Handbuch für Symantec™ Endpoint Protection und Symantec Network Access Control-Client

Handbuch für Symantec Endpoint Protection und Symantec Network Access Control-Client

Die im vorliegenden Handbuch beschriebene Software wird im Rahmen einer Lizenzvereinbarung zur Verfügung gestellt und darf nur im Einklang mit den Bestimmungen dieser Vereinbarung verwendet werden.

Produktversion: 12.1.2

Dokumentationsversion: 12.1.2, Version 1

Rechtlicher Hinweis

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043, USA

http://www.symantec.de

Technischer Support

Der technische Support von Symantec unterhält weltweit Supportcenter. Hauptaufgabe des technischen Supports ist es, bestimmte Anfragen zu Produktmerkmalen und -funktionen zu bearbeiten. Daneben erstellt die Gruppe "Technischer Support" Inhalte für unsere Online-Supportdatenbank. Die Gruppe "Technischer Support" arbeitet mit den anderen Funktionsbereichen von Symantec zusammen, um Ihre Fragen rechtzeitig zu beantworten. So arbeitet diese Gruppe z. B. mit der Produktentwicklung und Symantec Security Response zusammen, um Warnmeldungsdienste und Aktualisierungen der Virendefinitionen zur Verfügung zu stellen.

Folgende Leistungen sind in den Supportangeboten von Symantec enthalten:

- Verschiedene Supportoptionen, die Ihnen die Flexibilität geben, die richtige Anzahl von Diensten für Unternehmen aller Größen auszuwählen
- Telefon- und/oder webbasierter Support, der schnell reagiert und aktuelle Informationen bietet
- Upgrade-Versicherung, die Software-Upgrades liefert
- Globaler Support, der auf Basis regionaler Geschäftszeiten oder rund um die Uhr erworben werden kann
- Erstklassige Serviceangebote einschließlich Account Management Services

Informationen zu den Wartungsprogrammen von Symantec erhalten Sie auf unserer Website unter folgender URL:

www.symantec.com/de/de/business/support/

Alle Support-Dienste werden in Übereinstimmung mit Ihrer Supportvereinbarung und der zu dem Zeitpunkt geltenden technischen Enterprise-Support-Richtlinie bereitgestellt.

Kontaktaufnahmen mit dem technischen Support

Kunden mit einer aktuellen Supportvereinbarung können unter folgender URL auf technische Support-Informationen zugreifen:

http://www.symantec.com/de/de/business/support/

Bevor Sie den technischen Support kontaktieren, stellen Sie sicher, die Systemanforderungen, die in Ihrer Produktdokumentation aufgelistet sind, erfüllt zu haben. Sie sollten auch an dem Computer arbeiten, auf dem das Problem auftrat, falls es notwendig ist, das Problem zu replizieren.

Wenn Sie den technischen Support kontaktieren, halten Sie bitte folgende Informationen bereit:

- Produktversion
- Hardware-Daten
- Verfügbarer Arbeitsspeicher, Speicherplatz und NIC-Informationen
- Betriebssystem
- Version und Patch-Level
- Netzwerktopologie
- Router, Gateway und IP-Adressinformationen
- Problembeschreibung:
  - Fehlermeldungen und Protokolldateien
  - Durchgeführte Fehlerbehebung, vor Kontaktierung von Symantec
  - Aktuelle Software-Konfigurationsänderungen und Netzwerkänderungen

Lizenzierung und Registrierung

Wenn Ihr Symantec-Produkt die Registrierung oder einen Lizenzschlüssel erfordert, konsultieren Sie die Webseite unseres technischen Supports unter folgender URL:

http://www.symantec.com/de/de/business/support/

Kundenservice

Informationen zum Kundenservice sind unter folgender URL verfügbar:

www.symantec.com/de/de/business/support/

Der Kundenservice steht Ihnen bei nicht technischen Fragen zur Verfügung:

- Fragen bezüglich der Produktlizenzierung oder der Serialisierung
- Aktualisierung der Produktregistrierung, z. B. Adress- oder Namensänderungen
- Allgemeine Produktinformationen (Funktionen, verfügbare Sprachen, lokale Händler)
- Aktuelle Informationen zu Produkt-Updates und -Upgrades
- Informationen zu Upgrade-Versicherung und Supportverträgen
- Informationen zu den Symantec Buying Programs
- Hilfe zu den technischen Support-Optionen von Symantec
- Nicht technische Presales-Fragen
- Probleme mit Datenträgern (CD-ROM, DVD) oder Handbüchern

Supportvereinbarungsressourcen

Wenn Sie Symantec bezüglich einer vorhandenen Supportvereinbarung kontaktieren möchten, wenden Sie sich bitte an das für Supportvereinbarungen zuständige Team für Ihre Region:

Asien-Pazifik und Japan	customercare_apac@symantec.com
Europa, Naher Osten und Afrika	semea@symantec.com
Nordamerika und Lateinamerika	supportsolutions@symantec.com

Inhalt

Kapitel 1

Erste Schritte mit dem Client

In diesem Kapitel werden folgende Themen behandelt:

Info über den Symantec Endpoint Protection-Client

Der Symantec Endpoint Protection-Client kombiniert mehrere Schutzschichten, um Ihren Computer proaktiv vor bekannten und unbekannten Bedrohungen bzw. Netzwerkbedrohungen zu schützen.

Tabelle 1-1 beschreibt jede Schutzschicht.

Tabelle 1-1 Schutztypen

Schicht	Beschreibung
Viren- und Spyware-Schutz	Virus and Spyware Protection bekämpft eine Vielfalt von Bedrohungen, einschließlich Spyware, Würmer, Trojaner, Rootkits und Adware. Dateisystem-Auto-Protect prüft ununterbrochen alle Dateien auf Viren und Sicherheitsrisiken. Internet-E-Mail-Auto-Protect scannt die eingehenden und ausgehenden E-Mail-Nachrichten, die das POP3- oder SMTP-Kommunikationsprotokoll verwenden. "Microsoft Outlook Auto-Protect" scannt die eingehend und ausgehenden Microsoft Outlook-E-Mails. Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58.
Proaktiver Bedrohungsschutz	Die proaktive Bedrohungstechnologie umfasst SONAR, das Echtzeitschutz gegen neuartige Angriffe anbietet. SONAR kann Angriffe stoppen, sogar bevor traditionelle signaturbasierte Definitionen eine Bedrohung erkennen. SONAR verwendet Heuristiken sowie Dateireputationsdaten, um Entscheidungen über Anwendungen oder Dateien zu treffen. Siehe "Verwalten von SONAR auf Ihrem Clientcomputer" auf Seite 104.
Netzwerkbedrohungsschutz	Netzwerkbedrohungsschutz umfasst eine Firewall und ein Angriffsschutzsystem. Die richtlinienbasierte Firewall hindert nicht autorisierte Benutzer am Zugriff auf Ihren Computer. Das Intrusion Prevention-System erkennt und blockiert Netzwerkangriffe automatisch. Siehe "Verwalten des Firewall-Schutzes" auf Seite 107.

Ihr Administrator legt fest, welche Schutztypen der Management-Server auf Ihren Clientcomputer herunterladen soll. Der Client lädt automatisch die Virendefinitionen, IPS-Definitionen und Produkt-Updates auf Ihren Computer herunter. Benutzer, die mit tragbaren Computern reisen, können Virendefinitionen und Produkt-Updates direkt von LiveUpdate abrufen.

Siehe "Aktualisieren des Computerschutzes" auf Seite 41.

Info über den Symantec Network Access Control-Client

Der Symantec Network Access Control-Client bewertet, ob ein Computer geschützt ist und den Sicherheitsrichtlinien entspricht, bevor er eine Verbindung mit dem Unternehmensnetzwerk herstellen kann.

Der Client stellt sicher, dass Ihr Computer mit den Sicherheitsrichtlinien übereinstimmt, die Ihr Administrator konfiguriert hat. Anhand der Sicherheitsrichtlinien wird überprüft, ob auf dem Computer die aktuellste

Sicherheitssoftware ausgeführt wird (Virenschutz- und Firewall-Anwendungen). Wenn auf Ihrem Computer nicht die erforderliche Software ausgeführt wird, müssen Sie die Software manuell aktualisieren oder Ihr Client aktualisiert möglicherweise die Software automatisch. Solange Ihre Sicherheitssoftware nicht aktuell ist, wird Ihr Computer evtl. beim Herstellen einer Verbindung zum Netzwerk blockiert. Der Client führt regelmäßige Prüfungen aus, um sicherzustellen, dass Ihr Computer den aktuellen Sicherheitsrichtlinien entspricht.

Siehe "Wie Symantec Network Access Control funktioniert" auf Seite 133.

Erste Schritte auf der Status-Seite

Wenn Sie den Client öffnen, werden das Hauptfenster und die Seite "Status" angezeigt.

Tabelle 1-2 zeigt die Hauptaufgaben an, die Sie von der Menüleiste aus auf der linken Seite durchführen können.

Tabelle 1-2 Client-Hauptfenster

Klicken Sie auf diese Option	um diese Aufgaben auszuführen
Status	Prüfen Sie, ob der Computer geschützt und ob seine Lizenz aktuell ist. Die Farben und Warnsymbole auf der Status-Seite zeigen Ihnen, welche Technologien aktiviert sind und den Client schützen. Siehe "Warnsymbole auf der Status-Seite" auf Seite 17. Sie können Folgendes tun: ■ Aktivieren Sie oder deaktivieren Sie eine oder mehrere Schutztechnologien, wenn Ihr Administrator damit einverstanden ist. Siehe "Info zum Aktivieren und das Deaktivieren des Schutzes, wenn Sie Probleme beheben müssen" auf Seite 50. ■ Prüfen, ob Sie die neuesten Definitionsdateien für Viren- und Spyware-Schutz, proaktiven Bedrohungsschutz und Netzwerkbedrohungsschutz haben. ■ Ausführen eines Active Scan. Siehe "Sofortiges Scannen Ihres Computers" auf Seite 23. ■ Zeigen Sie die Liste der Bedrohungen und die Ergebnisse des letzten Viren- und Spyware-Scans an.

Klicken Sie auf diese Option	um diese Aufgaben auszuführen
Scannen auf Bedrohungen	■ Führen Sie einen Active Scan oder einen vollständigen Scan aus. Siehe "Sofortiges Scannen Ihres Computers" auf Seite 23. ■ Erstellen Sie einen neuen Scan, der zu einem bestimmten Zeitpunkt, Systemstart oder nach Bedarf ausgeführt wird. Siehe "Planen eines benutzerdefinierten Scans" auf Seite 73. Siehe "Einen Scan planen, der nach Bedarf oder beim Starten des Computers ausgeführt werden soll" auf Seite 77. ■ Führen Sie eine Hostintegritätsprüfung aus, wenn Sie Symantec Network Access Control installiert haben. Siehe "Ausführen einer Host-Integritätsprüfung" auf Seite 136.
Einstellungen ändern	Konfigurieren der Einstellungen für die folgenden Schutztechnologien und Funktionen: ■ Aktivieren und konfigurieren der Auto-Protect-Einstellungen. Siehe "Anpassen von Virus- und Spyware-Scan-Einstellungen" auf Seite 82. ■ Konfigurieren der Firewall-Einstellungen und der Intrusion Prevention-Systemeinstellungen. Siehe "Verwalten des Firewall-Schutzes" auf Seite 107. ■ Anzeigen und Hinzufügen von Scanausnahmen. Siehe "Ausschließen von Elementen von Scans" auf Seite 91. ■ Anzeigen des Benachrichtigungsbereichssymbols. Siehe "Ermitteln, ob der Client eine Verbindung hergestellt hat und geschützt ist" auf Seite 44. ■ Konfigurieren der Manipulationsschutzeinstellungen. Siehe "Manipulationsschutz aktivieren, deaktivieren und konfigurieren" auf Seite 55. ■ Erstellen eines Zeitplans, um Content- und Produkt-Updates auf den Client herunterzuladen. Siehe "Aktualisieren des Inhalts in geplanten Abständen" auf Seite 43. Siehe "Verwalten des Schutzes Ihres Computers" auf Seite 39.
Quarantäne anzeigen	Anzeigen der Viren und Sicherheitsrisiken, die der Client erkannt und isoliert hat. Sie können Dateien in der Quarantäne wiederherstellen, löschen, bereinigen, exportieren und hinzufügen. Siehe "Isolieren von Dateien" auf Seite 95.
Protokolle anzeigen	Zeigen Sie beliebige Client-Protokolle an. Siehe "Anzeigen von Protokollen" auf Seite 48.

Klicken Sie auf diese Option	um diese Aufgaben auszuführen
LiveUpdate	Sofortiges Ausführen von LiveUpdate. LiveUpdate lädt die neuesten Content-Definitionen und Produkt-Updates von einem Management-Server herunter, der sich innerhalb des Netzwerks Ihres Unternehmens befindet. Siehe "Sofortiges Aktualisieren des Inhalts" auf Seite 42.

Über verwaltete Clients und nicht-verwaltete Clients

Ihr Administrator kann den Client entweder als verwalteten Client (vom Administrator verwaltete Installation) oder nicht-verwalteten Client (Einzelplatzinstallation) installieren.

Tabelle 1-3 Unterschiede zwischen einem verwalteten und einem nicht-verwalteten Client

Client-Typ	Beschreibung
Verwalteter Client	Ein verwalteter Client kommuniziert mit einem Management-Server in Ihrem Netzwerk. Der Administrator konfiguriert die Schutz- und Standardeinstellungen, während der Management-Server die Einstellungen auf den Client herunterlädt. Wenn der Administrator eine Änderung am Schutz vornimmt, wird die Änderung umgehend auf den Client heruntergeladen. Administratoren können die Stufe, auf der Sie mit dem Client kommunizieren, folgendermaßen ändern: ■ Der Administrator verwaltet den Client vollständig. Sie müssen den Client nicht konfigurieren. Alle Einstellungen sind gesperrt oder nicht verfügbar, aber Sie können Informationen darüber anzeigen, was der Client auf Ihrem Computer tut. ■ Der Administrator verwaltet den Client, aber Sie können einige Clienteinstellungen ändern und einige Aufgaben durchführen. Beispielsweise sind Sie möglicherweise in der Lage, Ihre eigenen Scans auszuführen und Client-Updates und Schutz-Updates manuell abzurufen. Die Verfügbarkeit der Client-Einstellungen sowie die Werte der Einstellungen selbst können sich regelmäßig ändern. Beispielsweise könnte sich eine Einstellung ändern, wenn Ihr Administrator die Richtlinie aktualisiert, die Ihren Clientschutz steuert. ■ Der Administrator verwaltet den Client, aber Sie können alle Clienteinstellungen ändern und alle Schutzaufgaben durchführen.

Client-Typ	Beschreibung
Nicht-verwalteter Client	Ein nicht-verwalteter Client kommuniziert nicht mit einem Management-Server und kein Administrator verwaltet den Client. Ein nicht-verwalteter Client kann einer der folgenden Typen sein: ■ Ein Einzelplatzcomputer, der nicht mit einem Netzwerk verbunden ist, z. B. ein Heimcomputer oder ein Laptop. Der Computer muss eine Symantec Endpoint Protection-Installation enthalten, die entweder die Standard-Optionseinstellungen oder Voreinstellungen des Administrators verwendet. ■ Ein mit dem Unternehmensnetzwerk verbundener Remote-Computer, der vor dem Herstellen einer Verbindung die Sicherheitsanforderungen erfüllen muss. Auf dem Client sind die Standardeinstellungen eingerichtet, wenn er zum ersten Mal installiert wurde. Nachdem der Client installiert ist, können Sie alle Clienteinstellungen ändern und alle Schutzaufgaben durchführen.

Tabelle 1-4 beschreibt die Unterschiede bezüglich der Benutzeroberfläche zwischen einem verwalteten und einem nicht verwalteten Client.

Tabelle 1-4 Unterschiede zwischen einem verwalteten Client und einem nicht-verwalteten Client nach Funktionsbereich

Funktionsbereich	Zentral verwalteter Client	Selbst verwalteter Client
Viren- und Spyware-Schutz	Der Client zeigt eine gesperrte Vorhängeschloss-Option an und diejenigen Optionen, die Sie nicht konfigurieren können, werden abgeblendet angezeigt.	Der Client zeigt weder ein gesperrtes noch ein entsperrtes Vorhängeschloss an.
Proaktiver Bedrohungsschutz	Der Client zeigt eine gesperrte Vorhängeschloss-Option an und diejenigen Optionen, die Sie nicht konfigurieren können, werden abgeblendet angezeigt.	Der Client zeigt weder ein gesperrtes noch ein entsperrtes Vorhängeschloss an.
Einstellungen für Client Management und Netzwerkbedrohungsschutz	Die Einstellungen, die der Administrator festlegt, werden nicht angezeigt.	Alle Einstellungen werden angezeigt.

Siehe "Prüfen, ob der Client verwaltet oder nicht verwaltet ist" auf Seite 17.

Prüfen, ob der Client verwaltet oder nicht verwaltet ist

Um zu prüfen, wie viel Kontrolle Sie zum Konfigurieren des Schutzes auf Ihrem Client haben, prüfen Sie zuerst, ob Ihr Client verwaltet oder nicht verwaltet wird. Sie können mehr Einstellungen auf einem nicht verwalteten Client als auf einem verwalteten Client konfigurieren.

Siehe "Über verwaltete Clients und nicht-verwaltete Clients" auf Seite 15.

So überprüfen Sie, ob der Client verwaltet oder nicht verwaltet ist

1. Klicken Sie auf der Seite "Status" auf "Hilfe" > "Fehlerbehebung".
2. Klicken Sie im Dialogfeld "Fehlerbehebung" auf "Management".
3. Suchen Sie im Fenster "Management" unter "Allgemeine Informationen" neben "Server" nach den folgenden Informationen:
   - Wenn der Client verwaltet wird, wird im Feld "Server" entweder die Adresse des Management-Servers oder der Text "Offline" angezeigt. Bei der Adresse kann es sich um eine IP-Adresse, einen DNS-Namen oder NetBIOS-Namen handeln. Beispielsweise könnte ein DNS-Name SEPMServer1 lauten. Wenn der Client verwaltet wird, aber derzeit keine Verbindung zu einem Management-Server hergestellt ist, steht in diesem Feld "Offline".
   - Wenn der Client nicht verwaltet wird, wird im Feld "Server" die Option "Selbstverwaltet" angezeigt.
4. Klicken Sie auf "Schließen".

Warnsymbole auf der Status-Seite

Oben auf der Status-Seite werden verschiedene Warnsymbole angezeigt, um auf den Schutzstatus des Computers hinzuweisen.

Tabelle 1-5 Warnsymbole auf der Status-Seite

Symbol	Beschreibung
	Zeigt an, dass jeder Schutz aktiviert ist.

Symbol	Beschreibung
	Warnt Sie, dass die Virendefinitionen auf dem Client-Computer veraltet sind. Um die neuesten Virendefinitionen zu erhalten, können Sie LiveUpdate sofort ausführen, wenn Ihr Administrator damit einverstanden ist. Auf dem Symantec Network Access Control-Clientcomputer können folgende Probleme auftreten: ■ Auf dem Client-Computer schlug die Prüfung auf Einhaltung von Sicherheitsrichtlinien der Host-Integrität fehl. Prüfen Sie das Clientverwaltungssicherheitsprotokoll, um herauszufinden, was für das Bestehen der Prüfung erforderlich ist. ■ Es ist keine Host-Integrität hergestellt. Siehe "Aktualisieren des Computerschutzes" auf Seite 41.
	Zeigt an, dass eine oder mehrere Schutzlösungen deaktiviert sind oder dass der Client eine abgelaufene Lizenz aufweist. Um den Schutz zu aktivieren, klicken Sie auf "Beheben" oder "Alle beheben". Siehe "Info zum Aktivieren und das Deaktivieren des Schutzes, wenn Sie Probleme beheben müssen" auf Seite 50. Siehe "Aktivieren oder Deaktivieren des Schutzes auf dem Client-Computer" auf Seite 52.

Wie kann ich meinen Computer mit Symantec Endpoint Protection schützen?

Die Standardeinstellungen im Symantec Endpoint Protection-Client schützen Ihren Computer vor vielen Arten von Malware. Entweder handhabt der Client die Malware automatisch, oder er lässt Sie über die Vorgehensweise entscheiden.

Sie können prüfen, ob Ihr Computer infiziert ist und einige zusätzliche Aufgaben ausführen, wenn Ihnen die Sicherheit oder Leistung nicht ausreicht.

Hinweis: Auf verwalteten Clients werden einige Optionen nicht angezeigt, wenn Ihr Administrator sie entsprechend konfiguriert hat. Auf nicht verwalteten Clients werden die meisten Optionen angezeigt.

Tabelle 1-6 Häufig gestellte Fragen zum Schutz Ihres Computers

Frage	Beschreibung
Wie erkenne ich, ob mein Computer geschützt ist?	Dies wird Ihnen in der Clientkonsole oben auf Seite "Status" angezeigt. Farbe und Art des Warnsymbols zeigen den Schutzstatus Ihres Computers an. Weitere Informationen finden Sie im Teilfenster "Status" oder unter "Details". Siehe "Warnsymbole auf der Status-Seite" auf Seite 17. Siehe "Ermitteln, ob der Client eine Verbindung hergestellt hat und geschützt ist" auf Seite 44.
Wie erkenne ich, dass mein Computer infiziert ist?	Ist Ihr Computer infiziert, wird möglicherweise eine der folgenden Meldungen angezeigt: ■ Auto-Protect-Erkennung oder manuelle Scanerkennung. Diese Meldungen beschreiben die Bedrohung und die Aktion, die daraufhin ausgeführt wurde. Sie können zwischen mehreren Optionen für die Behandlung der Bedrohung wählen. Sie können die ausgewählte Aktion entweder entfernen, bereinigen, ausschließen, löschen oder rückgängig machen. Sie können den Scan auch anhalten, wenn Ihr Administrator dies zugelassen hat. Siehe "Reaktion auf eine Viren- oder Sicherheitsrisikoerkennung" auf Seite 30. Siehe "Info zu Scanergebnissen" auf Seite 29. Siehe "Unterbrechung und Verschiebung von Scans" auf Seite 24. ■ Eine Download Insight-Erkennung. Dieses Fenster enthält Informationen zu bösartigen und nicht eindeutigen Dateien, die Download Insight beim Herunterladen erkennt. Siehe "Reagieren auf Download Insight-Meldungen, in denen Sie gefragt werden, ob Sie die heruntergeladenen Dateien blockieren oder zulassen möchten" auf Seite 33. Siehe "Typen von Warnmeldungen und Benachrichtigungen" auf Seite 27.
Wie bereinige ich meinen infizierten Computer?	Wenn ein Scanfenster angezeigt wird, hat Ihr Administrator bereits festgelegt, dass Ihr Computer auf die Infektion reagiert. Sie können eventuell eine Aktion auswählen. Wenn Sie wissen, dass eine Datei infiziert ist, klicken Sie auf "Bereinigen" oder "Quarantäne". Stellen Sie für geplante Scans und Auto-Protect sicher, dass als Hauptaktion "Risiko bereinigen" und als sekundäre Aktion "Risiko in Quarantänebereich" oder "Löschen" festgelegt ist. Siehe "Reaktion auf eine Viren- oder Sicherheitsrisikoerkennung" auf Seite 30. Siehe "Funktionsweise von Viren- und Spyware-Scans" auf Seite 62. Siehe "Konfigurieren von Aktionen für Malware- und Sicherheitsrisikoerkennungen" auf Seite 84.

Frage	Beschreibung
Wie erhöhe ich die Sicherheit meines Computers?	Standardmäßig ist Ihr Clientcomputer maximal geschützt. Ihr Administrator hat möglicherweise einige Sicherheitseinstellungen des Clients geändert, um die Leistung des Clients zu verbessern. Ihr Administrator hat Ihnen eventuell auch ermöglicht, die Schutzeinstellungen Ihres eigenen Computers zu ändern. Wenn Sie diese Einstellungen ändern können, können Sie die folgenden Aufgaben ausführen: ■ Planen Sie regelmäßige vollständige Scans, normalerweise einmal täglich oder einmal wöchentlich. Siehe "Planen eines benutzerdefinierten Scans" auf Seite 73. ■ Lassen Sie Viren- und Spyware-Scans, Auto-Protect, SONAR, Intrusion Prevention und Insight jederzeit installiert und aktiviert und stellen Sie sicher, dass sie immer auf dem neuesten Stand sind. Siehe "Info zum Aktivieren und das Deaktivieren des Schutzes, wenn Sie Probleme beheben müssen" auf Seite 50. Siehe "Aktivieren oder Deaktivieren des Schutzes auf dem Client-Computer" auf Seite 52. Siehe "Aktivieren oder Deaktivieren von Auto-Protect" auf Seite 54. Auf einem nicht verwalteten Client können Sie die folgenden Aufgaben ausführen: ■ Laden Sie die richtigen Virendefinitionen mit LiveUpdate herunter und installieren Sie sie. Standardmäßig erhält Ihr Clientcomputer zweimal täglich die neuesten Virendefinitionen. Sie können die neuesten Definitionen jedoch auch selbst herunterladen. Siehe "Sofortiges Aktualisieren des Inhalts" auf Seite 42. ■ Führen Sie einen vollständigen Scan Ihres Computers mit allen aktivierten Scanverbesserungen aus. Standardmäßig wird jede Woche ein vollständiger Scan Ihres Computers ausgeführt. Sie können einen Scan jedoch jederzeit ausführen. Siehe "Planen eines benutzerdefinierten Scans" auf Seite 73. Siehe "Sofortiges Scannen Ihres Computers" auf Seite 23.

Frage	Beschreibung
Wie ändere ich meine Scaneinstellungen, wenn der Scan meine Arbeit verlangsamt?	Wenn Scans Ihren Computer verlangsamen, passen Sie die folgenden Einstellungen an: ■ Legen Sie fest, dass LiveUpdate die neuesten Virendefinitionen seltener oder dann herunterlädt, wenn Sie den Computer nicht verwenden. Siehe "Aktualisieren des Inhalts in geplanten Abständen" auf Seite 43. ■ Erstellen Sie einen geplanten vollständigen Scan, der außerhalb der Geschäftszeiten ausgeführt wird, oder wenn Sie den Computer nicht verwenden. Siehe "Planen eines benutzerdefinierten Scans" auf Seite 73. ■ Schließen Sie die Anwendungen und Dateien aus, die nicht gescannt werden müssen. Siehe "Ausschließen von Elementen von Scans" auf Seite 91. ■ Begrenzen Sie geplante Scans, Auto-Protect und Download-Insight auf Scandateierweiterungen für die Dateitypen, die häufig infiziert sind. Legen Sie beispielsweise fest, dass der Scan nach ausführbaren Dateien wie EXE, COM, BAT und VBS sucht. ■ Deaktivieren Sie in Auto-Protect die Option "Auf Sicherheitsrisiken scannen". Siehe "Anpassen von Virus- und Spyware-Scan-Einstellungen" auf Seite 82. **Warnung:** Sie können Auto-Protect deaktivieren, um die Leistung des Clientcomputers zu verbessern oder Probleme auf dem Client zu beheben. Jedoch empfiehlt Symantec, dass Sie Auto-Protect immer aktiviert lassen. Siehe "Aktivieren oder Deaktivieren von Auto-Protect" auf Seite 54. ■ Deaktivieren Sie die Scanverbesserungsoptionen in einem Active Scan, einem vollständigen Scan oder einem benutzerdefinierten Scan. Siehe "Planen eines benutzerdefinierten Scans" auf Seite 73. ■ Deaktivieren Sie Download Insight und die Insight-Suche. Siehe "Anpassen der Download Insight-Einstellungen" auf Seite 81. Siehe "Senden von Informationen über Erkennungen an Symantec Security Response" auf Seite 100. **Hinweis:** Sie können diese Einstellungen möglicherweise nicht ändern, wenn Ihr Administrator sie entsprechend konfiguriert hat.

Frage	Beschreibung
Was kann ich tun, wenn die Firewall das Surfen im Internet verhindert?	Standardmäßig blockiert die Firewall nicht den Zugriff auf das Internet. Wenn Sie nicht auf das Internet zugreifen können, wenden Sie sich an Ihren Administrator. Ihr Administrator blockiert möglicherweise den Zugriff auf bestimmte Websites oder lässt nicht zu, dass Ihr Computer auf einen bestimmten Browser zugreift. Sie verfügen eventuell über die erforderlichen Berechtigungen, um die Firewall-Regeln zu ändern. Auf einem nicht verwalteten Client können Sie die Firewall-Regeln ändern. Jedoch sollten Sie eine Firewall-Regel nicht ändern oder hinzufügen, bis Sie wissen, ob der von der Firewall-Regel blockierte Datenverkehr bösartig ist. Bevor Sie die Firewall-Regel ändern, stellen Sie folgende Fragen: ■ Ist die Webanwendung, die auf das Internet zugreift, legitim? ■ Greift die Webanwendung auf die richtigen Remote-Ports zu? HTTP-Datenverkehr ist legitimer Datenverkehr für Webanwendungen und HTTP-Datenverkehr verwendet TCP-Port 80 und 443. Sie können möglicherweise Datenverkehr von anderen Ports nicht vertrauen. ■ Ist die IP-Adresse der Website, auf die die Anwendung zugreift, richtig oder legitim?
Welche Aktionen nehme ich vor, wenn eine Meldung im Benachrichtigungsbereich angezeigt wird?	Lesen Sie die Meldung im Benachrichtigungsbereich auf der Symbolleiste. Die Benachrichtigungen informieren Sie über eines der folgenden Dinge: ■ Ihr Computer wurde möglicherweise angegriffen und der Client hat die Bedrohung behandelt. ■ Ihr Computer hat eine neue Sicherheitsrichtlinie erhalten. Die Sicherheitsrichtlinie wird automatisch aktualisiert. Sie können Ihre Sicherheitsrichtlinie auch jederzeit aktualisieren. Siehe "Manuelles Aktualisieren von Richtlinien auf dem Client" auf Seite 44. Siehe "Reaktion auf eine Viren- oder Sicherheitsrisikoerkennung" auf Seite 30. Siehe "Reaktion auf Meldungen, in denen Sie gefragt werden, ob eine Anwendung zugelassen oder blockiert werden soll" auf Seite 35. Weitere Informationen finden Sie je nach Bedrohungstyp in einem der Protokolle. Siehe "Anzeigen von Protokollen" auf Seite 48.

Siehe "Über verwaltete Clients und nicht-verwaltete Clients" auf Seite 15.

Siehe "Prüfen, ob der Client verwaltet oder nicht verwaltet ist" auf Seite 17.

Siehe "Verwalten des Schutzes Ihres Computers" auf Seite 39.

Sofortiges Scannen Ihres Computers

Sie können jederzeit manuell auf Viren und Sicherheitsrisiken scannen. Sie sollten Ihren Computer sofort scannen, wenn Sie vor kurzem den Client installiert haben, oder wenn Sie glauben, vor kurzem einen Virus oder ein Sicherheitsrisiko erhalten zu haben.

Wählen Sie hierzu eine einzelne Datei, eine Diskette oder Ihren gesamten Computer aus. Scans auf Anforderung umfassen den Active Scan und den vollständigen Scan. Außerdem können Sie einen benutzerdefinierten Scan erstellen, der auf Anforderung ausgeführt wird.

Siehe "Einen Scan planen, der nach Bedarf oder beim Starten des Computers ausgeführt werden soll" auf Seite 77.

Siehe "Aktualisieren des Computerschutzes" auf Seite 41.

Um weitere Informationen zu den Optionen in jedem Dialogfeld zu erhalten, klicken Sie auf "Hilfe".

So scannen Sie Ihren Computer sofort

- Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie im Client auf der Seite "Status" neben "Viren- und Spyware-Schutz" auf "Optionen" > "Active Scan ausführen".
  - Klicken Sie in der Seitenleiste des Clients auf "Scannen auf Bedrohungen". Führen Sie einen der folgenden Schritte aus:
    - Klicken Sie auf "Active Scan ausführen".
    - Klicken Sie auf "Vollständigen Scan ausführen".
    - In der Scanliste klicken Sie mit der rechten Maustaste auf einen beliebigen Scan und klicken dann auf "Jetzt scannen".
      Der Scan wird gestartet.
      Sie können den Scanstatus anzeigen, es sei denn, Ihr Administrator hat die Option deaktiviert. Um den Scanstatus anzuzeigen, klicken Sie auf den Meldungslink, der für den aktuellen Scan erscheint: *Scan* wird durchgeführt.
      Siehe "Info zu Scanergebnissen" auf Seite 29.

  Sie können den Scan auch anhalten oder abbrechen.

  Siehe "Unterbrechung und Verschiebung von Scans" auf Seite 24.

So scannen Sie Ihren Computer in Windows

- Klicken Sie im Fenster "Arbeitsplatz" oder im Windows Explorer mit der rechten Maustaste auf eine Datei, einen Ordner oder ein Laufwerk und wählen Sie "Suche nach Viren".

  Diese Funktion wird auf 32-Bit- und 64-Bit-Betriebssystemen unterstützt.

Hinweis: Die Insight-Suche scannt keinen Ordner oder kein Laufwerk, wenn Sie diesen Scantyp durchführen. Sie wird nicht ausgeführt, wenn Sie eine zu scannende Datei oder eine zu scannende Gruppe von Dateien auswählen.

Unterbrechung und Verschiebung von Scans

Die Option "Unterbrechen" bietet Ihnen die Möglichkeit, einen Scanvorgang zu einem beliebigen Zeitpunkt zu unterbrechen und die Ausführung später fortzusetzen. Sie können alle Scanvorgänge unterbrechen, die Sie selbst gestartet haben.

Ihr Administrator legt fest, ob Sie einen ob Sie von ihm geplante Scans unterbrechen können. Falls die Option "Scan unterbrechen" nicht verfügbar ist, hat Ihr Administrator die Funktion deaktiviert. Wenn eine der Verschiebungsfunktionen aktiviert ist, haben Sie die Möglichkeit, den Ausführungsbeginn um eine vorgegebene Zeitspanne zu verzögern.

Wenn ein Scan fortgesetzt wird, startet er dort wo er unterbrochen wurde.

Hinweis: Wenn Sie einen Scan unterbrechen, während der Client eine komprimierte Datei scannt, kann es einige Minuten dauern, bis der Client auf die Unterbrechungsanfrage reagiert.

Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58.

So unterbrechen Sie einen gestarteten Scan

1. Wenn der Scan ausgeführt wird, klicken Sie im Dialogfeld "Scan" auf "Scan unterbrechen".

   Der Scanvorgang wird sofort unterbrochen und das Dialogfeld "Scan" bleibt so lange geöffnet, bis Sie den Vorgang fortsetzen.

2. Klicken Sie im Dialogfeld "Scan" auf "Scan fortsetzen", um den Scan fortzusetzen.

So unterbrechen oder verzögern Sie einen vom Administrator geplanten Scan

1. Wenn ein vom Administrator geplanter Scan ausgeführt wird, klicken Sie im Dialogfeld "Scan" auf "Scan unterbrechen".
2. Im Dialogfeld "Unterbrechung eines geplanten Scans" führen Sie eine der folgenden Aktionen aus:
   - Um den Scan vorübergehend anzuhalten, klicken Sie auf "Anhalten".
   - Um den Scan zu verschieben, klicken Sie auf "1 Stunde verschieben" oder auf "3 Stunden verschieben".
     Der Administrator legt fest, für wie lange Sie den Scan hinausschieben können. Wenn die Unterbrechung das Limit erreicht, beginnt der Scan wieder von vorne. Der Administrator entscheidet außerdem, wie oft Sie den Scan verzögern können, bevor die Funktion deaktiviert wird.
   - Um den Scan ohne anzuhalten fortzusetzen, klicken Sie auf "Weiter".

Fehlerbehebung bei Computerproblemen mit dem Symantec Endpoint Protection-Support-Tool

Sie können ein Dienstprogramm herunterladen, um allgemeine Probleme bei der Installation und Verwendung von Symantec Endpoint Protection Manager oder dem Symantec Endpoint Protection-Client zu diagnostizieren.

Sie können das Support-Tool bei folgenden Problemen verwenden:

- Hiermit können Sie schnell und genau bekannte Probleme identifizieren.
- Wenn das Tool ein Problem erkennt, leitet es Sie zu den Ressourcen um, damit Sie das Problem selbst lösen können.
- Wenn ein Problem nicht gelöst wird, können Sie mit dem Tool leicht Daten an den Support für weitere Diagnose senden.

So beheben Sie Computerprobleme mit dem Symantec Endpoint Protection-Support-Tool

1. Führen Sie einen der folgenden Schritte aus:
   - Weitere Informationen finden Sie im Supportdatenbankartikel, Symantec Endpoint Protection SupportTool.
   - Klicken Sie in der Konsole auf "Hilfe > Support-Tool herunterladen".
2. Befolgen Sie die Anweisungen auf dem Bildschirm.

Kapitel 2

Reaktion auf Warnmeldungen und Benachrichtigungen

In diesem Kapitel werden folgende Themen behandelt:

Typen von Warnmeldungen und Benachrichtigungen

Der Client arbeitet im Hintergrund, um Ihren Computer vor bösartigen Aktivitäten zu schützen. Manchmal muss der Client Sie über eine Aktivität benachrichtigen oder Sie zu einem Feedback auffordern.

Tabelle 2-1 zeigt die Typen der Meldungen an, die Sie möglicherweise sehen und auf die Sie reagieren müssen.

Tabelle 2-1 Typen von Warnmeldungen und Benachrichtigungen

Warnmeldung	Beschreibung
<Scanname> gestartet am oder Dialogfeld "Erkennungsergebnisse für Symantec Endpoint Protection"	Wenn ein Scan einen Virus oder ein Sicherheitsrisiko erkennt, werden die Scanergebnisse oder das Dialogfeld "Erkennungsergebnisse für Symantec Endpoint Protection" mit Einzelheiten über die Infektion angezeigt. Das Dialogfeld zeigt auch die Aktion an, die der Scan am Risiko durchführte. Normalerweise ist es nicht nötig, weitere Aktionen vorzunehmen, als die Aktivität zu überprüfen und das Dialogfeld zu schließen. Sie können bei Bedarf jedoch eingreifen. Siehe "Info zu Scanergebnissen" auf Seite 29.
Dialogfelder "Andere Meldung"	Sie können Popup-Meldungen aus folgenden Gründen sehen: ■ Der Client aktualisiert die Clientsoftware automatisch. Siehe "Reaktion auf Meldungen, die Clientsoftware zu aktualisieren" auf Seite 37. ■ Der Client fordert Sie auf, eine Anwendung zuzulassen oder zu blockieren. Siehe "Reaktion auf Meldungen, in denen Sie gefragt werden, ob eine Anwendung zugelassen oder blockiert werden soll" auf Seite 35. ■ Die Evaluierungslizenz des Clients ist abgelaufen. Siehe "Reaktion auf Meldungen zu abgelaufenen Lizenzen" auf Seite 36.

Warnmeldung	Beschreibung

Meldungen über das Benachrichtigungsbereichssymbol	Benachrichtigungen, die im Benachrichtigungsbereich der Taskleiste angezeigt werden, treten in folgenden Situationen auf:
	■ Der Client blockiert eine Anwendung.
	Beispielsweise könnten Sie die folgende Benachrichtigung sehen:
	`Traffic has been blocked from this application: (application name)`
	Wenn der Client so konfiguriert wurde, dass der gesamte Datenverkehr blockiert wird, werden diese Benachrichtigungen häufig angezeigt. Wenn Ihr Client so konfiguriert wurde, dass der gesamte Datenverkehr zugelassen wird, werden diese Benachrichtigungen nicht angezeigt.
	Siehe "Reaktion auf Meldungen, in denen Sie gefragt werden, ob eine Anwendung zugelassen oder blockiert werden soll" auf Seite 35.
	■ Der Client erkennt einen Netzwerkangriff auf Ihren Computer.
	Sie konnten den folgenden Benachrichtigungstyp sehen:
	`Traffic from IP address 192.168.0.3 is blocked from 2/14/2010 15:37:58 to 2/14/2010 15:47:58. Port Scan attack is logged.`
	■ Die Prüfung zur Einhaltung der Sicherheit schlug fehl. Der Datenverkehr zu oder von Ihrem Computer wird möglicherweise blockiert.
	Sie müssen nichts anderes tun, als die Meldungen zu lesen.

Siehe "Ermitteln, ob der Client eine Verbindung hergestellt hat und geschützt ist" auf Seite 44.

Info zu Scanergebnissen

Für verwaltete Clients konfiguriert der Administrator gewöhnlich einen vollständigen Scan, der mindestens einmal wöchentlich ausgeführt wird. Bei nicht verwalteten Clients wird beim Starten des Computers ein automatisch generierter Active Scan ausgeführt. Standardmäßig wird Auto-Protect kontinuierlich auf Ihrem Computer ausgeführt.

Wenn Scans ausgeführt werden, wird ein Scandialogfeld angezeigt, um über den Fortschritt zu berichten und die Ergebnisse des Scans anzuzeigen. Nach Abschluss des Scans werden die Ergebnisse in der Liste angezeigt. Wenn der Client keine Viren oder Sicherheitsrisiken erkennt, bleibt die Liste leer und der Status lautet "Abgeschlossen".

Wenn der Client bei einem Scan Risiken erkennt, werden im Dialogfeld mit den Scanergebnissen Ergebnisse mit den folgenden Informationen angezeigt:

- Namen der Viren oder Sicherheitsrisiken
- Namen der infizierten Dateien
- Aktionen, die der Client an den Risiken durchführt

Wenn der Client einen Virus oder ein Sicherheitsrisiko erkennt, müssen Sie unter Umständen Aktionen an einer infizierten Datei ausführen.

Hinweis: Bei verwalteten Clients entscheidet sich Ihr Administrator unter Umständen dafür, das Dialogfeld mit den Scanergebnissen auszublenden. Wenn der Client nicht verwaltet wird, können Sie dieses Dialogfeld anzeigen oder ausblenden.

Wenn Sie oder Ihr Administrator die Client-Software so konfiguriert haben, dass ein Dialogfeld mit den Scanergebnissen angezeigt wird, können Sie den Scan unterbrechen, neu starten oder beenden.

Siehe "Über verwaltete Clients und nicht-verwaltete Clients" auf Seite 15.

Siehe "Reaktion auf eine Viren- oder Sicherheitsrisikoerkennung" auf Seite 30.

Siehe "Unterbrechung und Verschiebung von Scans" auf Seite 24.

Reaktion auf eine Viren- oder Sicherheitsrisikoerkennung

Wenn ein vom Administrator definierter, ein benutzerdefinierter oder ein Auto-Protect-Scan ausgeführt wird, wird ein Dialogfeld mit den Scanergebnissen angezeigt. Sie können das Dialogfeld mit den Scanergebnissen verwenden, um sofort eine Aktion an der betroffenen Datei auszuführen. beispielsweise wenn Sie die bereinigte Datei löschen möchten, um sie durch die ursprüngliche, nicht infizierte Version zu ersetzen.

Wenn Symantec Endpoint Protection einen Prozess oder eine Anwendung beenden oder einen Dienst anhalten muss, ist die Option "Risiken jetzt entfernen" aktiviert.

Möglicherweise kann das Dialogfeld nicht geschlossen werden, wenn Risiken im Dialogfeld eine Aktion erforderlich machen.

Sie können auch mithilfe des Quarantäne-, Risiko- oder Scanprotokolls später Maßnahmen für die Datei ergreifen.

So reagieren Sie auf einen Virus oder eine Erkennung im Scanergebnis-Dialogfeld

1. Im Scanergebnis-Dialogfeld wählen Sie die Dateien aus, die Sie behandeln möchten.
2. Klicken Sie mit der rechten Maustaste auf die Auswahl und wählen Sie anschließend eine der folgenden Optionen aus:

Bereinigen	Entfernt den Virus aus der Datei. Diese Option ist nur für die Viren verfügbar.
Ausschließen	Schließt die Datei vom erneuten Scannen aus.
Dauerhaft löschen	Löscht die infizierte Datei und alle anderen betroffenen Elemente. Verwenden Sie diese Aktion bei Sicherheitsrisiken mit Vorsicht. In manchen Fällen kann das Löschen eines Sicherheitsrisikos dazu führen, dass Anwendungen ihre Funktionalität verlieren.
Durchgeführte Aktion rückgängig machen	Stellt den Zustand vor der ausgeführten Aktion wieder her.
In Quarantäne	Platziert die infizierten Dateien in der Quarantäne. Bei Sicherheitsrisiken versucht der Client auch, die Auswirkungen zu entfernen oder zu reparieren. Wenn der Client ein Sicherheitsrisiko isoliert, kann in manchen Fällen eine Anwendung auch ihre Funktionalität verlieren.
Eigenschaften	Zeigt Informationen über den Virus bzw. das Sicherheitsrisiko an.

   In einigen Fällen steht die Aktion unter Umständen nicht zur Verfügung.
3. Im Dialogfeld klicken Sie auf "Schließen".

   Sie sind möglicherweise nicht in der Lage, das Dialogfeld zu schließen, wenn die aufgelisteten Risiken erfordern, dass Sie Maßnahmen ergreifen. Beispielsweise muss möglicherweise der Client einen Prozess oder eine Anwendung beenden oder einen Dienst anhalten.

   Wenn Sie Maßnahmen ergreifen müssen, wird eine der folgenden Benachrichtigungen angezeigt:

   - Entfernung des Risikos erforderlich

Wird angezeigt, wenn ein Risiko die Beendigung eines Prozesses erfordert. Wenn Sie das Risiko entfernen, wird anschließend das Dialogfeld mit den Ergebnissen wieder angezeigt. Wenn außerdem ein Neustart erforderlich ist, wird im Dialogfeld in der Zeile des Risikos angezeigt, dass ein Neustart erforderlich ist.

- Neustart erforderlich
  Wird angezeigt, wenn ein Risiko einen Neustart erfordert.
- Risiko muss entfernt und Neustart durchgeführt werden
  Wird angezeigt, wenn ein Risiko Prozessbeendigung erfordert und ein anderes Risiko einen Neustart erfordert.

4 Wenn das Dialogfeld "Risiken jetzt entfernen" erscheint, klicken Sie auf eine der folgenden Optionen:

- Risiken jetzt entfernen (empfohlen)
  Der Client entfernt das Risiko. Das Entfernen des Risikos macht unter Umständen einen Neustart erforderlich. Informationen im Dialogfeld weisen darauf hin, ob ein Neustart erforderlich ist oder nicht.
- Risiken nicht entfernen
  Das Ergebnis-Dialogfeld erinnert Sie daran, dass noch Maßnahmen ausgeführt werden müssen. Das Dialogfeld "Risiken jetzt entfernen" wird jedoch erst beim Neustart Ihres Computers wieder angezeigt.

5 Wenn das Ergebnis-Dialogfeld nicht in Schritt 3 geschlossen wurde, klicken Sie auf "Schließen".

Wenn ein Neustart erforderlich ist, ist die Entfernung oder Reparatur erst abgeschlossen, wenn Sie den Computer neu starten.

Möglicherweise erfordert ein Risiko eine Aktion, Sie möchten diese aber erst später ausführen.

Das Risiko kann auf die folgenden Arten zu einem späteren Zeitpunkt entfernt oder repariert werden:

- Sie können das Risikoprotokoll öffnen, mit der rechten Maustaste auf das Risiko klicken und die Aktion einleiten.
- Sie können einen Scan ausführen, um das Risiko erneut zu ermitteln und das Ergebnisdialogfeld zu öffnen.

Sie können im Dialogfeld mit der rechten Maustaste auf ein Risiko klicken und eine Aktion auswählen. Die verfügbaren Aktionen hängen von den Aktionen ab, die für den Typ von Risiko konfiguriert wurden, den der Scan erkannt hat.

Siehe "Reaktion von Scans auf eine Viren- oder Risikoerkennung" auf Seite 71.

Siehe "Anzeigen von Protokollen" auf Seite 48.

Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58.

Siehe "Verwalten von isolierten Dateien auf Ihrem Clientcomputer" auf Seite 93.

Reagieren auf Download Insight-Meldungen, in denen Sie gefragt werden, ob Sie die heruntergeladenen Dateien blockieren oder zulassen möchten

Download Insight-Benachrichtigungen zeigen Informationen über die bösartigen und nicht eindeutigen Dateien an, die Download Insight erkennt, wenn Sie versuchen, sie herunterzuladen.

Hinweis: Unabhängig davon, ob Benachrichtigungen aktiviert sind, erhalten Sie Erkennungsmeldungen, wenn die Aktion für noch nicht eingestufte Dateien "Eingabeaufforderung" ist.

Sie oder Ihr Administrator können ändern, wie sensibel Download Insight bösartige Dateien behandelt. Das Ändern der Empfindlichkeitsstufe ändert möglicherweise die Anzahl der Benachrichtigungen, die Sie erhalten.

Download Insight verwendet Insight, eine Technologie von Symantec, die eine Dateibewertung auswertet und festlegt, die auf einer globalen Community aus Millionen von Benutzern basiert.

Die Download Insight-Benachrichtigung zeigt die folgenden Informationen über die erkannte Datei an:

- Dateireputation
  Die Dateireputation gibt die Vertrauenswürdigkeit einer Datei an. Bösartige Dateien sind nicht vertrauenswürdig. Noch nicht eingestufte Dateien sind möglicherweise vertrauenswürdig.
- Wie verbreitet die Datei in der Community ist
  Das Verbreitung einer Datei ist wichtig. Dateien, die nicht verbreitet sind, sind mit größerer Wahrscheinlichkeit Bedrohungen.
- Wie neu die Datei ist
  Je neuer eine Datei ist, desto weniger Informationen hat Symantec über die Datei.

Die Informationen können Ihnen helfen zu entscheiden, ob die Datei zugelassen oder blockiert werden soll.

So reagieren Sie auf eine Download Insight-Erkennung, in der Sie gefragt werden, ob Sie eine Datei, die Sie herunterladen möchten, blockieren oder zulassen wollen

- Wählen Sie in der Download Insight-Erkennungsmeldung eine der folgenden Aktionen aus:
  - Klicken Sie auf "Diese Datei von meinem Computer entfernen".
    Download Insight verschiebt die Datei in die Quarantäne. Diese Option wird nur für noch nicht eingestufte Dateien angezeigt.
  - Klicken Sie auf "Diese Datei zulassen".
    Möglicherweise erscheint ein Berechtigungsdialogfeld, das Sie fragt, ob Sie sicher sind, dass Sie die Datei zulassen möchten.
    Wenn Sie beschließen, eine noch nicht eingestufte Datei zuzulassen, die nicht isoliert wurde, wird die Datei automatisch ausgeführt. Wenn Sie beschließen, eine isolierte Datei zuzulassen, wird die Datei nicht automatisch ausgeführt. Sie können die Datei über Ihren temporären Ordner "Internet" ausführen.
    Normalerweise lautet der Ordnerpfad wie folgt: `\\Dokumente und Einstellungen\`*`Benutzername`*`\Lokale Einstellungen\Temporäre Internetdateien`.
    Wenn Sie auf nicht verwalteten Clients eine Datei zulassen, erstellt der Client automatisch eine Ausnahme für die Datei auf diesem Computer. Wenn Ihr Administrator Sie auf verwalteten Clients Ausnahmen erstellen lässt, erstellt der Client automatisch eine Ausnahme für die Datei auf diesem Computer.

Siehe "Verwalten von Download Insight-Erkennungen auf Ihrem Computer" auf Seite 78.

Siehe "So trifft Symantec Endpoint Protection anhand von Bewertungsdaten Entscheidungen über Dateien" auf Seite 72.

Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58.

Reaktion auf Symantec Endpoint Protection-Popup-Benachrichtigungen auf Windows 8-Computern

Auf Windows 8-Clients werden Popup-Benachrichtigungen für Malwareerkennung und andere kritische Ereignisse in der Metro-Benutzeroberfläche und auf dem Desktop angezeigt. Die Benachrichtigungen weisen auf Ereignisse hin, die entweder in der Metro-Benutzeroberfläche oder auf dem Desktop aufgetreten sind, unabhängig davon, welche Oberfläche Sie derzeit verwenden. Details zu dem

Ereignis, das die Benachrichtigung ausgelöst hat, werden in einer Meldung auf dem Windows-Desktop angezeigt.

Auf verwalteten Clients hat der Administrator die Popup-Benachrichtigungen möglicherweise deaktiviert.

So reagieren Sie auf Popup-Benachrichtigungen von Symantec Endpoint Protection unter Windows 8

1 Sie haben folgende Möglichkeiten:

- Klicken Sie in der Metro-Benutzeroberfläche auf die Benachrichtigung. Der Desktop wird angezeigt.
- Klicken Sie auf dem Desktop auf die Benachrichtigung. Die Benachrichtigung wird nicht mehr angezeigt.

2 Überprüfen Sie die Erkennungsergebnisse oder andere Informationsmeldungen, die auf dem Desktop angezeigt werden.

Bei Viren- und Spywareerkennungen, die sich nicht auf Metro-Anwendungen beziehen, müssen Sie eventuell zusätzliche Reparaturen durchführen. Bei Erkennungen, die sich auf Metro-Anwendungen beziehen, ist die einzige verfügbare Aktion "Ausschließen".

Wenn Sie die Metro-Benutzeroberfläche erneut aufrufen, wird möglicherweise auf der betroffenen Anwendung ein Symbol angezeigt, das darauf hinweist, dass Sie die Anwendung erneut herunterladen müssen.

Siehe "Verwalten von Symantec Endpoint Protection-Popup-Benachrichtigungen auf Windows 8-Computern" auf Seite 99.

Siehe "Reaktion auf eine Viren- oder Sicherheitsrisikoerkennung" auf Seite 30.

Reaktion auf Meldungen, in denen Sie gefragt werden, ob eine Anwendung zugelassen oder blockiert werden soll

Wenn eine Anwendung auf Ihrem Computer versucht, auf das Netzwerk zuzugreifen, fragt Sie der Client unter Umständen, ob die Anwendung zugelassen oder blockiert werden soll. Sie können beschließen, den Zugriff einer Anwendung auf das Netzwerk zu blockieren, die Sie für unsicher halten.

Diese Typen von Benachrichtigungen werden aus folgenden Gründen angezeigt:

- Die Anwendung versucht, auf Ihre Netzwerkverbindung zuzugreifen.

- Eine Anwendung, die Zugriff auf Ihre Netzwerkverbindung hat, wurde aktualisiert.
- Ihr Administrator hat die Client-Software aktualisiert.

Unter Umständen wird Ihnen der folgende Meldungstyp angezeigt, der Sie darüber informiert, wenn eine Anwendung auf Ihren Computer zuzugreifen versucht:

```
IEXPLORE.EXE is attempting to access the network.
Do you want to allow this program to access the network?
```

So reagieren Sie auf eine Meldung, in der Sie gefragt werden, ob eine Anwendung zugelassen oder blockiert werden soll

1. Um die Meldung das nächste Mal zu unterdrücken, wenn die Anwendung versucht, auf das Netzwerk zuzugreifen, können Sie auch im Dialogfeld auf "Antwort behalten und Frage für diese Anwendung nicht nochmals anzeigen" klicken.
2. Führen Sie einen der folgenden Schritte aus:
   - Um der Anwendung den Zugriff auf das Netzwerk zu gewähren, klicken Sie auf "Ja".
   - Um der Anwendung den Zugriff auf das Netzwerkverbindung zu verweigern, klicken Sie auf "Nein".

   Sie können auch die Aktion der Anwendung im Feld "Ausgeführte Anwendungen" oder in der Liste "Anwendungen" ändern.

Siehe "Erstellen von Firewall-Regeln für Anwendungen beim Zugriff auf das Netzwerk von Ihrem Computer" auf Seite 124.

Reaktion auf Meldungen zu abgelaufenen Lizenzen

Der Client verwendet eine Lizenz zur Aktualisierung der Virendefinitionen für Scans und der Clientsoftware. Der Client kann eine Evaluierungslizenz oder eine bezahlte Lizenz verwenden. Wenn eine Evaluierungslizenz abgelaufen ist, aktualisiert der Client weder Inhalt noch Clientsoftware.

Tabelle 2-2 Typen von Lizenzen

Lizenztyp	Beschreibung

Evaluierungslizenz	Wenn eine Evaluierungslizenz abgelaufen ist, erscheint das Teilfenster "Status" des Clients oben rot und folgende Meldung wird angezeigt:
	
	`Evaluation License has expired.`
	
	`All content download will discontinue on` *`date`*`. Please contact your Administrator to purchase a full Symantec Endpoint Protection License.`
	
	Sie können das Ablaufdatum auch anzeigen, indem Sie auf "Hilfe" > "Info" klicken.

Bezahlte Lizenz	Wenn eine bezahlte Lizenz abgelaufen ist, erscheint das Teilfenster "Status" des Clients oben gelb und folgende Meldung wird angezeigt: `Virus and Spyware Protection definitions are out of date.`

Unabhängig vom Lizenztyp müssen Sie sich an Ihren Administrator wenden, um die Lizenz zu aktualisieren oder zu erneuern.

Siehe "Typen von Warnmeldungen und Benachrichtigungen" auf Seite 27.

Siehe "Anzeigen von Protokollen" auf Seite 48.

Reaktion auf Meldungen, die Clientsoftware zu aktualisieren

Wenn die Client-Software automatisch aktualisiert wird, können Sie die folgende Benachrichtigung sehen:

```
Symantec Endpoint Protection has detected that
a newer version of the software is available from
the Symantec Endpoint Protection Manager.
Do you wish to download it now?
```

So reagieren Sie auf eine Benachrichtigungen zu automatischen Aktualisierungen

1 Führen Sie eine der folgenden Aktionen aus:

- Um die Software sofort herunterzuladen, klicken Sie auf "Jetzt herunterladen".

- Um nach einer bestimmen Zeit erinnert zu werden, klicken Sie auf "Später erinnern".

2 Wenn eine Meldung angezeigt wird, nachdem der Installationsprozess für die aktualisierte Software begonnen hat, klicken Sie auf "OK".

Kapitel 3

Sicherstellen, dass Ihr Computer geschützt ist

In diesem Kapitel werden folgende Themen behandelt:

Verwalten des Schutzes Ihres Computers

Standardmäßig wird Ihr Clientcomputer geschützt und Sie brauchen den Client nicht zu konfigurieren. Jedoch empfiehlt es sich, Ihren Schutz aus folgenden Gründen zu überwachen:

- Auf dem Computer wird ein nicht verwalteter Client ausgeführt.
  Sobald ein nicht-verwalteter Client installiert wird, haben nur Sie die Kontrolle über den Schutz Ihres Computers. Ein nicht verwalteter Client wird standardmäßig geschützt, aber Sie müssen möglicherweise die Schutzeinstellungen des Computers ändern.
- Sie möchten eine oder mehrere Schutzlösungen aktivieren oder deaktivieren.

- Sie möchten überprüfen, ob Sie die neuesten Virendefinitionen haben.
- Sie haben von einen aktuellen Virus oder von eine Sicherheitsbedrohung gehört und möchten einen Scan ausführen.

Tabelle 3-1 Prozess für das Verwalten des Schutzes Ihres Computers

Schritt	Beschreibung
Reaktion auf Warnmeldungen oder Benachrichtigungen	Reaktion auf Meldungen, die angezeigt werden und zur Eingabe auffordern. Beispielsweise erkennt ein Scan möglicherweise einen Virus oder ein Sicherheitsrisiko und zeigt die Scanergebnisse an, die Ihnen empfehlen, Maßnahmen zu ergreifen. Siehe "Typen von Warnmeldungen und Benachrichtigungen" auf Seite 27.
Schutzstatus prüfen	Prüfen Sie regelmäßig die Seite "Status", um zu ermitteln, ob alle Schutztypen aktiviert sind. Siehe "Erste Schritte auf der Status-Seite" auf Seite 13. Siehe "Aktivieren oder Deaktivieren des Schutzes auf dem Client-Computer" auf Seite 52.
Virendefinitionen aktualisieren	Stellen Sie sicher, dass die neuesten Virendefinitionen auf dem Computer installiert sind. ■ Prüfen Sie, ob Sie die neuesten Schutz-Updates haben. Sie können das Datum und die Anzahl dieser Definitionsdateien auf der Seite "Status" des Clients unter jedem Schutztyp prüfen. ■ Rufen Sie die neuesten Schutz-Updates ab. Siehe "Aktualisieren des Computerschutzes" auf Seite 41. Sie können diese Aufgaben auf einem verwalteten Client durchführen, wenn Ihr Administrator damit einverstanden ist.
Ihren Computer scannen	Führen Sie einen Scan aus, um festzustellen, ob der Computer oder Ihre E-Mail-Anwendung mit Viren infiziert ist. Standardmäßig scannt der Client den Computer nach dem Einschalten, jedoch können Sie den Computer jederzeit scannen. Siehe "Sofortiges Scannen Ihres Computers" auf Seite 23.

Schritt	Beschreibung
Schutzeinstellungen anpassen	In den meisten Fällen bieten die Standardeinstellungen angemessenen Schutz für Ihren Computer. Bei Bedarf können Sie die folgenden Schutztypen verringern oder erhöhen: ■ Planen zusätzlicher Scans Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58. ■ Fügen Sie Firewall-Regeln hinzu (nur nicht verwalteter Client) Siehe "Verwalten des Firewall-Schutzes" auf Seite 107.
Anzeigen von Protokollen für Erkennungen oder Angriffe	Prüfen Sie die Protokolle, um festzustellen, ob Ihr Client einen Viren- oder Netzwerkangriff erkannt hat. Siehe "Anzeigen von Protokollen" auf Seite 48.
Sicherheitsrichtlinie aktualisieren (Nur verwalteter Client)	Prüfen Sie, ob der Client die neuesten Sicherheitsrichtlinien von einem Management-Server erhalten hat. Eine Sicherheitsrichtlinie enthält die aktuellsten Schutztechnologie-Einstellungen für Ihren Client. Die Sicherheitsrichtlinie wird automatisch aktualisiert. Um sicherzustellen, dass Sie über die neueste Richtlinie verfügen, können Sie sie manuell aktualisieren, indem Sie mit der rechten Maustaste auf das Client-Benachrichtigungsbereichssymbol klicken und anschließend auf "Richtlinie aktualisieren" klicken. Siehe "Ermitteln, ob der Client eine Verbindung hergestellt hat und geschützt ist" auf Seite 44.

Siehe "Über verwaltete Clients und nicht-verwaltete Clients" auf Seite 15.

Aktualisieren des Computerschutzes

Symantec-Produkte benötigen stets aktuelle Informationen, um Ihren Computer vor neu auftretenden Bedrohungen zu schützen. Symantec stellt diese Informationen über LiveUpdate zur Verfügung.

Bei Content-Updates handelt es sich um Dateien, die Ihre Symantec-Produkte mit der neuesten Bedrohungsschutztechnologie auf dem aktuellsten Stand halten. Die Content-Updates, die Sie erhalten, hängen davon ab, welcher Schutz auf Ihrem Computer installiert sind. Beispielsweise lädt LiveUpdate Virendefinitionsdateien für Virus and Spyware Protection und IPS-Definitionsdateien für Netzwerkbedrohungsschutz herunter.

LiveUpdate kann außerdem Verbesserungen für den installierten Client je nach Bedarf zur Verfügung stellen. Diese Verbesserungen werden im Allgemeinen erstellt, um die Betriebssystem- oder Hardwarekompatibilität zu erweitern, Leistungsprobleme anzupassen oder Produktfehler zu beheben.

LiveUpdate ruft die neuen Content-Dateien von einer Symantec-Site ab und ersetzt dann die älteren Content-Dateien. Ein Client-Computer kann diese Verbesserungen direkt von einem LiveUpdate-Server erhalten. Ein verwalteter Client-Computer kann diese Updates mit Verbesserungen automatisch von einem Management-Server in Ihrem Unternehmen erhalten. Wie Ihr Computer die Updates empfängt, hängt davon ab, ob Ihr Computer verwaltet oder nicht verwaltet ist, und wie Ihr Administrator Updates konfiguriert hat.

Tabelle 3-2 Methoden zur Aktualisierung von Inhalt auf Ihrem Computer

Aufgabe	Beschreibung
Aktualisieren des Inhalts in geplanten Abständen	Standardmäßig wird LiveUpdate automatisch in geplanten Abständen ausgeführt. Auf einem nicht-verwalteten Client können Sie einen LiveUpdate-Zeitplan deaktivieren oder ändern. Siehe "Aktualisieren des Inhalts in geplanten Abständen" auf Seite 43.
Sofortiges Aktualisieren des Inhalts	Basierend auf Ihren Sicherheitseinstellungen können Sie "LiveUpdate" sofort ausführen. Siehe "Sofortiges Aktualisieren des Inhalts" auf Seite 42.

Sofortiges Aktualisieren des Inhalts

Sie können die Content-Dateien mithilfe von LiveUpdate sofort aktualisieren. Sie sollten LiveUpdate aus folgenden Gründen manuell ausführen:

- Die Clientsoftware wurde vor kurzem installiert.
- Der letzte Scan liegt länger zurück.
- Sie vermuten, dass Sie einen Virus oder anderes Malwareproblem haben.

Siehe "Aktualisieren des Inhalts in geplanten Abständen" auf Seite 43.

Siehe "Aktualisieren des Computerschutzes" auf Seite 41.

So aktualisieren Sie Ihren Schutz sofort

- Klicken Sie im Client in der Seitenleiste auf LiveUpdate.

  LiveUpdate stellt eine Verbindung zum Symantec-Server her, überprüft auf verfügbare Updates, führt den Download aus und installiert sie automatisch.

Aktualisieren des Inhalts in geplanten Abständen

Sie können einen Zeitplan erstellen, damit LiveUpdate automatisch in geplanten Abständen ausgeführt wird. Es empfiehlt sich, die Ausführung von LiveUpdate während eines Zeitraums zu planen, in dem Sie Ihren Computer nicht verwenden.

Siehe "Sofortiges Aktualisieren des Inhalts" auf Seite 42.

Hinweis: Wenn Sie einen verwalteten Client haben, können Sie LiveUpdate nur für die Ausführung nach einem Zeitplan konfigurieren, wenn Ihr Administrator Sie dazu autorisiert hat. Wenn das Vorhängeschloss-Symbol erscheint und die Optionen ausgegraut sind, können Sie Ihren Inhalt auf einem Zeitplan nicht aktualisieren.

So aktualisieren Sie Ihren Schutz nach einem Zeitplan

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Klicken Sie neben "Client-Management" auf "Einstellungen konfigurieren".
3. Klicken Sie im Dialogfeld "Client-Management-Einstellungen" auf "LiveUpdate".
4. Aktivieren Sie auf der Registerkarte "LiveUpdate" die Option "Automatische Updates aktivieren".
5. Wählen Sie im Gruppenfeld "Intervall und Zeit" aus, ob die Updates täglich, wöchentlich oder monatlich ausgeführt werden sollen. Wählen Sie dann den Tag oder die Woche und die Uhrzeit aus, zu der die Updates ausgeführt werden sollen.

   Die Zeiteinstellungen hängen davon ab, was Sie im Gruppefeld "Häufigkeit" auswählen. Die Verfügbarkeit der anderen Optionen hängt auch von der ausgewählten Häufigkeit ab.
6. Im Gruppefeld "Fenster für Wiederholungen" aktivieren Sie "Versuch wiederholen" und geben dann das Zeitintervall an, während dessen der Client versucht, LiveUpdate wieder auszuführen.
7. Im Gruppefeld "Optionen für die zufällige Ausführung" aktivieren Sie "Startzeitpunkt zufällig + oder - wählen (in Stunden) " und geben dann die Anzahl von Stunden oder Tagen an.

   Diese Option legt einen Zeitraum vor oder nach der geplanten Zeit für den Start des Updates fest.

8 Im Gruppefeld "Leerlauferkennung" aktivieren Sie "Geplantes LiveUpdates verzögern, bis das System untätig ist. Überfällige Sitzungen werden schließlich unbedingt ausgeführt."

Sie können auch Optionen für die Proxy-Server-Verbindung zu einem internen LiveUpdate-Server konfigurieren. Informationen zu den Optionen finden Sie in der Online-Hilfe.

9 Klicken Sie auf "OK'".

Manuelles Aktualisieren von Richtlinien auf dem Client

Sie können die Richtlinien auf dem Clientcomputer manuell aktualisieren, wenn Sie denken, dass Sie nicht die neueste Richtlinie auf dem Client haben. Wenn der Client das Update nicht erhält, liegt möglicherweise ein Kommunikationsfehler vor.

Prüfen Sie die Seriennummer der Richtlinie, um zu prüfen, ob Ihre verwalteten Clientcomputer mit dem Management-Server kommunizieren können.

So aktualisieren Sie Richtlinien manuell vom Clientcomputer aus

1 Klicken Sie auf dem Clientcomputer in der Clientoberfläche auf "Hilfe > Fehlerbehebung".

2 Klicken Sie im Dialogfeld "Fehlerbehebung" in der linken Spalte auf "Verwaltung".

3 Klicken Sie im Teilfenster "Verwaltung" unter "Richtlinienprofil" auf "Aktualisieren".

Ermitteln, ob der Client eine Verbindung hergestellt hat und geschützt ist

Sie können das Symbol für den Benachrichtigungsbereich auf dem Client prüfen, um festzulegen, ob der Client mit einem Management-Server verbunden und ausreichend geschützt ist.

Das Symbol befindet sich rechts in der Taskleiste des Clientcomputers. Sie können mit der rechten Maustaste auf dieses Symbol klicken, um häufig verwendete Befehle anzuzeigen.

Hinweis: Auf verwalteten Clients wird das Symbol nur im Infobereich angezeigt, wenn der Administrator es entsprechend konfiguriert hat.

Tabelle 3-3 Symantec Endpoint Protection Symbole für den Client-Status

Symbol	Beschreibung
	Der Client wird ohne Probleme ausgeführt. Er ist entweder offline oder nicht-verwaltet. Nicht-verwaltete Clients sind nicht mit einem Management-Server verbunden. Das Symbol ist ein einfaches gelbes Schild.
	Der Client wird ohne Probleme ausgeführt. Er ist mit dem Server verbunden und kommuniziert mit ihm. Alle Komponenten der Sicherheitsrichtlinie schützen den Computer. Das Symbol ist ein gelbes Schild mit einem grünen Punkt.
	Der Client hat ein geringfügiges Problem. Beispielsweise können die Virendefinitionen veraltet sein. Das Symbol ist ein gelbes Schild und ein hellgelber Punkt, der ein schwarzes Ausrufezeichen enthält.
	Der Client wird nicht ausgeführt, hat ein schwerwiegendes Problem oder eine seiner Schutzkomponenten ist deaktiviert. Beispielsweise kann der Netzwerkbedrohungsschutz deaktiviert sein. Das Symbol ist ein gelbes Schild mit einem weißen Punkt und roter Umrandung und einer roten Linie über dem Punkt.

Tabelle 3-4 zeigt die Symbole für den Symantec Network Access Control-Client-Status an, die im Benachrichtigungsbereich erscheinen.

Tabelle 3-4 Symantec Network Access Control Symbole für den Client-Status

Symbol	Beschreibung
	Der Client wird ohne Probleme ausgeführt, hat die Host-Integritätsprüfung bestanden und die Sicherheitsrichtlinie aktualisiert. Er ist entweder offline oder nicht-verwaltet. Nicht-verwaltete Clients sind nicht mit einem Management-Server verbunden. Das Symbol ist ein einfacher goldener Schlüssel.
	Der Client wird ohne Probleme ausgeführt, hat die Host-Integritätsprüfung bestanden und die Sicherheitsrichtlinie aktualisiert. Er kommuniziert mit dem Server. Das Symbol ist ein goldener Schlüssel mit einem grünen Punkt.
	Entweder ist die Hostintegritätsprüfung des Clients fehlgeschlagen oder die Sicherheitsrichtlinie wurde nicht aktualisiert. Das Symbol ist ein goldener Schlüssel mit einem roten Punkt, der ein weißes "x" enthält.

Siehe "Aus- und Einblenden des Benachrichtigungsbereichssymbols" auf Seite 46.

Aus- und Einblenden des Benachrichtigungsbereichssymbols

Sie können das Benachrichtigungsbereichssymbol bei Bedarf ausblenden. Sie können es beispielsweise ausblenden, wenn Sie mehr Platz in der Windows-Taskleiste benötigen.

Siehe "Ermitteln, ob der Client eine Verbindung hergestellt hat und geschützt ist" auf Seite 44.

Hinweis: Auf verwalteten Clients können Sie das Benachrichtigungsbereichssymbol nicht ausblenden, wenn Ihr Administrator diese Funktion eingeschränkt hat.

So zeigen Sie das Benachrichtigungsbereichssymbol an oder verbergen es:

1. Klicken Sie im Hauptfenster in der Seitenleiste auf "Einstellungen ändern".
2. Klicken Sie auf der Seite "Einstellungen ändern" neben "Client-Management" auf "Einstellungen konfigurieren".
3. Aktivieren oder deaktivieren Sie im Dialogfeld "Client-Management-Einstellungen" auf der Registerkarte "Allgemein" unter "Optionen anzeigen" das Kontrollkästchen "Symantec Security-Symbol im Benachrichtigungsbereich anzeigen".
4. Klicken Sie auf "OK".

Info zu Protokollen

Protokolle enthalten Informationen über Client-Konfigurationsänderungen, sicherheitsbezogene Aktivitäten und Fehler. Diese Datensätze werden Ereignisse genannt.

Sicherheitsbezogene Aktivitäten enthalten Informationen über Virenerkennungen, Computerstatus und Datenverkehr zu oder von Ihrem Computer. Wenn Sie einen verwalteten Client verwenden, können die Protokolle regelmäßig zum Management-Server hochgeladen werden. Ein Administrator kann die Daten verwenden, um den Gesamtsicherheitsstatus des Netzwerkes zu analysieren.

Protokolle sind wichtig zur Überwachung der Computeraktivität und seiner Interaktion mit anderen Computern und Netzwerken. Sie können die Informationen in den Protokollen verwenden, um die Tendenzen zu überwachen, die auf Viren, Sicherheitsrisiken und Angriffe auf Ihrem Computer hinweisen.

Weitere Informationen zu einem Protokoll erhalten Sie, wenn Sie F1 drücken, um die Hilfe für dieses Protokoll anzuzeigen.

Tabelle 3-5 Client-Protokolle

Protokoll	Beschreibung
Scanprotokoll	Enthält die Einträge über die Scans, die im Laufe der Zeit auf Ihren Computer ausgeführt wurden.
Risikoprotokoll	Enthält die Einträge über Viren und Sicherheitsrisiken, wie beispielsweise Adware und Spyware, die Ihren Computer infiziert haben. Sicherheitsrisiken sind mit einem Link zur Webseite von Symantec Security Response versehen, auf der Sie zusätzliche Informationen finden. Siehe "Isolieren einer Datei aus dem Risiko- oder Scanprotokoll" auf Seite 96.
Systemprotokoll für Viren- und Spyware-Schutz	Enthält die Informationen über Systemaktivitäten auf Ihrem Computer, die sich auf Viren und Sicherheitsrisiken beziehen. Diese Informationen umfassen Konfigurationsänderungen, Fehler und Definitionsdateiinformationen.
Bedrohungsprotokoll	Enthält Informationen über Bedrohungen, die SONAR auf Ihrem Computer erkannt hat. SONAR erkennt alle Dateien, die sich verdächtig verhalten. SONAR erkennt auch Systemänderungen.
Systemprotokoll für proaktiven Bedrohungsschutz	Enthält die Informationen über Systemaktivitäten auf Ihrem Computer, die sich auf SONAR beziehen.
Datenverkehrsprotokoll	Enthält die Ereignisse, die den Firewall-Datenverkehr und Intrusion Prevention-Angriffe betreffen. Das Protokoll enthält Informationen über Verbindungen, die Ihr Computer über das Netzwerk herstellt. Mithilfe der Protokolle für den Netzwerkbedrohungsschutz können Sie Datenverkehr leichter bis zu seiner Quelle zurückverfolgen und mögliche Netzwerkangriffe beheben. Die Protokolle können Ihnen zeigen, wann Ihr Computer vom Netzwerk blockiert wurde und geben Ihnen Informationen dazu, warum Ihr Zugriff blockiert wurde.
Paketprotokoll	Enthält Informationen über Datenpakete, die über die Ports zu oder von Ihrem Computer gesendet werden. Standardmäßig ist das Paketprotokoll deaktiviert. Auf einem verwalteten Client können Sie das Paketprotokoll nicht aktivieren. Auf einem nicht verwalteten Client können Sie das Paketprotokoll aktivieren. Siehe "Aktivieren des Paketprotokolls" auf Seite 49.

Protokoll	Beschreibung
Steuerungsprotokoll	Enthält die Informationen über die Windows-Registrierungsschlüssel, Dateien und DLLs, auf die eine Anwendung zugreift, sowie die Anwendungen, die auf Ihrem Computer ausgeführt werden.
Sicherheitsprotokoll	Enthält Informationen über die Aktivitäten, die eine Bedrohung für Ihren Computer darstellen können. Beispielsweise werden möglicherweise Informationen über solche Aktivitäten wie Denial of Service-Angriffe, Port-Scans und Änderungen an ausführbaren Dateien angezeigt.
Systemprotokoll für Client-Management	Enthält Informationen über alle Betriebsänderungen, die auf Ihrem Computer aufgetreten sind. Die Änderungen umfassen möglicherweise die folgenden Aktivitäten: ■ Ein Dienst wird gestartet oder beendet ■ Der Computer erkennt Netzwerkanwendungen ■ Die Software wird konfiguriert
Protokoll zu Manipulationsschutz	Enthält die Einträge über die Versuche, die Symantec-Anwendungen auf Ihrem Computer zu manipulieren. Diese Einträge enthalten Informationen über die Versuche, die der Manipulationsschutz erkannte oder erkannte und vereitelte.
Debug-Protokolle	Enthält Informationen über Client, Scans und Firewall für Fehlerbehebungszwecke. Ihr Administrator fordert Sie unter Umständen auf, die Protokolle zu aktivieren oder zu konfigurieren und sie dann zu exportieren.

Siehe "Anzeigen von Protokollen" auf Seite 48.

Anzeigen von Protokollen

Sie können Protokolle auf Ihrem Computer anzeigen, um die Details der Ereignisse zu sehen.

Hinweis: Wenn "Netzwerkbedrohungsschutz" oder "Network Access Control" nicht installiert sind, können Sie das Sicherheitsprotokoll, Systemprotokoll oder Steuerungsprotokoll nicht anzeigen.

So zeigen Sie ein Protokoll an

1. Klicken Sie im Hauptfenster in der Seitenleiste auf "Protokolle anzeigen".
2. Klicken Sie auf "Protokolle anzeigen" neben einem der folgenden Elemente:
   - Viren- und Spyware-Schutz
   - Proaktiver Bedrohungsschutz
   - Netzwerkbedrohungsschutz
   - Client-Management
   - Network Access Control

   Einige Elemente werden abhängig von Ihrer Installation möglicherweise nicht angezeigt.
3. Wählen Sie im Dropdown-Menü das Protokoll aus, das Sie anzeigen möchten.

Siehe "Info zu Protokollen" auf Seite 46.

Aktivieren des Paketprotokolls

Alle Netzwerkbedrohungsschutz-Protokolle und Client-Management-Protokolle außer dem Paketprotokoll sind standardmäßig aktiviert. Auf nicht verwalteten Clients können Sie das Paketprotokoll aktivieren bzw. deaktivieren.

Auf verwalteten Clients lässt Sie Ihr Administrator das Paketprotokoll möglicherweise aktivieren oder deaktivieren.

Siehe "Info zu Protokollen" auf Seite 46.

So aktivieren Sie das Paketprotokoll

1. Klicken Sie im Client auf der Seite "Status" rechts vom Netzwerkbedrohungsschutz auf "Optionen" und anschließend auf "Einstellungen ändern".
2. Klicken Sie im Dialogfeld "Einstellungen für den Netzwerkbedrohungsschutz" auf "Protokolle".
3. Aktivieren Sie "Paketprotokoll aktivieren".
4. Klicken Sie auf "OK".

Info zum Aktivieren und das Deaktivieren des Schutzes, wenn Sie Probleme beheben müssen

Im Allgemeinen sollten Sie die Schutztechnologien auf einem Clientcomputer immer aktiviert lassen.

Sie müssen möglicherweise alle oder einzelne Schutztechnologien vorübergehend deaktivieren, wenn Sie ein Problem mit dem Client-Computer haben. Beispiel: Wenn eine Anwendung nicht oder nicht richtig ausgeführt wird, sollten Sie den Netzwerkbedrohungsschutz deaktivieren. Wenn das Problem weiterhin besteht, nachdem Sie alle Schutztechnologien deaktiviert haben, deinstallieren Sie den Client vollständig. Ist das Problem dann immer noch vorhanden, wissen Sie, dass es nicht an Symantec Endpoint Protection liegt.

Warnung: Denken Sie daran, eine Schutzanwendung nach der Durchführung Ihrer Aufgabe zur Fehlerbehebung wieder zu aktivieren, um sicherzustellen, dass der Computer weiterhin geschützt ist.

Tabelle 3-6 beschreibt die Gründe, warum es sich empfiehlt, jede Schutztechnologie zu deaktivieren.

Tabelle 3-6 Zweck des Deaktivierens einer Schutztechnologie

Schutztechnologie	Zweck des Deaktivierens der Schutztechnologie
Viren- und Spyware-Schutz	Wenn Sie diesen Schutz deaktivieren, deaktivieren Sie nur Auto-Protect. Die geplanten oder Startscans werden weiterhin ausgeführt, wenn Sie oder Ihr Administrator sie dafür entsprechend konfiguriert haben. Sie sollten Auto-Protect aus folgenden Gründen ggf. aktivieren oder deaktivieren: ■ Auto-Protect verhindert unter Umständen, dass Sie ein Dokument öffnen können. Beispiel: Wenn Sie ein Microsoft Word-Dokument mit Makros öffnen möchten, hindert Sie Auto-Protect möglicherweise daran. Wenn Sie wissen, dass das Dokument sicher ist, können Sie Auto-Protect deaktivieren. ■ Auto-Protect kann Sie vor einer virusähnlichen Aktivität warnen, von der Sie wissen, dass sie nicht durch einen Virus verursacht ist. Beispielsweise erhalten Sie unter Umständen eine Warnung, wenn Sie neue Computeranwendungen installieren. Wenn Sie planen, mehrere Anwendungen zu installieren und die Warnung unterdrücken möchten, können Sie Auto-Protect vorübergehend deaktivieren. ■ Auto-Protect kann Probleme bei der Windows-Treiberaktualisierung verursachen. ■ Auto-Protect verlangsamt unter Umständen den Clientcomputer. **Hinweis:** Wenn Sie Auto-Protect deaktivieren, deaktivieren Sie auch Download Insight, selbst wenn Download Insight zuvor aktiviert wurde. Außerdem kann SONAR heuristische Bedrohungen nicht erkennen. Die SONAR-Erkennung von Hostdatei- und Systemänderungen funktioniert weiterhin. Siehe "Aktivieren oder Deaktivieren von Auto-Protect" auf Seite 54. Wenn Auto-Protect ein Problem mit einer Anwendung verursacht, ist es besser, eine Ausnahme zu erstellen, als den Schutz dauerhaft zu deaktivieren. Siehe "Ausschließen von Elementen von Scans" auf Seite 91.
Proaktiver Bedrohungsschutz	Es empfiehlt sich, den proaktiven Bedrohungsschutz aus folgenden Gründen zu deaktivieren: ■ Sie erhalten zu viele Warnungen über vermeintliche Bedrohungen, die keine sind. ■ Proaktiver Bedrohungsschutz verlangsamt unter Umständen den Clientcomputer. Siehe "Aktivieren oder Deaktivieren des Schutzes auf dem Client-Computer" auf Seite 52.

Schutztechnologie	Zweck des Deaktivierens der Schutztechnologie
Netzwerkbedrohungsschutz	Es empfiehlt sich, den Netzwerkbedrohungsschutz aus folgenden Gründen zu deaktivieren: ■ Sie installieren eine Anwendung, die unter Umständen von der Firewall blockiert wird. ■ Eine Firewall-Regel oder -Einstellung blockiert eine Anwendung aufgrund eines Fehlers des Administrators. ■ Die Firewall bzw. das Angriffsschutzsystem verursacht Netzwerkverbindungsprobleme. ■ Die Firewall verlangsamt unter Umständen den Clientcomputer. ■ Sie können eine Anwendung nicht öffnen. Wenn Sie nicht sicher sind, ob der Netzwerkbedrohungsschutz das Problem verursacht, müssen Sie unter Umständen alle Schutztechnologien deaktivieren. Auf einem verwalteten Client sperrt Ihr Administrator den Netzwerkbedrohungsschutz möglicherweise vollständig, damit Sie ihn nicht aktivieren oder deaktivieren können. Siehe "Aktivieren oder Deaktivieren des Angriffsschutzes" auf Seite 130. Siehe "Aktivieren oder Deaktivieren des Schutzes auf dem Client-Computer" auf Seite 52.
Manipulationsschutz	Normalerweise sollten Sie den Manipulationsschutz aktiviert haben. Wenn Sie eine hohe Anzahl an Falschmeldungen erhalten, möchten Sie möglicherweise den Manipulationsschutz vorübergehend deaktivieren. Beispielsweise können Drittanbieter-Anwendungen Änderungen vornehmen, die unbeabsichtigterweise versuchen, Symantec-Einstellungen oder -Prozesse zu ändern. Wenn Sie sicher sind, dass eine Anwendung sicher ist, können Sie eine Manipulationsschutzausnahme für die Anwendung erstellen. Siehe "Manipulationsschutz aktivieren, deaktivieren und konfigurieren" auf Seite 55.

Aktivieren oder Deaktivieren des Schutzes auf dem Client-Computer

Für Fehlerbehebungzwecke müssen Sie möglicherweise Auto-Protect, proaktiven Bedrohungsschutz oder Netzwerkbedrohungsschutz deaktivieren.

Wenn Schutzfunktionen auf dem Client deaktiviert sind:

- Die Statusleiste ist oben auf der Seite "Status" rot.
- Das Client-Symbol erscheint mit einem universellen Nein-Zeichen (ein roter Kreis, der diagonal durchgestrichen ist). Das Client-Symbol erscheint als volles Schutzschild in der Taskleiste in der unteren rechten Ecke Ihres Windows-Desktops. In einigen Konfigurationen wird das Symbol nicht angezeigt.
  Siehe "Ermitteln, ob der Client eine Verbindung hergestellt hat und geschützt ist" auf Seite 44.

Auf einem verwalteten Client kann Ihr Administrator eine Schutztechnologie jederzeit aktivieren oder deaktivieren. Wenn Sie einen Schutz deaktivieren, aktiviert möglicherweise Ihr Administrator den Schutz später wieder. Ihr Administrator hat möglicherweise auch einen Schutz gesperrt, damit Sie ihn nicht deaktivieren können.

Warnung: Symantec empfiehlt, dass Sie nur Auto-Protect vorübergehend deaktivieren, wenn Sie Fehlerbehebung auf dem Clientcomputer durchführen müssen.

So aktivieren Sie Schutztechnologien von der Statusseite aus:

- Klicken Sie auf dem Client oben auf der Seite "Status" auf "Beheben" oder "Alle beheben".

So aktivieren oder deaktivieren Sie Schutztechnologien von der Taskleiste aus:

- Klicken Sie auf dem Windows-Desktop im Benachrichtigungsbereich mit der rechten Maustaste auf das Client-Symbol und führen Sie dann eine der folgenden Aktionen aus:
  - Klicken Sie auf "Symantec Endpoint Protection aktivieren".
  - Klicken Sie auf "Symantec Endpoint Protection deaktivieren".

So aktivieren oder deaktivieren Sie Schutztechnologien vom Client aus

- Führen Sie im Client auf der Seite "Status" neben "*Schutztyp* Schutz" eine der folgenden Aufgaben aus:
  - Klicken Sie auf "Optionen" > "Schutz *Schutztyp* aktivieren".
  - Klicken Sie auf "Optionen" > "Alle Schutzfunktionen *Schutztyp* deaktivieren".

So aktivieren oder deaktivieren Sie die Firewall

1. Klicken Sie im Client oben auf der Seite "Status" neben "Protokolle für Netzwerkbedrohungsschutz" auf "Optionen > Einstellungen ändern".
2. Aktivieren oder deaktivieren Sie auf der Registerkarte "Firewall" die Option "Firewall aktivieren".
3. Klicken Sie auf "OK".

Siehe "Info zum Aktivieren und das Deaktivieren des Schutzes, wenn Sie Probleme beheben müssen" auf Seite 50.

Siehe "Aktivieren oder Deaktivieren von Auto-Protect" auf Seite 54.

Aktivieren oder Deaktivieren von Auto-Protect

Sie können Auto-Protect für Dateien und Prozesse, Internet-E-Mail und E-Mail-Groupware-Anwendungen aktivieren oder deaktivieren. Wenn Auto-Protect vollständig deaktiviert ist, erscheint der Viren- und Spyware-Status auf der Seite "Status" rot.

Auf einem verwalteten Client könnte Ihr Administrator "Auto-Protect" sperren, damit Sie es nicht deaktivieren können. Ebenso könnte Ihr Administrator festlegen, dass Sie "Auto-Protect" zwar vorübergehend deaktivieren können, aber dass die Funktion nach einer bestimmten Zeit automatisch wieder aktiviert wird.

Hinweis: Wenn Sie Auto-Protect deaktivieren, deaktivieren Sie auch Download Insight, selbst wenn Download Insight zuvor aktiviert wurde. Außerdem kann SONAR heuristische Bedrohungen nicht erkennen, Hostdatei- und Systemänderungen werden jedoch weiterhin erkannt.

Warnung: Symantec empfiehlt, dass Sie Auto-Protect nur vorübergehend deaktivieren, wenn Sie eine Fehlerbehebung mit Auto-Protect durchführen müssen.

So aktivieren oder deaktivieren Sie Auto-Protect für das Dateisystem

- Führen Sie im Client auf der Status -Seite neben "Viren- und Spyware-Schutz" eine der folgenden Aktionen aus:
  - Klicken Sie auf "Optionen" > "Viren- und Spyware-Schutz aktivieren".
  - Klicken Sie auf "Optionen" > "Alle Viren- und Spyware-Schutzfunktionen deaktivieren".

So aktivieren Sie Auto-Protect für E-Mail

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Klicken Sie neben "Viren- und Spyware-Schutz" auf "Einstellungen konfigurieren".
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren oder deaktivieren Sie auf der Registerkarte "Auto-Protect für Internet-E-Mail" die Option "Auto-Protect für Internet-E-Mail aktivieren".
   - Aktivieren oder deaktivieren Sie auf der Registerkarte "Microsoft Outlook Auto-Protect" die Option "Auto-Protect für Microsoft Outlook aktivieren".
   - Aktivieren oder deaktivieren Sie auf der Registerkarte "Auto-Protect für Notes" die Option "Auto-Protect für Lotus Notes aktivieren".

Auto-Protect für Internet-E-Mail wird nicht auf Server-Betriebssystemen unterstützt. Auto-Protect für Microsoft Outlook wird automatisch auf den Computern installiert, auf denen Outlook ausgeführt wird.

4 Klicken Sie auf "OK".

Siehe "Informationen zu den Auto-Protect-Typen" auf Seite 68.

Siehe "Warnsymbole auf der Status-Seite" auf Seite 17.

Siehe "Info zum Aktivieren und das Deaktivieren des Schutzes, wenn Sie Probleme beheben müssen" auf Seite 50.

Manipulationsschutz aktivieren, deaktivieren und konfigurieren

Der Manipulationsschutz bietet Echtzeitschutz für Symantec-Anwendungen, die auf Servern und Clients ausgeführt werden. Er verhindert, dass Bedrohungen und Sicherheitsrisiken Symantec-Ressourcen manipulieren. Sie können den Manipulationsschutz aktivieren oder deaktivieren. Sie können auch die Aktion konfigurieren, die der Manipulationsschutz durchführt, wenn er einen Manipulationsversuch in Bezug auf die Symantec-Ressourcen auf Ihrem Computer erkennt.

Standardmäßig ist der Manipulationsschutz auf "Blockieren und nicht protokollieren" eingestellt.

Hinweis: Auf einem verwalteten Client sperrt Ihr Administrator möglicherweise die Einstellungen des Manipulationsschutzes.

Siehe "Info zum Aktivieren und das Deaktivieren des Schutzes, wenn Sie Probleme beheben müssen" auf Seite 50.

So aktivieren oder deaktivieren Sie den Manipulationsschutz

1 Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".

2 Klicken Sie neben "Client-Management" auf "Einstellungen konfigurieren".

3 Aktivieren oder deaktivieren Sie auf der Registerkarte "Manipulationsschutz" die Option "Hilft, die Symantec-Sicherheitssoftware vor Manipulationen oder unerwünschtem Beenden zu schützen".

4 Klicken Sie auf "OK".

So konfigurieren Sie den Manipulationsschutz

1 Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".

2 Klicken Sie neben "Client-Management" auf "Einstellungen konfigurieren".

3. Klicken Sie auf der Registerkarte "Manipulationsschutz" im Listenfeld "Durchzuführende Aktionen, wenn eine Anwendung versucht, die Symantec-Sicherheitssoftware zu manipulieren oder zu beenden" auf "Nur protokollieren", "Blockieren und nicht protokollieren" oder "Blockieren und protokollieren".
4. Klicken Sie auf "OK".

Kapitel 4

Verwalten von Scans

In diesem Kapitel werden folgende Themen behandelt:

- Verwalten von SONAR auf Ihrem Clientcomputer
- Ändern von SONAR-Einstellungen

Verwalten von Scans auf Ihrem Computer

Standardmäßig führt der Client täglich einen Active Scan aus. Auf einem verwalteten Client können Sie Ihre eigenen Scans konfigurieren, wenn Ihr Administrator diese Einstellungen zur Verfügung gestellt hat. Ein nicht verwalteter Client enthält eine Active Scan-Voreinstellung, die deaktiviert ist, aber Sie können Ihre eigenen Scans verwalten.

Tabelle 4-1 Verwalten von Scans

Aufgabe	Beschreibung
Über Funktionsweise von Scans informieren	Überprüfen Sie die Scantypen und die Typen von Viren und Sicherheitsrisiken. Siehe "Funktionsweise von Viren- und Spyware-Scans" auf Seite 62.
Virendefinitionen aktualisieren	Stellen Sie sicher, dass die neuesten Virendefinitionen auf Ihrem Computer installiert sind. Siehe "Aktualisieren des Computerschutzes" auf Seite 41.
Prüfen, ob Auto-Protect aktiviert ist	Auto-Protect ist standardmäßig aktiviert. Sie sollten Auto-Protect immer aktiviert haben. Wenn Sie Auto-Protect deaktivieren, deaktivieren Sie auch Download Insight und verhindern so, dass SONAR heuristische Erkennungen vornimmt. Siehe "Aktivieren oder Deaktivieren von Auto-Protect" auf Seite 54.
Ihren Computer scannen	Scannen Sie Ihren Computer regelmäßig auf Viren und Sicherheitsrisiken. Stellen Sie sicher, dass Scans regelmäßig ausgeführt werden, indem Sie das letzte Scandatum prüfen. Siehe "Sofortiges Scannen Ihres Computers" auf Seite 23. Siehe "Planen eines benutzerdefinierten Scans" auf Seite 73. Wenn Scans ausgeführt werden, sehen Sie möglicherweise ein Scanergebnis-Dialogfeld. Sie können das Scanergebnis-Dialogfeld verwenden, um einige Aktionen auf den Elementen durchzuführen, die Scans erkennen. Siehe "Reaktion auf eine Viren- oder Sicherheitsrisikoerkennung" auf Seite 30. Sie können einen begonnenen Scan anhalten. Auf einem verwalteten Client legt Ihr Administrator fest, ob Sie einen vom Administrator initiierten Scan anhalten können. Siehe "Unterbrechung und Verschiebung von Scans" auf Seite 24.

Aufgabe	Beschreibung
Scans zur Verbesserung der Computerleistung anpassen	Standardmäßig stellt Symantec Endpoint Protection eine hohe Sicherheitsstufe bereit, während die Auswirkung auf Ihre Computerleistung minimiert wird. Sie können Einstellungen anpassen, um die Computerleistung weiter zu erhöhen. Bei geplanten Scans und Scans nach Bedarf können Sie die folgenden Optionen ändern: ■ Scanfeinabstimmung Legen Sie die Scanfeinabstimmung auf "Optimale Leistung der Anwendungen" fest. ■ Komprimierte Dateien Ändern Sie die Anzahl der Stufen, um komprimierte Dateien zu scannen. ■ Fortsetzbare Scans Sie können eine maximale Häufigkeit für die Ausführung eines Scans angeben. Der Scan beginnt erneut, wenn der Computer untätig ist. ■ Scans nach dem Zufallsprinzip Sie können angeben, dass ein Scan seine Startzeit innerhalb eines bestimmten Zeitintervalls nach dem Zufallsprinzip festlegt. Sie können auch Startscans deaktivieren oder den Zeitplan für Ihre geplanten Scans ändern. Siehe "Anpassen von Virus- und Spyware-Scan-Einstellungen" auf Seite 82. Siehe "Planen eines benutzerdefinierten Scans" auf Seite 73.

Aufgabe	Beschreibung
Scans zur Erhöhung des Schutzes auf Ihrem Computer anpassen	In den meisten Fällen bieten die Standard-Scaneinstellungen angemessenen Schutz für Ihren Computer. In einigen Fällen sollten Sie den Schutz erhöhen. Wenn Sie den Schutz erhöhen, wirkt sich dies möglicherweise auf Ihre Computerleistung aus. Bei geplanten Scans und Scans nach Bedarf können Sie die folgenden Optionen ändern: ■ Scanleistung Legen Sie die Scanfeinabstimmung auf "Optimale Leistung des Scans" fest. ■ Scan-Aktionen Ändern Sie die Fehlerbehebungsaktionen, die stattfinden, wenn ein Virus erkannt wird. ■ Scandauer Standardmäßig werden die geplanten Scans ausgeführt, bis das angegebene Zeitintervall abläuft, und fortgesetzt, wenn der Clientcomputer inaktiv ist. Sie können den Scandauer auf "Bis Scannen fertig ist" festlegen. ■ Insight-Suche Sie sollten sicherstellen, dass Insight Lookup aktiviert ist. Die Einstellungen für Insight Lookup ähneln denen für Download Insight. ■ Erhöhen Sie den Bloodhound-Schutz. Bloodhound sucht und isoliert die logischen Regionen einer Datei, um virusähnliches Verhalten zu erkennen. Sie können die Erkennungsstufe von "Automatisch" in "Aggressiv" ändern, um den Schutz auf Ihrem Computer zu erhöhen. Die Einstellung "Aggressiv" wird jedoch wahrscheinlich mehr Falschmeldungen produzieren. Siehe "Anpassen von Virus- und Spyware-Scan-Einstellungen" auf Seite 82.
Scanausnahmen angeben	Schließen Sie eine sichere Datei bzw. einen sicheren Prozess vom Scannen aus. Siehe "Ausschließen von Elementen von Scans" auf Seite 91.
Informationen über Erkennungen an Symantec senden	Standardmäßig sendet Ihr Client-Computer Informationen über Erkennungen an Symantec Security Response. Sie können Übermittlungen ausschalten oder festlegen, welche Arten von Informationen gesendet werden. Symantec empfiehlt, dass Sie Übermittlungen immer aktivieren. Die Informationen helfen Symantec, Bedrohungen zu behandeln. Siehe "Senden von Informationen über Erkennungen an Symantec Security Response" auf Seite 100.

Aufgabe	Beschreibung
Isolierte Dateien verwalten	Symantec Endpoint Protection isoliert infizierte Dateien und verschiebt sie an einen Speicherort, an dem die Dateien keine andere Dateien auf dem Computer infizieren. Wenn eine isolierte Datei nicht repariert werden kann, müssen Sie entscheiden, wie damit zu verfahren ist. Sie können auch folgende Aktionen durchführen: ■ Löschen Sie eine isolierte Datei, wenn eine Backup-Datei vorhanden oder eine Ersatzdatei von einer vertrauenswürdigen Quelle verfügbar ist. ■ Lassen Sie Dateien mit unbekannten Infektionen in der Quarantäne, bis Symantec neue Virendefinitionen veröffentlicht. ■ Prüfen Sie regelmäßig isolierte Dateien, um das Ansammeln einer großen Zahl von Dateien zu vermeiden. Prüfen Sie isolierte Dateien, wenn ein neuer Virenausbruch im Netzwerk angezeigt wird. Siehe "Verwalten von isolierten Dateien auf Ihrem Clientcomputer" auf Seite 93. Siehe "Isolieren von Dateien" auf Seite 95.

Tabelle 4-2 zeigt zusätzliche Scaneinstellungen an, die Sie ändern können, wenn Sie den Schutz erhöhen, die Leistung verbessern oder Falschmeldungen reduzieren möchten.

Tabelle 4-2 Scaneinstellungen

Aufgabe	Beschreibung
Auto-Protect-Einstellungen ändern, um die Computerleistung zu verbessern oder den Schutz zu erhöhen	Bei Auto-Protect sollten Sie die folgenden Optionen ändern: ■ Datei-Cache Stellen Sie sicher, dass der Datei-Cache aktiviert ist (der Standardwert ist "aktiviert"). Wenn der Datei-Cache aktiviert ist, erinnert sich Auto-Protect an die virenfreien Dateien, die es scannte, und scannt sie nicht erneut. ■ Netzwerkeinstellungen Wenn Auto-Protect auf Remote-Computern aktiviert ist, stellen Sie sicher, dass "Nur wenn Dateien ausgeführt werden" aktiviert ist. ■ Sie können auch angeben, dass Auto-Protect Dateien auf Remote-Computern vertraut und einen Netzwerk-Cache verwendet. Standardmäßig scannt Auto-Protect die Dateien, während sie von Ihrem Computer auf einen Remote-Computer geschrieben werden. Auto-Protect scannt auch Dateien, wenn sie von einem Remote-Computer auf Ihren Computer geschrieben werden. Ein Netzwerk-Cache speichert eine Aufzeichnung der Dateien, die Auto-Protect von einem Remote-Computer gescannt hat. Wenn Sie einen Netzwerk-Cache verwenden, verhindern Sie, dass Auto-Protect die gleiche Datei mehrmals scannt. Siehe "Anpassen von Virus- und Spyware-Scan-Einstellungen" auf Seite 82.

Aufgabe	Beschreibung
ELAM-Erkennungen verwalten	Sie müssen die frühere Early Launch Anti-Malware-Erkennung (ELAM) des Clients aktivieren oder deaktivieren, wenn Sie denken, dass ELAM Ihre Computerleistung beeinträchtigt. Oder Sie müssen die Standarderkennungseinstellung aufheben, wenn Sie viele Falschmeldungen bei ELAM-Erkennungen erhalten. Siehe "Aktivieren/Deaktivieren von Early Launch Anti-Malware (ELAM)" auf Seite 98.
Verwalten von Download Insight-Erkennungen	Download-Insight untersucht Dateien, die Sie über Webbrowser und Chat-Clients bzw. andere Portale herunterladen möchten. Download-Insight verwendet Informationen von Symantec Insight, das Informationen über Dateireputationen sammelt. Download-Insight verwendet die Reputationsbewertung einer Datei, damit eine Datei zugelassen oder blockiert werden kann oder fordert den Benutzer auf, Maßnahmen für die Datei zu ergreifen. Siehe "Verwalten von Download Insight-Erkennungen auf Ihrem Computer" auf Seite 78.
Verwalten von SONAR	Sie können die Einstellungen für SONAR anpassen. Siehe "Verwalten von SONAR auf Ihrem Clientcomputer" auf Seite 104.

Funktionsweise von Viren- und Spyware-Scans

Viren- und Spyware-Scans identifizieren und neutralisieren oder beseitigen Viren und Sicherheitsrisiken auf Ihren Computern. Ein Scan beseitigt einen Virus oder ein Risiko mithilfe der folgenden Prozesse:

- Die Scan-Engine durchsucht Dateien und andere Komponenten auf dem Computer auf Spuren von Viren in Dateien. Jedes Virus hat ein erkennbares Muster, die sog. Signatur. Auf dem Client wird eine Virendefinitionsdatei mit den bekannten Virensignaturen, jedoch ohne schädlichen Virencode installiert. Die Scan-Engine vergleicht jede Datei oder Komponente mit der Virendefinitionsdatei. Wenn die Scan-Engine eine Übereinstimmung findet, ist die Datei infiziert.
- Die Scan-Engine verwendet die Definitionsdateien, um zu ermitteln, ob ein Virus oder ein Risiko die Infektion verursacht hat. Die Scan-Engine nimmt dann eine Fehlerbehebungsaktion an der infizierten Datei vor. Um die Infektion zu entfernen, bereinigt, löscht oder isoliert der Client die Datei.
  Siehe "Reaktion von Scans auf eine Viren- oder Risikoerkennung" auf Seite 71.

Hinweis: Symantec Endpoint Protection isoliert oder bereinigt kein Risiko, das in Anwendungen im Windows 8-Stil erkannt wird. Symantec Endpoint Protection löscht das Risiko stattdessen.

Tabelle 4-3 beschreibt die Komponenten, die der Client auf Ihrem Computer scannt.

Tabelle 4-3 Vom Client gescannte Computerkomponenten

Komponente	Beschreibung
Ausgewählte Dateien	Der Client scannt einzelne Dateien. Bei den meisten Scans können Sie entscheiden, welche Dateien gescannt werden sollen. Die Client-Software verwendet eine Suche nach bestimmten Mustern, um nach Spuren der Viren innerhalb der Dateien zu suchen. Die Spuren der Viren werden Muster oder Signaturen genannt. Die einzelnen Dateien werden mit den Mustern verglichen, die zur Identifizierung möglicher Viren in völlig ungefährlicher Form in der Definitionsdatei enthalten sind. Wenn ein Virus gefunden wird, versucht der Client, diesen aus der infizierten Datei zu entfernen. Wenn die Datei nicht bereinigt werden kann, isoliert der Client die Datei, um weitere Infektionen auf Ihrem Computer zu verhindern. Der Client sucht anhand des Scannens auf bestimmte Muster auch nach Sicherheitsrisiken in Dateien und Windows-Registrierungsschlüsseln. Wenn ein Sicherheitsrisiko gefunden wird, isoliert der Client die infizierten Dateien und versucht, die damit verbundenen Probleme zu beseitigen. Wenn der Client die Dateien nicht isolieren kann, protokolliert er den Versuch.
Arbeitsspeicher des Computers	Der Client durchsucht den Computerspeicher. Dateiviren, Boot-Sektor-Viren und Makroviren können speicherresident sein. Speicherresidente Viren kopieren sich selbst in den Arbeitsspeicher des Computers. Dort bleibt der Virus verborgen, bis er durch ein bestimmtes Ereignis aktiviert wird. Danach kann der Virus eine im Diskettenlaufwerk befindliche Diskette oder die Festplatte infizieren. Viren im Arbeitsspeicher können nicht bereinigt werden. Um den Virus aus dem Arbeitsspeicher zu entfernen, müssen Sie den Computer neu starten, wenn Sie dazu aufgefordert werden.
Boot-Sektor	Der Client prüft den Boot-Sektor des Computers auf Boot-Sektor-Viren. Es werden zwei Bereiche geprüft: die Partitionstabellen und der Master-Boot-Sektor.
Diskettenlaufwerk	Eine gängige Verbreitungsmethode von Viren ist über Disketten. Eine Diskette kann in einem Diskettenlaufwerk bleiben, wenn Sie Ihren Computer starten oder ausschalten. Beim Start einer Scans durchsucht der Client den Boot-Sektor und die Partitionstabellen einer Diskette, die sich im Diskettenlaufwerk befindet. Wenn Sie Ihren Computer ausschalten, werden Sie aufgefordert, den Datenträger zu entfernen, um mögliche Infektionen zu verhindern.

Informationen zu Viren und Sicherheitsrisiken

Symantec Endpoint Protection scannt sowohl auf Viren als auch auf Sicherheitsrisiken. Sicherheitsrisiken umfassen Spyware, Adware, Rootkits und andere Dateien, die einen Computer oder ein Netzwerk einem Risiko aussetzen können.

Viren und Sicherheitsrisiken können durch E-Mail oder Instant Messenger-Programme eintreffen. Sie können ein Risiko ohne es zu wissen herunterladen, indem Sie eine Endbenutzer-Lizenzvereinbarung von einem Software-Programm akzeptieren.

Viele Viren und Sicherheitsrisiken werden als Drive-by-Downloads installiert. Diese Downloads treten normalerweise auf, wenn Sie bösartige oder infizierte Websites besuchen, und das Download-Programm der Anwendung sie durch eine legitime Sicherheitslücke auf Ihren Computer installiert.

Sie können Informationen über bestimmte Risiken auf der Website von Security Response Web anzeigen.

Auf der Website von Symantec Security Response finden Sie die aktuellsten Informationen zu Bedrohungen und Sicherheitsrisiken. Darüber hinaus enthält sie ausführliche Referenzinformationen, z. B. White Papers und detaillierte Informationen zu Viren und Sicherheitsrisiken.

Siehe "Reaktion von Scans auf eine Viren- oder Risikoerkennung" auf Seite 71.

Abbildung 4-1 Wie Viren und Sicherheitsrisiken einen Computer angreifen

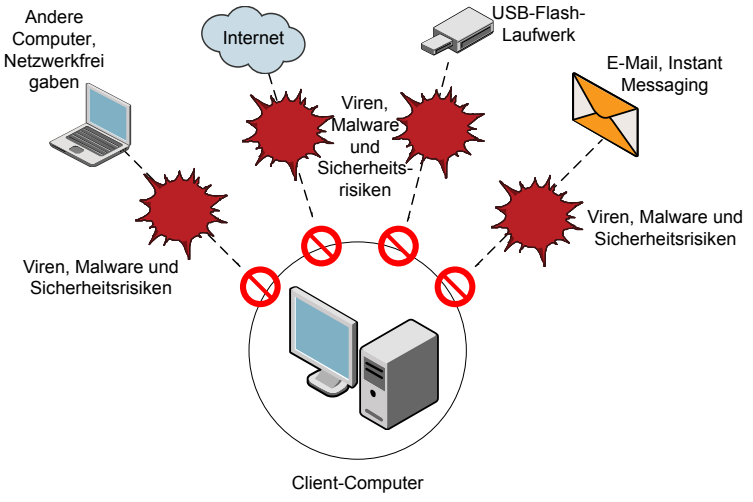

Tabelle 4-4 listet den Typ Viren und Risiken auf, die einen Computer angreifen können.

Tabelle 4-4 Viren und Sicherheitsrisiken

Risiko	Beschreibung
Viren	Programme oder Codes, die eine Kopie von sich selbst an andere Programme oder Dateien anhängen, wenn diese ausgeführt bzw. geöffnet werden. Wenn das infizierte Programm ausgeführt wird, wird das angehängte Virenprogramm aktiviert und hängt sich selbst an andere Programme und Dateien an. Die folgenden Typen von Bedrohungen sind in der Viruskategorie eingeschlossen: ■ Bösartige Internet-Bots Programme, die automatisierten Aufgaben über das Internet ausführen. Bots können verwendet werden, um Angriffe auf Computer zu automatisieren oder Informationen von Websites zu sammeln. ■ Würmer Programme, die sich selbst reproduzieren, ohne andere Programme zu infizieren. Einige Würmer verbreiten sich durch das Kopieren von Datenträger zu Datenträger, während andere im Arbeitsspeicher replizieren, um die Computerleistung zu reduzieren. ■ Trojanische Pferde Programme, die sich in harmlosen Objekten verbergen, etwa einem Spiel oder Dienstprogramm. ■ Komplexe Bedrohungen Hier handelt es sich um Bedrohungen, die die Merkmale von Viren, Würmern, Trojanischen Pferden und bösartigem Code mit Server- und Internet-Anfälligkeiten kombinieren, um einen Angriff zu initiieren, zu übertragen und zu verbreiten. Kombinierte Sicherheitsbedrohungen verwenden mehrere Methoden und Techniken, um sich schnell zu verbreiten und weitverbreiteten Schaden zu verursachen. ■ Rootkits Programme, die sich vor dem Betriebssystem eines Computers verstecken.
Adware	Programme, die Werbeinhalte liefern.
Dialer	Programme, die einen Computer dazu benutzen, ohne Erlaubnis oder Kenntnis des Benutzers über das Internet eine 0190er-Nummer oder eine FTP-Site anzuwählen. Gewöhnlich werden diese Nummern gewählt, um Gebühren zu verursachen.
Hacker-Tools	Programme, die von Hackern verwendet werden, um nicht autorisierten Zugriff auf den Computer eines Benutzers zu erhalten. So gibt es beispielsweise ein Hacker-Tool, das einzelne Tastaturanschläge erkennt und aufzeichnet, um die Daten anschließend zurück an den Hacker zu senden. Der Hacker kann anschließend Port-Scans ausführen oder nach Schwachstellen suchen. Mit Hacker-Tools können außerdem Viren erstellt werden.

Risiko	Beschreibung
Joke-Programme	Programme, die den Betrieb des Computers auf eine Art und Weise ändern oder unterbrechen, die lustig sein oder Angst machen soll. Beispielsweise könnte ein Scherzprogramm den Papierkorb weg von der Maus schieben, wenn der Benutzer versucht, ein Element zu löschen.
Irreführende Anwendungen	Anwendungen, die absichtlich den Sicherheitsstatus eines Computers verfälschen. Diese Anwendungen maskieren sich gewöhnlich als Sicherheitsmeldungen über gefälschte Infektionen, die entfernt werden müssen.
Kindersicherungsprogramme	Programme, die die Computernutzung überwachen oder begrenzen. Die Programme können verborgen ausführen und übermitteln gewöhnlich Überwachungsinformationen an einen anderen Computer.
Remote-Zugriffsprogramme	Programme, die den Zugriff auf einen Computer über das Internet ermöglichen, um Daten zu sammeln oder den Computer des Benutzers anzugreifen bzw. zu verändern.
Sicherheitsbewertungtool	Programme, die verwendet werden, um Informationen über nicht autorisierten Zugriff auf einen Computer zu sammeln.
Spyware	Unabhängige Programme, die die Systemaktivität unerkannt überwachen und Kennwörter und andere vertrauliche Informationen erkennen und an einen anderen Computer übertragen.
Trackware	Eigenständige oder angehängte Anwendungen, die den Weg eines Benutzers durch das Internet verfolgen und diese Informationen an ein Controller- oder Hacker-System senden.

Informationen zu den Scantypen

Symantec Endpoint Protection umfasst verschiedene Scantypen, um Schutz vor verschiedenen Typen von Viren, Bedrohungen und Risiken zu bieten.

Standardmäßig führt Symantec Endpoint Protection einen Active Scan täglich um 12:30 Uhr aus. Symantec Endpoint Protection führt auch einen Active Scan aus, wenn neue Definitionen auf dem Clientcomputer eintreffen. Auf nicht-verwalteten Computern umfasst Symantec Endpoint Protection auch einen Standard-Startscan, der deaktiviert ist.

Auf nicht verwalteten Clients sollten Sie sicherstellen, dass ein Active Scan täglich auf Ihrem Computer ausgeführt wird. Sie sollten evtl. einen vollständigen Scan einmal wöchentlich oder monatlich planen, wenn Sie eine inaktive Bedrohung auf Ihrem Computer vermuten. Vollständige Scans verbrauchen mehr Computerressourcen und wirken sich möglicherweise auf die Leistung des Computers aus.

Tabelle 4-5 Scantypen

Scantyp	Beschreibung
Auto-Protect	Auto-Protect prüft fortlaufend Dateien und E-Mail-Daten, sobald sie auf einen Computer geschrieben oder von ihm gelesen werden. Auto-Protect neutralisiert oder beseitigt erkannte Viren und Sicherheitsrisiken automatisch. Auto-Protect schützt auch E-Mail, die Sie möglicherweise senden oder empfangen. Siehe "Informationen zu den Auto-Protect-Typen" auf Seite 68.
Download Insight	Download Insight verstärkt die Sicherheit von Auto-Protect, indem Dateien untersucht werden, wenn Benutzer versuchen, sie von Browsern und anderen Portalen herunterzuladen. Download-Insight verwendet Informationen von Symantec Insight, das Informationen von Millionen Benutzern sammelt, um die Sicherheitsreputationen von Dateien in der Community festzulegen. Download-Insight verwendet die Reputationsbewertung einer Datei, damit eine Datei zugelassen oder blockiert werden kann oder fordert den Benutzer auf, Maßnahmen für die Datei zu ergreifen. Download Insight funktioniert als Teil von Auto-Protect und erfordert, dass Auto-Protect aktiviert ist. Wenn Sie Auto-Protect deaktivieren, Download Insight jedoch aktivieren, kann Download Insight nicht funktionieren. Siehe "So trifft Symantec Endpoint Protection anhand von Bewertungsdaten Entscheidungen über Dateien" auf Seite 72.

Scantyp	Beschreibung
Administratorscans und benutzerdefinierte Scans	Bei verwalteten Clients kann Ihr Administrator geplante Scans erstellen oder Scans nach Bedarf ausführen. Bei nicht-verwalteten Clients oder bei verwalteten Clients, für die Scaneinstellungen entsperrt sind, können Sie Ihre eigenen Scans erstellen und ausführen. Administrator- oder benutzerdefinierte Scans erkennen Viren und Sicherheitsrisiken, indem sie alle Dateien und Prozesse auf dem Clientcomputer überprüfen. Diese Typen von Scans können auch den Arbeitsspeicher und die Ladepunkte überprüfen. Die folgenden Typen von Administrator- oder der benutzerdefinierten Scans sind verfügbar: ■ Geplante Scans Ein geplanter Scan wird zu festgelegten Zeiten auf den Clientcomputern ausgeführt. Gleichzeitig geplante Scans werden nacheinander ausgeführt. Wenn ein Computer während eines geplanten Scans ausgeschaltet ist, wird der Scan nicht ausgeführt, außer er wurde so konfiguriert, dass verpasste Scans wiederholt werden. Sie können einen Active Scan, einen vollständigen oder benutzerdefinierten Scan planen. Sie können Ihre Einstellungen für geplante Scans als Vorlage speichern. Jeden Scan, den Sie als Vorlage speichern, können Sie als Basis für einen anderen Scan verwenden. Die Scanvorlagen können Ihnen Zeit sparen, wenn Sie mehrere Richtlinien konfigurieren. Eine Vorlage für geplante Scans ist standardmäßig in der Richtlinie enthalten. Der standardmäßige geplante Scan scannt alle Dateien und Ordner. ■ Scans bei Systemstart und ausgelöste Scans Scans bei Systemstart werden ausgeführt, wenn sich die Benutzer an den Computern einloggen. Ausgelöste Scans werden ausgeführt, wenn neue Virendefinitionen auf die Computer heruntergeladen werden. ■ Prüfungen auf Anforderung Scans nach Bedarf sind Scans, die Sie manuell starten. Sie können Scans nach Bedarf von der Seite "Scannen auf Bedrohungen" aus ausführen. Siehe "Funktionsweise von Viren- und Spyware-Scans" auf Seite 62.
SONAR	Es kann Angriffe unterbinden, noch bevor traditionelle signaturbasierte Definitionen eine Bedrohung erkennen. SONAR verwendet Heuristik sowie Dateireputationsdaten, um Entscheidungen über Anwendungen oder Dateien zu treffen. Siehe "Informationen zu SONAR" auf Seite 102.

Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58.

Informationen zu den Auto-Protect-Typen

Auto-Protect scannt Dateien sowie bestimmte Typen von E-Mail und E-Mail-Anhängen.

Wenn Ihr Client-Computer andere E-Mail-Sicherheitsprodukte wie Symantec Mail Security ausführt, brauchen Sie Auto-Protect für E-Mail unter Umständen nicht zu aktivieren.

Auto-Protect funktioniert nur auf Ihrem unterstützten E-Mail-Client. E-Mail-Server werden nicht vor Viren geschützt.

Hinweis: Wenn beim Öffnen Ihrer E-Mails ein Virus erkannt wird, kann es einige Sekunden dauern, bis die E-Mail-Nachricht geöffnet wird, da Auto-Protect erst den Scan abschließt.

Tabelle 4-6 Auto-Protect-Typen

Auto-Protect-Typ	Beschreibung
Auto-Protect	Scannt kontinuierlich Dateien, während sie von gelesen oder auf Ihren Computer geschrieben werden Auto-Protect ist standardmäßig für das Dateisystem aktiviert. Es lädt beim Computerstart. Er prüft alle Dateien auf Viren und Sicherheitsrisiken und blockiert die Installation von Sicherheitsrisiken. Er kann optional Dateien nach Dateierweiterung, Dateien auf Remote-Computern und Disketten auf Boot-Viren scannen. Er kann Dateien optional sichern, bevor er sie zu reparieren versucht, sowie Prozesse beenden und Dienste anhalten. Sie können Auto-Protect so konfigurieren, dass nur ausgewählte Dateierweiterungen gescannt werden. Wenn Auto-Protect die ausgewählten Erweiterungen scannt, kann es den Dateityp auch dann feststellen, wenn ein Virus die Dateierweiterung ändert. Wenn Sie nicht Auto-Protect für E-Mail ausführen, sind Ihre Clientcomputer weiterhin geschützt, wenn Auto-Protect aktiviert wird. Die meisten E-Mail-Anwendungen speichern Anhänge in einem temporären Ordner, wenn Benutzer E-Mail-Anhänge starten. Auto-Protect scannt die Datei, während sie in den temporären Ordner geschrieben wird, und erkennt Viren oder Sicherheitsrisiken. Auto-Protect erkennt den Virus auch, wenn der Benutzer versucht, einen infizierten Anhang auf einem lokalen Laufwerk oder einem Netzlaufwerk zu speichern.

Auto-Protect-Typ	Beschreibung
Auto-Protect für Internet-E-Mail	Scannt Internet-E-Mail (POP3 oder SMTP) und Anhänge auf Viren und Sicherheitsrisiken; führt auch ausgehenden E-Mail-Heuristikscans durch. Standardmäßig unterstützt Auto-Protect für Internet-E-Mail verschlüsselte Kennwörter und E-Mail über POP3- und SMTP-Verbindungen. Wenn Sie POP3 oder SMTP mit Secure Sockets Layer (SSL) verwenden, dann erkennt der Client sichere Verbindungen, scannt aber verschlüsselte Meldungen nicht. **Hinweis:** Aus Leistungsgründen wird Auto-Protect für Internet-E-Mail über POP3 auf Server-Betriebssystemen nicht unterstützt. Der E-Mail-Scan wird auch auf 64-Bit-Computern nicht unterstützt. E-Mail-Scannen unterstützt nicht IMAP-, AOL- oder HTTP-basierte E-Mail wie zum Beispiel Hotmail oder Yahoo! Mail.
Auto-Protect für Microsoft Outlook	Scannt Microsoft Outlook-E-Mail (MAPI und Internet) und Anhänge auf Viren und Sicherheitsrisiken Unterstützung für Microsoft Outlook 98/2000/2002/2003/2007/2010 (MAPI und Internet) Wenn Microsoft Outlook bereits auf dem Computer installiert ist, wenn Sie eine Client-Softwareinstallation durchführen, erkennt die Client-Software die E-Mail-Anwendung. Der Client installiert automatisch Microsoft Outlook Auto-Protect. Wenn Sie Microsoft Outlook über MAPI oder Microsoft Exchange-Client verwenden und Sie Auto-Protect für E-Mail aktiviert haben, werden Anhänge sofort heruntergeladen. Die Anhänge werden gescannt, wenn Sie den Anhang öffnen. Wenn Sie große Anhänge über eine langsame Verbindung herunterladen, wird die Arbeitsgeschwindigkeit der E-Mail-Anwendung beeinträchtigt. Sie können diese Funktion deaktivieren, wenn Sie regelmäßig große Anhänge erhalten. **Hinweis:** Auf einem Microsoft Exchange Server sollten Sie "Microsoft Outlook Auto-Protect" nicht installieren.
Auto-Protect für Lotus Notes	Scannt Lotus Notes-E-Mail und -Anhänge auf Viren und Sicherheitsrisiken Unterstützt für Lotus Notes 4.5 bis 8.x. Wenn Lotus Notes bereits auf dem Computer installiert ist, wenn Sie eine Client-Softwareinstallation durchführen, erkennt die Client-Software die E-Mail-Anwendung. Der Client installiert automatisch Auto-Protect für Lotus-Notes.

Reaktion von Scans auf eine Viren- oder Risikoerkennung

Bei durch Viren und Sicherheitsrisiken infizierten Dateien reagiert der Client auf die Bedrohungstypen auf unterschiedliche Weise. Für jeden Bedrohungstyp führt der Client eine erste Aktion aus und, wenn diese fehlschlägt, eine zweite.

Tabelle 4-7 Reaktion eines Scans auf Viren und Sicherheitsrisiken

Bedrohungstyp	Aktion
Virus	Wenn der Client einen Virus erkennt, geht er standardmäßig wie folgt vor: ■ Versucht zuerst, die mit dem Virus infizierte Datei zu bereinigen. ■ Wenn der Client die Datei bereinigt, entfernt er das Risiko vollständig von Ihrem Computer. ■ Wenn der Client die Datei nicht bereinigen kann, protokolliert er den Fehler und verschiebt die infizierte Datei in die Quarantäne. Siehe "Isolieren von Dateien" auf Seite 95. **Hinweis:** Symantec Endpoint Protection isoliert keine Viren, die in Metro-Anwendungen und -Dateien unter Windows 8 erkannt werden. Symantec Endpoint Protection löscht den Virus stattdessen.
Sicherheitsrisiko	Wenn der Client ein Sicherheitsrisiko erkennt, geht er standardmäßig wie folgt vor: ■ Er isoliert die infizierte Datei. ■ Der Client versucht, alle vom Sicherheitsrisiko vorgenommenen Änderungen zu entfernen oder zu reparieren. ■ Wenn der Client ein Sicherheitsrisiko nicht isolieren kann, protokolliert er es und unternimmt keine weiteren Schritte. Es kann vorkommen, dass Sie unwissentlich eine Anwendung installieren, die ein Sicherheitsrisiko, z. B. Adware oder Spyware, enthält. Wenn Symantec feststellt, dass das Isolieren des Risikos den Computer nicht schädigt, isoliert der Client das Risiko. Das sofortige Isolieren des Risikos könnte zur Instabilität des Computers führen. Um dies zu vermeiden, wird das Risiko erst nach Abschluss der Anwendungsinstallation isoliert. Anschließend werden die Nebeneffekte des Risikos repariert. **Hinweis:** Symantec Endpoint Protection isoliert keine Sicherheitsrisiken, die in Metro-Anwendungen und -Dateien unter Windows 8 erkannt werden. Symantec Endpoint Protection löscht das Risiko stattdessen.

Für jeden Scantyp können Sie die Einstellungen für die Behandlung der Viren und Sicherheitsrisiken durch den Client ändern. Sie können verschiedene Aktionen für Risikokategorien oder einzelne Sicherheitsrisiken festlegen.

So trifft Symantec Endpoint Protection anhand von Bewertungsdaten Entscheidungen über Dateien

Symantec sammelt Informationen über Dateien von seiner globalen Community von Millionen von Benutzern und aus seinem Global Intelligence Network. Die gesammelten Informationen bilden eine von Symantec gehostete Bewertungsdatenbank. Symantec-Produkte nutzen die Informationen, um Clientcomputer vor neuen, gezielten und mutierenden Bedrohungen zu schützen. Die Daten werden manchmal als "in der Cloud" bezeichnet, weil sie sich nicht auf dem Clientcomputer befinden. Der Clientcomputer muss Daten aus der Bewertungsdatenbank anfordern oder abfragen.

Symantec verwendet eine Technologie, die "Insight" genannt wird, um die Risikostufe oder Sicherheitsbewertung jeder Datei zu ermitteln.

Insight legt die Sicherheitsbewertung einer Datei fest, indem die folgenden Merkmale der Datei und ihres Kontextes überprüft werden:

- Die Quelle der Datei
- Wie neu die Datei ist
- Wie häufig die Datei in der Community vorkommt
- Weitere Sicherheitsdaten, z. B. mögliche Verbindungen der Datei zu Malware

Scanfunktionen in Symantec Endpoint Protection nutzen Insight, um Entscheidungen über Dateien und Anwendungen zu treffen. Der Viren- und Spyware-Schutz enthält eine Funktion, die als Download Insight bezeichnet wird. Download-Insight führt Erkennungen auf der Grundlage von Bewertungsinformationen durch. Wenn Sie Insight-Suchvorgänge deaktivieren, wird Download Insight ausgeführt, kann aber keine Erkennungen vornehmen. Sonstige Schutzfunktionen, wie zum Beispiel Insight Lookup und SONAR, verwenden Bewertungsinformationen für Erkennungen. Diese Funktionen können jedoch auch andere Technologien für Erkennungen verwenden.

Standardmäßig sendet ein Clientcomputer Informationen über Bewertungserkennungen zur Analyse an Symantec Security Response. Die Informationen helfen, die Insight-Bewertungsdatenbank weiter zu verfeinern. Je mehr Clients Informationen senden, desto nützlicher wird die Bewertungsdatenbank.

Sie können das Senden der Reputationsdaten deaktivieren. Symantec empfiehlt jedoch, die Sendefunktion aktiviert zu lassen.

Clientcomputer senden auch andere Arten von Informationen zu Erkennungen an Symantec Security Response.

Siehe "Verwalten von Download Insight-Erkennungen auf Ihrem Computer" auf Seite 78.

Siehe "Senden von Informationen über Erkennungen an Symantec Security Response" auf Seite 100.

Planen eines benutzerdefinierten Scans

Ein geplanter Scan ist eine wichtige Komponente beim Schutz vor Bedrohungen und Sicherheitsrisiken. Sie sollten mindestens einmal wöchentlich einen geplanten Scan ausführen, um sicherzustellen, dass Ihr Computer von Viren und Sicherheitsrisiken frei bleibt. Wenn Sie einen neuen Scan erstellen, wird der Scan in der Scanliste im Teilfenster "Scannen auf Bedrohungen" angezeigt.

Hinweis: Wenn Ihr Administrator einen geplanten Scan für Sie erstellt hat, wird er in der Scanliste im Teilfenster "Scannen auf Bedrohungen" angezeigt.

Zum geplanten Zeitpunkt des Scans muss der Computer eingeschaltet und die Symantec Endpoint Protection-Dienste müssen geladen sein. Standardmäßig werden Symantec Endpoint Protection-Dienste geladen, wenn Sie Ihren Computer starten.

Bei verwalteten Clients kann der Administrator diese Einstellungen überschreiben.

Siehe "Sofortiges Scannen Ihres Computers" auf Seite 23.

Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58.

Erwägen Sie die folgenden wichtigen Aspekte, wenn Sie einen geplanten Scan einrichten:

Bei benutzerdefinierten Scans muss der Benutzer nicht eingeloggt sein.	Ist der Benutzer, der einen Scan definiert hat, nicht eingeloggt, führt Symantec Endpoint Protection den Scan trotzdem aus. Sie können angeben, dass der Client den Scan nicht ausführen soll, wenn der Benutzer ausgeloggt ist.
Mehrere gleichzeitige Scans hintereinander ausgeführt	Wenn Sie mehrere Scans planen, die auf demselben Computer zur selben Zeit gestartet werden sollen, werden diese hintereinander ausgeführt. Nachdem ein Scan abgeschlossen ist, wird der nächste Scan gestartet. Beispiel: Sie haben drei verschiedene Scans geplant, die auf Ihrem Computer um 13 Uhr ausgeführt werden sollen. Jeder Scan scannt ein anderes Laufwerk. Ein Scan scannt Laufwerk C, der zweite Laufwerk D und der dritte Laufwerk E. Eine bessere Lösung ist, nur einen geplanten Scan zu erstellen, der die Laufwerke C, D und E scannt.

Verpasste geplante Scans werden möglicherweise nicht ausgeführt	Wenn Ihr Computer einen geplanten Scan aus einem bestimmten Grund verpasst, versucht Symantec Endpoint Protection standardmäßig, den Scan vor dem Starten oder bis zum Ablauf eines bestimmten Zeitintervalls durchzuführen. Wenn Symantec Endpoint Protection den verpassten Scan nicht innerhalb des Wiederholungsintervalls starten kann, wird der Scan nicht ausgeführt.
Zeit des geplanten Scans weicht möglicherweise ab	Symantec Endpoint Protection verwendet möglicherweise nicht die geplante Zeit, wenn der letzte Scan wegen der Scandauer oder den Einstellungen für verpasste geplante Scans zu einem anderen Zeitpunkt stattfand. Beispiel: Sie konfigurieren einen wöchentlichen Scan, der jeden Sonntag um Mitternacht ausgeführt werden soll, mit einem Wiederholungsintervall von einem Tag. Wenn der Computer den Scan verpasst und Montag um 6 Uhr morgens hochgefahren wird, startet der Scan zu diesem Zeitpunkt. Der nächste Scan wird eine Woche später um 6 Uhr morgens ausgeführt und nicht am darauffolgenden Sonntag um Mitternacht. Wenn der Computer erst am Dienstag um 6 Uhr morgens hochgefahren wird, wird das Wiederholungsintervall um zwei Tage überschritten. Daher wiederholt Symantec Endpoint Protection den Scan nicht erneut. Der Scan wird erst am darauffolgenden Sonntag um Mitternacht wiederholt. In beiden Fällen ändert sich der Zeitpunkt des letzten Scans möglicherweise, wenn die Startzeit des Scans zufällig gewählt wird.

Um weitere Informationen zu den Optionen in jedem Dialogfeld zu erhalten, klicken Sie auf "Hilfe".

So planen Sie einen benutzerdefinierten Scan

1. Klicken Sie in der Seitenleiste des Clients auf "Scannen auf Bedrohungen".
2. Klicken Sie auf "Neuen Scan erstellen".

3 Wählen Sie im Dialogfeld "Neuen Scan erstellen - Zu scannende Elemente" einen der folgenden Scantypen zur Planung aus:

Active Scan	Scannt die Bereiche des Computers, die am häufigsten durch Viren und Sicherheitsrisiken infiziert werden. Sie sollten täglich einen Active Scan ausführen.
Vollständiger Scan	Scannt den gesamten Computer auf Viren und Sicherheitsrisiken. Sie sollten einmal wöchentlich bzw. einmal monatlich einen vollständigen Scan ausführen. Vollständige Scans wirken sich möglicherweise auf die Leistung des Computers aus.
Benutzerdefinierter Scan	Scannt die ausgewählten Bereiche des Computers auf Viren und Sicherheitsrisiken.

4 Klicken Sie auf "Weiter".

5 Wenn Sie "Benutzerdefinierter Scan" ausgewählt haben, aktivieren Sie die entsprechenden Kontrollkästchen, um anzugeben, wo Sie scannen möchten, und klicken Sie dann auf "Weiter".

Die Symbole haben folgende Bedeutungen:

Die Datei, das Laufwerk oder der Ordner ist nicht ausgewählt. Wenn es sich bei dem Element um ein Laufwerk oder einen Ordner handelt, sind die darin enthaltenen Ordner bzw. Dateien ebenfalls nicht ausgewählt.

Die einzelne Datei oder der einzelne Ordner ist ausgewählt.

Der einzelne Ordner oder das Laufwerk ist ausgewählt. Alle Elemente innerhalb des Ordners oder Laufwerks sind ebenfalls ausgewählt.

Der einzelne Ordner oder das Laufwerk ist nicht ausgewählt, dafür sind jedoch ein oder mehrere Elemente innerhalb des Ordners oder Laufwerks ausgewählt.

6 Im Dialogfeld "Neuen Scan erstellen - Scanoptionen" können Sie eine der folgenden Optionen ändern:

Dateitypen	Ändern Sie die vom Client zu scannenden Dateierweiterungen. Standardmäßig werden alle Dateien gescannt.
Aktionen	Ändert die erste und zweite Aktion, die ausgeführt werden soll, wenn Viren und Sicherheitsrisiken erkannt werden.
Benachrichtigungen	Erstellt eine Meldung, die angezeigt wird, wenn ein Virus oder ein Sicherheitsrisiko gefunden wird. Sie können auch festlegen, ob Sie vor dem Ausführen von Fehlerbehebungsaktionen benachrichtigt werden möchten.
Erweitert	Ändern Sie zusätzliche Scanfunktionen wie beispielsweise das Anzeigen des Dialogfelds mit den Scanergebnissen.
Scanoptimierung	Ändern Sie die vom Client zu scannenden Computerkomponenten. Welche Optionen zur Verfügung stehen, hängt davon ab, was Sie in Schritt 3 gewählt haben.

7 Klicken Sie auf "Weiter".

8 Klicken Sie im Dialogfeld "Neuen Scan erstellen - Scanzeitpunkt" auf "Zum angegebenen Zeitpunkt", und klicken Sie anschließend auf "Weiter".

Sie können auch einen Scan auf Anforderung oder einen Startscan erstellen.

Siehe "Einen Scan planen, der nach Bedarf oder beim Starten des Computers ausgeführt werden soll" auf Seite 77.

9 Im Dialogfeld "Neuen Scan erstellen - Termin" geben Sie unter "Scantermin" die Häufigkeit und den Scanzeitpunkt an, und klicken Sie anschließend auf "Weiter".

10 Unter "Scandauer" können Sie einen Zeitraum angeben, in dem der Scan abschließen muss. Sie können die Scanstartzeit auch per Zufallsprinzip festlegen.

11 Unter "Verpasste geplante Scans" können Sie ein Intervall angeben, während dem ein Scan erneut versucht werden kann.

12 Geben Sie in das Dialogfeld "Neuen Scan erstellen - Scanname" einen Namen und eine Beschreibung für den Scan ein.

Nennen Sie den Scan beispielsweise: Freitag Morgen

13 Klicken Sie auf "Fertig stellen".

Einen Scan planen, der nach Bedarf oder beim Starten des Computers ausgeführt werden soll

Sie können einen geplanten Scan immer durch einen automatischen Scan ergänzen, wenn Sie Ihren Computer starten oder sich einloggen. Oft ist ein Startscan auf wichtige Ordner mit hohem Infektionsrisiko beschränkt, wie beispielsweise den Windows-Ordner und Ordner, die Microsoft Word- und Excel-Vorlagen enthalten.

Wenn Sie regelmäßig dieselben Dateien oder Ordner scannen, können Sie einen Scan auf Anforderung erstellen, in dem nur diese Elemente gescannt werden. Somit können Sie jederzeit schnell prüfen, ob die betreffenden Dateien und Ordner frei von Viren und Sicherheitsrisiken sind. Sie müssen Scans auf Anforderung manuell ausführen.

Wenn Sie mehrere Startscans erstellen, werden sie nacheinander in der Reihenfolge ausgeführt, in der sie erstellt wurden. Ihr Administrator hat unter Umständen den Client entsprechend konfiguriert, dass Sie keinen Startscan erstellen können.

Siehe "Sofortiges Scannen Ihres Computers" auf Seite 23.

Um weitere Informationen zu den Optionen in jedem Dialogfeld zu erhalten, klicken Sie auf "Hilfe".

So planen Sie einen Scan nach Bedarf oder beim Starten des Computers

1. Klicken Sie in der Seitenleiste des Client auf "Scannen auf Bedrohungen".
2. Klicken Sie auf "Neuen Scan erstellen".
3. Geben Sie an, was gescannt werden soll sowie etwaige Scanoptionen für den geplanten Scan.

   Siehe "Planen eines benutzerdefinierten Scans" auf Seite 73.
4. Führen Sie im Dialogfeld "Neuen Scan erstellen - Scanzeitpunkt" eine der folgenden Aktionen aus:
   - Klicken Sie auf "Beim Systemstart".
   - Klicken Sie auf "Auf Anforderung".
5. Klicken Sie auf "Weiter".
6. Geben Sie in das Dialogfeld "Neuen Scan erstellen - Scanname" einen Namen und eine Beschreibung für den Scan ein.

   Nennen Sie den Scan beispielsweise: Eigener Scan1
7. Klicken Sie auf "Fertig stellen".

Verwalten von Download Insight-Erkennungen auf Ihrem Computer

Auto-Protect enthält eine Funktion, die Download Insight genannt wird und die die Dateien überprüft, die Sie über Webbrowser, Text Messaging-Clients und andere Portale herunterzuladen versuchen. Auto-Protect muss aktiviert sein, damit Download Insight funktioniert.

Unterstützte Portale sind Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Windows Live Messenger und Yahoo Messenger.

Hinweis: Im Risikoprotokoll zeigen die Risikodetails für eine Download Insight-Erkennung nur die erste Portal-Anwendung an, die den Download versuchte. Beispielsweise könnten Sie Internet Explorer verwenden, um eine Datei, die Download Insight erkennt, herunterzuladen zu versuchen. Wenn Sie dann Firefox verwenden, um die Datei herunterzuladen zu versuchen, zeigt das Feld "Heruntergeladen von" in den Risikodetails Internet Explorer als das Portal an.

Hinweis: Auto-Protect kann auch Dateien scannen, die Benutzer als E-Mail-Anhänge erhalten.

Tabelle 4-8 Verwalten von Download Insight-Erkennungen auf Ihrem Computer

Aufgabe	Beschreibung
Herausfinden, wie Download Insight Bewertungsdaten verwendet, um Entscheidungen über Dateien zu treffen	Download Insight legt basierend auf der Dateibewertung fest, ob eine heruntergeladene Datei möglicherweise ein Risiko darstellt. Download Insight verwendet exklusiv Bewertungsinformationen, wenn Entscheidungen über heruntergeladene Dateien getroffen werden. Er verwendet keine Signaturen oder Heuristiken, um Entscheidungen zu treffen. Wenn Download Insight eine Datei zulässt, scannt Auto-Protect oder SONAR die Datei, wenn der Benutzer die Datei öffnet oder ausführt. Siehe "So trifft Symantec Endpoint Protection anhand von Bewertungsdaten Entscheidungen über Dateien" auf Seite 72.

Aufgabe	Beschreibung
Reaktion auf Download Insight-Erkennungen	Sie erhalten möglicherweise Benachrichtigungen, wenn Download Insight eine Erkennung macht. Bei verwalteten Clients entscheidet Ihr Administrator möglicherweise, Benachrichtigungen zur Download Insight-Erkennung zu deaktivieren. Wenn Benachrichtigungen aktiviert sind, sehen Sie Meldungen, wenn Download Insight eine bösartige Datei oder eine noch nicht eingestufte Datei erkennt. Bei noch nicht eingestuften Dateien müssen Sie entscheiden, ob die Datei zugelassen wird. Siehe "Reagieren auf Download Insight-Meldungen, in denen Sie gefragt werden, ob Sie die heruntergeladenen Dateien blockieren oder zulassen möchten" auf Seite 33.
Erstellen von Ausnahmen für bestimmte Dateien oder Internet-Domänen	Sie können eine Ausnahme für eine Anwendung erstellen, die Ihre Benutzer herunterladen. Sie können auch eine Ausnahme für eine bestimmte Internet-Domäne erstellen, die Sie als vertrauenswürdig einstufen. Standardmäßig überprüft Download Insight keine Dateien, die Benutzer von einer vertrauenswürdigen Internet- oder Intranetsite herunterladen. Vertrauenswürdige Sites werden auf der Registerkarte "Windows-Systemsteuerung > Vertrauenswürdige Internet-Sites > Sicherheit" konfiguriert. Wenn die Option "Aus dem Intranet heruntergeladenen Dateien automatisch vertrauen" aktiviert ist, lässt Symantec Endpoint Protection jede Datei zu, die ein Benutzer von einer der vertrauenswürdigen Sites herunterlädt. Download Insight kennt nur ausdrücklich konfigurierte vertrauenswürdige Sites an. Platzhalter sind zulässig, aber nicht-routingfähige IP-Adresse-Bereiche werden nicht unterstützt. Beispielsweise kann Download Insight 10 nicht erkennen.*.*.* als vertrauenswürdige Site. Download Insight unterstützt auch nicht die Sites, die durch die Option "Internetoptionen > Sicherheit > Intranet-Netzwerk automatisch erkennen" erkannt werden. Siehe "Ausschließen von Elementen von Scans" auf Seite 91.
Sicherstellen, dass Insight-Suchvorgänge aktiviert sind	Download Insight benötigt Bewertungsdaten, um Entscheidungen über Dateien zu treffen. Wenn Sie Insight-Suchvorgänge deaktivieren, wird Download Insight ausgeführt, kann aber keine Erkennungen vornehmen. Insight-Suchvorgänge sind standardmäßig aktiviert. Siehe "Senden von Informationen über Erkennungen an Symantec Security Response" auf Seite 100.

Aufgabe	Beschreibung
Download Insight-Einstellungen anpassen	Sie sollten Download Insight-Einstellungen aus folgenden Gründen anpassen: ■ Erhöhen oder Verringern der Anzahl von Download Insight-Erkennungen. Sie können den Empfindlichkeitsschieberegler für bösartigen Dateien justieren, um die Anzahl von Erkennungen zu erhöhen oder zu verringern. Bei niedrigeren Empfindlichkeitsstufen erkennt Download Insight weniger Dateien als bösartig und mehr Dateien als noch nicht eingestuft. Weniger Erkennungen sind Falscherkennungen. Bei höheren Empfindlichkeitsstufen erkennt Download Insight mehr Dateien als bösartig und weniger Dateien als noch nicht eingestuft. Mehr Erkennungen sind Falscherkennungen. ■ Ändern der Aktion bei bösartigen oder noch nicht eingestuften Dateierkennungen. Sie können anpassen, wie Download Insight bösartige oder noch nicht eingestufte Dateien bearbeitet. Sie können die Aktion bei noch nicht eingestuften Dateien ändern, damit Sie keine Benachrichtigungen für diese Erkennungen erhalten. ■ Erhalten von Warnmeldungen über Download Insight-Erkennungen. Wenn Download Insight eine Datei erkennt, die als bösartig eingeschätzt wird, wird eine Meldung auf dem Client-Computer angezeigt, wenn die Aktion auf "Quarantäne" festgelegt ist. Sie können die Quarantäne-Aktion rückgängig machen. Wenn Download Insight eine Datei erkennt, die als noch nicht eingestuft eingeschätzt wird, wird eine Meldung auf dem Client-Computer angezeigt, wenn Sie die Aktion bei noch nicht eingestuften Dateien auf "Eingabeaufforderung" oder "Quarantäne" festlegen. Wenn die Aktion auf "Eingabeaufforderung" festgelegt ist, können Sie die Datei zulassen oder blockieren. Wenn die Aktion "Quarantäne" ist, können Sie die Quarantäne-Aktion rückgängig machen. Sie können Benutzerbenachrichtigungen deaktivieren, damit Sie keine Auswahl haben, wenn Download Insight eine Datei erkennt, die als noch nicht eingestuft eingeschätzt wird. Wenn Sie Benachrichtigungen aktiviert lassen, können Sie die Aktion für noch nicht eingestufte Dateien auf "Ignorieren" festlegen, damit diese Erkennungen immer zugelassen werden und Sie nicht benachrichtigt werden. Wenn Benachrichtigungen aktiviert sind, wirkt sich die Empfindlichkeitseinstellung für bösartige Dateien auf die Anzahl der Benachrichtigungen aus, die Sie erhalten. Wenn Sie die Empfindlichkeit erhöhen, erhöhen Sie die Anzahl von Benutzerbenachrichtigungen, weil sich die Gesamtanzahl von Erkennungen erhöht. Siehe "Anpassen der Download Insight-Einstellungen" auf Seite 81.

Aufgabe	Beschreibung
Senden von Informationen über Reputationserkennungen an Symantec	Standardmäßig senden Clients Informationen über Reputationserkennungen an Symantec. Symantec empfiehlt, dass Sie Übertragungen für Reputationserkennungen aktivieren. Die Informationen helfen Symantec, Bedrohungen zu behandeln. Siehe "Senden von Informationen über Erkennungen an Symantec Security Response" auf Seite 100.

Anpassen der Download Insight-Einstellungen

Sie können ggf. Download Insight-Einstellungen anpassen, um Falscherkennungen auf Client-Computern zu verringern. Sie können anpassen, wie empfindlich Download Insight auf Dateibewertungsdaten reagiert, die zur Bewertung bösartiger Dateien verwendet werden. Sie können auch die Benachrichtigungen ändern, die Download Insight nach einer Erkennung auf Client-Computern anzeigt.

Siehe "Verwalten von Download Insight-Erkennungen auf Ihrem Computer" auf Seite 78.

Anpassen der Download Insight-Einstellungen

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Klicken Sie neben "Viren- und Spyware-Schutz" auf "Einstellungen konfigurieren".
3. Stellen Sie auf der Registerkarte "Download Insight" sicher, dass "Download Insight aktivieren, um in heruntergeladenen Dateien potenzielle Risiken basierend auf der Dateibewertung zu erkennen" aktiviert ist.

   Wenn Auto-Protect deaktiviert ist, funktioniert Download Insight selbst bei Aktivierung nicht.
4. Verschieben Sie den Schieberegler, um die Empfindlichkeit für bösartige Dateien zu ändern.

   Hinweis: Wenn Sie oder Ihr Administrator grundlegenden Viren- und Spyware-Schutz installiert haben, ist die Empfindlichkeit für bösartige Dateien automatisch auf Stufe 1 festgelegt und kann nicht geändert werden.

   Wenn Sie die Stufe erhöhen, erkennt Download Insight mehr Dateien als bösartig und weniger Dateien als noch nicht eingestuft. Höhere Einstellungen geben jedoch mehr Falscherkennungen zurück.

5 Aktivieren oder deaktivieren Sie die folgenden Optionen, um zusätzliche Kriterien für die Prüfung von noch nicht eingestuften Dateien zu verwenden:

- Dateien mit weniger als *x* Benutzer
- Dateien, die Benutzern weniger lang bekannt sind als *x* Tage
  Wenn noch nicht eingestufte Dateien diese Kriterien erfüllen, erkennt Download Insight die Dateien als bösartig.

6 Stellen Sie sicher, dass "Dateien, die von einer Intranet-Website heruntergeladen wurden, automatisch vertrauen" aktiviert ist.

Diese Option trifft auch auf Insight Lookup-Erkennungen zu.

7 Klicken Sie auf "Aktionen".

8 Unter "Bösartige Dateien" geben Sie eine erste Aktion und eine zweite Aktion an.

9 Unter "Noch nicht eingestufte Dateien" geben Sie die Aktion an.

10 Klicken Sie auf "OK".

11 Klicken Sie auf "Benachrichtigungen" und geben Sie an, ob eine Benachrichtigung angezeigt wird, wenn Download Insight eine Erkennung macht.

Sie können den Text der angezeigten Warnmeldung anpassen.

12 Klicken Sie auf "OK".

Anpassen von Virus- und Spyware-Scan-Einstellungen

Standardmäßig gewährt Symantec Endpoint Protection Ihrem Computer den erforderlichen Schutz vor Viren und Sicherheitsrisiken. Wenn Sie einen nicht-verwalteten Client haben, sollten Sie einige die Scaneinstellungen konfigurieren.

Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58.

So passen Sie einen benutzerdefinierten Scan an

1 Klicken Sie in der Seitenleiste des Clients auf "Scannen auf Bedrohungen".

2 Klicken Sie auf der Seite "Scannen auf Bedrohungen" mit der rechten Maustaste auf einen Scan und klicken auf "Bearbeiten".

3 Führen Sie auf der Registerkarte "Scan-Optionen" eine der folgenden Aufgaben aus:

- Klicken Sie auf "Insight-Suche", um Einstellungen für die Insight-Suche zu ändern.

Die Einstellungen für die Insight-Suche sind den Download Insight-Einstellungen ähnlich.
Siehe "Anpassen der Download Insight-Einstellungen" auf Seite 81.

- Um weniger Dateitypen für den Scan anzugeben, klicken Sie auf "Ausgewählte Erweiterungen" und anschließend auf "Erweiterungen".

  Hinweis: Benutzerdefinierte Scans scannen immer die Erweiterungen von Container-Dateien, es sei denn, dass Sie die Option für die komprimierte Datei unter "Erweitert" deaktivieren, oder dass Sie Ausnahmen für die Container-Erweiterungen erstellen.

- Klicken Sie auf "Aktionen", um anzugeben, welche erste und zweite Aktion der Client an einer infizierten Datei ausführen soll.
- Um Benachrichtigungsoptionen anzugeben, klicken Sie auf "Benachrichtigungen".
  Sie können die Benachrichtigungen, die in der Windows 8-Benutzeroberfläche angezeigt werden, separat aktivieren oder deaktivieren.
  Siehe "Verwalten von Symantec Endpoint Protection-Popup-Benachrichtigungen auf Windows 8-Computern" auf Seite 99.
- Um erweiterte Optionen für komprimierte Dateien, Backups und Feinabstimmung zu konfigurieren, klicken Sie auf "Erweitert".
  Sie können die Feinabstimmungsoptionen ändern, um Ihre Clientcomputerleistung zu verbessern.

Um weitere Informationen zu den Optionen in jedem Dialogfeld zu erhalten, klicken Sie auf "Hilfe".

4 Klicken Sie auf "OK".

So ändern Sie globale Scaneinstellungen

1 Führen Sie einen der folgenden Schritte aus:

- Auf dem Client klicken Sie in der Seitenleiste auf "Einstellungen ändern", und neben "Viren- und Spyware-Schutz" klicken Sie auf "Einstellungen konfigurieren"
- Auf dem Client klicken Sie in der Seitenleiste auf "Scannen auf Bedrohungen" und dann auf "Globale Scaneinstellungen anzeigen".

2 Ändern Sie auf der Registerkarte "Globale Einstellungen" unter "Scanoptionen" die Einstellungen für Insight oder Bloodhound.

3 Um Scanausnahmen anzuzeigen oder zu erstellen, klicken Sie auf "Liste anzeigen". Klicken Sie auf "Schließen", nachdem Sie Ausnahmen angezeigt oder erstellt haben.

4 Unter "Protokollaufbewahrung" oder "Internet-Browser-Schutz" nehmen Sie die gewünschten Änderungen vor.

5 Klicken Sie auf "OK".

So passen Sie Auto-Protect an

1 Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".

2 Klicken Sie neben "Viren- und Spyware-Schutz" auf "Einstellungen konfigurieren".

3 Führen Sie auf einer beliebigen Registerkarte "Auto-Protect" die folgenden Aufgaben aus:

- Um weniger Dateitypen für den Scan anzugeben, klicken Sie auf "Ausgewählte" und anschließend auf "Erweiterungen".
- Klicken Sie auf "Aktionen", um anzugeben, welche erste und zweite Aktion der Client an einer infizierten Datei ausführen soll.
- Um Benachrichtigungsoptionen anzugeben, klicken Sie auf "Benachrichtigungen".

Um weitere Informationen zu den Optionen in jedem Dialogfeld zu erhalten, klicken Sie auf "Hilfe".

4 Auf der Registerkarte "Auto-Protect" klicken Sie auf "Erweitert".

Sie können Optionen für den Dateicache sowie Optionen für Risikoverfolgung und Backups ändern. Sie können diese Optionen ändern, um Ihre Computerleistung zu verbessern.

5 Klicken Sie auf "Netzwerk", um Einstellungen für vertrauenswürdige Dateien auf Remote-Computern und das Festlegen eines Netzwerkcaches zu ändern.

6 Klicken Sie auf "OK".

Konfigurieren von Aktionen für Malware- und Sicherheitsrisikoerkennungen

Sie können die Aktionen konfigurieren, die der Symantec Endpoint Protection-Client beim Erkennen von Malware oder Sicherheitsrisiken ausführen soll. Sie können angeben, welche Aktion zuerst ausgeführt werden soll, und eine Ersatzaktion, falls die erste Aktion fehlschlägt.

Hinweis: Wenn Ihr Computer von einem Administrator verwaltet wird und diese Optionen ein Vorhängeschloss-Symbol aufweisen, können Sie diese nicht ändern, da sie durch Ihren Administrator gesperrt wurden.

Aktionen für alle Scans können auf dieselbe Art und Weise konfiguriert werden. Jeder Scan verfügt über eine eigene Aktionskonfiguration. Sie können verschiedene Aktionen für verschiedene Scans konfigurieren.

Hinweis: Sie konfigurieren Aktionen für Dowload Insight und SONAR separat.

Siehe "Anpassen von Virus- und Spyware-Scan-Einstellungen" auf Seite 82.

Siehe "Anpassen der Download Insight-Einstellungen" auf Seite 81.

Siehe "Ändern von SONAR-Einstellungen" auf Seite 106.

Sie können auf "Hilfe" klicken, um weitere Informationen über die Optionen zu erhalten, die im Verfahren verwendet werden.

So konfigurieren Sie Aktionen für Malware- und Sicherheitsrisikoerkennungen

1. Im Client klicken Sie in der Seitenleiste auf "Einstellungen ändern" oder "Scannen auf Bedrohungen".
2. Führen Sie einen der folgenden Schritte aus:
   - Neben "Viren- und Spyware-Schutz" klicken Sie auf "Einstellungen konfigurieren", und dann klicken Sie auf jeder Auto-Protect-Registerkarte auf "Aktionen".
   - Wählen Sie einen Scan aus und klicken Sie dann mit der rechten Maustaste und wählen "Bearbeiten" aus, und anschließend klicken Sie auf "Scanoptionen".
3. Klicken Sie auf "Aktionen".
4. Wählen Sie im Dialogfeld "Scan-Aktionen" in der Verzeichnisstruktur die Kategorie oder Unterkategorie unter "Malware" oder "Sicherheitsrisiken" aus.

   Standardmäßig wird jede Unterkategorie automatisch so konfiguriert, dass die für die gesamte Kategorie festgelegten Aktionen verwendet werden.

   Die Kategorien ändern sich dynamisch im Laufe der Zeit, wenn Symantec neue Informationen über Risiken erhält.
5. Führen Sie eine der folgenden Aktionen aus, um Aktionen nur für eine Unterkategorie zu konfigurieren:

- Aktivieren Sie das Kontrollkästchen "Für Malware konfigurierte Aktionen überschreiben" und legen Sie anschließend die Aktionen nur für diese Unterkategorie fest.

  Hinweis: Es gäbe möglicherweise eine einzelne Unterkategorie unter einer Kategorie, abhängig davon, wie Symantec derzeit Risiken klassifiziert. Beispielsweise gäbe es unter "Malware" möglicherweise eine einzelne Unterkategorie namens "Viren".

- Aktivieren Sie das Kontrollkästchen "Für Sicherheitsrisiken konfigurierte Aktionen überschreiben" und legen Sie anschließend die Aktionen nur für diese Unterkategorie fest.

6 Wählen Sie die erste und zweite Aktion aus den folgenden Optionen aus:

Von Risiko bereinigen

Entfernt den Virus aus der infizierten Datei. Diese Einstellung ist standardmäßig die erste Aktion bei einer Vireninfektion.

Hinweis: Diese Aktion ist nur als erste Aktion bei Viren verfügbar. Sie trifft nicht auf Sicherheitsrisiken zu.

Diese Einstellung sollte immer die erste Aktion für Viren sein. Wenn der Client einen Virus erfolgreich aus einer Datei entfernt, müssen Sie keine weiteren Schritte ausführen. Ihr Computer ist frei von Viren, sodass nicht länger die Gefahr besteht, dass sich die Infektion auf andere Bereiche des Computers ausbreitet.

Beim Bereinigen einer Datei entfernt der Client den Virus aus der infizierten Datei, dem Boot-Sektor oder aus Partitionstabellen. Er unterbindet auch die Möglichkeit einer Verbreitung des Virus. Normalerweise findet und entfernt der Client einen Virus, bevor dieser auf Ihrem Computer Schaden anrichten kann. Standardmäßig erstellt der Client ein Backup der Datei.

In einigen Fällen ist die bereinigte Datei jedoch nicht verwendbar. Der Virus könnte zu viel Schaden verursacht haben.

Manche infizierte Dateien können nicht bereinigt werden.

Hinweis: Symantec Endpoint Protection bereinigt keine Malware, die in Anwendungen und Dateien im Windows 8-Stil erkannt wird. Symantec Endpoint Protection löscht die Erkennung stattdessen.

Bedrohung isolieren	Verschiebt die infizierte Datei von ihrem ursprünglichen Speicherort in den Quarantänebereich. Infizierte Dateien innerhalb des Quarantänebereichs können keine Viren verbreiten. Wenn es sich um einen Virus handelt, wird die infizierte Datei von ihrem ursprünglichen Speicherort in die Quarantäne verschoben. Diese Einstellung ist standardmäßig die zweite Aktion bei einer Vireninfektion. Bei Sicherheitsrisiken verschiebt der Client die infizierten Dateien von ihrem ursprünglichen Speicherort in die Quarantäne und versucht, jegliche Auswirkungen zu entfernen oder zu reparieren. Diese Einstellung ist standardmäßig die erste Aktion bei Sicherheitsrisiken. Die Quarantäne enthält Aufzeichnungen aller durchgeführter Aktionen. Sie können den Status wiederherstellen, in dem sich der Computer vor der Entfernung des Risikos durch den Client befand. **Hinweis:** Symantec Endpoint Protection isoliert Malware, die in Anwendungen und Dateien im Windows 8-Stil erkannt wird, nicht. Symantec Endpoint Protection löscht die Erkennung stattdessen.
Bedrohung löschen	Löscht die infizierte Datei von der Festplatte Ihres Computers. Wenn der Client eine Datei nicht löschen kann, werden Informationen über die vom Client durchgeführten Aktionen im Dialogfeld "Benachrichtigung" angezeigt. Diese Informationen sind auch im Ereignisprotokoll enthalten. Verwenden Sie diese Aktion nur, wenn Sie die Datei durch eine viren- und risikofreie Backup-Kopie ersetzen können. Wenn der Client ein Risiko löscht, wird es permanent gelöscht. Die infizierte Datei kann nicht aus dem Papierkorb wiederhergestellt werden. **Hinweis:** Seien Sie vorsichtig beim Verwenden dieser Aktion, wenn Sie Aktionen für Sicherheitsrisiken konfigurieren. In manchen Fällen kann das Löschen von Sicherheitsrisiken dazu führen, dass Anwendungen ihre Funktionalität verlieren.

Nichts unternehmen (nur protokollieren)	Belässt die Datei unverändert in ihrem Zustand. Wenn Sie diese Aktion für Viren verwenden, bleibt der Virus in den infizierten Dateien. Der Virus kann sich auf andere Teile Ihres Computers verbreiten. Es wird ein entsprechender Eintrag in das Risikoprotokoll eingefügt, um die infizierte Datei zu erfassen. Sie können "Nichts unternehmen (nur protokollieren)" als zweite Aktion für Malware und Sicherheitsrisiken verwenden. Löschen Sie diese Aktion nicht, wenn Sie automatisierte Scans großen Umfangs durchführen, z. B. geplante Scans. Verwenden Sie diese Aktion, wenn Sie die Scanergebnisse anzeigen und später zusätzliche Aktionen ausführen möchten. Solch eine zusätzliche Aktion könnte das Verschieben der Datei in die Quarantäne sein. Bei Sicherheitsrisiken nimmt diese Aktion keine Änderung an der infizierten Datei vor und es wird ein entsprechender Eintrag in das Risikoprotokoll eingefügt, um die infizierte Datei zu erfassen. Mit dieser Option können Sie manuell steuern, wie der Client ein Sicherheitsrisiko handhabt. Diese Einstellung ist standardmäßig die zweite Aktion bei Sicherheitsrisiken. Ihr Administrator sendet möglicherweise eine benutzerdefinierte Nachricht, in der er erklärt, wie Sie vorgehen müssen.

7 Wiederholen Sie diese Schritte bei jeder Kategorie, für die Sie bestimmte Aktionen festlegen möchten, und klicken Sie dann auf "OK".

8 Wenn Sie eine Sicherheitsrisikokategorie ausgewählt haben, können Sie benutzerdefinierte Aktionen für eine oder mehrere bestimmte Instanzen dieser Sicherheitsrisikokategorie auswählen. Sie können ein Sicherheitsrisiko vom Scan ausschließen. Möglicherweise möchten Sie ein Adware-Programm ausschließen, das Sie für Ihre Arbeit benötigen.

9 Klicken Sie auf "OK".

Infos zum Ausschließen von Elementen von Scans

Bei Ausnahmen handelt es sich um bekannte Sicherheitsrisiken, Dateien, Dateierweiterungen und Prozesse, die Sie aus einem Scan ausgeschlossen werden sollen. Wenn Sie Ihren Computer gescannt haben und wissen, dass bestimmte Dateien sicher sind, können Sie sie ausschließen. In manchen Fällen können

Ausnahmen die Scanzeit reduzieren und die Systemleistung erhöhen. Normalerweise brauchen Sie keine Ausnahmen zu erstellen.

Bei verwalteten Clients hat Ihr Administrator unter Umständen Ausnahmen für Ihre Scans erstellt. Wenn Sie eine Ausnahme erstellen, die mit einer vom Administrator definierten Ausnahme in Konflikt steht, hat die vom Administrator definierte Ausnahme Vorrang. Ihr Administrator kann Sie auch daran hindern, irgendwelche Typen von Ausnahmen zu konfigurieren.

Hinweis: Wenn Ihre E-Mail-Anwendung alle E-Mails in einer einzigen Datei speichert, sollten Sie eine Dateiausnahme erstellen, um die Posteingangsdatei von den Scans auszuschließen. Standardmäßig isolieren Scans Viren. Wenn ein Scan einen Virus in der Posteingangsdatei erkennt, isoliert der Scan den gesamten Posteingang. In diesem Fall können Sie auf Ihre E-Mails nicht zugreifen.

Tabelle 4-9 Ausnahmetypen

Ausnahmetyp	Beschreibung
Datei	Trifft auf Virus und Spyware-Scans zu Scans ignorieren die Datei, die Sie auswählen.
Ordner	Gilt für Virus und Spyware-Scans oder SONAR bzw. für beide Scans ignorieren den Ordner, den Sie auswählen.
Bekannte Risiken	Trifft auf Virus und Spyware-Scans zu Scans ignorieren jedes bekannten Risiko, das Sie auswählen.
Erweiterungen	Trifft auf Virus und Spyware-Scans zu Scans ignorieren alle Dateien mit den angegebenen Erweiterungen.
Webdomäne	Trifft auf Virus und Spyware-Scans zu Download Insight ignoriert die angegebene vertrauenswürdige Webdomäne.
Anwendung	Trifft auf Virus- und Spyware-Scans und SONAR zu Scans ignorieren, protokollieren, isolieren oder beenden die Anwendung, die Sie hier angeben.

Ausnahmetyp	Beschreibung
DNS- oder Hostdateiänderung	Trifft auf SONAR zu Scans ignorieren, protokollieren oder blockieren eine Anwendung oder fordern den Benutzer zu einer Eingabe auf, wenn eine bestimmte Anwendung versucht, DNS-Einstellungen oder eine Hostdatei zu ändern.

Siehe "Ausschließen von Elementen von Scans" auf Seite 91.

Ausschließen von Elementen von Scans

Ausnahmen sind bekannte Sicherheitsrisiken, Dateien, Ordner, Dateierweiterungen, Webdomänen oder Anwendungen, die Sie von Scans ausschließen möchten. Wenn Sie Ihren Computer gescannt haben und wissen, dass bestimmte Dateien sicher sind, können Sie sie ausschließen. In manchen Fällen können Ausnahmen die Scanzeit reduzieren und die Systemleistung erhöhen. Sie können auch Ausnahmen für Anwendungen erstellen, die versuchen, eine DNS- oder Hostdateiänderung vorzunehmen. Gewöhnlich brauchen Sie keine Ausnahmen zu erstellen.

Bei verwalteten Clients hat Ihr Administrator unter Umständen Ausnahmen für Ihre Scans erstellt. Wenn Sie eine Ausnahme erstellen, die mit einer vom Administrator definierten Ausnahme in Konflikt steht, hat die vom Administrator definierte Ausnahme Vorrang.

SONAR unterstützt keine Dateiausnahmen. Verwenden Sie eine Anwendungsausnahme, um eine Datei von SONAR auszuschließen.

Hinweis: Auf der Server Core-Installation von Windows Server 2008 können sich die Dialogfelder von denen in diesen Verfahren beschriebenen Dialogfeldern unterscheiden.

So schließen Sie Elemente von Sicherheitsrisiko-Scans aus

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Klicken Sie neben "Ausnahmen" auf "Einstellungen konfigurieren".
3. Im Dialogfeld "Ausnahmen" klicken Sie unter "Benutzerdefinierte Ausnahmen" auf "Hinzufügen > Sicherheitsrisikoausnahmen".
4. Wählen Sie einen der folgenden Ausnahmetypen aus:
   - Bekannte Risiken

- Datei
- Ordner
- Erweiterungen
- Webdomäne

5 Führen Sie einen der folgenden Schritte aus:

- Bei bekannten Risiken aktivieren Sie die Sicherheitsrisiken, die Sie von Scans ausschließen möchten.
  Falls Sie ein Ereignis protokollieren möchten, wenn das Sicherheitsrisiko erkannt und ignoriert wird, aktivieren Sie "Protokollieren, wenn das Sicherheitsrisiko erkannt wird".
- Für Dateien oder Ordner wählen Sie die Datei oder den Ordner, die bzw. den Sie ausschließen möchten, oder geben Sie einen Datei- oder Ordnernamen ein.
  Wählen Sie den Scan-Typ ("Alle Scans", "Auto-Protect" oder "Geplant und nach Bedarf") und klicken Sie dann auf "OK".
- Bei Erweiterungen geben Sie die Erweiterung ein, die Sie ausschließen möchten.
  Sie können nur einen einen Erweiterungsnamen in das Textfeld aufnehmen. Wenn Sie mehrere Erweiterungen eingeben, behandelt der Client den Eintrag wie einen einzelnen Erweiterungsnamen.
- Für Domänen geben Sie eine Website oder eine IP-Adresse ein, die Sie von der Download-Insight- und SONAR-Erkennung ausschließen möchten.

6 Klicken Sie auf "OK".

So schließen Sie einen Ordner von SONAR aus

1 Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2 Klicken Sie neben "Ausnahmen" auf "Einstellungen konfigurieren".
3 Klicken Sie im Dialogfeld "Ausnahmen" unter "Benutzerdefinierte Ausnahmen" auf "Hinzufügen > Ausnahmen für SONAR > Ordner".
4 Wählen Sie den Ordner, den Sie ausschließen möchten, aktivieren oder deaktivieren Sie "Unterordner einschließen" und klicken Sie dann auf "OK".
5 Klicken Sie auf "Schließen".

So ändern Sie, wie alle Scans eine Anwendung behandeln

1 Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2 Klicken Sie neben "Ausnahmen" auf "Einstellungen konfigurieren".

3 Im Dialogfeld "Ausnahmen" klicken Sie unter "Benutzerdefinierte Ausnahmen" auf "Hinzufügen > Anwendungsausnahme".

4 Wählen Sie den Dateinamen der Anwendung aus

5 Wählen Sie im Dropdown-Feld "Aktion" die Option "Ignorieren", "Nur protokollieren", "Quarantäne", "Beenden" oder "Entfernen".

6 Klicken Sie auf "OK".

7 Klicken Sie auf "Schließen".

Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58.

Siehe "Infos zum Ausschließen von Elementen von Scans" auf Seite 89.

Verwalten von isolierten Dateien auf Ihrem Clientcomputer

Standardmäßig versucht Symantec Endpoint Protection, einen Virus von einer infizierten Datei zu bereinigen, wenn er erkannt wird. Wenn die Datei nicht bereinigt werden kann, legt der Scan die Datei in der Quarantäne auf Ihrem Computer ab. Bei Sicherheitsrisiken verschieben Scans infizierte Dateien in die Quarantäne und beheben alle Nebenwirkungen des Sicherheitsrisikos. Download Insight und SONAR isolieren möglicherweise auch Dateien.

Siehe "Isolieren von Dateien" auf Seite 95.

Tabelle 4-10 Verwalten von isolierten Dateien auf Ihrem Clientcomputer

Aufgabe	Beschreibung
Wiederherstellen einer isolierten Datei an ihrem ursprünglichen Speicherort	Manchmal gibt es für eine bereinigte Datei keinen Ablageort, an dem sie wiederhergestellt werden kann. Ein infizierter Dateianhang beispielsweise kann von einer E-Mail gelöst und im Quarantänebereich abgelegt worden sein. Sie müssen dann die Datei freigeben und einen Ablageort angeben.
Manuell ein Element isolieren	Sie können eine Datei manuell isolieren, indem Sie sie der Quarantäne hinzufügen oder indem Sie die Datei in Virus- und Spyware- oder SONAR-Protokollen auswählen. Siehe "Isolieren einer Datei aus dem Risiko- oder Scanprotokoll" auf Seite 96.

Aufgabe	Beschreibung
Permanentes Löschen der Dateien aus der Quarantäne	Sie können die nicht mehr benötigten Dateien aus dem Quarantänebereich löschen. Sie können auch eine Zeit festlegen, nach der die Dateien automatisch gelöscht werden. **Hinweis:** Ihr Administrator kann festlegen, wie viele Tage ein Element im Quarantänebereich bleiben kann. Nach Ablauf dieser Zeit wird es automatisch gelöscht.
Neuscannen von Dateien in der Quarantäne, nachdem Sie neue Definitionen erhalten	Wenn Sie Definitionen aktualisieren, werden Dateien in der Quarantäne möglicherweise automatisch gescannt, bereinigt und wiederhergestellt. Bei einigen Dateien erscheint der Reparaturassistent. Befolgen Sie die Bildschirmanweisungen, um den Neuscan und die Reparatur abzuschließen. Sie können auch Virus-infizierte Dateien in der Quarantäne manuell erneut scannen.
Exportieren von Quarantäneinformationen	Sie können den Inhalt der Quarantäne entweder in eine kommagetrennte Datei (.csv) oder in eine Microsoft Access-Datenbank-Datei (.mdb) exportieren.
Senden von infizierte Dateien in der Quarantäne an Symantec Security Response	Nachdem Elemente in der Quarantäne erneut gescannt wurden, sollten Sie eine Datei, die weiterhin infiziert ist, an Symantec Security Response zur weiteren Analyse senden. Siehe "Manuelles Senden einer potenziell infizierten Datei an Symantec Security Response zur Analyse" auf Seite 96.
Löschen von Backup-Objekten	Bevor er versucht, Objekte zu bereinigen oder zu reparieren, erstellt der Client standardmäßig Backup-Kopien von den infizierten Objekten. Nachdem der Client erfolgreich einen Virus entfernt hat, sollten Sie das Objekt manuell aus der Quarantäne löschen, weil das Daten-Backup noch infiziert ist.

Aufgabe	Beschreibung
Dateien automatisch aus der Quarantäne löschen	Sie können den Client so einrichten, dass er automatisch Elemente aus der Quarantäne nach einem angegebenen Zeitintervall entfernt. Sie können auch angeben, dass der Client Objekte entfernt, wenn der Ordner, in dem die Objekte gespeichert sind, eine bestimmte Größe erreicht. Diese Konfiguration verhindert, dass sich größere Mengen Dateien ansammeln, wenn Sie diese nicht manuell löschen. Siehe "Dateien automatisch aus der Quarantäne löschen" auf Seite 97.

Isolieren von Dateien

Wenn der Client eine infizierte Datei in die Quarantäne verschiebt, können der Virus oder das Risiko Ihren Computer oder andere Computer im Netzwerk nicht infizieren. Jedoch bereinigt die Quarantäne-Aktion nicht das Risiko. Das Risiko bleibt auf Ihrem Computer, bis der Client das Risiko bereinigt oder die Datei gelöscht hat. Sie haben keinen Zugriff auf die Datei, aber Sie können die Datei aus der Quarantäne entfernen.

Wenn Sie Ihren Computer mit neuen Virendefinitionen aktualisieren, überprüft der Client automatisch den Quarantänebereich. Sie können die Objekte im Quarantänebereich erneut scannen. Mit den neuesten Definitionen können die isolierten Dateien möglicherweise bereinigt oder repariert werden.

Die meisten Viren können isoliert werden. Boot-Sektor-Viren befinden sich im Boot-Sektor oder in den Partitionstabellen eines Computers. Diese Elemente können nicht in den Quarantänebereich verschoben werden. Manchmal erkennt der Client einen unbekannten Virus, der nicht mit den aktuellen Virendefinitionen beseitigt werden kann. Wenn Sie eine Datei als infiziert erachten, aber Scans keine Infektion erkennen, müssen Sie die Datei manuell isolieren.

Hinweis: Die Sprache des Betriebssystems, auf dem Sie den Client ausführen, kann eventuell einige Zeichen im Risikonamen nicht erkennen. Wenn das Betriebssystem die Zeichen nicht deuten kann, erscheinen die Zeichen als Fragezeichen in den Benachrichtigungen. Beispielsweise könnten einige Unicode-Risikonamen Double-Byte-Zeichen enthalten. Auf den Computern, die den Client auf einem englischen Betriebssystem ausführen, erscheinen diese Zeichen als Fragezeichen.

Siehe "Verwalten von isolierten Dateien auf Ihrem Clientcomputer" auf Seite 93.

Isolieren einer Datei aus dem Risiko- oder Scanprotokoll

Ob der Client die von Ihnen ausgewählte Aktion durchführen kann oder nicht, hängt von der voreingestellten Aktion beim Auffinden einer Bedrohung ab. Sie können eine Datei mit dem Risiko- oder Scan-Protokoll später isolieren.

Siehe "Isolieren von Dateien" auf Seite 95.

Siehe "Verwalten von isolierten Dateien auf Ihrem Clientcomputer" auf Seite 93.

So isolieren Sie eine Datei aus dem Risiko- oder Scanprotokoll

1. Klicken Sie im Client auf "Protokolle anzeigen".
2. Klicken Sie neben "Viren- und Spyware-Schutz" auf "Protokoll anzeigen" und wählen Sie anschließend "Risikoprotokoll" oder "Scanprotokoll" aus.
3. Wählen Sie die Datei aus, die Sie isolieren möchten, und klicken Sie anschließend auf "Isolieren".
4. Klicken Sie auf "OK" und anschließend auf "Schließen".

Manuelles Senden einer potenziell infizierten Datei an Symantec Security Response zur Analyse

Wenn Sie ein infiziertes Element von Ihrer Quarantäneliste an Symantec Security Response senden, kann Symantec Security Response dieses Element analysieren, um sicherzustellen, dass es nicht infiziert ist. Symantec Security Response verwendet diese Daten auch, um vor neuen oder sich entwickelnden Bedrohungen zu schützen.

Hinweis: Die Übermittlungsoption ist nicht verfügbar, wenn Ihr Administrator diese Übermittlungstypen deaktiviert.

Siehe "Verwalten von isolierten Dateien auf Ihrem Clientcomputer" auf Seite 93.

So senden Sie eine Datei vom Quarantänebereich an Symantec Security Response

1. Klicken Sie im Client in der Seitenleiste auf "Quarantäne anzeigen".
2. Wählen Sie die Datei in der Liste der isolierten Elemente aus.
3. Klicken Sie auf "Senden".
4. Folgen Sie den Anweisungen des Assistenten, um die erforderlichen Informationen zu sammeln und die Datei zur Analyse an Symantec Security Response weiterzuleiten.

Dateien automatisch aus der Quarantäne löschen

Sie können Ihre Software so einrichten, dass Elemente nach einem angegebenen Zeitraum automatisch aus der Quarantäne-Liste entfernt werden. Sie können auch angeben, dass der Client Objekte entfernt, wenn der Ordner, in dem die Objekte gespeichert sind, eine bestimmte Größe erreicht. Diese Konfiguration verhindert, dass sich größere Mengen Dateien ansammeln, wenn Sie diese nicht manuell löschen.

Siehe "Verwalten von isolierten Dateien auf Ihrem Clientcomputer" auf Seite 93.

So löschen Sie Dateien automatisch aus dem Quarantänebereich

1. Klicken Sie im Client in der Seitenleiste auf "Quarantäne anzeigen".
2. Klicken Sie auf "Bereinigungsoptionen".
3. Wählen Sie im Dialogfeld "Bereinigungsoptionen" eine der folgenden Registerkarten aus:
   - Isolierte Elemente
   - Backup-Elemente
   - Reparierte Elemente
4. Aktivieren oder deaktivieren Sie "Gespeicherte Dauer überschreitet", um die Fähigkeit des Clients, die Dateien nach Ablauf der konfigurierten Zeit zu aktivieren oder deaktivieren.
5. Wenn Sie das Kontrollkästchen "Der gespeicherte Zeitraum übersteigt" aktivieren, klicken Sie auf einen Pfeil, um den bestimmten Zeitraum einzugeben oder geben Sie ihn ein.
6. Wählen Sie die Maßeinheit der Zeit aus der Dropdown-Liste. Die Vorgabe ist 30 Tage.
7. Wenn Sie das Kontrollkästchen "Gesamtordnergröße übersteigt" aktivieren, geben Sie die maximal zuzulassende Ordnergröße in Megabyte an. Die Vorgabe ist 50 Megabyte.

   Wenn Sie beide Kontrollkästchen aktivieren, werden alle Dateien, die älter als die festgelegte Zeitspanne sind, zuerst gelöscht. Wenn die Größe des Ordners noch das von Ihnen gesetzte Limit übersteigt, löscht der Client die ältesten Dateien einzeln. Der Client löscht die ältesten Dateien, bis die Ordnergröße das Limit nicht mehr übersteigt.
8. Wiederholen Sie die Schritte 4 bis 7 auf allen anderen Registerkarten.
9. Klicken Sie auf "OK".

Aktivieren/Deaktivieren von Early Launch Anti-Malware (ELAM)

Early Launch Anti-Malware (ELAM) bietet Schutz beim Hochfahren des Computers, bevor Treiber anderer hersteller initialisiert werden. Bösartige Software kann geladen, da ein Treiber oder Rootkit angreifen kann, bevor das Betriebssystem vollständig hochgefahren ist und Symantec Endpoint Protection ausgeführt wird. Rootkits können sich vor Viren- und Spyware-Scans verbergen. Early Launch Anti-Malware erkennt diese Rootkits und bösartigen Treiber beim Systemstart.

Symantec Endpoint Protection beinhaltet einen Early Launch Anti-Malware-Treiber, der mit dem Early Launch Anti-Malware-Treiber von Microsoft zusammenarbeitet, um den Schutz zu gewährleisten. Die Einstellungen werden unter Microsoft Windows 8 unterstützt.

Hinweis: Sie können zwar keine Ausnahmen für einzelne ELAM-Erkennungen, aber eine globale Ausnahme erstellen, die alle bösartigen Treiber als unbekannt protokolliert.

Bei manchen ELAM-Erkennungen, für die Korrekturmaßnahmen erforderlich sind, müssen Sie eventuell Power Eraser ausführen. Power Eraser ist Teil des Support-Tools "Symantec Endpoint Protection".

So aktivieren bzw. deaktivieren Sie Early Launch Anti-Malware

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Klicken Sie neben "Viren- und Spyware-Schutz" auf "Einstellungen konfigurieren".
3. Aktivieren bzw. deaktivieren Sie auf der Registerkarte "Early Launch Anti-Malware" die Option "Early Launch Anti-Malware aktivieren".

   Der Early Launch Anti-Malware-Treiber von Windows muss aktiviert sein, damit diese Option in Kraft tritt.
4. Wenn Sie die Erkennungen nur protokollieren möchten, wählen Sie unter "Wenn Symantec Endpoint Protection einen potenziell bösartigen Treiber erkennt" die Option "Erkennung als 'Unbekannt' protokollieren, damit Windows das Laden des Treibers zulässt" aus.
5. Klicken Sie auf "OK'".

Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58.

Siehe "Fehlerbehebung bei Computerproblemen mit dem Symantec Endpoint Protection-Support-Tool" auf Seite 25.

Siehe "Ausschließen von Elementen von Scans" auf Seite 91.

Verwalten von Symantec Endpoint Protection-Popup-Benachrichtigungen auf Windows 8-Computern

Standardmäßig werden Popup-Benachrichtigungen auf der Metro-Benutzeroberfläche und dem Desktop für Malwareerkennungen und andere kritische Symantec Endpoint Protection-Ereignisse angezeigt.

Sie können die folgenden Aktionen durchführen, um die Popup-Benachrichtigungen zu verwalten:

- Ändern Sie im Client die globale Einstellung für die Metro-Benutzeroberflächen auf der Seite "Clientverwaltung - Einstellungen".
- Ändern Sie in Windows 8 die Benachrichtigungseinstellungen für das Betriebssystem.
  Symantec Endpoint Protection-Benachrichtigungen werden nur angezeigt, wenn Windows 8 entsprechend konfiguriert ist. Weitere Informationen finden Sie in der Dokumentation zu Windows 8.

Auf verwalteten Clients entscheidet möglicherweise Ihr Administrator, ob Popup-Benachrichtigungen in Windows 8 angezeigt werden.

Siehe "Reaktion auf Symantec Endpoint Protection-Popup-Benachrichtigungen auf Windows 8-Computern" auf Seite 34.

Senden von Informationen über Erkennungen an Symantec Security Response

Sie können Ihren Computer so konfigurieren, dass er Informationen über Erkennungen automatisch zur Analyse an Symantec Security Response sendet.

Symantec Security Response und das Global Intelligence Network verwenden diese übermittelten Informationen, um schnell Reaktionen auf neue und sich entwickelnde Sicherheitsbedrohungen zu formulieren. Die Daten, die Sie senden, verbessern die Fähigkeit von Symantec, auf Bedrohungen zu reagieren und den Schutz anzupassen. Symantec empfiehlt, dass Sie Übertragungen immer zulassen.

Siehe "Info über den Symantec Endpoint Protection-Client" auf Seite 11.

Sie können beschließen, folgende Datentypen zu senden:

- Dateibewertung

Informationen über die Dateien, die anhand ihrer Bewertung erkannt werden. Die Informationen über diese Dateien sind ein Beitrag für die Symantec Insight-Reputationsdatenbank und tragen dazu bei, Ihre Computer vor neuen Risiken zu schützen.

- Antivirus-Erkennungen
  Informationen über bei Viren- und Spyware-Scans erkannte Bedrohungen.
- Virenerkennung – Erweiterte heuristische Erkennungsübertragung
  Informationen über mögliche Bedrohungen, die von Bloodhound und anderen Viren- und Spyware-Heuristik-Scans erkannt werden.
  Diese Erkennungen laufen im Hintergrund ab und werden nicht im Risikoprotokoll verzeichnet. Informationen über diese Erkennungen werden zur statistischen Analyse verwendet.
- SONAR-Erkennungsübertragungen
  Informationen über von SONAR erkannten Bedrohungen. Dazu gehören Erkennungen mit niedrigem und hohem Risiko, Systemänderungsereignisse und verdächtiges Verhalten vertrauenswürdiger Anwendungen.
- SONAR-Heuristik
  SONAR-Heuristik-Erkennungen laufen im Hintergrund ab und werden nicht im Risikoprotokoll verzeichnet. Diese Informationen werden zur statistische Analyse verwendet.

Sie können auch manuell eine Probe an Response senden, entweder aus der Quarantäne oder über die Symantec-Website. Um eine Datei über die Symantec-Website zu senden, wenden Sie sich an den technischen Support von Symantec.

Siehe "Senden von Informationen über Erkennungen an Symantec Security Response" auf Seite 100.

Siehe "So trifft Symantec Endpoint Protection anhand von Bewertungsdaten Entscheidungen über Dateien" auf Seite 72.

Senden von Informationen über Erkennungen an Symantec Security Response

Symantec Endpoint Protection kann Computer schützen, indem die Informationen zum und vom Computer überwacht und Angriffsversuche blockiert werden.

Sie können Ihren Computer anpassen, um Informationen über erkannte Bedrohungen an Symantec Security Response zu senden. Symantec Security Response verwendet diese Informationen, um Ihre Clientcomputer vor neuen, gezielten und mutierenden Bedrohungen zu schützen. Alle von Ihnen übermittelte

Daten verbessern Symantecs Fähigkeit, auf Bedrohungen zu reagieren und den Schutz für Ihren Computer anzupassen. Symantec empfiehlt, dass Sie so viele Erkennungsinformationen wie möglich übermitteln.

Sie können auch manuell eine Virenprobe an Symantec Security Response von der Quarantäneseite aus senden. Die Quarantäneseite auch ermöglicht es Ihnen auch festzulegen, wie Elemente an Symantec Security Response gesendet werden.

So konfigurieren Sie Übertragungen an Symantec Security Response

1. Wählen Sie "Einstellungen ändern > Clientverwaltung".
2. Aktivieren Sie auf der Registerkarte "Übertragungen" die Option "Lässt diesen Computer ausgewählte anonyme Sicherheitsinformationen automatisch an Symantec weiterleiten". Mit dieser Option kann Symantec Endpoint Protection Informationen über Bedrohungen senden, die auf Ihrem Computer gefunden werden.

   Symantec empfiehlt, dass Sie diese Option aktiviert lassen.
3. Wählen Sie die zu sendenden Datentypen aus.

   Klicken Sie auf "Hilfe", um weitere Informationen zu diesen Optionen anzuzeigen.
4. Aktivieren Sie die Option "Insight-Lookups für die Erkennung von Bedrohungen zulassen", damit Symantec Endpoint Protection die Reputationsdatenbank von Symantec verwenden kann, um Entscheidungen über Bedrohungen zu treffen.
5. Klicken Sie auf "OK".

Siehe "Verwalten von isolierten Dateien auf Ihrem Clientcomputer" auf Seite 93.

Siehe "Senden von Informationen über Erkennungen an Symantec Security Response" auf Seite 99.

Informationen zum Client und dem Windows-Sicherheitscenter

Wenn Sie Windows Security Center (WSC) unter Windows XP mit Service Pack 2 oder Service Pack 3 verwenden, können Sie den Status von Symantec Endpoint Protection in WSC sehen.

Tabelle 4-11 zeigt Schutzstatus, wie in WSC beschrieben, an.

Tabelle 4-11 Status des Schutzes im WSC

Status des Symantec-Produkts	Status des Schutzes
Symantec Endpoint Protection ist nicht installiert	NICHT GEFUNDEN (rot)
Symantec Endpoint Protection ist mit vollem Schutz installiert	AKTIV (grün)
Symantec Endpoint Protection ist installiert und die Definitionen für Viren und Sicherheitsrisiken sind veraltet	VERALTET (rot)
Symantec Endpoint Protection ist installiert und Auto-Protect für das Dateisystem ist nicht aktiviert	INAKTIV (rot)
Symantec Endpoint Protection ist installiert, Auto-Protect für das Dateisystem ist nicht aktiviert und die Virus- und Sicherheitsrisikodefinitionen sind veraltet	INAKTIV (rot)
Symantec Endpoint Protection ist installiert und ccSvcHst wurde manuell deaktiviert	INAKTIV (rot)

Tabelle 4-12 zeigt den Symantec Endpoint Protection-Firewall-Status, wie in WSC beschrieben, an.

Tabelle 4-12 Firewall-Status im WSC

Status des Symantec-Produkts	Firewall-Status
Symantec-Firewall ist nicht installiert	NICHT GEFUNDEN (rot)
Symantec-Firewall ist installiert und aktiviert	AKTIV (grün)
Symantec-Firewall ist installiert, aber nicht aktiviert	INAKTIV (rot)
Symantec-Firewall ist nicht installiert oder aktiviert, aber eine Firewall anderer Hersteller ist installiert und aktiviert	AKTIV (grün)

Hinweis: In Symantec Endpoint Protection ist die Windows-Firewall standardmäßig deaktiviert.

Falls mehrere Firewalls aktiviert sind, wird vom Windows-Sicherheitscenter eine entsprechende Meldung ausgegeben.

Informationen zu SONAR

SONAR ist ein Echtzeitschutz, der potenziell bösartige Anwendungen erkennt, wenn sie auf dem Computer ausgeführt werden. SONAR bietet Schutz vor

neuartigen Angriffen, da es Bedrohungen erkennt, bevor entsprechende Viren- und Spywareerkennungsdefinitionen erstellt wurden.

SONAR verwendet Heuristiken sowie Reputationsdaten zum Erkennen neuer und unbekannter Bedrohungen. SONAR stellt einen besseren Schutz auf Clientcomputern bereit und ergänzt Ihren vorhandenen Virus and Spyware Protection, Angriffsschutz und Firewall-Schutz.

SONAR verwendet ein Heuristiksystem, das Symantecs Online-Informationsnetzwerk mit proaktiver lokaler Überwachung auf Computern nutzt, um neue Bedrohungen zu erkennen. SONAR erkennt auch Änderungen oder Verhalten auf Computern, die Sie überwachen sollten.

Hinweis: Auto-Protect verwendet auch Bloodhound, eine Art von Heuristik, zum Erkennen verdächtiger Verhaltensmuster in Dateien.

SONAR fügt möglicherweise Code in Anwendungen ein, die im Windows-Benutzermodus ausgeführt werden, um sie auf verdächtige Aktivitäten zu überwachen. In einigen Fällen kann diese Einfügung die Anwendungsleistung beeinträchtigen oder Probleme beim Ausführen der Anwendung verursachen. Sie können eine Ausnahme erstellen, um die Datei, den Ordner oder die Anwendung von diesem Typ der Überwachung auszuschließen.

Hinweis: SONAR fügt keinen Code in Anwendungen auf Clients mit Symantec Endpoint Protection 12.1 oder früher ein. Wenn Sie Symantec Endpoint Protection Manager 12.1.2 zur Verwaltung von Clients verwenden, wird eine SONAR-Dateiausnahme in einer Ausnahmerichtlinie auf veralteten Clients ignoriert. Wenn Sie eine veraltete Version von Symantec Endpoint Protection Manager zur Verwaltung von Clients verwenden, unterstützt die veraltete Richtlinie keine SONAR-Dateiausnahmen für Symantec Endpoint Protection 12.1.2-Clients. Sie können jedoch die SONAR-Codeeinbringung in Anwendungen auf diesen Clients verhindern, indem Sie eine Ausnahme für eine "Zu überwachende Anwendung" in der veralteten Richtlinie erstellen. Nachdem der Client die Anwendung gelernt hat, können Sie eine Anwendungsausnahme in der Richtlinie konfigurieren.

SONAR erkennt nicht den Anwendungstyp, sondern das Verhalten eines Prozesses. SONAR reagiert nur auf eine Anwendung, wenn sich diese böswillig verhält, unabhängig vom Typ. Beispiel: Wenn ein Trojaner oder Keylogger nicht böswillig agiert, wird er von SONAR nicht erkannt.

SONAR erkennt die folgenden Elemente:

Heuristische Bedrohungen	SONAR nutzt Heuristiken, um zu bestimmen, ob eine unbekannte Datei sich verdächtig verhält und möglicherweise ein hohes oder niedriges Risiko darstellt. Außerdem nutzt es Bewertungsdaten, um zu bestimmen, ob die Bedrohung ein hohes oder niedriges Risiko darstellt.
Systemänderungen	SONAR erkennt Anwendungen oder die Dateien, die versuchen, DNS-Einstellungen oder eine Hostdatei auf einem Clientcomputer zu ändern.
Vertrauenswürdige Anwendungen mit bösartigem Verhalten	Einige vertrauenswürdige Dateien könnten mit verdächtigem Verhalten verknüpft sein. SONAR erkennt diese Dateien als Ereignisse mit verdächtigem Verhalten. Beispiel: Eine gängige Anwendung zum gemeinsamen Nutzen von Dokumenten erzeugt Programmdateien.

Wenn Sie Auto-Protect deaktivieren, wird SONARs Fähigkeit eingeschränkt, Dateien mit hohem oder niedrigem Risiko zu erkennen. Wenn Sie Insight-Suchvorgänge (Bewertungsabfragen) deaktivieren, schränken Sie außerdem die SONAR-Erkennungsmöglichkeiten ein.

Siehe "Verwalten von SONAR auf Ihrem Clientcomputer" auf Seite 104.

Siehe "Ausschließen von Elementen von Scans" auf Seite 91.

Verwalten von SONAR auf Ihrem Clientcomputer

Sie verwalten SONAR als Teil des proaktiven Bedrohungsschutzes. Auf verwalteten Clients hat Ihr Administrator möglicherweise einige die Einstellungen gesperrt.

Tabelle 4-13 Verwalten von SONAR auf Ihrem Clientcomputer

Aufgabe	Beschreibung
Sicherstellen, dass SONAR aktiviert ist	Für den besten Schutz auf Ihrem Clientcomputer sollte SONAR aktiviert sein. SONAR ist standardmäßig aktiviert. Sie aktivieren SONAR, indem Sie den proaktiven Bedrohungsschutz aktivieren. Siehe "Info zum Aktivieren und das Deaktivieren des Schutzes, wenn Sie Probleme beheben müssen" auf Seite 50.

Aufgabe	Beschreibung
Sicherstellen, dass Insight-Suchvorgänge aktiviert sind	SONAR verwendet Reputationsdaten zusätzlich zu Heuristiken, um Erkennungen zu machen. Wenn Sie Insight-Suchvorgänge (Reputationsabfragen) deaktivieren, macht SONAR Erkennungen, indem nur Heuristiken verwendet werden. Die Rate von Falscherkennungen erhöht sich möglicherweise und der Schutz, den SONAR bietet, ist eingeschränkt. Siehe "Senden von Informationen über Erkennungen an Symantec Security Response" auf Seite 100.
Ändern der SONAR-Einstellungen	Sie können SONAR aktivieren oder deaktivieren. Sie können auch die Erkennungsaktion bei einigen Bedrohungstypen ändern, die SONAR erkennt. Sie können die Erkennungsaktion ändern, um Falscherkennungen zu reduzieren. Siehe "Ändern von SONAR-Einstellungen" auf Seite 106.
Erstellen von Ausnahmen für Anwendungen, die Sie als sicher einschätzen	SONAR erkennt möglicherweise Dateien oder Anwendungen, die Sie auf Ihrem Computer ausführen möchten. Sie können SONAR-Ausnahmen für die Dateien, Ordner oder Anwendungen auf der Seite "Ausnahmen > Einstellungen ändern" erstellen. Sie können auch eine Ausnahme für die Quarantäne erstellen. Siehe "Ausschließen von Elementen von Scans" auf Seite 91.
Verhindern der Prüfung einiger Anwendungen durch SONAR	In einigen Fällen kann eine Anwendung nicht ausführbar oder instabil werden, wenn SONAR zur Überprüfung einer Anwendung einen Code in diese einfügt. Sie können eine Datei- oder Anwendungsausnahme für die Anwendung erstellen. Siehe "Ausschließen von Elementen von Scans" auf Seite 91.
Informationen über SONAR-Erkennungen an Symantec Security Response senden	Symantec empfiehlt, dass Sie Informationen über Erkennungen an Symantec Security Response senden. Die Informationen helfen Symantec, Bedrohungen zu behandeln. Übertragungen sind standardmäßig aktiviert. Siehe "Senden von Informationen über Erkennungen an Symantec Security Response" auf Seite 100.

Siehe "Verwalten von Scans auf Ihrem Computer" auf Seite 58.

Siehe "Informationen zu den Scantypen" auf Seite 66.

Ändern von SONAR-Einstellungen

Sie können SONAR-Aktionen ändern, um die Rate von Falscherkennungen zu reduzieren. Sie können auch Benachrichtigungen für heuristische SONAR-Erkennungen ändern.

Siehe "Verwalten von SONAR auf Ihrem Clientcomputer" auf Seite 104.

Hinweis: Auf verwalteten Clients hat Ihr Administrator möglicherweise diese Einstellungen gesperrt.

So ändern Sie SONAR-Einstellungen

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Klicken Sie neben "Proaktiver Bedrohungsschutz" auf "Einstellungen konfigurieren".
3. Ändern Sie auf der Registerkarte "SONAR" die Aktionen für heuristische Bedrohungen mit hohem oder geringem Risiko.

   Sie können den aggressiven Modus bei Erkennungen mit geringem Risiko aktivieren. Diese Einstellung erhöht die SONAR-Empfindlichkeit für Erkennungen mit geringem Risiko. Sie erhöht möglicherweise die Falscherkennungen.
4. Optional ändern Sie die Benachrichtigungseinstellungen.
5. Auf der Registerkarte "Erkennung von verdächtigem Verhalten" ändern Sie die Aktion für Erkennungen mit hohem oder mit geringem Risiko. SONAR macht diese Erkennungen, wenn vertrauenswürdige Dateien verdächtigem Verhalten zugeordnet werden.
6. Auf der Registerkarte "Systemänderungsereignisse" ändern Sie die Scanaktion bei Erkennungen von Änderungen an den DNS-Server-Einstellungen oder an einer Hostdatei.
7. Klicken Sie auf "OK".

Kapitel 5

Verwalten der Firewall und der Intrusion Prevention

In diesem Kapitel werden folgende Themen behandelt:

- Verwalten des Firewall-Schutzes
- Verwalten von Firewall-Regeln
- Aktivieren oder Deaktivieren von Firewall-Einstellungen
- Zulassen oder Blockieren des Zugriffs von Anwendungen auf das Netzwerk
- Erstellen von Firewall-Regeln für Anwendungen beim Zugriff auf das Netzwerk von Ihrem Computer
- Konfigurieren des Clients, zum Blockieren von Datenverkehr bei aktivem Screensaver oder inaktiver Firewall
- Verwalten von Intrusion Prevention
- Wie Intrusion Prevention funktioniert
- Aktivieren oder Deaktivieren des Angriffsschutzes
- Konfigurieren der Intrusion Prevention-Benachrichtigungen

Verwalten des Firewall-Schutzes

Standardmäßig stellt der Symantec Endpoint Protection-Client die entsprechende Stufe des Firewall-Schutzes zur Verfügung, die Ihr Computer benötigt.

Ihr Administrator hat aber möglicherweise einige von den Firewall-Standardregeln und -Einstellungen geändert. Wenn Ihr Administrator Ihnen Rechte zum Ändern

des Firewall-Schutzes gegeben hat, können Sie die Firewall-Regeln oder die Firewall-Einstellungen ändern

Tabelle 5-1 beschreibt die Firewall-Aufgaben, die Sie durchführen können, um Ihren Computer zu schützen. Alle diese Aufgaben sind optional und können in beliebiger Reihenfolge durchgeführt werden.

Tabelle 5-1 Verwalten des Firewall-Schutzes

Aufgabe	Beschreibung
Infos zur Funktionsweise der Firewall	Erfahren Sie, wie die Firewall Ihren Computer vor Netzwerkangriffen schützt. Siehe "Funktionsweise einer Firewall" auf Seite 109.
Hinzufügen und Anpassen von Firewall-Regeln	Sie können neue Firewall-Regeln hinzufügen oder vorhandene Firewall-Regeln bearbeiten. Beispielsweise empfiehlt es sich, eine Anwendung zu blockieren, die Sie nicht auf Ihrem Computer ausführen möchten, wie z. B. eine Adware-Anwendung. Siehe "Verwalten von Firewall-Regeln" auf Seite 110. Sie können eine Firewall-Regel auch konfigurieren, damit Anwendungen auf das Netzwerk zugreifen können oder damit die Anwendungen am Zugreifen auf das Netzwerk gehindert werden. Siehe "Erstellen von Firewall-Regeln für Anwendungen beim Zugriff auf das Netzwerk von Ihrem Computer" auf Seite 124.
Konfigurieren von Firewall-Einstellungen	Zusätzlich zum Erstellen von Firewall-Regeln können Sie auch Firewall-Einstellungen aktivieren und konfigurieren, um Ihren Firewall-Schutz weiter zu erhöhen. Siehe "Aktivieren oder Deaktivieren von Firewall-Einstellungen" auf Seite 119.
Anzeigen von Firewall-Protokollen	Sie können den Firewall-Schutz-Status auf Ihrem Computer regelmäßig prüfen, um Folgendes festzulegen: ■ Die von Ihnen erstellten Firewall-Regeln funktionieren richtig. ■ Der Client blockierte alle Netzwerkangriffe. ■ Der Client blockierte alle Anwendungen, die ausgeführt werden sollten. Sie können das Datenverkehrsprotokoll und das Paketprotokoll verwenden, um den Firewall-Schutz-Status zu überprüfen. Standardmäßig ist das Paketprotokoll auf verwalteten Clients deaktiviert. Siehe "Info zu Protokollen" auf Seite 46. Siehe "Aktivieren des Paketprotokolls" auf Seite 49.

Aufgabe	Beschreibung
Anwendungen und bestimmten Datenverkehr blockieren oder zulassen	Für Extrasicherheit können Sie Netzwerkverkehr vom Zugreifen auf Ihren Computer in den folgenden Situationen blockieren. ■ Sie können Datenverkehr blockieren, wenn der Screensaver Ihres Computers eingeschaltet ist. ■ Sie können Datenverkehr blockieren, wenn die Firewall nicht ausgeführt wird. ■ Sie können Datenverkehr jederzeit blockieren. Siehe "Konfigurieren des Clients, zum Blockieren von Datenverkehr bei aktivem Screensaver oder inaktiver Firewall" auf Seite 126. ■ Sie können eine Meldung zulassen, blockieren oder anzeigen, um eine Anwendung das Zugreifen auf das Netzwerk zu erlauben oder sie zu blockieren. Diese Anwendungen werden bereits auf Ihrem Computer ausgeführt. Siehe "Zulassen oder Blockieren des Zugriffs von Anwendungen auf das Netzwerk" auf Seite 123. Siehe "Erstellen von Firewall-Regeln für Anwendungen beim Zugriff auf das Netzwerk von Ihrem Computer" auf Seite 124.
Aktivieren oder Deaktivieren der Firewall	Sie können den Netzwerkbedrohungsschutz für Fehlerbehebungzwecke vorübergehend deaktivieren. Beispielsweise möchten Sie ihn deaktivieren, damit Sie eine bestimmte Anwendung öffnen können. Siehe "Aktivieren oder Deaktivieren des Schutzes auf dem Client-Computer" auf Seite 52.

Funktionsweise einer Firewall

Eine Firewall führt folgende Aufgaben aus:

- Hindert alle nicht autorisierten Benutzer am Zugriff auf die Computer und Netzwerke in Ihrer Organisation, die mit dem Internet eine Verbindung herstellen
- Überwacht die Kommunikation zwischen Ihren Computern und anderen Computern im Internet
- Erstellt einen Schutzschild, der Zugriffe auf Daten auf Ihrem Computer zulässt oder blockiert.
- Warnt Sie vor Verbindungsversuchen von anderen Computern
- Warnt Sie vor Verbindungsversuchen von Anwendungen auf Ihrem Computer, die eine Verbindung zu anderen Computern herstellen.

Die Firewall überprüft die Datenpakete, die über das Internet übertragen werden. Ein Paket ist ein separates Datenstück, das Teil des Informationsflusses zwischen zwei Computern ist. Die Pakete werden am Ziel wieder zusammengesetzt und erscheinen als ununterbrochener Datenfluss.

Pakete enthalten folgende Informationen:

- Sendende Computer
- Beabsichtigte Empfänger
- Umgang mit Paketdaten
- Ports, die die Pakete empfangen

Ports sind die Kanäle, die den Datenstrom aus dem Internet teilen. Anwendungen, die auf einem Computer ausgeführt werden, hören die Ports ab. Die Anwendungen akzeptieren die Daten, die an die Ports gesendet werden.

Bei Netzwerkangriffen werden Schwachstellen anfälliger Anwendungen genutzt. Angreifer nutzen diese Schwachstellen, um Pakete mit bösartigem Programmiercode an Ports zu senden. Wenn anfällige Anwendungen die Ports abhören, erhalten die Angreifer durch bösartigen Code Zugriff auf den Computer.

Siehe "Verwalten des Firewall-Schutzes" auf Seite 107.

Verwalten von Firewall-Regeln

Firewall-Regeln steuern, wie die Firewall Clientcomputer vor bösartigen eingehenden Datenverkehr und Anwendungen schützt. Die Firewall prüft alle eingehenden und ausgehenden Pakete entsprechend der aktivierten Regeln. Sie lässt die Pakete zu oder blockiert sie, abhängig von den Firewall-Regel angegebenen Bedingungen.

Der Symantec Endpoint Protection-Client schließt zum Schutz Ihres Computers Standard-Firewall-Regeln ein. Jedoch können Sie die Firewall-Regeln für zusätzlichen Schutz ändern, wenn Ihr Administrator das zulässt oder wenn der Client nicht verwaltet ist.

Tabelle 5-2 enthält alle erforderlichen Informationen zum Verwalten von Firewall-Regeln.

Tabelle 5-2 Verwalten von Firewall-Regeln

Thema	Beschreibung
Funktionsweise und Komponenten von Firewall-Regeln	Bevor Sie die Firewall-Regeln ändern, sollten Sie folgende Informationen zur Funktionsweise von Firewall-Regeln lesen. ■ Die Anordnung der Regeln, sodass die strengsten Regeln zuerst und die allgemeinen Regeln zuletzt ausgewertet werden. Siehe "Info zur Verarbeitungsreihenfolge von Firewall-Regeln, Firewall-Einstellungen und Angriffsschutz" auf Seite 114. ■ Der Client nutzt Stateful Inspection, wodurch das Erstellen zusätzlicher Regeln überflüssig wird. Siehe "Verwendung von Stateful Inspection durch die Firewall" auf Seite 115. ■ Die Firewall-Komponenten, die die Firewall-Regel bilden. Siehe "Die Elemente einer Firewall-Regel" auf Seite 111.
Eine neue Firewall-Regel hinzufügen	Sie können folgende Aufgaben ausführen, um Firewall-Regeln zu verwalten: ■ Symantec Endpoint Protection wird mit Firewall-Standardregeln installiert, aber Sie können Ihre eigenen Regeln hinzufügen. Siehe "Hinzufügen einer Firewall-Regel" auf Seite 116. ■ Sie können eine Standardregel oder eine erstellte Regel anpassen, indem Sie die Kriterien der Firewall-Regel ändern. ■ Firewall-Regeln exportieren und importieren Eine andere Möglichkeit, eine Firewall-Regel hinzuzufügen, besteht darin, vorhandene Firewall-Regeln aus einer anderen Firewall-Richtlinie zu exportieren. Anschließend können Sie die Firewall-Regeln und -Einstellungen importieren, sodass Sie sie nicht neu erstellen müssen. Siehe "Exportieren und Importieren von Firewall-Regeln " auf Seite 118. ■ Firewall-Regeln kopieren und einfügen
Firewall-Regeln aktivieren oder deaktivieren	Firewall-Regeln sind automatisch aktiviert. Sie müssen eine Firewall-Regel jedoch möglicherweise vorübergehend deaktivieren, um die Regel zu prüfen. Deaktivierte Regeln werden von der Firewall nicht überprüft. Siehe "Aktivieren und Deaktivieren von Firewall-Regeln " auf Seite 118.

Die Elemente einer Firewall-Regel

Firewall-Regeln bestimmen, wie der Client Ihren Computer vor bösartigem Netzwerkverkehr schützt. Wird versucht, eine Verbindung zwischen zwei Computern herzustellen, vergleicht die Firewall den Verbindungstyp mit den Firewall-Regeln. Die Firewall überprüft automatisch alle eingehenden und ausgehenden Datenverkehrspakete anhand dieser Regeln. Die Pakete können anhand der Regeln blockiert oder zugelassen werden.

Sie können Auslöser verwenden, wie z. B. Anwendungen, Hosts und Protokolle, um die Firewall-Regeln zu definieren. Beispielsweise kann eine Regel ein Protokoll in Bezug auf eine Zieladresse identifizieren. Wenn die Firewall die Regel auswertet, müssen alle Auslöser zutreffend (true) sein, damit es zu einer positiven Entsprechung kommt. Stimmt einer der Auslöser im Hinblick auf das aktuelle Paket nicht, wendet die Firewall die Regel nicht an.

Sobald eine Firewall-Regel ausgelöst wird, werden keine anderen Firewall-Regeln ausgewertet. Wenn keine Regel ausgelöst wird, wird das Paket automatisch blockiert und das Ereignis wird nicht protokolliert.

Eine Firewall-Regel beschreibt die Bedingungen, in denen eine Netzwerkverbindung erlaubt werden oder blockiert werden kann. Beispielsweise ermöglicht eine Regel Netzwerkverkehr zwischen Remote-Port 80 und der IP-Adresse 192.58.74.0 täglich zwischen 9:00 und 17:00.

Tabelle 5-3 beschreibt die Kriterien, die Sie verwenden, um eine Firewall-Regel zu definieren.

Tabelle 5-3 Bedingungen für Firewall-Regeln

Bedingung	Beschreibung
Auslöser	Die Firewall-Regel-Auslöser sind folgende: ■ Anwendungen Wenn die Anwendung der einzige Auslöser ist, den Sie in einer Regel für die Zulassung von Datenverkehr definieren, lässt die Firewall zu, dass die Anwendung beliebige Netzwerkvorgänge durchführt. Die Anwendung ist der ausschlaggebende Wert, nicht die Netzwerkvorgänge, die die Anwendung durchführt. Nehmen wir an, dass Sie Internet Explorer zulassen und keine anderen Auslöser definieren. Die Benutzer können auf die Remote-Sites zugreifen, die HTTP, HTTPS, FTP, Gopher verwenden, und auf alle anderen Protokolle, die vom Web-Browser unterstützt werden. Sie können zusätzliche Auslöser definieren, um bestimmte Netzwerkprotokolle und Hosts zu beschreiben, mit denen die Kommunikation erlaubt ist. ■ Hosts Der lokale Host ist immer der lokale Clientcomputer und der Remote-Host ist immer ein Remote-Computer, der sich anderswo im Netzwerk befindet. Dieses Host-Verhältnis ist unabhängig von der Richtung des Datenverkehrs. Wenn Sie Host-Auslöser definieren, geben Sie den Host auf der standortfernen Seite der beschriebenen Netzwerkverbindung an. ■ Protokolle Ein Protokollauslöser identifiziert ein oder mehrere Netzwerkprotokolle, die in Bezug auf den beschriebenen Netzwerkverkehr signifikant sind. Der lokale Hostcomputer nutzt immer den lokalen Port und der Remote-Computer den Remote-Port. Dieses Port-Verhältnis ist unabhängig von der Richtung des Datenverkehrs. ■ Netzwerkadapter Wenn Sie einen Netzwerkkartenauslöser definieren, ist die Regel nur für den Datenverkehr relevant, der mithilfe der angegebenen Netzwerkkarte übermittelt oder empfangen wird. Sie können entweder jeden möglichen Adapter angeben oder denjenigen, der derzeit mit dem Client-Computer verbunden ist. Sie können die Auslöserdefinitionen zum Erstellen komplexerer Regeln kombinieren, z. B. zum Identifizieren eines bestimmten Protokolls in Bezug auf eine bestimmte Zieladresse. Wenn die Firewall die Regel auswertet, müssen alle Auslöser zutreffen (true), damit es zu einer positiven Entsprechung kommt. Wenn ein beliebiger Auslöser in Bezug auf das aktuelle Paket nicht zutrifft, wendet die Firewall die Regel nicht an.
Bedingungen	Zeitplan und Bildschirmschonerstatus. Die bedingten Parameter beschreiben keinen Aspekt einer Netzwerkverbindung. Stattdessen bestimmen die bedingten Parameter den aktiven Status einer Regel. Die bedingten Parameter sind optional und unwichtig, wenn sie nicht definiert sind. Sie können einen Zeitplan einrichten oder einen Bildschirmschonerzustand angeben, der vorschreibt, wann eine Regel als aktiv oder inaktiv angesehen werden soll. Die Firewall wertet die deaktivierten Regeln nicht aus, wenn die Firewall Pakete erhält.

Bedingung	Beschreibung
Aktionen	Zulassen oder Blockieren, Protokollieren oder nicht Protokollieren. Die Aktionsparameter geben an, welche Aktionen die Firewall ausführt, wenn sie erfolgreich einer Regel entspricht. Wenn die Regel als Reaktion auf ein erhaltenes Paket ausgewählt wird, führt die Firewall alle Aktionen durch. Die Firewall erlaubt oder blockiert das Paket und protokolliert das Paket oder nicht. Wenn die Firewall Datenverkehr zulässt, kann der in der Regel angegebene Datenverkehr auf das Netzwerk zugreifen. Wenn die Firewall Datenverkehr blockiert, kann der in der Regel angegebene Datenverkehr nicht auf das Netzwerk zugreifen.

Siehe "Verwendung von Stateful Inspection durch die Firewall" auf Seite 115.

Siehe "Hinzufügen einer Firewall-Regel" auf Seite 116.

Siehe "Verwalten von Firewall-Regeln" auf Seite 110.

Info zur Verarbeitungsreihenfolge von Firewall-Regeln, Firewall-Einstellungen und Angriffsschutz

Firewall-Regeln werden sequenziell geordnet, von der höchsten bis zur niedrigsten Priorität in der Regelliste. Wenn die erste Regel nicht angibt, wie ein Paket verarbeitet werden soll, wird die zweite Regel untersucht. Dieser Prozess wird fortgesetzt, bis die Firewall eine Entsprechung findet. Nachdem die Firewall eine Übereinstimmung findet, nimmt sie die Aktion vor, die die Regel angibt. Folgende Regeln niedrigerer Priorität werden nicht geprüft. Beispiel: Wenn eine Regel, die den gesamten Datenverkehr blockiert, zuerst aufgelistet wird, gefolgt von einer Regel, die den gesamten Datenverkehr zulässt, blockiert der Client den gesamten Datenverkehr.

Regeln können entsprechend ihrer Exklusivität geordnet werden. Die Regeln mit den meisten Einschränkungen werden zuerst ausgewertet, allgemeinere Regeln zuletzt. Beispielsweise sollten Regeln, mit denen Datenverkehr blockiert wird, weiter oben in der Liste abgelegt werden. Die Regeln, die weiter unten in der Liste stehen, lassen Datenverkehr mitunter zu.

Zu den bewährten Methoden für das Erstellen einer Regelbasis gehört die folgende Reihenfolge der Regeln:

1. Regeln, die den gesamten Datenverkehr blockieren.
2. Regeln, die den gesamten Datenverkehr zulassen.
3. Regeln, die bestimmte Computer zulassen oder blockieren.

4. Regeln, die bestimmte Anwendungen, Netzwerkdienste und Ports zulassen oder blockieren.

Tabelle 5-4 zeigt die Reihenfolge an, in der die Firewall die Regeln, die Firewall-Einstellungen und die Angriffsschutzeinstellungen verarbeitet.

Tabelle 5-4 Verarbeitungsreihenfolge

Priorität	Einstellung
1.	Benutzerdefinierte IPS-Signaturen
2.	Intrusion Prevention-Einstellungen, Datenverkehrseinstellungen und Stealth-Einstellungen
3.	Integrierte Regeln
4.	Firewall-Regeln
5.	Port-Scan-Prüfungen
6.	IPS-Signaturen, die durch LiveUpdate heruntergeladen werden

Siehe "Ändern der Reihenfolge von Firewall-Regeln" auf Seite 117.

Siehe "Funktionsweise einer Firewall" auf Seite 109.

Siehe "Wie Intrusion Prevention funktioniert" auf Seite 129.

Verwendung von Stateful Inspection durch die Firewall

Der Firewall-Schutz verwendet Stateful Inspection, um aktuelle Verbindungen zu verfolgen. Stateful-Inspection verfolgt Quell- und Ziel-IP-Adressen, Ports, Anwendungen und andere Verbindungsdaten. Bevor der Client die Firewall-Regeln überprüft, werden gemäß den Verbindungsinformationen Entscheidungen über den Datenverkehr getroffen.

Wenn beispielsweise eine Firewall zulässt, dass ein Client eine Verbindung mit einem Webserver herstellt, protokolliert die Firewall die Verbindungsinformationen. Wenn der Server antwortet, erkennt die Firewall, dass eine Reaktion des Webservers erwartet wird. Sie lässt den Datenverkehr des Webservers auf den entsprechenden Computer ohne Überprüfung der Regel zu. Eine Regel muss den ersten ausgehenden Datenverkehr zulassen, bevor die Firewall die Verbindung protokolliert.

Stateful Inspection macht die Erstellung neuer Regeln überflüssig. Für den in eine Richtung initiierten Datenverkehr müssen keine Regeln erstellt werden, um Datenverkehr in beide Richtungen zuzulassen. Der in eine Richtung initiierte

Clientdatenverkehr umfasst normalerweise Telnet (Port 23), HTTP (Port 80) und HTTPS (Port 443). Die Clientcomputer initiieren diesen ausgehenden Datenverkehr. Sie erstellen eine Regel, mit der ausgehender Datenverkehr für diese Protokolle zugelassen wird. Stateful Inspection lässt automatisch den zurückkommenden Datenverkehr zu, der auf den ausgehenden Datenverkehr reagiert. Weil die Firewall Stateful-Technologie nutzt, müssen Sie nur Regeln erstellen, die eine Verbindung initiieren, und nicht die Merkmale eines bestimmten Pakets. Alle Pakete, die zu einer zugelassenen Verbindung gehören, werden als integraler Bestandteil derselben Verbindung zugelassen.

Die Stateful Inspection-Technologie unterstützt alle Regeln, die den TCP-Datenverkehr lenken.

Stateful-Inspection unterstützt nicht die Regeln, die ICMP-Datenverkehr filtern. Im Falle von ICMP müssen Sie bei Bedarf Regeln erstellen, die Datenverkehr in beide Richtungen zulassen. Sollen Clients beispielsweise einen Ping-Befehl senden und Antworten erhalten, erstellen Sie eine Regel, die ICMP-Datenverkehr in beide Richtungen zulässt.

Siehe "Funktionsweise einer Firewall" auf Seite 109.

Siehe "Verwalten von Firewall-Regeln" auf Seite 110.

Hinzufügen einer Firewall-Regel

Wenn Sie eine Firewall-Regel hinzufügen, müssen Sie entscheiden, welche Wirkung die Regel haben soll. Beispielsweise soll aller Datenverkehr von einer bestimmten Quelle zugelassen werden oder die UDP-Pakete von einer Website sollen blockiert werden.

Firewall-Regeln werden automatisch aktiviert, wenn Sie sie erstellen.

So fügen Sie eine Firewall-Regel hinzu

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Klicken Sie neben "Netzwerkbedrohungsschutz" auf "Optionen" > "Firewall-Regeln konfigurieren".
3. Klicken Sie im Dialogfeld Firewall-Regeln konfigurieren auf Hinzufügen.
4. Auf der Registerkarte "Allgemein" geben Sie einen Namen für die Regel ein, und klicken Sie dann entweder auf "Diesen Datenverkehr blockieren" oder "Diesen Datenverkehr zulassen".
5. Um die Auslöser für die Regel zu definieren, klicken Sie auf die jeweilige Registerkarte und konfigurieren sie wunschgemäß.

6 Um den Zeitraum festzulegen, in dem die Regel aktiv oder deaktiviert ist, klicken Sie auf der Registerkarte "Planung" auf "Planung Aktivieren" und richten Sie dann einen Zeitplan ein.

7 Wenn Sie mit den Änderungen fertig sind, klicken Sie auf "OK".

8 Klicken Sie auf "OK".

Siehe "Die Elemente einer Firewall-Regel" auf Seite 111.

Siehe "Aktivieren und Deaktivieren von Firewall-Regeln " auf Seite 118.

Ändern der Reihenfolge von Firewall-Regeln

Die Firewall verarbeitet die Liste von Firewall-Regeln von oben nach unten. Sie können festlegen, wie die Firewall Firewall-Regeln verarbeitet, indem Sie die Reihenfolge ändern.

Eine Änderung der Reihenfolge wirkt sich nur auf den derzeit ausgewählten Ort aus.

Hinweis: Einen besseren Schutz erreichen Sie, indem Sie die restriktivsten Regeln zuerst und die am wenigsten restriktiven Regeln zuletzt aufführen.

So ändern Sie die Reihenfolge einer Firewall-Regel:

1 Klicken Sie im Client in der Seitenleiste auf "Status".

2 Klicken Sie neben "Netzwerkbedrohungsschutz" auf "Optionen" > "Firewall-Regeln konfigurieren".

3 Wählen Sie im Dialogfeld "Firewall-Regeln konfigurieren" die Regel aus, die Sie verschieben möchten.

4 Führen Sie einen der folgenden Schritte aus:

- Um die Firewall diese Regel vor der darüber stehenden Regel verarbeiten zu lassen, klicken Sie auf den Pfeil nach oben.
- Um die Firewall diese Regel nach der darunterstehenden Regel verarbeiten zu lassen, klicken Sie auf den Pfeil nach unten.

5 Wenn Sie mit dem Verschieben von Regeln fertig sind, klicken Sie auf "OK".

Siehe "Info zur Verarbeitungsreihenfolge von Firewall-Regeln, Firewall-Einstellungen und Angriffsschutz" auf Seite 114.

Aktivieren und Deaktivieren von Firewall-Regeln

Sie müssen Regeln aktivieren, damit sie von der Firewall verarbeitet werden können. Wenn Sie Firewall-Regeln hinzufügen, werden diese automatisch aktiviert.

Sie können eine Firewall-Regel vorübergehend deaktivieren, wenn Sie den Zugriff auf einen bestimmten Computer oder eine bestimmte Anwendung zulassen müssen.

So aktivieren und deaktivieren Sie Firewall-Regeln

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Klicken Sie neben "Netzwerkbedrohungsschutz" auf "Optionen" > "Firewall-Regeln konfigurieren".
3. Aktivieren oder deaktivieren Sie im Dialogfeld "Firewall-Regeln konfigurieren" in der Spalte "Regelname" das Kontrollkästchen neben der Regel, die Sie aktivieren bzw. deaktivieren möchten.
4. Klicken Sie auf "OK".

Siehe "Hinzufügen einer Firewall-Regel" auf Seite 116.

Exportieren und Importieren von Firewall-Regeln

Sie können die Regeln mit einem anderen Client gemeinsam nutzen, damit Sie sie nicht neu erstellen müssen. Sie können die Regeln aus einem anderen Computer exportieren und sie in Ihren Computer importieren. Wenn Sie Regeln importieren, werden sie in der Firewall-Regelliste unten angefügt. Importierte Regeln überschreiben vorhandene Regeln nicht, selbst wenn eine importierte Regel mit einer vorhandenen Regel identisch ist.

Die exportierten und importierten Regeln werden in einer .sar-Datei gespeichert.

So exportieren Sie Firewall-Regeln

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Neben Netzwerkbedrohungsschutz klicken Sie auf "Optionen" > "Firewall-Regeln konfigurieren".
3. Im Dialogfeld "Firewall-Regeln konfigurieren " wählen Sie die Regeln aus, die Sie exportieren möchten.
4. Klicken Sie mit der rechten Maustaste auf die Regeln und klicken Sie dann auf "Ausgewählte Regeln exportieren".
5. Im Dialogfeld "Export" geben Sie einen Dateinamen ein und klicken Sie dann auf "Speichern".
6. Klicken Sie auf "OK".

So importieren Sie Firewall-Regeln

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Neben Netzwerkbedrohungsschutz klicken Sie auf "Optionen" > "Firewall-Regeln konfigurieren".
3. Im Dialogfeld "Firewall-Regeln konfigurieren" klicken Sie mit der rechten Maustaste auf die Firewall-Regelliste und klicken dann auf "Regel importieren".
4. Suchen Sie im Import -Dialogfeld die .sar Datei mit den Regeln, die Sie importieren möchten.
5. Klicken Sie auf "Öffnen".
6. Klicken Sie auf "OK".

Siehe "Hinzufügen einer Firewall-Regel" auf Seite 116.

Aktivieren oder Deaktivieren von Firewall-Einstellungen

Sie können die Firewall-Einstellungen des Clients aktivieren, um Ihren Computer gegen bestimmte Typen von Netzwerkangriffen zu schützen. Einige der Einstellungen ersetzen die Firewall-Regeln, die Sie andernfalls hinzufügen müssten.

Hinweis: Ihr Administrator hat möglicherweise veranlasst, dass Sie einige dieser Einstellungen nicht konfigurieren können.

Tabelle 5-5 beschreibt die Arten von Firewall-Einstellungen, die Sie konfigurieren können, um Ihren Firewall-Schutz weiter anzupassen.

Tabelle 5-5 Firewall-Einstellungen

Kategorie	Beschreibung
Integrierte Regeln für wesentliche Netzwerkdienste	Symantec Endpoint Protection stellt die integrierten Regeln bereit, die den normalen Austausch von bestimmten wesentlichen Netzwerkdiensten ermöglichen. Integrierte Regeln beseitigen die Notwendigkeit, Firewall-Regeln zu erstellen, die ausdrücklich jene Dienste zulassen. Während der Verarbeitung werden diese integrierten Regeln vor Firewall-Regeln ausgewertet, damit die Pakete, die einem aktiven Vorkommnis einer integrierten Regel entsprechen, zulässig sind. Sie können eingebaute Regeln für DHCP-, DNS- und WINS-Dienste definieren.

Kategorie	Beschreibung
Datenverkehr und Web-Browsing im Stealth-Modus	Sie können verschiedene Einstellungen für Datenverkehr und Webbrowsing im Stealth-Modus aktivieren, um den Client vor bestimmten Arten von Netzwerkangriffen zu schützen. Sie können die Datenverkehrseinstellungen aktivieren, um den Datenverkehr, der über Treiber, NetBIOS und Token-Rings kommuniziert, zu erkennen und zu blockieren. Sie können Einstellungen zur Erkennung von Datenverkehr konfigurieren, der weniger offensichtliche Angriffe verwendet. Sie können auch das Verhalten für den IP-Datenverkehr steuern, der keinen Firewall-Regeln entspricht.
Netzwerkdatei- und Druckerfreigabe	Sie können den Client entweder zur Freigabe seiner Dateien oder zur Suche nach freigegebenen Dateien und Druckern im lokalen Netzwerk aktivieren. Um netzwerkbasierte Angriffe zu verhindern, können Sie die Freigabe von Netzwerkdateien und Druckern deaktivieren. Siehe "Aktivieren der Netzwerkdatei- und Druckerfreigabe" auf Seite 120.
Blockieren des angreifenden Computers	Wenn der Symantec Endpoint Protection-Client einen Netzwerkangriff erkennt, kann er die Verbindung automatisch blockieren, um die Sicherheit des Client-Computers zu gewährleisten. Der Client blockiert dann automatisch für einen bestimmten Zeitraum die gesamte ein- und ausgehende Kommunikation der IP-Adresse des angreifenden Computers. Die IP-Adresse des angreifenden Computers wird für einen einzelnen Standort blockiert.

So aktivieren oder deaktivieren Sie Firewall-Einstellungen

1. Klicken Sie im Client auf "Einstellungen ändern".
2. Klicken Sie neben "Netzwerkbedrohungsschutz" auf "Einstellungen konfigurieren".
3. Aktivieren Sie auf der Registerkarte "Firewall" die Einstellungen, die Sie aktivieren möchten.

   Klicken Sie auf "Hilfe", um weitere Informationen über die Einstellungen zu erhalten.
4. Klicken Sie auf "OK".

Siehe "Verwalten von Firewall-Regeln" auf Seite 110.

Aktivieren der Netzwerkdatei- und Druckerfreigabe

Sie können den Client entweder zur Freigabe seiner Dateien oder zur Suche nach freigegebenen Dateien und Druckern im lokalen Netzwerk aktivieren. Um netzwerkbasierte Angriffe zu verhindern, können Sie die Freigabe von Netzwerkdateien und Druckern deaktivieren.

Tabelle 5-6 Methoden zur Aktivierung der Netzwerkdatei- und Druckerfreigabe

Aufgabe	Beschreibung
Aktivieren Sie automatisch die Netzwerkdatei- und Druckerfreigabe-Einstellungen auf der Registerkarte "Microsoft Windows-Netzwerk".	Wenn eine Firewall-Regel diesen Datenverkehr blockiert, hat diese Regel vor der Einstellung Vorrang. So aktivieren Sie automatisch die Netzwerkdatei- und Druckerfreigabe
Aktivieren die Netzwerkdatei- und Druckerfreigabe manuell, indem Sie Firewall-Regeln hinzufügen.	Sie können Firewall-Regeln hinzufügen, wenn die zur Verfügung stehenden Einstellungen nicht flexibel genug sind. Wenn Sie beispielsweise eine Regel erstellen, können Sie einen bestimmten Host statt alle Hosts angeben. Die Firewall-Regeln ermöglichen den Zugriff auf die Ports, um das Netzwerk nach freigegebenen Dateien und Druckern zu durchsuchen. Sie können einen Satz Firewall-Regeln erstellen, damit der Client seine Dateien freigeben kann. Sie erstellen einen zweiten Satz Firewall-Regeln, damit der Client nach anderen Dateien und Druckern suchen kann. So aktivieren Sie Clients für die Suche von Dateien und Druckern manuell So aktivieren Sie andere Computer zum Durchsuchen von Dateien auf dem Client manuell

So aktivieren Sie automatisch die Netzwerkdatei- und Druckerfreigabe

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Neben "Netzwerkbedrohungsschutz" klicken Sie auf "Einstellungen konfigurieren".
3. Auf der Registerkarte "Microsoft Windows-Netzwerk" unter "Einstellungen" klicken Sie auf das Dropdown-Menü und wählen Sie den Adapter aus, für den diese Einstellungen gelten.
4. Um andere Computer und Drucker im Netzwerk zu suchen, klicken Sie auf "Dateien und Drucker im Netzwerk durchsuchen".
5. Um zuzulassen, dass andere Computer Dateien auf Ihrem Computer durchsuchen können, klicken Sie auf "Meine Dateien und Drucker für andere im Netzwerk freigeben".
6. Klicken Sie auf "OK".

So aktivieren Sie Clients für die Suche von Dateien und Druckern manuell

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Klicken Sie neben "Netzwerkbedrohungsschutz" auf "Optionen" > "Firewall-Regeln konfigurieren".
3. Klicken Sie im Dialogfeld Firewall-Regeln konfigurieren auf Hinzufügen.
4. Geben Sie auf der Registerkarte "Allgemein" einen Namen für die Regel ein und klicken Sie auf "Diesen Datenverkehr zulassen".
5. Klicken Sie auf der Registerkarte "Ports und Protokolle" in der Dropdown-Liste "Protokoll" auf "TCP".
6. Geben Sie in der Dropdown-Liste "Remote-Ports" Folgendes ein:

   88, 135, 139, 445
7. Klicken Sie auf "OK".
8. Klicken Sie im Dialogfeld Firewall-Regeln konfigurieren auf Hinzufügen.
9. Geben Sie auf der Registerkarte "Allgemein" einen Namen für die Regel ein und klicken Sie auf "Diesen Datenverkehr zulassen".
10. Klicken Sie auf der Registerkarte "Ports und Protokolle" in der Dropdown-Liste "Protokoll" auf "UDP".
11. Geben Sie in der Dropdown-Liste "Remote-Ports" Folgendes ein:

    88
12. Geben Sie in der Dropdown-Liste "Lokale Ports" Folgendes ein:

    137, 138
13. Klicken Sie auf "OK".

So aktivieren Sie andere Computer zum Durchsuchen von Dateien auf dem Client manuell

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Klicken Sie neben "Netzwerkbedrohungsschutz" auf "Optionen" > "Firewall-Regeln konfigurieren".
3. Klicken Sie im Dialogfeld Firewall-Regeln konfigurieren auf Hinzufügen.
4. Geben Sie auf der Registerkarte "Allgemein" einen Namen für die Regel ein und klicken Sie auf "Diesen Datenverkehr zulassen".
5. Klicken Sie auf der Registerkarte "Ports und Protokolle" in der Dropdown-Liste "Protokoll" auf "TCP".

6 Geben Sie in der Dropdown-Liste "Lokale Ports" Folgendes ein:

88, 135, 139, 445

7 Klicken Sie auf "OK".

8 Klicken Sie im Dialogfeld Firewall-Regeln konfigurieren auf Hinzufügen.

9 Geben Sie auf der Registerkarte "Allgemein" einen Namen für die Regel ein und klicken Sie auf "Diesen Datenverkehr zulassen".

10 Klicken Sie auf der Registerkarte "Ports und Protokolle" in der Dropdown-Liste "Protokoll" auf "UDP".

11 Geben Sie in der Dropdown-Liste "Lokale Ports" Folgendes ein:

88, 137, 138

12 Klicken Sie auf "OK".

Siehe "Aktivieren oder Deaktivieren von Firewall-Einstellungen" auf Seite 119.

Zulassen oder Blockieren des Zugriffs von Anwendungen auf das Netzwerk

Sie können die Aktion angeben, die der Client auf eine Anwendung ausführt, wenn sie versucht, auf das Netzwerk von Ihrem Computer zuzugreifen oder wenn sie versucht, auf Ihren Computer zuzugreifen. Beispielsweise können Sie Internet Explorer vom Zugriff auf Websites von Ihrem Computer aus blockieren.

Tabelle 5-7 beschreibt die Maßnahmen, die der Client bezüglich des Netzwerkverkehrs ergreift.

Tabelle 5-7 Aktionen, die die Firewall unternimmt, wenn Anwendungen auf den Client oder auf das Netzwerk zugreifen

Aktion	Beschreibung
Zulassen	Ermöglicht es dem eingehenden Datenverkehr, auf den Clientcomputer zuzugreifen, und dem ausgehenden Datenverkehr, auf das Netzwerk zuzugreifen. Wenn der Client Datenverkehr empfängt, zeigt das Symbol einen kleinen blauen Punkt in der unteren linken Ecke an. Wenn der Client Datenverkehr sendet, zeigt das Symbol den Punkt in der unteren rechten Ecke an.
Blockieren	Blockiert den eingehenden und den ausgehenden Datenverkehr, auf das Netzwerk oder auf eine Internetverbindung zuzugreifen.

Aktion	Beschreibung
Abfrage	Sie werden gefragt, ob die Anwendung auf das Netzwerk zugreifen soll, wenn Sie sie beim nächsten Mal zu starten versuchen.
Beenden	Stoppt den Prozess.

So lassen Sie den Zugriff einer Anwendung auf das Netzwerk zu oder blockieren ihn

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Neben "Netzwerkbedrohungsschutz" klicken Sie auf "Optionen > Netzwerkaktivität anzeigen".
3. Klicken Sie mit der rechten Maustaste im Dialogfeld "Netzwerkaktivität" auf die Anwendung oder den Dienst, und klicken Sie dann auf die Aktion, die der Client auf dieser Anwendung ausführen soll.
4. Klicken Sie auf "Schließen".

   Wenn Sie auf "Zulassen", "Blockieren" oder "Anfragen" klicken, können Sie eine Firewall-Regel nur für diese Anwendung erstellen.

   Siehe "Erstellen von Firewall-Regeln für Anwendungen beim Zugriff auf das Netzwerk von Ihrem Computer" auf Seite 124.

Erstellen von Firewall-Regeln für Anwendungen beim Zugriff auf das Netzwerk von Ihrem Computer

Sie können eine Firewall-Regel erstellen, die angibt, ob eine auf Ihrem Computer ausgeführte Anwendung auf das Netzwerk zugreifen kann. Der Client kann die Anwendung zulassen oder blockieren oder Sie zunächst fragen, ob die Anwendung zugelassen oder blockiert werden soll. Beispielsweise können Sie den Client so konfigurieren, dass er die Anzeige aller Websites in Ihrem Webbrowser verhindert.

Sie können auch bestimmen, zu welchem Zeitpunkt und auf welche Weise die Anwendung zugelassen oder blockiert wird. Sie können zum Beispiel angeben, dass ein Videospiel nur zu bestimmten Uhrzeiten auf das Netzwerk zugreifen kann. Diese Regeln werden als anwendungsbasierte Firewall-Regeln bezeichnet.

Hinweis: Besteht ein Konflikt zwischen einer Firewall-Regel und einer anwendungsbasierten Firewall-Regel, hat die Firewall-Regel Vorrang. Beispiel: Eine Firewall-Regel, die zwischen 1:00 und 8:00 Uhr morgens den gesamten Datenverkehr blockiert, setzt eine Anwendungsregel außer Kraft, die zulässt, dass "iexplore.exe" jederzeit ausgeführt wird.

Die Anwendungen, die im Dialogfeld "Netzwerkaktivität" angezeigt werden, sind die Anwendungen und Dienste, die seit dem Start des Clientdienstes ausgeführt wurden.

Siehe "Zulassen oder Blockieren des Zugriffs von Anwendungen auf das Netzwerk" auf Seite 123.

So erstellen Sie eine Firewall-Regel für eine Anwendung beim Zugriff auf das Netzwerk von Ihrem Computer

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Neben "Netzwerkbedrohungsschutz" klicken Sie auf "Optionen > Anwendungseinstellungen anzeigen".
3. Optional können Sie die Aktion im Dialogfeld "Anwendungseinstellungen anzeigen" ändern, indem Sie mit der rechten Maustaste auf die Anwendung klicken und anschließend auf "Zulassen", "Abfrage" oder "Blockieren" klicken.
4. Klicken Sie auf "Konfigurieren".
5. Konfigurieren Sie im Dialogfeld "Anwendungseinstellungen konfigurieren" die Einschränkungen für diese Anwendung.

   Weitere Informationen erhalten Sie, indem Sie auf das Textfeld und die Option zeigen und auf "Hilfe" klicken.

   Ist für die Aktion "Zulassen" im Schritt 3 festgelegt, sind alle von Ihnen konfigurierten Einstellungen Einschränkungen der Regel. Wenn Sie "Blockieren" ausgewählt haben, sind die von Ihnen konfigurierten Einstellungen Ausnahmen von der Regel.
6. Klicken Sie auf "OK".

   Sie können die für die Anwendung festgelegten Bedingungen entfernen, indem Sie auf "Entfernen" oder "Alle entfernen" klicken. Wenn Sie die Einschränkungen entfernen, wird die Aktion, die der Client bei der Anwendung ausführt, auch gelöscht. Wenn die Anwendung oder der Dienst versucht, zum Netzwerk wieder eine Verbindung herzustellen, könnten Sie wieder gefragt werden, ob die Anwendung erlaubt oder blockiert werden soll.
7. Klicken Sie auf "OK".

Siehe "Hinzufügen einer Firewall-Regel" auf Seite 116.

Konfigurieren des Clients, zum Blockieren von Datenverkehr bei aktivem Screensaver oder inaktiver Firewall

Sie können Ihren Computer so konfigurieren, dass eingehender und ausgehender Datenverkehr in den folgenden Situationen blockiert wird:

Wenn der Bildschirmschoner Ihres Computers aktiviert ist.	Sie können Ihren Computer so konfigurieren, dass der gesamte eingehende und ausgehende Datenverkehr der Netzwerkumgebung blockiert wird, wenn der Bildschirmschoner Ihres Computers aktiviert wird. Sobald der Bildschirmschoner deaktiviert ist, kehrt Ihr Computer zur vorher zugewiesenen Sicherheitsstufe zurück. So blockieren Sie Datenverkehr, wenn der Bildschirmschoner aktiviert wird
Wenn die Firewall nicht ausgeführt wird.	Der Computer ist ungeschützt, nachdem der Computer hochgefahren wurde und bevor der Firewall-Dienst startet oder nachdem der Firewall-Dienst beendet wird und der Computer heruntergefahren wird. Dieser Zeitrahmen stellt eine Sicherheitslücke dar, die nicht autorisierte Kommunikation zulassen kann. So blockieren Sie Datenverkehr, wenn die Firewall nicht ausfgeführt wird
Wenn Sie den gesamten ein- und ausgehenden Datenverkehr jederzeit blockieren möchten.	Sie wollen möglicherweise den gesamten Datenverkehr blockieren, wenn ein besonders zerstörerischer Virus Ihr Firmennetz oder Subnetz angreift. Unter normalen Umständen würden Sie den gesamten Datenverkehr nicht blockieren. **Hinweis:** Ihr Administrator kann diese Option so konfiguriert haben, dass sie nicht verfügbar ist. Sie können nicht den gesamten Datenverkehr auf einem nicht verwalteten Client blockieren. So blockieren Sie jederzeit den gesamten Verkehr

Sie können jeden Datenverkehr zulassen, indem Sie "Netzwerkbedrohungsschutz" deaktivieren.

Siehe "Aktivieren oder Deaktivieren des Schutzes auf dem Client-Computer" auf Seite 52.

So blockieren Sie Datenverkehr, wenn der Bildschirmschoner aktiviert wird

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Neben Netzwerkbedrohungsschutz klicken Sie auf "Einstellungen konfigurieren".
3. Auf der Registerkarte "Microsoft Windows-Netzwerk" klicken Sie unter "Bildschirmschoner-Modus" auf Solange der Bildschirmschoner ausgeführt wird".
4. Klicken Sie auf "OK".

So blockieren Sie Datenverkehr, wenn die Firewall nicht ausfgeführt wird

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Neben Netzwerkbedrohungsschutz klicken Sie auf "Einstellungen konfigurieren".
3. Auf der Registerkarte Firewall klicken Sie unter "Einstellungen für Datenverkehr" auf "Bis die Firewall gestartet und nachdem die Firewall angehalten wurde".
4. Klicken Sie optional auf "Anfänglichen DHCP-und NetBIOS-Datenverkehr erlauben".
5. Klicken Sie auf "OK".

So blockieren Sie jederzeit den gesamten Verkehr

1. Klicken Sie im Client in der Seitenleiste auf "Status".
2. Neben "Netzwerkbedrohungsschutz" klicken Sie auf "Optionen > Netzwerkaktivität anzeigen".
3. Klicken Sie auf "Extras" > "Sämtlichen Datenverkehr blockieren".
4. Klicken Sie zur Bestätigung auf "Ja".
5. Um zu den vorherigen Firewall-Einstellungen des Clients zurückzukehren, deaktivieren Sie "Extras" > "Sämtlichen Datenverkehr blockieren".

Siehe "Aktivieren oder Deaktivieren von Firewall-Einstellungen" auf Seite 119.

Verwalten von Intrusion Prevention

Sie verwalten Intrusion Prevention als Teil des Netzwerkbedrohungsschutzes.

Tabelle 5-8 Verwalten von Intrusion Prevention

Aktion	Beschreibung
Informationen zu Intrusion Prevention	Erfahren Sie, wie Intrusion Prevention Netzwerk- und Browserangriffe erkennt und blockiert. Siehe "Wie Intrusion Prevention funktioniert" auf Seite 129.
Download der neuesten IPS-Signaturen	Standardmäßig werden die neuesten Signaturen auf den Client heruntergeladen. Sie können die Signaturen jedoch sofort manuell herunterladen. Siehe "Aktualisieren des Computerschutzes" auf Seite 41.
Aktivieren oder Deaktivieren des Netzwerk- bzw. Browser-Angriffsschutzes	Sie können den Angriffsschutz für Fehlerbehebungzwecke deaktivieren, oder wenn Clientcomputer zu viele Falschmeldngen erzeugen. Üblicherweise sollten Sie Intrusion Prevention nicht deaktivieren. Sie können die folgenden Typen von Intrusion Prevention aktivieren oder deaktivieren: ■ Netzwerk-Intrusion Prevention ■ Browser-Intrusion Prevention Siehe "Aktivieren oder Deaktivieren des Angriffsschutzes" auf Seite 130. Sie können Intrusion Prevention auch aktivieren oder deaktivieren, wenn Sie den Netzwerkbedrohungsschutz aktivieren oder deaktivieren. Siehe "Info zum Aktivieren und das Deaktivieren des Schutzes, wenn Sie Probleme beheben müssen" auf Seite 50.
Konfigurieren der Intrusion Prevention-Benachrichtigungen	Sie können Benachrichtigungen so konfigurieren, dass sie angezeigt werden, wenn Symantec Endpoint Protection einen Angriffsversuch erkennt. Siehe "Konfigurieren der Intrusion Prevention-Benachrichtigungen" auf Seite 131.

Wie Intrusion Prevention funktioniert

Intrusion Prevention ist ein Teil des Netzwerkbedrohungsschutzes.

Intrusion Prevention erkennt und blockiert automatisch Netzwerkangriffe und Angriffe auf Browser. Intrusion Prevention ist die zweite Verteidigungsebene nach der Firewall, um Clientcomputer zu schützen. Intrusion Prevention wird manchmal IPS (Intrusion Prevention-System) genannt.

Intrusion Prevention fängt Daten auf der Netzwerkebene ab. Signaturen werden verwendet, um Pakete oder Paketströme zu scannen. Jedes Paket wird einzeln gescannt, indem nach Mustern gesucht wird, die Netzwerk- oder Browser-Angriffen entsprechen. Angriffsschutz erkennt Angriffe auf Betriebssystemkomponenten und der Anwendungsschicht.

Angriffsschutz stellt zwei Schutztypen bereit.

Tabelle 5-9 Typen des Angriffsschutzes

Typ	Beschreibung
Netzwerk-Intrusion Prevention	Netzwerk-Intrusion Prevention verwendet Signaturen, um Angriffe auf Clientcomputer zu identifizieren. Bei bekannten Angriffe verwirft Intrusion Prevention automatisch die Pakete, die den Signaturen entsprechen. Sie können keine benutzerdefinierten Signaturen auf dem Client erstellen. Sie können jedoch benutzerdefinierte Signaturen importieren, die Sie oder Ihr Administrator in Symantec Endpoint Protection Manager erstellt haben.
Browser-Intrusion Prevention	Browser-Intrusion Prevention überwacht Angriffe auf Internet Explorer und Firefox. Browser-Intrusion Prevention wird nicht auf anderen Browsern unterstützt. Firefox deaktiviert möglicherweise das Symantec Endpoint Protection-Plugin. Sie können es jedoch wieder aktivieren. Dieser Typ von Intrusion Prevention verwendet Angriffssignaturen sowie Heuristiken, um Angriffe auf Browser zu identifizieren. Bei einigen Browser-Angriffen erfordert Intrusion Prevention, dass der Client den Browser beendet. Eine Benachrichtigung erscheint auf dem Clientcomputer. Die neuesten Informationen zu den durch den Browser-Angriffsschutz geschützten Browsern finden Sie in der Supportdatenbank: Unterstützte Browserversionen für Browser-Angriffsschutz.

Siehe "Verwalten von Intrusion Prevention" auf Seite 127.

Aktivieren oder Deaktivieren des Angriffsschutzes

Wenn Sie den Angriffsschutz auf Ihrem Computer deaktivieren, ist Ihr Computer normalerweise weniger geschützt. Sie können diese Einstellungen allerdings deaktivieren, um Falscherkennungen zu verhindern oder um auf Ihren Computer Fehler zu beheben.

Symantec Endpoint Protection protokolliert unbefugte Zugriffsversuche und Ereignisse im Sicherheitsprotokoll. Symantec Endpoint Protection protokolliert möglicherweise Angriffsversuchsereignisse auch im Paketprotokoll, wenn Ihr Administrator dies konfiguriert hat.

Siehe "Verwalten von Intrusion Prevention" auf Seite 127.

Siehe "Anzeigen von Protokollen" auf Seite 48.

Sie können zwei Typen von Intrusion Prevention aktivieren oder deaktivieren:

- Netzwerk-Intrusion Prevention
- Browser-Intrusion Prevention

Hinweis: Ihr Administrator kann diese Optionen so konfiguriert haben, dass sie nicht verfügbar sind.

Siehe "Info zum Aktivieren und das Deaktivieren des Schutzes, wenn Sie Probleme beheben müssen" auf Seite 50.

Aktivieren und Deaktivieren von Intrusion Prevention-Einstellungen

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Neben "Netzwerkbedrohungsschutz" klicken Sie auf "Einstellungen konfigurieren".
3. Aktivieren oder deaktivieren Sie auf der Registerkarte "Intrusion Prevention" eine der folgenden Einstellungen:
   - Intrusion Prevention für Netzwerke aktivieren
   - Intrusion Prevention für Browser aktivieren

   Für weitere Informationen zu diesen Einstellungen klicken Sie auf "Hilfe".
4. Klicken Sie auf "OK".

Konfigurieren der Intrusion Prevention-Benachrichtigungen

Sie können Benachrichtigungen konfigurieren, die erscheinen, wenn der Client einen Netzwerkangriff auf Ihrem Computer erkennt oder wenn der Client den Zugriff einer Anwendung auf Ihren Computer blockiert. Sie können den Zeitraum einstellen, in dem diese Benachrichtigungen angezeigt werden und ob Sie einen Signalton hören, wenn die Benachrichtigung angezeigt wird. Sie müssen das Angriffsschutzsystem aktivieren, damit die Angriffsschutz-Benachrichtigungen angezeigt werden.

Wenn Angriffsschutz auf dem Computer aktiviert wird, können Windows-Clients und Mac-Clients diese Benachrichtigungen auslösen.

Hinweis: Ihr Administrator kann diese Optionen so konfiguriert haben, dass sie nicht verfügbar sind.

Siehe "Verwalten von Intrusion Prevention" auf Seite 127.

So konfigurieren Sie Angriffsschutzbenachrichtigungen auf einem Windows-Client

1. Klicken Sie im Client in der Seitenleiste auf "Einstellungen ändern".
2. Neben Netzwerkbedrohungsschutz klicken Sie auf "Einstellungen konfigurieren".
3. Klicken Sie im Dialogfeld "Einstellungen für den Netzwerkbedrohungsschutz" auf "Benachrichtigungen".
4. Aktivieren Sie "Intrusion Prevention-Benachrichtigungen anzeigen".
5. Um einzustellen, dass ein Signalton ertönt, wenn die Benachrichtigung angezeigt wird, aktivieren Sie "Beim Benachrichtigen von Benutzern Tonsignal ausgeben".
6. Klicken Sie auf "OK".

So konfigurieren Sie Angriffsschutzbenachrichtigungen auf einem Mac-Client

1. Klicken Sie auf dem Symantec QuickMenu auf "Symantec Endpoint Protection > Angriffsschutz-Einstellungen öffnen".
2. Klicken Sie auf das Schlosssymbol, um Änderungen vorzunehmen oder das Vornehmen weiterer Änderungen zu verhindern.

   Sie müssen Ihren Administratornamen und das Kennwort angeben, um die Angriffsschutz-Einstellungen zu sperren bzw. zu entsperren.
3. Klicken Sie auf "Angriffsschutz-Benachrichtigung anzeigen".

   Klicken Sie bei Bedarf auf "Beim Benachrichtigen von Benutzern Tonsignal ausgeben".

Kapitel 6

Verwalten von Symantec Network Access Control

In diesem Kapitel werden folgende Themen behandelt:

Wie Symantec Network Access Control funktioniert

Der Symantec Network Access Control-Client validiert und verstärkt die Einhaltung von Sicherheitsrichtlinien der Computer, die versuchen, eine Verbindung zum Netzwerk herzustellen. Dieser Vorgang wird gestartet, bevor der Computer eine Verbindung zum Netzwerk herstellt, und läuft für die Dauer der Verbindung. Die Host-Integritätsrichtlinie ist die Sicherheitsrichtlinie, die als Basis für alle Auswertungen und Aktionen dient. Die Host-Integrität wird auch als "Sicherheitsrichtlinieneinhaltung" bezeichnet.

Tabelle 6-1 beschreibt den Prozess von Network Access Control zum Durchsetzen der Einhaltung von Sicherheitsrichtlinien auf dem Client-Computer.

Tabelle 6-1 Funktionweise von Symantec Network Access Control

Aktion	Beschreibung
Der Client wertet kontinuierlich seine Compliance aus	Sie schalten den Client-Computer ein. Der Client führt eine Host-Integritätsprüfung durch, die die Konfiguration des Computers mit der Host-Integritätsrichtlinie vergleicht, die vom Management-Server heruntergeladen wurde. Die Host-Integritätsprüfung prüft Ihren Computer bezüglich der Einhaltung der Host-Integritätsrichtlinie für Antivirussoftware, Patches, Hotfixes und andere Sicherheitsanforderungen. Beispielsweise können die Richtlinien prüfen, wie aktuell die Virendefinitionen sind, und welches die letzten Patches waren, die auf das Betriebssystem angewendet wurden. Siehe "Ausführen einer Host-Integritätsprüfung" auf Seite 136.
Symantec Enforcer authentifiziert den Clientcomputer und gewährt den Netzwerkzugriff oder blockiert und isoliert nicht der Richtlinie entsprechende Computer.	Wenn der Computer allen Anforderungen der Richtlinien genügt hat, ist die Host-Integritätsprüfung bestanden. Der Enforcer bewilligt den Computern vollen Netzwerkzugriff, die die Host-Integritätsprüfung bestehen. Wenn der Computer nicht den Anforderungen der Richtlinien genügt, schlägt die Host-Integritätsprüfung fehl. Wenn eine Host-Integritätsprüfung fehlschlägt, blockiert der Client oder Symantec Enforcer Ihren Computer, bis Sie Ihren Computer bereinigen. Isolierte Computer haben begrenzten oder keinen Zugriff auf das Netzwerk. Siehe "Funktionsweise des Clients mit einem Enforcer" auf Seite 135.
Ihr Administrator hat die Richtlinien eventuell so eingerichtet, dass eine Host-Integritätsprüfung erfolgreich ist, selbst wenn eine bestimmte Anforderung nicht erfüllt ist.	Der Client zeigt möglicherweise jedes Mal eine Benachrichtigung an, wenn die Host-Integritätsprüfung erfolgreich ist. Siehe "Typen von Warnmeldungen und Benachrichtigungen" auf Seite 27.

Aktion	Beschreibung
Der Client bereinigt nicht der Richtlinie entsprechende Computer.	Wenn die Host-Integritätsprüfung erfolglos ist, installiert der Client die erforderliche Software bzw. fordert Sie auf, dies zu tun. Nachdem Ihr Computer bereinigt wurde, versucht er, wieder auf das Netzwerk zuzugreifen. Wenn der Computer die Richtlinie vollständig erfüllt, bewilligt das Netzwerk dem Computer den Netzwerkzugriff. Siehe "Bereinigen Ihres Computers" auf Seite 136.
Der Client überwacht die Compliance proaktiv.	Der Client überwacht aktiv die Compliance aller Clientcomputer. Wenn sich der Richtlinieneinhaltungsstatus des Computers ändert, ändern sich auch die Netzwerkzugriffsrechte des Computers.

Weitere Informationen zu den Ergebnissen der Host-Integritätsprüfung finden Sie im Sicherheitsprotokoll.

Siehe "Anzeigen von Protokollen" auf Seite 48.

Siehe "Anzeigen der Symantec Network Access Control-Protokolle" auf Seite 141.

Funktionsweise des Clients mit einem Enforcer

Der Client kommuniziert mit Symantec Enforcer. Der Enforcer stellt sicher, dass alle Computer, die eine Verbindung zum Netzwerk haben, das von ihm geschützt wird, die Client-Software ausführen und die richtigen Sicherheitsrichtlinien haben.

Siehe "Wie Symantec Network Access Control funktioniert" auf Seite 133.

Ein Enforcer muss den Benutzer oder den Client-Computer authentifizieren, bevor er dem Client-Computer erlaubt, auf das Netzwerk zuzugreifen. Symantec Network Access Control arbeitet mit mehreren Enforcer-Typen, um den Client-Computer zu authentifizieren. Symantec Enforcer ist die Netzwerk-Hardware-Appliance, die Host-Integritätsergebnisse und die Identität des Client-Computers überprüft, bevor sie dem Computer den Netzwerkzugriff erlaubt.

Der Enforcer überprüft die folgenden Informationen, bevor er einen Client-Zugriff auf das Netzwerk erlaubt:

- Die Version der Clientsoftware, die der Computer ausführt.
- Der Client hat eine eindeutige Kennung (UID).
- Der Client wurde auf die neueste Host-Integritätsrichtlinie aktualisiert.
- Der Client-Computer hat die Host-Integritätsprüfung bestanden.

Siehe "Konfigurieren des Clients auf 802.1x-Authentifizierung" auf Seite 137.

Ausführen einer Host-Integritätsprüfung

Ihr Administrator konfiguriert die Häufigkeit, mit der der Client Host-Integritätsprüfungen ausführt. Sie müssen eine Host-Integritätsprüfung eventuell sofort ausführen und können nicht auf die nächste Prüfung warten. Beispielsweise kann eine fehlgeschlagene Host-Integritätsprüfung melden, dass Sie die Virenschutzsignaturen auf Ihrem Computer aktualisieren müssen. Sie können eventuell angeben, ob die erforderliche Software sofort oder erst später heruntergeladen werden soll. Wenn Sie die Software sofort herunterladen, müssen Sie die Host-Integritätsprüfung nochmals ausführen, um zu überprüfen, ob Sie die richtige Software haben. Sie können entweder warten, bis die folgende geplante Host-Integritätsprüfung ausgeführt wird oder Sie können die Prüfung sofort ausführen.

So führen Sie eine Host-Integritätsprüfung aus

1. Klicken Sie im Client in der Seitenleiste auf "Status".
2. Klicken Sie neben "Network Access Control" auf "Optionen > Compliance prüfen".
3. Klicken Sie auf "OK".

   Falls der Netzwerkzugriff blockiert war, sollten Sie wieder auf das Netzwerk zugreifen können, wenn der Computer so aktualisiert wurde, dass er den Sicherheitsrichtlinien entspricht.

Siehe "Wie Symantec Network Access Control funktioniert" auf Seite 133.

Bereinigen Ihres Computers

Wenn der Client erkennt, dass eine Host-Integritätsrichtlinienanforderung nicht erfüllt wird, reagiert er auf eine der folgenden Weisen:

- Der Client lädt das Software-Update automatisch herunter.
- Der Client fordert Sie auf, das erforderliche Software-Update herunterzuladen.

So bereinigen Sie Ihren Computer

- Im Symantec Endpoint Protection-Dialogfeld, das erscheint, wählen Sie eine der folgenden-Aktionen:
  - Um zu sehen, welche Sicherheitsanforderungen Ihr Computer nicht erfüllt, klicken Sie auf "Details".
  - Um die Software sofort zu installieren, klicken Sie auf "Jetzt wiederherstellen"

Sie haben ggf. die Option, die Installation abzubrechen, nachdem sie gestartet wurde.

- Um die Softwareinstallation hinauszuschieben, klicken Sie auf "Später erinnern" und wählen einen Zeitabstand in der Dropdown-Liste.
  Der Administrator kann konfigurieren, wie oft Sie die Installation hinausschieben können.

Konfigurieren des Clients auf 802.1x-Authentifizierung

Wenn Ihr Unternehmensnetzwerk einen LAN-Enforcer zur Authentifizierung verwendet, muss der Client-Computer entsprechend konfiguriert werden, um die 802.1x-Authentifizierung durchzuführen. Entweder Sie oder Ihr Administrator können den Client konfigurieren. Ihr Administrator hat Ihnen unter Umständen die Berechtigung erteilt, die 802.1x-Authentifizierung zu konfigurieren.

Der 802.1x-Authentifizierungsprozess umfasst die folgenden Schritte:

- Ein nicht authentifizierter Client oder ein Nicht-Symantec-Supplicant sendet die Benutzerinformationen und die Richtlinieneinhaltungsinformationen an einen verwalteten 802.1x-Netzwerk-Switch.
- Der Netzwerk-Switch gibt die Informationen an den LAN-Enforcer weiter. Der LAN-Enforcer sendet die Benutzerinformationen an den Authentifizierungsserver zur Authentifizierung. Der RADIUS-Server ist der Authentifizierungs-Server.
- Wenn beim Client die Benutzerebenen-Authentifizierung fehlschlägt oder er die Host-Integritätsrichtlinie nicht einhält, kann der Enforcer den Netzwerkzugriff blockieren. Der Enforcer platziert den nicht der Richtlinie entsprechenden Client-Computer in einem Quarantäne-Netzwerk, in dem der Computer bereinigt werden kann.
- Nachdem der Client den Computer korrigiert und ihn auf Richtlinieneinhaltung konfiguriert hat, authentifiziert das 802.1x-Protokoll den Computer erneut und bewilligt dem Computer Zugriff auf das Netzwerk.

Um mit dem LAN-Enforcer zusammenzuarbeiten, kann der Client entweder einen Nicht-Symantec-Supplicant oder einen integrierten Supplicant verwenden.

Tabelle 6-2 beschreibt die Typen von Optionen, die Sie für die 802.1x-Authentifizierung konfigurieren können.

Tabelle 6-2 Optionen für 802.1x-Authentifizierung

Option	Beschreibung
Nicht-Symantec-Supplicant	Verwendet einen Nicht-Symantec-802.1x-Supplicant. Der LAN-Enforcer arbeitet mit einem RADIUS-Server und Nicht-Symantec-802.1x-Supplicants, um die Benutzerauthentifizierung durchzuführen. Der 802.1x-Supplicant fordert Sie zur Eingabe von Benutzerinformationen auf. Der LAN-Enforcer leitet diese Benutzerinformationen zur Authentifizierung auf Benutzerebene an den RADIUS-Server weiter. Der Client sendet das Client-Profil und den Host-Integritätsstatus zum Enforcer, damit der Enforcer den Computer authentifiziert. **Hinweis:** Wenn Sie den Symantec Network Access Control-Client mit einem Nicht-Symantec-Supplicant verwenden möchten, dann muss das Netzwerkbedrohungsschutz-Modul des Symantec Endpoint Protection-Client installiert sein.
Transparentmodus	Benutzt den Client als 802.1x-Supplicant. Sie verwenden diese Methode, wenn der Administrator keinen RADIUS-Server zur Benutzerauthentifizierung verwenden möchte. Der LAN-Enforcer wird im Transparentmodus ausgeführt und tritt als Pseudo-RADIUS-Server auf. Transparentmodus bedeutet, dass der Supplicant Sie nicht zur Eingabe von Benutzerinformationen auffordert. Im Transparentmodus tritt der Client als 802.1x-Supplicant auf. Der Client reagiert auf die EAP-Anforderung des Switch mit dem Client-Profil und dem Host-Integritätsstatus. Der Switch leitet dann die Informationen an den LAN-Enforcer weiter, der als ein Pseudo-RADIUS-Server auftritt. Der LAN-Enforcer validiert die Host-Integritäts- und Client-Profil-Informationen vom Switch und kann dementsprechend ein VLAN zulassen, blockieren oder dynamisch zuweisen. **Hinweis:** Um einen Client als 802.1x-Supplicant zu verwenden, müssen Sie Nicht-Symantec-802.1x-Supplicants vom Client-Computer deinstallieren oder deaktivieren.
Integrierter Supplicant	Verwendet den integrierten 802.1x-Supplicant des Client-Computers. Die integrierten Authentifizierungsprotokolle umfassen Smartcard, PEAP oder TLS. Nachdem Sie 802.1x-Authentifizierung aktiviert haben, müssen Sie angeben, welches Authentifizierungsprotokoll verwendet werden soll.

Warnung: Kontaktieren Sie Ihren Administrator, bevor Sie Ihren Client für 802.1x-Authentifizierung konfigurieren. Sie müssen wissen, ob Ihr Unternehmensnetzwerk den RADIUS-Server als Authentifizierungs-Server verwendet. Wenn Sie die 802.1x-Authentifizierung falsch konfigurieren, können Sie Ihre Verbindung zum Netzwerk unterbrechen.

So konfigurieren Sie den Client dafür, einen Nicht-Symantec-Supplicant zu verwenden

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Neben Network Access Control klicken Sie auf "Optionen > Einstellungen ändern > 802.1x-Einstellungen".
3. Klicken Sie im Dialogfeld "Einstellungen für Network Access Control" auf "802.1x-Authentifizierung aktivieren".
4. Klicken Sie auf "OK".

   Sie müssen auch eine Firewall-Regel einrichten, die Nicht-Symantec-802.1x-Supplicant-Treiber im Netzwerk zulässt.

   Siehe "Hinzufügen einer Firewall-Regel" auf Seite 116.

   Sie können den Client so konfigurieren, dass der integrierte Supplicant verwendet wird. Sie aktivieren den Client für 802.1x-Authentifizierung und als 802.1x-Supplicant.

So konfigurieren Sie den Client dafür, den Transparentmodus oder einen integrierten Supplicant zu verwenden

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Neben Network Access Control klicken Sie auf "Optionen > Einstellungen ändern > 802.1x-Einstellungen".
3. Klicken Sie im Dialogfeld "Einstellungen für Network Access Control" auf "802.1x-Authentifizierung aktivieren".
4. Klicken Sie auf "Client als 802.1x-Supplicant verwenden".
5. Führen Sie einen der folgenden Schritte aus:
   - Um den Transparentmodus auszuwählen, aktivieren Sie "Symantec-Transparentmodus verwenden".
   - Um einen integrierten Supplicant zu konfigurieren, klicken Sie auf "Benutzer kann Authentifizierungprotokoll selbst wählen". Sie müssen dann das Authentifizierungsprotokoll für Ihre Netzwerkverbindung auswählen.
6. Klicken Sie auf "OK".

So wählen Sie ein Authentifizierungsprotokoll aus

1. Auf dem Client-Computer klicken Sie auf "Start" > "Einstellungen" > "Netzwerkverbindungen" und klicken dann auf "Lokale Verbindung".

   Hinweis: Diese Schritte sind für Computer geschrieben, auf denen Windows XP ausgeführt wird. Ihre Vorgehensweise variiert möglicherweise.

2. Im Dialogfeld "LAN-Verbindungsstatus" klicken Sie auf "Eigenschaften".
3. Klicken Sie im Dialogfeld "Eigenschaften von LAN-Verbindung" auf die Registerkarte "Authentifizierung".
4. Wählen Sie auf der Registerkarte "Authentifizierung" in der Dropdown-Liste "EAP-Typ" eines der Authentifizierungsprotokolle aus.

   Vergewissern Sie sich, dass das Kontrollkästchen "IEEE 802.1x-Authentifizierung für dieses Netzwerk aktivieren" aktiviert ist.
5. Klicken Sie auf "OK".
6. Klicken Sie auf "Schließen".

Siehe "Wie Symantec Network Access Control funktioniert" auf Seite 133.

Erneutes Authentifizieren Ihres Computers

Wenn Ihr Computer die Host-Integritätsprüfung bestanden hat, aber der Enforcer Ihren Computer blockiert, ist es möglicherweise erforderlich, Ihren Computer erneut zu authentifizieren. Unter normalen Umständen sollte es nie nötig sein, Ihren Computer erneut zu authentifizieren.

Der Enforcer kann den Computer blockieren, wenn eines der folgenden Ereignisse eintritt:

- Die Benutzerauthentifizierung des Client-Computers schlug fehl, weil Sie Ihren Benutzernamen oder Ihr Kennwort falsch eingegeben haben.
- Ihr Client-Computer ist im falschen VLAN.
- Der Client-Computer erhielt keine Netzwerkverbindung. Eine unterbrochene Netzwerkverbindung tritt normalerweise auf, weil der Switch zwischen dem Client-Computer und dem LAN-Enforcer Ihren Benutzernamen und Ihr Kennwort nicht authentifizierte.
- Sie haben sich bei einem Client-Computer eingeloggt, der einen vorherigen Benutzer authentifizierte.
- Auf dem Client-Computer schlug die Prüfung der Richtlinieneinhaltung fehl.

Sie können den Computer nur erneut authentifizieren, wenn Sie oder Ihr Administrator den Computer mit einem integrierten Supplicant konfiguriert haben.

Hinweis: Ihr Administrator kann den Client möglicherweise so konfiguriert haben, dass der Befehl "Erneute Authentifizierung" nicht angezeigt wird.

So authentifizieren Sie Ihren Computer erneut

1. Klicken Sie mit der rechten Maustaste auf das Benachrichtigungsbereichssymbol.
2. Klicken Sie auf "Erneute Authentifizierung...".
3. Geben Sie im Dialogfeld "Erneut authentifizieren" Ihren Benutzernamen und das Kennwort ein.
4. Klicken Sie auf "OK".

Siehe "Wie Symantec Network Access Control funktioniert" auf Seite 133.

Anzeigen der Symantec Network Access Control-Protokolle

Der Symantec Network Access Control-Client verwendet die folgenden Protokolle, um verschiedene Aspekte seines Betriebs und die Ergebnisse der Host-Integritätsprüfung zu überwachen:

Sicherheit	Zeichnet die Ergebnisse und den Status der Host-Integritätsprüfungen auf.
System	Zeichnet alle Betriebsänderungen für den Client, wie die Verbindung zum Management-Server und Updates zu den Client-Sicherheitsrichtlinien, auf.

Wenn Sie einen verwalteten Client verwenden, können beide Protokolle regelmäßig auf den Server hochgeladen werden. Ihr Administrator kann den Inhalt in den Protokollen verwenden, um den Gesamtsicherheitsstatus des Netzwerkes zu analysieren.

Sie können die Protokolldaten aus diesen Protokollen exportieren.

So zeigen Sie Symantec Network Access Control-Protokolle an

1. Kicken Sie im Client in der Seitenleiste auf Status.
2. Um das "Sicherheitsprotokoll" anzuzeigen, klicken Sie neben Network Access Control auf "Optionen" > "Protokolle anzeigen".
3. In "Sicherheitsprotokoll" wählen Sie den ersten Protokoll-Eintrag aus.

   In der linken unteren Ecke erscheinen die Host-Integritätsprüfung-Ergebnisse. Wenn der Client bereits installiert wurde, wird die definierte Firewallanforderung zugelassen. Wenn der Client nicht installiert wurde, schlägt die definierte Firewallanforderung fehl, wird jedoch als "zugelassen" gemeldet.
4. Um das "Systemprotokoll" anzuzeigen, klicken Sie im Dialogfeld "Sicherheitsprotokoll - Symantec Network Access Control-Protokolle" auf "Ansicht" > "Systemprotokoll".
5. Klicken Sie auf "Datei > Schließen".

   Siehe "Info zu Protokollen" auf Seite 46.

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W