



# Intune4Windows - optionale Konfigurationen V22.3

im Endpoint Manager

## **Vorarlberger Standardschulinstallation**

Autor: Martin Schnetzer, Kuno Sandholzer,  
Lukas Franz, Dietmar Köb  
Besuchen Sie uns im Internet  
<http://www.vobs.at/rb>

© 2022 IT-Regionalbetreuer Vorarlberg  
6900 Bregenz , Römerstraße 14  
Alle Rechte vorbehalten

# Inhalt

1.	Windows Updates einrichten .....	3
1.1.	Allgemeines .....	3
1.2.	Konfiguration .....	3
2.	Gesichtserkennung (Windows Hello for Business) einrichten .....	5
2.1.	Allgemeines .....	5
2.1.1.	Gleich bei der Geräteregistrierung (also beim Rollout / beim ersten Login): .....	6
2.2.	Wunschkonfiguration .....	7
2.2.1.	Wunschkonfiguration umsetzen .....	7
2.3.	Gesichtserkennung auf dem Gerät einrichten .....	11
3.	Microsoft Edge Konfiguration .....	13
3.1.	Allgemeines .....	13
3.2.	Konfiguration - Startseite .....	13
3.3.	Konfiguration – Favoriten .....	16
4.	Proaktive Korrekturen .....	20
4.1.	Allgemeines von Microsoft: .....	20
4.2.	Einmalige Grundkonfiguration .....	21
4.3.	Erstellen einer Proaktiven Korrektur .....	22
4.4.	Universeller Druckertreiber/Druckerinstallation .....	25
4.5.	Veyon Installation und Konfiguration .....	25
4.5.1.	Grundvoraussetzung – Installation Client/Master: .....	25
4.5.2.	Veyon Konfiguration .....	27
4.6.	Skripte .....	28
4.6.1.	Veyon-Key Master (Lehrer) Geräte .....	28
4.6.2.	Veyon-Key Client (Schüler) Geräte .....	29
4.6.3.	Veyon-Klassenliste Aktualisierung .....	31
4.6.4.	HP-Drucker Installation mit dem HP Universal Drucker Treiber .....	33
4.6.5.	KonicaMinolta-Drucker Installation mit dem Universal Drucker Treiber .....	35
4.6.6.	Ricoh Universal Drucker Treiber .....	37
5.	McAfee Remover .....	39
5.1.	Allgemeines .....	39
5.2.	Automatisches Entfernen vom vorinstalliertem McAfee Live System .....	39
5.3.	Bereitstellen des Paketes: .....	41

# 1. Windows Updates einrichten

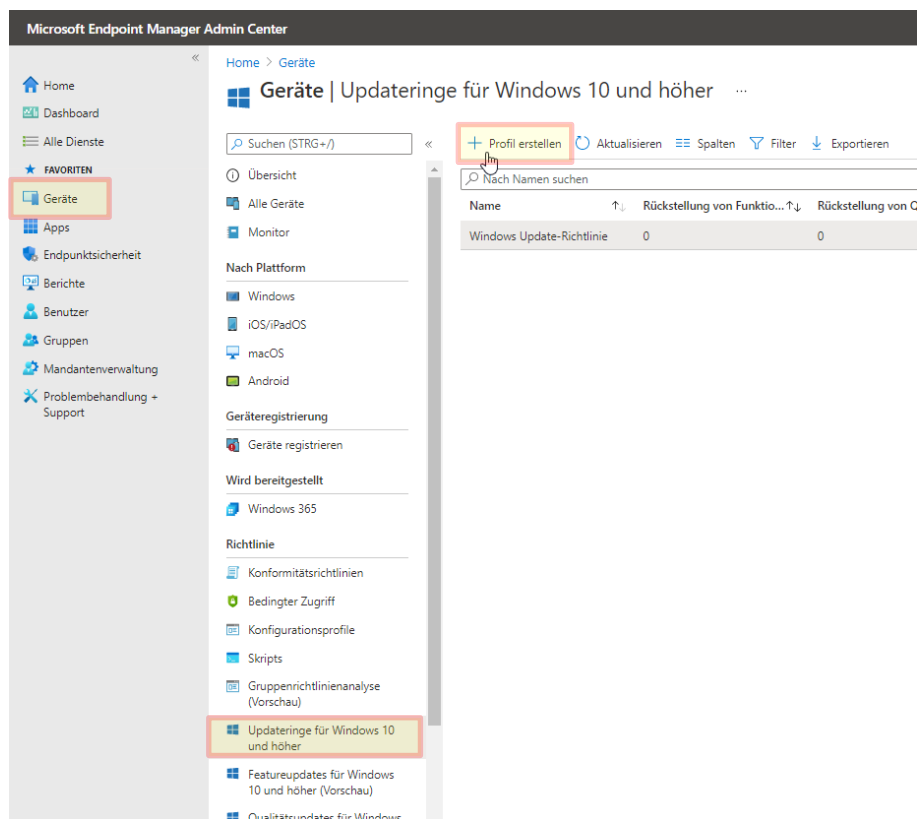
## 1.1. Allgemeines

Für einen sicheren Betrieb sind aktuelle Systeme erforderlich. Diese können über vorgegebene Richtlinien konfiguriert werden.

## 1.2. Konfiguration

- Öffnen des Endpoint Managers (<https://endpoint.microsoft.com>) → Geräte → Updatere für Windows 10 und höher.
- Profil erstellen mit dem Namen: Windows Updates für Schülergeräte
- Standardmäßig kann alles so eingestellt bleiben – evtl. die Nutzungszeit des Gerätes, wenn nötig ändern.
- Der Gruppe C\_SuS zuordnen

Analog dazu kann auch ein Update-Profil für die Lehrer-Geräte konfiguriert werden (Gruppe: C\_LuL).



Microsoft Endpoint Manager Admin Center

Home > Geräte >

## Updatierung für Windows 10 und höher erstellen

Windows 10 und höher

✓ Grundlagen ✓ Einstellungen für Updatierung ③ Zuweisungen ④ Überprüfen + erstellen

Name \*

Beschreibung

Zurück Weiter

Microsoft Endpoint Manager Admin Center

Home > Geräte >

## Updatierung für Windows 10 und höher erstellen

Windows 10 und höher

✓ Grundlagen ④ Einstellungen für Updatierung ③ Zuweisungen ④ Überprüfen + erstellen

### Einstellungen aktualisieren

Wartungskanal

Microsoft-Produktupdates \*

Windows-Treiber \*

Rückstellungszeitraum für Qualitätsupdates (Tage) \*

Rückstellungszeitraum für Funktionsupdates (Tage) \*

Zeitraum für das Deinstallieren von Featureupdates (2 bis 60 Tage) \*

### Einstellungen für Benutzeroberfläche

Automatisches Updateverhalten

Beginn der Nutzungszeit \*

Ende der Nutzungszeit \*

Neustartüberprüfungen

Option zum Anhalten von Windows-Updates

Option zum Suchen nach Windows-Updates

Benutzergenehmigung zum Schließen der Neustartbenachrichtigung erforderlich

Vor einem erforderlichen automatischen Neustart: Einrichten von Benutzer...

Zurück Weiter

Microsoft Endpoint Manager Admin Center

Home > Geräte >

## Updatierung für Windows 10 und höher erstellen

Windows 10 und höher

✓ Grundlagen ✓ Einstellungen für Updatierung ③ Zuweisungen ④ Überprüfen + erstellen

Eingeschlossene Gruppen

Alle Benutzer hinzufügen + Alle Geräte hinzufügen

Keine Gruppen ausgewählt

Ausgeschlossene Gruppen

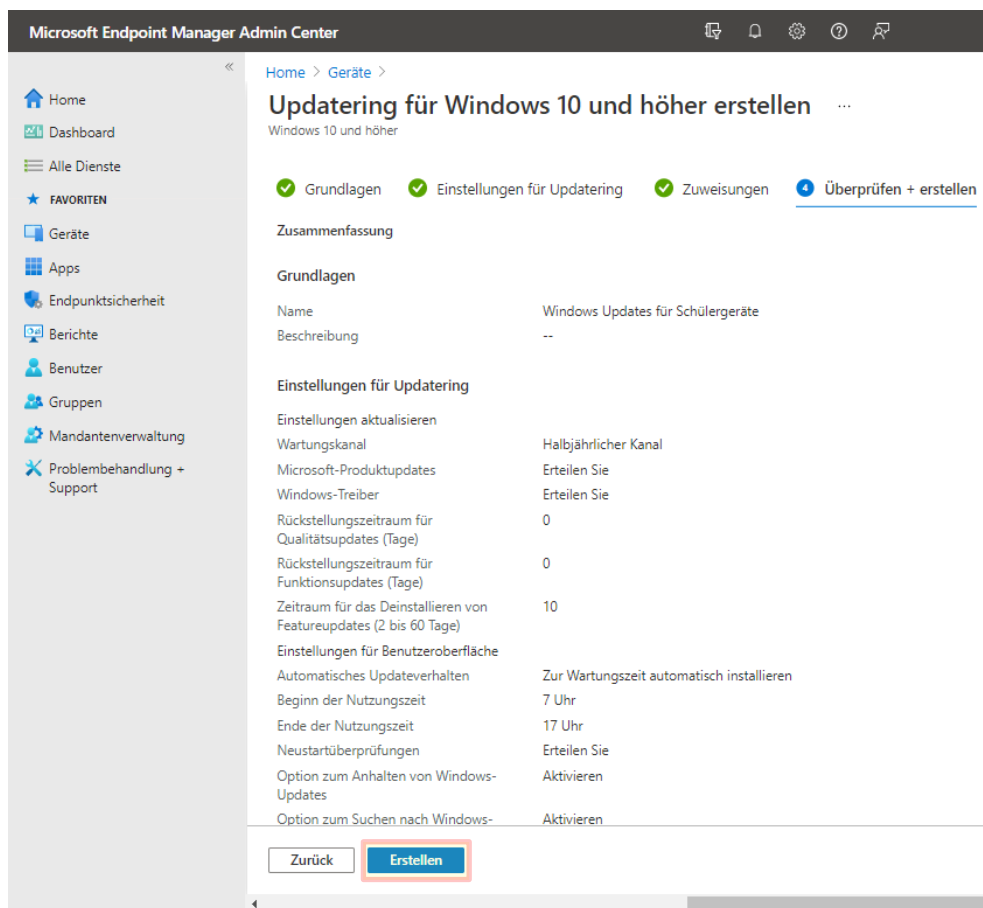
Beim Ausschließen von Gruppen können Benutzer- und Gerätegruppen in den Optionen "Ausschließen" nicht gemischt verwendet werden. Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück Weiter

### Wählen Sie die Gruppen aus, die eingeschlo...

Azure AD-Gruppen

Ausgewählte Elemente



## 2. Gesichtserkennung (Windows Hello for Business) einrichten

### 2.1. Allgemeines

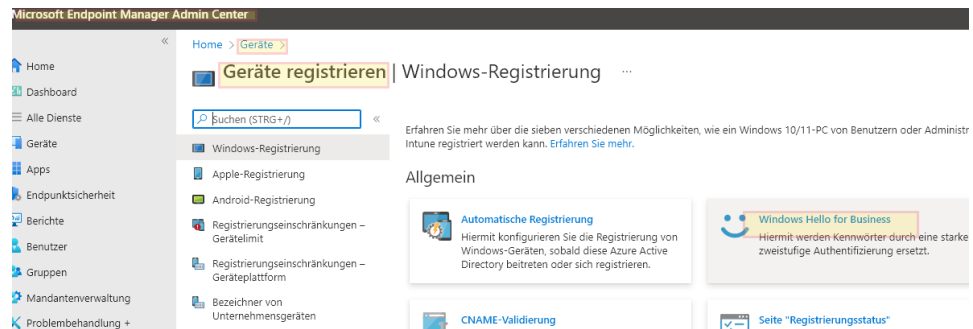
Die Windows-SurfaceGo2-Tablets bzw. die eingebauten Kameras unterstützen die Anmeldung am Gerät (anstatt der Eingabe von Benutzername und Passwort) per Gesichtserkennung. Um diese komfortable Loginvariante mit Gesichtserkennung überhaupt nutzen zu können, muss auf den Geräten „Windows Hello for Business“ über Intune aktiviert werden.

Hinweise dazu:

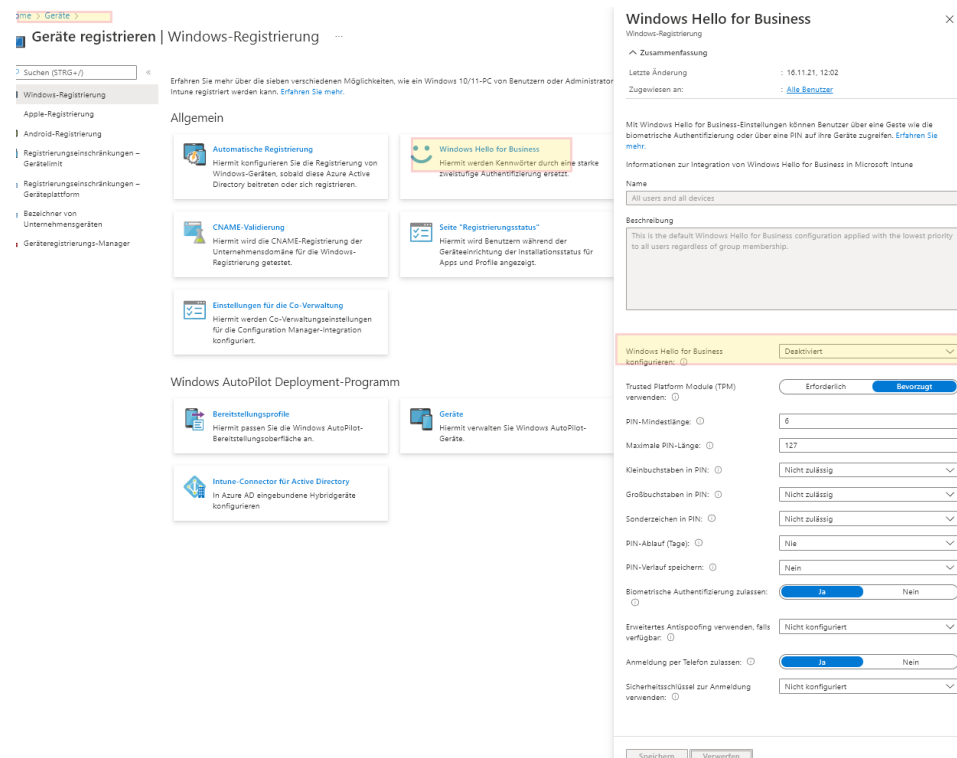
- Wird die Gesichtserkennung in Intune aktiviert, muss verbindlich auch ein PIN (min. 6 Zahlen – und nur Zahlen) vergeben werden. Zusätzlich muss für die PIN-Einrichtung **einmalig** ein Handy (TAN per SMS oder Authenticator-App installieren) zur Verfügung stehen.
- Die Einrichtung der Gesichtserkennung kann übersprungen werden (und später nach der erfolgreichen Anmeldung nachgeholt werden).
- PIN und eingerichtete Gesichtserkennung gelten nur für den angemeldeten Benutzer und nur für dieses eine Gerät, auf dem es eingerichtet wird.

Grundsätzlich kann „Windows Hello for Business“ in Intune auf mehrere Arten / an mehreren Stellen konfiguriert werden – z. B.:

### 2.1.1. Gleich bei der Geräteregistrierung (also beim Rollout / beim ersten Login):



Standardeinstellung sieht dort so aus:



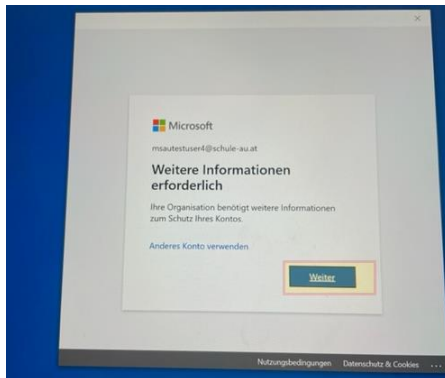
Wir belassen hier die Standardeinstellung bzw. stellen beim Punkt „Windows Hello for Business konfigurieren“ deaktiviert ein. Damit werden die „Windows Hello for Business“-Einstellungen nicht von Intune gesteuert. Bestehende Windows Hello for Business-Einstellungen auf Windows-Geräten werden nicht geändert.

Warum ist das **unsere Empfehlung**:  
Wird das hier aktiviert, **muss**

1. Windows Hello for Business (bei uns Gesichtserkennung und PIN-Einrichtung mit Handy) gleich bei der Registrierung (beim zweiten Login auf dem Gerät) mit eingerichtet werden.

Hinweis dazu:

Diese Aufforderung bei der Anmeldung kann übersprungen werden:



... **aber**: Diese Aufforderung zur Einrichtung erscheint bei jedem Login 😞.

2. „Windows Hello for Business“ **auf allen Geräten und von allen Benutzern** eingerichtet werden. Das wollen wir so nicht, weil einerseits die Einrichtung und Verwendung von „Windows Hello for Business“ nicht auf allen Geräten (z. B. Lehrergeräte, die von verschiedenen Benutzern verwendet werden) verbindlich gefordert werden soll und andererseits während des Rollout-Prozesses viele andere Dinge zu erledigen sind.

Mit dieser Einstellung alleine ist jedoch „Windows Hello for Business“ (eine Variante davon ist die „Gesichtserkennung“ als Anmeldeoption) auf allen Geräten deaktiviert und kann selbst vom lokalen Administrator auf den Geräten nicht aktiviert werden.

## 2.2. Wunschkonfiguration

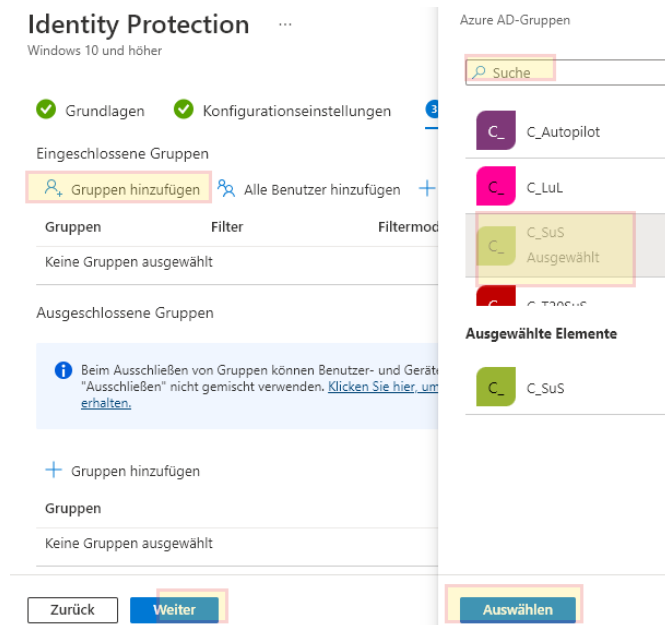
Unser Wunschkonfiguration wäre: Die „Windows Hello for Business“ – Aufforderung zur ersten Einrichtung soll während des Anmeldevorganges nie erscheinen. Es soll aber jedem User vorbehalten und möglich sein, die Gesichtserkennung nach der Anmeldung mit dem Kennwort jederzeit nachträglich einzurichten.

### 2.2.1. Wunschkonfiguration umsetzen

#### 1) „Windows Hello for Business“ über ein Konfigurationsprofil aktivieren

„Geräte“ -> „Konfigurationsprofile“ -> „+Profil erstellen“





-> keine Anwendbarkeitsregeln -> „Erstellen“

Damit wird „Windows Hello for Business“ nur für die Schüler-Gerätegruppe aktiviert.

**Wichtiger Hinweis:** Diese Einstellung bitte erst nach dem großen Rollout (= Geräte an die SuS verteilen, Erstregistrierung durchführen, alle Win-Updates machen ....) „scharf“ stellen (= erst dann eine Gerätegruppe (siehe oben „C\_SuS“) dieser Richtlinie zuordnen). Ansonsten kann es passieren, dass während der Anmeldung die Aufforderung zum Einrichten der Gesichtserkennung und des PINs erfolgt, weil die Registryeinträge (siehe unten) noch nicht vorhanden sind bzw. noch nicht greifen. Die „Einrichtungs-Aufforderung“ kann zwar übersprungen werden (siehe oben), stört aber während des Rollouts.

Damit die Aufforderung zur Einrichtung der Gesichtserkennung nicht bei jedem Login erscheint, müssen wir auch noch einen Registryeintrag setzen:

## 2) „Registryeintrag“:

Folgende zwei Registryeinträge sind dazu notwendig:

```
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\PassportForWork" /v Enabled /t REG_DWORD /d 1 /f
```

```
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\PassportForWork" /v DisablePostLogonProvisioning /t REG_DWORD /d 1 /f
```

Das kann z. B. über ein Powershellscript gemacht werden - Inhalt des Powershellscripts:

```
$Path = "HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork"
If (!(Test-Path $Path)) {
    New-Item -Path $Path
}
Set-ItemProperty -Path $Path -Name 'DisablePostLogonProvisioning' -Type "DWORD" -value "1" -FORCE
Set-ItemProperty -Path $Path -Name "Enabled" -Type 'DWORD' -value "1" -FORCE
```

Diese drei Befehlszeilen in eine Textdatei kopieren und z. B. als „No\_HelloEinrichtung\_bei\_Logon.ps1“ abspeichern.

... oder hier herunterladen:

[No\\_HelloEinrichtung\\_bei\\_Logon.ps1](#)

.. und das dann in Intune implementieren:

„Geräte“ -> „Windows“ -> „PowerShell-Skripts“ -> „+Hinzufügen“:

Microsoft Endpoint Manager Admin Center

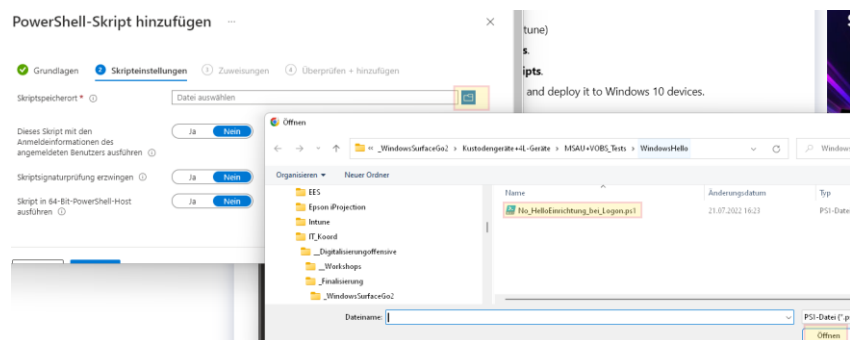
Home > Geräte > Windows >

### PowerShell-Skript hinzufügen

1 Grundlagen 2 Skripteinstellungen 3 Zuweisungen 4 Überprüfen + hinzufügen

Name \*

Beschreibung



### PowerShell-Skript hinzufügen

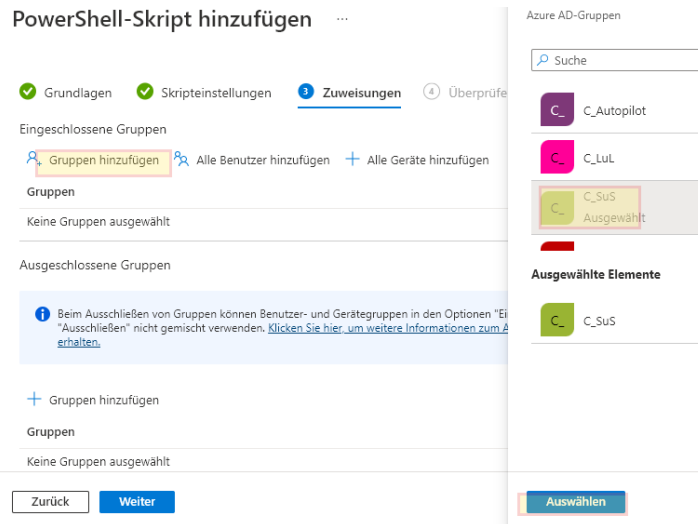
1 Grundlagen 2 Skripteinstellungen 3 Zuweisungen 4 Überprüfen

Skriptspeicherort \*

Dieses Skript mit den Anmeldeinformationen des angemeldeten Benutzers ausführen

Skriptsignaturprüfung erzwingen

Skript in 64-Bit-PowerShell-Host ausführen



-> „Hinzufügen“ -> fertig

Die Zuordnung zur Gerätegruppe kann und soll hier sehr wohl sofort gemacht werden (also schon bevor die Richtlinie oben scharf geschaltet wird).

### 2.3. Gesichtserkennung auf dem Gerät einrichten

Auf dem Gerät im Suchfeld links unten „Anmeldeoptionen“ eingegeben:

#### Anmeldeoptionen

#### Vorgehensweise für die Anmeldung an Ihrem Gerät verwalten

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

**Windows Hello-Gesichtserkennung**  
Mit Kamera anmelden (empfohlen)

Sie können sich bei Windows, Apps und Diensten anmelden, indem Sie Windows Hello beibringen, Ihr Gesicht zu erkennen.

[Weitere Informationen](#)

**Einrichten**

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

[Weitere Informationen](#)

**Los geht's** **Abbrechen**

Die Kamera erscheint und richtet Gesichtsmerkmale ein ...

Zusätzlich muss verbindlich eine PIN eingerichtet werden (min. 6 Zahlen – und nur Zahlen):

Noch ein paar Dinge...

Erstellen Sie eine PIN für den Fall, dass die Gesichtserkennung nicht verfügbar ist. Vermutlich werden Sie die PIN nie benötigen. Sie dient nur zur Sicherheit.

Sobald Sie Ihre PIN eingerichtet haben, können Sie sich per Gesichtserkennung anmelden.

Tipp: Wenn Sie beim Einrichten der Gesichtserkennung eine Brille trugen, wählen Sie "Erkennung verbessern" aus, um die Einrichtung erneut und ohne Brille durchzuführen. So können wir Sie mit und ohne Brille erkennen.

[Erkennung verbessern](#)

Windows Hello mit Ihrem Konto verwenden

Ihre Organisation verlangt, dass Sie Ihr Geschäfts-, Schul- oder Unikonto mit Windows Hello-Gesichtserkennung, der Fingerabdruckerkennung oder einer PIN einrichten.

Wenn Windows Hello auf diesem Gerät bereits eingerichtet ist, wird es automatisch für dieses Konto hinzugefügt. Sie werden möglicherweise zur erneuten Verifizierung bei Windows Hello aufgefordert.

Wenn Ihre Organisation eine komplexere PIN verlangt, werden Sie von Windows zur Änderung aufgefordert.



**PIN einrichten**

**OK**



msautestuser3@schule-au.at

## Weitere Informationen erforderlich

Ihre Organisation benötigt weitere Informationen zum Schutz Ihres Kontos.

[Anderes Konto verwenden](#)

[Weiter](#)

## Schützen Sie Ihr Konto

Für Ihre Organisation ist es erforderlich, die folgenden Methoden zum Nachweis Ihrer Identität einzurichten.

### Microsoft Authenticator



Rufen Sie zuerst die App ab.

Installieren Sie die Microsoft Authenticator-App auf Ihrem [herunterladen](#)

Nachdem Sie die Microsoft Authenticator-App auf Ihrem haben, wählen Sie "Weiter".

[Ich möchte eine andere Authentifikator-App verwenden](#)

[Ich möchte eine andere Methode einrichten.](#)

## Andere Methode auswählen

Welche Methode möchten Sie verwenden?

[Telefon](#)

[Abbrechen](#)

[Bestätigen](#)

## Telefon

Sie können Ihre Identität nachweisen, indem Sie einen Code per SMS an Ihr Telefon senden lassen.

Welche Telefonnummer möchten Sie verwenden?

[Austria \(+43\)](#) [664123123](#)

☒ Code per SMS an mich senden

Möglicherweise gelten die Nachrichten- und Datentarife. Durch Auswählen von "Weiter" erklären Sie sich mit den [Vertragsbedingungen](#) und [Bestimmungen zu Datenschutz und Cookies](#) einverstanden.

[Weiter](#)

## Telefon

Wir haben gerade einen 6-stelligen Code an +43 6646255330 gesendet.

[Code eingeben](#)

[Code erneut senden](#)

Telefon

[Die SMS wurde verifiziert. Ihr Telefon wurde erfolgreich registriert.](#)

[Weiter](#)

## Schützen Sie Ihr Konto

Für Ihre Organisation ist es erforderlich, die folgenden Methoden zum Nachweis Ihrer Identität einzurichten.

Erfolgreich!

Sehr gut! Ihre Sicherheitsinformationen wurden erfolgreich eingerichtet. Klicken Sie auf "Fertig", um die Anmeldung fortzusetzen.

Standardanmeldemethode:

[Telefon +43 6646](#)

[Fertig](#)

Windows-Sicherheit

## PIN einrichten

Erstellen Sie eine PIN, die anstelle von Kennwörtern verwendet wird. Eine PIN erleichtert die Anmeldung bei Geräten, Apps und Diensten.



Neue PIN

PIN bestätigen

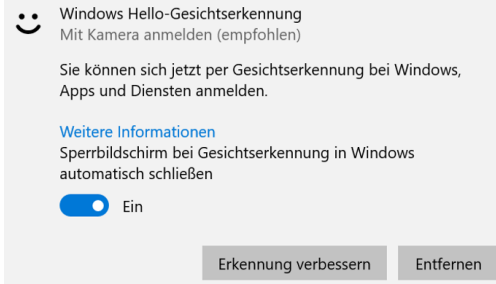
☐ Buchstaben und Symbole einschließen

[OK](#)

[Abbrechen](#)

erledigt:

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



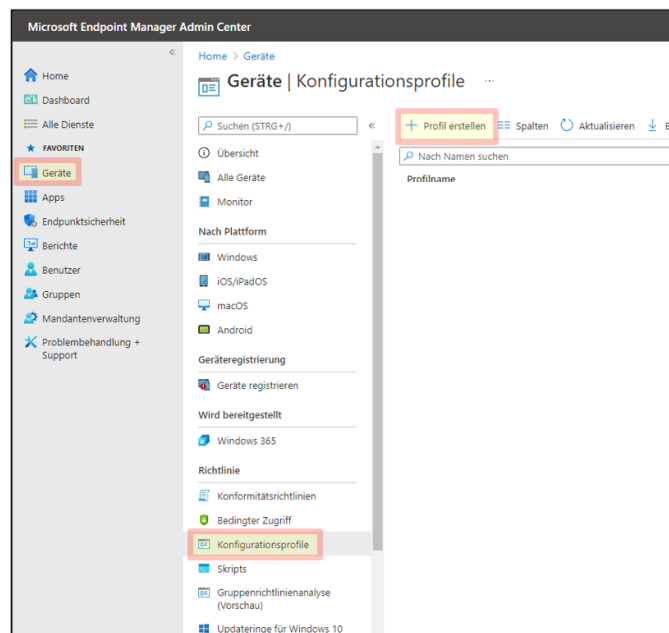
### 3. Microsoft Edge Konfiguration

#### 3.1. Allgemeines

Die Startseite kann nicht über die Standardrichtlinie für EDU konfiguriert werden, sondern muss zusätzlich mit einem Konfigurationsprofil eingerichtet werden.

#### 3.2. Konfiguration - Startseite

Öffnen des Endpoint Managers (<https://endpoint.microsoft.com>) → Geräte → Konfigurationsprofile  
→ Profil erstellen



### Profil erstellen

Plattform  
Windows 10 und höher

Profiltyp  
Vorlagen

Vorlagen enthalten Gruppen von Einstellungen, die nach Funktionalität angeordnet sind. Verwenden Sie eine Vorlage, wenn Sie Richtlinien nicht manuell erstellen oder Geräte für den Zugriff auf Unternehmensnetzwerke konfigurieren möchten, z. B. durch das Konfigurieren von WLAN oder VPN. [Weitere Informationen](#)

Suchen

Name der Vorlage

Administrative Vorlagen

Benutzerdefiniert

Domänenbeitritt

E-Mail

Editionsupgrade und Moduswechsel

Endpoint Protection

### Microsoft Endpoint Manager Admin Center

Home > Geräte > Profil erstellen

Administrative Vorlagen

Grundlagen Konfigurationseinstellungen Berichtstags Zuweisungen Überprüfen + erstellen

Name MS Edge Startseite

Beschreibung Konfiguration der Startseite und Schaltfläche Startseite auf Symbolleiste

Name:  
MS Edge Startseite

Beschreibung:  
Konfiguration der Startseite und Schaltfläche Startseite auf Symbolleiste

Grundlagen Konfigurationseinstellungen Berichtstags Zuweisungen Überprüfen + erstellen

Alle Einstellungen

Computerkonfiguration

Microsoft Edge

Benutzerkonfiguration

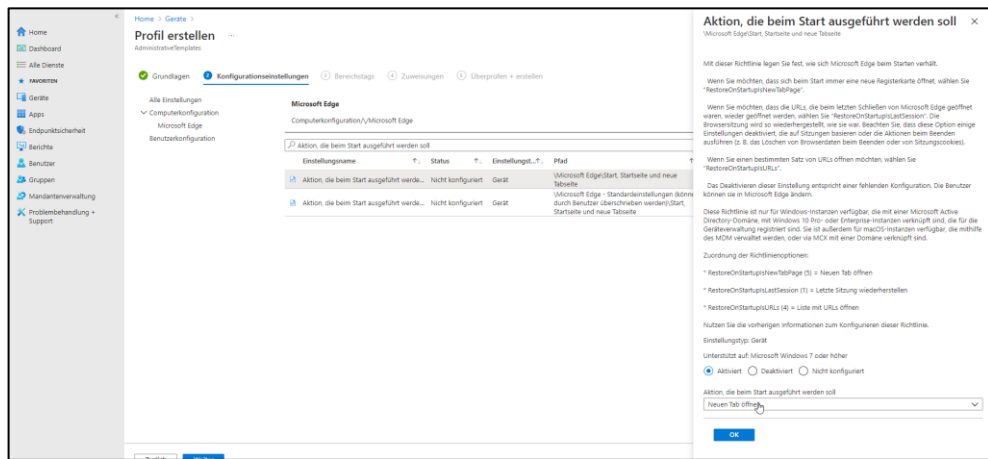
### Computerkonfiguration

Computerkonfiguration

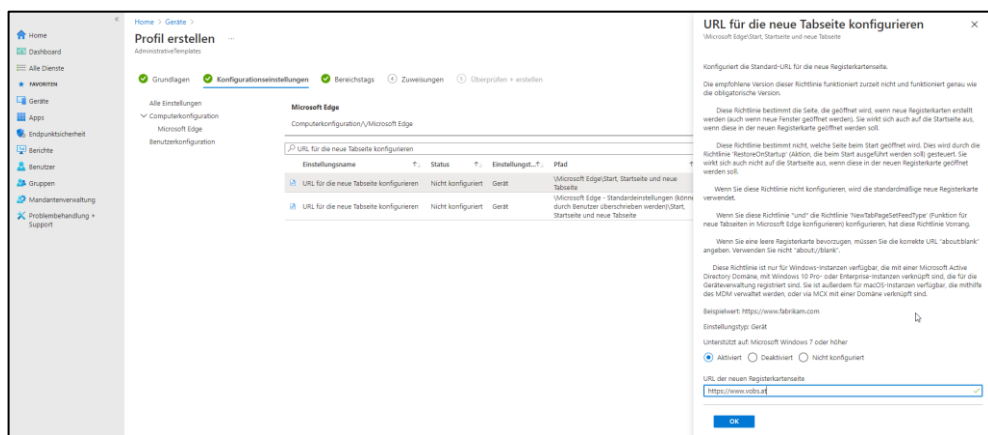
Suchen, um Elemente zu filtern...

Einstellungsname	Status	Einstellungstyp	Pfad
Drucker			
LAPS			
Microsoft Edge			
Microsoft Edge - Standardeinstellungen...			
Microsoft Edge WebView2			
Microsoft Edge-Update			
Microsoft Office 2016 (Computer)			
Microsoft PowerPoint 2016 (Computer)			

**Fünf Konfigurationen für Microsoft Edge:**



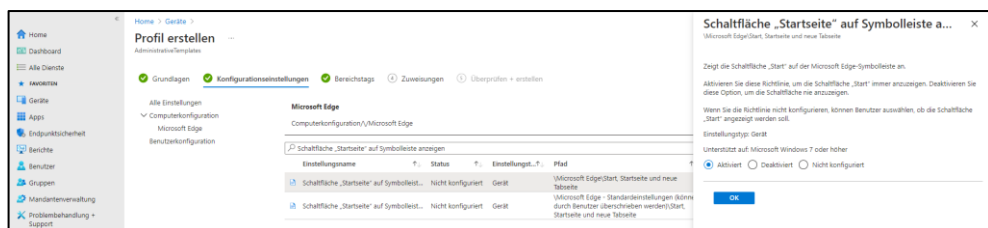
- Aktion, die beim Start ausgeführt werden soll
- Aktivieren und Neuen Tab öffnen



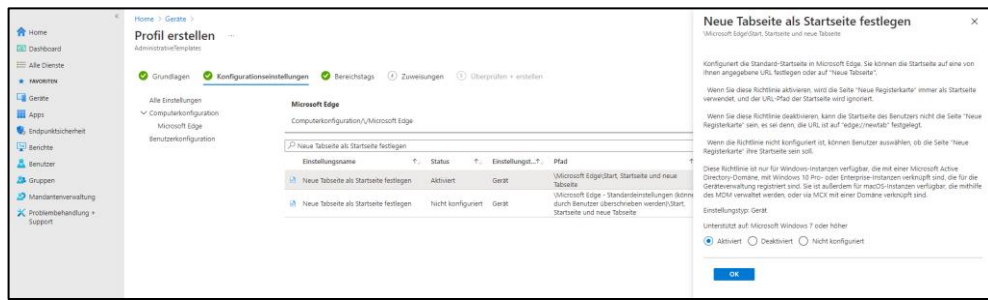
- URL für die neue Tabseite konfigurieren
- Aktivieren und gewünschte Seite angeben „https://www.vobs.at“



- Die Standardwebsites der obersten Ebene auf der neuen Tabseite ausblenden
- Aktivieren

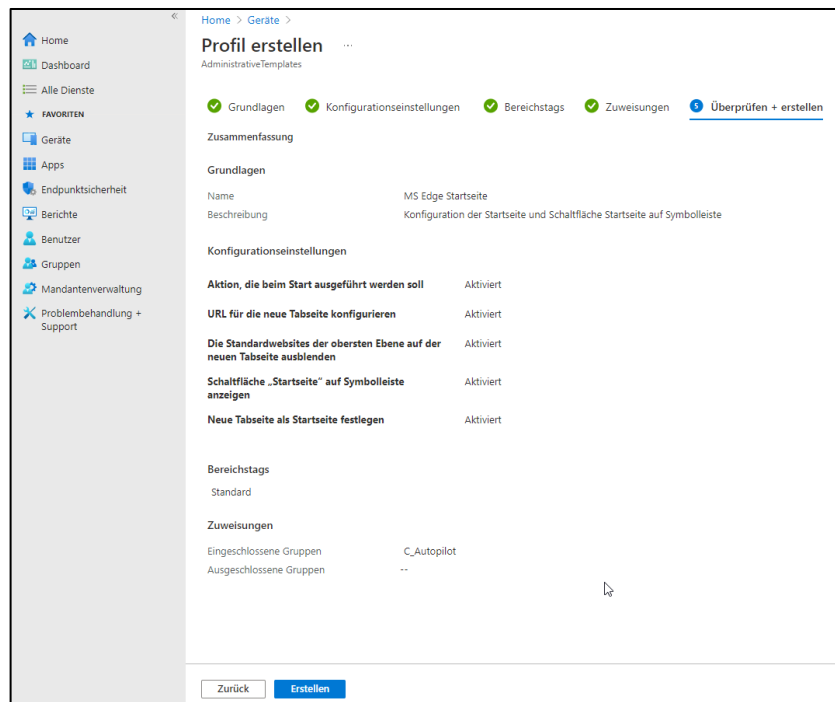


- Schaltfläche „Startseite“ auf Symbolleiste anzeigen
- Aktivieren



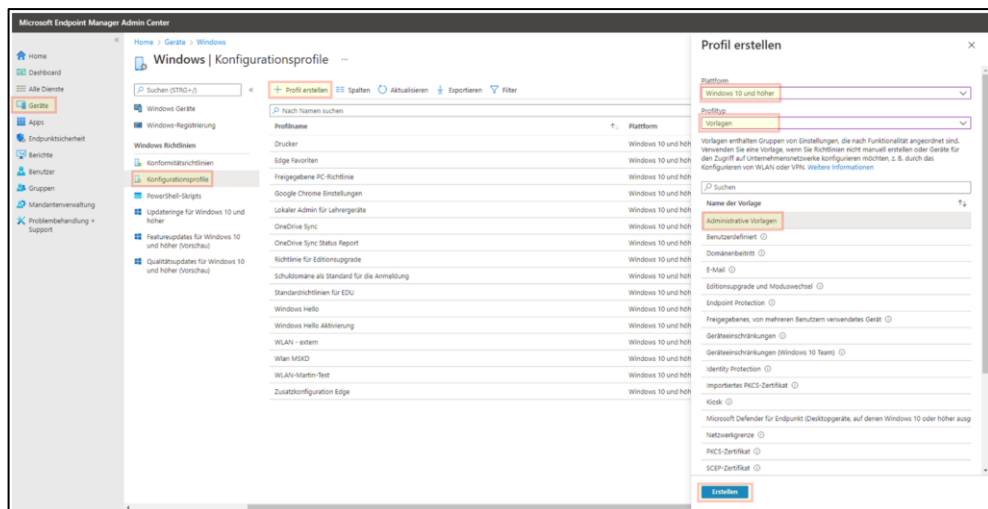
- Neue Tabseite als Startseite festlegen
- Aktivieren

Zuweisung der Gruppe C\_Autopilot.



### 3.3. Konfiguration – Favoriten

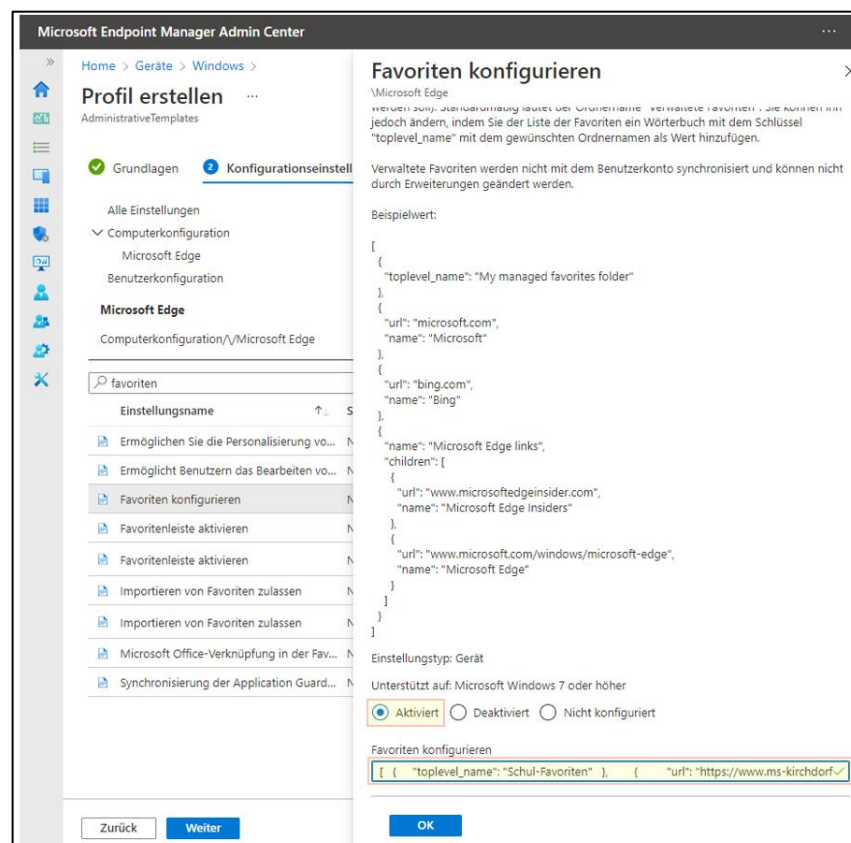
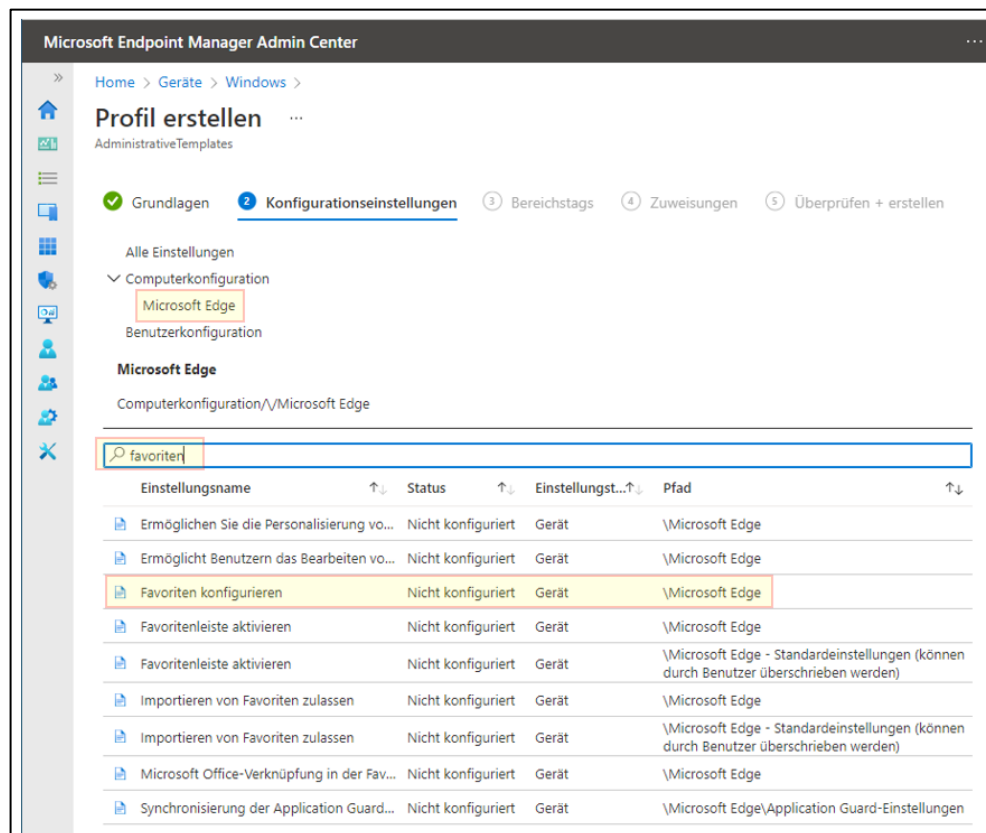
Erstellen eines neuen Geräte-Konfigurationsprofil



Name des Konfigurationsprofils: MS Edge Favoriten – Administratives Template

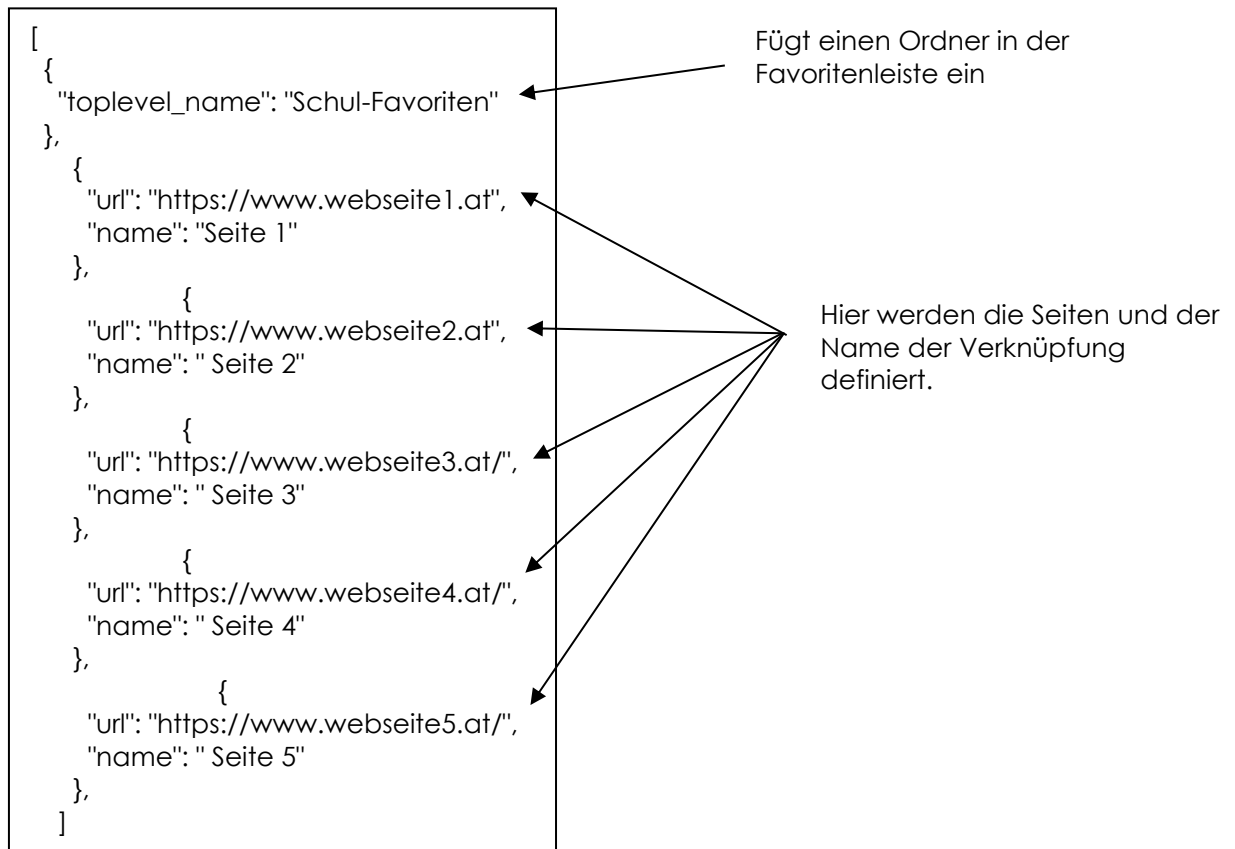
Beschreibung: Favoriten mit Liste bereitstellen

Nach dem „Erstellen“ klicken - Microsoft Edge in der Liste auswählen. Danach die „Favoriten“ im Suchfeld suchen.

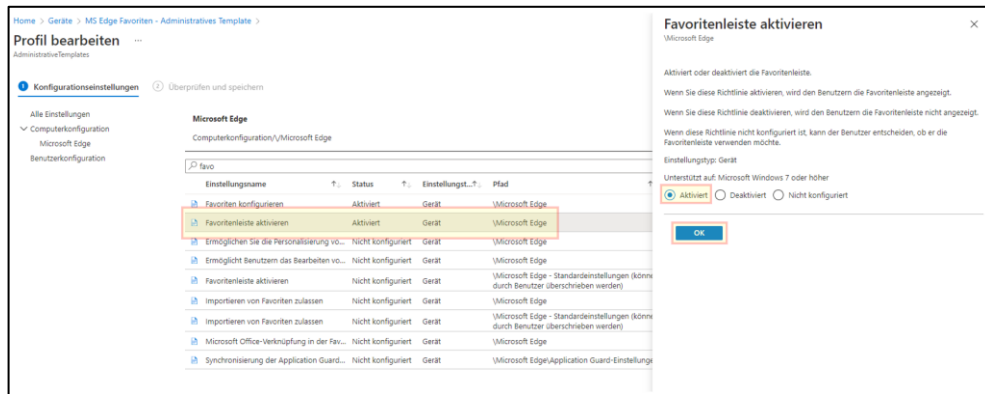


Im Feld „Favoriten konfigurieren“ wird nun folgender Eintrag hinzugefügt.

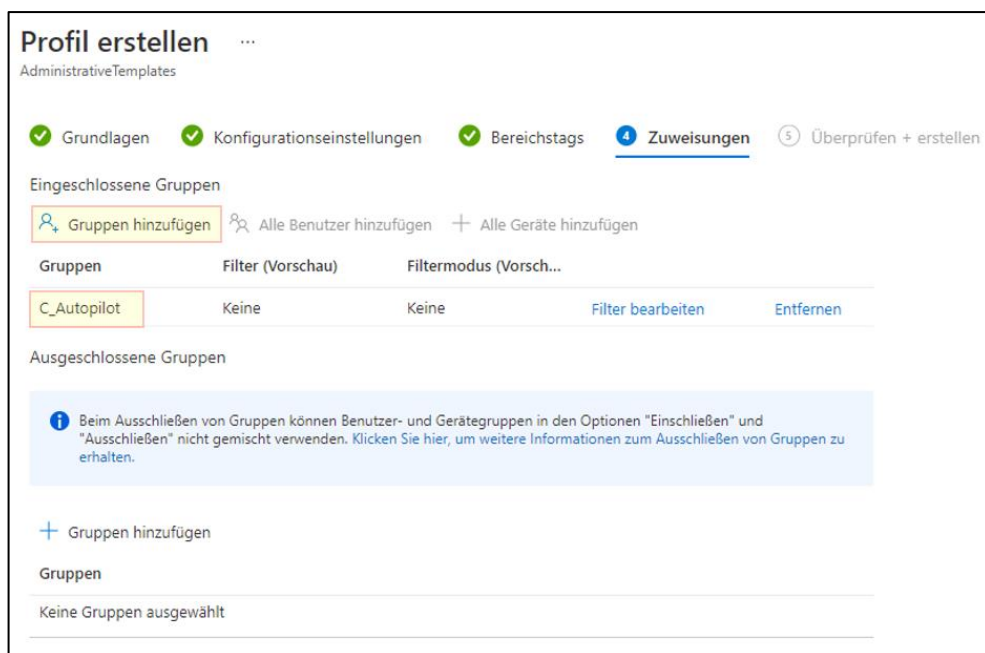
Beispiel:



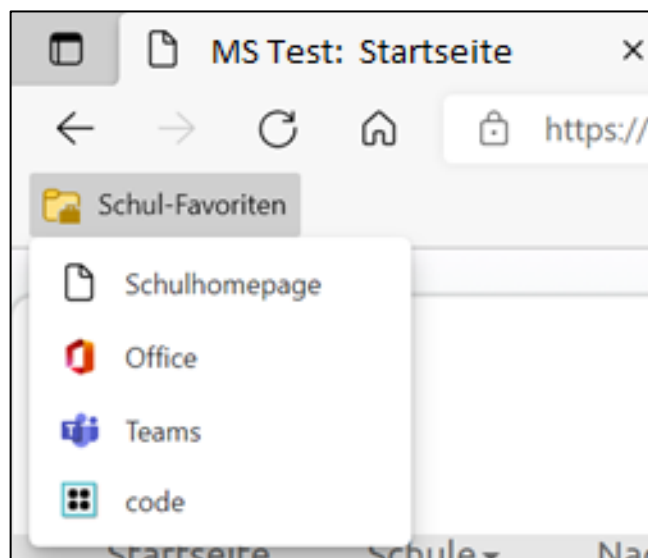
Im Anschluss wird noch die Favoritenleiste aktiviert



Im letzten Schritt fügen wir wiederum die entsprechende Gruppe hinzu. Z.B. C\_Autopilot



Zum Schluss alles nochmals Überprüfen und erstellen.



## 4. Proaktive Korrekturen

### 4.1. Allgemeines von Microsoft:

<https://learn.microsoft.com/de-de/mem/analytics/proactive-remediations>

#### Info zu proaktiven Korrekturen

Proaktive Korrekturen sind Skriptpakete, die häufige Supportprobleme auf dem Gerät eines Benutzers sogar erkennen und beheben können, bevor er bemerkt, dass ein Problem vorliegt. Diese Korrekturen können dazu beitragen, die Anzahl von Supportanrufen zu verringern. Sie können ein eigenes Skriptpaket erstellen oder eines der Skriptpakete bereitstellen, die wir geschrieben und in unserer Umgebung verwendet haben, um die Zahl der Supporttickets zu verringern.

Jedes Skriptpaket besteht aus einem Erkennungsskript, einem Wiederherstellungsskript und Metadaten. Mithilfe von Intune können Sie diese Skriptpakete bereitstellen und Berichte zu ihrer Effektivität anzeigen.

#### Voraussetzungen

- Geräte, die für Endpunktanalysen registriert sind.
  - Weitere Informationen finden Sie unter [Von Configuration Manager verwaltete Geräte registrieren](#) und [Von Intune verwaltete Geräte registrieren](#).

Unabhängig davon, ob Geräte über Intune oder Configuration Manager registriert werden, gelten für die Skripterstellung für proaktive Korrekturen die folgenden Anforderungen:

- Bei den Geräten muss es sich um in Azure AD eingebundene (Hybrid-) Geräte handeln, die eine der folgenden Bedingungen erfüllen:
  - Wird von Intune verwaltet und führt eine Enterprise-, Professional- oder Education-Edition von Windows 10 oder höher aus.
  - Ein [gemeinsam verwaltetes](#) Referenzgerät mit Windows 10, Version 1903 oder höher. Gemeinsam verwaltete Geräte in vorherigen Versionen von Windows 10 benötigen die [Client-Apps-Workload](#), die auf Intune verweist (gilt nur bis Version 1607).

#### Lizenzierung

Für proaktive Korrekturen ist die [Lizenzierung für Endpunktanalyse](#) erforderlich. Außerdem müssen die Benutzer der Geräte über eine der folgenden Lizenzen verfügen:

- Windows 10/11 Enterprise E3 oder E5 (enthalten in Microsoft 365 F3, E3 oder E5)
- Windows 10/11 Education A3 oder A5 (enthalten in Microsoft 365 A3 oder A5)
- Windows 10/11 Virtual Desktop Access (VDA) pro Benutzer

#### Skriptanforderungen

- Sie können bis zu 200 Skriptpakete haben.
- Ein Skriptpaket kann nur ein Erkennungsskript oder ein Erkennungsskript und ein Korrekturskript enthalten.
  - Ein Korrekturskript wird nur ausgeführt, wenn das Erkennungsskript Exitcode exit 1 verwendet, was bedeutet, dass das Problem erkannt wurde.
- Stellen Sie sicher, dass die Skripts in UTF-8 codiert sind.
  - Wenn die Option **Überprüfung der Skriptsignatur erzwingen** auf der Seite [Einstellungen](#) zur Erstellung eines Skriptpakets aktiviert ist, stellen Sie sicher, dass die Skripts in UTF-8 und nicht in UTF-8 BOM codiert sind.
- Die maximal zulässige Ausgabegrößenbeschränkung beträgt 2048 Zeichen.
- Wenn die Option **Überprüfung der Skriptsignatur erzwingen** auf der Seite [Einstellungen](#) zur Erstellung eines Skriptpakets aktiviert ist, wird das Skript mithilfe der PowerShell-Ausführungsrichtlinie des Geräts ausgeführt. Die Standardausführungsrichtlinie für Windows-Clientcomputer ist **Restricted**. Die Standardausführung für Windows Server-Geräte ist **RemoteSigned**. Weitere Informationen finden Sie im Artikel [PowerShell-Ausführungsrichtlinien](#).
  - Skripts, die in proaktive Korrekturen integriert sind, werden signiert, und das Zertifikat wird dem Zertifikatspeicher "**Vertrauenswürdige Herausgeber**" des Geräts hinzugefügt.
  - Wenn Sie signierte Drittanbieterskripts verwenden, stellen Sie sicher, dass sich das Zertifikat im Zertifikatspeicher "**Vertrauenswürdige Herausgeber**" befindet. Wie bei

jedem Zertifikat muss die Zertifizierungsstelle vom Gerät als vertrauenswürdig eingestuft werden.

- Skripts ohne **Überprüfung der Skriptsignatur erzwingen** verwenden die Ausführungsrichtlinie **Umgehen**.
- Fügen Sie keine Geheimnisse in Skripts ein. Erwägen Sie stattdessen die Verwendung von Parametern zum Behandeln von Geheimnissen.
- Fügen Sie keine Neustartbefehle in Erkennungs- oder Wartungsskripts ein.



Proaktive Skripte müssen im UTF-8 Format codiert sein.

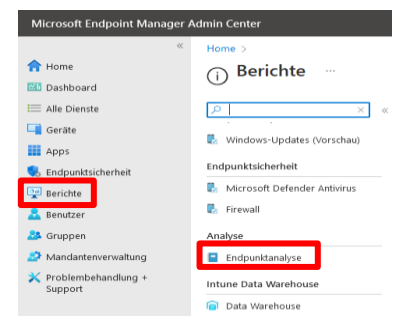
- Veyon Konfiguration Master, Client, Klassenliste (Installation erfolgt über ein intune-win Datei)
- Netzwerkdruckerinstallation mit Treiberinstallation (vobs)

### Jede proaktive Korrektur besteht aus zwei Teilen

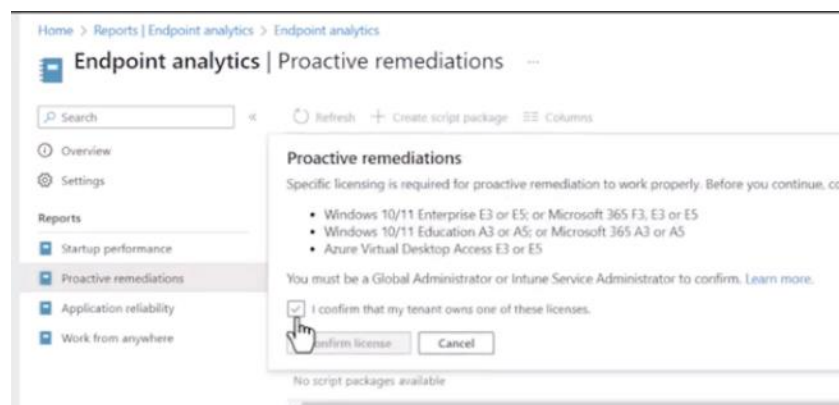
- Erkennungsskript
- Wiederherstellungsskript

## 4.2. Einmalige Grundkonfiguration

- ➔ Endpoint-Manager
- ➔ Berichte
- ➔ Endpunktanalyse



Beim erstmaligen öffnen sind die proaktiven Korrekturen ausgegraut. Auf Proaktive Korrekturen klicken und die Zustimmungserklärung bestätigen.



einmalige Grundeinrichtung abgeschlossen.

### 4.3. Erstellen einer Proaktiven Korrektur

Microsoft Endpoint Manager Admin Center

Home > Berichte | Endpunktanalyse > Endpunktanalyse

## Endpunktanalyse | Proaktive Korrekturen

Suche Aktualisieren + Skriptpaket erstellen Spalten

Erstellen und führen Sie Skriptpakete auf Geräten aus, um die wichtigsten Supportprobleme in Ihr Netzwerk zu finden und zu beheben. Verwenden Sie diese Tabelle, um den Status Ihrer bereitgestellten Skriptpakete anzuzeigen und die Ergebnisse der Erkennung und Korrektur zu überwachen. Ergebnisse werden für betroffene Geräte angezeigt. [Erfahren Sie mehr.](#)

Nach Skriptpaketname suchen

Skriptpaketname ↑↓	Autor	Status	Ohne
Restart stopped Office C2...	Microsoft	Nicht bereitgestellt	0
FastBoot	admin vsvobs	Aktiv	4
hp nochmals	admin vsvobs	Aktiv	3

In den Proaktiven Korrekturen auf „+ Skriptpaket erstellen“ klicken.

Home > Berichte | Endpunktanalyse > Endpunktanalyse | Proaktive Korrekturen >

### Benutzerdefiniertes Skript erstellen

1 Grundeinstellungen 2 Einstellungen 3 Bereichstags 4 Zuweisungen 5 Überprüfen + erstellen

Erstellen Sie ein neues benutzerdefiniertes Skriptpaket aus von Ihnen geschriebenen Skripts für Erkennung und Wartung.

Name \* Druckerinstallation Minolta ✓

Beschreibung Dies ist der Drucker Konica Minolta XYZ

Herausgeber admin vsvobs

Version 1

Zurück Weiter

Wählen eines aussagekräftigen Namens und Beschreibung (z.B. Standort des Druckers etc.)

## Benutzerdefiniertes Skript erstellen ...

✓ Grundeinstellungen 2 **Einstellungen** 3 Bereichstags 4 Zuweisungen 5 Überprüfen + erstellen

Erstellen Sie ein benutzerdefiniertes Skriptpaket aus Skripts, die Sie geschrieben haben. Standardmäßig werden Skripts täglich auf zugewiesenen Geräten ausgeführt.

Datei mit Erkennungsskript \*

Erkennungsskript 

# MS 09.02.2023  
# fuer Endpoint-Verwaltete Geraete - Druckerinstallation  
# Skript gemeinsam mit dem dazu passenden Wiederherstellungsskript verwenden: MS Endpoint Manager -> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...  
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswahlen -> der Geraetegruppe zuordnen

Datei mit Bereinigungsskript

Wiederherstellungsskript 

# MS 09.02.2023  
# fuer Endpoint-Verwaltete Geraete - Druckerinstallation  
# Skript gemeinsam mit dem dazu passenden Erkennungsskript verwenden: MS Endpoint Manager -> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...  
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswahlen -> der Geraetegruppe zuordnen

Dieses Skript mit den Anmeldeinformationen des angemeldeten Benutzers ausführen

Skriptsignaturprüfung erzwingen

Skript in 64-Bit-PowerShell ausführen

Bearbeitetes Erkennungs- und Wiederherstellungsskript hinzufügen. Skript in 64-Bit-Powershell ausführen auf JA stellen. Bereichstags überspringen.

Home > Berichte | Endpunktanalyse > Endpunktanalyse | Proaktive Korrekturen >

### Benutzerdefiniertes Skript erstellen ...

✓ Grundeinstellungen ✓ Einstellungen ✓ Bereichstags 4 **Zuweisungen** 5 Überprüfen + erstellen

Wählen Sie mindestens eine Gruppe aus, um das Skriptpaket zuzuweisen.

Eingeschlossene Gruppen

Zuweisen zu

Ausgewählte Gru...	Zeitplan	Filter	Filtermodus
Keine Gruppen ausgewählt			

Wählen Sie die Gruppen aus, die eingeschlossen werden sollen.

Ausgeschlossene Gruppen

Schließen Sie entweder Gerätegruppen oder Benutzergruppen ein oder aus. Innerhalb von Zuweisungen zum Einschließen oder Ausschließen dürfen Benutzer- und Gerätegruppen nicht kombiniert werden.

Ausgewählte Gruppen

Keine Gruppen ausgewählt

Wählen Sie die Gruppen aus, die ausgeschlossen werden sollen.

Wählen Sie die Gruppen aus, die eingeschlo...

Azure AD-Gruppen

☒ C\_Laptop  
☒ C\_LUL **Ausgewählt**  
☐ C\_surface  
☐ C\_SuS\_Test

Ausgewählte Elemente

☒ C\_LUL\_TEST

Nach dem hinzufügen der Gruppen kann nun der Zeitplan eingestellt werden. Es gibt standardmäßig drei verschiedene Möglichkeiten:

- Einmalig
- Stündlich (kürzestes Intervall: 1 Stunde)
- Täglich (zu einer festgesetzten Uhrzeit)

Home > Berichte | Endpunktanalyse > Endpunktanalyse | Proaktive Korrekturen >

### Benutzerdefiniertes Skript erstellen

Grundeinstellungen Einstellungen Bereichstags **Zuweisungen** Überprüfen + erstellen

Wählen Sie mindestens eine Gruppe aus, um das Skriptpaket zuzuweisen.

Eingeschlossene Gruppen

Zuweisen zu

Ausgewählte Gru...	Zeitplan	Filter	Filtermodus
C_LUL_TEST	<b>Täglich</b>	Keine	Keine

+ Wählen Sie die Gruppen aus, die eingeschlossen werden sollen.

Ausgeschlossene Gruppen

❗ Schließen Sie entweder Gerätegruppen oder Benutzergruppen ein oder aus. Innerhalb von Zuweisungen zum Einschließen oder Ausschließen dürfen Benutzer- und Gerätegruppen nicht kombiniert werden.

Ausgewählte Gruppen

Keine Gruppen ausgewählt

+ Wählen Sie die Gruppen aus, die ausgeschlossen werden sollen.

Zurück **Weiter**

**Einstellungen bear...** ×

Zeitplan  
Hiermit wird ein Zeitplan für die Ausführung dieses Skripts auf Geräten in der Gruppe "C\_LUL\_TEST" erstellt.

Häufigkeit

- Stündlich**
- Einmalig
- Stündlich
- Täglich

Anwenden Zurücksetzen

Home > Berichte | Endpunktanalyse > Endpunktanalyse | Proaktive Korrekturen >

### Benutzerdefiniertes Skript erstellen

Grundeinstellungen Einstellungen Bereichstags Zuweisungen **Überprüfen + erstellen**

Zusammenfassung

Grundeinstellungen

Name	Druckerinstallation Minolta
Beschreibung	Dies ist der Drucker Konica Minolta XYZ.
Herausgeber	admin vsvobs
Version	--

Einstellungen

Erkennungsskript	Ja
Wiederherstellungsskript	Ja
Dieses Skript mit den Anmeldeinformationen des angemeldeten Benutzers ausführen	Nein
Skriptsignaturprüfung erzwingen	Nein
Skript in 64-Bit-PowerShell ausführen	Ja

Bereichstags

Standard

Zuweisungen

Ausgewählte Grupp...	Zeitplan	Filter	Filterm
C_LUL	Stündlich	Keine	Keine

Ausgeschlossene Gruppen

Ausgewählte Gruppen

Keine Ergebnisse.

Zurück **Erstellen**

Nach dem Kontrollieren und Erstellen werden die Proaktiven Korrekturen laut Zeitplan ausgeführt.

#### 4.4. Universeller Druckertreiber/Druckerinstallation

Im Moment werden Proaktive Korrekturen für HP, KonicaMinolta und Ricoh Drucker (ÖBS-Shop) bereitgestellt. Es kann nicht gewährleistet werden, dass jeder in der Schule vorhandener (ältere Modelle) mit dem Druckertreiber funktioniert.

Ausschließlich die [HP Skripte für HP-Drucker](#), [KonicaMinolta Skripte für KonicaMinolta-Drucker](#) und [Ricoh-Skripte für Ricoh-Drucker](#) verwenden (gilt auch für die anderen).

Im Erkennungsskript ist ausschließlich der Druckername zu ändern. Im Wiederherstellungsskript ist derselbe Druckername und der Drucker Port (IP-Adresse des Druckers) zu ändern.

```
$druckername = "Drucker-Buero-HP1320"  
$druckerport = "10.176.232.49"
```



*Im Erkennungsskript und im Wiederherstellungsskript ist der GLEICHE DRUCKERNAME zu verwenden.*



*Das Skript für den HP-Drucker kann nicht für den Minolta Drucker bzw. Ricoh Drucker verwendet werden. Die Installation des universellen Druckertreibers erfolgt nicht auf die gleiche Art und Weise.*

Der Druckertreiber wird von uns bereitgestellt und wird direkt aus dem Downloadbereich vom VOBS und nicht vom Hersteller heruntergeladen. Das hat den Grund, dass sich die Namen der Treiber auf den Herstellerseiten ändern können.

#### 4.5. Veyon Installation und Konfiguration

##### 4.5.1. Grundvoraussetzung – Installation Client/Master:

Veyon muss mit einem Paket installiert werden. Dazu kann eine intunewin Datei erstellt oder vom VOBS heruntergeladen werden (Downloadbereich). Für den Client und den Master wird das gleiche Installationspaket verwendet. Es ändert sich jeweils der Installationsbefehl.

## Client Installation

Veyon als Windows-App (Win32) Paket hinzufügen, Pflichtfelder lt. Bild ausfüllen.

Anwendung bearbeiten ...  
Windows-App (Win32)

App-Informationen Programm Anforderungen Erkennungsregeln Überprüfen und speichern

Zu aktualisierende Datei auswählen \* [veyon-4.7.5.0-win64-setup.intune](#)

Name \*

Beschreibung \*

[Beschreibung bearbeiten](#)

Herausgeber \*

App-Version

Kategorie

Diese App als ausgewählte App im Unternehmensportal anzeigen ☐

Informations-URL

URL zu den Datenschutzbestimmungen

Entwickler

Besitzer

Hinweise

Logo

[Überprüfen und speichern](#) [Abbrechen](#)

Name: Veyon Client SuS  
Herausgeber: IT-Regionalbetreuer Vorarlberg  
App-Version: 4.7.5  
Informations-URL: <https://www.vobs.at>

App hinzufügen ...  
Windows-App (Win32)

App-Informationen Programm Anforderungen Erkennungsregeln Abhängigkeiten

Geben Sie die Befehle zum Installieren und Deinstallieren dieser App an:

Installationsbefehl \*

Deinstallationsbefehl \*

Installationsverhalten

Verhalten beim Gerätestart

Geben Sie Rückgabecodes an, um das Verhalten nach der Installation festzulegen:

Rückgabecode	Codetyp
0	Erfolgreich
1707	Erfolgreich
3010	Warmneustart
1641	Harter Neustart
1618	Wiederholen

[+ Hinzufügen](#)

Installationsbefehl: veyon-win64-setup.exe /S /NoMaster /NoStartMenuFolder  
Deinstallationsbefehl: C:\Program Files\Veyon\uninstall.exe /S

App hinzufügen ...  
Windows-App (Win32)

App-Informationen Programm Anforderungen Erkennungsregeln

Geben Sie die Anforderungen an, die Geräte vor dem Installieren der App erfüllen müssen:

Betriebssystemarchitektur \*

Mindestens erforderliches Betriebssystem \*

Erforderlicher Speicherplatz (MB)

Erforderlicher physischer Speicher (MB)

Mindestens erforderliche Anzahl logischer Prozessoren

Mindestens erforderliche CPU-Geschwindigkeit (MHz)

Konfigurieren Sie zusätzliche Anforderungsregeln.

Typ  Pfad/Kriterium

Keine Anforderungen angegeben.

[+ Hinzufügen](#)

Weiter

App hinzufügen ...  
Windows-App (Win32)

App-Informationen Programm Anforderungen Erkennungsregeln

Konfigurieren Sie App-spezifische Regeln zum Erkennen des Vorhandenseins der App.

Regelformat \*

Typ  Pfad/Kriterium

Keine Regeln angegeben.

[+ Hinzufügen](#)

Erkennungsregel

Erstellen Sie eine Regel, die das Vorhandensein dieser App erkennt.

Regeltyp \*

Pfad \*

Daten oder Ordner \*

Erkennungsmethode \*

Auf 64-Bit-Clienten einer 32-Bit-App zugreifen ☐

[+ Hinzufügen](#)

Erforderlich

Gruppenmodus	Gruppe	Filtermodus	Filter	Erkennungsmethode	Verfügbarkeit	Installationsrichtung
<input checked="" type="checkbox"/>	Erkennen	<input checked="" type="checkbox"/>	C:\Set\Text	keine	keine	keine

[+ Gruppe hinzufügen](#) [+ als Benutzer/Verwalter](#) [+ als Gast hinzufügen](#)

Regelformat: Erkennungsregel manuell konfigurieren  
Regel hinzufügen → Regeltyp: Datei  
Pfad: C:\Program Files\Veyon\  
Datei oder Ordner: veyon-cli.exe  
Erkennungsmethode: Datei oder Ordner ist vorhanden

Betreffende Gruppe zuordnen

## Master-Installation

Analog zur Clientinstallation, jedoch beim Punkt 2 Programm folgenden Installationsbefehl eintragen:

Installationsbefehl: veyon-win64-setup.exe /S

Alle anderen Installationsbefehle wie bei der Clientinstallation angeben.





### 4.5.2. Veyon Konfiguration

Die folgenden Veyon Skripte funktionieren nur, wenn die benötigten Dateien in einem geteilten OneDrive Ordner verortet sind. Das bedeutet, dass die unten angeführten Dateien in einem MS365-Verwaltungs-, MS365-Admin- oder MS-365-IT-Konto gespeichert sein müssen.

- Private\_Key.txt
- Public\_Key.txt
- Klassenliste.txt

Einen eigenen privaten und öffentlichen Key kann mit dem Veyon-Konfigurator erstellt und anschließend in den Onedrive Ordner Veyon kopiert werden.

Eigene Dateien > Veyon






 Name ▾
 klassenliste_vsvobs.txt
 privatekey.txt
 publickey.txt

Die Klassenliste als TXT-File erstellen, damit sie online im OneDrive auch bearbeitbar ist. Wird sie als CSV-Datei erstellt, kann sie online nicht bearbeitet werden.

Anschließend werden die drei Dateien freigegeben. **Jeder mit Link kann anzeigen.**


Die Freigabelinks in eine gesonderte TXT Datei kopieren, damit sie zu einem späteren Punkt verwendbar sind.


Eigene Dateien > Veyon

 Name ▾
  klassenliste_vsvobs.txt
 privatekey.txt
 publickey.txt


**Link senden**

Dokument.docx



 Jeder mit dem Link kann bearbeiten >

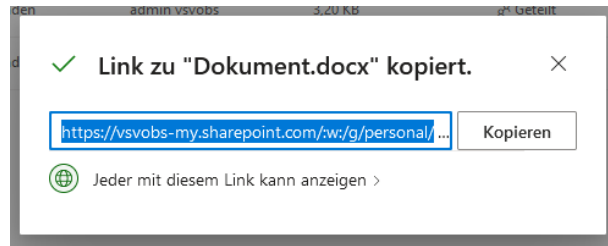
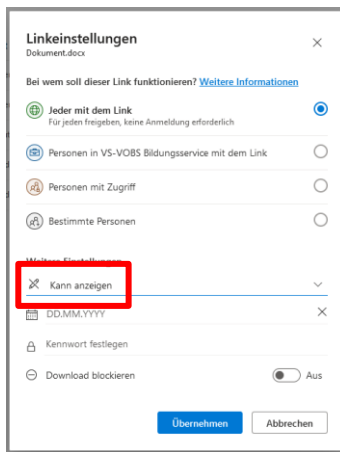
An: Name, Gruppe oder E-Mail 

Nachricht...

 Senden

**Link kopieren**

 Jeder mit dem Link kann bearbeiten >  Kopieren



- Den nun erhaltenen Link für den privatekey in das Wiederherstellungsskript einfügen (siehe Kapitel [4.6.1](#) gelb markierte Stelle).
- Den nun erhaltenen Link für den publickey in Wiederherstellungsskript einfügen (siehe Kapitel [4.6.1](#) und [4.6.2](#) gelb markierte Stelle).
- Den nun erhaltenen Link für die Klassenliste in Wiederherstellungsskript einfügen (siehe Kapitel [4.6.3](#) gelb markierte Stelle).

Anschließend die fertig geänderten Erkennungs- und Wiederherstellungsskripte wie in Punkt [4.3](#) beschrieben hinzufügen.

## 4.6. Skripte

### 4.6.1. Veyon-Key Master (Lehrer) Geräte

#### Erkennungsskript:

```
# MS 02.02.23
# fuer Endpoint-Verwaltete Geraete - Veyon Master Key / Authentifizierung
# Skript gemeinsam mit dem dazu passenden Wiederherstellungsskript verwenden: MS Endpoint Manager -
> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswahlen -> der
Lehrergeraetegruppe zuordnen
#=====

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\Veyon_Master-Erkennungsskript.txt"

Try {
    if (Test-Path C:\ProgramData\Veyon\keys\private\schluessel\key) {
        Write-Host "Privater Schluessel: $True"
        Stop-Transcript
        exit 0
    }
    else {
        Write-Host "Privater Schluessel: $False"
        Stop-Transcript
        exit 1
    }
}
Catch {
    Write-Warning $_
    Stop-Transcript
    exit 1
}
```

## Wiederherstellungsskript:

```
# MS 09.02.23
# fuer Endpoint-Verwaltete Geraete - Veyon Master Key / Authentifizierung
# Skript gemeinsam mit dem dazu passenden Erkennungsskript verwenden: MS Endpoint Manager -> Berichte
-> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der
Lehrergeraetegruppe zuordnen
#=====

#####
# Allgemeiner bearbeitbarer Teil #
#####

#Veyon Keys - Freigabelink hier einfuegen

$publickey = "FREIGABELINK DES PUBLIC KEY HIER EINFUEGEN"

$privatekey = "FREIGABELINK DES PRIVATE KEY HIER EINFUEGEN"

#####
# Installationscript - ab hier nichts aendern #
#####

#Speicherort der Key Dateien
$publicuri = "C:\ProgramData\Veyon\keys\public\schluessel"
$privateuri = "C:\ProgramData\Veyon\keys\private\schluessel"

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\Veyon_Master-Wiederherstellungsskript.txt"

#Key Ordner werden erstellt
New-Item -Path $privateuri -ItemType Directory -Force
New-Item -Path $publicuri -ItemType Directory -Force

#Key Dateien werden heruntergeladen
Invoke-WebRequest -uri $privatekey"&download=1" -OutFile $privateuri"\key"
Invoke-WebRequest -uri $publickey"&download=1" -OutFile $publicuri"\key"

# Set the location to the registry
Set-Location -Path "HKLM:\Software\"

#Neue Unterverzeichnisse erstellen
New-Item "HKLM:\SOFTWARE\Veyon Solutions\Veyon\Authentication" -force -ea SilentlyContinue;

#Neuer Registrierungseintrag mit Wert 1
New-ItemProperty -LiteralPath 'HKLM:\SOFTWARE\Veyon Solutions\Veyon\Authentication' -Name 'Method'
-Value 1 -PropertyType DWord -Force -ea SilentlyContinue;
Write-Host "Veyon Key und Registrierung wurden durchgefuehrt."

#Protokollierung - Ende
Stop-Transcript

exit 0
```

### 4.6.2. Veyon-Key Client (Schüler) Geräte

## Erkennungsskript:

```
# MS 02.02.23
# fuer Endpoint-Verwaltete Geraete - Veyon Client Key / Authentifizierung
# Skript gemeinsam mit dem dazu passenden Wiederherstellungsskript verwenden: MS Endpoint Manager -
> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der
Lehrergeraetegruppe zuordnen
#=====

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\Veyon_Client-Erkennungsskript.txt"

Try {
    if (Test-Path C:\ProgramData\Veyon\keys\public\schluessel\key) {
        Write-Host $True
        Stop-Transcript
        exit 0
    }
}
```

```

    }
    else {
        Write-Host $False
        Stop-Transcript
        exit 1
    }
}
Catch {
    Write-Warning $_
    Stop-Transcript
    exit 1
}
}

```

## Wiederherstellungsskript:

```

# MS 02.02.23
# fuer Endpoint-Verwaltete Geraete - Veyon Client Key / Authentifizierung
# Skript gemeinsam mit dem dazu passenden Erkennungsskript verwenden: MS Endpoint Manager -> Berichte
-> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der
Lehrergeraetegruppe zuordnen
#=====

#####
# Allgemeiner bearbeitbarer Teil #
#####

#Veyon Keys - Freigabelink hier einfuegen

$publickey = "FREIGABELINK DES PUBLIC KEY HIER EINFUEGEN"

#####
# Installationscript - ab hier nichts aendern #
#####

#Speicherort der Key Dateien
$publicuri = "C:\ProgramData\Veyon\keys\public\schluessel"

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\Veyon_Client-Wiederherstellungsskript.txt"

#Key Ordner werden erstellt
New-Item -Path $publicuri -ItemType Directory

#Key Datei wird heruntergeladen
Invoke-WebRequest -uri $publickey"&download=1" -OutFile $publicuri"\key"

#Registrierungseinstellungen
#Set the location to the registry
Set-Location -Path "HKLM:\Software\"

#Neue Unterverzeichnisse erstellen
New-Item "HKLM:\SOFTWARE\Veyon Solutions\Veyon\Authentication" -force -ea SilentlyContinue;

#Neuer Registrierungseintrag mit Wert 1
New-ItemProperty -LiteralPath 'HKLM:\SOFTWARE\Veyon Solutions\Veyon\Authentication' -Name 'Method'
-Value 1 -PropertyType DWord -Force -ea SilentlyContinue;

#Benachrichtigung Neue Unterverzeichnisse erstellen
New-Item "HKLM:\SOFTWARE\Veyon Solutions\Veyon\Service" -force -ea SilentlyContinue;

#Neuer Registrierungseintrag mit Wert true - Benachrichtigung
New-ItemProperty -LiteralPath 'HKLM:\SOFTWARE\Veyon Solutions\Veyon\Service' -Name
'FailedAuthenticationNotifications' -Value true -PropertyType STRING -Force -ea SilentlyContinue;

#Neuer Registrierungseintrag mit Wert true - Benachrichtigung
New-ItemProperty -LiteralPath 'HKLM:\SOFTWARE\Veyon Solutions\Veyon\Service' -Name
'RemoteConnectionNotifications' -Value true -PropertyType STRING -Force -ea SilentlyContinue;
Write-Host "Veyon Key und Registrierung wurden durchgefuehrt."

#Protokollierung - Ende
Stop-Transcript

exit 0

```

### 4.6.3. Veyon-Klassenliste Aktualisierung

#### Erkennungsskript:

```
# MS 09.02.23
# fuer Endpoint-Verwaltete Geraete - Veyon Master Klassenlisten Aktualisierung
# Skript gemeinsam mit dem dazu passenden Wiederherstellungsskript verwenden: MS Endpoint Manager -
> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der
Lehrergeraetegruppe zuordnen
#=====

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\Veyon_Klassenliste-Erkennungsskript.txt"

$testpfad = "C:\Program Files\Veyon\veyon-master.exe"

Try {
    if (-not (Test-Path $testpfad))
    {
        Write-Host "Veyon Master ist nicht installiert."
        stop-transcript
        exit 0
    }
    else
    {
        Write-Host "Veyon Master ist installiert und Klassenliste wird aktualisiert."
        stop-transcript
        exit 1
    }
}
Catch
{
    Write-Warning "Veyon Master ist installiert und Klassenliste wird aktualisiert."
    stop-transcript
    exit 1
}
```

#### Wiederherstellungsskript:

```
# MS 09.02.23
# fuer Endpoint-Verwaltete Geraete - Veyon Master Klassenlisten Aktualisierung
# Skript gemeinsam mit dem dazu passenden Erkennungsskript verwenden: MS Endpoint Manager -> Berichte
-> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der
Lehrergeraetegruppe zuordnen
#=====

#####
# Allgemeiner bearbeitbarer Teil #
#####

#Veyon Klassenliste - Freigabelink hier einfuegen

$klassenliste = "FREIGABELINK DER KLASSENLISTE HIER EINFUEGEN"

#####
# Installationsskript - ab hier nichts aendern #
#####

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\Veyon_Klassenliste-
Wiederherstellungsskript.txt"

#Zielverzeichnis fuer alle moeglichen Installationsdateien - bitte nicht aendern!!!
$verzeichnis = "C:\tmp"

If (Test-Path -Path $verzeichnis)
{
    Write-Host "Verzeichnis vorhanden."
}
else
{
    New-Item -path $verzeichnis -ItemType Directory -ErrorAction SilentlyContinue
```

```

    }

#Veyon Zieldatei
    $downloadlink = $klassenliste+"&download=1"
    $veyoncsv = $verzeichnis+"\klassenliste.csv"

    Start-BitsTransfer -Source $downloadlink -Destination $veyoncsv -TransferType Download
    Write-Host "Klassenliste heruntergeladen."

#Vorhandene Schueler-PCs loeschen
    $cmd = "C:\Program Files\Veyon\veyon-cli.exe"
    $arguments1 = "networkobjects","clear"
    & $cmd $arguments1
    sleep -Seconds 1

#Ueber Liste werden nun alle Schueler-PCs importiert
    $arguments2 =
"networkobjects","import","$verzeichnis\klassenliste.csv","format","%host%;%name%;%mac%;%location%
"
    & $cmd $arguments2
    Write-Host "Schueler-PCs geloescht und neu hinzugefügt."

#Heruntergeladene Klassenliste löschen
    remove-item $verzeichnis"\klassenliste.csv"

#Protokollierung - Ende
Stop-Transcript

exit 0

```

#### 4.6.4. HP-Drucker Installation mit dem HP Universal Drucker Treiber

##### Erkennungsskript:

```
# MS 31.01.2023
# fuer Endpoint-Verwaltete Geraete - Druckerinstallation
# Skript gemeinsam mit dem dazu passenden Wiederherstellungsskript verwenden: MS Endpoint Manager -
> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der Geraetegruppe
zuordnen
#=====

#####
# Allgemeiner bearbeitbarer Teil #
#####

$druckername = "HP1320-EG"

#####
# Abfrage Teil - ab hier nichts aendern #
#####

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\$druckername-Erkennungsskript.txt"

$ErrorActionPreference = "silentlycontinue"
$error.clear()

Try {
    if (get-printer -Name $druckername)
    {
        Write-Host "Der Drucker $druckername ist vorhanden"
        Set-PrintConfiguration -PrinterName $druckername -DuplexingMode OneSided -Color $false
        Write-Host "Duplex-Modus - Einseitig und SW-Ausdruck aktiviert."
        stop-transcript
        exit 0
    }
    else
    {
        Write-Host "Der Drucker $druckername ist nicht vorhanden und wird installiert."
        stop-transcript
        exit 1
    }
}
Catch
{
    Write-Warning "Der Drucker $druckername ist nicht vorhanden und wird installiert."
    stop-transcript
    exit 1
}
```

##### Wiederherstellungsskript:

```
# MS 09.02.2023
# fuer Endpoint-Verwaltete Geraete - Druckerinstallation
# Skript gemeinsam mit dem dazu passenden Erkennungsskript verwenden: MS Endpoint Manager -> Berichte
-> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der Geraetegruppe
zuordnen
#=====

#####
# Allgemeiner bearbeitbarer Teil #
#####

#Drucker definieren:
$druckername = "HP1320-EG"
$druckerport = "192.168.100.240"

#####
# Universeller Drucker-Treiber installieren - ab hier nichts aendern #
#####

#Zielverzeichnis fuer alle moeglichen Installationsdateien - bitte nicht aendern!!!
$verzeichnis = "C:\tmp"
```

```

$verzeichnis2 = "hp_upd"
$ausgabedatei = "hp_upd.zip"

#Download-Link des Universeller Drucker Treibers
$URI = "https://download.vobs.at/wp-content/uploads/UPD/"

#Drucker INF-Quelle im TMP - Ordner
$INFquelle = "$verzeichnis\$verzeichnis2\*.inf"

#Standardtreiber fuer Konica-Minolta Drucker
$druckertreiber = "HP Universal Printing PCL 6 (v7.0.1)"

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\$druckername-Wiederherstellungsskript.txt"

If (Test-Path -Path $verzeichnis)
{
    Write-Host "Verzeichnis vorhanden."
}
else
{
    New-Item -path $verzeichnis -ItemType Directory -ErrorAction SilentlyContinue
    New-Item -path $verzeichnis\$verzeichnis2 -ItemType Directory -ErrorAction SilentlyContinue
    Write-Host "Verzeichnis $verzeichnis und $verzeichnis2 wurden erstellt"
}

if (Test-Path -path $verzeichnis\$ausgabedatei)
{
    Expand-Archive -path $verzeichnis\$ausgabedatei -DestinationPath $verzeichnis\$verzeichnis2 -
Force
}
else
{
    Start-BitsTransfer -Source $uri$ausgabedatei -Destination $verzeichnis -TransferType Download
    Expand-Archive -path $verzeichnis\$ausgabedatei -DestinationPath $verzeichnis\$verzeichnis2 -
Force
}

$ErrorActionPreference = "silentlycontinue"
$error.clear()

if (get-printer -Name $druckername)
{
    Write-Host "$druckername bereits installiert."
}
else
{
    Set-Location $verzeichnis\$verzeichnis2
    .\install.exe /q /n$druckername /sm$druckerport
    Write-Host "$druckername wurde mit dem Druckerport $druckerport installiert."
}

#Protokollierung - Ende
stop-transcript

exit 0

```

#### 4.6.5. KonicaMinolta-Drucker Installation mit dem Universal Drucker Treiber

##### Erkennungsskript:

```
# MS 09.02.2023
# fuer Endpoint-Verwaltete Geraete - Druckerinstallation
# Skript gemeinsam mit dem dazu passenden Wiederherstellungsskript verwenden: MS Endpoint Manager -
> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der Geraetegruppe
zuordnen
#=====

#####
# Allgemeiner bearbeitbarer Teil #
#####

$druckername = "Minolta-C360i-OG"

#####
# Abfrage Teil - ab hier nichts aendern #
#####

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\$druckername-Erkennungsskript.txt"

$ErrorActionPreference = "silentlycontinue"
$error.clear()

Try {
    if (get-printer -Name $druckername)
    {
        Write-Host "Der Drucker $druckername ist vorhanden"
        Set-PrintConfiguration -PrinterName $druckername -DuplexingMode OneSided -Color $false
        Write-Host "Duplex-Modus - Einseitig und SW-Ausdruck aktiviert."
        stop-transcript
        exit 0
    }
    else
    {
        Write-Host "Der Drucker $druckername ist nicht vorhanden und wird installiert."
        stop-transcript
        exit 1
    }
}
Catch
{
    Write-Warning "Der Drucker $druckername ist nicht vorhanden und wird installiert."
    stop-transcript
    exit 1
}
```

##### Wiederherstellungsskript:

```
# MS 09.02.2023
# fuer Endpoint-Verwaltete Geraete - Druckerinstallation
# Skript gemeinsam mit dem dazu passenden Erkennungsskript verwenden: MS Endpoint Manager -> Berichte
-> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der Geraetegruppe
zuordnen
#=====

#####
# Allgemeiner bearbeitbarer Teil #
#####

#Drucker definieren:
$druckername = "Minolta-C360i-OG"
$druckerport = "192.168.100.241"

#####
# Universeller Drucker-Treiber installieren - ab hier nichts aendern #
#####

#Zielverzeichnis fuer alle moeglichen Installationsdateien - bitte nicht aendern!!!
$verzeichnis = "C:\tmp"
```

```

$verzeichnis2 = "km_upd"
$ausgabedatei = "minolta_upd.zip"

#Download-Link des Universeller Drucker Treibers
$URI = "https://download.vobs.at/wp-content/uploads/UPD/"

#Drucker INF-Quelle im TMP-Ordner
$Infquelle = "$verzeichnis\$verzeichnis2\*.inf"

#Drucker Ordner im Filerepository
$filterRepository = "kobxxk__01*"

#Druckertreibername im Filerepository
$treiberINF = "KOBxxK 01.inf"

#Standardtreiber fuer Konica-Minolta Drucker
$drukertreiber = "KONICA MINOLTA Universal V4 PCL"

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\$druckername-Wiederherstellung.txt"

If (Test-Path -Path $verzeichnis)
{
    Write-Host "Verzeichnis vorhanden."
}
else
{
    New-Item -path $verzeichnis -ItemType Directory -ErrorAction SilentlyContinue
    New-Item -path $verzeichnis\$verzeichnis2 -ItemType Directory -ErrorAction SilentlyContinue
    Write-Host "Verzeichnis $verzeichnis und $verzeichnis2 wurden erstellt"
}

if (Test-Path $verzeichnis\$ausgabedatei)
{
    Write-Host "Treiber wurde bereits heruntergeladen und entpackt."
    Expand-Archive -path $verzeichnis\$ausgabedatei -DestinationPath $verzeichnis\$verzeichnis2 -
Force
}
else
{
    Write-Host "Treiber wird heruntergeladen und entpackt."
    Start-BitsTransfer -Source $uri$ausgabedatei -Destination $verzeichnis -TransferType Download
    Expand-Archive -path $verzeichnis\$ausgabedatei -DestinationPath $verzeichnis\$verzeichnis2 -
Force
}

#Filerepository Ordner ueberpruefen
$ordner = Get-ChildItem -path "C:\Windows\System32\DriverStore\FileRepository" -Filter
$filterRepository -directory -Recurse | Sort-Object creationtime -Descending | Select-Object -First
1
$treiberordner = $ordner.FullName

if ($treiberordner)
{
    Write-Host "Universeller Druckertreiber $treiberINF bereits installiert."
}
else
{
    pnputil.exe /add-driver $Infquelle /install
    write-host "pnputil.exe /a $INFquelle"
    $ordner = Get-ChildItem -path "C:\Windows\System32\DriverStore\FileRepository" -Filter
$filterRepository -directory -Recurse | Sort-Object creationtime -Descending | Select-Object -First
1
$treiberordner = $ordner.FullName
$infpath = $treiberordner+"\$treiberinf"
Add-PrinterDriver -Name $drukertreiber -InfPath $infpath
Write-Host "Universeller Druckertreiber $treiberINF wurde installiert."
}

#Druckerport hinzufuegen
$port = Get-WmiObject -Class Win32_TCIPPPrinterPort -Filter "Name='$drukertreiber'"

If ($port) {
    Write-Host "Port Name: $($port.Name)"
    Write-Host "Druckerport bereits hinzugefuegt."
} else {
    Write-Host "Der Druckerport $drukertreiber wird hinzugefuegt."
    Add-PrinterPort -Name $drukertreiber -PrinterHostAddress $drukertreiber
}

```

```
#Drucker hinzufuegen mit dem Universellen Drucker Treiber

$printer = Get-WmiObject -Class Win32_Printer -Filter "Name='$druckername'"

if ($printer) {
    Write-Host "Printer Name: $($printer.Name)"
    Write-Host "Driver Name: $($printer.DriverName)"
    Write-Host "Port Name: $($printer.PortName)"
    Write-Host "Printer Status: $($printer.Status)"
} else {
    Write-Host "Der Drucker $druckername wurde nicht gefunden und wird installiert."
    Add-Printer -DriverName $druckertreiber -Name $druckername -PortName $druckerport -
ErrorAction Continue
    write-host "Add-Printer -DriverName $druckertreiber -Name $druckername -PortName
$druckerport"
    Write-Host "Drucker $druckername wurde erfolgreich hinzugefuegt."
}

#Protokollierung - Ende
Stop-Transcript

exit 0
```

#### 4.6.6. Ricoh Universal Drucker Treiber

##### Erkennungsskript:

```
# MS 02.02.2023
# fuer Endpoint-Verwaltete Geraete - Druckerinstallation
# Skript gemeinsam mit dem dazu passenden Wiederherstellungsskript verwenden: MS Endpoint Manager -
> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der Geraetegruppe
zuordnen
#=====

#####
# Allgemeiner bearbeitbarer Teil #
#####

$druckername = "Ricoth-Drucker"

#####
# Abfrage Teil - ab hier nichts aendern #
#####

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\$druckername-Erkennungsskript.txt"

$ErrorActionPreference = "silentlycontinue"
$error.clear()

Try {
    if (get-printer -Name $druckername)
    {
        Write-Host "Der Drucker $druckername ist vorhanden"
        Set-PrintConfiguration -PrinterName $druckername -DuplexingMode OneSided -Color $false
        Write-Host "Duplex-Modus - Einseitig und SW-Ausdruck aktiviert."
        stop-transcript
        exit 0
    }
    else
    {
        Write-Host "Der Drucker $druckername ist nicht vorhanden und wird installiert."
        stop-transcript
        exit 1
    }
}
Catch
{
    Write-Warning "Der Drucker $druckername ist nicht vorhanden und wird installiert."
    stop-transcript
    exit 1
}
```

## Wiederherstellungsskript:

```
# MS 09.02.2023
# fuer Endpoint-Verwaltete Geraete - Druckerinstallation
# Skript gemeinsam mit dem dazu passenden Wiederherstellungsskript verwenden: MS Endpoint Manager -
> Berichte -> Endpunktanalyse -> Proaktive Korrekturen -> Skriptpaket erstellen ...
# Skript in 64-bit-Powershell-Host ausfuehren aktivieren -> Zeitplan auswaehlen -> der Geraetegruppe
zuordnen
#=====

#####
# Allgemeiner bearbeitbarer Teil #
#####

#Drucker definieren:
$druckername = "Test-Drucker"
$druckerport = "192.168.100.242"

#####
# Universeller Drucker-Treiber installieren - ab hier nichts aendern #
#####

#Zielverzeichnis fuer alle moeglichen Installationsdateien - bitte nicht aendern!!!
$verzeichnis = "C:\tmp"
$verzeichnis2 = "ricoh_upd"
$ausgabedatei = "ricoh_upd.zip"

#Download-Link des Universeller Drucker Treibers
$URI = "https://download.vobs.at/wp-content/uploads/UPD/"

#Drucker INF-Quelle im TMP-Ordner
$Infquelle = "$verzeichnis\$verzeichnis2\*.inf"

#Drucker Ordner im Filerepository
$filterRepository = "oemsetup.inf*"

#Druckertreibername im Filerepository
$treiberINF = "oemsetup.inf"

#Standardtreiber fuer Ricoh Drucker
$druckertreiber = "PCL6 Driver for Universal Print"

#Protokollierung - Start
start-transcript -path "c:\Windows\Logs\Korrekturen\$druckername-Wiederherstellung.txt"

If (Test-Path -Path $verzeichnis)
{
    Write-Host "Verzeichnis vorhanden."
}
else
{
    New-Item -path $verzeichnis -ItemType Directory -ErrorAction SilentlyContinue
    New-Item -path $verzeichnis\$verzeichnis2 -ItemType Directory -ErrorAction SilentlyContinue
    Write-Host "Verzeichnis $verzeichnis und $verzeichnis2 wurden erstellt"
}

if (Test-Path $verzeichnis\$ausgabedatei)
{
    Write-Host "Treiber wurde bereits heruntergeladen und entpackt."
    Expand-Archive -path $verzeichnis\$ausgabedatei -DestinationPath $verzeichnis\$verzeichnis2 -
Force
}
else
{
    Write-Host "Treiber wird heruntergeladen und entpackt."
    Start-BitsTransfer -Source $uri$ausgabedatei -Destination $verzeichnis -TransferType Download
    Expand-Archive -path $verzeichnis\$ausgabedatei -DestinationPath $verzeichnis\$verzeichnis2 -
Force
}

#Filerepository Ordner ueberpruefen
$ordner = Get-ChildItem -path "C:\Windows\System32\DriverStore\FileRepository" -Filter
$filterRepository -directory -Recurse | Sort-Object creationtime -Descending | Select-Object -First
1
$treiberordner = $ordner.FullName
```

```

    if ($streiberordner)
    {
        Write-Host "Universeller Druckertreiber $streiberINF bereits installiert."
    }
    else
    {
        pnputil.exe /add-driver $Infquelle /install
        write-host "pnputil.exe /a $INFquelle"
        $ordner = Get-ChildItem -path "C:\Windows\System32\DriverStore\FileRepository" -Filter $filterRepository -directory -Recurse | Sort-Object creationtime -Descending | Select-Object -First 1
        $streiberordner = $ordner.FullName
        $infpath = $streiberordner+"\$streiberinf
        Add-PrinterDriver -Name $druckertreiber -InfPath $infpath
        Write-Host "Universeller Druckertreiber $streiberINF wurde installiert."
    }

#Druckerport hinzufuegen
$port = Get-WmiObject -Class Win32_TCPIPPrinterPort -Filter "Name='$druckerport'"

If ($port) {
    Write-Host "Port Name: $($port.Name)"
    Write-Host "Druckerport bereits hinzugefuegt."
} else {
    Write-Host "Der Druckerport $druckerport wird hinzugefuegt."
    Add-PrinterPort -Name $druckerport -PrinterHostAddress $druckerport
}

#Drucker hinzufuegen mit dem Universellen Drucker Treiber
$printer = Get-WmiObject -Class Win32_Printer -Filter "Name='$druckername'"

    if ($printer) {
        Write-Host "Printer Name: $($printer.Name)"
        Write-Host "Driver Name: $($printer.DriverName)"
        Write-Host "Port Name: $($printer.PortName)"
        Write-Host "Printer Status: $($printer.Status)"
    } else {
        Write-Host "Der Drucker $druckername wurde nicht gefunden und wird installiert."
        Add-Printer -DriverName $druckertreiber -Name $druckername -PortName $druckerport -
ErrorAction Continue
        write-host "Add-Printer -DriverName $druckertreiber -Name $druckername -PortName $druckerport"
        Write-Host "Drucker $druckername wurde erfolgreich hinzugefuegt."
    }

#Protokollierung - Ende
Stop-Transcript

exit 0

```

## 5. McAfee Remover

### 5.1. Allgemeines

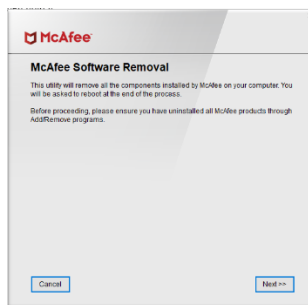
Die in der Geräteinitiative ausgeschrieben Lenovo Laptops haben bestimmte Programme vorinstalliert. Die kostenlose Testversion von McAfee stört hingegen das interne Windows Sicherheitstool und muss daher deinstalliert werden. Dies kann automatisiert mit folgender Anleitung (gilt momentan nur für Lenovo Thinkbook 20VD).

Die fertige IntuneWin Datei ist im Download enthalten. Die nächsten Schritte zeigen das Erstellen dieser. Verteilung des Paketes siehe [Bereitstellung des Paketes](#).

### 5.2. Automatisches Entfernen vom vorinstalliertem McAfee Live System

1. [McAfee Consumer Product Removal Tool herunterladen](https://download.mcafee.com/molbin/iss-loc/SupportTools/MCPR/MCPR.exe)  
(<https://download.mcafee.com/molbin/iss-loc/SupportTools/MCPR/MCPR.exe>)
2. Starten des heruntergeladenen **MCPR.exe** und **geöffnet lassen und nicht "next"...**

3. Navigieren während dieses **Dialogfelds** zu den entpackten Quelldateien in: %localappdata%\temp



4. Kopieren des Ordners **MCPR** an einen geeigneten Ort für die Paketierung, z. B. **c:\temp\McAfeeRemover**
5. **Schließen** des noch offenen **McAfee Software Removal Tool --> Cancel**
6. Erstellen eines Powershell-Skripts im obigen Ordner,  
z. B. c:\temp\McAfeeRemover\McAfeeRemover.ps1

### Skript-Inhalt: (copy/paste)



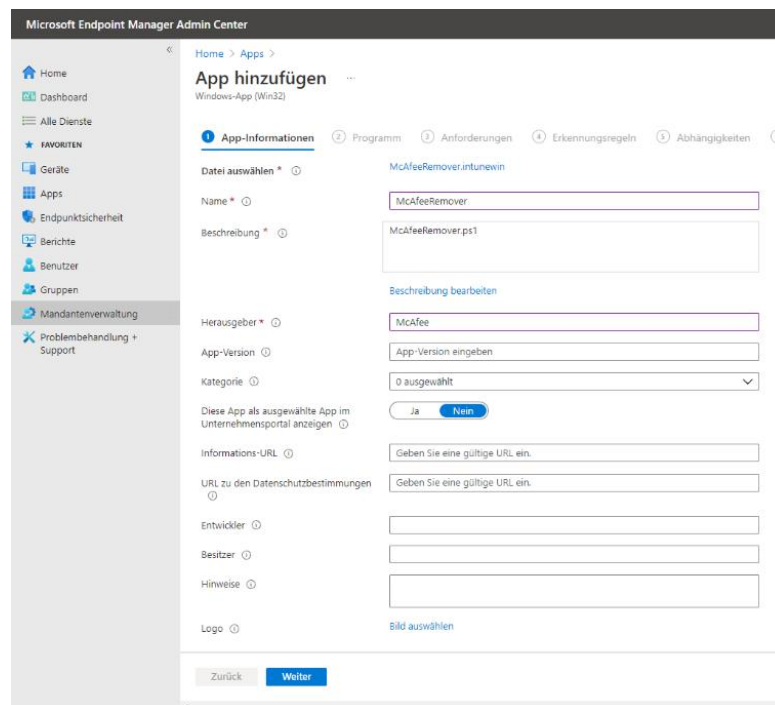
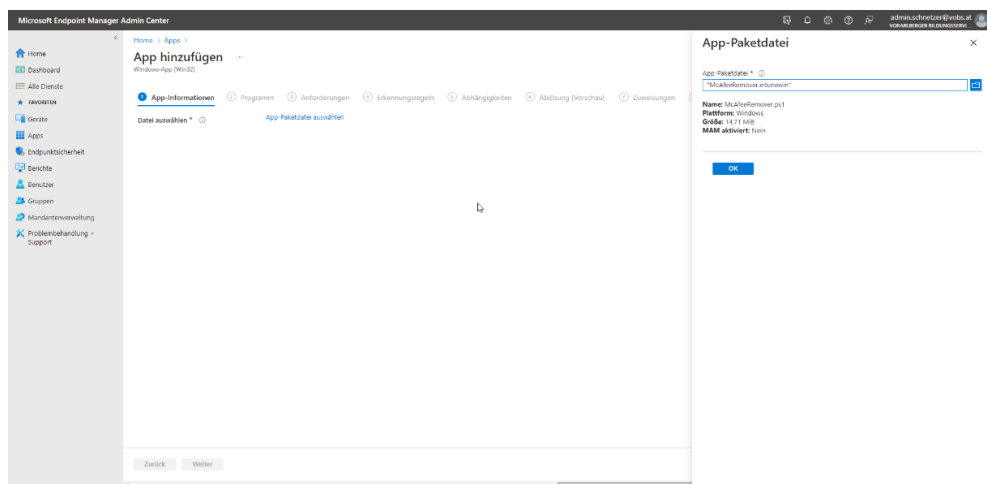
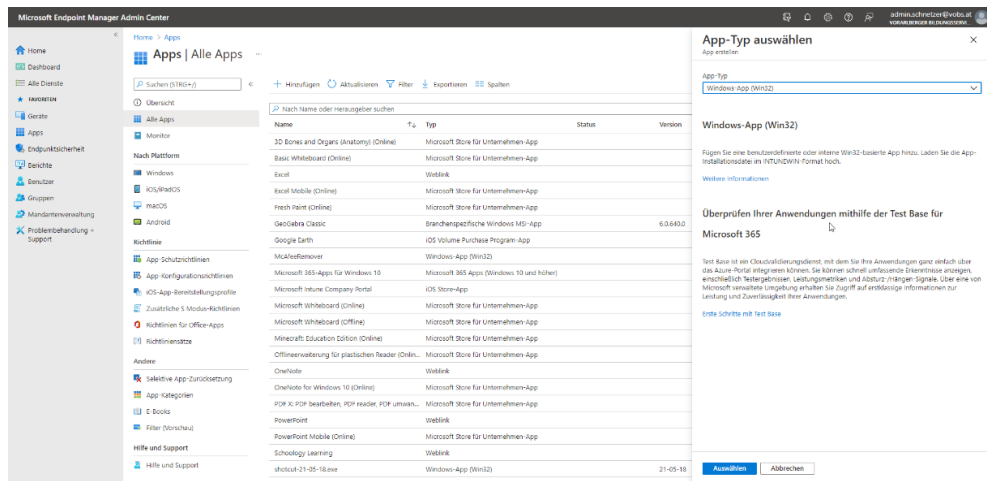
```
# Run the cleanup tool
$program= ".\McCleanup.exe"
$programArg=
StopServices,MFSY,PEF,MXD,CSP,Sustainability,MOCP,MFP,APPSTATS,Auth,EMproxy,FWdiver,HW,MAS,MAT,MBK
,MCPR,McProxy,McSvcHost,VUL,MHN,MNA,MOBK,MPFP,MPFPCU,MPS,SHRED,MPSCU,MQC,MQCCU,MSAD,MSHR,MSK,MSKCU
,MWL,NMC,RedirSvc,VS,REMEDICATION,MSC,YAP,TRUEKEY,LAM,PCB,Symlink,SafeConnect,MGS,WMIRemover,RESIDU
E -v -s"
$process = Start-Process $program -ArgumentList $ProgramArg -passthru -Wait -NoNewWindow

# Remove the Store apps from McAfee
$RemoveApp = 'Mcafee'
Get-AppxPackage -AllUsers | Where-Object {$_.Name -Match $RemoveApp} | Remove-AppxPackage
Get-AppxPackage | Where-Object {$_.Name -Match $RemoveApp} | Remove-AppxPackage
Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Match $RemoveApp} | Remove-
AppxProvisionedPackage -Online
```

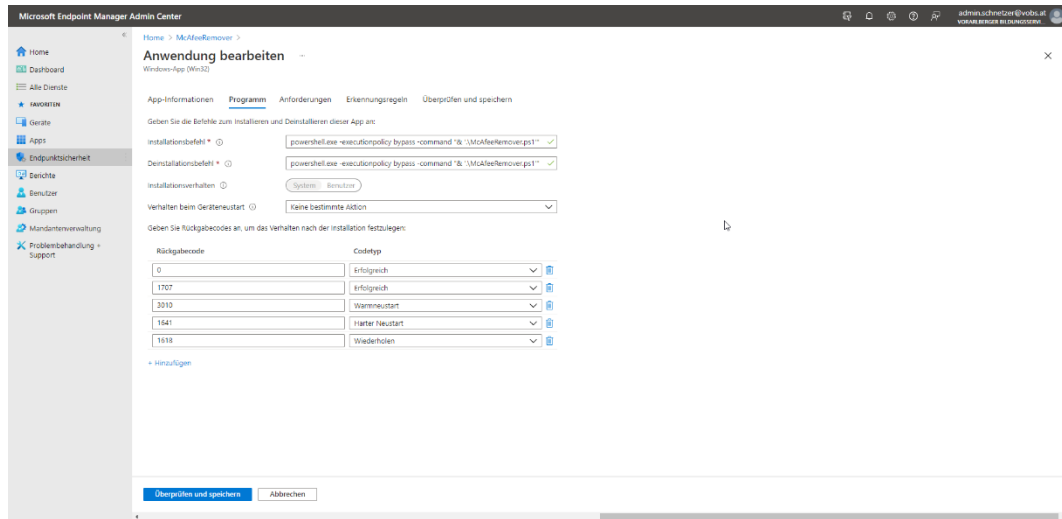
### Erstellen des IntuneWin-Paketes

```
.\IntuneWinAppUtil.exe -c "c:\temp\McAfeeRemover" -s "McAfeeRemover.ps1" -o "c:\temp" -q
```

### 5.3. Bereitstellen des Paketes:



Beim nächsten Schritt „**Programm**“ folgende Einträge machen.



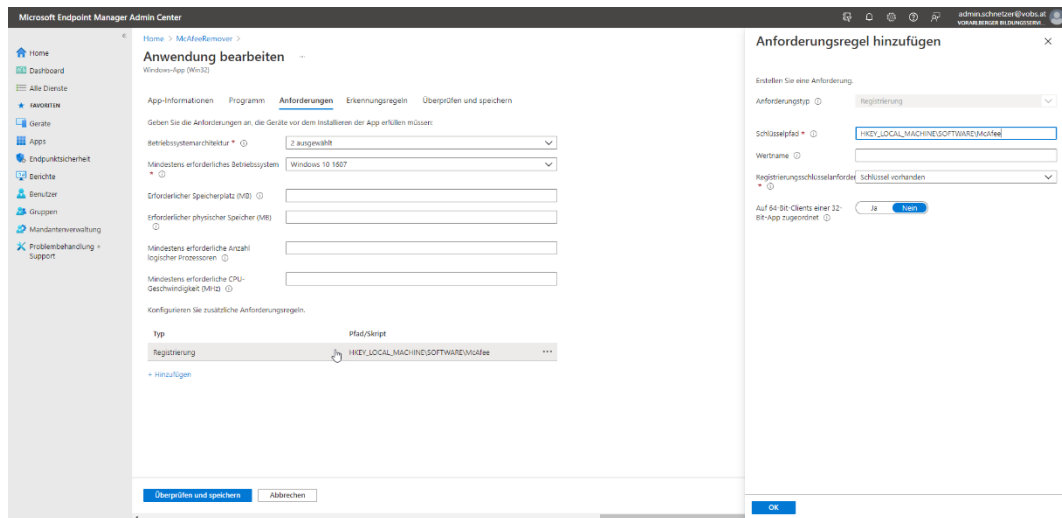
### Installationsbefehl:

```
powershell.exe -executionpolicy bypass -command "& '.\McAfeeRemover.ps1'"
```

### Deinstallationsbefehl:

```
powershell.exe -executionpolicy bypass -command "& '.\McAfeeRemover.ps1'"
```

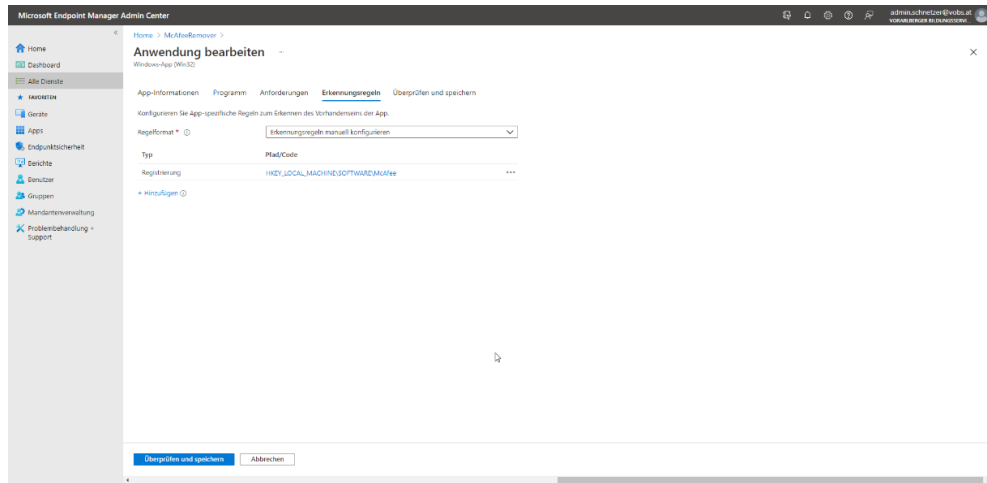
### Schritt 3: „Anforderungen“



Schlüsselpfad: HKEY\_LOCAL\_MACHINE\SOFTWARE\McAfee

Registrierungsschlüsselanforderungen: Schlüssel vorhanden

### Schritt 4: „Erkennungsregeln“



Schlüsselpfad: HKEY\_LOCAL\_MACHINE\SOFTWARE\McAfee

Registrierungsschüsselanforderungen: Schlüssel **nicht** vorhanden

Letzter Schritt: Gruppe hinzufügen und **warten bis das Paket hochgeladen ist**.