	Ersteller/Editor	Rechenzentrum ZS	Datum	14.06.2023
		Alfred Fuchs		

Anleitung für IT-Betreuer
Defender for Endpoint (MDE) & Intune Massenbereitstellung (Bulk Enrollment)

1 Einleitung

Diese Anleitung beschreibt die Durchführung der Massenregistrierung für Windowsgeräte in Microsoft Intune. Damit werden die Geräte mit Azure AD, dem Cloud gestützten Verzeichnisdienst von Microsoft verbunden, in die Geräteverwaltung Intune integriert und in das Defender for Endpoint Portal aufgenommen. Außerdem wird der Virenscanner Sophos Endpoint Protection entfernt.

2 Gültigkeit

Das Paket darf ausschließlich auf Dienstgeräten der Universität Regensburg angewendet werden. Es kann alternativ zur manuellen Registrierung benutzt werden. Das Paket darf nur an Mitarbeitende der Universität Regensburg, die ihr Dienstgerät verbinden möchten, weitergegeben werden. Es darf keinesfalls an unberechtigte Dritte weitergegeben werden.

3 Besondere Hinweise

Im Gegensatz zur manuellen Registrierung wird bei der Massenregistrierung kein administratives Azure-Konto verbunden.

Die Anmeldung nach dem Join erfolgt anders als vorher: Lokale Konten statt mit LocalUsername nun mit .\LocalUsername und Azure-Konten mit vip12345@ads.uni-regensburg.de.

Das Paket ist mit einem Ablaufdatum versehen, nach dem es nicht mehr eingesetzt werden kann.

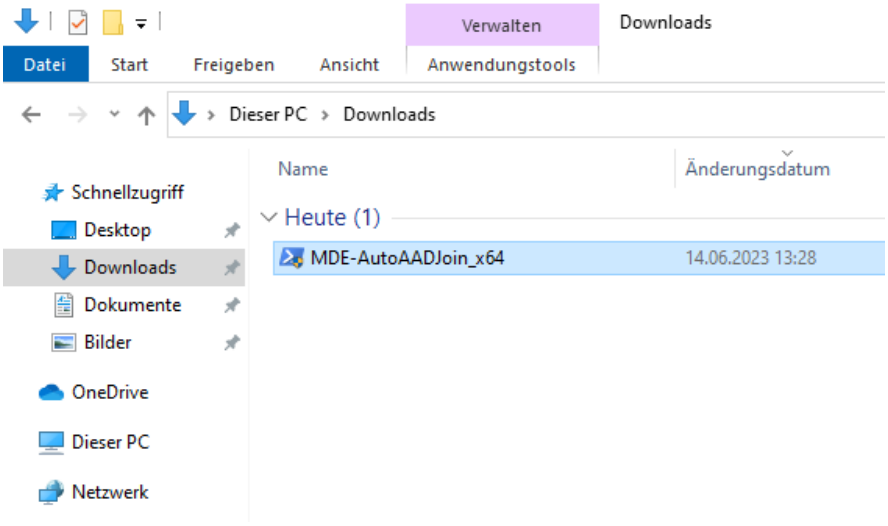
4 Voraussetzungen

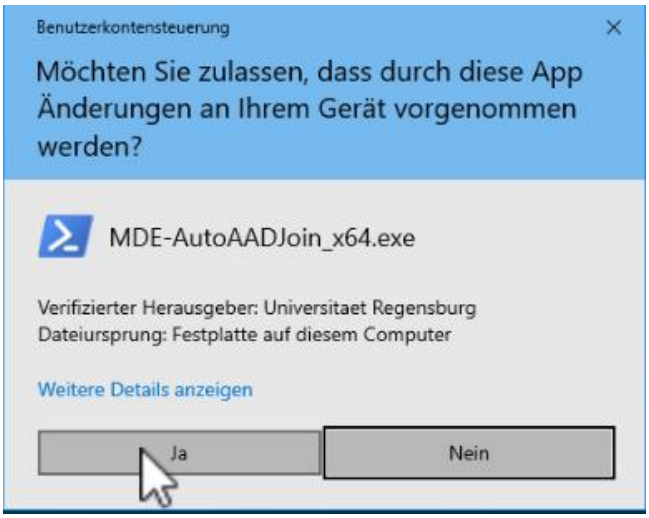
- Unterstützt werden nur Windows 10 und Windows 11 Geräte.
- Das Gerät ist bisher nicht in Azure AD oder in die lokale Domäne eingebunden. Wird durch Skript automatisch geprüft.
- Es ist der Account (Benutzername / Kennwort) eines Kontos mit lokaler Administratorberechtigung bekannt.

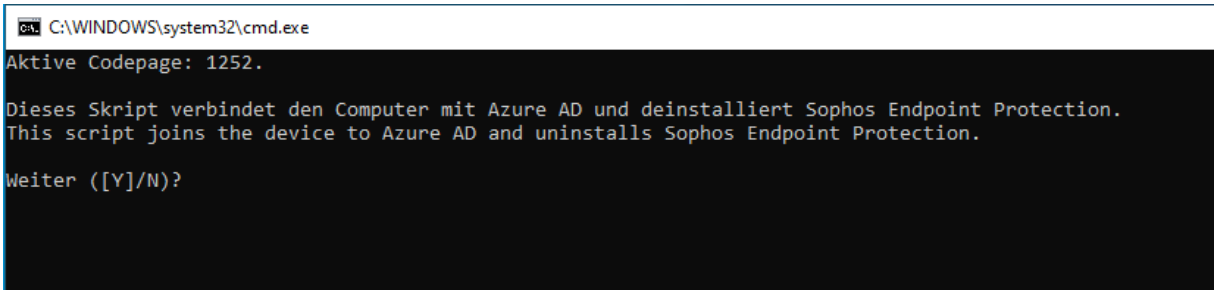
5 Durchführung

5.1 Massendeployment

Laden Sie das Paket „Defender BulkEnrollment Windows“ aus dem Softwarekatalog herunter (Kategorie „Defender for Endpoint“) und führen Sie dieses aus:

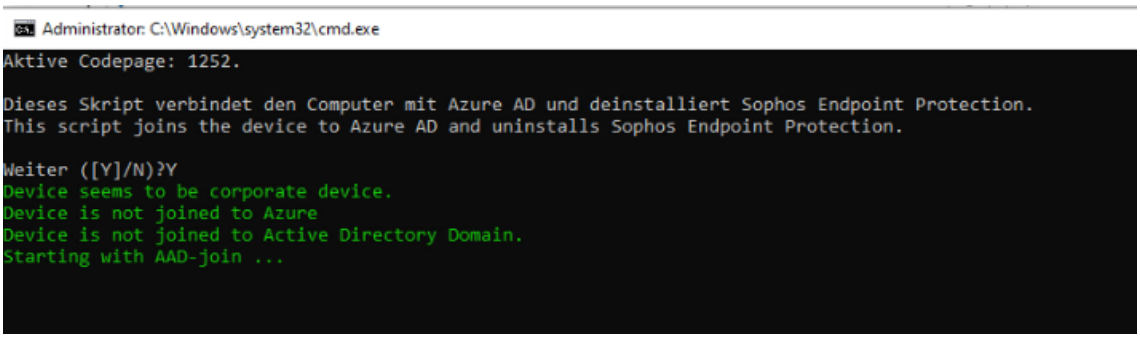






Bestätigen Sie die Ausführung mit Y.

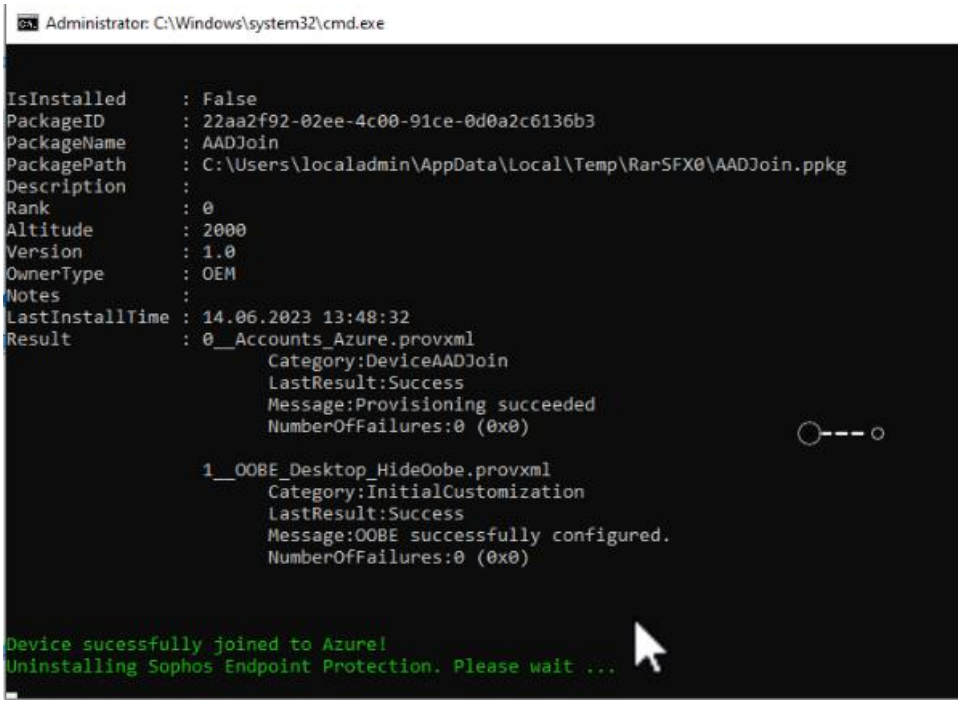
Es beginnt der Join …



Sofern das Skript das Gerät nicht als Dienstgerät mit entsprechendem Gerätenamen identifizieren kann, bricht es die Ausführung ab.

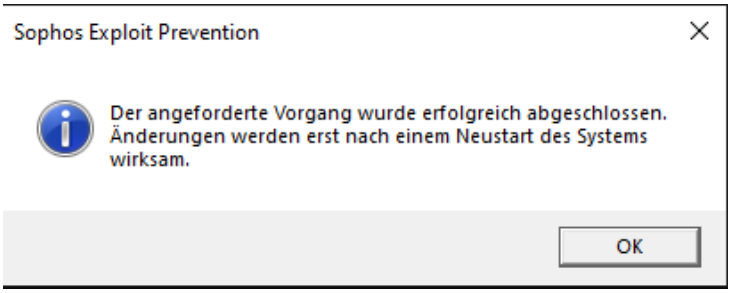
Sofern es sich trotzdem um ein Dienstgerät handelt, ist durch den zuständigen IT-Betreuer ein manueller Join des Gerätes durchzuführen.

Sind alle Prüfungen erfolgreich, erfolgt der Join …

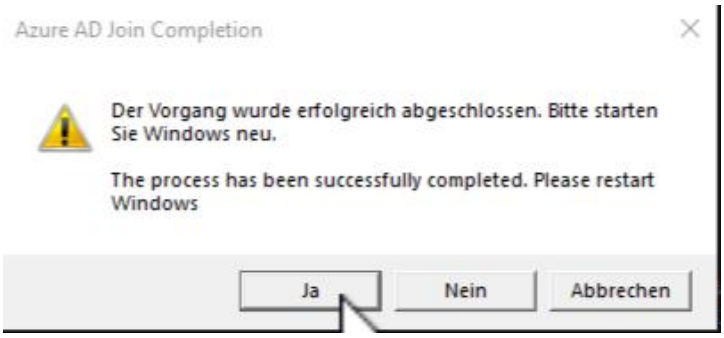


… und danach die Deinstallation des alten Sophos Virenscanners.

Das Skript zur Deinstallation von Sophos benötigt einige Minuten.



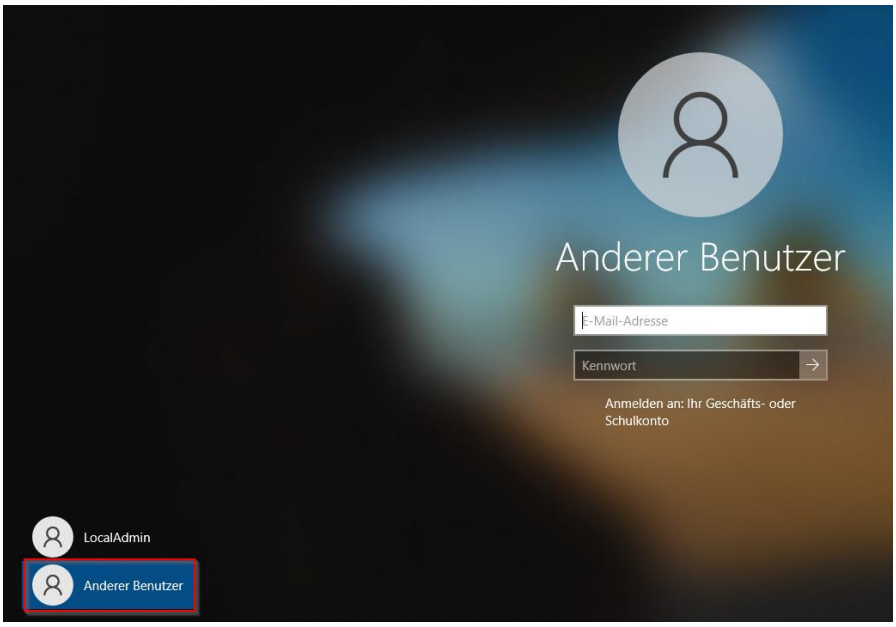
Danach erscheint eine Aufforderung zum Neustart des Geräts.



5.2 Anmeldung

Achtung: Nach dem Neustart erfolgt die Anmeldung nicht mehr wie gewohnt. Bitte lesen Sie VOR dem Neustart das Kapitel zur Anmeldung!

Nach einem Neustart können Sie sich mit dem Azure-Account anmelden:

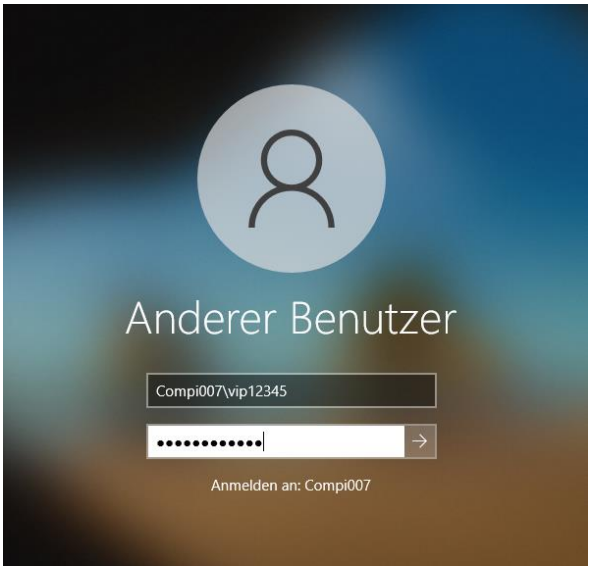


Es wird ein neues Benutzerprofil erzeugt.

Sie können auch weiterhin Ihre lokalen Konten benutzen. Die Anmeldung mit einem lokalen Konto erfordert allerdings die Angabe des Kontos in der Form

Rechnername\Konto oder **.\Konto**

Beispiele:

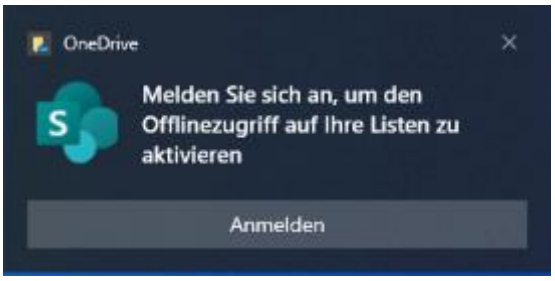


Bitte beachten Sie: Das Konto *vip12345@ads.uni-regensburg.de* ist ein AAD-Geschäftskonto und nicht identisch mit dem eventuell bereits vorhandenen lokalen Benutzerkonto *vip12345*. Es kann hier durchaus zwei getrennte lokale Profile geben.

5.2.1 Meldungen

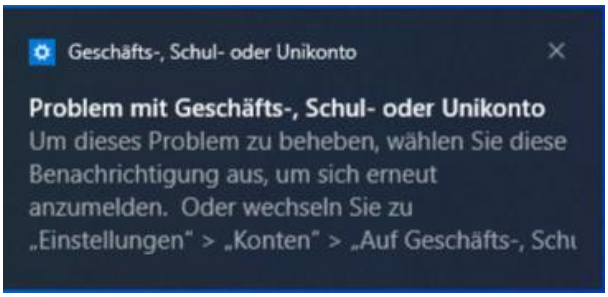
Nach der Anmeldung mit einem neuen Profil erscheinen i.d.R. einige neue Systemmeldungen von Windows.

OneDrive



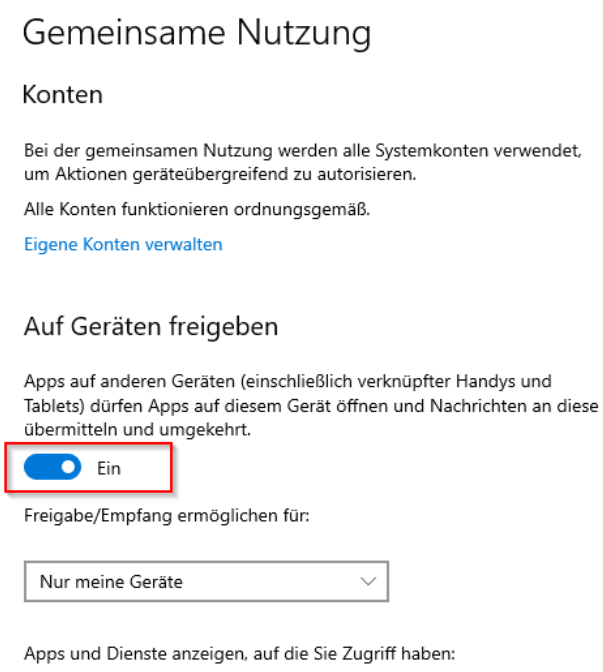
Ggf. wird Sie OneDrive auffordern, sich anzumelden. Wir weisen darauf hin, dass unsere Richtlinien zur Nutzung von Onlinediensten für die Ablage von personenbezogenen Daten sowie Daten mit erhöhtem Schutzbedarf zu beachten sind.
Es ist i.d.R. aus diesen Gründen eher nicht empfehlenswert, die Empfehlung von Microsoft zur Sicherung der kompletten Ordner wie „Dokumente“ anzunehmen:

Geschäfts- Schul- oder Unikonto



Diese Meldung tritt gelegentlich auf, wenn die zwischengespeicherten Microsoft-Anmeldedaten noch nicht synchronisiert wurden. Sie können diese Meldung ignorieren oder auf die Meldung klicken und dort den Button „Jetzt beheben“ verwenden.

Sofern Sie die Funktion „Gemeinsame Nutzung“ (auf die sich die Problemmeldung bezieht) nicht nutzen, können Sie die Funktion „Auf Geräten freigeben“ auch deaktivieren.



5.2.2 Windows Hello

Windows Hello for Business ist derzeit standardmäßig für alle Benutzer deaktiviert.

Wer zuvor bereits Windows Hello zur kennwortlosen Anmeldung mit PIN oder Biometrieverfahren genutzt hat und das auch weiter nutzen möchte, sollte sich VOR dem Join in die Ausnahmegruppe eintragen lassen. Ohne die entsprechende Gruppenmitgliedschaft wird Windows Hello hinterher nicht mehr funktionieren.

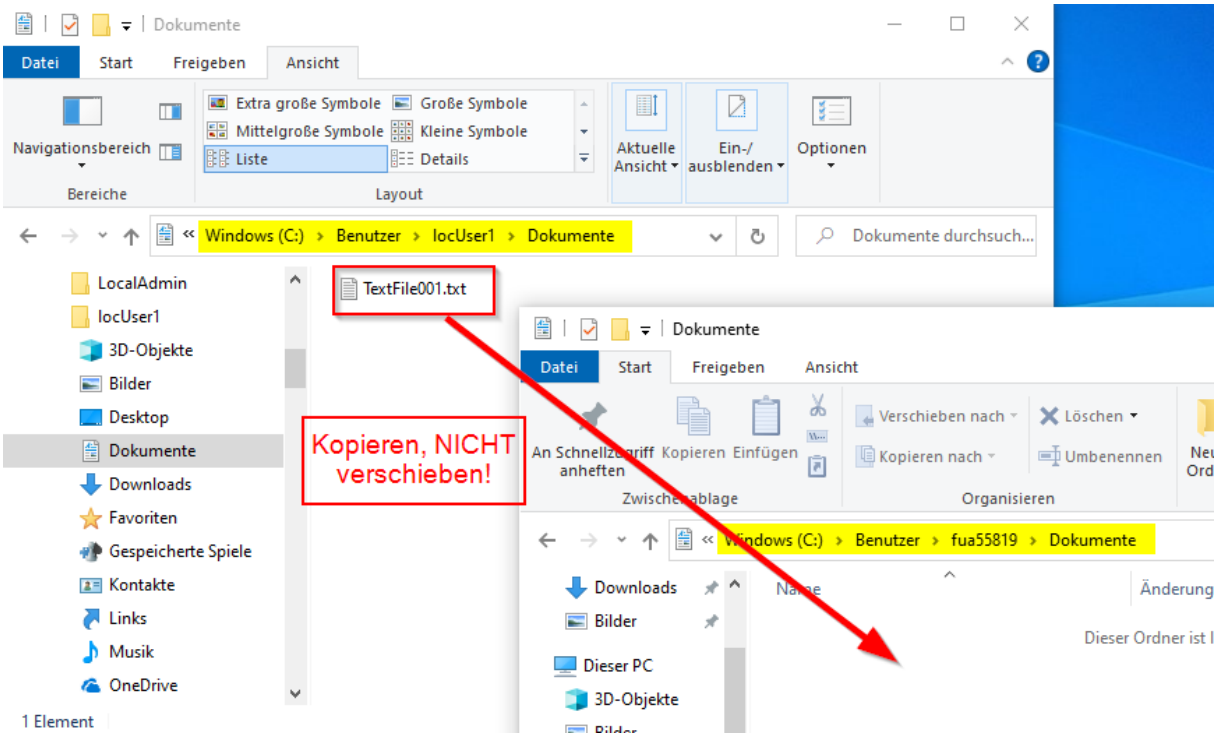
5.2.3 Intune & Defender for Endpoint

Mit dem Join zu Azure AD erfolgt zugleich automatisch im Hintergrund eine Integration des Computers in die Geräteverwaltung Intune. Mit Intune können z.B. Updates verteilt, Software installiert oder Richtlinien angewendet werden.

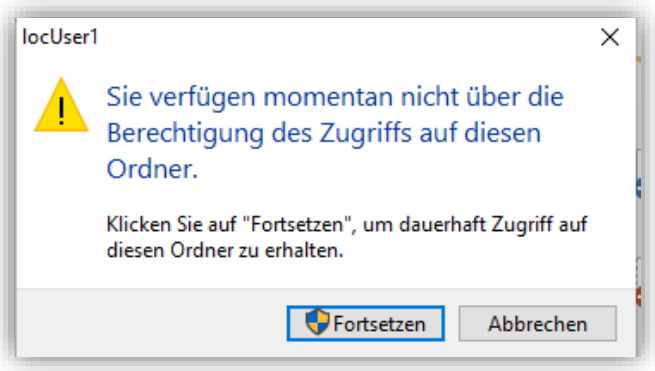
Außerdem wird das Gerät im Defender for Endpoint-Portal registriert. Defender for Endpoint ist eine Next Generation Virenschutzlösung von Microsoft.

5.3 Datenmigration

Sofern Sie in Zukunft unter dem Azure-Account arbeiten (empfohlen), können Sie die Daten teilweise aus dem alten in das neue Profil kopieren.



Beim Zugriff auf das alte Profil werden lokale Administrationsrechte abgefragt:



Zumeist vermisst man vor allem die Browserfavoriten. Diese können im alten Profil exportiert und im neuen Profil wieder importiert werden. Zum Verfahren suchen Sie bitte in der Hilfe des jeweiligen Browsers.