Akademie für Lehrerfortbildung und Personalführung

Handreichung
zur Installation von Windows 10
in Schulen

Vorbereitung einer Windows-Installation zum Klonen

Die einfachste Art einen Computerraum einzurichten ist das Klonen eines vorbereiteten Muster-Computers mit allen installierten Programmen und Einstellungen. Das Systemimage dieses vorbereiteten Computers wird dabei auf alle anderen Computer übertragen. Diese Handreichung beschreibt, wie man einen Muster-Computer mit dem Betriebssystem Windows 7, Windows 8 oder Windows 10 vorbereitet, damit das Klonen – auch bei unterschiedlicher Hardware – gelingt.

IMPRESSUM

Akademie für Lehrerfortbildung und Personalführung, Dillingen (http://alp.dillingen.de)

Die in der Handreichung beschriebenen Verfahren wurden im Rahmen der Fortbildungsinitiative SCHULNETZ zur Qualifizierung von Systembetreuerinnen und Systembetreuern von IT-Multiplikatoren erarbeitet. Die Handreichung ist unter der Adresse http://alp.dillingen.de/schulnetz/materialien abrufbar.

Dokumentation: Georg Schlagbauer, Akademie Dillingen
Barbara Maier, Bürgernetz Dillingen
Thomas Pickel, Maximilian-Kolbe-Schule Neumarkt
Manfred Maier, Staatl. Realschule Zirndorf
E-Mail: schlagbauer@alp.dillingen.de
Stand: November 2019

INHALT

ANLAGEN

GRUNDSÄTZLICHES VORGEHEN

Eigentlich ist das Klonen einer Systeminstallation sehr einfach: Man installiert das Betriebssystem mit allen Programmen auf einem Muster-Computer, nimmt eine beliebige Imaging-Software und verteilt das System auf alle anderen Computer.

Speziell bei Windows können dabei folgende Probleme auftreten:

Unterschiedliche Hardware: Windows führt nicht bei jedem Neustart eine Hardwareerkennung durch. Wenn sich die Hardware zu deutlich unterscheidet, läuft das geklonte System nicht.

Gleicher Computername: Windows setzt voraus, dass innerhalb eines Netzes jeder Computer einen anderen Namen hat.

Gleiche System- und Benutzer-IDs: Microsoft setzt voraus, dass unterschiedliche Computer und unterschiedliche Benutzer auch unterschiedliche IDs haben. Wenn dies nicht der Fall ist, können irgendwann Probleme auftreten, die nicht mehr lokalisierbar sind. Insbesondere die Aktivierung von Microsoft-Volumenlizenzen benötigt eindeutige System-IDs auf allen Clients.

Microsoft schlägt deshalb ein anderes Verfahren zur Installation und zum Klonen von Windows vor:

INSTALLATION VON WINDOWS IM AUDIT-MODUS (SYSTEMVORBEREITUNGS-MODUS)

Windows wird auf einem Muster-Computer im Audit-Modus installiert. Ebenso werden alle notwendigen Programme installiert und der Desktop bzw. das Benutzerprofil werden angepasst. Gegebenenfalls werden auch zusätzliche Treiber für unterschiedliche Hardware in das System integriert.

VERSIEGELN DES COMPUTERS MIT SYSPREP

Diese Musterinstallation von Windows wird anschließend mit dem Befehl Sysprep „generalisiert“, das heißt, es werden einige systemspezifische Daten entfernt und der Computer wird anschließend heruntergefahren. Das auf dem Computer installierte Windows befindet sich jetzt in im „versiegelten Modus“.

KLONEN DES SYSTEMS IM VERSIEGELTEN MODUS

In diesem Zustand kann Windows – auch auf unterschiedlicher Hardware – geklont werden.

Das Klonen selbst wird mit einem Imaging-System durchgeführt, z. B. WinPE mit DISM, Acronis, DriveSnapshot, WDS, FOG, Clonezilla, etc.

NEUSTART DER GEKLONTEN COMPUTER UND MINI-INSTALLATION

Beim ersten Start durchläuft der geklonte Computer eine „Mini-Installation“. Diese kennt man von neuen Computern, die man mit vorinstalliertem Windows-Betriebssystem kauft.

Der erste Start mit der Mini-Installation dauert geringfügig länger als ein normaler Systemstart, zusätzlich werden noch ein paar Fragen gestellt (z. B Ländereinstellungen, Eula, Benutzername), die man jedoch mit einer vorbereiteten Antwortdatei unterbinden kann.

VORBEREITENDE ARBEITEN

AUSWAHL DES MUSTER-COMPUTERS

Im Prinzip kann man hier jeden Computer verwenden, auf dem sich Windows installieren lässt.

Wenn man in der glücklichen Lage ist, von der Hardware her ausschließlich identische Computer zu besitzen, kann man einen von diesen verwenden. Der Vorteil ist, dass man auf die Nachinstallation von zusätzlichen Hardware-Treibern verzichten kann.

In allen anderen Fällen ist es eine sehr gute Wahl, wenn man als Mustercomputer keinen realen Computer, sondern eine virtuelle Maschine (z. B. unter VirtualBox) verwendet. Mit dieser virtuellen Maschine wird keine zusätzliche Hardware belegt. Vor allem aber kann man während der Installation mit Snapshots sehr einfach Zustände konservieren und bei Bedarf wieder dorthin zurückkehren.

Wer den Umgang mit VirtualBox oder einer anderen Virtualisierungsumgebung beherrscht, sollte dies als bevorzugte Umgebung betrachten.

WINPE-LIVE-SYSTEM

Das WinPE-Live-System ist zum Klonen mit DISM notwendig. Ebenso wird es benötigt, wenn dem im Audit-Modus vorbereiteten Computer zusätzliche Treiber für unterschiedliche Hardware „untergeschoben“ werden sollen.

Falls mit einem anderen System geklont werden soll (z. B. FOG) und keine zusätzlichen Treiber benötigt werden, könnte man zum Klonen auf das WinPE-Live-System verzichten. Ein Windows-Live-System ist jedoch zum Troubleshooting ein immer ein gutes Werkzeug.

Wie man das WinPE-Live-System erstellt ist in der Handreichung „Erstellung eines WinPE-Live-Systems“ beschrieben (siehe http://alp.dillingen.de/schulnetz/materialien/WinPE10.pdf).

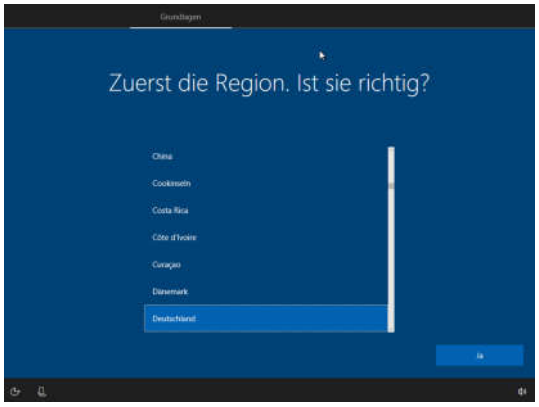
AUSWAHL DER WINDOWS-VERSION

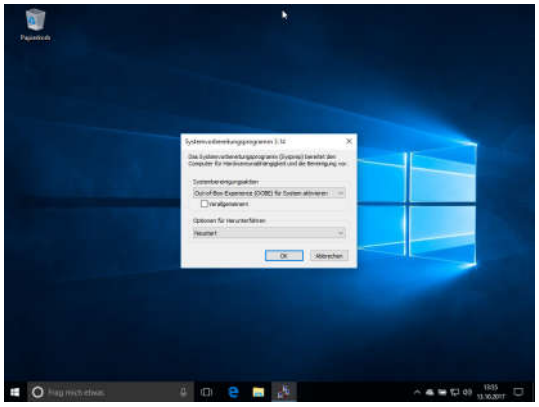
Zum Klonen von Windows 10 eignen sich die Versionen **Windows 10 Enterprise, Windows 10 Education** und **Windows 10 Professional**. Für andere Windows 10-Versionen gibt es keine Volumenlizenzen.

Um Probleme mit verpflichtenden Versions-Upgrades von Windows 10 zu vermeiden, die im Audit-Modus technisch nicht möglich sind, kann Windows 10 Enterprise LTSB/LTSC (Long Term Stability Branch/Channel) eingesetzt werden. Diese Version erhält nur normale Sicherheitsupdates, aber keine Versionsupgrades und wird von Microsoft jeweils fünf Jahre lang unterstützt. Die meisten Volumenlizenzverträge erlauben Schulen die Verwendung dieser Version, oft allerdings erst auf Nachfrage. Andererseits unterstützt die LTSB/LTSC-Version von Windows 10 keine Windows-Store-Apps und insbesondere nicht die OneNote-App, die auf Windows-Tablets zur Stifteingabe häufig verwendet werden soll.

INSTALLATION VON WINDOWS IM AUDIT-MODUS

Das grundsätzliche Verfahren ist seit Windows Vista gleich geblieben. Windows wird ganz normal von DVD installiert. Gegen Ende der Installation erfolgen computer- und benutzerspezifische Eingaben. Diese werden nicht durchgeführt, sondern an dieser Stelle wird durch die Tastenkombination **Strg + Shift + F3** der weitere Ablauf unterbrochen, der PC wird automatisch neu gestartet und im **Audit-Modus** wieder hochgefahren.





Wenn man sich unsicher ist, ob man an der richtigen Stelle ist, um die Installation abzubrechen, probiert man die Tastenkombination **Strg + Shift + F3** einfach aus.

Im Audit-Modus ist das vordefinierte Benutzerkonto Administrator (ohne Passwort) aktiviert. Auf dem Desktop ist das Programm-Fenster des Microsoft-Bereitstellungstools Sysprep.exe geöffnet. Es kann ohne Probleme geschlossen werden (Abbrechen-Button). Bei jedem Neustart fährt der PC automatisch wieder im Audit-Modus hoch und zwar so lange, bis das System versiegelt wird.

Im Audit-Modus können Programme und Treiber installiert und der Computer nach Wunsch konfiguriert werden.

Wurde Windows nicht im Audit-Modus installiert, kann Windows auch nachträglich in den Audit-Modus versetzt werden (C:\windows\system32\sysprep\sysprep.exe /audit). Gegebenenfalls ist es in diesem Fall sinnvoll, die bisher angelegten Benutzer und deren Profile zu löschen. Microsoft empfiehlt, den Computer nicht nachträglich in den Audit-Modus zu versetzen.

WINDOWS-PRODUKTSCHLÜSSEL - AKTIVIERUNG

Im Audit-Modus sollte kein „echter“ Produktschlüssel (MAK-Key) eingetragen werden, da sonst bei jedem Klonen des Mustercomputers eine automatische Aktivierung von Windows durchgeführt wird und die MAK-Keys bald verbraucht sind.

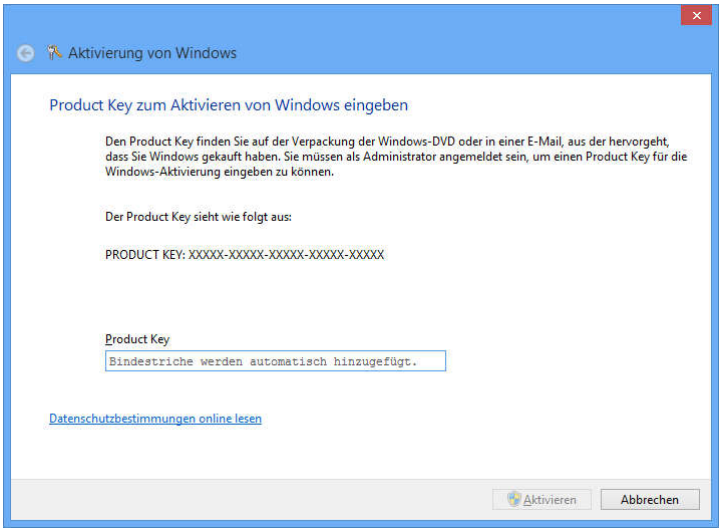
Wenn ein KMS-Host eingerichtet ist, wird Windows automatisch darüber aktiviert (falls der korrekte KMS-Client-Key als Produktschlüssel eingetragen ist).

Nähere Informationen sind in der Handreichung „Windows 7 - Produktaktivierung“ enthalten.

Bei **Windows 10 Enterprise** ist standardmäßig ein Produktschlüssel (Product Key) für die KMS-Aktivierung eingetragen. Dieser Produktschlüssel kann so belassen werden. Wenn an der Schule ein KMS-Host eingerichtet ist, aktiviert sich Windows automatisch.

Bei **Windows 10 Professional** kann der Produktschlüssel für die KMS-Aktivierung eingetragen werden. Windows fragt dann beim ersten Neustart nicht nach einem gültigen Schlüssel und aktiviert sich automatisch, wenn ein KMS-Host zur Verfügung steht.

Der Produktschlüssel kann nachträglich geändert werden:



- *Systemsteuerung – System und Sicherheit – System – Windows aktivieren*
- *Kommandozeile (als Administrator): slmgr -ipk XXXXX - XXXXX - XXXXX - XXXXX – XXXXX*
- *Alternativ kann der Produktschlüssel auch in der Antwortdatei mitgegeben werden.*

Je nach Konfiguration versucht Windows die Aktivierung automatisch durchzuführen. Dies misslingt bei einem KMS-Key, wenn kein KMS-Host erreichbar ist. Der neue Produktschlüssel ist trotzdem eingetragen.

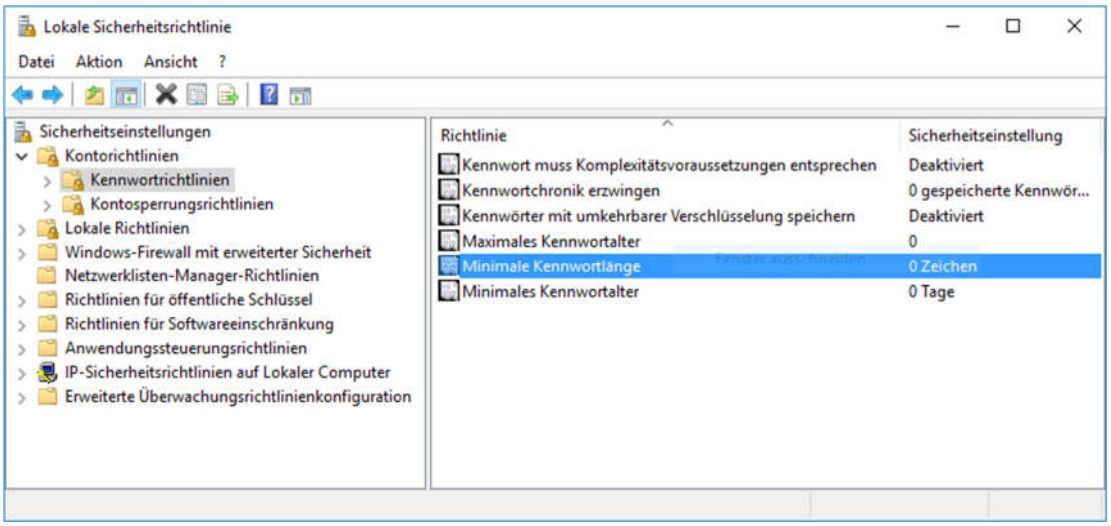
Die Produktschlüssel für die KMS-Aktivierung hat Microsoft unter http://technet.microsoft.com/en-us/library/jj612867.aspx veröffentlicht.

ANPASSEN VON EINSTELLUNGEN

KENNWORTRICHTLINIE

Standardmäßig müssen Benutzer alle 42 Tage ihr Kennwort ändern. Im nachfolgenden Beispiel wird die Kennwortrichtlinie so geändert, dass Kennwörter nicht ablaufen. Über die lokale Sicherheitsrichtlinie kann diese Einstellung geändert werden.

Aufruf der lokalen Sicherheitsrichtlinie: **secpol.msc**



ANSICHT IM WINDOWS-EXPLORER

z. B. Detailansicht, Dateiendungen anzeigen

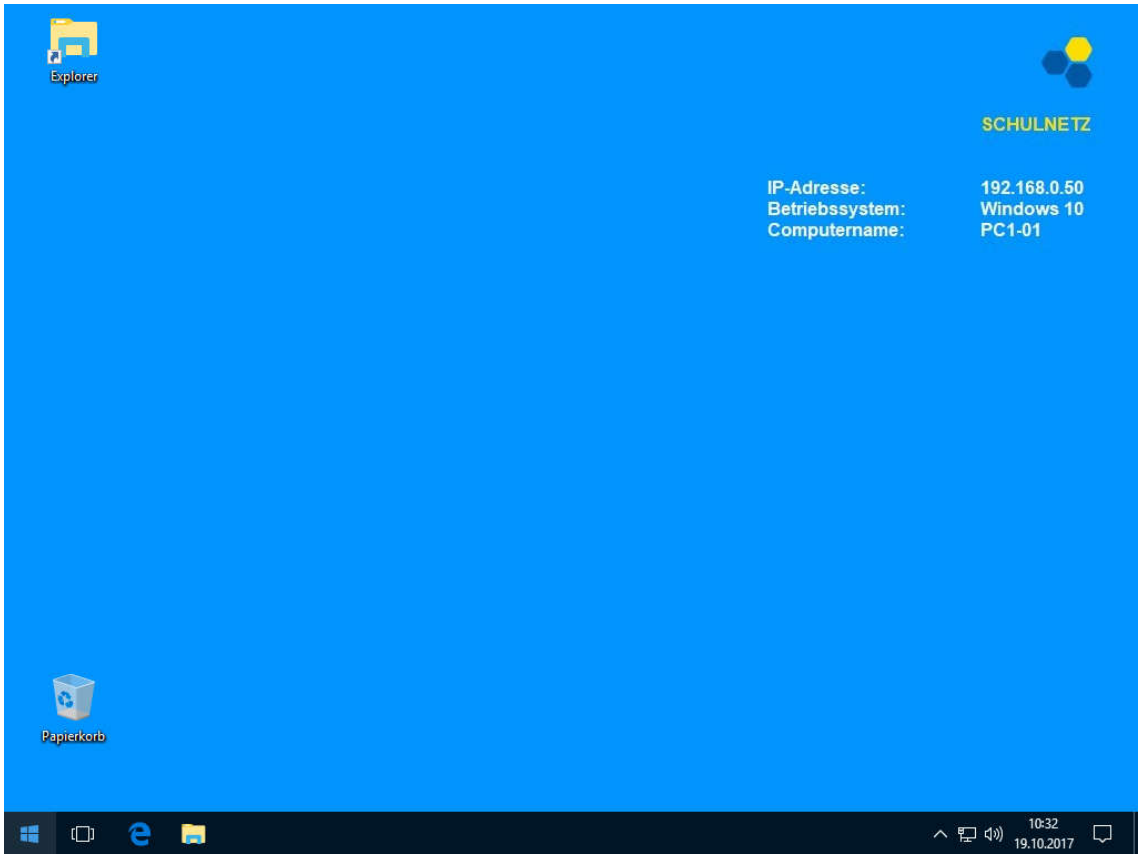
ANSICHT IM KOMMANDOZEILENFENSTER

z. B. Schriftgröße und Farben anpassen

HINTERGRUNDBILD

Leider kann das Hintergrundbild bei Windows 10 nicht problemlos angepasst werden, solange Windows nicht aktiviert ist. Wenn man einen KMS-Host hat, kann man Windows 10 auch im Audit-Modus aktivieren. Ansonsten kann man eine beliebige Bilddatei mittels Rechtsklick als Hintergrundbild setzen.

Falls ein Schul-Logo oder Informationen wie die aktuelle IP-Adresse, der Computername o. ä. auf dem Hintergrund angezeigt werden sollen, ist eventuell das Sysinternals-Programm BGInfo interessant:



DRUCKERINSTALLATION

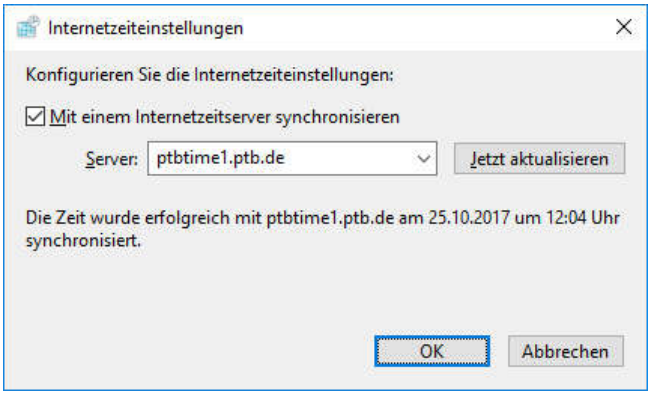
Netzwerkdrucker mit den dazugehörigen Treibern können installiert werden. Sie sollten über die IP-Adresse angesprochen werden. Herstellereigene Verfahren zum Ansprechen der Drucker sind oft unzuverlässig.

EINRICHTEN VON NETZWERKVERBINDUNGEN

Dauerhafte Netzwerkverbindungen (z. B. allgemeiner Zugriff auf ein Austauschverzeichnis) können eingerichtet werden.

ZEITSYNCHRONISIERUNG

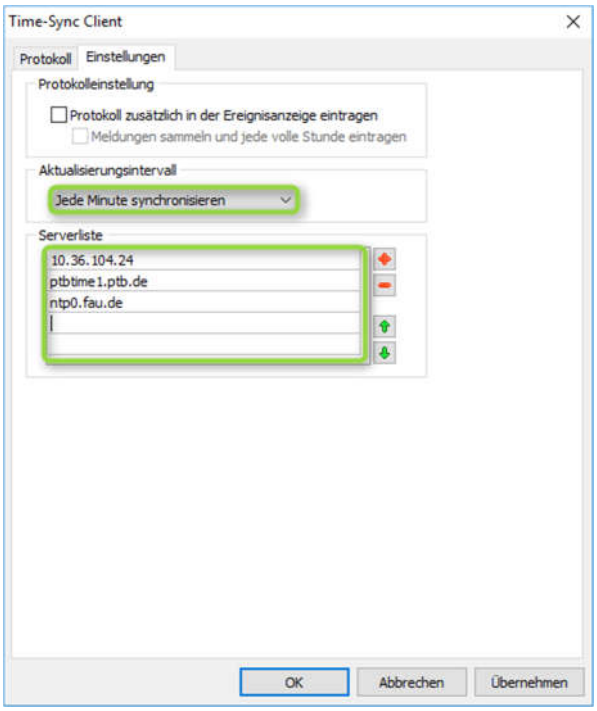
Die automatische Zeitsynchronisation mit dem voreingestellten Zeitserver time.windows.com arbeitet nicht immer zuverlässig. Viele Programme, die über das Netzwerk kommunizieren, verlassen sich jedoch auf eine korrekte Uhrzeit. Unter Windows kann bei den Zeiteinstellungen „Datum und Uhrzeit“ ein anderer Zeitserver eingetragen werden.



Das Aktualisierungsintervall (ca. 1-2 Aktualisierungen pro Tag) ist in der Registry festglegt und kann dort gegebenenfalls auf ein kürzeres Intervall abgeändert werden.

TIME-SYNC

Falls es dauerhafte Probleme mit der Zeitsynchronisierung gibt (z. B. wenn die PC-interne Uhr nicht sauber arbeitet), kann auch auf ein externes Programm, wie Time Sync zurückgegriffen werden. Dieses ermöglicht neben der Verwendung von mehreren Zeitservern (z. B. intern und extern) auch die Konfiguration von z. B. minütlichen Aktivierungsintervallen.



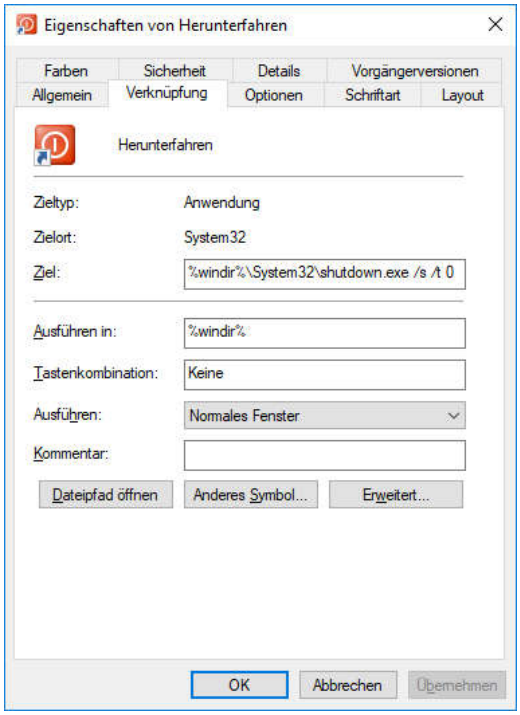
ABSCHALTEN UNNÖTIGER DIENSTE

Da auf Schüler-Computern in der Regel keine Daten und Dokumente gespeichert werden, kann der Windows-Indexierungsdienst („Windows Search“) über die Diensteverwaltung (services.msc) abgeschaltet werden. Auf langsamen Rechnern oder Rechnern ohne SSD beschleunigt dies Windows deutlich.

DESKTOP-ICON ZUM HERUNTERFAHREN DES COMPUTERS

Beim „normalen“ Herunterfahren benutzt Windows einen „Schnellstart-Modus“, der dem Befehl shutdown /s /hybrid /t 0 entspricht. Das Vollständige Herunterfahren von Windows entspricht dem Befehl shutdown /s /t 0.

Am Desktop kann eine Verknüpfung erzeugt werden, die den PC bei einem Doppelklick sofort herunterfährt.



Leider werden nicht alle Anpassungen von Windows bei der Mini-Installation übernommen. Nicht übernommen werden z. B. Programme in der Taskleiste, die Anpassung der Apps oder Datenschutzeinstellungen.

INSTALLATION VON PROGRAMMEN

Programme, die allgemein benötigt werden und die erfahrungsgemäß keinen großen Ärger machen, können installiert werden. Die Programme sollten mindestens einmal aufgerufen werden und die Grundeinstellungen sollten gegebenenfalls angepasst werden. Automatische Updates der Programme sollten nach Möglichkeit deaktiviert werden.

Auf dem Desktop können entsprechende Verknüpfungen zum Starten der Programme angelegt werden.

MICROSOFT OFFICE

Microsoft Office (ab Version 2010) kann bei der Office-KMS-Aktivierung Probleme machen, wenn die Computer nicht als „unterschiedlich“ erkannt werden. Beim ersten Start von Office wird eine Office-UID generiert, die beim Versiegeln nicht automatisch zurückgesetzt wird (rearm). Dies muss ggf. vor dem Versiegeln manuell erfolgen:

Office 2010:

C:\Program Files\Common Files\microsoft shared\OfficeSoftwareProtectionPlatform

```
OSPPREARM.EXE
```

Office 2013 bzw. Office 2016:

C:\Program Files (x86)\Microsoft Office\OfficeXX

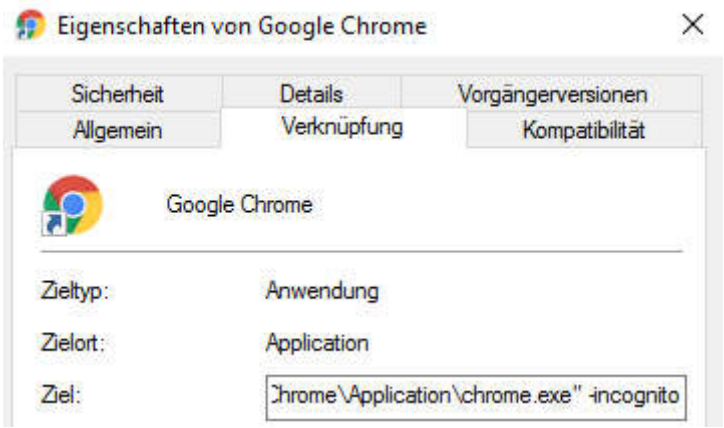
```
cscript ospp.vbs /rearm
```

Details sind in der Handreichung „KMS-Aktivierung von Microsoft Office“ beschrieben:

http://alp.dillingen.de/schulnetz/materialien/Office-KMS-Aktivierung.pdf

WEB-BROWSER

Beim Browser sollte eine sinnvolle Startseite vorgegeben und ein eventuell nötiger Proxy konfiguriert werden. Wenn die PCs von vielen Schülern abwechselnd benutzt werden, ist es sinnvoll, zusätzlich den Inkognito-Modus des Browsers zu aktivieren. Bei Chrome muss die Desktopverknüpfung angepasst werden. Beim „Ziel“ ergänzt man wie in der Abbildung „-incognito“:



Der Incognito-Modus in Chrome ignoriert standardmäßig die voreingestellte Browser-Startseite. Soll beim Programmstart dennoch eine bestimmte Startseite aufgerufen warden, muss zusätzlich die Ergänzung “-homepage https://meine.startseite.de” an das Ziel angefügt werden.

Bei Firefox wird das Kürzel „-private“ an das Ziel der Desktopverknüpfung angehängt. Um auch eine vordefinierte Startseite zu laden wird „https://meine.startseite.de“ ergänzt.

Um für Chrome einen Proxy-Server festzulegen muss “--proxy-server=ip.des.proxy.server:port“ an das Verknüpfungsziel angefügt werden. Bei Firefox erfolgt dies über die Programmeinstellungen.

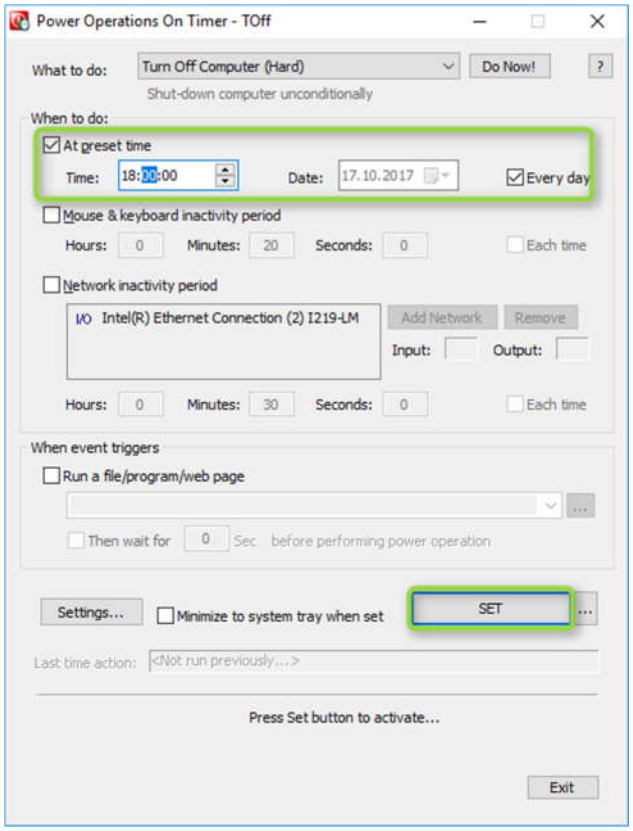
.NET-FRAMEWORK

Viele ältere Programme benötigen das Microsoft .NET Framework 3.5. Daher ist es oft sinnvoll, es zu installieren. Die Installation erfolgt über die Systemsteuerung per „Windows-Features aktivieren oder deaktivieren“.

HILFSPROGRAMME

TOFF

Zum zuverlässigen und automatischen Herunterfahren der Computer zu einer bestimmten Uhrzeit kann die Software TOff verwendet werden. Einmal konfiguriert startet diese immer automatisch mit Windows.



DESKTOPOK

Windows bringt häufig die Anordnung der Desktop-Icons durcheinander, insbesondere, wenn die Bildschirmauflösung der Schüler-Computer nicht einheitlich ist oder wenn ein Beamer im Betrieb an- oder abgeschaltet wird.

Das kostenlose Programm DesktopOK kann die Position der Icons abspeichern und wiederherstellen und ist über die Kommandozeile und damit über Skripte steuerbar.

STANDARDEINSTELLUNGEN ERHALTEN

Um nach dem Mini-Setup die Standardprogramme, das angepasste Startmenü sowie weitere Nutzereinstellungen beizubehalten, müssen vor dem Versiegeln die sogenannten AppAssociations exportiert und anschließend direkt wieder importiert werden. Dies wird in einer administrativen Eingabeaufforderung mittels folgender Befehle durchgeführt:

```
dism /online /Export-DefaultAppAssociations:%TMP%\AppAssoc.xml
dism /online /Import-DefaultAppAssociations:%TMP%\AppAssoc.xml
```

Die Windows-Taskleiste wird bei dieser Aktion leider nicht übernommen.

ANGEPASSTES STARTMENÜ BEIBEHALTEN:

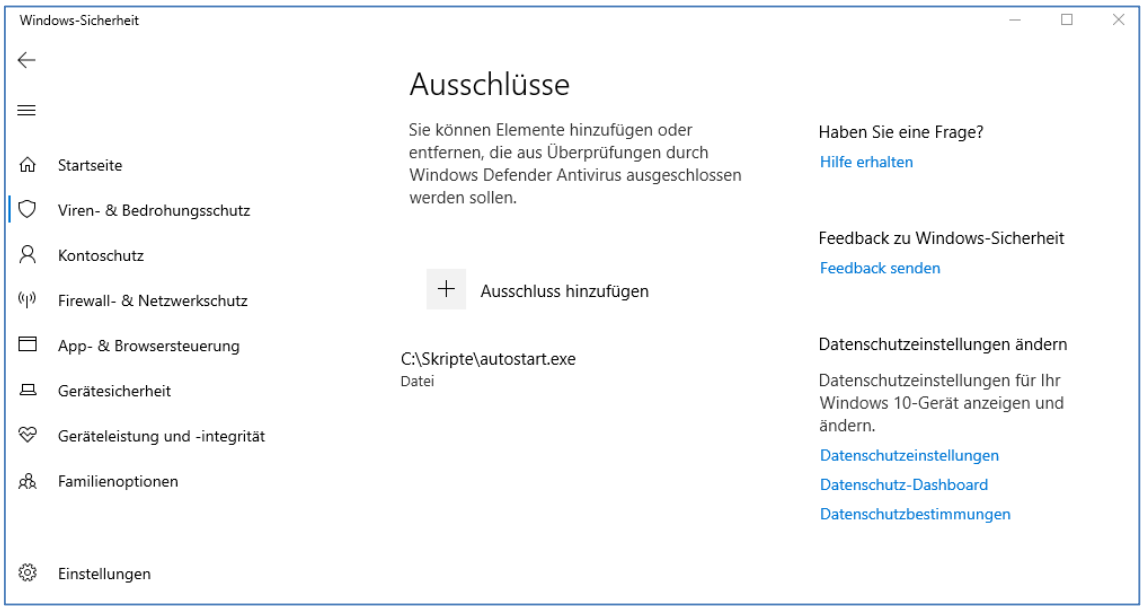
Um das angepasste Startmenü beim Klonen beizubehalten öffnet man im Audit-Modus die Windows PowerShell mit administrativen Rechten und führt folgenden Befehl (eine Zeile) aus:

```
Export-StartLayout –Path C:\Users\Administrator\AppData\Local\Microsoft\Windows\Shell\LayoutModification.xml
```

PROGRAMME VON DER PRÜFUNG DURCH WINDOWS DEFENDER AUSNEHMEN

Bei aktiviertem Windows Defender kann es vorkommen, dass dieser „unsichere“ .exe-Dateien als Virus einstuft und sie anschließend löscht bzw. in die Quarantäne verschiebt.

Das Problem hierbei ist, dass Windows Defender in der Regel auch selbst erstellte .exe-Dateien (z. B. aus Batch-Dateien) als Virus ansieht. Um das Löschen dieser Dateien zu verhindern muss die entsprechende .exe-Datei oder der Ordner, in dem sie liegt, als Ausschlussdatei/-ordner definiert werden.



Einstellungen – Update und Sicherheit – Windows Sicherheit – Viren- & Bedrohungsschutz – „Einstellungen für Viren- und Bedrohungsschutz“ verwalten – Ausschlüsse hinzufügen/entfernen.

WINDOWS UPDATES

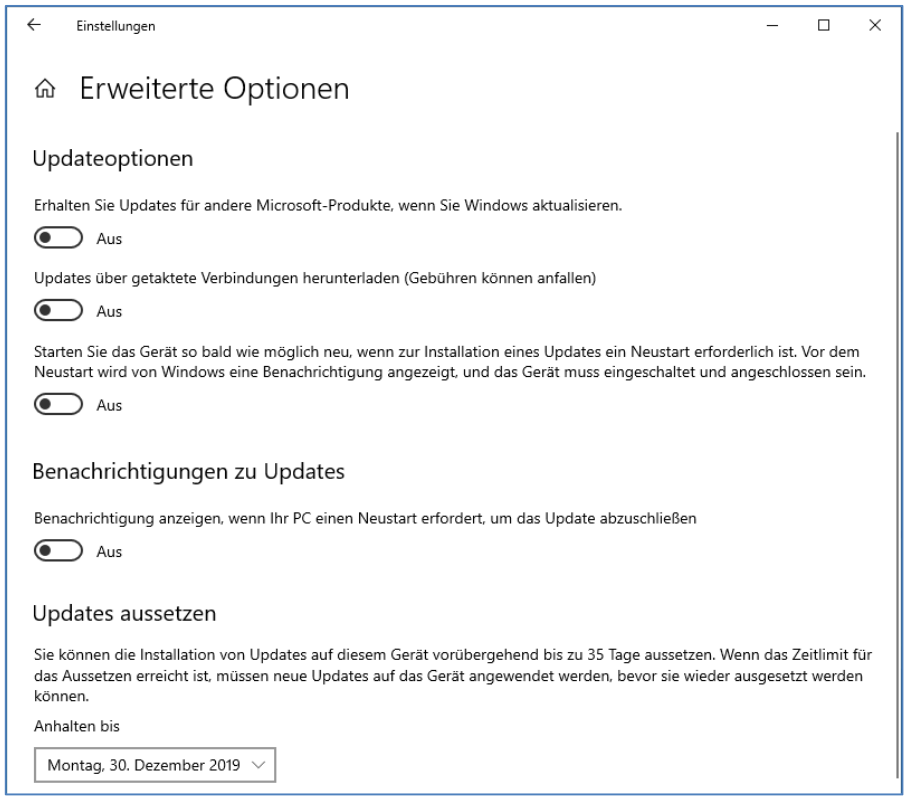
Vor dem Versiegeln des Computers sollten Windows- und gegebenenfalls Programm-Updates durchgeführt werden. Dies kann relativ viel Zeit in Anspruch nehmen.

Ob an den geklonten Arbeitsstationen regelmäßig Windows- und Programmupdates durchgeführt werden sollen, ist vom Konzept abhängig.

- Bei einer schnellen Internetanbindung und schnellen Computern stören gelegentliche Updates normalerweise nicht. Die Update-Einstellungen können unverändert beibehalten werden.
- Bei der Verwendung einer Protektorlösung sollten automatische Windows-Updates unterbunden werden.
- Wenn die Rechner häufig geklont werden, kann auf Updates verzichtet werden.
- Mit dem Deaktivieren der Updates funktioniert auch die automatische Treibersuche von Windows 10 nach dem Klonen des Computers nicht mehr.
- Mit dem Deaktivieren der Updates funktioniert auch die Aktualisierung des Windows-eigenen Virenscanners (Windows Defender Antivirus) nicht mehr.

AUTOMATISCHE WINDOWS-UPGRADES ZURÜCKSTELLEN

Bei Windows 10 können Upgrades zumindest vorübergehend zurückgestellt werden. Sicherheitsupdates sind nicht davon betroffen.



Einstellungen – Windows Updates – Erweiterte Optionen.

AUTOMATISCHE WINDOWS-UPDATES UNTERBINDEN

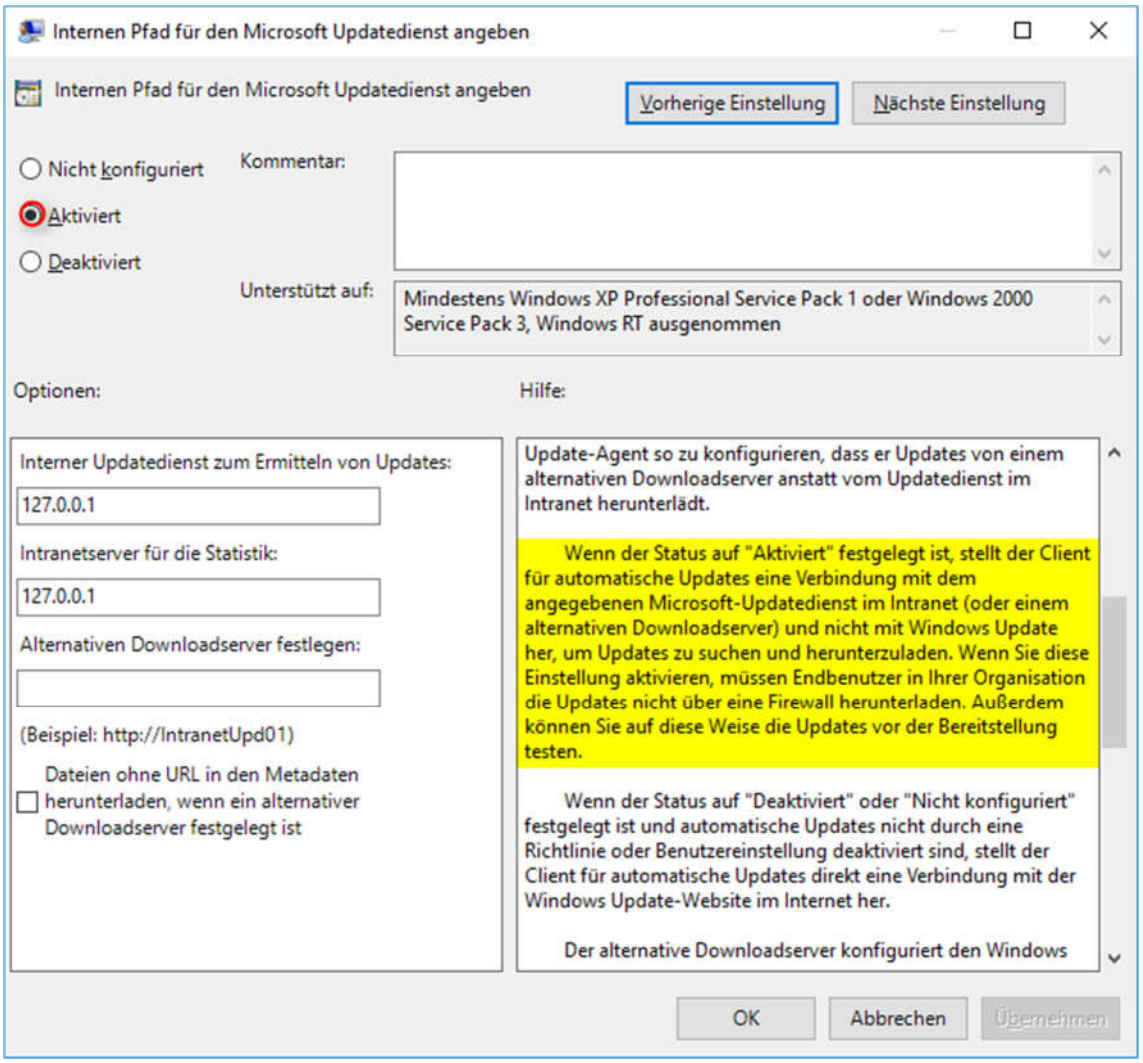
Seit Windows 10 lassen sich die automatischen Windows-Updates nur umständlich deaktiveren. Auch unterscheiden sich die Möglichkeiten je nach Version von Windows 10 (1607, 1703, 1709 …) zum Teil erheblich. Es gibt jedoch zwei zuverlässige Methoden.

DEAKTIVIERUNG DER UPDATES PER GRUPPENRICHTLINIE

Die benötigte Gruppenrichtlinie findet man in den lokalen Gruppenrichtlinien unter

Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Windows Update

Als alternativen Update- und Statistik-Server trägt man bei der Richtlinie „Internen Pfad für den Microsoft Updatedienst angeben“ die Loopback-IP-Adresse des Computers ein: 127.0.0.1 Dadurch findet der Computer keine Updates mehr.



DEAKTIVIERUNG DES UPDATE-DIENSTES PER SKRIPT

Alternativ lassen sich automatische Updates deaktivieren, indem man den Windows-Update-Dienst über die Diensteverwaltung oder folgenden Kommandozeilenbefehl abschaltet:

```
sc config wuauserv start= disabled
```

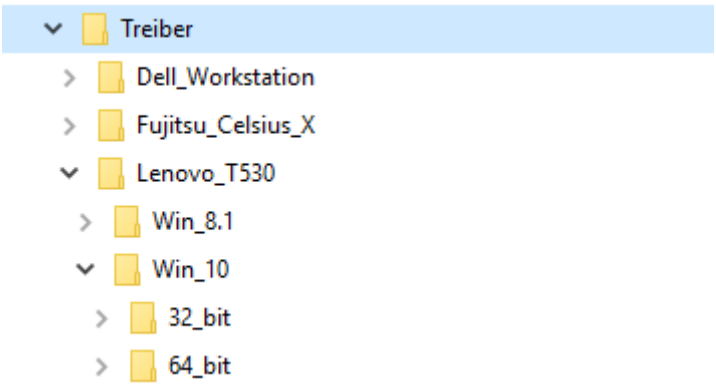
Da diese Einstellung das Klonen mit Sysprep nicht übersteht, muss sie nach Abschluss des Mini-Setups auf jedem Computer durchgeführt werden. Ein Verfahren zur Automatisierung dieses Vorgangs ist im Abschnitt „Automatisierung von Aufgaben nach dem Mini-Setup“ beschrieben.

INTEGRATION VON TREIBERN

Es ist möglich, in die Musterinstallation Treiber für die eigenen Computer zu integrieren. Nach dem Klonen stehen diese Treiber dann zur Verfügung.

Bei Windows 10 kann man eventuell auf diesen Schritt verzichten. Windows 10 sucht bei einer bestehenden Internetverbindung selbständig nach fehlenden Treibern. Voraussetzung ist natürlich, dass zumindest der Treiber für die Netzwerkkarte vorhanden ist.

Der größte Aufwand besteht darin, für die eigenen Computer die richtigen Treiber im richtigen Format (.cat, .sys, .inf) zu bekommen. Die Treiber sollten auch einzeln getestet sein. Es ist sinnvoll, die Treiber an einem Ort zu sammeln, z. B. in einer entsprechenden Struktur nach folgendem Muster



Durch diese Struktur können Treiber von ausgemusterten Computern leicht wieder entfernt werden.

Es ist kein Problem, wenn Treiber für unterschiedliche Betriebssysteme (Windows 7,8,10 bzw. 32-bit, 64-bit) zur Verfügung stehen. Windows erkennt dies und integriert nur die passenden Treiber.

Ein Weg, wie man Treiber aus einer bestehenden Windows-Installation extrahieren kann, ist im Anhang beschrieben.

EINBINDEN DER TREIBER

Folgende konkrete Schritte sind zum Einbinden der Treiber notwendig:

- Der Computer muss von einem WinPE-Live-System gestartet werden.
- Der Laufwerksbuchstabe der bestehenden Windows-Installation muss ermittelt werden (z. B. D:\)
- Die Verbindung zum Verzeichnis „Treiber“ ist (z. B. mit `net use`) herzustellen (z. B. N:\Treiber).
- `dism /image:D:\ /add-driver /recurse /driver:N:\Treiber`

Die Treiber werden dadurch dem Treibervorrat der Musterinstallation hinzugefügt. Erst wenn Windows nach dem Klonen auf neuer Hardware startet, werden die dafür erforderlichen Treiber aus diesem Treibervorrat installiert.

Das Hinzufügen der Treiber kann sowohl vor als auch nach dem Versiegeln des Mustercomputers (siehe nächster Abschnitt) geschehen. Entscheidet man sich für das Hinzufügen nach dem Versiegeln, hat man immer einen „sauberen“ Mustercomputer ohne zusätzliche Treiber. Dies erleichtert die Pflege des Mustercomputers über mehrere Jahre.

VERSIEGELN DES MUSTERCOMPUTERS

VERSIEGELN MIT QUICKPREP

Quickprep ist ein kleines Programm, das das Erstellen der Antwortdatei und das Versiegeln des Mustercomputes übernimmt. Quickprep wurde speziell für Schulen programmiert und setzt die nachfolgend in dieser Handreichung beschriebenen Arbeitsabläufe jeweils „auf Mausklick“ um.

Quickprep findet man unter http://alp.dillingen.de/schulnetz -> Materialien.

ANTWORTDATEI

Die Antwortdatei mit dem Namen **unattend.xml** wird auf den Mustercomputer in den Ordner **C:\Windows\Panther\Unattend** oder direkt in den Ordner **C:\Windows\Panther** kopiert.

Zum Erstellen einer Antwortdatei für die spätere Mini-Installation stellt Microsoft das Werkzeug WSIM (Windows System Image Manager) bereit. Dieses Werkzeug ist sehr mächtig, erfordert jedoch etwas Einarbeitungszeit. Wer diese Einarbeitungszeit nicht investieren will, kann auch eine vorbereitete Antwortdatei (z. B. mit Quickprep) für sein System übernehmen.

Das Erstellen einer Antwortdatei mit WSIM ist in der Anlage beschrieben.

CHECKLISTE VOR DEM VERSIEGELN

Unmittelbar vor dem Versiegeln sollte man noch einmal überlegen, ob nichts Wichtiges vergessen wurde:

- alle gewünschten Updates installiert?
  (Windows, Java, Browser, PDF-Reader, VLC, …)
- Updates deaktiviert? (falls gewünscht)
- falls Office gestartet wurde: rearm-Befehl ausgeführt?
- Papierkorb / Browser-Verlauf / Windows-Explorer-Verlauf / Download-Ordner leeren
- Falls FOG verwendet wird: FOG-Service deaktivieren
- Snapshot bzw. Backup der Musterinstallation angelegt?

NACH DEM VERSIEGELN

Seit mehreren Windows-10-Versionen besteht ein Problem beim Neuanlegen der Benutzer während des Entsiegelungsvorgangs. Dabei wird das Profil des Administrator-Benutzers aus dem Audit-Modus ins Profil der neu angelegten Benutzer übernommen. Im sogenannten Web-Cache sind dabei allerdings ausdrückliche Referenzen auf Dateien im Administrator-Profil vorhanden, auf die der neu angelegte Benutzer aber keine Zugriffsrechte hat. In Folge gibt es immer wieder Probleme mit dem Startmenü, der Systemsteuerung sowie mit dem Internet Explorer und Edge.

Um diesen Problemen vorzubeugen, muss das System nach dem Versiegeln und vor dem Aufzeichnen des Images von einem Windows-PE-Live-System gestartet werden. Dort löscht man den Inhalt der beiden folgenden Ordner:

- \Users\Administrator\AppData\Local\Microsoft\Windows\Webcache
- \Users\Administrator\AppData\Local\Microsoft\Windows\INetCache

Außerdem löscht man folgende Datei:

Users\Administrator\AppData\Local\Microsoft\Windows\WebcacheLock.dat

CHECKLISTE AN DER AKADEMIE DILLINGEN

Wenn für die Computerräume und vor allem für den IT-Bereich an der Akademie in Dillingen ein neues Windows-Image erstellt wird, wird nachfolgende Checkliste abgearbeitet.

Die Installation erfolgt in einer virtuellen Maschine auf einem ESXi-Server oder unter VirtualBox. Es werden regelmäßig Snapshots angefertigt und geprüft, ob die Versiegelung und die Mini-Installation funktionieren. Fehlerhafte Programme oder Einstellungen können dadurch leichter lokalisiert werden.

GRUNDINSTALLATION

- Erstellen einer virtuellen Maschine
- Bootreihenfolge festlegen: ISO-Image - Festplatte
- Installation von Windows 10 Enterprise LTSC (als virtuelle Maschine) im Audit-Modus
- Installations-ISO-Image aus dem Laufwerk entfernen
- Automatische Aktivierung per KMS überprüfen

ANTWORTDATEI

- mit Quickprep: „Windows-Features aktivieren oder deaktivieren“ - .NET-Framework 3.5 installieren, Quickprep installieren
- ohne Quickprep: Vorbereitete Antwortdatei (unattend.xml) nach c:\windows\panther kopieren;

EINSTELLUNGEN

- Kennwortrichtlinie ändern (secpol.msc; max. Kennwortalter=0; keine Beschränkungen)
- Windows-Explorer: Detailansicht, Dateiendungen anzeigen, Versteckte Dateien anzeigen
  Explorer-Icon auf dem Desktop
- Eingabeaufforderung (Desktop-App) sowie Programm Cmd.exe:
  Darstellung schwarz auf weiß, größere Schrift
- gegebenenfalls Zeitserver einstellen auf ptbtime1.ptb.de
- Desktop-Icon zur Druckerinstallation: (Verknüpfung zu „`control printers`“).
  Icon der Verknüpfung anpassen (aus der Datei c:\windows\System32\shell32.dll)
- Batch-Datei zur Laufwerksverbindung in den Autostart-Ordner (Ausführen „`shell:startup`“)
  Laufwerk.cmd:
  `net use n: \\10.36.104.10\Alle /user:Teilnehmer Teilnehmer /persistent:no`

PROGRAMMINSTALLATION

- Installation von Chrome, Dekstop-Icon, Startseite: http://alp.dillingen.de, Incognito-Modus
  (Desktop-Verknüpfung anpassen: „…chrome.exe“ –incognito)
- Installation von Firefox, Desktop-Icon, Startseite: http://alp.dillingen.de, privater Modus, Firefox als Standard-Browser festlegen
- Desktop-Icon Internet-Explorer löschen
- Installation von Putty.exe nach C:\Windows\system32;
  Standardeinstellungen ändern (schwarz auf weiß, größere Schrift)
- Installation von VLC (ohne Desktop-Icon)
- Installation von Libre Office, Desktop Icon; Online-Update ausschalten
- gegebenenfalls: Installation von 7zip

INSTALLATION VON MICROSOFT OFFICE

- Installation von Microsoft Office 2016 (anpassen)
- Automatische Aktivierung per KMS überprüfen
- Verknüpfungen zu Word, Excel, PowerPoint auf den Desktop
- Test von Word, Excel und PowerPoint, Updates aktivieren
- Rearm der Installation
  als Administrator: C:\Program Files\Microsoft Office\Office16> `cscript ospp.vbs /rearm`

ANPASSUNG

- Standardprogramme festlegen (Standardeinstellungen nach APP festlegen)
- Installation der USB-Konsolentreiber für Bintec RS123 (wird nicht automatisch gefunden)
  ```
  net use n: \\10.36.104.24\Vorlagen /user:xxx xxx
  dism /image:d:\ add-driver /recurse /driver:n:\Treiber
  ```
- ggf: Standardeinstellungen behalten:
  ```
  dism /online /Export-DefaultAppAssociations:%TMP%\AppAssoc.xml
  dism /online /Import-DefaultAppAssociations:%TMP%\AppAssoc.xml
  ```

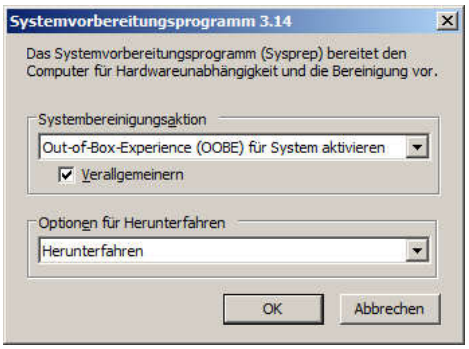
VOR DEM VERSIEGELN

- Automatische Windows-Updates (Standardeinstellung), Updates anstoßen
- Gegebenenfalls Windows Updates ausführen
- Download-Ordner leeren; Papierkorb leeren
- Windows-Explorer: Verlauf löschen
- Internet-Explorer: Browserverlauf löschen
- Firefox: Chronik löschen

VERSIEGELN MIT SYSPREP

Zum Versiegeln des Mustercomputers wird Sysprep mit der Option **Verallgemeinern** (generalize) ausgeführt.

C:\Windows\System32\Sysprep\sysprep.exe



Auf Kommandozeile entspricht dies dem Befehl

```
C:\Windows\System32\Sysprep\sysprep.exe /generalize /oobe /shutdown
```

Falls die Antwortdatei unattend.xml nicht gefunden wird, kann Sysprep auf Kommandozeile mit der Zusatzoption /unattend und dem Pfad zur Antwortdatei angegeben werden.

```
C:\Windows\System32\Sysprep\sysprep.exe /generalize /oobe /shutdown
/unattend:C:\Windows\Panther\unattend.xml
```
(eine Zeile)

Der Mustercomputer wird nun versiegelt und fährt herunter.

Durch das Versiegeln werden z. B. die Security-ID und andere computer- und hardwarespezifischen Informationen entfernt.

Nach dem Versiegeln wird der Computer mit einem Live-System (z. B. WinPE) gestartet, die Windows-Installation wird als Image (z. B. mit DISM, Drive Snapshot, Acronis, FOG etc.) gespeichert und auf die zu klonenden Computer verteilt. Dieser Vorgang ist z. B. in der Handreichung „Windows-Systemsicherung mit WinPE und DISM beschrieben“.

TROUBLESHOOTING

Falls Windows beim ersten Hochfahren hängt, besteht die Möglichkeit, über die Tastenkombination **<Shift> + <F10>** eine Kommandozeile zu öffnen und ggf. mit dem Befehl msoobe.exe den Prozess neu anzustoßen (cd oobe; msoobe.exe). Normalerweise ist dies jedoch ein Zeichen, dass irgendeine installierte Software mit der Hardware nicht zurechtkommt.

ANLAGEN

AUTOMATISIERUNG VON AUFGABEN NACH DEM MINI-SETUP

Manche Einstellungen werden beim ersten Neustart des Computers nach dem Klonen („Mini-Setup“) auf Standardwerte zurückgesetzt. Dies betrifft unter anderem die Einstellungen zu Windows Updates, zur Taskleiste, aber auch viele andere.

Oft hilft es dann, diese Einstellungen über ein Skript nach dem Mini-Setup durchzuführen. Dazu erzeugt man vor dem Versiegeln in der Musterinstallation den Ordner C:\Windows\Setup\scripts und darin die Batchdatei SetupComplete.cmd. Die Befehle in dieser Datei werden mit administrativen Rechten ganz am Ende des Mini-Setups **genau einmal** auf jedem einzelnen PC ausgeführt.

Hier können beispielsweise auch Programme automatisiert installiert werden, die Probleme mit der Versiegelung haben (z.B. manche Protektor-Software und Virenscanner).

Sollen Programme mit administrativen Rechten bei jedem folgenden Systemstart ausgeführt werden, kann über das SetupComplete-Skript ein weiteres Skript eingerichtet werden.

Beispiele für die SetupComplete.cmd:

```
REM FOG Service aktivieren:
 sc config FOGService start= auto

REM Standbymodus deaktivieren:
 powercfg /change standby-timeout-ac 0
 powercfg /change monitor-timeout-ac 0

REM Protektor-Software in Silent-Mode installieren:
 cd \setup
 start /wait setup.exe /s /norestart

REM Warten, bis Installation sicher abgeschlossen ist:
 timeout /T 120

REM Admin-Autostart-Skript aktivieren
 schtasks /RU "SYSTEM" /create /tn "adminscript"
     /tr:"C:\adminscript.cmd" /sc:onstart

REM Neustart:
  shutdown -t 0 -r
```

Der schtasks-Befehl führt dazu, dass das Skript C:\adminscript.cmd bei jedem folgenden Systemstart mit administrativen Rechten ausgeführt wird. Das kann eine Sicherheitslücke darstellen, andererseits aber auch die Administration vereinfachen.

Beispiel für adminscript.cmd:

```
REM Windows Update Dienst deaktivieren:
REM Windows aktiviert seit Version 1903 den Dienst automatisch nach
REM einigen Tagen wieder, daher muss dieser Befehl bei jedem
REM Systemstart neu ausgeführt werden
 sc config wuauserv start= disabled


REM Adobe Update Service deaktivieren
 sc config AdobeARMService start= disabled
```

STARTSKRIPTE

Soll bei jedem Start des Computers ein Skript ausgeführt werden, legt man dieses im Autostart-Ordner ab. Dieser ist bei jeder Windows-Version an einer anderen Stelle, kann aber einfach gefunden werden:

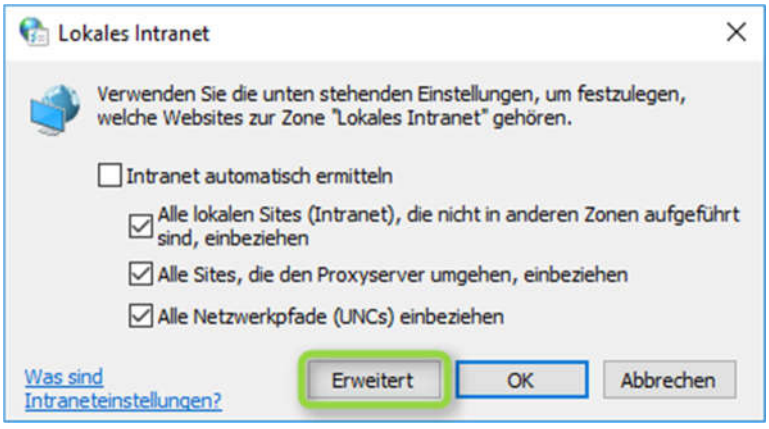
Die Tastenkombination Windows+R öffnet das Fenster „Ausführen“. Dort gibt man den Befehl „shell:common startup“ ein und es öffnet sich ein Windows Explorer mit dem für alle Benutzerkonten des Computers gültigen Autostart-Ordner.

STARTSKRIPT IM NETZ

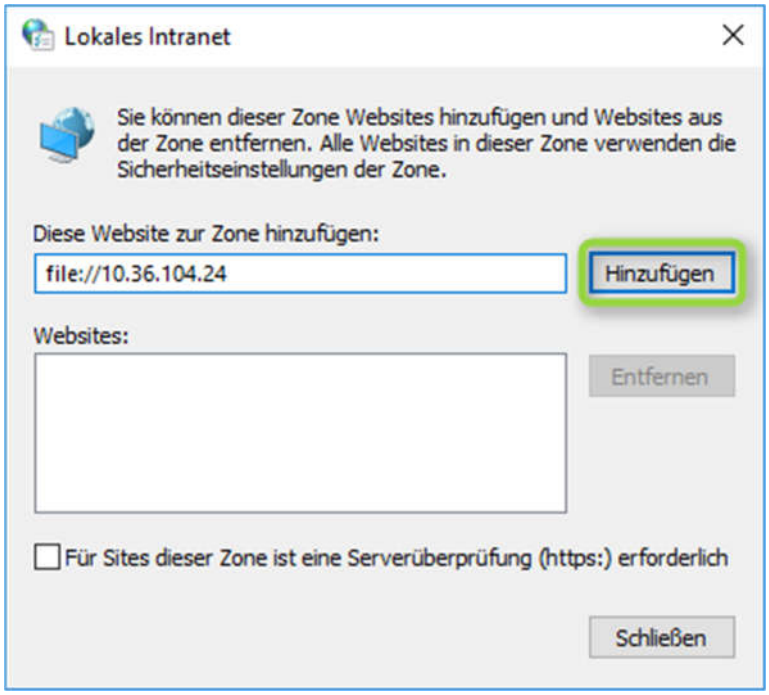
Um auch nach dem Klonen der PCs Änderungen am Startskript vornehmen zu können, legt man im Autostart-Ordner wie im letzten Abschnitt beschrieben ein lokales Startskript an, das nur ein Netzlaufwerk verbindet und von dort das eigentliche Startskript aufruft.

Damit dies ohne Sicherheitsabfragen möglich ist, muss der Speicherort des Startskripts im Netz als vertrauenswürdig deklariert werden.

Dazu öffnet man in der Systemsteuerung die Internetoptionen, Reiter Sicherheit, Lokales Intranet, Sites. Die angebotenen Einstellungen unterscheiden sich je nach Windows-Version; wichtig ist, dass alle lokalen Sites und alle Netzwerkpfade zur Zone „Lokales Intranet“ gehören:



Unter „Erweitert“ wird die URL der NAS-Box bzw. des Servers eingegeben, auf dem das Startskript gespeichert ist. Die Syntax lautet file://ip.des.servers.



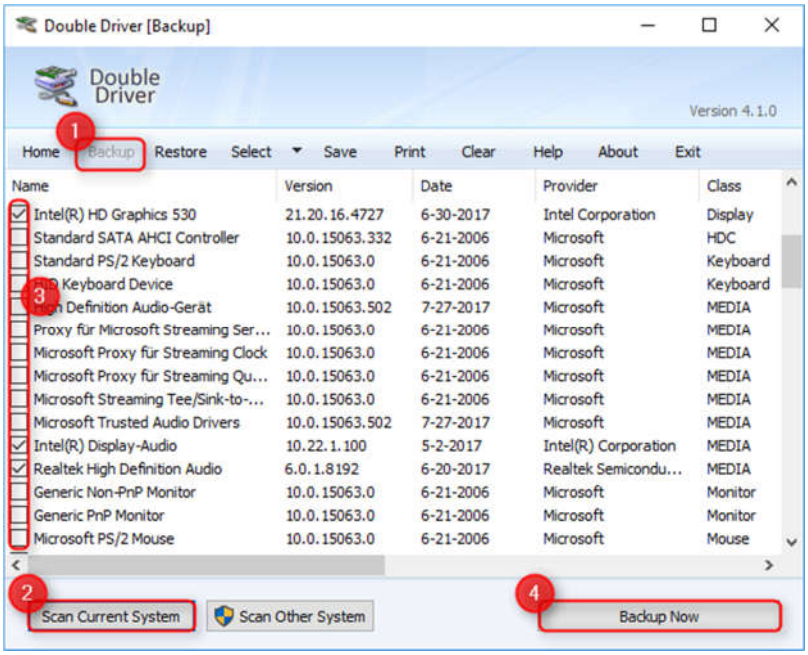
Anschließend klickt man auf „Hinzufügen“ und auf „Schließen“. Skripte und Programme von diesem Speicherort können jetzt ohne Sicherheitsabfrage ausgeführt werden.

EXTRAHIEREN VON TREIBERN AUS EINER LAUFENDEN WINDOWS-INSTALLATION

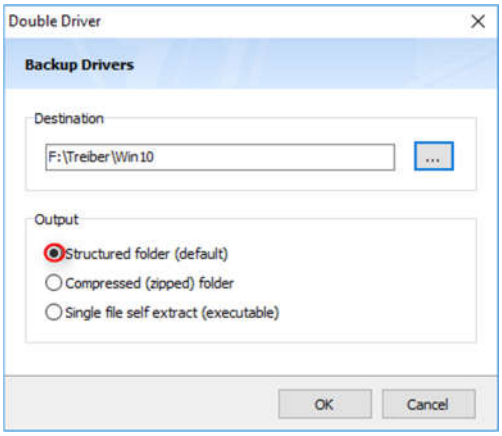
Um an die Treiber für eine bestimmte Computerhardware zu kommen, kann man die Webseiten des Herstellers durchsuchen. Die Treiber werden für die oben beschriebene Integration allerdings in einem speziellen Format benötigt (.cat/.sys/.inf-Dateien), das nicht von allen Herstellern angeboten wird.

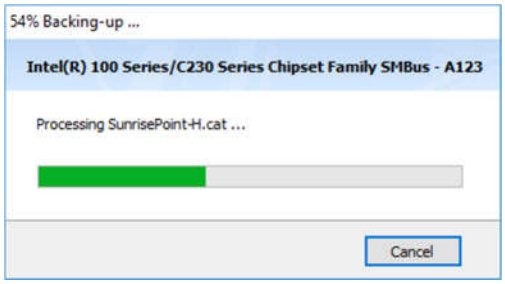
Im Folgenden wird ein alternativer Weg beschrieben:

Auf der neuen Hardware werden die Treiber zunächst mit dem vom Hersteller vorgesehenen Programm installiert (mitgelieferte DVD, Download eines speziellen Tools im Internet etc.). Um die nicht von Microsoft Windows stammenden Treiber zu sichern scannt man mit der Software DoubleDriver den aktuellen Computer nach Treibern. Das Programm wählt hierbei bereits die zusätzlich installierten Treiber aus.

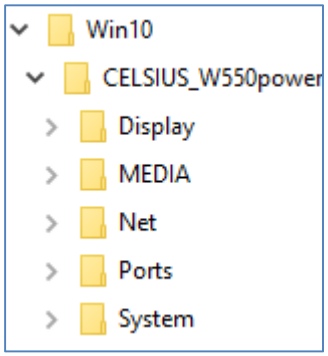


Um diese Treiber im für uns passenden Format abzuspeichern belässt man in den Output-Optionen die Auswahl bei „Structured Folder“.





DoubleDriver legt im Zielverzeichnis automatisch einen Ordner mit der passenden Computerbezeichnung an und speichert darin die entsprechenden Treiberdateien in jeweils eigenen Unterordnern ab.



IMPORT VON WLAN-PROFILEN

Sollen den geklonten Computern WLAN-Verbindungen mitgegeben werden, so muss man hier ähnlich vorgehen wie bei den Treibern.

Man verbindet sich mit einem Notebook mit dem gewünschten WLAN-Netzwerk und extrahiert über die Eingabeaufforderung mit dem folgenden Befehl die vorhandenen WLAN-Profile des Notebooks:

```
netsh wlan export profile key=clear folder=<Ziel>
```

```
netsh wlan export profile key=clear folder=C:\WLAN
```

Dieser Befehl erzeugt für jedes gespeicherte WLAN-Netzwerk eine XML-Datei mit verschlüsseltem WLAN-Kennwort im Zielordner (hier: C:\WLAN).

```
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
    <name>ALP-HS18</name>
  - <SSIDConfig>
      - <SSID>
            <hex>414C502D48533138</hex>
            <name>ALP-HS18</name>
        </SSID>
    </SSIDConfig>
    <connectionType>ESS</connectionType>
    <connectionMode>auto</connectionMode>
  - <MSM>
      - <security>
          - <authEncryption>
                <authentication>WPA2PSK</authentication>
                <encryption>AES</encryption>
                <useOneX>false</useOneX>
            </authEncryption>
          - <sharedKey>
                <keyType>passPhrase</keyType>
                <protected>true</protected>
                <keyMaterial>01000000D08C9DDF0115D11</keyMaterial>
            </sharedKey>
        </security>
    </MSM>
  - <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profile/v3">
        <enableRandomization>false</enableRandomization>
    </MacRandomization>
</WLANProfile>
```

Nach dem Klonvorgang und Durchlaufen des Mini-Setups können die XML-Dateien der gespeicherten Profile mittels Eingabeaufforderung importiert werden:

```
netsh wlan add profile filename="C:\WLAN\HS18.xml" interface="WLAN"
```

Beispiel für ein Autostart-Skript, das bei jedem Systemstart ausgeführt wird und prüft, ob die Profile bereits importiert wurden:

```
@echo off
if exist C:\WLAN\%username%_importiert.txt goto ende
netsh wlan add profile filename="C:\WLAN\WLAN1.xml" interface="WLAN"
netsh wlan add profile filename="C:\WLAN\WLAN2.xml" interface="WLAN"
echo WLAN-Profile importiert > C:\WLAN\%username%_importiert.txt
:ende
Exit
```


ABSICHERN EINES COMPUTERS MIT LOKALEN GRUPPENRICHTLINIEN

LOKALE GRUPPENRICHTLINIEN

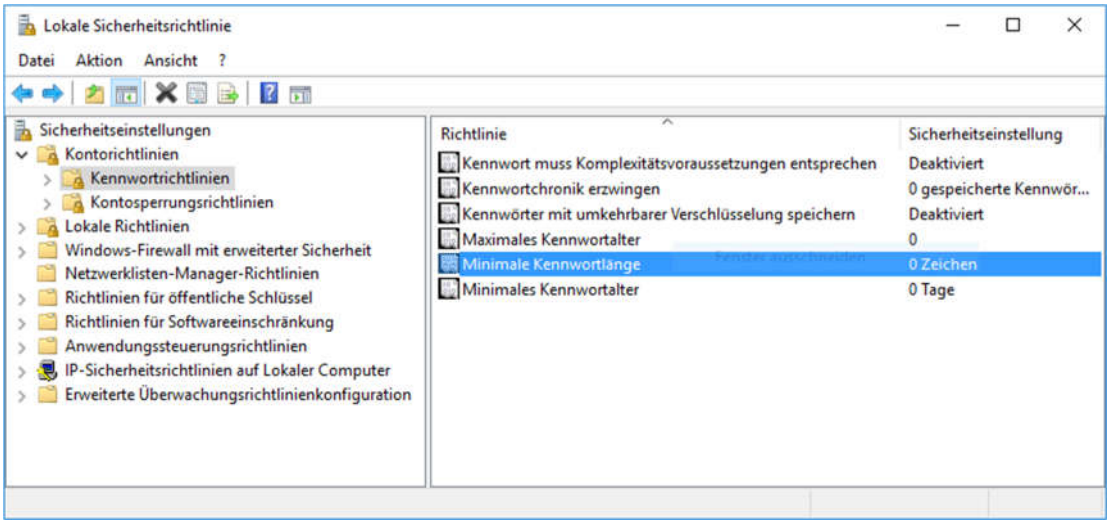
Einige Standardeinstellungen lassen sich auch über die lokalen Gruppenrichtlinien bzw. die lokalen Sicherheitseinstellungen verändern.

- Aufruf der lokalen Gruppenrichtlinien: **gpedit.msc**
- Aufruf der lokalen Sicherheitsrichtlinie: **secpol.msc**

(Die lokalen Sicherheitsrichtlinien sind ein Teil der lokalen Gruppenrichtlinien, durch den direkten Aufruf der Sicherheitsrichtlinien erspart man sich gegebenenfalls ein paar Mausklicks.)

KENNWORTRICHTLINIE ÄNDERN

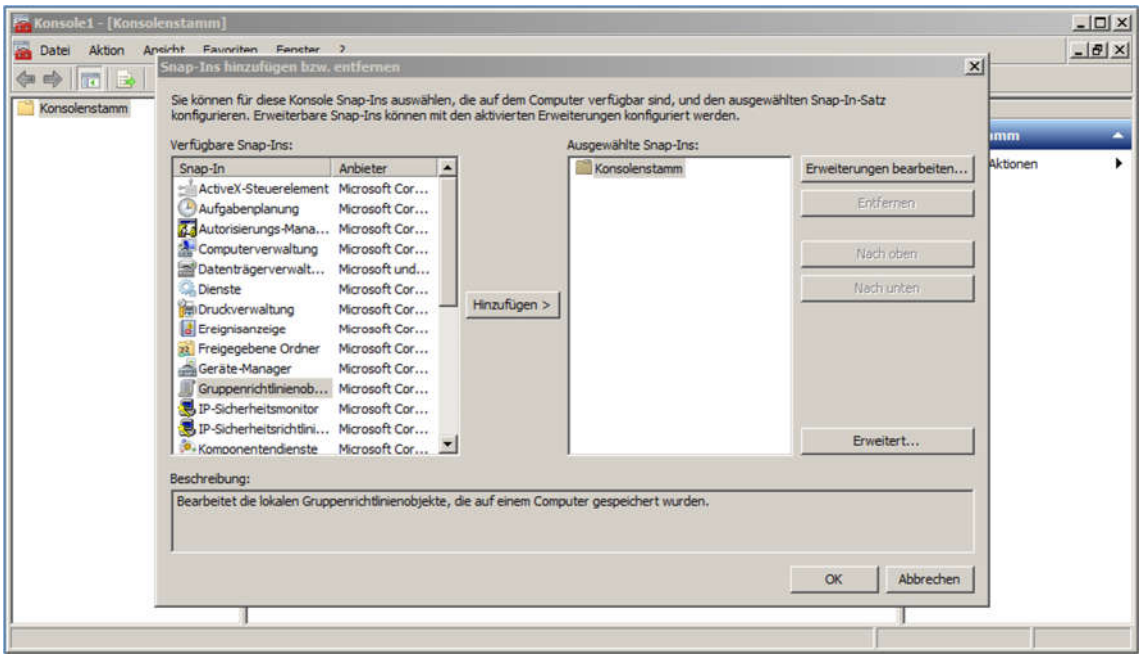
Standardmäßig müssen Benutzer alle 42 Tage ihr Kennwort ändern. Im nachfolgenden Beispiel wird die Kennwortrichtlinie so geändert, dass Kennwörter nicht ablaufen.



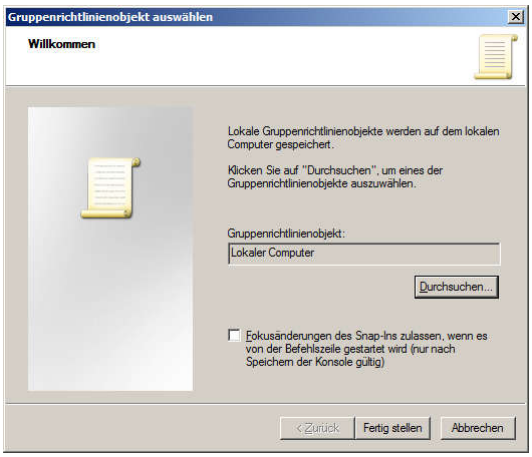
DIFFERENZIERTE GRUPPENRICHTLINIEN FÜR ADMINISTRATOREN UND NICHT-ADMINISTRATOREN

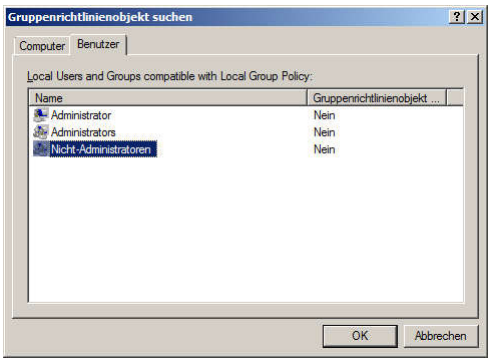
Seit Windows 7 lassen sich lokale Benutzerrichtlinien differenziert für einzelne Benutzer oder Gruppen (z. B. für Administratoren und Nicht-Administratoren) vergeben. Beispielsweise könnte man damit „normalen“ Benutzern verbieten, die Systemsteuerung aufzurufen. Mit etwas Aufwand und genügend Systemkenntnissen lässt sich Windows damit prinzipiell weitgehend gegen unerwünschte Veränderungen absichern.

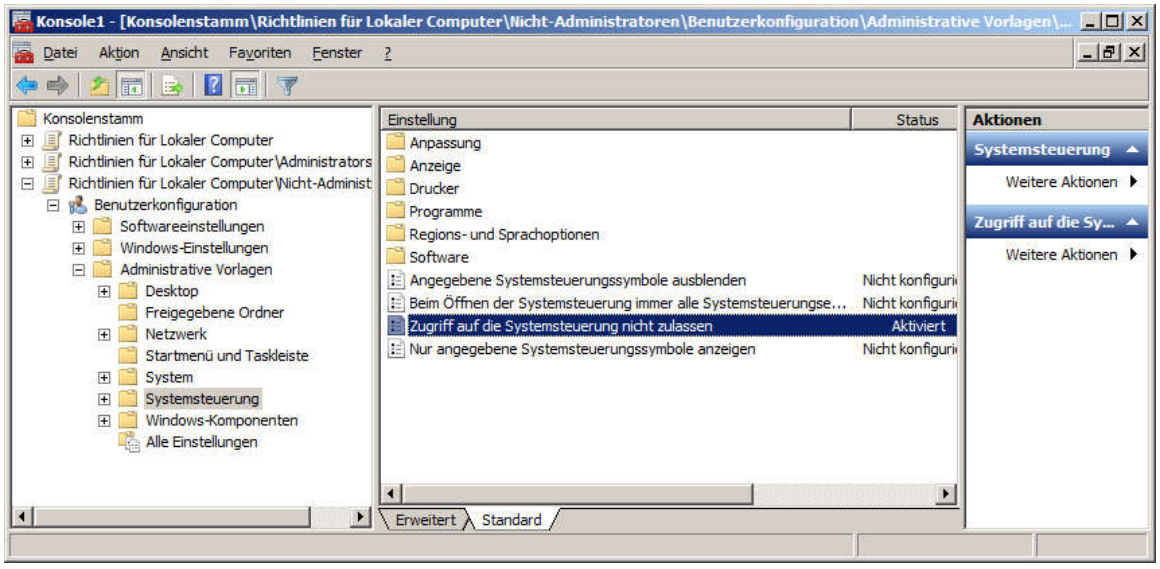
Die differenzierten Gruppenrichtlinien sind über die Microsoft Management Konsole (mmc) erreichbar.



Über das Snap-In „Gruppenrichtlinienobjekte“ lassen sich Gruppenrichtlinienobjekte für den lokalen Computer oder die existierenden Benutzer und Benutzergruppen hinzufügen.







Im angegebenen Beispiel wird der Zugriff auf die Systemsteuerung für Nicht-Administratoren deaktiviert.

ERSTELLEN EINER ANTWORTDATEI

Zum Erstellen einer Antwortdatei für die spätere Mini-Installation stellt Microsoft das Werkzeug WSIM (Windows System Image Manager) bereit. Dieses Werkzeug ist sehr mächtig, erfordert jedoch etwas Einarbeitungszeit. Wer diese Einarbeitungszeit nicht investieren will, kann auch eine vorbereitete Antwortdatei (z. B. mit Quickprep) für sein System übernehmen.

QUICKPREP

Quickprep ist ein kleines Programm, das alle Schritte zur Vorbereitung und zum Versiegeln des Mustercomputes übernimmt. Quickprep wurde speziell für Schulen programmiert und setzt die nachfolgend in dieser Handreichung beschriebenen Arbeitsabläufe jeweils „auf Mausklick“ um.

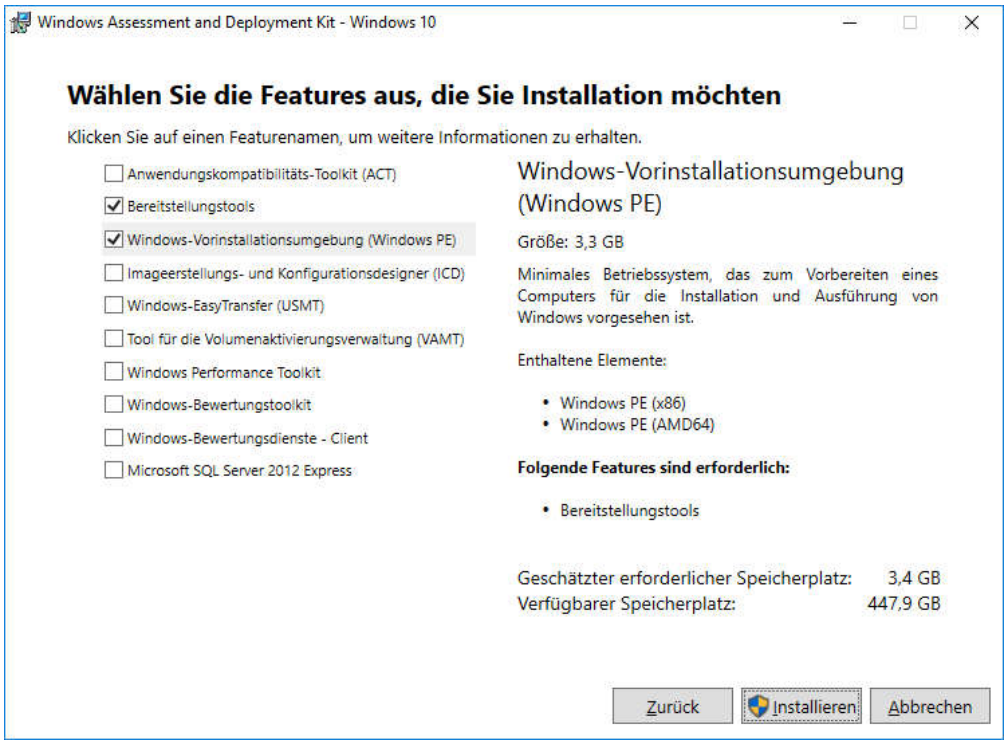
Wer Quickprep einsetzt, kann sich das Weiterlesen dieser Handreichung gegebenenfalls ersparen.

Quickprep findet man unter http://alp.dillingen.de/schulnetz -> Materialien.

INSTALLATION VON ADK

Das zum Erstellen der Antwortdatei notwendige Programm WSIM ist im ADK (Windows Assessment and Deployment Kit) enthalten. ADK wird über eine Setup-Routine von Microsoft zum Download angeboten (Suchbegriffe: Windows ADK).

ADK sollte nicht auf dem Mustercomputer installiert werden. Für diesen benötigt man später nur die fertige Antwortdatei.



WSIM

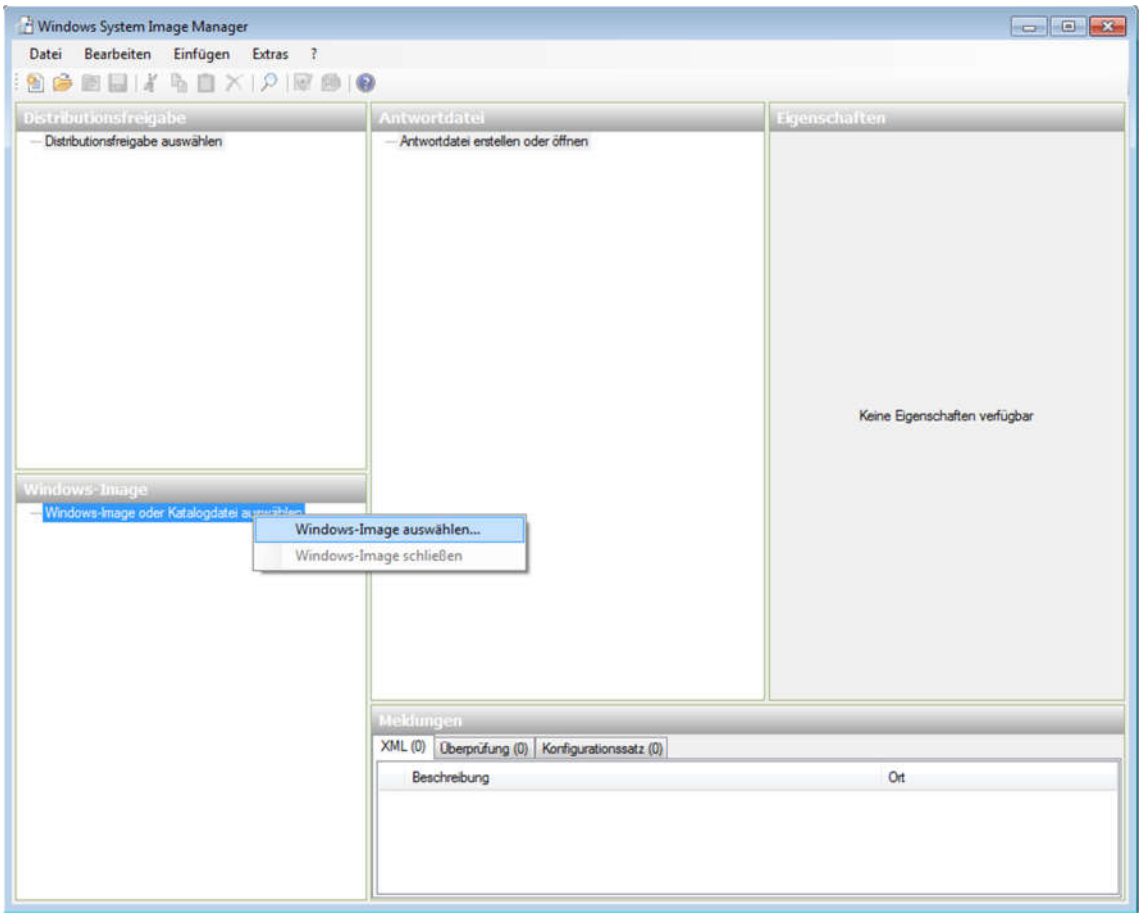
Nach der Installation von ADK startet man den „Windows System Image Manager“ (WSIM).

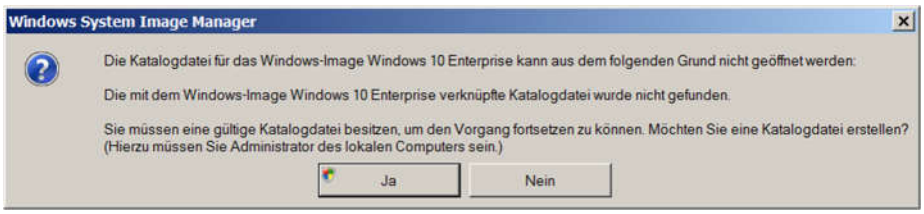
```
Programme -> Microsoft Windows AIK -> Windows System Image Manager
```

WSIM benötigt zum Erstellen einer Antwortdatei eine Vorlage. Diese ist als Katalog in einer Katalogdatei (Endung clg) mit dem zugehörigen Wim-Image gespeichert. In der Katalogdatei ist festgelegt, welche Einstellungen angepasst werden können.

KATALOGDATEI ERSTELLEN

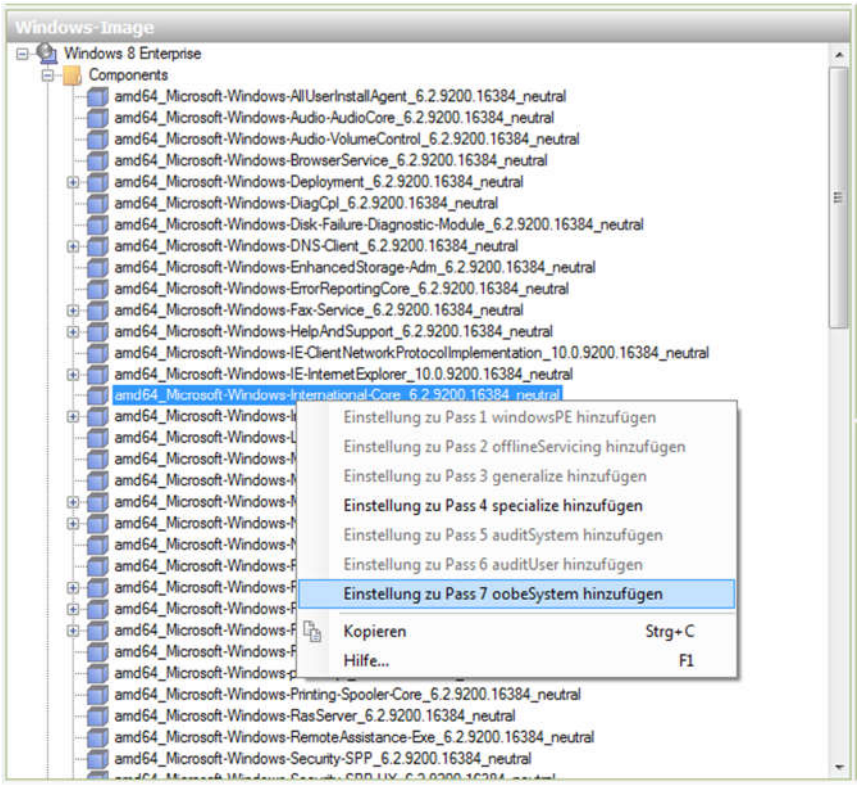
Bei Windows 10 muss die Katalogdatei selbst erzeugt werden. Dazu wird das Windows-Image **install.wim**, das sich im Ordner **sources** auf der Windows 10-DVD befindet, in einen Ordner mit Schreibrechten kopiert. Wird im WSIM das entsprechende Windows-Image ausgewählt, kann die Katalogdatei erzeugt werden.



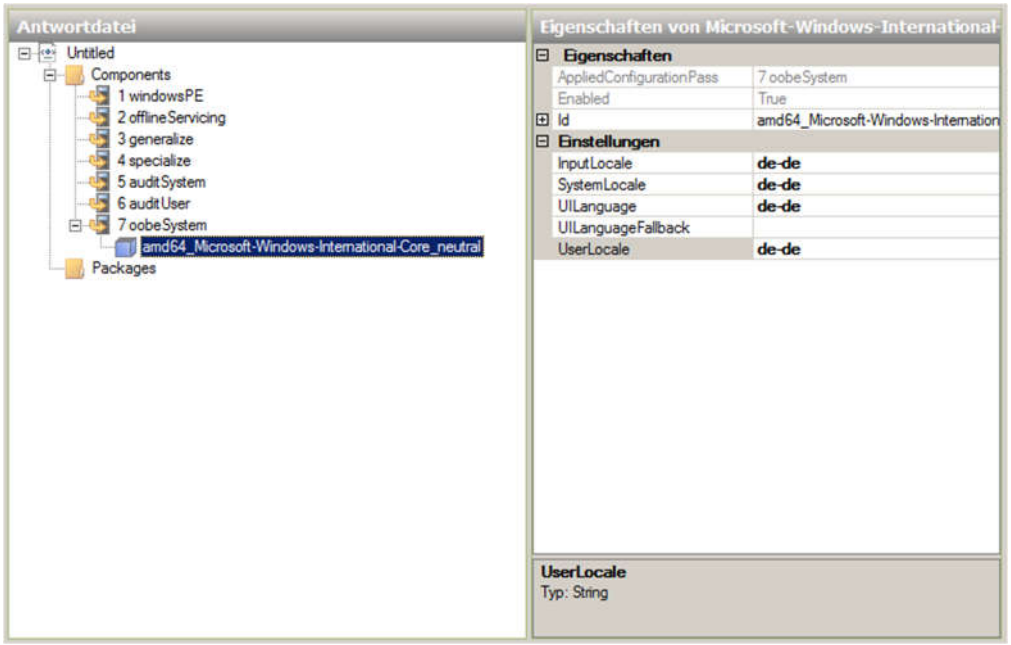


ANTWORTDATEI ERSTELLEN

Nach dem Anlegen einer neuen Antwortdatei können im Fenster „Windows-Image“ unter **Components** die Komponenten ausgewählt werden, die in die Antwortdatei übernommen werden sollen.



Die gewünschten Komponenten werden ausgewählt, der Antwortdatei hinzugefügt und konfiguriert. In diesem Schritt steckt die eigentliche Arbeit. Da es sehr viele Möglichkeiten gibt, kommt man ohne Anleitung oder ein genaues Lesen der kontextbasierten Hilfe (F1) kaum weiter.



Die nachfolgend aufgeführten Einstellungen sind so ausgewählt, dass die Mini-Installation ohne Benutzereingriff durchlaufen wird. Es werden die Benutzer „**Admin**“ (passwortgeschützt, mit administrativen Rechten) und „**standard**“ (normaler Benutzer ohne Passwort) angelegt. Die Profileinstellungen aus dem Audit-Modus werden kopiert und der Benutzer „standard“ wird automatisch angemeldet.

(PASS 3 GENERALIZE)	EIGENSCHAFT	WERT
Microsoft-Windows-Pnp Sysprep	DoNotCleanUpNonPresent-Devices PersistAllDeviceInstalls	True True
(PASS 4 SPEZIALIZE)	**EIGENSCHAFT**	**WERT**
Microsoft-Windows-Shell-Setup	ComputerName CopyProfile ProductKey	* True FJ82H-… *(siehe Hinweise)*
(PASS 7 OOBESYSTEM)	**EIGENSCHAFT**	**WERT**
Microsoft-Windows-International-Core	InputLocale SystemLocale UILanuage UserLocale	de-de de-de de-de de-de
Microsoft-Windows-Shell-Setup	TimeZone	W. Europe Standard Time
Microsoft-Windows-Shell-Setup / AutoLogon	Enabled Username Password Value	True standard *leere Zeichenkette* *(siehe Hinweise)*
Microsoft-Windows-Shell-Setup / OOBE	HideEULAPage NetworkLocation HideWirelessSetupInOOBE ProtectYourPC	true Work true 3
Microsoft-Windows-Shell-Setup / User Accounts / Local Accounts / Local Account	Action Group Name Password Value	AddListItem users Standard *leere Zeichenkette* *(siehe Hinweise)*
Microsoft-Windows-Shell-Setup / User Accounts / Local Accounts / Local Account	Action Group Name Password Value	AddListItem administrators Admin 12345

HINWEISE

- Die Einstellungen in Pass4 (spezialize) werden nur dann ausgeführt, wenn sysprep mit der Option /generalize (Verallgemeinern) ausgeführt wird.
- Der Eigenschaft **Computername=*** bewirkt, dass ein zufälliger Name vergeben wird. Wenn die Eigenschaft nicht gesetzt ist, wird beim ersten Hochfahren des Computers nach dem Namen gefragt.
- Die Eigenschaft **CopyProfile=true** bewirkt, dass die Profileinstellungen (Erscheinungsbild) aus dem Audit-Modus nach „Default User“ kopiert werden und deshalb für alle neu angelegten Benutzer gelten.
- Bei **Windows 10 Enterprise** ist keine Eingabe des Produktschlüssels erforderlich, da der Produkt-Key für die KMS-Aktivierung bereits im Image enthalten ist. Bei **Windows 10 Professional** kann der KMS-Key in der Antwortdatei mitgegeben oder im Vorfeld in der Systemsteuerung eingetragen werden (siehe Seite 6).
- Beim Benutzer „standard“ ist kein Passwort vergeben. Damit dies mit der automatischen Anmeldung nicht zu Fehlern führt, wählt man durch einen Rechtsklick auf Value den Wert „leere Zeichenkette vergeben“.

SPEICHERN DER ANTWORTDATEI

Die Antwortdatei wird unter dem Namen **unattend.xml** gespeichert und auf den Mustercomputer in den Ordner **C:\Windows\Panther\Unattend** oder direkt in den Ordner **C:\Windows\Panther** kopiert.