Faronics™
Simplifying Computer Management

FARONICS
ANTI-VIRUS™

ADVANCED
System Integrity

Benutzerhandbuch

www.faronics.com

Letzte Änderung: Januar 2023

Inhalt

Vorwort

Dieses Benutzerhandbuch erläutert die Installation und Verwendung von Faronics Anti-Virus.

Themen

Wichtige Informationen

Dieser Abschnitt enthält wichtige Informationen über Ihr Faronics-Produkt.

Über Faronics

Faronics liefert marktführende Lösungen, die dabei helfen, komplexe IT-Umgebungen zu verwalten, zu vereinfachen und abzusichern. Unsere Produkte stellen eine hundertprozentige Verfügbarkeit von Maschinen sicher und haben bereits einen dramatischen Einfluss auf das tägliche Leben Tausender von Fachleuten im Informationstechnologiebereich gehabt. Bildungsinstitutionen, Einrichtungen des Gesundheitswesens, Bibliotheken, Regierungsorganisationen und Firmen profitieren von den marktzentrisch fokussierten Technologieinnovationen von Faronics.

Produktdokumentation

Die folgenden Dokumente bilden das Dokumentationspaket für Faronics Anti-Virus:

- Faronics Anti-Virus Benutzerhandbuch – Dieses Dokument hilft Ihnen bei der Verwendung des Produkts.
- Faronics Anti-Virus Versionshinweise – Dieses Dokument führt die neuen Funktionen sowie bekannte und gelöste Probleme auf.

Technischer Support

Alle Anstrengungen wurden unternommen, um diese Software benutzerfreundlich und problemfrei zu gestalten. Sollten dennoch Probleme auftreten, setzen Sie sich bitte mit unserem technischen Kundendienst in Verbindung.

E-Mail: support@faronics.com

Tel: 1-800-943-6422 oder 1-604-637-3333

Geschäftsstunden: Montag bis Freitag 07:00 Uhr bis 17:00 Uhr (Pazifische Zeit)

Kontaktinformationen

- Internet: www.faronics.com
- E-Mail: sales@faronics.com
- Tel: 1-800-943-6422 oder 1-604-637-3333
- Fax: 1-800-943-6488 oder 1-604-637-8188
- Geschäftsstunden: Montag bis Freitag 07:00 Uhr bis 17:00 Uhr (Pazifische Zeit)
- Adresse:

  Faronics Technologies USA Inc.
  5506 Sunol Blvd, Suite 202
  Pleasanton, CA, 94566
  USA

  Faronics Corporation (Kanada und International)
  609 Granville Street, Suite 1400
  Vancouver, BC V7Y 1G5
  Kanada

  Faronics Corporation (Europa)
  8 The Courtyard, Eastern Road,
  Bracknell, Berkshire,
  RG12 2XB, United Kingdom

Begriffsdefinitionen

Begriff	Definition
Aktiver Schutz	Der aktive Schutz ist eine Echtzeitmethode für die Erkennung von Malware. Der aktive Schutz läuft still im Hintergrund, während Sie arbeiten oder im Internet surfen und überwacht kontinuierlich die Dateien, die ausgeführt werden, ohne ihr System spürbar zu verlangsamen.
Adware	Adware, gelegentlich auch als Werbesoftware bezeichnet, ist häufig kontext- oder verhaltensbasiert und verfolgt Browsing-Gewohnheiten, um Werbebotschaften Dritter anzuzeigen, die für den Benutzer relevant sein sollen. Die Werbeanzeigen können unterschiedliche Formate haben, beispielsweise Pop-Ups, Pop-Unders, Banner oder Links, die in Webseiten oder Teile der Windows-Benutzeroberfläche eingebunden sind. Adware-Werbung kann auch aus Textanzeigen bestehen, die innerhalb der Anwendung selbst oder in Seitenleisten, Suchleisten oder Suchergebnissen angezeigt werden.
Firewall	Eine Firewall bietet bidirektionalen Schutz und schützt Sie vor sowohl eingehendem als auch abgehendem Datenverkehr. Eine Firewall schützt Ihr Netzwerk vor unbefugten Eindringlingen.
Quarantäne	Der Quarantänebereich ist ein sicherer Bereich auf Ihrem Computer, den Faronics Anti-Virus verwendet, um Malware oder infizierte Dateien, die nicht desinfiziert werden konnten, zu speichern. Wenn sich Ihr Computer bzw. eine Datei auf Ihrem Computer nicht normal verhält, nachdem ein Element hier hinterlegt wurde, haben Sie die Möglichkeit, die Details eines Risikos zu überprüfen, es näher zu untersuchen und aus dem Quarantänebereich zu entfernen. Es wird dann an seiner ursprünglichen Position auf dem Computer wiederhergestellt. Sie können die riskanten Elemente auch dauerhaft aus der Quarantäne entfernen.
Rogue-Sicherheitsprogramm	Ein Rogue-Sicherheitsprogramm ist Software mit unbekannter oder fraglicher Herkunft oder zweifelhaftem Wert. Ein Rogue-Sicherheitsprogramm meldet sich normalerweise auf Websites oder in Spam-E-Mails als aufdringliche Warnmeldung zu Worte und behauptet, Ihr Computer sei infiziert. Es bietet dann an, diesen zu durchsuchen und zu reinigen. Diesen Programmen sollte niemals vertraut werden. Seriöse Antivirus- oder Antispyware-Anbieter verwenden diese Methode niemals, um Sie zu *benachrichtigen*. Ein Rogue-Sicherheitsprogramm kann wie ein normales Antivirus- oder Antimalware-Programm erscheinen, versucht dann aber, Sie zu überlisten oder zu belästigen, bis Sie das Programm kaufen. Während manche Rogue-Sicherheitsprogramme lediglich *Quacksalberprodukte* sind, die keinen Nutzen bringen, können andere tatsächlich schädlich sein, indem sie Malware installieren oder gar die von Ihnen eingegebenen Kreditkarteninformationen stehlen, was potenziell zu Identitätsdiebstahl führen kann. Des Weiteren müssen Sie gut aufpassen, wenn Sie diese Warnmeldungen schließen oder löschen, selbst wenn Sie wissen, dass sie gefälscht sind.

Begriff	Definition
Rootkits	Ein Rootkit ist ein Programm, das Dateien und Daten versteckt, um eine Erkennung zu vermeiden. Gleichzeitig erlaubt es einem Angreifer, den Rechner ohne Wissen des Benutzers zu übernehmen. Rootkits werden normalerweise von Malware wie Viren, Spyware, Trojanern und Backdoors verwendet, um sich vor dem Benutzer und Malware-Erkennungssoftware wie Antivirus- und Antispyware-Anwendungen zu verstecken. Rootkits werden außerdem von bestimmten Adware-Anwendungen und DRM-Programmen (digitales Rechtemanagement) verwendet, um die Entfernung der unerwünschten Software durch Anwender zu verhindern.
Spyware	Spyware ist Software, die Informationen an Dritte überträgt, ohne. Sie davon in Kenntnis zu setzen. Sie wird auch als Trackware, Hijackware, Scumware, Snoopware und Thiefware bezeichnet. Einige Datenschützer bezeichnen sogar legitime Software für Zugangsberechtigungen, Filterung, Internet-Überwachung, Passwortwiederherstellung, Sicherheit und Überwachung als *Spyware*, da diese Programme verwendet werden können, ohne Sie zu benachrichtigen.
Trojaner	Ein Trojaner wird unter falscher oder betrügerischer Vortäuschung installiert, häufig ohne das Wissen und die Zustimmung durch den Benutzer. In anderen Worten: was für einen Benutzer völlig harmlos aussehen mag, ist in Wahrheit gefährlich, da es schädlichen Code enthält. Die meisten Trojaner legen eine Form schädlicher, feindlicher oder gefährlicher Funktionalität oder Verhaltensweise an den Tag.
Virus	Ein Computervirus ist schädlicher Code, der die Fähigkeit hat, sich zu replizieren und in andere Programme und Dateien einzudringen, um sich innerhalb des infizierten Rechners auszubreiten. Viren breiten sich normalerweise aus, wenn Benutzer infizierte Dateien ausführen oder infizierte Medien laden, insbesondere Wechseldatenträger wie CD-ROMs oder USB-Sticks. Viren können sich außerdem per E-Mail über infizierte Anhänge und Dateien ausbreiten. Die meisten Viren enthalten sogenannte *Payloads*, die das gesamte Spektrum von nervig über störend bis hin zu schädlich und gefährlich abdecken. Viren können ein System beschädigen, zum Verlust wertvoller Daten führen oder zur Installation weiterer Malware eingesetzt werden.
Wurm	Ein Wurm ist ein schädliches Programm, das sich ohne Eingriffe des Benutzers ausbreitet. Würmer sind Viren insofern ähnlich, als dass sie sich selbst replizieren. Im Gegensatz zu Viren breiten sich Würmer jedoch aus, ohne sich an andere Programme oder Dateien zu hängen bzw. diese zu infizieren. Ein Wurm kann sich über Sicherheitslücken auf angreifbaren Rechnern, die an ein Computernetzwerk angeschlossen sind, über gesamte Netzwerke ausbreiten. Würmer können sich auch über E-Mail ausbreiten, indem sie Kopien ihrer selbst an alle Kontakte im Adressbuch eines Benutzers schicken. Ein Wurm kann erhebliche Systemressourcen beanspruchen und dazu führen, dass ein Rechner spürbar langsam und unzuverlässig wird. Manche Würmer können verwendet werden, um infizierte Rechner zu kompromittieren und zusätzliche schädliche Software herunterzuladen.

Einführung

Faronics Anti-Virus bietet Schutz vor Sicherheitsbedrohungen, ohne Computer aufgrund langsamer Suchzeiten und erheblichem Platzbedarf zu verlangsamen. Faronics Anti-Virus, das mit Technologie der nächsten Generation erstellt wurde, bietet Ihnen eine leistungsstarke integrierte Antiviren-, Anti-Rootkit- und Anti-Spyware-Software, die Sie gegen aktuelle komplexe Malware-Bedrohungen schützt. Gleichzeitig lässt sie sich reibungslos mit Faronics Deep Freeze und Faronics Anti-Executable integrieren, um so eine vollständige mehrstufige Sicherheitslösung zu bilden.

Themen

Faronics Anti-Virus – Überblick

Faronics Anti-Virus schützt Arbeitsplätze vor den folgenden Bedrohungen:

- Adware
- Rogue-Sicherheitsprogramme
- Rootkits
- Spyware
- Trojaner
- Würmer

Faronics Anti-Virus kann über Faronics Core auf mehreren Arbeitsplätzen installiert werden. Weitere Informationen zu Faronics Core finden Sie im Faronics Core-Benutzerhandbuch. Das neueste Benutzerhandbuch ist unter http://www.faronics.com/html/library.asp erhältlich.

Bei Installation gemeinsam mit Deep Freeze können die Antivirus-Definitionen auf Arbeitsplätzen ohne einen *Reboot Thawed* oder einen Neustart im *Maintenance Mode* aktualisiert oder verwaltet werden. Weitere Informationen hierzu finden Sie im Deep Freeze Enterprise-Benutzerhandbuch. Das neueste Benutzerhandbuch ist unter http://www.faronics.com/html/library.asp erhältlich.

Systemanforderungen

Anforderungen für Faronics Anti-Virus

Das Faronics Anti-Virus-Loadin erfordert:

- Faronics Core 3,7 oder höher

Der Faronics Anti-Virus-Client auf dem Arbeitsplatz erfordert eines der folgenden Betriebssysteme:

- Windows XP SP3 (32-Bit) oder Windows XP SP2 (64-Bit)
- Windows 7 (32-Bit oder 64-Bit)
- Windows 8.1 (32-Bit oder 64-Bit)
- Windows 10 bis Version 22H2 (32-Bit oder 64-Bit)
- Windows 11 bis Version 22H2
- Windows Server 2008 R2 (64-Bit)
- Windows Server 2012 (64-Bit)
- Windows Server 2016 (64-Bit)
- Windows Server 2019 (64-Bit
- Windows Server 2022 (64-Bit

Es wird nachdrücklich empfohlen, sämtliche Komponenten über ein Windows-Administratorkonto zu installieren.

Anforderungen für Faronics Core

Informationen über die Systemanforderungen für Faronics Core finden Sie im Faronics Core-Benutzerhandbuch. Das neueste Benutzerhandbuch ist unter http://www.faronics.com/html/library.asp erhältlich.

Anforderungen für Deep Freeze

Informationen über die Systemanforderungen für Deep Freeze finden Sie im Deep Freeze Enterprise-Benutzerhandbuch. Das neueste Benutzerhandbuch ist unter http://www.faronics.com/html/library.asp erhältlich.

Um Faronics Anti-Virus auf Arbeitsplätzen auszuführen, die über Deep Freeze verwaltet werden, ist Deep Freeze Enterprise 7.0 oder höher erforderlich.

Faronics Anti-Virus – Lizenzierung

Die Faronics Anti-Virus-Lizenz kann über die Faronics Core Console angewandt werden. Führen Sie die folgenden Schritte aus, um die Faronics Anti-Virus-Lizenz anzuwenden:

1. Starten Sie die Faronics Core Console.
2. Klicken Sie mit der rechten Maustaste auf den *Core Server*, und wählen Sie *Eigenschaften* aus.
3. Klicken Sie auf die Registerkarte *Anti-Virus*. Die Registerkarte „Anti-Virus" zeigt die *Version*, den *Lizenzschlüssel* (wenn es sich um eine lizenzierte Version handelt) und das *Ablaufdatum der Lizenz* an.
4. Klicken Sie auf *Bearbeiten*, und geben Sie den *Lizenzschlüssel* in das Feld *Lizenzschlüssel* ein.
5. Klicken Sie auf *Anwenden*. Klicken Sie auf *OK*.

Die Lizenzierung von Faronics Anti-Virus funktioniert folgendermaßen:

- Der Core Server (eine Komponente von Faronics Core) übermittelt den Lizenzschlüssel automatisch an die Arbeitsplätze, auf denen der Faronics Anti-Virus Client installiert ist (wenn die Computer offline sind, wird der Lizenzschlüssel angewandt, sobald diese wieder online sind).

Wenn der Lizenzschlüssel für Faronics Anti-Virus bei der Installation des Loadins eingegeben wurde, braucht er nicht erneut über die Registerkarte Eigenschaften eingegeben zu werden.

Die Virusdefinitionen können nicht heruntergeladen werden, wenn der Lizenzschlüssel von Faronics Anti-Virus abgelaufen ist.

Faronics Anti-Virus installieren

Dieses Kapitel beschreibt die Installation von Faronics Anti-Virus.

Themen

Installationsübersicht

Faronics Anti-Virus besteht aus zwei Komponenten:

- Faronics Anti-Virus-Loadin – wird auf einem Computer installiert, auf dem Faronics Core läuft.
- Faronics Anti-Virus-Client – wird auf Arbeitsplätzen installiert, die über das Faronics Anti-Virus-Loadin verwaltet werden sollen.

Für die Installation und Konfiguration von Faronics Anti-Virus sind die folgenden Schritte erforderlich:

- Installation von Faronics Core und Generierung/Implementierung des Installationsprogramms für den Core Agent
- Installation des Faronics Anti-Virus-Loadins
- Implementierung des Faronics Anti-Virus-Client

Faronics Core installieren

Weitere Informationen über die Installation von Faronics Core und die Generierung und Implementierung des Core Agent finden Sie im Benutzerhandbuch zu Faronics Core. Das neueste Benutzerhandbuch ist unter http://www.faronics.com/html/library.asp erhältlich.

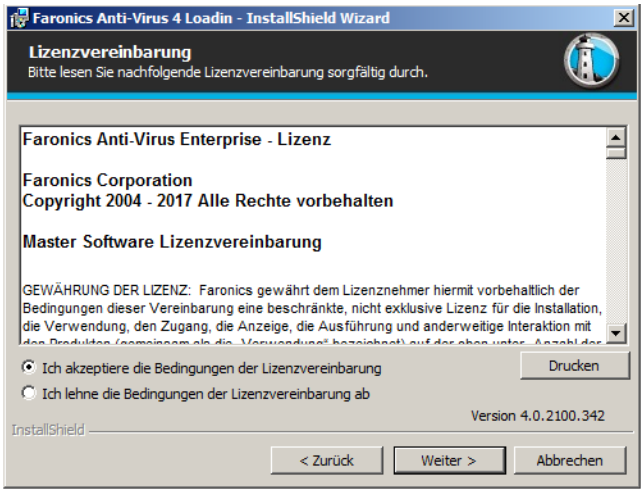
Das Faronics Anti-Virus-Loadin installieren

Führen Sie die folgenden Schritte aus, um das Faronics Anti-Virus-Loadin zu installieren:

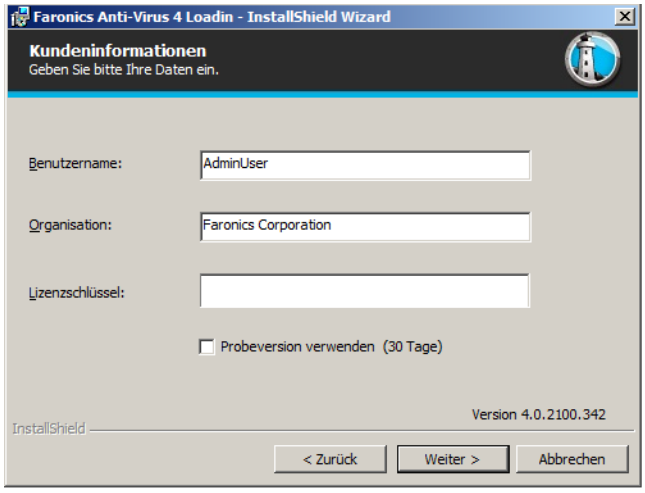
Das Anti-Virus -Loadin kann nicht auf einem Computer installiert werden, auf dem die Faronics Core Console (oder der Faronics Core Server) nicht installiert ist.

1. Klicken Sie doppelt auf *Anti-VirusLoadinInstaller.exe*. Klicken Sie auf *Weiter*.

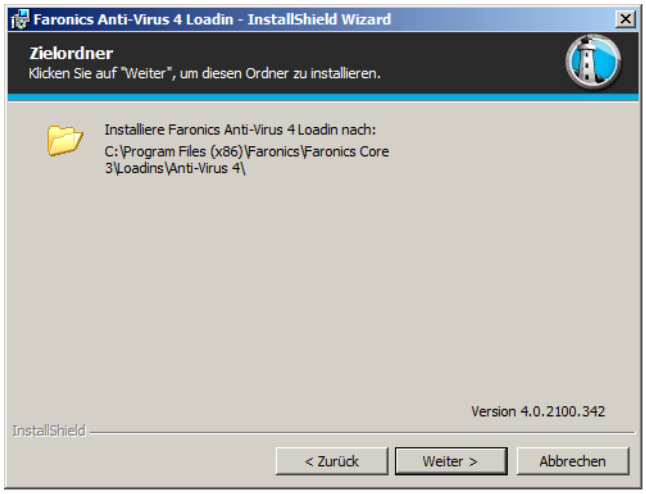
2. Lesen und akzeptieren Sie die Lizenzvereinbarung. Klicken Sie auf *Weiter*.



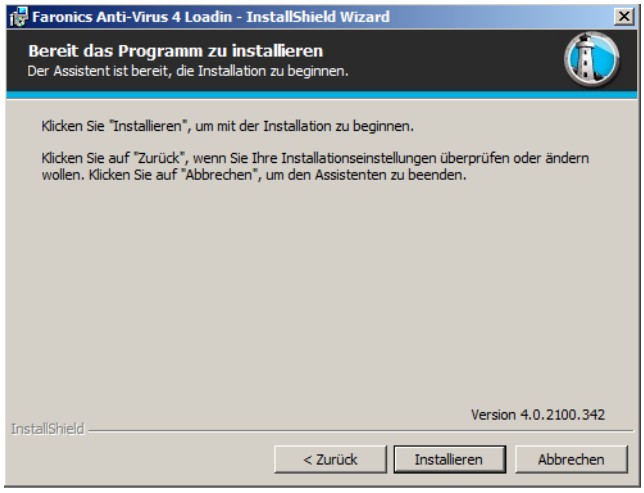
3. Geben Sie den *Benutzernamen*, die *Organisation* und den *Lizenzschlüssel* ein. Alternativ können Sie auch das Markierungsfeld *Probeversion verwenden* auswählen. Faronics Anti-Virus läuft nach einer Probezeit von 30 Tagen ab. Klicken Sie auf *Weiter*.



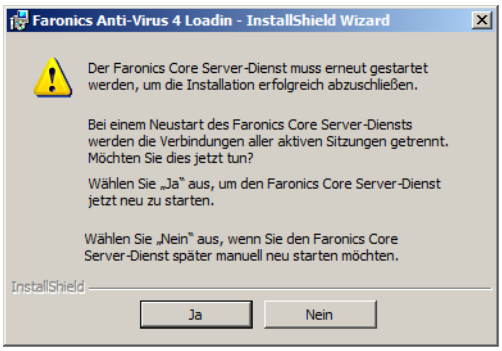
4. Die Standardposition ist *C:\Programme\Faronics\Faronics Core 3\Loadins\Anti-Virus*.



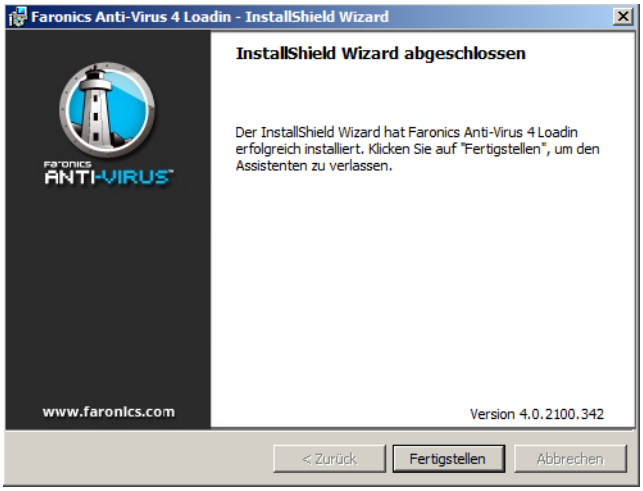
5. Klicken Sie auf *Installieren*, um das Faronics Anti-Virus-Loadin zu installieren.



6. Die folgende Meldung wird angezeigt. Klicken Sie auf *Ja*, um den Faronics Core Server-Dienst neu zu starten. Klicken Sie auf *Nein*, um den Faronics Core Server-Dienst später manuell zu starten.



7. Klicken Sie auf *Fertigstellen*, um die Installation abzuschließen.



Faronics Anti-Virus über Faronics Core auf einem Arbeitsplatz installieren oder aktualisieren

Der Core Agent, der Teil von Faronics Core ist, muss auf jedem Arbeitsplatz installiert werden, der über Faronics Anti-Virus verwaltet werden soll. Weitere Informationen über die Installation des Core Agent finden Sie im Faronics Core-Benutzerhandbuch. Das neueste Benutzerhandbuch ist unter http://www.faronics.com/html/library.asp erhältlich.

Nachdem der Core Agent installiert wurde, werden die Arbeitsplätze im Netzwerk erkannt und in Core Console angezeigt.

Wählen Sie für eine Installation oder Aktualisierung von Faronics Anti-Virus einen einzelnen Arbeitsplatz oder mehrere Arbeitsplätze aus:

1. Klicken Sie im rechten Teilfenster auf "Arbeitsplätze konfigurieren", und wählen Sie *Erweitert* > *Faronics Anti-Virus Client installieren/aktualisieren* aus.
2. Wählen Sie die folgenden Optionen aus, wenn bereits ein anderes Antivirus-Programm installiert ist:
   > Nicht kompatible Antivirus-Produkte vor der Installation des Faronics Anti-Virus Enterprise-Arbeitsplatzes entfernen.
   > Faronics Anti-Virus auch dann installieren, wenn ein anderes Antivirus-Produkt vorhanden ist oder nicht entfernt werden konnte.

Der Arbeitsplatz wird nach einer erfolgreichen Installation oder Aktualisierung neu gestartet.

Wenn mehr als ein Loadin installiert ist, können Sie auf das Kontextmenü für Faronics Anti-Virus zugreifen, indem Sie mit der rechten Maustaste auf einen Arbeitsplatz klicken und dann zunächst *Anti-Virus* und anschließend die gewünschte Aktion auswählen.

Faronics Anti-Virus manuell auf einem Arbeitsplatz installieren

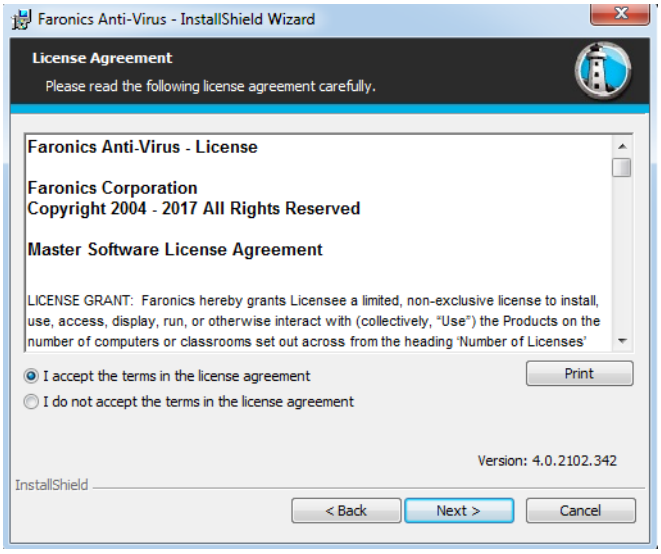
Kopieren Sie vor der Installation des Faronics Anti-Virus-Client auf einem Arbeitsplatz die entsprechende *.msi*-Datei vom Pfad *C:\Programme\Faronics\Faronics Core 3\Loadins\Anti-Virus\Wks Installers* auf dem Computer, auf dem das Anti-Virus-Loadin installiert ist, auf einen Arbeitsplatz bzw. auf mehrere Arbeitsplätze.

Wiederholen Sie den Prozess für jeden Arbeitsplatz, der über Faronics Anti-Virus geschützt werden soll.

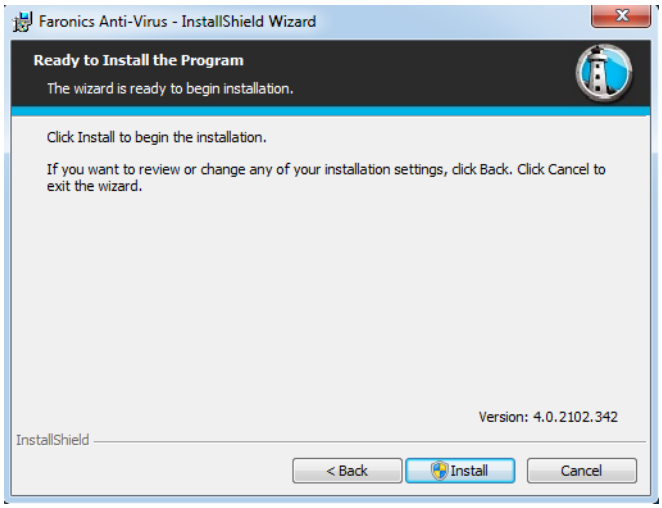
Führen Sie die folgenden Schritte aus, um Faronics Anti-Virus auf dem Arbeitsplatz zu installieren:

1. Klicken Sie doppelt auf *AntiVirus_Ent_32-bit.msi* für ein 32-Bit-Betriebssystem, bzw. auf *AntiVirus_Ent_64-bit.msi* für ein 64-Bit-Betriebssystem. Klicken Sie auf *Weiter*.

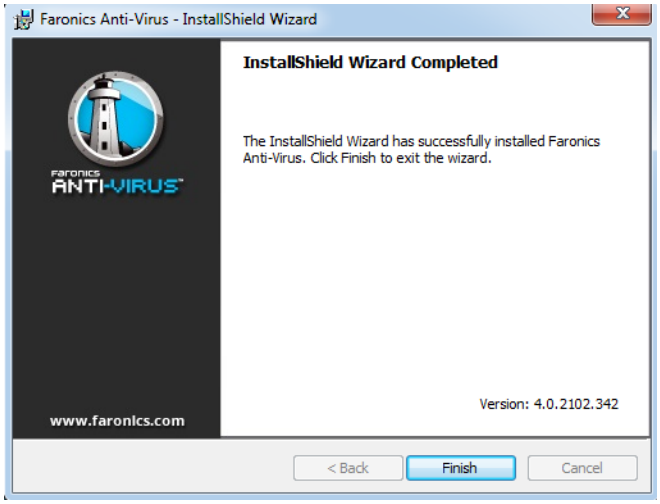
2. Lesen und akzeptieren Sie die Lizenzvereinbarung. Klicken Sie auf *Weiter*.



3. Klicken Sie auf *Installieren*, um Faronics Anti-Virus zu installieren.



4. Klicken Sie auf *Fertigstellen*, um die Installation abzuschließen.



Nach der Installation des Anti-Virus-Client auf dem Arbeitsplatz wird ein sofortiger Neustart empfohlen.

Faronics Anti-Virus verwenden

Dieses Kapitel beschreibt die Verwendung von Faronics Anti-Virus.

Themen

Faronics Anti-Virus – Überblick

Faronics Anti-Virus kann folgendermaßen verwendet werden:

Faronics Anti-Virus über die Faronics Core Console verwalten:

- Das Faronics Anti-Virus-Loadin installieren (weitere Informationen hierzu finden Sie unter Das Faronics Anti-Virus-Loadin installieren)
- Faronics Anti-Virus-Client auf dem Arbeitsplatz bzw. den Arbeitsplätzen implementieren.
- Eine Antivirenrichtlinie erstellen, bearbeiten, löschen und anwenden
- Einen Arbeitsplatz bzw. Arbeitplätze über die Faronics Core Console durchsuchen
- Firewall Aktivieren/Deaktivieren
- Suchverlauf anzeigen
- In Quarantäne gestellte Dateien anzeigen und Aktionen für diese ausführen
- Antivirus-Definitionen über die Faronics Core Console aktualisieren
- Berichte generieren
- Aktiven Schutz Aktivieren/Deaktivieren
- Protokolle anzeigen

Faronics Anti-Virus auf dem Arbeitsplatz verwenden

- Faronics Anti-Virus auf dem Arbeitsplatz starten
- Den Arbeitsplatz durchsuchen
- Antivirus-Definitionen auf dem Arbeitsplatz aktualisieren
- Aktiven Schutz Aktivieren/Deaktivieren
- Firewall Aktivieren/Deaktivieren
- Suchverlauf anzeigen
- In Quarantäne

Faronics Anti-Virus über die Faronics Core Console verwalten

Nachdem das Faronics Anti-Virus-Loadin installiert wurde, können die Arbeitsplätze über die Faronics Core Console verwaltet werden. In den nachfolgenden Abschnitten werden diverse Aspekte der Verwaltung von Faronics Anti-Virus über die Faronics Core Console erläutert.

Faronics Anti-Virus-Client auf dem Arbeitsplatz bzw. den Arbeitsplätzen implementieren

Führen Sie die folgenden Schritte aus, um den Faronics Anti-Virus-Client auf dem Arbeitsplatz bzw. den Arbeitsplätzen zu installieren:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster „Baumstruktur der Konsole“ auf *Faronics Core Console>[Name des Core Servers]>Arbeitsplätze>Verwaltete Arbeitsplätze*.
3. Klicken Sie mit der rechten Maustaste auf einen Arbeitsplatz bzw. auf mehrere Arbeitsplätze, und wählen Sie *Arbeitsplätze konfigurieren>Erweitert>Anti-Virus-Client installieren/aktualisieren* aus.

Der Faronics Anti-Virus-Client wird auf dem Arbeitsplatz bzw. den Arbeitsplätzen installiert.

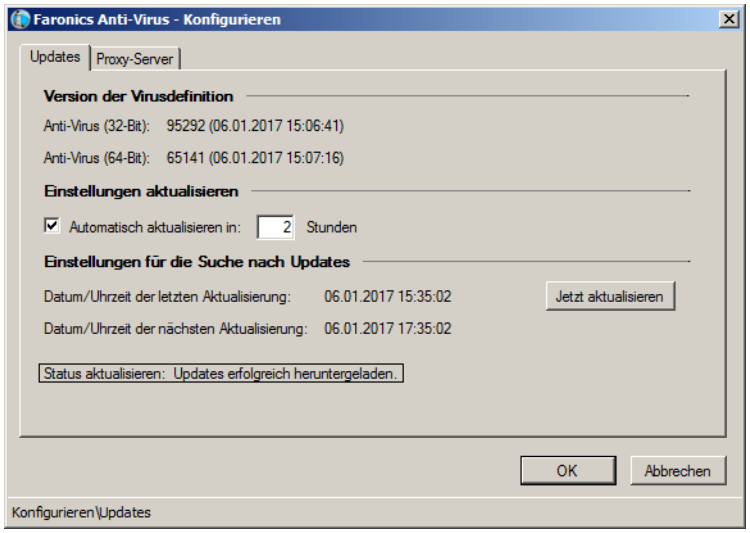
Nach einer erfolgreichen Implementierung verfügt der Arbeitsplatz über die Standardrichtlinie und die aktuellsten Virusdefinitionen.

Faronics Anti-Virus konfigurieren

Führen Sie die folgenden Schritte aus, um Faronics Anti-Virus zu konfigurieren:

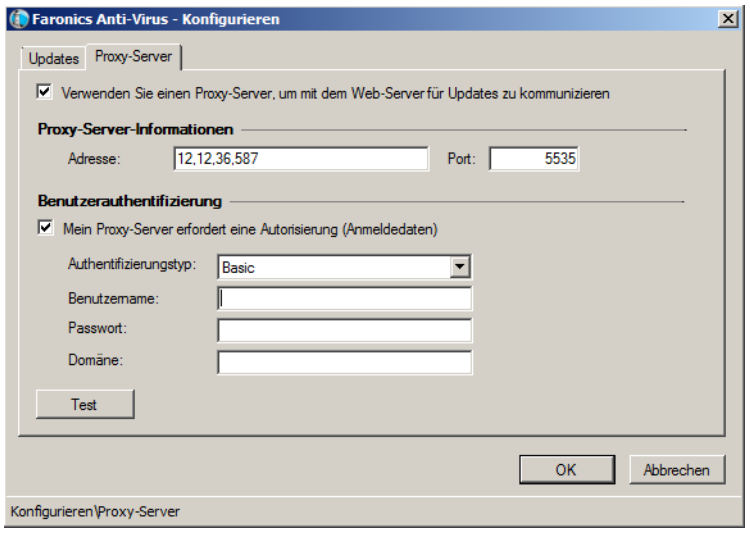
1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster „Baumstruktur der Konsole“ auf *Faronics Core Console>[Name des Core Servers]>Arbeitsplätze>Verwaltete Arbeitsplätze>Anti-Virus*.
3. Klicken Sie mit der rechten Maustaste auf Anti-Virus, und wählen Sie *Anti-Virus konfigurieren* aus.
4. Die Registerkarte „Updates“ des Dialogs „Faronics Anti-Virus konfigurieren“ wird angezeigt.

5. Die Registerkarte „Updates“ zeigt die Version der Scan-Engine sowie die Version der Virusdefinition an. Geben Sie die folgenden Optionen an:



   > Automatisch aktualisieren (in Stunden) – wählen Sie dieses Markierungsfeld aus, um die Virusdefinitionen automatisch zu aktualisieren.
   > Stunden – Geben Sie einen Wert zwischen 1 und 72 Stunden an.
   > Jetzt aktualisieren – klicken Sie auf diese Schaltfläche, um die Anti-Virus-Definitionen zu aktualisieren.

6. Klicken Sie auf die Registerkarte „Proxy-Server”, und geben Sie Werte für die folgenden Optionen an:



7. Wählen Sie „Proxy-Server verwenden, um mit dem Web-Server für Updates zu kommunizieren” aus, und geben Sie die folgenden Informationen an:

   > Adresse – Geben Sie die IP-Adresse oder die URL an.
   > Port – Geben Sie den Port an.

8. Wählen Sie „Proxy-Server verwenden, um mit dem Web-Server für Updates zu kommunizieren“ aus, und geben Sie die folgenden Einstellungen an:
   > Authentifizierungstyp
   > Benutzername
   > Passwort
   > Domäne
9. Klicken Sie auf *Test*, um die Verbindung zu testen. Klicken Sie auf OK, um die Proxy-Einstellungen zu speichern.

Faronics Anti-Virus aktualisieren

Führen Sie die folgenden Schritte aus, um die Einstellungen eines einzelnen Arbeitsplatzes, auf dem Faronics Anti-Virus läuft, abzurufen:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster „Baumstruktur der Konsole“ auf *Faronics Core Console>[Name des Core Servers]>Arbeitsplätze>Verwaltete Arbeitsplätze*.
3. Klicken Sie mit der rechten Maustaste auf einen Arbeitsplatz, und wählen Sie *Anti-Virus aktualisieren* aus.
4. Faronics Anti-Virus wird aktualisiert, und die folgenden Spalten werden auf den neusten Stand gebracht:
   > Richtlinienname
   > Status
   > % des Suchlaufs abgeschlossen
   > Definitionsversion
   > Datum der letzten Aktualisierung
   > Datum des letzten Suchlaufs
   > Datum der letzten erkannten Bedrohung
   > Version

Faronics Anti-Virus-Richtlinie

Eine Antivirusrichtlinie enthält alle Konfigurationseinstellungen darüber, wie Faronics Anti-Virus auf dem Arbeitsplatz bzw. den Arbeitsplätzen läuft. Eine Richtlinie enthält die vom Programm durchgeführten Aktionen, den Zeitplan, den Proxy-Server, Fehlerberichte und die für den Benutzer auf dem Arbeitsplatz bzw. den Arbeitsplätzen zugängliche Funktionalität. Die folgenden Abschnitte erläutern die Erstellung und Anwendung einer Antivirusrichtlinie.

Wenn Sie das veraltete Anti-Virus verwenden, führen Sie die folgenden Schritte aus, um zum neuen Anti-Virus zu migrieren:

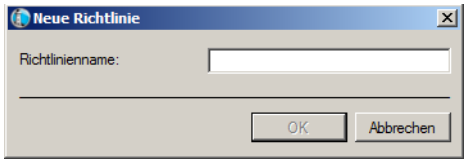
1. Deinstallieren Sie das veraltete Anti-Virus von den verwalteten Arbeitsplätzen.
2. Konfigurieren Sie die neue Anti-Virus-Richtlinie.
3. Installieren Sie das neue Anti-Virus auf den verwalteten Arbeitsplätzen.

Faronics Anti-Virus enthält eine *Standard*richtlinie. Die Standardrichtlinie enthält die optimalen Konfigurationseinstellungen für die Verwaltung von Faronics Anti-Virus.

Antivirusrichtlinien erstellen

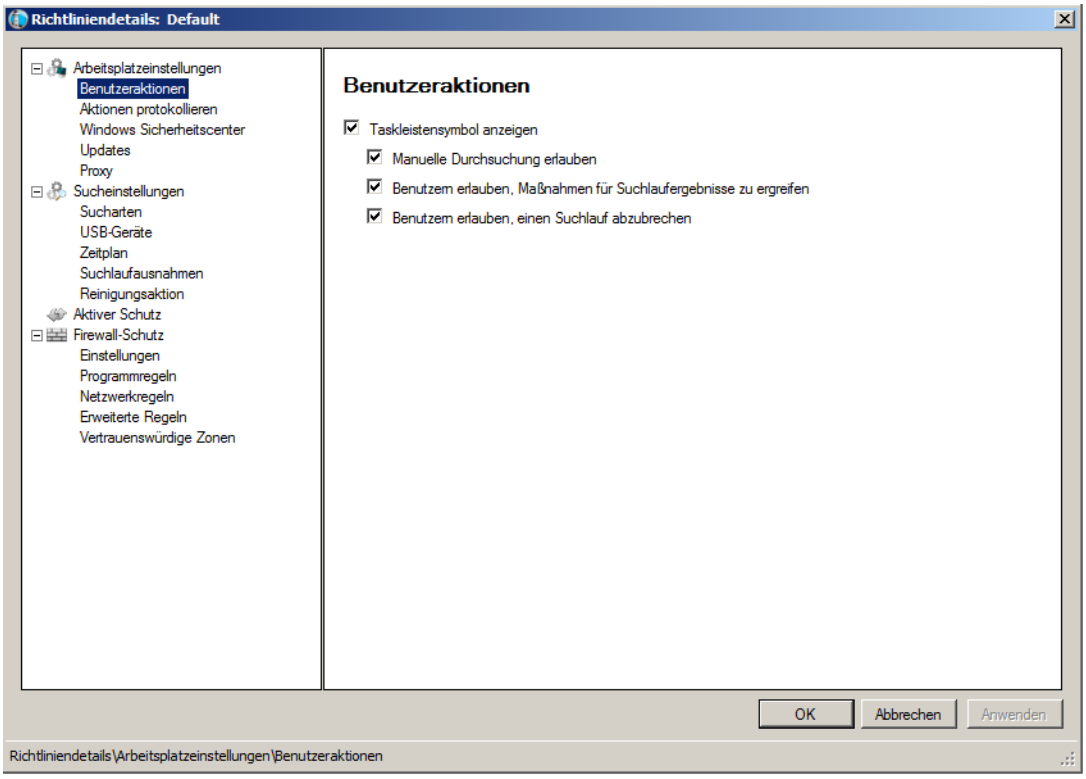
Führen Sie die folgenden Schritte aus, um eine neue Antivirusrichtlinie zu erstellen:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster *Baumstruktur der Konsole* auf *Faronics Core Console>[Name des Core Servers]>Arbeitsplätze>Verwaltete Arbeitsplätze>Anti-Virus*.
3. Klicken Sie mit der rechten Maustaste auf *Anti-Virus*, und wählen Sie *Neue Richtlinie* aus.
4. Geben Sie im Dialog *Neue Richtlinie* einen Namen für die Richtlinie an. Klicken Sie auf *OK*. Eine neue Richtlinie wird unter dem Knoten *Antivirusrichtlinie* erstellt. Sie können die neue Richtlinie beispielsweise *Neue Richtlinie 1* nennen.



5. Klicken Sie mit der rechten Maustaste auf *Neue Richtlinie 1*, und wählen Sie *Richtliniendetails* aus. Der Dialog *Richtliniendetails* wird angezeigt.
6. Geben Sie die Einstellungen unter dem Knoten *Arbeitsplatzeinstellungen* an.

- Teilfenster *Benutzeraktionen*



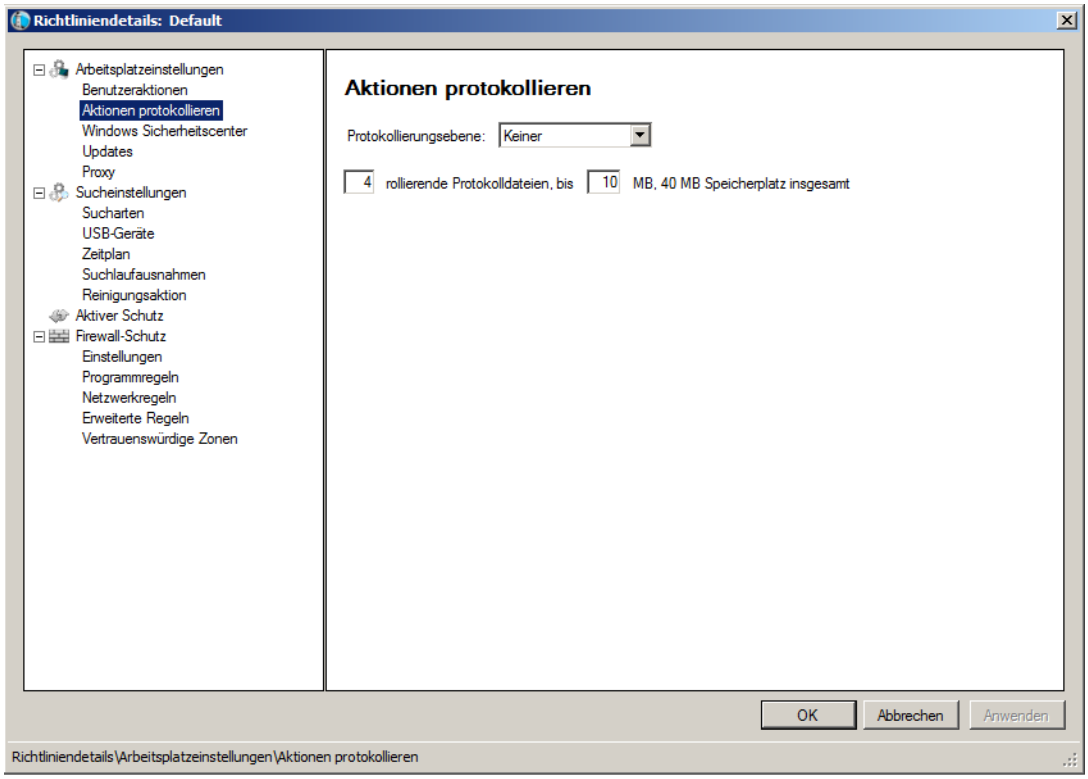
> Taskleistensymbol anzeigen – Wählen Sie dieses Markierungsfeld aus, um das Faronics Anti-Virus-Symbol in der Taskleiste des Arbeitsplatzes bzw. der Arbeitsplätze anzuzeigen. Wenn dieses Markierungsfeld nicht ausgewählt ist, wird Faronics Anti-Virus für den Benutzer ausgeblendet.

~ Manuelle Durchsuchung erlauben – Wählen Sie dieses Markierungsfeld aus, um es Benutzern zu erlauben, einen Faronics Anti-Virus-Suchlauf auf dem Arbeitsplatz bzw. den Arbeitsplätzen manuell anzustoßen.

~ Benutzern erlauben, Maßnahmen für Suchlaufergebnisse zu ergreifen – Wählen Sie dieses Markierungsfeld aus, um es Benutzern des Arbeitsplatzes zu erlauben, Maßnahmen für Suchlaufergebnisse zu ergreifen.

~ Benutzern erlauben, einen Suchlauf lokal abzubrechen – Wählen Sie dieses Markierungsfeld aus, um es Benutzern zu erlauben, den Suchlauf lokal auf dem Arbeitsplatz abzubrechen.

- Teilfenster *Aktionen protokollieren*

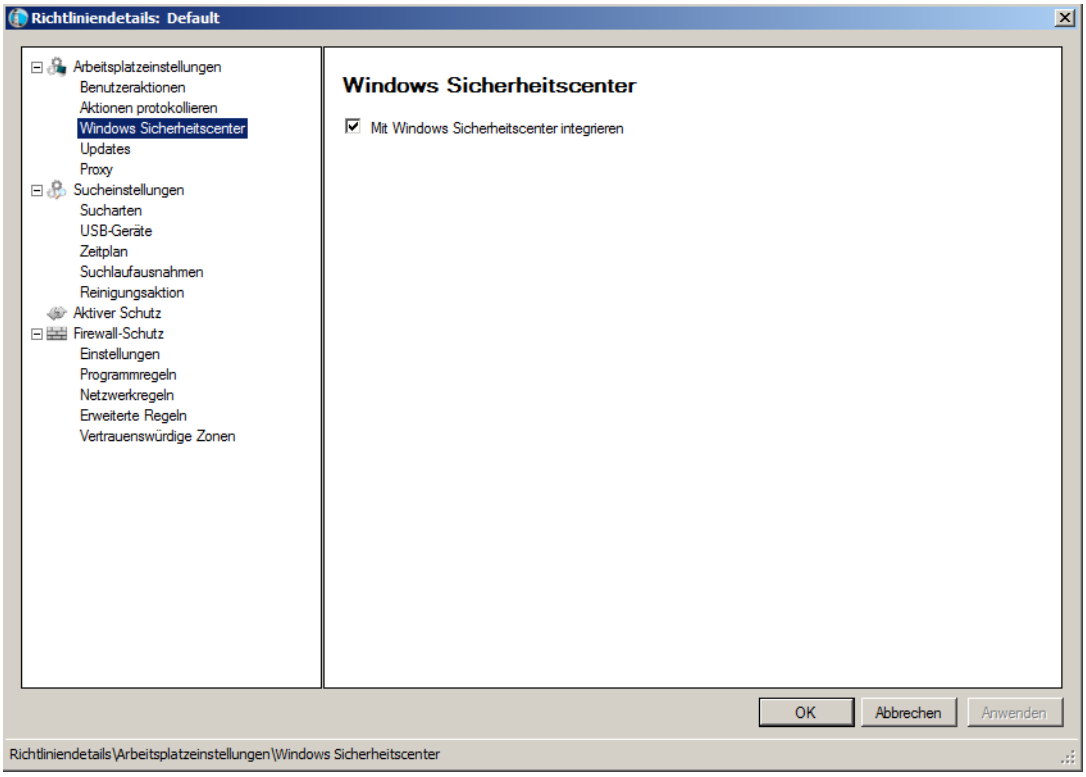


> Protokollierungsebene – Wählen Sie die Protokollierungsebene aus. Wählen Sie *Keine* aus, um keine Protokollierung einzustellen. Wählen Sie *Fehler* aus, um die Fehlermeldung zu protokollieren. Wählen Sie *Trace* für eine Nachverfolgung aus. Wählen Sie *Ausführlich* aus, um eine detaillierte Protokollierung zu erhalten.

> Anzahl Protokolldateien – Geben Sie die Anzahl der Protokolldateien an. Die Protokollinformationen werden seriell in den Dateien gespeichert. Wenn es beispielsweise drei Dateien A, B und C gibt, schreibt Faronics Anti-Virus die Fehlerprotokolle zunächst in Datei A. Wenn Datei A voll ist, werden die Protokolle in Datei B geschrieben, und schließlich in Datei C. Sobald Datei C voll ist, werden die Daten in Datei A gelöscht und mit neuen Protokolldaten überschrieben.

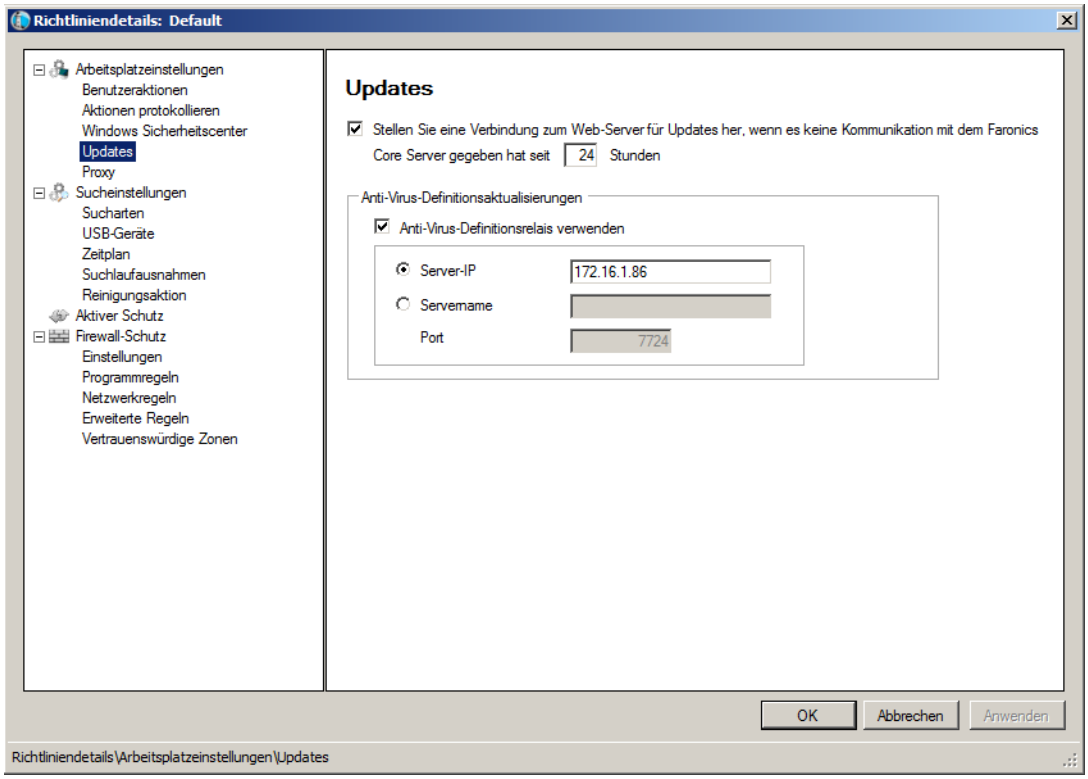
> Dateigröße – Wählen Sie die Größe der einzelnen Dateien in MB aus.

- Teilfenster *Windows Sicherheitscenter*



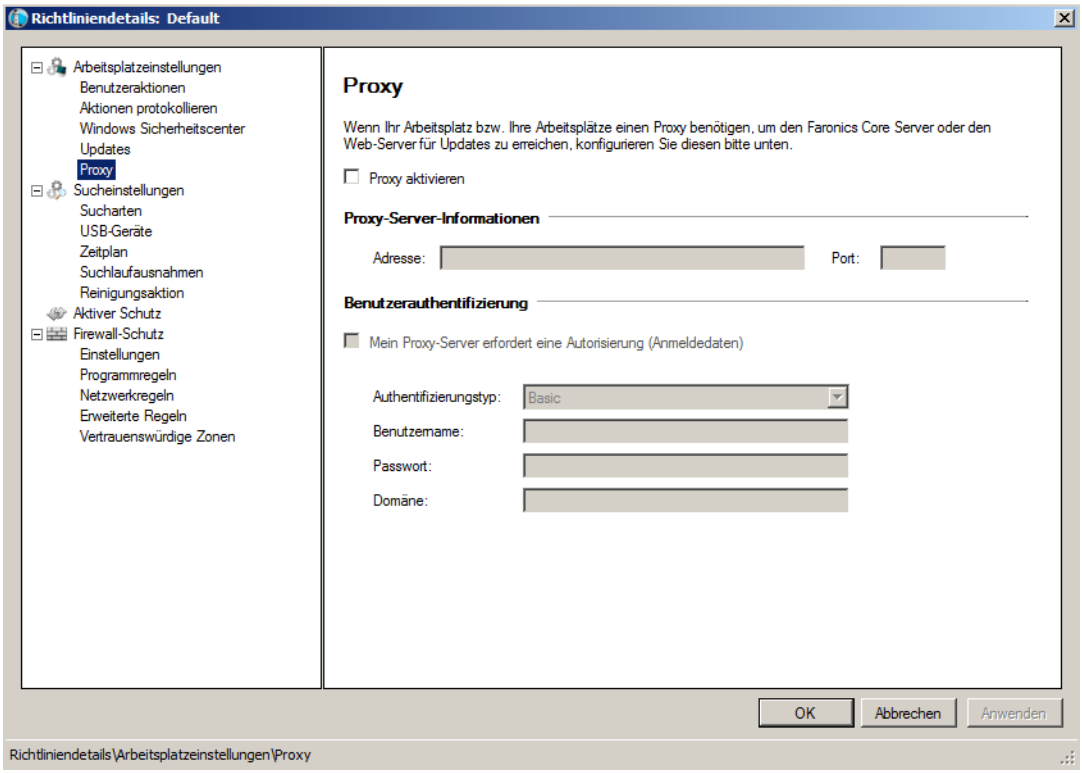
> Mit Windows Sicherheitscenter integrieren – Wählen Sie dieses Markierungsfeld aus, um Faronics Anti-Virus mit dem Windows Sicherheitscenter zu integrieren. Das Windows Sicherheitscenter informiert Sie über die Taskleiste, ob Faronics Anti-Virus aktiv oder inaktiv ist.

- Teilfenster *Updates*



> Verbindung zum Web-Server für Updates herstellen, wenn es in den letzten x Stunden keine Kommunikation mit dem Faronics Core Server gab – Wählen Sie dieses Markierungsfeld aus, um eine Verbindung zum Web-Server für Updates herzustellen und Virusdefinitionen herunterzuladen, wenn der Kontakt zwischen dem Arbeitsplatz und dem Faronics Core Server unterbrochen wurde. Wenn Sie dieses Markierungsfeld nicht auswählen, werden die Virusdefinitionen nicht aktualisiert, wenn die Verbindung zwischen dem Arbeitsplatz und dem Faronics Core Server unterbrochen wird.

- Teilfenster *Proxy*



> Proxy aktivieren – Wählen Sie dieses Markierungsfeld aus, wenn der Arbeitsplatz bzw. die Arbeitsplätze einen Proxy benötigen, um den Faronics Core Server oder den Web-Server für Updates zu erreichen.

> Proxy-Server-Informationen – Geben Sie die *Adresse* und den *Port* an.

> Benutzerauthentifizierung

Mein Proxy-Server erfordert eine Autorisierung (Anmeldedaten) – Wenn der Server eine Authentifizierung erfordert, geben Sie Werte für die folgenden Felder an:

~ Authentifizierungstyp – Wählen Sie den Authentifizierungstyp aus.

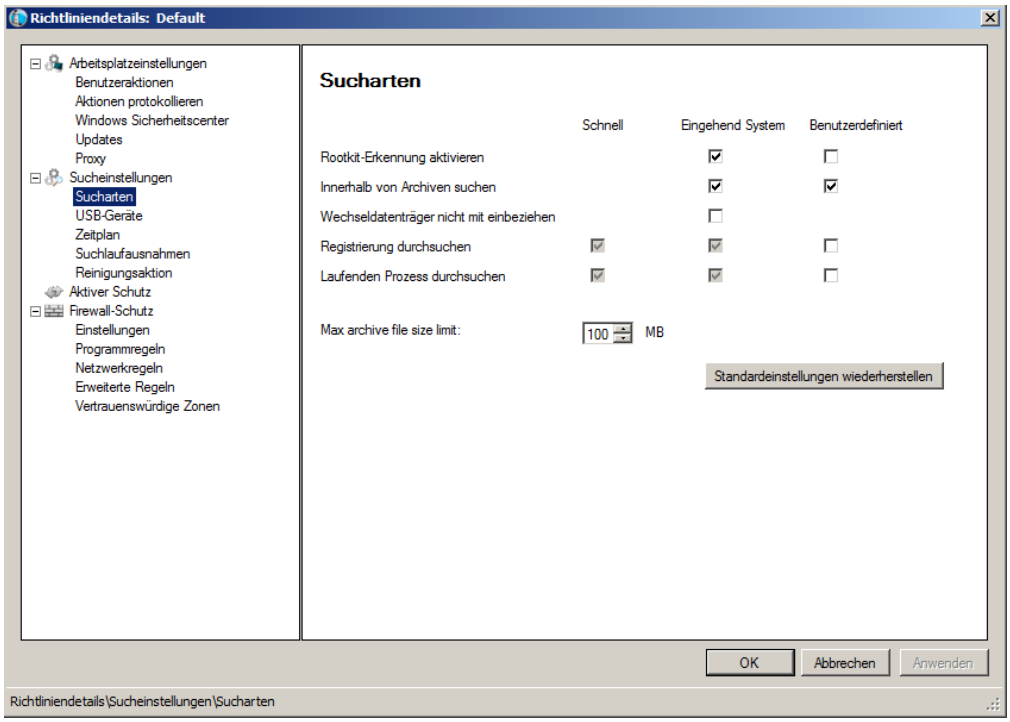
~ Benutzername – Geben Sie den Benutzernamen an.

~ Passwort – Geben Sie das Passwort an.

~ Domäne – Geben Sie die Domäne an.

7. Geben Sie die Einstellungen unter dem Knoten *Sucheinstellungen* an.

- Teilfenster *Sucharten*



Faronics Anti-Virus bietet drei Arten von Suchläufen:

> Schnellsuchlauf – Durchsucht die am häufigsten betroffenen Bereiche Ihres Computers. Die Dauer dieses Suchlaufs ist kürzer als die der eingehenden Systemdurchsuchung. Der Schnellsuchlauf verwendet außerdem weniger Speicherplatz als die eingehende Systemdurchsuchung.

> Eingehende Systemdurchsuchung – Führt einen gründlichen Suchlauf für alle Bereiche des Computers aus. Die für den Suchlauf in Anspruch genommene Zeit hängt von der Größe Ihrer Festplatte ab.

> Benutzerdefinierter Suchlauf – Führt einen Suchlauf auf der Basis der im Dialog *Richtliniendetails* ausgewählten Optionen durch.

Wählen Sie für die einzelnen Sucharten die folgenden Optionen aus (manche Optionen sind, je nach Art des Suchlaufs, möglicherweise ausgeblendet):

> Rootkit-Erkennung aktivieren – Erkennt, ob der Computer mit einem Rootkit infiziert ist.

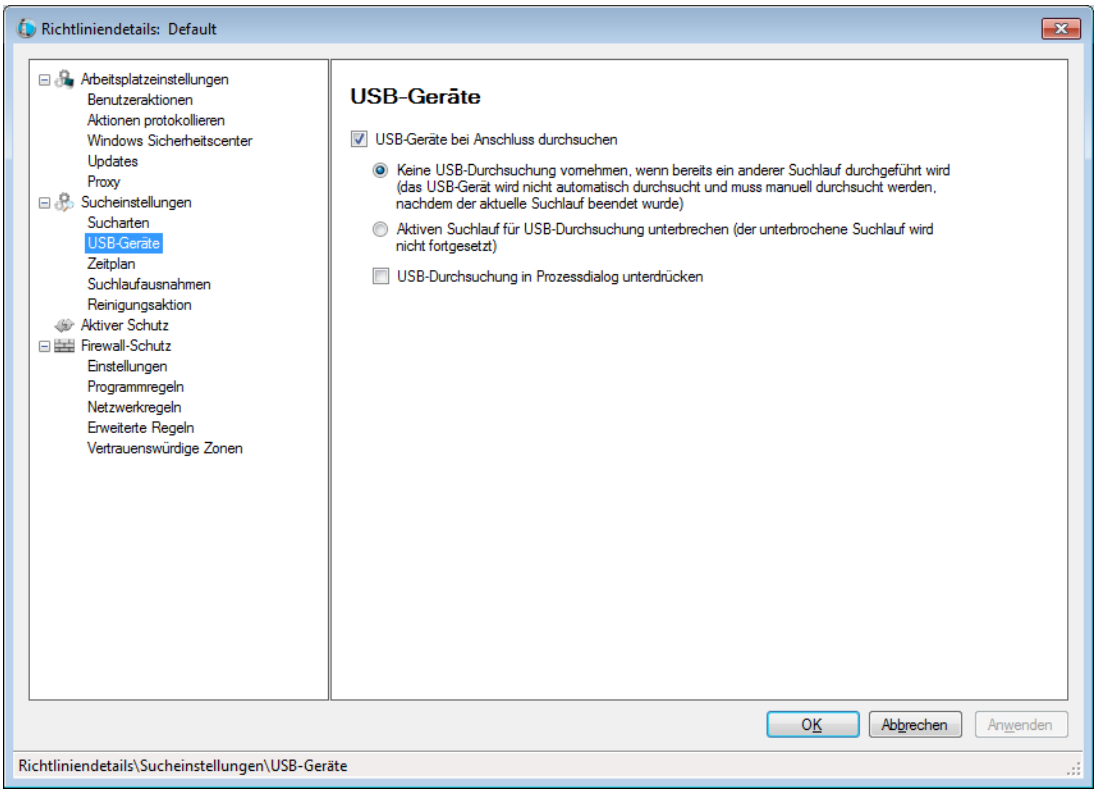
> Innerhalb von Archiven suchen – Durchsucht den Inhalt einer ZIP-Datei. Wenn Sie diese Option auswählen, berücksichtigt der Suchlauf auch Archivdateien wie .RAR- und .ZIP-Dateien. Wenn innerhalb einer .RAR-Datei eine infizierte Datei gefunden wird, wird die .RAR-Datei in Quarantäne gestellt. Wenn innerhalb einer .ZIP-Datei eine infizierte Datei gefunden wird, wird die infizierte Datei in Quarantäne gestellt und durch eine .TXT-Datei ersetzt, deren Text darauf hinweist, dass die Datei infiziert war und in Quarantäne gestellt wurde. Geben Sie die *Höchstgrenze für Dateigröße* an.

> Wechseldatenträger (z.B. USB) nicht mit einbeziehen – Schließt Wechseldatenträger aus dem Suchlauf aus. Externe Festplatten, USB-Laufwerke, etc. werden nicht durchsucht.

> Registrierung durchsuchen – Durchsucht die Registrierung.

> Laufenden Prozess durchsuchen – Durchsucht alle laufenden Prozesse.

- Teilfenster *USB-Geräte*



USB-Laufwerke bei Anschluss durchsuchen – Wählen Sie dieses Markierungsfeld aus, um USB-Laufwerke bei Anschluss zu durchsuchen, und wählen Sie eine der folgenden Optionen aus:

> Keine USB-Durchsuchung durchführen, wenn ein anderer Suchlauf bereits läuft – Wählen Sie diese Option aus, um sicherzustellen, dass ein aktiver Suchlauf nicht unterbrochen wird, wenn ein USB-Laufwerk angeschlossen wird. Das USB-Laufwerk muss manuell durchsucht werden, sobald der aktive Suchlauf abgeschlossen wurde.

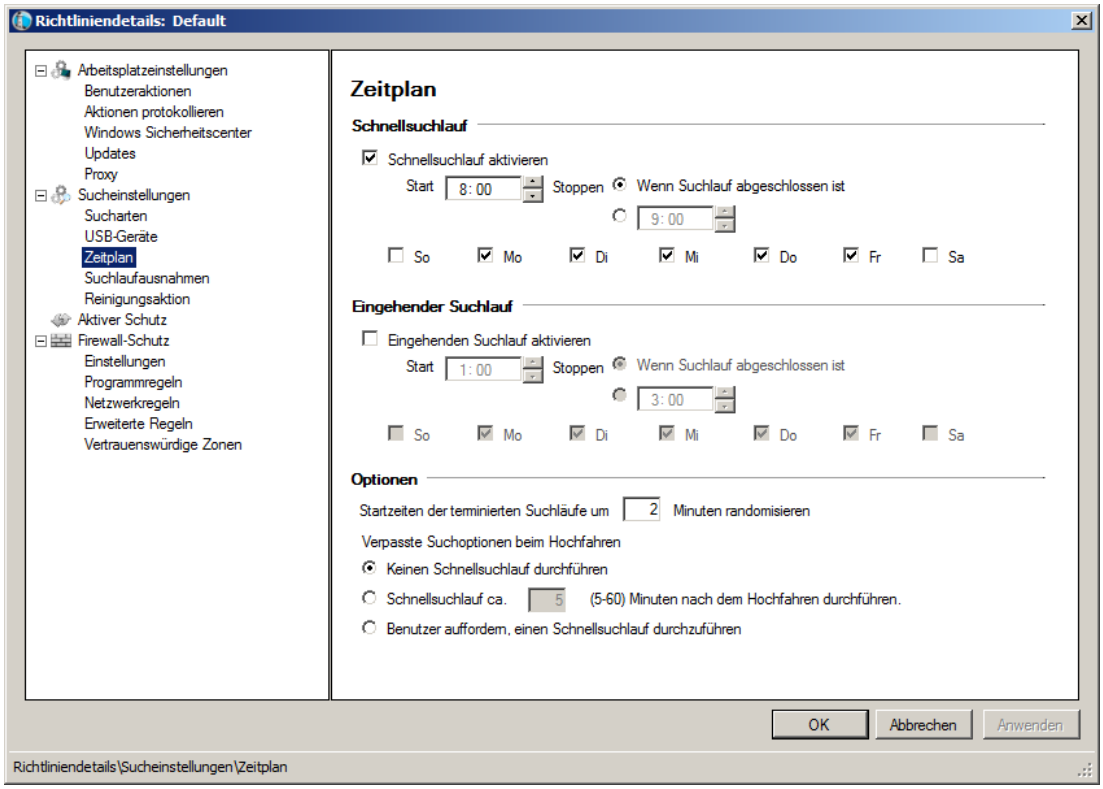
> Aktiven Suchlauf für USB-Durchsuchung unterbrechen – Wählen Sie diese Option aus, um einen aktiven Suchlauf zu unterbrechen, um ein neu angeschlossenes USB-Laufwerk zu durchsuchen. Nachdem der aktive Suchlauf unterbrochen wurde, wird er nicht automatisch fortgesetzt und muss manuell neu gestartet werden.

> USB-Durchsuchung in Prozessdialog unterdrücken – Wählen Sie diese Option aus, um Anzeichen dafür, dass Anti-Virus USB-Geräte nach deren Anschluss durchsucht, auszublenden; es öffnet sich keine Anti-Virus-Benutzeroberfläche, und das Taskleistensymbol zeigt keine Tool-Tipps, die auf eine laufende Durchsuchung hindeuten. Benutzer werden am Ende eines Suchlaufs benachrichtigt, wenn ein Virus gefunden wurde. Wurden jedoch keine Viren erkannt, gibt es keine enachrichtigung über die Durchführung des Suchlaufs.

  Beachten Sie, dass diese Option ignoriert wird, wenn die Option USB-Laufwerke bei Anschluss durchsuchen nicht ausgewählt ist.

Wenn das Markierungsfeld *Manuelle Durchsuchung erlauben* im Teilfenster *Benutzeraktionen* der Registerkarte *Arbeitsplatzeinstellungen* ausgewählt ist, wird das USB-Gerät automatisch durchsucht. Wenn das Markierungsfeld *Manuelle Durchsuchung erlauben* nicht ausgewählt ist, wird das USB-Gerät nicht automatisch durchsucht.

- Teilfenster *Zeitplan*



Schnellsuchlauf:

> Schnellsuchlauf aktivieren – Wählen Sie dieses Markierungsfeld aus, um den Schnellsuchlauf zu aktivieren.

> Start – Geben Sie die Startzeit an.

> Ende – Geben Sie die Endzeit an. Die maximale Dauer zwischen der *Startzeit* und der *Endzeit* beträgt *23:59* Stunden. Der Suchlauf endet, wenn vor Erreichen der *Endzeit* alle Dateien durchsucht wurden. Wenn der Suchlauf bis zur *Endzeit* nicht abgeschlossen ist, wird er zum *Endzeitpunkt* abgebrochen. Alternativ hierzu können Sie auch die Option *Wenn Suchlauf abgeschlossen ist* auswählen, um sicherzustellen, dass der Suchlauf abgeschlossen wird.

> Tage – Wählen Sie die Tage aus, an denen der terminierte Schnellsuchlauf durchgeführt werden soll.

Eingehender Suchlauf:

> Eingehenden Suchlauf aktivieren – Wählen Sie dieses Markierungsfeld aus, um den eingehenden Suchlauf zu aktivieren.

> Start – Geben Sie die Startzeit an.

> Ende – Geben Sie die Endzeit an. Die maximale Dauer zwischen der *Startzeit* und der *Endzeit* beträgt *23:59* Stunden. Der Suchlauf endet, wenn vor Erreichen der *Endzeit* alle Dateien durchsucht wurden. Wenn der Suchlauf bis zur *Endzeit* nicht abgeschlossen ist, wird er zum *Endzeitpunkt* abgebrochen. Alternativ hierzu können Sie auch die Option *Wenn Suchlauf abgeschlossen ist* auswählen, um sicherzustellen, dass der Suchlauf abgeschlossen wird.

> Tage – Wählen Sie die Tage aus, an denen der terminierte eingehende Suchlauf durchgeführt werden soll.

Optionen:

> Startzeiten der terminierten Suchläufe um x Minuten randomisieren – Geben Sie die Anzahl der Minuten an. Die Startzeit der terminierten Suchläufe wird randomisiert, um die Auswirkungen auf den Datenverkehr im Netzwerk zu minimieren. Faronics Anti-Virus sendet eine Meldung an Faronics Core, wenn der Suchlauf beginnt. Dies kann zu einem erhöhten Datenaufkommen im Netzwerk führen, wenn der Suchlauf für mehrere Systeme gleichzeitig angestoßen wird.

Optionen für verpasste Suchläufe beim Hochfahren – Wählen Sie eine der folgenden Optionen aus, die bestimmen, wie ein Suchlauf durchgeführt wird, wenn der Arbeitsplatz zum Zeitpunkt eines terminierten Suchlaufs nicht *eingeschaltet* war:

> Keinen Schnellsuchlauf durchführen – Wählen Sie diese Option aus, wenn Sie beim Hochfahren keinen Schnellsuchlauf durchführen möchten.

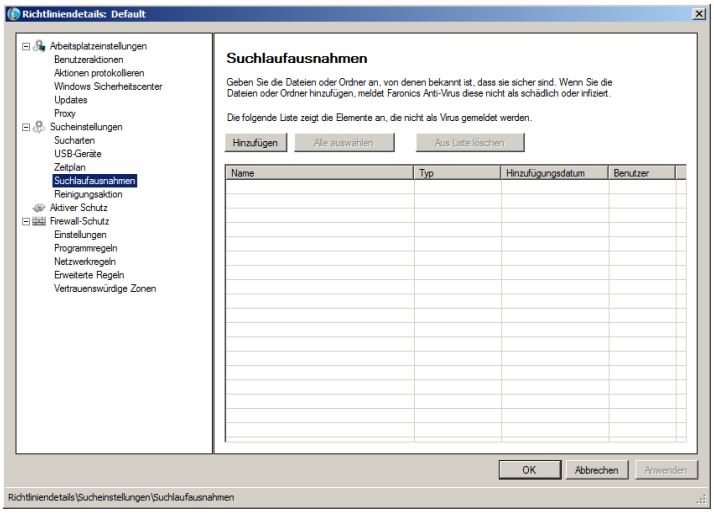
> Schnellsuchlauf ca. x Minuten nach dem Hochfahren durchführen – Geben Sie an, wie viele Minuten nach dem Hochfahren Faronics Anti-Virus einen Schnellsuchlauf durchführen soll.

> Benutzer auffordern, einen Schnellsuchlauf durchzuführen – Wählen Sie diese Option aus, um den Benutzer aufzufordern, einen Schnellsuchlauf durchzuführen.

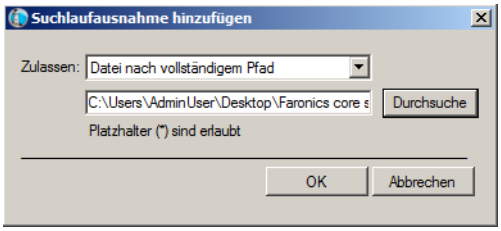
- Teilfenster *Suchlaufausnahmen*

  Ordner oder Dateien, von denen bekannt ist, dass sie sicher und infektionsfrei sind, können zur Registerkarte Suchlaufausnahmen hinzugefügt werden. Dateien, die zur Registerkarte Suchlaufausnahmen hinzugefügt werden, werden immer von Faronics Anti-Virus durchsucht. Faronics Anti-Virus meldet die Dateien jedoch niemals als schädlich oder infiziert. Diese Funktion ist nützlich, da Dateien und Ordner, von denen der Administrator weiß, dass sie sicher sind, nicht als schädlich gemeldet werden.

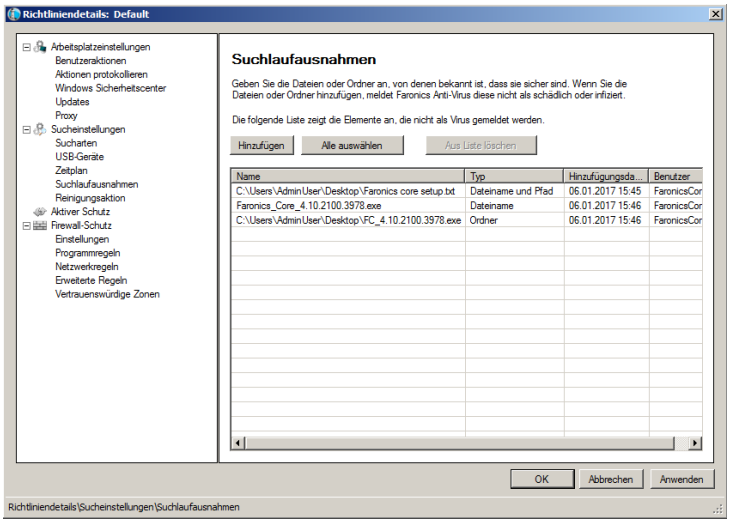
  A. Klicken Sie auf *Hinzufügen*.



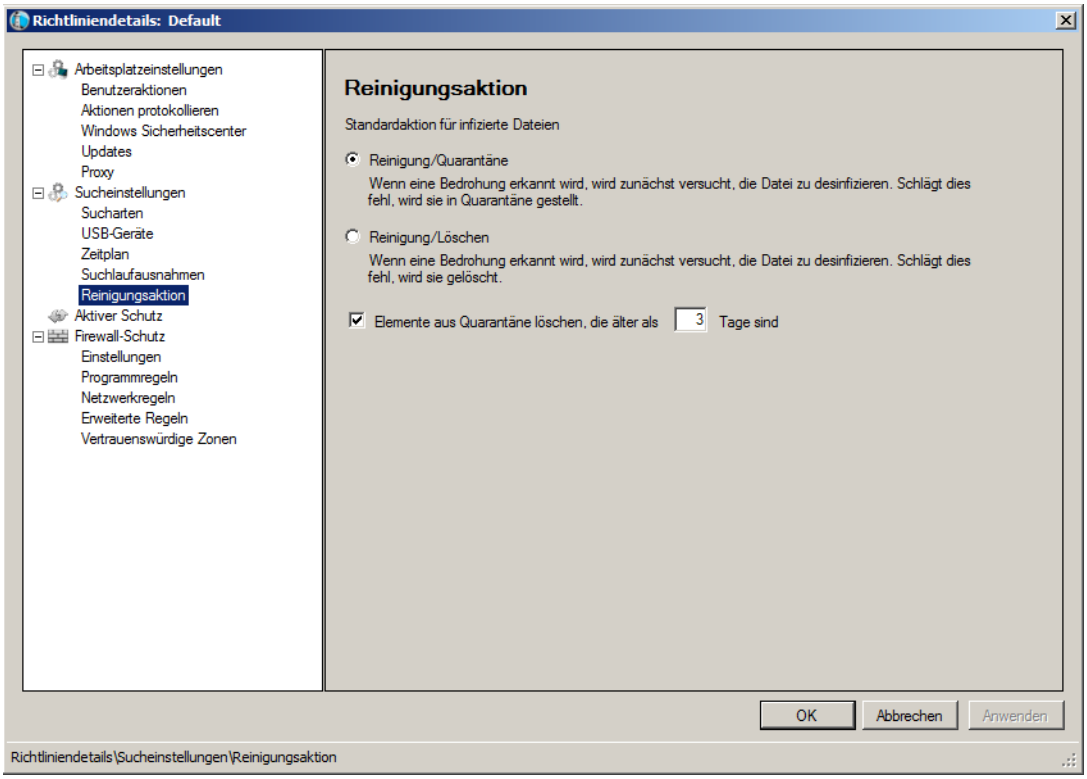
  B. Wählen Sie im Dialog *Hinzufügen* entweder *Datei nach vollständigem Pfad*, oder *Gesamter Ordner* aus. Klicken Sie auf Durchsuchen, um die Datei oder den Ordner auszuwählen, und klicken Sie auf *OK*.



  C. Die Option *Datei nach vollständigem Pfad* wird zum Teilfenster Suchlaufausnahmen hinzugefügt.



- Teilfenster *Reinigungsaktion*

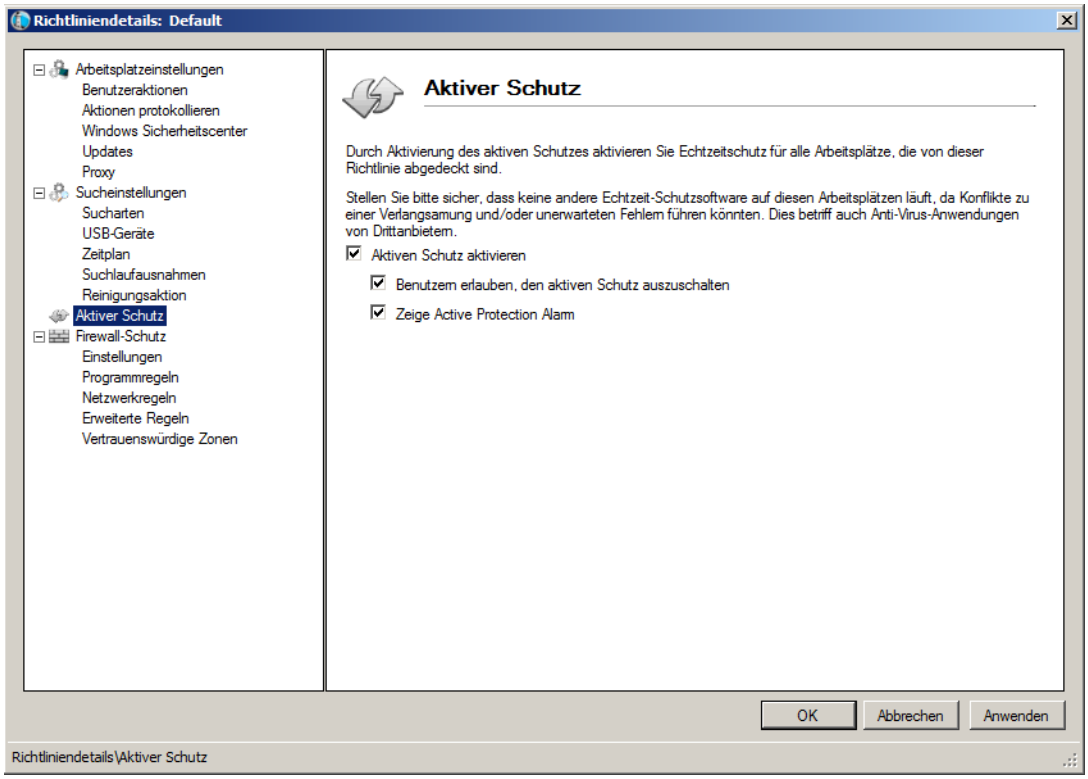


> Reinigung/Quarantäne – Wenn eine Bedrohung erkannt wird, wird zunächst versucht, die Datei zu desinfizieren. Schlägt dies fehl, wird sie in Quarantäne gestellt.

> Reinigung/Löschen – Wenn eine Bedrohung erkannt wird, wird zunächst versucht, die Datei zu desinfizieren. Schlägt dies fehl, wird sie gelöscht.

> Elemente aus Quarantäne löschen, die älter sind als – Geben Sie die Anzahl der Tage an, während derer Elemente in der Quarantäne vorgehalten werden sollen. Der Standardwert ist 3 Tage.

8. Geben Sie die Einstellungen im Teilfenster *Aktiver Schutz* an.

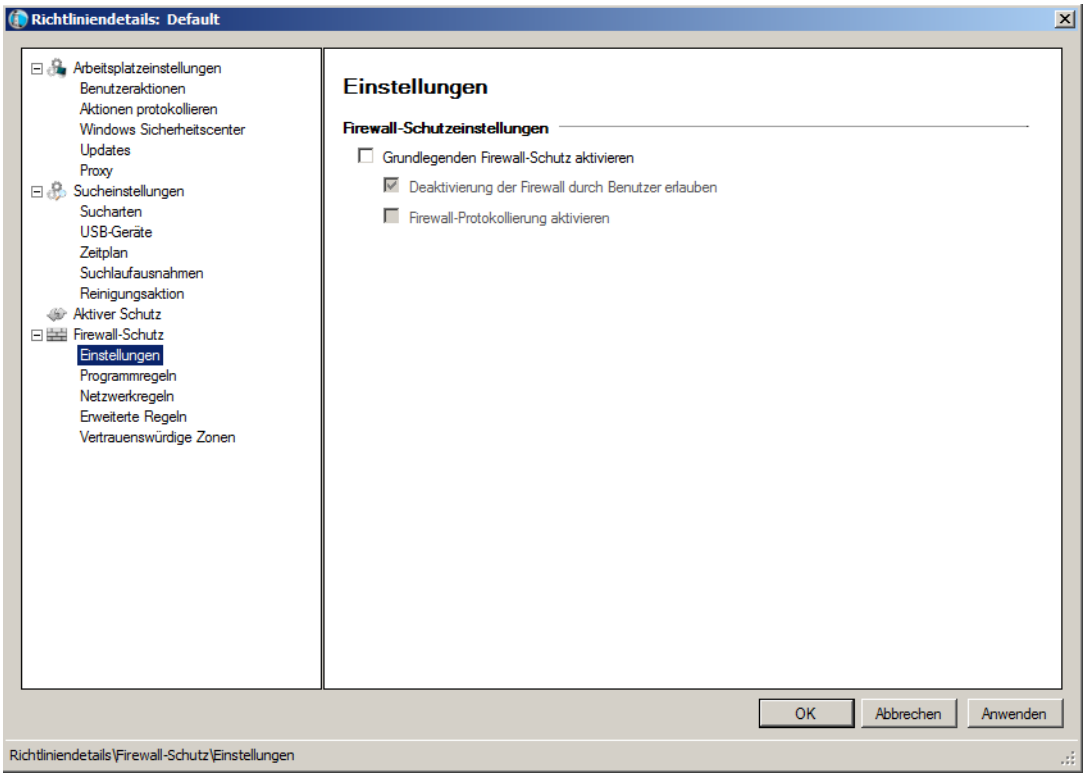


- Aktiven Schutz aktivieren – Wählen Sie diese Option aus, um Echtzeitschutz zu aktivieren. Der aktive Schutz ist die Echtzeitdurchsuchung, die Faronics Anti-Virus im Hintergrund ohne Auswirkungen auf die Systemleistung durchführt. Wenn das Risiko einer Echtzeitvirusinfektion über das Internet besteht, sollten Sie diese Option auswählen.
  - > Benutzern erlauben, den aktiven Schutz auszuschalten – Wählen Sie diese Option aus, um es Benutzern zu erlauben, den aktiven Schutz auszuschalten. Wenn Benutzer Software installieren oder verwenden, die fälschlicherweise als Virus erkannt werden könnte (beispielsweise erweiterte Makros in Microsoft Office oder komplexe Batch-Dateien), wählen Sie diese Option aus.
  - > Warnmeldung zum aktiven Schutz anzeigen – Wählen Sie diese Option aus, um eine Warnmeldung anzuzeigen, wenn während des aktiven Schutzes eine Bedrohung erkannt wird. Wählen Sie dieses Markierungsfeld nicht aus, wenn keine Warnmeldung angezeigt werden soll.

9. Geben Sie die Einstellungen unter dem Knoten *Firewall-Schutz* an.

   Der Knoten Firewall-Schutz bietet bidirektionalen Schutz und schützt Sie vor sowohl eingehendem als auch abgehendem Datenverkehr. Sie können individuell angepasste Regeln erstellen, um Ihr Netzwerk zu schützen. Sie können die Kommunikation entweder *Zulassen* oder *Blockieren*.

- Teilfenster *Einstellungen*



Firewall-Schutzeinstellungen

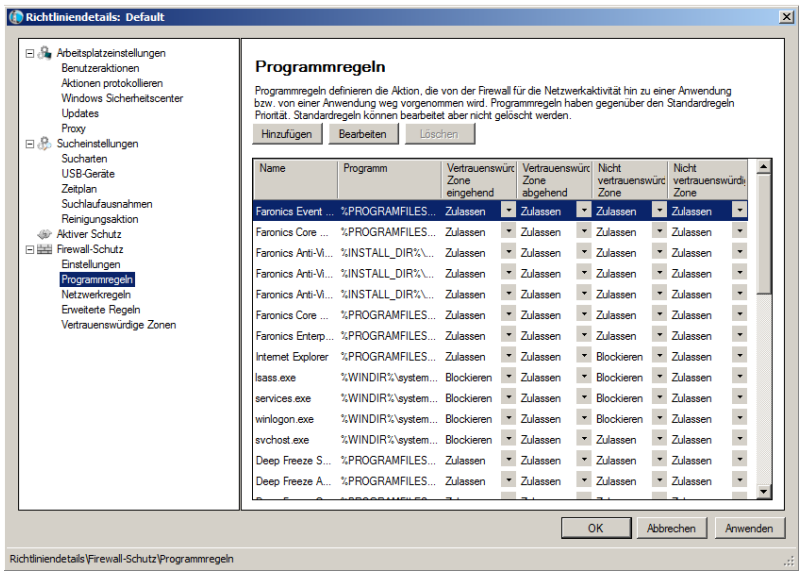
> Grundlegenden Firewall-Schutz aktivieren – Wählen Sie dieses Markierungsfeld aus, um den Firewall-Schutz zu aktivieren. Der Firewall-Schutz hindert Hacker oder schädliche Software daran, sich über das Internet oder das Netzwerk Zugriff auf Ihren Computer zu verschaffen.

  ~ Deaktivierung der Firewall durch Benutzer erlauben – wählen Sie diese Option auf, um es Benutzern zu erlauben, die Firewall am Computer zu deaktivieren.

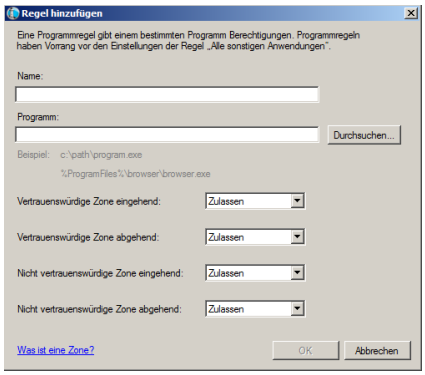
  ~ Firewall-Protokollierung aktivieren – wählen Sie diese Option aus, um alle mit der Firewall zusammenhängenden Aktionen zu protokollieren.

- Teilfenster *Programmregeln*

  Programmregeln definieren die Aktion, die von der Firewall für die Netzwerkaktivität hin zu einer Anwendung bzw. von einer Anwendung weg vorgenommen wird. Programmregeln haben gegenüber den Standardregeln Priorität. Standardregeln können bearbeitet aber nicht gelöscht werden.



Klicken Sie auf *Hinzufügen*, um eine neue Programmregel hinzuzufügen. Geben Sie die entsprechenden Optionen ein, oder wählen Sie sie aus, und klicken Sie auf *OK*. Die folgenden Parameter werden angezeigt:



> Name – Name der Regel.

> Programm – Name des Programms, einschließlich des vollständigen Pfads und der Erweiterung.

> Vertrauenswürdige Zone eingehend – die Aktion wird für eingehende Kommunikation an das Programm in einer vertrauenswürdigen Zone vorgenommen (*Zulassen* oder *Sperren*).

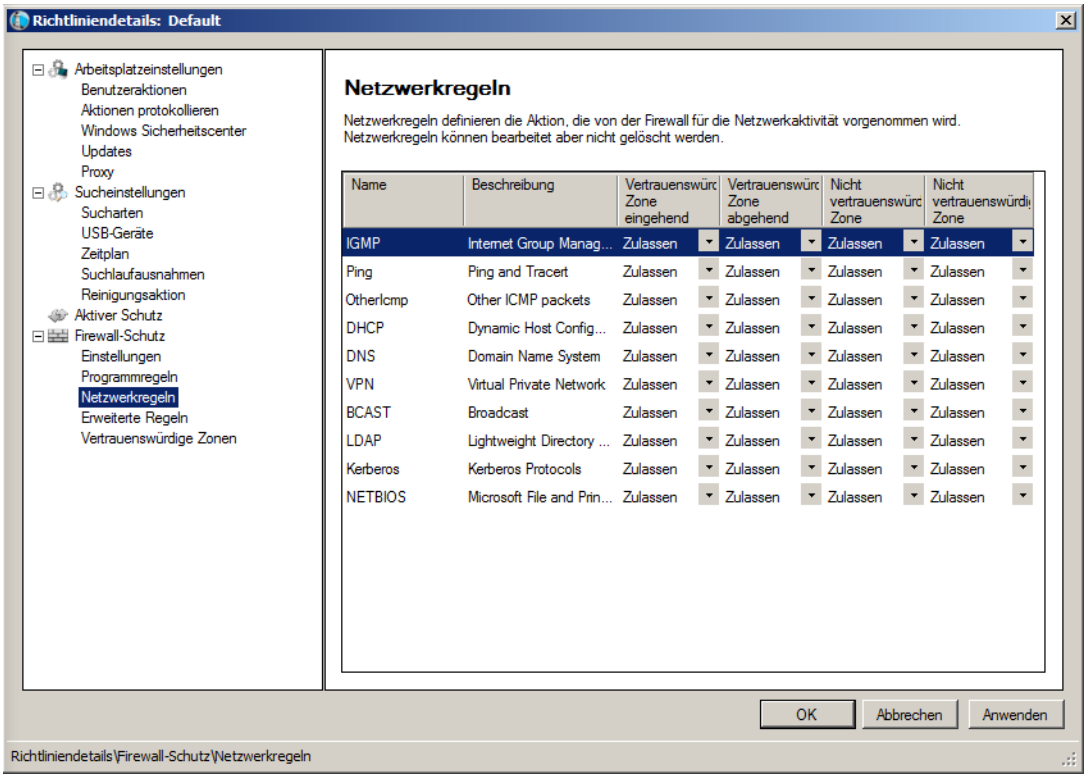
> Vertrauenswürdige Zone abgehend – die Aktion wird für abgehende Kommunikation vom Programm in eine vertrauenswürdige Zone vorgenommen (*Zulassen* oder *Sperren*).

> Nicht vertrauenswürdige Zone eingehend – die Aktion wird für eingehende Kommunikation an das Programm in einer nicht vertrauenswürdigen Zone vorgenommen (*Zulassen* oder *Sperren*).

> Nicht vertrauenswürdige Zone abgehend – die Aktion wird für abgehende Kommunikation vom Programm in eine nicht vertrauenswürdige Zone vorgenommen (*Zulassen* oder *Sperren*).

- Teilfenster *Netzwerkregeln*

  Netzwerkregeln definieren die Aktion, die von der Firewall für die Netzwerkaktivität vorgenommen wird. Netzwerkregeln können bearbeitet aber nicht gelöscht werden.

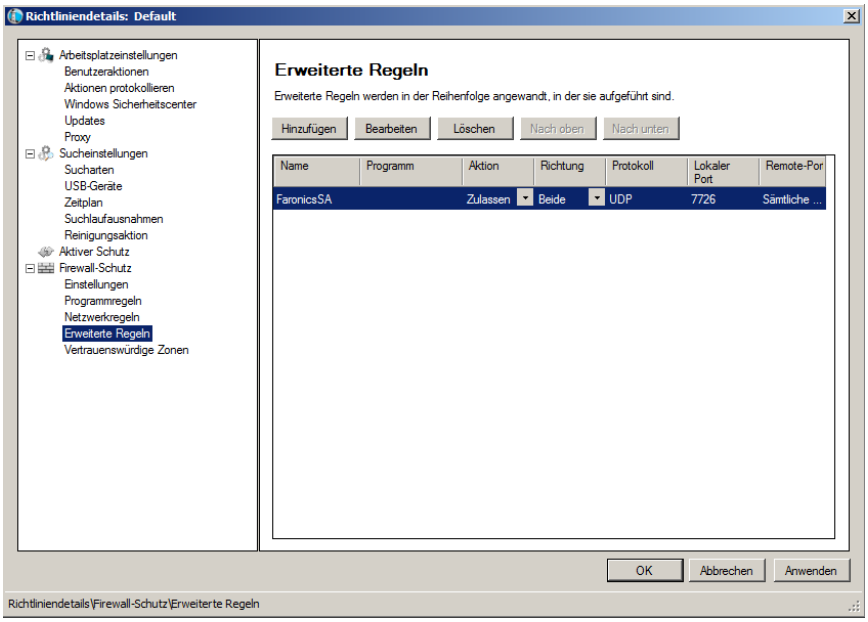


Wählen Sie für Folgendes die Netzwerkregeln aus:

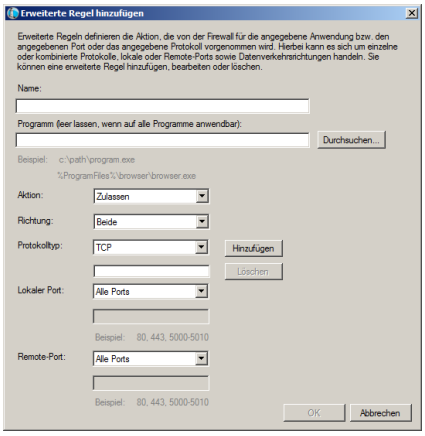
Name	Beschreibung	Vertrauenswürdige Zone eingehend	Vertrauenswürdige Zone abgehend	Nicht vertrauenswürdige Zone eingehend	Nicht vertrauenswürdige Zone eingehend
IGMP	Internet Group Management Protocol	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
Ping	Ping und Tracert	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
OtherIcmp	Andere ICMP-Pakete	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
DHCP	Dynamic Host Configuration Protocol	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
DNS	Domain Name System	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
VPN	Virtual Private Network	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
BCAST	Broadcast	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
LDAP	Lightweight Directory Access Protocol	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
Kerberos	Kerberos-Protokolle	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus
NETBIOS	Microsoft Gemeinsame Datei- und Druckernutzung	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus	Wählen Sie „Zulassen“ oder „Sperren“ aus

- Teilfenster *Erweiterte Regeln*

  Erweiterte Regeln definieren die Aktion, die von der Firewall für die angegebene Anwendung bzw. den angegebenen Port oder das angegebene Protokoll vorgenommen wird. Hierbei kann es sich um einzelne oder kombinierte Protokolle, lokale oder Remote-Ports sowie Datenverkehrsrichtungen handeln. Sie können eine erweiterte Regel hinzufügen, bearbeiten oder löschen.



Klicken Sie auf *Hinzufügen*, um eine neue erweiterte Regel hinzuzufügen. Geben Sie die entsprechenden Optionen ein, oder wählen Sie sie aus, und klicken Sie auf *OK*. Die folgenden Parameter werden im Teilfenster Erweiterte Regeln angezeigt:



> Name – Name der Regel.

> Programm – Name des Programms und Pfad.

> Aktion – die von der Firewall für Kommunikation von der angegebenen Anwendung bzw. dem angegebenen Port oder Protokoll ergriffene Maßnahme (*Zulassen*, *Blockieren* oder *Benutzeraufforderung*).

> Richtung – die Richtung der Kommunikation (*Beides*, *Eingehend*, oder *Abgehend*).

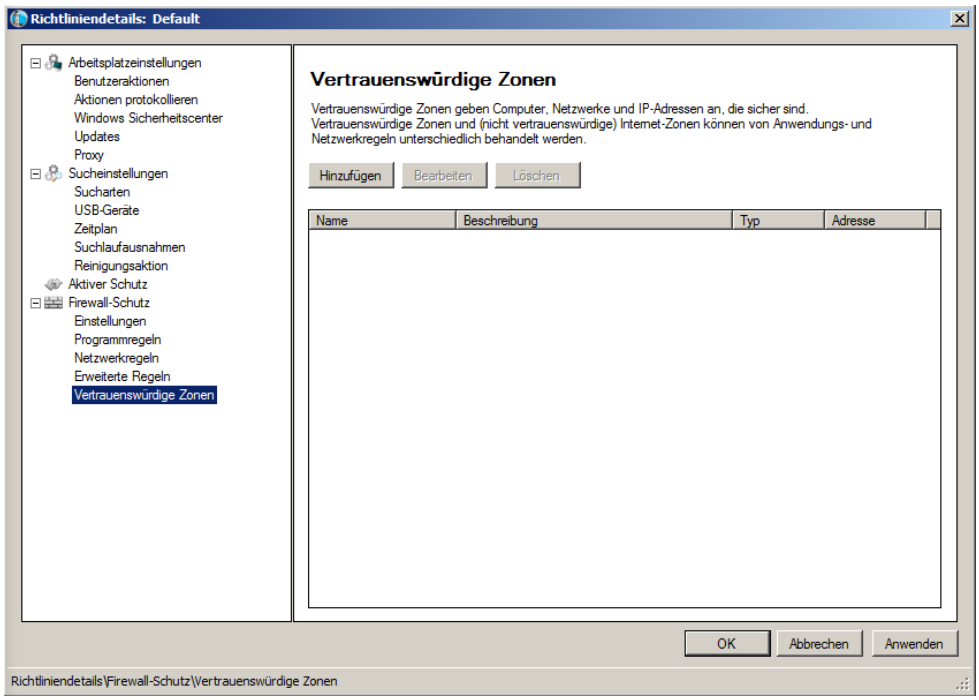
> Protokolltyp – der Typ (ICMP, IGMP, TCP, UDP) und der Name des Protokolls.

> Lokaler Port – Details des lokalen Port.

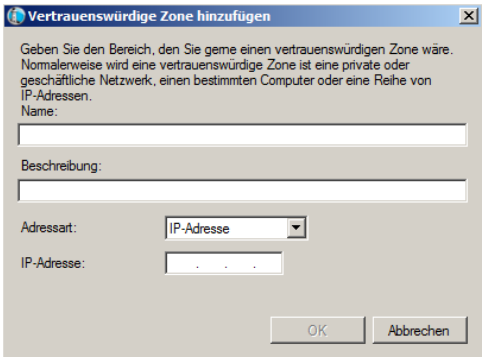
> Remote-Port – Details des Remote-Port.

- Teilfenster *Vertrauenswürdige Zonen*

  Vertrauenswürdige Zonen geben Computer, Netzwerke und IP-Adressen an, die vertrauenswürdig sind. Vertrauenswürdige Zonen und (nicht vertrauenswürdige) Internet-Zonen können von Programm- und Netzwerkregeln unterschiedlich behandelt werden.



Klicken Sie auf *Hinzufügen*, um eine neue vertrauenswürdige Zone hinzuzufügen. Geben Sie die entsprechenden Optionen ein, oder wählen Sie sie aus, und klicken Sie auf *OK*. Die folgenden Parameter werden angezeigt:



> Name – Name der vertrauenswürdigen Zone.

> Beschreibung – Beschreibung der vertrauenswürdigen Zone.

> Art – Art der vertrauten Zone (IP-Adresse, oder Netzwerk).

10. Klicken Sie auf *OK*. Die neue Richtlinie *Neue Richtlinie 1* wird unterhalb des Knotens *Anti-Virus* angezeigt.

Eine Antivirusrichtlinie anwenden

Nachdem eine Antivirusrichtlinie erstellt wurde, kann sie über die Faronics Core Console auf einen oder mehrere Arbeitsplätze angewandt werden. Führen Sie die folgenden Schritte aus, um die Richtlinie anzuwenden:

1. Wählen Sie einen oder mehrere Arbeitsplätze aus. Klicken Sie mit der rechten Maustaste, und wählen Sie *Richtlinie neu zuordnen*aus.
2. Der Dialog *Arbeitsplatz/Arbeitsplätze der Richtlinie neu zuordnen* wird angezeigt. Wählen Sie im Drop-Down-Feld *Richtlinie zuordnen* die gewünschte Richtlinie aus, und klicken Sie auf *OK*.
3. Die Richtlinie wird auf den ausgewählten Arbeitsplatz bzw. die ausgewählten Arbeitsplätze angewandt.

Eine Antivirusrichtlinie anzeigen oder ändern

Nachdem die Antivirusrichtlinie erstellt wurde, kann sie angezeigt oder geändert werden. Führen Sie die folgenden Schritte aus, um eine Richtlinie anzuzeigen oder zu ändern:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster *Baumstruktur der Konsole* auf *Faronics Core Console>[Core Server]>Verwaltete Arbeitsplätze>Anti-Virus>[Richtlinienname]*.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie *Richtliniendetails* aus.
4. Sie können die Richtlinie bearbeiten, indem Sie die Einstellungen auf den Registerkarten gemäß der Beschreibung unter Antivirusrichtlinien erstellen anpassen.
5. Klicken Sie auf *OK*, um die Änderungen anzuwenden.
6. An einer Richtlinie vorgenommene Änderungen werden automatisch auf den bzw. die über die Richtlinie verwalteten Arbeitsplatz/Arbeitsplätze angewandt.

Eine Antivirusrichtlinie umbenennen

Nachdem die Antivirusrichtlinie erstellt wurde, kann sie umbenannt werden. Führen Sie die folgenden Schritte aus, um eine Richtlinie umzubenennen:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster *Baumstruktur der Konsole* auf *Faronics Core Console>[Core Server]>Verwaltete Arbeitsplätze>Anti-Virus>[Richtlinienname]*.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie *Richtlinie umbenennen* aus. Der Dialog *Richtlinie umbenennen* wird angezeigt.
4. Geben Sie den *Neuen Richtliniennamen* ein, und klicken Sie auf *OK*.

Eine Richtlinie kopieren

Eine bestehende Richtlinie kann problemlos in eine neue Richtlinie kopiert werden. Alternativ hierzu können die Daten in einer bestehenden Richtlinie in eine andere bestehende Richtlinie kopiert werden.

Führen Sie die folgenden Schritte aus, um eine Richtlinie zu kopieren:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster *Baumstruktur der Konsole* auf *Faronics Core Console>[Core Server]>Verwaltete Arbeitsplätze>Anti-Virus>[Richtlinienname]*.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie *Richtlinie kopieren* aus. Der Dialog *Richtlinie kopieren* wird angezeigt.
4. Wählen Sie in der Drop-Down-Liste eine *Zielrichtlinie* aus, oder klicken Sie auf *Neu*, um die Daten in eine neue Richtlinie zu kopieren. Geben Sie einen Namen für die neue Richtlinie an.
5. Klicken Sie auf *Richtliniendaten jetzt kopieren*.

Die Daten werden in eine bestehende Richtlinie kopiert, bzw. es wird eine neue Richtlinie mit den in Schritt 3 ausgewählten Daten erstellt.

Eine Antivirusrichtlinie löschen

Führen Sie die folgenden Schritte aus, um eine bestehende Richtlinie zu löschen:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster *Baumstruktur der Konsole* auf *Faronics Core Console>[Core Server]>Verwaltete Arbeitsplätze>Anti-Virus>[Richtlinienname]*.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie *Richtlinie löschen* aus. Der Dialog *Richtlinie löschen* wird angezeigt.
4. Klicken Sie auf *Ja*, um die Richtlinie zu löschen.

Wenn eine Richtlinie gelöscht wird, die einem Arbeitsplatz zugeordnet ist, wird sie durch die Standardrichtlinie ersetzt. Die Standardrichtlinie kann nicht gelöscht werden.

Eine Antivirusrichtlinie importieren

Eine vorkonfigurierte Antivirusrichtlinie kann in eine bestehende Richtlinie importiert werden. Diese Funktion spart Zeit ein, da nicht die gesamte Richtlinie neu konfiguriert werden muss.

Führen Sie die folgenden Schritte aus, um eine bestehende Richtlinie zu importieren:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster *Baumstruktur der Konsole* auf *Faronics Core Console>[Core Server]>Verwaltete Arbeitsplätze>Anti-Virus>[Richtlinienname]*.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie *Richtlinie importieren* aus. Klicken Sie auf *Ja*, um die aktuellen Einstellungen der bestehenden Richtlinie zu überschreiben.
4. Klicken Sie auf Durchsuchen, um die Richtlinie, die importiert werden soll, zu suchen und auszuwählen. Es können nur Richtlinien importiert werden, die zuvor im XML-Format exportiert wurden.
5. Wählen Sie eine zuvor exportierte Richtlinie aus, und klicken Sie auf *Öffnen*. Die Richtlinie wird importiert.

Eine Antivirusrichtlinie exportieren

Eine vorkonfigurierte Antivirusrichtlinie kann zur Wiederverwendung exportiert werden. Diese Funktion spart Zeit ein, da nicht die gesamte Richtlinie neu konfiguriert werden muss.

Führen Sie die folgenden Schritte aus, um eine bestehende Richtlinie zu exportieren:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster *Baumstruktur der Konsole* auf *Faronics Core Console>[Core Server]>Verwaltete Arbeitsplätze>Anti-Virus>[Richtlinienname]*.
3. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie *Richtlinie exportieren* aus.
4. Klicken Sie auf Durchsuchen, um die Position auszuwählen.
5. Geben Sie einen Dateinamen an, und klicken Sie auf *Speichern*. Die Richtlinie wird im XML-Format exportiert.

Suchlauf über die Faronics Core Console ausführen

Ein Suchlauf kann manuell, gemäß dem Zeitplan der Antivirusrichtlinie oder durch Terminierung einer Aufgabe über die Faronics Core Console durchgeführt werden. Führen Sie die folgenden Schritte aus, um einen Arbeitplatz bzw. mehrere Arbeitsplätze über die Faronics Core Console zu durchsuchen:

1. Starten Sie die Faronics Core Console.
2. Wechseln Sie zum Teilfenster *Arbeitsplatzliste*.
3. Klicken Sie mit der rechten Maustaste auf mindestens einen Arbeitsplatz, und wählen Sie *Suchlauf* aus.
   - > Wählen Sie *Suchlauf*>*Schnell* aus, um einen Schnellsuchlauf durchzuführen.
   - > Wählen Sie *Suchlauf*>*Eingehend* aus, um einen eingehenden Suchlauf durchzuführen.
   - > Wählen Sie Jetzt reparieren aus, um die aktuellsten Virusdefinitionen herunterzuladen und einen Suchlauf durchzuführen. Wenn der aktive Schutz vom Benutzer vorrübergehend deaktiviert wurde, wird er aktiviert, sobald Jetzt reparieren ausgewählt wird.

Der Fortschritt des Suchlaufs (*% des Suchlaufs abgeschlossen*) wird im Teilfenster *Arbeitsplatzliste* in der Faronics Core Console angezeigt.

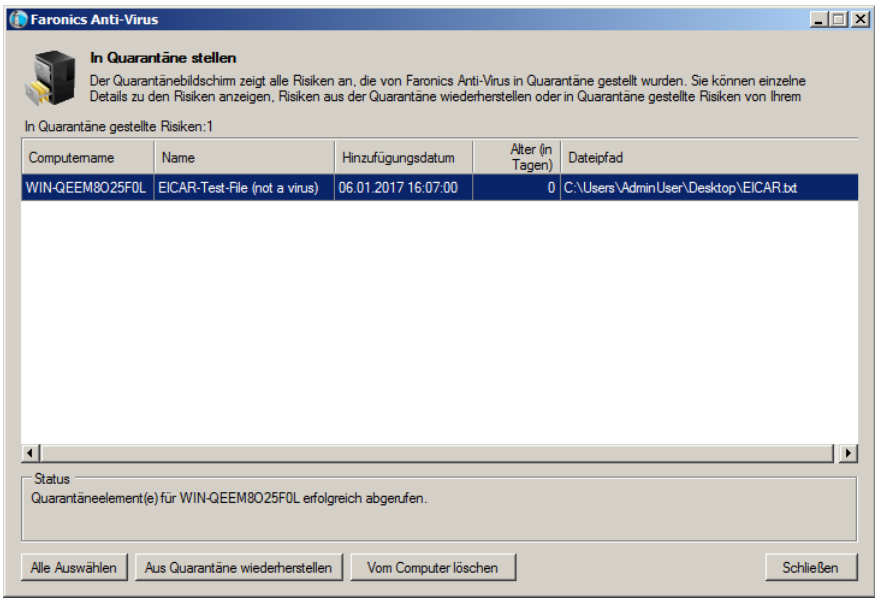
Wenn mehr als ein Loadin installiert ist, können Sie auf das Kontextmenü für Faronics Anti-Virus zugreifen, indem Sie mit der rechten Maustaste auf einen Arbeitsplatz klicken und dann zunächst *Faronics Anti-Virus* und anschließend die gewünschte Aktion auswählen.

Der aktive Schutz muss aktiviert sein, damit die Funktion Jetzt reparieren über die Faronics Core Console funktioniert.

In Quarantäne gestellte Dateien anzeigen und Aktionen für diese ausführen

Führen Sie die folgenden Schritte aus, um die von Faronics Anti-Virus in Quarantäne gestellten Dateien anzuzeigen:

1. Starten Sie die Faronics Core Console.
2. Wechseln Sie zum Teilfenster *Arbeitsplatzliste*.
3. Wählen Sie den gewünschten Arbeitsplatz aus.
4. Klicken Sie mit der rechten Maustaste auf den Arbeitsplatz, und wählen Sie *Quarantäne anzeigen* aus. Die Liste der in Quarantäne gestellten Dateien wird angezeigt.



5. Die folgenden Informationen zu den einzelnen infizierten Dateien werden angezeigt:
   - > Risikoname
   - > Dateiname
   - > Ursprüngliche Position
   - > Hinzufügungsdatum
   - > Alter (in Tagen)
6. Wählen Sie die folgenden Aktionen aus:
   - > Details – Wählen Sie eine Datei aus, und klicken Sie auf Details, um die Details der infizierten Datei anzuzeigen. Hierdurch wird außerdem die empfohlene Aktion angezeigt.
   - > Alle auswählen – Wählt alle Dateien aus.
   - > Von Computer löschen – Löscht die ausgewählte Datei vom Computer.
   - > Aus Quarantäne wiederherstellen – Stellt die ausgewählte Datei auf dem Computer wieder her.
   - > Schließen – Schließt den Dialog.

Faronics Anti-Virus über die Faronics Core Console aktualisieren

Die Faronics Anti-Virus-Definitionen können über die Faronics Core Console auf den Arbeitsplätzen aktualisiert werden. Faronics Core fungiert als Anti-Virus-Update-Repository für die verwalteten Arbeitsplätze. Die Anti-Virus-Updates werden von Faronics Core automatisch an Remote-Arbeitsplätze gesandt. Darüber hinaus kann der Faronics Core-Administrator die Virusdefinitionen wie nachfolgend beschrieben manuell aktualisieren.

Führen Sie die folgenden Schritte aus, um Faronics Anti-Virus auf dem Arbeitsplatz bzw. den Arbeitsplätzen zu aktualisieren:

1. Starten Sie die Faronics Core Console.
2. Wechseln Sie zum Teilfenster *Arbeitsplatzliste*.
3. Klicken Sie mit der rechten Maustaste auf mindestens einen Arbeitsplatz, und wählen Sie *Update* aus.
   > Wählen Sie *Update>Vollständiges Update* aus – Hierdurch werden die Anti-Virus-Definitionen aktualisiert.
   > Wählen Sie *Update>Vollständiges Update erzwingen* – Hierdurch werden die bestehenden Anti-Virus-Definitionen gelöscht und durch die neuesten Anti-Virus-Definitionen ersetzt.

Faronics Anti-Virus-Aktionen über die Faronics Core Console terminieren

Ereignisse in Faronics Anti-Virus und der Faronics Core Console können so terminiert werden, dass sie auf einem Arbeitsplatz bzw. auf mehreren Arbeitsplätzen zu einem Datum und einer Uhrzeit auftreten, die für den Administrator günstig sind. Klicken Sie auf mindestens einen Arbeitsplatz, und wählen Sie *Aktion terminieren* aus. Die daraufhin angezeigten Untermenüs enthalten die folgende Liste verfügbarer Aktionen:

Über die Faronics Core Console kontrollierte Aktionen:

- Herunterfahren
- Neu starten
- Aufwecken

Über Faronics Anti-Virus kontrollierte Aktionen

- Aktiver Schutz>aktivieren
- Aktiver Schutz>deaktivieren
- Suchlauf>Schnell
- Suchlauf>Eingehend
- Update>Vollständiges Update
- Update>Vollständiges Update erzwingen
- Jetzt reparieren
- Anti-Virus Client installieren/Upgrade durchführen
- Anti-Virus Client deinstallieren

Bei Auswahl einer Aktion wird ein Menü *Zeitplan* angezeigt, über das der Administrator die Häufigkeit (einmalig, täglich, wöchentlich oder monatlich) angeben kann. Auf Basis der Häufigkeit können Sie die entsprechende Uhrzeit bzw. den Wochentag, das Datum oder den gewünschten Monat auswählen.

Eine über eine Anti-Virus-Richtlinie eingerichtete Task hat immer Vorrang vor Aktionen, die über die Faronics Core Console eingerichtet wurden.

Berichte generieren

Faronics Anti-Virus bietet zahlreiche Berichte, um die Aktivitäten auf den einzelnen Arbeitsplätzen zu überwachen. Es gibt zwei Berichtskategorien:

- Globale Berichte – Diese Berichte beruhen auf allen Arbeitsplätzen, die über Faronics Anti-Virus geschützt werden.
- Arbeitsplatzspezifische Berichte – Diese Berichte sind für den ausgewählten Arbeitsplatz spezifisch.

Globale Berichte

Führen Sie die folgenden Schritte aus, um einen globalen Bericht zu erstellen:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster *Baumstruktur der Konsole* auf *Faronics Core Console>[Core Server]>Verwaltete Arbeitsplätze>Anti-Virus*.
3. Klicken Sie im Teilfenster *Aktion* auf *Globale Berichte*.
4. Wählen Sie einen Bericht aus, und geben Sie im Dialog, der angezeigt wird, einen Zeitraum ein. Klicken Sie auf *OK*. Die folgenden Berichte sind verfügbar:
   > Bedrohungen nach Anzahl der erkannten Fälle – Die erkannten Bedrohungen nach Anzahl der erkannten Fälle auf allen Arbeitsplätzen, die von Faronics Anti-Virus verwaltet werden, werden angezeigt.
   > Zusammenfassung des Schweregrads der Bedrohungen – Die Zusammenfassung des Schweregrads der Bedrohungen wird angezeigt.
   > Die 25 am stärksten infizierten Rechner – Die 25 am stärksten infizierten Rechner werden angezeigt.

Der ausgewählte Bericht wird im Teilfenster *Baumstruktur der Konsole* unter dem Knoten *Berichte* angezeigt.

Arbeitsplatzspezifische Berichte

Führen Sie die folgenden Schritte aus, um einen arbeitsplatzspezifischen Bericht zu erstellen:

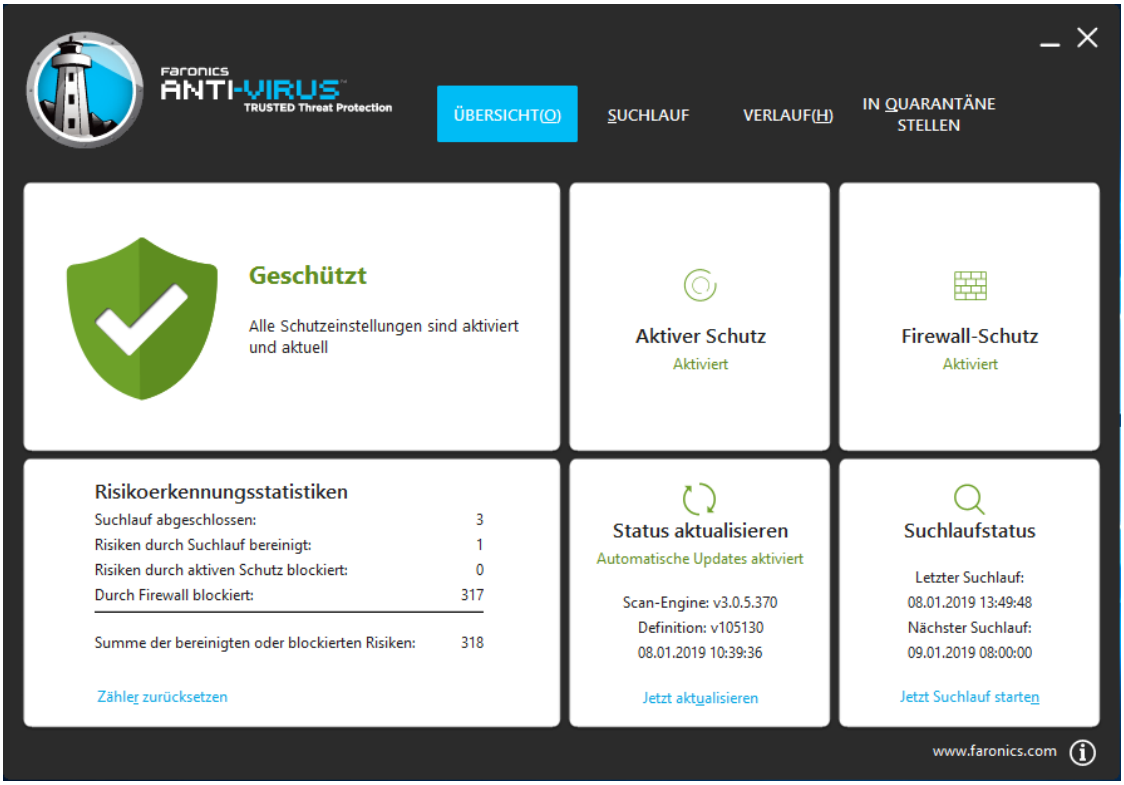
1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster *Baumstruktur der Konsole* auf *Faronics Core Console>[Core Server]>Verwaltete Arbeitsplätze*.
3. Wählen Sie den Arbeitsplatz aus, für den der Bericht erstellt werden soll.
4. Klicken Sie mit der rechten Maustaste auf den Arbeitsplatz, und wählen Sie *Berichte* aus.
5. Wählen Sie einen Bericht aus, und geben Sie im Dialog, der angezeigt wird, einen Zeitraum ein. Klicken Sie auf *OK*. Die folgenden Berichte sind verfügbar:
   > Arbeitsplatzdetails
   > Letzter Suchlauf
   > Suchverlauf
   > Verlauf des aktiven Schutzes
   > Quarantäne
   > E-Mail-Schutz – Verlauf
   > Systemereignismeldungen
6. Der ausgewählte Bericht wird im Teilfenster *Baumstruktur der Konsole* unter dem Knoten *Berichte* angezeigt.

Faronics Anti-Virus auf dem Arbeitsplatz verwenden

Die über Faronics Anti-Virus auf dem Arbeitsplatz verfügbaren Funktionen hängen voll und ganz von den in der Antivirusrichtlinie ausgewählten Einstellungen ab. Weitere Informationen über Antivirusrichtlinien finden Sie unter Faronics Anti-Virus-Richtlinie.

Faronics Anti-Virus auf dem Arbeitsplatz starten

Gehen Sie auf *Start>Programme>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Alternativ hierzu können Sie auch doppelt auf das Faronics Anti-Virus-Symbol in der Tastleiste klicken.



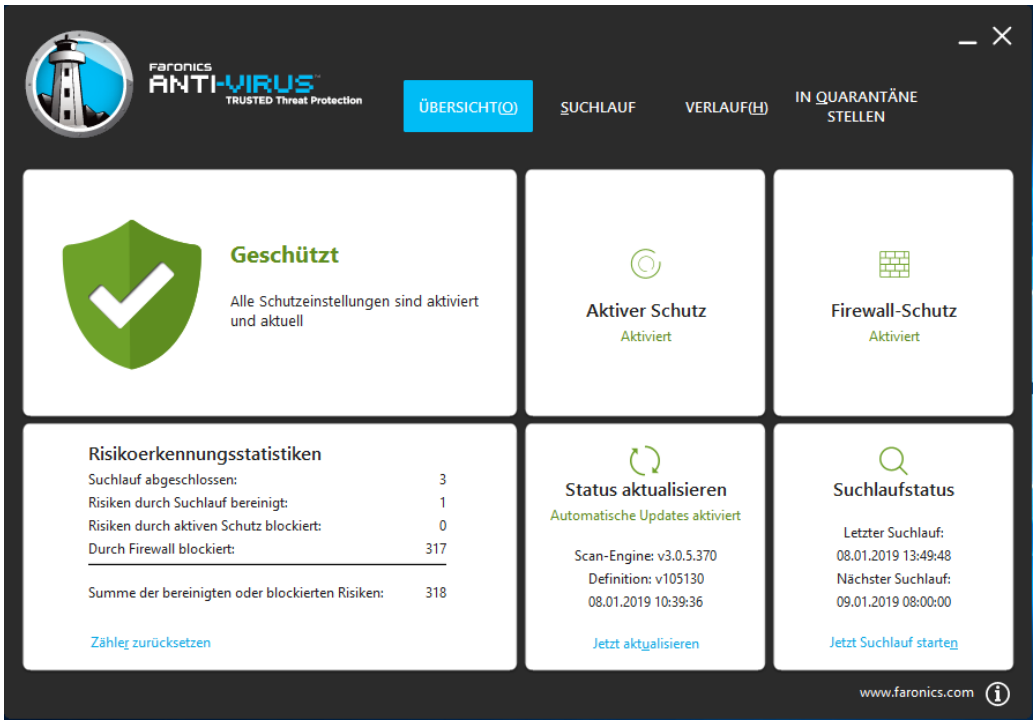
Die folgenden Teilfenster zeigen dem Benutzer wichtige Informationen an.

- *Geschützt* oder *Nicht geschützt* wird angezeigt, um anzugeben, ob der Computer geschützt ist oder nicht. Wenn „Nicht geschützt" angezeigt wird, klicken Sie auf die Schaltfläche *Jetzt reparieren* unter der Anzeige *Nicht geschützt*.
- *Suchlaufstatus* zeigt an, wann der letzte Suchlauf durchgeführt wurde. Sie können sofort einen Suchlauf durchführen, indem Sie auf den Link *Jetzt Suchlauf starten* klicken.
- *Update-Status* zeigt an, wann das letzte Update durchgeführt wurde. Sie können die Virusdefinitionen aktualisieren, indem Sie auf den Link *Jetzt alle aktualisieren* klicken.
- *Aktiver Schutz* zeigt an, ob der Echtzeitschutz aktiviert ist.
- Der Firewall-Schutz wird angezeigt, wenn der Arbeitsplatz durch die Firewall geschützt ist.
- *Risikoerkennungsstatistiken* zeigt die Statistiken für die von Faronics Anti-Virus ergriffenen Maßnahmen an. Klicken Sie auf *Zähler zurücksetzen*, um die Zähler auf null zurückzusetzen.

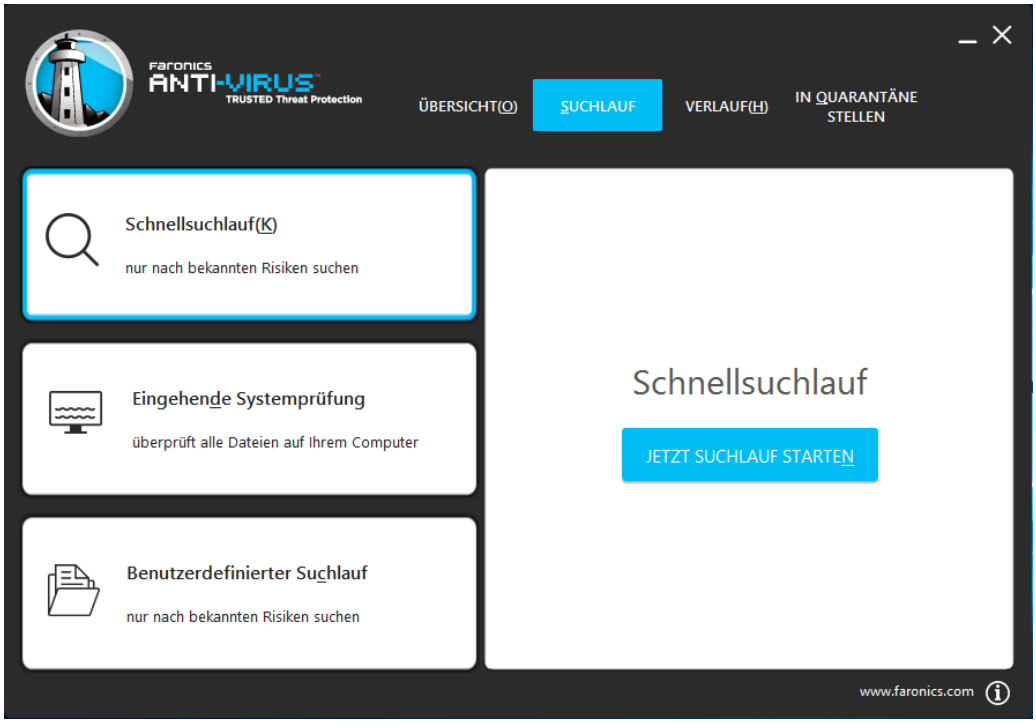
Den Arbeitsplatz durchsuchen

Führen Sie die folgenden Schritte aus, um einen Arbeitsplatz zu durchsuchen:

1. Gehen Sie auf *Start>Programme>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Alternativ hierzu können Sie auch doppelt auf das Faronics Anti-Virus-Symbol in der Tastleiste klicken.



2. Klicken Sie im Teilfenster *Suchlaufstatus* auf *Jetzt Suchlauf starten*. Die Registerkarte *Suchlauf* wird angezeigt. Alternativ hierzu können Sie auch auf die Registerkarte *Suchlauf* klicken.



3. Wählen Sie eine der folgenden Optionen aus:
   > Schnellsuchlauf – Sucht nur nach bekannten Bedrohungen.
   > Eingehende Systemdurchsuchung – Ein detaillierter Suchlauf aller Dateien auf dem Arbeitsplatz.
   > Benutzerdefinierter Suchlauf (Wählen Sie eine der folgenden Optionen aus):
      ~ Laufende Prozesse durchsuchen – Durchsucht die auf dem Arbeitsplatz laufenden Prozesse.
      ~ Registrierung durchsuchen – Durchsucht die Registrierungsdatenbank.
      ~ Cookies durchsuchen – Durchsucht die auf dem Arbeitsplatz gespeicherten Cookies.
      ~ Geben Sie Laufwerke und Ordner an, die *durchsucht werden sollen*: Klicken Sie auf *Durchsuchen*, um die Ordner auszuwählen.
4. Klicken Sie auf *Jetzt Suchlauf starten*. Das sich drehende Symbol weist darauf hin, dass derzeit ein Suchlauf durchgeführt wird. Nach Beendigung des Suchlaufs werden die Suchlaufergebnisse angezeigt.
5. Wenn Sie eine Datei auswählen, stehen die folgenden Optionen zur Verfügung:
   > Wählen Sie *Reinigungsmaßnahme ändern>Empfohlene Maßnahme* aus, um die von Faronics Anti-Virus empfohlenen Maßnahmen umzusetzen.
   > Wählen Sie *Reinigungsmaßnahme ändern>In Quarantäne stellen/Desinfizieren* aus, um die Datei in Quarantäne zu stellen oder zu desinfizieren.
   > Wählen Sie *Reinigungsmaßnahme ändern>Löschen* aus, um die Datei zu löschen.
   > Wählen Sie *Reinigungsmaßnahme ändern>Zulassen* aus, um die Datei zuzulassen.
   > Klicken Sie auf *Alle auswählen,* um alle in den *Suchlaufergebnissen* angezeigten Dateien auszuwählen.
   > Klicken Sie auf *Details*, um die Details des Risikos anzuzeigen.
   > Klicken Sie auf *Abbrechen*, um den Dialog zu schließen, ohne Maßnahmen durchzuführen.
   > Klicken Sie auf *Bereinigen*, um die Datei zu entfernen und den Dialog zu schließen.

Die Maßnahmen können auch über die Faronics Core Console ergriffen werden. Weitere Informationen hierzu finden Sie unter In Quarantäne gestellte Dateien anzeigen und Aktionen für diese ausführen.

Eine Datei bzw. einen Ordner per Rechtsklick durchsuchen

Dateien oder Ordner (einzelne oder mehrere) können leicht auf Viren untersucht werden. Wenn Faronics Anti-Virus auf einem Arbeitsplatz installiert ist, wird die Option „Nach Viren durchsuchen“ zum Rechtsklickmenü hinzugefügt.

Führen Sie die folgenden Schritte aus, um eine Datei oder einen Ordner auf dem Computer zu durchsuchen:

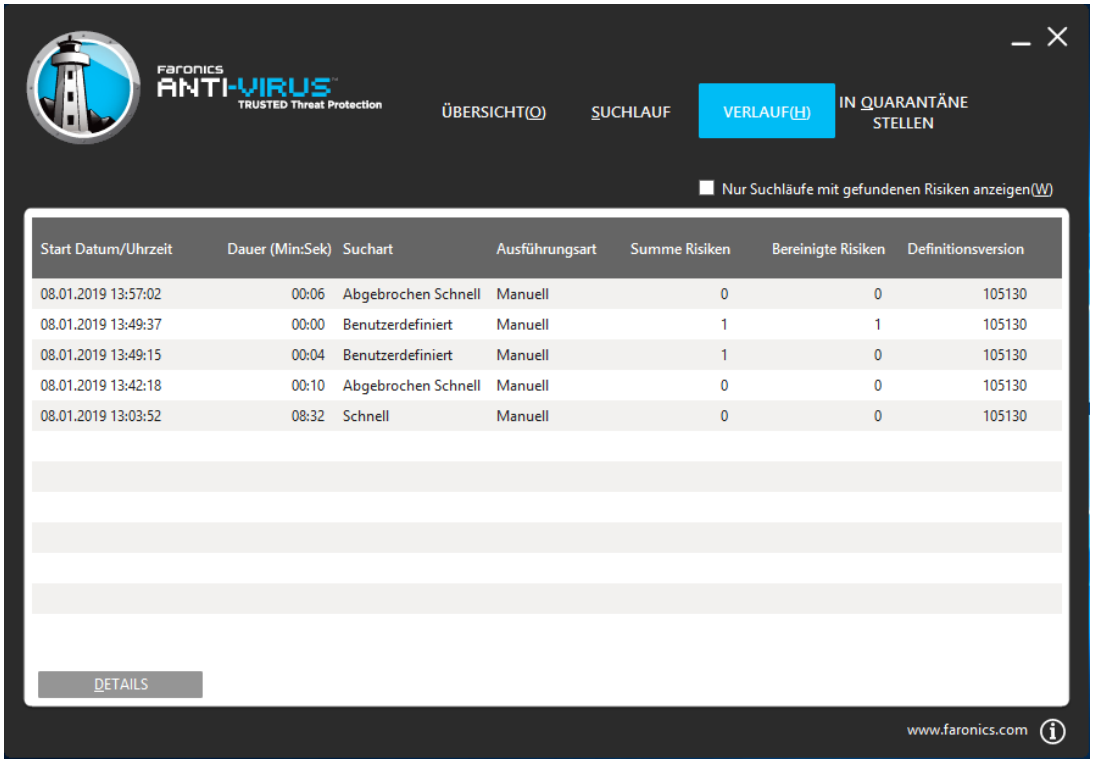
1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner.
2. Wählen Sie *Nach Viren durchsuchen* aus.

Der Suchlauf wird durchgeführt, und die Ergebnisse werden angezeigt.

Suchverlauf anzeigen

Führen Sie die folgenden Schritte aus, um den Suchverlauf anzuzeigen:

1. Gehen Sie auf *Start*>*Programme*>*Faronics*>*Anti-Virus Enterprise*>*Faronics Anti-Virus Enterprise*. Alternativ hierzu können Sie auch doppelt auf das Faronics Anti-Virus-Symbol in der Tastleiste klicken.
2. Klicken Sie auf die Registerkarte *Verlauf*.

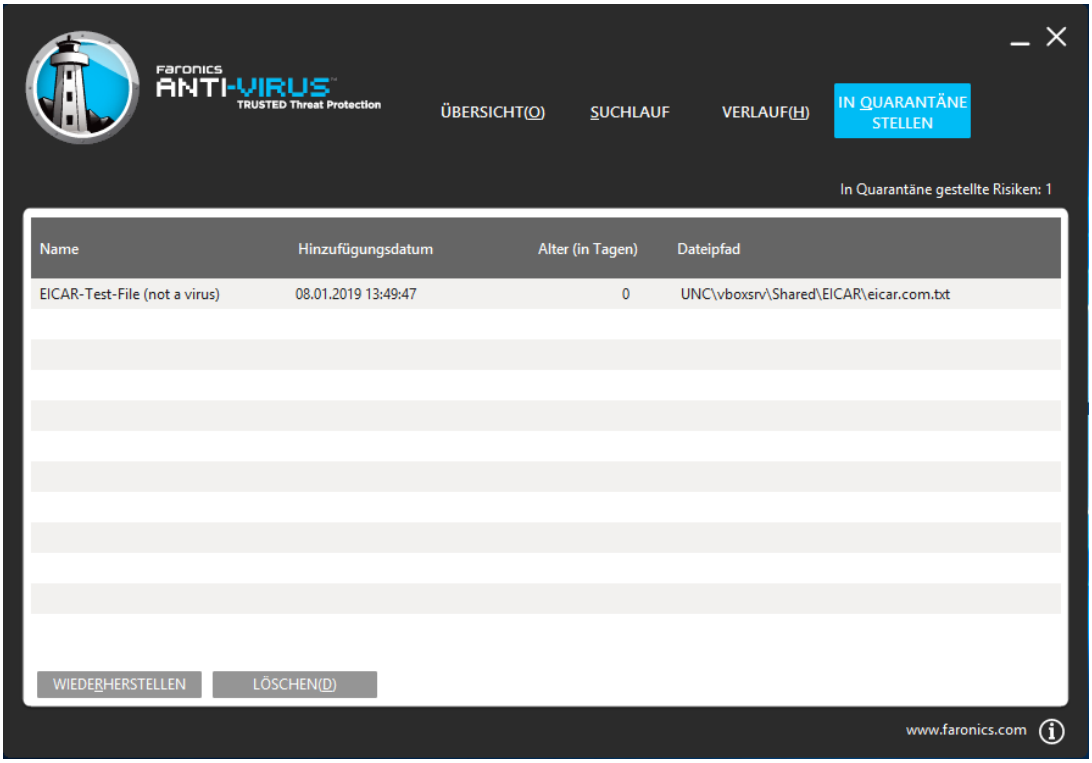


3. Wählen Sie die folgenden Aktionen aus:
   > Nur Suchläufe mit gefundenen Risiken anzeigen – Wählen Sie diese Option aus, um die diejenigen Suchläufe anzuzeigen, bei denen Risiken erkannt wurden.
   > Details – Wählen Sie einen Eintrag aus, und klicken Sie auf "Details", um detaillierte Informationen zum Suchlauf anzuzeigen.

In Quarantäne gestellte Dateien anzeigen und Aktionen für diese ausführen

Führen Sie die folgenden Schritte aus, um die Quarantäne anzuzeigen:

1. Gehen Sie auf *Start>Programme>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Alternativ hierzu können Sie auch doppelt auf das Faronics Anti-Virus-Symbol in der Tastleiste klicken.
2. Klicken Sie auf die Registerkarte *Quarantäne*.

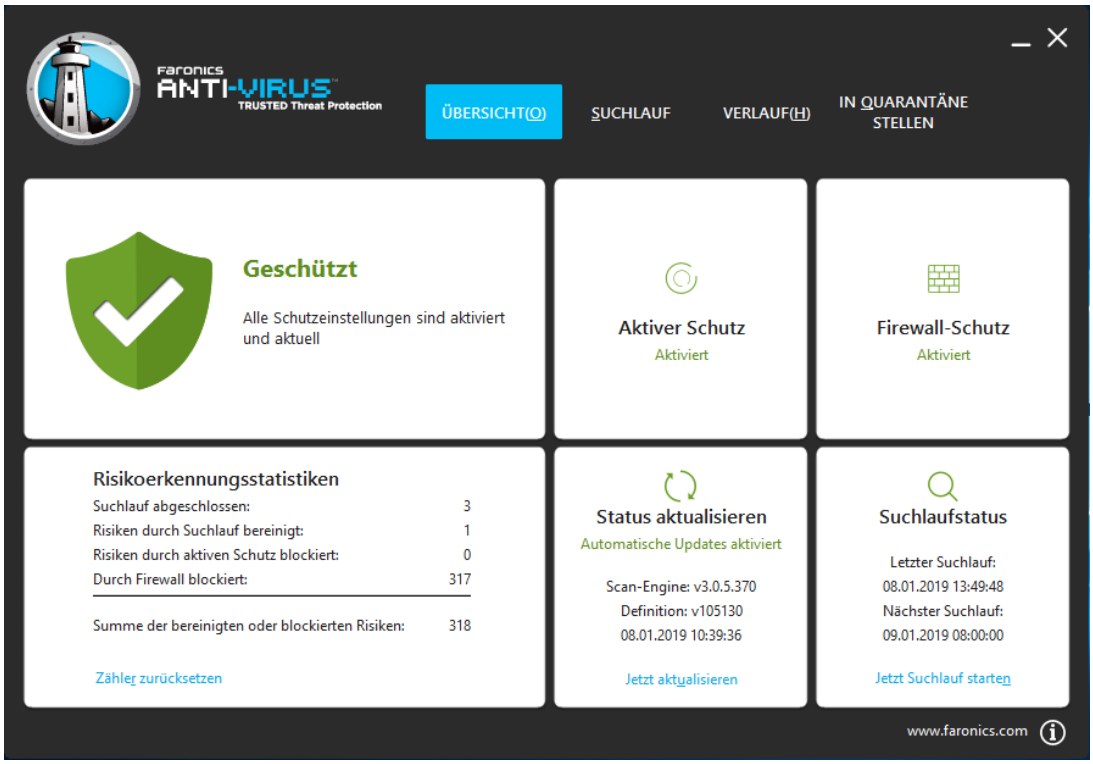


3. Klicken Sie auf *Risikodetails*. Die folgenden Informationen zu den einzelnen infizierten Dateien werden angezeigt:
   - > Name
   - > Risikokategorie
   - > Hinzufügungsdatum
   - > Alter (in Tagen)
   - > In Quarantäne gestellt von

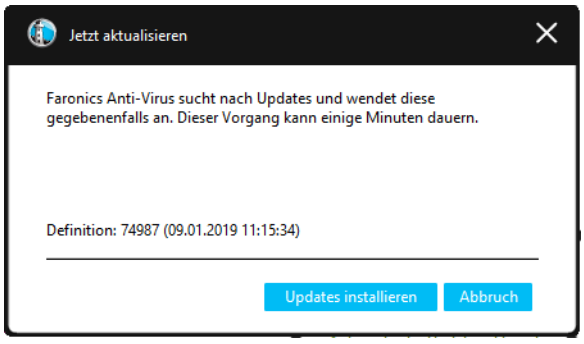
Antivirus-Definitionen auf dem Arbeitsplatz aktualisieren

Führen Sie die folgenden Schritte aus, um Anti-Virus-Definitionen auf dem Arbeitsplatz bzw. den Arbeitsplätzen zu aktualisieren:

1. Gehen Sie auf *Start>Programme>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Alternativ hierzu können Sie auch doppelt auf das Faronics Anti-Virus-Symbol in der Tastleiste klicken.



2. Klicken Sie im Teilfenster *Update-Status* auf *Jetzt aktualisieren*. Der Dialog *Jetzt aktualisieren* wird angezeigt.



3. Klicken Sie auf *Updates installieren*. Die Virusdefinitionen werden auf dem Arbeitsplatz aktualisiert.

Faronics Anti-Virus über die Taskleiste auf dem Arbeitsplatz verwalten

Faronics Anti-Virus kann auf dem Arbeitsplatz über ein Menü verwaltet wird, das in der Taskleiste angeboten wird.

Klicken Sie mit der rechten Maustaste auf das Faronics Anti-Virus-Symbol in der Tastleiste. Die folgenden Optionen sind verfügbar:

- Faronics Anti-Virus öffnen – Startet Faronics Anti-Virus auf dem Arbeitsplatz.
- Aktiver Schutz
  - > *Aktiver Schutz>Aktiven Schutz aktivieren* – aktiviert den aktiven Schutz.
  - > *Aktiver Schutz>Aktiven Schutz deaktivieren> [Option auswählen]* – Wählen Sie aus, wie lange der aktive Schutz deaktiviert werden soll. Wählen Sie 5 Minuten, 15 Minuten, 30 Minuten, 1 Stunde, Bis zum Neustart oder Dauerhaft aus. Diese Option wird nur angezeigt, wenn sie in der Antivirenrichtlinie ausgewählt wurde.
- *Jetzt Suchlauf starten>[Option auswählen]* – Wählen Sie Suchlauf abbrechen, Suchlauf anhalten, Suchlauf fortsetzen, Schnellsuchlauf oder Eingehender Suchlauf aus. Diese Option wird nur angezeigt, wenn sie in der Antivirenrichtlinie ausgewählt wurde.
- *Firewall-Schutz>Aktivieren* oder *Deaktivieren*.

Die voranstehenden Optionen stehen dem Benutzer nur dann zur Verfügung, wenn dies in der Antivirusrichtlinie vorgegeben wurde. Weitere Informationen hierzu finden Sie unter Antivirusrichtlinien erstellen.

Befehlszeilensteuerung

Dieses Kapitel erläutert die verschiedenen Befehlszeilensteuerungen, die für Faronics Anti-Virus verfügbar sind.

Themen

Befehlszeilensteuerung

Die Faronics Anti-Virus-Befehlszeilensteuerung bietet Netzwerkadministratoren zusätzliche Flexibilität bei der Verwaltung von Faronics Anti-Virus-Arbeitsplätzen, indem sie eine Steuerung über Management-Tools und/oder zentrale Management-Lösungen von Drittanbietern ermöglicht.

Führen Sie die folgenden Schritte aus, um die Befehle für Faronics Anti-Virus auszuführen:

1. Gehen Sie auf dem Arbeitsplatz über die Eingabeaufforderung zu *<Systemverzeichnis>:\Programme\Faronics\Faronics Anti-Virus Enterprise*
2. Geben Sie `AVECLI/[Befehl]` ein].

Die folgenden Befehle stehen zur Verfügung:

Befehl	Definition
`definitionversion`	Zeigt die Version der Virusdefinition an.
`scanengineversion`	Zeigt die Version der Scan Engine an.
`updatedefs`	Aktualisiert Virusdefinitionen und wendet diese an.
`scanquick`	Startet einen Schnellsuchlauf.
`scandeep`	Startet einen eingehenden Suchlauf.
`fixnow`	Lädt die aktuellste Virusdefinition herunter. Aktiviert den aktiven Schutz sowie E-Mail-Schutz. Führt den standardmäßigen eingehenden Suchlauf durch.
`setlicense[Schlüssel]`	Wendet einen angegebenen Lizenzschlüssel an.
`enableap`	Aktiviert den aktiven Schutz.
`fixnow /quick`	Führt gegebenenfalls einen Schnellsuchlauf durch.

Syntax:

```
AVECLI/definitionversion
```

Faronics Anti-Virus deinstallieren

Dieses Kapitel beschreibt die Deinstallation von Faronics Anti-Virus.

Themen

Deinstallation – Übersicht

Das Faronics Anti-Virus-Loadin wird auf dem System der Faronics Core Console (bzw. des Faronics Core Servers) installiert. Der Faronics Anti-Virus-Client wird auf Arbeitsplätzen installiert.

Deinstallieren Sie den Faronics Anti-Virus-Client manuell auf dem Arbeitsplatz oder über die Faronics Core Console. Deinstallieren Sie anschließend das Faronics Anti-Virus-Loadin wird auf dem System der Faronics Core Console (bzw. des Faronics Core Servers).

Das Deinstallationsverfahren wird in den nächsten Abschnitten erläutert.

Den Faronics Anti-Virus-Client über die Faronics Core Console deinstallieren

Führen Sie die folgenden Schritte aus, um den Faronics Anti-Virus-Client über die Faronics Core Console zu deinstallieren:

1. Starten Sie die Faronics Core Console.
2. Gehen Sie im Teilfenster *Baumstruktur der Konsole* auf *Faronics Core Console>[Core Server]>Verwaltete Arbeitsplätze*.
3. Wählen Sie den Arbeitsplatz bzw. die Arbeitsplätze aus, auf denen der Faronics Anti-Virus-Client deinstalliert werden soll.
4. Klicken Sie mit der rechten Maustaste, und wählen Sie *Arbeitsplätze konfigurieren>Erweitert>Anti-Virus-Client deinstallieren* aus.

Der Faronics Anti-Virus-Client wird auf dem Arbeitsplatz bzw. den Arbeitsplätzen deinstalliert.

Den Faronics Anti-Virus-Client über Programme Hinzufügen oder Entfernen auf dem Arbeitsplatz deinstallieren

Führen Sie die folgenden Schritte aus, um Faronics Anti-Virus unter Windows über *Programme Hinzufügen oder Entfernen* zu deinstallieren:

1. Klicken Sie auf *Start*>*Systemsteuerung*>*Software*.
2. Wählen Sie *Faronics Anti-Virus Enterprise Workstation* aus.
3. Klicken Sie auf *Entfernen*.

Der Faronics Anti-Virus-Client wird auf dem Arbeitsplatz deinstalliert.

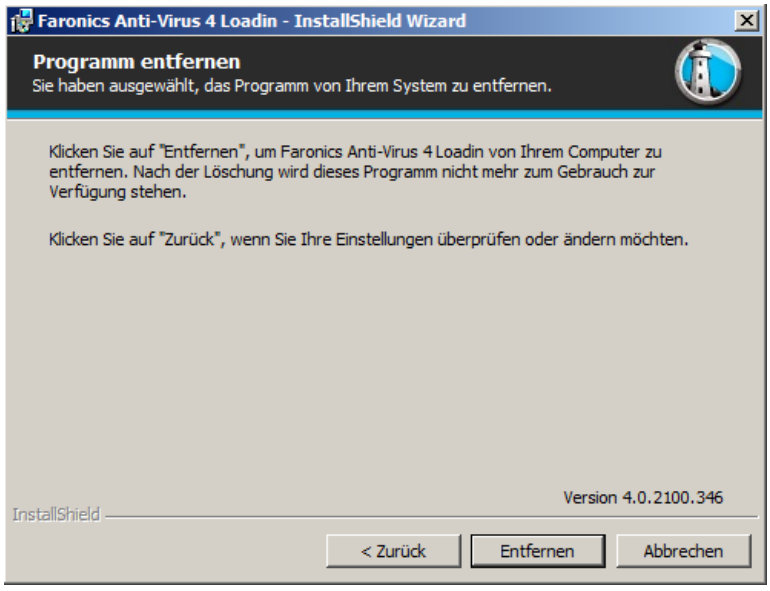
Das Faronics Anti-Virus-Loadin über das Installationsprogramm deinstallieren

Führen Sie die folgenden Schritte aus, um das Faronics Anti-Virus-Loadin zu deinstallieren:

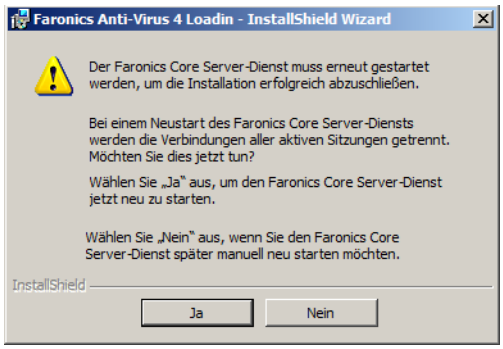
1. Klicken Sie doppelt auf *Anti-VirusLoadinInstaller.exe*. Klicken Sie auf *Weiter*.

2. Wählen Sie *Entfernen* aus. Klicken Sie auf *Weiter*.

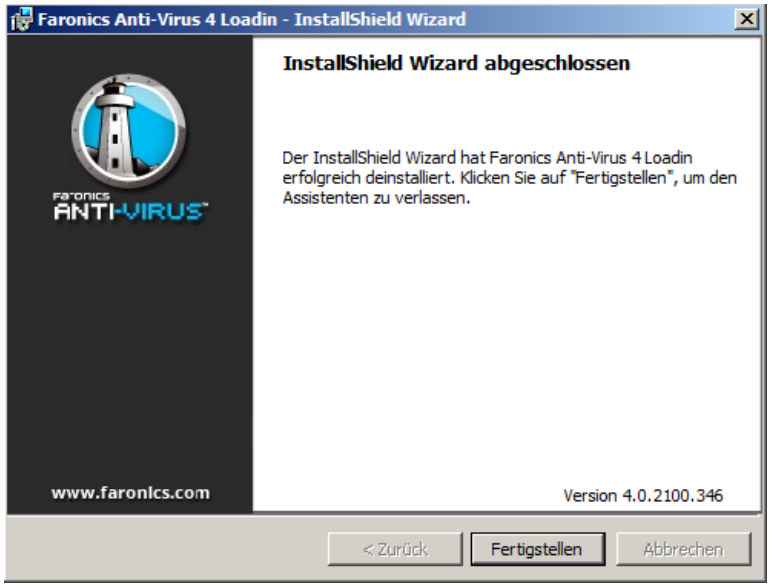
3. Klicken Sie auf *Entfernen*.



4. Die folgende Meldung wird angezeigt. Klicken Sie auf *Ja*, um den *Faronics Core Server*-Dienst neu zu starten, oder auf *Nein*, um den *Faronics Core Server*-Dienst zu einem späteren Zeitpunkt manuell neu zu starten.



5. Das Faronics Anti-Virus-Loadin wird von Ihrem Computer entfernt. Klicken Sie auf *Fertigstellen*, um die Deinstallation abzuschließen.



Das Faronics Anti-Virus-Loadin über „Programme hinzufügen oder entfernen“ deinstallieren

Führen Sie die folgenden Schritte aus, um das Faronics Anti-Virus-Loadin unter Windows über *Programme Hinzufügen oder Entfernen* zu deinstallieren:

1. Klicken Sie auf *Start*>*Systemsteuerung*>*Software*.
2. Wählen Sie *Faronics Anti-Virus-Loadin* aus.
3. Klicken Sie auf *Entfernen*.