Nr. **169**/Juni 2021 € 5,00 ISSN 1022-1611

QEWS

CLUBCOMPUTER · DIGITAL SOCIETY

P.b.b. 16Z040679 M ClubComputer, Siccardsburggasse 4/1/22 1100 Wien

CLUBSYSTEM

WINDOWS 10 TEIL 3

CC BY NC ND

Inhalt

LIESMICH

CLUBSYSTEM

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)

Franz Fiala

Autoren

***Fiala** Franz Dipl.-Ing. 1948* **1,2**

Präsident von ClubComputer, Leitung der Redaktion und des Verlags der PCNEWS, Lehrer für Nachrichtentechnik 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

office@zahler.at
http://www.zahler.at/

Inserenten

techbold **32**

techbold
Dresdner Straße 89 1200 Wien
+43 1 34 34 333
office@techbold.at
http://www.techbold.at

Produkte Reparatur, Aufrüstung, Softwareinstallation, Datenrettung. 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 Verleger **ClubComputer**
Siccardsburggasse 4/1/22 1100 Wien
01-6009933-11 FAX: -12
buero@clubcomputer.at
https://clubcomputer.at/
ZVR: 085514499
IBAN: AT74 1400 0177 1081 2896
Mitgliedsbeitrag 2019: 46,-Euro
Konto: AT74 1400 0177 1081 2896
oder
PayPal office@clubcomputer.at

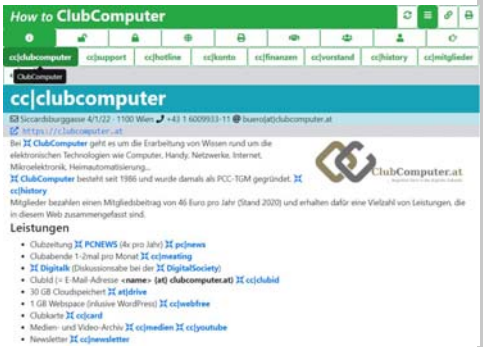
Digital Society
Graben 17/10 1010 Wien
01-314 22 33
info@DigiSociety.at
https://digisociety.at/
ZVR: 547238411
IBAN: AT45 3266 7000 0001 9315

Druck **Ultra Print**
Pluhová 49, SK-82103 Bratislava
http://www.ultraprint.eu/
Versand 16Z040679 M
PDF-Version http://d.pcnews.at/_pdf/n169.pdf

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

Services

http://buero.clubcomputer.at?svc=xx|yyy



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 🔗Link-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.

Verein

cc|clubcomputer · cc|finanzen · cc|history · cc|hotline · cc|konto · cc|mitglieder · cc|support · cc|vorstand ·

Öffentlich

at|wissen · cc|allapps · cc|exweb · cc|inhalte · cc|newsletter · cc|wapps · pc|123 · pc|pdf ·

Persönlich

at|asp · at|billing · at|domain · at|drive · at|ftp · at|mail · at|panel · at|php · at|press · at|server ·

Extern

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

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|digisociety · pc|mtm · pc|pcnews · pc|ultraprint ·

Wir

cc|calendar · cc|heuriger · cc|meating · cc|weihnacht · ds|digitalk ·

Du

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

Hilfe

cc|statuten · xx|hilfe · xx|links · xx|pages · xx|sitemap · xx|standorte ·

Windows 10 *Inhaltsverzeichnis*

Christian Zahler

Teil 1 *PCNEWS-167*

Teil 2 *PCNEWS-168*

Teil 3 *PCNEWS-169*

Teil 4 *PCNEWS-170*

9 Benutzerverwaltung

Christian Zahler

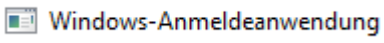
9.1 Ablauf des Anmeldevorgangs in Windows

Wenn Windows gestartet wird, so ist der erste Systemprozess, der im Benutzermodus 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; in dieser Sitzung laufen viele Systemprozesse, 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.



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

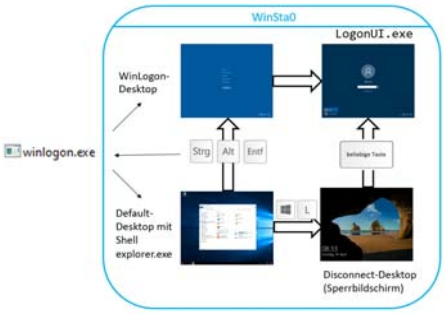
- Er erstellt eine Windows-Station mit dem Namen **WinSta0**. Eine Windows-Station repräsentierte eine „Sicherheitsgrenze“ und kann mehrere Desktops sowie eine Zwischenablage (clipboard) enthalten. In Benutzersitzungen gibt es nur diese eine Windows-Station.
- In dieser Windows-Station werden mehrere 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 wird angezeigt, wenn User Account Control-Abfragen durchgeführt werden.
- Er 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.
- 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 **`WinLogon`** den Prozess **`LogonUI`**; dieser Prozess hat die Aufgabe, Anmeldeinformationen von den Benutzern zu bekommen. LogonUI arbeitet mit den sogenannten **Anmeldeinformationsanbietern** (Credential Provider, CP) zusammen. Der Standard-CP von Windows unterstützt **Kennwörter** und **Smartcards**; Windows 10 enthält aber auch einen alternativen Anmeldeinformationsanbieter mit dem Namen **Windows Hello**, der biometrische Anmeldemöglichkeiten wie Fingerabdruck oder Gesichtserkennung unterstützt. Wenn LogonUI die Anmeldeinformationen bekommen hat, übergibt es diese Information an die LSA und wird beendet. (Anmerkung: Ältere Windows-Systeme verwendeten statt der CPs die sogenannte **GINA** = Graphical Identification and Authentication DLL; diese wird seit Windows Vista nicht mehr unterstützt.) Die installierten Credential Provider sind in der Registry aufgelistet:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers
  ```

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

Der Prozess **`WinInit`** führt ähnliche Vorgänge wie **`WinLogon` in der Sitzung 0** 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.

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

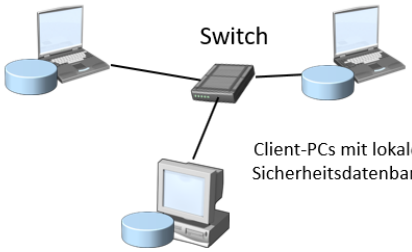


Der Grund für die Verwendung einer SAS besteht darin, Benutzer vor Programmen zu schützen, die den Anmeldeprozess simulieren und auf diese Weise Kennwörter abfangen können – Anwendungen, die im Benutzermodus laufen, können die SAS-Tastenfolge nicht abgreifen.

Immer, wenn eine Benutzeranmeldung erfolgen soll, so startet der WinLogon-Prozess dafür.

9.1.1 Arbeitsgruppenbetrieb

In einer Arbeitsgruppe (Workgroup) sind die Sicherheitsinformationen (also Benutzername und Kennwort) in einer lokalen Datenbank (Fachausdruck: SAM, Security Account Manager) auf jedem Rechner gespeichert:



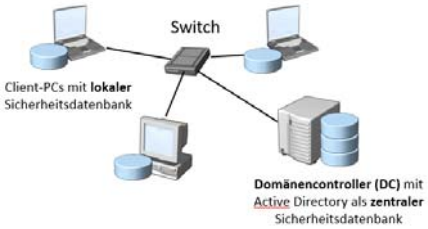
Sie können sich hier nur lokal anmelden. Es reicht, den jeweiligen Benutzernamen als Anmeldenamen zu verwenden.

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

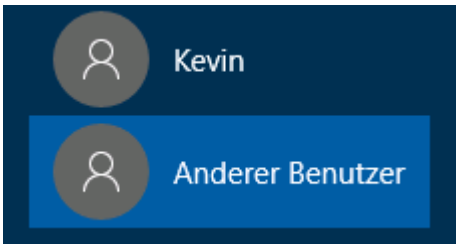
In einer Domäne existiert zusätzlich zu den lokalen Sicherheitsdatenbanken eine zentrale, leistungsfähige Sicherheitsdatenbank (Fachausdruck: Active Directory, AD) auf einem speziellen Server-PC, der als Domänencontroller (DC) bezeichnet wird.



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

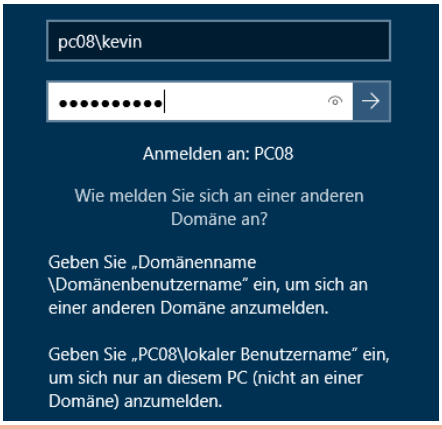
- Nach wie vor eine **lokale Anmeldung** an Ihrem PC. Damit können Sie nur lokal arbeiten. Ein Zugriff auf benötigte Dateien und Programme im Netzwerk ist nicht möglich.
- Eine **Anmeldung an der Domäne**: Hier überprüft der Domänencontroller, ob Sie Ihren Namen und Ihr Kennwort korrekt eingegeben haben. 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 eine Domänenanmeldung durchführen wollen:

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

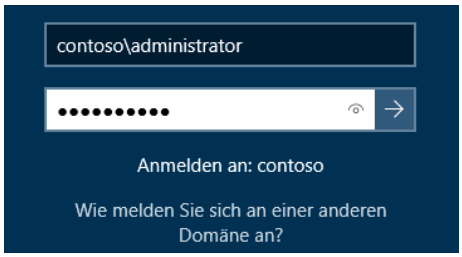


Eine lokale Anmeldung bewirkt, dass Sie auf Ressourcen in der Domäne **nicht zugreifen** können!

- **Domänenanmeldung:** Hier bestehen 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



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

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 **NetBIOS-Domänenname\Benutzername** gewählt werden.

9.2 Arten von Benutzerkonten

Die Anmeldedaten der Benutzer sind standardmäßig in Sicherheitsdatenbanken gespeichert.

- **Microsoft-Konten**: Diese Konten sind 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.

Vordefinierte Konten:

- 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 Single-sign-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.

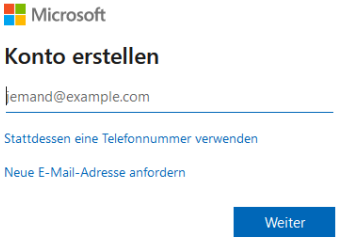
Viele Personen haben bereits ein Microsoft-Konto, ohne dass es ihnen bewusst ist:

- 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.
- XBox-Konto
- 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

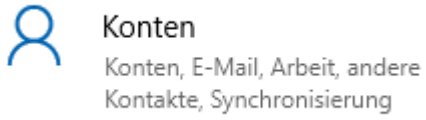
Sie können dabei Ihre gewohnte E-Mail-Adresse eintragen und diese als Microsoft-Kontonamen verwenden.



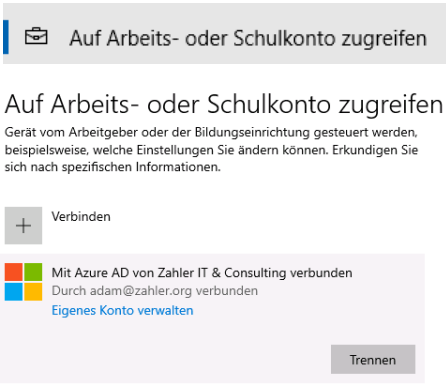
9.2.2 Microsoft Azure AD-Konto (Office 365-Konto)

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**.



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



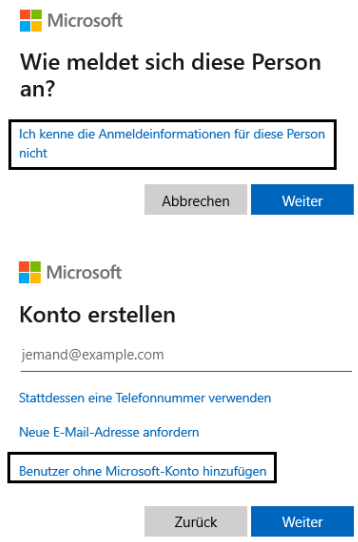
AzureAD-Konten kann man auch mit der Command Shell-Anweisung **whoami** identifizieren:

```
C:\>whoami
C:\>azuread\heinrichadam
```

9.2.3 Lokales Benutzerkonto

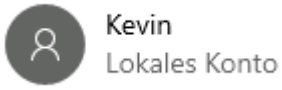
Es ist nach wie vor möglich, auch ein lokales Benutzerkonto zu erstellen, obwohl diese Möglichkeit nicht mehr empfohlen wird.

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



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).

Das neue lokale Konto wird nun angezeigt:

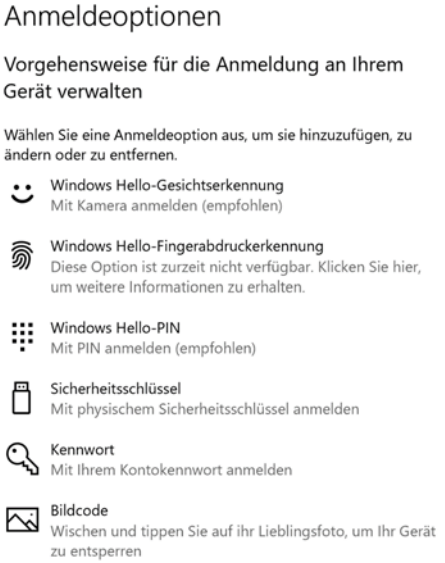


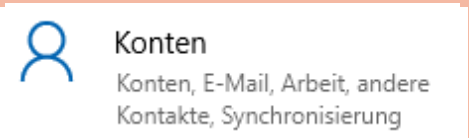
9.3 Anmeldeoptionen und Windows Hello

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**.





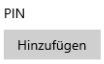
Die verfügbaren Optionen können sich von Gerät zu Gerät unterscheiden.

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.)

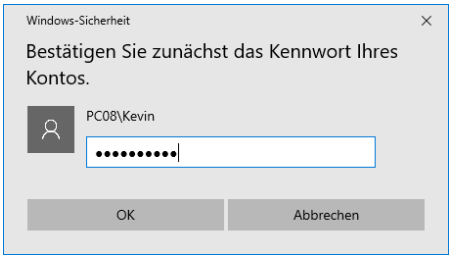
9.3.1 Windows Hello-PIN einrichten

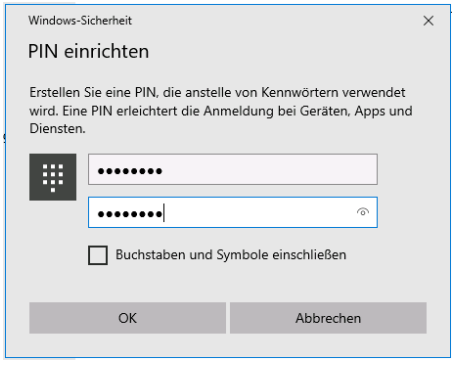
Sinn: Der PIN ist nur Anmeldung an dem PC gültig, an welchem er erstellt wurde (Unterschied zum Kennwort!).

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



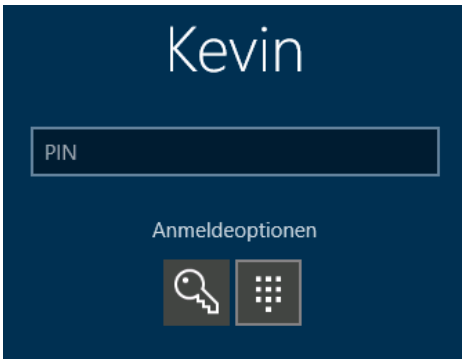
Es ist möglich, für einen angemeldeten Benutzer die Anmeldung mittels PIN zu aktivieren. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**.





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

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

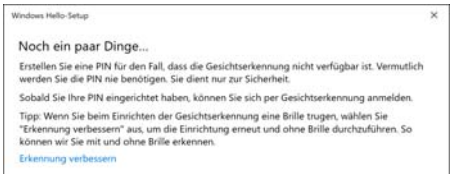


Hinweis: Aus Sicherheitsgründen ist eine Remote Desktop-Anmeldung mit PIN nicht möglich!

9.3.2 Windows Hello-Gesichtserkennung

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

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.



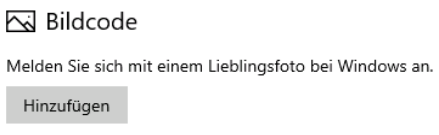
Klicken Sie auf **PIN einrichten**, um die PIN zu konfigurieren.

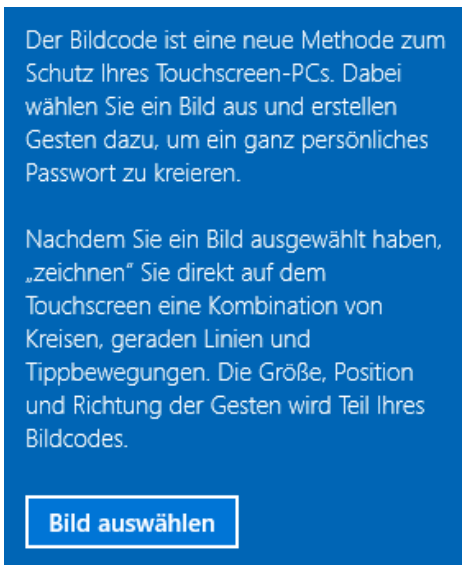
9.3.3 Windows Hello-Fingerabdruckerkennung

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.





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

Windows kann Geräte verwenden, die mit Ihrem PC gekoppelt sind, um zu erkennen, ob Sie Ihren Arbeitsplatz verlassen haben, und Ihren PC sperren, kurz nachdem Ihr gekoppeltes Gerät außerhalb der Bluetooth-Reichweite ist. Dies verhindert, dass Personen Ihr Gerät verwenden können, wenn Sie sich von Ihrem PC entfernen und vergessen, ihn zu sperren.

9.4 Security Principals

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

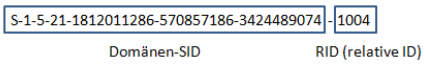
Zu den wichtigsten Security Principals zählen:

- Benutzerkonten
- Computerkonten
- Gruppenkonten
- Dienste

Benutzer-, Computer- und Gruppenkonten 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".



- **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 `PsGetSID` angezeigt werden (Download unter http://www.microsoft.com/technet/sysinternals/utilities/psgetsid.mspx).

Andere Möglichkeiten:

```
wmic useraccount where name="Benutzername" get sid
whoami /user
```

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

Auswahl wichtiger Spezialidentitäten:

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.

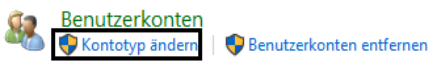
Wenn Betriebssystemdateien gelöscht werden müssen, so muss zunächst der Besitz übernommen werden, dann ein Berechtigungseintrag neu erstellt werden, der die Löschberechtigungen erteilt.

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

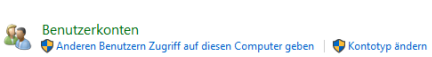
Navigieren Sie in der Systemsteuerung in den Bereich **Benutzerkonten** und klicken Sie auf **Kontotyp ändern**.



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

9.5.2 Vorgangsweise im Domänenbetrieb

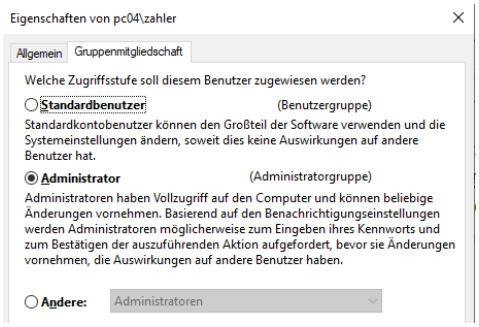
Im Domänenbetrieb sind die Einstellungen auch in der Systemsteuerung im Bereich **Benutzerkonten** zu verwalten, die Oberfläche sieht aber etwas anders aus.

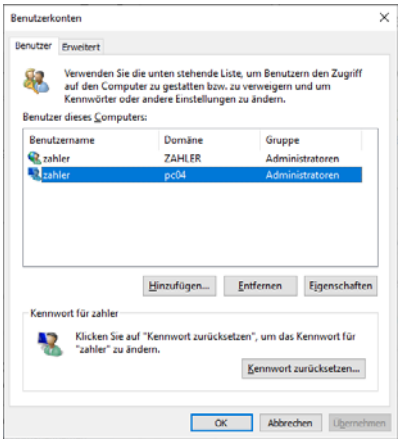


Sie können wieder auf Kontotyp ändern klicken; allerdings wird dann ein Dialogfeld mit zwei Registerkarten angezeigt.

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 Objekt 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 angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-2	Network (Netzwerk)	Gruppe, die alle Benutzer enthält, die sich über eine Netzwerkverbindung angemeldet 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 Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-9	Enterprise Domain Controllers (Domänencontroller der Organisation)	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 Self (Selbstprinzipal)	Platzhalter in einem vererbbaren ACE-Eintrag für ein Konto- oder Gruppenobjekt im Active Directory. Wenn der ACE-Eintrag geerbt wird, ersetzt das System diesen 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 authentifiziert wurden. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-13	Terminal Server Users (Terminalserverbenutzer)	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 Administratorengruppe 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.





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.

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.

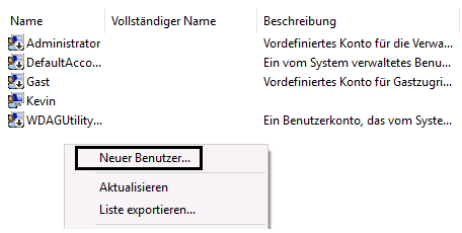
In ähnlicher Form sind Windows-Anmeldeinformationen einsehbar.

9.7 Benutzerverwaltung lokaler Benutzer in der Computerverwaltung

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

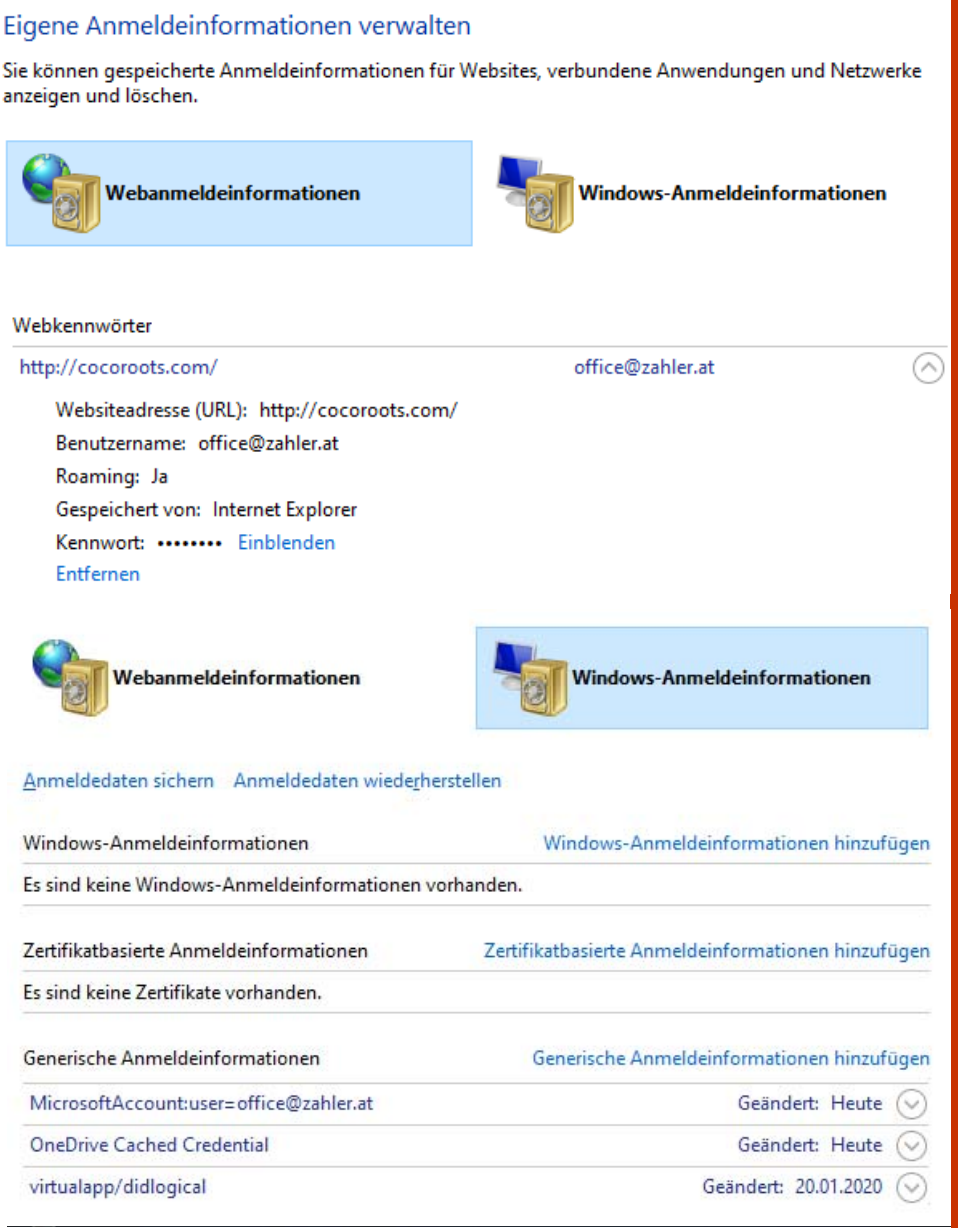
Navigieren Sie innerhalb der Rubrik **System** zum Bereich **Lokale Benutzer und Gruppen**.

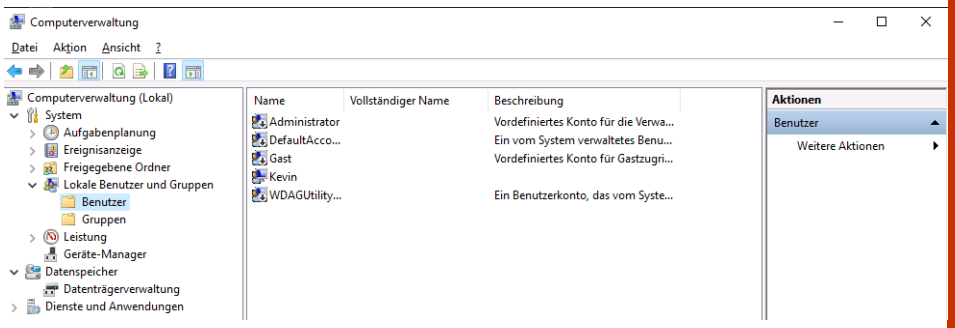
Um einen neuen lokalen Benutzer anzulegen, klicken Sie mit der rechten Maustaste in einen freien Bereich und wählen den Kontextmenüeintrag **Neuer Benutzer…**:



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

Vermeiden Sie Sonderzeichen für den Benutzernamen.





Verboten sind:

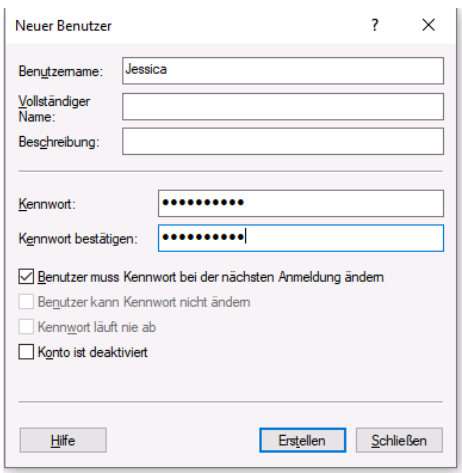
```
" / | \ < > ? * = [ ] : ;
```

Der Benutzername ist nicht case-sensitiv, beim Passwort wird allerdings Groß- und Kleinschreibung unterschieden.

Kennwörter können bis zu 128 Zeichen lang sein.

Bei der lokalen Anmeldung überprüft die „Local Security Authority“ (LSA), ob Benutzername und Kennwort mit einem in der SAM-Datenbank gespeicherten Datensatz übereinstimmen. Wenn ja, wird die Anmeldung durchgeführt.

Hinweis: Aus eigenem Interesse sollten Sie als Administrator die Option **Benutzer**



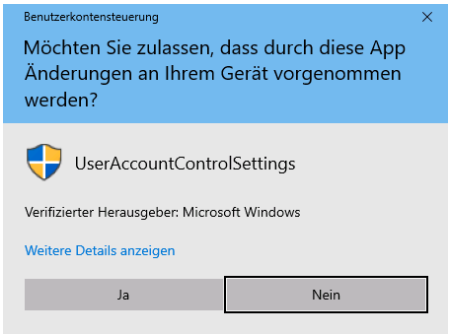
muss Kennwort bei der nächsten Anmeldung ändern aktivieren; es ist nicht förderlich und entspricht auch nicht der gängigen Security-Praxis, wenn der Systemadministrator die Kennwörter aller Benutzer weiß!

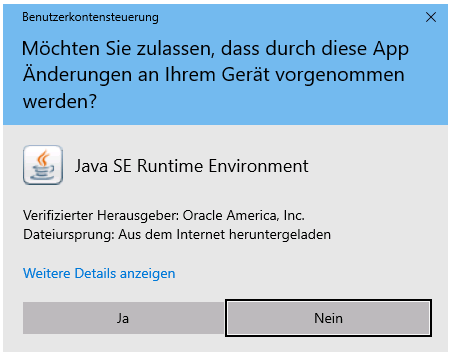
Das neue Konto wird nun in der Benutzerliste angezeigt.

9.8 UAC (Benutzerkontosteuerung, User Account Control)

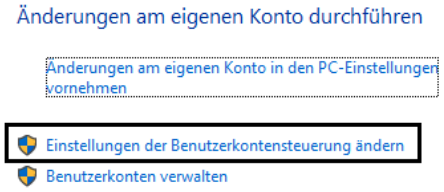
Die Benutzerkontosteuerung ermöglicht eine Abwägung zwischen der Flexibilität und dem Berechtigungsumfang eines Administratorkontos und der Sicherheit eines Standardbenutzerkontos.

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.



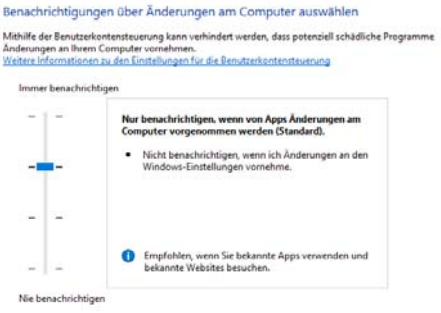


In Windows 10 kann das Verhalten der Benutzerkontosteuerung fein abgestimmt werden. Öffnen Sie dazu die Systemsteuerung und navigieren Sie in den Bereich **Benutzerkonten**.



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



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, können Sie für Ihre Kinder Standardbenutzerkonten 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

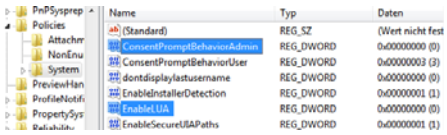
Über die Registry kann das Standardverhalten der UAC für Administratoren und für Standardbenutzer konfiguriert werden.

Im Schlüssel

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

befinden sich drei dafür vorgesehene Einträge vom Typ REG_DWORD:

- ConsentPromptBehaviorAdmin (Standardwert 5)
- ConsentPromptBehaviorUser (Standardwert 3)
- EnableLUA (Standardwert 1)



Die beiden ConsentPromptBehavior-Einträge können folgende Werte annehmen:

0 Keine Aufforderungen mehr seitens der Benutzerkontensteuerung - alle Programme werden mit höheren Rechten ausgeführt

5 „Lockerste“ Einstellung

2 „Strengste“ Einstellung

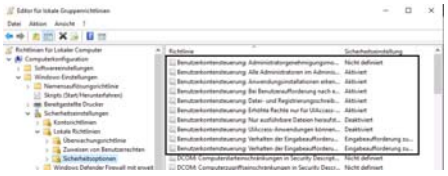
Der Wert EnableLUA muss auf 0 gesetzt werden, um die UAC auszuschalten.

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 / Sicherheitseinstellungen / Lokale Richtlinien / Sicherheitsoptionen.



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.

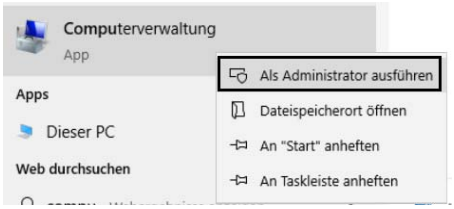
Um ein Programmfenster mit geändertem Benutzerkontext zu erstellen, gibt es folgende Möglichkeiten:

(a) Über die grafische Oberfläche:

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

und wählen Sie aus dem Kontextmenü den Eintrag **Als Administrator ausführen**.

Sie werden dann nach Anmeldeinformationen für ein Konto mit administrativen Berechtigungen gefragt.

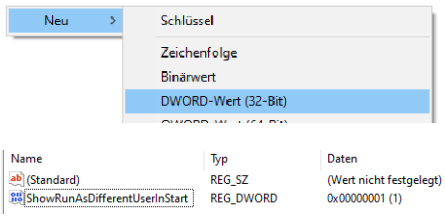


Die bisher vorhandene Möglichkeit, ein Programm im Kontext eines nicht-administrativen Benutzers auszuführen, steht in Windows 10 standardmäßig nicht zur Verfügung.

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):

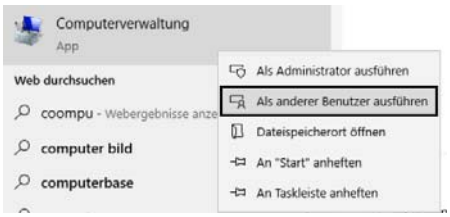
```
\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer
```

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.



(b) Über die Command Shell

Mit dem Befehl runas kann ein Programm 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 nicht-administratives Konto an, so gelten die Berechtigungen dieses Kontos, und zwar nur für dieses eine Programmfenster.

Der Parameter **/noprofile** bewirkt, dass das Benutzerprofil des Administrators 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 Druckerverbindungen sowie weitere festgelegte Einstellungen. 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:

- Die Datei NTUSER.DAT stellt einen Teil der Registry dar und enthält benutzerdefinierte Systemeinstellungen.
- Eine Reihe von Ordnern enthalten benutzerdefinierte Dateien; bekannt sind etwa die Ordner „Dokumente“ oder „Desktop“.

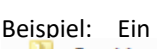
Das Profil „Default“ stellt eine Vorlage dar, die beim erstmaligen Anmelden eines Benutzers kopiert wird und den Ausgangsstatus für das neue Benutzerprofil bildet.

Das Profil „All Users“ gibt es eigentlich nicht mehr; es stellt nur mehr einen System-Link zum Verzeichnis C:\ProgramData dar. Dieses Verzeichnis enthält die Startmenüdateien für „alle Benutzer“ in folgendem Pfad:

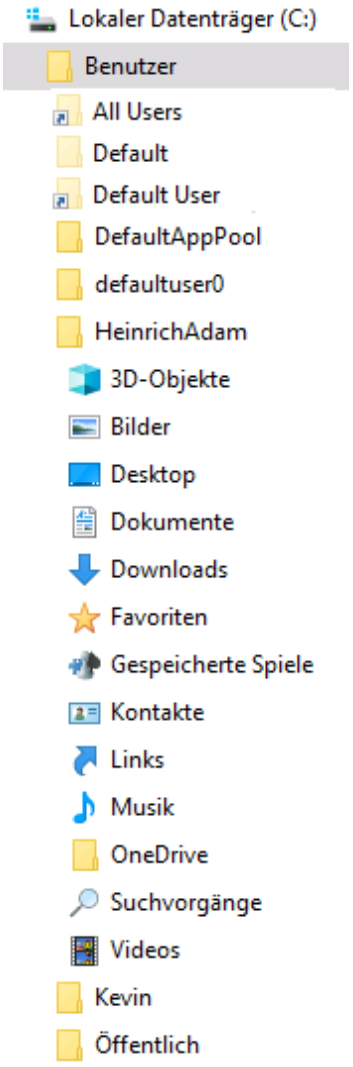
```
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
```

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 meisten Fällen nicht direkt zugegriffen werden.

Hinweis: Junctions werden nur sichtbar, wenn in den Ordneroptionen in der Karteikarte „Ansicht“ die Einstellung „Geschützte Systemdateien ausblenden“ deaktiviert wird.

Beispiel: Ein Klick auf den Verweis 

führt zur Meldung:



Um nun herauszufinden, auf welchen Ordner eine Verbindung zeigt, kann der Command-Shell-Befehl dir /a verwendet werden:

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

 Verzeichnis von c:\Users

04.04.2020  08:04    <DIR>          .
04.04.2020  08:04    <DIR>          ..
30.08.2019  07:31    <DIR>          administrator
30.08.2019  07:30    <DIR>          alexander
19.03.2019  07:02    <SYMLINKD>     All Users [C:\ProgramData]
30.08.2019  07:35    <DIR>          Default
19.03.2019  07:02    <JUNCTION>     Default User [C:\Users\Default]
19.03.2019  06:49               174 desktop.ini
30.08.2019  08:25    <DIR>          Public
04.04.2020  08:04    <DIR>          raphaela
26.03.2020  09:06    <DIR>          zahler.ZAHLER
               1 Datei(en),            174 Bytes
              11 Verzeichnis(se), 26.581.475.328 Bytes frei
```

Beachten Sie die Kennzeichnung des "All Users"-Profils als System-Link!

```
C:\Users\Christian>dir /a
 Volume in Laufwerk C: hat keine Bezeichnung.
 Volumeseriennummer: 7448-CE17
 Verzeichnis von C:\Users\Christian
11.06.2009  09:16    <DIR>          .
11.06.2009  09:16    <DIR>          ..
26.05.2009  11:04    <VERBINDUNG>   Anwendungsdaten
[C:\Users\Christian\AppData\Roaming]
26.05.2009  11:04    <DIR>          AppData
26.05.2009  11:05    <DIR>          Contacts
26.05.2009  11:04    <VERBINDUNG>   Cookies
[C:\Users\Christian\AppData\Roaming\
Microsoft\Windows\Cookies]
12.06.2009  16:58    <DIR>          Desktop
12.06.2009  16:55    <DIR>          Documents
26.05.2009  11:49    <DIR>          Downloads
26.05.2009  11:04    <VERBINDUNG>   Druckumgebung
[C:\Users\Christian\AppData\Ro
aming\Microsoft\Windows\Printer Shortcuts]
26.05.2009  11:04    <VERBINDUNG>   Eigene Dateien
[C:\Users\Christian\Documents]
```

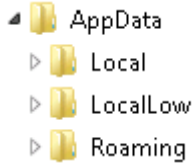
Hier sehen Sie, dass es sich beim Ordner Cookies um eine Verbindung (Junction) auf den tatsächlich existierenden Ordner

CLUBSYSTEM.NET

C:\Users\Christian\AppData\Roaming\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.
- **Ordner „Documents“, „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.

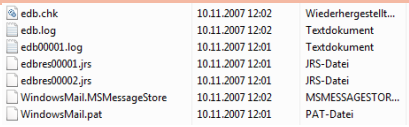


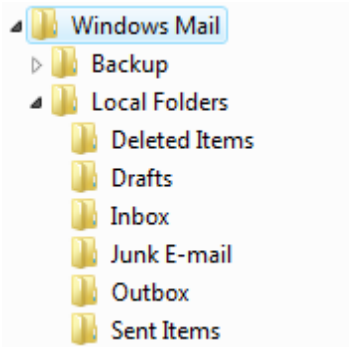
  - Der Ordner „Local“ enthält lokal gespeicherte Informationen.
  - Der Ordner „LocalLow“
  - Der Ordner „Roaming“ enthält die servergespeicherten Anteile des Profils.
- Ordner **„AppData\Local\Microsoft“:** In diesem Ordner sind unter anderem auch die lokalen Mail-Datenbanken gespeichert, die alle eingegangenen 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

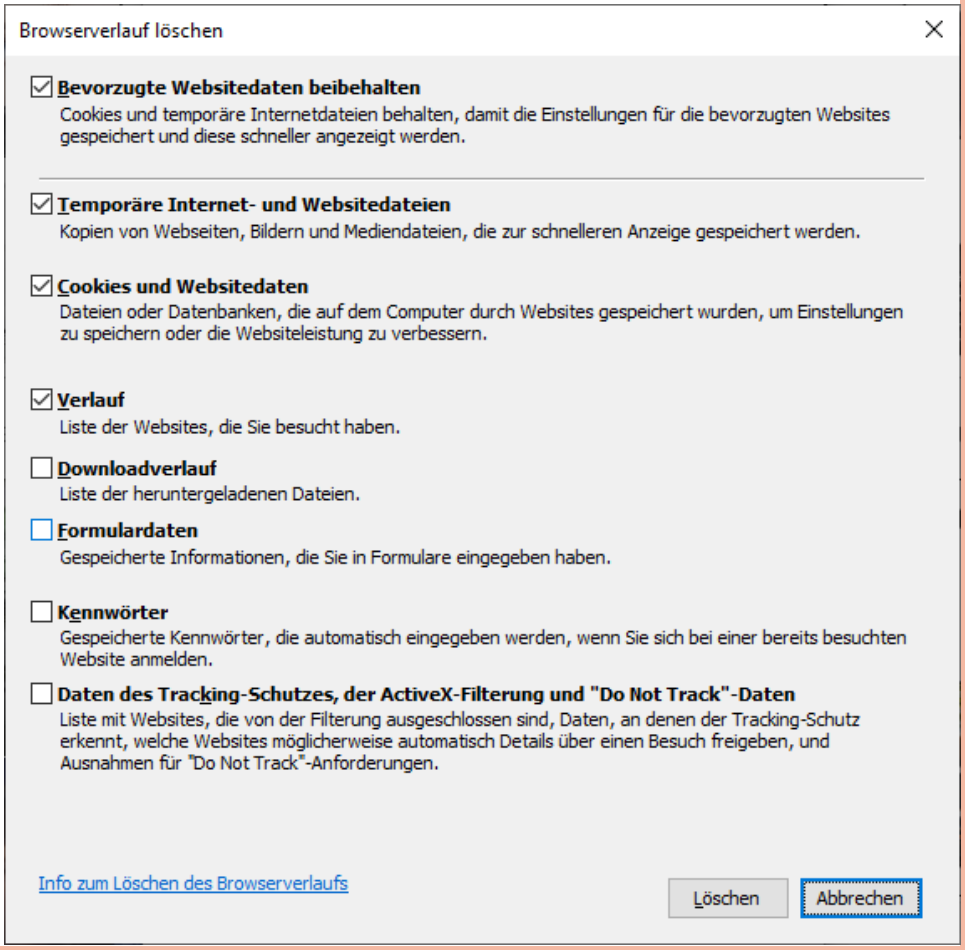
  *.ost-Dateien: Offline-Cache; enthält heruntergeladene, zwischengespeicherte E-Mails und andere Outlook-Elemente

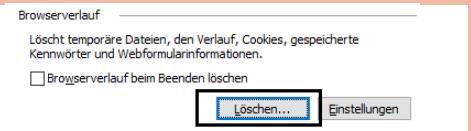
- **Windows Mail – Ordner „AppData\Local\Microsoft\Windows Mail“:** Von Windows Mail wird eine komplette Ordnerstruktur erzeugt. Die Nachrichten landen im Windows.MSMessageStore, werden aber innerhalb der einzelnen Mailordner (etwa „Inbox“) noch einmal als *.eml (E-Mail-Datei) angezeigt.





- **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.
- **Ordner „AppData\Local\Microsoft\Windows\INetCache“:** 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.

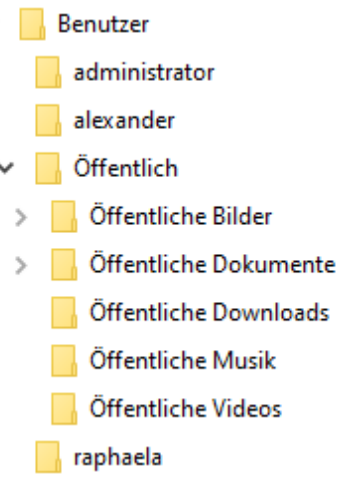
- **Ordner „AppData\Local\Microsoft\Windows\History“** (Verlauf): Hier speichert der Internet Explorer Links zu besuchten Websites.
- **Ordner „AppData\Roaming\Microsoft\Windows\Start Menu“** (Startmenü): Dieser Ordner enthält Verknüpfungen zu Programmen, die im Startmenü – zusammengefasst in Gruppen – angezeigt werden.
- **Ordner „AppData\Roaming\Microsoft\Windows\Recent“** (Zuletzt verwendete Dokumente)**:** Dieser Ordner enthält Verknüpfungen zu Dokumenten und Ordnern,

die in der letzten Zeit vom Benutzer verwendet wurden. Diese Verknüpfungen werden an der entsprechenden Stelle im Startmenü angezeigt.

Typen von Benutzerprofilen

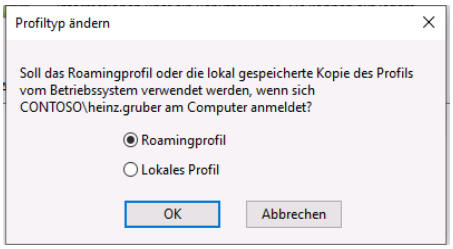
- **Lokales Benutzerprofil:** Das lokale Benutzerprofil wird beim ersten Anmelden bei einem Computer erstellt und auf der lokalen Festplatte des betreffenden Computers gespeichert. Sämtliche Änderungen an Ihrem lokalen Benutzerprofil sind nur für den Computer wirksam, auf dem die Änderungen vorgenommen 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 NTUSER.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 "Super-mandatory 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!

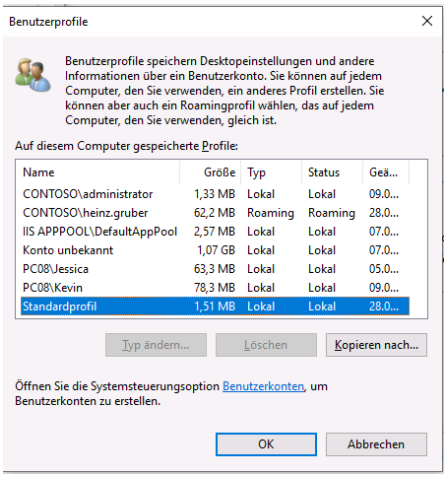
Kopieren von Benutzerprofilen: Benutzerprofile können dupliziert und lokal gelöscht werden; dafür steht das Dialogfeld „Systemeigenschaften“ zur Verfügung



(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!).





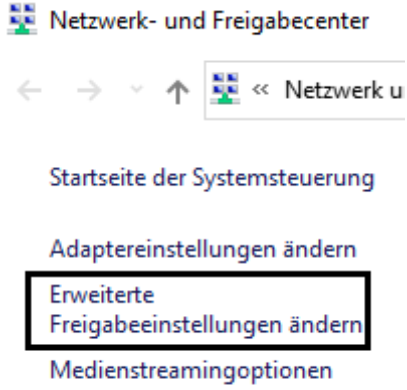
9.11 Öffentliche Ordner

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

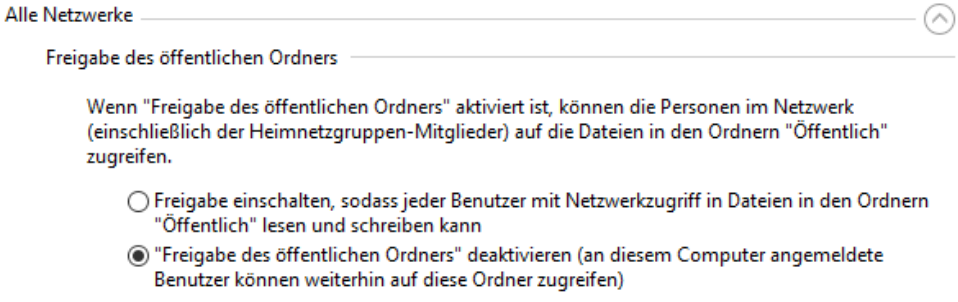
Die in diesem Profil enthaltenen Daten stehen allen Benutzern zur Verfügung, die lokal auf diesem PC arbeiten.

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.



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.



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:

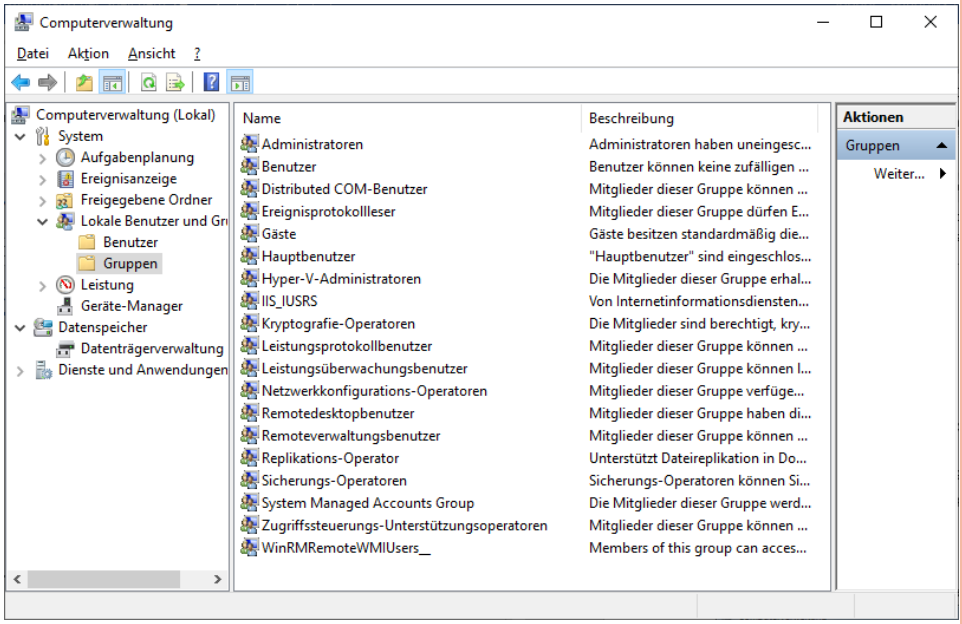
- Lokale Benutzerkonten
- Lokal verfügbare integrierte Sicherheitsprinzipale (Jeder, Authentifizierte Benutzer, …)
- Globale bzw. Universelle Gruppen im Active Directory (Voraussetzung: Computer ist Domänenmitglied)

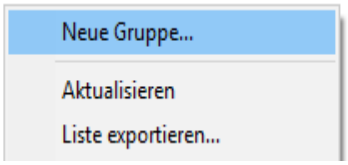
Lokale Gruppen können daher keine anderen benutzerdefinierten Lokalen Gruppen enthalten.

Anlegen von lokalen Gruppen

Öffnen Sie das MMC-Snap-In **Computerverwaltung**. Navigieren Sie in der linken Spalte zum Punkt System – Lokale Benutzer und Gruppen – Lokale Gruppen.

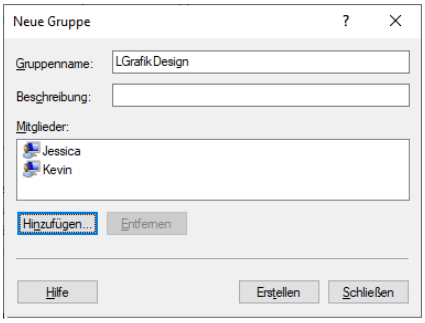
Klicken Sie mit der rechten Maustaste in den freien Bereich und wählen Sie im Kontextmenü **Neue Gruppe**.



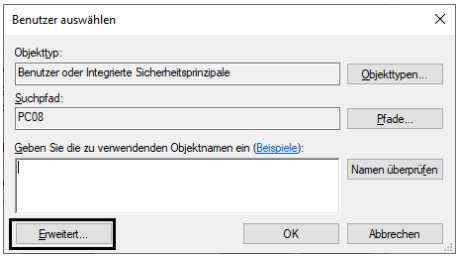


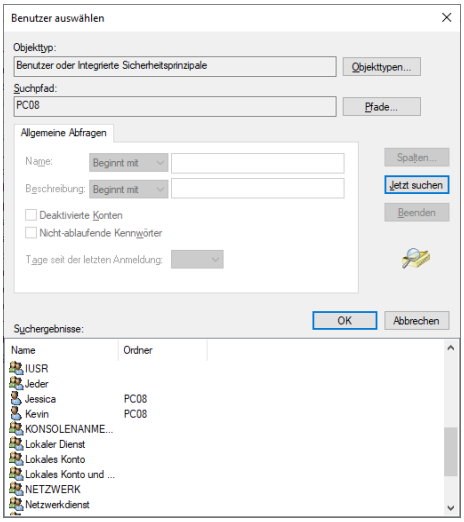
Legen Sie den Namen der lokalen Gruppe fest.

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.

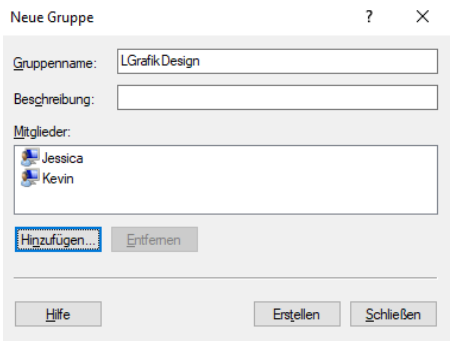


Zum Auswählen von Benutzerkonten, die Mitglieder der lokalen Gruppe werden sollen, klicken Sie auf **Hinzufügen**.

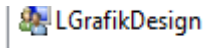




Wählen Sie alle Benutzerkonten aus, die Mitglied bei der lokalen Gruppe werden sollen, und klicken Sie dann auf **OK**. Die neu hinzugefügten Mitglieder werden nun angezeigt:



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



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 NTFS-Berechtigungen wird als **DACL (Discretionary Access Control List)** bezeichnet; die einzelnen Einträge heißen 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:

- Lesen und Ausführen: beinhaltet die Lese-Berechtigung
- Ändern = Lesen + Ausführen + Schreiben
- Vollzugriff = alles (inkl. Besitzrechte 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:

✓ Diese Berechtigungen wurden vom 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.

Man kann nicht eine ererbte positive Berechtigung entziehen („wegklicken“), aber man kann negative Berechtigungen („verweigern“) setzen!

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.

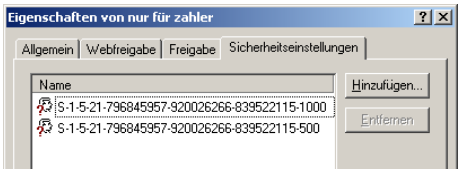
Beispiel: Auf die Datei Projektdoku.xlsx haben folgende Gruppen Zugriffsberechtigungen:

- Administratoren: Vollzugriff
- 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 unsichtbaren) SIDs angezeigt werden.



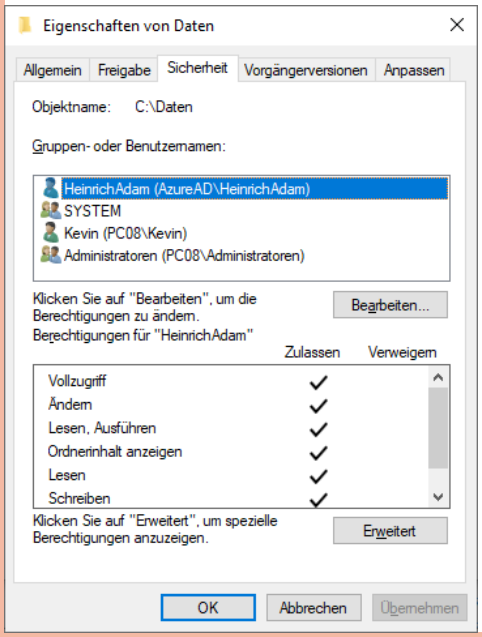
Mögliche Ursachen dafür:

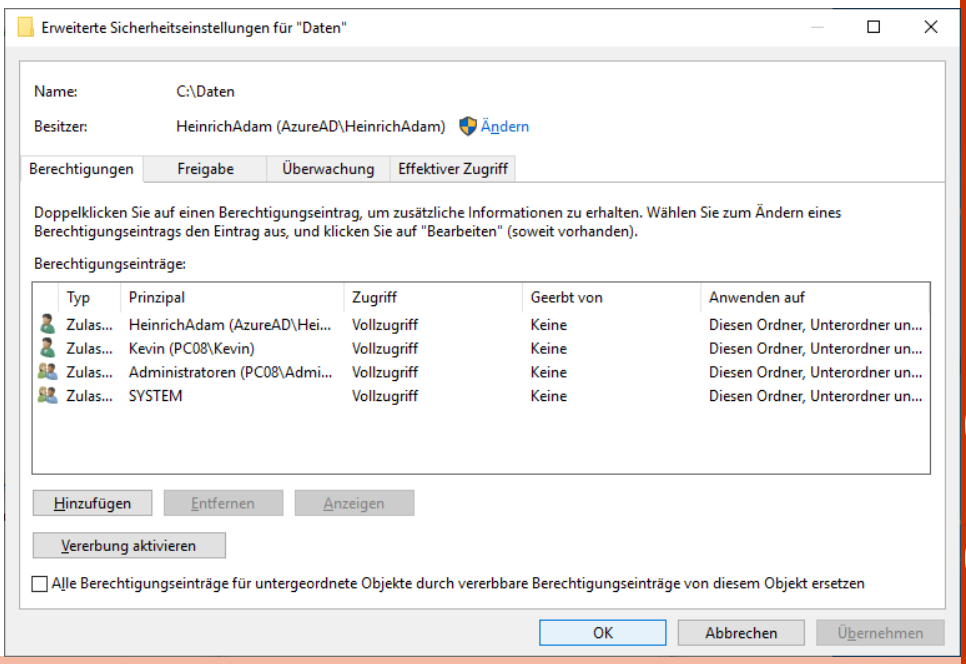
- Das ursprüngliche Benutzerkonto wurde in der Datenbank gelöscht, die Berechtigungen aber noch nicht
- Domain Controller ist momentan nicht erreichbar, der Kontoname kann daher nicht aufgelöst werden
- Infrastrukturmaster in der Domäne arbeitet nicht oder ist nicht erreichbar (möglicherweise auf Grund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

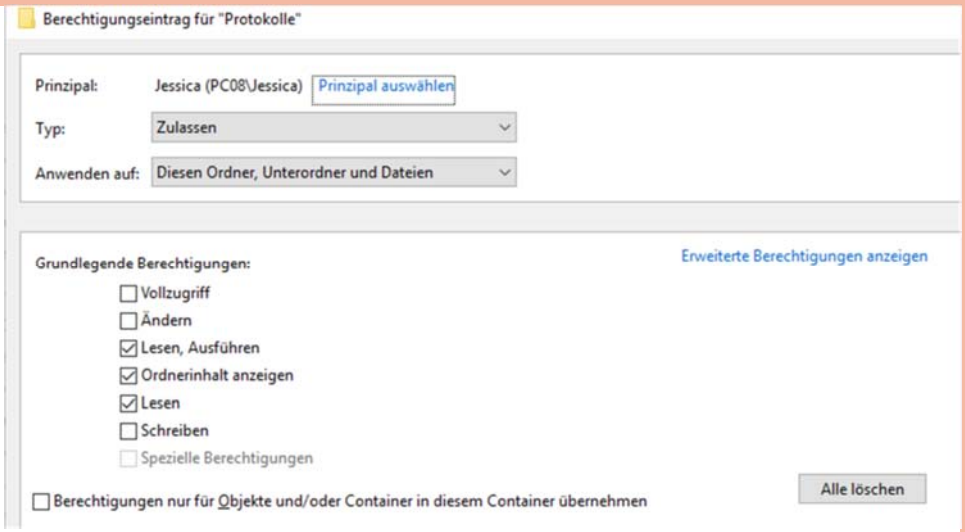
Man kann allerdings diese Vererbung blockieren und die Berechtigungen neu festlegen. Dazu klickt man auf die Schaltfläche



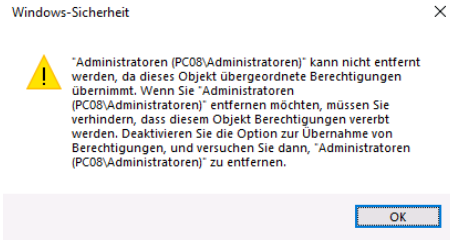


„Erweitert“, in der nun folgenden Ansicht auf „Bearbeiten“:

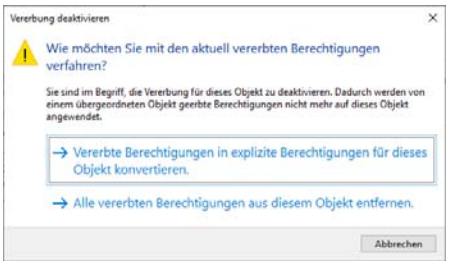
Die Schaltfläche **Vererbung aktivieren** bewirkt, dass beim Erstellen untergeordneter Ordner bzw. beim Hineinkopieren von Dateien in den Ordner die NTFS-Berechtigungseinstellungen auf diese untergeordneten Objekte „vererbt“ werden; dies würde auch für Änderungen gelten.



Ererbte Berechtigungen können nicht direkt entfernt werden:

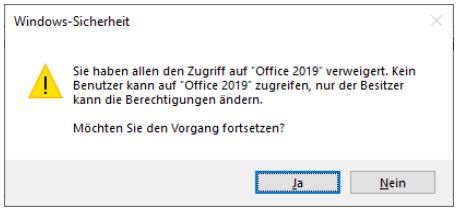


Durch Klicken auf die Schaltfläche **Vererbung deaktivieren** wird die Vererbungskette genau an dieser Stelle unterbrochen. Sie erhalten eine Meldung der folgenden Art:



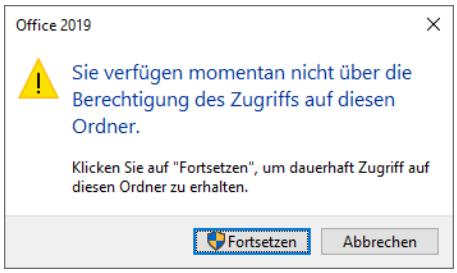
Klicken Sie die erste Option an, so werden aus den geerbten Berechtigungen explizite Berechtigungen, die nun unabhängig geändert werden können. Die zweite Option (**Entfernen**) bewirkt, dass alle NTFS-Berechtigungen für die jeweilige Zeile entfernt werden. Nun hat kein Benutzer Zugriff:

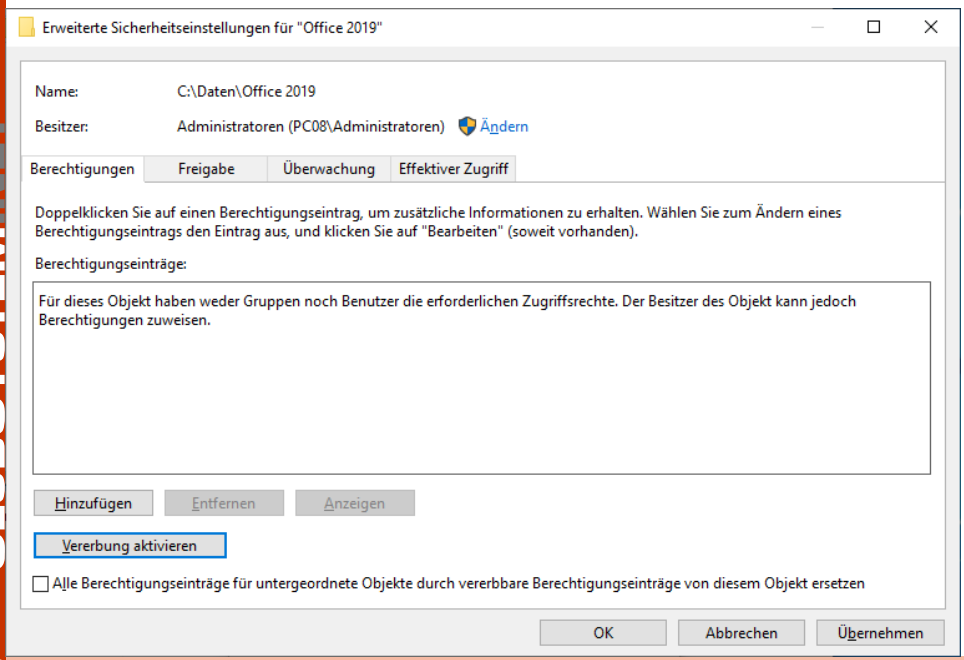
Sie bekommen nun eine Warnmeldung, dass kein Benutzer auf den angegebenen Ordner Zugriff hat.



In diesem Fall kann **nur der Besitzer** (in diesem Fall die lokale Administratoren-Gruppe) weitere Berechtigungen setzen.

Wenn kein Benutzer auf Grund fehlender Berechtigung Zugriff auf einen Ordner hat und der Besitzer versucht auf den Ordner zuzugreifen, so wird folgende Meldung angezeigt:



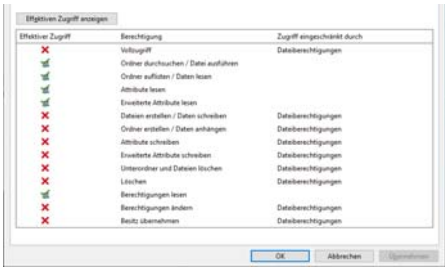


Setzen einer Berechtigung:

10.2.3 Anzeigen der effektiven Berechtigungen für einen Benutzer

In der Registerkarte **Effektiver Zugriff** können die wirklichen Berechtigungen detailliert eingesehen werden:

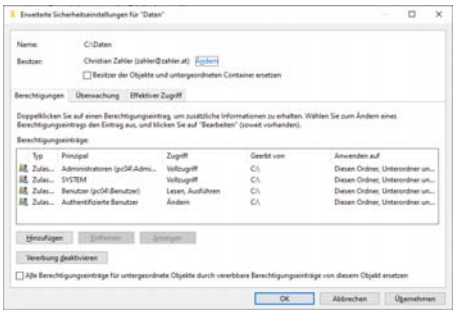
Klicken Sie nun auf die Schaltfläche **Effektiven Zugriff anzeigen**.



10.2.4 Besitzer und Besitzübernahme

Die Berechtigung "Besitz übernehmen" ist die "oberste Berechtigung", da sie geeignet ist, alle anderen Berechtigungen beliebig festzulegen.

Der Besitzer hat immer die Berechtigung, den Besitz an einem Objekt zu übernehmen.



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

Für das Verständnis von NTFS-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.*

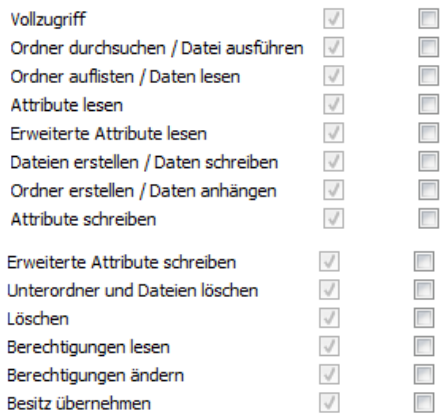
Problem:

Wenn man alle NTFS-Berechtigungen entzieht, kann niemand mehr (auch der Administrator 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:

Beispiel: Berechtigungen für Ordner entsprechen (ähnlich wie bei Linux) den Berechtigungen für Dateien



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

10.2.6 Tipps und Strategien

Es ist günstig, Dateien mit gleichen Sicherheitsanforderungen im selben Ordner zu 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.
- Halten Sie Ihre Berechtigungsstruktur 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

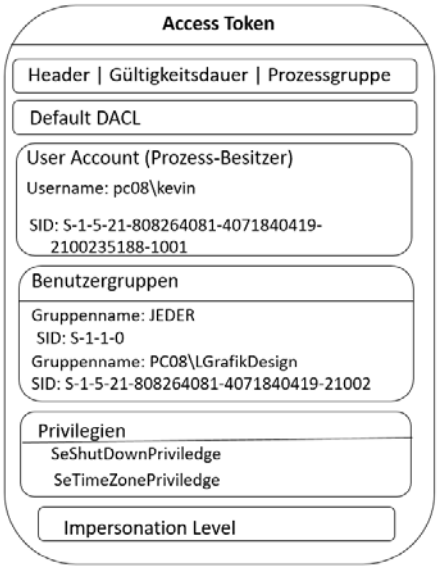
In Windows hat jeder Prozess ein sogenanntes Zugriffstoken (access token). Dieses Zugriffstoken beinhaltet die SID, die Gruppenzugehörigkeiten und sogenannte Privilegien. Das Token wird üblicherweise durch `winlogon.exe` erzeugt. Wenn sich nun ein Benutzer an Windows anmeldet, bekommt der Initialisierungsprozess 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
```

angezeigt werden.

Die folgende Grafik zeigt den grundsätzlichen Aufbau eines Access Token.



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 vordefinierte Benutzergruppen wie VORDEFINIERT\BENUTZER (S-1-5-32-545) oder VORDEFINIERT\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 herunterzufahren
  `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.
- Die Benutzerin Maria hat Lese-/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	○	●	●	●	●	
Windows 10 Windows Server 2016 Windows Server 2019	○	●	●	●	●	●

Außerdem gibt es noch eine **Systemzugriffsliste** (SACL, System Access Control List). Diese Zugriffsliste regelt, welche Operationen im systemweiten Sicherheitsprotokoll aufgezeichnet werden. In unserem Beispiel wird jede Operation, die der Benutzer Kevin auf die Datei ausführt, protokolliert.

10.4 Netzwerkerkennung und Freigaben

Um Ordner, Drucker und Dateien im Netzwerk gemeinsam verwenden zu können, 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 System)** wurde im Jahr 1983 entwickelt und 1988 von Microsoft im frühesten Netzwerkbetriebssystem **LAN-Manager** erstmals verwendet und erreichte große Popularität in den Versionen Windows for Workgroups und Windows 95/98. 1996 wurde es mit Windows NT 4.0 in die aktuelle Betriebssystemfamilie eingeführt.

● wird unterstützt
○ „optionale" Unterstützung, SMB 1.0 ist standardmäßig nicht aktiviert

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 Freigaben					●	●
Verschlüsselung	keine	AES-128-	AES-128-			
Art der File Handles	–	durable	resilient	persistent		
Übersteht Serverausfälle				●	●	●
Unterstützung sym-		●	●	●	●	●
Sicherheit beim Zugriff auf Standardfreigaben (SYSVOL, NETLOGON)						SMB-Signatur, SHA512-Verschlüsselung
SMB Direct, RDMA				●	●	●
SMB Multichannel				●	●	●
Anzahl Befehle	>100	19				
Ports	NetBIOS: TCP 139 Sonst: TCP 445	TCP 445				

manserver, Anzeigename: Server): wird 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/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. Dieser Dienst hatte den Namen **ComputerBrowser** (Dienstname: Browser) und arbeitete mit NetBIOS-Namensbroadcasts.

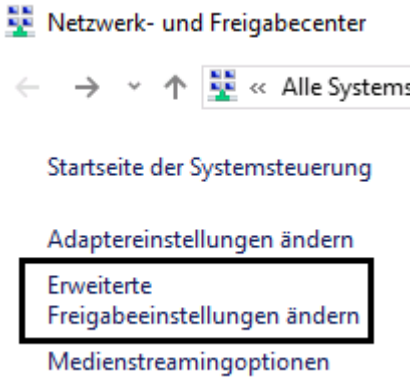
Obwohl der Dienst aus Gründen der Abwärtskompatibilität auch in Windows 10 noch enthalten ist (er ist aber nicht gestartet), wurde bereits in Windows Vista ein völlig neues Protokoll entwickelt, das nun für diese Aufgaben zuständig ist: die **Verbindungsschicht-Topologieerkennung (engl. Link Layer Topology Discovery, LLTD**; Dienstname: lltdsvc). 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.

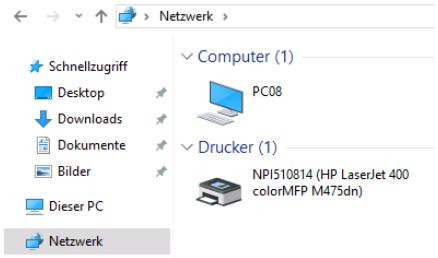
Windows 10 deaktiviert im Profil **Privates Netzwerk** standardmäßig die Netzwerkerkennung (das Auffinden von anderen SMB-Servern im Netzwerk) und die Dateifreigabe. In diesem Fall wird folgende Fehlermeldung angezeigt:

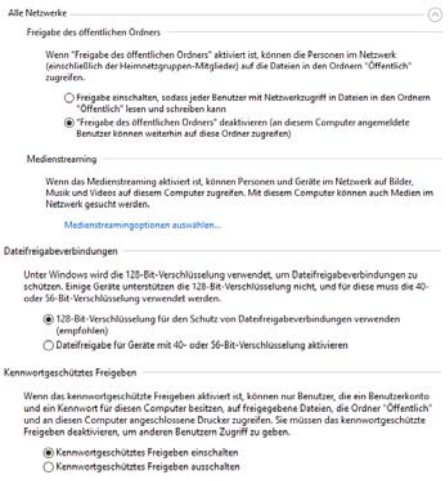
Nach Bestätigung durch Klicken auf **OK** wird anschließend eine Information eingeblendet, dass die Netzwerkerkennung und/oder Dateifreigabe deaktiviert ist. Klickt man auf die Meldung, so können durch Auswahl des Menüpunkts Netzwerkerkennung und Dateifreigabe aktivieren sowohl Netzwerkerkennung als auch Dateifreigabe ermöglicht werden.

Die Netzwerkerkennung und Dateifreigabe können im Systemsteuerungs-App **Netzwerk- und Freigabecenter** durch Anklicken des Links **Erweiterte Freigabeeinstellungen ändern** konfiguriert werden.



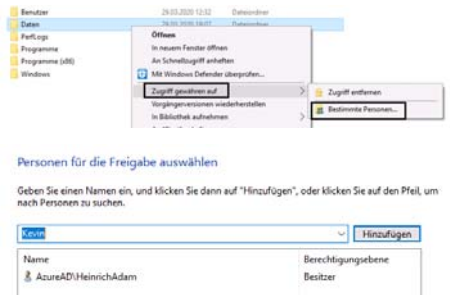
Wird die Netzwerkerkennung eingeschaltet, so werden im Windows-Explorer beim Klick auf das Symbol **Netzwerk** jene Netzwerkcomputer angezeigt, welche ebenfalls die Netzwerkerkennung eingeschaltet haben:





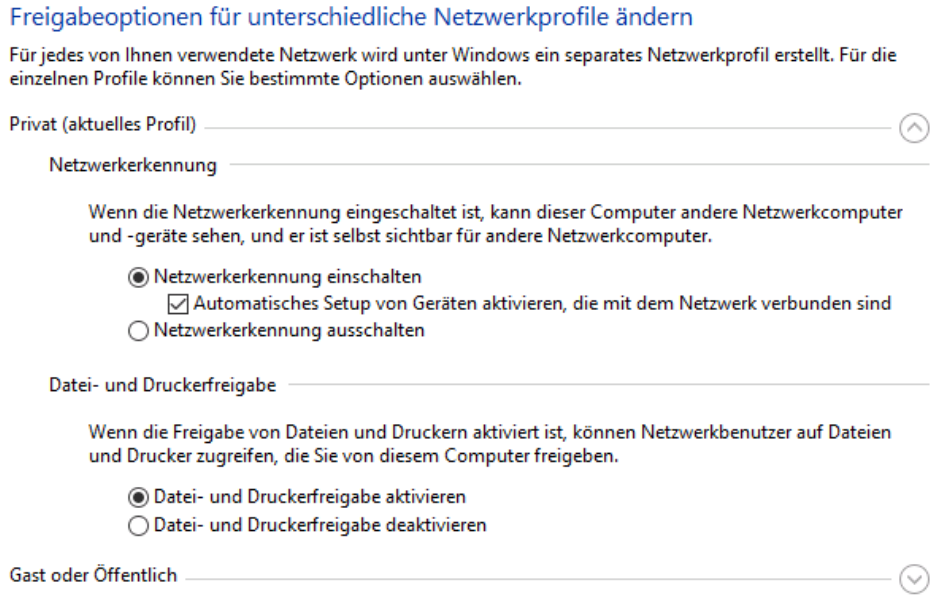
10.4.3 Erstellen von freigegebenen Ordnern mit dem Freigabe-Assistenten

Wählen Sie im Kontextmenü (rechte Maustaste) des freizugebenden Ordners den Eintrag **Zugriff gewähren auf – Bestimmte Personen…:**



Fügen Sie nun alle Benutzer hinzu, die auf den Ordner übers Netzwerk zugreifen dürfen. Standardmäßig erhalten diese hinzugefügten Benutzer die Berechtigungsebene **Lesen**. Beim Zugriff übers Netzwerk dürfen Dateien im freigegebenen Ordner weder geändert noch gelöscht werden.

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



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

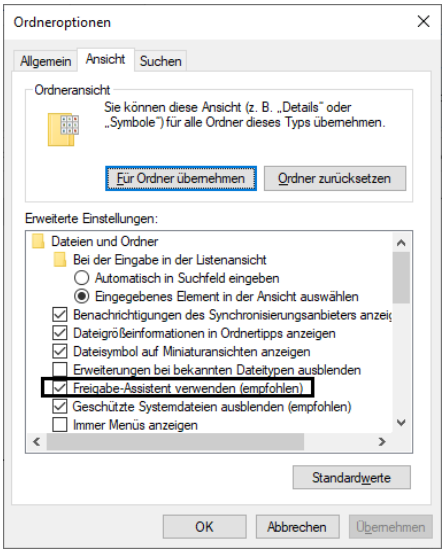
10.4.4 Freigabe-Assistent deaktivieren

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.



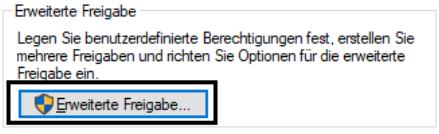
10.4.5 Freigabe-Berechtigungen

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.

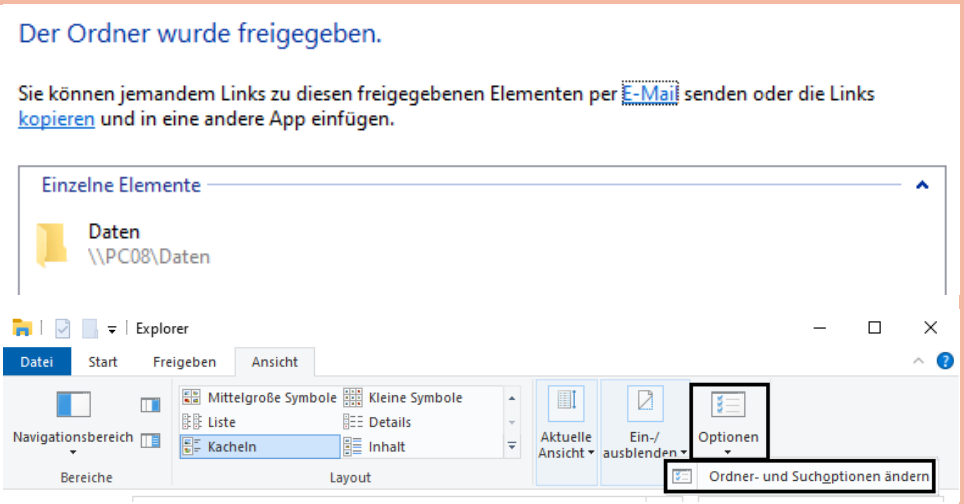
Um Freigabe-Berechtigungen vergeben oder nachträglich ändern zu können, ruft man die Eigenschaften des freigegebenen Ordners auf, Karteikarte **Freigabe.**

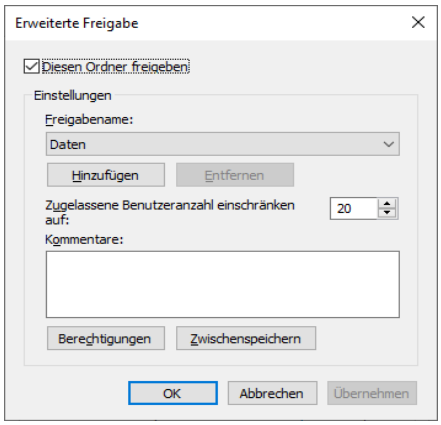
Klicken Sie auf die Schaltfläche **Erweiterte Freigabe…**:



Es erscheint das rechts dargestellte Dialogfeld.

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





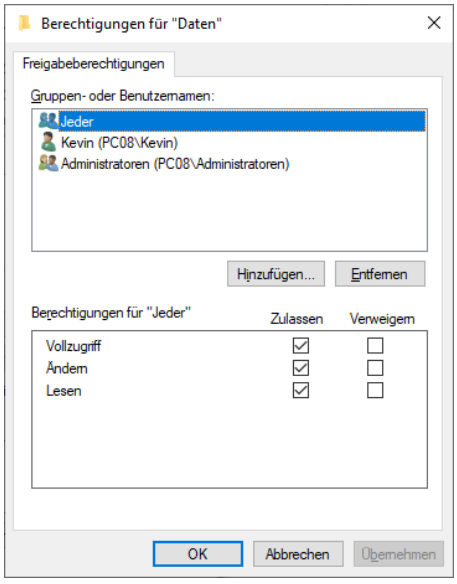
Man unterscheidet nur drei Berechtigungsstufen:

- 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.



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.

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.

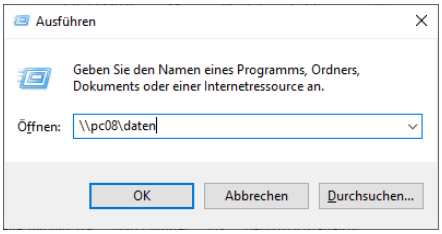
Diese speziellen Freigaben sind in MMC-Konsole **Computerverwaltung** sichtbar.

10.4.9 Zugriff auf freigegebene Ordner

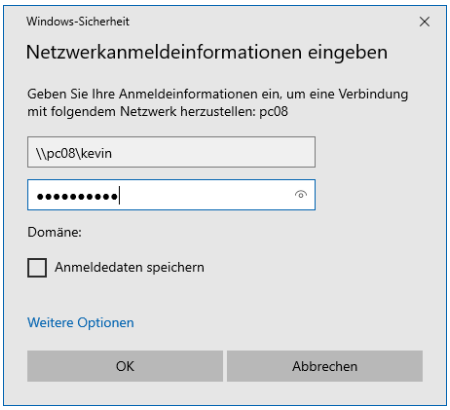
Die Freigabe ist in der Netzwerkumgebung als verbundener Ordner sichtbar.

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

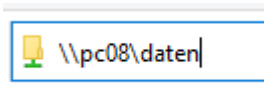
Sie können den freigegebenen Ordner auch mit + R und Eingabe des UNC-Pfades aufrufen:



Gegebenenfalls werden noch die nötigen Netzwerkanmeldeinformationen abgefragt:



Im Explorer wird nun der Inhalt des freigegebenen Ordners angezeigt:



10.4.10 Zuordnen von Laufwerksbuchstaben zu Freigaben („Mapping“)

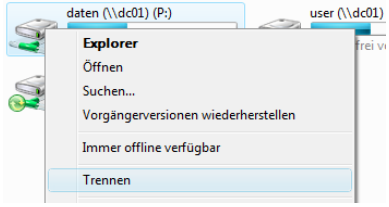
Jeder Freigabe kann ein Laufwerksbuchstabe zugeordnet werden:

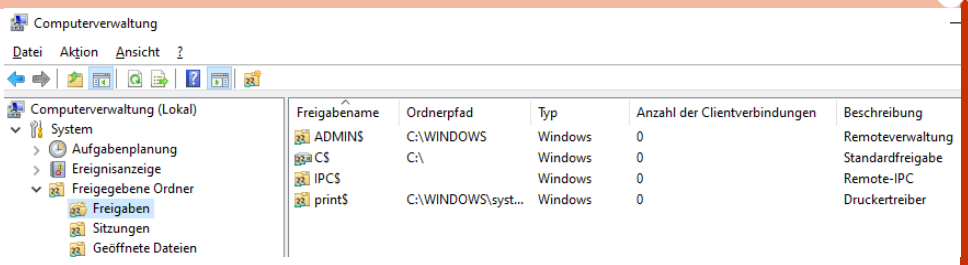
Laufwerksbuchstabenzuordnung in der Kommandozeile mit der Anweisung *net use*:

Beispiel:

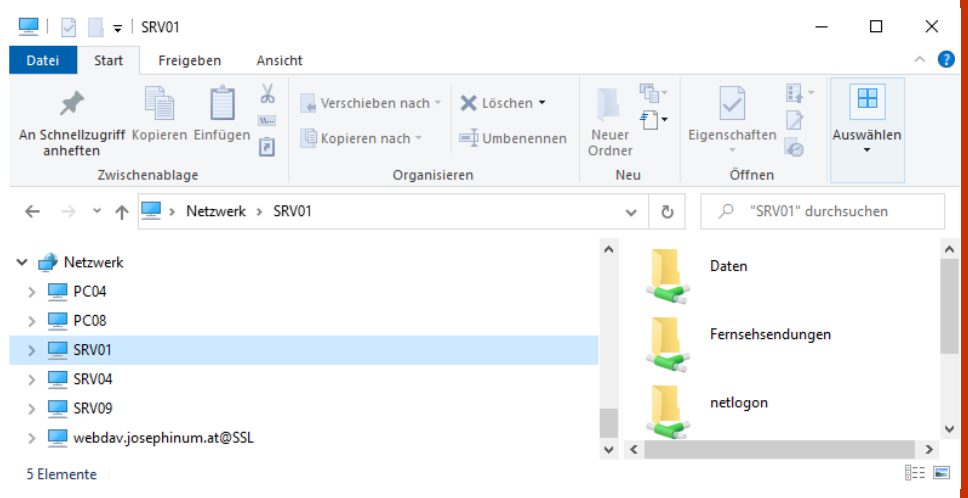
```
C:\>net use M: \\r10\Testordner

Der Befehl wurde erfolgreich ausgeführt.
```

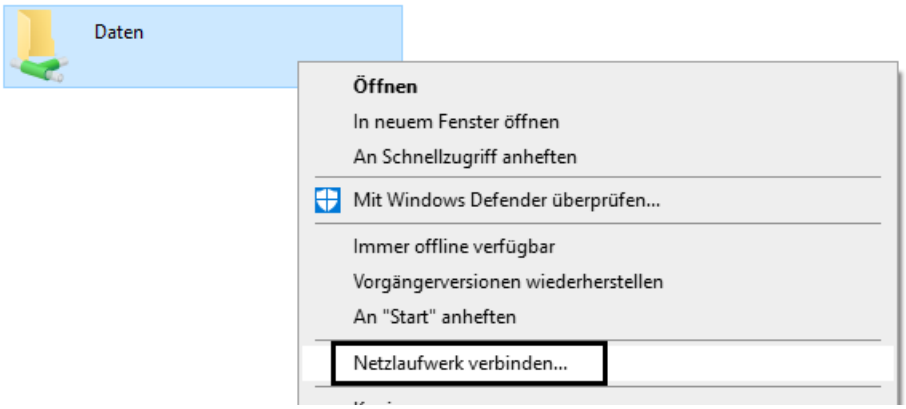
Werden zugeordnete Laufwerksbuchstaben nicht mehr benötigt, so kann die Freigabe wieder getrennt werden:





Name	Bedeutung der administrativen Freigabe
ADMIN$	zeigt auf den Systemordner (zum Beispiel C:\WINDOWS) - für administrative 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)





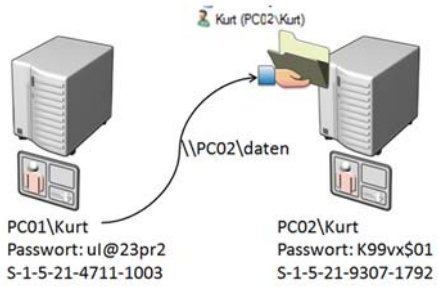
bzw.

```
C:\>net use M: /delete
```

10.4.11 Fernanmeldung, automatische Fernanmeldung

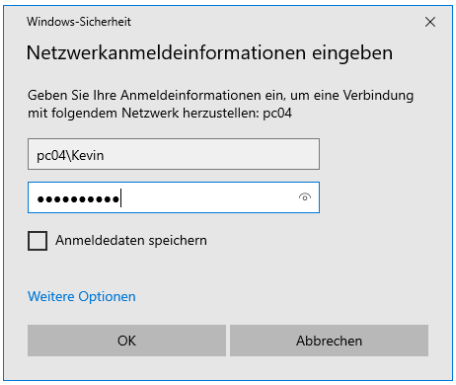
Beispiel: Wir nehmen an, dass auf einem Rechner mit dem Namen PC02 ein freigegebener Ordner mit dem Freigabenamen „daten“ existiert. Auf beiden Rechnern wurde ein lokaler Benutzer mit dem Anmeldenamen Kurt erzeugt. Die beiden Benutzer haben unterschiedliche Kennwörter und natürlich auch unterschiedliche SIDs.

Die Sicherheitsberechtigungen für den Ordner „daten“ wurden so eingerichtet, dass nur der Benutzer Kurt Zugriffsrechte (zum Beispiel „Ändern“) auf diesen Ordner hat.



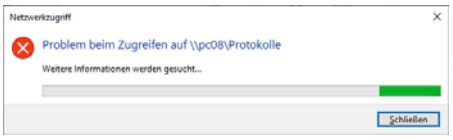
Wir nehmen nun an, dass sich PC01\Kurt mit dem UNC-Pfad \\PC02\daten zum freigegebenen Ordner verbinden will. Die

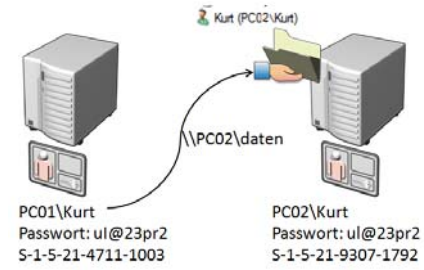
LSA (Local Security Authority) auf PC02 überprüft Benutzername, Kennwort und SID. Nur eine von diesen drei Eigenschaften stimmt überein (der Benutzername), daher wird PC01\Kurt nicht ohne weiteres der Zugriff auf den Ordner gewährt; es erscheint ein **Dialogfeld für die Fernanmeldung**:



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:





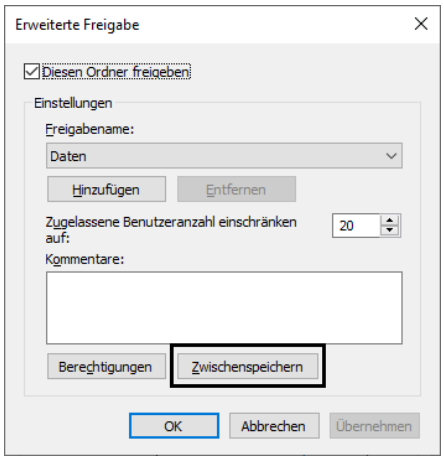
Modifizieren wir nun das Beispiel so, dass die Kennwörter der beiden Benutzerkonten übereinstimmen. Wieder überprüft die LSA auf PC02 Benutzername, Kennwort und SID – zwei dieser drei Eigenschaften stimmen überein (Benutzername und Kennwort). Nun erscheint kein Dialogfeld; es erfolgt eine **automatische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

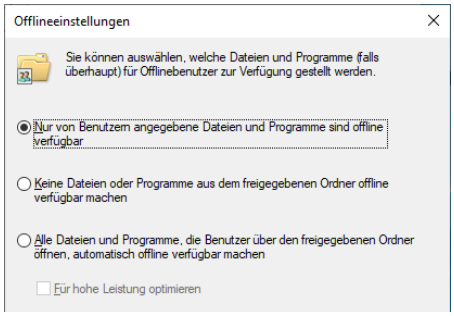
10.4.12 Offline-Ordner und Synchronisierungscenter

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 freigegebene Ordner befindet) gerade nicht erreichbar sein sollte.

Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie im Kontextmenü den Eintrag **Zugriff gewähren auf – Erweiterte Freigabe**. Klicken Sie auf die Schaltfläche **Erweiterte Freigabe**.

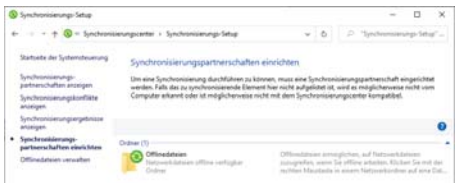
Im Dialogfeld Erweiterte Freigabe klicken Sie auf die Schaltfläche **Zwischenspeichern**.





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

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



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.

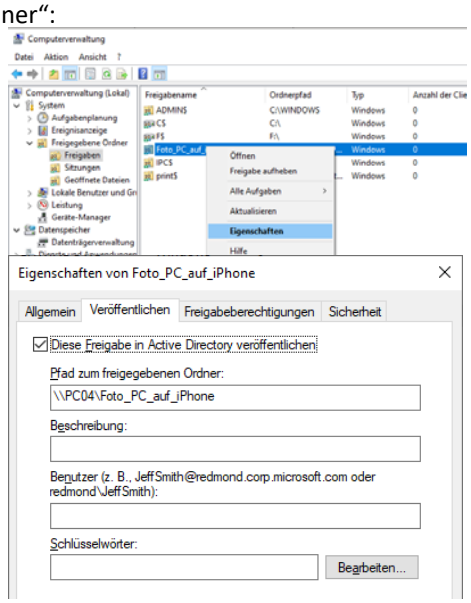
Bei der bidirektionalen Synchronisierung werden Dateien in beide Richtungen kopiert, um die Dateien an beiden Orten synchron zu halten. Jedes Mal, wenn Sie eine Datei an einem Ort hinzufügen, ändern oder löschen, wird dieselbe Änderung am anderen Ort ausgeführt. Es spielt keine Rolle, ob Sie die Änderungen auf einem Computer, einem mobilen Gerät oder in einem Ordner auf einem Netzwerkserver 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“:



11Fernwartung und Fernzugriff

Christian Zahler

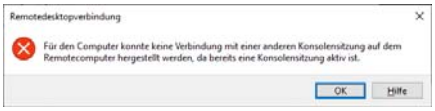
Eine typische Aufgabe im IT-Systemadministrationsbereich ist die Unterstützung anderer Benutzer bei Problemen. Oft ist es aus Zeitgründen nicht sinnvoll, persönlich zum entsprechenden Problemort zu reisen. Die heute übliche Methode besteht in der Fernwartung von Geräten.

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:



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.

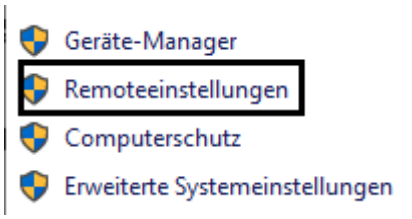
Vergleich: Stellen Sie sich einfach vor, Sie würden Ihre Tastatur, Ihre Maus und Ihren Monitor mit einem „sehr langen Kabel" mit dem entfernten PC verbinden.

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

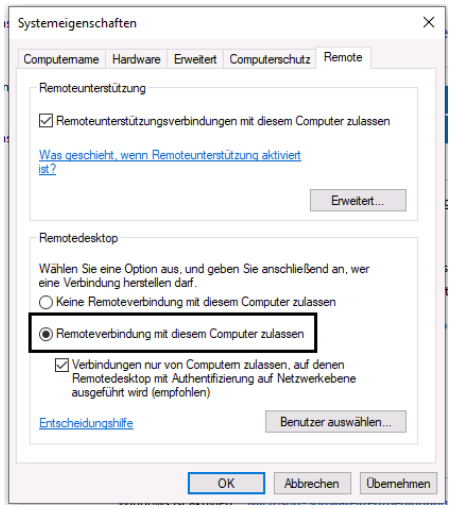
Vorgangsweise:

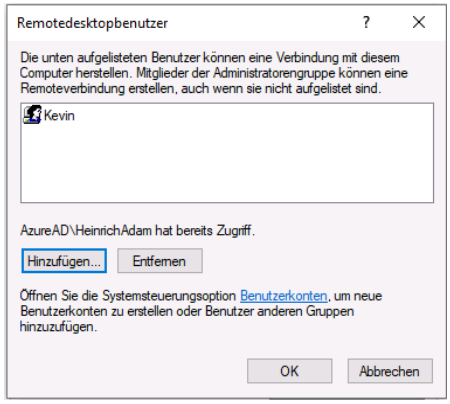
1. Schritt: Einrichten des „Servers" (das ist der Windows 10-PC, zu dem Sie sich von der Ferne aus verbinden wollen)

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



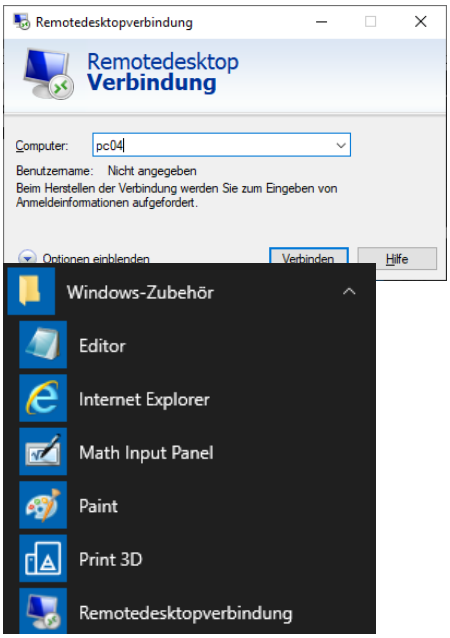
Standardmäßig ist diese Remoteverbindung bereits für den lokalen Administrator zugelassen, unter der Schaltfläche **Benutzer auswählen…** können jedoch beliebige lokale Benutzer eingetragen werden, die Remoteverbindungen herstellen können.



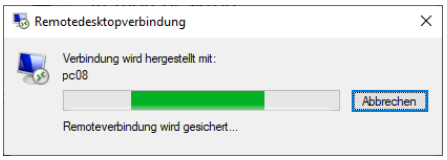


2. Schritt: Verbinden zum eingerichteten Server vom „Client" aus (das ist der PC, auf dem Sie arbeiten und von welchem aus Sie den entfernen Computer ansprechen wollen):

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.

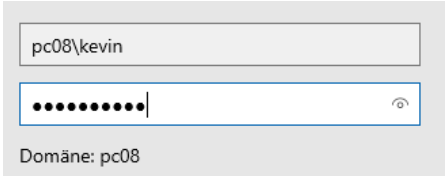


Sie müssen sich noch am entfernten PC anmelden. Standardmäßig wird Ihnen das Benutzerkonto vorgeschlagen, mit dem Sie selbst an Ihrem eigenen PC angemeldet sind.

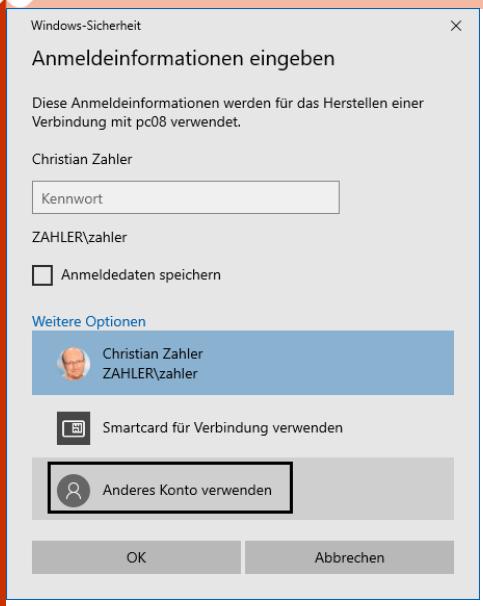
Das wird aber nicht in jedem Fall funktionieren; klicken Sie daher auf den Link **Weitere Optionen** und wählen Sie **Anderes Konto** verwenden.

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

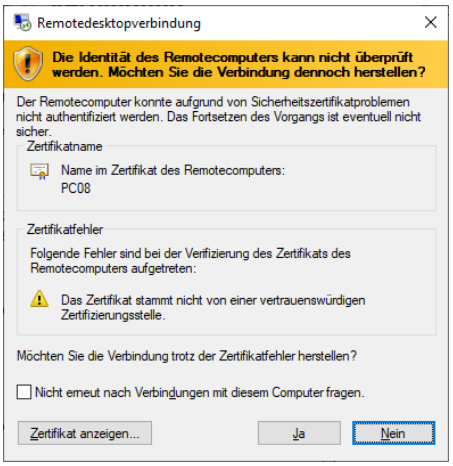
Achtung: Für ein lokales Konto müssen Sie den Computernamen mit angeben, etwa **pc08\kevin**:



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



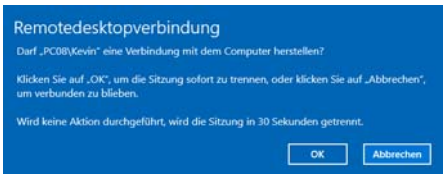
Falls der angesprochene Computer kein vertrauenswürdiges Zertifikat liefert, erscheint folgende Fehlermeldung:



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

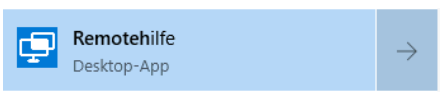
Klickt man „Ja“, so wird der Client aufgefordert zu warten.

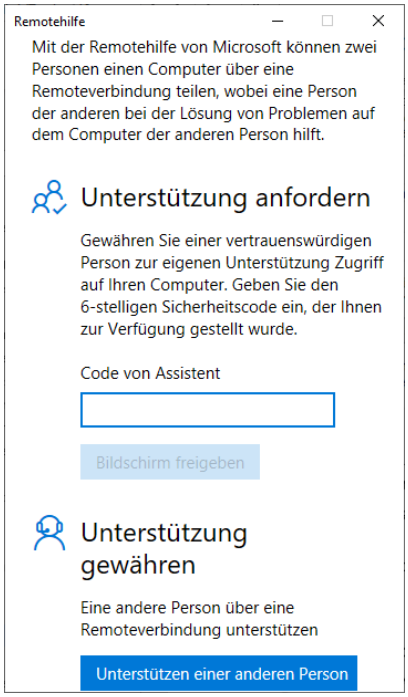
Am „Server“ erscheint folgende Meldung:

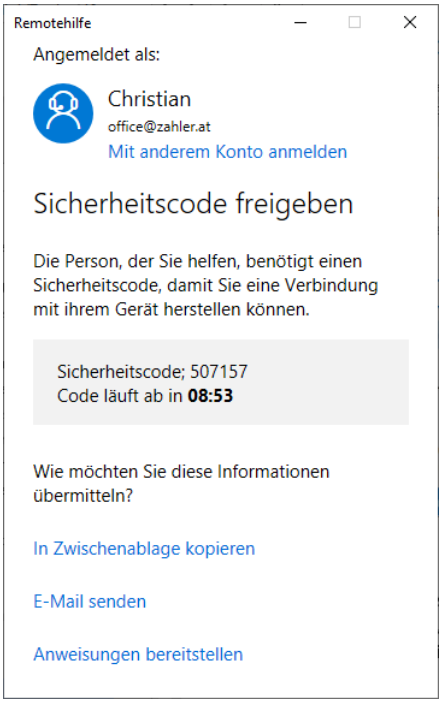


11.2 Remotehilfe

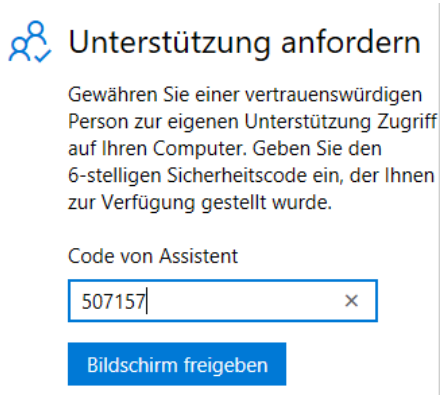
Starten Sie die Desktop-App **Remotehilfe**.







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**.

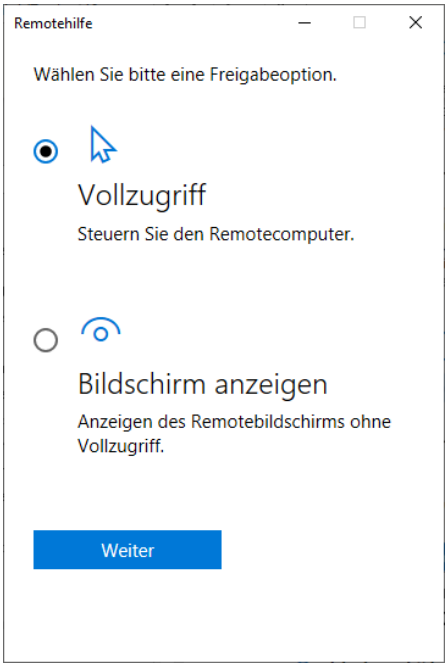
Es erscheint die Meldung

Verbindung wird hergestellt

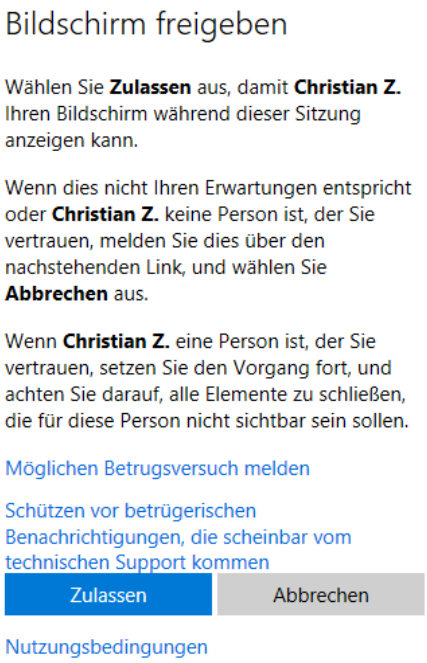
und dann

Warten auf Teilnehmer für Berechtigungserteilung

Nun muss die hilfesuchende Person am Remotecomputer den Bildschirm freigen.

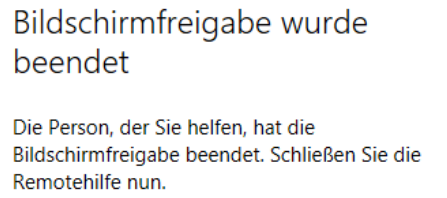


Hilfesuchende Person:



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

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



Remotehilfe-Fenstern im Modus „Bildschirm anzeigen“:

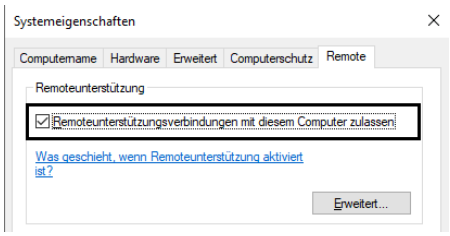
Remotehilfe-Fenstern im Modus „Vollbild“: Nur in diesem Modus ist die Fernsteuerung möglich. Es gibt zusätzliche Schaltflächen für den Neustart des Remotecomputers und das Aufrufen des Task-Managers am Remote-PC.

11.3 Remoteunterstützung

Das Feature Remoteunterstützung basiert auf dem **Remote Desktop Protocol** (RDP) und ist ein Feature, welches nur mehr aus Kompatibilitätsgründen auf Windows 10 verfügbar ist. Es wird in naher Zukunft nicht mehr zur Verfügung stehen.

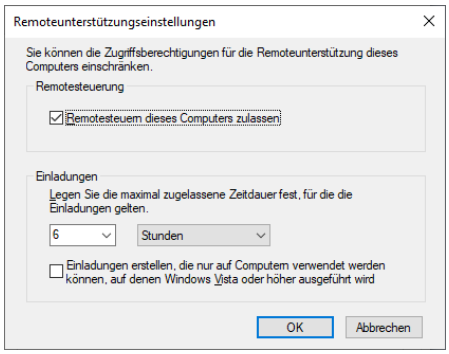
Das Feature Remoteunterstützung dient dazu, die Fernsteuerung anderer Bildschirme zur Unterstützung von Anwender/innen zu ermöglichen.

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.



Dies bewirkt, dass der Teredo-Dienst gestartet wird. Dieser Dienst ermöglicht es 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.

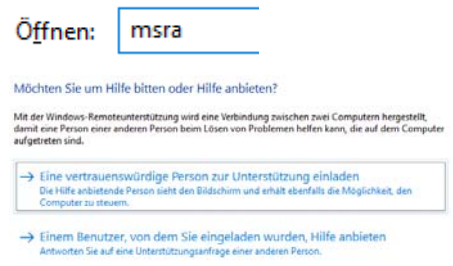
Klicken Sie auf die Schaltfläche **Erweitert...**, um detailliertere Einstellungen festzulegen.



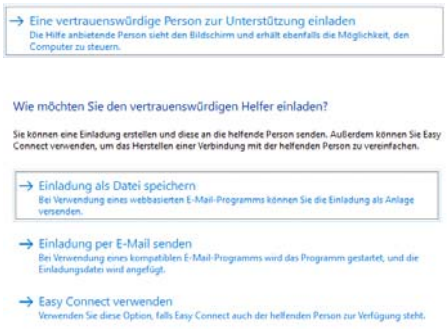
Schritt 2: Senden einer Remoteunterstützungsanforderung (am PC der hilfesuchenden Person)

Sie 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 unterstützt.

Die Remoteunterstützung ist nicht mehr im Startmenü verfügbar, sondern muss mit + R direkt aufgerufen werden:

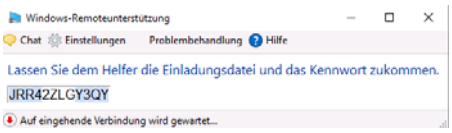


Schritt 1 – PC der hilfesuchenden Person:



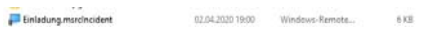
Am einfachsten ist EasyConnect; für EasyConnect müssen beiden Computer Windows 10 ausführen und PNRP unterstützen (Peer Name Resolution Protocol), die verwendeten Router müssen IPv6-Tunneling und UPnP unterstützen.

Auf dem Bildschirm der hilfesuchenden Person erscheint nun folgende Meldung:

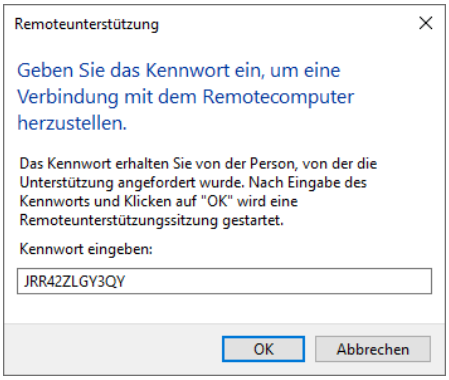


Schritt 2 – PC der helfenden Person:

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

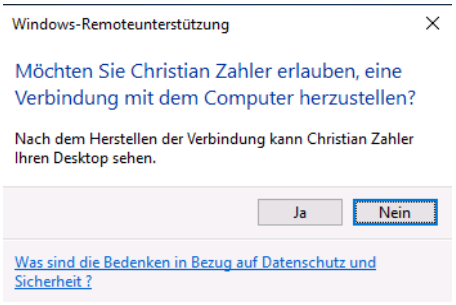


Doppelklick auf diese Einladung öffnet folgendes Fenster, in welches der Code eingegeben werden muss, den die hilfesuchende Person angezeigt bekommt.

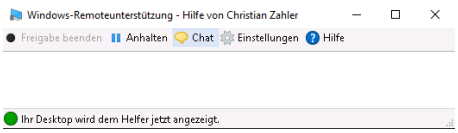


Klicken Sie anschließend auf OK.

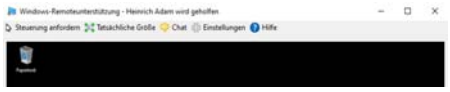
Schritt 3 – PC der hilfesuchenden Person: Hier wird nun gefragt, ob der Helfer eine Verbindung herstellen darf. Klicken Sie auf **Ja**, um dies zu erlauben.



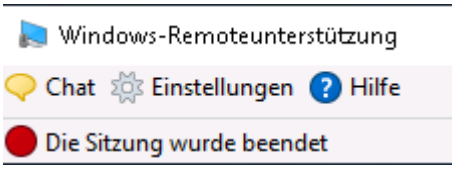
Es erscheint danach folgende Darstellung:



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.



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



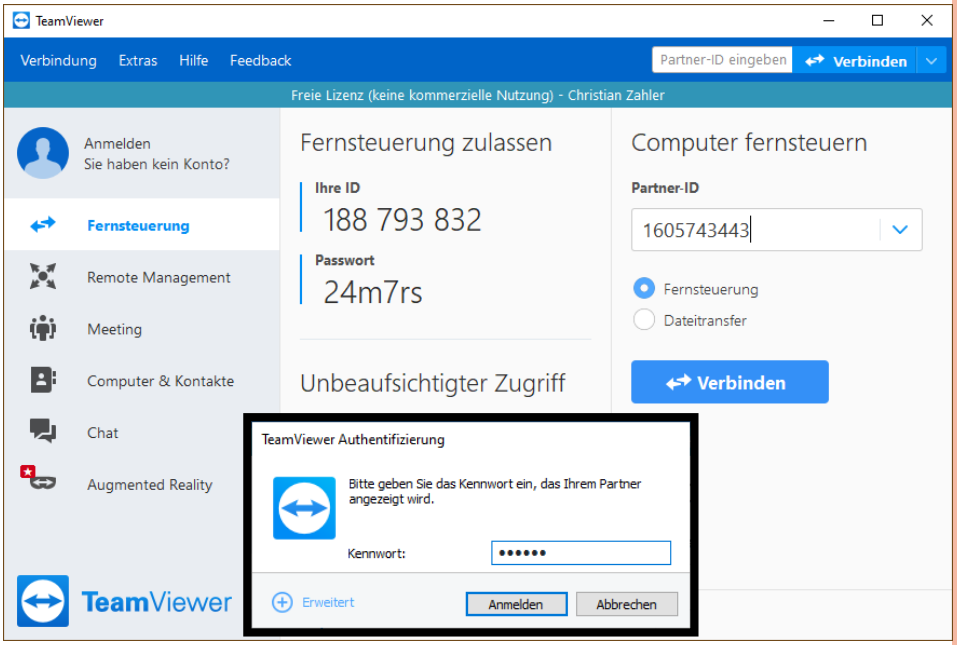
11.4 TeamViewer

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 diesen 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.

Nachteil: Keine Unterstützung von Active Directory-integrierten Gruppenrichtlinien.

Voraussetzung: Windows 10 Pro oder 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.

12.3 BranchCache

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. BranchCache speichert eine lokale Kopie von Daten, auf die Clients über Remoteweb- und -dateiserver zugreifen. Der Cache kann auf einem gehosteten Server in der Zweigstelle platziert werden oder sich auf den Computern der einzelnen Benutzer befinden. Wenn ein anderer Client die gleiche Datei anfordert, lädt er die Datei 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 selben Druckertreiber unterstützt.

Um also von Windows aus drucken zu können, muss ein **logisches Druckerobjekt** eingerichtet werden. Dabei unterscheidet 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 oder externer Netzwerkkarte (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.

Ausschnitt einer PostScript-Druckdatei:

```
F /F0 0 /256 T /Helvetica mF

/F0S53 F0 [83 0 0 -83 0 0 ] mFS

F0S53 Ji

473 550 M (Dieser Text soll gedruckt wer-
den.)[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
59 46 28 46 46 46
 0]xS

1708 550 M ( )S

473 646 M ( )S

LH

(%%[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).

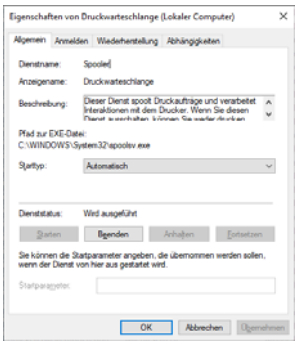
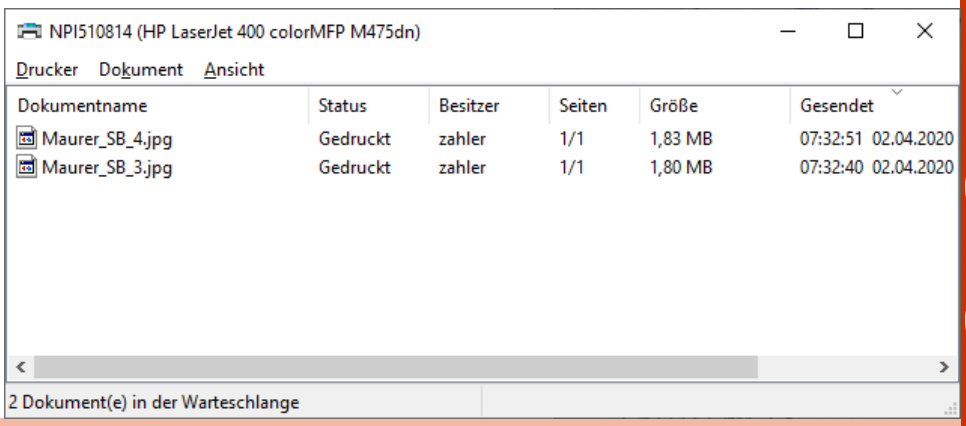


Abbildung: Eigenschaften des Dienstes **Druckwarteschlange (Spooler)**



3. Die Druckdateien werden dann an den angegebenen Drucker weitergeleitet. Dabei kann der Drucker immer nur so viele Daten empfangen, wie er in seinem Arbeitsspeicher unterbringen kann.

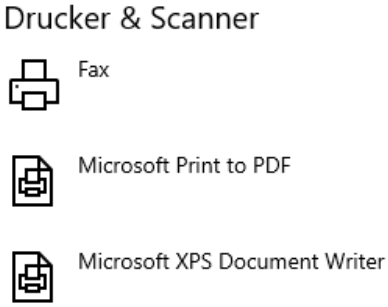
4. Der Drucker arbeitet die in seinem Arbeitsspeicher befindlichen Druckaufträge seitenweise (Laserdrucker) bzw. zeilenweise (Nadel-, Tintenstrahldrucker) ab. Nicht benötigte Druckinformationen werden gelöscht, sodass im RAM Platz für weitere Teile des Druckauftrags bzw. neue Druckaufträge geschaffen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

13.2 Einrichten eines lokalen Druckerobjekts

Die Verwaltung von Druckern und Scanner erfolgt über die Systemeinstellungen:

Standardmäßig gibt es drei Druckerobjekte, die bereits installiert sind:

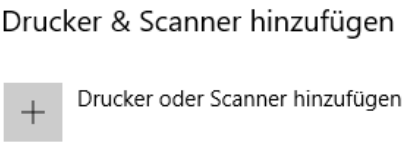
- **Fax:** Ermöglicht das Senden von Fax, falls eine Wählverbindung hergestellt werden kann
- **Microsoft Print to PDF:** Druckt ein Dokument nicht aus, sondern erstellt eine PDF-Datei (PDF = Portable Document Format). PDF ist ein geräte- und systemunabhängiges Druckformat; PDF-Dokumente sehen auf allen 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.



Um ein Druckerobjekt hinzuzufügen, welchem einem physischen Druckgerät entspricht, gibt es zwei Möglichkeiten – über die Systemeinstellungen oder über die Systemsteuerung.

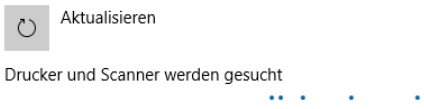
Variante 1: Druckerhinzufügen in den Systemeinstellungen

Klicken Sie auf **Drucker oder Scanner hinzufügen.**

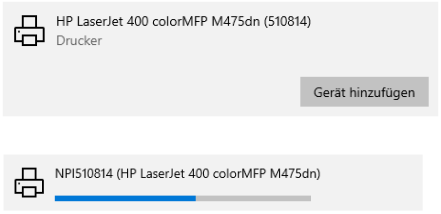


Es startet folgender Assistent:

Zunächst versucht Windows, neue Druckgeräte im Netzwerk zu finden. Dieser Vorgang kann einige Zeit dauern. Wenn möglich, werden die Treiber automatisch installiert und die Druckerobjekte erzeugt.



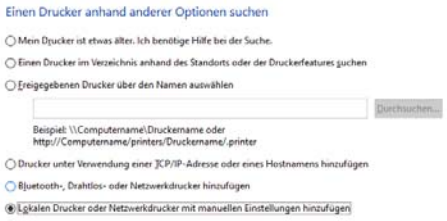
Nach einiger Zeit werden alle gefundenen Drucker im Netzwerk aufgelistet. Klicken Sie auf das Druckerobjekt und anschließend auf die Schaltfläche **Gerät hinzufügen**, damit der Druckertreiber installiert wird und ein logisches Druckerobjekt erzeugt wird.



Das Druckerobjekt wird nach Abschluss der Treiberinstallation angezeigt:

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

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

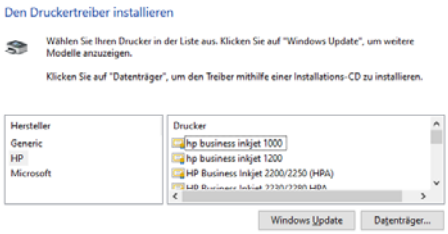


2. Schritt: Wählen Sie den **Druckeranschluss** aus oder erstellen Sie einen neuen Anschluss.

Folgende Anschlüsse sind bereits standardmäßig vorhanden:

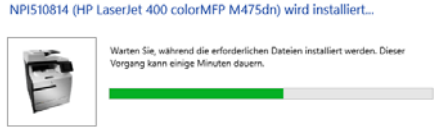
- Parallele Anschlüsse (LPT1, …): Früher der Standard-Druckeranschluss; erforderlich ist ein paralleles Kabel mit Centronics-Stecker.
- Serielle Anschlüsse (COM1, …): Wurde häufig für CAD-Plotter verwendet. Voraussetzung für das Funktionieren des Druckers ist die übereinstimmende Konfiguration der seriellen 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 Typ 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**

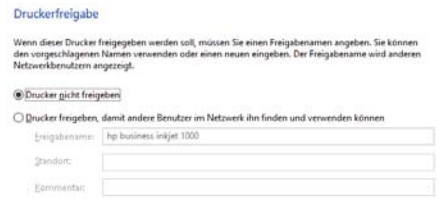


4. Schritt: Drucker benennen

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

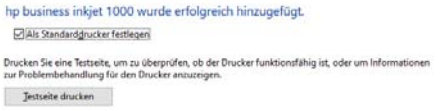


5. Schritt: Druckerfreigabe



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!).



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

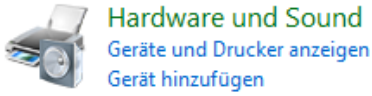
- grafischen Informationen,
- Systemschrift-Texten und
- TrueType-Schrift-Texten

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:

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.

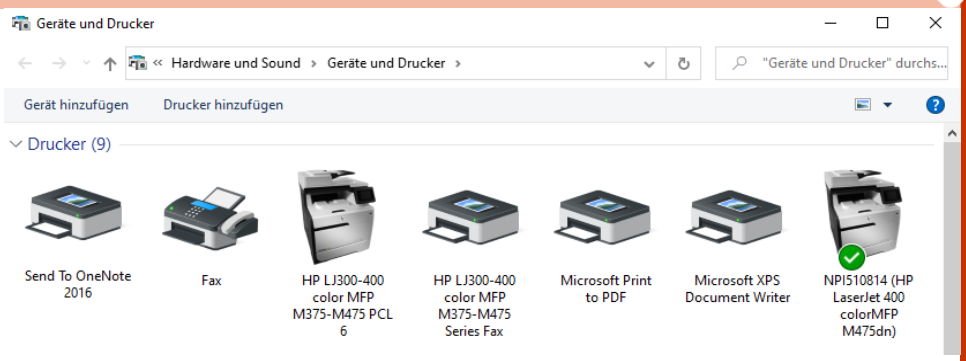


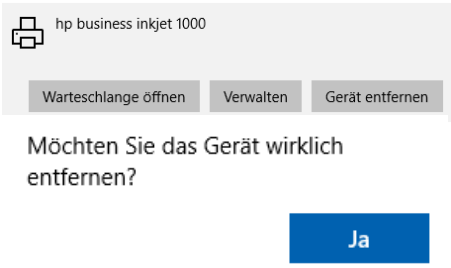
Der Assistent führt durch denselben Konfigurationsprozess wie in den Systemeigenschaften.

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**.

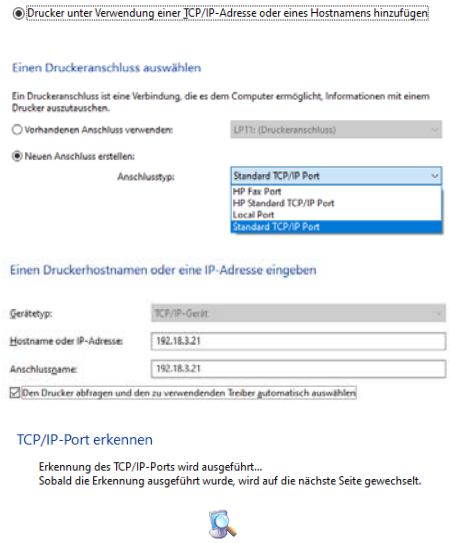


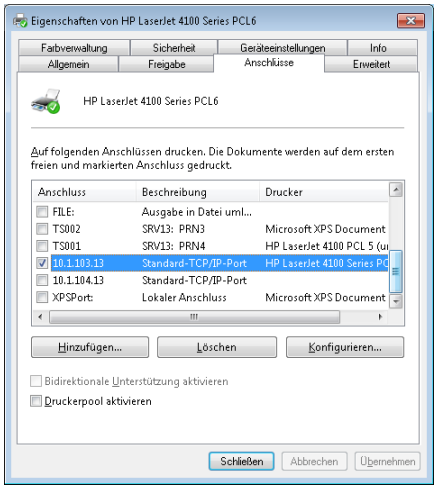


13.4 Erzeugen eines TCP/IP-Druckeranschlusses

Dies ist notwendig, wenn der lokale Drucker über eine eigene Netzwerkkarte bzw. über eine externe Netzwerkkarte (falsch auch als „Printserver“ bezeichnet, etwas korrekter „Netport“) verfügt.

Im Assistenten wählen Sie folgende Option:





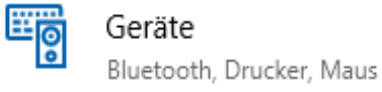
13.5 Druckserver konfigurieren

Schritt 1: Drucker freigeben

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.

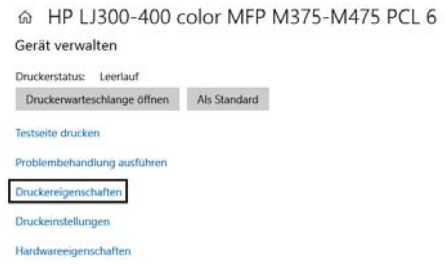
Zunächst müssen die Freigabeoptionen des logischen Druckerobjekts geändert werden.

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



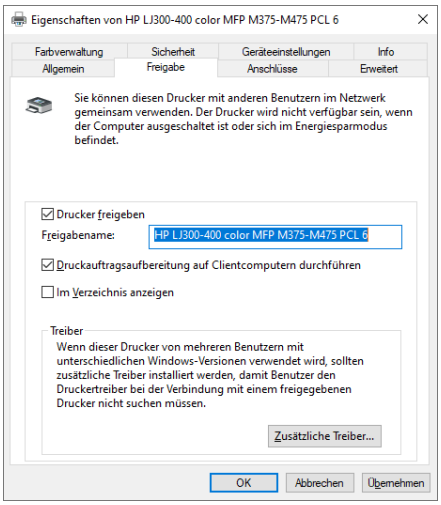
Klicken Sie in der Druckerliste auf den freizugebenden Drucker; klicken Sie anschließend auf die Schaltfläche **Verwalten**.

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



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).

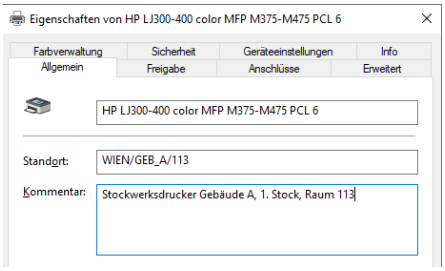


***Wichtig:** Ein freigegebener Drucker wird auch als **Druck-Server** bezeichnet!*

2. Schritt: Standortangabe und Kommentar

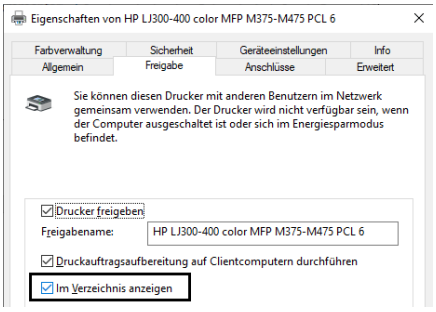
In einer größeren Organisation gibt es oft viele Drucker. Damit sie auch lokalisiert werden können, sollte man freigegebene Drucker mit einer Standort-Angabe und einem Kommentar versehen. Beim Standort-Eintrag sollten Sie eine Hierarchie berücksichtigen, mit Hilfe derer der Drucker wieder gefunden werden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

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

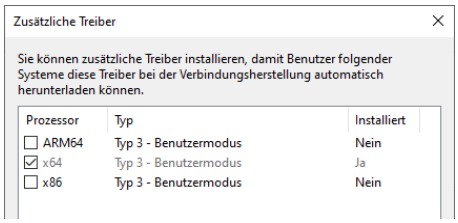


Wenn Sie einen Druckserver konfiguriert haben (zur Erinnerung: das ist ein freigegebener Drucker), dann haben Sie zwei weitere Möglichkeiten:

- 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).

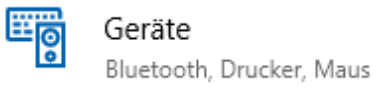


- Bei der Freigabe von Druckern wird automatisch eine administrative Freigabe PRINT$ erzeugt, die zu einem Ordner führt, in welchem passende Druckertreiber vorhanden sind. Bei der Installation eines Netzwerkdruckers können Client-PCs diese Treiber herunterladen, ohne das Druckermodell kennen zu müssen. 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.

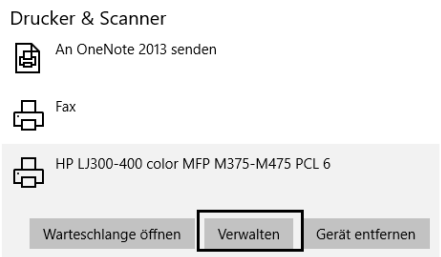


13.6 Druckerverwaltung

Um Drucker zu konfigurieren und Druckeinstellungen sowie Druckereigenschaften zu verwalten, rufen Sie in den Einstellungen den Bereich **Geräte** auf und klicken dann auf **Drucker und Scanner**.



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

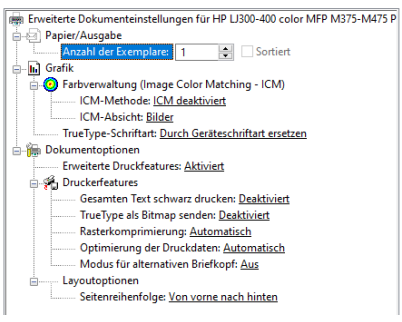


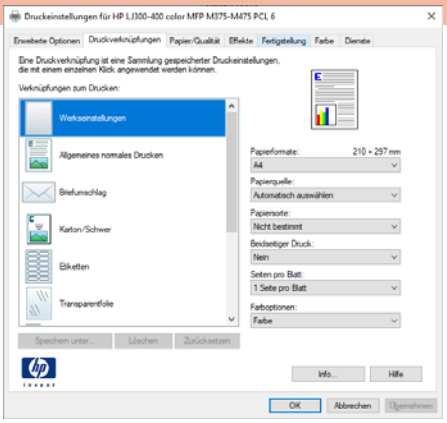
13.6.1 Druckeinstellungen

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.



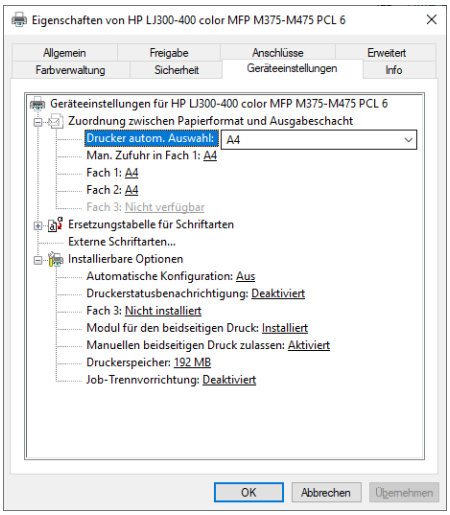


13.6.2 Druckereigenschaften

Druckereigenschaften

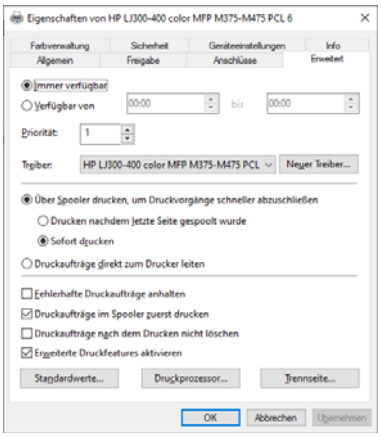
Hier können Sie die Eigenschaften des Druckerobjekts bearbeiten.

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

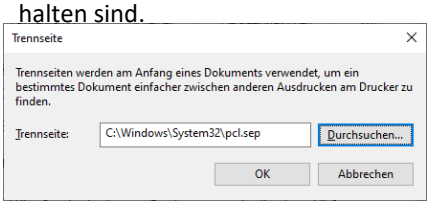


In der Karteikarte „Erweitert“ kann konfiguriert werden:

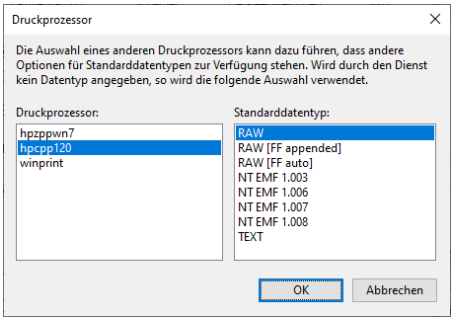
- **Priorität der Druckaufträge** (zwischen 1 und 99): Aufträge mit geringerer Priorität werden in der Druckwarteschlage nachgereiht und daher später gedruckt.
- **Spooler umgehen:** Hier kann der Druckauftrag direkt zum Drucker gesendet werden. Das hat den Nachteil, dass der Druckvorgang länger dauert, 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.



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



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



13.7 Einrichten eines Druckerpools

Unter einem Druckerpool versteht man mehrere gleichartige physische Drucker, die unter demselben Namen im Netzwerk angesprochen werden sollen. Es ist daher **ein** logisches Druckerobjekt zu erstellen, welchem **zwei** oder mehrere physische Drucker zugeordnet werden.

Dazu ist es nötig, zuerst einen der beiden Drucker wie beschrieben zu installieren und dann die Eigenschaften des logischen Druckerobjekts zu bearbeiten.

Zunächst muss ein zweiter Druckeranschluss hinzugefügt werden (da es sich in der Praxis meist um TCP/IP-Drucker handelt, 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!

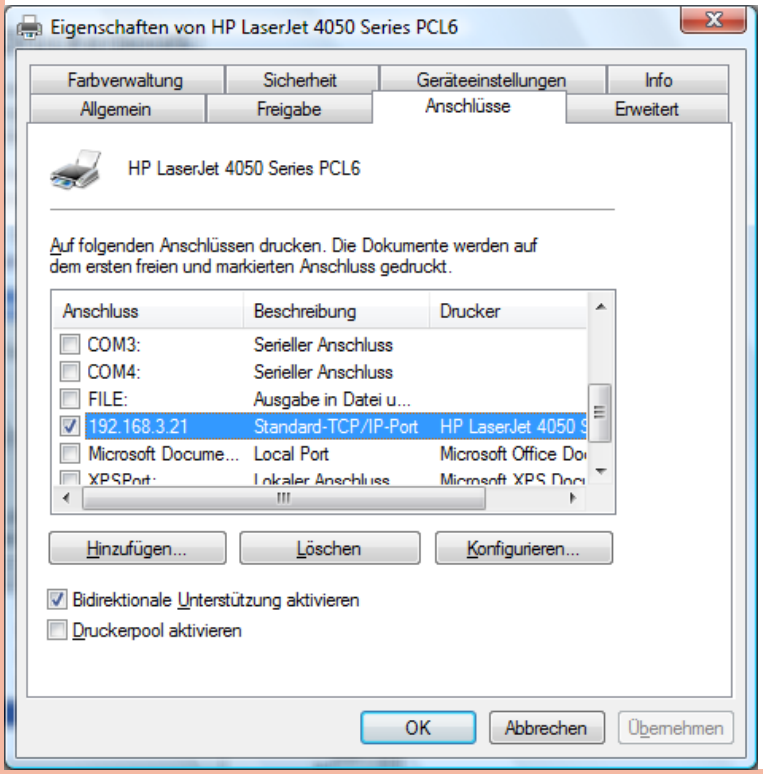
13.8 Berechtigungen für logische Druckerobjekte

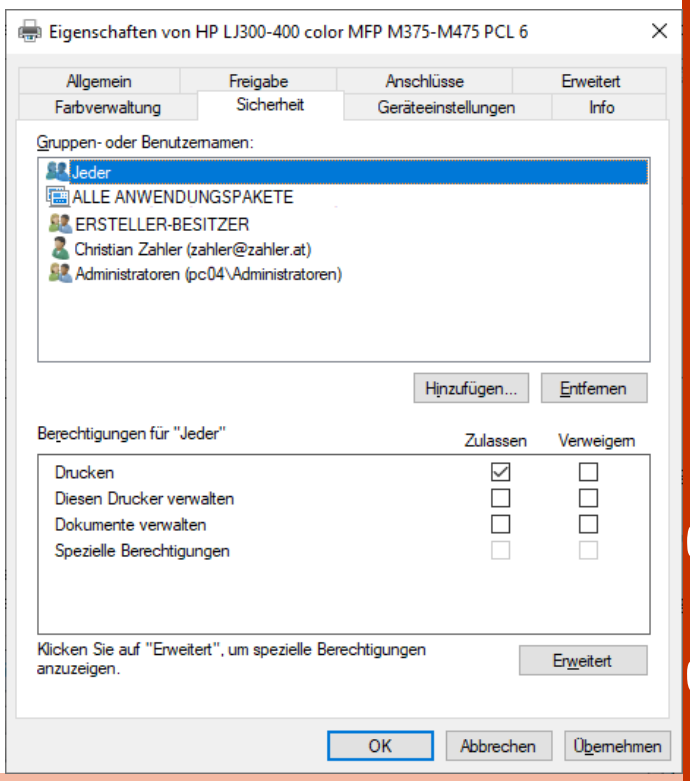
So wie für Dateien und Ordner können auch Berechtigungen für logische Druckerobjekte erstellt werden.

Für Drucker existieren spezielle Berechtigungen:

- Drucken (das muss nicht speziell erklärt werden)
- Dokumente verwalten (mit dieser Berechtigung können Druckaufträge aus der Druckwarteschlange entfernt werden)
- Drucker verwalten (damit können logische 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).





techbold

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.

www.techbold.at/pc-zusammenstellen

BERATUNG
Umfangreicher Support von zertifizierten Experten

QUALITÄT
Ausschließlich geprüfte Markenkomponenten

TESTS
Jede Konfiguration wird umfangreich getestet

GARANTIE
3 Jahre Garantie auf alle individuellen PC-Systeme