



Windows 10

CLUBSYSTEM

WINDOWS 10 T <mark>EIL 3</mark>

9 Benutzerverwaltung und Anmeldung
10 Rechte und Berechtigungen
11 Fernwartung und Fernzugriff
12 Serverfeatures
13 Drucker



leil

Inhalt

LIESMICH



(•)



Windows begleitet uns nun schon seit fast 30 Jahren. Christian Zahler ermöglicht uns eine ausführliche sehr Beschreibung in mehreren Teilen.

- 2 Liebe Leser, Inhalt Franz Fialo
- 2 Impressum, Autoren, Inserenten, Services

CLUBSYSTEM

- Inhaltsverzeichnis 3 Christian Zahler
- 9 Benutzerverwaltung und Anmeldung 4 Christian Zahler
- 10 Rechte und Berechtigungen 14
- 11 Fernwartung und Fernzugriff 23 Christian Zahler
- 12 Serverfeatures 26 Christian Zahler
- 13 Drucker 27 Christian Zahler

Liebe Leser!

Franz Fiala

Windows 10 Teil 3

Wir setzen unseren Lehrgang über Windows 10 von Christian Zahler mit den Kapiteln Benutzerverwaltung und Anmeldung, Rechte und Berechtigungen, Fernwartung und Fernzugriff, Serverfeatures, und Drucker fort (Seite 3 bis 31).

Wie sang schon Marika Röck im Film "Kora Terry" 1940: "Im Leben geht alles vorüber, auch das Glück doch zum Glück auch das Leid". In diesem Sinn schauen wir in eine hoffentlich normalisierte Zukunft. Nicht vergessen: -> Hier geht's zur Impfung



(Stiegenaufgang zum Austria Center)



Autoren

Fiala Franz Dipl.-Ing. 1948



1,2 Präsident von ClubComputer, Leitung der Redaktion und des Verlags der PCNEWS, Lehrer für Nachrichten-technik und Elektronik .i.R. Werdegang Arsenal-Research, TGM Elektronik Absolvent TU-Wien, Nachrichtentechnik franz.fiala@clubcomputer.at http://fiala.cc/

Zahler Christian Ing. Mag. 1968 3-31



Erwachsenenbildung, MCSE, Lehrer für Elektro- und Automatisierungstechnik, Technische Mechanik und Informatik am Francisco-Josephinum Wieselburg Firma HBLFA Francisco-Josephinum; WIFI

Absolvent TU-Wien <u>office@zahler.at</u> http://www.zahler.at/

Inserenten

techbold

Dresdner Straße 89 1200 Wien +43 134 34 333 office@techbold.at http://www.techbold.at

Produkte Reparatur, Aufrüstung, Softwareinstallation, Daten-rettung, Installation und Wartung von IT-Anlagen.



Impressum

Impressum, Offenlegung

Richtung Auf Anwendungen im Unterricht bezogene Informationen über Personal Computer Systeme. Berichte über Veranstaltungen des Herausgebers.

Erscheint 4 mal pro Jahr: Mär, Jun, Sep, Nov ISSN 1022-1611

Herausgeber und ClubComputer Verleger Siccardsburggasse 4/1/22 1100 Wien 01-6009933-11 FAX: -12

<u>https://clubcomputer.at/</u> ZVR: 085514499 IBAN: AT74 1400 0177 1081 2896 Mitgliedsbeitrag 2019: 46,-Euro Konto: AT74 1400 0177 1081 2896 oder PayPal<u>office@clubcomputer.at</u>

Digital Society Graben 17/10 1010 Wien 01-314 22 33 info@DigiSociety.at https://digisociety.at/

<u>https://digiso</u> ZVR: 547238411 IBAN: AT45 3266 7000 0001 9315

Druck Ultra Print Pluhová 49, SK-82103 Bratislava http://ww

PDF-Version http://d.pcnews.at/ pdf/n169.pdf



Services



Diese Adresse zeigt alle Aspekte einer Mitgliedschaft bei ClubComputer. Online sind alle Inhalte menügeführt. Das Kürzel ist wichtig für den Verweis auf eine konkrete Seite.

Wer lieber ein gedrucktes Dokument liest, kann ein solches über den 🖶 Druck-Button rechts oben herstellen. Über den Menü-Button kann man das Menü ausblenden, über den ØLink-Button kann man über einen QR-Code die Seite am Handy anzeigen lassen. Über � kann man im Verlauf der bereits besuchten Seiten blättern.

In der PDF-Version dieser Ausgabe führen die Links direkt zu der betreffenden Seite.

A Verein

32

cc|clubcomputer · cc|finanzen · cc|history · cc|hotl ine · cc|konto · cc|mitglieder · cc|support · cc|vorst and ·

Giffentlich

 $\underline{at|wissen} \cdot \underline{cc|allapps} \cdot \underline{cc|exweb} \cdot \underline{cc|inhalte} \cdot \underline{cc|n}$ ewsletter · cc|wapps · pc|123 · pc|pdf ·

Persönlich

 $\underline{at|asp} \cdot \underline{at|billing} \cdot \underline{at|domain} \cdot \underline{at|drive} \cdot \underline{at|ftp} \cdot \underline{a}$ t|mail · at|panel · at|php · at|press · at|server ·

6 Extern

at|facebook · at|status · cc|facebook · cc|medien · cc|youtube ds|facebook ds|medien ds|youtub е

🖶 Druck

cc|folder · cc|pp · cc|visit · ds|folder · pc|news ·

Partner

at | cccat · at | htl3r · cc | adim · cc | jix · cc | kultur · cc | mcca cc|metro cc|techbold cc|tgm ds|digisoci ety pc|mtm pc|pcnews pc|ultraprint

🙁 Wir

cc|calendar · cc|heuriger · cc|meating · cc|weihnac ht ds digitalk

💄 Du

cc|card · cc|clubid · cc|mitmachen · cc|webfree · cc welcome

🖝 Hilfe

<u>cc|statuten · xx|hilfe · xx|links</u> · <u>xx|pages</u> · <u>xx|sitema</u> <u>p · xx|standorte</u> ·

Versand 16Z040679 M

Namensnennung, nicht kommerziell, keine Bearbeitungen http://creativecommons.org/licenses/by-nc-nd/4.0/

Windows 10 Inhaltsverzeichnis

Christian Zahler

Teil 1 PCNEWS-167 7.2 7.3 74

- 1 **Das Betriebssystem Microsoft** Windows 10 (Seite 7) 1.1 Editionen (SKUs, Stock Keeping Units) von Windows 10 1.2 Übersicht: Neue Features in Windows 10 1.3 Prozessorarchitektur: 32 bit/64 bit-Versionen 1.4 Hardwarevoraussetzungen 1.5 Architektur von Windows Informationsquellen und Hilfe (Seite 2 11) 2.1 Knowledge Base 2.2 Whitepapers Hilfefunktionen 2.3 Windows 10-Installation (Seite 12) 3 3.1 Grundsätzlicher Installationsablauf Ablauf einer beaufsichtigten Neuinstal-3.2 lation
- 3.3 Startfähiges USB-Installationsmedium mit dem Media Creation Tool
- 3.4 Upgrade von Windows 7, Windows 8 oder 8.1 auf Windows 10
- Windows 10-Lizenzierung und Pro-3.5 duktaktivierung
- 3.6 Windows 10-Funktionsupgrades
- Hinzufügen von optionalen Features 37 An- und Abmeldung, Benutzerkonten 4 und Kennwörter (Seite 20)
- 4.1 Anmeldung und Abmeldung
- 4.2 Computer sperren und entsperren
- Benutzer wechseln 4.3
- 4.4 Windows herunterfahren
- 45 Kennwörter (Passwords)
- 4.6 Kennwörter ändern Desktop, Startmenü, Taskleiste, Datei-5 management (Seite 23)
- 5.1 Startmenü
- Finden und Aufrufen von Apps 5.2 5.3 App-Symbole an die Taskleiste anheften
- 5.4 Sprunglisten
- Info-Center 5.5
- 5.6 Arbeiten mit Desktop-Apps Virtuelle Desktops
- 5.7
- 5.8 Screenshots
- Videos und Screencasts mit Windows 5.9 10-Bordmitteln
- 5.10 Tabletmodus
- 5.11 Der Windows-Explorer
- 5.12 OneDrive
- 5.13 Präsentieren mit Laptop und Videobeamer
- 5.14 Webbrowser

Teil 2 PCNEWS-168

- Softwareinstallation und -6
- deinstallation (Seite 7) 6.1 Beziehen von Apps aus dem Microsoft
- Store 6.2
- Apps installieren und deinstallieren 6.3
- Installation von Office 2019 Enterprise Edition
- Windows 10-Verwaltung (Seite 9)
- 7.1 Grafische Verwaltungstools

- Textorientierte Oberflächen
- Hintergrundbild ändern
- Sperrbildschirm konfigurieren,
- Windows-Blickpunkt
- 7.5 Schriftgröße einstellen 7.6 Anpassen der Bildschirmeinstellungen
- 7.7 Energieverwaltung
- 7.8 Task- und Prozessverwaltung
- 7.9 Registry (Registrierungsdatenbank)
- Windows 10 im Netzwerk (Seite 20) 8
- 8.1 Netzwerk-Grundlagen, wichtige Begriffe
- 8.2 Netzwerkeinstellungen
- Konfiguration der Netzwerkkarte: IP-8.3 Adressen
- 8.4 Verbindung mit einem WLAN herstellen
- 8.5 Netzwerkprofile
- Virtualisierung Client Hyper-V (Seite 16 25
- Client Hyper-V 16.1
- Booten von VHD Dual- bzw. Multi-16.2 Boot-Konfigurationen
- 16.2.1 Erstellen einer VHD auf grafischem Weg
- 16.2.2 Erstellen einer virtuellen Festplatte mit diskpart
- 16.2.3 Windows im virtuellen Datenträger bereitstellen und Startmenüeintrag erstellen

Teil 3 PCNEWS-169

- 9 Benutzerverwaltung und Anmeldung (Seite 4) 9.1 Ablauf des Anmeldevorgangs in Windows 9.2 Arten von Benutzerkonten 9.3 Anmeldeoptionen und Windows Hello Security Principals 9.4 9.5 Kontotyp: Lokale Benutzer zu lokalen Administratoren machen 9.6 Kennwörter an Webseiten und eigene Anmeldeinformationen verwalten 9.7 Benutzerverwaltung lokaler Benutzer in der Computerverwaltung 9.8 UAC (Benutzerkontosteuerung, User Account Control)
- Programmausführung mit geändertem 9.9 Benutzerkontext
- 9 1 0 Benutzerprofile
- Öffentliche Ordner 9.11
- Rechte und Berechtigungen (Seite 14) 10
- 10.1 Lokale Gruppen 10.2
- NTFS-Berechtigungen Zugriffstoken und Sicherheitsdes-10.3 kriptoren
- 10.4 Netzwerkerkennung und Freigaben

Fernwartung und Fernzugriff (Seite 11

- 23) 11.1 Remotedesktop
- 11.2 Remotehilfe
- Remoteunterstützung 11.3
- 11.4 TeamViewer
- Windows 10-Features mit Windows 12 Server 2016/2019 (Seite 26)
- 12.1 Always On VPN
- 12.2 Neue Remote Desktop-Dienste 12.3 BranchCache

- Drucker (Seite 27) 13
- 13.1 Ablauf des Druckvorgangs
- Einrichten eines lokalen Druckerob-13.2 iekts
- Drucker entfernen 13.3
- Erzeugen eines TCP/IP-13.4
- Druckeranschlusses
- 13.5 Druckserver konfigurieren
- Druckerverwaltung 13.6
- 13.7 **Einrichten eines Druckerpools**
- 13.8 Berechtigungen für logische Druckerobjekte

Teil 4 PCNEWS-170

- Datenträgerverwaltung, Startvorgang 14
- und Notfallwiederherstellung
- 14.1 Datenspeicherung auf Datenträgern
- 14.2 Formatierung und Dateisysteme
- Dynamische Datenträger und RAID 14.3 Speicherpools und Speicherplätze 14.4
- (Storage Pools, Storage Spaces)
- 14.5 Befehlszeilentools zur Datenträgerverwaltung
- 14.6 Speicheroptimierung
- 14.7 Defragmentierung
- 14.8 ReadyBoost

14.15

14.16

14.17

15

15.1

15.2

15.3

15.4

15.5

17.1

17.2

17.3

17.4

17.5

17.6

17.7

17.8

17.9

17.10

17.11

17

- 14.9 Startvorgang von Windows 10
- 14.10 Boot-Optionen, Aktivieren von
 - Windows RE
- 14.11 Backup und Restore, Notfallwiederherstellung
- 14.12 Systemleistungsoptionen und Auslagerungsdatei

Treiber und Hardware-Installation

Allgemeine Tastenkombinationen

JBSYSTEM.NE

3

PCNEWS-169

Anwendungsprogramme (Apps)

Windows 10-Sicherheitseinstellungen

Konfigurieren von Benachrichtigungen

14.13 Ereignisanzeige (Event Viewer) Leistungsüberwachung 14.14

Debugging Blue Screens

BitLocker Drive Encryption

Bedienung der Tastatur

Tastatur- und Maustasten bei Desktop-

Microsoft Internet Explorer

Microsoft Management Console:

Microsoft Management Console:

Problembehandlung

Windows-Sicherheit

und Meldungen

AppLocker

Elementen

Dialogfelder

Eingabehilfen

Zeichentabelle

Hauptfenster

Konsolenfenster

17.12 Remotedesktop-Verbindungen

Windows Explorer

Windows Update

Wichtige Tasten

9 Benutzerverwaltung

Christian Zahler

9.1 Ablauf des Anmeldevorgangs in Windows

Wenn Windows gestartet wird, so ist der erste Systemprozess, der im Benutzermo- • Er dus gestartet wird, der Sitzungs-Manager %SystemRoot%\System32**smss.exe**. Er führt eine Reihe von Initialisierungsvorgängen aus und startet dann schließlich zwei Sitzungen:

- Sitzung 0: eine nicht interaktive Sitzung; zesse, die keine Interaktion mit Benutzern haben.
- Sitzung 1: eine interaktive Sitzung (in dieser Sitzung arbeitet der erste angemeldete Benutzer)

Wenn sich weitere Benutzer anmelden (etwa über Remote Desktop), dann werden für jeden Benutzer weitere Sitzungen (Sitzung 2, 3, ...) erzeugt.

Außerdem startet der Sitzungs-Manager für die nicht interaktive Sitzung den Prozess WinInit, für die interaktive Sitzung den Prozess WinLogon (im Task-Manager als Windows-Anmeldeanwendung bezeichnet) Anschließend wird der smss.exe-Prozess beendet.

Windows-Anmeldeanwendung

WinLogon führt eine Reihe von Initialisierungvorgängen in der Sitzung 1 durch, unter anderem:

- Er erstellt eine Windows-Station mit dem Namen WinSta0. Eine Windows-Station repräsentierte eine "Sicherheitsgrenze" und kann mehrere Desksowie eine Zwischenablage tops (clipboard) enthalten. In Benutzersitzungen gibt es nur diese eine Windows- • Wenn die Authentifizierung erfolgreich Station.
- In dieser Windows-Station werden mehrere Desktops erzeugt, wobei die ersten beiden wesentlich sind:
 - WinLogon-Desktop: Diese Darstellung ist auch als "Sicherheitsbildschirm" bekannt. Hier findet man die Menüpunkte Sperren, Abmelden, Kennwort ändern und Task-M
- Default-Desktop: In dieser Oberfläche arbeitet der Windows-Benutzer; auch die Taskleiste gehört zu diesem Bildschirm.
- Disconnect-Desktop: Dieser Desktop wird angezeigt, während ein Bildschirmschoner aktiv ist. Beim Neustart von Windows wird dieser Bildschirm als Standard gesetzt.
- ° Secure Desktop: Diese Oberfläche

Control-Abfragen durchgeführt werden.

- startet den Dienststeuerungs-Manager services.exe.
- Er startet die lokale Sicherheitsinstanz lsass.exe (Local Security Authority, LSA), die für die Überprüfung der Benutzeranmeldung (Authentifizierung) zuständig ist.
- in dieser Sitzung laufen viele Systempro- Wenn am WinLogon-Desktop die der Secure Attention Sequence (SAS) Strg + Alt + Del oder - in Windows 8/8.1/10 auch eine beliebige andere Taste – gedrückt wird, so startet Win-Logon den Prozess LogonUI; dieser Prozess hat die Aufgabe, Anmeldeinformationen von den Benutzern zu bekom- Der Grund für die Verwendung einer SAS nannten tern (Credential Provider, CP) zusammen. Der Standard-CP von Windows unterstützt Kennwörter und Smartcards; Windows 10 enthält aber auch einen alternativen Anmeldeinformationskeiten wie Fingerabdruck oder Ge- Prozess dafür. sichtserkennung unterstützt. Wenn LogonUI die Anmeldeinformationen beand Authentication DLL; diese wird seit gespeichert: Windows Vista nicht mehr unterstützt.) Die installierten Credential Provider sind der Registry aufgelistet: in

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wind ows\CurrentVersion\Authentication\Credenti al Providers

ist, so erstellt WinLogon die Anfangsprozesse der Benutzersitzung. Einer der wichtigsten User-Prozesse ist Init.exe: Dieser Prozess arbeitet Anmeldescripts ab, stellt die Netzwerkverbindung (wieder) her und startet die Shell – standardmäßig **explorer.exe**. Anschließend wird der Prozess User-Init.exe beendet.

Der Prozess WinInit führt ähnliche Vorgänge wie WinLogon in der Sitzung O durch, allerdings ohne Benutzeranmeldung. Die Windows-Stationen in der Sitzung 0 haben einen Namen wie zum Beispiel service-0x0-3e7\$, wobei die Nummer auch anders sein kann.

Hauptaufgabe des WinLogon-Eine Prozesses ist die Erkennung der Secure Attention Sequence (SAS) Strg + Alt + Del.

wird angezeigt, wenn User Account Immer wenn diese Tastenkombination gedrückt wird, wechselt WinLogon zum WinLogon-Desktop. Dadurch sieht es für den Anwender so aus, als würden "alle geöffneten Fenster und die Taskleiste verschwinden".



men. LogonUI arbeitet mit den soge- besteht darin, Benutzer vor Programmen Anmeldeinformationsanbie- zu schützen, die den Anmeldeprozess simulieren und auf diese Weise Kennwörter abfangen können – Anwendungen, die im Benutzermodus laufen, können die SAS-Tastenfolge nicht abgreifen.

anbieter mit dem Namen Windows Hel- Immer, wenn eine Benutzeranmeldung lo, der biometrische Anmeldemöglich- erfolgen soll, so startet der WinLogon-

9.1.1 Arbeitsgruppenbetrieb

kommen hat, übergibt es diese Informa- In einer Arbeitsgruppe (Workgroup) sind tion an die LSA und wird beendet. die Sicherheitsinformationen (also Benut-(Anmerkung: Ältere Windows-Systeme zername und Kennwort) in einer lokalen verwendeten statt der CPs die soge- Datenbank (Fachausdruck: SAM, Security nannte GINA = Graphical Identification Account Manager) auf jedem Rechner



Sie können sich hier nur lokal anmelden. Es reicht, den jeweiligen Benutzernamen als Anmeldenamen zu verwenden.

Beachten Sie:

- Pro PC sind nur maximal 20 gleichzeitige Zugriffe über das Netzwerk erlaubt. (Diese Einstellung soll verhindern, dass Windows 10 als "preisgünstiger Datei-Server" verwendet wird.)
- Hinweis[.] In früheren Windows-Versionen war die Anzahl der Zugriffe auf 10 beschränkt.
- Eine Arbeitsgruppe ohne Server-PC eignet sich für maximal 3 bis 5 PCs.

9.1.2 Active Directory-Domänenbetrieb

In einer Domäne existiert zusätzlich zu den lokalen Sicherheitsdatenbanken eine zentrale, leistungsfähige Sicherheitsdaten- • bank (Fachausdruck: Active Directory, AD) auf einem speziellen Server-PC, der als Domänencontroller (DC) bezeichnet wird.



Sie haben also nun zwei Möglichkeiten, um sich an Ihrem Computer anzumelden:

- Nach wie vor eine lokale Anmeldung an Ihrem PC. Damit können Sie nur lokal arbeiten. Ein Zugriff auf benötigte Dateien und Programme im Netzwerk ist nicht möglich.
- Eine Anmeldung an der Domäne: Hier überprüft der Domänencontroller, ob Sie Ihren Namen und Ihr Kennwort korrekt eingegeben haben. Erst dadurch bekommen Sie Zugang zu benötigten Informationen ("Ressourcen") in Ihrem Netzwerk.

Grundsätzlich wird im Anmeldedialog immer der zuletzt angemeldete Benutzer angezeigt. Wenn Sie sich mit einem anderen Benutzerkonto anmelden möchten, so klicken Sie auf Anderer Benutzer:



Wenn Ihr PC Mitglied einer Domäne ist, so müssen Sie bei der Anmeldung entscheiden, ob Sie eine lokale Anmeldung oder • Microsoft-Konten: Diese Konten sind eine Domänenanmeldung durchführen wollen:

• Lokale Anmeldung: Geben Sie Ihren Benutzernamen in der Form NetBIOS-Computername\Benutzername ein, zum Beispiel:



Eine lokale Anmeldung bewirkt, dass Sie auf Ressourcen in der Domäne nicht Vordefinierte Konten: zugreifen können!

zwei Möglichkeiten.

Die folgende Abbildung zeigt die herkömmliche (zu Windows NT 4.0 und Windows 9x kompatible) Anmeldung an einer Domäne mit der Schreibweise

NetBIOS-Domänenname\Benutzername

contoso\administrator	
•••••	$\circ \rightarrow$
Anmelden an: cor	itoso
Wie melden Sie sich an ei Domäne an?	iner anderen

Alternative: Sie können auch den sogenannten UPN-Namen ("User Principal Name") zur Anmeldung verwenden. Dieser sieht ähnlich aus wie eine E- Viele Personen haben bereits ein Micro-Mail-Adresse:

administrator@contoso.at		
•••••	0	\rightarrow
Anmelden an: contoso.at		

Hinweis: Die Anmeldung mit einem Windows-Domänenkonto ist auch übers Web möglich. Je nach verwendeter Betriebssystem- und Browser-Version kann es sein, dass zwei oder drei Zeilen im Anmeldefenster angezeigt werden. Bei zweizeiligem Dialog muss die Schreibweise • XBox-Konto NetBIOS-Domänenname\Benutzername gewählt werden.

9.2 Arten von Benutzerkonten

Die Anmeldedaten der Benutzer sind standardmäßig in Sicherheitsdatenbanken gespeichert.

- Microsoft-Konten und werden standardmäßig sowohl für die lokale Anmeldung am Windows 10-Gerät als auch für den Zugriff auf Cloud-Dienste wie etwa OneDrive benötigt. Microsoft plant, dass ein Installationsvorgang von Windows 10 nur möglich ist, wenn ein Microsoft-Konto vorhanden ist.
- Lokale Benutzerkonten: liegen auf dem lokalen PC in der SAM-Datenbank (SAM = Security Account Manager).
- Domänen-Benutzerkonten: liegen im Active Directory und sind in der Domäne und allen vertrauten Domänen verfügbar
- AzureAD-Benutzerkonten (Office 365-Konten): Microsoft stellt allen Office 365-Kunden ein eigenes Cloud-Active Directory zur Verfügung, in welchem Benutzerinformationen gespeichert und

verwaltet werden können.

Domänenanmeldung: Hier bestehen • Administrator: kann nicht gelöscht werden, aber umbenannt

• Gast

9.2.1 Microsoft-Konto

Mit einem Microsoft-Konto können Sie sich an diverse Microsoft-Websites und -Dienste wie Onedrive, Skype, Outlook und Xbox live anmelden, und zwar an alle mit denselben Anmeldedaten. Diesen Singlesign-on-Dienst bietet Microsoft schon länger an, in der Vergangenheit aber unter anderen Namen. Er hieß im Laufe der Jahre bereits unter anderem Microsoft Passport, .NET Passport und zuletzt Windows Live ID. Seit Windows 8 heißt der Dienst nun Microsoft-Konto.

Das Microsoft-Konto wird auch zum Herunterladen von Apps aus dem Microsoft Store benötigt.

soft-Konto, ohne dass es ihnen bewusst ist:

- Ehemaliges Hotmail-Postfach: Die damals verwendete E-Mail-Adresse (endet mit @hotmail.com) ist ein Microsoft-Konto.
- Skype-Konto: Meldet man sich mit einer E-Mail-Adresse an Skype an, so ist diese ein Microsoft-Konto.
- Ehemaliges Windows Live-Konto (Messenger, Outlook Express): Die E-Mail-Adressen dieser Konten sind Microsoft-Konten.
- Auch Office 365-Konten können als Anmeldekonten verwendet werden. Genaueres dazu im nächsten Abschnitt.

Wenn Sie noch kein Microsoft-Konto haben, so können Sie auf der folgenden Seite eines erstellen:

https://account.microsoft.com

Ein Konto für alles, was mit Microsoft zu tun hat

Ein Konto. Ein Ort, um alles zu verwalten. Willkommen bei Ihrem Konto-Dashboard.

Anmelden > Erstellen Sie ein Microsoft-Konto >

Sie können dabei Ihre gewohnte E-Mail-Adresse eintragen und diese als Microsoft-Kontonamen verwenden.

Microsoft

Konto erstellen

iemand@example.com

Neue E-Mail-Adresse anfordern

Stattdessen eine Telefonnummer verw



9.2.2 Microsoft Azure AD-Konto (Office 365-Konto)

Für alle, die Office 365 nutzen, stellt Microsoft einen cloud-basierenden Active Directory-Dienst mit dem Namen **Azure AD** zur Verfügung. In diesem sind alle Benutzerkonten einer Organisation bzw. Bildungseinrichtung gespeichert.

In den Einstellungen klicken Sie auf Konten.



Konten

Konten, E-Mail, Arbeit, andere Kontakte, Synchronisierung

Klicken Sie dann auf den Menüpunkt Auf Arbeits- oder Schulkonto zugreifen.

ē	Auf Arbeits- oder Schulkonto zugreifen
Auf A	Arbeits- oder Schulkonto zugreifen
Gerät vom	a Arbeitgeber oder der Bildungseinrichtung gesteuert werden,
beispielsw	weise, welche Einstellungen Sie ändern können. Erkundigen Sie
sich nach s	spezifischen Informationen.



AzureAD-Konten kann man auch mit der Command Shell-Anweisung **whoami** identifizieren:

C:\>whoami

C:\>azuread\heinrichadam

9.2.3 Lokales Benutzerkonto

Es ist nach wie vor möglich, auch ein lokales Benutzerkonto zu erstellen, obwohl diese Möglichkeit nicht mehr empfohlen wird.

Im Assistent für neue Benutzerkonten müssen Sie den Link anklicken Ich kenne die Anmeldeinformationen dieser Person nicht:

Microsoft

Wie meldet sich diese Person an?



Sie kommen dann zu einem Formular, mit dem Sie ein neues **lokales Benutzerkonto** erstellen können. Legen Sie einen Benutzernamen fest, vergeben Sie ein Anmeldekennwort und beantworten Sie drei Sicherheitsfragen (falls das Anmeldekennwort vergessen wird, kann es nach richtiger Beantwortung dieser Fragen zurückgesetzt werden).

Konto für	diesen PC	erstellen			
Wenn Sie ein K eicht zu merke	ennwort verwend n, aber von ander	len möchten, da ren schwer zu er	nn wählen : raten ist,	Sie ein Kennv	wort aus, das
Von wern wird	dieser PC genutz	rt?			

Cennwor	erneut eingeben
---------	-----------------



Das neue lokale Konto wird nun angezeigt:



9.3 Anmeldeoptionen und Windows Hello

Grundsätzlich werden die Anmeldeoptionen von den installierten Anmeldeinformationsanbietern (Credential Provider, CP) bestimmt. Es ist daher möglich, dass auf unterschiedlichen Geräten unterschiedliche Anmeldeoptionen zur Verfügung stehen.

Windows Hello ist ein neuer Anmeldeinformationsanbieter (Credential Provider), der seit Windows 10 verfügbar ist. Er unterstützt zusätzlich die Anmeldung mit PIN -Codes sowie bestimmte biometrische Verfahren wie Gesichtserkennung oder Fingerabdruckerkennung.

In den Windows-Einstellungen im Bereich Konten gibt es einen Menüeintrag Anmeldeoptionen.

Anmeldeoptionen

Vorgehensweise für die Anmeldung an Ihrem Gerät verwalten

Wählen Sie eine Anmeldeoption aus, um sie hinzuzufügen, zu ändern oder zu entfernen.

- Windows Hello-Gesichtserkennung Mit Kamera anmelden (empfohlen)
- Windows Hello-Fingerabdruckerkennung Diese Option ist zurzeit nicht verfügbar. Klicken Sie hier, um weitere Informationen zu erhalten.
- Windows Hello-PIN Mit PIN anmelden (empfohlen)
- Sicherheitsschlüssel Mit physischem Sicherheitsschlüssel anmelden
- Kennwort Mit Ihrem Kontokennwort anmelden
 - Bildcode
- Wischen und tippen Sie auf ihr Lieblingsfoto, um Ihr Gerät zu entsperren



Konten, E-Mail, Arbeit, andere Kontakte, Synchronisierung

Die verfügbaren Optionen können sich von Gerät zu Gerät unterscheiden.

Steht eine Option nicht zur Verfügung, so wird die Meldung "Diese Option ist zurzeit nicht verfügbar." angezeigt (in der Grafik rechts sieht man beispielsweise, dass das Gerät keine Fingerabdruckerkennung unterstützt.)

9.3.1 Windows Hello-PIN einrichten

Sinn: Der PIN ist nur Anmeldung an dem PC gültig, an welchem er erstellt wurde (Unterschied zum Kennwort!).

Rufen Sie in den Windows-Einstellungen den Bereich Konten und dort den Menüeintrag Anmeldeoptionen auf.

PIN	
Hinzufügen	

Es ist möglich, für einen angemeldeten Benutzer die Anmeldung mittels PIN zu aktivieren. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**.

Window	Windows-Sicherheit >					
Bestätigen Sie zunächst das Kennwort Ihres Kontos.						
R	PC08\Kevin					
	•••••					
	ОК	Abbrechen				
	_					
Windo	Windows-Sicherheit $ imes$					
PIN	PIN einrichten					
Erstell wird. I Dienst	Erstellen Sie eine PIN, die anstelle von Kennwörtern verwendet wird. Eine PIN erleichtert die Anmeldung bei Geräten. Apps und Diensten.					
	•••••]			
_	••••••					
Buchstaben und Symbole einschließen						
	ОК	Abbrechen				

An derselben Stelle ist es nun auch möglich, die PIN zu ändern, zu entfernen und gegebenenfalls eine vergessene PIN zurückzusetzen.





PIN vergessen

Ändern

Ab diesem Zeitpunkt werden auf dem Anmeldebildschirm die verfügbaren Anmeldeoptionen dargestellt, in diesem Fall Kennwort (Schlüssel-Symbol) und PIN (Tastatur-Symbol).



Kevin



Hinweis: Aus Sicherheitsgründen ist eine Remote Desktop-Anmeldung mit PIN nicht möglich!

9.3.2 Windows Hello-Gesichtserkennung

Die Windows Hello-Gesichtserkennung ist natürlich nur verfügbar, wenn das Gerät über eine entsprechende Kamera verfügt.

Willkommen bei Windows Hello Ihr Gerät ist jetzt für Sie personalisiert, und die Eingabe komplexer Kennwörter gehört der Vergangenheit an. Verwenden Sie jetzt die Gesichtserkennung, um Ihr Gerät zu entsperren Ihre Identität nachzuweisen und im Store einzukaufen.

Klicken Sie auf Los geht's. Die Kamera wird aktiviert, Sie sehen sich einige Sekunden lang selbst. Anschließend müssen Sie eine Windows Hello-PIN einrichten, damit eine Anmeldung auch bei defekter Kamera bzw. veränderten Gesichtskonturen (Bart, Brille, andere Frisur etc.) möglich bleibt.

Windows Hello-Setup	×
Noch ein paar Dinge	
Erstellen Sie eine PIN für den Fall, dass die Gesichtserkennung nicht verfügbar ist. Vermutlich werden Sie die PIN nie benötigen. Sie dient nur zur Sicherheit.	
Sobald Sie Ihre PIN eingerichtet haben, können Sie sich per Gesichtserkennung anmelden.	
Tipp: Wenn Sie beim Einrichten der Gesichtserkennung eine Brille trugen, wählen Sie "Erkennung verbessern" aus, um die Einrichtung erneut und ohne Brille durchzuführen. So können wir: Sie mit und ohne Brille erkennen.	
Erkennung verbessern	

Klicken Sie auf PIN einrichten, um die PIN zu konfigurieren.

9.3.3 Windows Hello-Fingerabdruckerkennung

Voraussetzung dafür ist ein funktionsfähiger Fingerabdruck-Scanner, wie er auf vielen Tablets oder Notebooks zur Verfügung steht.

9.3.4 Anmeldung mit Bildcode einrichten

Die Anmeldung mit Bildcode wurde für Tablets bzw. Notebooks mit Touchscreen entwickelt. Die Anmeldung erfolgt hier durch Wiederholung einer Abfolge von Touchbewegungen, die auf einer bestimmten Position eines angezeigten Fotos ablaufen müssen.

Bildcode

Melden Sie sich mit einem Lieblingsfoto bei Windows an.

Hinzufügen

Der Bildcode ist eine neue Methode zum Schutz Ihres Touchscreen-PCs. Dabei wählen Sie ein Bild aus und erstellen Gesten dazu, um ein ganz persönliches Passwort zu kreieren.

Nachdem Sie ein Bild ausgewählt haben, "zeichnen" Sie direkt auf dem Touchscreen eine Kombination von Kreisen, geraden Linien und Tippbewegungen. Die Größe, Position und Richtung der Gesten wird Teil Ihres Bildcodes.

Bild auswählen

9.3.5 Anmeldung mit Sicherheitsschlüssel (Token)

Ein Sicherheitsschlüssel ist ein Hardwaregerät, das Sie anstelle Ihres Benutzernamens und Kennworts verwenden können, um sich im Web anzumelden. Da er zusätzlich zu einem Fingerabdruck oder einer PIN verwendet wird, können Sie sich nicht ohne die von Ihnen erstellte PIN oder den Fingerabdruck anmelden, selbst wenn jemand Ihren Sicherheitsschlüssel besitzt. Sicherheitsschlüssel können in der Regel von Händlern erworben werden, die PC-Zubehör verkaufen.

9.3.6 Dynamische Sperre

Ihrem PC gekoppelt sind, um zu erkennen, ob Sie Ihren Arbeitsplatz verlassen haben, <u>http://www.microsoft.com/technet/</u> und Ihren PC sperren, kurz nachdem Ihr sysinternals/utilities/psgetsid.mspx). gekoppeltes Gerät außerhalb der Bluetooth-Reichweite ist. Dies verhindert, dass Personen Ihr Gerät verwenden können, wmic useraccount where name="Benutzername" get sid wenn Sie sich von Ihrem PC entfernen und whoami /user vergessen, ihn zu sperren.

🗛 Dynamische Sperre

Windows kann gesperrt werden, wenn sich Geräte, die mit Ihrem PC gekoppelt sind, nicht mehr in Reichweite befinden.

Zulassen, dass Windows Ihr Gerät in Ihrer Abwesenheit automatisch sperrt

Bluetooth- und andere Geräte

9.4 Security Principals

Unter diesem Begriff werden Objekte zusammengefasst, denen Berechtigungen zugewiesen werden können.

Zu den wichtigsten Security Principals zählen:

- Benutzerkonten
- Computerkonten
- Gruppenkonten
- Dienste

Benutzer-, Computer- und Gruppenkonten Auswahl wichtiger Spezialidentitäten: werden nicht über ihren Namen, sondern über einen internen Primärschlüssel, den sogenannten Security Identifier (SID),

verwaltet. Alle Berechtigungen für Benutzer-, Computer- und Gruppenkonten werden intern mit dieser SID gespeichert.

Aufbau einer SID:

- Alle SIDs beginnen mit dem Buchstaben S, der die Zeichenkette als SID identifiziert.
- Nach dem ersten Bindestrich folgt die Revisionsnummer - diese ist bei allen bisher verwendeten SIDs immer 1.
- Danach kommt die Kennung der Identifier Authority. So bedeutet der Wert 5 "NT Authority".

S-1-5-21-1812011286-570857186-3424489074 - 1004 Domänen-SID RID (relative ID)

- Domänen-SID: Im Fall von lokalen Benutzerkonten spezifiziert diese Nummer den PC, bei Domänen-Benutzerkonten die Domäne. Alle lokalen Benutzerkonten auf demselben PC haben dieselbe Domänen-SID; alle AD-Benutzer derselben Domäne haben ebenfalls dieselbe Domänen-SID
- ID (Relative ID): Diese oft vierstellige Nummer ist spezifisch für jedes Benutzer-, Computer- oder Gruppenkonto. Dabei hat das vordefinierte Administrator-Konto immer die RID 500. So hätte das Administrator-Konto des obigen PCs folgende SID:

S-1-5-21-1812011286-570857186-3424489074-500

SIDs können beispielsweise mit dem Tool Windows kann Geräte verwenden, die mit PsGetSID angezeigt werden (Download unter

Andere Möglichkeiten:

Well-Known SIDs (auch: Integrierte Sicherheitsprinzipale)

Einige Security Principals haben SIDs, die nicht wie oben beschrieben aufgebaut sind. Es handelt sich dabei um Spezialidentitäten, die vom System her vorgesehen sind und sich in vielen Fällen ähnlich wie Gruppenkonten verhalten. Die wichtigste Gemeinsamkeit dieser speziellen Objekte ist die immer gleiche SID – egal auf welchem PC oder in welcher Domäne. Die Mitgliedschaft wird vom Betriebssystem gesteuert und kann nicht geändert werden.

Eine Liste von Spezialidentitäten findet man im Internet unter:

https://docs.microsoft.com/de-de/ windows/security/identity-protection/ access-control/security-identifiers

UBSYSTEM

TrustedInstaller-Dienst: Neu seit Windows Vista ist die Möglichkeit, auch bestimmten Diensten SIDs und damit NTFS-Berechtigungen zuzuweisen. In Windows Vista ist der TrustedInstaller-Dienst Besitzer der meisten Betriebssystem-Dateien; daher hat auch nur dieser Dienst Vollzugriff auf diese Dateien. Das soll Prozesse, die im Administrator- oder Local System-Kontext ausgeführt werden, hindern, Betriebssystemdateien auszutauschen, zu löschen oder zu ändern.

Wenn Betriebssystemdateien gelöscht werden müssen, so muss zunächst der Besitz übernommen werden, dann ein Berechtigungseintrag neu erstellt werden, der die Löschberechtigungen erteilt.

9.5 Kontotyp: Lokale Benutzer zu lokalen Administratoren machen

Lokale Benutzer können entweder Standardbenutzer oder lokale Administratoren sein. Standardbenutzer haben Zugriff auf installierte Anwendungssoftware haben und dürfen bestimmte Systemeinstellungen konfigurieren (Bildschirmhintergrund, Auflösung etc.). Während Standardbenutzer nicht die Berechtigung haben, Software zu installieren oder die Netzwerkeinstellungen zu ändern, haben Administratoren den lokalen Vollzugriff auf das gesamte System.

9.5.1 Vorgangsweise im Arbeitsgruppenbetrieb

Navigieren Sie in der Systemsteuerung in den Bereich Benutzerkonten und klicken Sie auf Kontotyp ändern.



Wählen Sie den Benutzer aus, dessen Kontotyp Sie ändern möchten.

\$	R Heinrich Adam AzureAD'HeinrichAdam Kennwortgeschützt	8	Kevin Lokales Konto Kennwortgeschützt
Neuen	Kontotyp für Kevin auswähle Kevin	n	
	Lokales Konto Kennwortgeschützt		
Stand Autom	ardbenutzer können den Großteil der S rkungen auf andere Benutzer oder die	oftware verwenden Sicherheit des PCs I	und Systemeinstellungen ändern, die k haben.
O Admir Admir alle Di	nistrator nistratoren haben vollständige Kontroll steien und Apps zugreifen, die auf den	le über den PC. Sie i NPC gespeichert sin	können alle Einstellungen ändern und a id.
1.	t ein Standardkonto emofoblen?		

9.5.2 Vorgangsweise im Domänenbetrieb

Eige

Allo

Im Domänenbetrieb sind die Einstellungen auch in der Systemsteuerung im Bereich Benutzerkonten zu verwalten, die Oberfläche sieht aber etwas anders aus.

Benutzerkonten Panderen Benutzern Zugriff auf diesen Computer geben | Skontotyp ändern

Sie können wieder auf Kontotyp ändern klicken; allerdings wird dann ein Dialogfeld mit zwei Registerkarten angezeigt.

Sie können bestehende Einträge bearbeiten, indem Sie auf Eigenschaften klicken.

SID	Name	Beschreibung
S-1-1-0	Everyone (Jeder)	Gruppe, die alle Benutzer einschließlich der anonymen Benutzer und Gäste enthält. Die Mitgliedschaft wird vom Betriebssystem gesteuert. Hinweis: Seit Windows XP Service Pack 2 (SP2) sind anonyme Benutzer standardmäßig nicht mehr Mitglied der Gruppe "Everyone".
S-1-3-0	Creator Owner (Ersteller- Besitzer)	Platzhalter in einem vererbbaren ACE-Eintrag. Wenn der ACE-Eintrag geerbt wird, ersetzt das System diesen SID durch den SID des Objekterstellers.
S-1-3-1	Creator Group (Erstellergruppe)	Platzhalter in einem vererbbaren ACE-Eintrag. Wenn der ACE-Eintrag geerbt wird, ersetzt das System diesen SID durch den SID der primären Gruppe des Users. der das Obiekt erzeugt hat.
S-1-3-4	Owner Rights	Diese SID gibt es ab Windows Vista und wird verwendet, um die Rechte des Objektbesitzers zu kontrollieren. Sie unterscheidet sich von der Ersteller-Besitzer -SID.
S-1-5-1	Dialup (DFÜ)	Gruppe, die alle Benutzer enthält, die sich über eine DFÜ-Verbindung angemel- det haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-2	Network (Netzwerk)	Gruppe, die alle Benutzer enthält, die sich über eine Netzwerkverbindung ange- meldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-3	Batch (Batch)	Gruppe, die alle Benutzer enthält, die sich über eine Batch- Warteschlangeneinrichtung angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-4	Interactive (Interaktiv)	Gruppe, die alle Benutzer enthält, die sich interaktiv angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-6	Service (Dienst)	Gruppe, die alle Sicherheitsprinzipale enthält, die sich als Dienst angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-7	Anonymous (Anonym)	Gruppe, die alle Benutzer enthält, die sich anonym angemeldet haben. Die Mit- gliedschaft wird vom Betriebssystem gesteuert.
S-1-5-9	Enterprise Do- main Controllers (Domänencontrol er der Organisati- on)	Gruppe, die alle Domänencontroller in einer Gesamtstruktur enthält, die einen Verzeichnisdienst des Active Directory verwenden. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-10	Principal Seli (Selbstprinzipal)	Platzhalter in einem vererbbaren ACE-Eintrag für ein Konto- oder Gruppenobjekt im Active Directory. Wenn der ACE-Eintrag geerbt wird, ersetzt das System die- sen SID durch den SID des Sicherheitsprinzipals, dem das Konto gehört.
S-1-5-11	Authenticated Users (Authentifizierte Benutzer)	Gruppe, die alle Benutzer enthält, deren Identitäten bei der Anmeldung authen- tifiziert wurden. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-13	Terminal Server Users (Terminalserverb enutzer)	Gruppe, die alle Benutzer enthält, die sich bei einem Terminaldiensteserver angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-18	Local System (Lokales System)	Dienstkonto, das vom Betriebssystem genutzt wird.
S-1-5-19	NT Authority (NT- Autorität)	Lokaler Dienst
S-1-5-20	NT-Autorität	Netzwerkdienst
S-1-5-32- 544	Administratoren	Vordefinierte Gruppe. Nach der Erstinstallation des Betriebssystems ist das Administratorkonto einziges Mitglied der Gruppe. Wenn ein Computer einer Domäne beitritt, wird die Gruppe "Domänen-Admins" der Administratorengrup- pe hinzugefügt. Wenn ein Server zum Domänencontroller wird, wird die Gruppe "Organisations-Admins" ebenfalls zur Administratorengruppe hinzugefügt.
S-1-5-32- 545	Benutzer	Vordefinierte Gruppe. Nach der Erstinstallation des Betriebssystems ist die Gruppe der authentifizierten Benutzer einziges Mitglied dieser Gruppe. Wenn ein Computer einer Domäne beitritt, wird die Gruppe der Domänenbenutzer zur Benutzergruppe auf dem Computer hinzugefügt.
S-1-5-32- 546	Gäste	Vordefinierte Gruppe. Standardmäßig ist das Gastkonto einziges Mitglied dieser Gruppe. Die Gästegruppe ermöglicht es Gelegenheitsbenutzern oder einmaligen Benutzern, sich mit eingeschränkten Berechtigungen über das vordefinierte Gastkonto auf einem Computer anzumelden

		Benutzer Erweitert		
genschaften von pc04\zahler	×	Verwenden S auf den Com	ie die unten stehende List puter zu gestatten bzw. z	te, um Benutzern den Zugriff u verweigern und um
Allgemein Gruppenmitgliedschaft		Benutzer dieses Comp	oder andere Einstellunger uters:	i zu ändern.
Welche Zugriffsstufe soll diesem Benutzer zugewiesen werden?		Benutzername	Domäne	Gruppe
Standardbenutzer (Benutzergruppe)		😪 zəhler	ZAHLER	Administratoren
Standardkontobenutzer können den Großteil der Software verwen Systemeinstellungen ändern, soweit dies keine Auswirkungen auf Benutzer hat.	den und die andere	Szahler	pc04	Administratoren
<u>Administrator</u> (Administratorgruppe)				
Administratoren haben Vollzugriff auf den Computer und können Änderungen vornehmen. Basierend auf den Benachrichtigungsein werden Administratoren möglicherweise zum Eingeben ihres Ken zum Bestätigen der auszuführenden Aktion aufgefordert, bevor si vornehmen, die Auswirkungen auf andere Benutzer haben.	i beliebige nstellungen nworts und e Änderungen	-Kennwort für zahler	Hinzufügen	Entfernen Eigenschaften
○ Agdere: Administratoren ∨		Klicken Sie "zahler" zu	auf "Kennwort zurücksel andern.	tzen", um das Kennwort für

Benutzerkonter

OK Abbrechen Ub

8

In der Registerkarte Gruppenmitgliedschaft kann ein Benutzerkonto entweder zur Standardbenutzer-Gruppe oder zur lokalen Adminstratoren-Gruppe hinzugefügt werden. Zusätzlich gibt es noch den Eintrag **Andere**, mit der sich weitere Berechtigungsstufen realisieren lassen.

In der Registerkarte **Benutzer** können auch die lokalen Benutzer-Kennwörter zurückgesetzt werden, dafür steht die Schaltfläche **Kennwort zurücksetzen...** zur Verfügung.

9.6 Kennwörter an Webseiten und eigene Anmeldeinformationen verwalten

Im Systemsteuerungsbereich **Anmeldeinformationsverwaltung** können Sie auch die Zuordnungen zu Webanmeldeinformationen einsehen, hinzufügen und ändern.

Anmeldeinformationsverwaltung

Klickt man auf Webanmeldeinformation, so erhält man eine Liste aller zwischengespeicherten Konto/Passwort-Kombinationen für Webseiten, die eine Anmeldung erfordern:

Das Kennwort wird standardmäßig zwar nicht angezeigt, lässt sich aber durch Klick auf den Link **Einblenden** anzeigen. Die Anmeldeinformation kann durch Klicken auf Entfernen **gelöscht** werden.

In ähnlicher Form sind Windows-Anmeldeinformationen einsehbar.

9.7 Benutzerverwaltung lokaler Benutzer in der Computerverwaltung

Dies wird mit der App **Computerverwaltung** (eigentlich ein vordefiniertes MMC-Snap-In) erledigt:



Navigieren Sie innerhalb der Rubrik System zum Bereich Lokale Benutzer und Gruppen.

Um einen neuen lokalen Benutzer anzulegen, klicken Sie mit der rechten Maustaste in einen freien Bereich und wählen den Kontextmenüeintrag **Neuer Benutzer...**:

Name		Vollständiger Name	Beschreibung
🛃 Adminis	strator		Vordefiniertes Konto für die Verwa
🛃 Default/	Acco		Ein vom System verwaltetes Benu
🛃 Gast			Vordefiniertes Konto für Gastzugri
🛃 Kevin			
🛃 WDAGU	Itility		Ein Benutzerkonto, das vom Syste
	A L	leuer Benutzer ktualisieren iste exportieren	

Legen Sie einen Benutzernamen und ein Kennwort für die erstmalige Anmeldung fest.

Vermeiden Sie Sonderzeichen für den Benutzernamen.

Eigene Anmeldeinformationen verwalten

Sie können gespeicherte Anmeldeinformationen für Websites, verbundene Anwendungen und Netzwerke anzeigen und löschen.



g

MELISIASEII

dung ändern aktivieren; es ist nicht för- Benutzerkonten. derlich und entspricht auch nicht der gängigen Security-Praxis, wenn der Systemadministrator die Kennwörter aller Benutzer weiß!

Das neue Konto wird nun in der Benutzerliste angezeigt.

Vollständiger Name

- 🕵 Administrator
- 🛃 DefaultAcco...
- 🛃 Gast

Name

- 💻 Jessica Jessica
- 🜉 Kevin Kevin

🛃 WDAGUtility...

9.8 UAC (Benutzerkontosteuerung, User Account Control)

Die Benutzerkontosteuerung ermöglicht eine Abwägung zwischen der Flexibilität und dem Berechtigungsumfang eines Administratorkontos und der Sicherheit eines Standardbenutzerkontos.

Wenn Sie eine administrative Aufgabe ausführen möchten, wie z. B. die Installation eines neuen Programms, fordert sind "elevated privileges" notwendig. Die UAC "dimmt" den Bildschirm und fordert Sie zur Bestätigung auf, dass Sie das Programm installieren möchten, bevor Sie diese administrativen Aufgaben ausführen können. Auf diese Weise wird die Verwendung von Administratorberechtigungen minimiert, wodurch es für bösartige Software (Malware) wie Viren, Würmer, Spyware und andere potenziell unerwünschte Programme schwieriger wird, den PC weitreichend zu befallen.

Benutzerkontensteuerung Möchten Sie zulassen, G Änderungen en Usram	dass durch diese App	×		
werden?	Gerat vorgenommen			
	olSettings			
Verifizierter Herausgeber: Microsoft Windows				
Weitere Details anzeigen				
Ja	Nein			
Benutzerkontensteuerung		\times		
Möchten Sie zulassen, Änderungen an Ihrem werden?	dass durch diese App Gerät vorgenommen			
Java SE Runtime Er	nvironment			
Verifizierter Herausgeber: Oracle America, Inc. Dateiursprung: Aus dem Internet heruntergeladen				
Weitere Details anzeigen				
Weitere Details anzeigen				

In Windows 10 kann das Verhalten der befinden sich drei dafür vorgesehene Ein-Benutzerkontosteuerung fein abgestimmt träge vom Typ REG_DWORD: werden. Öffnen Sie dazu die Systemsteue-

muss Kennwort bei der nächsten Anmel- rung und navigieren Sie in den Bereich

Änderungen am eigenen Konto durchführen

Anderungen am eigenen Konto in den PC-Einstellunger vornehmen

💎 Einstellungen der Benutzerkontensteuerung ändern 😌 Benutzerkonten verwalten

Es gibt vier Sicherheitsebenen:

- Immer benachrichtigen
- Standard nur benachrichtigen, wenn Änderungen an meinem Computer von Programmen (nicht vom User selbst) vorgenommen werden
- nur benachrichtigen, wenn Änderungen an meinem Computer von Programmen (nicht vom User selbst) vorgenommen werden sowie Desktop nicht abblenden ("dimmen")
- Nie benachrichtigen

Benachrichtigungen über Änderungen am Computer auswählen Mithilfe der Benutzerkontensteuerung kann verhindert werden, dass potenziell schädlic Anderungen an Ihrem Computer vornehmen. Weitzer Informationer zu den Einstellungen für die Benutzerkontensteuerung en für die Benutzerkontensteuerung

-	Nur benachrichtigen, wenn von Apps Änderungen am Computer vorgenommen werden (Standard).
	 Nicht benachrichtigen, wenn ich Änderungen an den Windows-Einstellungen vornehme.
	Empfohlen, wenn Sie bekannte Apps verwenden und bekannte Websites besuchen.

Der Benutzerkontoschutz dient auch dem Schutz der Computer von Familienmitgliedern vor Malware. Malware ist häufig in Programmen versteckt, die für Kinder reizvoll sind. Um Ihren Computer abzusichern, Sicherheitseinstellungen / Lokale Richtlikönnen Sie für Ihre Kinder Standardbenut- nien / Sicherheitsoptionen. zerkonten erstellen. Wenn Ihr Kind versucht, eine Softwarekomponente zu installieren, fordert das System die Eingabe des Kennworts eines Administratorkontos an. Dadurch können Ihre Kinder neue Programme nicht selbständig installieren.

Technischer Hintergrund

In Windows 10 werden zwei Sicherheitstoken für ein Administratorkonto erzeugt. Die Verwendung des Administratorkontos muss autorisiert werden.

9.8.1 Konfigurieren der UAC über die Registry

Über die Registry kann das Standardverhalten der UAC für Administratoren und für Standardbenutzer konfiguriert werden.

Im Schlüssel

HKEY LOCAL MACHINE\Software\Micros oft\Windows\CurrentVersion\Policies\Sy stem

ConsentPromptBehaviorAdmin

(Standardwert 5)

- ConsentPromptBehaviorUser (Standardwert 3)
- EnableLUA (Standardwert 1)

PnPSysprep *	Name	Тур	Daten
a 🕌 Policies	ab (Standard)	REG_SZ	(Wert nicht fest
Attachm	ConsentPromptBehaviorAdmin	REG_DWORD	0x00000000 (0)
NonEnu	22 ConsentPromptBehaviorUser	REG_DWORD	0x0000003 (3)
Den joution	20 dontdisplaylastusername	REG_DWORD	0x00000000 (0)
ProfileNotify	200 EnableInstallerDetection	REG_DWORD	0x00000001 (1)
PropertySur	EnableLUA	REG_DWORD	0x00000000 (0)
Reliability	22 EnableSecureUIAPaths	REG_DWORD	0x00000001 (1)

Die beiden ConsentPromptBehavior-Einträge können folgende Werte annehmen:

- **O**Keine Aufforderungen mehr seitens der Benutzerkontensteuerung - alle Programme werden mit höheren Rechten ausgeführt
- 5 "Lockerste" Einstellung
- 2 "Strengste" Einstellung

Der Wert EnableLUA muss auf 0 gesetzt werden, um die UAC auszuschalten.

Achtung:

Aus Sicherheitsgründen sollte davon abgesehen werden, die Benutzerkontensteuerung auf dem Weg der Registry zu beeinflussen.

9.8.2 Konfigurieren der UAC über lokale Gruppenrichtlinien

Das Verhalten der UAC kann mit Hilfe von Gruppenrichtlinien gesteuert werden. Diese Richtlinien können sowohl lokal als auch in der Domäne konfiguriert werden.

Man findet die Richtlinien in Computerkonfiguration / Windows-Einstellungen /

Rohtlinen für Lokaler Computer	ficteline	Schehelseindellung	
ComputationReportion ComputationReport Construction Construction Status Construction Status Construction Status Construction Construction	Industriant Annual Manifesting and Annual Annu	Note definitet Aktivet Aktivet Aktivet Aktivet Sektivet Sektivet Sektivet Sektivet Sektivet Sektivet Sektivet	

9.9 Programmausführung mit geändertem Benutzerkontext

Die dauerhafte Anmeldung mit einem Benutzerkonto, das administrative Berechtigungen ausweist, wird nicht empfohlen.

Stattdessen sollten auch Personen, die mit administrativen Tätigkeiten betraut sind, die "Normalanmeldung" mit einem Standard-Benutzerkonto ohne erweiterte Berechtigungen durchführen.

Um ein Programmfenster mit geändertem Benutzerkontext zu erstellen, gibt es folgende Möglichkeiten:

(a) Über die grafische Oberfläche:

Klicken Sie mit der rechten Maustaste auf das Programm, das Sie mit administrativen Berechtigungen ausführen möchten,

den Eintrag Als Administrator ausführen.

Sie werden dann nach Anmeldeinformationen für ein Konto mit administrativen dass das Benutzerprofil des Administra-Berechtigungen gefragt.

G Als Administrator ausführen
Dateispeicherort öffnen
-⇔ An "Start" anheften
-⇔ An Taskleiste anheften

Die bisher vorhandene Möglichkeit, ein Programm im Kontext eines nichtadministrativen Benutzers auszuführen, steht in Windows 10 standardmäßig nicht dungen sowie weitere festgelegte Einstelzur Verfügung.

Durch Änderung eines Registry-Eintrags lässt sich dieses Verhalten jedoch ändern: Navigieren Sie zu folgendem Schlüssel (sollte der Schlüssel Explorer nicht existieren, so legen Sie ihn an):

\HKEY_LOCAL_MACHINE\SOFTWARE\Polici • Die Datei NTUSER.DAT stellt einen Teil es\Microsoft\Windows\Explorer

Erstellen Sie einen neuen DWORD-Wert (32-Bit) mit dem Namen ShowRunAsDifferentUserInStart und belegen Sie ihn mit dem Wert 1.



Starten Sie anschließend den Windows-Explorer neu (über den Task-Manager beenden, dann neuen Task mit explorer.exe erzeugen).

Auswirkung: Im Kontextmenü des Startmenüs ist nun ein neuer Eintrag Als anderer Benutzer ausführen zu sehen.

Computerverwaltung App	
Web durchsuchen	G Als Administrator ausführen
0 coompu - Webernehnisse an	Als anderer Benutzer ausführen
Coumpa mesergeomise an	Dateispeicherort öffnen
✓ computer bild	-🛱 An "Start" anheften
	-🛱 An Taskleiste anheften

(b) Über die Command Shell

Mit dem Befehl runas kann ein Programm teikarte mit einem beliebigen Benutzerkontext gestartet werden:

C:\>runas /noprofile / user:Administrator@zahler.at explorer.exe

Nach der Kennworteingabe für das Administratorkonto wird das angegebene Programm mit administrativen Berechtigungen gestartet; gibt man ein nichtadministratives Konto an, so gelten die

und wählen Sie aus dem Kontextmenü Berechtigungen dieses Kontos, und zwar nur für dieses eine Programmfenster.

> Der Parameter /noprofile bewirkt, tors nicht geladen wird; dies hat den Vorteil, dass das gewünschte Programm schneller geladen wird; unter Umständen kann die Anwendung dann aber nicht funktionieren. (Gegenteil: Parameter / profile)

9.10 Benutzerprofile

In Benutzerprofilen sind benutzerdefinierte Desktopumgebungen definiert. Dazu gehören individuelle Einstellungen für die Anzeige, Netzwerk- und Druckerverbinlungen. Ihre Desktopumgebung kann vom Benutzer selbst oder vom Systemadministrator eingerichtet werden. Technisch gesehen handelt es sich bei Benutzerprofilen um Unterordner von C:\Benutzer, wobei folgende Komponenten das Profil bilden:

- der Registry dar und enthält benutzerdefinierte Systemeinstellungen.
- Eine Reihe von Ordnern enthalten benutzerdefinierte Dateien; bekannt sind etwa die Ordner "Dokumente" oder "Desktop".

Das Profil "Default" stellt eine Vorlage dar, die beim erstmaligen Anmelden eines Benutzers kopiert wird und den Ausgangsstatus für das neue Benutzerprofil bildet.

nicht mehr; es stellt nur mehr einen Sys- ner eine Verbindung zeigt, kann der Comtem-Link zum Verzeichnis C:\ProgramData mand-Shell-Befehl dir /a verwendet werdar. Dieses Verzeichnis enthält die Startmenüdateien für "alle Benutzer" in folgendem Pfad:

C:\ProgramData\Microsoft\Window s\Start Menu\Programs

Einträge, die mit einem Verknüpfungssymbol gekennzeichnet sind (kleiner schwarzer, nach rechts oben weisender Pfeil

🜁), stellen keine echten Ordner dar, sondern sind eine sogenannte Verbindung (engl. Junction) zu einem anderen Ordner. Auf solche Verknüpfungen kann in den Beachten Sie die Kennzeichnung des "All meisten Fällen nicht direkt zugegriffen Users"-Profils als System-Link! werden.

Hinweis: Junctions werden nur sichtbar. wenn in den Ordneroptionen in der Kar-"Ansicht" die Einstellung "Geschützte Systemdateien ausblenden" deaktiviert wird.

Beispiel: Ein Klick auf den Verweis Disk Cookies führt zur Meldung:

X	Auf Cr\Users\zahler.ZAHLER.000\Cookies kann nicht zugegriffen wer	den.
-	Zugnff verweigert	



Das Profil "All Users" gibt es eigentlich Um nun herauszufinden, auf welchen Ordden:

c:\Users>dir /a Volume in Laufwerk C: hat keine Bezeichnung. Volumeseriennummer: E073-F6A8

Verzeichnis von c:\Users

04.04.2020	08:04	<dir></dir>		
04.04.2020	08:04	<dir></dir>		
30.08.2019	07:31	<dir></dir>		administrator
30.08.2019	07:30	<dir></dir>		alexander
19.03.2019	07:02	<symlinkd></symlinkd>		All Users [C:\ProgramData]
30.08.2019	07:35	<dir></dir>		Default
19.03.2019	07:02	<junction></junction>		Default User [C:\Users\Default]
19.03.2019	06:49		174	desktop.ini
30.08.2019	08:25	<dir></dir>		Public
04.04.2020	08:04	<dir></dir>		raphaela
26.03.2020	09:06	<dir></dir>		zahler.ZAHLER
	1 Dat	ei(en),		174 Bytes
	11 Ver	zeichnis(se), 20	5.581.475.328 Bytes frei

C:\Users\C	hristian>	dir /a	
Volume in	Laufwerk	C: hat keine Be	zeichnung.
Volumeseri	ennummer:	7448-CE17	
Verzeichni	s von C:\	Users\Christian	I.
11.06.2009	09:16	<dir></dir>	
11.06.2009	09:16	<dir></dir>	
26.05.2009	11:04	<verbindung></verbindung>	Anwendungsdaten
[C:\Users\C	hristian\	AppData\Roaming]
26.05.2009	11:04	<dir></dir>	AppData
26.05.2009	11:05	<dir></dir>	Contacts
26.05.2009	11:04	<verbindung></verbindung>	Cookies
[C:\Users\C	hristian\	AppData\Roaming	1
Microsoft\W	indows\Cc	okies]	
12.06.2009	16:58	<dir></dir>	Desktop
12.06.2009	16:55	<dir></dir>	Documents
26.05.2009	11:49	<dir></dir>	Downloads
26.05.2009	11:04	<verbindung></verbindung>	Druckumgebung
[C:\Users\C	hristian\	AppData\Ro	
aming\Micro	soft\Wind	lows∖Printer Sho	rtcuts]
26.05.2009	11:04	<verbindung></verbindung>	Eigene Dateien

Hier sehen Sie, dass es sich beim Ordner Cookies um eine Verbindung (Junction) auf den tatsächlich existierenden Ordner

C:\Users\Christian\AppData\Roam ing\Microsoft\Windows\Cookies handelt. In diesen Ordner können Sie im Explorer ohne Berechtigungsprobleme hineinschauen.

Einige wichtige Elemente im Benutzerprofil:

- Ordner "Desktop": Dieser Ordner enthält Dateien, die am Desktop gespeichert sind.
- "Documents", Ordner "Pictures", "Music", "Videos": Diese Ordner enthalten Dateien des beschriebenen Typs.
- Ordner "Download": Dieser Ordner ist ein Standardspeicherort für aus dem Internet heruntergeladene Dateien.
- Ordner "Favoriten": Dieser Ordner enthält Verknüpfungen zu bevorzugten Websites, Dateien und Verzeichnissen.
- Ordner "AppData": Dieser Ordner enthält verschiedene Anwendungsdaten, sortiert nach Position und Verwendung.
 - 🔺 🕌 AppData
 - 🖻 퉲 Local
 - LocalLow
 - 🖻 鷆 Roaming
 - Der Ordner "Local" enthält lokal 0 gespeicherte Informationen.
 - Der Ordner "LocalLow" Ο
 - Der Ordner "Roaming" enthält die 0 servergespeicherten Anteile des Profils.
- Ordner "AppData\Local\Microsoft": In diesem Ordner sind unter anderem auch die lokalen Mail-Datenbanken gespeichert, die alle eingegangenen und gesendeten E-Mails, alle Kontakte und auch die Terminpläne enthalten, die in Outlook bzw. Windows Mail (Nachfolger von Outlook Express) gespeichert sind.

*.pst-Dateien: Lokale Datenbank für

Outlook-Elemente; wird generell eine lokale Postfachdatei verwendet, so hat diese den Namen outlook.pst



*.ost-Dateien: Offline-Cache; heruntergeladene, zwischengespeicherte E-Mails und andere **Outlook-Elemente** office@zah

Windows Mail – Ordner

"AppData\Local\Microsoft\Windows Mail": Von Windows Mail wird eine komplette Ordnerstruktur erzeugt. Die Nachrichten landen im Windows.MSMessageStore, werden aber innerhalb der einzelnen Mailordner (etwa "Inbox") noch einmal als *.eml (E-Mail-Datei) angezeigt.

🚳 edb.chk	10.11.2007 12:02	Wiederhergestellt				
edb.log	Textdokument					
edb00001.log	10.11.2007 12:01	Textdokument				
edbres00001.jrs	10.11.2007 12:01	JRS-Datei				
edbres00002.jrs	10.11.2007 12:01	JRS-Datei				
WindowsWail.pat	10.11.2007 12:02	NSWESSAGESTUK				
windowsiviali.pat	10.11.2007 12:01	PAT-Date				
📕 Windows Mai	I		•			
Backup						
a 🃗 Local Folder	rs					
퉬 Deleted Ite	ems		•			
퉬 Drafts			•			
퉬 Inbox						
퉬 Junk E-ma	ail					
퉬 Outbox						

Windows Mail-E-Mail-Nachricht

• Ordner "AppData\Local\Temp": enthält temporäre Dateien, die von Anwendungsprogrammen oder Diensten während der Laufzeit erzeugt werden (beispielsweise bei der Installation neuer Software). Er sollte immer leer sein.

Sent Items

a) 10B16CC4-00000001.eml 10.11.2007 12:02

Ordner

"AppData\Local\Microsoft\Windows\I NetCache": stellt den Webcache des Internet Explorers dar. In ihm werden alle besuchten Websites und dazu nötige Cookies zwischengespeichert. Auch dieser Ordner sollte regelmäßig gelöscht werden. Das Löschen dieses Ordners ist auch im Internet Explorer über das Menü Einstellungen - Internetoptionen, Karteikarte Allgemein möglich:



- In folgendem Dialogfeld können temporäre Dateien, die während des Surfens gespeichert wurden, gelöscht werden: (siehe Bild unten rechtes)
- Unter Cookies versteht man kleine Textdateien, die beim Anwählen bestimmter Internetsites lokal gespeichert werden und zum Datenaustausch zwischen Client und Server dienen. In Cookies können persönliche Vorlieben, Datum und Zeit des letzten Besuchs oder Benutzernamen und Kennwörter gespeichert werden.

cookie:zahler@csl-computer.eu/	Cookie:zahler@csl-computer.eu/
cookie:zahler@dainese.com/	Cookie:zahler@dainese.com/
cookie:zahler@de.wikipedia.org/	Cookie:zahler@de.wikipedia.org/

Ordner

"AppData\Local\Microsoft\Windows\H istory" (Verlauf): Hier speichert der Internet Explorer Links zu besuchten Websites.

Ordner

"AppData\Roaming\Microsoft\Windo ws\Start Menu" (Startmenü): Dieser Ordner enthält Verknüpfungen zu Programmen, die im Startmenü – zusammengefasst in Gruppen - angezeigt werden.

Ordner

"AppData\Roaming\Microsoft\Windo ws\Recent" (Zuletzt verwendete Dokumente): Dieser Ordner enthält Verknüpfungen zu Dokumenten und Ordnern,

×

Browserverlauf löschen

Bevorzugte Websitedaten beibehalten

Cookies und temporäre Internetdateien behalten, damit die Einstellungen für die bevorzugten Websites gespeichert und diese schneller angezeigt werden.

<u>Temporäre Internet- und Websitedateien</u>

Kopien von Webseiten, Bildern und Mediendateien, die zur schnelleren Anzeige gespeichert werden.

Cookies und Websitedaten

Dateien oder Datenbanken, die auf dem Computer durch Websites gespeichert wurden, um Einstellungen zu speichern oder die Websiteleistung zu verbessern.

🗸 Verlauf

Liste der Websites, die Sie besucht haben.

Downloadverlauf Liste der heruntergeladenen Dateien.

Formulardaten

Gespeicherte Informationen, die Sie in Formulare eingegeben haben.

Kennwörter

Gespeicherte Kennwörter, die automatisch eingegeben werden, wenn Sie sich bei einer bereits besuchten Website anmelden.

Daten des Tracking-Schutzes, der ActiveX-Filterung und "Do Not Track"-Daten Liste mit Websites, die von der Filterung ausgeschlossen sind, Daten, an denen der Tracking-Schutz erkennt, welche Websites möglicherweise automatisch Details über einen Besuch freigeben, und Ausnahmen für "Do Not Track"-Anforderungen.

Info zum Löschen des Browserverlaufs

Löschen

Abbrechen



ler.at.ost

die in der letzten Zeit vom Benutzer Kopieren von Benutzerprofilen: Benutzer-Stelle im Startmenü angezeigt.

Typen von Benutzerprofilen

- Lokales Benutzerprofil: Das lokale Benutzerprofil wird beim ersten Anmelden bei einem Computer erstellt und auf der lokalen Festplatte des betreffenden Computers gespeichert. Sämtliche Änderungen an Ihrem lokalen Benutzerprofil sind nur für den Computer wirksam, auf dem die Änderungen vorgenommen wurden.
- Servergespeichertes Benutzerprofil (Roamingprofil): Das servergespeicherte Benutzerprofil wird vom Systemadministrator erstellt und auf einem Server gespeichert. Dieses Profil steht immer zur Verfügung, wenn Sie sich an einem Computer im Netzwerk anmelden. An Ihrem servergespeicherten Benutzerprofil vorgenommene Änderungen werden auf dem Server aktualisiert. Voraussetzung ist die Verwendung einer Active Directory-Domäne.
- Verbindliches Benutzerprofil: Das verbindliche Benutzerprofil ist ebenfalls ein servergespeichertes Profil, mit dessen Hilfe bestimmte Einstellungen für einzelne Benutzer oder einer Benutzergruppe festgelegt werden können. Änderungen an den verbindlichen Benutzerprofilen können lediglich von den Systemadministratoren vorgenommen werden. Verbindliche Benutzerprofile erhält man, indem die Datei NTU-SER.DAT in NTUSER.MAN (für "mandatory") umbenannt wird. Diese Technologie sollte heute nicht mehr verwendet werden; sie wurde durch Gruppenrichtlinienobjekte ersetzt.
- Super-Verbindliches Benutzerprofil: Wenn der Name des Profilordners selbst mit der Erweiterung .MAN versehen wird, so erhält man ein "Supermandatory Profile". Ein solches Profil verhält sich wie ein "normales" verbindliches Benutzerprofil, mit dem Unterschied, dass sich Benutzer mit einem solchen Profil nicht anmelden können, wenn der Server unerreichbar ist, auf dem das super-verbindliche Profil gespeichert ist.
- Temporäres Benutzerprofil: Ein temporäres Profil wird in jeder Situation ausgegeben, in der durch eine Fehlerbedingung das Laden des Benutzerprofils verhindert wird. Temporäre Profile werden am Ende einer Sitzung gelöscht. Änderungen, die der Benutzer an den Desktopeinstellungen und Dateien vorgenommen hat, gehen beim Abmelden des Benutzers verloren. Hinweis: Der Benutzer "Gast" erhält stets ein temporäres Benutzerprofil!

verwendet wurden. Diese Verknüpfun- profile können dupliziert und lokal gegen werden an der entsprechenden löscht werden; dafür steht das Dialogfeld "Systemeigenschaften" zur Verfügung



(erreichbar über das Kontextmenü des Arbeitsplatzes oder über Systemsteuerung System):

Mit der Schaltfläche **Typ ändern** kann ein servergespeichertes Profil in ein lokales geändert werden (nicht umgekehrt!).

Profiltyp ändern				X
Soll das Roamingprofil oder vom Betriebssystem verwer CONTOSO\heinz.gruber am	die lokal det werde Compute ngprofil Profil	gespeicher en, wenn si er anmelde Abbree	te Kopie d ch t?	es Profils
		Abbre	inen	
Benutzerprofile				×
Auf diesem Computer, den Sie ver können aber auch ein Computer, den Sie ver Auf diesem Computer gespeiche	n Benutzerk wenden, eir Roamingpr wenden, gle erte <u>P</u> rofile:	onto. Sie kö n anderes Pr ofil wählen, eich ist.	nnen auf jed ofil ersteller das auf jede	dem I. Sie em
Name	Größe	Тур	Status	Geä
CONTOSO\administrator	1,33 MB	Lokal	Lokal	09.0
CONTOSO\heinz.gruber	62,2 MB	Roaming	Roaming	28.0
IIS APPPOOL\DefaultAppPool	2,57 MB	Lokal	Lokal	07.0
Konto unbekannt	1,07 GB	Lokal	Lokal	07.0
PC08\Jessica	63,3 MB	Lokal	Lokal	05.0
PC08\Kevin	78,3 MB	Lokal	Lokal	09.0
Standardprofil	1,51 MB	Lokal	Lokal	28.0
<u>T</u> yp ändern		<u>L</u> öschen	Kopie	eren nach
Öffnen Sie die Systemsteuerung Benutzerkonten zu erstellen.	soption <u>Ber</u>	nutzerkonter	<u>ı</u> , um	
		ОК	Ab	brechen

9.11 Öffentliche Ordner

Im Benutzerprofilordner C:\Benutzer gibt es neben den privaten Profilordnern, auf die nur die jeweiligen Benutzer Zugriff haben, auch ein Benutzerprofil Öffentlich.

Die in diesem Profil enthaltenen Daten stehen allen Benutzern zur Verfügung, die lokal auf diesem PC arbeiten.

Alle Benutzer, die sich an diesem Computer anmelden, haben Zugriff auf die Dateien in den öffentlichen Ordnern.

Die öffentlichen Ordner werden standardmäßig nicht angezeigt, sie müssen erst im Netzwerk- und Freigabecenter durch Klicken auf den Link Erweiterte Freigabeeinstellungen ändern aktiviert werden.

👯 Netzwerk- und Freigabecenter



Adaptereinstellungen ändern

Erweiterte
Freigabeeinstellungen ändern
Medienstreamingoptionen

In den erweiterten Freigabeeinstellungen kann man die Freigabe des öffentlichen Ordners auf Benutzer mit Netzwerkzugriff erweitern. In diesem Fall kann jeder Benutzer mit Netzwerkzugriff in den öffentlichen Ordnern lesen und schreiben.

Alle Netzwerke

Freigabe des öffentlichen Ordners

Wenn "Freigabe des öffentlichen Ordners" aktiviert ist, können die Personen im Netzwerk (einschließlich der Heimnetzgruppen-Mitglieder) auf die Dateien in den Ordnern "Öffentlich" zuareifen.

- Freigabe einschalten, sodass jeder Benutzer mit Netzwerkzugriff in Dateien in den Ordnern "Öffentlich" lesen und schreiben kann
- Freigabe des öffentlichen Ordners" deaktivieren (an diesem Computer angemeldete Benutzer können weiterhin auf diese Ordner zugreifen)

10 Rechte und Berechtigungen

Christian Zahler

Man unterscheidet zwischen:

- Rechten (engl. rights): Darunter versteht man die Möglichkeit, dass ein Benutzer eine Systemaktion durchführen darf. Beispiel: Ändern der Uhrzeiteinstellungen. Viele dieser Einstellungen werden über Gruppenrichtlinien festgelegt.
- Berechtigungen (engl. permissions): Darunter versteht man Objektzugriffsberechtigungen, also die Möglichkeit, auf Dateien, Drucker und Laufwerke zugreifen zu dürfen. Solche Einstellungen werden in Form von NTFS-Zugriffskontrolleinträgen festgelegt.

10.1 Lokale Gruppen

Lokale Gruppen werden für den Zugriff auf lokale Ressourcen verwendet. Einer lokale Gruppe können lokale Benutzer, Domänenbenutzer oder auch Benutzer einer fremden Domäne zugeordnet werden. Zweite Verwendung: PC, der zu keiner Domäne gehört, administrieren.

Wieder gibt es vordefinierte Gruppen.

- Administratoren
- Benutzer
- Gäste
- · Hauptbenutzer: hat in Windows 10 eigentlich keine Bedeutung mehr, in früheren Windows-Versionen für Benutzern mit eingeschränkten administrativen Rechten verwendet.

Lokale Gruppen können nur folgende Security Principals zugeordnet sein:

- Lokale Benutzerkonten
- Lokal verfügbare integrierte Sicherheitsprinzipale (Jeder, Authentifizierte Benutzer. ...)
- Globale bzw. Universelle Gruppen im Active Directory (Voraussetzung: Computer ist Domänenmitglied)

Lokale Gruppen können daher keine anderen benutzerdefinierten Lokalen Gruppen enthalten.

Anlegen von lokalen Gruppen

Öffnen Sie das MMC-Snap-In Computerverwaltung. Navigieren Sie in der linken Zum Auswählen von Benutzerkonten, die Spalte zum Punkt System – Lokale Benut- Mitglieder der lokalen Gruppe werden zer und Gruppen – Lokale Gruppen.

Klicken Sie mit der rechten Maustaste in den freien Bereich und wählen Sie im Kontextmenü Neue Gruppe.



Liste exportieren...

Legen Sie den Namen der lokalen Gruppe fest.

Tipp: Zur Unterscheidung der Gruppentypen ist es sinnvoll, eine **lokale** Gruppe mit einem Erkennungsbuchstaben zu kennzeichnen. Diese Vorgangsweise macht sich dann bezahlt, wenn verschachtelte Berechtigungsstrukturen erstellt werden müssen. (Genaueres dazu in der Arbeitsunterlage: Windows Server 2016/2019 Grundlagen und Domänenbetrieb!) Eine Möglichkeit ist, lokale Gruppen mit dem Großbuchstaben L beginnen zu lassen.

-				
Neue Gruppe			?	\times
Gruppenname:	LGrafik Design			
Beschreibung:				
<u>Mitglieder:</u>				
💭 Jessica 🧶 Kevin				
Hi <u>n</u> zufügen	Entfernen			
<u>H</u> ilfe		Ers <u>t</u> ellen	<u>S</u> chlie	eßen

sollen, klicken Sie auf Hinzufügen.

Objekttypen... Suchpfad PC08 Erweitert. ОК Abbrechen

Benutzer auswählen				×
Objekttyp:				
Benutzer oder Integrier	te Sicherheitsprinzipale	•	Qbjek	ttypen
Suchpfad:				
PC08			<u>Pf</u>	ade
Allgemeine Abfragen				
Name: Begi	nnt mit 👘 🖂			Spa <u>t</u> ten
Beschreibung: Begi	nnt mit 🔍			Jetzt suchen
Deaktivierte Kont	en			Beenden
Nicht-ablaufende	Kenn <u>w</u> örter			_
T <u>ag</u> e seit der letzten	Anmeldung:	\sim		÷
Suchergebnisse:			OK	Abbrechen
Name	Ordner			^
LUSR .				
Jeder				
Jessica	PC08			
KONSOLENANME	1000			
Lokaler Dienst				
Konto				
Lokales Konto und				
Netzwerk				
A INCLEWEI KOIEITSL				~

Wählen Sie alle Benutzerkonten aus, die Mitglied bei der lokalen Gruppe werden sollen, und klicken Sie dann auf OK. Die neu hinzugefügten Mitglieder werden nun angezeigt:

4	
C	\mathbf{v}

Neue Gruppe			?	×
<u>G</u> ruppenname:	LGrafik Design			
Beschreibung:				
<u>M</u> itglieder:				
鯚 Jessica 鯚 Kevin				
Hinzufügen	Entfemen			
<u>H</u> ilfe		Ers <u>t</u> ellen	<u>S</u> chliel	ßen

Klicken Sie auf Erstellen, um die lokale Gruppe zu erzeugen.

🌆 LGrafikDesign

10.2 NTFS-Berechtigungen

NTFS-Berechtigungen regeln den Zugriff auf Dateien und Ordner.

10.2.1 Anzeigen und Bearbeiten von **NTFS-Berechtigungen**

Die NTFS-Sicherheitseinstellungen findet man für jeden Ordner, jede Datei, jedes Laufwerk und jeden Drucker im Kontextmenü Eigenschaften, Karteikarte Sicherheit.

Die angeführte Liste von Berechtigungen wird als (Discretionary Access Control List) bezeichnet; die einzelnen Einträge heißen ("verweigern") setzen! ACE (Access Control Entry).

Die angeführten Berechtigungen werden nicht nach dem Benutzer- oder Gruppennamen gespeichert, sondern mit der eindeutigen Objekt-SID (Security Identifier).

Berechtigungen kann man in Grundkategorien einteilen:

Voneinander unabhängig sind

- Lesen
- Schreiben

Voneinander abhängig sind:

Х Erweiterte Sicherheitseinstellungen für "Daten' \times 📕 Eigenschaften von Daten Allgemein Freigabe Sicherheit Vorgängerversionen Anpassen Name C:\Daten HeinrichAdam (AzureAD\HeinrichAdam) 🛛 🗣 Ändern Besitzer: Objektname: C:\Daten Berechtigungen Freigabe Überwachung Effektiver Zugriff Gruppen- oder Benutzernamen 21 ichAdam (AzureAD\HeinrichAda Doppelklicken Sie auf einen Berechtigungseintrag, um zusätzliche Informationen zu erhalten. Wählen Sie zum Ändern eines Berechtigungseintrags den Eintrag aus, und klicken Sie auf "Bearbeiten" (soweit vorhanden). SYSTEM Kevin (PC08\Kevin) Berechtigungseinträge: Administratoren (PC08\Administratoren) Тур Prinzipal Zugriff Geerbt vor Anwenden auf Klicken Sie auf "Bearbeiten", um die Bearbeiten.. 🧸 Zulas... HeinrichAdam (AzureAD\Hei... Vollzuariff Keine Diesen Ordner Unterordner un. Berechtigungen zu ändem. Be<u>r</u>echtigungen für "HeinrichAdam Vollzugriff Zulas... Kevin (PC08\Kevin) Keine Diesen Ordner, Unterordner un... Zulas... Administratoren (PC08\Admi... Vollzugriff Keine Diesen Ordner, Unterordner un... Zulassen Verweigem Zulas... SYSTEM Vollzugriff Diesen Ordner, Unterordner un... Keine Vollzuariff Ändem Lesen, Ausführen Ordnerinhalt anzeigen Lesen Hinzufügen Entfernen Anzeigen Schreiben Klicken Sie auf "Erweitert", um spezielle Vererbung aktivieren Erweitert Berechtigungen anzuzeiger 🗌 Alle Berechtigungseinträge für untergeordnete Objekte durch vererbbare Berechtigungseinträge von diesem Objekt ersetzen Abbrechen Übernehmen OK ОК Abbrechen Ü<u>b</u>ernehmen

- Lesen und Ausführen: beinhaltet die Beispiel: Auf die Datei Projektdoku.xlsx Lese-Berechtigung
- Ändern = Lesen + Ausführen + Schreiben
- Vollzugriff = alles (inkl. Besitzrechte Administratoren: Vollzugriff übernehmen, Berechtigungen ändern)

(Bild links unten)

Berechtigungen können an Unterordner und die darin befindlichen Dateien vererbt werden; diese Vererbung geschieht standardmäßig automatisch.

In der DACL sieht man, welche Berechtigungen vom übergeordneten Verzeichnis ererbt worden sind:

übergeordneten Verzeichnis ererbt

✓ Diese Berechtigungen wurden im aktuellen Verzeichnis gesetzt

Weiters unterscheidet man positive Berechtigungen (Zulassen) und negative Berechtigungen (Verweigern).

Die Berechtigungsvergabe erfolgt kumulativ, d.h. ererbte Berechtigungen und neu vergebene Berechtigungen sammeln sich an.

NTFS- Man kann nicht eine ererbte positive Be-**DACL** rechtigung entziehen ("wegklicken"), aber man kann negative Berechtigungen

Wichtig:

Verweigerungsberechtigungen haben Vorrang vor positiven Berechtigungen.

Ausnahme: Explizit gesetzte positive Berechtigungen haben Vorrang vor ererbten negativen Berechtigungen.

Wenn in einer ACL kein Eintrag für einen Benutzer steht, dann wird im Zweifelsfall negativ entschieden.

haben folgende Gruppen Zugriffsberechtigungen:

- Sicherungsoperatoren: Berechtigung "Lesen verweigern"

Herr Meier gehört zu beiden Gruppen. Darf er auf diese Datei lesend zugreifen?

Antwort: Nein, weil die Verweigerungsberechtigung Vorrang hat!

Hinweis: Es kann auch vorkommen, dass in der Registerkarte Sicherheit von Dateien und Ordnern statt den Benutzer- oder Gruppenkontonamen die (normalerweise Diese Berechtigungen wurden vom unsichtbaren) SIDs angezeigt werden.

Eigenschaften von nur für zahler	<u>?</u> ×
Allgemein Webfreigabe Freigabe	Sicherheitseinstellungen
Name	<u>H</u> inzufügen
 ♣ S-1-5-21-796845957-920026266 ♣ S-1-5-21-796845957-920026266 	-839522115-1000 -839522115-500

Mögliche Ursachen dafür:

- Das ursprüngliche Benutzerkonto wurde in der Datenbank gelöscht, die Berechtigungen aber noch nicht
- Domain Controller ist momentan nicht erreichbar, der Kontoname kann daher nicht aufgelöst werden
- Infrastrukturmaster in der Domäne arbeitet nicht oder ist nicht erreichbar (möglicherweise auf Grund von DNS-Problemen)

Keinesfalls sollten solche in der Karteikarte "Sicherheitseinstellungen" auftauchenden SIDs einfach gelöscht werden. Das könnte zu Zugriffsproblemen führen.

10.2.2 Vererbung deaktivieren; explizite **NTFS-Berechtigungen festlegen**

Man kann allerdings diese Vererbung blockieren und die Berechtigungen neu festlegen. Dazu klickt man auf die Schaltfläche

HUBSYSTEM.NE





10.2.5 Regeln für das Verhalten von Berechtigungen beim Kopieren und Verschieben von Dateien und Ordnern

Für das Verständnis von Berechtigungen ist es wichtig zu wissen, was beim Kopieren und Verschieben von Ordnern und Dateien geschieht.

Verschieben: Wenn ein Ordner auf demselben NTFS-Laufwerk verschoben wird, werden die Berechtigungen "mitgenommen".

Wenn ein Ordner in ein anderes NTFS-Laufwerk verschoben wird, werden die Berechtigungen nicht mitgenommen! Ein Verschiebevorgang lässt sich als Abfolge eines Kopiervorgangs mit anschließendem Löschen des Originals erklären.

Kopieren: Beim Kopieren werden die Berechtigungen nicht mitübernommen! (Kopieren = Neuerstellen + Lesen im alten Ordner) Man erhält als vererbte Berechtigungen nur die im Zielordner

Problem:

Wenn man alle NTFS-Berechtigungen entzieht, kann niemand mehr (auch der Ad- • Halten Sie Ihre Berechtigungsstruktur ministrator nicht) Änderungen durchführen!

Abhilfe: Der Administrator und die Gruppe der Sicherungsoperatoren haben das Recht, bestehende Zugriffsrechte zu ignorieren (dies wird aber mitprotokolliert!) dies geschieht durch die Übernahme des Besitzes an diesem Ordner/dieser Datei.

Mit der Berechtigung "Ordner durchsuchen" kann man den Ordner nicht öffnen, aber eine Verknüpfung zu einer im Ordner befindlichen Datei erstellen und auf diese Datei zugreifen. Mit der Berechtigung "Ordner auflisten" kann der Ordnerinhalt angezeigt werden:

sprechen (ähnlich wie bei Linux) den Berechtigungen für Dateien

Vollzugriff	1
Ordner durchsuchen / Datei ausführen	1
Ordner auflisten / Daten lesen	1
Attribute lesen	1
Erweiterte Attribute lesen	1
Dateien erstellen / Daten schreiben	1
Ordner erstellen / Daten anhängen	1
Attribute schreiben	1
Erweiterte Attribute schreiben	1
Unterordner und Dateien löschen	1
Löschen	1
Berechtigungen lesen	~
Berechtigungen ändern	~
Besitz übernehmen	1

Also: Attribute werden für Dateien anders angezeigt werden. interpretiert als für Ordner!

10.2.6 Tipps und Strategien

Es ist günstig, Dateien mit gleichen Sicherheitsanforderungen im selben Ordner zu NTFS- speichern!

> Für die Berechtigungsvergabe gibt es zwei stark unterschiedliche Strategien:

- Ich entziehe den Benutzern nur die Berechtigungen, die dem System Schaden zufügen können - sehr liberale Strategie.
- Ich gebe den Benutzern nur die Berechtigungen, die sie unbedingt benötigen sehr strenge Strategie.

Grundsätzlich sollten Sie folgende Regeln beachten:

- Vergeben Sie NTFS-Berechtigungen nicht an einzelne Benutzer, sondern an lokale Gruppen. Weisen Sie Benutzer mit denselben Anforderungen einer Gruppe zu. (Das Gesamtkonzept für Active Directory-Domänen wird im Skriptum "Windows Server 2016/2019 -Grundlagen und Domänenbetrieb" ausführlich beschrieben.)
- Vermeiden Sie es, Verweigerungsberechtigungen zu setzen.
- möglichst einfach.

Im Wurzelverzeichnis C:\ hat jeder Benutzer Lesezugriff. In einer neuen NTFS-Partition hat ebenfalls standardmäßig jeder Benutzer Lesezugriff.

Allerdings werden die Berechtigungen nicht an die Verzeichnisse %SystemRoot% (zum Beispiel C:\Windows) oder % ProgramFiles% (zum Beispiel C:\Programme) weitervererbt (d.h. die Vererbungskette ist standardmäßig unterbrochen).

10.3 Zugriffstoken und Sicherheitsdeskriptoren

In Windows hat jeder Prozess ein soge-Beispiel: Berechtigungen für Ordner ent- nanntes Zugriffstoken (access token). Dieses Zugriffstoken beinhaltet die SID, die Gruppenzugehörigkeiten und sogenannte Privilegien. Das Token wird üblicherweise durch winlogon.exe erzeugt. Wenn sich nun ein Benutzer an Windows anmeldet, bekommt der Initialisierungsprozess durch von winlogon.exe ein Zugriffstoken; da nachfolgende Prozesse dieses Token erben, kann man vereinfacht sagen, dass dieses Token eine Art "Personalausweis" darstellt, mit dem verschiedene Berechtigungen verbunden sind.

> Die wesentlichen Inhalte des aktiven Zugriffstokens des angemeldeten Benutzers können mit dem Command-Shell-Befehl

whoami /all

Die folgende Grafik zeigt den grundsätzlichen Aufbau eines Access Token.

Access Token
Header Gültigkeitsdauer Prozessgruppe
Default DACL
User Account (Prozess-Besitzer)
Username: pc08\kevin
SID: S-1-5-21-808264081-4071840419- 2100235188-1001
Benutzergruppen
Gruppenname: JEDER SID: S-1-1-0
Gruppenname: PC08\LGrafikDesign SID: S-1-5-21-808264081-4071840419-21002
Privilegien
SeShutDownPriviledge
SeTimeZonePriviledge
Impersonation Level

Quelle: Microsoft "How Access Tokens work"

Nach dem Header, der unter anderem Informationen zur Gültigkeitsdauer des Zugriffstoken enthält, folgen die wichtigen Daten:

- User Account: Prozess-Besitzer; als Detailinformationen werden der Anmeldename und die SID gespeichert. Prozesse, die der Benutzer gestartet hat, werden im Task-Manager unter diesem Benutzernamen angeführt.
- Benutzergruppen: Hier sind alle Benutzergruppen (wieder mit Name und SID) aufgelistet, bei denen der Benutzer Mitglied ist; dazu gehören auch vordefinier-Benutzergruppen wie VORDEFIte NIERT\BENUTZER (S-1-5-32-545) oder VORDEFI-

NIERT\Remotedesktopbenutzer (SID S-1 -5-32-555). (Die in der Grafik dargestellte Gruppenliste ist nicht vollständig!)

- Impersonation Level: Ein sehr interessantes Feature ist die Möglichkeit, dass ein Benutzer durch einen sogenannten "Identitätswechsel" Berechtigungen eines anderen Benutzers bzw. Prozesses annehmen kann.
- Privilegien: Darunter versteht man Berechtigungen zur Durchführung bestimmter Aktionen. Beispiele:

SeShutDownPriviledge Berechtigung, das System herunterzu-

fahren

SeTimeZonePriviledge Berechtigung, die Zeitzone zu ändern

SeSystemTimePriviledge

Berechtigung, die Systemzeit zu ändern SeBackupPriviledge

Berechtigung, eine Sicherung durchzuführen

SeRestorePriviledge

Berechtigung, eine Wiederherstellung durchzuführen

Privilegien können erteilt bzw. entzogen werden, indem man die Lokale Sicherheitsrichtlinie bearbeitet.

Default DACL: Diese Standard-Zugriffskontrollliste wird dazu verwendet, einen neuen Security Descriptor zu erzeugen, wenn der zugehörige Benutzer eine neue Ressource (etwa einen neuen Ordner oder eine neue Datei) erstellt. Diese Default DACL wird beim Anmeldevorgang bereits zusammengestellt, damit nicht bei jeder Ressourcenerzeugung eine neue DACL erstellt werden muss. Sie ist klarerweise so aufgebaut, dass der Erzeuger der Ressource auch Besitzer der Ressource wird.

Jedes Dateisystemobjekt (Datei, Ordner) besitzt einen sogenannten Sicherheitsdeskriptor, der beim Erzeugen des Objekt festgelegt wird. (Auch die Einträge in der zentralen Active Directory-Datenbank einer Domäne sicht durch einen Sicherheitsdeskriptor geschützt.)

Dieser Sicherheitsdeskriptor besteht aus einem Header und der bereits besprochenen DACL.

Die DACL enthält einen Header und mehrere Zugriffskontrolleinträge (ACE = Access Control Entries).

Header			
SID des Besitzers:			
S-1-5-21-808264081-4071840419-			
2100235188-1001			
Gruppen-SID			

DACL - Header				
Deny	pc08\Tracy	111111		
Allow	pc08\Kevin	111111		
Allow	pc08\Maria	110000		
Allow	JEDER	100000		

	SACL - Header	
Audit	pc08\Kevin	111111

Bedeutung:

- Die Spezialidentität JEDER hat Lese-Zugriff.
- Benutzerin Maria hat Lese-/ • Die Änderungs-Zugriff.
- Der Benutzer Kevin hat Vollzugriff.
- Der Benutzerin Tracy wurden alle Zugriffe verweigert (Deny-Eintrag), daher hat sie keinen Zugriff.

In der DACL können auch Gruppen spezifiziert sein. Bei Kollisionen gelten die bereits besprochenen Regeln (Deny vor Allow, ansonsten Rechtekumulierung).

Sonderfälle:

- NULL-DACL: Security Descriptor enthält überhaupt keine DACL (eine sogenannte "NULL-DACL"). Das bedeutet, dass jeder beliebig auf die Datei/den Ordner zugreifen kann.
- Leere DACL: Existiert die DACL, aber sie enthält keine Einträge (keine ACEs), dann darf NIEMAND auf die Datei/den Ordner zugreifen.

	SMB 1	SMB 2.0.2	SMB 2.1	SMB 3.0	SMB 3.0.2	SMB 3.1.1
Windows Vista	•	•				
Windows 7 Windows Server 2008 R2	•	•	•			
Windows 8 Windows Server 2012	•	•	•	•		
Windows 8.1	0	•	•	•	•	
Windows 10 Windows Server 2016 Windows Server 2019	0	•	•	•	•	•

Außerdem gibt es noch eine Systemzugriffsliste (SACL, System Access Control List). Diese Zugriffsliste regelt, welche Operationen im systemweiten Sicherheitsprotokoll aufgezeichnet werden. In unse- System) wurde im Jahr 1983 entwickelt rem Beispiel wird jede Operation, die der und 1988 von Microsoft im frühesten Benutzer Kevin auf die Datei ausführt, Netzwerkbetriebssystem protokolliert.

10.4 Netzwerkerkennung und Freigaben Um Ordner, Drucker und Dateien im Netz- wurde es mit Windows NT 4.0 in die aktuwerk gemeinsam verwenden zu können, elle Betriebssystemfamilie eingeführt. ist die Einrichtung von Freigaben nötig.

10.4.1 SMB (Server Message Blocks)

Voraussetzung für die Verwendung freigegebener Ordner ist das SMB-Protokoll. SMB 1.0 (CIFS = Common Internet File

- wird unterstützt
- 0 "optionale" Unterstützung, SMB 1.0 ist standardmäßig nicht aktiviert

LAN-Manager erstmals verwendet und erreichte große Popularität in den Versionen Windows for Workgroups und Windows 95/98. 1996

Es besteht aus einer Client- und einer Serverkomponente, deren (nostalgischer) Dienstname noch immer auf das ursprüngliche Betriebssystem verweist:

[•] SMB-Serverdienst (Dienstname: lan-

	SMB 1	SMB	SMB 2.1	SMB 3.0	SMB	SMB
Mehrere parallele Zugriffe über das Netzwerk auf Frei- gaben					•	•
Verschlüsselung	keine	AES-128-	AES-128-			
Art der File Handles	-	durable	resilient	persistent		
Übersteht Server- ausfälle				•	•	•
Unterstützung sym-		•	•	•	•	•
Sicherheit beim Zugriff auf Standard- freigaben (SYSVOL, NETLOGON)						SMB- Signatur, SHA512- Verschlüs- selung
SMB Direct, RDMA				•	•	•
SMB Multichannel				•	•	•
Anzahl Befehle	>100	19				
Ports	NetBIOS: TCP 139 Sonst: TCP 445	TCP 445				

manserver, Anzeigename: Server): wird erkennung benötigt, um Freigaben zu erstellen

 SMB-Clientdienst (Dienstname: lanmanworkstation. Anzeigename: Arbeitsstationsdienst) wird benötigt, um auf freigegebenen Ordner und Drucker zugreifen zu können

In TCP/IP-Netzwerken lief SMB ursprünglich über den NetBIOS-Port 139, und die Namensauflösung erfolgte mittels WINS. In der Zwischenzeit wurde auch DNS als Namensauflösungsmechanismus hinzugefügt, der aber unter SMB 1.0 nur verwendet wird, wenn NetBIOS-Namen nicht verfügbar sind. Zurzeit läuft SMB auch als Dienst microsoft-ds über den Port TCP/ stellungen ändern konfiguriert werden. UDP 445.

Grundsätzlich werden zwei Hauptversionen unterschieden, die wiederum verschiedene "Dialekte" umfassen; dabei werden oft alle Versionen ab SMB 2.0.2 mit dem Oberbegriff "SMB2" bezeichnet.

Freigaben dürfen von Administratoren und Benutzern erstellt werden (beim Server auch Server-Operatoren).

10.4.2 Netzwerkerkennung und Dateifreigabe

In den Windows-Betriebssystemen von Windows for Workgroups 3.11 bis Windows XP/Server 2003 gab es einen Netzwerkdienst, der die Aufgabe hatte, Computer im Netzwerk zu erkennen. den Dieser Dienst hatte Namen ComputerBrowser (Dienstname: Browser) falls die Netzwerkerkennung eingeschaltet den Ordner übers Netzwerk zugreifen und arbeitete mit NetBIOS-Namens- haben: broadcasts.

Obwohl der Dienst aus Gründen der Abwärtskompatibilität auch in Windows 10 noch enthalten ist (er ist aber nicht gestartet), wurde bereits in Windows Vista ein völlig neues Protokoll entwickelt, das nun für diese Aufgaben zuständig ist: Verbindungsschicht-Topologieerdie kennung (engl. Link Layer Topology Discovery, LLTD; Dienstname: Iltdsvc). Der LLTD-Dienst ist zwar standardmäßig installiert, wird aber nur bei aktivierter Netzwerkerkennung gestartet.

Klickt man im Windows-Explorer auf den Eintrag Netzwerk, so hängt die Reaktion von den Einstellungen der Netzwerkerkennung ab.

Windows 10 deaktiviert im Profil Privates Netzwerk standardmäßig die Netzwerkerkennung (das Auffinden von anderen SMB-Servern im Netzwerk) und die Dateifreigabe. In diesem Fall wird folgende Fehlermeldung angezeigt:

Netzwe	nk X
8	Die Netzwerkerkennung ist ausgeschaltet. Netzwerkcomputer und -geräte sind nicht sichtbar. Schalten Sie die Netzwerkerkennung im Netzwerk- und Freigabecenter ein.
	OK

Nach Bestätigung durch Klicken auf OK wird anschließend eine Information eingeblendet, dass die Netzwerk-

und/oder Dateifreigabe deaktiviert ist. Klickt man auf di Meldung, so können durch Auswahl de Menüpunkts Netzwerkerkennung un Dateifreigabe aktivieren sowo Netzwerkerkennung als auc Dateifreigabe ermöglicht werden.



Die Netzwerkerkennung und Dateifreiga be können im Systemsteuerungs-Ap Netzwerk- und Freigabecenter durch Anklicken des Links Erweiterte Freigabeein-



Wird die Netzwerkerkennung eingeschaltet, so werden im Windows-Explorer beim Klick auf das Symbol Netzwerk jene Netzwerkcomputer angezeigt, welche eben- Fügen Sie nun alle Benutzer hinzu, die auf



Freigabe des öffentlichen Ordners
Wenn "Freigabe des öffentlichen Ordners" aktiviert ist, können die Personen im Netzwerk (einschließlich der Heimnetzgruppen-Mitglieder) zuf die Dateien in den Ordnern "Öffentlich"
zugreifen.
Freigabe einschalten, sodass jeder Benutzer mit Netzwerkzugriff in Dateien in den Ordnern " öffentlich" lesen und schreiben kann
Freigabe des öffentlichen Ordners" deaktivieren (an diesem Computer angemeldete Benutzer können weiterhin auf diese Ordner zugreifen)
Medienstreaming
Wenn das Medienstraming aktiviert ist, können Personen und Geräte im Netzwerk auf Bilder, Musik und Videos auf diesem Computer zugreifen. Mit diesem Computer können auch Medien im Netzwerk gesucht werden.
Medienstreamingoptionen auswählen
Dateifreigabeverbindungen
Unter Windows wird die 128-Bit-Verschlüsselung verwendet, um Dateifreigabeverbindungen zu schützen. Einige Genzie unterstützen die 128-Bit-Verschlüsselung nicht, und für diese muss die 40- oder 56-Bit-Verschlüsstelung verwendet werden.
(a) 128-Bit-Verschlüsselung für den Schutz von Dateifreigabeverbindungen verwenden (empfohlen)
Dateifreigabe für Geräte mit 40- oder 56-Bit-Verschlüsselung aktivieren
Kennwortgeschütztes Freigeben
Wenn das kennwortgeschützte Freigeben aktiviert ist, können nur Benutzer, die ein Benutzerkonto und ein Kennwort für diesen Computer besitzen, auf freigegebene Dateien, die Ordner "Offentlich"

diesen Computer angeschlossene Drucker zugreiten. Sie in deaktivieren, um anderen Benutzern Zugriff zu geben

Kennwortgeschütztes Freigeben einschalten Kennwortgeschütztes Freigeben ausschalten

10.4.3 Erstellen von freigegebenen Ordnern mit dem Freigabe-Assistenten

Wählen Sie im Kontextmenü (rechte Maustaste) des freizugebenden Ordners den Eintrag Zugriff gewähren auf - Bestimmte Personen...:

	29/03/2020 12:32 Detect-direr	
luten	28.50 PERMISSION PROVIDENT	
FerfLogs	Offnes	
Programma	In neuem Fersiter Offinen	
Programme (x86)	An Schnellzugriff anheften	
Windows	Mit Windows Defender überprüfen	
	Zupitt gewähren auf	> 🚊 Zugriff entfernen
	Vorgängerversionen wiederherstellen	at Eastimote Eastern
	In Bibliothek aufrehmen	> a reasonaria
Personen für d	e Freigabe auswählen	
Personen für d Seben Sie einen Na Sach Personen zu s	ie Freigabe auswählen men ein, und klicken Sie dann auf "Hinzufügen uchen.	", oder klicken Sie auf den Pfe
Personen für d Seben Sie einen Na sach Personen zu s Kevin	ie Freigabe auswählen men ein, und klicken Sie dann auf "Hinzufügen uchen.	*, oder klicken Sie auf den Pfe
Personen für d Geben Sie einen Na Geben Personen zu s Kesin Name	ie Freigabe auswählen men ein, und klicken Sie dann auf "Hinzufügen Ichen.	*, oder klicken Sie auf den Pfe V Hinzufügen Berechtigungsebene

dürfen. Standardmäßig erhalten diese hinzugefügten Benutzer die Berechtigungsebene Lesen. Beim Zugriff übers Netzwerk dürfen Dateien im freigegebenen Ordner weder geändert noch gelöscht werden.

Besitzer
Lesen 🔻

Klicken Sie nun auf die Schaltfläche Freigeben, um den Vorgang durchzuführen.

Freigabeoptionen für unterschiedliche Netzwerkprofile ändern

Für jedes von Ihnen verwendete Netzwerk wird unter Windows ein separates Netzwerkprofil erstellt. Für die einzelnen Profile können Sie bestimmte Optionen auswählen.

Priva	at (aktuelles Profil)
	Netzwerkerkennung
	Wenn die Netzwerkerkennung eingeschaltet ist, kann dieser Computer andere Netzwerkcomputer und -geräte sehen, und er ist selbst sichtbar für andere Netzwerkcomputer.
	Netzwerkerkennung einschalten Automatisches Setup von Geräten aktivieren, die mit dem Netzwerk verbunden sind Netzwerkerkennung ausschalten
	Datei- und Druckerfreigabe
	Wenn die Freigabe von Dateien und Druckern aktiviert ist, können Netzwerkbenutzer auf Dateien und Drucker zugreifen, die Sie von diesem Computer freigeben.
	Datai- und Druckarfreigabe aktivieren

- (●) Datei- und Druckerfreigabe aktivieren
- O Datei- und Druckerfreigabe deaktivieren

Gast oder Öffentlich

UBSYSTEM NE



Es werden vom Assistenten die entsprechenden NTFS-Berechtigungen geändert; die Freigabeberechtigungen werden auf Jeder – Vollzugriff und Administratoren – Vollzugriff erweitert.

10.4.4 Freigabe-Assistent deaktivieren

Um den Freigabe-Assistenten nicht verwenden zu müssen, starten Sie zunächst den Windows-Explorer und klicken auf **Optionen – Ordner- und Suchoptionen ändern**.

In der Registerkarte **Ansicht** deaktivieren Sie die Option **Freigabe-Assistent verwenden (empfohlen)**.

Ab diesem Zeitpunkt können Ordner und Drucker ohne Freigabe-Assistent freigegeben werden.

Das Kontext-Menü **Zugriff gewähren auf** bietet jetzt nur mehr die Option **Erweiterte Freigabe** an.



10.4.5 Freigabe-Berechtigungen Zweck von Freigabeberechtigungen

- Auch unter einem FAT16/FAT32-Dateisystem kann der Zugriff auf eine Ressource über das Netzwerk grob geregelt werden.
- Unter NTFS ist das Arbeiten mit Freigabeberechtigungen meist nicht üblich.

Um Freigabe-Berechtigungen vergeben oder nachträglich ändern zu können, ruft man die Eigenschaften des freigegebenen Ordners auf, Karteikarte **Freigabe.**

Klicken	Sie auf	die	Schaltfläche	Erweiterte
Freigab	e:			

Leger mehre Freiga	n Sie benutzerde ere Freigaben un abe ein.	finierte Ber d richten S	echtigunge ie Optionen	n fest, erstellen Sie i für die erweiterte
•	<u>E</u> rweiterte Freig	abe		

Es erscheint das rechts dargestellte Dialogfeld.

Klicken Sie auf die Schaltfläche **Berechtigungen**, um bestehende Freigabeberechtigungen anzuzeigen bzw. zu ändern.

Der Ordner wurde freigegeben.

Sie können jemandem Links zu diesen freigegebenen Elementen per E-Mail senden oder die Links kopieren und in eine andere App einfügen.



F

Erweiterte Freigabe	×
Diesen Ordner freiaeben	
Einstellungen	
Ereigabename:	
Daten 🗸	
Hinzufügen Entfernen	
Zugelassene Benutzeranzahl einschränken 20	
Berechtigungen Zwischenspeichern	
OK Abbrechen Übernehme	n

Man unterscheidet nur drei Berechtigungsstufen:

- Vollzugriff
- Ändern
- Lesen
- Wichtig:

Standardmäßig ist in Windows nur für den Ersteller der Freigabe ein Zugriffsrecht eingetragen. Alle weiteren Berechtigungen müssen manuell konfiguriert werden.

Berechtigungen für die Freigabe gelten auch für alle Unterordner und alle Dateien in der Freigabe.

📕 Berechtigungen für "Daten"	I.		×
Freigabeberechtigungen Gruppen- oder Benutzemamen:			
Vevin (PC08\Kevin)	inistratoren)		
	Hinzufügen	<u>E</u> ntfemen	
Berechtigungen für "Jeder"	Zulassen	Verweigem	
Vollzugriff Ändem Lesen			

Freigabeberechtigungen setzen immer auf den NTFS-Berechtigungen auf. Freigabeberechtigungen können daher niemals NTFS-Berechtigungen erweitern, nur einschränken (sie wirken als eine Art zusätzliches "Filter", das beim Zugriff über das Netzwerk aktiv wird).

10.4.6 Freigabe beenden

Dazu reicht es aus, im Ordner-Kontextmenü Zugriff gewähren auf – Erweiterte Freigabe auf die Schaltfläche Freigabe zu klicken und dort das Kontrollkästchen Diesen Ordner freigeben zu deaktivieren.

rweiterte Freigabe	×	
Diesen Ordner freigeben		

Sollten Benutzer gerade über das Netzwerk eine Verbindung mit dieser Freigabe aktiv haben, so erscheint folgende Warnmeldung:



10.4.7 Verdeckte Freigaben

Freigabenamen mit einem \$-Zeichen am Ende sind "unsichtbar". (Verknüpfungen zu diesen Freigaben können nur dann eingerichtet werden, wenn der Freigabename bekannt ist)

10.4.8 Administrative Freigaben

Administrative Freigaben sind spezielle Freigaben, die bereits vom System angelegt werden und (standardmäßig) nicht gelöscht werden können bzw. bei Löschung automisch beim nächsten Neustart neu angelegt werden. Sie können nur von Mitgliedern der Administrator-Gruppe verwendet werden. Auch werden die administrativen Freigaben für ein fehlerfreies Funktionieren des Betriebssystems benötigt.

Diese speziellen Freigaben sind in MMC-Konsole **Computerverwaltung** sichtbar.

10.4.9 Zugriff auf freigegebene Ordner

Die Freigabe ist in der Netzwerkumgebung als verbundener Ordner sichtbar.

Hinweis: Beachten Sie, dass Windows 10 für den Zugriff auf freigegebene Ordner ein Konto mit Kennwort verlangt!

Sie können den freigegebenen Ordner auch mit **##** + R und Eingabe des UNC-Pfades aufrufen:



Gegebenenfalls werden noch die nötigen Netzwerkanmeldeinformationen abgefragt:

Windows-Sicherheit	×		
Netzwerkanmeldeinformationen eingeben			
Geben Sie Ihre Anmeldeinformat mit folgendem Netzwerk herzust	ionen ein, um eine Verbindung ellen: pc08		
\\pc08\kevin			
•••••	୕		
Domäne:			
Anmeldedaten speichern			
Weitere Optionen			
ОК	Abbrechen		

Im Explorer wird nun der Inhalt des freigegebenen Ordners angezeigt:



10.4.10 Zuordnen von Laufwerksbuchstaben zu Freigaben ("Mapping")

Jeder Freigabe kann ein Laufwerksbuchstabe zugeordnet werden:

Laufwerksbuchstabenzuordnung in der Kommandozeile mit der Anweisung *net use*:

Beispiel:

C:\>net use M: \\r10\Testordner

Der Befehl wurde erfolgreich ausgeführt.

Werden zugeordnete Laufwerksbuchstaben nicht mehr benötigt, so kann die Freigabe wieder getrennt werden:





Name	Bedeutung der administrativen Freigabe
ADMIN\$	zeigt auf den Systemordner (zum Beispiel C:\WINDOWS) - für administ- rative Zugriffe
PRINT\$	für Druckeradministration; Print-Operatoren, Administratoren haben Vollzugriff
C\$, D\$, E\$, …	Systemfreigabe für jeden Laufwerksbuchstaben
IPC\$	für die Verwaltung der Freigaben nötig (Inter-Process Communication)



 Öffnen

 In neuem Fenster öffnen

 An Schnellzugriff anheften

 Immer offline verfügbar

 Vorgängerversionen wiederherstellen

 An "Start" anheften

 Netzlaufwerk verbinden...

bzw.

C:\>net use M: /delete

Daten

10.4.11 Fernanmeldung, automatische Fernanmeldung

Beispiel: Wir nehmen an, dass auf einem Rechner mit dem Namen PCO2 ein freigegebener Ordner mit dem Freigabenamen "daten" existiert. Auf beiden Rechnern wurde ein lokaler Benutzer mit dem Anmeldenamen Kurt erzeugt. Die beiden Benutzer haben unterschiedliche Kennwörter und natürlich auch unterschiedliche SIDs.

Die Sicherheitsberechtigungen für den Ordner "daten" wurden so eingerichtet,

dass nur der Benutzer Kurt Zugriffsrechte (zum Beispiel "Ändern") auf diesen Ordner hat.



Wir nehmen nun an, dass sich PC01\Kurt mit dem UNC-Pfad \\PC02\daten zum freigegebenen Ordner verbinden will. Die überprüft Benutzername, Kennwort und den Ordner und wählen Sie im Kontext- keine Rolle, ob Sie die Änderungen auf SID. Nur eine von diesen drei Eigen- menü den Eintrag Zugriff gewähren auf - einem Computer, einem mobilen Gerät schaften stimmt überein (der Benutzerna- Erweiterte Freigabe. Klicken Sie auf die oder in einem Ordner auf einem Netzme), daher wird PC01\Kurt nicht ohne Schaltfläche Erweiterte Freigabe. weiteres der Zugriff auf den Ordner gewährt; es erscheint ein Dialogfeld für die Im Dialogfeld Erweiterte Freigabe klicken Fernanmeldung:

Windows-Sicherheit	×			
Netzwerkanmeldeinfor	mationen eingeben			
Geben Sie Ihre Anmeldeinformationen ein, um eine Verbindung mit folgendem Netzwerk herzustellen: pc04				
pc04\Kevin				
•••••	୕			
Anmeldedaten speichern				
Weitere Optionen				
ОК	Abbrechen			

Wenn die Anmeldeinformationen zum Zugriff auf den Ordner berechtigen, so wird der Ordnerinhalt im Windows-Explorer angezeigt; die Netzwerkanmeldeinformationen werden zwischengespeichert. Für weitere Zugriffe werden die Anmeldeinformationen nicht mehr abgefragt, es sei denn, der Benutzer auf dem Dateiserver hat sein Kennwort geändert.

Sollte die Freigabe inzwischen widerrufen worden sein, so erscheint folgende Fehlermeldung:



Modifizieren wir nun das Beispiel so, dass die Kennwörter der beiden Benutzerkonten übereinstimmen. Wieder überprüft die LSA auf PCO2 Benutzername, Kennwort und SID - zwei dieser drei Eigenschaften stimmen überein (Benutzername und Kennwort). Nun erscheint kein Dialogfeld; es erfolgt eine automatische Fernanmeldung. Die Zugriffsberechtigungen für PC01\Kurt sind so, als hätte er sich als PC02\Kurt angemeldet.

10.4.12 Offline-Ordner und Synchronisierungscenter

Es ist möglich, Dateien, auf die über einen freigegebenen Ordner zugegriffen wurde, lokal zwischenzuspeichern. Das hat den Vorteil, dass die Dateien auch erreichbar sind, falls der Server (auf dem sich der synchron zu halten. Jedes Mal, wenn Sie freigegebene Ordner befindet) gerade eine Datei an einem Ort hinzufügen, ännicht erreichbar sein sollte.

Sie auf die Schaltfläche Zwischenspeichern.

Erweiterte Freigabe	×
Diesen Ordner freigeben	
Einstellungen	
<u>F</u> reigabename:	
Daten 🗸	
Hinzufügen Entfernen	
Zugelassene Benutzeranzahl einschränken 20	
Berechtigungen Zwischenspeichern	
OK Abbrechen Übernehme	n
Offlineeinstellungen	×

Sie können auswählen, welche Dateien und Programme ifalls überhaupt) für Offinebenutzer zur Verfügung gestellt werden.
Image And Angeletic A
○ Keine Dateien oder Programme aus dem freigegebenen Ordner offline verfügbar machen
O Alle Dateien und Programme, die Benutzer über den freigegebenen Ordner öffnen, automatisch offline verfügbar machen
Für baba Leistung antimiaran

Standardmäßig wird für das Zwischenspeichern 10 % der Festplatte verwendet; dieser Wert kann geändert werden.

Die Konfiguration kann zentral auch über das "Synchronisierungs-Center" erfolgen:

Synchronisierungs-Setup			- 🗆 X
t + 🕲 = Synchroni	ieungcenter + Synchronisierungs-Setup	~ 0	P. "Systemianip Setup"
Statuete der Systemsteuerung	Synchronisierungspartnerschaften	einrichten	
Synchronisierungs- partnerschaften anzeigen	Um eine Synchronisierung durchführen zu können, muss eine Synchronisierungspartnerschaft eingelichtet werden. Fals das zu sonchronisierende Element har nicht aufzallicht ist, wird es reisblichervesse eicht som		itierungspartnerschaft eingerichtet wird es möglicherweise nicht vom
Synchroniserungskonflikte anseigen	Computer erkannt oder ist möglicherweise ni	cht mit dem Synchronisien	ungocenter kompatibel.
Synchronisierungkergebnisse anteigen			0
Synchronikierungs- partnerschaften einrichten	Didner (1)		· · · · · · · · · · · · · · · · · · ·
Offinedateien verwahen	Contractions officer configuration Contractions	Differentiationer anter Antroprettan, searce 1 mailline Manatanile -	opiction, auf Natzwerkünteren Se offine artaiten, Kluiter Sie rot det in anere Netzwerkündere auf eine Dat

In Windows bezeichnet Synchronisierung den Vorgang, Dateien an zwei oder mehr Orten identisch zu halten.

Die Synchronisierung kann unidirektional oder bidirektional erfolgen. Bei der unidirektionalen Synchronisierung werden jedes Mal, wenn Sie eine Datei oder andere Informationen an einem Ort hinzufügen, ändern oder löschen, dieselben Informationen am anderen Ort hinzugefügt, geändert oder gelöscht. Es werden jedoch nie Änderungen am ersten Ort ausgeführt, da die Synchronisierung nur in einer Richtung erfolgt.

Bei der bidirektionalen Synchronisierung werden Dateien in beide Richtungen kopiert, um die Dateien an beiden Orten dern oder löschen, wird dieselbe Ände-

LSA (Local Security Authority) auf PC02 Klicken Sie mit der rechten Maustaste auf rung am anderen Ort ausgeführt. Es spielt werkserver vorgenommen haben. Dieselben Änderungen werden an beiden Orten ausgeführt. Die bidirektionale Synchronisierung wird meist in Arbeitsumgebungen verwendet, in denen Dateien häufig an mehreren Orten aktualisiert und dann mit anderen Orten synchronisiert werden.

> Im Synchronisierungscenter können Sie den Computer mit Netzwerkordnern, mobilen Geräten und kompatiblen Programmen synchronisieren. Das Synchronisierungscenter kann Dateien und Ordner an verschiedenen Orten automatisch synchron halten.

10.4.13 Veröffentlichen von Freigaben im Active Directory

Nur im Domänenbetrieb möglich!

Über das MMC-Snap-In "Computerverwaltung" unter "Freigegebene Ordner":

Computerverwaltung				
atei Aktion Ansicht ?				
• 🔶 🙍 📷 🖾 🧟 🕞	2 🖬			
Computerverwaltung (Lokal) System Cardination Cardination Cardination Computerverwaltung Cardination C	Freigabename	Ordnerpfad C//WINDOWS C/\ F/\	Typ Windows Windows Windows	Anzahl der Cli 0 0 0
Ereigaben B. Strungen B. Strungen B. Geoffnete Dateien So Leistung Geräte-Manager So Datenspeicher Datenstrigerverwaltung	30 IPCS 30 printS Freigabe 4 Alte Aufge Aktualisie Bigenschu	Offnen Freigabe aufheben Alle Aufgaben Altualisieren Bigenschaften Häfe	Windows L. Windows	0
Eigenschaften von E	ata DC auf	Dhone		~
Allgemein Veroffent Diese Freigabe in <u>P</u> fad zum freigeg \\PC04\Foto P	n Active Direc ebenen Ordno Cauf iPhone	abeberechtigungen story veröffentlichen er:	Sicherheit	
B <u>e</u> schreibung:				
Benutzer (z. B., J redmond \JeffSmi	leffSmith@red ith):	lmond.corp.microsoft.c	om oder	
Schlüsselwörter:			Be <u>a</u> rbeiten.	

22

11Fernwartung und Fernzugriff

Christian Zahler

typische Aufgabe IT-Fine im Systemadministrationsbereich ist die Unterstützung anderer Benutzer bei Problemen. Oft ist es aus Zeitgründen nicht sinnvoll, persönlich zum entsprechenden Problemort zu reisen. Die heute übliche Methode besteht in der Fernwartung von Geräten.

Von Microsoft gibt es das Feature Remoteunterstützung; ein sehr beliebtes Tool, vor allem zur Unterstützung von Privatpersonen und KMUs ist TeamViewer.

11.1 Remotedesktop

Der Remotedesktop ermöglicht die Übertragung des Bildschirms eines entfernten Computers. Der zugrunde liegende Dienst wird als Terminal-Server bezeichnet. Während es auf Server-Betriebssystemen möglich ist, bei entsprechender Installation und Lizenzierung beliebig viele Terminal-Sitzungen aufzubauen, ist die Anzahl der gleichzeitigen Verbindungen bei Client -Betriebssystemen auf eine aktive Verbindung limitiert.

Wenn am Remotecomputer bereits eine Konsolensitzung aktiv ist (beispielsweise ist ein Benutzer angemeldet und arbeitet auf dem PC), so ist keine Remotedesktopverbindung möglich. Dies wird durch folgende Fehlermeldung angezeigt:

Remot	sdesktopverbindung	,
8	Für den Computer konnte keine W Remotecomputer hergestellt werd	erbindung mit einer anderen Konsolensitzung auf dem Ien, da bereits eine Konsolensitzung aktiv ist.
		OF HIT

Mit der Remotedesktop-Funktionalität können Sie einen entfernten Computer so bedienen, als ob Sie direkt vor ihm sitzen würden. Das funktioniert bei entsprechender Konfiguration natürlich auch über das Internet.

Vergleich: Stellen Sie sich einfach vor, Sie würden Ihre Tastatur, Ihre Maus und Ihren Monitor mit einem "sehr langen Kabel" mit dem entfernten PC verbinden.

Hinweis: Beachten Sie, dass Windows 10 für den Zugriff mittels Remotedesktopverbindung ein Konto mit Kennwort verlangt!

Vorgangsweise:

1. Schritt: Einrichten des "Servers" (das ist der Windows 10-PC, zu dem Sie sich von der Ferne aus verbinden wollen)

In den Systemeigenschaften (**III** + Pause) wählen Sie Remoteeinstellungen. Dort wählen Sie Remoteverbindung mit diesem Computer zulassen.



Standardmäßig ist diese Remoteverbindung bereits für den lokalen Administrator zugelassen, unter der Schaltfläche Benutzer auswählen... können jedoch beliebige lokale Benutzer eingetragen werden, die Remoteverbindungen herstellen können.

Systemeigenschaften					×
Computername Hardware	Erweitert	Computerschutz	Remote		
Remoteunterstützung					
Remoteunterstützungs	sverbindung	jen mit diesem Com	nputer zula	issen	
<u>Was geschieht, wenn Re</u> i <u>st?</u>	moteunters	tützung aktiviert			
			Erweite	ert	
Remotedesktop					
Wählen Sie eine Option aus, und geben Sie anschließend an, wer eine Verbindung herstellen darf. ○ Keine Remoteverbindung mit diesem Computer zulassen					
Remoteverbindung mit diesem Computer zulassen					
Verbindungen nur von Computern zulassen, äuf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird (empfohlen)					
Entscheidungshilfe		Benutz	er auswäh	len	
	(OK Abbred	chen	Überneh	imen
Remotedesktonhenutzer				,	\mathbf{v}



2. Schritt: Verbinden zum eingerichteten Server vom "Client" aus (das ist der PC, auf dem Sie arbeiten und von welchem aus Sie den entfernen Computer anspre- den Computernamen mit angeben, etwa chen wollen):

Wählen Sie im Startmenü Windows-Zubehör – Remotedesktopverbindung oder wählen Sie Start – Ausführen + R) und geben mstsc ein (Microsoft Terminal Services Client):



Dort geben Sie dann den Computernamen (DNS-Namen) oder die IP-Adresse des entfernten PCs an, auf dem Sie arbeiten wollen.

퉣 Ren	notedesktopverbindung	×
5	Verbindung wird hergestellt mit: pc08	
	Remoteverbindung wird gesichert	Abbrechen

Sie müssen sich noch am entfernten PC anmelden. Standardmäßig wird Ihnen das Benutzerkonto vorgeschlagen, mit dem Sie selbst an Ihrem eigenen PC angemeldet sind.

Das wird aber nicht in jedem Fall funktionieren; klicken Sie daher auf den Link Weitere Optionen und wählen Sie Anderes Konto verwenden.

Geben Sie dann Benutzername und Kennwort für ein Konto an, welches die Berechtigung hat, auf dem entfernten PC zu arbeiten.

Achtung: Für ein lokales Konto müssen Sie pc08\kevin:

pc08\kevin		
•••••	୕	
Domäne: pc08		

Wichtiger Hinweis: Aus Sicherheitsgründen ist keine Anmeldung mit PIN am Remote-PC möglich!



Falls der angesprochene Computer kein vertrauenswürdiges Zertifikat liefert, erscheint folgende Fehlermeldung:



Wenn am "Server" bereits ein Benutzer angemeldet ist, so erscheint am "Client" folgende Meldung:



Klickt man "Ja", so wird der Client aufgefordert zu warten.



	Remotehil	lfe —	□ ×
	Mit de	er Remotehilfe von Microsoft kö	nnen zwei
	Personen einen Computer über eine		
	Remoteverbindung teilen, wobei eine Person		
	der an	Computer der Losung von Prob	iemen aur
	den e		
	Ŕ	Unterstützung anfo	ordern
		Gewähren Sie einer vertrauens	würdigen
		Person zur eigenen Unterstütz	ung Zugriff
		auf Ihren Computer. Geben Sie	den
		6-stelligen Sicherheitscode ein zur Verfügung gestellt wurde	, der Ihnen
		zur verlagang gestellt marae.	
		Code von Assistent	
	\mathbf{O}	Unterstützung	
	\cap	gowähren	
		gewannen	
		Eine andere Person über eine	
		Remoteverbindung unterstütze	en
		Unterstützen einer anderen F	Person
Re	motehilfe		
	Angem	eldet als:	
	Angem		
		Christian	
	\bigcirc	office@zahler.at	
		Mit anderem Konto anmel	den
	C: -1-		
	Siche	erneitscode freigeb	en
	D:- D		
	Die Per	rson, der Sie neifen, benötigt (einen
	mit ihre	em Gerät herstellen können.	indung
	Sich	erbeitscode: 507157	
	Cod	le läuft ab in 08:53	
	Wie mö	öchten Sie diese Informatione	n
	übermi	itteln?	
	IN ZWIS	chenablage kopieren	
	E-Mail :	senden	
		1. N. 1. H.	
	A		
	Anweis	sungen bereitstellen	
	Anweis	sungen bereitstellen	
	Anweis	sungen bereitstellen	

Hilfesuchende Person: Geben Sie nun den 6-stelligen Sicherheitscode ein, der ihnen von der helfenden Person übermittelt wurde. Klicken Sie auf **Bildschirm freigeben**.



Warten auf den Helfer, um diese Sitzung einzurichten

Auf dem Bildschirm des Helfers muss nun die Art des Zugriffs ausgewählt werden:

- Vollzugriff: Nur in diesem Modus können Sie den Remotecomputer fernsteuern.
- Bildschirm anzeigen: Es wird zwar der Bildschirm des Remotecomputers angezeigt, er kann aber nicht gesteuert werden.

Klicken Sie auf Weiter.

Es erscheint die Meldung

Verbindung wird hergestellt

und dann

Warten auf Teilnehmer für Berechtigungserteilung

Nun muss die hilfesuchende Person am Remotecomputer den Bildschirm freigen.



Hilfesuchende Person:

Bildschirm freigeben

Wählen Sie Zulassen aus, damit Christian Z. Ihren Bildschirm während dieser Sitzung anzeigen kann.

Wenn dies nicht Ihren Erwartungen entspricht oder Christian Z. keine Person ist, der Sie vertrauen, melden Sie dies über den nachstehenden Link, und wählen Sie Abbrechen aus.

Wenn Christian Z. eine Person ist, der Sie vertrauen, setzen Sie den Vorgang fort, und achten Sie darauf, alle Elemente zu schließen, die für diese Person nicht sichtbar sein sollen.

Möglichen Betrugsversuch melden

Schützen vor betrügerischen		
technischen Support kommen		
Zulassen Abbrechen		

Nutzungsbedingungen

ein Fenster, in dem der Bildschirm der hilfesuchenden Person dargestellt wird. Es ist nun möglich, den Bildschirm der hilfesuchenden Person fernzusteuern.

Remotehilfe	-		×	
Bildschirmfreigabe ein		Ш	Ê.	

Die Bildschirmfreigabe kann von der hilfesuchenden Person jederzeit beendet werden. Am PC des Helfers erscheint dann folgende Meldung:

Bildschirmfreigabe wurde beendet

Die Person, der Sie helfen, hat die Bildschirmfreigabe beendet. Schließen Sie die Remotehilfe nun.

Remotehilfe-Fenstern im Modus "Bildschirm anzeigen":



Remotehilfe-Fenstern im Fernsteuerung möglich. Es gibt zusätzliche chenden Person) Schaltflächen für den Neustart des Remotecomputers und das Aufrufen des Task- Sie Managers am Remote-PC.



11.3 Remoteunterstützung

Das Feature Remoteunterstützung basiert Die Remoteunterstützung ist nicht mehr auf dem Remote Desktop Protocol (RDP) im Startmenü verfügbar, sondern muss und ist ein Feature, welches nur mehr aus Kompatibilitätsgründen auf Windows 10

verfügbar ist. Es wird in naher Zukunft nicht mehr zur Verfügung stehen.

Das Feature Remoteunterstützung dient dazu, die Fernsteuerung anderer Bildschirme zur Unterstützung von Anwender/ innen zu ermöglichen.

Schritt 1: In den Systemeigenschaften (+ Pause) wählen Sie die erweiterte Konfiguration und zeigen die Karteikarte Remote an. Dort überprüfen Sie, ob Remoteunterstützungsverbindungen mit diesem Computer zulassen aktiviert ist.

Systemeigensch	aften					
Computername	Hardware	Erweitert	Computerschutz	Remote		
Remoteunter	stützung					
Bemoteunterstützungsverbindungen mit diesem Computer zulassen						
Was geschiel ist?	Was geschieht, wenn Remoteunterstützung aktiviert ist?					
				<u>E</u> rweitert		

Dies bewirkt, dass der Teredo-Dienst gestartet wird. Dieser Dienst ermöglicht es Am Bildschirm des Helfers erscheint nun dem Helfer, über die meisten Router (verkabelt oder drahtlos), die die Netzwerkadressübersetzung (NAT) verwenden, eine Verbindung mit Ihrem Computer herzustellen. Der Dienst fordert bei einem Microsoft Teredo-Server eine IPv6-Adresse für die Remoteverbindung an. Die Windows-Remoteunterstützung wird von der Windows-Firewall zugelassen, sodass die Kommunikation mit dem Computer des Helfers möglich ist.

> Klicken Sie auf die Schaltfläche Erweitert..., um detailliertere Einstellungen festzulegen.

Remoteunterstützungseinstellungen	×
Sie können die Zugriffsberechtigungen für die Remoteunterstützung dieses Computers einschränken.	
Remotesteuerung	
Remotesteuem dieses Computers zulassen	
Einladungen Legen Sie die maximal zugelassene Zeitdauer fest, für die die Einladungen gelten.	
6 V Stunden V	
Einladungen erstellen, die nur auf Computem verwendet werden können, auf denen Windows <u>Vi</u> sta oder höher ausgeführt wird	
OK Abbrechen	

Modus Schritt 2: Senden einer Remoteunterstüt-"Vollbild": Nur in diesem Modus ist die zungsanforderung (am PC der hilfesu-

> können Windows-Remoteunterstützungsanforderung mithilfe einer E-Mail oder einer Datei senden und empfangen. Sie können Sofortnachrichten verwenden, um sich mit der Person auszutauschen, der Sie helfen oder die Sie unter- Klicken Sie anschließend auf OK. stützt.

mit 📕 + R direkt aufgerufen werden:

Öffnen:	msra
o intern	

Möchten Sie um Hilfe hitten oder Hilfe anhieten?

Schritt 1 – PC der hilfesuchenden Person:

trauenswürdige Person zur Unterstützung einladen Ibietende Person sieht den Bildschirm und erhält ebenfalls die Möglichkeit, den

Wie möchten Sie den vertrauenswürdigen Helfer einladen?

×

Sie können eine Einladung erstellen und diese an die helfende Person senden. Außerdem können Sie Easy Connect verwenden, um das Herstellen einer Verbindung mit der helfenden Person zu vereinfachen.

- → Einladung als Datei speich Einladung per E-Mail senden

Am einfachsten ist EasyConnect; für EasyConnect müssen beiden Computer Windows 10 ausführen und PNRP unterstützen (Peer Name Resolution Protocol), die verwendeten Router müssen IPv6-Tunneling und UPnP unterstützen.

Auf dem Bildschirm der hilfesuchenden Person erscheint nun folgende Meldung:

Windows-Remoteunters	tützung		-		×
🔁 Chat 🎄 Einstellungen	Problembehandlung	Hilfe			
Lassen Sie dem Helfe JRR42ZLGY3QY	r die Einladungsdat	ei und das K	ennwort z	ukomn	nen.
Auf also ask and a Mashin doub	and the second se				

Schritt 2 – PC der helfenden Person:

Wird die Einladung als Datei gespeichert, so entsteht folgende Datei:

Einladung marcincident 02.04.2020 19:00 Windows-Remote...

Doppelklick auf diese Einladung öffnet folgendes Fenster, in welches der Code eingegeben werden muss, den die hilfesuchende Person angezeigt bekommt.

Remoteunterstützung	×
Geben Sie das Kennwort ein, um eine Verbindung mit dem Remotecomputer herzustellen.	
Das Kennwort erhalten Sie von der Person, von der die Unterstützung angefordert wurde. Nach Eingabe des Kennworts und Klicken auf "OK" wird eine Remoteunterstützungssitzung gestartet.	
Kennwort eingeben:	
JRR42ZLGY3QY	
OK Abbrech	en

Schritt 3 – PC der hilfesuchenden Person: Hier wird nun gefragt, ob der Helfer eine Verbindung herstellen darf. Klicken Sie auf Ja, um dies zu erlauben.



Schritt 4 - PC der helfenden Person: Der Bildschirm des Remotecomputers wird nun angezeigt. Wenn auf die Schaltfläche Steuerung anfordern geklickt wird, so ist eine Fernsteuerung des entfernten PCs möglich.

_		×
	-	- 0

Wird die Sitzung von einem der beiden Partner beendet, so wird dies im Windows-Remoteunterstützungs-Fenster angezeigt.



11.4 TeamViewer

TeamViewer ist der Marktführer bei den Fernverwaltungs-Tools. Er stammt nicht von Microsoft.

Mit TeamViewer lässt sich ein Bildschirm remote steuern; auch die Fernbedienung der Maus wird unterstützt.

Beide Partner benötigen die TeamViewer-App, die von www.teamviewer.com heruntergeladen und installiert werden muss. Beide rufen nun Teamviewer auf und telefonieren miteinander.

Die Person, die Hilfe benötigt, gibt dem IT -Experten die ID (eine Zahl mit 9 – 10 Stellen) bekannt, dieser trägt diese ID unter Partner-ID ein und klickt dann auf Verbinden. Anschließend gibt der IT-Experte das Passwort des Gegenübers ein; es wird dann eine Verbindung aufgebaut und der Bildschirm des Gegenübers angezeigt. Nun kann die Problembehebung direkt am Gerät erfolgen.



12 Serverfeatures

Features mit Windows Server 2016/2019

Christian Zahler

Hinweis: Die technischen Details zu die- 12.3 BranchCache sen Features werden im Skriptum "Windows Server 2019 – Netzwerkinfrastruktur" behandelt.

12.1 Always On VPN

Always On VPN ist die Nachfolgetechnologie für DirectAccess. Es geht dabei um die VPN-Anbindung von Clients, die nicht direkt mit dem Unternehmensnetzwerk verbunden sind, etwa Notebooks von Außendienstmitarbeitern, HomeOffice etc.

Always On VPN stellt immer dann automatisch eine VPN-Verbindung zum Unternehmensnetzwerk her, wenn der Client eine Internetverbindung verfügbar hat.

Directory-integrierten Gruppenrichtlinien.

Enterprise.

12.2 Neue Remote Desktop-Dienste

Es ist nun möglich, dass Clients einen Windows 10-basierenden Remote Desktop-Zugriff erhalten, der vom Windows Server aus bereitgestellt wird.

Neu ist, dass Anwender mit einem HTML5 -Client per Remote Desktop Web Access auf den Remote Desktop zugreifen können.

In Zweigstellenszenarios, in denen lange Reaktionszeiten bei Anwendungen die Produktivität der Benutzer beeinträchtigen können, stellt das Optimieren der Netzwerk-Bandbreitenauslastung und Verbessern der Anwendungsreaktionszeit eine der größten Herausforderung dar. Mit BranchCache wird das Reaktionsverhalten von Intranetanwendungen für Remoteniederlassungen verbessert und gleichzeitig die Auslastung von WANs (Wide Area Network) reduziert. Branch-Cache speichert eine lokale Kopie von Daten, auf die Clients über Remotewebund -dateiserver zugreifen. Der Cache kann auf einem gehosteten Server in der Zweigstelle platziert werden oder sich auf Nachteil: Keine Unterstützung von Active den Computern der einzelnen Benutzer befinden. Wenn ein anderer Client die gleiche Datei anfordert, lädt er die Datei Voraussetzung: Windows 10 Pro oder über das lokale Netzwerk herunter, ohne sie über das WAN abrufen zu müssen. Mit BranchCache wird sichergestellt, dass nur autorisierte Clients auf angeforderte Daten zugreifen.

> Das Feature ist mit sicherem Datenabruf über SSL oder IPSec kompatibel. Nach der Installation des Features am Dateiserver über den Server-Manager müssen die Client-PCs unter Windows 10 mit Gruppenrichtlinien konfiguriert sowie die Kommunikation über spezielle Firewallregeln erlaubt werden. Die Funktion lässt sich mit den Befehlen netsh branchcache show status bzw. netsh branchcache show localcache überprüfen.



13 Drucker

Christian Zahler

Man unterscheidet grundsätzlich:

Physischer Drucker (Druckge



Darunter versteht man die eigentliche Hardware.

Logisches Druckerobjekt (Drucker, printer object)



Darunter versteht man die Kombination eines Druckertreibers (Software) mit bestimmten Konfigurationseinstellungen.

Einem physischen Drucker können mehrere logische Druckerobjekte (mit unterschiedlichen Treibern und Konfigurationseinstellungen) zugeordnet werden; umgekehrt kann ein logisches Druckerobjekt mit mehreren physischen Druckern gleicher Bauart verknüpft werden ("Druckerpool").

Windows 10 verwendet sogenannte Typ 4 -Druckerklassentreiber. Diese sind in der Lage, sowohl 32 bit- als auch 64 bit-Plattformen zu unterstützen; häufig werden auch mehrere Druckermodelle vom Ausschnitt einer PostScript-Druckdatei: selben Druckertreiber unterstützt.

Um also von Windows aus drucken zu können, muss ein logisches Druckerobjekt /F0S53 F0 [83 0 0 -83 0 0] mFS eingerichtet werden. Dabei unterscheidet F0S53 Ji man grundsätzlich:

Lokale Drucker(objekte)



Lokale Druckerobjekte werden lokal erstellt. Sie werden in der lokalen Registrierdatenbank (Registry) des jeweiligen Rechners gespeichert.

Lokale Druckerobjekte müssen mit einem Treiber und Anschlussinformationen hinterlegt werden.

Es ist nicht zwingend nötig, dass der Drucker physisch mit dem PC verbunden ist;

so gelten auch Drucker mit eingebauter 59 46 28 46 46 46 oder Netzwerkkarte externer (umgangssprachlich auch als "Printserver" bezeichnet) als lokale Drucker.

Arten von Anschlüssen:

- Parallel (LPT1)
- Seriell (COM1)
- USB
- Netzwerkkarten mit IP-Adresse
- PDF-Drucker

Netzwerkdrucker(objekte)



Netzwerkdruckerobjekte verweisen zu freigegebenen lokalen Druckerobjekten, die auf einem anderen PC erstellt wurden.

Netzwerkdruckerobjekte müssen mit einem UNC-Pfad zur entsprechenden Freigabe hinterlegt werden, zum Beispiel \\server02\HPLaserJet.

13.1 Ablauf des Druckvorgangs

Wird ein Druckvorgang durchgeführt, so laufen dabei folgende Schritte ab:

1. Je nach installiertem Drucker wird eine Druckdatei erstellt. Diese Druckdatei kann zum Beispiel in den Druckersprachen PCL (Printer Control Language), PS (PostScript) oder HPGL (Hewlett Packard Graphics Language) geschrieben sein. Es handelt sich dabei immer um eine Textdatei, die Anweisungen an den jeweiligen Drucker enthält.

F /FO 0 /256 T /Helvetica mF

473 550 M (Dieser Text soll gedruckt werden.) 60 18 46 42 46 28 23 52 46 42 23 23 42 46 18 18 24 46 46 46 29 46 42 43 23 23

🚍 NPI510814 (HP LaserJet 400 colorMFP M475dn)							\times
<u>D</u> rucker Do <u>k</u> ument <u>A</u> nsicht							
Dokumentname	Status	Besitzer	Seiten	Größe	Gese	ndet	
🖬 Maurer_SB_4.jpg	Gedruckt	zahler	1/1	1,83 MB	07:32	2:51 02.04	4.2020
🖻 Maurer_SB_3.jpg	Gedruckt	zahler	1/1	1,80 MB	07:32	2:40 02.04	4.2020

0]xS 1708 550 M ()S 473 646 M ()S ΙH (%%[Page: 1]%%) = %%PageTrailer

2. Diese Druckdatei wird an den **Druckspooler** (Spool = Simultaneous Peripheral Operation On-Line, auch: Simultaneous Peripheral Output On-Line) weitergeleitet. Es handelt sich dabei um einen lokal operierenden Dienst, der Druckaufträge (englisch: Jobs) in Druckwarteschlangen (englisch: Queues) verwaltet.

Die Druckwarteschlangen können lokal vorhanden sein – oder, im Fall eines Druckservers - auch auf anderen Rechnern.

Wichtig: Für die Druckaufträge muss ausreichend Platz auf der Festplatte vorhanden sein (Druckaufträge können mehrere 100 MB groß werden, siehe Abbildung!).

In der Druckwarteschlangenverwaltung können Druckaufträge gelöscht werden, der Drucker "angehalten" werden (das bedeutet, der Spool-Vorgang wird unterbrochen).

	melden Wiederhenstellung Abhängigkeiten
Dienstname:	Spooled
Anzeigename	 Druckwarteschlange
Beschreibung	Dieser Dienst spoot Druckaufträge und verarbeitet Interaktionen mit dem Drucker. Wenn Sie diesen Dienst auserhalten krimmen Sie weder drucken
Pfad zur EXE C:\WINDOW	-Datel: (5\System32\spoolsv.exe
Starttyp:	Automatisch
	Wird ausgeführt
Sie können d wenn der Die	le Statparameter angeben, die übernommen werden sollen, nst von hier aus gestartet wird.

Abbildung: Eigenschaften des Dienstes Druckwarteschlange (Spooler)

<	
2 D	okument(e) in der Warteschlange

- - 3. in seinem Arbeitsspeicher unterbrin- stalliert und die Druckerobjekte erzeugt. gen kann.
 - 4. Der Drucker arbeitet die in seinem Arbeitsspeicher befindlichen Druckaufträge seitenweise (Laserdrucker) bzw. zeilenweise (Nadel-, Tintenstrahldrucker) ab. Nicht benötigte Druckinformationen werden gelöscht, sodass im RAM Platz für weitere Teile des Druckauftrags bzw. neue Druckaufträge geschaffen wird.

13.2 Einrichten eines lokalen Druckerobjekts

Die Verwaltung von Druckern und Scanner erfolgt über die Systemeinstellungen:

> Drucker & Scanner Systemeinstellungen

Standardmäßig gibt es drei Druckerobjekte, die der Treiberinstallation angezeigt: bereits installiert sind:

- Fax: Ermöglicht das Senden von Fax, falls eine Wählverbindung hergestellt werden kann
- Microsoft Print to PDF: Druckt ein Dokument nicht aus. sondern erstellt eine PDF-Datei (PDF = Portable Document Format). PDF ist ein geräteund systemunabhängiges Druckformat; PDF-Dokumente sehen auf allen Systemen gleich aus.
- Microsoft XPS Document Writer: Druckt ein Dokument nicht aus, sondern erstellt eine XPS-Datei (XPS = XML Paper Specification Format). XPS ist ähnlich wie PDF - ein formatstabiles Dateiformat von Microsoft.

Drucker & Scanner



Microsoft Print to PDF



Um ein Druckerobjekt hinzuzufügen, welchem einem physischen Druckgerät entspricht, gibt es zwei Möglichkeiten - über 2. Schritt: Wählen Sie den Druckerandie Systemeinstellungen oder über die Systemsteuerung.

Variante 1: Druckerhinzufügen in den Systemeinstellungen

Klicken Sie auf Drucker oder Scanner hinzufügen.

Drucker & Scanner hinzufügen



Drucker oder Scanner hinzufügen

Es startet folgender Assistent:

den angegebenen Drucker weiterge- geräte im Netzwerk zu finden. Dieser Vorleitet. Dabei kann der Drucker immer gang kann einige Zeit dauern. Wenn mögnur so viele Daten empfangen, wie er lich, werden die Treiber automatisch in-

> Aktualisieren ()

Drucker und Scanner werden gesucht

Nach einiger Zeit werden alle gefundenen Drucker im Netzwerk aufgelistet. Klicken Sie auf das Druckerobjekt und anschließend auf die Schaltfläche Gerät hinzufügen, damit der Druckertreiber installiert wird und ein logisches Druckerobjekt erzeugt wird.

HP LaserJet 400 colorMFP M475dn (5108 Drucker	14)
	Gerät hinzufügen
NPI510814 (HP LaserJet 400 colorMFP M47	'5dn)

Das Druckerobjekt wird nach Abschluss

ß	NPI510814 (HP LaserJet 400 colorMFP M475dn Bereit)
		App abru

Wenn Sie manuell ein neues Druckerobjekt hinzufügen möchten, dann klicken Sie auf den Link Der gewünschte Drucker ist nicht aufgelistet.

Der gewünschte Drucker ist nicht aufgelistet.

1. Schritt: Wählen Sie im ersten Dialogfeld des Assistenten Lokalen Drucker oder Netzwerkdrucker mit manuellen Einstellungen hinzufügen.

01	fein Drucker ist etwas älter. Ich benötige Hilfe bei der Suche.	
OF	inen Drucker im Verzeichnis anhand des Standorts oder der Druckerfeatures guchen	
0	reigegebenen Drucker über den Namen auswählen	
		Durchsuchen
	Beispiel: \\Computername\Druckername oder http://Computername/printers/Druckername/.printer	
0	lrucker unter Verwendung einer JCP/IP-Adresse oder eines Hostnamens hinzufügen	
0	juetooth-, Drahtlos- oder Netzwerkdrucker hinzufügen	
۹Ĩ	gkalen Drucker oder Netzwerkdrucker mit manuellen Einstellungen hinzufügen	

schluss aus oder erstellen Sie einen neuen Anschluss.

Einen Druckeranschluss auswählen		
Ein Druckeranschluss ist eine Verbindung, die o Drucker auszutauschen.	es dem Computer ermöglicht, Informatione	n mit einem
<u>V</u> orhandenen Anschluss verwenden:	LPT1: (Druckeranschluss)	Y
Neuen Anschluss erstellen:		
Arachlustyp:	HP Fax Port	

Folgende Anschlüsse sind bereits standardmäßig vorhanden:

• Parallele Anschlüsse (LPT1, ...): Früher der Standard-Druckeranschluss; erforderlich ist ein paralleles Kabel mit Centronics-Stecker.

- Die Druckdateien werden dann an Zunächst versucht Windows, neue Druck- Serielle Anschlüsse (COM1, ...): Wurde häufig für CAD-Plotter verwendet. Voraussetzung für das Funktionieren des Druckers ist die übereinstimmende Konfiguration der seriellen Schnittstellen auf PC und Drucker (zum Beispiel Übertragungsrate – 9600 bps).
 - Umleitung in Datei (FILE:): Die Druckdaten werden nicht an den Druckspooler gesendet, sondern in eine Druckdatei geschrieben (Dateierweiterung *.prn). Der Ausdruck selbst kann dann später bzw. auf einem nicht lokal vorhandenen Drucker erfolgen.
 - Umleitung in Datei (PORTPROMPT:) Dieser Port stellt den Nachfolger des lokalen FILE-Ports dar. Er wird genauso verwendet, unterstützt aber die neuen Tvp 4-Druckerklassentreiber. Der Drucker Microsoft Print to PDF verwendet diesen Port.
 - Dummy-Drucker (NUL:): Mit diesem Port wird der Druckauftrag "ins Nirvana umgeleitet". Man braucht diese Möglichkeit, wenn man möchte, dass der Druckvorgang zwar durchgeführt werden soll, aber weder eine Datei noch ein ausgedrucktes Blatt erwünscht ist, etwa in Lernprogrammen oder Prüfungstools.
 - TCP/IP-Anschlüsse: Diese werden gebraucht, wenn der Drucker über eine Netzwerkkarte verfügt, die mit dem Netzwerk verbunden ist. Sie müssen manuell erstellt werden; dies wird später erläutert.

3. Schritt: Auswählen des Druckertreibers

Den Druckertreiber installierer Wählen Sie Ihren Drucker in der Liste aus. Klicken Sie auf "Windows Update", um weitere Modelle anzuzeigen. Klicken Sie auf "Datenträger", um den Treiber mithilfe einer Installations-CD zu installieren

Hersteller	Drucker	^
Generic	hp business inkjet 1000	
HP	iii hp business inkjet 1200	
Microsoft	HP Business Inkjet 2200/2250 (HPA)	
	ID Rusiners Inkiel 2220/2280 LIDA	v
	٤	>
	Windows Update	Datenträger

4. Schritt: Drucker benennen

Geben Sie eine	en Druckernamen ein	
Druckername:	hp business inkjet 1000	

Nun werden die nötigen Treiber installiert. Der Installationsfortschritt wird angezeigt.

NPI510814 (HP LaserJet 400 colorMFP M475dn) wird installiert...



5. Schritt: Druckerfreigabe

Druckerfreigabe

Wenn dieser Drucker freigegeben werden soll, müssen Sie einen Freigabenamen angeben. Sie ko den vorgeschlagenen Namen verwenden oder einen neuen eingeben. Der Freigabename wird a Netzweckberutzern angezeigt.

Connectes These und	even .
O Drucker freigeben	damit andere Benutzer im Netzwerk ihn finden und verwenden können
Ereigsbenamm	hg business inkjet 1000
grandort:	
Earrimentary	

28

6. Schritt: Standarddrucker festlegen; **Testseite drucken**

Die Konfiguration als Standarddrucker ist insofern wesentlich, als viele Softwaretools grundsätzlich auf dem Standarddrucker auswählen (zum Beispiel wird bei der Druckerauswahl im Menü Datei - Drucken nur der Standarddrucker geändert!).



宿 Geräte und Drucker

Gerät hinzufügen

V Drucker (9)

Eine letzte Kontrolle des eingerichteten Druckers stellt die Testseite dar, die aus

- grafischen Informationen,
- Systemschrift-Texten und
- TrueType-Schrift-Texten

besteht. Überprüfen Sie speziell, ob diese drei Elemente korrekt dargestellt werden. Wenn nicht, sollten Sie einen anderen Druckertreiber wählen.

So sollte eine Drucker-Testseite aussehen: Dies ist notwendig, wenn der lokale Dru-

Der HP L1300-400 rolor	MEP M 875-M475 PCI. 6 words auf PCO4 notitig installent.	
PRINTER PROPERTI	5	
Sesender:	113103	
Datum:	29.01.2020	
Benutzemame	ZAHLERizahier	
Computername	PCH4	
Druckername:	HP-L130C-400 color MPP-M375-M475 PCL 6	
Druckermodel:	HP L1300-400 color MFP M375-M475 PCL 6	
Farbuntestützung	14	
Anochiussnamietro:	HPLaserJet800colorM7PM875cin	
Daterformat.	BADA	
Druckerfreigabename		
Druckenstandort		
Druckprozensor:	hotpp120	
Koninertal.		
Ort der Trennseiter.		
Betrieberystem.	Windows x64	
PRINT DRIVER PRO	PERTIES	
Tellamane	HP 12100-400 calor MPP M325-M475 PCL 6	
Detuer Type	Tex 3 - Benutzerroudus	
Telbenenint	61 130 9 12292	

Variante 2: Einrichten von Druckern über die Systemsteuerung

Klicken Sie in der Systemsteuerung auf den Bereich Hardware und Sound. Dort können Sie den Assistenten durch Klicken auf Gerät hinzufügen starten.



Hardware und Sound Geräte und Drucker anzeigen Gerät hinzufügen

Der Assistent führt durch denselben Konfigurationsprozess wie in den Systemeigenschaften.

Klickt man auf Geräte und Drucker anzeigen, so wird ein Fenster dargestellt, in welchem unter anderem alle installierten Druckerobjekte angezeigt werden. (Bild rechts oben)

13.3 Drucker entfernen

In den Systemeinstellungen navigieren Sie zum Bereich Drucker und Scanner, klicken in der angezeigten auf das Druckerobjekt, das Sie entfernen möchten, und klicken anschließend auf die Schaltfläche Gerät entfernen. Die Sicherheitsmeldung bestätigen Sie mit Ja.

Warteschlange öffnen Verwalten Gerät entfernen

→ · · · ↑ 🖓 « Hardware und Sound → Geräte und Drucker →

Drucker hinzufüger

Möchten Sie das Gerät wirklich entfernen?



13.4 Erzeugen eines TCP/IP-Druckeranschlusses

cker über eine eigene Netzwerkkarte bzw. über eine externe Netzwerkkarte (falsch auch als "Printserver" bezeichnet, etwas korrekter "Netport") verfügt.

Im Assistenten wählen Sie folgende Option:

Drucker unter Verwendung einer TCP/IP-Adresse oder eines Hostnamens hinzufügen

Einen Druckeranschluss auswähl Ein Druckeranschluss ist eine Verbindung, die es den Drucker auszutauschen. O Vorhandenen Anschluss ver Angebluster rd TCP/IP Port HP Fax Port AP Standard TCP/IP Port

Einen Druckerhostnamen oder eine IP-Adresse eingeber

Gerätetyp:	TCP/IP-Gerit:	
Hostname oder IP-Adresse:	192.18.3.21	
Anschlusspame:	192.18.3.21	

TCP/IP-Port erkennen

Erkennung des TCP/IP-Ports wird ausgeführt... Sobald die Erkennung ausgeführt wurde, wird auf die nächste Seite gewechselt.



Farbverwaltung Allgemein	Sicherheit Gerä Freigabe An	äteeinstellungen Info schlüsse Erweitert
HP LaserJ	et 4100 Series PCL6	
if folgenden Anscl ien und markierte Anschluss	nlüssen drucken. Die Dokun n Anschluss gedruckt. Beschreibung	nente werden auf dem ersten Drucker
EILE:	Ausgabe in Datei uml	
TS002	SBV13: PBN3	Microsoft XPS Document
TS001	SBV13: PBN4	HP Laserlet 4100 PCL 5 (u
10.1.103.13	Standard-TCP/IP-Port	HP LaserJet 4100 Series PC
10.1.104.13	Standard-TCP/IP-Port	
XPSPort:	Lokaler Anschluss	Microsoft XPS Document
	m	
<u>H</u> inzufügen	Löschen	Konfigurieren
Bidirektionale Un	erstützung aktivieren	
Druckernool aktiv	ieren	

13.5 Druckserver konfigurieren Schritt 1: Drucker freigeben

5 v

Eine Druckerfreigabe basiert auf denselben technischen Grundlagen wie Ordnerfreigaben. Als Freigabename muss ein NetBIOS-kompatibler Name verwendet werden, wenn die Integration mit älteren Betriebssystemen gewünscht wird.

NPI510814 (HP

LaserJet 400

olorMED

M475dn)

♀ "Geräte und Drucker" durchs...

Zunächst müssen die Freigabeoptionen des logischen Druckerobjekts geändert werden.

In den Windows-Einstellungen navigieren Sie in den Bereich Geräte und klicken auf Drucker und Scanner.



Geräte

Bluetooth, Drucker, Maus

Klicken Sie in der Druckerliste auf den freizugebenden Drucker; klicken Sie anschließend auf die Schaltfläche Verwalten.

HP LJ300-400 color MF	P M375-M475	PCL 6
Warteschlange öffnen	Verwalten	Gerät entfernen

Sie kommen nun zu einer eigenen Darstellung, in welcher Sie verschiedene Einstellungsmöglichkeiten für das Druckerobjekt vorfinden. Klicken Sie auf Druckereigenschaften.

Gerät verwalten	color MFP	M375-M475 PCL 6
Druckerstatus: Leerlauf		
Druckerwarteschlange öffnen	Als Standard	
Testseite drucken		
Problembehandlung ausführen		
Druckereigenschaften		
Druckeinstellungen		
Understand allow		

1. Schritt: Drucker freigeben

In der Kartekarte Freigabe aktivieren Sie das Kontrollkästchen Drucker freigeben; legen Sie einen Freigabename fest (es wird ein Vorschlag erstellt, den Sie auch unverändert übernehmen können).

SYSTEM.NE



auch als Druck-Server bezeichnet!

2. Schritt: Standortangabe und Kommentar

viele Drucker. Damit sie auch lokalisiert werden können, sollte man freigegebene Drucker mit einer Standort-Angabe und einem Kommentar versehen. Beim Standort-Eintrag sollten Sie eine Hierarchie berücksichtigen, mit Hilfe derer der Drucker wieder gefunden werden kann.

Sie dürfen keine Punkte bei der Standortangabe verwenden; Hierarchieebenen sind mit / zu trennen.

Farbverwaltur	ng	Sicherheit	Geräteeinstellungen	Info	
Allgemein		Freigabe	Anschlüsse	Erweitert	
S	HP L.	1300-400 color MF	P M375-M475 PCL 6		
stand <u>o</u> rt:	WIEN	I/GEB_A/113			
Kommentar: Stockwerksdrucker Gebäude A, 1. Stock, Raum 113					

Wenn Sie einen Druckserver konfiguriert haben (zur Erinnerung: das ist ein freigegebener Drucker), dann haben Sie zwei weitere Möglichkeiten:

• Veröffentlichung der Druckerfreigabe im Active Directory (nur in AD-Domänen möglich): Dazu muss überprüft werden, ob der Eintrag "Im Verzeichnis anzeigen" aktiviert ist (defaultmäßig ist er aktiviert).

Allgemein	Sicherheit Freigabe	Geräteeinstellungen Anschlüsse	Info Erweitert		
Sie könn gemeins der Com befindet	nen diesen Drucker m sam verwenden. Der l nputer ausgeschaltet :.	it anderen Benutzern im Drucker wird nicht verfü ist oder sich im Energie:	ı Netzwerk gbar sein, wenn ;parmodus		
✓ Drucker frei	geben				
Freigabename:	HP LJ300-40	HP LJ300-400 color MFP M375-M475 PCL 6			
	and thereit up a suf (laren		
✓ Druckauftra	gsaurbereitung aur c	lientcomputern durchfi	unien		

tomatisch eine administrative Freigabe

PRINT\$ erzeugt, die zu einem Ordner führt, in welchem passende Druckertreiber vorhanden sind. Bei der Installation eines Netzwerkdruckers können Client-PCs diese Treiber herunterladen, ohne das Druckermodell kennen zu müssen. Standardmäßig werden in diese Freigabe nur Treiber für Windows 2000/ XP/2003 gestellt; mit der Schaltfläche "Zusätzliche Treiber" können auch Treiber für ältere Windows-Plattformen in diese Freigabe gestellt werden.

Zusätzliche Trei	iber	×
Sie können zu: Systeme diese herunterladen	sätzliche Treiber installieren, damit Be Treiber bei der Verbindungsherstellu können.	enutzer folgender ng automatisch
Prozessor	Тур	Installiert
ARM64	Typ 3 - Benutzermodus	Nein
🗹 x64	Typ 3 - Benutzermodus	Ja
🗌 x86	Typ 3 - Benutzermodus	Nein

13.6 Druckerverwaltung

Um Drucker zu konfigurieren und Druckeinstellungen sowie Druckereigenschaften In einer größeren Organisation gibt es oft zu verwalten, rufen Sie in den Einstellun-

> 8 gen l den Bereich Geräte auf und klicken dann auf Drucker und Scanner.



Geräte Bluetooth, Drucker, Maus

Klicken Sie auf das entsprechende Druckerobjekt. Klicken Sie anschließend auf die Schaltfläche Verwalten.



13.6.1 Druckeinstellungen

Druckeinstellungen

In den Druckeinstellungen legen Sie fest, auf welche Art und Weise der Ausdruck erfolgen soll.

In der Registerkarte Erweiterte Optionen lassen sich noch weitere Parameter - abhängig vom verwendeten Druckermodell konfigurieren.



🖶 Druckeinstellun	gen für HP LJ300-400	color MFP M37	5-M475 P	CL 6				×
Enveiterte Optionen	Druckverknüpfungen	Papier/Qualtit	Effekte	Fertigstellung	Fabe	Dienste		
Eine Druckverknüp die mit einem einzei	fung ist eine Sammlung hen Klick angewendet w	gespeicherter Dru verden können.	ckeinstell	ungen,	E			
Verknüpfungen zur	n Drucken:							
Werkse	sinstellungen		^		1			
Algene	sines nomales Drucken		P	apierformate:		210 - 29	7 mm	
			1	4			\sim	
			P	apierquelle:				
Bielum	schlag		1	lutomatisch aus	wählen		\sim	
			P	apiersorte:				
T Karton	Schwer			licht bestimmt			\sim	
			B	eidseitiger Druck	k:			
88				lein			\sim	
	m		5	eiten pro Blatt:				
- WX			1	Seite pro Blatt			\sim	
Transp	arentfolie		E.	aboptionen:				
			v 1	abe			~	
Speichern unte	er Löschen	Zurücksetze	m					
Ø					info		Hife	
				04		hashee	Ohernah	-

13.6.2 Druckereigenschaften

Druckereigenschaften

Hier können Sie die Eigenschaften des Druckerobjekts bearbeiten.

Die Karteikarte Geräteeinstellungen enthält Konfigurationseinstellungen zu Papierschächten, Postscript-Optionen und Drucker-RAM.

Fativerwaltung Geräteeinstellungen Goräteeinstellungen Gorücker aute Man. Zufuhn Fach 1: A4 Fach 2: A4 Fach 2: A4 Fach 3: Nich M 3 Si Erstzungstabell	Sicherheit für HP LJ300- chen Papierfo m. Auswahl: in Fach 1: <u>A4</u> t verfügbar	Geräteeinste 400 color MFP N rmat und Ausga A4	ellungen 1375-M475 beschacht	Info PCL 6
Geräteeinstellungen Ducker auto Man. Zufuhr Fach 1: <u>A4</u> Fach 2: <u>A4</u> Fach 3: <u>Nich</u> B - <u>B</u> ³	für HP LJ300- chen Papierfo om. Auswahl: in Fach 1: <u>A4</u> t verfügbar	400 color MFP N rmat und Ausga A4	1375-M475 beschacht	PCL 6
Externe Schriftan installierbare Op Automatisch Druckerstatu Fach 3: <u>Nich</u> Modul für dı Manuellen b Druckerspeic Job-Trennvo	e für Schriftart ten tionen ne Konfiguratic sisbenachrichtig tinstalliert en beidseitigen Dristeitigen Dri eidseitigen Dri cher: <u>192 MB</u> rrichtung: <u>Dea</u>	en m: <u>Aus</u> gung: <u>Deaktivier</u> n Druck: <u>Installie</u> uck zulassen: <u>Ak</u> <u>ktiviert</u>	t rt tiviert	

In der Karteikarte "Erweitert" kann konfiguriert werden:

- Priorität der Druckaufträge (zwischen 1 und 99): Aufträge mit geringerer Priorität werden in der Druckwarteschlage nachgereiht und daher später gedruckt.
- Spooler umgehen: Hier kann der Druckauftrag direkt zum Drucker gesendet werden. Das hat den Nachteil, dass der Druckvorgang länger dauert, da der im Drucker vorhandene RAM meist zu klein ist, um den kompletten Druckauftrag zwischenzuspeichern. Deshalb muss gewartet werden, bis der komplette Druckauftrag zum Drucker gesendet wurde, bevor weitergearbeitet werden kann.

NET2V2EU



• Trennseite: Hier ist es möglich, eine Trennseite für Druckaufträge zu konfigurieren, auf der Informationen wie der Benutzername des Auftraggebers enthalten sind.

Trennseite		×
Trennseiten wer bestimmtes Dol finden.	den am Anfang eines Dokuments verwend rument einfacher zwischen anderen Ausdr	let, um ein ucken am Drucker zu
<u>T</u> rennseite:	C:\Windows\System32\pcl.sep	Durchsuchen
	ОК	Abbrechen

 Druckprozessor: Hier kann die Verarbeitung von Grafiken geändert werden. Die voreingestellte Konfiguration (WinPrint/ RAW) ist für viele Anwendungen ideal und muss nicht angepasst werden.

Druckprozessor	×
Die Auswahl eines anderen Druckprozes: Optionen für Standarddatentypen zur Ve kein Datentyp angegeben, so wird die fo	sors kann dazu führen, dass andere ıfügung stehen. Wird durch den Dienst Igende Auswahl verwendet.
Druckprozessor:	Standarddatentyp:
hpzppwn7 hpcpp120 winprint	RAW RAW [FF appended] RAW [FF auto] NTEMF 1.003 NT EMF 1.006 NT EMF 1.007 NT EMF 1.007 NT EMF 1.008 TEXT TEXT
	OK Abbrechen

Juni 2021

13.7 Einrichten eines Druckerpools

Unter einem Druckerpool versteht man mehrere gleichartige physische Drucker, So wie für Dateien und Ordner können die unter demselben Namen im Netzwerk angesprochen werden sollen. Es ist daher ein logisches Druckerobjekt zu erstellen, welchem zwei oder mehrere physische Für Drucker existieren spezielle Berechti-Drucker zugeordnet werden.

Drucker wie beschrieben zu installieren und dann die Eigenschaften des logischen • Dokumente verwalten (mit dieser Be-Druckerobjekts zu bearbeiten.

Zunächst muss ein zweiter Druckeranschluss hinzugefügt werden (da es sich in der Praxis meist um TCP/IP-Drucker han- • Drucker verwalten (damit können logidelt, sind in der Abbildung zwei TCP/IP-Ports dargestellt) (Bild links unten).

Danach muss die Einstellung "Druckerpool aktivieren" angekreuzt werden; beachten Sie, dass alle Anschlüsse, die zum Druckerpool gehören sollen, mit Kontrollkästchen aktiviert sein müssen!

13.8 Berechtigungen für logische Druckerobjekte

auch Berechtigungen für logische Druckerobjekte erstellt werden.

gungen:

- Dazu ist es nötig, zuerst einen der beiden Drucken (das muss nicht speziell erklärt werden)
 - rechtigung können Druckaufträge aus der Druckwarteschlange entfernt werden)
 - sche Druckerobjekte umkonfiguriert werden)

Standardmäßig hat nur die Spezial-Identität ERSTELLER-BESITZER die Berechtigung, Druckaufträge zu löschen. Das hat zur Folge, dass ein normaler Benutzer nur seine eigenen Druckaufträge aus der Warteschlange löschen kann, solange er nicht eine andere Drucker-Berechtigung bekommen hat (Bild rechts unten).

Eigenschaften von H	HP LaserJet 4050 Ser	ries PCL6	×	🖶 Eigenschaften von	HP LJ300-400 colo	r MFP M375-M475 PCL 6	×
Farbverwaltung Allgemein	Sicherheit Freigabe	Geräteeinstellungen Anschlüsse	Info Erweitert	Allgemein Farbverwaltung	Freigabe Sicherheit	Anschlüsse Geräteeinstellungen	Erweitert Info
Auf folgenden Anschlüdem ersten freien und	t 4050 Series PCL6 issen drucken. Die Do markierten Anschluss g	kumente werden auf	_	Gruppen- oder Benutze Gruppen- oder Benutze ALLE ANWENDU ERSTELLER-BE: Christian Zahler (z Administratoren (p	mamen: INGSPAKETE SITZER tahler@zahler.at) cc04\Administratoren)	
Anschluss COM3: COM4: FILE:	Beschreibung Serieller Anschlus Serieller Anschlus Ausgabe in Datei	Drucker	^			Hinzufügen	<u>E</u> ntfemen
 ✓ 192.168.3.21 Microsoft Docume 	Standard-TCP/IP e Local Port	-Port HP LaserJet 4050 S Microsoft Office Do	E	Berechtigungen für "Je	der"	Zulassen	Verweigem
XPSPort·	Lokaler Anschluse III	s Microsoft XPS Doci	•	Drucken Diesen Drucker verv	valten		
Hinzufügen	<u>L</u> öschen	Konfigurieren		Dokumente verwalte Spezielle Berechtigu	n ngen		
Bidirektionale Unter Druckerpool aktivie	stützung aktivieren ren			Klicken Sie auf "Erweit anzuzeigen.	ert", um spezielle Ber	rechtigungen	Er <u>w</u> eitert
		OK Abbrechen	Ü <u>b</u> ernehmen		[OK Abbrechen	0 <u>b</u> ernehmen

techold WIR BAUEN DEINEN PC

Nutze die langjährige Erfahrung der techbold Computer Experten für die perfekte Konfiguration deines PC-Systems. Egal ob Gaming Maschine, Office-PC oder Workstations für professionelle Anwendungen wie CAD, 3D Grafik und Videoschnitt – wir erstellen dir ein Angebot mit dem perfekten Preis-Leistungs-Verhältnis.

0

www.techbold.at/pc-zusammenstellen

BERATUNG

Umfangreicher Support von

zertifizierten Experten



QUALITÄT Ausschließlich geprüfte Markenkomponenten

-		_	
	-		
	_	_	1
1	_	Y	7

TESTS Jede Konfiguration wird umfangreich getestet



techbold

GARANTIE 3 Jahre Garantie auf alle individuellen PC-Systeme