


Windows 10 Unterschiede	3
Treiber:	4
Treiber sichern:	4
weitere Treiber Infos	4
CMD Tipps:	5
CMD als Admin öffnen wenn die CMD bereits gestartet ist:	5
Weitere TIPPS:	5
PowerShell	6
Computer-Kennwort zurücksetzen	6
PowerShell Remote ausführen	6
BitLocker	6
In welchen Versionen ist es enthalten	6
Wie arbeitet BitLocker	7
Welche Möglichkeiten habe ich zur Wiederherstellung bei Verlust des Full-Volume encryption Keys	7
Quick-Tipp:	7
BadUsb Sticks: Tarnen sich als Tastatur :	7
Storage Spaces (Seit Windows 8 und Windows Server 2012)	7
Simple	8
Mirror	8
Parity	8
Remote Session über PowerShell	8
Starten einer interaktiven Sitzung:	8
Ausführen eines Remote- Befehls (Run a Remote Command)	9
Ausführen eines Skripts / Run a Script	9
Quick-Tipp:	9
Kerberos Ticket verwerfen:	9
UE-V	9
UE-V Generator Templates erstellen und anwenden	10
VPN unter Windows 10	10
Grundsätzlich	10
Hinzufügen oder Ändern einer VPN-Verbindung unter Windows 10	11
Was ist DirectAccess	12
DirectAccess mit Windows 10	12

Erweiterte Informationen für Admins:	13
DirectAccess-Server mit Windows Server 2012 R2/2016 einrichten	13
DirectAccess in der RemoteAccess Management Console verwalten	14
Clients mit der DirectAccess-Konfiguration anbinden	14
Microsoft Windows DirectAccess Client Troubleshooting Tool	15
Offline-Domänenaufnahme mit Djoin.exe	15
Voraussetzungen für die Verwendung	16
Durchführen der Offline-Domänenaufnahme	16
Offline-Domänenaufnahme bei einer unbeaufsichtigten Installation über Antwortdatei	17
Lösen von Problemen bei Dateizugriff	19
Zugriff verweigert oder Fehler beim Zugreifen auf und Bearbeiten von Dateien und Ordnern in Windows	19
NTFS-Berechtigungen richtig einrichten	19
Access-based Enumeration	19
Was sind Bedingungen im Bereich der Sicherheitseinstellungen (ab 2012 Server)	19
EFS (Encrypting File System)	19
Probleme mit EFS	20
Wie kann man Daten wiederherstellen	20
Lösen von Problemen mit Druckern	20
Welche Probleme gibt es	20
Was ist bei Druckertreibern zu beachten	21
Was lässt sich in den Eigenschaften eines Druckers konfigurieren	21
Microsoft Workfolders (Arbeitsordner)	21
Rolle installieren	23
Hinweise zur Benutzerordnerstruktur (Quelle: TechNet):	23
Schritt 2 – Zertifikatsbindung für Workfolders	24
Workfolders unter einem Client einrichten	24
Leistungsprobleme unter Windows 10 beheben	24
Quick Tipp:	24
Bereitstellen von Paketen für Windows 10	25
Bereitstellen allgemeiner Einstellungen für die Erstbereitstellung für PCs (Desktop-Assistent)	25

Windows 10 Unterschiede

Find out which
Windows 10 edition
 is right for you.



Try Windows today >

Core features Business features

Existing Fundamentals	Home	Pro	Enterprise	Education
Device Encryption ⁶	x	x	x	x
Domain Join		x	x	x
Group Policy Management		x	x	x
BitLocker ²		x	x	x
Enterprise Mode Internet Explorer (EMIE)		x	x	x
Assigned Access 8.1		x	x	x
Remote Desktop		x	x	x
Direct Access			x	x
Windows To Go Creator			x	x
AppLocker			x	x
BranchCache			x	x
Start Screen Control with Group Policy			x	x

Management and Deployment

Side-loading of line of business apps	x	x	x	x
Mobile device management	x ⁸	x	x	x
Ability to join Azure Active Directory, with single sign-on to cloud-hosted apps ^{7,8}		x	x	x
Business Store for Windows 10 ⁸		x	x	x
Granular UX Control			x	x
Easy Upgrade from Pro to Enterprise Edition		x	x	
Easy Upgrade from Home to Education Edition	x			x

Security

	Home	Pro	Enterprise	Education
Microsoft Passport	x	x	x	x
Enterprise Data Protection ⁸		x	x	x
Credential Guard ⁹			x	x
Device Guard ⁹			x	x

Delivering Windows as a Service

Windows Update	x	x	x	x
Windows Update for Business		x	x	x
Current Branch for Business		x	x	x
Long Term Servicing Branch			x	

Treiber:

Es kommt vor, dass Windows nicht alle Treiber automatisch erkennt. In so einem Fall kann man folgendes tun:

Hardware-ID suchen, dann auf PCIDatabase.com

Treiber sichern:

Folgenden Ordner in Netzfriegabe sichern:

C:\Windows\System32\DriverStore\FileRepository

weitere Treiber Infos

Mit dem Kommandozeilentool "**pnputil.exe**" können Sie sich die Treiber aus dem Driver Store von Windows anzeigen lassen. Der Driver Store liegt unter "**%SystemRoot%\System32\DriverStore**", hier werden alle Treiber abgelegt, die dem **System** bekannt sind.

Nicht mehr benötigte, fehlerhafte oder alte Treiber können wieder entfernt oder auch neue Treiber hinzufügen werden, ohne dafür die entsprechende Hardware haben zu müssen.

Der Driver Store wird benötigt, wenn sich normale Anwender (ohne administrative Berechtigungen) am System anmelden und entsprechende Plug&Play Hardware anschließen. Diesen Anwender können nur Treiber aus den Verzeichnis zur Verfügung gestellt werden.

Über den Befehl "**pnputil -e**" werden alle Treiber von anderen Herstellern aufgelistet, die sich im Driver Store befinden.

Über den Befehl "**pnputil -d [treibername]**" können Sie einen entsprechenden Treiber entfernen.

Eine Übersicht der Parameter erhalten Sie über **pnputil /?**

Parameter	Beschreibung
-e	Alle Drittanbieterpakete auflisten
-d [Treibername]	Paket löschen: Beispiel: pnputil -d oem1.inf
-f -d [Treibername]	Löschen des Paketes erzwingen
-a [Verzeichnis\Datei]	Pakete hinzufügen Beispiel: pnputil -a c:\drv\oem11.inf (Sie können auch mit Wildcard arbeiten. Also C:\drv*.inf fügt alle Treiber aus dem Verzeichnis drv hinzu).

-i -a
[Verzeichnis\Datei]

CMD Tipps:

CMD als Admin öffnen wenn die CMD bereits gestartet ist:

- In der Taskleiste auf das CMD Fenster bei gedrückter STRG+Shift Taste mit links klicken.

Weitere TIPPS:

- F7 öffnet die History mit Nummern:
- F9 zum Auswählen
- Farbe Ändern: Color f0

Windows X öffnet das wichtigste Kontextmenu von Windows 10

BCDEdit ist ein Befehlszeilentool zum Verwalten von BCD-Speichern. Das Programm kann vielfältig verwendet werden, u. a. zum Erstellen neuer Speicher, Ändern vorhandener Speicher und Hinzufügen von Startmenüoptionen usw. BCDEdit dient im Wesentlichen demselben Zweck wie Bootcfg.exe

Mehr Details:

[https://technet.microsoft.com/de-de/library/cc709667\(v=ws.10\).aspx](https://technet.microsoft.com/de-de/library/cc709667(v=ws.10).aspx)

PowerShell

Computer-Kennwort zurücksetzen

Reset-ComputerMachinePassword Setzt das Kennwort für das Computerkonto des Computers zurück.

-Server <string>

Gibt den Namen des zu verwendenden Domänencontrollers beim Festlegen des Kennworts für das Computerkonto an.

- PowerShell ISE : Zum testen eines Scriptes
- TAB: Die ersten Buchstaben des Befehls eingeben und dann mit TAB
- Shift + TAB = ZURÜCK

Dieser Parameter ist optional. Wenn Sie diesen Parameter weglassen, wird ein Domänencontroller zum Behandeln des Befehls ausgewählt.

PowerShell Remote ausführen

Invoke-Command -Computername Server-1, Server-2 {Befehle}

BitLocker

Unterscheiden muss man: Datenverschlüsselung und Festplattenverschlüsselung

In welchen Versionen ist es enthalten

Pro und Enterprise

Wie arbeitet BitLocker

Festplatte:

Man benötigt 2 Partitionen

1.) System-Reserve

2.) TPM Modul (**Trusted Plattform Modul**) **Chip**: Neuere PCs haben einen TPM Chip 1.2 oder höher. Die Verschlüsselungen kann somit auf diesen Chip gespeichert werden. D.h. die Verschlüsselungs-Informationen werden auf der Hardware gespeichert.

BitLocker verschlüsselt die Festplatte anhand eines Schlüssels (Private oder öffentliche Schlüssel- Full-Volume encryption Key, wird in der Systemreserve abgespeichert). Dieser wird durch den "Volume Master Key" verschlüsselt-Dieser wird im TPM Modul abgespeichert.

Welche Möglichkeiten habe ich zur Wiederherstellung bei Verlust des Full-Volume encryption Keys

- Wiederherstellungsagenten über GPO und Zertifikate
- 56 Zeichen Langer Schlüssel falls der Full Volume Decryption verloren geht oder ich kann diesen über ein Windows internes Tool wiederherstellen.

Quick-Tipp:

BadUsb Sticks: Tarnen sich als Tastatur :

<https://github.com/brandonlw/Psychson>

Storage Spaces (Seit Windows 8 und Windows Server 2012)

Was macht es: Erzeugt aus egal welchen Platten ein Just Bond of Discs (JBOD). Im Gegensatz zu einem Raid Controller.

Es gibt folgende Möglichkeiten:

Simple

steht analog zu RAID 0 für Striping. Es erzielt von den 3 Verfahren die beste Performance, weil jeder Schreibvorgang gleichzeitig auf mehrere Platten verteilt wird. Dafür bietet diese Variante keine Redundanz und damit auch keine Ausfallsicherheit. Man kann sie aber schon mit einer Disk nutzen und hält sich damit Möglichkeit offen, bei Bedarf später weitere Laufwerke hinzuzufügen. *Mirror* setzt mindestens 2 Disks voraus. Da es sich nicht um eine einfache File-basierte Plattenspiegelung handelt, können für das Mirroring auch mehrere Platten verwendet werden. Windows verteilt die Daten in Blöcken von 256MB oder Vielfachen davon ("slabs") über die verschiedenen Datenträger. Sind 2 vorhanden, dann verkraftet Mirroring den Ausfall von einer Disk, bei einem 3er-Paket sogar von 2.

Mirror

ist der Vorgabewert im Assistenten, weil es den besten Kompromiss zwischen Performance und Sicherheit bietet. Sein Nachteil besteht im relativ hohen Platzverbrauch.

Parity

funktioniert nach dem Muster von RAID 5 und setzt daher mindestens 3 Laufwerke in einem Storage-Pool voraus. Es bietet Redundanz bei geringerem Platzverbrauch, dafür geht die Berechnung des Parity-Bits auf Kosten der Performance, vor allem bei Schreibzugriffen. Daher eignet sich diese Variante vor allen für große Dateien, die nicht allzu oft verändert werden, etwa für Videos. Sie lässt sich jedoch nicht in Failover-Clustern einsetzen.

Remote Session über PowerShell

Starten einer interaktiven Sitzung:

```
Enter-PSSession Server01
```

Um die interaktive Sitzung zu beenden, geben Sie Folgendes ein:

```
Exit-PSSession
```


Ausführen eines Remote- Befehls (Run a Remote Command)

Zum Ausführen eines Befehls auf einem oder mehreren Remotecomputern verwenden Sie das Cmdlet [Invoke-Command](#). To run any command on one or many remote computers, use the [Invoke-Command](#) cmdlet. Um beispielsweise einen [Get-UICulture](#)-Befehl auf den Remotecomputern „Server01“ und „Server02“ auszuführen, geben Sie Folgendes ein:

```
Invoke-Command -ComputerName Server01, Server02 {Get-Hostname}
```

Ausführen eines Skripts / Run a Script

Zum Ausführen eines Skripts auf einem oder mehreren Remotecomputern verwenden Sie den Parameter „FilePath“ des Cmdlets „Invoke-Command“. To run a script on one or many remote computers, use the FilePath parameter of the Invoke-Command cmdlet. Das Skript muss sich auf dem lokalen Computer befinden oder für diesen verfügbar sein.

```
Invoke-Command -ComputerName Server01, Server02 -FilePath c:\Scripts\DiskCollect.ps1
```

Mehr Infos:

<https://docs.microsoft.com/de-de/powershell/scripting/core-powershell/running-remote-commands?view=powershell-5.1>

IPv6

FE80::/ 64 Link Local (APIPA)

FD00:: /16 Privat dann folgt die Netzkennung und die hinteren Blöcke Host

FF00::/ 8 Multicast 00 FLAG BITS

Quick-Tipp:

Kerberos Ticket verwerfen:

klist purge

UE-V

Mit UE-V werden Windows-Betriebssystem- und Anwendungseinstellungen dem Benutzer zentral bereitgestellt. D.h. der Benutzer findet an jedem Computer, Notebook, Tablet oder jeder VDI-Sitzung, an dem er sich anmeldet, immer die gleichen Einstellungen seiner Anwendungen vor. Auch diese Templates sind nicht lokal auf dem jeweiligen Rechner

vorhanden, sondern werden zentralisiert auf einem Server gespeichert. Standardmäßig werden von Microsoft Templates für alle Microsoft Anwendungen bereits mitgeliefert, die dann noch entsprechend angepasst werden können.

Ebenso wie bei App-V, handelt es sich bei UE-V nicht um eine einzelne Anwendung, sondern auch um mehrere Komponenten. Dies sind der

- UE-V Agent,
- UE-V Template Generator und
- das Company Settings Center.

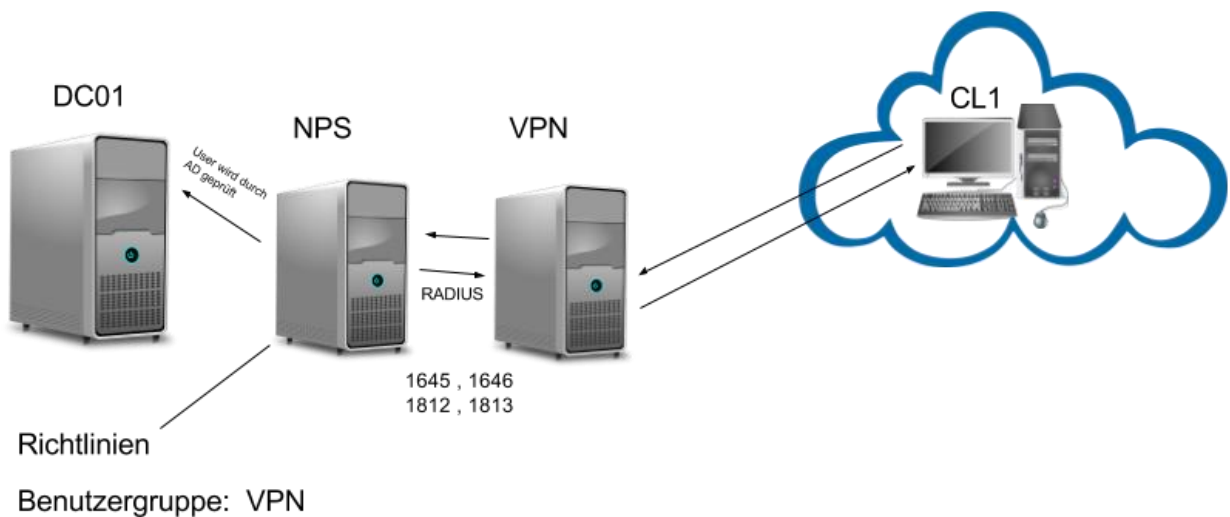
Auch für die UE-V Komponenten erfolgt eine detaillierte Beschreibung im dritten Teil dieser Blogserie. Bis zur Version 1511 waren die UE-V Komponenten ebenfalls ausschließlich über das MDOP-Paket erhältlich. Die letzte veröffentlichte Version von UE-V innerhalb des MDOP-Paketes war 2.1 SP1. Mit der Version 1607 hat sich dies nun ebenfalls geändert. Der UE-V Agent ist jetzt, ebenso wie der App-V Client, direkt in Windows 10 integriert. Zusätzlich hat sich noch der Name geändert. Der UE-V Agent heißt jetzt UE-V Service. Der UE-V Template Generator ist ausschließlich über das Windows ADK erhältlich. Dagegen wurde der Company Settings Generator entfernt und ist nicht länger verfügbar.

UE-V Generator Templates erstellen und anwenden

<https://www.einfaches-netzwerk.at/ue-v-generator-templates/>

VPN unter Windows 10

Grundsätzlich



Hinzufügen oder Ändern einer VPN-Verbindung unter Windows 10

Eine VPN-Verbindung bietet Ihnen mehr Sicherheit beim Herstellen einer Verbindung mit Ihrem Firmennetzwerk oder dem Internet.

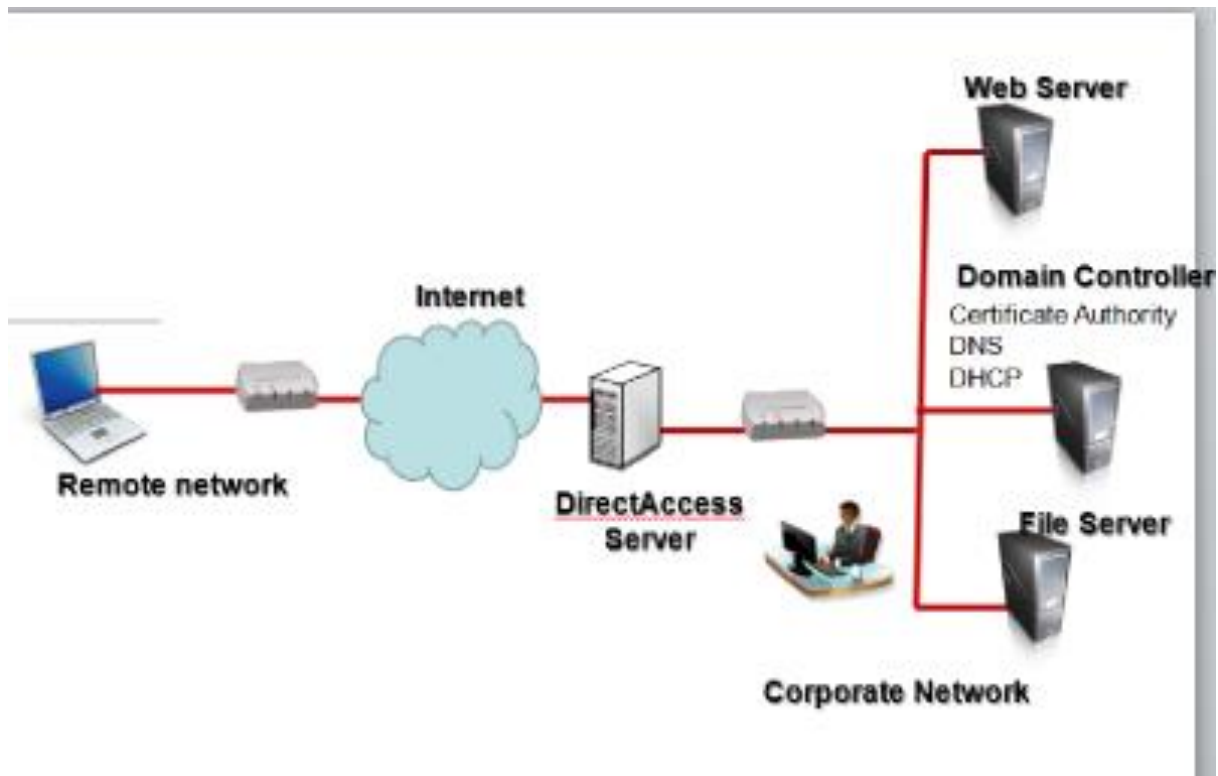
- So erstellen Sie eine neue VPN-Verbindung: Wählen Sie **Start** Windows logo Start button > **Einstellungen** Gear-shaped Settings icon > **Netzwerk und Internet** > **VPN** > **VPN-Verbindung hinzufügen** aus.
 1. Wählen Sie unter **VPN-Anbieter** die Option **Windows (integriert)** aus.
 2. Geben Sie im Feld **Verbindungsname** einen Anzeigenamen für das VPN-Verbindungsprofil ein.
 3. Geben Sie im Feld **Servername oder -adresse** die Adresse des VPN-Servers ein.
 4. Wählen Sie unter **VPN-Typ** den Typ der zu erstellenden VPN-Verbindung aus. Sie müssen wissen, welche Art von VPN-Verbindung Ihr Unternehmen oder VPN-Dienst verwendet.

5. Wählen Sie unter **Anmeldeinformationstyp** den Typ der zu verwendenden Anmeldeinformationen aus.
 6. Wählen Sie nun **Speichern** aus.
- Wenn Sie ein VPN-Profil eingerichtet haben, können Sie eine Verbindung herstellen.
 - Wählen Sie ganz rechts auf der Taskleiste das Symbol **Netzwerk** aus. Wählen Sie unter der gewünschten VPN-Verbindung **Verbinden** aus. Alternativ können Sie **Einstellungen** Gear-shaped Settings icon > **Netzwerk und Internet** > **VPN** öffnen und die VPN-Verbindung dort auswählen. Geben Sie bei der entsprechenden Aufforderung Ihre Anmeldeinformationen ein. Wenn die Verbindung hergestellt wurde, wird unter dem Namen der VPN-Verbindung **Verbunden** angezeigt.
 - Wenn Sie die VPN-Verbindungsinformationen bearbeiten oder weitere Einstellungen festlegen möchten, wählen Sie die VPN-Verbindung unter **Einstellungen** Gear-shaped Settings icon > **Netzwerk und Internet** > **VPN** und dann **Erweiterte Optionen** aus.

Was ist DirectAccess

DirectAccess mit Windows 10

Am besten geeignet ist Windows 10, da Microsoft in der neuen Windows-Version die Verschlüsselung verbessert und beschleunigt hat. Windows 7 verschlüsselt die Verbindungen von DirectAccess zusätzlich noch mit SSL/TLS, obwohl die Verbindung bereits durch IPsec verschlüsselt ist. Das erzeugt einen Overhead, der die Leistung der Verbindung mindert.



Außerdem kann Windows 10 mehr gleichzeitige Kanäle zwischen Notebook und Firmennetzwerk aufbauen, was die Leistung verbessert. Ab Windows 10 dürfen die DirectAccess-Server in einer DMZ positioniert sein, die durch ein Edge-Security-System mit NAT angebunden ist.

Zusätzlich unterstützt DirectAccess mit Windows 10 die Anbindung in einer Multi-Site-Umgebung. Dadurch lassen sich geografische Redundanzen erreichen, da Windows 10-Rechner mit allen konfigurierten Endpunkten eine Verbindung aufbauen können – was unter Windows 7/8/8.1 nicht möglich ist. Dabei initiiert Windows 10 einen Verbindungsaufbau zu dem Verbindungspunkt, der am schnellsten erreichbar ist und kann bei einem Ausfall automatisch einen Wechsel vornehmen.

Außerdem ist die Verwaltung von DirectAccess in Windows 10 über die grafische Oberfläche wesentlich besser steuerbar – lässt sich aber auch über die PowerShell managen

Erweiterte Informationen für Admins:

https://www.msxfaq.de/windows/directaccess/directaccess_namensaufloesung_nrpt.htm

DirectAccess-Server mit Windows Server 2012 R2/2016 einrichten

Die Installation von DirectAccess und Remotezugriff erfolgt in Windows Server 2012 R2 mithilfe des Server-Managers. Über "Verwalten/Rollen und Funktionen hinzufügen/Remotezugriff" installieren Sie die notwendigen Funktionen auf dem Server (siehe Abbildung 1). Die Installation kann auch über die PowerShell erfolgen. Dazu wird der Befehl "Install-WindowsFeature DirectAccess-[VPN](#) -IncludeManagementTools" verwendet.

Administratoren starten die Einrichtung über die Remotezugriffs-Verwaltungskonsole. Diese ist im Menüpunkt "Tools" des Server-Managers zu finden (siehe Abbildung 2). Durch die Einrichtung führt ein Assistent, über den alle notwendigen Konfigurationen vorgenommen werden können.

Im Rahmen der Einrichtung werden zunächst die Topologie des Netzwerkes und der Standort des DirectAccess-Servers ausgewählt. Außerdem können Administratoren für den Zugriff den FQDN oder die öffentliche IP-Adresse angeben. Danach richtet der Assistent die notwendigen Funktionen ein, und erstellt Gruppenrichtlinien, um die Konfiguration an die DirectAccess-Clients zu verteilen (siehe Abbildung 4).

DirectAccess in der RemoteAccess Management Console verwalten

Nach der ersten Einrichtung erfolgt die weitere Konfiguration in der RemoteAccess Management Console. Diese startet automatisch nach der ersten Konfiguration (siehe Abbildung 5). Administratoren können diese aber auch jederzeit mit dem Befehl "ramgmtui" starten. Über verschiedene Schritte lässt sich die Konfiguration jetzt an die eigenen Anforderungen anpassen.

Standardmäßig erlaubt der Einrichtungs-Assistent den Zugriff per DirectAccess für alle Domänencomputer. Diese Einstellung sollten Administratoren anpassen und eine eigene Sicherheitsgruppe erstellen. Computer, deren Konten Mitglied in dieser Gruppe sind, dürfen sich dann über DirectAccess verbinden.

Clients mit der DirectAccess-Konfiguration anbinden

Nach der Einrichtung von DirectAccess erhalten Clientcomputer die Konfiguration über die Gruppenrichtlinien, die der Assistent konfiguriert hat. Die Verwaltung findet am besten in der PowerShell statt. "Get-DnsClientNrptPolicy" zeigt die Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) von Direct Access an. "Get-NCSPolicyConfiguration" zeigt die vom Assistenten bereitgestellten Einstellungen für die Statusanzeige der Netzwerkkonnektivität an.

Administratoren können die Einstellungen über die Verwaltungskonsole anpassen. Die Optionen sind im Bereich "Infrastrukturserver-Setup" über "Bearbeiten" zu erreichen. Hier können Administratoren den Server und das dazugehörige Zertifikat auswählen, über den ein Client überprüfen kann, ob er sich gerade im Firmennetzwerk befindet, oder ob er von außerhalb verbunden ist und DirectAccess nutzen muss (siehe Abbildung 6).

Clients, die per DirectAccess verbunden sind, finden Administratoren über den Link "Remoteclientstatus" in der Remotezugriffs-Verwaltungskonsole. Die Gruppenrichtlinien für die Anbindung an DirectAccess erstellen Firewallregeln und Verbindungssicherheitsregeln. Diese lassen Sie über "wf.msc" auf dem Client anzeigen (siehe Abbildung 7). Während der

Einrichtung legt der Assistent auch [DNS](#)-Einträge fest, mit denen er überprüfen kann, ob sich Clients im internen Netzwerk befinden oder über DirectAccess verbunden sind. Verbindet sich ein Client mit DirectAccess, sehen Anwender die Verbindung, wenn sie auf das Netzwerksymbol klicken. Der Befehl "Get-DAConnectionStatus" zeigt "ConnectedRemotely" an, wenn ein Computer von außerhalb verbunden ist, also DirectAccess nutzt.

Microsoft Windows DirectAccess Client Troubleshooting Tool

Auch wenn DirectAccess generell recht einfach einzurichten ist, und Microsoft Assistenten für die Konfiguration zur Verfügung stellt, ist das Troubleshooting nicht gerade trivial. Microsoft bietet zur Fehlerbehebung das Werkzeug "[Microsoft Windows DirectAccess Client Troubleshooting Tool](#)" kostenlos an, mit dem Anwender auf ihren Rechnern die Anbindung testen können. Das Tool ist aktuell noch nicht für Windows 10 freigegeben, funktioniert aber bereits (siehe Abbildung 8). Um das Tool zu verwenden, muss es nur aufgerufen werden, eine Installation ist nicht notwendig.

Damit DirectAccess auf einem Rechner funktioniert, müssen die erstellten Gruppenrichtlinien angewendet werden. Dazu können Administratoren auf den Ziel-Rechnern die Befehle "rsop.msc" oder "gpresult /r" nutzen. Damit lässt sich überprüfen, ob die Richtlinien übertragen wurden. Nach einer Änderung der Gruppenmitgliedschaft müssen Computer neu gestartet werden, um die Richtlinien zu übernehmen. Zudem muss die Firewall auf den Rechnern gestartet sein.

Offline-Domänenaufnahme mit Djoin.exe

In Windows Server 2008 R2 lassen sich mit dem Tool Djoin Computerkonten von Windows 7- Computern auch dann einer Domäne hinzufügen, wenn diese aktuell keine Verbindung mit dem Domänencontroller haben. Sobald der Client eine Verbindung aufbaut, wendet er die notwendigen Einstellungen und Berechtigungen an, die für eine Domänenaufnahme notwendig sind. So ist es zum Beispiel möglich, Clients von Niederlassungen in Domänen aufzunehmen, wenn aktuell keine Verbindung zur Domäne besteht. Dieser Workshop zeigt die Offline-Domänenaufnahme mit und ohne Antwortdatei.

In Windows Server 2008 R2 lassen sich mit dem Tool Djoin Computerkonten von Windows 7- Computern auch dann einer Domäne hinzufügen, wenn diese aktuell keine Verbindung mit dem Domänencontroller haben. Sobald der Client eine Verbindung aufbaut, wendet er die notwendigen Einstellungen und Berechtigungen an, die für eine Domänenaufnahme notwendig sind. So ist es zum Beispiel möglich, Clients von Niederlassungen in Domänen aufzunehmen, wenn aktuell keine Verbindung zur Domäne besteht.

Dieser Workshop zeigt die Offline-Domänenaufnahme mit und ohne Antwortdatei. Wollen Sie zum Beispiel viele virtuelle Computer auf einmal in die Domäne aufnehmen, beispielsweise in einem Virtual Desktop Infrastructure-Szenario, können Sie das Active Directory so vorbereiten, dass sich die Computer schnell und problemlos anbinden lassen. Sobald ein

solcher Client das erste Mal startet, führt er die notwendigen Änderungen durch – ein erneuter Start des Rechners ist daher nicht notwendig.

Das beschleunigt auch das Bereitstellen von Windows 7-Computern im Netzwerk. Djoin funktioniert auch zusammen mit schreibgeschützten Domänencontrollern (RODC). Dazu nehmen Sie mit Djoin die Computer auf und lassen die Konten zum RODC replizieren. Sobald sich die Computer in der Niederlassung mit dem Netzwerk verbinden, authentifizieren sie sich am schreibgeschützten Domänencontroller und sind im Active Directory verfügbar. Ein weiterer Vorteil ist die automatisierte Domänenaufnahme von neuen Computern beim Deployment von Windows 7 im Unternehmen, indem Sie die notwendigen Befehle für die Domänenaufnahme in die Antwortdatei der automatischen Installation aufnehmen.

Voraussetzungen für die Verwendung

Damit Sie die Offline-Domänenaufnahme verwenden können, müssen Sie Windows 7 oder Windows Server 2008 R2 als Betriebssystem einsetzen. Sie können diese Betriebssysteme aber auch in Domänen aufnehmen, die noch keine Domänencontroller unter Windows Server 2008 R2 betreiben. In diesem Fall verwenden Sie die Option `"/downlevel"`. Standardmäßig geht Djoin davon aus, dass eine Verbindung zu einem Domänencontroller unter Windows Server 2008 R2 besteht. Zusammenfassend heißt das, dass Sie nur Computer, auf denen Windows 7 oder Windows Server 2008 R2 installiert ist, per Djoin zu einer Domäne aufnehmen können. Bei der Domäne kann es sich auch um ein Active Directory unter Windows Server 2008 handeln.

Nur Benutzer, die über die Rechte verfügen, Computer einer Domäne hinzuzufügen, können Djoin nutzen. Dazu müssen Sie entweder über Domänen-Adminrechte verfügen oder ein Administrator muss die entsprechenden Rechte delegieren. Die Rechte, Computer in eine Domäne aufzunehmen, setzen Sie über Gruppenrichtlinien. Bearbeiten Sie dazu den Wert "Hinzufügen von Arbeitsstationen zur Domäne" unter "Computerkonfiguration / Richtlinien / Windows-Einstellungen / Sicherheitseinstellungen / Lokale Richtlinien / Zuweisen von Benutzerrechten". Nehmen Sie hier die Benutzerkonten auf, die über die entsprechenden Rechte verfügen sollen.

Durchführen der Offline-Domänenaufnahme

Die Offline-Domänenaufnahme erfolgt über Djoin in der Befehlszeile auf einem Computer unter Windows 7 oder Windows Server 2008 R2, der bereits Mitglied der Domäne ist. Sie müssen für die Verwendung über das Kontextmenü eine Eingabeaufforderung mit Administratorrechten starten und über Rechte verfügen, Computerkonten zur Domäne hinzuzufügen. Die Ausgabe in die Datei oder auf dem Bildschirm enthält die Metadaten für die Domänenaufnahme. Microsoft bezeichnet diese auch als "Blob".

Bei der Ausführung können Sie entweder eine verschlüsselte Datei erstellen, die Sie auf dem Clientrechner dann verwenden müssen oder Sie speichern die Daten in einer Datei

unattend.xml, um Antwortdateien vollkommen zu automatisieren. Das Tool Djoin.exe hat verschiedene Optionen, die wir im Kasten am Ende des Artikels genauer auflisten.

Generell ist der Ablauf bei einer Domänenaufnahme recht einfach: Zunächst erstellen Sie mit *djoin /provision* Metadaten für die Domänenaufnahme des Zielcomputers. Als Option geben Sie die Domäne an. Achten Sie darauf, dass Sie die Eingabeaufforderung im Administratormodus öffnen. Ein Beispiel für die Datei wäre

```
djoin /provision /domain contoso.com  
/machine client134 /savefile  
c:\client134.txt.
```

Inhalt der Datei sind das Kennwort der Maschine, Name der Domäne und des Domänencontrollers, sowie die SID der Domäne. Kopieren Sie die Datei auf den Rechner. Der Inhalt ist verschlüsselt und von Außenstehenden nicht lesbar. Auf dem Zielcomputer verwenden Sie

```
djoin /requestODJ /loadfile  
c:\client134.txt /windowspath  
{SystemRoot} /localos
```

um den Rechner zur Domäne aufzunehmen. Starten Sie den Zielcomputer, wird der Computer automatisch in die Domäne aufgenommen, sobald eine Verbindung zu einem Domänencontroller besteht.

Offline-Domänenaufnahme bei einer unbeaufsichtigten Installation über Antwortdatei

Wollen Sie eine Offline-Domänenaufnahme während der Installation, zum Beispiel im unbeaufsichtigten Modus durchführen, ist das ebenfalls möglich. Dazu müssen Sie beim Erstellen des Computerkontos auf der Domäne den Inhalt der Metadaten statt in einer verschlüsselten Datei in eine Antwortdatei integrieren. Antwortdateien unter Windows Server 2008 R2 und Windows 7 tragen normalerweise die Bezeichnung *Unattend.xml*. Sie müssen in der Antwortdatei dazu eine neue Sektion erstellen. Diese trägt die Bezeichnung "Microsoft-Windows-UnattendJoin / Identification / Provisioning". Diese Sektion enthält darüber hinaus eine Unterstruktur, die folgendermaßen aussieht:

```
<Component>  
  <Component name=Microsoft-Windows-UnattendedJoin>  
    <Identification>  
      <Provisioning>  
        <AccountData>Base64Encoded Blob</AccountData>  
      </Provisioning>  
    </Identification>  
  </Component>
```

Sie müssen die Metadaten, die Sie beim Erstellen der Datei erhalten, zwischen die Tags "<AccountData>" und "</AccountData>" einfügen. Nachdem Sie die Datei erstellt haben,

können Sie den Computer unbeaufsichtigt installieren. Die Syntax bei Antwortdateien ist *setup /unattend:{Antwortdatei}*.

Optionen von djoin.exe

/provision

Erstellen eines Computerkontos in der Domäne.

/domain {Name der Domäne}

Domäne, in der Sie das Konto erstellen wollen.

/machine {Name}

Name des Computers, den Sie zur Domäne hinzufügen.

/machineou {Organisationseinheit}

OU, in der das Konto erstellt werden soll. Ohne Angabe einer OU verwendet Djoin die OU Computer.

/dcname {Name}

Name des Domänencontrollers, auf dem das Konto zuerst verfügbar sein soll.

/reuse

Verwenden eines bereits vorhandenen Computerkontos, dessen Kennwort zurückgesetzt wird.

/downlevel

Aufnehmen eines Computers auf einem Domänencontroller, auf dem nicht Windows Server 2008 R2 installiert ist.

/savefile {Name der Datei}.txt

Verschlüsselte Textdatei mit den Daten der Domänenaufnahme für die Ausführung auf dem Client.

/defpwd

Verwendet das standardmäßige Kennwort für Computerkonten (nicht notwendig).

/nosearch

Überspringt Konflikte, wenn das Konto bereits vorhanden ist. Benötigt die Option "/dcname".

/printblob

Gibt einen base64-kodierten Wert für Antwortdateien aus.

/requestodj

Führt eine Offline-Domänenaufnahme beim nächsten Neustart aus.

/loadfile

Verwendet die Ausgabe einer vorherigen Ausführung von djoin.exe.

/windowspath {Pfad}

Pfad zum Windows-Verzeichnis, wenn nicht der Standard verwendet werden soll.

/loalos

Zielcomputer, den Sie der Domäne hinzufügen wollen (nicht auf einem Domänencontroller ausführbar).

Lösen von Problemen bei Dateizugriff

Zugriff verweigert oder Fehler beim Zugreifen auf und Bearbeiten von Dateien und Ordnern in Windows

<https://support.microsoft.com/de-at/help/2623670/-access-denied-or-other-errors-when-you-access-or-work-with-files-and>

NTFS-Berechtigungen richtig einrichten

<https://www.tecchannel.de/a/windows-praxis-ntfs-berechtigungen-richtig-einrichten,2034293,5>

Access-based Enumeration

<https://www.tecchannel.de/a/access-based-enumeration,461619,2>

Was sind Bedingungen im Bereich der Sicherheitseinstellungen (ab 2012 Server)

Mehr Informationen:

[https://technet.microsoft.com/en-us/library/jj134043\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj134043(v=ws.11).aspx)

EFS (Encrypting File System)

EFS ist eine Datenverschlüsselungs-Technologie, die auf einzelne oder alle Dateien in einem Ordner angewendet werden kann. Die mit EFS verschlüsselten Dateien können ohne die entsprechenden Schlüsselinformationen nicht entschlüsselt werden. Dabei ist zu beachten, dass EFS, im Gegensatz zur Microsoft BitLocker™-Laufwerksverschlüsselung (BitLocker), nicht auf Dateien angewendet werden kann, die für das Starten des Betriebssystems benötigt werden.

Probleme mit EFS

In bestimmten Situationen kann es zu Problemen beim Zusammenspiel von LDAP, dem EFS und TCP/IP kommen, die dazu führen, dass TCP-Verbindungen nicht korrekt geschlossen werden. Im Extremfall kann es dadurch passieren, dass kein weiterer Zugriff auf den Server erlaubt wird, weil die maximale Zahl der LDAP-Verbindungen erreicht ist. Falls mit dem EFS gearbeitet wird, sollte im Artikel 891307 der Knowledge Base überprüft werden, ob das Problem in der eigenen Umgebung auftreten kann.

Wie kann man Daten wiederherstellen

Die verschlüsselten Dateien dem Computer zugänglich machen, auf dem der Recovery Key gespeichert ist und dann dort das Verschlüsselungs-Häkchen wegnehmen. Bei vielen Dateien würde ich mir cipher.exe ansehen:

```
cipher /a /d /s:<directory name>
```

- /a alle Dateien (auch in Unterverzeichnissen)
- /d entschlüsseln
- /s: Verzeichnisname

Lösen von Problemen mit Druckern

Welche Probleme gibt es

- Druckertreiber falsch
- Druckertreiber defekt
- Zugriff auf Drucker
- Netzwerkprobleme
- Drucker aus

Was ist bei Druckertreibern zu beachten

Viele Anbieter bieten unterschiedliche Druckertreiber an:

- PCL 5 -Treiber
- PCL 6 -Treiber
- PostScript -Treiber bzw. KPD L Treiber
- Universal Drucker Treiber

Diese gibt es für unterschiedliche Betriebssysteme. Hier sollte man den richtigen wählen.

Zudem bieten einige Druckerhersteller mehrere Treiber an, die unterschiedliche Einstellmöglichkeiten anbieten:

Beispiel Kyocera KX-Treiber

Druckertreiber in der richtigen Version:

- 32-Bit Treiber
- 64-Bit Treiber

Verwenden Sie stets einen Microsoft signierten Treiber !

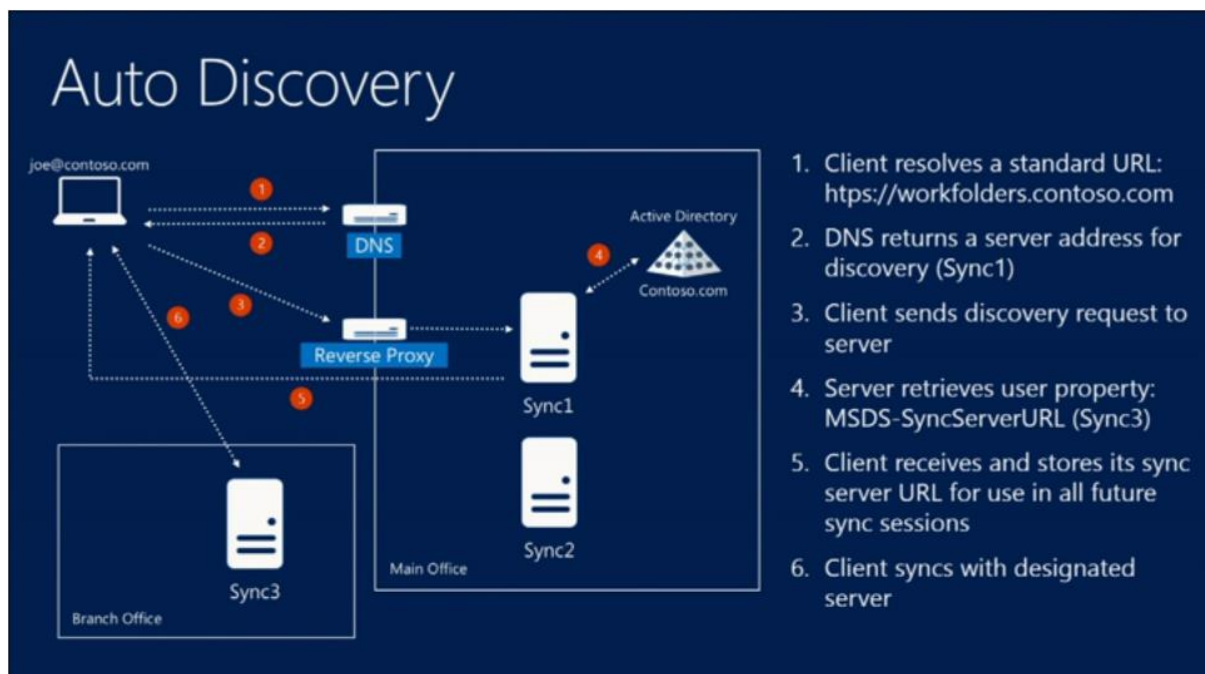
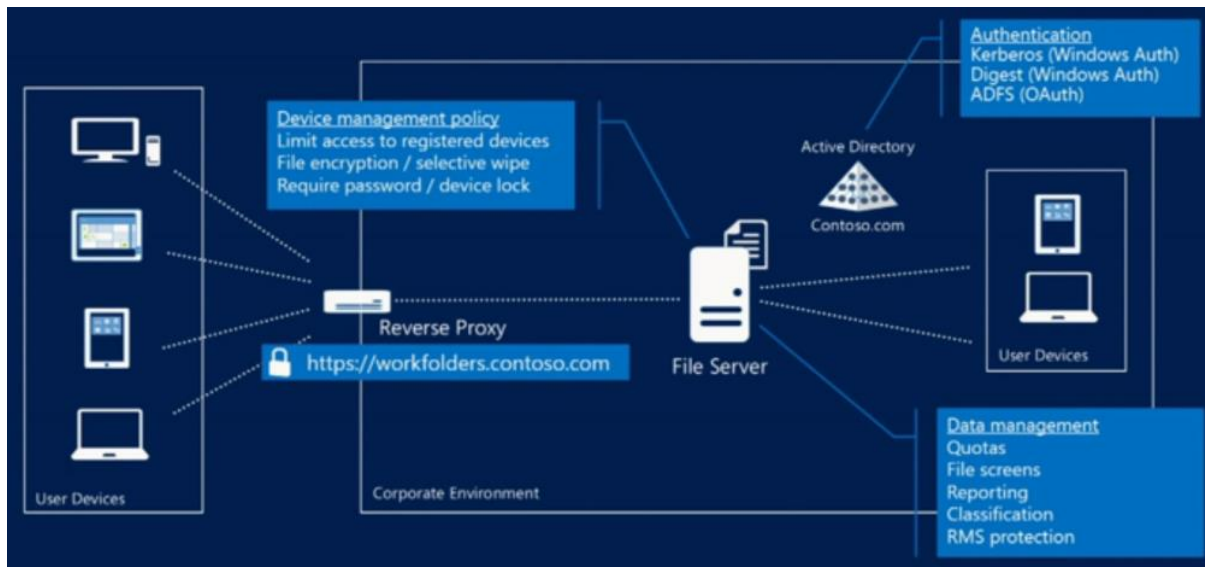
Was lässt sich in den Eigenschaften eines Druckers konfigurieren

- Format
- Fach
- Spooler
- u.v.m.

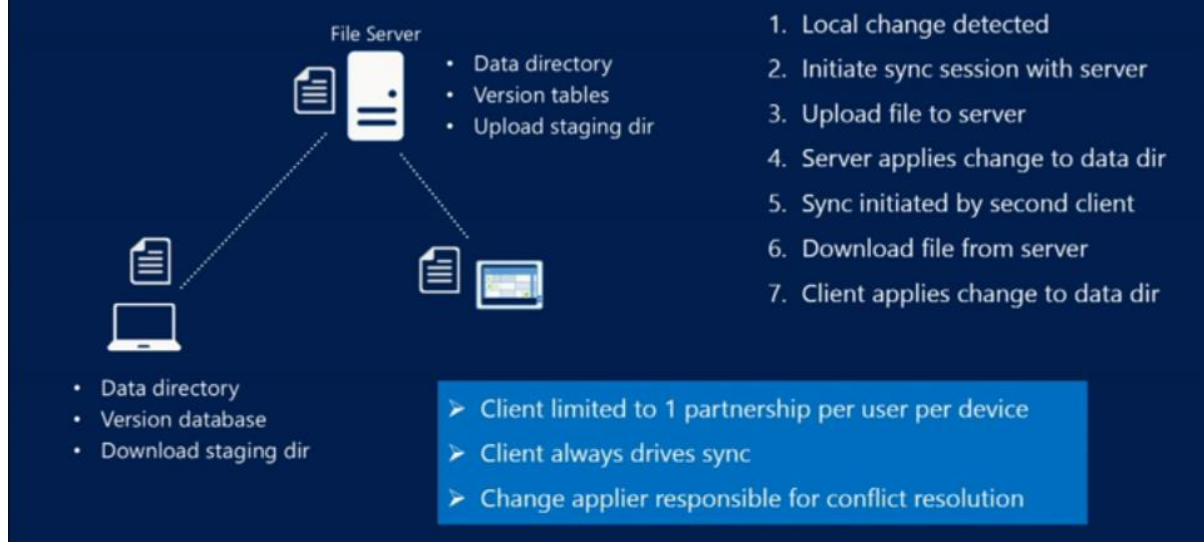
Microsoft Workfolders (Arbeitsordner)

Arbeitsordner ermöglichen die Verwendung von Arbeitsdateien auf verschiedenen Computern, einschließlich Arbeitsgeräten und persönlichen Geräten. So können mithilfe von

Arbeitsordnern Benutzer Dateien hosten und synchronisieren – unabhängig davon, ob Benutzer im Netzwerk oder über das Internet auf ihre Dateien zugreifen. = Dropbox on Premise.



How A File Stays In Sync



Rolle installieren

1. Auf dem Fileserver den Server Manager öffnen
2. Rollen hinzufügen auswählen
3. Datei und Speicherdienste → Datei und iSCSI Dienste → Arbeitsordner auswählen → erforderliche Features hinzufügen → Weiter ([Bild 1](#))
4. Den Assistenten abschließen und Rollendienst installieren lassen
5. Über den Server Manager zu Arbeitsordner navigieren ([Bild 2](#))
6. Den Einrichtungsassistenten öffnen mit Klick auf „Starten Sie zum Erstellen eine neuen...“
 1. Vorbereitungsfenster → Weiter ([Bild 3](#))
 2. Server und Pfad bestimmen → Weiter ([Bild 4](#))
 3. Benutzerordnerstruktur konfigurieren → Weiter ([Bild 5](#))
 4. Namen der Synchronisierungsfreigabe festlegen → Weiter ([Bild 6](#))
 5. Synchronisierungszugriff definieren → Weiter ([Bild 7](#))
 6. Geräterichtlinien Konfigurieren → Weiter ([Bild 8](#))
 7. Bestätigung und Übersicht → Weiter ([Bild 9](#))
 8. Freigabe wurde erstellt → Fertig ([Bild 10](#))
7. Fertig

Hinweise zur Benutzerordnerstruktur (Quelle: TechNet):

Benutzeralias erstellt Benutzerordner, die keinen Domännennamen enthalten. Wählen Sie diese Benennungskonvention aus, wenn Sie eine Dateifreigabe verwenden, die bereits mit

der Ordnerumleitung oder einer anderen Benutzerdatenlösung genutzt wird. Optional können Sie das Kontrollkästchen **Nur den folgenden Unterordner synchronisieren** aktivieren, um nur einen bestimmten Unterordner zu synchronisieren, z. B. den Ordner „Dokumente“.

Benutzeralias@Domäne erstellt Benutzerordner, die einen Domännennamen enthalten. Wählen Sie diese Benennungskonvention aus, wenn Sie keine bereits mit der Ordnerumleitung oder einer anderen Benutzerdatenlösung genutzte Dateifreigabe verwenden. Durch diese Einstellung werden Konflikte bei der Ordnerbenennung verhindert, wenn mehrere Benutzer der Freigabe identische Aliase haben (dies kann passieren, wenn die Benutzer unterschiedlichen Domänen angehören).

Schritt 2 – Zertifikatsbindung für Workfolders

- Workfolders funktionieren ausschließlich mit SSL Zertifikaten.
- Zertifikat erstellen, dabei immer den richtigen DNS eintragen!
- In der Rolle des DNS muss jetzt ein neuer HOST Eintrag hinzugefügt werden (Beispiel: Workfolders)
- Im IIS muss das Zertifikat nun in der Default Site eingebunden werden.

Workfolders unter einem Client einrichten

<http://www.dummies.com/computers/operating-systems/windows-10/how-to-set-up-work-folders-in-windows-10/>

Leistungsprobleme unter Windows 10 beheben

- Windows 10 muss aktiviert sein, da sonst keine persönlichen Einstellungen vorgenommen werden können.
- 1X aktiviert, ist der Schlüssel für den PC auf Lebenszeit für das Gerät aktiviert. Dabei wird ein Hardware Hash angelegt.

Quick Tipp:

CMD:

SLMGR.VBS /ATO
SLMGR.VBS /IPIC
SLMGR.VBS /DLI

Bereitstellen von Paketen für Windows 10

Die Windows-Bereitstellung erleichtert IT-Administratoren die Konfiguration von Endbenutzergeräten, ohne ein Image erstellen zu müssen. Mithilfe der Windows-Bereitstellung kann ein IT-Administrator die gewünschte Konfiguration und die Einstellungen für die Registrierung der Geräte bei der Verwaltung auf einfache Weise angeben und die Konfiguration binnen Minuten auf Zielgeräte anwenden. Diese Methode eignet sich am besten für kleine bis mittlere Unternehmen mit Bereitstellungen von ein paar Dutzend bis zu einigen Hundert Computern.

Ein Bereitstellungspaket (.ppkg) ist ein Container für eine Sammlung von Konfigurationseinstellungen. Mit Windows 10 können Sie Bereitstellungspakete erstellen, die Ihnen das schnelle und effiziente Konfigurieren eines Geräts ermöglichen, ohne ein neues Image installieren zu müssen.

Bereitstellungspakete sind so einfach aufgebaut, dass Lernende oder Mitarbeiter ohne technischen Hintergrund nur eine kurze schriftliche Anleitung benötigen, um damit ihr Gerät zu konfigurieren. Dies kann eine erhebliche Verringerung des Zeitaufwands bedeuten, der zum Konfigurieren einer größeren Zahl von Geräten in Ihrem Unternehmen anfällt.

Das [Windows Assessment and Deployment Kit \(ADK\) für Windows 10](#) enthält Windows-Konfigurations-Designer, ein Tool für die Konfiguration von Bereitstellungspaketen. Windows-Konfigurations-Designer steht auch als [App im Microsoft Store zur Verfügung](#).

Bereitstellen allgemeiner Einstellungen für die Erstbereitstellung für PCs (Desktop-Assistent)

<https://docs.microsoft.com/de-de/windows/configuration/provisioning-packages/provision-pcs-for-initial-deployment>