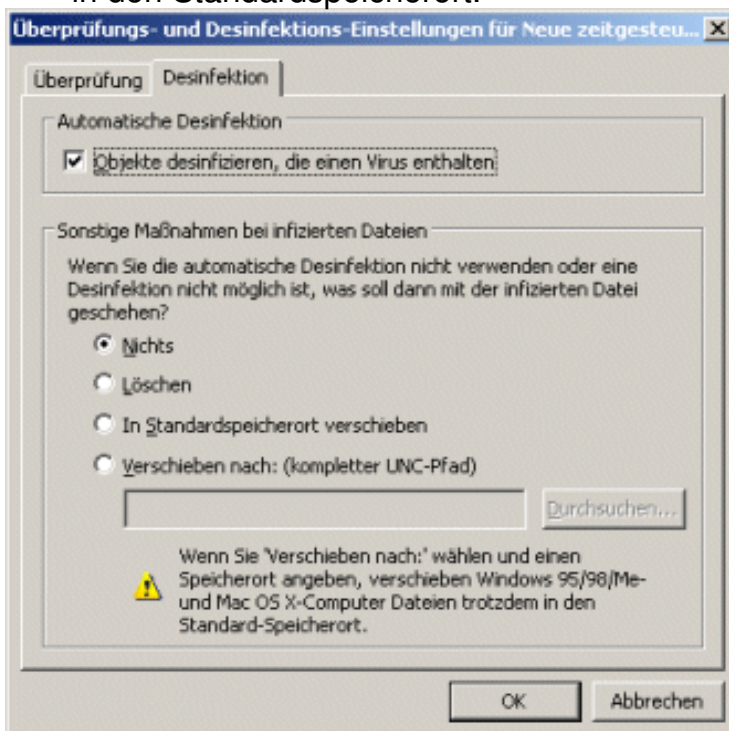


Zeitgesteuerte Überprüfungen laufen nur auf Windows-Computern.

1. Markieren Sie die Gruppe, in der sich die Computer befinden, die Sie desinfizieren möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Klicken Sie im Dialogfenster **Antiviren-Richtlinie** im Bereich **Zeitgesteuerte Überprüfung** auf **Hinzufügen** (oder markieren Sie eine bestehende Überprüfung und klicken Sie auf **Bearbeiten**).
3. Markieren Sie im Dialogfenster **Einstellungen der zeitgesteuerten Überprüfung** die Objekte, die Sie überprüfen möchten, und richten Sie einen Termin für die Überprüfung ein. Die Überprüfung kann auch ganz zeitnah stattfinden. Klicken Sie dann auf **Konfigurieren** unten im Fenster.
4. Klicken Sie auf die Registerkarte **Desinfektion**. Wählen Sie die Option **Objekte desinfizieren, die einen Virus enthalten**. Im Bereich **Sonstige Maßnahmen bei infizierten Dateien** können Sie angeben, was getan werden soll, wenn die Desinfektion fehlschlägt.



Wenn Sie wählen **Verschieben nach:** und einen Speicherort angeben, verschieben Windows 95/98/Me-Computer infizierte Objekte trotzdem in den Standardspeicherort.



5. Wenn eine zeitgesteuerte Überprüfung startet, werden die Computer, sofern möglich, desinfiziert. Sollten danach noch infizierte Dateien vorhanden sein, lesen Sie bitte Computer manuell desinfizieren.

Den Computer nach Nebeneffekten wiederherstellen

Die Wiederherstellung ist abhängig von der Art und Weise, wie der Virus den Computer infiziert hat. Einige Viren haben gar keine Nebeneffekte, bei anderen sind sie jedoch so extrem, dass Sie eine ganze Festplatte wiederherstellen müssen.

Einige Viren verändern allmählich Daten. Diese Art der Schädigung ist besonders schwer zu entdecken. Es ist daher sehr wichtig, dass Sie die Virenanalyse auf der Sophos Website lesen und das Dokument nach der Desinfektion sorgfältig überprüfen.

Sicherungskopien sind unerlässlich. Sie sollten die originalen Programme auf schreibgeschützten Datenträgern aufbewahren, so dass infizierte Programme einfach ersetzt werden können. Wenn Sie keine Sicherungskopien hatten, bevor Sie infiziert wurden, sollten Sie auf jeden Fall welche für die Zukunft erstellen.

Unter Umständen können Sie Daten von Datenträgern, die von einem Virus geschädigt wurden, wiederherstellen. Sophos kann Tools zur Verfügung stellen, die bei der Reparatur von Schäden durch Viren helfen. Wenn Sie Hilfe benötigen, wenden Sie sich bitte an den technischen Support von Sophos.

Einrichten der automatischen Desinfektion

Wenn ein Virus gefunden wurde, können die entsprechenden Dateien automatisch desinfiziert werden.

Dieser Abschnitt erläutert, wie die automatische Desinfektion für die On-Access-Überprüfung eingerichtet wird. Wenn Sie dies tun, versucht Sophos Anti-Virus, infizierte Objekte zu desinfizieren, sobald ein Benutzer versucht, auf sie zuzugreifen.

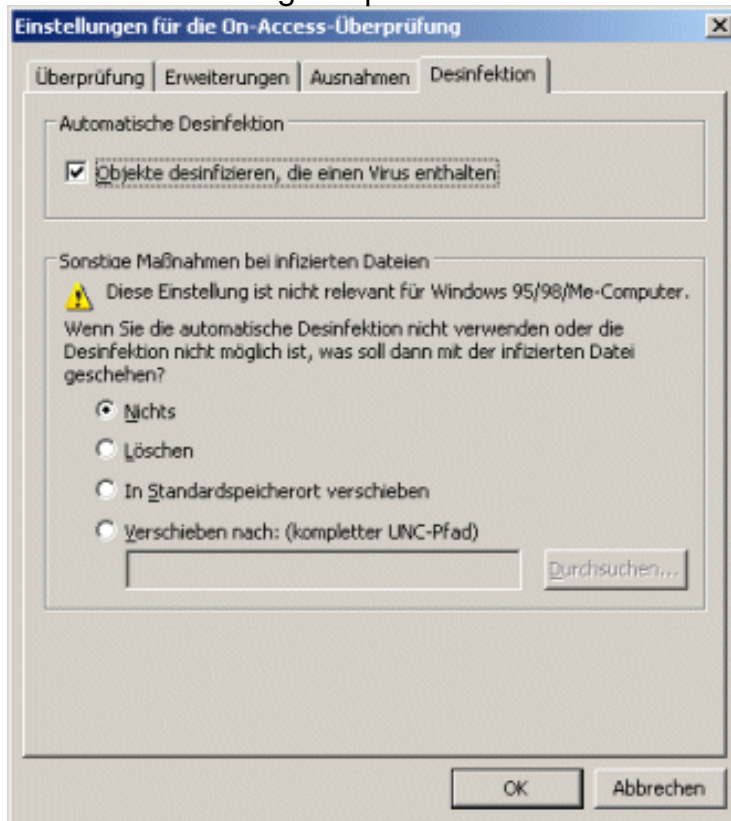
Sie können auch zeitgesteuerte Überprüfungen so konfigurieren, dass sie Desinfektionen automatisch durchführen. Lesen Sie dazu Computer bei einer zeitgesteuerten Überprüfung desinfizieren.

1. Markieren Sie die Gruppe, für die Sie die Einstellungen ändern möchten. Klicken Sie auf das Symbol **SAV-Richtlinie** in der Werkzeugleiste.
2. Klicken Sie im Dialogfenster **Antiviren-Richtlinie** im Bereich **Sophos Anti-Virus konfigurieren** auf **On-Access**.
3. Klicken Sie auf die Registerkarte **Desinfektion**. Wählen Sie die Option **Objekte desinfizieren, die einen Virus enthalten**. Im Bereich **Sonstige Maßnahmen bei infizierten Dateien** können Sie angeben, was getan

werden soll, wenn die Desinfektion fehlschlägt.



Wenn Sie wählen **Verschieben nach:** und einen Speicherort angeben, verschieben Mac OS X Computer infizierte Dateien trotzdem in den standardmäßigen Speicherort.



Wie kann ich Reports erzeugen?

Sie können Report über Virenalarme in Ihrem Netzwerk erzeugen.

Klicken Sie dazu auf das **Reports**-Symbol in der Werkzeugleiste und verwenden Sie dann die **Reports**-Optionen, wie in diesem Abschnitt erläutert.

Sie können:

- einen Report erzeugen
- sich einen Report in Form einer Tabelle anzeigen lassen
- sich einen Report in Form eines Diagramms anzeigen lassen
- sich die Anzahl der Alarme pro Virus anzeigen lassen
- sich die Anzahl der Alarme pro Ort anzeigen lassen
- sich die Häufigkeit von Virenalarmen anzeigen lassen
- sich Details von Virenalarmen anzeigen lassen
- einen Report ausdrucken
- einen Report in eine Datei exportieren
- das Report-Layout ändern

Einen Report erzeugen

Um einen Report zu erstellen, tun Sie Folgendes:

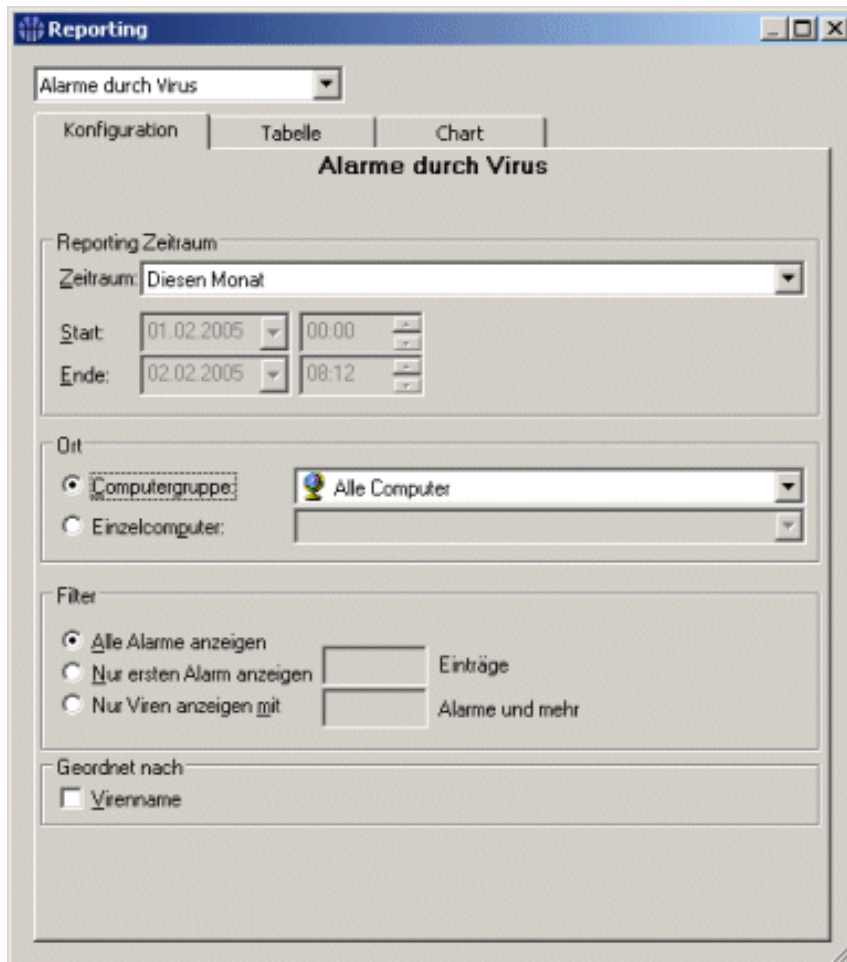
1. Öffnen Sie in der Sophos Enterprise Console das **Werkzeuge**-Menü und wählen Sie **Reports**.
2. Es öffnet sich das Dialogfenster **Reporting**.

Klicken Sie im Drop-Down-Menü auf den gewünschten Report-Typ.

- ◆ **Alarme durch Virus** zeigt die Anzahl an Alarmen für jeden Virus an, der in Ihrem Netzwerk erkannt wurde.
- ◆ **Alarme pro Ort** zeigt die Anzahl an Alarmen für jeden Computer oder jede Computergruppe an.
- ◆ **Alarme nach Zeit** zeigt die Häufigkeit von Virenalarmen während eines bestimmten Zeitraums an.
- ◆ **Alarminformationen** zeigt ausführliche Informationen über jeden Virenalarm an.

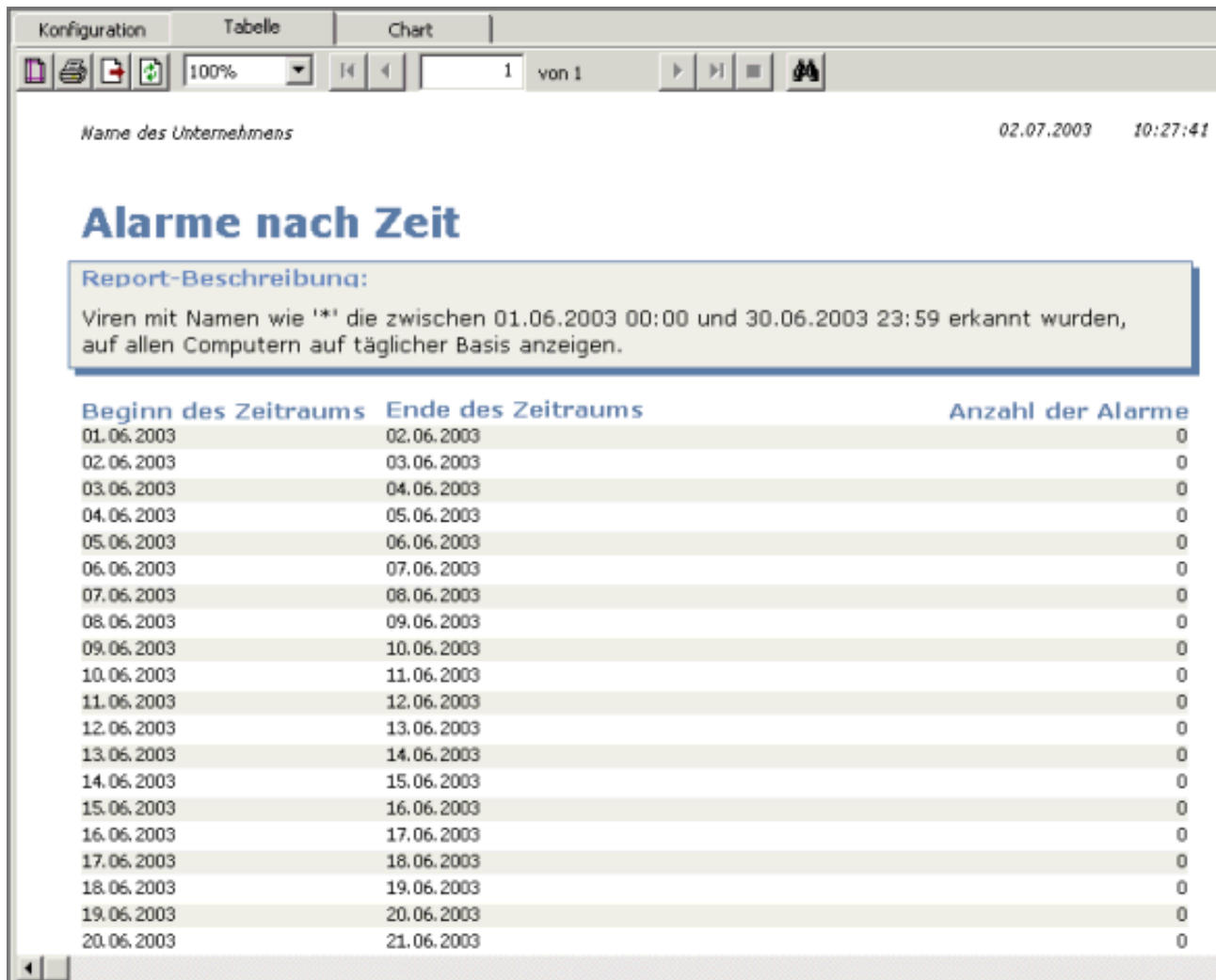
In der Registerkarte **Konfiguration** können Sie den Report anpassen.

Klicken Sie dann auf die Registerkarte **Tabelle** oder **Chart**, um sich den Report anzusehen.



Einen Report in Form einer Tabelle anzeigen

1. Öffnen Sie in der Sophos Enterprise Console das **Werkzeuge**-Menü und wählen Sie **Reports**.
2. Wählen Sie im Dialogfenster **Reporting** im Drop-Down-Menü den Report-Typ, den Sie erstellen möchten. Konfigurieren Sie in der Registerkarte **Konfiguration** den Report. Klicken Sie auf die Registerkarte **Tabelle**.
3. Es wird die Tabelle angezeigt. Die **Report-Beschreibung** fasst die Kriterien (z. B. den Zeitraum) zusammen, aufgrund derer der Report erstellt wurde.



Konfiguration Tabelle Chart

100% 1 von 1

Name des Unternehmens 02.07.2003 10:27:41

Alarmer nach Zeit

Report-Beschreibung:

Viren mit Namen wie '*' die zwischen 01.06.2003 00:00 und 30.06.2003 23:59 erkannt wurden, auf allen Computern auf täglicher Basis anzeigen.

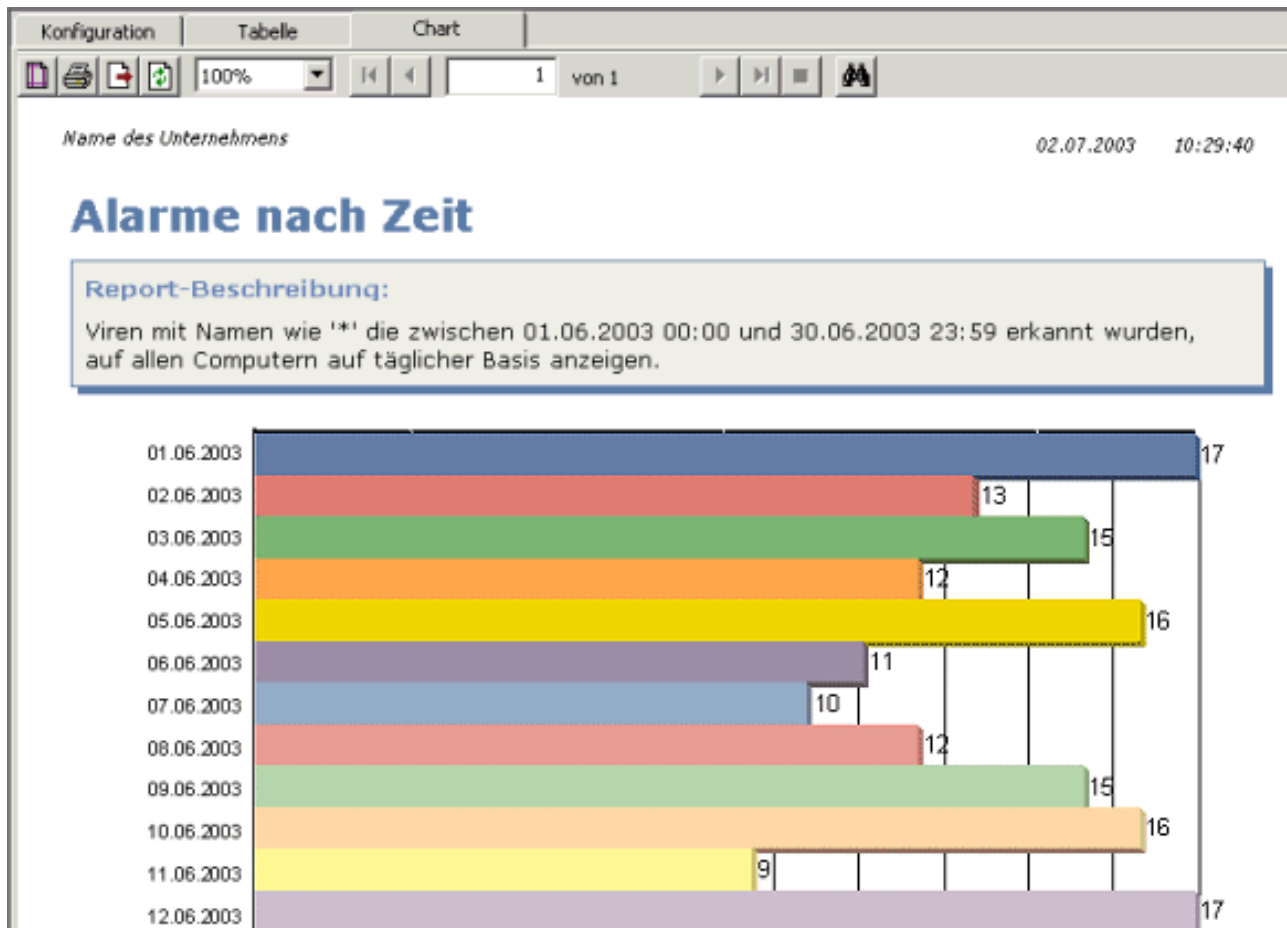
Beginn des Zeitraums	Ende des Zeitraums	Anzahl der Alarme
01.06.2003	02.06.2003	0
02.06.2003	03.06.2003	0
03.06.2003	04.06.2003	0
04.06.2003	05.06.2003	0
05.06.2003	06.06.2003	0
06.06.2003	07.06.2003	0
07.06.2003	08.06.2003	0
08.06.2003	09.06.2003	0
09.06.2003	10.06.2003	0
10.06.2003	11.06.2003	0
11.06.2003	12.06.2003	0
12.06.2003	13.06.2003	0
13.06.2003	14.06.2003	0
14.06.2003	15.06.2003	0
15.06.2003	16.06.2003	0
16.06.2003	17.06.2003	0
17.06.2003	18.06.2003	0
18.06.2003	19.06.2003	0
19.06.2003	20.06.2003	0
20.06.2003	21.06.2003	0

Einen Report in Form eines Diagramms anzeigen



Für den Report-Typ "Alarminformationen" steht keine Diagramm-Ansicht zur Verfügung.

1. Öffnen Sie in der Sophos Enterprise Console das **Werkzeuge**-Menü und wählen Sie **Reports**.
2. Wählen Sie im Dialogfenster **Reporting** im Drop-Down-Menü den Report-Typ, den Sie erstellen möchten. Konfigurieren Sie in der Registerkarte **Konfiguration** den Report. Klicken Sie auf die Registerkarte **Chart**.
3. Es wird das Diagramm angezeigt. Die **Report-Beschreibung** fasst die Kriterien (z. B. den Zeitraum) zusammen, aufgrund derer der Report erstellt wurde.



Die Anzahl der Alarme pro Virus anzeigen

1. Öffnen Sie in der Sophos Enterprise Console das **Werkzeuge**-Menü und wählen Sie **Reports**.
2. Wählen Sie im Dialogfenster **Reporting** im Drop-Down-Menü **Alarme durch Virus**.
3. In der Registerkarte **Konfiguration** können Sie die nachfolgend erläuterten Optionen auswählen. Wenn Sie damit fertig sind, klicken Sie auf eine der anderen Registerkarten, um sich den Report als Diagramm oder Tabelle anzeigen zu lassen.

The screenshot shows a window titled "Reporting" with a dropdown menu set to "Alarmer durch Virus". Below this are three tabs: "Konfiguration", "Tabelle", and "Chart". The "Konfiguration" tab is active, displaying the title "Alarmer durch Virus".

The "Reporting Zeitraum" section includes a "Zeitraum" dropdown set to "Diesen Monat", and "Start" and "Ende" date/time pickers. The "Start" is set to 01.02.2005 00:00 and the "Ende" is set to 02.02.2005 08:12.

The "Ort" section has two radio buttons: "Computergruppe" (selected) and "Einzelcomputer". The "Computergruppe" dropdown is set to "Alle Computer".

The "Filter" section has three radio buttons: "Alle Alarmer anzeigen" (selected), "Nur ersten Alarm anzeigen" (with an input field for "Einträge"), and "Nur Viren anzeigen mit" (with an input field for "Alarmer und mehr").

The "Geordnet nach" section has a checkbox for "Virename" which is currently unchecked.

Reporting Zeitraum

Klicken Sie im Textfeld **Zeitraum** auf den Drop-Down-Pfeil und wählen Sie einen Zeitraum. Sie können entweder einen festen Zeitraum wählen, z. B. **Letzter Monat**, oder Sie wählen **Benutzerdefiniert** und geben den gewünschten Zeitraum in den Textfeldern **Start** und **Ende** ein.

Ort

Klicken Sie auf **Computergruppe** oder auf **Einzelcomputer**. Klicken Sie dann auf den Drop-Down-Pfeil, um eine Gruppe oder einen Computernamen anzugeben.

Filter

Als Standard listet der Report alle Viren und die Anzahl der Alarmer für jeden Virus auf. Sie können den Report aber auch so konfigurieren, dass er nur Folgendes anzeigt:

- ◆ die x Viren, die die meisten Alarmer verursacht haben (wobei x eine Zahl ist, die Sie angeben) oder

- ◆ Viren, die mehr als eine bestimmte Anzahl Alarme verursacht haben.
- Geordnet nach**

Als Standard listet der Report Viren absteigend nach der Anzahl der Alarme pro Virus auf. Markieren Sie den **Virennamen**, wenn die Viren alphabetisch aufgelistet werden sollen.

Anzahl der Alarme pro Ort anzeigen

1. Öffnen Sie in der Sophos Enterprise Console das **Werkzeuge**-Menü und wählen Sie **Reports**.
2. Wählen Sie im Dialogfenster **Reporting** im Drop-Down-Menü **Alarme pro Ort**.
3. In der Registerkarte **Konfiguration** können Sie die nachfolgend erläuterten Optionen auswählen. Wenn Sie damit fertig sind, klicken Sie auf eine der anderen Registerkarten, um sich den Report als Diagramm oder Tabelle anzeigen zu lassen.

The screenshot shows the 'Reporting' dialog box with the 'Konfiguration' tab selected. The title bar reads 'Reporting'. Below the title bar is a dropdown menu set to 'Alarme pro Ort'. There are three tabs: 'Konfiguration', 'Tabelle', and 'Chart'. The main content area is titled 'Alarme pro Ort' and contains several sections:

- Reporting Zeitraum:** A dropdown menu set to 'Diesen Monat'. Below it are 'Start' and 'Ende' fields. 'Start' is set to '01.02.2005' and '00:00'. 'Ende' is set to '02.02.2005' and '08:15'.
- Ort:** Radio buttons for 'Computer' and 'Gruppe', with 'Gruppe' selected.
- Filter:** Radio buttons for 'Alle Orte anzeigen', 'Nur den ersten anzeigen', and 'Nur Orte anzeigen mit'. The 'Nur Orte anzeigen mit' option has two input fields: 'Einträge' and 'Alarme und mehr'. Below this is a dropdown menu for 'Ort anzeigen, wenn er einen Virus enthält wie:' with 'x' selected.
- Geordnet nach:** A checkbox for 'Ort' which is currently unchecked.

Reporting Zeitraum

Klicken Sie im Textfeld **Zeitraum** auf den Drop–Down–Pfeil und wählen Sie einen Zeitraum. Sie können entweder einen festen Zeitraum wählen, z. B. **Letzter Monat** oder Sie wählen **Benutzerdefiniert** und geben den gewünschten Zeitraum in die Textfelder **Start** und **Ende** ein.

Ort

Klicken Sie auf **Computer**, um sich die Alarme pro Computer oder pro **Gruppe** für jede SAVAdmin–Computergruppe anzeigen zu lassen.

Filter

Als Standard zeigt der Report alle Computer oder Gruppen an (abhängig von der Auswahl unter **Ort**). Sie können den Report aber so konfigurieren, dass er nur Folgendes anzeigt:

- ◆ die x Orte, für die die meisten Alarme verzeichnet wurden (wobei x eine Zahl ist, die Sie angeben) oder
- ◆ die Orte mit mehr als einer bestimmten Anzahl Alarmen.

Sie können den Report auch so konfigurieren, dass nur Orte angegeben werden, die einen bestimmten Virus oder bestimmte Viren gemeldet haben. Um einen einzelnen Virus anzugeben, klicken Sie auf den Drop–Down–Pfeil und klicken dort auf den Virennamen in der Liste. Um mehr als einen Virus anzugeben, geben Sie unter Verwendung von Platzhaltern einen Namen in das Textfeld ein. Verwenden Sie ? für ein einzelnes Zeichen im Namen und * für eine Folge von mehreren Zeichen. Zum Beispiel spezifiziert W32/* alle Viren, deren Namen mit W32/ beginnen.

Geordnet nach

Als Standard listet der Report die Orte absteigend nach der Anzahl der Alarme pro Ort auf. Markieren Sie den **Ort**, wenn die Viren alphabetisch aufgelistet werden sollen.

Die Häufigkeit von Virenalarmen anzeigen

1. Öffnen Sie in der Sophos Enterprise Console das **Werkzeuge**–Menü und wählen Sie **Reports**.
2. Wählen Sie im Dialogfenster **Reporting** im Drop–Down–Menü **Alarme nach Zeit**.
3. In der Registerkarte **Konfiguration** können Sie die nachfolgend erläuterten Optionen auswählen. Wenn Sie damit fertig sind, klicken Sie auf eine der

anderen Registerkarten, um sich den Report als Diagramm oder Tabelle anzeigen zu lassen.

The screenshot shows the 'Reporting' window with the following configuration:

- Report Title: Alarmer nach Zeit
- Reporting Zeitraum: Zeitraum: Diesen Monat
- Start: 01.02.2005 00:00
- Ende: 02.02.2005 08:15
- Ort: Computergruppe: Alle Computer; Einzelcomputer: TITANIC
- Filter: Nur Viren einbeziehen, wie: *
- Intervalle, in denen die Rate gemessen wird: Tag

Reporting Zeitraum

Klicken Sie im Textfeld **Zeitraum** auf den Drop-Down-Pfeil und wählen Sie einen Zeitraum. Sie können entweder einen festen Zeitraum wählen, z. B. **Letzter Monat** oder Sie wählen **Benutzerdefiniert** und geben den gewünschten Zeitraum in den Textfeldern **Start** und **Ende** ein.

Ort

Klicken Sie auf **Computergruppe** oder auf **Einzelcomputer**. Klicken Sie dann auf den Drop-Down-Pfeil, um eine Gruppe oder einen Computernamen anzugeben.

Filter

Wenn der Report Statistiken nur für einen bestimmten Virus oder eine Virengruppe anzeigen soll, verwenden Sie das Textfeld **Nur Viren einbeziehen, wie**. Um einen einzelnen Virus anzugeben, klicken Sie auf

den Drop–Down–Pfeil und klicken dort auf den Virennamen in der Liste. Um mehr als einen Virus anzugeben, geben Sie unter Verwendung von Platzhaltern einen Namen in das Textfeld ein. Verwenden Sie ? für ein einzelnes Zeichen im Namen und * für eine Folge von mehreren Zeichen. Zum Beispiel spezifiziert W32/* alle Viren, deren Namen mit W32/ beginnen.

Intervalle, in denen die Häufigkeit gemessen wird

Um die Zeitintervalle anzugeben, in denen die Häufigkeit von Virenalarmen gemessen wird, z. B. jede Stunde oder jeden Tag, klicken Sie auf den Drop–Down–Pfeil und wählen ein Intervall aus.

Details von Virenalarmen anzeigen

1. Öffnen Sie in der Sophos Enterprise Console das **Werkzeuge**–Menü und wählen Sie **Reports**.
2. Wählen Sie im Dialogfenster **Reporting** im Drop–Down–Menü **Alarminformationen**.
3. In der Registerkarte **Konfiguration** können Sie die nachfolgend erläuterten Optionen auswählen. Wenn Sie damit fertig sind, klicken Sie auf eine der anderen Registerkarten, um sich den Report als Diagramm oder Tabelle anzeigen zu lassen.

The screenshot shows the 'Reporting' window with the following configuration:

- Alarminformationen: [Dropdown]
- Tabs: Konfiguration | Tabelle
- Section: Alarminformationen
- Reporting Zeitraum:
 - Zeitraum: Diesen Monat
 - Start: 01.02.2005 00:00
 - Ende: 02.02.2005 08:38
- Ort:
 - Computergruppe: Alle Computer
 - Einzelcomputer: TITANIC
- Filter:
 - Nur Viren anzeigen wie: *
- Geordnet nach:
 - Virename:
 - Computername:
 - Gruppenname:
 - Datum und Uhrzeit:

Reporting Zeitraum

Klicken Sie im Textfeld **Zeitraum** auf den Drop-Down-Pfeil und wählen Sie einen Zeitraum. Sie können entweder einen festen Zeitraum wählen, z. B. **Letzter Monat** oder Sie wählen **Benutzerdefiniert** und geben den gewünschten Zeitraum in den Textfeldern **Start** und **Ende** ein.

Ort

Klicken Sie auf **Computergruppe** oder auf **Einzelcomputer**. Klicken Sie dann auf den Drop-Down-Pfeil, um eine Gruppe oder einen Computernamen anzugeben.

Filter

Wenn der Report Statistiken nur für einen bestimmten Virus oder eine Virengruppe anzeigen soll, verwenden Sie das Textfeld **Nur Viren einbeziehen, wie**. Um einen einzelnen Virus anzugeben, klicken Sie auf den Drop-Down-Pfeil und klicken dort auf den Virennamen in der Liste. Um mehr als einen Virus anzugeben, geben Sie unter Verwendung von Platzhaltern einen Namen in das Textfeld ein. Verwenden Sie ? für ein

einzelnes Zeichen im Namen und * für eine Folge von mehreren Zeichen. Zum Beispiel spezifiziert W32/* alle Viren, deren Namen mit W32/ beginnen.

Geordnet nach

Als Standard sind die Alarminformationen nach dem **Virennamen** geordnet. Reports können aber auch nach den **Computernamen**, den **Gruppennamen** oder nach **Datum und Uhrzeit** geordnet werden.

Einen Report ausdrucken

Um einen Report auszudrucken, klicken Sie auf das **Drucker**-Symbol in der Werkzeugleiste im oberen Bereich des Reports.



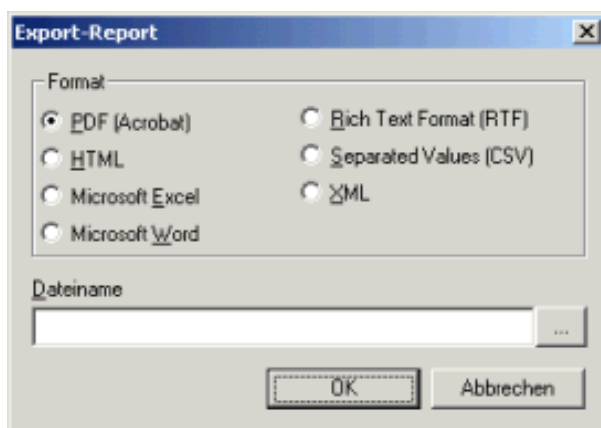
Einen Report in eine Datei exportieren

So exportieren Sie einen Report in eine Datei:

1. Klicken Sie auf das **Export**-Symbol in der Werkzeugleiste im oberen Bereich des Reports.



2. Wählen Sie im Dialogfenster **Export-Report** das Dokumentenformat oder Tabellenformat, in das Sie den Report exportieren möchten. Klicken Sie auf die Schaltfläche **Dateiname**, um einen Speicherort auszuwählen. Geben Sie dann einen Namen ein. Klicken Sie auf **OK**.



Das Report–Layout ändern

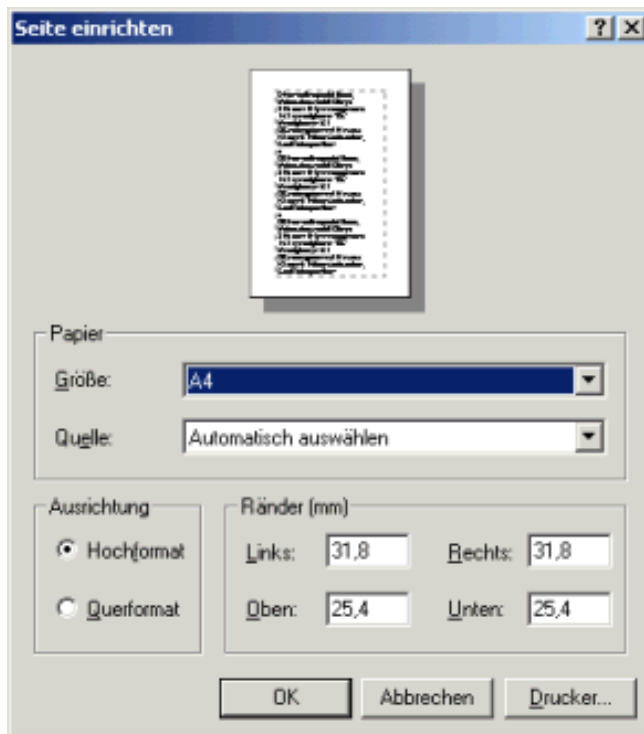
Sie können das Seiten–Layout für die Reports ändern. Sie können sich beispielsweise einen Report im Querformat anzeigen lassen.

1. Klicken Sie auf das Seiten–Layout–Symbol in der Werkzeugleiste im oberen Bereich des Reports.



2. Geben Sie im Dialogfenster **Seite einrichten** die Seitengröße, die Ränder und die Ausrichtung an. Klicken Sie auf **OK**. Der Report wird nun mit diesen Seiteneinstellungen angezeigt.

Diese Seiteneinstellungen werden auch verwendet, wenn der Report ausgedruckt oder exportiert wird.



Fehlersuche

Dieser Abschnitt erläutert, wie Sie mit Problemen umgehen, die bei der Verwendung von Enterprise Console auftreten können.

- Einstellungen für den Ordner "Nicht zugewiesen" können nicht geändert werden
- Computer im Ordner "Nicht zugewiesen" können nicht geschützt werden
- Computer werden nicht aktualisiert
- Antiviren-Einstellungen werden von Macs nicht übernommen
- Einstellungen der On-Access-Überprüfung werden nicht übernommen
- "Neue Überprüfung" erscheint unerwartet auf Windows 2000/XP
- Mehr Hilfe

Einstellungen für den Ordner "Nicht zugewiesen" können nicht geändert werden

Der Ordner "Nicht zugewiesen" ist nur für Computer vorgesehen, die noch keiner Gruppe zugeordnet sind. Sie können seine Einstellungen nicht ändern ("Richtlinien" erstellen) oder Computer in diesem Ordner schützen.

Erstellen Sie Ihre eigene Gruppe oder Gruppen und erstellen Sie dann für diese Richtlinien.

Computer im Ordner "Nicht zugewiesen" können nicht geschützt werden

Der Ordner "Nicht zugewiesen" ist nur für Computer vorgesehen, die noch keiner Gruppe zugeordnet sind. Sie können keine Computer vor Viren schützen, solange sie sich nicht in einer anderen Gruppe befinden.

Computer werden nicht aktualisiert

Wenn sich Computer nicht aktualisieren, sollten Sie überprüfen, ob:

- sie die neuesten Updates von Sophos herunterladen. Klicken Sie auf das **Libraries**-Symbol in der Werkzeuggeste, um Sophos EM Library zu öffnen und prüfen Sie, ob der Download korrekt eingerichtet ist.
- die Gruppe, in der sich die Computer befinden, eine "Update-Richtlinie" haben. Klicken Sie mit der rechten Maustaste auf die Gruppe, wählen Sie **Update-Richtlinie einrichten** und prüfen Sie, ob diese Richtlinie für jeden Computertyp eingerichtet wurde.

- sich die Computer über einen Proxyserver aktualisieren können, sofern einer verwendet wird. Klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie **Update-Richtlinie einrichten**, wählen Sie den Computertyp und klicken Sie dann in der Registerkarte **Primary Server** auf **Proxy-Details**.

Antiviren-Einstellungen werden von Macs nicht übernommen

Manche Antiviren-Einstellungen können von Macintosh-Computern nicht übernommen werden. In diesem Fall wird auf dieser Seite eine Warnung angezeigt.

Sie können die Antiviren-Einstellungen auf Macintosh-Computern mit einem anderen Sophos-Tool ändern, mit dem Mac Update Manager.

Einstellungen der On-Access-Überprüfung werden nicht übernommen

Bei Windows NT, 95, 98 und Me Computern haben Änderungen bestimmter Einstellungen auf den Einstellungen-Seiten für die On-Access-Überprüfung keine Auswirkungen. In den entsprechenden Seiten wird eine Warnung darüber angezeigt.

In diesem Fall wirken sich Änderungen, die Sie in den Einstellungen-Seiten für zeitgesteuerte Überprüfungen vornehmen, auf die zeitgesteuerte und die On-Access-Überprüfung aus. Der Grund dafür liegt im Design von Sophos Anti-Virus für diese früheren Windows-Versionen.

Neue Überprüfung erscheint unerwartet auf Windows 2000/XP

Wenn Sie sich die lokale Kopie von Sophos Anti-Virus auf Windows 2000/XP-Computern anschauen, sehen Sie möglicherweise eine neue "Verfügbare Überprüfung" in der Liste, auch wenn der Benutzer gar keine erstellt hat.

Diese neue Überprüfung ist eigentlich eine zeitgesteuerte Überprüfung, die Sie von der Konsole aus eingerichtet haben. Diese Überprüfung sollten Sie nicht löschen.

Mehr Hilfe

Für weitere Hilfe besuchen Sie

www.sophos.de/support

Technischer Support

Für weitere Informationen über den technischen Support besuchen Sie

www.sophos.de/support

Wenn Sie den technischen Support kontaktieren, geben Sie so viele Informationen wie möglich an, einschließlich Versionsnummern der Sophos Software, Betriebssysteme und Patch-Level und den genauen Wortlaut aller Fehlermeldungen.

Copyright © 2005 by Sophos Plc

Alle Rechte vorbehalten. Kein Teil dieser Publikation darf in jeglicher Form, weder elektronisch oder mechanisch, reproduziert, elektronisch gespeichert oder übertragen werden, noch fotokopiert oder aufgenommen werden, es sei denn Sie haben entweder eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit den Lizenzvereinbarungen reproduziert werden darf oder Sie haben eine schriftliche Genehmigung des Copyright-Inhabers.

Jeder Name gilt als Warenzeichen, sofern nicht anderweitig gekennzeichnet.
InterCheck und *Sophos* sind eingetragene Warenzeichen von Sophos Plc.