GFI-Produkthandbuch

GFI EndPointSecurity™

Administratorhandbuch

Die Informationen in diesem Dokument dienen ausschließlich Informationszwecken und werden in der vorliegenden Form ohne (ausdrückliche oder stillschweigende) Haftung jeglicher Art bereitgestellt, insbesondere ohne Gewährleistung der Marktgängigkeit, der Eignung für einen bestimmten Zweck oder der Nichtverletzung von Rechten. GFI Software haftet nicht für etwaige Schäden, einschließlich Folgeschäden, die sich aus der Nutzung dieses Dokuments ergeben. Die Informationen stammen aus öffentlich zugänglichen Quellen. Trotz sorgfältiger Prüfung der Inhalte übernimmt GFI keine Haftung für die Vollständigkeit, Richtigkeit, Aktualität und Eignung der Daten. Des Weiteren ist GFI nicht für Druckfehler, veraltete Informationen und Fehler verantwortlich. GFI übernimmt keine Haftung (ausdrücklich oder stillschweigend) für die Richtigkeit oder Vollständigkeit der in diesem Dokument enthaltenen Informationen.

Nehmen Sie mit uns Kontakt auf, wenn Ihnen in diesem Dokument Sachfehler auffallen. Wir werden Ihre Hinweise sobald wie möglich berücksichtigen.

Alle hier aufgeführten Produkte und Firmennamen sind Marken der jeweiligen Eigentümer.

GFI EndPointSecurity unterliegt dem urheberrechtlichen Schutz von GFI SOFTWARE LTD. – 1999-2013GFI Software Ltd. Alle Rechte vorbehalten.

Dokumentenversion: 1.1.1

Zuletzt aktualisiert (Monat/Tag/Jahr): 1/28/2014

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

Durch die zunehmende Verbreitung von Verbrauchergeräten wie iPods, USB-Geräten und Smartphones erhöhte sich das Risiko bewusster und/oder unbeabsichtigter Datenlecks und anderer illegaler Aktivitäten. 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 einzuschmuggeln. Mit GFI EndPointSecurity können Sie diese Bedrohungen schnell und einfach bekämpfen, ohne dass Sie alle Anschlüsse sperren und die tägliche Abläufe einschränken müssen.

Themen in diesem Kapitel

1.1 Begriffe und Konventionen dieses Handbuchs

Tabelle 1: Begriffe und Konventionen dieses Handbuchs

Begriff	Beschreibung
	Zusätzliche Informationen und Referenzen, die für die ordnungsgemäße Funktion von GFI EndPointSecurity wichtig sind.
	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. benut-zerdefinierte Pfade und Dateinamen.
`Code`	Einzugebende Textwerte, z. B. Befehle und Adressen.

1.2 Tragbare Speichermedien und ihre Gefahren

Der Hauptvorteil von tragbaren Speichermedien besteht in ihrer einfachen Handhabung und der schnellen Zugänglichkeit. Theoretisch ist dies ein großer Vorteil für Organisationen. Es zeigt sich

jedoch auch immer wieder, dass ein Datentransfer auf diesem Weg auf Kosten der Sicherheit geht, sofern keine Schutzmaßnahmen implementiert sind.

Die Entwicklung tragbarer Speichermedien schreitet rasant voran. Verschiedene Versionen tragbarer Speichermedien, wie Flashspeicher, haben sich hinsichtlich Folgendem verbessert:

- Höhere Speicherkapazität
- Verbesserte Leistung
- Einfachere und schnellere Installation
- Kompakte Abmaße, die für höchste Mobilität sorgen.

Netzwerkinterne Benutzer können somit (ob nun wissentlich oder unabsichtlich):

- vertrauliche Daten entwenden,
- vertrauliche Daten veröffentlichen,
- bösartigen Code einschleppen (z. B. Viren oder Trojaner), der den gesamten Netzwerkbetrieb zum Erliegen bringt,
- unerwünschte oder beleidigende Inhalte auf Unternehmensrechner übertragen,
- persönliche Kopien von Unternehmensdaten und geistigem Eigentum anfertigen und
- von produktivem Arbeiten abgehalten werden.

Mehr und mehr Firmen stellen Richtlinien auf, die den Einsatz (privater) tragbarer Speichermedien am Arbeitsplatz verbieten sollen. In der Praxis zeigt sich, das man sich nicht auf eine freiwillige Einhaltung durch die Mitarbeiter verlassen kann. Nur durch den Einsatz technologischer Sperren lässt sich die Verwendung tragbarer Medien im Netzwerk umfassend kontrollieren.

1.3 Informationen zu GFI EndPointSecurity

GFI EndPointSecurity sichert die Integrität von Daten und verhindert den unautorisierten Zugriff auf tragbare Speichermedien sowie den Datenaustausch auf und von folgender Hardware oder Schnittstellen:

- USB-Anschlüsse (z. B. Speicherkartenleser und USB-Sticks)
- FireWire-Anschlüsse (z. B. Digitalkameras, FireWire-Kartenleser)
- Funkschnittstellen (z. B. Bluetooth- und Infrarot-Dongle)
- Diskettenlaufwerke (intern und extern)
- Optische Laufwerke (z. B. CD, DVD)
- Optische MO-Laufwerke (intern und extern)
- USB-Festplattenlaufwerke
- Andere Laufwerke wie Zip- und Bandlaufwerke (intern und extern).

GFI EndPointSecurity ermöglicht es Ihnen, den Zugriff zu erlauben oder zu sperren und darüber hinaus volle Zugriffsrechte oder nur Leserechte zu erteilen für:

- Geräte (z. B. CD-/DVD-Laufwerke, PDAs)
- Lokale oder Active Directory-Benutzer/-Benutzergruppen.

Der Zugriff auf sämtliche mobile Geräte, die an kontrollierte Computer angeschlossen werden, lässt sich zudem mit Informationen zu Datum und Uhrzeit der Verwendung sowie zum Gerätebenutzer protokollieren.

1.4 Komponenten von GFI EndPointSecurity

Bei der Installation von GFI EndPointSecurity werden folgende Komponenten eingerichtet:

» GFI EndPointSecurity-Verwaltungskonsole Verwaltungskonsole

» GFI EndPointSecurity-Agent.

1.4.1 GFI EndPointSecurity-Verwaltungskonsole

Mithilfe der 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.

1.4.2 GFI EndPointSecurity-Agent

Der Agent von GFI EndPointSecurity sorgt dafür, dass die Schutzrichtlinien auf dem/den zu kontrollierenden Computer(n) 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.

1.5 Hauptfunktionen

GFI EndPointSecurity enthält folgende Hauptfunktionen:

Tabelle 2: GFI EndPointSecurity-Funktionen

GFI EndPointSecurity-Funktionen	
Gruppenbasierter Zugriffsschutz	GFI EndPointSecurity erlaubt es Ihnen, Computer in Gruppen einzuteilen, für die eigene Schutzrichtlinien definiert sind. Richtlinieneinstellungen gelten übergreifend für alle Mitglieder einer Gruppe.
Differenzierte Zugriffskontrolle	Mit GFI EndPointSecurity können Sie ausgewählten Netzwerkbenutzern den Zugriff auf ein bestimmtes Einzelgerät erlauben oder untersagen. Erteilen Sie zudem für alle freigegebenen Geräte (z. B. CD/DVD-Laufwerke, PDAs) je nach Benutzer lediglich Lese- oder auch Vollzugriffsrechte.
Geplante Bereitstellungen	GFI EndPointSecurity ermöglicht die Planung der Bereitstellung von Schutzrichtlinien und die Änderung verwandter Konfigurationen, ohne dass die GFI EndPointSecurity-Verwaltungskonsole geöffnet werden muss. Die Bereitstellungsfunktion steuert auch fehlgeschlagene Bereitstellungen durch eine automatische Neuplanung.

GFI EndPointSecurity-Funktionen	
Zugriffskontrolle	GFI EndPointSecurity erlaubt es Ihnen, den Zugriff nicht nur unter Berücksichtigung einzelner Gerätekategorien zu sperren, sondern auch über: » **Dateityp** – Benutzer dürfen beispielsweise Dateien im doc-Format öffnen, exe-Dateien sind jedoch gesperrt. » **Physische Schnittstelle** – Alle Geräte, die über physische Schnittstellen wie USB angeschlossen sind. » **Gerätekennung** – Unter Berücksichtigung der eindeutigen Hardware-ID kann der Zugriff für ein einzelnes Gerät unterbunden werden. **HINWEIS** Unter Microsoft Windows 7 kann die Funktion BitLocker To Go verwendet werden, um Daten auf Wechseldatenträgern zu verschlüsseln und zu schützen. GFI EndPointSecurity überprüft gültige Dateitypen, die mit BitLocker To Go von Windows 7 verschlüsselt wurden.
Geräte-Whitelist und -Blacklist	Administratoren können einzelne Geräte, die stets oder nie zugänglich sein dürfen, auf eine Whitelist bzw. Blacklist setzen.
Hauptbenutzer	Administratoren können Benutzer oder Gruppen festlegen, die auf Geräte, die ansonsten durch GFI EndPointSecurity blockiert sind, stets Vollzugriff haben.
Zeitlich begrenzter Zugriff	Administratoren haben die Möglichkeit, auf einem bestimmten Computer den Zugriff auf ein tragbares Gerät oder eine Gerätegruppe zeitlich begrenzt zu gestatten. Mithilfe eines speziell erstellten Entsperrcodes kann ein Mitarbeiter mit dieser Funktion somit innerhalb einer festgelegten Frist ein für seinen Computer zuvor gesperrtes Gerät oder eine Schnittstelle nutzen, selbst wenn der Agent von GFI EndPointSecurity keine Verbindung mit dem Netzwerk hält.
Statusanzeige	Die Benutzeroberfläche des Dashboards zeigt den Status von bereitgestellten Agenten zum Zugriffsschutz, der Datenbank und Warnservern, des GFI EndPointSecurity-Dienstes sowie grafisch aufbereitete statistische Daten an. Der aktuelle Status sämtlicher bereitgestellter Agenten zum Zugriffsschutz wird von der Hauptanwendung kontinuierlich überprüft. Wartungsaufgaben werden automatisch durchgeführt, sobald ein Agent online ist.
Active Directory-Bereitstellung per MSI	Über die GFI EndPointSecurity-Verwaltungskonsole lässt sich eine MSI-Datei erstellen, die später mithilfe der Active Directory-Funktion für Gruppenrichtlinienobjekte oder mithilfe anderer Bereitstellungsoptionen bereitgestellt werden kann. Eine MSI-Datei umfasst alle in einer einzelnen Schutzrichtlinie festgelegten Sicherheitseinstellungen.
Kennwortgeschützte Verwaltung von Agenten	Funktionen zur Verwaltung von Agenten (z. B. zur Aktualisierung oder Deinstallation) sind über ein individuell festlegbares Kennwort geschützt. Andere Instanzen von GFI EndPointSecurity können agentenspezifische Verwaltungsoptionen somit nicht aufrufen.
Geräteerkennung	Das GFI EndPointSecurity-Modul dient dem Scannen und Erkennen von mobilen Geräten im Netzwerk, selbst auf Computern, die keiner Schutzrichtlinie zugewiesen sind. Unter Verwendung der gewonnenen Daten über erkannte Geräte lassen sich für einzelne Geräte Sicherheitsrichtlinien erstellen und Zugriffsrechte zuweisen.
Protokoll-Browser	Administratoren können mit dem integrierten Tool die von GFI EndPointSecurity im Datenbank-Backend aufgezeichneten Protokolle zur Benutzeraktivität und Geräteverwendung anzeigen.
Ausgabe von Warnungen	GFI EndPointSecurity ermöglicht es Ihnen, E-Mail-Warnungen, Netzwerkmeldungen und SMS-Nachrichten zu konfigurieren, die an angegebene Empfänger gesendet werden, wenn Geräte angeschlossen/getrennt werden, wenn der Gerätezugriff zugelassen oder blockiert wird und nach diensterstellten Ereignissen.
Anpassbare Popup-Meldungen	Wird Benutzern beispielsweise der Zugang zu einem Gerät verwehrt, werden sie durch eine Popup-Meldung über die Sperrung informiert. GFI EndPointSecurity ermöglicht die Anpassungen dieser Meldungen.
Datenbankwartung	Zur Kontrolle der Größe des Datenbank-Backends kann GFI EndPointSecurity so konfiguriert werden, dass Ereignisse, die älter als ein festgelegter Zeitraum sind, gesichert oder gelöscht werden.

GFI EndPointSecurity-Funktionen	
Geräteverschlüsselung	Für eine maximale Sicherheit kann GFI EndPointSecurity so konfiguriert werden, dass Speichergeräte mithilfe der AES 256-Verschlüsselung verschlüsselt werden. Durch die Ausführung von Agenten im Netzwerk kann die Verschlüsselung auf bestimmten Geräten erzwungen werden.
Bewertung des Datenleck-Risikos	Über das Dashboard können Benutzer das potentielle Datenleck-Risiko für jeden Endpunkt anzeigen. Nutzen Sie die bereitgestellten Tipps, und führen Sie die vorgeschlagenen Aktionen aus, um die Risikostufen zu verringern.
Inhaltsprüfung	Mit der Inhaltsprüfung können Benutzer in Dateien schauen, welche die Endpunkte über Wechseldatenträger passieren. Der Inhalt wird basierend auf vordefinierten (oder benutzerdefinierten) regulären Ausdrücken und Wörterbuchdateien identifiziert. Die Funktion sucht standardmäßig nach geschützten, vertraulichen Informationen wie Kennwörtern und Kreditkartennummern.

1.6 Funktionsweise von GFI EndPointSecurity – Bereitstellung und Überwachung

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

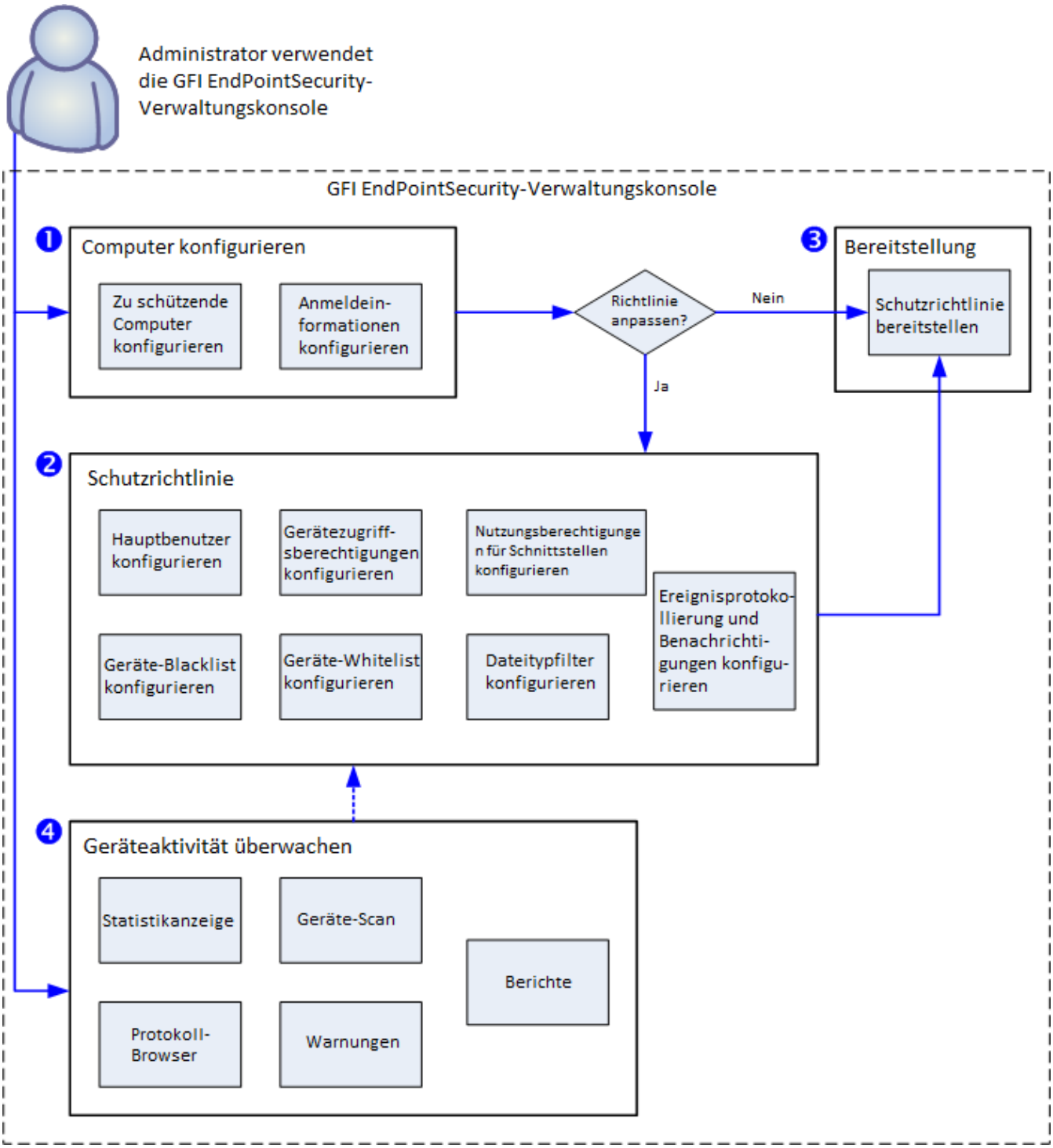


Abbildung 1: Schutzrichtlinie - Bereitstellung und Überwachung

In der folgenden Tabelle werden die oben abgebildeten Phasen beschrieben.

Tabelle 3: 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.

1.7 Funktionsweise von GFI EndPointSecurity - Gerätezugriff

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

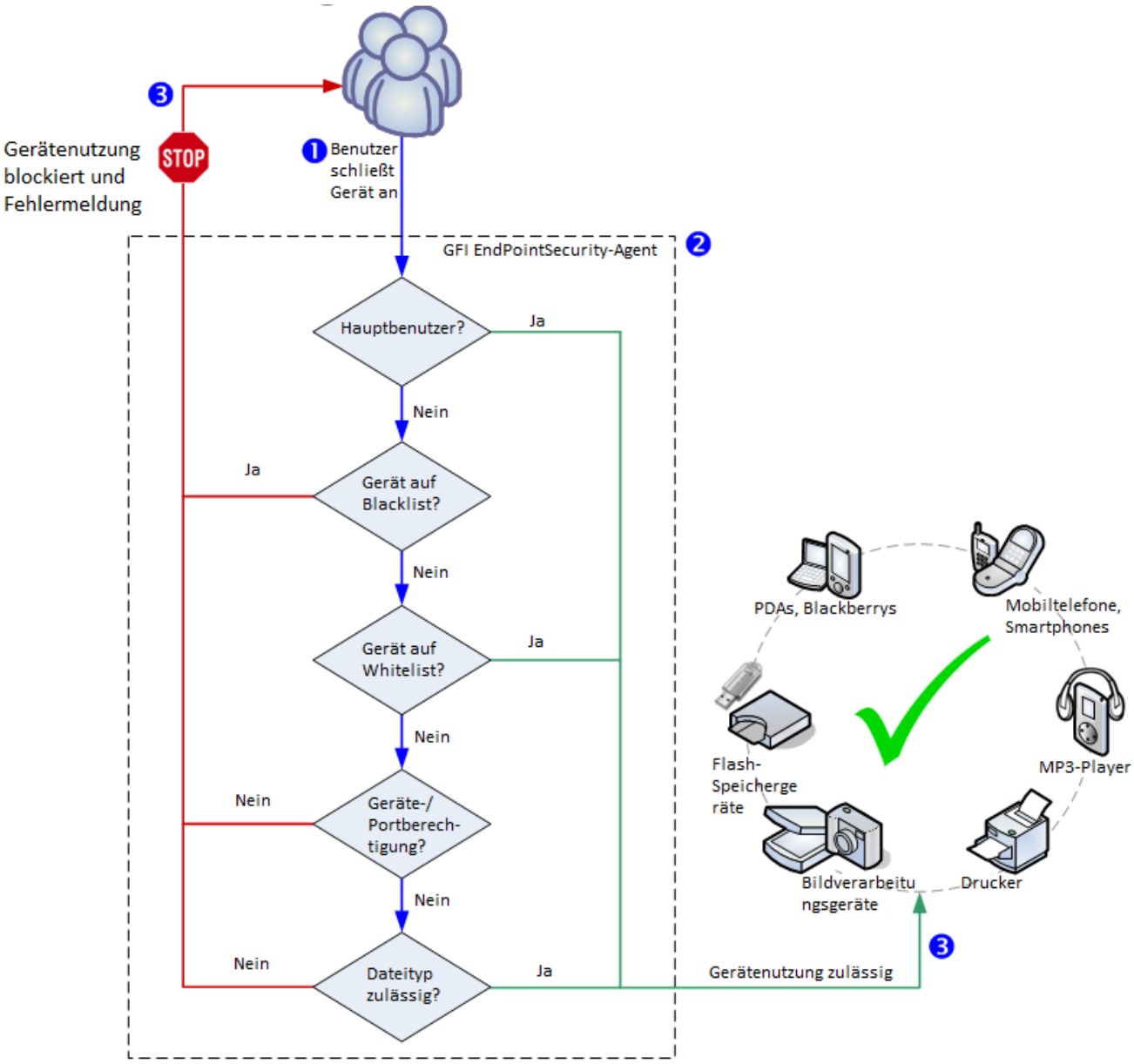


Abbildung 2: Gerätezugriff

In der folgenden Tabelle werden die oben abgebildeten Phasen beschrieben.

Tabelle 4: 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 blockiert wurde, oder der Zugriff wird zugelassen.

1.8 Funktionsweise von GFI EndPointSecurity - Zeitlich begrenzter Zugriff

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

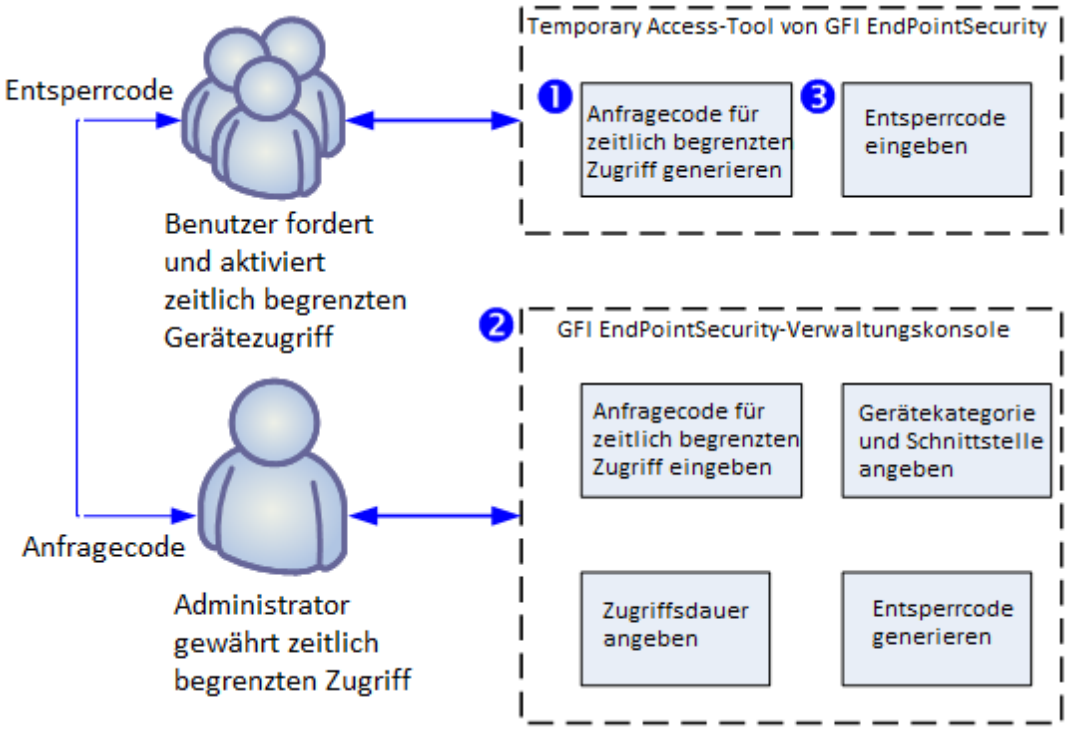


Abbildung 3: Anfordern/ Zulassen eines zeitlich begrenzten Zugriffs

In der folgenden Tabelle werden die oben abgebildeten Phasen beschrieben.

Tabelle 5: 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 dieser im Temporary-Access-Tool von GFI EndPointSecurity eingegeben werden, um den zeitlich begrenzten Zugriff zu aktivieren und die erforderlichen Geräte/Schnittstellen nutzen zu können.

1.9 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).

1.10 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).

1.11 Navigieren in der Verwaltungskonsole

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

Screenshot 1: Navigieren auf der Benutzeroberfläche von GFI EndPointSecurity

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

Abschnitt	Beschreibung
	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.
	Untergeordnete Registerkarten Weitere Einstellungen und/oder Informationen zur ausgewählten Registerkarte aus Abschnitt 1.
	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.
	Rechter Bereich Konfiguration der Konfigurationsoptionen, die im linken Bereich ausgewählt wurden. Nur bei manchen Registerkarten verfügbar.

2 Erzielen von Ergebnissen

Dieses Kapitel bietet Ihnen schrittweise Anleitungen, wie Sie nicht autorisierte Geräte im Netzwerk blockieren und Endpunkte mithilfe von GFI EndPointSecurity schützen können. Dieses Kapitel hilft Ihnen, positive Ergebnisse bei der Einhaltung gesetzlicher Vorschriften zu erzielen und gleichzeitig sicherzustellen, dass Ihr Netzwerk durch die neuesten Methoden und Techniken zur Erkennung von Sicherheitsrisiken geschützt ist.

Themen in diesem Kapitel

2.1 Verhindern von Datenlecks und Malware-Infektionen

Datendiebstahl tritt am häufigsten intern durch Mitarbeiter auf, die manuell Daten auf Wechseldatenträger übertragen. Die Verwendung von nicht autorisierten Wechseldatenträgern kann das Netzwerk einem höheren Risiko durch Malware-Infektionen aussetzen. Mit GFI EndPointSecurity können Sie umfassend den Zugriff auf Wechseldatenträger mit minimalem administrativen Aufwand kontrollieren. Endbenutzern kann der temporäre Zugriff auf ein Gerät an einem bestimmen Computer für einen bestimmten Zeitraum gewährt werden.

1. Agenten auf Computern bereitstellen, die geschützt werden sollen

GFI EndPointSecurity-Agenten werden verwendet, um Computer im Netzwerk zu schützen. Agenten können manuell auf bestimmten Computern oder automatisch auf neu im Netzwerk erkannten Endpunkten bereitgestellt werden. Weitere Informationen finden Sie in den folgenden Abschnitten:

- Manuelles Hinzufügen von Computern
- Automatisches Hinzufügen von Computern
- Konfigurieren der Anmeldeinformationen.

2. Eine Schutzrichtlinie erstellen, um Wechseldatenträger zu blockieren

Agenten schützen Computer basierend auf Einstellungen einer zugewiesenen Sicherheitsrichtlinie. Sie können so viele Sicherheitsrichtlinien wie erforderlich erstellen. Jede Richtlinie kann dabei verschiedene Einstellungen für unterschiedliche Autorisierungsebenen enthalten. Weitere Informationen finden Sie in den folgenden Abschnitten:

- Erstellen von Schutzrichtlinien
- Zuweisen von Schutzrichtlinien
- Sofortiges Bereitstellen von Richtlinien
- Festlegen eines Zeitplans für die Richtlinienbereitstellung
- Bereitstellen von Richtlinien über Active Directory
- Überprüfung der Bereitstellung von Schutzrichtlinien.

3. Einstellungen der Schutzrichtlinien konfigurieren

Konfigurieren Sie die Schutzrichtlinie, um Wechseldatenträger zu blockieren. Dadurch können Endbenutzer keine Geräte verwenden, mit denen sie Daten von einem Computer auf einen anderen übertragen. Weitere Informationen finden Sie in den folgenden Abschnitten:

» Konfigurieren kontrollierter Gerätekategorien

» Konfigurieren von Zugriffsberechtigungen für Gerätekategorien

» Konfigurieren von Zugriffsberechtigungen für einzelne Geräte

» Konfigurieren von Berechtigungsprioritäten

» Anzeigen von Zugriffsberechtigungen

» Konfigurieren der Geräte-Blacklist.

4. Benachrichtigungen bei versuchter Verletzung der Sicherheitsrichtlinie konfigurieren

GFI EndPointSecurity kann Benachrichtigungen an einzelne Empfänger oder Empfängergruppen senden, wenn ein Endbenutzer eine Sicherheitsrichtlinie verletzt. Dadurch können Sie sofort die erforderlichen Maßnahmen ergreifen und die nicht autorisierte Nutzung der Wechseldatenträger beenden. Weitere Informationen finden Sie in den folgenden Abschnitten:

» Konfigurieren der Alarme

» Konfigurieren der Warnoptionen

» Konfigurieren des Administratorkontos für Warnungen

» Konfigurieren der Warnungsempfänger

» Konfigurieren der Gruppen von Warnungsempfängern.

5. Temporären Zugriff für die legitime Nutzung von Wechseldatenträgern konfigurieren

Wenn eine Schutzrichtlinie zum Blockieren aktiv ist, können Sie mit GFI EndPointSecurity dennoch den temporären Zugriff auf ein Gerät ermöglichen, um legitim Daten von einem Computer auf einen anderen zu übertragen. Weitere Informationen finden Sie in den folgenden Abschnitten:

» Funktionsweise von GFI EndPointSecurity – Zeitlich begrenzter Zugriff

» Konfigurieren der Hauptbenutzer

» Konfigurieren zeitlich begrenzter Zugriffsrechte

» Konfigurieren der Geräte-Whitelist

» Konfigurieren von Benutzermeldungen.

2.2 Automatischer Netzwerkschutz

Nach der Konfiguration von GFI EndPointSecurity können Sie automatisch neue Computer schützen, die in erreichbaren Netzwerken erkennt werden. Geben Sie dazu die Domäne(n) und/oder Arbeitsgruppe(n) an, die nach neuen Computern gescannt werden sollen. Bei Erkennung eines Computers installiert GFI EndPointSecurity automatisch einen Agenten und weist die Standardrichtlinie zu. Richtlinien können auf der Registerkarte „Konfiguration“ > untergeordnete Registerkarte „Computer“ geändert werden.

1. Automatisch Geräte im Netzwerk erkennen

Mit GFI EndPointSecurity können Sie automatisch neue Computer hinzufügen, die mit dem Netzwerk verbunden sind. Dadurch können Sie eine angegebene Domäne oder Arbeitsgruppe durchsuchen und die darin gefundenen Computer hinzufügen. Weitere Informationen finden Sie in den folgenden Abschnitten:

» Ausführen eines Gerätescans

» Analysieren der Ergebnisse des Gerätescans

» Hinzufügen erkannter Geräte zur Datenbank.

2. Agenten auf neu erkannten Geräten bereitstellen

GFI EndPointSecurity kann so konfiguriert werden, dass Agenten automatisch auf neu zur Datenbank hinzugefügten Computern installiert werden. Ein Agent muss auf jedem Computer installiert werden, der geschützt werden soll. Weitere Informationen finden Sie in den folgenden Abschnitten:

» Automatisches Hinzufügen von Computern

» Konfigurieren von erweiterten Optionen

» Konfigurieren der Anmeldeinformationen.

3. (Optional) Schutzrichtlinie konfigurieren, die neu erkannten Geräten zugewiesen wird

Wenn für die Bereitstellung keine Schutzrichtlinie konfiguriert ist, erstellen Sie eine Richtlinie, die neu installierten Agenten auf erkannten Computern zugewiesen werden kann. Die Standardrichtlinie muss einem neuen Agenten zugewiesen werden, kann jedoch auf der Registerkarte „Konfiguration“ > Unterregisterkarte „Computer“ geändert werden. Die Richtlinie erkennt die Sicherheitseinstellungen und das Geräteverhalten. Weitere Informationen finden Sie im folgenden Abschnitt:

» Anpassen von Schutzrichtlinien

» Festlegen einer Standardrichtlinie.

4. Schutzrichtlinien automatisch zuweisen

Konfigurieren Sie GFI EndPointSecurity so, dass Schutzrichtlinien automatisch auf neuen Agenten bereitgestellt werden. Weitere Informationen finden Sie in den folgenden Abschnitten:

» Festlegen eines Zeitplans für die Richtlinienbereitstellung

» Bereitstellen von Richtlinien über Active Directory

» Überprüfung der Bereitstellung von Schutzrichtlinien.

5. Geräteaktivität überwachen

Mit GFI EndPointSecurity können Sie einen Überwachungspfad für Aktivitätsprotokolle einrichten, die von Agenten auf Netzwerkcomputern (Ereignisprotokollierung muss aktiviert sein) erstellt werden. Auf den Registerkarten „Status“ und „Aktivität“ können Sie die Status und statistischen Informationen der Endpunkte, Agenten und von GFI EndPointSecurity anzeigen. Weitere Informationen finden Sie in den folgenden Abschnitten:

» Konfigurieren der Ereignisprotokollierung

» Aktivität zur Geräteverwendung anzeigen

» Statistik zur Geräteverwendung anzeigen.

2.3 Überwachen der Netzwerkaktivität von einem zentralen Standort aus

Agenten erzeugen Aktivitätsprotokolle, die in einer SQL Server-Datenbank gespeichert werden. GFI EndPointSecurity pflegt einen Überwachungspfad dieser Protokolle und bietet Informationen in verschiedenen Dashboard-Anzeigen. Über die umfassenden Dashboard-Anzeigen von GFI EndPointSecurity können Sie die Netzwerkaktivität in Echtzeit überwachen und es dem Administrator so ermöglichen, sofortige Maßnahmen gegen ein erkanntes Sicherheitsrisiko zu ergreifen. Konfigurieren Sie GFI EndPointSecurity so, dass regelmäßig (täglich/wöchentlich/monatlich) Berichte erstellt und für eine Analyse der Endpunktsicherheitsstatus an das IT- und Verwaltungspersonal geschickt werden.

1. Netzwerkweite Aktivität analysieren

Über die Unterregisterkarten der Registerkarten „Status“ und „Aktivität“ können Sie die Netzwerkaktivität von einem zentralen Standort überwachen. Diese Registerkarten enthalten Risikobewertungen, Statistiken, Status, Aktivitätsprotokolle und Bereitstellungsinformationen dargestellt in Diagrammen und Tabellen. Weitere Informationen finden Sie in den folgenden Abschnitten:

- Analysieren von Risikobewertungsdetails
- Analysieren von Statistiken
- Analysieren von Statusinformationen
- Analysieren von Agentenbereitstellungsdetails
- Analysieren von Aktivitätsprotokollen.

2. Berichte basierend auf Aktivitätsprotokollen erstellen, die von Agenten im Netzwerk erstellt wurden

GFI EndPointSecurity enthält eine umfangreiche Liste an Berichten, die so wie sie sind oder modifiziert für Ihre Berichterstellungsanforderungen verwendet werden können. Das ReportPack enthält sowohl technische Berichte für IT-Mitarbeiter als auch Übersichtsberichte für Verwaltungszwecke. Weitere Informationen finden Sie in den folgenden Abschnitten:

- Verwenden des GFI EndPointSecurity ReportPack
- Erstellen von Übersichtsberichten.

3. Datenbank-Backend pflegen

GFI EndPointSecurity speichert Ereignisprotokolle in einer SQL Server-Datenbank. In einem großen Netzwerk mit viel Aktivität kann die Größe der Datenbank exponentiell anwachsen und so die Schreib-/Leseleistung zwischen GFI EndPointSecurity und der Datenbank verringern. Es wird empfohlen, die Einstellungen für die Protokollaufbewahrung so zu konfigurieren, dass alte oder unerwünschte Ereignisse automatisch gelöscht werden oder sogar eine neue Datenbank erstellt wird, wenn die aktuelle Datenbank eine bestimmte Größe erreicht. Weitere Informationen finden Sie in den folgenden Abschnitten:

- Warten des Datenbank-Backends
- Verwenden einer vorhandenen SQL Server-Instanz.

3 Hinzufügen von kontrollierten Computern

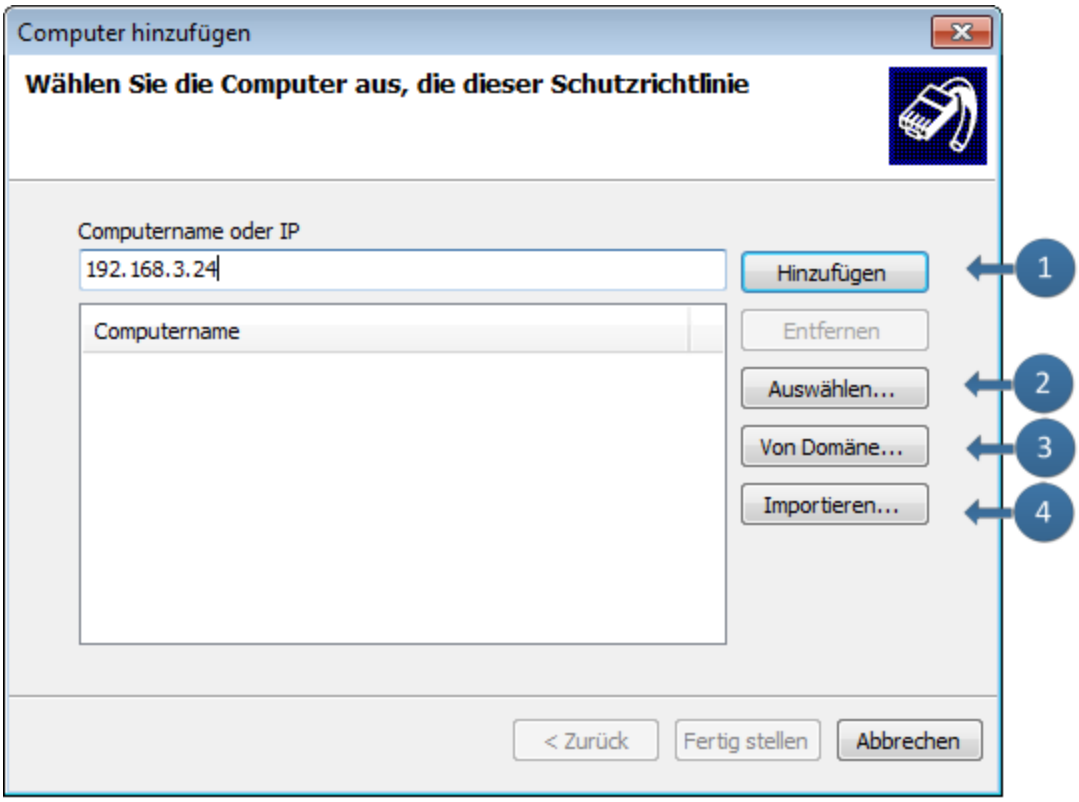
GFI EndPointSecurityIn können Sie die Computer angeben, auf denen Agenten und Schutzrichtlinien bereitgestellt werden sollen.
Themen in diesem Kapitel

3.1 Manuelles Hinzufügen von Computern

So fügen Sie einen kontrollierten Computer manuell hinzu:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Computer hinzufügen...**



Screenshot 2: Manuelles Hinzufügen von Computern

3. In der folgenden Tabelle werden die im Dialogfeld **Computer hinzufügen** verfügbaren Optionen beschrieben:

Tabelle 6: Optionen im Dialogfeld „Computer hinzufügen“

Option	Beschreibung
1	Geben Sie den Namen/die IP-Adresse des zu kontrollierenden Computers ein, und klicken Sie auf **Hinzufügen**. Wiederholen Sie diesen Schritt für jeden kontrollierten Computer, der dieser Schutzrichtlinie hinzugefügt werden soll.

Option	Beschreibung
2	Klicken Sie auf **Auswählen…**. Wählen Sie im Dialogfeld **Computer auswählen** die relevante Domäne/Arbeitsgruppe aus der Dropdown-Liste aus, und klicken Sie auf **Suchen**. Aktivieren Sie den/die gewünschten Computer, und klicken Sie auf **OK**.
3	Klicken Sie auf **Von Domäne…**. Geben Sie den/die gewünschten Computer aus der Domäne/Arbeitsgruppe an, in der GFI EndPointSecurity installiert ist.
4	Klicken Sie auf **Importieren**. Suchen Sie die Textdatei, die eine Liste der zu importierenden Computer enthält. **Hinweis** Geben Sie NUR einen Computernamen/eine IP-Adresse pro Zeile an.

4. Klicken Sie auf **Fertig stellen**.

3.2 Automatisches Hinzufügen von Computern

GFI EndPointSecurity kann in festgelegten Zeitabständen nach neuen an das Netzwerk angeschlossenen Computern suchen und diese hinzufügen. Auf diese Weise können Sie Computer automatisch hinzufügen, sobald sie im Netzwerk erkannt werden. Mithilfe der Funktion zur autom. Erkennung können folgende Einstellungen konfiguriert werden:

» Häufigkeit und Zeitplan der Suchen,

» für die Erkennung zu scannende Domäne/Arbeitsgruppe,

» Richtlinie, die neu erkannten Computern zugewiesen wird, und Anmeldeinformationen.

Standardmäßig geschieht Folgendes:

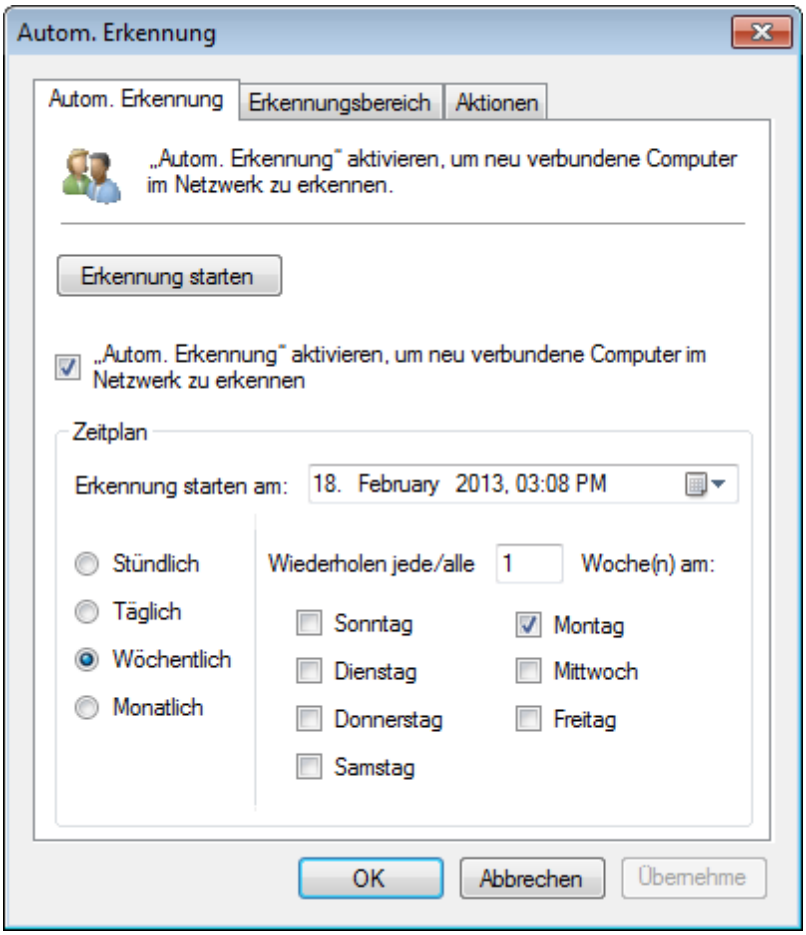
» Die autom. Erkennung ist so konfiguriert, dass die aktuelle Domäne/Arbeitsgruppe durchsucht wird (Domäne/Arbeitsgruppe in der GFI EndPointSecurity installiert ist).

» Die Installationseinstellungen sind so konfiguriert, dass die Standardschutzrichtlinie **Allgemeine Kontrolle** neu erkannten Computern zugewiesen wird.

So konfigurieren Sie die autom. Erkennung:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Autom. Erkennung konfigurieren...**

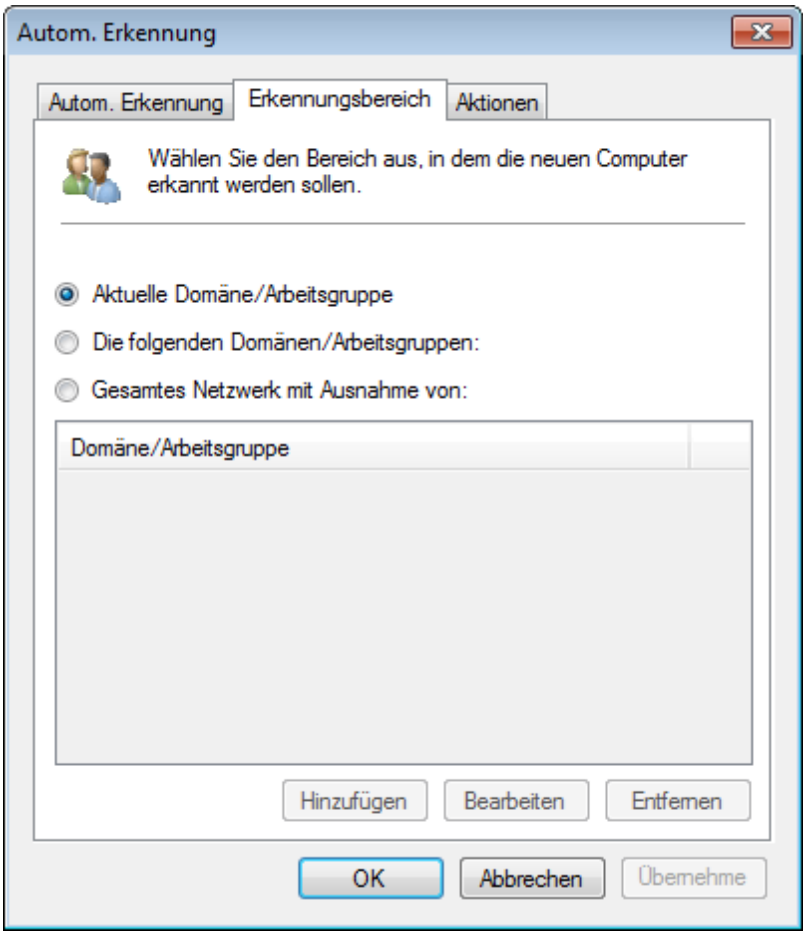


Screenshot 3: Optionen für die autom. Erkennung - Registerkarte „Autom. Erkennung"

3. Klicken Sie auf **Erkennung starten**, um die autom. Erkennung auszuführen.

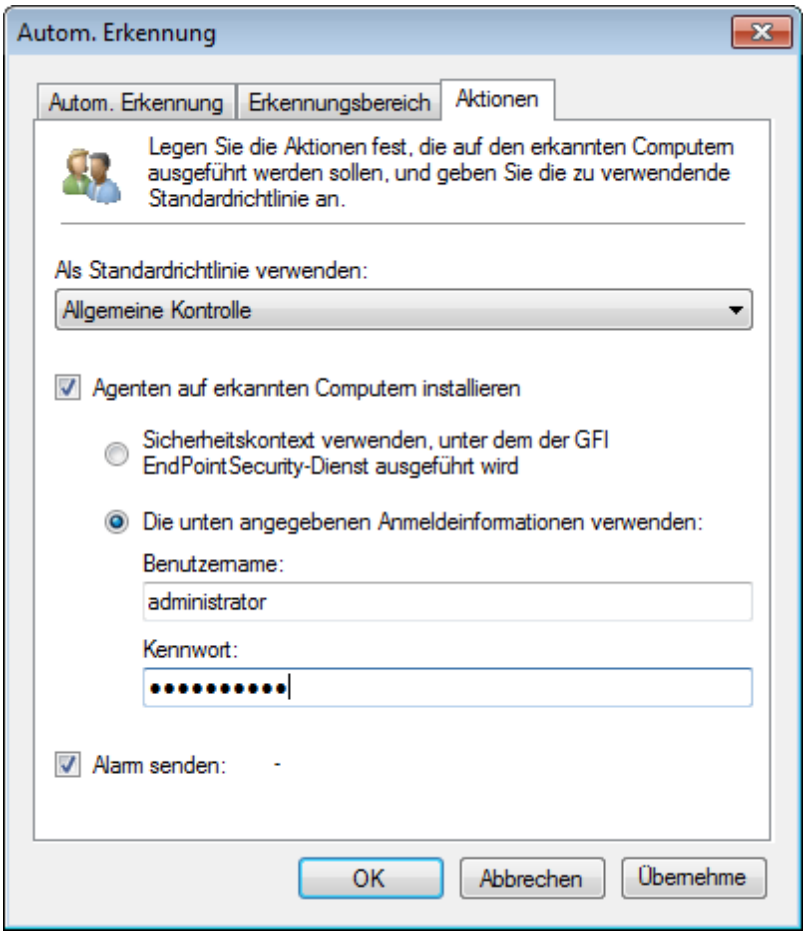
4. Aktivieren/Deaktivieren Sie **„Autom. Erkennung aktivieren", um neu verbundene Computer im Netzwerk zu erkennen.**, um die automatische Erkennung zu aktivieren/deaktivieren.

5. Wählen Sie im Bereich **Zeitplan** das Startdatum und die Häufigkeit der Suchen mit den Optionen Stündlich, Täglich, Wöchentlich oder Monatlich aus.



Screenshot 4: Optionen für die autom. Erkennung - Registerkarte „Erkennungsbereich“

6. Wechseln Sie auf die Registerkarte **Erkennungsbereich**, und wählen Sie den zu durchsuchenden Bereich für die autom. Erkennung aus. Klicken Sie für die Optionen **Die folgenden Domänen/Arbeitsgruppen** und **Gesamtes Netzwerk mit Ausnahme von** auf **Hinzufügen**, und geben Sie den Namen der Domäne/Arbeitsgruppe ein.



Screenshot 5: Optionen für die autom. Erkennung - Registerkarte „Aktionen“

7. Wechseln Sie auf die Registerkarte **Aktionen**, und wählen Sie aus dem Dropdown-Menü **Als Standardrichtlinie verwenden** die Richtlinie aus, die Sie neu entdeckten Computern zuweisen möchten.

8. Aktivieren/Deaktivieren Sie **Agenten auf erkannten Computern installieren**, um die automatische Agentenbereitstellung zu aktivieren/deaktivieren. Klicken Sie auf **Ja**, um die Aktivierung des automatischen Schutzes zu bestätigen.

9. Wählen Sie den Anmeldemodus aus, der von GFI EndPointSecurity für die Anmeldung auf den kontrollierten Computern und die Bereitstellung von Agenten/Schutzrichtlinien verwendet wird. GFI EndPointSecurity verwendet standardmäßig die Anmeldeinformationen des aktuell angemeldeten Benutzers, unter dem GFI EndPointSecurity ausgeführt wird.

10. Aktivieren/Deaktivieren Sie **Warnung senden**, um die Warnoptionen zu aktivieren/deaktivieren. Weitere Informationen finden Sie unter Konfigurieren der Warnoptionen (page 120).

11. Klicken Sie auf **Übernehmen** und **OK**.

3.3 Konfigurieren der Anmeldeinformationen

GFI EndPointSecurity muss sich an den zu kontrollierenden Computern anmelden, um:

» Agenten und Aktualisierungen für Schutzrichtlinien bereitzustellen,

» den Schutzstatus der zu kontrollierenden Computer zu kontrollieren.

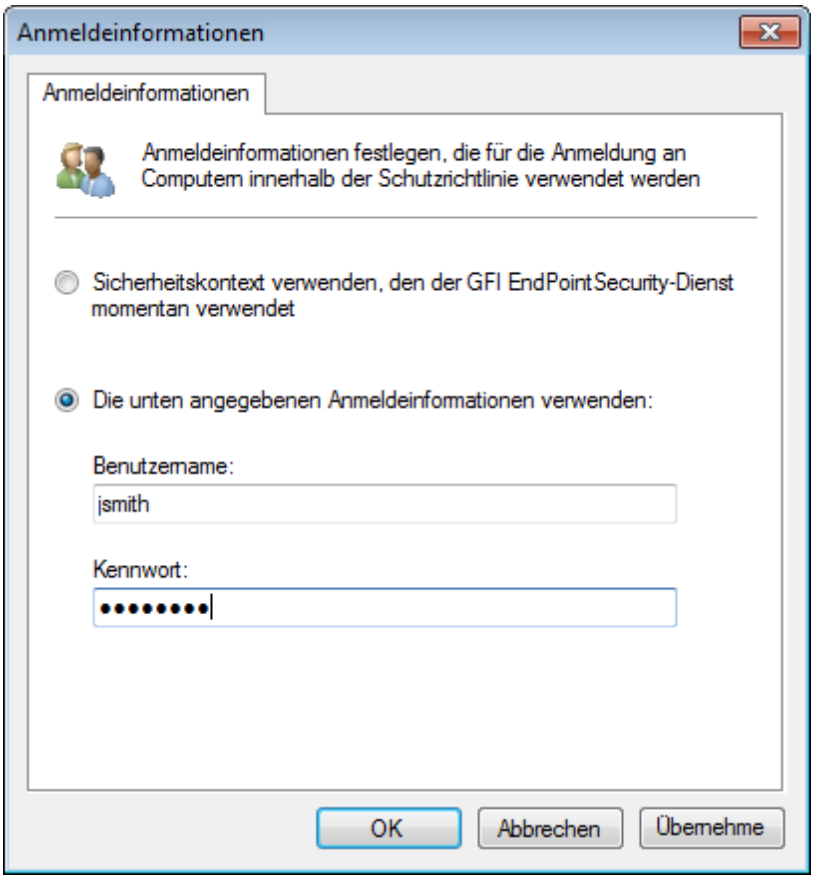
Hierfür ist erforderlich, dass GFI EndPointSecurity unter einem Konto mit administrativen Berechtigungen für die im Netzwerk zu kontrollierenden Computer läuft (z. B. Domänenadministratorkonto).

So legen Sie die Anmeldeinformationen für einen zu kontrollierenden Computer fest:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie mit der rechten Maustaste auf einen Computer in der Liste, und klicken Sie dann auf **Anmeldeinformationen festlegen...**.

> **Hinweis**
>
> Wenn Sie für mehrere Computer dieselben Anmeldeinformationen festlegen möchten, markieren Sie die gewünschten Computer, klicken Sie mit der rechten Maustaste auf einen der Computer, und klicken Sie dann auf **Anmeldeinformationen festlegen...**. Alternativ können Sie unter **Aktionen** auf **Anmeldeinformationen festlegen...** klicken.



Screenshot 6: Optionen im Dialogfeld „Anmeldeinformationen“

3. In der folgenden Tabelle werden die verfügbaren Anmeldeinformationen beschrieben:

Tabelle 7: Optionen für Anmeldeinformationen

Option	Beschreibung
Sicherheitskontext verwenden, unter dem der GFI EndPointSecurity-Dienst ausgeführt wird	Es werden dieselben Anmeldeinformationen wie für GFI EndPointSecurity verwendet.
Die unten angegebenen Anmeldeinformationen verwenden:	Geben Sie alternative Anmeldeinformationen für die Anmeldung bei kontrollierten Remote-Computern an. **Hinweis** Verwenden Sie Anmeldeinformationen mit Administratorberechtigungen auf den Scanzielen.

4. Klicken Sie auf **Übernehmen** und **OK**.

> **Hinweis**
>
> GFI EndPointSecurity verwendet standardmäßig die Anmeldeinformationen des aktuell angemeldeten Benutzerkontos, unter dem GFI EndPointSecurity ausgeführt wird.

4 Verwaltung von Schutzrichtlinien

In diesem Kapitel wird beschrieben, wie neu erstellte Schutzrichtlinien bereitgestellt und geplant werden. Vor der Bereitstellung können Sie ebenfalls die Einstellungen für Ihre Schutzrichtlinie ändern.
Themen in diesem Kapitel

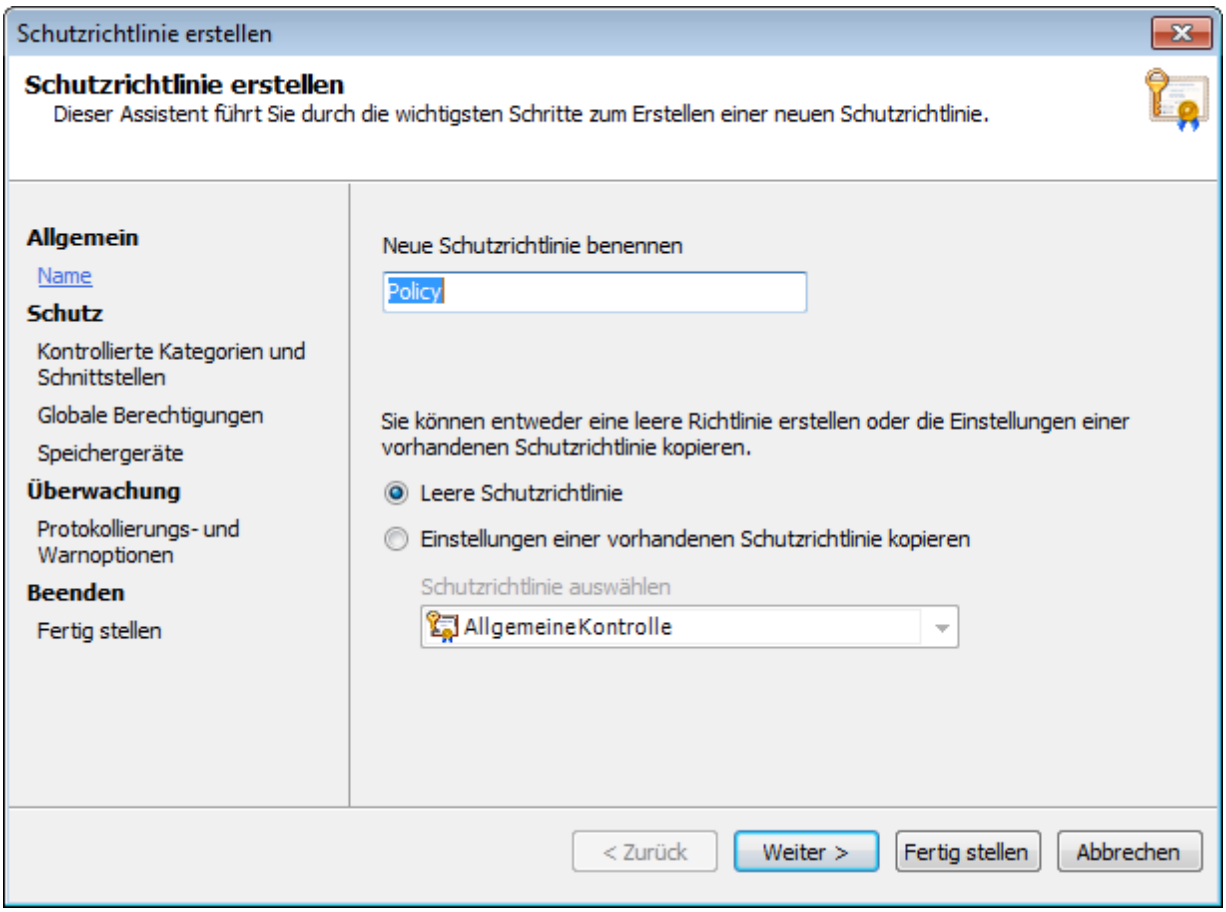
4.1 Erstellen einer neuen Schutzrichtlinie

GFI EndPointSecurity wird mit einer Standardschutzrichtlinie geliefert, so dass die Software nach der Installation sofort betriebsbereit ist. Sie können weitere Schutzrichtlinien erstellen, um den Gerätezugriff unternehmensspezifisch anzupassen.

So erstellen Sie eine neue Schutzrichtlinie:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

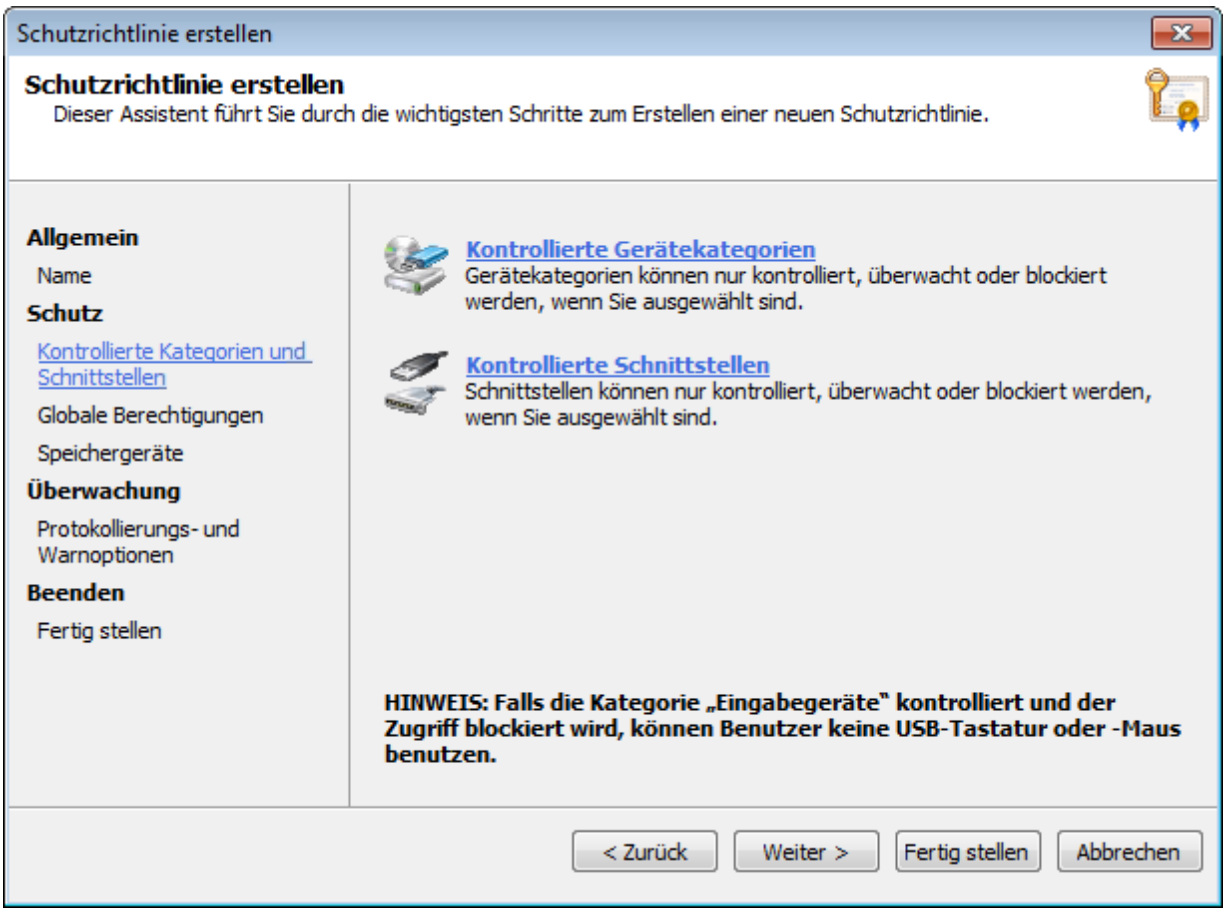
2. Klicken Sie unter **Allgemeine Aufgaben** auf **Neue Schutzrichtlinie erstellen...**.



Screenshot 7: Erstellen einer neuen Schutzrichtlinie - Allgemeine Einstellungen

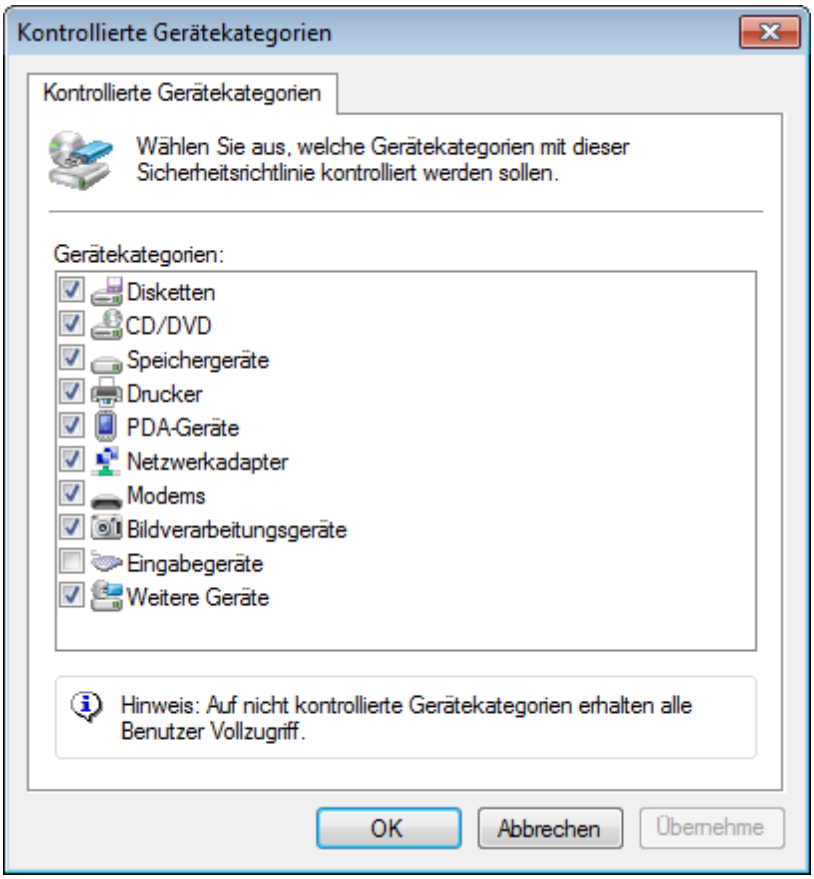
3. Geben Sie einen eindeutigen Namen für die neue Schutzrichtlinie ein.

4. Wählen Sie aus, ob Sie entweder eine leere Richtlinie erstellen oder die Einstellungen einer vorhandenen Schutzrichtlinie kopieren möchten. Klicken Sie auf **Weiter**. Wählen Sie im Einstellungsbereich die erforderliche Vererbungsoption aus:



Screenshot 8: Erstellen einer neuen Richtlinie - Einstellungen für kontrollierte Kategorien und Schnittstellen

5. Klicken Sie auf **Kontrollierte Gerätekategorien**.

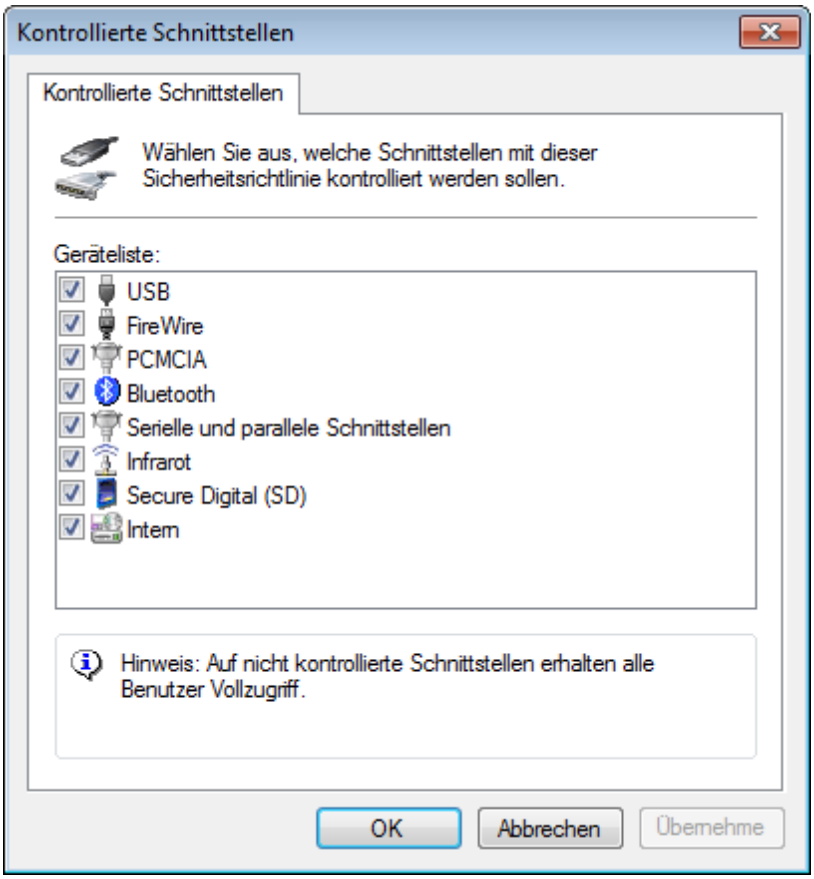


Screenshot 9: Optionen für kontrollierte Gerätekategorien

6. Wählen Sie im Dialogfeld **Kontrollierte Gerätekategorien** die erforderlichen Gerätekategorien aus, die Sie mit dieser neuen Richtlinie kontrollieren möchten. Klicken Sie auf **OK**, um das Dialogfeld **Kontrollierte Gerätekategorien** zu schließen und zum Assistenten zurückzukehren.

> **Wichtig**
>
> Falls die Option „Eingabegeräte“ aktiviert ist und der Zugriff verweigert wird, können Benutzer keine USB-Tastaturen oder -Mäuse verwenden, die an die durch diese Schutzrichtlinie kontrollierten Computer angeschlossen sind.

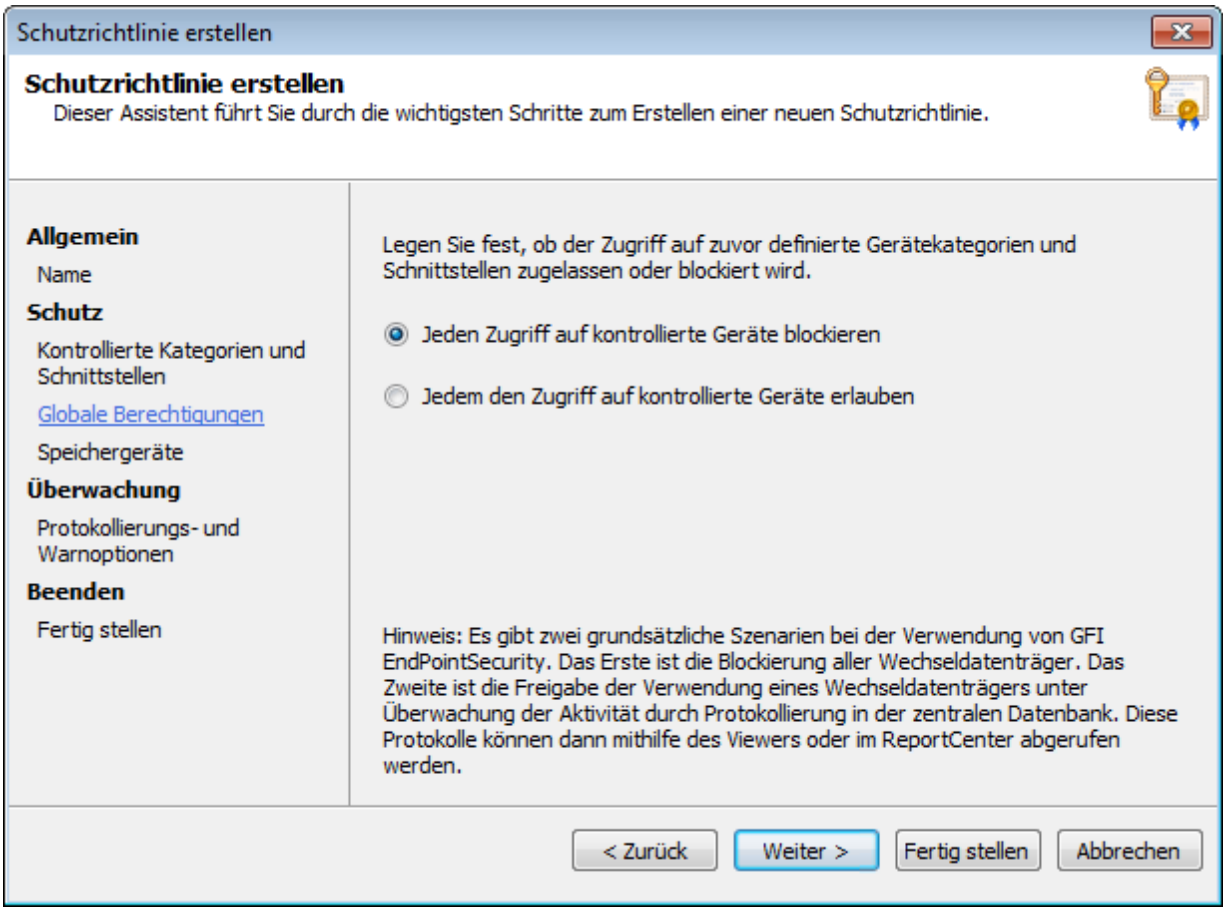
7. Klicken Sie auf **Kontrollierte Schnittstellen**.



Screenshot 10: Optionen für kontrollierte Schnittstellen

8. Wählen Sie im Dialogfeld **Kontrollierte Schnittstellen** die erforderlichen Schnittstellen aus, die Sie mit dieser neuen Richtlinie kontrollieren möchten. Klicken Sie auf **OK**, um das Dialogfeld **Kontrollierte Schnittstellen** zu schließen und zum Assistenten zurückzukehren.

9. Klicken Sie auf **Weiter**.



Screenshot 11: Erstellen einer neuen Richtlinie - Einstellungen für globale Berechtigungen

10. Wählen Sie im Dialogfeld **Globale Berechtigungen** die erforderlichen globalen Zugriffsberechtigungen aus Folgendem aus:

» **Jeden Zugriff auf kontrollierte Geräte blockieren** – Zur Blockierung des Zugriffs auf alle ausgewählten Geräte/Schnittstellen.

» **Jedem den Zugriff auf kontrollierte Geräte erlauben** – Zur Zulassung des Zugriffs auf alle ausgewählten Geräte/Schnittstellen. Falls Sie diese Option auswählen, erfolgt dennoch eine Aktivitätsüberwachung auf allen durch diese Schutzrichtlinie kontrollierten Computern.

11. Klicken Sie auf **Weiter**.

12. Klicken Sie auf **Dateitypfilter**, und fügen Sie die Dateitypen hinzu, die durch diese Richtlinie blockiert bzw. zugelassen werden sollen.

Hinweis

GFI EndPointSecurity bietet die Möglichkeit, den Zugriff basierend auf Dateitypen einzuschränken. Außerdem kann der wahre Inhalt der meisten Dateitypen (z. B. .doc oder .xls) erkannt werden. Dadurch können die für den Dateityp erforderlichen Maßnahmen ergriffen werden. Das ist besonders nützlich, wenn Dateierweiterungen böswillig manipuliert werden. Weitere Informationen finden Sie unter Konfigurieren der Dateitypfilter (page 72).

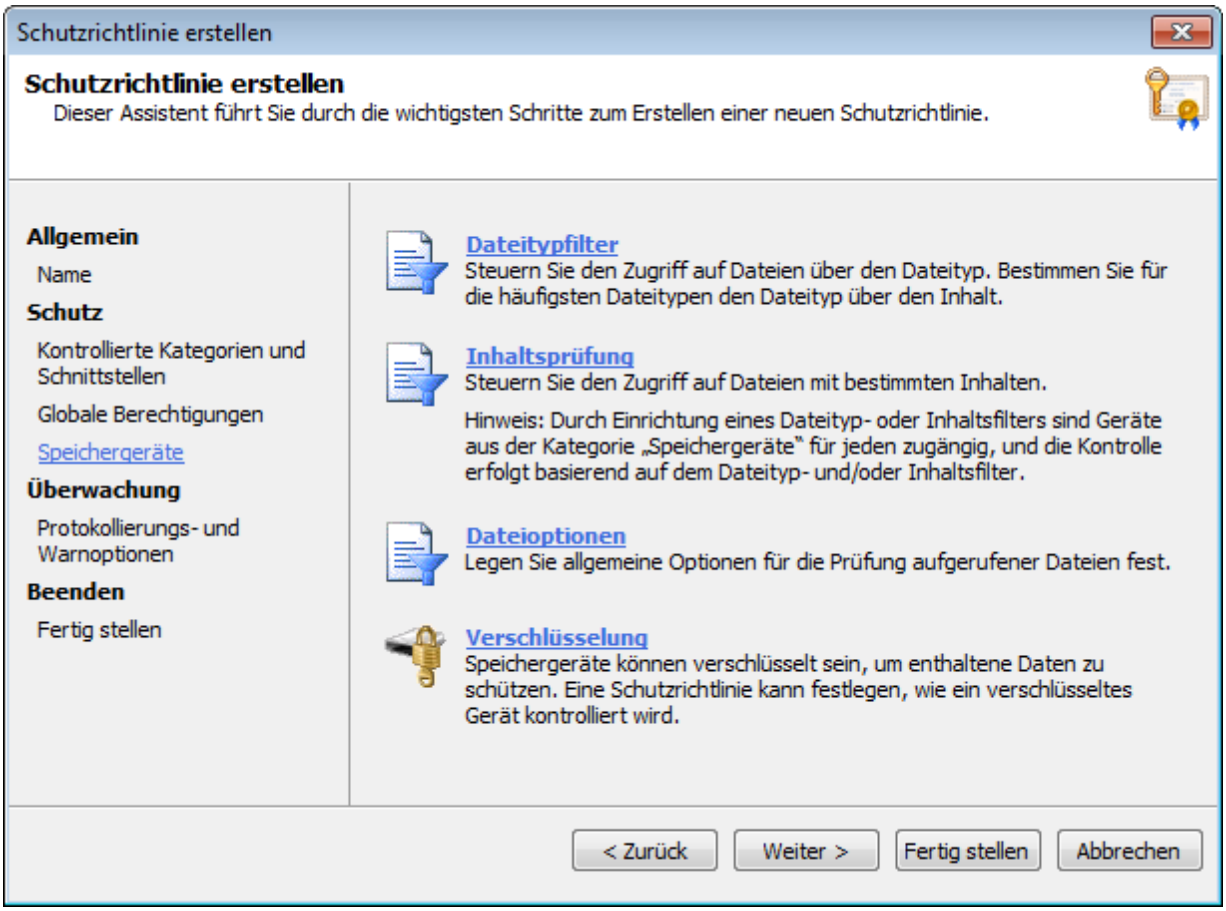
13. Klicken Sie auf **OK**, um das Dialogfeld **Dateitypfilter** zu schließen und zum Assistenten zurückzukehren.

14. Klicken Sie auf **Verschlüsselung**, und aktivieren Sie das gewünschte Verschlüsselungsmodul.

> **Hinweis**
>
> Zusätzlich kann in GFI EndPointSecurity für Active Directory (AD)-Benutzer und/oder -Benutzergruppen der Zugriff auf bestimmte Dateitypen auf Geräten, die mit BitLocker To Go verschlüsselt wurden, eingeschränkt werden. Diese Einschränkungen werden angewendet, wenn verschlüsselte Geräte an die durch die Schutzrichtlinie kontrollierten Computer angeschlossen werden. Weitere Informationen finden Sie unter Konfigurieren der Sicherheitsverschlüsselung (page 79).

15. Klicken Sie auf **OK**, um das Dialogfeld **Verschlüsselung** zu schließen und zum Assistenten zurückzukehren.

16. Klicken Sie auf **Weiter**.



17. Wählen Sie unter **Speichergeräte** die erforderlichen Optionen aus, die Sie über die unten beschriebenen Registerkarten steuern möchten:

Tabelle 8: Einstellungen für die autom. Erkennung

Registerkarte	Beschreibung
Dateitypfilter	GFI EndPointSecurity gibt Ihnen die Möglichkeit, Einschränkungen für Dateitypen zu definieren, beispielsweise für Dateien der Formate .doc oder .xls, um zu verhindern, dass diese auf oder von erlaubten Geräten kopiert werden. Diese Einschränkungen können Active Directory (AD)-Benutzern und/oder -Benutzergruppen zugewiesen werden.
Inhaltsprüfung	Mit GFI EndPointSecurity können Sie Dateiinhaltsbeschränkungen für eine bestimmte Schutzrichtlinie angeben. Die Inhaltsprüfung prüft Dateien, die den Endpunkt über Wechseldatenträger passieren und identifiziert Inhalt basierend auf vorkonfigurierten und benutzerdefinierten regulären Ausdrücken und Wörterbuchdateien. Das Modul sucht standardmäßig nach geschützten, vertraulichen Informationen wie Sozialversicherungsnummern und primären Kontonummern, Informationen zu Unternehmen, Namen von Erkrankungen, Drogen, gefährlichen Chemikalien sowie alltäglicher Sprache und ethnischen/rassistischen Begriffen. » Sie können die Inhaltsprüfung als eine globale Richtlinie ähnlich dem Dateiüberprüfungsmodul konfigurieren.
Dateioptionen	Mit GFI EndPointSecurity können Sie Optionen angeben, die zum Blockieren oder Zulassen von Dateien basierend auf deren Größe erforderlich sind. Außerdem ermöglicht GFI EndPointSecurity das Ignorieren von großen Dateien, wenn der Dateityp, der Inhalt oder archivierte Dateien überprüft werden.
Verschlüsselung	GFI EndPointSecurity ermöglicht Ihnen die Konfiguration von Einstellungen speziell für verschlüsselte Geräte. Sie können auch Geräte verschlüsseln, die bisher noch nicht gesichert wurden.

Hinweis

Weitere Informationen finden Sie unter Weitere Informationen finden Sie unter Anpassen von Schutzrichtlinien (page 45).

18. Konfigurieren Sie die Protokollierungs- und Warnoptionen für diese Schutzrichtlinie, und klicken Sie auf **Weiter**.

Hinweis

Weitere Informationen finden Sie unter Konfigurieren der Ereignisprotokollierung und Konfigurieren der Warnungen.

19. Überprüfen Sie auf der Übersichtsseite die Details zur Richtlinie, und klicken Sie auf **Fertig stellen**.

4.2 Zuweisen einer Schutzrichtlinie

Im nächsten Schritt werden die relevanten Berechtigungen für Geräte- und Schnittstellenzugriff mit den jeweiligen Computern verknüpft. Dies erfolgt durch die Zuweisung von Schutzrichtlinien an zu kontrollierende Computer.

Hinweis

Zu kontrollierenden Computern kann nur jeweils eine Schutzrichtlinie zugewiesen werden.

So weisen Sie eine Schutzrichtlinie einem zu kontrollierenden Computer zu:

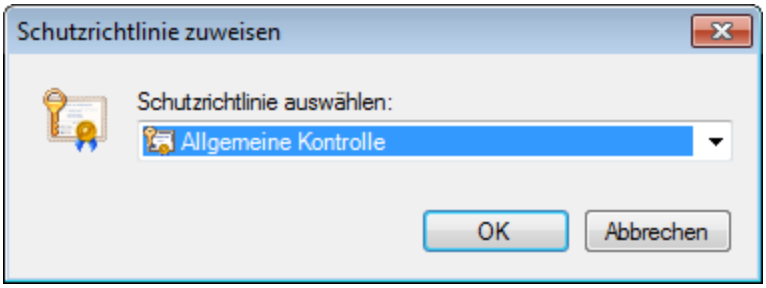
1. Wählen Sie in der Verwaltungskonsole von GFI EndPointSecurity die Option **Konfiguration**.

2. Klicken Sie auf **Computer**.

3. Markieren Sie den/die gewünschten zu kontrollierenden Computer.

> **Hinweis**
>
> Wenn Sie die gleiche Richtlinie mehreren kontrollierten Computern zuweisen, markieren Sie alle gewünschten zu kontrollierenden Computer gleichzeitig, und legen Sie anschließend die Schutzrichtlinie für die ausgewählten kontrollierten Computer fest.

4. Klicken Sie im linken Bereich im Abschnitt **Aktionen** auf den Hyperlink **Schutzrichtlinie zuweisen**.



Screenshot 12: Optionen zur Zuweisung von Schutzrichtlinien

5. Wählen Sie im Dialog **Schutzrichtlinie zuweisen** die erforderliche Schutzrichtlinie aus dem Drop-down-Menü aus, und klicken Sie auf **OK**.

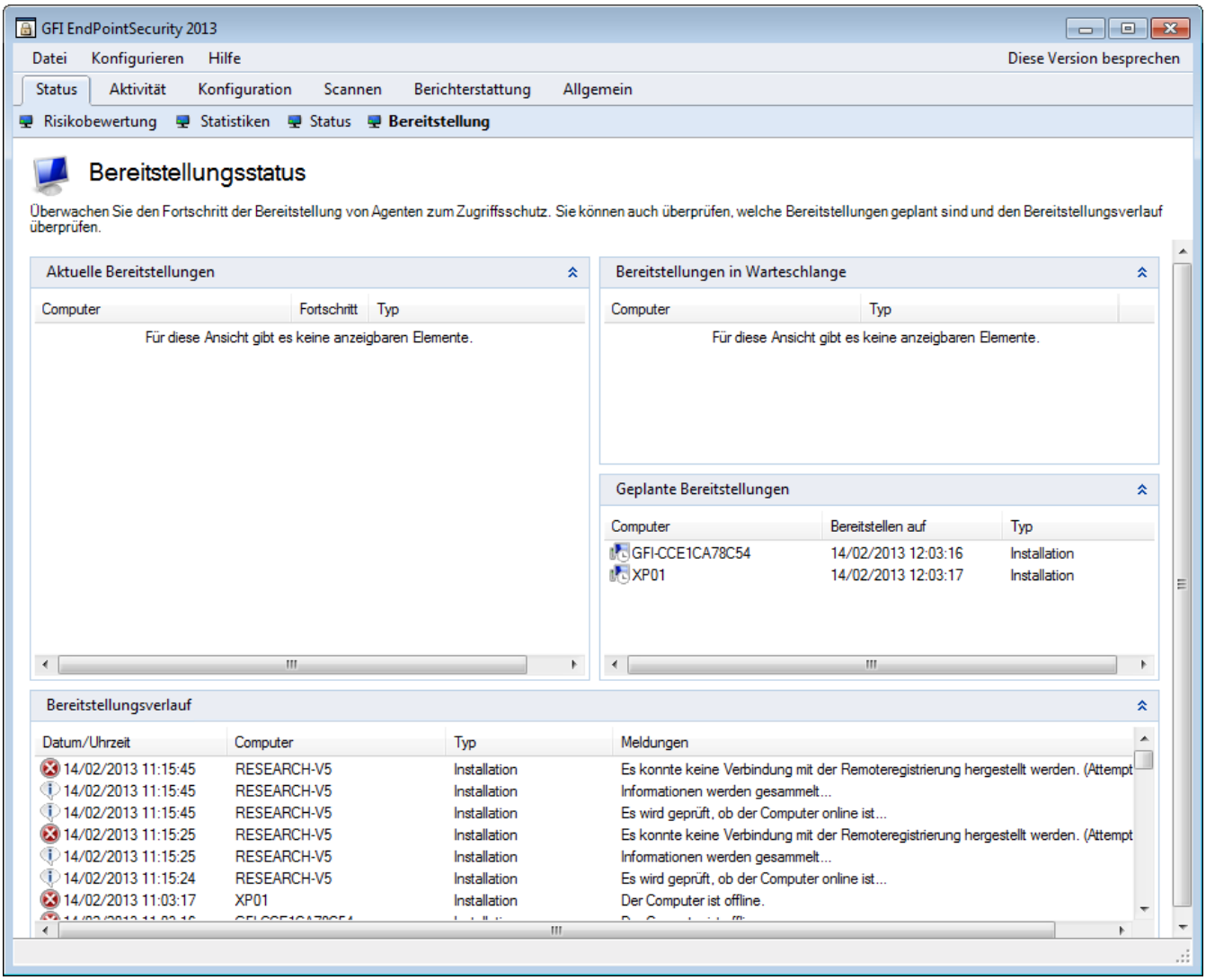
4.2.1 Sofort bereitstellen

So stellen Sie eine Schutzrichtlinie sofort auf zu kontrollierenden Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Computer**.

2. Markieren Sie die gewünschten zu kontrollierenden Computer. Falls mehr als eine Bereitstellung erforderlich ist, können Sie alle gewünschten zu kontrollierenden Computer gleichzeitig markieren und anschließend die Schutzrichtlinie für den ausgewählten Computer bereitstellen.

3. Klicken Sie unter **Aktionen** auf **Bereitstellen...**. Die Ansicht sollte automatisch zu **Status > Bereitstellung wechseln**.



Screenshot 13: Sofortiges Bereitstellen einer Richtlinie - untergeordnete Registerkarte „Bereitstellung“

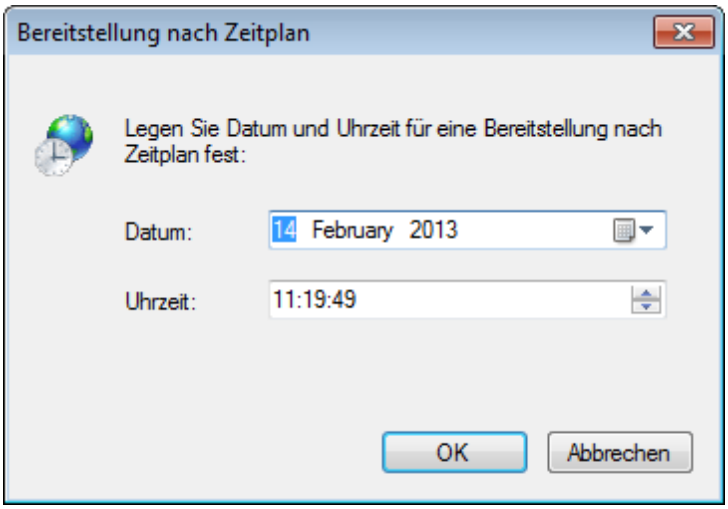
4.2.2 Bereitstellung von Richtlinien nach Zeitplan

So legen Sie einen Zeitplan für die Bereitstellung einer Schutzrichtlinie fest:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Markieren Sie den/die gewünschten zu kontrollierenden Computer. Falls mehr als eine Bereitstellung erforderlich ist, können Sie alle gewünschten zu kontrollierenden Computer gleichzeitig markieren und anschließend die Schutzrichtlinie für alle ausgewählten Computer bereitstellen.

3. Klicken Sie unter **Aktionen** auf **Zeitplan für Bereitstellung festlegen...**.



Screenshot 14: Optionen für die Bereitstellung nach Zeitplan

4. Wählen Sie im Dialogfeld **Zeitplan für Bereitstellung festlegen** das Datum und die Uhrzeit für die Bereitstellung aus. Klicken Sie anschließend auf **OK**.

> **Hinweis**
>
> Falls der zu kontrollierende 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.

4.2.3 Bereitstellen von Richtlinien über Active Directory

Standardmäßige Schutzrichtlinien können auch über ein Windows Installer-Paket (MSI-Installationsdatei) mit Hilfe von Active Directory-Gruppenrichtlinien auf zu kontrollierenden Computern in Ihrer Domäne bereitgestellt werden.

So erstellen Sie ein Windows Installer-Paket:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

2. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die ein Windows Installer-Paket erstellt werden soll.

3. Klicken Sie im rechten Bereich im Abschnitt **Bereitstellung** auf **Über Active Directory bereitstellen**.

4. Geben Sie den **Dateinamen** der .msi-Datei ein, und suchen Sie den Zielpfad.

5. Klicken Sie auf **Speichern**.

> **Hinweis**
>
> Weitere Informationen zur Bereitstellung von Software mithilfe von Active Directory-Gruppenrichtlinien unter Microsoft Windows Server 2003 und Microsoft Windows Server 2008 finden Sie unter http://support.microsoft.com/kb/816102.

4.3 Überprüfung der Bereitstellung von Schutzrichtlinien

Nach der Bereitstellung einer Schutzrichtlinie sollten Sie überprüfen, ob die Richtlinie auf die kontrollierten Computer angewendet wird. Überprüfen Sie in folgenden Bereichen, ob die Bereitstellung erfolgreich war:

» Bereich „Bereitstellungsverlauf“

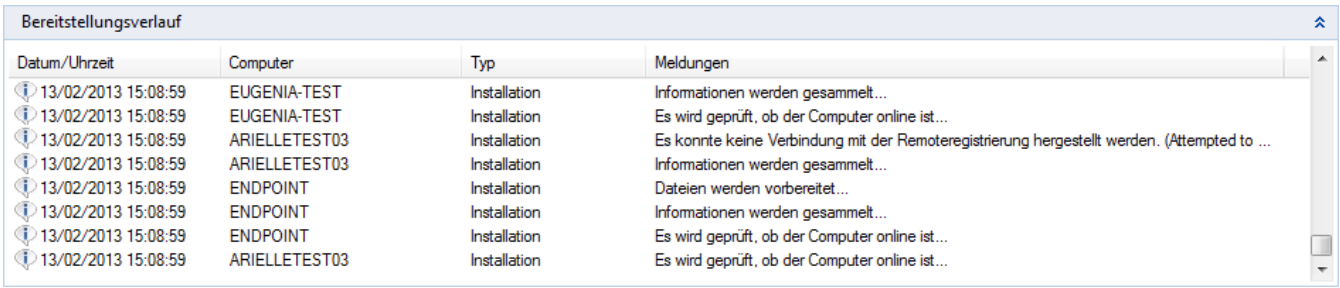
» Bereich „Agentenstatus“

4.3.1 Bereitstellungsverlauf

Verwenden Sie die Informationen aus dem Bereich „Bereitstellungsverlauf“, um zu bestimmen, ob die Bereitstellung für jeden zu kontrollierenden Computer erfolgreich war oder ob Fehler vorliegen.

So zeigen Sie den Bereitstellungsverlauf an:

1. Klicken Sie auf **Status** >**Bereitstellung**.



Screenshot 15: Bereich „Bereitstellungsverlauf“

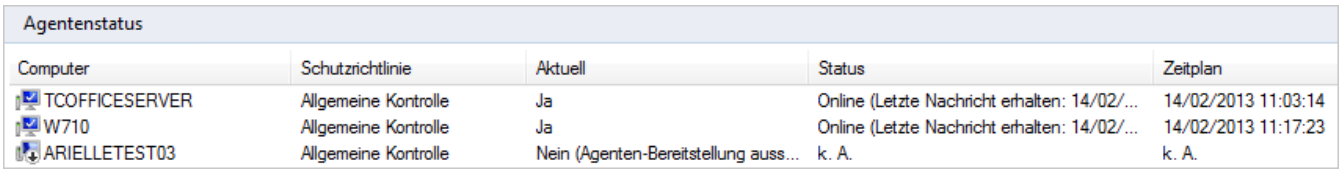
2. Überprüfen Sie im Bereich **Bereitstellungsverlauf** den erfolgreichen Abschluss der Aktualisierung auf dem lokalen Computer. Weitere Informationen finden Sie unter Anzeige des Bereitstellungsstatus (page 110).

4.3.2 Agentenstatus

Verwenden Sie die Informationen aus dem Bereich „Agentenstatus“, um den Status aller Bereitstellungsvorgänge auf den kontrollierten Computern zu bestimmen.

So zeigen Sie den Agentenstatus an:

3. Klicken Sie auf **Status** >**Agenten**.



Screenshot 16: Bereich „Agentenstatus“

4. Bestätigen Sie unter **Agentenstatus** die erfolgreiche Zuweisung der richtigen Schutzrichtlinie auf dem/den zu kontrollierenden Computer(n) und dass die Agentenbereitstellung auf dem neuesten Stand ist.

Hinweis

Jeder Agent sendet regelmäßig seinen Onlinestatus an die Hauptinstallation von GFI EndPointSecurity. Falls diese Daten nicht von der Hauptinstallation empfangen werden, wird der Agent als offline angesehen.

Hinweis

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.

Weitere Informationen zum Bereich „Agentenstatus“ finden Sie im Kapitel „Statusüberwachung“ im Abschnitt Anzeige des Agentenstatus.

5 Anpassen von Schutzrichtlinien

In diesem Kapitel erhalten Sie Informationen zum Ändern der Einstellungen vorkonfigurierter Schutzrichtlinien. Auf diese Weise können Sie Einstellungen jederzeit optimieren, wenn Sie neue Sicherheitsprobleme und potenzielle Sicherheitsrisiken erkennen.

Themen in diesem Kapitel

5.1 Konfigurieren kontrollierter Gerätekategorien

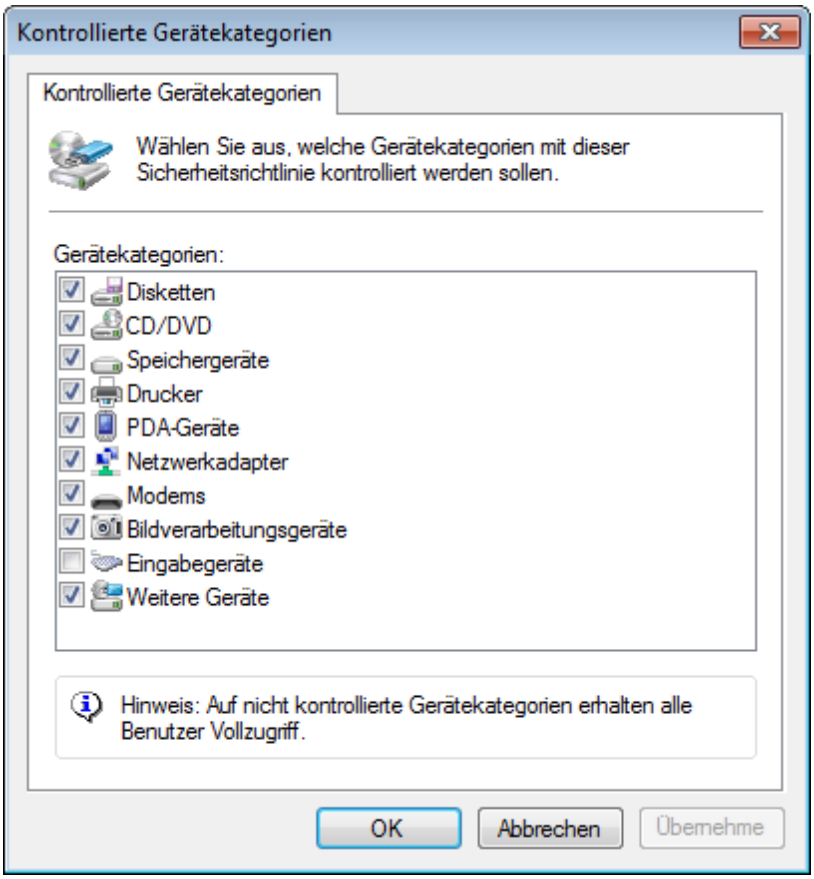
GFI EndPointSecurity bietet Ihnen die Möglichkeit, festzulegen, welche unterstützten Gerätekategorien durch eine Schutzrichtlinie kontrolliert werden sollen. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

Hinweis

Nicht festgelegte Geräte sind über die von der Schutzrichtlinie kontrollierten Computer uneingeschränkt zugänglich. Dadurch kann GFI EndPointSecurity Geräte nicht überwachen oder blockieren, die in eine nicht von der Schutzrichtlinie kontrollierte Kategorie fallen.

So konfigurieren Sie durch eine Schutzrichtlinie kontrollierte Geräte:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.
2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.
3. Klicken Sie auf **Sicherheit**.
4. Klicken Sie unter **Allgemeine Aufgaben** auf **Überwachte Gerätekategorien bearbeiten...**



Screenshot 17: Optionen für kontrollierte Gerätekategorien

5. Aktivieren bzw. deaktivieren Sie im Dialogfeld **Kontrollierte Gerätekategorien** die erforderlichen Gerätekategorien, die durch die Schutzrichtlinie kontrolliert werden sollen, und klicken Sie auf **OK**.

Wichtig

Wenn Sie die Option „Eingabegeräte“ aktivieren und den Zugriff verweigern, können Benutzer keine USB-Tastaturen oder -Mäuse verwenden, die an die durch diese Schutzrichtlinie kontrollierten Computer angeschlossen sind.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.2 Konfigurieren kontrollierter Schnittstellen

GFI EndPointSecurity bietet Ihnen die Möglichkeit, festzulegen, welche Schnittstellen durch eine Schutzrichtlinie kontrolliert werden sollen. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

> **Hinweis**
>
> Nicht festgelegte Schnittstellen sind über die von der Schutzrichtlinie kontrollierten Computer uneingeschränkt zugänglich. Dadurch kann GFI EndPointSecurity Geräte nicht überwachen oder blockieren, die an eine nicht von der Schutzrichtlinie kontrollierte Schnittstelle angeschlossen werden.

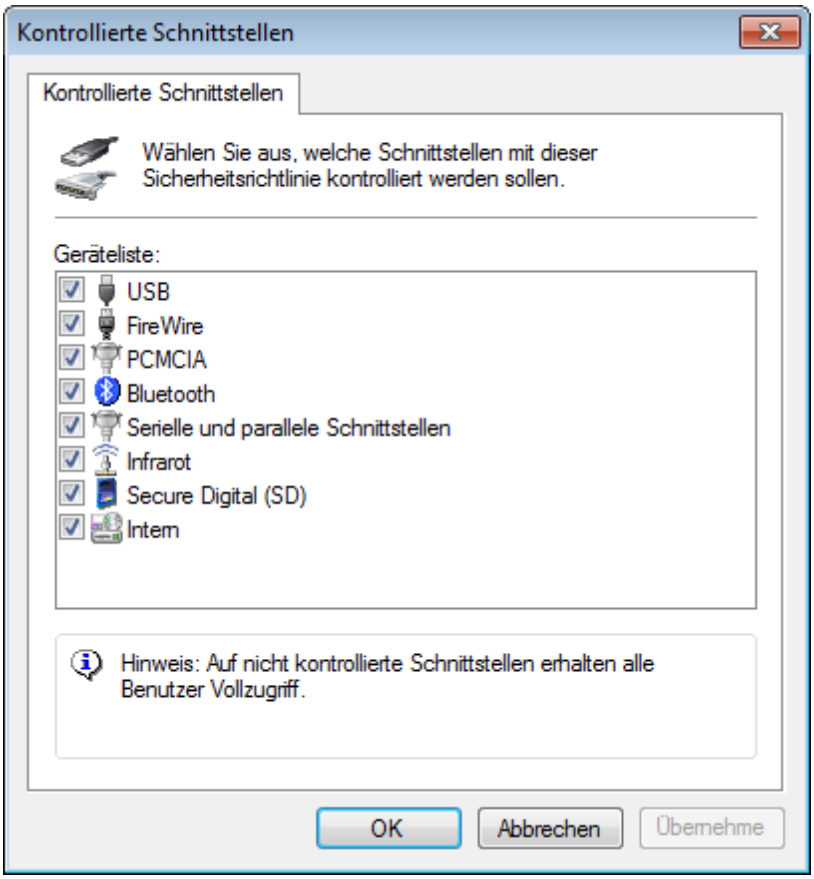
So geben Sie die Schnittstellen an, die durch eine bestimmte Schutzrichtlinie kontrolliert werden sollen:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie auf **Sicherheit**.

4. Klicken Sie unter **Allgemeine Aufgaben** auf **Überwachte Schnittstellen bearbeiten...**



Screenshot 18: Optionen für kontrollierte Schnittstellen

5. Aktivieren bzw. deaktivieren Sie im Dialogfeld **Kontrollierte Schnittstellen** die erforderlichen Schnittstellen, die durch die Schutzrichtlinie kontrolliert werden sollen, und klicken Sie auf **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.3 Konfigurieren der Hauptbenutzer

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Active Directory (AD)-Benutzer und/oder -Benutzergruppen als Hauptbenutzer festzulegen. Hauptbenutzer besitzen automatisch vollen Zugriff auf alle Geräte, die an einem durch eine Schutzrichtlinie kontrollierten Computer angeschlossen sind. Es können mehrere Hauptbenutzer für jede Schutzrichtlinie definiert werden.

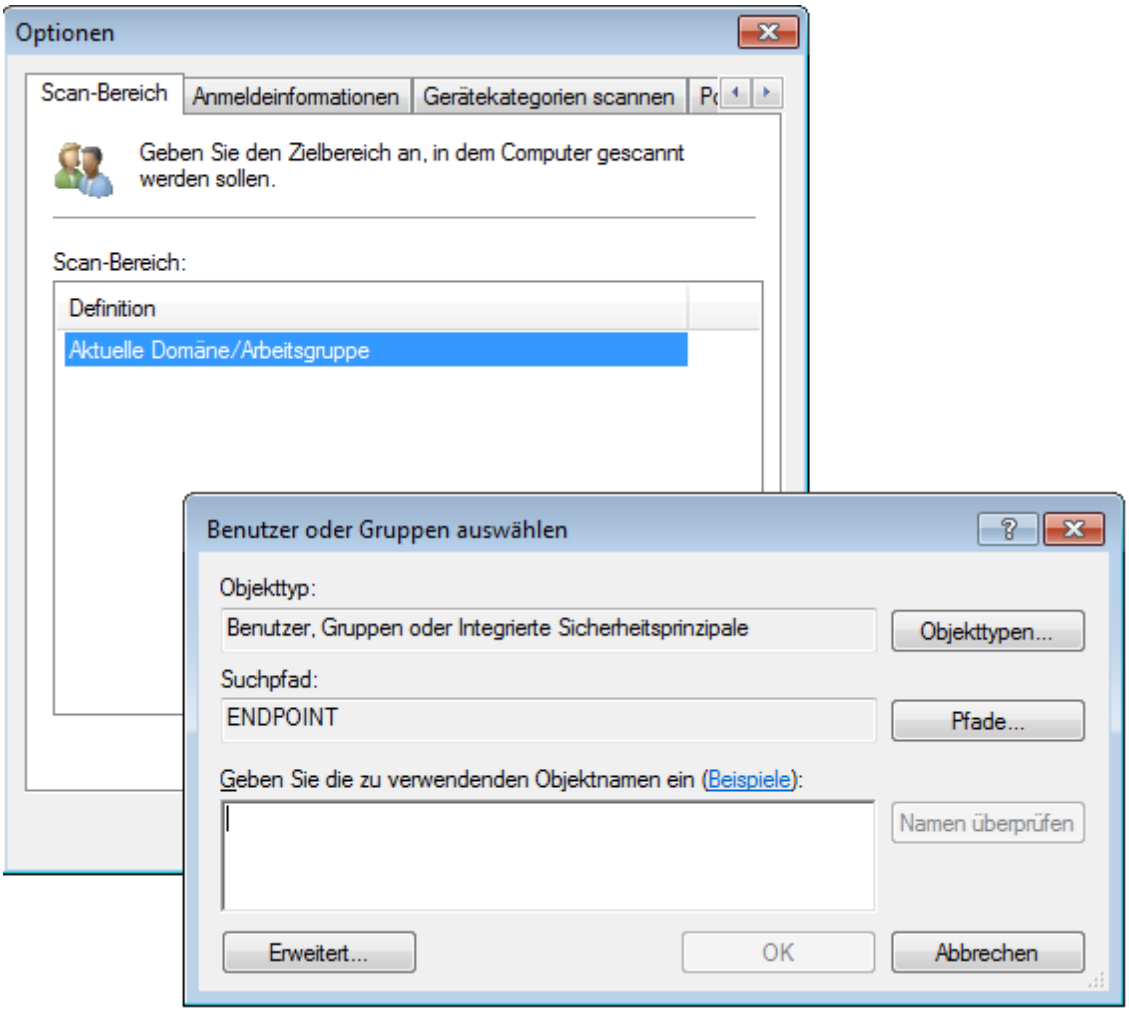
Bei der Definition von Hauptbenutzern ist große Vorsicht geboten, da für diese Benutzer sämtliche durch die jeweilige Schutzrichtlinie definierten Einschränkungen nicht gelten.

So legen Sie Hauptbenutzer für eine Schutzrichtlinie fest:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie im rechten Bereich im Abschnitt **Sicherheit** auf **Hauptbenutzer**.



Screenshot 19: Optionen für Hauptbenutzer

4. Führen Sie im Dialogfeld „Hauptbenutzer“ eine der folgenden Optionen durch:

» **Option 1**: Klicken Sie auf **Hinzufügen**, um die Benutzer/Gruppen festzulegen, die für diese Schutzrichtlinie die Hauptbenutzer sein sollen. Klicken Sie anschließend auf **OK**.

» **Option 2**: Markieren Sie die Benutzer/Gruppen, die keine Hauptbenutzer mehr sein sollen, und klicken Sie auf **Entfernen**. Klicken Sie anschließend auf **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.4 Konfigurieren von Zugriffsberechtigungen für Gerätekategorien

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Berechtigungen für Gerätekategorien den Active Directory (AD)-Benutzern und/oder -Benutzergruppen zuzuweisen. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

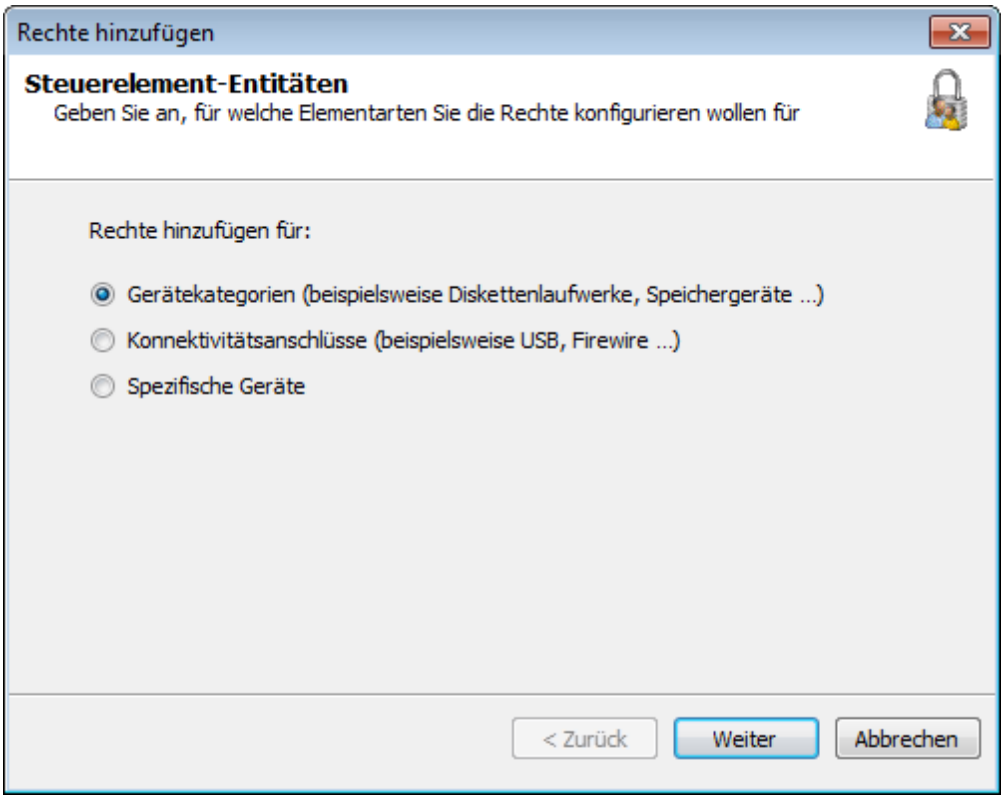
Wenn eine Gerätekategorie nicht durch eine Schutzrichtlinie kontrolliert wird, ist der jeweilige Eintrag deaktiviert. Weitere Informationen finden Sie unter Konfigurieren kontrollierter Gerätekategorien (page 45).

So konfigurieren Sie Berechtigungen für den Zugriff auf Gerätekategorien für Benutzer innerhalb einer Schutzrichtlinie:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

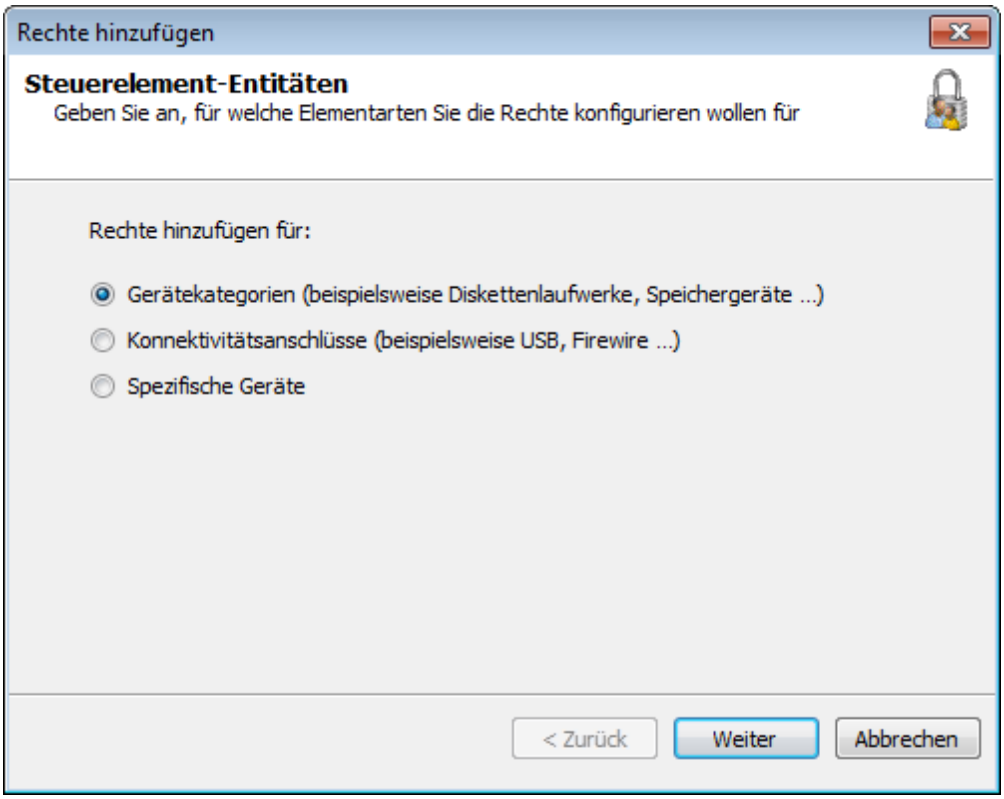
2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie unter **Allgemeine Aufgaben** auf **Berechtigung(en) hinzufügen...**



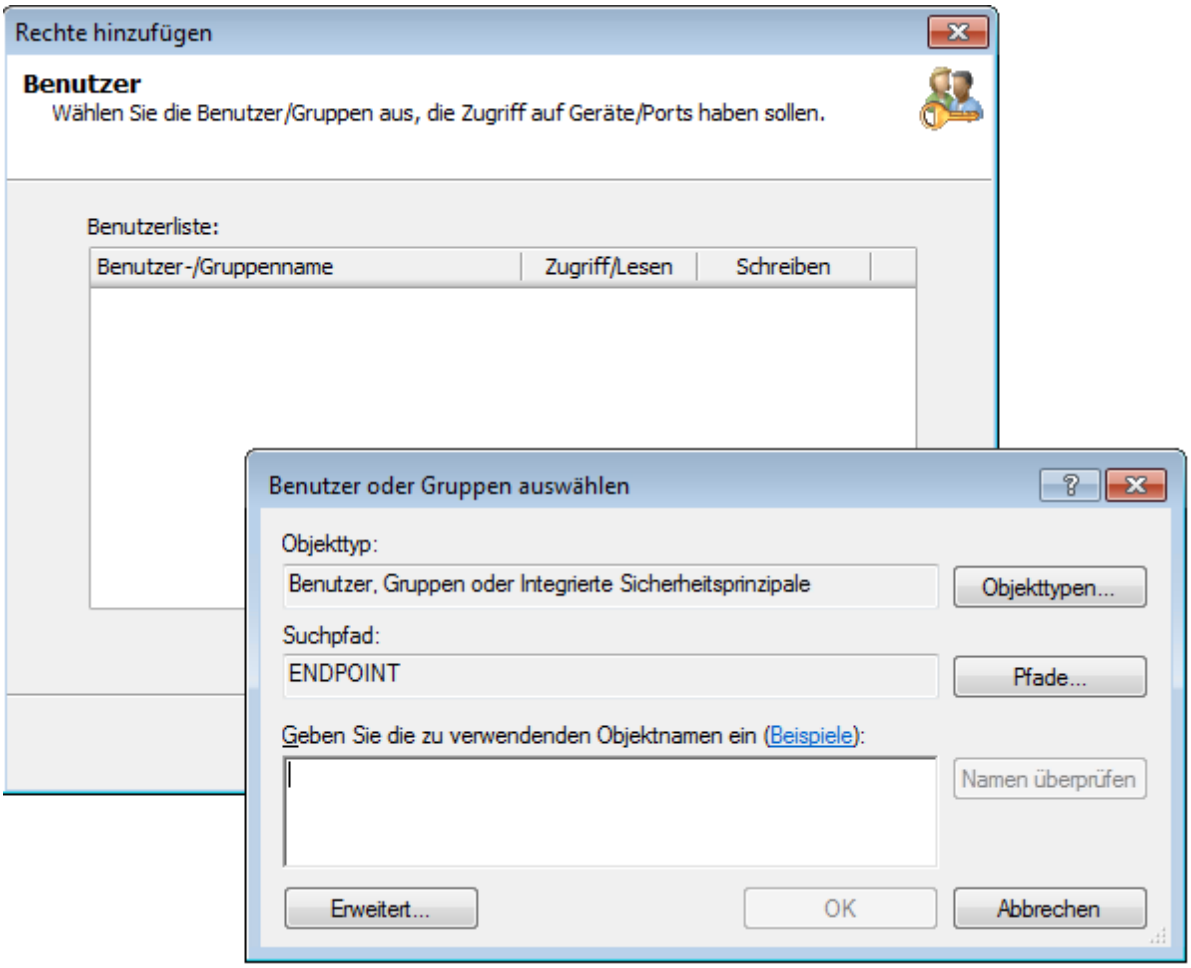
Screenshot 20: Optionen zum Hinzufügen von Berechtigungen - Steuerelement-Entitäten

4. Wählen Sie im Dialogfeld **Berechtigungen hinzufügen** die Option **Gerätekategorien**, und klicken Sie auf **Weiter**.



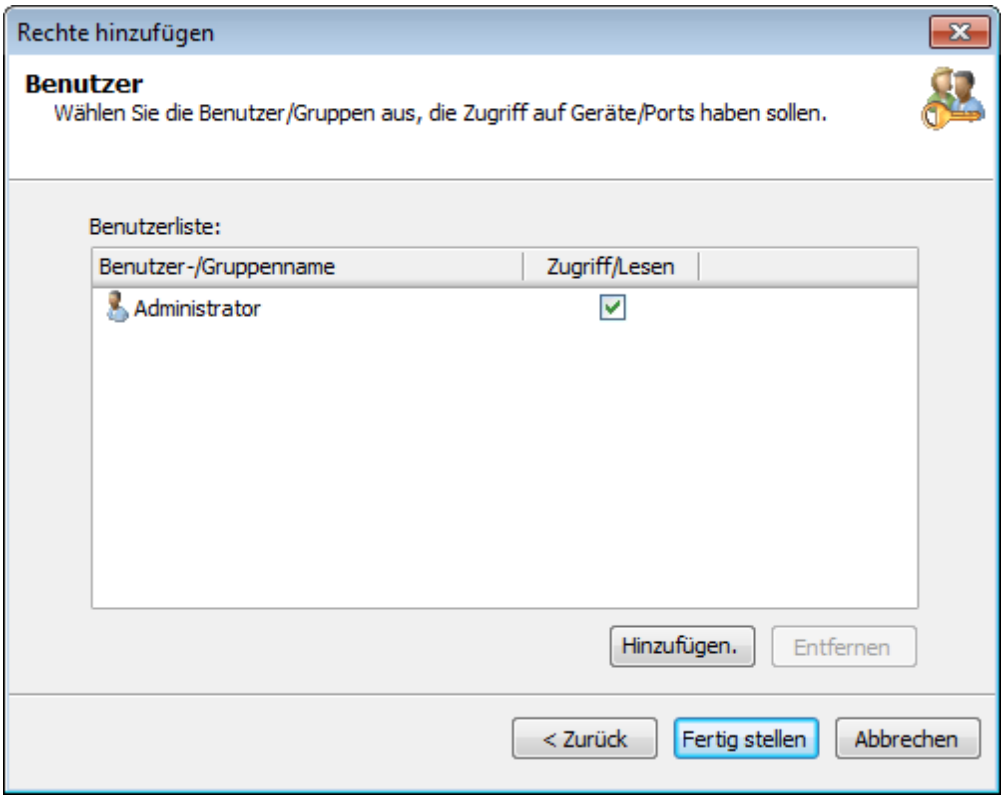
Screenshot 21: Optionen zum Hinzufügen von Berechtigungen - Gerätekategorien

5. Aktivieren oder deaktivieren Sie die gewünschten Gerätekategorien, für die Berechtigungen konfiguriert werden sollen. Klicken Sie anschließend auf **Weiter**.



Screenshot 22: Optionen zum Hinzufügen von Berechtigungen - Benutzer

6. Klicken Sie auf **Hinzufügen...**, um den/die Benutzer/Gruppe(n) festzulegen, der/die auf die festgelegten Gerätekategorien in dieser Schutzrichtlinie Zugriff hat/haben. Klicken Sie anschließend auf **OK**.



Screenshot 23: Optionen zum Hinzufügen von Berechtigungen - Benutzer

7. Aktivieren oder deaktivieren Sie die Zugriffs- sowie Lese- und Schreibberechtigungen für die festgelegten Benutzer/Gruppen. Klicken Sie anschließend auf **Fertig stellen**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.5 Konfigurieren von Zugriffsberechtigungen für Schnittstellen

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Berechtigungen für Schnittstellen den Active Directory (AD)-Benutzern und/oder -Benutzergruppen zuzuweisen. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

Wenn eine Schnittstelle nicht durch eine Schutzrichtlinie kontrolliert wird, ist die jeweilige Berechtigung deaktiviert. Weitere Informationen finden Sie unter Konfigurieren kontrollierter Schnittstellen (page 47).

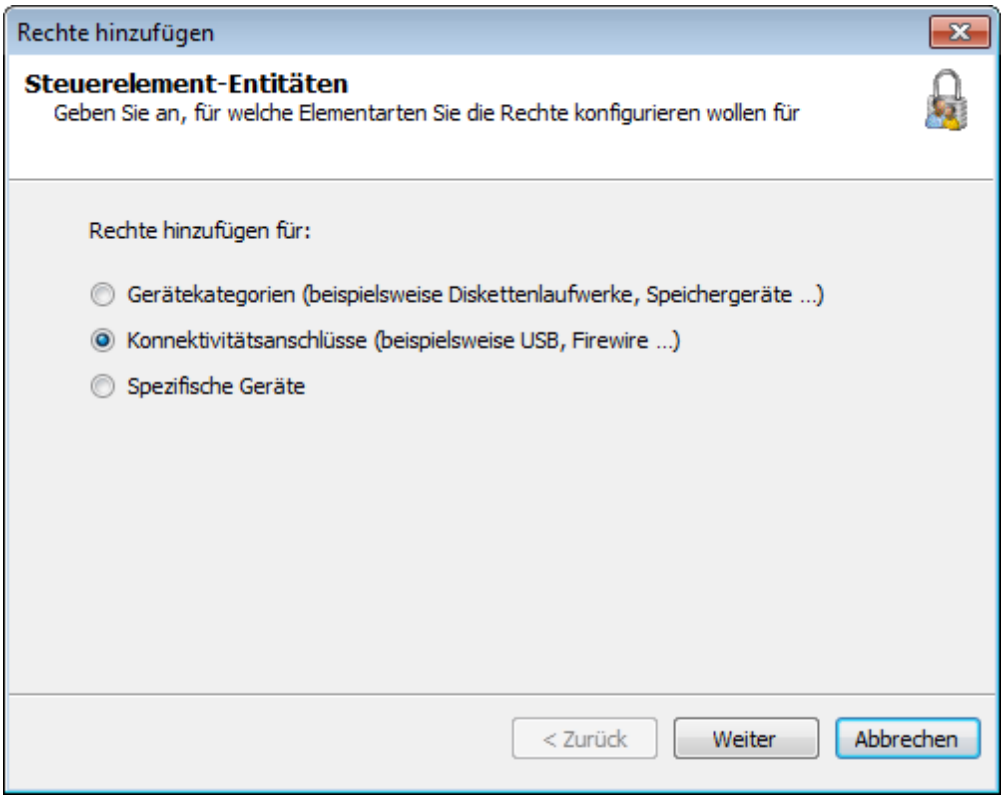
So konfigurieren Sie Benutzerberechtigungen für die Verwendung von Schnittstellen innerhalb einer Schutzrichtlinie:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

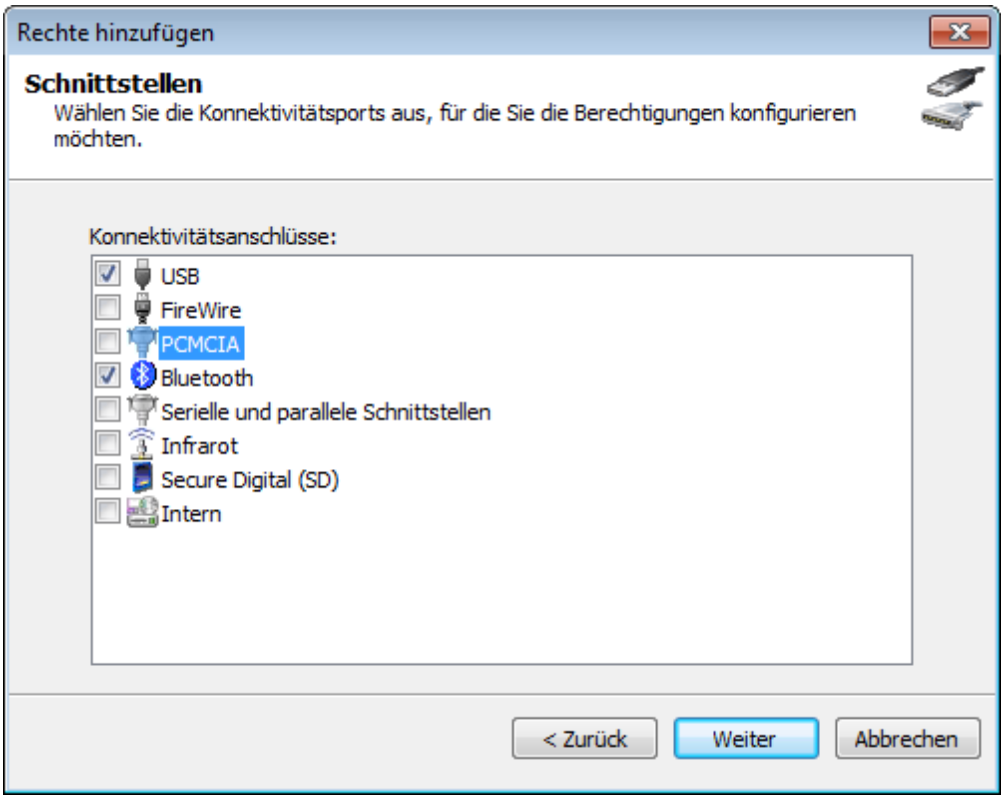
3. Klicken Sie auf **Sicherheit** > **Berechtigungen festlegen**.

4. Klicken Sie unter **Allgemeine Aufgaben** auf **Berechtigung(en) hinzufügen...**



Screenshot 24: Optionen zum Hinzufügen von Berechtigungen - Steuerelement-Entitäten

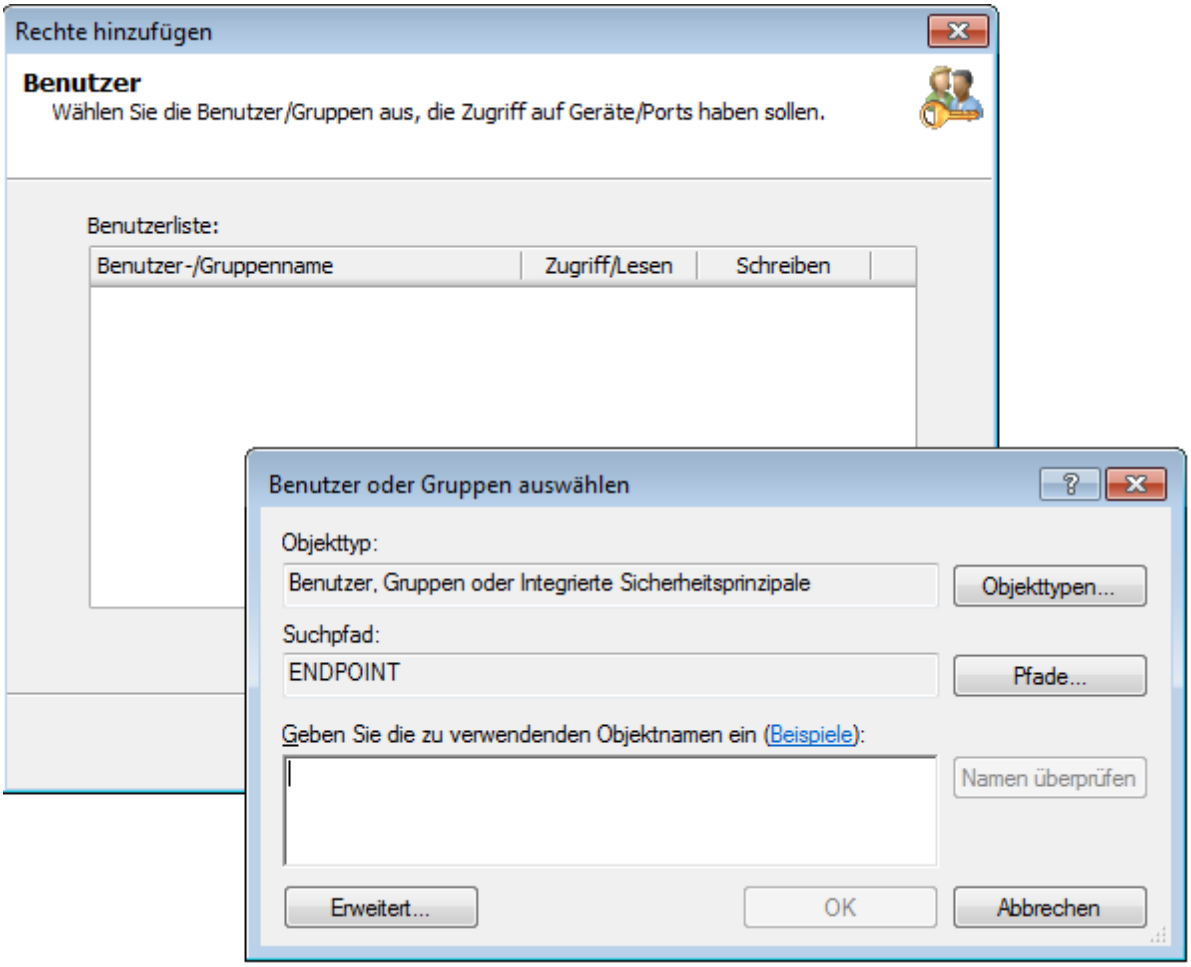
5. Wählen Sie im Dialogfeld **Berechtigungen hinzufügen** die Option **Schnittstellen**, und klicken Sie auf **Weiter**.



Screenshot 25: Optionen zum Hinzufügen von Berechtigungen - Schnittstellen

6. Aktivieren oder deaktivieren Sie die gewünschten Schnittstellen, für die Berechtigungen konfiguriert werden sollen. Klicken Sie anschließend auf **Weiter**.

7. Klicken Sie auf **Hinzufügen...**, um die Benutzer/Gruppe(n) festzulegen, die auf die festgelegten Schnittstellen in dieser Schutzrichtlinie Zugriff haben. Klicken Sie anschließend auf **OK**.



Screenshot 26: Optionen zum Hinzufügen von Berechtigungen - Benutzer

8. Aktivieren oder deaktivieren Sie die Zugriffs-/Leseberechtigungen für den/die jeweilige(n) festgelegte(n) Benutzer/Gruppe. Klicken Sie anschließend auf **Fertig stellen**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.6 Konfigurieren von Zugriffsberechtigungen für einzelne Geräte

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Berechtigungen für einzelne Geräte den Active Directory (AD)-Benutzern und/oder -Benutzergruppen zuzuweisen. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

Beispielsweise können Sie für einen bestimmten unternehmensintern erlaubten USB-Speicherstick den Lesezugriff erlauben. Versuche, auf andere USB-Sticks zuzugreifen, werden hingegen blockiert.

Hinweis

Führen Sie für eine Liste von Geräten, die momentan an kontrollierten Computern angeschlossen sind, einen Gerätescan durch, und fügen Sie die erkannten Geräte der Gerätedatenbank hinzu, um Zugriffsberechtigungen für einzelne Geräte zu konfigurieren. Weitere Informationen finden Sie unter Erkennen von Geräten (page 91).

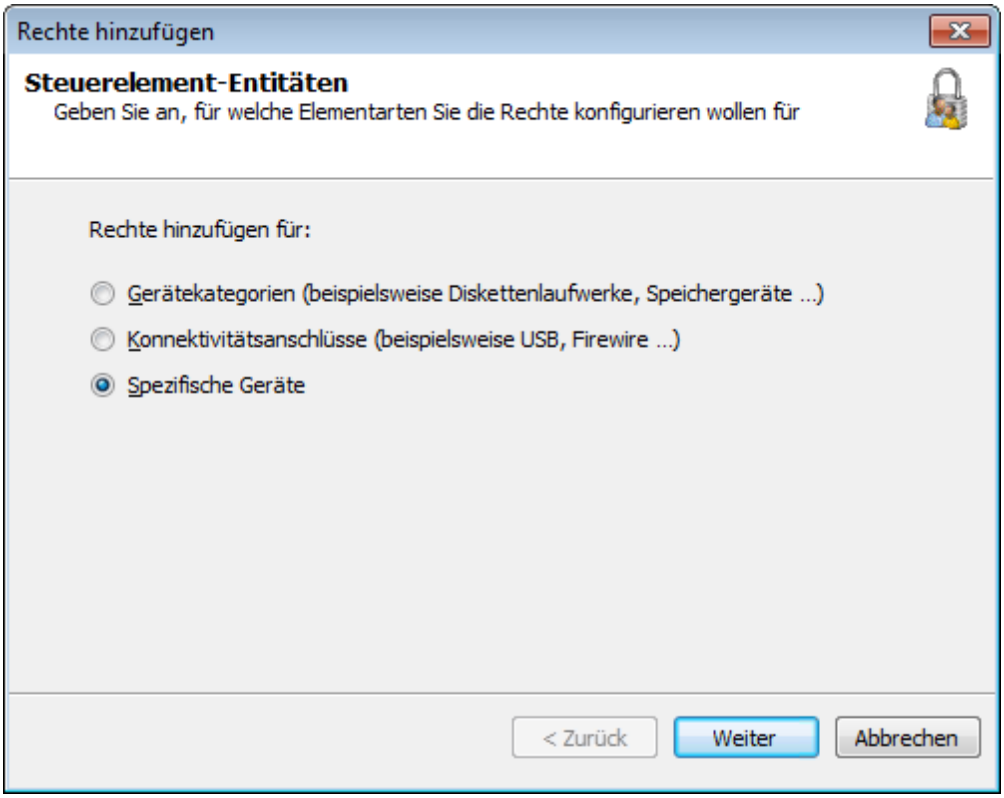
So konfigurieren Sie Berechtigungen für den Zugriff auf bestimmte Geräte für Benutzer innerhalb einer Schutzrichtlinie:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie auf den Unterknoten **Sicherheit**.

4. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf **Berechtigung(en) hinzufügen...**

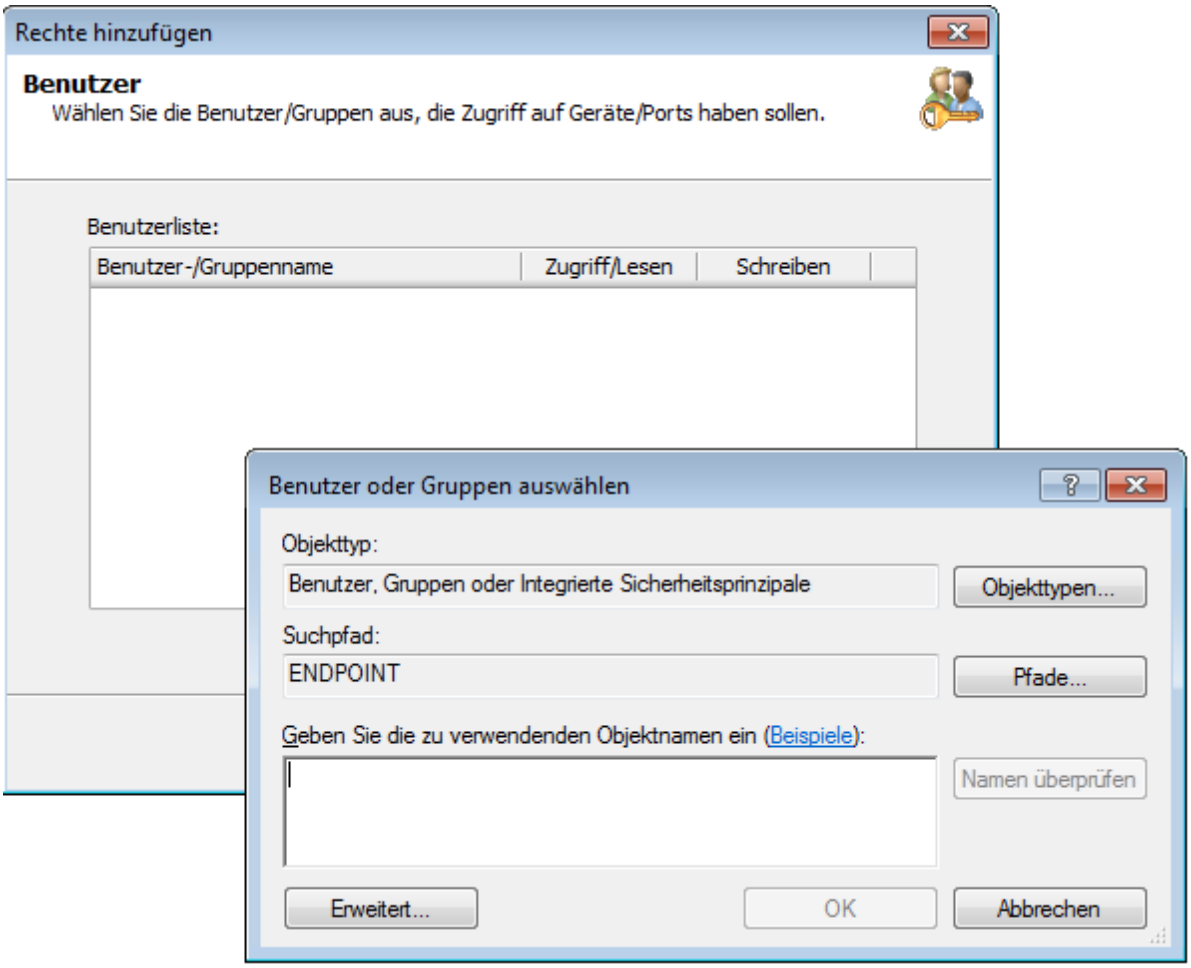


Screenshot 27: Optionen zum Hinzufügen von Berechtigungen - Steuerelement-Entitäten

5. Wählen Sie im Dialogfeld **Berechtigungen hinzufügen** die Option **Spezifische Geräte**, und klicken Sie auf **Weiter**.

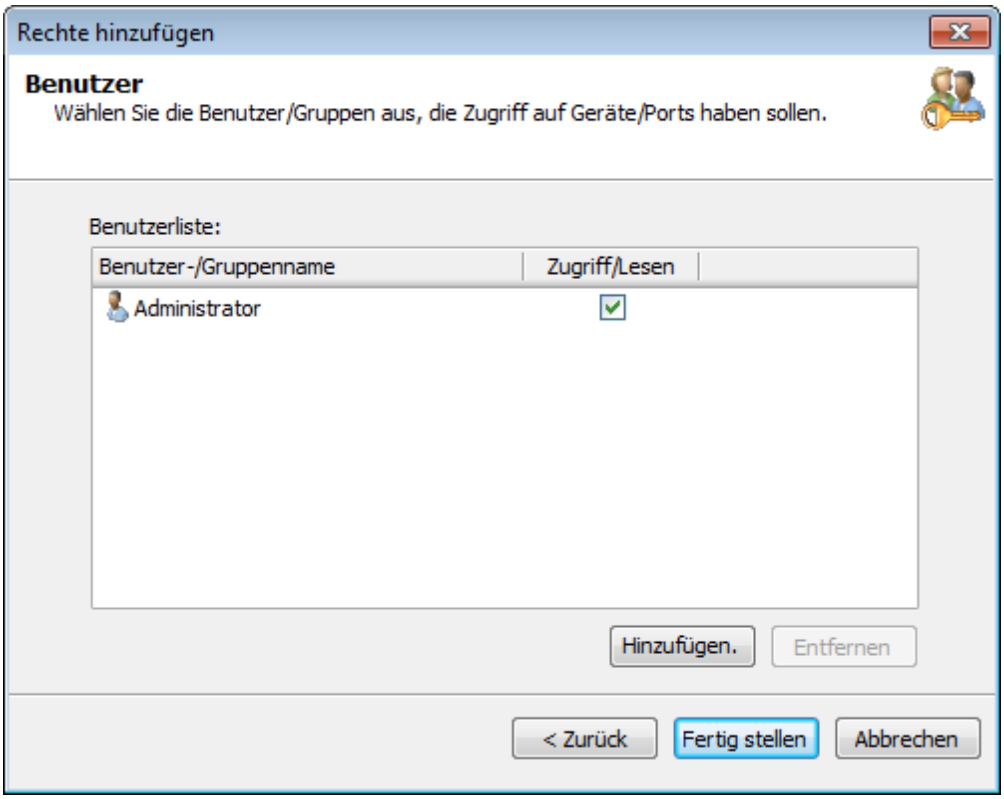
Screenshot 28: Optionen zum Hinzufügen von Berechtigungen - Spezifische Geräte

6. Aktivieren oder deaktivieren Sie die gewünschten Geräte in der Geräteliste, für die Berechtigungen konfiguriert werden sollen. Klicken Sie anschließend auf **Weiter**. Falls ein gewünschtes Gerät nicht aufgelistet ist, klicken Sie auf **Neues Gerät hinzufügen...**, um die Details des Geräts, für das Berechtigungen konfiguriert werden sollen, festzulegen. Klicken Sie anschließend auf **OK**.



Screenshot 29: Optionen zum Hinzufügen von Berechtigungen - Benutzer

7. Klicken Sie auf **Hinzufügen...**, um den/die Benutzer/Gruppe(n) festzulegen, der/die auf die festgelegten Geräte in dieser Schutzrichtlinie Zugriff hat/haben. Klicken Sie anschließend auf **OK**.



Screenshot 30: Optionen zum Hinzufügen von Berechtigungen - Benutzer

8. Aktivieren oder deaktivieren Sie die Zugriffs- sowie Lese- und Schreibberechtigungen für den/die festgelegte(n) Benutzer/Gruppe. Klicken Sie anschließend auf **Fertig stellen**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.7 Anzeigen von Zugriffsberechtigungen

GFI EndPointSecurity bietet Ihnen die Möglichkeit, alle Berechtigungen anzuzeigen, die Active Directory (AD)-Benutzern und/oder -Benutzergruppen zugewiesen sind. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

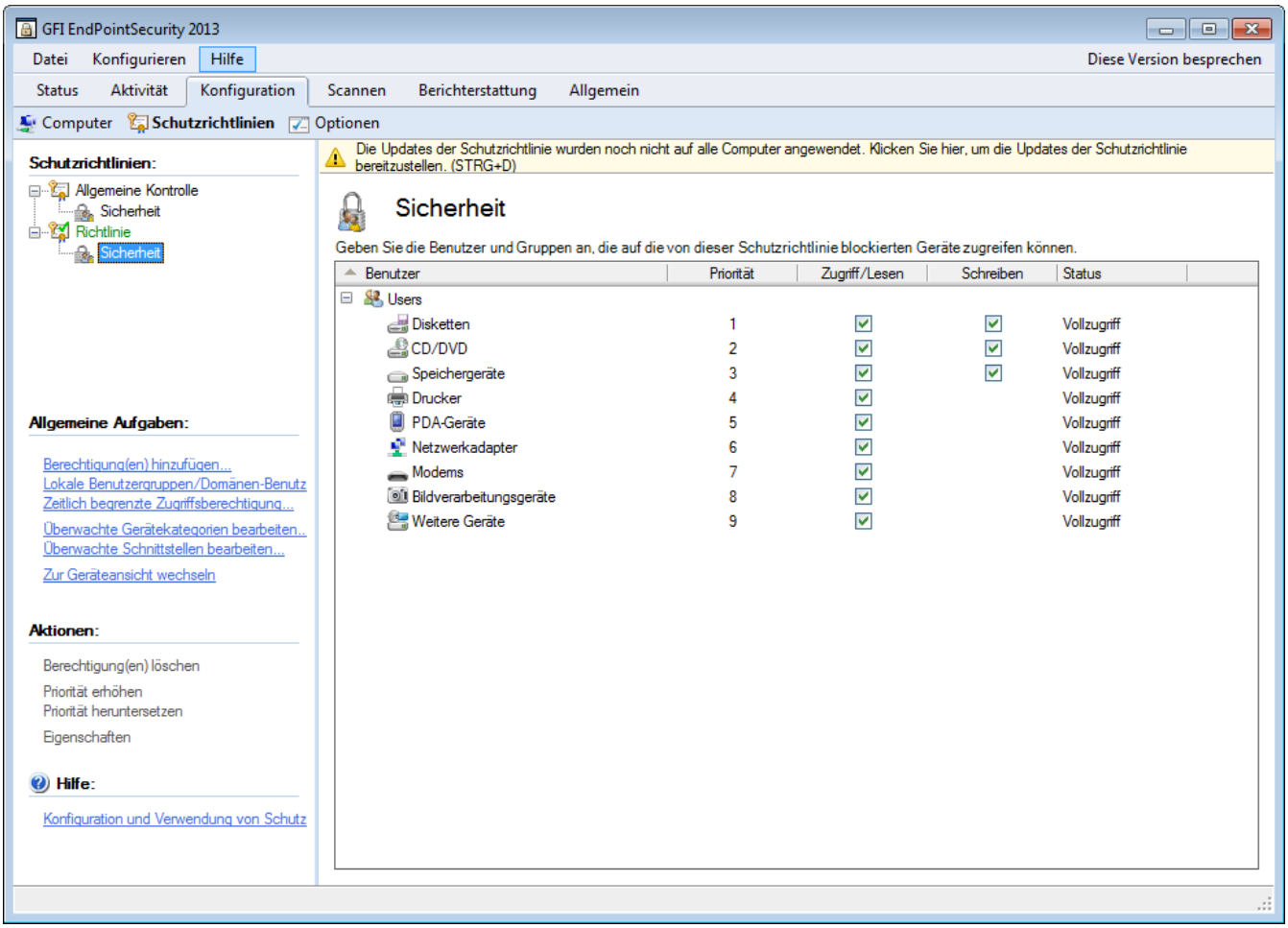
Wenn eine Gerätekategorie oder Schnittstelle nicht durch eine Schutzrichtlinie kontrolliert wird, ist die jeweilige Berechtigung deaktiviert. Weitere Informationen finden Sie unter Konfigurieren kontrollierter Gerätekategorien oder Konfigurieren kontrollierter Schnittstellen.

So zeigen Sie alle Benutzerberechtigungen innerhalb einer Schutzrichtlinie an:

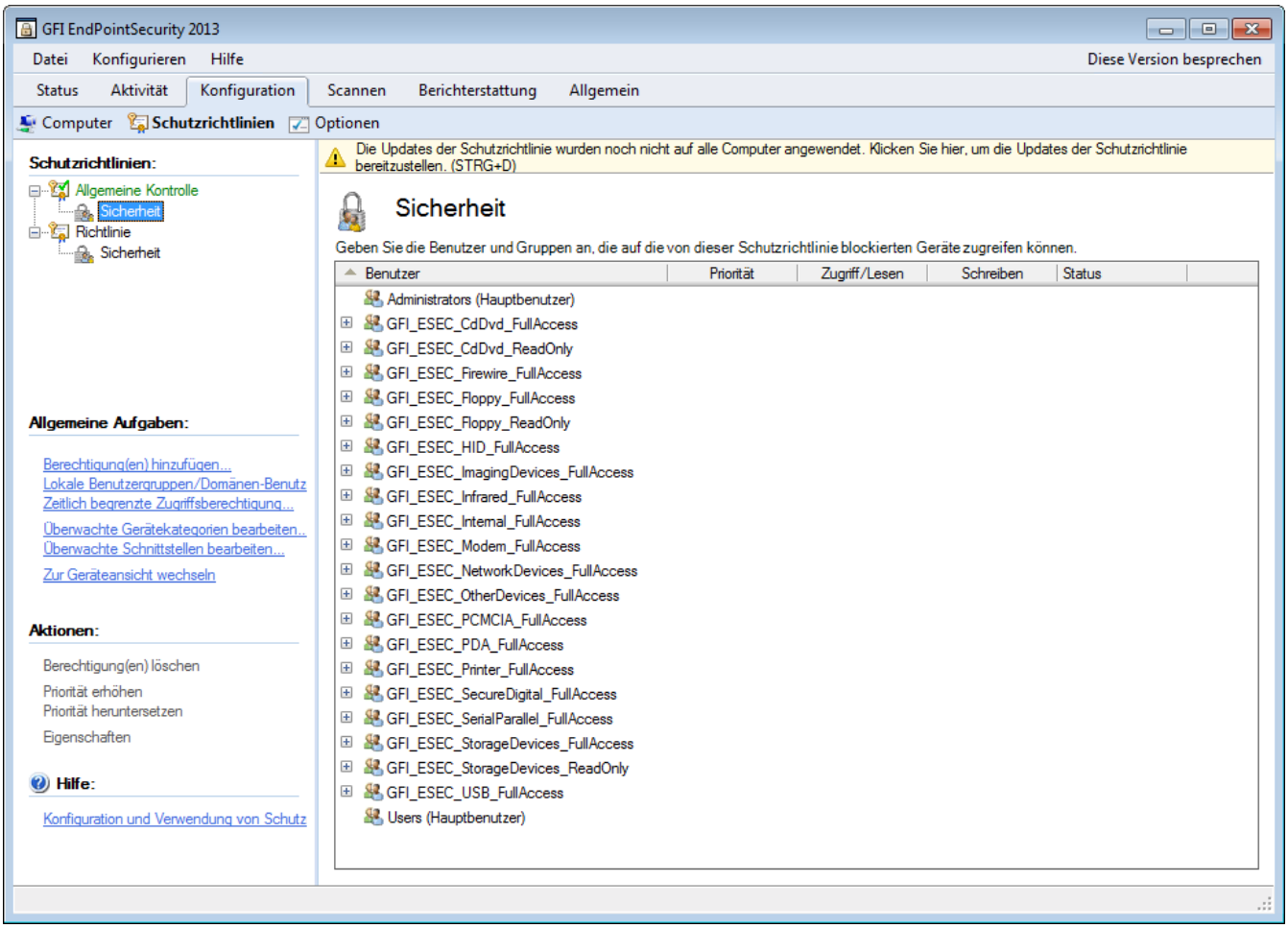
1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie auf **Sicherheit**. Im rechten Bereich werden alle für die Schutzrichtlinie festgelegten Berechtigungen angezeigt.



Screenshot 31: Untergeordnete Registerkarte „Schutzrichtlinien“ - Geräteansicht



Screenshot 32: Untergeordnete Registerkarte „Schutzrichtlinien“ - Benutzeransicht

4. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf **Zur Geräteansicht wechseln** oder auf **Zur Benutzeransicht wechseln**, um Berechtigungen gruppiert nach Gerät/Schnittstelle oder Benutzer anzuzeigen.

> **Hinweis**
>
> In der Benutzeransicht sehen Sie zudem die für die Schutzrichtlinie festgelegten Hauptbenutzer.

5.8 Konfigurieren von Berechtigungsprioritäten

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Berechtigungen zu priorisieren, die Active Directory (AD)-Benutzern und/oder -Benutzergruppen zugewiesen sind. Diese Konfigurierung kann für jede einzelne Richtlinie und jeden einzelnen Benutzer erfolgen.

Beispielsweise können Sie benutzerspezifisch innerhalb einer Schutzrichtlinie angeben, dass die Zugriffsberechtigungen für USB-Anschlüsse die Priorität 1 haben sollen, während für CD-/DVD-Laufwerke die Priorität 2 gilt. Schließt in diesem Fall ein Benutzer ein externes CD-/DVD-Laufwerk über den USB-Anschluss an einen kontrollierten Computer an, haben die USB-Zugriffsberechtigungen Vorrang vor denen des CD-/DVD-Laufwerks.

Screenshot 33: Untergeordnete Registerkarte „Schutzrichtlinien“ - Bereich „Sicherheit“

So priorisieren Sie Benutzerberechtigungen innerhalb einer Schutzrichtlinie:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie auf den Unterknoten **Sicherheit**.

4. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf **Zur Benutzeransicht wechseln**, um nach Benutzern gruppierte Berechtigungen anzuzeigen.

5. Klicken Sie mit der rechten Maustaste auf den Abschnitt **Sicherheit**, und wählen Sie **Alle erweitern** aus.

6. Markieren Sie das gewünschte Gerät oder die gewünschte Schnittstelle.

7. Klicken Sie im linken Bereich im Abschnitt **Aktionen** auf **Priorität erhöhen** oder **Priorität herunterstellen**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.9 Konfigurieren der Geräte-Blacklist

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Geräte festzulegen, auf die nicht jeder Zugriff hat. Mithilfe einer differenzierten Blacklist können sogar per Seriennummer identifizierte Einzelgeräte blockiert werden. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

Führen Sie für eine Liste von Geräten, die momentan an kontrollierten Computern angeschlossen sind, einen Gerätescan durch, und fügen Sie die erkannten Geräte der Gerätedatenbank hinzu, bevor Sie sie der Geräte-Blacklist hinzufügen. Weitere Informationen finden Sie unter Erkennen von Geräten (page 91).

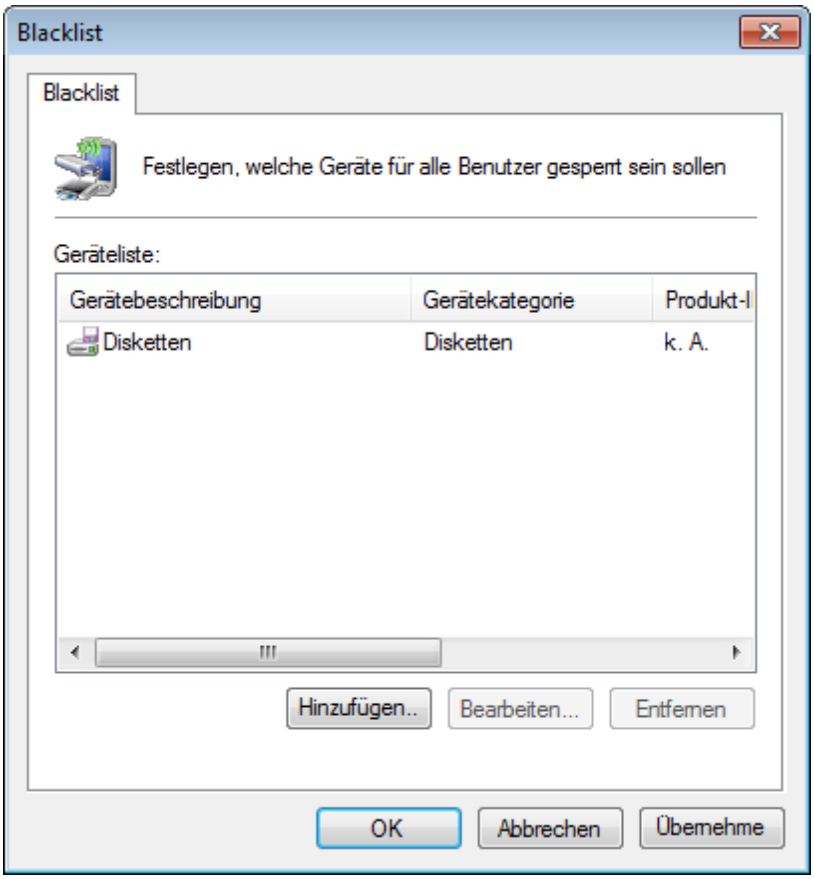
> **Hinweis**
>
> Hauptbenutzer können auf alle Geräte auf der Blacklist zugreifen.

So fügen Sie Geräte einer Schutzrichtlinie der Blacklist hinzu:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

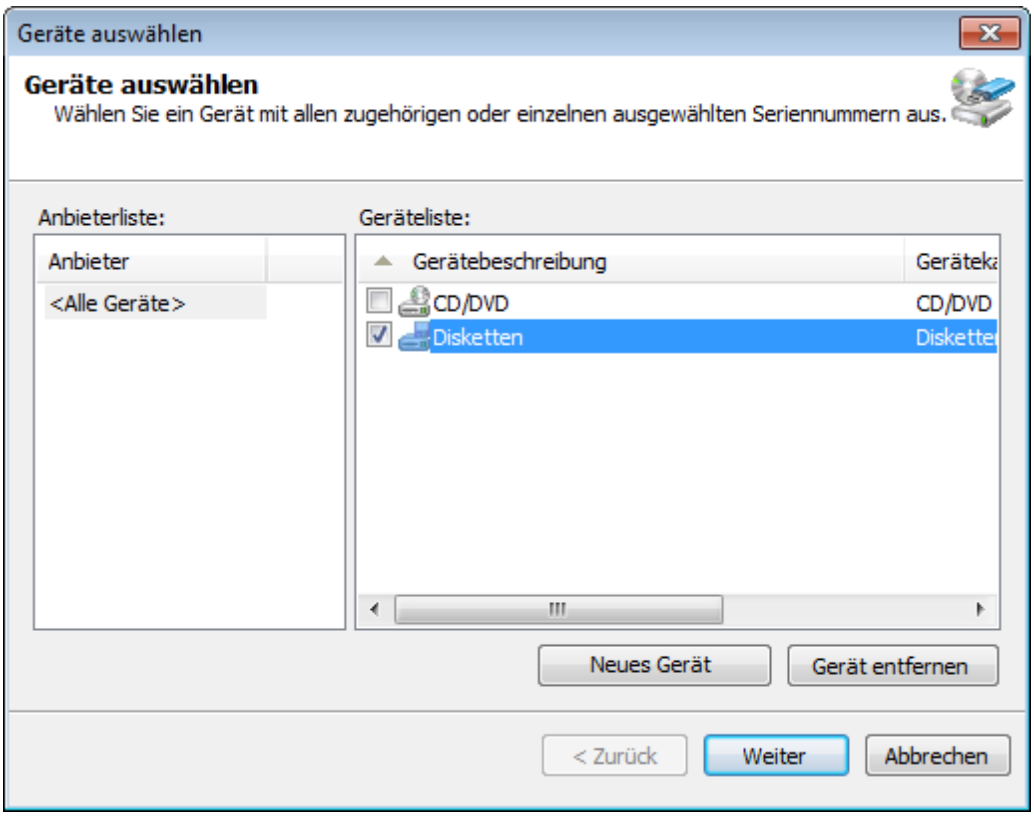
2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie im rechten Bereich des Abschnitts **Allgemeine Kontrolle** auf **Geräte-Blacklist**.



Screenshot 34: Blacklist-Optionen

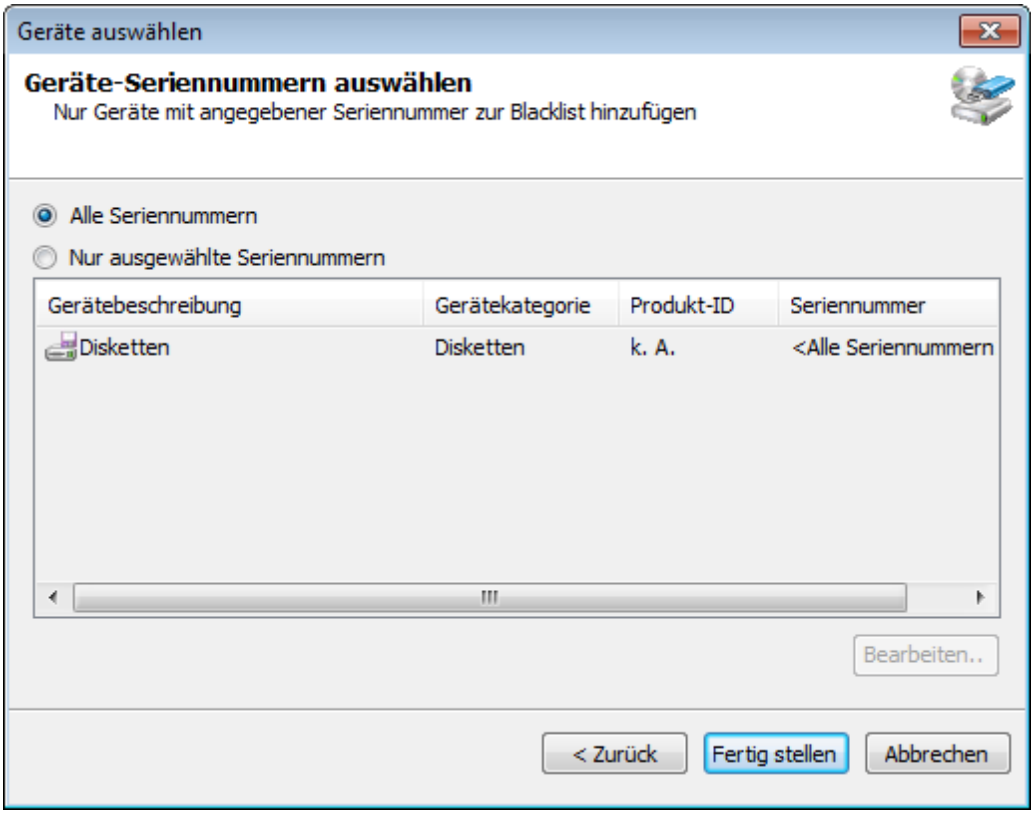
4. Klicken Sie im Dialogfeld **Blacklist** auf die Option **Hinzufügen…**, um Geräte für die Blacklist auszuwählen.



Screenshot 35: Optionen zur Geräteauswahl

5. Aktivieren oder deaktivieren Sie im Dialogfeld **Geräte auswählen** die Geräte, die aus der Geräteliste der Blacklist hinzugefügt werden sollen. Klicken Sie anschließend auf **Weiter**.

> **Hinweis**
>
> Falls ein gewünschtes Gerät nicht aufgelistet ist, klicken Sie auf **Neues Gerät hinzufügen…**, um die Details des Geräts, das der Blacklist hinzugefügt werden soll, festzulegen. Klicken Sie anschließend auf **OK**.

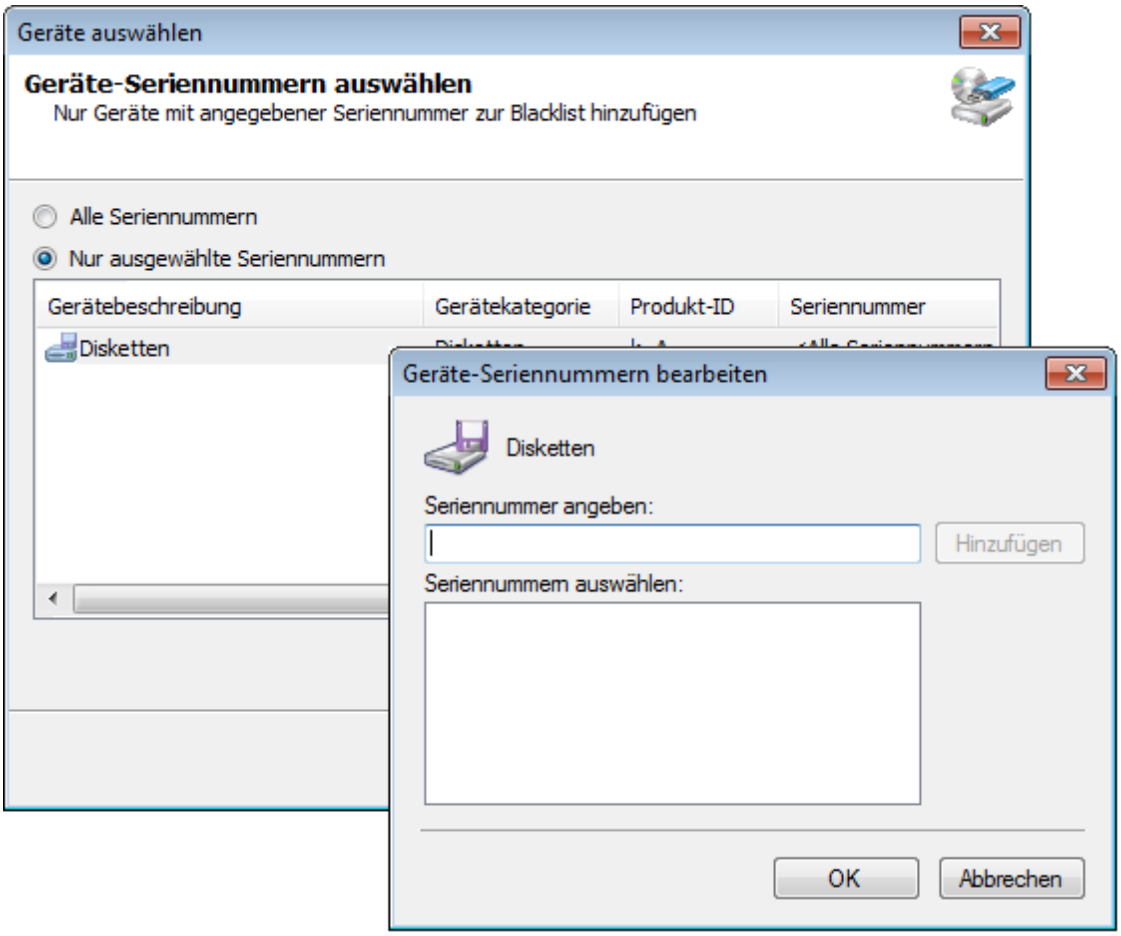


Screenshot 36: Optionen zur Geräteauswahl - Auswahl der Geräteseriennummer

6. Wählen Sie die gewünschte Option für die Seriennummern aus:

» **Alle Seriennummern** – Um alle Seriennummern eines Geräts der Blacklist hinzuzufügen. Klicken Sie auf **Fertig stellen** und **OK**.

» **Nur ausgewählte Seriennummern** – Um nur bestimmte Seriennummern von Geräten der Blacklist hinzuzufügen. Markieren Sie anschließend das Gerät, und klicken Sie auf **Bearbeiten…**, um eine Seriennummer anzugeben. Klicken Sie auf **OK**, **Fertig stellen** und **OK**.



Screenshot 37: Optionen zur Geräteauswahl - Bearbeiten der Geräteseriennummern

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.10 Konfigurieren der Geräte-Whitelist

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Geräte festzulegen, auf die jeder Zugriff hat. Mithilfe einer differenzierten Whitelist können sogar bestimmte, per Seriennummer identifizierte Einzelgeräte zugänglich gemacht werden. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

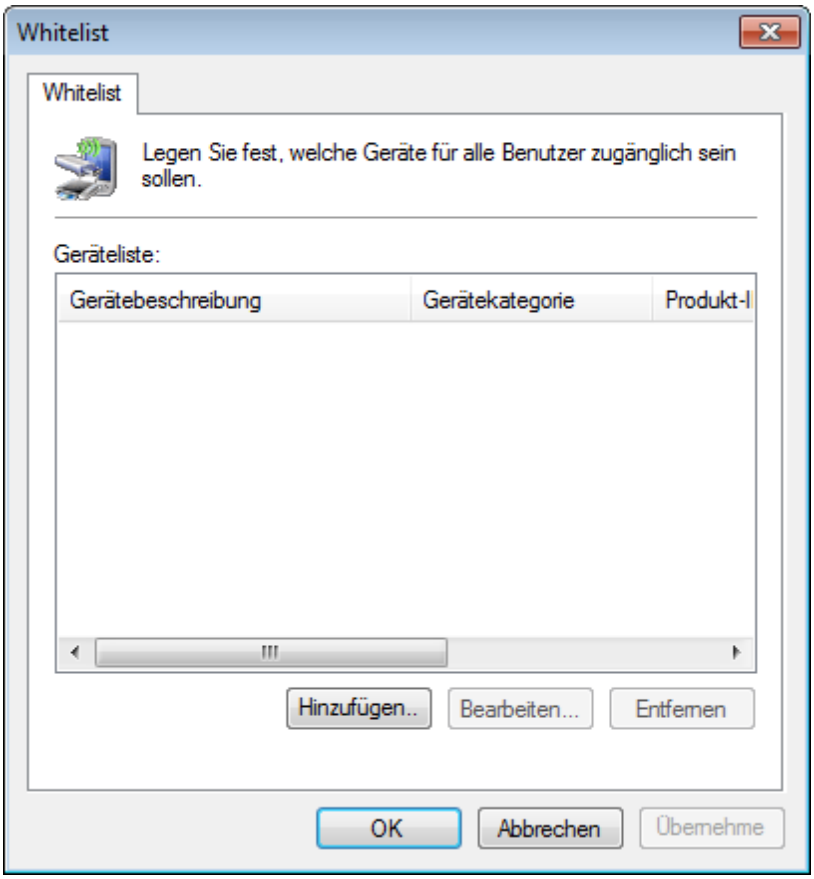
Führen Sie für eine Liste von Geräten, die momentan an kontrollierten Computern angeschlossen sind, einen Gerätescan durch, und fügen Sie die erkannten Geräte der Gerätedatenbank hinzu, bevor Sie sie der Geräte-Whitelist hinzufügen. Weitere Informationen finden Sie unter Erkennen von Geräten (page 91).

So fügen Sie Geräte der Whitelist einer Schutzrichtlinie hinzu:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

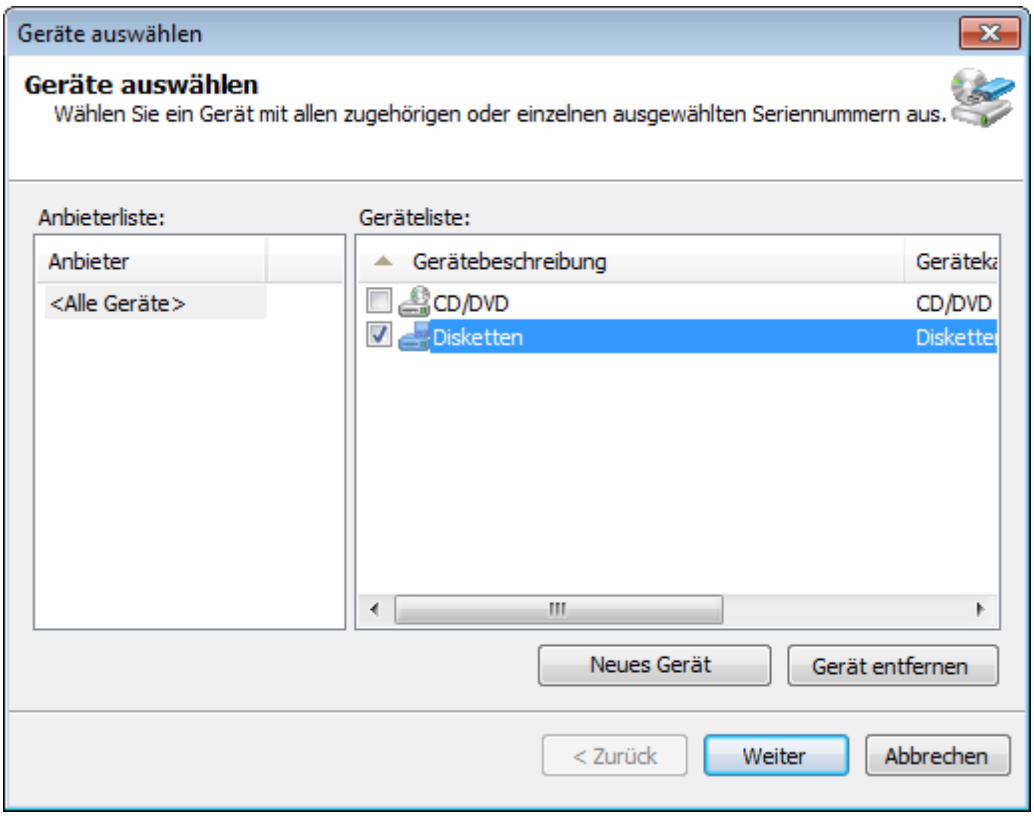
2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie im rechten Bereich des Abschnitts **Allgemeine Kontrolle** auf **Geräte-Whitelist**.



Screenshot 38: Whitelist-Optionen

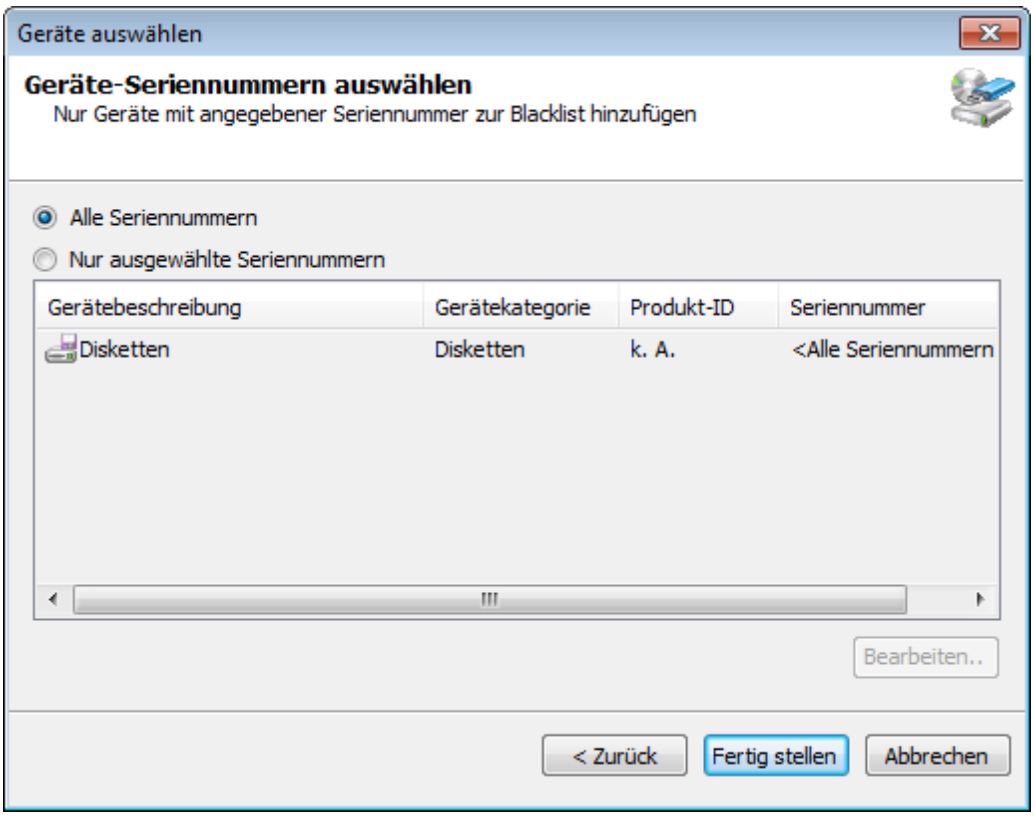
4. Klicken Sie im Dialogfeld **Whitelist** auf die Option **Hinzufügen…**, um Geräte für die Whitelist auszuwählen.



Screenshot 39: Optionen zur Geräteauswahl

5. Aktivieren oder deaktivieren Sie im Dialogfeld **Geräte auswählen** die Geräte, die aus der Geräteliste der Whitelist hinzugefügt werden sollen. Klicken Sie anschließend auf **Weiter**.

> **Hinweis**
>
> Falls ein gewünschtes Gerät nicht aufgelistet ist, klicken Sie auf **Neues Gerät hinzufügen…**, um die Details des Geräts, das der Whitelist hinzugefügt werden soll, festzulegen. Klicken Sie anschließend auf **OK**.

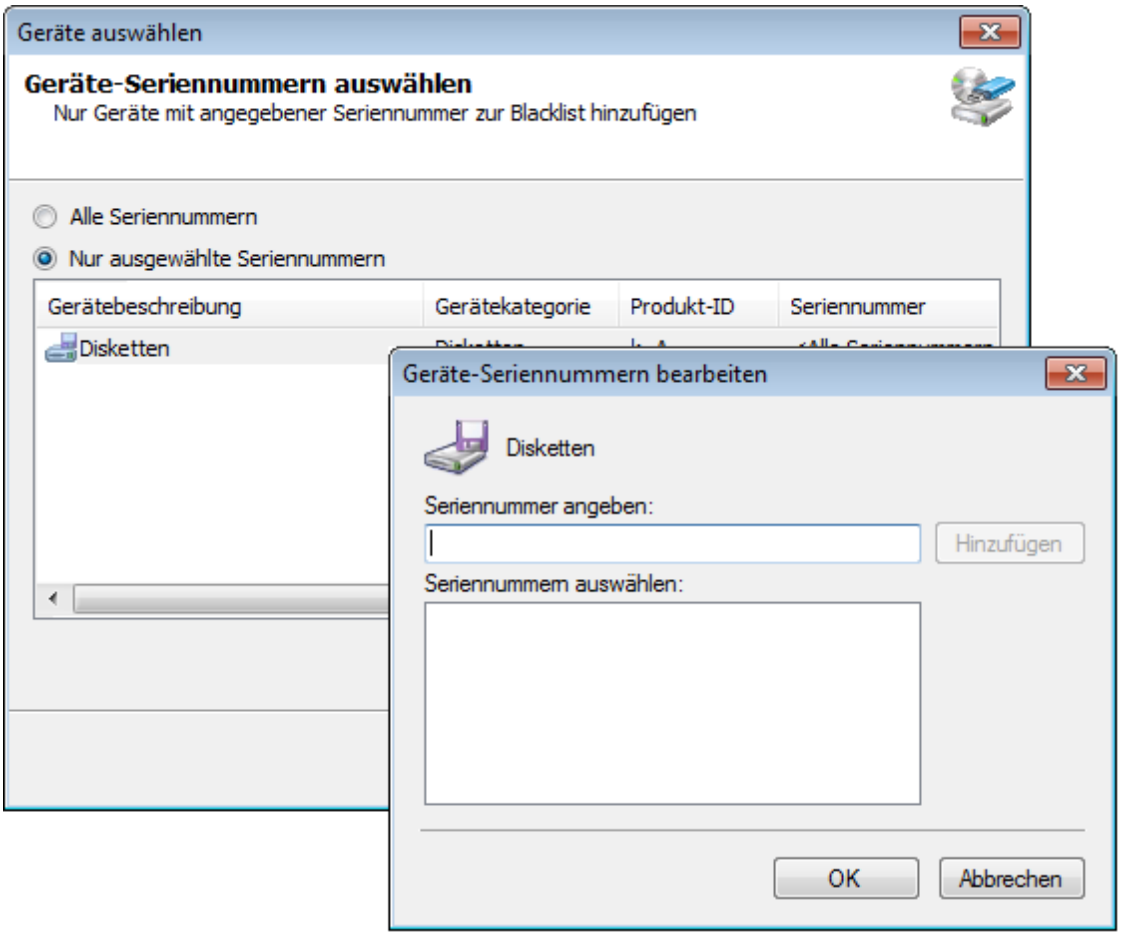


Screenshot 40: Optionen zur Geräteauswahl - Auswahl der Geräteseriennummer

6. Wählen Sie die gewünschte Option für die Seriennummern aus:

» **Alle Seriennummern** – Um alle Seriennummern eines Geräts der Whitelist hinzuzufügen. Klicken Sie auf **Fertig stellen** und **OK**.

» **Nur ausgewählte Seriennummern** – Um nur die Seriennummern bestimmter Geräte der Whitelist hinzuzufügen. Markieren Sie anschließend das Gerät, und klicken Sie auf **Bearbeiten…**, um eine Seriennummer der Whitelist hinzuzufügen. Klicken Sie auf **OK**, **Fertig stellen** und **OK**.



Screenshot 41: Optionen zur Geräteauswahl - Bearbeiten der Geräteseriennummern

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.11 Konfigurieren zeitlich begrenzter Zugriffsrechte

Mit GFI EndPointSecurity können Sie Benutzern zeitlich begrenzte Zugriffsrechte gewähren. Auf diese Weise können Sie für eine bestimmte Dauer oder in einem bestimmten Zeitfenster auf Geräte und Schnittstellen auf geschützten kontrollierten Computern zugreifen. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

Wenn ein zeitlich begrenzter Zugriff gewährt wird, werden alle Berechtigungen und Einstellungen (z. B. Dateitypfilter) dieser Schutzrichtlinie für diesen Computer temporär aufgehoben.

Weitere Informationen finden Sie unter Funktionsweise von GFI EndPointSecurity - Zeitlich begrenzter Zugriff (page 18).

» Beantragen des zeitlich begrenzten Zugriffs auf einen geschützten Computer

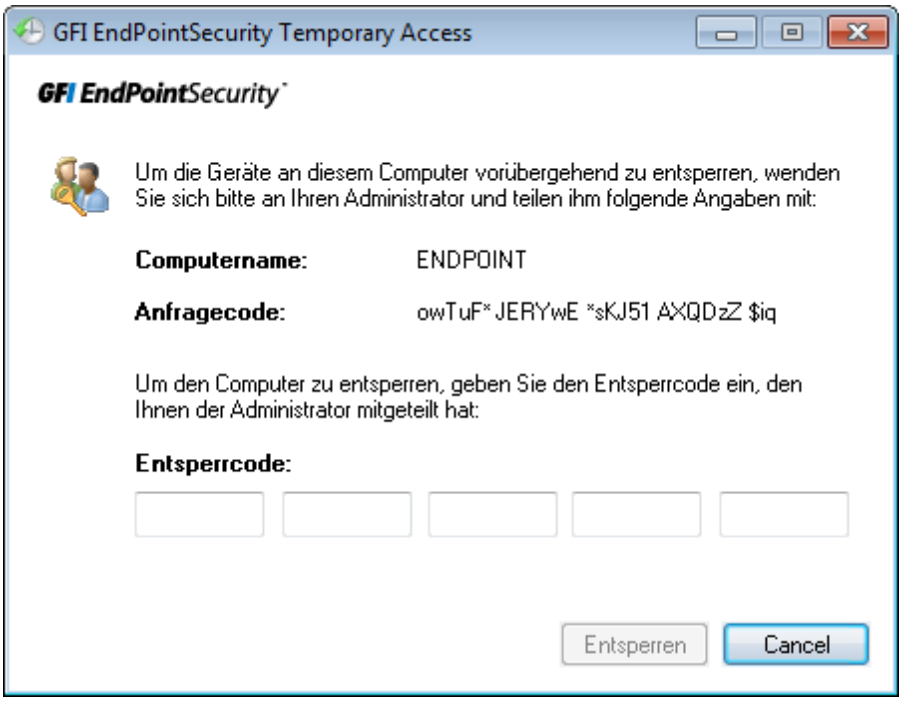
» Gewähren des zeitlich begrenzten Zugriffs auf einen geschützten Computer

5.11.1 Beantragen des zeitlich begrenzten Zugriffs auf einen geschützten Computer

So generieren Sie einen Anfragecode: Tool:

Screenshot 42: Symbol „Temporärer Zugriff auf Geräte“

1. Klicken Sie in der **Systemsteuerung** auf **Zeitlich begrenzter Gerätezugriff**.



Screenshot 43: GFI EndPointSecurityTemporary-Access-Tool

2. Notieren Sie den im Dialogfeld **GFI EndPointSecurity Zeitlich begrenzter Zugriff** generierten **Anfragecode**. Teilen Sie Ihrem Sicherheitsadministrator die folgenden Details mit:

- Anfragecode
- Gerät-/Schnittstellentyp
- Wann Sie Zugriff benötigen
- Für wie lange Sie Zugriff benötigen.

Lassen Sie GFI EndPointSecurity Temporary-Access-Tool geöffnet.

3. Nachdem Sie vom Administrator den Entsperrcode erhalten haben, geben Sie ihn in das Feld **Entsperrcode** ein.

> **Hinweis**
>
> Wird der Entsperrcode nicht innerhalb des festgelegten Zeitraums auf dem geschützten Computer eingegeben, ist kein Zugriff möglich.

4. Klicken Sie auf **Entsperren**, um den zeitlich begrenzten Zugriff zu aktivieren. Nun kann auf das gewünschte Geräte und/oder die Schnittstelle zugegriffen werden.

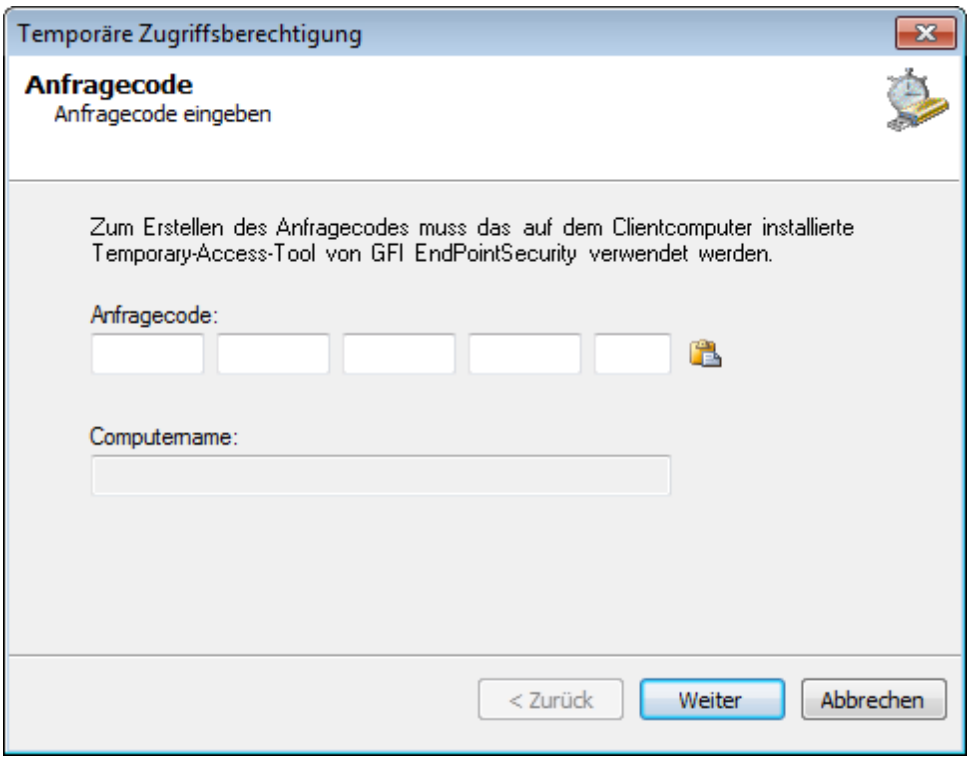
5.11.2 Gewähren des zeitlich begrenzten Zugriffs auf einen geschützten Computer

So gewähren Sie zeitlich begrenzten Zugriff:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Schutzrichtlinien**.

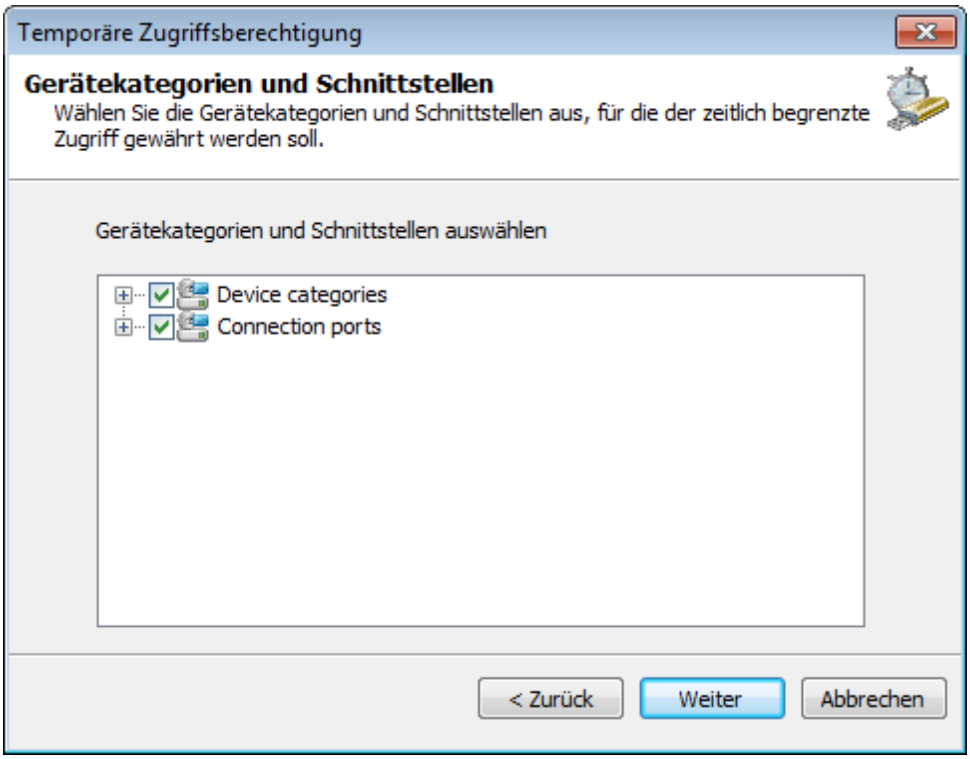
2. Wählen Sie im linken Bereich die Schutzrichtlinie aus, die den Computer kontrolliert, für den ein zeitlich begrenzter Zugriff gewährt werden soll.

3. Klicken Sie im rechten Bereich im Abschnitt **Zeitlich begrenzte Zugriffsberechtigung** auf **Zeitlich begrenzter Zugriff**.



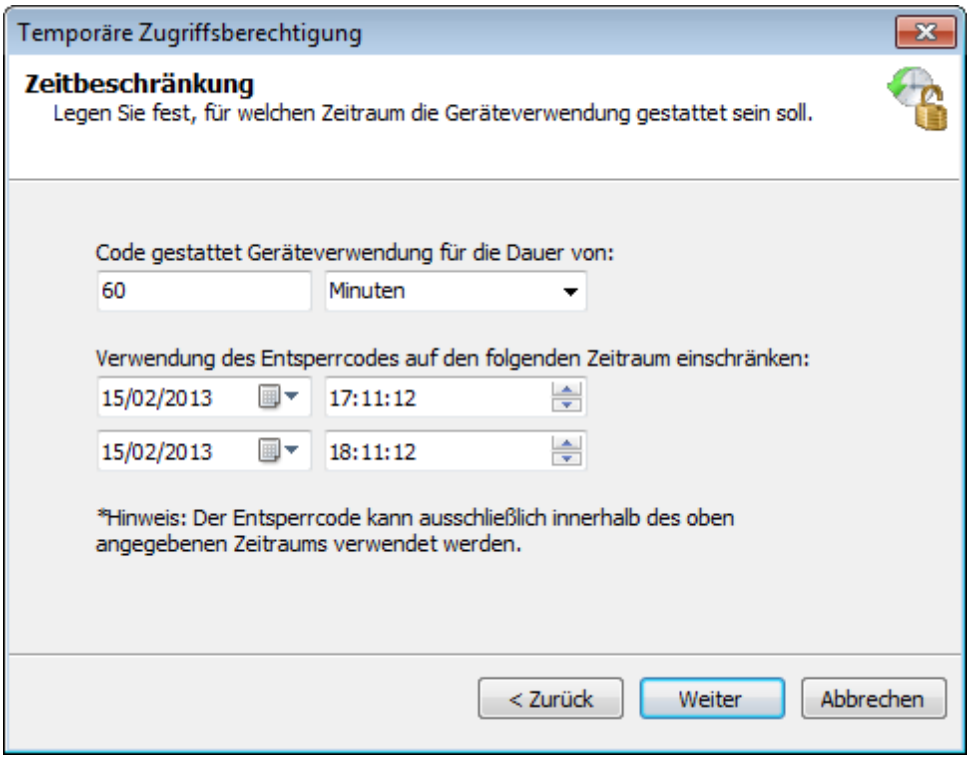
Screenshot 44: Optionen zur Gewährung des zeitlich begrenzten Zugriffs - Anfragecode

4. Geben Sie im Dialogfeld **Zeitlich begrenzte Zugriffsberechtigung** den vom Benutzer erhaltenen Anfragecode im Feld **Anfragecode** ein. Der Name des Computers, auf dem der Anfragecode generiert wurde, wird im Feld **Computername** angezeigt. Klicken Sie auf **Weiter**.



Screenshot 45: Optionen zur Gewährung des zeitlich begrenzten Zugriffs - Gerätekategorien und Schnittstellen

5. Aktivieren Sie die erforderlichen Gerätekategorien und/oder Schnittstellen, auf die Zugriff gewährt werden soll, in der Liste. Klicken Sie anschließend auf **Weiter**.



Screenshot 46: Optionen zur Gewährung des zeitlich begrenzten Zugriffs - Zeitbeschränkung

6. Geben Sie die Dauer des erlaubten Zugriffs und den Zeitraum an, in dem der Entsperrcode eingegeben werden muss. Klicken Sie anschließend auf **Weiter**.

7. Notieren Sie den generierten **Entsperrcode**. Teilen Sie den Code dem Benutzer mit, der den zeitlich begrenzten Zugriff angefragt hat. Klicken Sie anschließend auf **Fertig stellen**.

5.12 Konfigurieren der Dateitypfilter

GFI EndPointSecurity gibt Ihnen die Möglichkeit, Einschränkungen für Dateitypen zu definieren, beispielsweise für Dateien der Formate .doc oder .xls, um zu verhindern, dass diese auf oder von erlaubten Geräten kopiert werden. Diese Einschränkungen können Active Directory (AD)-Benutzern und/oder -Benutzergruppen zugewiesen werden. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

Die Filterung basiert auf der Überprüfung von Dateierweiterungen und Echtzeitüberprüfungen des wahren Dateityps. Die Echtzeitüberprüfung erfolgt für folgende Dateitypen:

AVI	BMP	CAB	CHM	DLL	DOC	EMF	EXE	GIF	HLP
HTM	JPE	JPEG	JPG	LNK	M4A	MDB	MP3	MPEG	MPG
MSG	MSI	OCX	P7M	PDF	PPT	RAR	RTF	SCR	SYS
TIF	TIFF	TXT	URL	WAV	XLS	ZIP	DOCX	XLSX	PPTX

HINWEIS 1

Nicht aufgelistete Dateitypen werden nur basierend auf der Dateierweiterung gefiltert.

HINWEIS 2

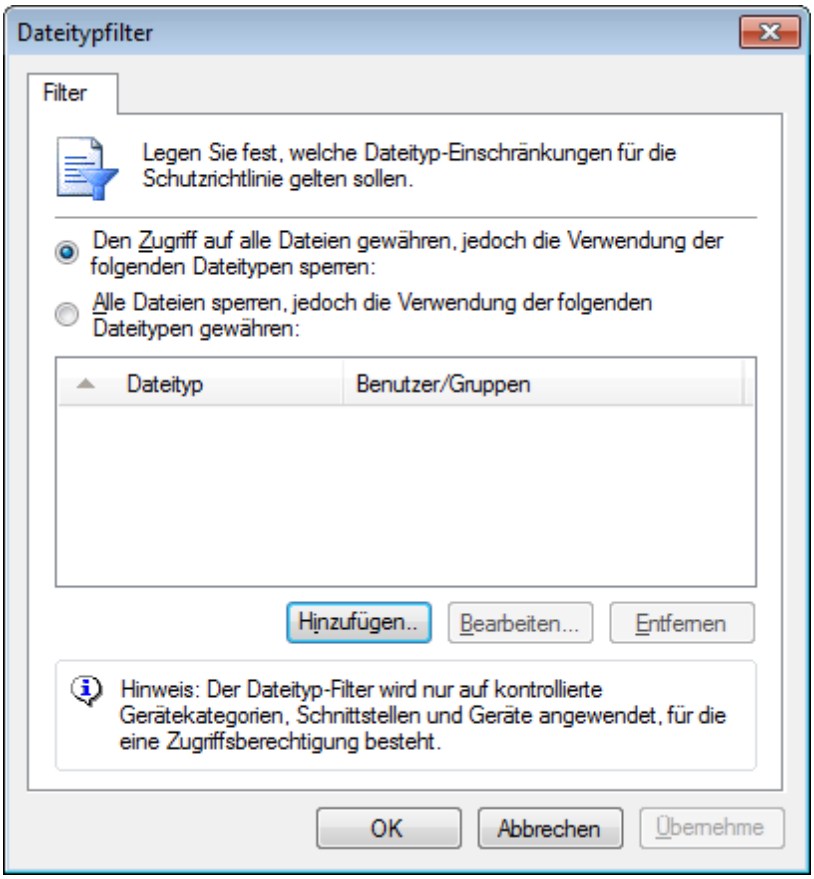
Die Dateityp-Filterung erfolgt nur für Gerätekategorien und/oder Schnittstellen, auf die zugegriffen werden kann.

So konfigurieren Sie Dateitypeinschränkungen für Benutzer innerhalb einer Schutzrichtlinie:

1. Klicken Sie in der Verwaltungskonsole von GFI EndPointSecurity auf die Registerkarte **Konfiguration** >**Schutzrichtlinien**.

2. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die Sie Dateitypeinschränkungen definieren möchten.

3. Klicken Sie im rechten Bereich im Abschnitt **Dateiüberwachung** auf **Dateitypfilter**.

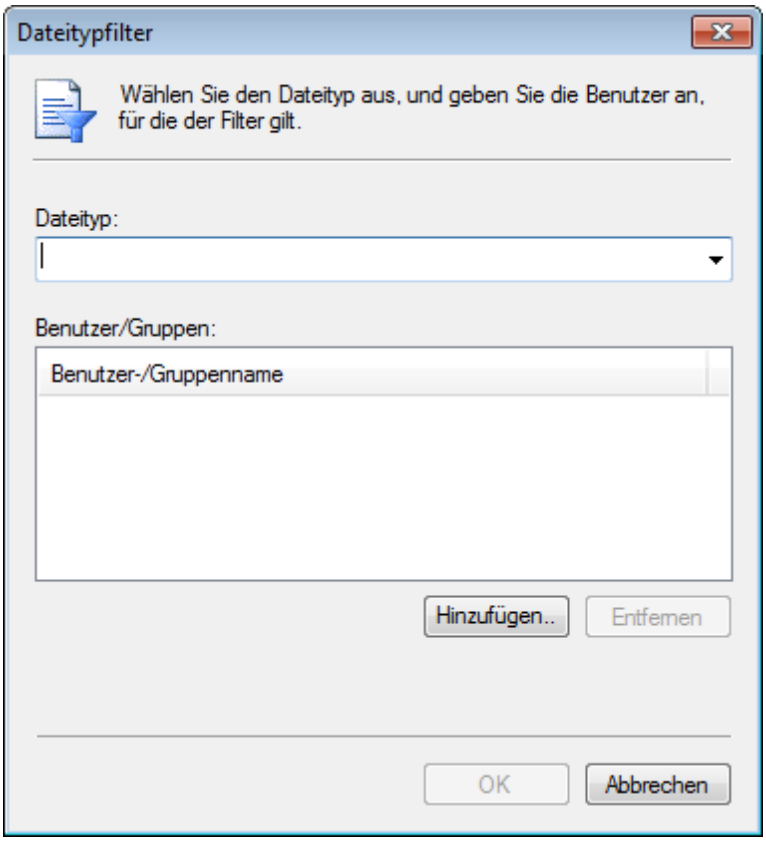


Screenshot 47: Optionen für Dateitypfilter

4. Wählen Sie im Dialogfeld „Dateitypfilter“ die auf diese Schutzrichtlinie anzuwendende Einschränkung aus:

» Den Zugriff auf alle Dateien gewähren, jedoch die Verwendung der folgenden Dateitypen sperren

» Alle Dateien sperren, jedoch die Verwendung der folgenden Dateitypen gewähren



Screenshot 48: Optionen für Dateitypfilter und Benutzer

5. Klicken Sie auf **Hinzufügen…**, und wählen Sie den Dateityp aus dem Dropdown-Menü **Dateityp** aus, oder geben Sie ihn ein.

6. Klicken Sie auf **Hinzufügen...**, um die Benutzer/Gruppen festzulegen, die auf diesen Dateityp zugreifen können oder dafür gesperrt sind. Klicken Sie anschließend auf **OK**. Wiederholen Sie die vorherigen zwei Unterschritte für jeden zu beschränkenden Dateityp.

7. Klicken Sie zweimal auf **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Computer**.

2. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**

5.13 Konfigurieren der Inhaltsprüfung

Mit GFI EndPointSecurity können Sie Dateiinhaltsbeschränkungen für eine bestimmte Schutzrichtlinie angeben. Die Inhaltsprüfung prüft Dateien, die den Endpunkt über Wechseldatenträger passieren und identifiziert Inhalt basierend auf vorkonfigurierten und benutzerdefinierten regulären Ausdrücken und Wörterbuchdateien. Das Modul sucht standardmäßig nach geschützten, vertraulichen Informationen wie Sozialversicherungsnummern und primären Kontonummern, Informationen zu Unternehmen, Namen von Erkrankungen, Drogen, gefährlichen Chemikalien sowie alltäglicher Sprache und ethnischen/rassistischen Begriffen.

» Sie können die Inhaltsprüfung als eine globale Richtlinie ähnlich dem Dateiüberprüfungsmodul konfigurieren.

5.13.1 Verwalten von Inhaltsprüfungsoptionen

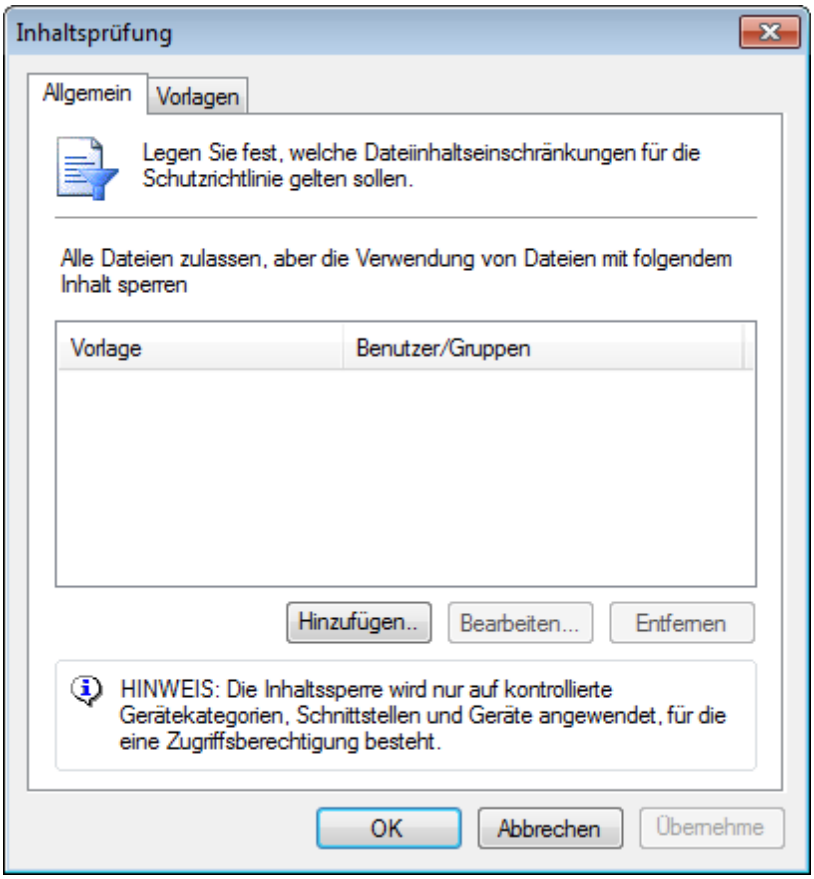
So konfigurieren Sie Inhaltsprüfungsoptionen für Benutzer

in einer bestimmten Schutzrichtlinie:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration > Schutzrichtlinien**.

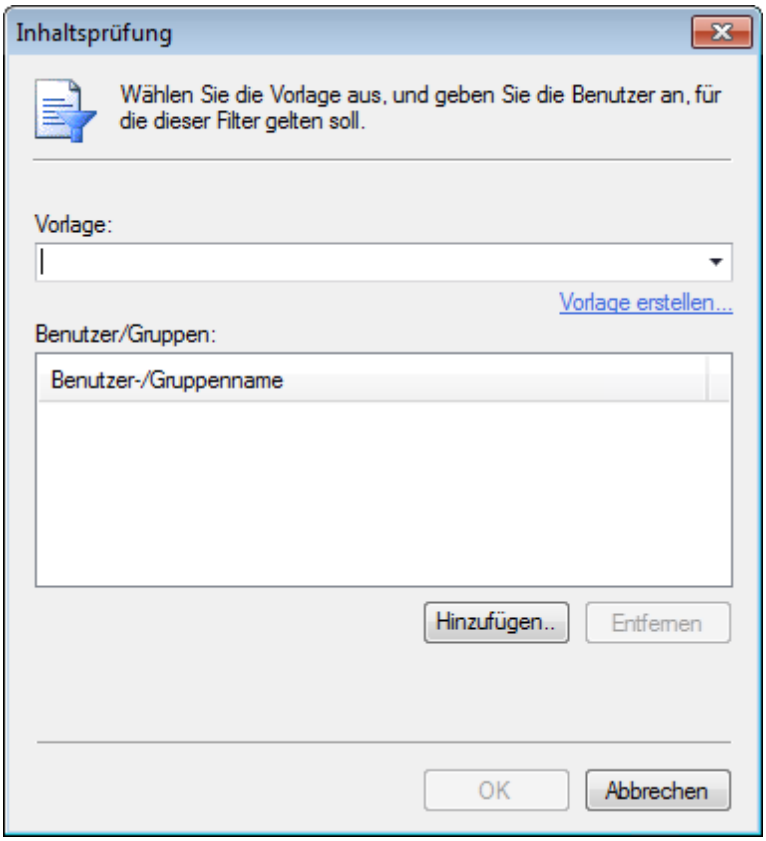
2. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die Inhaltsbeschränkungen angegeben werden sollen.

3. Klicken Sie im rechten Bereich im Abschnitt **Dateiüberwachung** auf **Inhaltsprüfung**.



Screenshot 49: Inhaltsprüfungsoptionen

4. Klicken Sie im Dialogfeld „Inhaltsprüfung“ auf **Hinzufügen**, um die Vorlage für diese Richtlinie auszuwählen:

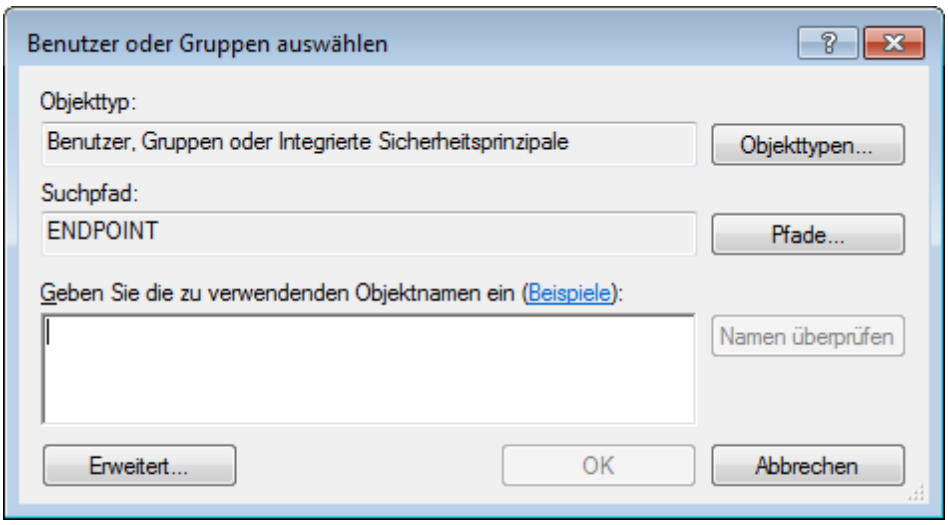


Screenshot 50: Hinzufügen einer neuen Vorlage

5. Klicken Sie auf **Hinzufügen…**, und wählen Sie eine Vorlage aus dem Dropdown-Menü **Vorlage** aus oder geben Sie sie ein.

6. Klicken Sie auf **Hinzufügen…**, um die Benutzer/Gruppe(n) anzugeben. Klicken Sie anschließend auf **OK**. Wiederholen Sie die vorherigen beiden Schritte für jede Vorlage, die angewendet werden soll.

7. Klicken Sie auf **OK**.



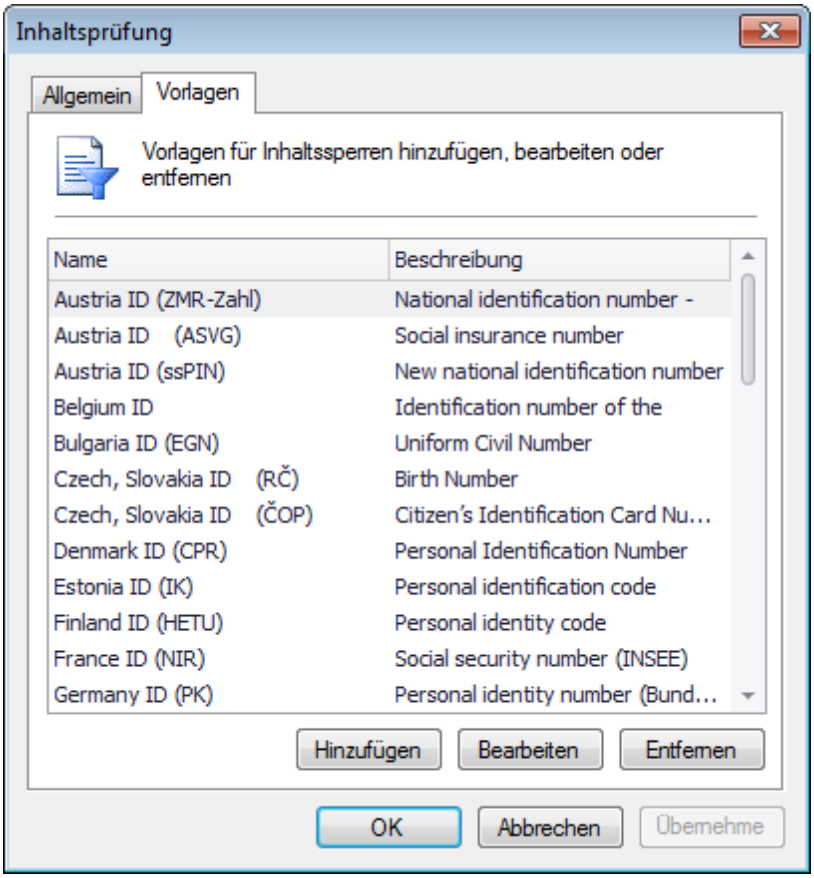
Screenshot 51: Auswählen von Benutzern oder Gruppen

5.13.2 Verwalten von Vorlagenoptionen

So fügen Sie vordefinierte Vorlagen hinzu oder entfernen sie:

1. Klicken Sie auf **Vorlagen**, und wählen Sie eine Vorlage aus der Liste **Vorlage** aus.

2. Klicken Sie auf **Hinzufügen**, **Bearbeiten** oder **Entfernen**, um Vorlagen zu ändern oder zu löschen.



Screenshot 52: Verwaltung von Vorlagen

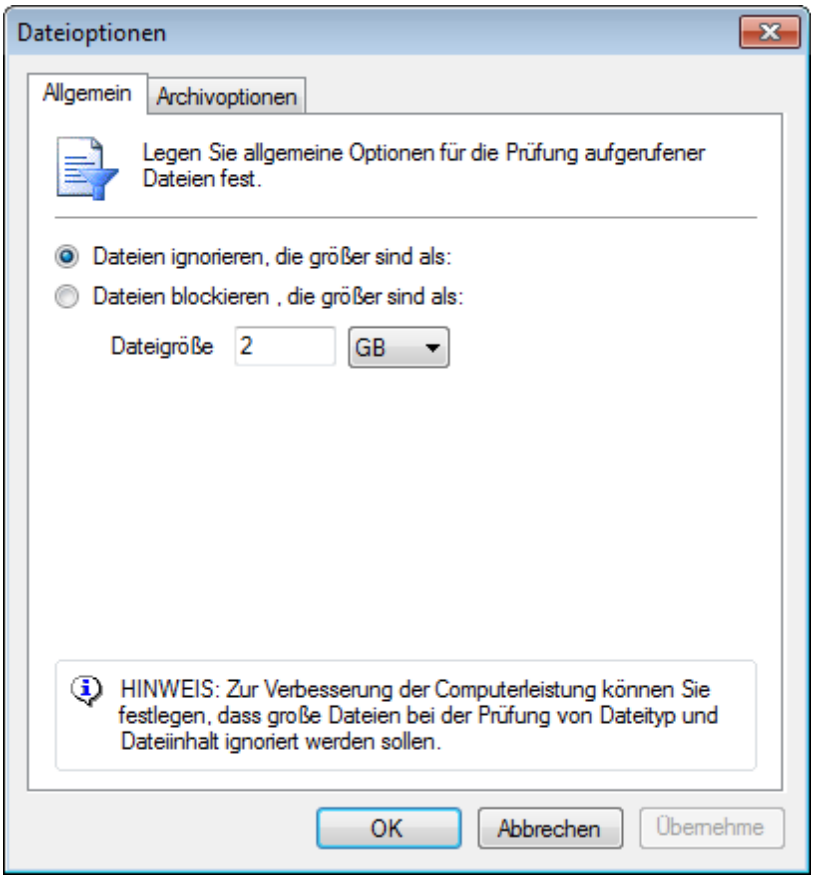
5.14 Konfigurieren von Dateioptionen

Mit GFI EndPointSecurity können Sie Optionen angeben, die zum Blockieren oder Zulassen von Dateien basierend auf deren Größe erforderlich sind. Außerdem ermöglicht GFI EndPointSecurity das Ignorieren von großen Dateien, wenn der Dateityp, der Inhalt oder archivierte Dateien überprüft werden.

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration > Schutzrichtlinien**.

2. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die Sie Dateibeschränkungen einrichten möchten.

3. Klicken Sie im rechten Bereich im Abschnitt **Dateiüberwachung** auf **Dateioptionen**.

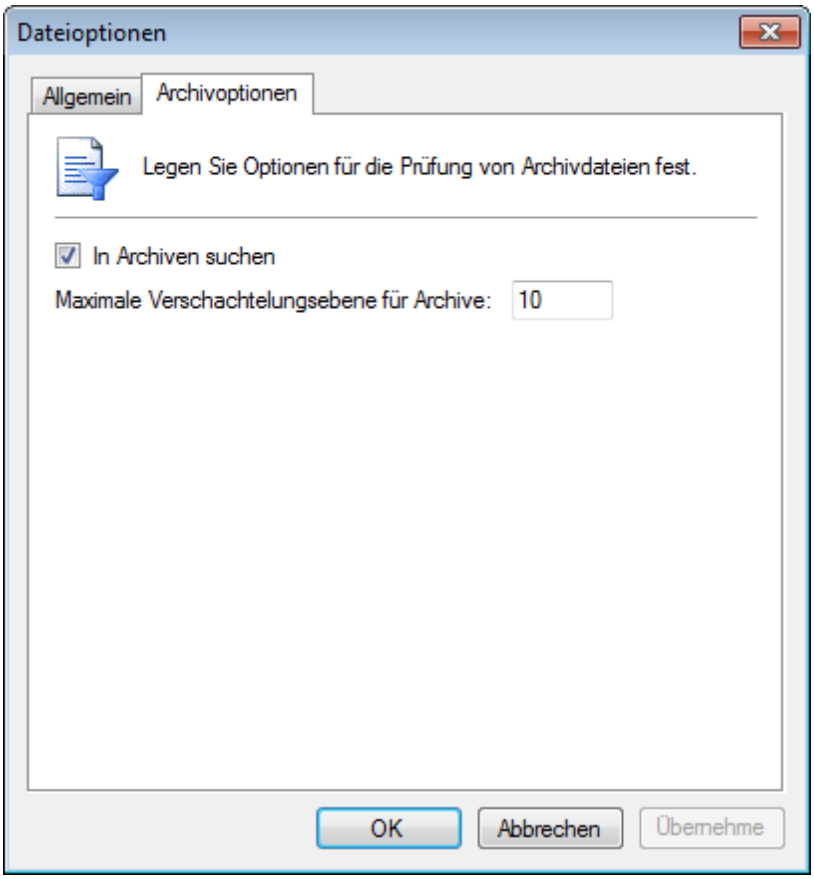


Screenshot 53: Dateioptionen

4. Wählen Sie im Dialogfeld „Dateioptionen“ unter folgenden Optionen aus:

Tabelle 9: Dateioptionen - Benutzeroptionen

Option	Beschreibung
Dateien ignorieren, die größer sind als:	Bei der Überprüfung aufgerufener Dateien werden Dateien ignoriert, die größer als angegeben sind.
Dateien blockieren, die größer sind als:	Bei der Überprüfung aufgerufener Dateien werden Dateien blockiert, die größer als angegeben sind.



Screenshot 54: Optionen für Dateitypfilter und Benutzer

5. Aktivieren/deaktivieren Sie auf der Registerkarte **Archivoptionen** die Option **In Archiven suchen**, und geben Sie die Verschachtelungsebene für das Archiv an, die bei der Überprüfung von Archivdateien angewendet werden soll.

6. Klicken Sie auf **OK**.

5.15 Konfigurieren der Sicherheitsverschlüsselung

GFI EndPointSecurity ermöglicht Ihnen die Konfiguration von Einstellungen speziell für verschlüsselte Geräte. Sie können auch Geräte verschlüsseln, die bisher noch nicht gesichert sind.

» Konfigurieren von Microsoft BitLocker To Go-Geräten

» Konfigurieren der Laufwerksverschlüsselung

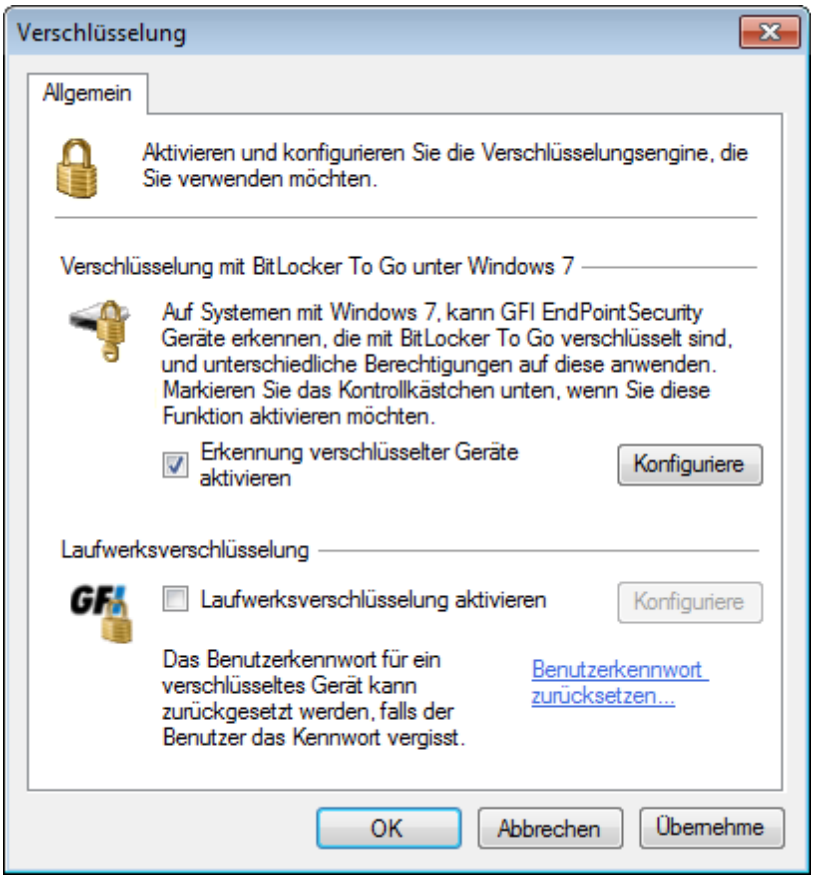
5.15.1 Konfigurieren von Microsoft BitLocker To Go-Geräten

GFI EndPointSecurity kann mit Microsoft BitLocker To Go verschlüsselte Speichergeräte erkennen. Dadurch können Sie verschiedene Berechtigungen für solche Geräte konfigurieren. So aktivieren Sie die Microsoft BitLocker To Go-Erkennung:

1. Klicken Sie in der Verwaltungskonsole von GFI EndPointSecurity auf die Registerkarte **Konfiguration** >**Schutzrichtlinien**.

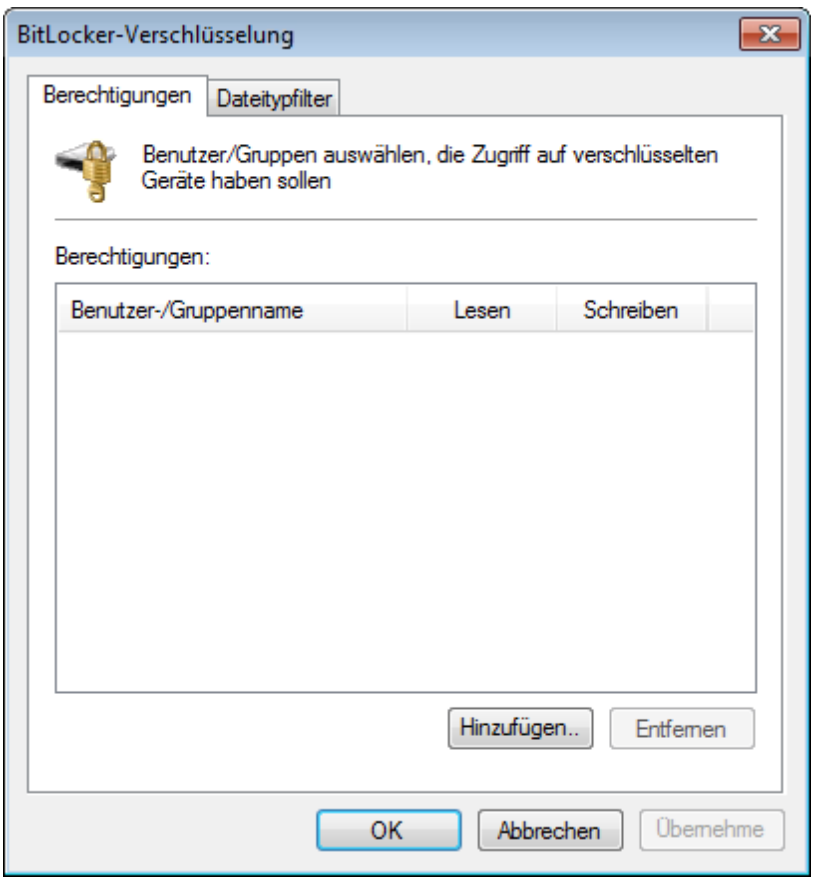
2. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die die Verschlüsselungsrichtlinie gelten soll.

3. Klicken Sie im rechten Bereich im Abschnitt **Sicherheit** auf **Verschlüsselung**.



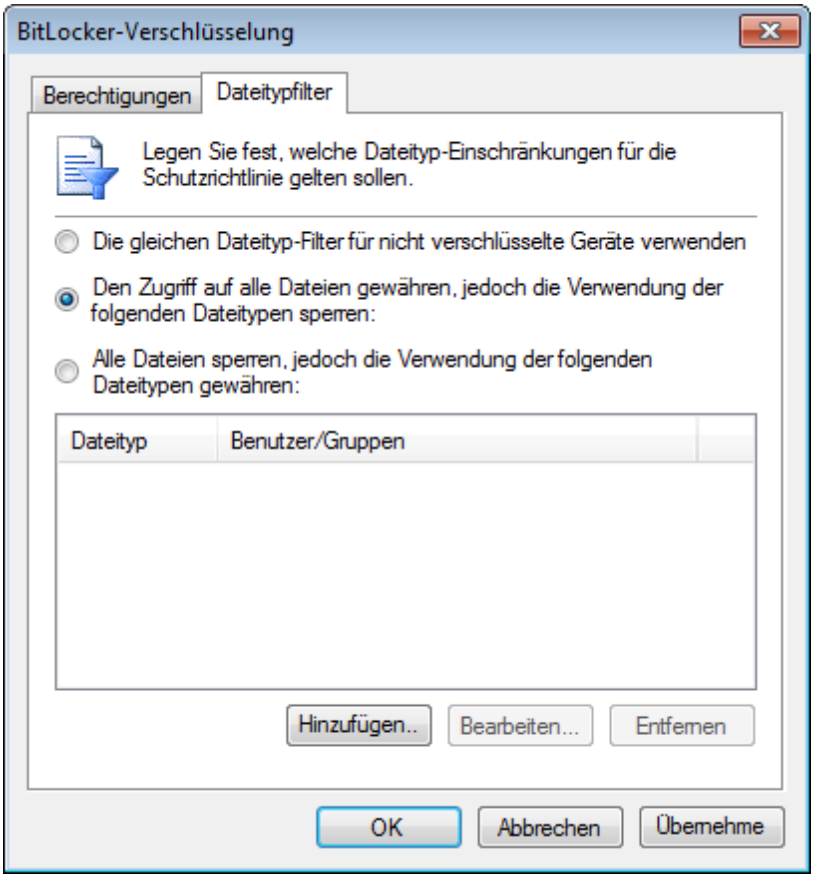
Screenshot 55: Verschlüsselungsoptionen - Registerkarte „Allgemein“

4. Wählen Sie **Erkennung verschlüsselter Geräte aktivieren**, und klicken Sie auf **Konfigurieren**.



Screenshot 56: Verschlüsselungsoptionen - Registerkarte „Berechtigungen“

5. Klicken Sie auf **Hinzufügen...**, um die Benutzer und Gruppen mit Zugriff auf verschlüsselte Geräte anzugeben.



Screenshot 57: Verschlüsselungsoptionen - Registerkarte „Dateitypfilter“

6. Wählen Sie die Registerkarte **Dateitypfilter**, um die einzuschränkenden Dateitypen zu konfigurieren.

7. Wählen Sie die auf diese Schutzrichtlinie anzuwendende Einschränkung aus:

» Die gleichen Dateityp-Filter für nicht verschlüsselte Geräte verwenden

» Den Zugriff auf alle Dateien gewähren, jedoch die Verwendung der folgenden Dateitypen sperren

» Alle Dateien sperren, jedoch die Verwendung der folgenden Dateitypen gewähren

8. Verwenden Sie die Schaltflächen **Hinzufügen, Bearbeiten** und **Entfernen**, um die Dateitypen zu verwalten.

9. Klicken Sie auf **OK**.

5.15.2 Konfigurieren der Laufwerksverschlüsselung

Mithilfe der Laufwerksverschlüsselung können Sie die Inhalte von USB-Geräten mit AES 256 verschlüsseln. Wenn die Laufwerksverschlüsselung erzwungen wird, müssen Benutzer ein Kennwort angeben, um Daten auf Speichergeräten zu verschlüsseln oder darauf zuzugreifen. So erzwingen Sie die Laufwerksverschlüsselung auf installierten Agenten:

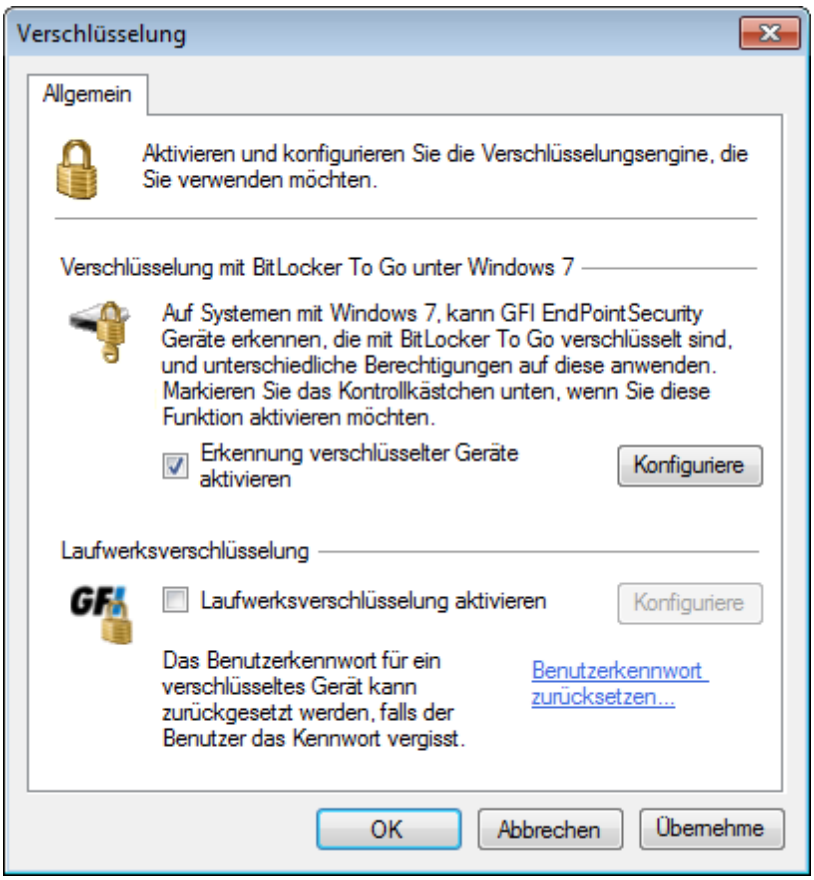
Hinweis

Verschlüsselung bei Bedarf ist möglich, selbst wenn sie nicht direkt vom Administrator angeordnet wurde. Der Benutzer kann dazu im Shell-Kontextmenü eines Wechseldatenträgers auf den Eintrag **Verschlüsseln...** klicken.

1. Klicken Sie in der Verwaltungskonsole von GFI EndPointSecurity auf die Registerkarte **Konfiguration** >**Schutzrichtlinien**.

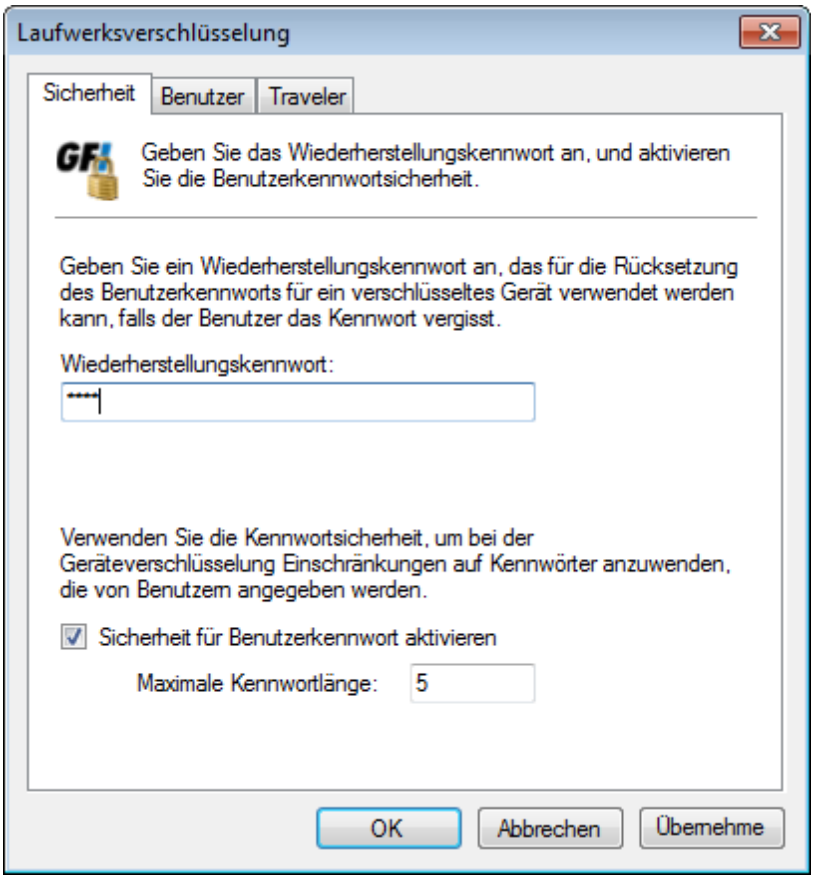
2. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die die Verschlüsselungsrichtlinie gelten soll.

3. Klicken Sie im rechten Bereich im Abschnitt **Sicherheit** auf **Verschlüsselung**.



Screenshot 58: Verschlüsselungsoptionen - Registerkarte „Allgemein“

4. Wählen Sie **Laufwerksverschlüsselung aktivieren**. Klicken Sie auf **Konfigurieren**. Klicken Sie auf **Benutzerkennwort zurücksetzen**, um das Verschlüsselungskennwort für einen bestimmten Benutzer zurückzusetzen.

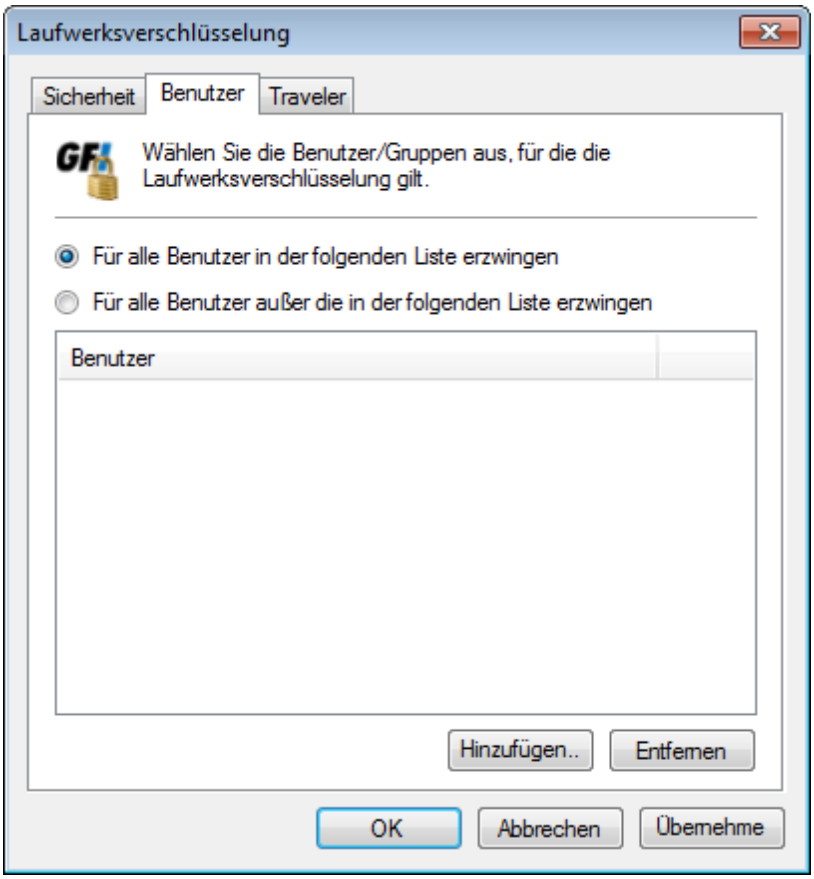


Screenshot 59: Verschlüsselungsoptionen - Registerkarte „Sicherheit“

5. Konfigurieren Sie auf der Registerkarte **Sicherheit** die unten beschriebenen Funktionen:

Tabelle 10: Laufwerksverschlüsselung - Sicherheitsoptionen

Option	Beschreibung
Wiederherstellungskennwort	Geben Sie ein Kennwort ein für den Fall, dass Benutzer ihr Kennwort vergessen oder verlieren.
Sicherheit für Benutzerkennwort aktivieren	Erzwingen Sie Einschränkungen für die von Benutzern eingegebenen Kennwörter. Geben Sie unter **Mindestkennwortlänge** die minimale Länge an, damit ein Kennwort akzeptiert wird.

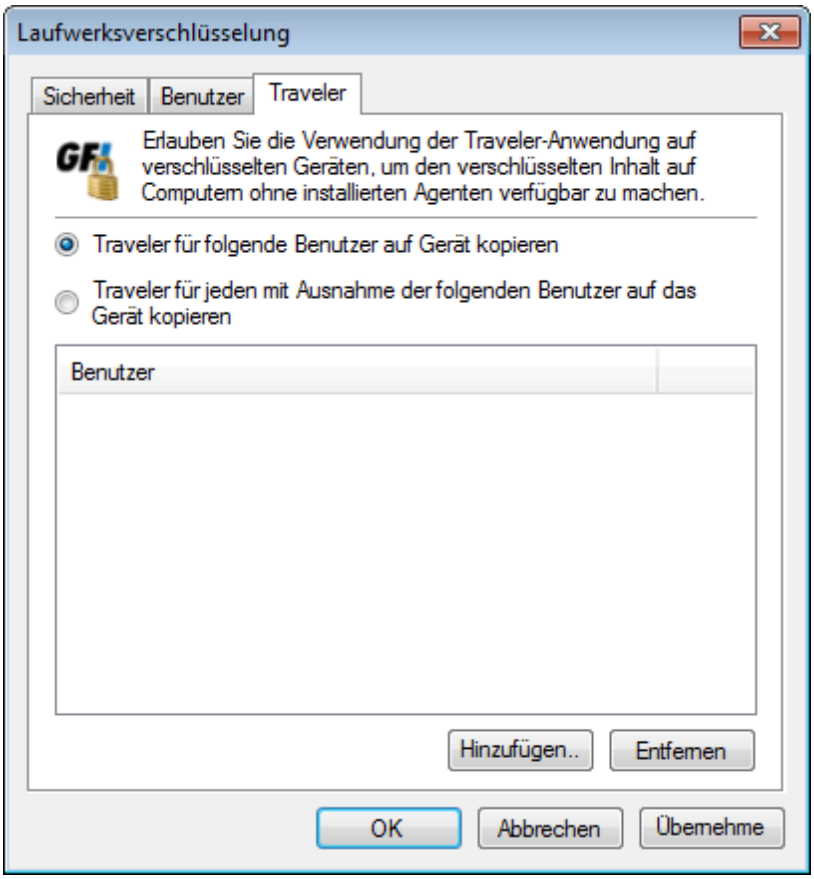


Screenshot 60: Verschlüsselungsoptionen - Registerkarte „Benutzer“

6. Wählen Sie die Registerkarte **Benutzer**, und konfigurieren Sie die folgenden Optionen:

Tabelle 11: Laufwerksverschlüsselung - Benutzeroptionen

Option	Beschreibung
Für alle Benutzer in der folgenden Liste erzwingen	Wählen Sie die Benutzer aus, für die die Laufwerksverschlüsselung auf portablen Geräten erzwungen wird. Verwalten Sie mithilfe der Schaltfläche **Hinzufügen** und **Entfernen** die ausgewählten Benutzer.
Für alle Benutzer außer die in der folgenden Liste erzwingen	Wählen Sie die Benutzer aus, die von der Laufwerksverschlüsselung ausgeschlossen werden. Verwalten Sie mithilfe der Schaltfläche Hinzufügen und Entfernen die ausgewählten Benutzer.



Screenshot 61: Verschlüsselungsoptionen - Registerkarte „Traveler“

Hinweis

Traveler ist eine Anwendung, die mithilfe von GFI EndPointSecurity automatisch auf Speichergeräten installiert werden kann. Mit dieser Anwendung können Sie die von GFI EndPointSecurity verschlüsselten Daten auf Speichergeräten entschlüsseln, auf denen kein GFI EndPointSecurity-Agent ausgeführt wird.

7. Wählen Sie die Registerkarte **Traveler**, und konfigurieren Sie die folgenden Optionen:

Tabelle 12: Laufwerksverschlüsselung - Traveler-Optionen

Option	Beschreibung
Traveler für folgende Benutzer auf Gerät kopieren	Wählen Sie die Benutzer aus, für die Traveler auf ihren Computern installiert wird. Verwalten Sie mithilfe der Schaltfläche **Hinzufügen** und **Entfernen** die ausgewählten Benutzer.
Traveler für alle außer die folgenden Benutzer auf Gerät kopieren	Wählen Sie die Benutzer aus, für die Traveler nicht installiert wird. Verwalten Sie mithilfe der Schaltfläche **Hinzufügen** und **Entfernen** die ausgewählten Benutzer.

8. Klicken Sie auf **Übernehmen** und **OK**.

5.16 Konfigurieren der Ereignisprotokollierung

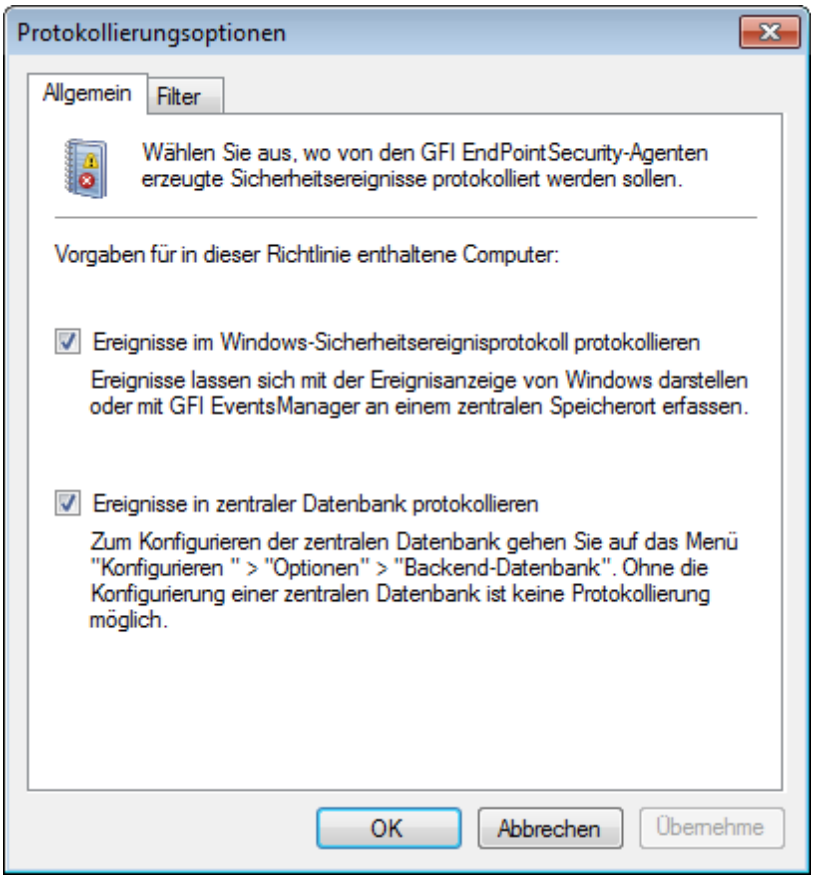
GFI EndPointSecurity-Agenten erfassen auf kontrollierten Computern alle Ereignisse zu Zugriffsversuchen auf Geräte und Schnittstellen. Sie erfassen außerdem dienstspezifische Ereignisse. Sie können festlegen, wo diese Ereignisse gespeichert werden und auch, welche Ereignisarten protokolliert werden. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

So legen Sie Protokollierungsoptionen für Benutzer innerhalb einer Schutzrichtlinie fest:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie im rechten Bereich im Abschnitt **Protokollierung und Warnungen** auf **Protokolloptionen festlegen**.



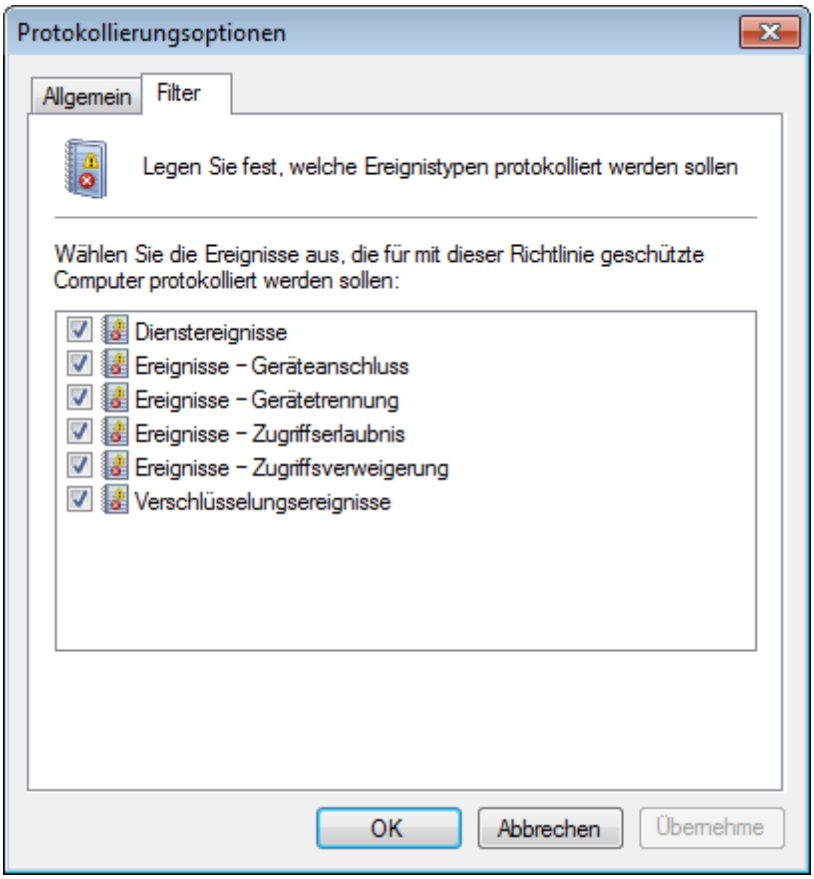
Screenshot 62: Protokollierungsoptionen - Registerkarte „Allgemein“

4. Klicken Sie im Dialogfeld **Protokollierungsoptionen** auf die Registerkarte **Allgemein**.

5. Aktivieren bzw. deaktivieren Sie die Speicherorte, an denen von dieser Schutzrichtlinie generierte Ereignisse gespeichert werden sollen.

Option	Beschreibung
Ereignisse im Windows-Sicherheitsereignisprotokoll protokollieren	Sie können Ereignisse in der Windows-Ereignisanzeige jedes kontrollierten Computers oder über GFI EventsManager anzeigen, nachdem sie an einem zentralen Speicherort gesammelt wurden.
Ereignisse in zentraler Datenbank protokollieren	Sie können Ereignisse auf der Unterregisterkarte **Protokoll-Browser** in der Verwaltungskonsole von GFI EndPointSecurity anzeigen. Diese Option erfordert die Konfiguration einer zentralen Datenbank. Weitere Informationen finden Sie unter Verwalten des Datenbank-Backends (page 117).

Falls beide Optionen aktiviert sind, werden die gleichen Daten an beiden Speicherorten protokolliert.



Screenshot 63: Protokollierungsoptionen - Registerkarte „Filter“

6. Wählen Sie auf der Registerkarte **Filter** die Ereignistypen aus, die durch diese Schutzrichtlinie protokolliert werden sollen. Klicken Sie auf **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.17 Konfigurieren der Warnungen

GFI EndPointSecurity kann so konfiguriert werden, dass bei bestimmten Ereignissen Warnungen an festgelegte Empfänger gesendet werden. Sie können die Warnungen über verschiedene Warnoptionen konfigurieren und auch die Ereignisarten festlegen, für die Warnungen gesendet werden. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

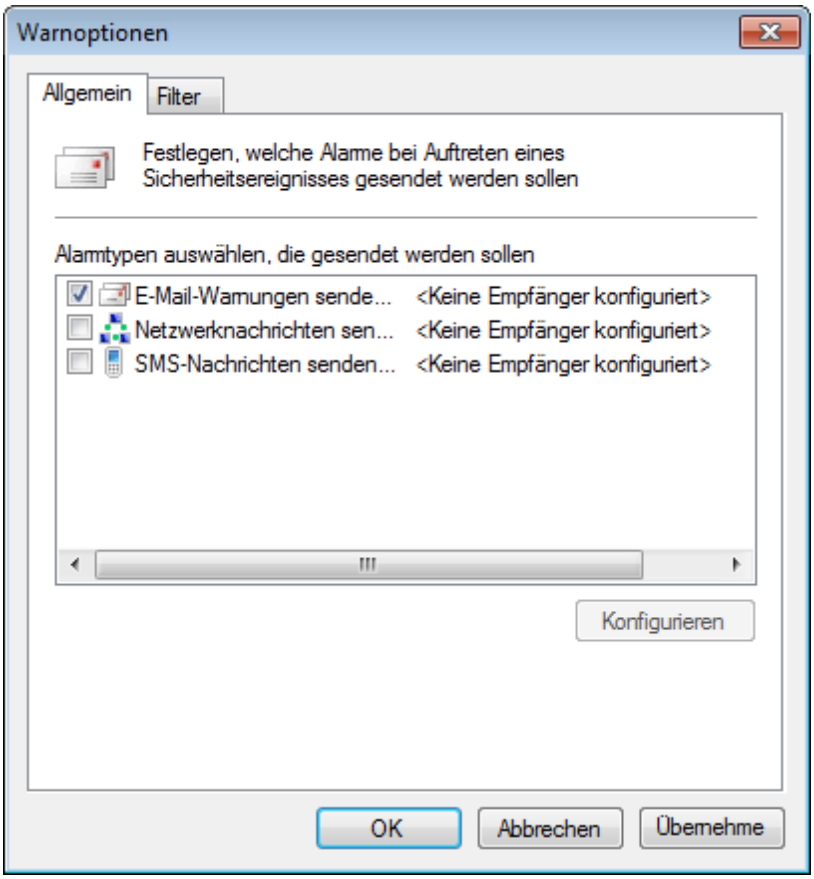
Warnungsempfänger sind weder Active Directory (AD)-Benutzer und/oder Benutzergruppen. Sie stellen von GFI EndPointSecurity erstellte Profilkonten dar, die die Kontaktdaten der Benutzer enthalten, die Warnmeldungen erhalten sollen. Warnungsempfänger sollten vor der Warnmeldungskonfiguration erstellt werden. Weitere Informationen finden Sie unter Konfigurieren der Warnungsempfänger (page 127).

So legen Sie Warnoptionen für Benutzer innerhalb einer Schutzrichtlinie fest:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie im rechten Bereich im Abschnitt **Protokollierung und Warnungen** auf **Warnoptionen**.



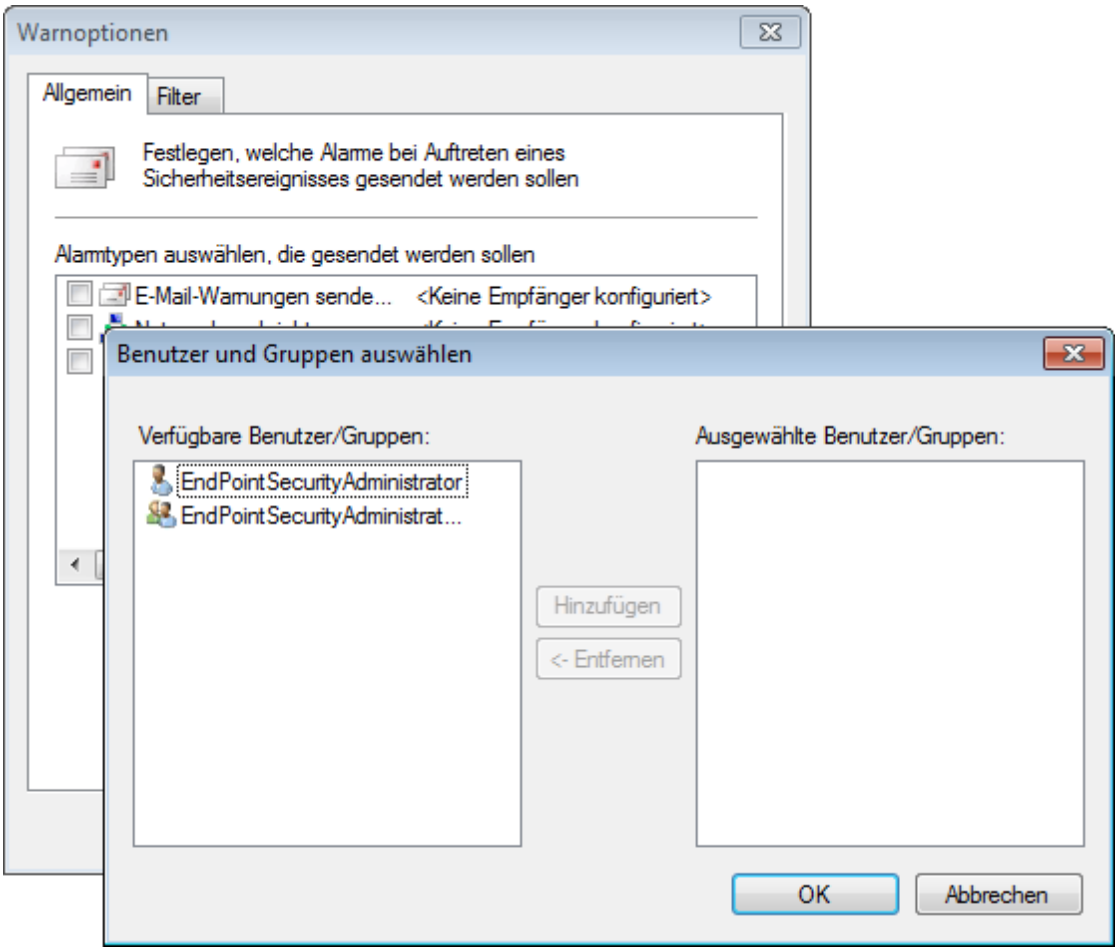
Screenshot 64: Warnoptionen - Registerkarte „Allgemein“

4. Klicken Sie im Dialogfeld **Warnoptionen** auf die Registerkarte **Allgemein**, und wählen Sie die zu sendenden Warnungstypen aus:

» E-Mail-Warnungen,

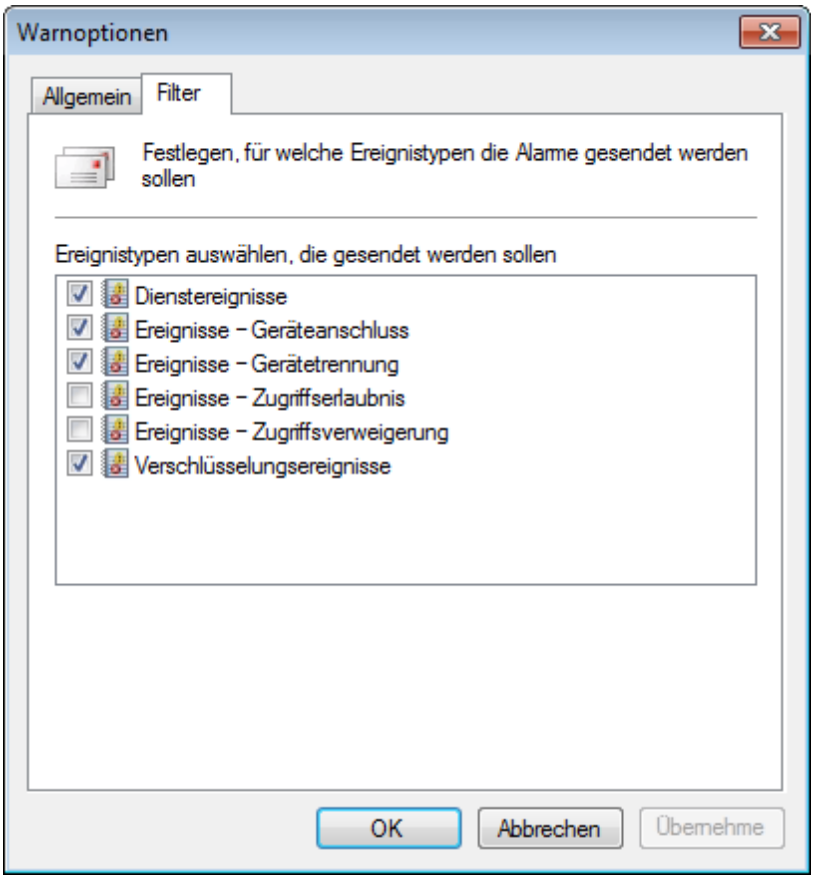
» Netzwerknachrichten,

» SMS-Nachrichten.



Screenshot 65: Warnoptionen - Konfigurieren von Benutzern und Gruppen

5. Markieren Sie eine aktivierte Warnmeldung, und klicken Sie auf **Konfigurieren**, um Warnungsempfänger anzugeben. Klicken Sie auf **OK**.



Screenshot 66: Warnoptionen - Registerkarte „Filter“

6. Wählen Sie auf der Registerkarte **Filter** aus den folgenden Ereignistypen aus, für die Warnungen durch diese Schutzrichtlinie gesendet werden sollen. Klicken Sie auf **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den in der Schutzrichtlinie angegebenen kontrollierten Computern bereit:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Computer**.

2. Klicken Sie unter **Allgemeine Aufgaben** auf **Auf allen Computern bereitstellen...**.

5.18 Festlegen einer Standardrichtlinie

GFI EndPointSecurity gibt Ihnen die Möglichkeit, eine Schutzrichtlinie zu erstellen, die durch die Bereitstellungsfunktion neu erkannten Computern zugewiesen wird. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

Standardmäßig ist die Bereitstellungsfunktion für Agenten so konfiguriert, dass sie die Schutzrichtlinie **Allgemeine Kontrolle** verwendet. Sie können jedoch auch eine andere Richtlinie als Standard festlegen.

So legen Sie eine andere Schutzrichtlinie als Standard fest:

1. Klicken Sie auf die Registerkarte **Konfiguration** > **Schutzrichtlinien**.

2. Wählen Sie unter **Schutzrichtlinien > Sicherheit** die zu konfigurierende Schutzrichtlinie aus.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf **Als Standardrichtlinie festlegen**.

6 Erkennen von Geräten

GFI EndPointSecurity gibt Ihnen die Möglichkeit, Endpunkte im Unternehmensnetzwerk schnell und transparent abzufragen und alle Geräte, die an den gescannten kontrollierten Computern angeschlossen sind oder waren, zu melden. Diese werden anschließend mit detaillierten Informationen angezeigt.

Verwenden Sie die Registerkarte **Scannen**, um kontrollierte Computer zu scannen und angeschlossene Geräte zu erkennen. Standardmäßig scannt GFI EndPointSecurity alle unterstützten Gerätekategorien und Schnittstellen.

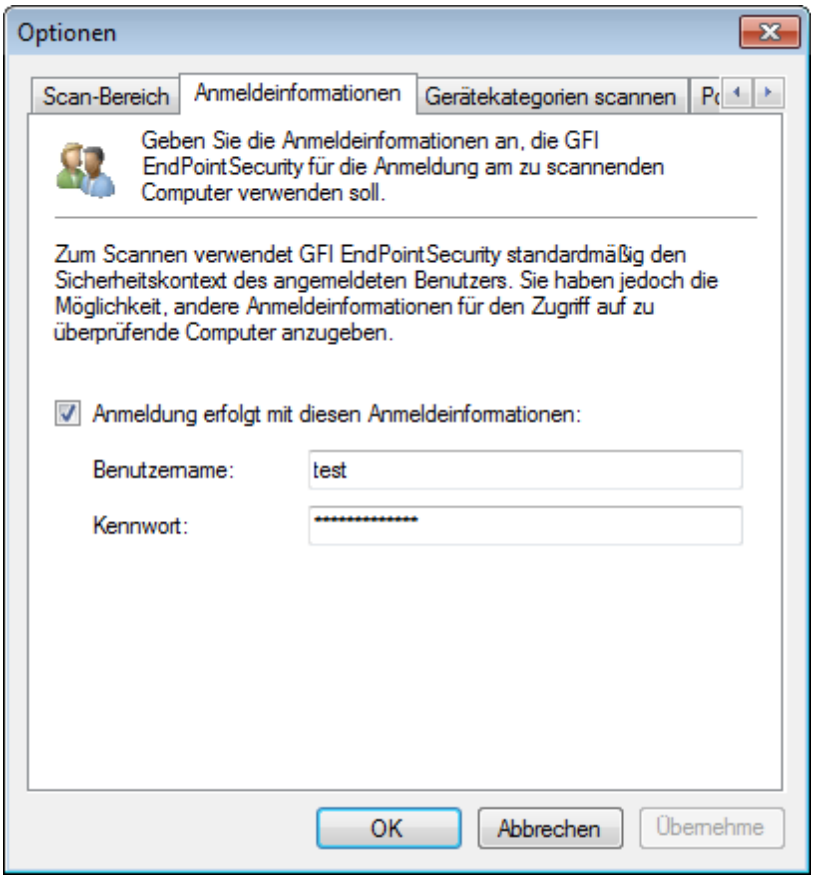
Ein erkannter kontrollierter Computer kann ein beliebiger Computer im Netzwerk sein und muss nicht unter eine Schutzrichtlinie von GFI EndPointSecurity fallen. Der Gerätescan muss unter einem Konto mit administrativen Berechtigungen für den/die kontrollierten Computer durchgeführt werden.

Themen in diesem Kapitel

6.1 Ausführen eines Gerätescans

So führen Sie einen Gerätescan aus:

1. Klicken Sie auf die Registerkarte **Scannen**.
2. Klicken Sie unter **Allgemeine Aufgaben** auf **Optionen**.
3. Wählen Sie unter **Optionen** die Registerkarte **Anmeldeinformationen**.

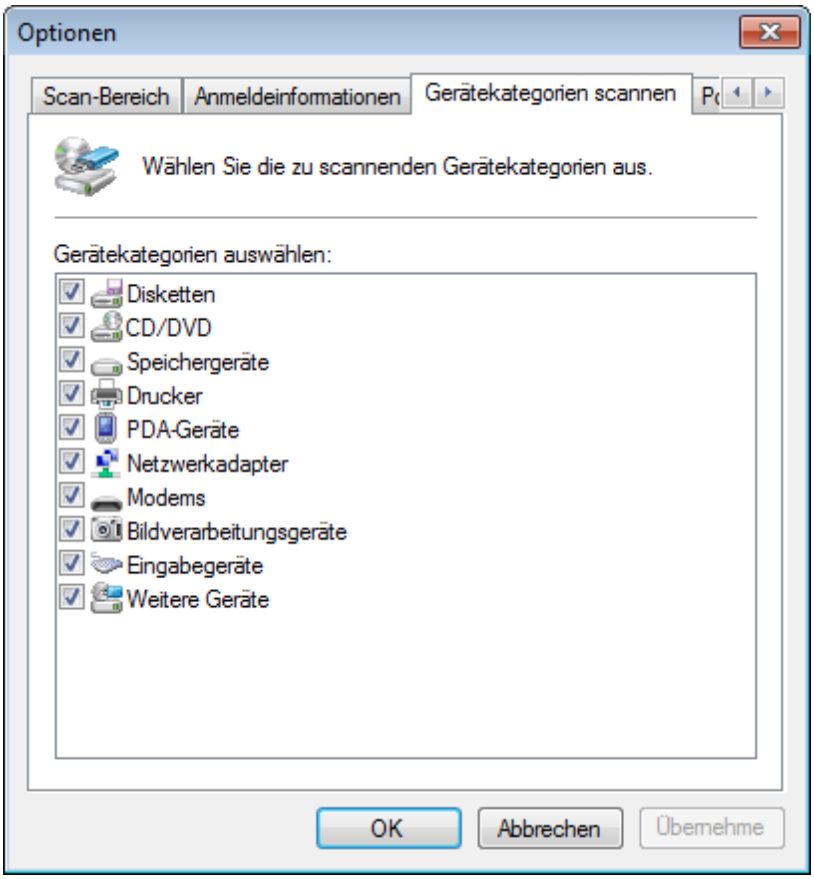


Screenshot 67: Ausführen eines Gerätescans - Registerkarte „Anmeldeinformationen“

4. Aktivieren/Deaktivieren Sie im Dialogfeld **Optionen** auf der Registerkarte **Anmeldeinformationen** die Option **Anmeldung erfolgt mit diesen Anmeldeinformationen**, um die Verwendung alternativer Anmeldeinformationen zu aktivieren/deaktivieren.

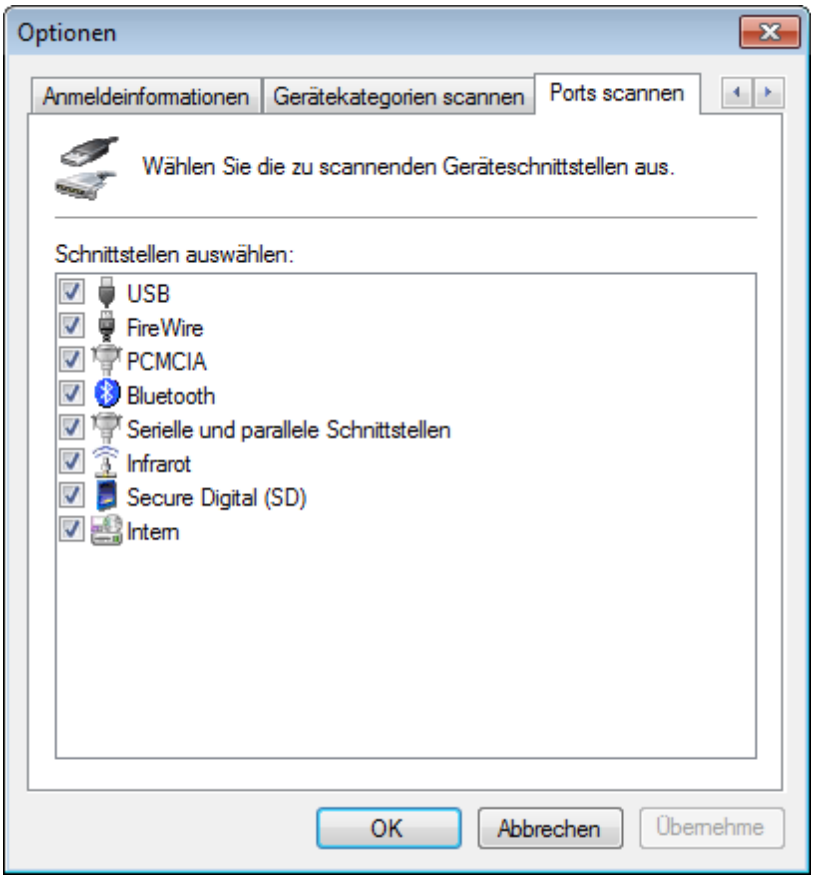
Hinweis

Wenn Sie keine Anmeldeinformationen angeben, versucht GFI EndPointSecurity sich mit dem aktuell angemeldeten Benutzer bei den kontrollierten Computern anzumelden.



Screenshot 68: Ausführen eines Gerätescans- Registerkarte „Gerätekategorien scannen“

5. Klicken Sie auf die Registerkarte **Gerätekategorien scannen**, und wählen Sie die Gerätekategorien aus, die in den Scanvorgang eingeschlossen werden sollen.



Screenshot 69: Ausführen eines Gerätescans - Registerkarte „Ports scannen“

6. Klicken Sie auf die Registerkarte **Ports scannen**, und wählen Sie die Schnittstellen aus, die in den Scanvorgang eingeschlossen werden sollen.

7. Klicken Sie auf **Übernehmen** und **OK**.

8. So legen Sie zu scannende kontrollierte Computer fest:

» Geben Sie im rechten Bereich in das Textfeld **Scanziel** den Computernamen oder die IP-Adresse des/der zu scannenden kontrollierten Computer(s) ein. Klicken Sie auf **Neuer Scan**, um den Scan des angegebenen Computers zu starten.

6.2 Analysieren der Ergebnisse des Gerätescans

Die Ergebnisse des Gerätescans werden in zwei Abschnitte unterteilt:

» Computer

» Geräteliste

6.2.1 Computer

Computer	Schutzrichtlinie	Aktuell	Status	Zeitplan
TCOFFICESERVER	Allgemeine Kontrolle	Nein (Aktualisierung ausstehend)	Online (Letzte Nachricht erhalten: 18/02/...	k. A.
W710	Allgemeine Kontrolle	Nein (Aktualisierung ausstehend)	Online (Letzte Nachricht erhalten: 18/02/...	k. A.
ARIELLETEST03	Allgemeine Kontrolle	Nein (Agenten-Bereitstellung auss...	k. A.	k. A.
ENDPOINT	Allgemeine Kontrolle	Nein (Aktualisierung ausstehend)	Online (Letzte Nachricht erhalten: 18/02/...	k. A.
EUGENIA-TEST	Allgemeine Kontrolle	Nein (Agenten-Bereitstellung auss...	k. A.	k. A.

Screenshot 70: Bereich „Computer“

In diesem Bereich wird eine Zusammenfassung der Ergebnisse des Gerätescans für jeden gescannten kontrollierten Computer angezeigt. Folgende Informationen werden angezeigt:

» Computername/IP-Adresse,

» Aktuell angemeldeter Benutzer,

» Schutzstatus, d. h. ob der Computer unter eine Schutzrichtlinie von GFI EndPointSecurity fällt,

» Gesamtzahl aktuell und zuvor verbundener Geräte,

» Anzahl aktuell verbundener Geräte.

Gehört ein gescannter kontrollierter Computer zu keiner Schutzrichtlinie von GFI EndPointSecurity, können Sie wählen, ob er einer Richtlinie zugewiesen werden soll. Gehen Sie dazu wie folgt vor:

1. Klicken Sie in der Spalte **Computer** mit der rechten Maustaste auf den gewünschten Computernamen/die gewünschte IP-Adresse, und wählen Sie **Agent(en) bereitstellen...**

2. Wählen Sie die bereitzustellende Schutzrichtlinie aus. Klicken Sie zum Fortfahren auf **Weiter** und zum Start der Bereitstellung auf **Fertig stellen**.

6.2.2 Geräteliste

Devices list:

Device Name	Device Description	Connected	Device Category	Connection Port	Vendor ID
Floppy disk drive		Yes	Floppy Disks	Internal	
Msft Virtual CD/ROM		Yes	CD / DVD	Internal	msft

Screenshot 71: Bereich „Geräteliste“

In diesem Bereich wird eine detaillierte Liste der erkannten Geräte für jeden gescannten Computer angezeigt. Folgende Informationen werden angezeigt:

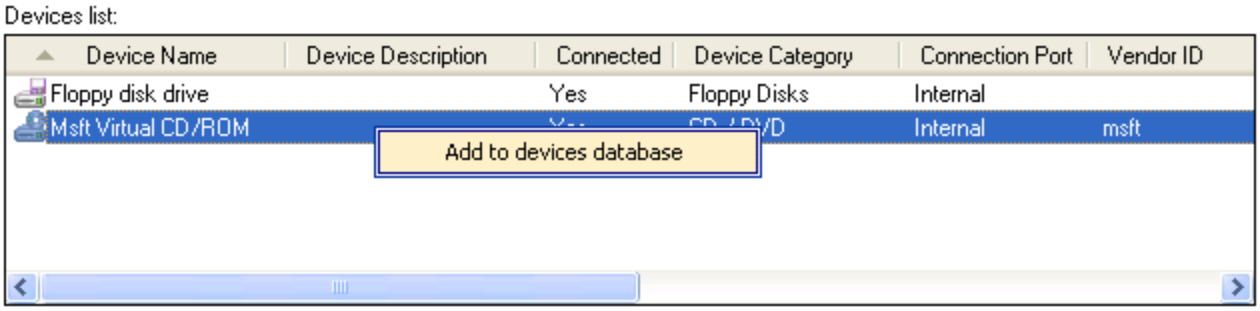
» Gerätename, Beschreibung und Kategorie

» Schnittstelle

» Verbindungsstatus, d. h. ob das Gerät aktuell angeschlossen ist.

6.3 Hinzufügen entdeckter Geräte zur Datenbank

Unter **Geräteliste** können Sie ein oder mehrere erkannte Geräte auswählen und diese der Gerätedatenbank hinzufügen. Diese Geräte werden dann aus dieser Datenbank abgefragt, wenn GFI EndPointSecurity für die Blacklist und Whitelist die momentan an die kontrollierten Computer angeschlossenen Geräte auflistet. Weitere Informationen finden Sie unter Konfigurieren der Geräte-Blacklist oder Konfigurieren der Geräte-Whitelist.



Screenshot 72: Bereich „Geräteliste“ - Hinzufügen von Geräten zur Gerätedatenbank

So fügen Sie Geräte der Gerätedatenbank hinzu:

1. Wählen Sie im Abschnitt **Geräteliste** ein oder mehrere Geräte aus, die der Gerätedatenbank hinzugefügt werden sollen.

2. Klicken Sie mit der rechten Maustaste auf die ausgewählten Geräte, und wählen Sie **Zur Gerätedatenbank hinzufügen**.

3. Klicken Sie auf **OK**.

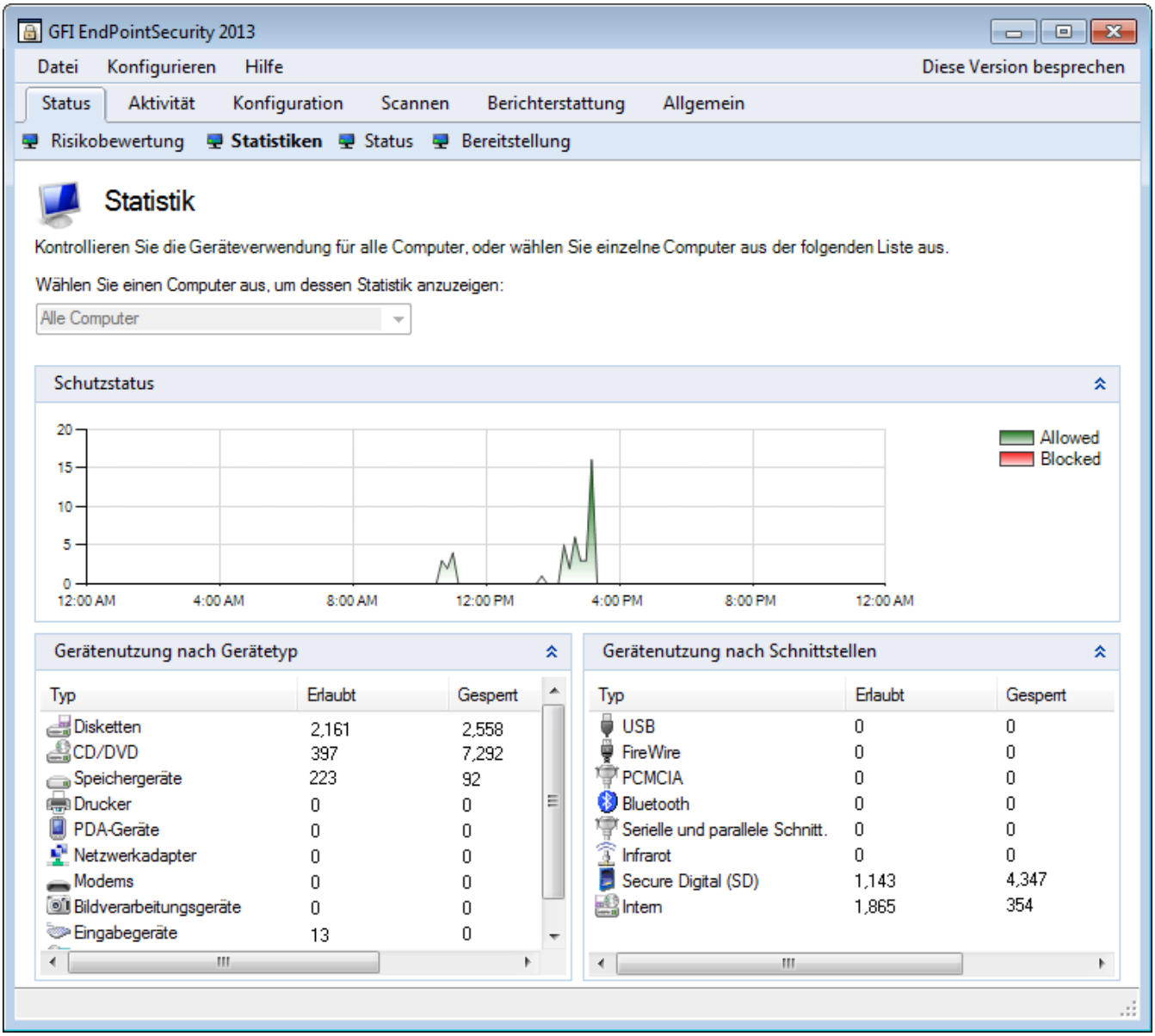
7 Überwachen der Geräteverwendung

Dieses Kapitel enthält Informationen zur Überwachung der Verwendung von Netzwerkgeräten. GFI EndPointSecurity ermöglicht die Nachverfolgung aller Ereignisse, die durch GFI EndPointSecurity-Agenten auf Netzwerkcomputern verursacht werden. Zum Führen eines Überwachungspfades muss die Protokollierung aktiviert sein. Weitere Informationen finden Sie unter Konfigurieren der Ereignisprotokollierung (page 85).

Themen in diesem Kapitel

7.1 Statistik

Über die untergeordnete Registerkarte „Statistik“ können Sie Trends in der täglichen Geräteaktivität feststellen und eine Statistik zu einzelnen oder allen Computern Ihres Netzwerks abrufen.



Screenshot 73: Untergeordnete Registerkarte „Statistik“

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte „Statistik“ in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Status** > **Statistik**.

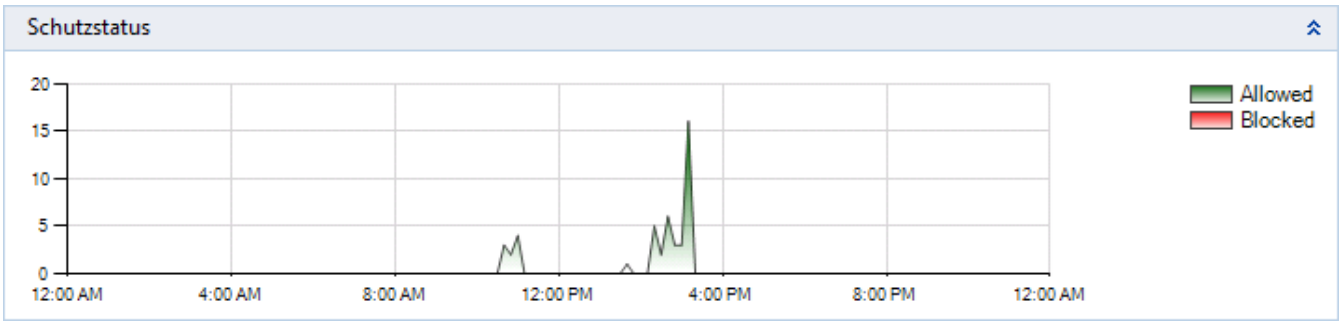
Der Abschnitt **Statistik** enthält folgende Informationen:

» Schutzstatus

» Gerätenutzung nach Gerätetyp

» Gerätenutzung nach Schnittstellen

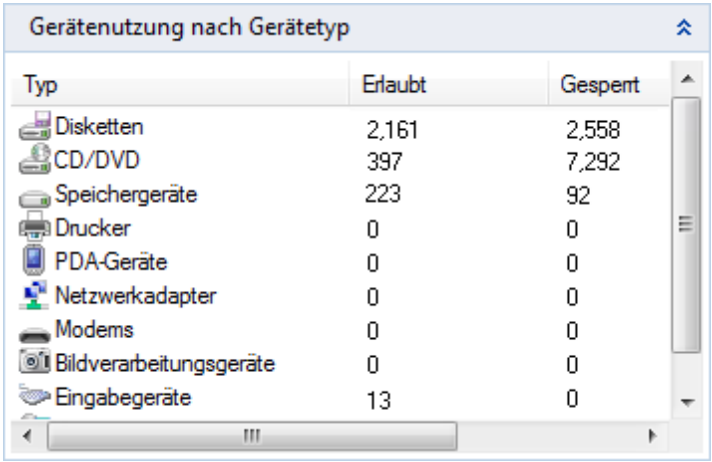
7.1.1 Schutzstatus



Screenshot 74: Bereich „Schutzstatus“

In diesem Bereich wird die Geräteaktivität auf Computern im Tagesverlauf anhand eines Diagramms angezeigt. Zugelassene und gesperrte Geräte werden farblich unterschieden. Die bereitgestellten Informationen können für einen einzelnen oder für alle Netzwerkcomputer angezeigt werden.

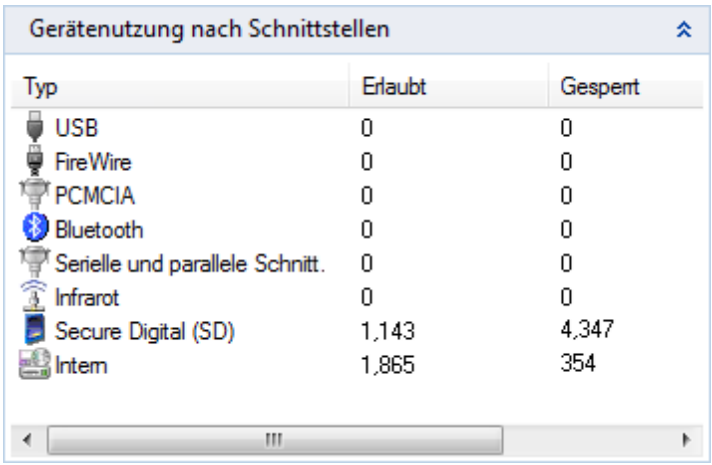
7.1.2 Gerätenutzung nach Gerätetyp



Screenshot 75: Bereich „Gerätenutzung nach Gerätetyp“

Dieser Bereich informiert Sie über zugelassene oder blockierte Verbindungsversuche einzelner Gerätekategorien. Die bereitgestellten Informationen können für einen einzelnen oder für alle Netzwerkcomputer angezeigt werden.

7.1.3 Gerätenutzung nach Schnittstellen



Screenshot 76: Bereich „Gerätenutzung nach Schnittstellen“

Dieser Bereich informiert Sie über zugelassene oder blockierte Verbindungsversuche über einzelne Schnittstellen. Die bereitgestellten Informationen können für einen einzelnen oder für alle Netzwerkcomputer angezeigt werden.

7.2 Aktivität

Verwenden Sie die Registerkarte „Aktivität“, um die Geräteverwendung im Netzwerk und protokollierte Ereignisse für einen bestimmten Computer oder für alle Computer im Netzwerk zu überwachen.

Der Abschnitt „Aktivität“ enthält folgende Informationen:

» Aktivitätsprotokoll

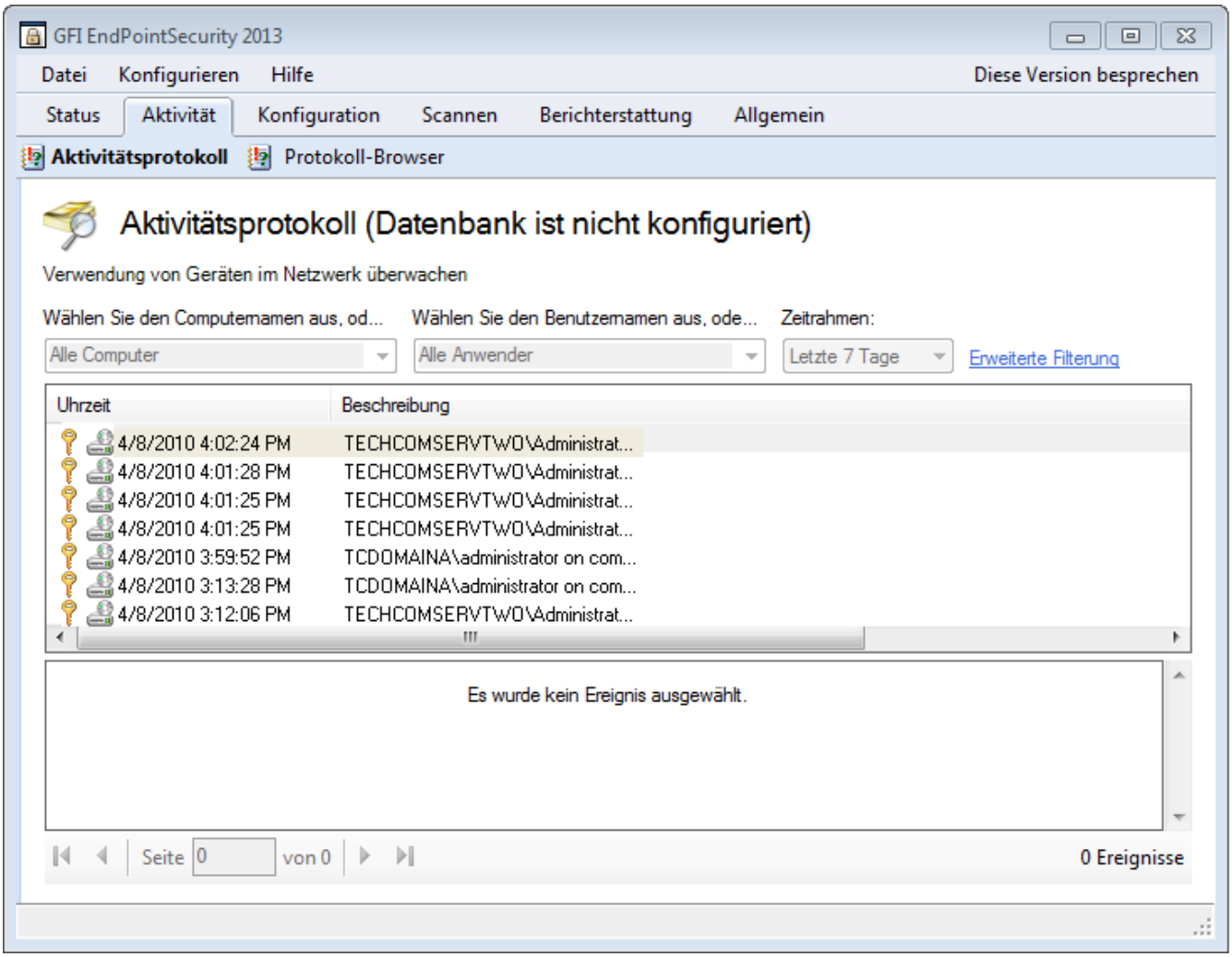
» Erweiterte Filterung

» Protokoll-Browser

» Erstellen von Ereignisabfragen

7.2.1 Aktivitätsprotokoll

Mit dieser untergeordneten Registerkarte überwachen Sie die Geräte, die im Netzwerk verwendet werden. Wählen Sie den Computer und/oder den Benutzer aus den jeweiligen Dropdown-Menüs aus, um das Aktivitätsprotokoll nach Computer und/oder Benutzer zu filtern. Zusätzlich ermöglicht diese Registerkarte, die Liste nach bereitgestellten Zeitfiltern weiter zu filtern.



Screenshot 77: Untergeordnete Registerkarte „Aktivitätsprotokoll“

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte „Aktivitätsprotokoll“ in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Aktivität** > **Aktivitätsprotokoll**.

Klicken Sie für weitere Details zu einem Ereignis auf das jeweilige Ereignis. Zusätzliche Informationen werden im Bereich zur Ereignisbeschreibung im unteren Bereich der untergeordneten Registerkarte angezeigt.

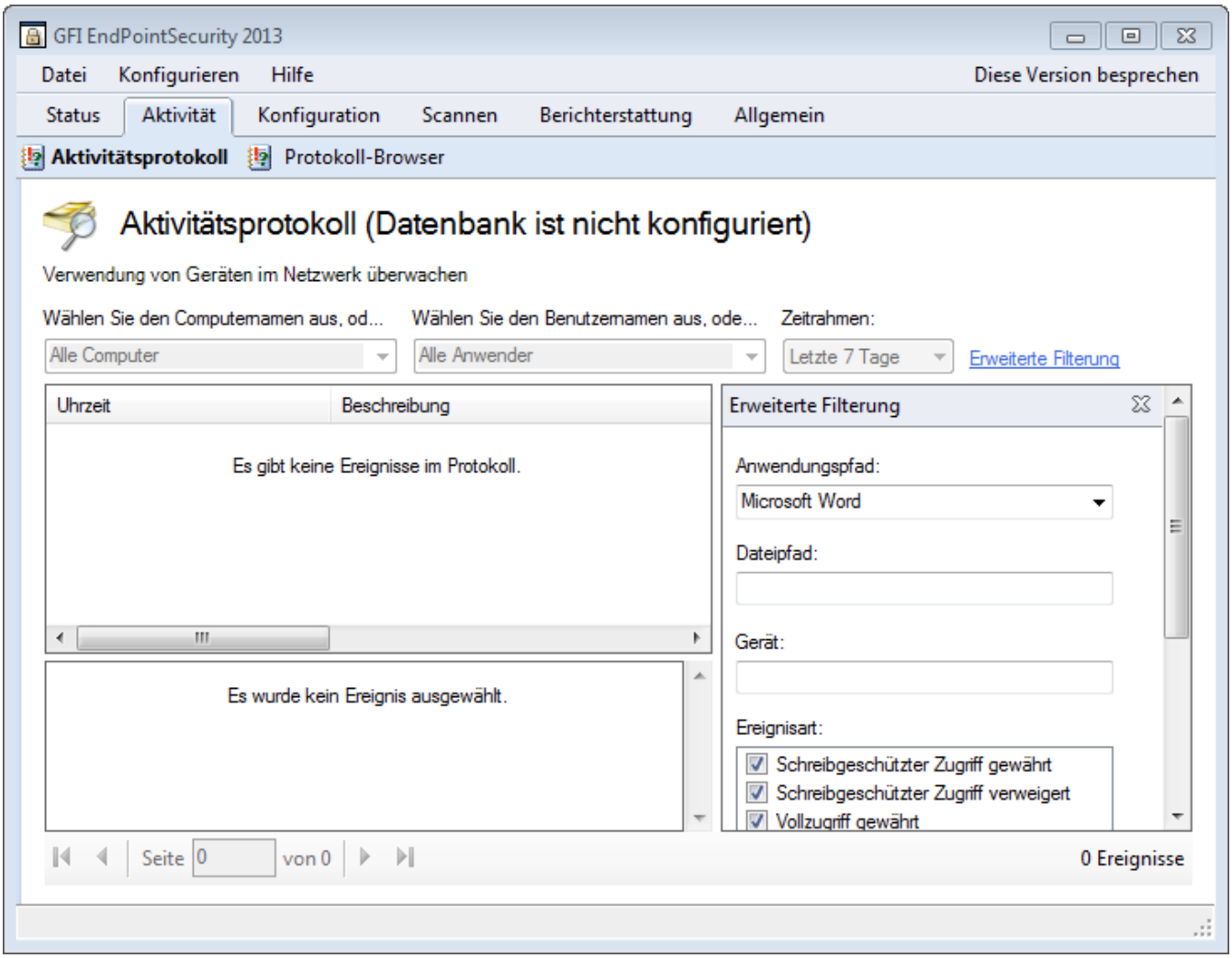
Um die Registerkarte „Aktivitätsprotokoll“ den Anforderungen Ihres Unternehmens anzupassen, klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie die Spalten, die der Ansicht hinzugefügt oder daraus entfernt werden sollen.

Ziehen Sie zur Änderung der Spaltenreihenfolge eine Spalte am Spaltenkopf an die gewünschten Stelle.

7.2.2 Erweiterte Filterung

Diese Funktion ermöglicht die weitere Filterung der Protokolle zum Geräteverwendungsverlauf mithilfe der folgenden Kriterien:

- Anwendungspfad
- Dateipfad
- Gerät
- Ereignisart.



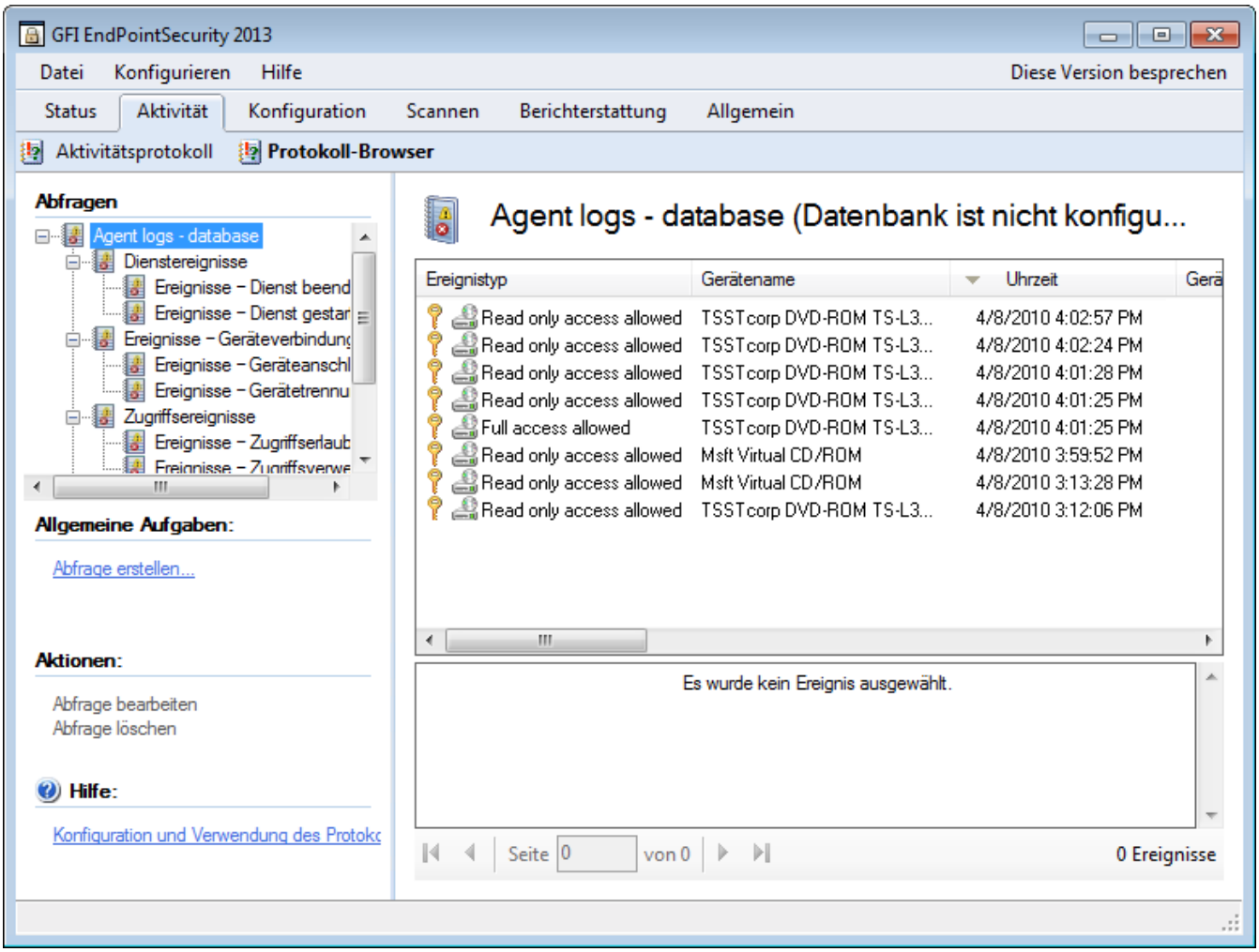
Screenshot 78: Untergeordnete Registerkarte „Aktivitätsprotokoll“ - Erweiterte Filterung

Um auf die erweiterten Filteroptionen des Aktivitätsprotokoll zuzugreifen, klicken Sie auf der untergeordneten Registerkarte **Aktivitätsprotokoll** auf **Erweiterte Filterung**.

7.2.3 Protokoll-Browser

Über die untergeordnete Registerkarte „Protokoll-Browser“ können Sie im Datenbank-Backend gespeicherte Ereignisse anzeigen und durchsuchen.

GFI EndPointSecurity verfügt außerdem über einen Abfragegenerator, mit dem sich die Suche nach bestimmten Ereignissen vereinfachen lässt. Er unterstützt Sie bei der Erstellung eigener Filter zur Filterung von Ereignisdaten und zur Darstellung von Informationen, die für die Suche notwendig sind, ohne dass diese aus dem Datenbank-Backend gelöscht werden.



Screenshot 79: Untergeordnete Registerkarte „Protokoll-Browser“

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte „Protokoll-Browser“ in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Aktivität** > **Protokoll-Browser**.

Klicken Sie für weitere Details zu einem Ereignis auf das jeweilige Ereignis. Zusätzliche Informationen werden im Bereich zur Ereignisbeschreibung im unteren Bereich der untergeordneten Registerkarte angezeigt.

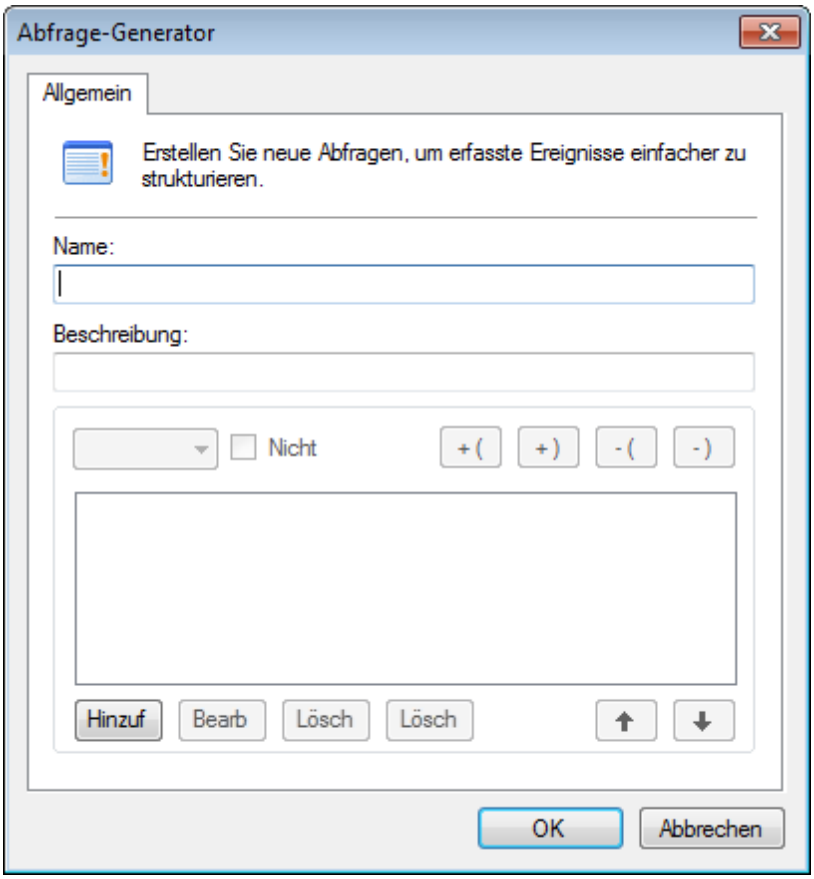
7.2.4 Erstellen von Ereignisabfragen

So erstellen Sie eine eigene Ereignisabfrage:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Aktivität**.

2. Klicken Sie auf die untergeordnete Registerkarte **Protokoll-Browser**.

3. Klicken Sie im linken Bereich mit der rechten Maustaste auf den Knoten **Agentenprotokolle - Datenbank**, und wählen Sie **Abfrage erstellen...**.



Screenshot 80: Optionen des Abfrage-Generators

4. Geben Sie im Dialogfeld **Abfrage-Generator** einen Namen und eine Beschreibung für die neue Abfrage ein.

5. Klicken Sie auf **Hinzufügen…**, konfigurieren Sie die erforderliche(n) Abfragebedingung(en), und klicken Sie auf **OK**. Wiederholen Sie dies, bis alle erforderlichen Abfragebedingungen festgelegt wurden.

6. Klicken Sie auf **OK**, um die Einstellungen fertig zu stellen. Ihre Abfrage wird als Unterknoten des Knotens **Agentenprotokolle - Datenbank** aufgeführt.

Hinweis

Sie können auch die Ergebnisse vorhandener Ereignisabfragen durch Erstellen weiterer spezifischer Unterabfragen filtern. Klicken Sie dazu mit der rechten Maustaste auf eine Abfrage, und wählen Sie **Abfrage erstellen...**.

8 Statusüberwachung

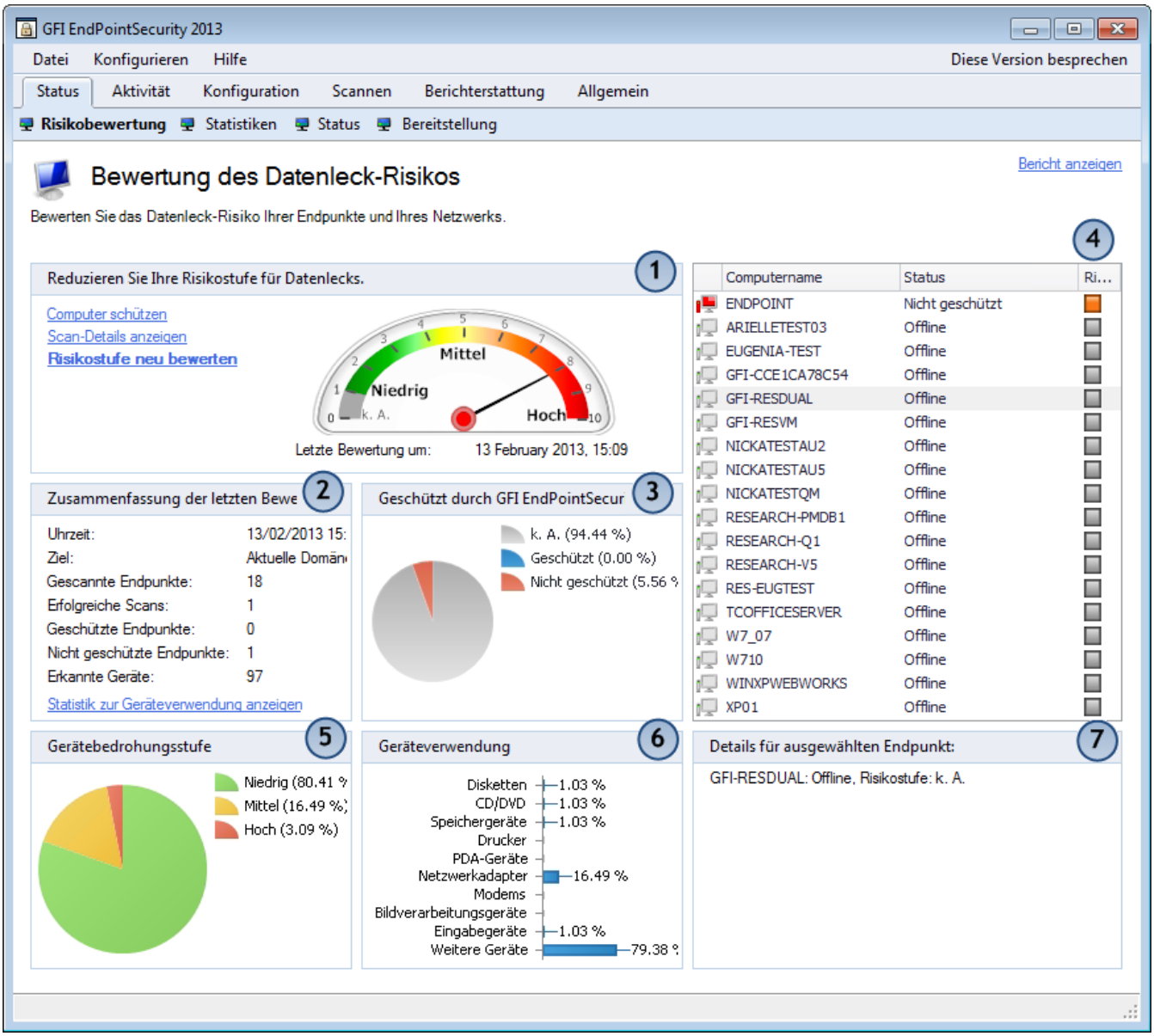
Dieses Kapitel enthält Informationen zur Überwachung des Status von GFI EndPointSecurity sowie des Status von GFI EndPointSecurity-Agenten. Die Statusanzeigen liefern Diagramme und statistische Informationen zur Verwendung mobiler Geräte.

Themen in diesem Kapitel

8.1 Ansicht „Riskikobewertung“

Verwenden Sie die Unterregisterkarte „Risikobewertung“ um den Status folgender Elemente anzuzeigen:

- Risikobewertungsstufe auf Netzwerkcomputern mit installierten GFI EndPointSecurity-Agenten.
- Auf Netzwerkcomputern bereitgestellte GFI EndPointSecurity-Agenten.
- Geräteverwendung, wie die Anzahl und Prozentsätze der gesperrten und der zugelassenen Geräte.
- Bedrohungsstufe der Geräte im Netzwerk.



Screenshot 81: Unterregisterkarte „Risikobewertung“

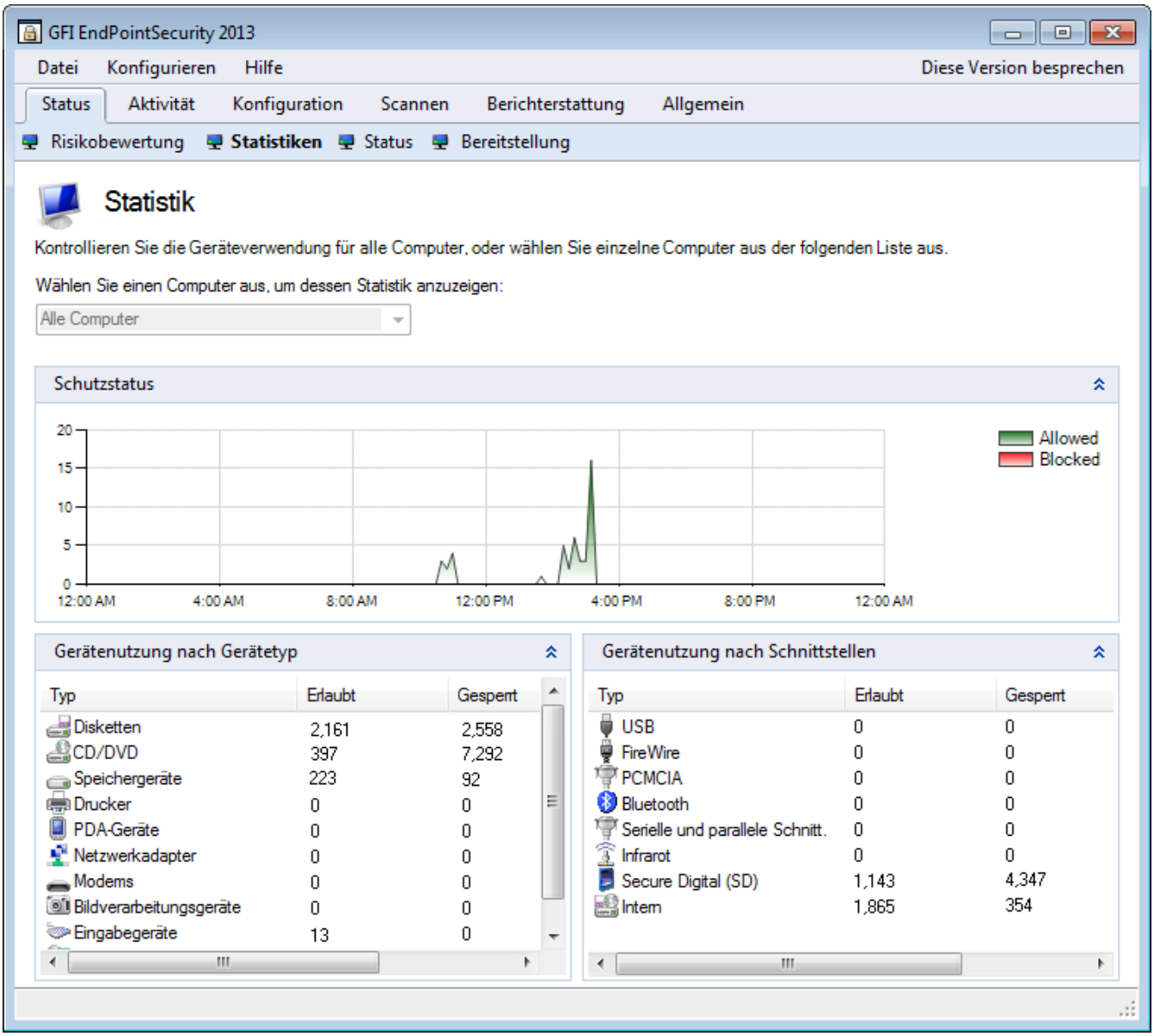
Klicken Sie zum Zugriff auf die Unterregisterkarte „Risikobewertung“ in der Verwaltungskonsole von GFI EndPointSecurity auf die Registerkarte **Status** >**Risikobewertung**.

Funktion	Beschreibung
1	In diesem Abschnitt wird Folgendes angezeigt: » Die Anzeige der Risiskobewertungsergebnisse der Netzwerkcomputer. » Die Option zum erneuten Scannen des Netzwerks, um die neuesten Risikobewertungsergebnisse zu erhalten. » Die Uhrzeit der letzten Risikobewertung.

Funktion	Beschreibung
2	Dieser Bereich enthält die kumulativen Werte zur Anzahl der: » Gescannte Endpunkte » Erfolgreiche Scans » Geschützte Endpunkte » Ungeschützte Endpunkte » Erkannte Geräte Dieser Abschnitt enthält des Weiteren: » Das Netzwerk, in dem die Agenten installiert sind. » Die Zeit und das Datum, zu dem der Dienst zuletzt gestartet wurde.
3	Dieser Bereich informiert anhand eines Diagramms über die Anzahl der Agenten, die momentan: » Auf Netzwerkcomputern installiert werden müssen, » Durch GFI EndPointSecurity geschützt » Nicht durch GFI EndPointSecurity geschützt
4	Dieser Abschnitt enthält alle Agenten, die auf Netzwerkcomputern bereitgestellt sind. Dabei wird zwischen online und offline unterschieden. Weitere Informationen finden Sie unter Ansicht „Status“ (page 109).
5	Dieser Abschnitt enthält Darstellungen zum Prozentsatz der Gerätebedrohung, die von Agenten auf Netzwerkcomputern mit installiertem GFI EndPointSecurity protokolliert wurde.
6	In diesem Bereich wird in einem Diagramm der von den Agenten protokollierte Prozentsatz der Benutzerzugriffe pro Gerätekategorie im Vergleich zur Gesamtzahl der Gerätezugriffe angezeigt. Benutzerzugriffe auf Geräte beziehen sich sowohl auf zugängliche als auch blockierte Geräte.
7	Dieser Bereich beinhaltet: » Das Benutzerkonto, auf dem der GFI EndPointSecurity-Dienst ausgeführt wird. » Der Risikofaktor. » Der aktuelle Verschlüsselungsstatus am Endpunkt. » Der Funktionsstatus der Dateitypüberprüfung. » Der Funktionsstatus der Inhaltsüberprüfung. » Die Uhrzeit der letzten Risikobewertung.

8.2 Statistikanzeige

Über die untergeordnete Registerkarte „Statistik“ können Sie Trends in der täglichen Geräteaktivität feststellen und eine Statistik zu einzelnen oder allen Computern Ihres Netzwerks abrufen.



Screenshot 82: Untergeordnete Registerkarte „Statistik“

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte „Statistik“ in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Status** > **Statistik**.

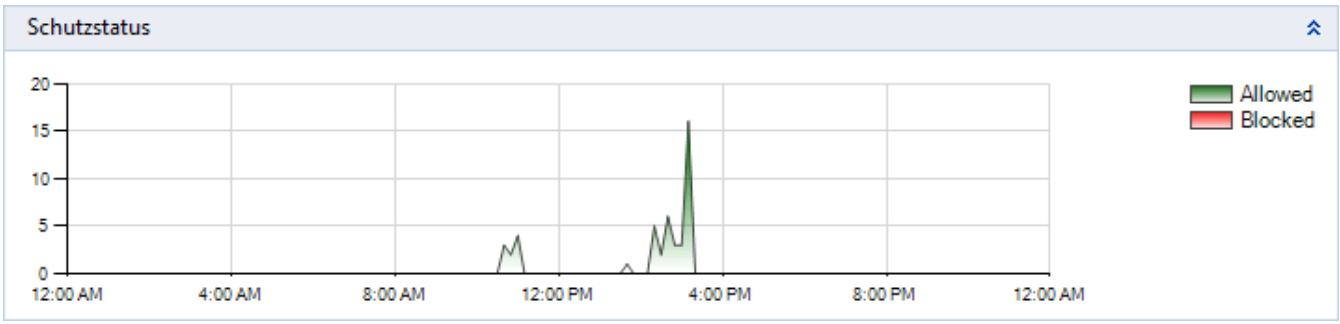
Der Abschnitt **Statistik** enthält folgende Informationen:

» Schutzstatus

» Gerätenutzung nach Gerätetyp

» Gerätenutzung nach Schnittstellen

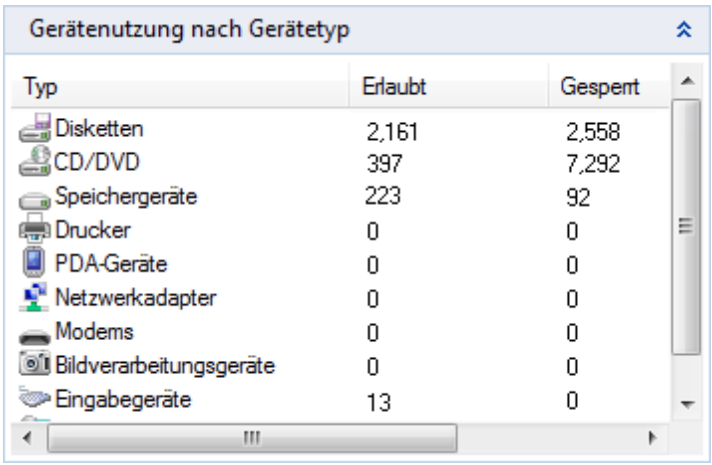
8.2.1 Schutzstatus



Screenshot 83: Bereich „Schutzstatus“

In diesem Bereich wird die Geräteaktivität auf Computern im Tagesverlauf anhand eines Diagramms angezeigt. Zugelassene und gesperrte Geräte werden farblich unterschieden. Die bereitgestellten Informationen können für einen einzelnen oder für alle Netzwerkcomputer angezeigt werden.

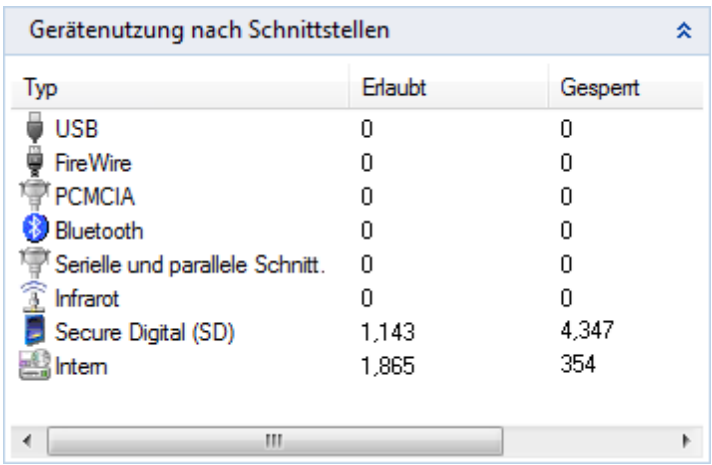
8.2.2 Gerätenutzung nach Gerätetyp



Screenshot 84: Bereich „Gerätenutzung nach Gerätetyp“

Dieser Bereich informiert Sie über zugelassene oder blockierte Verbindungsversuche einzelner Gerätekategorien. Die bereitgestellten Informationen können für einen einzelnen oder für alle Netzwerkcomputer angezeigt werden.

8.2.3 Gerätenutzung nach Schnittstellen

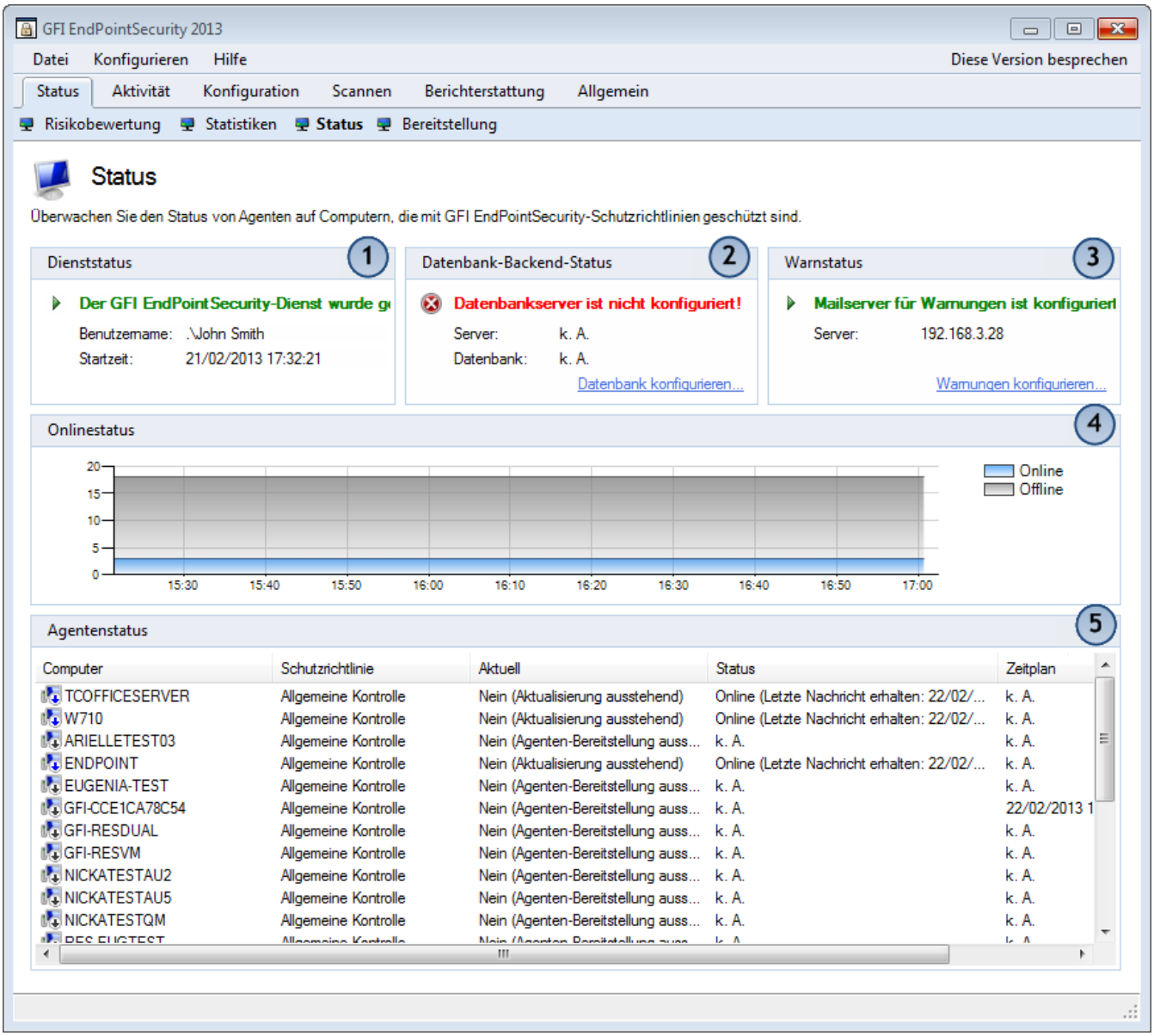


Screenshot 85: Bereich „Gerätenutzung nach Schnittstellen“

Dieser Bereich informiert Sie über zugelassene oder blockierte Verbindungsversuche über einzelne Schnittstellen. Die bereitgestellten Informationen können für einen einzelnen oder für alle Netzwerkcomputer angezeigt werden.

8.3 Ansicht „Status“

Verwenden Sie die Unterregisterkarte „Status“, um den Status aller Bereitstellungsaktionen auf Ihren Netzwerkzielen zu bestimmen. Folgende Informationen werden für jeden kontrollierten Computer angezeigt:



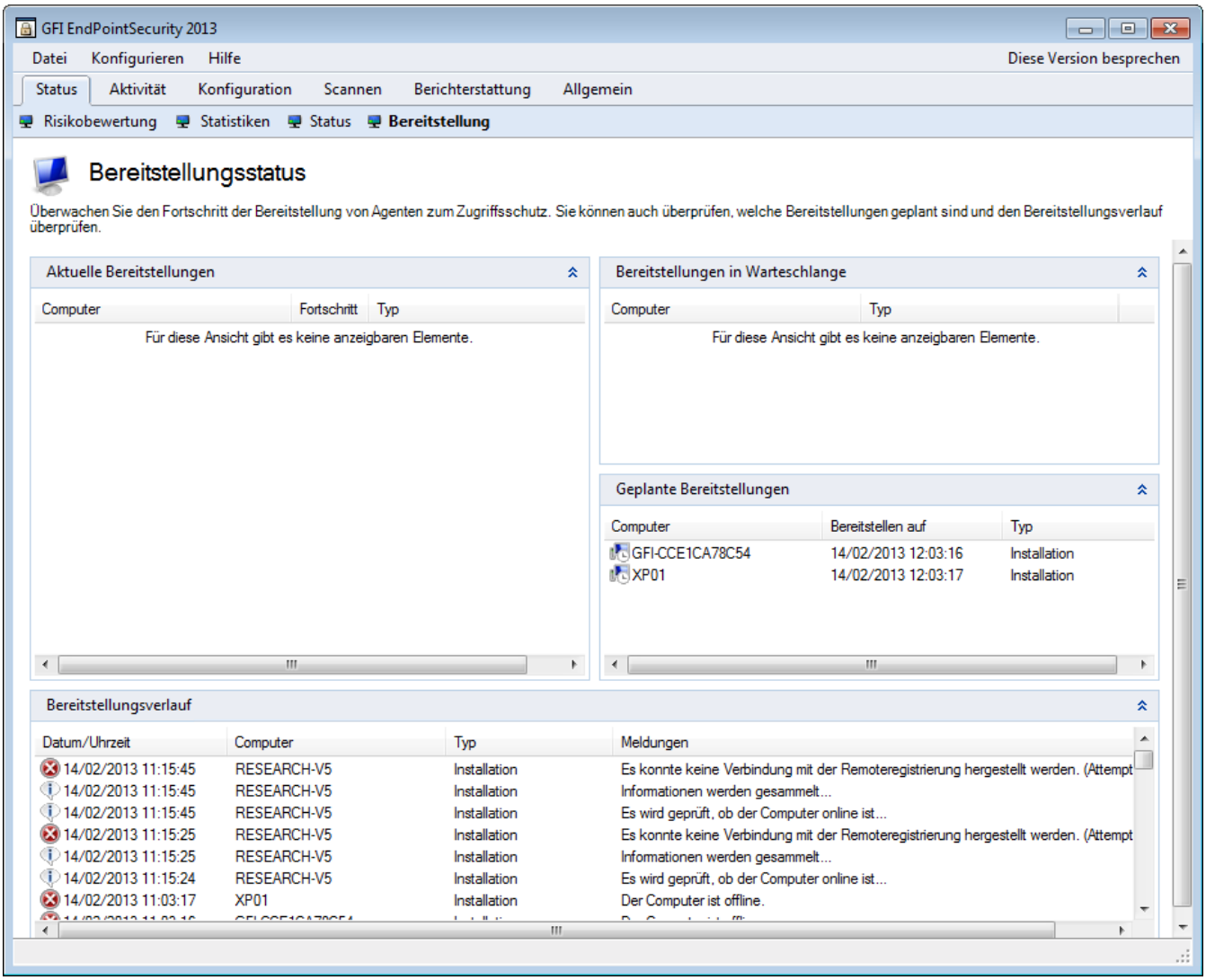
Screenshot 86: Unterregisterkarte „Status“

Funktion	Beschreibung
1	Dieser Abschnitt enthält: » Den Betriebsstatus der Verwaltungskonsole von GFI EndPointSecurity. » Das Benutzerkonto, auf dem der GFI EndPointSecurity-Dienst ausgeführt wird. » das Datum und die Uhrzeit des letzten Starts des Dienstes.

Funktion	Beschreibung
2	Dieser Abschnitt enthält: » Den Betriebsstatus des aktuell von GFI EndPointSecurity genutzten Datenbankservers. » Den Namen oder die IP-Adresse des aktuell von GFI EndPointSecurity genutzten Datenbankservers. » Den Namen der Datenbank, in der GFI EndPointSecurity Ereignisse archiviert. Um die aktuellen Datenbankeinstellungen zu ändern, klicken Sie auf **Datenbank konfigurieren…**. Dadurch wird das Dialogfeld **Datenbank-Backend** geöffnet. Weitere Informationen finden Sie unter Verwalten des Datenbank-Backends (page 117).
3	Dieser Abschnitt enthält: » Den Betriebsstatus des aktuell von GFI EndPointSecurity genutzten Warnservers. » Den Namen oder die IP-Adresse des aktuell von GFI EndPointSecurity genutzten Warnservers. Um die aktuellen Warneinstellungen zu ändern, klicken Sie auf **Warnungen konfigurieren...** Dadurch wird das Dialogfeld **Warnoptionen** geöffnet. Weitere Informationen finden Sie unter Konfigurieren der Warnungen (page 87).
4	Dieser Abschnitt enthält eine Darstellung aller auf den Netzwerkcomputern bereitgestellten Agenten. Dabei wird zwischen online und offline unterschieden.
5	Dieser Abschnitt enthält: » Den Namen des kontrollierten Computers und die zutreffende Schutzrichtlinie. » Den Status des GFI EndPointSecurity-Agenten, d. h. ob er aktuell bereitgestellt wird und auf dem neuesten Stand ist, oder ob die Bereitstellung aussteht. » Status der kontrollierten Computer (online/offline). So stellen Sie ausstehende Agenten bereit: 1. Wählen Sie einen oder mehrere Computer aus dem Abschnitt **Agentenstatus** aus. 2. Klicken Sie mit der rechten Maustaste auf die ausgewählten Computer, und wählen Sie die Option **Ausgewählte(n) Agenten bereitstellen** oder **Bereitstellungszeitplan für ausgewählte(n) Agenten festlegen...** 3. Klicken Sie auf **OK**. **Hinweis** Wenn ein kontrollierter Computer offline ist, wird die Bereitstellung um eine Stunde verschoben. GFI EndPointSecurity versucht, diese Richtlinie jede Stunde bereitzustellen, bis der kontrollierte Computer wieder online ist. **Hinweis** Jeder Agent sendet regelmäßig seinen Onlinestatus an GFI EndPointSecurity. Falls diese Daten nicht von der Hauptinstallation empfangen werden, wird der Agent als offline angesehen.

8.4 Anzeige des Bereitstellungsstatus

8.4.1 Informationen zur Anzeige des Bereitstellungsstatus



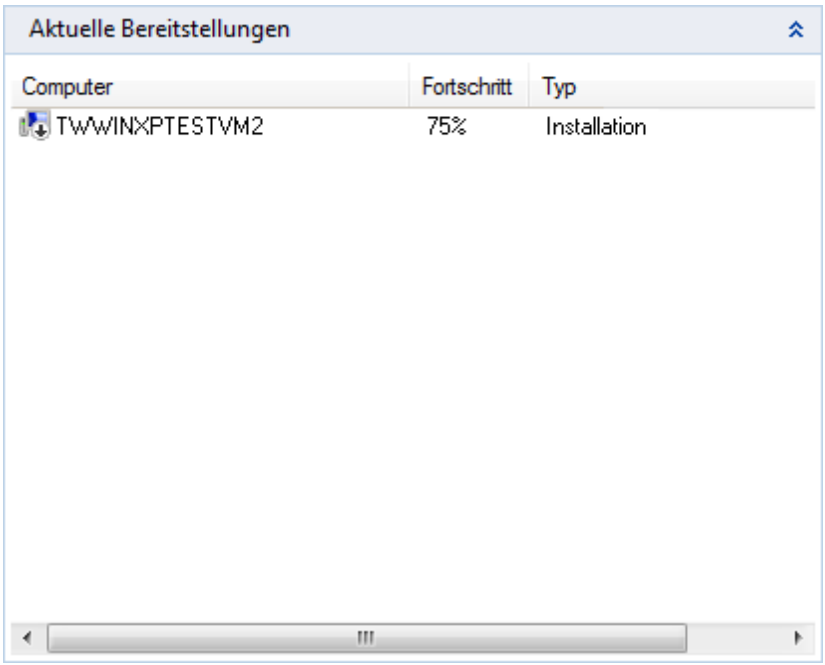
Screenshot 87: Untergeordnete Registerkarte „Bereitstellung“

Folgende Informationen werden auf der untergeordneten Registerkarte „Bereitstellung“ angezeigt:

- Aktuelle Bereitstellungsabläufe,
- Bereitstellungen in Warteschlange,
- Geplante Bereitstellungen,
- Bereitstellungsverlauf.

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte „Bereitstellung“ in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Status** > **Bereitstellung**.

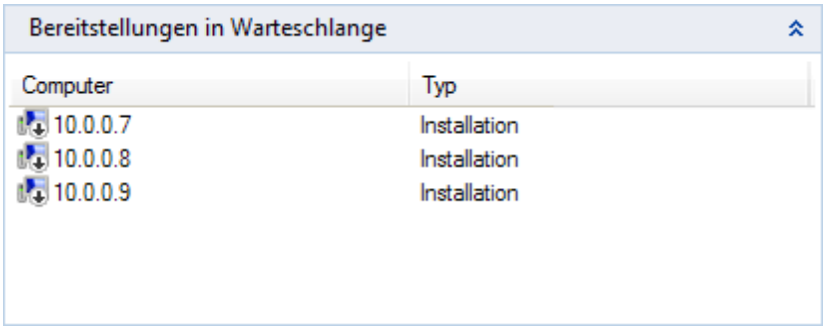
8.4.2 Aktuelle Bereitstellungen



Screenshot 88: Bereich „Aktuelle Bereitstellungen“

In diesem Bereich werden alle aktuell aktiven Bereitstellungen angezeigt. Sie erhalten Informationen zum Namen des Computers, zum Bereitstellungsfortschritt und zum Bereitstellungstyp. Bei der Bereitstellung handelt es sich um eine Installation, Deinstallation oder Aktualisierung.

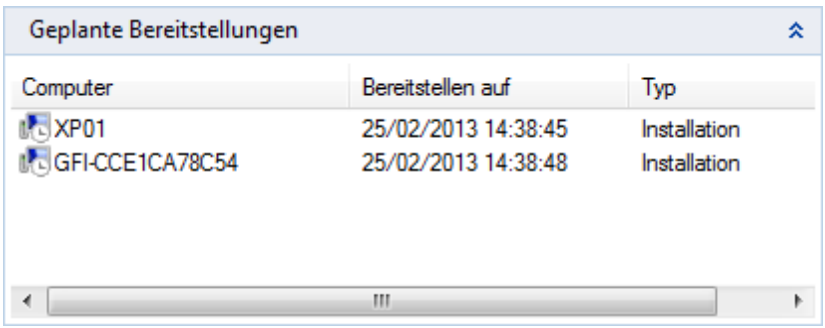
8.4.3 Bereitstellungen in Warteschlange



Screenshot 89: Bereich „Bereitstellungen in Warteschlange“

In diesem Bereich werden alle ausstehenden Bereitstellungen angezeigt, die sich in der Warteschlange befinden. Sie erhalten Informationen zum Namen des Computers und zum Bereitstellungstyp.

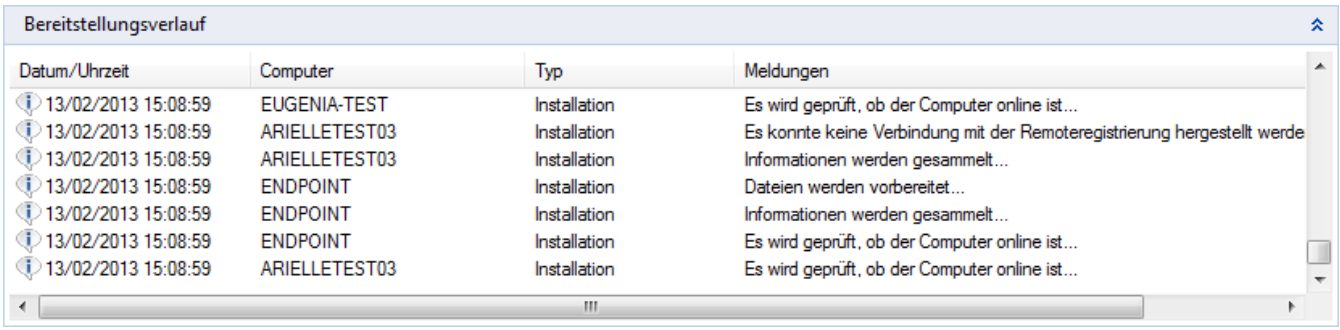
8.4.4 Geplante Bereitstellungen



Screenshot 90: Bereich „Geplante Bereitstellungen“

In diesem Bereich werden alle geplanten Bereitstellungen angezeigt. Sie erhalten Informationen zum Namen des Computers, zur geplanten Zeit und zum Bereitstellungstyp.

8.4.5 Bereitstellungsverlauf



Screenshot 91: Bereich „Bereitstellungsverlauf“

In diesem Bereich sind alle Stadien aller von GFI EndPointSecurity durchgeführten Agenten- bzw. Schutzrichtlinienbereitstellungen anhand eines Überwachungspfades aufgeführt. Die bereitgestellten Informationen beinhalten einen Zeitstempel für jeden Protokolleintrag, Computernamen, Bereitstellungstyp, Fehler und während der Bereitstellung generierte Informationenbenachrichtigung. Weitere Informationen finden Sie unter Fehlerbehebung und Support (page 140).

Um angezeigte Protokolleinträge zu entfernen, klicken Sie im Bereich **Bereitstellungsverlauf** auf **Alle Nachrichten löschen**.

9 Berichterstattung

Das GFI EndPointSecurity GFI ReportPack ist ein vollständig integrierbares, umfassendes Reporting-Modul für GFI EndPointSecurity. Mit dem ReportPack können die von GFI EndPointSecurity erfassten Daten automatisch nach Zeitplan in Form von aussagekräftigen IT- und Management-Berichten ausgegeben werden. So bleiben Sie über mit dem Netzwerk verbundene Geräte informiert und erhalten unter anderem Trend-Daten zur Verwendung von Geräten je Rechner oder Benutzer. Sogar über mobile Hardware ausgetauschte Dokumente werden inklusive ihrer Dateinamen angezeigt.

Themen in diesem Kapitel

9.1 GFI EndPointSecurity GFI ReportPack

Zum Erstellen von Berichten müssen Sie das Add-On GFI EndPointSecurity GFI ReportPack herunterladen und installieren. Rufen Sie zum Herunterladen des Add-Ons folgende Website auf:http://www.gfi.com/endpointsecurity/esecreportpack.htm

Weitere Informationen zu GFI EndPointSecurity GFI ReportPack:

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

2. Wählen Sie im linken Bereich entweder **GFI EndPointSecurity GFI ReportPack** oder **GFI ReportCenter** aus.

> **Hinweis**
>
> Es ist eine Internetverbindung erforderlich.

9.2 Erstellen von Übersichtsberichten

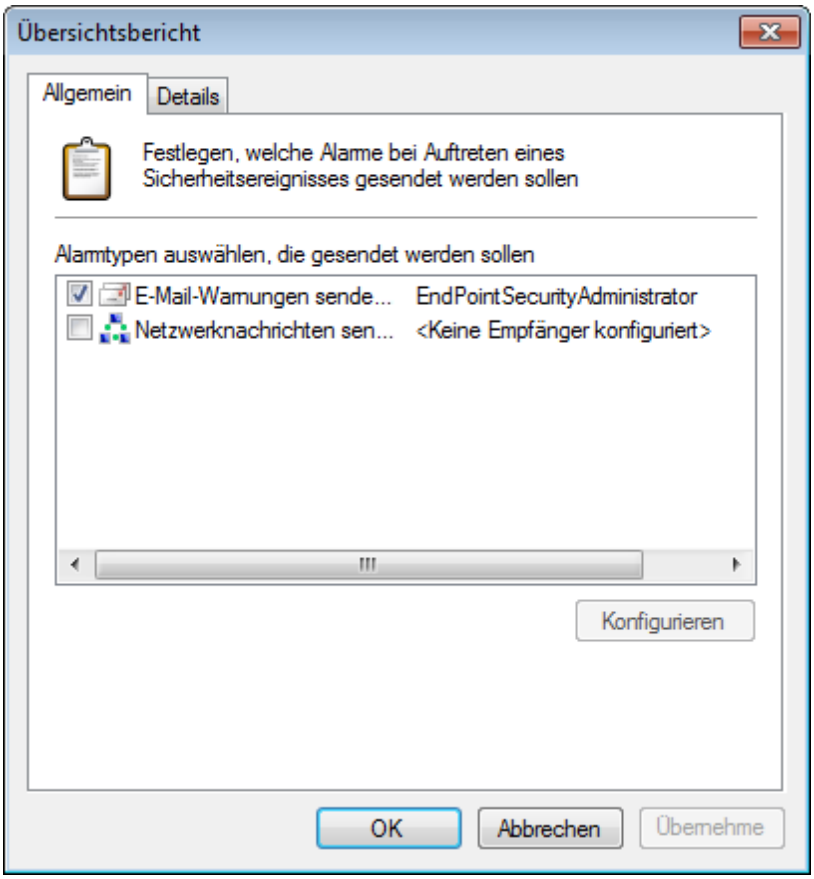
In GFI EndPointSecurity können Sie Übersichtsberichte für die konfigurierten Empfänger erstellen. Übersichtsberichte enthalten eine Zusammenfassung von Statistiken zu periodischen Aktivitäten, wie sie von GFI EndPointSecurity erkannt wurden.

Warnungsempfänger sind weder Active Directory (AD)-Benutzer und/oder Benutzergruppen. Sie stellen von GFI EndPointSecurity erstellte Profilkonten dar, die die Kontaktdaten der Benutzer enthalten, die Warnmeldungen erhalten sollen. Warnungsempfänger sollten vor der Warnmeldungskonfiguration erstellt werden. Weitere Informationen finden Sie unter Konfigurieren der Warnungsempfänger (page 127).

So konfigurieren Sie Übersichtsberichte:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

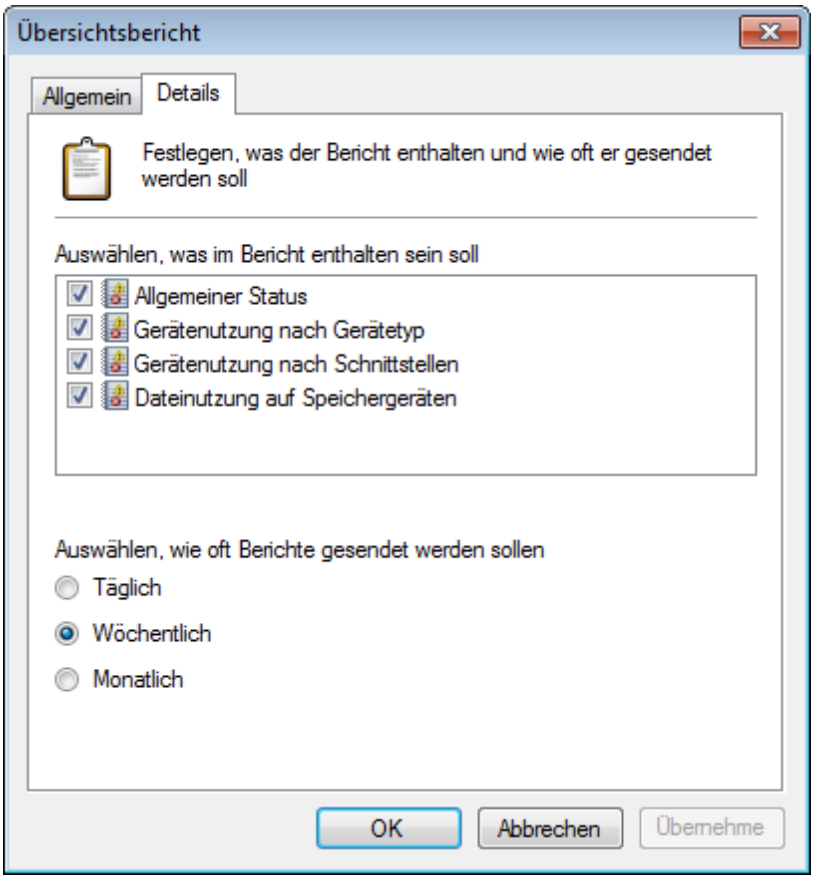
2. Klicken Sie unter **Konfigurieren** auf **Warnoptionen**, und klicken im rechten Bereich auf **Übersichtsbericht konfigurieren**.



Screenshot 92: Optionen für Übersichtsbericht - Registerkarte „Allgemein“

3. Aktivieren/Deaktivieren Sie im Dialogfeld **Übersichtsbericht** auf der Registerkarte **Allgemein** die bevorzugte Warnmethode.

4. Klicken Sie für jede ausgewählte Warnmeldung auf **Konfigurieren**, um Benutzer/Gruppe(n) als Empfänger anzugeben.



Screenshot 93: Optionen für Übersichtsbericht - Registerkarte „Details“

5. Klicken Sie auf die Registerkarte **Details**, um die im Übersichtsbericht zu berücksichtigenden Berichtsinhalte zu aktivieren bzw. deaktivieren.

6. Legen Sie die Häufigkeit des Berichts fest, indem Sie **Täglich, Wöchentlich** oder **Monatlich** auswählen.

7. Klicken Sie auf **Übernehmen** und **OK**.

10 Verwalten des Datenbank-Backends

In diesem Kapitel erhalten Sie Informationen zur Verwaltung und Wartung der Datenbank, in der die von GFI EndPointSecurity gesammelten Daten gespeichert werden. Nach der Installation von GFI EndPointSecurity können Sie zwischen folgenden Optionen wählen:

» Sie können eine Instanz von Microsoft SQL Server Express Edition herunterladen und installieren, um automatisch eine Datenbank für GFI EndPointSecurity zu erstellen. Dies kann über den **Schnellstart-Assistenten** erfolgen.

» Sie können eine Verbindung mit einem vorhandenen Microsoft SQL Server herstellen und entweder eine vorhandene Datenbank verwenden oder eine neue erstellen. Dies kann über den **Schnellstart-Assistenten** oder die untergeordneten Registerkarten **Allgemeiner Status** oder **Optionen** erfolgen.

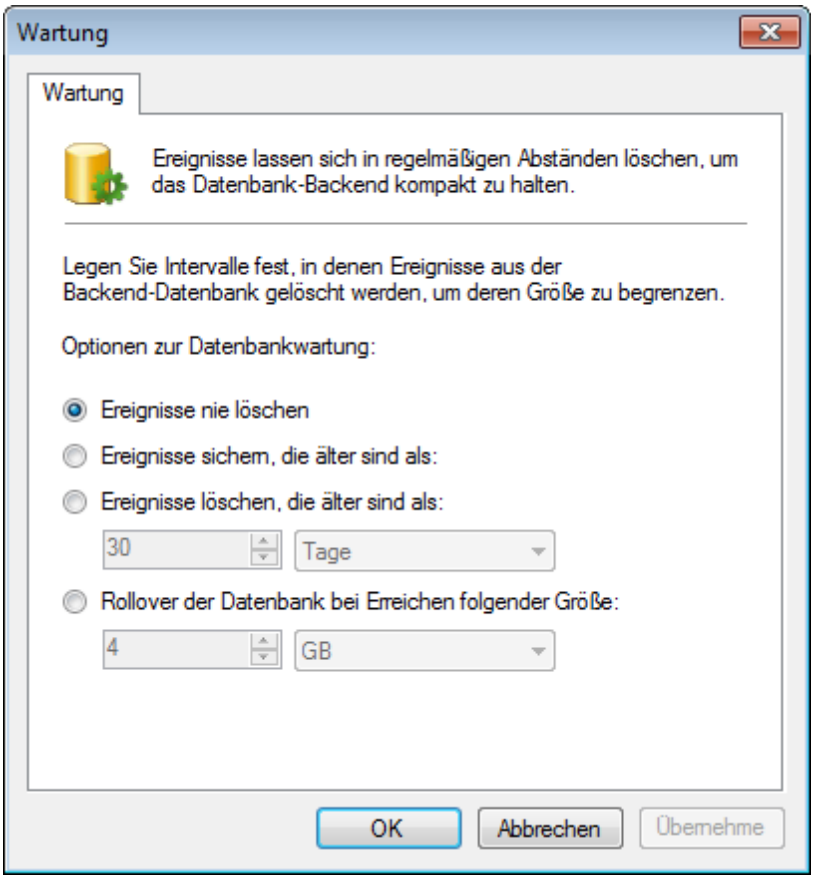
Themen in diesem Kapitel

10.1 Warten des Datenbank-Backends

Die Datenbank muss regelmäßig gewartet werden, um weiterhin effizient nutzbar zu sein. GFI EndPointSecurity bietet die Möglichkeit, Parameter, mit denen sich die automatische Wartung des Datenbank-Backends steuern lässt, zu konfigurieren.

So konfigurieren Sie die Wartung des Datenbank-Backends:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.
2. Wählen Sie unter **Konfigurieren** die Option **Datenbank-Backend**.
3. Klicken Sie im rechten Bereich auf **Datenbankwartung**.



Screenshot 94: Wartungsoptionen

4. Konfigurieren Sie im Dialogfeld **Wartung**, wie oft Ereignisse aus dem Datenbank-Backend gelöscht werden. Wählen Sie eine der unten beschriebenen Optionen:

Tabelle 13: Datenbank-Wartungsoptionen

Option	Beschreibung
Ereignisse nie löschen	Alle Ereignisse in Datenbank-Backend aufbewahren, ohne alte Ereignisse zu löschen **Hinweis** Stellen Sie sicher, dass alte Datensätze manuell gelöscht werden, um Leistungseinbußen bei GFI EndPointSecurity zu vermeiden.
Ereignisse sichern, die älter sind als	Geben Sie bei dieser Option an, wie lange Ereignisse zurückliegen müssen, bevor sie in einer separaten Datenbank gesichert werden.
Ereignisse löschen, die älter sind als:	Geben Sie bei dieser Option an, wie lange Ereignisse zurückliegen müssen, bevor sie gelöscht werden.
Rollover der Datenbank bei Erreichen folgender Größe	Geben Sie an, wie groß die Datenbank maximal werden darf, bevor GFI EndPointSecurity automatisch zu einer neuen Datenbank wechselt.

5. Klicken Sie auf **Übernehmen** und **OK**.

Hinweis

Da die Größe der Datenbank bei Microsoft SQL Express 2005 auf 4 GB und bei Microsoft SQL Express 2008 R2 auf 10 GB begrenzt ist, empfiehlt sich die Verwendung der Rollover-Option. Weitere Informationen zur Microsoft SQL Server-Edition und Engine-Spezifikationen finden Sie unter http://go.gfi.com/?pageid=ESEC_SqlSpecs

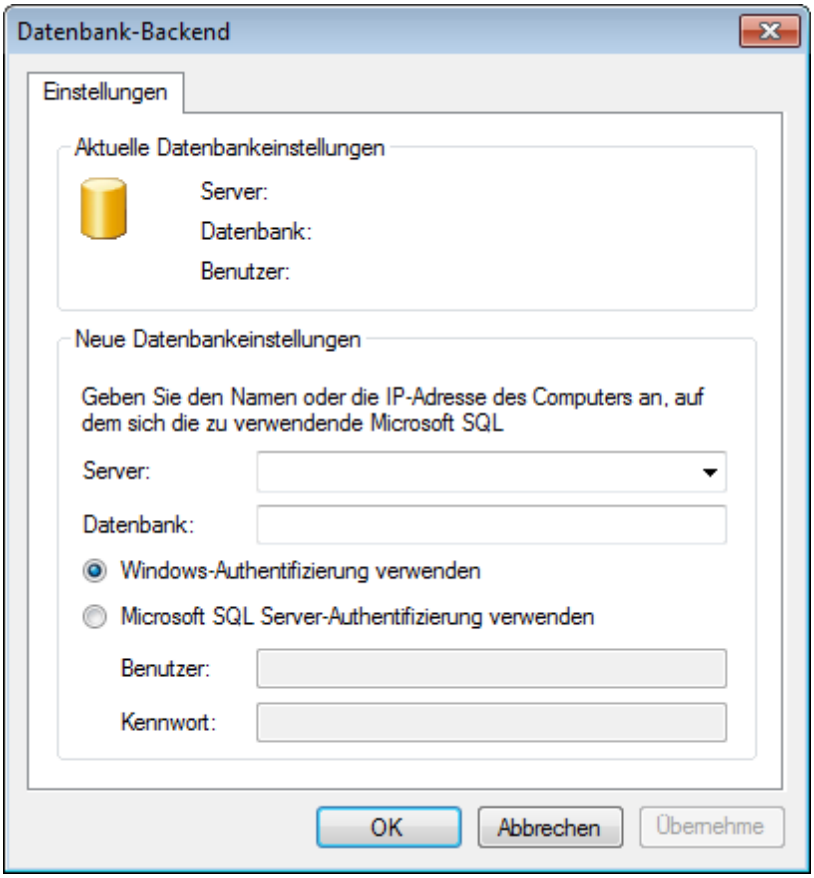
10.2 Verwenden einer vorhandenen SQL Server-Instanz

So stellen Sie eine Verbindung zu einer vorhandenen SQL Server-Instanz her:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

2. Wählen Sie unter **Konfigurieren** die Option **Datenbank-Backend**.

3. Klicken Sie im rechten Bereich auf **Datenbank-Backend ändern**.



Screenshot 95: Datenbank-Backend ändern

4. Wählen Sie aus dem Dropdown-Menü **Server** den gewünschten SQL Server aus.

5. Geben Sie im Textfeld **Datenbank** den Namen der Datenbank an.

6. Wählen Sie den Authentifizierungsmodus aus, und geben Sie bei Bedarf die Anmeldeinformationen an.

7. Klicken Sie auf **Übernehmen** und **OK**.

11 Warnoptionen

Dieses Kapitel enthält Informationen zur Konfiguration der Warnoptionen und Warnungsempfänger für GFI EndPointSecurity. Warnungen sind ein wichtiger Bestandteil von GFI EndPointSecurity, helfen Sie doch, Korrekturmaßnahmen zu ergreifen, sobald eine Bedrohung erkannt wird.

Themen in diesem Kapitel

11.1 Konfigurieren der Warnoptionen

Mit GFI EndPointSecurity können Sie folgende Warnoptionen konfigurieren:

» Mailserver-Einstellungen, Absenderdetails und die E-Mail-Nachricht, die für E-Mail-Warnungen verwendet werden,

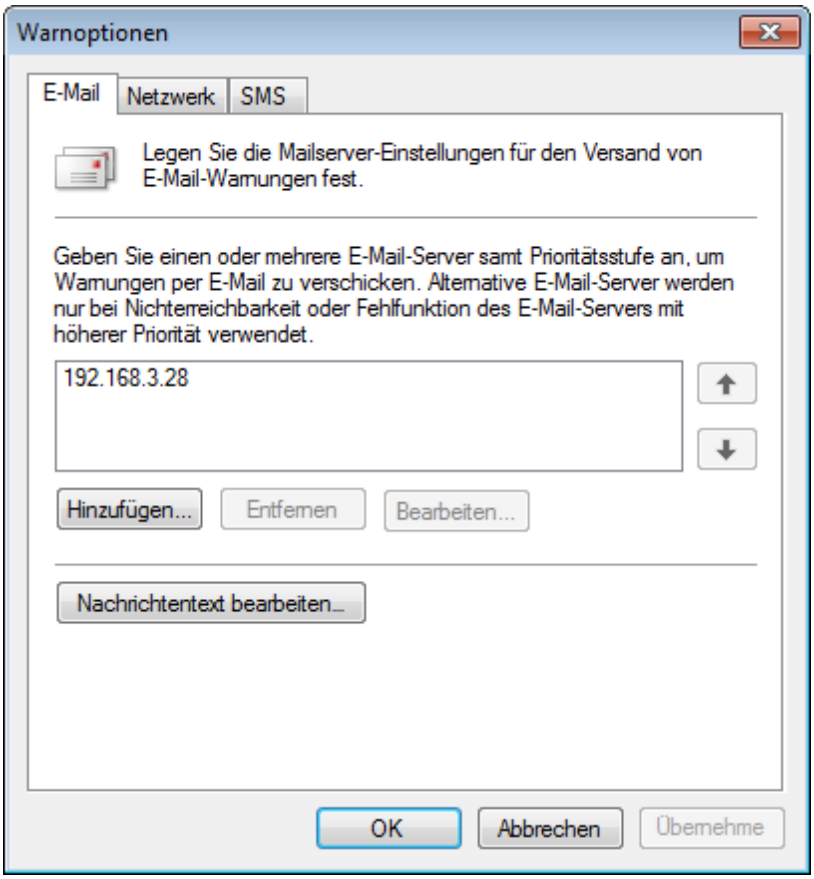
» Netzwerknachricht, die bei Netzwerkwarnungen gesendet wird,

» SMS-Gateway und SMS-Nachricht zum Senden von SMS-Warnungen.

So konfigurieren Sie Warnoptionen:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

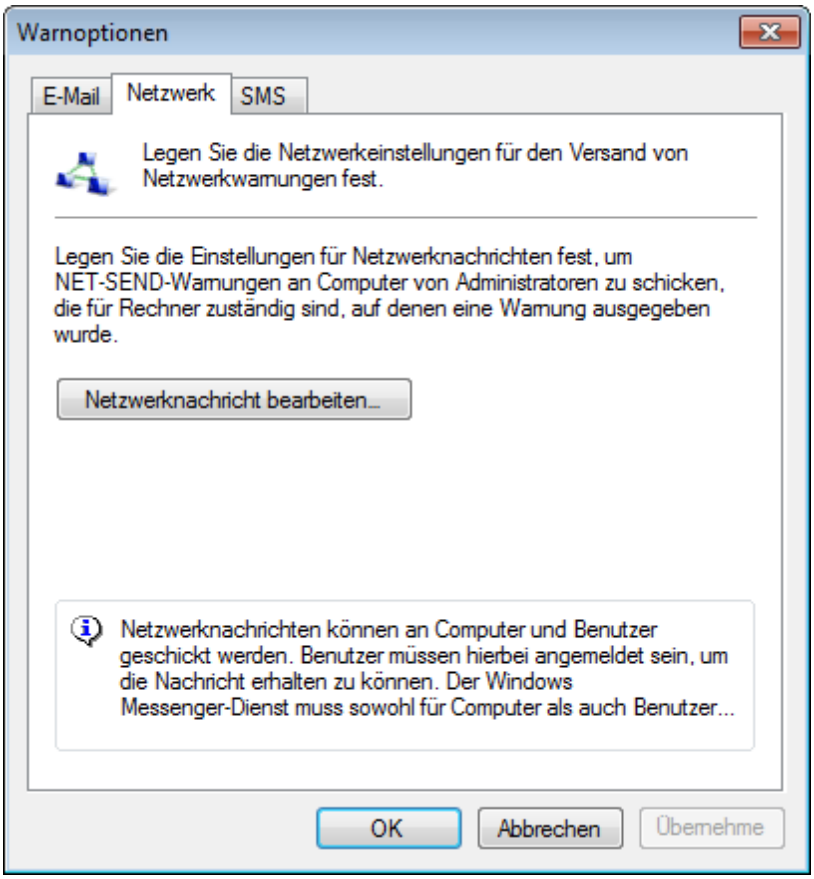
2. Klicken Sie unter **Konfigurieren** mit der rechten Maustaste auf den Knoten **Warnoptionen**, und wählen Sie **Warnoptionen bearbeiten...**.



Screenshot 96: Warnoptionen - Registerkarte „E-Mail“

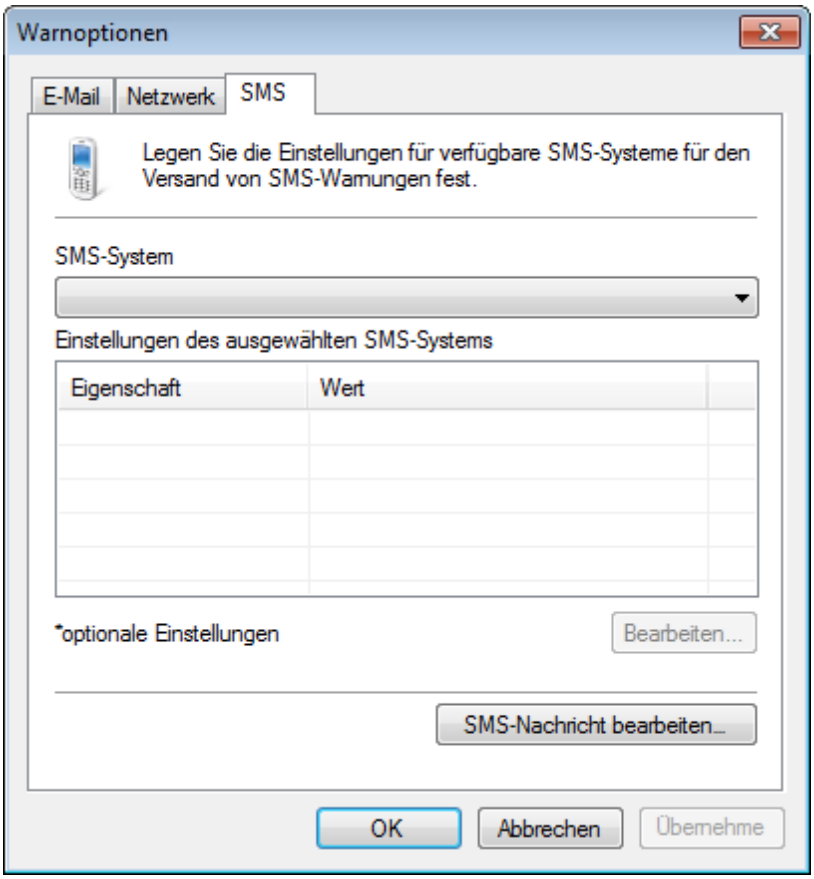
3. Klicken Sie auf der Registerkarte **E-Mail** auf **Hinzufügen...**, um die Einstellungen für den Mailserver anzugeben. Klicken Sie auf **OK**, um das Dialogfeld **Mailserver-Eigenschaften** zu schließen.

4. Um die E-Mail-Nachricht zu bearbeiten, klicken Sie auf **Nachrichtentext bearbeiten...**, ändern Sie die Felder **Betreff** und **Nachricht**, und klicken Sie auf **Speichern**.



Screenshot 97: Warnoptionen - Registerkarte „Netzwerk“

5. Klicken Sie auf die Registerkarte **Netzwerk > Netzwerknachricht bearbeiten...**, um die Netzwerknachricht zu bearbeiten. Klicken Sie auf **Speichern**.



Screenshot 98: Warnoptionen - Registerkarte „SMS“

6. Klicken Sie auf die Registerkarte **SMS**, und wählen Sie aus dem Dropdown-Menü **SMS-System auswählen** das zu verwendende SMS-Gateway aus. Unterstützte SMS-Systeme sind:

- Integrierter GSM SMS-Server
- GFI FaxMaker-SMS-Gateway
- E-Mail-zu-SMS-Gateway Clickatell
- Allgemeines SMS-Anbieter-Gateway.

7. Markieren Sie im Bereich **Einstellungen des ausgewählten SMS-Systems** die zu konfigurierende Eigenschaft, und klicken Sie auf **Bearbeiten**. Wiederholen Sie diesen Schritt für jede SMS-Systemeigenschaft, die Sie ändern möchten.

8. Klicken Sie zum Bearbeiten des Betreffs und der Nachricht auf **SMS-Nachricht bearbeiten...**. Klicken Sie auf **Speichern**.

9. Klicken Sie auf **OK**.

11.2 Konfigurieren des Administratorkontos für Warnungen

GFI EndPointSecurity gibt Ihnen die Möglichkeit, Profilkonten zu konfigurieren, um Kontaktdetails von Benutzern zu speichern, die E-Mail-Warnungen, Netzwerknachrichten und SMS-Nachrichten erhalten sollen. Nach der Installation erstellt GFI EndPointSecurity automatisch ein Administratorkonto für Warnungen. Warnadministratoren sind keine Active Directory (AD)-Benutzer und/oder -Benutzergruppen.

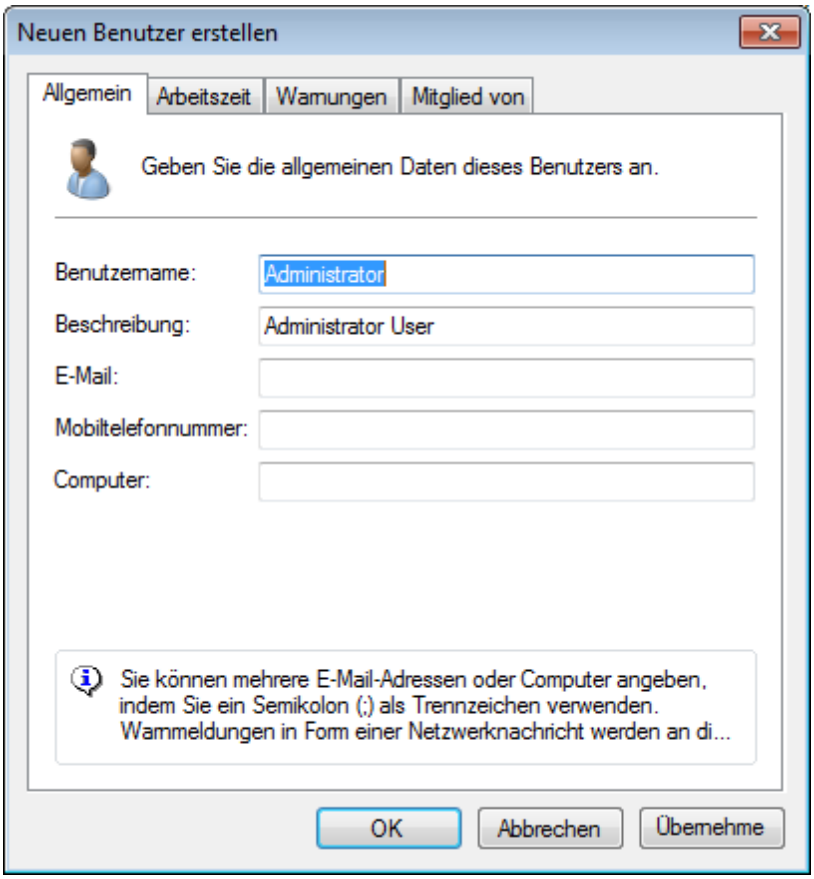
GFI EndPointSecurity erstellt nach der Installation automatisch das Konto EndPointSecurityAdministrator (für Warnungen) und legt es als Mitglied der Benachrichtigungsgruppe EndPointSecurityAdministratoren fest.

So konfigurieren Sie das GFI EndPointSecurityAdministrator-Konto:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

2. Klicken Sie unter **Konfigurieren** auf **Warnoptionen > Benutzer**.

3. Klicken Sie auf der rechten Seite mit der rechten Maustaste auf **EndPointSecurityAdministrator**, und wählen Sie **Eigenschaften** aus.

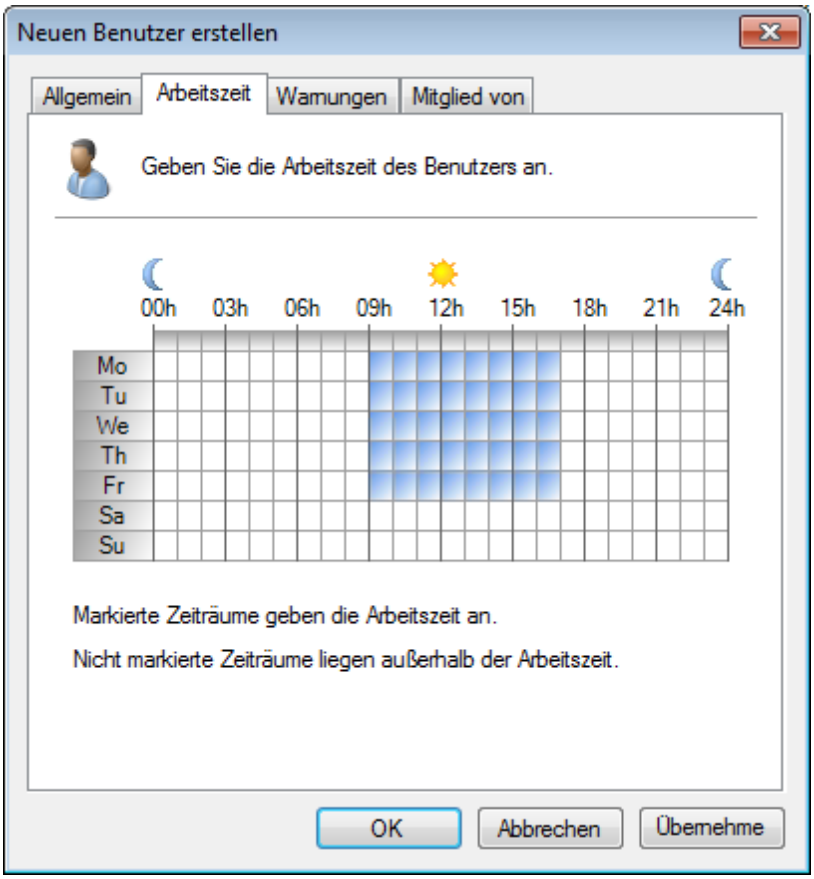


Screenshot 99: EndPointSecurityAdministrator-Eigenschaftsoptionen - Registerkarte „Allgemein“

4. Geben Sie auf der Registerkarte „Allgemein“ die folgenden Details ein:

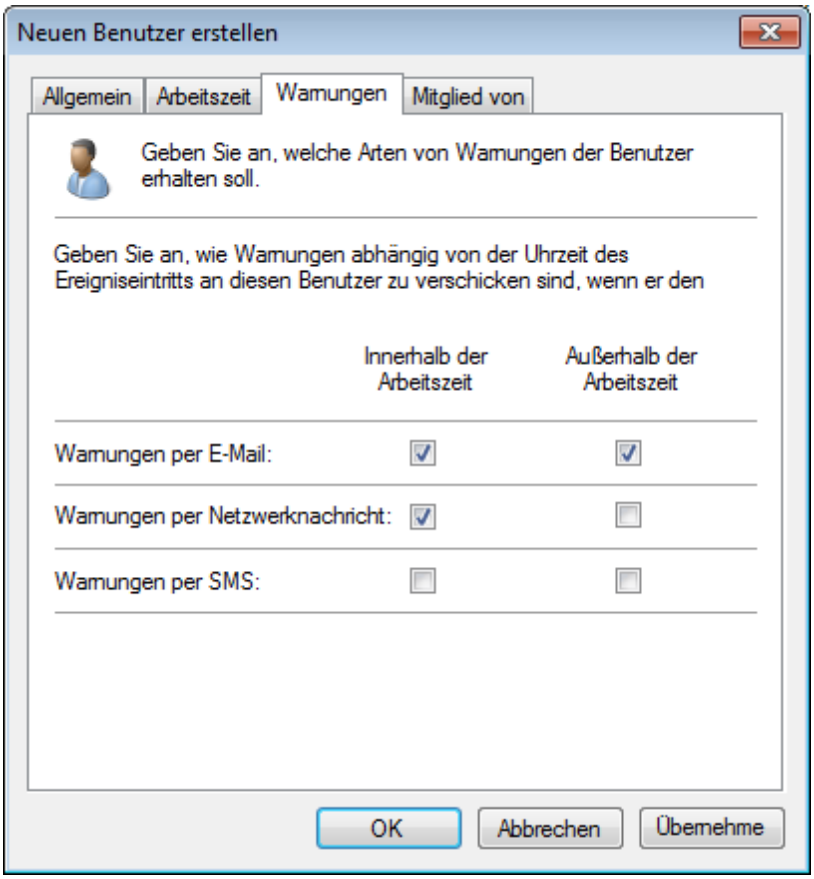
- Kontobenutzername
- Kontobeschreibung
- E-Mail-Adresse
- Mobiltelefonnummer
- Computer (Netzwerknachrichten werden an die angegebenen Computer gesendet)

> **Hinweis**
>
> Es können mehrere E-Mail-Adressen und Computernamen/IP-Adressen angegeben werden. Diese müssen dann jeweils mit einem Semikolon (;) von einander getrennt sein.



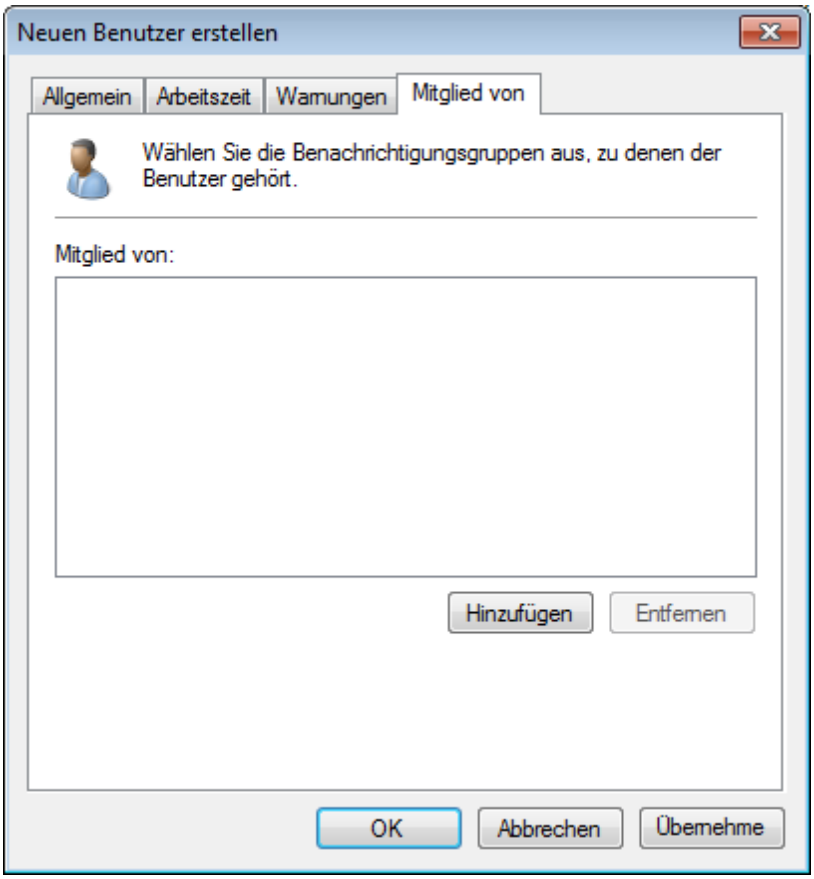
Screenshot 100: EndPointSecurityAdministrator-Eigenschaftsoptionen - Registerkarte „Arbeitszeit“

5. Klicken Sie auf die Registerkarte **Arbeitszeit** , und markieren Sie die Kernarbeitszeit des Benutzers. Markierte Zeiträume geben die Arbeitszeit an.



Screenshot 101: EndPointSecurityAdministrator-Eigenschaftsoptionen - Registerkarte „Warnungen“

6. Klicken Sie auf die Registerkarte **Warnungen**, und wählen Sie die zu sendenden Warnungen sowie den Zeitpunkt für den Sendevorgang aus.



Screenshot 102: EndPointSecurityAdministrator-Eigenschaftsoptionen - Registerkarte „Mitglied von“

7. Klicken Sie auf die Registerkarte **Mitglied von**, und klicken Sie dann auf **Hinzufügen**, um den Benutzer Benachrichtigungsgruppen hinzuzufügen.

8. Klicken Sie auf **Übernehmen** und **OK**.

11.3 Konfigurieren der Warnungsempfänger

GFI EndPointSecurity gibt Ihnen die Möglichkeit, andere Profilkonten als das GFI EndPointSecurity-Administratorkonto zu konfigurieren, um Kontaktdetails von Benutzern zu speichern, die E-Mail-Warnungen, Netzwerknachrichten und SMS-Nachrichten erhalten sollen.

Warnungsempfänger sind weder Active Directory (AD)-Benutzer und/oder Benutzergruppen. Sie stellen von GFI EndPointSecurity erstellte Profilkonten dar, die die Kontaktdaten der Benutzer enthalten, die Warnmeldungen erhalten sollen.

» Erstellen von Warnungsempfängern

» Bearbeiten der Warnungsempfängereigenschaften

» Löschen von Warnungsempfängern

11.3.1 Erstellen von Warnungsempfängern

So erstellen Sie einen neuen Warnungsempfänger:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

2. Klicken Sie unter **Konfigurieren** auf **Warnoptionen > Benutzer**.

3. Klicken Sie im linken Bereich auf **Benutzer erstellen...**.

4. Weitere Informationen zum Konfigurieren der Einstellungen zum Erstellen eines neuen Empfängers finden Sie unter Konfigurieren des Administratorkontos für Warnungen.

11.3.2 Bearbeiten der Warnungsempfängereigenschaften

So bearbeiten Sie Warnungsempfängereigenschaften:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

2. Klicken Sie unter **Konfigurieren** auf **Warnoptionen > Benutzer**.

3. Klicken Sie auf der rechten Seite mit der rechten Maustaste auf den zu bearbeitenden Benutzer, und wählen Sie **Eigenschaften** aus.

4. Weitere Informationen zum Konfigurieren der Einstellungen zum Bearbeiten eines Empfängers finden Sie unter Konfigurieren des Administratorkontos für Warnungen.

11.3.3 Löschen von Warnungsempfängern

So löschen Sie einen Warnungsempfänger:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

2. Klicken Sie unter **Konfigurieren** auf **Warnoptionen > Benutzer**.

3. Klicken Sie auf der rechten Seite mit der rechten Maustaste auf den zu bearbeitenden Benutzer, und wählen Sie **Löschen** aus.

4. Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.

11.4 Konfigurieren der Gruppen von Warnungsempfängern

GFI EndPointSecurity ermöglicht die Einteilung Ihrer Warnungsempfänger in Gruppen, um die Verwaltung der Warnungsempfänger zu vereinfachen.

» Erstellen der Gruppen von Warnungsempfängern

» Bearbeiten von Eigenschaften einer Gruppe von Warnungsempfängern

» Löschen der Gruppen von Warnungsempfängern

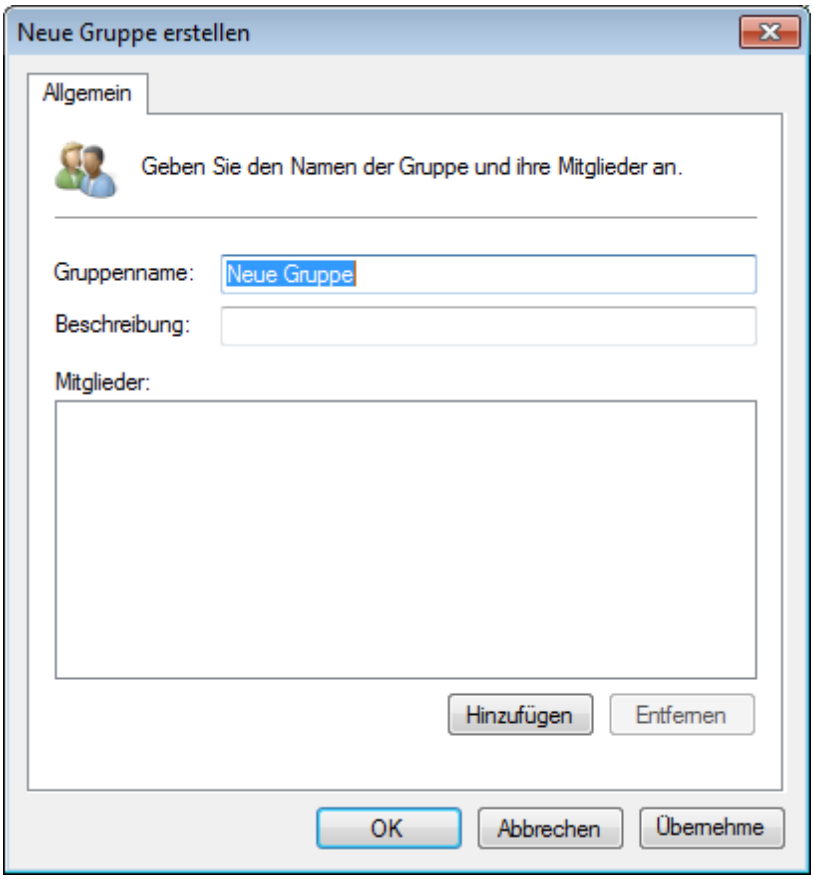
11.4.1 Erstellen der Gruppen von Warnungsempfängern

So erstellen Sie eine neue Gruppe von Warnungsempfängern:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

2. Klicken Sie auf **Warnoptionen > Gruppen**.

3. Klicken Sie auf der linken Seite auf **Gruppe erstellen...**.



Screenshot 103: Optionen für das Erstellen neuer Gruppen

4. Geben Sie im Dialogfeld **Neue Gruppe erstellen** den Gruppennamen und eine optionale Beschreibung ein.

5. Klicken Sie auf **Hinzufügen**, um den/die zur Benachrichtigungsgruppe gehörenden Benutzer auszuwählen, und klicken Sie anschließend auf **OK**.

11.4.2 Bearbeiten von Eigenschaften einer Gruppe von Warnungsempfängern

So bearbeiten Sie die Eigenschaften für eine Gruppe von Warnungsempfängern:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

2. Klicken Sie auf **Warnoptionen > Gruppen**.

3. Klicken Sie auf der rechten Seite mit der rechten Maustaste auf die zu bearbeitenden Gruppe, und wählen Sie **Eigenschaften** aus.

4. Weitere Informationen zum Bearbeiten von Gruppeneinstellungen finden Sie unter Erstellen der Gruppen von Warnungsempfängern.

11.4.3 Löschen der Gruppen von Warnungsempfängern

So löschen Sie eine Gruppe von Warnungsempfängern:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

2. Klicken Sie auf **Warnoptionen > Gruppen**.

3. Klicken Sie auf der rechten Seite mit der rechten Maustaste auf die zu löschende Gruppe, und wählen Sie **Löschen** aus.

4. Klicken Sie auf **Ja**, um das Löschen der Gruppe zu bestätigen.

12 Konfigurieren von GFI EndPointSecurity

Mit GFI EndPointSecurity können Sie die Computer konfigurieren, auf denen Sie Updates installieren und Benutzermeldungen anzeigen möchten.

Themen in diesem Kapitel

12.1 Konfigurieren von erweiterten Optionen

Mit GFI EndPointSecurity können Sie die folgenden erweiterten Agentenoptionen konfigurieren:

» TCP/IP-Port für die Hauptkommunikation

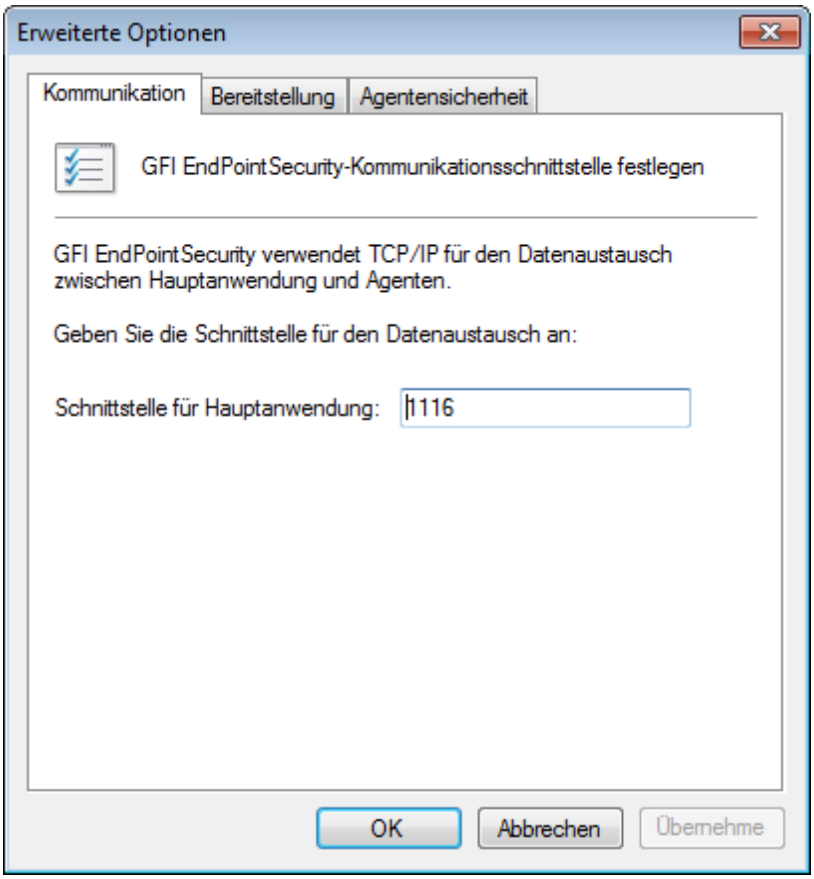
» Bereitstellungsoptionen

» Kennwort zur Agentenkontrolle.

So konfigurieren Sie die erweiterten Optionen:

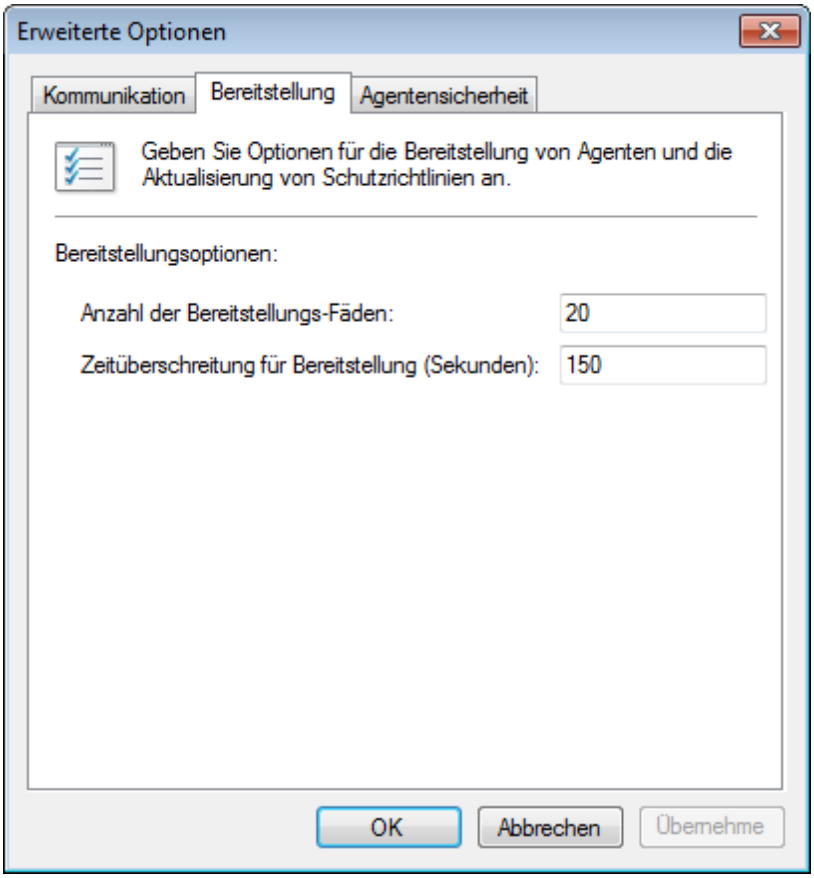
1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

2. Klicken Sie unter **Konfigurieren** mit der rechten Maustaste auf den Knoten **Erweitere Optionen**, und wählen Sie **Erweiterte Optionen ändern...**.



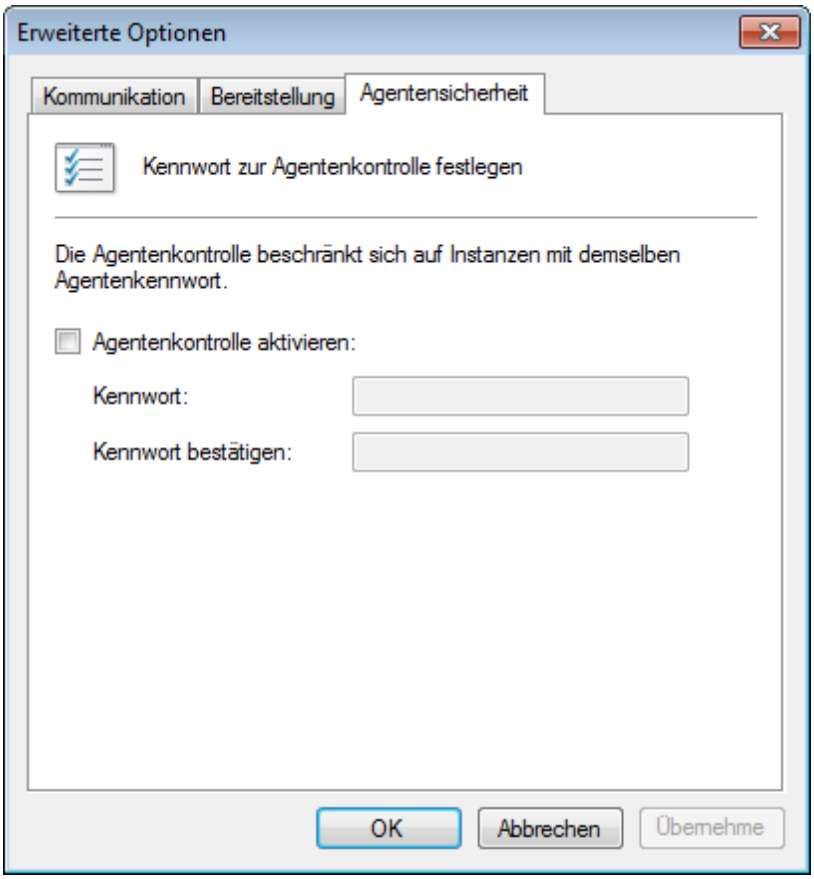
Screenshot 104: Erweiterte Optionen - Registerkarte „Kommunikation“

3. Geben Sie auf der Registerkarte **Kommunikation** die für die Kommunikation zwischen GFI EndPointSecurity und GFI EndPointSecurity-Agenten erforderliche TCP/IP-Portnummer ein. Standardmäßig ist Port **1116** angegeben.



Screenshot 105: Erweiterte Optionen - Registerkarte „Bereitstellung“

4. Klicken Sie auf die Registerkarte **Bereitstellung**, und geben Sie unter **Anzahl der Bereitstellungs-Threads** und **Zeitüberschreitung für Bereitstellung (Sekunden)** die erforderlichen Werte ein.



Screenshot 106: Erweiterte Optionen - Registerkarte „Agentensicherheit“

5. Klicken Sie auf die Registerkarte **Agentensicherheit**, und aktivieren bzw. deaktivieren Sie die Option **Agentenkontrolle aktivieren**. Weisen Sie mithilfe dieser Option allen im Netzwerk bereitgestellten GFI EndPointSecurity-Agenten bestimmte Anmeldeinformationen zu.

6. Klicken Sie auf **Übernehmen** und **OK**.

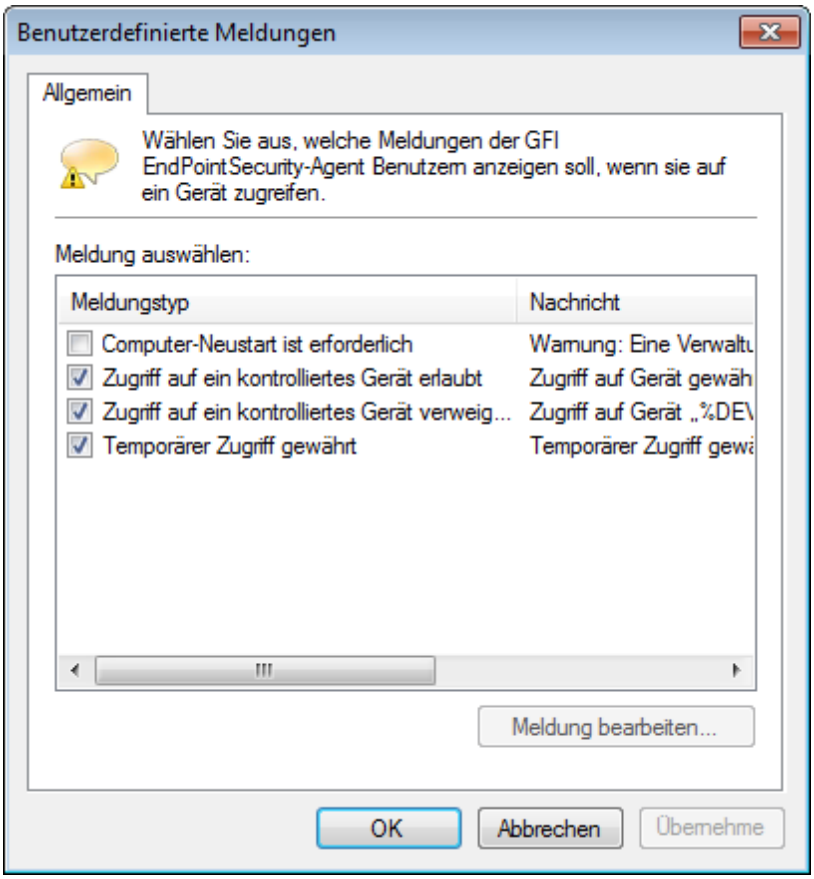
12.2 Konfigurieren von Benutzermeldungen

In GFI EndPointSecurity haben Sie die Möglichkeit, die von den GFI EndPointSecurity-Agenten auf den kontrollierten Computern beim Zugriff auf Geräte angezeigten Meldungen anzupassen.

So passen Sie Benutzermeldungen an:

1. Klicken Sie auf die Registerkarte **Konfiguration** > untergeordnete Registerkarte **Optionen**.

2. Klicken Sie unter „Konfigurieren“ mit der rechten Maustaste auf „Benutzerdefinierte Meldungen“, und wählen Sie „Benutzermeldungen anpassen“ aus.



Screenshot 107: Optionen im Dialogfeld „Benutzerdefinierte Meldungen“

3. Aktivieren bzw. Deaktivieren Sie die anzupassenden Meldungstypen.

4. Klicken Sie für jede aktivierte Meldung auf **Meldung bearbeiten…**, um sie nach Bedarf zu ändern. Klicken Sie anschließend auf **Speichern**. Wiederholen Sie diesen Schritt für jede zu ändernde Meldung.

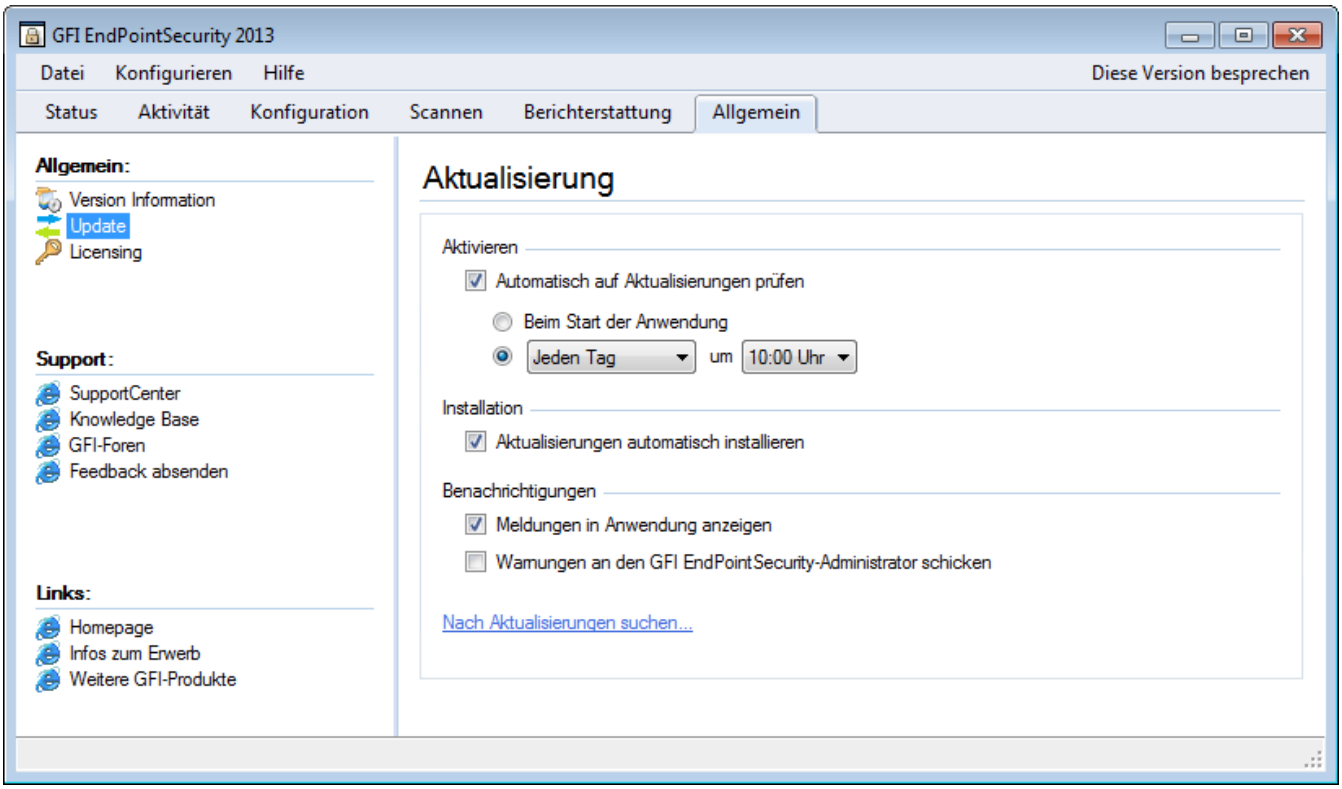
5. Klicken Sie auf **Übernehmen** und **OK**..

12.3 Konfigurieren von GFI EndPointSecurity-Aktualisierungen

GFI EndPointSecurity kann so konfiguriert werden, dass Aktualisierungen automatisch nach einem Zeitplan oder beim Starten heruntergeladen und installiert werden. So konfigurieren Sie Aktualisierungen:

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

2. Klicken Sie im linken Bereich auf **Aktualisierungen**.



Screenshot 108: Registerkarte „Allgemein“ - Aktualisierungen

3. Konfigurieren Sie im rechten Bereich die nachfolgend beschriebenen Optionen:

Tabelle 14: Aktualisierungsoptionen

Option	Beschreibung
Automatisch auf Aktualisierungen prüfen	Stellt eine Verbindung zu den GFI-Aktualisierungsservern her und lädt Produktaktualisierungen automatisch herunter. Wählen Sie „Beim Starten der Anwendung“, oder geben Sie einen Tag und eine Uhrzeit ein, wenn eine Prüfung stattfinden und die Aktualisierungen heruntergeladen werden sollen.
Aktualisierungen automatisch installieren	Eine gefundene Aktualisierung wird von GFI EndPointSecurity heruntergeladen und automatisch installiert.
Meldungen in Anwendung anzeigen	Bei einer gefundenen und installierten Aktualisierung wird in der GFI EndPointSecurity-Anwendung eine Meldung angezeigt.
Warnungen an GFI EndPointSecurity-Administrator senden	Bei einer gefundenen und installierten Aktualisierung wird eine E-Mail-Nachricht an den GFI EndPointSecurity-Administrator gesendet. Weitere Informationen finden Sie unter Konfigurieren des Administratorkontos für Warnungen (page 123).
Auf Aktualisierungen prüfen	Klicken Sie auf den Link, um das GFI EndPointSecurity-Aktualisierungsmodul sofort auszuführen und fehlende Aktualisierungen herunterzuladen sowie zu installieren.

13 Diverses

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

Themen in diesem Kapitel

13.1 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 109: 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.

13.2 Deinstallation von GFI EndPointSecurity

GFI EndPointSecurity ermöglicht die Deinstallation von GFI EndPointSecurity-Agenten und der GFI EndPointSecurity-Anwendung.

In diesem Kapitel werden folgenden Themen behandelt:

» Deinstallation von GFI EndpointSecurity-Agenten

» Deinstallation der GFI EndpointSecurity-Anwendung

Achtung

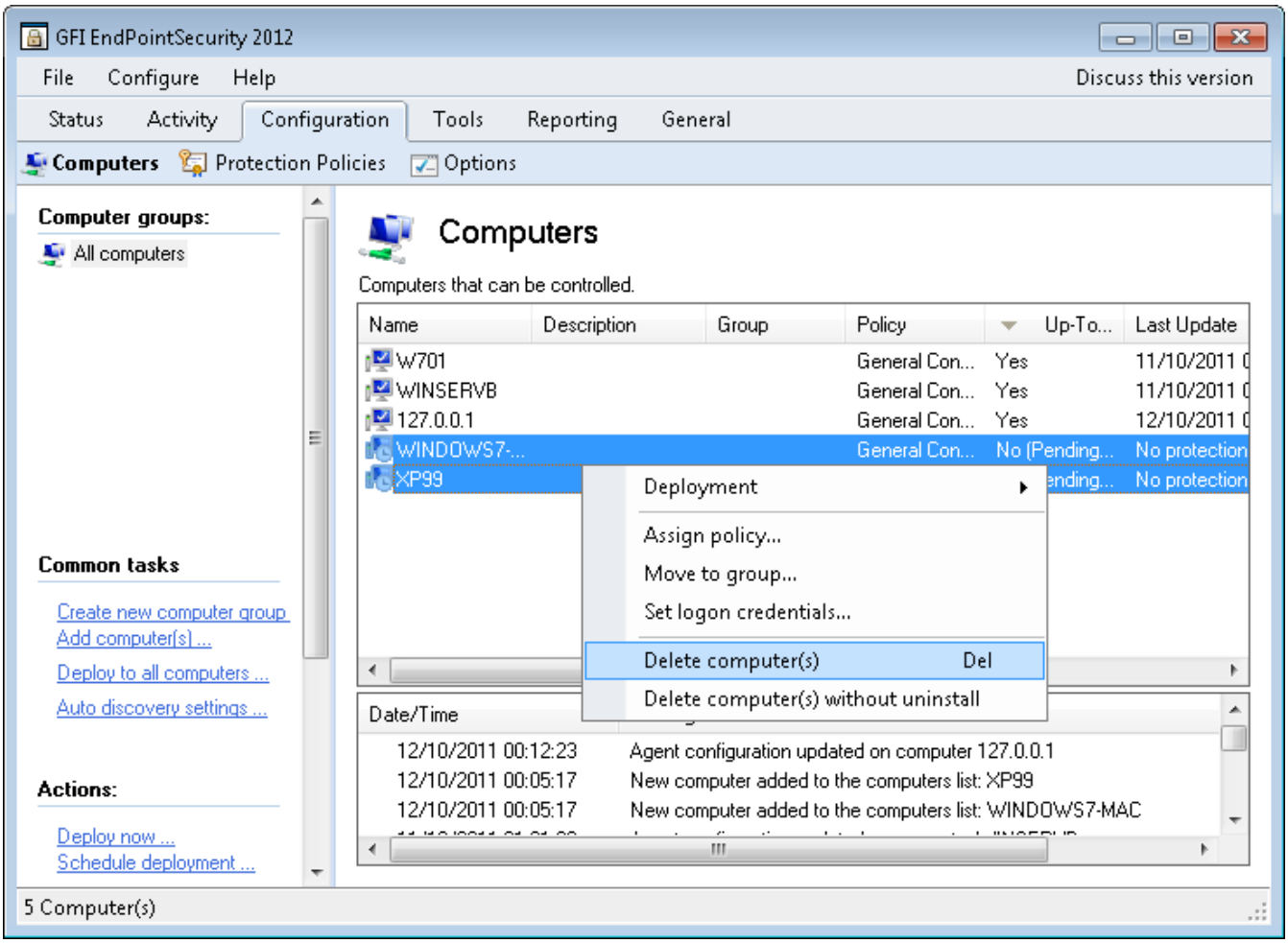
GFI EndPointSecurity-Agenten werden bei der Deinstallation der GFI EndPointSecurity-Anwendung nicht automatisch deinstalliert. Deinstallieren Sie zunächst die GFI EndPointSecurity-Agenten, bevor Sie die GFI EndPointSecurity-Anwendung deinstallieren.

13.2.1 Deinstallation von GFI EndPointSecurity-Agenten

So deinstallieren Sie einen GFI EndPointSecurity-Agenten:

1. Klicken Sie in der Verwaltungskonsole von GFI EndPointSecurity auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

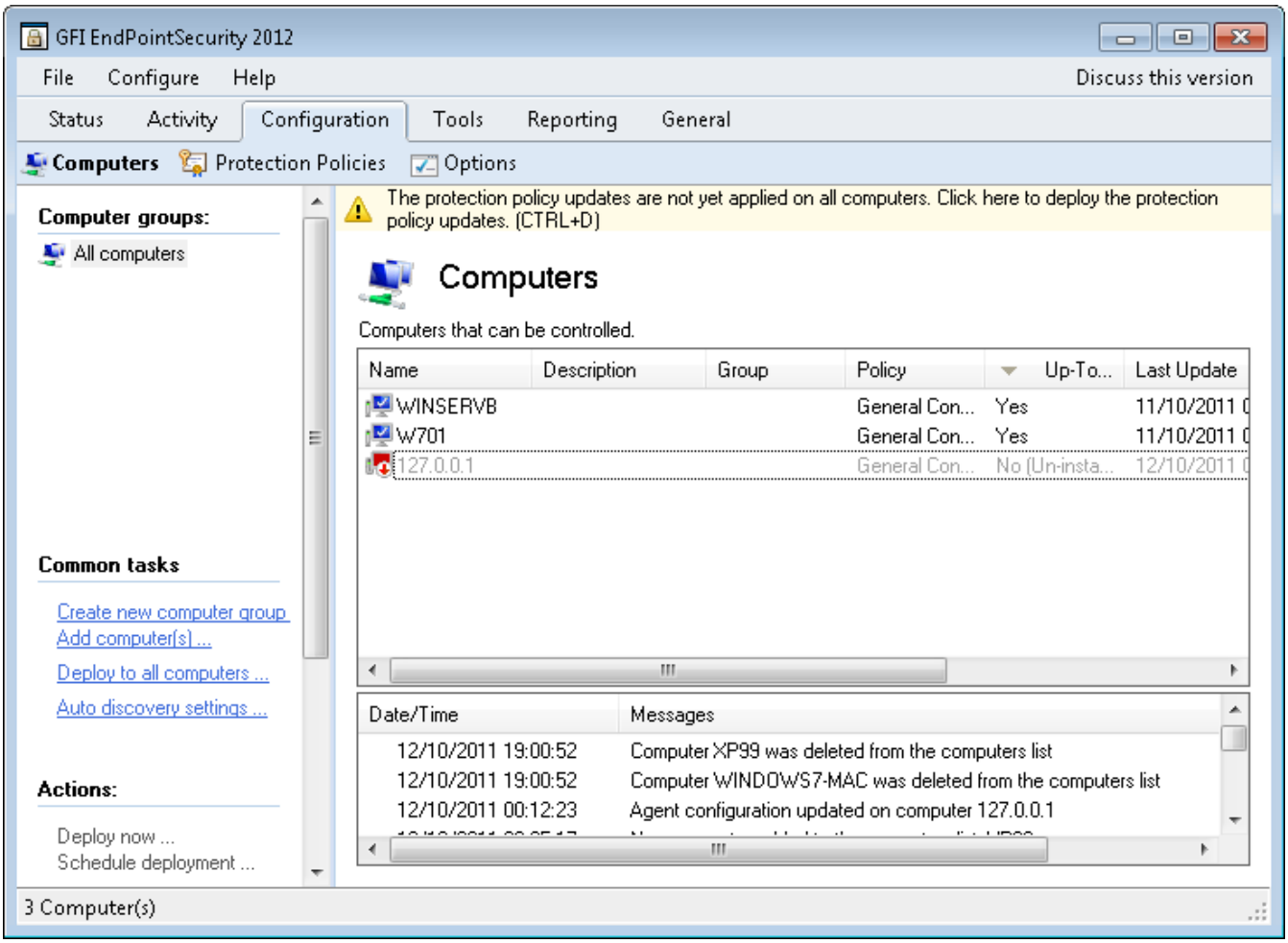


Screenshot 110: Untergeordnete Registerkarte „Computer“ - Computer löschen

3. Klicken Sie im rechten Fenster mit der rechten Maustaste auf den kontrollierten Computer, den sie löschen möchten. Folgende Optionen stehen im Kontextmenü zur Verfügung:

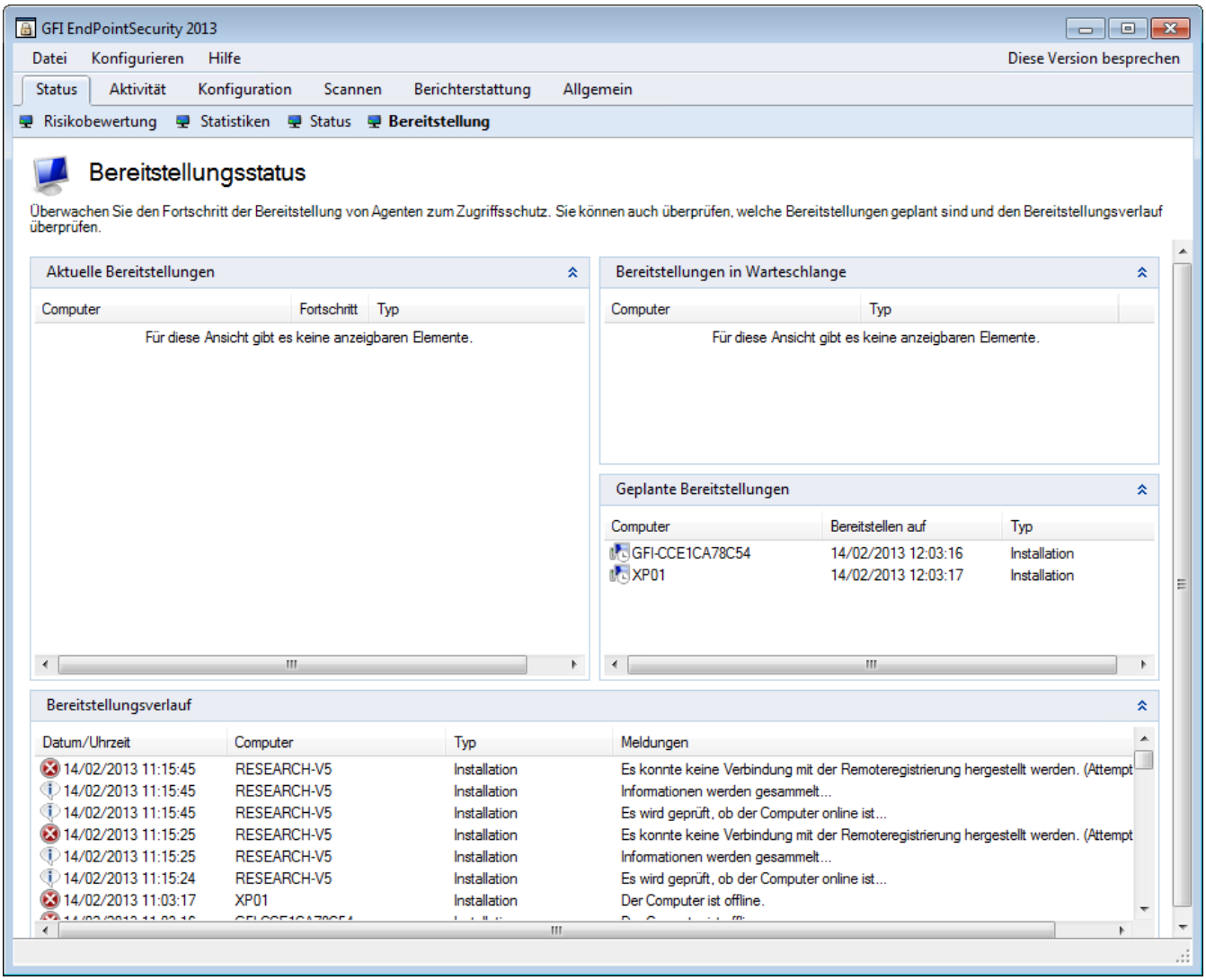
Löschen von Computern	
Löschen von Computern - **mit** Deinstallation	GFI EndPointSecurity stellt zu aktualisierende Schutzrichtlinien bereit und deinstalliert den Agenten.
Löschen von Computern - **ohne** Deinstallation	GFI EndPointSecurity stellt zu aktualisierende Schutzrichtlinien bereit und und entfernt die entsprechenden Computereinträge aus der Computerliste. Der Agent bleibt jedoch auf dem kontrollierten Computer installiert. Diese Option ist geeignet, wenn der kontrollierte Computer aus dem Netzwerk entfernt wurde und die GFI EndPointSecurity-Anwendung keine Verbindung zu diesem Computer herstellen kann, um den Agenten zu deinstallieren.

4. Klicken Sie auf **Ja**, um den Löschvorgang des ausgewählten Computers zu bestätigen.



Screenshot 111: Untergeordnete Registerkarte „Computer“ - ausstehende Deinstallation

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



Screenshot 112: Untergeordnete Registerkarte „Bereitstellung“

6. Prüfen Sie im Bereich **Bereitstellungsverlauf** den erfolgreichen Abschluss der Deinstallation vom kontrollierten Computer.

13.2.2 Deinstallation der GFI EndPointSecurity-Anwendung

So deinstallieren Sie die GFI EndPointSecurity-Anwendung:

> **Hinweis**
>
> Führen Sie das Deinstallationsprogramm als Administrator auf dem Computer aus.

1. Wählen Sie in der **Microsoft Windows-Systemsteuerung** die Optionen **Software** bzw. **Programme und Funktionen**.

2. Wählen Sie GFI EndPointSecurity aus.

3. Klicken Sie auf **Ändern**, um die Deinstallation der GFI EndPointSecurity-Anwendung zu starten.

4. Klicken Sie auf dem Willkommensbildschirm auf **Weiter**, um mit der Deinstallation fortzufahren.

Screenshot 113: Informationsmeldung zur Deinstallation

Hinweis

Wenn Agenten noch auf dem Computer installiert sind, werden Sie in einem Informationsdialog gefragt, ob Sie mit der Deinstallation fortfahren möchten (die Agenten bleiben auf dem Computer installiert und als verwaiste Agenten erhalten), oder ob Sie die Deinstallation abbrechen möchten. Weitere Informationen zur Deinstallation von Agenten finden Sie im Abschnitt Deinstallation von GFI EndPointSecurity-Agenten in diesem Kapitel.

5. Wählen Sie die Option **Deinstallieren, aber Konfigurationsdateien beibehalten** oder **Vollständig deinstallieren**, und klicken Sie zum Fortfahren auf **Weiter**.

6. Klicken Sie dann auf **Fertig stellen**, um die Deinstallation abzuschließen.

13.3 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.

14 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 15: 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.
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 114: 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 115: 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 116: 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 117: 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.

15 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.

16 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®