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

Inhalt

1. Windows Updates einrichten

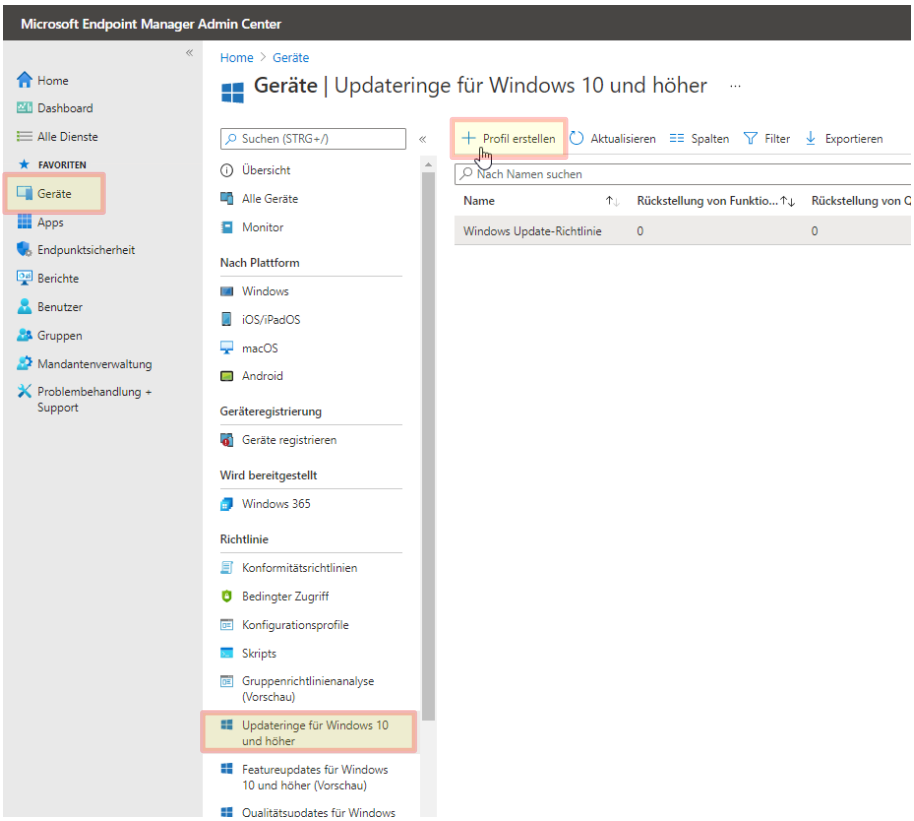
1.1. Allgemeines

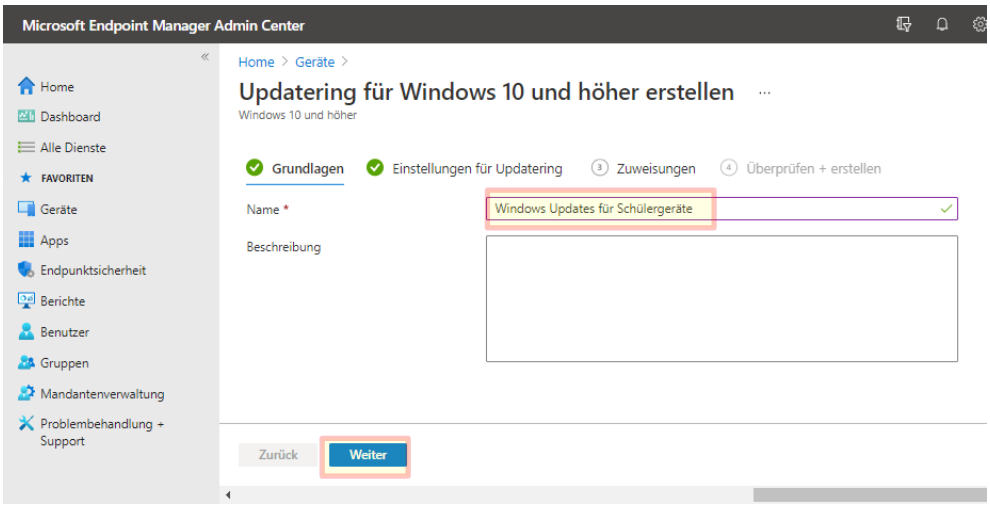
Für einen sicheren Betrieb sind aktuelle Systeme erforderlich. Diese können über vorgegebene Richtlinien konfiguriert werde.

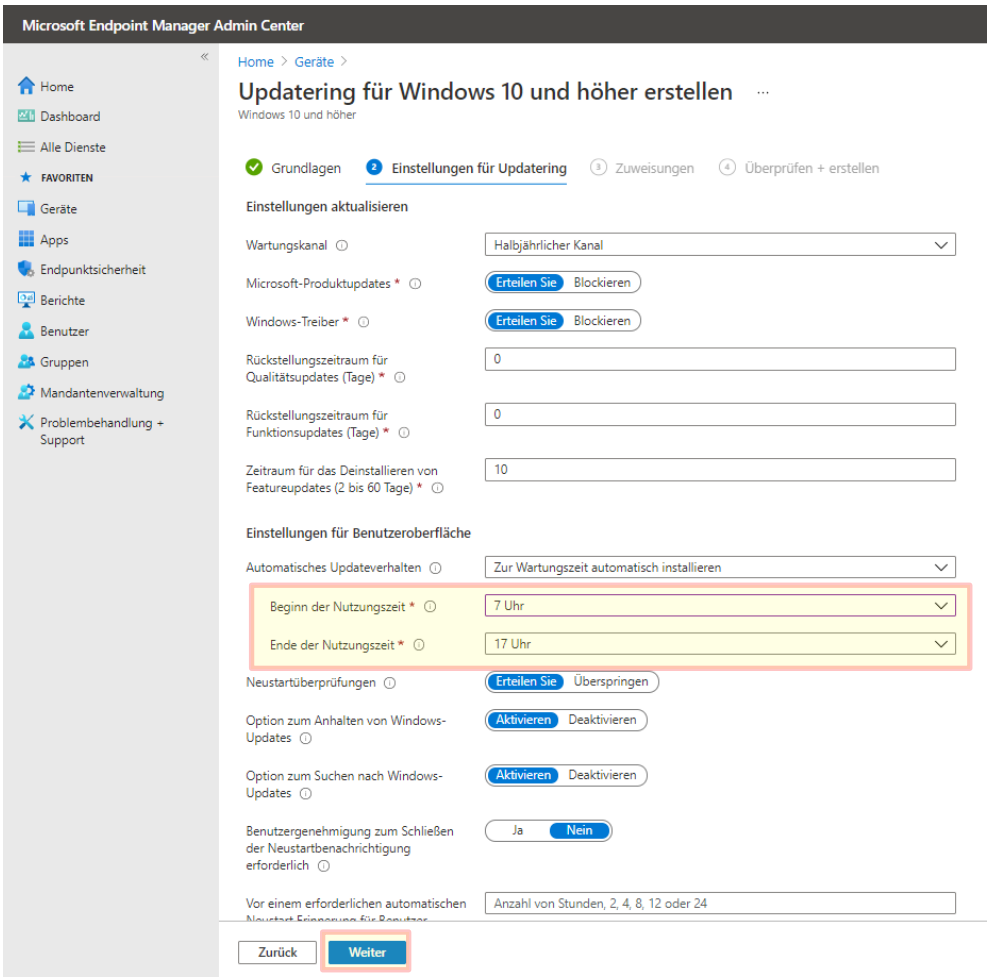
1.2. Konfiguration

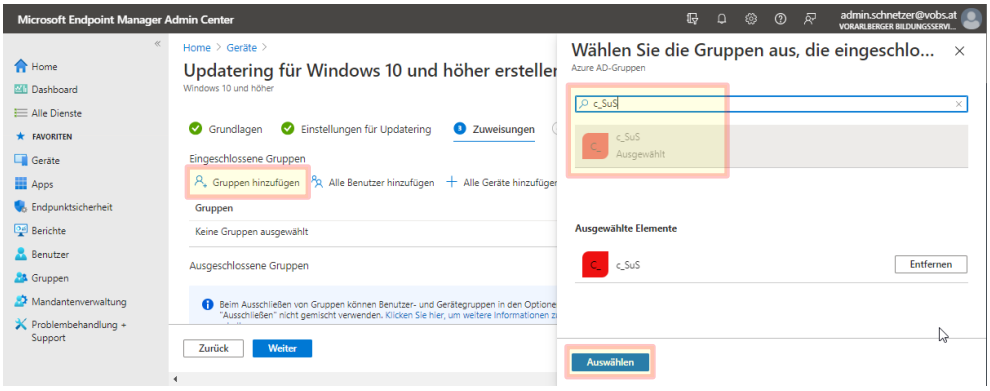
- Öffnen des Endpoint Managers (https://endpoint.microsoft.com) → Geräte → Updateringe für Windows 10 und höher.
- Profil erstellen mit dem Namen: Windows Updates für Schülergeräte
- Standardmäßig kann alles so eingestellt bleiben – evtl. die Nutzungszeit des Gerätes, wenn nötig ändern.
- Der Gruppe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

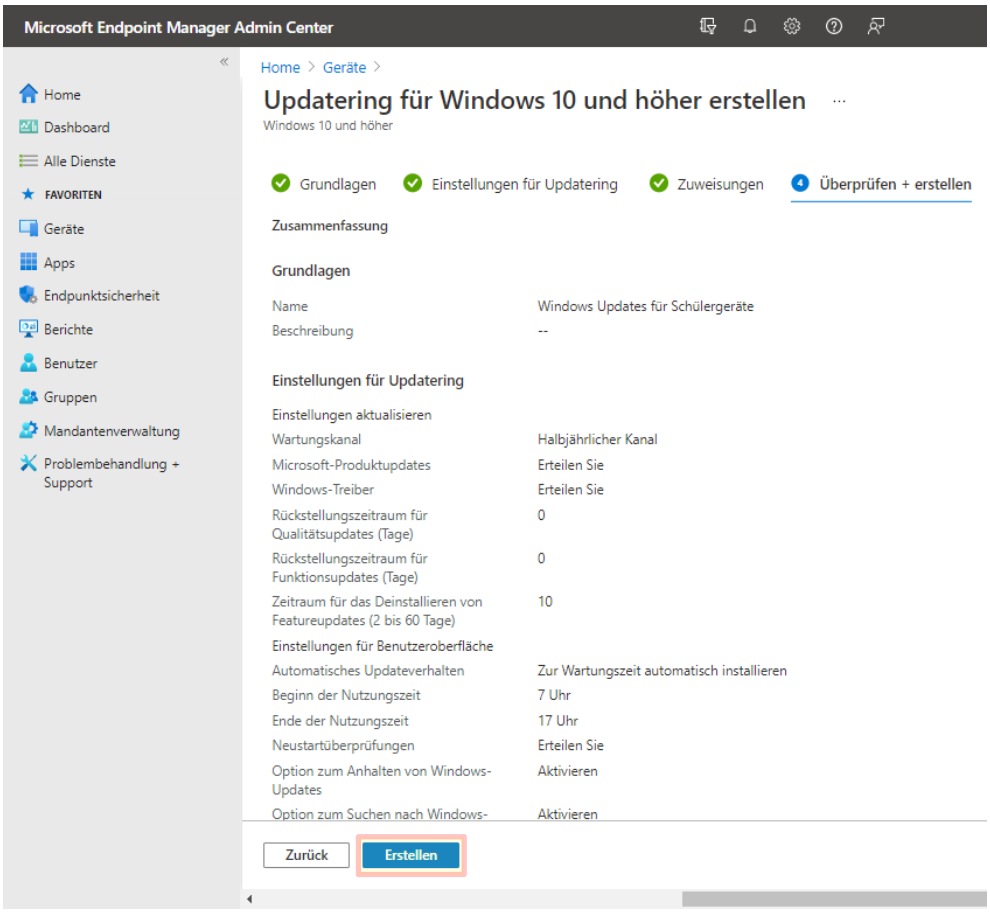
Analog dazu kann auch ein Update-Profil für die Lehrer-Geräte konfiguriert werden (Gruppe: C_LuL).




Microsoft Endpoint Manager Admin Center
Home
Dashboard
Alle Dienste
FAVORITEN
Geräte
Apps
Endpunktsicherheit
Berichte
Benutzer
Gruppen
Mandantenverwaltung
Problembehandlung + Support
Home > Geräte >
Updatering für Windows 10 und höher erstellen
Windows 10 und höher
Grundlagen
Einstellungen für Updatering
Zuweisungen
Überprüfen + erstellen
Name *
Windows Updates für Schülergeräte
Beschreibung
Zurück
Weiter


Microsoft Endpoint Manager Admin Center
Home > Geräte >
Updatering für Windows 10 und höher erstellen
Windows 10 und höher
Grundlagen
Einstellungen für Updatering
Zuweisungen
Überprüfen + erstellen
Einstellungen aktualisieren
Wartungskanal
Halbjährlicher Kanal
Microsoft-Produktupdates *
Erteilen Sie Blockieren
Windows-Treiber *
Erteilen Sie Blockieren
Rückstellungszeitraum für Qualitätsupdates (Tage) *
0
Rückstellungszeitraum für Funktionsupdates (Tage) *
0
Zeitraum für das Deinstallieren von Featureupdates (2 bis 60 Tage) *
10
Einstellungen für Benutzeroberfläche
Automatisches Updateverhalten
Zur Wartungszeit automatisch installieren
Beginn der Nutzungszeit *
7 Uhr
Ende der Nutzungszeit *
17 Uhr
Neustartüberprüfungen
Erteilen Sie Überspringen
Option zum Anhalten von Windows-Updates
Aktivieren Deaktivieren
Option zum Suchen nach Windows-Updates
Aktivieren Deaktivieren
Benutzergenehmigung zum Schließen der Neustartbenachrichtigung erforderlich
Ja Nein
Anzahl von Stunden, 2, 4, 8, 12 oder 24
Zurück
Weiter


Microsoft Endpoint Manager Admin Center
admin.schnetzer@vobs.at
Updatering für Windows 10 und höher erstellen
Grundlagen
Einstellungen für Updatering
Zuweisungen
Eingeschlossene Gruppen
Gruppen hinzufügen
Alle Benutzer hinzufügen
Alle Geräte hinzufügen
Gruppen
Keine Gruppen ausgewählt
Ausgeschlossene Gruppen
Zurück
Weiter
Wählen Sie die Gruppen aus, die eingeschlo...
Azure AD-Gruppen
c_SuS
Ausgewählt
Ausgewählte Elemente
Entfernen
Auswählen



2. Gesichtserkennung (Windows Hello for Business) einrichten

2.1. Allgemeines

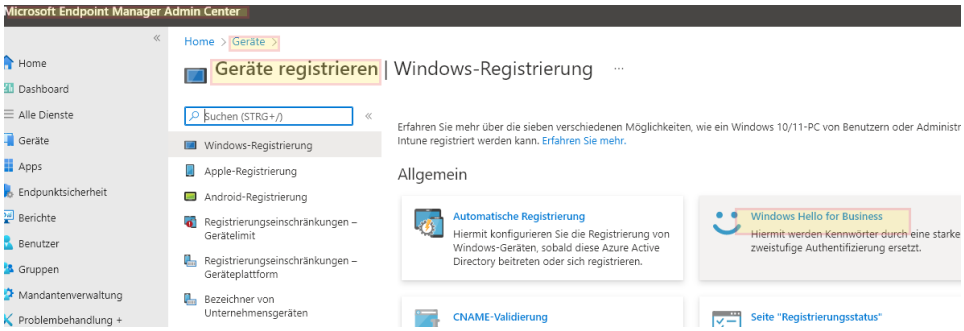
Die Windows-SurfaceGo2-Tablets bzw. die eingebauten Kameras unterstützen die Anmeldung am Gerät (anstatt der Eingabe von Benutzername und Passwort) per Gesichtserkennung.
Um diese komfortable Loginvariante mit Gesichtserkennung überhaupt nutzen zu können, muss auf den Geräten „Windows Hello for Business“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

Hinweise dazu:

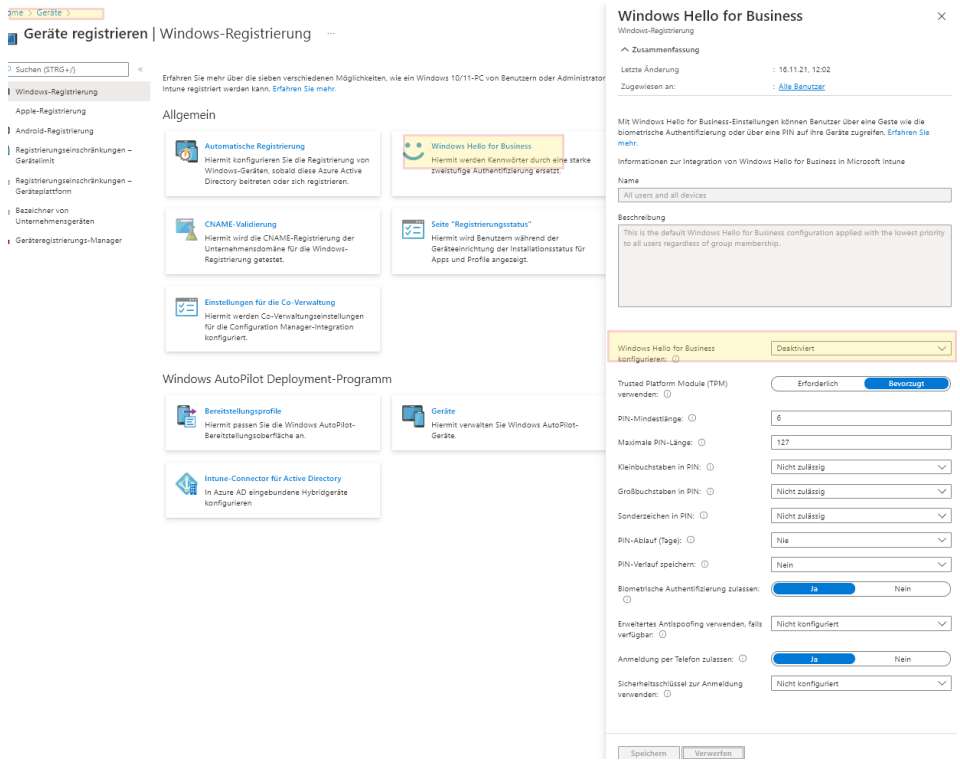
- Wird die Gesichtserkennung in Intune aktiviert, muss verbindlich auch ein PIN (min. 6 Zahlen – und nur Zahlen) vergeben werden. Zusätzlich muss für die PIN-Einrichtung **einmalig** ein Handy (TAN per SMS oder Authenticator-App installieren) zur Verfügung stehen.
- Die Einrichtung der Gesichtserkennung 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:

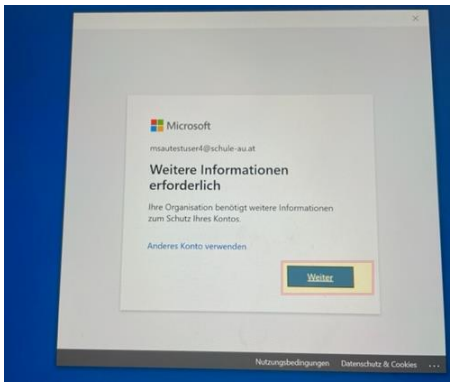


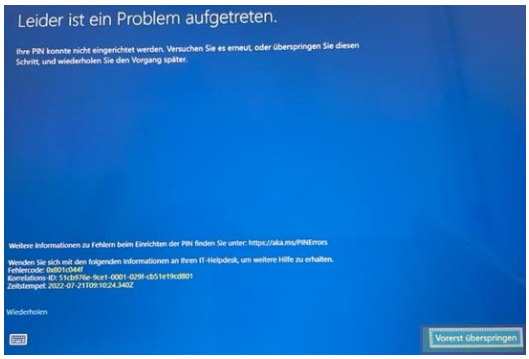
Wir belassen hier die Standardeinstellung bzw. stellen beim Punkt „Windows Hello for Business konfigurieren“ deaktiviert ein. Damit werden die „Windows Hello for Business“-Einstellungen nicht von Intune gesteuert. Bestehende Windows Hello for Business-Einstellungen auf Windows-Geräten werden nicht geändert.

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.

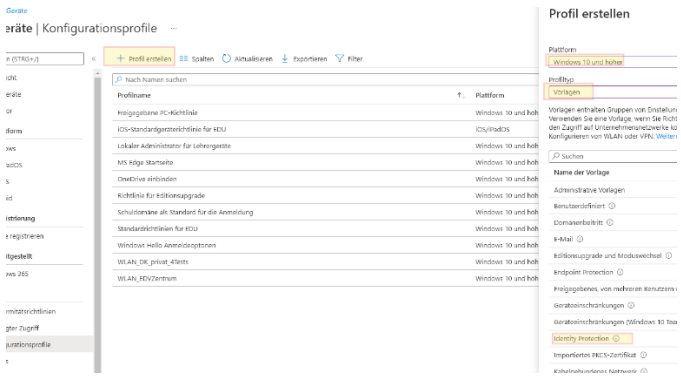
2.2. Wunschkonfiguration

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.

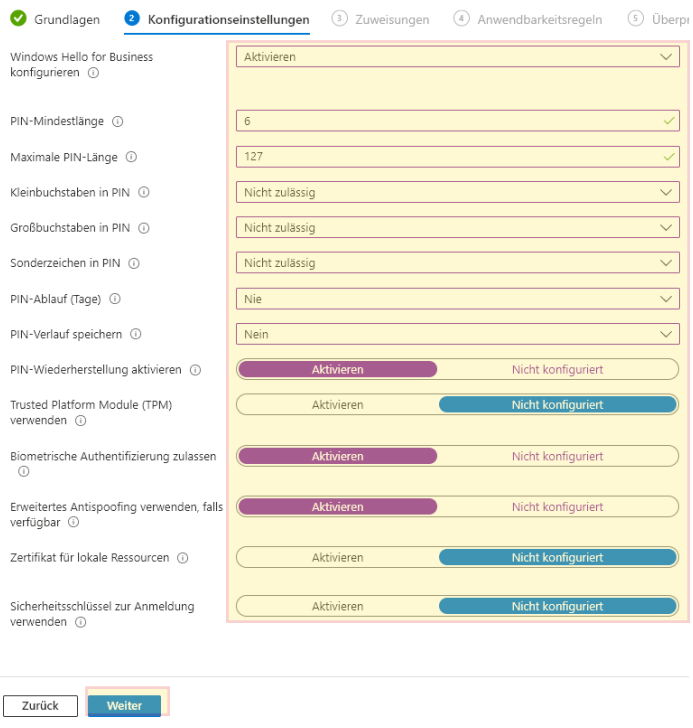
2.2.1. Wunschkonfiguration umsetzen

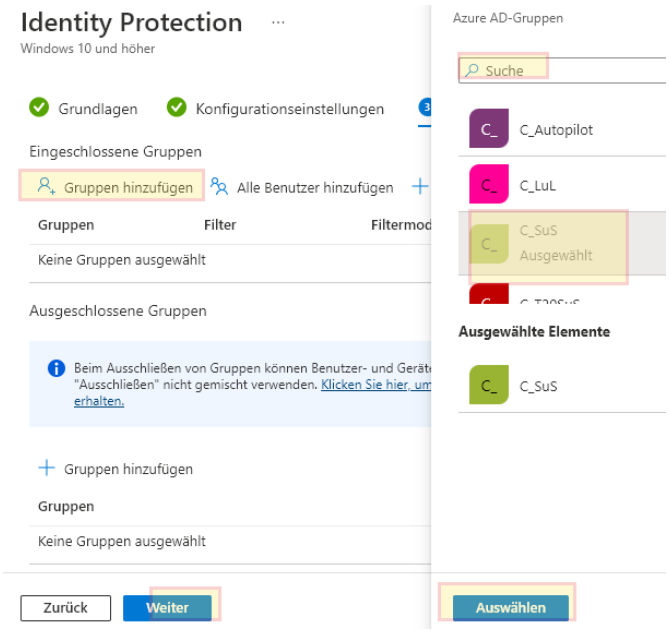
1) „Windows Hello for Business“ über ein Konfigurationsprofil aktivieren

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


Profil erstellen


Identity Protection
Windows 10 und höher
Grundlagen
Überprüfen und speichern
Name *
Windows Hello aktivieren
Beschreibung
"Windows Hello for Business" aktivieren, damit die Gesichtserkennung eingerichtet werden kann
Plattform
Windows 10 und höher
Profiltyp
Identity Protection
Zurück
Weiter


Grundlagen
Konfigurationseinstellungen
Zuweisungen
Anwendbarkeitsregeln
Windows Hello for Business konfigurieren
Aktivieren
PIN-Mindestlänge
6
Maximale PIN-Länge
127
Kleinbuchstaben in PIN
Nicht zulässig
Großbuchstaben in PIN
Nicht zulässig
Sonderzeichen in PIN
Nicht zulässig
PIN-Ablauf (Tage)
Nie
PIN-Verlauf speichern
Nein
PIN-Wiederherstellung aktivieren
Aktivieren
Nicht konfiguriert
Trusted Platform Module (TPM) verwenden
Aktivieren
Nicht konfiguriert
Biometrische Authentifizierung zulassen
Aktivieren
Nicht konfiguriert
Erweitertes Antispoofing verwenden, falls verfügbar
Aktivieren
Nicht konfiguriert
Zertifikat für lokale Ressourcen
Aktivieren
Nicht konfiguriert
Sicherheitsschlüssel zur Anmeldung verwenden
Aktivieren
Nicht konfiguriert
Zurück
Weiter



-> 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:

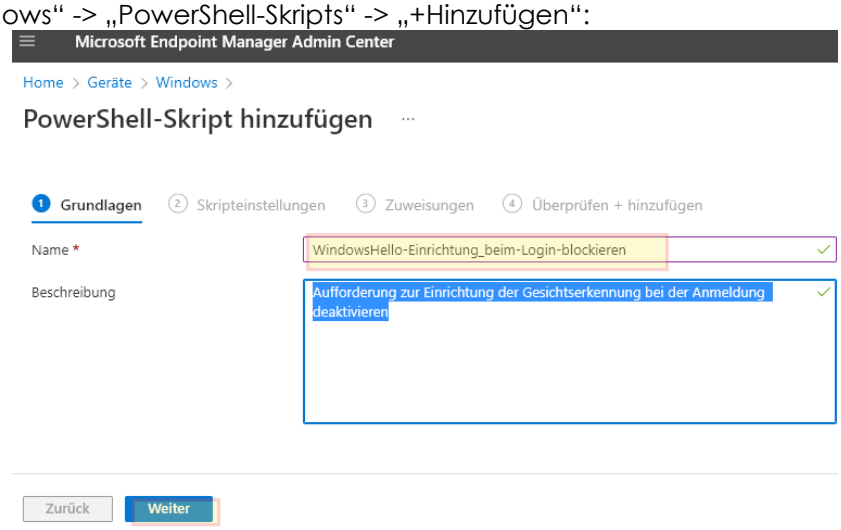
```
$Path = "HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork"
If (!(Test-Path $Path)) {
  New-Item -Path $Path
}
Set-ItemProperty -Path $Path -Name 'DisablePostLogonProvisioning' -Type "DWORD" -Value "1" -FORCE
Set-ItemProperty -Path $Path -Name "Enabled" -Type 'DWORD' -Value "1"  -FORCE
```

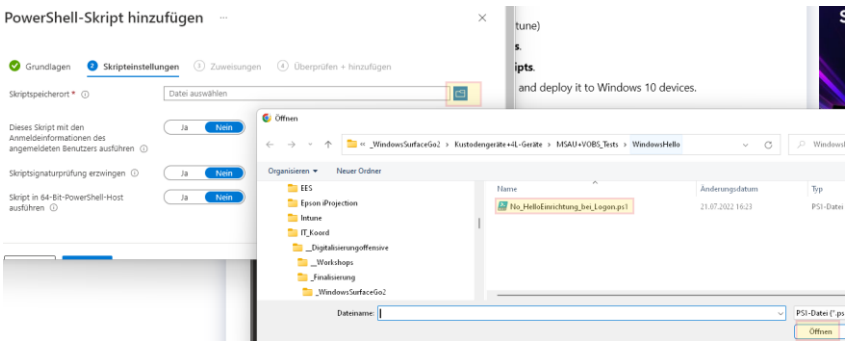
Diese drei Befehlszeilen in eine Textdatei kopieren und z. B. als „No_HelloEinrichtung_bei_Logon.ps1“ abspeichern.

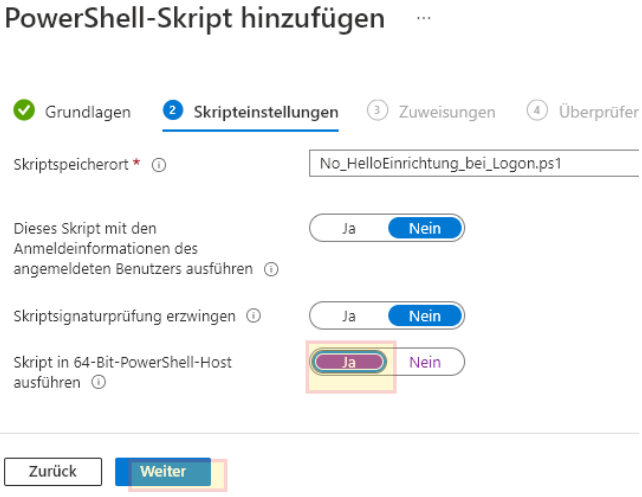
… oder hier herunterladen:
No_HelloEinrichtung_bei_Logon.ps1

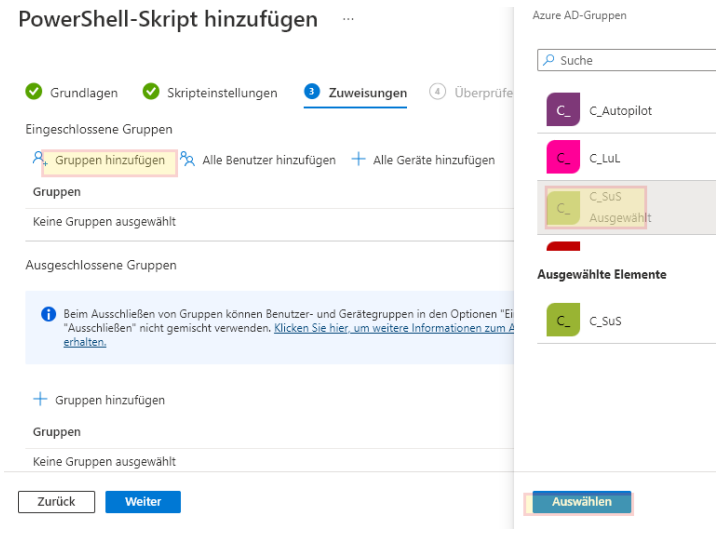
.. und das dann in Intune implementieren:

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







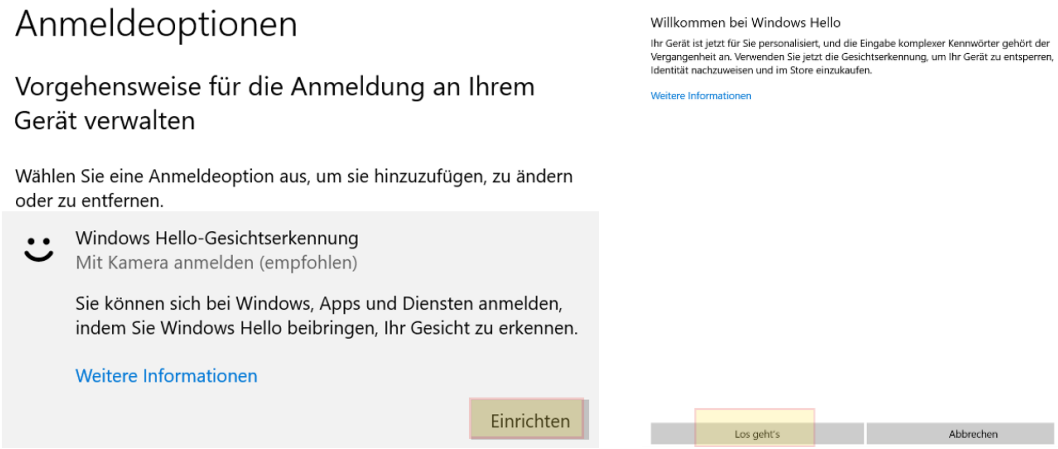


-> „Hinzufügen“ -> fertig

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“ eigegeben:

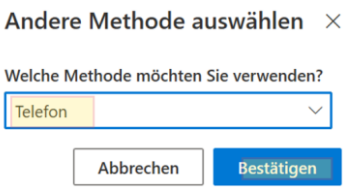


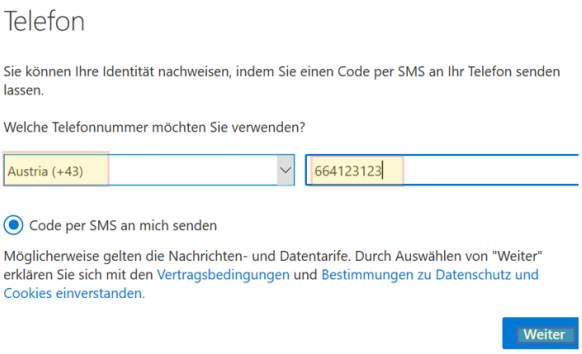
Die Kamera erscheint und richtet Gesichtsmerkmale ein …

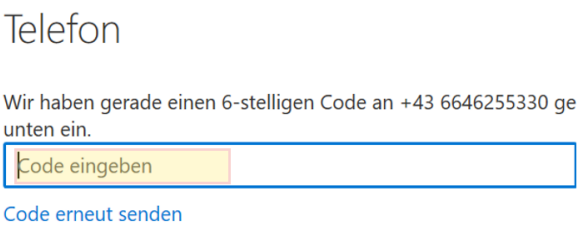
Zusätzlich muss verbindlich eine PIN eingerichtet werden (min. 6 Zahlen – und nur Zahlen):


Microsoft
msautestuser3@schule-au.at
Weitere Informationen erforderlich
Ihre Organisation benötigt weitere Informationen zum Schutz Ihres Kontos.
Anderes Konto verwenden
Weiter

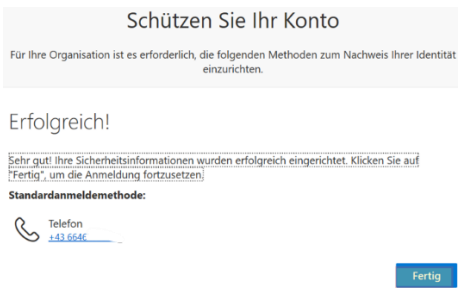

Schützen Sie Ihr Konto
Für Ihre Organisation ist es erforderlich, die folgenden Methoden zum Na einzurichten.
Microsoft Authenticator
Rufen Sie zuerst die App ab.
Installieren Sie die Microsoft Authenticator-App auf Ihrer herunterladen
Nachdem Sie die Microsoft Authenticator-App auf Ihrem haben, wählen Sie "Weiter".
Ich möchte eine andere Authentifikator-App verwenden
ich möchte eine andere Methode einrichten.

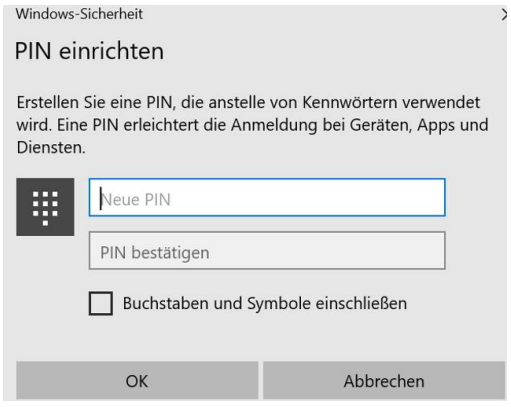

Andere Methode auswählen
Welche Methode möchten Sie verwenden?
Telefon
Abbrechen
Bestätigen


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

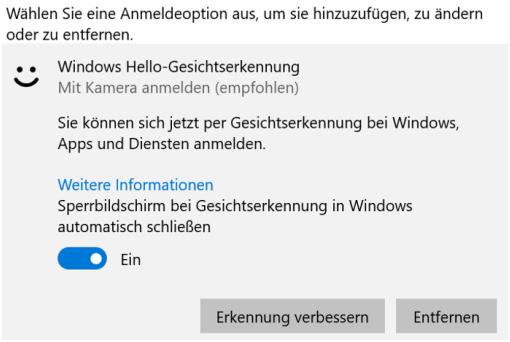

Telefon
Wir haben gerade einen 6-stelligen Code an +43 6646255330 ge unten ein.
Code eingeben
Code erneut senden


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
+43 664
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:



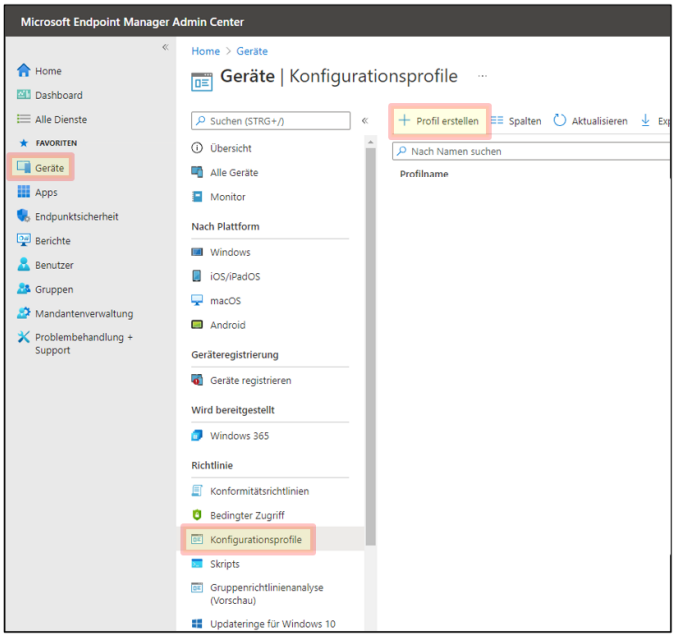
3. Microsoft Edge Konfiguration

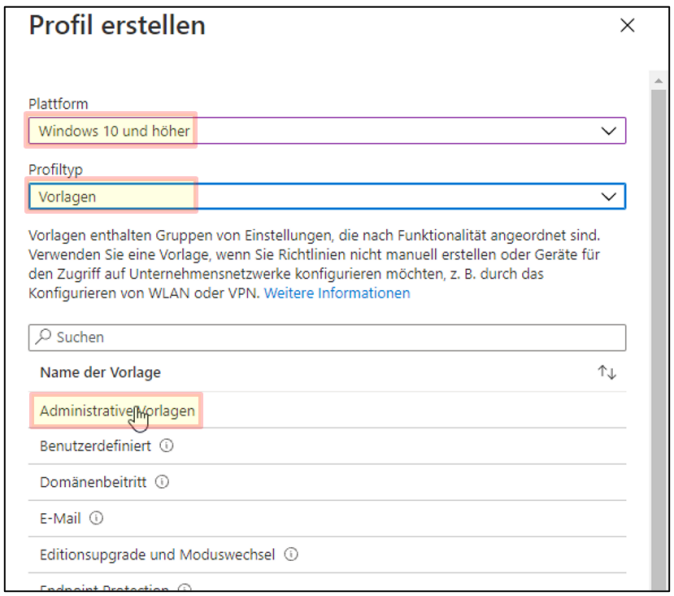
3.1. Allgemeines

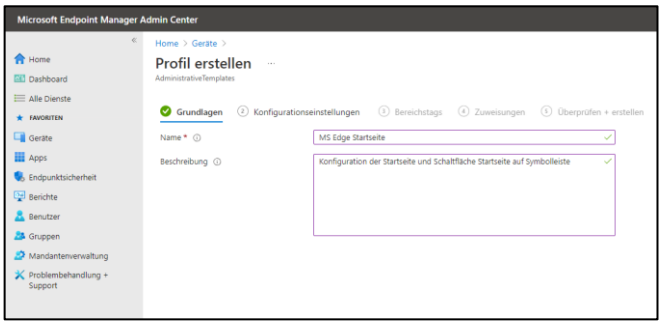
Die Startseite kann nicht über die Standardrichtlinie für EDU konfiguriert werden, sondern muss zusätzlich mit einem Konfigurationsprofil eingerichtet werden.

3.2. Konfiguration - Startseite

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

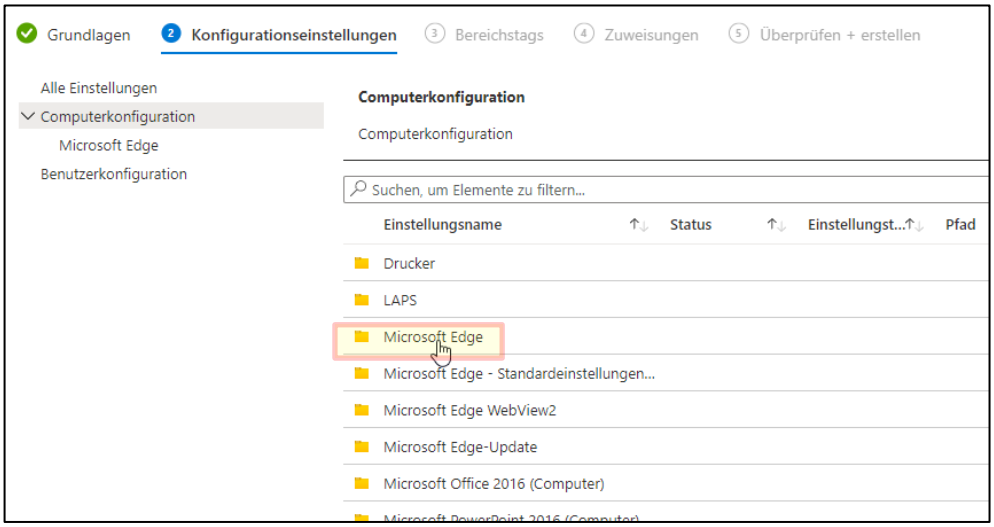




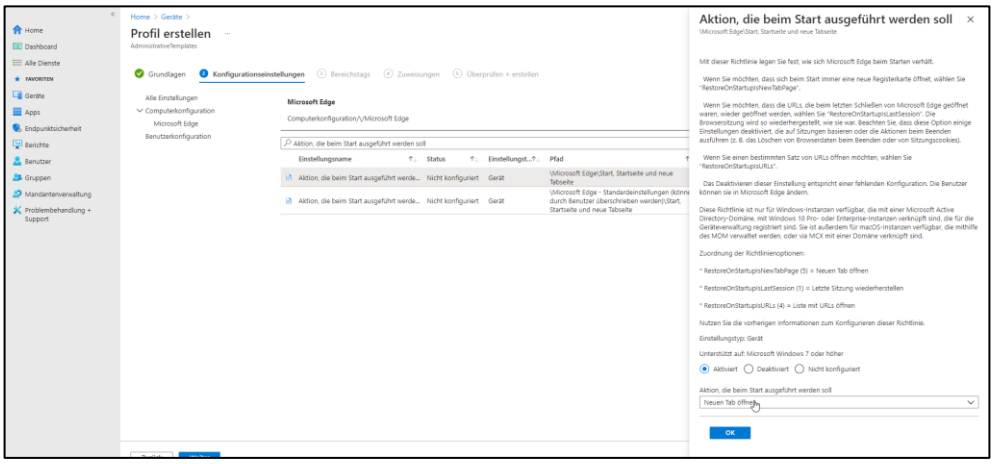


Name:
`MS Edge Startseite`

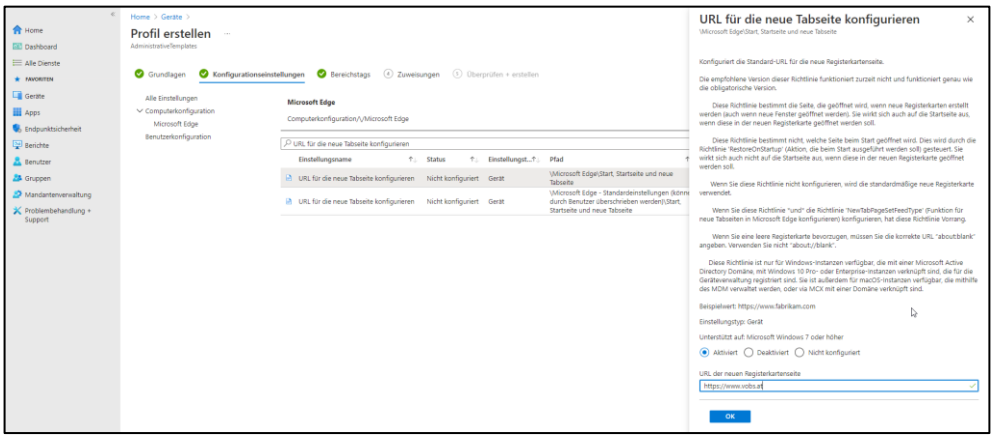
Beschreibung:
`Konfiguration der Startseite und Schaltfläche Startseite auf Symbolleiste`



Fünf Konfigurationen für Microsoft Edge:

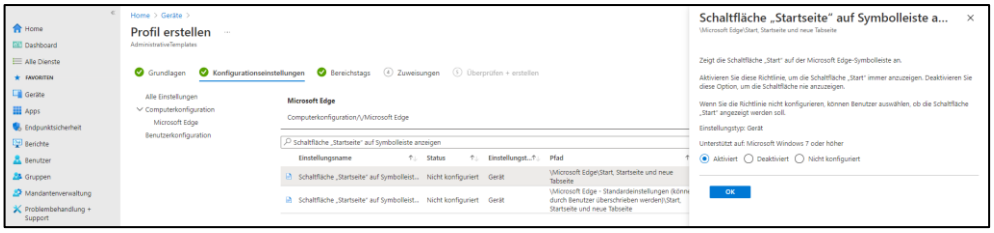


- Aktion, die beim Start ausgeführt werden soll
- Aktivieren und Neuen Tab öffnen

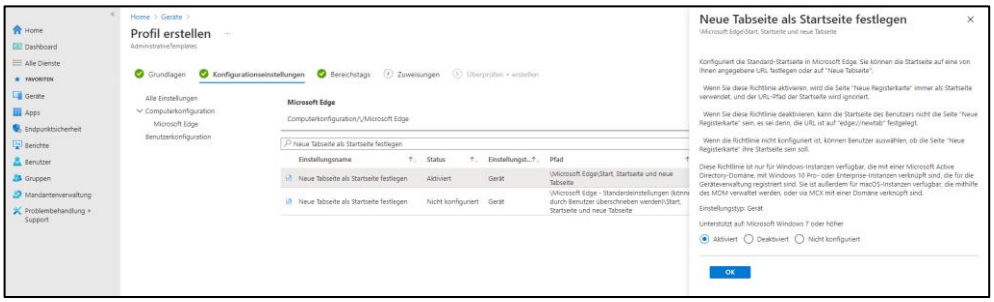


- URL für die neue Tabseite konfigurieren
- Aktivieren und gewünschte Seite angeben „https://www.vobs.at“

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

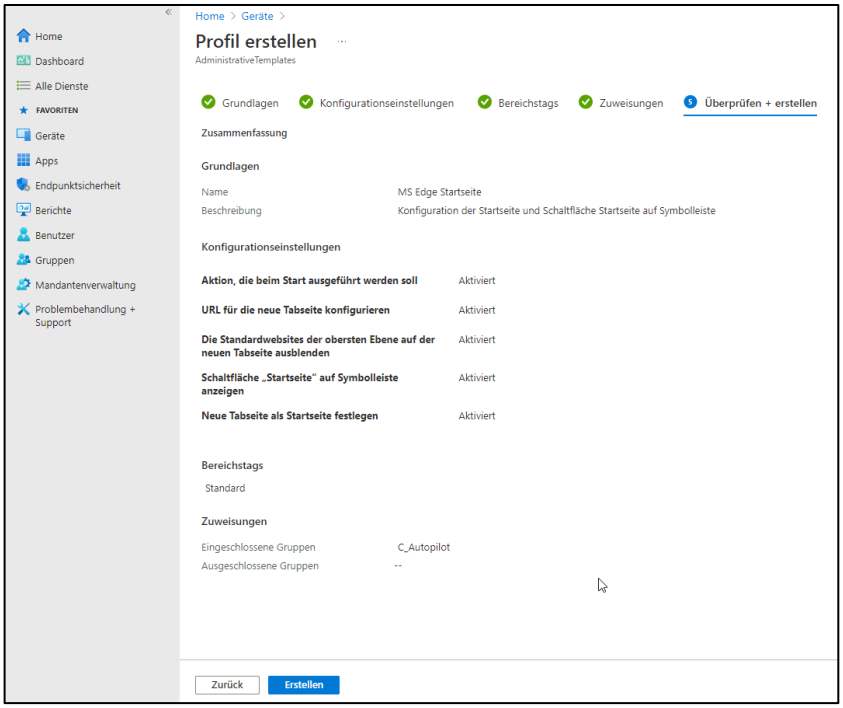


- Schaltfläche „Startseite“ auf Symbolleiste anzeigen
- Aktivieren



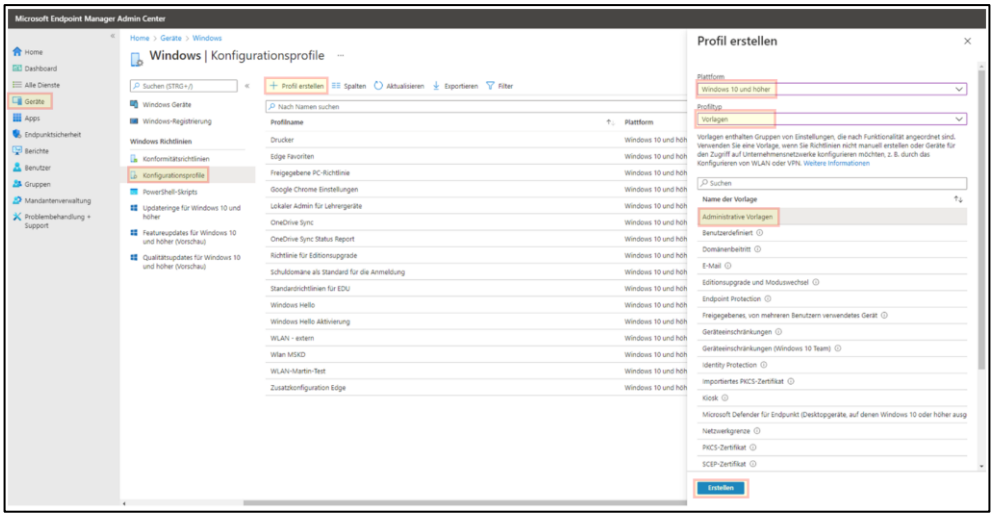
- `Neue Tabseite als Startseite festlegen`
- `Aktivieren`

Zuweisung der Gruppe C_Autopilot.



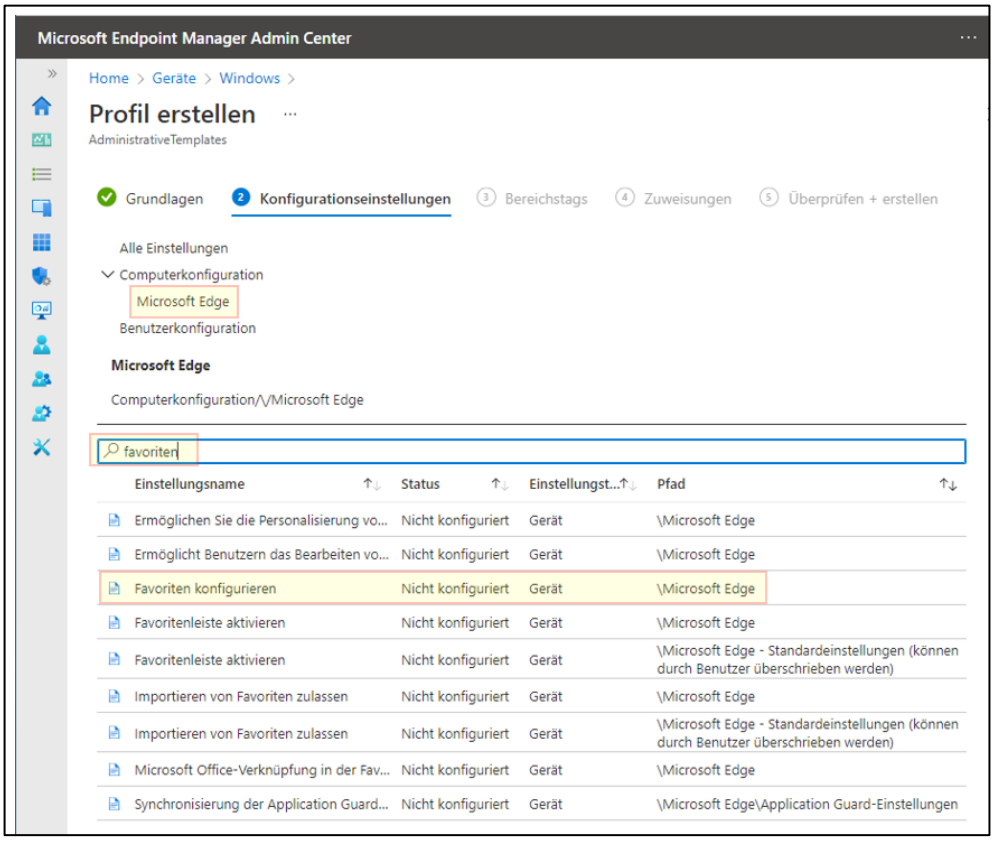
3.3. Konfiguration – Favoriten

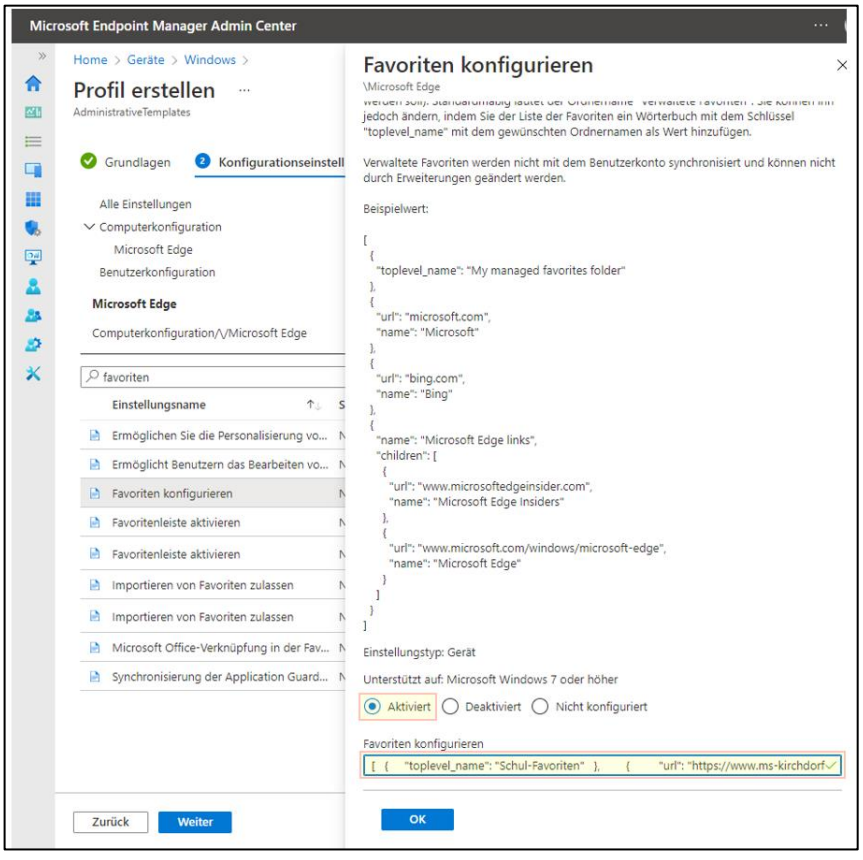
Erstellen eines neuen Geräte-Konfigurationsprofil



Name des Konfigurationsprofils: MS Edge Favoriten – Administratives Template
Beschreibung: Favoriten mit Liste bereitstellen

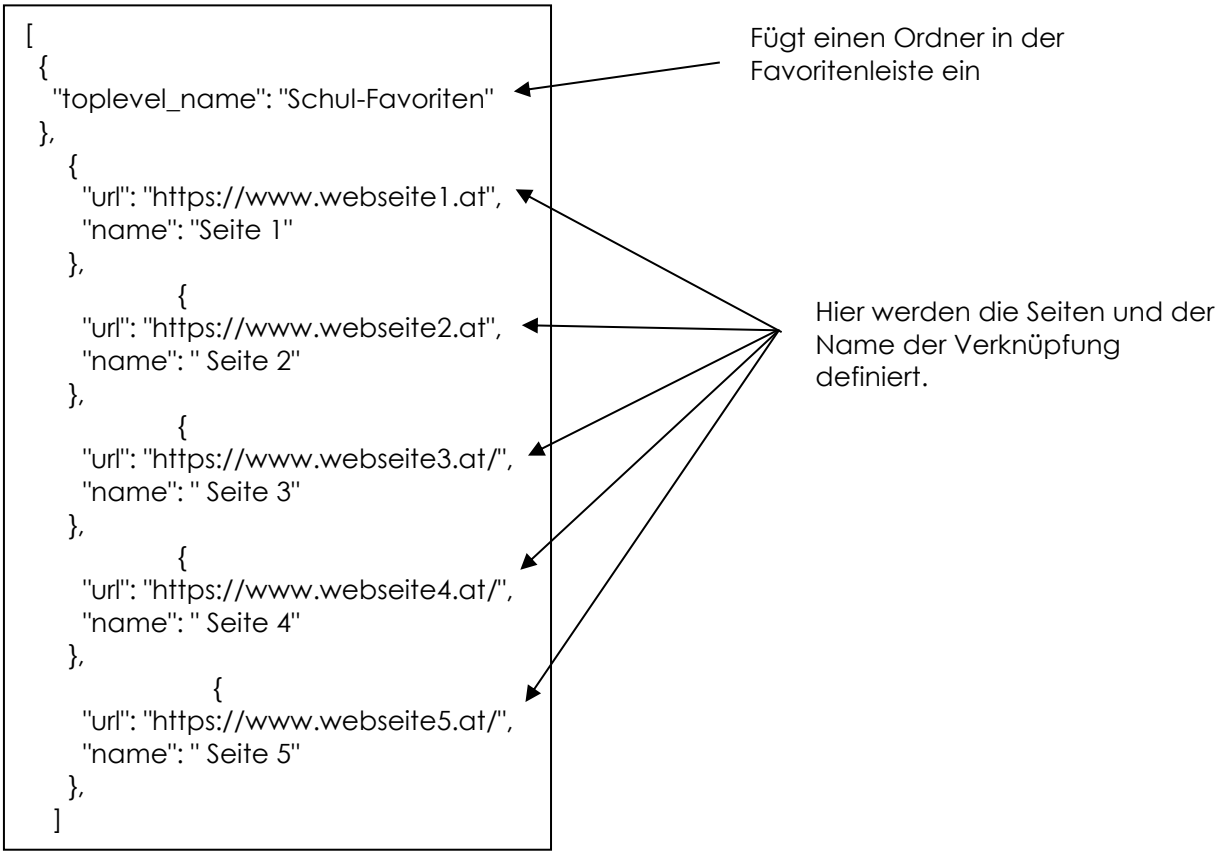
Nach dem „Erstellen“ klicken - Microsoft Edge in der Liste auswählen. Danach die „Favoriten“ im Suchfeld suchen.



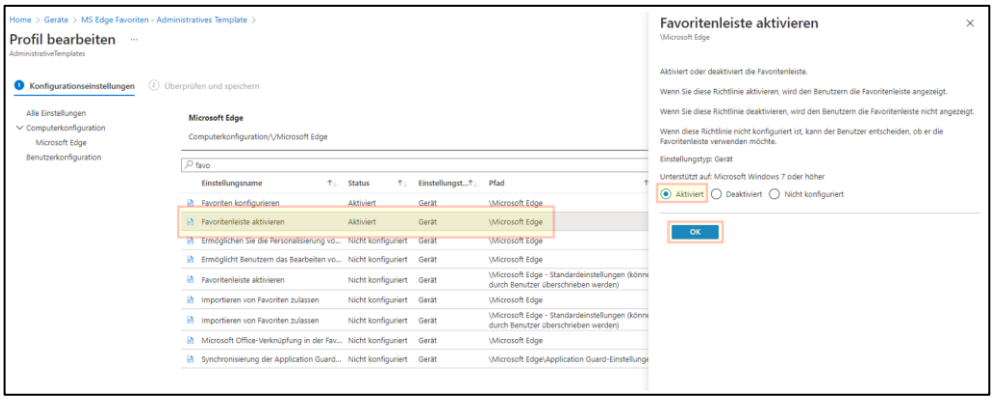


Im Feld „Favoriten konfigurieren“ wird nun folgender Eintrag hinzugefügt.

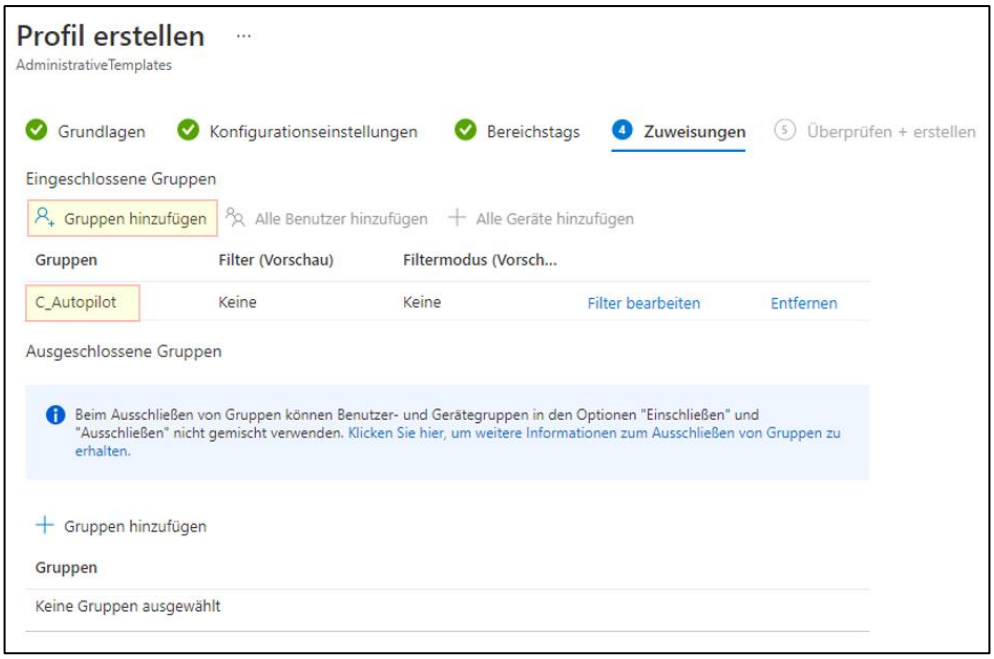
Beispiel:



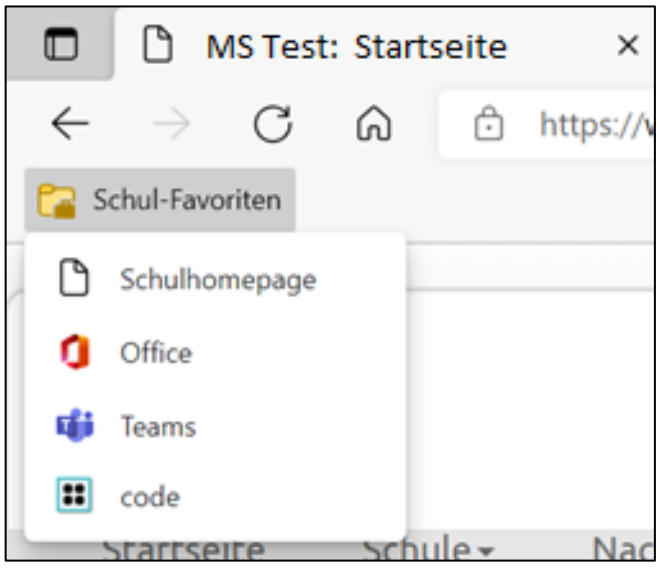
Im Anschluss wird noch die Favoritenleiste aktiviert



Im letzten Schritt fügen wir wiederum die entsprechende Gruppe hinzu. Z.B. C_Autopilot



Zum Schluss alles nochmals Überprüfen und erstellen.



4. McAfee Remover

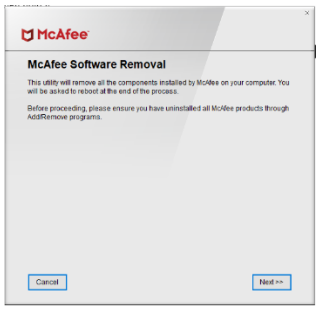
4.1. Allgemeines

Die in der Geräteinitiative ausgeschriebenen 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.

4.2. 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)
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

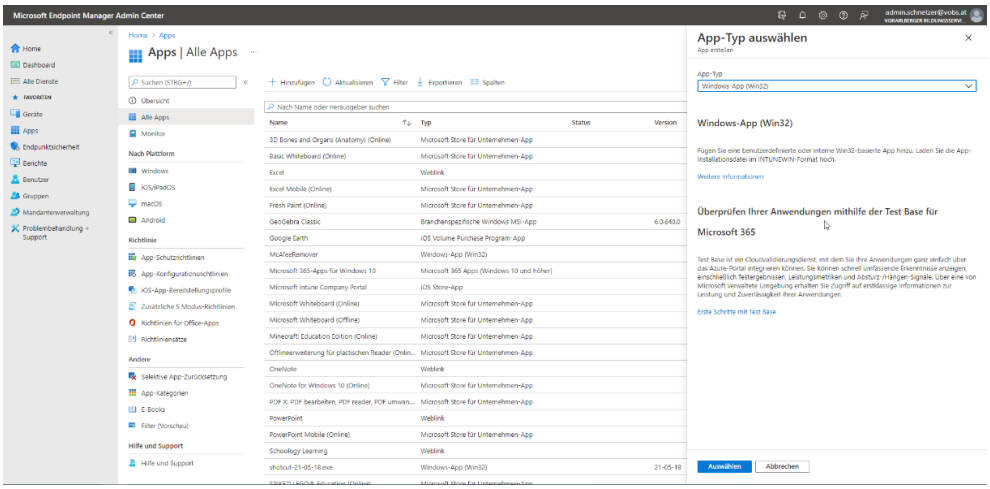
Skript-Inhalt: (copy/paste)

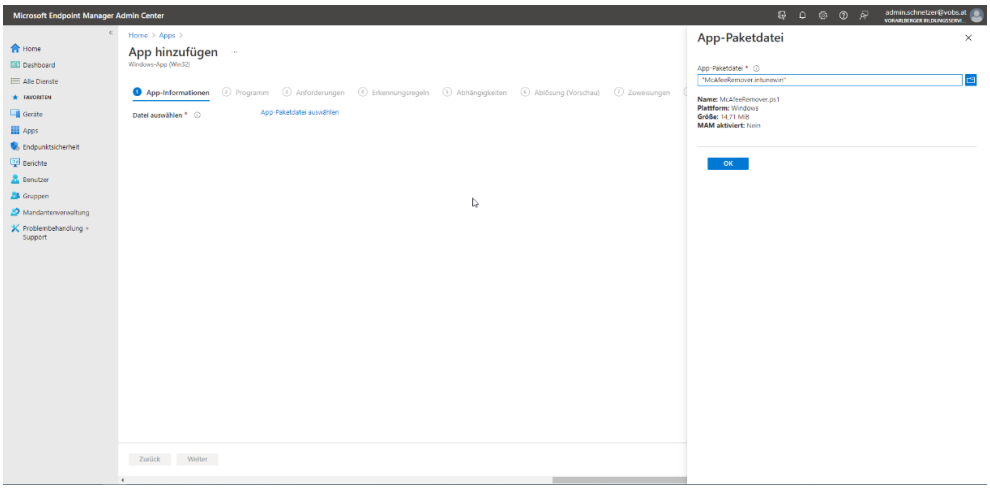
```
# Run the cleanup tool
$program= ".\McCleanup.exe"
$programArg= "-p
StopServices,MFSY,PEF,MXD,CSP,Sustainability,MOCP,MFP,APPSTATS,Aut
h,EMproxy,FWdiver,HW,MAS,MAT,MBK,MCPR,McProxy,McSvcHost,VUL,MHN,MN
A,MOBK,MPFP,MPFPCU,MPS,SHRED,MPSCU,MQC,MQCCU,MSAD,MSHR,MSK,MSKCU,M
WL,NMC,RedirSvc,VS,REMEDIATION,MSC,YAP,TRUEKEY,LAM,PCB,Symlink,Saf
eConnect,MGS,WMIRemover,RESIDUE -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
```

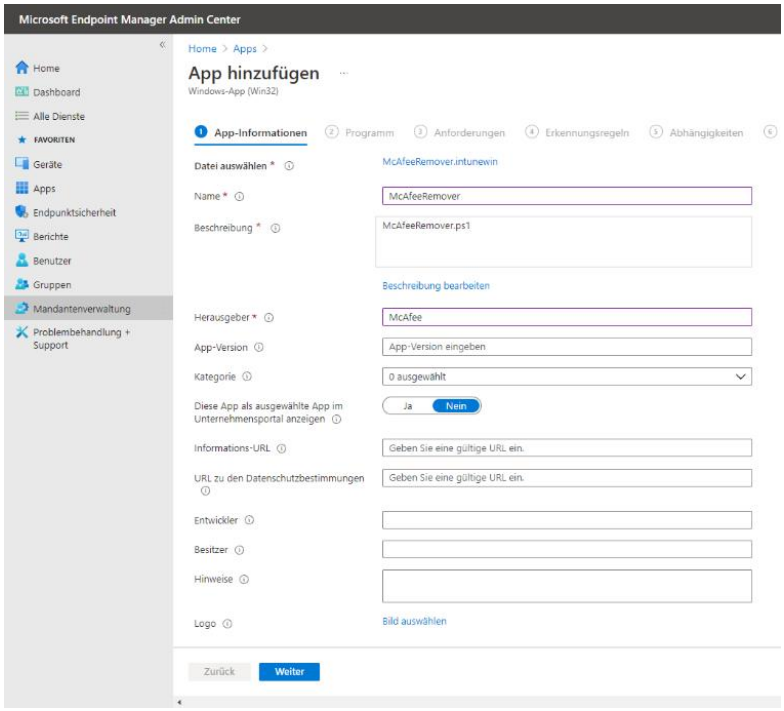
Erstellen des InuneWin-Paketes

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

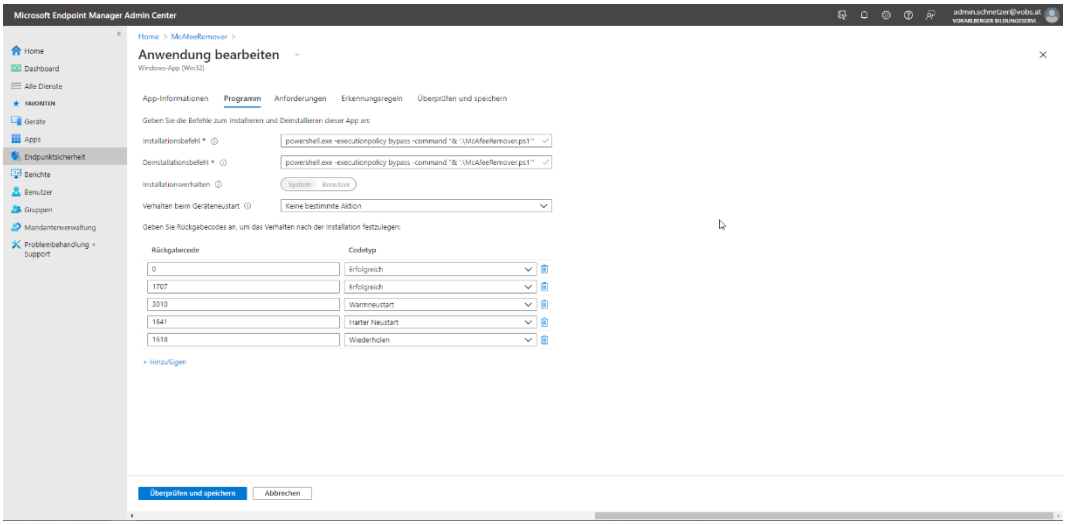
4.3. Bereitstellen des Paketes:







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

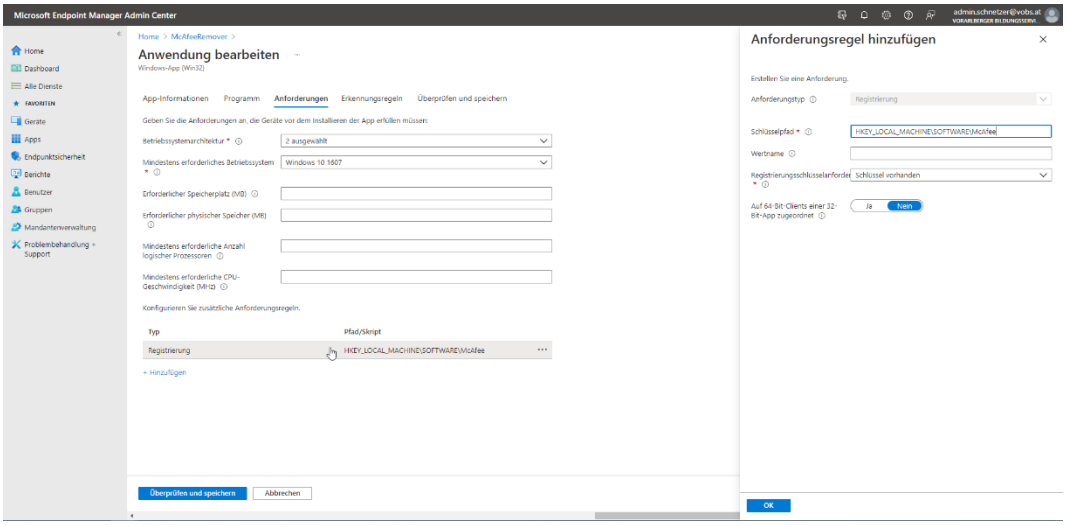


Installationsbefehl:

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

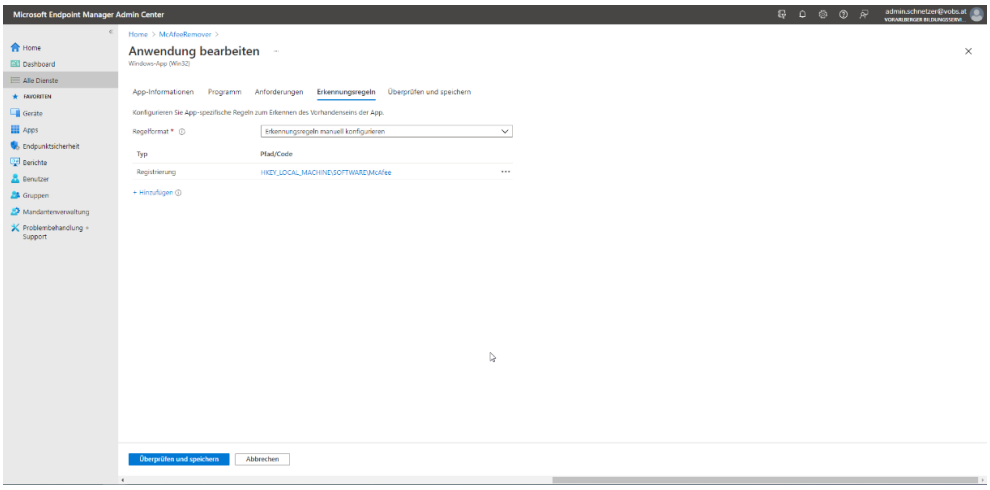
Deinstallationsbefehl:
```
powershell.exe -executionpolicy bypass -command "& '.\McAfeeRemover.ps1'"
```

Schritt 3: **„Anforderungen“**



Schlüsselpfad: `HKEY_LOCAL_MACHINE\SOFTWARE\McAfee`
Registrierungsschlüsselanforderungen: `Schlüssel vorhanden`

Schritt 4: **„Erkennungsregeln“**



Schlüsselpfad: `HKEY_LOCAL_MACHINE\SOFTWARE\McAfee`
Registrierungsschlüsselanforderungen: `Schlüssel` **`nicht`** `vorhanden`

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