GFI-Produkthandbuch

GFI EndPointSecurity™

Erste Schritte

Dokumentenversion: 1.1.1

Zuletzt aktualisiert (Monat/Tag/Jahr): 1/29/2014

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

Durch die zunehmende Verbreitung von Verbrauchergeräten wie iPods, USB-Geräten und Smartphones erhöhte sich das Risiko bewusster und unbeabsichtigter Datenlecks und anderer illegaler Aktivitäten erheblich. Für einen Mitarbeiter ist es sehr einfach, große Mengen vertraulicher Daten auf einen iPod oder USB-Stick zu kopieren oder bösartige bzw. illegale Software über diese Geräte ins Netzwerk einzuschleusen. Mit GFI EndPointSecurity können Sie diese Bedrohungen schnell und einfach bekämpfen, ohne dass Sie alle Anschlüsse sperren müssen.

Themen in diesem Kapitel

1.1 Informationen zu GFI EndPointSecurity

In GFI EndPointSecurity können Administratoren aktiv den Benutzerzugriff verwalten und Aktivitäten protokollieren in Verbindung mit:

» MP3-Playern, einschließlich iPod, Creative Zen usw.

» USB-Laufwerken, CompactFlash, Speicherkarten, CDs, Disketten und anderen tragbaren Speichermedien

» iPhone, BlackBerry und Android-Handhelds, Mobiltelefonen, Smartphones und ähnlichen Kommunikationsgeräten

» Netzwerkkarten, Laptops und anderen Netzwerkverbindungen.

Funktionsweise von GFI EndPointSecurity – Bereitstellung und Überwachung

Die Bereitstellung von Schutzrichtlinien und die Überwachung durch GFI EndPointSecurity erfolgt in den folgenden vier Phasen:

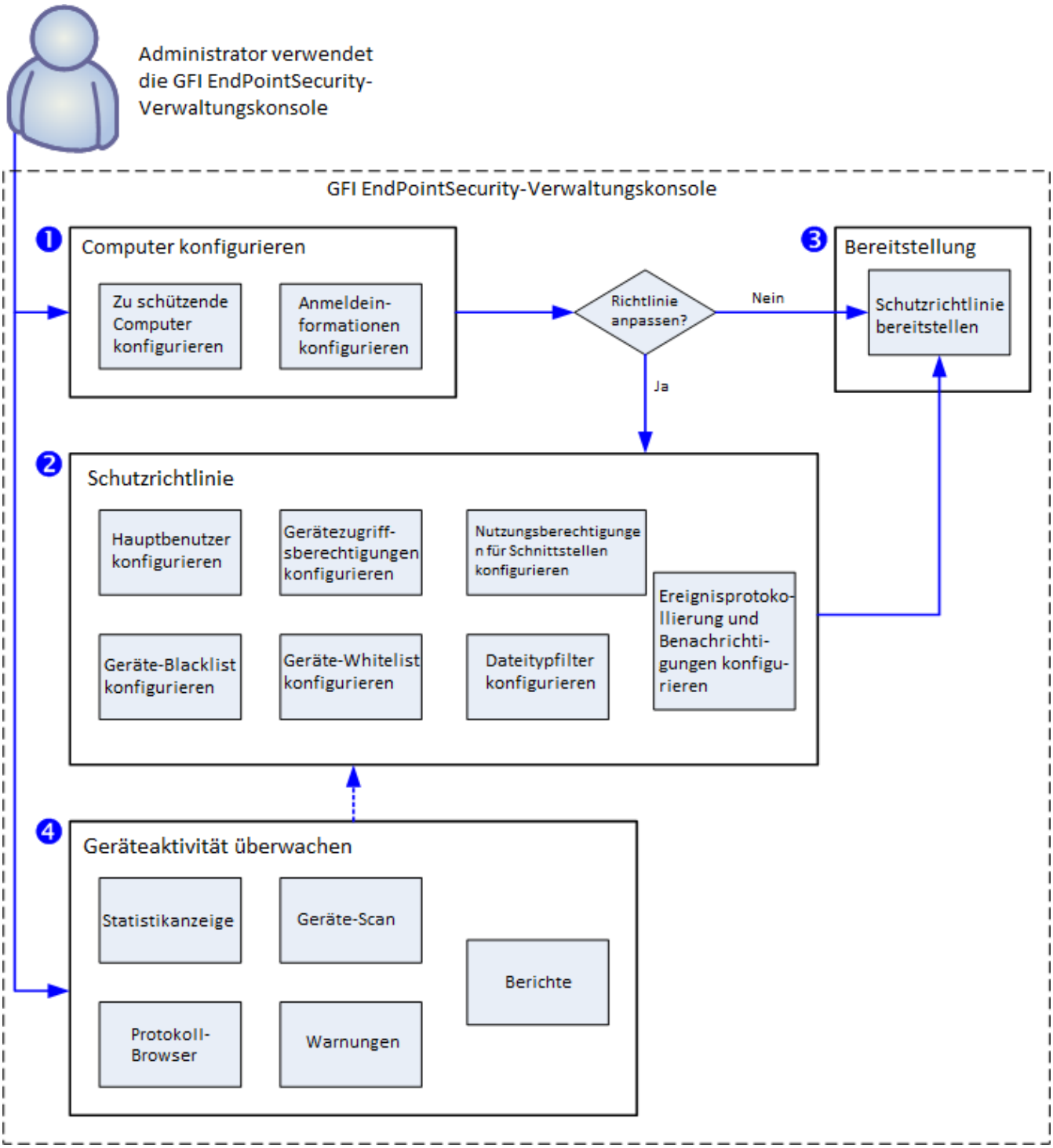


Abbildung 1: Schutzrichtlinie - Bereitstellung und Überwachung

In der folgenden Tabelle werden die oben abgebildeten Phasen beschrieben.

Tabelle 1: Bereitstellung und Überwachung einer Schutzrichtlinie

Phase	Beschreibung
Phase 1 - Konfigurieren von Computern	Der Administrator muss festlegen, welche Schutzrichtlinie welchen Computern zugewiesen wird. Zudem sind die von GFI EndPointSecurity zu verwendenden Anmeldeinformationen anzugeben, die für den Zugriff auf zu kontrollierende Computer und die Bereitstellung des Agenten erforderlich sind.
Phase 2 - Anpassen von Schutzrichtlinien	Vor oder nach der Bereitstellung einer Schutzrichtlinie kann diese vom Administrator angepasst werden. Beispielsweise können Hauptbenutzer angegeben, Geräte auf die Blacklist/Whitelist gesetzt und Zugriffsberechtigungen für Geräte definiert werden.

Phase	Beschreibung
Phase 3 - Bereitstellen von Schutzrichtlinien	Der Administrator stellt die Schutzrichtlinie bereit. Bei der ersten Bereitstellung einer Schutzrichtlinie wird automatisch ein GFI EndPointSecurity-Agent auf dem zu kontrollierenden Netzwerkcomputer installiert. Bei weiteren Bereitstellungen der gleichen Schutzrichtlinie wird der Agent aktualisiert, nicht neu installiert.
Phase 4 - Überwachen des Gerätezugriffs	Ist der Agent auf den zu kontrollierenden Computern bereitgestellt, kann der Administrator alle Zugriffsversuche auf Geräte über die Verwaltungskonsole überwachen sowie über GFI EndPointSecurity GFI ReportPack Warnungen empfangen und Berichte generieren.

Funktionsweise von GFI EndPointSecurity - Gerätezugriff

Der mit GFI EndPointSecurity kontrollierte und gesteuerte Gerätezugriff erfolgt in drei Phasen:

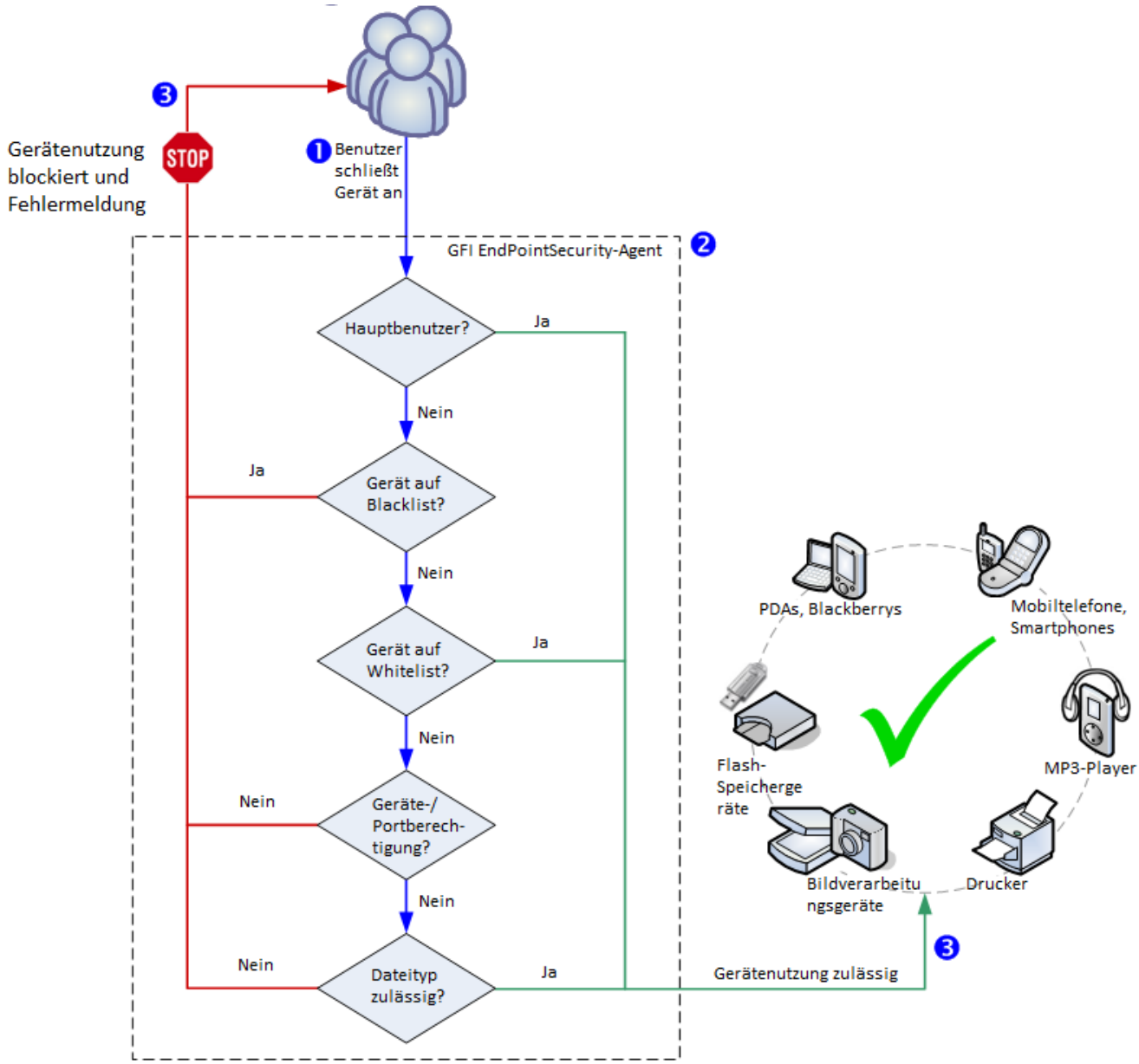


Abbildung 2: Gerätezugriff

In der folgenden Tabelle werden die oben abgebildeten Phasen beschrieben.

Tabelle 2: Bereitstellung und Überwachung einer Schutzrichtlinie

Phase	Beschreibung
Phase 1 - Anschließen eines Geräts an einen Computer	Ein Benutzer schließt ein Gerät an einen durch GFI EndPointSecurity kontrollierten Computer an.
Phase 2 - Durchsetzen von Schutzrichtlinien	Der auf dem kontrollierten Computer installierte GFI EndPointSecurity-Agent für den Zugriffsschutz erkennt das angeschlossene Gerät und überprüft die für den Computer/Benutzer anzuwendenden Schutzrichtlinien. Dieser Vorgang bestimmt, ob der Zugriff auf das Gerät zugelassen oder blockiert wird.
Phase 3 - Freigeben/Sperren der Verwendung eines Geräts	Je nach Ergebnis der Prüfung aus Phase 2 erhält der Benutzer entweder eine Meldung, dass ein Zugriff auf das angeschlossene Gerät untersagt wurde, oder der Zugriff wird zugelassen.

Funktionsweise von GFI EndPointSecurity - Zeitlich begrenzter Zugriff

Der durch GFI EndPointSecurity zeitlich begrenzte Gerätezugriff erfolgt in drei Phasen:

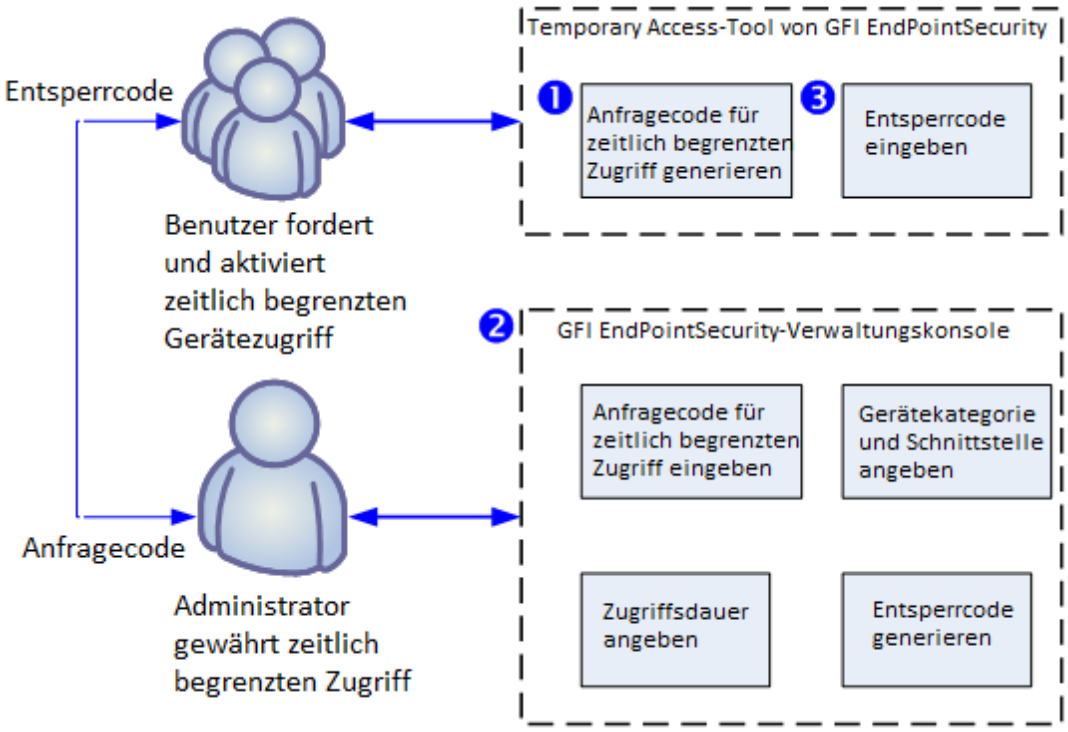


Abbildung 3: Anfordern/ Zulassen eines zeitlich begrenzten Zugriffs

In der folgenden Tabelle werden die oben abgebildeten Phasen beschrieben.

Tabelle 3: Bereitstellung und Überwachung einer Schutzrichtlinie

Phase	Beschreibung
Phase 1 - Benutzeranfrage für zeitlich begrenzten Gerätezugriff	Soll auf ein an einen Computer angeschlossenes Gerät zugegriffen werden, startet der Benutzer dort das Temporary Access-Tool von GFI EndPointSecurity. Mit diesem Tool wird eine Anfrage mit Anfragecode für den zeitlich begrenzten Gerätezugriff an den Administrator übermittelt. Der Benutzer muss neben der Dauer des gewünschten Zugriffs auch die Gerätekategorie oder die Schnittstelle angeben, auf die zugegriffen wird.
Phase 2 - Freigabe des zeitlich begrenzten Gerätezugriffs	Der Administrator verwendet die Funktion für den zeitlich begrenzten Zugriff der GFI EndPointSecurity-Verwaltungskonsole, um den Anfragecode einzugeben sowie die Geräte/Schnittstellen und die Zugriffsdauer festzulegen. Daraufhin wird ein Entsperrcode erstellt und zur vorübergehenden Freischaltung des Geräts an den Benutzer übermittelt.

Phase	Beschreibung
Phase 3 - Benutzer aktiviert zeitlich begrenzten Gerätezugriff	Sobald der Benutzer den Entsperrcode vom Administrator erhält, muss der Code im Temporary Access-Tool von GFI EndPointSecurity eingegeben werden, um den zeitlich begrenzten Zugriff zu aktivieren und die erforderlichen Geräte/Schnittstellen nutzen zu können.

1.2 Komponenten von GFI EndPointSecurity

Bei der Installation von GFI EndPointSecurity werden folgende Komponenten bereitgestellt:

» GFI EndPointSecurity-Verwaltungskonsole

» GFI EndPointSecurity-Agent

1.2.1 GFI EndPointSecurity-Verwaltungskonsole

Mithilfe der GFI EndPointSecurity-Verwaltungskonsole können Sie:

» Schutzrichtlinien erstellen und verwalten, und festlegen, welche Gerätekategorien und Schnittstellen kontrolliert werden sollen.

» Schutzrichtlinien und Agenten per Fernzugriff auf den zu kontrollierenden Computern bereitstellen sowie zeitlich begrenzten Zugriff auf Computer gewähren, um bestimmte Geräte zu nutzen.

» Den Schutzstatus jedes überwachten Computers anzeigen.

» kontrollierte Computer scannen, um aktuell oder zuvor verbundene Geräte zu identifizieren.

» Protokolle prüfen, und analysieren, welche Geräte mit den einzelnen Netzwerkcomputern verbunden waren.

» verfolgen, auf welchen Computern der Agent bereitgestellt wurde und welche Agenten aktualisiert werden müssen.

1.2.2 GFI EndPointSecurity-Agent

Der Agent von GFI EndPointSecurity sorgt dafür, dass die Schutzrichtlinien auf den zu kontrollierenden Computern eingerichtet werden. Dieser Dienst wird automatisch auf dem zu kontrollierenden Netzwerkcomputer installiert, nachdem die erste relevante Schutzrichtlinie von der GFI EndPointSecurity-Verwaltungskonsole bereitgestellt wurde. Bei weiteren Bereitstellungen der gleichen Schutzrichtlinie wird der Agent aktualisiert, nicht neu installiert.

1.3 Administratorhandbuch

Detaillierte Administrations- und Konfigurationsanweisungen finden Sie im GFI EndPointSecurity von Administratorhandbuch, das zusammen mit dem Produkt installiert wird und unter folgender Adresse heruntergeladen werden kann: http://www.gfi.com/esec/esecmanual.pdf

Das Administratorhandbuch ergänzt diese Kurzanleitung und bietet weitere Informationen zur Nutzung und Anpassung der Tools und Funktionen von GFI EndPointSecurity.

1.4 Konventionen dieses Handbuchs

Tabelle 4: Begriffe und Konventionen dieses Handbuchs

Begriff	Beschreibung
	Zusätzliche Informationen und Referenzen, die für die ordnungsgemäße Funktion von GFI EndPointSecurity wichtig sind.

Begriff	Beschreibung
	Wichtige Hinweise und Warnungen bezüglich potentieller, oft auftretender Probleme.
>	Schritt-für-Schritt-Anleitungen für den Zugriff auf eine Funktion.
Fetter Text	Auszuwählende Elemente wie Knoten, Menüoptionen und Befehlsschaltflächen.
Kursiver Text	Parameter und Werte, die durch einen zutreffenden Wert ersetzt werden müssen, z. B. benutzerdefinierte Pfade und Dateinamen.
`Code`	Einzugebende Textwerte, z. B. Befehle und Adressen.

1.5 Unterstützte Schnittstellen

GFI EndPointSecurity sucht nach Geräten, die an folgenden Schnittstellen angeschlossen sind oder waren:

USB

Secure Digital (SD)

FireWire

Bluetooth

Infrarot

PCMCIA

Serielle und parallele Schnittstellen

Interne (z. B. optische Laufwerke, intern an PCI angeschlossen)

1.6 Unterstützte Gerätekategorien

GFI EndPointSecurity unterteilt kontrollierte Hardware in folgende Gerätekategorien:

Disketten

CDs/DVDs

Drucker

PDAs, einschließlich:

- Pocket-PCs
- Smartphones

Netzwerkadapter, einschließlich:

- Ethernet-Adapter
- WiFi-Adapter
- Entfernbare Adapter (USB, FireWire, PCMCIA)

Modems, einschließlich:

- Smartphones
- Mobiltelefone

Bildverarbeitungsgeräte:

- Digitalkameras
- Webcams
- Scanner

Eingabegeräte:

- Tastaturen
- Mäuse
- Spiel-Controller

Speichergeräte, einschließlich:

- USB-Speichersticks
- Multimedia-Player (z. B. MP3-/MP4-Player)
- Kartenleser für CompactFlash- und andere Speicherkarten
- USB-Multi-Drives (d. h. Geräte, die nicht als einzelnes Laufwerk angeschlossen werden)

Weitere Geräte

- Bluetooth-Dongles/Schnittstellen
- Infrarot-Dongles/Schnittstellen
- Zip-Laufwerke
- Bandlaufwerke
- MO-Laufwerke (intern und extern).

2 Installieren von GFI EndPointSecurity

Dieses Kapitel enthält Informationen zur Vorbereitung Ihrer Netzwerkumgebung für die erfolgreiche Bereitstellung von GFI EndPointSecurity.

Themen in diesem Kapitel

2.1 Systemanforderungen

Hardwareanforderungen

In der folgenden Tabelle werden die Hardwareanforderungen für GFI EndPointSecurity und GFI EndPointSecurity-Agenten aufgeführt:

Tabelle 5: Systemanforderungen: Hardware

	GFI EndPointSecurity	GFI EndPointSecurity-Agent
Prozessor	Mindestens: 2 GHz Empfohlen: 2 GHz	Mindestens: 1 GHz Empfohlen: 1 GHz
RAM	Mindestens: 512 MB Empfohlen: 1 GB	Mindestens: 256 MB Empfohlen: 512 MB
Freier Speicherplatz	Mindestens: 100 MB Empfohlen: 100 MB	Mindestens: 50 MB Empfohlen: 50 MB

Unterstützte Betriebssysteme (x64/x86)

GFI EndPointSecurity und GFI EndPointSecurity-Agenten können auf Computern mit folgenden Betriebssystemen installiert werden:

- Microsoft Windows Server 2012
- Microsoft Windows Small Business Server 2011 (Standard-Edition)
- Microsoft Windows Server 2008 R2 (Standard- oder Enterprise-Edition)
- Microsoft Windows Server 2008 (Standard- oder Enterprise-Edition)
- Microsoft Windows Small Business Server 2008 (Standard-Edition)
- Microsoft Windows Server 2003 (Standard-, Enterprise- oder Web-Edition)
- Microsoft Windows Small Business Server 2003
- Microsoft Windows 8 (Professional oder Enterprise)
- Microsoft Windows 7 (Professional-, Enterprise- oder Ultimate-Edition)
- Microsoft Windows Vista (Enterprise-, Business- oder Ultimate-Edition)
- Microsoft Windows XP Professional Service Pack 3.

Agent - Hardwareanforderungen

- Prozessor: CPU mit 1 GHz oder höher
- RAM: mindestens 256 MB; 512 MB empfohlen
- Festplattenspeicher: 50 MB freier Speicherplatz

Agent – Softwareanforderungen

- Prozessor: CPU mit 1 GHz oder höher
- RAM: mindestens 256 MB; 512 MB empfohlen
- Festplattenspeicher: 50 MB freier Speicherplatz

Andere Softwarekomponenten

Für eine Bereitstellung mit vollem Funktionsumfang benötigt GFI EndPointSecurity die folgenden Softwarekomponenten:

- Microsoft Internet Explorer 5.5 oder höher
- Microsoft .NET Framework 2.0 oder höher
- Microsoft SQL Server 2000, 2005 oder 2008 als Backend-Datenbank

Hinweis

Für das Speichern von Gerätezugriffsdaten und die Berichtserstellung wird ein Datenbank-Backend benötigt. GFI EndPointSecurity bietet die Möglichkeit, entweder einen verfügbaren Microsoft SQL Server zu verwenden oder automatisch Microsoft SQL Server 2005 Express auf den Computer herunterzuladen und zu installieren, auf dem die GFI EndPointSecurity-Verwaltungskonsole installiert ist.

Firewall-Ports

TCP-Port 1116 (Standard) – wird von GFI EndPointSecurity-Agenten für Statusmeldungen an GFI EndPointSecurity und zum Senden von Gerätezugriffsereignissen benötigt. Ohne diesen offenen Port muss der Administrator die Ereignisse entweder manuell auf jedem kontrollierten Computer oder automatisch mit GFI EventsManager überwachen. Weitere Informationen finden Sie unter http://www.gfi.com/eventsmanager.

2.2 Aktualisieren von GFI EndPointSecurity

Aktualisieren von GFI EndPointSecurity 3 oder höher

Falls Sie GFI LanGuard Portable Storage Control oder eine ältere Version von GFI EndPointSecurity besitzen, können Sie wie nachfolgend beschrieben auf die neueste Version von GFI EndPointSecurity umsteigen. Ein Umstieg von GFI EndPointSecurity 3 oder höher auf GFI EndPointSecurity 2013 ist leicht durchzuführen. Die Aktualisierung ist bereits Teil der Installation von GFI EndPointSecurity 2013 und umfasst:

- Deinstallieren von GFI EndPointSecurity 3 oder höher
- Importieren der Konfigurationseinstellungen aus GFI EndPointSecurity 3.

Bei der Installation von GFI EndPointSecurity müssen Sie den Import der Konfigurationseinstellungen der vorherigen Version gesondert bestätigen. Klicken Sie auf **Ja**, um die Konfigurationen zu

importieren. Sie werden danach gefragt, welche der folgenden Einstellungen importiert werden sollen:

- Schutzrichtlinien:
  - Computer
  - Sicherheitseinstellungen
- Optionen:
  - Protokollierungsoptionen
  - Datenbankoptionen.

Aktualisieren von GFI LanGuard Portable Storage Control

Wird der Computer, auf dem GFI EndPointSecurity installiert werden soll, durch den Agenten von GFI LanGuard Portable Storage Control geschützt, muss der Agent zuvor deinstalliert werden. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie die Konfigurationskonsole von GFI LanGuard Portable Storage Control.

2. Löschen Sie den Agenten auf dem Computer, auf dem GFI EndPointSecurity installiert werden soll.

> **Hinweis**
>
> Führen Sie den Vorgang nur auf dem Computer aus, auf dem GFI EndPointSecurity installiert werden soll.

3. Schließen Sie die Konfigurationskonsole von GFI LanGuard Portable Storage Control, und beginnen Sie mit der Installation von GFI EndPointSecurity.

4. Bei der Installation von GFI EndPointSecurity müssen Sie den Import der Konfigurationseinstellungen der vorherigen Version gesondert bestätigen. Klicken Sie auf **Ja**, um die Konfigurationen zu importieren.

> **Hinweis**
>
> Alle weiteren Agenten, die mit GFI LanGuard Portable Storage Control auf zu kontrollierenden Computern installiert wurden, werden in GFI EndPointSecurity automatisch einer Schutzrichtlinie mit dem Namen **LegacyAgents** hinzugefügt.

2.3 Installieren einer neuen Instanz von GFI EndPointSecurity

So installieren Sie GFI EndPointSecurity:

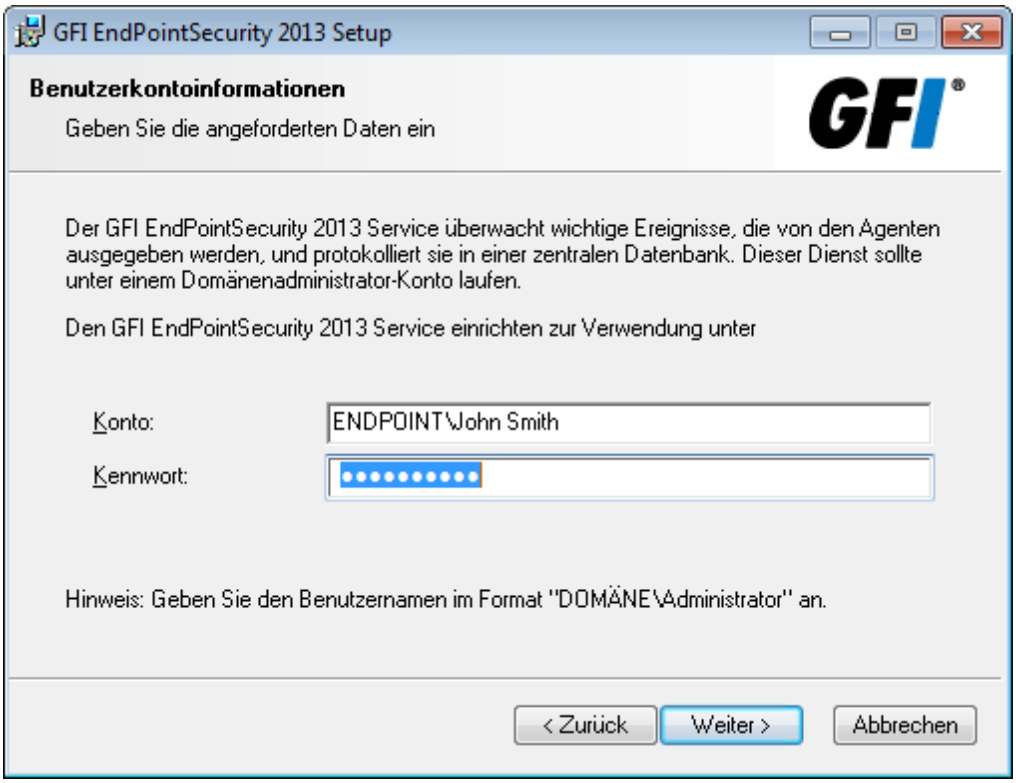
1. Melden Sie sich auf dem Rechner an, auf dem Sie GFI EndPointSecurity installieren möchten (mit Administratorrechten).

2. Doppelklicken Sie auf die ausführbare Datei für GFI EndPointSecurity.

2. Wählen Sie die gewünschte Sprache für die Installation aus, und klicken Sie auf **OK**.

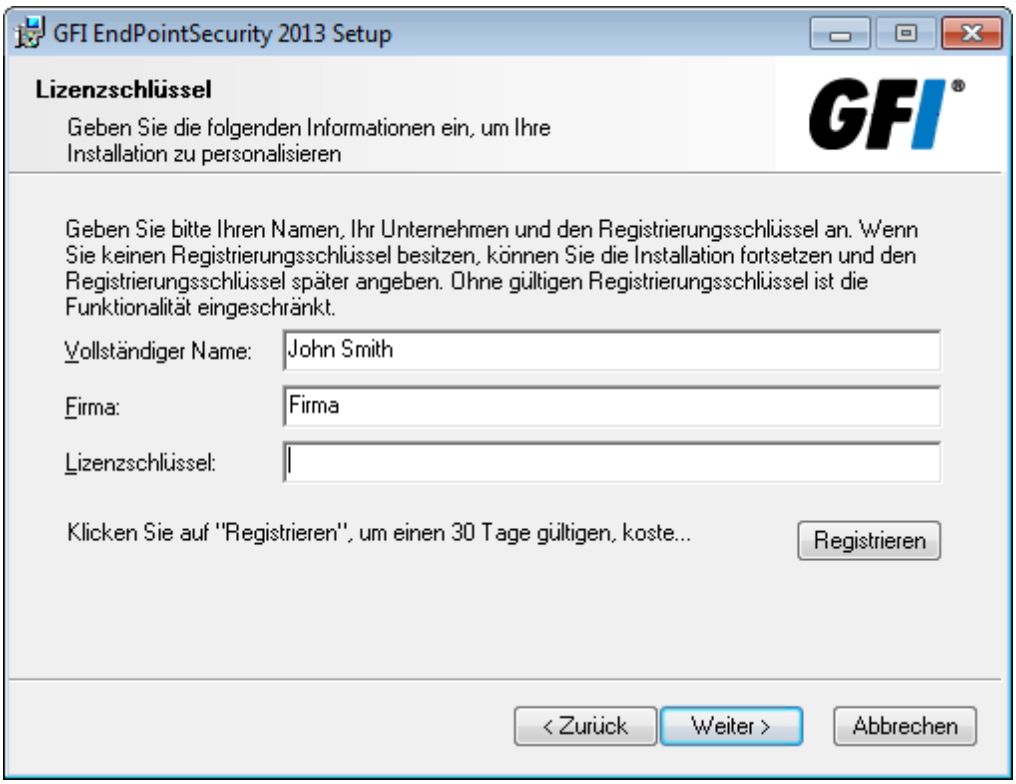
3. Klicken Sie auf dem Willkommensbildschirm auf **Weiter**, um die Einrichtung zu starten.

4. Lesen Sie die Endbenutzer-Lizenzvereinbarung sorgfältig durch. Wenn Sie mit den Bedingungen der Vereinbarung einverstanden sind, wählen Sie **Ich stimme der Lizenzvereinbarung zu**, und klicken Sie auf **Weiter**.



Screenshot 1: GFI EndPointSecurity-Installation: Einrichtung des Domänenadministrator-Kontos

5. Geben Sie die Anmeldeinformationen eines Kontos mit administrativen Berechtigungen ein, und klicken Sie zum Fortfahren auf **Weiter**.



Screenshot 2: GFI EndPointSecurity-Installation: Lizenzschlüsseldaten

6. Geben Sie den **Vollständigen Namen** und die **Firma** ein. Falls Sie einen Lizenzschlüssel besitzen, aktualisieren Sie die Daten unter **Lizenzschlüssel**, und klicken Sie auf **Weiter**.

> **Hinweis**
>
> Der Lizenzschlüssel kann nach der Installation oder nach Ablauf des Testzeitraums von GFI EndPointSecurity eingegeben werden. Weitere Informationen finden Sie unter Produktlizenzierung (page 29).

7. Geben Sie gegebenenfalls einen alternativen Installationspfad ein, oder verwenden Sie dafür die Schaltfläche „Durchsuchen“. Falls Sie den Standardpfad verwenden möchten, klicken Sie auf **Weiter**, um mit der Installation fortzufahren.

8. Klicken Sie auf **Zurück**, um die Installationsinformationen zu ändern, oder klicken Sie auf **Weiter**, um die Installation abzuschließen.

9. Aktivieren oder deaktivieren Sie nach der Installation das Kontrollkästchen „GFI EndPointSecurity starten“, und klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.

2.4 Konfigurationsschritte nach der Installation

Beim ersten Start der GFI EndPointSecurity-Verwaltungskonsole wird der Schnellstart-Assistent automatisch gestartet. Auf diese Weise können Sie die wichtigsten Einstellungen von GFI EndPointSecurity für die erste Verwendung konfigurieren.

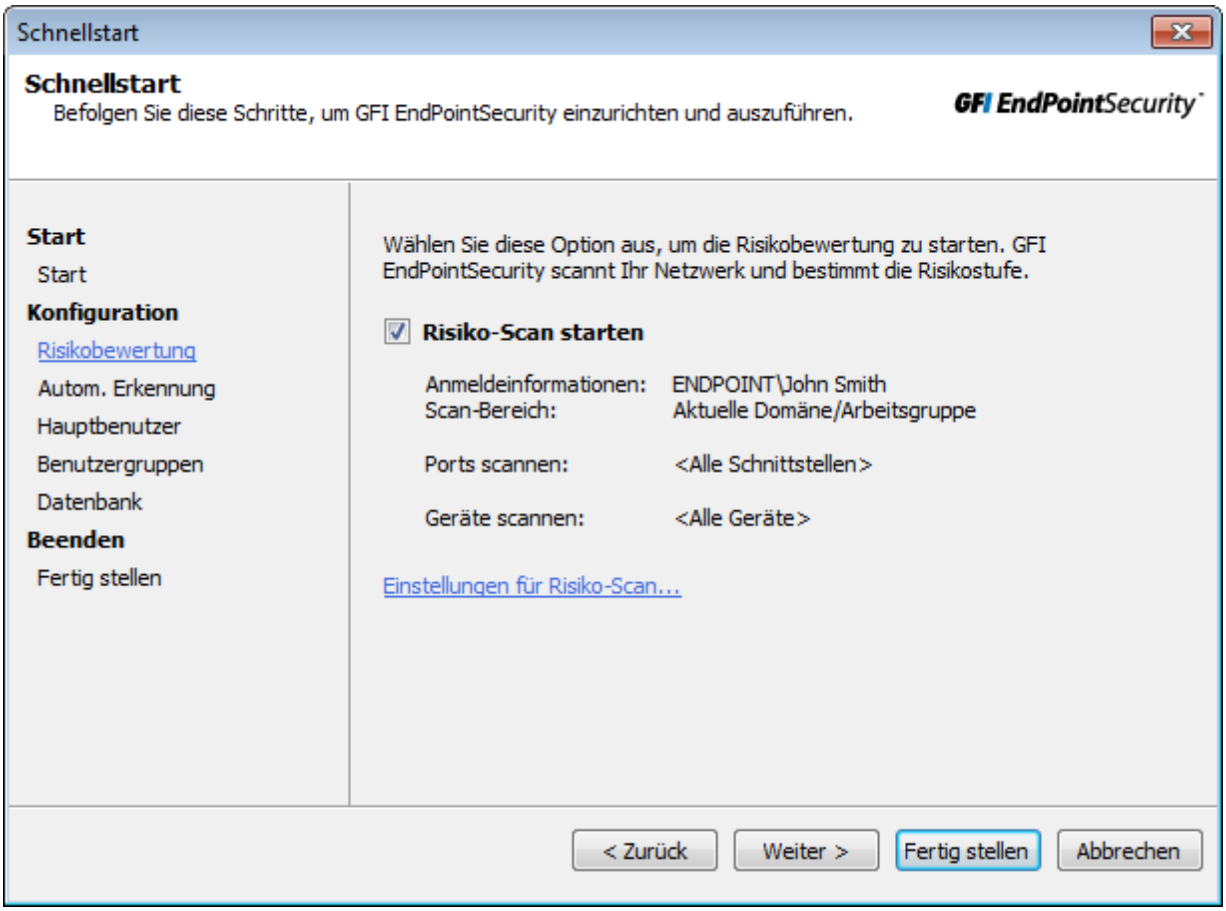
Der Schnellstart-Assistent leitet Sie durch die folgenden Konfigurationsschritte:

- Risikobewertung
- Automatische Erkennung
- Hauptbenutzer
- Benutzergruppen
- Datenbank-Backend.

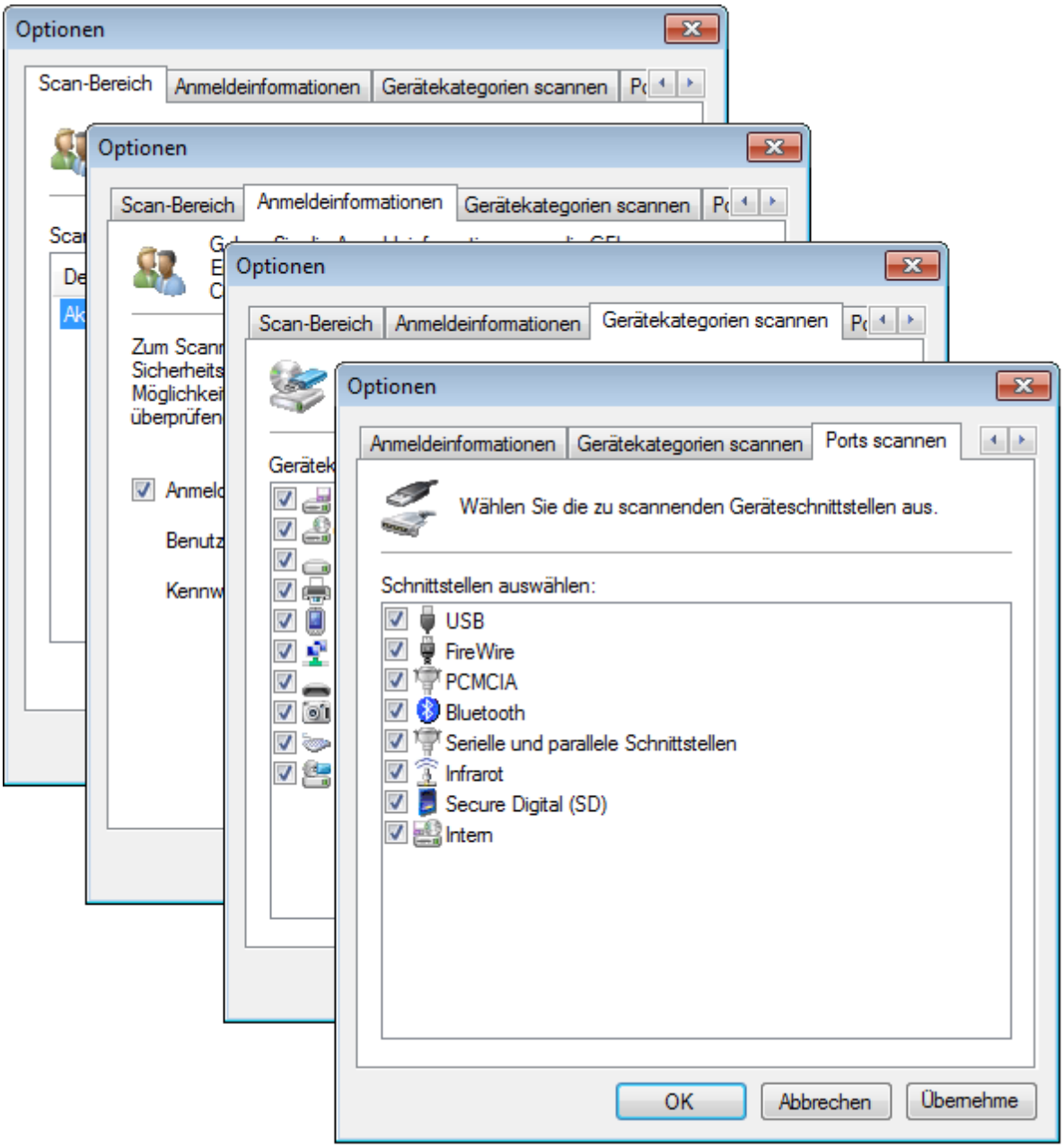
> **Hinweis**
>
> Der Schnellstart-Assistent kann über **Datei > Schnellstart-Assistent…** erneut gestartet werden.

So verwenden Sie den Schnellstart-Assistenten:

1. Klicken Sie auf dem Willkommensbildschirm des Assistenten auf **Weiter**.



2. Aktivieren/deaktivieren Sie unter **Risikobewertung** die Option **Risiko-Scan starten**, um die Funktion zum Starten eines Scans Ihres Netzwerks zur Bestimmung der Risikostufe zu aktivieren/deaktivieren.

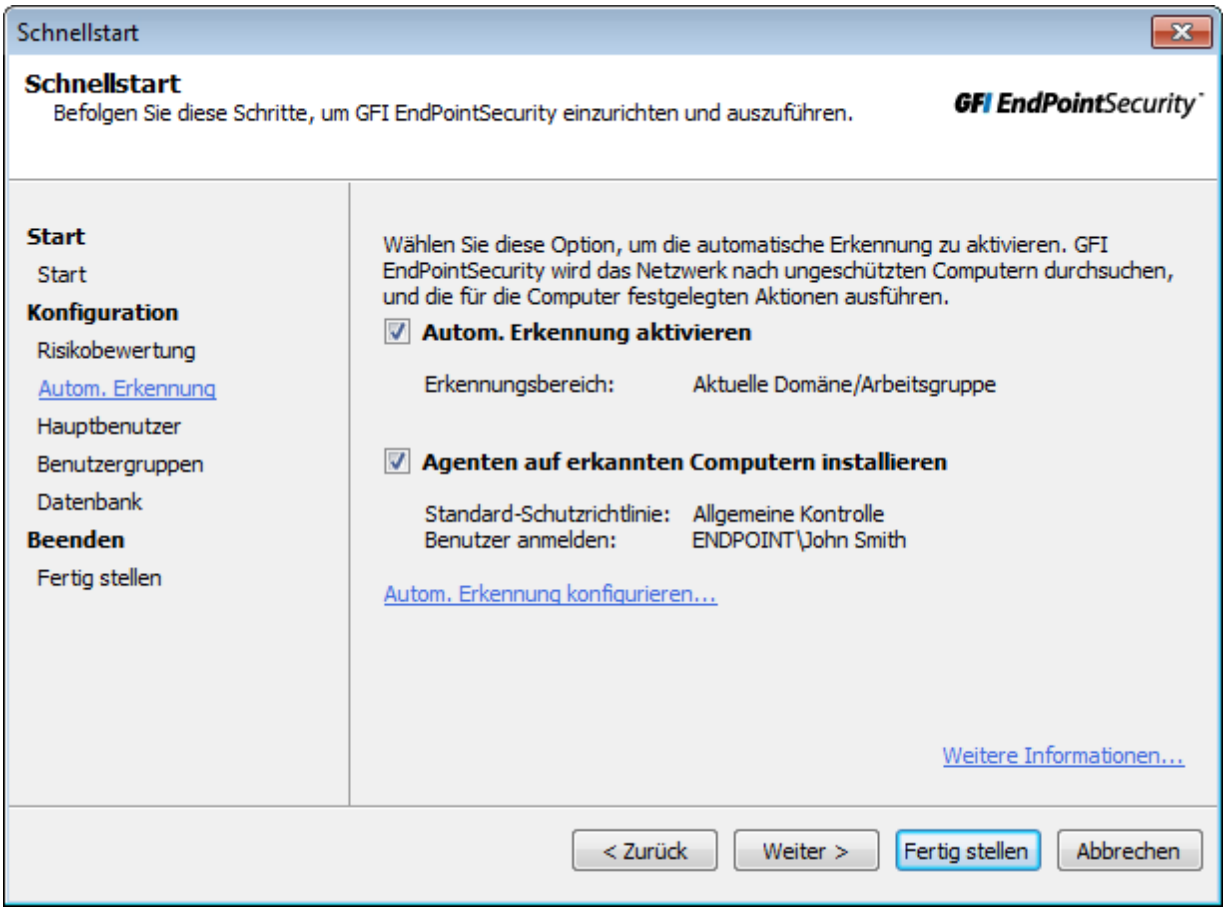


3. (Optional) Klicken Sie auf **Einstellungen für Risiko-Scan...**, und konfigurieren Sie die Einstellungen in den unten beschriebenen Registerkarten:

Tabelle 6: Einstellungen für die autom. Erkennung

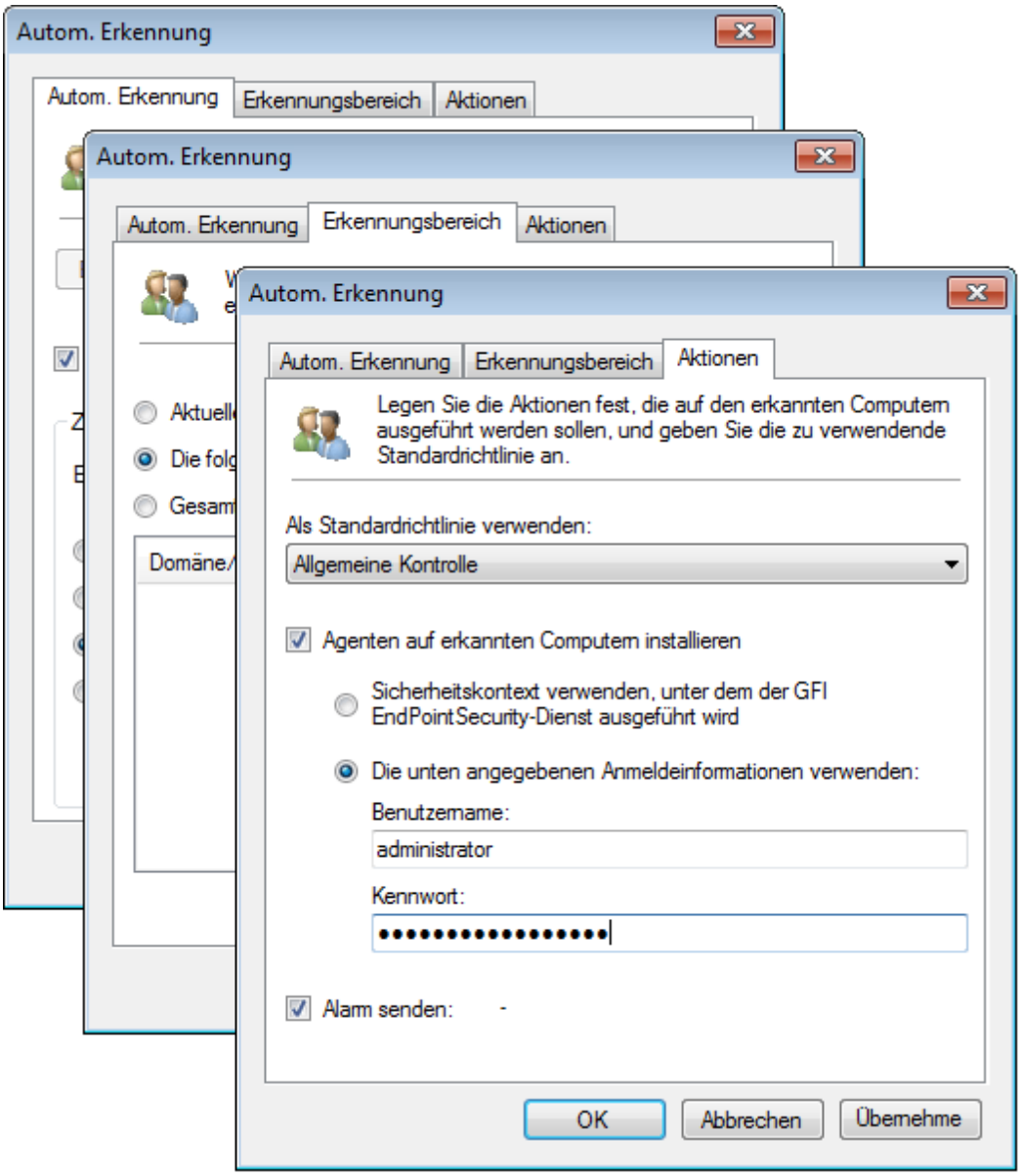
Registerkarte	Beschreibung
Scan-Bereich:	Wählen Sie den Zielbereich aus, in dem GFI EndPointSecurity die Computer des Netzwerks scannt. » **Aktuelle Domäne/Arbeitsgruppe** – GFI EndPointSecurity sucht in derselben Domäne/Arbeitsgruppe, in der das Programm installiert ist, nach neuen Computern. » **Die folgenden Domänen/Arbeitsgruppen** – Wählen Sie diese Option, und klicken Sie auf **Hinzufügen**. Geben Sie die Domänen an, in denen GFI EndPointSecurity nach neuen Computern suchen soll, und klicken Sie auf **OK**. » **Gesamtes Netzwerk mit Ausnahme von** – Wählen Sie diese Option, und klicken Sie auf **Hinzufügen**. Geben Sie die Domäne/Arbeitsgruppe an, die von der autom. Erkennung ausgeschlossen werden soll, und klicken Sie auf **OK**. » **IP-Bereich** – Wählen Sie diese Option, und klicken Sie auf **Hinzufügen**. Geben Sie den Bereich der IP-Adressen an, die während der automatischen Erkennung einbezogen oder ausgeschlossen werden sollen, und klicken Sie auf **OK**. » **Computerliste** – Wählen Sie diese Option aus, und klicken Sie auf **Hinzufügen**. Geben Sie die Domäne/Arbeitsgruppe an, die während der automatischen Erkennung einbezogen oder ausgeschlossen werden soll, und klicken Sie auf **OK**.
Anmeldeinformationen	Aktivieren/deaktivieren Sie die Option **Anmeldung erfolgt mit diesen Anmeldeinformationen**, und geben Sie die Anmeldeinformationen an, die GFI EndPointSecurity für den Zugriff auf die zu scannenden Computer verwenden soll.
Gerätekategorien scannen	Wählen Sie die Gerätekategorien aus, die GFI EndPointSecurity in den Scan einbeziehen soll.
Ports scannen	Wählen Sie die Geräteanschlussports aus, die GFI EndPointSecurity in den Scan einbeziehen soll.

4. Klicken Sie auf **Übernehmen** und **OK**, um das Dialogfeld „Risikobewertung“ zu schließen, und klicken Sie im Schnellstart-Assistent auf **Weiter**.



5. Aktivieren/deaktivieren Sie unter **Autom. Erkennung** die Option **Autom. Erkennung aktivieren**, um die automatische Erkennung zu aktivieren bzw. deaktivieren. Bei Aktivierung der autom. Erkennung wird von GFI EndPointSecurity das Netzwerk regelmäßig nach neuen Computern durchsucht.

6. Aktivieren/deaktivieren Sie **Agenten auf erkannten Computern installieren**, um die automatische Bereitstellung von GFI EndPointSecurity-Agenten auf neu erkannten Computern zu aktivieren bzw. deaktivieren.

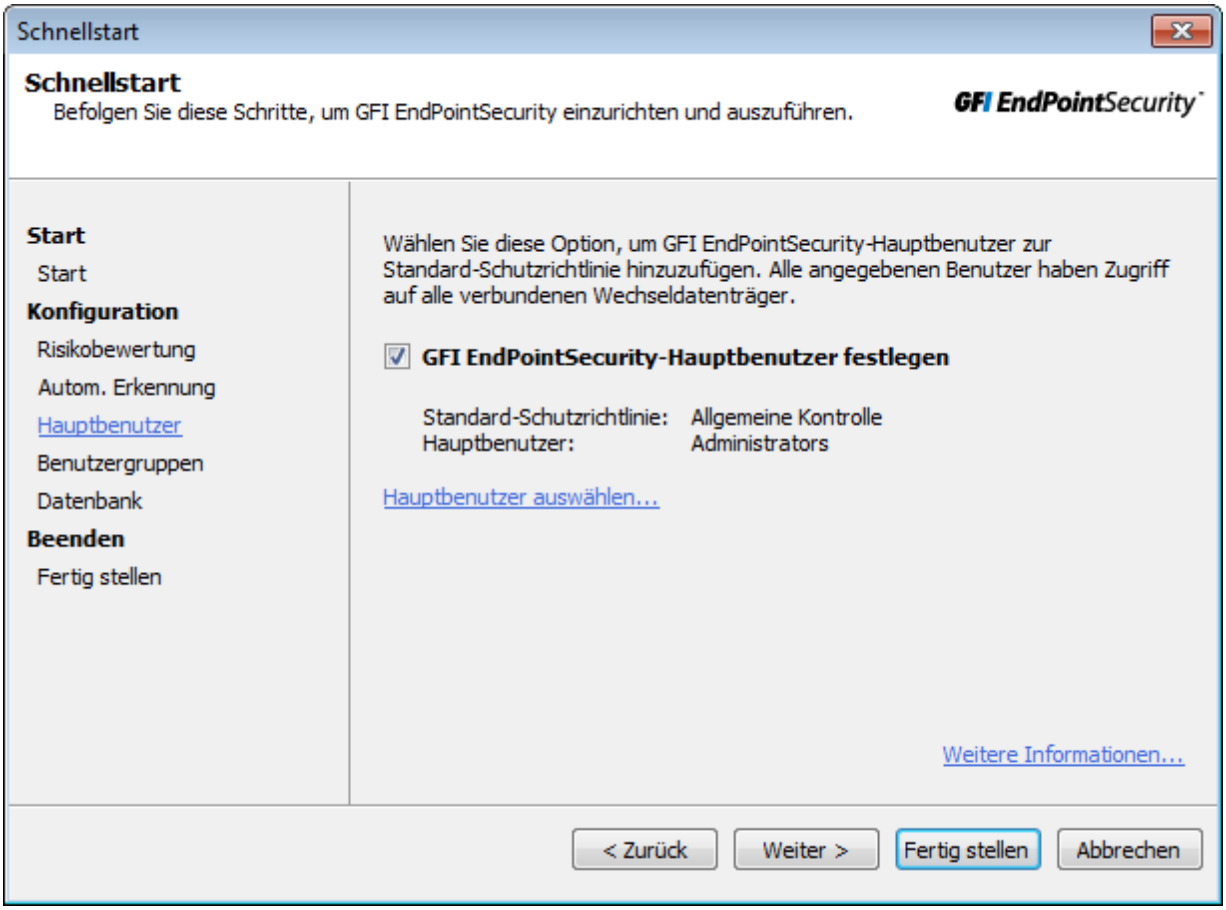


7. (Optional) Klicken Sie auf **Autom. Erkennung konfigurieren...**, und konfigurieren Sie die Einstellungen auf den nachfolgend beschriebenen Registerkarten:

Tabelle 7: Einstellungen für die autom. Erkennung

Registerkarte	Beschreibung
Autom. Erkennung	Aktivieren/Deaktivieren Sie die autom. Erkennung, und konfigurieren Sie einen Zeitplan, wann GFI EndPointSecurity das Netzwerk nach neuen Computern durchsucht.
Erkennungsbereich	Wählen Sie aus, wo GFI EndPointSecurity nach neuen Computern sucht. Zur Auswahl stehen: » **Aktuelle Domäne/Arbeitsgruppe** - GFI EndPointSecurity sucht in derselben Domäne/Arbeitsgruppe, in der das Programm installiert ist, nach neuen Computern. » **Die folgenden Domänen/Arbeitsgruppen** - Wählen Sie diese Option, und klicken Sie auf **Hinzufügen**. Geben Sie die Domänen an, in denen GFI EndPointSecurity nach neuen Computern suchen soll, und klicken Sie auf **OK**. » **Gesamtes Netzwerk mit Ausnahme von** - Wählen Sie diese Option, und klicken Sie auf **Hinzufügen**. Geben Sie die Domäne/Arbeitsgruppe an, die von der autom. Erkennung ausgeschlossen werden soll, und klicken Sie auf **OK**.
Aktionen	Konfigurieren Sie die Aktionen, die von GFI EndPointSecurity bei Erkennung eines neuen Computers ausgeführt werden sollen. Wählen Sie außerdem die Richtlinie aus, auf die sich diese Einstellungen beziehen.

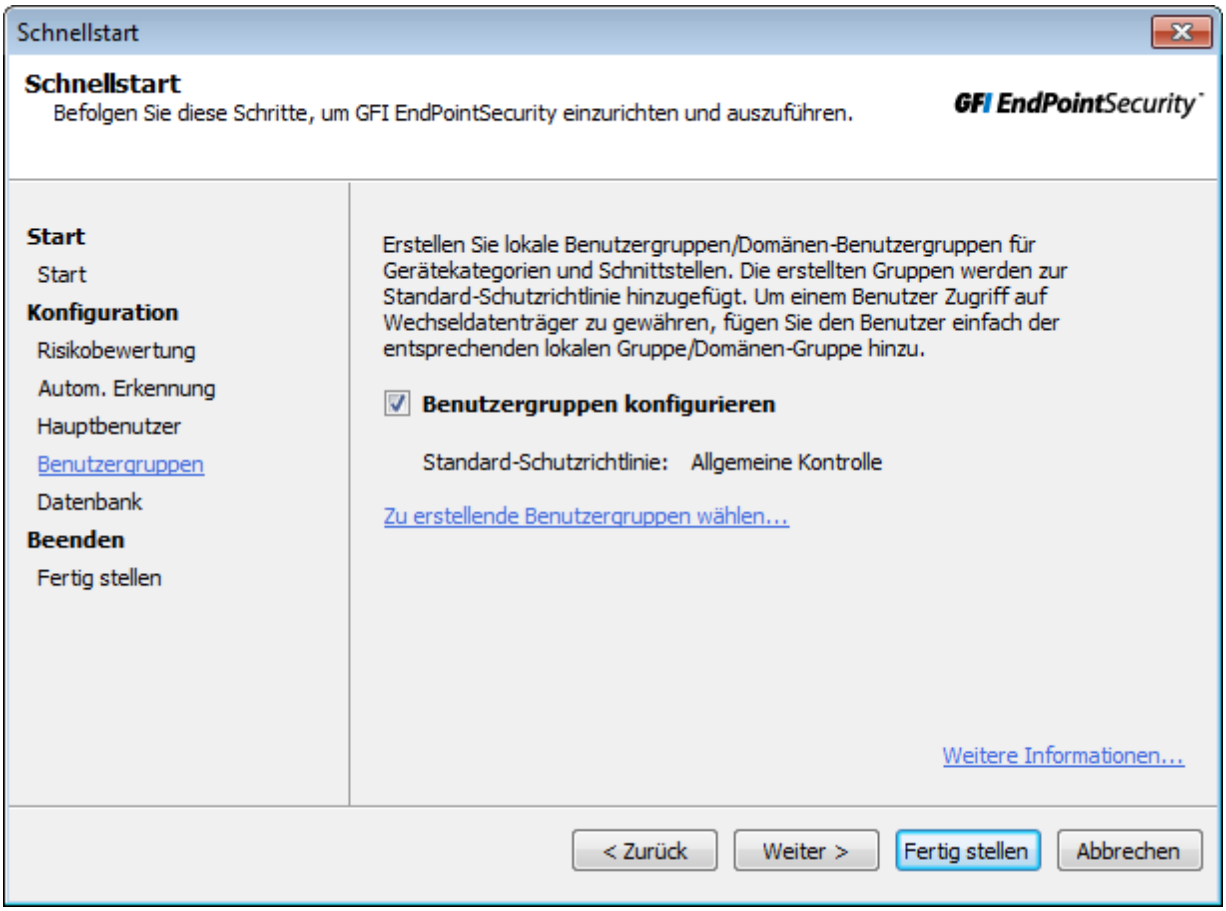
8. Klicken Sie auf **Übernehmen** und **OK**, um das Dialogfeld „Autom. Erkennung“ zu schließen, und klicken Sie im Schnellstart-Assistenten auf **Weiter**.



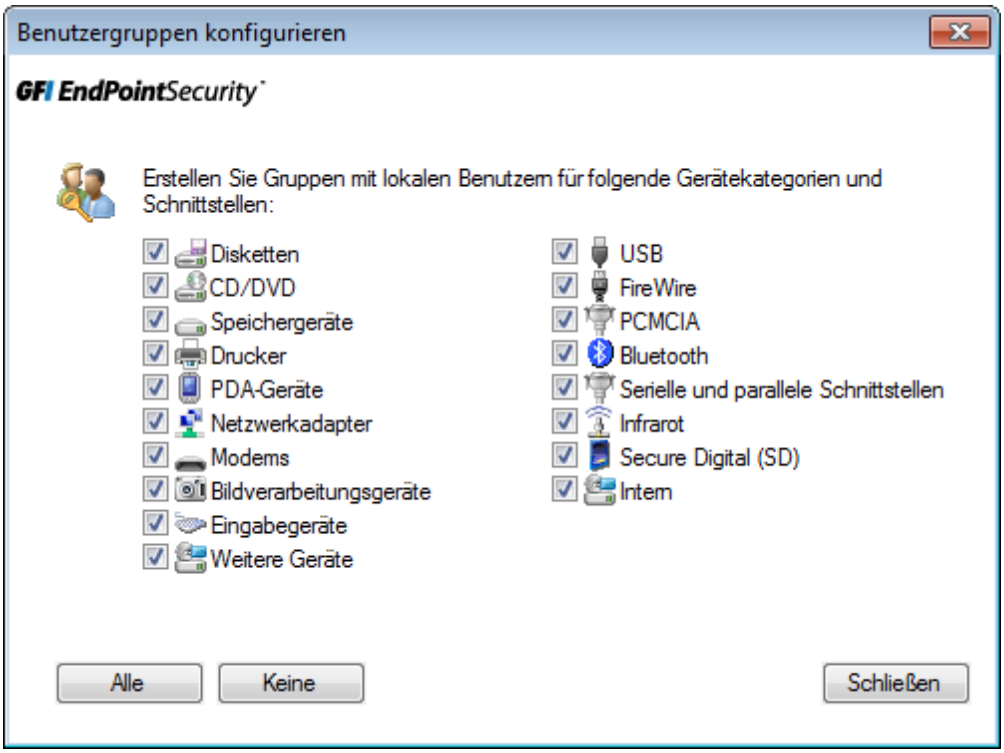
9. Aktivieren/deaktivieren Sie unter **Hauptbenutzer** die Option **Hauptbenutzer von GFI EndPointSecurity festlegen**, um die Hauptbenutzerfunktionen zu aktivieren bzw. deaktivieren. Mitglieder der Hauptbenutzergruppe haben Zugriff auf alle verbundenen Geräte, die von dieser Richtlinie betroffen sind.

10. Klicken Sie auf **Hauptbenutzer auswählen...**, und klicken Sie dann im Dialogfeld „Hauptbenutzer“ auf **Hinzufügen...**, um Benutzer aus Ihrer Domäne/Arbeitsgruppe hinzuzufügen.

11. Klicken Sie auf **Übernehmen** und **OK**, um das Dialogfeld „Hauptbenutzer“ zu schließen, und klicken Sie im Schnellstart-Assistenten auf **Weiter**.

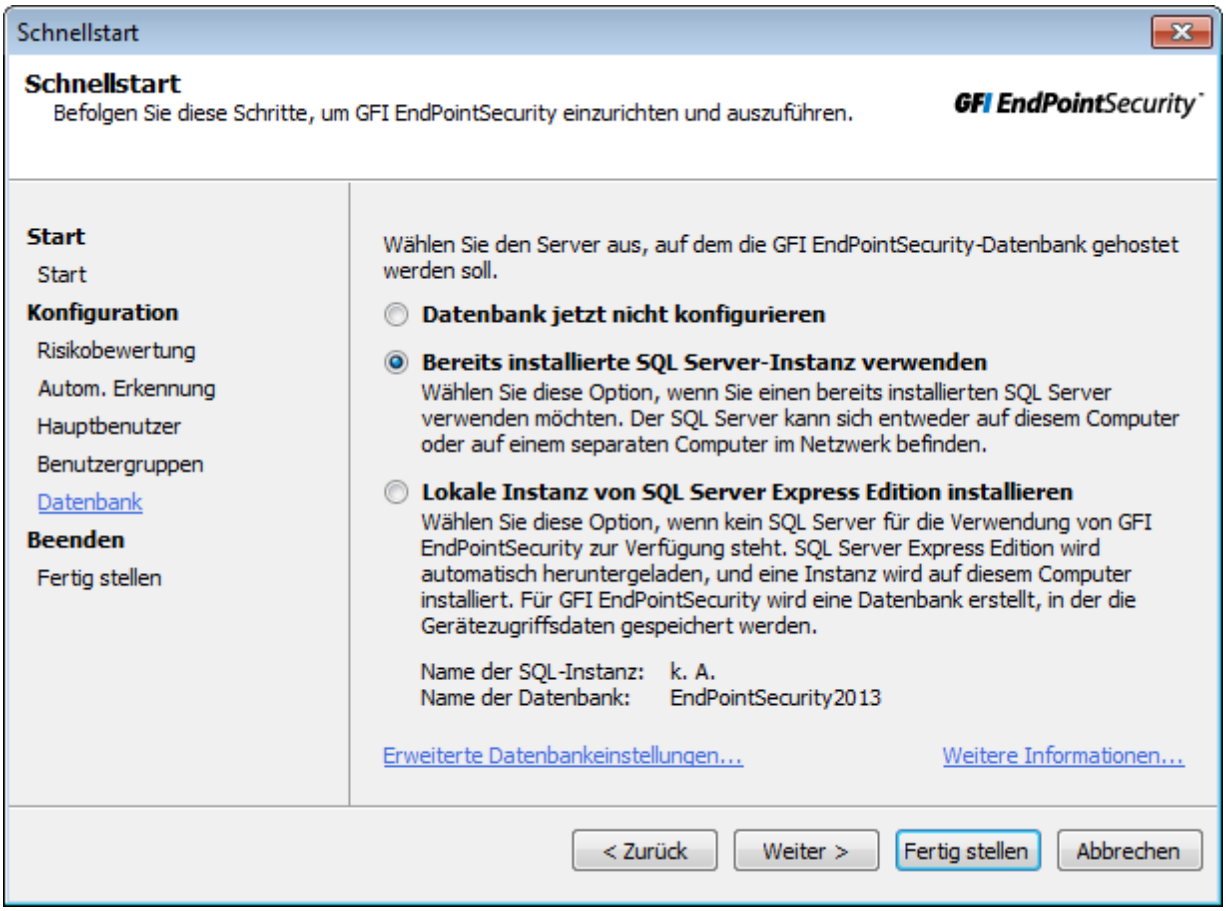


12. Aktivieren/deaktivieren Sie unter **Benutzergruppen** die Option **Benutzergruppen konfigurieren**, um Domänen-/Arbeitsgruppenbenutzer zu erstellen und mit den im nächsten Schritt ausgewählten Einstellungen für Gerätekategorien und Anschlüsse zu verknüpfen.



13. Klicken Sie auf **Zu erstellende Benutzergruppen wählen...**. Wählen Sie im Dialogfeld „Benutzergruppen konfigurieren“ die Geräte und/oder Schnittstellen aus, für die Benutzer erstellt werden. Klicken Sie zur Verwaltung aller durch diese Richtlinie unterstützten Geräte und Anschlüsse auf **Alle auswählen**.

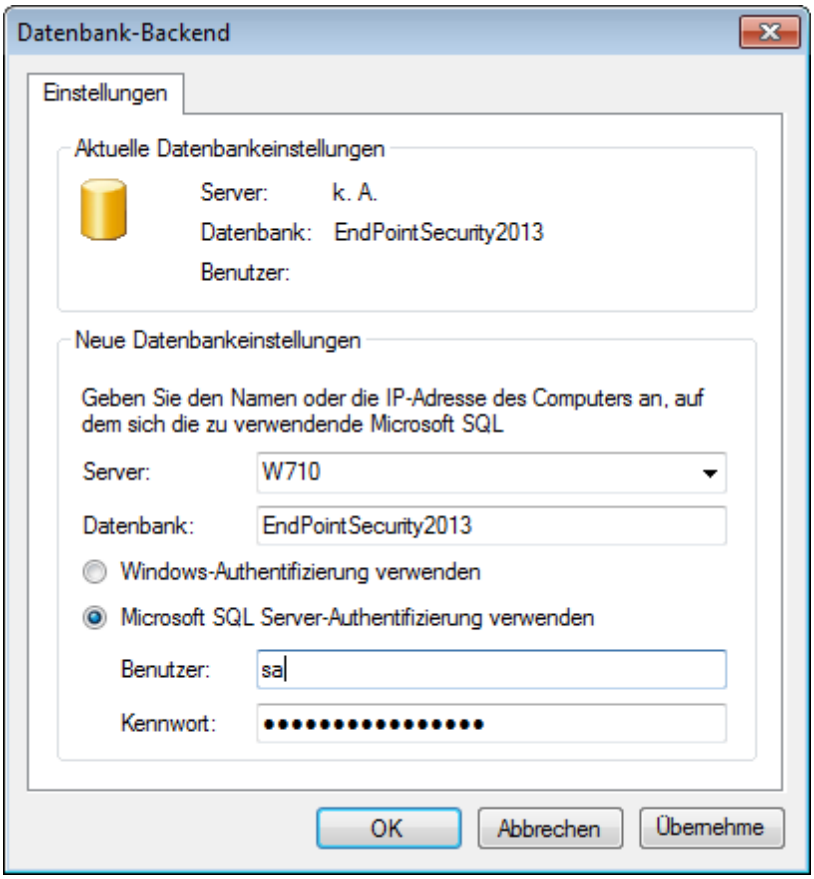
14. Klicken Sie auf **Schließen**, um das Dialogfeld **Benutzergruppen konfigurieren** zu schließen, und klicken Sie im Schnellstart-Assistenten auf **Weiter**.



15. Wählen Sie unter „Datenbank“ den Datenbanktyp aus, den Sie als Datenbank-Backend verwenden möchten. Wählen Sie eine der unten beschriebenen Optionen:

Tabelle 8: Optionen für Datenbank-Backend

Option	Beschreibung
Datenbank jetzt nicht konfigurieren	Schließen Sie den Schnellstart-Assistenten ab, und konfigurieren Sie das Datenbank-Backend später. Weitere Informationen finden Sie im ACM
Bereits installierte SQL Server-Instanz verwenden	Verwenden Sie eine Instanz von Microsoft SQL Server, die bereits auf demselben Computer wie GFI EndPointSecurity oder einen anderen Computer im Netzwerk installiert ist.
Lokale Instanz der SQL Server Express Edition installieren	Wählen Sie diese Option, um eine Instanz von Microsoft SQL Server auf denselben Computer wie GFI EndPointSecurity oder einen anderen Computer im Netzwerk herunterzuladen und dort zu installieren. Es ist eine Internetverbindung erforderlich.

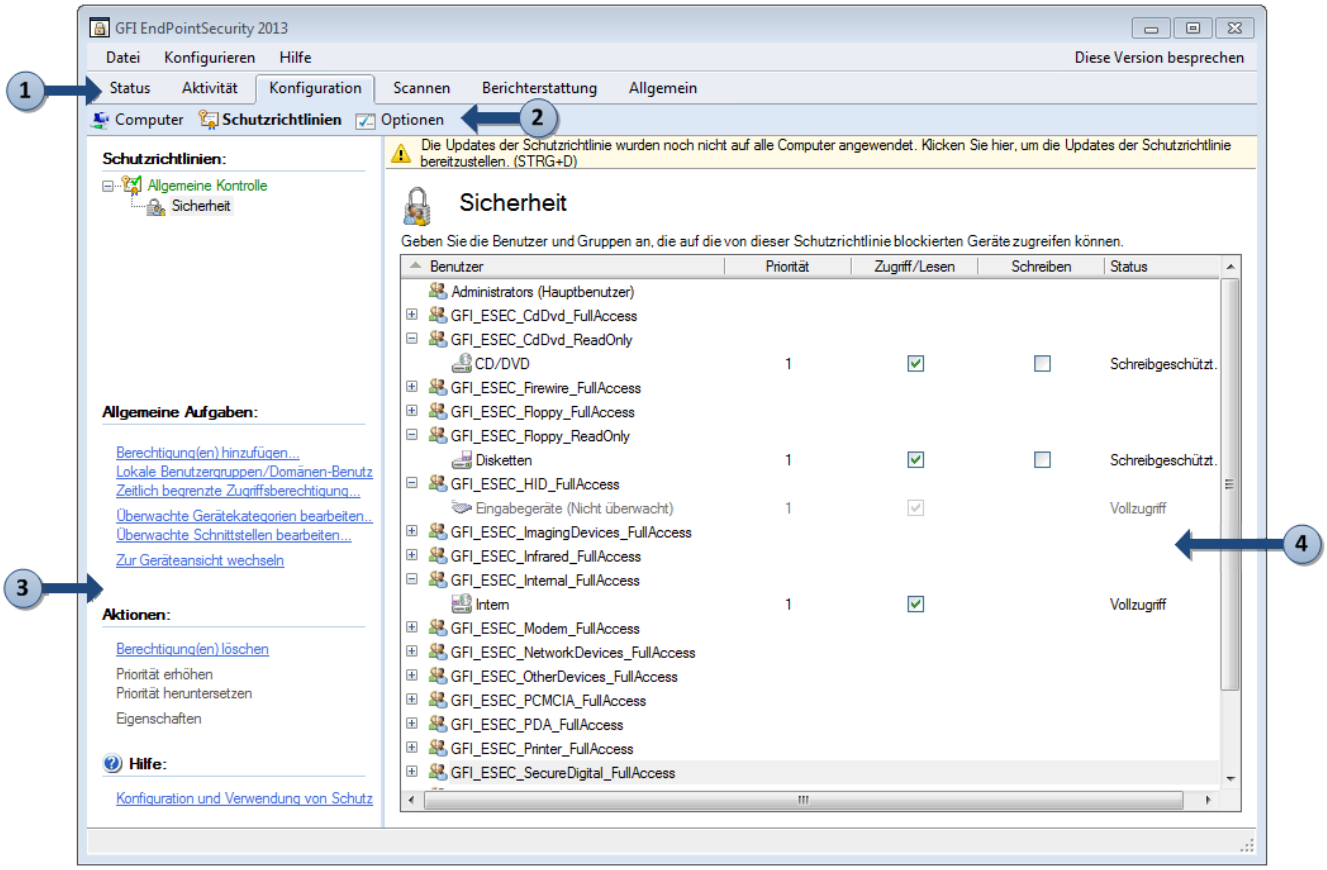


16. (Optional) Klicken Sie auf **Erweiterte Datenbankeinstellungen...**, um die SQL Server-Adresse, den Datenbanknamen, die Anmeldemethode und die zugehörigen Anmeldeinformationen anzugeben. Klicken Sie auf **Übernehmen** und **OK**, um das Dialogfeld „Datenbank-Backend“ zu schließen.

17. Klicken Sie auf **Weiter**, und warten Sie, bis die Einstellungen übernommen wurden. Klicken Sie auf **Fertig stellen**, um den Schnellstart-Assistenten zu schließen.

2.5 Navigieren in der Verwaltungskonsole

Die GFI EndPointSecurity-Verwaltungskonsole enthält alle administrativen Funktionen, die für die Überwachung und Verwaltung des Gerätezugriffs notwendig sind.



Screenshot 3: Navigieren auf der Benutzeroberfläche von GFI EndPointSecurity

Die GFI EndPointSecurity-Verwaltungskonsole besteht aus den drei unten beschriebenen Abschnitten:

Abschnitt	Beschreibung
1	**Registerkarten** Navigieren zwischen den verschiedenen Registerkarten der GFI EndPointSecurity-Verwaltungskonsole. Die verfügbaren Registerkarten sind: » **Status** - Ermöglicht die Überwachung des Programmstatus von GFI EndPointSecurity und von statistischen Zugriffsdaten. » **Aktivität** - Ermöglicht die Überwachung der im Netzwerk verwendeten Geräte. » **Konfiguration** - Ermöglicht den Aufruf und die Anpassung der standardmäßigen Schutzrichtlinien. » **Scannen** - Ermöglicht den Scan von kontrollierten Computern zur Erkennung von angeschlossenen Geräten. » **Berichterstattung** - Ermöglicht das Herunterladen oder Starten von GFI EndPointSecurityGFI ReportPack zum Erstellen von Berichten. » **Allgemein** - Ermöglicht die Prüfung auf GFI EndPointSecurity-Aktualisierungen sowie die Anzeige der Version und Lizenzierungsdetails.
2	**Untergeordnete Registerkarten** Weitere Einstellungen und/oder Informationen zur ausgewählten Registerkarte aus Abschnitt 1.
3	**Linker Bereich** Zugriff auf Konfigurationsoptionen in GFI EndPointSecurity. Die Konfigurationsoptionen sind in drei Abschnitten zusammengefasst, einschließlich **Allgemeine Aufgaben**, **Aktionen** und **Hilfe**. Nur bei manchen Registerkarten verfügbar.
4	**Rechter Bereich** Konfiguration der Konfigurationsoptionen, die im linken Bereich ausgewählt wurden. Nur bei manchen Registerkarten verfügbar.

3 Prüfen der Installation

Prüfen Sie die Funktion von GFI EndPointSecurity, sobald die Installation und der Schnellstart-Assistent abschlossen sind. Folgen Sie den Anweisungen dieses Abschnitts, um die ordnungsgemäße Funktion von GFI EndPointSecurity und der Standardschutzrichtlinie zu prüfen.

Themen in diesem Kapitel

3.1 Prüfungsvoraussetzungen

Die folgenden Prüfungsvoraussetzungen und Einstellungen werden NUR für diese Prüfung benötigt:

Geräteeinrichtung

Für die folgende Prüfung wird Folgendes benötigt:

» ein mit dem lokalen Computer verbundenes CD-/DVD-Laufwerk,

» eine CD/DVD mit zugänglichen Daten (vorzugsweise eine CD/DVD, auf die vor der Installation von GFI EndPointSecurity zugegriffen werden konnte).

Hinweis

Es können auch andere Geräte und Medien wie Disketten und Speichersticks verwendet werden.

Benutzerkonten

Für diese Prüfung müssen zwei Benutzerkonten auf demselben Computer eingerichtet sein, auf dem GFI EndPointSecurity installiert ist:

» ein Benutzerkonto ohne administrative Berechtigungen,

» ein Benutzerkonto mit administrativen Berechtigungen.

Konfigurationseinstellungen

Die Konfiguration des Schnellstart-Assistenten ermöglicht die Feinabstimmung von GFI EndPointSecurity, damit das Programm genau den Ansprüchen Ihres Unternehmen entspricht. Diese können natürlich von den für die Prüfung benötigten Einstellungen abweichen. Daher müssen einige Einstellungen von GFI EndPointSecurity wie folgt für die Prüfung angepasst werden:

» Stellen Sie sicher, dass der lokale Computer in der Anzeige **Status > Agenten** aufgelistet ist. Falls der lokale Computer nicht aufgelistet ist, fügen Sie ihn manuell hinzu. Weitere Informationen finden Sie im Administrations- und Konfigurationshandbuch von GFI EndPointSecurity.

» Stellen Sie sicher, dass die Standardschutzrichtlinie auf dem lokalen Computer bereitgestellt und auf dem neuesten Stand ist. Um dies zu kontrollieren, prüfen Sie unter **Status > Agenten** ob:

- die Schutzrichtlinie „Allgemeine Kontrolle“ lautet.

- die Bereitstellung auf dem neuesten Stand ist.
- der lokale Computer online ist.

> **Hinweis**
>
> Falls die Bereitstellung des Agenten auf dem lokalen Computer nicht auf dem neuesten Stand ist, führen Sie die Bereitstellung manuell durch. Weitere Informationen finden Sie im GFI-Konfigurations- und Administrationshandbuch.

» Stellen Sie sicher, dass das Benutzerkonto ohne administrative Berechtigungen für die Standardschutzrichtlinie „Allgemeine Kontrolle“ nicht als Hauptbenutzer festgelegt ist.

> **Hinweis**
>
> Falls das Benutzerkonto als Hauptbenutzer festgelegt ist, entfernen Sie es manuell aus der Hauptbenutzergruppe der Standardschutzrichtlinie „Allgemeine Kontrolle“. Weitere Informationen finden Sie im Administrations- und Konfigurationshandbuch von GFI EndPointSecurity.

3.2 Prüffall

Zugriff auf eine CD/DVD

Unter Beachtung der zuvor aufgeführten Prüfungsbedingungen haben nicht administrative Benutzer keinen Zugriff mehr auf Geräte oder Schnittstellen des lokalen Computers.

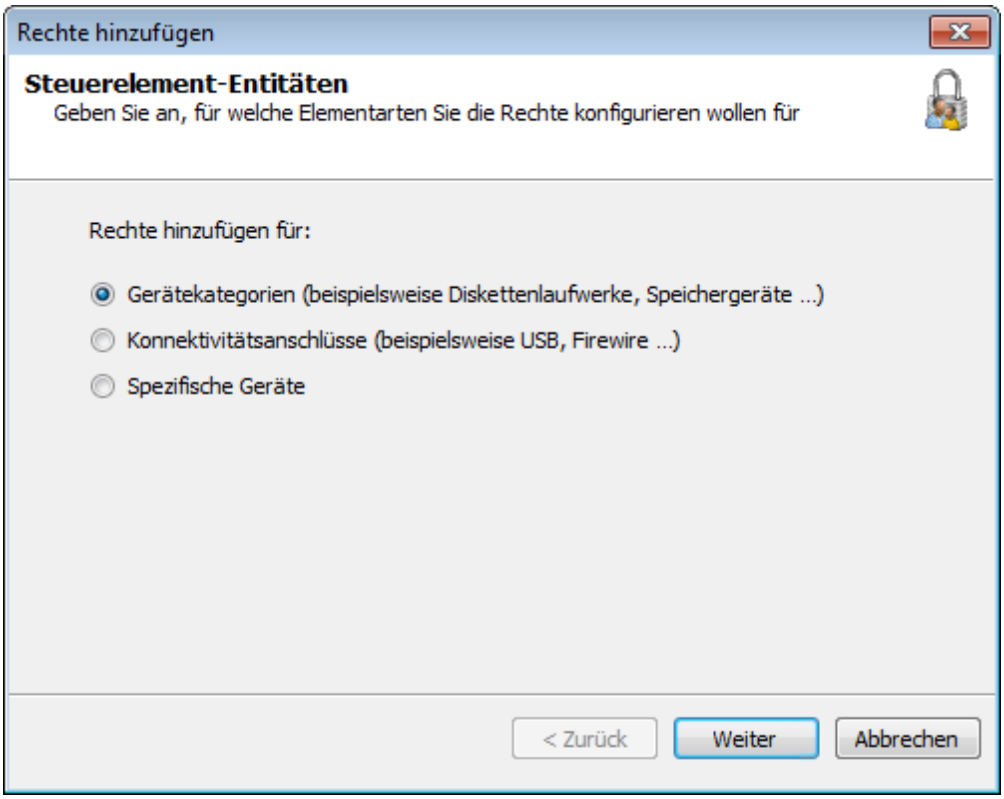
So prüfen Sie, ob der Zugriff auf das Gerät und das Medium für nicht administrative Benutzer möglich ist:

1. Melden Sie sich am lokalen Computer als Benutzer ohne administrative Berechtigungen an.
2. Legen Sie eine CD/DVD in das CD/DVD-Laufwerk ein.
3. Wählen Sie im **Windows Explorer** das CD/DVD-Laufwerk aus, und prüfen Sie, ob Sie die Inhalte der CD/DVD anzeigen oder öffnen können.

Zuweisen von Rechten an Benutzer ohne administrative Berechtigungen

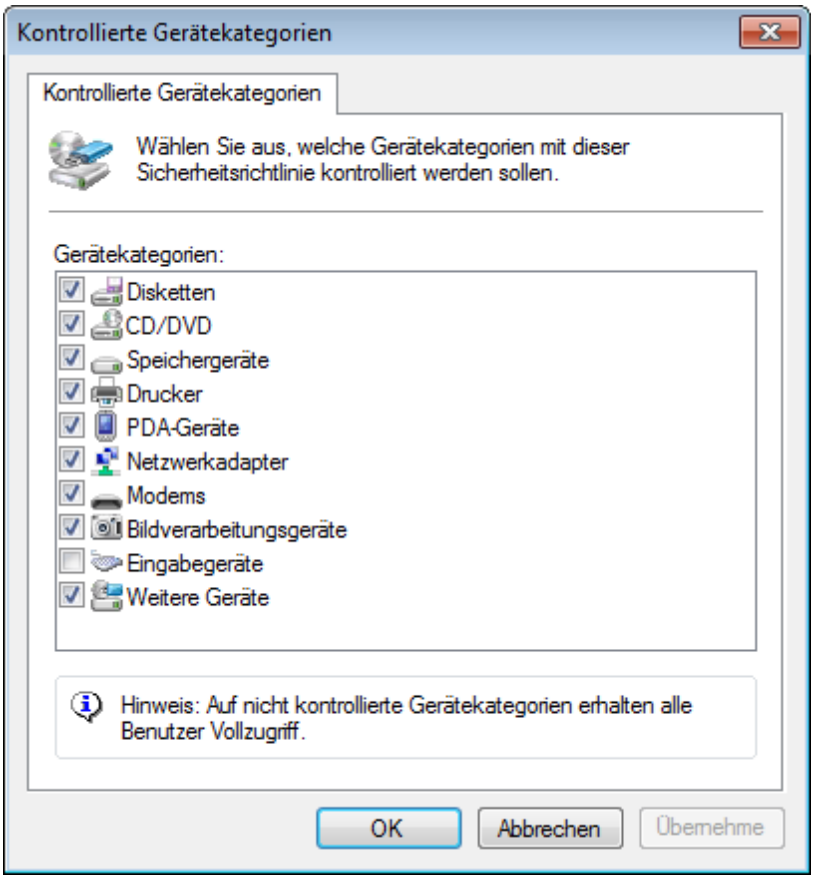
So weisen Sie einem Benutzer ohne administrative Berechtigungen Zugriffsrechte auf ein CD/DVD-Laufwerk zu:

1. Melden Sie sich am lokalen Computer als Benutzer mit administrativen Berechtigungen an.
2. Starten Sie GFI EndPointSecurity.
3. Klicken Sie auf die Registerkarte **Konfiguration**.
4. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.
5. Wählen Sie im linken Bereich die Schutzrichtlinie **Allgemeine Kontrolle** aus.
6. Klicken Sie auf den Unterknoten **Sicherheit**.
7. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Berechtigung (en) hinzufügen...**.



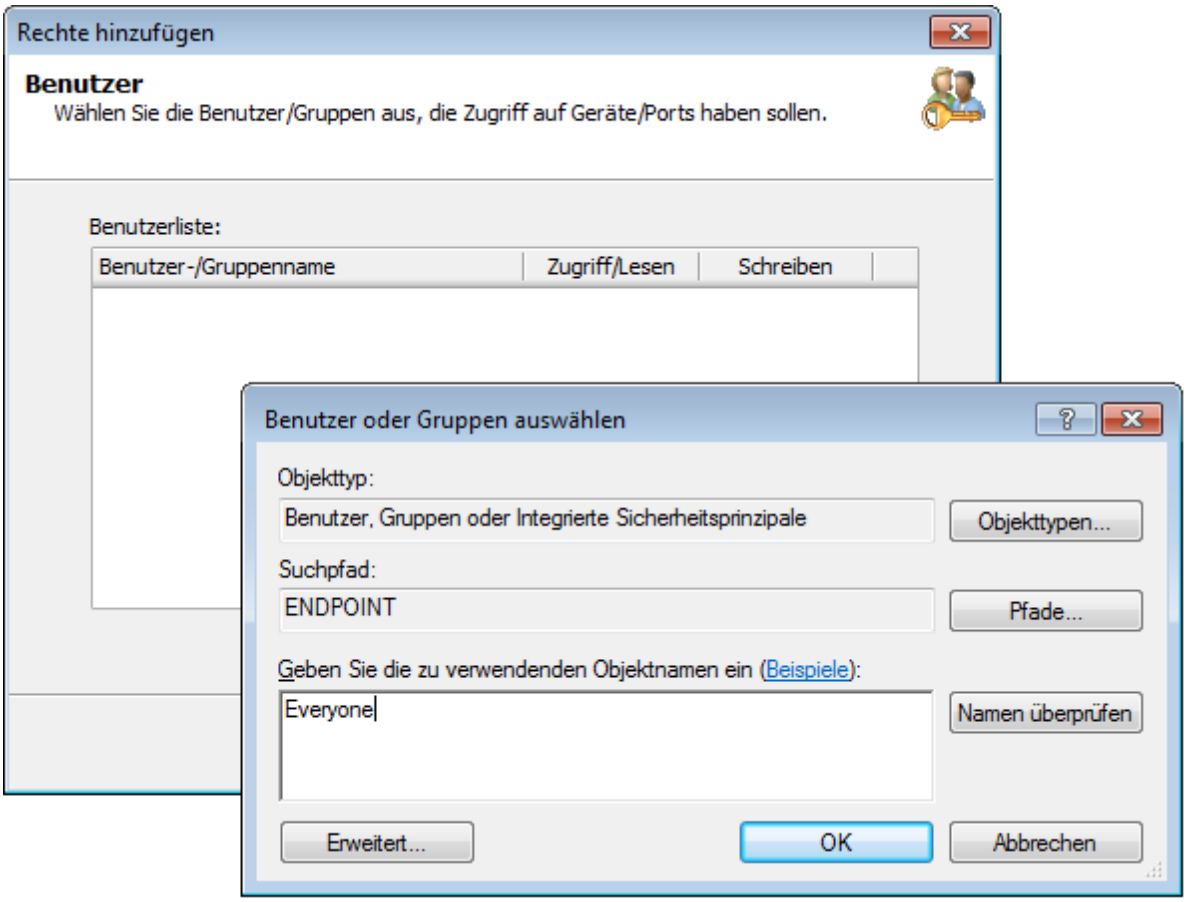
Screenshot 4: Steuerungsauswahl

8. Wählen Sie im Dialogfeld **Berechtigungen hinzufügen** die Option **Gerätekategorien** aus, und klicken Sie zum Fortfahren auf **Weiter**.



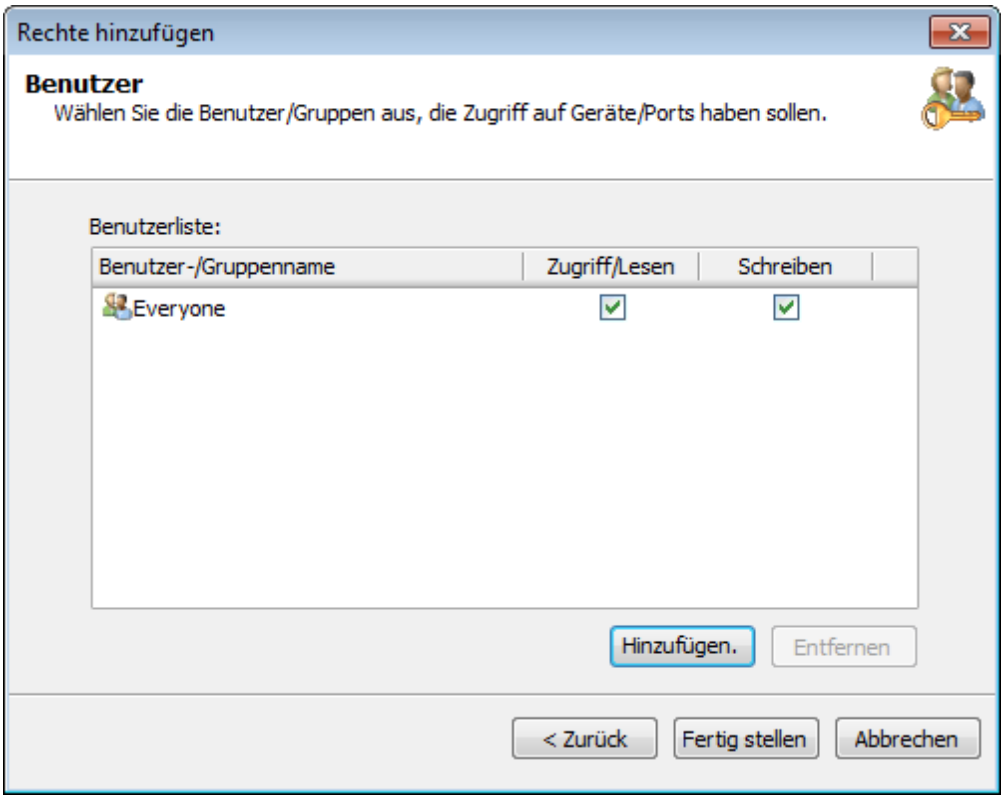
Screenshot 5: Auswahl der Gerätekategorien zur Zuweisung von Berechtigungen

9. Aktivieren Sie die Gerätekategorie **CD/DVD**, und klicken Sie auf **Weiter**.



Screenshot 6: Hinzufügen von Benutzern oder Gruppen

10. Klicken Sie auf **Hinzufügen**, und wählen Sie den Benutzer ohne administrative Berechtigungen aus, um ihm Zugriff auf die in dieser Schutzrichtlinie festgelegte Gerätekategorie CD/DVD zu gewähren. Klicken Sie anschließend auf **OK**.



Screenshot 7: Auswahl der Berechtigungen für Benutzer oder Gruppen

11. Aktivieren Sie die Berechtigungen **Zugriff/Lesen** und **Schreiben**. Klicken Sie anschließend auf **Fertig stellen**.

So stellen Sie Updates für Schutzrichtlinien auf dem lokalen Computer bereit:

1. Klicken Sie im rechten Bereich auf die oberste Warnmeldung, um die Updates für Schutzrichtlinien bereitzustellen. Die Ansicht sollte automatisch zu **Status > Bereitstellung wechseln**.

2. Überprüfen Sie im Bereich **Bereitstellungsverlauf** den erfolgreichen Abschluss der Aktualisierung auf dem lokalen Computer.

Erneuter Zugriff auf eine CD/DVD

Bei der Zuweisung von Benutzerberechtigungen sollte der Benutzer ohne administrative Berechtigungen nun Zugriff auf die CD/DVD im entsprechenden Laufwerk des lokalen Computers haben.

So prüfen Sie, ob der Zugriff auf das Gerät und das Medium nun für nicht administrative Benutzer möglich ist:

1. Melden Sie sich am lokalen Computer als Benutzer ohne administrative Berechtigungen an.

2. Legen Sie die gleiche CD/DVD in das CD/DVD-Laufwerk ein.

3. Wählen Sie im **Windows Explorer** das CD/DVD-Laufwerk aus, und prüfen Sie, ob Sie nun die Inhalte der CD/DVD anzeigen oder öffnen können.

3.3 Wiederherstellen der Standardeinstellungen

Um die Einstellungen von GFI EndPointSecurity auf den Zustand vor der Prüfung zurückzusetzen, muss für den Benutzer ohne administrative Berechtigungen Folgendes vorgenommen werden:

1. Entfernen Sie das Benutzerkonto vom lokalen Computer, falls dieses nur für die Prüfung erstellt wurde und nicht länger gebraucht wird.

2. Nehmen Sie den Benutzer manuell in die Hauptbenutzerliste auf, falls dieser vor der Prüfung ein Hauptbenutzer war. Weitere Informationen finden Sie im Administrations- und Konfigurationshandbuch von GFI EndPointSecurity.

3. Löschen Sie die Zugriffrechte des Benutzers auf das CD/DVD-Laufwerk, falls dieser vor der Prüfung keinen Zugriff darauf hatte. Weitere Informationen finden Sie im Administrations- und Konfigurationshandbuch von GFI EndPointSecurity.

4 Diverses

Dieses Kapitel beinhaltet alle Informationen, die nicht der Erstkonfiguration von GFI EndPointSecurity zugeordnet werden können.

Themen in diesem Kapitel

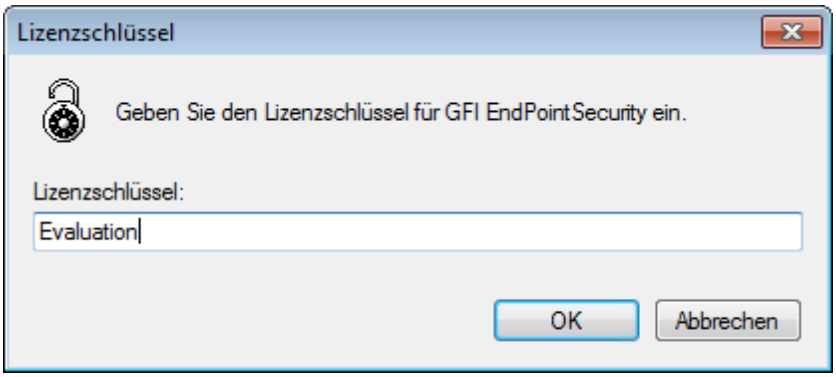
4.1 Produktlizenzierung

Nach der Installation von GFI EndPointSecurity können Sie den Lizenzschlüssel eingeben, ohne die Anwendung erneut zu installieren oder zu konfigurieren.

So geben Sie Ihren Lizenzschlüssel ein:

1. Klicken Sie auf die Registerkarte **Allgemein**.

2. Wählen Sie im linken Bereich die Option **Registrierung**.



Screenshot 8: Eingabe des Lizenzschlüssels

3. Klicken Sie im rechten Bereich auf **Bearbeiten…**

4. Geben Sie im Textfeld **Lizenzschlüssel** den Lizenzschlüssel ein, den Sie von GFI Software Ltd erhalten haben.

5. Klicken Sie auf **OK**, um den Lizenzschlüssel zu übernehmen.

4.2 Informationen zur Produktversion

GFI Software Ltd. veröffentlicht regelmäßig Produktaktualisierungen, die manuell oder automatisch von der GFI-Website heruntergeladen werden können.

So prüfen Sie, ob eine neuere Version von GFI EndPointSecurity zum Herunterladen verfügbar ist:

1. Klicken Sie auf die Registerkarte **Allgemein**.

2. Wählen Sie im linken Bereich **Versionsinformationen**.

3. Klicken Sie im rechten Bereich auf **Auf neuere Version prüfen**, um zu überprüfen, ob eine neuere Version von GFI EndPointSecurity zur Verfügung steht. Wählen Sie alternativ die Option **Bei Programmstart auf neuere Version prüfen**, um bei jedem Start von GFI EndPointSecurity automatisch zu prüfen, ob eine neuere Version zum Herunterladen verfügbar ist.

5 Fehlerbehebung und Support

In diesem Kapitel wird erklärt, wie bei der Installation von GFI EndPointSecurity auftretende Probleme behoben werden können. Die wichtigsten verfügbaren Informationsquellen zum Beheben dieser Probleme lauten wie folgt:

In diesem Abschnitt und in den anderen Kapiteln des GFI EndPointSecurityAdministratorhandbuch-s finden Sie Lösungen zu allen Problemen, die auftreten können. Wenden Sie sich an den GFI-Support, wenn Sie ein Problem nicht lösen können.

Häufige Probleme

In der folgenden Tabelle sind die am häufigsten auftretenden Probleme aufgeführt, die bei der Grundkonfiguration und erstmaligen Verwendung von GFI EndPointSecurity auftreten können, sowie mögliche Lösungen für die Probleme:

Tabelle 9: Fehlerbehebung - Häufige Probleme

Problem	Mögliche Ursache	Mögliche Lösung
Der Computer ist offline.	Die GFI EndPointSecurity-Verwaltungskonsole schickt bei der Bereitstellung einen Ping an den zu kontrollierenden Computer, um festzustellen, ob dieser online ist. Falls der Computer nicht online ist, wird diese Fehlermeldung angezeigt.	Falls ein zu kontrollierender Computer offline ist, erfolgt eine Stunde später automatisch ein erneuter Versuch. GFI EndPointSecurity versucht die Richtlinie so lange jede Stunde bereitzustellen, bis der zu kontrollierende Computer wieder online ist. Stellen Sie sicher, dass der kontrollierte Computer eingeschaltet und mit dem Netzwerk verbunden ist.
Es konnte keine Verbindung mit der Remoteregistrierung hergestellt werden. (Fehler)	GFI EndPointSecurity konnte keine Daten aus der Registry des kontrollierten Computers extrahieren.	Stellen Sie sicher, dass Ihre Firewall-Einstellungen die Kommunikation zwischen kontrollierten Computern und dem GFI EndPointSecurity-Server zulassen. Weitere Informationen finden Sie unter Systemanforderungen (page 8).
Erforderliche Informationen konnten nicht ermittelt werden. (Fehler)	GFI EndPointSecurity konnte keine Versionsdaten des zu kontrollierenden Computer extrahieren (Version des Betriebssystems und der Agentenversion von GFI EndPointSecurity).	Verwenden Sie die Systemfehlermeldung (in Klammern) für weitere Details zur Fehlerursache und einer möglichen Lösung.
Fehler beim Erstellen der erforderlichen Installationsdateien. (Fehler)	GFI EndPointSecurity konnte nicht die notwendigen Konfigurationsinformationen in die Bereitstellungsdatei (.msi-Installationsdatei) des GFI EndPointSecurity-Agenten einfügen. Dieser Fehler tritt auf, bevor die Bereitstellungsdatei auf den zu kontrollierenden Computer kopiert wird.	Verwenden Sie die Systemfehlermeldung (in Klammern) für weitere Details zur Fehlerursache und einer möglichen Lösung.

Problem	Mögliche Ursache	Mögliche Lösung
Fehler beim Kopieren der Dateien zur Remoteregistrierung. (Fehler)	GFI EndPointSecurity konnte die Bereitstellungsdatei (.msi-Installationsdatei) nicht auf den zu kontrollierenden Computer kopieren. Es kann sein, dass die administrative Freigabe (C$), die GFI EndPointSecurity für die Verbindung mit dem zu kontrollierenden Computer verwendet, deaktiviert ist.	Verwenden Sie die Systemfehlermeldung (in Klammern) für weitere Details zur Fehlerursache und einer möglichen Lösung. Weitere Informationen zur Netzwerkkonnektivität und zu Sicherheitsberechtigungen finden Sie unter: http://kb.gfi.com/articles/SkyNet_Article/KBID003754?retURL=%2Fapex%2FSupportHome&popup=true
Zeitüberschreitung	Die Bereitstellung des Agenten auf dem zu kontrollierenden Computer dauert entweder zu lange oder wird blockiert.	Versuchen Sie erneut, den GFI EndPointSecurity-Agenten bereitzustellen.
Fehler bei der Installation des Bereitstellungsdienstes. (Fehler)	Der GFI EndPointSecurity-Agent konnte aufgrund eines ausgeführten Dienstes auf dem zu kontrollieren Computer nicht installiert/deinstalliert werden.	Verwenden Sie den Systemfehler (in Klammern) für weitere Details zur Fehlerursache und einer möglichen Lösung.
Installation fehlgeschlagen.	Die Installation des GFI EndPointSecurity-Agenten wurde abgeschlossen, wird aber nicht als installiert in der Registry gekennzeichnet. Die Versions- und Build-Nummer des GFI EndPointSecurity-Agenten entsprechen nicht der Versions- und Build-Nummer der GFI EndPointSecurity-Verwaltungskonsole.	Konsultieren Sie die Installationsprotokolldateien des Agenten auf dem zu kontrollierenden Computer für weitere Details zur Fehlerursache und einer möglichen Lösung: **%windir%\EndPointSecurity**.
Deinstallation fehlgeschlagen.	Die Deinstallation des GFI EndPointSecurity-Agenten wurde abgeschlossen, wird aber nicht als deinstalliert in der Registry gekennzeichnet.	Konsultieren Sie die Installationsprotokolldateien des Agenten auf dem zu kontrollierenden Computer für weitere Details zur Fehlerursache und einer möglichen Lösung: **%windir%\EndPointSecurity**.
Der Vorgang ist aufgrund einer unbekannten Ausnahme fehlgeschlagen.	GFI EndPointSecurity hat einen unerwarteten Fehler erkannt.	Verwenden Sie den Problembehandlungs-Assistenten, um den technischen Support von GFI zu kontaktieren. Klicken Sie zum Öffnen des Problembehandlungs-Assistenten auf **Start > Programme > GFI EndPointSecurity 2013 > GFI EndPointSecurity 2013 Problembehandlung**.

Verwenden des GFI EndPointSecurity-Tools zur Problembehandlung

So verwenden Sie das Tool zur Problembehandlung von GFI EndPointSecurity:

1. Klicken Sie auf **Start > Programme >GFI EndPointSecurity 2013 > GFI EndPointSecurity 2013 Problembehandlung**.

2. Klicken Sie auf dem Willkommensbildschirm des Assistenten auf **Weiter**.

Screenshot 9: Geben Sie Details zum Kontakt und zum Kauf an.

3. Geben Sie Ihre Kontaktdetails ein, sodass das Support-Team Sie erreichen kann, wenn es weitere Informationen zur Analyse benötigt. Klicken Sie auf **Weiter**.

Screenshot 10: Geben Sie Fehlerdetails und weitere relevante Informationen an, die zum Reproduzieren des Problems erforderlich sind.

4. Geben Sie Fehlermeldungen und sonstige Informationen an, die dem Support-Team beim Reproduzieren des Problems helfen. Klicken Sie auf **Weiter**.

Screenshot 11: Erfassung der Computerinformationen

5. Das Problembehandlungs-Tool untersucht Ihr System, um die erforderlichen Hardwareinformationen zu erfassen. Sie können in dem zur Verfügung stehenden Feld manuell weitere Informationen eingeben oder auf **Weiter** klicken.

Screenshot 12: Abschließen des Problembehandlungs-Assistenten

6. An diesem Punkt wird vom Problembehandlungs-Assistenten ein Paket mit den Informationen zusammengestellt, die in den vorherigen Schritten erfasst wurden. Senden Sie als nächstes dieses

Paket an unser Support-Team, damit sie mit der Analyse des Problems und der Fehlerbehebung beginnen können. Klicken Sie auf die unten beschriebenen Schaltflächen mit weiteren Optionen zum Sendevorgang:

» **Inhaltsordner öffnen** – Öffnet den Ordner mit dem Paket für die Problembehandlung, sodass Sie das Paket manuell per E-Mail senden können.

» **GFI-Support** – Öffnet die Support-Seite der GFI-Website.

7. Klicken Sie auf **Fertig stellen**.

GFI SkyNet

GFI pflegt ein umfangreiches Knowledge Base-Repository, in dem Lösungen für die häufigsten Probleme beschrieben sind. GFI SkyNet enthält immer die aktuelle Liste der Fragen, die an den technischen Support gerichtet wurden, sowie die neuesten Patches. Wenn die Informationen in dieser Anleitung nicht ausreichen, um Ihre Probleme zu lösen, sehen Sie bitte unter GFI SkyNet nach: http://kb.gfi.com/.

Webforum

Über das GFI-Webforum erhalten Sie technischen Support von Benutzer zu Benutzer. Zum Webforum gelangen Sie über folgende URL-Adresse: http://forums.gfi.com/.

Technischen Support anfragen

Wenn Sie mit keiner der oben angegebenen Ressourcen Ihre Probleme beheben können, wenden Sie sich bitte an das technische Supportteam von GFI. Füllen Sie dazu ein Online-Support-Formular aus, oder rufen Sie an.

» **Online**: Füllen Sie das Anfrageformular für den Support aus, und befolgen Sie genau die Anweisungen auf dieser Seite, um Ihre Support-Anfrage unter folgendem Link zu übermitteln: http://support.gfi.com/supportrequestform.asp.

» **Telefon**: Die korrekte Telefonnummer für den technischen Support Ihrer Region finden Sie unter: http://www.gfi.com/company/contact.htm.

> **HINWEIS**
>
> Halten Sie bitte Ihre Kundennummer bereit, wenn Sie sich an den technischen Support wenden. Ihre Kundennummer entspricht der Online-Kontonummer, die Sie bei der ersten Registrierung Ihrer Lizenzschlüssel im GFI-Kundenbereich unter folgendem Link erhalten haben: http://customers.gfi.com.

Für die Beantwortung Ihrer Anfrage benötigt GFI je nach Ihrer Zeitzone maximal 24 Stunden.

Dokumentation

Wenn dieses Handbuch Ihren Erwartungen nicht entspricht oder Sie der Meinung sind, dass die Dokumentation verbessert werden kann, senden Sie uns bitte eine E-Mail an: documentation@gfi.com.

6 Glossar

A

Active Directory

Eine Technologie, die verschiedene Netzwerkdienste bereitstellt (darunter LDAP-ähnliche Verzeichnisdienste).

Administratorkonto für Warnungen

Ein Warnungsempfängerkonto, das automatisch nach der Installation von GFI EndPointSecurity erstellt wird.

Assistent zur Erstellung von Schutzrichtlinien

Ein Assistent für die Erstellung und Konfiguration von neuen Schutzrichtlinien. Konfigurationseinstellungen beinhalten die Auswahl von zu kontrollierenden Gerätekategorien und Schnittstellen sowie die Festlegung, ob diese zugängig oder blockiert sind. Dieser Assistent ermöglicht außerdem die Konfiguration von Dateitypfiltern, von Verschlüsselungsberechtigungen sowie von Protokollierungs- und Warnoptionen.

Automatische Erkennung

Eine zeitgesteuerte GFI EndPointSecurity-Funktion zur Suche und Erkennung von Computern, die neu im Netzwerk angeschlossen wurden.

B

Benutzerbenachrichtigung

Eine Nachricht, die von GFI EndPointSecurity-Agenten auf kontrollierten Computern angezeigt wird, wenn ein Zugriff auf Geräte erfolgt.

Bereitstellungsfehlermeldungen

Fehler, die nach der Bereitstellung der GFI EndPointSecurity-Agenten durch die GFI EndPointSecurity-Verwaltungskonsole auftreten können.

BitLocker To Go

Eine Funktion von Microsoft Windows 7 zum Schutz und zur Verschlüsselung von Daten auf Wechseldatenträgern.

D

Dateitypfilter

Ein Satz von Einschränkungen, die Benutzer und Gruppen auf Dateitypbasis zugewiesen werden. Die Filterung basiert auf der Überprüfung von Dateierweiterungen und Signatur des wahren Dateityps.

Datenbank-Backend

Eine von GFI EndPointSecurity genutzte Datenbank, in der alle Ereignisse, die von GFI EndPointSecurity-Agenten auf kontrollierten Computern erzeugt wurden, in der Form eines Überwachungspfads gespeichert werden.

E

Eingabegeräte

Eine Spezifikation, die Teil des Universal Serial Bus (USB)-Standards für eine Klasse von Peripheriegeräten ist. Diese Geräte, wie Mäuse, Tastaturen und Joysticks, ermöglichen dem Benutzer die Eingabe von Daten oder die direkte Interaktion mit dem Computer.

Ereignisprotokollierung

Eine GFI EndPointSecurity-Funktion, die auf kontrollierten Computern alle Ereignisse zu Zugriffsversuchen auf Geräte und Schnittstellen erfasst.

G

Geräte-Blacklist

Eine Liste einzelner Geräte, deren Zugriff auf kontrollierten Computern blockiert wird, die der Schutzrichtlinie angehören.

Gerätekategorie

Eine Gruppe von Peripheriegeräten, die in einer Kategorie verwaltet werden.

Gerätescan

Eine GFI EndPointSecurity-Funktion, zur Suche aller Geräte, die an kontrollierten Computern angeschlossen sind und waren.

Geräte-Whitelist

Eine Liste einzelner Geräte, deren Zugriff auf kontrollierten Computern zugelassen wird, die der Schutzrichtlinie angehören.

GFI EndPointSecurity-Agent

Ein Agent auf den zu kontrollierenden Computern, der dafür sorgt, dass die Schutzrichtlinien auf diesem/diesen kontrollierten Computer(n) eingerichtet und durchgesetzt werden.

GFI EndPointSecurity-Anwendung

Eine Sicherheitsanwendung auf dem Server, die die Integrität von Daten sichert und den unautorisierten Zugriff auf tragbare Speichermedien sowie den Datenaustausch auf und von Hardware und Schnittstellen verhindert.

GFI EndPointSecurity-Verwaltungskonsole

Die Benutzeroberfläche der GFI EndPointSecurity-Anwendung auf dem Server.

Globale Berechtigungen

Ein Schritt innerhalb des Assistenten zur Erstellung von Schutzrichtlinien, der den Benutzer auffordert, den Zugriff auf alle Geräte zu gewähren oder zu blockieren, die einer Kategorie angehören oder die an eine Schnittstelle eines kontrollierten Computers angeschlossen sind, der durch die Schutzrichtlinie kontrolliert wird.

GPO

Siehe Gruppenrichtlinienobjekte.

Gruppenrichtlinienobjekte

Ein zentrales Verwaltungs- und Konfigurationssystem für Active Directory, mit dem festgelegt wird, was Benutzern in einem Computernetzwerk erlaubt und untersagt ist.

H

Hauptbenutzer

Ein Hauptbenutzer besitzt automatisch vollen Zugriff auf alle Geräte, die am von der Schutzrichtlinie kontrollierten Computer angeschlossen sind.

K

Kontrollierter Computer

Ein Computer, der durch eine GFI EndPointSecurity-Schutzrichtlinie geschützt wird.

M

MSI-Datei

Eine von GFI EndPointSecurity generierte Datei für die spätere Bereitstellung mithilfe von Gruppenrichtlinienobjekten oder anderen Bereitstellungsoptionen. Diese Datei kann für alle Schutzrichtlinien generiert werden und enthält alle konfigurierten Sicherheitseinstellungen. Dazu gehören auch Installationseinstellungen für ungeschützte kontrollierte Computer.

S

Schnellstart-Assistent

Ein Assistent für die benutzerdefinierte Konfiguration von GFI EndPointSecurity. Er wird beim ersten Start der GFI EndPointSecurity-Verwaltungskonsole automatisch gestartet.

Schnittstelle

Eine Schnittstelle zwischen Computern und Geräten.

Schutzrichtlinie

Ein Berechtigungssatz für den Zugriff auf Geräte und Schnittstellen, der unternehmensspezifisch konfiguriert werden kann.

Sicherheitsverschlüsselung

Ein Einschränkungssatz, der Benutzern/Gruppen den Zugriff auf Dateitypen gewährt oder blockiert, die mit BitLocker To Go verschlüsselt auf Geräten gespeichert sind. Diese Einschränkungen werden angewendet, wenn verschlüsselte Geräte an die durch die Schutzrichtlinie kontrollierten Computer angeschlossen werden.

T

Temporary Access-Tool von GFI EndPointSecurity

Ein Tool auf kontrollierten Computern. Es wird vom Benutzer dafür verwendet, einen Anfragecode zu generieren und später einen Entsperrcode einzugeben, um einen zeitlich begrenzten Zugriff zu aktivieren, sobald dieser vom Administrator gewährt wird. Bei Aktivierung hat

der Benutzer auf seinem kontrollierten Computer für eine bestimmte Dauer und ein bestimmtes Zeitfenster Zugriff auf Geräte und Schnittstellen (wenn der Zugriff normalerweise blockiert wird).

Ü

Übersichtsbericht

Eine zusammenfassender Bericht mit statistischen Daten zur von GFI EndPointSecurity erfassten Kontoaktivität.

W

Warnungen

Benachrichtigungen (E-Mail-Warnungen, Netzwerknachrichten oder SMS-Nachrichten), die beim Auftreten eines bestimmten Ereignisses an Warnungsempfänger gesendet werden.

Warnungsempfänger

Ein GFI EndPointSecurity-Profilkonto, das die Kontaktdetails von Benutzern enthält, die E-Mail-Warnungen und Netzwerk- bzw. SMS-Nachrichten erhalten sollen.

Z

Zeitlich begrenzter Zugriff

Ein Zeitraum, in dem Benutzern der Zugriff auf Geräte und Schnittstellen auf kontrollierten Computern (wenn der Zugriff normalerweise blockiert wird) gewährt wird.

Zugriffsberechtigungen

Berechtigungen (Zugriff, Lesen und Schreiben), die Benutzern und Gruppen pro Gerätekategorie, Schnittstelle oder einem einzelnen Gerät zugewiesen werden.

7 Index

USA, KANADA, MITTEL- UND SÜDAMERIKA

4309 Emperor Blvd, Suite 400, Durham, NC 27703, USA

Telefon: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

GROSSBRITANNIEN UND IRLAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telefon: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPA, MITTLERER OSTEN UND AFRIKA

GFI House, Territorials Street, Mriehel, BKR 3000, Malta

Telefon: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIEN UND NEUSEELAND

83 King William Road, Unley 5061, South Australia

Telefon: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI®