System Center

Endpoint Protection für Mac

Installations- und Benutzerhandbuch

Microsoft

Inhalt

System Center Endpoint Protection

Aufgrund der steigenden Beliebtheit von Unix-basierten Betriebssystemen wird immer häufiger Malware entwickelt, die auf Mac-Benutzer abzielt. System Center Endpoint Protection bietet einen starken und effizienten Schutz gegen diese neuen Bedrohungen. System Center Endpoint Protection ist außerdem in der Lage, Windows-Bedrohungen abzuwehren und dadurch Mac-Benutzer zu schützen, wenn sie mit Windows-Benutzern interagieren und umgekehrt. Malware für Windows stellt zwar keine direkte Bedrohung für Mac-Systeme dar, aber durch die Deaktivierung von Schadsoftware, die einen Mac-Computer infiziert hat, kann die Ausbreitung auf Windows-basierte Computer über ein lokales Netzwerk oder das Internet verhindert werden.

Systemanforderungen

Um mit System Center Endpoint Protection eine optimale Leistung zu erreichen, sollten die folgenden Hardware- und Softwareanforderungen erfüllt sein:

System Center Endpoint Protection:

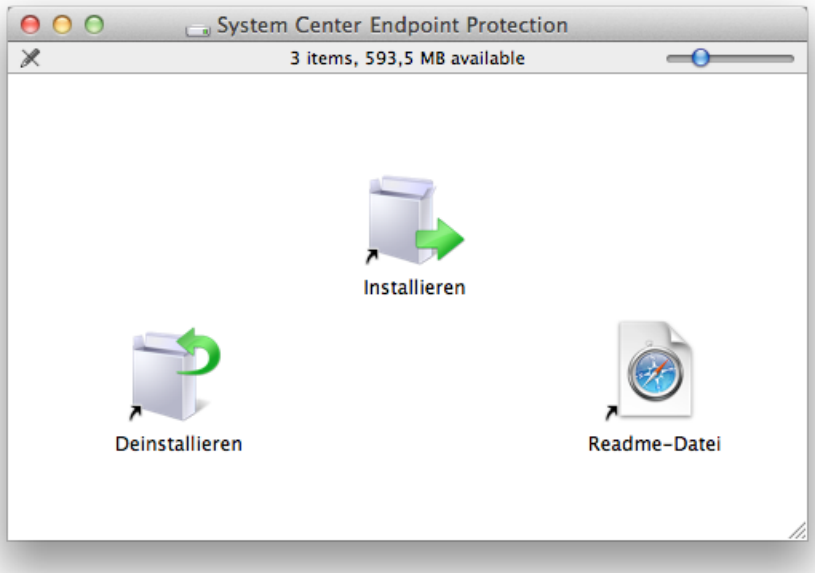
	Systemanforderungen
Prozessorarchitektur	Intel® Prozessor mit 32/64 Bit
Betriebssystem	Mac OS X 10.6 oder höher
Arbeitsspeicher	512 MB
Freier Speicher	100 MB

Installation

Bitte schließen Sie alle laufenden Programme, bevor Sie mit der Installation beginnen. System Center Endpoint Protection enthält Komponenten, durch die es zu Konflikten mit anderen Virenschutzprogrammen auf Ihrem Computer kommen kann. Es wird daher dringend empfohlen, alle anderen Virenschutzprogramme zu deinstallieren, um Probleme zu vermeiden. Sie können System Center Endpoint Protection von einer Installations-CD/-DVD oder aus einer Download-Datei von unserer Website installieren.

Führen Sie einen der folgenden Schritte aus, um den Installationsassistenten zu starten:

- Bei der Installation per CD/DVD legen Sie diese in Ihren Computer ein, öffnen Sie sie über den Desktop oder ein Finder-Fenster und doppelklicken Sie auf das Symbol **Installieren**.
- Wenn Sie zur Installation eine heruntergeladene Datei verwenden, öffnen Sie diese und doppelklicken Sie auf das Symbol **Installieren**.



Starten Sie das Installationsprogramm. Der Installationsassistent unterstützt Sie bei der Installation. Nachdem Sie der Software-Lizenzvereinbarung zugestimmt und die Datenschutzerklärung gelesen haben, können Sie eine der folgenden Installationsarten wählen:

- Typisch 4
- Benutzerdefiniert 5

Standardinstallation

Bei der Standardinstallation wird eine Konfiguration verwendet, die für die Anforderungen der meisten Benutzer geeignet ist. Sie bietet optimale Sicherheit und gleichzeitig gute Systemleistung. Die Standardinstallation wird daher empfohlen, wenn Sie keine speziellen Anforderungen an die Konfiguration haben.

Nach Auswahl der Installationsart **Typisch** (Standardinstallation) richten Sie zunächst die Option **Prüfen auf „Evtl. unerwünschte Anwendungen“** ein. Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können. Diese Anwendungen sind oft mit anderen Programmen gebündelt und daher während des Installationsvorgangs schwer erkennbar. Obwohl bei solchen Anwendungen während der Installation gewöhnlich eine Benachrichtigung angezeigt wird, können sie auch leicht ohne Ihre Zustimmung installiert werden.

Nach der Installation von System Center Endpoint Protection sollte geprüft werden, ob auf dem Computer Schadcode vorhanden ist. Klicken Sie dazu im Hauptprogrammfenster auf **Computer prüfen** und dann auf **Smart-Prüfung**. Nähere Informationen zur On-Demand-Prüfung finden Sie im Abschnitt On-Demand-Prüfung 10.

Benutzerdefinierte Installation

Die benutzerdefinierte Installation eignet sich für fortgeschrittene Benutzer, die während der Installation die erweiterten Einstellungen ändern möchten.

Nach Auswahl der Installationsart **Benutzerdefiniert** wird zunächst ein ggf. verwendeter **Proxyserver** eingerichtet. Wenn Sie einen Proxyserver verwenden, können Sie die entsprechenden Parameter festlegen. Wählen Sie dazu die Option **Ich nutze einen Proxyserver**. Geben Sie unter **Adresse** die IP-Adresse oder URL des Proxyservers ein. Im Feld „Port“ können Sie den Port angeben, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Falls für den Proxyserver Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie einen gültigen **Benutzernamen** und das **Passwort** ein. Wenn Sie sicher sind, dass Sie keinen Proxyserver verwenden, wählen Sie die Option **Keinen Proxyserver verwenden**. Wenn Sie unsicher sind, können Sie Ihre aktuellen Systemeinstellungen verwenden. Wählen Sie dazu **Systemeinstellungen verwenden (empfohlen)**.

Im nächsten Schritt können Sie **privilegierte Benutzer definieren**, die berechtigt sind, die Programmkonfiguration zu ändern. Wählen Sie aus der Liste links die Benutzer aus und fügen Sie sie über die Schaltfläche **Hinzufügen** zur Liste **Privilegierte Benutzer** hinzu. Um alle Systembenutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen**.

Im nächsten Schritt der Installation wird die Option **Prüfen auf „Evtl. unerwünschte Anwendungen“** konfiguriert. Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können. Diese Anwendungen sind oft mit anderen Programmen gebündelt und daher während des Installationsvorgangs schwer erkennbar. Obwohl bei solchen Anwendungen während der Installation gewöhnlich eine Benachrichtigung angezeigt wird, können sie auch leicht ohne Ihre Zustimmung installiert werden.

Nach der Installation von System Center Endpoint Protection sollte geprüft werden, ob auf dem Computer Schadcode vorhanden ist. Klicken Sie dazu im Hauptprogrammfenster auf **Computer prüfen** und dann auf **Smart-Prüfung**. Nähere Informationen zur On-Demand-Prüfung finden Sie im Abschnitt On-Demand Prüfung 10.

Deinstallation

Zur Deinstallation von System Center Endpoint Protection wählen Sie eine der folgenden Methoden:

- Legen Sie die Installations-CD/-DVD von System Center Endpoint Protection in Ihren Computer ein, öffnen Sie sie über den Desktop oder ein Finder-Fenster und doppelklicken Sie auf das Symbol **Deinstallieren**.
- Öffnen Sie die Installationsdatei von System Center Endpoint Protection (*DMG*-Datei) und doppelklicken Sie auf das Symbol **Deinstallieren**.
- Öffnen Sie im **Finder** den Ordner **Programme** auf Ihrer Festplatte, halten Sie die Ctrl-Taste gedrückt, klicken Sie auf das Symbol von System Center Endpoint Protection und wählen Sie **Paketinhalt zeigen**. Öffnen Sie den Ordner **Contents > Helpers** und doppelklicken Sie auf das Symbol zur **Uninstaller**.

Erste Schritte

Dieses Kapitel enthält eine einführende Übersicht über System Center Endpoint Protection und die Grundeinstellungen des Programms.

Benutzeroberfläche

Das Hauptprogrammfenster von System Center Endpoint Protection ist in zwei Abschnitte unterteilt. Das primäre Fenster (rechts) zeigt Informationen zu den im Hauptmenü (links) ausgewählten Optionen an.

Im Folgenden werden die Optionen des Hauptmenüs beschrieben:

- **Schutzstatus** - Informationen zum Schutzstatus von System Center Endpoint Protection. Wenn die Option **Erweiterter Modus** aktiviert ist, wird das Untermenü **Statistiken** angezeigt.
- **Computer prüfen** - In diesem Abschnitt können Sie bei Bedarf eine On-Demand-Prüfung starten oder die Einstellungen dazu ändern.
- **Update** - Informationen über Updates der Signaturdatenbank.
- **Einstellungen** - Wählen Sie diese Option, um die Sicherheitsstufe Ihres Computers anzupassen. Wenn die Option **Erweiterter Modus** aktiviert ist, wird das Untermenü **Viren- und Spyware-Schutz** angezeigt.
- **Tools** - Zugriff auf **Log-Dateien**, **Quarantäne** und **Taskplaner**. Diese Option wird nur im **Erweiterten Modus** angezeigt.
- **Hilfe** - Informationen zum Programm und Zugriff auf die Hilfedateien.

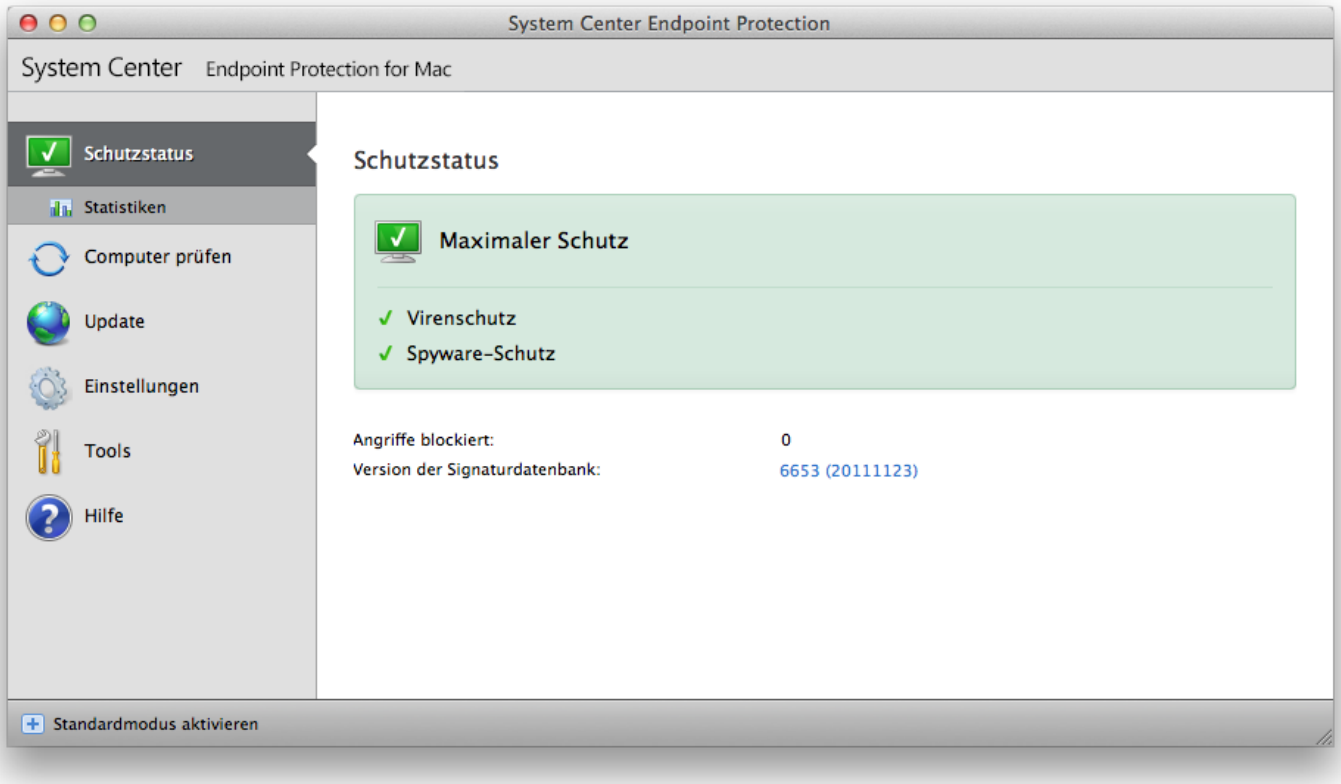
Über die System Center Endpoint Protection-Benutzeroberfläche können Sie zwischen Standardmodus und erweitertem Modus wechseln. Im Standardmodus können Sie auf Funktionen zugreifen, die für allgemeine Vorgänge benötigt werden. Die erweiterten Einstellungen werden nicht angezeigt. Um zwischen den Modi zu wechseln, klicken Sie auf das Pluszeichen (**+**) neben **Erweiterten Modus aktivieren/Standardmodus aktivieren** links unten im Hauptprogrammfenster oder drücken Sie Cmd+M.

Beim Wechsel in den erweiterten Modus wird dem Hauptmenü die Option **Tools** hinzugefügt. Über die Option **Tools** können Sie auf Untermenüs zu **Log-Dateien**, **Quarantäne** und **Taskplaner** zugreifen.

HINWEIS: Die weiteren Anweisungen in diesem Handbuch beziehen sich auf den **Erweiterten Modus**.

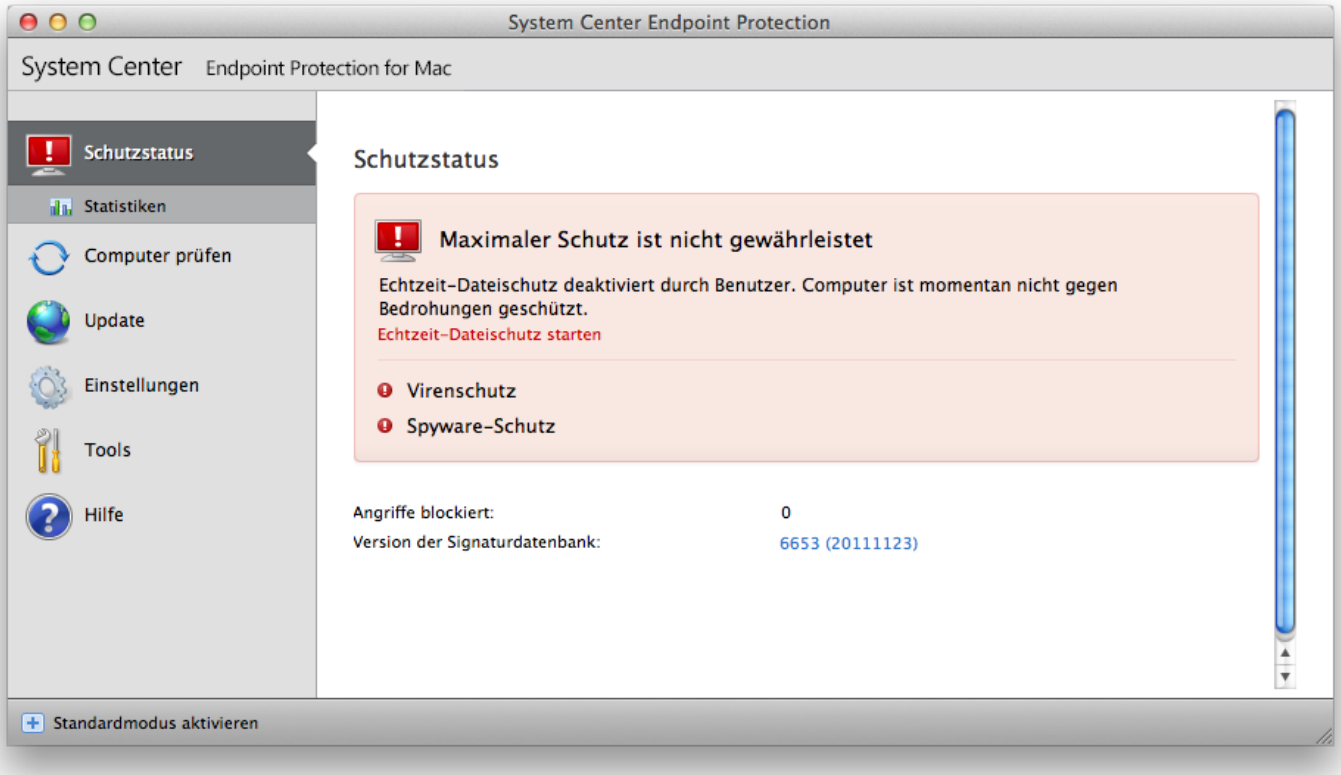
Überprüfen der Funktionsfähigkeit des Systems

Zum Anzeigen des **Schutzstatus** klicken Sie auf die oberste Option im Hauptmenü. Im primären Fenster befindet sich eine Darstellung des aktuellen Betriebszustands von System Center Endpoint Protection, außerdem wird ein Untermenü mit **Statistiken** angezeigt. Wählen Sie es aus, um genaue Informationen und Statistiken zu Prüfungen anzuzeigen, die auf Ihrem System durchgeführt wurden. Das Fenster „Statistiken“ steht nur im erweiterten Modus zur Verfügung.



Vorgehensweise bei fehlerhafter Ausführung des Programms

Wenn die aktivierten Module ordnungsgemäß arbeiten, sind sie mit einem grün hinterlegten Häkchen markiert. Andernfalls wird ein rotes oder orangefarbenes Symbol mit Ausrufezeichen angezeigt. Weitere Informationen zu dem Modul erhalten Sie im oberen Teil des Fensters. Unter anderem finden Sie dort einen Vorschlag zur Behebung des Problems. Um den Status einzelner Module zu ändern, klicken Sie im Hauptmenü auf **Einstellungen** und wählen das gewünschte Modul aus.



Arbeiten mit System Center Endpoint Protection

Viren- und Spyware-Schutz

Der Virenschutz bewahrt das System vor Attacken, indem er potenziell gefährliche Dateien verändert. Wird eine Bedrohung durch Schadcode erkannt, kann das Virenschutz-Modul den Code unschädlich machen, indem es die Ausführung des Codes blockiert und dann den Code entfernt bzw. die Datei löscht oder in die Quarantäne verschiebt.

Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle für den Virenschutz relevanten Systemereignisse. Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf Ihrem Computer auf Schadcode geprüft. Der Echtzeit-Dateischutz wird beim Systemstart gestartet.

Einstellungen für Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle Datenträger auf das Eintreten bestimmter Ereignisse. Er kann für neu erstellte und vorhandene Dateien unterschiedlich gestaltet werden. Neu erstellte Dateien können einer noch gründlicheren Prüfung unterzogen werden.

Der Echtzeit-Dateischutz wird standardmäßig beim Systemstart gestartet und fortlaufend ausgeführt. In besonderen Fällen (z. B. bei einem Konflikt mit einem anderen Echtzeit-Prüfprogramm) kann der Echtzeit-Dateischutz durch Klicken auf das System Center Endpoint Protection-Symbol in der oberen Menüleiste und Auswählen der Option **Echtzeit-Dateischutz deaktivieren** beendet werden. Der Echtzeit-Dateischutz kann auch im Hauptfenster deaktiviert werden (**Einstellungen** > **Viren- und Spyware-Schutz** > **Deaktivieren**).

Um die erweiterten Einstellungen für den Echtzeit-Dateischutz zu ändern, gehen Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Schutz** > **Echtzeit-Dateischutz** und klicken neben **Erweiterte Einstellungen** auf **Einstellungen** (siehe Abschnitt Erweiterte Optionen für Prüfungen 8).

Prüfen beim (Prüfen bei Ereignis)

Standardmäßig werden alle Dateien beim **Öffnen**, **Ausführen** und **Erstellen** geprüft. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. So bietet der Echtzeit-Dateischutz auf Ihrem Computer maximale Sicherheit.

Erweiterte Optionen für Prüfungen

In diesem Fenster können Sie die zu prüfenden Objekttypen festlegen, die **Advanced Heuristik** aktivieren bzw. deaktivieren sowie die Einstellungen für Archive und den Datei-Cache ändern.

Die Standardwerte im Abschnitt **Standard-Archiveinstellungen** sollten Sie nur ändern, um konkrete Probleme zu lösen, da höhere Archivverschachtelungswerte die Systemleistung beeinträchtigen können.

Sie können die Advanced Heuristik für ausführbare, erstellte und geänderte Dateien einzeln ein- bzw. ausschalten. Aktivieren Sie dazu jeweils das Kontrollkästchen **Advanced Heuristik** im Abschnitt des entsprechenden Prüfmodul-Parameters.

Um eine möglichst geringe Systembelastung während des Echtzeit-Dateischutzes zu gewährleisten, können Sie die Größe des Optimierungs-Cache festlegen. Dieses Verhalten ist aktiv, wenn Sie die Option **Cache für nicht infizierte Dateien aktivieren** verwenden. Ist diese Option deaktiviert, werden alle Dateien bei jedem Zugriff geprüft. Ansonsten werden nicht infizierte Dateien bis zur festgelegten Cache-Größe im Cache gespeichert und anschließend nicht mehr geprüft, es sei denn, sie wurden geändert. Nach einem Update der Signaturdatenbank werden die Dateien sofort wieder geprüft.

Klicken Sie auf **Cache für nicht infizierte Dateien aktivieren**, um diese Funktion zu aktivieren bzw. deaktivieren. Um die Anzahl der Dateien festzusetzen, die im Cache gespeichert werden sollen, geben Sie einfach den gewünschten Wert ins Feld **Cache-Größe** ein.

Zusätzliche Prüfparameter können im Fenster **Prüfmodul-Einstellungen** festgelegt werden. Sie können angeben, welche Typen von **Objekten** geprüft werden sollen, mit welchen **Optionen** und auf welcher **Säuberungsstufe**. Außerdem können Sie die **Erweiterungen** und **Grenzen** für Dateigrößen für den Echtzeit-Dateischutz definieren. Das Fenster mit den Prüfmodul-Einstellungen erreichen Sie über die Schaltfläche **Einstellungen** neben **Prüfmodul** im Fenster **Erweiterte Einstellungen**. Ausführliche Informationen zu den Prüfmodul-Einstellungen finden Sie im Abschnitt Prüfmodul-Einstellungen 13.

Ausschlussfilter für Prüfungen

In diesem Bereich können Sie festlegen, dass bestimmte Dateien und Ordner von Prüfungen ausgenommen werden.

- **Pfad** - Pfad zu den auszuschließenden Dateien/Ordnern
- **Bedrohung** – Steht neben einer ausgeschlossenen Datei der Name einer Bedrohung, so gilt die Ausnahme nicht generell für die Datei, sondern nur für diese bestimmte Bedrohung. Wird die Datei also später durch andere Schadsoftware infiziert, erkennt der Virenschutz dies.

- **Hinzufügen...** - Objekte von der Prüfung ausnehmen. Geben Sie den Pfad zum Objekt ein (Platzhalter *und ?werden unterstützt) oder wählen Sie den Ordner bzw. die Datei in der Baumstruktur aus.
- **Bearbeiten...** - Ausgewählten Eintrag bearbeiten
- **Löschen** - Ausgewählten Eintrag löschen
- **Standard** - Alle Ausnahmen löschen.

Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Dateischutz ist die wichtigste Komponente für ein sicheres System. Änderungen an den Parametern des Echtzeit-Dateischutzes sind mit Bedacht vorzunehmen. Es wird empfohlen, nur in einzelnen Fällen die Parameter zu verändern. Es kann beispielsweise erforderlich sein, wenn ein Konflikt mit einer bestimmten Anwendung oder der Echtzeit-Prüfung eines anderen Virenschutzprogramms vorliegt.

Bei der Installation von System Center Endpoint Protection werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Um die Standardeinstellungen wiederherzustellen, klicken Sie auf die Schaltfläche **Standard** unten links im Fenster **Echtzeit-Dateischutz** (**Einstellungen** > **Erweiterte Einstellungen** > **Schutz** > **Echtzeit-Dateischutz**).

Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz aktiv ist und Viren erkennt, verwenden Sie die Testdatei eicar.com. Diese Testdatei ist harmlos und wird von allen Virenschutzprogrammen erkannt. Die Datei wurde vom EICAR-Institut (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen.

Zur Remote-Überprüfung des Echtzeit-Dateischutzes stellen Sie über **Terminal** eine Verbindung zum Clientcomputer her und geben Sie den folgenden Befehl ein:

```
/Applications/.scep/Contents/MacOS/scep_daemon --status
```

Der Status des Echtzeit-Scanners wird entweder als `RTPStatus=Enabled` oder als `RTPStatus=Disabled` angezeigt.

Die Ausgabe des Terminal-Bash enthält zudem folgende Statusangaben:

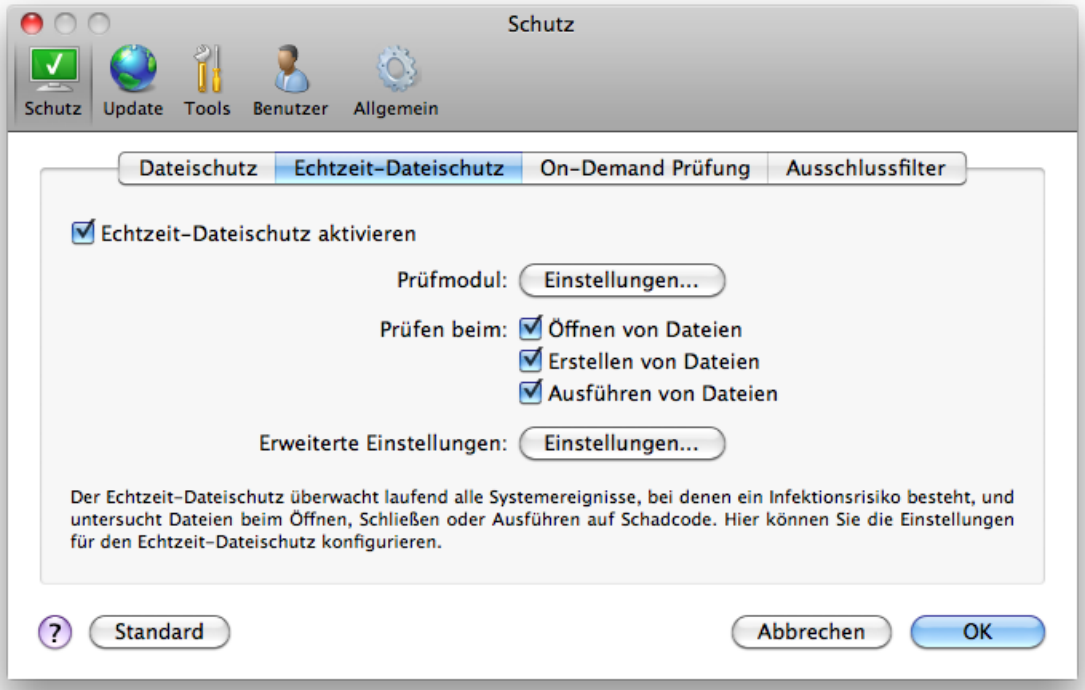
- Version des auf dem Clientcomputer installierten System Center Endpoint Protection
- Datum und Version der Signaturdatenbank
- Pfad zum Update-Server

HINWEIS: Das Terminal sollte nur von fortgeschrittenen Benutzern verwendet werden.

Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

In diesem Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

Echtzeit-Dateischutz ist deaktiviert
Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Dateischutz wieder zu aktivieren, wählen Sie **Einstellungen** > **Viren- und Spyware-Schutz**, und klicken Sie auf den Link **Echtzeit-Dateischutz aktivieren** (rechts) im Hauptprogrammfenster. Alternativ dazu können Sie den Echtzeit-Dateischutz im Fenster **Erweiterte Einstellungen** unter **Schutz** > **Echtzeit-Dateischutz** aktivieren. Wählen Sie dazu die Option **Echtzeit-Dateischutz aktivieren**.



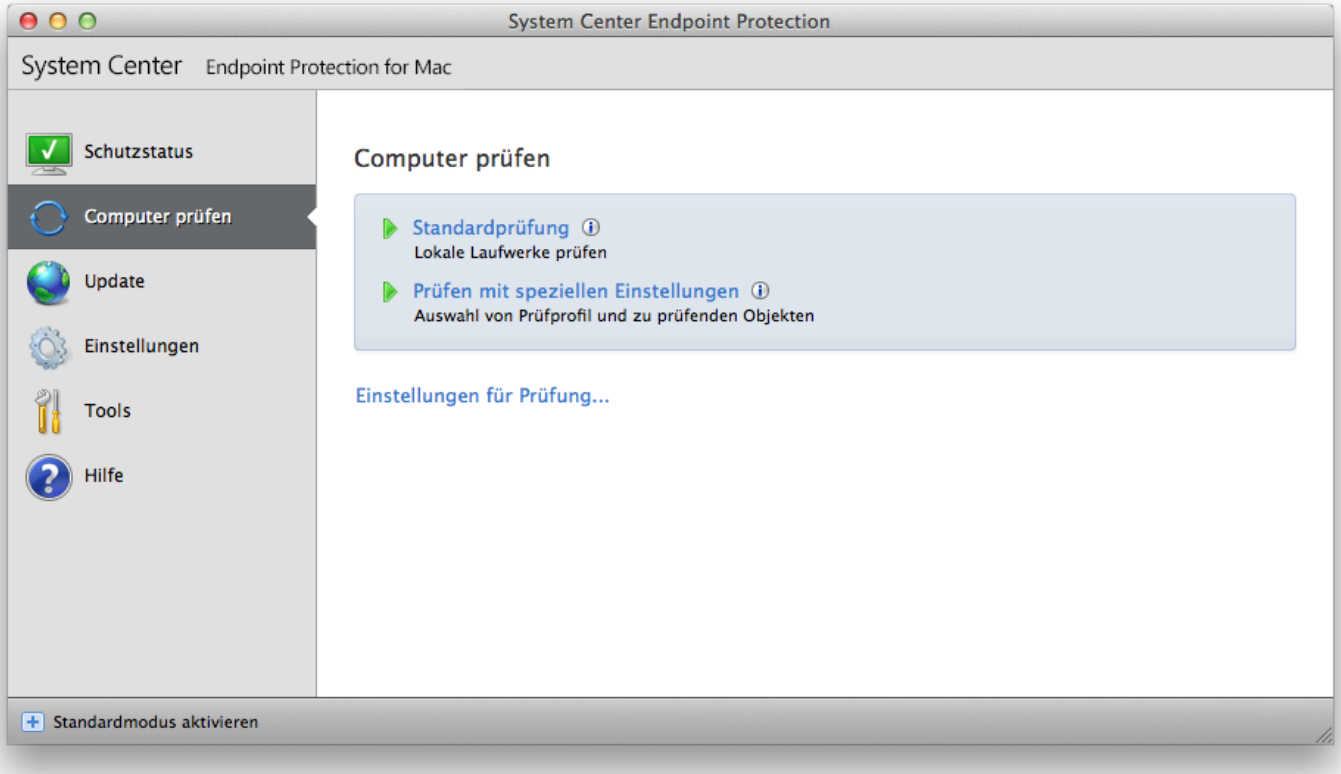
Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode
Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel ausgeführte Schutzprogramme können miteinander in Konflikt geraten. Wir empfehlen Ihnen, alle anderen Virusschutzprogramme zu deinstallieren.

Echtzeit-Dateischutz startet nicht
Wenn der Echtzeit-Dateischutz nicht automatisch beim Systemstart startet, können Konflikte mit anderen Programmen vorliegen. Sollte dies der Fall sein, wenden Sie sich an einen der Experten vom Support.

On-Demand-Prüfung

Wenn Sie den Verdacht haben, dass Ihr Computer infiziert ist (anormales Verhalten), starten Sie über **Computer prüfen** > **Smart-Prüfung** eine manuelle Prüfung, um Ihren Computer auf eingedrungene Schadsoftware zu untersuchen. Um maximalen Schutz zu gewährleisten, sollten Sie solche Prüfungen routinemäßig durchführen und nicht nur, wenn eine Infektion vermutet wird. Durch regelmäßige Prüfungen kann eingedrungene Schadsoftware erkannt werden, die vom Echtzeit-Dateischutz zum Zeitpunkt der Speicherung der Schadsoftware nicht erkannt wurde. Dies kommt z. B. vor, wenn die Echtzeit-Prüfung zum Zeitpunkt der Infektion deaktiviert war oder die Signaturdatenbank nicht auf dem neuesten Stand ist.

Sie sollten mindestens einmal im Monat eine On-Demand-Prüfung vornehmen. Sie können die Prüfung als Task unter **Tools** > **Taskplaner** konfigurieren.



Sie können auch ausgewählte Dateien und Ordner von Ihrem Desktop oder aus dem Finder-Fenster per Drag & Drop auf dem Hauptbildschirm, Dock-Symbol, Menüleistensymbol (oberer Bildschirmrand) oder Anwendungssymbol (im Ordner */Programme*) von System Center Endpoint Protection ablegen.

Prüfungstyp

Es gibt zwei verschiedene Arten von On-Demand-Prüfungen. Bei der **Smart-Prüfung** (Standardprüfung) wird das System schnell überprüft, ohne dass Sie dafür weitere Prüfparameter konfigurieren müssen. Bei der Methode **Benutzerdefinierte Prüfung** können Sie ein vordefiniertes Prüfprofil und die zu prüfenden Objekte auswählen.

Smart-Prüfung

Mit der Smart-Prüfung (Standardprüfung) können Sie schnell den Computer prüfen und infizierte Dateien säubern, ohne eingreifen zu müssen. Die Bedienung ist einfach, und es ist keine ausführliche Konfiguration erforderlich. Bei der Smart-Prüfung werden alle Dateien in allen Ordnern geprüft, und erkannte Infiltrationen werden automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungsarten finden Sie unter Säubern 14.

Benutzerdefinierte Prüfung

Über die Option **Benutzerdefinierte Prüfung** können Sie Prüfparameter wie die zu prüfenden Objekte oder Prüfmethoden festlegen. Der Vorteil dieser Methode ist die Möglichkeit zur genauen Parameterkonfiguration. Verschiedene Konfigurationen können als benutzerdefinierte Prüfprofile gespeichert werden. Das ist sinnvoll, wenn Prüfungen wiederholt mit denselben Parametern ausgeführt werden.

Zum Festlegen der zu prüfenden Objekte wählen Sie **Computer prüfen** > **Benutzerdefinierte Prüfung** und wählen dann bestimmte **Zu prüfende Objekte** aus der Baumstruktur aus. Sie können ein zu prüfendes Objekt auch genauer bestimmen, indem Sie den Pfad zu dem Ordner oder den Dateien eingeben, die geprüft werden sollen. Wenn Sie nur das System ohne zusätzliche Säuberung prüfen möchten, wählen Sie die Option **Nur Prüfen, keine Aktion**. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf **Einstellungen** > **Säubern**.

Eine Prüfung des Computers mit dieser Methode wird nur fortgeschrittenen Benutzern empfohlen, die Erfahrung im Umgang mit Virenschutzprogrammen haben.

Zu prüfende Objekte

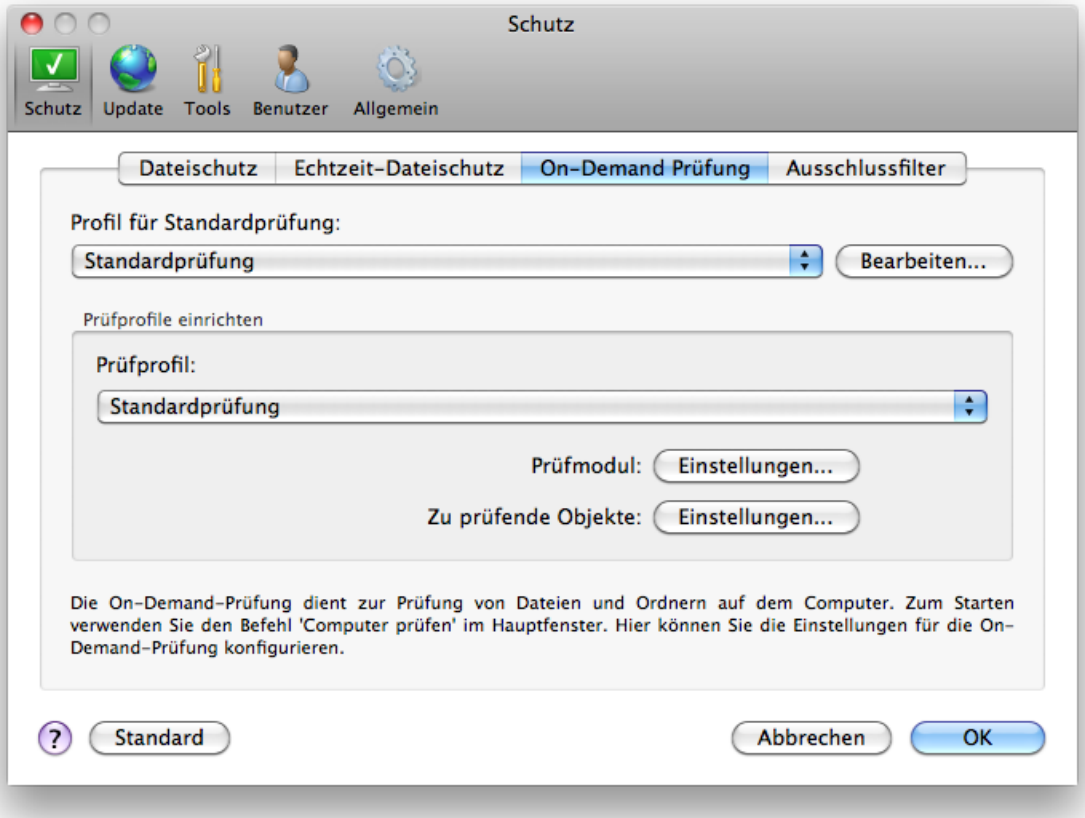
In der Baumstruktur der zu prüfenden Objekte können Sie Dateien und Ordner auswählen, die auf Viren geprüft werden sollen. Im Prüfprofil können Sie die Prüfung von Ordnern festlegen.

Sie können ein zu prüfendes Objekt auch genauer definieren, indem Sie den Pfad zu dem Ordner oder den Dateien eingeben, die geprüft werden sollen. Wählen Sie die zu prüfenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Ordner aufgelistet werden.

Prüfprofile

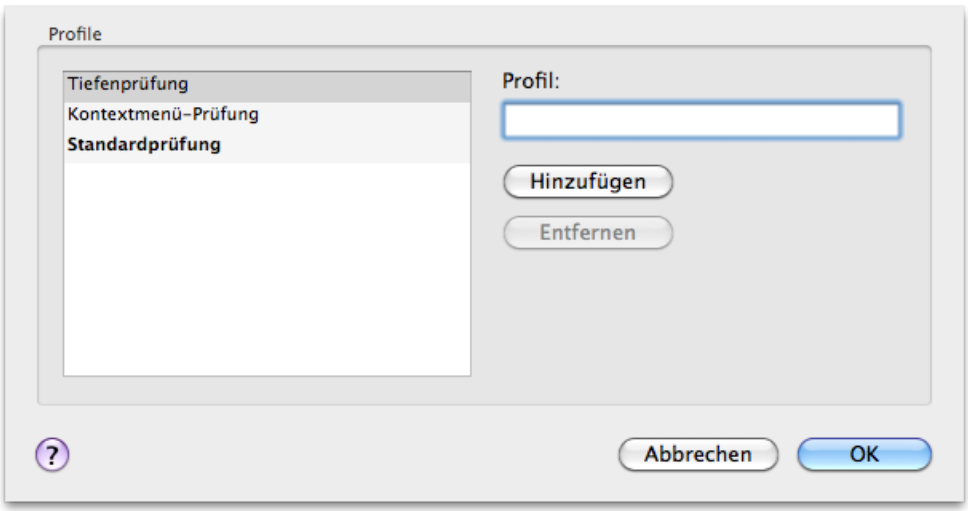
Ihre benutzerdefinierten Einstellungen können für zukünftige Prüfungen gespeichert werden. Wir empfehlen Ihnen, für jede regelmäßig durchgeführte Prüfung ein eigenes Profil zu erstellen (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern).

Zur Erstellung eines neuen Profils gehen Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Schutz** > **Computer prüfen** und klicken auf **Bearbeiten** neben der Liste der aktuell bestehenden Profile.



Eine Beschreibung der einzelnen Prüfeinstellungen finden Sie im Abschnitt Prüfmodul-Einstellungen 13. So können Sie ein Prüfprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

Beispiel: Nehmen wir an, Sie möchten Ihr eigenes Prüfprofil erstellen. Die Smart-Prüfung eignet sich in gewissem Maße, aber Sie möchten nicht die laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen prüfen. Außerdem möchten Sie die Option „Automatisch säubern“ anwenden. Geben Sie im Fenster **Profile für On-Demand-Scanner** den Profilnamen ein, klicken Sie auf **Hinzufügen** und bestätigen Sie mit **OK**. Passen Sie dann die Parameter unter **Prüfmodul** und **Zu prüfende Objekte** an Ihre Anforderungen an.



Prüfmodul-Einstellungen

Die Prüftechnologie von System Center Endpoint Protection arbeitet proaktiv, d. h., sie schützt das System auch während der ersten Stunden eines neuen Angriffs. Eingesetzt wird eine Kombination verschiedener Methoden (Code-Analyse, Code-Emulation, allgemeine Signaturen, Virussignaturen), die zusammen die Systemsicherheit deutlich erhöhen. Das Prüfmodul kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Diese Technologie entfernt auch Rootkits erfolgreich.

In den Prüfmodul-Einstellungen können Sie verschiedene Prüfparameter festlegen:
- Dateitypen und -erweiterungen, die geprüft werden sollen
- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

Zum Öffnen der Einstellungen klicken Sie auf **Einstellungen** > **Viren- und Spyware-Schutz** > **Einstellungen für Viren- und Spyware-Schutz** und dann auf die Schaltfläche **Einstellungen** im Bereich **Systemschutz**, **Echtzeit-Dateischutz** bzw. **Computer prüfen**. Je nach Anforderung sind eventuell verschiedene Sicherheitseinstellungen erforderlich. Dies sollte bei den individuellen Prüfmodul-Einstellungen für die folgenden Schutzmodule berücksichtigt werden:
- **Systemschutz** > Prüfung Systemstartdateien
- **Echtzeit-Dateischutz** > Echtzeit-Dateischutz
- **Computer prüfen** > On-Demand-Prüfung

Die Prüfmodul-Einstellungen sind für jedes Modul optimal eingerichtet, und eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Echtzeit-Dateischutz dazu führen, dass das System langsamer arbeitet. Es wird daher empfohlen, die Prüfmodul-Standardeinstellungen für alle Module unverändert beizubehalten. Änderungen sollten nur im Modul „Computer prüfen“ vorgenommen werden.

Objekte

Im Bereich **Objekte** können Sie festlegen, welche Dateien auf Schadcode geprüft werden sollen.

- **Dateien** - Prüfung der gängigen Dateitypen (Programm-, Bild-, Audio-, Video-, Datenbankdateien usw.).
- **Symbolische Links** - (Nur bei On-Demand-Prüfung) Prüfung spezieller Dateitypen, die eine Textfolge enthalten, die vom Betriebssystem ausgewertet und als Pfad zu einer anderen Datei oder einem anderen Verzeichnis genutzt wird.
- **E-Mail-Dateien** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von Dateien, die E-Mail-Nachrichten enthalten.
- **Postfächer** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von Benutzerpostfächern im System. Die unsachgemäße Anwendung dieser Option kann zu Konflikten mit Ihrem E-Mail-Programm führen.
- **Archive** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von komprimierten Archivdateien (.rar, .zip, .arj, .tar usw.).
- **Selbstentpackende Archive** - (nicht verfügbar in Echtzeit-Dateischutz) Prüfung von Dateien in selbstentpackenden Archiven.
- **Laufzeitkomprimierte Dateien** - Laufzeitkomprimierte Dateien werden (anders als Standard-Archivtypen) im Arbeitsspeicher dekomprimiert, zusätzlich zu statisch laufzeitkomprimierten Dateien (UPX, yoda, ASPack, FGS etc.).

Optionen

Im Abschnitt **Optionen** können Sie die Methoden festlegen, die während einer Prüfung des Systems auf Infiltrationen angewendet werden sollen. Die folgenden Optionen stehen zur Verfügung:

- **Heuristik** - Heuristische Methoden verwenden einen Algorithmus, der (bösartige) Aktivitäten von Programmen analysiert. Mit ihrer Hilfe können bis dato unbekannte Schadprogramme oder Viren, die nicht in der Liste bekannter Viren (Signaturdatenbank) aufgeführt waren, erkannt werden.
- **Advanced Heuristik** - Als Advanced Heuristik werden besondere heuristische Verfahren bezeichnet, die für die Erkennung von Würmern und Trojanern optimiert sind, die in höheren Programmiersprachen geschrieben wurden. Die Erkennungsrate des Programms ist dadurch wesentlich gestiegen.
- **Evtl. unerwünschte Anwendungen** - Bei diesen Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken mit sich bringen, aber negative Auswirkungen auf Leistung und Verhalten Ihres Computers haben können. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Verhalten vor der Installation). Dazu zählen vor allem ungewollte Popup-Fenster, die Aktivierung und Ausführung versteckter Prozesse, die erhöhte Inanspruchnahme von Systemressourcen, Änderungen in Suchergebnissen sowie die Kommunikation von Anwendungen mit Remote-Servern.
- **Potenziell unsichere Anwendungen** - In diese Kategorie fallen legitime Programme von seriösen Herstellern, die jedoch von Angreifern ausgenutzt werden können, wenn sie ohne Wissen des Benutzers installiert werden. Da hierzu auch Programme für das Fernsteuern von Computern gehören, ist diese Option standardmäßig deaktiviert.

Säubern

In den Säuberungseinstellungen wird festgelegt, wie das Programm die infizierten Dateien säubert. Es gibt drei Arten der Schadcodeentfernung:

- **Nicht säubern** - Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und Sie werden aufgefordert, eine Aktion auszuwählen.
- **Normales Säubern** - Das Programm versucht, den Schadcode automatisch aus der Datei zu entfernen oder eine infizierte Datei zu löschen. Wenn es nicht möglich ist, die passende Aktion automatisch zu bestimmen, wird der Benutzer aufgefordert, eine Aktion auszuwählen. Diese Auswahl wird dem Benutzer auch dann angezeigt, wenn eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden konnte.
- **Automatisch säubern** - Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht diese Dateien (einschließlich Archiven). Ausnahmen gelten nur für Systemdateien. Wenn es nicht möglich ist, den Schadcode zu entfernen, werden Sie in der angezeigten Warnung aufgefordert, eine Aktion auszuwählen.

Warnung: Im Standardmodus „Normales Säubern“ wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Sind auch nicht infizierte Dateien vorhanden, wird die Archivdatei nicht gelöscht. Im Modus „Automatisch säubern“ wird die gesamte Archivdatei gelöscht, auch wenn sie nicht infizierte Dateien enthält.

Erweiterungen

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt der Datei. In diesem Teil der Prüfmodul-Einstellungen können Sie die Dateitypen festlegen, die nicht geprüft werden sollen.

In der Standardeinstellung werden alle Dateien unabhängig von ihrer Erweiterung geprüft. Jede Erweiterung kann der Liste auszuschließender Dateien hinzugefügt werden. Über die Schaltflächen **Hinzufügen** und **Entfernen** können Sie festlegen, welche Erweiterungen geprüft werden sollen.

Der Ausschluss bestimmter Dateien ist dann sinnvoll, wenn die Prüfung bestimmter Dateitypen die Funktion eines Programms beeinträchtigt. Es wird beispielsweise empfohlen, die Erweiterungen *.log*, *.cfg* und *.tmp* auszuschließen.

Grenzen

Im Bereich **Grenzen** können Sie die Maximalgröße von Elementen und Stufen verschachtelter Archive festlegen, die geprüft werden sollen:

- **Maximale Größe:** Definiert die maximale Größe von zu prüfenden Objekten. Der Virenschutz prüft dann nur die Elemente, deren Größe unter der angegebenen Maximalgröße liegt. Der Standardwert sollte nicht geändert werden; für gewöhnlich besteht dazu auch kein Grund. Diese Option sollte nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, größere Objekte von der Prüfung auszuschließen.
- **Maximale Prüfzeit:** Definiert die maximale Dauer, die für die Prüfung eines Objekts zur Verfügung steht. Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet der Virenschutz die Prüfung eines Elements, sobald diese Zeit abgelaufen ist, und zwar ungeachtet dessen, ob die Prüfung abgeschlossen ist oder nicht.
- **Maximale Verschachtelungstiefe:** Legt die maximale Tiefe der Archivprüfung fest. Der Standardwert 10 sollte nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund. Wenn die Prüfung aufgrund der Anzahl verschachtelter Archive vorzeitig beendet wird, bleibt das Archiv ungeprüft.
- **Maximale Dateigröße:** Über diese Option können Sie die maximale Dateigröße der entpackten Dateien festlegen, die in zu prüfenden Archiven enthalten sind. Wenn die Prüfung aufgrund dieses Grenzwerts vorzeitig beendet wird, bleibt das Archiv ungeprüft.

Weitere

Wenn die Smart-Optimierung aktiviert ist, werden die optimalen Einstellungen verwendet, um die effizienteste Prüfung bei höchster Geschwindigkeit zu gewährleisten. Die verschiedenen Schutzmodule führen eine intelligente Prüfung durch. Dabei verwenden sie unterschiedliche Prüfmethoden für die jeweiligen Dateitypen. Die Smart-Optimierung ist innerhalb des Produkts nicht starr definiert. Unser Entwicklungsteam fügt ständig neue Ergänzungen hinzu, die dann über die regelmäßigen Updates in System Center Endpoint Protection integriert werden. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im Prüfmodul des entsprechenden Moduls für die Prüfung verwendet.

Alternative Datenströme prüfen (Nur bei On-Demand-Prüfung)
Bei den von Dateisystemen verwendeten alternativen Datenströmen (Ressourcen-/Daten-Forks) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Prüftechniken nicht erkannt werden können. Eingedrungene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.

Eingedrungene Schadsoftware wurde erkannt

Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Infektionswege sind Webseiten, freigegebene Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs, Disketten usw.).

Wenn Ihr Computer die Symptome einer Malware-Infektion aufweist (Computer arbeitet langsamer als gewöhnlich, hängt sich oft auf usw.), sollten Sie folgendermaßen vorgehen:

1. Öffnen Sie System Center Endpoint Protection und klicken Sie auf **Computer prüfen**.
2. Klicken Sie auf **Smart-Prüfung** (weitere Informationen siehe Abschnitt Smart-Prüfung 11).
3. Nachdem die Prüfung abgeschlossen ist, überprüfen Sie im Log die Anzahl der geprüften, infizierten und gesäuberten Dateien.

Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, wählen Sie **Benutzerdefinierte Prüfung** und anschließend die Bereiche, die auf Viren geprüft werden sollen.

Das folgende allgemeine Beispiel soll veranschaulichen, wie in System Center Endpoint Protection mit Schadsoftware umgegangen wird. Nehmen wir einmal an, der Echtzeit-Dateischutz verwendet die Standard-Säuberungsstufe und erkennt eingedrungene Schadsoftware. Daraufhin wird der Versuch gestartet, den Schadcode aus der Datei zu entfernen oder die Datei zu löschen. Ist für den Echtzeitschutz keine vordefinierte Aktion angegeben, müssen Sie in einem Warnungsfenster zwischen verschiedenen Optionen wählen. In der Regel stehen die Optionen **Säubern**, **Löschen** und **Keine Aktion** zur Auswahl. Es wird nicht empfohlen, die Option **Keine Aktion** zu wählen, da sonst die infizierten Dateien nicht behandelt werden. Einzige Ausnahme: Sie sind sich sicher, dass die Datei harmlos ist und versehentlich erkannt wurde.

Säubern und löschen – Wählen Sie „Säubern“, wenn eine Datei von einem Virus mit Schadcode infiziert wurde. In einem solchen Fall sollten Sie zuerst versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

Dateien in Archiven löschen – Im Standardmodus der Aktion „Säubern“ wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Archive, die auch nicht infizierte Dateien enthalten, werden also nicht gelöscht. Die Option **Automatisch säubern** sollten Sie hingegen mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und zwar unabhängig vom Status der übrigen Archivdateien.

Aktualisieren des Programms

Für optimalen Schutz muss System Center Endpoint Protection regelmäßig aktualisiert werden. Die Updates für die Signaturdatenbank halten das Programm fortlaufend auf dem neuesten Stand.

Über den Punkt **Update** im Hauptmenü können Sie sich den aktuellen Update-Status anzeigen lassen. Sie sehen hier Datum und Uhrzeit des letzten Updates und können feststellen, ob ein Update erforderlich ist. Um ein Update manuell zu starten, klicken Sie auf **Signaturdatenbank aktualisieren**.

Wenn keinerlei Zwischenfälle beim Update-Download auftreten, wird im Update-Fenster der Hinweis *Update nicht erforderlich - die Signaturdatenbank ist auf dem neuesten Stand* angezeigt.

Die Versionsnummer der Signaturdatenbank wird hier ebenfalls angezeigt. Diese Nummer ist ein aktiver Link zur Website, auf der alle Signaturen aufgeführt werden, die bei dem entsprechenden Update hinzugefügt wurden.

Einstellungen für Updates

Um den Testmodus zu aktivieren (d. h. Updates vor ihrer offiziellen Veröffentlichung herunterzuladen), klicken Sie neben **Erweiterte Einstellungen** auf **Einstellungen** und aktivieren das Kontrollkästchen **Testmodus aktivieren**. Um die Meldungen im Infobereich der Taskleiste zu deaktivieren, die nach jedem erfolgreichen Update angezeigt werden, aktivieren Sie das Kontrollkästchen **Keine Meldung über erfolgreiches Update anzeigen**.

Um alle vorübergehend gespeicherten Update-Daten zu löschen, klicken Sie auf die Schaltfläche **Leeren** neben **Update-Cache leeren**. Dies kann helfen, wenn Probleme beim Update auftreten.

So erstellen Sie Update-Tasks

Mit der Option **Signaturdatenbank aktualisieren** können Updates manuell ausgeführt werden. Klicken Sie dazu im Hauptmenü auf **Update**, und wählen Sie im daraufhin angezeigten Dialogfenster die entsprechende Option aus.

Darüber hinaus können Sie Updates auch als geplante Tasks einrichten. Um einen Task zu konfigurieren, klicken Sie auf **Tools** > **Taskplaner**. Standardmäßig sind in System Center Endpoint Protection folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Anmelden des Benutzers**

Diese Update-Tasks können bei Bedarf bearbeitet werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie im Abschnitt Taskplaner 17.

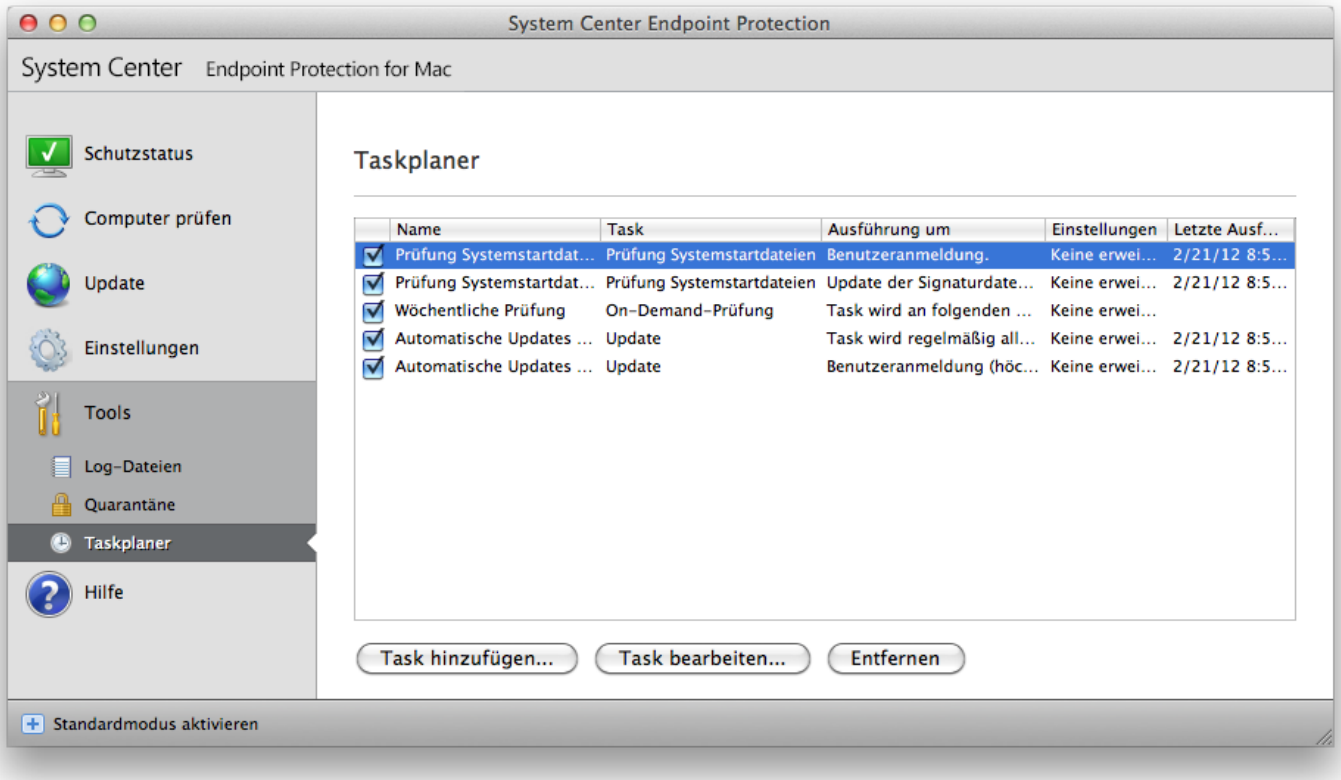
Upgrade auf ein neues Build

Um maximalen Schutz zu gewährleisten, ist es wichtig, immer das neueste Build von System Center Endpoint Protection zu verwenden. Klicken Sie auf **Update** im Hauptmenü links, um zu prüfen, ob eine neue Version verfügbar ist. Ist ein neues Build verfügbar, wird unten im Fenster die Meldung *Eine neue Produktversion ist verfügbar!* angezeigt. Klicken Sie auf **Mehr Informationen**, um ein neues Fenster mit der Versionsnummer des neuen Builds und dem Änderungsprotokoll anzuzeigen.

Klicken Sie auf **Herunterladen**, um das neueste Build herunterzuladen. Klicken Sie auf **Schließen**, um das Fenster zu schließen und das Upgrade später herunterzuladen.

Taskplaner

Der **Taskplaner** steht zur Verfügung, wenn Sie die Einstellungen von System Center Endpoint Protection im erweiterten Modus anzeigen. Um ihn zu öffnen, klicken Sie im Hauptmenü von System Center Endpoint Protection unter **Tools** auf **Taskplaner**. Der Taskplaner umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Prüfprofils.



Standardmäßig werden im Taskplaner die folgenden Tasks angezeigt:

- Automatische Updates in festen Zeitabständen
- Automatische Updates beim Anmelden des Benutzers
- Prüfung Systemstartdateien nach Anmeldung des Benutzers
- Prüfung Systemstartdateien nach Update der Signaturdatenbank
- Log-Wartung (nach Aktivieren der Option **System-Tasks anzeigen** in den Taskplaner-Einstellungen)
- Wöchentliche Prüfung

Um die Konfiguration eines vorhandenen Standardtasks oder eines benutzerdefinierten Tasks zu ändern, halten Sie die Ctrl-Taste gedrückt, klicken auf den Task und dann auf **Bearbeiten**. Alternativ können Sie den Task, den Sie ändern möchten, auswählen und dann auf **Task bearbeiten** klicken.

Verwendung von Tasks

Der Taskplaner verwaltet und startet Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften. Konfiguration und Eigenschaften enthalten Informationen wie Datum und Uhrzeit und bestimmte Profile, die bei Ausführung des Tasks verwendet werden.

Erstellen von Tasks

Zum Erstellen eines Tasks im Taskplaner klicken Sie auf **Task hinzufügen** oder halten die Ctrl-Taste gedrückt, klicken auf das leere Feld und wählen dann im Kontextmenü die Option **Hinzufügen**. Es gibt fünf Arten von Tasks:

- **Anwendung starten**
- **Update**
- **Log-Wartung**
- **On-Demand-Prüfung**
- **Prüfung Systemstartdateien**

Da Update-Tasks zu den meistverwendeten Tasks gehören, wird im Folgenden das Hinzufügen eines neuen Update-Tasks beschrieben.

Wählen Sie in der Liste **Geplanter Task** den Task **Update**. Geben Sie im Feld **Taskname** den Namen des Tasks ein. Wählen Sie in der Liste **Task ausführen** das gewünschte Ausführungsintervall. Die folgenden Optionen stehen zur Verfügung: **Benutzerdefiniert**, **Einmalig**, **Wiederholt**, **Täglich**, **Wöchentlich** und **Bei Ereignis**. Je nach ausgewähltem Intervall werden Ihnen verschiedene Update-Parameter angezeigt.

Bei der Auswahl **Benutzerdefiniert** werden Sie aufgefordert, Datum und Uhrzeit im cron-Format anzugeben (nähere Informationen siehe Abschnitt Erstellen eines benutzerdefinierten Tasks 18).

Im nächsten Schritt legen Sie eine Aktion für den Fall fest, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann. Folgende Optionen stehen zur Verfügung:

- **Nächste Ausführung genau nach Planung**
- **Ausführung zum nächstmöglichen Zeitpunkt**
- **Sofort ausführen, wenn Intervall seit letzter Ausführung überschritten** (das Intervall kann über die Option **Mindestintervall für Task** festgelegt werden)

Im nächsten Schritt wird eine Übersicht der Einstellungen zum geplanten Task angezeigt. Klicken Sie auf **Fertig stellen**.

Der neue geplante Task wird der Liste der aktuellen Tasks hinzugefügt.

Einige Standardtasks sind für die ordnungsgemäße Funktion des Systems unerlässlich. Diese System-Tasks sollten nicht modifiziert werden. Die Anzeige ist standardmäßig ausgeschaltet. Um dies zu ändern und die Anzeige einzuschalten, klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Tools** > **Taskplaner** und aktivieren die Option **System-Tasks anzeigen**.

Erstellen eines benutzerdefinierten Tasks

Datum und Uhrzeit von Tasks des Typs **Benutzerdefiniert** müssen im cron-Langformat mit Jahr angegeben werden (Zeichenfolge aus 6 Feldern, jeweils getrennt durch ein Whitespace-Zeichen):

```
Minute(0-59) Stunde(0-23) Tag(1-31) Monat(1-12) Jahr(1970-2099) Wochentag(0-7)(Sonntag = 0 oder 7)
```

Beispiel:

```
30 6 22 3 2012 4
```

In cron-Ausdrücken werden die folgenden Sonderzeichen unterstützt:

- Sternchen (`*`) - Steht für alle möglichen Werte des betreffenden Felds. Beispiel: Sternchen im dritten Feld (Tag) = jeder Tag im Monat
- Bindestrich (`-`) - Definition von Zeiträumen, z. B. `3-9`
- Komma (`,`) - Trennt mehrere Einträge einer Liste, z. B. `1,3,7,8`
- Schrägstrich (`/`) - Definition von Intervallen in Zeiträumen. Beispiel: `3-28/5` im dritten Feld (Tag) = am 3. des Monats und anschließend alle 5 Tage.

Textbezeichnungen für Tage und Monate („Montag-Sonntag“, „Januar-Dezember“ bzw. die englische Entsprechung) werden nicht unterstützt.

HINWEIS: Werden sowohl Tag als auch Wochentag angegeben, so wird der Befehl nur ausgeführt, wenn beide Bedingungen erfüllt sind.

Quarantäne

Die Hauptaufgabe der Quarantäne ist die sichere Verwahrung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von System Center Endpoint Protection fälschlicherweise erkannt worden sind.

Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, bei der Virenprüfung jedoch nicht erkannt werden.

Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (Hinzugefügt durch Benutzer...) und die Anzahl der Bedrohungen (z. B. bei Archiven, in denen an mehreren Stellen Schadcode erkannt wurde) enthält. Der Quarantäneordner mit den Quarantänedateien (*/Library/Application Support/Microsoft/scep/cache/quarantine*) verbleibt auch nach der Deinstallation von System Center Endpoint Protection auf dem System. Die Quarantänedateien werden sicher verschlüsselt gespeichert und können nach der Reinstallation von System Center Endpoint Protection wiederhergestellt werden.

Quarantäne für Dateien

System Center Endpoint Protection kopiert gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **Quarantäne** klicken. Alternativ kann auch das Kontextmenü zu diesem Zweck verwendet werden: Halten Sie die Ctrl-Taste gedrückt, klicken Sie in das leere Feld, wählen Sie **Quarantäne**, wählen Sie die Datei, die in die Quarantäne verschoben werden soll und klicken Sie auf **Öffnen**.

Wiederherstellen aus Quarantäne

Dateien aus der Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Verwenden Sie dazu die Schaltfläche **Wiederherstellen**. Sie können die Funktion auch über das Kontextmenü aufrufen. Halten Sie dazu die Ctrl-Taste gedrückt, klicken Sie im Fenster **Quarantäne** auf die gewünschte Datei und wählen Sie dann **Wiederherstellen**. Das Kontextmenü enthält außerdem die Option **Wiederherstellen nach**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

Log-Dateien

Die Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen. Das Erstellen von Logs ist unabdingbar für die Systemanalyse, die Erkennung von Problemen oder Risiken sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt aus System Center Endpoint Protection heraus angezeigt werden. Das Archivieren von Logs erfolgt ebenfalls direkt über das Programm.

Log-Dateien können über das Hauptfenster von System Center Endpoint Protection aufgerufen werden, indem Sie auf **Tools** > **Log-Dateien** klicken. Wählen Sie in der Liste **Log** im oberen Bereich des Fensters das gewünschte Log aus. Folgende Logs sind verfügbar:

1. **Erkannte Bedrohungen** - Über diese Option können Sie sämtliche Informationen über Ereignisse bezüglich der Erkennung eingedrungener Schadsoftware anzeigen.
2. **Ereignisse** - Diese Option kann von Systemadministratoren und Benutzern zur Lösung von Problemen verwendet werden. Alle von System Center Endpoint Protection ausgeführten wichtigen Aktionen werden in den Ereignis-Logs aufgezeichnet.
3. **Computer prüfen** - In diesem Fenster werden die Ergebnisse aller durchgeführten Prüfungen angezeigt. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu der entsprechenden On-Demand-Prüfung anzeigen.

In jedem Abschnitt können die angezeigten Informationen direkt in die Zwischenablage kopiert werden. Dazu wählen Sie die gewünschten Einträge aus und klicken auf **Kopieren**.

Log-Wartung

Die Log-Konfiguration für System Center Endpoint Protection können Sie aus dem Hauptprogrammfenster aufrufen. Klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Tools** > **Log-Dateien**. Für Log-Dateien können die folgenden Einstellungen vorgenommen werden:

- **Alte Log-Einträge automatisch löschen** - Log-Einträge, die älter als die angegebene Anzahl Tage sind, werden automatisch gelöscht.
- **Log-Dateien automatisch optimieren** - Die Logs werden beim Erreichen des vordefinierten Fragmentierungsgrads automatisch optimiert.

Alle auf der grafischen Benutzeroberfläche angezeigten relevanten Informationen sowie Meldungen zu Bedrohungen und Ereignissen können in visuell lesbare Textformate wie unformatierten Text oder durch Komma getrennte Werte (*.csv) gespeichert werden. Wenn diese Dateien zur Verarbeitung durch Programme von Drittanbietern verfügbar sein sollen, aktivieren Sie das Kontrollkästchen neben **Protokollierung in Textdateien ermöglichen**.

Zur Festlegung des Zielordners, in dem die Log-Dateien gespeichert werden sollen, klicken Sie neben **Erweiterte Einstellungen** auf **Einstellungen...**.

Je nach den unter **Text-Log-Dateien: Bearbeiten** ausgewählten Optionen, können Sie Log-Dateien mit den folgenden Informationen speichern:

- Bei der Prüfung der Systemstartdateien, vom Echtzeit-Dateischutz oder von der On-Demand Prüfung gefundene Bedrohungen werden in der Datei mit der Bezeichnung threatslog.txt gespeichert.
- Ereignisse wie *Benutzername oder Passwort falsch*, *Update der Signaturdatenbank fehlgeschlagen* usw. werden in die Datei eventslog.txt geschrieben.
- Die Ergebnisse aller abgeschlossenen Prüfungen werden im Format scanlog.NUMMER.txt gespeichert.

Zur Filtereinrichtung für **Standardfilter für Log-Einträge zu Computerprüfung** klicken Sie neben der genannten Option auf **Bearbeiten...** und aktivieren/deaktivieren Sie die jeweiligen Logs wie gewünscht. Weitere Erläuterungen zu den jeweiligen Log-Typen finden Sie in diesem Kapitel 20.

Log-Filter

In den Logs werden Informationen über wichtige Systemereignisse gespeichert. Mit dem Log-Filter können Sie sich gezielt Einträge zu einer bestimmten Ereignisart anzeigen lassen.

Die gängigsten Eintragsarten sind:

- **Kritische Warnungen** - Kritische Systemfehler (z. B. „Virenschutz konnte nicht gestartet werden“)
- **Fehler** - Fehler wie z. B. *„Fehler beim Herunterladen einer Datei“* und kritische Fehler
- **Warnungen** - Warnmeldungen
- **Informationen** - Meldungen wie erfolgreiche Updates, Warnungen usw.
- **Diagnosedaten** - Alle bisher genannten Einträge sowie Informationen, die für die Feineinstellung des Programms erforderlich sind.

Benutzeroberfläche

Über die Konfigurationsoptionen für die Benutzeroberfläche von System Center Endpoint Protection können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Sie erreichen diese Optionen unter **Einstellungen** > **Erweiterte Einstellungen** > **Benutzer** > **Oberfläche**.

In diesem Bereich können Sie über die Option „Erweiterter Modus“ in die erweiterte Anzeige der Einstellungen schalten. Hier werden erweiterte Einstellungen und zusätzliche Steuerelemente für System Center Endpoint Protection angezeigt.

Um das Startbild beim Programmstart zu aktivieren, aktivieren Sie die Option **Startbild anzeigen**.

Unter **Standardmenü verwenden** können Sie mit den Optionen **Im Standardmodus/Im erweiterten Modus** festlegen, in welchen Anzeigemodi das Standardmenü im Hauptprogrammfenster verwendet werden soll.

Um QuickInfos anzuzeigen, aktivieren Sie die Option **QuickInfo anzeigen**. Wenn die Option **Versteckte Dateien anzeigen** aktiviert ist, können Sie im Einstellungsbereich **Zu prüfende Objekte** der Funktion **Computer prüfen** auch versteckte Dateien sehen und diese auswählen.

Warnungen und Hinweise

Im Bereich **Warnungen und Hinweise** können Sie konfigurieren, wie Warnungen und Systemmeldungen in System Center Endpoint Protection behandelt werden.

Wenn Sie die Option **Warnungen anzeigen** deaktivieren, werden keinerlei Warnfenster angezeigt. Dies ist nur in bestimmten Situationen sinnvoll. Für die meisten Benutzer empfiehlt es sich, die Standardeinstellung (aktiviert) beizubehalten.

Wenn Sie die Option **Hinweise auf dem Desktop anzeigen** aktivieren, werden Warnfenster, die keinen Benutzereingriff erfordern, auf dem Desktop angezeigt (standardmäßig oben rechts auf dem Bildschirm). Wie lang solche Hinweise erscheinen, können Sie über den Wert **Hinweise automatisch schließen nach** X **Sekunden** festlegen.

Erweiterte Einstellungen für Warnungen und Hinweise

Nur Hinweise anzeigen, die ein Eingreifen des Benutzers erfordern
Aktivieren/Deaktivieren der Anzeige von Meldungen, die ein Eingreifen des Benutzers erfordern.

Hinweise, die ein Eingreifen des Benutzers erfordern, nur anzeigen, wenn Anwendungen im Vollbildmodus laufen
Diese Option ist praktisch für Präsentationen oder andere Anwendungen, die die gesamte Bildschirmfläche benötigen.

Berechtigungen

Die Einstellungen von System Center Endpoint Protection können im Hinblick auf die Sicherheitsrichtlinien Ihres Unternehmens von großer Wichtigkeit sein. Unbefugte Änderungen können die Stabilität und den Schutz Ihres Systems gefährden. Deshalb können Sie auswählen, welche Benutzer die Programmkonfiguration bearbeiten dürfen.

Zum Festlegen der privilegierten Benutzer klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Benutzer** > **Berechtigungen**.

Maßgeblich für einen wirksamen Schutz Ihres Systems sind die korrekten Einstellungen des Programms. Bei unzulässigen Änderungen können wichtige Daten verloren gehen. Um die Liste der privilegierten Benutzer einzurichten, wählen Sie die gewünschten Benutzer links in der Liste **Benutzer** aus und klicken auf **Hinzufügen**. Um einen Benutzer zu entfernen, wählen Sie ihn in der Liste **Privilegierte Benutzer** rechts aus und klicken auf **Entfernen**.

HINWEIS: Wenn die Liste der privilegierten Benutzer leer ist, können alle Systembenutzer die Programmeinstellungen bearbeiten.

Kontextmenü

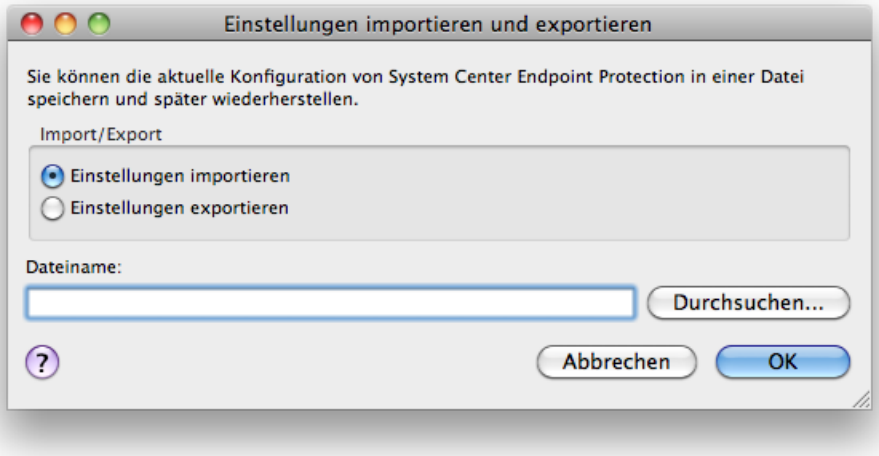
Die Kontextmenü-Integration kann unter **Einstellungen** > **Erweiterte Einstellungen** > **Benutzer** > **Kontextmenü** durch Aktivieren des Kontrollkästchens **In Kontextmenü integrieren** aktiviert werden.

Fortgeschrittene Benutzer

Einstellungen importieren/exportieren

Konfigurationen für System Center Endpoint Protection können im erweiterten Modus unter **Einstellungen** im- bzw. exportiert werden.

Die Optionen Import und Export verwenden Archivdateien zum Speichern der Konfiguration. Diese Funktionen sind nützlich, wenn Sie die aktuelle Konfiguration von System Center Endpoint Protection für eine spätere Verwendung sichern möchten. Die Exportfunktion bietet sich auch für Benutzer an, die ihre bevorzugte Konfiguration von System Center Endpoint Protection auf mehreren Systemen verwenden möchten. Um die gewünschten Einstellungen zu übernehmen, wird die Konfigurationsdatei einfach importiert.



Einstellungen importieren

Die Schritte zum Importieren einer Konfiguration sind sehr einfach. Klicken Sie im Hauptmenü auf **Einstellungen** > **Einstellungen importieren/exportieren**, und wählen Sie die Option **Einstellungen importieren**. Geben Sie den Namen der Konfigurationsdatei ein oder klicken Sie auf **Durchsuchen**, um die Konfigurationsdatei zu suchen, die Sie importieren möchten.

Einstellungen exportieren

Der Export einer Konfiguration verläuft sehr ähnlich. Klicken Sie im Hauptmenü auf **Einstellungen** > **Einstellungen importieren/exportieren**. Wählen Sie die Option **Einstellungen exportieren** und geben Sie den Namen der Konfigurationsdatei ein. Suchen Sie mithilfe des Browsers einen Speicherort auf Ihrem Computer aus, an dem Sie die Konfigurationsdatei speichern möchten.

Einstellungen für Proxyserver

Die Einstellungen für den Proxyserver können unter **Allgemein** > **Proxyserver** konfiguriert werden. So legen Sie die allgemeinen Proxyserver-Einstellungen für alle Funktionen von System Center Endpoint Protection fest. Diese Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet benötigen.

Um die Proxyserver-Einstellungen für diese Ebene festzulegen, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben im Feld **Proxyserver** die entsprechende IP-Adresse bzw. URL ein. Geben Sie dann im Feld „Port“ den Port an, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Wenn der Proxyserver eine Authentifizierung benötigt, aktivieren Sie das Kontrollkästchen **Proxysever erfordert Authentifizierung** und geben einen gültigen **Benutzernamen** sowie das entsprechende **Passwort** ein.

Sperre für Wechselmedien

Wechselmedien (z. B. CDs oder USB-Sticks) können Schadcode enthalten und Ihren Computer gefährden. Um Wechselmedien zu sperren, aktivieren Sie das Kontrollkästchen neben **Sperre für Wechselmedien aktivieren**. Um den Zugriff auf bestimmte Medientypen zu erlauben, deaktivieren Sie das Kontrollkästchen neben den zulässigen Medientypen.

Aktivieren Sie das Kontrollkästchen neben **Sonstige**, wenn diese Einstellungen auf andere Medientypen als CD, DVD, FireWire oder USB angewendet werden sollen. Diese Einstellung gilt vor allem für Peripheriegeräte, die über die Thunderbolt-Schnittstelle an den Computer angeschlossen sind.

Glossar

Schadsoftwaretypen

Bei Schadsoftware handelt es sich um bösartige Software, die versucht, in einen Computer einzudringen und/oder auf einem Computer Schaden anzurichten.

Viren

Bei einem Computervirus handelt es sich um eingedrungene Schadsoftware, die Dateien auf Ihrem Computer beschädigt. Ihren Namen haben sie nicht umsonst mit den Viren aus der Biologie gemein. Schließlich verwenden sie ähnliche Techniken, um sich von einem zum anderen Computer auszubreiten.

Computerviren greifen hauptsächlich ausführbare Dateien, Skripte und Dokumente an. Um sich zu vermehren, hängt sich ein Virus mit seinem „Körper“ an das Ende einer Zieldatei. Und so funktioniert ein Computervirus: Durch Ausführung der infizierten Datei wird der Virus aktiviert (noch bevor die eigentliche Anwendung gestartet wird) und führt seine vordefinierte Aufgabe aus. Erst dann wird die eigentliche Anwendung gestartet. Ein Virus kann einen Computer also nur dann infizieren, wenn der Benutzer (versehentlich oder absichtlich) das bösartige Programm ausführt oder öffnet.

Computerviren unterscheiden sich nach Art und Schweregrad der durch sie verursachten Schäden. Einige von ihnen sind aufgrund ihrer Fähigkeit, Dateien von der Festplatte gezielt zu löschen, äußerst gefährlich. Andererseits gibt es aber auch Viren, die keinen Schaden verursachen. Ihr einziger Zweck besteht darin, den Benutzer zu verärgern und die technischen Fähigkeiten ihrer Urheber unter Beweis zu stellen.

Viren werden (im Vergleich zu Trojanern oder Spyware) immer seltener, da sie keinen kommerziellen Nutzen für ihre Urheber haben. Außerdem wird der Begriff „Virus“ oft fälschlicherweise für alle Arten von Schadsoftware verwendet. Heute setzt sich mehr und mehr der neue, treffendere Ausdruck „Malware“ (engl. bösartige Software) durch.

Wenn Ihr Computer mit einem Virus infiziert wurde, ist es notwendig, den Originalzustand der infizierten Dateien wiederherzustellen - das heißt, den Schadcode mithilfe eines Virenschutzprogrammes daraus zu entfernen.

Beispiele für Viren sind: *OneHalf*, *Tenga* und *Yankee Doodle*.

Würmer

Bei einem Computerwurm handelt es sich um ein Programm, das Schadcode enthält, der Hostcomputer angreift und sich über Netzwerke verbreitet. Der grundlegende Unterschied zwischen Viren und Würmern besteht darin, dass Würmer in der Lage sind, sich selbstständig zu vermehren und zu verbreiten. Sie sind unabhängig von Hostdateien (oder Bootsektoren). Würmer verbreiten sich über die E-Mail-Adressen in Ihrer Kontaktliste oder nutzen Sicherheitslücken von Anwendungen in Netzwerken.

Daher sind Würmer wesentlich funktionsfähiger als Computerviren. Aufgrund der enormen Ausdehnung des Internets können sich Würmer innerhalb weniger Stunden über den gesamten Globus verbreiten - manchmal sogar schon in wenigen Minuten. Da sich Würmer unabhängig und rasant vermehren können, sind sie gefährlicher als andere Arten von Schadsoftware.

Ein innerhalb eines Systems aktivierter Wurm kann eine Reihe von Unannehmlichkeiten verursachen: Er kann Dateien löschen, die Systemleistung beeinträchtigen oder Programme deaktivieren. Aufgrund ihrer Beschaffenheit können Würmer als Transportmedium für andere Arten von Schadcode fungieren.

Wurde Ihr Computer mit einem Wurm infiziert, empfiehlt es sich, alle betroffenen Dateien zu löschen, da sie höchstwahrscheinlich Schadcode enthalten.

Zu den bekanntesten Würmern zählen: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* und *Netsky*.

Trojaner

Trojaner galten früher als eine Klasse von Schadprogrammen, die sich als nützliche Anwendungen tarnen, um den Benutzer zur Ausführung zu verleiten. Heute müssen sich Trojaner nicht mehr tarnen. Ihr einzige Absicht besteht darin, sich möglichst leicht Zugang zu einem System zu verschaffen, um dort den gewünschten Schaden anzurichten. Der Ausdruck „Trojaner“ ist zu einem sehr allgemeinen Begriff geworden, der jegliche Form von Schadsoftware beschreibt, die nicht einer bestimmten Kategorie zugeordnet werden kann.

Aus diesem Grund wird die Kategorie „Trojaner“ oft in mehrere Gruppen unterteilt.

- Downloader - Ein bösartiges Programm zum Herunterladen von Schadsoftware aus dem Internet.
- Dropper - Trojaner, der auf angegriffenen Computern weitere Schadsoftware absetzt („droppt“).
- Backdoor - Anwendung, die Angreifern Zugriff auf ein System verschafft, um es zu kontrollieren.
- Keylogger - Programm, das die Tastenanschläge eines Benutzers aufzeichnet und die Informationen an Angreifer sendet.

- Dialer - Dialer sind Programme, die Verbindungen zu teuren Einwahlnummern herstellen. Dass eine neue Verbindung erstellt wurde, ist für den Benutzer nahezu unmöglich festzustellen. Dialer sind nur eine Gefahr für Benutzer von Einwahlmodems. Diese werden allerdings nur noch selten eingesetzt.
- Trojaner treten häufig in Form von ausführbaren Dateien auf. Wenn auf Ihrem Computer eine Datei als Trojaner identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

Zu den bekanntesten Trojanern zählen: *NetBus*, *Trojandownloader.Small.ZL*, *Slapper*.

Adware

Adware ist eine Abkürzung für durch Werbung (engl. Advertising) unterstützte Software. In diese Kategorie fallen Programme, in denen Werbung angezeigt wird. Adware-Anwendungen öffnen häufig in Internetbrowsern neue Popup-Fenster mit Werbung oder ändern die Startseite des Browsers. Adware gehört oftmals zu Freeware-Programmen, damit die Freeware-Entwickler auf diesem Weg die Entwicklungskosten ihrer (gewöhnlich nützlichen) Anwendungen decken können.

Adware selbst ist nicht gefährlich. Allerdings werden die Benutzer mit Werbung belästigt. Bedenklich ist aber, dass Adware auch dazu dienen kann, Daten zu sammeln (wie es bei Spyware der Fall ist).

Wenn Sie sich dafür entscheiden, ein Freeware-Produkt zu verwenden, sollten Sie bei der Installation besonders aufmerksam sein. Die meisten Installationsprogramme benachrichtigen Sie über die Installation eines zusätzlichen Adware-Programms. In vielen Fällen ist es möglich, diesen Teil der Installation abzubrechen und das Programm ohne Adware zu installieren.

In einigen Fällen lassen sich Programme jedoch nicht ohne die Adware installieren, oder nur mit eingeschränktem Funktionsumfang. Das bedeutet, dass Adware häufig ganz „legal“ auf das System zugreift, da sich die Benutzer damit einverstanden erklärt haben. In diesem Fall gilt: Vorsicht ist besser als Nachsicht. Wenn auf Ihrem Computer eine Datei als Adware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

Spyware

Der Begriff „Spyware“ fasst alle Anwendungen zusammen, die vertrauliche Informationen ohne das Einverständnis/Wissen des Benutzers versenden. Diese Programme verwenden Überwachungsfunktionen, um verschiedene statistische Daten zu versenden, z. B. eine Liste der besuchten Websites, E-Mail-Adressen aus dem Adressbuch des Benutzers oder eine Auflistung von Tastatureingaben.

Die Entwickler von Spyware geben vor, auf diesem Weg die Interessen und Bedürfnisse der Benutzer erkunden zu wollen. Ziel sei es, gezieltere Werbeangebote zu entwickeln. Das Problem dabei ist, dass nicht wirklich zwischen nützlichen und bösartigen Anwendungen unterschieden werden kann. Niemand kann sicher sein, dass die gesammelten Informationen nicht missbraucht werden. Die von Spyware gesammelten Daten enthalten möglicherweise Sicherheitscodes, PINs, Kontonummern usw. Spyware wird oft im Paket mit kostenlosen Versionen eines Programms angeboten, um so Einkünfte zu erzielen oder einen Anreiz für den Erwerb der kommerziellen Version zu schaffen. Oft werden die Benutzer bei der Programminstallation darüber informiert, dass Spyware eingesetzt wird, um sie damit zu einem Upgrade auf die kommerzielle, Spyware-freie Version zu bewegen.

Beispiele für bekannte Freeware-Produkte, die zusammen mit Spyware ausgeliefert werden, sind Client-Anwendungen für P2P-Netzwerke. Programme wie Spyfalcon oder Spy Sheriff gehören zur einer besonderen Kategorie von Spyware: Getarnt als Spyware-Schutzprogramme üben sie selbst Spyware-Funktionen aus.

Wenn auf Ihrem Computer eine Datei als Spyware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

Potenziell unsichere Anwendungen

Es gibt zahlreiche seriöse Programme, die die Verwaltung miteinander vernetzter Computer vereinfachen sollen. Wenn sie aber in die falschen Hände geraten, kann mit ihnen Schaden angerichtet werden. Mit System Center Endpoint Protection können solche Bedrohungen erkannt werden.

Zur Kategorie der „potenziell unsicheren Anwendungen“ zählen Programme, die zwar erwünscht sind, jedoch potenziell gefährliche Funktionen bereitstellen. Dazu zählen beispielsweise Programme für das Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Keylogger (Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden).

Sollten Sie feststellen, dass auf Ihrem Computer eine potenziell unsichere Anwendung vorhanden ist (die Sie nicht selbst installiert haben), wenden Sie sich an Ihren Netzwerkadministrator oder entfernen die Anwendung.

Evtl. unerwünschte Anwendungen

Eventuell unerwünschte Anwendungen sind nicht unbedingt und absichtlich schädlich, sie können aber die Leistung Ihres Computers negativ beeinflussen. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Verhalten vor der Installation). Die gravierendsten Veränderungen sind:

- neue Fenster werden angezeigt,
- versteckte Prozesse werden gestartet,
- Prozessor und Speicher werden stärker belastet als zuvor,
- Suchergebnisse ändern sich,
- die Anwendung kommuniziert mit Servern im Internet.