

Webcode - Übungsdateien

F9BC-494A-D89B



Stattl. Berufsschule I Landshut - HERDT|Campus - Jahreslizenz

In Kooperation mit dem HERDT-Verlag stellen wir Ihnen eine PDF inkl. Zusatzmedien für Ihre persönliche Weiterbildung zur Verfügung. In Verbindung mit dem Programm HERDT-Campus ALL YOU CAN READ stehen diese PDFs nur Lehrkräften und Schüler\*Innen der oben genannten Lehranstalt zur Verfügung. Eine Nutzung oder Weitergabe für andere Zwecke ist ausdrücklich verboten und unterliegt dem Urheberrecht. Jeglicher Verstoß kann zivil- und strafrechtliche Konsequenzen nach sich ziehen.

## Windows 10

Thomas Joos

Systembetreuer: Workstation

2. Ausgabe, September 2018

W10S



ISBN 978-3-86249-831-4

Schulversion

<b>1 Informationen zu diesem Buch</b>	<b>4</b>	<b>7 Microsoft Management Console (MMC)</b>	<b>74</b>
1.1 Voraussetzungen und Ziele	4	7.1 Konsole und Snap-Ins	74
1.2 Aufbau und Konventionen	5	7.2 Mit der MMC lösbarer Aufgaben	75
<b>2 Das Betriebssystem Windows 10</b>	<b>8</b>	7.3 Aufbau und Menüs der MMC	76
2.1 Windows 10 einsetzen	8	7.4 Konsole erstellen und anpassen	77
2.2 Dateisysteme für Windows 10	10	7.5 Aufgabenblocks und Aufgaben erstellen	79
2.3 Die Windows-10-Oberfläche	12	7.6 Konsole sichern und Zugriff beschränken	81
2.4 Windows 10 mit Tastenkombinationen bedienen	13	7.7 MMC-Konsole öffnen	83
2.5 Weitere Änderungen bei Windows 10 im Vergleich zu Windows 7/8	13	7.8 Windows Server 2012 R2/2016 mit Windows 10 verwalten	83
2.6 Übung	15	7.9 Virtualisieren mit Windows 10	84
		7.10 Übung	87
<b>3 Grundlagen des Netzwerkbetriebs</b>	<b>16</b>	<b>8 Netzwerkeinstellungen verwalten</b>	<b>88</b>
3.1 Aufbau von Netzwerken	16	8.1 Netzwerkidentifikation ändern	88
3.2 Netzwerkprotokolle	19	8.2 Netzwerkeinstellungen ändern	91
3.3 Identifikation im Netzwerk	21	8.3 Netzwerkkomponenten verwalten	99
3.4 Übung	22	8.4 Übung	99
<b>4 Installation</b>	<b>24</b>	<b>9 Hardware hinzufügen</b>	<b>100</b>
4.1 Die Installation vorbereiten	24	9.1 Hardware-Komponenten und Treiber verwenden	100
4.2 Installationsdateien bereitstellen	28	9.2 Hardware automatisch installieren	101
4.3 Windows 10 neu installieren	29	9.3 Hardware manuell konfigurieren	103
4.4 Systemeinstellungen vornehmen	31	9.4 Hardware deaktivieren und deinstallieren	104
4.5 Auf Windows 10 aktualisieren	34	9.5 Treiber- und Hardware-Probleme behandeln	105
4.6 Windows 10 aktivieren	35	9.6 Übung	107
4.7 Updates installieren	37		
4.8 Fehlerbehandlung	37		
4.9 Übung	39		
<b>5 Systemstart</b>	<b>40</b>	<b>10 Internetzugang einrichten und konfigurieren</b>	<b>108</b>
5.1 Der Bootvorgang	40	10.1 Internetzugang – Grundlagen	108
5.2 Windows 10 startet	44	10.2 Internetzugang einrichten	110
5.3 Die Anmeldung	45	10.3 Internetzugang konfigurieren	110
5.4 Optionen des Systemstarts	46	10.4 Internet Explorer und Microsoft Edge konfigurieren	113
5.1 Übung	49	10.5 Microsoft Edge – Der neue Microsoft Browser	117
		10.6 Remotedesktop einrichten	120
		10.7 Übung	122
<b>6 Anpassungen</b>	<b>50</b>		
6.1 Workstation konfigurieren – die Systemsteuerung	50	<b>11 Lokale Benutzerverwaltung</b>	<b>122</b>
6.2 Desktop anpassen	52	11.1 Konzept der Benutzerverwaltung	122
6.3 Anzeigeeigenschaften einstellen	52	11.2 Anmelden	125
6.4 Anwendungsprogramme installieren	56	11.3 Benutzer verwalten	127
6.5 Windows-10-Einstellungen vornehmen	57	11.4 Lokale Gruppen verwalten	132
6.6 Windows-Funktionen aktivieren/deaktivieren	60	11.5 Benutzerumgebung verwalten	133
6.7 Aktuelle Konfiguration einsehen und dokumentieren	62	11.6 Benutzerprofile verwalten	134
6.8 Einstellungen des Betriebssystems ändern	63	11.7 Windows Hello – Anmeldung an Windows 10 mit Gesichtserkennung oder Biometrie	136
6.9 Dienste starten und verwalten	66	11.8 Übung	137
6.10 Geräte aktivieren und deaktivieren	69		
6.11 Energieverwaltung	69		
6.12 Der Sprachassistent Cortana	71	<b>12 Gruppenrichtlinien</b>	<b>138</b>
6.13 Virtuelle Desktops erstellen und steuern	72	12.1 Grundlagen zu Gruppenrichtlinien	138
6.14 Übung	72	12.2 Richtlinien mit der MMC verwalten	140
		12.3 Computerkonfiguration	141
		12.4 Benutzerkonfiguration	143

12.5 Anwendungsbeispiele	144	<b>17 Die Registrierungsdatenbank</b>	<b>204</b>
12.6 Sicherheitsvorlagen verwenden	145	17.1 Die Windows-10-Registrierung	204
12.7 Gruppenrichtlinien-Einstellungen – Erweiterte Möglichkeiten	147	17.2 Registrierungsdaten ansehen	206
12.8 Windows 10 mit Gruppenrichtlinien verwalten	148	17.3 Registrierungsdaten bearbeiten	207
12.9 Übung	151	17.4 Registrierungsdaten hinzufügen	209
17.5 Schlüsselsicherheit verwalten	210		
<b>13 Zugriffsberechtigungen und Freigaben</b>	<b>152</b>	<b>18 Speicherplätze und Sicherungsmethoden</b>	<b>212</b>
13.1 Ressourcen gemeinsam nutzen	152	18.1 Speicherplätze – Speicherpools und virtuelle Datenträger	212
13.2 Berechtigungen auf Freigabeebene einsetzen	154	18.2 Dateisicherung	216
13.3 NTFS-Berechtigungen einsetzen	155	18.3 Sicherungen mit dem Dateiversionsverlauf	217
13.4 NTFS-Berechtigungen verwalten	157	18.4 Dateiversionen wiederherstellen	220
13.5 Übung	159	18.5 Wiederherstellung	220
		18.6 Übung	223
<b>14 Drucker und Druckgeräte</b>	<b>160</b>	<b>19 Eingabeaufforderung und PowerShell</b>	<b>224</b>
14.1 Drucken im Netzwerk	160	19.1 Nutzen der Eingabeaufforderung	224
14.2 Drucker installieren	162	19.2 Die Eingabeaufforderung anpassen	225
14.3 Drucker konfigurieren	166	19.3 Eingabeaufforderung und Batchdateien	226
14.4 Druckerwarteschlange verwalten	168	19.4 Die PowerShell – ein kurzer Überblick	229
14.5 Druckaufträge verwalten	169	19.5 Übung	231
14.6 Berechtigungen und Gruppen verwalten	171		
14.7 Mehrere Druckerwarteschlangen verwalten	172	<b>20 Windows 10 aktualisieren</b>	<b>232</b>
14.8 Probleme beim Drucken beheben	173	20.1 Betriebssystem-Software aktualisieren	232
14.9 Übung	173	20.2 Windows Update verwenden	232
		20.3 Probleme mit Windows Updates beheben	236
		20.4 Client-Computer über Gruppenrichtlinien an Windows Server Update Services anbinden	237
		20.5 Übung	238
<b>15 Datenträgerverwaltung</b>	<b>174</b>	<b>21 Fehlerdiagnose und Fehlerbehebung</b>	<b>239</b>
15.1 Datenträger und Volumes	174	21.1 Allgemeine Hinweise zur Fehlerbehandlung	239
15.2 Datenträger und Volumes einrichten	177	21.2 Hilfe und Problembehandlung	240
15.3 Volumes verwalten	180	21.3 Support mit Remotehilfe leisten	242
15.4 Kontingente zuweisen	183	21.4 Problemaufzeichnung/Schrittaufzeichnung verwenden	244
15.5 BitLocker benutzen	184		
15.6 Übung	187	<b>Stichwortverzeichnis</b>	<b>246</b>
<b>16 Systemüberwachung und -pflege</b>	<b>188</b>		
16.1 Ereignisanzeige	188		
16.2 Task-Manager und Problemanalyse	191		
16.3 Auslastung der Netzwerksfreigaben kontrollieren	194		
16.4 Leistungsüberwachung	195		
16.5 Wartungscenter	200		
16.6 Datenschutzeinstellungen in Windows 10 beachten	202		
16.7 Übung	203		

# 1 Informationen zu diesem Buch

## In diesem Kapitel erfahren Sie

- ✓ wie Sie dieses Buch einsetzen können
- ✓ welche Vorkenntnisse Sie mitbringen sollten
- ✓ welche Konventionen für dieses Buch gelten

## 1.1 Voraussetzungen und Ziele

### Zielgruppe

Dieses Buch wendet sich an Systembetreuer, deren Aufgabe der Support von Arbeitsstationen unter Windows 10 sein wird. Es ist gleichermaßen für Kursteilnehmer mit Support-Erfahrungen mit älteren Windows-Betriebssystemen geeignet wie für Neueinsteiger in die Systembetreuung.

### Empfohlene Vorkenntnisse

Voraussetzung für die erfolgreiche Arbeit mit diesem Buch sind Grundkenntnisse in der PC-Technik und im Umgang mit modernen Windows-Betriebssystemen. Hilfreich ist Erfahrung im Support von Computern unter Windows XP, Windows Vista und insbesondere Windows 7/8.1/10.

### Lernziele

Nach dem Durcharbeiten des Buches besitzen Sie fundierte Kenntnisse im Umgang mit dem Betriebssystem Windows 10 und seiner neuen Windows-10-Oberfläche und können die wesentlichen Konfigurationsaufgaben erledigen. Sie sind in der Lage, Windows 10 auf Arbeitsplatz-Computern zu installieren und korrekt zu konfigurieren. Sie können neue Hardware hinzufügen und einrichten, Drucker installieren und verwalten sowie die Werkzeuge für lokale Benutzeroberfläche einsetzen. Sie sind in der Lage, die Berechtigungen für Ressourcen (Dateien, Drucker usw.) zu vergeben und anzupassen. Ferner können Sie das System in ein lokales Netzwerk integrieren, die Hilfsprogramme für die Systemverwaltung verwenden und Fehler beheben.

### Hinweise zu Soft- und Hardware

Für die erfolgreiche Arbeit mit diesem Buch benötigt jeder Kursteilnehmer einen PC unter Windows 10, bei nur einem Kursteilnehmer wird ein zusätzlicher Computer benötigt. Die Computer müssen über einen Netzwerkadapter verfügen und über ein TCP/IP-Netzwerk miteinander verbunden werden können. Ein Internetzugang ist erforderlich, nicht jedoch die Mitgliedschaft in einer Windows-Domäne.

Das Buch beschreibt den vollen Funktionsumfang von Windows 10 Enterprise. Diese Edition verfügt über alle Funktionen von Windows 10. Einige der beschriebenen Funktionen wie z. B. BitLocker sind in der Edition Windows 10 Home nicht verfügbar, dafür aber in den Editionen Pro und Education.



Der Begriff Windows 10 steht zum einen für die **gesamte Betriebssystem-Familie** und zum anderen für die **Einsteigerversion**.

Downloadbare ISO-Images einer 90-Tage-Testversion von Windows 10 Enterprise als 32- und 64-Bit-Version finden Sie unter <https://technet.microsoft.com/de-de/evalcenter>. Verfügen Sie über eine gültige Lizenz von Windows 7/8.1, können Sie sich die ISO-Datei von Windows 10 bei Microsoft kostenlos auf der Seite <https://www.microsoft.com/de-de/software-download/windows10> herunterladen. Die kostenlose Aktualisierung ist nicht für die Enterprise-Edition möglich.

Die Testversion eignet sich für Neuinstallationen und Upgrades von älteren Windows-Versionen. Sie benötigt **keinen Produktschlüssel**. Die Testversion muss jedoch spätestens nach 10 Tagen aktiviert werden, anderenfalls fährt das System nach einer Stunde automatisch herunter. Der Testzeitraum kann nicht verlängert werden. Deshalb muss das Testsystem nach Ablauf des Testzeitraums neu installiert werden. Ein späteres Upgrade ist nicht möglich, daher sollten Sie die Testversion nicht auf Produktivsystemen installieren.

Alle anderen Windows-Versionen benötigen für die Installation einen **gültigen Produktschlüssel**. Für weitere Informationen besuchen Sie <http://www.microsoft.com/de-de/windows>.

## 1.2 Aufbau und Konventionen

### Aufbau des Buches

Sie finden in diesem Buch thematisch gegliederte Kapitel, die Ihnen in der Regel zunächst jeweils die theoretischen Grundlagen und anschließend die praktische Vorgehensweise zur Erledigung einer bestimmten Konfigurationsaufgabe näherbringen. Die praktischen Teile der Kapitel enthalten jeweils Arbeitsanleitungen, die Sie durch die Arbeitsschritte einer bestimmten Verwaltungsaufgabe führen.

### Inhaltliche Gliederung

Nach einer Einführung in die Grundlagen des Betriebssystems Windows 10 und den Betrieb von Computer-Netzwerken erhalten Sie Informationen zur Installation von Windows 10 auf einem Arbeitsplatzrechner.

Nach einer Beschreibung der Vorgänge beim Systemstart werden Sie mit den Möglichkeiten vertraut gemacht, die Windows 10 zur individuellen Anpassung an verschiedene Benutzer und Einsatzbereiche bietet.

Den Hauptteil des Buches bilden Beschreibungen der Lösung typischer Verwaltungsaufgaben, die auf einem Arbeitsplatzrechner unter Windows 10 anfallen.

Abschließend erhalten Sie Informationen zu seltener anfallenden Aufgaben, zur Systemüberwachung und -pflege sowie zur Fehlerdiagnose und -behebung.

### Typografische Konventionen

Damit Sie bestimmte Elemente auf einen Blick erkennen und zuordnen können, werden diese im Text durch eine besondere Formatierung hervorgehoben. So werden beispielsweise Bezeichnungen für Programmelemente wie Register oder Schaltflächen immer *kursiv* geschrieben und wichtige Begriffe **fett** hervorgehoben.

Kursivschrift	kennzeichnet alle vom Programm vorgegebenen Bezeichnungen für Schaltflächen, Dialogfenster, Symbolleisten, Menüs bzw. Menüpunkte, Datei- und Verzeichnisnamen sowie Internetadressen.
Courier	wird für Systembefehle und Benutzereingaben verwendet.
Spitze Klammern <>	kennzeichnen Platzhalter.

### Was bedeuten die Symbole im Buch?



Hilfreiche Zusatzinformation



Praxistipp



Warnhinweis

## HERDT BuchPlus – unser Konzept:

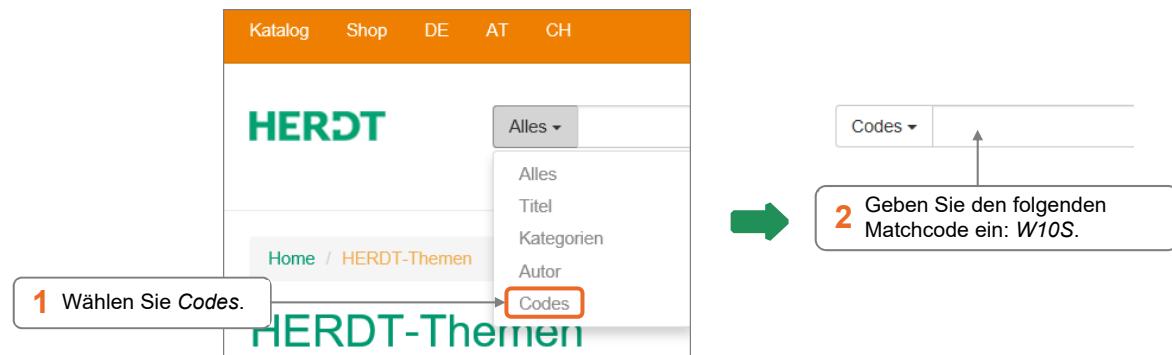
Problemlos einsteigen – Effizient lernen – Zielgerichtet nachschlagen

(weitere Infos unter [www.herdt.com/BuchPlus](http://www.herdt.com/BuchPlus))

Nutzen Sie dabei unsere maßgeschneiderten, im Internet frei verfügbaren Medien:



- ▶ Rufen Sie im Browser die Internetadresse [www.herdt.com](http://www.herdt.com) auf.





## 2 Das Betriebssystem Windows 10

### In diesem Kapitel erfahren Sie

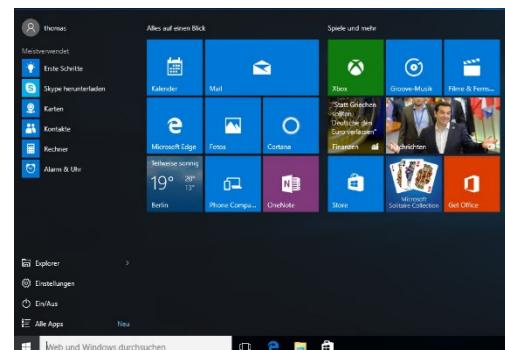
- ✓ für welchen Einsatzbereich Windows 10 konzipiert wurde
- ✓ wie Windows 10 aufgebaut ist
- ✓ wie Sie die Windows-10-Oberfläche bedienen

### 2.1 Windows 10 einsetzen

#### Entwicklung der Windows-Familien

Mit Windows 10 ist es erstmalig möglich, eine neue Windows-Version nicht nur von der Vorversion (Windows 8 und Windows 8.1) zu aktualisieren, sondern auch von der **Version davor**, also Windows 7. Sie können Rechner mit Windows 7/8/8.1 kostenlos zu Windows 10 aktualisieren, mit Ausnahme der Enterprise-Edition. Da diese aber in den meisten Fällen in Verbindung mit speziellen Verträgen an Kunden ausgeliefert wird, steht auch diese Edition kostenlos zur Verfügung.

Das neue Betriebssystem basiert im Wesentlichen auf der gleichen technischen Plattform wie seine Vorgänger Windows 7/8/8.1. Die Benutzeroberfläche und vor allem das Startmenü wurden im Vergleich zu Windows 7 jedoch stark verändert, im Vergleich zu Windows 8/8.1 ebenfalls. Das klassische Startmenü aus Windows 7 ist einem Startmenü mit einer zusätzlichen bunten Oberfläche gewichen, die auf zahlreichen bunten **Kacheln** die wichtigsten Anwendungen anzeigt. Die Anwendungen für die Windows-10-Oberfläche werden als **Apps (Applications)** oder **Windows-10-Apps** bezeichnet, wie sie von Smartphones bekannt sind. Diese unterscheiden sich von herkömmlichen Anwendungen in der **Art der Installation** und der **Oberfläche**. Die Installation erfolgt über den **App-Store**, der ebenfalls als Kachel zur Verfügung steht.



Das Windows-10-Startmenü ersetzt die Startseite von Windows 8

Die Oberfläche ist für Berührungen optimiert, lässt sich aber auch mit der Maus durchführen. Im Gegensatz zu Windows 7/8.1 wurde Windows 10 für den Einsatz mit Maus und Tastatur optimiert. Der Desktop verhält sich in Windows 10 wie in Windows 7. Die Erstellung weiterer, virtueller Desktops ist erlaubt. Das war mit Zusatzttools bereits in Windows 7/8 möglich, ist jetzt aber fest in das Betriebssystem integriert. Hier gibt es im Grunde keine Unterschiede in der Bedienung. Die Windows-10-Oberfläche ist an die Oberfläche moderner Kommunikationsgeräte angepasst, sodass die Bedienung und Funktionalität auf einem Handy, Tablet, Notebook und Desktop-PC gleich oder sehr ähnlich ist.

Eine Einführung in die neue Windows-10-Oberfläche finden Sie im Kapitel 2.3.

#### Einsatzbereich von Windows 10

Im **Privatbereich** wird Windows 10 entweder in kleinen Heimnetzwerken oder als Einzelgerät eingesetzt. Eine Verbindung zum Internet ist zur sinnvollen Verwendung erforderlich. Nur darüber lassen sich Apps installieren und notwendige Windows-Updates herunterladen.

Im **professionellen Bereich** kann Windows 10 als **Client-Computer** ins Firmennetzwerk eingebunden werden. In diesen Netzwerken mit **Client-Server-Architektur** gibt es generell zwei Typen von Computern: die Clients und die Server. Ein **stationärer Client** wird auch als **Workstation** oder **Arbeitsplatzrechner** bezeichnet. Der Client gewährt dem Benutzer den Zugriff auf Programme und Anwendungen, während der Server Netzwerkfunktionalitäten wie zentrale Datenspeicherung, Benutzerverwaltung, Informationsverwaltung und Druckdienste oder Internetzugang bietet.

Neben den stationären Clients setzen Außendienstmitarbeiter zunehmend **mobile Geräte** wie Notebooks, Tablets oder Smartphones ein. Diesen Geräten müssen die Firmendaten über das Internet zugänglich gemacht werden und trotzdem soll eine hohe Sicherheit gewährleistet bleiben. Windows 10 ist noch stärker als Windows 7 auf sicheren mobilen und flexiblen Einsatz ausgerichtet. Anwender können zwischen Tablet, Smartphone und PC sehr einfach Daten austauschen.

Windows 10 ist ein Client-Betriebssystem für **x86-Computer**. Es gab mit Windows 8 die spezielle Version Windows RT als eine Variante für mobile Geräte mit ARM-Prozessor. Auf der RT-Version laufen jedoch keine x86-Anwendungen. Mit Windows 10 hat Microsoft Windows RT eingestellt. Auf Smartphones und kleinen Tablets wird **Windows 10 for Mobile** installiert. Windows 10 for Mobile nutzt den gleichen Systemkern wie andere Windows-10-Versionen. Als Server-Betriebssystem dienen Windows Server 2012/2012 R2 und die neue Version Windows Server 2016 sowie dessen Nachfolger Windows Server 1709/1803 und Windows Server 2019. Alle Systeme auf allen Plattformen basieren auf demselben Windows-Kern, unterscheiden sich jedoch in Funktionsumfang und Einsatzzweck. Die Benutzer sollen ihre Aufgaben auf verschiedenen Geräten ortsunabhängig erledigen können. Besonders wichtig ist, dass Mitarbeiter einer Firma auch unterwegs niemals den Unternehmenskontext mit seinen detaillierten Sicherheitseinstellungen und Vorgaben verlassen. Ein Smartphone oder Tablet soll genauso zu administrieren sein wie der herkömmliche Arbeitsplatzrechner.

## Editionen von Windows 10

Die Anzahl der Windows-10-Editionen wurde im Vergleich zu Windows 7 stark reduziert.

Mögliche Windows-10-Editionen und ihre Unterscheidungsmerkmale:

Windows 10	Diese Edition ist für <b>Privatbenutzer</b> vorgesehen. Sie enthält keine Datei- und Festplattenverschlüsselung und kann keine VHD-Images booten. Auf Rechner mit dieser installierten Windows-10-Version kann nicht per Remote Desktop zugegriffen werden, sie können keiner Domäne beitreten und lassen sich nicht per Gruppenrichtlinien verwalten. Windows-Updates werden automatisch installiert, Benutzer können die Installation nicht beeinflussen.
Windows 10 Pro	<b>Professionelles Betriebssystem für Unternehmen.</b> Was in der oben genannten Version nicht geht, ist unter der Pro-Edition freigeschaltet. Zusätzlich gibt es zur Desktop-Virtualisierung den Hyper-V-Client. Die Installation von Windows-Updates lässt sich anpassen.
Windows 10 Enterprise und Windows 10 Education	Für die Enterprise-Edition ist der Abschluss eines Software Assurance Agreements zwingend erforderlich, damit richtet sich diese Version ganz klar an <b>Unternehmen</b> . Aus diesem Grund sollen in diese Edition zusätzlich zu den Features der Pro-Version Funktionalitäten für große IT-Strukturen implementiert werden, was Management, Deployment, Sicherheit und Virtualisierung betrifft. Der Enterprise-Edition vorbehalten bleiben Windows To Go, DirectAccess, AppLocker und BranchCache sowie die Möglichkeit, Windows-10-Apps unter Umgehung des Windows Stores zu installieren. Auch hier lässt sich die Installation von Windows-Updates konfigurieren. Windows 10 Education entspricht den Funktionen von Windows 10 Enterprise und ist für Bildungseinrichtungen und Schulen konzipiert worden.

<b>Windows 10 for Mobile</b>	Windows 10 for Mobile ist die Windows-Version für <b>Smartphones und kleine Tablets</b> . Sie wird von den Providern vorinstalliert, aber von Microsoft aktualisiert.
<b>Windows 10 S</b>	Bei Windows 10 S handelt es sich um eine stark abgespeckte Version von Windows 10, die zum Beispiel von Schülern oder Lehrern genutzt werden kann. Generell handelt es sich dabei um eine angepasste Version von Windows 10 Pro, das nur Apps aus dem Windows-Store unterstützt.

Die Installation zusätzlicher **Sprachpakete** ist jetzt (bis auf einige landesspezifische Versionen wie z. B. die chinesische) in allen Editionen möglich.

 Windows 10 unterstützt nur einen physischen Prozessor, während die Pro- und die Enterprise-Edition zwei physische Prozessoren unterstützen. Alle 32-Bit-Versionen von Windows 10 unterstützen bis zu 32 Prozessorkerne und alle 64-Bit-Versionen bis zu 256 Prozessorkerne.

 Eine Upgrade-Installation von Windows XP oder Windows Vista zu Windows 10 ist nicht möglich. Sie können nur von Windows 7 und Windows 8.1 zu Windows 10 aktualisieren.

#### **Ergänzende Lerninhalte:** *Die Architektur von Windows 10.pdf*

Hier erfahren Sie, welche Funktionen für den professionellen Anwender interessant sind und wie Windows aufgebaut ist.

## 2.2 Dateisysteme für Windows 10

### Verfügbare Dateisysteme

Das Dateisystem eines Datenträgers legt fest, wie und mit welchen Zusatzinformationen die Daten abgelegt werden. Das Dateisystem enthält Begrenzungen von Größe und Anzahl der darauf gespeicherten Dateien, die meist nach einigen Jahren eine Erweiterung oder eine Umstellung des Dateisystems erforderlich machen. Unter Windows gibt es für Festplatten und Wechseldatenträger folgende wichtige Dateisysteme:

- ✓ **NTFS** (New Technology File System) ist seit mehr als zehn Jahren das Standard-Dateisystem aller Windows-Versionen.
- ✓ **FAT** (File Allocation Table) stammt noch aus der MS-DOS-Ära, wird aber auch heute noch als FAT16 bei Flashspeichern bis 2 GB und als FAT32 bei externen Festplatten und USB-Sticks eingesetzt.
- ✓ **exFAT** (Extended FAT) wurde mit Windows Embedded CE 6.0 eingeführt und wird vor allem für die Formatierung von Flashspeichern verwendet (z. B. SDXC; **SD-eXtended Capacity Cards**).

Windows 10 lässt sich genau wie seine Vorgänger ausschließlich auf NTFS-Partitionen installieren, Sie sollten aber auch bei weiteren Partitionen grundsätzlich das Dateisystem NTFS einsetzen. FAT32 oder exFAT sollten Sie nur einsetzen, wenn dafür ein besonderer Grund vorliegt.

Windows 10 unterstützt Datenträger, die mit FAT16, FAT32 oder exFAT formatiert sind, kann jedoch keine FAT32-Partitionen über 32 GB erstellen. Beim ältesten Dateisystem FAT16 und bei FAT32 sind die maximale Datenträger- und Dateigröße sowie Datensicherheit und Zugriffsschutz stark eingeschränkt. Obwohl alle externen Datenträger mit exFAT formatiert werden können, sollte exFAT nur für die großen SDXC-Cards und MemorySticks XC verwendet werden.

 Nur wenn es um den Datenaustausch mit Medienabspielgeräten mit USB-Anschluss oder Nicht-Windows-Computern wie Linux, UNIX oder macOS X geht, bietet sich die Verwendung von FAT32 als kleinster gemeinsamer Nenner an. Auch von DOS und DOS-basierten Windows-Versionen wird NTFS nicht unterstützt.

Das Lesen von NTFS-Partitionen ist unter Linux und macOS X seit 2002 bzw. 2003 möglich. Für beide Betriebssysteme sowie auch für einige UNIX-Derivate erlaubt der kostenlose Treiber **NTFS-3G** auch das Schreiben.

## Das Dateisystem NTFS

Gegenüber dem alten FAT-Dateisystem hat NTFS wesentliche Vorteile und Zusatzfunktionen zu bieten:

Zugriffsteuerung auf Benutzerebene	Jeder Benutzer von Windows 10 erhält gezielt einstellbare NTFS-Berechtigungen für Objekte auf einem NTFS-Datenträger. NTFS-Berechtigungen sind bei lokalem Zugriff und bei Netzwerkzugriff wirksam.
Dateikomprimierung	Dateien und Ordner auf einem NTFS-Datenträger können komprimiert werden, um Speicherplatz zu sparen.
Verschlüsselung	Dateien und Ordner können verschlüsselt gespeichert werden, entweder über das Encrypted File System (EFS) oder über BitLocker.
Datenträgerkontingente (Quotas)	Der Festplattspeicherplatz von Benutzern und Gruppen kann beschränkt werden.
Datenträger indizieren	Datenträger, Verzeichnisse und Dateien können zur schnelleren Suche indiziert werden. Dabei wird eine Datenbank mit Informationen zu Inhalt, Text, Änderungsdatum etc. des Objektes angelegt, die bei den folgenden Suchen ausgewertet wird.
Transaktionsbasiert	Veränderungen am Dateisystem werden erst dann ausgeführt, wenn die komplette Transaktion erfolgreich durchgeführt werden konnte.
Verweise und Verknüpfungen	NTFS bietet unter Windows 10 mehrere Möglichkeiten, um auf eine Datei oder einen Ordner an einem anderen Ort zu verweisen, z. B. durch Soft Links (symbolische Verknüpfungen), Hard Links oder Junctions (Abzweigungspunkte).
Mounten von Datenträgern im Verzeichnisbaum über Bereitstellungspunkte	Datenträger können mit dem UNIX-Befehl <code>mount</code> an beliebiger Stelle im Verzeichnisbaum eingebunden werden, ohne dass ein Laufwerkbuchstabe zugewiesen werden muss. Dadurch kann die gesamte Ordnerstruktur jederzeit flexibel erweitert werden.

## Zukünftiges Dateisystem ReFS

Zukünftig soll auch das neue Dateisystem **Resilient File System** (ReFS) unterstützt werden. Bisher kommt ReFS nur bei Windows Server 2012/2012 R2, Windows Server 2016 sowie Windows Server 1709/1803 und Windows Server 2019 zum Einsatz. ReFS ist weitgehend kompatibel mit NTFS, verzichtet aber auf einige der oben genannten Features von NTFS, um das neue Dateisystem möglichst schlank zu halten. So fallen unter anderem die Datenkompression auf Dateiebene, Quotas und Hard Links weg, dafür kommen neue Techniken für den sicheren und flexiblen Umgang mit verteilten Speicherlösungen hinzu. Hier werden mehrere physische Festplatten in Speicherpools zusammengefasst, die virtuelle Laufwerke, die Speicherplätze, zur Verfügung stellen. Sie können zwar jetzt schon unter Windows 10 Pools und Speicherplätze anlegen, diese verwenden jedoch kein ReFS, sondern NTFS.

## Master Boot Record (MBR)

Auf Computern mit BIOS verfügen alle Datenträger mit Partitionierung über einen Master Boot Record (MBR), in dem Informationen über die Aufteilung des Datenträgers und bei Systemfestplatten ein Bootloader enthalten sind. Dieser Bootloader wird vom BIOS geladen und startet seinerseits das Betriebssystem.

Der seit Jahrzehnten verwendete MBR stößt bei einer Partitionsgröße jenseits von 2 Terabyte an seine Grenzen und auch das BIOS soll eigentlich schon seit Jahrzehnten durch seinen Nachfolger Extensible Firmware Interface (EFI) ersetzt werden. Das EFI bietet alle Funktionen des BIOS mit grafischer Oberfläche sowie zusätzliche Funktionen wie Booten von GPT-Festplatten. Es wird seit einigen Jahren von allen Apple-Computern verwendet und soll sich in Zukunft auch bei allen Computern mit Windows 10 durchsetzen.

### GUID Partition Table (GPT)

Windows 10 unterstützt bevorzugt Computer mit EFI, obwohl auch die Installation auf Computern mit herkömmlichem BIOS möglich ist. Nur mit EFI kann Windows 10 von einer Festplatte mit dem MBR-Nachfolger GPT (GUID Partitionstabelle) booten, während Linux auch auf einem BIOS-Mainboard von einer GPT-Festplatte starten kann.

BIOS und MBR erlauben maximal 4 primäre Partitionen oder 3 primäre und 1 erweiterte Partition pro Festplatte und eine Maximalgröße von 2 Terabyte für bootfähige Systemfestplatten. Bei GPT sind es 128 Partitionen und maximal 8194 Exabyte, also 4 Milliarden Mal so viel.

Wenn ein GPT-Datenträger zusätzlich zur Bootfestplatte eingesetzt wird, kann schon Windows XP damit umgehen. GPT ist vor allem für Festplatten über 2 Terabyte von Bedeutung.

## 2.3 Die Windows-10-Oberfläche

Das neue Startmenü von Windows 10 weist im Grunde dieselben Funktionen auf wie das alte Startmenü in Windows 7 – es sieht bloß alles anders aus. Im Gegensatz zu Windows 8/8.1 ist Windows 10 wieder deutlich mehr auf die Bedienung mit Maus und Tastatur ausgelegt.

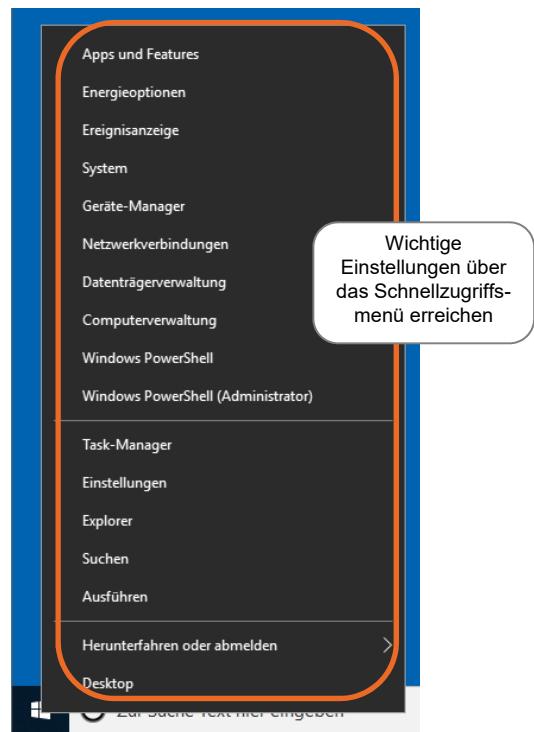


Die neue Oberfläche von Windows 10

In Windows 8 fehlte der Startknopf. In Windows 8.1 hat Microsoft den Startknopf integriert, mit Windows 10 wird das aus Windows 7 bekannte Startmenü wieder eingeführt, inklusive der Möglichkeiten der Startseite in Windows 8/8.1. Über das Kontextmenü des Startknopfes öffnen Sie das **Schnellzugriffsmenü**, über das Sie die wichtigsten Einstellungen von Windows 10 starten können.

Microsoft hat bei Windows 10 ab Version 1803 (April 2018 Update, Redstone 4) die Systemsteuerung aus dem Kontextmenü entfernt. Sie können die Systemsteuerung aber durch Eingabe des Suchbegriffs „Systemsteuerung“ weiterhin im Suchfeld der Taskleiste starten.

**Windows-Apps** öffnen sich im Tabletmodus, den Sie über das Info-Center am rechten Rand in der Taskleiste aktivieren können, stets im Vollbildmodus. Alle **Desktop-Anwendungen** öffnen sich wie gewohnt in einem Fenster auf dem Desktop. Arbeiten Sie mit dem Desktopmodus, werden auch die neuen Windows-Apps im normalen Fenstermodus geöffnet und bieten die gleichen Titelleisten und Möglichkeiten wie klassische Anwendungen. Viele Kacheln zeigen wechselnde Inhalte, daher werden sie auch **Live-Kacheln** oder **Live Tiles** genannt. Diese können Sie im Startmenü integrieren.



## 2.4 Windows 10 mit Tastenkombinationen bedienen

Das Bedienungskonzept bietet Ihnen die Chance, die Produktivität zu steigern und im Umgang mit dem Computer schneller zu werden. Mit Tastenkombinationen kommen Sie schneller an das gewünschte Ziel. Zentraler Bestandteil ist dabei die Windows-Taste .

Tastenkombination	Ergebnis
 	Aktiviert den Zuhören-Modus im Sprachassistenten Cortana
 	Öffnet die Einstellungen
 	Umschalten zwischen Apps und virtuellen Desktops, die Kombination muss nicht gehalten werden, sondern verbleibt in diesem Modus
 	Umschalten zwischen allen Anwendungen
 	Schließt Windows-Apps und Desktop-Anwendungen
 	Öffnet Einstellungen für Präsentation und zwei Monitore
 	Öffnet das Schnellzugriffsmenü
 	Öffnet die Seite zum Verbinden von Geräten
<b>Suchen</b>	
 	Suche öffnen
<b>Sonstiges</b>	
 	Zeigt den Desktop
 	Speichert einen Screenshot im PNG-Format in <i>Bilder</i>
 	Öffnet die Systemeigenschaften
 	Befehl ausführen
 	Öffnet ein Explorer-Fenster



Ergänzende Lerninhalte: *Nützliche Tastenkombinationen.pdf*

Hier finden Sie weitere nützliche Tasten und Tastenkombinationen.

## 2.5 Weitere Änderungen bei Windows 10 im Vergleich zu Windows 7/8

### Was neu ist

Windows 10 bietet z. B. folgende Veränderungen:

#### Oberfläche

- ✓ Ab Windows 10 sind Startknopf und Startmenü wieder unten links verfügbar.
- ✓ Neues Design des Windows-Desktops
- ✓ Windows-10-Apps und Windows Store im Fenstermodus mit Titelleiste
- ✓ Microsoft Edge als Nachfolger des Internet Explorers
- ✓ Windows Online-Speicherplatz OneDrive und Integration in die Microsoft-Cloud
- ✓ Neuer Bluescreen mit verständlicheren Fehlermeldungen und ohne Stop-Codes
- ✓ Neuer Boot-Manager und neu gestaltete Startoptionen
- ✓ Bessere Wiederherstellungsmöglichkeiten

### Funktionalität

- ✓ Datei-Explorer mit Menüband (Ribbon)
- ✓ Neue Explorer-Ansicht, keine Bibliotheken mehr
- ✓ *Computer* heißt jetzt im Explorer *Dieser PC*
- ✓ Verbesserter Dialog für das Kopieren und Verschieben von Dateien
- ✓ Neuer Task-Manager
- ✓ Neue PowerShell mit mehr Möglichkeiten
- ✓ Verschiedene Hintergrundbilder und Taskleiste auf mehreren Monitoren
- ✓ Schnelleres Booten und Herunterfahren durch Ruhezustand-Mechanismen
- ✓ Verbesserte Netzwerkeinstellungen, Umgang mit wechselnden Netzen (UMTS, WLAN, Ethernet)
- ✓ Neue Treiberklassen für USB 3.0, Bewegungssensoren, UMTS-Modems und viele andere Geräte
- ✓ Neues Treibermodell für Grafikkarten WDDM 1.2 und DirectX11.1
- ✓ Arbeitsordner und Arbeitsnetzwerke für den Unternehmenseinsatz mit Windows Server 2012 R2/2016/1709/1803/2019

### Datenspeicherung und Virtualisierung

- ✓ Hyper-V, die gleiche virtuelle Umgebung wie auf Windows Server 2016 mit kleineren Einschränkungen
- ✓ Virtuelle Laufwerke für Dateien in den Formaten ISO, VHD und VHDX ohne Zusatzsoftware
- ✓ Dateiversionsverlauf (File History) als Sicherungsstrategie, vergleichbar mit Apples Time Machine
- ✓ Ab Windows 10, Version 1803 Timeline-Funktion zum Wiederherstellen verschiedener Versionen von Dokumenten
- ✓ Virtuelle Datenspeicher mit Speicherpools und Speicherplätzen
- ✓ Windows To Go, eine bootfähige Windows-Installation auf einem USB-Stick
- ✓ Windows Assessment and Deployment KIT (ADK) als Nachfolger von WAIK und OPK

### Sicherheit

- ✓ Verbesserte BitLocker-Verschlüsselung
- ✓ SmartScreen-Schutz (nicht nur im Internet Explorer, sondern systemweit)
- ✓ Verbesserter Windows Defender, beinhaltet nun den VirensScanner aus den Microsoft Security Essentials

### Was nicht mehr vorhanden ist

- ✓ XP-Modus
- ✓ Startschaltfläche, klassische Ansicht, Aero-Design (transparente 3D-Fenster)
- ✓ Desktop-Gadgets und die Windows-Sidebar
- ✓ Vorherige Dateiversionen (außer bei entsprechend eingerichteten Netzwerkfreigaben)

## 2.6 Übung

### Grundlagen zum Betriebssystem Windows 10

Übungsdatei: --

Ergebnisdatei: *Uebung02\_E.pdf*

1. Welche Funktionen sind der Edition Windows 10 Enterprise vorbehalten?
2. Welche Editionen können Mitglied von Active Directory-Domänen werden?
3. Welche Betriebssystemversionen lassen sich direkt zu Windows 10 aktualisieren?
4. Mit welcher Tastenkombination öffnen Sie das erweiterte Startmenü?
5. Wie heißt der neue Browser in Windows 10?

# 3 Grundlagen des Netzwerkbetriebs

## In diesem Kapitel erfahren Sie

- ✓ was ein Netzwerk ist
- ✓ welche Funktionen über Netzwerke bereitgestellt werden können
- ✓ welches die am weitesten verbreiteten Netzwerktechnologien sind

## 3.1 Aufbau von Netzwerken

### Gründe für den Einsatz eines Netzwerkes

Computer werden seit Jahren zunehmend über Netzwerke miteinander verbunden, um Zugriff auf das Internet zu haben und Ressourcen im lokalen Netzwerk (**Local Area Network, LAN**) gemeinsam nutzen zu können. Solche Netzwerkressourcen sind z. B. Druckgeräte, Verzeichnisfreigaben und Funktionen, die von einem zentralen Server zur Verfügung gestellt werden.

Um diese Ressourcen zur Verfügung stellen und nutzen zu können, werden Netzwerkfunktionalitäten benötigt. In diesem Kapitel sollen Ihnen die Netzwerkgrundlagen vermittelt werden. Sie erfahren, welche Funktionen es in einem Netzwerk gibt und wie die Kommunikation zwischen Computern grundlegend aufgebaut ist.

### Grundlagen der Datenkommunikation

Damit Informationen zwischen Computern ausgetauscht werden können, müssen diese über verschiedene Komponenten verbunden werden. Die Kommunikation im Netzwerk funktioniert im Prinzip wie das Telefonieren.

Wollen zwei Personen miteinander kommunizieren, benötigen sie diverse Komponenten:

- ✓ einen Telefonapparat, der Schallwellen in elektrische Signale und wieder zurückverwandelt;
- ✓ eine Einrichtung zur Übertragung der Signale, beispielsweise Anschlusskabel oder Funk;
- ✓ eine Telefonnummer, die dazu dient, den Empfänger zu adressieren;
- ✓ eine gemeinsame Sprache, in der sich die Gesprächspartner verstündigen können.

### Netzwerkadapter

Auch Computer benötigen einen Apparat, um die Informationen in elektrische Signale zu übersetzen, die dann über die Leitung geschickt werden. Diese Aufgabe übernehmen Modems oder Netzwerkadapter. In modernen Netzwerken werden meist Ethernet-Karten oder Funknetzwerkadapter zur drahtlosen Datenübertragung (Wireless LAN bzw. WLAN) eingesetzt.

### Anschluss und Verkabelung

Ähnlich wie Telefone über die Telefonleitung müssen auch Computer im Netzwerk miteinander verbunden werden. Die Signalübertragung erfolgt bei Ethernetadapters über **Twisted-Pair-Kabel**, die vier miteinander verdrillte Adernpaare enthalten. Es gibt verschiedene Ausführungen und Normen für Netzwerkkabel. Bei den fest verlegten Kabeln werden die Adernpaare mit einer Abschirmung aus Drahtgeflecht (S = Shielded) oder Metallfolie (F = Foil) versehen, wodurch sie für längere Übertragungsstrecken geeignet sind, während die letzten Meter von der Netzwerksteckdose bis zum Computer meist mit einem ungeschirmten (U = Unshielded) und flexiblen Kabel überbrückt wird. Es gibt auch Varianten ohne Adernpaarabschirmung, dafür mit einer Gesamtabschirmung des Kabels, besonders hochwertige und teure Kabel verfügen über beides.

Grundsätzlich gilt: Je mehr Abschirmung ein Netzwerkkabel besitzt, desto teurer, unempfindlicher und steifer wird es. Außerdem werden Netzwerkkabel in Qualitätskategorien eingeteilt, die ihre Eignung für bestimmte Netzwerkgeschwindigkeiten und maximale Übertragungsstrecken angeben. Weit verbreitet sind Kabel der Kategorie CAT 5, die bei kurzen Strecken prinzipiell für Gigabit-Ethernet ausreichend sind. Bei Neuinstallationen sollten Sie allerdings Kabel mit CAT 6(A) oder CAT 7(A) verwenden, da diese auch für die höheren Geschwindigkeitsstufen geeignet und damit zukunftssicher sind.

Das moderne Ethernet hat seine Wurzeln in einer Verbindung mehrerer Computer über einen Bus, also einer Reihenverbindung über ein einziges Netzwerkkabel. Vom logischen Aufbau her ist Ethernet auch heute noch eine Bus-Topologie, auch wenn diese nun meist auf eine sternförmige Verkabelung mit einem zentralen Verteilerknoten abgebildet wird. Früher wurde als Verteiler ein Hub eingesetzt, der blindlings allen ankommenden Datenverkehr an sämtliche erreichbaren Ziele weiterschickte. Heute übernehmen **Switches** diese Funktion. Dabei handelt es sich um Knotenpunkte mit Eigenintelligenz, die wie ein Weichenstellwerk den Verkehr durch das Netzwerk gezielt nur an den richtigen Empfänger weiterleiten. Switches können außerdem zwischen verschiedenen Netzwerkgeschwindigkeiten hin- und herschalten, ohne dabei wie früher beim Hub die Geschwindigkeit für alle anderen Teilnehmer zu reduzieren. Darüber hinaus erfüllen moderne Switches noch weitere Funktionen wie Signalauffrischung/-verstärkung und Segmentierung des Netzwerkes, die sicherstellt, dass lokaler Verkehr nicht das gesamte Netzwerk behindert.

### Übertragungsgeschwindigkeiten

Für die Übertragung von Daten im Netzwerk gibt es unterschiedliche Übertragungsgeschwindigkeiten. Diese werden nicht in Byte, sondern in **Bit pro Sekunde** angegeben. Oft findet man auch die englische Bezeichnung „bits per second“ (bps). Die Standardgeschwindigkeit im Ethernet ist heute 1 Gigabit/s (Gigabit-Ethernet), ältere Installationen liefern nur 100 MBit/s (Fast Ethernet). Im Laufe der nächsten Jahre wird die nächste Geschwindigkeitsstufe mit 10 Gigabit/s zunehmend Verbreitung finden. Zurzeit werden 10-Gigabit-Netze hauptsächlich in größeren Netzwerken im Backbone-Bereich eingesetzt, die die Server und Teilnetze miteinander verbinden und so das Rückgrat des Firmennetzes bilden.

Im **Funknetzwerk WLAN** liegen die theoretischen Werte zwischen 54 Mbit/s (802.11g) und 600 Mbit/s (802.11n). Der Standard 802.11ac kann über 1 Gigabit/s ermöglichen. Während man im Kabelnetzwerk im Idealfall sehr nahe an die Maximalwerte herankommen kann, lassen sich per Funk bestenfalls 40 % der jeweiligen Bruttowerte erreichen. Je mehr Teilnehmer das WLAN benutzen und je mehr WLANs in der Umgebung zu finden sind, desto mehr stören sie sich gegenseitig und die nutzbare Übertragungsrate sinkt.

### Adressen

Das Gegenstück zur Telefonnummer ist im Computernetzwerk die **IP-Adresse** (IP = Internetprotokoll). Eine IP-Adresse besteht aus vier Gruppen mit Zahlen von 0 bis 255. Analog zur Telefonnummer wäre die erste Zahlengruppe die Landesvorwahl, die zweite Gruppe die Ortsvorwahl, die dritte Gruppe die Rufnummer der Firmentelefonzentrale und die letzte Gruppe die Durchwahl für den Telefonanschluss im Büro.

### Sprachen

Die Protokolle in der Datenübertragung sind die Sprache, die die Computer benutzen, um sich zu verstündigen. Genau wie beim Telefonieren kann Kommunikation nur erfolgreich sein, wenn die Kommunikationspartner dieselbe Sprache sprechen. Außerdem muss sichergestellt sein, dass auch wirklich der richtige Teilnehmer am Apparat ist, daher müssen sich die Gesprächspartner auf sichere Weise gegenseitig identifizieren können. Das kann im einfachsten Fall durch die Nennung des Namens oder das Erkennen der Stimme geschehen oder für besondere Sicherheitsansprüche zum Beispiel durch Austausch eines vorher vereinbarten Codewortes.

Außerdem wäre noch eine Verschlüsselung des Gesprächs möglich, sodass es nicht mehr so leicht abgehört werden kann. All diese Funktionen übernehmen im Netzwerk die beteiligten Protokolle, die sich um die Suche von Kommunikationspartnern, den Verbindungsaufbau, Gesprächsübermittlung und -verschlüsselung kümmern. Dieser Teil der Netzwerkkommunikation erfolgt weitgehend automatisch und erfordert normalerweise keine Eingriffe vom Computerbenutzer, daher wird er hier nicht weiter behandelt. Die Einstellungen an Arbeitsplatzcomputern betreffen nur das Adressierungs- und Übertragungsprotokoll TCP/IP und werden weiter unten erläutert.

## Heimnetzgruppe

Die Heimnetzgruppe ist mit Windows 7 eingeführt worden und Windows 10 hat sie so beibehalten. Die Heimnetzgruppe vereinfacht die gemeinsame Nutzung von Drucken, Dateien und Medien wie Bildern, Musik oder Filmen. Dabei wird vor allem das Bibliothekskonzept verfolgt, bei dem die einzelnen Benutzer entscheiden können, welche ihrer Bibliotheken sie für die anderen Teilnehmer freigeben wollen. Auf diese Weise kann man sehr bequem auf die über die einzelnen Computer eines Netzwerks verteilten Medien zugreifen. Durch Eingabe eines Kennwortes, das vom ersten Teilnehmer der Gruppe erstellt wurde, kann man der Gruppe beitreten, dazu muss man jedoch Mitglied derselben Arbeitsgruppe sein. Für größere Firmennetzwerke ist die Heimnetzwerkgruppe ungeeignet. In diesem Fall ist eine Windows-Domäne besser geeignet.

In kleineren Unternehmen kann der Einsatz aber durchaus Sinn ergeben, da dadurch die Möglichkeit erreicht wird, schnell und einfach Daten im Netzwerk auszutauschen, gemeinsam auf Drucker zuzugreifen und den Dateiversionsverlauf (vgl. Abschnitt 13.4) auf einem gemeinsamen Datenträger im Netzwerk abzulegen.

## Arbeitsgruppen

Wenn mehrere Computer in einem Netzwerk als gleichberechtigte Partner stehen, wird dies als Arbeitsgruppe oder als Peer-to-Peer(Partner-zu-Partner)-Netzwerk bezeichnet. Jeder Rechner in der Arbeitsgruppe funktioniert als allein stehende, vollwertige Einheit, die aber bei Bedarf Daten mit anderen Einheiten austauschen kann. Diese Einheiten können sowohl andere Rechner als auch beispielsweise Drucker sein.

Da in einer Arbeitsgruppe keine übergeordnete Verwaltungsinstantz existiert, müssen alle Verwaltungsarbeiten lokal an jedem Rechner vorgenommen werden. Für die Datensicherheit müssen auf den Computern lokale Benutzerkonten eingerichtet werden, bei denen sich die Mitarbeiter unter Verwendung eines Benutzernamens und eines Kennwortes anmelden. Wenn Sie über 10 Computer verfügen und 30 Mitarbeiter auf alle Computer zugreifen sollen, müssen an jedem einzelnen Computer für jeden Mitarbeiter Benutzerkonten angelegt werden. Es müssten also insgesamt 300 Konten angelegt und gepflegt werden. Jede Änderung an Benutzerkonten, z. B. eine Passwortänderung, müsste auf allen Computern einzeln eingestellt werden. Hier wird klar, dass Arbeitsgruppen nur in sehr kleinen Netzwerken sinnvoll sind. Um eine größere Anzahl von Benutzern und Geräten in einem Netzwerk zu verwalten, sollten Sie eine Domäne einrichten.

## Domänen

Eine Domäne ist ein Verbund von Computern, die hierarchisch organisiert sind. Dabei übernimmt ein Server die Rolle des **Domänencontrollers**, der bestimmt, welche Berechtigungen jeder Computer und Benutzer in der Domäne hat. Neben dem Domänencontroller gibt es im Netzwerk oft noch weitere Server, die auch Member- oder Mitgliedserver genannt werden. Diese speziellen Computer stellen im Netzwerk Funktionen, Dienstleistungen oder Ressourcen bereit. Die Mehrzahl der Computer sind üblicherweise Arbeitsplatzrechner. Sie werden auch als **Clients** oder Client-PCs bezeichnet und verfügen normalerweise über ein Microsoft-Client-Betriebssystem wie Windows 10.

Jeder Client überträgt dem Domänencontroller die Aufgabe, die Konteninformationen von Benutzern zu verifizieren. So reicht es aus, wenn der Benutzer über ein Konto auf dem Domänencontroller verfügt. Dadurch muss nicht mehr jeder Benutzer auf jedem Computer ein lokales Benutzerkonto erhalten und der Verwaltungsaufwand reduziert sich beträchtlich. Ein weiterer Vorteil des Client-Server-Modells ist die zentrale Verwaltung der Benutzerdaten und die Möglichkeit, detailliert zu bestimmen, welche Einstellungen die Benutzer auf dem Arbeitsplatzrechner vorfinden, welche Software sie ausführen und auf welche Ressourcen sie zugreifen können.

Andererseits erfordern Einrichtung und Betrieb eines Servers zusätzliche Fachkenntnisse, teure Server-Betriebssysteme und leistungsfähige und ausfallsichere Hardware. Es ist daher unwirtschaftlich und unverhältnismäßig, wenn in kleinen Netzen mit wenigen Benutzern eine Domäne eingerichtet wird. Eine Ausnahme bildet im Firmenumfeld der preisgünstige Windows Small Business Server, der die Einrichtung und Administration einer kleinen Domäne auch ohne umfassende IT-Kenntnisse ermöglicht. Für den Heimbereich ist der Windows Home Server erhältlich, der ohne Domäne alle Benutzer in einer Heimnetzgruppe verbindet und schnell als Multimedia-Server mit zentraler Datenablage und Datensicherung einzurichten ist.



**Ergänzende Lerninhalte:** Aufgabenverteilung im Netzwerk.pdf

Hier finden Sie Grundbegriffe und Konzepte zu Clients und Servern.

## 3.2 Netzwerkprotokolle

### Wie Netzwerkprotokolle eingesetzt werden

Die Netzwerkprotokolle dienen der Kommunikationssteuerung im Netzwerk. Über sie werden Computer identifiziert und Kommunikationswege etabliert. Sie steuern die Prozesse der Datenübermittlung zwischen den Programmen und dem physischen Übertragungsweg sowie zwischen den Computern.

### TCP/IP

Die am weitesten verbreitete Protokollfamilie ist **Transmission Control Protocol/Internet Protocol** (Übertragungssteuerungsprotokoll/Internetprotokoll). TCP und IP sind zwei getrennte Protokolle, die der Protokollfamilie wegen ihrer häufigen Verwendung und Wichtigkeit den Namen gaben. Alle modernen Netzwerkbetriebssysteme unterstützen sie, und die Kommunikation mit dem Internet ist ohne TCP/IP nicht möglich.

Viele Windows-Funktionen im Netzwerk, wie die Domänenanmeldung am Active Directory, werden nur unterstützt, wenn auch TCP/IP installiert ist. Daher sollte TCP/IP immer als Standardprotokoll installiert sein.

Bei Windows 10 ist standardmäßig nicht nur das altbekannte IP-Protokoll mit der Versionsnummer 4 (IPv4) aktiv, sondern auch die neue Version IPv6. Beide Protokolle können problemlos nebeneinander existieren. In Zukunft wird die Bedeutung von IPv6 für das Internet immer weiter zunehmen, aber auch in lokalen Netzwerken gibt es inzwischen Gründe, auf IPv6 umzustellen. Moderne Windows-Funktionen wie HomeGroups und DirectAccess sind nur mit IPv6 möglich.

### Eine IPv4-Adresse und ihre Bestandteile

Der wichtigste Bestandteil von TCP/IP ist die IP-Adresse. Sie ist die „Telefonnummer“ des Computers und besteht in der Version 4 des Protokolls aus vier Dezimalzahlen zwischen 0 und 255. Jede Zahlengruppe ist eine achtstellige Binärzahl, daher werden sie auch als Oktette bezeichnet. Insgesamt ist die IPv4-Adresse also 32 Bit lang. Diese Zahlengruppen haben die gleiche Aufgabe wie die Telefonnummer mit Orts- und Landesvorwahl.

<b>TCP/IP-Adresse:</b>	192.168.178.104
<b>Subnetzmaske:</b>	255.255.255.0
<b>Netzadresse:</b>	192.168.178.x
<b>Hostadresse:</b>	.104

*Die Grenze zwischen Netz- und Hostadresse wird durch die Subnetzmaske definiert*

Bei langen Telefonnummern ist es wichtig zu wissen, wo die Vorwahl aufhört und die Anschlussnummer anfängt. Nur so weiß man, welchen Teil der Nummer man weglassen kann, wenn man einen Anschluss in der gleichen Stadt an wählt. Auch für Netzwerkgeräte ist es wichtig, die Netzadresse von der Hostadresse zu trennen und zu erkennen, ob sich zwei Geräte im selben Netzabschnitt befinden. Für diese Trennung wird die Netzmase verwendet. Sie wird auch **Subnetzmaske** genannt, weil damit ein Netzwerk in Subnetze unterteilt werden kann, um so Strukturen eines Netzwerkes zu ordnen und Zugriffe auf Computer innerhalb des Netzes genauer zu regulieren.

Die Vergabe von IP-Adressen ist von zentraler Bedeutung für die Funktionsfähigkeit eines Netzwerks und muss mit den zuständigen Stellen koordiniert werden. Doppelt vergebene oder unpassende IP-Adressen können den Betrieb des Netzwerkes stören.



### IPv6

In der Version 6 des IP-Protokolls wurde neben einigen anderen Änderungen und Erweiterungen vor allem die 32 Bit lange IP-Adresse auf 128 Bit erweitert. Damit erhöht sich die Anzahl der theoretisch möglichen IP-Adressen von ca. 4 Milliarden auf etwa 340 Sextillionen oder  $3,4 \cdot 10^{36}$ . Die Schreibweise für IPv6-Adressen unterscheidet sich in mehreren Punkten von IPv4. So werden IPv6-Adressen als hexadezimale Zeichenkette angegeben, in der acht Blöcke mit je 16 Bit bzw. 2 Bytes gruppiert und durch einen Doppelpunkt von der nächsten Gruppe getrennt werden.

Ein oder mehrere aufeinanderfolgende Blöcke mit dem Wert 0000 können zur bequemeren Eingabe durch eine Null ersetzt oder ganz weggelassen werden. Führende Nullen können ebenfalls entfallen. IPv6 führt eine klare Trennung zwischen Netzwerknummer und Hostadresse ein und vereinfacht dadurch die Zuordnung. Die ersten 64 Bits der IPv6-Adresse geben nun stets die Netzwerknummer an, die letzten 64 Bits die Adresse des Netzwerkadapters im Zielcomputer, auch Interface Identifier genannt.

Beispiele für IPv6-Adressen:

- ✓ 2001:0db10:105a3:010d3:1319:10a2e:0370:7344
- ✓ fe100:0000:0000:0000:0000:5e3a:36c1:00a2

Die untere Adresse kann auch abgekürzt geschrieben werden: fe100::5e3a:36c1:a2

Für die letzten vier Bytes der Adresse darf auch die herkömmliche dezimale Schreibweise von IPv4 verwendet werden. Das ist nützlich, wenn man den Adressraum von IPv4 in IPv6 einbetten möchte.

- ✓ 2001:0db10:105a3:010d3:1319:10a2e:7f00:1 entspricht
- ✓ 2001:0db10:105a3:010d3:1319:10a2e:127.0.0.1

## Netzadressen

Die Netzadresse dient der Lokalisation eines Rechners. So können in einer Firma mehrere Netzwerke vorhanden sein, die sich durch unterschiedliche Netzadressen auszeichnen. Wenn ein Computer dann eine Verbindung zu einem anderen Computer in einem anderen Netzwerk aufbauen soll, muss diese Verbindung über einen Rechner vermittelt werden, der eine Verbindung zu beiden Netzen hat. Dieser Vorgang wird als Routing bezeichnet.

## Routing

Routing kommt von dem englischen Wort „Route“ und bedeutet so viel wie „Verkehrsführung“. Der Router hat die Aufgabe, den Weg zu einer Adresse in einem anderen Netz zur Verfügung zu stellen. Jeder Router muss sich in mindestens zwei Netzen befinden, wobei ein Netz auch das Internet sein kann. Die Netze können physisch (z. B. Glasfaser- und Twisted-Pair-Kabel) oder logisch (verschiedene Adressbereiche) voneinander getrennt sein.

## Standardgateway

Den Standardweg in andere Netze vermittelt das sogenannte Standardgateway. Es handelt sich dabei um die Adresse des Rechners, der das Routing in andere Netze übernimmt. Meist stellt das Standardgateway eine Verbindung zum Internet zur Verfügung.

## NetBIOS

Ein weiteres Protokoll basiert auf dem Standard von NetBIOS (Network Basic Input/Output System). Mit NetBIOS werden Computer in Windows-Netzwerken über einfache Namen identifiziert, z. B. als PC01 statt PC01.firma.intern. Dabei gibt es Konventionen, die einzuhalten sind:

- ✓ Der Name darf nicht länger als 15 Zeichen sein.
- ✓ Die Buchstaben a bis z, A bis Z, die Zahlen von 0 bis 9 und der Bindestrich sind erlaubt.

Wird unter Windows 10 ein Computername mit mehr als 15 Zeichen benutzt, kürzt das System den Namen ab, wenn die Kommunikation mit anderen Betriebssystemen hergestellt werden muss, die den NetBIOS-Standard befolgen. NetBIOS ist ein sehr altes Protokoll und wird nur noch aus Kompatibilitätsgründen unterstützt. Es wird in einer Domäne durch die Funktionen von Active Directory und DNS überflüssig und sollte deaktiviert werden.

### 3.3 Identifikation im Netzwerk

#### Adressen und Namen

Generell werden zur Identifikation eines Rechners im IPv4-Netzwerk drei Informationen benötigt:

- ✓ Die **MAC-Adresse** ist eine vom Hersteller direkt der Netzwerkkarte zugewiesene Identifikationsnummer, die weltweit eindeutig sein sollte. Anhand der MAC-Adresse kann der Netzwerkadapter, und damit auch der Computer, identifiziert werden. Sie ist vergleichbar mit der Personalausweisnummer oder Sozialversicherungsnummer.
- ✓ Der MAC-Adresse wird eine **IP-Adresse** zugeordnet, die einer Telefonnummer entspricht. Wie das geht, wird weiter unten beschrieben.
- ✓ Benutzer können einen Rechner auch über den **Namen** ansprechen, z. B. als *FS01.unsere-firma.intern.de*. Der Name wird dann wie von einer Telefonauskunft vom DNS-Server (oder vom WINS über NetBIOS) in die MAC-Adresse oder die IP-Adresse aufgelöst und die Verbindung kann hergestellt werden.

Bei IPv6 ist im Autokonfigurationsmodus die MAC-Adresse standardmäßig Teil des **Interface Identifiers** und damit Teil der IP-Adresse.



#### Manuelle Konfiguration von IP-Adressen

Die manuelle Konfiguration von IPv4-Adressen erfordert eine Vereinbarung innerhalb des Netzes über die Vergabe von Netzwerkadressen, Rechneradressen und Serveradressen. Dann kann jedem Rechner über ein Dialogfenster eine Adresse zugewiesen werden. Da diese Informationen jedoch zueinanderpassen und diverse Kriterien erfüllen müssen, sollten Sie sie nur dann von Hand einfügen, wenn Sie sich mit Ihrem Netzwerkadministrator abgesprochen haben. Doppelt belegte oder falsch gewählte IP-Adressen können schwere Probleme im Netzwerk verursachen. In bestimmten Fällen ist eine manuelle Konfiguration der IP-Adresse zwingend erforderlich. Der betreffende Computer erhält so eine statische oder feste IP-Adresse. Dies ist vor allem dann sinnvoll, wenn der Rechner ständig für andere Teilnehmer im Netzwerk verfügbar sein muss und stets unter derselben Adresse angesprochen werden soll.

#### Automatische Vergabe von IPv4-Adressen

<b>Autokonfiguration</b>	Wie bei den älteren Windows-Versionen ist es auch mit Windows 10 möglich, zur Vergabe der IPv4-Adresse gar nichts zu unternehmen. Die im Netzwerk aktiven Rechner handeln dann untereinander die Adressen aus. Dieses APIPA (Automatic Private IP Addressing) genannte Verfahren sollte nicht verwendet werden. Es eignet sich allenfalls für kleine Netze, in denen keine statischen Adressen gebraucht werden.
<b>Dynamisches IP mit DHCP-Servern</b>	Die Vergabe von IPv4-Adressen wird unter Windows 10 noch auf eine andere Art automatisiert, die standardmäßig verwendet wird. Dabei bittet der Computer beim Starten automatisch einen spezialisierten Server um die Zuweisung einer IP-Adresse. Dieser Server wird DHCP-Server genannt und übergibt neben der IP-Adresse auf Wunsch auch die IP-Adressen von Default Gateway, DNS-Servern und WINS-Servern.

#### Automatische Vergabe von IPv6-Adressen

<b>Autokonfiguration IPv6</b>	IPv6 kann den Netzwerkadapter über Autokonfiguration eigenständig mit einer IPv6-Adresse versorgen. Dazu kommuniziert es mit den Routern in seinem Netzwerksegment und stimmt sich auch mit den Nachbargeräten ab. Im Gegensatz zu APIPA ist die automatische Konfiguration bei IPv6 empfehlenswert.
<b>Dynamisches IPv6 mit DHCPv6-Servern</b>	Seit Windows Vista ist in allen Microsoft-Betriebssystemen eine an IPv6 angepasste Version von DHCP namens DHCPv6 enthalten, die auf verschiedene Weise mit der IPv6-Autokonfiguration zusammenarbeiten kann. So kann z. B. der DNS-Server durch DHCPv6 vorgegeben werden, während die IP-Adresse weiterhin durch IPv6-Autokonfiguration festgelegt wird.

### DHCP-Server

DHCP steht für **Dynamic Host Configuration Protocol** und bedeutet, dass einem Rechner automatisch eine IP-Adresse zugewiesen wird. Diese Adresse kann für einen gewissen Zeitraum, die sogenannte Leasedauer, vergeben werden. Daneben können dem Rechner auch noch weitere Informationen über Adressen von wichtigen Servern wie DNS, WINS und Standardgateway übermittelt werden, die eine reibungslose Kommunikation im Netzwerk ermöglichen und aufwendige manuelle Konfigurationsarbeiten ersparen. In größeren Netzwerken ist DHCP für die Vergabe von IP-Adressen für Client-Computer unverzichtbar.

DHCP kann als Serverrolle auf einem Microsoft-Server installiert werden, kann aber auch von anderen Geräten im Netzwerk übernommen werden. In kleinen Firmen- oder Privatnetzwerken wird diese Aufgabe meist vom Internet-Router übernommen.



Alle netzwerkfähigen Geräte der letzten Jahre können ihre Netzwerkadresse über DHCP beziehen und sind IPv6-fähig. Dennoch ist es bei der Umstellung eines Firmennetzes auf IPv6 empfehlenswert, jedes einzelne Gerät auf seine IPv6-Fähigkeit zu überprüfen, insbesondere die Switches und Router.

### DNS-Server

Der DNS-Server (**Domain Name System**) hält eine Datenbank bereit, in der die Rechnernamen den zugehörigen IP-Adressen zugeordnet sind. Er hat die Aufgabe einer Telefonauskunft für das Netzwerk und löst auf Anfrage Namen in IP-Adressen auf. Besonders wichtig wird DNS, wenn die Kommunikation mit dem Internet hergestellt werden soll.

Wenn eine Adresse nicht aufgelöst werden kann, verweist der DNS-Server auf einen weiteren DNS-Server, bis die Adressauflösung funktioniert oder klar wird, dass die Adresse nicht aufgelöst werden kann.

Das DNS-Server-System löste in den 1980er-Jahren die lokalen Hosts-Dateien für die Namensauflösungen ab, die der Zahl der Neueinträge im Internet nicht mehr gewachsen waren. Mit DNS wird der Namensraum im Internet in Zonen unterteilt und in sogenannten Zonen-Dateien gespeichert. Dabei ist jede Zone getrennt administrierbar. In Windows-Netzwerken wird DNS auch zur internen Adressauflösung verwendet und kann in Verbindung mit DHCP die Adressen dynamisch verwalten.

### WINS-Server

Vor etwa 20 Jahren konnten die Microsoft-Betriebssysteme die Adressen noch nicht mit DNS auflösen, sondern benutzten dafür das auf NetBIOS basierende WINS.

Der Windows Internet Naming Service ist ein von Microsoft entwickeltes System zur dynamischen Adressauflösung unter Windows NT. Aus Gründen der Abwärtskompatibilität unterstützt auch Windows 10 noch die Namenskonventionen von WINS. Allerdings sollte in modernen Netzen auf WINS verzichtet werden, da die Verwendung von NetBIOS die Netzlast deutlich erhöht.

## 3.4 Übung

### Grundlagen zum Netzwerkbetrieb

Übungsdatei: --

Ergebnisdatei: *Uebung03\_E.pdf*

1. Was ist eine MAC-Adresse?
2. Welche Aufgabe hat ein DNS-Server?



# 4 Installation

## In diesem Kapitel erfahren Sie

- ✓ wie Sie die Installation von Windows 10 vorbereiten
- ✓ welche Hard- und Software die Installation voraussetzt
- ✓ wie Sie Windows 10 neu installieren
- ✓ welche Schritte Sie zur Lösung von Installationsproblemen unternehmen können
- ✓ wie Sie den Boot-Manager von Windows 10 reparieren
- ✓ wie Sie Windows 10 über den Installationsdatenträger reparieren können

## 4.1 Die Installation vorbereiten

Bevor Sie die Installation beginnen, müssen Sie die richtige Edition auswählen, die notwendigen Seriennummern besorgen und teilweise auch einen Installationsdatenträger erstellen.



Viele Rechner verfügen über kein DVD-Laufwerk. In diesem Fall können Sie den Rechner mit einem USB-Stick starten und Windows 10 booten. Wenn Ihnen die Installationsdateien als ISO-Datei vorliegen, müssen Sie diese auf DVD brennen. Auch hier können Sie auf Wunsch einen USB-Stick erstellen.

### Vorbemerkung zur 90-Tage-Testversion von Windows 10 Enterprise



Microsoft stellt Windows 10 Enterprise als kostenlose Testversion zur Verfügung. Die Testversion ist zeitlich beschränkt und nicht für den Produktiveinsatz geeignet, da sich die Testversion nicht in eine zeitlich unbeschränkte Version umwandeln lässt. Sie sollten vor dem Experimentieren mit der Testversion ein komplettes Backup Ihrer Daten und ein Systemabbild anfertigen. Empfehlenswert ist die Verwendung eines zusätzlichen Computers oder einer virtuellen Umgebung. Ohne manuelle Änderungen an Konfigurationsdateien lässt sich kein Upgrade eines bestehenden Windows-Systems auf die Testversion durchführen.

- Laden Sie die ISO-Datei von <http://technet.microsoft.com/de-de/evalcenter/hh699156.aspx>.

Anschließend können Sie mit der ISO-Datei entweder eine virtuelle Maschine installieren, oder Sie brennen die Datei als Abbild auf eine DVD. Dazu steht Ihnen in Windows 10 und Windows 7 über das Kontextmenü der ISO-Datei der Befehl *Datenträgerabbild brennen* zur Verfügung. Verfügen Sie über eine gültige Lizenz für Windows 7/8 oder 10, können Sie die Installationsdateien für Windows 10 direkt bei Microsoft auf der Seite <http://www.microsoft.com/de-de/software-download/windows10> herunterladen.

### Schritte der Installationsvorbereitung

Windows 10 ist der direkte Nachfolger von Windows 8.1. Es ist ein weiteres Betriebssystem aus der Windows-NT-Schiene. Vor der Installation von Windows 10 müssen ähnliche Vorbereitungen getroffen werden wie bei den bisherigen Betriebssystemen.

Berücksichtigen Sie vor der Installation folgende Themenbereiche:

- ✓ Systemanforderungen an den zur Installation ausgewählten PC,
- ✓ Auswahl von Installationsverfahren und Installationsmedium,

- ✓ Zusammenstellung von Treibern, z. B. für RAID-Systeme oder zusätzliche SATA-Controller,
- ✓ weitere benötigte Konfigurationsinformationen wie z. B. Netzwerkeinstellungen und Windows-Key.

Denken Sie außerdem daran, die verwendete Hardware, BIOS- und Netzwerkeinstellungen, die Installationsart und die Konfiguration jedes Computers sorgfältig zu dokumentieren. Mögliche Probleme können so leichter gefunden und schneller behoben werden.



### Hardware-Mindestanforderungen ermitteln

Laut Microsoft sind die Minimalanforderungen für Windows 10 identisch mit denen für Windows 7:

Komponente	Anforderung
Prozessor	Intel-kompatibler x86-Prozessor mit 1 GHz (x64-fähig für 64 Bit)
Arbeitsspeicher	1 GB RAM (32 Bit), 2 GB RAM (bei 64 Bit)
Festplatte	Mindestens 16 GB frei für x86 (32 Bit), mindestens 20 GB frei für x64 (64 Bit)
Grafikkarte	DirectX 9.0 mit WDDM 1.0 Treiber
Display	Mindestauflösung 800 x 600, 1366 x 760 für das Anheften von Windows-Apps

Die aktuellen Anforderungen listet Microsoft auch auf der Seite <https://www.microsoft.com/de-de/windows/windows-10-specifications> auf. In der Praxis sollten alle diese Werte deutlich übertroffen werden, damit ein flüssiges Arbeiten möglich ist. Bedenken Sie, dass Sie auf der Festplatte auch Platz für weitere Anwendungen, Systemwiederherstellungspunkte, zukünftige Windows-Updates und Service Packs sowie Ihre Dokumente und Dateien benötigen.

### Hyper-V-Kompatibilität

Im Gegensatz zu Windows 7 kennt Windows 10 keinen XP-Modus mehr, verfügt nun jedoch über die von den Servern bekannte **Virtualisierungsumgebung Hyper-V**. Hier kann man z. B. virtuelle Maschinen mit anderen Betriebssystemen erstellen und bestehende Computer virtualisieren. Dabei ist die Virtualisierung sehr hardwarenah, sodass auch anspruchsvolle Software wie Spiele ohne nennenswerte Leistungseinbußen funktionieren. Hyper-V ist nur auf Windows-Systemen mit 64 Bit verfügbar.

Für den Einsatz von Hyper-V, der virtuellen Umgebung von Microsoft, ist ein 64-Bit-Prozessor mit den Virtualisierungstechniken Intel VT-X bzw. AMD-V sowie **SLAT** (Second Level Address Translation, erweiterte Speicheradressierung) erforderlich. Auf einem SLAT-fähigen Prozessor kann die Geschwindigkeit der virtuellen Maschine gesteigert werden, weil die CPU die Speicherseitenverwaltung der virtuellen Maschine ohne weitere Virtualisierung übernehmen kann. AMD nennt das **RVI** (Rapid Virtualization Indexing), bei Intel heißt es **EPT** (Extended Page Table). SLAT ist bei allen Intel-CPUs der Core-i-Reihe ab 2010 verfügbar, bei AMD ist es bei allen Prozessoren mit K10-Architektur ab 2007 vorhanden. Unter <https://docs.microsoft.com/en-us/sysinternals/downloads/coreinfo> ist das kostenlose Tool **coreinfo** erhältlich, mit dem Sie auf der Kommandozeile mit `coreinfo -v` herausfinden können, ob die CPU Hyper-V-fähig ist. Bei Windows 10 kann auch das Kommandozeilentool **systeminfo** die Eignung für Hyper-V anzeigen.



## Installationsverfahren auswählen

Sie können die Verkaufsversion von Windows 10 von verschiedenen Medien installieren. Wählen Sie entsprechend den Anforderungen des Unternehmens oder des Benutzers ein Installationsverfahren aus. Sie haben auch die Möglichkeit, Windows 7/8.1 zu installieren und danach auf Windows 10 zu aktualisieren.

Aufgabe	Lösungsweg
Computer ohne Betriebssystem oder Multiboot-Konfiguration	Starten Sie den Computer von der Installations-DVD und nehmen Sie eine manuelle Installation vor.
Computer ohne DVD-Laufwerk (z. B. Netbooks, Tablets oder Ultrabooks)	Verwenden Sie ein USB-DVD-Laufwerk oder erstellen Sie einen bootfähigen USB-Stick für die Windows-Installation.
Windows 10 auf mehreren Computern installieren	Für die automatisierte Mehrfachinstallation kann ein angepasstes Windows Image und das Installationsskript <i>unattend.xml</i> verwendet werden. Geeignete Wege für die automatische Installation: <ul style="list-style-type: none"> <li>✓ Installation von bootfähigem USB-Datenträger,</li> <li>✓ Installation von selbst erstellter DVD mit angepasstem Windows Image und <i>unattend.xml</i>,</li> <li>✓ Netzwerkinstallation über die Windows-Bereitstellungsdienste WDS und PXE-bootfähige Netzwerkverbindung.</li> </ul> Microsoft stellt umfangreiche Softwarepakete und Tools zur Verteilung und Installation von Windows 10 zur Verfügung. Wichtig sind hier vor allem das <b>ADK</b> (Assessment and Deployment Kit) und das <b>MDT 2013 Update 1</b> (Microsoft Deployment Toolkit). Viele Werkzeuge wie z. B. das <b>Windows USB/DVD Download Tool</b> funktionieren auch mit Windows 10. Hinweise dazu finden Sie in der technischen Referenz zu Windows 10. Für die Verteilung von Windows 10 ist außerdem kommerzielle Software von Drittanbietern erhältlich.
Eine Aktualisierung auf Windows 10 (gilt nicht für die 90-Tage-Testversion)	Ein direktes Upgrade des Betriebssystems ist von Windows 7 und Windows 8/8.1 aus möglich. Sie können nicht von einem 32-Bit-System auf Windows 10 mit 64 Bit upgraden und umgekehrt. Beide Systeme müssen die gleiche Plattform haben, entweder x86 (32 Bit) oder x64 (64 Bit). Als Installationsmedien geeignet sind ISO-Abbildungen, DVDs, USB-Sticks oder Netzwerkreigaben. Sie können während der Installation die aktuelle Windows-Version auch von <a href="http://www.microsoft.com/de-de/software-download/windows10">http://www.microsoft.com/de-de/software-download/windows10</a> herunterladen, dazu wird jedoch wegen der Dateigröße von mehreren Gigabyte eine schnelle Internetverbindung benötigt. Von Windows Server, Windows Vista, Windows XP und noch älteren Windows-Versionen ist kein direktes Upgrade möglich, es wird daher stets eine Neuinstallation ausgeführt. Während des Installationsvorgangs wird eine Übernahme der Benutzerdaten angeboten. Theoretisch ist auch ein stufenweises Upgrade von Windows NT4 über Windows 2000, XP, Vista und Windows 7 zu Windows 10 möglich, aber nicht ratsam.

## Konfigurationsinformationen zusammenstellen

Stellen Sie folgende Konfigurationsinformationen zusammen, bevor Sie mit der Installation beginnen:

- ✓ Angaben zur Partitionierung und Formatierung der Festplatte,
- ✓ Daten für Administrator und Erstbenutzer,
- ✓ geplanter Computername,

- ✓ Konfigurationsdaten für das Netzwerk.
- ✓ Seriennummern der zu installierenden Programme

### Partitionen und Dateisysteme

Festplatten können bei der Installation von Windows 10, wie bereits bei den Vorgängerversionen, in mehrere **Partitionen** unterteilt werden. Jede Partition bildet dabei einen physisch eigenständigen Bereich. Für einzelne Arbeitsplatz-PCs ist meistens eine einzige Partition ausreichend, die sich über die gesamte Festplatte erstreckt. Entscheiden Sie mithilfe der folgenden Tabelle, auf welche Weise die Festplatte des Computers partitioniert werden soll.

Die Festplatte ...	Vorgehensweise
ist nicht partitioniert	Legen Sie während der Installation die Größe der benötigten Partition fest oder überlassen Sie dem Windows-Setup die Partitionierung der Festplatte.
enthält eine NTFS-Partition mit mindestens 16 bzw. 20 GB freiem Speicherplatz	Sie können diese Partition für die Installation von Windows 10 verwenden.
enthält eine ausreichend große Partition mit einem anderen Dateisystem, z. B. FAT32	Windows kann nur installiert werden, wenn die Partition neu mit NTFS formatiert wird. Dabei gehen alle Daten auf der Partition verloren. Eine Konvertierung von FAT32 nach NTFS ist während der Installation nicht möglich.
enthält eine Partition mit Windows 10 oder Windows 7 darauf	Sie können zwischen einer Upgrade- und einer Neuinstallation wählen. Nach einer Neuinstallation befinden sich die alten Systemdateien im Ordner <i>Windows.old</i> . Ihre Benutzerdaten können in jedem Fall übernommen werden, bei einer Upgrade-Installation auch die installierten Programme und Windows-Einstellungen.
enthält eine NTFS-Partition mit anderen Windows-Versionen wie XP oder Vista darauf	Es ist eine Neuinstallation erforderlich, Ihre Benutzerdaten können jedoch übernommen werden. Das alte Windows befindet sich im Ordner <i>Windows.old</i> . Um diese Dateien zu löschen, öffnen Sie nach der Installation das Tool <i>cleanmgr</i> und lassen sich die Systemdateien anzeigen. Hier können Sie alte Betriebssystemdateien schnell und einfach löschen lassen.
enthält eine zu kleine Partition, aber ausreichend nicht partitionierten Bereich	Sie können während der Installation eine neue Partition ausreichender Größe im unpartitionierten Bereich erstellen und diese für die Installation verwenden.
enthält eine nicht mehr benötigte Partition	Löschen Sie diese Partition während der Installation und erstellen Sie anschließend im unpartitionierten Bereich eine neue Partition für Windows 10.

Für die Formatierung der Partition für Windows 10 kann nur das Dateisystem NTFS verwendet werden, obwohl es im Betrieb auch Daten von FAT16- oder FAT32-Partitionen lesen kann. Das Setup-Programm wird eine neu anzulegende Partition automatisch mit NTFS formatieren.



Nutzen Sie einen USB-Stick zur Installation, muss dieser mit FAT32 formatiert sein.

### Checkliste

Überprüfen Sie mithilfe der folgenden Checkliste, ob Sie alle Vorbereitungsschritte erledigt haben.

Vorbereitungsschritt	Erfüllt
Sind die Mindestanforderungen an die Hardware erfüllt?	
Ist die Hardware mit Windows 10 kompatibel?	

Vorbereitungsschritt	Erfüllt
Halten Sie aktuelle Hardwaretreiber bereit, vor allem für die Netzwerkadapter?	
Steht genügend Festplattenkapazität für die Installation bereit?	
Steht die Anzahl der benötigten Partitionen fest?	
Haben Sie einen gültigen Windows-Lizenzschlüssel?	

## 4.2 Installationsdateien bereitstellen

Bei OEM-Datenträgern von Computerherstellern ist oft nur eine Edition vorhanden oder es handelt sich um einen Recovery-Datenträger zum Wiederherstellen des Systems in den Ursprungszustand. Ein Sonderfall sind die Enterprise-Editionen, die jeweils einzeln auf DVD für 32 Bit und 64 Bit zu finden sind.

### USB-Stick für Windows 10 erstellen

Am schnellsten und einfachsten lässt sich die Installation durchführen, wenn Sie einen USB-Stick erstellen. Mit diesem können Sie Windows 10 auch auf PCs installieren, auf denen kein DVD-Laufwerk verfügbar ist. Sie können mit dem Diskpart-Befehl von Windows 7/8 auch USB-Sticks für Windows 10 erstellen.

Um einen USB-Stick für die Installation von Windows 10 anzufertigen, benötigen Sie zunächst die Installationsdateien als bereitgestellte ISO-Datei oder als DVD-Laufwerk. Anschließend verbinden Sie den Stick mit einem Windows-PC und bereiten diesen für die Windows-10-Installation vor. Verwenden Sie einen Windows 7/8- oder Windows-10-PC, da nur hier die entsprechenden Tools verfügbar sind.

- ▶ Starten Sie eine Eingabeaufforderung über das Kontextmenü im Administratormodus. Geben Sie dazu zum Beispiel cmd auf der Startseite ein, öffnen Sie das Kontextmenü der Eingabeaufforderung und klicken Sie auf *Als Administrator ausführen*.
- ▶ Geben Sie diskpart und anschließend list disk ein.
- ▶ Geben Sie den Befehl select disk <Nummer des USB-Sticks aus list disk> ein. Sie erkennen den Stick an dessen Größe.
- ▶ Geben Sie clean und anschließend create partition primary ein.
- ▶ Um die Partition zu aktivieren, geben Sie active ein.  
Dies ist für den Bootvorgang notwendig, denn nur so kann der USB-Stick booten.
- ▶ Formatieren Sie den Datenträger mit format fs=fat32 quick.
- ▶ Geben Sie den Befehl assign ein, um im Explorer einen Laufwerkbuchstaben zuzuordnen.
- ▶ Beenden Sie Diskpart mit exit.
- ▶ Kopieren Sie den Inhalt der Windows-10-DVD bzw. ISO-Datei in den Stammordner des USB-Sticks.

Booten Sie einen PC mit diesem Stick, startet die Windows-10-Installation.

Microsoft stellt ein Freeware-Tool zur Verfügung, mit dem Sie aus einer ISO-Datei ebenfalls einen bootfähigen USB-Stick erstellen können.

- ▶ Laden Sie dazu das kostenlose Windows USB/DVD-Download-Tool von der Webseite <https://www.microsoft.com/en-us/download/windows-usb-dvd-download-tool> herunter.

## Tool zur Medienerstellung und ADK nutzen

Microsoft unterstützt Kunden mit einem kostenlosen Tool zur Medienerstellung (<http://www.microsoft.com/de-de/software-download/windows10>), um die Installationsdateien herunterzuladen. Voraussetzung ist ein gültiger Produktschlüssel für Windows. Nach dem Download können Sie sich einen bootfähigen USB-Stick (oder eine ISO-Datei) erstellen.

Um Windows 10 im Unternehmen bereitzustellen, stellt Microsoft das kostenlose **Windows Assessment and Deployment Kit (ADK)** zur Verfügung. Dieses stellt den Nachfolger des Windows Automated Installation Kit (WAIK) dar. ADK bietet neue Werkzeuge und neue Funktionen, um Windows 10 im Unternehmen zur Verfügung zu stellen (<https://docs.microsoft.com/de-de/windows-hardware/get-started/adk-install>).

Das ADK unterstützt auch die Bereitstellung von Windows Server 2012/2012 R2/2016 und von Windows 7/8/8.1. Oft ist auf neuen Rechnern kein Aufkleber mit dem Produktschlüssel wie noch bei Windows 7. Dies liegt daran, dass der Schlüssel oft im BIOS des Rechners gespeichert ist. Wollen Sie einen solchen Schlüssel auslesen, verwenden Sie Tools wie Nirsoft ProduKey ([http://www.nirsoft.net/utils/product\\_cd\\_key\\_viewer.html](http://www.nirsoft.net/utils/product_cd_key_viewer.html)). Das Tool funktioniert auch mit Windows 10.

Wenn Sie über Windows Update einen Rechner von Windows 7/8/8.1 zu Windows 10 kostenlos aktualisieren, ändert sich auch die Seriennummer. Sie können den Rechner zwar komplett neu installieren, sollten aber vorher den neuen Schlüssel auslesen. Diesen verwenden Sie dann zur Neuinstallation.



## 4.3 Windows 10 neu installieren

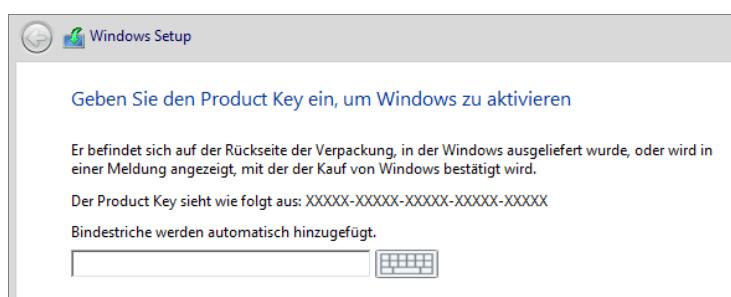
Die Installation von DVD oder einem USB-Stick ist das Standardverfahren zur manuellen Neuinstallation von Windows 10. Die Installations-DVD und der im vorhergehenden Abschnitt erstellte USB-Stick sind bootfähig. Sie können den PC direkt von der Installations-DVD starten, auch wenn noch kein Betriebssystem installiert ist. Windows 10 verfügt über den Sprachassistenten Cortana. Dieser begleitet bereits bei der Installation, kann aber jederzeit deaktiviert werden.

Achten Sie darauf, dass im BIOS als erstes Startlaufwerk der Installationsdatenträger ausgewählt ist. Alternativ können Sie bei den meisten Mainboards mit **F12** die Bootreihenfolge für diesen Startvorgang ändern.

- ▶ Legen Sie den Datenträger ein und starten Sie den Computer.

Nach dem Start vom Installationsdatenträger wird zunächst die Hardware überprüft und dann das Setup-Programm gestartet.

- ▶ Wählen Sie im ersten Bildschirmdialog die gewünschte Installationssprache, das Uhrzeit- und Währungsformat sowie die Tastaturbelegung.
- ▶ Starten Sie anschließend die Installation von Windows 10, indem Sie auf *Weiter* klicken.
- ▶ Geben Sie im nächsten Dialog den **Windows-Produktschlüssel** (engl. Product Key) ein.  
Das Fenster erscheint allerdings nicht bei allen Editionen/Versionen.
- ▶ Stimmen Sie anschließend dem Endbenutzer-Lizenzvertrag (EULA, End User License Agreement) zu.



Außer bei der 90-Tage-Testversion ist es nicht möglich, die Installation ohne die Eingabe eines Product Keys fortzusetzen. Im Gegensatz zu den Vorgängerversionen lässt sich Windows 10 nicht 30 Tage lang als zeitlich limitierte Testversion betreiben. Im Internet sind einige Anleitungen zu finden, wie Sie über die Konfigurationsdatei *ei.cfg* auch ohne Product Key installieren können.

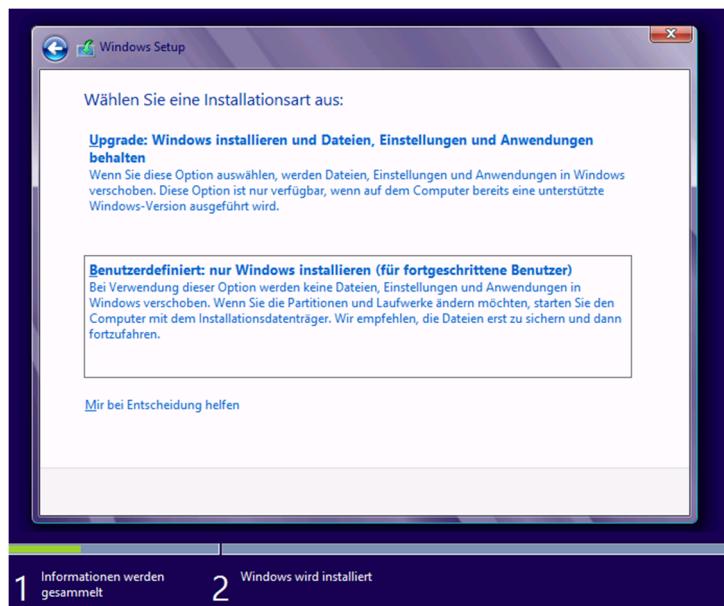


## Installationsmethode wählen

Im nebenstehenden Dialogfenster können Sie zwischen einer Neuinstallation (benutzerdefiniert) oder einem Upgrade eines vorhandenen Betriebssystems (wenn vorhanden) wählen.

Bei der 90-Tage-Testversion wird die Upgrade-Installation zwar angezeigt, ist jedoch nicht verfügbar.

- Klicken Sie für eine Neuinstallation auf *Benutzerdefiniert*.



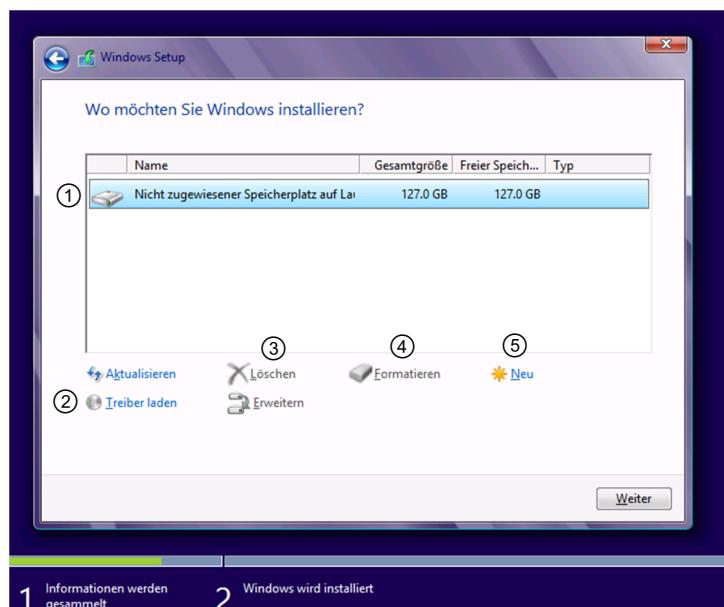
## Installationspartition auswählen

Der Partitionsmanager wird angezeigt. Hier haben Sie die Möglichkeit, eine Partition für die Windows-10-Installation auszuwählen oder vorhandene Partitionen zu bearbeiten.

- Klicken Sie auf die gewünschte Partition ① oder einen freien Bereich, der groß genug ist.

Sollte auf dem Windows-Installationsdatenträger der benötigte Treiber für den von Ihnen verwendeten Festplattencontroller nicht enthalten sein, können Sie diesen nach Bedarf über *Treiber laden* ② hinzufügen.

Sie können vor der Installation manuell die Partitionierung der Festplatte ändern, indem Sie bestehende Partitionen löschen ③, formatieren ④ oder neue Partitionen anlegen ⑤.



Wenn Sie einen unformatierten Datenträger auswählen, um Windows 10 zu installieren, beachten Sie, dass der Assistent für Sie automatisch zwei Partitionen erstellt: eine versteckte Bootpartition ohne Laufwerkbuchstaben und den Rest des Datenträgers als eine einzige Partition mit dem Laufwerkbuchstaben C:.



In manchen Fällen kann es passieren, dass Windows während einer Neuinstallation keine Partition anlegen kann. Dies passiert vor allem bei neuen Festplatten. Überprüfen Sie in diesem Fall, ob im BIOS des Rechners die eingebaute Festplatte in der Boentreihenfolge ganz oben steht. Entfernen Sie außerdem alle SD-Karten, USB-Sticks und externen Datenträger. Starten Sie den Rechner neu, lässt sich die Partition normalerweise neu erstellen.

Achten Sie im BIOS darauf, dass eine eventuell im System vorhandene SSD-Festplatte als erstes Bootmedium eingetragen ist. Dies muss teilweise an mehreren Stellen erfolgen. Wenn Sie Windows 10 auf einer SSD installieren, kann es passieren, dass der Rechner nicht auf das SSD-Laufwerk zugreifen kann. In jedem Fall hilft es, alle externen Datenträger zu entfernen. Besteht das Problem weiterhin, öffnen Sie den Rechner und ziehen Sie vorübergehend die Kabel aller anderen Datenträger ab.

- Bestätigen Sie mit *Weiter*.

Das Installationsprogramm kopiert alle benötigten Dateien und startet das System neu. Die Installation von Windows 10 verläuft schneller als bei Windows 7.

### Sprachpakete installieren

Haben Sie ein englischsprachiges Windows-System vorliegen oder auch eine Installation in einer anderen Sprache, können Sie beliebig weitere Sprachen installieren. Diese stehen bei Microsoft über CAB-Dateien zur Verfügung. Sie installieren die CAB-Datei und aktivieren die Sprache in Windows. Zukünftig wird die Oberfläche in der gewünschten Sprache angezeigt.

Liegt Ihnen die Sprachdatei vor, suchen Sie auf der Startseite nach *lpksetup*. Haben Sie die Sprache installiert, muss diese zunächst noch aktiviert werden. Wechseln Sie dazu (in der entsprechenden Sprache des Betriebssystems) zu *Systemsteuerung - Zeit, Sprache und Region - Sprache*. Klicken Sie anschließend auf die Sprache, auf die Sie Ihr System umstellen möchten, und dann auf *Optionen*. Hier können Sie die Sprache aktivieren.

## 4.4 Systemeinstellungen vornehmen

Nach dem Neustart von Windows 10 können Sie verschiedene Einstellungen für Windows vornehmen. Die Einstellungen unterscheiden sich etwas von Windows 8/8.1 und deutlich von der Konfiguration nach der Installation von Windows 7. Microsoft aktualisiert die Seiten ständig. Wir gehen nachfolgend von der Installation mit Windows 10, Version 1803 (April 2018 Update) aus.

Hier werden die verschiedenen Einstellungen auf einzelnen Seiten vorgenommen. Zunächst wählen Sie aus, ob Sie mit der Sprachsteuerung die Einstellungen fortsetzen wollen. Deaktivieren Sie den Lautsprecher, erfolgt die weitere Einrichtung wie bisher über Maus und Tastatur. Im Rahmen der Einrichtung von Windows 10 legen Sie darüber hinaus fest, ob Sie den Sprachassistenten Cortana nutzen wollen oder nicht.

### Tastaturlayout, Region und Benutzernamen steuern

Im Rahmen der Einrichtung legen Sie auf den weiteren Fenstern die Region, in der Sie den Rechner installieren und das gewünschte Tastaturlayout fest.

Arbeiten Sie mit einem lokalen Benutzer, können Sie seit Windows 10, Version 1803 auch Sicherheitsfragen hinterlegen, mit denen ein Anwender sein lokales Kennwort selbst zurücksetzen kann. Das funktioniert allerdings nicht in Active Directory-Umgebungen.

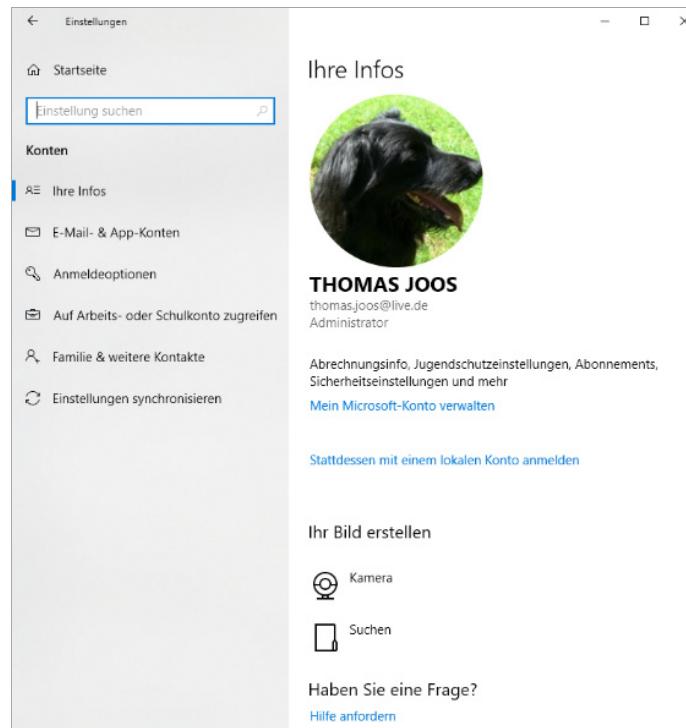


## Benutzernamen und Einstellungen anpassen

Wenn der Computer bereits mit dem Internet verbunden ist, können Sie Ihre E-Mail-Adresse und das Kennwort für die Anmeldung eingeben. Wollen Sie lieber mit einem lokalen Konto arbeiten, finden Sie die Einstellungen dazu ebenfalls bei der Einrichtung.

 Sie können im laufenden Betrieb jederzeit über **Startmenü - Einstellungen - Konten** zwischen einem lokalen Konto und einem Microsoft-Konto wechseln (vgl. Abschnitt 6.1). Sie sehen die Möglichkeiten im Bild rechts. Ein Microsoft-Konto ist zum Beispiel eine E-Mail-Adresse, die Sie bei Microsoft anlegen können.

Hier haben Sie die Möglichkeit, ein neues Microsoft-Konto zu erstellen oder ein lokales Konto, welches Sie nur für die Anmeldung am PC nutzen können.



## Benutzeranmeldung unter Windows 10 Enterprise

Die einzelnen Schritte dauern einige Minuten, bis sie abgeschlossen sind. Danach legen Sie fest, ob Sie sich mit einem Microsoft-Konto anmelden wollen oder an einer Domäne. Dazu klicken Sie auf **Stattdessen der Domäne beitreten**. Dadurch haben Sie die Möglichkeit sich mit einem lokalen Benutzerkonto anzumelden und können hier auch gleich Kennwort und Sicherheitsfragen angeben, mit denen die Anmeldung bei Windows erfolgt. Sie müssen drei Sicherheitsfragen auswählen und die dazu passenden Anmeldungen. Dadurch können Anwender auch selbst ihr Kennwort zurücksetzen.

## Datenschutzeinstellungen vornehmen

Mit jeder Windows-10-Version passt Microsoft die Datenschutzfunktionen in Windows 10 an. Im Rahmen der Installation können Sie im Assistenten mit wenigen Mausklicks festlegen, ob Sie den Sprachassistenten Cortana nutzen wollen, die Sprachsteuerung einsetzen wollen und ob Microsoft den Standort des aktuellen Rechners verwenden darf.



Außerdem können Sie festlegen, dass der PC über Ihr Microsoft-Konto auch gefunden werden kann, ähnlich wie das bei Smartphones und Tablets möglich ist. Auch das Übertragen von Diagnosedaten zu Microsoft können Sie erlauben oder verweigern, genauso wie die Eingabeerkennung von Daten, die Sie freihändig hinterlegen. Dazu kommen weitere Fenster, die den Datenschutz betreffen. Diese sollten durchgearbeitet werden. Microsoft ermöglicht für jeden einzelnen Bereich die Steuerung, ob Daten übertragen werden dürfen oder nicht.

### Benutzeranmeldung über Microsoft-Konto

Melden Sie sich mit einer E-Mail-Adresse über ein Microsoft-Konto an, müssen Sie noch einen **Code** für die Verwendung eingeben. Dazu wird Ihnen eine mehrstellige Zahl zur E-Mail-Adresse zugeschickt, die Sie als Sicherheits-Adresse bei Microsoft auf der Webseite der Adresse konfiguriert haben. Sie finden die Einstellung in der Weboberfläche der E-Mail-Adresse, zum Beispiel bei <http://www.outlook.com>. Diesen Code müssen Sie anschließend im Fenster eingeben. Bei lokalen Konten ist das nicht notwendig.

Haben Sie sich mit der Adresse bereits bei mehreren PCs angemeldet, können Sie auswählen, ob Sie einen der bereits hinterlegten Rechner neu installiert haben oder ob Sie einen neuen Rechner installieren. Anschließend haben Sie auch die Möglichkeit, das Aussehen der Startseite auf den neuen Rechner zu synchronisieren. Bei einer Neuinstallation entfällt das.

Danach erhalten Sie noch den Hinweis, dass OneDrive auf dem Rechner verfügbar ist. Dazu blendet Windows 10 im Navigationsbereich auf der linken Seite des Explorers den neuen OneDrive-Bereich ein. Über diesen können Sie Dateien zwischen dem Internetspeicher und Ihrem Rechner synchronisieren lassen. Nach dieser Konfiguration wird das Konto eingerichtet und der Rechner neu gestartet.

- ✓ Als E-Mail-Adresse ist eine **Outlook.com-Adresse** empfehlenswert. Diese können Sie kostenlos registrieren. Sie erhalten dazu auch kostenlosen Cloudspeicher von Microsoft.
- ✓ Sie können jederzeit zwischen lokalen Konten und Microsoft-Konten wechseln. Die Einstellungen dazu sind in den *Einstellungen* im Bereich *Konten* zu finden. Die Einstellungen dazu sehen Sie im Bild oben rechts auf der vorherigen Seite.



### Microsoft-Konto einsetzen

Windows 10 benötigt ein Microsoft-Konto, damit folgende Funktionen genutzt werden können:

- ✓ Installation von Windows-Apps nur über den **Microsoft Store**,
- ✓ Verwendung von **OneDrive** (Zugriff auf eigene Daten und Medien über das Internet),
- ✓ automatisches Anmelden bei allen Apps, die Microsoft-Konten verwenden, z. B. E-Mail, Messenger, Microsoft Store,
- ✓ automatische Mitnahme von Windows-Apps und Benutzereinstellungen auf einen anderen Windows-10-PC. Alle dafür benötigten Benutzerinformationen werden von Microsoft in der **Cloud** gespeichert, auch die Verwendung vieler Apps. Verwenden Sie ein Microsoft-Konto für die Anmeldung, können Sie die mit diesem Konto gekauften Apps auf einem anderen, oder neu installiert PC mit dem gleichen Konto wieder installieren.
- ✓ Gerät suchen lassen, wenn Sie es nicht mehr finden, zum Beispiel ein Notebook mit Windows 10.

Sie können sich in Windows 10 auch zunächst als lokaler Benutzer anmelden und später dieses Benutzerkonto mit dem Microsoft-Konto verlinken. Dabei können Sie auswählen, in welchen Fällen Ihr Microsoft-Konto verwendet wird. Alternativ können Sie die beiden Konten vollkommen getrennt halten und sich nur bei Bedarf mit dem Microsoft-Konto anmelden. In **Firmendomänen** erfolgt die Windows-Anmeldung wie gewohnt über Domänenkonten.

Beachten Sie, dass dieser erste Benutzer Mitglied der lokalen Gruppe der Administratoren wird.



Das Kennwort sollte mindestens acht Zeichen lang sein und von den vier möglichen Zeichtypen Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen mindestens drei Typen enthalten. Verwenden Sie niemals Klartextwörter oder Namen, die mit Wörterbüchern und Telefonbüchern ermittelt werden könnten.

### Späteres Hinzufügen/Entfernen von Benutzern



Während der Ersteinrichtung können Sie nur **einen** Benutzer hinzufügen. Wenn Sie später noch weitere Benutzer hinzufügen wollen, öffnen Sie über das Startmenü die *Einstellungen - Konten*. Auf der vorhergehenden Seite sehen Sie oben rechts die Möglichkeiten, die an dieser Stelle zur Verfügung stehen.

## 4.5 Auf Windows 10 aktualisieren

Wollen Sie Windows 7/8/8.1 auf Windows 10 aktualisieren, haben Sie verschiedene Möglichkeiten.

Um von Windows 7/8/8.1 zu Windows 10 zu aktualisieren, müssen Sie

- ✓ entweder direkt mit einem Windows-10-Installationsdatenträger die Installation starten,
- ✓ oder Sie aktualisieren den Rechner über Windows Update. Das funktioniert allerdings nicht mit der Enterprise-Version von Windows 7/8/8.1.

Zur Aktualisierung starten Sie Windows Update über den Befehl `wuapp` und rufen dann die Aktualisierung auf. Den Rest erledigt der Installations-Assistent.

Windows XP und Windows Vista können Sie nicht direkt auf Windows 10 aktualisieren. Hier müssen Sie neu installieren (empfohlen) oder erst auf Windows 7 und dann auf Windows 10 aktualisieren.

### Windows 7/8/8.1 mit einem Windows-10-Installationsdatenträger aktualisieren

Wollen Sie Windows 7/8/8.1 mit einem Windows-10-Datenträger aktualisieren, starten Sie zunächst Windows, legen den Windows-10-Datenträger ein und starten das Installationsprogramm. Lassen Sie zunächst die Setup-dateien aktualisieren. Hier lädt der Assistent neue Dateien für die Installation aus dem Internet.

Im nächsten Fenster müssen Sie meist die Seriennummer für Windows 10 eingeben. Danach bestätigen Sie die Lizenzbedingungen für Windows 10.

Im Anschluss können Sie auswählen, welche Daten Sie bei der Aktualisierung behalten wollen. Am besten belassen Sie hier die Auswahl auf *Windows-Einstellungen, persönliche Dateien und Apps behalten*. Klicken Sie auf *Weiter*, führt der Assistent noch verschiedene Vorbereitungen zur Installation durch. Nach einigen Tests erhalten Sie vom Installations-Assistenten den Hinweis, dass das System bereit für die Installation von Windows 10 ist. Klicken Sie auf *Installieren*, beginnt der Assistent mit der eigentlichen Installation und aktualisiert Ihr Windows-System zu Windows 10.

Klicken Sie auf den Link *Auswahl ändern*, gelangen Sie im Assistenten zur Seite für die Auswahl der zu übernehmenden Daten zurück. Nach der Installation startet der Einrichtungs-Assistent von Windows 10, wie bei einer Neuinstallation.

Ändern Sie bei einer Aktualisierung von Windows 7/8/8.1 zu Windows 10 den Anmeldetyp von einem lokalen Konto zu einem Microsoft-Konto ab, übernimmt der Assistent alle Einstellungen und Daten des alten Profils. Sie müssen nachträglich keine Änderungen oder Konfigurationen mehr vornehmen.

## 4.6 Windows 10 aktivieren

### Was die Aktivierung ist

Um den Einsatz unrechtmäßiger Kopien von Windows 10 zu unterbinden, fordert Microsoft die **Aktivierung** des Betriebssystems. Dabei handelt es sich nicht um die optionale **Registrierung** des Kunden, sondern um einen eigenständigen Prozess, der automatisch stattfindet, sobald eine Internetverbindung vorhanden ist. Die bisher übliche 30-Tage-Frist für die Aktivierung gibt es jetzt nicht mehr. Windows 10 muss spätestens zwei Tage nach der Installation durch Microsoft aktiviert werden, sonst meldet Windows, es habe den Echtheitstest nicht bestanden. Nach Ablauf des Aktivierungszeitraums erscheint eine entsprechende Warnmeldung, der Desktophintergrund wird dauerhaft schwarz und nach einer Stunde wird Windows automatisch heruntergefahren.

Bei der Aktivierung wird aus dem **Product Key**, der bei der Installation eingegeben wurde, und der **Hardware** des Computers eine **eindeutige Kennung** generiert und an Microsoft übertragen. Mit dieser Kennung schaltet Microsoft das Betriebssystem frei. Diese Aktivierung ist bei jeder Windows-Neuinstallation erforderlich oder wenn mehrere Hardware-Komponenten ausgetauscht wurden. Nach einem Wechsel der Hardware kann üblicherweise dreimal neu über das Internet aktiviert werden, danach müssen Sie die Aktivierung telefonisch vornehmen.

Windows 10 muss im **Unternehmen** genau wie Windows 7/8/8.1 im Rahmen des sogenannten **Volume Licensing** aktiviert werden. Es besteht jedoch für Firmen die Möglichkeit, diese Aktivierung über einen lokalen Serverdienst zu zentralisieren und die Informationen gesammelt an Microsoft zu übermitteln. Derart aktivierte Windows-10-Computer müssen jedoch regelmäßigen Kontakt zum Aktivierungsserver haben, sonst verfällt die Aktivierung. Wenn Sie einen Rollout von vielen Windows-10-Installationen planen und sich den Aufwand einzelner Aktivierungen sparen wollen, erkundigen Sie sich bei Ihrem Lizenzierungspartner oder bei Microsoft nach einer Volumenlizenz auf Basis eines **MAK** (**M**ultiple **A**ctivation **K**ey) bis 25 Computer oder **KMS** (**K**ey **M**anagement **S**ervice) ab 25 Computern. Beim MAK verbinden sich zur Aktivierung alle Computer direkt mit Microsoft, während beim KMS die Aktivierung zentral über den KMS-Server stattfindet.

Ein wichtiges Werkzeug ist das **Volume Activation Management Tool** (VAMT), das Bestandteil des Windows Automated Distribution Kits (Windows ADK) ist. Mit dem VAMT können Sie für MAK einen Proxyserver einrichten oder zwischen MAK und KMS wechseln.

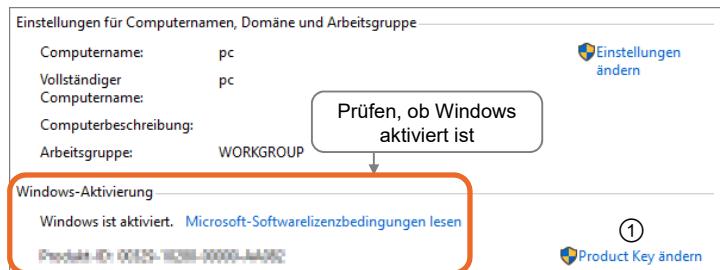


### Die Aktivierung durchführen

Windows 10 wird durch den Windows Product Key automatisch aktiviert, die Aktivierung ist daher kein getrennter Vorgang mehr. Windows meldet nur bei fehlendem oder ungültigem Produktschlüssel, dass es nicht aktiviert ist. Wenn dieser Fall eintritt, können Sie einen neuen Schlüssel eingeben. Den Stand der Aktivierung sehen Sie in den Eigenschaften von *Dieser PC* in Windows 10. Wenn Sie zu Windows 10 aktualisieren, sollten Sie Windows am besten vorher aktivieren. Die Aktivierung wird normalerweise bei der Aktualisierung übernommen. Wenn nicht, können Sie diese jederzeit nachholen.

Wenn der Computer bisher noch nicht aktiviert wurde, werden Sie automatisch über ein Informationsfenster zur Aktivierung aufgefordert. Nach Ablauf von 30 Tagen fordert Windows 10 Sie erneut zur Aktivierung auf. Mit dem Befehl `slui` starten Sie den Assistenten zur Aktivierung aus dem Startmenü heraus.

- ▶ Rufen Sie im Explorer die Eigenschaften von *Dieser PC* auf und klicken Sie im unteren Bereich auf die Möglichkeiten zur Aktivierung.
- ▶ Klicken Sie auf *Product Key ändern* oder *Windows aktivieren* ① und geben Sie Ihren Windows-10-Key ein, wenn hier noch kein Key verfügbar ist.



Sie erhalten die Meldung, dass die Aktivierung erfolgreich war.

Die telefonische Aktivierung ist auch bei Windows 10 möglich, allerdings ist der entsprechende Assistent nur durch die Eingabe von `sldi 4` in einer Eingabeaufforderung mit Administratorrechten erreichbar.



In der Befehlszeile aktivieren Sie Windows 10 mit dem Befehl `sldmgr /ato`.

### Verlängerung des Testzeitraums

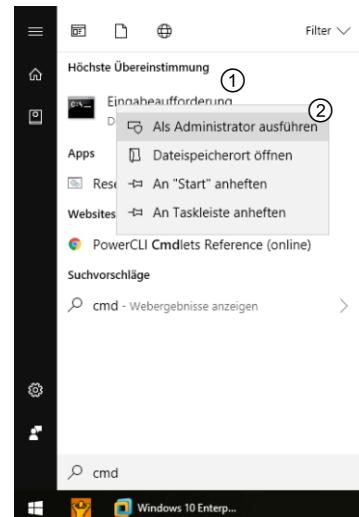
Besonders für Testsysteme, auf denen Sie neue Hard- oder Software und Updates ausprobieren, bevor sie in der Produktivumgebung eingesetzt werden, machte es bisher wenig Sinn, sofort eine Windows-Lizenz zu verwenden und Windows zu aktivieren. Dieses Verfahren funktioniert bei regulären Windows-Versionen nicht mehr, da diese schon nach zwei Tagen eine Aktivierung erfordern, es kann jedoch noch bei der 90-Tage-Testversion angewendet werden. Nachdem die ersten 90 Tage verstrichen sind, können Sie den Testzeitraum von Windows 10 insgesamt dreimal auf 90 Tage zurücksetzen. Dazu benötigen Sie eine Eingabeaufforderung mit Administratorrechten:

- ▶ Öffnen Sie eine Kommandozeile, indem Sie im Startbildschirm `cmd` eingeben.
- ▶ Klicken Sie mit der rechten Maustaste auf ① und anschließend auf *Als Administrator ausführen* ②.  
*oder*
- ▶ Geben Sie `cmd` [Strg] [↑] [←] ein.

Es öffnet sich auf dem Desktop eine Eingabeaufforderung.

- ▶ Geben Sie `sldmgr /rearm` [←] ein.

Nach einem Neustart haben Sie wieder 90 Tage Zeit, um Windows zu aktivieren.



Kontextmenü für cmd.exe

Sie möchten ...	
den Status überprüfen	▶ Geben Sie <code>sldmgr /dli</code> oder <code>sldmgr /dlv</code> ein.
weitere Optionen auflisten	▶ Geben Sie <code>sldmgr /?</code> ein.
Windows online aktivieren	▶ Geben Sie <code>sldmgr /ato</code> ein.
detaillierte Infos für alle installierten Lizenzen anzeigen	▶ Geben Sie <code>sldmgr /dlv all</code> ein.

Sie können den Product Key einer Windows-10-Installation auch in der Befehlszeile anpassen. Dazu benötigen Sie eine Eingabeaufforderung, die Sie mit Administratorrechten starten:

- ▶ Geben Sie zum optionalen Löschen des alten Product Keys in der Eingabeaufforderung den Befehl `sldmgr /upk` ein.
- ▶ Bestätigen Sie das Löschen.
- ▶ Geben Sie den neuen Product Key mit `sldmgr /ipk xxxxx-xxxxx-xxxxx-xxxxx-xxxxx` ein.
- ▶ Aktivieren Sie Windows 10 mit `sldmgr /ato`.

### 90-Tage-Testversion von Windows 10 Enterprise

Von Microsoft wird für Systembetreuer und Administratoren eine spezielle Version von Windows 10 Enterprise zum Download bereitgestellt. Diese Version ist 90 Tage lang lauffähig und muss nach spätestens 10 Tagen aktiviert werden. Nach Ablauf der Aktivierungsfrist oder nach 90 Tagen wird das System nach einer Stunde Betrieb automatisch heruntergefahren. Der Download der Testversion erfordert ein Microsoft-Konto und ist erhältlich unter: <http://technet.microsoft.com/de-DE/evalcenter>.

## 4.7 Updates installieren

Nach der Installation von Windows 10 sollten Sie über die Auswahl von Einstellungen im Startmenü zunächst bei *Update und Sicherheit - Windows Update* aktuelle Updates suchen und installieren lassen.

- ▶ Klicken Sie auf *Nach Updates suchen*.
- ▶ Werden Updates angezeigt, klicken Sie auf *Jetzt Installieren* beziehungsweise auf *Herunterladen*.
- ▶ Wiederholen Sie den Vorgang, bis keine Updates gefunden werden.
- ▶ Klicken Sie auf *Erweiterte Optionen*.
- ▶ Wählen Sie hier die erweiterten Funktionen zur Aktualisierung aus, wie zum Beispiel den Download von anderen Microsoft-Produkten, wie z. B. Microsoft Office über Windows Update.

Aktivieren Sie auf PCs mit Windows 10 Pro/Enterprise die Option *Upgrades aussetzen*, werden die meisten Updates mehrere Wochen später heruntergeladen und installiert. Sicherheitsupdates sind von der Zurückstellung ausgenommen. Die genaue Verzögerung können Sie in den erweiterten Optionen festlegen. Aktualisierungen wie das April 2018-Update von Windows 10 werden von Microsoft auch als **Funktionsupdate** bezeichnet.



## 4.8 Fehlerbehandlung

### Allgemeine Probleme beheben

Die folgende Tabelle fasst die häufigsten Probleme, die bei einer Installation von Windows 10 auftreten können, zusammen und macht Vorschläge zur Lösung.

Problem	Ursachen und Lösungsmöglichkeiten
Die Installation startet nicht.	Die Bootreihenfolge ist nicht korrekt eingestellt oder ein Teil Ihrer Hardware ist nicht mit Windows 10 kompatibel. Ersetzen Sie die problematische Komponente.
Die Installation bricht ab oder geht nicht weiter.	Starten Sie den Computer neu und versuchen Sie es erneut. Möglicherweise kann Windows die Installation sogar reparieren und fortsetzen. Installationsfehler hängen oft mit Lese-/Schreibproblemen der Festplatte, des USB-Mediums oder optischen Laufwerks und den Controllern zusammen, an die sie angeschlossen sind. Bei der Installation von Windows 10 in virtuellen Maschinen sind geeignete Einstellungen für Laufwerke und Controller besonders wichtig.
Die Installation wird mit einem Bluescreen angehalten.	Ein Bluescreen deutet auf einen Hardwarefehler hin. Überprüfen Sie alle Hardware-Komponenten und deren Kompatibilität mit Windows 10. Stellen Sie sicher, dass keine inkompatible Hardware in den Computer eingebaut ist. Weitere Hinweise zu den Fehlermeldungen finden Sie in der technischen Referenz von Microsoft zu Windows 10 oder in der Knowledge Base unter der URL <a href="http://support.microsoft.com">http://support.microsoft.com</a> .

## Setup-Protokolle verwenden

Das Installationsprogramm für Windows 10 speichert verschiedene Protokolldateien ab, die während der Installation erstellt wurden. Diese Dateien sind nach der Installation zugänglich. Falls während der Installation ein Problem aufgetaucht ist, können Sie mithilfe der Protokolle oft dessen Ursache ermitteln und eine Lösung versuchen. Die meisten Protokolldateien befinden sich im Ordner *Windows\Panther*. Unter anderem werden folgende Dateien angelegt:

- ✓ das Aktionsprotokoll %SYSTEMROOT%\Panther\setupact.log,
- ✓ das Fehlerprotokoll %SYSTEMROOT%\Panther\setuperr.log.

Die Datei *setupact.log* zeichnet alle Aktionen auf, die das Installationsprogramm ausführt, beispielsweise das Kopieren von Dateien und das Erstellen von Registry-Einträgen. Bei der Ausführung der Aktionen aufgetretene Fehler werden ebenfalls in das Protokoll aufgenommen.

Die Datei *setuperr.log* beinhaltet neben einer Liste der aufgetretenen Fehler auch eine Bewertung nach der Ernsthaftigkeit der Fehler. Wenn die Windows-Installation fehlerhaft war, wird dieses Fehlerprotokoll am Ende der Installation angezeigt. Alle Protokolle können Sie mit Notepad oder einem anderen ASCII-Texteditor öffnen und einsehen.

## Boot-Manager reparieren

Startet Ihr System nicht mehr, haben Sie die Möglichkeit, über die **Computerreparaturoptionen** den Boot-Manager zu reparieren. Dazu starten Sie den Rechner mit der Windows-10-Installations-DVD oder einer Rettungs-CD. Zur Reparatur starten Sie am besten eine Eingabeaufforderung in den Bootoptionen. Wählen Sie *Problembehandlung - Erweiterte Optionen - Eingabeaufforderung*. Danach geben Sie Befehle ein, mit denen Sie häufig den Boot-Manager Ihres Rechners reparieren können:

- ✓ Mit dem Befehl bootrec /fixmbr haben Sie eine große Chance, das System zu retten. Der Befehl schreibt den Master Boot Record (MBR) neu an den Beginn der Festplatte.
- ✓ Hilft das nicht, lassen Sie mit bootrec /scanos die Betriebssysteme anzeigen, die nicht im Boot-Manager eingetragen sind. Hier sehen Sie schnell, ob es Systeme gibt, die der Manager erkennt, aber noch nicht eingebunden hat.
- ✓ Der Befehl bootrec /rebuildbcd kann diese Systeme wieder in den Boot-Manager eintragen.
- ✓ Oft hilft auch bootrec /fixboot, wenn Sie parallel zu Windows 10 noch ein anderes Betriebssystem wie beispielsweise Windows 7/8/8.1 auf dem Computer installiert haben. Der Befehl erstellt den Boot-Manager bootmgr neu.

Windows 10 startet von Bootpartitionen, die als aktiv gekennzeichnet sein müssen. Ist dies nicht der Fall, verweigern beide den Start. Um die entsprechende Festplatte als aktiv zu markieren, gehen Sie folgendermaßen vor:

- ▶ Starten Sie den PC mit der Installations-DVD oder, falls noch möglich, mit der F8-Taste in den Computerreparaturoptionen.
- ▶ Öffnen Sie eine Eingabeaufforderung.
- ▶ Geben Sie im Diskpart-Kontext den Befehl select disk 0 ein, um die erste Festplatte im System auszuwählen.
- ▶ Geben Sie select partition 1 ein.
- ▶ Geben Sie active ein.
- ▶ Beenden Sie Diskpart mit exit und starten Sie den Computer neu.

## Computerreparaturoptionen aufrufen

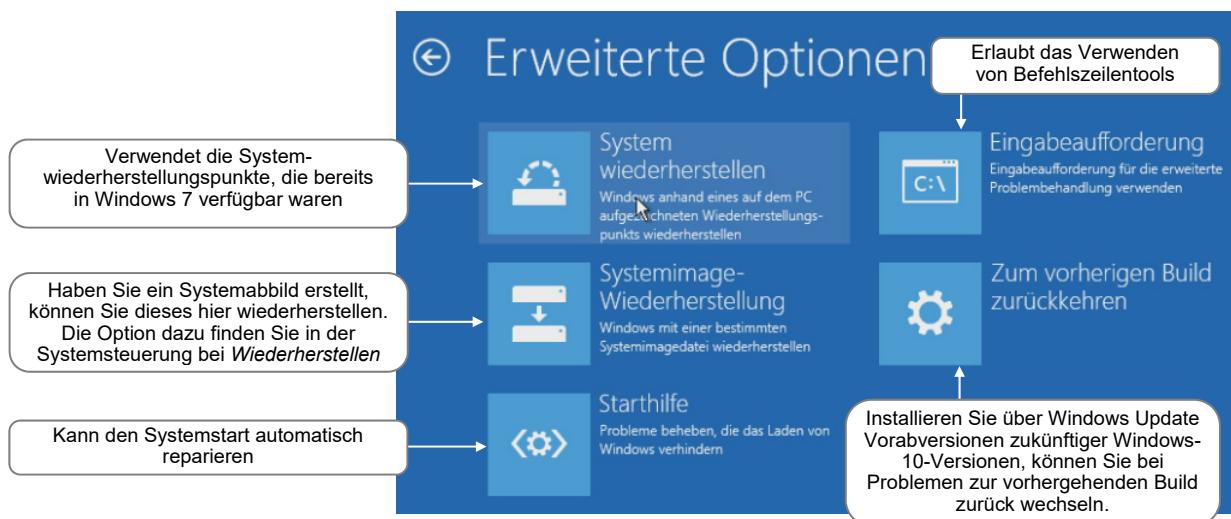
Starten Sie von einem Windows-10-Installationsdatenträger, können Sie durch Auswahl von *Computerreparaturoptionen* verschiedene Wiederherstellungsmaßnahmen auswählen:

- Klicken Sie dazu nach dem Start der *Computerreparaturoptionen* auf *Problembehandlung*.

Auf der neuen Seite stehen verschiedene Optionen zur Verfügung:

- ✓ *Diesen PC zurücksetzen* – Stellt das Betriebssystem wieder her und kann eigene Daten erhalten oder löschen. Installierte Anwendungen gehen in jedem Fall verloren.
- ✓ *Erweiterte Optionen* – Zusätzliche Reparaturoptionen, wie die Möglichkeit, den Start des Betriebssystems automatisch zu reparieren, Wiederherstellungspunkte zu nutzen und vieles mehr.

In den erweiterten Optionen stehen zahlreiche Möglichkeiten zur Verfügung, um Windows 10 zu reparieren:



## 4.9 Übung

### Windows 10 installieren

Übungsdatei: --

Ergebnisdatei: Uebung04\_E.pdf

1. Mit welcher Software lässt sich Windows 10 im Unternehmen bereitstellen?
2. Kann Windows 10 auch ohne DVD-Laufwerk erstellt werden?
3. Wie erhalten Sie eine ISO-Datei für Windows 10?
4. Mit welchen beiden Befehlen lässt sich die Aktivierung von Windows 10 starten?
5. Wie rufen Sie die erweiterten Optionen von Windows Update auf?
6. Wie rufen Sie die Computerreparaturoptionen auf?

# 5 Systemstart

## In diesem Kapitel erfahren Sie

- ✓ wie Windows 10 startet
- ✓ wie Sie sich unter Windows 10 anmelden können
- ✓ welche Startoptionen Sie für die Problembehebung nutzen können

## 5.1 Der Bootvorgang

### Computer mit EFI bzw. UEFI und GPT

Bei Computern mit dem BIOS-Nachfolger **Unified Extensible Firmware Interface** (UEFI) ist das Verfahren ähnlich wie beim BIOS. Beim Start des Computers werden einige Tests durchgeführt und die Hardware initialisiert, nach bootfähigen Datenträgern gesucht und das Betriebssystem gestartet. Dieser Vorgang geht bei den meisten UEFI-Mainboards schneller vonstatten als bei BIOS-Mainboards. Als Besonderheit verfügt jedes UEFI über einen BIOS-Kompatibilitätsmodus namens **Compatibility Support Module (CMS)**, der manuell aktiviert werden kann. Anschließend verhält sich das Mainboard wie ein herkömmliches BIOS-Mainboard.

Wenn ein GPT-Datenträger mit UEFI-Bootloader gefunden wird, wird davon gestartet, ansonsten schaltet das UEFI automatisch in den CMS-Modus und kann so auch von herkömmlichen Datenträgern mit MBR booten. Auf diese Weise können auch Betriebssysteme gestartet werden, die kein UEFI und GPT unterstützen. Dies betrifft alle Windows-Versionen mit 32 Bit, auch Windows 10.

Der Bootloader, der Boot-Manager und die BCD werden in der EFI-Systempartition gespeichert, die sowohl auf einer Festplatte mit MBR als auch auf einer mit GPT liegen kann.

### Computer mit BIOS und MBR

#### Selbsttest

Wenn Sie einen Computer mit herkömmlichem BIOS einschalten, führt er automatisch den **POST (Power-on Self Test)** durch. Dabei wird die Größe des Arbeitsspeichers ermittelt und die angeschlossenen Hardware-Komponenten werden überprüft. Im BIOS kann eingestellt werden, wie ausführlich diese Tests sein sollen.

#### Der Windows Boot-Manager

Anschließend versucht das BIOS, das Betriebssystem zu starten. Dazu werden die Geräte in der Bootreihenfolge angesprochen, bis ein bootfähiger Datenträger gefunden wird, z. B. erst das optische Laufwerk, dann die erste Festplatte, dann USB usw. Normalerweise befindet sich das Windows-Betriebssystem auf einer magnetischen Festplatte oder SSD.

Auf der ersten Festplatte im System befindet sich im ersten Sektor der **Masterbootsektor (MBR, Master Boot Record)**, aus dem das BIOS die Partitionstabelle liest.

Daraufhin wird aus dem ersten Sektor der Systempartition, d. h. aus dem sogenannten **Bootsektor**, der Startcode für das Betriebssystem in den Speicher geladen und gestartet. Nun wird das Dateisystem festgelegt und die Datei *Bootmgr* gestartet. Dies ist der **Windows-10-Boot-Manager**, der in etwa die Funktion der Datei *ntldr* bei älteren NT-basierten Betriebssystemen übernimmt.

## BCD, Boot Configuration Data

Der **Bootmgr** wurde während der Installation von Windows 10 auf der ersten Partition des Laufwerks hinterlegt. Dies ist standardmäßig eine von Windows eingerichtete Bootpartition ohne zugewiesenen Laufwerkbuchstaben, daher ist sie nur in der Datenträgerverwaltung sichtbar. Die Bootpartition ist zwischen 350 MB und mehreren Gigabyte groß und enthält neben dem **Bootmgr** auch das **BCD (Boot Configuration Data)**. Das BCD ist eine der Windows Registry ähnliche Datenbank mit Konfigurationsdaten, die während des Bootvorgangs benötigt werden. Sie ersetzt die Konfigurationsdatei *boot.ini*.

Wenn Windows 10 bei der Installation keine versteckte Partition anlegen konnte, befindet sich der **Bootmgr** auf der Systempartition und das BCD im versteckten Ordner *boot* auf der ersten Partition der ersten Festplatte im System. Da Windows 10 für die eigene Systempartition stets den Laufwerkbuchstaben C: verwendet, kann die erste Partition auch einen anderen Laufwerkbuchstaben haben und auf einer anderen Festplatte liegen.

Während dieser Anfangsphase des Windows-Starts können Sie durch **[F8]** oder **[↑] [F8]** die Windows-Startoptionen aufrufen. Dies funktioniert allerdings nicht auf allen Systemen, da das Zeitfenster zu kurz ist.

Startet Windows 10 noch, können Sie den abgesicherten Modus über die Systemkonfiguration (msconfig.exe) im Suchfeld des Startmenüs starten. Rufen Sie das Tool auf und wechseln Sie zur Registerkarte *Start*. Aktivieren Sie das Kontrollkästchen *Abgesicherter Start*. Klicken Sie auf *OK* und starten Sie dann den Rechner neu. Damit Windows 10 wieder normal startet, rufen Sie im abgesicherten Modus wieder msconfig auf und deaktivieren den Modus wieder. Anschließend wählen Sie *Erweiterte Optionen* und danach *Starteinstellungen*. Klicken Sie danach auf *Neu starten*, erscheint ein Systemmenü, in dem Sie auch den abgesicherten Modus starten können.

Brechen Sie den Startvorgang von Windows 10 zwei- bis dreimal ab, startet automatisch die *Automatische Reparatur* von Windows 10. Um hier in den abgesicherten Modus zu wechseln, rufen Sie im Reparaturmenü zunächst *Erweiterte Optionen* auf. Im Dialogfenster *Option auswählen* wählen Sie *Problembehandlung* aus.

Wenn auf Ihrem System mehrere Betriebssysteme installiert sind, wird der Bootvorgang anschließend angehalten. Sie können nun mit der Maus oder den Cursortasten **[↑]** und **[↓]** das gewünschte Betriebssystem auswählen. Außerdem können Sie auf dieser Seite Einstellungen zum Windows-Start vornehmen, die in Abschnitt 5.4 beschrieben werden.

Um Einträge in der BCD editieren zu können, wird von Microsoft zusammen mit Windows 10 das komplexe **Kommandozeilentool BCDEdit** ausgeliefert.

Mit dem Aufruf **bcdedit .exe /?** erhalten Sie eine detaillierte Übersicht über alle möglichen Befehle.

Beachten Sie, dass Sie durch unbedachten Einsatz von BCDEdit Ihre Windows-Installation beschädigen können. Der Einsatz von BCDEdit erfordert Administratorrechte.



## Auszug aus verfügbaren BCDEdit-Befehlen

**BCD-Kommandos, die für Speicherbereiche gelten:**

<b>/createstore</b>	Legt einen neuen Konfigurationsspeicher an
<b>/export</b>	Exportiert die Inhalte des Systemspeichers in eine Datei
<b>/import</b>	Stellt den Zustand des Systemspeichers aus einer Datei wieder her
<b>/sysstore</b>	Legt auf EFI-Systemen bis zum Neustart das Systemspeichergerät neu fest



BCDEdit-Kommandos, die auf Einträge innerhalb eines Speicherbereichs angewandt werden können:

/copy	Fertigt eine Kopie eines Booteintrages im selben Systemspeicher an
/create	Legt einen neuen Eintrag an
/delete	Löscht ein Element aus dem angegebenen Eintrag
/mirror	Erstellt eine Spiegelung der Einträge im Speicher

BCDEdit-Kommandos, die auf Eintragsoptionen angewandt werden können:

/deletevalue	Löscht ein spezifiziertes Element aus einem Booteintrag
/set	Setzt einen Wert für einen Booteintrag

BCDEdit-Kommandos, die den Boot-Manager direkt konfigurieren:

/bootsequence	Legt einmalig für den nächsten Systemstart die Anzeigereihenfolge der zu bootenden Betriebssysteme fest
/default	Gibt den Defaulteintrag in der Liste an, der geladen wird, wenn der Benutzer innerhalb des Timeouts keinen Eintrag wählt
/displayorder	Legt die Reihenfolge fest, in der die Booteinträge dem Benutzer angezeigt werden
/timeout	Legt die Wartezeit fest, bevor der Defaulteintrag geladen wird
/toolsdisplayorder	Legt die Reihenfolge fest, in der das Tools-Menü im Boot-Manager angezeigt wird

Einträge wie zum Beispiel zum Festlegen der Anzeigereihenfolge im Auswahlmenü werden über ihre **GUID** (**Global Unique Identifier**) angesprochen. Das Festlegen der Anzeigereihenfolge von drei Menüeinträgen würde dann in der Eingabeaufforderung z. B. so aussehen:

```
bcdedit.exe /displayorder {c84b751a-ff09-11d9-9e6e-0030482375e6} {c74b751a-ff09-11d9-9e6e-0030482375e4} {c34b751a-ff09-11d9-9e6e-0030482375e7}
```

Möchten Sie die Reihenfolge der Betriebssysteme im Boot-Manager von Windows anpassen, benötigen Sie wieder eine Eingabeaufforderung mit Administratorrechten. Geben Sie `bcdedit` ein und notieren Sie sich den Wert bei *Bezeichner* des Eintrags des Betriebssystems.

Sie können den Eintrag auch in die Zwischenablage kopieren, wenn Sie das Menü der Eingabeaufforderung öffnen und *Bearbeiten - Markieren* wählen. Markieren Sie den neben *Bezeichner* angegebenen Eintrag und bestätigen Sie mit der *←*-Taste. Um die Reihenfolge anzupassen, verwenden Sie den folgenden Befehl:

```
bcdedit /displayorder {current} {<Bezeichner des anderen Systems>}
```

Wollen Sie vorhandene Einträge kopieren, um diese z. B. testweise zu bearbeiten, verwenden Sie den Befehl:

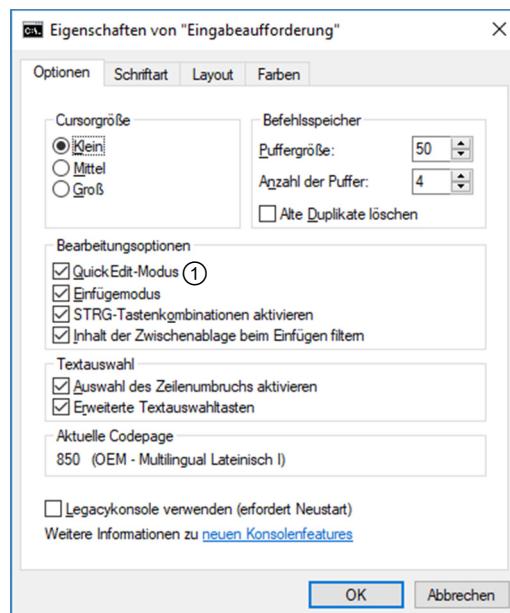
```
bcdedit /copy {current} /d "<Neuer Name>"
```

Weitere Optionen von `bcdedit` erhalten Sie mit der Option `/?`.

### Zusätzlichen Booteintrag erstellen

Um auch ohne funktionierende F8-Taste Zugriff auf die erweiterten Starteinstellungen zu erlangen, können Sie mit BCDEdit einen neuen Eintrag ins Bootmenü einfügen. Auf diesem Weg können Sie zum Beispiel ein zweites Windows 8-System registrieren, das Sie zu Windows 10 aktualisieren. Alternativ erstellen Sie einen Eintrag für Windows 10 im abgesicherten Modus wie folgt:

- ▶ Öffnen Sie eine Eingabeaufforderung mit Administratorrechten, indem Sie im Startbildschirm cmd eingeben und die Verknüpfung mit der rechten Maustaste öffnen.
- ▶ Aktivieren Sie den QuickEdit-Modus, indem Sie mit der rechten Maustaste in die Titelzeile klicken und im Kontextmenü *Eigenschaften* auswählen.
- ▶ Aktivieren Sie im Register *Optionen* den *QuickEdit-Modus* ①. Bestätigen Sie mit OK.



QuickEdit-Modus der Eingabeaufforderung

Diesen Modus benötigen Sie, um einen GUID-Bezeichner in der Eingabeaufforderung kopieren zu können. Der Bezeichner soll in folgendes Kommando eingefügt werden:

```
bcDEDit.exe /copy <Bezeichner> /d "Windows 10 Safe Mode"
```

- ▶ Geben Sie bcDEDit.exe /enum /v ↵ ein, um alle Booteinträge anzuzeigen. Suchen Sie nach dem Bezeichner unter *Windows-Startladeprogramm*.
- ▶ Geben Sie bcDEDit.exe /copy ↵ ein (schließen Sie die Eingabe aber noch nicht mit ↵ ab).
- ▶ Markieren Sie den gesamten Bezeichner ② unter *Windows-Startladeprogramm* mit der Maus.
- ▶ Klicken Sie mit der rechten Maustaste rechts neben das bcDEDit.exe /copy, bis die GUID eingefügt wurde ③.
- ▶ Fügen Sie den restlichen Befehl hinzu, um den neuen Eintrag zu benennen. Geben Sie dazu z. B. /d "Windows 10 Safe Mode" ↵ ④ ein.
- ▶ Überprüfen Sie den neuen Booteintrag ④ durch bcDEDit.exe /enum /v ↵.

```
Administrator: Eingabeaufforderung
Windows-Startladeprogramm
-----
Bezeichner      {d3b40908-36b4-11e5-a014-e0e86700a42e} ②
device          partition=C:
path            \Windows\system32\winload.exe
description    Windows 10
locale         de-DE
inherit        {6efb52bf-1766-41db-a6b3-0ee5eff72bd7}
recoverysequence {d3b40909-36b4-11e5-a014-e0e86700a42e}
recoverenabled Yes
allowedinmemorysettings 0x15000075
osdevice       partition=C:
systemroot     \Windows
resumeobject   {d3b40907-36b4-11e5-a014-e0e86700a42e}
nx             OptIn
bootmenupolicy Standard
④
C:\Windows\system32>bcDEDit /copy {d3b40908-36b4-11e5-a014-e0e86700a42e} /d "Windows 10 Safe Mode"
Der Eintrag wurde erfolgreich in {d3b4090b-36b4-11e5-a014-e0e86700a42e} kopiert.
```

Nun müssen Sie den Starteintrag mit der Systemkonfiguration bearbeiten:

- Geben Sie im Startbildschirm `msconfig.exe` ein, um die Systemkonfiguration zu öffnen.
- Klicken Sie im Register *Start* auf den neuen Booteintrag ①.
- Aktivieren Sie *Abgesicherter Start* ② und *Starteinstellungen sollen immer gelten* ③.

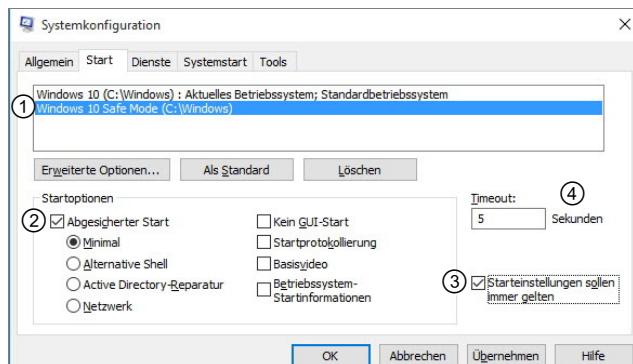
Unter *Timeout* ④ können Sie die Anzeigedauer der Betriebssystemauswahl einstellen. Bei Bedarf können Sie weitere Einstellungen vornehmen.

- Übernehmen Sie die Einstellungen mit *OK* und starten Sie Windows neu, um die Einstellungen in Kraft zu setzen.

Ab sofort gelangen Sie bei jedem Systemstart in die Betriebssystemauswahl. Von dort können Sie auch die Startoptionen erreichen.



Eine weitere Lösung, um beim nächsten Windows-Start in die erweiterten Startoptionen zu gelangen, ist das Anlegen einer neuen Verknüpfung auf dem Desktop mit dem Befehl `shutdown.exe /r /o /f /t 00`. So können Sie per Doppelklick einen Neustart mit erweiterten Startoptionen auslösen.



*Editieren des neuen Booteintrags mit MSConfig*

## 5.2 Windows 10 startet

### Boot-Manager reparieren

Startet Ihr produktives System nicht mehr, haben Sie die Möglichkeit, den Boot-Manager über die **Computerreparatuoptionen** von Windows 10 zu reparieren. Zur Reparatur öffnen Sie eine Eingabeaufforderung über die Bootoptionen. Dazu starten Sie die *Computerreparatuoptionen* über die Windows-10-DVD oder einen Wiederherstellungsdatenträger, den Sie mit `recoverydrive.exe` erstellen. Das Tool `recdisc.exe` gibt es in Windows 10 nicht mehr. Wählen Sie *Problembehandlung*, dann *Erweiterte Optionen* und anschließend *Eingabeaufforderung* (vgl. Abschnitt 4.8).

### Vorgängerversion bei Problemen wieder aktivieren

Windows 10 bietet auch in der Version 1803 die Möglichkeit, zur vorhergehenden Windows-10-Version zu wechseln, in diesem Fall Windows 10, Version 1709. Über den Menüpunkt *Update und Sicherheit - Wiederherstellung*, können Sie bei *Zur vorherigen Version von Windows 10 zurückkehren* die Installation der aktuellen Windows-10-Version rückgängig machen.

Funktioniert Windows 10 nicht mehr, kann mit der Option *Diesen PC zurücksetzen* das Betriebssystem repariert werden. Das kann auch bei Virenbefall eine Lösung sein. Allerdings sind nach dem Zurücksetzen alle Apps entfernt und alle Daten gelöscht. Das Zurücksetzen entspricht im Grunde genommen einer Neuinstallation, ohne dass ein Installationsmedium notwendig ist. Beim Zurücksetzen lässt sich aber auf Wunsch das Behalten eigener Dateien konfigurieren.

## 5.3 Die Anmeldung

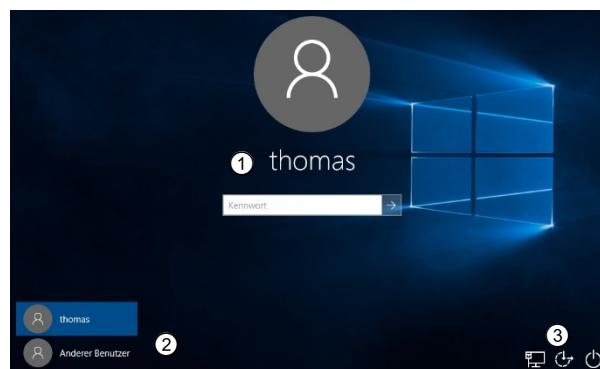
Nach dem Windows-Start wird der **Sperrbildschirm** angezeigt. Benutzerunabhängig werden stets die Uhrzeit, das Datum und der Status der Netzwerkverbindung angezeigt.

Wenn ein Benutzer angemeldet ist, können außerdem noch ungelesene E-Mails, Termine und Kurznachrichten angezeigt werden. Diese Elemente lassen sich in den Einstellungen anpassen.

- Um zur **Benutzeranmeldung** zu gelangen, betätigen Sie eine beliebige Taste.

### Lokale Anmeldung

Wenn Sie Windows 10 das erste Mal nach einer Neuinstallation starten und die Workstation noch nicht Mitglied einer Domäne ist, ist nur das während der Installation angelegte Konto verfügbar. In der folgenden Abbildung wurde ein Konto erstellt. Microsoft-Konten sind an den getrennten Vor- und Nachnamen zu erkennen, während lokale Konten ① keine Leerzeichen enthalten dürfen.



- Klicken Sie auf ein Benutzerbild und geben Sie das Kennwort ein.  
oder Wechseln Sie mit ② und ③ zwischen den Benutzern.

Sie können unter ② unter verschiedenen Anmeldenamen auswählen. Haben Sie Ihren Rechner über die Einstellungen in einer Domäne aufgenommen, können Sie sich über die Auswahl *Anderer Benutzer* z. B. an ein Active Directory oder Azure Active Directory anmelden.

Auf dem Anmeldebildschirm haben Sie außerdem die Möglichkeit, den Computer herunterzufahren oder neu zu starten ③.

### Anmelden in der Domäne

Gehört die Workstation einer Domäne an, kann sich jeder Domänenbenutzer und Domänenadministrator direkt in der Domäne anmelden. Beim Einsatz von Windows 10 Enterprise können Sie eine Arbeitsstation auch an Azure Active Directory anbinden lassen. Der Vorteil dabei ist, dass Sie für den Betrieb keine eigenen Domänencontroller benötigen.

- Geben Sie Benutzername und Kennwort ein und bestätigen Sie mit ④.
- Wollen Sie sich an einer anderen als der aktuellen Domäne anmelden, so geben Sie den Benutzernamen in der Form <Domänenname>\<Benutzername> ein. Alternativ verwenden Sie die Syntax <Benutzername>@<Domäne>.

### Fernanmeldung

Gehört ein Computer nicht der Domäne an, müssen Sie sich zunächst mit einem lokalen Benutzerkonto anmelden. Ein Zugriff auf Domänenressourcen gelingt jedoch nur mit einer Domänenanmeldung. Dazu werden die Informationen der lokalen Anmeldung (Benutzername und Kennwort) an einen Domänencontroller weitergeleitet und dort geprüft. Stimmen diese Informationen mit einem Benutzerkonto der Domäne überein, erfolgt eine automatische Fernanmeldung. Stimmen die Informationen nicht überein, müssen Sie einen in der Domäne gültigen Benutzernamen und ein Kennwort eingeben. Dieser Mechanismus funktioniert nur, wenn auf Ihrem lokalen Rechner ein DNS-Server eingestellt wurde, der die Active Directory-Domäne kennt.

Wenn innerhalb einer Arbeitsgruppe auf einen zweiten Rechner zugegriffen wird, werden ebenfalls Ihre Benutzerdaten mit den vorhandenen Benutzerkonten auf dem zweiten Rechner verglichen. Der Zugriff ist nur erfolgreich, wenn ein Benutzerkonto mit Ihrem Benutzernamen und Kennwort vorhanden ist.

## 5.4 Optionen des Systemstarts

### Nutzen der erweiterten Startoptionen

Falls Windows 10 nicht ordnungsgemäß startet, wird automatisch versucht, das System zu reparieren. In vielen Fällen ist dies auch ohne Eingreifen des Benutzers erfolgreich. Im Prinzip sind neben mehreren neuen Funktionen auch alle von Windows 7/8 bekannten Mechanismen und Startoptionen vorhanden.

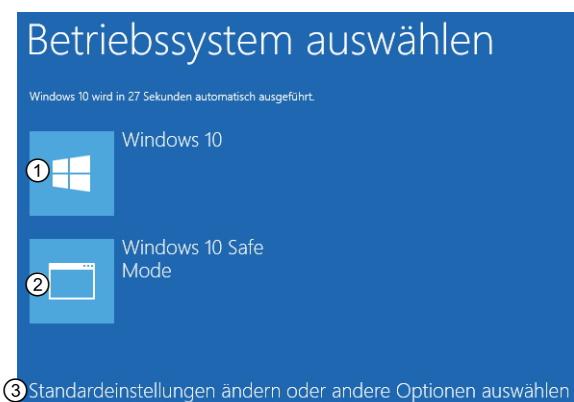
Auf vielen Systemen funktioniert das Unterbrechen des Systemstarts mit **[F8]** oder **[↑] [F8]** nicht zuverlässig. Auf diesen Systemen können Sie entweder wie oben beschrieben einen zweiten Booteintrag erstellen oder von einem Installationsmedium booten.

Mithilfe bestimmter Startoptionen können Sie wählen, auf welche Weise der Startvorgang fortgesetzt werden soll. So besteht die Möglichkeit, den Bootvorgang zu untersuchen und die Fehlerquelle zu erkennen (Startprotokollierung) oder Windows 10 in einem Standardmodus (abgesichert) zu starten, der verhindert, dass bestimmte benutzerdefinierte Einstellungen und Treiber verwendet werden, die Probleme verursachen könnten.

### Betriebssystem und weitere Optionen auswählen

Hier können Sie zwischen verschiedenen Booteinträgen wählen ①. (In der Abbildung ist der zweite Eintrag ② manuell hinzugefügt worden.)

Unter ③ können Sie die Starteinstellungen verändern und auf weiteren Bildschirmseiten andere Optionen auswählen.



### Optionen (Optionen 1)

Auf dem ersten Optionsbildschirm können Sie ...

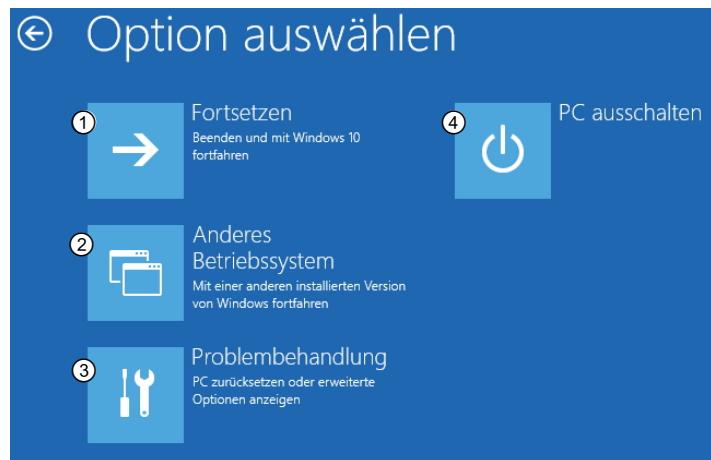
- ✓ die Dauer der Betriebssystemauswahl einstellen ①,
  - ✓ das Standardbetriebssystem auswählen ②,
  - ✓ weitere Optionen auswählen ③ oder
  - ✓ zur vorherigen Seite zurückkehren ④.
- Klicken Sie auf ③, um weitere Optionen auszuwählen.



## Weitere Optionen (Optionen 2)

Auf dem zweiten Optionsbildschirm können Sie ...

- ✓ Windows normal starten ①,
  - ✓ ein anderes Betriebssystem wählen ②,
  - ✓ die Problembehandlung starten ③ oder
  - ✓ den PC ausschalten ④.
- Klicken Sie auf ③, um die Problembehandlung zu starten.



## Problembehandlung

Auf dem Bildschirm *Problembehandlung* können Sie ...

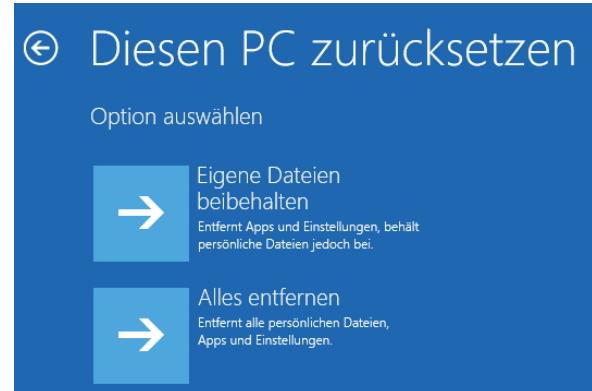
- ✓ den PC auf die Originaleinstellung zurücksetzen (Reset) ① oder
- ✓ die erweiterten Optionen aufrufen ②.



## PC zurücksetzen (Reset)

Beim Zurücksetzen bleiben Ihre Dateien erhalten. Alle Apps und Desktop-Anwendungen werden jedoch entfernt.

Bevor Sie einen PC zurücksetzen, sollten Sie versuchen, zu einem Systemwiederherstellungspunkt zurückzukehren, denn dabei bleiben auch alle installierten Apps und Desktop-Anwendungen erhalten. Wenn Sie über ein aktuelles Backup der Benutzerdateien verfügen, kann auch eine Systemabbildwiederherstellung geeigneter sein als ein Reset.



*Beim Reset werden alle Desktopanwendungen entfernt*

## Erweiterte Optionen

Auf dem Bildschirm *Erweiterte Optionen* können Sie ...

- ✓ zu einem bestehenden Systemwiederherstellungspunkt zurückkehren,
- ✓ ein bestehendes Systemabbild einspielen,
- ✓ eine automatische Reparatur durchführen,
- ✓ eine Eingabeaufforderung starten,
- ✓ Starteinstellungen ändern,
- ✓ zum vorherigen Build zurückkehren, wenn Sie Testerweiterungen in Windows 10 installieren.



*Erweiterte Optionen zu Systemstart und -wiederherstellung*

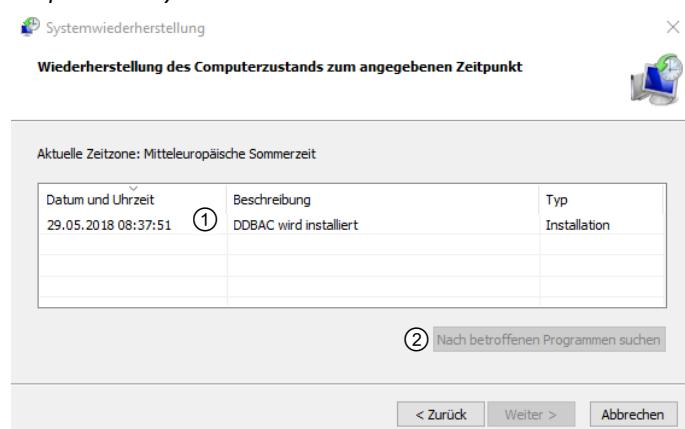
## Systemwiederherstellung

Windows 10 bietet die Möglichkeit, am Betriebssystem vorgenommene Änderungen, etwa die Installation neuer Hard- oder Software, wieder rückgängig zu machen. Dazu erstellt das System im Normalbetrieb sogenannte **Wiederherstellungspunkte**, für die jeweils die aktuelle Konfiguration abgespeichert wird. Wiederherstellungspunkte werden bei den meisten Änderungen der Systemkonfiguration automatisch erstellt, können aber auch manuell erzeugt werden. Falls nach einer Konfigurationsänderung Probleme auftreten, können Sie alle Änderungen am System bis zu einem Wiederherstellungspunkt rückgängig machen, ohne dabei Benutzerdaten zu beeinflussen.

Bei Windows 10 können Sie die Systemwiederherstellung über die erweiterten Einstellungen des Bootmenüs starten. Dazu können Sie eine Windows-DVD verwenden. Sie können aber auch eine Wiederherstellung durchführen, wenn Sie sich direkt in Windows 10 befinden. Dazu suchen Sie nach dem Tool *rstrui.exe*.

- Starten Sie Windows vom Installationsmedium, klicken Sie im Dialog *Windows Setup* auf *Weiter* und dann auf *Computerreparaturoptionen*.
- Klicken Sie auf *Problembehandlung - Erweiterte Optionen - System wiederherstellen*.
- Wählen Sie ein Benutzerkonto aus und melden Sie sich an.
- Klicken Sie auf *Weiter* und wählen Sie im Dialogfenster *Systemwiederherstellung* den Zeitpunkt, zu dem Sie Ihren Computer wiederherstellen wollen ①.
- Unter ② können Sie prüfen, welche Programme durch eine Wiederherstellung betroffen wären.
- Klicken Sie auf *Weiter* und dann auf *Fertig stellen*. Bestätigen Sie, dass Sie den Vorgang fortsetzen wollen.

Das System wird in den ausgewählten Zustand zurückversetzt.



*Einen Wiederherstellungspunkt auswählen*

## Systemimagewiederherstellung

In der Systemimagesicherung bzw. Systemabildsicherung können Sie ein bestehendes Systemabbild einspielen oder ein neues Systemabbild anfertigen. Ein **Systemabbild** umfasst den gesamten Zustand des Systems. Wenn Sie ein Abbild angefertigt haben, können Sie dieses jederzeit wieder zurückspielen. Damit ist das System wieder auf dem vorherigen Stand.

## Starteinstellungen

Nachdem Sie in den Windows-Starteinstellungen einen Neustart ausgelöst haben, erreichen Sie die Starteinstellungen. Diese entsprechen in etwa den erweiterten Startoptionen, die Sie bei älteren Windows-Versionen mit **[F8]** beim Systemstart aufrufen konnten.

Alle Einstellungen, die Sie hier vornehmen, gelten nur für diesen einen Systemstart.

Treffen Sie mit den Funktionstasten oder Nummerntasten Ihre Auswahl. Hier können Sie ...

- ✓ den Debugmodus aktivieren ①,
- ✓ die Startprotokollierung aktivieren ②,
- ✓ Windows mit niedriger Videoauflösung starten ③,
- ✓ Windows in drei verschiedenen abgesicherten Modi starten ④,
- ✓ zu Testzwecken beim nächsten Start einen unsigned Treiber zulassen ⑤,
- ✓ das Überprüfen von Treibern durch Windows Defender deaktivieren ⑥,
- ✓ den automatischen Neustart nach einem Systemfehler deaktivieren ⑦,
- ✓ die Computerdiagnose starten und Reparaturen durchführen ⑧ oder
- ✓ Windows mit **[←]** normal starten ⑨.

## Starteinstellungen

Drücken Sie eine Nummerntaste, um eine der Optionen unten auszuwählen:

Verwenden Sie die Nummerntasten oder die Funktionstasten F1-F9.

- 1) Debugmodus aktivieren ①
- 2) Startprotokollierung aktivieren ②
- 3) Video mit niedriger Auflösung aktivieren ③
- 4) Abgesicherten Modus aktivieren ④
- 5) Abgesicherten Modus mit Netzwerktreibern aktivieren
- 6) Abgesicherten Modus mit Eingabeaufforderung aktivieren
- 7) Erzwingen der Trebersignatur deaktivieren ⑤
- 8) Schutz des Antischadsoftware-Frühstarts deaktivieren ⑥
- 9) Automatischen Neustart bei Systemfehler deaktivieren ⑦

Drücken Sie zur Anzeige weiterer Optionen F10. ⑧

Drücken Sie die EINGABETASTE, um zum Betriebssystem zurückzukehren. ⑨

## Abgesicherten Modus verwenden

Der abgesicherte Modus ist auch bei Windows 10 vorhanden. Im abgesicherten Modus lädt Windows nur für den Start unbedingt notwendige Komponenten und Treiber. Sie können einen vor Auftreten des Startproblems installierten Gerätetreiber manuell deinstallieren und danach versuchen, Windows wieder normal zu starten. Sie haben die Auswahl zwischen dem abgesicherten Modus mit oder ohne Netzwerk und einer Eingabeaufforderung.

- Wählen Sie in den erweiterten Windows-Starteinstellungen mit **[F4]**, **[F5]** oder **[F6]** den abgesicherten Modus mit grafischer Oberfläche ohne Netzwerkanbindung ④, mit Netzwerkanbindung oder nur mit Eingabeaufforderung aus.
- Windows startet im abgesicherten Modus.
- Deinstallieren Sie die problematische Komponente mit dem Geräte-Manager.
- Beenden Sie Windows 10 im abgesicherten Modus und entfernen Sie die problematische Hardware aus dem Computer.
- Starten Sie Windows 10 und testen Sie, ob das System jetzt stabil läuft.

Anschließend können Sie versuchen, einen aktuellen Treiber für das Gerät oder weitergehende Informationen aus dem Internet zu erhalten.

Der abgesicherte Modus wird selten benötigt, denn die automatische Diagnose- und Reparaturfunktion von Windows 10 kann in vielen Fällen problematische Treiber selbstständig deaktivieren und entfernen.



## 5.1 Übung

### Windows 10 booten

**Übungsdatei: --**

**Ergebnisdatei: Uebung05\_E.pdf**

1. Mit welchem Befehlszeilentool bearbeiten Sie den Bootmanager?
2. Mit welchem Befehl kopieren Sie einen Booteintrag?

# 6 Anpassungen

## In diesem Kapitel erfahren Sie

- ✓ wie Sie die Arbeitsumgebung auf einer Workstation anpassen
- ✓ wie Sie Anwendungen und Windows-8/10-Apps installieren
- ✓ wie Sie die Einstellungen des Betriebssystems ändern
- ✓ wie Sie die Hardware-Profile erstellen
- ✓ wie Sie die Energiemanagement-Optionen verwalten
- ✓ wie Sie Cortana konfigurieren und nutzen

## 6.1 Workstation konfigurieren – die Systemsteuerung

### Überblick über die Systemsteuerung

- Klicken Sie mit der rechten Maustaste in die linke untere Bildschirmecke und wählen Sie im Schnellzugriffsmenü *Systemsteuerung*.  
Ab Windows 10, Version 1803 ist die Systemsteuerung nicht mehr direkt zu finden. Ab dieser Version suchen Sie nach „*systemsteuerung*“ im Suchfeld des Startmenüs. Microsoft integriert immer mehr Funktionen aus der Systemsteuerung in die Einstellungs-App von Windows 10, die Sie über das Startmenü erreichen.



Neben der Systemsteuerung nehmen Sie fast alle Konfigurationen in Windows 10 über die neue Einstellungs-App vor. Diese finden Sie über dem Menüpunkt *Einstellungen* im Startmenü oder in der entsprechenden Schaltfläche im Explorer. Alternativ verwenden Sie

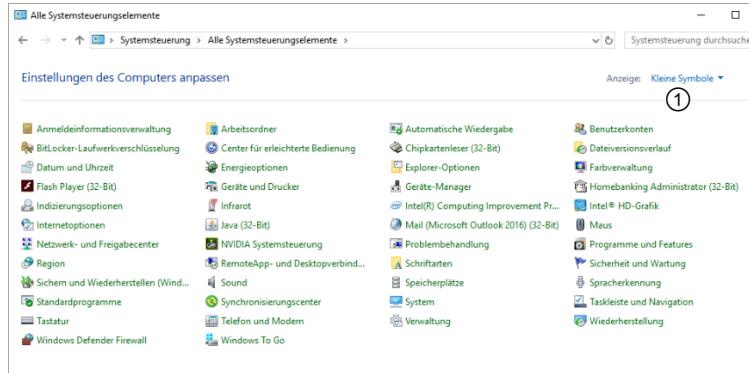
Über die Systemsteuerung können Sie viele Funktionen zur Konfiguration eines Computers aufrufen. Windows 10 unterteilt genau wie Windows 7/8/8.1 die Systemsteuerung in acht Kategorien (grüne Schrift) mit zahlreichen Unterkategorien (blaue Schrift). Wenn Sie auf eine grüne Kategorie klicken, gelangen Sie auf eine Überblickseite, ein Klick auf die blauen Links führt Sie direkt zu der jeweiligen Einstellung.

 <b>System und Sicherheit</b> Status des Computers überprüfen Sicherungskopien von Dateien mit dem Dateiversionsverlauf speichern Sichern und Wiederherstellen (Windows 7)	Hier finden Sie das Wartungscenter, Windows Defender Firewall, System-eigenschaften, Windows Update, Energieoptionen, Dateisicherung und Systemabbilder, BitLocker-Laufwerkverschlüsselung, Festplattenverwaltung und Einstellungen für Software von Drittherstellern, wie z. B. Adobe Flash Player.
 <b>Benutzerkonten</b> 	Hier können Sie lokale Benutzerkonten verwalten. Mit der Anmelde-informationenverwaltung erhalten Sie einen zentralen Passwortmanager für Windows-Netzwerke und das Internet.
 <b>Netzwerk und Internet</b> 	Hier finden Sie das Netzwerk- und Freigabecenter, die Internetoptionen und weitere Netzwerkeinstellungen.
 <b>Darstellung und Anpassung</b>	Hier können Sie Anzeigeeinstellungen vornehmen, Explorer-Ordneroptionen und Taskleiste steuern und an Ihre Anforderungen anpassen. Einstellungen für die Windows-10-Oberfläche sind hier nicht möglich. Die meisten Einstellungen sind mittlerweile in die Windows-10-Einstellungs-App gewandert, zum Beispiel die Einstellungen zur Auflösung. Diese erreichen Sie auch über das Kontextmenü, wenn Sie auf den Desktop klicken.
 <b>Hardware und Sound</b> 	Hier richten Sie Geräte, Drucker und Sounds ein, außerdem können Sie die automatische Wiedergabe (Autoplay), die Energieoptionen und deren Anzeige einstellen.

 Zeit und Region Datums-, Uhrzeit- oder Zahlenformat ändern	Hier können Sie Datum, Uhrzeit, Eingabe- und Systemsprache sowie die Region einstellen.
 Programme Programm deinstallieren	Hier können Sie Windows-Funktionen aktivieren, Programme deinstallieren und reparieren sowie Standardprogramme einstellen.
 Erleichterte Bedienung Einstellungen empfehlen lassen Visuelle Darstellung des Bildschirms optimieren	Hier finden Sie die Einstellungen für die Spracherkennung und Hilfen, die die Bedienung des Computers bei körperlichen Einschränkungen erleichtern.

Windows 10 kann die Systemsteuerung auch in der klassischen Listenansicht darstellen.

- ▶ Um die Darstellung auf Listenansicht umzuschalten, klicken Sie auf den Link neben Anzeige ① und wählen Sie **Kleine Symbole**.
- ▶ Geben Sie im Suchfeld der Systemsteuerung ein kleines L ein, also l, sehen Sie in der Liste alle verfügbaren Einstellungen.



Listenansicht der Systemsteuerung

## Netzwerkeinstellungen anpassen

Klicken Sie mit der rechten Maustaste auf das Netzwerksymbol in der Taskleiste, können Sie die Netzwerkeinstellungen aus der Windows-10-Einstellungs-App aufrufen. In der Systemsteuerung rufen Sie das **Netzwerk- und Freigabecenter** auf, wenn Sie erweiterte Netzwerkeinstellungen vornehmen wollen. Hier sehen Sie bei **Aktive Netzwerke anzeigen** auch den Netzwerktyp. Ist hier **Öffentliches Netzwerk** hinterlegt, funktioniert der Rechner kaum im internen Netzwerk. Sie können die Einstellungen aber jederzeit ändern:

- ▶ Rufen Sie über die Startschaltfläche die Einstellungen auf.
- ▶ Klicken Sie auf **Netzwerk und Internet**.
- ▶ Klicken Sie auf **Verbindungseigenschaften ändern**. Hier stellen Sie das Netzwerkprofil ein.

In der Registry können Sie diesen Wert ebenfalls ändern:

- ▶ Öffnen Sie **regedit**.
- ▶ Navigieren Sie zu **HKLM\Software\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles\<Name des Profils>**.
- ▶ Ändern Sie den Wert des DWORD-Wertes **Category** ab:
  - ✓ 0 – Öffentliches Netzwerk
  - ✓ 1 – Privates Netzwerk
  - ✓ 2 – Arbeitsplatznetzwerk (Active Directory-Domäne)

## Microsoft-Konto in lokales Konto ändern und umgekehrt

Wollen Sie kein Microsoft-Konto mehr verwenden, haben Sie in Windows 10 die Möglichkeit, ohne Verlust von Daten oder Einstellungen zu einem lokalen Konto zu wechseln. Dazu gehen Sie folgendermaßen vor:

- ▶ Drücken Sie  ①.
- ▶ Wählen Sie im Fenster **Einstellungen** die Kategorie **Konten**.
- ▶ Klicken Sie unterhalb der E-Mail-Adresse Ihres Microsoft-Kontos auf **Stattdessen mit einem lokalen Konto anmelden**.
- ▶ Geben Sie das Kennwort für das Microsoft-Konto ein.
- ▶ Geben Sie jetzt den Benutzernamen, das Kennwort und einen Kennworthinweis für das neue lokale Konto ein.
- ▶ Melden Sie sich ab und neu an.

## 6.2 Desktop anpassen

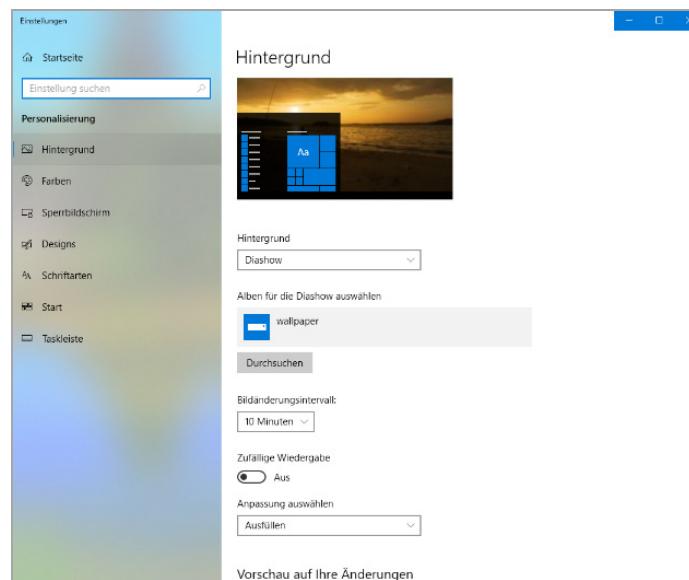
### Benutzereinstellungen

Die Einstellungen des Desktops sind benutzerspezifisch und werden im Benutzerprofil gespeichert. Das Benutzerprofil liegt standardmäßig auf der Startpartition unter *Benutzer* in einem Unterordner mit dem Benutzerkontonamen. Um auch den versteckten Ordner *AppData* sehen zu können, müssen Sie im Explorer unter *Ansicht - Optionen* im Register *Ansicht* die Darstellung der versteckten Dateien erlauben.

### Desktopfarben und Design einstellen

Bei Windows 10 gibt es keine klassische Ansicht mehr, und auch das Aero-Design mit seinen Transparenz-, Schatten- und 3D-Effekten ist nicht mehr verfügbar. Alle Fensterelemente sind nun vollflächig einfarbig und die Fensterecken sind nicht mehr abgerundet. Sie können nur noch zwischen verschiedenen Farbschemas auswählen.

- ▶ Klicken Sie mit der rechten Maustaste auf den Desktop und klicken Sie im Kontextmenü auf *Anpassen*.
- ▶ Wählen Sie im neuen Fenster aus, welche Bereiche in Windows 10 Sie anpassen wollen. Sie können auf der linken Seite die Optionen wechseln und danach rechts die entsprechenden Einstellungen vornehmen.



Windows 10 an die eigenen Bedürfnisse anpassen

## 6.3 Anzeigeeigenschaften einstellen

### Bildschirmdarstellung anpassen

Da viele Benutzer täglich mehrere Stunden auf den Bildschirm schauen müssen, ist es wichtig, dass Sie für jeden Benutzer die Darstellung nach seinem persönlichen Geschmack anpassen.

Aus ergonomischer Sicht sollte die Darstellung auf einem Arbeitsplatzmonitor in Relation zur Monitorentfernung nicht zu fein aufgelöst sein und das Display muss entspiegelt sein. Der Monitor sollte der aktuellen TCO-Norm entsprechen. Die Leuchtkraft sollte passend zum Arbeitsplatz regelbar sein; wünschenswert ist hier eine automatische Anpassung an wechselnde Lichtverhältnisse. Für Bildbearbeitung werden besondere Ansprüche an die Farbneutralität gestellt.

Auch alle anderen ergonomischen und arbeitsrechtlichen Aspekte eines Bildschirmarbeitsplatzes müssen berücksichtigt werden. Dazu gehört auch die obligatorische fünfminütige Bildschirmpause pro Stunde.

Die Bildschirmdarstellung ist abhängig von mehreren Faktoren, wovon einige in Windows beeinflusst werden können, andere hingegen nur am Monitor oder durch die Wahl eines anderen Anzeigegerätes:

Bildschirmauflösung	Heutige Flachbildschirme sollten Sie wenn möglich in ihrer tatsächlichen (nativen) Auflösung betreiben, sonst wird die Darstellung unscharf. Falls Sie die Einstellung dennoch ändern, werden bei einer kleinen Auflösung des Bildschirms (minimal 1024 × 768 Bildschirmpunkte) die Informationen am Monitor zwar größer angezeigt, gleichzeitig passen jedoch weniger Elemente auf den Desktop. Bei einer größeren Auflösung (z. B. 1920 × 1200) haben mehr Elemente Platz auf dem Bildschirm, die einzelnen Fensterelemente und die Schrift können jedoch so klein werden, dass sie kaum noch zu lesen sind. Sie können dies ausgleichen, indem Sie die Schrift- und Elementgröße erhöhen.
DPI	Wie fein eine Darstellung auf dem Bildschirm aufgelöst ist, wird durch die Anzahl der Bildpunkte (Pixel) auf einer bestimmten Fläche bestimmt. Bei Monitoren ist dafür DPI (Dots per Inch, Punkte pro Zoll) gebräuchlich. Für Flachbildschirme gilt ein Wert zwischen 90 und 120 DPI als ideal. Dies ist zum Beispiel bei 19"-Monitoren mit 1280 × 1024 oder 23"-Monitoren mit 1920 × 1200 der Fall. Notebookdisplays und einige besonders fein auflösende Monitore liegen zum Teil erheblich darüber, ein 15,4"-Notebookdisplay mit 1920 × 1200 hat z. B. knapp 150 DPI und die Windows-Darstellung wird von vielen Personen als zu fein empfunden.
Farben	Je mehr Farben (Farbtiefe) verwendet werden, desto naturgetreuer wird die Farbdarstellung z. B. von Bildern. Standardfarbtiefe sind 32 Bit.
Bildschirmfrequenz (Bildwiederholrate)	Die Bildschirmfrequenz gibt Auskunft darüber, wie oft die Darstellung auf dem Bildschirm erneuert wird. Bei den veralteten Röhrenmonitoren musste noch eine Frequenz von mindestens 75 Hertz für flimmerfreie Darstellung sorgen, bei den heutigen flimmerfreien Flachbildschirmen liegt die Frequenz bei 60 Hz und muss selten verändert werden. Bei Windows 10 wird sie <b>Bildaktualisierungsrate</b> genannt.
Leuchtdichte	Die Leuchtdichte wird in Candela (cd) pro m <sup>2</sup> angegeben und oft als Displayhelligkeit bezeichnet. Je nach Umgebungshelligkeit benötigt ein Bildschirm zwischen 60 und 400 cd/m <sup>2</sup> , um angenehm lesbar zu bleiben. Spiegelnde Displayoberflächen erfordern im direkten Sonnenlicht enorme Leuchtdichten, um die Reflexionen zu überstrahlen. Die Leuchtdichte lässt sich über das Einstellungsmenü des Monitors, Softwareeinstellungen oder automatisch über Lichtsensoren regeln.
Farbprofile und Farbtemperatur	Neben den Einstellungen am Monitor selbst können in Windows Farbprofile für den Monitor hinterlegt werden, die für eine möglichst neutrale Farbdarstellung sorgen. Für viele Monitore wird automatisch das richtige Profil ausgewählt. Sie können die Farbprofile aber auch über <i>Anzeigeeinstellungen - Erweiterte Anzeigeeinstellungen - Farbkalibrierung</i> wechseln.

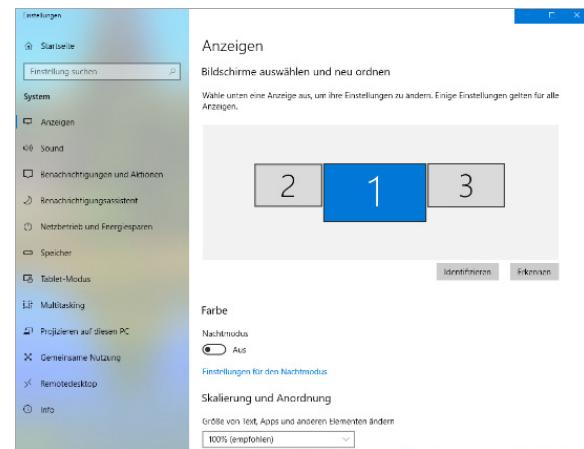
### Bildschirmeinstellungen vornehmen

In Windows 10 können Sie mehrere Bildschirmeinstellungen vornehmen. Dazu müssen Sie den Dialog *Bildschirmauflösung* öffnen:

- ▶ Klicken Sie mit der rechten Maustaste auf eine freie Stelle des Desktops und wählen Sie den Kontextmenüpunkt *Anzeigeeinstellungen*.

## Bildschirmauflösung ändern

- Klicken Sie auf das Feld im Bereich *Auflösung*. Hier können Sie die gewünschte Auflösung auswählen.



Anpassen der Auflösung für Monitore

## Bildschirmhelligkeit einstellen

Bei Notebooks und Monitoren mit Helligkeitssensor lässt sich die Helligkeit auch in Windows einstellen. Diese Einstellung finden Sie im Info-Center bei den Schnelleinstellungen im unteren Bereich oder indem Sie auf das Akku-Symbol im Traybereich neben der Uhr klicken. Tippen Sie auf das Helligkeits-Symbol, können Sie die Helligkeit in Stufen einstellen. In den erweiterten Einstellungen von Energiesparplänen finden Sie diese Einstellung ebenfalls, wie bereits in Windows 8.1.

## Tablet-Modus korrekt konfigurieren

Nutzen Sie einen Hybrid-PC oder ein Notebook mit Touch-Bedienung, können Sie im Info-Center zwischen dem Desktop-Modus und dem Tablet-Modus hin- und herwechseln. Sie können außerdem festlegen, wie sich der Rechner bezüglich des Neustarts verhalten soll, wenn Sie den Tablet-Modus oder Desktop-Modus aktiviert haben. Die Konfiguration dazu nehmen Sie über *Einstellungen - System - Tablet-Modus* vor. Hier können Sie ebenfalls den Tablet-Modus aktivieren oder deaktivieren. Alternativ können Sie hier festlegen, wie sich der Rechner bei der Anmeldung verhalten soll und ob Windows automatisch zwischen Tablet- und Desktop-Modus wechselt darf, wenn Sie Maus und Tastatur vom Rechner entfernen oder verbinden.

## Einstellungen eines weiteren Monitors anpassen

Windows 10 unterstützt den **Multimonitorbetrieb**. Wenn an Ihrem Rechner zwei (oder mehr) Monitore von Windows erkannt wurden, wird dies beim Aufrufen der *Anzeigeeinstellungen* angezeigt. Sie sehen im Bild oben rechts, wie diese Optionen aussehen.

- Klicken Sie auf den Monitor, dessen Einstellungen Sie anpassen wollen
- Sie können den Bildschirm mit der Schaltfläche *Identifizieren* erkennen, dann erscheint auf jedem Monitor die Nummer, die Windows ihm zugewiesen hat.

Jeder Monitor kann in Windows 10 ein eigenes Hintergrundbild verwenden. Mit oder verschieben Sie das aktuell aktivierte Fenster auf den anderen Monitor und wieder zurück. Sie erreichen die Einstellungen für die Anzeige über die Eingabe von `desk.cpl` im Suchfeld der Taskleiste.

- Ziehen Sie zuerst die Monitore per Drag & Drop in die richtige Reihenfolge, und stellen Sie für Monitore die jeweils korrekte Auflösung ein.
- Markieren Sie im Anschluss den Monitor, auf dem Sie das Startmenü und die Taskleiste anzeigen wollen, und aktivieren Sie das Kontrollkästchen *Diese Anzeige als Hauptanzeige verwenden*. Dieses Kontrollkästchen wird nicht angezeigt, wenn der aktive Monitor bereits die Hauptanzeige ist.
- ✓ Mit können Sie die Anzeige der beiden Bildschirme anpassen.
- ✓ Auf dem Desktop lassen sich über das Kontextmenü der Taskleiste im unteren Bereich weitere Einstellungen vornehmen. Sie haben z.B. hier die Möglichkeit, die Taskleiste auch auf dem zweiten Bildschirm anzuzeigen.

## Desktopsymbole und Anzeige für kleine Displays und Tablet-PCs anpassen

Viele Anwender wollen nicht die großen Symbole auf dem Desktop nutzen, die in Windows 10 standardmäßig eingestellt sind. Sie können die Größe der Symbole auf dem Desktop anpassen, indem Sie mit der rechten Maustaste auf den Desktop klicken und im daraufhin geöffneten Kontextmenü einen geeigneten Eintrag im Untermenü *Ansicht* auswählen.

Sie können die Größe der Desktopsymbole mit der Maus stufenlos anpassen:

- ✓ Klicken Sie dazu ein beliebiges Symbol auf dem Desktop an oder klicken Sie mit der linken Maustaste auf einen leeren Bereich des Desktops, und halten Sie dann die **Strg**-Taste gedrückt.
- ✓ Mit dem Scrollrad der Maus lässt sich die Größe der Symbole stufenlos anpassen. Dies funktioniert auch in fast allen anderen Fenstern in Windows 10, auch innerhalb von Ordnern.

Sie können auch per Rechtsklick auf den Desktop und die Auswahl von *Anzeigeeinstellungen* die Größe der Symbole und Schriftart anpassen, ohne dass darunter die Auflösung leidet:

- ▶ Klicken Sie rechts unten im Fenster auf den Link *Erweiterte Anzeigeeinstellungen*.  
Die Skalierungskonfiguration finden Sie über *Erweiterte Skalierungseinstellungen*.
- ▶ Klicken Sie auf *Benutzerdefinierte Skalierung*.
- ▶ Aktivieren Sie die gewünschte Ansicht.
- ▶ Nach der Änderung müssen Sie sich meistens ab- und neu anmelden.

## Anzeige der Schriftarten und der Farben verbessern

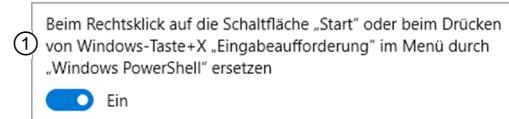
Windows 10 verfügt über zwei Tools, mit denen Sie die Anzeige der Schriftarten und der Farben verbessern können. Geben Sie im Startmenü `cttune` ein und folgen Sie den Schritten des Assistenten, um die Anzeige von Schriftarten zu verbessern. Setzen Sie mehrere Monitore ein, können Sie die Anzeige für alle Monitore verbessern.

Über den Assistenten zeigt Ihnen Windows verschiedene Fenster an. Sie müssen auswählen, in welchem Fenster die Anzeige am besten ist, damit Windows weiß, wie die Anzeige zukünftig erfolgen soll. Auf die gleiche Weise können Sie auch die Farbeinstellungen verbessern. Dazu geben Sie auf der Startseite den Befehl `dccw` ein und folgen den Schritten des Assistenten.

## Einstellungsmöglichkeiten für Bildschirmecken und PowerShell nutzen

Rufen Sie in Windows 10 über das Kontextmenü der Taskleiste die *Taskleisteneinstellungen* auf.

Die Option ① ersetzt die Eingabeaufforderung über das Kontextmenü der Start-Schaltfläche mit der Möglichkeit, die PowerShell zu starten.



Sie können aber auch in der PowerShell Befehle aus der Eingabeaufforderung nutzen. In der PowerShell können Sie mit `cmd` zur Eingabeaufforderung wechseln und von der Eingabeaufforderung mit `powershell` in die PowerShell. Mit `ise` rufen Sie die grafische Oberfläche der PowerShell auf.

## Schnellzugriff im Datei-Explorer konfigurieren

Im Datei-Explorer finden Sie oben links den neuen Bereich *Schnellzugriff*. Hier können Sie einige Favoriten ablegen. Windows 10 fügt hier auch **automatisch** Verknüpfungen zu häufig geöffneten Verzeichnissen hinzu. Sie können festlegen, dass Windows 10 keine automatische Pflege dieses Bereiches vornimmt. Dazu klicken Sie mit der rechten Maustaste auf *Schnellzugriff* und rufen *Optionen* auf.

Im Bereich *Datenschutz* finden Sie die beiden Optionen:

- ✓ *Zuletzt verwendete Dateien im Schnellzugriff anzeigen*
- ✓ *Häufig verwendete Ordner im Schnellzugriff anzeigen*

Deaktivieren Sie diese Optionen, erscheinen keine automatischen Einträge mehr. Außerdem können Sie hier auch den Verlauf des Explorers löschen lassen. Über die Option *Datei-Explorer öffnen für* legen Sie fest, welche Laufwerke der Explorer standardmäßig anzeigen soll. Hier ist die Option *Dieser PC* empfehlenswert.

### Startmenü anpassen

Auf der **linken** Seite des Startmenüs finden Sie häufig verwendete Programme und die *Alle Apps*-Ansicht mit allen installierten Programmen.

Auf der **rechten** Seite sind die Kacheln zu sehen, so wie in der Startseite von Windows 8/8.1. Über das Kontextmenü der Kacheln können Sie diese vom Startmenü entfernen, deren Größe anpassen oder die Live-Kachelfunktion aktivieren und deaktivieren. Haben Sie alle Kacheln vom Startmenü entfernt, können Sie dieses am Rand an die gewünschte Größe anpassen.

## 6.4 Anwendungsprogramme installieren

### Software von Wechseldatenträger mit Autoplay-Funktion installieren

Sobald Sie einen Datenträger einlegen oder anschließen, wird er vom System automatisch untersucht und eine Meldung im Windows-10-Look wird angezeigt. Ein Klick darauf zeigt Ihnen eine Auswahl von Aktionen, die durchgeführt werden können, unter anderem auch die vom Herausgeber voreingestellte Autoplay-Aktion *autorun.exe ausführen*.

### Installation von einem beliebigen Ort

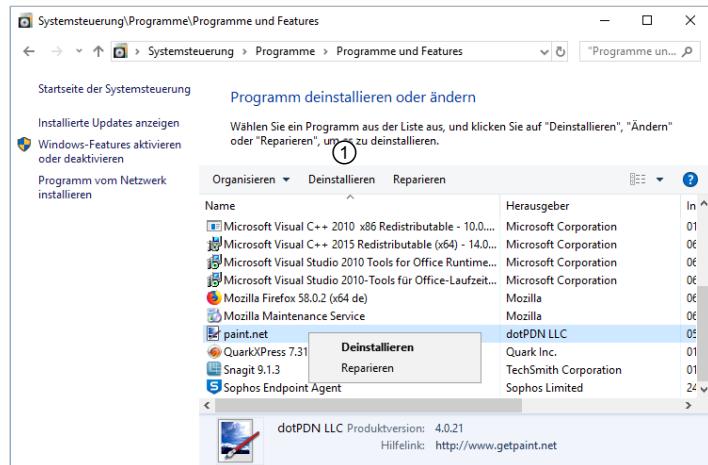
Falls Sie nicht über einen Datenträger mit Autostart-Funktion verfügen, gehen Sie wie folgt vor:

- Starten Sie mit  den Explorer und navigieren Sie zu dem Laufwerk und Ordner, worin sich die Installationsdateien befinden.
- Stellen Sie sicher, dass im Menüband des Explorers auf der Registerkarte *Ansicht* im Bereich *Ein-/ausblenden* die Option *Dateinamenerweiterungen* aktiviert ist.
- Suchen Sie nach ausführbaren Dateien mit Namen wie *Setup* oder *Install* mit der Endung *\*.exe* oder *\*.msi*.

Alternativ können Sie Treiber, die nicht über ein Setup-Programm verfügen, über das Kontextmenü der INF-Dateien installieren. Die Option dazu finden Sie über das Kontextmenü der entsprechenden Datei.

## Programme deinstallieren oder ändern

- ▶ Suchen Sie im Startmenü nach `appwiz.cpl` oder klicken Sie auf den Eintrag `Systemsteuerung\Alle Systemsteuerungselemente\Programme und Features`.
- Die Systemsteuerung starten Sie ab Windows 10, Version 1803 nicht mehr über das Kontextmenü des Startmenüs, sondern durch die Eingabe von „`systemsteuerung`“ im Suchfeld des Startmenüs.
- ▶ Markieren Sie in der Liste das entsprechende Programm.  
Abhängig vom Programm werden z. B. die Optionen `Deinstallieren` und `Ändern` angezeigt.
- ▶ Klicken Sie auf gewünschte Option, z. B. `Deinstallieren` ①.
- ▶ Bestätigen Sie in den programm-abhängigen Dialogen die Deinstallation.



Programme entfernen bzw. ändern

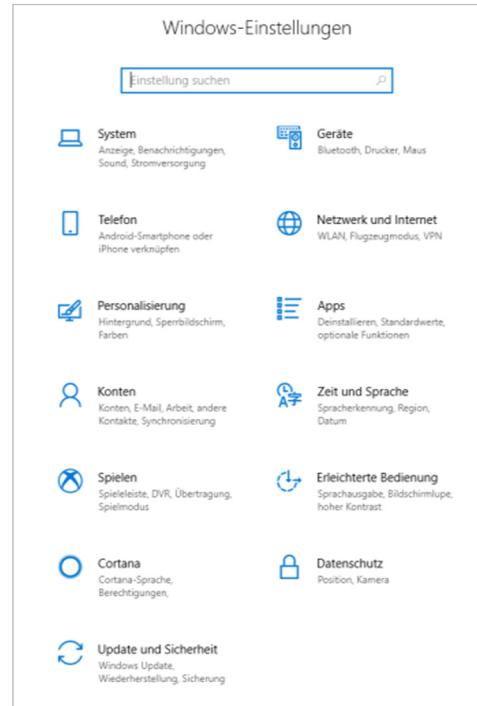
Der Ablauf der Deinstallation ist abhängig vom jeweiligen Programm. Einige Programme bieten Schaltflächen wie `Ändern`, `Reparieren` und `Deinstallieren` und fragen, ob Sie die Programmeinstellungen und -daten behalten wollen. Einige Programme beginnen sofort nach dem Klick auf `Deinstallieren` mit dem Entfernen der Software und löschen **ohne Warnung** sämtliche Daten. Bei wichtigen Daten sollten Sie daher vor einer Deinstallation sicherheitshalber eine Kopie der wichtigen Anwendungseinstellungen und -dateien anfertigen.



## 6.5 Windows-10-Einstellungen vornehmen

Die meisten Einstellungen von Windows 10 lassen sich auch über den neuen Bereich *Einstellungen* der Windows-10-Oberfläche vornehmen. Sie finden den Bereich direkt im Startmenü. Microsoft verlegt immer mehr Einstellungen aus der Systemsteuerung in die Einstellungs-Apps von Windows 10.

- ✓ Sie erreichen die Einstellungen am schnellsten, indem Sie betätigten.
- ✓ In den Einstellungen gibt es mehrere Unterkategorien. Hier verschiebt Microsoft auch bei Updates die verschiedenen Menüpunkte teilweise neu. Außerdem erscheinen bei jedem Update neue Funktionen, die aus der Systemsteuerung übernommen wurde.
- ✓ Unter *Personalisierung* finden Sie Einstellungen zum Sperr- und Startbildschirm sowie zum Benutzerprofilbild.
- ✓ Unter *Konten* können Sie weitere Benutzer hinzufügen und zwischen lokaler Anmeldung und einem Microsoft-Konto wechseln.
- ✓ Über das Suchfeld oben finden Sie die Einstellungen am schnellsten.



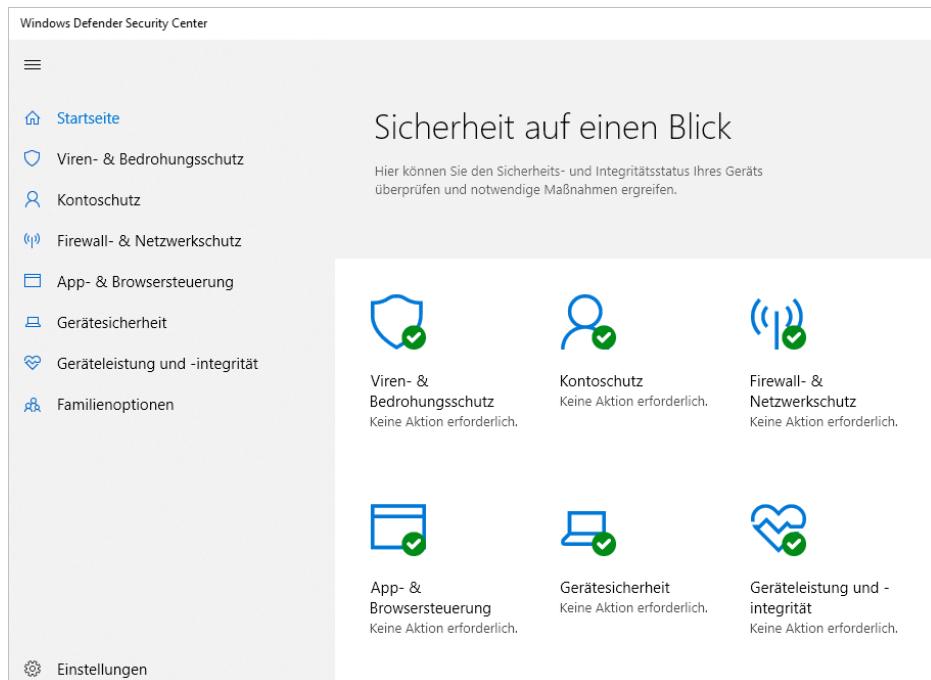
## Neue Windows-10-Einstellungen verstehen und anpassen

In Windows 10 gibt es zahlreiche Einstellungen, die sich von Windows 8/8.1 unterscheiden: Ziehen Sie im Startmenü Kacheln per Drag & Drop an die gewünschte Position, um sie nach Ihren Wünschen anzutragen. Klicken Sie mit der rechten Maustaste auf eine App, können Sie deren Größe jetzt in vier Stufen ändern. Außerdem können Sie über das Startmenü die Gruppen umbenennen und Kacheln im Startmenü zu neuen Gruppen zusammenfassen.

## Windows Defender Security Center für mehr Sicherheit nutzen

In der Einstellungs-App von Windows 10 kann mit der Schaltfläche *Windows Defender Security Center öffnen* im Bereich *Update und Sicherheit\Windows-Sicherheit*. Alternativ steht das Center auch als App im Startmenü zur Verfügung.

Hier sind auf einen Blick die wichtigsten Sicherheitsinformationen für Windows 10 zu erkennen. Im oberen Bereich zeigt Windows 10 das Datum der Definitionsdateien des Virensenders an sowie das Datum der letzten Überprüfung. Über *Viren- & Bedrohungsschutz* kann eine schnelle oder gründliche Überprüfung gestartet werden. Außerdem ist hier zu sehen, ob Bedrohungen gefunden wurden. Auch Einstellungen sind hier überprüfbar.



## Einstellungen synchronisieren über die Cloud

Bei der Verwendung eines Microsoft-Kontos kann Windows über das Internet automatisch Ihre Windows-Einstellungen und installierten Windows-Apps mit jedem Computer abgleichen, an dem Sie sich anmelden. Dadurch finden Sie überall die gleiche Windows-10-Umgebung vor, egal, welches Gerät Sie benutzen. Diese neue Funktion ist vor allem für Privatbenutzer interessant, die die Windows-10-Oberfläche und Windows-Apps verwenden. Um die Synchronisierung zu nutzen, müssen Sie die Optionen in den *Einstellungen* unter *Konten - Einstellungen synchronisieren* einschalten.

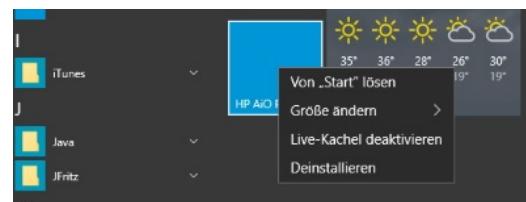
## Windows-10-Apps hinzufügen und entfernen

### Apps aus dem Store herunterladen

Windows-Apps lassen sich ausschließlich über den **Store** hinzufügen. Um den Store benutzen zu können, müssen Sie sich mit einem Microsoft-Konto anmelden. Der Store bietet eine Vielzahl kostenloser oder kommerzieller Apps an, die in Bereiche wie z. B. Spiele, Unterhaltungsmedien, Fotos, Tools und Sicherheit unterteilt sind. Aber auch Tools für Administratoren, zum Beispiel für den Remotedesktop, sind hier zu finden.

## Apps entfernen oder deinstallieren

Um eine Windows-App zu entfernen, klicken Sie mit der rechten Maustaste auf die App. Die Einträge im Kontextmenü sind abhängig von der App. Hier können Sie die App vom Startbildschirm lösen oder deinstallieren. Im gleichen Kontextmenü können Sie auch die Größe der Kachel umschalten und die Live-Inhalte der Kachel deaktivieren.

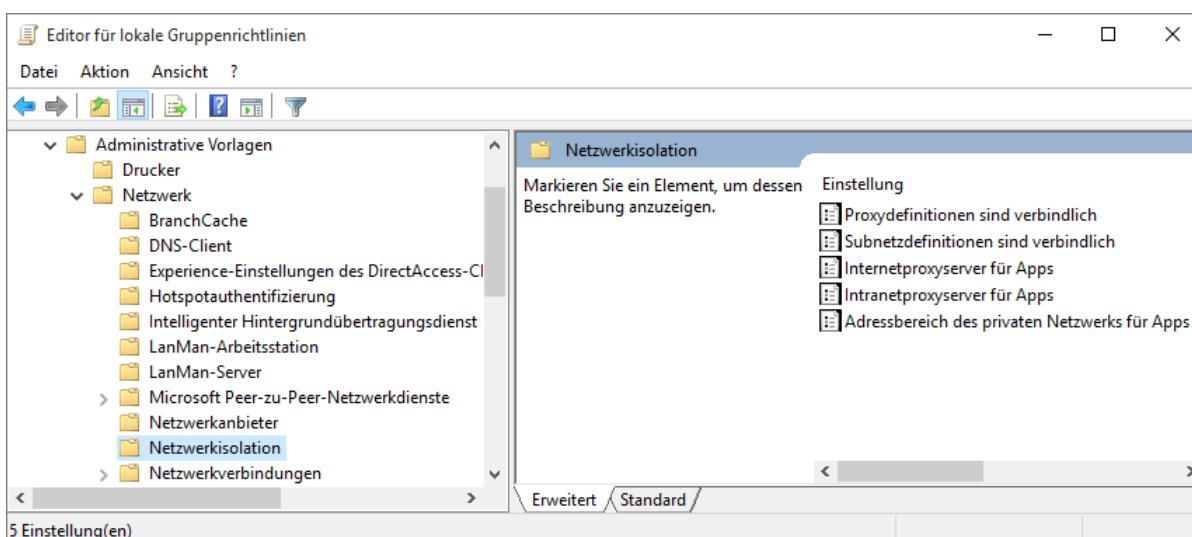


App entfernen, deinstallieren oder deaktivieren

## Proxy für Windows-10-Apps und den Store verwenden

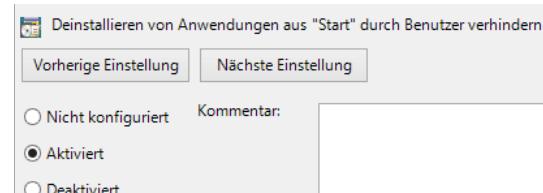
In manchen Umgebungen ist das Internet nicht direkt über die IP-Einstellungen auf dem Rechner erreichbar, sondern über einen Proxyserver. Standardmäßig erreichen Windows-10-Apps das Internet nur direkt. Wenn Sie einen Proxyserver einsetzen, müssen Sie im System Änderungen vornehmen, damit die Apps eine Verbindung mit dem Internet herstellen können.

Da in solchen Umgebungen normalerweise Windows 10 Pro oder Enterprise im Einsatz sind, können Sie die Einstellungen über Gruppenrichtlinien setzen. Öffnen Sie die Verwaltung der Richtlinien mit `gpedit.msc` und navigieren Sie zu *Computerkonfiguration - Administrative Vorlagen - Netzwerk - Netzwerkisolation*. Auf der rechten Seite finden Sie die Einstellungen, um die Apps über einen Proxy mit dem Internet zu verbinden. Aktivieren Sie die Einstellung für den Proxy und geben Sie die URL und den Port ein, auf dem der Proxy auf Anfragen wartet.



## Deinstallation von Apps verhindern

Über die Richtlinien in Windows 10 Pro und Enterprise können Sie verhindern, dass Anwender Apps deinstallieren können. Rufen Sie dazu `gpedit.msc` auf. Navigieren Sie zu *Benutzerkonfiguration - Administrative Vorlagen - Startmenü und Taskleiste*.



Öffnen Sie auf der rechten Seite die Einstellung *Deinstallieren von Anwendungen aus "Start" durch Benutzer verhindern*. Aktivieren Sie diese Option, können Anwender keine Apps mehr deinstallieren.

## Apps oder Updates aus dem Windows Store installieren

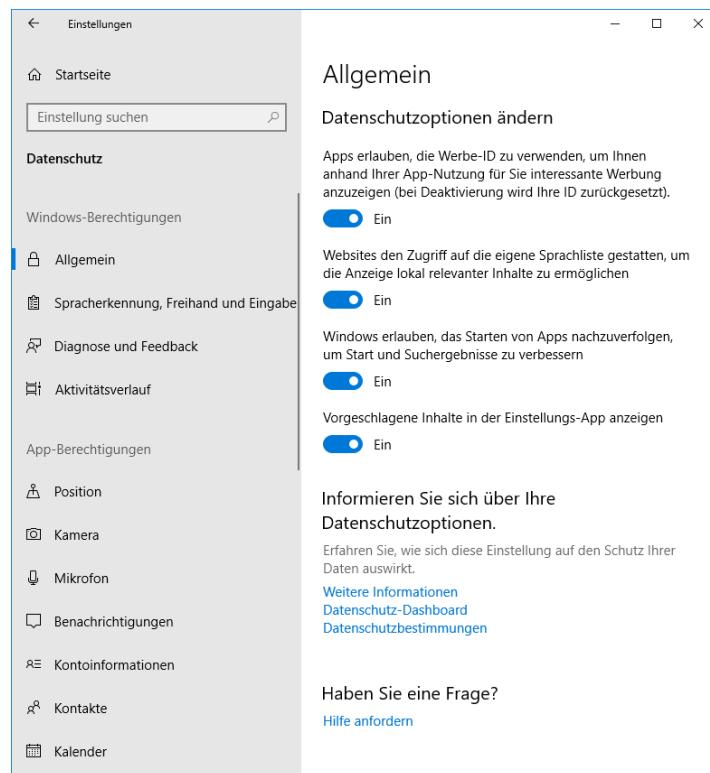
Um Apps aus dem Windows Store zu installieren, rufen Sie den Store über das Startmenü auf. Anschließend stellt der PC eine Verbindung zum Internet her. Um eine App zu installieren, klicken Sie auf deren Kachel und wählen anschließend *Installieren* aus. Nach kurzer Zeit erhalten Sie die Information, dass die App installiert ist. Sie erscheint anschließend auf der Startseite.

Wie für Windows selbst, gibt es auch für Apps regelmäßig Updates. Diese werden aber nicht über Windows Update installiert, sondern die Updates werden über den Store automatisch installiert. Sie sehen im Startmenü über die Verknüpfung des App-Stores oder in den Einstellungen des Windows Stores, wie viele Updates für Ihre Apps zur Verfügung stehen.

## Datenschutz in Windows 10

Das zentrale Instrument, um den Datenschutz in Windows 10 anzupassen, besteht darin, dass Sie in der Einstellungs-App zum Bereich *Datenschutz* wechseln. Hier stehen zahlreiche Optionen zur Verfügung. Mit Windows 10, Version 1803 hat Microsoft an dieser Stelle, aber auch in anderen Bereichen von Windows 10 Möglichkeiten integriert, um den Datenschutz zumindest etwas zu verbessern.

In der Einstellungs-App von Windows 10, Version 1803 stehen über *Datenschutz* die neuen Menüpunkte *Dokumente*, *Bilder*, *Kamera* und *Dateisystem* zur Verfügung. Hierüber können Sie festlegen, welche Apps und Betriebssystemkomponenten Zugriff auf diese Funktionen und Daten in Windows 10 erhalten sollen.



Mit Windows 10, Version 1803 führt Microsoft die **Timeline** ein. Dabei handelt es sich um eine Funktion, die Aktivitäten und Aktionen in Dateien in der Vergangenheit bis zu 30 Tage wiederherstellen kann. Die Timeline wird über das Icon in der Taskbar oder mit aufgerufen. Microsoft hat in der Einstellungs-Apps im Bereich *Datenschutz* bei *Aktivitätsverlauf* die Funktionen integriert, die Timeline zu löschen und Einstellungen bezüglich der Timeline vorzugeben.

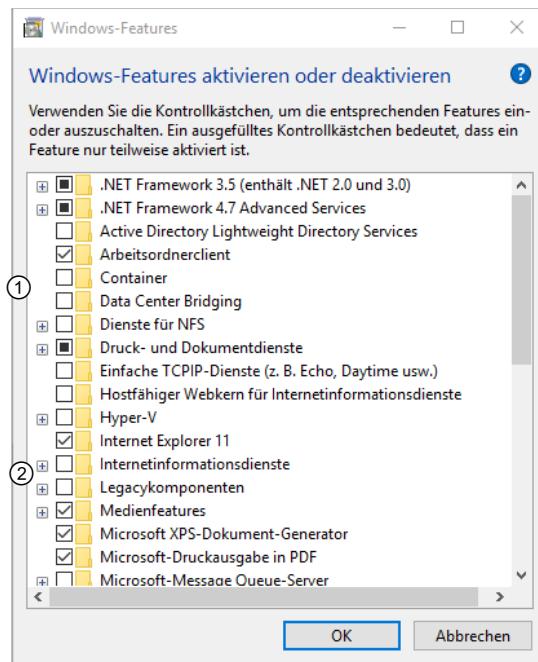
## 6.6 Windows-Funktionen aktivieren/deaktivieren

### Windows-Features einschalten und ausschalten

Falls Sie bestimmte Funktionen (Features) von Windows 10 benötigen, die nicht standardmäßig aktiviert sind, können Sie diese leicht nachträglich aktivieren, und durch Deaktivieren nicht benötigter Komponenten können Sie in bestimmten Fällen Systemressourcen frei machen und die Sicherheit erhöhen.

Alle benötigten Daten für zusätzliche Funktionen liegen bereits im Windows-Verzeichnis, ein Zugriff auf das Installationsmedium ist nicht erforderlich. Im Gegensatz zu früheren Windows-Versionen werden kaum Dateien kopiert, es werden lediglich Funktionen aktiviert oder deaktiviert. Durch die Deaktivierung von Windows-Funktionen gewinnen Sie keinen Festplattenspeicherplatz zurück.

- ▶ Suchen Sie nach optionalfeatures.
  - ▶ Aktivieren Sie zum Hinzufügen von Windows-Funktionen das entsprechende Kontrollfeld ① einer Funktion, deaktivieren Sie das Kontrollfeld zum Entfernen.
  - ▶ Bei einigen Funktionen können Sie festlegen, welche Komponenten Sie installieren möchten. Öffnen Sie dazu eine Baumstruktur ② und wählen Sie in den Unterpunkten die benötigten Komponenten aus.
  - ▶ Bestätigen Sie Ihre Auswahl mit *OK*.
- Windows 10 nimmt die entsprechenden Einstellungen vor. Eventuell ist ein Neustart des Computers erforderlich.

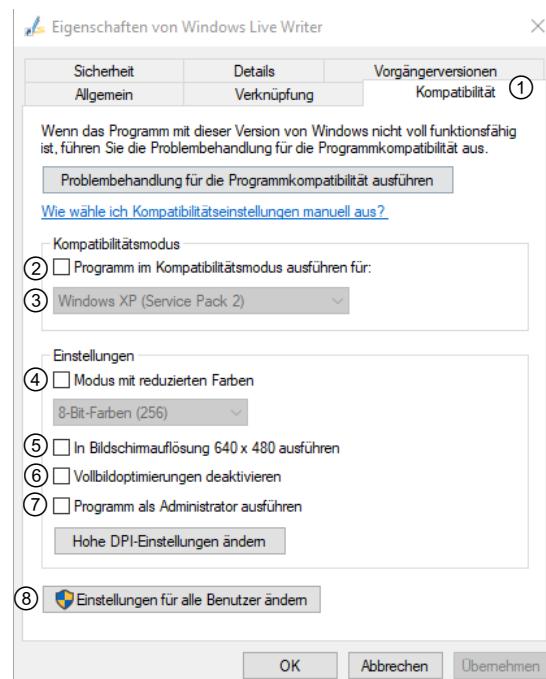


## Programmkompatibilität

Manche älteren Programme, die nicht für Windows 10 entwickelt wurden, funktionieren nicht richtig. In vielen Fällen kann der Programmkompatibilitäts-Assistent oder eine manuelle Einstellung helfen, die betreffende Anwendung in eine ähnliche Umgebung wie bei einer der folgenden früheren Windows-Versionen versetzt:

- ✓ Windows 95 / Windows 98/ME
- ✓ Windows XP (Service Pack 2 und 3)
- ✓ Windows Vista (Service Pack 1 und 2)
- ✓ Windows 7
- ✓ Windows 8/8.1
- ▶ Klicken Sie mit rechts auf die betroffene Anwendung und öffnen Sie die Eigenschaften.
- ▶ Wählen Sie die Registerkarte *Kompatibilität* ①.
- ▶ Aktivieren Sie den Kompatibilitätsmodus ② und legen Sie die Betriebssystemumgebung ③ fest, in der das Programm gestartet werden soll.

Bei Bedarf können Sie auch noch die Farbtiefe ④ und Bildschirmauflösung ⑤ reduzieren und die Skalierung deaktivieren ⑥, die sonst bei erhöhter Textgröße bei manchen Programmen Probleme macht. Sie können außerdem das Programm als Administrator ausführen lassen ⑦ und bestimmen, dass die Einstellungen für alle Benutzer gelten sollen ⑧.



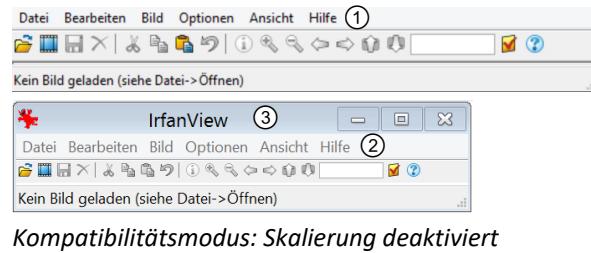
*Programmkompatibilität konfigurieren*

Die Einstellungen ④, ⑤ und ⑥ lassen sich nicht für Windows-eigene Applikationen wie z. B. *Notepad.exe* vornehmen.



## Skalierung deaktivieren

Die Option *Hohe DPI-Einstellungen ändern* kann sich bei vielen Programmen bewähren, deren Oberfläche sich nicht an große Schriften und Fensterelemente anpasst und dadurch vollkommen unbedienbar wird. Selbst bei Windows-Einstellungen mit sehr großen Schriften (z. B. 150 %) ① bleibt bei einer Software mit deaktiverter Skalierung die Schriftgröße und Skalierung der Symbole auf Normalgröße ②.



 Im Kompatibilitätsmodus für Windows XP oder ältere Windows-Versionen erscheinen viele Programmfenster in einem anderen Design mit grauer Farbe und abgerundeten Fensterecken ③. Dies trifft jedoch nicht für alle Programme zu.

## 6.7 Aktuelle Konfiguration einsehen und dokumentieren

### Systeminformationsprogramm MSInfo32 starten

- Betätigen Sie  und geben Sie `msinfo32`  ein.

Im Verwaltungswerkzeug *Systeminformationen* können Sie sich durch Doppelklicken auf die betreffenden Ordner genaue Informationen über die aktuellen Einstellungen des Systems anzeigen lassen:

- ✓ Systemübersicht ①
- ✓ Hardwareressourcen ②
- ✓ Komponenten ③
- ✓ Softwareumgebung ④

Systeminformationen																																																			
Datei Bearbeiten Ansicht ?																																																			
Systemübersicht ①																																																			
Hardwareressourcen ②	<table> <tr> <td>Element</td><td>Wert</td></tr> <tr> <td>Betriebssystemname</td><td>Microsoft Windows 10 Enterprise</td></tr> <tr> <td>Version</td><td>10.0.17134 Build 17134</td></tr> <tr> <td>Weitere Betriebssystembeschreib..</td><td>Nicht verfügbar</td></tr> <tr> <td>Betriebssystemhersteller</td><td>Microsoft Corporation</td></tr> <tr> <td>Systemname</td><td>THOMAS-PC</td></tr> <tr> <td>Systemhersteller</td><td>MSI</td></tr> <tr> <td>Systemmodell</td><td>MS-7817</td></tr> <tr> <td>Systemtyp</td><td>x64-basierter PC</td></tr> <tr> <td>System-SKU</td><td>To be filled by O.E.M.</td></tr> <tr> <td>Prozessor</td><td>Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz, 3601 MHz, 4 Kern(e), American Megatrends Inc. V10.1385, 10.04.2014</td></tr> <tr> <td>BIOS-Version/-Datum</td><td></td></tr> <tr> <td>SMBIOS-Version</td><td>2.8</td></tr> <tr> <td>Version des eingebetteten Cont...</td><td>255.255</td></tr> <tr> <td>BIOS-Modus</td><td>UEFI</td></tr> <tr> <td>Hauptplatinenhersteller</td><td>MSI</td></tr> <tr> <td>Hauptplatinenmodell</td><td>Nicht verfügbar</td></tr> <tr> <td>Hauptplatinenname</td><td>Hauptplatine</td></tr> <tr> <td>Plattformrolle</td><td>Desktop</td></tr> <tr> <td>Sicherer Startzustand</td><td>Aus</td></tr> <tr> <td>PCR7-Konfiguration</td><td>Bindung nicht möglich</td></tr> <tr> <td>Windows-Verzeichnis</td><td>C:\WINDOWS</td></tr> <tr> <td>Systemverzeichnis</td><td>C:\WINDOWS\system32</td></tr> <tr> <td>Startgerät</td><td>\Device\Harddisk\volume1</td></tr> <tr> <td>Gebietschema</td><td>Deutschland</td></tr> </table>	Element	Wert	Betriebssystemname	Microsoft Windows 10 Enterprise	Version	10.0.17134 Build 17134	Weitere Betriebssystembeschreib..	Nicht verfügbar	Betriebssystemhersteller	Microsoft Corporation	Systemname	THOMAS-PC	Systemhersteller	MSI	Systemmodell	MS-7817	Systemtyp	x64-basierter PC	System-SKU	To be filled by O.E.M.	Prozessor	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz, 3601 MHz, 4 Kern(e), American Megatrends Inc. V10.1385, 10.04.2014	BIOS-Version/-Datum		SMBIOS-Version	2.8	Version des eingebetteten Cont...	255.255	BIOS-Modus	UEFI	Hauptplatinenhersteller	MSI	Hauptplatinenmodell	Nicht verfügbar	Hauptplatinenname	Hauptplatine	Plattformrolle	Desktop	Sicherer Startzustand	Aus	PCR7-Konfiguration	Bindung nicht möglich	Windows-Verzeichnis	C:\WINDOWS	Systemverzeichnis	C:\WINDOWS\system32	Startgerät	\Device\Harddisk\volume1	Gebietschema	Deutschland
Element	Wert																																																		
Betriebssystemname	Microsoft Windows 10 Enterprise																																																		
Version	10.0.17134 Build 17134																																																		
Weitere Betriebssystembeschreib..	Nicht verfügbar																																																		
Betriebssystemhersteller	Microsoft Corporation																																																		
Systemname	THOMAS-PC																																																		
Systemhersteller	MSI																																																		
Systemmodell	MS-7817																																																		
Systemtyp	x64-basierter PC																																																		
System-SKU	To be filled by O.E.M.																																																		
Prozessor	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz, 3601 MHz, 4 Kern(e), American Megatrends Inc. V10.1385, 10.04.2014																																																		
BIOS-Version/-Datum																																																			
SMBIOS-Version	2.8																																																		
Version des eingebetteten Cont...	255.255																																																		
BIOS-Modus	UEFI																																																		
Hauptplatinenhersteller	MSI																																																		
Hauptplatinenmodell	Nicht verfügbar																																																		
Hauptplatinenname	Hauptplatine																																																		
Plattformrolle	Desktop																																																		
Sicherer Startzustand	Aus																																																		
PCR7-Konfiguration	Bindung nicht möglich																																																		
Windows-Verzeichnis	C:\WINDOWS																																																		
Systemverzeichnis	C:\WINDOWS\system32																																																		
Startgerät	\Device\Harddisk\volume1																																																		
Gebietschema	Deutschland																																																		
Komponenten ③																																																			
Softwareumgebung ④																																																			
Suchen nach: <input type="text"/>																																																			
<input type="checkbox"/> Nur ausgewählte Kategorie durchsuchen <input type="checkbox"/> Nur Kategorienamen durchsuchen																																																			
<input type="button" value="Suchen"/> <input type="button" value="Suche schließen"/>																																																			

*Systeminformationen einsehen mit msinfo32.exe*

### Systemübersicht

Im rechten Fensterbereich (Detailfensterbereich) ⑤ erhalten Sie Informationen über die Version des Betriebssystems, den Prozessor, das BIOS sowie die Größe des Speichers.

Hardware-Ressourcen	Ressourcenkonflikte, DMA, IRQs, belegte Arbeitsspeicheradressen etc.
Komponenten	Installierte Hardware und installierte Treiber etc.
Software-Umgebung	Systemtreiber, signierte Treiber, Umgebungsvariablen, Tasks und Dienste etc.

## Aktuelle Konfiguration dokumentieren

Sie können alle Informationen aus dem Detailfensterbereich direkt in eine ASCII-Datei schreiben lassen, um sie z. B. für eine eventuell nötige Systemwiederherstellung zur Verfügung zu haben.

- ▶ Je nachdem, welchen Bereich Sie exportieren möchten, aktivieren Sie den entsprechenden Ordner und wählen Sie das Menü *Datei - Exportieren*.
- ▶ Bestimmen Sie einen Pfad für die Datei und geben Sie einen Namen ein.
- ▶ Klicken Sie auf *Speichern*.

Das System aktualisiert nun die Informationen und speichert sie ab.

## 6.8 Einstellungen des Betriebssystems ändern

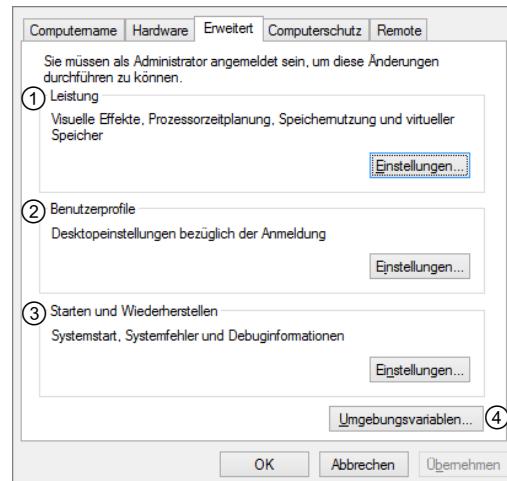
### Erweiterte Systemeigenschaften öffnen

- ▶ Klicken Sie im Schnellzugriffsmenü auf *System*. Damit gelangen Sie in der Windows-10-Einstellungs-App. Die klassische Ansicht erhalten Sie, wenn Sie im Suchfeld des Startmenüs nach „*sysdm.cpl*“ suchen und das Tool starten. Hier lassen sich auch in Windows 10, Version 1803 die Einstellungen noch effektiver vergeben.
- ▶ Wechseln Sie in das Register *Erweitert*.

Das Register *Erweitert* enthält drei **Bereiche**, auf die im Folgenden Bezug genommen wird:

- ✓ *Leistung* ①
- ✓ *Benutzerprofile* ②
- ✓ *Starten und Wiederherstellen* ③

Ebenfalls vorhanden ist ein Link zu den Umgebungsvariablen ④.



### Bevorzugtes Betriebssystem festlegen

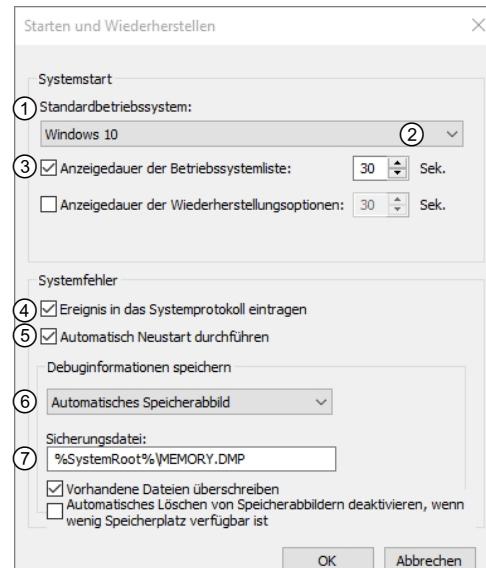
Wenn auf der Workstation eine Multibootkonfiguration erstellt wurde, können Sie festlegen, welches Betriebssystem beim Hochfahren des Systems als Standardsystem in der Auswahlliste des Boot-Managers erscheinen soll. Außerdem können Sie festlegen, nach welcher Wartezeit das Standardsystem automatisch gestartet wird, wenn keine Auswahl im Bootmenü getroffen wird.

- ▶ Klicken Sie in den Systemeinstellungen im Register *Erweitert* im Bereich *Starten und Wiederherstellen* auf *Einstellungen*.

Im Feld ① können Sie das **Standardbetriebssystem** festlegen.

Im Feld ② können Sie die **Wartezeit** bis zur automatischen Auswahl des Standardbetriebssystems bestimmen.

Durch Deaktivieren des Kontrollfelds ③ können Sie bestimmen, dass beim Hochfahren kein Bootmenü angezeigt wird, sondern sofort das Standardbetriebssystem gestartet wird.



*Verhalten bei Systemstart und Systemfehlern*

## Systemverhalten bei schwerwiegenden Fehlern steuern

- ✓ Durch Aktivieren des Kontrollfelds ④ nimmt Windows 10 bei Systemfehlern Eintragungen ins Systemprotokoll vor.
- ✓ Mit Kontrollfeld ⑤ können Sie festlegen, dass das System nach einem schweren Systemfehler automatisch neu startet.
- ✓ In Feld ⑥ legen Sie den Umfang und im Feld ⑦ den Ort des RAM-Speicherabbildes fest, das Windows 10 im Moment des Systemfehlers abspeichert (engl. Core-Dump = Kernspeicherabbild).

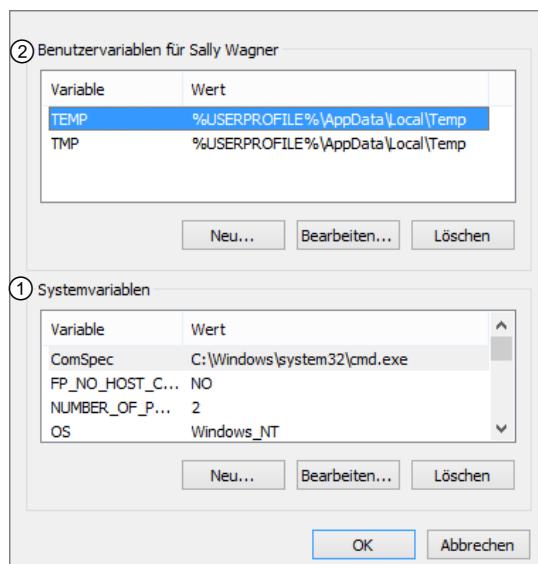
Dabei handelt es sich um eine 1:1-Kopie des Arbeitsspeichers, dessen Größe je nach der ausgewählten Option (klein, nur Kernel oder gesamter Speicher) stark variiert. Das Anlegen dieses Speicherabbildes kann vonnöten sein, wenn Sie die Hilfe z. B. des Microsoft Software Service in Anspruch nehmen und dieser Schnapschuss zum Zeitpunkt eines Problems zu Debuggingzwecken benötigt wird. Damit ein Speicherabbild angefertigt werden kann, muss die Auslagerungsdatei auf der gleichen Partition liegen wie das Betriebssystem.

## Umgebungsvariablen des Systems einsehen

- Klicken Sie in den Systemeigenschaften im Register *Erweitert* auf *Umgebungsvariablen*.

In Bereich ① sehen Sie Einstellungen für das System, die Windows 10 während der Installation angelegt hat. Die meisten gelten für alle Benutzer, allerdings können einige durch die Benutzerumgebungsvariablen für das Benutzerkonto ② überschrieben werden. Änderungen an diesen Einstellungen sind nur in seltenen Fällen notwendig und erfordern Administratorrechte.

- Mithilfe der Schaltflächen *Neu*, *Bearbeiten* und *Löschen* können Sie neue Umgebungsvariablen anlegen und bestehende ändern bzw. löschen.



*Umgebungsvariablen*

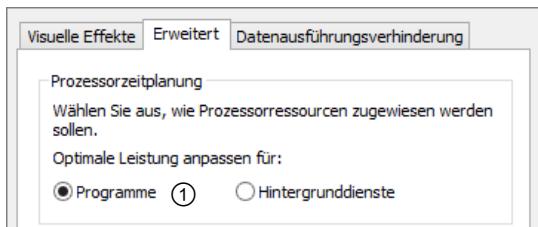


Systemumgebungsvariablen sind für den ordnungsgemäßen Betrieb einer Workstation unbedingt erforderlich. Löschen Sie deshalb keine der vom Betriebssystem angelegten Variablen.

## Multitasking und virtuellen Arbeitsspeicher optimieren

Sie können in Windows 10 festlegen, ob den gestarteten Anwendungsprogrammen mehr oder gleich viel Prozessorleistung und Arbeitsspeicher zugewilligt werden soll wie Hintergrunddiensten (z. B. Druckvorgängen). Im Normalfall ist hier die Standardeinstellung, also die Optimierung der Leistung für Anwendungen, zu bevorzugen. Änderungen können nur von Administratoren durchgeführt werden.

- Klicken Sie in den Systemeigenschaften im Register *Erweitert* im Bereich *Leistung* auf *Einstellungen*.
- Legen Sie mit den entsprechenden Optionsfeldern ① fest, wofür die Systemleistung optimiert werden soll.
- Bestätigen Sie Ihre Eingabe mit *OK*.



*Multitasking-Eigenschaften*

## Größe des virtuellen Arbeitsspeichers ändern

Für das Auslagern von momentan nicht benötigten Speicherseiten und falls der physische Arbeitsspeicher (RAM) knapp wird, verwendet Windows 10 **Auslagerungsdateien** auf Festplatten. Grundsätzlich kann auf jeder Partition ein bestimmter Bereich für eine solche Auslagerungsdatei (Dateiname *pagefile.sys*) reserviert werden. Dazu sind Administratorrechte erforderlich.

Sie sollten auf keinen Fall Auslagerungsdateien auf mehreren Partitionen **auf demselben Laufwerk** anlegen, sonst leidet die Geschwindigkeit bei herkömmlichen Magnetfestplatten wegen des sich ständig hin und her bewegenden Schreib-/Lesekopfs enorm.



Die automatische Verwaltung der Auslagerungsdateigröße durch Windows ist eine brauchbare Lösung, Sie können die Größe jedoch auch selbst bestimmen. Wählen Sie als Anfangsgröße die Größe des Arbeitsspeichers und als maximale Größe das Doppelte. Diese Einstellung vermeidet eine Fragmentierung der Festplatte und stellt für besondere Situationen ausreichend Kapazität zur Verfügung.

Beobachten Sie anschließend den Speicherbedarf und passen Sie im Bedarfsfall die Werte an Ihre Bedürfnisse an.

Windows verwendet standardmäßig nur das Betriebssystem-Laufwerk für die Auslagerung. Falls Ihr System über mehr als eine Festplatte verfügt, können Sie die Leistung erhöhen, indem Sie auf allen Laufwerken eine Auslagerungsdatei einrichten. So können Zugriffe auf die Auslagerungsdatei parallel erfolgen.

Wenn Ihr System über eine SSD verfügt, sollten Sie nur auf der schnellen SSD eine Auslagerungsdatei einrichten.

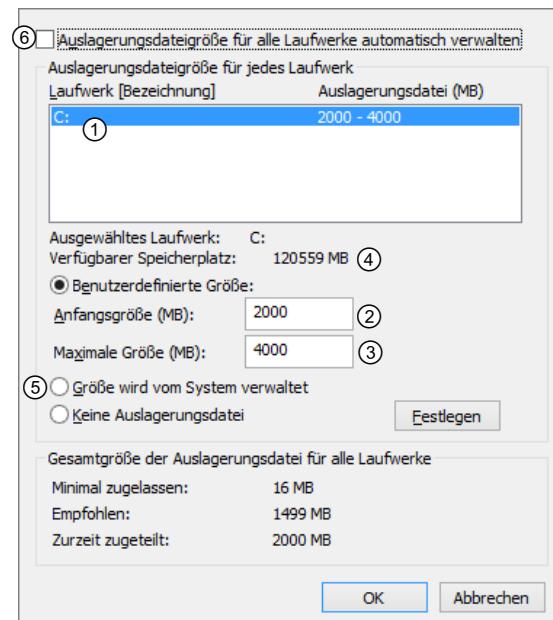
- Betätigen Sie in den erweiterten Systemeigenschaften im Bereich *Leistung* die Schaltfläche *Einstellungen*.
- Klicken Sie im Dialogfenster *Leistungsoptionen* im Register *Erweitert* auf *Ändern*.

Im oberen Bereich des Dialogfensters *Virtueller Arbeitsspeicher* sehen Sie die verfügbaren Laufwerke ① und die minimale und die maximale Größe der dort reservierten Auslagerungsdatei.

- Zum Ändern der Werte markieren Sie das entsprechende Laufwerk.
- Geben Sie die neuen Werte für die Mindest- ② und für die Maximalgröße ③ ein.

Orientieren Sie sich dabei auch am verfügbaren Speicherplatz ④ auf dem entsprechenden Laufwerk.

*oder* Anstatt selbst die Größe des virtuellen Speichers zu bestimmen, können Sie diese auch vom System verwalten lassen. Wählen Sie dazu das Optionsfeld *Größe wird vom System verwaltet* ⑤.



Größe des virtuellen Arbeitsspeichers einstellen

*oder* Wenn Sie sich mit der Konfiguration der Auslagerungsdateien gar nicht befassen wollen, überlassen Sie Windows 10 die Verwaltung sämtlicher Parameter ⑥. Dies ist die Standardeinstellung.

- Klicken Sie auf die Schaltfläche *Festlegen*, um die Änderungen für dieses Laufwerk zu übernehmen.
- Um Ihre Änderungen abzuschließen, klicken Sie auf *OK*.
- Windows 10 muss nach Einstellungen an der Auslagerungsdatei neu gestartet werden.

## Datenausführungsverhinderung

Die Datenausführungsverhinderung (**Data Execution Prevention, DEP**) ist ein Feature, das seit Windows XP SP2 in das Betriebssystem integriert ist. Zusammen mit geeigneter Prozessorhardware (im CPU-Umfeld wird dieses Feature als NX-Flag, für No-Execute-Flag, bezeichnet) soll verhindert werden, dass Schadsoftware über typische Sicherheitslücken in Programmen ausgeführt wird. Bei solchen Angriffen wird z. B. beim **Buffer Overflow Exploit** ein Überlaufen von Datenpuffern dazu genutzt, in geschützten Speicherbereichen schädlichen Code auszuführen. Dabei werden diese sensiblen Speicherbereiche auf eine nicht standardgemäße Weise angesprochen. Dieser Vorgang kann durch DEP bemerkt und verhindert werden.

Werden Exploitversuche in der Hardware erkannt, so beendet das Betriebssystem die betroffene Software zwangsweise, und die Schadsoftware kann nicht ausgeführt werden. Standardmäßig schützt Windows zunächst nur die eigenen Dienste und Programme, Sie können DEP aber auch für alle Programme und Dienste einschalten und dadurch die Sicherheit erheblich erhöhen.

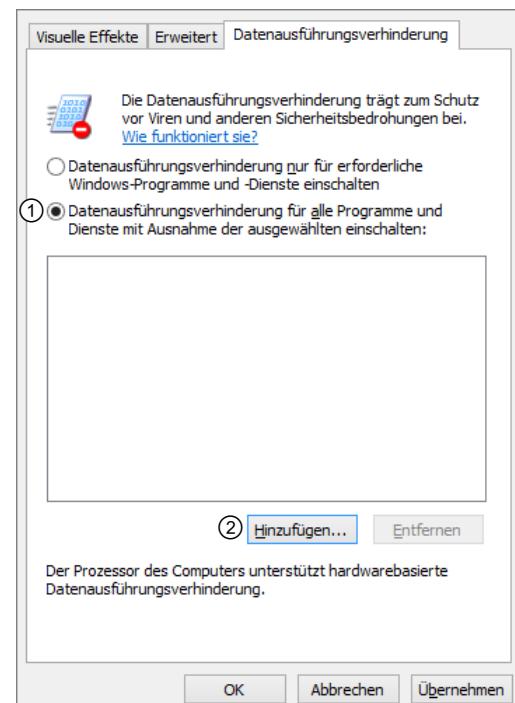
Vor einer dauerhaften Umstellung sollten Sie testen, ob alle von Ihnen genutzten Programme damit kompatibel sind. Einige Software wird wegen unsauberer Programmierung fälschlicherweise wegen eines „Exploits“ vom Betriebssystem beendet. Solche Programme können von DEP ausgenommen werden.

- ▶ Klicken Sie in den erweiterten Systemeigenschaften im Bereich *Leistung* auf *Einstellungen*.
- ▶ Klicken Sie in den Leistungsoptionen auf das Register *Datenausführungsverhinderung*.
- ▶ Klicken Sie die von Ihnen gewünschte Handhabung ① der DEP-Einstellungen an.

Software, die bei aktiviertem DEP nicht mehr lauffähig ist, können Sie zu der Liste mit Ausnahmen hinzufügen ②.



Windows 10 verfügt zusätzlich über eine Software-DEP, die auch auf Computern ohne DEP-Hardwareunterstützung funktioniert. Diese Funktion wird ebenfalls über die Datenausführungsverhinderung eingeschaltet. Die Software-DEP ist kein Ersatz der Hardware-DEP, sondern eine Ergänzung.



*DEP konfigurieren*

## 6.9 Dienste starten und verwalten

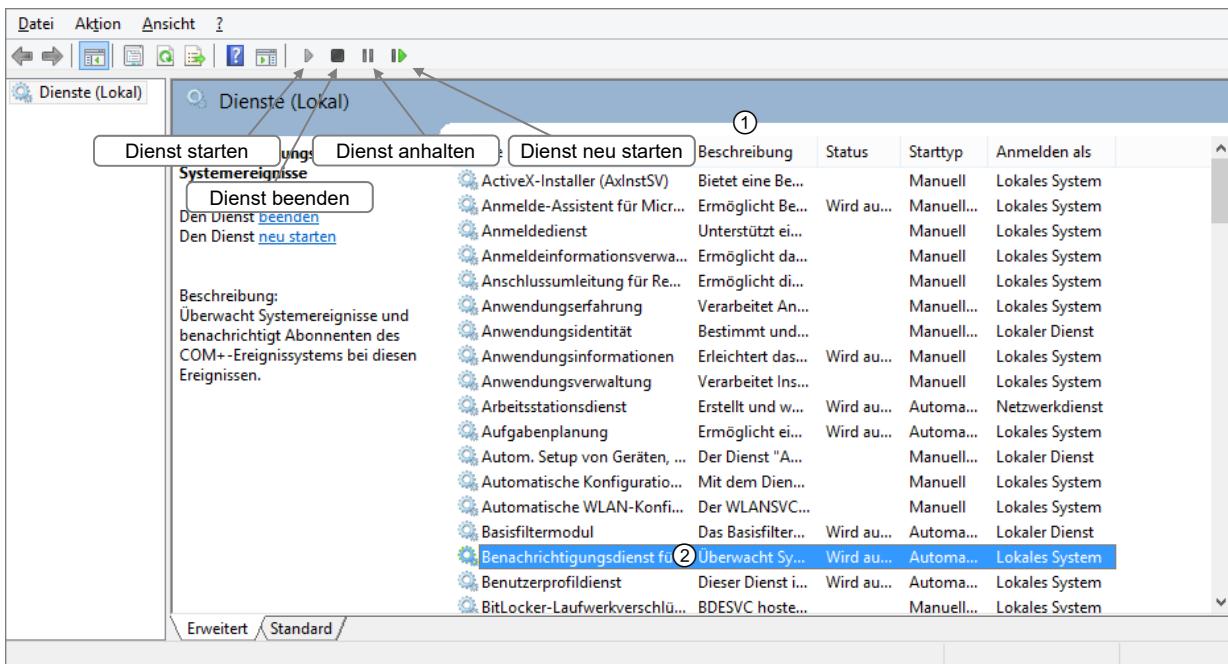
### Was sind Dienste?

Dienste sind Komponenten des Betriebssystems, die in der Regel im Hintergrund arbeiten, wie z. B. der Ereignisprotokoldienst oder die Druckwarteschlange. Nur wenn Sie Mitglied der Gruppe der Administratoren sind, können Sie alle Dienste verwalten.

### Dienstverwaltung öffnen

- ▶ Geben Sie `services.msc` im Suchfeld der Taskleiste ein.  
Die lokale Dienstverwaltung öffnet sich.

Alternativ können Sie auch im Schnellzugriffsmenü die *Computerverwaltung* auswählen. Anschließend klicken Sie auf *Dienste und Anwendungen - Dienste*.



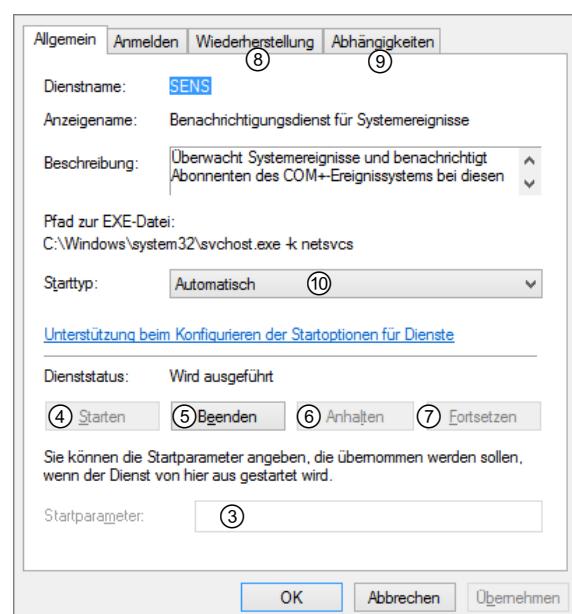
### Diensteverwaltung von Windows 10

In der Spalte **Beschreibung** ① und im linken Fensterbereich erhalten Sie eine kurze Beschreibung des Dienstes. In den weiteren Spalten wird außerdem angezeigt, ob der Dienst gerade aktiv ist und auf welche Weise er gestartet wird. Durch Markieren eines Dienstes und Klicken auf die entsprechenden Symbole können Sie Dienste starten, beenden, anhalten, fortsetzen oder neu starten.

### Dienst verwalten

- ▶ Klicken Sie doppelt auf den gewünschten Dienst in der Liste ② (vgl. Abb. *Diensteverwaltung von Windows 10*).
- ▶ Falls erforderlich, geben Sie im Feld ③ einen Startparameter ein.
- ▶ Klicken Sie auf eine der vier Schaltflächen, um den Dienst zu starten ④, zu beenden ⑤, anzuhalten ⑥ oder fortzusetzen ⑦.

Im Register **Wiederherstellung** ⑧ können Sie festlegen, wie Windows reagieren soll, wenn ein Dienst ausfällt. Unter Umständen kann es sinnvoll sein, den Rechner in diesem Fall neu starten zu lassen.



### Eigenschaften eines Dienstes

Beachten Sie, dass manche Dienste voneinander abhängig sind. Im Register **Abhängigkeiten** ⑨ können Sie einsehen, mit welchen anderen Diensten der ausgewählte Dienst verbunden ist. Dabei wird unterschieden in Dienste, für deren Start der ausgewählte Dienst eine Voraussetzung darstellt, und solche, von denen der ausgewählte Dienst abhängig ist.



## Starttyp festlegen

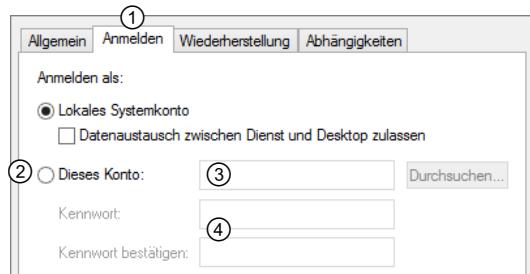
- Stellen Sie im Feld ⑩ den gewünschten Starttyp ein.

<b>Automatisch</b>	Dienst startet automatisch beim Hochfahren des Systems.
<b>Automatisch (Verzögerter Start)</b>	Dienst startet automatisch beim Hochfahren des Systems, allerdings mit einer zeitlichen Verzögerung.
<b>Manuell</b>	Dienst muss entweder vom Benutzer oder von einem anderen Dienst gestartet werden.
<b>Deaktiviert</b>	Dienst kann weder vom Benutzer noch von einem anderen Dienst gestartet werden.

## Dienst mit einem Benutzerkonto anmelden

Sie können Dienste auch so konfigurieren, dass diese sich bei einem Systemstart unter einem bestimmten Benutzernamen am lokalen Rechner oder an anderen Rechnern anmelden und mit den entsprechenden Berechtigungen dieses Benutzerkontos ihre Arbeit verrichten.

- Nach einem Doppelklick auf den entsprechenden Dienst in der Liste wechseln Sie in das Register *Anmelden* ①.
- Aktivieren Sie das Optionsfeld *Dieses Konto* ② und tragen Sie in die Felder den Benutzernamen ③ und zweimal das Kennwort ein ④.



Dienst mit anderem Benutzerkonto ausführen



Achten Sie unbedingt darauf, dass das verwendete Benutzerkonto sein Passwort **nicht** regelmäßig ändern muss. Falls z. B. alle 42 Tage eine Änderung für alle Benutzerkonten vorgeschrieben ist, kann der Dienst am 43. Tag nicht mehr gestartet werden, da er sich nicht anmelden und auch nicht selbstständig sein Passwort ändern kann. Als Ausgleich sollten Sie Dienstekonten grundsätzlich sehr lange und komplexe Passwörter zuweisen.

## Einige wichtige Standarddienste von Windows 10

<b>Anmeldedienst</b>	Unterstützt bei Arbeitsstationen das Weiterleiten der Echtheitsbestätigung bei der Anmeldung in der Domäne, auch bekannt als LSASS-Systemdienst
<b>Computerbrowser</b>	Verwaltet die aktuelle Liste der Computer und stellt dieser Anwendungen zur Verfügung
<b>Druckwarteschlange</b>	Verwaltet die anfallenden Druckdateien
<b>Windows-Ereignisprotokoll</b>	Zeichnet Ereignisse, Warnungen und Fehler im Systemprotokoll, Sicherheitsprotokoll oder Anwendungsprotokoll auf
<b>Server</b>	Unterstützung für Freigaben und Datenverbindungen zwischen Netzwerkprozessen
<b>Aufgabenplanung</b>	Erlaubt die automatische Ausführung von Aufgaben über den Taskplaner
<b>Benutzerprofildienst</b>	Erforderlich für lokale Anmeldung und Domänenanmeldung
<b>DHCP-Client</b>	Empfang von dynamischer IP-Adresse und DNS-Aktualisierungen
<b>DNS-Client</b>	Ermöglicht Anfragen an einen DNS-Server zur Namensauflösung



In den meisten Fällen ist es nicht nötig, in die Verwaltung der Dienste manuell einzutreten, und bei heutiger Hardware ist ein zu erwartender Leistungszuwachs durch Abschalten von Diensten zu vernachlässigen. Das manuelle Abschalten wichtiger Dienste kann schwerwiegende Fehler erzeugen. Sie sollten sich genau informieren, bevor Sie irgendwelche Systemdienste deaktivieren oder Einstellungen verändern.

## 6.10 Geräte aktivieren und deaktivieren

### Geräte-Manager verwenden

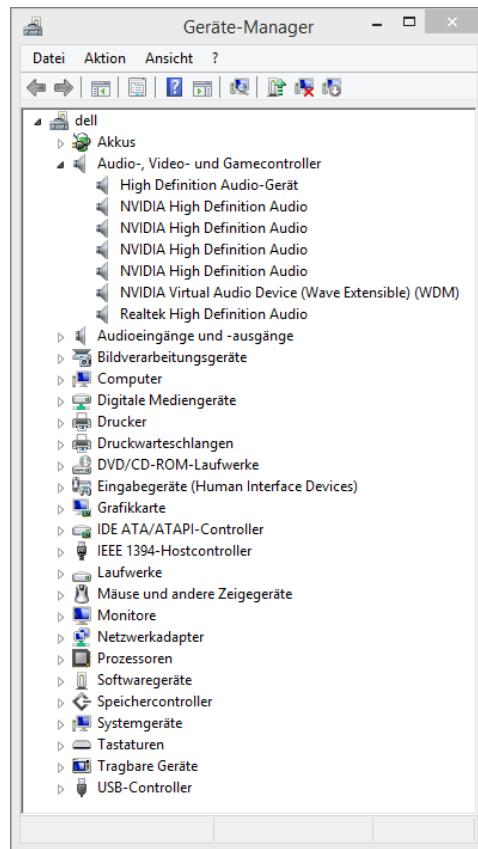
Sie benötigen Administratorrechte, um im Gerät-Manager Änderungen vornehmen zu können.

- ▶ Wählen Sie im Schnellzugriffsmenü den Menüpunkt **Geräte-Manager** oder suchen Sie auf der Startseite nach `devmgmt.msc`.
- ▶ Wählen Sie in der Liste das Gerät aus, dessen Status Sie ändern wollen.
- ▶ Führen Sie einen Rechtsklick auf das Gerät durch.
- ▶ Wählen Sie im Kontextmenü, ob Sie das Gerät deaktivieren, komplett deinstallieren oder eine Treiberaktualisierung vornehmen möchten.

### Deaktiviertes Gerät

Wenn ein Gerät deaktiviert ist, wird sein Symbol mit einem kaum erkennbaren grauen Pfeil  versehen.

Das Aktivieren und Deaktivieren von Geräten ist dann sinnvoll, wenn Sie nicht ständig mit der gleichen Hardware arbeiten. Dadurch, dass Sie ein Gerät deaktivieren, halten Sie den entsprechenden Gerätetreiber an und Windows 10 versucht nicht mehr, auf das Gerät zuzugreifen.



Geräte-Manager-Ansicht: Geräte nach Typ

### Andere Ansichtsmodi

Probieren Sie einmal alle verschiedenen Ansichten aus, die Sie im Menü **Ansicht** auswählen können. Auf diese Weise können Sie die Geräte und Ressourcen nach Typ oder Verbindung anzeigen lassen.

## 6.11 Energieverwaltung

### Advanced Configuration and Power Interface (ACPI)

Die Energieverwaltung von Windows 10 erfolgt mithilfe des Industriestandards ACPI (Advanced Configuration and Power Interface), das ältere APM (Advanced Power Management) wird nicht mehr unterstützt.

ACPI ist der Standard für moderne Motherboards. Er besteht aus zwei Teilen, der **Konfiguration** (Unterstützung von Plug & Play) und der **Energieverwaltung**. ACPI-Boards können das Betriebssystem zum einen über die aktuelle Gerätekonfiguration und über die möglichen bzw. erlaubten Betriebsarten von ACPI-tauglichen Geräten informieren. Zum anderen kann Windows 10 über ACPI die komplette Steuerung der Energieverwaltung und das Zu- und Abschalten von Geräten übernehmen.

ACPI unterstützt z. B. das Herunterfahren von Festplatten oder das Abschalten momentan nicht benötigter Karten. Bei geeigneter Hardware und Software kann ein Computer bei Nichtgebrauch in einen tiefen Schlafzustand fallen, in dem er nur sehr wenig Energie verbraucht und dennoch blitzschnell wieder aufgeweckt werden kann. Je nach Einsatzzweck eines Computers kann so ein Großteil des üblichen Energieverbrauchs eingespart werden.

Ziel von ACPI ist eine flexible zustandsorientierte Energieverwaltung, die zum einen erkennt, wenn ein Programm auch ohne Benutzereingaben Rechenleistung benötigt, und dementsprechend die Prozessorleistung nicht reduziert, gleichzeitig aber Monitor, Grafikkarte und Drucker auf Stand-by-Betrieb setzt. Zum anderen kann der Computer durch das Signal eines Eingabegeräts (Maus, Tastatur, Touchpad) oder einer Netzwerkkarte aus einem Energiesparzustand schnell wieder aktiviert werden.

Wenn Sie überprüfen möchten, ob ein Windows-Computer ACPI verwendet, rufen Sie den Geräte-Manager auf und klicken Sie in der Geräteliste doppelt auf *Computer*. Bei einem Windows-8/10-Computer wird dort *ACPI-x64-basierter Computer* oder *ACPI-x8/106-basierter-Computer* angezeigt, je nachdem, ob Sie Windows 10 mit 32 Bit oder 64 Bit einsetzen.

### Energiesparende Systemzustände

 Im hybriden Stand-by-Modus von Windows 10 wird der Computer in einen Energiesparmodus versetzt, in dem zunächst alle Inhalte des Arbeitsspeichers auf der Systemfestplatte gesichert werden. (Dieses Vorgehen entspricht dem Ruhezustand.) Anschließend schaltet sich der Computer weitgehend ab, nur der Arbeitsspeicher wird noch mit Energie versorgt, um die Inhalte zu erhalten (entspricht dem herkömmlichen Stand-by-Modus).

Durch Betätigen einer Taste wird der Computer wieder aktiviert. Wenn sich die Inhalte noch im Arbeitsspeicher befinden, kann die Arbeit schnell fortgesetzt werden, anderenfalls wird beim Einschalten des Computers der Speicherinhalt aus der Ruhezustandsdatei *hiberfil.sys* von der Festplatte eingelesen und die Arbeit kann am zuvor gesicherten Punkt fortgesetzt werden.

### Connected Standby (Verbundener Stand-by)

Dieser neuartige Energiesparmodus sorgt dafür, dass der Computer ähnlich wie ein Smartphone auch während des Energiesparens erreichbar bleibt („Always on“) und die Netzwerkverbindung aufrechterhalten wird. Dieser Modus ist nur für Computer mit Trusted Platform Module (TPM) Version 2.0 verfügbar, die außerdem noch weitere Voraussetzungen erfüllen müssen.

### Ruhezustand und Stand-by

Die aus älteren Windows-Betriebssystemen bekannten Zustände *Stand-by* (eine Sicherung der Speicherinhalte nur im Arbeitsspeicher) und *Ruhezustand* (Sicherung der Speicherinhalte nur auf der Festplatte) sind nicht mehr offen verfügbar. Es gibt jetzt nur noch die Auswahl zwischen *Energie sparen*, *Herunterfahren* und *Neu starten*.



Sie erreichen die Auswahl zum Ausschalten des Computers am schnellsten über die Startschaltfläche. Auf dem Desktop funktioniert aber auch weiterhin **[Alt] [F4]**.

Das Verfahren des Ruhezustands wird bei Windows 10 auch beim normalen Herunterfahren verwendet, um beim nächsten Systemstart schneller betriebsbereit zu sein. Das Verfahren wird **Hybrid Boot** genannt und ist ebenso wie der Ruhezustand nur auf physischen Computern verfügbar, nicht jedoch in virtuellen Maschinen. Sie können die Bootzeiten vergleichen, indem Sie Windows mit dem Kommandozeilen-Tool `shutdown /s` ohne Hybrid Boot herunterfahren und beim nächsten Mal mit dem Parameter `/hybrid` verwenden. Messen Sie jeweils die Zeit bis zum Sperrbildschirm.

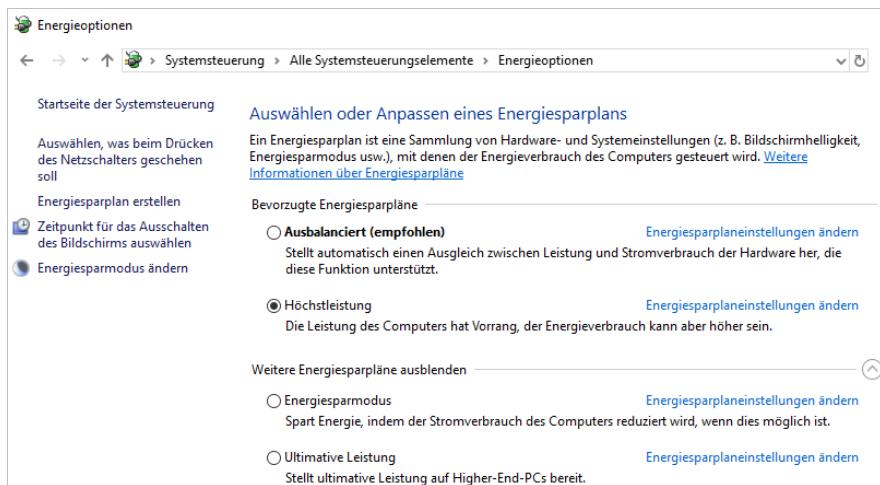
### Energiesparpläne

Sie können mit Energiesparplänen das Energiesparverhalten des Systems festlegen. Darin wird in zahlreichen Einstellungen bestimmt, wie schnell und unter welchen Bedingungen das System in einen Energiesparzustand wechseln kann. Es liegen bereits vordefinierte Pläne vor:

- ✓ Ausbalanciert (empfohlen)
- ✓ Energiesparmodus
- ✓ Höchstleistung

## Energiesparplan auswählen und anpassen

- ▶ Öffnen Sie die Systemsteuerung und klicken Sie auf den Hyperlink **Energieoptionen**.
- ▶ Führen Sie Ihre Anpassungen durch, indem Sie den entsprechenden Link anklicken.



## Weitere Einstellungen am Energiesparverhalten vornehmen

Ein sehr mächtiges Werkzeug ist das Kommandozeilentool `powercfg`, das mit Adminrechten ausgeführt werden muss. Mit `powercfg /hibernate on` können Sie beispielsweise den Hibernate-Modus (Ruhezustand) einschalten. Mit `powercfg /list` werden alle Energiesparpläne angezeigt, mit `powercfg/available-sleepstates` können Sie alle verfügbaren Energiesparmodi (S1 bis S5) auflisten. Weitere Befehlsparameter bekommen Sie über `powercfg /?` angezeigt. Geben Sie in der Eingabeaufforderung den Befehl `powercfg /energy` ein, erstellt Windows einen HTML-Bericht und gibt zusätzlich an, in welchem Ordner der Bericht gespeichert wurde.

## 6.12 Der Sprachassistent Cortana

Windows 10 verfügt über einen Sprachassistenten. Cortana unterstützt Sie auch bei der normalen Windows-Suche. Mit jeder neuen Windows-10-Version erweitert Microsoft die Funktionen von Cortana. Sie können sich beim Einrichten Ihres Windows-10-Computers entscheiden, ob Sie die Funktion nutzen wollen oder nicht. Der Assistent zum Einrichten von Cortana startet durch einen Klick in das Suchfeld der Taskleiste oder das Symbol mit der Lupe. Klicken Sie auf das Suchfeld, zeigt Cortana zunächst Nachrichten an, wenn der Computer mit dem Internet verbunden ist. Die verschiedenen Einstellungen für Cortana finden Sie am schnellsten, wenn Sie im Suchfeld den Begriff „cortana“ eingeben. Cortana starten Sie auch über das Kontextmenü des Startmenüs durch Auswahl von *Suchen*.

Damit Cortana Informationen anzeigen kann, müssen Sie zunächst einige Einstellungen anpassen:

- ▶ Rufen Sie Cortana über das Suchfeld auf und klicken auf das Zahnrad-Symbol.  
Hier können Sie Einstellungen vornehmen.
- ✓ Aktivieren Sie Funktionen in Cortana, die Sie benötigen.
- ✓ Sie können an dieser Stelle zum Beispiel Cortana generell ein- und ausschalten.
- ✓ Über das Notizbuch können Sie die Fertigkeiten von Cortana verwalten.
- ✓ Cortana kann Ihnen auch automatisiert Informationen zu Staus, Verkehrsinformationen oder Routen zu Strecken anzeigen, die Sie häufiger benötigen, zum Beispiel zum Ausweichen vor Staus. Dazu rufen Sie im Notizbuch die Option *Pendelstrecke und Verkehr* auf. Hier können Sie alle wichtigen Einstellungen dazu vornehmen. Sinnvoll ist das, wenn Sie Cortana auch mobil nutzen.
- ✓ Damit diese Funktion optimal genutzt werden kann, sollten Sie im Notizbuch in den Einstellungen (Stift-Symbol) Ihre Lieblingsorte eingeben.



## Sprachsteuerung mit Cortana

Haben Sie ein Mikrofon im Rechner verfügbar, können Sie auch die Sprachsteuerung von Cortana aktivieren. Dazu tippen Sie mit dem Finger oder der Maus auf das Mikrofon-Symbol neben dem Suchfeld in der Taskleiste, oder Sie sagen den Satz „Hey Cortana“. Ob Cortana darauf reagieren soll, konfigurieren Sie in den Einstellungen.

Microsoft Edge arbeitet ebenfalls mit Cortana zusammen. Markieren Sie Teile eines Satzes, können Sie über das Kontextmenü eine Suche mit Cortana starten. Auf einer Liste im linken Bildrand erhalten Sie anschließend Informationen zu dem gesuchten Begriff.

Wollen Sie Cortana nicht mehr nutzen und sicherstellen, dass Ihre privaten Daten vom PC entfernt werden, rufen Sie die Einstellungen von Cortana auf. Hier können Sie alles deaktivieren, was Sie nicht benötigen, auch Cortana selbst.

### Cortana und Gruppenrichtlinien

In den Gruppenrichtlinien von Windows Server 2016 oder den lokalen Richtlinien in Windows 10 können Sie über *Computerkonfiguration - Administrative Vorlagen - Windows-Komponenten - Suche* auf der rechten Seite einige Einstellungen vornehmen, die auch Cortana betreffen. Mit der Richtlinieneinstellung *Cortana zulassen* können Sie durch Setzen der Option *Deaktivieren* Cortana auf **allen Rechnern** ausschalten. Die Anwender können in diesem Fall nur noch die normale Suche verwenden.

## 6.13 Virtuelle Desktops erstellen und steuern

Die virtuellen Desktops zeigen, wie beim Verwenden der Mini-Ansicht in der Taskbar, auch den Inhalt des aktuellen Desktops an. Nutzen Sie die Funktion nicht, können Sie diese ausblenden. Dazu klicken Sie die Taskleiste mit der rechten Maustaste an und deaktivieren die Option *Taskansicht-Schaltfläche anzeigen*. Sie können aber weiterhin die Tastenkombinationen dazu verwenden.

Sie möchten ...	Drücken Sie ...
die Oberfläche zum Erstellen von virtuellen Desktops starten	►
einen neuen Desktop erstellen	►  [Strg] [D]
einen virtuellen Desktop schließen	►  [Strg] [F4]
zwischen virtuellen Desktops wechseln	►  [Strg] [← bzw.  [Strg] [→]]

Sie können zwischen den Desktops wechseln, wie beim Wechseln zwischen Anwendungen auf einem einzelnen Desktop.

Grundsätzlich lassen sich die Apps auch zwischen Desktops verschieben. Dazu öffnen Sie die Ansicht der verschiedenen Desktops. Fahren Sie mit der Maus über einen Desktop im unteren Bereich, sehen Sie im Hauptfenster die Anwendungen, die auf dem Desktop laufen. Über das Kontextmenü und die Auswahl von *Verschieben nach* können Sie die Anwendungen verschieben. Schließen Sie einen Desktop, werden die geöffneten Anwendungen auf andere Desktops verschoben.

## 6.14 Übung

### Windows 10 anpassen

Übungsdatei: --

Ergebnisdatei: *Uebung06\_E.pdf*

1. Wie ändern Sie die Einstellung *Öffentliches Netzwerk* zu *Privates Netzwerk* ab?
2. Wie zeigen Sie die Desktop-Symbole an?
3. Wie deinstallieren oder ändern Sie Programme?
4. Wie fügen Sie Optionen zu Windows 10 hinzu?
5. Wie öffnen Sie die Diensteverwaltung?
6. Wie aktivieren und konfigurieren Sie Cortana?



# 7 Microsoft Management Console (MMC)

## In diesem Kapitel erfahren Sie

- ✓ was die Microsoft Management Console ist
- ✓ welche Funktionen sie erfüllt
- ✓ wie Sie mit der Management Console arbeiten können
- ✓ wie Sie eigene Konsolen erstellen und konfigurieren können
- ✓ wie Sie Server lokal virtualisieren und verwalten

## Voraussetzungen

- ✓ Grundlagen der Bedienung von Windows 10
- ✓ Grundkenntnisse in den administrativen Aufgaben in Windows 10

## 7.1 Konsole und Snap-Ins

### Die Konsole

Die **Microsoft Management Console** (MMC) dient zur Erstellung individuell angepasster Werkzeuge für die Verwaltungarbeit unter Windows 10. Die MMC ist eine einheitliche Oberfläche für verschiedene Anwendungen zur Verwaltung und Problembehandlung. Diese Oberfläche wird als **Konsole** bezeichnet. Die einzelnen Anwendungen stehen als vorbereitete **Snap-Ins** zur Verfügung, die einer Konsole nach Bedarf hinzugefügt und darin organisiert werden können.

Eine Konsole kann ein einzelnes Snap-In enthalten, es können aber auch mehrere Snap-Ins kombiniert und konfiguriert werden. So ergibt sich eine Palette von Verwaltungswerkzeugen, die in ihrer Funktion gezielt der jeweiligen Aufgabe angepasst werden können.

Eine mit der MMC erstellte Konsole kann als Datei gespeichert werden. Diese Datei mit der Erweiterung *.msc* enthält Informationen über alle eingefügten Snap-Ins und deren Einstellungen. Sie kann weitergegeben und auch auf anderen Computern gestartet werden. Dies ist vor allem nützlich, wenn ein Administrator sich seine Werkzeuge für den eigenen Bedarf zusammenstellt oder wenn für bestimmte Benutzergruppen ein spezielles Werkzeug bereitgestellt werden soll, das genau die benötigten Informationen und Funktionen enthält und dem Benutzer alles andere vorenthält. Auf diese Weise sind Sie als Systembetreuer in der Lage, verschiedene administrative Aufgaben an andere Benutzer zu delegieren.



Installieren Sie auf einem Rechner mit Windows 10 die Remoteserver-Verwaltungstools, können Sie auch die Serverdienste von Windows Server 2012 R2 und Windows Server 2012 in die Managementkonsole einbinden sowie die Verwaltungsdienste für Windows Server 2016/1709 und 1803. Auch der Server-Manager steht dann zur Verfügung, mit allen Möglichkeiten, die auch auf einem lokalen Server mit Windows Server 2012/2012 R2 und 2016 zur Verfügung stehen. Alternativ können Sie zusätzlich über Microsoft Edge mit dem Windows Admin Center arbeiten, wenn Sie dieses im Netzwerk installiert haben.

### Die Snap-Ins

Es stehen zwei Kategorien von Snap-Ins zur Verfügung. **Eigenständige Snap-Ins** werden direkt einer Konsole hinzugefügt und stellen so die Funktionalität für eine bestimmte Verwaltungsaufgabe bereit.

**Snap-In-Erweiterungen** bieten zusätzliche Funktionen für Snap-Ins, indem sie auf deren speziellen Funktionen aufbauen. Beim Hinzufügen eines Snap-Ins zu einer Konsole werden automatisch alle kompatiblen Erweiterungen mit eingeschlossen. Sie können jedoch anschließend einzeln entfernt werden.

Viele Snap-Ins sind auch für die Fernverwaltung geeignet und ermöglichen so die Bearbeitung von Verwaltungsaufgaben und Problemen auch auf räumlich entfernten Computern.



### Die Zugriffsmodi

Grundsätzlich lassen sich zwei Zugriffsmodi unterscheiden, in denen mit der MMC gearbeitet werden kann: Benutzermodus und Autorenmodus. Diese Modi bestimmen, welche Berechtigungen der Benutzer einer Konsole erhält.

Nur im **Autorenmodus** ist es dem Benutzer der Konsole möglich, Snap-Ins hinzuzufügen und zu entfernen. Wenn Sie für den Benutzer einen der drei Benutzermodi festlegen, kann er keine Snap-Ins hinzuzufügen bzw. entfernen.

In der MMC werden drei Stufen des **Benutzermodus** unterschieden. In der Einstellung *Benutzermodus - Vollzugriff* ist es dem Benutzer erlaubt, die ganze Struktur der Konsole einzusehen und mehrere Ansichten zu erstellen. In der Einstellung *Benutzermodus - beschränkter Zugriff, mehrere Fenster* kann der Benutzer nur einen Teil der Struktur einsehen, aber eigene Ansichten erstellen. In der Einstellung *Benutzermodus - beschränkter Zugriff, Einzelfenster* darf der Benutzer nur einen Teil der Struktur einsehen und kann keine eigenen Ansichten erstellen.

## 7.2 Mit der MMC lösbar Aufgaben

### Verfügbare Snap-Ins

Die MMC ist als wichtigstes Werkzeug zur Verwaltung von Windows konzipiert. Windows 10 enthält deshalb bereits eine Sammlung vorbereiteter Snap-Ins, mit denen ein großer Teil der Verwaltungsaufgaben des Systembetreuers erledigt werden kann. Durch die Installation der Remoteserver-Verwaltungstools für Windows 10 können Sie auch die Serverrollen von Windows Server 2012 R2 und Windows Server 2012 sowie Windows Server 2016 in Konsolen einbinden. Diese lassen sich uneingeschränkt auf den Servern verwalten. Die Standardsammlung enthält unter anderem folgenden Snap-Ins:

- |                         |   |
|-------------------------|---|
| ✓ Computerverwaltung    | ✓ Freigegebene Ordner                   |
| ✓ Datenträgerverwaltung | ✓ Geräte-Manager                        |
| ✓ Defragmentierung      | ✓ Leistungskontrolle und Warnungen      |
| ✓ Dienste               | ✓ Lokale Benutzer und Gruppen           |
| ✓ Ereignisanzeige       | ✓ Sicherheitskonfiguration und -analyse |

### Das Snap-In Computerverwaltung

Das Snap-In *Computerverwaltung* ist ein Standardwerkzeug für die wichtigsten Verwaltungsaufgaben des Systembetreuers. Es bietet eine Kombination verschiedener Verwaltungswerkzeuge. Wenn Sie eine Konsole mit dem Snap-In *Computerverwaltung* ausstatten, stehen Ihnen folgende Funktionen gleichzeitig zur Verfügung:

- |                                       |                           |
|---------------------------------------|---------------------------|
| ✓ System                              | ✓ Datenspeicher           |
| ✓ Aufgabenplanung                     | ✓ Datenträgerverwaltung   |
| ✓ Ereignisanzeige                     | ✓ Dienste und Anwendungen |
| ✓ Freigegebene Ordner                 | ✓ Dienste                 |
| ✓ Lokale Benutzer und Gruppen         | ✓ WMI-Steuerung           |
| ✓ Leistung (Protokolle und Meldungen) |                           |
| ✓ Geräte-Manager                      |                           |

## Andere Snap-Ins

Zur Weitergabe an Benutzer eignen sich am besten Snap-Ins, die für einzelne administrative Aufgaben konzipiert sind, z. B. das Snap-In *Lokale Benutzer und Gruppen*. Mit einer gezielten Auswahl der Snap-Ins kann die Funktionalität einer Konsole wirkungsvoll beschränkt werden. Ein Benutzer erhält so nur diejenigen Verwaltungswerzeuge, die er für eine bestimmte administrative Aufgabe benötigt.

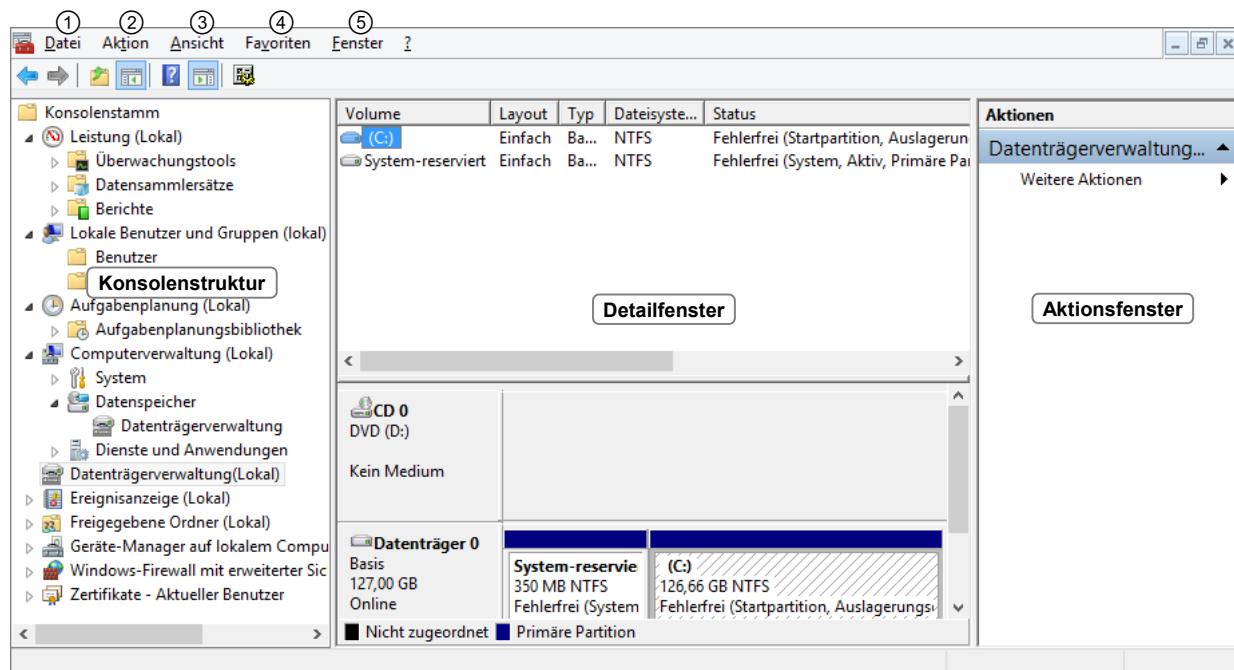


Auch andere Software-Hersteller können die MMC als Plattform für die Administration ihrer Produkte nutzen. Dazu müssen sie lediglich eigene Snap-Ins mit der benötigten Funktionalität bereitstellen. Die Palette der verfügbaren Snap-Ins für Windows 10 dürfte sich daher in Zukunft noch erweitern.

## 7.3 Aufbau und Menüs der MMC

### Programm- und Konsolenfenster

Eine neue Konsole besteht aus zwei Fenstern: einem Programm- und einem Konsolenfenster. Das Programmfenster bezieht sich auf die MMC, während sich das Konsolenfenster nur mit den Inhalten der hinzugefügten Snap-Ins beschäftigt. Das Konsolenfenster ist in das Programmfenster eingebettet und enthält links die Konsolenstruktur, in der Mitte im Detailfenster detaillierte Informationen und rechts die zur Verfügung stehenden Aktionen im Aktionsfenster.



Ansicht einer MMC mit dem eingefügten Snap-In Computerverwaltung (Lokal)

### Verfügbare Menüs

Je nachdem, ob Sie gerade eine neue Konsole erstellen oder mit einer bestehenden arbeiten, stehen Ihnen bestimmte Menüs zur Verfügung. Ob die Menübefehle angezeigt werden, ist abhängig von dem Zugriffsmodus sowie von den hinzugefügten Snap-Ins.

Menü Datei ①	Hier können Sie Snap-Ins hinzufügen, die Konsole speichern und allgemeine Optionen einstellen.
Menü Aktion ②	Abhängig vom gerade aufgerufenen Snap-In können Sie hier kontextbezogene Aktionen starten. Die gleichen Aktionen finden Sie auch im Aktionsfenster unter Weitere Aktionen.

<b>Menü Ansicht ③</b>	Wählen Sie hier die aus Windows-Ordnern bekannten Anzeigoptionen aus.
<b>Menü Favoriten ④</b>	Hier können Sie ähnlich wie im Internet Explorer bestimmte z. B. häufig angesteuerte Konsolenelemente eines Snap-Ins den Favoriten hinzufügen und verwalten.
<b>Menü Fenster ⑤</b>	Öffnen Sie hier neue Fenster oder ordnen Sie bestehende Fenster neu an.

## 7.4 Konsole erstellen und anpassen

### MMC starten

- ▶ Betätigen Sie und geben Sie mmc ein.  
Alternative: , im Ausführen-Dialog mmc eingeben
- ▶ Bestätigen Sie die UAC-Meldung.

Wenn Sie die MMC mit der hier beschriebenen Vorgehensweise starten, wird automatisch eine neue leere Konsole im Autorenmodus geöffnet.

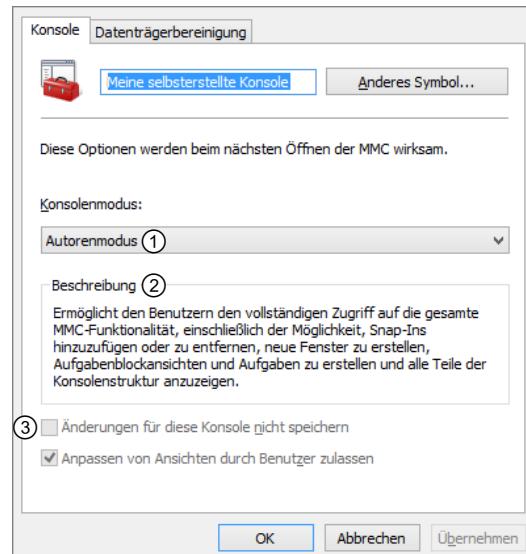
### Zugriffsmodus einstellen

- ▶ Um den eingestellten Zugriffsmodus einzusehen bzw. zu ändern, rufen Sie den Menüpunkt *Datei - Optionen* auf.
- ▶ Legen Sie im Listenfeld *Konsolenmodus* ① die Zugriffsart fest.

Informationen zu den vier Konsolenmodi werden in dem Bereich *Beschreibung* ② angezeigt, wenn Sie den jeweiligen Modus markieren.

Autoren- und Benutzermodus unterscheiden sich in der Speicherung von vorgenommenen Änderungen an der Konsole. Im **Autorenmodus** werden Sie beim Schließen der Konsole gefragt, ob und in welche Datei die Konsole gespeichert werden soll. Im **Benutzermodus** werden Ihre Änderungen automatisch gesichert, sofern dies nicht explizit durch das entsprechende Kontrollfeld ③ ausgeschlossen wurde.

- ▶ Verlassen Sie das Dialogfenster mit *OK*.



### Zugriffsmodus einsehen/ändern

### Snap-In hinzufügen

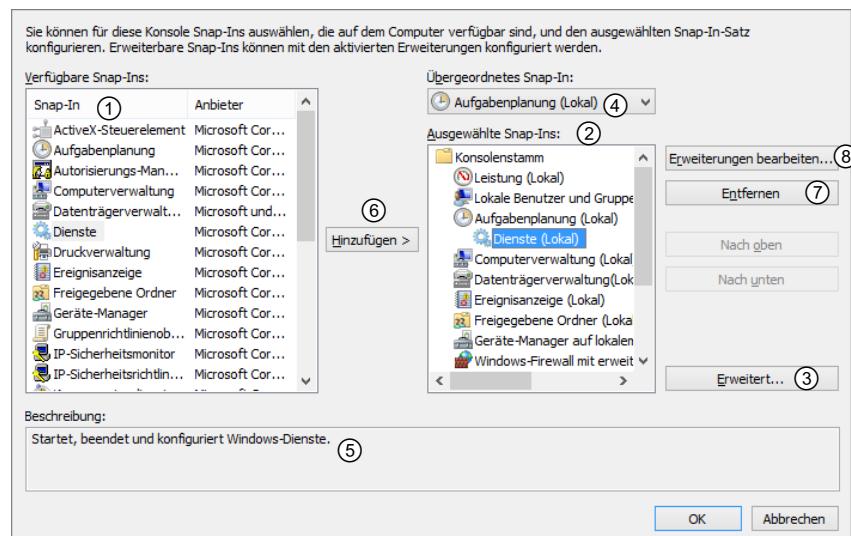
Die Funktionen einer Konsole werden durch die installierten **Verwaltungswerzeuge**, die **Snap-Ins**, bestimmt. Snap-Ins lassen sich nur im Autorenmodus hinzufügen, entfernen bzw. erweitern.

Eine neue Konsole beginnt immer mit dem Konsolenstamm und lässt sich von dort aus erweitern, indem Sie Snap-Ins hinzufügen. Es ist auch möglich, neue Snap-Ins in übergeordnete Snap-Ins einzugliedern, wenn Sie vorher die entsprechende Option aktiviert haben.

- Rufen Sie den Menüpunkt *Datei - Snap-In hinzufügen/entfernen* auf.

Links sehen Sie die verfügbaren Snap-Ins ①, daneben die bereits ausgewählten Snap-Ins ②.

- Falls Sie ein Snap-In nicht dem Konsolenstamm, sondern einem anderen, übergeordneten Snap-In hinzufügen möchten, klicken Sie auf *Erweitert* ③ und aktivieren Sie die Option *Ändern des übergeordneten Snap-Ins zulassen*. Wählen Sie unter *Übergeordnetes Snap-In* ④ das Konsolenelement aus, unter dem Sie ein Snap-In hinzufügen wollen.
- Wählen Sie aus den verfügbaren Snap-Ins eines aus (z. B. *Dienste*). Informationen zu dem jeweiligen Snap-In erhalten Sie im Bereich *Beschreibung* ⑤.
- Klicken Sie auf *Hinzufügen* ⑥.



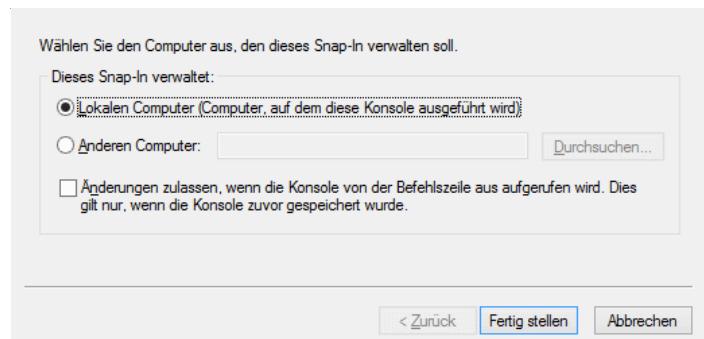
*Snap-In hinzufügen oder entfernen*

Es öffnet sich bei den meisten Snap-Ins ein Dialogfenster, in dem Sie für das jeweilige Snap-In festlegen, für welchen Computer das Snap-In gelten soll.

- Klicken Sie hier auf das Optionsfeld *Lokalen Computer (Computer, auf dem diese Konsole ausgeführt wird)*.

In anderen Fällen (z. B. bei dem Snap-In *ActiveX-Steuerelement*) öffnet sich ein Assistent, der Sie durch den Hinzufügen-Vorgang leitet.

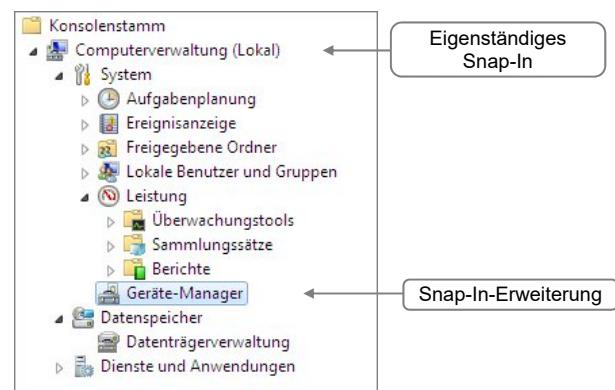
- Beenden Sie das Hinzufügen eines Snap-Ins mit *Fertig stellen*.



*Snap-In hinzufügen*

### Snap-In entfernen

- Wählen Sie den Menüpunkt *Datei - Snap-In hinzufügen/entfernen*.
- Klicken Sie in der Liste der ausgewählten Snap-Ins auf das zu entfernende Snap-In.
- Betätigen Sie die Schaltfläche *Entfernen* ⑦.



*Eigenständige Snap-Ins und Snap-In-Erweiterungen*

## Snap-In erweitern

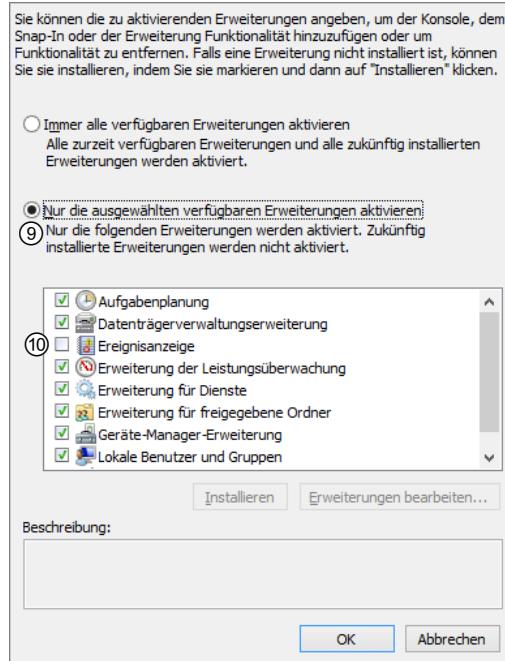
Die von Windows 10 zur Verfügung gestellten eigenständigen Snap-Ins bestehen zum Teil wiederum selbst aus Snap-Ins, den Snap-In-Erweiterungen. In vielen Fällen unterscheiden sich eigenständige und Snap-In-Erweiterungen nicht voneinander. Sie können Snap-In-Erweiterungen hinzufügen oder weglassen, z. B. wenn Sie eine bestimmte Snap-In-Erweiterung an einer anderen Stelle als eigenständiges Snap-In anzeigen möchten.

**Beispiel:** Weil Sie die Snap-In-Erweiterung *Ereignisanzeige* später als eigenständiges Snap-In aktivieren wollen, möchten Sie sie aus dem eigenständigen Snap-In *Computerverwaltung* entfernen.

- ▶ Wählen Sie in der MMC den Menüpunkt *Datei - Snap-In hinzufügen/entfernen*.
- ▶ Wählen Sie das zu bearbeitende Snap-In *Computerverwaltung* aus und klicken Sie auf *Erweiterungen bearbeiten* ⑧.
- ▶ Um vorhandene Snap-Ins zu entfernen, aktivieren Sie im folgenden Dialog das Optionsfeld *Nur die ausgewählten verfügbaren Erweiterungen aktivieren* ⑨.

Nun können Sie das Kontrollfeld für die Snap-In-Erweiterung *Ereignisanzeige* deaktivieren ⑩.

- ▶ Bestätigen Sie mit *OK*.



*Snap-In-Erweiterung bearbeiten*

## 7.5 Aufgabenblocks und Aufgaben erstellen

### Aufgabenblocks und Aufgaben

Eine nützliche Möglichkeit zur Erleichterung von häufigen Arbeiten stellen Aufgaben (engl. Tasks) dar. Dies sind bestimmte Befehle und Abläufe, die auf speziellen Oberflächen, sogenannten **Aufgabenblockansichten** (engl. Taskpads), angeordnet werden. Drei Arten von Befehlstypen existieren:

- ✓ **Menübefehl:** Sie können alle Befehle, die sich mithilfe des Kontextmenüs innerhalb der Konsolenstruktur aufrufen lassen, als Aufgabe definieren.
- ✓ **Shellbefehl:** Sie können aus der Konsole heraus weitere Programme oder Skripts starten.
- ✓ **Navigation:** Sie können eine Aufgabe auch nutzen, um innerhalb der Konsole mithilfe von Favoriten zu bestimmten Orten der Konsolenstruktur zu springen.

**Beispiel:** Da diese Workstation als alleiniger Rechner mit Internetzugang genutzt wird, müssen Sie des Öfteren neue Benutzer anlegen. Außerdem müssen Sie gelegentlich Veränderungen an den Eigenschaften der Benutzerkonten vornehmen und sind das Klicken durch die Unterordner der Computerverwaltung leid. Sie möchten die erforderlichen Arbeitsschritte in Ihrer Konsole direkt aufrufen und bei Bedarf möglichst schnell zur Benutzerübersicht gelangen. Sie möchten also ...

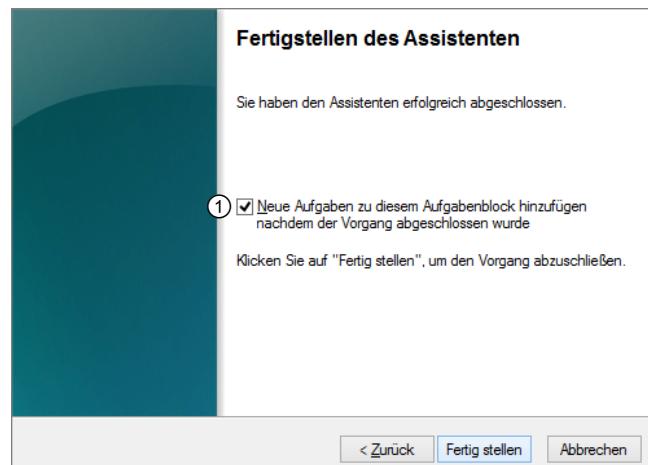
- ✓ einen neuen Aufgabenblock *Benutzerverwaltung* erstellen,
- ✓ eine Menüaufgabe *Neuen Benutzer anlegen* erstellen,
- ✓ eine Navigationsaufgabe *Link zur Benutzerübersicht* erstellen.

## Aufgabenblock erstellen

- ▶ Markieren Sie in der linken Spalte der MMC das Konsolenelement, in dem die Taskpad-Ansicht angezeigt werden soll (z. B. *Computerverwaltung (Lokal)*).
- ▶ Rufen Sie den Menüpunkt *Aktion - Neue Aufgabenblockansicht erstellen* auf.

Ein Assistent leitet Sie durch mehrere Dialogfenster, in denen Sie für den Aufgabenblock die Ansicht des Detailfensters, den Namen (z. B. *Benutzerverwaltung*) und eine Beschreibung festlegen können.

Am Ende starten Sie automatisch (wenn das entsprechende Kontrollfeld ① aktiviert ist) mit *Fertig stellen* den Assistenten für neue Aufgaben.



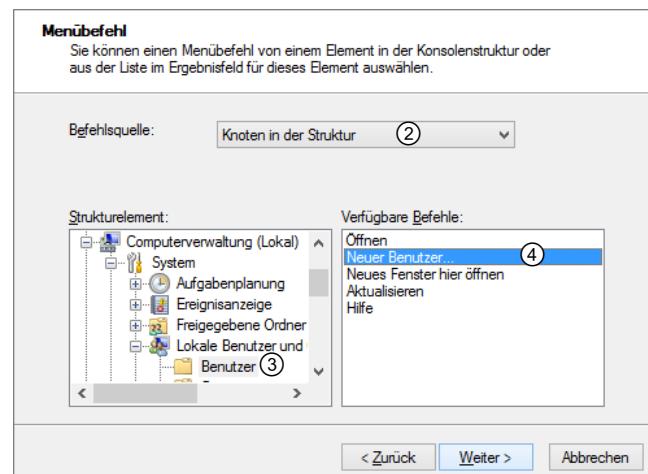
Automatisch den Assistenten für neuen Task starten

## Menübefehl erstellen

- ▶ Im Assistenten für eine neue Aufgabe wählen Sie als Befehlstyp *Menübefehl* aus.
- ▶ Drücken Sie *Weiter*.
- ▶ Als Befehlsquelle wählen Sie im entsprechenden Listenfeld *Knoten in der Struktur* ② aus.
- ▶ Suchen Sie nun in der Konsolenstruktur das Konsolenelement *Benutzer* ③ (unter *Computerverwaltung - System - Lokale Benutzer und Gruppen - Benutzer*) und markieren Sie es.
- ▶ Wählen Sie den Befehl *Neuer Benutzer* ④ aus.
- ▶ Zum Fortsetzen des Assistenten klicken Sie *Weiter*.

In den folgenden Dialogfenstern können Sie einen Namen für die Aufgabe (z. B. *Neuen Benutzer anlegen*) sowie ein Symbol auswählen.

- ▶ Beenden Sie den Assistenten durch einen Klick auf *Fertig stellen*.



Erstellen einer Aufgabe „Neuen Benutzer anlegen“

## Aktuelle Ansicht den Favoriten hinzufügen

Um zu einem bestimmten Punkt in der Konsolenstruktur schnell wechseln zu können, müssen Sie diesen zuerst den Favoriten hinzufügen.

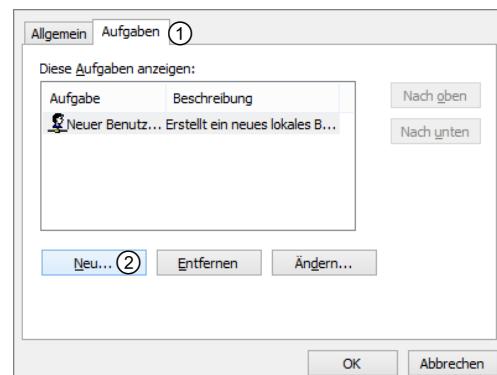
- ▶ Wechseln Sie in der Konsolenstruktur zu dem Konsolenelement *Benutzer* und rufen Sie den Menüpunkt *Favoriten - Zu Favoriten hinzufügen* auf.

Anschließend können Sie dem Favoriten einen Namen geben (z. B. *Benutzerübersicht*).

- ▶ Schließen Sie das Dialogfenster durch Klicken auf *OK*.

## Navigationsbefehl erstellen

- ▶ Wechseln Sie zum erstellten Aufgabenblock *Benutzerverwaltung* (unter *Computerverwaltung*).
- ▶ Rufen Sie den Menübefehl *Aktion - Aufgabenblockansicht bearbeiten* auf.
- ▶ Wechseln Sie in das Register *Aufgaben* ①.
- ▶ Betätigen Sie *Neu* ②.
- ▶ Im Fenster *Assistent für neue Aufgabe* wählen Sie als Befehlstyp das Optionsfeld *Navigation*.
- ▶ Klicken Sie auf *Weiter*.
- ▶ Wählen Sie nun in dem Feld *Favoriten* als Ziel der Verknüpfung den Favoriten *Benutzerübersicht* aus.
- ▶ Setzen Sie den Assistenten durch das Klicken auf *Weiter* fort.

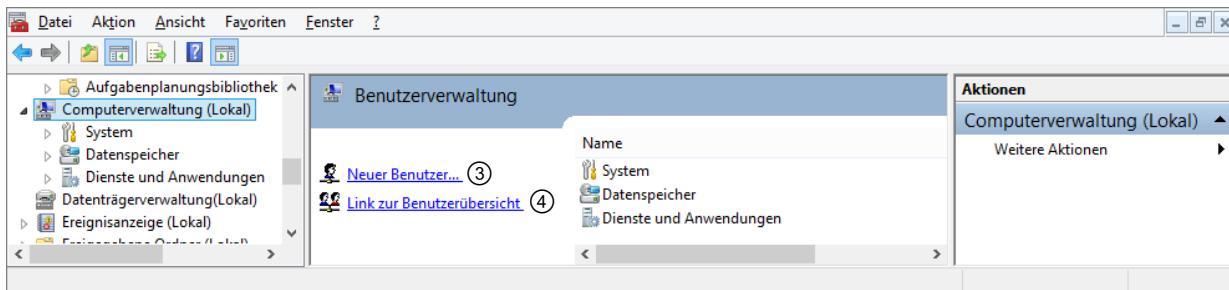


Neue Aufgabe in Aufgabenblock erstellen

In den darauf folgenden Dialogfenstern des Assistenten können Sie einen Namen für die Aufgabe (z. B. *Link zur Benutzerübersicht*) bestimmen und ein Symbol auswählen.

- ▶ Beenden Sie den Assistenten mit *Fertig stellen*.

Sie haben unter dem von Ihnen gewählten Konsolenelement eine neue Aufgabenblockansicht und auf dieser zwei neue Aufgaben erstellt, die Sie durch einen Klick auf die entsprechenden Hyperlinks (③ und ④) aktivieren können.



Aufgabenblockansicht mit hinzugefügten Aufgaben

## 7.6 Konsole sichern und Zugriff beschränken

### Konsole speichern

Die Konsolen werden als Dateien mit der Erweiterung *.msc* gespeichert. Dabei werden die Angaben über die aktivierte Snap-Ins, die Ansicht und Einstellungen der Konsole sowie der Zugriffsmodus gesichert und beim nächsten Öffnen der Konsole wiederhergestellt. Die meisten vordefinierten Konsolen liegen im Verzeichnis *windows\system32*.

- ▶ Rufen Sie den Menüpunkt *Datei - Speichern* unter auf.
- ▶ Stellen Sie den gewünschten Pfad ein.
- ▶ Geben Sie einen Namen ein und klicken Sie auf *Speichern*.

### MMC-Konsole dem eigenen Startbildschirm hinzufügen

- ▶ Speichern Sie die MMC-Konsole im Standardverzeichnis unter *Benutzer\Ihr Benutzername\AppData\Roaming\Microsoft\Windows\Startmenü\Programme\Verwaltung* (kurzer Pfad: *%APPDATA%\Roaming\Microsoft\Windows\Startmenü\Programme\Verwaltung*).

Nun können Sie in MMC über das Menü *Datei - Öffnen* die gespeicherte Konsole laden.

## MMC-Konsole allen Benutzern der Workstation zugänglich machen

- Sichern Sie die Konsole unter *Benutzer\Öffentlich\Öffentlicher Desktop* (kurzer Pfad: %PUBLIC%\Öffentlicher Desktop).

Nun erscheint die Konsole bei allen Benutzern auf dem Desktop und diese können die Konsole entsprechend ihren Rechten öffnen, einsehen und benutzen. Zur häufigen Verwendung empfiehlt sich das Hinzufügen der MMC-Konsole zum Startbildschirm über das Kontextmenü.



Sowohl *Verwaltung* als auch *Öffentlicher Desktop* sind nur sichtbar, wenn in den Ansichtsoptionen des Datei-Explorers das Anzeigen von ausgeblendeten Dateien aktiviert ist.

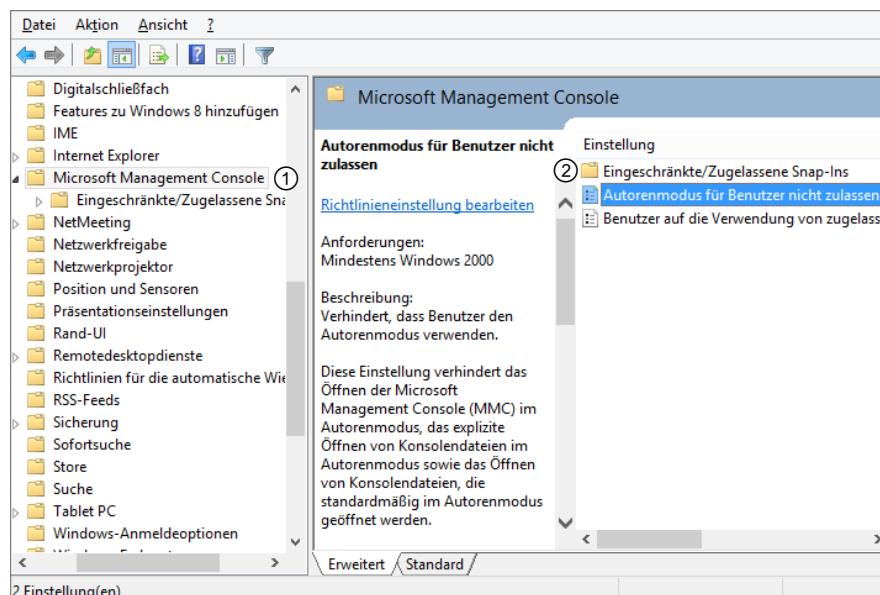
## Zugriff auf Autorenmodus durch Gruppenrichtlinie beschränken

Als Systembetreuer können Sie allen Benutzern dieser Workstation (auch sich selbst) bestimmte MMC-Verwaltungs-Tools zur Verfügung stellen und andere sperren. Dazu müssen Sie eine lokale Gruppenrichtlinie konfigurieren. Wenn Sie in einer Domäne arbeiten, können Sie die Gültigkeit der Gruppenrichtlinie auf bestimmte Benutzer beschränken, indem Sie sie z. B. auf eine Organisationseinheit anwenden.

Voraussetzungen:

- ✓ Sie haben Administratorrechte.
- ✓ Sie wollen für alle Benutzer des Computers die Berechtigungen zur Erstellung und Veränderung von Konsolen beschränken.
- Geben Sie im Startbildschirm gpedit.msc ↩ ein.  
Es öffnet sich die vordefinierte MMC-Konsole *Editor für lokale Gruppenrichtlinien*.
- Wählen Sie in der Konsolenstruktur *Benutzerkonfiguration - Administrative Vorlagen - Windows-Komponenten - Microsoft Management Console* ①.
- Doppelklicken Sie im Detailfenster auf die Richtlinie *Autorenmodus für Benutzer nicht zulassen*.
- Aktivieren Sie im Register *Einstellung* das Optionsfeld *Aktiviert*.  
Wenn Sie diese Richtlinie aktivieren, kann kein Benutzer dieses Computers eine neue oder eine bestehende Konsole im Autorenmodus öffnen.

Durch Aktivieren/Deaktivieren der Richtlinien unter *Eingeschränkte/Zugelassene Snap-Ins* ② können Sie genau festlegen, welche Snap-Ins auf diesem Computer genutzt werden können und welche nicht.



*Einstellungen für den Autorenmodus der MMC*

## 7.7 MMC-Konsole öffnen

### Bestehende Konsole im Standardzugriffsmodus öffnen

- ▶ Öffnen Sie den Explorer und doppelklicken Sie auf die entsprechende Konsolendatei.

### Bestehende Konsole im Autorenmodus öffnen

- ▶ Öffnen Sie den Explorer und klicken Sie mit der rechten Maustaste auf die entsprechende Konsolendatei. Wählen Sie den Menüpunkt *Im Autorenmodus öffnen*.
- oder Geben Sie in einer Eingabeaufforderung <Pfad>\<Konsolename>.msc /A ein.

## 7.8 Windows Server 2012 R2/2016 mit Windows 10 verwalten

### RSAT (Remote Server Administration Tools) installieren

Um Windows Server 2012 R2/2016 mit Windows 10 zu verwalten, bietet Microsoft die Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT) zum Download an (<https://www.microsoft.com/en-us/download/details.aspx?id=45520>).

Die Remoteserver-Verwaltungstools für Windows 10 enthalten

- ✓ den Server-Manager von Windows Server 2012 R2/2016/1709/1803
- ✓ Verwaltungstools der Serverrollen und
- ✓ Features von Windows Server 2012 R2/2016 sowie Windows Server 1709/1803

Über den Server-Manager binden Sie die verschiedenen Server im Netzwerk an, auf denen Windows Server 2012 R2/2016 installiert ist. Sie installieren mit dem Server-Manager in Windows 10 auch auf Servern mit Windows Server 2012/2012 R2/2016/1709/1803 neue Serverrollen, genauso wie auf dem lokalen Server mit Windows Server 2012/2012 R2/2016/1709/1803. Im Server-Manager von Windows Server 2012 R2/2016 können Sie auch andere Server mit Windows Server 2012 R2/2016 im Netzwerk verwalten. Windows Server 1709/1803 stehen nur als Core-Server zur Verfügung.

Die Remoteserver-Verwaltungstools für Windows 10 unterstützen auch die Remoteverwaltung von Servern mit einer Core-Installation oder mit der Minimal Server Graphical Interface-Konfiguration von Windows Server 2012 R2 sowie Windows Server 1709/1803. Allerdings wird die neue Nano-Installation von Windows Server 2016, eine noch eingeschränktere Version des Core-Servers, nicht unterstützt. Hier ist nur eine Verwaltung über die PowerShell oder WMI möglich. Der Nano-Server steht ab Windows Server 1709 und auch im Nachfolger von Windows Server 2016 nur noch als Container-Image zur Verfügung, nicht mehr als eigenständige Installation.

- ✓ Windows 10 installiert RSAT wie jedes andere Update auch. Entfernen Sie vorher alle älteren Versionen der Verwaltungstools oder Remoteserver-Verwaltungstools, auch früherer Vorabversionen sowie Versionen der Tools für verschiedene Sprachen.
- ✓ Wenn Sie Windows 7/8.1 auf Windows 10 aktualisiert haben, müssen Sie die Remoteserver-Verwaltungstools für Windows 10 installieren, Sie können nicht die alten Versionen für Windows 7/8.1 parallel betreiben.



### RSAT einstellen

Nach der Installation finden Sie die Remoteserver-Verwaltungstools im Startmenü in der Alle-Apps-Ansicht. Im Gegensatz zu Windows 7 sind alle Verwaltungstools nach der Installation bereits aktiv.

## 7.9 Virtualisieren mit Windows 10

Mit der Clientversion von Windows 10 stellt Microsoft auch die Virtualisierungstechnik Hyper-V von Windows Server 2016 auf dem Client zur Verfügung. Auf diesem Weg lassen sich auf PCs virtuelle Maschinen erstellen. Allerdings verfügen nur die 64-Bit-Editionen Windows 10 Pro und Enterprise über diese Funktion.

### Hyper-V installieren und verwalten

Die Installation von Hyper-V nehmen Sie über die Aktivierung der Windows-Funktion *Hyper-V* in den Features von Windows 10 vor. Suchen Sie dazu im Startmenü nach dem Programm optionalfeatures und installieren Sie das Feature. Außerdem müssen Sie sicherstellen, dass vor der Installation im BIOS des Servers die Virtualisierungsfunktionen des Prozessors aktiviert sind.



Sie können auch mit Bordmitteln überprüfen, ob der PC generell tauglich für Hyper-V ist. Geben Sie dazu in einer Eingabeaufforderung den Befehl `systeminfo` ein. Im unteren Bereich finden Sie *Anforderungen für Hyper-V*. Hier sind Informationen aufgeführt, ob der PC für Hyper-V geeignet ist.

Nach der Installation finden Sie im Startmenü den Hyper-V-Manager. Über diesen Manager werden virtuelle Computer erstellt und verwaltet. In der Mitte der Konsole sehen Sie nach der Erstellung die verschiedenen virtuellen Computer. Auf der rechten Seite stehen die verschiedenen Befehle zur Verwaltung der virtuellen Computer zur Verfügung. Über den Link *Neu* erstellen Sie einen neuen virtuellen Computer.

Der generelle Ablauf bei der Installation der Computer in einer Hyper-V-Umgebung ist folgender:

- ✓ Sie erstellen virtuelle Netzwerke.
- ✓ Sie erstellen und konfigurieren die virtuellen Computer.
- ✓ Sie installieren das Betriebssystem auf den virtuellen Computern.

### Virtuelle Switches

Alle von Ihnen erstellten virtuellen Computer, auch virtuelle Maschinen genannt, verwenden einen virtuellen Switch auf dem Windows-10-Computer. Dieser verbindet die virtuellen Computer mit den physischen Netzwerkarten des Computers und erlaubt eine Kommunikation der virtuellen Computer mit dem Rest des Netzwerks. Bevor Sie virtuelle Computer installieren, besteht der erste Schritt in der Konfiguration des virtuellen Switches. Dazu steht im Hyper-V-Manager der Bereich *Manager für virtuelle Switches* zur Verfügung.

Zunächst erstellen Sie für die einzelnen physischen Netzwerkarten im Computer jeweils einen virtuellen Switch durch die Auswahl von *Neuer virtueller Switch* und Klick auf *Virtuellen Switch erstellen*. Im Assistenten wählen Sie die physische Netzwerkarte aus, die Sie dem Switch zuweisen wollen und wählen aus, welche Art von Netzwerk Sie dem Switch zuordnen:

<b>Extern</b>	Dieses Netzwerk ermöglicht dem virtuellen Computer eine Kommunikation mit dem Netzwerk und zwischen virtuellen Computern auf dem Host. Sie können im Hyper-V-Manager immer nur ein externes Netzwerk pro verfügbarer Netzwerkarte erstellen, aber mehrere virtuelle Computer können sich dieses externe Netzwerk und damit die Geschwindigkeit der Karte teilen.
<b>Intern</b>	Diese Netzwerke erlauben eine Kommunikation der virtuellen Computer untereinander auf dem physischen Host. Die Computer können nicht mit dem Netzwerk kommunizieren, außer mit dem Hyper-V-Host selbst und den anderen virtuellen Computern. Dafür ist für diese Verbindung keine Netzwerkarte erforderlich, da die Verbindung virtuell stattfindet.
<b>Privat</b>	Diese Netzwerke erlauben eine Kommunikation zwischen den einzelnen virtuellen Computern auf dem Host. Die Kommunikation mit dem Host selbst ist bei diesem Netzwerk nicht möglich.

Haben Sie die physischen Netzwerkarten des Computers einem virtuellen Switch zugeordnet, lassen sich diese den einzelnen virtuellen Computern zuweisen. Dies erfolgt beim Erstellen der virtuellen Maschine (VM) oder nachträglich in den Einstellungen einer VM über den Bereich *Netzwerkkarte*. Die erste Einstellung besteht in der Zuweisung des virtuellen Switches. Anschließend lassen sich Einstellungen vornehmen.

Nach der Erstellung der virtuellen Netzwerke finden Sie auf dem Host in den Netzwerkverbindungen die erstellten Verbindungen wieder. Um die Netzwerkverbindungen anzuzeigen, tippen Sie `ncpa.cpl` im Suchfeld des Startmenüs. Wichtig in diesem Bereich ist, dass Sie zukünftig IP-Einstellungen nicht mehr in der physischen Netzwerkverbindung vornehmen, sondern in den Einstellungen des virtuellen Switches. Diesen verwendet zukünftig auch der physische Windows-10-Host für die Kommunikation mit dem Internet, außer Sie verfügen über mehrere Netzwerkadapter im Windows-PC.

## Virtuelle Computer erstellen und installieren

Nachdem Sie die virtuellen Netzwerke für Ihre virtuellen Computer angelegt haben, erstellen Sie die Computer, die Sie virtualisieren wollen. Bei der Erstellung der virtuellen Computer können Sie als Installationsmedium entweder eine DVD auswählen oder eine \*.iso-Datei. Um virtuelle Computer zu erstellen, gehen Sie wie folgt vor:

- ▶ Starten Sie den Hyper-V-Manager.  
Warten Sie, bis der Manager eine Verbindung zum lokalen Computer aufgebaut hat.
- ▶ Klicken Sie auf *Neu - Virtueller Computer*.  
*oder*  
Verwenden Sie das Kontextmenü des Hosts zum Erstellen eines virtuellen Computers.
- ▶ Geben Sie auf der nächsten Seite den Namen des Computers ein.  
Der Name hat nichts mit dem eigentlichen Computernamen zu tun. Hierbei handelt es sich um den Namen in der Konsole.
- ▶ Aktivieren Sie die Option *Virtuellen Computer an einem anderen Speicherort* speichern.  
Standardmäßig speichert der Assistent die Daten des Computers im Installationsverzeichnis von Hyper-V.  
Sie können dieses Verzeichnis im Hyper-V-Manager über Hyper-V-Einstellungen festlegen. Hier nehmen Sie darüber hinaus weitere Einstellungen vor, die für Hyper-V selbst und alle virtuellen Computer gemeinsam gelten.
- ▶ Wählen Sie das Verzeichnis aus, in dem Sie die Daten des virtuellen Computers speichern wollen.  
Sie sollten für jeden Computer einen eigenen Pfad verwenden.
- ▶ Wählen Sie aus, wie viel Arbeitsspeicher Sie dem Computer zuweisen wollen.  
Generell sollten Sie darauf achten, dass der gemeinsame Arbeitsspeicher aller virtuellen Server nicht den physischen Speicher des Hosts überschreitet. Der Arbeitsspeicher des virtuellen Computers lässt sich auch nach der Installation jederzeit anpassen.

Sie können an dieser Stelle auch den **dynamischen Arbeitsspeicher** aktivieren. Diese Funktion ermöglicht es, dass virtuelle Computer, die nicht ihren gesamten zugewiesenen Arbeitsspeicher ausnutzen, diesen Arbeitsspeicher anderen virtuellen Computern zur Verfügung stellen können. Virtuelle Computer können sich über Hyper-V den Arbeitsspeicher teilen. Sie können für virtuelle Computer in den Einstellungen einen Startwert und einen maximalen Wert für den Arbeitsspeicher zuteilen. Die Zuteilung des tatsächlichen Arbeitsspeichers steuert Hyper-V auch auf Basis der Prioritäten, die Sie den virtuellen Computern zuweisen. Um Dynamic Memory zu nutzen, aktivieren Sie die Option *Dynamischen Arbeitsspeicher für diesen virtuellen Computer verwenden*. An dieser Stelle können Sie aber keine Werte konfigurieren. Dazu rufen Sie später über das Kontextmenü die Einstellungen auf und klicken auf *Arbeitsspeicher*.

- ▶ Wählen Sie das Netzwerk aus, das Sie für die virtuellen Server erstellt haben.  
Hier stehen die virtuellen Switches zur Verfügung, die Sie im Vorfeld angelegt haben.
- ▶ Auf den nächsten Seiten aktivieren Sie die Option *Virtuelle Festplatte erstellen* und wählen den Pfad und die Größe aus.

- ▶ Im nächsten Schritt wählen Sie aus, wie Sie das Betriebssystem installieren wollen.  
Am besten aktivieren Sie die Option *Physisches CD/DVD-Laufwerk oder Abbild-Datei*.
- ▶ Schließen Sie auf der nächsten Seite die Erstellung der virtuellen Maschine ab, lassen Sie diese aber nicht starten.

Nach der erfolgreichen Erstellung der virtuellen Computer können Sie im Hyper-V-Manager weitere Einstellungen vornehmen.

- ▶ Rufen Sie dazu im Kontextmenü des virtuellen Computers den Eintrag *Einstellungen* auf. Klicken Sie in den Einstellungen des Computers auf *Hardware hinzufügen*, wenn Sie zusätzliche Hardware zur virtuellen Maschine hinzufügen wollen.
- ▶ Legen Sie die Installations-DVD in das Laufwerk des physischen Hosts oder laden Sie die \*.iso-Datei in den Einstellungen des virtuellen Computers.
- ▶ Klicken Sie im Hyper-V-Manager den virtuellen Computer mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Starten* aus.
- ▶ Um sich mit der virtuellen Maschine zu verbinden, klicken Sie im Hyper-V-Manager im Kontextmenü der virtuellen Maschine auf *Verbinden*.

Anschließend startet der Installations-Assistent den Server. Beenden Sie das Verbindungsfenster zum virtuellen Computer, bleibt dieser weiter gestartet. Sie sehen den Status der entsprechenden virtuellen Computer im Hyper-V-Manager.

### Prüfpunkte von virtuellen Servern erstellen

Hyper-V ermöglicht die Erstellung von Prüfpunkten. Die Prüfpunkte bieten die Möglichkeit, einen Server vor einer Konfigurationsänderung zu sichern. Den entsprechenden Befehl finden Sie im Kontextmenü der virtuellen Computer im Hyper-V-Manager.

Während der Erstellung bleibt der Computer online und steht weiterhin den Anwendern zur Verfügung. Die erstellten Prüfpunkte zeigt der Hyper-V-Manager im mittleren Bereich der Konsole an. Im Kontextmenü von Prüfpunkten stehen verschiedene Möglichkeiten zur Verfügung:

<b>Einstellungen</b>	Hierüber rufen Sie die Einstellungen des virtuellen Computers auf, zu dem dieser Prüfpunkt gehört.
<b>Anwenden</b>	Wählen Sie diese Option aus, setzt der Assistent den virtuellen Computer wieder auf den Stand zurück, an dem Sie diesen Prüfpunkt erstellt haben.
<b>Umbenennen</b>	Mit dieser Option weisen Sie dem Prüfpunkt einen anderen Namen zu.
<b>Prüfpunkt löschen</b>	Löscht den Prüfpunkt und die dazugehörigen Daten
<b>Prüfpunkt-Unterstruktur löschen</b>	Diese Option löscht den aktuellen Prüfpunkt sowie alle Sicherungen, die Sie nach dem Prüfpunkt erstellt haben und die auf diesen aufbauen.

### Virtuelle Computer exportieren und importieren

Über das Kontextmenü eines virtuellen Computers können Sie diesen exportieren. Auf einem anderen Windows-10-Computer haben Sie dann die Möglichkeit, den gleichen Computer wieder zu importieren. Im Hyper-V-Manager können Sie über den Assistenten *Virtuellen Computer importieren* den Vorgang durchführen.

## 7.10 Übung

### Mit MMC und Hyper-V arbeiten

Übungsdatei: --

Ergebnisdatei: *Uebung07\_E.pdf*

1. Wie erstellen Sie eine eigene MMC-Konsole?
2. Wie installieren Sie Hyper-V?

# 8 Netzwerkeinstellungen verwalten

## In diesem Kapitel erfahren Sie

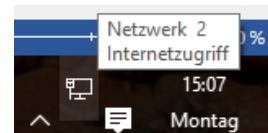
- ✓ wie Sie einen Rechner für das Netzwerk konfigurieren können
- ✓ wie Sie einen Rechner in eine Domäne oder Arbeitsgruppe aufnehmen können
- ✓ wie Sie Netzwerkprotokolle hinzufügen oder entfernen können
- ✓ wie ein Internetzugang eingerichtet und kontrolliert werden kann
- ✓ wie ein Client remote verwaltet werden kann

## Voraussetzungen

- ✓ Netzwerkgrundlagen

## 8.1 Netzwerkidentifikation ändern

Ist Ihr Computer korrekt mit dem Netzwerk verbunden, zeigt Windows ein entsprechendes Symbol unten rechts in der Taskleiste an. Klicken Sie auf das Symbol, zeigt Windows weitere Informationen an. Fahren Sie mit der Maus über das Symbol, zeigt Windows auch an, ob der PC über eine Internetverbindung verfügt. Bei fehlender Internetverbindung erscheint ein Ausrufezeichen, bei fehlender physischer Netzwerkverbindung ein rotes x.



Die Konfiguration der Netzwerkverbindungen hat Microsoft seit Windows 10, Version 1709 verbessert. In den Netzwerkeinstellungen, die sich über das Kontextmenü der Netzwerkverbindungen in der Taskleiste anzeigen lassen, erkennen Sie, ob Sie mit dem Internet verbunden sind. Das ist bereits seit längerer Zeit so.

Mit *Verbindungseigenschaften ändern* können Sie festlegen, ob die Netzwerkverbindung *Privat* oder *Öffentlich* ist. Nutzen Sie ein fremdes WLAN, sollten Sie die Einstellung auf *Öffentlich* setzen, da Windows dadurch sicherer im Netzwerk unterwegs ist. Zuhause verwenden Sie die Einstellung *Privat*. Dadurch lässt sich auch die Anbindung an Unternehmensnetzwerke vereinfachen und sicherer betreiben.

### Namen als Basis der Identifikation in einem Netzwerk

In jedem Netzwerk benötigen alle Computer eine Identifikation durch einen eindeutigen Namen und/oder eine IP-Adresse. Da in vielen Netzwerken die Verwaltung der Protokolleinstellungen durch einen DHCP-Server erfolgt, wird die IP-Adresse meist automatisch vergeben. Auch andere wichtige IP-Adressen (DNS-Server, Standardgateway) können über DHCP automatisch an die Computer übermittelt werden.

### Netzwerkidentifikation einsehen

Windows 10 verwendet standardmäßig das DNS-Namenskonzept, das auch bei der Namensvergabe im Internet eingesetzt wird. Dabei setzt sich ein Netzwerkname aus dem individuellen Rechnernamen sowie einem Anhang (DNS-Suffix) zusammen, der Informationen über den Namensraum und die Domäne gibt. Die einzelnen Bereiche des Namens werden durch Punkte voneinander getrennt.

Ein Beispiel wäre *Rechner25.Verwaltung.Herdt.de*.

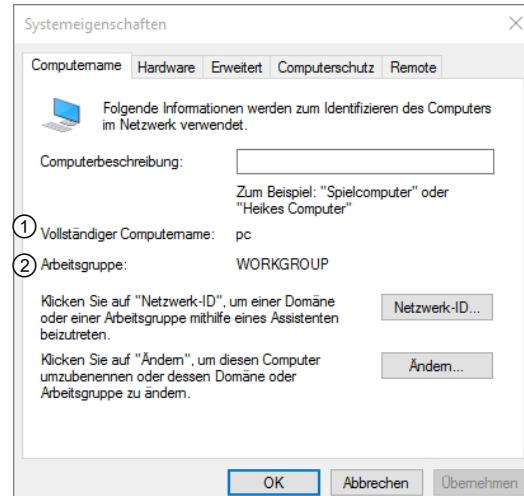
Um einen Computer mit dem Netzwerk zu verbinden, muss zuerst die Netzwerkkarte im Geräte-Manager erkannt und installiert werden.

- ✓ Ist der Treiber Ihrer Netzwerkkarte nicht ordnungsgemäß installiert, ist in Windows 10 möglicherweise kein Treiber für die Netzwerkkarte integriert. Sie sollten nicht einfach einen alten Treiber installieren, sondern auf der Homepage des Herstellers prüfen, ob es einen aktuellen Windows-10-Treiber gibt, und diesen installieren. Finden Sie keinen Treiber, funktionieren aber auch Treiber für Windows 7/8.1. Allerdings sind alte Treiber nicht empfehlenswert. In diesem Fall sollten Sie den Adapter ersetzen.
- ✓ Den Geräte-Manager (vgl. Abschnitt 6.10) finden Sie in Windows 10 über *Systemsteuerung - System und Sicherheit - System*, Link *Geräte-Manager* auf der linken Seite des Fensters. Alternativ tippen Sie `devmgmt.msc` im Startmenü ein oder verwenden Falls Sie nicht als Administrator angemeldet sind, meldet sich beim Aufruf des Geräte-Managers die Benutzerkontensteuerung.



Während der Installation von Windows wurden Sie aufgefordert, einen Namen für den Computer zu vergeben. Sie können diesen Namen später ändern:

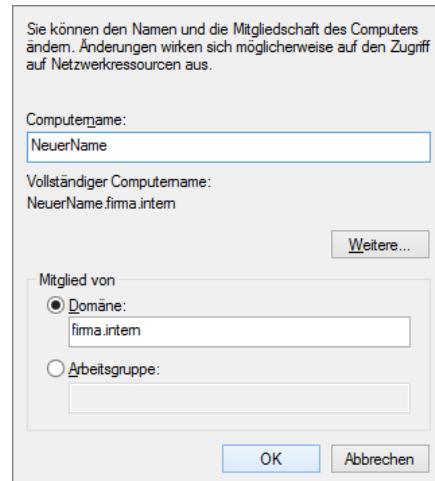
- Wählen Sie im Schnellzugriffsmenü den Kontextmenüpunkt *System* aus. Alternativ suchen Sie im Startmenü nach `sysdm.cpl` und starten das Fenster direkt.
- Klicken Sie auf **Ändern**.
- ✓ Bei *Vollständiger Computername* ① können Sie den gesamten Namen des Rechners inklusive DNS-Suffix sehen.
- ✓ Bei *Arbeitsgruppe* (bzw. *Domäne*) ② können Sie sehen, welcher Domäne oder Arbeitsgruppe der Rechner angehört.



*Computername anzeigen lassen*

### Computernamen ändern

- Geben Sie den neuen Namen ein. Das Feld, in dem der Name steht, ist automatisch markiert. Sollten Sie sich in einer Domäne befinden, werden Sie nach dem Benutzernamen und dem Kennwort eines Kontos gefragt, das berechtigt ist, den Rechner in der Domäne umzubenennen (Domänen-Admin oder höher).
- Klicken Sie auf *Weitere*, um das primäre DNS-Suffix des Computers zu verändern, das Kontrollfeld zur DNS-Suffix-Anpassung zu aktivieren oder den NetBIOS-Namen einzusehen.
- Bestätigen Sie Ihre Änderungen mit **OK**.



*Computernamen ändern*

### Computer einer Arbeitsgruppe hinzufügen

Um einen Computer in eine Arbeitsgruppe aufzunehmen, muss der Name der existierenden Arbeitsgruppe bekannt sein. Verfügt der Computer bereits über eine funktionierende Netzwerkanbindung, können Sie im Explorer von Windows die Netzwerkumgebung öffnen. Es werden aktive Arbeitsgruppen und Domänen des Netzwerks mit ihren Namen angezeigt. Falls Sie eine Arbeitsgruppe erst erstellen möchten, geben Sie einen neuen Namen an.

- Klicken Sie im Dialogfenster *Systemeigenschaften* im Register *Computername* auf **Ändern**.
  - Aktivieren Sie das Optionsfeld *Arbeitsgruppe*, geben Sie den Namen der Arbeitsgruppe ein, der Sie beitreten möchten, und bestätigen Sie mit **OK**.
- Sie sehen nun ein Meldungsfenster, das Sie in der Arbeitsgruppe willkommen heißt.
- Starten Sie den Computer neu, um die Änderungen zu übernehmen.

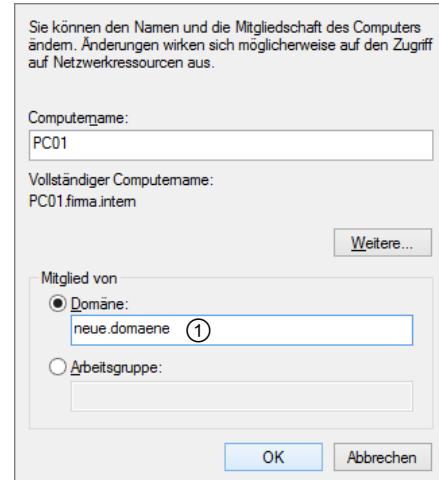
## Computer einer Domäne hinzufügen

Um einen Computer in eine Domäne aufzunehmen, benötigen Sie den Namen der Domäne (eventuell auch der Anmeldedomäne) sowie Benutzername und Kennwort eines Domänenbenutzers, vorausgesetzt es wurde vorher von der Administration schon ein neues Computerkonto in der Domäne erstellt. Falls es noch kein Computerkonto gibt, sind Domänen-Administratorrechte (oder höher) erforderlich, um den Computer der Domäne hinzuzufügen.

Eventuell müssen Sie in den Netzwerkeinstellungen einen anderen DNS-Server eintragen (vgl. Abschnitt 8.2), damit die Domäne gefunden werden kann.

So fügen Sie den Computer einer Domäne hinzu:

- ▶ Klicken Sie im Dialogfenster *Systemeigenschaften* im Register *Computername* auf **Ändern**.
- ▶ Wählen Sie die Option *Domäne* aus und geben Sie den Namen ① der Domäne an, der der Computer beitreten soll.  
Geben Sie nun Benutzername und Kennwort eines Kontos ein, das berechtigt ist, den Rechner in die Domäne aufzunehmen. Standardmäßig sind hierzu die Domänen-Admins berechtigt.  
Sie sehen nun ein Meldungsfenster, das Sie in der Domäne willkommen heißt.
- ▶ Starten Sie den Computer neu, um die Änderungen zu übernehmen und sich in der Domäne anzumelden.

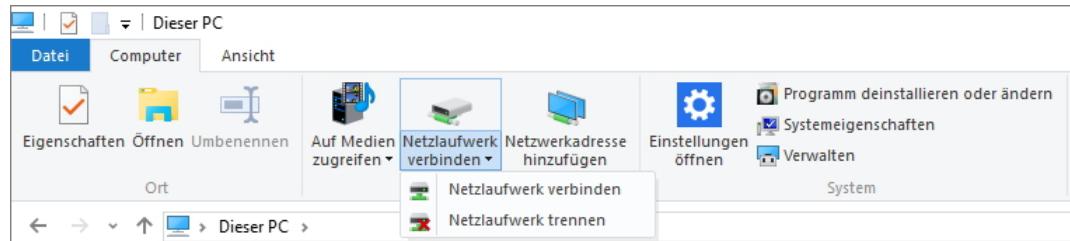


*Beitritt zu einer Domäne*

## Verbinden von Freigaben im Netzwerk als Netzlaufwerk

Wenn Sie eine Freigabe eines anderen Computers im Netzwerk als Laufwerk auf Ihrem Computer verbinden wollen, öffnen Sie den Explorer und klicken im Navigationsbereich auf *Dieser PC*.

- ▶ Wählen Sie im Menüband den Eintrag *Netzlaufwerk verbinden* aus.



*Verbinden eines Netzlaufwerks im Explorer*

- ▶ Geben Sie den Freigabenamen im Feld *Ordner* ein.  
Die Syntax dazu lautet: \\<Computername oder IP-Adresse>\<Name der Freigabe>.  
**oder** Klicken Sie auf *Durchsuchen* und dann doppelt auf den Computer, auf dem sich die Freigabe befindet, mit der Sie sich verbinden wollen.
- ▶ Klicken Sie auf *Fertig stellen*, öffnet sich eventuell ein Anmeldefenster, in dem Sie die Authentifizierungsdaten eines Benutzers auf dem Remotecomputer eingeben müssen.

Wenn Sie sich am Computer mit dem gleichen Benutzernamen und Kennwort anmelden wie auf dem Computer, auf dem Sie die Freigabe öffnen, müssen Sie keine Authentifizierung eingeben, auch nicht, wenn beide Computer in der gleichen Active Directory-Gesamtstruktur sind. Hier erkennt Windows 10 automatisch, dass es sich um den entsprechenden Benutzer handelt.

### Mit `net use` arbeiten

Eine weitere Möglichkeit, Netzlaufwerke zu verbinden, steht Ihnen über die Eingabeaufforderung mit dem Befehl `net use` zur Verfügung.

Eine Eingabeaufforderung öffnen Sie durch Eintippen von `cmd` auf der Startseite. Alternativ drücken Sie und geben den Befehl `cmd` im Ausführen-Dialogfeld ein. Rechtsklick in die linke untere Bildschirmcke (alternativ und den Eintrag *Eingabeaufforderung* oder *Eingabeaufforderung (Administrator)* anklicken ist eine weitere Möglichkeit.



<code>net use</code>	Zeigt alle verbundenen Netzlaufwerke an
<code>net use &lt;Laufwerksbuchstabe&gt;: /del</code>	Trennt das angegebene Netzlaufwerk. Verwenden Sie *, trennt Windows alle Netzlaufwerke.
<code>net use &lt;Laufwerksbuchstabe&gt;: \\&lt;Computer mit Freigabe&gt;\&lt;Freigabename&gt;</code>	Durch Eingabe dieses Pfads verbinden Sie das Netzlaufwerk. Verwenden Sie *, aktiviert Windows den nächsten freien Buchstaben.

Sie können den Befehl auch mit der Syntax `net use <Laufwerksbuchstabe>: \\<Computer mit Freigabe>\<Freigabename> <Benutzername> <Kennwort>` angeben, um ein Laufwerk mithilfe eines anderen Benutzers als dem derzeitig angemeldeten zu verbinden.



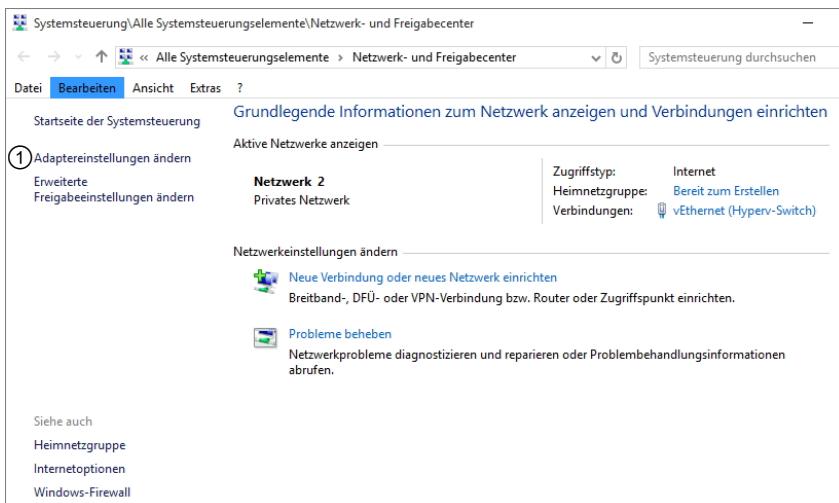
Verbundene Netzlaufwerke zeigt Windows im Explorer an. Sie können verbundene Laufwerke per Rechtsklick wieder trennen.

## 8.2 Netzwerkeinstellungen ändern

### Aktuelle Einstellungen einsehen

Sie können das Netzwerk- und Freigabecenter über die Systemsteuerung oder über das Kontextmenü des Netzwerk-Symbols in der Taskleiste starten. Das funktioniert in neueren Versionen von Windows 10 nicht mehr. Ab Windows 10, Version 1709 starten Sie das Freigabecenter über den Link *Netzwerk- und Freigabecenter*, wenn Sie im Traybereich der Taskleiste über das Kontextmenü der Netzwerkverbindung *Netzwerk- und Internet-einstellungen öffnen* ausgewählt haben.

- ▶ Klicken Sie auf *Adapttereinstellungen ändern* ①. Diesen Bereich erreichen Sie schneller, wenn Sie über das Startmenü direkt `ncpa.cpl` aufrufen.



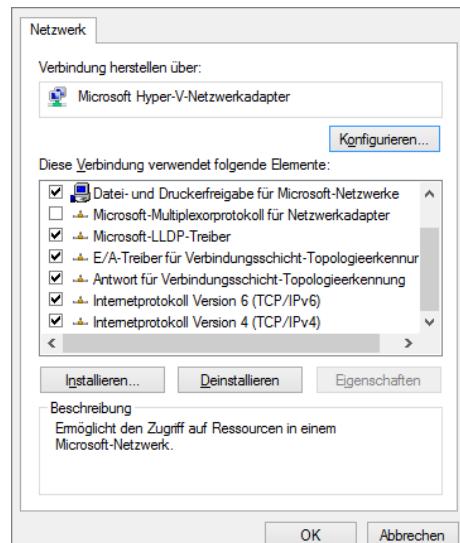
Das Netzwerk- und Freigabecenter von Windows 10

- ▶ Klicken Sie im Kontextmenü der Ethernet-Verbindung auf *Status*, um Informationen über diese Verbindung zu bekommen.
- ▶ Rufen Sie anschließend im Kontextmenü der Verbindung den Menüpunkt *Eigenschaften* auf.
- ▶ Die Einstellungen der Netzwerkkarten erreichen Sie noch schneller, wenn Sie nach *ncpa.cpl* suchen.

Im Register *Netzwerk* sehen Sie eine Übersicht über die aktivierte Komponenten und Protokolle, die an diese Netzwerkkarte gebunden sind.

Sie können die Eigenschaften einer Komponente einsehen bzw. verändern, weitere Komponenten installieren sowie eine installierte Komponente deinstallieren.

Im Kontextmenü von Netzwerkverbindungen stehen Ihnen folgende Optionen zur Verfügung:



*Eigenschaften der Ethernet-Verbindung*

<b>Deaktivieren</b>	Wenn Sie diese Option auswählen, wird die Verbindung zum Netzwerk getrennt, die Netzwerkkarte wird im Geräte-Manager deaktiviert. Die Karte verhält sich so, als wäre sie nicht installiert.
<b>Status</b>	Wenn Sie diesen Menüpunkt auswählen, werden Ihnen ausführliche Informationen über die Konfiguration der Netzwerkverbindung angezeigt sowie die Datenpakete, die über das Netzwerk gesendet wurden. Sie erkennen, mit welcher Geschwindigkeit die Verbindung aufgebaut ist, wie lange die Netzwerkverbindung besteht und wie viele Datenpakete empfangen und gesendet worden sind. Klicken Sie auf die Schaltfläche <i>Details</i> , werden Ihnen ausführlichere Informationen über die Konfiguration der Netzwerkverbindung angezeigt. Sie erkennen die IP-Adresse, die MAC-Adresse sowie eine Vielzahl weiterer Informationen, die vor allem bei der Fehlersuche hilfreich sein können.
<b>Diagnose</b>	Startet einen Assistenten, der die Konfiguration des Adapters überprüft und Vorschläge zur Problemlösung unterbreitet
<b>Verbindungen überbrücken</b>	Wenn Sie diese Option aus dem Kontextmenü einer Netzwerkverbindung auswählen, können Sie den Computer als Verbindung zwischen zwei Netzwerken einsetzen.

### TCP/IP als Standardprotokoll

Windows 10 unterstützt wie schon seine Vorgänger beide Versionen des IP-Protokolls. Sowohl IPv4 als auch IPv6 sind standardmäßig installiert und aktiviert.

### TCP/IP konfigurieren

Standardeinstellungen bei Verwendung von Microsoft TCP/IP sind:

<b>Dynamische IP-Konfiguration</b>	Die dynamische IP-Konfiguration ist standardmäßig aktiviert. Ist ein DHCP-Server im Netzwerk vorhanden, erhält der Computer automatisch eine IP-Adresse zugewiesen.
<b>IP-Autokonfiguration</b>	Die IP-Autokonfiguration (APIPA, Automatic Private IP Addressing) ist ebenfalls standardmäßig aktiviert. Damit kann sich der Computer selbst eine IP-Adresse zuweisen, falls kein DHCP-Server antwortet.



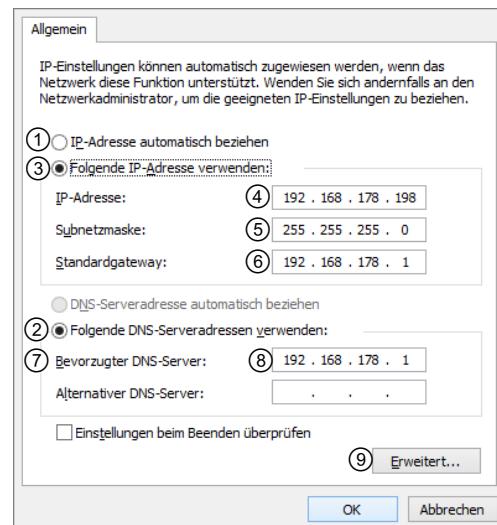
Die fehlerhafte Vergabe von IP-Adressen führt zu ernsten Störungen der Netzwerkkommunikation.

## IPv4-Adresse vergeben

Standardmäßig ist das Optionsfeld *IP-Adresse automatisch beziehen* ① aktiviert und die IP-Adresse und die DNS-Server-Adresse werden automatisch vom DHCP-Server bezogen ②.

In folgenden Fällen jedoch müssen Sie eine konstante IP-Adresse vergeben:

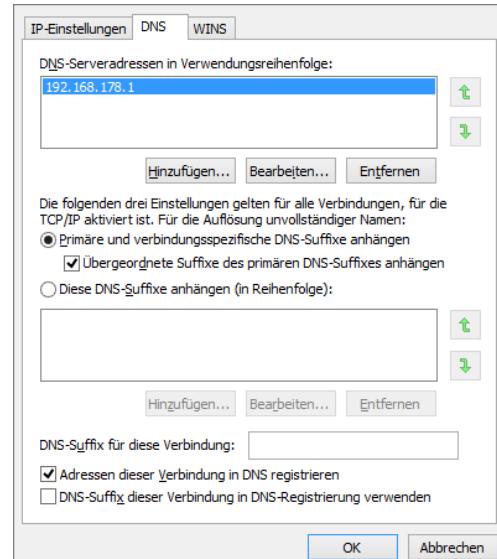
- ✓ wenn der Rechner immer unter der gleichen IP-Adresse erreichbar sein soll,
- ✓ wenn kein DHCP-Server im Netzwerk vorhanden ist und IP-Autokonfiguration unerwünscht ist.
- ▶ Markieren Sie im Dialogfenster *Eigenschaften von Verkabelte Ethernet-Verbindung* das Internetprotokoll Version 4 (TCP/IPv4) und klicken Sie auf *Eigenschaften*.
- ▶ Aktivieren Sie das Optionsfeld *Folgende IP-Adresse verwenden* ③.
- ▶ Geben Sie eine eindeutige IP-Adresse in das Feld ④ ein. Durch Betätigen der Taste  bzw. können Sie den Cursor in den nächsten Block setzen. Geben Sie die Subnetzmaske Ihres Netzwerks in das Feld ⑤ ein.
- ▶ Bestätigen Sie mit *OK*.
- Die Änderungen werden erst wirksam, wenn Sie alle Einstellungsfenster geschlossen haben.
- ▶ Geben Sie unter ⑥ die Standardgateway-Adresse ein, die Ihnen vom Netzwerkadministrator mitgeteilt wurde.



*TCP/IP konfigurieren*

## Einstellungen für DNS-Server vornehmen

- ▶ Aktivieren Sie das Optionsfeld ⑦ und geben Sie unter ⑧ die IP-Adressen der DNS-Server ein, die Ihnen vom Netzwerkadministrator mitgeteilt wurden.
  - ▶ Falls Sie weitere Einstellungen zu DNS vornehmen möchten, klicken Sie auf *Erweitert* ⑨ (in Abb. *TCP/IP konfigurieren*) und wechseln Sie zum Register *DNS*.
- Dort können Sie weitere DNS-Server angeben, die Adressen bearbeiten sowie die Reihenfolge der DNS-Server anpassen. Sie können hier auch die DNS-Suffixe definieren, die automatisch angehängt werden sollen, wenn unvollständige Namen aufzulösen sind.



*Konfiguration der DNS-Einstellungen*

## DNS-Namensauflösung in Active Directory verstehen

Auf der Registerkarte *DNS* in den erweiterten IP-Einstellungen von Netzwerkkarten werden notwendige Einstellungen vorgenommen, um Windows 10 besser in eine Windows-Domäne einzubinden. Die Einstellungen sind sehr wichtig für das Verständnis von DNS und die Namensauflösung in Active Directory. Zunächst sind standardmäßig die folgenden Optionen aktiviert:

- ✓ Primäre und verbindungsspezifische DNS-Suffixe anhängen
- ✓ Übergeordnete Suffixe des primären DNS-Suffixes anhängen
- ✓ Adressen dieser Verbindung in DNS registrieren

Die einzelnen Optionen spielen bei der Namensauflösung in einer DNS-Infrastruktur eine erhebliche Rolle:

✓ **Primäre und verbindungsspezifische DNS-Suffixe anhängen**

Durch die Aktivierung dieser Option wird festgelegt, dass der Rechner versucht, bei der Auflösung von Rechnernamen immer **automatisch** das konfigurierte primäre DNS-Suffix des eigenen Computernamens anzuhängen. Wollen Sie zum Beispiel einen Rechnernamen mit der Bezeichnung *dc01* auflösen, versucht der Rechner eine Namensauflösung nach *dc01.contoso.com*, wenn das primäre DNS-Suffix des Computers *contoso.com* ist.

✓ **Übergeordnete Suffixe des primären DNS-Suffixes anhängen**

Diese Option bedeutet, dass auch **die Namen von übergeordneten Domänen** bei der Namensauflösung verwendet werden. Wenn Sie zum Beispiel in einer untergeordneten Domäne mit der Bezeichnung *muenchen.de*.*contoso.com* einen Servernamen *dc05* auflösen wollen, versucht der Rechner zunächst die Auflösung über *dc05.muenchen.de.contoso.com*, falls dies das primäre DNS-Suffix des Computers ist. Im Anschluss wird versucht, den Namen über *dc05.de.contoso.com* und dann über *dc05.contoso.com* aufzulösen, da diese Domänen der Domäne *muenchen.de.contoso.com* übergeordnet sind.

✓ **DNS-Suffix für diese Verbindung**

Zusätzlich haben Sie noch die Möglichkeit, in diesem Bereich ein weiteres **beliebiges DNS-Suffix** einzutragen. Wenn der Rechner den eingegebenen Namen bei seinem konfigurierten DNS-Server nicht über sein eigenes primäres DNS-Suffix finden kann, versucht er es mit dem DNS-Suffix in diesem Feld. Wollen Sie zum Beispiel den Servernamen *dc06* auflösen, versucht der Computer zunächst die Auflösung in *dc06.contoso.com*, sofern das sein primäres DNS-Suffix ist. Tragen Sie im Feld *DNS-Suffix für diese Verbindung* noch ein Suffix in der Form *muenchen.de.microsoft.com* ein, versucht der Computer, auch den Namen nach *dc06.muenchen.de.microsoft.com* aufzulösen.

✓ **Adressen dieser Verbindung in DNS registrieren**

Auch diese Option ist bereits standardmäßig aktiviert. Ein DNS-Server unter Windows Server hat die Möglichkeit, **Einträge dynamisch** zu registrieren. Durch dieses dynamische DNS müssen Hosteinträge nicht mehr manuell durchgeführt werden. Sobald sich ein Rechner im Netzwerk anmeldet, versucht er, seinen FQDN beim konfigurierten DNS-Server automatisch einzutragen, sofern diese Option nicht deaktiviert wurde. Dieser Punkt ist für die interne Namensauflösung in einem Active Directory-Netzwerk von sehr großer Bedeutung.

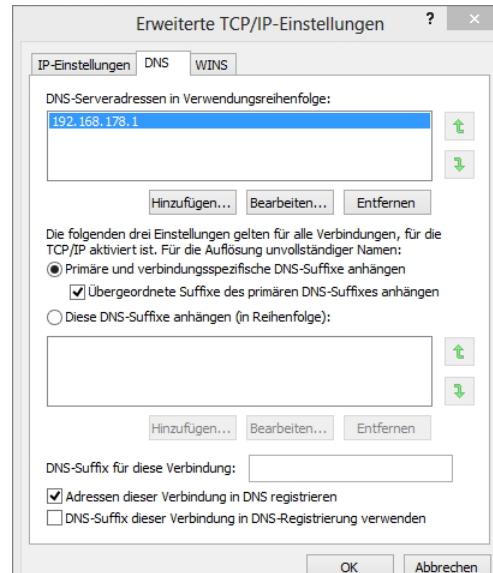
Außer den standardmäßig aktivierte Optionen gibt es noch weitere Möglichkeiten, die Sie in diesem Fenster konfigurieren können:

✓ **Diese DNS-Suffixe anhängen**

Wenn Sie diese Option aktivieren, können Sie DNS-Suffixe konfigurieren, nach denen **unvollständige Rechnernamen** aufgelöst werden. Aktivieren Sie diese Option, werden weder das primäre DNS-Suffix des Servers noch die DNS-Suffixe dieser Verbindung verwendet. Es werden die DNS-Suffixe in der Reihenfolge angehängt, die im Feld *Diese DNS-Suffixe anhängen (in Reihenfolge)* konfiguriert sind. Achten Sie bei der Konfiguration darauf, dass möglichst das DNS-Suffix der Windows-Domäne, in der dieser Server Mitglied ist, als Erstes in dieser Liste eingetragen ist. Diese Option wird häufig verwendet, um die Namensauflösung in Gesamtstrukturen mit mehreren Strukturen zu lösen. Dazu werden in der Reihenfolge alle Strukturen der Gesamtstruktur eingetragen, um eine Namensauflösung innerhalb von Active Directory zu gewährleisten.

✓ **DNS-Suffix dieser Verbindung in DNS-Registrierung verwenden**

Wenn Sie diese Option aktivieren, wird der Computername in DNS mit seinem Computernamen und seinem primären DNS-Suffix registriert, seinem **FQDN (Fully Qualified Domain Name)**. Zusätzlich wird der Name mit dem DNS-Suffix auch beim DNS-Server registriert, das im Bereich *DNS-Suffix für diese Verbindung* konfiguriert ist.



Erweiterte IP-Einstellungen in Windows 10 konfigurieren



Wenn Sie schnell und effizient Servernamen in verschiedenen DNS-Zonen auflösen wollen, aktivieren Sie auf dem Computer in den IP-Einstellungen über die Schaltfläche *Erweitert* auf der Registerkarte *DNS* die Option *Diese DNS-Suffixe anhängen (in Reihenfolge)*. Tragen Sie zuerst den Namensraum der eigenen Struktur ein, und hängen Sie danach die Namensräume der anderen Strukturen an.

Der Sinn dieser Konfiguration ist die schnelle Auflösung von Servern in den anderen Strukturen. Wenn Sie zum Beispiel den Domänencontroller *dc1* in der Struktur *contoso.com* auflösen wollen, müssen Sie immer *dc1.contoso.com* eingeben, wenn Ihr Computer nicht Mitglied dieser Struktur ist.

Diese Einstellung ist zwar optional, erleichtert aber die Stabilität der Namensauflösung in Active Directory. Sie sollten diese Einstellung auf jedem Domänencontroller sowie auf jedem Server in Ihrer Gesamtstruktur und auch auf Computern von Administratoren oder Powerusers durchführen, die ständig eine Verbindung zu anderen Domänen aufbauen müssen. Zuerst sollten immer die eigene Domäne und der eigene Namensraum eingetragen werden, bevor andere Namensräume abgefragt werden.

Wenn Sie diese Maßnahme durchgeführt haben, können Sie mit *nslookup* den Effekt überprüfen. Sie können an dieser Stelle lediglich *dc1* eingeben. Der Server fragt seinen bevorzugten DNS-Server, ob ein Server mit dem Namen *dc1.microsoft.com* gefunden wird, wenn es sich hier um Ihr primäres DNS-Suffix handelt. Da dieser Server unter Umständen in dieser Domäne nicht vorhanden ist, wird der nächste Namensraum abgefragt. Das ist in diesem Beispiel *contoso.com*.

### Anzeigen der IP-Adresse

Es können Situationen auftreten, in denen Sie die IP-Adressinformationen für einen bestimmten Computer anzeigen müssen. Dies ist der Fall, wenn Ihr Computer beispielsweise nicht mit anderen Computern im Netzwerk kommuniziert oder wenn andere Computer nicht mit Ihrem Computer kommunizieren können. In solchen Situationen müssen Sie die IP-Adresse der anderen Computer kennen, um die Ursache des Problems bestimmen zu können.

Im Dialogfeld *Eigenschaften von Internetprotokoll (TCP/IP)* können Sie statische TCP/IP-Informationen anzeigen.

Windows enthält ein Befehlszeilendienstprogramm mit der Bezeichnung *ipconfig*, um TCP/IP-Informationen anzuzeigen. Mit diesem Dienstprogramm werden die TCP/IP-Konfigurationsoptionen auf einem Host überprüft, aber nicht festgelegt. Zu diesen Optionen zählen die IP-Adresse, die Subnetzmaske und das Standardgateway. Die Befehlssyntax für dieses Dienstprogramm lautet *ipconfig*. Mit *ipconfig* können Sie jedoch nicht bestimmen, ob die IP-Adresse mithilfe der statischen oder der dynamischen Methode zugewiesen wurde. Starten Sie das Programm am besten über eine Eingabeaufforderung (*cmd*).

Informationen zu allen TCP/IP-Konfigurationsoptionen erhalten Sie mit dem Dienstprogramm *ipconfig*, wenn Sie zusätzlich die Option */all* angeben (Eingabeaufforderung *ipconfig /all*). Sie sehen, ob DHCP aktiviert ist. Ist dies der Fall und wird eine IP-Adresse für einen DHCP-Server angezeigt, dann wurde die IP-Adresse mithilfe von DHCP bezogen.

Zusätzlich lassen sich beim Aufruf von *ipconfig* die beiden Optionen */renew* und */release* angeben:

<code>ipconfig /release</code>	Entfernt die IP-Adresse vom Client und fordert keine neue an. Wenn ein Client Probleme hat, eine Verbindung mit einem DHCP-Server herzustellen, sollten Sie immer zuerst die IP-Adresse beim Client zurücksetzen.
<code>ipconfig /renew</code>	Fordert vom DHCP-Server eine erneute Verlängerung des Lease oder eine neue IP-Adresse an. Sollte der Befehl nicht funktionieren, geben Sie zunächst <i>ipconfig /release</i> ein.

Ein PC kommuniziert über seine IP-Adresse über den Router mit dem Internet. Dabei nutzen verschiedene Programme unterschiedliche Ports. In der Befehlszeile können Sie überprüfen, welche Ihrer Programme eine Verbindung zum Internet aufbauen. So lassen sich auch Viren und Trojaner erkennen. Wenn Sie bestimmte Programme nicht identifizieren können, suchen Sie nach diesen im Internet. In den meisten Fällen finden Sie recht schnell Informationen zu allen Programmen.

Geben Sie in der Befehlszeile den Befehl `netstat -an` ein, zeigt Windows die geöffneten Ports. Ausführlichere Informationen erscheinen mit `netstat -banvo`. Die Routingtabelle des Computers wird mit `netstat -r` angezeigt, Statistiken zu TCP/IP sehen Sie mit `netstat -s` an. Auf diesem Weg lassen sich also umfassende Informationen zu Netzwerkeinstellungen eines Computers abrufen.

## TCP/IPv6 konfigurieren

Sollte in Ihrem Netzwerk die Autokonfiguration von IPv6-Adressen unerwünscht sein, können Sie analog zu IPv4 die Einstellungen des IPv6-Protokolls ändern.

## Grundlagen zu IPv6

IPv6 ist der Nachfolger des gegenwärtig im Internet noch überwiegend verwendeten IPv4. Beide Protokolle sind Standards für die Netzwerkschicht des OSI-Modells und regeln die Adressierung und das Routing von Datenpaketen durch ein Netzwerk. Das bisherige IPv4 bietet einen Adressraum von ca. 4 Milliarden IP-Adressen, mit denen Computer und andere Geräte angesprochen werden können. In den Anfangstagen des Internets, als nur wenige Rechner eine IP-Adresse benötigten, galt dies als ausreichend.

Eine IPv6-Adresse ist 128 Bit lang (IPv4: 32 Bit). Damit stehen ca.  $3,4 \times 1038$  (340,28 Sextillionen) IPv6-Adressen zur Verfügung. IPv6-Adressen werden in hexadezimaler Notation mit Doppelpunkten geschrieben, die die Adresse in acht Blöcke mit einer Länge von jeweils 16 Bit unterteilen. Beispiel einer IPv6-Adresse:

`2001:0db7:85b3:07d3:1319:8a2d:437a:63d4`

Eine oder mehrere 16-Bit-Gruppen mit dem Wert 0000 können durch zwei aufeinanderfolgende Doppelpunkte ersetzt werden. Die resultierende Adresse darf höchstens einmal zwei aufeinanderfolgende Doppelpunkte enthalten. `2001:0db8::1428:57ab` ist gleichbedeutend mit `2001:0db8:0000:0000:0000:1428:57ab`, aber `2001::25de::cade` ist nicht korrekt, da nicht nachvollzogen werden kann, wie viele 16-Bit-Gruppen durch die zwei Doppelpunkte jeweils ersetzt wurden. Führende Nullen einer 16-Bit-Gruppe dürfen ausgelassen werden, `2001:db8::28:b` ist gleichbedeutend mit `2001:0db8::0028:000b`.

Netzmasken, wie sie bei IPv4 verwendet wurden, gibt es bei IPv6 nicht. Die ersten 64 Bit der IPv6-Adresse dienen der **Netzadressierung**, die letzten 64 Bit werden zur **Host-Adressierung** verwendet. Beispiel: Hat ein Netzwerkgerät die IPv6-Adresse `2001:0db7:85b3:07d3:1319:8a2d:437a:63d4`, so stammt es aus dem Subnetz `2001:0db7:85b3:07d3::/64`.

## IPv6-Technologien unter Windows nutzen

Windows und Windows Server nutzen beide den **Next Generation TCP/IP-Stack**. Hierbei handelt es sich um einen neu entworfenen TCP/IP-Protokollstack, in den sowohl IPv4 (Internet Protocol version 4) als auch IPv6 (Internet Protocol version 6) integriert sind. Wenn eine DNS-Abfrage beispielsweise eine IPv6- und IPv4-Adresse zurückgibt, dann versucht der Stack zuerst, über IPv6 zu kommunizieren. Die Bevorzugung von IPv6 gegenüber IPv4 bietet IPv6-fähigen Anwendungen eine bessere Netzwerkkonnektivität.

IPv6-Verbindungen sind in der Lage, IPv6-Technologien wie **Teredo** zu nutzen. Teredo ist eine IPv6-Technologie, die durch ein oder mehrere NATs voneinander getrennte IPv6/IPv4-Knoten eine End-to-End-Kommunikation mit globalen IPv6-Adressen ermöglicht. IPv6-Netzwerkverkehr auf Basis von Teredo kann ein NAT ohne eine Neukonfiguration des NAT oder eine Änderung der Anwendungsprotokolle passieren. Teredo ist in Windows XP/Vista Service Pack 2 und Windows Server 2003 Service Pack 1 enthalten. Teredo ist auf Domänencomputern aktiviert. Beim Teredo-Netzwerkverkehr handelt es sich um IPv6-Pakete, die in IPv4-UDP-Nachrichten gekapselt wurden.

Die standardmäßige Aktivierung von IPv6 und die Bevorzugung von IPv6 haben keine negativen Auswirkungen auf die IPv4-Konnektivität. In Netzwerken, in denen keine IPv6-DNS-Einträge zur Verfügung stehen, wird beispielsweise nicht über IPv6-Adressen kommuniziert. Um die Vorteile einer IPv6-Konnektivität zu nutzen, müssen Netzwerkanwendungen aktualisiert werden.

## Vorteile von IPv6 gegenüber Ipv4

IPv6 bietet gegenüber IPv4 die folgenden Vorteile:

- ✓ **Größerer Adressraum**

Der 128-Bit-Adressraum von IPv6 bietet genügend Platz, um jedes Gerät im bestehenden und zukünftigen Internet mit einer eigenen, global gültigen Adresse auszustatten.

- ✓ **Effizienteres Routing**

Durch den überarbeiteten IPv6-Header und das neue Adressierungsschema, das eine hierarchische Routing-Infrastruktur unterstützt, können IPv6-Router den entsprechenden Netzwerkverkehr schneller weiterleiten.

- ✓ **Einfache Konfiguration**

IPv6-Hosts können sich entweder über DHCP oder mithilfe eines lokalen Routers selbst konfigurieren.

- ✓ **Verbesserte Sicherheit**

Die IPv6-Standards beheben einige der Sicherheitsprobleme von IPv4. Sie bieten einen besseren Schutz vor Adress- und Portscans. Sie schreiben vor, dass IPv6-Implementierungen **IPsec** (Internet Protocol Security) unterstützen müssen.

## Windows 10 und IPv6

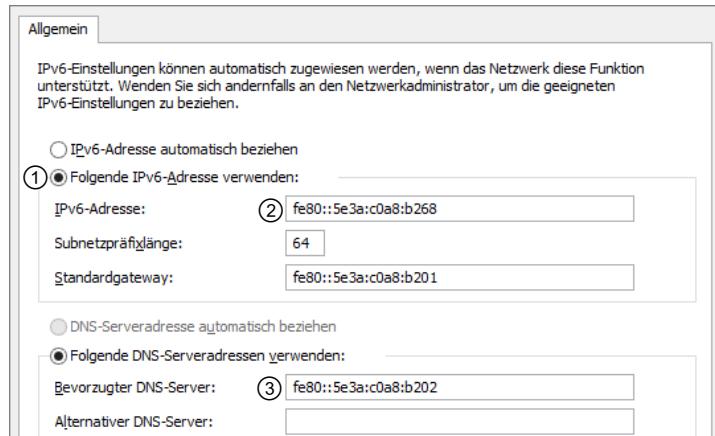
Windows 10 unterstützt nach der Installation das neue IP-Protokoll Version 6 (IPv6). Wenn Sie die Eigenschaften der Netzwerkverbindung anzeigen, sehen Sie, dass IPv6 automatisch mit den Netzwerkverbindungen verknüpft wird.

IPv6 wurde so entworfen, dass es einfacher als IPv4 zu konfigurieren ist. IPv6 kann sich automatisch selbst konfigurieren, auch ohne DHCPv6 (Dynamic Host Configuration Protocol for IPv6). Alle IPv6-Knoten konfigurieren für jede physische oder logische IPv6-Schnittstelle automatisch eine lokale Adresse mit dem Präfix **fe80::/64**. Diese Adressen können nur zur Kommunikation mit benachbarten Knoten verwendet werden. Sie werden nicht im DNS registriert, und wenn Daten an eine solche Adresse gesendet werden sollen, ist zusätzlich eine Zonen-ID notwendig.



Wenn Sie einen Computer mit Windows 10 für IPv6 konfigurieren, sind folgende automatische Einstellungen möglich:

- ✓ Ein IPv6-Host sendet eine Multicast-Nachricht und empfängt eine oder mehrere Router-Nachrichten. In diesen Router-Nachrichten finden sich Subnet-Präfixe (diese nutzt der IPv6-Host zum Festlegen weiterer IPv6-Adressen und zum Hinzufügen von Routen zur IPv6-Routingtabelle) und weitere Konfigurationsparameter (zum Beispiel das Standardgateway).
- ✓ Über DHCPv6 erhält der IPv6-Host Subnet-Präfixe und andere Konfigurationsparameter. Oft wird DHCPv6 bei IPv6-Hosts unter Windows zum Beispiel dazu genutzt, die IPv6-Adressen der DNS-Server zu konfigurieren, was über die Routererkennung nicht möglich ist.
  
- Öffnen Sie die Eigenschaften von Internetprotokoll Version 6 (TCP/IPv6).
- Wählen Sie *Folgende IPv6-Adresse verwenden* ①.
- Geben Sie die zugewiesene IPv6-Adresse in der hexadezimalen Schreibweise ein ②.
- Falls nötig, geben Sie auch eine DNS-Serveradresse an ③.



TCP/IPv6-Einstellungen bearbeiten

## Bindungsreihenfolge der Netzwerkverbindungen konfigurieren

Wenn Sie mehrere Netzwerkkarten in Ihrem Computer eingebaut haben, werden Netzwerkpakete nicht immer an alle Netzwerkkarten gleichzeitig verschickt, sondern immer in einer bestimmten Reihenfolge. Damit die Antwortzeiten im Netzwerk optimiert werden, sollte Ihre produktive Netzwerkkarte in der Reihenfolge ganz oben stehen:

- ▶ Klicken Sie im Netzwerk- und Freigabecenter auf den Link *Adapttereinstellungen ändern*, um diese Reihenfolge festlegen zu können.
- ▶ Aktivieren Sie die Menüleiste durch Drücken der **[Alt]**-Taste.
- ▶ Klicken Sie im Menü auf *Erweitert - Erweiterte Einstellungen*.  
Es öffnet sich ein neues Fenster, über das Sie unter anderem die Bindungsreihenfolge der Netzwerkkarten einstellen können.
- ▶ Klicken Sie auf der Registerkarte *Adapter und Bindungen* im Bereich *Verbindungen* auf die ausgewählte LAN-Verbindung.  
Mit den Pfeil-Schaltflächen können Sie die Reihenfolge ändern.

## Verwenden von Befehlszeilentoools für Netzwerkinformationen

Mithilfe von Befehlszeilentoools können Sie schnell Informationen über Ihren Computer und Ihr Netzwerk abrufen sowie diese zur Diagnose von Netzwerkproblemen einsetzen. Die Befehle in diesem Thema beziehen sich auf TCP/IP-Netzwerke. Nachfolgend finden Sie die Befehle zu den häufigsten Fragen zur Ermittlung von Netzwerkinformationen in der Eingabeaufforderung.

Wie ermittele ich den Computernamen?	Geben Sie in der Eingabeaufforderung <code>hostname</code> ein.
Wie ermittele ich die IP-Adresse meines Computers?	Geben Sie in der Eingabeaufforderung <code>ipconfig</code> ein.
Wie ermittele ich die physische Adresse meines Computers (MAC-Adresse, Media Access Control)?	Geben Sie in der Eingabeaufforderung <code>ipconfig /all</code> ein. Falls Ihr Computer mit mehreren Netzwerkadapters ausgestattet ist, wird die physische Adresse für jeden Adapter einzeln aufgeführt.
Wie erhalte ich eine neue IP-Adresse?	Geben Sie in der Eingabeaufforderung <code>ipconfig /release</code> ein. Hierdurch geben Sie Ihre aktuelle IP-Adresse frei. Geben Sie in der Eingabeaufforderung als Nächstes <code>ipconfig /renew</code> ein, um eine neue IP-Adresse zu erhalten.
Wie löse ich anhand des DNS-Namens (Domain Name System) eine IP-Adresse auf?	Geben Sie in der Eingabeaufforderung <code>ping &lt;DNS-Name&gt;</code> ein. Dieser Vorgang wird Reverse-Lookup genannt.
Wie teste ich die Kommunikation mit einem anderen Computer?	Geben Sie in der Eingabeaufforderung <code>ping &lt;IP-Adresse&gt;</code> des zu testenden Computers ein.

Weitere wichtige Optionen von `ipconfig` sind folgende:

<code>ipconfig /registerdns</code>	Erneuert die Registrierung des Clients am konfigurierten DNS-Server, wenn für die DNS-Zone die dynamischen Updates aktiviert sind. Diese Option ist nur für Rechner in Unternehmen interessant.
<code>ipconfig /displaydns</code>	Zeigt den lokalen DNS-Cache an, auch die zuletzt geöffneten Internetseiten und aufgelösten DNS-Namen. Löschen Sie den Verlauf im Browser, sind die Daten dennoch an dieser Stelle vorhanden. Sie müssen den lokalen DNS-Cache getrennt löschen, indem Sie <code>ipconfig /flushdns</code> verwenden.
<code>ipconfig /flushdns</code>	Löscht den lokalen DNS-Cache

## 8.3 Netzwerkkomponenten verwalten

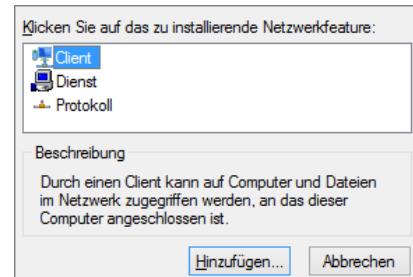
### Übersicht über die wichtigsten Netzwerkkomponenten von Windows 10

Unter Netzwerkkomponenten versteht man Client-Programme, Dienste und Protokolle, die zur Verfügung stehen müssen, um bestimmte Funktionen im Netzwerk wahrnehmen zu können.

Komponentenklasse	Komponente	Funktion
<b>Client</b>	Client für Microsoft-Netzwerke	Ermöglicht den Zugriff auf NetBIOS-Ressourcen im Netzwerk
<b>Dienst</b>	Datei- und Druckerfreigabe für Microsoft-Netzwerke	Ermöglicht anderen Microsoft-Rechnern den Zugriff auf Ressourcen Ihres Rechners
<b>Dienst</b>	QoS-Paketplaner (Quality of Service)	Zeitkritische Anwendungen können Netzwerkverbindungen mit Mindestqualität aufbauen.
<b>Protokoll</b>	Internetprotokoll Version 4 (TCP/IPv4)	Altes Standardprotokoll im Internet
<b>Protokoll</b>	Internetprotokoll Version 6 (TCP/IPv6)	Neues Standardprotokoll im Internet
<b>Protokoll</b>	E/A-Treiber für Verbindungsschicht-Topologieerkennung	Erkennung und Anzeige der Netzwerktopologie, in der sich ein Windows-Computer befindet
<b>Protokoll</b>	LLDP-Treiber (Link Layer Discovery Protocol)	Neues Protokoll zum Informationsaustausch zwischen Nachbargeräten im Netzwerk

### Netzwerkkomponenten hinzufügen oder entfernen

- ▶ Um weitere Komponenten in Ihr System einzubinden, klicken Sie im Dialog *Eigenschaften* Ihrer Netzwerkverbindung auf *Installieren*. Sie können aus den drei Kategorien *Client*, *Dienst* oder *Protokoll* auswählen. Wählen Sie z. B. das Protokoll *Reliable Multicast-Protokoll* aus.
- ▶ Um eine markierte Komponente zu deinstallieren, klicken Sie im Dialog *Eigenschaften* Ihrer Netzwerkverbindung auf *Deinstallieren* und bestätigen Sie mit *Ja*.



Installieren von Netzwerkkomponenten

## 8.4 Übung

### Netzwerkeinstellungen

Übungsdatei: --

Ergebnisdatei: Uebung08\_E.pdf

1. Wie fügen Sie den Computer einer Domäne hinzu?
2. Wie ändern Sie die Netzwerkeinstellungen und die IP-Adresse?
3. Wie zeigen Sie in der Befehlszeile die IP-Adresse an und rufen eine neue IP-Adresse von einem DHCP-Server ab?

# 9 Hardware hinzufügen

## In diesem Kapitel erfahren Sie

- ✓ welche Hardware-Komponenten Windows 10 unterstützt
- ✓ wozu Treiber benötigt werden
- ✓ wie Sie Plug-&-Play-Hardware installieren können
- ✓ wie Sie nicht Plug-&-Play-fähige Hardware installieren können

## 9.1 Hardware-Komponenten und Treiber verwenden

### Windows 10 und Plug & Play

Der Schwerpunkt der Hardware-Verwaltung von Windows 10 liegt auf Plug & Play. Plug & Play ermöglicht es, dass Geräte automatisch erkannt, installiert und verwendet werden können. Dazu müssen folgende Voraussetzungen erfüllt sein:

- ✓ Plug-&-Play-fähige Komponente (Standard)
- ✓ Plug-&-Play-BIOS mit ACPI (Standard)
- ✓ Plug-&-Play-Betriebssystem (Standard), z. B. Windows 10. Das System konfiguriert die Komponente so weit wie möglich automatisch, lädt den passenden Treiber und startet das neue Gerät.

**ACPI (Advanced Configuration and Power Management)** ist Voraussetzung für die Installation von Windows 10 und sorgt dafür, dass Windows die volle Kontrolle über die Hardwareverwaltung und -konfiguration erhält. Früher musste diese Aufgabe vom BIOS übernommen werden.



Windows 10 verfügt über ein internes Tool, um geladene Treiber anzuzeigen. Sie können das Tool über die Eingabeaufforderung mit dem Befehl `driverquery` aufrufen. Mit dem Befehl `driverquery >C:\temp\driver.txt` können Sie die Ausgabe in eine Datei umleiten lassen.

### Treiber für die Hardware-Komponenten

Die Kommunikation von Hardware-Komponenten mit dem Betriebssystem wird über **Treiber** abgewickelt. Treiber sind kleine Programme, die das Betriebssystem benötigt, um Hardware-Komponenten verwenden zu können. Sie sind spezifisch auf die Hardware-Komponente abgestimmt und müssen daher bei Austausch einer Komponente ebenfalls ersetzt werden. Windows 10 kann entweder Microsoft-eigene Treiber verwenden oder die Treiber des Hardware-Herstellers installieren.

Windows 10 unterstützt das **Windows Driver Model (WDM)** und das **Windows Display Driver Model (WDDM)**, insbesondere für Audio- und Videogerätetreiber. In WDM- und WDDM-Treibern werden hardwarenahe Funktionen nicht implementiert – das erledigen Kernfunktionen von Windows selbst. Dies bewirkt, dass bei einem Treiberwechsel oder bei einer Aktivierung und Deaktivierung des betroffenen Gerätes das Betriebssystem seltener neu gestartet werden muss. Direkte Hardwarezugriffe durch die Treiber werden von Windows nicht zugelassen, was für ein stabileres Betriebssystem und eine wirksame Durchsetzung von Kopierschutzmaßnahmen für Audio- und Videodaten sorgt.

Windows 10 setzt außerdem eine **digitale Signatur** für Treiber und einen speziellen **Treiberschutz** ein, um Probleme mit falschen oder fehlerhaften Treibern zu vermeiden.

### Signierte Treiber

Microsofts **Windows Hardware Quality Lab (WHQL)** überprüft Treiber auf Funktion und Betriebssicherheit unter Windows 10. Wenn ein Treiber diese Tests besteht, wird er mit einer digitalen Signatur versehen und erhält das Windows-Logo. Auch Hersteller können ihre Treiber selbst signieren. Sie sind dann zwar nicht WHQL-zertifiziert, lassen sich aber in allen Windows-10-Versionen installieren. Diese zertifizierten oder signierten Treiber sollen eine höhere Stabilität und Sicherheit bieten und weniger Probleme verursachen. Alle Systemdateien und mitgelieferten Treiber von Windows 10 besitzen eine solche digitale Signatur.

Der spezielle Kernelschutz-Modus in der 64-Bit-Version von Windows 10 verbietet grundsätzlich die Installation unsignierter Treiber. Es ist daher im Normalfall nicht möglich, einen Treiber ohne Signatur in der 64-Bit-Version von Windows 10 zu verwenden, es gibt allerdings die Möglichkeit, den Treiber selbst zu signieren. Auf diese Weise kann das Problem eleganter gelöst werden als durch die Abschaltung der Signaturprüfung mittels irgendeiner Tricks aus dem Internet.



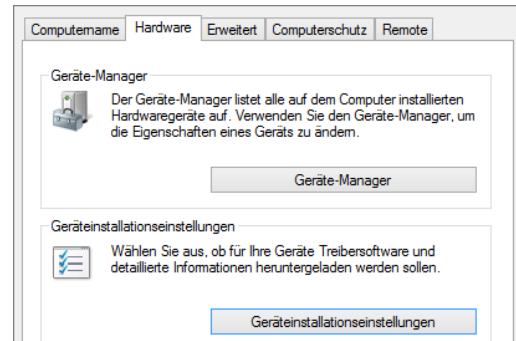
Microsoft bietet zum Signieren von Software das **Windows Driver Kit (WDK)** kostenlos zum Download an. Weitere Informationen finden Sie in der WDK-Dokumentation.

### Treiber über Windows Update herunterladen

Wenn in Windows 10 kein Treiber für eine Hardwarekomponente enthalten ist und auch die Hardwarehersteller keinen Treiber anbieten, haben Sie unter Umständen Chancen, bei einem Windows-Update über das Internet einen Treiber zu finden.

Ein manuelles Windows-Update können Sie über *Einstellungen - Update und Sicherheit - Windows Update* anstoßen.

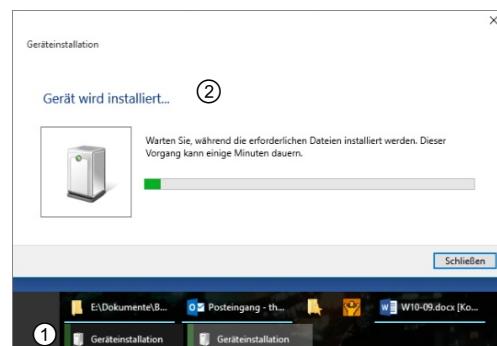
Die Konfiguration des Downloads von Treibern über Windows Update nehmen Sie über *Systemsteuerung - System und Sicherheit - System - Erweiterte Systemeinstellungen*, Registerkarte *Hardware*, Schaltfläche *Geräteinstallationseinstellungen* vor.



## 9.2 Hardware automatisch installieren

### Plug-&-Play-Hardware installieren

Seit einigen Jahren ist alle PC-Hardware Plug-&-Play-fähig. Die Installation neuer Geräte ist daher recht einfach, erfordert meist keine Benutzereingriffe und setzt keine Administratorberechtigungen voraus. Die Erkennung neuer Hardware und deren Installation laufen im Hintergrund ab und sind nur durch ein minimiertes Fenster auf dem Desktop ersichtlich. Erst ein Klick auf das Symbol in der Taskbar ① öffnet den Installationsdialog ②, in dem der Benutzer den Stand der Installation verfolgen kann. Oft läuft die Installation ohne Benutzereingriffe ab, anderenfalls wird der Benutzer zu Handlungen aufgefordert.



Automatische Installation eines neuen Gerätes

### Externe Geräte installieren

- ✓ Geräte für USB (Universal Serial Bus), IEEE 1394 (FireWire), eSATA, Thunderbolt sowie PCMCIA Cards und ExpressCards können Sie im laufenden Betrieb anschließen.

- ✓ Ältere Legacy-Geräte für die alten seriellen, parallelen oder PS/2-Schnittstellen wie Modems, Drucker und Tastaturen dürfen nur bei ausgeschaltetem Computer angeschlossen werden.

Das neue Gerät wird automatisch identifiziert ①, und wenn passende Treiber verfügbar sind, werden diese ohne Nachfrage oder Meldung installiert. Dazu durchsucht Windows 10 seine Treiberdatenbank, die deutlich umfangreicher ist und wesentlich mehr Klassentreiber für Gerätegruppen enthält als bei älteren Windows-Versionen. Anschließend ist das neue Gerät verwendbar und Sie erhalten eine entsprechende Meldung. Falls kein geeigneter Treiber für die Hardware-Komponente gefunden wurde, können Sie entweder aus einer Liste von Treibern auswählen, den Pfad zur Treibersoftware eingeben oder über Windows Update danach suchen lassen.



Wenn Sie auf Performance und Stabilität Wert legen, sollten Sie immer die wichtigsten Treiber für Ihren PC (für Chipsatz, Grafikkarte und Netzwerkkarte) direkt vom jeweiligen Hersteller herunterladen und verwenden. Diese Treiber sind meist besser an das System angepasst als jene, die das Betriebssystem mitbringt. Sie finden die entsprechenden Treiber entweder auf den Herstellerseiten mithilfe von Tools wie Slimdrivers oder über spezielle Internetadressen wie [www.treiber.de](http://www.treiber.de).

### Interne Erweiterungskarten installieren

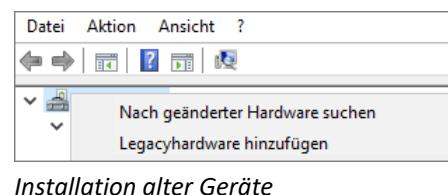
- Um eine PCI- oder PCI-Express-Erweiterungskarte in einem Desktop-Computer zu installieren, schalten Sie zunächst den Computer aus.  
Dies gilt auch für das Einsetzen von Speicherriegeln und den Einbau interner Datenträger.
- Ziehen Sie den Netzstecker, öffnen Sie das Gehäuse und treffen Sie Maßnahmen gegen statische Aufladung, bevor Sie elektronische Bauteile berühren.
- Setzen Sie die Karte in einen geeigneten Steckplatz und sichern Sie sie mit Schrauben oder Klemmen gegen Herausrutschen. Schließen Sie das Gehäuse und schalten Sie den Computer wieder ein.

Nach dem Einschalten läuft die Installation ab wie oben beschrieben.

### Nicht Plug-&-Play-fähige Hardware automatisch installieren

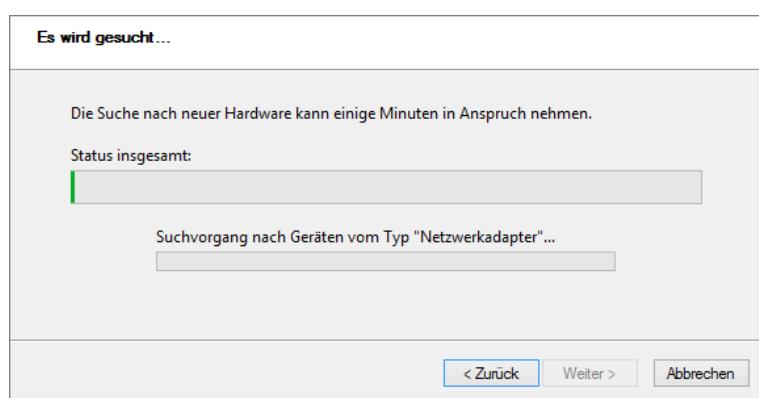
Falls Sie sehr alte Geräte unter Windows 10 betreiben müssen, die noch kein Plug-& Play unterstützen, stehen die Chancen insbesondere bei 64-Bit-Systemen eher schlecht, dafür einen funktionierenden Treiber zu finden. Einen Versuch ist es jedoch wert. Der Hardware-Assistent von Windows 10 kann oftmals auch nicht Plug-& Play-fähige Geräte erkennen und automatisch installieren. Sie benötigen dafür Administratorberechtigungen.

- Öffnen Sie den Geräte-Manager mit einem Klick im Schnellzugriffsmenü oder betätigen Sie und klicken Sie auf *Geräte-Manager*.
- Klicken Sie mit der rechten Maustaste auf den Namen Ihres Computers und wählen Sie *Legacyhardware hinzufügen*.



Der Hardware-Assistent sucht nun nach neuen Hardware-Komponenten. Falls dabei eine Komponente erkannt wird, kann sie jetzt installiert werden und Sie erhalten eine entsprechende Meldung.

- Gehen Sie alle Installationsschritte mit dem Assistenten durch.
- Beenden Sie den Assistenten mit *Fertig stellen*.  
Die Komponente ist jetzt installiert und betriebsbereit.



*Der Hardware-Assistent sucht neue Komponenten*

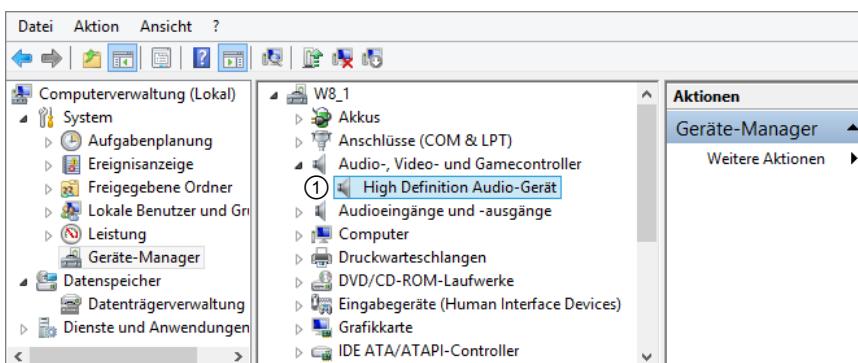
Die automatische Hardware-Erkennung funktioniert bei alten Geräten manchmal nicht. In diesem Fall müssen Sie die Installation manuell mit dem Hardware-Assistenten durchführen.

## 9.3 Hardware manuell konfigurieren

### Hardware-Komponenten mit dem Gerät-Manager konfigurieren

Mit dem Gerät-Manager können Sie installierte Hardware-Komponenten manuell konfigurieren, mögliche Probleme beheben und neue Treiber für die Komponenten installieren. Ein Eingriff ist normalerweise nur erforderlich, wenn bei der Installation Probleme aufgetreten sind. Sie können den Gerät-Manager auch über die Computerverwaltung erreichen:

- ▶ Klicken Sie im Schnellzugriffsmenü auf *Computerverwaltung*.
  - ▶ Wählen Sie das Snap-In *Gerät-Manager*. Sie können den Gerät-Manager auch durch Eingabe von `devmgmt.msc` starten.
- Der Gerät-Manager zeigt in einer Liste die installierten Geräte an und markiert ein Gerät mit Problemen oder noch fehlenden Treibern mit einem gelben Ausrufezeichen ①.
- ▶ Klicken Sie doppelt auf das Gerät, das konfiguriert werden soll.



Die Liste installierter Hardware im Snap-In Gerät-Manager

Je nach Komponententyp bietet das folgende Dialogfenster mehrere Register an, beispielsweise *Allgemein*, *Treiber* und *Ressourcen*.

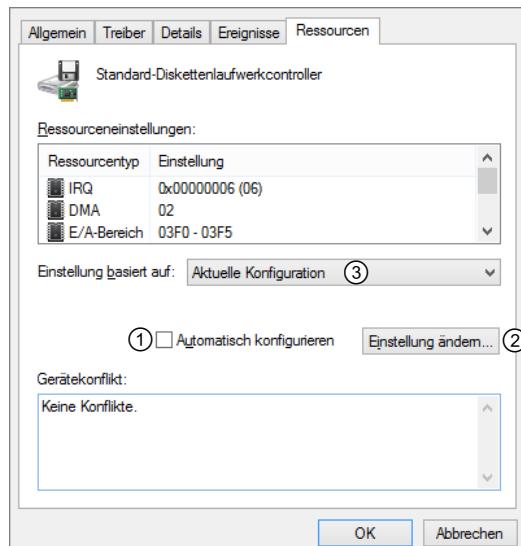
Im Register *Allgemein* erhalten Sie Informationen über den Betriebszustand der Komponente und können diese aktivieren oder deaktivieren.

Im Register *Treiber* können Sie Detailinformationen zum Gerätetreiber abrufen oder den Treiber aktualisieren.

Im Register *Ressourcen* werden der E/A-Adressbereich (Eingabe/Ausgabe), der Speicherbereich und der IRQ (Interrupt Request, Unterbrechungsanforderung für den Prozessor) konfiguriert.

- ▶ Deaktivieren Sie das Kontrollfeld *Automatisch konfigurieren* ①.
- ▶ Markieren Sie im Register *Ressourcen* die betreffende Ressource und klicken Sie auf *Einstellung ändern* ②. Falls dies nicht zugelassen wird, ändern Sie die Einstellung im Feld ③, wo verschiedene Basiskonfigurationen angeboten werden.
- ▶ Geben Sie die erforderlichen Werte für jede Ressource an und klicken Sie auf *OK*. Falls die gewählte Einstellung zu Konflikten mit anderen Hardware-Komponenten führt, erscheint eine Warnmeldung und Sie müssen andere Werte verwenden.

Bei Plug-&-Play-Komponenten übernimmt Windows die Vergabe der Ressourcen, und die Einstellungsoptionen sind nicht verfügbar. Die Einstellungen für ein manuell zu installierendes Gerät finden Sie in der Dokumentation zu diesem Gerät. Stellen Sie sicher, dass die Einstellungen im Register *Ressourcen* mit diesen Werten übereinstimmen.



Eine Ressource manuell konfigurieren

### Treiber für SSD-Zugriff überprüfen

Um SSD-Festplatten optimal mit Windows 10 zu nutzen, müssen Sie im BIOS für die Festplatte den **AHCI-Modus** aktivieren. Außerdem muss Windows den passenden Treiber für die SSD verwenden. Diesen nutzt Windows 10 für die optimale Zusammenarbeit mit SSDs. Der Treiber muss deshalb für den Controller aktiviert sein, an dem Sie die SSD angeschlossen haben. Sie können dies im Geräte-Manager überprüfen:

- ▶ Öffnen Sie den Geräte-Manager.
- ▶ Navigieren Sie zu dem Treiber für den Controller und rufen Sie dessen Eigenschaften auf.
- ▶ Wechseln Sie zur Registerkarte *Treiber*.
- ▶ Klicken Sie auf *Treiberdetails*.

Der Treiber mit der Bezeichnung AHCI im Namen muss geladen sein, damit Windows 10 SSDs optimal unterstützt.

## 9.4 Hardware deaktivieren und deinstallieren

### Hardware vorübergehend deaktivieren

- ▶ Starten Sie den Geräte-Manager über das Schnellzugriffsmenü.
- ▶ Öffnen Sie in der Liste die betreffende Gerätekategorie ① und klicken Sie mit der rechten Maustaste auf die gesuchte Komponente.
- ▶ Klicken Sie im Kontextmenü auf *Deaktivieren* ② und bestätigen Sie die folgende Warnmeldung mit *Ja*.



Die betreffende Komponente wird jetzt abgeschaltet und kann nicht mehr verwendet werden. Sie wird deshalb im Geräte-Manager mit einem Pfeil nach unten markiert, der leicht zu übersehen ist.

- ▶ Klicken Sie im Kontextmenü der Komponente auf den Eintrag *Aktivieren*, um sie wieder zu verwenden.

## Hardware dauerhaft deinstallieren

- ▶ Starten Sie den Geräte-Manager und navigieren Sie zu der betreffenden Komponente.
- ▶ Öffnen Sie mit der rechten Maustaste das Kontextmenü und klicken Sie auf *Deinstallieren* ③, um die Komponente dauerhaft zu entfernen.
- ▶ Bestätigen Sie die angezeigte Warnmeldung mit *OK*.  
Die Komponente wird jetzt deinstalliert.
- ▶ Schalten Sie den Computer ab und entfernen Sie jetzt die Komponenten aus dem Computer.

Beachten Sie, dass deinstallierte Plug-&-Play-Komponenten beim Neustart des Computers erneut installiert werden, solange sie eingebaut oder angeschlossen sind. Komponenten, die angeschlossen bleiben, aber nicht erneut installiert werden sollen, müssen Sie deshalb deaktivieren.



## Nicht im Geräte-Manager angezeigte Hardware entfernen

Einige nicht Plug-&-Play-fähige Treiber sowie Geräte, die bisher installiert waren, jetzt aber nicht mehr angeschlossen sind, werden im Geräte-Manager standardmäßig nicht angezeigt. Sie müssen diese Komponenten erst sichtbar machen, damit sie entfernt werden können.

- ▶ Starten Sie den Geräte-Manager und klicken Sie im Menü *Ansicht* auf *Ausgeblendete Geräte anzeigen*. Anschließend werden alle Komponenten angezeigt und Sie können die Hardware wie üblich entfernen.

## Hot-Plugging-fähige Hardware entfernen

Externe Anschlüsse wie FireWire, PC-Card, ExpressCard, Speicherkartenleser und USB unterstützen Hot-Plugging, also das Entfernen von Geräten **im laufenden Betrieb**. Durch vorzeitiges Entfernen einer Komponente besteht jedoch bei Speichermedien die Möglichkeit, dass Daten verloren gehen, daher sollten Sie alle externen Datenträger auf folgende Art entfernen:

- ▶ Klicken Sie in der Taskleiste auf das Symbol *Hardware sicher entfernen*.
  - ▶ Klicken Sie in der angezeigten Liste auf das zu entfernende Gerät, um es anzuhalten.  
Alle Operationen werden zu Ende geführt und das Gerät wird aus dem System abgemeldet.
- Warten Sie die Meldung ab, dass das Gerät jetzt entfernt werden kann, bevor Sie es abziehen.

## 9.5 Treiber- und Hardware-Probleme behandeln

### Bedeutung der Hardware-Probleme

Nicht korrekt installierte und konfigurierte sowie fehlerhafte Hardware-Komponenten können schwere Probleme verursachen. Das Betriebssystem kann instabil werden oder lässt sich überhaupt nicht mehr starten. Windows 10 bietet mehrere Verfahren zur Vermeidung und Lösung solcher Probleme:

- ✓ Installation nicht signierter Treiber verhindern,
- ✓ Treiberaktualisierung und Treiberzurücksetzung,
- ✓ abgesicherter Modus,
- ✓ Systemwiederherstellung.

### Installation unsignierter Treiber

Von Microsoft erfolgreich getestete Treiber für Windows 10 besitzen eine digitale Signatur. Während auf 64-Bit-Systemen eine Installation verweigert wird, können auf 32-Bit-Systemen von Administratoren auch unsignierte Treiber installiert werden.

## Treiberinstallation ohne Administratorberechtigungen

Eine Treiberinstallation mit normalen Benutzerberechtigungen funktioniert nur bei signierten Treibern, die außerdem in der Windows-Treibersammlung (Driver Store) vorliegen müssen. Der Driver Store befindet sich in `%SYSTEMROOT%\System32\DriverStore\FileRepository`. Um Treiber hinzuzufügen oder zu entfernen, können Sie das Kommandozeilenwerkzeug `pnputil.exe` verwenden. Dazu muss die INF-Datei zugänglich sein, möglicherweise müssen Sie also das Treiberpaket vorher entpacken. Sie benötigen eine Administrator-Eingabeaufforderung:

- ▶ Klicken Sie dafür im Schnellzugriffsmenü auf *Eingabeaufforderung (Administrator)*. Alternativ können Sie im Startbildschirm cmd eingeben und anschließend **Strg** ↗ ↙ drücken.
- ✓ `pnputil -a C:\neuetreiber\*.inf` fügt alle Treiberpakete aus *C:\neuetreiber* hinzu.
- ✓ `pnputil -e` zeigt alle im Driver Store enthaltenen Treiber von Fremdherstellern an.
- ✓ `pnputil ?` zeigt alle Parameter und die Syntax an.

## Treiber für ältere Windows-Versionen im Kompatibilitätsmodus installieren

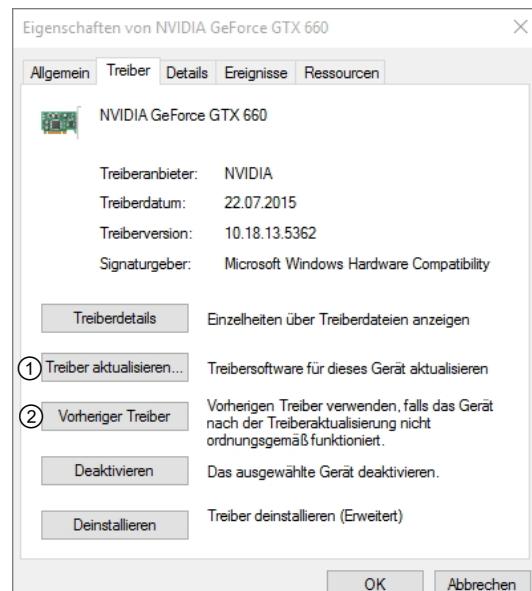
Kurz nach Markteinführung wird es für viele Geräte noch keine für Windows 10 zertifizierten Treiber geben, und für ältere Geräte werden nur selten angepasste Treiber bereitgestellt. Da sich am Aufbau der Treiber seit Windows Vista nichts Grundlegendes geändert hat, stehen die Chancen gut, dass ein Treiber für Windows 7 oder 8 auch bei Windows 10 funktioniert.

In einigen Fällen bricht die Treiberinstallation jedoch mit der Fehlermeldung ab, der Treiber sei für diese Betriebssystemversion nicht geeignet. Dieser Fehler tritt auf, wenn während der Installation die Version von Windows mit den Informationen aus der INF-Datei verglichen wird und nicht die Vorgaben erfüllt. Ein möglicher Ansatz zur Behebung ist das manuelle Ändern der INF-Dateien oder einfacher über die Kompatibilitätseinstellungen (vgl. Kapitel 6). Mithilfe der Kompatibilitätseinstellungen ist es in vielen Fällen möglich, ältere Treiber zu installieren.

## Treiber aktualisieren oder zurücksetzen

Wenn ein Treiber Probleme verursacht, können Sie versuchen, diesen durch eine neue Version zu ersetzen.

- ▶ Öffnen Sie den Gerät-Manager und navigieren Sie zur Komponente, deren Treiber durch eine neue Version ersetzt werden soll.
- ▶ Klicken Sie mit der rechten Maustaste auf den Eintrag der Komponente und klicken Sie auf *Eigenschaften*.
- ▶ Wechseln Sie in das Register *Treiber* und klicken Sie auf *Treiber aktualisieren* ①.
- ▶ Legen Sie mit dem Hardwareupdate-Assistenten fest, wie nach neuen Treibern gesucht werden soll.  
Alternativ können Sie auch einen Datenträger mit aktuellen Treibern angeben.
- ▶ Stellen Sie den Assistenten fertig.



Windows 10 verwendet jetzt den neuen Treiber. Falls dieser Treiber ebenfalls Probleme verursacht, können Sie ihn zurücksetzen und den alten Treiber wieder einsetzen.

- ▶ Klicken Sie auf *Vorheriger Treiber* ②, um wieder den alten Treiber zu verwenden.



Die jeweils aktuellen Treiber und Datenbanken über problematische Treiber erhalten Sie, wenn Sie die Funktion *Windows Update* verwenden. Dabei werden die lokalen Treiberdatenbanken aktualisiert und können anschließend für die Aktualisierung installierter Gerätetreiber verwendet werden.

## Geräte verwalten mit den Windows-10-Einstellungen

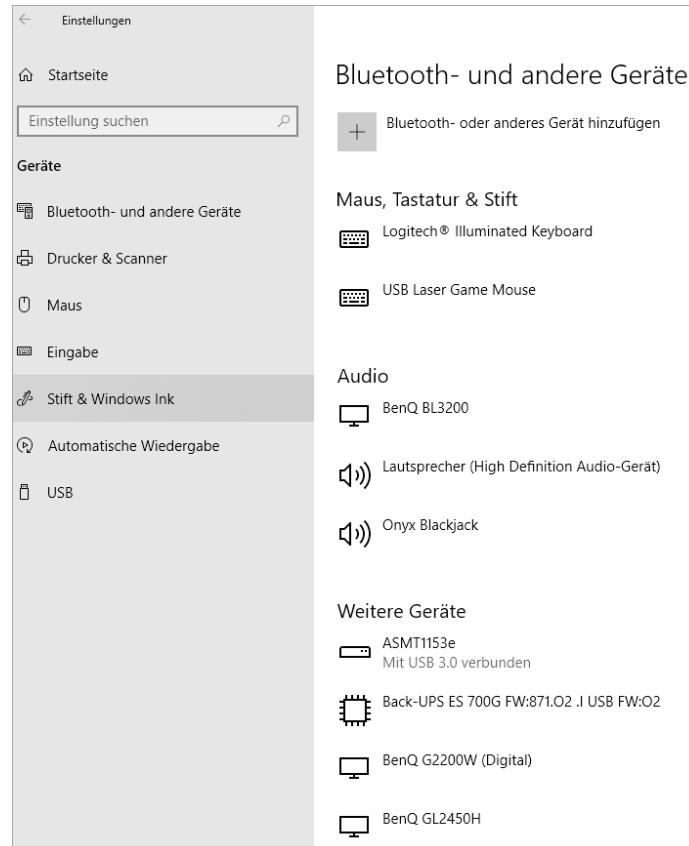
Windows 10 ermöglicht mit der Windows-App *Einstellungen*, angeschlossene Geräte zu verwalten.

- Rufen Sie über das Startmenü die *Einstellungen* auf. Wählen Sie den Bereich *Geräte*.
- oder* Drücken Sie und klicken Sie auf *Geräte*.

Hier können Sie neue Geräte hinzufügen und installierte Geräte entfernen (deinstallieren). Üblicherweise werden alle Geräte mit Plug & Play sofort beim Anschließen erkannt und installiert, deshalb muss die Suche selten manuell gestartet werden. Ältere Geräte findet die Suche nicht, und es können auch keine Legacy-Geräte hinzugefügt werden. Markieren Sie ein installiertes Gerät, können Sie das Gerät über die Schaltfläche *Gerät entfernen* deinstallieren.

Die Option *Download über getaktete Verbindungen* auf dieser Seite der Einstellungen ganz unten ist standardmäßig ausgeschaltet. Sie sorgt dafür, dass bei Wähl- oder Mobilfunkverbindungen keine Treiber und Software heruntergeladen werden, um Bandbreite und Kosten zu sparen.

Die Möglichkeiten, mit den Einstellungen Geräte zu installieren oder Einstellungen der Treiber zu ändern, sind im Vergleich zum vollwertigen Gerätemanager in der Systemsteuerung begrenzt. Für Tablet-PCs reichen die Möglichkeiten der Windows-Oberfläche aber oft aus.



## 9.6 Übung

### Treiber

**Übungsdatei:** --

**Ergebnisdatei:** *Uebung09\_E.pdf*

1. Wie können Sie Ihre geladenen Treiber anzeigen?
2. Wie aktualisieren Sie Treiber oder setzen diese zurück?
3. Mit welcher Windows-App können Sie angeschlossene Geräte verwalten?

# 10 Internetzugang einrichten und konfigurieren

## In diesem Kapitel erfahren Sie

- ✓ wie Sie einen Internetzugang erstellen
- ✓ wie Sie auf ein vorhandenes E-Mail-Konto zugreifen können
- ✓ wie Sie den Internet Explorer konfigurieren können
- ✓ wie Sie Sicherheitsvorkehrungen für den Zugriff auf das Internet treffen können

## Voraussetzungen

- ✓ Hinzufügen von Hardware
- ✓ Grundlagenwissen zu Netzwerken

## 10.1 Internetzugang – Grundlagen

### Windows 10 im Internet/Intranet

Windows 10 ist stark auf die Verwendung von Ressourcen im Internet ausgerichtet und die Installation und Verwendung von Windows-Apps ist ohne Internetzugang nicht möglich. Microsoft bietet jedem Windows-Benutzer mit einem **Microsoft-Konto** einen kostenlosen Online-Speicher namens **OneDrive**. Zusammen mit anderen kostenlosen Live-Diensten wird daraus Microsofts Version der Internet-Cloud. Alle Daten, die in der Cloud gespeichert wurden, sind auf jedem Gerät mit Internetzugang schnell verfügbar und leicht zu handhaben, was den Umgang mit verschiedenen Geräten mit Windows-Betriebssystem (Smartphone, Tablet und PC) erleichtern soll.



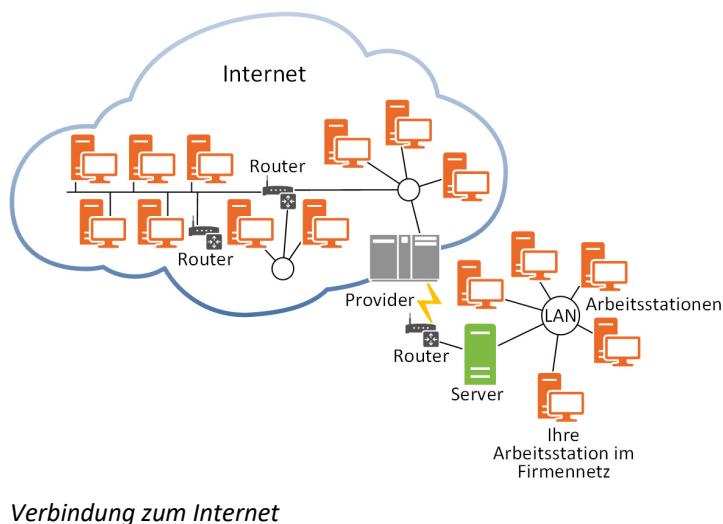
Wollen Sie OneDrive in Windows 10 nicht nutzen, können Sie das Programm über Gruppenrichtlinien deaktivieren. Dazu öffnen Sie den Editor für lokale Gruppenrichtlinien (`gredit.msc`) und navigieren zu *Computerkonfiguration - Administrative Vorlagen - Windows-Komponenten - OneDrive*. Hier finden Sie die passenden Einstellungen und können die Verwendung von OneDrive auf Unternehmenscomputern verhindern.

Die Wolke (Cloud) ist jederzeit erreichbar. Ähnlich wie die Benutzer im Firmennetzwerk nicht wissen müssen, auf welcher Festplatte und Hardware die Daten im Unternehmen physisch gespeichert werden, müssen auch die Cloud-Benutzer sich nicht mehr darum kümmern, auf welche Weise und an welchem Ort ihre Daten gespeichert werden. Wichtig ist nur, dass sie jederzeit Zugriff darauf haben. Im Unternehmen bietet die Cloud zwar viel-versprechende Möglichkeiten, es gibt jedoch auch Bedenken und potenzielle Gefahren.

Trotz der Ausrichtung auf Internetressourcen ist Windows 10 wie seine Vorgänger auch weiterhin für den Zugriff auf Ressourcen im lokalen Netzwerk geeignet, obwohl auch hier der Benutzer immer seltener wissen muss, ob die benötigten Ressourcen lokal vorhanden oder über das Internet erreichbar sind. Der Übergang ist fließend, so werden z. B. im Datei-Explorer **alle Pfadangaben** für Dateien genauso wie im Internet Explorer als **Adressen** bezeichnet.

Im Folgenden wird als Beispiel die Einrichtung eines Internetzugangs auf einer Workstation dargestellt, die sich in einem lokalen Firmennetzwerk befindet. Dabei wird angenommen, dass das LAN über folgende Gegebenheiten verfügt:

- ✓ eigene Internetdomäne,
- ✓ Webserver,
- ✓ **Router**, der das interne Firmennetz über einen **Provider** (Internetdienstanbieter) mit dem Internet verbindet,
- ✓ E-Mail-Server,
- ✓ Proxyserver.



### Aufgaben von Firewall und DMZ

Grundsätzlich sollte sich zwischen dem LAN und dem Internet eine Firewall befinden, über die alle Zugriffe auf das Internet erfolgen. Eine Firewall leitet nur bestimmte Anfragen weiter und wehrt alle anderen Zugriffsversuche ab. Bei höherem Sicherheitsbedarf kann die Firewall auch mit einer DMZ (**Demilitarized Zone**, entmilitarisierte Zone) kombiniert werden. Die DMZ ist ein gesicherter Bereich, über den sämtliche Verbindungen zwischen lokalem Netzwerk und Internet abgewickelt werden und in dem alle von außen erreichbaren Ressourcen wie E-Mail-Server, Webserver, Proxyserver bereitgestellt werden. Die DMZ trennt durch eine oder mehrere Firewalls das lokale Netz vollständig vom Internet und verfügt so über maximale Kontrolle über den Datenverkehr in beiden Richtungen. Durch die Einrichtung einer DMZ wird das lokale Netz bestmöglich abgeschirmt und vor Angriffen von außen geschützt.

### Grundbegriffe des Internets

Eigene Internetdomäne	Eine im Internet eingetragene Adresse, durch die ein Webserver eindeutig identifiziert werden kann. Zum Beispiel ist aus der Internetadresse <a href="http://www.herdt.de">www.herdt.de</a> ersichtlich, dass hier der HERDT-Verlag eine Internetdomäne in Deutschland mit seinem Namen betreibt.
E-Mail-Server	Er nimmt eingehende E-Mails an und leitet sie an den Empfänger weiter. Zudem nimmt er die abgeschickten E-Mails entgegen und bereitet sie zur Versendung im Internet vor.
Proxyserver	Ein Server, der stellvertretend (proxy = Stellvertreter) für Anfragen aus dem LAN (z. B. nach einer Internetseite) auf das Internet zugreift. Das Ergebnis (z. B. die gefundene Internetseite) wird an den anfragenden Rechner weitergeleitet. Häufig vorkommende Anfragen können oftmals aus dem lokalen Zwischenspeicher des Proxyservers beantwortet werden, was den Internet-Datenverkehr reduziert und Zugriffe beschleunigt. Ein Proxyserver kann mit Firewall-Funktionen ausgestattet sein.
Firewall	Damit wird Soft- bzw. Hardware bezeichnet, die den Zugriff von Rechnern aus dem LAN auf das Internet und vor allem umgekehrt aus Sicherheitsgründen beschränkt. Die Unterscheidung von erlaubten und unerlaubten Anfragen basiert dabei z. B. auf den verwendeten Protokollen oder den Quell- und Ziel-IP-Adressen.

## 10.2 Internetzugang einrichten

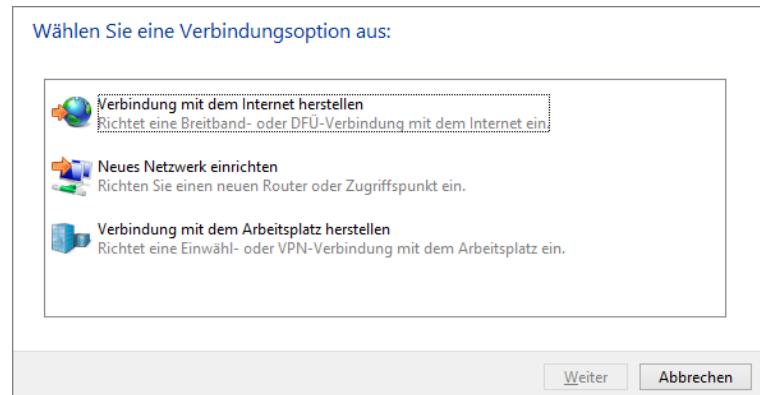
### Vorüberlegungen zum Internetzugang

Windows 10 ist auf einen Internetzugang ausgerichtet und versucht schon während der Installation, wichtige Sicherheitsupdates aus dem Internet herunterzuladen. Dies funktioniert allerdings nur, wenn Windows über einen passenden Treiber für den Netzwerkadapter verfügt. Der Computer muss über ein Netzwerkkabel mit einem Netzwerk verbunden sein, in dem ein DHCP-Server vorhanden ist.



In einem Netzwerk ohne DHCP können IP-Adresse, Default-Gateway und DNS-Server bei einer automatisierten Installation auch mithilfe der Antwortdatei *autoounattend.xml* übergeben werden. Auch eine Verwendung von WLAN-Adaptoren schon bei der Installation ist grundsätzlich möglich, erfordert aber erweiterte PowerShell-Kenntnisse.

Wenn Ihr Netzwerk über einen DHCP-Server verfügt, übermittelt dieser bei der Konfiguration neben der IP-Adresse üblicherweise auch die IP-Adresse des Standardgateways und des DNS-Servers, sodass keine weiteren Netzwerk-einstellungen vorgenommen werden müssen. Bei allen gängigen WLAN-Routern für DSL-Anschlüsse ist die DHCP-Funktion standardmäßig aktiviert. In einem Netzwerk ohne DHCP oder wenn Sie eine feste IP-Adresse vergeben möchten, müssen Sie diese Einstellungen wie in Kapitel 8 beschrieben manuell vornehmen.



Eine Verbindung oder ein Netzwerk einrichten

Wenn Sie den Zugang über eine Einwählverbindung, über ein VPN (Virtual Private Network), DSL-Adapter, UMTS-Modem, ISDN-Verbindung oder ein analoges Modem aufbauen wollen, müssen Sie die Verbindung zuerst einrichten. Hierbei unterstützt Sie in Windows 10 der Assistent für neue Verbindungen. Im Folgenden wird davon ausgegangen, dass die Hardware, die für die (Einwähl-)Verbindung genutzt werden soll, schon installiert wurde.

### Assistent starten

- ▶ Rufen Sie über das Kontextmenü der Netzwerkverbindung unten in der Taskleiste *Netzwerk- und Interneteinstellungen öffnen* auf und dann den Link *Netzwerk- und Freigabecenter*.
- ▶ Klicken Sie auf *Neue Verbindung oder neues Netzwerk einrichten*.
- ▶ Wählen Sie den Netzwerktyp, den Sie einrichten möchten, und klicken Sie auf *Weiter*.  
In den folgenden Dialogfenstern werden Sie durch die Einrichtung geführt. Dabei werden installierte Geräte gesucht und zur Auswahl angeboten. Wenn Sie die nötigen Anmeldedaten, Telefonnummern oder die Internetadresse bereithalten, ist die Einrichtung problemlos und schnell erledigt.

## 10.3 Internetzugang konfigurieren

### Übersicht über die Konfiguration des Internetzugangs

Zur optimierten Nutzung des Internetzugangs müssen Sie folgende Punkte auf dem Rechner konfigurieren:

- ✓ Windows-Firewall aktivieren/deaktivieren,
- ✓ Proxyserver einstellen, falls vorhanden.

## Proxyserver auswählen

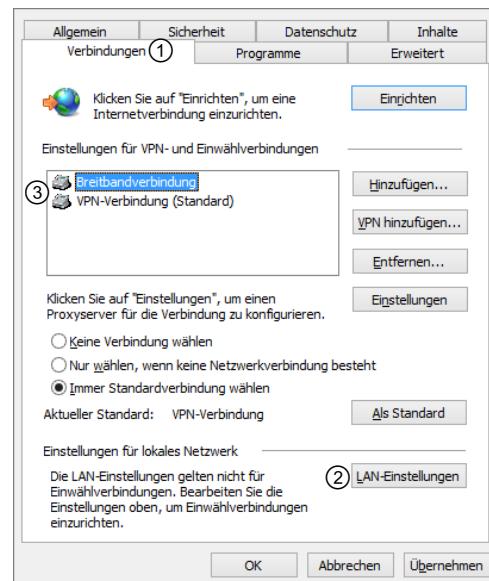
Für den Standard-Webbrowser von Windows 10 (Microsoft Edge) können Sie die automatische Erkennung von Proxyservern und deren Einstellungen nutzen oder selbst einen Proxyserver angeben und konfigurieren:

- ▶ Starten Sie die Systemsteuerung und suchen Sie nach *Internetoptionen*. Wechseln Sie in das Register *Verbindungen* ①.
- Hier können Sie getrennt die Einstellungen für Verbindungen über ein LAN ② und für VPN- oder Einwahlverbindungen ③ festlegen.
- ▶ Wählen Sie die entsprechende Schaltfläche *Einstellungen* bzw. *LAN-Einstellungen*.

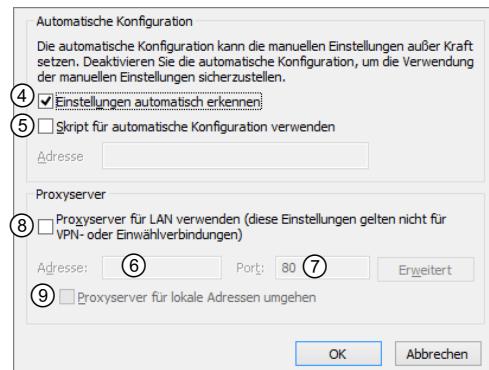
Da ein Proxyserver für eine Einwahlverbindung nur in bestimmten Fällen angegeben werden sollte, wird im Folgenden die Proxy-Konfiguration für das LAN ② gezeigt:

- ▶ Wählen Sie aus, ob die Konfiguration der Proxy-Einstellungen automatisch ablaufen soll ④ und ob dazu ein Skript zur Verfügung steht ⑤.
- ▶ Um selbst die Adresse ⑥ und den Port des Proxyservers ⑦ im LAN anzugeben, aktivieren Sie das Kontrollfeld ⑧ und geben Sie die Werte ein.
- ▶ Aktivieren Sie das Kontrollfeld ⑨, um für lokale Adressen den Proxyserver zu umgehen. Dies verbessert in den meisten Fällen die Zugriffsperformance, da Proxyserver meist für den Zugang zum Internet und seltener für das Intranet optimiert sind.

In Microsoft Edge finden Sie die Einstellungen über das Menü mit den drei Punkten oben rechts und der Auswahl von *Einstellungen - Erweiterte Einstellungen anzeigen - Proxeinstellungen öffnen*.



## Eigenschaften von Internet



*LAN-Einstellungen für einen Proxyserver*

## Windows-Firewall aktivieren/deaktivieren

Unter Windows 10 kann die Firewall den Netzwerkverkehr beschränken, den ein Rechner absendet und empfängt. Dazu werden die verwendeten Ports geprüft und nur bestimmte Ports erlaubt, sodass auch nur bestimmte Protokolle möglich sind (z. B. Port 80 für HTTP). Der Status wird für jede einzelne Anfrage gespeichert, die vom Rechner nach außen, also z. B. aus dem LAN ins Internet geschickt wird. Die Firewall lässt nur Antworten von außen (aus dem Internet) durch, für die auch Anfragen aus dem LAN vorliegen. Alle anderen eingehenden Anfragen werden standardmäßig blockiert. Die Firewall wird für Verbindungen mit dem Internet dringend empfohlen und bietet sich auch in Kombination mit einer Internetverbindungs freigabe an.

Die Windows-Firewall wurde hauptsächlich für Privatbenutzer und kleine Heimnetze konzipiert. Sie genügt grundlegenden Sicherheitsanforderungen und macht damit Personal Firewalls von Drittherstellern überflüssig. Die Firewall trägt in Windows 10, Version 1803 und neuer die neue Bezeichnung **Windows Defender Firewall**. Damit ist aber weiterhin die normale Windows-Firewall gemeint. Die Steuerungsinstrumente sind die gleichen.



Die Windows Defender Firewall verfügt über einen erweiterten Modus, in dem die Zugriffsregeln detailliert eingestellt werden können. Sie erreichen die Firewall mit erweiterter Sicherheit, indem Sie im Startmenü `firewall` ↩ eingeben. Für die erweiterten Einstellungen geben Sie `wf.msc` ein.

Obwohl die Windows Defender Firewall über einen großen Funktionsumfang verfügt, der in Firmennetzwerken auch zentral über Richtlinien konfiguriert werden kann, sollte sie in größeren Netzwerken keinesfalls die einzige Firewall sein, die die Computer und das Netzwerk schützt. In Firmennetzwerken sollte zur Ergänzung der Client-Firewalls an zentraler Stelle eine leistungsfähigere und flexiblere Hard- oder Softwarelösung eingesetzt werden.



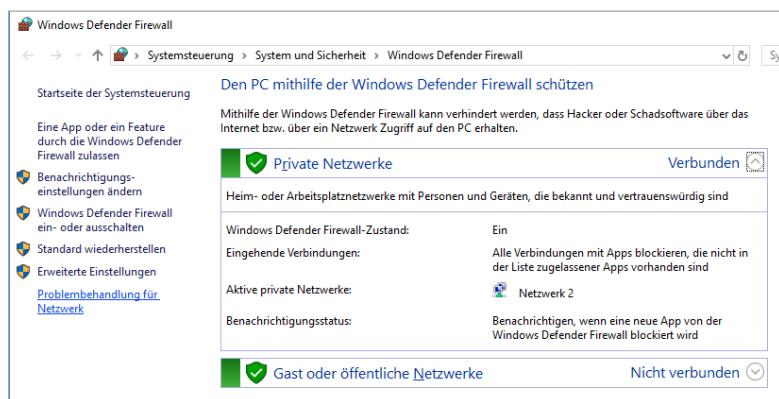
Unter Windows 10 können Sie die Firewall getrennt für Domänennetzwerke, private Netzwerke oder öffentliche Netzwerke einstellen. Wenn Sie sich mit Ihrem Notebook vom Firmennetzwerk abmelden und sich später in einem öffentlichen WLAN in einem Internet-Café einwählen, wird Windows 10 automatisch die Firewalleinstellungen für öffentliche Netzwerke benutzen.



Die von Windows 7/8/8.1 und Windows Vista her bekannten Heim- und Arbeitsplatznetzwerke werden unter **privaten Netzwerken** zusammengefasst.

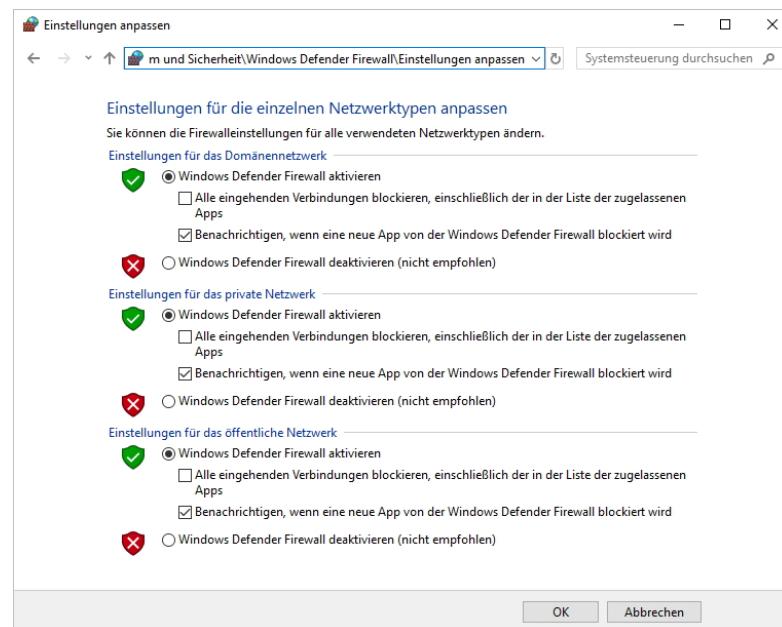
So stellen Sie die Firewall für die verschiedenen Netzwerktypen ein:

- Öffnen Sie *Systemsteuerung - System und Sicherheit - Windows Defender Firewall*. Alternativ suchen Sie im Startmenü nach `firewall.cpl`.
- oder Rufen Sie in der Systemsteuerung unter *Netzwerk- und Freigabe-center* die Windows Defender Firewall auf.
- Klicken Sie auf *Windows Defender Firewall ein- oder ausschalten*.



Im Dialog *Einstellungen anpassen* können Sie die Windows-Firewall deaktivieren oder wieder aktivieren.

Wenn Sie sich mit Ihrem Computer in einem potenziell unsicheren Netzwerk befinden (z. B. im WLAN an einem Flughafen oder im Firmennetzwerk einer Partnerfirma), können Sie jeden externen Zugriff unterbinden, indem Sie das Kontrollfeld markieren.



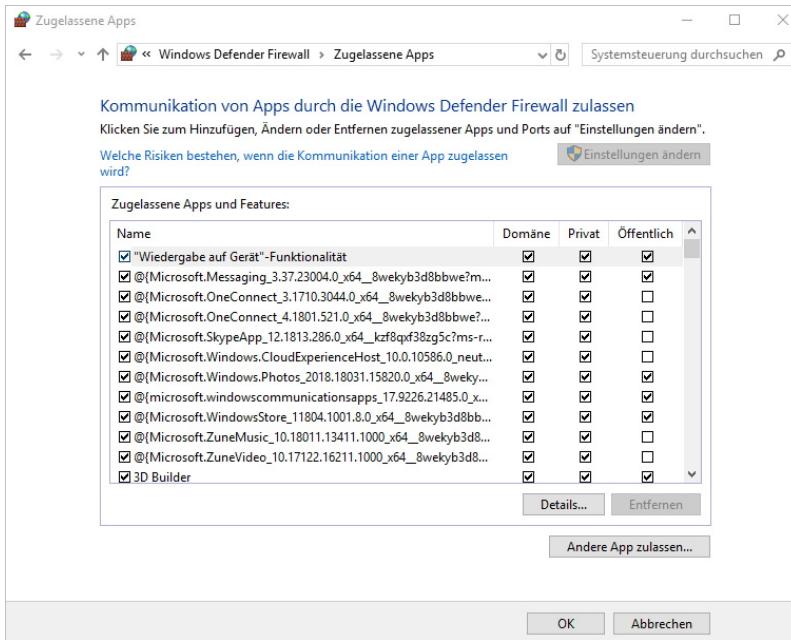
*Firewall für verschiedene Netzwerktypen ein- oder ausschalten*

### Ausnahmen definieren und bearbeiten

Für manche Anwendungen und Server-Funktionen werden Ausnahmen von den geltenden Firewallregeln benötigt. In der Standardeinstellung erlaubt die Windows Defender Firewall lediglich Remoteunterstützung und Zugriffe auf Datei- und Druckfreigaben innerhalb des lokalen Netzwerks, außerdem sind standardmäßig schon einige Ausnahmen für Microsoft-Anwendungen und -Dienste eingetragen. Durch die Installation von Windows-Apps oder Desktop-Anwendungen kommen weitere automatische Einträge hinzu.

Normalerweise werden die Ausnahmen während der Installation korrekt eingerichtet, in manchen Fällen ist aber ein manueller Eingriff erforderlich.

- Rufen Sie die Firewall-Ausnahmen auf, indem Sie auf *Eine App oder ein Feature durch die Windows Defender Firewall zulassen* klicken.



#### Ausnahmen für die Windows Defender Firewall definieren

- ▶ Aktivieren Sie das Kontrollfeld für den benötigten Dienst im entsprechenden Netzwerkprofil oder wählen Sie nach Betätigen der Schaltfläche *Andere App zulassen* ein Programm, dem Sie erlauben wollen, durch die Firewall hindurch Verbindungen entgegenzunehmen.

#### Windows Defender Security Center für mehr Sicherheit nutzen

- ▶ Öffnen Sie das Windows Defender Security Center in der Einstellungs-App von Windows 10 über die Schaltfläche *Windows Defender Security Center öffnen* im Bereich *Update und Sicherheit - Windows Defender*. Alternativ steht das Center auch als App im Startmenü zur Verfügung.

- ✓ Hier sind auf einen Blick die wichtigsten Sicherheitsinformationen für Windows 10 zu erkennen. Im oberen Bereich zeigt Windows 10 das Datum der Definitionsdateien des Virensenders an sowie das Datum der letzten Überprüfung.
- ✓ Über *Viren- & Bedrohungsschutz* kann eine schnelle oder gründliche Überprüfung gestartet werden. Außerdem ist hier zu sehen ob Bedrohungen gefunden wurden.
- ✓ Auch Einstellungen sind hier überprüfbar. Die Windows-Firewall trägt jetzt die Bezeichnung *Windows Defender Firewall*. Ansonsten hat sich an der Konfiguration nicht viel geändert.

The screenshot shows the Windows Defender Security Center main interface. On the left is a navigation sidebar with links like Startseite, Viren- & Bedrohungsschutz, Kontoschutz, Firewall- & Netzwerkschutz, App- & Browsersteuerung, Gerätesicherheit, Geräteleistung und -integrität, and Familienoptionen. The main area is titled 'Sicherheit auf einen Blick' (Security at a glance) and provides an overview of the device's security status across several categories:

- Viren- & Bedrohungsschutz:** Keine Aktion erforderlich.
- Kontoschutz:** Keine Aktion erforderlich.
- Firewall- & Netzwerkschutz:** Keine Aktion erforderlich.
- App- & Browsersteuerung:** Keine Aktion erforderlich.
- Gerätesicherheit:** Keine Aktion erforderlich.
- Geräteleistung und -integrität:** Keine Aktion erforderlich.
- Familienoptionen:** Verwalten Sie, wie Ihre Familie die Geräte verwendet.

Das Windows Defender Security Center

## 10.4 Internet Explorer und

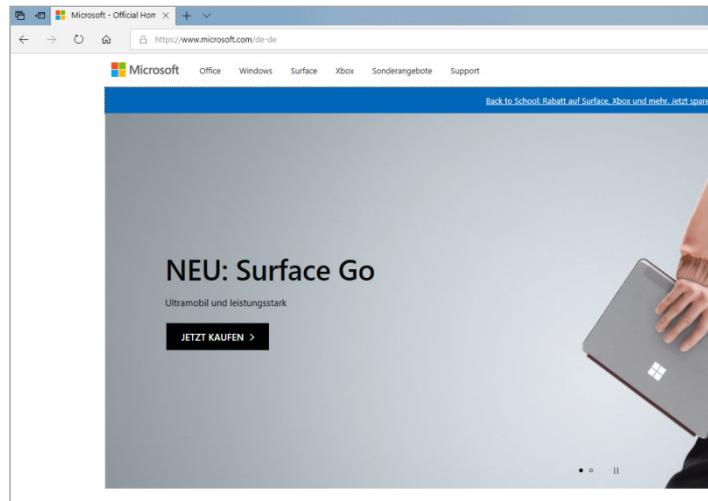
## Microsoft Edge konfigurieren

In Windows 10 steht weiterhin der Internet Explorer 11 zur Verfügung, aber auch der neue Microsoft Browser Edge. Dieser ist auch der Standardbrowser. Während es sich beim Internet Explorer um eine herkömmliche Desktop-Anwendung handelt, steht Microsoft Edge als Windows-App zur Verfügung. Die beiden Anwendungen haben nichts miteinander zu tun, sondern werden parallel auf dem System eingesetzt.

### Microsoft Edge

Mit dem Pluszeichen öffnen Sie eine neue leere Registerkarte, bei Edge **Tab** genannt. Wenn Sie auf das Symbol mit den drei Punkten  klicken und *Neues InPrivate-Fenster* wählen, öffnet sich ein neues Fenster, in dem Sie sicherer surfen, da keine Daten beim Surfen gespeichert werden.

Weitere Browser-Optionen finden Sie über  - *Einstellungen*.



### Internet Explorer 11

### Microsoft Edge als Windows-App

Der IE11 ähnelt im Funktionsumfang und Aufbau dem Vorgänger IE9/10. Gegenüber dem Vorgänger wurde die Geschwindigkeit verbessert und die CSS-Kompatibilität (**Cascading Style Sheets**, geschachtelte Gestaltungsvorlagen) erhöht. Neu ist die Unterstützung von HTML5 mit erweiterten Multimedia-Funktionen. Der Internet Explorer sollte nicht mehr zum Surfen verwendet werden, sondern nur noch für interne Webseiten, die Probleme mit Microsoft Edge oder einem anderen Browser haben.

### Internetoptionen einstellen

Neben den Netzwerksverbindungseinstellungen können Sie in den Internetoptionen Einstellungen zur Sicherheit, Privatsphäre und zu Webinhalten vornehmen:

- Starten Sie den Internet Explorer und wechseln Sie in das Menü *Extras - Internetoptionen*.

Vorgenommene Einstellungen gelten für den Internet Explorer. Um auch für Microsoft Edge einen Proxy festzulegen, rufen Sie über das Startmenü *Einstellungen - Netzwerk und Internet - Proxy* auf. Hier können Sie einen Proxy-Server hinterlegen.

### Registerkarte Allgemein

Hier können Sie:

- ✓ die Startseite festlegen,
- ✓ das Verhalten bei neuen Registerkarten (Tabs) einstellen,
- ✓ Browserverlauf und Internet-Cache einstellen und löschen,
- ✓ Darstellung, Farbe und Schriftgröße anpassen.

## Registerkarte Sicherheit

Hier können Sie die verschiedenen Internet-Sicherheitszonen einstellen.

### Internetzonen und Sicherheitsstufen des Internet Explorers

Das Sicherheitsmodell von Microsoft enthält vier verschiedene Zonen, denen eine Webseite zugeordnet wird: *Internet*, *Lokales Intranet*, *Vertrauenswürdige Sites* und *Eingeschränkte Sites*. Für jede Zone lassen sich die Sicherheitseinstellungen separat einstellen. Lokale Seiten haben weniger strenge Sicherheitsregeln als Internetseiten, und Sie können bei vertrauenswürdigen Seiten die Sicherheit reduzieren und diese im Gegenzug bei verdächtigen oder unerwünschten Seiten erhöhen. Es wird empfohlen, die Standardeinstellungen beizubehalten, Sie können die Einstellungen jedoch auch anpassen.

Zone	Standardstufe	Beschreibung
 Internet	Mittel bis hoch	Beinhaltet alle Internetseiten, die keiner der drei anderen Zonen zugeordnet wurden.
 Lokales Intranet	Niedrig	Beinhaltet alle Seiten des Intranets sowie die Seiten, die den Proxyserver umgehen. Sie können dieser Zone manuell weitere Seiten zuordnen.
 Vertrauenswürdige Sites	Mittel	Einzelne vertrauenswürdige Internetseiten können dieser Zone mit reduzierten Sicherheitsanforderungen zugeordnet werden.
 Eingeschränkte Sites	Hoch	Verdächtige Seiten sollten dieser Zone mit der höchsten Sicherheitsstufe zugeordnet werden. Sie sollten solche Seiten nur in Ausnahmefällen besuchen.

## Registerkarte Erweitert

In den erweiterten Sicherheitseinstellungen können Sie zusätzliche Funktionen wie den Smartscreen-Filter deaktivieren und z. B. das Verhalten bei verschlüsselten Seiten mit HTTPS und SSL oder veralteten, fehlenden oder zurückgezogenen Serverzertifikaten steuern.

Die hier getätigten Einstellungen gelten für alle Sicherheitsstufen und alle Zonen.

### Sicherheitseinstellungen mithilfe von Gruppenrichtlinien erzwingen



Standardmäßig können alle Benutzer der Workstation die Sicherheitseinstellungen des Internet Explorers selbst ändern. Dadurch könnten Sicherheitslücken entstehen. Als Administrator können Sie mithilfe von Gruppenrichtlinien die Sicherheitseinstellungen für den Internet Explorer für alle Benutzer fixieren. Verwenden Sie dazu das MMC-Snap-In *Gruppenrichtlinienobjekt-Editor*. Im Konsolenelement *Richtlinien für lokaler Computer - Computerkonfiguration - Administrative Vorlagen - Windows-Komponenten - Internet Explorer* können Sie den Zugriff aller Benutzer (auch des Administrators) auf die Sicherheitseinstellungen einschränken. Bevor Sie die Sicherheitseinstellungen ändern können, müssen Sie zunächst die bestehende Richtlinie aufheben.

## Registerkarte Datenschutz

Hier können Sie die Weitergabe des physischen Standorts und die Handhabung von Cookies sowie den Popup-Blocker einstellen. Sie können Symbolleisten und Add-ons im InPrivate-Modus deaktivieren, die sonst möglicherweise Rückschlüsse auf Ihre Surfgewohnheiten weitergeben könnten. Standardmäßig ist die Stufe *Mittel* eingestellt, Sie können aber auch höhere Sicherheitsstufen wählen, die bis zum vollständigen Blockieren aller Cookies gehen. Sie können außerdem Ausnahmeregeln für bestimmte Seiten erstellen.

## Registerkarte Inhalte

Hier können Sie Einstellungen zum Jugendschutz und zum Autovervollständigen vornehmen, Zertifikate ansehen und RSS-Feeds und Web Slices (Microsoft-eigenes Feed-Format) für Nachrichtenschlagzeilen und Kurzmeldungen aktivieren.

### Registerkarte *Programme*

Hier können Sie Add-ons für den Internet Explorer verwalten, die Standardanwendung für E-Mails, das Öffnen von URLs und das Bearbeiten von HTML-Dateien sowie verschiedene Dateitypen festlegen.

### Zurücksetzen von Internet Explorer auf die Standardeinstellungen

Durch das Zurücksetzen auf die Standardeinstellungen versetzen Sie den Internet Explorer in den Zustand, den er bei der Installation auf Ihrem Computer hatte. Dies ist bei der Behebung von Fehlern nützlich, die möglicherweise durch die Änderung von Einstellungen nach der Installation verursacht wurden. Durch das Zurücksetzen des Internet Explorers auf die Standardeinstellungen werden Ihre Favoriten und Feeds **nicht gelöscht**. Um den Internet Explorer zurückzusetzen, gehen Sie folgendermaßen vor:

- ▶ Schließen Sie alle geöffneten Internet Explorer- oder Explorer-Instanzen bis auf eine.
- ▶ Klicken Sie auf die Schaltfläche *Extras* (das Zahnradsymbol) und dann auf *Internetoptionen*.
- ▶ Wählen Sie auf der Registerkarte *Erweitert* die Schaltfläche *Zurücksetzen*.
- ▶ Klicken Sie im Dialogfeld *Internet Explorer-Einstellungen* zurücksetzen auf *Zurücksetzen*.
- ▶ Sobald der Internet Explorer die Wiederherstellung der Standardeinstellungen beendet hat, klicken Sie auf *Schließen* und dann auf *OK*.
- ▶ Schließen Sie den Internet Explorer.

Die Änderungen treten beim nächsten Start von Internet Explorer in Kraft. In manchen Fällen müssen Sie den PC neu starten, damit die Änderungen aktiv werden.



Startet der Internet Explorer nach Anpassungen nicht mehr, können Sie die Standardeinstellungen des Browsers über den Befehl `rundll32 inetcpl.cpl ResetIEtoDefaults` in einer Eingabeaufforderung wiederherstellen. Achten Sie auf die korrekte Groß- und Kleinschreibung.

### Einstellungen des Internet Explorers über Richtlinien vorgeben

Setzen Sie Windows 10 Pro oder Enterprise ein, können Sie viele Einstellungen des Internet Explorers auch mit Richtlinien vorgeben. Zusammen mit Windows Server 2012/2012 R2/2016 und Active Directory können Sie diese Richtlinien auch zentral für alle Computer im Unternehmen vorgeben.

Arbeiten Sie an einem Rechner mit mehreren Benutzerkonten, können Sie die Einstellungen für den Internet Explorer zentral vorgeben. Dazu starten Sie den Editor für lokale Gruppenrichtlinien durch Eingabe von `gpedit.msc` auf der Startseite.

- ✓ Die Einstellungen unter *Computerkonfiguration* wendet Windows an, wenn das System startet.
- ✓ Die Einstellungen unter *Benutzerkonfiguration* wendet Windows auf die Profile der einzelnen Anwender an, wenn sich diese beim PC anmelden.

In der Konsolenstruktur unter *Benutzerkonfiguration - Richtlinien - Administrative Vorlagen - Windows-Komponenten - Internet Explorer* können Sie den Internet Explorer über eine lokale Gruppenrichtlinie konfigurieren. Klicken Sie diesen Eintrag an, können Sie auf der rechten Seite die Clients konfigurieren.

Über den Knoten *Benutzerkonfiguration - Richtlinien - Administrative Vorlagen - Windows-Komponenten - Internet Explorer* in der Konsolenstruktur können Sie die Möglichkeit, Änderungen im Internet Explorer vorzunehmen, deaktivieren.

An dieser Stelle finden Sie zahlreiche Einstellmöglichkeiten für den Internet Explorer. Nehmen Sie diese vier vor:

- ✓ *Assistenten für Internetzugang deaktivieren*
- ✓ *Änderung der Verbindungseinstellungen deaktivieren*
- ✓ *Änderung der Proxyeinstellungen verhindern*
- ✓ *Änderung der Einstellungen für automatische Konfiguration deaktivieren*

### Kioskmodus des Internet Explorer nutzen

Eine Möglichkeit, den Internet Explorer immer im Vollbildmodus zu starten, ist der sogenannte **Kioskmodus**. Dazu erstellen Sie über das Kontextmenü des Desktops eine neue Verknüpfung und geben als Befehl "C:\Program Files\Internet Explorer\iexplore.exe" -k an.

Starten Sie den Internet Explorer über diese Verknüpfung, startet dieser immer im Vollbildmodus. Der Vollbildmodus lässt sich nicht beenden. Beenden können Sie den Browser in diesem Fall nur über den Task-Manager. Diesen starten Sie über **Strg Alt Entf**.

## 10.5 Microsoft Edge – Der neue Microsoft Browser

Beim Starten von Edge zeigt der Browser zunächst eine Standardseite mit verschiedenen Nachrichten an, die derzeit von den meisten Anwendern verwendet werden. Über die drei Punkte oben rechts erreichen Sie die Einstellungen von Microsoft Edge. Hier lassen sich verschiedene Startverhalten des Browsers hinterlegen.

Alternativ lassen sich Webseiten automatisch öffnen:

- ✓ die beim Schließen von Edge geöffnet waren (*Vorherige Seiten*)
- ✓ oder bestimmte benutzerdefinierte Startseiten (*Bestimmte Seite(n)*). Die Reihenfolge der Webadressen können Sie über Drag & Drop ändern. Entscheiden Sie sich zu einem späteren Zeitpunkt für eine andere *Öffnen mit*-Option, werden die erfassten benutzerdefinierten Webadressen gelöscht.

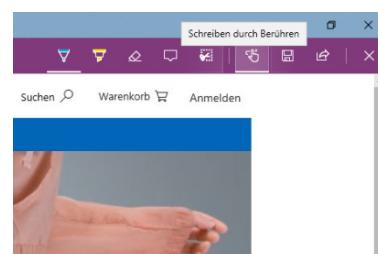
Im Bereich *Neue Tabs öffnen mit* können Sie das Verhalten von neuen Tabs steuern,

- ✓ ob Sie eine leere Seite öffnen wollen (*Leere Seite*)
- ✓ oder Informationen von derzeit beliebten Webseiten (*Beste Websites*)
- ✓ oder eine Liste der beliebtesten Websites und eine Auswahl wichtiger Informationen (*Beste Websites und empfohlener Inhalt*).

### Wesitennotizen erstellen und mit anderen Anwendern teilen

Neu in Microsoft Edge ist die Möglichkeit, Webseiten zu bearbeiten und danach mit anderen Anwendern zu teilen:

- Klicken Sie rechts oben im Menü auf *Notizen hinzufügen* . Danach stehen Ihnen Möglichkeiten zur Verfügung, Inhalte der Webseite zu markieren bzw. hervorzuheben, mit einer Notiz zu kommentieren und Teile der Webseite auszuschneiden. Die Webseitennotizen lassen sich z. B. in einem OneNote-Notizbuch speichern und auf diesem Weg auch offline oder auf anderen Rechnern verwenden.



Anwender haben die Möglichkeit, das OneNote-Notizbuch direkt in ihrem OneDrive-Konto zu speichern. Dadurch stehen die Notizen auf anderen Geräten zur Verfügung, lassen sich aber auch mit anderen Anwendern teilen. Über das Teilen-Symbol lassen sich Webseiten mit anderen Anwendern teilen, auch per E-Mail.

### Webseiten besser lesen und speichern

Microsoft Edge bietet einen **Lesemodus** für Webseiten, um das Lesen der Seiten angenehmer zu gestalten. Im Lesemodus werden die Seiten leseoptimiert angezeigt. Edge ändert dazu die Ansicht der Seite und passt diese an das Ausgabegerät an. Störende Teile der Webseite werden ausgeblendet, zum Beispiel Bilder, Werbung und interaktive Elemente.

Unterstützt eine Webseite diese Funktion, lässt sich der Lesemodus über die Schaltfläche  oben rechts aktivieren. Webseiten lassen sich im Lesemosus in Leselisten speichern und zwischen allen Geräten eines Anwenders synchronisieren.

### Webseiten an Startseite anheften oder als PDF speichern

Webseiten, die Anwender häufiger aufrufen, lassen sich über das Menü in Microsoft Edge im Startmenü speichern. Hier steht auch die Option zum Drucken zur Verfügung. Über das Druckmenü lassen sich Internetseiten mit *Microsoft Print to PDF* als PDF abspeichern.

Drucken  
An „Start“ anheften

### Microsoft Edge anpassen

Nach dem Starten des Browsers stehen über die drei Punkte oben rechts im Menü die Optionen von Microsoft Edge zur Verfügung. Diese Optionen hat Microsoft im Vergleich zum Internet Explorer deutlich abgespeckt. Am Ende der Optionen finden Sie *Einstellungen* und über die Einstellungen gelangen Sie mit *Erweiterte Einstellungen anzeigen* zu den erweiterten Einstellungen.

### Standard-Browser und Standard-Programme für Windows 10 festlegen

Nicht alle Anwender wollen Microsoft Edge nutzen. Andererseits wollen viele Anwender ihren Standard-Browser zu Microsoft Edge ändern. Diese Einstellungen werden am besten in der Einstellungs-App von Windows 10 gesteuert. Die Einstellungen der Standardprogramme sind über *Apps - Standard-Apps* zu finden. Hier lässt sich auch der Standardbrowser hinterlegen. Dieser wird automatisch geöffnet, wenn Anwender eine URL anklicken.

### Kennwörter speichern, Kennwortliste anzeigen und löschen

Wie bei anderen Browsern, können Anwender auch in Microsoft Edge Kennwörter für bestimmte Webdienste speichern. Dieses Verhalten lässt sich grundsätzlich über *Einstellungen - Erweiterte Einstellungen anzeigen* anpassen. Die Option ist über *Speichern von Kennwörtern anbieten* zu finden. Diese Option müssen Sie aktivieren. Durch den Link *Kennwörter verwalten* erhalten Sie eine Liste der gespeicherten Kennwörter und können sowohl die kompletten Kennworteinträge als auch die Bestandteile der einzelnen Kennworteinträge verwalten.

### Tastenkombinationen zum Surfen nutzen

Mit Tastenkombinationen können Anwender auch in Microsoft Edge schneller surfen. Edge bietet zahlreiche Tastenkombinationen, die teilweise auch mit Vorgängerversionen wie dem Internet Explorer funktionieren.

Tastenkombination	Funktion
 	Öffnet eine neue Registerkarte
 	Öffnet ein neues Fenster
 	Blendet das Favoritenfenster ein
 	Blendet die Leseliste ein
 	Blendet das Verlaufs-Fenster ein
 	Fügt die aktuelle Seite zu den Favoriten hinzu
 	Durchsucht eine Webseite nach einem Begriff
 ... 	Wechselt zwischen den geöffneten Registerkarten. Die Tastenkombination  wechselt zur letzten Registerkarte.
 	Kopiert die aktuell geöffnete Registerkarte zu einer neuen Registerkarte
 	Schließt die aktuelle Registerkarte
 	Öffnet den Download-Manager

Tastenkombination	Funktion
[Strg] [←]	Wechseln zwischen Registerkarten



### Ergänzende Lerninhalte: Nützliche Tastenkombinationen.pdf

Hier finden Sie weitere nützliche Tasten und Tastenkombinationen.

## Microsoft Edge im sicheren InPrivate-Modus betreiben

Eine wichtige Sicherheitsfunktion von Edge ist der InPrivate-Modus. Diesen gab es bereits im Internet Explorer. Aktivieren Anwender diesen Modus über [Strg] [↑] [P] beziehungsweise über [⋮], speichert Edge keinerlei temporäre Daten wie Cookies oder den Verlauf.

Anwender, die mit Edge sicherer unterwegs sein wollen, können über *Einstellungen - Erweiterte Einstellungen anzeigen* Sicherheitsoptionen setzen:

Einstellung	Hier können Sie...
Popups blockieren <input checked="" type="checkbox"/> Ein	Popups blockieren, damit beim Surfen keine Popup-Fenster erscheinen.
Adobe Flash Player verwenden <input checked="" type="checkbox"/> Ein	die Funktion ausschalten, falls Sie nicht ständig Adobe Flash-Seiten besuchen. Dazu wird der Schieberegler von <i>Adobe Flash Player verwenden</i> deaktiviert. Auf Wunsch lässt sich diese Funktion immer noch aktivieren, wenn Adobe auf einer Seite benötigt wird. Da Flash immer häufiger im Fokus von Angreifern steht, sollte die Funktion generell deaktiviert sein, außer Flash ist notwendig.
„Do Not Track“-Anforderungen (nicht nachverfolgen) senden <input type="checkbox"/> Aus	die Option „ <i>Do not Track</i> “-Anforderungen (nicht nachverfolgen) senden aktivieren. Das ist zwar kein zuverlässiger Schutz, verhindert aber dennoch grundsätzlich das Tracking von Webseiten, wenn besuchte Webseiten die Anforderungen unterstützen.
Cookies Alle Cookies blockieren	die Option <i>Alle Cookies blockieren</i> aktivieren. Das verhindert das Speichern von Cookies.
Browserdaten löschen Zu lösches Element auswählen	Um Cookies zu löschen, können Sie die Schaltfläche <i>Zu lösches Element auswählen</i> in den Einstellungen unter <i>Browserdaten löschen</i> verwenden. Durch die Auswahl dieser Option erscheint ein Auswahlmenü, mit dem Sie auswählen können, welche Cookies gelöscht werden.
Meinen PC mit SmartScreen-Filter vor schädlichen Websites und Downloads schützen <input checked="" type="checkbox"/> Ein	die neue Version des SmartScreen-Filters zum Schutz vor gefährlichen Webseiten aktivieren.

## Microsoft Edge wird verbessert

Mit Windows 10, Version 1803 wird auch Edge verbessert. Webseiten können über Edge das Info-Center von Windows 10 nutzen und Benachrichtigungen erstellen. Die Benachrichtigungen werden auch dann aktualisiert, wenn Edge nicht gestartet ist.

Microsoft Edge kann so konfiguriert werden, dass Videos auf Webseiten nicht automatisch abgespielt werden. Dazu kommt die Möglichkeit, dass Edge die Funktion erhält, Formulare automatisch auszufüllen. Tabs lassen sich einfacher stumm schalten, und der Dark-Mode bietet eine kontrastreiche Oberfläche beim Surfen.

Außerdem hat Microsoft den Vollbildmodus ([F11]) in Edge verbessert. Dieser zeigt die aktuell geöffnete Webseite im Vollbild an und erlaubt das einfachere Umschalten zwischen den anderen Webseiten in Edge. Im oberen Bereich kann die URL angezeigt werden.

Weitere Verbesserungen sind Kennwörter im privaten Modus und das Verwenden von Erweiterungen im privaten Modus. Das Speichern von Kennwörtern ist im privaten Modus natürlich auch weiterhin nicht erlaubt.

## 10.6 Remotedesktop einrichten

### Nutzen und Technik des Remotedesktops

Der Remotedesktop ermöglicht es einem Benutzer, einen anderen Computer fernzusteuern. So können Sie z. B. von Ihrem Bürocomputer auf Ihren zu Hause stehenden Windows-10-Rechner zugreifen. Auf dem Bülorechner sehen Sie dann den gleichen Windows-Desktop und haben alle Programme, Dateien und nahezu alle Funktionalitäten zur Verfügung, als wenn Sie direkt an Ihrem Rechner zu Hause säßen.

Windows 10 verwendet dazu das **Remote-Desktop-Protokoll** (RDP) und die Technik, mit der auch Terminaldienste auf Windows-Servern betrieben werden. Die RDP-Software ist seit Windows XP Teil des Betriebssystems. Auch für andere Betriebssysteme sind Remotedesktop-Clients verfügbar und so können Windows-Systeme auch von Linux-, UNIX und Mac-OS-Clients ferngesteuert werden. Das RDP sendet über die Netzwerkverbindung nur die Eingaben auf Tastatur und Maus zu dem Remoterechner und empfängt nur die Informationen über die geänderte Bildschirmanzeige. Die tatsächliche Programmabarbeitung findet auf dem Remoterechner statt.

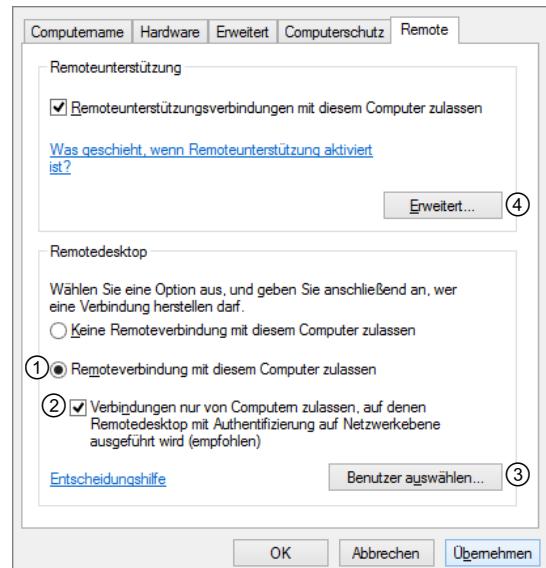
### Voraussetzungen für Remotedesktop

Für eine Remotedesktopverbindung müssen folgende Bedingungen erfüllt sein:

- ✓ Es muss eine Verbindung über das LAN oder das Internet zwischen Client- und Remoterechner bestehen.
- ✓ Auf dem Clientrechner muss Remotedesktopsoftware vorhanden sein.
- ✓ Auf dem Remoterechner muss die Funktion für Remotedesktop aktiviert sein (erfordert Administratorrechte).
- ✓ Sie müssen über ein lokales Konto oder Domänenkonto verfügen, um auf den Remoterechner über Remotedesktop zuzugreifen.

### Remotedesktop aktivieren

- Wählen Sie im Schnellzugriffsmenü *System* und klicken Sie auf *Remoteeinstellungen*.
- Erlauben Sie Remotedesktopverbindungen, indem Sie die Option ① aktivieren.  
Durch Deaktivieren des Kontrollfelds ② können auch ältere Computer mit Windows XP, die nicht über eine Netzwerkauthentifizierung verfügen, eine Verbindung aufzubauen. Es wird empfohlen, die Option aus Sicherheitsgründen aktiviert zu lassen.
- Unter *Benutzer auswählen* ③ können Sie Benutzer hinzufügen, die eine Remotedesktopverbindung herstellen dürfen. Administratoren ist es **automatisch** erlaubt, einen Zugriff über Remotedesktop aufzubauen.  
Unter *Erweitert* ④ können Sie das Remotesteuern abschalten, die Zeitdauer festlegen und bestimmen, dass Einladungen nur auf Computern mit Windows Vista und neuer ausgeführt werden können. Damit unterbinden Sie eine Remoteverbindung durch ältere Windows-Versionen und andere Betriebssysteme.
- Schließen Sie das Dialogfenster mit *OK*.



*Remotedesktop aktivieren*

## Remotedesktopverbindung aufbauen

Windows 10 verfügt über den von Windows 7/8/8.1 bekannten Remotedesktop-Client für den Desktop. Im Store finden Sie eine App zum Herunterladen und Installieren. Diese ist allerdings nicht so funktionsstark wie der Desktop-Client.

- ▶ Starten Sie die Remotedesktopverbindung, indem Sie im Startbildschirm `mstsc.exe` oder `remote` eingeben.

Sie können aus der Liste der zuletzt verwendeten Verbindungen wählen ① oder im Feld ② den Namen oder die IP-Adresse des Remotecomputers eingeben.

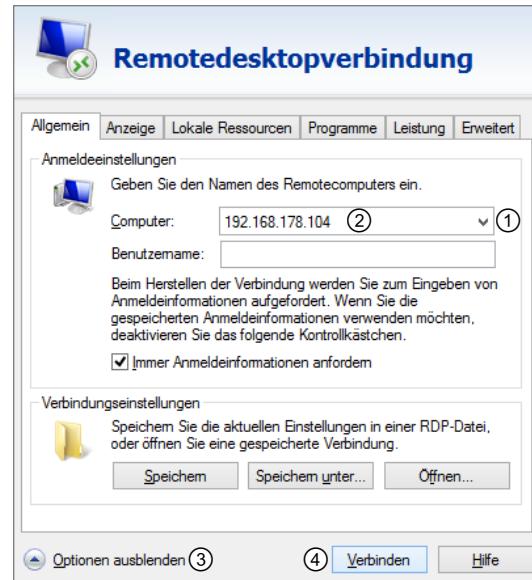
Unter *Optionen einblenden bzw. ausblenden* ③ haben Sie Zugriff auf weitere Verbindungsparameter.

Wenn Sie gespeicherte Anmeldeinformationen verwenden möchten, müssen Sie die Option *Immer Anmeldeinformationen anfordern* deaktivieren.

- ▶ Klicken Sie auf *Verbinden* ④, um die Verbindung herzustellen.

Bei einer Verbindung zu älteren Windows-Versionen erscheint eine Warnmeldung, dass die Verbindung nur geringe Sicherheit bietet. Bestätigen Sie dies mit *Verbinden*.

- ▶ Melden Sie sich mit einem auf dem Remotecomputer gültigen Benutzerkonto an.  
Sie sehen nun den Bildschirm des Remotecomputers vor sich.
- ▶ Um die Verbindung wieder zu beenden, melden Sie sich auf dem Remotecomputer ab, indem Sie auf *Trennen* klicken.



*Remotedesktopverbindung aufbauen*

## 10.7 Übung

### Windows-Firewall und Remotedesktop

Übungsdatei: --

Ergebnisdatei: *Uebung10\_E.pdf*

1. Wie rufen Sie die Verwaltungsprogramme der Windows-Firewall auf?
2. Wie aktivieren Sie den Remotedesktop?

# 11 Lokale Benutzerverwaltung

## In diesem Kapitel erfahren Sie

- ✓ wie Sie lokale Benutzer und Gruppen anlegen und verwalten
- ✓ wie Sie bestehende Gruppen und Benutzer auf einer Workstation integrieren
- ✓ wie Sie die Arbeitsumgebung für Benutzer einer Workstation anpassen

## Voraussetzungen

- ✓ Grundkenntnis des Netzwerkkonzeptes

## 11.1 Konzept der Benutzerverwaltung

### Benutzer und Benutzerkonten

Damit mehrere Personen an einem Windows-10-Computer arbeiten und auf Ressourcen lokal und im Netzwerk zugreifen können, wird jeder Person mindestens ein **Benutzerkonto** zugeordnet.

Das gesamte Sicherheitskonzept stützt sich auf diese Benutzerkonten. Immer wenn im Netzwerk auf eine Ressource zugegriffen werden soll, muss dies über eine kontogebundene Zugriffsberechtigung erlaubt werden. Es geht immer um die Frage: „Wer darf was?“ Nur so können bestimmten Benutzern speziell auf sie zugeschnittene Berechtigungen erteilt und die Zugriffe geregelt werden.

### Netzwerkressourcen und Objekte

Im Netzwerk geht es in erster Linie für die Benutzer darum, Zugriff auf Netzwerkressourcen wie Dateien, Datenbanken, Drucker und andere Geräte zu erhalten. Diese Ressourcen zählen zu den sogenannten **Objekten**, die aber auch Benutzer, Richtlinien oder andere Verwaltungseinheiten umfassen können. Objekte können in Objektklassen zusammengefasst werden, was die Organisation erheblich erleichtert.

### Gruppen

Zur Vereinfachung der Benutzerverwaltung lassen sich Benutzerkonten in **Gruppen** zusammenfassen. Die Regelung der Berechtigungen erfolgt dann über diese Gruppen. Eine Gruppe erhält für ein spezielles Objekt bestimmte **Berechtigungen**. Benutzer, die Mitglied der betreffenden Gruppe sind, übernehmen automatisch diese Berechtigung. Ein Benutzer muss mindestens einer Gruppe angehören, kann aber Mitglied beliebig vieler weiterer Gruppen sein.



Sie sollten Berechtigungen stets an Gruppen vergeben, niemals an einzelne Benutzer. Damit sorgen Sie für einen klaren strukturellen Aufbau und können bei späteren Änderungen, z. B. bei einem Abteilungswechsel, die Berechtigungen für den Mitarbeiter viel leichter anpassen.

## Benutzer- und Gruppenstruktur planen

Benutzer- und Gruppenstruktur sollten vor dem Aufbau eines Netzes **sorgfältig geplant** werden. Nur so lässt sich die Verwaltung effizient auf die zukünftigen Bedürfnisse der Benutzer und die notwendige Sicherheit abstimmen. Die Frage, die bei der Planung der Gruppenstruktur im Mittelpunkt steht, lautet: „Was braucht Benutzer X? Was darf er nicht?“ Entsprechend den Antworten wird seine Gruppenmitgliedschaft bestimmt. Diese Struktur sollte so einfach wie möglich gehalten werden und muss dabei allen Ansprüchen genügen. Schließlich sollte eine genaue Dokumentation der Benutzer- und Gruppenstruktur erfolgen, um Veränderungen effizient durchführen zu können.

## Benutzeranmeldung und Authentifizierung

Benutzer müssen sich anmelden, bevor sie an einem Computer unter Windows arbeiten und auf das Netzwerk zugreifen können. Dazu verwenden sie den **Anmeldenamen** ihres Benutzerkontos und ein **Kennwort**, es ist aber auch eine Authentifizierung durch PIN (persönliche Identifikationsnummer), Chipkarten, biometrische Methoden (Fingerabdruck, Iris, Stimme etc.) oder Bildcodes möglich, bei denen man bestimmte Punkte und Linien auf einem Bild nachfährt. Falls die Anmeldeinformationen gültig sind, wird der Benutzer authentifiziert.

Die Authentifizierung kann an verschiedenen Orten im Netzwerk durchgeführt werden. Es werden deshalb folgende Anmeldearten unterschieden:

Anmeldungsart	Mechanismus der Authentifizierung
Lokale Anmeldung (Computer in einer Windows-Arbeitsgruppe)	Kennwort und Benutzername werden lokal von dem Computer überprüft, an dem sich der Benutzer anmeldet. Die Authentifizierung gilt nur lokal, für Netzwerkgzugriffe ist eine zusätzliche Remoteanmeldung erforderlich.
Remoteanmeldung	Anmeldung für den Netzwerkgzugriff auf einen anderen Computer der Arbeitsgruppe oder einer fremden Domäne. Die Remoteanmeldung erfolgt automatisch und vom Benutzer unbemerkt, falls die lokalen Anmeldeinformationen auch für die fremde Ressource gültig sind (gleicher Benutzername und gleiches Kennwort).
Netzwerkanmeldung in der Windows-Domäne	Anmeldename und Kennwort werden im Active Directory überprüft. Das Zugriffsticket wird von einem sogenannten Schlüsselverteilungszentrum erstellt.

### Mechanismus der lokalen Authentifizierung

Für die lokale Authentifizierung ist der **Security Account Manager** (SAM) zuständig. Dabei werden Daten verwendet, die auf der lokalen Festplatte des Computers gespeichert sind. Da der SAM sicherheitskritische Daten wie Benutzernamen und Passwörter enthält, wird er besonders geschützt.

Der SAM ist im System an zwei Stellen zu finden:

- ✓ In der Registry unter: HKEY\_LOCAL\_MACHINE\SAM  
Dieser Ast in der Registrierung ist für direkte Zugriffe gesperrt.
- ✓ Als Datei unter: %Systemroot%\System32\Config\SAM, wobei auch diese Datei während des Betriebs von Windows für Zugriffe gesperrt ist.

Jedes Konto (Benutzer, Gruppe oder Computer) wird dabei durch eine eindeutige Identifizierungsnummer (**SID**, **Security Identifier**) repräsentiert, mit der das System die Benutzer unterscheidet. Für das System ist der Benutzername nur eine Zusatzinformation zur (Benutzer-)SID und kann ohne Einfluss auf die SID geändert werden.

Eine SID wird bei der Erstellung eines Kontos generiert und ist einmalig. Die SID wird nicht wiederverwendet, falls das Konto einmal gelöscht wurde. Ein neues Benutzerkonto mit dem gleichen Namen erhält eine neue SID, es handelt sich aus Sichtweise des Systems also um einen anderen Benutzer.



## Vordefinierte lokale Benutzer und Gruppen

Bei der Installation von Windows 10 werden einige Benutzerkonten und Gruppen automatisch angelegt und mit bestimmten Rechten ausgestattet.

### Vordefinierte Benutzerkonten

<b>Administrator</b>	Dieses Benutzerkonto ist auf jedem Windows-10-System vorhanden. Das Konto kann nicht gelöscht und nicht aus der Gruppe der Administratoren entfernt werden. Es ist aus Sicherheitsgründen bei Windows 10 standardmäßig deaktiviert und sollte nicht verwendet werden.
<b>Gast</b>	An diesem Konto werden Benutzer angemeldet, für die kein Benutzerkonto auf der Workstation angelegt ist. Es ist standardmäßig deaktiviert und sollte nur in Ausnahmefällen verwendet werden.
<b>&lt;erster Benutzer&gt;</b>	Dieses Benutzerkonto trägt den Namen, den Sie während der Installation eingegeben haben. Das Windows-10-Setup nimmt dieses Benutzerkonto automatisch in die Gruppe der Administratoren auf. Dieses Konto sollten Sie für administrative Tätigkeiten nutzen und für alltägliche Aufgaben ein weiteres Konto mit Benutzerrechten anlegen.

### Wichtige vordefinierte Gruppen

<b>Administratoren</b>	Alle Gruppenmitglieder können den Computer uneingeschränkt verwalten. Der erste Benutzer ist automatisch Gruppenmitglied. Gehört die Workstation einer Domäne an, erhält die globale Gruppe <i>Domänen-Admins</i> automatisch die Mitgliedschaft.
<b>Benutzer</b>	Das ist die Standardgruppe für gewöhnliche Benutzer. Diese Gruppe enthält alle Benutzer des Computers. Gehört der Computer einer Domäne an, erhält die globale Gruppe <i>Domänen-Benutzer</i> automatisch die Mitgliedschaft in der Gruppe.
<b>Gäste</b>	Über diese Gruppe definieren Sie die Rechte, die Sie fremden Personen gewähren wollen. Der Benutzer <i>Gast</i> ist Mitglied dieser Gruppe.
<b>Hauptbenutzer</b>	Hauptbenutzer sind in Windows 10 nur noch aus Gründen der Rückwärtskompatibilität vorhanden und sollten nicht mehr verwendet werden.
<b>Netzwerk-konfigurations-Operatoren</b>	Diese Gruppe dient zur Delegation von Verwaltungsaufgaben, welche die Netzwerkkonfiguration betreffen. Mitglieder dieser Gruppe haben eingeschränkte administrative Rechte zur Konfiguration des Netzwerks.
<b>Remotedesktop-benutzer</b>	Mitgliedern dieser Gruppe ist es erlaubt, eine Remotedesktopverbindung zu diesem Computer aufzubauen.
<b>Replikations-Operator</b>	Die Mitglieder verfügen über die nötigen Rechte, um den Verzeichnisreplikationsdienst zu starten.
<b>Sicherungs-Operatoren</b>	Mitglieder können Dateien sichern und wiederherstellen. Die Mitglieder dieser Gruppe besitzen alle Berechtigungen, die für Datensicherungen und die Wiederherstellung von gesicherten Informationen von einem Band erforderlich sind.

## 11.2 Anmelden

### Anmeldeoptionen auswählen

Standardmäßig müssen Sie für die Anmeldung in Windows 10 im Anmeldebildschirm auf das Benutzerkonto, mit dem Sie sich anmelden möchten, klicken und ein Kennwort eingeben. Erst dann werden Sie am System angemeldet.

### Automatisch anmelden mit Autologon

Das Anmelden mit einem Benutzerkonto ist aus Sicherheitsgründen nicht immer zwingend notwendig. Dies ist zum Beispiel dann der Fall, wenn Sie am entsprechenden Rechner alleine arbeiten, kein weiteres Benutzerkonto existiert und kein anderer Anwender Zugriff auf Ihr System hat. In diesem Fall ist die Anmeldung oft störender, als dass sie die Sicherheit erhöht.

Microsoft bietet daher das Sysinternals-Tool Autologon an (<http://technet.microsoft.com/de-de/sysinternals/bb963905>), mit dem Sie schnell und einfach eine automatische Anmeldung an Computern konfigurieren können. Das Tool funktioniert auch, wenn Sie ein Microsoft-Konto nutzen.

Das Tool Autologon verfügt über eine grafische Oberfläche und muss nicht installiert werden. Nach dem Start wird Ihnen ein Fenster angezeigt, in das Sie den Benutzernamen, das Kennwort und die Domäne oder den Rechnernamen eingeben, mit der zukünftig der Computer automatisch starten soll. Melden Sie sich mit einem Microsoft-Konto an, verwenden Sie als Username die Syntax:

*MicrosoftAccount\<E-Mail-Adresse, mit der Sie sich anmelden>.*

Username:	<input type="text" value="MicrosoftAccount\thomas"/>	<input type="button" value="Enable"/>
Domain:	<input type="text" value="WIN81"/>	<input type="button" value="Disable"/>
Password:	<input type="password" value="*****"/>	<input type="button" value="About"/>

Konfigurieren der automatischen  
Anmeldung an einem Computer

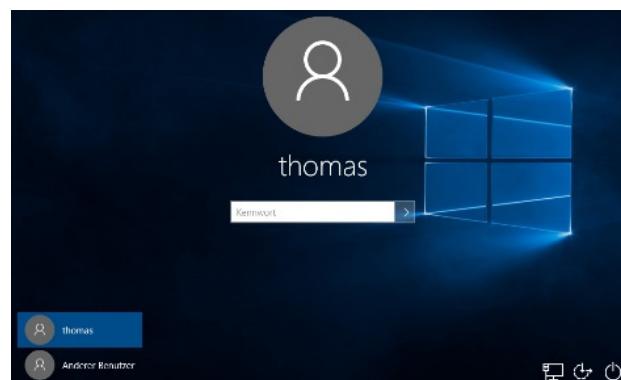
Klicken Sie auf *Enable*, ist die automatische Anmeldung aktiviert. Wollen Sie diese wieder ausschalten, starten Sie das Tool erneut und klicken auf die Schaltfläche *Disable*.

Das Tool installiert keine Erweiterungen auf dem Computer, sondern ändert lediglich Einträge in der Registry. Das Kennwort verschlüsselt das Tool, es ist aus der Registry nicht auslesbar.

### Art der Anmeldung umschalten

Die Anzeige aller Benutzernamen auf der Anmeldungsseite ist unter Sicherheitsgesichtspunkten bedenklich. In einer Domänenumgebung speichert Windows 10 üblicherweise den Namen des zuletzt angemeldeten Benutzers.

Sie können die Speicherung des letzten Benutzers über lokale Richtlinien oder Domänenrichtlinien ausschalten. Lokal geschieht das über den Editor für lokale Sicherheitsrichtlinien, den Sie im Startbildschirm durch Eingabe von `secpol.msc` aufrufen können. Alternativ können Sie den Editor über *Systemsteuerung - Verwaltung - Lokale Sicherheitsrichtlinie* aufrufen.



Klassische Benutzeranmeldung nach der Umstellung

- ▶ Um die Anzeige des letzten Benutzers zu unterbinden und die klassische Anmeldung mit Eingabe des Benutzernamens zu verwenden, aktivieren Sie im Editor für lokale Sicherheitsrichtlinien den Punkt *Sicherheitseinstellungen - Lokale Richtlinien - Sicherheitsoptionen - Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen*.

Richtlinie	Sicherheitseinstellung
Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken	Nicht definiert
Herunterfahren: Auslagerungsdatei des virtuellen Arbeitsspeichers löschen	Deaktiviert
Herunterfahren: Herunterfahren des Systems ohne Anmeldung zulassen	Aktiviert
Interaktive Anmeldung: Anwender vor Ablauf des Kennworts zum Ändern des Kennworts auf...	5 Tage
Interaktive Anmeldung: Anzahl zwischenzuspeichernder vorheriger Anmeldungen (für den Fa...	10 Anmeldungen
Interaktive Anmeldung: Benutzerinformationen anzeigen, wenn Sitzung gesperrt ist	Nicht definiert
Interaktive Anmeldung: Domänencontrollerauthentifizierung zum Aufheben der Sperrung de...	Deaktiviert
Interaktive Anmeldung: Inaktivitätsgrenze des Computers	Nicht definiert
Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich	Nicht definiert
<b>Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen</b>	<b>Aktiviert</b>
Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelden wollen	
Interaktive Anmeldung: Nachrichtentitel für Benutzer, die sich anmelden wollen	

Einstellungen zur Benutzeranmeldung mit „Secpol.msc“

Eine weitere Möglichkeit, die klassische Anmeldung einzuschalten, ist ein Eintrag in die Registry. Ändern Sie dazu in HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ den Wert von *dontdisplaylastusername* in "1" um.

**[Strg] [Alt] [Entf]** löst einen Hardware-Interrupt aus, der bei einigen Betriebssystemen für einen Neustart des Computers genutzt wird und bei Windows 10 fest mit der Windows-Sicherheit verbunden ist und zum Anmelde-dialog führt, wenn noch kein Benutzer angemeldet ist. Selbst ein Spionageprogramm, das vorgibt, die Windows-Anmeldung zu sein, wird nach dieser Tastenkombination in den Hintergrund befördert und der echte Login-Dialog wird angezeigt. Diese Methode bietet erhöhten Schutz vor Passwortspionage und ist deshalb für die Benutzeranmeldung empfehlenswert.

### Anmeldung in einer Domänenumgebung

Mit **[Strg] [Alt] [Entf]** gelangen Sie in das Dialogfenster zur Windows-Anmeldung.

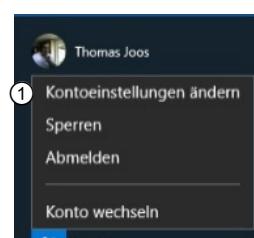
- Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.  
Beachten Sie beim Kennwort die Groß- und Kleinschreibung. Die Zeichen, die Sie eingeben, werden durch je einen Punkt repräsentiert.

Wollen Sie sich an einer anderen Domäne anmelden, so stellen Sie den Domänennamen vor Ihren Benutzernamen und trennen Sie ihn durch einen Backslash ab: Domänenname\Benutzername. Alternativ verwenden Sie die Syntax Benutzername@Domäne.

Wenn das System Sie nicht anmelden konnte, überprüfen Sie, ob versehentlich die Feststelltaste (Capslock) betätigt wurde. Beachten Sie, dass bei der Passwoerteingabe zwischen Groß- und Kleinschreibung unterschieden wird. Prüfen Sie außerdem links unten, ob das Tastaturlayout Ihrer Eingabesprache entspricht, und korrigieren Sie dies gegebenenfalls.

### Eigenes Benutzerkennwort des lokalen Kontos ändern

- Melden Sie sich wie gewohnt an.
- Klicken Sie im Startmenü auf Ihren Benutzernamen ganz oben.
- Klicken Sie auf *Kontoeinstellungen ändern* ①.
- Klicken Sie auf *Anmeldeoptionen* und dann bei *Kennwort* auf *Ändern*.
- Geben Sie Ihr altes Kennwort und anschließend das neue Kennwort ein.  
Über diesen Weg ändern Sie auch das Kennwort für Microsoft-Konten.



Anpassen von  
Benutzerkonten



Falls Sie sich mit einem Microsoft-Konto angemeldet haben, können Sie das Kennwort auch direkt auf der Internetseite <https://account.live.com/password/Change> ändern.

## 11.3 Benutzer verwalten

### Werkzeuge zur Benutzerverwaltung

Windows 10 bietet zahlreiche Möglichkeiten und Wege, um neue Benutzerkonten anzulegen und bestehende Konten zu verwalten:

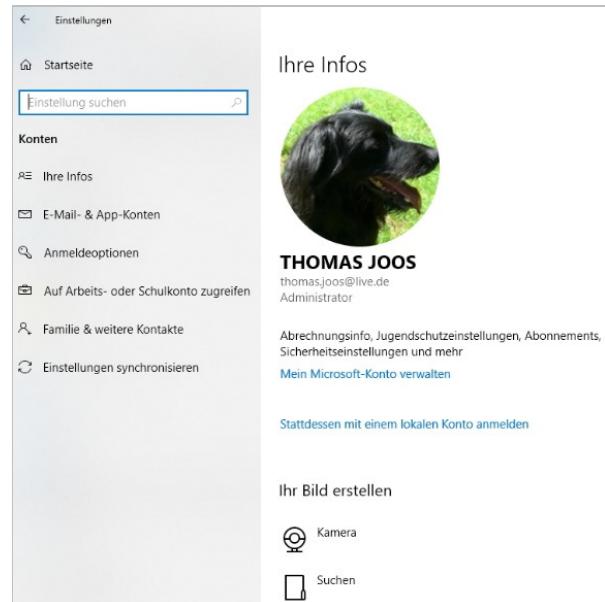
- ✓ den Bereich *Konten* in *Einstellungen*,
- ✓ *Benutzerkonten* in der Systemsteuerung,
- ✓ das MMC-Snap-In *Lokale Benutzer und Gruppen*, auch „Erweiterte Benutzerverwaltung“ genannt.

### Kontoeinstellungen

In den *Einstellungen* können Sie im Register *Konten* am eigenen Konto Einstellungen vornehmen und neue Benutzer hinzufügen.

Über *Einstellungen - Konten - Anmeldeoptionen* können Sie auch ein PIN für die Anmeldung verwenden. Diese PIN ist lediglich auf dem lokalen Rechner gültig, sperrt also zuverlässig Hacker aus.

Hier können Sie zwischen einem lokalen Konto und einem Microsoft-Konto wechseln, das eigene Kennwort ändern, einen Bildcode oder eine PIN als alternative Authentifizierungsmethode einrichten. Außerdem können Sie weitere Benutzer hinzufügen. Hier aktivieren Sie auch die neue Anmeldetechnologie **Windows Hello**. Allerdings steht die Option nur dann zur Verfügung, wenn Sie über einen Fingerabdruckscanner oder eine kompatible Webcam verfügen. Bei Microsoft-Konten wird stets die E-Mail-Adresse angegeben, ansonsten wird *Lokales Konto* angezeigt.



Anpassen der Benutzerkonten in Windows 10

Über den Link *Stattdessen mit einem lokalen Konto anmelden* können Sie jederzeit von einem Microsoft-Konto zu einem lokalen Konto oder einem Domänenkonto wechseln. Alle Daten und Einstellungen bleiben dabei erhalten.

Über den gleichen Weg wechseln Sie von einem lokalen Konto zu einem Microsoft-Konto, indem Sie den Link *Stattdessen mit einem Microsoft-Konto anmelden* auswählen. Bei der Umstellung hilft ein Assistent. Als Sicherheitseinstellungen werden die Einstellungen verwendet, die Sie in Ihrem Microsoft-Konto hinterlegt haben. Dieses erreichen Sie über die URL <https://account.microsoft.com>.

### Profilbild ändern

Sie können das eigene Profilbild über *Einstellungen - Konten - Ihre Infos - Suchen* ändern. Hier können Sie Ihren Computer nach Bildern durchsuchen oder mit einer angeschlossenen Webcam ein Foto machen. Falls Sie Bildbearbeitungs-Apps installiert haben, werden diese zur Erstellung eines Bildes angezeigt.

### Sperrbildschirm und Startmenü ändern

In *Einstellungen - Personalisierung* können Sie Einstellungen für den Sperrbildschirm und das Startmenü vornehmen.

## Einstellungen über die Systemsteuerung

Über **Systemsteuerung - Benutzerkonten** können Sie auch Einstellungen vornehmen, die sich mit *Einstellungen* im Startmenü nicht bewerkstelligen lassen, z. B. Einstellungen für andere lokale Benutzerkonten.

Hier können Sie alle eigenen Anmeldeinformationen für das Netzwerk und das Internet verwalten ①, eine Kennwortrücksetzdiskette erstellen ②, EFS-Verschlüsselungszertifikate verwalten ③, den Kontotyp umstellen ④ und eigene Umgebungsvariablen ändern ⑤ sowie weitere Programme in der Systemsteuerung öffnen ⑥.

Sie können außerdem in die Einstellungen für Benutzer wechseln ⑦, den eigenen Kontonamen ⑧ oder Kontotyp ⑨ ändern oder ein anderes Konto verwalten ⑩.

Sie können in der Systemsteuerung auch Einstellungen zur Benutzerkontensteuerung (UAC) vornehmen ⑪.



*Benutzerkonteneinstellungen in der Systemsteuerung*

## Benutzerkontensteuerung anpassen

Auch wenn die Benutzerkontensteuerung einige Sicherheit bietet und in Windows 10 nicht mehr so viele Informationen zeigt wie noch bei Windows Vista/7, hat sie vor allem für geübte Anwender den Nachteil, dass sehr viele Anpassungen am System erst bestätigt werden müssen.

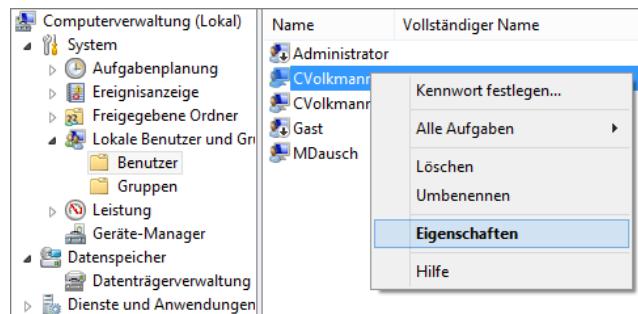
Die Benutzerkontensteuerung (**User Account Control, UAC**) blendet dazu den Desktop aus und zeigt ein Meldungsfeld an. Viele Poweranwender wollen diese Schutzfunktion daher zunächst deaktivieren, bevor sie Windows 10 an ihre Bedürfnisse anpassen. Sie finden die Konfiguration der Benutzerkontensteuerung über *Sicherheit und Wartung* und die Auswahl des Menüpunkts *Einstellungen der Benutzerkontensteuerung ändern*. Am schnellsten rufen Sie das Wartungscenter über das Suchfeld der Taskleiste auf.

Auf PCs in Unternehmen mit Active Directory oder auch auf einzelnen Computern lässt sich das Verhalten der Benutzerkontensteuerung auch per Gruppenrichtlinie konfigurieren. Die dazu notwendigen Einstellungen finden Sie über *Computerkonfiguration - Windows-Einstellungen - Sicherheitseinstellungen - Lokale Richtlinien - Sicherheitsoptionen* (vgl. Abschnitt 12.3).

## Lokale Benutzer verwalten über die Computerverwaltung

Die Benutzereinstellungen über die Windows-App und die Systemsteuerung richten sich eher an normale Benutzer, während das MMC-Snap-In *Lokale Benutzer und Gruppen* besser für Systembetreuer geeignet ist und erweiterte Möglichkeiten bietet. Das Snap-In kann auch separat als *lusrmgr.msc* (Local User Manager) aufgerufen werden.

- ▶ Klicken Sie im Schnellzugriffsmenü auf *Computerverwaltung* oder öffnen Sie eine MMC mit hinzugefügtem Snap-In *Lokale Benutzer und Gruppen*. Alternativ können Sie auch im Startmenü `lusrmgr.msc` eingeben.
- ▶ Klicken Sie doppelt auf *Lokale Benutzer und Gruppen* und anschließend auf *Benutzer*.
- ▶ Klicken Sie mit der rechten Maustaste auf das Symbol des Benutzers, den Sie bearbeiten wollen, und rufen Sie den Kontextmenüpunkt *Eigenschaften* auf, um die kompletten Optionen zur Benutzerverwaltung zur Verfügung zu haben.



Lokale Benutzer- und Gruppenverwaltung

### Neuen Benutzer anlegen

- ▶ Klicken Sie im linken Bereich mit der rechten Maustaste auf den Knoten *Benutzer* und wählen Sie den Kontextmenüpunkt *Neuer Benutzer*.
- ▶ Geben Sie nun den Benutzernamen ① und optional den vollständigen Namen und eine Beschreibung des Benutzers ein.
- ▶ Geben Sie das Kennwort ein ②.
- ▶ Wählen Sie, ob der Benutzer das Kennwort bei der Anmeldung ändern muss ③ und ob das Konto zunächst deaktiviert sein soll ④.
- ▶ Klicken Sie auf *Erstellen*, um das Konto anzulegen.

The screenshot shows the 'Neuer Benutzer' (New User) dialog box. It contains fields for 'Benutzername' (User name) ①, 'Vollständiger Name' (Full name), 'Beschreibung' (Description), 'Kennwort' (Password) ②, and 'Kennwort bestätigen' (Confirm password). Below these are four checkboxes: ③ 'Benutzer muss Kennwort bei der nächsten Anmeldung ändern' (User must change password at next login), ④ 'Benutzer kann Kennwort nicht ändern' (User cannot change password), ⑤ 'Kennwort läuft nie ab' (Password never expires), and ⑥ 'Konto ist deaktiviert' (Account is disabled). At the bottom are 'Hilfe', 'Erstellen' (Create), and 'Schließen' (Close) buttons.

### Deaktivierte Konten und gesperrte Konten

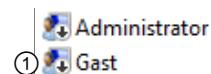
Wenn ein Benutzer nicht mehr auf sein Konto zugreifen kann, kann dies folgende Gründe haben:

- ✓ Der Benutzername oder das Kennwort wurde falsch geschrieben.
- ✓ Der Benutzer verfügt über kein Konto an dem Anmeldeort (kein lokales Konto / kein Domänenkonto).
- ✓ Das Konto wurde von einem Administrator deaktiviert.
- ✓ Das Konto wurde vom System gesperrt, weil ein Verstoß gegen die Sicherheitsrichtlinien vorliegt.

### Konto deaktivieren

Wenn Sie ein Konto für eine gewisse Zeitspanne unzugänglich machen möchten, sollten Sie das Konto deaktivieren. Dadurch können Sie z. B. einen unerlaubten Zugriff auf ein nur manchmal benötigtes Konto wie das Gastkonto regulieren oder ein Benutzerkonto während der Urlaubszeit deaktivieren.

- ▶ Klicken Sie in *Lokale Benutzer und Gruppen - Benutzer* mit der rechten Maustaste auf einen Benutzer und wählen Sie im Kontextmenü *Eigenschaften*.
  - ▶ Aktivieren Sie im folgenden Dialog das Kontrollfeld *Konto ist deaktiviert*. Bestätigen Sie anschließend mit *OK*.
- Deaktivierte Benutzerkonten werden genau wie deaktivierte Geräte im Gerät-Manager mit einem kleinen schwarzen Pfeil nach unten in einem weißen Kreis gekennzeichnet ①.



Deaktivierte Konten

## Konto aktivieren

Um das Konto wieder zu aktivieren, entfernen Sie das Häkchen im Kontrollfeld *Konto ist deaktiviert*.

## Konto sperren

Um einen unerlaubten Zugriff auf ein Konto zu verhindern, können Sie mittels einer Richtlinie festlegen, dass ein Konto nach einer gewissen Anzahl von fehlerhaften Kennworteingaben für einen bestimmten Zeitraum gesperrt und danach wieder freigegeben wird. Die entsprechende Gruppenrichtlinie können Sie im Gruppenrichtlinieneditor bearbeiten:

- ▶ Geben Sie im Startbildschirm `gpedit.msc` ein.
- ▶ Wechseln Sie zu *Computerkonfiguration - Windows-Einstellungen - Sicherheitseinstellungen - Kontorichtlinien - Kontosperrungsrichtlinien*.
- ▶ Legen Sie in der Richtlinie *Kontosperrungsschwelle* fest, nach wie vielen fehlgeschlagenen Anmeldeversuchen ein Konto gesperrt wird.
- ▶ Legen Sie unter *Kontosperrdauer* fest, ob und nach welcher Zeit ein gesperrtes Konto automatisch wieder entsperrt wird.
- ▶ Legen Sie die Zurücksetzungsdauer des Kontosperrungszählers fest.

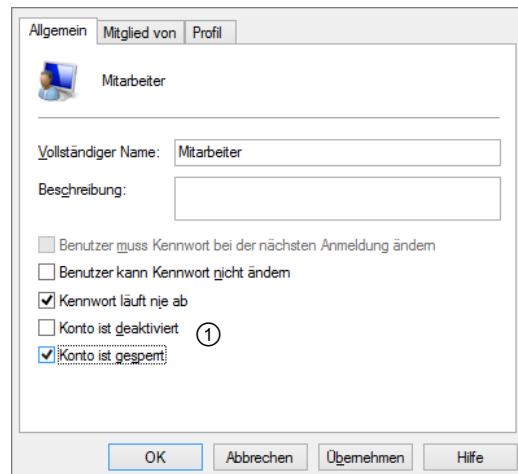
## Konto entsperren

- ▶ Rufen Sie in der MMC *Lusrmgr.msc* (Local User Manager) die Eigenschaften des Benutzers auf, dessen Konto Sie entsperren möchten, indem Sie auf das Symbol des Benutzers einen Doppelklick ausführen.
- ▶ Entfernen Sie nun das Häkchen im Kontrollfeld *Konto ist gesperrt* ① und klicken Sie auf *OK*.

Da die Kontosperrung nur vom System vorgenommen werden kann, ist das Kontrollfeld inaktiv, wenn keine Sperrung vorhanden ist.

 Wenn die Kontosperrung so lange aktiv bleiben soll, bis ein Administrator die Sperrung aufhebt, müssen Sie in der Richtlinie die Dauer auf 0 setzen. Eine Einstellung für diesen Wert lässt sich aber nur vornehmen, wenn auch ein Wert für die zulässige Höchstanzahl der Anmeldeversuche eingegeben wurde.

Seien Sie vorsichtig beim Setzen dieser Werte. Benutzer, die sich nicht am System anmelden können, verursachen Arbeitsaufwand beim Administrator.



*Kontosperrung aufheben*

## Konto umbenennen

Wenn ein Benutzer etwa durch eine Heirat einen neuen Namen annimmt, ist es nicht sinnvoll, ein neues Konto zuzuweisen, sondern das Konto umzubenennen, um so die Gruppenzugehörigkeiten und andere Einstellungen für den neuen Benutzernamen zu übernehmen.

- ▶ Öffnen Sie das Snap-In *Computerverwaltung* und wechseln Sie zu *Computerverwaltung (Lokal) - System - Lokale Benutzer und Gruppen - Benutzer*.
- ▶ Klicken Sie mit der rechten Maustaste auf den Benutzernamen, den Sie verändern wollen, und wählen Sie den Kontextmenüpunkt *Umbenennen*.
- ▶ Geben Sie den neuen Benutzernamen ein und bestätigen Sie mit ↵.

## Konto löschen

Benutzen Sie das Snap-In *Lokale Benutzer und Gruppen* in der MMC, um ein Konto zu löschen. Denken Sie daran, dass das Löschen eines Kontos **nicht** wieder rückgängig gemacht werden kann. Mit dem Löschen eines Kontos werden auch sämtliche Pfade, Rechte und Berechtigungen sowie Einstellungen unwiederbringlich gelöscht.

Selbst wenn Sie sofort nach dem Löschen ein neues Konto mit dem alten Benutzernamen anlegen, wird dies aus der Sicht des Betriebssystems ein anderes Konto sein, da automatisch eine neue SID generiert und zugeordnet wird. Darum sollten Sie im Hinblick auf eine mögliche Rückkehr oder späteren Zugriff auf die Benutzerdaten eine Deaktivierung des Kontos vorziehen. Löschen Sie das Benutzerkonto erst, wenn sicher ist, dass keinerlei Daten mehr benötigt werden.



- ▶ Öffnen Sie das Snap-In *Computerverwaltung* und wechseln Sie zu *Computerverwaltung (Lokal) - System - Lokale Benutzer und Gruppen - Benutzer*.
- ▶ Klicken Sie mit der rechten Maustaste auf den Benutzer, den Sie löschen wollen, und wählen Sie den Kontextmenüpunkt *Löschen*.
- ▶ Bestätigen Sie den Vorgang mit *Ja*.

## Windows 10 vor unbefugtem Zugriff schützen

In Windows 10 Pro und Enterprise können Sie alle fehlgeschlagenen Anmeldeversuche protokollieren lassen:

- ▶ Rufen Sie über die Startseite `secpol.msc` auf.
- ▶ Navigieren Sie zu *Sicherheitseinstellungen - Lokale Richtlinien - Überwachungsrichtlinie*.
- ▶ Aktivieren Sie bei *Anmeldeversuche überwachen* die Option *Fehler*. Aktivieren Sie außerdem *Erfolgreich*, protokolliert Windows auch erfolgreiche Anmeldungen.

Das Überwachungsprotokoll finden Sie in der Ereignisanzeige:

- ▶ Rufen Sie über die Startseite `eventvwr.msc` auf.
  - ▶ Klicken Sie auf *Windows-Protokolle - Sicherheit*.
- Hier sehen Sie die verschiedenen Anmeldungen am Rechner, auch die Anmeldungen über andere Rechner, wenn Sie den Computer in einer Heimnetzwerkgruppe aufgenommen haben.

Setzen Sie Windows 10 Pro oder Enterprise ein, haben Sie die Möglichkeit, über lokale Richtlinien Sicherheits-einstellungen vorzunehmen. Eine dieser Möglichkeiten ist die Festlegung, dass sich Windows nach einer bestimmten Anzahl von ungültigen Anmeldeversuchen automatisch sperren kann:

- ▶ Rufen Sie über die Startseite `gpedit.msc` auf.
- ▶ Navigieren Sie zu *Computerkonfiguration - Windows-Einstellungen - Sicherheitseinstellungen - Kontorichtlinien - Kontosperrungsrichtlinien*.
- ▶ Klicken Sie doppelt auf *Kontosperrungsschwelle*.
- ▶ Geben Sie die Anzahl zulässiger Login-Versuche bis zur Sperrung ein.
- ▶ Mit *Kontosperrdauer* legen Sie fest, wie lange das Konto gesperrt sein soll.
- ▶ Über *Zurücksetzungsdauer des Kontosperrungszählers* tragen Sie die Zeitspanne ein, nach der Windows erneut mit dem Zählen beginnt.

Auf der Registerkarte *Erklärung* finden Sie zu den Einstellungen eine ausführliche Hilfe.

Gibt ein Benutzer das Kennwort so oft falsch ein, wie Sie in der Kontosperrungsschwelle eingegeben haben, wird es gesperrt. Dem Benutzer wird eine Information angezeigt.

Sie können als Administrator die Sperrung aufheben. Dazu melden Sie sich an und rufen über die Startseite den Befehl `lusrmgr.msc` auf. Zeigen Sie die Eigenschaften des Benutzers an und entfernen Sie das Häkchen bei *Konto ist gesperrt*.

## 11.4 Lokale Gruppen verwalten

### Lokale Gruppe und Gruppenmitgliedschaft

Eine **lokale Gruppe** dient der Steuerung von Zugriffsberechtigungen für Ressourcen auf diesem Computer. Durch Mitgliedschaft in einer lokalen Gruppe mit bestimmten Berechtigungen für die lokale Ressource, z. B. eine Netzwerkfreigabe, erhalten Benutzer die Möglichkeit, darauf zuzugreifen.

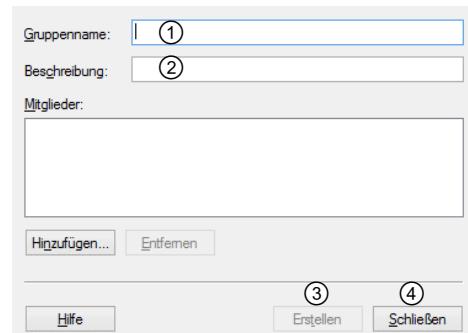


Die meisten Firmen verfügen über eine Active Directory-Domäne, wo alle Berechtigungen durch domänenlokale oder globale Gruppen zentral gesteuert werden. In Domänen werden Sie daher nur selten mit lokalen Gruppen arbeiten.

**Beispiel:** In einer Arbeitsgruppe wird eine neue Sekretärin der lokalen Gruppe *Sekretariat* hinzugefügt und hat damit automatisch die Berechtigung, auf Dateien und Programme zuzugreifen, die sie benötigt. Soll die Sekretärin auf der anderen Seite nicht mehr die Berechtigungen haben, auf bestimmte Anwendungen und Daten zuzugreifen, werden die Berechtigungen automatisch entfernt, wenn sie aus der Gruppe *Sekretariat* entfernt wird.

### Lokale Gruppen anlegen

- ▶ Klicken Sie im Schnellzugriffsmenü auf *Computerverwaltung* und wechseln Sie zu *Computerverwaltung (Lokal) - System - Lokale Benutzer und Gruppen*.
- ▶ Klicken Sie mit der rechten Maustaste auf *Gruppen* und wählen Sie den Kontextmenüpunkt *Neue Gruppe*.
- ▶ Geben Sie nun den Gruppennamen ① und eine Beschreibung der Gruppe ② (optional) ein und bestätigen Sie mit *Erstellen* ③.
- ▶ Um den Assistenten für das Erstellen neuer Gruppen zu verlassen, klicken Sie auf *Schließen* ④.



### Lokale Gruppenmitgliedschaft verwalten

Sie können einer neuen Gruppe gleich beim Erstellen Mitglieder hinzufügen oder Sie fügen später einer bereits existierenden Gruppe Mitglieder hinzu.

- ▶ Klicken Sie im Schnellzugriffsmenü auf *Computerverwaltung* und wechseln Sie zu *Computerverwaltung (Lokal) - System - Lokale Benutzer und Gruppen - Gruppen*.
- ▶ Klicken Sie mit der rechten Maustaste auf die Gruppe, deren Mitglieder Sie verwalten möchten, und wählen Sie im Kontextmenü *Eigenschaften*.

Sie sehen eine Liste der Mitglieder der Gruppe.

Durch Auswahl von Objekten im Bereich *Mitglieder* und Klicken von *Entfernen* können Sie Benutzer oder Gruppen aus der Gruppe entfernen.

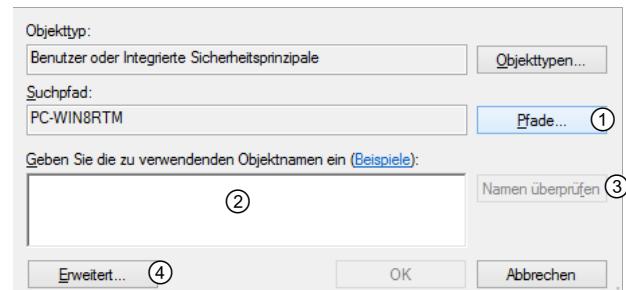
Über *Hinzufügen* gelangen Sie zum Dialogfenster für die Auswahl von Benutzern und Gruppen.

- ▶ Wählen Sie mithilfe der Schaltfläche *Pfade* ① die Domäne oder den Computer aus, zu dem die Benutzer oder Gruppen gehören, die Sie hinzufügen möchten.
- ▶ Geben Sie in den Bereich ② die zu suchenden Objektnamen durch Semikola getrennt ein.

Mit *Namen überprüfen* ③ können Sie die Objektnamen suchen und prüfen lassen.

oder

Alternativ können Sie mit *Erweitert* ④ nach Benutzern und Gruppen suchen.



Benutzer oder Gruppen einer Gruppe hinzufügen

- ▶ Klicken Sie auf *OK*.
- ▶ Wenn alle Änderungen an Mitgliedschaften durchgeführt sind, bestätigen Sie mit *OK*.

### Lokale Gruppen löschen

- ▶ Öffnen Sie das Snap-In *Computerverwaltung* und wechseln Sie zu *Computerverwaltung (Lokal) - System - Lokale Benutzer und Gruppen - Gruppen*.
- ▶ Klicken Sie mit der rechten Maustaste auf die Gruppe, die Sie löschen möchten, und wählen Sie im Kontextmenü den Punkt *Löschen*.  
Sie werden nun darauf hingewiesen, dass das Löschen einer Gruppe auch deren eindeutige Identifizierungsnummer (die SID) entfernt und daher ein erneutes Erstellen einer gleichnamigen Gruppe nicht gleichbedeutend mit dem Wiederherstellen der Gruppe ist.
- ▶ Bestätigen Sie Ihre Aktion mit *Ja*.

## 11.5 Benutzerumgebung verwalten

### Die Benutzerumgebung

Ein Benutzer arbeitet in einer bestimmten Arbeitsumgebung. Entsprechend den Aufgaben, die ein Benutzer durchzuführen hat, sollte für ihn eine geeignete Arbeitsumgebung definiert werden. Die Arbeitsumgebung muss den Anforderungen des Benutzers gerecht werden und betrifft unter anderem folgende Elemente:

- ✓ Desktop und Hintergrundbild;
- ✓ Zugriffsrechte auf Ordner und Dateien;
- ✓ die Möglichkeit, Dateien auf einem oder mehreren Druckgeräten auszudrucken;
- ✓ die den Erfordernissen entsprechende Anpassung des Startbildschirms und der Taskleiste;
- ✓ automatische Verbindungen zu Netzwerklauferwerken und freigegebenen Ordnern;
- ✓ gegebenenfalls den automatischen Start einer Anwendung nach der Anmeldung;
- ✓ einen Ordner, in dem der Benutzer seine persönlichen Dateien ablegen kann (Basisordner).

Für die Definition einer Arbeitsumgebung für den Benutzer stehen Ihnen zwei Werkzeuge zur Verfügung: **Benutzerprofile** und **Anmeldeskripte**. Welches der beiden Werkzeuge Sie nutzen oder ob Sie sogar beide verwenden, hängt beispielsweise von den Gegebenheiten im Netzwerk ab.

### Benutzerprofil

Ein Benutzerprofil ist ein **besonderer Ordner**. Das Profil wird beim Anmelden eines Benutzers automatisch geladen. Jeder Windows-Computer pflegt standardmäßig ein Profil für jeden Benutzer, sobald dieser sich einmal an diesem Computer angemeldet hat. Ausgenommen hiervon sind Benutzer, die sich als Gast anmelden.

Das Benutzerprofil umfasst zahlreiche Konfigurationsdaten des Benutzers. Dies sind unter anderem:

- ✓ Einstellungen von Sperrbildschirm, Startbildschirm und Benutzerbild;
- ✓ Anmeldeinformationen für Windows, Netzwerkfreigaben, E-Mail, Internetkonten;
- ✓ persönliche Dateien und Bibliotheken;
- ✓ installierte Apps und Desktop-Anwendungen;
- ✓ Schriftgröße, Desktopeinstellungen, Verknüpfungen;
- ✓ Eingabegeräte und Spracheinstellungen;
- ✓ Freigaben und Netzlaufwerke;
- ✓ Drucker und Geräte.

Standardmäßig kann ein normaler Benutzer ohne Administratorrechte die meisten oben aufgezählten Einstellungen seines Benutzerprofils selbst vornehmen, andere Einstellungen können nur mit Administratorrechten vorgenommen werden. Zu diesen Einstellungen zählen z. B. Sicherheitseinstellungen, Netzwerkeinstellungen oder Netzwerkdrucker oder die Änderung der Arbeitsgruppe.

### Speicherort der Benutzerprofile ändern

Unter Windows 10 sind alle Benutzerprofile auf der Systempartition im Ordner *C:\Users* untergebracht (im Explorer als *C:\Benutzer* angezeigt), außerdem sind zahlreiche Verweise in der Registry zu finden. Es ist nicht vorgesehen, den Speicherort eines Benutzerprofils zu ändern, und Sie dürfen auf keinen Fall den Profilordner manuell verschieben.

### Profilordner kopieren mit Robocopy und symbolischen Links

Die folgende Methode zum Verschieben des Profilordners funktioniert sowohl bei bestehenden Benutzerprofilen als auch vor einer Neuinstallation.



Bei bestehenden Systemen sollten Sie vor der Durchführung unbedingt ein Systemabbild erstellen.

Die Zielpartition muss entweder mit NTFS oder ReFS formatiert sein, denn das Umlenken auf andere Dateisysteme ist nicht möglich.

Mit einem kleinen Trick können Sie auf recht einfache Weise den Profilordner verschieben. Dies erreichen Sie über einen symbolischen Link, der auf ein Verzeichnis auf einer anderen Partition verweist, ohne dass Windows davon etwas merkt. Wenn Sie nun das Verzeichnis *C:\Users* über den symbolischen Link z. B. nach *D:\Users* umleiten, werden alle Daten ab jetzt dort abgelegt. Bestehende Benutzerdaten können mit dem Tool Robocopy in das neue Verzeichnis kopiert werden.

- ▶ Booten Sie von einer Installations-DVD.
- ▶ Betätigen Sie nach dem Erscheinen der Sprachauswahl , um eine Eingabeaufforderung zu öffnen.
- ▶ Geben Sie `robocopy c:\users d:\users /mir /sec /xj ↵` ein, um den gesamten Inhalt des Profilordners zu verschieben.  
Die Parameter `/mir` und `/sec` sorgen dabei für das Kopieren aller Unterobjekte inklusive der Rechte, und `/xj` bewirkt, dass das System symbolische Verknüpfungen beim Kopieren nicht verfolgt.
- ▶ Löschen Sie nach dem Kopieren den alten Profilordner mit `rd c:\users /s /q ↵`.
- ▶ Erstellen Sie den symbolischen Link mit `mklink c:\users d:\users /j ↵` und starten Sie den Computer neu.

Von nun an befinden sich alle vorhandenen und neu erstellten Benutzerprofile auf *D:\Users*.

## 11.6 Benutzerprofile verwalten

### Speicherort von Benutzerprofilen

Benutzerprofile werden vom System standardmäßig bei der ersten Anmeldung des Benutzers erzeugt. Die Dateien, die im Profilordner unter *Default* gespeichert sind, werden unter dem Benutzernamen auf dem Startvolumen unter *Benutzer* gespeichert. Für alle Benutzer gelten die Einstellungen im Ordner *Öffentlich*. Diese Einstellungen sind durch das System geschützt und Sie sollten hier keine Änderungen vornehmen.

### Standardbenutzerprofil

Auf jedem Windows-10-Computer liegt bereits ein Standardbenutzerprofil namens *Default* auf der lokalen Festplatte vor. Dieses Standardbenutzerprofil wird geladen, wenn sich ein Benutzer erstmals an diesem Computer anmeldet.

Der Inhalt von *Default* ist versteckt und durch das System gesichert. Wenn Sie ihn untersuchen möchten, müssen Sie zuerst im Explorer die Option zum Anzeigen versteckter Ordner aktivieren. Manuelle Änderungen durch den Administrator sind hier von Microsoft nicht vorgesehen.

Lokales Benutzerprofil	Standardmäßig speichert Windows 10 das Profil eines Benutzers auf der lokalen Festplatte der Workstation. Deshalb kann auf jedem Windows-Computer, an dem sich der Benutzer anmeldet, ein anderes Benutzerprofil für diesen Benutzer vorliegen.
Servergespeichertes Benutzerprofil	Um zu gewährleisten, dass der Benutzer unabhängig von der Workstation bei der Anmeldung immer die gleiche Arbeitsumgebung vorfindet (Roaming Profiles), kann das Profil auf einem Netzlaufwerk abgelegt werden.

Servergespeicherte Benutzerprofile sind nur in einer Active Directory-Domäne sinnvoll einsetzbar, denn dort können die entsprechenden Einstellungen zentral vorgenommen werden. Vom Verlegen der Benutzerprofile auf die Netzwerkfreigabe auf einem normalen Computer ist dringend abzuraten.



### Standardumgebungen erzeugen

In Windows 10 funktionieren viele der aus älteren Windows-Versionen bekannten Methoden zur Erstellung eines Standard-Desktops und Startmenüs für alle Benutzer nicht mehr, da der Zugriff auf die entsprechenden Verzeichnisse gesperrt ist. Durch das Wegfallen des herkömmlichen Startmenüs ist es auch nicht mehr vorgesehen, durch manuelles Hinzufügen von Verknüpfungen den Startbildschirm einzurichten.

Aus diesem Grund wird hier darauf verzichtet, mit Tricks dennoch eine Anpassung von Client-Computern in der Arbeitsgruppe zu erzwingen.

Microsoft wird für die Enterprise-Edition Werkzeuge bereitstellen, die im Zusammenspiel mit Active Directory erweiterte Möglichkeiten bieten, um den Benutzerdesktop und die Windows-Oberfläche vorzukonfigurieren. Dabei soll auch die Verwendung und Verteilung von Apps ermöglicht werden, die nicht aus dem Windows Store stammen.

### Synchronisierung über Microsoft-Konto einrichten

Microsoft hat mit Windows 10 Möglichkeiten für ein **portables Benutzerprofil** geschaffen. Sie können es so einrichten, dass auf jedem Computer, auf dem Sie sich mit Ihrem Microsoft-Konto anmelden, automatisch Ihr persönlicher Startbildschirm mit Ihren Windows-Apps erscheint. Die Einstellungen dafür finden Sie in den Einstellungen.

- ▶ Melden Sie sich mit einem Microsoft-Konto an.
- ▶ Rufen Sie über das Startmenü *Einstellungen - Konten - Einstellungen synchronisieren* auf.
- ▶ Schalten Sie *Synchronisierungseinstellungen* ein.
- ▶ Wählen Sie aus, welche Einstellungen synchronisiert werden sollen.

Standardmäßig werden alle verfügbaren Einstellungen synchronisiert. Auch bei Verwendung von getakteten Verbindungen (UMTS, GPS oder Analog-Modem) wird der Abgleich regelmäßig vorgenommen, lediglich beim Einsatz von Roaming unterbleibt die automatische Synchronisierung aus Kostengründen.

Kurz nach dem Einschalten der Synchronisierung erhalten Sie von Microsoft eine E-Mail oder SMS, auf die Sie reagieren müssen, um die Synchronisierung freizuschalten. Dabei müssen Sie entweder auf einen Link klicken oder auf einer Microsoft-Internetseite einen Code eingeben. Die Einstellungen sind abhängig davon, was Sie in der Weboberfläche Ihres Microsoft-Kontos angegeben haben.

### Vertraute PCs vom Microsoft-Konto entfernen

Alle Computer, an denen Sie sich mit Ihrem Microsoft-Konto angemeldet haben, werden in den Einstellungen des Kontos angezeigt. Sie können nicht mehr benötigte Geräte in der Weboberfläche Ihres Microsoft-Kontos entfernen. Dazu rufen Sie die Webseite <https://account.microsoft.com/devices> auf und melden sich mit Ihrem Konto an. Geräte, die Sie nicht mehr nutzen, können Sie über den Link *Handy entfernen* oder *PC entfernen* von Ihrem Microsoft-Konto trennen. Eine Liste aller Geräte sehen Sie als Zusammenfassung auch auf der Seite <https://account.microsoft.com>.

## 11.7 Windows Hello – Anmeldung an Windows 10 mit Gesichtserkennung oder Biometrie

Mit Windows 10 will sich Microsoft langsam von der Anmeldung mit Benutzernamen und Kennwort verabschieden. Anwender sollen biometrische Möglichkeiten mit PINs kombinieren und dabei wesentlich sicherer unterwegs sein als bisher. Dazu kommt die Möglichkeit, die Authentifizierung an Windows auch für Webseiten und Cloud-Dienste zu nutzen.

In Windows 10 hat Microsoft die Möglichkeit integriert, dass sich Anwender nicht nur mit Fingerabdruck anmelden können, sondern auch über eine Gesichtserkennung. Die Technologie mit der Bezeichnung „Windows Hello“ ist in allen Editionen von Windows 10 enthalten.

Windows Hello kombiniert die Anmeldung per PIN, Fingerabdruck, Gesichtserkennung und Iriserkennung. Das System soll sehr sicher sein, Daten werden nur lokal gespeichert und die Sicherheitsfunktionen lassen sich miteinander kombinieren.

Um die Gesichtserkennung mit Windows Hello zu nutzen, müssen Sie eine Webcam einsetzen, die 3D-Bilder erkennen kann, infrarotfähig und für Windows Hello auch zertifiziert ist. Derzeit gibt es in diesem Bereich nur Intel RealSense 3D (<https://software.intel.com/de-de/realsense/f200camera?language=en>). Intel stellt diese Kamera derzeit für Entwickler auch als alleinstehendes Gerät zur Verfügung. Damit lassen sich Tests für eigene Apps durchführen, um Windows Hello zu testen.

- ▶ Um Windows Hello einzurichten, melden Sie sich an Windows 10 an und wechseln zu *Konten - Anmeldeoptionen*.  
Hier sehen Sie, welche Geräte an Ihrem PC kompatibel mit Windows Hello sind. Erscheint der Menüpunkt nicht, ist am PC kein entsprechendes Gerät angeschlossen.

Im ersten Schritt müssen Sie in diesem Bereich eine PIN definieren, mit der Sie sich authentifizieren müssen, bevor Sie Einstellungen in Windows Hello oder an anderer Stelle ändern. Diese Vorgehensweise dient als zusätzliche Sicherheitsstufe.

- ▶ Die PIN legen Sie ebenfalls im Bereich *Konto - Anmeldeoptionen* fest.
- ▶ Sobald Sie die PIN festgelegt haben, rufen Sie über *Einrichten* den Assistenten zur Konfiguration von Windows Hello auf.

Hier sehen Sie auch, welche Optionen Windows Hello auf Ihrem PC unterstützt.

Im Falle eines Fingerabdruckscanners startet anschließend der Assistent zur Einrichtung des Fingerabdrucks. Damit der Fingerabdruck ordnungsgemäß gespeichert wird, müssen Sie mehrere Male über den Sensor fahren.

## 11.8 Übung

### Benutzerkonten und Windows Hello

Übungsdatei: --

Ergebnisdatei: *Uebung11\_E.pdf*

1. Wie legen Sie in Windows 10 Benutzerkonten an?
2. Wo richten Sie die neue Anmeldefunktion „Windows Hello“ ein?

# 12 Gruppenrichtlinien

## In diesem Kapitel erfahren Sie

- ✓ was Gruppenrichtlinien sind
- ✓ wie Gruppenrichtlinien eingesetzt werden können, um Ihr System abzusichern
- ✓ wie Sie Sicherheitsrichtlinien zur Absicherung des Systems einsetzen können

## Voraussetzungen

- ✓ Verständnis des Sicherheitskonzeptes unter Windows 10
- ✓ Kenntnisse im Umgang mit der MMC und der Benutzerverwaltung

## 12.1 Grundlagen zu Gruppenrichtlinien

### Einsatzmöglichkeiten von Gruppenrichtlinien

Mit Gruppenrichtlinien (Group Policies) können Benutzerrechte und verschiedene Bereiche des Betriebssystems angepasst, eingeschränkt oder erweitert werden. Sie erlauben eine skalierte Anpassung des Betriebssystems. So kann z. B. einer bestimmten Benutzergruppe über eine entsprechende Richtlinie das Recht auf Herunterfahren des Systems genommen werden, um ein versehentliches Abschalten des Druckservers zu verhindern.

Der Einsatz von Richtlinien ermöglicht zahlreiche Einstellungen, die sich mit der Systemsteuerung nicht erreichen lassen, und vermeidet so direkte Eingriffe in die Registry, die die Systemintegrität gefährden könnten.

Windows 10 kann umfassend mit Gruppenrichtlinien gesteuert werden. Um alle Gruppenrichtlinien-Funktionen nutzen zu können, ist häufig Windows 10 Enterprise notwendig. Für Windows 10 Enterprise bietet Microsoft zudem eine spezielle Lizenzierungsvariante, die sich Long Time Service Branch (LTSB) nennt. Bei dieser Version müssen keine neuen Funktionen und Erweiterungen installiert werden, um für zehn Jahre Support zu erhalten. Sicherheits- und Stabilitätspatches müssen allerdings auch in dieser Version eingespielt werden, jedoch keine Feature-Updates oder neuen Builds. Damit verspricht Microsoft, dass Unternehmen mit LTSB nicht dazu gezwungen werden, stets die aktuellste Windows-Version zu nutzen. Zusammen mit der Steuerung der Einstellungen über Gruppenrichtlinien ist Windows 10 Enterprise LTSB also durchaus prädestiniert für den Unternehmenseinsatz.

Zwar bietet Windows 10 Pro ebenfalls die Absicherung über Gruppenrichtlinien, allerdings fehlen hier einige Einstellungen. So lässt sich in Windows 10 Pro zum Beispiel der Microsoft Store nicht über Gruppenrichtlinien deaktivieren. Es gibt aber zahlreiche weitere Möglichkeiten, mit denen sich Einstellungen über Gruppenrichtlinien delegieren lassen.

Sie können auch Benutzerrechte für verschiedene Einstellungen und Ordner über Gruppenrichtlinien delegieren. Das ist dann sinnvoll, wenn Benutzer für bestimmte Verzeichnisse auf einem Computer Zugriff erhalten sollen. Die entsprechenden Einstellungen sind in der Gruppenrichtlinienverwaltung über *Computerkonfiguration - Richtlinien - Windows-Einstellungen - Sicherheitseinstellungen* zu finden. Hier stehen auch über *Lokale Richtlinien* zahlreiche Einstellungen zur Verfügung, die dabei helfen, Benutzerrechte in Windows zu steuern.

### Definition

Richtlinien dienen dazu, die Rechte von Benutzern und Einstellungen des Systems zu regulieren. Der Gültigkeitsbereich kann auf einen Computer oder Benutzer, bestimmte Gruppen oder auch komplette Domänen festgelegt werden.

Richtlinien können verschiedene Zustände haben: *Aktiviert*, *Deaktiviert* oder *Nicht konfiguriert*.

Erst wenn eine Richtlinie auf *Aktiviert* gestellt wurde, lassen sich weitere Einstellungen vornehmen. Je nach Typ und Einsatzgebiet einer Richtlinie sind unterschiedlich viele Benutzereingaben und Einstellungen möglich.

Wert	Auswirkung
<i>Aktiviert</i>	Die Richtlinie wird angewendet und die Werte werden in die Registry übernommen.
<i>Deaktiviert</i>	Die zugehörigen Registry-Schlüssel werden auf ihre Standardwerte zurückgesetzt.
<i>Nicht konfiguriert</i>	Bestehende Werte werden beibehalten, keine Änderungen an der Registry

## Geltungsbereich

Gruppenrichtlinien werden als Richtlinien für ein bestimmtes Objekt definiert. Dieses Objekt kann ein bestimmter Computer, eine Domäne oder Organisationseinheit oder ein Standort im Sinne des Active Directory sein.

Sie können hier auch selbst ein Objekt definieren und anpassen, für welche Objekte eine Richtlinie gültig sein soll. So lassen sich die Rechte und Beschränkungen individuell an die Bedürfnisse von Benutzern anpassen. Von großer Bedeutung sind Richtlinien im Netzwerk, wo sie für alle Beteiligten gültig sind. Die Richtliniendateien werden zentral auf einem Server gespeichert. So hat ein Netzwerkadministrator die Möglichkeit, Konfigurationen für Computer und Restriktionen für Benutzer zu vereinheitlichen und zentral zu verwalten.

## Sicherheitsvorlagen

Unter Windows 10 gibt es die Möglichkeit, mit voreingestellten Sicherheitsrichtlinien eine automatisierte Richtlinienverwaltung durchzuführen, um so typische Szenarien zu erfassen. Es ist aber wichtig, sich zuerst mit dem Konzept der Richtlinien und ihren Anwendungsmöglichkeiten vertraut zu machen, bevor durch das Aktivieren von Sicherheitsvorlagen tief greifende Eingriffe in das System erfolgen. Nur so kann erreicht werden, dass Sie anschließend Konfigurationsfehler des Systems richtig diagnostizieren und entsprechend beheben können. Lesen Sie daher zuerst die Abschnitte, die sich mit den einzelnen Richtlinien befassen, bevor Sie sich mit den Sicherheitsrichtlinien beschäftigen.

Um jeweils die neusten Sicherheitseinstellungen von Windows 10 über Gruppenrichtlinien zu verteilen, ist nicht unbedingt Windows Server 2016 notwendig. Die Vorlagen, die Microsoft kostenlos zur Verfügung stellt, können auch in Windows Server 2012/2012 R2 eingebunden werden. Auch auf Servern mit Windows Server 2016 müssen die Vorlagen integriert werden. Denn Windows Server 2016 verfügt standardmäßig nur über die Richtlinieneinstellungen von Windows 10 **vor** den aktuellen Windows-10-Versionen. Die Vorlagen für die Gruppenrichtlinieneinstellungen, inklusive Windows 10 April 2018 Update (Version 1803) können hier heruntergeladen werden: <https://www.microsoft.com/de-de/download/details.aspx?id=56880>

Nach dem Download müssen die ADMX-Dateien mit den Einstellungen sowie die dazugehörigen Sprachdateien (ADML) auf die Domänencontroller kopiert werden. Das Standardverzeichnis dafür ist *C:\PolicyDefinitions*. Im Richtlinien-Editor sind anschließend die neuen Einstellungen verfügbar. Die ADML-Dateien müssen in die entsprechenden Unterordner für die Sprache kopiert werden. Es bietet sich an, neben den ADMX-Dateien und den deutschen ADML-Dateien auch die englischen ADML-Dateien zu kopieren.

## Speichern von Richtlinien

Richtlinien werden als *ntuser.pol* im Verzeichnis *Benutzer\All Users* oder als *Registry.pol* im Verzeichnis *%Systemroot%\system32\GroupPolicy\Machine* gespeichert. Wenn Sie mehrere gleichartige Rechner mit der selben Konfiguration betreiben möchten, können Sie entsprechend die Richtlinie, die Sie auf einem Rechner erstellt haben, an den identischen Speicherort der anderen Rechner kopieren. Beim nächsten Start werden dann die Registry-Einträge durch die in der Richtlinie definierten Werte überschrieben.

## Lokale Richtlinien

Die Gruppenrichtlinien für einen lokalen Computer haben auch nur auf diesem Gültigkeit. Daher werden sie nur dann eingesetzt, wenn es gilt, einen einzelnen Rechner gegen Fehler der Benutzer abzusichern. So lässt sich beispielsweise ein Computer, der an öffentlich zugänglicher Stelle steht und über den Funktionen wie Informationssysteme bereitgestellt werden sollen, gegen unbeabsichtigtes Herunterfahren oder den Zugriff auf die Konsole absichern.

## Domänenweite Richtlinien und das Active Directory

Wenn auf einem Domänencontroller domänenweite Richtlinien erstellt werden, dann überschreiben diese jegliche lokale Einstellung, die auf einem Rechner erstellt wurde, der zur Domäne gehört.



In einer Domäne ist es wenig sinnvoll, lokale Richtlinien zu erstellen, die nur für einen Rechner gelten sollen. Durch die Möglichkeit, Organisationseinheiten (OUs) zu bilden und darin beliebige Gruppen, Benutzer oder Computer zusammenzufassen, lässt sich eine zentralisierte Verwaltung aufbauen, die sich jederzeit an geänderte Gegebenheiten anpassen lässt. Über domänenweite Richtlinien werden die Vorgaben an die Client-Computer ausgeliefert.

## Richtlinien einsetzen

Setzen Sie Richtlinien immer dann ein, wenn es um die Sicherheit des Systems geht. Bedenken Sie dabei das generelle Sicherheitskonzept von Windows: Die Objektsicherheit wird durch Freigabe- und NTFS-Berechtigungen gesteuert, die Systemsicherheit durch Sicherheitsrichtlinien.



Durch das Anpassen von Sicherheitsrichtlinien können Sie gewährleisten, dass Anmeldevorgänge, Eingriffe in das System und weitere Aktionen, die eine potenzielle Gefahr für Ihr System darstellen könnten, unmöglich werden. Eingriffe in das System sind jedoch stets mit der Gefahr verbunden, dass danach wichtige Mechanismen nicht mehr funktionieren. Planen Sie daher genau, welche Veränderungen an den Sicherheitsrichtlinien wirklich nötig sind, und führen Sie vor der Anwendung Funktionstests an einem Versuchssystem durch.

## 12.2 Richtlinien mit der MMC verwalten

### Das Richtlinienverwaltungs-Snap-In verwenden

Bei Windows 10 gibt es Tausende von Einstellungsmöglichkeiten, die mit Gruppenrichtlinien vorgenommen werden können. Dazu wird in der MMC das Snap-In *Gruppenrichtlinienobjekt-Editor* hinzugefügt.

- ▶ Rufen Sie die MMC auf und klicken Sie im Menü *Datei* auf *Snap-In hinzufügen/entfernen*.
- ▶ Klicken Sie auf die Schaltfläche *Hinzufügen* und wählen Sie das Snap-In *Gruppenrichtlinienobjekt-Editor* aus. Bestätigen Sie anschließend, dass Sie Gruppenrichtlinien für den lokalen Computer einrichten möchten, indem Sie auf *Hinzufügen* klicken.

Sie können im Verzeichnis der Domäne ein anderes Objekt (eine Gruppe oder einen Computer) auswählen, wenn Sie Mitglied einer Domäne mit Active Directory sind.

- ▶ Schließen Sie das Dialogfenster mit *OK*.
- ▶ Öffnen Sie die Konsolenstruktur, um einen Überblick über die einzelnen Richtliniengruppen zu erlangen. Die dazugehörigen Richtlinien können Sie im rechten Konsolenfenster sehen.

Die Konsole *Richtlinien für Lokaler Computer* ist in die Hauptbereiche *Computerkonfiguration* ① und *Benutzerkonfiguration* ② unterteilt. Diese beinhalten jeweils auf der zweiten Gliederungsebene die drei Bereiche *Softwareeinstellungen*, *Windows-Einstellungen* und *Administrative Vorlagen*.

The screenshot shows the 'Konsolenstamm' (Console Root) on the left and a table of policy objects on the right.

**Konsolenstamm:**

- Richtlinien für Lokaler Computer
  - Computerkonfiguration
    - Softwareeinstellungen
    - Windows-Einstellungen
      - Namensauflösungsrichtlinie
      - Skripts (Start/Herunterfahren)
      - Bereitgestellte Drucker
      - Sicherheitseinstellungen
      - Richtlinienbasierter QoS
    - Administrative Vorlagen
      - Drucker
      - Netzwerk
      - System
      - Systemsteuerung
      - Windows-Komponenten
      - Alle Einstellungen
  - Benutzerkonfiguration
    - Softwareeinstellungen
    - Windows-Einstellungen
    - Administrative Vorlagen

**Table (Name and Description):**

Name	Beschreibung
Kontorichtlinien	Kennwort- und Kontosperrungsrichtlinien
Lokale Richtlinien	Richtlinien für die Überwachung, Benutzerrechte...
Windows-Firewall mit erweiterter Sicherheit	Windows-Firewall mit erweiterter Sicherheit
Netzwerklisten-Manager-Richtlinien	Gruppenrichtlinien für Netzwerkname, Netzwer...
Richtlinien für öffentliche Schlüssel	
Richtlinien für Softwareeinschränkung	
Anwendungssteuerungsrichtlinien	Anwendungssteuerungsrichtlinien
IP-Sicherheitsrichtlinien auf Lokaler Com...	Internet Protocol Security (IPsec)-Verwaltung: ...
Erweiterte Überwachungsrichtlinienkonfi...	Erweiterte Überwachungsrichtlinienkonfigurati...

### Sicherheitseinstellungen für den lokalen Computer

Die **Computerkonfiguration** enthält grundsätzliche Einstellungen für einen Computer, die unabhängig vom angemeldeten Benutzer gelten, während in der **Benutzerkonfiguration** Einstellungen für einzelne Benutzer oder Benutzergruppen vorgenommen werden. Die Einstellungen aus der Benutzerkonfiguration gelten unabhängig vom Computer, auf dem sich die Benutzer anmelden.

Die einzelnen Elemente dieser Baumstruktur werden auch als **Knoten** bzw. **Unterknoten** bezeichnet.

Im Folgenden werden die wichtigsten Knoten und Unterknoten und ihre Einsatzgebiete kurz erläutert. Um dennoch ein klares Verständnis der Richtlinien zu erhalten, sollten Sie während des Lesens die Struktur der Gruppenrichtlinien am Computer mitverfolgen.

Im darauf folgenden Teil sollen Ihnen Anwendungsbeispiele den praktischen Umgang mit den Richtlinien vermitteln. Diese Beispiele sollten Sie ebenfalls am Computer nachvollziehen.

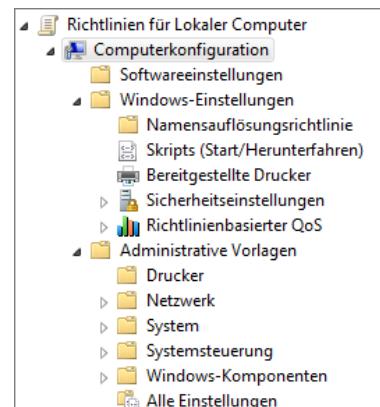
## 12.3 Computerkonfiguration

### Computerspezifische Konfigurationen

Alle Richtliniengruppen unterhalb des Knotens *Computerkonfiguration* sind computerspezifisch. Das heißt, dass sie unabhängig vom gerade angemeldeten Benutzer für diesen Computer gelten. Sie werden angewendet, sobald der Computer gestartet wird.

Die Computerkonfiguration enthält drei Unterknoten: *Softwareeinstellungen*, *Windows-Einstellungen* und *Administrative Vorlagen*.

Der Knoten *Softwareeinstellungen* ist bei lokalen Richtlinien sowohl in der Computer- als auch in der Benutzerkonfiguration stets leer.



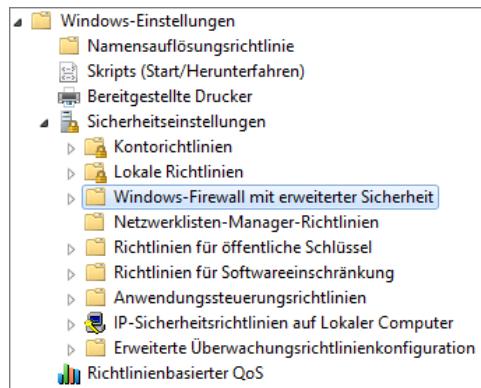
Computerkonfiguration

## Windows-Einstellungen

Unter *Windows-Einstellungen* befinden sich die Richtlinien, die beim Systemstart Verwendung finden. Die Sicherheitseinstellungen sind besonders wichtig, da sie jene Teile der Richtlinien beinhalten, die für die Benutzerverwaltung und die Absicherung des Systems relevant sind.

### Sicherheitseinstellungen

Im Unterknoten *Sicherheitseinstellungen* befinden sich die Richtlinien, mit denen Sie als Systembetreuer am häufigsten zu tun haben werden:



Windows-Einstellungen

<i>Kontorichtlinien</i>	Hier werden in zwei Unterknoten die Kennwortrichtlinien und die Kontosperrungsrichtlinien behandelt.
<i>Lokale Richtlinien</i>	Die Unterknoten behandeln die Überwachungsrichtlinien, das Zuweisen von Berechtigungen und die Sicheritsoptionen.
<i>Windows-Firewall mit erweiterter Sicherheit</i>	Hier können Sie Regeln für die Windows-Firewall erstellen und umfangreiche Regelsätze erstellen, die unter anderem auch die Verwendung von IPSec mit einbeziehen.
<i>Netzwerklisten-Manager-Richtlinien</i>	Hier können Sie einstellen, ob am Computer Netzwerktyp und Netzwerkname geändert werden dürfen.
<i>Richtlinien für öffentliche Schlüssel</i>	Hier finden Sie den Agenten für die Wiederherstellung öffentlicher Schlüssel. Darin ist die Verwaltung öffentlicher und privater Schlüssel untergebracht.
<i>Richtlinien für Softwareeinschränkungen</i>	Anhand von Regeln können Sie festlegen, welche Software ausgeführt werden darf und welche nicht.
<i>Anwendungssteuerungsrichtlinien</i>	AppLocker-Regeln bestimmen, welche Anwendungen gestartet werden dürfen.
<i>IP-Sicherheitsrichtlinien</i>	Hier befindet sich die Verwaltung der Sicherheitsmechanismen für die Kommunikation zwischen Clients und Servern.
<i>Erweiterte Überwachungsrichtlinienkonfiguration</i>	Hier finden Sie alle Richtlinien für die Systemüberwachung, z. B. für die Protokollierung von Anmeldungen und Objektzugriffen.

## Administrative Vorlagen

Unter *Administrative Vorlagen* werden alle Richtlinieneinstellungen aus der Registry für den Bereich *HKEY\_LOCAL\_MACHINE* angezeigt. Hier können über 11000 Richtlinien eingestellt werden.

Standardmäßig finden sich hier die folgenden Unterknoten:

<i>Drucker</i>	Die Richtlinien zur Druckereinstellung und zu den dazugehörigen Rechten werden an dieser Stelle vorgenommen.
<i>Netzwerk</i>	Unter diesem Unterknoten finden Sie die Richtlinien zu Offline-Dateien und zu Netzwerkverbindungen etc.
<i>System</i>	Hier befinden sich Richtlinien zur Gestaltung des Systems und in diversen Unterknoten Richtlinien zu den Einstellungen zu Systembestandteilen wie DNS-Client, Datenträgerkontingente etc.

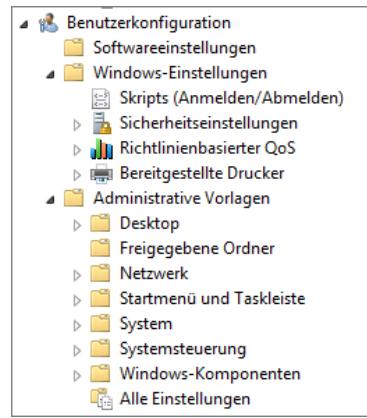
<b>Systemsteuerung</b>	Hier finden Sie Richtlinien zum Steuern der Benutzerkonten oder Regions- und Sprachoptionen des Betriebssystems.
<b>Windows-Komponenten</b>	In den Unterknoten befinden sich die Richtlinien für Programme wie den Internet Explorer.
<b>Alle Einstellungen</b>	Dieser Unterknoten enthält eine Liste aller Richtlinien aus den administrativen Vorlagen.

## 12.4 Benutzerkonfiguration

### Unterschiede zum Knoten *Computerkonfiguration*

Die unter *Benutzerkonfiguration* festgelegten Richtlinien sind für Benutzerkonten gültig, unabhängig vom Computer, auf dem die Benutzer eingeloggt sind. Die untergeordneten Knoten sind ähnlich strukturiert wie bei der Computerkonfiguration, orientieren sich aber stärker an benutzerrelevanten Faktoren wie der Bedienung und dem Funktionsumfang von Windows-Anwendungen. Da die Benutzerrichtlinien erst bei Anmeldung eines Benutzers abgearbeitet werden, überschreiben sie vorhandene Werte aus der Computerkonfiguration. Auf diese Weise kann etwas grundsätzlich auf einem Computer verboten sein, für Administratoren jedoch wieder erlaubt werden.

Der Knoten *Softwareeeinstellungen* ist bei lokalen Richtlinien stets leer.



Benutzerkonfiguration

### Windows-Einstellungen

Unter *Windows-Einstellungen* befinden sich Richtlinien, die beim Anmelden des Benutzers an dem Computer Verwendung finden. Diese befinden sich in den Unterknoten *Skripts (Anmelden/Abmelden)* und *Sicherheits-einstellungen*.

### Administrative Vorlagen

Unter *Administrative Vorlagen* sind alle Richtlinien aus dem Registry-Bereich *HKEY\_CURRENT\_USER* zu finden. Hier können über 1500 Richtlinien eingestellt werden. Standardmäßig finden sich hier die folgenden Unterknoten:

<b>Desktop</b>	Hier finden Sie Richtlinien zur Anpassung des Desktops.
<b>Freigegebene Ordner</b>	Hier kann eingestellt werden, ob Freigaben im Active Directory veröffentlicht werden dürfen.
<b>Netzwerk</b>	Hier befinden sich Richtlinien zu Netzwerkverbindungen, Offlinedateien und zur Konfiguration von Funknetzwerken mit WCN (Windows Connect Now).
<b>Startmenü und Taskleiste</b>	Hier finden Sie Richtlinien zur Anpassung des Startmenüs, der Taskleiste und des Startmenüs bzw. der Windows-Oberfläche.
<b>System</b>	In dieser Kategorie finden Sie Richtlinien zu diversen Systemprogrammen, zur Treiberinstallation, zu Wechselmedien und Registry.
<b>Systemsteuerung</b>	Hier wird geregelt, welche Systemeinstellungen verfügbar sind.
<b>Windows-Komponenten</b>	Dies ist mit Abstand die umfangreichste Gruppe, in der u. a. Richtlinien zum Internet Explorer, Microsoft Store und MMC zu finden sind.
<b>Alle Einstellungen</b>	Dieser Unterknoten enthält eine Liste aller Richtlinien aus den administrativen Vorlagen.

## 12.5 Anwendungsbeispiele

### Gruppenrichtlinien einrichten

Nachfolgend soll anhand einiger typischer Anwendungen der Umgang mit den Gruppen- und Sicherheitsrichtlinien erläutert werden. Dabei werden auch Richtlinien einbezogen, die nur im Zusammenhang mit Windows-Domänen von Bedeutung sind.

Richten Sie als Erstes die Richtlinien für den lokalen Computer ein. Sie können diese Übung später auch für andere Computer oder Objekte aus dem Active Directory vollziehen, wenn Sie über ausreichende Berechtigungen verfügen.

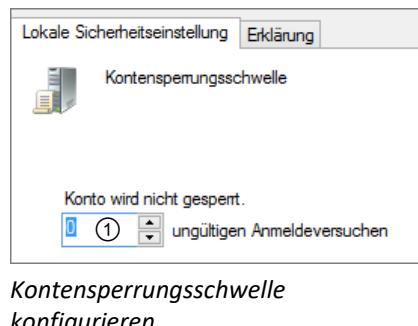
- ▶ Fügen Sie in der MMC das Snap-In *Gruppenrichtlinienobjekt-Editor* mit dem Gruppenrichtlinienobjekt *Lokaler Computer* hinzu.

Sie sehen nun in der Struktur der MMC das Snap-In *Richtlinien für Lokaler Computer*.

### Kontosperrung einrichten

Standardmäßig ist Windows so eingestellt, dass beliebig oft ein falsches Passwort eingegeben werden kann, ohne dass das Benutzerkonto gesperrt wird. Dies sollte aus Sicherheitsgründen sofort geändert werden.

- ▶ Wählen Sie im Snap-In *Richtlinien für Lokaler Computer* den Unterknoten *Computerkonfiguration - Windows-Einstellungen - Sicherheitseinstellungen - Kontorichtlinien - Kontosperrungsrichtlinien*.
- ▶ Klicken Sie anschließend doppelt auf die Richtlinie *Kontosperrungsschwelle* und setzen Sie die Zahl der ungültigen Anmeldeversuche ① auf 6. Bestätigen Sie mit *OK*.  
Sie werden informiert, dass die Werte für Kontosperrdauer und Zurücksetzungsdauer des Kontosperrungszählers auf die empfohlenen Werte gesetzt werden.
- ▶ Bestätigen Sie diese Änderung ebenfalls.  
Alle beteiligten Richtlinien weisen jetzt Werte auf und die Kontosperrungsrichtlinie ist aktiviert.



### System überwachen

Sie haben die Möglichkeit, mit Überwachungsrichtlinien Protokolle verschiedener Ereignisse einzurichten. Die einzelnen Ereignisse werden darin als erfolgreich oder fehlgeschlagen protokolliert und können so einen wertvollen Beitrag zur Systemsicherheit, -verwaltung und -kontrolle darstellen. Entnehmen Sie hierzu der folgenden Tabelle die verschiedenen Ereignisse, die Sie an dieser Stelle überwachen können.



Die Datenschutzbestimmungen können für bestimmte Überwachungen eine Absprache mit dem Betriebs- oder Personalrat erforderlich machen. Bedenken Sie auch, dass eine Überwachung Ressourcen benötigt und das System ausbremsen kann.

Richtlinie	Funktion
<i>Verzeichnisdienstzugriff überwachen</i>	Mit dieser Richtlinie werden Zugriffe auf das Active Directory protokolliert. Dadurch lässt sich eine Effizienzanalyse der Verzeichnisstruktur durchführen. Wegen des hohen Datenaufkommens ist diese Überwachung für den Normalbetrieb nicht empfehlenswert.
<i>Anmeldeereignisse überwachen</i>	Hiermit wird das lokale Anmeldeereignis an einem Rechner protokolliert. Dabei spielt es keine Rolle, wo die Anmeldung verifiziert wird.

Richtlinie	Funktion
Anmeldeversuche überwachen	Diese Richtlinie aktiviert die Überwachung aller Anmeldeversuche auf dem für die Anmeldung zuständigen Rechner (dem Domänencontroller).
Kontenverwaltung überwachen	Hiermit wird die Zugriffsüberwachung auf die Kontenverwaltung aktiviert. Dabei werden Vorgänge wie das Erzeugen, Bearbeiten und Löschen von Benutzer- oder Gruppenkonten protokolliert.
Objektzugriffsversuche überwachen	Die Objektzugriffsüberwachung entspricht der Überwachung von Active Directory-Zugriffen, bezieht sich aber auf Objekte außerhalb vom Active Directory. Solange die Objektüberwachung nicht etabliert wurde, werden auch dann keine Überwachungseinträge im Sicherheitsprotokoll vorgenommen, wenn die Richtlinien zur Überwachung an einem Objekt aktiviert werden (Eigenschaften von Objekt, Register <i>Sicherheit</i> , Schaltfläche <i>Erweitert</i> , Register <i>Überwachung</i> ).
Prozessverfolgung überwachen	Mit dieser Richtlinie wird ein Protokoll der Prozessverläufe anfertigt.
Rechteverwendung überwachen	Hier wird überwacht, ob und wie ein Benutzer von seinen Rechten Gebrauch macht.
Richtlinienänderungen überwachen	Hiermit werden Zugriffe auf die Richtlinien protokolliert. Diese Einstellung kann helfen, erfolgreiche Angriffe auf das System aufzudecken.
Systemereignisse überwachen	Durch Aktivieren dieser Richtlinie wird die Systemprotokollierung eingeschaltet. Hier werden Ereignisse wie das Herunterfahren oder Fehler beim Starten von Diensten eingetragen.

Die genannten Richtlinien können Sie im Snap-In *Richtlinien für Lokaler Computer* im Knoten *Computerkonfiguration - Windows-Einstellungen - Sicherheitseinstellungen - Lokale Richtlinien - Überwachungsrichtlinien* konfigurieren.

Die Ergebnisse Ihrer Überwachungen werden im Sicherheitsprotokoll festgehalten. Dieses wird standardmäßig unter %Systemroot%\System32\config\SecEvent.Evt gespeichert. Sie können das Protokoll in der Ereignisanzeige anschauen, indem Sie im Startmenü *ereignis*  eingeben oder in der MMC das Snap-In *Ereignisanzeige* hinzufügen.

Sie müssen die Richtlinie *Objektzugriffsversuche überwachen* für *erfolgreich* und *fehlgeschlagen* aktivieren, sonst bleibt jede Objektüberwachung, die Sie am Objekt einstellen, wirkungslos.



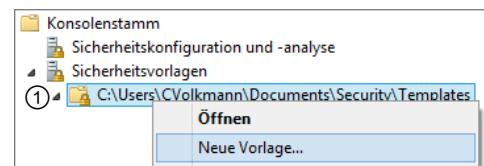
## 12.6 Sicherheitsvorlagen verwenden

### Überblick über Sicherheitsvorlagen

- ✓ Mit dem MMC-Snap-In *Sicherheitsvorlagen* und dem Snap-In *Sicherheitskonfiguration und -Analyse* haben Sie Werkzeuge, die es Ihnen erlauben, eine individuelle Sicherheitspolitik für Ihr System zu etablieren oder sich an bestehenden Sicherheitsstandards für bestimmte Situationen zu orientieren.
- ✓ Sie können das Snap-In *Sicherheitsvorlagen* nutzen, um eigene neue Vorlagen zu definieren, die Sie dann auf mehreren Rechnern verteilen, oder um einfach nur die dortigen Sicherheitseinstellungen mit Ihrer Vorlage vergleichen zu können.

## Sicherheitsvorlage erstellen

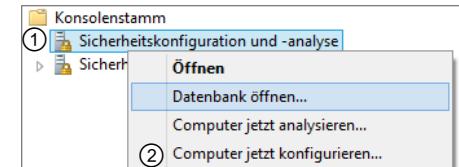
- ▶ Rufen Sie das Snap-In *Sicherheitskonfiguration und -analyse* in der MMC auf.
- ▶ Erweitern Sie den Knoten *Sicherheitsvorlagen*, klicken Sie mit der rechten Maustaste auf den angezeigten Vorlagenpfad ① und wählen Sie *Neue Vorlage...*.
- ▶ Geben Sie Namen und Speicherort für die neue Vorlage an. Anschließend können Sie die Vorlage konfigurieren, indem Sie doppelt darauf klicken.



*Neue Sicherheitsvorlage erstellen*

## Konfigurationsdatenbank erstellen

- ▶ Klicken Sie mit der rechten Maustaste auf *Sicherheitskonfiguration und -analyse* und wählen Sie im Kontextmenü den Punkt *Datenbank öffnen*.
- ▶ Geben Sie nun einen neuen Namen für die zu erstellende Datenbank ein und klicken Sie anschließend auf *Öffnen*. Damit wird eine Konfigurationsdatenbank für Ihr System hergestellt.
- ▶ Aktivieren Sie die Sicherheitsstufe, indem Sie im Kontextmenü des Snap-Ins *Sicherheitskonfiguration und -analyse* ① den Punkt *Computer jetzt konfigurieren* ② wählen. Bestätigen Sie anschließend den Pfad zur Protokolldatei. Die Konfiguration wird nun durchgeführt. Anschließend können Sie den Computer analysieren lassen ③ und im selben Kontextmenü können Sie sich auch die Protokolldatei anzeigen lassen ④.



*Sicherheitsdatenbank öffnen*



Sie sollten sich mit den Sicherheitsvorlagen wie auch mit allen anderen Richtlinien zunächst in einer Testumgebung vertraut machen, um unerwünschte Effekte zu vermeiden.

## 12.7 Gruppenrichtlinien-Einstellungen – Erweiterte Möglichkeiten

Viele Systemeinstellungen und Konfigurationen für Anwendungen erfordern Änderungen an der Windows-Registrierung. Wollen Sie solche Änderungen an mehreren Rechnern im Netzwerk durchführen, bietet sich die Verwendung von Gruppenrichtlinien an.

### Group Policy Preferences einsetzen

Mit den *Group Policy Preferences* in einer Gruppenrichtlinie lassen sich auf Windows-Rechnern Einstellungsvorschläge für Systemeinstellungen über Gruppenrichtlinien erstellen. Diese Vorgaben müssen Anwender nicht zwingend übernehmen. Sie geben bestimmte Einstellungen vor, die Rechner übernehmen, z. B. neue Ordner anlegen oder Systemeinstellungen ändern. Die Einstellungen können die Anwender auf ihrem Rechner abändern.

Im Gegensatz zu den Richtlinien in den Gruppenrichtlinien stellen Group Policy Preferences (Gruppenrichtlinien-Einstellungen) nur bestimmte Einstellungen um, aber nicht unumkehrbar.

Über den Knoten *Einstellungen* erreichen Sie diese *Group Policy Preferences* im Editor für Gruppenrichtlinien. Nehmen Sie im Knoten *Einstellungen* im Gruppenrichtlinienverwaltungs-Editor Anpassungen vor, verwendet dieser Editor oft die gleiche grafische Oberfläche wie die entsprechende Einstellung auf dem Computer selbst.

Sie wählen zunächst den Bereich der Einstellungen aus, klicken mit der rechten Maustaste in den Ergebnisbereich rechts und wählen im Kontextmenü den Eintrag *Neu*. Anschließend können Sie Einstellungen vorgeben, welche an die Computer übergeben werden. Über diese Einstellungen können Sie beispielsweise auch neue Ordner oder Dateien im Dateisystem auf den Rechnern anlegen lassen.

Über die Registerkarte *Gemeinsame Optionen* einer solchen Einstellung können Sie darüber hinaus mit Filtern auswählen, auf welche Art von Rechnern die Richtlinie angewendet werden soll. Das ist dann sinnvoll, wenn Sie die Einstellungen über Gruppenrichtlinien weitergeben. Über diese Einstellungen können Sie zum Beispiel auch Netzwerkspeicher verbinden lassen. Die Einstellungen sind weitgehend selbsterklärend.

Wollen Sie zum Beispiel Registry-Einträge auf den Rechnern vornehmen, können Sie das ebenfalls über die Group Policy Preferences durchführen:

- ▶ Wählen Sie im Gruppenrichtlinieditor *Computerkonfiguration* oder *Benutzerkonfiguration*.
- ▶ Klicken Sie auf *Einstellungen* und navigieren Sie zu *Windows-Einstellungen - Registrierung*.
- ▶ Klicken Sie mit der rechten Maustaste in den Ergebnisbereich rechts und wählen Sie die Option *Neu - Registrierungselement*.

Im neuen Fenster können Sie vorhandene Einstellungen anpassen, aktualisieren oder einen neuen Wert erstellen.

- ▶ Um zum Beispiel einen neuen Wert in der Registry zu erstellen, wählen Sie *Registrierungselement* aus. Über einen Browser wählen Sie den Registrypfad, ähnlich zum Registry-Editor auf dem lokalen Rechner.
- ▶ Wählen Sie die Option *Aktualisieren*, setzt die Preference den Wert immer auf den festgelegten Wert zurück, auch wenn ein Benutzer diesen lokal ändert.

Bei der Auswahl von *Ersetzen* wird der lokale Pfad auf dem Rechner gelöscht und gegen den Wert in der Preference ersetzt.

Über die Option *Neu - Registrierungs-Assistent* können Sie auch Einstellungen von einem Quellrechner exportieren und auf die Zielrechner importieren, denen die gewünschte Group Policy Preference zugeordnet wird.



### Richtlinien nutzen

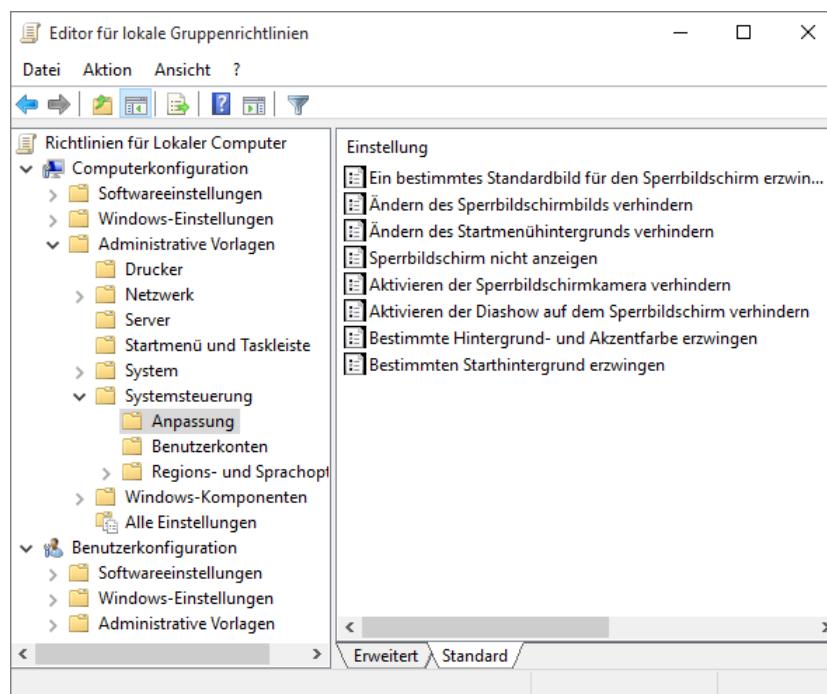
Richtlinien sind feste Vorgaben, die Anwender zwingend übernehmen müssen. Eine Änderung auf dem Client ist nicht möglich, da die Richtlinie die entsprechenden Einstellungen deaktiviert. Das heißt, Sie setzen lokal auf dem Rechner oder über einen Server Einstellungen in Gruppenrichtlinien, zum Beispiel wie sich Windows beim Herunterladen von Patches verhalten soll. Die Clientrechner übernehmen diese Einstellungen und lassen keine lokale Änderung mehr zu. Die Optionen dazu sind ausgegraut.

## 12.8 Windows 10 mit Gruppenrichtlinien verwalten

Viele Einstellungen in Windows 10 können Sie mit Gruppenrichtlinien anpassen. Dazu verwenden Sie entweder den lokalen Editor für Gruppenrichtlinien, den Sie mit `gpedit.msc` starten, oder Sie erstellen Gruppenrichtlinien auf Servern mit Windows Server 2012 R2/2016 und weisen diese den Arbeitsstationen mit Windows 10 zu. Neue Funktionen in Windows 10 stehen nur zur Verfügung, wenn Sie die Richtlinien lokal einsetzen oder mindestens einen Domänencontroller auf Windows Server 2012 R2/2016 umstellen. Die neuen Einstellungen für Windows 10 sind in Windows Server 2016 standardmäßig bereits verfügbar. Auf Servern mit Windows Server 2012 R2 müssen Sie diese als Vorlagen erst zur Verfügung stellen. Microsoft stellt die administrativen Vorlagen für Windows 10 kostenlos zur Verfügung (<https://www.microsoft.com/de-de/download/details.aspx?id=48257>).

### Sperrbildschirm über Richtlinien steuern

Manche Unternehmen wollen zum Beispiel den Sperrbildschirm nicht nutzen. Sie können in Windows 10 den Sperrbildschirm deaktivieren und dazu die Gruppenrichtlinien nutzen. Starten Sie die Gruppenrichtlinien und wechseln Sie zu *Computerkonfiguration - Administrative Vorlagen - Systemsteuerung - Anpassung*. Auf der rechten Seite können Sie verschiedene Einstellungen vornehmen, auch den Sperrbildschirm deaktivieren. Hier können Sie zum Beispiel auch ein bestimmtes Hintergrundbild für den Anmeldebildschirm festlegen und verhindern, dass Anwender Startseite und Anmeldebildschirm anpassen.



Anmeldebildschirm in den Gruppenrichtlinien anpassen

Windows 10 zeigt häufig Benachrichtigungen am oberen Bildschirm an. Sie können in den Einstellungen des Betriebssystems festlegen, welche Einstellungen angezeigt werden sollen und welche Windows ausblenden soll. Für Unternehmensrechner lassen sich diese Einstellungen in den Gruppenrichtlinien festlegen. Sie finden die entsprechenden Einstellungen im Bereich *Benutzerkonfiguration - Administrative Vorlagen - Startmenü und Taskleiste - Benachrichtigungen*. Hier lassen sich verschiedene Einstellungen vornehmen sowie Einstellungsmöglichkeiten der Anwender auf den PCs unterbinden.

## Startmenü über Richtlinien steuern und mehr

In Windows 10 können Sie mit dem Cmdlet `Export-StartLayout` in der PowerShell das Aussehen und die Konfiguration des Startmenüs in eine Datei exportieren (`Export-StartLayout -path <Pfad zur XML-Datei>`).

Administratoren in Unternehmensnetzwerken können Veränderungen an der Startseite über Richtlinien verbieten. Sie können Veränderungen im Startmenü untersagen. Dazu gibt es in den Richtlinien von Windows 10 und Windows Server 2016 die Option *Startseitenlayout*. Diese ist im Bereich *Benutzerkonfiguration - Administrative Vorlagen - Startmenü und Taskleiste* zu finden. In diesem Bereich können Sie auch die Layoutdatei hinterlegen, die Sie vorher mit dem Cmdlet `Export-StartLayout` exportiert haben.

Mit einer Gruppenrichtlinieneinstellung auf Windows-10-Rechnern können Sie Windows 10 teilweise deutlich schneller starten lassen. Vor allem in Netzwerken mit Gruppenrichtlinien ist die folgende Einstellung sinnvoll.

Sie können in Windows 10 Gruppenrichtlinien lokal auf den Rechnern speichern. Beim Anmelden müssen die Rechner nicht alle Einstellungen auf den Client herunterladen, sondern können direkt die Einstellungen auf dem Rechner nutzen. Nur neue Einstellungen überträgt der Client dann aus dem Internet. Gehen Sie zur Aktivierung folgendermaßen vor:

- ▶ Navigieren Sie zu *Computerkonfiguration - Administrative Vorlagen - System - Gruppenrichtlinie*.
- ▶ Klicken Sie doppelt auf *Zwischenspeichern von Gruppenrichtlinien konfigurieren*.
- ▶ Aktivieren Sie die Einstellung.

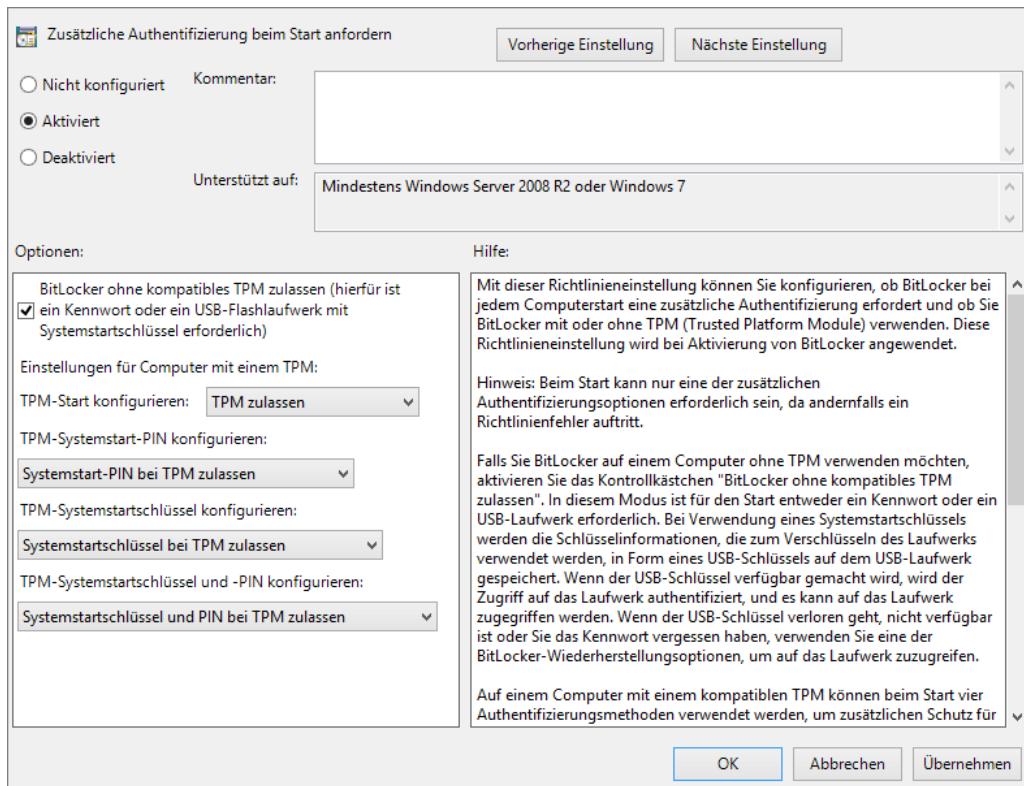
Windows 10 bietet weiterhin die Möglichkeit, verschiedene Ordner innerhalb des Profils auf ein Serverlaufwerk umzuleiten. Dadurch ist sichergestellt, dass die Daten der Anwender sicher auf einem Server gespeichert werden, aber dennoch transparent zugreifbar sind, wenn ein Anwender zum Beispiel seinen Dokumentenordner öffnet. Die Größe der Profile ist dadurch reduziert, die Anmeldezeit verkürzt. Sie finden die Ordnerumleitungen unter *Benutzerkonfiguration - Richtlinien - Windows-Einstellungen - Ordnerumleitungen*.

## BitLocker schnell und einfach aktivieren

BitLocker (vgl. Abschnitt 15.5) können Sie auch dann nutzen, wenn kein Verschlüsselungs-Chip im Rechner eingebaut ist. Die Laufwerkverschlüsselung ist Bestandteil der Editionen Pro und Enterprise von Windows 10.

Gehen Sie zur Konfiguration folgendermaßen vor:

- ▶ Wechseln Sie im Navigationsbereich zum Eintrag *Computerkonfiguration - Administrative Vorlagen - Windows-Komponenten - BitLocker-Laufwerkverschlüsselung - Betriebssystemlaufwerke*.
- ▶ Doppelklicken Sie im rechten Bereich des Fensters auf die Richtlinie *Zusätzliche Authentifizierung beim Start anfordern*.
- ▶ Aktivieren Sie im Dialogfeld die Option *Aktiviert*.
- ▶ Stellen Sie sicher, dass das Kontrollkästchen *BitLocker ohne kompatibles TPM zulassen* aktiviert ist.
- ▶ Klicken Sie auf *OK*.  
Die Richtlinie erhält darauf in der Statusspalte den Status *Aktiviert*.
- ▶ Nachdem diese Aufgaben durchgeführt sind, können Sie BitLocker aktivieren. Starten Sie die Konfigurationsoberfläche von BitLocker über *Systemsteuerung - System und Sicherheit - BitLocker-Laufwerkverschlüsselung*.



*BitLocker ohne Verschlüsselungs-Chip (TPM) über Richtlinien aktivieren*

### Sicherheit in Windows 10 mit AppLocker steuern

Administratoren in Windows-Netzwerken können mit Windows Server 2012 R2/2016 und Windows 10 über Richtlinien unerwünschte Anwendungen sperren und so Sicherheitslücken schließen. Die Funktionen sind der Enterprise-Version von Windows 10 vorbehalten. Sie können in Windows 10 Einstellungen für Windows-Apps und die Startseite in AppLocker hinterlegen.

AppLocker kann automatische Regeln erstellen und bestimmte Ordner auf neue Programme hin überwachen. Neben Gruppenrichtlinien können Sie über Sicherheitsgruppen filtern.

Um AppLocker zu verwenden, navigieren Sie in der Gruppenrichtlinienverwaltung zu *Computerkonfiguration - Windows-Einstellungen - Sicherheitseinstellungen - Anwendungssteuerungsrichtlinien*. Klicken Sie auf *AppLocker*. Neu seit Windows 8 ist der Knoten *App-Paketregeln*. Hier steuern Sie den Zugriff der Anwender auf Windows-Apps auf den Windows-10-PCs.

### Sicherheit in Windows 10 verbessern

Microsofts Sprach- und Suchassistent Cortana wird ständig ausgebaut. Unter anderem besteht die Möglichkeit, den Assistenten auch über den Sperrbildschirm zu nutzen. Damit sind nicht alle Unternehmen einverstanden. Die Einstellungen für den neuen Suchassistenten sind in den Gruppenrichtlinien im Bereich *Computerkonfiguration - Administrative Vorlagen - Windows-Komponenten - Suche* zu finden.

Über Gruppenrichtlinieneinstellungen lässt sich Cortana bremsen. Mit der Option *Nicht im Web suchen und keine Webergebnisse in der Suche anzeigen* wird verhindert, dass Anwender über Cortana direkt im Internet nach Informationen suchen.

## Microsoft Edge über Gruppenrichtlinien konfigurieren

Der Nachfolger des Internet Explorers wird in Windows 10 ausgebaut. Es ist zum Beispiel möglich, Erweiterungen zu installieren wie bei Google Chrome oder Mozilla Firefox. Microsoft Edge lässt sich über Gruppenrichtlinien steuern. Zu finden sind die Einstellungsmöglichkeiten über *Computerkonfiguration - Richtlinien - Administrative Vorlagen - Windows-Komponenten - Microsoft Edge*.

## Den Modus Überwachter Ordnerzugriff steuern

Ab Windows 10, Version 1709 lassen sich Verzeichnisse auf Computern vor Ransomware schützen. Dazu wird der überwachte Ordnerzugriff aktiviert. Danach dürfen nur noch genehmigte Apps Änderungen an Dateien in den hinterlegten Ordnern vornehmen. Die Einstellungen lassen sich lokal in den Einstellungen von Windows 10 über das neue Windows Defender Security Center vornehmen, in der PowerShell oder über Gruppenrichtlinien. Dazu müssen die neuen ADMX-Dateien importiert werden.

Die neuen Optionen für den überwachten Ordnerzugriff stehen bei *Computerkonfiguration - Richtlinien - Administrative Vorlagen - Windows-Komponenten - Windows Defender Antivirus - Windows Defender Exploit Guard - Überwachter Ordnerzugriff* zur Verfügung. Hier kann konfiguriert werden, welche Ordner geschützt werden sollen, welche Anwendungen Änderungen vornehmen dürfen und, ob der überwachte Ordnermodus nur überwachen oder Änderungen auch blockieren soll. Generell stehen bei *Windows Defender Exploit Guard* noch weitere Einstellungen zur Verfügung, die Windows-10-Rechner besser vor Angreifern schützen.

## Exploit-Schutz per Gruppenrichtlinie steuern

Windows 10 bietet ab Version 1709 einen Exploit-Schutz, der Windows vor unbekannten Angreifern schützen soll. Auch hier finden sich die neuen Einstellungen in der Einstellungs-App über das Windows Defender Security Center. Über Gruppenrichtlinien kann diese Einstellung bei *Computerkonfiguration - Richtlinien - Administrative Vorlagen - Windows-Komponenten - Windows Defender Exploit Guard - Exploit-Schutz* gefunden werden.

## 12.9 Übung

### Mit Richtlinien arbeiten

Übungsdatei: --

Ergebnisdatei: *Uebung12\_E.pdf*

1. Welche Zustände können Richtlinien einnehmen?
2. Wie rufen Sie die Richtlinienverwaltung in Windows 10 auf?

# 13 Zugriffsberechtigungen und Freigaben

## In diesem Kapitel erfahren Sie

- ✓ wie Sie lokale Ressourcen anderen Benutzern zugänglich machen
- ✓ wie der Zugriff auf freigegebene Dateien und Ordner geregelt wird

## 13.1 Ressourcen gemeinsam nutzen

### Grundlagen der gemeinsamen Nutzung von Dateien und Ordnern

Windows 10 kann Dateien und Ordner (Ressourcen) mehreren Benutzern für die gemeinsame Nutzung zur Verfügung stellen. Nach der Installation von Windows 10 ist der PC zunächst in einer Arbeitsgruppe organisiert und noch kein Mitglied einer Windows-Domäne. Sie können mithilfe des Freigabe-Assistenten bestimmte Ressourcen für einzelne Benutzer oder Benutzergruppen unter einem **Freigabennamen** im Netzwerk freigeben. Der Zugriff auf Freigaben wird über **Freigabeberechtigungen** für Benutzer und Gruppen geregelt. Auf NTFS-Datenträgern können zusätzlich die **NTFS-Berechtigungen** für die Zugriffsregelung verwendet werden, wobei ein Zugriff nur möglich ist, wenn beide Berechtigungen dies erlauben. Die effektive Berechtigung wird aus der Schnittmenge der beiden Berechtigungen gebildet, also dem kleinsten gemeinsamen Nenner.



Beachten Sie, dass die Windows-Firewall möglicherweise den Zugriff über das Netz auf die freigegebenen Ordner verhindert. Überprüfen Sie daher bei Problemen die Windows-Firewalleinstellungen und erlauben Sie den Zugriff über das Netzwerk.

### UNC-Netzwerkpfade

Im Netzwerk werden Adressen von Ressourcen nach der universellen Namenskonvention **UNC (Uniform Naming Convention)** bezeichnet. Ein UNC-Pfad beginnt unter Windows stets mit \\ und sieht z. B. so aus:

- ✓ \\Servername\Freigabename\Pfad (z. B. \\Notebook\Öffentlich)
- ✓ \\IP-Adresse\Freigabename\Pfad (z. B. \\192.168.0.1\Datenaustausch)
- ✓ \\?\Lokales\_Laufwerk:\Ordnername (z. B. \\?\C:\Programme)



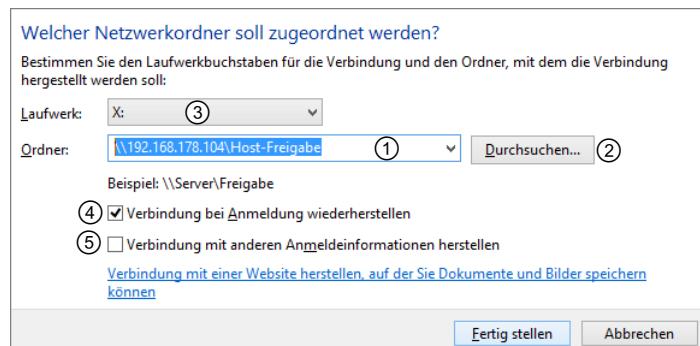
Das Fragezeichen im UNC-Pfad \\?\ signalisiert, dass es sich um eine Netzwerkressource auf dem lokalen Rechner handelt. Auf diese Weise kann der Computer die Adresse auflösen und zeigt alle vorhandenen Ordner und Dateien an, selbst wenn sie nicht im Netzwerk freigegeben wurden.

### Mit einer Freigabe verbinden

Um auch nach dem nächsten Windows-Start dauerhaften Zugang zu einer Netzwerkfreigabe zu erhalten, können Sie Freigaben als Netzlaufwerk verbinden:

- Klicken Sie im Datei-Explorer im Kontextmenü einer Freigabe auf *Netzlaufwerk verbinden*, so ist der UNC-Pfad zur Freigabe im nächsten Dialog bereits eingetragen ①.  
*oder*
  - Klicken Sie im Datei-Explorer im Kontextmenü von *Dieser PC* auf *Netzlaufwerk verbinden*. Geben Sie den Netzwerkpfad ein ① oder durchsuchen Sie das Netzwerk nach Freigaben ②.
  - Wählen Sie den Laufwerkbuchstaben für das Netzlaufwerk aus ③.
- Für eine dauerhafte Verbindung können Sie das Kontrollfeld *Verbindung bei Anmeldung wiederherstellen* ④ aktivieren.

- Wenn die Freigabe über ein anderes Benutzerkonto erfolgt, aktivieren Sie ⑤. Daraufhin werden Sie bei der Anmeldung nach Benutzernamen und Kennwort gefragt, mit dem Sie sich anmelden wollen.
- Klicken Sie auf *Fertig stellen*. Die Freigabe ist jetzt als Laufwerk unter dem angegebenen Buchstaben verfügbar.



Ein Netzlaufwerk verbinden

### Freigabe-Assistenten deaktivieren

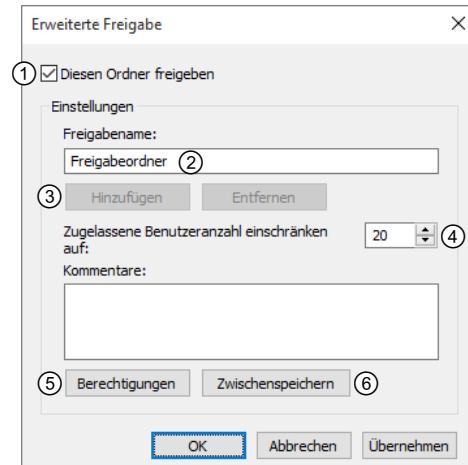
Im Auslieferungszustand ist bei Windows 10 der Freigabe-Assistent eingeschaltet, mit dem Sie einen Ordner für einzelne Benutzer oder Benutzergruppen freigeben und bestimmen können, ob die Benutzer nur lesen oder auch schreiben dürfen. Das ist für Heimnetzwerke und kleine Arbeitsgruppen vollkommen ausreichend. Um jedoch in größeren Firmennetzwerken die erweiterten Freigabeeinstellungen nutzen zu können, muss der Assistent deaktiviert werden:

- Klicken Sie im Datei-Explorer auf *Ansicht - Optionen*.
- Deaktivieren Sie im Register *Ansicht* das Kontrollfeld *Freigabe-Assistent verwenden (empfohlen)*.
- Klicken Sie auf *Übernehmen* und *OK*.

### Ordner und Laufwerke freigeben

- Klicken Sie im Kontextmenü des freizugebenden Ordners oder Datenträgers auf *Freigeben für - Erweiterte Freigabe*. Ist *Erweiterte Freigabe* nicht verfügbar, wählen Sie im Explorer *Ansicht - Optionen - Ordner und Suchoptionen ändern* und deaktivieren im Register *Ansicht* das Kontrollfeld *Freigabe-assistent verwenden*.
- Wählen Sie im Register *Freigabe* die Option *Erweiterte Freigabe*.
- Aktivieren Sie *Diesen Ordner freigeben* ①.
- Übernehmen Sie den Ordnernamen als Freigabenamen ② oder erstellen Sie unter *Hinzufügen* ③ einen neuen Freigabenamen. Sie können außerdem die Zahl der gleichzeitigen Zugriffe (1–20) einstellen ④, die Freigabeberechtigungen ändern ⑤ und die Offline-Einstellungen für die Freigabe anpassen ⑥.
- Klicken Sie auf *Übernehmen* und *OK*.

Nach der erfolgreichen Freigabe wird der Ordner als freigegeben markiert.



Sie können auf der Registerkarte *Sicherheit* in den Eigenschaften des Ordners zusätzlich noch Berechtigungen auf Basis des Dateisystems vergeben. Klicken Sie dazu auf *Bearbeiten*.

Freigaben lassen sich in der Eingabeaufforderung durch den Befehl `net share <Name der Freigabe> <Pfad des Verzeichnisses, das freigegeben werden soll>` ebenfalls freigeben.



Wenn Sie eine Freigabe beenden möchten, deaktivieren Sie *Diesen Ordner freigeben* wieder. Die Freigabe wird beendet, die Einstellungen der Freigabeberechtigungen bleiben aber erhalten.

Wenn eine Freigabe eine Anmeldung erfordert, ist es nicht möglich, sich dort unter einem lokalen Benutzerkonto mit leerem Kennwort anzumelden. Das lokale Benutzerkonto muss mit einem Kennwort ausgestattet sein.



## Die verfügbaren Freigabeberechtigungen

Berechtigungen auf Freigabeebene regeln den Netzwerkzugriff auf freigegebene Ressourcen, sind aber bei lokalen Zugriffen unwirksam. Freigabeberechtigungen können für Ordner auf Datenträgern mit FAT und NTFS vergeben werden. Es kann nur der freigegebene Ordner mit seinem gesamten Inhalt reglementiert werden, jedoch keine einzelnen darin enthaltenen Unterordner und Dateien.

Windows 10 kennt drei Freigabeberechtigungen:

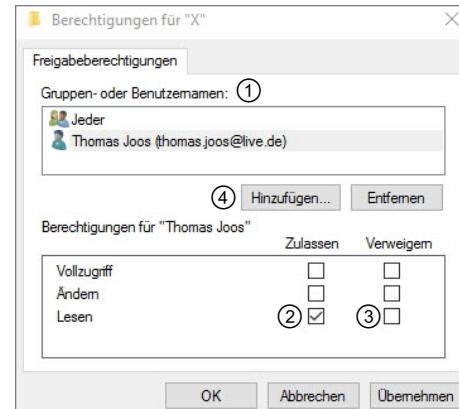
Freigabeberechtigung	Zugriffsmöglichkeiten
<i>Lesen</i>	Ein Benutzer kann alle Dateien und Ordner, Dateiinhalte und Dateiattribute ansehen und Programme ausführen. Dies ist die Standardeinstellung.
<i>Ändern</i>	Zusätzlich zur Berechtigung <i>Lesen</i> kann der Benutzer Ordner und Dateien erstellen, verändern und löschen sowie Dateiattribute ändern.
<i>Vollzugriff</i>	Zusätzlich zur Berechtigung <i>Ändern</i> kann der Benutzer den Besitz an Dateien übernehmen und die Berechtigungen für Dateien ändern.

Jede dieser Freigabeberechtigungen können Sie einzeln vergeben oder verweigern, die Berechtigungen sind jedoch kumulativ. Ein Benutzer erhält die höchste Berechtigungsstufe, die ihm aus seinen individuellen Berechtigungen und seiner Gruppenmitgliedschaft erwächst. Beachten Sie auch die Besonderheiten in Kombination mit NTFS-Berechtigungen, die weiter unten beschrieben werden.

## 13.2 Berechtigungen auf Freigabeebene einsetzen

### Freigabeberechtigungen verwalten

- ▶ Klicken Sie im Dialog *Erweiterte Freigabe* auf *Berechtigungen*. Markieren Sie im Feld *Gruppen- oder Benutzernamen* ① den benötigten Eintrag.
- ▶ Aktivieren Sie die Kontrollfelder *Zulassen* ② oder *Verweigern* ③ für die jeweilige Berechtigung nach Bedarf. Falls der benötigte Benutzer oder die Gruppe noch nicht genannt ist, besitzt er/sie derzeit noch keine Zugriffsberechtigungen auf die Ressource.
- ▶ Klicken Sie auf *Hinzufügen* ④, um einem weiteren Benutzer oder einer Gruppe Zugriffsberechtigungen zu erteilen.
- ▶ Das Dialogfenster *Benutzer oder Gruppen wählen* wird geöffnet. Markieren Sie dort den betreffenden Benutzer oder die Gruppe und klicken Sie auf *Hinzufügen*.
- ▶ Verlassen Sie das Dialogfenster mit *OK* und weisen Sie die Berechtigungen zu wie beschrieben.
- ▶ Klicken Sie auf *Übernehmen* und auf *OK*.



Freigabeberechtigungen sind nicht geeignet zur differenzierten Zugriffskontrolle. Wenn Sie Dateien in einem freigegebenen Ordner einzeln reglementieren wollen, müssen Sie NTFS-Berechtigungen verwenden.



Grundsätzlich sollten Sie die Freigabeberechtigungen über Gruppen und nicht über Einzelbenutzer steuern. Gewöhnen Sie sich diese Verfahrensweise an, denn über Gruppenzugehörigkeit können Sie die Berechtigungen einer Person viel effektiver regeln, vor allem, wenn die Berechtigungen später geändert werden müssen.

### 13.3 NTFS-Berechtigungen einsetzen

#### Grundlagen zu NTFS-Berechtigungen

NTFS-Berechtigungen sind nur auf NTFS-Datenträgern verfügbar. Sie bieten deutlich höhere Sicherheit gegen unberechtigten Zugriff als Freigabeberechtigungen.

NTFS-Berechtigungen ermöglichen...

- ✓ feine Abstufung der Zugriffsberechtigungen,
- ✓ **Vererbung** (automatische Berechtigungsübertragung) auf untergeordnete Ordner und Dateien,
- ✓ differenzierte Zugriffsbeschränkungen für Dateien und Ordner,
- ✓ Wirksamkeit auch bei lokaler Anmeldung eines Benutzers.

Weisen Sie einem Benutzerkonto die Berechtigung *Lesen* für ein Verzeichnis zu und bekommt zusätzlich eine Gruppe, in der dieser Benutzer Mitglied ist, die Berechtigung *Schreiben* zugewiesen, ergeben die effektiven Berechtigungen *Lesen und Schreiben*. Es gelten grundsätzlich die engsten Einschränkungen der Zugriffsberechtigungen. Wenn ein Benutzer *Vollzugriff* auf eine Freigabe hat und ein Verzeichnis auf dem PC nur lesen darf, darf er es auch tatsächlich nur lesen, auch wenn er per Vollzugriff über das Netzwerk zugreift. Hat er im Dateisystem *Vollzugriff* und wurde auf die Freigabe nur das Leserecht vergeben, darf er auf das Verzeichnis über das Netzwerk nur lesend zugreifen. Er kann allerdings lokal auf dem Computer oder über andere überlappende Freigaben, die diese Einschränkung nicht haben, mit mehr Rechten zugreifen. Die Berechtigungen bilden daher immer eine Schnittmenge zwischen Freigabeberechtigungen und Berechtigungen auf dem Dateisystem (NTFS).

Berechtigungen für den Zugriff über das Netzwerk nehmen Sie über die Registerkarte *Freigabe* in den Eigenschaften des Ordners über die Schaltfläche *Erweiterte Freigabe* vor. Mit Berechtigungen legen Sie fest, wer über das Netzwerk auf den PC zugreifen darf. Den jeweiligen Benutzer müssen Sie vorher auf dem PC mit der Freigabe anlegen. Das können Sie über *Einstellungen - Konten - Weitere Benutzer* durchführen oder durch die Eingabe von `lusrmgr.msc` auf der Startseite.

Die Festlegung auf NTFS-Ebene, also für das Dateisystem, erfolgt über die Eigenschaften eines Ordners auf der Registerkarte *Sicherheit*. Nach jeweils einem Klick auf die Schaltfläche *Bearbeiten* und *Hinzufügen* können Sie neue Benutzer, denen Sie Berechtigungen gewähren wollen, hinzufügen. Dabei haben Sie folgende Möglichkeiten:

NTFS-Dateiberechtigung	Zugriffsmöglichkeiten
<i>Lesen</i>	Datei lesen, Berechtigungen, Besitzrechte und Attribute einsehen
<i>Schreiben</i>	Datei überschreiben, Berechtigungen und Besitzrechte einsehen, Attribute ändern
<i>Lesen, Ausführen</i>	Lesen und Anwendungen ausführen
<i>Ändern</i>	Datei ändern und löschen (beinhaltet <i>Lesen, Schreiben und Ausführen</i> )
<i>Vollzugriff</i>	Besitz übernehmen und Berechtigungen ändern (beinhaltet alle anderen Berechtigungen)

Für Ordner können umfangreichere NTFS-Berechtigungen vergeben werden:

NTFS-Ordnerberechtigung	Zugriffsmöglichkeiten
<i>Lesen</i>	Unterordner auflisten, Dateien lesen, Berechtigungen, Besitzrechte und Attribute einsehen
<i>Schreiben</i>	Unterordner erstellen, Dateien erstellen, Berechtigungen und Besitzrechte einsehen und Attribute ändern
<i>Ordnerinhalt anzeigen</i>	Unterordner und Dateien auflisten
<i>Lesen, Ausführen</i>	Durch einen Ordner navigieren, auch wenn für diesen Ordner und die enthaltenen Dateien keine Leseberechtigung vorliegt (beinhaltet <i>Lesen</i> und <i>Ordnerinhalt anzeigen</i> )

NTFS-Ordnerberechtigung	Zugriffsmöglichkeiten
Ändern	Ordner löschen (beinhaltet <i>Lesen, Schreiben, Anzeigen des Ordnerinhalts und Ausführen</i> )
Vollzugriff	Unterordner und Dateien löschen, den Besitz übernehmen und Berechtigungen ändern (beinhaltet alle anderen Berechtigungen)



Diese standardisierten Datei- und Ordnerberechtigungen sind jeweils eine Kombination aus 14 einzelnen Berechtigungen. Es ist jedoch möglich, die Einzelberechtigungen anders zu kombinieren, um für Sonderfälle **spezielle Berechtigungen** vergeben zu können.

### Effektive Berechtigungen

Die tatsächlichen (effektiven) NTFS-Berechtigungen eines Benutzers für eine lokale Ressource setzen sich kumulativ aus allen NTFS-Berechtigungen zusammen, die er aufgrund seiner Mitgliedschaft in verschiedenen Gruppen besitzt. Ein Benutzer verfügt über die Summe aller NTFS-Berechtigungen der Gruppen, deren Mitglied er ist. So kann z. B. ein Benutzer aus der Gruppe *Mitarbeiter* lediglich die Berechtigung erhalten, Dateien zu lesen, aus der Mitgliedschaft der Administratorengruppe heraus hat er jedoch Vollzugriff.

### Zugriffsverweigerung hat Vorrang

Das explizite Verweigern des Zugriffs auf eine Ressource hat immer Vorrang vor dem Zulassen. Wenn Sie einem Benutzer oder einer Gruppe eine Berechtigung verweigern, kann die Verweigerung nicht durch andere Berechtigungen wieder außer Kraft gesetzt werden. Wenn Sie einem Benutzer die Berechtigung *Vollzugriff* für eine Ressource verweigern, kann er unter keinen Umständen mehr darauf zugreifen, auch wenn durch seine Gruppenmitgliedschaft eigentlich Zugriffe zugelassen sind.

### Datei- und Ordnerberechtigungen kombinieren

Hat ein Benutzer aufgrund seiner Gruppenmitgliedschaft mehrere NTFS-Berechtigungen für eine Datei, sind diese auf Dateiebene wiederum kumulativ. Der Benutzer verfügt über die Summe aller Berechtigungen, die ihm selbst oder den Gruppen, in denen er Mitglied ist, für die Datei erteilt wurden. Diese Dateiberechtigungen haben Vorrang vor Ordnerberechtigungen, überschreiben also Ordnerberechtigungen. So kann eine Benutzergruppe bei genauer Kenntnis des Pfades auch dann auf eine Datei zugreifen, wenn sie für den übergeordneten Ordner keine entsprechende Berechtigung besitzt.

### NTFS-Berechtigungen mit Freigabeberechtigungen kombinieren

Bei Freigaben können Freigabeberechtigungen und NTFS-Berechtigungen gemeinsam verwendet werden. In dieser Kombination bestimmt die am meisten **einschränkende** Zugriffsberechtigung der beiden Berechtigungstypen den Zugang.

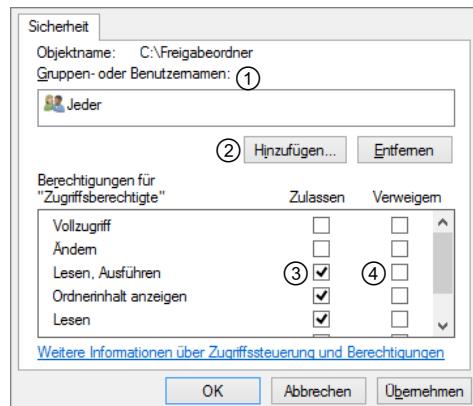
Sollte ein Laufwerk, auf dem Sie Berechtigungen vergeben wollen, mit dem FAT-Dateisystem formatiert sein, bietet Windows einen einfachen Befehl, mit dem das Dateisystem von FAT in NTFS umgewandelt werden kann. Dateien gehen dabei keine verloren. Eine optimale Datensicherheit erhalten Sie nur mit dem NTFS-Dateisystem. Außerdem ist dieses Dateisystem performanter und wesentlich stabiler. Eine Konvertierung von FAT zu NTFS ergibt daher für jeden PC-Anwender Sinn. So wandeln Sie das FAT-Dateisystem in NTFS um:

- ▶ Suchen Sie auf der Startseite nach cmd, klicken Sie mit der rechten Maustaste auf *Eingabeaufforderung*, und wählen Sie *Als Administrator ausführen*.
- ▶ Geben Sie in der Eingabeaufforderung den Befehl convert <Laufwerkbuchstabe>: /fs:ntfs ein. Windows beginnt daraufhin mit der Konvertierung und meldet die erfolgreiche Umstellung.
- ▶ Unter Umständen meldet Windows, dass der Datenträger in Benutzung ist. Bestätigen Sie das Beenden dieser sogenannten „Bezüge“ mit J.

## 13.4 NTFS-Berechtigungen verwalten

### NTFS-Berechtigungen einstellen

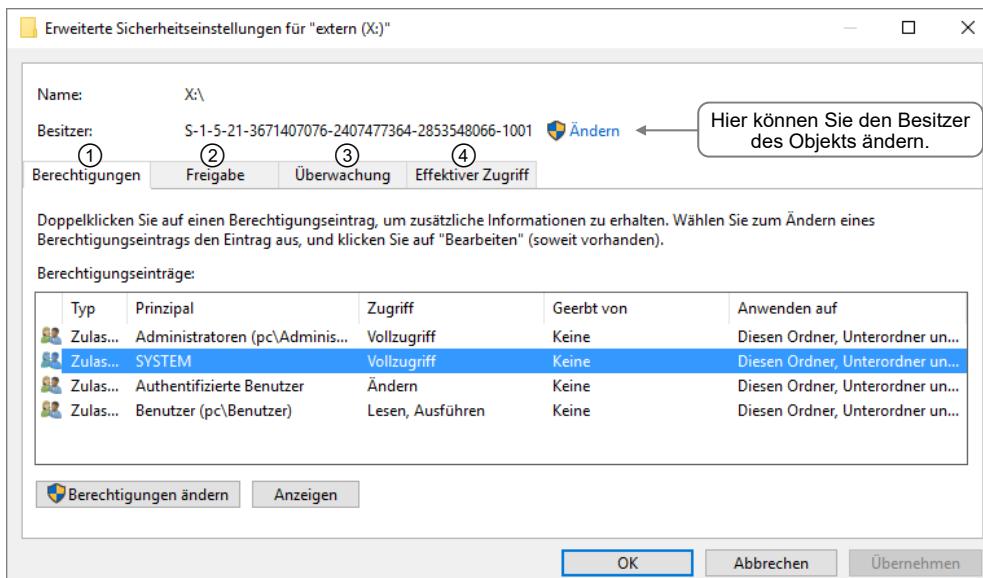
- ▶ Klicken Sie in den Dateieigenschaften des Freigabeordners im Register *Sicherheit* auf *Bearbeiten*.
- ▶ Markieren Sie im Feld *Gruppen- oder Benutzernamen* ① den gewünschten Eintrag.
- ▶ Falls der gesuchte Eintrag noch nicht vorhanden ist, klicken Sie auf *Hinzufügen* ② und wählen Sie das benötigte Objekt aus.
- ▶ Legen Sie mit den Kontrollfeldern *Zulassen* ③ fest, welche Berechtigung erteilt werden soll.
- ▶ Wenn Sie einem Benutzer oder einer Gruppe den Zugriff vollständig nehmen wollen, entfernen Sie den Eintrag aus der Liste *Gruppen- oder Benutzernamen*.
- ▶ Aktivieren Sie *Verweigern* ④ für einzelne NTFS-Berechtigungen oder den Vollzugriff nur, um den Zugriff ausdrücklich zu verbieten.
- ▶ Klicken Sie auf *Übernehmen* und *OK*.



*NTFS-Berechtigungen erteilen*

### Erweiterte Sicherheitseinstellungen

Mit einem Klick auf *Erweitert* im Register *Sicherheit* öffnen Sie die erweiterten Sicherheitseinstellungen, wo Sie auf vier Registern detaillierte Einstellungen vornehmen können.



### Umfassende Kontrolle der Zugangsberechtigungen

- ✓ Auf dem ersten Register *Berechtigungen* ① können Sie durch einen Doppelklick auf ein Objekt die grundlegenden oder erweiterten NTFS-Berechtigungen einsehen und verändern.
- ✓ Das zweite Register *Freigabe* ② zeigt die Freigabeberechtigungen an, hier können Sie jedoch nichts ändern.
- ✓ Das dritte Register *Überwachung* ③ erlaubt das Einschalten und detaillierte Einstellen der Zugriffsüberwachung, mit der Sie z. B. fehlgeschlagene Zugriffe durch eine bestimmte Benutzergruppe erfassen können.
- ✓ Das letzte Register *Effektiver Zugriff* ④ zeigt nach Auswahl eines Benutzerobjekts dessen tatsächlichen Zugriff an. Diese Ansicht ist bei der Überprüfung von Zugriffsproblemen sehr hilfreich.

Windows 10 bietet die Möglichkeit, den Zugriff von Gruppen und Benutzern auf Ordner und Dateien zu überwachen und Zugriffe im Ereignisprotokoll zu notieren. Wenn der Zugriff auf eine Ressource überwacht werden soll, tragen Sie die betreffende Gruppe im Register *Überwachung* des Dialogfensters *Erweiterte Sicherheitseinstellungen für "Objektname"* ein.

Erstellen Sie anschließend eine Gruppenrichtlinie zur Zugriffsüberwachung:

- Öffnen Sie die lokale Richtlinie für den Computer über den Befehl `gpedit.msc`.  
Es öffnet sich der Editor für lokale Gruppenrichtlinien.
- Navigieren Sie zu *Computerkonfiguration - Windows-Einstellungen - Sicherheitseinstellungen - Lokale Richtlinien - Überwachungsrichtlinien*.

In den Standardeinstellungen ist die Überwachung zunächst nicht aktiviert. Nach der Aktivierung der einzelnen Optionen müssen Sie noch auswählen, ob Windows erfolgreiche und/oder fehlgeschlagene Zugriffsversuche protokollieren soll.

Um spezielle Berechtigungen zu setzen und weitere Einstellungen vorzunehmen, wählen Sie im Eigenschaftenfenster der Elemente (Datei oder Verzeichnis) auf der Registerkarte *Sicherheit* die Schaltfläche *Erweitert*. Standardmäßig verwenden Dateien und Verzeichnisse die Berechtigungen des übergeordneten Verzeichnisses. Mit der Schaltfläche *Vererbung deaktivieren* schalten Sie diese Vererbung aus und können für ein Verzeichnis eigene Rechte erteilen. Bei der Deaktivierung können Sie die bestehenden Rechte als Vorlage übernehmen oder die vorhandenen Rechte ganz löschen, um neue Rechte zu setzen.

Um die erweiterten Berechtigungen zu konfigurieren, klicken Sie im neuen Fenster doppelt auf den entsprechenden Eintrag. Sie können entweder bestehende Einträge bearbeiten oder neue Benutzerkonten hinzufügen, denen Sie dann spezielle Berechtigungen zuweisen. Damit Sie für ein Verzeichnis erweiterte Berechtigungen zuweisen können, müssen Sie entscheiden, wie weit sich diese Berechtigungen auswirken sollen. Dazu wählen Sie aus der Liste *Anwenden auf* in den Eigenschaften eines Eintrags aus, in welchem Bereich sich die speziellen Berechtigungen auswirken sollen:

<i>Nur dieser Ordner</i>	Windows setzt die Berechtigungen nur für diesen Ordner. Die Einstellungen gelten nicht für darin enthaltene Unterordner oder Dateien.
<i>Dieser Ordner, Unterordner und Dateien</i>	Das System wendet die Berechtigungen auf die komplette Verzeichnisstruktur an, auch für alle Verzeichnisse und Dateien unterhalb dieses Verzeichnisses.
<i>Dieser Ordner, Unterordner</i>	Windows setzt die neuen Rechte nur auf dieses Verzeichnis und alle Unterverzeichnisse. Dateien sind davon ausgenommen.
<i>Dieser Ordner, Dateien</i>	Die Berechtigungen gelten nur für dieses Verzeichnis und die darin enthaltenen Dateien.
<i>Nur Unterordner und Dateien</i>	Dieses Verzeichnis ist von der Vergabe der Berechtigungen ausgenommen. Die Rechte gelten nur für die im Verzeichnis enthaltenen Dateien und andere Verzeichnisse.
<i>Nur Unterordner</i>	Nur Unterordner sind betroffen, nicht das Verzeichnis selbst.
<i>Nur Dateien</i>	Nur Dateien werden verwendet, keinerlei Verzeichnisse.

Zunächst werden nur die grundlegenden Berechtigungen angezeigt. Klicken Sie auf den Link *Erweiterte Berechtigungen anzeigen*, um zusätzliche Berechtigungen anzuzeigen. Über die Schaltfläche *Alle löschen* können Sie die Liste der gesetzten Berechtigungen wieder löschen. Auch bei Dateien gibt es eine Unterteilung in grundlegende und erweiterte Berechtigungen.

### Besitz an einer Ressource übernehmen



In einigen Fällen ist es möglich, dass Sie als Administrator nicht die Berechtigung haben, die NTFS-Berechtigungen einer Ressource anzuzeigen oder zu verändern. Dann müssen Sie zunächst den Besitz an der Ressource übernehmen, bevor Sie Berechtigungseinstellungen vornehmen können.

Besitzer eines Objekts ist zunächst derjenige Benutzer, der es erstellt hat. Nur der Besitzer kann die Berechtigungen verändern und so auch Administratoren vom Zugriff ausschließen. Das ist beispielsweise erforderlich für private Benutzerordner. Ein Administrator kann jedoch unabhängig von den vorhandenen Berechtigungen den Besitz an einem Objekt übernehmen und sich anschließend die nötigen Leserechte verschaffen, die zur Anzeige und Änderung der Berechtigungen nötig sind.

- ▶ Klicken Sie in den Dateieigenschaften des Objekts, dessen Besitz Sie übernehmen wollen, im Register *Sicherheit* auf *Erweitert*.
- ▶ Klicken Sie im folgenden Dialogfenster *Erweiterte Sicherheitseinstellungen* auf *Besitzer ändern*.
- ▶ Geben Sie den Namen des neuen Besitzers ein oder suchen Sie unter *Erweitert* nach Benutzerobjekten. Bestätigen Sie Ihre Auswahl mit *Übernehmen* und *OK*.

### Verschlüsselte Dateien freigeben

NTFS bietet die Verschlüsselung von Dateien auf dem Datenträger (**EFS, Encrypting File System**). Unter Windows 10 ist die Freigabe verschlüsselter Dateien für andere Benutzer möglich. Dieser Zugriff muss vom Benutzer für die betreffende Ressource jedem einzelnen berechtigten Benutzer explizit erteilt werden. Der EFS-Treiber greift dann auf diesen Schlüssel im betreffenden (servergespeicherten) Benutzerprofil zu und entschlüsselt damit die freigegebene Datei, bevor sie im Klartext über das Netz übertragen wird.

### Freigaben anzeigen

Freigegebene Ressourcen sind im Explorer von Windows 10 nur als Freigabe zu erkennen, wenn unter *Ansicht* der Detailbereich aktiviert wurde. Im Detailbereich wird angezeigt, für wen der Ordner freigegeben ist.



Sie können alle Freigaben in der Computerverwaltung ansehen und bearbeiten:

- ▶ Klicken Sie im Schnellzugriffsmenü auf *Computerverwaltung*.
- ▶ Wählen Sie *Freigegebene Ordner - Freigaben*, um alle aktiven Freigaben zu sehen.

Im Kontextmenü einer Freigabe können Sie weitere Einstellungen vornehmen.

Um alle Freigaben eines Computers zu sehen, können Sie auch in der Eingabeaufforderung net share eingeben.

Freigabename	Ordnerpfad	Beschreibung
ADMIN\$	C:\Windows	Remoteverwaltung
CS	C:\	Standardfreigabe
<b>Freigabeordner</b>	<b>C:\Freigabeordner</b>	
IPCS		Remote-IPC

Anzeige aller Freigaben in der Computerverwaltung

### Verbogene Freigaben

Alle Freigaben mit angehängtem \$-Zeichen sind in der Netzwerkumgebung unsichtbar. Dies ist bei allen vom System erstellten Freigaben der Fall. Sie können aber auch selbst unsichtbare Freigaben erstellen. Über die Syntax \\<Name des Computers>\<Laufwerksbuchstabe>\$ greifen Sie über das Netzwerk auf diese Freigaben zu.



### Vorherige Dateiversionen in Freigaben

Obwohl Windows 10 die vorherigen Dateiversionen durch den Dateiversionsverlauf (File History) ersetzt hat, kann es als Client auch weiterhin die vorherigen Versionen in Freigaben auf anderen Windows-Systemen nutzen.

## 13.5 Übung

### Mit Zugriffsberechtigungen und Freigaben arbeiten

Übungsdatei: --

Ergebnisdatei: Uebung13\_E.pdf

1. Wie geben Sie einen Ordner frei?
2. Wie verwalten Sie die Freigabeberechtigungen?
3. Wie verwalten Sie die Rechte auf dem Dateisystem (NTFS)?

# 14 Drucker und Druckgeräte

## In diesem Kapitel erfahren Sie

- ✓ was der Unterschied zwischen Drucken und Druckgeräten ist
- ✓ wie Sie Drucker installieren, verwalten und freigeben
- ✓ wie Sie Drucker überwachen
- ✓ wie Sie Probleme beim Drucken beseitigen

## Voraussetzungen

- ✓ Lokale Benutzerverwaltung

## 14.1 Drucken im Netzwerk

In Windows 10 können Sie Drucker, die **Near Field Communication (NFC)** beherrschen, direkt über WLAN erreichen, ohne dass ein Treiber installiert sein muss. Setzen Sie Drucker mit WLAN-Fähigkeit ein, lässt sich Windows 10 einfach mit dem Gerät verbinden, auch ohne NFC.

### Bezeichnungen und Begriffe

Microsoft verwendet seit Jahren die gleiche Bezeichnungsweise rund um das Drucken. Als Systembetreuer sollten Sie diese Windows-Terminologie kennen und durchgehend verwenden, auch wenn viele Benutzer dies nicht tun.

#### Druckgeräte

**Druckgeräte** sind physisch vorhandene **Geräte**, die den eigentlichen Druckvorgang ausführen.

**Netzwerkfähige Druckgeräte** sind eigenständige Druckgeräte, die über eine Netzwerkschnittstelle verfügen. Sie können im Netzwerk direkt angesprochen werden und übernehmen oft die Funktion eines Druckservers mit eigener Druckerwarteschlange. **Lokal angeschlossene Druckgeräte** sind am weitesten verbreitet. Sie werden meist über USB mit dem Computer verbunden.

#### Drucker

**Drucker** sind das, was Sie während der Druckerinstallation erstellen und einrichten und was daraufhin in *Geräte und Drucker* zu sehen ist. Drucker sind **Softwareschnittstellen** zwischen dem Dokument und dem Druckgerät. Der Drucker umfasst alle notwendigen Treiber für ein bestimmtes **Druckgerät** und stellt eine eigene Druckerwarteschlange zur Verfügung.

**Lokale Drucker** sind Drucker, deren Treiber lokal installiert wurden und die eine lokale Druckerwarteschlange zur Verfügung stellen. Wo das dazugehörige Druckgerät steht, ist dabei nebensächlich.

#### Der Spooler-Dienst

**Spooling** ist die englische Bezeichnung für das Zwischenspeichern von Druckaufträgen in einer Spooldatei und die Verteilung der Aufträge an die lokal installierten Drucker. Bei Windows heißt dieser Dienst **Druckerwarteschlange** oder **Spooler**. Der Spooler wertet dabei die Priorität der Drucker aus und gibt den Druckern mit höherer Priorität beim Zugang zum Druckgerät den Vorzug. Dadurch können auch später hinzugefügte wichtige Druckaufträge eher ausgedruckt werden als in der Warteschlange vorhandene Aufträge mit geringerer Priorität. Wenn der Spooler ausfällt oder hängt, kann nicht mehr gedruckt werden.



Wenn ein Ausdruck nicht funktioniert, hilft es oft, wenn Sie in der Dienstesteuerung (*services.msc*) den Systemdienst *Druckwarteschlange* beenden und neu starten. In einer Befehlszeile mit Administratorberechtigungen beenden Sie den Dienst mit *net stop spooler* und starten ihn mit *net start spooler* neu.

### Die Druckerwarteschlange (Queue)

Unter Windows werden Druckaufträge standardmäßig in eine Druckerwarteschlange gestellt, aus der sie vom Drucker an das Druckgerät weitergeleitet werden. Alle auf einem Computer installierten Drucker verfügen über eine eigene Warteschlange, die vom Spooler-Dienst aus dem zentralen Spoolordner gespeist wird. Diese Zwischenspeicherung sorgt dafür, dass Druckaufträge auch dann an einen Drucker gerichtet werden können, wenn das Druckgerät gerade beschäftigt oder ausgeschaltet ist.

### Druckdienste im Netzwerk

Als **Netzwerldrucker** werden Drucker bezeichnet, auf deren Druckerwarteschlange über das Netzwerk zugegriffen werden kann. Die Warteschlange befindet sich dabei nicht auf dem Computer, von dem der Druckauftrag stammt, sondern auf dem Remotecomputer oder im Druckgerät selbst. Es ist unwichtig, auf welche Weise die dazugehörigen Druckgeräte an den Computer angeschlossen sind und an welchem Ort sie sich befinden.

**Druckserver** sind Computer, deren Aufgabe die Bereitstellung von Druckern im Netzwerk ist. Sie sorgen durch ihre zentrale Verwaltung der Druckerwarteschlangen für eine effizientere Nutzung der Druckgeräte. Bei hohem Druckaufkommen wird dabei erhebliche Prozessor-, Festplatten- und Speicherkapazität belegt. Der Druckserver muss stets eingeschaltet sein, um die Druckdienste zur Verfügung zu stellen. Bei Windows-Serverbetriebssystemen ist der Druckserver ein Rollendienst der Serverrolle *Druck- und Dokumentdienste*.

**LPR-Drucker** (Line-Printer-Remote) werden vom System als lokale Drucker behandelt, die Ausgabe wird jedoch auf einen zentralen Druckserver umgeleitet. Sie finden sich vor allem in großen Rechenzentren mit UNIX-Server, auf denen das Server-Gegenstück, der Line Printer Daemon (LPD), läuft.

**Druckerpools** müssten eigentlich Druckgerätepools heißen, denn es handelt sich hier tatsächlich um eine Ansammlung funktionsgleicher Druckgeräte, die über einen einzigen Drucker angesteuert werden.

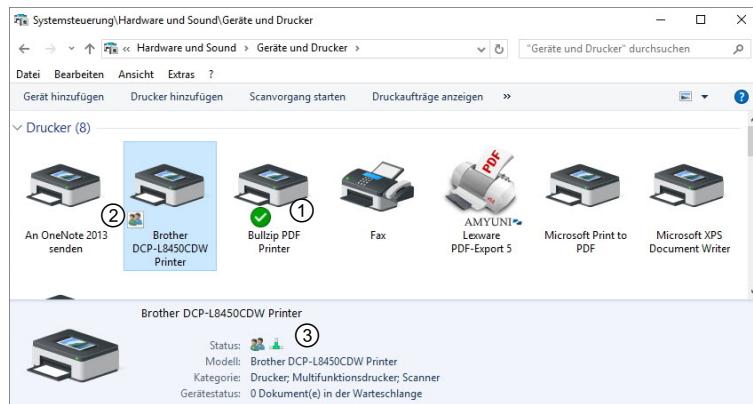
### Zusammenfassung aller Begriffe:

Drucker	Softwareschnittstelle, besteht aus Treibern und Druckerwarteschlange
Druckgerät	Hardware
Netzwerkfähiges Gerät	Druckgerät mit Netzwerkschnittstelle
Lokal angeschlossenes Gerät	Druckgerät wird über USB direkt am Computer angeschlossen
Lokaler Drucker	Drucker mit lokaler Druckerwarteschlange
Spooler	Windows-Dienst zur Verwaltung aller Druckerwarteschlangen
Druckerwarteschlange	Liste der Druckaufträge eines Druckers
Netzwerldrucker	Druckerwarteschlange wird über das Netzwerk freigegeben
Druckserver	Computer, der Druckdienste im Netzwerk bereitstellt
LPR-Drucker	UNIX-Druckerserver zur Ausgabe von Druckaufträgen über das Netzwerk
Druckerpool	Baugleiche Druckgeräte, die über einen Drucker angesprochen werden

## Geräte und Drucker

Im Ordner *Geräte und Drucker* finden Sie Informationen zur Konfiguration und zum Status der verfügbaren Drucker. Jedes Druckersymbol stellt eine Druckerwarteschlange dar und offenbart bestimmte Eigenschaften des Druckers.

- Zeigen Sie alle installierten Drucker an, indem Sie in der Systemsteuerung in der Kategorie *Hardware und Sound* auf *Geräte und Drucker* klicken.



Häkchen im grünen Kreis ①	Für den aktuellen Benutzer wurde dieser Drucker als Standarddrucker definiert.
Icon für mehrere Benutzer neben dem Drucker ②	Der Drucker ist im Netzwerk freigegeben und andere Benutzer können darauf drucken.
Netzwerkkabel unter dem Drucker ③ <Druckername> an <Computername>	Dieser Drucker wurde auf einem anderen Rechner freigegeben und von diesem Rechner wurde eine Verbindung zu ihm aufgebaut. Die Bezeichnung zeigt ebenfalls, dass der Drucker an einem anderen Computer freigegeben wurde.

## 14.2 Drucker installieren

### Lokal angeschlossenes Druckgerät automatisch erkennen und installieren

Alle Druckgeräte der letzten Jahre beherrschen Plug & Play, daher werden sie sofort beim Anschließen erkannt und installiert, wenn ein Treiber vorhanden ist. Sie können diesen Vorgang aber auch manuell ausführen:

- Klicken Sie in *Geräte und Drucker* auf *Geräte und Drucker hinzufügen*.  
Windows sucht daraufhin nach Geräten mit Plug & Play. Wenn ein passender Treiber vorhanden ist, wird er installiert.
- Sollte Windows 10 die Treiber nicht finden, legen Sie die Treiber-CD ein (falls vorhanden) oder suchen Sie auf Ihrem Computer oder im Internet nach dem passenden Treiber.  
Falls es für Windows 10 keine Treiber gibt, suchen Sie nach Treibern für Windows 7/8.1, dann erst nach Vista-Treibern usw. Achten Sie bei der Auswahl des Treibers auf die richtige Windows-Plattform, also x106 (32 Bit) oder x64 (64 Bit). Windows XP-Treiber sind nur noch in Ausnahmefällen verwendbar und sollten nur für nicht kritische Geräte wie Drucker eingesetzt werden. Hier setzen Sie aber möglichst auf interne Treiber.
- Beantworten Sie die weiteren Fragen des Assistenten, wie z. B. nach dem Namen des Druckers und ob dieser auch gleich freigegeben werden soll.  
Sie haben auch die Möglichkeit, eine Testseite drucken zu lassen.
- Stellen Sie den Assistenten fertig.

Der Drucker ist nun fertig eingerichtet und kann benutzt werden. Sie finden das Symbol für den installierten Drucker im Druckerordner. Wenn es sich um den ersten Drucker auf diesem Rechner handelt, wird er automatisch als Standarddrucker festgelegt.

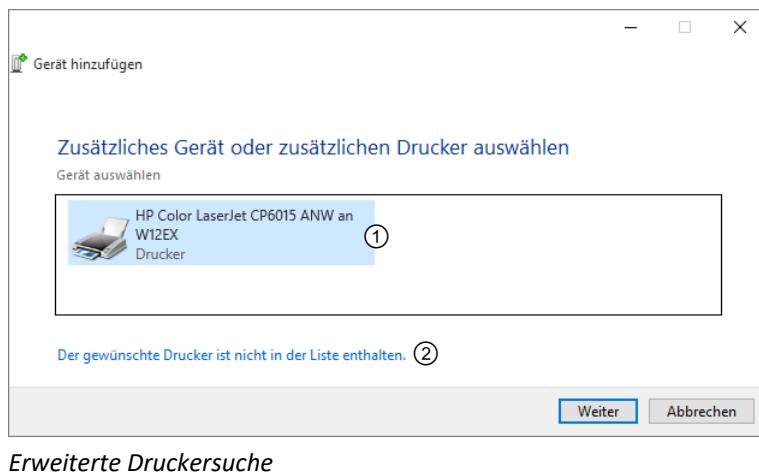


Die Windows-Installation benötigt den Pfad zur INF-Datei. Das bedeutet, dass Sie so gut wie alle Treiber aus dem Internet erst entpacken müssen, da es sich um selbstentpackende Setup-Programme handelt. Bei solchen ausführbaren Dateien ist es einfacher, sie direkt auszuführen und den Windows-Assistenten nicht zu verwenden.

## Lokalen Drucker ohne Plug & Play installieren

Wenn das Druckgerät nicht automatisch erkannt wurde, beherrscht es kein Plug & Play und muss von Hand eingerichtet werden:

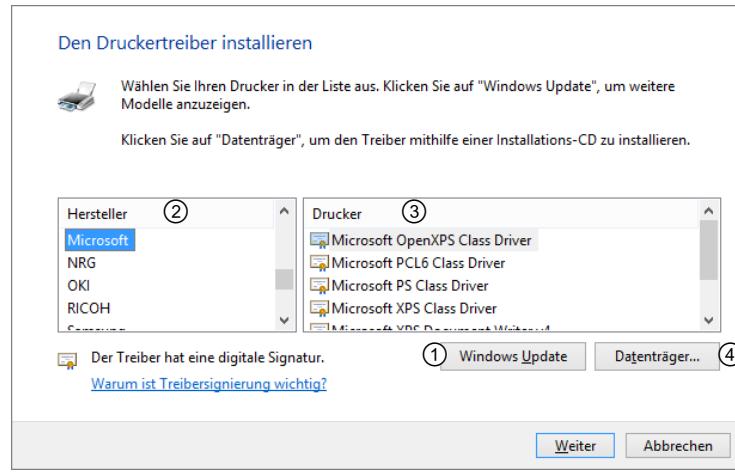
- ▶ Klicken Sie in *Geräte und Drucker* auf *Drucker hinzufügen*.  
Der Assistent sucht nun lokal und im Netzwerk nach verfügbaren Druckern.
- ▶ Wählen Sie den Drucker aus ① und klicken Sie auf *Weiter*.  
Daraufhin öffnet sich der Dialog zur Auswahl des Druckertreibers.
- ▶ Falls der Drucker nicht angezeigt wird, klicken Sie auf *Der gewünschte Drucker ist nicht in der Liste enthalten* ②.  
Es öffnet sich der Dialog *Einen Drucker anhand anderer Optionen suchen*.



## Druckertreiber auswählen und Einrichtung abschließen

Die hier beschriebenen Schritte gelten für die Einrichtung von Druckgeräten, die nicht automatisch erkannt wurden. Hier können Sie manuell den Treiber auswählen und die Druckereinrichtung abschließen.

- ▶ Klicken Sie auf *Windows Update* ①, um die Treiberdatenbank zu aktualisieren.
- ▶ Wählen Sie in der linken Spalte den Hersteller ② und in der rechten den Druckertyp ③ aus.
- ▶ Falls der Treiber nicht aufgeführt ist, klicken Sie auf *Datenträger* ④, um auf Ihrem Computer die INF-Datei des Treibers zu öffnen.
- ▶ Klicken Sie auf *Weiter*.
- ▶ Wählen Sie einen Namen für den Drucker.  
Standardmäßig gibt Windows den Namen des Druckermodells vor.



*Druckerhersteller und Druckertyp auswählen*

Im nächsten Dialogfenster können Sie wählen, ob der Drucker freigegeben werden soll.

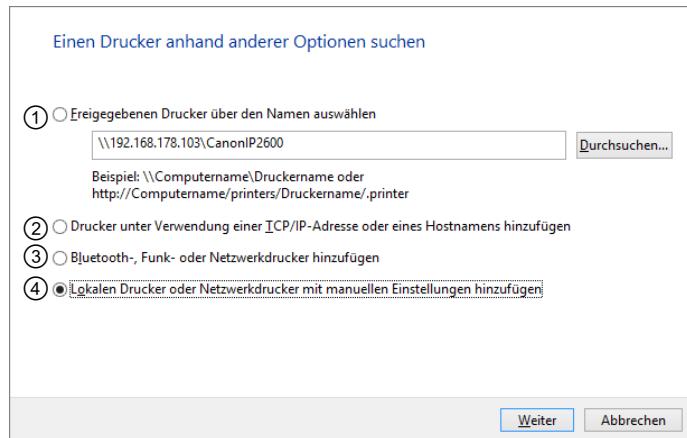
- ▶ Markieren Sie das entsprechende Optionsfeld und geben Sie einen Freigabenamen ein bzw. übernehmen Sie den von Windows vorgeschlagenen Namen.
- ▶ Über ein Optionsfeld können Sie den Drucker zum Standarddrucker für den angemeldeten Benutzer machen.
- ▶ Schließen Sie den Assistenten ab, indem Sie die Schaltfläche *Fertig stellen* betätigen.

## Einen Drucker anhand anderer Optionen suchen

Hier können Sie Drucker einrichten, die nicht automatisch gefunden werden konnten.

Wählen Sie aus, welche Art von Drucker oder Druckgerät Sie einrichten wollen: einen im Netzwerk freigegebenen Drucker ①, einen Netzwerkdrucker bzw. ein netzwerkfähiges Druckgerät mit eigener IP-Adresse ②, ein Plug-&-Play-fähiges Gerät ③ oder einen Drucker, bei dem Sie sämtliche Einstellungen per Hand vornehmen ④.

- Wählen Sie eine Option und klicken Sie auf *Weiter*.



*Art des Druckers auswählen*

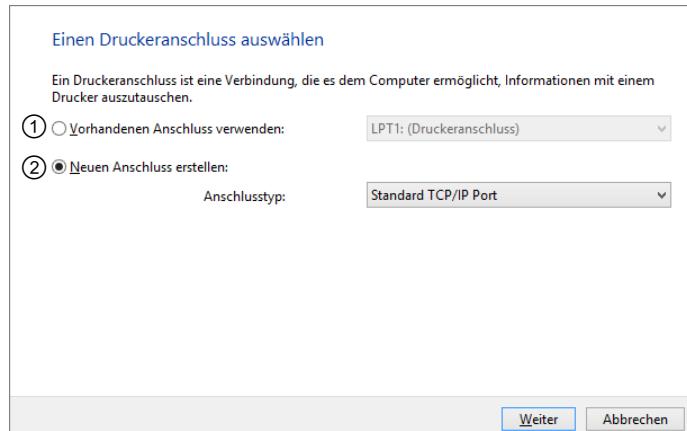
## Druckeranschluss einstellen

Für den neuen Drucker müssen Sie einen bestehenden Druckeranschluss festlegen ① oder einen neuen Anschluss erstellen ②.

- Bei einem lokal angeschlossenen Druckgerät geben Sie den Port an, an dem der Drucker angeschlossen wird.
- Bei einem netzwerkfähigen Druckgerät aktivieren Sie im Feld *Typ* die Einstellung *Standard TCP/IP Port*.

In den darauf folgenden Dialogfenstern können Sie Netzwerkeigenschaften des Druckers, die IP-Adresse und das verwendete Protokoll festlegen.

- Klicken Sie nach Auswahl des Druckeranschlusses auf *Weiter*. Es öffnet sich der Dialog zur Treiberauswahl.



*Druckeranschluss auswählen*

## Drucker freigeben

- Klicken Sie in der Systemsteuerung auf *Geräte und Drucker*.
- Klicken Sie im Kontextmenü des freizugebenden Druckers auf *Druckereigenschaften*.
- Wechseln Sie in das Register *Freigabe*.
- Aktivieren Sie das Optionsfeld *Drucker freigeben* und geben Sie einen Freigabenamen ein.
- Bestätigen Sie Ihre Eingaben mit *OK*.

Nach diesen Maßnahmen steht der Drucker im Netzwerk zur Verfügung. Damit sich dieser auf Clientcomputern verbinden lässt, ist der einfachste Weg, im Explorer die Zeichenfolge `\\PC-Name des Drucker-Hosts\<Name der Druckerfreigabe>` einzugeben. Den Drucker sehen Sie auch im Explorer, wenn Sie auf *Netzwerk* klicken. Ist der Drucker nicht sofort ersichtlich, klicken Sie auf den Namen des Computers, der den Drucker zur Verfügung stellt.



Um die Freigabe wieder zu beenden, deaktivieren Sie das Optionsfeld *Drucker freigeben*.

## Drucker über Heimnetzgruppen verwalten

Druckereinstellungen können Sie über die Einstellungen eines Heimnetzwerkes anpassen, indem Sie im Netzwerk- und Freigabecenter auf den Link *Beigetreten* im Bereich *Heimnetzgruppe* klicken oder eine neue Heimnetzwerkgruppe erstellen. Die Einstellungen können Sie für jedes Mitglied der Heimnetzgruppe ändern.

Sie können z. B. Drucker installieren, die im Netzwerk verfügbar sind. Diese Einstellung gilt dann nur für das entsprechende Mitglied der Gruppe. Möchten Sie den Drucker nicht freigeben, öffnen Sie an dem Computer, an dem der Drucker angeschlossen ist, die Systemsteuerung, Kategorie *Netzwerk und Internet* und wählen *Heimnetzgruppe*.

Hier können Sie über *Für die Heimnetzgruppe freigegebene Elemente ändern* genau einstellen, welche Objekte auf dem PC für andere Computer im Netzwerk verfügbar sein sollen, das gilt auch für Drucker. Diese Einstellungen sind auch für kleine Firmennetzwerke interessant, die über keinen Domänencontroller verfügen.

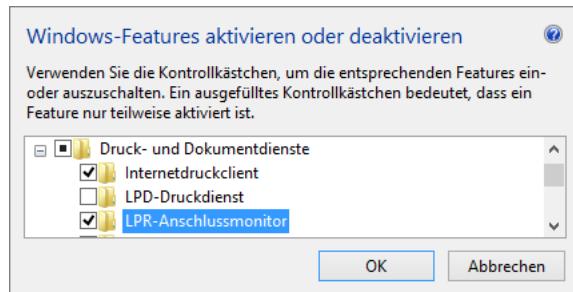


## LPR-Drucker einrichten

Um einen LPR-Drucker (UNIX-Netzwerkdrucker) einrichten zu können, muss die Windows-Funktion **LPR-Anschlussmonitor** installiert werden.



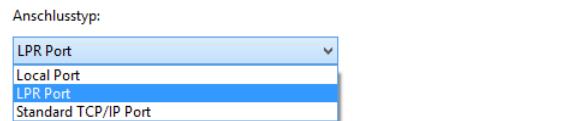
- ▶ Suchen Sie im Suchfeld des Startmenüs nach *optionalfeatures*.  
Alternativ können Sie *Systemsteuerung - Programme und Features - Windows-Funktionen aktivieren oder deaktivieren* aufrufen.
- ▶ Aktivieren Sie unter *Druck- und Dokumentdienste* den *LPR-Anschlussmonitor*.



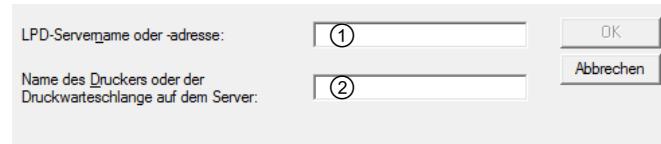
Beginnen Sie die Installation genauso wie für ein lokal angeschlossenes Druckgerät ohne Plug-&-Play-Erkennung.

- ▶ Wählen Sie im Dialogfenster *Einen Druckeranschluss auswählen* das Optionsfeld *neuen Anschluss erstellen* und markieren Sie im Feld *Anschlusstyp* den Eintrag *LPR Port*.
- ▶ Geben Sie den DNS-Namen ① oder die IP-Adresse des Rechners ein, auf dem der Line Printer Daemon (LPD) läuft, und geben Sie den Namen des Druckers oder der Druckerwarteschlange ② ein.
- ▶ Folgen Sie den Anweisungen des Assistenten und schließen Sie die Installation ab.

### LPR-Anschlussmonitor installieren



### Anschlusstyp auf LPR Port einstellen



### LPR-Port konfigurieren

## Druckerpool einrichten

Wenn Sie mehrere identische Druckgeräte lokal an einen Druckserver anschließen, können Sie diese über einen einzigen Drucker ansprechen, indem Sie die Funktion *Druckerpool* aktivieren. Wenn nun mehrere Aufträge an diesen Drucker geschickt werden, vergibt der Druckserver den ersten Auftrag an das erste freie Druckgerät, den nächsten Auftrag an das nächste freie Gerät und so weiter.

- ▶ Öffnen Sie *Geräte und Drucker*.
- ▶ Installieren Sie den Drucker.
- ▶ Klicken Sie nach Abschluss der Installation im Kontextmenü dieses Druckers auf *Druckereigenschaften*.
- ▶ Wechseln Sie in das Register *Anschlüsse* und aktivieren Sie das Kontrollfeld *Druckerpool aktivieren*.

- ▶ Nun können Sie in der Spalte *Anschluss* alle Ports auswählen, an denen die baugleichen Druckgeräte angeschlossen sind.
- ▶ Bestätigen Sie Ihre Eingabe mit *Übernehmen* und *OK*.



Oft können nicht nur baugleiche, sondern auch ähnliche Geräte eines Herstellers in einem Pool vereint werden, wenn Sie den Treiber bzw. Funktionsumfang des „kleinsten“ Gerätes verwenden.

## 14.3 Drucker konfigurieren

### Druckerverwaltungskonsole

Sie können die installierten Drucker und Druckertreiber z. B. über die spezielle Druckerverwaltungskonsole verwalten. Geben Sie auf der Startseite `printmanagement.msc` ein, um die Konsole zu starten. Diese Konsole ist nur in den Editionen Pro und Enterprise von Windows 10 integriert.

### Senden-an-Menü um Drucken erweitern

Über das Kontextmenü von Dateien und Ordnern erreichen Sie den Befehl *Senden an*. Wenn Sie dem Senden-an-Menü die Verknüpfung eines Druckers hinzufügen, können Sie Dateien über das Senden-an-Menü auch ausdrucken.

- ▶ Geben Sie den Befehl `shell:PrintersFolder` auf der Startseite ein und bestätigen Sie mit der -Taste.
- Der Ordner *Drucker* wird geöffnet.
- ▶ Öffnen Sie parallel den Ordner *sendto* mit dem Befehl `shell:sendto`.
- ▶ Ziehen Sie über Drag & Drop den gewünschten Drucker aus dem Ordner *Drucker* in den Ordner *sendto*.



Sie haben in Windows 10 die Möglichkeit, die Verknüpfungen des Senden-an-Menüs zu bearbeiten. Geben Sie dazu `shell:sendto` auf der Startseite ein und bestätigen Sie mit der -Taste. Erstellen Sie in diesem Ordner Verknüpfungen, die Sie benötigen, oder löschen Sie Verknüpfungen, die Sie nicht benötigen.

### Standarddrucker festlegen

- ▶ Öffnen Sie den Geräte- und Druckerordner.
- ▶ Klicken Sie mit der rechten Maustaste auf den Drucker, den Sie als Standarddrucker festlegen möchten, und wählen Sie im Kontextmenü den Menüpunkt *Als Standarddrucker festlegen*.

### Standarddruckereinstellungen für alle Benutzer definieren

Für alle Benutzer kann eine Standard-Druckkonfiguration festgelegt werden.

- ▶ Öffnen Sie *Geräte und Drucker* und wählen Sie im Kontextmenü des Druckers, den Sie bearbeiten möchten, den Menüpunkt *Druckeinstellungen*.
- ▶ Klicken Sie im Register *Erweitert* auf *Standardwerte*.  
Im folgenden Dialog können Sie die Einstellungen für die Orientierung des Ausdrucks, für die Seitenreihenfolge und die Anzahl der Seiten pro Blatt festlegen.  
Es besteht auch die Möglichkeit, den Einzugsschacht des Druckgeräts oder die Papierart zu bestimmen.



Achten Sie darauf, keine Einstellungen (z. B. zusätzliches Papierfach oder Duplexeinheit) zu aktivieren, die am Druckgerät gar nicht vorhanden sind.

### Standarddruckeinstellungen für einen Benutzer definieren

Jeder Benutzer kann eine eigene Standard-Druckkonfiguration festlegen, die die vom System vorgegebenen Standardwerte überschreibt. Im Gegenzug überschreiben alle Anwendungseinstellungen beim Drucken die Standard-Druckkonfiguration des Benutzers.

Um diese Einstellung vorzunehmen, muss der betreffende Benutzer angemeldet sein.

- ▶ Bitten Sie den Benutzer, dessen Druckeinstellungen Sie ändern wollen, sich anzumelden.
- ▶ Öffnen Sie *Geräte und Drucker* und wählen Sie im Kontextmenü des Druckers, den Sie bearbeiten möchten, den Menüpunkt *Druckeinstellungen*.
- ▶ Klicken Sie im Register *Allgemein* auf *Einstellungen*.

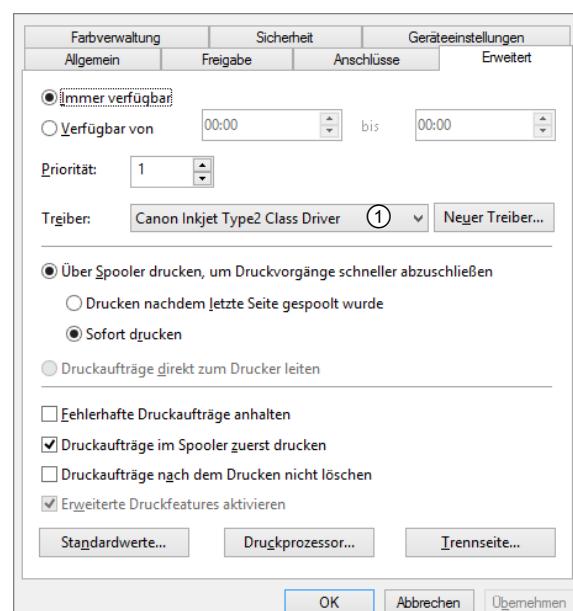
Im folgenden Dialog können Sie die Einstellungen für die Orientierung des Ausdrucks, für die Seitenreihenfolge und die Anzahl der Seiten pro Blatt für den Benutzer festlegen.

### Druckertreiber für den lokalen Drucker aktualisieren

- ▶ Öffnen Sie im Kontextmenü des Druckers den Menüpunkt *Druckereigenschaften*.
- ▶ Wechseln Sie in das Register *Erweitert*.

Der aktuell verwendete Druckertreiber wird im Feld *Treiber* ① angezeigt. Er kann folgendermaßen aktualisiert werden:

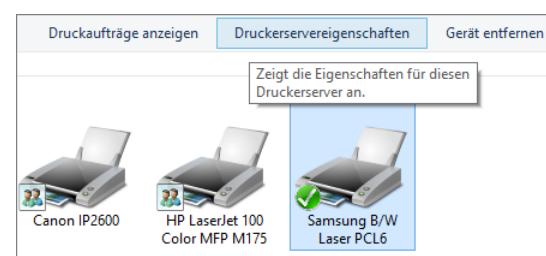
- ▶ Betätigen Sie die Schaltfläche *Neuer Treiber*. Windows 10 öffnet einen Assistenten für die Druckertreiberinstallation.
- ▶ Klicken Sie in einem der folgenden Dialogfenster auf *Datenträger* und wählen Sie den Speicherort der INF-Datei des neuen Druckertreibers aus.
- ▶ Folgen Sie den Anweisungen des Assistenten.



Druckertreiber aktualisieren

### Druckertreiber für den Druckserver aktualisieren

- ▶ Öffnen Sie den Geräte- und Druckerordner und klicken Sie zuerst auf einen installierten Drucker, dann auf *Druckervereigenschaften*.
- ▶ Wählen Sie das Register *Treiber*.



Druckervereigenschaften bearbeiten

### Druckertreiber für andere Betriebssysteme hinzufügen

Es ist unter Windows 10 möglich, für freigegebene Drucker die Treiber für andere Windows-Versionen und Plattformen zentral verfügbar zu machen und so den Clients im Bedarfsfall die Installation der Treiber vom Druckerverserver aus zu ermöglichen.

Treiber können für Windows XP, Vista, 7 und 10 in 32 Bit oder 64 Bit hinterlegt werden.

- ▶ Klicken Sie auf *Hinzufügen* ①.
- Windows 10 startet den Assistenten für die Druckertreiberinstallation.
- ▶ Aktivieren Sie die Kontrollfelder der Prozessorenplattformen x106 und x64, für die Sie Treiber zur Verfügung stellen wollen.
- ▶ Wählen Sie den passenden Treiber aus wie bei einer normalen Treiberinstallation.
- ▶ Wiederholen Sie den Vorgang, falls Sie beide Plattformen angewählt haben.
- ▶ Schließen Sie die Installation der Druckertreiber mit einem Klick auf *Fertig stellen* ab.

Windows wird Sie gegebenenfalls nach Datenträgern fragen, auf denen sich die Druckertreiber befinden. Geben Sie hier den Pfad zur INF-Datei an. Gegebenenfalls müssen Sie dazu das Treiberpaket entpacken.

Auf einem x64-System können Sie die Windows-Treiber für x106 von einem 32-Bit-Windows-Installationsmedium entnehmen und umgekehrt.



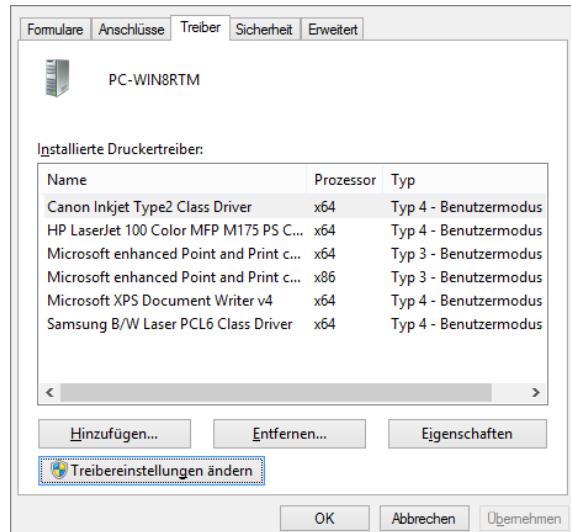
Die Druckerbezeichnung muss in den INF-Dateien für x106 und x64 identisch sein, sonst erkennt Windows nicht, dass es sich um denselben Drucker handelt. Ändern Sie gegebenenfalls die Bezeichnung.

### Standortunabhängiges Drucken

Standortunabhängiges Drucken ermöglicht durch die Standorterkennung über die Netzwerk-ID, dass Druckaufträge automatisch an den nächstgelegenen Drucker gesendet werden. Dieses Feature ist nur bei Mobilgeräten und erst ab Windows 10 Pro verfügbar.

Wenn die Funktion aktiv ist, erscheint im Geräte- und Druckerordner ein zusätzlicher Menüpunkt *Standarddrucker verwalten*.

Sie können mithilfe dieses Menüs entscheiden, welcher Drucker für Ihr Notebook der Standarddrucker sein soll, abhängig davon, in welchem Netzwerk Sie sich gerade aufhalten.



*Auf dem Druckserver installierte Treiber*

## 14.4 Druckerwarteschlange verwalten

### Druckerwarteschlange konfigurieren

Alle eingehenden Druckaufträge werden als Datei im Spoolordner abgelegt. Sobald die Spooldatei erstellt ist, kann die Anwendung, die den Ausdruck angefordert hat, wieder benutzt werden. Die Ausgabe des Druckauftrags an den Drucker erfolgt im Hintergrund, während der Benutzer schon wieder mit der Anwendung arbeitet. Der Spooler-Dienst ordnet sie den jeweiligen Druckerwarteschlangen zu und sortiert die Aufträge nach ihrer Priorität.

Druckaufträge können auch dann in die Druckerwarteschlange gestellt werden, wenn das Druckgerät nicht angeschlossen, nicht eingeschaltet oder deaktiviert (offline) ist. Wenn Sie den Drucker in den Eigenschaften der Druckerwarteschlange auf *Offline* geschaltet haben, werden die Druckaufträge gespeichert und in dem Moment ausgeführt, sobald Sie ihn wieder als online festgelegt haben.

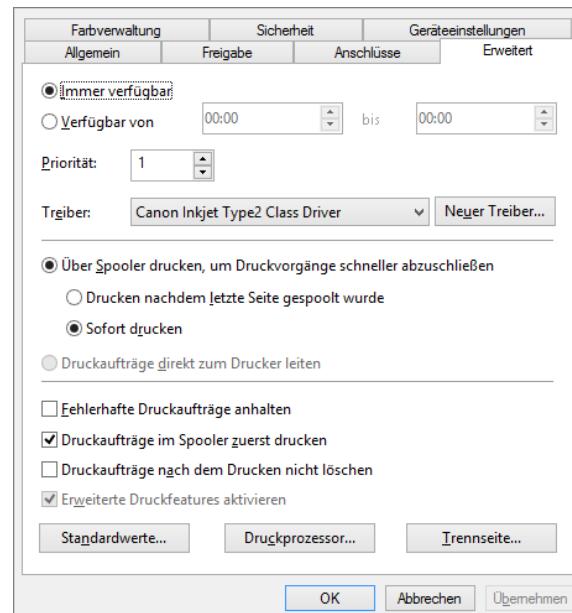
## Druckerwarteschlange beeinflussen

Die Standardeinstellungen von Windows 10 für die Druckerwarteschlangen sind für die meisten Anforderungen geeignet und müssen nicht geändert werden. Sie können jedoch für jeden installierten Drucker detaillierte Einstellungen vornehmen:

- ▶ Klicken Sie im Kontextmenü des Druckers, den Sie bearbeiten möchten, auf *Druckereigenschaften*.
- ▶ Wechseln Sie in das Register *Erweitert*.

Hier können Sie z. B. folgende Einstellungen vornehmen:

- ✓ Verfügbarkeit und Priorität des Druckers,
- ✓ Drucken sofort starten oder erst nachdem die letzte Seite gespoolt wurde (kann das Spooling beschleunigen),
- ✓ Druckaufträge direkt an den Drucker leiten (schaltet die Druckerwarteschlange ab und umgeht den Spooler),
- ✓ Druckaufträge nach dem Drucken nicht löschen,
- ✓ Druckprozessor ändern,
- ✓ Trennseite zwischen Druckaufträgen einfügen und einstellen.



Einstellungen der Druckerwarteschlange

## Spoolordner verschieben

Wenn ein Druckserver regelmäßig große Datenmengen zu verarbeiten hat, kann es sinnvoll sein, den Spoolordner auf ein anderes Laufwerk mit viel freiem Speicherplatz zu verschieben. Diese Einstellung betrifft alle installierten Drucker.

- ▶ Markieren Sie im Gerät- und Druckerordner einen beliebigen Drucker und klicken Sie auf *Druckerserver-eigenschaften*.
- ▶ Klicken Sie im Register *Erweitert* auf *Erweiterte Einstellungen* ändern.
- ▶ Geben Sie im Feld einen anderen Pfad für den Spoolordner ein.

## 14.5 Druckaufträge verwalten

### Status von Druckaufträgen einsehen

- ▶ Klicken Sie im Gerät- und Druckerordner doppelt auf den entsprechenden Drucker.
- oder Klicken Sie doppelt auf das Druckersymbol neben der Uhrzeitanzeige in der Taskleiste.

Das Druckersymbol in der Taskleiste wird nur bei ausstehenden Druckaufträgen angezeigt. Bei mehreren Druckerwarteschlangen wird für jede aktuell verwendete Druckerwarteschlange ein eigenes Fenster geöffnet.

In der Spalte *Status* ① wird angezeigt, ob das Dokument gerade gedruckt wird, ob der Ausdruck des Dokuments angehalten wurde oder ob es gerade in die Warteschlange geladen wird.

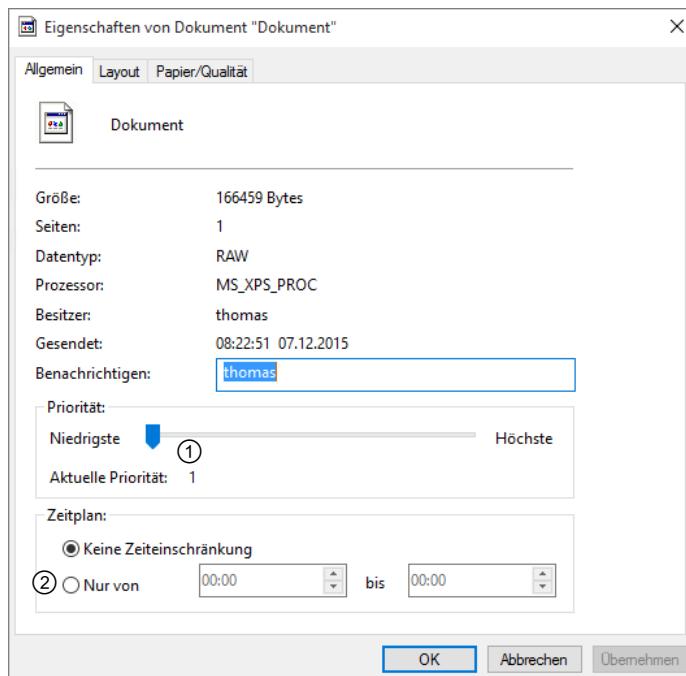
Drucker	Dokument	Ansicht				
Dokumentname	Status	①	Besitzer	Seiten	Größe	Gesendet
■ Dokument	Fehler - Wird gedruckt		thomas	1	162 KB	08:22:51 07.12.2015
< 1 Dokument(e) in der Warteschlange						

Die geöffnete Druckerwarteschlange

## Priorität und Zeitplan von Druckaufträgen verändern

Wenn es im Drucker nicht anders konfiguriert wurde, erhalten standardmäßig alle Druckaufträge innerhalb einer Druckerwarteschlange die geringste Priorität (1) und werden in Ein- gangsreihenfolge bearbeitet.

- ▶ Öffnen Sie die Druckerwarteschlange.
- ▶ Wählen Sie im Kontextmenü eines Dokuments den Menüpunkt *Eigenschaften*.
- ▶ Wechseln Sie in das Register *Allgemein*. Sie können die Priorität des Druckauftrags mit dem Schieberegler ① verändern. Aufträge mit höherer Priorität werden zuerst ausgedruckt.
- ▶ Um den Zeitplan des Druckauftrags zu ändern, aktivieren Sie das Optionsfeld ② und geben Sie einen Zeitraum ein, in dem der Druckauftrag ausgeführt werden soll.



## Drucker und die PowerShell

Über die PowerShell können Sie z. B. Ausgaben von Cmdlets, beliebige Texte, Informationen und Inhalte von Textdateien drucken.

Sie möchten ...	
die Ausgabe von Cmdlets drucken	<ul style="list-style-type: none"> <li>▶ Übergeben Sie die Ausgabe von Cmdlets mit der Option <code>  Out-Printer</code> an das Cmdlet <code>Out-Printer</code>. Die PowerShell gibt die Ausgabe auf dem Standarddrucker aus. Den Drucker können Sie auch in Anführungszeichen und die Bezeichnung in der Druckersteuerung angeben.</li> </ul>
beliebige Texte drucken	<ul style="list-style-type: none"> <li>▶ Geben Sie den Befehl <code>&lt;Text&gt;   out-printer</code> ein.</li> </ul>
beliebige Texte auf einem bestimmten Netzwerldrucker ausgeben	<ul style="list-style-type: none"> <li>▶ Geben Sie den Befehl <code>&lt;Text&gt;"   out-printer -name \\&lt;Druckserver&gt;\&lt;Freigegebener Drucker&gt;</code> ein.</li> </ul>
eine Liste aller aktuell gestarteten Prozesse drucken	<ul style="list-style-type: none"> <li>▶ Geben Sie den Befehl <code>get-process   out-printer</code> ein.</li> </ul>
den Inhalt von Textdateien direkt auf Druckern ausgeben	<ul style="list-style-type: none"> <li>▶ Geben Sie den Befehl <code>get-content &lt;Datei&gt;   Out-Printer</code> ein.</li> </ul>

## Druckerinformationen

Mit dem CmdLet `Get-WmiObject` können Sie Druckerinformationen auslesen. Verwenden Sie dazu folgende Erweiterungen:

Erweiterung	Information
<code>Win32_Printer</code>	Druckerwarteschlangen
<code>Win32_PrintJob</code>	Druckjobs

Erweiterung	Information
Win32_PrinterDriver	alle Treiber, die installiert sind
Win32_TCPIPPrinterPort	IP-Ports
Win32_PrinterConfiguration	Druckerkonfiguration
Win32_PrinterSetting	Druckerinformationen zu allen Druckern
Win32_PrinterShare	Freigaben der Drucker
Win32_PrinterDriverDll	installierte DLLs

Auf diesem Weg erhalten Sie schnell wichtige Informationen zu den Druckern, den Warteschlangen und den installierten Treibern und Konfigurationen.

Um sich eine Liste der installierten Drucker anzuzeigen, verwenden Sie in der PowerShell in Windows 10 das CMDlet Get-Printer. Sie erhalten ausführliche Informationen, z. B. zum Treiber und Status des Druckers. Wollen Sie zum Beispiel eine Druckerliste anzeigen, die Standort, Name und Status anzeigt, verwenden Sie:

`Get-Printer | fl Name, Location, PrinterStatus.`



### Drucker mit der PowerShell einstellen

Sie können die Einstellungen von Druckern in der PowerShell anpassen. Dazu verwenden Sie das CMDlet Set-PrinterConfiguration.

Über die PowerShell können Sie auch direkt auf die Druckaufträge der einzelnen Drucker zugreifen. So lassen sich die Aufträge z. B. anhalten, fortsetzen und löschen. Auf Wunsch können Sie auch für alle Drucker alle Aufträge anzeigen und diese filtern:

`Get-Printer | Get-PrintJob | fl`



## 14.6 Berechtigungen und Gruppen verwalten

### Standard-Berechtigungen für das Drucken und für Drucker

Sie können im Zusammenhang mit dem Drucken bestimmten Gruppen Berechtigungen erteilen und verweigern. Dazu gehören insbesondere die Berechtigungen zum Drucken, zur Verwaltung des Druckers und zur Verwaltung einzelner Dokumente in der Druckerwarteschlange.

Die Standardeinstellungen sind wie folgt:

Gruppe	Drucken	Drucker verwalten	Dokumente verwalten
Administratoren	X	X	X
ERSTELLER-BESITZER			X
Jeder	X		

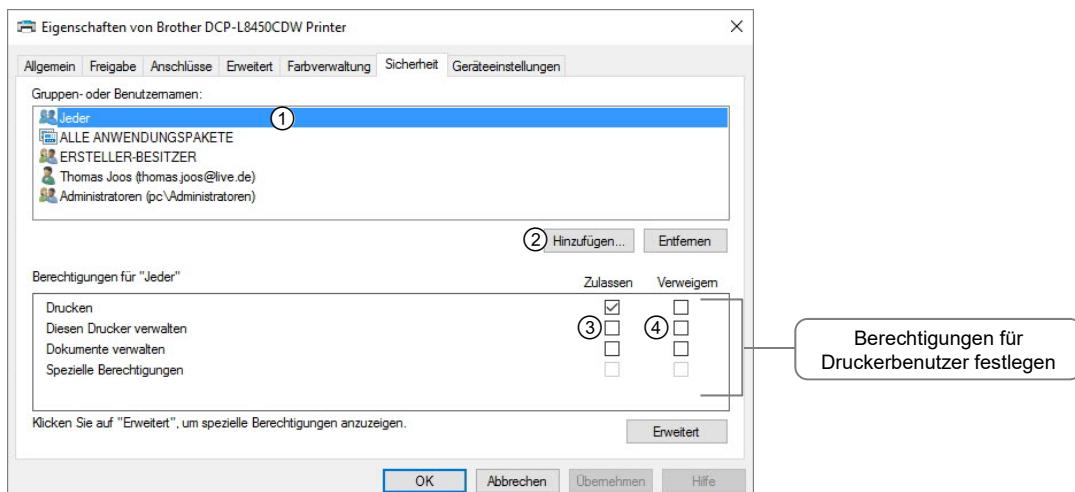
Durch diese Einstellungen kann ein Benutzer, der einen Druckauftrag in die Druckerwarteschlange gestellt hat und somit Mitglied der Gruppe **ERSTELLER-BESITZER** geworden ist, seinen eigenen Druckauftrag verwalten. Administratoren können auch Druckaufträge anderer Personen verwalten.

- Wechseln Sie in den Druckereigenschaften des Druckers, für den Sie die Berechtigungen anpassen möchten, in das Register *Sicherheit*.

Hier können Sie durch Markieren der einzelnen Benutzergruppen deren Berechtigungen einsehen ①.

### Gruppen hinzufügen

- Klicken Sie auf *Hinzufügen* ② und fügen Sie der Liste neue Benutzer oder Gruppen hinzu.
- Passen Sie anschließend die Berechtigungen an, indem Sie die Kontrollfelder für *Zulassen* ③ bzw. für *Verweigern* ④ aktivieren.
- Bestätigen Sie Ihre Eingaben mit *OK*.



Sie können Gruppen oder Personen die Berechtigung zum Drucken nehmen, indem Sie sie aus der Liste entfernen oder indem Sie ihnen die Berechtigung verweigern. Durch das Verweigern der Berechtigung werden die betroffenen Personen explizit vom Zugriff auf den Drucker ausgeschlossen, unabhängig davon, in welcher Gruppe sie sich befinden.

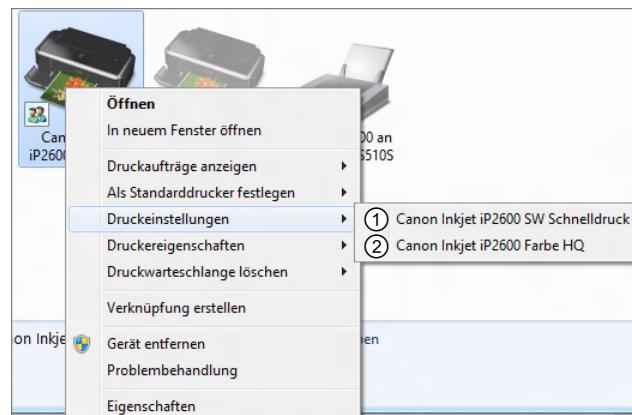
## 14.7 Mehrere Druckerwarteschlangen verwalten

### Mehrere Drucker für ein Druckgerät nutzen

Es kann sinnvoll sein, mehrere Drucker (Druckerwarteschlangen) für ein physisches Druckgerät einzurichten. Auf einer Workstation könnten den verschiedenen Druckern z. B. unterschiedliche Druckformate zugewiesen werden. Auf einem Druckserver könnte durch unterschiedliche Prioritäten und Druckberechtigungen für die einzelnen Drucker gesteuert werden, wer zuerst auf dem Druckgerät drucken darf. So können eilige Briefe über den Drucker mit hoher Priorität sofort ausgedruckt werden, während die Broschüre mit 200 Seiten auf dem Drucker mit niedriger Priorität wartet, bis keine anderen Druckaufträge mehr vorliegen.

**Beispiel:** Durch das manuelle Hinzufügen von zwei Druckern mit demselben Treiber haben Sie nun zwei Drucker: einmal für Schnelldruck in Schwarz-Weiß ① mit Priorität 10 und einmal für Farbdruck ② mit Priorität 1. Beide Drucker greifen auf das gleiche Druckgerät zu. Das Druckgerät ist wegen Wartungsarbeiten momentan noch ausgeschaltet. In beiden Druckerwarteschlangen befindet sich jeweils mindestens ein Dokument.

Wenn das Druckgerät wieder eingeschaltet wird, wird wegen der höheren Priorität zuerst der Druckauftrag in Schwarz-Weiß ausgeführt.



Beispiel: zwei Druckerwarteschlangen

## 14.8 Probleme beim Drucken beheben

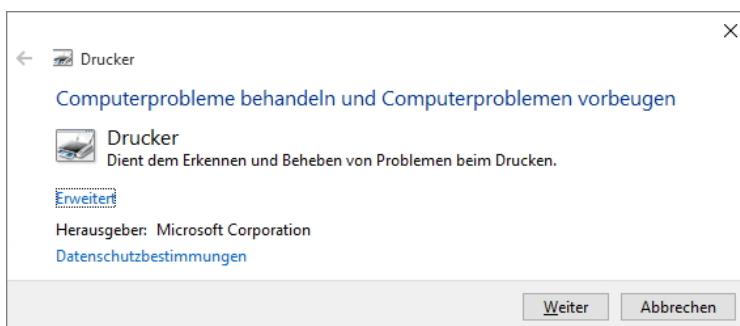
### Assistent zur Drucker-Problembeseitigung

Windows 10 bietet bei Druckproblemen Hilfe in Form eines Assistenten an. Dieser Assistent versucht, Probleme rund ums Drucken zu erkennen und zu benennen, zu beseitigen oder Lösungshinweise zu geben.

#### Assistent zur Drucker-Problembeseitigung starten

- Geben Sie druckprobleme ↵ ein, um den Assistenten zu starten.
- Wählen Sie den problematischen Drucker aus und starten Sie die Überprüfung mit Weiter.
- Folgen Sie den Anweisungen am Bildschirm.

Wenn das Problem nicht erkannt und keine Lösung gefunden werden konnte, bietet der Assistent unter *Zusätzliche Optionen durchsuchen* weiterführende Links zum Thema.



## 14.9 Übung

### Drucker einstellen

Übungsdatei: --

Ergebnisdatei: Uebung14\_E.pdf

1. Wie geben Sie einen Drucker frei?
2. Wie ändern Sie den Standarddrucker?

# 15 Datenträgerverwaltung

## In diesem Kapitel erfahren Sie

- ✓ den Unterschied zwischen einem Basisdatenträger und einem dynamischen Datenträger
- ✓ wie Sie Partitionen, logische Laufwerke und Volumes anlegen
- ✓ wie Sie Datenträgerkontingente einrichten und verwalten können
- ✓ wie Sie die BitLocker-Verschlüsselung verwenden

## Voraussetzungen

- ✓ Unterschiedliche Dateisysteme unter Windows 10 kennen

## 15.1 Datenträger und Volumes

### Grundlagen zu Datenträgern und Volumes

Datenträger sind alle Speichermedien, auf denen Daten dauerhaft abgelegt werden können, z. B. magnetische Festplatten oder Flashspeicher wie Solid-State-Disks (SSD) oder USB-Sticks. Im Gegensatz dazu stehen flüchtige Speichermedien, auf denen gespeicherte Daten mit Abschalten der Betriebsspannung verloren gehen, wie der Hauptspeicher (RAM, Random Access Memory), Grafikkartenspeicher oder Cache-Speicher auf Prozessoren. Auf Datenträgern können Volumes eingerichtet werden; diese können mit einem Dateisystem formatiert werden und sind dann über Laufwerkbuchstaben oder -pfade ansprechbar.

Ein Volume kann in der Ordnerstruktur bereitgestellt (**gemountet**) werden. Das bedeutet, dass ihm kein Laufwerkbuchstabe zugeordnet wird, sondern dass es in einem beliebigen leeren Ordner innerhalb eines anderen NTFS-formatierten Volumes eingehängt werden kann. Dieser Ordner wird dann als Bereitstellungspunkt bezeichnet. Der Benutzer bemerkt das Mounten allenfalls an einem geänderten Ordnersymbol, ansonsten ist der Vorgang transparent.

### Basisdatenträger und Basisvolumes

Die klassisch eingerichtete Standardfestplatte ist unter Windows ein Basisdatenträger. Jeder Basisdatenträger kann bis zu vier primäre Partitionen enthalten. Da Bootinformationen im sogenannten **Master Boot Record (MBR)** liegen, wird dieser Datenträgertyp unter Windows 10 auch als MBR-Datenträger bezeichnet. Sind mehr als vier Partitionen auf einem Basisdatenträger erwünscht, kann eine primäre Partition durch eine erweiterte Partition ersetzt werden, die wiederum in beliebig viele logische Laufwerke unterteilt werden kann. Folglich können maximal drei primäre Partitionen und eine erweiterte Partition eingerichtet werden.

Partitionen und logische Laufwerke werden auch **Basisvolumes** genannt. Um ein Basisvolume verwenden zu können, muss es formatiert und ihm ein Laufwerkbuchstabe oder -pfad zugeordnet werden.

### GPT-Datenträger

Das Datenträgerpartitionsformat MBR (**Master Boot Record**) unterstützt Volumes mit einer Größe von bis zu zwei Terabytes und bis zu vier Primärpartitionen pro Datenträger (oder drei Primärpartitionen, eine erweiterte Partition und eine unbegrenzte Anzahl logischer Laufwerke).

Im Vergleich dazu unterstützt das Partitionsformat **GPT (GUID-Partitionstabelle)** Volumes mit einer Größe von bis zu 110 Exabytes und bis zu 1210 Partitionen pro Datenträger. Anders als bei Datenträgern mit dem MBR-Partitionsformat werden Daten, die für den Betrieb der Plattform zwingend erforderlich sind, in Partitionen abgelegt und nicht in Sektoren ohne Partition oder in versteckten Sektoren.

Außerdem besitzen Datenträger mit dem GPT-Partitionsformat redundante Primär- und Sicherungspartitionstabellen, wodurch die Integrität der Partitionsdatenstruktur verbessert wird. Auf GPT-Datenträgern können Sie dieselben Aufgaben wie auf MBR-Datenträger durchführen. Die Konvertierung eines MBR-Datenträgers in einen GPT-Datenträger und umgekehrt kann nur durchgeführt werden, wenn der Datenträger leer ist. Die Umwandlung nehmen Sie über das Kontextmenü des Datenträgers auf der linken Seite in der Datenträgerverwaltung vor.

Wenn Sie die Eigenschaften des Datenträgers in der Datenträgerverwaltung (`diskmgmt.msc`) aufrufen, finden Sie den Partitionierungsstil auf der Registerkarte *Volumes*. In der PowerShell können Sie den Partitionierungsstil mit `Get-Disk | Select FriendlyName, PartitionStyle` anzeigen.

Sie können auf diesem Weg eine Festplatte auch offline oder online schalten. Dazu zeigen Sie mit `Get-Disk` zunächst die Festplatten im System an. Anschließend schalten Sie die Festplatte mit dem folgenden Befehl online:



```
Set-Disk <Nummer> -isOffline $false.
```

Den Partitionierungsstil legen Sie dann mit dem folgenden Befehl auf GPT fest:

```
Initialize-Disk <Nummer> -PartitionStyle GPT.
```

Ein weiteres Beispiel, um mit der PowerShell einen Datenträger zu erstellen und zu formatieren, ist:

```
Get-Disk 1 | Clear-Disk -RemoveData  
New-Partition -DiskNumber 1 -UseMaximumSize -IsActive -DriveLetter Z |  
Format-Volume -FileSystem NTFS -NewFileSystemLabel Data.
```

## Dynamische Datenträger und dynamische Volumes

Dynamische Datenträger erweitern die Möglichkeiten, den Speicherplatz von Datenträgern einzuteilen und zur Verfügung zu stellen. Basisdatenträger können in dynamische Datenträger umgewandelt werden. Alle Basisvolumes auf diesem Datenträger werden dann zu dynamischen Volumes.

Dynamische Datenträger können eine unbegrenzte Anzahl von dynamischen Volumes enthalten und funktionieren wie die primären Partitionen, die auf Basisdatenträgern verwendet werden. Der Hauptunterschied zwischen Basisdatenträgern und dynamischen Datenträgern besteht darin, dass dynamische Datenträger Daten zwischen zwei oder mehreren dynamischen Festplatten eines Computers freigeben und Daten auf mehrere Festplatten verteilen können. Beispielsweise kann sich der Speicherplatz eines einzelnen dynamischen Volumes auf zwei separaten Festplatten befinden. Zudem können dynamische Datenträger Daten zwischen zwei oder mehreren Festplatten duplizieren, um dem Ausfall einer einzelnen Festplatte vorzubeugen. Diese Fähigkeit erfordert mehr Festplatten, erhöht jedoch die Zuverlässigkeit.

Um einen vorhandenen Basisdatenträger in einen dynamischen Datenträger umzuwandeln, müssen Sie im unteren Bereich der Datenträgerverwaltung beim Eintrag der Festplatte über das Kontextmenü den Befehl *In dynamischen Datenträger umwandeln* aufrufen. Es wird ein Dialogfeld angezeigt, in dem Sie die zu aktualisierenden Basisfestplatten auswählen können. Es können in einem Schritt alle noch vorhandenen Basisfestplatten in einem System aktualisiert werden.

## Datenträger im RAID-Verbund

Ein weitverbreiteter Begriff beim Zusammenschluss von mehreren Datenträgern ist **RAID**, das Redundant Array of Independent Disks, ein redundanter Verbund von Festplatten. Es gibt verschiedene RAID-Level, die anzeigen, wie die Festplatten verbunden sind und welche Datenausfallsicherheit gegeben ist. Außerdem wird zwischen Software-RAID (wie unter Windows), Host-RAID (günstiger RAID-Controller auf dem Motherboard) und Hardware-RAID (professionelle Variante mit leistungsfähigem Controller) unterschieden.



Unter Windows 10 lassen sich Festplatten zu RAID 0 (Stripeset) und RAID 1 (gespiegeltes Volume) zusammenschließen. RAID 5 ist im Menü sichtbar, kann jedoch nicht angewählt werden. RAID 5 können nur mit einer Windows-Server-Version erstellt werden. Sie können allerdings bei Windows 10 mit den Speicherplätzen virtuelle Volumes einrichten, die **weitgehend** einem RAID 5 entsprechen.

Windows 10 unterstützt vier Arten dynamischer Volumes:

<b>Einfache Volumes</b>	Einfache Volumes können um nicht zugeordneten Speicherplatz auf einem Datenträger erweitert werden. Befindet sich dieser hinzugefügte Platz auf demselben Datenträger, ist das Ergebnis wieder ein einfaches Volume.
<b>Übergreifende Volumes</b>	Hier handelt es sich um einfache Volumes, die um nicht zugeordneten Speicherplatz auf anderen Datenträgern erweitert wurden. <b>Vorteil:</b> Dateien, die größer sind als einzelne Datenträger, werden möglich. <b>Nachteil:</b> Fällt einer der Datenträger aus, ist das ganze Volume unlesbar.
<b>Stripesetvolumes</b>	Ein Stripesetvolume besteht aus maximal 32 einzelnen Speicherbereichen gleicher Größe. Für ein Stripeset kann jeweils nur ein freier Speicherbereich pro Datenträger verwendet werden. Stripesets können nicht erweitert werden und werden auch mit RAID 0 (Redundant Array of Independent Disks) bezeichnet. Die 0 wurde gewählt, weil so ein Verbund eben <b>nicht</b> redundant ist. <b>Vorteil:</b> Erhöhung der Lese- und Schreibgeschwindigkeit durch gleichzeitige Zugriffe auf mehrere Datenträger <b>Nachteil:</b> Fällt einer der Datenträger aus, ist das ganze Volume unlesbar.
<b>Gespiegeltes Volume</b>	Ein gespiegeltes Volume besteht aus maximal 32 einzelnen Speicherbereichen gleicher Größe. Für einen Spiegelsatz kann jeweils nur ein freier Speicherbereich pro Datenträger verwendet werden. Spiegelsätze können nicht erweitert werden. Durch das doppelte Vorhandensein der Daten ist dieser Festplattenverbund redundant, daher wird er mit RAID 1 bezeichnet. <b>Vorteil:</b> Erhöhung der Datensicherheit durch gleichzeitiges Schreiben und Lesen identischer Daten von allen Datenträgern <b>Nachteil:</b> Höhere Kosten für Datenträger ohne Speicherplatzzuwachs, Performanceverlust durch notwendige Vergleichsoperationen

Ein dynamischer Datenträger wird von der Datenträgerverwaltung verwaltet und kann ohne Neustart aus einem Basisdatenträger konvertiert werden. Er ist dann aber nur noch von Betriebssystemen ab Windows 2000 lesbar. Auch die Rückkonvertierung ist im laufenden Betrieb möglich, dabei dürfen allerdings keine Volumes auf dem dynamischen Datenträger liegen. Sie müssen alle Volumes löschen. Inzwischen sind jedoch einige Tools von Drittanbietern verfügbar, die damit beworben werden, dass sie ohne Datenverlust in der Lage sind, dynamische Datenträger in Basisdatenträger zurückzukonvertieren.



System- und Startvolumes können weder erweitert werden noch Teil eines Stripesets sein.

## 15.2 Datenträger und Volumes einrichten

### Voraussetzungen

Bei der Installation von Windows 10 stehen nur Basisdatenträger und -volumes (oder GPT-Datenträger, sollte die verwendete Festplatte größer als 2 TB sein) zur Verfügung. Die Funktionalitäten zum Erzeugen und Verwalten dynamischer Datenträger und Volumes sowie GPT-Datenträger können erst unter Windows 10 selbst zur Verfügung gestellt werden, da erst mit dem Betriebssystem die entsprechenden Dienste gestartet werden. Die Verwaltungsschnittstelle für die Datenträgerwartung und -konfiguration ist die Datenträgerverwaltungskonsole in der MMC (Microsoft Management Console).

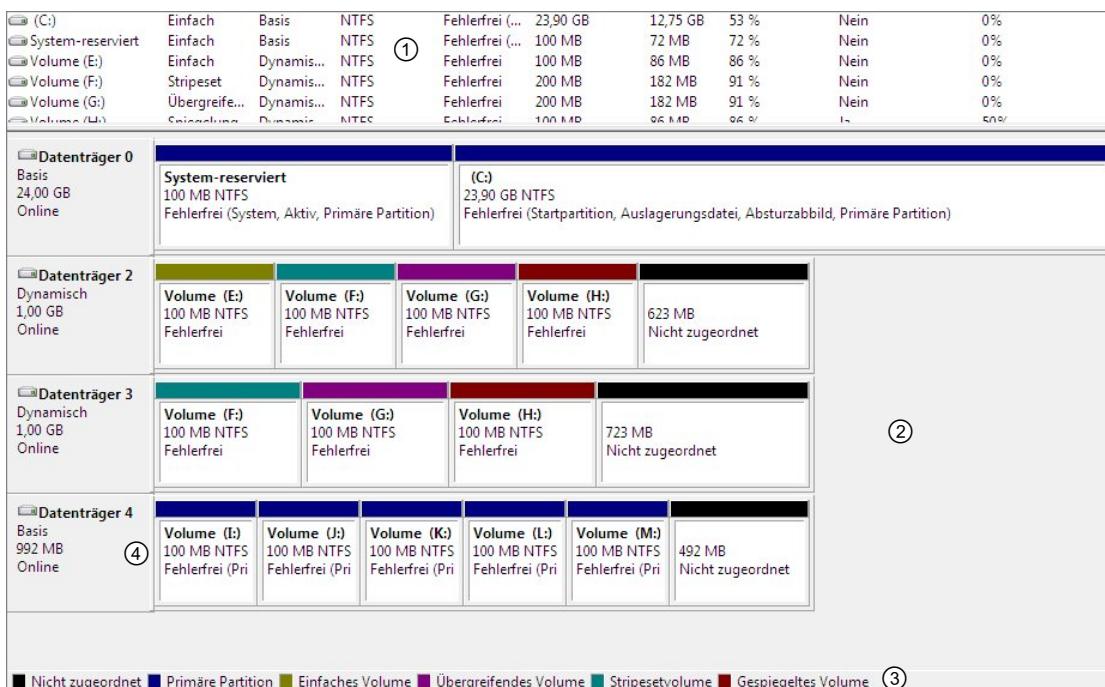
### Festplattenzugriffe im Gerät-Manager beschleunigen

Standardmäßig aktiviert Windows 10 automatisch den Zwischenspeicher für den schnellen Zugriff auf die SSD. Sie sollten die Aktivierung nachprüfen.

- ▶ Rufen Sie devmgmt.msc über die Startseite auf, um den Gerät-Manager zu starten.
  - ▶ Öffnen Sie das Eigenschaftenfenster der Festplatte, zum Beispiel einer SSD im Gerät-Manager, und wechseln Sie zur Registerkarte *Richtlinien*.
- Stellen Sie sicher, dass das Kontrollkästchen *Schreibcache auf dem Gerät aktivieren* eingeschaltet ist.

### Datenträgerverwaltungskonsole starten

- ▶ Klicken Sie im Schnellzugriffsmenü auf *Datenträgerverwaltung*.  
Sie können auch im Startmenü diskmgmt.msc eingeben, um das MMC-Snap-In *Datenträgerverwaltung* zu öffnen.



### MMC-Snap-In Datenträgerverwaltung

Die Datenträgerverwaltungskonsole ist zweigeteilt, wobei im oberen Textfeld ① detaillierte Informationen zu den Volumes aufgelistet und im unteren Textfeld ② die Datenträger grafisch dargestellt werden. Die Legende der Farbschlüssel wird unten ③ erklärt.



Wenn Sie sich in der obigen Abbildung Datenträger 4 genauer betrachten, so werden Sie feststellen, dass auf diesem 5 primäre Partitionen ④ existieren – bei MBR-Datenträgern eine Unmöglichkeit. Datenträger 4 wurde zu einem GPT-Datenträger konvertiert, um 5 primäre Partitionen darauf anlegen zu können.

Sie können die Eigenschaften der Darstellung im Menü *Ansicht* anpassen. Dabei gibt es die Möglichkeit, den oberen und den unteren Bereich der Konsole getrennt zu verwalten.

### Datenträger hinzufügen

- ▶ Verbinden Sie den neuen Datenträger mit dem Computer und starten Sie das System.  
Wenn Sie die Datenträgerverwaltungskonsole aufrufen, werden Sie automatisch mit dem Assistenten zum Initialisieren und Konvertieren von Datenträgern verbunden, falls die Festplatte noch nie initialisiert wurde.
- ▶ Klicken Sie auf *Weiter*, um zum Datenträgerauswahlmenü zu gelangen.  
Hier können Sie den Datenträger auswählen, den Sie initialisieren möchten, und entscheiden, ob es ein MBR- oder GPT-Datenträger werden soll.
- ▶ Klicken Sie auf *Weiter* und gehen Sie identisch vor, wenn Sie den neuen Datenträger gleich in einen dynamischen konvertieren möchten.  
Nun wird Ihnen eine Übersicht der von Ihnen vorgenommenen Einstellungen gezeigt. Bestätigen Sie die Einstellungen, indem Sie auf *Fertig stellen* klicken.

Der Datenträger ist damit initialisiert und kann weiter eingerichtet werden.

### Basisdatenträger umwandeln

Eine Konvertierung eines Basisdatenträgers von GPT nach MBR und umgekehrt ist nur möglich, wenn noch keine Volumes darauf vorhanden sind.

- ▶ Klicken Sie mit der rechten Maustaste auf den Datenträger, den Sie umwandeln möchten.
- ▶ Wählen Sie den Datenträgertyp aus, in den Sie den Datenträger umwandeln wollen.
- ▶ Bestätigen Sie Ihre Auswahl mit *OK*.  
Der Datenträger wird nun konvertiert.



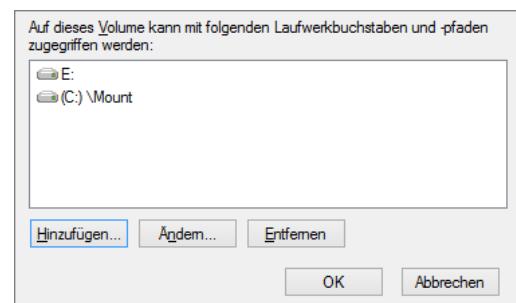
*Datenträger konvertieren*

### Bestehendes Volume in leerem NTFS-Ordner bereitstellen (Mounten)

Bei der Einrichtung eines neuen Volumes können Sie wählen, ob Sie einen Laufwerkbuchstaben oder einen Pfad zuweisen möchten. Sie können aber auch bestehende Volumes nachträglich mounten:

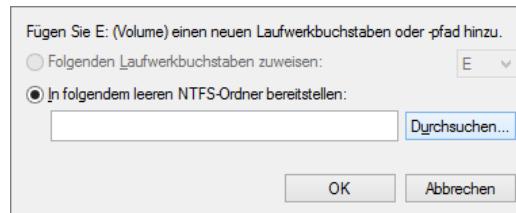
- ▶ Öffnen Sie die Datenträgerverwaltung über das Schnellzugriffsmenü.
- ▶ Klicken Sie im Kontextmenü eines Volumes auf *Laufwerkbuchstaben und -pfade ändern*.

Im Dialog *Laufwerkbuchstaben und Pfade ändern* können Sie auswählen, ob Sie einen Laufwerkbuchstaben oder Pfad hinzufügen, den bestehenden ändern oder entfernen wollen.



*Volume im Dateisystem mounten*

- ▶ Klicken Sie auf *Hinzufügen*, um ein bestehendes Volume mit Laufwerkbuchstaben zusätzlich in einem leeren Ordner bereitzustellen.
- ▶ Wählen Sie als Bereitstellungspunkt einen leeren Ordner aus.
- ▶ Bestätigen Sie mit *OK*.



*Bereitstellungspunkt wurde ausgewählt*

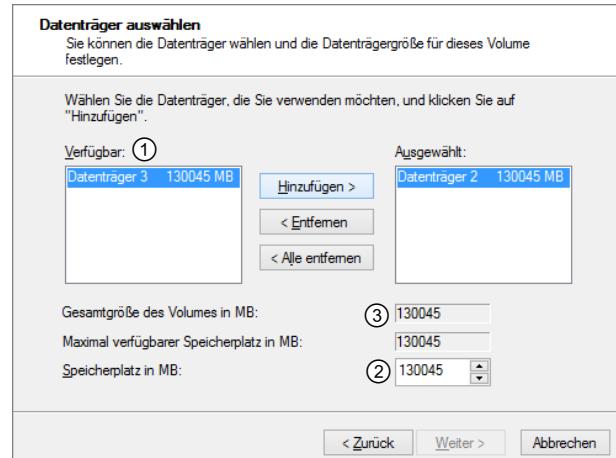
### Volume erstellen

Im Folgenden wird mithilfe des Assistenten zum Erstellen neuer Volumes ein Stripesetvolume erstellt. Alle anderen Volumetypen können Sie auf die gleiche Weise erstellen, es sind aber dann nicht alle Einstellungen des folgenden Beispiels möglich bzw. nötig.

Falls Sie Basisvolumes erstellen möchten, wird der Assistent zum Erstellen von Partitionen gestartet. Dieser wurde im Wesentlichen von den älteren Windows-Versionen übernommen und verwendet deshalb noch die alten Bezeichnungen für Basisvolumes, nämlich primäre und erweiterte Partition und logisches Laufwerk.

Wenn Sie auf einem Datenträger ein Stripesetvolume erstellen wollen, gehen Sie folgendermaßen vor:

- ▶ Klicken Sie mit der rechten Maustaste auf den freien Bereich des Datenträgers und wählen Sie *Neues Stripesetvolume*. Ein Assistent öffnet sich.
- ▶ Klicken Sie auf *Weiter*.
- ▶ Wählen Sie im Auswahlfeld *Verfügbar* ① die Datenträger aus, die am Stripeset teilnehmen sollen, und klicken Sie auf *Hinzufügen*.
- ▶ Geben Sie nun im Textfeld *Speicherplatz in MB* ② die Größe der einzelnen Stripes an. Voreingestellt ist die *Gesamtgröße des Volumes in MB* ③. Klicken Sie anschließend auf *Weiter*.
- ▶ Wählen Sie im nächsten Dialog einen Laufwerkbuchstaben oder einen Pfad in der Ordnerstruktur und klicken Sie auf *Weiter*.

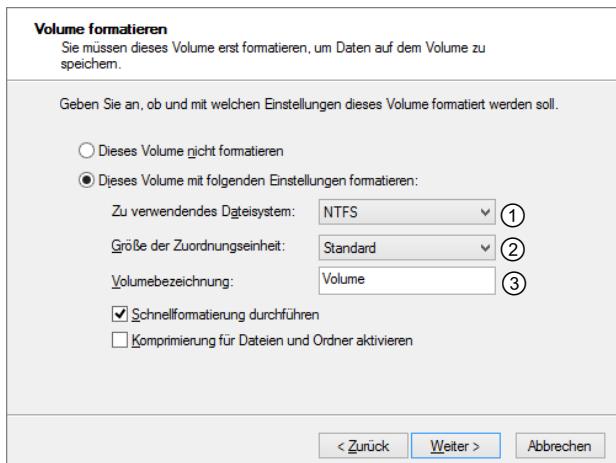


*Neues Stripeset (RAID 0) einrichten*

### Volume formatieren

- ▶ Wählen Sie nun, ob und wie Sie dieses Volume formatieren wollen.

Dazu sehen Sie zwei Felder, in denen Sie das Format ① und die Größe der Zuordnungseinheiten ② (Cluster) festlegen können. Weiterhin können Sie dem Volume eine Bezeichnung ③ zuweisen und in den Kontrollfeldern festlegen, ob Sie die Formatierung mit Schnellformatierung durchführen wollen und ob die Komprimierung für Dateien und Ordner aktiviert werden soll.



*Formatieroptionen des Assistenten*

Auch wenn die Festplatten immer größer werden, haben viele Anwender das Problem, dass der Platz irgendwann knapp wird. Windows 10 bietet die Funktion, Ordner auf der Festplatte zu komprimieren. Der Vorteil ist, dass Sie auf die Daten wie gewohnt zugreifen können, diese aber deutlich weniger Platz auf der Festplatte belegen.

Dateien, mit denen Sie ständig arbeiten, sollten Sie nicht komprimieren, da der Zugriff auf diese Daten etwas langsamer sein kann. Archive oder Verzeichnisse mit Bildern im BMP-Format, auf die Sie nicht häufig zugreifen, lassen sich deutlich verkleinern.

Die Funktion steht nur auf NTFS-Datenträgern zur Verfügung. Die Platzersparnis können Sie in den Eigenschaften des Ordners leicht nachprüfen. Dort werden auf der Registerkarte *Allgemein* die originale Größe und der tatsächliche Plattenverbrauch angezeigt.

Die Komprimierung lässt sich jederzeit wieder deaktivieren. Bereits komprimierte Dateien wie MP3s, JPG-Dateien oder bereits komprimierte Archive wie ZIP-Dateien profitieren nicht von der Komprimierung und werden nicht weiter verkleinert. Werden neue Dateien in bereits komprimierte Ordner verschoben, müssen sie gegebenenfalls nachträglich komprimiert werden, da die Funktion nicht automatisch auf neue Dateien überprüft.

Sie erhalten anschließend noch einmal eine Übersicht der von Ihnen zusammengestellten Daten und können den Prozess durch Betätigen der Schaltfläche *Fertig stellen* starten.



Benötigen Sie schnellstmöglichen Datenzugriff, ist es empfehlenswert, gleichartige Festplatten in einem Stripe-set (RAID 0) zu verwenden, da sonst eine langsamere Platte das gesamte System herunterbremst. Beachten Sie jedoch, dass bei einem Ausfall einer einzigen Platte alle Daten verloren sind. Mit jedem zusätzlichen Datenträger im RAID steigt die Ausfallwahrscheinlichkeit exponentiell an!

Die standardmäßig vorgegebene Volumebezeichnung ist *Volume*.

### Volumes löschen

- ▶ Klicken Sie mit der rechten Maustaste auf das Volume, das Sie löschen möchten, und wählen Sie aus dem Kontextmenü *Volume löschen*.
- ▶ Sie werden nun gewarnt, dass Sie ein Volume eines bestimmten Typs löschen, und können dies mit *Ja* bestätigen.  
Damit ist das Volume gelöscht und der Speicherplatz auf dem Datenträger wieder verfügbar.

## 15.3 Volumes verwalten

### Volume auf Fehler überprüfen

Sie sollten diese Maßnahme nach Möglichkeit zu einer Zeit durchführen, wenn keine anderen Benutzer auf das Volume zugreifen müssen, da es während der Überprüfung für den alleinigen Zugriff gesperrt wird. Für die Überprüfung benötigen Sie Administratorrechte.

- ▶ Klicken Sie im Schnellzugriffs menü auf *Eingabeaufforderung (Administrator)*, um die Eingabeaufforderung zu öffnen.
- ▶ Geben Sie `chkdsk <Volume> /v` ein, um ein Volume zu überprüfen. Ersetzen Sie dabei `<Volume>` durch den entsprechenden Laufwerkbuchstaben oder -pfad.
- ▶ Sollen Fehler behoben werden, geben Sie zusätzlich die Option `/f` an.  
Zur Ausführung von chkdsk muss das zu prüfende Volume gesperrt werden.
- ▶ Ist eine Prüfung der Datenträgeroberfläche gewünscht, geben Sie außerdem die Option `/r` an.

Beachten Sie, dass in einem Volume bereitgestellte andere Volumes nicht mitgeprüft werden.

Falls das Volume nicht für den alleinigen Zugriff gesperrt werden kann, erhalten Sie eine Meldung, dass nicht sofort überprüft werden kann. Nun können Sie bestimmen, ob die Überprüfung beim nächsten Start des Computers vorgenommen werden soll.

Die Ausführung von `chkdsk` beim Systemstart wird in der Ereignisanzeige im Anwendungsprotokoll als Information der Quelle *Winlogon* protokolliert.



## Größe eines Volumes ändern

Windows 10 bietet bei einigen Datenträgertypen und Volumetypen die Möglichkeit, die Größe eines Volumes nachträglich zu ändern.

- ▶ Klicken Sie rechts auf das Volume, dessen Größe Sie ändern wollen.
- ▶ Wählen Sie aus, ob Sie das Volume erweitern (vergrößern) oder verkleinern wollen.
- ▶ Geben Sie im Assistenten die gewünschte Größenänderung an.

Bei Verkleinerungen berechnet Windows 10 für Sie automatisch die maximal mögliche Verkleinerung.

Bei Vergrößerungen können Sie auswählen, welcher unpartitionierte Bereich des Datenträgers dem Volume zugeordnet werden soll.

- ▶ In einigen Fällen muss der Datenträger vor der Größenänderung in einen dynamischen Datenträger umgewandelt werden. Bestätigen Sie diese Umwandlung.
- ▶ Bestätigen Sie Ihre Eingaben im Assistenten und lassen Sie Windows die Konvertierung abschließen.



*Verkleinern eines Laufwerks*

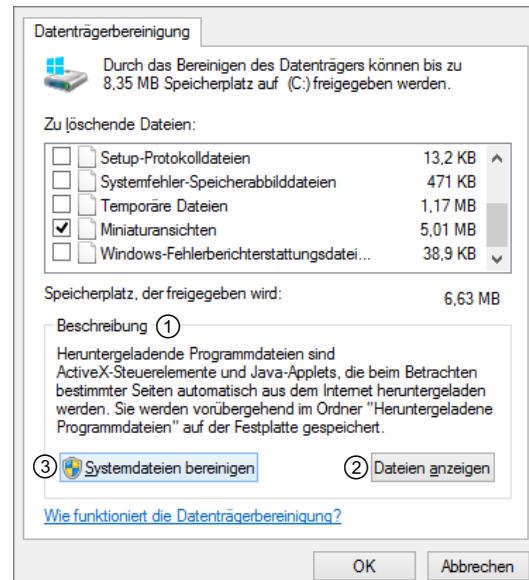
## Volume bereinigen

Wenn der freie Speicherplatz auf einem Volume knapp wird, empfiehlt es sich, nicht mehr benötigte Dateien zu löschen und selten genutzte Dateien zu komprimieren. Die Suche nach und das Löschen von solchen Dateien lässt sich mit der Datenträgerbereinigung vereinfachen.

- ▶ Öffnen Sie den Datei-Explorer oder die Datenträgerverwaltungskonsole.
- ▶ Klicken Sie in den Eigenschaften des Volumes im Register *Allgemein* auf *Bereinigen*.
- Es wird berechnet, wie viel Speicherplatz durch das Bereinigen freigegeben werden kann. Anschließend gelangen Sie zum Dialogfenster *Bereinigen des Datenträgers*.
- ▶ Wählen Sie im Register *Datenträgerbereinigung* im Feld die Dateigruppen aus, die Sie löschen möchten.

Unter ① erhalten Sie eine Beschreibung der Kategorie, bei *Dateien anzeigen* ② können Sie sich die Dateien aus der aktuellen Kategorie anzeigen lassen.

Wenn Sie auf *Systemdateien bereinigen* ③ klicken, wird erneut überprüft, welche Dateien gelöscht werden können. Anschließend verfügt der Datenträgerbereinigungs-Dialog über die zusätzliche Registerkarte *Weitere Optionen*, auf der Sie nicht mehr benötigte Windows-Komponenten und Programme entfernen und bis auf den letzten Wiederherstellungspunkt alle Punkte löschen können.



*Bereinigen eines Volumes*

- Bestätigen Sie Ihre Auswahl mit *OK* oder verlassen Sie das Dialogfenster mit *Abbrechen*.



Wenn Sie auf diese Art und Weise Dateien löschen, sind diese nicht mehr im Papierkorb und können ohne vorherige Sicherung nicht wiederhergestellt werden.

## Laufwerke optimieren

Durch Kopier- und Löschgänge werden im Dateisystem des Volumes Lücken erzeugt, die dann bei neuen Schreibzugriffen mit Teilen von anderen Dateien beschrieben werden. Dadurch entsteht die sogenannte **Dateifragmentierung**. Bei starker Fragmentierung können die Dateien nicht im Stück gelesen oder geschrieben werden und bei herkömmlichen magnetischen Festplatten muss der Lesekopf häufig bewegt werden. Dadurch werden Zugriffe auf fragmentierte Dateien immer langsamer. Bei Festplatten hilft hier die Defragmentierung, um die einzelnen Dateifragmente wieder zusammenzuführen.

Bei modernen **Solid State Disks (SSD)** ist keine Defragmentierung nötig. Sie ist im Gegenteil eher schädlich und wird deshalb für SSDs auch automatisch deaktiviert. (Auch wenn zunächst eine Defragmentierung angeboten werden sollte, wechselt die Anzeige auf *Optimierung nicht verfügbar*, sobald die Defragmentierung gestartet wird.)

Unter Windows 10 heißt die Defragmentierung **Optimierung** und einige Bezeichnungen gegenüber älteren Windows-Versionen sind geändert. So wird nicht mehr der Grad der Fragmentierung angezeigt, sondern die Speicherplatzeffizienz. Liegt diese bei 100 %, ist das Laufwerk zu 0 % fragmentiert.

Die Optimierung findet automatisch wöchentlich statt, Sie können den Defragmentierungsvorgang jedoch auch manuell starten.

- Klicken Sie im Datei-Explorer oder in der Datenträgerverwaltung im Kontextmenü eines Volumes auf *Eigenschaften*. Klicken Sie im Register *Tools* auf *Optimieren*.
- oder*
- Geben Sie `defrag` ein. Wählen Sie *Festplatte defragmentieren*.
  - Betätigen Sie `[Strg]` und wählen Sie die Laufwerke aus.  
Sie können die Laufwerke erst untersuchen ① oder sofort optimieren lassen ②.
  - Um den Zeitplan zu ändern und Laufwerke für die automatische Optimierung auszuwählen, klicken Sie auf *Einstellungen ändern* ③.

Durch die Optimierung der Laufwerke können Sie eine effizientere Ausführung des Computers erreichen. Sie können die Laufwerke auch analysieren, um festzustellen, ob sie optimiert werden müssen. Es werden nur Laufwerke auf dem Computer bzw. die damit verbundenen Laufwerke angezeigt.

Laufwerk	Medientyp	Zuletzt ausgeführt	Aktueller Status
(C:)	Für schlanke Speicherzu...	13.09.2012 14:49	OK (100% Speicherplatzeffizienz)
Volume (E: C:\Mo...)	Für schlanke Speicherzu...	Noch nie ausgeführt	OK
Volume (F:)	Solid-State-Laufwerk	Noch nie ausgeführt	Optimierung nicht verfügbar
System-reserviert	Für schlanke Speicherzu...	13.09.2012 14:49	OK (100% Speicherplatzeffizienz)

①     ②

**Geplante Optimierung**

**Ein**  
Die Laufwerke werden automatisch optimiert.  
Häufigkeit: wöchentlich

③

Defragmentierungskonsole eines Volumes

## Virtuelle Volumes

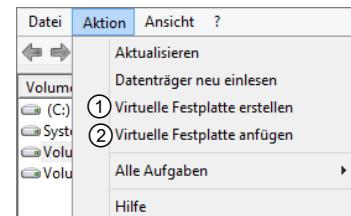
Windows 10 kann mit virtuellen Festplatten so arbeiten, als wären diese real im Computer angeschlossene Geräte. Dabei wird das von Virtual PC bekannte VHD-Dateiformat (**Virtual Hard Disk**) verwendet oder das erweiterte Nachfolgeformat VHDx (extended), das auch bei Hyper-V eingesetzt wird.

Den Assistenten zum Erstellen virtueller Festplatten starten Sie in der Datenträgerverwaltung im Menü **Aktion - Virtuelle Festplatte erstellen** ①. Im Assistenten beantworten Sie dann Fragen nach der Größe und dem Speicherort der VHD-Dateien und legen die Art und Weise fest, wie die Datei angelegt werden soll.

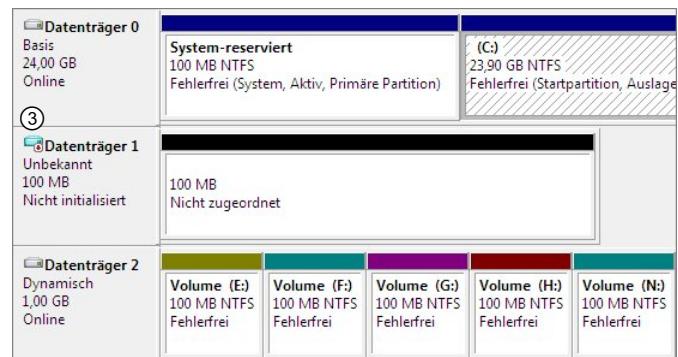
Sie haben auch die Möglichkeit, bereits existierende Dateien auf diese Weise in Ihrem System verfügbar zu machen. Sie können dazu im Menü **Aktion** auf **Virtuelle Festplatte anfügen** ② klicken.

Mit einem virtuellen Datenträger ist es nach dessen Erstellung möglich, genauso zu arbeiten, als wäre dies eine reale Festplatte. In der Datenträgerverwaltung erkennen Sie den Unterschied lediglich am türkisfarbenen Festplatten-Symbol  ③.

Am roten Pfeil erkennen Sie, dass die virtuelle Festplatte noch initialisiert werden muss.



*Virtuelle Festplatte erstellen*



*Virtueller Datenträger in der Verwaltungsoberfläche*

Die Möglichkeit, virtuelle Datenträger wie reale zu nutzen, eröffnet neue Wege, den Anwendern Daten zur Verfügung zu stellen und sie leichter zu verteilen. Besonders interessant ist darüber hinaus die Fähigkeit von Windows 10, direkt aus einer virtuellen Festplatte heraus in ein dort installiertes Windows 10 zu booten. Dieses Feature ist ab der Professional-Edition verfügbar.

## 15.4 Kontingente zuweisen

### Einsatzmöglichkeiten von Kontingenzen

NTFS-Volumes ermöglichen die Zuweisung von Datenträgerkontingenzen (Diskquotas), bei denen der Speicherplatz, der den Benutzern zur Verfügung steht, beschränkt wird. Dies kann vor allem auf zentral zugänglichen Volumes ein Überlaufen des Volumes verhindern. Auf diese Weise kann vermieden werden, dass ein Benutzer durch Unwissenheit oder mit Absicht den gesamten freien Speicherplatz eines Volumes für sich beansprucht und allen anderen Benutzern damit den Zugriff auf das Volume unmöglich macht.

Sollte auf dem Startvolume nicht mehr ausreichend Platz für die Auslagerungsdatei des Betriebssystems sein, besteht die Gefahr, dass das Betriebssystem instabil wird. Dieser Überlauf des Startvolumes wird durch entsprechend dimensionierte Benutzerkontingente unmöglich gemacht. Bedeutung hat dies vor allem, wenn die Ordner *Programme* und *Dokumente* und *Einstellungen* auf dem Startvolume belassen werden (Standard-einstellung).



NTFS-Kontingente sind weniger flexibel als Benutzerkontingente, die auf einem Dateiserver eingerichtet werden, und in dem neuen Dateisystem ReFS sind sie gar nicht mehr vorhanden. Ihre sinnvolle Nutzung ist daher hauptsächlich auf Einzelrechner außerhalb einer Domäne beschränkt.

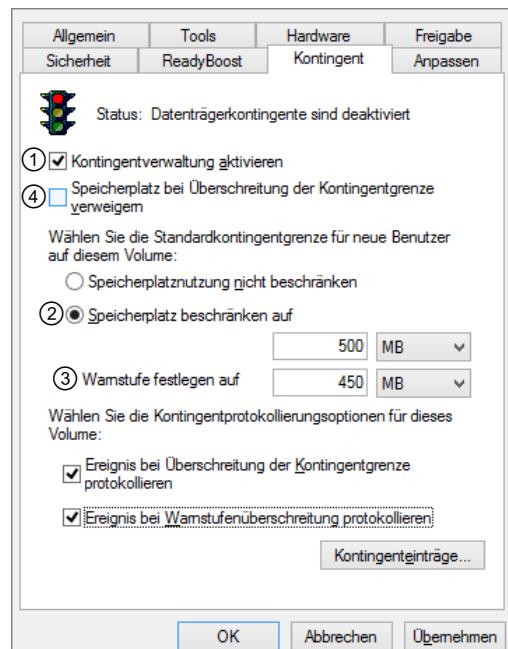


## Datenträgerkontingente einrichten

Um mit der Kontingentverwaltung zu arbeiten, legen Sie zuerst einen Standardwert für neue Volumebenutzer fest:

- ▶ Rufen Sie unter den Eigenschaften des Volumes das Register *Kontingent* auf und klicken Sie auf *Kontingent-einstellungen anzeigen*.
  - ▶ Aktivieren Sie *Kontingentverwaltung aktivieren* ①.
  - ▶ Legen Sie fest, ob und auf welche Größe der Speicherplatz beschränkt werden soll ②, und definieren Sie, bei wie viel belegtem Speicher gewarnt werden soll ③.
- Mit dem Kontrollfeld *Speicherplatz bei Überschreitung der Kontingentgrenze verweigern* können Sie festlegen, ob der Benutzer die begonnene Speicheraktion noch zu Ende führen darf ④.

Das Verweigern des Speicherns führt unter Umständen dazu, dass ein Benutzer seine Arbeitsresultate nicht mehr speichern kann. Wenn der Benutzer noch speichern darf, eröffnet dies eine Möglichkeit, mit riesigen Dateien das Volume trotz Kontingentbeschränkung zum Überlaufen bringen.



*Kontingente bearbeiten*

Wollen Sie anschließend noch gesonderte Kontingente für spezielle Benutzer vergeben oder die vorhandenen Kontingenteinträge einsehen und verwalten, aktivieren Sie die Schaltfläche *Kontingenteinträge* und bearbeiten Sie die Kontingente im Dialogfenster *Kontingenteinträge* über die Menüfunktionen. In der Befehlszeile verwenden Sie dazu `fsutil quota query <Laufwerk>`.

## 15.5 BitLocker benutzen

### Verschlüsselung von Laufwerksinhalten

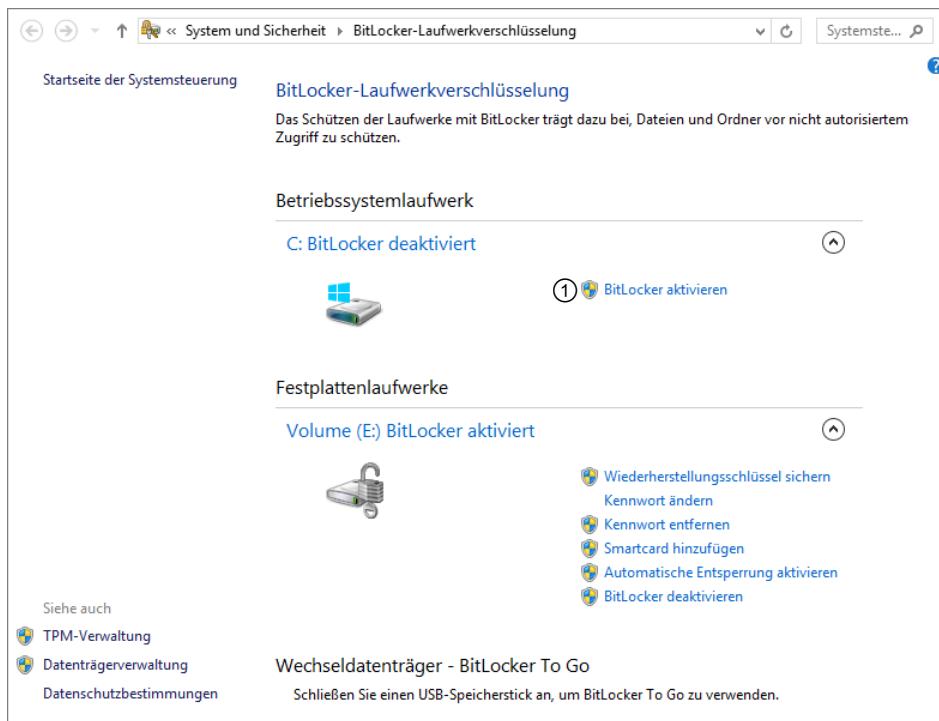
BitLocker ist eine Verschlüsselungstechnologie von Microsoft, die im Gegensatz zum Encrypting Filesystem (EFS) die Daten auf einer Festplatte nicht dateiweise verschlüsselt, sondern partitionsweise.

Bei der Verwendung von BitLocker sollten Sie folgende Dinge beachten:

- ✓ Sie müssen Windows 10 Pro oder Enterprise verwenden.
- ✓ Das Computermainboard ist im Idealfall mit einem TPM-Chip (Trusted-Platform-Module) v1.2 oder höher ausgestattet, dies ist jedoch nicht zwingend erforderlich. Während Datenpartitionen auch ohne TPM verschlüsselt werden können, wird für die Verschlüsselung der Betriebssystempartition standardmäßig TPM benötigt. Weiter unten wird beschrieben, wie Sie das umgehen können.
- ✓ Der Wiederherstellungsschlüssel kann im Microsoft-Konto des Benutzers, auf einem USB-Stick oder in einer Datei gespeichert werden. Es ist ebenfalls möglich, den Schlüssel auszudrucken.
- ✓ BitLocker kann zur Identifizierung anstelle eines Kennworts auch eine SmartCard verwenden.
- ✓ Ihre Festplatte benötigt mindestens 2 Partitionen. Eine für das Betriebssystem (wird nachher verschlüsselt) und eine aktive Partition, mit der zuerst gebootet wird (bleibt unverschlüsselt). Hierfür kann die standardmäßig bei der Installation von Windows 10 eingerichtete unsichtbare Partition verwendet werden.
- ✓ Beide Partitionen müssen mit NTFS formatiert sein.

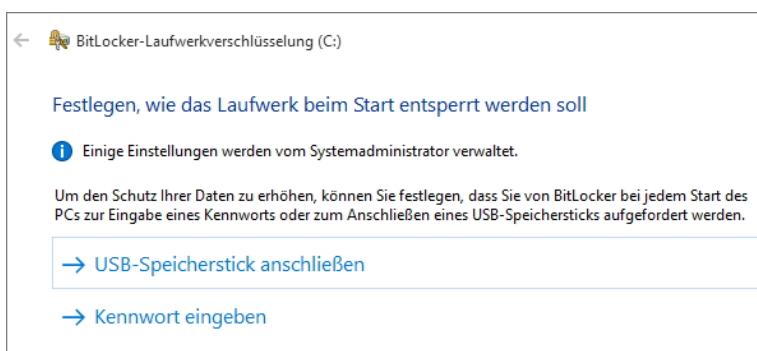
## BitLocker aktivieren

- ▶ Öffnen Sie die Systemsteuerung und geben Sie BitLocker ein.
- ▶ Wählen Sie BitLocker-Laufwerkverschlüsselung.
- ▶ Um BitLocker für ein Laufwerk einzuschalten, klicken Sie auf BitLocker aktivieren ①. Ein Assistent wird gestartet und überprüft die Voraussetzungen.



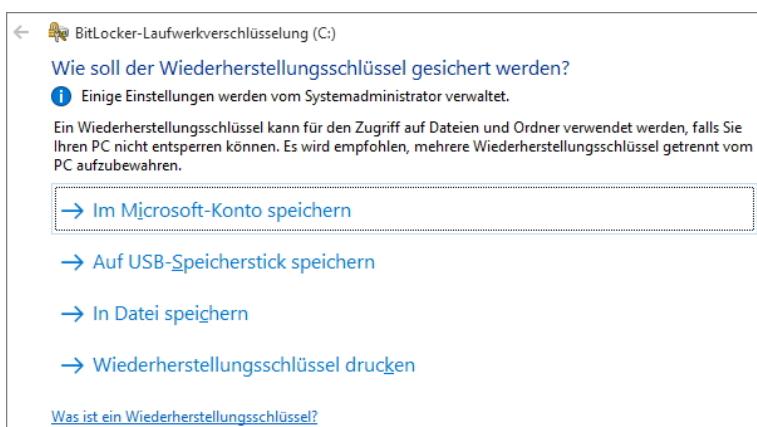
### BitLocker-Laufwerkverschlüsselung

- ▶ Wählen Sie die Methode zum Entsperren des Laufwerks aus. Sie können sich mit einem Kennwort oder über einen USB-Stick identifizieren.



### Identifikation über Kennwort oder USB-Stick

- ▶ Wählen Sie aus, auf welche Weise Sie den Wiederherstellungsschlüssel sichern wollen. Der Vorgang wird nun abgeschlossen und der Datenträger wird verschlüsselt. Abhängig von Größe und Füllgrad kann dies sehr lange dauern.



### Methode zur Schlüsselsicherung auswählen

## BitLocker für Betriebssystemlaufwerke ohne TPM verwenden

Um die BitLocker-Verschlüsselung für das Betriebssystemlaufwerk auch ohne TPM zu ermöglichen, starten Sie den Gruppenrichtlinien-Editor gredit.msc.

- ▶ Öffnen Sie den Pfad *Computerkonfiguration - Administrative Vorlagen - Windows-Komponenten - BitLocker-Laufwerkverschlüsselung - Betriebssystemlaufwerke*.
- ▶ Klicken Sie doppelt auf den Eintrag *Zusätzliche Authentifizierung beim Starten anfordern*.
- ▶ Aktivieren Sie die Gruppenrichtlinie und aktivieren Sie die Option *BitLocker ohne kompatibles TPM zulassen*.



Aktivieren Sie diese Einstellung nur, wenn Sie über mindestens eine Kopie des Startschlüssels und des Wiederherstellungsschlüssels an einem sicheren Ort verfügen, sonst sind bei Verlust des Schlüssels alle Daten verloren.

## BitLocker To Go

In Windows 10 ist die Funktion BitLocker To Go enthalten, die es Ihnen erlaubt, nicht nur fest eingebaute Datenträger zu verschlüsseln, sondern auch Wechselmedien wie z. B. USB-Flashspeicher.

Verfügbare Speichermedien werden Ihnen zusätzlich zu den Volumes in der BitLocker-Übersicht angezeigt. Wenn Sie BitLocker To Go aktivieren wollen, klicken Sie beim entsprechenden Datenträger auf *BitLocker aktivieren* ①.

Analog zum Assistenten für die Festplattenverschlüsselung können Sie nun für BitLocker To Go definieren, mit welcher Methode der Datenträger geschützt werden soll. Der Assistent fordert Sie zudem auch auf, eine Wiederherstellungsdatei anzulegen für den Fall, dass Sie Ihr Passwort vergessen haben oder die Smartcard verloren gegangen sein sollte.

Sobald Sie den Assistenten fertiggestellt haben, beginnt dieser mit der Verschlüsselung des Laufwerks. Warten Sie, bis der Verschlüsselungsvorgang abgeschlossen ist, und entfernen Sie den Datenträger nicht, ohne zumindest den Vorgang vorher mittels der entsprechenden Schaltfläche anzuhalten.

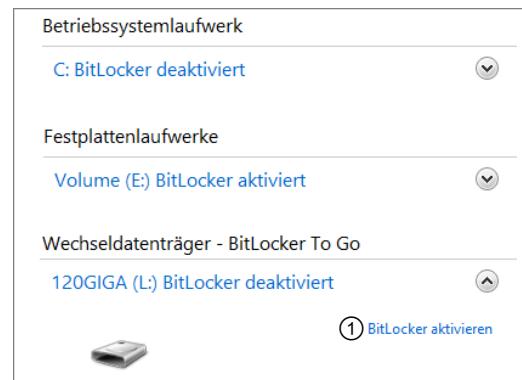
## Verschlüsselte Datenträger auf anderen Computern verwenden

Nach dem Abschluss der Verschlüsselung können Sie den Datenträger an jeden beliebigen Computer mit Windows 8/8.1 oder 10 anschließen, der daraufhin nach Ihrem Passwort oder Ihrer Smartcard fragt und die Inhalte entschlüsselt.

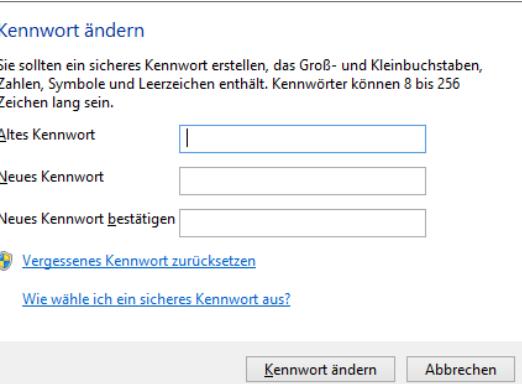
Wenn Sie einen Datenträger mit BitLocker To Go an ein System mit Windows XP oder Vista anschließen, wird eine spezielle Version von BitLocker To Go gestartet, die allerdings nur den Lesezugriff auf die enthaltenen Daten erlaubt.

## Verschlüsselung ändern oder beenden

Sie haben in der BitLocker-Laufwerkverwaltung auch die Möglichkeit, die Passwörter von Datenträgern zu ändern, neue Wiederherstellungsdateien zu generieren oder die Verschlüsselung wieder rückgängig zu machen.



*BitLocker für externe Laufwerke aktivieren*



*Ändern des Kennworts*

## 15.6 Übung

### Datenträger verwalten

Übungsdatei: --

Ergebnisdatei: *Uebung15\_E.pdf*

1. Wie starten Sie die Datenträgerverwaltungskonsole?
2. Wie überprüfen Sie die Festplatte und das Dateisystem auf Fehler?

# 16 Systemüberwachung und -pflege

## In diesem Kapitel erfahren Sie

- ✓ welche Werkzeuge Sie zur Überwachung des Computers nutzen können
- ✓ wie Sie Anwendungen überwachen können
- ✓ wie Sie die Leistungsengpässe Ihres Systems finden können

## 16.1 Ereignisanzeige

### Arbeiten mit Protokollen

Ereignisprotokolle sammeln Einträge von verschiedenen Quellen. Hier wird z. B. festgehalten, wenn ein Dienst regelmäßig mit einem Fehler beendet wird. In so einem Fall können Sie sich mithilfe der Ereignis-ID auf die Suche nach einer Lösung für das Problem machen. Voraussetzung dafür ist die regelmäßige Kontrolle der Protokolle.

### Grundlagen von Ereignisprotokollen

Die Ereignisanzeige ist der Ort, an dem die Protokolle eingesehen werden können. Sie können die Ereignisanzeige entweder für den eigenen Rechner einrichten oder die Protokolle eines entfernten Computers einsehen, wenn Sie die Berechtigung dazu haben. Zusätzlich haben Sie die Möglichkeit, Sammlungen von Ereignissen verschiedener Rechner in Abonnements zusammenzufassen. Im Folgenden wird davon ausgegangen, dass Sie die Ereignisanzeige Ihres eigenen Rechners einsehen wollen. Die Ereignisanzeige gliedert sich in vier Abschnitte:

<b>Benutzerdefinierte Ansichten</b>	Unter benutzerdefinierten Ansichten können bestimmte Arten von Ereignissen gefiltert zusammengefasst werden. In den Standardeinstellungen werden hier administrative Ereignisse dargestellt. Administrative Ereignisse sind kritische, Fehler- und Warnungsereignisse aller Protokolle, die für die Administration wichtig sind.
<b>Windows-Protokolle</b>	In Windows-Protokollen finden Sie die wichtigsten Informationen zum aktuellen Zustand des Betriebssystems.
<b>Anwendungs- und Dienstprotokolle</b>	Je nach aktivierten Funktionen und installierten Anwendungen können sich hier spezifische Protokolle finden.
<b>Abonnements</b>	Ein Abonnement definiert eine Sammlung von Ereignissen, die auf verschiedenen Computern im Netzwerk stattfinden. Angezeigt werden diese unter <i>Windows-Protokolle - Weitergeleitete Ereignisse</i> .

### Windows-Protokolle

<b>Anwendung</b>	In diese Sektion schreiben Anwendungen wie das Sicherungsprogramm, die Druckverwaltung und der Windows-Anmeldeprozess ihre Ereignismeldungen.
<b>Sicherheit</b>	Im Sicherheitsprotokoll finden Sie Informationen zu sicherheitssensiblen Aktivitäten. Teilweise werden diese automatisch überwacht, teilweise können Sie die Überwachung von Objekten festlegen. Beispiele dafür sind die Protokollierung des Systemstarts, Zugriffsüberwachungen auf Dateien, die Überwachung von Benutzeraktionen oder Anmeldevorgängen.
<b>Installation</b>	Jede Installation einer Software wird im Installationsprotokoll vermerkt. Zusätzlich finden sich hier Informationen wie ein ausstehender Neustart, der für das Fertigstellen einer Installation benötigt wird.

<b>System</b>	In diese Sektion werden systeminterne Ereignisse eingetragen. Dabei werden nicht nur Fehler, sondern auch erfolgreiche Ereignisse protokolliert (z. B. der Start eines Dienstes).
<b>Weitergeleitete Ereignisse</b>	Wenn Sie Abonnements eingerichtet haben, finden sich hier die entsprechenden Ereignisse.

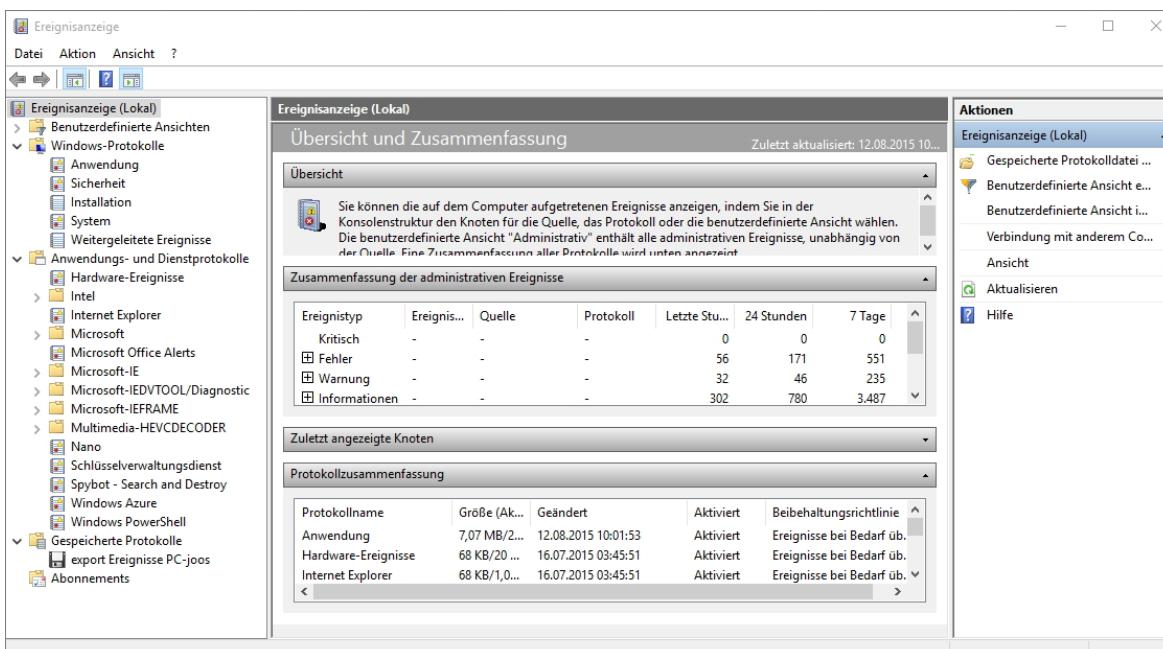
## Ereignisebenen

Ereignisebenen (früher Ereignistypen) beschreiben, wie ein Ereignis einzustufen ist. Insbesondere für benutzerdefinierte Ansichten können Sie bestimmte Ebenen filtern.

<b>Kritisch</b>	Kritische Ereignisse werden protokolliert, wenn eine Anwendung, ein Dienst oder eine Komponente einen Fehler aufweist, der einen Neustart oder Weiterbetrieb unmöglich macht. Ein Beispiel wäre das Überlaufen der Systempartition.
<b>Fehler</b>	Diese Meldung erscheint, wenn ein schwerwiegender Fehler aufgetreten ist, etwa ein Dienst nicht gestartet werden konnte.
<b>Warnung</b>	Warnungen sagen aus, dass ein nicht kritisches Ereignis aufgetreten ist, das später zu Fehlern führen kann. Ein Beispiel wäre, dass kein Domänencontroller gefunden werden konnte.
<b>Informationen</b>	Unter <b>Informationen</b> wird festgehalten, dass eine Aktion erfolgreich durchgeführt wurde, beispielsweise ein Treiber geladen wurde.
<b>Überwachung erfolgreich</b>	Ein Eintrag im Sicherheitsprotokoll erscheint als erfolgreich, wenn eine Legitimierung durchgeführt wurde. Dies findet z. B. statt, wenn ein Benutzer sich mit dem korrekten Kennwort angemeldet hat.
<b>Überwachung gescheitert</b>	Ein Eintrag dieser Art im Sicherheitsprotokoll bedeutet, dass ein Benutzer versucht hat, etwas zu tun, zu dem er nicht legitimiert war, etwa sich mit einem falschen Kennwort anzumelden.

## Protokoll in der Ereignisanzeige einsehen

- Geben Sie `eventvwr.msc` ein und wählen Sie *Ereignisprotokolle anzeigen*. Alternativen: *Systemsteuerung - Verwaltung - Ereignisanzeige* oder `eventvwr.msc` (Startmenü).



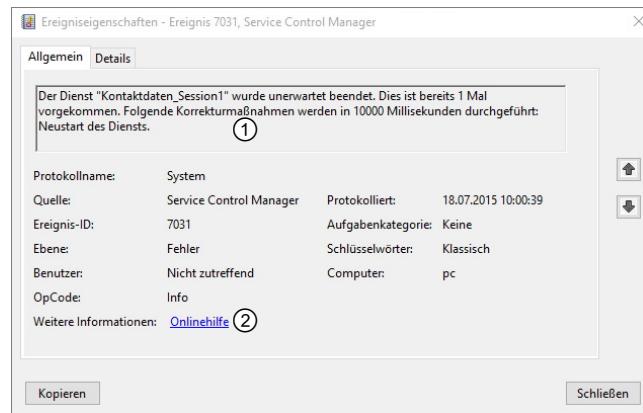
Ereignisanzeige - Gesamtübersicht

## Ereignisdetails anzeigen

- Wählen Sie in der Baumstruktur eine Struktur und klicken Sie doppelt auf den Protokoll-eintrag.

Der obere Bereich ① liefert Ihnen Informationen über einen Fehler oder über einen Vorgang, der erfolgreich ausgeführt werden konnte.

Genauere Informationen über das Ereignis können Sie über den Hyperlink ② beziehen, der Sie zur Microsoft Knowledge Base weiterleitet.



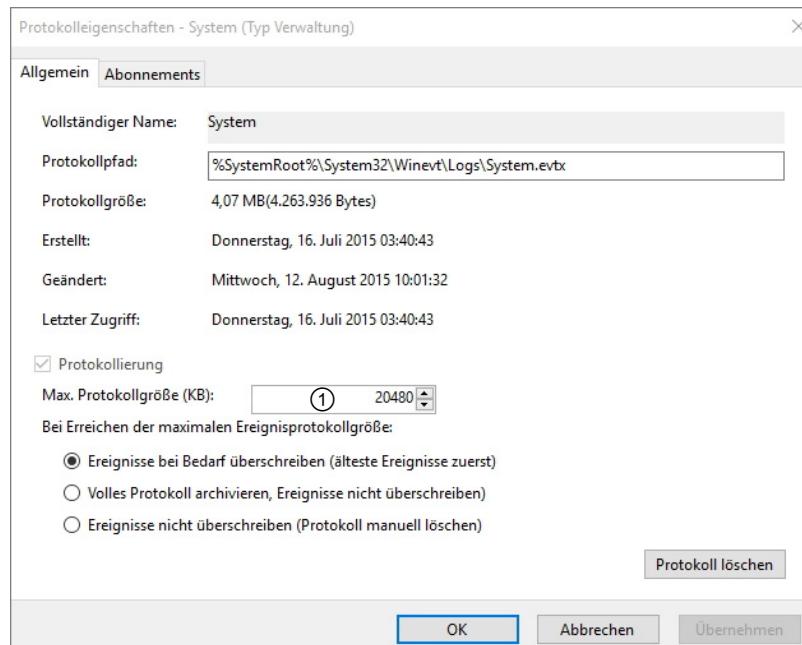
 Wenn Sie zusätzliche Sicherheitsereignisse protokollieren möchten, müssen Sie dies zuerst mit Überwachungsrichtlinien aktivieren.

Haben Sie den Fehler genauer eingegrenzt und Fehlermeldungen in der Ereignisanzeige und der Diagnose festgestellt, suchen Sie auf der Internetseite <http://www.eventid.net> nach diesen Fehlern. Auf dieser Seite gibt es zu so gut wie jedem Eintrag der Ereignisanzeige Hinweise und mögliche Lösungsansätze.

Außerdem können Sie den Fehler in einer Suchmaschine oder in speziellen Supportseiten eingeben, wie zum Beispiel <http://www.experts-exchange.com>. Auch die Suche in der Microsoft Knowledge Base unter <http://support.microsoft.com> hilft oft weiter. Suchen Sie allerdings in der englischen Microsoft Knowledge Base immer nur nach englischen Begriffen, da Sie hier mehr Antworten erhalten.

## Protokoll konfigurieren

- Klicken Sie mit der rechten Maustaste auf das Protokoll, das Sie anpassen möchten, und wählen Sie *Eigenschaften* aus.
- Legen Sie im Register *Allgemein* im Bereich *Protokollgröße* ① die maximale Protokollgröße fest und nach welchen Kriterien das Protokoll überschrieben bzw. gelöscht werden soll.



### Eigenschaften eines Protokolls

Im Register *Abonnements* können Sie einstellen, ob und von welchen anderen Computern ebenfalls Ereignismeldungen gesammelt werden sollen, sodass sie Ihnen ebenfalls zur Ansicht lokal zur Verfügung stehen.

## Protokoll manuell löschen

Alle Protokolle (auch solche, für die Sie einen automatischen Löschkvorgang definiert haben) können Sie manuell löschen. Dabei werden alle Protokolleinträge des betreffenden Protokolls gelöscht.

- Rufen Sie das Kontextmenü des Protokolls auf, das Sie löschen möchten, und aktivieren Sie den Kontextmenüpunkt *Protokoll löschen*.

## 16.2 Task-Manager und Problemanalyse

### Verwendung des Task-Managers

Der Task-Manager von Windows 10 verfügt über sieben Registerkarten.

- |            |               |            |           |
|------------|---------------|------------|-----------|
| ✓ Prozesse | ✓ App-Verlauf | ✓ Benutzer | ✓ Dienste |
| ✓ Leistung | ✓ Autostart   | ✓ Details  |           |

**Prozesse** zeigt eine Übersicht des Ressourcenbedarfs einzelner Anwendungen oder Systemprozesse. Um den Task-Manager zu starten, betätigen Sie **Strg** **↑** **Esc**. Alternativ können Sie den Task-Manager auch über das Menü aufrufen, das mit der Tastenkombination **Strg** **Alt** **Entf** erscheint oder durch Eintippen von `taskmgr` im Startmenü.

Wählen Sie im Task-Manager *Optionen - Immer im Vordergrund*, bleibt der Task-Manager immer im vorderen Bereich der Anzeige. So können Sie eine Analyse von Programmen durchführen, ohne den Task-Manager immer erneut in den Vordergrund holen zu müssen.

### Prozesse

Im Register **Prozesse** werden in der Standardansicht alle Apps (Anwendungen), Hintergrundprozesse und Windows-Prozesse getrennt voneinander aufgelistet ① und die Auslastung von CPU ②, Arbeitsspeicher ③, Datenträger ④ und Netzwerk ⑤ wird angezeigt. Klicken Sie auf die verschiedenen Spalten auf der Registerkarte **Prozesse** oder **Details**, erkennen Sie schnell, welche Prozesse am meisten Leistung benötigen.

### Mit Spalten arbeiten

Mit einem Rechtsklick auf die Spaltentitel ⑥ können Sie im Kontextmenü weitere Spalten hinzufügen oder entfernen.

Alle Spalten lassen sich mit einem Klick auf den Spaltentitel sortieren.

Prozesse						
Name	Status	2% CPU	36% Arbeitss...	6% Datenträ...	1% Netzwerk	0%
Apps (2) ①		②	③	④	⑤	⑥
▷ Paint		1,6%	16,9 MB	0 MB/s	0 MBit/s	
▷ Task-Manager		0%	7,9 MB	0 MB/s	0 MB/s	
Hintergrundprozesse (7)						
▷ Communications Service		0%	4,4 MB	0 MB/s	0 MBit/s	
▷ Hostprozess für Windows-Aufg...		0%	2,0 MB	0 MB/s	0 MBit/s	
▷ Microsoft Windows Search-Inde...		0%	4,7 MB	0 MB/s	0 MBit/s	
▷ Print Filter Pipeline Host		0%	0,3 MB	0 MB/s	0 MBit/s	
▷ Runtime Broker		0%	0,4 MB	0 MB/s	0 MBit/s	
▷ Spoolersubsystem-Anwendung		0%	1,8 MB	0 MB/s	0 MBit/s	
▷ Windows-Lizenzüberwachungs...		0%	0,3 MB	0 MB/s	0 MBit/s	
Windows-Prozesse (24)						
▷ Antimalware Service Executable		0%	21,5 MB	0,1 MB/s	0 MBit/s	
▷ Anwendung für Dienste und Co...		0%	2,4 MB	0 MB/s	0 MBit/s	
⑦ Weniger Details						
Task beenden						

Rufen Sie den Task-Manager über das Suchfeld der Taskleiste mit `taskmgr` auf und halten die Tastenkombination **Strg** **↑** **Alt** gedrückt, können Sie die Einstellungen des Task-Managers auf die Standardwerte zurücksetzen.

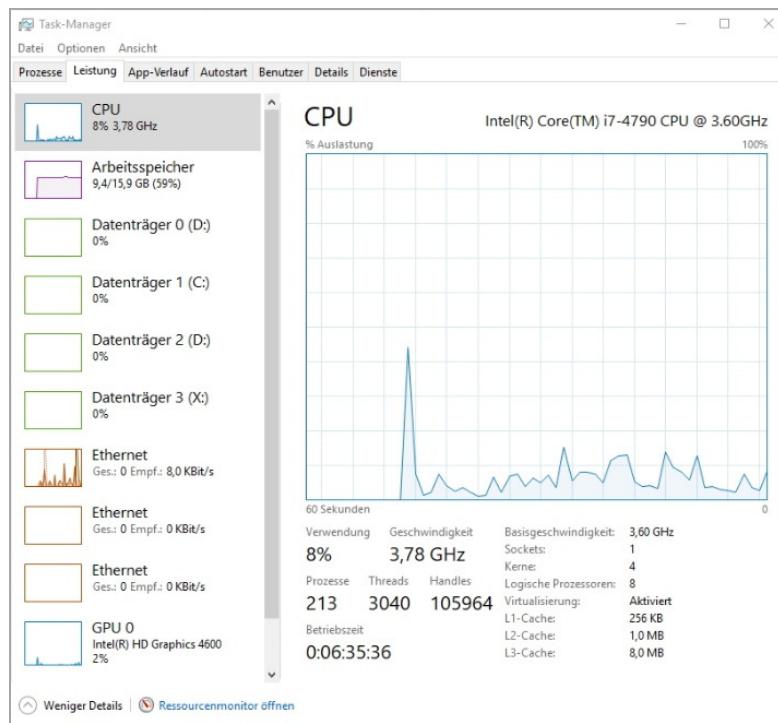
## Leistung

Im Register *Leistung* sehen Sie in der linken Spalte kleine Abbildungen des Leistungsverlaufs für CPU und Arbeitsspeicher, gefolgt von einem Diagramm für jeden Datenträger und jede Netzwerkverbindung.

Seit Windows 10, Version 1709 ist auf der Registerkarte *Leistung* nicht nur die Auslastung von CPU, Datenträger und Netzwerkadapter zu sehen, sondern auch die Auslastung der Grafikadapter des Systems.

Wenn Sie links auf eine Kategorie klicken, wird auf der rechten Seite eine detaillierte Darstellung mit weiteren Informationen angezeigt.

Über das Kontextmenü der linken und rechten Seite können Sie die jeweils andere Spalte ausblenden.



Im unteren Bereich befindet sich ein Link, über den Sie den **Ressourcenmonitor** öffnen. Hier finden Sie eine detaillierte Ansicht des aktuellen CPU-Verbrauchs, des Arbeitsspeichers, der Datenträger und des Netzwerkverkehrs.

Die Gesamtleistung eines Systems wird durch verschiedene Faktoren begrenzt. Hierzu zählen etwa die

- ✓ Zugriffsgeschwindigkeit der physischen Datenträger,
- ✓ die für alle laufenden Prozesse zur Verfügung stehende Speichermenge,
- ✓ die Prozessorgeschwindigkeit und
- ✓ der Datendurchsatz der Netzwerkschnittstellen.

Nachdem die einschränkenden Faktoren auf der Hardwareseite identifiziert wurden, kann der Ressourcenverbrauch einzelner Anwendungen und Prozesse überprüft werden. Anhand einer umfassenden Leistungsanalyse, die sowohl die Auswirkungen von Anwendungen als auch die Gesamtkapazität berücksichtigt, können IT-Experten einen Bereitstellungsplan entwickeln und an die jeweiligen Anforderungen anpassen. Alternativ können Sie diese Funktion auch über `perfmon /res` starten. Durch Erweitern der Ressourcenübersicht können Sie zusätzliche Informationen anzeigen und überprüfen, welche Ressourcen von welchen Prozessen genutzt werden.

Der Bereich mit der Ressourcenübersicht enthält vier animierte Diagramme, die die Auslastung der CPU-, Datenträger-, Netzwerk- und Speicherressourcen des lokalen Computers in Echtzeit anzeigen. Unter den Diagrammen befinden sich vier erweiterbare Bereiche, in denen Einzelheiten zur jeweiligen Ressource angezeigt werden können. Klicken Sie zur Anzeige dieser Informationen auf den Abwärtspfeil rechts neben dem jeweiligen Balken.

## App-Verlauf

Im Register **App-Verlauf** können Sie sehen, wie viel CPU-Zeit ①, Netzwerkverkehr ② und Kachelupdates ③ die installierten Windows-10-Apps seit dem Einschalten des Computers verursacht haben.

Sie können alle Werte auf null setzen, indem Sie auf *Auslastungsverlauf löschen* ④ klicken.

Mit einem Rechtsklick auf eine App können Sie zu dieser App wechseln.

Task-Manager					
Ressourcenauslastung seit 16.07.2015 für aktuelles Benutzerkonto.					
Auslastungsverlauf löschen ④					
Name	① CPU-Zeit	② Netzwerk	③ Getaktet (Netz...)	④ Kachelupdates	
3D Builder	0:00:00	0 MB	0 MB	0 MB	^
Alarm & Uhr	0:00:01	0 MB	0 MB	0 MB	
Cortana	0:20:55	0 MB	0 MB	0 MB	
Erste Schritte	0:00:03	0 MB	0 MB	0 MB	
Filme & Fernsehsendung...	0:00:06	0 MB	0 MB	0 MB	
Finanzen	0:00:00	0 MB	0 MB	0 MB	
Fotos	12:44:32	0 MB	0 MB	0 MB	
Gesundheit & Fitness	0:00:00	0,4 MB	0 MB	0,4 MB	
Groove-Musik	0:01:22	0 MB	0 MB	0 MB	

[Weniger Details](#)

## Ressourcenverbrauch der Windows-10-Apps

## Autostart

Im Register **Autostart** sehen Sie alle Anwendungen, die über den Autostart-Ordner oder einen Autostart-Eintrag in der Registry gestartet werden.

## Benutzer

Im Register **Benutzer** sehen Sie alle angemeldeten Benutzer und deren Ressourcenverbrauch, aufgegliedert in CPU ①, Arbeitsspeicher ②, Datenträger ③ und Netzwerk ④.

Mit einem Doppelklick auf einen Benutzer werden alle Benutzerprozesse angezeigt.

Durch einen Klick mit der rechten Maustaste auf einen Benutzer können Sie den Benutzer trennen oder in die Benutzerverwaltung wechseln.

Task-Manager					
Ressourcenverbrauch der Windows-10-Apps					
Ressourcenverbrauch der Windows-10-Apps					
Benutzer	① CPU	② Arbeitsspeicher	③ Datenträger	④ Netzwerk	
@hotmail.de (10)	0,7%	103,8 MB	0 MB/s	0 MBit/s	
Client-Server-Laufzeitproz...	0%	1,1 MB	0 MB/s	0 MBit/s	
Communications Service	0%	0,4 MB	0 MB/s	0 MBit/s	
Desktopfenster-Manager	0%	32,1 MB	0 MB/s	0 MBit/s	
Hostprozess für Windows-...	0%	2,0 MB	0 MB/s	0 MBit/s	
Microsoft Management C...	0%	2,3 MB	0 MB/s	0 MBit/s	
Paint	0,7%	11,8 MB	0 MB/s	0 MBit/s	
Runtime Broker	0%	0,4 MB	0 MB/s	0 MBit/s	
Task-Manager	0%	9,1 MB	0 MB/s	0 MBit/s	
Windows-Anmeldeanwen...	0%	0,6 MB	0 MB/s	0 MBit/s	
Windows-Explorer	0%	44,1 MB	0 MB/s	0 MBit/s	

[Weniger Details](#)

[Trennen](#)

## Ressourcenverbrauch Benutzer

## Details

Im Register **Details** sehen Sie eine genaue Auflistung aller System- und Benutzerprozesse ①, deren CPU- und Arbeitsspeicherauslastung ②, den Ausführungsstatus ③ und einer Beschreibung ④.

Im Kontextmenü eines Prozesses können Sie den Prozess oder die gesamte Prozessstruktur beenden, die Priorität und CPU-Bindung festlegen, den Dateipfad zur Anwendung öffnen, sich die Dateieigenschaften anzeigen lassen und im Internet nach dem Dateinamen suchen.

Task-Manager						
Ressourcenverbrauch Benutzer						
Ressourcenverbrauch Benutzer						
Name	① PID	Status	③ Benutzernam...	CPU	Arbeitsspeich...	Beschreibung
AAM Updates Notifi...	3032	Wird ausgeführt	Thomas	00	320 K	AAM Updates Notifier Application
Adobe Desktop Servi...	5172	Wird ausgeführt	Thomas	00	34.864 K	Creative Cloud
AdobePCBroker.exe	11136	Wird ausgeführt	Thomas	00	1.728 K	Adobe IPC Broker
AnkerMonEx.exe	11240	Wird ausgeführt	Thomas	00	5.392 K	AnkerMonEx.exe
AppleMobileDeviceS...	3004	Wird ausgeführt	SYSTEM	00	3.416 K	MobileDeviceService
ApplicationFrameHo...	2172	Wird ausgeführt	Thomas	00	3.272 K	Application Frame Host
APSDaemon.exe	9380	Wird ausgeführt	Thomas	00	3.536 K	Apple Push
audiogd.exe	7800	Wird ausgeführt	Lokaler Di...	00	12.080 K	Windows Graphisolierung für Audiogeräte
BrCclSys.exe	3204	Wird ausgeführt	Thomas	00	1.208 K	ControlCenter UX System
BrCtrlCntr.exe	8348	Wird ausgeführt	Thomas	00	1.072 K	ControlCenter Main Process
BrYNsVc.exe	11304	Wird ausgeführt	SYSTEM	00	1.568 K	BrYNCSvc
CCLibrary.exe	11952	Wird ausgeführt	Thomas	00	340 K	CCLibraries
chrome.exe	7636	Wird ausgeführt	Thomas	00	8.700 K	Google Chrome
chrome.exe	696	Wird ausgeführt	Thomas	02	125.124 K	Google Chrome
chrome.exe	8904	Wird ausgeführt	Thomas	01	141.904 K	Google Chrome
chrome.exe	12000	Wird ausgeführt	Thomas	00	9.748 K	Google Chrome

## Detaillierte Prozessansicht

## Dienste

Im Register *Dienste* werden alle vorhandenen Dienste aufgelistet, die auf dem System laufen. Neben dem Namen des Dienstes ① wird auch die Prozess-ID ②, eine Beschreibung ③ und der Ausführungsstatus ④ sowie die Zugehörigkeit zu einer Dienstgruppe (z. B. *Local-Service*, *NetworkService*) angezeigt ⑤.

Im Kontextmenü eines Dienstes können Sie den Dienst starten, anhalten und neu starten. Außerdem können Sie den Namen des Dienstes im Internet suchen oder die MMC Dienste öffnen.

Name ①	PID ②	Beschreibung ③	Status ④	Gruppe ⑤
WSearch	2864	Windows Search	Wird ausgeführt	
WMPNetworkSvc		Windows Media Player-Netzwerk...	Beendet	
wmiApSrv		WMI-Leistungsadapter	Beendet	
WLMS	1328	Windows-Lizenzüberwachungs...	Wird ausgeführt	
WinDefend	1284	Windows Defender-Dienst	Wird ausgeführt	
wbengine		Blockebenen-Sicherungsmodul	Beendet	
VSS		Volumeschattenkopie	Beendet	
vds	3928	Virtueller Datenträger	Wird ausgeführt	
VaultSvc	596	Anmeldeinformationsverwaltung	Wird ausgeführt	
UIODetect		Erkennung interaktiver Dienste	Beendet	
TrustedInstaller		Windows Modules Installer	Beendet	
sppsvc	4708	Software Protection	Wird ausgeführt	
Spooler	1036	Druckwarteschlange	Wird ausgeführt	

(⑥) Weniger Details | (⑦) Dienste öffnen

Auflistung aller Dienste

## Diagnose des Arbeitsspeichers

Häufig sind die Probleme auf einem Server auf defekten Arbeitsspeicher zurückzuführen. In Windows 10 wurde daher ein spezielles Diagnoseprogramm integriert, welches den Arbeitsspeicher ausführlich auf Fehler überprüft. Sie können das Tool über `mdsched` aufrufen. Entweder können Sie den Computer sofort neu starten und eine Diagnose durchführen oder festlegen, dass die Diagnose erst beim nächsten Systemstart durchgeführt werden soll. Während der Speicherdiagnose prüft das Programm, ob der eingebaute Arbeitsspeicher Fehler aufweist, was eine häufige Ursache für ungeklärte Abstürze ist. Nachdem der Test abgeschlossen ist, startet der Computer automatisch neu und meldet das Ergebnis über ein Symbol im Infobereich der Taskleiste.

Über die Funktionstaste **F1** gelangen Sie zu den Optionen der Überwachung, können verschiedene Überprüfungsmethoden auswählen und mit **F10** starten. Ist der Test beendet, startet der Server automatisch wieder. Sie müssen nicht warten, bis der Test abgeschlossen ist, damit der Server wieder zur Verfügung steht.



Auf der Ultimate Boot CD (<http://www.ultimatebootcd.com>) befinden sich im Bereich *Memory* ebenfalls einige Testtools für den Arbeitsspeicher.

## 16.3 Auslastung der Netzwerkf freigaben kontrollieren

### Freigaben anzeigen

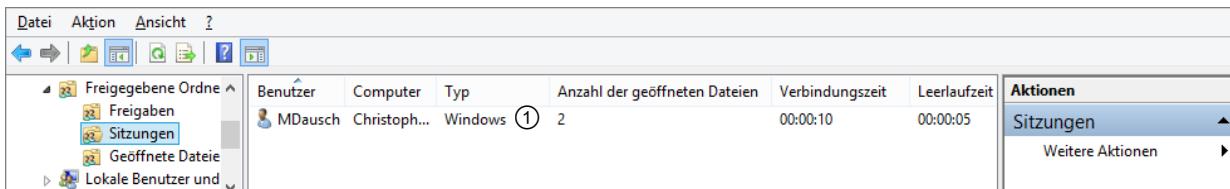
In *Computerverwaltung - System - Freigegebene Ordner - Freigaben* werden alle Freigaben auf Ihrem Computer aufgelistet, darunter auch die Freigabe für die Remoteverwaltung ①, die administrativen Freigaben für alle Partitionen ② und selbst eingerichtete Freigaben ③.

Freigabename	Ordnerpfad	Typ	Anzahl der Clientverbindungen	Beschreibung
ADMIN\$	C:\Windows	① Windows	0	Remoteverwaltung
C\$	C:\	② Windows	0	Standardfreigabe
E\$	E:\	Windows	0	Standardfreigabe
Freigabeordn...	C:\Freigabeordner	③ Windows	0	
IPC\$		Windows	0	Remote-IPC
print\$	C:\Windows\system...	Windows	0	Druckertreiber

Anzeige aller Freigaben

### Verbundene Benutzer anzeigen

In *Computerverwaltung - System - Freigegebene Ordner - Sitzungen* können Sie sehen, welche Rechner und welche Benutzer momentan mit Ihrem System verbunden sind ①. Sie können das Programm auch über *fsmgmt.msc* starten. Sie können eine Verbindung im Kontextmenü des verbundenen Benutzers oder des Computers trennen. Möchten Sie alle bestehenden Verbindungen trennen, wählen Sie im Kontextmenü des Konsolenelementes *Sitzungen* den Punkt *Alle Sitzungen trennen*.



*Verbundene Benutzer anzeigen*

### Geöffnete Dateien anzeigen

Unter dem Konsolenelement *Geöffnete Dateien* können Sie einsehen, welche Dateien gerade vom System als geöffnet geführt werden und welche Benutzer damit verbunden sind. Sie können diese Verbindungen trennen, indem Sie im Kontextmenü den entsprechenden Punkt wählen.

### Freigaben verwalten

Unter dem Konsolenelement *Freigaben* erhalten Sie einen Überblick über die auf Ihrem Rechner angelegten Freigaben und können diese über das Kontextmenü aufheben. Außerdem können Sie die Eigenschaften der Freigaben hier einsehen und diese wie gewohnt bearbeiten.

## 16.4 Leistungsüberwachung

### Grundlagen der Systemüberwachung

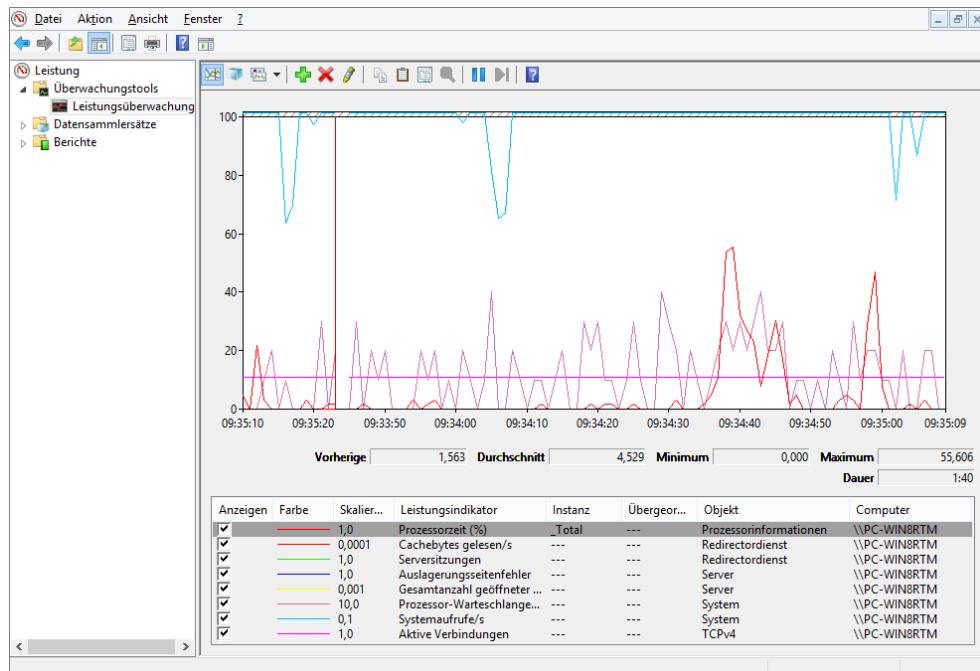
Ein wichtiges Aufgabengebiet des Systembetreuers betrifft die Analyse des laufenden Systems, insbesondere das Aufspüren von Engpässen und Schwachstellen.

Die Leistungsüberwachung mit dem Programm *perfmon.exe* dient zum Anzeigen und Aufzeichnen der Systembelastung, indem Messdaten einzelner Systemkomponenten (etwa Prozessorauslastung) dargestellt oder protokolliert werden.

Der Systemmonitor verfügt über drei Funktionen zur Auswertung der erfassten Messdaten:

- ✓ Diagramm: Messdaten anzeigen
- ✓ Warnungen: Engpässe melden
- ✓ Protokoll: Messdaten in eine Datei speichern, um sie zu einem späteren Zeitpunkt anzeigen zu lassen

- ▶ Rufen Sie die Leistungsüberwachung über **Systemsteuerung - Verwaltung - Leistungsüberwachung** auf. Alternativ können Sie auch im Startmenü **perfmon** eingeben.
- ▶ Klicken Sie in der linken Spalte auf **Überwachungstools - Leistungsüberwachung**.



Auslastungsverlauf verschiedener Parameter



Wenn Sie nur das Snap-In für die Leistungsüberwachung einer MMC-Konsole hinzufügen möchten, wählen Sie im Dialogfenster **Snap-In hinzufügen** den Eintrag **Leistungsüberwachung** aus. Schließen Sie den Vorgang wie üblich ab.

Die Bedienung des Systemmonitors erfolgt unter Windows 10 über eine Reihe von Symbolen, die im Folgenden beschrieben werden. Sie können außerdem eine Beschreibung jedes Symbols erhalten, indem Sie mit dem Mauszeiger auf das Symbol zeigen.



Symbolleiste des Systemmonitors

	Aktuellen Vorgang anzeigen	Zeigt im Hauptfenster aktuelle Daten in Echtzeit an.
	Protokolldateien anzeigen	Mit diesem Symbol stellen Sie von aktueller Datenerfassung auf Auswertung gespeicherter Datensätze um.
	Diagrammtyp	Diese Option dient dazu, zwischen verschiedenen Diagrammtypen umzuschalten.
	Hinzufügen	Fügen Sie neue Datenquellen hinzu, indem Sie dieses Symbol betätigen.
	Löschen	Löschen Sie die im unteren Bereich markierte Datenquelle.
	Markierung	Mit diesem Symbol können Sie die im unteren Feld markierte Datenquelle in der Darstellung hervorheben.
	Eigenschaften kopieren	Kopieren Sie mit diesem Symbol die Eigenschaften des Systemmonitors.
	Leistungsindikatoren-liste einfügen	Fügen Sie hiermit eine Liste von Datenquellen in einen Systemmonitor ein.
	Eigenschaften	Zeigen Sie die Eigenschaften des Systemmonitors an.

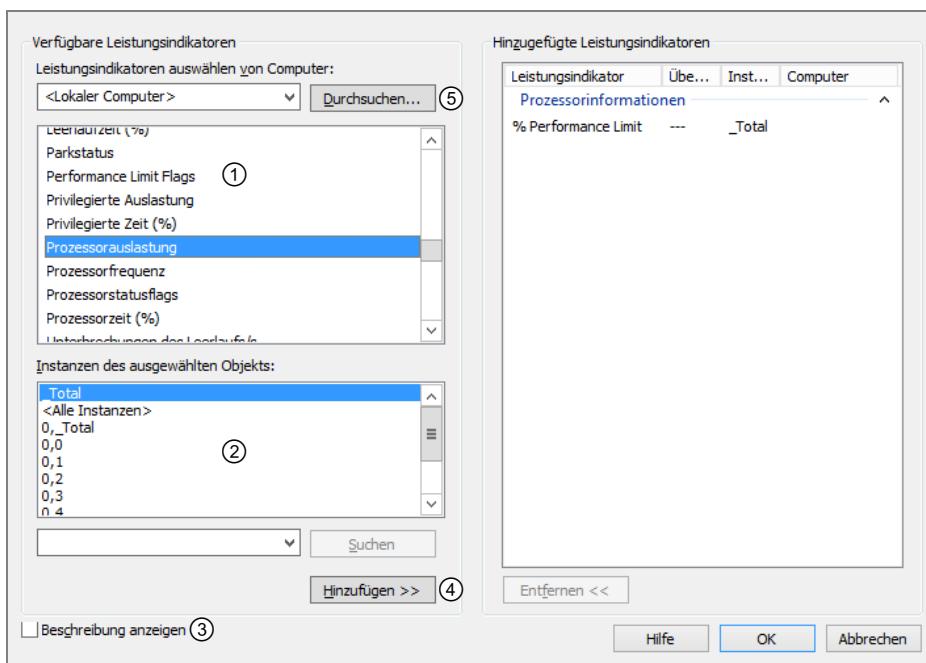
	<b>Zoom</b>	Ermöglicht das Heranzoomen an dargestellte Leistungsgrafiken
	<b>Anzeige fixieren</b>	Fixieren Sie die Anzeige des Systemmonitors.
	<b>Daten aktualisieren</b>	Aktualisieren Sie die Daten bei fixierter Anzeige.

Bei der Leistungsüberwachung werden folgende Objekte unterschieden:

<b>Datenobjekt</b>	Hier wird das zu beobachtende Objekt ausgewählt (z. B. Prozessor, logischer Datenträger).
<b>Leistungsindikator</b>	Zu den meisten Objekten sind mehrere Datenquellen verfügbar.
<b>Instanz</b>	Sind von einem Objekt mehrere Instanzen vorhanden (z. B. Multiprozessorsystem oder mehrere physische Datenträger), muss hier eine Instanz angegeben werden.

### Art der Messdaten definieren

- ▶ Klicken Sie auf .
- ▶ Wählen Sie im Dialogfenster *Leistungsindikatoren hinzufügen* anhand der Felder ① und ② die Systemkomponente, die überwacht werden soll.
- ✓ Durch Aktivieren des Kontrollfelds *Beschreibung anzeigen* ③ können Sie sich eine Beschreibung anzeigen lassen.
- ✓ Mit *Hinzufügen* ④ nehmen Sie die Komponente in die Überwachung auf.
- ✓ Mit *Durchsuchen* ⑤ können Sie wählen, ob die Messdaten lokal oder auf einem entfernten Computer gesammelt werden.



### Leistungsindikatoren hinzufügen

Bei der Überwachung eines entfernten Computers ist eine Anmeldung mit einem Benutzerkonto erforderlich, das dort administrative Rechte besitzt.

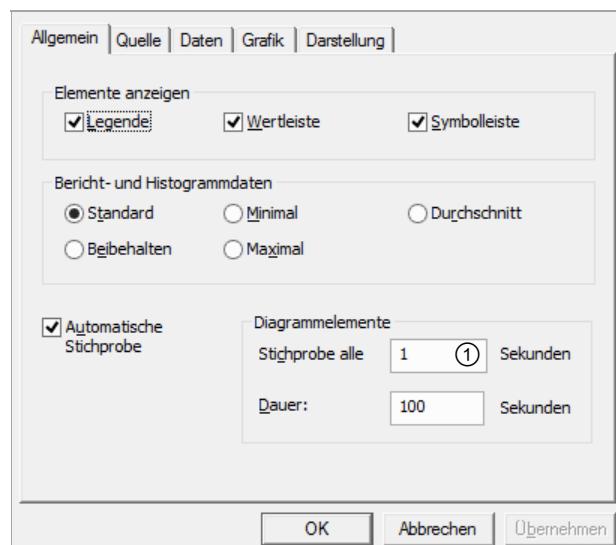
## Anzeige des Diagramms verändern

- ▶ Betätigen Sie das Symbol *Eigenschaften* .
- ▶ Wählen Sie im Dialogfenster *Eigenschaften von Leistungsüberwachung* im Register *Allgemein* die gewünschte Diagrammart.
- ▶ Legen Sie gegebenenfalls bei ① das Zeitintervall für die Aktualisierung fest.

Die Messdaten des Diagramms werden entweder als Kurve (Grafik), als Balkendiagramm (Histogramm) oder als Bericht angezeigt.

Wenn Sie die Datenquelle verändern möchten, wählen Sie unter dem Register *Quelle* das Messprotokoll aus, das Sie darstellen möchten. Unter dem Register *Daten* können Sie auch mit *Hinzufügen/Entfernen* zum Dialogfenster *Leistungsindikatoren hinzufügen* gelangen.

Weitere Merkmale der Darstellung können Sie in den Registern *Grafik* und *Darstellung* verändern.



*Eigenschaften von Leistungsüberwachung*

## Datensammlersatz erstellen



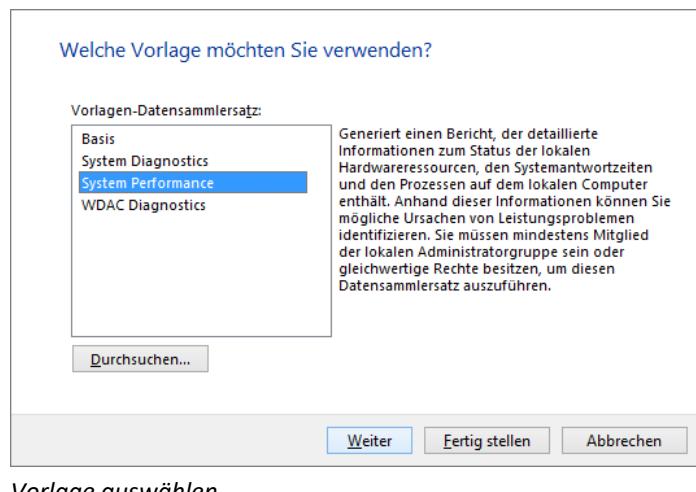
Mithilfe von Datensammlersätzen können Sie verschiedene Überwachungskonstellationen erstellen und speichern, die Sie jederzeit wieder aufrufen und auch auf anderen Systemen weiterverarbeiten können. Sie sollten sich angelehnen, stets einen neuen Satz anzufertigen, anstatt jedes Mal alle Messdaten neu zusammenzustellen. Die Datensammlersätze können auf Vorlagen basieren, Sie können jedoch auch neue Sätze zusammenstellen und bestehende Sätze verändern. Durch die Datensammlersätze wird die Leistungsüberwachung erst zu einem brauchbaren Werkzeug.

- ▶ Wechseln Sie in der Konsole zum Konsolenelement *Datensammlersätze - Benutzerdefiniert* und klicken Sie mit der rechten Maustaste auf den Unterknoten *Benutzerdefiniert*.
- ▶ Rufen Sie im Kontextmenü *Neu - Datensammlersatz* auf.
- ▶ Geben Sie einen Namen für den neuen Datensammlersatz ein.
- ▶ Wählen Sie aus, ob Sie eine Vorlage verwenden oder manuell einen komplett neuen Satz erstellen wollen, und klicken Sie auf *Weiter*.

## Vorlage verwenden

Wenn Sie eine Vorlage verwenden wollen, können Sie auf der nächsten Seite aus den vorhandenen Datensammlersatzvorlagen auswählen. Es handelt sich dabei um XML-Dateien, die standardmäßig im System32-Verzeichnis liegen. Sie können auch selbst erstellte Datensammlersätze als Vorlage verwenden.

- ▶ Wählen Sie eine Vorlage aus der Liste aus oder klicken Sie auf *Durchsuchen*, um eine Vorlage an einem anderen Speicherort auszuwählen.
- ▶ Klicken Sie auf *Weiter*.



### Vorgang abschließen

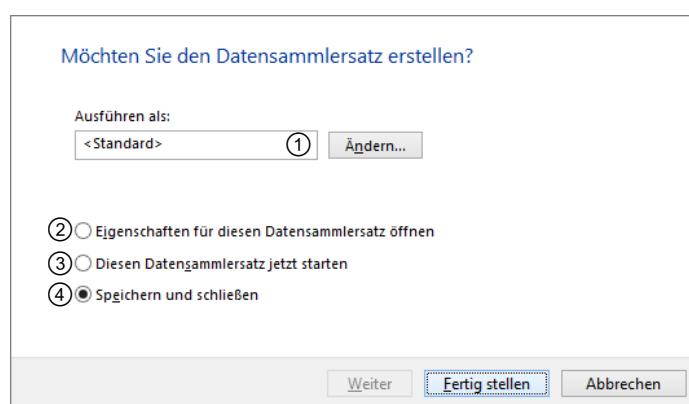
- Bestimmen Sie den Speicherort des Datensammlersatzes und klicken Sie auf *Weiter*.

Auf der letzten Dialogseite können Sie andere Anmeldeinformationen eintragen ①, nach der Fertigstellung den Eigenschaftendialog aufrufen ②, den Datensammlersatz starten ③ oder speichern und schließen ④.

- Klicken Sie auf *Fertig stellen*.

Damit haben Sie den Datensammlersatz erfolgreich eingerichtet.

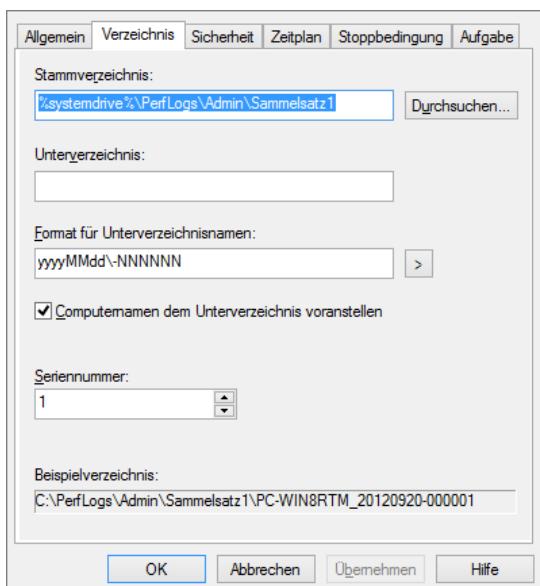
Der Datensammlersatz wird gespeichert und ist in der Leistungsüberwachung unter *Leistung - Datensammlersätze - Benutzerdefiniert* zu finden.



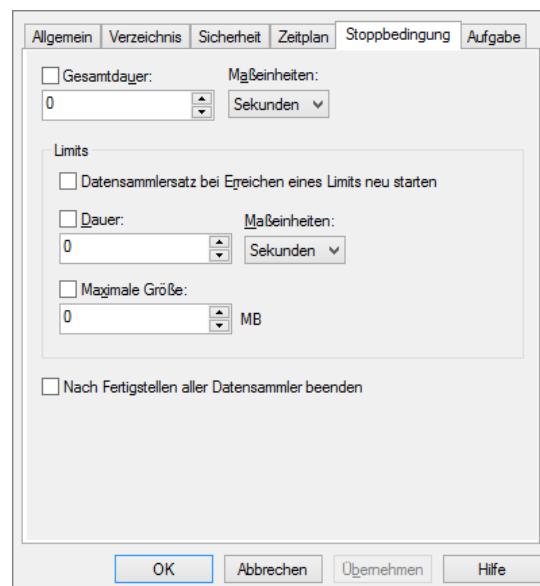
*Fertigstellung des Datensammlersatzes*

### Eigenschaften des Satzes ändern

- Legen Sie im Eigenschaftendialog des Datensammlersatzes im Register *Allgemein* eine Beschreibung und Schlüsselwörter für den Satz fest.
- Legen Sie im Register *Verzeichnis* den Speicherort und das Benennungsschema für die Protokolle fest.
- Legen Sie im Register *Zeitplan* fest, wann eine Datensammlung beginnen soll.
- Definieren Sie im Register *Stoppbedingung*, nach welcher Zeitspanne oder nach welchem Ereignis eine Datensammlung enden soll.
- Legen Sie im Register *Aufgabe* fest, welches Programm oder Skript ausgeführt werden soll, nachdem die Datensammlung beendet wurde.
- Nachdem Sie alle Einstellungen abgeschlossen haben, klicken Sie auf *Übernehmen* und *OK*.



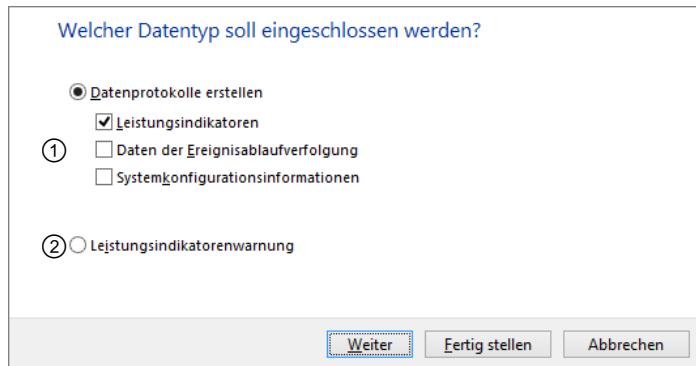
*Eigenschaften des Datensammlersatzes ändern*



## Eigenen Datensammlersatz zusammenstellen

Wenn Sie sich entschlossen haben, einen neuen Satz zu erstellen, können Sie auf der nächsten Seite auswählen, welche Datentypen in den Datenprotokollen enthalten sein sollen ①. Alternativ können Sie lediglich Leistungsindikatorwarnungen anzeigen lassen und auf Protokolle verzichten ②.

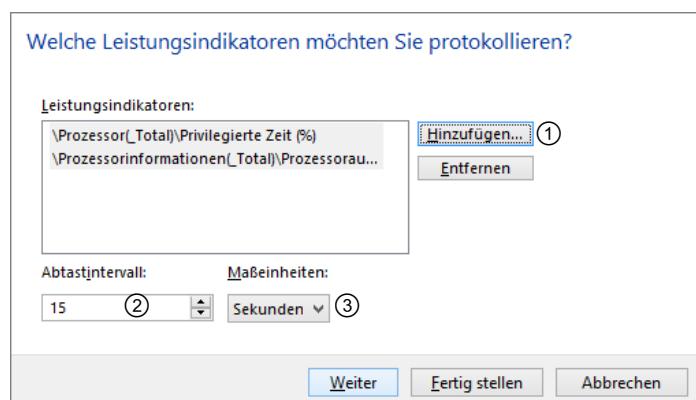
- Treffen Sie Ihre Auswahl und klicken Sie auf *Weiter*.



### Datenprotokolleinträge oder Leistungsindikatorwarnung

- Fügen Sie die zu überwachende Systemkomponente unter ① hinzu.
- Geben Sie mithilfe der Felder ② und ③ das gewünschte Abtastintervall ein und klicken Sie auf *Weiter*.

Anschließend läuft der Vorgang wie oben beschrieben ab: Sie können einen Speicherort und abweichende Anmeldeinformationen angeben und schließlich können Sie entscheiden, was nach der Fertigstellung passieren soll.



### Messwerte hinzufügen

## 16.5 Wartungscenter

### Mehr Sicherheit mit Windows 10

Im Wartungscenter von Windows 10 werden viele Prozesse, die mit der Sicherheit und Wartung eines Computers zusammenhängen, in einem Bereich übersichtlich zusammengefasst.

Das Wartungscenter überwacht die Aktivität folgender Komponenten:

- ✓ Windows-Firewall und Windows Update sowie Sicherung,
- ✓ Schutz vor Spyware und Virenschutz, Suche nach Lösungen für Problemberichte,
- ✓ Benutzerkontensteuerung und Netzwerkzugriffsschutz.

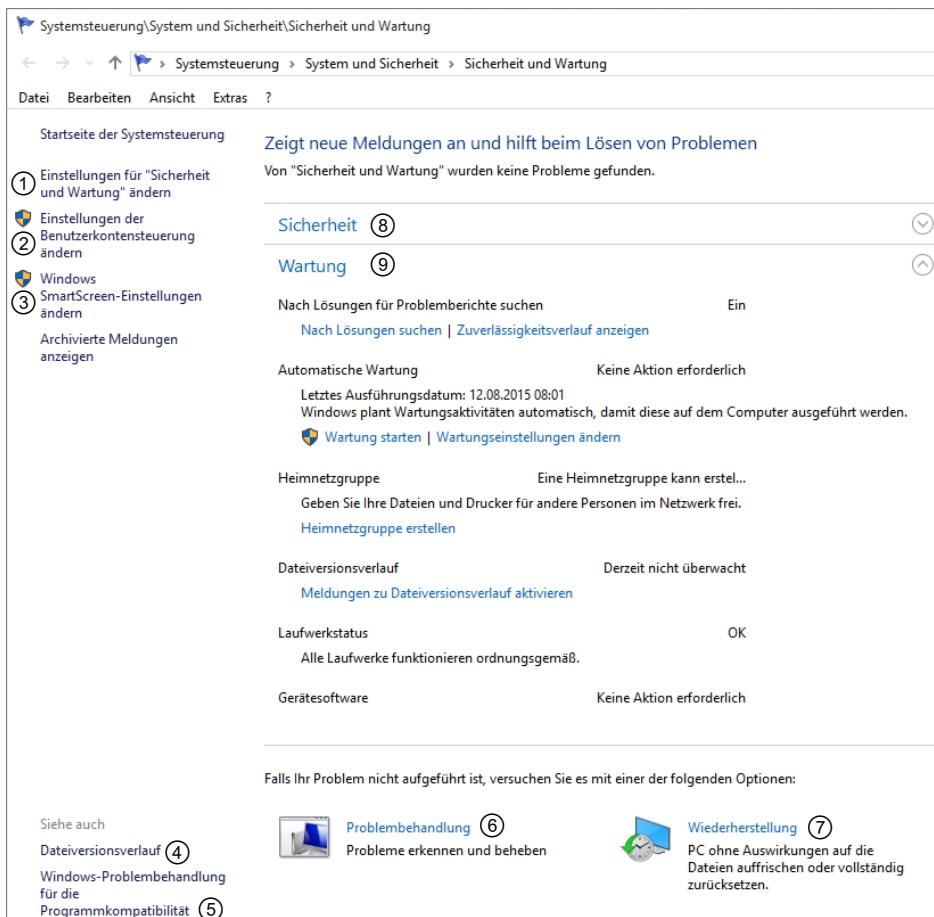
Gibt es mit einer dieser Komponenten ein Problem, so gibt das Wartungscenter dem Benutzer eine entsprechende Warnmeldung aus. Dies soll zum Beispiel den Benutzer auch warnen, wenn schädliche Software sicherheitsrelevante Prozesse wie die Firewall oder den Antivirus deaktiviert hat.

### Mit dem Wartungscenter arbeiten

Falls vom System ein Problem erkannt wurde, wird dies durch eine Meldung in der Taskleiste angezeigt, über die Sie das Wartungscenter öffnen können. Sie können das Wartungscenter auch über die Systemsteuerung erreichen. Alternativ starten Sie `wscui .cpl` über das Startmenü oder das Suchfeld.

Das Wartungscenter bietet Ihnen einen schnellen Zugriff auf zahlreiche für die Sicherheit und Funktion relevante Komponenten Ihres Systems.

In der linken Spalte können Sie die Einstellungen für das Wartungscenter ①, die UAC ② und den SmartScreen ③ vornehmen und über Links direkt zum Dateiversionsverlauf (File History) ④, den Assistenzern für Kompatibilitätsbehandlung ⑤, Problembehandlung ⑥ und Wiederherstellung ⑦ gelangen. Auf der rechten Seite sind die Meldungen in die Kategorien *Sicherheit* ⑧ und *Wartung* ⑨ unterteilt.



### Schaltzentrale für Wartung und Sicherheit

Windows 10 überprüft mit dem SmartScreen-Filter alle Programme, ob diese unter Umständen gefährlich für das System sind, und sperrt diese vom Start aus.

Sie können den SmartScreen-Filter deaktivieren. Die Optionen dazu finden Sie im Wartungscenter, indem Sie auf *Windows SmartScreen-Einstellungen ändern* ③ klicken.

#### Wie soll mit unbekannten Apps verfahren werden?

Windows SmartScreen trägt zur Optimierung der Sicherheit des PCs bei, indem Sie vor dem Ausführen unbekannter Apps aus dem Internet benachrichtigt werden.

- Vor dem Ausführen unbekannter Apps aus dem Internet die Genehmigung des Administrators anfordern (empfohlen)
- Vor dem Ausführen unbekannter Apps warnen, aber keine Administratorgenehmigung erforderlich machen
- Keine Aktion (Windows SmartScreen deaktivieren)

**OK** **Abbrechen**

Einige Informationen zu den Dateien und Apps, die auf dem PC ausgeführt werden, werden an Microsoft gesendet.  
[Datenschutzerklärung](#)

#### Windows SmartScreen einstellen

Von dem Startmenü aus können Sie die Optionen schnell mit dem Befehl `smartscreensettings` erreichen.

## 16.6 Datenschutzeinstellungen in Windows 10 beachten

Den Datenschutz optimieren Sie in Windows 10 unter *Einstellungen - Datenschutz*. In den Datenschutz-Einstellungen lassen sich mit Schiebereglern viele Verbesserungen bezüglich der Sicherheit in Windows 10 erreichen.

Register	Beschreibung
Allgemein	Hier ist es empfehlenswert, dass die Option <i>Apps die Verwendung der Werbungs-ID für App-übergreifende Erlebnisse erlauben</i> deaktiviert wird. Die Option für SmartScreen-Filter für Apps aus dem App-Store sollte aktiviert bleiben. Zu jeder Option gibt es eine Erklärung.
Konto-informationen	Nach der Installation von Windows 10 können Sie hier festlegen, ob Apps das Recht erhalten, auf Informationen des Microsoft-Kontos zuzugreifen.
Kontakte	Über <i>Kontakte</i> können Sie Zugriff auf Kontakte und Mails steuern.
Kalender	Den Zugriff auf den Kalender und dessen Daten steuern Sie über <i>Kalender</i> .
Messaging	<i>Messaging</i> erlaubt die Einstellung der Rechte für Apps, die Nachrichten lesen oder erstellen können. Sind hier keine Apps aufgelistet, dann gibt es auf dem lokalen Rechner keine Apps, die den Zugriff benötigen. Die Einstellungen sollten auch dazu genutzt werden zu überprüfen, ob es aktuell Apps mit zu vielen Rechten in Windows gibt.
Hintergrund-Apps	Hier sehen Sie, welche Anwendungen im Hintergrund Daten herunterladen, Benachrichtigungen senden und Informationen auslesen.
Position, Kamera, Mikrofon	Wer seinen Windows 10-Rechner oder sein Tablet <b>mobil</b> nutzt, sollte weitere Einstellungen bezüglich des Datenschutzes vornehmen. Hier bieten sich vor allem die Menüs <i>Position, Kamera, Mikrofon</i> und <i>Funkempfang</i> an.
Position	Über <i>Position</i> lässt sich die generelle Positionserkennung für einen Rechner aktivieren oder deaktivieren. Außerdem lässt sich die aktuelle Position explizit ausblenden. Die Bewegungsdaten eines Anwenders lassen sich über den Bereich <i>Positionsverlauf</i> löschen.
Kamera, Mikrofon	Hier können Sie festlegen, welche Apps Zugriff auf die Kamera des Rechners, Notebooks oder Tablets haben. Wie bei den Bewegungsdaten, können Sie genau steuern, welche Apps Zugriff auf die Kamera haben. Das Gleiche gilt für die Verwendung des Mikrofons von Computern. Auch hierzu lassen sich dedizierte Einstellungen für Apps vornehmen.
Weitere Geräte	Über <i>Weitere Geräte</i> können Sie den Datenaustausch und die Synchronisierung mit externen Geräten einstellen. Dabei handelt es sich vor allem um Smartphones oder Tablets, die Daten mit Windows 10 synchronisieren. Sie können festlegen, ob Apps auf dem PC generell das Recht erhalten, auf das Smartphone zuzugreifen.

Über *Einstellungen - System - Benachrichtigungen und Aktionen* lassen sich Einstellungen vornehmen, welche Apps Benachrichtigungen in Windows anzeigen können. Außerdem steuern Sie hier bei *Schnelle Aktionen*, welche Apps im System im unteren Bereich des neuen Info-Centers angezeigt werden. Dieses blendet Windows ein, wenn auf die Sprechblase neben der Uhr geklickt wird.

### Weitere Einstellungen beim Microsoft-Browser Edge vornehmen

Befehl	Beschreibung
Weitere Aktionen ... - Einstellungen	Die Browsetereinstellungen werden über den Bereich <i>Browserdaten löschen</i> gelöscht. Hier können Anwender den Browserverlauf, Cookies, zwischengespeicherte Daten, aber auch Downloadverlauf, Kennwörter und Formulardaten aus dem Browser löschen.
Einstellungen - Erweiterte Einstellungen anzeigen	Hier lassen sich viele wichtige Einstellungen vornehmen. Im Abschnitt <i>Datenschutz und Dienste</i> sind die entsprechenden Sicherheitseinstellungen für den Browser zu finden.

## 16.7 Übung

### Mit der Systemüberwachung arbeiten

Übungsdatei: --

Ergebnisdatei: *Uebung16\_E.pdf*

1. Wie öffnen Sie die Ereignisanzeige?
2. Wo finden Sie die Datenschutzeinstellungen in Windows 10?

# 17 Die Registrierungsdatenbank

## In diesem Kapitel erfahren Sie

- ✓ Grundlagen zur Windows-10-Registrierung
- ✓ etwas über Aufbau und Funktion der Registrierungsdatenbank
- ✓ wie Sie mit einem Registrierungsseditor die Registrierungsdatenbank bearbeiten

## 17.1 Die Windows-10-Registrierung

### Aufbau und Funktion der Registrierung

Windows 10 speichert Informationen zur Konfiguration von System und Software in einer zentralen Datenbank namens **Registrierung (Registry)**. Einträge in der Registrierungsdatenbank steuern das Betriebssystem und Anwendungen sowie den Betrieb von Hardware-Komponenten und Gerätetreibern.

### Einträge in der Registrierungsdatenbank

Einträge in der Registrierungsdatenbank werden beispielsweise automatisch geändert und ergänzt, wenn

- ✓ ein neues Anwendungsprogramm oder eine neue Hardware-Komponente installiert wird;
- ✓ Einstellungen im Betriebssystem, etwa die Bildschirmauflösung, verändert werden;
- ✓ Einstellungen in Anwendungsprogrammen geändert werden;
- ✓ Hardware-Komponenten anders konfiguriert werden.

Die Registrierungsdatenbank kann auch manuell bearbeitet werden, um bestimmte Änderungen durchzuführen.



Ein **manueller** Eingriff in die Registrierungsdatenbank sollte nur vorgenommen werden, wenn **keine** andere Möglichkeit besteht und die Auswirkungen auf das System genau bekannt sind. Falsche Einstellungen können die Funktion von Windows 10 stark beeinflussen oder das Betriebssystem so beschädigen, dass es nicht mehr funktioniert. Durch unbeabsichtigte Registrierungsänderungen kann eine Systeminstallation so schwer beschädigt werden, dass sie nur durch eine Systemwiederherstellung repariert werden kann.

### Systemkonfiguration manuell ändern

Eine elegantere Methode zur manuellen Änderung der Systemkonfiguration ist das Erstellen von Gruppen- oder Systemrichtlinien. Ermitteln Sie deshalb vor Eingriffen in die Registrierung, ob Sie die gewünschte Einstellung nicht auch über Richtlinien vornehmen können.

### Struktur der Registrierungsdatenbank

Windows 10 speichert die Einträge der Registrierungsdatenbank hierarchisch strukturiert ab. Dazu werden vier Grundelemente verwendet:

Element	Beschreibung
Unterstruktur (Teilstruktur)	Basiselement auf der untersten Ebene der Registrierungsdatenbank, entspricht etwa dem Stammverzeichnis (root) auf einer Festplatte. Windows 10 verwendet zwei Basisschlüssel: HKEY_LOCAL_MACHINE und HKEY_USER.
Schlüssel	Element der nächsthöheren Ebene der Registrierungsdatenbank, entspricht etwa den Ordnern im Dateisystem. Kann Unterschlüssel und Einträge enthalten.

Element	Beschreibung
Unterschlüssel (Teilschlüssel)	Vergleichbar mit einem Unterordner im Dateisystem. Kann Unterschlüssel oder Einträge enthalten.
Wert (Eintrag)	Dies ist die eigentliche Konfigurationsinformation.

### Funktion der Unterstrukturen

Die Registrierungsdatenbank besteht aus fünf Unterstrukturen mit folgenden Informationen:

Unterstruktur	Abgelegte Informationen
HKEY_CLASSES_ROOT	Hier werden Daten zur Konfiguration der Anwendungsprogramme gespeichert, unter anderem auch die Verknüpfung zwischen Dateiendung und zugehörigem Programm.
HKEY_CURRENT_USER	Diese Unterstruktur enthält die Konfiguration für den aktuell angemeldeten Benutzer. Dieser Zweig wird als Kopie der entsprechenden Einstellungen aus HKEY_USERS übernommen.
HKEY_LOCAL_MACHINE	Hier liegen die wesentlichen Informationen zur Konfiguration des lokalen Computers. Diese Unterstruktur umfasst installierte Hardware und Software. Die Einträge werden bei der Installation neuer Komponenten aktualisiert und sind benutzerunabhängig.
HKEY_USERS	Diese Unterstruktur enthält Einträge zu allen Benutzern, die bei Windows 10 eingetragen sind. Hier sind beispielsweise alle benutzerspezifischen Desktop-Einstellungen, die Bildschirm- oder Mauseinstellungen abgelegt.
HKEY_CURRENT_CONFIG	Beim Computerstart erzeugt Windows diese Unterstruktur entsprechend dem ausgewählten Hardware-Profil als Kopie von HKEY_LOCAL_MACHINE.

### Wertetypen

Die tatsächliche Einstellung einer Konfiguration wird durch den eingetragenen Wert festgelegt. Die Windows-Registrierung verwendet sechs verschiedene Datentypen für den Wert einer Konfigurationseinstellung:

Datentyp	Eigenschaften
REG_BINARY	Einzelner binärer Wert
REG_DWORD (Double Word)	Einzelner Wert aus 1 bis 10 Hexadezimalzeichen (32 Bit)
REG_QWORD (Quadruple Word)	Einzelner Wert bis 16 Hexadezimalzeichen (nur 64-Bit-Windows)
REG_SZ	Wert besteht aus einer Zeichenkette
REG_EXPAND_SZ	Wert besteht aus einer erweiterbaren Zeichenkette
REG_MULTI_SZ	Wert besteht aus mehreren Zeichenketten
REG_FULL_RESOURCE_DESCRIPTOR	Eine Ressourcenliste, die nicht konfiguriert werden kann

## 17.2 Registrierungsdaten ansehen

### Der Registrierungsseditor

Der Inhalt der Windows-Registrierungsdatenbank kann mithilfe des Registrierungsseditors *Regedit.exe* angezeigt werden.



Um mit dem Registrierungsseditor arbeiten zu können, müssen Sie an den entsprechenden Computern als Administrator angemeldet sein.

### Regedit verwenden

- Geben Sie **regedit** ein und bestätigen Sie die Meldung der Benutzerkontensteuerung mit *Ja*.

Sie sehen die Unterstrukturen ① im Fenster *Registrierungs-Editor*.

- Rufen Sie die Schlüssel ② und Unterschlüssel ③ mit Doppelklicken auf eine Unterstruktur auf.

Die einzelnen Werte ④ eines Schlüssels werden rechts angezeigt.

The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under 'Computer\HKEY\_CURRENT\_USER\Control Panel\Desktop'. The right pane lists the values for this key, including 'Standard', 'ActiveWndTrkTimeout', 'AutoColorization', 'BlockSendInputResets', 'CaretWidth', 'ClickLockTime', 'CoolSwitchColumns', 'CoolSwitchRows', 'CursorBlinkRate', 'DockMoving', 'DragFromMaximize', 'DragFullWindows', 'DragHeight', 'DragWidth', 'FocusBorderHeight', and 'FocusBorderWidth'. The status bar at the bottom shows the path 'Computer\HKEY\_CURRENT\_USER\Control Panel\Desktop'.

Name	Typ	Daten
Standard	REG_SZ	(Wert nicht festgelegt)
ActiveWndTrkTimeout	REG_DWORD	0x00000000 (0)
ActiveWndTrkTimeout	REG_DWORD	0x00000000 (0)
AutoColorization	REG_DWORD	0x00000001 (1)
BlockSendInputResets	REG_SZ	0
CaretWidth	REG_DWORD	0x00000001 (1)
ClickLockTime	REG_DWORD	0x000004b0 (1200)
CoolSwitchColumns	REG_SZ	7
CoolSwitchRows	REG_SZ	3
CursorBlinkRate	REG_SZ	530
DockMoving	REG_SZ	1
DragFromMaximize	REG_SZ	1
DragFullWindows	REG_SZ	1
DragHeight	REG_SZ	4
DragWidth	REG_SZ	4
FocusBorderHeight	REG_DWORD	0x00000001 (1)
FocusBorderWidth	REG_DWORD	0x00000001 (1)

Registrierungsdaten ansehen

### Registrierung durchsuchen

Der Registrierungsseditor bietet eine Suchfunktion, mit der beispielsweise Schlüssel und Einträge (Werte) gefunden werden können. Es wird stets nach unten gesucht, ausgehend von der momentan markierten Struktur.

- Markieren Sie den Ort, bei dem die Suche beginnen soll.
- Rufen Sie *Bearbeiten - Suchen* auf
- oder Drücken Sie **Strg F** und geben Sie die gewünschte Zeichenfolge ein.

Unter *Suchoptionen* können Sie bestimmen, ob Sie nach Schlüsseln, Werten oder Daten suchen möchten.

The screenshot shows the search options dialog. It contains a search input field 'Suchen nach:' and several checkboxes under 'Suchoptionen': 'Schlüssel' (checked), 'Werte' (checked), 'Daten' (checked), and 'Ganze Zeichenfolge vergleichen' (unchecked). There are also 'Weitersuchen' and 'Abbrechen' buttons.

Schlüssel in der Registrierung suchen

- Aktivieren Sie *Ganze Zeichenfolge vergleichen*, wenn Sie nach genau diesem Begriff suchen.

Mit **F3** können Sie erneut suchen und so schnell zur nächsten Fundstelle springen.



Bei der Suche wird nicht zwischen Groß- und Kleinschreibung unterschieden.

### Registrierungsdaten drucken

- Klicken Sie doppelt auf das Ordnersymbol des Schlüssels, dessen Inhalt Sie drucken möchten.
- Rufen Sie den Menüpunkt *Datei - Drucken* auf.
- Klicken Sie im Dialogfenster *Drucken* auf die Schaltfläche *Drucken*.

## 17.3 Registrierungsdaten bearbeiten

### Schlüssel sichern und Werte bearbeiten

Prüfen Sie, ob sich die gewünschte Konfigurationsänderung nicht mit einer Gruppenrichtlinie erreichen lässt. Falls Sie Einträge in der Registrierung bearbeiten müssen, sollten Sie zuvor eine Sicherungskopie anfertigen, indem Sie den betreffenden Teilschlüssel in eine Datei exportieren.



- ▶ Wählen Sie im Registrierungseditor den betreffenden Schlüssel aus.
- ▶ Rufen Sie den Menüpunkt *Datei - Exportieren* auf.
- ▶ Geben Sie im Dialogfenster *Registrierungsdatei exportieren* einen Ordner und einen Dateinamen an und klicken Sie auf *Speichern*.

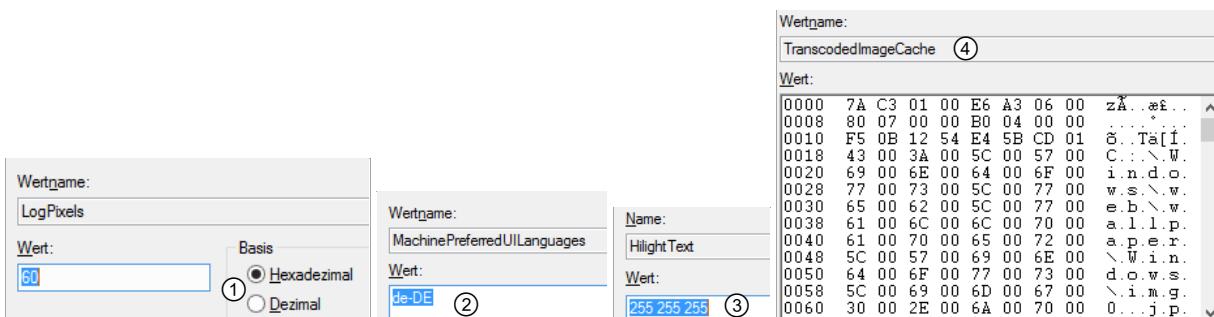
Die erzeugte Binärdatei mit der Erweiterung *.reg* wird im angegebenen Verzeichnis abgelegt und kann später für die Wiederherstellung der bestehenden Konfiguration herangezogen werden.

### Werte ändern

- ▶ Öffnen Sie den betreffenden Schlüssel und klicken Sie doppelt auf den Wert, den Sie ändern möchten.

Je nach Datentyp des ausgewählten Wertes wird ein entsprechender Editor geöffnet. Bei D-Word-Werten können Sie zwischen Hexadezimaldarstellung und Dezimaldarstellung wählen ①. Bei mehrteiligen ② und einfachen Zeichenfolgen ③ können Sie die Werte als Text eingeben, Binärwerte werden im Hex-Editor bearbeitet ④.

- ▶ Verändern Sie den Wert wie erforderlich und bestätigen Sie mit *OK*.

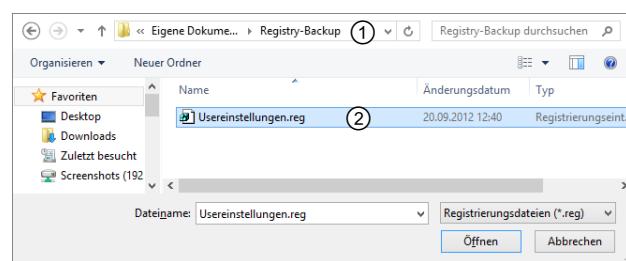


Editoren für die verschiedenen Formate DWORD, mehrteilige und einfache Zeichenfolge sowie Binärwert

### Schlüssel wiederherstellen

Wenn Sie einen Schlüssel verändert haben und das System sich anschließend nicht erwartungsgemäß verhält, können Sie die ursprüngliche Konfiguration wiederherstellen.

- ▶ Öffnen Sie im Explorer den Ordner, in dem sich die Registrierungsdatei mit dem benötigten Schlüssel befindet ①.
- ▶ Klicken Sie doppelt auf die Datei ②.
- ▶ Bestätigen Sie die angezeigte Warnung mit *Ja*.



Registrierungsdatei zur Wiederherstellung auswählen

Der Registrierungseditor überschreibt jetzt die aktuellen Daten in der Registrierung mit den Informationen aus der gespeicherten Datei und gibt danach eine entsprechende Meldung aus.

## Sperren der Registry für bestimmte Benutzer

Besteht die Gefahr, dass weitere Benutzer versuchen, Änderungen an der Registry vorzunehmen, wäre es sinnvoll, lediglich dem Administrator Zugriff auf den Registrierungs-Editor zu gewähren. Zum Sperren des Editors führen Sie die folgenden Schritte aus:

- ▶ Melden Sie sich am Computer mit dem Benutzerkonto des Benutzers an, für den der Zugriff gesperrt werden soll.
- ▶ Öffnen Sie in der Registry den Pfad `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System`. Ist er nicht vorhanden, legen Sie ihn an.
- ▶ Erstellen Sie einen neuen Wert vom Typ `DWORD` mit dem Namen `DisableRegistryTools` und setzen Sie für diesen den Wert 1.

Nachdem der Computer neu gestartet wurde, kann nur noch der Administrator den Registrierungs-Editor aufrufen.

Diese Einstellung können Sie auch über die Gruppenrichtlinien vornehmen. Sie finden die Einstellung *Zugriff auf Programme zum Bearbeiten der Registrierung verhindern* entweder über die lokalen Richtlinien (`gpedit.msc`) oder in den Gruppenrichtlinien über *Benutzerkonfiguration - Administrative Vorlagen - System*.

## Keine Installation einer .reg-Datei per Doppelklick

Standardmäßig öffnet ein Doppelklick auf eine .reg-Datei nicht den Editor, sondern führt nach einer Sicherheitsabfrage die Installation aus.

Bestätigt der Benutzer die Abfrage versehentlich, können ungewollte Registry-Änderungen erfolgen. Deshalb ist es sinnvoll, eine .reg-Datei so zu konfigurieren, dass sie nach einem Doppelklick standardmäßig den Windows-Editor öffnet, anstatt sich zu installieren. Diese Einstellung können Sie über die Registry vornehmen. Gehen Sie zum Üben wie folgt vor:

- ▶ Schreiben Sie folgende Zeilen in einen Editor und speichern Sie die Datei unter der Endung `.reg`.

```
Windows Registry Editor Version 5.00
HKCR\regfile\shell]
@=@"edit"
```

In der zweiten Zeile wird der betreffende Schlüssel aufgerufen. In der dritten Zeile verwenden Sie das Zeichen @, um den Standardwert, hier `edit`, zuzuweisen.

Der Eintrag *Zusammenführen* ist im Kontextmenü einer .reg-Datei hervorgehoben. Dieser Befehl leitet die Installation ein. Hervorgehobene Einträge kennzeichnen das Standardverhalten bei einem Doppelklick.

Nachdem Sie die obige .reg-Datei installiert haben, wird im Kontextmenü der Eintrag *Bearbeiten* hervorgehoben und somit zum Standard beim Doppelklick. Die Installation ist jetzt nicht mehr per Doppelklick möglich, sondern nur noch über den Kontextmenueintrag *Zusammenführen*.

## Tools zur Verwaltung der Registry

Neben dem herkömmlichen Tool zur Verwaltung der Registry bietet Windows 10 weitere Bordmittel, um die Registry zu bearbeiten. Sie finden die ausführliche Hilfe dieser Tools, wenn Sie in der Befehlszeile den Toolnamen mit der Bezeichnung /? aufrufen. Meistens werden in Unternehmen nachfolgend beschriebene Befehle verwendet.

## Registry in der Befehlszeile bearbeiten

Hierbei handelt es sich um ein Tool für die Eingabeaufforderung, das Sie auch in Skripts verwenden können. Mit *Reg.exe* lassen sich zum Beispiel einzelne Schlüsselstrukturen kopieren oder vergleichen. Außerdem können Sie auch die Registry eines Rechners im Netzwerk anpassen.

Wollen Sie zum Beispiel auf einem PC für mehrere Benutzer alle Registry-Einstellungen ändern, öffnen Sie zunächst die versteckte Registry-Datei *Ntuser.DAT* des jeweiligen Benutzers. Die Datei finden Sie in dessen Profilverzeichnis bei Windows 10 unter *C:\Benutzer\<Benutzername>*.

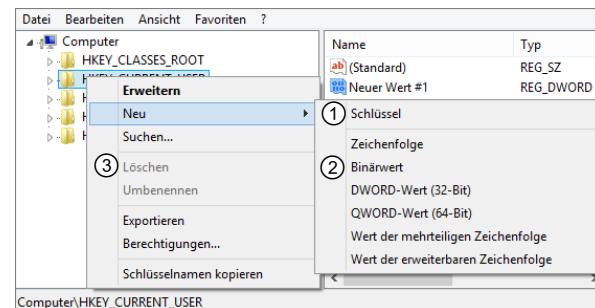
- ▶ Geben Sie für jeden Benutzer einzeln den Befehl `reg load HKU\<Benutzername> <Benutzerordner>\ntuser.dat` ein.
  - ▶ Vergleichen Sie alle Einträge eines Schlüssels mit denen Ihres eigenen Profils, indem Sie ebenfalls für jeden Benutzer einzeln die Zeile `reg compare HKU\<Benutzername>\<Schlüssel> HKCU\<Schlüssel> > c:\<Benutzer>.txt` eingeben.
- Die Unterschiede der beiden Registry-Schlüssel finden Sie anschließend in der Datei *C:\<Benutzer>.txt*.

## 17.4 Registrierungsdaten hinzufügen

### Schlüssel und Werte hinzufügen

Sie können der Registrierung manuell neue Schlüssel und Werte hinzuzufügen. Erstellen Sie jedoch vor einer Veränderung eine Sicherungsdatei der übergeordneten Unterstruktur oder des Schlüssels.

- ▶ Öffnen Sie den Registrierungseditor und klicken Sie mit der rechten Maustaste auf den Schlüssel, dem Sie einen neuen Schlüssel und Werte hinzufügen wollen.
- ▶ Rufen Sie im Kontextmenü den Menüpunkt *Neu - Schlüssel* ① auf.  
Der neue Schlüssel wird hinzugefügt.
- ▶ Benennen Sie den neuen Schlüssel nach Bedarf um.



*Schlüssel oder Einträge hinzufügen*

### Werte erstellen

- ▶ Klicken Sie mit der rechten Maustaste auf den Schlüssel, dem Sie einen neuen Wert hinzufügen wollen.
- ▶ Klicken Sie im Kontextmenü *Neu* auf den Wert, den Sie benötigen, z. B. *Binärwert* ②.  
Der neue Wert wird hinzugefügt.
- ▶ Klicken Sie doppelt auf den Wert und tragen Sie die erforderlichen Zeichen ein. Klicken Sie auf *OK*.

### Schlüssel und Werte löschen

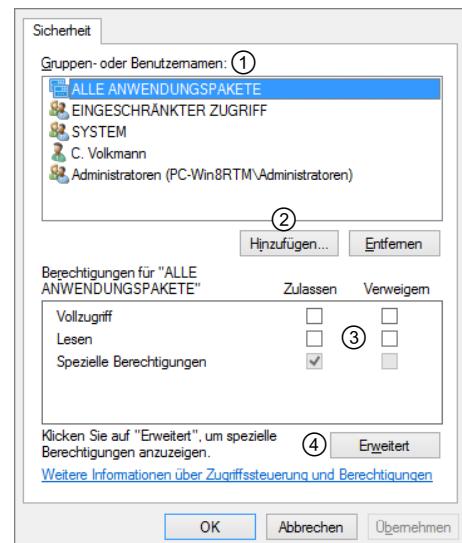
- ▶ Klicken Sie mit der rechten Maustaste auf den Schlüssel oder Wert, den Sie aus der Registrierung entfernen wollen.
- ▶ Klicken Sie auf den Kontextmenüpunkt *Löschen* ③ und bestätigen Sie die Warnmeldung mit *OK*.

## 17.5 Schlüsselsicherheit verwalten

### Zugriffsberechtigungen für Schlüssel verwalten

Registrierungsschlüssel lassen sich vor unbefugtem Zugriff sichern. Auf diese Weise lässt sich das System vor Fehlern durch manuelle Beschädigung der Registrierung schützen. Für den reibungslosen Betrieb von Windows müssen das System und auch der Benutzer ständig auf viele Bereiche der Registry zugreifen können. Sie sollten daher nur ausgewählte Bereiche vor dem Zugriff schützen und nur in Sonderfällen die Leseberechtigung entziehen.

- ▶ Klicken Sie im Registrierungsseditor mit der rechten Maustaste auf den Schlüssel, für den Sie Zugriffsberechtigungen erteilen möchten.
- ▶ Rufen Sie im Kontextmenü den Menüpunkt *Berechtigungen* auf.
- ▶ Markieren Sie im Feld *Gruppen- oder Benutzernamen* ① die Gruppe oder die Benutzer, deren Berechtigungen Sie ändern wollen.
- ▶ Klicken Sie auf *Hinzufügen* ②, um neue Benutzer oder Gruppen in die Liste aufzunehmen.
- ▶ Konfigurieren Sie mithilfe der Kontrollfelder *Zulassen* und *Verweigern* ③ die Berechtigungen.  
Wenn Sie spezielle Berechtigungen vergeben wollen, klicken Sie auf die Schaltfläche *Erweitert* ④ und verfahren Sie wie bei der Vergabe spezieller NTFS-Berechtigungen.
- ▶ Klicken Sie auf *OK*.

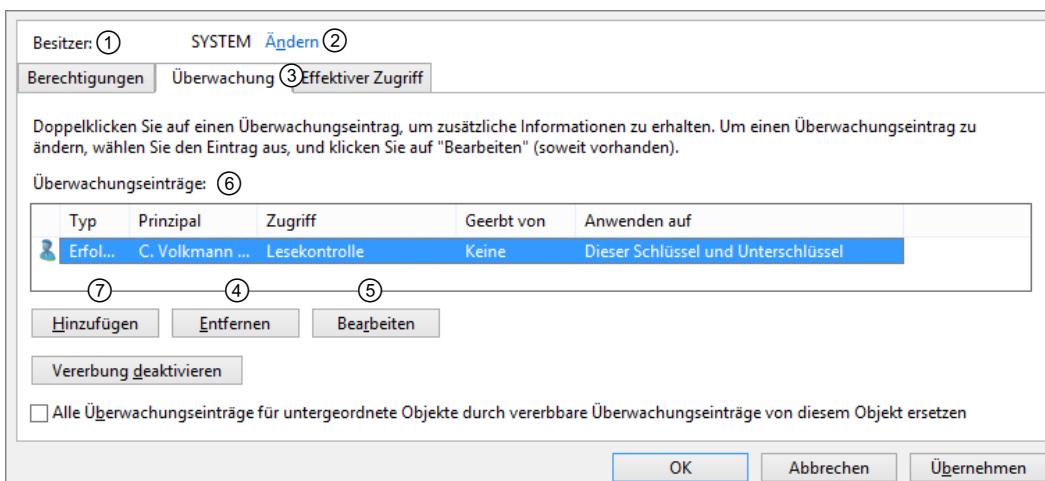


Zugriffsberechtigungen verwalten

### Besitz an einem Schlüssel übernehmen

Falls ein Registrierungsschlüssel nicht im Besitz der Gruppe *Administratoren* ist, können Sie ihn als Administrator möglicherweise nicht verwalten. Sie müssen dann den Besitz an diesem Schlüssel übernehmen, beispielsweise um ihn zu löschen. Seien Sie hier besonders vorsichtig, denn diese Bereiche der Registry werden aus gutem Grund auf diese Weise geschützt.

- ▶ Klicken Sie im Kontextmenü des Schlüssels, den Sie in Besitz nehmen wollen, auf *Berechtigungen* und im nächsten Dialog auf *Erweitert*.  
Der aktuelle Besitzer ① des Schlüssels wird Ihnen angezeigt.
- ▶ Klicken Sie auf *Ändern* ② und wählen Sie im Folgedialog die Gruppe der Administratoren. Bestätigen Sie mit *OK*.
- ▶ Klicken Sie auf *Übernehmen* und *OK*.

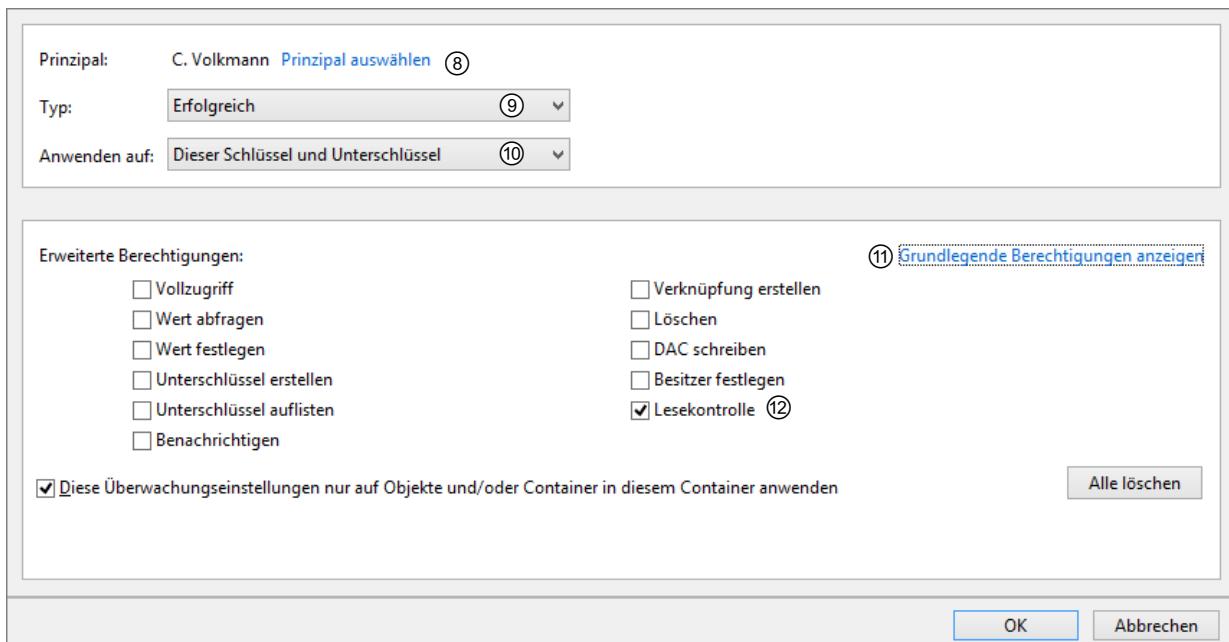


Besitz an einem Schlüssel übernehmen und Überwachung einrichten

## Schlüsselzugriffe überwachen

Der Zugriff auf die Registrierung und einzelne Schlüssel kann überwacht werden, um den Urheber von Änderungen ausfindig zu machen.

- Klicken Sie in den erweiterten Sicherheitseinstellungen des Schlüssels, für den Sie den Zugriff überwachen möchten, auf die Registerkarte *Überwachung* ③.
- Entfernen ④ oder bearbeiten ⑤ Sie vorhandene Überwachungseinträge ⑥.
- Klicken Sie auf *Hinzufügen* ⑦.
- Das Dialogfenster *Überwachungseintrag für...* wird geöffnet.
- Legen Sie unter *Prinzipal auswählen* ⑧ fest, für welche Benutzer die Überwachung gilt.
- Legen Sie im Feld *Typ* ⑨ fest, welche Aktion überwacht werden soll. Wählen Sie zwischen *Alles*, *Erfolgreich* und *Fehlgeschlagen* aus.
- Wählen Sie, ob die Überwachung für Schlüssel, Unterschlüssel oder beides gelten soll ⑩.
- Klicken Sie auf den Link ⑪, um zwischen grundlegenden und erweiterten Berechtigungen umzuschalten.



### Überwachungseintrag bearbeiten

Achten Sie darauf, dass die Lesekontrolle ⑫ aktiviert ist.

- Übernehmen Sie die Einstellungen mit *OK*, *Übernehmen* und *OK* und schließen Sie den Registrierungsseditor.

Beachten Sie, dass zusätzlich eine Gruppenrichtlinie definiert werden muss, die eine Überwachung von Objektzugriffen zulässt, bevor die Überwachung in Kraft treten kann. Gruppenrichtlinien werden mit dem entsprechenden Snap-In der MMC erstellt.



# 18 Speicherplätze und Sicherungsmethoden

## In diesem Kapitel erfahren Sie

- ✓ wie Sie einen Verbund von Datenträgern einrichten
- ✓ wie Sie den Dateiversionsverlauf (File History) zur Datensicherung einrichten
- ✓ wie Sie gesicherte Daten wiederherstellen
- ✓ wie die automatische Systemwiederherstellung arbeitet

## 18.1 Speicherplätze – Speicherpools und virtuelle Datenträger

Sowohl in Firmen als auch in Privathaushalten steigt der Bedarf an Speicherplatz, auf dem persönliche Dateien und Multimediainhalte abgelegt und verfügbar gemacht werden können. Windows 10 führt mit den **Speicherpools** und **Speicherplätzen (virtuellen Datenträgern)** die Wege zur Bereitstellung von Speicherplatz fort. Für die Verfügbarkeit ist zunehmend unwichtiger zu wissen, auf welchem Datenträger eine Datei tatsächlich liegt. Viel wichtiger ist, dass die Informationen stets auf einfache Weise zugänglich sind. Kurz gesagt, die Speicherplätze von Windows 10 sind eine lokale Speicher-Cloud.

### Speicherpools

Hierbei handelt es sich um eine Ansammlung mehrerer physischer Datenträger, die zu einem Pool zusammengeschlossen werden. Bei den Datenträgern kann es sich um eingebaute oder externe Festplatten, Solid-State-Disks (SSD), USB-Sticks und andere Flashspeicher handeln. Möglich (wenn auch nicht sinnvoll) ist sogar die Verwendung virtueller Festplatten. Optische Laufwerke sind nicht geeignet (auch nicht mit wiederbeschreibbaren Medien). Die Größe eines Speicherpools und die Anzahl von Datenträgern sind praktisch unbegrenzt.

### Virtuelle Datenträger

Jeder Speicherpool kann einen oder mehrere Speicherplätze enthalten. Diese logischen Datenträger können mit einem Laufwerkbuchstaben versehen und wie üblich vom System angesprochen werden. Aus Sicht von Windows unterscheidet sich so ein virtuelles Volume nicht von einer gewöhnlichen Festplattenpartition. Speicherplätze werden hauptsächlich verwendet, um mit der Vergabe von Laufwerkbuchstaben und Bezeichnungen sowohl für Anwendungen als auch für den Benutzer den gewohnten Rahmen zu schaffen.

### Schlanke Speicherzuweisung mit Thin Provisioning

Bei der Erstellung von Speicherplätzen kann ähnlich wie bei dynamischen virtuellen Festplatten mehr Speicherplatz zugeteilt werden, als physisch im Speicherpool verfügbar ist. Sobald der physische Speicherplatz zur Neige geht, wird vom Speicherplatz eine Warnmeldung ausgegeben. Daraufhin kann der Speicherplatz aufgestockt werden, indem weitere Festplatten angeschlossen werden. Dieses Konzept nennt man **Thin Provisioning** oder schlanke Speicherzuweisung.

Alle Speicherplätze in einem Speicherpool teilen den physisch vorhandenen Speicherplatz unter sich auf. Wenn also in einem Speicherplatz durch das Löschen von Dateien Platz freigemacht wurde, steht dieser Platz anschließend auch den anderen Speicherplätzen zur Verfügung.

## Speicherplatz planen

Es gibt eine Reihe von Überlegungen, die Sie vor der Einrichtung des Speicherplatzes berücksichtigen sollten:



- ✓ Vor der Einrichtung eines Speicherpools sollten Sie alle dafür vorgesehenen Datenträger mit dem System verbinden bzw. einbauen. Bevorzugen Sie für Speicherpools interne Laufwerke.
- ✓ Alle Daten auf einem Datenträger gehen verloren, sobald er einem Speicherpool hinzugefügt wird.
- ✓ Alle Daten eines Datenträgers, der aus einem Speicherpool entfernt wurde, sind unlesbar.
- ✓ Vermeiden Sie den Zusammenschluss von Datenträgern mit völlig unterschiedlichen Leistungsdaten in einem Speicherpool, z. B. keine 1-Terabyte-Festplatte zusammen mit einem 1-GB-USB-Stick.
- ✓ Alle Datenträger des Speicherpools müssen ständig angeschlossen und eingeschaltet sein. Externe Datenträger dürfen also nicht entfernt werden, solange der Speicherpool existiert.
- ✓ Die neuartigen Speicherplätze können ausschließlich von Windows 8/8.1/10 oder Windows Server 2012/2012 R2/2016 verwendet werden. Alle anderen Betriebssysteme können nicht darauf zugreifen. Erstellen Sie aber Freigaben auf diesen Speicherplätzen, sind diese auch für andere Systeme erreichbar.
- ✓ Speicherplätze können umbenannt und vergrößert, jedoch nicht verkleinert werden.
- ✓ Der Resilienztyp (Spiegelung, Parität, ohne) eines Speicherplatzes kann nicht geändert werden.
- ✓ Es gibt bisher kaum Erfahrungswerte in Bezug auf Zuverlässigkeit und Datenwiederherstellung.

## Datensicherheit

Die Datensicherheit kann mithilfe von Spiegelungsverfahren (mehrfache Speicherung auf verschiedenen Datenträgern) oder Paritätsinformationen, die eine Rekonstruktion der Daten auch nach Ausfall eines Datenträgers ermöglichen, erhöht werden. Die dabei eingesetzten Verfahren erfüllen in etwa dieselbe Funktion wie die RAID-Level 1 und 5, sind aber nicht gleichzusetzen.

Bei der **Spiegelung** (Mirroring) werden die Daten auf mindestens zwei Datenträgern gespeichert, sodass selbst bei Ausfall eines Datenträgers die Daten noch vorhanden sind. Bei der 3-Wege-Spiegelung dürfen sogar 2 Datenträger ausfallen, ohne dass dabei Daten verloren gehen. Bei Verwendung von **Parität** (Parity) werden Paritätsinformationen für die Dateien des einen Datenträgers auf den anderen Datenträgern gespeichert und umgekehrt. Aus diesen Paritätsinformationen können die Daten bei Ausfall des Datenträgers rekonstruiert werden. Parität benötigt weniger Speicherplatz als eine Spiegelung, die Schreibvorgänge belasten den Prozessor jedoch spürbar und sind erheblich langsamer. Am schnellsten ist die Raid-0-ähnliche Variante ohne Ausfallsicherheit (keine Resilienz / No Resiliency). Sie sollten diesen Typ jedoch wegen der großen Ausfallwahrscheinlichkeit nicht verwenden.

Verwenden Sie Spiegelung für alle Laufwerke mit gemischten Dateien, die sich häufig ändern, und Parity für Laufwerke mit großen Dateien wie z. B. Filmen, die sich selten ändern und wenig Schreibzugriffe erfordern, denn besonders die Schreibzugriffe sind mit Parität wesentlich langsamer als bei den anderen Modi.



Bevor Sie den Speicherplätzen von Windows 10 Ihre wichtigen Daten anvertrauen, sollten Sie eine Kopie Ihres Datenbestands anfertigen. Bei der Verwendung neuer Speichertechnologien sollten Sie stets kritisch und vorsichtig vorgehen.



## Speicherpool einrichten

Es ist möglich, einen Speicherpool mit einem einzigen Datenträger zu erstellen. Wenn schon ein Speicherpool existiert, können Sie entweder Datenträger hinzufügen oder einen weiteren Speicherpool erstellen. Mehrere Pools sorgen für vollständige physische Trennung der Daten, was im Hinblick auf Datensicherheit vorteilhaft sein kann.

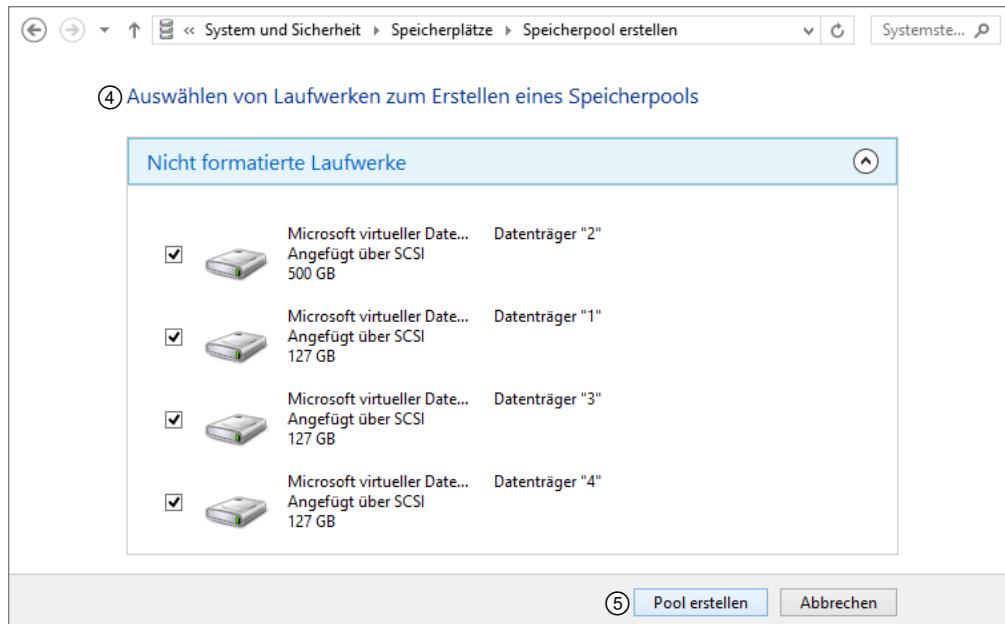
- ▶ Geben Sie **speicherpl** ein und starten Sie **Speicherplatz verwalten**.
- ▶ Bestätigen Sie mit **↵**, um die Speicherplatzverwaltung zu öffnen.  
Alternativ können Sie die Speicherplätze auch über die Systemsteuerung erreichen.

Im Dialog *Speicherplätze* können Sie existierende Speicherpools und Speicherplätze managen. Außerdem können Sie von hier aus zu den Einstellungen für den Dateiversionsverlauf (File History) ① und BitLocker ② gelangen.



### Speicherplätze verwalten

- Um einen neuen Pool zu erstellen, klicken Sie auf *Neuen Pool und Speicherplatz erstellen* ③.
- Wählen Sie aus den verfügbaren Datenträgern aus, welche in den neuen Pool aufgenommen werden sollen ④.
- Klicken Sie auf *Pool erstellen* ⑤.



### Auswahl der verfügbaren Laufwerke

Sie können jederzeit weitere Laufwerke zu einem Pool hinzufügen, es ist jedoch nicht vorgesehen, dass Sie Laufwerke aus dem Pool wieder entfernen.

## Speicherplatz erstellen

Nach der Erstellung des Pools geht es im nächsten Dialog um die Einrichtung eines Speicherplatzes. Wenn Sie hier auf *Abbrechen* klicken, können Sie den Speicherplatz auch später erstellen.

- Weisen Sie dem Speicherplatz einen Namen ① und einen Laufwerkbuchstaben sowie das Dateisystem ② zu.

Der Name entspricht der Laufwerksbezeichnung, wie sie hinterher im Datei-Explorer zu sehen ist.

- Stellen Sie unter *Resilienztyp* ③ die Ausfallsicherheit des Speicherplatzes ein.

Falls Sie mehrere Speicherplätze in Ihrem Pool haben, kann jedes dieser virtuellen Volumes einen anderen Resilienztyp haben. Die gesamte Poolkapazität ④ ist die Gesamtgröße des Speicherpools, die verfügbare Poolkapazität ⑤ zeigt an, wie viel davon noch für einen neuen Speicherplatz verfügbar ist.

- Weisen Sie unter *Größe (Maximum)* ⑥ dem neuen Speicherplatz eine Maximalgröße zu.

Name, Resilienztyp und Größe für den Speicherplatz eingeben		
Name und Laufwerkbuchstabe		
Name:	Speicherplatz ①	
Laufwerkbuchstabe:	E: ②	
Dateisystem:	NTFS	
Resilienz		
Resilienztyp: ③	Zwei-Wege-Spiegelung	
<small>i Bei einem Speicherplatz mit Zwei-Wege-Spiegelung werden zwei Kopien Ihrer Daten geschrieben, sodass die Daten vor dem Ausfall eines einzelnen Laufwerks geschützt sind. Für einen Speicherplatz mit Zwei-Wege-Spiegelung sind mindestens zwei Laufwerke erforderlich.</small>		
Größe		
Gesamte Poolkapazität:	378	GB ④
Verfügbare Poolkapazität:	378	GB ⑤
Größe (Maximum):	187	GB ⑥
Einschließlich Resilienz:	374	GB ⑦
<small>i Ein Speicherplatz kann größer sein als die im Speicherpool verfügbare Kapazität. Wenn die Kapazität im Pool knapp wird, können Sie weitere Laufwerke hinzufügen.</small>		
⑧ Speicherplatz erstellen		Abbrechen

Diese Maximalgröße kann durch das Thin Provisioning sogar über der physischen Poolgröße liegen. Bei *Einschließlich Resilienz* ⑦ wird angezeigt, wie viel Platz dieser Speicherplatz im Pool maximal belegen kann. Je nach eingestellter Sicherheit ist dies entweder die Größe des logischen Laufwerks (keine Resilienz), die 1,5-fache Größe (Parität), die doppelte Größe (Zwei-Wege-Spiegelung) oder die dreifache Größe (Drei-Wege-Spiegelung).

- Übernehmen Sie die Einstellungen und erstellen Sie einen neuen Speicherplatz ⑧.

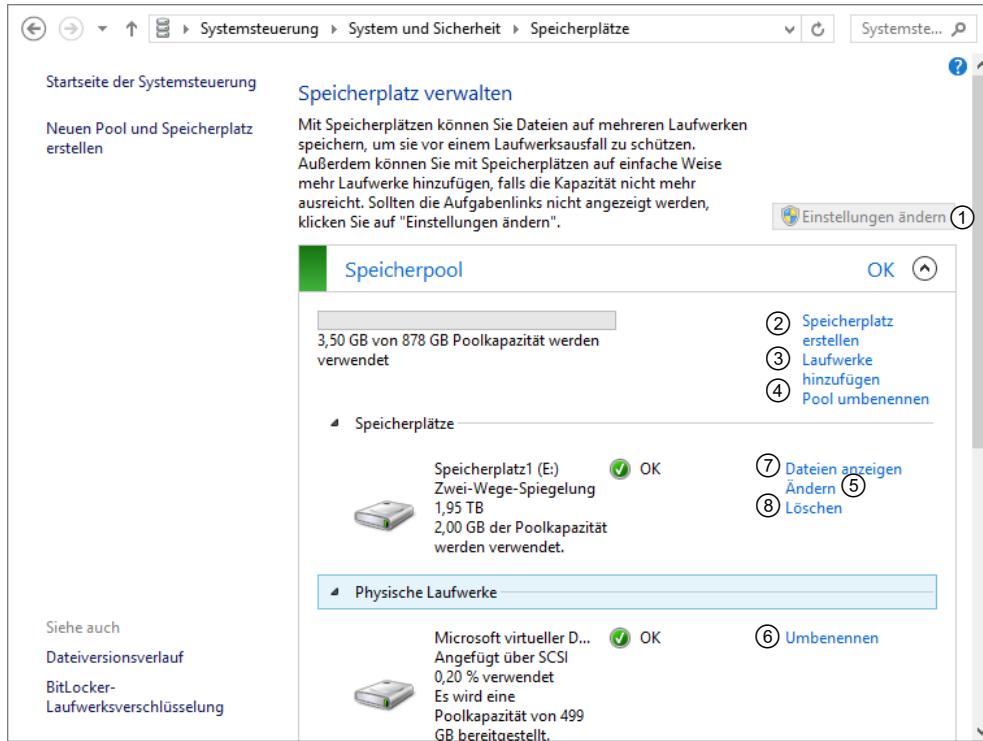
## Weitere Einstellungen an Speicherpools und Speicherplätzen

Bevor Sie weitere Einstellungen vornehmen, bedenken Sie, dass falsche oder ungewollte Einstellungen in der Verwaltung der Speicherplätze schnell zu totalem Datenverlust führen können. Um weitere Einstellungen am bestehenden Speicherpool und den darin enthaltenen Speicherplätzen vornehmen zu können, benötigen Sie Administratorrechte.

- Klicken Sie auf *Einstellungen ändern* ① und bestätigen Sie die UAC-Meldung.

Sie sehen eine Übersicht über alle vorhandenen Pools und Speicherplätze. Sie können...

- ✓ in einem Pool einen neuen Speicherplatz erstellen ②, zusätzliche Datenträger zum Pool hinzufügen ③ oder den Pool umbenennen ④.
- ✓ außerdem bestehende Speicherplätze ändern ⑤ oder physische Laufwerke umbenennen ⑥.
- ✓ sich einen Speicherplatz im Datei-Explorer anzeigen lassen ⑦ oder ihn löschen ⑧.



### Übersicht über Pools und Spaces



Es ist möglich, die Größe eines Speicherplatzes zu erweitern, er kann jedoch nicht verkleinert werden. Ebenso wenig ist es möglich, den Resilienztyp nachträglich zu ändern.

## 18.2 Dateisicherung

### Klassische Sicherungsarten

Auch wenn in Windows 10 die Dateisicherung mit ihren unterschiedlichen Sicherungsarten für den Anwender kaum noch nachvollziehbar ist, sollten Sie die verschiedenen Sicherungsarten und -strategien kennen, die seit Jahrzehnten erfolgreich im Einsatz sind:

<b>Normale Sicherung</b>	Jede Datei wird gesichert und als gesichert markiert (Voll-Backup).
<b>Kopiesicherung</b>	Jede Datei wird gesichert, aber nicht als gesichert markiert.
<b>Tägliche Sicherung</b>	Jede Datei in einem ausgewählten Pfad, die das Datum des aktuellen Tages trägt, wird gesichert, aber nicht als gesichert markiert.
<b>Inkrementelle Sicherung</b>	Nur veränderte oder ungesicherte Dateien werden gesichert und als gesichert markiert. Der Zeitaufwand für die Sicherung ist niedriger, der für die Wiederherstellung höher als bei einer differenziellen Sicherung.
<b>Differenzielle Sicherung</b>	Nur veränderte oder ungesicherte Dateien werden gesichert, aber nicht als gesichert markiert. Der Zeitaufwand für die Sicherung ist höher, der für die Wiederherstellung niedriger als bei einer inkrementellen Sicherung.



Um eine Datei als gesichert zu markieren, verwendet Windows das sogenannte Archivattribut. Dieses Dateiattribut wird automatisch immer dann aktiviert, wenn eine neue Datei erstellt oder eine bestehende verändert wird. Wird eine Datei verschoben, hat dies keinen Einfluss auf ihr Archivattribut. Bei einer normalen (auch als Komplettsicherung bezeichnet) und bei einer inkrementellen Sicherung werden diese Archivattribute wieder deaktiviert. Sie können ein Archivattribut auch manuell verändern, indem Sie im Datei-Explorer den Kontextmenüpunkt *Eigenschaften* der betreffenden Datei auswählen, dort auf die Schaltfläche *Erweitert* klicken und das Kontrollfeld *Datei kann archiviert werden* aktivieren oder deaktivieren.

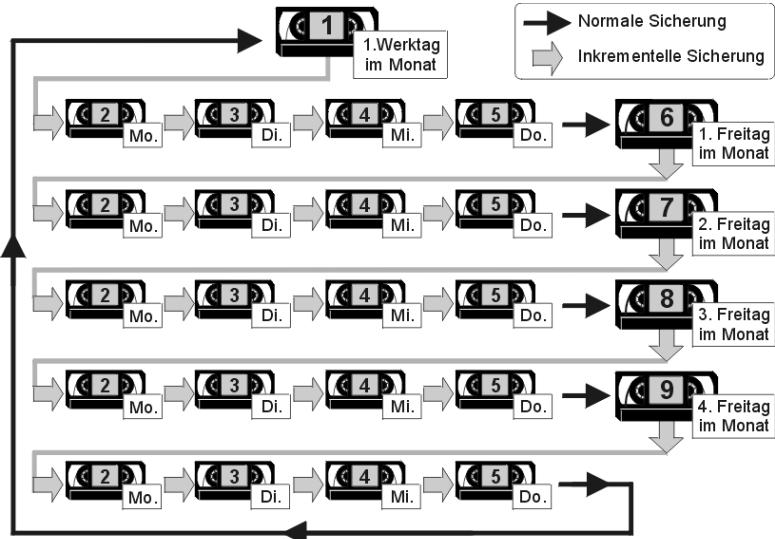
### Klassische Sicherungsstrategien

Vor der Datensicherung sollten Sie sich einen genauen Plan zurechtlegen, wie Sie vorgehen wollen. Berücksichtigen Sie dabei sowohl den Wert der Daten als auch die Häufigkeit der Änderungen sowie den zeitlichen und materiellen Aufwand für Sicherung und eine eventuelle Wiederherstellung.

Angenommen, Ihre Daten werden täglich (Montag bis Freitag) geändert, und Sie möchten diese Änderungen ab dem Monat Januar täglich sichern. Beginnen Sie Ihre Datensicherung mit einer normalen Sicherung, auch als VollBackup bezeichnet. Anschließend können Sie jeden Tag eine Datensicherung nach folgendem Plan durchführen:

Jeden Freitag wird eine normale Sicherung durchgeführt. Dazu werden die Datenträger 1 und 6 bis 9 verwendet. Mit den Datenträgern 2 bis 5 werden jeden Wochentag inkrementelle Sicherungen durchgeführt. Auf diese Weise lassen sich die Zustände der letzten 4 Freitage sowie jedes Vortages herstellen. In einer Woche lässt sich jeder Vortageszustand wiederherstellen.

Dieses Sicherungsverfahren mit einem Voll-Backup pro Monat und Woche mit täglichen inkrementellen Backups ist auch als **Großvater-Vater-Sohn-Backup** bekannt.



Sicherungsstrategie mit vierwöchiger Sicherheit und täglicher Sicherheit

Da die Datenträger 2 bis 5 im Rotationsverfahren mehrmals benutzt werden, sollten sie nach einer gewissen Zeit erneuert werden.

Der Vorteil einer solchen Strategie besteht darin, dass neben der Version des Vortages, die vor allem bei Hardware-Fehlern wichtig ist, auch der Zustand von vor mehreren Wochen wiederhergestellt werden kann. So kann z. B. ein Zustand wiederhergestellt werden, der vor der Infektion mit einem Virus lag, das erst nach einiger Zeit aktiv wurde.

### 18.3 Sicherungen mit dem Dateiversionsverlauf

Die regelmäßige Sicherung der Datenbestände bietet Schutz vor Datenverlusten, die beispielsweise durch irreparable Festplattenfehler oder Computerviren verursacht werden können. Daher sollten Sie in regelmäßigen Abständen eine Sicherung des Systems und vor allem Ihrer persönlichen Dateien durchführen.

Bei traditionellen Backup-Konzepten läuft dieser Vorgang vollkommen getrennt vom täglichen Betrieb ab. Dort wird unterschieden zwischen Voll-Backups, inkrementellen und differenziellen Sicherungen und verschiedene Datenträger werden nach dem Großvater-Vater-Sohn-Prinzip rotiert. Die Sicherungsmedien werden dann an einem sicheren Ort verwahrt. Während das klassische Backup in Firmennetzwerken weiterhin eingesetzt wird, verlieren all diese Mechanismen weitestgehend ihre Bedeutung, wenn Sie den **Dateiversionsverlauf** verwenden.

## Funktionsweise des Dateiversionsverlaufs

Der Dateiversionsverlauf vereint klassische Sicherungskonzepte und die aus älteren Windows-Versionen bekannten *Vorherigen Dateien*. Das Prinzip ist einfach: Auf einer Netzwerkfreigabe oder einem zweiten Datenträger (bzw. einem Speicherplatz) werden in einstellbaren Abständen automatisch Sicherungskopien aller geänderten Benutzerdateien gespeichert. Dabei sorgt die Differenzialkomprimierung durch das Vergleichen von Dateien auf Bit-Ebene dafür, dass nur geänderte Dateibestandteile gespeichert werden. Durch dieses Verfahren verschwimmt die Grenze zwischen Voll-Backup und inkrementellem Backup, denn von außen betrachtet wird jedes Mal ein Voll-Backup durchgeführt, in Wirklichkeit werden aber ähnlich wie beim inkrementellen Backup nur geänderte Daten geschrieben.

Damit für den sinnvollen Einsatz des Dateiversionsverlaufs das Backup-Medium nicht permanent mit dem Computer verbunden sein muss, wird für die Speicherung ein Offlinecache auf dem Quelllaufwerk verwendet. Die Größe des Zwischenspeichers kann zwischen 5 und 20 % der Laufwerkskapazität eingestellt werden. Sobald das Backup-Laufwerk dann wieder verfügbar ist, werden die Verlaufsdaten automatisch abgeglichen. Ähnlich wie Time Machine von Apple schützt der Dateiversionsverlauf vor versehentlichem Löschen und kann sozusagen die Zeit zurückdrehen. Sie können z. B. Word-Dokumente auf den Stand der letzten Stunden zurückversetzen oder eine misslungene Fotoretusche rückgängig machen. Falls der Backup-Datenträger ständig mitläuft, schützt er sogar vor Datenverlust durch den Ausfall des Quell-Datenträgers, wird durch den Dauerbetrieb im Gegenzug allerdings ebenfalls anfälliger für mechanische Fehler.

Der Dateiversionsverlauf möchte dem Benutzer alle Sorgen abnehmen, wenn es um eine regelmäßige und sinnvolle Datensicherung und um die Verwaltung älterer Dateiversionen geht. Er erfüllt die Rolle eines magischen Papierkorbs mit Backup-Funktionen im privaten Bereich recht gut. Im Unternehmensumfeld werden die Benutzerdaten meist zentral auf einem Server oder in der Cloud gespeichert, daher ist hier allenfalls der ergänzende Einsatz sinnvoll.

## Backup-Format des Dateiversionsverlaufs

Der Dateiversionsverlauf kann für jeden Benutzer getrennt eingeschaltet und eingestellt werden. Für jeden Benutzer wird auf dem Backup-Datenträger im Ordner *File History* ein Ordner mit dem Benutzernamen erstellt. Darin wird für jeden Computer ein Ordner angelegt, worin sich im Verzeichnis *Data* die Laufwerke befinden, auf denen die Bibliotheken liegen. Über das Verzeichnis *Users* geht es zur Bibliothek des Benutzers. Somit ergibt sich das Schema wie folgt: *Laufwerk\file History\Benutzer\Computername\Laufwerk\Users\Benutzernname\Bibliothek*

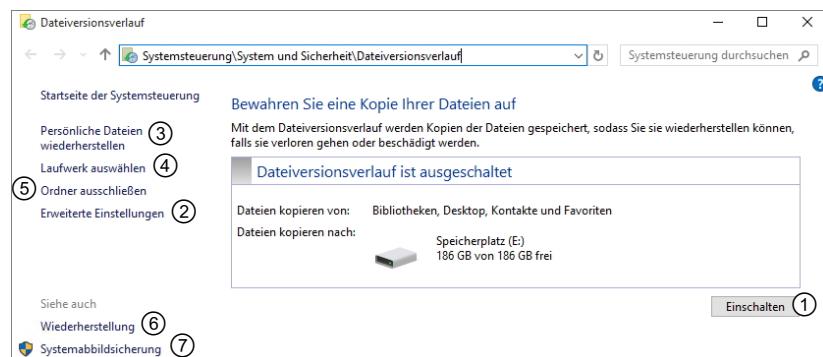


Alle Dateien im Ordner *File History* sind ganz normal lesbar. Es ist jedoch nicht empfehlenswert, auf diese Weise auf die Daten zuzugreifen. Verwenden Sie dafür die Wiederherstellungsfunktion des Dateiversionsverlaufs.

## Dateiversionsverlauf einschalten

- ▶ Geben Sie *dateiversion* ein. Wählen Sie *Dateiversionsverlauf*.
- Alternativ können Sie den Dateiversionsverlauf auch über die Systemsteuerung erreichen.
- ▶ Klicken Sie auf *Einschalten* ①, um den Dateiversionsverlauf einzuschalten.
- ▶ Wählen Sie bei mehreren Datenträgern im nächsten Dialog den Speicherort aus. Bestätigen Sie Ihre Auswahl mit *OK*.

Die File History ist nun eingeschaltet und fertigt gemäß den Einstellungen ② Kopien Ihrer Bibliotheken an.



Der Dialog für den Dateiversionsverlauf

Im Hauptfenster der File History können Sie Ihre persönlichen Daten wiederherstellen ③, das Speicherlaufwerk ändern ④, Ordner von der Sicherung ausschließen ⑤ oder in den erweiterten Einstellungen z. B. die Backup-Intervalle ② ändern. Außerdem gelangen Sie von hier aus zu den Optionen der Systemwiederherstellung ⑥ und zur Systemabildsicherung ⑦. Wenn der Verlauf eingeschaltet ist, können Sie über den Link *Jetzt ausführen* jederzeit manuell eine Sicherung starten.

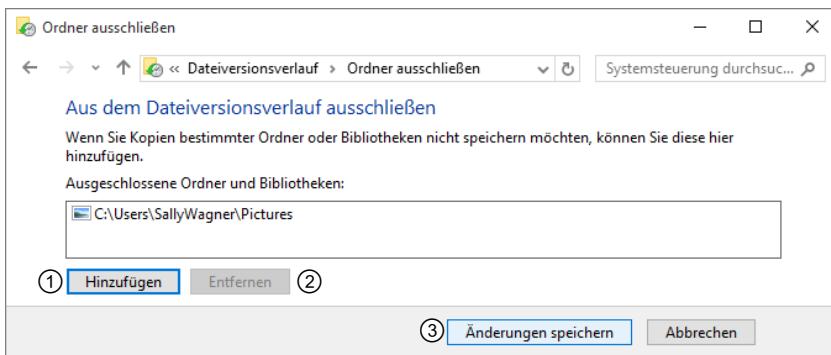
## Auswahl der Sicherungsdaten

Für das Backup von Systemordnern oder Programmen ist der Dateiversionsverlauf nicht geeignet, denn er erfasst ausschließlich die Bibliotheken des Benutzers sowie seine Kontakte, Favoriten und den Desktop. Sie müssen also alle Ordner außerhalb der Standardbibliotheken (Bilder, Dokumente, Musik und Videos) zu einer bestehenden oder neuen Bibliothek hinzufügen, damit sie im Verlauf gesichert werden können.

### Dateien vom Backup ausnehmen

Standardmäßig werden sämtliche Bibliotheks Inhalte gesichert. Das bedeutet, dass Sie bei umfangreichen Multi-mediasammlungen eine sehr große Festplatte bereitstellen müssen oder einen ausreichend großen Speicherplatz in einem Speicherpool. Sie können auch Bibliotheken oder Ordner von der Sicherung ausschließen:

- ▶ Klicken Sie im Dialog *Dateiversionsverlauf* auf *Ordner ausschließen*.
- ▶ Klicken Sie auf *Hinzufügen* ①, um einen Ort aus dem Dateiversionsverlauf auszuschließen.
- ▶ Um einen Ort wieder in den Dateiversionsverlauf aufzunehmen, markieren Sie ihn und klicken Sie auf *Entfernen* ②.
- ▶ Schließen Sie den Vorgang mit *Änderungen speichern* ③ ab.



*Ordner oder Bibliotheken ausschließen*

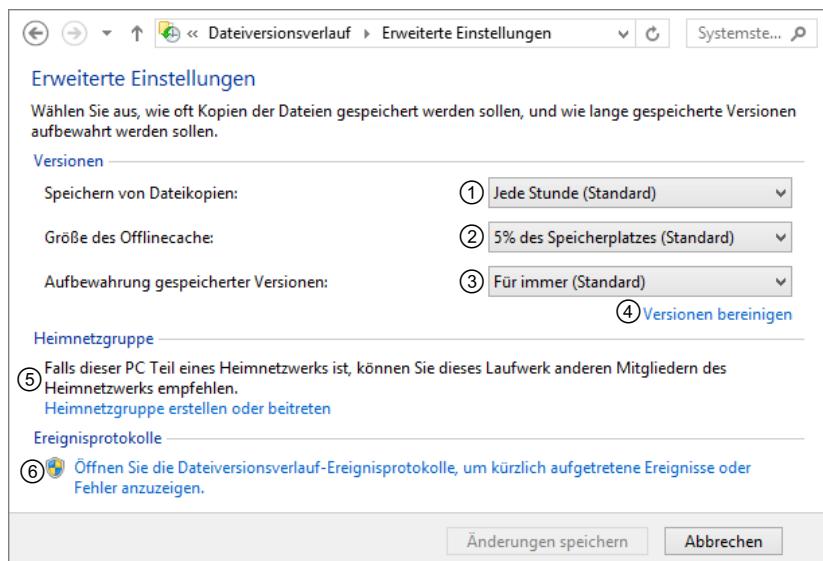
### Erweiterte Einstellungen vornehmen

Hier können Sie in Zeiträumen zwischen 10 Minuten und einem Tag einstellen, wie oft Kopien angefertigt werden ① (Standard ist eine Stunde).

Die Größe des Offlinecache bestimmt, wie viel Speicherplatz auf Ihrer Systemfestplatte für die Speicherung von den Verlaufsdateien reserviert wird ②.

Die Nutzung des Offlinecache erlaubt eine Fortsetzung des Dateiversionsverlaufs auch dann, wenn das Backup-Laufwerk nicht angeschlossen ist.

Sie können wählen, wie lange die Dateiversionen aufbewahrt werden sollen ③ (1 Monat bis 2 Jahre, für immer oder bis der Platz benötigt wird).



Unter *Versionen bereinigen* ④ können Sie ältere Dateiversionen löschen und so Speicherplatz zurückgewinnen.

Falls der Computer Mitglied in einem Heimnetzwerk ist, können Sie anderen Benutzern das Backup-Laufwerk weiterempfehlen ⑤ und zur Verfügung stellen.

Außerdem können Sie die Protokolle für den Dateiversionsverlauf in der Ereignisanzeige öffnen ⑥.

## 18.4 Dateiversionen wiederherstellen

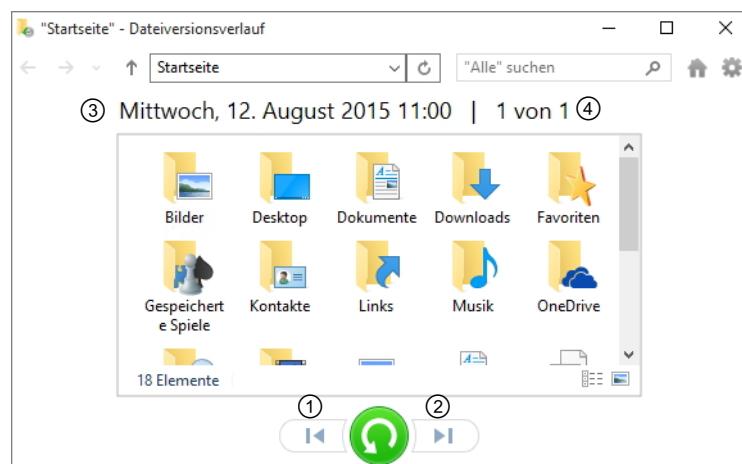
- Geben Sie `dateiversion` ein und wählen Sie *Stellt Dateien mit dem Dateiversionsverlauf wieder her*.

Alternativ können Sie den Dateiversionsverlauf auch über die Systemsteuerung aufrufen und auf *Persönliche Daten wiederherstellen* klicken.

Im Wiederherstellungsdialog können Sie mit den Tasten ① und ② durch die vorhandenen Dateiversionen blättern. Dabei wird Ihnen das Datum des Sicherungspunktes angezeigt ③ und wie viele Sicherungen es insgesamt gibt ④.

Sie sehen alle Bibliotheken sowie die Spezialordner *Desktop*, *Favoriten* und *Kontakte*, die in der Sicherung enthalten sind.

- Klicken Sie doppelt auf einen Ordner oder eine Datei, um eine Vorschau des Inhalts zu sehen.



*Wiederherstellung älterer Dateiversionen*

Im Kontextmenü eines Objekts können Sie ebenfalls die Vorschau aufrufen. Die grüne Schaltfläche stellt die Datei ebenfalls am Ursprungsort wieder her. Falls Dateien schon vorhanden sind, werden sie nicht sofort überschrieben. Sie können in solchen Fällen auswählen, was geschehen soll.

## 18.5 Wiederherstellung

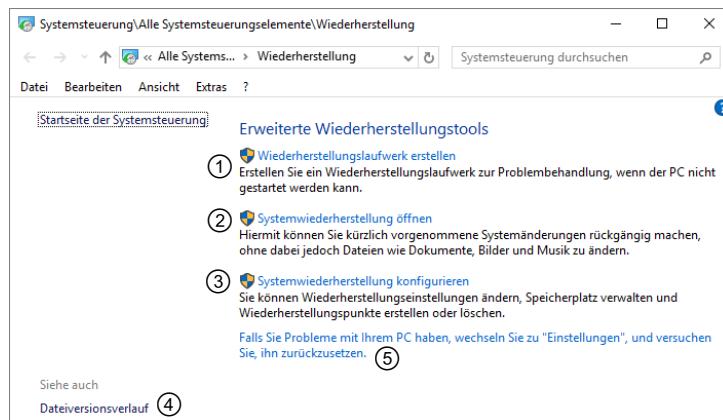
Während der Dateiversionsverlauf sich ausschließlich um die Daten der Benutzer kümmert, ist die Wiederherstellung von Windows 10 für die Sicherung des Betriebssystems und des gesamten Computers zuständig.

- Geben Sie `wiederher` im Startmenü ein. Es werden zahlreiche Einstellungen rund um die Wiederherstellung angezeigt. Wählen Sie *Wiederherstellung*.

Alternativ können Sie die Systemsteuerung öffnen und dort auf *Wiederherstellung* klicken.

Hier können Sie einen Wiederherstellungsdatenträger erstellen, von dem Sie auch bei Startproblemen booten können ①, zu bisherigen Systemwiederherstellungspunkten zurückkehren ② und weitere Einstellungen vornehmen ③.

Sie können außerdem zum Dateiversionsverlauf springen ④ oder die Windows-10-Einstellungen öffnen, um den PC in den Originalzustand zurückzuversetzen ⑤.



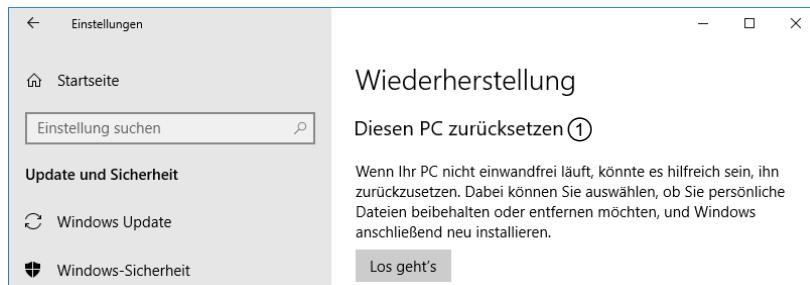
Möglichkeiten zur Wiederherstellung von Windows 10

## Reset in Windows 10

Windows 10 kann eine Windows-Installation reparieren, ohne dass dabei die persönlichen Daten verloren gehen. Dieser Vorgang wird **PC zurücksetzen** ① genannt. Es ist außerdem möglich, den PC in den Ursprungszustand zu versetzen. Dabei werden sämtliche Benutzerdaten und -einstellungen gelöscht. Dieser Reset-Vorgang eignet sich z. B. für den Verkauf oder die Weitergabe eines gebrauchten Computers. Beide Schritte können Sie über den Assistanten zum Zurücksetzen des Betriebssystems vornehmen.

Die beiden Wiederherstellungsoptionen lassen sich auch über die Einstellungen des Startmenüs aufrufen:

- Betätigen Sie ①.
- Klicken Sie auf *Update und Sicherheit - Wiederherstellung*.



Das Zurücksetzen des Computers ähnelt einer Reparaturinstallation bei Windows 7 oder Vista. Alle installierten Anwendungen gehen dabei verloren. Sie sollten das Zurücksetzen nur verwenden, wenn die Windows-Installation ernsthafte Probleme aufweist, die sich auch durch eine Systemwiederherstellung nicht lösen lassen.



*Das Auffrischen deinstalliert alle Desktop-Programme*

Booten Sie den Computer mit einer Windows-10-DVD, um eine Wiederherstellung zu starten, wenn Windows nicht mehr funktioniert. Klicken Sie im zweiten Fenster auf *Computerreparaturoptionen* und danach auf *Problembehandlung*.

Auch hier steht die Möglichkeit zum Zurücksetzen zur Verfügung. Bestätigen Sie im nächsten Fenster die Meldung zur Wiederherstellung. Nicht jeder Anwender kann einen PC zurücksetzen. Vor dem Start des Vorgangs müssen Sie sich erst mit einem Administratorbenutzer authentifizieren. Außerdem benötigen Sie einen Windows-10-Installationsdatenträger.

Im folgenden Fenster wählen Sie die Windows-Installation aus, die Sie zurücksetzen wollen. Als Nächstes starten Sie den Vorgang. Das Betriebssystem stellt sich jetzt selbstständig wieder her.

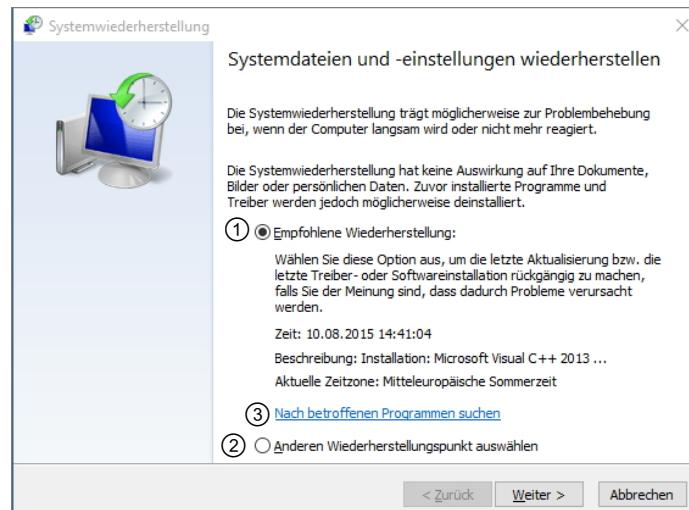
Nach der Wiederherstellung startet Windows 10 automatisch neu.

## Systemwiederherstellung verwenden

Die Systemwiederherstellung ist ein bewährtes Mittel zur Problembeseitigung, z. B. nach Systemfehlern oder fehlgeschlagenen Installationen. Am schnellsten starten Sie das Tool durch Eingabe von `rstrui.exe`.

Auf der ersten Seite des Assistenten können Sie auswählen, ob Sie zum letzten Wiederherstellungspunkt ① oder zu einem anderen Punkt zurückkehren möchten ②.

Sie können sich anzeigen lassen, welche Programme von dieser Wiederherstellung betroffen wären ③.

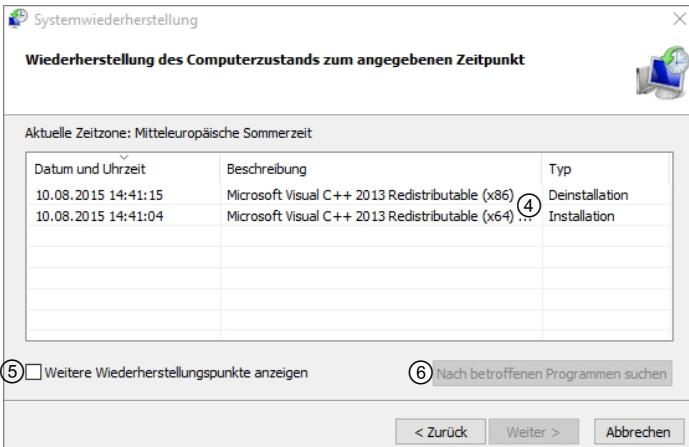


Erste Seite des Wiederherstellungsassistenten

Falls Sie Option ② gewählt haben, können Sie auf der nächsten Seite einen Punkt aus der Liste auswählen ④. Mit ⑤ können Sie weitere versteckte Punkte anzeigen lassen. Unter ⑥ können Sie sehen, welche Programme bei einer Wiederherstellung zum gewählten Punkt betroffen wären.

- Klicken Sie auf *Weiter* und folgen Sie den Anweisungen des Assistenten, um die Wiederherstellung zu starten.

Bei einer Systemwiederherstellung können möglicherweise auch persönliche Dateien verloren gehen oder mit älteren Versionen überschrieben werden.



Wiederherstellungszeitpunkt auswählen

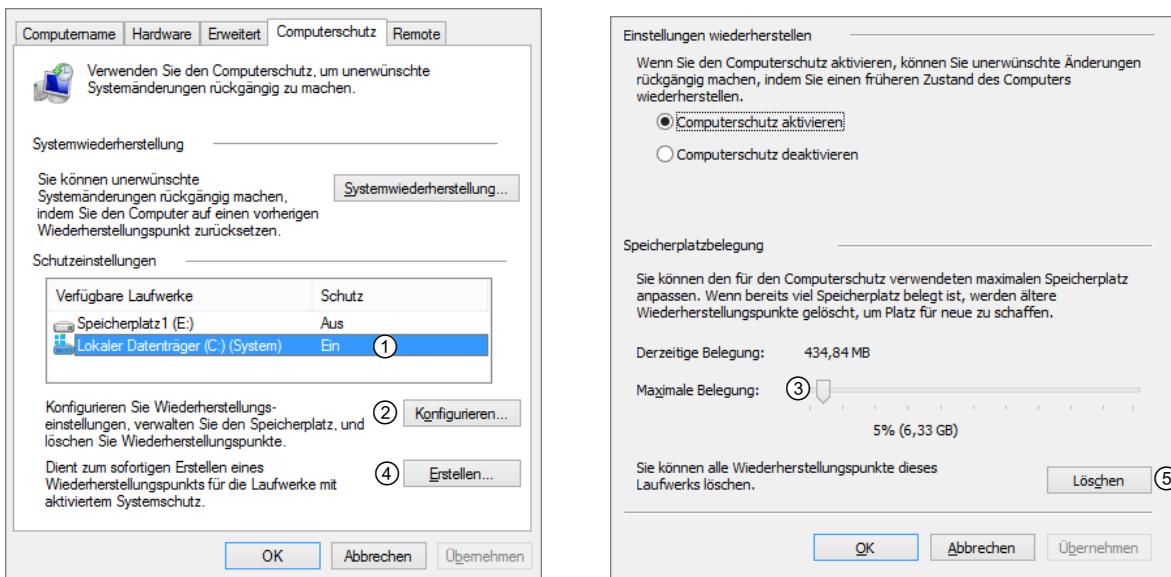
## Systemwiederherstellung konfigurieren

Sie erreichen die Optionen für den Computerschutz über die Systemeigenschaften. Betätigen Sie dazu und klicken Sie auf *Computerschutz*.

Sie können hier für jeden Datenträger ① unter *Konfigurieren* ② den Computerschutz ein- oder ausschalten.

Ist die Systemwiederherstellung für einen Datenträger aktiv, können Sie auch festlegen, wie viel Speicherplatz ③ für die Wiederherstellungsdaten verwendet werden darf.

Klicken Sie auf *Erstellen* ④, um für das gewählte Laufwerk einen Wiederherstellungspunkt zu erzeugen. Um alle vorhandenen Punkte zu löschen, klicken Sie auf *Löschen* ⑤.



Eigenschaften der Systemwiederherstellung konfigurieren

### Systemabbild erstellen

Die aus Windows 7 bekannte Funktion zum Sichern und Wiederherstellen ist in Windows 10 aus Kompatibilitätsgründen weiterhin vorhanden, wurde aber in Windows 10 entfernt. Sie finden sie in der Systemsteuerung von Windows 10 unter *System und Sicherheit - Sichern und Wiederherstellen (Windows 7)*. Sie können hier neben einer normalen Dateisicherung auch Systemabbilder anfertigen, die auf Wunsch das komplette System mit allen Datenträgern in einem Abbild speichern. Diese Systemabbilder können beim Start des Computers in den erweiterten Startoptionen wieder eingespielt werden und sind gut geeignet, den Zustand des Gesamtsystems zur schnellen Wiederherstellung zu sichern:

- ▶ Klicken Sie auf den Link *Systemabbild erstellen*.
  - ▶ Wählen Sie den Laufwerkbuchstaben des externen Laufwerks aus, auf dem Sie die Sicherung speichern wollen, und klicken Sie auf *Weiter*.
  - ▶ Klicken Sie auf *Sicherung starten*, damit der Computer komplett gesichert wird.
- Sie können im Fenster zusätzlich auswählen, welche Daten Sie bei der Sicherung erfassen wollen.

Die Sicherung wird jetzt abgeschlossen und steht als Wiederherstellungsoption über den Windows-10-Installationsdatenträger zur Verfügung. Alternativ erstellen Sie einen Wiederherstellungsdatenträger mit `recoverydrive.exe`.

## 18.6 Übung

### Sicherungsmethoden

Übungsdatei: --

Ergebnisdatei: *Uebung18\_E.pdf*

1. Wie schalten Sie den Dateiversionsverlauf ein?
2. Wie starten Sie die Wiederherstellungsmöglichkeiten in Windows 10?
3. Wie erstellen Sie in Windows 10 ein Systemabbild?

# 19 Eingabeaufforderung und PowerShell

## In diesem Kapitel erfahren Sie

- ✓ wozu Sie die Eingabeaufforderung benötigen
- ✓ wie Sie die Eingabeaufforderung konfigurieren
- ✓ welche Möglichkeiten die PowerShell bietet

## Voraussetzungen

- ✓ Grundlagen MS-DOS

## 19.1 Nutzen der Eingabeaufforderung

### Aufgabe und Funktion der Eingabeaufforderung

Warum benötigt ein Betriebssystem mit einer grafischen Benutzeroberfläche eine Eingabeaufforderung?

Ein wichtiges Stichwort lautet „Abwärtskompatibilität“. Darunter wird die Möglichkeit verstanden, auch unter Windows 10 Programme ausführen zu können, die für ältere Betriebssysteme wie Windows 3.x und MS-DOS geschrieben wurden.



Bei 64-Bit-Versionen von Windows können diese alten Programme, die auch als Legacy-Software (Altlast) bezeichnet werden, nicht mehr ausgeführt werden. Um dennoch solche alten Anwendungen zu starten, wird Drittanbietersoftware wie z. B. DOSBox benötigt. Eine weitere Möglichkeit sind virtuelle Maschinen.

Ein weiteres Stichwort ist „Wartung“. Einige Dienstprogramme lassen sich nur in der Eingabeaufforderung starten, beispielsweise das Tool *ping* zur Prüfung von TCP/IP-Netzwerken. Viele Systemeinstellungen lassen sich über die Eingabeaufforderung schneller und eleganter vornehmen als mit der grafischen Oberfläche.



Unter Windows 10 in der 32-Bit-Version wird zur Ausführung von MS-DOS-Programmen und -Befehlen das MS-DOS-Subsystem verwendet. Es arbeitet immer dann, wenn Sie die Eingabeaufforderung starten.

Die Eingabeaufforderung ist ähnlich wie die ursprüngliche MS-DOS-Oberfläche gestaltet. Das jeweils aktuelle Verzeichnis wird mit einer entsprechenden Pfadangabe ① angezeigt. Die Befehlseingabe erfolgt immer an der Stelle, an der der Cursor blinkt, und wird mit der Taste ② abgeschlossen.

Sie haben die Möglichkeit, mithilfe der Bildlaufleiste ② und der Bildlaufpfeile ③ innerhalb der Eingabeaufforderung zu scrollen und die zuletzt angezeigten Informationen und Befehle noch einmal einzusehen.

```
c:\>ping www.herdt.com

Ping wird ausgeführt für www.herdt.com [195.243.78.74] mit 32 Bytes Daten:
Antwort von 195.243.78.74: Bytes=32 Zeit=7ms TTL=56
Antwort von 195.243.78.74: Bytes=32 Zeit=6ms TTL=56
Antwort von 195.243.78.74: Bytes=32 Zeit=6ms TTL=56
Antwort von 195.243.78.74: Bytes=32 Zeit=6ms TTL=56

Ping-Statistik für 195.243.78.74:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 6ms, Maximum = 7ms, Mittelwert = 6ms

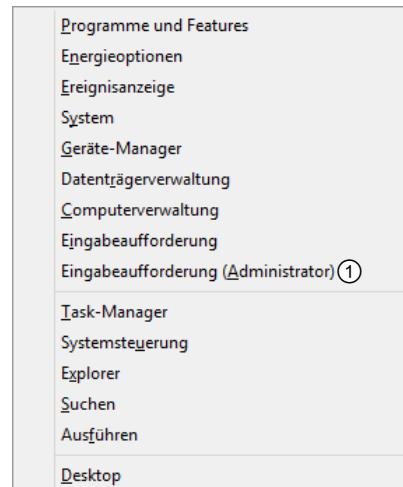
c:\>①
```

Die Windows-Eingabeaufforderung

### Eingabeaufforderung starten und beenden

- ▶ Betätigen Sie zum Starten der Eingabeaufforderung und geben Sie in die Suchzeile cmd ein. Schließen Sie die Eingabe mit ab.
  - ▶ Um eine Eingabeaufforderung mit Administratorrechten zu öffnen, schließen Sie die Eingabe von cmd mit ab.
- oder*
- ▶ Alternativ können Sie die Eingabeaufforderung auch mit über das Schnellzugriffsmenü aufrufen ①.
  - ▶ Um die Eingabeaufforderung zu beenden, geben Sie dort den Befehl exit ein und bestätigen Sie mit .

Falls Sie mithilfe der Eingabeaufforderung ein MS-DOS-Programm gestartet haben, kann dieses von Windows 10 nicht ordnungsgemäß beendet werden, solange es noch aktiv ist. Schließen Sie deshalb nicht einfach das DOS-Fenster, sondern beenden Sie das MS-DOS-Programm über den vorgesehenen Weg.



CMD im Schnellzugriffsmenü

Ein Schließen des DOS-Anwendungsfensters hat die gleiche Wirkung wie das Beenden eines Prozesses im Task-Manager. Die Anwendung wird „abgeschossen“ und alle ungespeicherten Daten der DOS-Anwendung sind verloren.

## 19.2 Die Eingabeaufforderung anpassen

### Eingabeaufforderung konfigurieren

- ▶ Starten Sie die Eingabeaufforderung und klicken Sie mit der rechten Maustaste auf die Titelleiste des Eingabeaufforderungsfensters.
- ▶ Klicken Sie im Kontextmenü auf *Standardwerte*.

Sie können jetzt einige Konfigurationseinstellungen vornehmen. Diese Einstellungen werden beim nächsten Öffnen der Eingabeaufforderung als Standard übernommen.

Unter dem Menüpunkt *Eigenschaften* können Sie ebenfalls die benötigten Einstellungen vornehmen. Windows 10 wendet diese Einstellungen dann automatisch auf alle Eingabeaufforderungsfenster an.

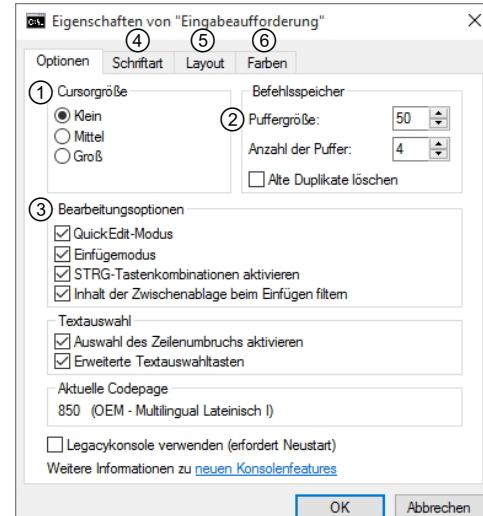
- ▶ Klicken Sie auf *OK*, um die Auswahl zu bestätigen und die Einstellungen zu übernehmen.

### Übersicht über die Einstellungsmöglichkeiten

Im Register *Optionen* können Sie die Cursorgröße ①, die Größe des Befehlspuffers ② und die Bearbeitungsoptionen wie z. B. den *QuickEdit-Modus* ③ festlegen.

Darüber hinaus können Sie in den übrigen Registern folgende Einstellungen vornehmen:

- ✓ *Schriftart* ④: Schriftart und Zeichengröße
- ✓ *Layout* ⑤: Fenstergröße und -position
- ✓ *Farben* ⑥: Hintergrundfarbe und Schriftfarbe



Einstellungen der Eingabeaufforderung

## Der QuickEdit-Modus

Mithilfe des QuickEdit-Modus können Sie im Fenster der Eingabeaufforderung Text markieren und einfügen.

- ▶ Markieren Sie mit gedrückter linker Maustaste einen Bereich.
- ▶ Klicken Sie mit der rechten Maustaste auf die Stelle der Eingabezeile, wo Sie den Text einfügen wollen.  
Der markierte Text wird in die Zwischenablage übernommen.
- ▶ Klicken Sie erneut mit der rechten Maustaste an die Stelle. Der Inhalt der Zwischenablage wird eingefügt.

Auf diese Weise können Sie auch Textpassagen aus anderen Anwendungen einfügen. Sie können zum Kopien und Einfügen auch eine Textstelle markieren und im Kontextmenü der Titelleiste der Eingabeaufforderung den Menüpunkt *Bearbeiten - Kopieren* und anschließend *Bearbeiten - Einfügen* aufrufen.

## Funktionen und Tastenkombinationen

Hier sind einige Tipps, um den Umgang mit der Eingabeaufforderung angenehmer und schneller zu machen:

- ✓ Sie können mit **[Shift]** Datei- und Ordnernamen vervollständigen. Falls Sie schon die ersten Buchstaben geschrieben haben, werden bei mehrfachem Betätigen der Taste alle Ordner oder Dateien in alphabetischer Reihenfolge angezeigt, die diesem Muster entsprechen. Bei Betätigen von **[Up]** **[Shift]** wird die Reihenfolge umgekehrt. Auf diese Weise können Sie sich in Verbindung mit dem Befehl `cd` schnell durch die Ordnerstruktur bewegen.
- ✓ Sie können Kommandos nachträglich editieren und z. B. einen Dateinamen austauschen.
- ✓ Mit **[Up]** und **[Down]** können Sie durch die letzten eingegebenen Kommandos blättern.
- ✓ Durch Betätigen von **[Space]** oder **[F]** in einer neuen Eingabe erscheint Buchstabe für Buchstabe das letzte Kommando.
- ✓ Mit **[F2]** können Sie den letzten Befehl bis zu einem bestimmten Buchstaben wiederholen, der Rest wird abgeschnitten.
- ✓ Mit **[Esc]** löschen Sie die aktuelle Zeile.
- ✓ Mit **[F7]** lassen sich die letzten Befehle auflisten. Mit **[Up]** und **[Down]** können Sie einen Befehl auswählen, mit **[Space]** übernehmen Sie den Befehl in die Eingabezeile und mit **[Enter]** wird er sofort ausgeführt.
- ✓ Wenn Sie die ersten Buchstaben eines bereits verwendeten Befehls eingeben, können Sie ihn mit **[F8]** vervollständigen. Durch mehrfaches Betätigen werden alle Befehle angezeigt, die dem Muster entsprechen.
- ✓ Mit **[Alt] [F7]** löschen Sie die bisherige Befehlsliste.
- ✓ Geben Sie `cls` ein, um die Bildschirmausgabe zu löschen.
- ✓ Wenn Sie eine Datei oder einen Ordner aus dem Datei-Explorer in die Eingabeaufforderung ziehen (Drag & Drop), erscheint der komplette Pfad des Objekts in der Eingabezeile.

## 19.3 Eingabeaufforderung und Batchdateien

### Die Befehle der Eingabeaufforderung

Die Eingabeaufforderung von Windows 10 bietet Ihnen etwa 75 Befehle und Programme. Gut die Hälfte stammt noch aus Zeiten von DOS, viele der alten Befehle wurden jedoch mit zusätzlichen Optionen und Fähigkeiten ausgestattet.



Weitere Informationen zu Befehlen für die Eingabeaufforderung von Windows 10 erhalten Sie in der Eingabeaufforderung mit dem Befehl `Help`. Wenn Sie Informationen zu einem einzelnen Befehl wünschen, geben Sie `help <Befehl>` ein (z. B. `help start`) oder `<Befehl> /?` (z. B. `start /?`).

Über die Eingabeaufforderung sind zahlreiche Anwendungen erreichbar, die nicht durch den Help-Befehl aufgelistet werden, z. B. `winver` zur Anzeige der Windows-Version oder `netstat` zur Netzwerkdagnostik.

Sie können die Befehle entweder direkt in der Eingabeaufforderung verwenden, oder Sie schreiben eine Batchdatei.

## Mit Batchdateien arbeiten

Für Batchdateien können Sie einfach die Befehle in eine neue Textdatei schreiben und dieser die Endung `.cmd` oder `.bat` zuweisen. Ziehen Sie einen Pfad aus der Adressleiste des Explorers in die Eingabeaufforderung, wird dieser direkt als Text eingefügt.

Alternativ halten Sie im Explorer die -Taste gedrückt, wenn Sie einen Ordner mit der rechten Maustaste anklicken, und wählen dann *Eingabeaufforderung hier öffnen*.

Suchen Sie bestimmte Dateien in einem Ordner, geben Sie `dir <Dateinamen>` ein.

Kennen Sie nur einen Teil des Namens, verwenden Sie den Platzhalter `*`, zum Beispiel `dir *sys*`.

Wollen Sie nach der Datei oder dem Ordner in allen Unterordnern des aktuellen Ordners suchen, verwenden Sie `dir *sys* /s`. Alle Möglichkeiten des Dir-Befehls erhalten Sie mit `dir /?`.

## Mit der Eingabeaufforderung arbeiten

- ▶ Geben Sie `cmd` auf der Startseite ein, wird die Eingabeaufforderung geöffnet.
- ▶ Geben Sie in der Eingabeaufforderung `powershell` ein, öffnet sich innerhalb des Fensters eine PowerShell-Sitzung.

In dieser Sitzung können Sie alle Befehle der Eingabeaufforderung und alle Befehle der PowerShell (vgl. Abschnitt 19.4) verwenden. Mit `cmd` kommen Sie wieder in die Eingabeaufforderung zurück.

```

Windows PowerShell
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\thomas>powershell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\thomas> ise
PS C:\Users\thomas>

```

Innerhalb der PowerShell starten Sie mit `ise` die grafische Oberfläche der PowerShell in einem eigenen Fenster.

Die wichtigsten Befehle der Eingabeaufforderung sind nachfolgend aufgelistet:

<code>append</code>	Sucht nach Dateien im Unterordner
<code>assign</code>	Weist dem Laufwerk einen anderen Buchstaben genau zu
<code>attrib</code>	Zeigt Dateiattribute an oder ändert diese
<code>c:</code>	Wechselt zum Laufwerk C:
<code>call</code>	Ruft eine Batchdatei aus einer anderen heraus mit Rücksprung auf
<code>cd</code>	Der Befehl <code>cd</code> zeigt Ihnen den Namen des aktuellen Ordners an oder wechselt den aktuellen Ordner. Wird <code>cd</code> nur mit einem Laufwerkbuchstaben (z.B. <code>cd c:\temp</code> ) verwendet, zeigt es diesen Laufwerkbuchstaben und den Namen des Ordners an, der auf dem Laufwerk der aktuelle Ordner ist. Ohne Parameter zeigt <code>cd</code> das aktuelle Laufwerk und den aktuellen Ordner an.
<code>chkdsk</code>	Überprüft Datenträger
<code>choice</code>	Erlaubt verschiedene Auswahlmöglichkeiten innerhalb von Batchdateien
<code>cls</code>	Löscht den Bildschirm
<code>comp</code>	Vergleicht Dateien miteinander
<code>copy</code>	Kopiert Dateien
<code>date</code>	Zeigt das aktuelle Datum an oder ändert dieses
<code>del</code>	Löscht eine oder mehrere Dateien
<code>deltree</code>	Löscht komplett Verzeichnisbäume

<code>dir</code>	Zeigt die Datenträgervolumenbezeichnung und Seriennummer des Datenträgers, gefolgt von einer Liste der Ordner und Dateien auf dem Datenträger, einschließlich der entsprechenden Namen, des Datums und der Uhrzeit der letzten vorgenommenen Änderung an. Bei Dateien zeigt <code>dir</code> die Namenerweiterung und die Größe in Bytes an.
<code>echo</code>	Zeigt Meldungen auf dem Bildschirm aus einer Batchdatei heraus an; schaltet die Befehlsanzeige ein bzw. aus
<code>exit</code>	Beendet das aktuelle Batchskript (mit dem Parameter <code>/b</code> ) oder das Programm <code>cmd.exe</code> und kehrt zu dem Programm zurück, das über <code>cmd.exe</code> gestartet wurde
<code>expand</code>	Expandiert eine oder mehrere komprimierte Dateien
<code>fc</code>	Vergleicht Dateien
<code>find</code>	Sucht Textstellen in Dateien
<code>for</code>	Batchbefehle zur mehrfachen Wiederholung eines DOS-Befehls
<code>format</code>	Bereitet Festplatten vor (formatieren)
<code>ftp</code>	Öffnet die FTP-Verbindung
<code>goto</code>	Sprungbefehl in einer Batchdatei
<code>if</code>	Setzt Bedingungen in Batchdateien
<code>label</code>	Weist einen Datenträgernamen zu und ermöglicht das Ändern oder Löschen
<code>md</code>	Erstellt einen Unterordner
<code>menucolor</code>	Legt die Farben für das Multikonfigurationsmenü fest
<code>move</code>	Verschiebt Dateien, benennt Ordner um
<code>path</code>	Legt den Suchpfad für ausführbare MS-DOS-Befehlsdateien fest oder zeigt ihn an
<code>pause</code>	Stoppt innerhalb von Batchdateien und wartet auf einen Tastendruck
<code>ping</code>	Testet eine Netzwerkverbindung
<code>print</code>	Druckt Textdateien im Hintergrund aus
<code>rd</code>	Löscht einen Unterordner
<code>rem</code>	Fügt Kommentare in Batchdateien ein
<code>ren</code>	Benennt Dateien um
<code>subst</code>	Ersetzt einen Ordnernamen durch einen Laufwerkbezeichner
<code>telnet</code>	Öffnet das Telnet-Fenster. Dazu muss aber die Funktion Telnetclient installiert sein.
<code>time</code>	Zeigt die Systemzeit an und ändert diese
<code>tree</code>	Zeigt die Ordnerstruktur eines Datenträgers grafisch an
<code>type</code>	Zeigt den Inhalt einer Datei auf dem Bildschirm an
<code>vol</code>	Zeigt den Namen und die Seriennummer eines Datenträgers an
<code>xcopy</code>	Erweitertes Kopierprogramm mit zusätzlichen Möglichkeiten zur Übertragung von Dateien und kompletten Verzeichnisbäumen. Mit <code>xcopy</code> lassen sich Dateien und Ordner einschließlich der Unterordner kopieren. Die Syntax dazu lautet: <code>xcopy Quelle [Ziel] [/c] [/v] [/l] [/d[:TT.MM.JJ]] [/u] [/s [/e]] [/t] [/k] [/r] [/h] [/y -y] [/z]</code> .



Arbeiten Sie mit der Eingabeaufforderung, können Sie schneller die verschiedenen Befehle aufrufen, wenn Sie den Anfangsbuchstaben des Verzeichnisses eingeben, zu dem Sie sich bewegen wollen, und dann die -Taste drücken. Windows vervollständigt anschließend den Befehl. Wollen Sie zum Beispiel zum Stammverzeichnis der Partition wechseln, geben Sie den Befehl `cd\` ein. Um vom Stammverzeichnis aus das Verzeichnis `Programme` zu öffnen, reicht es auch, wenn Sie `P` eingeben und so lange die -Taste drücken, bis das richtige Verzeichnis erscheint.

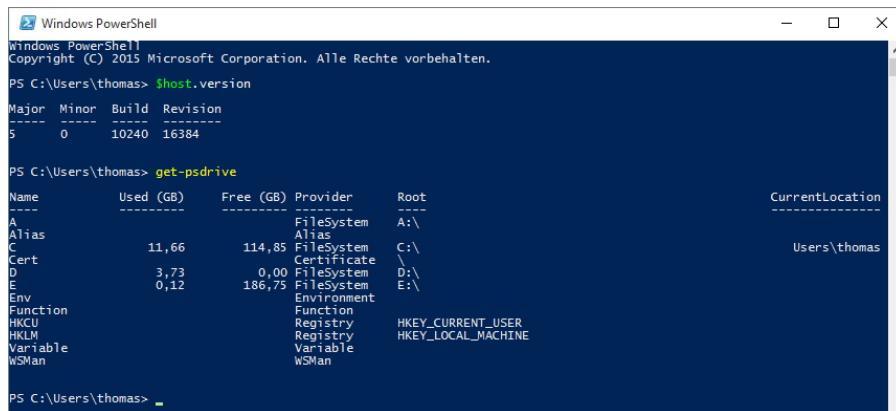
In der Eingabeaufforderung tragen die vom System erstellten Verzeichnisse meistens englische Bezeichnungen, außer die Verzeichnisse, die Sie selbst erstellen. Diese können zwar auch englische Bezeichnungen erhalten, allerdings nur optional.

Wollen Sie aus dem Explorer direkt einen Pfad in der Eingabeaufforderung öffnen, klicken Sie auf das Verzeichnis mit gedrückter -Taste und Rechtsklick und wählen Sie *Eingabeaufforderung hier öffnen*.

## 19.4 Die PowerShell – ein kurzer Überblick

### Was die PowerShell ist

Die PowerShell ist eine Alternative zur Kommandozeile und zum Windows Scripting Host (WSH). Sie basiert auf dem .NET-Framework und orientiert sich bei der Bedienung und dem Funktionsumfang an den UNIX-Shells. Sie ermöglicht objektorientierte Skriptprogrammierung und ist ein weitaus mächtigeres Werkzeug als die Eingabeaufforderung. Ein Großteil der Befehle aus der Eingabeaufforderung funktioniert weiterhin, damit die Umstellung leichter fällt und vorhandene Skripte funktionieren. Die PowerShell-Version können Sie mit dem Befehl `$host.version` anzeigen lassen.

```

Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Users\thomas> $host.version
Major Minor Build Revision
----- -----
5      0      10240 16384

PS C:\Users\thomas> get-psdrive
Name     Used (GB)   Free (GB) Provider    Root           CurrentLocation
----     -----   -----   -----    ----           -----
A       Alias          Alias      FileSystem  A:\           Users\thomas
C       11,66        114,85  FileSystem  C:\           Users\thomas
Cert    3,73         0,00   FileSystem  D:\           Users\thomas
D       0,12         186,75  FileSystem  E:\           Users\thomas
Env    Function        Function   Registry   HKEY_CURRENT_USER
Function          Function   Registry   HKEY_LOCAL_MACHINE
HKCU   Registry        Registry   Registry   HKEY_CURRENT_USER
HKLM   Registry        Registry   Registry   HKEY_LOCAL_MACHINE
Variable          Variable   WSMAN
WSMan

PS C:\Users\thomas>

```

Die PowerShell sieht aus wie eine farbige Eingabeaufforderung, kann aber viel mehr

Mit Windows 10 und Windows Server 2016 kommt die neue Version 5.0 der PowerShell. Mit dieser liefert Microsoft unter anderem das OneGet-Framework mit aus. Dieses bietet die Möglichkeit, Programme als **Paket** in Windows 10 zu installieren oder für mehrere Windows 10-Rechner im Netzwerk zu verteilen. Microsoft OneGet-Framework ist kompatibel mit den Softwarepaketen von NuGet (<http://www.nuget.org>). Diese OpenSource-Lösung bietet etwa 2.000 Softwarepakete. Das heißt, mit der PowerShell 5.0 lassen sich auf einen Schlag gleich tausende Anwendungen im Netzwerk bereitstellen. OneGet kann außerdem Chocolatey Repositories (<http://chocolatey.org>) installieren, um Zugriff auf tausende Programme zu erhalten, die Sie schnell und einfach über die PowerShell installieren können. Eine weitere Neuerung in der PowerShell ist die Möglichkeit, Zip-Archive zu erstellen oder zu entpacken.

### Die PowerShell starten

Die PowerShell starten Sie entweder über die Verknüpfung auf der Startseite oder Sie geben `powershell` in einer Eingabeaufforderung ein. Innerhalb der PowerShell können Sie mit dem Befehl `ise` die grafische Oberfläche starten.



### Cmdlets

Die PowerShell ist eine Kommandozentrale, von der aus sich das gesamte System steuern lässt. Dabei können alle Arten von Skripten, Programmen oder Benutzerdateien verarbeitet werden. Je nach Dateityp werden automatisch die notwendigen Anwendungen oder Umgebungen gestartet. Die wahre Stärke ist das sogenannte **Cmdlet** (gesprochen: Commandlet), ein vordefinierter Skriptbaustein, der alle möglichen Funktionen erfüllen kann.

Die PowerShell verfügt inzwischen über mehr als 1100 solcher Cmdlets, und es können beliebig viele neue hinzugefügt werden. Mithilfe solcher Cmdlets können praktisch alle Vorgänge im Computer gesteuert werden, und so bietet sich die PowerShell für die Steuerung und Verwaltung vieler Computer im Netzwerk über WMI an (Windows Management Instrumentation, eine Verwaltungstechnologie von Microsoft).

Die PowerShell ist auf 64-Bit-Systemen sowohl für 32 Bit (x106) als auch für 64 Bit verfügbar.

## PowerShell-Skripts und ISE

Wenn Sie immer wieder bestimmte Befehlsfolgen ausführen oder ein PowerShell-Skript für eine komplexe Aufgabe entwickeln, empfiehlt es sich, die Befehle nicht einzeln einzugeben, sondern in einer Datei zu speichern. Die Dateierweiterung für Windows PowerShell-Skripts lautet **.ps1** (das dritte Zeichen der Dateierweiterung ist die Zahl 1). Sie erstellen dafür einfach eine Textdatei mit der entsprechenden Endung.

Zusätzlich gibt es eine Ausführung der PowerShell mit ISE (Integrated Scripting Environment), einer integrierten Skriptumgebung, in der die Erstellung eigener Skripte und Cmdlets enorm erleichtert wird.

```

24
25 # Change the $path to whatever path you want. Your computers.txt will need to be in
26 # The results.csv will also be put in this folder once the script has run.
27 $path = "C:\scripts\drive_info"
28 $exportPath = "C:\scripts\drive_info" # I change this to a central fileshare
29 $computers = gc $path\computers.txt
30
31 # Start HTML Output file style
32 $style = ""
33 $style = $style + "Body{background-color:white;font-family:Arial;font-size:10pt;}"
34 $style = $style + "Table{border-width: 1px; border-style: solid; border-color: black; width: 100%;}"
35 $style = $style + "TH{border-width: 1px; padding: 2px; border-style: solid; border-color: black; text-align: left; width: 15%;}"
36 $style = $style + "TD{border-width: 1px; padding: 5px; border-style: solid; border-color: black; text-align: left; width: 85%;}"
37 $style = $style + ""
38 # End HTML Output file style

```

```

PS C:\> Get-Command -noun command
 CommandType      Name
-----      -----
 Cmdlet      Get-Command
 Cmdlet      Invoke-Command
 Cmdlet      Measure-Command
 Cmdlet      Show-Command
 Cmdlet      Trace-Command

PS C:\> Get-Command -Module storage -CommandType |

```

### Die PowerShell ISE - ein komplexer Skript-Editor

- Wenn Sie im Startbildschirm `power` eingeben, werden alle verfügbaren PowerShells angezeigt.

In der PowerShell 5.0 ist die Ausführungsrichtlinie für Skripts standardmäßig auf **RemoteSigned** gesetzt. Die Ausführungsrichtlinie bestimmt, ob Skripts ausgeführt werden dürfen und ob diese digital signiert sein müssen. Standardmäßig blockiert die PowerShell Skripts in der PowerShell 3.0. Ab 4.0 sind die Skripte erlaubt. Sie können die Ausführungsrichtlinie mit dem Cmdlet `Set-ExecutionPolicy` ändern und mit `Get-ExecutionPolicy` anzeigen. Dabei stehen folgende Einstellungen zur Verfügung:

- ✓ **Restricted:** Standardeinstellung. Keine Skripts erlaubt.
- ✓ **AllSigned:** Nur signierte Skripts sind erlaubt.
- ✓ **RemoteSigned:** Bei dieser Einstellung müssen Sie Skripts durch eine Zertifizierungsstelle signieren lassen.
- ✓ **Unrestricted:** Mit dieser Einstellung funktionieren alle Skripts.

- ✓ Nach der Eingabe von `Set-ExecutionPolicy Unrestricted` müssen Sie die Ausführung noch bestätigen. Anschließend funktionieren eigene Skripts. Die Ausführungsrichtlinie speichert Ihre Daten in der Windows-Registrierung.

## Mit Cmdlets arbeiten

Generell ist der Umgang mit der PowerShell nicht sehr kompliziert. Geben Sie `Get-Command` ein, sehen Sie alle Befehle, welche die Shell zur Verfügung stellt. Die wenigsten Anwender kennen alle Cmdlets und deren verschiedenen Optionen, die Microsoft zur Verfügung stellt. Die Verwaltungsshell bietet jedoch eine ausführliche Hilfe an. Haben Sie nur den Teil eines Befehls in Erinnerung, können Sie mit dem Platzhalter \* arbeiten.

Der Befehl `Get-Command *computer` zeigt zum Beispiel alle Cmdlets an, deren Namen mit `computer` endet. Ist der gesuchte Befehl nicht dabei, können Sie auch mehrere Platzhalter verwenden, zum Beispiel den Befehl `Get-Command *computer*`. Dieser Befehl zeigt alle Befehle an, in denen an einer beliebigen Stelle das Wort `computer` vorkommt.

Haben Sie das gewünschte Cmdlet gefunden, unterstützt Sie die PowerShell mit weiteren Möglichkeiten. Für nahezu alle Cmdlets gilt die Regel, dass diese in vier Arten vorliegen:

- ✓ mit dem Präfix `New-`, um ein Objekt zu erstellen, zum Beispiel `New-Item`,
- ✓ mit `Remove-`, um ein Objekt zu löschen, zum Beispiel `Remove-Item`,
- ✓ mit dem Präfix `Set-`, um ein Objekt anzupassen, zum Beispiel `Set-Item`,
- ✓ mit dem Präfix `Get-`, zum Beispiel `Get-Item`, um Informationen zum Objekt abzurufen.

Neben diesen Cmdlets gibt es natürlich noch viele andere, zum Beispiel Start- und Stop- oder Export- und Import-Cmdlets. Allerdings bestehen die meisten Administrationsausgaben aus den erwähnten New-, Remove-, Set- und Get-Cmdlets. Geben Sie nur diesen Befehl ein, passiert entweder überhaupt nichts, das Cmdlet zeigt Objekte an, oder Sie werden nach der Identität des Objekts gefragt.

Mit Get-Cmdlets lassen Sie sich Informationen zu Objekten anzeigen. Die Option `| fl` formatiert die Ausgabe. Wollen Sie aber nicht alle Informationen, sondern nur einzelne Parameter anzeigen, können Sie diese nach der Option `| fl` anordnen. Dazu geben Sie eine der Spalten an, die Sie mit dem Get-Cmdlet abgefragt haben.

## Desired State Configuration (DSC)

Eine wesentliche Neuerung der PowerShell 4.0 ist die Desired State Configuration (DSC). Diese ist in 5.0 weiterhin verfügbar und wurde verbessert. Mit dieser neuen Funktion können Sie die Konfiguration von bestimmten Systemdiensten in Konfigurationsdateien speichern und auf Computern verteilen. Sie können in der Datei zum Beispiel hinterlegen, dass bei der Ausführung auf einem Computer bestimmte Dateien kopiert, Dienste gestartet oder installiert und Programme ausgeführt werden. Auch Systemeinstellungen lassen sich in der Datei hinterlegen. Haben Sie die Steuerdatei erstellt, führen Sie diese mit dem neuen Cmdlet `Start-DscConfiguration` aus.

Ausführliche Anleitungen zu den Möglichkeiten finden sich in der TechNet (<http://blogs.technet.com/b/privatecloud/archive/2013/01/29/introducing-powershell-desired-state-configuration-dsc.aspx>).



## 19.5 Übung

### Datenträger verwalten

Übungsdatei: --

Ergebnisdatei: *Uebung19\_E.pdf*

1. Warum wird eine Eingabeaufforderung benötigt?
2. Wie öffnen Sie Befehlszeile, PowerShell und PowerShell ISE am schnellsten?
3. Was ist ein Cmdlet?

# 20 Windows 10 aktualisieren

## In diesem Kapitel erfahren Sie

- ✓ wie Sie nach aktuellen Treibern für Windows 10 suchen können
- ✓ wie Sie Windows Updates einstellen und installieren
- ✓ wie Sie Service Packs für Windows 10 verwenden

## 20.1 Betriebssystem-Software aktualisieren

### Was und warum aktualisiert werden sollte

Betriebssysteme wie Windows sind sehr komplexe Gebilde aus Treibern, Anwendungen, Diensten und Werkzeugen. Unzählige Zeilen von Programmcode müssen auf korrekte Weise zusammenarbeiten, um das Neben- und Miteinander von Dutzenden Prozessen zu ermöglichen. Trotz aller Sorgfalt werden deshalb auch nach Erscheinen der fertigen Verkaufsversion in der Einführungsphase zahlreiche Fehler oder Probleme auftauchen, die mithilfe von **Updates** oder **Patches** (engl. für Flicken) beseitigt werden müssen. Diese Fehler können sowohl die Software des Betriebssystems als auch Treiber für Hardware-Komponenten betreffen. Besonders kritisch sind neu entdeckte Sicherheitslücken, die den Computer für Angriffe aus dem Internet verwundbar machen. Daher sollten Sie Windows 10 stets über Windows Update auf dem aktuellen Stand halten und Sicherheitsupdates sofort installieren.

### Windows Update und Service Packs verwenden

Microsoft bietet über Windows Update den automatischen Download von Systemupdates an. Üblicherweise erscheint frühestens ein Jahr nach Erscheinen einer neuen Windows-Version ein Service Pack, in dem alle bisher erschienenen Sicherheitsupdates und Patches zusammengefasst werden. Service Packs werden von Microsoft im Internet zum Download bereitgestellt und sind kostenpflichtig auch als optischer Datenträger erhältlich.

## 20.2 Windows Update verwenden

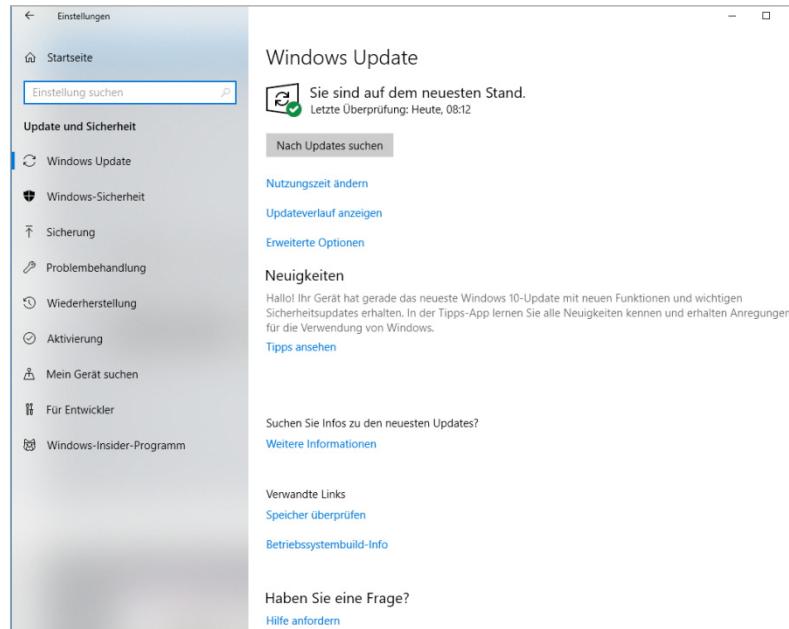
### Die Funktion von Windows Update

Windows 10 stellt mit Windows Update eine Funktion zur Verfügung, mit der Verbesserungen und Erweiterungen für das Betriebssystem unmittelbar nach deren Veröffentlichung installiert werden können. Dazu gehören z. B. Sicherheitspatches, neue Treiber, aktualisierte Systemdateien und Antiviren-Updates sowie nützliche Tools, die Microsoft im Internet kostenlos zur Verfügung stellt. Auch Support-Informationen können Sie hier abrufen. Windows 10 ist standardmäßig so eingestellt, dass neue Updates automatisch heruntergeladen und nachts installiert werden, diese Einstellungen lassen sich jedoch auch anpassen. Falls der Computer zu dieser Zeit nicht angeschaltet ist, werden die Updates bei der nächsten Gelegenheit installiert.

In Firmennetzwerken können die Administratoren alle Updates zentral über einen sogenannten **WSUS-Server** (**Windows Server Update Service**) sammeln, genehmigen und an die Clientrechner verteilen. Dadurch behalten sie die volle Kontrolle und können alle Updates vor der Auslieferung gründlich auf eventuelle Nebenwirkungen untersuchen. Außerdem wird so die Internetverbindung entlastet, da nicht jeder einzelne Computer die Updates herunterladen muss. Über Windows Update können auf Wunsch auch Updates für andere Microsoft-Produkte wie das Office-Paket bezogen werden.

## Windows Update ausführen

- Öffnen Sie das Startmenü und klicken Sie auf *Einstellungen - Update und Sicherheit - Windows Update*.
- Klicken Sie auf *Nach Updates suchen*.
- Klicken Sie auf *Jetzt Installieren*, um alle angewählten Updates zu installieren. In der Home-Edition von Windows 10 werden Updates automatisch installiert.



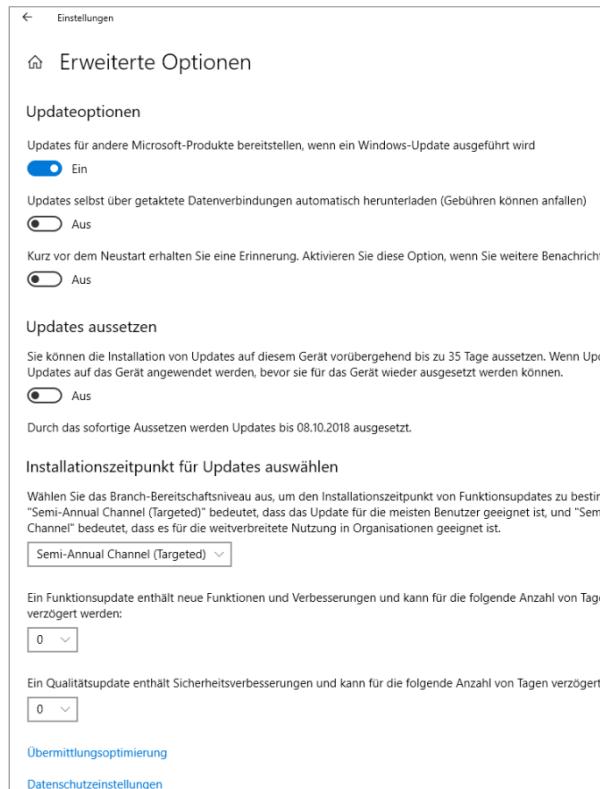
## Update-Einstellungen ändern

Sie können in den Editionen Pro und Enterprise von Windows 10 teilweise selbst bestimmen, wie mit neuen Updates umgegangen werden soll.

- Klicken Sie auf *Einstellungen - Update und Sicherheit - Windows Update - Erweiterte Optionen*.

Im neuen Fenster können Sie auswählen, wie Windows sich in Bezug auf Updates verhalten soll:

- ✓ *Updates für andere Microsoft-Produkte bereitstellen, wenn ein Windows-Update ausgeführt wird* – zum Beispiel für Microsoft Office.
- ✓ *Updates aussetzen* – Dadurch werden Updates erst nach weiteren Wochen installiert.
- ✓ *Übermittlungsoptimierung* – Windows 10 kann Updatedateien für andere Rechner im Netzwerk bereitstellen und von diesen Rechnern abrufen. Diese Funktion können Sie hier deaktivieren.

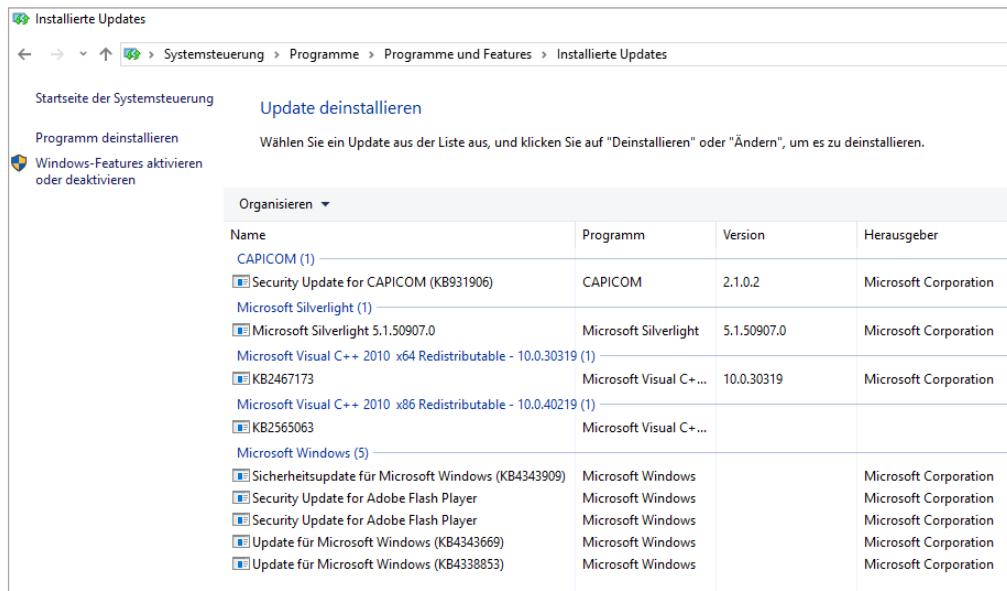


*Update-Einstellungen vornehmen*

## Updates deinstallieren

Falls ein Update fehlerhaft ist oder Probleme verursacht, können Sie es wieder deinstallieren.

- ▶ Geben Sie im Suchfeld `appwiz.cpl` ein und wählen Sie *Installierte Updates anzeigen*, oder rufen Sie die Systemsteuerung auf und klicken Sie auf *Programme und Features - Installierte Updates anzeigen*.
- ▶ Klicken Sie doppelt auf das Update, das Sie deinstallieren möchten.  
Alternativ können Sie das Update auswählen und auf *Deinstallieren* klicken.
- ▶ Bestätigen Sie die Deinstallation mit *Ja*.



### Entfernen von Updates



Nicht alle Updates können wieder deinstalliert werden. Bei diesen Updates passiert beim Doppelklick gar nichts, und es wird auch kein Menüpunkt *Deinstallieren* angezeigt.

## Treiber automatisch herunterladen

Windows 10 verfügt über die Möglichkeit, automatisch nach passenden Gerätetreibern zu suchen, wenn Sie neue Hardware an den Rechner anschließen. Sie können das Verhalten bei der Geräteinstallation einstellen.

- ▶ Geben Sie *geräteinst* im Suchfeld ein und klicken Sie auf *Geräteinstallationseinstellungen ändern*.
- ▶ Wählen Sie Ihre bevorzugten Treiberinstallationseinstellungen.

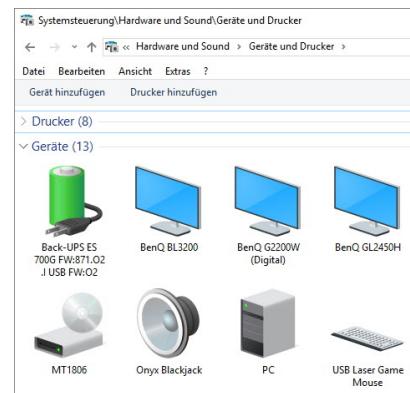
Wählen Sie *Ja*, wenn Sie möchten, dass Windows automatisch Treiber (und Symbole Ihrer Hardware) aus dem Internet nachlädt. Diese Einstellung ist empfehlenswert.



Automatischer Download von Treibern

Die Treiberinstallation über Windows Update ist ausreichend, wenn es sich um Standardgeräte ohne besondere Spezialfunktionen handelt. Falls Sie jedoch sicherstellen möchten, dass alle Funktionen der Hardware voll ausgenutzt werden, sollten Sie auch auf der Herstellerwebseite nach Treibern mit größerem Funktionsumfang und weiter reichenden Einstellmöglichkeiten suchen.

Die darstellungsgereuen Symbole erleichtern das schnelle Auffinden von Geräten im Dialog *Geräte und Drucker* durch die realitätsnahe Abbildung des Gerätes, sofern der Hersteller in der Windows-Treiberdatenbank entsprechende Abbildungen hinterlegt hat.



*Realistische Abbildungen*

#### Frequenz der automatischen Updatesuche anpassen

Windows 10 sucht nach einem internen Algorithmus in regelmäßigen Abständen nach neuen Updates. In den Gruppenrichtlinien können Sie diese Frequenz an Ihre eigenen Bedürfnisse anpassen. Dazu rufen Sie mit `gpedit.msc` die Verwaltung der Richtlinien auf und navigieren zu *Computerkonfiguration - Administrative Vorlagen - Windows-Komponenten - Windows Update*.

Auf der rechten Seite finden Sie die Einstellungen für Windows Update. Die Frequenz ändern Sie mit der Einstellung *Suchhäufigkeit für automatische Updates*. In der Richtlinie finden Sie auch die Erklärung, wie die Suche normalerweise funktioniert.

#### Patches in der grafischen Oberfläche und der Eingabeaufforderung installieren – *Wusa.exe*

Über *Einstellungen - Update und Sicherheit - Windows Update - Erweiterte Optionen - Updateverlauf anzeigen* können Sie anzeigen, welche Updates heruntergeladen und installiert worden sind. Hier erhalten Sie auch Informationen, wie etwa die ID des Patches, die Sie in der Eingabeaufforderung verwenden können.

Sie können in der Eingabeaufforderung auch mit dem Tool *Wusa.exe* Patches installieren und deinstallieren, zum Beispiel mit dem Befehl:

`Wusa.exe Windows6.1-KB976462-v2-x64.msu /quiet /norestart`

*oder*

`Wusa.exe d:\934307\Windows6.0-KB934307-x106.msu.`

<code>/quiet</code>	Installiert ohne Rückmeldung
<code>/norestart</code>	Startet den PC auch dann nicht neu, wenn der Patch das benötigt
<code>/uninstall</code>	Deinstalliert installierte Updates wieder Zusätzlich benötigen Sie die Option <code>/kb</code> . Hier geben Sie die Knowledge-Base-ID des Patches mit, zum Beispiel mit dem Befehl <code>Wusa.exe /uninstall /kb:976932.</code>
<code>/extract</code>	Entpackt den Inhalt des Updates in einen Zielordner
<code>/warnrestart</code>	Warnt bei der Verwendung von <code>/quiet</code> bei einem Neustart
<code>/forcerestart</code>	Erzwingt den Neustart des Rechners

In der Ereignisanzeige finden Sie Fehler und Einträge, wenn Sie nach der Quelle *WUSA* filtern.

In der Eingabeaufforderung können Sie auch die installierten Updates des Rechners anzeigen. Dazu verwenden Sie den Befehl `wmic qfe`. Oder Sie zeigen die installierten Updates durch den Aufruf von `systeminfo` an.

## 20.3 Probleme mit Windows Updates beheben

### Systemwiederherstellung und Updates

Startet Windows noch, funktioniert aber nicht mehr korrekt, ist der schnellste Weg, einen Systemwiederherstellungspunkt vor der Installation der Updates zurückzusetzen. Windows 10 fertigt bei jeder Installation einer Aktualisierung zunächst einen Systemwiederherstellungspunkt an. Wollen Sie diesen wiederherstellen, gehen Sie folgendermaßen vor:

- ▶ Öffnen Sie die Systemsteuerung.
  - ▶ Klicken Sie auf *System und Sicherheit - System*.
  - ▶ Wählen Sie auf der linken Seite des Fensters die Option *Computerschutz* aus.
  - ▶ Klicken Sie auf die Schaltfläche *Systemwiederherstellung*.
- oder* Geben Sie den Befehl `rstrui` über die Startseite oder die Eingabeaufforderung ein, um das Fenster *Systemwiederherstellung* direkt zu öffnen.
- ▶ Wählen Sie den Systemwiederherstellungspunkt aus, den Windows vor der Installation der Updates erstellt hat.

Sie sollten anschließend überprüfen, welche Aktualisierung die Probleme verursacht hat und diese von der zukünftigen Installation ausschließen.



Wenn Sie keine Möglichkeit haben, mit einer Windows-10-DVD einen PC zu reparieren, nachdem Windows 10 nicht mehr startet, können Sie mit einer Hardcore-Methode in den automatischen Reparaturmodus wechseln. Dazu starten Sie den PC und schalten ihn beim Booten drei bis vier Mal mit der Ausschalttaste des Computers aus. Wichtig ist, dass Windows bereits zu booten begonnen hat. Nach etwa drei bis vier Versuchen wechselt Windows 10 automatisch in den Modus zur automatischen Reparatur. In diesem Modus können Sie dann auf die bereits beschriebenen Werkzeuge zur Reparatur von Windows 10 zurückgreifen.

Die Auswahl von *Problembehandlung - Erweiterte Optionen - Starteinstellungen - Neu starten* bootet den Rechner neu und erlaubt die Auswahl der bereits von Vorgängerversionen bekannten Bootoptionen.

### Automatischen Neustart nach Updates erzwingen

Haben Sie Windows auf die aktuelle Version aktualisiert, können Sie einstellen, dass der PC automatisch neu startet, wenn Updates installiert wurden. Das ist in sicheren Umgebungen ein wichtiger Punkt. Haben Sie die Option aktiviert, dass Updates automatisch installiert werden sollen, wird jedes neue Update automatisch heruntergeladen und installiert. Diese Option ist seit April 2013 in Windows integriert. Die Einstellungen zum automatischen Neustart können Sie mit einem Registry-Eintrag setzen. Dazu öffnen Sie die Registry und navigieren zu:

`HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU`.

Erstellen Sie, falls nicht vorhanden, auf der rechten Seite einen neuen DWORD-Wert mit der Bezeichnung `AlwaysAutoRebootAtScheduledTime`. Setzen Sie den Wert auf 0, startet Windows nicht automatisch. Setzen Sie den Wert auf 1, startet Windows nach der Installation von Patches automatisch neu.

### Automatischen Neustart nach Updates deaktivieren

Viele Anwender stören sich daran, dass Windows nach der automatischen Installation von Updates sofort neu startet. Wollen Sie diese Funktion nicht, können Sie diese deaktivieren. Setzen Sie Windows 10 Pro oder Enterprise ein, können Sie dazu die Richtlinienverwaltung verwenden. Die Deaktivierung über Richtlinien nehmen Sie folgendermaßen vor:

- ▶ Rufen Sie über die Startseite den Editor für lokale Gruppenrichtlinien auf (`gpedit.msc`).
- ▶ Navigieren Sie zu *Computerkonfiguration - Administrative Vorlagen - Windows-Komponenten - Windows Update*.

Im rechten Bereich stehen Ihnen verschiedene Einstellungen für Windows Update zur Verfügung, die in der normalen Verwaltungsoberfläche der Systemsteuerung nicht verfügbar sind.

- Deaktivieren Sie die Option *Erneut zu einem Neustart für geplante Installation auffordern*. Zusätzlich sollten Sie noch die Option *Keinen automatischen Neustart für geplante Installationen ausführen* aktivieren.

### Windows Update mit Bordmitteln überprüfen – System Update Readiness Tool

Es passiert, dass Systemdateien nicht mehr funktionieren und sich Windows nicht mehr über Windows Update aktualisieren kann. Dazu hat Microsoft in Windows 10 das System Update Readiness Tool fest eingebaut. Sie können bei Problemen oder zu Testzwecken einen manuellen Scavorgang starten. Achten Sie darauf, dass ein solcher Scan durchaus bis zu einer halben Stunde dauern kann. Um einen Scavorgang zu starten, öffnen Sie eine Eingabeaufforderung mit Administratorrechten.

- Geben Sie den folgenden Befehl ein:

```
DISM /Online /Cleanup-Image /Scanhealth
```

Geben Sie folgenden Befehl ein ...	
DISM /Online /Cleanup-Image /Checkhealth	... bei Problemen nach dem Scavorgang. Dieser Befehl überprüft, ob eine Fehlermeldung im System von einem früheren Scavorgang vorliegt.
DISM /Online /Cleanup-Image /Restorehealth	... um Fehler zu reparieren.

Das Tool scannt die wichtigsten Systemdateien in Windows 10 und kann diese bei Problemen, zum Beispiel bei einer defekten Festplatte, wiederherstellen. Auch die Registry wird auf Konsistenz und einige wichtige Werte überprüft. Danach sollten Sie mit `sfc /scannow` weitere Systemdateien überprüfen. Sind Fehler auf dem System vorhanden, überprüfen Sie die Protokolldatei *CBS.Log* im Ordner *C:\Windows\Logs\CMS*.

## 20.4 Client-Computer über Gruppenrichtlinien an Windows Server Update Services anbinden

Mit Windows Server 2012 und Windows Server 2012 R2/2016 haben Unternehmen auch die Möglichkeit, zentral Patches mit den **Windows Server Update Services** (WSUS) an die Client-Computer zu verteilen. Dazu müssen die Computer über Richtlinien an den Server angebunden werden.

WSUS scannt heruntergeladene Updates und referenziert diese automatisch mit den verbundenen Clients. Einstellungen können Sie über Gruppenrichtlinien verteilen. Damit die Clients Updates installieren, müssen diese so konfiguriert sein, dass sie keine Patches aus dem Internet herunterladen, sondern den internen WSUS verwenden. WSUS verteilt die Patches nicht automatisch an die Clients, sondern lädt die Aktualisierungen nur aus dem Internet herunter und stellt diese bereit. Die Clients holen die Patches selbst vom WSUS-Server und installieren diese automatisch, abhängig von den lokalen Einstellungen beziehungsweise den Einstellungen in den Gruppenrichtlinien. Um Arbeitsstationen und Server mit Patches zu versorgen, erstellen Sie am besten spezielle Gruppenrichtlinien.

Die Konfiguration der automatischen Updates in den Gruppenrichtlinien nehmen Sie unter *Computerkonfiguration - Richtlinien - Administrative Vorlagen - Windows-Komponenten - Windows Update* vor.

Die Arbeitsstationen lassen sich so konfigurieren, dass diese automatisch Aktualisierungen vom WSUS herunterladen und installieren. Auf diesem Weg aktualisieren Sie auch den Server. Starten Sie anschließend die Computer neu und überprüfen Sie in der Windows Update-Steuerung der Systemsteuerung, ob die Anbindung erfolgreich war.

In der Systemsteuerung erhalten Sie Hinweise, falls Einstellungen zentral durch Gruppenrichtlinien vorgegeben sind. Klicken Sie auf *Einstellungen ändern*, sehen Sie, dass der Client Einstellungen über Richtlinien erhält. Diese sind für die Änderung auf dem Client festgesetzt und lassen sich nicht deaktivieren.

Anwender können aber nach der Anbindung an WSUS über den Link *Online nach Updates aus Windows Update suchen* auch im Internet nach Aktualisierungen suchen, die noch nicht auf dem WSUS zur Verfügung stehen.

Nach der Konfiguration der Gruppenrichtlinie kann es einige Zeit dauern, bis die Arbeitsstationen und Server mit WSUS verbunden sind und in der Administrationsoberfläche des WSUS erscheinen. Auf den einzelnen Rechnern können Sie in der Eingabeaufforderung durch Eingabe des Befehls `wuaclt /detectnow` eine sofortige Verbindung zum WSUS erzwingen. Ist der Client noch immer nicht angebunden, geben Sie in der Befehlszeile `gpupdate /force` und dann `Wuaclt.exe /reportnow /detectnow` ein.

## 20.5 Übung

### Windows 10 aktualisieren

Übungsdatei: --

Ergebnisdatei: *Uebung20\_E.pdf*

1. Wie starten Sie die Windows-Update-Funktion in Windows 10?
2. Wie deinstallieren Sie Updates in Windows 10?

# 21 Fehlerdiagnose und Fehlerbehebung

## In diesem Kapitel erfahren Sie

- ✓ welche Diagnose- und Fehlerbehandlungstools Windows 10 bietet
- ✓ wie das Hilfe- und Supportcenter für Windows 10 funktioniert
- ✓ wie Sie die Remoteunterstützung verwenden können
- ✓ wie Sie verschiedene Supporttools von Microsoft nutzen können

## Voraussetzungen

- ✓ Grundkenntnisse zur Eingabeaufforderung oder PowerShell

## 21.1 Allgemeine Hinweise zur Fehlerbehandlung

### Was im Fehlerfall unternommen werden kann

Trotz vieler Tests und umfangreicher Kontrollen lassen sich, schon aufgrund der Vielfalt der angebotenen Hard- und Software und der dadurch möglichen Gerätekombinationen, Fehler und Probleme nicht ausschließen. Viele Problemursachen lassen sich oft schneller und effektiver finden und beheben, wenn dazu eine standardisierte Vorgehensweise verwendet wird. Sie sollten beim Auftreten eines Fehlers zunächst folgende Schritte unternehmen:

- ✓ Benachrichtigen Sie, soweit erforderlich, andere Administratoren und Benutzer über die aufgetretene Funktionsstörung. So erhalten Sie möglicherweise bereits einige hilfreiche Zusatzinformationen.
- ✓ Arbeiten Sie folgende Checkliste ab:
  - ✓ Lässt sich das Problem reproduzieren?
  - ✓ Erscheinen neue Meldungen in der Ereignisanzeige?
  - ✓ Betrifft das Problem nur einen einzigen oder mehrere Benutzer?
  - ✓ Tritt das Problem nur auf dem lokalen Computer oder auf mehreren Computern auf?
  - ✓ Wurde irgendetwas an der lokalen Konfiguration geändert (Hardware, Treiber, Anwendungen)?
  - ✓ Funktioniert das Netzwerk?
  - ✓ Wurde auf einem Server die Konfiguration verändert?
  - ✓ Wurde ein zusätzlicher Server in Betrieb genommen?
  - ✓ Ist auf dem Computer oder einem Server die Beta-Version eines Softwareprodukts im Einsatz?
  - ✓ Sind aktuellere Treiber notwendig und verfügbar?
  - ✓ Sind für Windows 10 Updates (oder ein Service Pack) verfügbar, die das Problem beheben?
- ✓ Wenn Sie die Checkliste bearbeitet haben, verfügen Sie meist schon über recht detaillierte Informationen zu dem Problem und möglichen Lösungen. Sie können dann mithilfe einiger Werkzeuge versuchen, die Problemursache weiter einzuzgrenzen und zu beheben oder sich weitere Informationen beschaffen.

Unter Umständen ist es gerade die Aktualisierung des Betriebssystems mit einem Service Pack, die zu Problemen mit dem Computer führt. Oftmals treten auch Probleme mit Software von Drittherstellern auf, die noch nicht auf den Betrieb unter Windows 10 vorbereitet ist. In solchen Fällen sollten Sie sich nach einem Patch Ihrer Anwendung bzw. einer speziell für Windows 10 entwickelten Variante erkundigen.



## 21.2 Hilfe und Problembehandlung

### Screenshot in Windows 10 erstellen

Um Fehler zu dokumentieren hilft es oft, einen Screenshot zu erstellen. Das lässt sich in Windows 10 mit Bordmitteln erledigen. Mit Druck erstellen Sie einen Screenshot aller Bildschirme in Windows 10. Den Screenshot können Sie in jedes kompatible Programm einfügen. Entweder nutzen Sie dazu das Bearbeiten-Menü und *Einfügen* oder V. Zusätzlich wird der Screenshot als Datei im Benutzerprofil (*C:\Benutzer\<Benutzername>\Bilder*) im PNG-Format gespeichert.

Betätigen Sie nur die Drucktaste, wird keine Datei erstellt, sondern der Screenshot nur in der Zwischenablage abgelegt. Wollen Sie einen Screenshot vom aktiven Fenster machen, verwenden Sie Druck. Dabei wird der Screenshot ebenfalls nicht als Datei gespeichert, sondern in der Zwischenablage.

Verwenden Sie das Bordmittel-Tool **Snipping Tool**, können Sie einen Screenshot erstellen und diesen bearbeiten. Das Snipping Tool, das Sie über das Startmenü aufrufen, hilft bei der Erstellung und Bearbeitung von Screenshots. Sie können durch Ziehen mit der Maus einen Bereich des Desktops in die Zwischenablage kopieren und als Grafikdatei abspeichern.

### Hilfe verwenden

Mit der Hilfe bietet Windows 10 ein Portal zu den wichtigsten lokalen Informationsquellen und Tools zur Fehlerbehandlung. Sie können zusätzlich auch Microsoft-Websites in die Informationssuche einbeziehen. Folgende Themenbereiche lassen sich mit dem Hilfe- und Supportcenter bearbeiten:

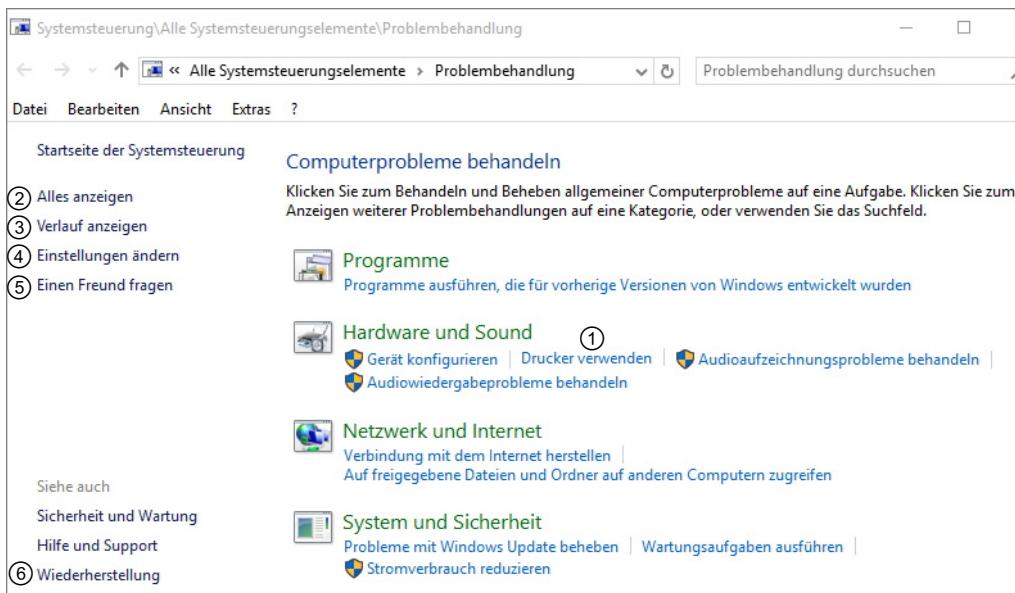
- ✓ Suche nach Begriffen
- ✓ Lösung von Hardwareproblemen (Geräte und Treiber, Windows Update und Update-Katalog)
- ✓ Lösung von Netzwerkproblemen (Internet, Kommunikation, Drucken)
- ✓ Lösung von Problemen mit der Systemkonfiguration und Anwendungsprogrammen

Bei der fertigen Verkaufsversion von Windows 10 liegt der Großteil der Inhalte des Hilfe- und Supportcenters auf Deutsch vor, es gibt aber immer noch zahlreiche Seiten, die nur auf Englisch existieren. Voraussichtlich werden die Inhalte im Laufe der Zeit weiter verändert und verbessert. Um die Hilfe zu starten, suchen Sie im Suchfeld der Taskleiste nach *Erste Schritte*.

### Problembehandlung verwenden

Windows 10 verfügt über mehrere Assistenten zur Beseitigung von Problemen und Störungen, die unter dem Begriff **Problembehandlung** in der Systemsteuerung zu finden sind. Sie starten die Sammlung auch durch Eingabe des Begriffs im Suchfeld des Startmenüs. Die Assistenten werden in vier Kategorien eingeteilt:

- |                      |                         |
|----------------------|-------------------------|
| ✓ Programme          | ✓ Netzwerk und Internet |
| ✓ Hardware und Sound | ✓ System und Sicherheit |



#### Das Hilfe- und Supportcenter zu Windows 10

- Geben Sie problembehandlung  ein.
- Klicken Sie auf einen Link, der Ihrem Problem entspricht, z. B. Drucker verwenden ①.

Es wird ein Assistent gestartet, der Sie durch die Problemerkennung und Neueinstellung leitet. Falls im Internet ein Update für die Problembehandlung vorhanden ist, wird es automatisch heruntergeladen. Auf der ersten Seite des Assistenten können Sie mit einem Klick auf *Erweitert* zusätzliche Optionen aktivieren.

Sie können eine Liste aller verfügbaren Assistenten anzeigen lassen, indem Sie auf *Alles anzeigen* ② klicken.

Sie können nachschauen, welche Assistenten bisher aufgerufen wurden ③.

In den Einstellungen ④ können Sie wählen, ob das System bei der Erkennung von Problemen Hilfe durch einen Assistenten anbieten soll und ob online nach Lösungen gesucht werden darf.

#### Kostenlose Fernwartung mit der Remotehilfe in Windows 10

Zentrales Instrument zur Verbindung zu Windows 10 über das Netzwerk oder Internet ist das Tool **Remotehilfe**. Es wird auf dem Rechner gestartet, auf dem eine Unterstützung benötigt wird und auf dem Rechner, mit dem eine Verbindung aufgebaut wird.

- Um das Tool zu starten, geben Sie `remotehilfe` im Suchfeld des Startmenüs ein.

## 21.3 Support mit Remotehilfe leisten

### Aufgabe und Funktion der Remotehilfe

Mit der Remotehilfe ist es möglich, den Bildschirminhalt eines entfernten Windows-Computers zu sehen und mit der Erlaubnis des Benutzers auch zu steuern, um Hilfe bei Problemen zu leisten. Die Verbindung wird hergestellt, indem eine Person an die andere eine Einladung zur Hilfeleistung oder ein Hilfeangebot schickt. Die Verbindung kommt nur zustande, wenn die Hilfe suchende Person die Verbindung akzeptiert.

Um eine Remotehilfe durchzuführen, muss zunächst die Remotehilfe-App auf beiden beteiligten Rechnern gestartet werden. Danach klickt der Anwender, der eine Remoteverbindung durchführen will auf *Unterstützung gewähren*. Im Gegensatz zur alten Remoteunterstützung wird die Codeerstellung nicht auf dem Rechner durchgeführt, der ferngewartet wird, sondern auf dem Rechner, der die Fernwartung durchführt.

Der Hauptunterschied zu einer Remotedesktopverbindung (vgl. Kapitel 10) besteht darin, dass hier beide Benutzer den Desktop sehen können und der lokale Benutzer vor Ort volle Kontrolle über seinen Computer behält.

Die Remotehilfe kann eingesetzt werden, wenn folgende Bedingungen erfüllt sind:

- ✓ Beide Computer nutzen Windows 10.
- ✓ Es besteht eine Netzwerkverbindung zwischen beiden Computern über LAN oder Internet.
- ✓ Wird auf beiden beteiligten Computern Windows 10 ausgeführt, besteht die Möglichkeit, eine Remoteunterstützungsverbindung mit einem Code aufzubauen. Hierbei muss keine Einladungsdatei verschickt werden. Es reicht die Eingabe des richtigen Codes.



*Remoteunterstützung nutzen*

### Remotehilfe starten

- Geben Sie im Suchfeld `remotehilfe` ein.
- Wählen Sie aus, ob Sie Remotehilfe anfordern wollen oder selbst Remotehilfe bieten.
- Danach klickt der Anwender, der eine Remoteverbindung durchführen will, auf *Unterstützung gewähren*.

Anschließend erstellt die App auf dem Computer einen 6-stelligen Sicherheitscode. Der Code bleibt 10 Minuten aktiv. Danach muss wieder ein neuer Code erstellt werden. Der Benutzer, auf dessen PC zugegriffen werden soll, benötigt diesen 6-stelligen Code.

Der Benutzer, der Hilfe benötigt, startet die App ebenfalls und wählt *Unterstützung anfordern*. Danach gibt der Benutzer den Code ein, den er vom ersten Benutzer erhalten hat und klickt auf *Senden*.



*Remotehilfe anbieten*

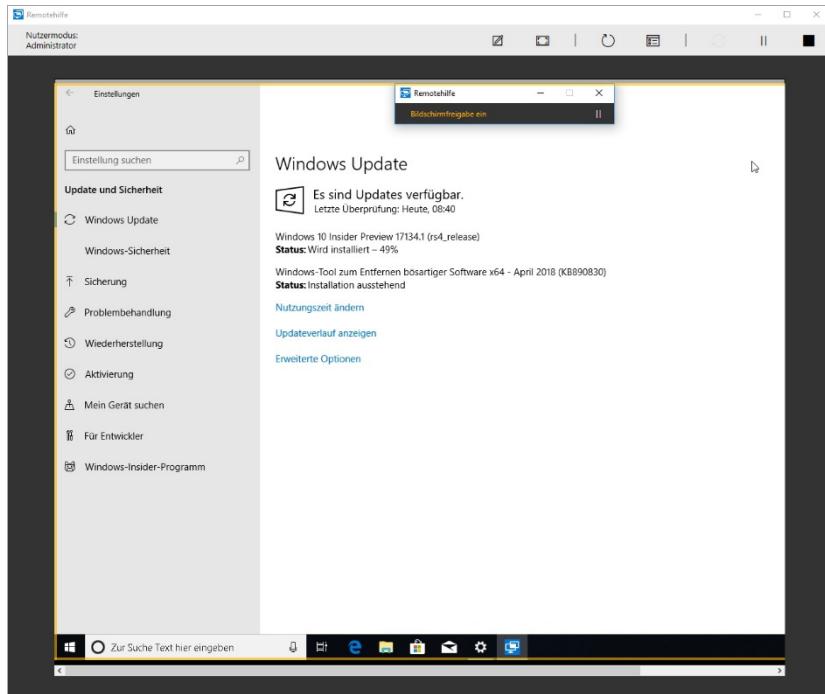
### Remotehilfe zulassen

Bevor der zugreifende Benutzer aber Zugriff erhält, erscheint ein Warnfenster, das darauf hinweist, dass ein Benutzer Zugriff auf den Rechner erhält. Der Benutzer, der Hilfe braucht, kann jetzt noch in Ruhe Programme schließen und Dokumente speichern. Danach kann die Verbindung mit *Zulassen* aktiviert werden.

Sobald die Verbindung hergestellt wird, sieht der zugreifende Benutzer den Bildschirm des anderen Computers innerhalb der Remotehilfe. Der Hilfe suchende Benutzer kann mit der Pause-Taste der Remotehilfe die Verbindung anhalten.

### Remoteunterstützung aus Sicht des Helfers

In der Kopfzeile des Fensters befinden sich einige Steuerelemente. Hier kann der Helfer die Steuerung vom Hilfesuchenden anfordern und die Darstellung anpassen.

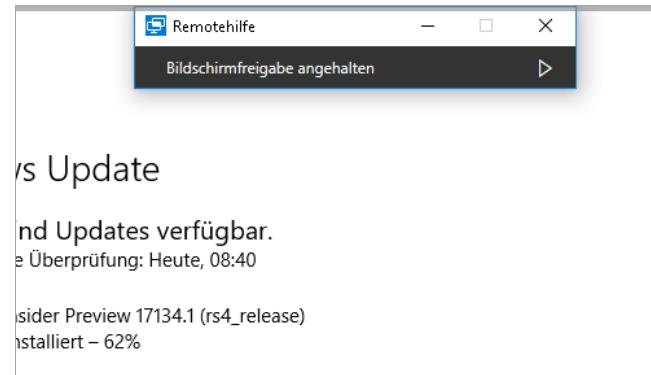


*Remoteunterstützung aus Sicht des Helfers*

### Remoteunterstützung aus Sicht des Hilfesuchenden

Beim Hilfesuchenden wird ein Fenster mit einigen Bedienflächen angezeigt. Hier kann die Steuerungsfreigabe beendet oder die Bildausgabe pausiert werden, falls der Helfer etwas nicht sehen soll. Der Benutzer hat jederzeit Kontrolle über seinen Computer und sieht alle Aktionen, die der fernwartende Benutzer durchführt.

Sinnvoll ist das zum Beispiel, wenn ein Kennwort eingegeben wird oder der zugreifende Benutzer den Inhalt des Bildschirms nicht sehen soll. Sobald die Verbindung angehalten wurde, sieht der zugreifende Benutzer den Inhalt des Bildschirms nicht mehr und erhält eine entsprechende Meldung. Die Verbindung bleibt aber bestehen.



*Remoteunterstützungsfenster des Hilfesuchenden*

## 21.4 Problemaufzeichnung/Schrittaufzeichnung verwenden

### Problemaufzeichnung/Schrittaufzeichnung verwenden

Das Windows-Tool **Problemaufzeichnung** (engl. **Problem Step Recorder** – PSR), in aktuellen Windows-10-Versionen auch als „Schrittaufzeichnung“ bezeichnet, ist ein Tool, das Hilfesuchende dabei unterstützt, eine Aufzeichnung eines nachvollziehbaren Problems anzufertigen, das anschließend von einem Helfer leicht ausgewertet werden kann.

Bei der Aufzeichnung werden alle Handlungen Schritt für Schritt als Bilder aufgenommen und in einer HTML-Datei eingefügt. Der Hilfesuchende kann dabei wichtige Bildbereiche rot hervorheben und Kommentare anfügen.

- ▶ Betätigen Sie  und geben Sie PSR in das Suchfeld ein.  
Die Symbolleiste **Schrittaufzeichnung** wird eingeblendet.
- ▶ Starten Sie eine Aufnahme, indem Sie auf **Aufzeichnung starten** ① klicken. Sie können jederzeit die Aufzeichnung anhalten und fortsetzen.
- ▶ Führen Sie nun die Arbeitsschritte aus, die zu dem Problem führen, und geben Sie falls notwendig an der entsprechenden Stelle schriftlich einen Kommentar ② ein.
- ▶ Um die Aufzeichnung abzuschließen, klicken Sie auf **Aufzeichnung beenden** ③. Speichern Sie nun die Aufzeichnung in Form einer ZIP-Datei ab, die ein HTML-Dokument enthält, oder versenden Sie die Aufzeichnung als ZIP-Datei per E-Mail.



Steuerung der Schrittaufzeichnung

Ihr Helfer kann die Aufzeichnung dann mit einem beliebigen HTML-Browser ansehen.

Die Aufzeichnungsdatei enthält neben den bebilderten Handlungsschritten, bei denen das aktive Element grün hervorgehoben ist, eine zusätzliche Auflistung der einzelnen Schritte in Textform.

```

Schritt 15: Klick mit der linken Maustaste durch Benutzer auf "Deaktivieren (Menüelement)"
Programm: Windows-Explorer, 6.2.8250.0 (winmain_win8beta.120217-1520), Microsoft Corporation,
Benutzeroberflächenelemente: Deaktivieren, Kontextmenü, #32768

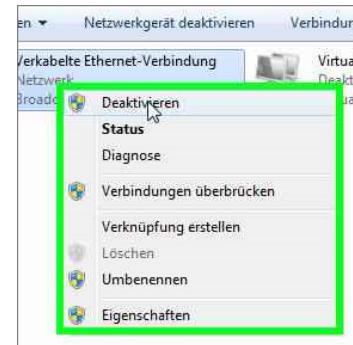
Schritt 16: Start des Ziehens mit der Maustaste durch Benutzer auf "Elementansicht (Liste)" ↪
Programm: Windows-Explorer, 6.2.8250.0 (winmain_win8beta.120217-1520), Microsoft Corporation,
Benutzeroberflächenelemente: Elementansicht, UIItemsView, Shellordneransicht, DUILListView, OI

Schritt 17: Ende des Ziehens mit der Maustaste durch Benutzer auf "Netzwerkverbindungen (Fenster)" ↪
Programm: Windows-Explorer, 6.2.8250.0 (winmain_win8beta.120217-1520), Microsoft Corporation,
Benutzeroberflächenelemente: TravelBand, ReBarWindow32, WorkerW, Netzwerkverbindungen, CabinetView

Schritt 18: Benutzerkommentar: "Wichtig!"
Programm:
Benutzeroberflächenelemente:

Schritt 19: Klick mit der rechten Maustaste durch Benutzer auf "Deaktiviert (Bearbeiten)" in
Programm: Windows-Explorer, 6.2.8250.0 (winmain_win8beta.120217-1520), Microsoft Corporation,
```

Zusätzliche Auflistung der Handlungsschritte in Textform



Automatische Hervorhebung



<b>A</b>					
Abgesicherter Modus	49	Benutzerkontingente	183	Datenobjekt	197
ACPI (Advanced Configuration and Power Interface)	69, 100	Benutzernamen festlegen	32	Datenquelle	198
ADK, Assessment and Deployment Kit	26	Benutzerprofile	133	Datensammlersatz	198
Administrator	124	Benutzerprofile verwalten	134	Datenschutz	60
Aktualisieren auf Windows 10	34	Benutzerprozesse überwachen	193	Datenschutzeinstellungen	32, 115
Aktuelle Konfiguration einsehen	62	Benutzerumgebung	133	Datensicherheit	213
Anmelden	125	Benutzerverwaltung	122	Datensicherung, Arten	216
Anmeldeversuche überwachen	131	Bereitstellen, Mounten	178	Datensicherung, Strategien	217
Anmeldung umschalten	125	Bereitstellungspunkt	174	Datenträger	174
Anmeldung, Domäne	45	Besitz übernehmen	158	Datenträger hinzufügen	178
Anmeldung, Fernanmeldung	45	Besitz übernehmen, Registrierungsschlüssel	210	Datenträger initialisieren	178
Anmeldung, lokale	45	Betriebssystem aktualisieren	232	Datenträger konvertieren	176, 178
Anwendungsprogramme deinstallieren	57	Betriebssystem auswählen	46	Datenträger, dynamischer	175
Anwendungsprogramme installieren	56	Bildschirmauflösung	53	Datenträgerbereinigung	181
Anwendungsprotokoll	188	Bildschirmdarstellung anpassen	52	Datenträgerverwaltungskonsole	177
Anzeige für kleine Displays	55	Bildschirmecellen	55	Deinstallation, Anwendungsprogramme	57
Anzeigeeigenschaften einstellen	52	Bildschirmfrequenz	53	DHCP	21
APIPA (Automatic Private IP Addressing)	21, 92	Bindungsreihenfolge der Netzwerkverbindungen	98	DHCPv6	21
AppLocker	150	BitLocker	184	Dienste überwachen	194
Apps entfernen	59	BitLocker aktivieren	149	Dienste verwalten	66
Apps herunterladen	58	BitLocker To Go	186	Dienste, Starttyp	68
Apps/Applications	8	Booteintrag erstellen	43	Differenzialkomprimierung	218
App-Verlauf überwachen	193	Bootvorgang	40	Digitale Signatur für Treiber	101
Arbeitsgruppe	18	Buffer Overflow	66	Diskquota	183
Arbeitsgruppe, Computer hinzufügen	89	<b>C</b>		DMZ (Demilitarized Zone)	109
Arbeitsspeicher, Diagnose	194	CAT	17	DNS (Domain Name System)	22
ARM, Prozessor	9	Checkliste für Installation	27	DNS, Einstellungen	93
Auffrischen	221	chkdsk	180	DNS-Namensauflösung	93
Aufgabe	79	Client	18, 99	DNS-Suffix	89
Aufgabenblock	79	Cloud, Einstellungen synchronisieren	58	DNS-Suffix automatisch anhängen	93
Auslagerungsdatei konfigurieren	65	Cluster	179	DNS-Suffix-Anpassung	89
Authentifizierung	123	Cmdlet, PowerShell	229	Domäne	18
Autologon	125	Cmdlets	229	Domäne, Computer hinzufügen	90
Autostarts überwachen	193	CMS	40	DPI, Dots per Inch	53
<b>B</b>		Commandlet, PowerShell	229	Driver Store	106
Basisdatenträger	174	Computernamen	89	Druckauftrag verwalten	169
Basisvolumes	174	Computernamen ändern	89	Drucken, Berechtigungen verwalten	171
Batchdateien	227	Computerreparaturoptionen	38	Drucken, Probleme beheben	173
Benutzer anlegen	129	Connected Standby	70	Drucker	160
Benutzer verwalten	127	Cookies	115	Drucker freigeben	164
Benutzer, verbundene anzeigen	195	Core-Dump	64	Drucker, Bezeichnungen	160
Benutzeranmeldung	123	<b>D</b>		Drucker, LPR-Drucker einrichten	165
Benutzereinstellungen, Ablageort	52	Datei-Explorer siehe <i>Internet Explorer</i>		Drucker, Standarddrucker festlegen	166
Benutzerkontensteuerung	128	Dateien, geöffnete anzeigen	195	Druckerordner	162
Benutzerkontensteuerung anpassen	128	Dateisystem NTFS	11	Druckerpool	161
		Dateisysteme für Installation	27	Druckerpool einrichten	165
		Dateiversionsverlauf	217	Druckertreiber aktualisieren	167
		Daten wiederherstellen	220	Druckerwarteschlange	161
		Datenausführungsverhinderung	66	Druckerwarteschlange verwalten	168
				Druckgeräte	160
				Druckserver	161
				DSC (Desired State Configuration)	231

<b>E</b>	Edge 114, 202 Edge anpassen 118 Edge, Browser 114, 202 Editionen, Windows 10 9 Effektive Berechtigungen 156 EFS und Freigaben 159 Eingabeaufforderung 224, 227	Gruppen verwalten 132 Gruppenmitgliedschaft verwalten 132 Gruppenrichtlinien 138, 148, 158 Gruppenrichtlinien, Benutzerkonfiguration 143 Gruppenrichtlinien, Computerkonfiguration 141	<b>J</b> Junctions 11
<b>F</b>	Fehler, Ereignisanzeige 189 Fehlerbehandlung 239 Fehlversuchüberwachung 189 File History 217 Firewall 109, 142 Formatierung 179 Fragmentierung 182 Freigabe 152 Freigabe anzeigen 194 Freigabe verwalten 195 Freigabe, Verbinden mit 152 Freigabeberechtigungen verwalten 154 Freigaben verbinden 90	Hard Links 11 Hardware deaktivieren 104 Hardware deinstallieren 105 Hardware entfernen, Hot-Plugging 105 Hardware hinzufügen 100 Hardware, Probleme behandeln 105 Hardware-Mindestanforderungen 25 Hauptbenutzer 124 Heimnetzgruppe 18 Hilfesuchender, Remotehilfe 242 Histogramm 198 HKEY, Unterstrukturen der Registrierung 205	<b>K</b> Kernelschutz 101 Kernspeicherabbild 64 Kioskmodus 117 Komprimierung 179 Konfiguration einsehen 62 Kontingente 183 Kontingentverwaltung 184 Konto aktivieren/deaktivieren 129 Konto löschen 131 Konto sperren/entsperren 130 Konto umbenennen 130 Konto wechseln 32 Kontorichtlinien 142 Kontosperrung einrichten 144
<b>G</b>	Gast 124 Gateway 20 Geräte aktivieren/deaktivieren 69 Geräte installieren 101 Geräte-Manager 69, 103 Geräte-Manager, ausgeblendete Geräte anzeigen 105 GPT-Datenträger 174 Group Policy Preferences 147 Gruppen 122 Gruppen anlegen 132 Gruppen löschen 133	Information, Ereignisanzeige 189 InPrivate-Modus 115 Installation, Anwendungsprogramme 56 Installation, Treiber ohne gültige Signatur 105 Installation, Windows 10 24 Instanz 197 Internet Explorer auf die Standard-einstellungen zurücksetzen 116 Internet Explorer, Datenschutzeinstellungen 115 Internet Explorer, Richtlinien 116 Internet Explorer, Sicherheitseinstellungen 115 Internet Protocol 19 Internetdomäne 109 Internetoptionen 114 Internetzugang einrichten 110 Internetzugang, Grundlagen 108 IP-Adresse anzeigen 95 IP-Adresse, Konfiguration 21 ipconfig 95 IPv4-Adresse 19 IPv4-Adresse vergeben 93 IPv6-Adresse 96 ISE (Integrated Scripting Environment) 230	<b>L</b> LAN 16 Laufwerke optimieren 182 Leasedauer 22 Legacy 224 Leistungsindikator 197 Leistungsindikatorenliste 196 Lesemodus für Webseiten 117 Line Printer Daemon 161 Local Area Network 16 Lokale Anmeldung 123 Lokale Drucker 160 LPR (Line Printer Remote) 161 LPR-Anschlussmonitor 165
<b>M</b>	MAC-Adresse 21 MBR (Master Boot Record) 11, 40 MBR-Datenträger 174 Messdaten anzeigen 195 Messdaten definieren 197 Microsoft Edge 114 Microsoft-Konto 33, 51 Mirroring 213 MMC (Microsoft Management Console) 74 MMC starten 77 MMC, Aufgabe 79 MMC, Aufgabenblock 79 MMC, Detailfenster 76 MMC, Zugriff beschränken 82 MMC, Zugriffsmodi 75, 77 MMC-Konsole 74 MMC-Konsole öffnen 83		

MMC-Konsole sichern	81	Public Key, Richtlinien	142	Schlüsselzugriffe überwachen, Registrierung	211
mount	11			Schnellformatierung	179
Mounten	174			Schrittaufzeichnung	244
MS-DOS-Subsystem	224			Service Pack	232
MSINFO32	62			<i>setupact.log</i>	38
Multimonitorbetrieb	54			<i>setuperr.log</i>	38
Multitasking optimieren	64			Setup-Protokolle	38
<b>N</b>					
<i>net use</i>	91	RAID 0	176, 180	Sicherheitsereignisse	190
NetBIOS	20	RAID-Level	176	Sicherheitsprotokoll	145, 188
NetBIOS-Name	89	ReFS (Resilient File System)	11	Sicherheitsvorlagen	139
Netzwerk	16	REG, Wertetypen der Registrierung	205	Sicherheitsvorlagen anwenden	146
Netzwerkanmeldung	123	<i>Regedit.exe</i>	206	Sichern und Wiederherstellen	223
Netzwerkdrucker	161	Registrierung (Registry)	204	Sicherungs-Operator	124
Netzwerkfreigabe kontrollieren	195	Registrierungsdaten drucken	206	SID (Security Identifier)	123
Netzwerkidentifikation	21, 88	Registrierungsdaten hinzufügen	209	Snap-In	74
Netzwerkkomponenten	99	Registrierungsdatenbank	204	Snap-In entfernen	78
Netzwerkkonfigurations-Operator	124	Registrierungseditor	206	Snap-In hinzufügen	77
NTFS (New Technology File System)	10, 27	Registry sperren	208	Snap-In, eigenständiges	79
NTFS-Berechtigungen	155	Registry, Tools zur Verwaltung	208	Snap-In, Erweiterungen	79
NTFS-Berechtigungen einstellen	157	Remoteanmeldung	123	Soft Links	11
NX-Flag	66	Remotedesktop	120	Speicherplätze	212
<b>O</b>					
Oktette	19	Remotedesktop aktivieren	120	Speicherpools	212
OneDrive	33	Remotedesktopbenutzer	124	Spezielle Berechtigungen	156
<b>P</b>					
Parität (Parity)	213	Remote-Desktop-Protokoll	120	Spiegelung	213
Partitionen für Installation	27	Remotehilfe	242	Spooler	160
Peer-to-Peer-Netzwerk	18	Remotehilfe starten	242	Spoolordner	161
Plug & Play	100	Replikations-Operator	124	Spoolordner verschieben	169
POST	40	Reset	221	Sprachpakete installieren	31
Power-on Self Test	40	Resiliency	213	Standardbenutzerprofil	135
PowerShell	229	Ressourcen zuweisen	103	Standardbetriebssystem	63
PowerShell starten	229	Richtlinien für Internet Explorer	116	Standardgateway	20
PowerShell, Befehle	227	Richtlinien verwalten	140	Standortunabhängiges Drucken	168
PowerShell-Skripts	230	Richtlinien, domänenweite	140	Startoptionen, erweiterte	41, 46
Problemaufzeichnung	244	Richtlinien, lokale	140	Startvolume	176, 183
Problembehandlung	47	Roaming Profiles	135	Store, Proxy verwenden	59
Probleme beheben bei der Installation	37	<i>robocopy</i>	134	Stripesetvolume	176, 179
Product Key, Windows-Aktivierung	35	Router	20	Subnetzmaske	19
Profilbild ändern	127	Routing	20	Switch	17
Profilordner verschieben	134	RSAT (Remote Server Administration Tools)	83	Symbolischer Link	134
Programmkompatibilität	61	SAM (Security Account Manager)	123	Synchronisierung	135
Protokoll löschen	191	Sammlungssatz	198	System überwachen	144, 193
Protokolldatei	196	Schlüssel (Registrierung)	204	System Update Readiness Tool	237
Proxyserver	109	Schlüssel sichern, Registrierung	207	Systemabbild	48
Prozesse überwachen	191	Schlüssel und Werte löschen, Registrierung	209	Systemabbild erstellen	223
Prozessorauslastung	195	Schlüssel wiederherstellen, Registrierung	207	Systemeigenschaften	63
Prüfpunkte, Hyper-V	86	Schlüsselsicherheit verwalten, Registrierung	210	Systeminformationen	62
<b>S</b>					
SAM (Security Account Manager)	123	Systeminformationsprogramm	62	Systeminformationsprogramm	62
Sammlungssatz	198	Systemleistung überwachen	192	Systemleistung überwachen	192
Schlüssel (Registrierung)	204	Systemmonitor	195	Systemmonitor	195
Schlüssel sichern, Registrierung	207	Systemmonitor, Anzeige verändern	198	Systemmonitor, Anzeige verändern	198
Schlüssel und Werte löschen, Registrierung	209	Systemprotokoll	189	Systemprotokoll	189
Schlüssel wiederherstellen, Registrierung	207	Systemstart	40	Systemstart	40
Schlüsselsicherheit verwalten, Registrierung	210	Systemstart, Optionen	46	Systemstart, Optionen	46
		Systemsteuerung	50	Systemsteuerung	50

Systemverhalten	64	Updates Probleme beheben	236	Werte bearbeiten, Registrierung	207				
Systemvolume	176	Updatesuche anpassen	235	Windows 10	9				
Systemwiederherstellung	222	USB-Stick erstellen	28	Windows 10 aktivieren	35				
<b>T</b>									
Task-Manager	191	Verbindung trennen	195	Windows 10 Education	9				
TCP (Transmission Control Protocol)	19	Verborgene Freigaben	159	Windows 10 Enterprise	9				
TCP/IP	19, 92	Vererbung, NTFS	155	Windows 10 for Mobile	10				
TCP/IP konfigurieren	92	Versionen, Windows	8	Windows 10 installieren	29				
Testzeitraum verlängern	36	VHD (Virtual Hard Disk)	183	Windows 10 Pro	9				
Thin Provisioning	212	Virtualisierungstechnik, Windows 10	84	Windows aktualisieren	232				
TPM-Chip	184	Virtuelle Switches	84	Windows einsetzen	8				
Treiber	104	Virtuelle Volumes	183	Windows Hello	136				
Treiber	100	Virtueller Arbeitsspeicher	64, 65	Windows Server 2012 R2 mit Windows 8.1 zu verwalten	83				
Treiber aktualisieren oder zurücksetzen	106	Volume	174	Windows Update verwenden	232				
Twisted-Pair-Kabel	16	Volume bereinigen	181	Windows-7-Dateiwiederherstellung	223				
<b>U</b>									
UAC	128	Volume erstellen	179	Windows-Firewall aktivieren	111				
Übertragungsgeschwindigkeit	17	Volume formatieren	179	Windows-Firewall, Ausnahmen definieren	112				
Überwachen, Zugriffe	157	Volume löschen	180	Windows-Firewall, Funktionsweise	111				
Überwachungsrichtlinien	144, 190	Volume prüfen	180	Windows-Funktionen ein-/ausschalten	60				
UEFI (Unified Extensible Firmware Interface)	40	Volume, dynamisches	175	WINS	22				
UEFI, Compatibility Support Module	40	Volume, einfaches	176	Wireless LAN	16				
Umgebungsvariablen	64	Volume, übergreifendes	176	WLAN	16				
UNC (Uniform Naming Convention)	152	Volumebezeichnung	179, 180	WMI (Windows Management Instrumentation)	230				
Unterstruktur, Registrierung	204	<b>W</b>							
Updates installieren	235	Warnung, Ereignisanzeige	189	<b>Z</b>					
		Wartungsscenter	200	Zeitplan	199				
		WDK (Windows Driver Kit)	101	Zugriffsberechtigungen	132				
		Websitenotizen	117	Zuordnungseinheit	179				
		Wert, Registrierung	205						

# Impressum

Matchcode: W10S

Autor: Thomas Joos

Produziert im HERDT-Digitaldruck

2. Ausgabe, September 2018

HERDT-Verlag für Bildungsmedien GmbH  
Am Kümmerling 21-25  
55294 Bodenheim  
Internet: [www.herdt.com](http://www.herdt.com)  
E-Mail: [info@herdt.com](mailto:info@herdt.com)

© HERDT-Verlag für Bildungsmedien GmbH, Bodenheim

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder einem anderen Verfahren) ohne schriftliche Genehmigung des Verlags reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Dieses Buch wurde mit großer Sorgfalt erstellt und geprüft. Trotzdem können Fehler nicht vollkommen ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Wenn nicht explizit an anderer Stelle des Werkes aufgeführt, liegen die Copyrights an allen Screenshots beim HERDT-Verlag. Sollte es trotz intensiver Recherche nicht gelungen sein, alle weiteren Rechteinhaber der verwendeten Quellen und Abbildungen zu finden, bitten wir um kurze Nachricht an die Redaktion.

Die in diesem Buch und in den abgebildeten bzw. zum Download angebotenen Dateien genannten Personen und Organisationen, Adress- und Telekommunikationsangaben, Bankverbindungen etc. sind frei erfunden. Eventuelle Übereinstimmungen oder Ähnlichkeiten sind unbeabsichtigt und rein zufällig.

Die Bildungsmedien des HERDT-Verlags enthalten Verweise auf Webseiten Dritter. Diese Webseiten unterliegen der Haftung der jeweiligen Betreiber, wir haben keinerlei Einfluss auf die Gestaltung und die Inhalte dieser Webseiten. Bei der Bucherstellung haben wir die fremden Inhalte daraufhin überprüft, ob etwaige Rechtsverstöße bestehen. Zu diesem Zeitpunkt waren keine Rechtsverstöße ersichtlich. Wir werden bei Kenntnis von Rechtsverstößen jedoch umgehend die entsprechenden Internetadressen aus dem Buch entfernen.

Die in den Bildungsmedien des HERDT-Verlags vorhandenen Internetadressen, Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen waren zum Zeitpunkt der Erstellung der jeweiligen Produkte aktuell und gültig. Sollten Sie die Webseiten nicht mehr unter den angegebenen Adressen finden, sind diese eventuell inzwischen komplett aus dem Internet genommen worden oder unter einer neuen Adresse zu finden. Sollten im vorliegenden Produkt vorhandene Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen nicht mehr der beschriebenen Software entsprechen, hat der Hersteller der jeweiligen Software nach Drucklegung Änderungen vorgenommen oder vorhandene Funktionen geändert oder entfernt.