

NETOP™

ProtectOn™ PRO

Endpoint Protection Software

Benutzerhandbuch

Version 1.1



Copyright© 1981-2010 Netop Business Solutions A/S. Alle Rechte vorbehalten.
Teile unter Lizenz Dritter.

Senden Sie Ihre Anmerkungen und Kommentare bitte an::

Netop Business Solutions A/S

Bregnerodvej 127

DK- 3460 Birkerod

Dänemark

Fax: Int +45 45 90 25 26

E-mail: info@netop.com

Internet: www.netop.com

Netop™ ist eine Marke von Netop Business Solutions A/S. Alle anderen in diesem Dokument erwähnten Produkte sind Marken ihrer jeweiligen Hersteller. Netop Business Solutions A/S weist jedwede Verantwortung für Schäden, die sich direkt oder indirekt aus der Verwendung des vorliegenden Dokuments ergeben, von sich. Der Inhalt dieses Dokuments kann sich jederzeit ohne Vorankündigung ändern. Netop Business Solutions A/S behält das Urheberrecht an diesem Dokument.
Das Dokument ist optimiert für doppelseitiges Ausdrucken.

Inhalt

1 Netop ProtectOn Pro - Überblick.....	3
1.1 Einführung in Netop ProtectOn Pro	3
1.2 Funktionsweise von Netop ProtectOn Pro.....	4
1.3 Unterstützte Betriebssysteme	6
2 Konfigurations- und Verbindungseinstellungen.....	7
2.1 Servereinstellungen.....	7
2.2 Konsoleneinstellungen	10
2.3 Agenteinstellungen	11
2.4 Remoteinstallation des Agentmoduls.....	12
3 Netop ProtectOn Pro Konsole.....	14
3.1 Benutzeroberfläche der Konsole.....	14
3.2 Eine Netzwerkstruktur durchsuchen	15
3.3 Active Directory-Netzwerke verwalten.....	16
3.4 Details des Microsoft Windows Netzwerkcomputers anzeigen	17
3.5 Netzwerkcomputer fernstarten (WOL)	19
3.6 Remoteinstallation des Agentmoduls.....	20
3.7 Eine Remotesitzung auf einem Netzwerkcomputer öffnen.....	21
4 Gruppen erstellen.....	23
4.1 Eine Gruppe erstellen	23
4.2 Eine Gruppe umbenennen, kopieren oder löschen	23
5 Richtlinien definieren und übernehmen.....	25
5.1 Info über Richtlinien.....	25
5.2 Eine Richtlinie erstellen.....	29
5.3 Eine Richtlinie zum Festplattenschutz definieren	29
5.4 Eine Richtlinie zum Gerätezugriff definieren	30
5.5 Richtlinien zum Gerätezugriff.....	31
5.5.1 Zugriffsrechte pro Gerätetyp definieren.....	31
5.5.2 Zugriffsrechte pro Einzelgerät definieren.....	31
5.5.3 Zugriffsrechte für ein USB-Laufwerk definieren.....	32
5.5.4 Zugriffsrechte für ein WiFi-Gerät definieren.....	34
5.5.5 Inhalt einer Festplatte verbergen.....	34
5.5.6 Mit der USB-Datenbank arbeiten	35
5.5.7 Eine USB-Gerätekategorie zu einer Weißen Liste hinzufügen.....	35
5.5.8 Ein USB-Gerät zu einer Weißen Liste hinzufügen.....	36
5.6 Eine Webrichtlinie definieren	37
5.7 Eine Anwendungsrichtlinie definieren	37
5.8 Gültige Richtlinien für ein Gruppenmitglied anzeigen	37
5.9 Eine Richtlinie umbenennen, kopieren oder löschen.....	38
5.10 Registerkarten zu Richtlinien	38
5.10.1 Registerkarte Festplattenschutz.....	38
5.10.2 Registerkarte "Gerätezugriff".....	40

5.10.3 Registerkarte Internet.....	41
5.10.4 Registerkarte Anwendung.....	42
5.10.5 Registerkarte Zeitplan.....	43
5.10.6 Registerkarte Zugewiesen.....	43
6 Überlappende Richtlinien.....	44
6.1 Richtlinien zusammenführen.....	44
6.2 Richtlinien zum Festplattenschutz zusammenführen.....	46
6.3 Richtlinien zum Gerätezugriff zusammenführen.....	47
6.4 Webrichtlinien zusammenführen.....	58
6.5 Anwendungsrichtlinien zusammenführen.....	61
7 Remoteverwaltung.....	64
7.1 Info über Remoteverwaltung.....	64
7.2 Verwaltungsfenster.....	64
7.3 Laufwerke.....	66
7.4 Ereignisanzeige.....	66
7.5 Task-Manager.....	67
7.6 Registrierung.....	67
7.7 Dienste.....	67
7.8 Freigabeordner.....	69
7.9 Bestand.....	70
7.10 Befehlskonsole.....	70
7.11 Systemsteuerung.....	71
7.12 Lokale Benutzer und Gruppen.....	71
7.13 Drittanbieteranwendungen integrieren.....	74
7.14 Netop Sitzungen.....	75
Index.....	77

1 Netop ProtectOn Pro - Überblick

1.1 Einführung in Netop ProtectOn Pro

Netop ProtectOn Pro dient IT-Administratoren zur Verwaltung von Netzwerkcomputern, einschließlich Computern ohne feste Benutzer. Netzwerke mit vielen verschiedenen Benutzern finden sich beispielsweise in Schulen, Internetcafés und Hotels. IT-Administratoren von Computern, auf die von vielen verschiedenen Benutzern zugegriffen wird, sind in der Regel für die folgenden Aufgaben zuständig:

- Verhindern, dass Benutzer auf Netzwerkcomputern Software installieren und dadurch den freien Speicherplatz reduzieren
- Schutz der Daten vor versehentlicher oder vorsätzlicher Änderung sowie Schutz vor der Ausführung von böartigem Code
- Verhindern, dass unangemessene Online-Inhalte aufgerufen werden oder zum Vergnügen gesurft wird
- Verhindern, dass unangemessene Software verwendet wird
- Sicherstellen, dass die Computerressourcen bestmöglich genutzt werden

Netop ProtectOn Pro Funktionen

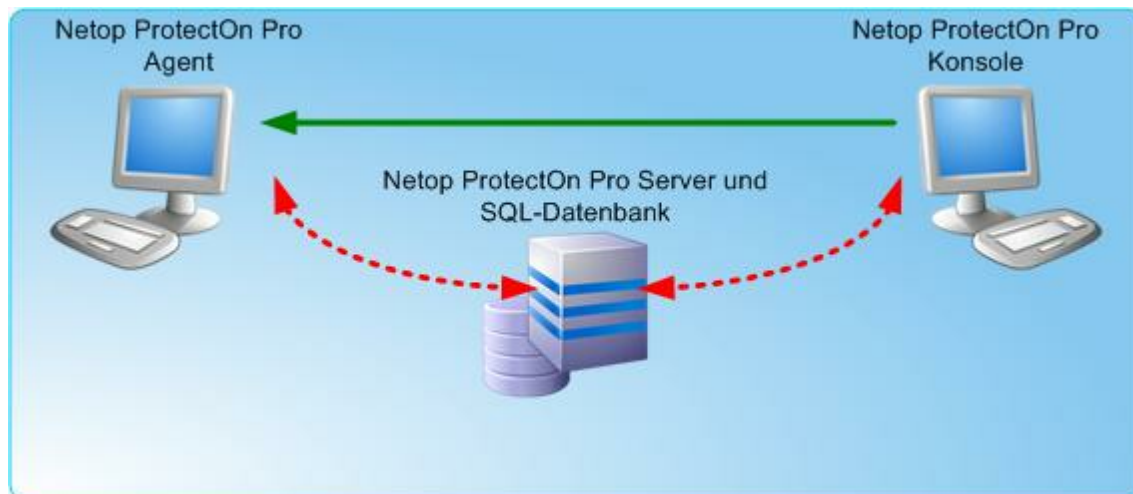
Um den IT-Administrator bei diesen Aufgaben zu unterstützen, bietet Netop ProtectOn Pro unter anderem folgende Funktionen:

- Automatisches Entfernen aller Änderungen an der Festplatte und Wiederherstellen des ursprünglichen Zustands. Es können Ausnahmen für bestimmte Ordner festgelegt werden, bei denen Änderungen erlaubt sind. Außerdem kann festgelegt werden, dass bestimmte Anwendungen – wie z. B. Antivirensoftware – dauerhafte Änderungen an der Festplatte vornehmen dürfen.
- Zulassen oder Verweigern des Zugriffs auf Systemgeräte, wie z. B. Festplatten, DVD-/CD- und Diskettenlaufwerke, parallele und serielle Schnittstellen, USB- und WiFi-Geräte
- Verbergen von Festplatteninhalt vor Benutzern oder Anzeigen von ausgewählten Ordnern
- Verweigern des Zugriffs auf unangemessene Internetseiten
- Sperren von bestimmten Anwendungen
- Durchsuchen von Microsoft Windows Netzwerken, um Informationen über Netzwerkcomputer zu erhalten
- Fernverwaltung von Netzwerkcomputern

Netop ProtectOn Pro Komponenten

Netop ProtectOn Pro besteht aus drei Komponenten:

- Netop ProtectOn Pro Server
- Netop ProtectOn Pro Konsole
- Netop ProtectOn Pro Agent



Über den Server wird der Zugriff zur SQL-Datenbank verwaltet, die sich entweder auf demselben Computer befinden kann, auf dem der Server installiert ist, oder auf einem anderen Computer. Die Konsole ist das Administrationstool zur Verwaltung von Richtlinien und anderen Verwaltungsfunktionen. Der Agent wird auf den Computern installiert, denen der Administrator Richtlinien zuweisen oder die er über die Konsole verwalten möchte.

1.2 Funktionsweise von Netop ProtectOn Pro

Netop ProtectOn Pro basiert auf den Konzepten *Gruppen* und *Richtlinien*; Richtlinien werden Gruppen zugewiesen.

Eine Gruppe kann folgende Objekte umfassen:

- Windows Domänenobjekte: Computer (Workstations und Server), Windows Netzwerkbenutzer, Windows Netzwerkgruppen.
- Active Directory-Objekte: Alle Windows Domänenobjekte (Benutzer, Gruppen, Computer), Container, Unternehmenseinheiten.

Es gibt vier Arten von Richtlinien:

Richtlinie zum Festplattenschutz	Eine Richtlinie zum Festplattenschutz schützt die Inhalte von Festplatten vor schädlichen Änderungen. Über eine Festplattenrichtlinie kann der Administrator zu schützende Laufwerke auswählen, das Zurücksetzen einer Festplatte in ihren ursprünglichen Status bei Neustart aktivieren, Ausnahmeordner wählen, deren Inhalte beim Neustart nicht gelöscht werden, und Anwendungen festlegen, die dauerhafte Änderungen an Festplatten vornehmen dürfen.
Richtlinie zum Gerätezugriff	Über eine Richtlinie zum Gerätezugriff kann der Zugriff auf Systemgeräte, wie Disketten- und DVD/CD-ROM-Laufwerke, USB-Geräte, Bluetooth-Geräte und serielle Schnittstellen, zugelassen oder verweigert werden. Außerdem können die Inhalte von Festplatten vor den Benutzern verborgen werden.
Webrichtlinie	Eine Webrichtlinie kann den Zugriff auf Websites zulassen oder verweigern.
Anwendungsrichtlinie	Über eine Anwendungsrichtlinie kann festgelegt werden, welche Anwendungen ausgeführt werden dürfen.

Sie können so viele Richtlinien derselben Art wie erforderlich erstellen.

Jede Richtlinie ist einer Gruppe zugewiesen, die aus den oben aufgeführten Objekten bestehen kann. Grundsätzlich wird eine Richtlinie jedoch auf Computer oder Benutzer angewendet. Enthält eine Gruppe beispielsweise eine Active Directory-Unternehmenseinheit, werden die Richtlinien auf die Benutzer und Computer angewendet, die in dieser Einheit enthalten sind. Enthält diese Einheit wiederum andere Einheiten, gelten die Richtlinien auch für deren Mitglieder. Das Gleiche gilt für Windows Netzwerkgruppen.

Wird eine Richtlinie auf einen Benutzer angewendet, ist sie nur für einen bestimmten Active Directory-Benutzer oder Windows Netzwerkbenutzer gültig. Wird eine Richtlinie auf einen Computer angewendet, gilt sie für alle Benutzer, die diesen Computer verwenden.

Eine Richtlinie zum Festplattenschutz kann nur auf Computer angewendet werden, während Gerätezugriffs-, Web- und Anwendungsrichtlinien sowohl für Computer als auch Benutzer gelten können. Wird eine Festplattenschutzrichtlinie einer Gruppe zugewiesen, die Computer und Benutzer umfasst, werden die Benutzer dieser Gruppe ignoriert; die Richtlinie wird nur auf die Computer angewendet.

Bei gleicher Richtlinienkategorie haben Richtlinien, die sich auf Benutzer beziehen, oberste Priorität: Gibt es Richtlinien auf Benutzerebene, werden die Richtlinien auf Computerebene ignoriert. Wenden Sie beispielsweise zwei unterschiedliche Richtlinien an, von denen eine Computer 1 den Zugriff auf die Website www.lustigsteundcoolstespiele.de verweigert, während die andere Richtlinie Benutzern von Computer 1 den Zugriff auf diese Website erlaubt, hat letztere Vorrang. Der Zugriff auf die Website ist also erlaubt. Es gibt jedoch eine Richtlinienoption, mit der Sie die Priorität einer Richtlinie bestimmen können, so dass sie andere Richtlinien derselben Art aufheben kann.

1.3 Unterstützte Betriebssysteme

Netop ProtectOn Pro unterstützt eine Vielzahl von Betriebssystemen. Folgende Funktionen stehen jeweils unter den einzelnen Betriebssystemen zur Verfügung:

Betriebssysteme ▶ ▼ Module oder Sitzungen	2008/2003/ Windows 7/Vista/ XP²⁾ (64 Bit)¹⁾	2008/2003/ Windows 7/Vista/ XP²⁾/2000³⁾	NT4³⁾
Netop ProtectOn Pro Server	x	x	
Netop ProtectOn Pro Konsole	x	x	
Agent: Festplattenschutz	x	x	x
Agent: Gerätezugriff	x	x	
Agent: Zugriff auf Anwendungen	x	x	x
Agent: Webzugriff	x	x	x
Remoteverwaltung	x	x	x
Fernsteuerung	x	x	x

1) Windows Server 2008, 2003 Standard, Web Edition, Enterprise Edition. Windows 2000 Server und Advanced Server. Windows 2000 Professional, Service Pack 2.

2) Windows XP, Service Pack 2

3) Einschließlich der Windows 2000, Service Pack 4 und NT4 Serverversionen, Service Pack 6.

Hinweis

- Die Fernsteuerungsfunktion hängt davon ab, ob Netop Remote Control installiert wurde oder nicht: Wenn der Netop Remote Control Guest auf dem Computer installiert ist, auf dem auch die Netop ProtectOn Pro Konsole verfügbar ist, aktiviert Netop ProtectOn Pro dieses Programm. Wenn der Netop Remote Control Guest NICHT installiert wurde, ist die Windows **Remotedesktopverbindung** aktiviert.
-

2 Konfigurations- und Verbindungseinstellungen

2.1 Servereinstellungen

Nach der Installation verfügt die Serverkomponente über Standardeinstellungen und ist ohne weitere Konfiguration einsatzbereit. Änderungen an den Standardeinstellungen, beispielsweise zu Testzwecken oder wenn der SQL-Server oder die SQL-Datenbank geändert wurden, können über die Netop ProtectOn Pro Servereinstellungen vorgenommen werden.

Das Dialogfeld für die Servereinstellungen wird über das Windows **Startmenü** geöffnet:
Programme > Netop ProtectOn Pro > Serverkonfiguration.

☐ Registerkarte "**Verbindungseigenschaften**"

Die Registerkarte **Verbindungseigenschaften** definiert, wie die Serverkomponente mit der SQL-Serverdatenbank zusammenarbeitet, die die Geräterichtlinien speichert.

Konfigurations- und Verbindungseinstellungen

Option	Beschreibung
Servername	Um einen anderen SQL-Server zu verwenden, geben Sie den Namen des Servers ein. Der Netop ProtectOn Pro Server findet automatisch den SQL-Server im Netzwerk.
Windows NT Integrated Security verwenden	Integrated Security verwendet die aktuelle Windows Identität, um auf die SQL-Serverdatenbank zuzugreifen. Sie können dann Datenbank und Berechtigungen eines SQL-Servers die Windows Identität zuweisen. Dies ist die Standardeinstellung.
Verwenden Sie einen spezifischen Benutzernamen und ein spezifisches Kennwort.	Wählen Sie diese Option, wenn Sie einen Benutzernamen und ein Kennwort verwenden möchten, die nicht mit dem Windows Benutzernamen und Kennwort identisch sind.
Datenbankname	Um eine andere Datenbank zu verwenden, geben Sie den Namen einer vorhandenen Datenbank auf dem SQL-Server ein. Klicken Sie nach der Änderung des Datenbanknamens auf Testverbindung .

Ein Hinweis zur Änderung der Datenbank nach der Installation

Sie sollten den Datenbanknamen nicht ändern, wenn Sie keine Erfahrung mit der Verwaltung von SQL-Datenbanken haben.

Das Installationsprogramm erstellt und initialisiert automatisch eine leere SQL-Datenbank. Wenn Sie die Datenbank nach der Erstkonfiguration ändern möchten, müssen Sie die Datenbank manuell erstellen. Nach der Erstellung der Datenbank müssen Sie das Skript DB_All.sql manuell ausführen. Das Skript wurde mit dem Netop ProtectOn Pro Server installiert. Wenn Sie einen anderen Datenbanknamen als den standardmäßig vorgegebenen (NPP_DB) verwenden möchten, können Sie in der Skriptdatei den Namen suchen und ersetzen.

Portnummer	Port 1973 ist der Standardport. Die Portnummer kann geändert werden, sollte jedoch mit der Servereinstellung des Ports auf der Konsole und dem Agent übereinstimmen. Eine Beschreibung und Anleitung zum Festlegen dieser Einstellungen finden Sie in den Abschnitten Konsoleneinstellungen und Agenteneinstellungen .
------------	---

Hinweis

Kehren Sie nach der Konfiguration der Konsole zu dieser Registerkarte zurück und

testen Sie die Verbindung.

Über die Schaltfläche **Testverbindung** können Sie überprüfen, ob die Datenbank für den Server sichtbar ist und ob der Benutzer über ausreichende Berechtigungen für den Zugriff auf die Datenbank verfügt.

☐ Registerkarte "Lizenz"

Die Registerkarte **Lizenz** zeigt die aktuellen Lizenzen an.

Option	Beschreibung
Lizenzname	Name der Lizenzdatei. Klicken Sie auf Installieren , um eine neue Lizenzdatei hinzuzufügen, oder auf Entfernen , um eine vorhandene Lizenzdatei zu entfernen.
Begrenzung	Die Anzahl an Netop ProtectOn Pro Agents, die von der Netop ProtectOn Pro Konsole gesteuert werden können. <hr/> Hinweis Die Liste kann mehrere Lizenzen beinhalten; die aufgelisteten Zahlen werden einfach zusammengezählt. Wenn Sie beispielsweise eine 10-Benutzer-Lizenz und eine 20-Benutzer-Lizenz haben, kann das System 30 Benutzer steuern.
Abgelaufen	Das Datum, an dem die Lizenz abläuft.
Typ	Liste der Module, die die Netop ProtectOn Pro Installation umfasst: <ul style="list-style-type: none">• Anwendungssperre• Websperre• Festplattenschutz• Gerätezugriff Zu diesen Bereichen können Richtlinien definiert werden.
Kommentare	Textkommentare aus der Lizenzdatei.

Klicken Sie auf die Schaltfläche **Verbindungen zurücksetzen**, um die Anzahl aktiver Agents zu berechnen. Diese Funktion ist nützlich, wenn die Begrenzung der Agentinstallationen erreicht wurde und ein oder mehrere Computer mit installierter Agentsoftware aus dem Netzwerk entfernt werden. Durch Klicken auf **Verbindungen zurücksetzen** wird sichergestellt, dass die nicht mehr im Netzwerk befindlichen Computer von der Berechnung ausgeschlossen werden.

☐ Registerkarte "Verschiedenes"

Konfigurations- und Verbindungseinstellungen

Option	Beschreibung
Intervall der Netzwerksuche	Das Intervall, in dem der Netop ProtectOn Pro Server das Netzwerk nach MAC-Adressen und USB-Geräten durchsuchen soll. Die empfohlene Einstellung ist 3600 Sekunden.
RM-Portnummer	Die Portnummer auf dem Netop ProtectOn Pro Server, die für die Remoteverwaltung verwendet wird. Die Standardeinstellung ist Port 1972.
Intervall der Downloadrichtlinie	Das Intervall, in dem der Netop ProtectOn Pro Server neue und geänderte Richtlinien auf die Agents herunterlädt. Die empfohlene Einstellung ist 900 Sekunden.
Intervall zur Übernahme einer Richtlinie	Das Intervall, in dem der Netop ProtectOn Pro Server neue und geänderte Richtlinien für Agents übernimmt. Die empfohlene Einstellung ist 900 Sekunden.

2.2 Konsoleneinstellungen

Nach der Installation der Konsole verfügt diese über Standardeinstellungen und ist ohne weitere Konfiguration einsatzbereit. Wenn Sie die Konsole von Netop ProtectOn Pro nach der Installation zum ersten Mal starten, öffnet sich zu Informationszwecken das Dialogfeld **Einstellungen**. Nachträgliche Änderungen an den Standardeinstellungen, beispielsweise wenn der Server auf einem anderen Computer installiert wird, können im Dialogfenster **Einstellungen** vorgenommen werden.

Das Dialogfenster Konsoleneinstellungen wird über die Netop ProtectOn Pro Konsole geöffnet: **Datei > Einstellungen**.

Option	Beschreibung
Computername	Der Name des Computers auf dem der Netop ProtectOn Pro Server installiert ist.
Portnummer (Netop ProtectOn Pro Server)	Die Portnummer auf dem Netop ProtectOn Pro Server, die für die Kommunikation mit der Konsole verwendet wird. Die Portnummer kann geändert werden, sollte jedoch mit der Servereinstellung des Ports auf dem Netop ProtectOn Pro Server und dem Netop ProtectOn Pro Agent übereinstimmen. Eine Beschreibung und Anleitung zum Festlegen dieser Einstellungen finden Sie im Abschnitt Servereinstellungen und Agenteneinstellungen .
Portnummer (Remoteverwaltung)	Die Portnummer auf der Konsole, die für die Remoteverwaltung bei Agentcomputern verwendet wird.

Wenn Sie sich an einem Netop ProtectOn Pro Server anmelden, für den Sie keine korrekten Anmeldedaten haben, erhalten Sie die Nachricht "Fehler beim Verbinden mit dem ProtectOn Pro Server". Wenn Sie bei der Frage, ob Sie andere Anmeldedaten eingeben möchten, auf **Nein** klicken, können Sie die Daten vom Netop ProtectOn Pro Server anzeigen, jedoch keine Änderungen vornehmen.

Wenn Sie bei der Frage auf **Ja** klicken und die neuen Anmeldedaten die des Administrators sind, können Sie neue Richtlinien und Gruppen erstellen sowie bereits vorhandene Richtlinien und Gruppen ändern.

2.3 Agenteinstellungen


Nach der Installation des Agents verfügt dieser über die Standardeinstellungen und ist ohne weitere Konfiguration einsatzbereit. Änderungen an den Standardeinstellungen, beispielsweise wenn der Server auf einem anderen Computer neu installiert wird oder sich die Protokollierungsanforderungen beim Test ändern, können im Dialogfeld **Netop ProtectOn Pro Agenteinstellungen** eingestellt werden.

Das Dialogfeld für die Einstellungen des Agents wird über das Windows' **Startmenü** geöffnet: **Alle Programme > Netop ProtectOn Pro > Agentkonfiguration**.

Hinweis

Um nicht autorisierte Agentbenutzer daran zu hindern, Konfigurationsänderungen vorzunehmen, kann der Zugriff auf das Dialogfeld Agenteinstellungen durch ein Kennwort geschützt werden. Das Kennwort wird über die Konsole definiert: Klicken Sie im Menü **Datei** auf **Agenteinstellungen**.

☐ Registerkarte "Allgemein"

Option	Beschreibung
Host-Name	Der Name des Computers, auf dem der Netop ProtectOn Pro Server installiert ist. Um sich mit einem anderen Server zu verbinden, geben Sie den Namen eines anderen Computers ein. Wenn Sie sich mit einem nicht verfügbaren Servernamen verbinden, ändert sich das Serversymbol im Benachrichtigungsbereich in grau.
Portnummer	Die Portnummer, die für die Gerätesteuerung verwendet wird. Port 1973 ist die Standard-Portnummer.
Dienstkonto	Wählen Sie diese Option, um sich mit der Windows-Authentifizierung mit dem Netop ProtectOn Pro Server zu verbinden.
Dieses Konto	Wählen Sie diese Option, um andere Zugriffsrechte zu definieren. Klicken Sie auf die Schaltfläche Durchsuchen (), um ein Konto auszuwählen.
Portnummer (Remoteverwaltungsverbindung)	Die Portnummer, die für die Remoteverwaltung verwendet wird. Die Standardeinstellung ist Port

1972.

Hinweis

Die Portnummern können geändert werden, sollten jedoch mit der Port-Servereinstellung auf dem Server und der Konsole übereinstimmen. Eine Beschreibung und Anleitung zum Festlegen dieser Einstellungen finden Sie im Abschnitt [Servereinstellungen](#) und [Konsoleneinstellungen](#).

☐ Registerkarte "Einschränkungsmeldungen"

Verwenden Sie die Optionen, um festzulegen, ob der Agent von Netop ProtectOn Pro alle, einige oder keine Nachrichten anzeigen soll, die den Benutzer über die Einschränkungen informieren, die den Zugriff auf die Verwendung von Geräten, Programmen oder Websites sperren.

Die Einstellungen auf dieser Registerkarte können ebenfalls über das Dialogfeld Netop ProtectOn Pro Agent geändert werden, dass mit einem Doppelklick auf das Symbol für den Agent von Netop ProtectOn Pro im Benachrichtigungsbereich geöffnet wird:



Das Agentsymbol kann unterschiedlich aussehen:

- Normal, wie oben gezeigt.
- Grau. Konnte sich der Agent mit dem Netop ProtectOn Pro Server nach drei Versuchen hintereinander nicht verbinden, wird das Symbol grau. Dies soll den Benutzer darauf hinweisen, dass es Verbindungsprobleme gibt. Der Agent versucht weiterhin, die Verbindung unter Verwendung der alten Richtlinien aufzubauen. Ist die Verbindung aufgebaut, wechselt das Symbol in den Normalzustand.
- Rotes **X**. Über dem Symbol wird ein rotes **X** angezeigt, wenn die Lizenzbedingungen verletzt wurden. Wenn beispielsweise ein sechster Agentcomputer versucht, sich mit einem Netop ProtectOn Pro Server zu verbinden, der nur über fünf Lizenzen verfügt, wird der Zugriff verweigert und ein **X** über dem Symbol dargestellt. Der Agent kann dann nicht mit dem Netop ProtectOn Pro Server kommunizieren.

☐ Registerkarte "Protokollierung"

Verwenden Sie die Optionen auf dieser Registerkarte, um den Umfang der Protokollierung zu definieren: ob wiederholte Meldungen protokolliert und ob Protokolldateien nach Größe oder Zeit begrenzt werden. Ist eine Protokolldatei begrenzt, wird diese regelmäßig wiederverwendet, sobald die Größen- oder Stundengrenze erreicht ist.

2.4 Remoteinstallation des Agentmoduls

Um in Netop ProtectOn Pro Festplattenschutz bzw. die Steuerung des Zugriffs auf Programme, Ressourcen und Internetseiten zu verwenden, muss das Agentmodul tatsächlich auf den Clientcomputern installiert sein und als Dienst ausgeführt werden.

Da es sich um eine Vielzahl von Computern an verschiedenen Orten handeln kann, verfügt die Konsole über Funktionen zur Remoteinstallation und -deinstallation des Agentmoduls.

Wenn Sie den Agent jedoch an eine große Anzahl von Clientcomputern verteilen möchten, ist diese Methode evtl. ungeeignet. In diesem Fall ist die Verwendung der Agentinstallationsdatei (NPPAgentSetup.msi) möglicherweise vorzuziehen.

Hinweis

Wie bei anderen Installationsarten sind für die Remoteinstallation Administratorrechte auf dem Computer erforderlich, auf dem das Agentmodul installiert wird.

☐ Das Agentmodul über die Konsole installieren

1. Wählen Sie im Fenster **Netzwerk** einen Computer unter **Active Directory** oder **Microsoft Windows Netzwerk** aus.
2. Klicken Sie mit der rechten Maustaste auf den Computer, und wählen Sie im Kontextmenü **Agent installieren**.

Die Verlaufsleiste zeigt den Installationsfortschritt an. Klicken Sie nach der Beendigung des Vorgangs auf **Schließen**.

Der Agent wird installiert und als Dienst gestartet. Der Computer wird dann durch Richtlinien geschützt, die über die Konsole festgelegt werden.

Wenn Sie das Agentmodul zu einem späteren Zeitpunkt von einem Computer entfernen möchten, klicken Sie mit der rechten Maustaste auf den Computer und dann auf **Agent deinstallieren**.

☐ Das Agentmodul über die Agentinstallationsdatei installieren

Eine Installationsdatei kann auf unterschiedliche Weise verteilt und ausgeführt werden, zum Beispiel über ein Anmeldeskript oder über Gruppenrichtlinien im Active Directory.

Die Installationsdatei für den Agent muss unter Angabe von Parametern ausgeführt werden, die den Namen sowie den Port des Netop ProtectOn Pro Servers enthalten. Um einen Agent so zu konfigurieren, dass er eine Verbindung zu **Name des Richtlinienservers** herstellt und den Port **Port** verwendet, wird folgende Befehlszeile verwendet:

```
NPPAgentSetup.msi ACTION=INSTALL POLICYSERVER=Name des Richtlinienservers SERVERPORT=Port
```

Ersetzen Sie **Name des Richtlinienservers** und **Port** durch die entsprechenden Einstellungen Ihrer aktuellen Umgebung.

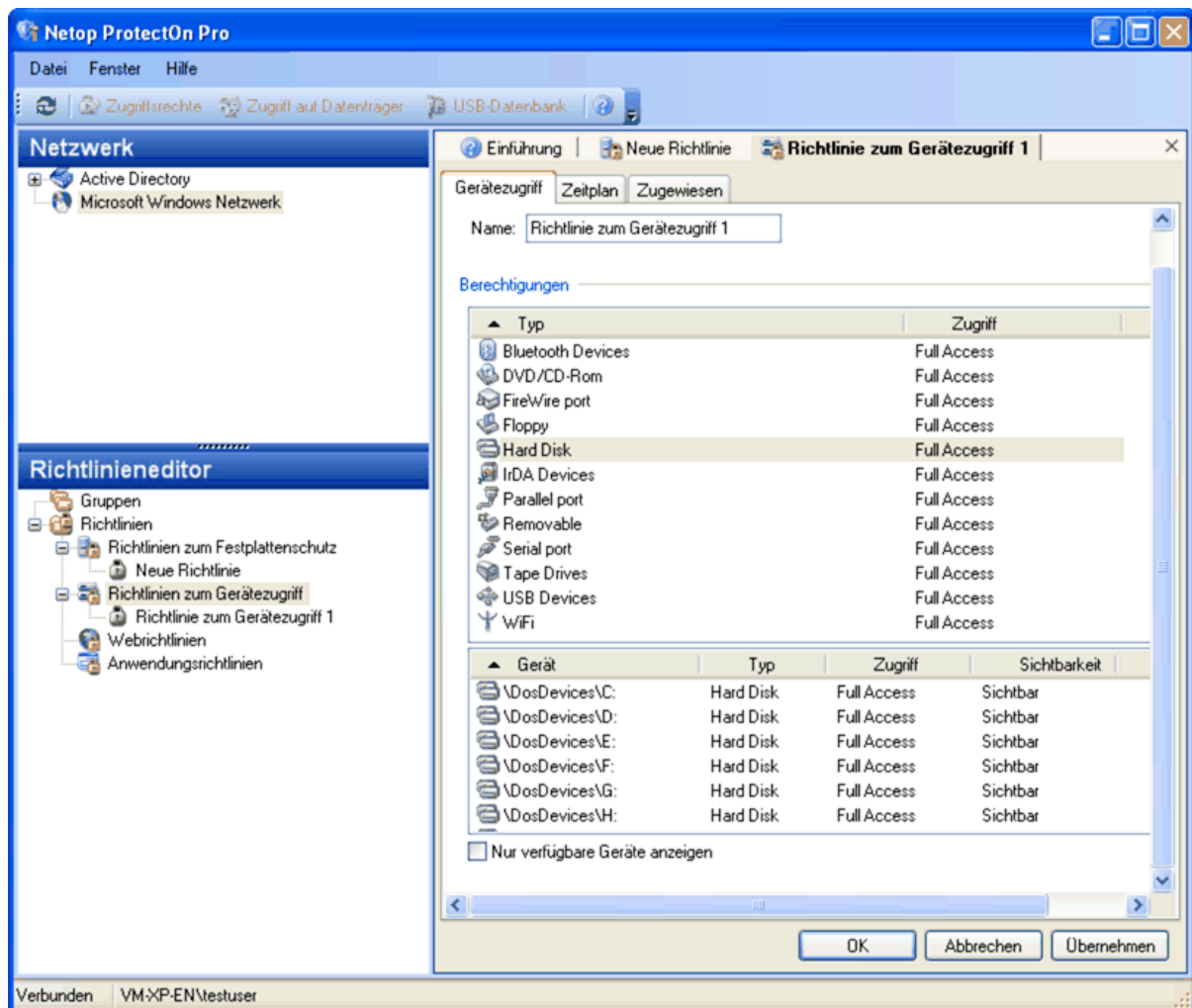
Um eine Übertragungsdatei (MST) für die MSI-Datei zu erstellen, ist die Angabe der Eigenschaften von POLICYSERVER und SERVERPORT erforderlich.

3 Netop ProtectOn Pro Konsole

3.1 Benutzeroberfläche der Konsole

Die Benutzeroberfläche der Netop ProtectOn Pro Konsole besteht aus folgenden vier Komponenten:

- Menüleiste und Symbolleiste
- Fenster "Netzwerk"
- Fenster "Richtlinieneditor"
- Datenfenster



Menüleiste und Symbolleiste

Die Menüleiste besteht aus den Menüs **Datei**, **Ansicht**, **Fenster** und **Hilfe**. Weitere Menüs sind je nach Auswahl des Objekts im Fenster **Netzwerk**, im Fenster **Richtlinieneditor** oder im Datenfenster verfügbar.

Die Symbolleiste unterhalb der Menüleiste enthält Schaltflächen für Menübefehle. Die Anzahl und Verfügbarkeit der Schaltflächen ist ebenfalls abhängig von der Auswahl des Objekts im Fenster **Netzwerk**, im Fenster **Richtlinieneditor** oder im Datenfenster.

Fenster "Netzwerk"




Das Fenster **Netzwerk** ermöglicht Ihnen folgende Aktionen:

- Durchsuchen des Active Directory- und des Microsoft Windows Netzwerks nach Objekten, die in Gruppen aufgenommen werden sollen.
- Verwaltung des Active Directory-Netzwerks über das standardmäßige Snap-In Active Directory-Benutzer und -Computer der Microsoft Management Console.
- Anzeige der QuickInfo mit Informationen über Arbeitsstationen des Microsoft Windows Netzwerks, einschließlich Domänen- und Benutzername, IP-Adresse und Betriebssystem.
- Öffnen einer Sitzung auf einem Netzwerkcomputer, auf dem ein Agentmodul installiert ist.

Fenster "Richtlinieneditor"

Das Fenster **Richtlinieneditor** ermöglicht Ihnen folgende Aktionen:

- Erstellen von vier Arten von Richtlinien: Richtlinien zum Festplattenschutz, Richtlinien zum Gerätezugriff, Webrichtlinien und Anwendungsrichtlinien.
- Erstellen von Objektgruppen, denen Richtlinien zugewiesen werden sollen.
- Zuweisung von Richtlinien zu Gruppen.

Wenn eine Richtlinie mindestens einer Gruppe zugewiesen wurde, wird sie mit dem Symbol  gekennzeichnet. Wenn eine Richtlinie keiner Gruppe zugewiesen wurde, wird sie mit dem Symbol  gekennzeichnet. Wenn eine Richtlinie andere Richtlinien überschreibt, wird sie mit einem Ausrufezeichen gekennzeichnet ().

Datenfenster

Im Datenfenster werden Informationen über ein Objekt angezeigt, wenn Sie auf dieses Objekt im Fenster **Netzwerk** oder im Fenster **Richtlinieneditor** doppelklicken.



Mögliche Objekte:

- Netzwerkobjekt
- Richtlinie
- Gruppe, der eine Richtlinie zugewiesen werden soll

Es können ein oder mehrere Datenfenster gleichzeitig geöffnet werden.

Standardmäßig werden die Informationen zu den unterschiedlichen Objekten in Registerkarten dargestellt. Sie können die Darstellung jedoch ändern, indem Sie in der Menüleiste **Fenster > Überlappend** oder **Fenster > Nebeneinander** wählen.

3.2 Eine Netzwerkstruktur durchsuchen

Um die Struktur des **Active Directory** oder des **Microsoft Windows Netzwerks** zu durchsuchen, verwenden Sie  und  zum Erweitern bzw. Ausblenden der Verzeichnisse.

Doppelklicken Sie auf ein Objekt in der Struktur, um dessen Eigenschaften im Datenfenster anzuzeigen.

Wenn Sie **Active Directory** Netzwerke durchsuchen, können Sie zu jeder Netzwerkdomäne eine Verbindung herstellen. Über die Verbindungsherstellung zu einer

anderen Domäne können Sie jeden mit dem Netzwerk verbundenen Computer erreichen.

Verbindung zu einer Domäne herstellen

1. Klicken Sie im Fenster **Netzwerk** mit der rechten Maustaste auf **Active Directory**, und wählen Sie **Verbindung zu einer Domäne herstellen**.
2. Geben Sie im Dialogfeld **Verbindung zu einer Domäne herstellen** den Namen der gewünschten Domäne ein, oder klicken Sie auf **Durchsuchen**, um einen Eintrag aus der Domänenliste auszuwählen.

Hinweis

Nach dem Neustart der Netop ProtectOn Pro Konsole wird die Standarddomäne im Active Directory-Knoten angezeigt. Die Standarddomäne ist jeweils die Domäne, bei der der Computer Mitglied ist.

3.3 Active Directory-Netzwerke verwalten

Im Fenster **Netzwerk** können Sie Active Directory-Netzwerke einfach verwalten, indem Sie das Snap-In **Active Directory-Benutzer und -Computer** der **Microsoft Management Console** (MMC) verwenden. Über **Active Directory-Benutzer und -Computer** können Sie Benutzer, Gruppen, Unternehmenseinheiten sowie alle anderen Active Directory-Objekte verwalten.

Hinweis

Um ein **Active Directory**-Netzwerk zu verwalten, müssen Sie zunächst die Microsoft Management Console installieren, sofern diese nicht bereits als Teil des Betriebssystems installiert wurde. MMC ist in Windows 2000 und höheren Betriebssystemversionen enthalten. Installieren Sie das Snap-In **Active Directory-Benutzer und -Computer** auch auf dem Administratorcomputer. Dieses Snap-In ist ein Bestandteil des Win2003/Win2008 Admin Pack und wird mit Windows 2003/2008 geliefert. Es kann auch unter Windows 2000 und XP installiert werden. MMC wird im [Microsoft Download Center](#) zur Verfügung gestellt.

Ein Active Directory-Objekt verwalten

1. Wählen Sie ein Objekt aus der **Active Directory**-Struktur.
2. Klicken Sie mit der rechten Maustaste auf das Objekt, und wählen Sie im Kontextmenü **In MMC öffnen** aus.

Die **Microsoft Management Console** wird geöffnet und das gewünschte Objekt angezeigt.

Sie können auch den Befehl **Eigenschaften in MMC öffnen** im Kontextmenü verwenden. Über diese Option können Sie nicht nur MMC öffnen, sondern auch die Eigenschaften des gewünschten Objekts direkt anzeigen. Diese Menüoption ist nur dann verfügbar, wenn Windows 2000, XP, 2003 oder 2008 auf dem Computer installiert ist. Die Optionen **In MMC öffnen** und **Eigenschaften in MMC öffnen** sind auch über das Menü **Ansicht** verfügbar, wenn ein Active Directory-Objekt aus dem Fenster **Netzwerk** ausgewählt wurde.

3. Nehmen Sie die gewünschten Änderungen an den Objekteigenschaften in MMC vor. Informationen zur Verwendung von MMC finden Sie in der MMC-Hilfe.

Eine Gruppenrichtlinie verwalten

Gruppenrichtlinien können auch für Active Directory-Domänen und Organisationseinheiten verwaltet werden. Dazu sollten die folgenden Softwarekomponenten auf dem Computer installiert sein, auf dem auch die Konsole installiert ist:

- **Objekteditor für Gruppenrichtlinien (GPOE)**. Diese Software ist ein MMC-Snap-In und Bestandteil des Win 2003/2008 Admin Pack.
- **Verwaltungskonsole für Gruppenrichtlinien (GPMC)**. Dieses MMC-Snap-In ist eine eigenständige Software.

1. Klicken Sie in der **Active Directory**-Struktur mit der rechten Maustaste auf die Domäne oder die Organisationseinheit, und wählen Sie **Gruppenrichtlinien in MMC öffnen** aus.

2. Das Dialogfeld **Gruppenrichtlinien** wird geöffnet und zeigt Folgendes an:

- Wenn nur GPOE auf dem Computer installiert ist, enthält das Dialogfeld die Liste der gültigen Gruppenrichtlinien. Um eine Richtlinie zu bearbeiten, wählen Sie die gewünschte Richtlinie aus, und klicken Sie auf **Bearbeiten**.
- Wenn GPMC auf dem Computer installiert ist, zeigt das Dialogfeld die Schaltfläche **Öffnen** an. Klicken Sie auf diese Schaltfläche, um die **Verwaltungskonsole für Gruppenrichtlinien (GPMC)** zu öffnen. Informationen zur Verwendung der Konsole finden Sie in der Microsoft Management Console-Hilfe.

3.4 Details des Microsoft Windows Netzwerkcomputers anzeigen

Während des Durchsuchens des **Microsoft Windows Netzwerks** über das Fenster **Netzwerk** können Sie Informationen zum vernetzten Computer abfragen. Fahren Sie dazu mit der Maus über einen Computernamen in der Strukturansicht, um eine QuickInfo mit folgenden Informationen anzuzeigen:

- Name der Computerdomäne
- Computername
- IP-Adresse des Computers
- Version des auf dem Computer installierten Betriebssystems
- Typ des Betriebssystems, und andere Systeminformationen, dargestellt durch Akronyme und Abkürzungen.

☐ Liste der Akronyme und Abkürzungen

Abkürzung	Beschreibung
BBS	Server, auf dem der Sicherungsbrowser-Dienst (Backup Browser Service) ausgeführt wird
MBS	Server, auf dem der Hauptbrowser-Dienst (Master Browser Service) ausgeführt wird
BDC	Sicherungsdomänen-Controller (Backup Domain Controller)
PDC	Primärdomänen-Controller

Netop ProtectOn Pro Konsole

Abkürzung	Beschreibung
NTC	NT Cluster
DFS	Stamm einer DFS-Struktur
DMBS	Server, auf dem der Domänen-Hauptbrowser-Dienst (Domain Master Browser Service) ausgeführt wird
LOCAL	Server, die über den Browserdienst verwaltet werden
MEMB	LAN Manager 2.x Domänenmitglied
NWS	Novell Server
WNT	Windows NT/2000/XP/2003 (Workstation oder Server)
WDE	Microsoft Windows Server 2003, Datacenter Edition
WEE	Microsoft Windows Server 2003, Enterprise Edition
WSE	Microsoft Windows Server 2003, Standard Edition
WWE	Microsoft Windows Server 2003, Web Edition
WS	Microsoft Windows NT/2000/2003 Server
WAS	Microsoft Windows 2000 Advanced Server
WDS	Microsoft Windows 2000 Datacenter Server
WEES	Microsoft Exchange 2000 Enterprise Server
WES	Microsoft Exchange 2000 Server
WISS	Microsoft Internet Security und Acceleration Server 2000
WSPS	Microsoft SharePoint Portal Server 2001
WSMS	Microsoft Systems Management Server
WMOM	Microsoft Operations Manager 2000
WMAC	Microsoft Application Center 2000
WTPC	Microsoft Windows XP Tablet PC Edition
NTS	Windows NT/2000/2003 Server (nicht DC)
PBS	Server, auf dem der Browserdienst ausgeführt werden kann
PDOM	Primäre Domäne
SPQ	Server mit freigegebener Druckerwarteschlange

Abkürzung	Beschreibung
SQL	Alle Server, auf denen der SQL Server ausgeführt wird
TSS	Server, auf dem der Zeitquellendienst (Time Source Service) ausgeführt wird
WIN	Alle Windows-Betriebssysteme
16	Windows 16-Bit-Betriebssysteme
32	Windows 32-Bit-Betriebssysteme
64	Windows 64-Bit-Betriebssysteme
WFWS	Server, auf dem Windows für Arbeitsgruppen ausgeführt wird
WFW	Workstation, auf der Windows für Arbeitsgruppen ausgeführt wird
WS	Alle Workstations
WTS	Server, auf dem die Windows Terminal Services ausgeführt werden
CTS	Server, auf dem die Citrix Terminal Services ausgeführt werden
MAC	Jede MAC Workstation
MACS	Jeder MAC Server
LINUX	Jede Linux Workstation
LINUXS	Jeder Linux Server
SOL	Jede Solaris Workstation
SOLS	Jeder Solaris Server

3.5 Netzwerkcomputer fernstarten (WOL)

Sie können vom Fenster **Netzwerk** aus ein Fernstartsignal senden, um einen Netzwerkcomputer zu starten. Dies kann nützlich sein, wenn Sie mit Remotecomputern arbeiten müssen, die für Sie nicht zugänglich sind und nicht rund um die Uhr eingeschaltet bleiben können, jedoch gelegentlich gestartet werden müssen.

Ein Fernstartsignal senden

1. Wählen Sie im Fenster **Netzwerk** einen Computer unter **Active Directory** oder **Microsoft Windows Netzwerk** aus.
2. Klicken Sie mit der rechten Maustaste auf den gewünschten Computer, und wählen Sie im Kontextmenü **Kommunikationsanfrage starten**.

Hinweis

Um diese Funktion nutzen zu können, müssen Sie sicherstellen, dass der fernzustartende Computer an eine elektrische Stromversorgung angeschlossen und der Schalter auf dessen Rückseite eingeschaltet ist. Außerdem sollten Sie prüfen, ob diese Funktion vom BIOS des Remotecomputers unterstützt wird, und diese gegebenenfalls in den Einstellungen des Netzwerkadapters aktivieren.

Netzwerkadapter-Einstellungen ändern

1. Klicken Sie auf **Start > Systemsteuerung**.
2. Öffnen Sie **System**, und klicken Sie auf der Registerkarte **Hardware** auf **Geräte-Manager**.
3. Suchen Sie unter **Netzwerkadapter** ihren Netzwerkadapter, und doppelklicken Sie auf diesen, um dessen Eigenschaften anzuzeigen.
4. Klicken Sie im Eigenschaftsdialogfenster auf die Registerkarte **Erweitert**, und wählen Sie **Fernstartfunktionen (WOL)** aus der Liste **Eigenschaft** aus. Wählen Sie in der Liste **Wert Magic & adressierte Pakete**.
5. Klicken Sie auf **OK**, um Änderungen zu speichern.

Beachten Sie, dass die genauen Schritte und Befehle vom jeweiligen Betriebssystem abhängen.

3.6 Remoteinstallation des Agentmoduls

Um in Netop ProtectOn Pro Festplattenschutz bzw. die Steuerung des Zugriffs auf Programme, Ressourcen und Internetseiten zu verwenden, muss das Agentmodul tatsächlich auf den Clientcomputern installiert sein und als Dienst ausgeführt werden.

Da es sich um eine Vielzahl von Computern an verschiedenen Orten handeln kann, verfügt die Konsole über Funktionen zur Remoteinstallation und -deinstallation des Agentmoduls.

Wenn Sie den Agent jedoch an eine große Anzahl von Clientcomputern verteilen möchten, ist diese Methode evtl. ungeeignet. In diesem Fall ist die Verwendung der Agentinstallationsdatei (NPPAgentSetup.msi) möglicherweise vorzuziehen.

Hinweis

Wie bei anderen Installationsarten sind für die Remoteinstallation Administratorrechte auf dem Computer erforderlich, auf dem das Agentmodul installiert wird.

☐ Das Agentmodul über die Konsole installieren

1. Wählen Sie im Fenster **Netzwerk** einen Computer unter **Active Directory** oder **Microsoft Windows Netzwerk** aus.
2. Klicken Sie mit der rechten Maustaste auf den Computer, und wählen Sie im Kontextmenü **Agent installieren**.

Die Verlaufsleiste zeigt den Installationsfortschritt an. Klicken Sie nach der Beendigung des Vorgangs auf **Schließen**.

Der Agent wird installiert und als Dienst gestartet. Der Computer wird dann durch Richtlinien geschützt, die über die Konsole festgelegt werden.

Wenn Sie das Agentmodul zu einem späteren Zeitpunkt von einem Computer entfernen

möchten, klicken Sie mit der rechten Maustaste auf den Computer und dann auf **Agent deinstallieren**.

☐ **Das Agentmodul über die Agentinstallationsdatei installieren**

Eine Installationsdatei kann auf unterschiedliche Weise verteilt und ausgeführt werden, zum Beispiel über ein Anmeldeskript oder über Gruppenrichtlinien im Active Directory.

Die Installationsdatei für den Agent muss unter Angabe von Parametern ausgeführt werden, die den Namen sowie den Port des Netop ProtectOn Pro Servers enthalten. Um einen Agent so zu konfigurieren, dass er eine Verbindung zu **Name des Richtlinienservers** herstellt und den Port **Port** verwendet, wird folgende Befehlszeile verwendet:

```
NPPAgentSetup.msi ACTION=INSTALL POLICYSERVER=Name des Richtlinienservers SERVERPORT=Port
```

Ersetzen Sie **Name des Richtlinienservers** und **Port** durch die entsprechenden Einstellungen Ihrer aktuellen Umgebung.

Um eine Übertragungsdatei (MST) für die MSI-Datei zu erstellen, ist die Angabe der Eigenschaften von POLICYSERVER und SERVERPORT erforderlich.

3.7 Eine Remotesitzung auf einem Netzwerkcomputer öffnen

Über die Konsole von Netop ProtectOn Pro können Sie eine Sitzung auf einem beliebigen Computer im Netzwerk öffnen.

Hinweis

Um eine Remotesitzung auf einem Netzwerkcomputer zu öffnen, müssen Sie über Administratorrechte auf dem Remotecomputer verfügen. Außerdem muss der Netop ProtectOn Pro Agent auf dem Remotecomputer installiert sein.

Bei der Remoteverwaltung von Agentcomputern stehen unter anderem folgende Funktionen zur Verfügung:

- Informationen zu verfügbaren Laufwerken und deren Eigenschaften anzeigen.
- Das Windows-Ereignisprotokoll anzeigen.
- Auf den Task-Manager zugreifen.
- Computerdienste verwalten.
- Computerfreigaben, z. B. Laufwerke und Ordner, verwalten.
- Hardware- und Softwarebestände anzeigen.

Eine Remotesitzung starten

1. Wählen Sie einen Computer im Fenster **Netzwerk**.
2. Klicken Sie mit der rechten Maustaste auf den Computer, und wählen Sie **Verwalten**.

Die Oberfläche für die Remoteverwaltung wird im Datenfenster angezeigt.

Eine Remotesitzung mit anderen Anmeldedaten starten

Sie können eine Sitzung auf einem Netzwerkcomputer mit anderen Anmeldedaten starten.

Netop ProtectOn Pro Konsole

1. Wählen Sie einen Computer im Fenster **Netzwerk**.
2. Öffnen Sie das Kontextmenü durch Klicken mit der rechten Maustaste, und wählen Sie **Verwalten als**.
3. Geben Sie Benutzernamen und Kennwort ein, und klicken Sie auf **OK**.

Siehe auch:

[Verwaltungsfenster](#)

4 Gruppen erstellen

4.1 Eine Gruppe erstellen

Richtlinien können nur Gruppen zugewiesen werden, nicht aber einzelnen Objekten, wie z. B. Benutzern oder Computern. Um daher einem einzelnen Objekt eine Richtlinie zuzuweisen, müssen Sie zunächst eine Gruppe erstellen und dieser dann das Objekt zuordnen. Eine Gruppe besteht jedoch in der Regel aus mehreren Objekten. Hierbei kann es sich um **Active Directory**-Objekte oder um **Microsoft Windows Netzwerkobjekte** handeln.

Eine Gruppe erstellen

1. Klicken Sie im Fenster **Richtlinienditor** mit der rechten Maustaste auf **Gruppen**, und wählen Sie **Neue Richtliniengruppe**.

Es wird eine neue Gruppe mit einem Standardnamen erstellt.

2. Geben Sie einen geeigneten Namen für die Gruppe ein.

Sobald eine Gruppe erstellt wurde, können Mitglieder hinzugefügt werden.

3. Gehen Sie im Fenster **Netzwerk** zu einem Objekt, das Sie zur Gruppe hinzufügen möchten.

4. Verschieben Sie das Objekt vom Fenster **Netzwerk** über Drag & Drop in die Gruppe.

Das Objekt ist nun Teil der Gruppe.

Mitglieder können der Gruppe auch durch Verschieben von Mitgliedern aus anderen Gruppen hinzugefügt werden:

- Um ein Mitglied zu einer Gruppe hinzuzufügen, ohne es aus der ursprünglichen Gruppe zu löschen, drücken Sie die Strg-Taste, und ziehen Sie das Mitglied in die Zielgruppe.
- Um ein Mitglied von einer Gruppe zu einer anderen zu verschieben, drücken Sie die Umschalttaste, und ziehen Sie das Mitglied in die Zielgruppe.

Um ein Mitglied aus einer Gruppe zu entfernen, klicken Sie mit der rechten Maustaste auf das Objekt, das Sie entfernen möchten, und wählen Sie im Kontextmenü **Aus der Gruppe entfernen** aus.

4.2 Eine Gruppe umbenennen, kopieren oder löschen

Eine Gruppe umbenennen

1. Klicken Sie im Fenster **Richtlinienditor** mit der rechten Maustaste auf die Gruppe, die Sie umbenennen möchten, und wählen Sie **Umbenennen**.
2. Geben Sie einen geeigneten Namen für die Gruppe ein.

Eine Gruppe kopieren

Das Kopieren von Gruppen kann sich als nützlich erweisen, wenn Sie eine Gruppe auf Basis einer bereits vorhandenen Gruppe erstellen möchten. Dies erspart Ihnen die Mühe, der

Gruppen erstellen

neuen Gruppe Mitglieder hinzuzufügen. Eine Kopie der alten Gruppe enthält dieselben Mitglieder wie die alte Gruppe. Sie müssen sie nur noch umbenennen und gegebenenfalls kleinere Änderungen an den Mitgliedern vornehmen. Die Kopie übernimmt jedoch keine zugewiesenen Richtlinien der alten Gruppe; diese müssen erneut zugewiesen werden.

1. Klicken Sie im Fenster **Richtlinieneditor** mit der rechten Maustaste auf die Gruppe, die Sie kopieren möchten, und wählen Sie **Kopieren**.

Es wird eine neue Gruppe mit einem Standardnamen erstellt.

2. Geben Sie einen geeigneten Namen für die Gruppe ein.

Eine Gruppe löschen

Wenn eine Gruppe nicht mehr verwendet wird, können Sie sie löschen. Es gibt keine Einschränkungen beim Löschen einer Gruppe; eine Gruppe kann auch dann gelöscht werden, wenn ihr gültige Richtlinien zugewiesen wurden. Gruppenverweise auf Richtlinien werden gelöscht, während die Richtlinien selbst unverändert bleiben.

1. Klicken Sie im Fenster **Richtlinieneditor** mit der rechten Maustaste auf die Gruppe, die Sie löschen möchten, und wählen Sie **Löschen**.

Ein Dialogfeld wird geöffnet, das Sie zur Bestätigung des Löschvorgangs auffordert.

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

5 Richtlinien definieren und übernehmen

5.1 Info über Richtlinien

Netop ProtectOn Pro kann zur Implementierung von vier verschiedenen Kategorien von Richtlinien verwendet werden:

- Richtlinien zum Festplattenschutz
- Richtlinien zum Gerätezugriff
- Webrichtlinien
- Anwendungsrichtlinien

Richtlinien werden im Richtlinieneditor erstellt, indem Sie mit der rechten Maustaste auf den Knoten mit dem Namen der entsprechenden Richtlinienkategorie klicken. Die Eigenschaften einer Richtlinie werden auf drei Registerkarten festgelegt, die nach der Erstellung der Richtlinie über das Datenfenster zugänglich sind. Die erste Registerkarte bezieht sich auf die Kategorie der Richtlinie. Hier wird der Name und der Umfang der Richtlinie festgelegt. Die zweite Registerkarte bezieht sich auf die Begrenzung des Zeitplans, wenn die Richtlinie nicht rund um die Uhr gelten soll. Die dritte Registerkarte listet die Gruppen auf, denen die Richtlinie zugewiesen wurde.

Im Folgenden werden die einzelnen Arten der Richtlinien beschrieben sowie allgemeine Beispiele zur Festlegung der einzelnen Arten gegeben.

☐ **Richtlinien zum Festplattenschutz**

Das Ziel der Richtlinie zum Festplattenschutz besteht darin, ausgewählte Laufwerke vor schädlichen Änderungen zu schützen und ein Roll-Back durchführen zu können. Das bedeutet, dass ein früherer Zustand wiederhergestellt werden kann. Dadurch werden alle neuen Programme und Einstellungen entfernt, die nach Inkrafttreten der Richtlinie zum Festplattenschutz implementiert wurden.

Beachten Sie, dass der Computer zur Aktivierung des Schutzes neu gestartet werden muss. So stellen Sie sicher, dass alle Änderungen erfasst wurden. Nach der Aktivierung sind alle Änderungen an der Konfiguration des Computers in einem virtuellen verborgenen Ordner gespeichert; Änderungen betreffen die Installation von Programmen, Registrierungseinträge und die Benutzeroberfläche. Beim Zurücksetzen auf einen früheren Stand (Roll-Back) wird der Inhalt des virtuellen Ordners gelöscht.

BEISPIEL: Richtlinie zum Festplattenschutz

Die erste Registerkarte mit dem Namen **Festplattenschutz** zeigt unter der Überschrift **Ausgewählte Laufwerke schützen** eine Liste der zu schützenden Laufwerke an. Wählen Sie die zu schützenden Laufwerke aus. Der Schutz wird nach dem Neustart des Computers wirksam.

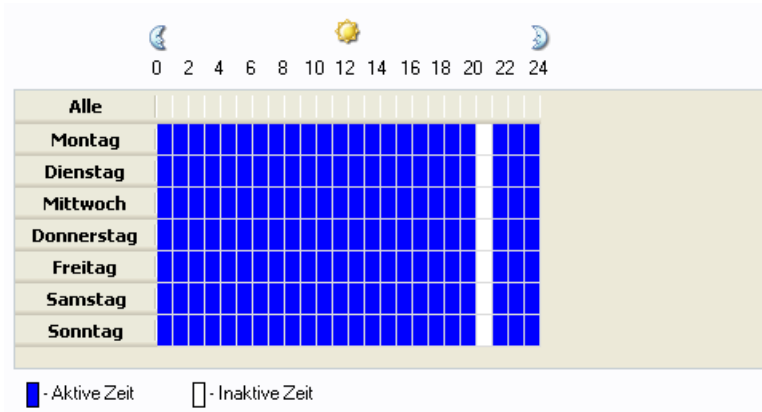
Die Einrichtung der Roll-Back-Funktionalität kann unabhängig vom Zeitpunkt, zu dem der Laufwerkschutz eingerichtet wird, erfolgen. Wählen Sie **Wiederherstellen bei Neustart aktivieren**, und beim nächsten Neustart des Computers wird der Inhalt des virtuellen Ordners gelöscht und der Computer auf den Stand zurückgesetzt, als der Schutz zum ersten Mal aktiviert wurde.

Bestimmte Ordner und Prozesse, wie zum Beispiel Antivirenprogramme oder Service Packs, sollten nicht zurückgesetzt werden. Ordner und Prozesse können vom Roll-Back ausgeschlossen werden, indem sie zu den Ausnahmelisten hinzugefügt werden.

Für eine täglich geplante Wiederherstellung der Festplatte, deaktivieren Sie den

Richtlinien definieren und übernehmen

Festplattenschutz für eine bestimmte Zeitspanne (zum Beispiel zwischen 20 und 21 Uhr).



Computer mit aktivierter Festplatten-Richtlinie werden dann jede Nacht um 20 Uhr wiederhergestellt.

Um die Richtlinie zu aktivieren, klicken Sie auf **Übernehmen**, oder klicken Sie auf **OK**, um die Richtlinie zu aktivieren und das Fenster zu schließen.

☐ Richtlinien zum Gerätezugriff

Das Ziel einer Richtlinie zum Gerätezugriff besteht darin, den Zugriff auf verschiedene Arten interner und externer Geräte zu definieren, um sie beispielsweise vor bösartigen Programmen zu schützen, die das Unternehmensnetzwerk infizieren, oder um das Kopieren von Unternehmensdaten auf externe Geräte zu unterbinden. Die erste Registerkarte mit dem Namen **Gerätezugriff** listet Gerätetypen auf, auf die die Richtlinien angewendet werden können. Klicken Sie mit der rechten Maustaste auf einen Gerätetyp, um die verfügbaren Optionen anzuzeigen:

- Für **USB-Geräte** können Sie vollen Zugriff gewähren, oder die Einstellung **Kein Zugriff** festlegen und dann eine Weiße Liste definieren. Dies ermöglicht dem IT-Administrator eine hohe Flexibilität bei der genauen Definition der für das Unternehmen erforderlichen USB-Richtlinie.
- Bei **Festplatte** sind die möglichen Optionen **Vollzugriff, Lesen, Schreiben, Formatieren** oder **Kein Zugriff**. Zusätzlich können Sie genauere Zugriffsrechte für jede einzelne Festplatte definieren, sowie Angaben zu Ordnern und Dateien, die verborgen werden sollen.

Zugriffsmatrix

Die untere Tabelle zeigt die Zugriffsarten an, die für die verschiedenen Gerätetypen gewährt werden können.

Möglicher Zugriff	Gerätetyp
Vollzugriff/Kein Zugriff/Weiße Liste	USB-Geräte, WiFi
Vollzugriff/Kein Zugriff oder Lesen, Schreiben, Formatieren, Dateien und Ordner verbergen	Festplatte
Vollzugriff/Kein Zugriff oder Lesen, Schreiben, Auswerfen	DVD/CD-ROM

Möglicher Zugriff	Gerätetyp
Vollzugriff/Kein Zugriff oder Lesen, Schreiben, Formatieren	Diskette, Wechselmedium
Vollzugriff/Kein Zugriff oder Auswerfen	Bandlaufwerke
Vollzugriff/Kein Zugriff	Bluetooth-Geräte, FireWire-Port, IrDA-Geräte, parallele Schnittstelle, serielle Schnittstelle, USB-Geräte, WiFi

BEISPIEL: DVD/CD-ROM

Klicken Sie auf der **Registerkarte Gerätezugriff** mit der rechten Maustaste auf **DVD/CD-ROM**, und wählen Sie **Zugriffsrechte** aus, um die Zugriffsoption **Lesen**, **Schreiben** oder **Auswerfen** zu aktivieren oder zu deaktivieren. **Vollzugriff** bedeutet, dass alle drei Zugriffsarten aktiviert werden. Werden alle drei Zugriffsarten deaktiviert, entspricht dies der Einstellung **Kein Zugriff**.

Um die Richtlinie zu aktivieren, klicken Sie auf **Übernehmen**, oder klicken Sie auf **OK**, um die Richtlinie zu aktivieren und das Fenster zu schließen.

BEISPIEL: USB-Geräte

Klicken Sie mit der rechten Maustaste auf **USB-Geräte**, und stellen Sie sicher, dass im Kontextmenü nicht die Einstellung **Vollzugriff** ausgewählt ist, sondern die Einstellung **Kein Zugriff**. Der unten gezeigte Bereich der Weißen Liste für USB ist nun verfügbar.

In der Weißen Liste für USB können Sie zwischen folgenden Einstellungen wählen:

- **Klassen hinzufügen:** Die Richtlinie deckt alle Arten von USB-Geräten ab, die zur ausgewählten Klasse gehören.
- **Geräte hinzufügen > Geräte hinzufügen:** Wählen Sie USB-Geräte aus der Datenbank, und fügen Sie diese zur Weißen Liste hinzu.
- **Geräte hinzufügen > Lokale Geräte hinzufügen:** Wählen Sie USB-Geräte am lokalen Computer, und fügen Sie diese zur Weißen Liste hinzu.
- **Geräte hinzufügen > Computer durchsuchen:** Durchsucht das Computernetzwerk nach USB-Geräten. Nach der Suche können Geräte ausgewählt und zur Weißen Liste hinzugefügt werden.

Alternativ können Sie auf die Schaltfläche **USB-Datenbank** klicken, um ein Fenster mit einer Liste von Geräten aus der USB-Datenbank und derselben oben beschriebenen Funktion zu öffnen.

BEISPIEL: Festplatte

Verwenden Sie die Funktion **Festplatte**, um Dateien und Ordner, wie zum Beispiel Musikdateien (MP3, MP4 oder WMA), zu verbergen. Das folgende Beispiel zeigt, wie MP3-Dateien verborgen werden.

1. Klicken Sie mit der rechten Maustaste auf **Festplatte**, und wählen Sie **Zugriff auf Datenträger**.
2. Wählen Sie ein oder mehrere Laufwerke, die Sie verbergen möchten.

Ein Laufwerk zu verbergen bedeutet, dass das Laufwerk weder für den Benutzer noch für das Betriebssystem sichtbar ist. Der nächste Schritt ist, diese Laufwerke

Richtlinien definieren und übernehmen

auszuschließen, so dass sie wieder sichtbar sind, und auf dieselbe Art und Weise schließen Sie auch MP3-Dateien von dieser Regelung aus. Sind MP3-Dateien nicht Teil der Ausnahme, bleiben sie verborgen.

3. Klicken Sie auf **Hinzufügen** , und wählen Sie **Von Festplatte hinzufügen**.
4. Geben Sie im Feld Ordner 'C:\' ein, oder gehen Sie an den entsprechenden Speicherort.
5. Geben Sie im Feld Dateitypen '*.mp3' ein, und wählen Sie die Option **Nur diese Dateitypen ausschließen** aus.

Das bedeutet, dass MP3-Dateien von der Ausnahme ausgeschlossen werden.

6. Wählen Sie **Unterordner einbeziehen** , und klicken Sie auf **OK**.

Das Ergebnis dieser Einstellungen ist, dass das Laufwerk C: sichtbar ist, alle MP3-Dateien aber verborgen sind.

Um die Richtlinie zu aktivieren, klicken Sie auf **Übernehmen** , oder klicken Sie auf **OK** , um die Richtlinie zu aktivieren und das Fenster zu schließen.

☐ Webrichtlinien

Das Ziel einer Webrichtlinie besteht darin, den Zugriff auf Websites zu unterbinden, die nicht für Geschäfts- oder Bildungszwecke geeignet sind. So wird das Unternehmens- oder Schulnetzwerk indirekt geschützt, da eine derartige Richtlinie das Herunterladen von Malware reduziert.

Klicken Sie auf der Registerkarte **Internet** auf die Einstellung **Alle verweigern** oder **Alle zulassen**, und definieren Sie anschließend Ausnahmen für die allgemeine Strategie. Wir empfehlen, zuerst mit der Erstellung einer Liste **Benutzerdefiniert** zu beginnen, da diese Liste für alle weiteren Webrichtlinien grundlegend ist und für die Erstellung der **Ausnahme** -Liste für jede einzelne Webrichtlinie verwendet werden kann. Die Liste **Benutzerdefiniert** wird erstellt, indem Schlüsselwörter oder vollständige Links hinzugefügt werden, nachdem Sie auf **Hinzufügen** in der rechten unteren Ecke geklickt haben.

BEISPIEL: Webrichtlinie

1. Wählen Sie die Einstellung **Alle zulassen** , und fügen Sie als Ausnahme das Wort „XXX“ hinzu. Diese Webrichtlinie sperrt alle Links, die das Wort XXX enthalten.
2. Um die Richtlinie zu aktivieren, klicken Sie auf **Übernehmen** , oder klicken Sie auf **OK** , um die Richtlinie zu aktivieren und das Fenster zu schließen.

☐ Anwendungsrichtlinien

Das Ziel einer Anwendungsrichtlinie besteht darin, die Verwendung von Anwendungen zu unterbinden, die nicht für Geschäfts- oder Bildungszwecke geeignet sind. So wird das Unternehmens- oder Schulnetzwerk indirekt geschützt, da eine derartige Richtlinie die Verwendung unzulässiger und somit potenziell gefährlicher Anwendungen reduziert.

Klicken Sie auf der Registerkarte **Anwendung** auf die Einstellung **Alle verweigern** oder **Alle zulassen**, und definieren Sie anschließend Ausnahmen für die allgemeine Strategie. Die Liste Anwendungen enthält gruppierte Standardanwendungen in den Ordnern **Desktop**, **Startmenü** und **Standardprogrammverzeichnis**; Sie können auch Ihre eigene Liste **Benutzerdefiniert** erstellen. Diese vier Ordner sind grundlegend für alle erstellten Anwendungsrichtlinien und können bei der Erstellung der **Ausnahme** -Liste für jede einzelne Webrichtlinie verwendet werden.

BEISPIEL: Anwendungsrichtlinie

1. Wählen Sie die Einstellung **Alle zulassen** , und fügen Sie als Ausnahme das Wort „YYY“ hinzu. Diese Anwendungsrichtlinie sperrt anschließend die Anwendung YYY.
2. Um die Richtlinie zu aktivieren, klicken Sie auf **Übernehmen** , oder klicken Sie auf **OK** , um die Richtlinie zu aktivieren und das Fenster zu schließen.

5.2 Eine Richtlinie erstellen

1. Wählen Sie im Fenster **Richtlinieneditor** die Option **Richtlinien**, klicken Sie mit der rechten Maustaste auf die zu erstellende Richtlinienkategorie, zum Beispiel **Anwendungsrichtlinien**, und wählen Sie **Neue Richtlinie**.

Es wird eine neue Richtlinie mit einem Standardnamen erstellt.

2. Geben Sie einen geeigneten Namen für die Richtlinie ein.

Sobald die Richtlinie erstellt wurde, können Sie die Eigenschaften festlegen. Informationen zum Definieren von Richtlinien finden Sie unter [Eine Richtlinie zum Festplattenschutz definieren](#), [Eine Richtlinie zum Gerätezugriff definieren](#), [Eine Webrichtlinie definieren](#) oder [Eine Anwendungsrichtlinie definieren](#).

5.3 Eine Richtlinie zum Festplattenschutz definieren

Um eine Richtlinie zum Festplattenschutz zu definieren, erstellen Sie zunächst die Richtlinie. Anweisungen hierzu finden Sie unter [Eine Richtlinie erstellen](#).

1. Öffnen Sie eine bestehende Richtlinie, indem Sie im Verzeichnis **Richtlinien zum Festplattenschutz** auf die gewünschte Richtlinie doppelklicken.

Die Richtlinieneigenschaften werden auf drei Registerkarten im Datenfenster angezeigt.

2. Legen Sie die Eigenschaften auf den Registerkarten **Festplattenschutz** und **Zugewiesen** fest.

Beschreibungen zu den Optionen auf den zwei Registerkarten finden Sie unter [Registerkarte "Festplattenschutz"](#), [Registerkarte "Zeitplan"](#) und [Registerkarte "Zugewiesen"](#).

3. Nachdem Sie die Richtlinie definiert haben, klicken Sie auf die Schaltfläche **Übernehmen** , um die Änderungen zu speichern.

Computer neustarten, nachdem eine Richtlinie übernommen wurde

Wurde eine Richtlinie zum Festplattenschutz definiert und übernommen, müssen die Computer, auf denen die Richtlinie übernommen wurde, neu gestartet werden, um einen eindeutigen Wiederherstellungspunkt der Computer und die Datenkonsistenz der Festplatte zu gewährleisten.

Der erforderliche Neustart wird durch ein gelbes Hinweissymbol unten im Dialog angezeigt.

- Klicken Sie im Dropdown-Menü **Neustart** auf **Neustarten und Änderungen der Richtlinien übernehmen**.

Der Befehl ist nur verfügbar, wenn die Richtlinie mindestens einer Gruppe mit tatsächlichen Mitgliedern zugewiesen wurde.

Richtlinien definieren und übernehmen

Diese Option ist nützlich, wenn Richtlinien zum ersten Mal definiert oder bestehende Richtlinien aktualisiert werden. Wenn beispielsweise in der ersten Richtlinie definiert wurde, dass das Laufwerk C: geschützt wird, könnte ein Update den Ordner "Eigene Dateien" vom Schutz ausschließen.

Wenn Sie an Agentcomputer einen Befehl zum Neustart senden, können Sie eine Nachricht definieren, die vor dem Neustart auf den entsprechenden Computern angezeigt werden soll. Zum Beispiel:

Ihr Computer wird in 2 Minuten neu gestartet. Speichern Sie Ihre Dateien.

Das Zeitintervall vor dem Neustart kann ebenfalls festgelegt werden. Diese Einstellungen festlegen:

- Klicken Sie im Dropdown-Menü **Neustart** auf **Optionen für Neustart**.

Wenn zuvor eine Richtlinie übernommen wurde, kann der Neustart auch ein Rollback auf den vorherigen Wiederherstellungspunkt beinhalten. Das bedeutet, wenn der Computer neu startet, werden alle Änderungen wie installierte oder entfernte Programme rückgängig gemacht, und der Computer wird wieder auf den vorherigen Stand zurückgesetzt.

- Klicken Sie im Dropdown-Menü **Neustart** auf **Neustarten, Wiederherstellen und Änderungen der Richtlinien übernehmen**.

Diese Option ist nützlich in Umgebungen, in denen Benutzer häufig unerwünschte Änderungen vornehmen, wie z. B. in PC-Räumen von Schulen oder in Umgebungen, wo Computer öffentlich zur Verfügung stehen, wie in Hotels oder Internetcafés.

5.4 Eine Richtlinie zum Gerätezugriff definieren

Um eine Gerätezugriffsrichtlinie zu definieren, erstellen Sie zunächst die Richtlinie. Anweisungen finden Sie im Abschnitt [Eine Richtlinie erstellen](#).

1. Öffnen Sie eine bestehende Richtlinie durch einen Doppelklick auf diese im Verzeichnis **Gerätezugriffsrichtlinien**.

Die Richtlinieneigenschaften werden auf drei Registerkarten im Datenfenster angezeigt.

2. Legen Sie die Eigenschaften auf den Registerkarten **Anwendung**, **Zeitplan** und **Zugewiesen** fest.

Beschreibungen zu den Optionen auf den Registerkarten finden Sie in den Abschnitten [Registerkarte "Gerätezugriff"](#), [Registerkarte "Zeitplan"](#) und [Registerkarte "Zugewiesen"](#).

3. Nachdem Sie die Richtlinie definiert haben, klicken Sie auf die Schaltfläche **Übernehmen**, um die Änderungen anzunehmen.

Sehen Sie hierzu auch:

[Zugriffsrechte pro Gerätetyp definieren](#)

[Zugriffsrechte pro Einzelgerät definieren](#)

[Zugriffsrechte für USB-Laufwerke definieren](#)

[Inhalt einer Festplatte verbergen](#)

5.5 Richtlinien zum Gerätezugriff

5.5.1 Zugriffsrechte pro Gerätetyp definieren

1. Wählen Sie im Bereich der Liste **Berechtigungen** einen Gerätetyp aus, für den Sie Zugriffsrechte definieren möchten.

Standardmäßig ist allen Gerätetypen der Vollzugriff zugewiesen.

2. Klicken Sie mit der rechten Maustaste auf den Typ, und wählen Sie im Kontextmenü die Option **Zugriffsberechtigungen** aus.
3. Aktivieren oder deaktivieren Sie im Dialogfeld **Zugriffsberechtigungen** die entsprechenden Kontrollkästchen.

In diesem Dialogfeld können Sie für die einzelnen Gerätetypen unterschiedliche Optionen auswählen. Grundsätzlich enthält das Dialogfeld die Option **Aktivieren**, die Sie auswählen sollten, um das Gerät verfügbar zu machen. Es können jedoch noch weitere Kontrollkästchen angezeigt werden:

- Für DVD-/DC-ROM- und Tape-Laufwerke ist die Option **Auswerfen** verfügbar, über die Sie das Öffnen der Laufwerke und Entfernen der Datenträger zulassen oder verhindern können.
- Für Disketten, externe Festplatten, DVDs/CDs, CD/DVD-RW und Wechseldatenträger sind außerdem die Optionen **Lesen**, **Schreiben** und **Formatieren** verfügbar, um Lese-, Schreibe- und Formatierungsvorgänge zuzulassen oder zu verhindern.

Bei Auswahl eines Gerätetyps im obersten Fenster sind all diese Optionen außerdem über das Kontextmenü verfügbar.

4. Drücken Sie auf OK, um Änderungen zu speichern.

Hinweis

Bei Festlegung von Berechtigungen für WiFi- und Bluetooth Adapter in einer Richtlinie zum Gerätezugriff werden bereits bestehende Verbindungen nicht unterbrochen.

Siehe auch:

[Zugriffsrechte pro Einzelgerät definieren](#)

[Zugriffsrechte für ein USB-Laufwerk definieren](#)

[Inhalt einer Festplatte verbergen](#)

5.5.2 Zugriffsrechte pro Einzelgerät definieren

1. Wählen Sie im Bereich der Liste **Berechtigungen** den Gerätetyp aus, zu dem Ihr Gerät gehört.

Daraufhin wird im unteren Fensterbereich die vollständige Liste von Geräten dieses Typs angezeigt.

2. Wählen Sie das Gerät, für das Sie Zugriffsberechtigungen festlegen möchten.

Um die Liste auf die Geräte zu begrenzen, die nur auf dem Administratorcomputer verfügbar sind, aktivieren Sie das Kontrollkästchen Nur verfügbare Geräte anzeigen.

3. Klicken Sie mit der rechten Maustaste auf das Gerät, und wählen Sie im Kontextmenü die Option **Zugriffsberechtigungen** aus.

Das Dialogfeld **Zugriffsberechtigungen** für Einzelgeräte ist mit dem Dialogfeld für

Richtlinien definieren und übernehmen

entsprechende Gerätetypen identisch.

4. Aktivieren oder deaktivieren Sie im Dialogfeld **Zugriffsberechtigungen** die entsprechenden Kontrollkästchen.

Wenn Sie die Zugriffsberechtigungen für ein einzelnes Gerät ändern, ändert sich der Zugriff für dessen Gerätetyp zu **Benutzerdefiniert**, und die Einstellungen auf Gerätetypenebene werden gelöscht. Die Zugriffsberechtigungen für die übrigen Geräte dieses Typs bleiben unverändert.

Denken Sie daran, dass unten im Bereich **Berechtigungen** entweder sämtliche oder – wenn das Kontrollkästchen **Nur verfügbare Geräte anzeigen** aktiviert ist – nur die zurzeit auf dem Administratorcomputer installierten Geräte angezeigt werden. Um Zugriffsberechtigungen für weitere Geräte dieses Typs zu definieren, die nicht auf dem Administratorcomputer, aber auf den Agentcomputern installiert sind, verwenden Sie die Option **Andere**.

Hinweis

Berechtigungen für WiFi- und Bluetooth Adapter in einer Gerätezugriffsrichtlinie haben keine Auswirkungen auf bereits bestehende Verbindungen.

Siehe auch:

[Zugriffsrechte pro Gerätetyp definieren](#)

[Zugriffsrechte für ein USB-Laufwerk definieren](#)

[Inhalt einer Festplatte verbergen](#)

5.5.3 Zugriffsrechte für ein USB-Laufwerk definieren

Hinweis

Die folgenden Erläuterungen gelten nur für USB-Geräte.

Der Zugriff auf USB-Geräte kann für einen ganzen USB-Gerätetyp zugelassen oder verweigert werden. Doch selbst, wenn der Zugriff auf einen ganzen USB-Gerätetyp verweigert wird, können Sie den Zugriff auf ausgewählte USB-Geräte oder USB-Geräteklassen mithilfe von Weißen Listen für USB und der USB-Datenbank zulassen.

Eine Weiße Liste für USB umfasst USB-Geräte und USB-Geräteklassen, auf die zugegriffen werden kann, auch wenn eine Richtlinie zum Gerätezugriff den Zugriff auf den USB-Gerätetyp insgesamt verweigert. Für jede Richtlinie zum Gerätezugriff kann eine eigene Weiße Liste definiert werden. Weiße Listen können in CSV-Dateien exportiert oder aus CSV-Dateien importiert werden. Geräte können aus der USB-Datenbank oder mithilfe der unten stehenden Vorgehensweisen zur Weißen Liste hinzugefügt werden.

Die USB-Datenbank enthält Informationen zu USB-Geräten. Sie dient der einfachen und bequemen Erstellung von Weißen Listen; Einträge aus der Datenbank werden einfach in die Weiße Liste übertragen. Die Datenbank kann in eine CSV-Datei exportiert oder aus einer CSV-Datei importiert werden. Grundsätzlich kann die Datenbank folgendermaßen befüllt werden:

- Durch Hinzufügen von Informationen über USB-Geräte, die entweder zurzeit oder in der Vergangenheit mit dem Administratorcomputer verbunden sind/waren.
- Durch Durchsuchen aller Netzwerkcomputer mithilfe des Agents, um Geräte zu finden, die mit diesen Computern bisher verbunden waren.

Außerdem können Sie die USB-Datenbank manuell befüllen, indem Sie die CSV-Datei

bearbeiten. Das Importieren von Daten aus anderen CSV-Dateien wird ebenfalls unterstützt. Die Daten in einer CSV-Datei weisen folgendes Format auf:

;USB\Vid_4102&Pid_1007&Rev_0001;iriver Internet Audio Player IFP-700;USB\Class_ff&SubClass_ff&Prot_ff;04/04/2006 12:56:32
;USB\Vid_03f0&Pid_1016&Rev_0000;HP USB Sync;USB\Class_ff&SubClass_ff&Prot_ff;04/04/2006 12:56:32
;USB\Vid_045e&Pid_001c&Rev_0500;Microsoft Integrated USB Hub;USB\Class_09&SubClass_00&Prot_00;04/04/2006 12:56:32
;USB\Vid_045e&Pid_0095&Rev_0424;USB Human Interface Device;USB\Class_03&SubClass_01&Prot_02;04/04/2006 12:56:32
;USB\Vid_046e&Pid_5100&Rev_0800;USB Human Interface Device;USB\Class_03&SubClass_01&Prot_01;04/04/2006 13:11:41

Sie bestehen aus folgenden Informationen, die durch ein Semikolon (;) getrennt sind:

- Geräteerkennung;
- Gerätebeschreibung;
- Geräteklasse;
- Datum und Zeitpunkt der Geräteerkennung.

Jede Kennung (zum Beispiel USB\Vid_4102&Pid_1007&Rev_0001) enthält die folgenden, durch "\" und "&" getrennten Informationen:

Beispiel	Beschreibung
USB	Gerätetyp, immer USB.
Vid_4102	Hersteller-ID: Diese individuelle ID wird dem Gerätehersteller vom USB Implementers Forum, Inc. (www.usb.org) zugewiesen. Wenden Sie sich an diese Organisation, um die Hersteller-ID anzufordern.
Pid_1007	Produkt-ID: Jedes Produkt hat eine vom Hersteller ausgewiesene Identifikationsnummer. Wenden Sie sich an den Hersteller, um die Produkt-ID anzufordern.
Rev_0001	Revisionsnummer des Produkts. Diese Information können Sie ebenfalls über den Hersteller beziehen.

Standardmäßig wird einem USB-Gerätetyp bei Erstellung einer neuen Gerätezugriffsrichtlinie der **Vollzugriff** zugewiesen, und die Weiße Liste ist leer. Wenn Sie den Zugriff auf den gesamten USB-Gerätetyp verweigern möchten und eine Zugriffsberechtigung pro USB-Geräteklasse und Einzelgerät zuweisen möchten, gehen Sie folgendermaßen vor:

1. Deaktivieren Sie den gesamten USB-Gerätetyp (siehe [Zugriffsrechte pro Gerätetyp definieren](#)).
2. Erstellen Sie die Weiße Listeder USB-Geräte und USB-Geräteklassen, auf die immer zugegriffen werden darf.

Wählen Sie dazu auf der Registerkarte **Gerätezugriff** im Bereich **Berechtigungen** die Option **USB-Geräte** aus. Die Weiße Liste für USB wird unten auf der Registerkarte **Gerätezugriff** angezeigt. Bei neu erstellten Richtlinien ist diese Liste leer.

Siehe auch:

[Eine USB-Geräteklasse zur Weißen Liste hinzufügen](#)

[Ein USB-Gerät zur Weißen Liste hinzufügen](#)

[Mit der USB-Datenbank arbeiten](#)

5.5.4 Zugriffsrechte für ein WiFi-Gerät definieren

Der Zugriff auf ein drahtloses lokales Netzwerk (WLAN), oder WiFi, kann entweder vollständig oder gar nicht zugelassen werden. Auf der Registerkarte **Gerätezugriff** kann **Zugriff** entweder auf "Kein Zugriff" oder auf "Vollzugriff" eingestellt werden:

- Klicken Sie mit der rechten Maustaste auf den WiFi-Gerätetyp, und klicken Sie auf **Vollzugriff**. Die Einstellung wechselt zwischen "Kein Zugriff" oder "Vollzugriff".

Wenn "Kein Zugriff" eingestellt wurde, wird unten auf der Registerkarte **Gerätezugriff** die Weiße Liste angezeigt. Verwenden Sie die Weiße Liste, um Benutzern den Zugriff auf ein oder mehrere bestimmte drahtlose Netzwerke zu gewähren.

Ein WiFi-Gerät zur Weißen Liste hinzufügen:

- Klicken Sie auf die Schaltfläche **Hinzufügen**, und geben Sie den Netzwerknamen des drahtlosen Geräts, z. B. "MeinDrahtloses", ein.

5.5.5 Inhalt einer Festplatte verbergen

Hinweise

- Die folgenden Erläuterungen gelten nur für Festplattengeräte.
- Werden Inhalte verbergen, können Benutzer Programme und Dateien in verborgenen Ordnern weder *sehen* noch *verwenden*. Netop ProtectOn Pro stellt jedoch sicher, dass das Laufwerk, auf dem das Betriebssystem installiert ist, nicht verbergen werden kann. Die vom Betriebssystem angeforderten Ordner und Dateien bleiben sichtbar und behalten ihre volle Funktionalität.

Für Festplatten können Sie nicht nur Zugriffsrechte pro Gerätetyp und Einzelgerät festlegen, sondern auch den Inhalt der Festplatten auf Agentcomputern vor ihren Benutzern verbergen. Netop ProtectOn Pro ermöglicht Ihnen, entweder ganze Laufwerke zu verbergen oder Ausnahmeordner zu bestimmen, deren Inhalt von Benutzern angezeigt werden kann.

Wenn Sie z. B. einen Computerraum verwalten, in dem alle Computer ein C-Laufwerk mit Betriebssystem und Programmdateien und ein D-Laufwerk mit einem Ordner "Work" haben, in dem Studenten und andere Benutzer ihre Arbeit speichern sollen, können Sie für Laufwerk C einen Schreibschutz aktivieren und den Inhalt des D-Laufwerks mit Ausnahme des Ordners **Work** verbergen. So stellen Sie sicher, dass die Studenten und anderen Benutzer ihre Dateien nur im Ordner "Work" speichern.

Inhalte der auf einem Agentcomputer installierten Festplatten vor Benutzern dieses Computers verbergen

1. Klicken Sie in der Liste **Berechtigungen** mit der rechten Maustaste auf **Festplatte**, und wählen Sie im Kontextmenü **Zugriff auf Datenträger**.
2. Führen Sie im Dialogfeld **Zugriff auf Datenträger** folgende Aktionen durch:
 - Wählen Sie aus der Liste **Ausgewählte Laufwerke verbergen** die Laufwerke aus, die Sie vor den Benutzern verbergen möchten.
 - Klicken Sie auf die Schaltfläche **Hinzufügen**, und wählen Sie **Von Festplatte hinzufügen**, um die Laufwerke auszuwählen, die nicht vor dem Benutzer verbergen werden sollen.

Benutzer können nur den Inhalt dieses Verzeichnisses und seiner Unterverzeichnisse sehen (falls diese Option aktiviert ist). Sollen die Benutzer zum Beispiel Lehrmaterialien im Verzeichnis `C:\Unterrichtsmaterialien\Unterstufe\Biologie` anzeigen dürfen, fügen Sie diesen Ordner zur Liste der Ausnahmeordner hinzu, damit die Benutzer den Inhalt des Unterordners "Biologie" sehen können. Der Inhalt der Ordner `Unterrichtsmaterialien` und `Unterstufe` bleibt nach wie vor verborgen.

5.5.6 Mit der USB-Datenbank arbeiten

1. Wählen Sie in der Liste **Berechtigungen USB-Geräte** aus und klicken Sie auf die Schaltfläche **USB-Datenbank**.

Das Dialogfeld **USB-Datenbank** wird geöffnet und zeigt eine Liste der USB-Datenbankinhalte an.

Um Einträge zur Datenbank hinzuzufügen, stehen zwei Optionen zur Verfügung:

- Klicken Sie auf **Lokale Geräte hinzufügen**, um auf dem Computer verfügbare Geräte hinzuzufügen.
- Klicken Sie auf **Computer durchsuchen**, um Netzwerkcomputer nach Geräten zu durchsuchen.

Um ein Gerät aus der USB-Datenbank zu löschen, wählen Sie es in der Liste aus und klicken Sie auf **Löschen**.

Um eine USB-Datenbank aus einer CSV-Datei zu importieren, klicken Sie auf **Laden** und wählen Sie die Datei aus, die die Datenbank enthält.

Um eine USB-Datenbank in eine CSV-Datei zu exportieren, klicken Sie auf **Speichern** und geben Sie den Namen der Datenbankdatei ein.

2. Klicken Sie auf **OK** im Dialogfeld **USB-Datenbank**.
3. Klicken Sie auf der Registerkarte **Gerätezugriff** auf **Übernehmen**, um die Änderungen zu speichern.

Siehe auch:

[Zugriffsrechte pro Gerätetyp definieren](#)

[Zugriffsrechte pro Einzelgerät definieren](#)

[Inhalt einer Festplatte verbergen](#)

5.5.7 Eine USB-Geräteklasse zu einer Weißen Liste hinzufügen

1. Klicken Sie auf die Schaltfläche **Klassen hinzufügen**.

Die Schaltflächen **Klassen hinzufügen** und **Geräte hinzufügen** sind nicht verfügbar, wenn den USB-Geräten Vollzugriff gewährt wurde. Klicken Sie in der Liste **Berechtigungen** auf **USB-Geräte**, und stellen Sie sicher, dass die Einstellung **Vollzugriff** nicht ausgewählt ist.

2. Wählen Sie im Dialogfeld **USB-Klasse auswählen** eine oder mehrere Klassen, und klicken Sie auf **Hinzufügen**.

Enthält die Weiße Liste bereits Geräte der Klasse oder Klassen, die Sie hinzufügen möchten, werden Sie in einer Systemmeldung darüber informiert. Diese einzelnen Geräte werden aus der Liste entfernt, und die gesamte Klasse wird stattdessen zugelassen.

3. Klicken Sie auf der Registerkarte **Gerätezugriff** auf **Übernehmen**, um die Änderungen

zu speichern.

Siehe auch:

[Zugriffsrechte pro Gerätetyp definieren](#)

[Zugriffsrechte pro Einzelgerät definieren](#)

[Inhalt einer Festplatte verbergen](#)

5.5.8 Ein USB-Gerät zu einer Weißen Liste hinzufügen

Um ein Einzelgerät oder mehrere Geräte zur Weißen Liste hinzuzufügen, klicken Sie auf die Schaltfläche **Geräte hinzufügen**, und wählen Sie einen der drei verfügbaren Befehle:

☐ Geräte hinzufügen

- Wählen Sie das Gerät, das Sie hinzufügen möchten, und klicken Sie auf die Schaltfläche **Hinzufügen**.

Wenn die benötigten Geräte in der USB-Datenbank nicht verfügbar sind, können Sie sie für einen späteren schnelleren Zugriff hinzufügen. Weitere Informationen zum Hinzufügen von Geräten zur USB-Datenbank erhalten Sie unter [Mit der USB-Datenbank arbeiten](#).

☐ Lokale Geräte hinzufügen

Die Liste zeigt Geräte an, die derzeit an den Computer angeschlossen sind. Sie können die Liste durch Geräte ergänzen, die bereits am Computer angeschlossen waren, indem Sie das Kontrollkästchen **Alle lokalen Geräte anzeigen** aktivieren.

- Wählen Sie die Geräte aus, die der Weißen Liste hinzugefügt werden sollen, und klicken Sie auf **OK**.

☐ Computer durchsuchen

1. Wählen Sie aus, ob nur bestimmte Computer, oder alle Computer durchsucht werden sollen.

2. Klicken Sie auf **Jetzt durchsuchen**, um die Suche zu starten.

Wenn Sie das gesamte Netzwerk durchsuchen, kann dies recht zeitaufwändig sein. Nach der Suche werden die erkannten USB-Geräte in der Liste **Gefundene USB-Geräte** angezeigt.

3. Wählen Sie in der Liste **Gefundene USB-Geräte** die Geräte, die Sie hinzufügen möchten, und klicken Sie auf **Hinzufügen**.

Sind die USB-Geräteklassen, zu denen die Geräte gehören, bereits in der Weißen Liste vorhanden, werden Sie in einer Systemmeldung darüber informiert. Die ausgewählten Geräte werden nicht zur Weißen Liste hinzugefügt, da sie bereits als Teil ihrer Klassen zugelassen sind.

Siehe auch:

[Zugriffsrechte pro Gerätetyp definieren](#)

[Zugriffsrechte pro Einzelgerät definieren](#)

[Inhalt einer Festplatte verbergen](#)

5.6 Eine Webrichtlinie definieren

Um eine Webrichtlinie zu definieren, erstellen Sie zunächst die Richtlinie. Anweisungen finden Sie im Abschnitt [Eine Richtlinie erstellen](#).

1. Öffnen Sie eine bestehende Richtlinie, indem Sie im Verzeichnis **Webrichtlinien** auf die gewünschte Richtlinie doppelklicken.

Die Richtlinieneigenschaften werden auf drei Registerkarten im Datenfenster angezeigt.

2. Legen Sie die Eigenschaften auf den Registerkarten **Internet** , **Zeitplan** und **Zugewiesen** fest.

Beschreibungen zu den Optionen auf den Registerkarten finden Sie in den Abschnitten [Registerkarte "Internet"](#), [Registerkarte "Zeitplan"](#) und [Registerkarte "Zugewiesen"](#).

3. Nachdem Sie die Richtlinie definiert haben, klicken Sie auf die Schaltfläche **Übernehmen**, um die Änderungen zu speichern.

5.7 Eine Anwendungsrichtlinie definieren

Um eine Anwendungsrichtlinie zu definieren, erstellen Sie zunächst die Richtlinie. Anweisungen finden Sie im Abschnitt [Eine Richtlinie erstellen](#).

1. Öffnen Sie eine bestehende Richtlinie, indem Sie im Verzeichnis **Anwendungsrichtlinien** auf die gewünschte Richtlinie doppelklicken.

Die Richtlinieneigenschaften werden auf drei Registerkarten im Datenfenster angezeigt.

2. Legen Sie die Eigenschaften auf den Registerkarten **Anwendung** , **Zeitplan** und **Zugewiesen** fest.

Beschreibungen zu den Optionen auf den Registerkarten finden Sie in den Abschnitten [Registerkarte "Anwendung"](#), [Registerkarte "Zeitplan"](#) und [Registerkarte "Zugewiesen"](#).

3. Nachdem Sie die Richtlinie definiert haben, klicken Sie auf die Schaltfläche **Übernehmen**, um die Änderungen zu speichern.

5.8 Gültige Richtlinien für ein Gruppenmitglied anzeigen

So erhalten Sie Informationen zu gültigen Richtlinien für Gruppenmitglieder:

1. Suchen Sie das gewünschte Gruppenmitglied im Fenster **Richtlinieneditor** unter **Gruppen**.
2. Klicken Sie mit der rechten Maustaste auf das Mitglied, und wählen Sie im Kontextmenü **Gültige Richtlinien anzeigen** aus.

Im Datenfenster werden Informationen zu den Richtlinien angezeigt, die diesem Gruppenmitglied zugewiesen wurden. Die Liste der gültigen Richtlinien enthält eine kurze Beschreibung jeder Richtlinie. Doppelklicken Sie auf eine Richtlinie, um ausführlichere Informationen zu dieser Richtlinie im Datenfenster anzuzeigen.

5.9 Eine Richtlinie umbenennen, kopieren oder löschen

Eine Richtlinie umbenennen

1. Klicken Sie im Fenster **Richtlinieneditor** mit der rechten Maustaste auf die Richtlinie, die Sie umbenennen möchten, und wählen Sie **Umbenennen**.
2. Geben Sie einen geeigneten Namen für die Richtlinie ein.

Eine Richtlinie kopieren

Über das Kopieren einer Richtlinien können Sie eine Richtlinie auf Basis einer bereits vorhandenen Richtlinie erstellen. Dies erspart Ihnen die Mühe, eine neue Richtlinie zu erstellen. Die Kopie einer alten Richtlinie enthält dieselben Einstellungen wie die alte Richtlinie. Sie muss nur noch umbenannt werden.

1. Klicken Sie im Fenster **Richtlinieneditor** mit der rechten Maustaste auf die Richtlinie, die Sie kopieren möchten, und wählen Sie **Kopieren**.

Es wird eine neue Richtlinie mit einem Standardnamen erstellt.

2. Geben Sie einen geeigneten Namen für die Richtlinie ein.

Eine Richtlinie löschen

Wenn eine Richtlinie nicht mehr verwendet wird, können Sie sie löschen. Es gibt keine Einschränkungen beim Löschen einer Richtlinie; eine Richtlinie kann gelöscht werden, wenn sie einer Gruppe zugewiesen wurde.

1. Klicken Sie im Fenster **Richtlinieneditor** mit der rechten Maustaste auf die zu löschende Richtlinie, und wählen Sie **Löschen**.

Ein Dialogfeld wird geöffnet, das Sie zur Bestätigung des Löschvorgangs auffordert.

2. Klicken Sie auf **Ja**, um das Löschen der Richtlinie zu bestätigen.

5.10 Registerkarten zu Richtlinien

5.10.1 Registerkarte Festplattenschutz

Über die Registerkarte **Festplattenschutz** können Sie zu schützende Festplattenlaufwerke auswählen, Ausnahmeordner festlegen, in denen dauerhafte Änderungen zulässig sind, und Prozesse hinzufügen, die dauerhafte Änderungen an Festplatten vornehmen dürfen.

Die Registerkarte umfasst die folgenden Bereiche:

Ausgewählte Laufwerke schützen	Zu schützende Laufwerke: Die Geräteliste enthält Buchstaben von C bis Z. Bei Auswahl von Laufwerken, die keine Festplatten auf den Agentcomputern sind, wird diese Einstellung ignoriert.
Wiederherstellen aktivieren	Wählen Sie Wiederherstellen bei Neustart aktivieren , um alle vorgenommenen Änderungen an den im Bereich Ausgewählte Laufwerke schützen ausgewählten Laufwerken nach dem Neustart zu entfernen.

Hinweis

Wenn Sie Laufwerke auswählen, die geschützt werden sollen, aber das Wiederherstellen bei Neustart nicht aktivieren, werden die von Benutzern vorgenommenen Änderungen nicht zurückgesetzt. Wenn Sie das Wiederherstellen über längere Zeit nicht aktivieren, kann sich die Systemleistung reduzieren. Verwenden Sie in diesem Fall die Option **Wiederherstellen bei Neustart aktivieren**, um die Änderungen zu entfernen.

Schaltfläche "Neustart" mit folgenden Optionen:

Neustarten, Wiederherstellen und Änderungen der Richtlinien übernehmen

Fahren Sie Computer, auf denen die Richtlinie angewendet wird, herunter, führen Sie ein Roll-Back der Festplatte auf den letzten Wiederherstellungspunkt durch, und wenden Sie die Richtlinie an.

Neustarten und Änderungen der Richtlinien übernehmen

Fahren Sie die Computer, auf denen die Richtlinie angewendet wird, herunter, und wenden Sie die Richtlinie an.

Optionen für Neustart

Legen Sie Standardeinstellungen zum Neustart von Agentcomputern fest:

- Zeitintervall vor den Neustart
- Benachrichtigung, die die Benutzer vor dem Neustart ihrer Computer erhalten
- Abbrechen des Neustartbefehls durch Benutzer zulassen
- Sollen die Agentcomputer auch wiederhergestellt werden?

Die Einstellungen werden verwendet, wenn Sie in der Symbolleiste auf "Agentcomputer erneut starten" klicken oder mit der rechten Maustaste im Richtlinieneditor auf eine Richtlinie zum Festplattenschutz klicken.

Ausnahmeordner Ordner, in denen dauerhafte Änderungen zulässig sind.

Die folgenden Befehle sind über die Schaltfläche **Hinzufügen** verfügbar: Verwenden Sie **Hinzufügen**, um einen Ordnernamen manuell einzugeben, oder **Von Festplatte hinzufügen**, um zu den Ordnern zu navigieren, die Sie hinzufügen möchten.

Tipp

Die Ordnerliste im Dialogfeld **Ausnahmeordner hinzufügen** enthält eine Reihe von Standardordnern, wie Eigene Dateien, Eigene Bilder, Benutzerprofil, Desktop und Programme, deren Inhalt regelmäßig von den Benutzern geändert wird.

Ausnahmeprozesse

Prozesse, die dauerhafte Änderungen an den Festplatten vornehmen dürfen. Sie können Ausnahmeprozesse über einen der drei Befehle auf der Schaltfläche **Hinzufügen** hinzufügen:

Hinzufügen: Geben Sie den Pfad zu den ausführbaren Dateien eines Prozesses manuell an.

Hinweis

Stellen Sie bei der manuellen Eingabe eines Anwendungspfads sicher, dass Sie den absoluten lokalen Pfad auf dem Agentcomputer eingeben. Der Pfad kann Umgebungsvariablen, wie %AppData%, %SystemRoot%, %UserName% und %UserProfile%, enthalten.

Aus Prozessen hinzufügen: Wählen Sie aus der Liste der aktuell ausgeführten Prozesse einen Eintrag aus.

Von Festplatte hinzufügen: Wählen Sie eine ausführbare Datei aus, indem Sie die Festplatteninhalte durchsuchen. Der Pfad muss ein absoluter lokaler Pfad sein. Beim Installieren von Anwendungen in Ordnern auf Agentcomputern, die nicht identisch mit den Ordnern auf dem Administratorcomputer sind, müssen Sie die tatsächliche Ordnerstruktur angeben und anschließend den absoluten lokalen Pfad manuell eingeben.

5.10.2 Registerkarte "Gerätezugriff"

Über die Registerkarte **Gerätezugriff** können Sie Zugriffsberechtigungen für verschiedene Gerätetypen definieren.

Oben im Bereich **Berechtigungen** wird die vollständige Liste der Gerätetypen angezeigt, die gesteuert werden können. Bei Auswahl eines Geräts im oberen Bereich werden im unteren Bereich entweder alle Geräte dieses Typs, die auf dem Administratorcomputer installiert sind, angezeigt (sofern das Kontrollkästchen **Nur verfügbare Geräte anzeigen** aktiviert ist) oder sämtliche Geräte dieses Typs.

Im unteren Bereich ist auch der Typ **<Andere>** aufgeführt. Über den Typ **<Andere>** können Einzelgeräte überwacht werden, die auf Agentcomputern, nicht aber auf dem Administratorcomputer installiert sind.

Hinweis

Ausnahmen sind USB- und WiFi-Geräte.

Für USB-Geräte werden im unteren Bereich nicht einzelne Geräte, sondern die Weiße Liste angezeigt, in der die USB-Geräte und USB-Geräteklassen aufgeführt sind, die auch verfügbar sind, wenn USB-Geräte grundsätzlich deaktiviert sind. Weitere Informationen über die Weiße Liste erhalten Sie unter [Zugriffsrechte für USB-Laufwerke definieren](#).

Für WiFi-Geräte wird im unteren Bereich die Weiße Liste angezeigt. Diese Liste enthält WiFi-Geräte, die verfügbar sind, obwohl der Zugriff für den WiFi-Gerätetyp auf "Kein

Zugriff" eingestellt ist. Weitere Informationen über das Hinzufügen eines WiFi-Geräts zur Weißen Liste erhalten Sie unter [Zugriffsrechte für ein WiFi-Gerät definieren](#).

Überwachungsgrade

Sie können den Gerätezugriff auf folgenden Ebenen steuern:

- Gerätetyp** Hier wird die Zugriffsregel auf den gesamten Gerätetyp angewendet; die Richtlinie deckt alle Geräte dieses Typs ab, die auf Agentcomputern installiert sind. Weitere Informationen zur Definition von Zugriffsrechten für Gerätetypen finden Sie unter [Zugriffsrechte pro Gerätetyp definieren](#).
- Einzelgerät** Hier wird die Zugriffsregel nur auf ein einziges Gerät angewendet. Weitere Informationen zur Definition von Zugriffsrechten für ein einzelnes Gerät finden Sie unter [Zugriffsrechte pro Einzelgerät definieren](#).
- Um den Zugriff bei USB-Geräten pro Einzelgerät zu steuern, sollten Sie eine Weiße Liste erstellen und die immer verfügbaren Geräte hinzufügen.
- USB-Geräteklassen** Die folgenden Erläuterungen gelten nur für USB-Geräte.
- Sie können den Zugriff auf Geräteklassen wie USB-Eingabegeräte, USB-Drucker und Smart-Card-Geräte zulassen. Die Zugriffssteuerung pro Geräteklasse wird durch die Weiße Liste für USB ermöglicht, in der Sie USB-Geräte und USB-Geräteklassen festlegen können, die immer verfügbar sind. Informationen über die Verwendung der Weißen Liste erhalten Sie unter [Zugriffsrechte für ein USB-Laufwerk definieren](#).

Geräte werden sowohl über ihren Benutzermodusnamen oder -buchstaben (z. B. A:, COM1) als auch über interne Namen (z. B. \Gerät\Floppy0, \Gerät\Serial0) erkannt. So können auch unbenannte Geräte verwaltet werden.

5.10.3 Registerkarte Internet

Über die Registerkarte **Internet** legen Sie fest, ob der Zugriff auf alle Websites allgemein zugelassen oder allgemein verweigert werden soll, und ob zu dieser allgemeinen Richtlinie Ausnahmen definiert werden sollen.

Die Liste **Ausnahme** enthält die Ausnahmen zur allgemeinen Richtlinie. Wenn die Richtlinienkategorie auf **Alle zulassen** gesetzt ist, zeigt die Liste **Ausnahme** die Internetadressen an, für die der Zugriff gesperrt wurde. Einträge können dieser Liste entweder manuell hinzugefügt oder über Drag & Drop aus der Liste **Internetadressen** verschoben werden. Diese Liste kann sowohl vollständige URLs enthalten, wie beispielsweise www.google.com oder Teile von URLs, wie beispielsweise *google* oder *game*.

Über die Liste **Internetadressen** können Sie eine benutzerdefinierte Liste erstellen, aus der Sie Internetressourcen auswählen können. Diese Liste ist für alle Richtlinien gültig; Sie können über jede Richtlinie auf die Liste zugreifen und diese erweitern. Die Liste kann auch vollständige Links und Masken enthalten. Wenn nur eine Maske definiert ist, erlaubt oder verweigert die Richtlinie den Zugriff auf alle Internetseiten, die dieser Maske entsprechen.

Die Liste **Zu durchsuchende Ports** enthält die Ports, die ProtectOn Pro durchsucht und die für Zugriffe gesperrt werden können, wenn eine mit dem Internet-Zugriff verbundene

Richtlinien definieren und übernehmen

Richtlinie festgelegt wird. Wenn der Port, den Ihre Computerumgebung für den Internet-Zugriff verwendet, nicht in der Liste enthalten ist, sollten Sie ihn durch Klicken auf die Schaltfläche **Bearbeiten** hinzufügen. Verwendet Ihre Computerumgebung einen Proxy-Server für den Internet-Zugriff, stellen Sie sicher, dass der Proxy-Port in der Liste enthalten ist.

Einen Eintrag zur Ausnahmeliste hinzufügen

- Klicken Sie auf die Schaltfläche **Hinzufügen** unterhalb der Liste **Ausnahme**, geben Sie einen Link oder den Teil eines Links ein, und drücken Sie die Eingabetaste, um die Änderungen zu speichern.

Einen Eintrag zur Liste "Internetadressen" hinzufügen

- Klicken Sie auf die Schaltfläche **Hinzufügen** unterhalb der Liste **Internetadressen**, geben Sie einen Link oder den Teil eines Links ein, und drücken Sie die Eingabetaste, um die Änderungen zu speichern.

5.10.4 Registerkarte Anwendung

Auf der Registerkarte **Anwendung** wird festgelegt, ob als allgemeine Anwendungsstrategie die Verwendung aller Anwendungen zugelassen oder der Zugriff auf alle Anwendungen verweigert werden soll. Außerdem werden auf dieser Registerkarte die Ausnahmen zur allgemeinen Strategie definiert.

Die Liste **Ausnahme** enthält die Ausnahmen zur allgemeinen Richtlinie. Wenn die Richtlinienkategorie z. B. auf **Alle zulasseneingestellt** ist, zeigt die Liste **Ausnahme** die Anwendungen an, für die der Zugriff gesperrt wurde. Die Ausnahmeliste muss keine Pfade enthalten, kann aber beispielsweise eine Datei wie excel.exe sein.

Die Liste **Anwendungen** zeigt die Anwendungen, die auf dem Administrator-Computer installiert sind. Die Liste ist verfügbar, um den Aufwand bei der erneuten Eingabe von Pfaden zu ausführbaren Dateien zu ersparen. Außerdem können Elemente dieser Liste einfach zur Ausnahmeliste auf der linken Seite hinzugefügt werden. Standardmäßig enthält die Liste **Anwendungen** den **Desktop**,, **das Startmenü** und die **Standardprogramme**. Wenn Sie auf die Schaltfläche **Erneut suchen** klicken, durchsucht Netop ProtectOn Pro diese Ordner nach ausführbaren Dateien. Sie können andere Anwendungen zum Ordner **Benutzerdefiniert** hinzufügen.

Einen Eintrag zur Ausnahmeliste hinzufügen

1. Klicken Sie auf die Schaltfläche **Hinzufügen** unterhalb der **Ausnahme** -Liste, und wählen Sie **Von Festplatte hinzufügen**.
2. Gehen Sie zum Speicherort der Anwendung, die Sie hinzufügen möchten, damit der vollständige Pfad automatisch hinzugefügt wird.

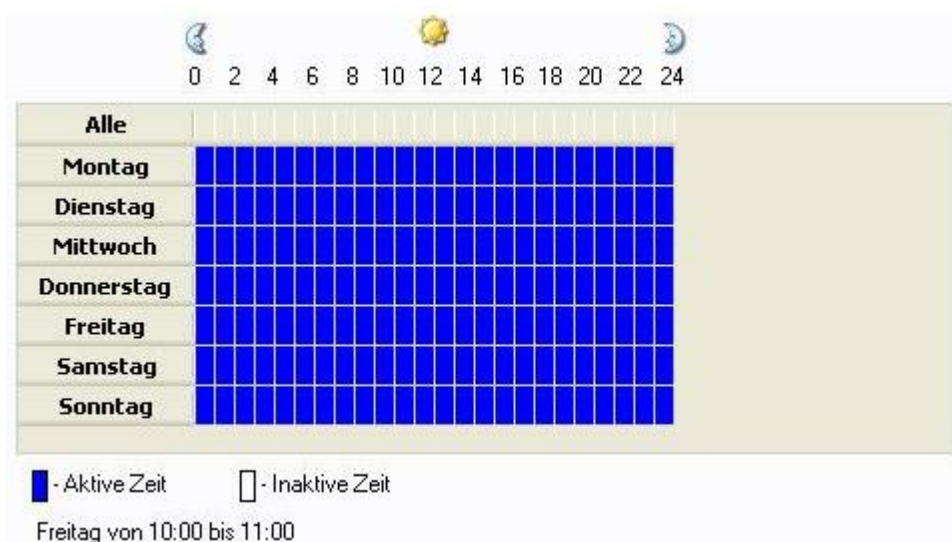
Einen Eintrag zur Anwendungsliste hinzufügen

1. Klicken Sie auf die Schaltfläche **Hinzufügen** unterhalb der Liste **Anwendungen** , und wählen Sie **Von Festplatte hinzufügen**.
2. Gehen Sie zum Speicherort der Anwendung, die Sie hinzufügen möchten, damit der vollständige Pfad automatisch hinzugefügt wird.

5.10.5 Registerkarte Zeitplan

Für alle vier Arten von Richtlinien kann ein Zeitplan festgelegt werden

Die Registerkarte **Zeitplan** wird verwendet, um den Gültigkeitszeitraum der Richtlinie zu definieren. Das unten stehende Diagramm zeigt eine Richtlinie, die während der Arbeitszeit aktiv ist.




Um **aktive Zeit** in **inaktive Zeit** zu ändern, klicken Sie mit der rechten Maustaste auf die Zelle, die Sie ändern möchten.

5.10.6 Registerkarte Zugewiesen

Die Registerkarte **Zugewiesen** wird verwendet, um Richtlinien vorhandenen Gruppen zuzuweisen. Informationen zum Erstellen von Gruppen finden Sie unter [Eine Gruppe erstellen](#).

Einer Gruppe eine Richtlinie zuweisen

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.
2. Wählen Sie im Dialogfeld **Richtliniengruppen** eine oder mehrere Gruppen aus, und klicken Sie auf **Hinzufügen**.

Wenn Sie der Richtlinie eine höhere Priorität als den anderen Richtlinien dieser Art zuweisen möchten, aktivieren Sie das Kontrollkästchen **Andere Richtlinien überschreiben**. Wenn das Flag gesetzt wurde, wird dies durch die Änderung des Symbols im Fenster "Richtlinieneditor" angezeigt . Wenn mehr als eine Richtlinie Priorität hat, werden diese wie Richtlinien ohne gesetztes Flag zusammengeführt. Weitere Informationen zur Richtlinienpriorität finden Sie unter [Zusammenführung von Richtlinien](#).

6 Überlappende Richtlinien

6.1 Richtlinien zusammenführen

Wenn mehr als eine Richtlinie einer Kategorie definiert wurde, beispielsweise drei Anwendungsrichtlinien, löst Netop ProtectOn Pro mögliche Inkonsistenzen automatisch auf und ermittelt, wie die innerhalb der jeweiligen Richtlinie definierten Regeln in ihrer Gesamtheit angewandt werden. Dies bedeutet, dass Sie sich nicht zwangsläufig um Inkonsistenzen kümmern müssen. Es könnte aber nützlich sein zu verstehen, wie die Richtlinien zusammengeführt werden, um die Ergebnisse der Richtlinienübernahme nachvollziehen zu können.

Ein einfaches Beispiel: Die Benutzergruppe mit Namen "Marketing" beinhaltet alle Mitarbeiter der Marketingabteilung. Die Mitglieder der Gruppe dürfen alle Anwendungen verwenden, für die das Unternehmen Lizenzen besitzt, mit Ausnahme einiger Entwicklungsprogramme wie .NET Framework. Der Benutzer Peter ist ein Mitglied der Marketinggruppe. Da er jedoch die Website des Unternehmens verwaltet, ist er auch Mitglied der Gruppe "Entwickler". Da die Entwickler den allgemeinen Zugriff "Alle zulassen" auf Entwicklungsprogramme haben, hat Peter auch Zugriff auf .NET Framework-Tools, selbst wenn die Marketinggruppe an sich keinen Zugriff hat.

Aus technischer Sicht ist nur eine Richtlinie pro Kategorie wirksam und diese eine Richtlinie wird automatisch erstellt, indem mehrere Richtlinien zu einer zusammengeführt werden. Wenn Sie Gruppen definiert und ihnen Richtlinien zugewiesen haben, wendet Netop ProtectOn Pro einen internen Algorithmus an, um eine wirksame Richtlinie der jeweiligen Kategorie zu definieren. Dies geschieht in zwei Schritten:

1. Ermittlung von Richtlinien der jeweiligen Kategorie
2. Zusammenführen von Richtlinien der jeweiligen Kategorie

Ermittlung von Richtlinien der jeweiligen Kategorie

Richtlinien der jeweiligen Kategorie werden für den *Computer* und für den *Benutzer* ermittelt, auf den sie angewandt werden sollen. Die folgende Reihenfolge gilt für jede der vier Richtlinienkategorien:

1. Die Liste von Gruppen wird ermittelt, zu denen der Benutzer gehört.

Eine Gruppe wird zum Element der Liste, wenn der Benutzer ein Mitglied der Gruppe ist, oder wenn der Benutzer ein Mitglied einer anderen Gruppe oder eines Unternehmensbereichs ist, die oder der zur Gruppe gehört. Die resultierende Liste von Gruppen wird verwendet, um zu ermitteln, welche Richtlinien dem Benutzer zugewiesen werden.

Das Ergebnis ist eine Liste von Richtlinien, die als "dem Benutzer zugewiesen" gekennzeichnet wird.

2. Die Liste von Gruppen wird ermittelt, zu denen der Computer gehört.

Eine Gruppe wird zum Element der Liste, wenn der Computer ein Mitglied der Gruppe ist, oder wenn der Computer ein Mitglied einer anderen Gruppe oder eines Unternehmensbereichs ist, die oder der zur Gruppe gehört. Die resultierende Liste von Gruppen wird verwendet, um zu ermitteln, welche Richtlinien dem Computer zugewiesen werden.

Das Ergebnis ist eine Liste von Richtlinien, die als "dem Computer zugewiesen" gekennzeichnet wird.

3. Die zwei Listen von Richtlinien werden jeweils in zwei weitere Listen unterteilt: Zur

ersten Liste gehören Richtlinien, für die die Option **Andere Richtlinien überschreiben** auf der Registerkarte **Zugewiesen** ausgewählt wurde. Die anderen Richtlinien werden zu Elementen der zweite Liste.

Als Ergebnis wird eine Prioritätsliste von Richtlinien erstellt:

Priorität	Andere Richtlinien überschreiben	Zugewiesen	Beschreibung
1	+	Benutzer ¹⁾	Richtlinien, die Benutzern zugewiesen und mit dem Kennzeichen 'Überschreiben' versehen sind, haben höchste Priorität.
2	+	Computer	Richtlinien, die Computern zugewiesen und mit dem Kennzeichen 'Überschreiben' versehen sind, haben die nächsthöhere Priorität.
3	-	Benutzer ¹⁾	Wenn Richtlinien nicht mit dem Kennzeichen 'Überschreiben' versehen sind, haben die Richtlinien, die Benutzern zugewiesen sind, die höhere Priorität.
4	-	Computer	

1) Richtlinien zum Festplattenschutz werden nur pro Computer angewandt, nicht pro Benutzer. Das bedeutet, dass die Listen 1 und 3 für die Richtlinienkategorie **Festplattenschutz** immer leer sind.

Richtlinien der jeweiligen Kategorie zusammenführen

In diesem Schritt wird gemäß der oben erläuterten Zusammenführung von Richtlinien, die für den Computer und den Benutzer definiert wurden, die wirksame Richtlinie festgelegt.

Wenn die oben genannten Listen leer sind, wird eine Standardrichtlinie angewandt. Die Standardrichtlinie wird individuell für jede Richtlinienkategorie definiert.

☐ Standardrichtlinie

Die unten stehende Tabelle beschreibt, wie die Standardrichtlinie für jede Richtlinienkategorie definiert wird.

Überlappende Richtlinien

Richtlinienkategorie	Beschreibung der Standardrichtlinie
Richtlinie zum Festplattenschutz	Es gibt keine geschützten Festplatten in der Standardrichtlinie.
Richtlinie zum Gerätezugriff	Die Standardrichtlinie erlaubt die Nutzung aller Geräte.
Webrichtlinie	Die Standardrichtlinie erlaubt den Benutzerzugriff auf sämtliche Adressen.
Anwendungsrichtlinie	Die Standardrichtlinie erlaubt das Ausführen aller Anwendungen.

Die folgenden Abschnitte beschreiben die Regeln zum Zusammenführen zweier Richtlinien der jeweiligen Kategorie. Mehr als zwei Richtlinien werden zusammengeführt, indem jeweils zwei Richtlinien nacheinander zusammengeführt werden. Beispiel: Es gibt drei wirksame Richtlinien einer Kategorie: p1, p2 und p3. Diese Richtlinien werden über ((p1 mit p2 zusammenführen) mit p3 zusammenführen) zusammengeführt, das heißt: Zuerst wird die Zusammenführung von p1 und p2 ermittelt. Die resultierende Richtlinie wird mit p3 zusammengeführt.

6.2 Richtlinien zum Festplattenschutz zusammenführen

Wenn einem Computer mehrere Richtlinien zum Festplattenschutz zugewiesen sind, werden diese zusammengeführt. Die nachfolgende Tabelle gibt einen schematischen Überblick über die Zusammenführung der Richtlinien.

Richtlinien	Wiederherstellen bei Neustart	Geschützte Laufwerke	Ausnahmeordner	Ausnahmeprozesse
Richtlinie 1	Aktiviert	Laufwerke 1	Ordner 1	Prozesse 1
Richtlinie 2	Deaktiviert	Laufwerke 2	Ordner 2	Prozesse 2
Resultierende Richtlinie	Aktiviert	Laufwerke 1 \cup Laufwerke 2 ¹⁾	Ordner 1 \cup Ordner 2	Prozesse 1 \cup Prozesse 2

1) " \cup " ist das Symbol für mathematische Vereinigung: A oder B oder beide (einschließende Vereinigung)

Beispiele

Ein Beispiel der Zusammenführung finden Sie in nachstehender Tabelle.

Richtlinien zum Festplattenschutz sind nur auf einzelne Computer oder eine Gruppe von Computern anwendbar, jedoch nicht auf Benutzer.

Überlappende Richtlinien

Richtlinien	Wiederherstellen bei Neustart	Geschützte Laufwerke	Ausnahmeordner	Ausnahmeprozesse
Richtlinie zum Festplattenschutz 1	Aktiviert	C D E	C:\Ordner C1 D:\Ordner D1 E:\Ordner E1	Prozess 1 Prozess 2
Richtlinie zum Festplattenschutz 2	Deaktiviert	D E F	D:\Ordner D1 E:\Ordner E2 F:\Ordner F1	Prozess 3 Prozess 4

Resultierende Richtlinie	Wiederherstellen bei Neustart	Resultierende geschützte Laufwerke	Resultierende Ausnahmeordner	Resultierende Ausnahmeprozesse
Richtlinie zum Festplattenschutz	Aktiviert	C D E F	C:\Ordner C1 D:\Ordner D1 E:\Ordner E1, E2 F:\Ordner F1	Prozess 1 Prozess 2 Prozess 3 Prozess 4

Wenn Sie Dateitypen festlegen, die in den Ausnahmeordnern geändert werden dürfen, müssen diese Dateitypen auch in allen Ordnern der resultierenden Richtlinie geändert werden dürfen. Wenn die Dateitypen in mindestens einem Ausnahmeordner der resultierenden Richtlinie nicht geändert werden dürfen, sind auch keine Änderungen in allen anderen Ausnahmeordnern der resultierenden Richtlinie möglich.

Hinweis

Bei der Erstellung mehrerer Richtlinien zum Festplattenschutz ist die Zusammenführung von Ausnahmeordnern möglicherweise nicht leicht nachvollziehbar. Daher sollten Sie nur eine Richtlinie zum Festplattenschutz verwenden, die alle Festplatten abdeckt.

6.3 Richtlinien zum Gerätezugriff zusammenführen

Wenn einem Benutzer, Computer oder anderen Objekt mehrere Richtlinien zum Gerätezugriff zugewiesen sind, werden diese zusammengeführt.

Gerätezugriffsrechte können pro Typ (bzw. Klasse bei USB-Geräten) oder pro Gerät definiert werden. Dies wird bei der Zusammenführung der Richtlinien berücksichtigt.

Überlappende Richtlinien

Die nachfolgende Tabelle gibt einen kompakten schematischen Überblick über alle in den Richtlinien zum Gerätezugriff enthaltenen Gerätetypen.

Richtlinien	Verborgene Laufwerke	Ausnahmeordner	Gerätemasken	Gerätetypmasken	Geräte auf der Weißen Liste für USB
Richtlinie 1	Laufwerke 1	Ordner 1	Gerätemaske n 1	Gerätetypmasken 1	Geräte auf der Weißen Liste 1
Richtlinie 2	Laufwerke 2	Ordner 2	Gerätemaske n 2	Gerätetypmasken 2	Geräte auf der Weißen Liste 2
Resultierende Richtlinie	Laufwerke 1 \cup Laufwerke 2 ¹⁾	Ordner 1 \cup Ordner 2	Gerätemasken 1 \cup Gerätemasken 2 ²⁾	Gerätetypmasken 1 \cup Gerätetypmasken 2 ²⁾	Geräte auf der Weißen Liste 1 \cup Geräte auf der Weißen Liste 2

1) " \cup " ist das Symbol für mathematische Vereinigung: A oder B oder beide (einschließende Vereinigung)

2) Wenn beide Gruppen (Gerätemasken 1 und Gerätemasken 2) Masken für ein Gerät enthalten, werden diese Masken zusammengeführt. Wenn Gerätemasken 1 beispielsweise die Maske "Lesen" und Gerätemasken 2 die Maske "Schreiben" für dasselbe Gerät enthalten, resultiert daraus die Maske "Lesen UND Schreiben". Diese Regel gilt auch für Gerätetypmasken.

Beispiele

Beispiele für die Zusammenführung von Richtlinien zum Gerätezugriff finden Sie in den folgenden Tabellen.

Die ersten drei Beispiele zeigen unterschiedliche Szenarien für das Zusammenführen von DVD-/CD-ROM-Richtlinien. Bei den folgenden Gerätetypen werden die Richtlinien auf ähnliche Weise zusammengeführt:

- Diskette
- Wechselmedium
- Bandlaufwerke

Hinweis

Bei der Zusammenführung setzen sich stets die strengsten Einstellungen durch.

In der nachstehenden Tabelle steht "n. v. " für "nicht verfügbar".

Beispiel 1 – für DVD/CD:

Richtlinien	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie 1	n. v.	n. v.	Lesen aktiviert Schreiben aktiviert	Pro Typ	n. v.
Richtlinie 2	n. v.	n. v.	Lesen aktiviert Schreiben deaktiviert	Pro Typ	n. v.

Resultierende Richtlinie	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie	n. v.	n. v.	Lesen aktiviert Schreiben aktiviert	Pro Typ	n. v.

Hinweis

Die Richtlinie wird für alle DVD-/CD-ROM-Laufwerke übernommen, da sie „pro Typ“ definiert ist.

Überlappende Richtlinien

Beispiel 2 – für DVD/CD:

Richtlinien	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie 1	n. v.	n. v.	Lesen aktiviert Schreiben aktiviert	Pro Typ	n. v.
Richtlinie 2	n. v.	n. v.	Lesen aktiviert Schreiben deaktiviert	Pro Gerät (Richtlinie ist aktiviert für \Device\CdRom0)	n. v.
Richtlinie 3	n. v.	n. v.	Lesen aktiviert Schreiben deaktiviert	Pro Typ	n. v.

Beispiel 2 – für DVD/CD – Zwischenschritt, Zusammenführung von Richtlinie 1 und 2:

Richtlinie 1 und 2	n. v.	n. v.	Lesen aktiviert Schreiben deaktiviert	Pro Gerät Richtlinie nur gültig für \Device\CdRom0	n. v.
			Lesen aktiviert Schreiben aktiviert	Pro Typ Für andere Geräte dieses Typs	
Richtlinie 3	n. v.	n. v.	Lesen aktiviert Schreiben aktiviert	Pro Gerät (Richtlinie ist aktiviert für \Device\CdRom0)	n. v.

Überlappende Richtlinien

Resultierende Richtlinie	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie	n. v.	n. v.	Lesen aktiviert Schreiben deaktiviert	Pro Gerät Richtlinie nur gültig für \Device\CdRom0	n. v.
			Lesen aktiviert Schreiben aktiviert	Pro Typ Für andere Geräte dieses Typs	

Beispiel 3 – für DVD/CD:

Richtlinien	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie 1	n. v.	n. v.	Lesen deaktiviert Schreiben deaktiviert	Pro Typ	n. v.
Richtlinie 2	n. v.	n. v.	Lesen aktiviert Schreiben deaktiviert	Pro Gerät (Richtlinie ist aktiviert für \Device\CdRom0)	n. v.
Richtlinie 3	n. v.	n. v.	Lesen aktiviert Schreiben aktiviert	Pro Gerät (Richtlinie ist aktiviert für \Device\CdRom0)	n. v.

Überlappende Richtlinien

Beispiel 3 – für DVD/CD – Zwischenschritt, Zusammenführung von Richtlinie 1 und 2:

Richtlinie 1 und 2	n. v.	n. v.	Lesen deaktiviert Schreiben deaktiviert	Pro Typ (= Richtlinie wird für alle DVD-/CD-ROM-Laufwerke übernommen)	n. v.
Richtlinie 3	n. v.	n. v.	Lesen aktiviert Schreiben aktiviert	Pro Gerät (Richtlinie ist aktiviert für \Device\CdRom0)	n. v.

Resultierende Richtlinie	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie	n. v.	n. v.	Lesen deaktiviert Schreiben deaktiviert	Pro Typ (= Richtlinie wird für alle DVD-/CD-ROM-Laufwerke übernommen)	n. v.

Eine Richtlinie zum Gerätezugriff kann auch eine Weiße Liste für USB enthalten. Folgende Regeln finden Anwendung, wenn zwei oder mehr Richtlinien zum USB-Gerätezugriff zusammengeführt werden:

- Wenn nur der Zugriff gemäß der Weißen Liste zulässig ist, schließt die resultierende Weiße Liste USB-Geräte aller Weißen Listen ein.
- Die strengste Richtlinie lautet „Kein Zugriff“. Wenn diese Richtlinie mit einer anderen USB-Richtlinie (Vollzugriff unter „Zugriff gemäß Weißer Liste“) zusammengeführt wird, lautet die resultierende Richtlinie „Kein Zugriff“.

Beispiel 4 – für USB:

Richtlinien	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie 1	n. v.	n. v.	Vollzugriff	Pro Typ	n. v.
Richtlinie 2	n. v.	n. v.	Kein Zugriff - nur Weiße Liste	Pro Typ	HID-Klasse ¹⁾

Resultierende Richtlinie	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Endgültige Richtlinie	n. v.	n. v.	Nur Zugriff gemäß Weißer Liste	Pro Typ	HID-Klasse HID-Geräte sind auf allen Computern verfügbar

1) Der Inhalt der Weißen Liste besteht aus der HID-Klasse (Human Interface Device), wie zum Beispiel Maus oder Tastatur.

Die folgenden Beispiele beziehen sich auf die Zusammenführung dreier Richtlinien zum Gerätezugriff; UC_A, UC_B und UC_C können jeweils ein einzelner Benutzer oder Computer sein, aber auch eine Gruppe von Benutzern/Computern.

Beispiel 5 – für USB:

Richtlinien	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie 1	n. v.	n. v.	Kein Zugriff - Weiße Liste	Pro Gerät (nur gültig für UC_A)	HID-Klasse
Richtlinie 2	n. v.	n. v.	Kein Zugriff - Weiße Liste	Pro Gerät (Richtlinie umfasst UC_A, UC_B und UC_C)	Massenspeicher-klasse
Richtlinie 3	n. v.	n. v.	Kein Zugriff	Pro Typ (nur gültig für UC_C)	n. v.

Überlappende Richtlinien

Beispiel 5 – für USB – Zwischenschritt, Zusammenführung von Richtlinie 1 und 2:

Richtlinie 1 und 2	n. v.	n. v.	Kein Zugriff – Weiße Liste	Pro Gerät (nur gültig für UC_A)	HID-Klasse
			Kein Zugriff – Weiße Liste	Pro Gerät (Richtlinie umfasst UC_A, UC_B und UC_C)	Massenspeicherklasse
Richtlinie 3	n. v.	n. v.	Kein Zugriff	Pro Typ (nur gültig für UC_C)	n. v.

Resultierende Richtlinie	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie	n. v.	n. v.	Kein Zugriff – Weiße Liste	Pro Gerät (nur gültig für UC_A)	HID-Klasse
			Kein Zugriff – Weiße Liste	Pro Gerät (nur gültig für UC_B)	Massenspeicherklasse
			Kein Zugriff	Pro Typ (nur gültig für UC_C)	

Beispiel 6 – für USB:

Richtlinien	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie 1	n. v.	n. v.	Kein Zugriff – Weiße Liste	Pro Gerät (nur gültig für UC_A)	HID-Klasse
Richtlinie 2	n. v.	n. v.	Kein Zugriff – Weiße Liste Andere Richtlinien überschreiben	Pro Gerät (Richtlinie umfasst UC_A, UC_B und UC_C)	Massenspeicherklasse
Richtlinie 3	n. v.	n. v.	Kein Zugriff	Pro Typ (nur gültig für UC_C)	n. v.

Beispiel 6 – für USB – Zwischenschritt, Zusammenführung von Richtlinie 1 und 2:

Richtlinie 1 und 2	n. v.	n. v.	Kein Zugriff – Weiße Liste Andere Richtlinien überschreiben	Pro Gerät (Richtlinie umfasst UC_A, UC_B und UC_C)	<i>Richtlinie 2 überschreibt die anderen Richtlinien:</i> Massenspeicherklasse
Richtlinie 3	n. v.	n. v.	Kein Zugriff	Pro Typ (nur gültig für UC_C)	n. v.

Resultierende Richtlinie	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie	n. v.	n. v.	Kein Zugriff – Weiße Liste Andere Richtlinien überschreiben	Pro Gerät (Richtlinie umfasst UC_A, UC_B und UC_C)	<i>Richtlinie 2 überschreibt die anderen Richtlinien:</i> Massenspeicherklasse

Eine Richtlinie zum Gerätezugriff kann auch eine Richtlinie zum Festplattenschutz sein, die den Zugriff auf Laufwerke, Ordner und Dateien festlegt. Nachfolgend finden Sie Beispiele

Überlappende Richtlinien

für resultierende Richtlinien zum Festplattenschutz bei zwei oder mehr zusammenzuführenden Richtlinien.

"Verbergen" bedeutet, dass die Laufwerke, Ordner oder Dateien für den Benutzer oder das Betriebssystem nicht sichtbar sind. Um sicherzustellen, dass sich eine Richtlinie zum Festplattenschutz nicht auf das Betriebssystem auswirkt, wird eine in Netop ProtectOn Pro integrierte Funktion ausgeführt. Wenn in einer Richtlinie zum Festplattenschutz daher "Laufwerk C: Verbergen" (wo Windows in der Regel installiert ist) festgelegt wird, bleiben einige Standardordner und -dateien sichtbar, damit das Windows Betriebssystem weiterhin ausgeführt werden kann. Die Namen der Standardordner und -dateien werden hier nicht aufgeführt, da sie vom jeweiligen Betriebssystem abhängen.

Beispiel 7 – für die Festplatte:

Richtlinien	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie 1	Laufwerk C:	Standardordner	n. v.	Pro Gerät (nur gültig für UC_A)	n. v.
Richtlinie 2	n. v.	n. v.	n. v.	Pro Typ (Richtlinie umfasst UC_A und UC_B)	n. v.

Resultierende Richtlinie	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie	Laufwerk C:	Standardordner	n. v.	Pro Gerät (nur gültig für UC_A)	n. v.

Andere Laufwerke – Vollzugriff

Beispiel 8 – für die Festplatte:

Richtlinien	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie 1	n. v.	n. v.	n. v.	Pro Typ (nur gültig für UC_A)	n. v.
Richtlinie 2	Laufwerk D:	Standardordner	n. v.	Pro Gerät (Richtlinie umfasst UC_A, UC_B und UC_C)	n. v.
Richtlinie 3	Laufwerk C:	zwei Ordner, je nach Umgebungsvariablen und Standardordnern	Ausschließen = Nein Rekursiv=Ja	Pro Gerät (nur gültig für UC_C)	n. v.

Beispiel 8 – für die Festplatte – Zwischenschritt, Zusammenführung von Richtlinie 1 und 2:

Richtlinie 1 und 2	Laufwerk D:	Standardordner	n. v.	Pro Gerät (Richtlinie umfasst UC_A, UC_B und UC_C)	n. v.
Richtlinie 3	Laufwerk C:	zwei Ordner, je nach Umgebungsvariablen und Standardordnern	Ausschließen = Nein Rekursiv=Ja	Pro Gerät (nur gültig für UC_C)	n. v.

Überlappende Richtlinien

Resultierende Richtlinie	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie	Laufwerk D: Laufwerk C:	Standard-ordner zwei Ordner, je nach Umgebungsvariablen und Standard-ordnern	Ausschließen = Nein Rekursiv=Ja	Pro Gerät (Richtlinie umfasst UC_A, UC_B und UC_C) Pro Gerät (nur gültig für UC_C)	n. v.

Die Zusammenführung von Richtlinien zum Gerätezugriff ist für die übrigen Geräte – Bluetooth-Geräte, FireWire-Port, IrDA-Geräte, parallele und serielle Schnittstelle und WiFi – einfach: Es gibt zwei Änderungsoptionen für diese Geräte: Vollzugriff oder kein Zugriff.

Die strengste Regel wird zur resultierenden Regel.

Beispiel 9 – für Infrarot:

Richtlinien	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie 1	n. v.	n. v.	n. v.	Infrarot – Vollzugriff	n. v.
Richtlinie 2	n. v.	n. v.	n. v.	Infrarot – kein Zugriff	n. v.

Resultierende Richtlinie	Verborgene Laufwerke	Ausnahmeordner	Geräte-masken	Gerätetyp-masken	Geräte auf der Weißen Liste für USB
Richtlinie	n. v.	n. v.	n. v.	Infrarot – kein Zugriff	n. v.

6.4 Webrichtlinien zusammenführen

Wenn einem Benutzer, Computer oder anderen Objekt mehrere Webrichtlinien zugewiesen sind, werden diese zusammengeführt.

Die nachfolgende Tabelle gibt einen schematischen Überblick über die Zusammenführung von Webrichtlinien. In der Übersicht kann "Websites" für eine Zahl, einen Buchstaben, einen teilweisen oder einen vollständigen Link stehen. Je kürzer die ursprüngliche Ausnahme ist, desto mehr wird gesperrt.

Überlappende Richtlinien

Bei- spiel- Nr.	Ursprüngliche Richtlinien	Ursprüngliche Ausnahmen	Resultierende Richtlinie	Resultierende Ausnahmen
1	Richtlinie 1 Alle zulassen	Websites 1	Alle zulassen	Alle Websites in Websites 1 und 2 ausschließen
	Richtlinie 2 Alle zulassen	Websites 2		
2	Richtlinie 1 Alle verweigern	Websites 1	Alle verweigern	Websites in Websites 1 ausschließen, wenn sie nicht in Websites 2 definiert sind
	Richtlinie 2 Alle zulassen	Websites 2		
3	Richtlinie 1 Alle zulassen	Websites 1	Alle verweigern	Websites in Websites 2 ausschließen, wenn sie nicht in Websites 1 definiert sind
	Richtlinie 2 Alle verweigern	Websites 2		
4	Richtlinie 1 Alle verweigern	Websites 1	Alle verweigern	Alle Websites sowohl in Websites 1 als auch in Websites 2 ausschließen
	Richtlinie 2 Alle verweigern	Websites 2		

Beispiele für die Zusammenführung finden Sie in nachstehender Tabelle. UC_A, UC_B und UC_C können jeweils ein einzelner Benutzer oder Computer sein, aber auch eine Gruppe von Benutzern oder Computern.

Beispiel 1:

Ursprüngliche Richtlinien	Ursprüngliche Ausnahmen	Resultierende Richtlinie	Resultierende Ausnahmen
Richtlinie 1 Alle zulassen (gültig für UC_A und UC_B)	Wort 1 Website 1 Wort 2 Website 2 Wort 3	Alle zulassen	Die Ausnahmen für UC_A sind: Wort 1 Website 1 Wort 2 Website 2 Wort 3 Die Ausnahmen für UC_B sind: Wort 1 Website 1 Wort 2 Website 2 Wort 3 Website 3 Wort 4 Wort 5
Richtlinie 2 Alle zulassen (nur gültig für UC_B)	Wort 1 Website 2 Wort 4 Website 3 Wort 5		

Überlappende Richtlinien

Beispiel 2:

Ursprüngliche Richtlinien	Ursprüngliche Ausnahmen	Resultierende Richtlinie	Resultierende Ausnahmen
Richtlinie 1 Alle zulassen	Wort 1 Website 1 Wort 2 Website 2 Wort 3	Alle verweigern	Wort 4 Website 3 Wort 5
Richtlinie 2 Alle verweigern	Wort 1 Website 2 Wort 4 Website 3 Wort 5		

Beispiel 3:

Ursprüngliche Richtlinien	Ursprüngliche Ausnahmen	Resultierende Richtlinie	Resultierende Ausnahmen
Richtlinie 1 Alle verweigern	Wort 1 Website 1 Wort 2 Website 2 Wort 3	Alle zulassen	Wort 1 Website 1 Wort 2 Website 2 Wort 3 Wort 4 Website 3 Wort 5
Richtlinie 2 Alle verweigern	Wort 1 Website 2 Wort 4 Website 3 Wort 5		

Ein Beispiel für die Zusammenführung von drei Richtlinien finden Sie in der unten stehenden Tabelle.

Beispiel 4:

Ursprüngliche Richtlinien	Ursprüngliche Ausnahmen	Resultierende Richtlinie	Resultierende Ausnahmen
Richtlinie 1 Alle zulassen (nur gültig für UC_A)	Keine	UC_A: Alle zulassen	Die Ausnahmen für UC_A und UC_B sind: Wort 1 Website 1 Wort 2 Website 2 Wort 3 Die Ausnahmen für UC_C sind: Wort 4 Website 3 Wort 5
Richtlinie 2 Alle zulassen (gültig für UC_A, UC_B und UC_C)	Wort 1 Website 1 Wort 2 Website 2 Wort 3	UC_B: Alle zulassen	
Richtlinie 3 Alle verweigern (nur gültig für UC_C)	Wort 1 Website 2 Wort 4 Website 3 Wort 5	UC_C: Alle verweigern	

6.5 Anwendungsrichtlinien zusammenführen

Wenn einem Benutzer, Computer oder anderen Objekt mehrere Anwendungsrichtlinien zugewiesen sind, werden diese zusammengeführt. Die nachfolgende Tabelle gibt einen schematischen Überblick über die Zusammenführung von Richtlinien.

Überlappende Richtlinien

Beispiel-Nr.	Ursprüngliche Richtlinien	Ursprüngliche Ausnahmen	Resultierende Richtlinie	Resultierende Ausnahmen
1	Richtlinie 1 Alle zulassen	Anwendungen 1	Alle zulassen	Alle Anwendungen in Anwendungen 1 und 2 ausschließen
	Richtlinie 2 Alle zulassen	Anwendungen 2		
2	Richtlinie 1 Alle verweigern	Anwendungen 1	Alle verweigern	Anwendungen in Anwendungen 1 ausschließen, wenn sie nicht in Anwendungen 2 definiert sind
	Richtlinie 2 Alle zulassen	Anwendungen 2		
3	Richtlinie 1 Alle zulassen	Anwendungen 1	Alle verweigern	Anwendungen in Anwendungen 2 ausschließen, wenn sie nicht in Anwendungen 1 definiert sind
	Richtlinie 2 Alle verweigern	Anwendungen 2		
4	Richtlinie 1 Alle verweigern	Anwendungen 1	Alle verweigern	Anwendungen sowohl in Anwendungen 1 als auch Anwendungen 2 ausschließen
	Richtlinie 2 Alle verweigern	Anwendungen 2		

Nachfolgende Beispiele beziehen sich auf Anwendungslisten.

Beispiel 1:

Ursprüngliche Richtlinien	Ursprüngliche Ausnahmen	Resultierende Richtlinie	Resultierende Ausnahmen
Richtlinie 1 Alle zulassen	Anwendung 1 Anwendung 2 Anwendung 3 Anwendung 4	Alle zulassen	Anwendung 1 Anwendung 2 Anwendung 3 Anwendung 4 Anwendung 5 Anwendung 6
Richtlinie 2 Alle zulassen	Anwendung 1 Anwendung 2 Anwendung 5 Anwendung 6		

Beispiel 2:

Ursprüngliche Richtlinien	Ursprüngliche Ausnahmen	Resultierende Richtlinie	Resultierende Ausnahmen
Richtlinie 1 Alle verweigern	Anwendung 1 Anwendung 2 Anwendung 3 Anwendung 4	Alle verweigern	Anwendung 3 Anwendung 4
Richtlinie 2 Alle zulassen	Anwendung 1 Anwendung 2 Anwendung 5 Anwendung 6		

Beispiel 3:

Ursprüngliche Richtlinien	Ursprüngliche Ausnahmen	Resultierende Richtlinie	Resultierende Ausnahmen
Richtlinie 1 Alle zulassen	Anwendung 1 Anwendung 2 Anwendung 3 Anwendung 4	Alle verweigern	Anwendung 5 Anwendung 6
Richtlinie 2 Alle verweigern	Anwendung 1 Anwendung 2 Anwendung 5 Anwendung 6		

Beispiel 4:

Ursprüngliche Richtlinien	Ursprüngliche Ausnahmen	Resultierende Richtlinie	Resultierende Ausnahmen
Richtlinie 1 Alle verweigern	Anwendung 1 Anwendung 2 Anwendung 3 Anwendung 4	Alle verweigern	Anwendung 1 Anwendung 2
Richtlinie 2 Alle verweigern	Anwendung 1 Anwendung 2 Anwendung 5 Anwendung 6		

7 Remoteverwaltung

7.1 Info über Remoteverwaltung

Remoteverwaltung wird über das **Microsoft Windows-Netzwerk** im Fenster **Netzwerk** aktiviert.

- Suchen Sie nach dem Computer, den Sie verwalten möchten, klicken Sie mit der rechten Maustaste auf den Computernamen, und wählen Sie im Kontextmenü den Befehl **Verwalten**.

Die Fernsteuerungssitzung öffnet im Datenfenster eine neue Registerkarte.

Für den remote verwalteten Computer werden die **Laufwerke**, der **Ereignis-Viewer**, der **Task-Manager**, die **Registrierung**, die **Dienste**, die **Freigabeordner**, der **Bestand**, die **Befehlskonsole**, die **Systemsteuerung** und **Lokale Benutzer und Gruppen** angezeigt.

Wenn Netop Remote Control auf dem Computer installiert ist, auf dem auch die Konsole von Netop ProtectOn Pro installiert ist, wird das Programm Netop Remote Control automatisch in den Fensterbereich **Netop-Sitzungen** integriert.

Andere Programme von Drittanbietern können in ihrem eigenen Fensterbereich installiert werden. Klicken Sie im Menü **Datei** auf **Integration eines Drittanbieter-Programms**. Fügen Sie als ersten Schritt Ihren eigenen Fensterbereich hinzu, und fügen Sie anschließend Verknüpfungen zu wichtigen Programmen hinzu.

Unter Verwendung von **Active Directory** und der Wahl eines Benutzers kann dieser über einen Rechtsklick auf den Benutzernamen und den Befehl **In MMC öffnen** im Kontextmenü verwaltet werden.

7.2 Verwaltungsfenster

Wenn der Administrator eine Remotesitzung über die Konsole gestartet hat, zeigt das Datenfenster der Konsole die verfügbaren Verwaltungstools in drei oder mehr Bereichen an. Die Anzeige des Agentcomputers ändert sich nicht.



Ereignisanzeige

Der erste Bereich ermöglicht den Zugriff auf die **Verwaltungstools**. Über das Menü **Verwaltung** können Sie ebenfalls auf die Tools zugreifen. Dieses Menü wird beim Öffnen einer Remoteverwaltungssitzung zur Netop ProtectOn Pro Menüleiste hinzugefügt.

Weitere Informationen zu den einzelnen Tools finden Sie in den folgenden Abschnitten.

Eigener Bereich und Klassenraumverwaltung

Dieser Bereich ist vollständig benutzerdefiniert und wird nicht vom System vorgegeben. Dieser Abschnitt enthält in Netop ProtectOn Pro integrierte Drittanbieteranwendungen. Weitere Informationen über das Hinzufügen von Bereichen und Anwendungen finden Sie unter [Drittanbieteranwendungen integrieren](#).

Der dritte Bereich im Beispiel-Screenshot ist ebenfalls ein benutzerdefinierter Bereich. Sowohl die Überschrift des Bereichs als auch die integrierten Anwendungen sind vollständig benutzerdefiniert.

Netop Sitzungen

Über den vierten Bereich können Sie auf Befehle von **Netop Sitzungen** zugreifen. Einen kurzen Überblick über die Befehle finden Sie unter [Netop Sitzungen](#)

Details

Der fünfte Bereich dient nur zu Informationszwecken und zeigt folgende Daten an:

- den Namen des Agentcomputers, auf den extern zugegriffen wird
- den Namen des Netzwerks, in dem sich der Agentcomputer befindet
- den Namen des Netzwerks und des Benutzers, der die Fernsteuerungssitzung geöffnet hat
- die IP-Adresse des Agentcomputers
- das Betriebssystem des Agentcomputers
- den Typ des Agentcomputers
- die Dauer der Remoteverwaltungssitzung in folgendem Format: HH:MM:SS

7.3 Laufwerke

Klicken Sie im Bereich Verwaltung auf **Laufwerke**, um verfügbare Laufwerke des Agentcomputers und deren Eigenschaften anzuzeigen.

Verwenden Sie das Tool **Laufwerke**, um einen Überblick über den verfügbaren Festplattenspeicher eines Netzwerkcomputers zu erhalten.

Die Anzeigeeoptionen sind über das Menü **Laufwerke** und über das Kontextmenü verfügbar, das durch Klicken der rechten Maustaste auf das Datenfenster geöffnet wird.

7.4 Ereignisanzeige

Klicken Sie auf **Ereignisanzeige** im Bereich **Verwaltung**, um die Windows-Ereignisprotokolle auf dem Agentcomputer anzuzeigen.

Verwenden Sie das Tool **Ereignisanzeige** für folgende Aktionen:

- Protokolleigenschaften anzeigen und ändern.
- Eigenschaften eines Ereignisprotokolls anzeigen und in die Zwischenablage kopieren.
- Protokolle löschen.
- Ein Protokoll auf dem Administrator- oder Agentcomputer speichern.
- Ein auf dem Administrator- oder Agentcomputer gespeichertes Protokoll öffnen.

Hinweis

Ereignisprotokolle werden nur unter Windows NT oder höheren Versionen (2008, 2003, XP und 2000) aufgezeichnet. Der Befehl "Ereignisanzeige" ist daher nur aktiviert, wenn auf dem Host-Computer Windows NT oder ein höheres Betriebssystem ausgeführt wird.

Wie die Windows-Ereignisanzeige enthält das Tool "Ereignisanzeige" drei Datenkategorien: **Anwendung**, **Sicherheit** und **System**.

Über die vierte Registerkarte **Datei** kann ein gespeichertes Ereignisprotokoll angezeigt werden.

Die folgenden Befehle sind über das Menü **Ereignisanzeige** und über das Kontextmenü verfügbar, das durch Klicken mit der rechten Maustaste auf das Datenfenster geöffnet wird:

Befehl	Beschreibung
Öffnen	Ein Ereignisprotokoll wird geöffnet, das zuvor über den Befehl Speichern gespeichert wurde. Ereignisprotokolldateien haben die Erweiterung .evt.
<hr/> Hinweis Beim Öffnen eines gespeicherten Ereignisprotokolls werden alle ursprünglichen Inhalte der Registerkarte Datei überschrieben.	
Speichern	Ein Ereignisprotokoll wird als Datei an einem angegebenen Ort gespeichert. Die Datei muss die Erweiterung .evt haben.
Löschen	Das Anwendungs-, Sicherheits- oder Systemereignisprotokoll wird von Windows gelöscht.

Sie können die Daten in einer Protokolldatei für eine spätere Überprüfung speichern, bevor das Ereignisprotokoll gelöscht wird. Die Protokolldatei sollte mit der Erweiterung .evt gespeichert werden.

- Aktualisieren** Neue Daten werden vom Agentcomputer abgerufen, um die Registerkartenanzeige zu aktualisieren.
- Protokolleigenschaften** Das Fenster "Eigenschaften" für die Anwendungs-, Sicherheits- oder Systemprotokolldatei wird geöffnet. Protokollgröße und Filtereigenschaften können angezeigt und geändert werden.
- Ereigniseigenschaften** Eigenschaften des ausgewählten Ereignisses werden angezeigt.
Verwenden Sie die Pfeile, um sich in der Ereignisliste nach oben und unten zu bewegen. Klicken Sie auf die Schaltfläche **Kopieren**, um die Protokolleigenschaften in die Zwischenablage zu kopieren.

7.5 Task-Manager

Klicken Sie auf **Task-Manager** im Bereich **Verwaltung**, um Listen mit Anwendungen und Prozessen anzuzeigen, die auf dem Agentcomputer ausgeführt werden.

Das Tool **Task-Manager** funktioniert ähnlich wie der **Windows Task-Manager**, wird allerdings auf einem ferngesteuerten Computer ausgeführt. Das Tool kann verwendet werden, um Anwendungen anzuzeigen und zu steuern, Prozesse zu beenden und um die Computerlasten und Prozessthreads anzuzeigen.

7.6 Registrierung

Klicken Sie auf **Registrierung** im Bereich **Verwaltung**, um die Windows Registrierung auf dem Agentcomputer zu öffnen.

Das Tool **Registrierung** funktioniert ähnlich wie der **Windows Registrierungseditor**, nur auf einem ferngesteuerten Computer.

Info über die Windows Registrierung

Die Windows Registrierung speichert die Konfiguration des Windows Betriebssystems in einer strukturierten Datenbank. Die Registrierung wird beim Installieren von Windows auf dem Computer erstellt und automatisch geändert, sobald Anwendungen installiert und verwendet werden und Benutzer persönliche Einstellungen erstellen oder ändern. Die Registrierungseinstellungen sollten mit Bedacht geändert werden, da fehlerhafte Dateneinträge zu Funktionsstörungen des Computers führen können.

Weitere Informationen zur Erstellung und Änderung von Einträgen finden Sie in der Hilfe des Windows Registrierungseditors.

7.7 Dienste

Klicken Sie auf **Dienste** im Abschnitt **Verwaltung**, um eine Liste mit Diensten anzuzeigen, die auf dem Agentcomputer ausgeführt werden. *Dienste* sind Programme, die im Hintergrund ausgeführt werden können, also nicht angezeigt werden. Sie unterstützen die Funktionen des Betriebssystems bzw. der Anwendungen.

Über das Tool **Dienste** können Sie Dienste des Agentcomputers starten, beenden, unterbrechen, fortsetzen und neu starten. Außerdem können Sie Dienste hinzufügen und entfernen sowie deren Eigenschaften ändern.

Hinweis

Dienste können nur unter Windows NT oder höher (Windows 2008, 2003, XP, 2000 und NT) verwaltet werden. Der Befehl **Dienste** wird daher nur aktiviert, wenn auf dem Agentcomputer Windows NT oder ein höheres Betriebssystem ausgeführt wird.

Die folgenden Befehle sind über das Menü **Dienste** und über das Kontextmenü ausführbar, das sich beim Klicken mit der rechten Maustaste in das Datenfenster öffnet:

Hinzufügen...	Einen Dienst zum Agentcomputer hinzufügen. Folgen Sie den Hinweisen des sich öffnenden Assistenten.
Entfernen	Dienst wird gelöscht. Wenn der Eintrag für einen Dienst gelöscht wird, werden Dienststatus und Autostart-Typ auf Beendet und Deaktiviert gesetzt. Der Eintrag wird entfernt, wenn die Anwendung, die den Dienst verwendet, beendet wird.

Hinweis

Das Löschen eines **Dienst**-Eintrags wirkt sich auf die abhängigen Dienste aus. Abhängigkeiten werden in der Registerkarte **Abhängigkeiten** im Dialogfeld **Eigenschaften** angezeigt: Öffnen Sie das Kontextmenü durch Klicken mit der rechten Maustaste und wählen Sie **Eigenschaften**.

Neustart	Der Dienst wird beendet und neu gestartet.
----------	--

Hinweis

Das Beenden, Unterbrechen oder Neustarten eines Dienstes kann sich auch auf die abhängigen Dienste auswirken. Abhängigkeiten werden in der Registerkarte **Abhängigkeiten** im Dialogfeld **Eigenschaften** angezeigt: Öffnen Sie das Kontextmenü durch Klicken mit der rechten Maustaste und wählen Sie **Eigenschaften**.

Aktualisieren	Neue Daten werden vom Agentcomputer abgerufen, um die angezeigten Daten zu aktualisieren.
Eigenschaften	Die Eigenschaften des Dienstes werden auf drei Registerkarten angezeigt.

Hinweis

Nehmen Sie nur dann Änderungen an den Diensteeigenschaften vor, wenn Sie mit diesem Vorgang vertraut sind. Notieren Sie sich die vorgenommenen Änderungen, um ggf. Eigenschaften wiederherstellen zu können, falls Änderungen zu einem unerwarteten Verhalten führen.

Registerkarte "Allgemein"

Verwenden Sie das Feld **Autostart-Typ**, um festzulegen, wie der Dienst gestartet wird.

Hinweis

Wenn Sie den **Autostart-Typ** in **Deaktiviert** ändern, wird der Status eines bereits gestarteten oder unterbrochenen Dienstes nicht geändert. Wenn der Dienst jedoch beendet wurde, kann er nicht mehr gestartet werden.

Verwenden Sie die Schaltflächen **Starten**, **Beenden**, **Unterbrechen** und **Fortsetzen**, um den Dienst zu steuern.

Das Feld **Startparameter** wird aktiviert, wenn ein Dienst **beendet** wird. Geben Sie alle Parameter ein, die beim Starten des Dienstes angewendet werden sollen, z. B. Befehlszeilenoptionen.

Hinweis

Startparameter werden nicht gespeichert. Ein umgekehrter Schrägstrich (\) wird als ein ESCAPE-Zeichen interpretiert. Geben Sie für jeden umgekehrten Schrägstrich in einem Parameter zwei umgekehrte Schrägstriche an.

☐ **Registerkarte "Anmelden"**

Verwenden Sie die Optionen unter **Anmelden als**, um festzulegen, wie die Anmeldung an einem Dienst über ein anderes Konto erfolgt.

- Verwenden Sie das **Lokale Systemkonto**, um sich mit einem lokalen Systemkonto anzumelden, das über umfassende Berechtigungen für den Agentcomputer, jedoch nicht für andere Computer verfügt (normalerweise die Standardeinstellung).
- Verwenden Sie **Dieses Konto**, um sich als ein bestimmter Benutzer anzumelden, und geben Sie die Anmeldedaten des Benutzers in die Felder ein.

Geben Sie `NT AUTHORITY\LocalService` ein, damit der ausgewählte Agentcomputerdienst das Konto "Lokaler Dienst" verwendet. Geben Sie `NT AUTHORITY\NetworkService` ein, damit das Konto "Netzwerkdienst" verwendet wird. Geben Sie für diese Konten kein Kennwort an; beide Konten verfügen über integrierte Kennwörter.

☐ **Registerkarte "Abhängigkeiten"**

Abhängigkeiten und abhängige Objekte werden angezeigt. Sie können auf dieser Registerkarte keine Abhängigkeiten ändern.

7.8 Freigabeordner

Klicken Sie auf **Freigabeordner** im Bereich **Verwaltung**, um freigegebene Ressourcen des Agentcomputers anzuzeigen und zu verwalten. Außerdem können Sie die Verbindung von Sitzungen trennen, in denen freigegebene Ressourcen und Dateien verwendet werden.

☐ **Registerkarte Freigaben**

Remoteverwaltung

Für Verwaltungs- und Systemzwecke erstellt das Betriebssystem automatisch spezielle Freigaben als verborgene Ressourcen, deren Namen in der Regel auf \$ enden. Spezielle Freigaben sollten weder gelöscht noch geändert werden. Sie werden sonst möglicherweise wiederhergestellt, wenn der Serverdienst beendet und neu gestartet oder der Computer neu gestartet wird.

Diese speziellen Freigaben werden ggf. auf der Registerkarte "Freigaben" angezeigt:

<Laufwerksbuchstabe>\$	Ermöglicht Administratoren die Verbindung mit dem Stammverzeichnis eines Laufwerks.
ADMIN\$	Ermöglicht die Remoteverwaltung eines Computers. Sein Pfad ist immer der Pfad zum Stammverzeichnis des Systems.
IPC\$	Ermöglicht die Kommunikation zwischen Programmen durch benannte Pipes. IPC\$ wird während der Remoteverwaltung eines Computers und beim Anzeigen der freigegebenen Ressourcen eines Computers verwendet und kann nicht gelöscht werden.
NETLOGON	Erforderlich bei Domänen-Controllern. Das Entfernen führt zur Beeinträchtigung von Funktionen auf Client-Computern der Domäne.
SYSVOL	Erforderlich bei Domänen-Controllern. Das Entfernen führt zur Beeinträchtigung von Funktionen auf Client-Computern der Domäne.
PRINT\$	Verwendet bei der Remoteverwaltung von Druckern.
FAX\$	Ein Serverordner, der beim Faxversand von Clients verwendet wird. Dort werden temporäre Faxdateien und Faxdeckblätter gespeichert.

7.9 Bestand

Klicken Sie auf **Bestand** im Abschnitt **Verwaltung**, um einen Überblick über den Hardware- und Softwarebestand des Agentcomputers zu erhalten.

7.10 Befehlskonsole

Klicken Sie im Bereich **Verwaltung** auf **Befehlskonsole**, um ein Eingabeaufforderungsfenster auf dem Agentcomputer zu öffnen. Sie können diese Funktion auch über **Ausführen** im Windows **Startmenü** unter Angabe von `cmd` ausführen; beachten Sie dabei jedoch, dass das Eingabeaufforderungsfenster den *Agentcomputer* anstelle der Konsole anzeigt.

Vor dem Öffnen des Eingabeaufforderungsfensters ist die Eingabe von Anmeldeinformationen (Benutzername, Kennwort und Domäne) erforderlich, die auf dem Agentcomputer gültig sind.

7.11 Systemsteuerung

Klicken Sie auf **Systemsteuerung** im Bereich **Verwaltung**, um den Status des Agentcomputers zu steuern.

In der Systemsteuerung können folgende Aktionen ausgeführt werden:

- Computer sperren (nur Windows NT, 2000 oder XP)
- Benutzer abmelden
- Computer neu starten
- Computer herunterfahren.

Sie können entscheiden, ob der Benutzer vor der Ausführung einer dieser Aktionen gewarnt werden soll, z. B. mit folgender Warnmeldung:

Computerupdates sind erforderlich. Sie werden in wenigen Minuten abgemeldet. Speichern Sie Ihre Arbeit und schließen Sie alle offenen Programme.

Verwenden Sie den Bereich **Optionen**, um festzulegen, ob der Benutzer gewarnt werden soll. Außerdem können Sie die Anzahl der Sekunden zwischen dem Benachrichtigen des Benutzers und dem Ausführen der unter **Durchzuführende Aktion** ausgewählten Aktion angeben.

Abbrechen durch Benutzer zulassen

Normalerweise können Sie einen Befehl der Systemsteuerung nicht abbrechen. Mit Auswahl dieser Option wird jedoch die Schaltfläche **Abbrechen** im Meldungsfenster aktiviert, damit der Benutzer den Befehl abbrechen kann.

Offene Programme schließen, ohne Daten zu speichern

Daten werden in der Regel gespeichert, bevor der ausgewählte Systemsteuerungsbefehl ausgeführt wird. Wählen Sie diese Option, um alle offenen Programme ohne Abspeichern der Daten zu schließen.

7.12 Lokale Benutzer und Gruppen

Klicken Sie auf **Lokale Benutzer und Gruppen** im Abschnitt **Verwaltung**, um Benutzer und Gruppen auf dem Agentcomputer zu verwalten.

Unter **Lokale Benutzer und Gruppen** können Sie folgende Aktionen ausführen:

- Neue Benutzer und Gruppen hinzufügen.
- Eigenschaften von vorhandenen lokalen Benutzern und Gruppen anzeigen und bearbeiten.
- Benutzerkennwörter festlegen.
- Benutzer und Gruppen umbenennen oder löschen.

☐ Registerkarte "Benutzer"

Die Registerkarte **Benutzer** enthält eine Liste mit Benutzern des Agentcomputers.

Im Kontextmenü können folgende Befehle ausgeführt werden:

Remoteverwaltung

Neuer Benutzer Wählen Sie diesen Befehl, um einen neuen Benutzer hinzuzufügen.
Geben Sie im Dialogfeld **Neuer Benutzer** die gewünschten Daten ein, und aktivieren oder deaktivieren Sie kennwort- und kontorelevante Optionen. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

Anmerkungen

Eingegebene Benutzernamen dürfen bereits vorhandenen Benutzer- oder Gruppennamen auf dem verwalteten Computer nicht entsprechen. Ein Gruppenname kann bis zu 20 Groß- oder Kleinbuchstaben bzw. Zeichen enthalten, mit Ausnahme folgender Zeichen: " / \ [] : ; | = , + * ? < > . Ein Benutzername kann nicht nur aus Punkten (.) oder Leerzeichen bestehen.

Ein Kennwort kann bis zu 127 Zeichen enthalten. Wenn Sie jedoch Windows 2000 oder Windows XP in einem Netzwerk verwenden, in dem auch Computer mit Windows 95 oder Windows 98 verwendet werden, wird ein Kennwort mit höchstens 14 Zeichen empfohlen. Windows 95 und Windows 98 unterstützen nur Kennwörter mit bis zu 14 Zeichen. Wenn Ihr Kennwort länger ist, können Sie möglicherweise mit diesen Computern nicht auf Ihr Netzwerk zugreifen.

Kennwort festlegen Wählen Sie diesen Befehl, um das gewählte Benutzerkennwort zu ändern.

Löschen Wählen Sie diesen Befehl, um den gewählten Benutzer zu löschen.

Hinweis

Deaktivieren Sie das Benutzerkonto, bevor Sie es entfernen. Wenn Sie davon ausgehen können, dass die Deaktivierung des Kontos keine Probleme verursacht hat, können Sie es problemlos löschen. Um das Konto zu deaktivieren, wählen Sie **Konto ist deaktiviert** im Dialogfeld **Eigenschaften**. Ein gelöscht Benutzerkonto kann nicht wiederhergestellt werden. Die integrierten Administrator- und Gastkonten können nicht gelöscht werden.

Umbenennen Wählen Sie diesen Befehl, um den gewählten Benutzer umzubenennen. Geben Sie einen neuen Namen ein, und drücken Sie die Eingabetaste, um zu speichern.

Hinweis

Da ein umbenanntes Benutzerkonto seine Sicherheitskennung beibehält, werden auch alle anderen Eigenschaften beibehalten, wie zum Beispiel Beschreibung, Kennwort, Gruppenmitgliedschaften, Benutzerumgebungsprofil, Kontoinformationen sowie alle zugewiesenen Berechtigungen und Rechte. Eingegebene Benutzernamen dürfen bereits vorhandenen Benutzer- oder Gruppennamen auf dem verwalteten Computer nicht entsprechen. Ein Benutzername kann bis zu 20 Groß- oder Kleinbuchstaben bzw. Zeichen enthalten, mit Ausnahme von: " / \ [] : ; | = , + * ? < > . Ein Benutzername kann nicht nur aus Punkten (.) oder Leerzeichen bestehen.

Aktualisieren F5	Wählen Sie diesen Befehl, um neue Daten vom Agentcomputer abzufragen und die Registerkartenanzeige zu aktualisieren.
Eigenschaften	Wählen Sie diesen Befehl, um die Eigenschaften eines Benutzerkontos anzuzeigen und zu ändern. Wenn ein Benutzer über den Befehl Neuer Benutzer erstellt wurde, muss er einer Gruppe hinzugefügt werden. Dazu wird die Registerkarte Mitglied von im Dialogfeld "Eigenschaften" verwendet.

Hinweis

Zur Administratorgruppe hinzugefügte Benutzer erhalten unbegrenzte Zugriffsrechte.

☐ Registerkarte "Gruppen"

Die Registerkarte **Gruppen** enthält eine Liste der Gruppen auf dem Agentcomputer. Im Kontextmenü können folgende Befehle ausgeführt werden:

Neue Gruppe Wählen Sie diesen Befehl, um eine neue Gruppe hinzuzufügen.

Geben Sie im Dialogfeld **Neue Gruppe** die gewünschten Daten ein, und klicken Sie auf **Hinzufügen**, um zur Gruppe vorhandene Benutzer hinzuzufügen. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

Hinweis

Namen von lokalen Gruppen dürfen bereits vorhandenen Gruppen- oder Benutzernamen auf dem verwalteten Computer nicht entsprechen. Ein Gruppenname kann bis zu 256 Groß- oder Kleinbuchstaben bzw. Zeichen enthalten, mit Ausnahme folgender Zeichen: " / \ [] : ; | = , + * ? < > . Ein Gruppenname kann nicht nur aus Punkten (.) oder Leerzeichen bestehen.

Löschen Wählen Sie diesen Befehl, um die gewählte Gruppe zu löschen.

Anmerkungen

Die folgenden integrierten Gruppen können nicht gelöscht werden: Administratoren, Sicherungs-Operatoren, Hauptbenutzer, Benutzer, Gäste, Replikations-Operatoren.

Eine gelöschte Gruppe kann nicht wiederhergestellt werden.

Beim Löschen einer lokalen Gruppe wird nur die Gruppe entfernt; die Benutzerkonten und globalen Gruppen, die Mitglieder dieser Gruppe waren, werden nicht gelöscht.

Wenn Sie eine Gruppe löschen und dann eine andere Gruppe mit demselben Namen erstellen, müssen Sie der neuen Gruppe neue Berechtigungen zuweisen; Berechtigungen werden nicht aus der alten Gruppe übernommen.

Umbenennen Wählen Sie diesen Befehl, um die gewählte Gruppe umbenennen. Geben Sie einen neuen Namen ein, und drücken Sie die Eingabetaste, um den Namen zu speichern.

Hinweis

Da eine umbenannte Gruppe ihre Sicherheitskennung beibehält, werden auch alle anderen Eigenschaften beibehalten, wie zum Beispiel Beschreibung und Mitglieder. Eingegebene Gruppennamen dürfen bereits vorhandenen Benutzer- oder Gruppennamen auf dem verwalteten Computer nicht entsprechen. Ein Gruppename kann bis zu 20 Groß- oder Kleinbuchstaben bzw. Zeichen enthalten, mit Ausnahme folgender Zeichen: " / \ [] : ; | = , + * ? < > . Ein Gruppename kann nicht nur aus Punkten (.) oder Leerzeichen bestehen.

Aktualisieren F5 Wählen Sie diesen Befehl, um neue Daten vom Agentcomputer abzufragen und die Registerkartenanzeige zu aktualisieren.

Eigenschaften Wählen Sie diesen Befehl, um Benutzer zur Gruppe hinzuzufügen oder daraus zu entfernen.

7.13 Drittanbieteranwendungen integrieren

Wenn Sie Anwendungen regelmäßig über Remoteverwaltung verwenden, können Sie Ihren eigenen Bereich im Verwaltungsfenster erstellen und Befehle hinzufügen, um beliebige Drittanbieteranwendungen zu öffnen. Der benutzerdefinierte Bereich im Verwaltungsfenster ist unter dem Bereich "Verwaltung" angeordnet (siehe Abbildung und Beschreibung im Bereich [Verwaltungsfenster](#)). Im benutzerdefinierten Bereich können Drittanbieteranwendungen unterhalb von Überschriften für benutzerdefinierte Gruppen, wie z. B. **Programme** oder **Extras**, hinzugefügt werden.

Eine Drittanbieteranwendung hinzufügen

1. Klicken Sie im Menü **Datei** auf **Integration eines Drittanbieterprogramms**.
2. Klicken Sie auf **Bereich hinzufügen**, um den Bereich zu erstellen und zu benennen.

Die Bereichsüberschrift könnte beispielsweise **Klassenraumverwaltung** lauten.

Beachten Sie, dass der Abschnitt erst angezeigt wird, wenn ein oder mehrere Programme hinzugefügt wurden.

3. Wählen Sie einen Bereich und klicken Sie auf **Programm hinzufügen**.
4. Klicken Sie im Dialogfeld **Programm hinzufügen** auf die Schaltfläche "Durchsuchen", um nach ausführbaren Dateien zu suchen.

Dies könnte zum Beispiel C:\Programme\GenevaLogic\Vision\XL\MeSuAx.exe sein.

Über diese Datei würde das Teacher-Modul von Vision6 hinzugefügt. Beachten Sie, dass das Modul einen Befehlszeilenparameter benötigt, um ordnungsgemäß zu starten: / InvokeVerb:OpenDashboard.

Wenn dieser Parameter zum Feld **Befehlszeile** hinzugefügt wird, wird er automatisch verwendet und zum Feld **Dateiname** hinzugefügt.

Das Feld **Arbeitsordner** wird automatisch aktualisiert.

5. Klicken Sie auf **OK**, um das Programm hinzuzufügen und das Dialogfeld zu schließen.

☐ Optionale Parameter

Zusätzlich zum Namen der ausführbaren Datei können auch optionale Parameter angegeben werden.

Angezeigter Name	Geben Sie den Programmnamen ein, der im neuen Bereich angezeigt werden soll. Wenn dieser Parameter nicht gesetzt ist, wird der Name der ausführbaren Datei (zum Beispiel: excel.exe) angezeigt.
QuickInfo	Geben Sie den Text ein, der angezeigt werden soll, wenn Sie den Mauszeiger über den Programmnamen führen. Wenn dieser Parameter nicht gesetzt ist, wird der Name der ausführbaren Datei (zum Beispiel: excel.exe) angezeigt.
Befehlszeile	Definieren Sie die Programmparameter, mit denen das Programm aufgerufen werden soll: Die folgenden integrierten Parameter können verwendet werden: %%CN: Name des Hostcomputers %%CD: Domäne des Hostcomputers %%LU: am Hostcomputer angemeldeter Benutzer %%LD: am Hostcomputer angemeldete Domäne %%IA: IP-Adresse des Hostcomputers %%MA: MAC-Adresse des Hostcomputers
Arbeitsordner	Wählen Sie den Ordner, in dem die Programmdateien gespeichert werden sollen. Wenn dieser Parameter nicht gesetzt ist, wird der Ordner verwendet, in dem die ausführbare Datei liegt.
Ausführen als	Wählen Sie aus, wie das Programmfenster angezeigt werden soll: Normales Fenster, minimiert, Vollbild, verborgen.

Tipp

Jedes Programm, das auf dem Netop ProtectOn Pro Konsolencomputer installiert ist und über die Befehlszeile ausgeführt werden kann, kann integriert werden. Um erforderliche Befehlszeilenparameter anzuzeigen, öffnen Sie das Dialogfeld "Programmeigenschaften": Klicken Sie mit der rechten Maustaste auf das Windows Startmenü und dann auf **Eigenschaften**.

7.14 Netop Sitzungen

Der Bereich **Netop Sitzungen** ist nur dann verfügbar, wenn

- Netop Remote Control Guest auf dem Computer installiert wurde, auf dem auch die Konsole von Netop ProtectOn Pro installiert ist.
- Netop Remote Control Host auf dem Computer installiert wurde, auf dem auch der Agent von Netop ProtectOn Pro installiert ist.

Die folgenden Befehle sind im Bereich **Netop Sitzungen** verfügbar:

Fernsteuerung Fernsteuerungssitzung mit dem verbundenen Host starten/beenden.

Remoteverwaltung

Dateiübertragung	Dateiübertragungssitzung mit dem verbundenen Host starten/beenden.
Chat	Chat-Sitzung mit dem verbundenen Host starten/beenden.
Audio-Chat	Audio-Chat-Sitzung mit dem verbundenen Host starten/beenden.

Hinweis

Das Starten des **Audio-Chats** ist deaktiviert, wenn nicht sowohl für den Guest- als auch für den Host-Computer interaktives Audio aktiviert wurde bzw. wenn der Guest-Computer eine andere Audio-Sitzung ausführt. Über die Guest-Zugriffssicherheit des Host kann einem Guest-Computer das Starten einer Sitzung verweigert werden. Informationen hierzu finden Sie unter "Guest-Autorisierung" in der Dokumentation zu Netop Remote Control.

Wenn Netop Remote Control nicht auf dem Computer verfügbar ist, auf dem die Konsole von Netop ProtectOn Pro installiert ist, wird der Bereich **Netop Sitzungen** durch den Bereich **Remotedesktop** ersetzt, der auf die **Remotedesktopverbindung** des Betriebssystems zugreift:



Index

6

64-Bit-Unterstützung 4

A

Abkürzungen 17

Active Directory (AD)

Agent remote installieren 12, 20

durchsuchen 14

Fernstarten 19

Objekte 4

offene Sitzung 14

verwalten 16

Agent

allgemeine Einstellungen 11

Benutzeroberfläche 11

Protokollierungseinstellungen 11

Agent installieren 12, 20

Agent remote installieren 12, 20

Agent verteilen 12, 20

Akronyme 17

Andere Richtlinien überschreiben 43

Anwendungsrichtlinie 4

Registerkarte Anwendung 42

Ausnahmeordner 34

Autostart-Informationen 70

B

Befehlskonsole 70

Benachrichtigung senden 29

Benachrichtigung vor Neustart 29

Benutzer vor Neustart warnen 29

Benutzeroberfläche

Agent 11

NDC-Konsole 14

Task-Leiste 11

Benutzeroberfläche des Agents 11, 14

Bestand 70

Betriebssysteme – unterstützt 6

Bluetooth Adapter 31

Bluetooth Geräte 40

C

CD-ROM-Laufwerke 40

Computer-Details anzeigen 17

D

Datenbank 7

Datenbank ändern 7

Datenfenster 14

Dienste 67

Diskettenlaufwerke 40

E

einer Gruppe zuordnen 23

Ereignisanzeige 66

F

Fenster Netzwerk 15

Fenster Remoteverwaltung 64

Festgelegte Richtlinie 25

Festplatteninhalt verbergen 34

FireWire (IEEE 1394) Ports 40

Freigabeordner

Registerkarte Allgemein 69

Registerkarte Dateien öffnen 69

Registerkarte Freigabeberechtigungen 69

Registerkarte Freigaben 69

Registerkarte Sitzung 69

spezielle Freigaben 69

Funktionen 3

G

Geräteliste 25

GPMC (Verwaltungskonsole für Gruppenrichtlinien) 16

GPOE (Objekteditor für Gruppenrichtlinien) 16

Gruppe 4

erstellen 14

gültige Richtlinien 37

umbenennen 23

Gruppe umbenennen 23

Index

Gruppen erstellen 14
gültige Richtlinien einer Gruppe 37

I

IrDA-Geräte 40

L

Laufwerke 66
Laufwerkstypen 66
Lokale Benutzer und Gruppen 71

M

Microsoft Management Console (MMC) 64
MMC (Microsoft Management Console) 64

N

Netzwerkcomputer fernstarten 19
Neustarten 29

O

Objekt
 Active Directory (AD) 4
 Windows Domäne 4

Objekteditor für Gruppenrichtlinien (GPOE)
16

P

Parallele Schnittstellen 40

R

Regeln
 Zusammenführen von Richtlinien 44
Registerkarte Allgemein 69
Registerkarte Dateien öffnen 69
Registerkarte Festplattenschutz
 ausgewählte Laufwerke schützen 38
 Ausnahmeanwendungen 38
 Ausnahmeordner 38
 Ausnahmeprozesse 38
 Wiederherstellen aktivieren 38
Registerkarte Freigabeberechtigungen 69
Registerkarte Freigaben 69
Registerkarte Gerätezugriff
 Berechtigungen 40

Registerkarte Sitzung 69
Registerkarte Zeitplan 29
Registrierung
 Schlüsselfenster 67
 Wertefenster 67
Remoteverwaltung 64
 Dienste 67
 Ereignisanzeige 66
 Laufwerke 66
 Registrierung 67
 Task-Manager 67
 Windows-Ereignisprotokoll 66

Richtlinie 4
 erstellen 14, 29
 festlegen 25
 Servereinstellungen 10
 überschreiben 14
 umbenennen 38
 Zeitplan 43
 Zuweisen 43
Richtlinie überschreiben 14
Richtlinie umbenennen 38
Richtlinie zum Festplattenschutz 4
Richtlinie zum Gerätezugriff 4, 25
 USB-Klasse 32
 Zugriffsrechte 31

Richtlinien erstellen 14, 29
Richtlinien festlegen
 Richtlinie zum Festplattenschutz 25
Richtlinien zuweisen 43
Richtlinieneditor 14
Richtliniensymbole 14
rotes X 11

S

Serielle Schnittstellen 40
Server 10
Servereinstellungen 10
Sitzung
 auf Netzwerkcomputer öffnen 14
Sitzungen 75

<p>spezielle Freigaben 69</p> <p>Symbole 14</p> <p>Symbolleiste 14</p> <p>Systeminformationen 17</p> <p>Systemsteuerung</p> <ul style="list-style-type: none"> aktueller Hoststatus 71 durchzuführende Aktionen 71 Optionen 71 <p>T</p> <p>Tape-Laufwerke 40</p> <p>Task-Leiste (Benachrichtigungsbereich)</p> <ul style="list-style-type: none"> Agentsymbol – grau 11 Agentsymbol – rotes X 11 <p>Task-Manager 67</p> <p>U</p> <p>Überwachungsgrade 40</p> <p>USB</p> <ul style="list-style-type: none"> Computer durchsuchen 36 Datenbank 35, 36 Lokale Geräte 36 USB-Geräteklasse hinzufügen 35 <p>USB-Datenbank 35, 36</p> <p>USB-Geräte 40</p> <p>USB-Klasse 35</p> <p>USB-Klasse auswählen 35</p> <p>V</p> <p>Verwaltungskonsole für Gruppenrichtlinien (GPMC) 16</p> <p>W</p> <p>Weberichtlinie 4</p> <ul style="list-style-type: none"> Registerkarte Internet 41 <p>Wechseldatenträger 40</p> <p>Weißer Liste 32</p> <p>Weißer Liste für USB 32</p> <p>Wiederherstellen 29</p> <p>WiFi-Adapter 31</p> <p>WiFi-Geräte 40</p> <p>Windows Netzwerk</p>	<ul style="list-style-type: none"> Agent remote installieren 12, 20 durchsuchen 15 Fernstarten 19 mit Domäne verbinden 15 Objektdetails 17 Objekte 4 offene Sitzung 14 <p>Windows-Ereignisprotokoll 66</p> <p>Z</p> <p>Zeitplanrichtlinie 43</p> <p>Zugriff auf Datenträger 34</p> <p>Zugriffsrechte 40</p> <ul style="list-style-type: none"> CD 31 CD-ROM-RW 31 DVD 31 Gerätetypen 31 pro Einzelgerät 31 <p>zuordnen</p> <ul style="list-style-type: none"> hinzufügen 23 <p>Zusammenführen</p> <ul style="list-style-type: none"> Anwendungsrichtlinien 61 Richtlinien zum Festplattenschutz 46 Richtlinien zum Gerätezugriff 47 von Anwendungsrichtlinien 61 von Richtlinien zum Gerätezugriff 47 von Weberichtlinien 58 Weberichtlinien 58 zweier Richtlinien zum Festplattenschutz 46 <p>Zwei Richtlinien zusammenführen 44</p>
---	---