

E-BOOK

WINDOWS 11

DIE WICHTIGSTEN NEUERUNGEN IN WINDOWS 11 26H2 FÜR PROFESSIONELLE ANWENDER

Windows 11

EXTRA
COMPUTER GMBH

INHALTSVERZEICHNIS

01 Einleitung 04 |

1.1 Innovationen auf der alten Plattform 05

1.2 Unkompliziertes Upgrade 06

1.3 Inkonsistenzen zwischen ARM und Intel 06

02 Roadmap: OS soll entrümpelt werden 06 |

2.1 Rückzug von Copilot 07

2.2 Strafferes OOBE 07

03 Hohe RAM-Preise erzwingen Optimierung 08 |

3.1 Macs oder Winodws 10 als Alternative 08

3.2 Minimale Systemanforderungen nicht praxistauglich 08

3.3 Geplante Verbesserungen 10

3.4 Surface-Modelle wieder mit 8 GB RAM 10

04 Überarbeitetes Benutzer Interface 11 |

4.1 Flexible Positionierung der Taskbar 11

4.2 Kompaktes Startmenü 12

4.3 Desktop-Suche ohne Web-Ergebnisse 12

4.4 Weitere GUI-Verbesserungen 13

05 Änderungen bei Updates 14 |

5.1 Komfort zu Lasten der Sicherheit? 14

5.2 Updates während OOBE überspringen 14

5.3 Unbegrenzter Aufschub für Updates 15

5.4 Umgehung der Installation beim Neustart 15

5.5 Schnellere Installation, weniger Reboots 15

5.6 Neue Richtlinien für verwaltete Geräte 16

5.7 Neue Gruppenrichtlinie für Wartungsfenster 16

5.8 Defekte Treiber setzen 18

INHALTSVERZEICHNIS

06 Neue Reparatur- und Wiederherstellungsfunktionen 19 |

6.1 Wiederherstellung aus WinRE 19

6.2 Point-in-Time Restore auf einen VSS-Snapshot 20

6.3 System über Cloud Rebuild wiederherstellen 21

6.4 Wiederherstellung von Benutzereinstellungen 24

07 Neu: GNU Coreutils, Admin Protecition, WSL-Container 26 |

7.1 Administratorschutz als UAC-Alternative 27

7.2 Smart App Control 27

7.3 IAKerb und lokales KDC nicht an Bord 28

7.4 WSLc: Linux-Container ohne Docker ausführen 29

7.5 Intelligent Terminal 31

7.6 Windows Developer Config 31

08 ADMX v3.0: 17 neue Einstellungen 32 |

8.1 MSIX-Pakete 32

8.2 Drei Einstellungen für CLAT 33

8.3 Sharing Sheet 33

8.4 Restore von Windows Backup for Organizations 34

8.5 Active Directory und Entra ID 34

8.6 Windows Update 34

8.7 Inkonsistenzen in der Dokumentation 35

09 Zusammenfassung 36 |

01 EINLEITUNG

Auf den ersten Blick wirken die aktuellen Entwicklungen bei Windows 11 widersprüchlich: Zum einen kündigte Microsoft eine weitreichende Kurskorrektur in Richtung höherer Produktqualität und geringerer Systemvoraussetzungen an. Zum anderen basiert 26H2 aber noch auf der gleichen Plattform („Germanium“) wie 24H2 und 25H2. Entsprechend besteht das Upgrade bloß aus der Installation eines Enablement-Packages.

Die Diskrepanz zwischen einer ambitionierten Roadmap und einem relativ mageren Release 26H2 erklärt sich durch Microsofts Konzept der kontinuierlichen Innovationen. Es sieht vor, dass alle Releases, die sich einen Service-Branch teilen, die neuen Features gleichermaßen erhalten. Entsprechend hat 26H2 gegenüber seinen Vorgängern nicht viel Neues zu bieten, obwohl seit letztem Jahr insgesamt einige interessante Funktionen hinzugekommen sind.

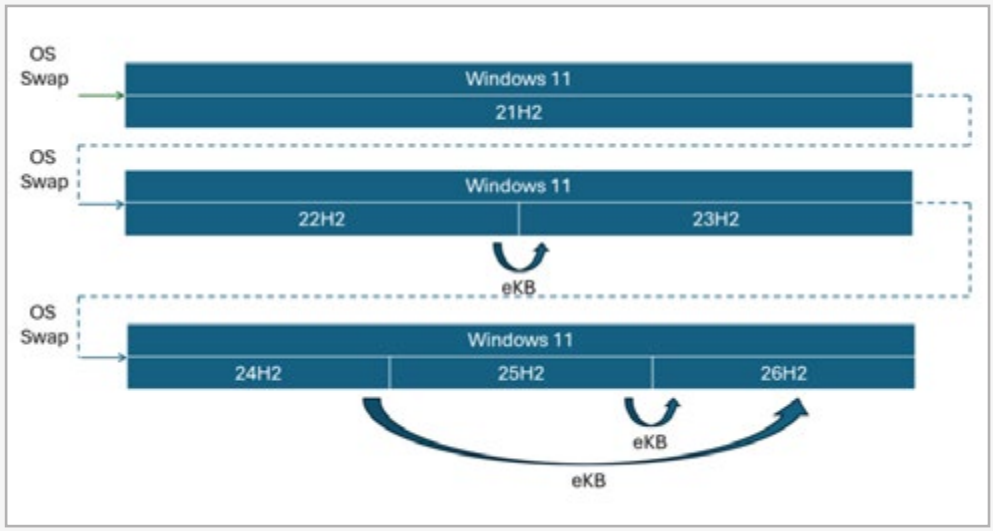


Abb. 1: Die Releases 24H2, 25H2 und 26H2 beruhen auf dem gleichen Service-Branch. Update erfolgen daher via Enablement-Package (eKB).

Während private Nutzer seit dem Erscheinen von 25H2 alle neuen Funktionen nach und nach über die monatlichen Updates erhielten, blieben diese auf verwalteten Geräten standardmäßig deaktiviert. Erst das Enablement-Package (eKB) für 26H2 schaltet diese auf einen Schlag frei, so dass in professionellen Umgebungen der Eindruck eines echten Feature-Releases entsteht.

Unternehmen haben aber die Möglichkeit, die neuen Features bereits bei ihrer Auslieferung per Gruppenrichtlinie oder Intune sofort freizuschalten. Die zuständige Einstellung heißt Aktivieren von Funktionen, die über die Wartung eingeführt wurden und standardmäßig deaktiviert sind („Enable features introduced via servicing that are off by default“).

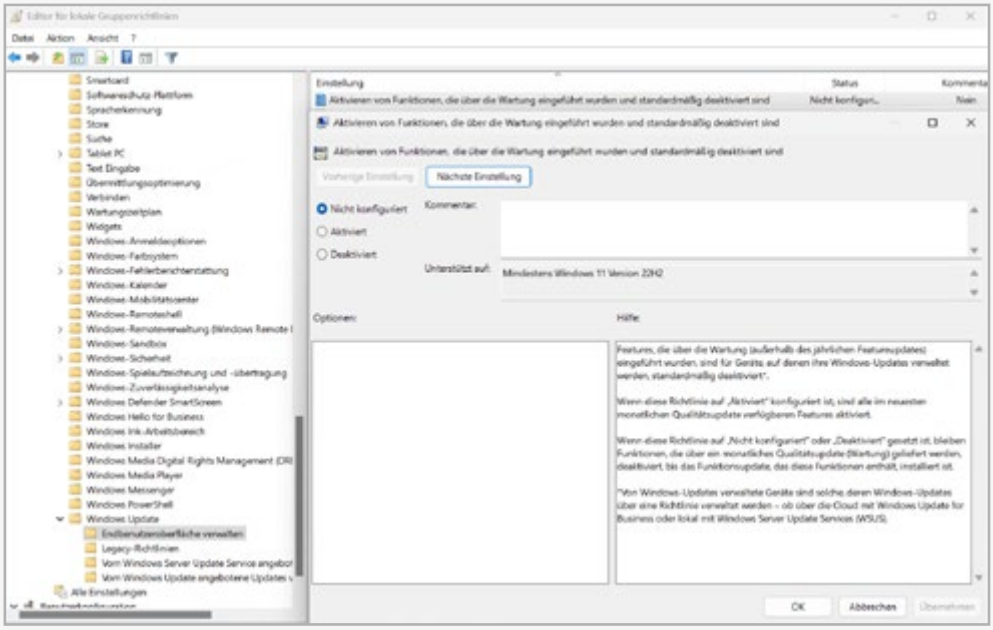


Abb. 2: Neue Features lassen sich in verwalteten Umgebungen bereits vorab freischalten.

Darüber hinaus setzt das eKB die interne Versionsnummer des OS auf 26300 hoch und startet den Support-Zeitraum neu. Die Editionen Home, Pro, Pro Education und Pro for Workstations werden ab dann wie gewohnt 24 Monate, Enterprise und Education 36 Monate unterstützt.

1.1 INNOVATIONEN AUF DER ALTEN PLATTFORM

Die im März ausgerufene Qualitätsoffensive lässt sich zu einem gewissen Grad auch ohne Upgrade des Kernsystems umsetzen, welches erst wieder mit 27H2 ansteht. Ein wesentliches Versprechen Microsofts bestand etwa darin, das System von den zahlreichen (unerwünschten) Zugaben zu entrümpeln oder den Benutzern bei der Installation von Updates mehr Flexibilität zuzugestehen.

Weniger klar ist, wie weit die Optimierung des Speicherverbrauchs ohne Update des Kernels gehen kann. Aber selbst in dieser Hinsicht reklamiert Microsoft bereits Fortschritte auf Basis der aktuellen Plattform.

Bei solchen tieferen Eingriffen in das System legt sich der Hersteller in der Regel jedoch nicht auf die Verfügbarkeit in einem bestimmten Release fest. Aktuell sind einige solcher Neuerungen in der Pipeline, die es wahrscheinlich nicht in die 26H2 GA schaffen. Dazu zählen etwa die Admin Protection oder IAKerb. Ob Anwender diese noch über ein Update für 26H2 erhalten oder dafür auf 27H2 warten müssen, bleibt derzeit noch offen.

Einige der über die letzten Monate vorgestellten Neuerungen betreffen indes nicht das Betriebs-system selbst, sondern Microsofts Service-Infrastruktur insgesamt. Dazu zählen neue Backup- und Wiederherstellungsoptionen in der Cloud oder Rollbacks beim Update fehlerhafter Treiber.

1.2 UNKOMPLIZIERTES UPGRADE

Aus der Sicht von Admins hat die Beibehaltung des 24H2- und 25H2-Branches für 26H2 einige Vorteile. Das Upgrade per eKB ist weit weniger aufwändig als ein klassisches Wipe and Load. Ein solches ist für 26H2 nur fällig, wenn auf Rechnern noch Windows 11 23H2 Enterprise läuft. Dessen Support endet am 10. November 2026.

Aufgrund des einheitlichen Basissystems sind zudem kaum Kompatibilitätsprobleme mit vorhandenen Anwendungen zu erwarten, so dass entsprechende Tests kürzer ausfallen oder sich eventuell auf kritische Apps beschränken können.

1.3 INKONSISTENZEN ZWISCHEN ARM UND INTEL

Das im Februar dieses Jahres veröffentlichte reine OEM-Release 26H1 für ARM erhält dagegen kein Upgrade auf 26H2. Es beruht nämlich schon auf einer neueren Codebasis („Bromine“) als 26H2 („Germanium“).

Benutzer eines ARM-Rechners müssen sich mithin bis zum nächsten Jahr gedulden, um ein neues OS-Release zu erhalten. Sie bleiben damit entweder auf 24H2 oder 25H2, sofern sie nicht kürzlich ein Gerät mit 26H1 erworben haben.

Mit 27H2 wird Microsoft dann alle Architekturen auf der Bromine-Plattform zusammenführen. Dabei handelt es sich wohl um das System, auf das sich verschiedene Gerüchte immer wieder als Windows 12 beziehen.

02 ROADMAP: OS SOLL ENTRÜMPELT WERDEN

Im März 2026 reagierte Microsoft auf die zunehmende Kritik der Kunden an der Überfrachtung von Windows 11 mit unerwünschten Apps und Widgets oder dem allgegenwärtigen Copilot. Der Unmut der Anwender gilt zudem den ständigen Qualitätsmängeln des Betriebssystems und fehlerhaften Updates.

Die von Microsoft in das System gepackte Crapware ist im professionellen Einsatz nicht nur lästig, sondern stellt im Fall von Copilot dort auch ein Datenschutzproblem dar. Ein unübersehbarer Indikator für diese Fehlentwicklung ist das Entstehen mehrerer Tools, mit denen man Windows 11 von unnötigen Funktionen befreien und die Privatsphäre schützen kann. Dazu gehören etwa Winslop, Remove Windows AI, Winhance oder ShutUp10.

2.1 RÜCKZUG VON COPILOT

Für Ärger sorgte vor allem auch die wahllose Integration von Copilot an allen möglichen Ecken und Enden des Betriebssystems. Als Reaktion darauf entfernte Microsoft das AI-Tool bereits aus Apps wie dem Snipping Tool, Photos, Widgets und Notepad. Stattdessen möchte der Hersteller die AI-Funktionen planvoller in das OS integrieren.

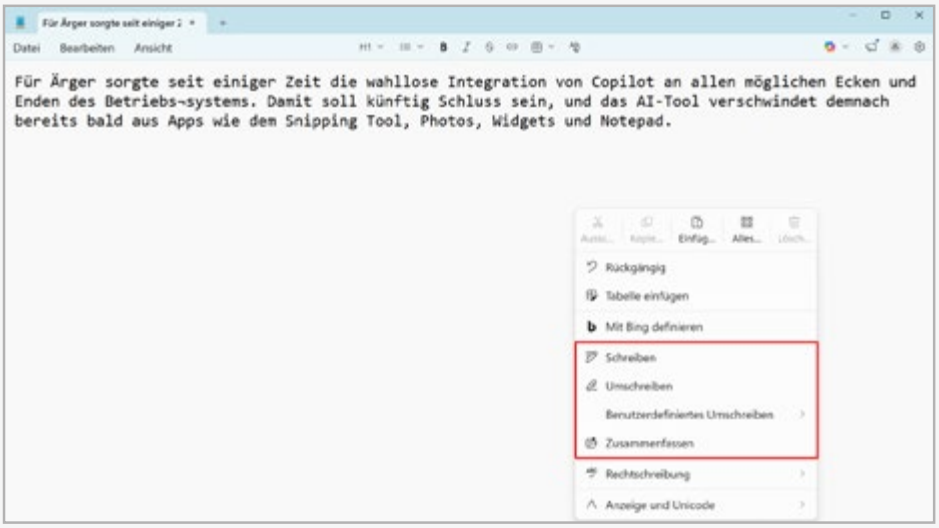


Abb. 3: Microsoft hat die Copilot-Funktionen wieder aus Notepad und anderen Apps entfernt.

2.2 STRAFFERES OOBE

Die lange Kaskade an Dialogen bei der ersten Anmeldung eines Benutzer nach der Windows-Installation bietet ebenfalls Potenzial zur Verschlankung. Microsoft nutzt diesen Prozess unter anderem für Produktwerbung, beispielsweise um den Anwendern ein Office-Abo anzudienen.

Äußerungen von Microsofts Scott Hanselmann auf Social Media zufolge steht dort auch der Zwang zur Anmeldung mit einem Microsoft-Konto auf der Kippe und das Aufdrängen des Edge-Browsers als Standard soll auch ein Ende finden.

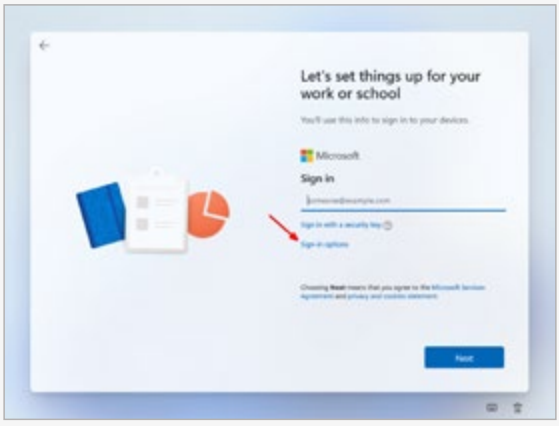


Abb. 4: Der Zwang zur Anmeldung mit einem Microsoft-Konto während der OOBE-Phase steht wohl zur Disposition.

03 HOHE RAM-PREISE ERZWINGEN OPTIMIERUNG

Der AI-Boom treibt die Speicherpreise in die Höhe, was die Anschaffung neuer Rechner erheblich verteuert. Das gilt besonders für Windows-PCs, die für ein zügiges Arbeiten typischerweise 16 GB Speicher benötigen, bei Copilot+ PCs werden diese sogar ausdrücklich verlangt.

Seit 2024 haben sich aber nicht nur die RAM-Preise vervielfacht, sondern auch andere PC-Komponenten wie SSDs oder CPUs sind deutlich teurer geworden. In dieser Situation erweist sich ein Ressourcen-hungriges OS als Hemmschuh für PC-Verkäufe.

3.1 MACS ODER WINDOWS 10 ALS ALTERNATIVE

Anwender können in dieser Situation einen Wechsel zu Apple in Betracht ziehen, das alltagstaugliche Notebooks bereits mit 8 GB anbietet. Wahrscheinlicher ist indes, dass vorhandene Rechner mit Windows 10 einfacher länger laufen werden.

Dieses OS begnügt sich mit deutlich weniger Hardware und kann durch den Bezug von ESUs weiterhin sicher betrieben werden. Dies ist besonders für private Nutzer interessant, die Updates bis zum 12. Oktober 2027 kostenlos erhalten können, wenn sie sich mit einem Microsoft-Konto am PC anmelden.

Da eine Entspannung bei den PC-Preisen nicht in Sicht ist und Microsoft die Migration auf Windows 11 vorantreiben möchte, sieht sich der Hersteller nun gezwungen, in überfällige Maßnahmen zur Qualitätsverbesserung des OS zu investieren. Microsoft arbeitet über die Version 26H2 hinaus daran, den Speicherverbrauch von Windows 11 zu senken und die UI durch nativen Code zu beschleunigen.

3.2 MINIMALE SYSTEMANFORDERUNGEN NICHT PRAXISTAUGLICH

Offiziell beträgt Microsofts minimale Speicheranforderung für Windows 11 nur 4 GB. Ein praxistaugliches Gerät erhält man damit garantiert nicht, eine solche RAM-Ausstattung reicht nur für die bloße OS-Installation. Aber selbst 8 GB genügen nur für einfache Anwendungen, weil das OS hier beim Start schon gut die Hälfte des RAM in Beschlag nimmt. Dies lässt sich mit RamMap relativ einfach zeigen.

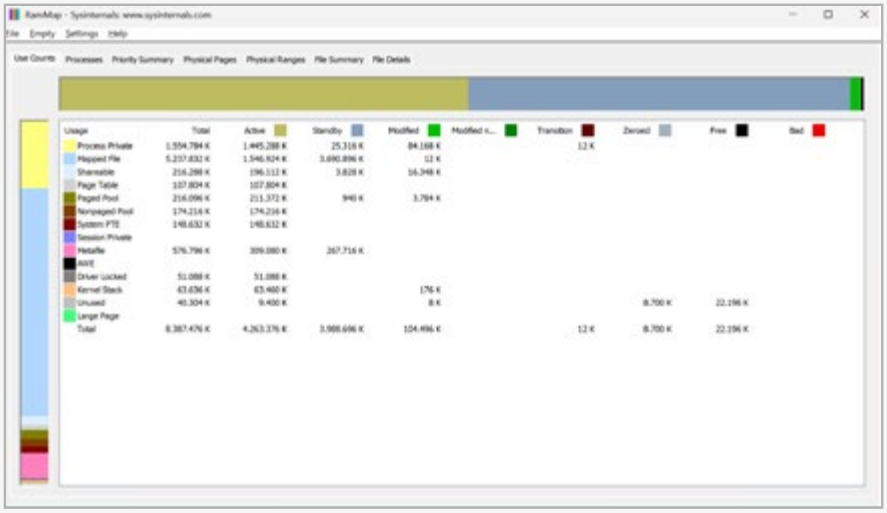


Abb. 5: Auf einem System mit 8 GB belegt das OS laut RamMap nach dem Start ungefähr die Hälfte des Speichers.

Der hohe RAM-Bedarf von Windows 11 ist vor allem drei Faktoren geschuldet:

- Nutzung von Webview2 für verschiedene Systemkomponenten und Apps: Es handelt sich dabei um eine Browser-basierte Laufzeitumgebung, die zumeist pro Anwendung eine eigene Prozessgruppe erzeugt. Selbst eine relativ triviale Anwendung wie die Wetter-App konsumiert deswegen gleich beim Start schon ein halbes GB RAM.
- Webview2-Anwendungen starten relativ langsam, weil sie erst die ganze Web-Infrastruktur hochfahren müssen. Daher greift Microsoft zum Preloading, um den Start zu beschleunigen. Der Code wird also schon in den Speicher geladen, bevor User die betreffende App oder Komponente überhaupt brauchen. Wie man sich leicht überzeugen kann, gilt das etwa für den Teams-Client oder den SearchHost.
- Bei einer Ausstattung ab 8 GB aktiviert Microsoft automatisch Memory Integrity, ein Feature, das zur Virtualization-based Security (VBS) gehört. Dafür startet Windows den Hypervisor und richtet eine isolierte VBS-Umgebung ein.

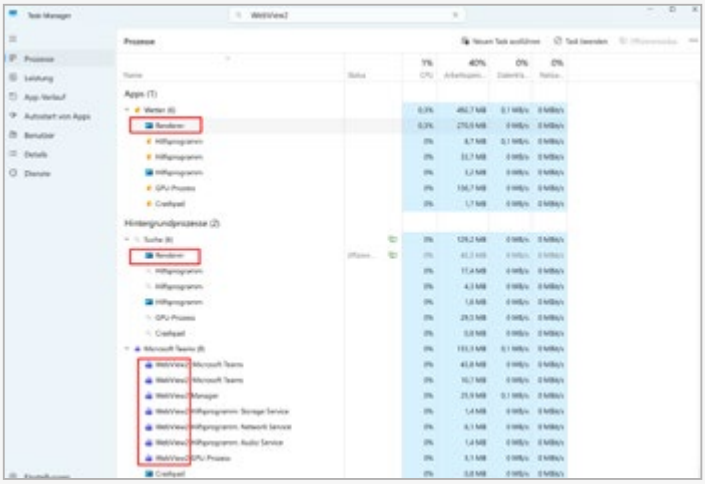


Abb. 6: Mehrere schwerfällige Web-Apps lädt Microsoft gleich beim Systemstart in den Speicher.

3.3 GEPLANTE VERBESSERUNGEN

In der am 31. Juli 2026 veröffentlichten Zwischenbilanz betont Pavan Davuluri, dass die Entwickler bei der Speicherverwaltung des OS bereits Fortschritte gemacht hätten.

3.3.1 Native GUI-Entwicklung

Eine wesentliche Rolle spielt dabei der Wechsel zu einem nativen Programmiermodell für die Benutzeroberfläche, wo künftig WinUI 3 die Webview2-Komponenten ersetzen soll. Microsoft empfiehlt auch Drittanbietern, diesem Beispiel zu folgen.

Die bis vor nicht allzu langer Zeit gehypten Progressive Web Apps und Desktop-Anwendungen auf Basis von WebView2/React verlieren damit an Bedeutung. Im Fall von Teams oder dem neuen Outlook wird Microsoft diese Design-Entscheidung aber nicht mehr rückgängig machen können.

In aktuellen Insider Previews sind Teile der Shell, etwa die Dialoge für Datei- und Verzeichniseigenschaften, die Widgets oder die Ausführen-Box bereits neu in WinUI 3 implementiert. Letzteres wurde zudem in puncto Speicherverbrauch überarbeitet.

3.3.2 Besseres Antwortverhalten

Explizit formuliertes Ziel ist es nun, Windows 11 für PCs ab 8 GB RAM zu optimieren und das System reaktionsschneller zu gestalten. Das kommt nicht bloß durch den geringeren Speicherverbrauch zustande, sondern liegt natürlich auch an der besseren Performance von nativem Code.

Auch wenn es bei einer Ausstattung mit 8 GB zu Engpässen kommen kann, soll sich das System subjektiv für die Benutzer trotzdem schneller anfühlen. Aus diesem Grund ist auch der Explorer Gegenstand von Performance-Maßnahmen mittels WinUI-3-Refectoring.

Eine weitere Rolle spielt dabei das so genannte ***Windows 11 CPU Boost*** (auch „Low Latency Profile“). Dabei fordert das OS bei kurzen interaktiven Aktionen wie dem Öffnen von Startmenü oder Ordnern für einige Sekunden eine höhere CPU-Leistungsstufe an. Seit dem August-Update greift dieses Feature auch beim Starten von Anwendungen.

3.4 SURFACE-MODELLE WIEDER MIT 8-GB RAM

Microsoft ist vom Erfolg seiner Maßnahmen zur Reduktion des RAM-Verbrauchs offenbar überzeugt. Der Hersteller brachte nämlich für Surface 13 und Surface Pro 12 wieder 8-GB-Konfigurationen auf den Markt, obwohl diese Modelle ursprünglich mit mindestens 16 GB angeboten wurden.

Erste Tests noch vor der Verfügbarkeit des optimierten OS bestätigen jedoch die Erfahrung der meisten Benutzer, dass 8 GB RAM für Windows 11 aktuell noch nicht reichen. Auch hier zeigte sich, dass das OS nach dem Start bereits die Hälfte des Arbeitsspeichers belegt und dass mehrere offene Apps wegen des Speicherdrucks zu regelmäßigen Hängern führen.

04 ÜBERARBEITETES BENUTZER-INTERFACE

Ein wesentliches Ziel bei der Generalüberholung der Windows-Oberfläche besteht in der Reduktion des Ressourcenverbrauchs und in einem besseren Ansprechverhalten des Explorers. Dies soll Windows 11 auch auf Rechnern mit weniger RAM-Ausstattung vernünftig nutzbar machen.

Im August 2026 brachte KB5120998 indes vor allem UI-Neuerungen, die den Benutzern mehr Flexibilität bei der Gestaltung von Elementen wie Startmenü, Taskleiste oder der Suche geben.

4.1 FLEXIBLE POSITIONIERUNG DER TASKBAR

Viel Aufhebens macht Microsoft schon länger um die freie Positionierung der Taskleiste an den Bildschirmrändern. Dieses Feature stand wohl bei vielen Benutzern auf der Wunschliste, weil bereits Windows 10 in der Lage war, die Taskbar an jeder Seite des Bildschirms anzuzeigen. Das Vorgänger-OS erlaubte die Positionierung per Drag & Drop und bot eine Option zu ihrer Fixierung, um ein versehentliches Verschieben zu vermeiden.

KB5120998 hingegen ergänzte die App ***Einstellungen*** um einen Abschnitt, in dem man eine der vier möglichen Positionen und die Größe der Taskleiste festlegen kann. Dieser findet sich unter *Personalisierung => Taskleiste*.

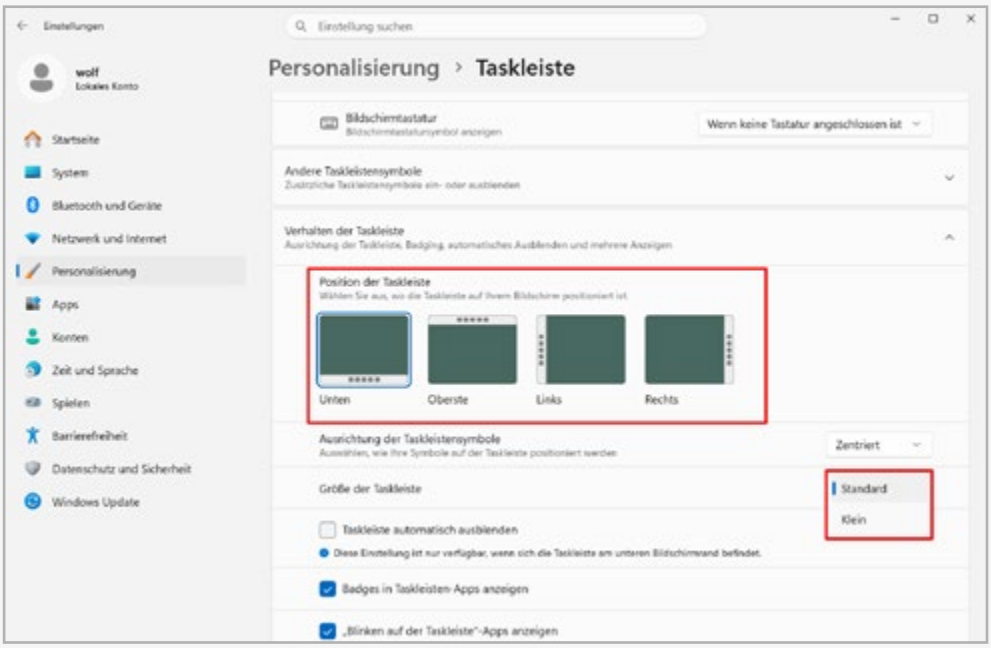


Abb. 7: Optionen zur Positionierung und Größenänderung der Taskleiste.

4.2 KOMPAKTES STARTMENÜ

Beim Startmenü beschränkt sich die neue Einstellung, die man unter *Personalisierung => Start* findet, auf die Auswahl zwischen einer großen und einer kleinen Darstellung. Dies bezieht sich nicht auf die Dimensionen der Symbole oder Schrift, sondern bestimmt, wie viele Abschnitte eingeblendet werden.

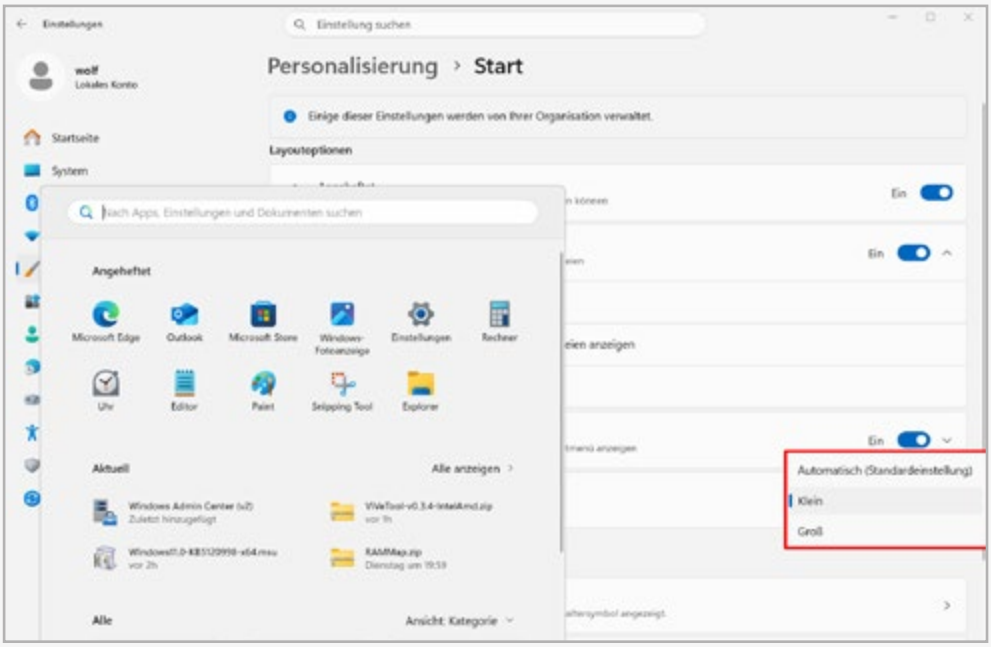


Abb. 8: Das kleine Startmenü ist wesentlich kompakter als die Standardansicht.

4.3 DESKTOP-SUCHE OHNE WEB-ERGEBNISSE

Das Einblenden von Ergebnissen der Web-Suche gehört zu den zahlreichen Zwangsbeglückungen, mit denen Microsoft seine Marktposition nutzt, um weitere Dienste und Anwendungen unter die Leute zu bringen. In der Regel will man aber keine Ergebnisse aus dem Web, wenn man etwas auf seinem Rechner sucht.

Für verwaltete Umgebungen gibt es schon länger eine Gruppenrichtlinie, mit der man Bing zum Schweigen bringen kann. Endbenutzer hatten bis dato aber keine Möglichkeit, dieses Verhalten interaktiv zu ändern.

Die App *Einstellungen* erhält nun eine solche Option unter *Datenschutz und Sicherheit => Suche*. Hier kann man für jede einzelne App, die für die Windows-Suche registriert wurde, festlegen, ob sie aktiv sein soll. Standardmäßig ist hier nur Bing vertreten.

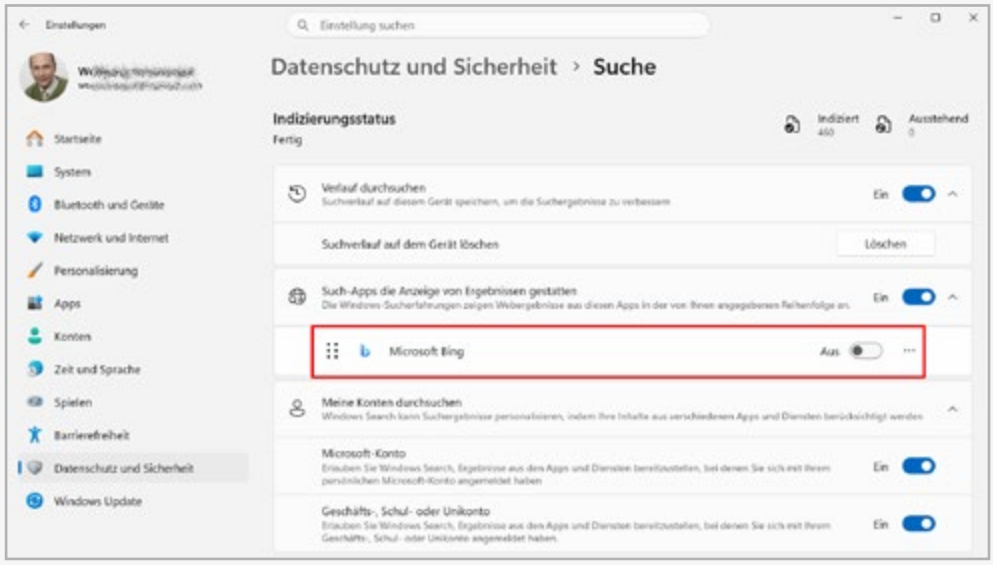


Abb. 9: Endbenutzer können nun die Ergebnisse aus der Web-Suche über die GUI deaktivieren.

Im Juli brachte schon KB5101684 weitere Verbesserungen für die Suche in Windows 11. So findet sie nun mit Hilfe einer unscharfen Suche die gewünschten Ergebnisse auch dann, wenn der Suchbegriff Tippfehler enthält.

Bereits zuvor befähigte Microsoft die Suche endlich dazu, Dateien zu finden, deren Name nicht mit dem Suchbegriff beginnt, sondern diesen an anderer Position enthält (Search by Substring). Dateien beispielsweise mit den Namen *MeetingNotesApril.docx* oder *ProjectStatusReport.pptx* lassen sich so auch durch die Eingabe von „April" oder „Status" finden.

4.4 WEITERE GUI-VERBESSERUNGEN

Die Release Notes für KB5120998 zählen noch einige zusätzliche Verbesserungen für das Benutzererlebnis auf. Dazu gehören:

- Der Explorer startet schneller und bietet ein besseres Antwortverhalten
- Microsoft vereinheitlicht die Fortschrittsanzeige mit einem neuen Design
- Schnelleres Umschalten zwischen virtuellen Desktops

05 ÄNDERUNGEN BEI UPDATES

Jeder Windows-User kennt die Situation, in der das Betriebssystem zur Unzeit ein Update einspielt. Ewige Wartezeiten beim Herunterfahren des Notebooks nerven besonders dann, wenn man in Eile aufbrechen möchte. Meist unwillkommen ist ein Neustart selbst über Nacht, wenn man mehrere Anwendungen geöffnet hat, um am nächsten Tag noch schnell ein Projekt fertigzustellen.

Dieses Verhalten kommt allerdings nicht von ungefähr, sondern resultiert aus Microsofts Versuch, eine Balance zwischen Benutzerkomfort und Sicherheit zu finden. Über die Jahre verfolgte der Hersteller dabei mehrere Ansätze.

Dazu zählt etwa, dass man einen Reboot vermeiden konnte, solange ein Benutzer angemeldet ist. Neuerdings bestimmen die „Active Hours", dass ein Neustart auf Zeiten verlegt wird, in denen der User das Gerät üblicherweise nicht verwendet.

5.1 KOMFORT ZU LASTEN DER SICHERHEIT?

Insgesamt schlug das Pendel in den letzten Jahren jedoch zunehmend in Richtung Sicherheit aus. Dies zeigt sich auch bei der mit Windows 10 eingeführten Gruppenrichtlinie „Stichtage für automatische Updates und Neustarts angeben", die den Countdown für die Installation von Updates bereits bei deren Erscheinen startet.

Das neue Update-Verhalten stellt in dieser Hinsicht einen radikalen Kurswechsel dar. Es erlaubt Anwendern, praktisch nach Belieben Patches zu installieren.

5.2 UPDATES WÄHREND OOBE ÜBERSPRINGEN

Dies beginnt bereits mit der Möglichkeit, die Suche nach Updates während der OOBE-Phase zu überspringen. Abhängig vom Alter der Installationsmedien startet der User dann mit einem Gerät, das möglicherweise kritische Schwachstellen aufweist.

Windows 11 lädt die Updates somit zu einem späteren Zeitpunkt herunter, wobei der User dann entscheidet, wann ihm die Installation genehm ist.

Nicht betroffen von dieser Änderung sind Computer, die mittels Autopilot und Intune betankt werden. Hier entscheiden nach wie vor Admins, ob Updates während der OOBE-Phase eingespielt werden sollen.

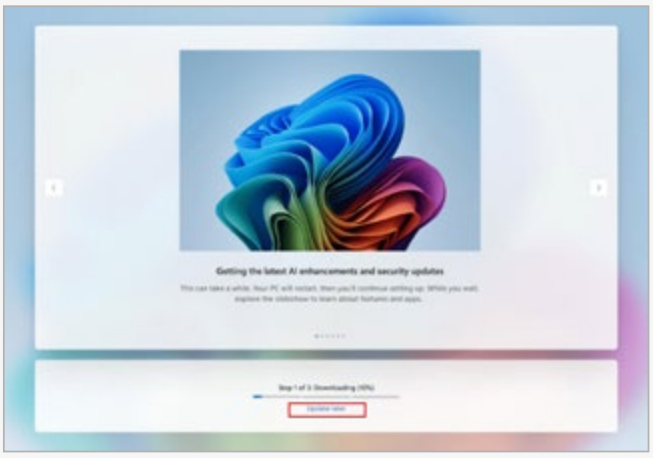


Abb. 10: Wenn Benutzer die OS-Installation schnell abschließen möchten, können sie die Updates überspringen.

5.3 UNBEGRENZTER AUFSCHUB FÜR UPDATES

Bis dato waren die Optionen für das Verzögern von Updates relativ beschränkt. Die App ***Einstellungen*** enthielt einen Button „Für eine Woche anhalten“. Nun findet sich an dieser Stelle ein Kalender-Control, mit dem die Benutzer einen Tag ihrer Wahl für die Update-Installation aussuchen können. Damit sind sie in der Lage, das Update bis zu 35 Tage aufzuschieben, und wenn das nicht reicht, können sie diese Frist verlängern.

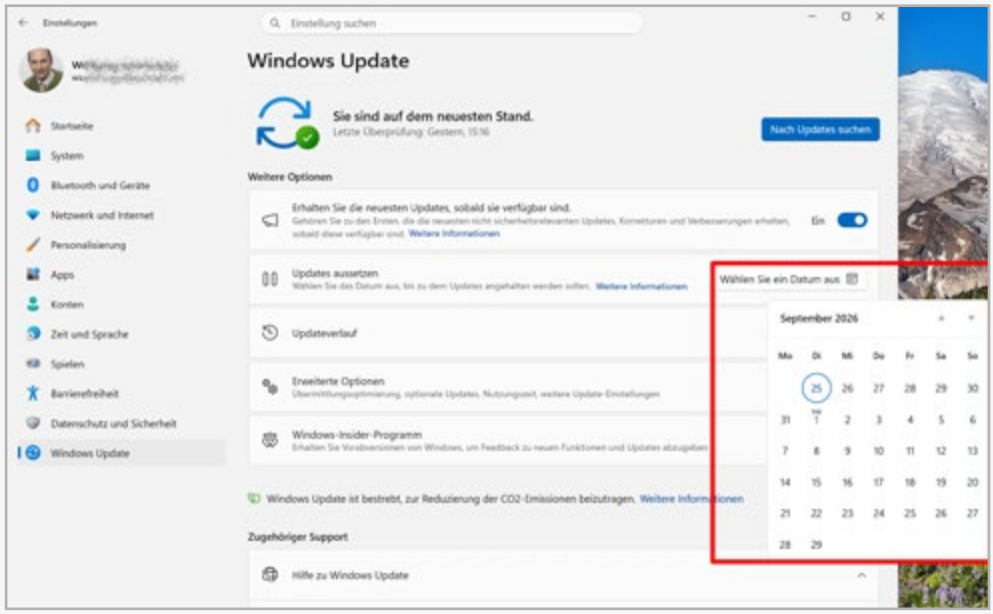


Abb. 11: Die Installation von Updates lässt sich gezielt für einen bestimmten Tag terminieren.

5.4 UMGEHUNG DER INSTALLATION BEIM NEUSTART

Wenn man bisher die Installation von Updates verzögert hat, so konnte man diese spätestens beim Herunterfahren oder Neustart des Rechners nicht mehr verhindern. Das Startmenü enthielt nur noch die Einträge ***Update und Herunterfahren*** bzw. ***Update und neu starten***.

Diese Menüpunkte gibt es zwar auch weiterhin, aber zusätzlich bleiben die Einträge für ***Herunterfahren*** und ***Neu starten*** erhalten. Benutzer können auf diese Weise verhindern, dass diese Aktionen durch eine langwierige Installation von Updates verzögert werden.

5.5 SCHNELLERE INSTALLATION, WENIGER REBOOTS

Security-, .NET- und Firmware-Updates sollen in Zukunft nach und nach im Hintergrund heruntergeladen und dann in einem Durchgang installiert werden. Auf diese Weise wäre nur noch ein Reboot pro Monat erforderlich.

Eine weitere Reduktion der Update-Größen und die daraus resultierende Beschleunigung der Installation soll Benutzer zusätzlich motivieren, das Patchen nicht übermäßig aufzuschieben. Außerdem erhalten Geräte, die nur über einen langsamen Internet-Zugang verfügen, die Updates schneller als bisher.

5.6 NEUE RICHTLINIEN FÜR VERWALTETE GERÄTE

Erwartungsgemäß lieferte Microsoft mit 26H2 eine neue Policy, mit der sich der beliebige Aufschub von Updates unterbinden lässt. Die folgende Einstellung beschränkt die Zahl der Tage, die User im Kalender-Widget auswählen können:

- Maximale Anzahl von Tagen konfigurieren, für die Updates pausiert werden können („Configure the maximum number of days that updates can be paused“)

Die Beschreibung der Richtlinie legt nahe, dass Benutzer den gewährten Zeitraum damit nicht beliebig oft wiederholen können:

„Wenn die Richtlinie konfiguriert ist, können Benutzer Updates nur bis zum Ende des in der Richtlinie angegebenen Zeitraums anhalten. Sobald das konfigurierte Limit erreicht ist, können Benutzer die Pause nicht mehr verlängern.“

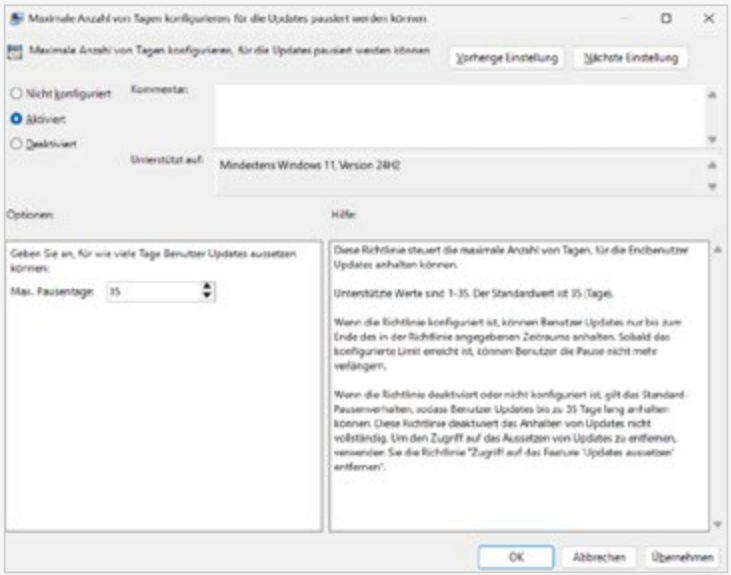


Abb. 12: Der Aufschub von Updates mittels Kalender-Widgets lässt sich per GPO begrenzen.

Will man Benutzern über dieses neue Feature generell keinen Aufschub von Updates einräumen, dann kann man das Widget mit dieser schon länger vorhandenen Einstellung deaktivieren:

- Zugriff auf das Feature „Updates aussetzen“ entfernen (Remove access to „Pause updates“ feature)

Beide Einstellungen finden sich unter *Computerkonfiguration* => *Richtlinien* => *Administrative Vorlagen* => *Windows-Komponenten* => *Windows-Update* => *Endbenutzeroberfläche verwalten.*

5.7 NEUE GRUPPENRICHTLINIE FÜR WARTUNGSFENSTER

Die ADMX-Vorlagen für Windows 11 brachten in der Version 3.0 eine neue Richtlinie, die eine detaillierte Konfiguration der Zeitfenster erlaubt, in denen Updates heruntergeladen und installiert bzw. der Rechner neu gestartet werden darf.

Microsoft positioniert die neue Policy nicht für reguläre PCs, sondern für kritische Geräte, deren Betrieb nur zu eng umrissenen Zeiten unterbrochen werden soll. Das gilt etwa für Rechner in medizinischen Einrichtungen oder in der Produktionssteuerung. Updates für normale PCs sollten über die bisherigen Einstellungen konfiguriert werden.

5.7.1 Richtlinie für Wartungsfenster konfigurieren

Die Einstellung heißt *Wartungsfenster für automatische Updates konfigurieren* („Configure maintenance windows for automatic updates“) und findet sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Windows-Update => Endbenutzeroberfläche verwalten*.

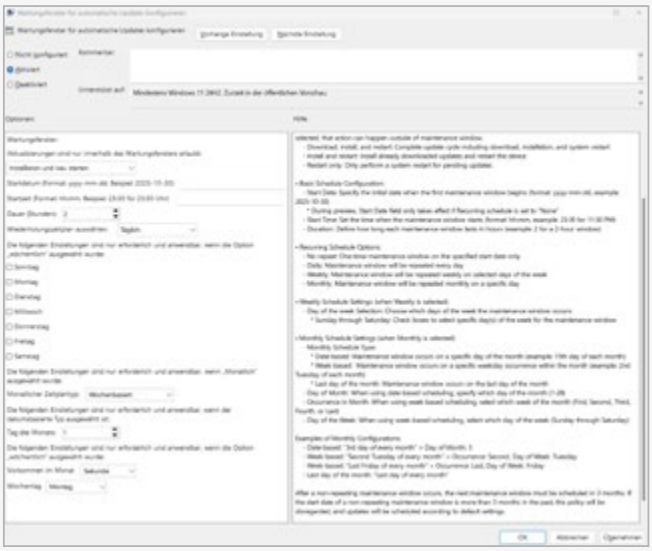


Abb. 13: Neue Einstellung zur Konfiguration von Wartungsfenstern für Windows Update.

5.7.2 Aktionen während eines Wartungsfensters

Für Aktionen, die innerhalb eines Wartungsfensters ausgeführt werden, kann man zwischen diesen Optionen wählen:

1. Herunterladen, installieren und neu starten
2. Installieren und neu starten
3. Nur neu starten

Wie man erkennt, lassen sich für das Herunterladen, Installieren und den Neustart keine jeweils eigenen Wartungsfenster definieren, um beispielsweise die Updates am Dienstagabend herunterzuladen, am Donnerstag zu installieren und den Rechner am Wochenende neu zu starten. Jede Auswahl enthält nämlich bereits alle Aktionen der darunterliegenden.

Will man mit dieser Richtlinie etwa nur den Zeitpunkt für den Reboot konfigurieren, dann kann man komplementär den Download und die Installation wie gewohnt über die Gruppenrichtlinie *Automatische Updates konfigurieren* steuern.

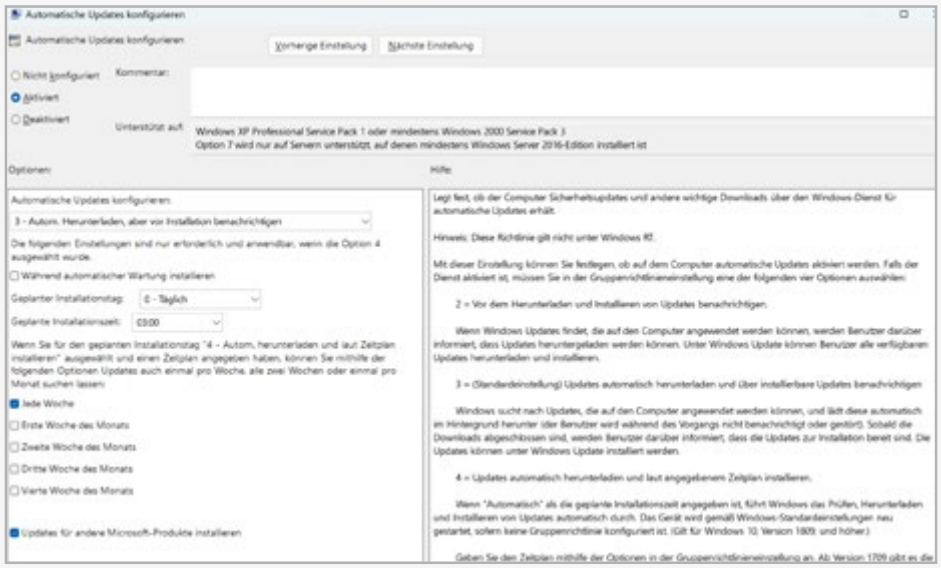


Abb. 14: Die altbekannte Einstellung für automatische Updates steuert ebenfalls den Download und die Installation.

5.7.3 Einmalige vs. wiederkehrende Wartungsfenster

Als Wartungsfenster kann man einen einmaligen oder einen sich wiederholenden Zeitraum angeben. Zur Auswahl stehen:

- Keine Wiederholung
- Täglich
- Wöchentilch
- Monatlich

Entscheidet man sich für keine Wiederholung, dann gilt das Wartungsfenster nur für den Zeitraum, den man über die Felder ***Startdatum***, ***Startzeit*** und ***Dauer*** festgelegt hat. Ist diese Frist verstrichen, dann wird diese Einstellung automatisch ignoriert, wenn sie mehr als drei Monate in der Vergangenheit liegt, und es greifen dann die Standardwerte von Windows Update.

Wählt man als Zeitplan ***wöchentlich***, dann hakt man einen oder mehrere Wochentage an.

Bevorzugt man den monatlichen Rhythmus, dann kann man über ***datumsbasiert*** einen Wert zwischen 1 und 28 nehmen. Ein späteres Datum ist nicht vorgesehen, weil es nicht in allen Monaten existiert. Alternativ wählt man zwischen erster, zweiter, dritter, vierter und letzter Woche (***Sekunde*** und ***Vorherige*** sind falsche Übersetzungen von ***second*** und ***last***) und darin den gewünschten Wochentag.

5.8 DEFEKTE TREIBER ERSETZEN

Das so genannte Cloud-Initiated Driver Recovery soll Probleme durch fehlerhafte Treiber beseitigen. Wenn bei einem Gerätetreiber nach der Verteilung über Windows Update Qualitätsmängel auftreten, dann kann Microsoft einen Rollback veranlassen. Er wird dann durch eine funktionierende Version ersetzt, die sich entweder zuletzt als gut erwiesen hat, oder ein Upgrade, das den fehlerhaften Treiber auf Windows Update ersetzt.

Dieser Mechanismus beschränkt sich allerdings nur auf Treiber, die bei der Evaluierung in Microsofts Shiproom Qualitätsmängel zeigen, und ist kein genereller Fix für mangelhafte Produkte. Der Vorgang selbst erfordert keinen Eingriff von Seiten der Anwender oder der OEMs.

06 NEUE REPARATUR- UND WIEDERHERSTELLUNGSFUNKTIONEN

Microsoft hat zuletzt drei neue Funktionen zur Wiederherstellung des Systems und von Daten vorgestellt. Dazu gehören ***Quick Machine Recovery***, ***Point-in-Time Restore*** und ***Backup für Organisationen***. Sie ergänzen eine ganze Reihe ähnlicher Features, die schon länger an Bord sind.

Eine dysfunktionale Windows-Installation kann verschiedene Ursachen haben. Diese reichen von einem defekten Treiber über fehlerhafte Updates bis zur Fehlkonfiguration durch die Benutzer. Für einige dieser Ursachen enthält Windows Reparaturprogramme, die aber oft erfolglos sind. Wenn sich das Problem damit nicht beheben lässt, bleibt nur ein Reset oder die Neuinstallation.

6.1 WIEDERHERSTELLUNG AUS WINRE

Welche Funktion man nimmt, hängt unter anderem davon ab, ob Windows noch startet. Ist das nicht der Fall, dann ist man auf die Optionen angewiesen, die Windows RE bietet.



Abb. 15: Tools für die Wiederherstellung in der Problembehandlung von WinRE.

Insgesamt kommt man dort auf vier Varianten der Systemwiederherstellung:

- Die neue Zeitpunktwiederherstellung mit einem Rollback auf einen Snapshot
- Zurücksetzen auf einen herkömmlichen Wiederherstellungspunkt („System wiederherstellen" in den erweiterten Optionen)
- Diesen PC zurücksetzen (mit optionaler Beibehaltung der Benutzerdaten)
- Systemimage-Wiederherstellung für den Restore mittels eines Backups

Alle sind mit einem gewissen Datenverlust verbunden. Bei herkömmlichen Wiederherstellungspunkten können Programme, Updates oder Treiber auf der Strecke bleiben, die nach dem Erstellen des Snapshots installiert wurden. Betroffen sind unter Umständen auch Systemeinstellungen.

6.2 POINT-IN-TIME RESTORE AUF EINEN VSS-SNAPSHOT

Point-in-Time Restore („Zeitpunktwiederherstellung“) wirkt sich ähnlich aus wie der Rollback einer VM auf einen Prüfpunkt. Dieses Feature sichert den Zustand des Systems periodisch, standardmäßig alle 24 Stunden. Allerdings gibt es keine Garantie, dass ein Snapshot in den festgelegten Intervallen erstellt wird, etwa wenn ein Rechner stark ausgelastet ist.

Die altbekannten Wiederherstellungspunkte („System Restore Points“) werden dagegen entweder über bestimmte Ereignisse wie das Installieren von Software oder das Ändern der Systemeinstellungen automatisch angelegt. Alternativ kann man sie über die Systemsteuerung manuell erzeugen.

Während die herkömmlichen Wiederherstellungspunkte erhalten bleiben, bis der VSS-Speicher erschöpft ist, werden die Point-in-Time Restore Points per Voreinstellung nach 72 Stunden automatisch verworfen. Aber auch hier führt Speichermangel zum vorzeitigen Löschen von Restore Points.

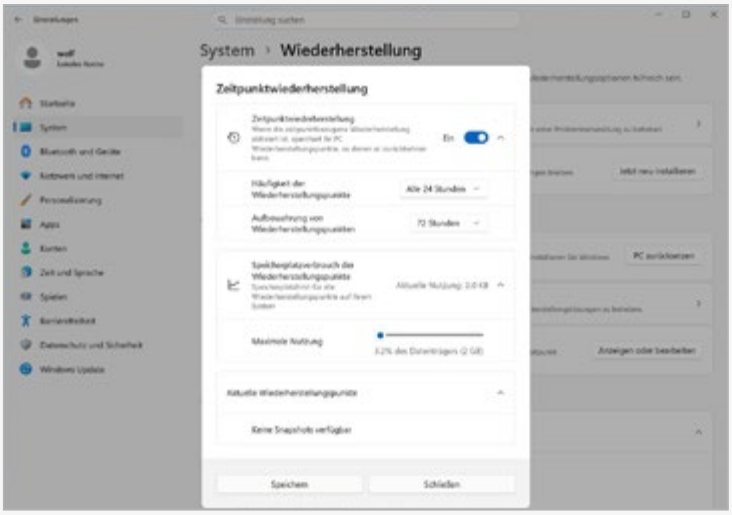


Abb. 16: Optionen für Point-in-Time Restore in der App Einstellungen.

Der wichtigste Unterschied gegenüber den bisherigen Wiederherstellungspunkten besteht darin, dass die Zeitpunktwiederherstellung eine Momentaufnahme des gesamten Systems erstellt. Dazu gehören auch die Benutzerdaten inklusive Einstellungen, Passwörtern, Zertifikaten oder Passkeys.

Die Sicherung ist jedoch auf das Systemlaufwerk beschränkt, so dass Benutzerdateien nicht enthalten sind, wenn sie etwa auf einem File-Share oder auf OneDrive liegen.

6.2.1 Aktivierung und Verwaltung

Im Unterschied zu den alten Wiederherstellungspunkten wird Point-in-Time Restore nicht über die Systemsteuerung, sondern über die App Einstellungen unter ***System => Wiederherstellung*** verwaltet.

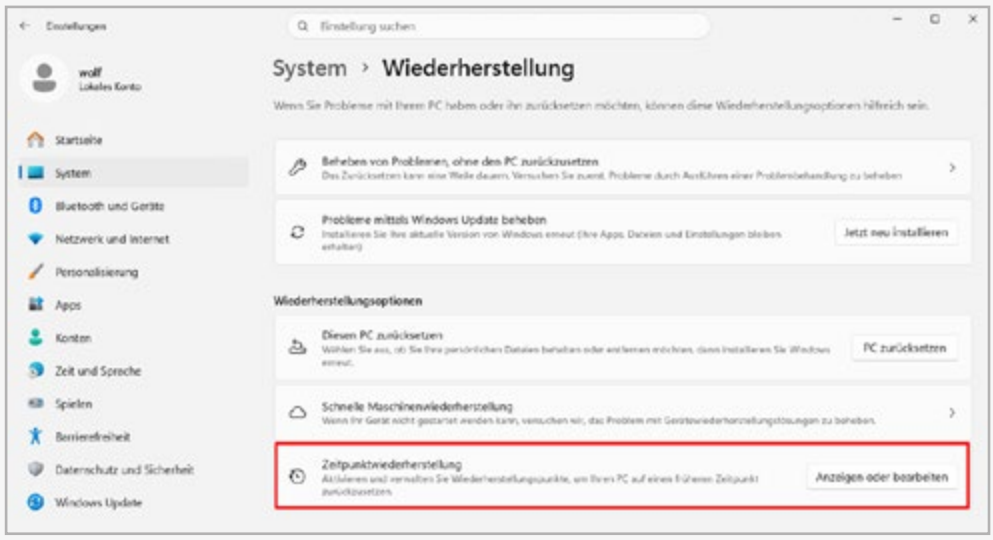


Abb. 17: Verwaltung von Point-in-Time Restore in der App Einstellungen.

Auf Rechnern mit einem Laufwerk mit mehr als 200 GB Speicher ist das Feature automatisch aktiviert, bei kleineren Disks kann man es hier manuell einschalten. Dort konfiguriert man außerdem das Intervall für das Anlegen von Wiederherstellungspunkten, ihre Aufbewahrungsfristen und den maximal dafür verfügbaren Speicherplatz.

Während man die herkömmlichen Wiederherstellungspunkte mittels Gruppenrichtlinien deaktivieren oder deren Konfiguration unterbinden kann, existiert diese Option für Point-in-Time Restore (derzeit noch) nicht. Das Gleiche gilt für das Management via PowerShell.

Allerdings können die Snapshots wie bei den alten Wiederherstellungspunkten mittels vssadmin verwaltet werden. Sie lassen sich damit zum Beispiel anzeigen oder löschen.

Zu einem späteren Zeitpunkt möchte Microsoft noch das Remote-Management von Point-in-Time Restore ergänzen. Aktuell ist die Wiederherstellung zudem noch auf WinRE beschränkt.

6.3 SYSTEM ÜBER CLOUD REBUILD WIEDERHERSTELLEN

Die Insider Preview 26300.8772 brachte eine weitere Option für das Wiederherstellen des Betriebssystems, wobei das Installationsmedium aus der Cloud heruntergeladen wird. Das Feature ist aktuell noch in Preview. Eine ähnliche Möglichkeit bietet bereits „Diesen PC zurücksetzen“ mit dem Cloud-Download.

Das neue Verfahren geht jedoch weiter und erlaubt ein vollständiges Re-Imaging aus der Cloud, das durch Autopilot, Backup for Organizations (neuerdings „Windows settings backup and restore“) und Intune ergänzt wird. Aktuell lässt sich die Cloudwiederherstellung nur aus WinRE starten, es erhielt dort unter ***Problembehandlung*** einen eigenen Eintrag.



Abb. 18: Eintrag für Cloud Rebuild in der Problembehandlung von Windows RE.

Klickt man auf diese Kachel, dann erhält man im nächsten Dialog einen Überblick über die Details der bevorstehenden Neuinstallation (Version, Edition, Sprache).

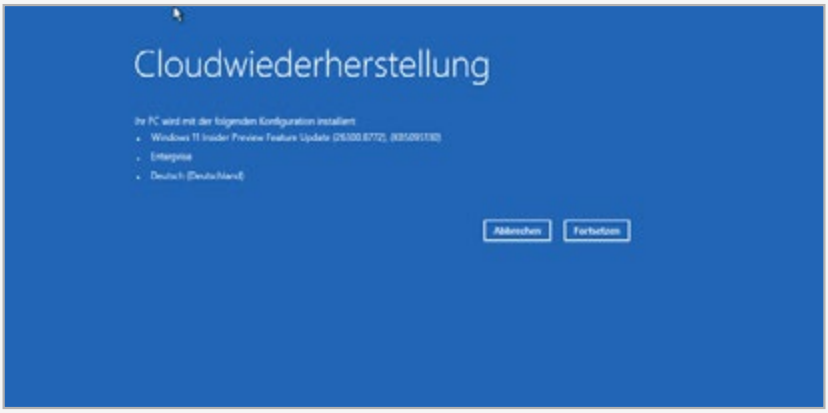


Abb. 19: Details zur geplanten Neuinstallation von Windows.

Fährt man fort, dann erhält man eine Warnung vor Datenverlusten, denn Cloud Rebuild löscht alle lokal gespeicherten Konten, Dateien und Einstellungen. Darüber hinaus gehen alle installierten Programme verloren, weil dieses Feature das Systemlaufwerk formatiert und Windows von den heruntergeladenen Medien neu installiert und dabei auch alle Treiber aus dem Netz bezieht.



Abb. 20: Die Cloudwiederherstellung klärt die Benutzer über die Folgen der bevorstehenden Aktion auf.

6.3.1 Voraussetzungen

Es liegt auf der Hand, dass die ***Cloudwiederherstellung*** nur klappt, wenn sich der Rechner in ein funktionstüchtiges WinRE booten lässt. Dieses muss zudem in der Lage sein, eine Netzwerkverbindung aufzubauen, sei es über LAN oder WiFi.

Das Gerät muss natürlich auch die minimalen Hardware-Anforderungen für Windows 11 erfüllen, so dass etwa ausreichend Platz für Re-Imaging vorhanden ist. Klar ist zudem, dass man den Rechner während der Neuinstallation nicht

6.3.2 Fehlender Baustein für Re-Imaging aus der Cloud

Grundsätzlich verfügt Microsoft über eine ganze Kette an Tools, die alle Schritte vom Entra-ID-Join über die Installation der Software bis hin zur Wiederherstellung der Benutzereinstellungen abdecken. Bis dato fehlte jedoch noch eine Option für eine Bare-Metal-Installation des OS.

Die Funktion „Diesen PC zurücksetzen" erlaubt zwar auch das erneute Aufsetzen des Betriebssystems auf Basis eines Cloud-Downloads. Sie richtet Windows aber auf dem bestehenden Systemlaufwerk ein und behält die lokal vorhandenen Treiber bei. In hartnäckigen Fällen könnte das nicht ausreichen.



Abb. 21: Auch das Zurücksetzen des PCs bietet die Möglichkeit, die Installationsdateien aus der Cloud zu laden.

Auf einem nicht verwalteten PC bootet Windows in die OOBE, und die Benutzer müssen alle Apps und Einstellungen manuell nachziehen.

6.3.3 Konfiguration über Autopilot und Intune

Über die Cloud verwaltete Rechner lesen während der OOBE-Phase dagegen das Autopilot-Profil ein, welches für den Beitritt zu Entra ID sorgt und das Gerät bei Intune registriert. Letzteres ordnet dem Client dann die vorgesehenen Richtlinien zu und installiert die zugewiesenen Apps.

Zu diesem Zeitpunkt hat der User auch wieder Zugang zu OneDrive, von dem Microsoft annimmt, dass alle Benutzerdateien dort gespeichert wurden. Schließlich müssen noch die benutzerspezifischen Einstellungen restauriert werden.

6.4 WIEDERHERSTELLUNG VON BENUTZEREINSTELLUNGEN

Ein neu hinzugekommenes Feature, das aufgrund seines ursprünglichen Namens falsche Erwartungen erweckte, ist Backup für Organisationen. Dieses heißt mittlerweile ***Sicherung und Wiederherstellung von Windows-Einstellungen*** („Windows settings backup and restore“). Es kümmert sich nur um die Migration von Benutzereinstellungen auf einen neuen oder neu installierten Rechner während der OOBE-Phase und setzt voraus, dass dieser Mitglied in Entra ID ist.

Seit Mai 2026 führt Microsoft die Verwaltung von Backup für Organisationen und von Enterprise State Roaming (ESR) zusammen. Dies bedeutet eigentlich nur, dass man ESR seit dem 1. Juli nicht mehr über das Entra Admin Center, sondern ebenfalls nur noch per GPO oder Intune-Richtlinie verwalten kann. Dieses Feature synchronisiert die Benutzereinstellungen zwischen mehreren Geräten.

Die Sicherung der Benutzereinstellungen ist in Windows 11 26H2 per Voreinstellung aktiviert und speichert die benutzerspezifischen Anpassungen standardmäßig alle acht Tage. In der EU müssen Admins das Backup aufgrund des Digital Markets Act jedoch selbst aktivieren, hier verzichtet Microsoft auf die automatische Ausführung.

Dies lässt sich über Intune oder die ***Gruppenrichtlinie Windows-Sicherung aktivieren*** („Enable Windows Backup“) bewerkstelligen. Sie befindet sich wie alle anderen Richtlinien für dieses Backup-Feature unter ***Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Einstellungen synchronisieren***.

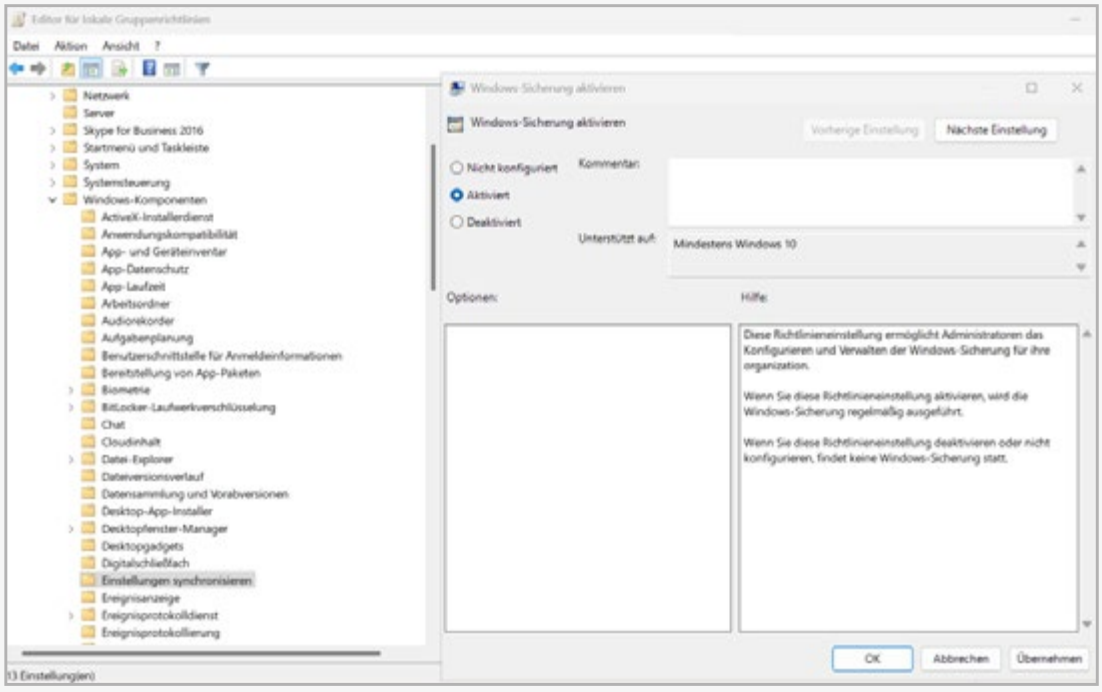


Abb. 22: Windows-Backup für Organisationen lässt sich per GPO aktivieren.

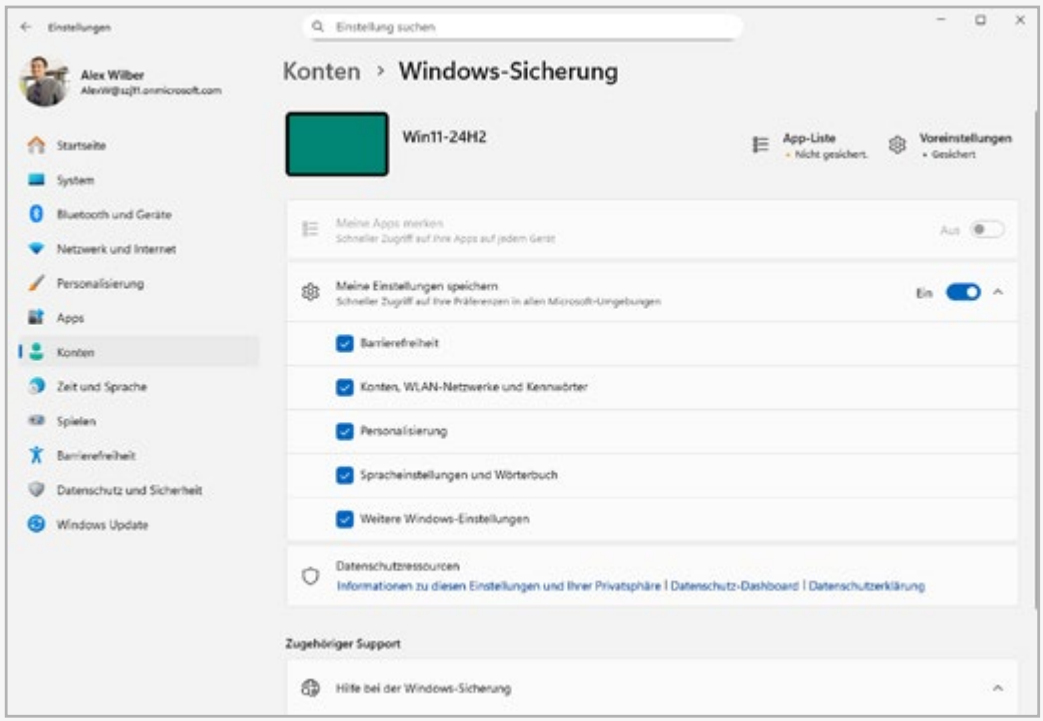


Abb. 23: Wird das Backup vom Admin bloß aktiviert, dann können User bestimmen, ob und welche Daten gesichert werden.

Alternativ können Admins über Gruppenrichtlinien oder Intune granular steuern, was gesichert werden soll. In der App *Einstellungen* sind die entsprechenden Optionen dann ausgegraut.

07 NEU: GNU COREUTILS, ADMIN PROTECTION, WSL-CONTAINER

Microsoft hat im Lauf der letzten Jahre eine Reihe von Linux-Utilities auf Windows portiert, darunter sudo, cURL oder tar. Nun erhalten Admins die GNU Coreutils, eine umfangreiche Sammlung an CLI-Programmen. Bis dato musste man eine Emulationsschicht wie Cygwin installieren, um die nativen Linux-Programme auf Windows ausführen zu können.

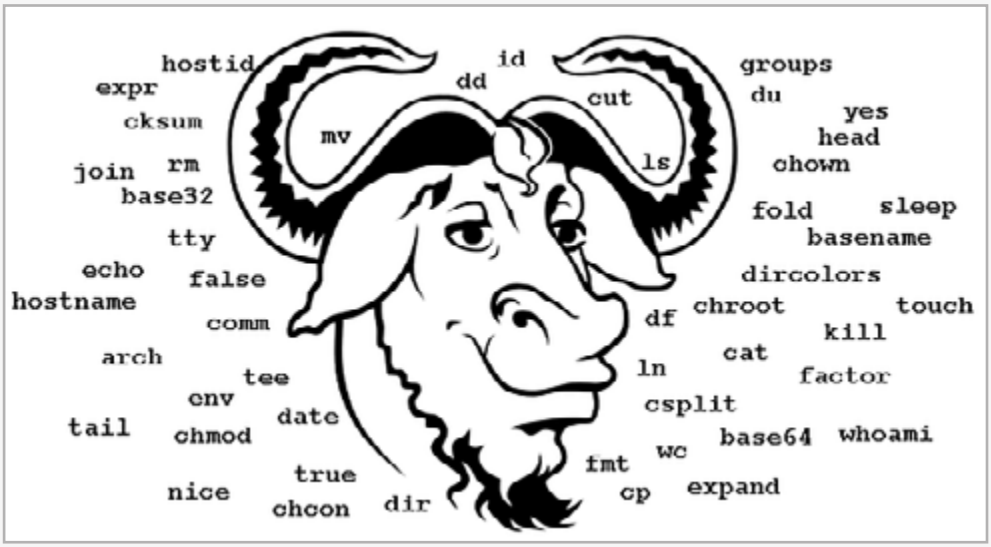


Abb. 24: Die GNU Coreutils umfassen zahlreiche Befehle.

Microsoft brachte neben den *GNU Coreutils* einige Programme von *GNU grep* und *GNU findutils* auf Windows. Die aktuell 78 Tools kommen nicht nur Linux-Admins entgegen, die nebenbei auch Windows-Rechner betreuen. Vielmehr empfehlen sie sich auch für Aufgaben, die sich mit PowerShell nur wesentlich umständlicher und mit der alten Batch-Umgebung gar nicht erledigen lassen.

Beispiele dafür sind etwa *uptime*, das die aufwändige Berechnung der Zeit seit dem letzten Systemstart klar vereinfacht. Entsprechendes gilt auch für die Codierung und Decodierung von Daten mit Base64, das mit PowerShell einen Zweizeiler erfordert oder ansonsten mit certutil bestenfalls eine Krücke für diesen Zweck bietet. Ein weiteres Beispiel ist touch, für das man in PowerShell ein Script benötigt.

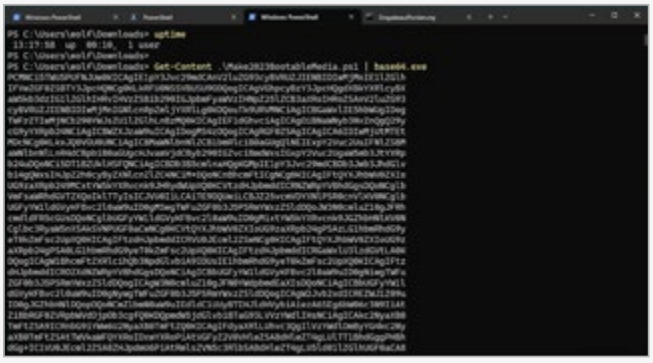


Abb. 25: Laufzeit eines Rechners mit uptime anzeigen und Daten mit base64 kodieren.

Bei einer Kommandozeile, in der sowohl PowerShell-Cmdlets und herkömmliche Dienstprogramme als auch die Coreutils nebeneinander existieren, sind Konflikte natürlich absehbar. Befehle wie ***date***, ***find***, ***mkdir***, ***rmdir***, ***hostname*** oder ***sort*** gab es schon bisher und die Coreutils bringen ihre eigenen Versionen mit. Die Version, die weiter vorne im Suchpfad steht oder direkt von cmd.exe ausgeführt wird, setzt sich durch.

Die Überschneidung mit PowerShell ist besonders groß, weil diese eine große Zahl an Aliases vordefiniert, die sich speziell an Linux-Admins richten. Dazu gehören etwa ***ls***, ***pushd***, ***mv***, ***cp*** oder ***cat.*** Aus diesem Grund kann man beim Setup entscheiden, ob die GNU-Utilities im Pfad vor den Windows-eigenen ***find*** oder ***sort*** stehen sollen. Außerdem deaktiviert es auf Wunsch die Aliase, die sich mit Namen der Coreutils überschneiden.

7.1 ADMINISTRATORSCHUTZ ALS UAC-ALTERNATIVE

Anders als die UAC beruht der Administratorschutz nicht auf einem Konto und zwei Tokens, sondern operiert mit zwei Accounts. Einer davon ist jener, mit dem man sich an Windows anmeldet, der andere ist ein System Managed Administrator Account (SMAA).

Dabei handelt es sich um ein lokales passwortloses Konto, das zusätzlichen Einschränkungen unterliegt. So dürfen sich nur bestimmte Systemprozesse unter dieser Kennung anmelden. Es verfügt über ein eigenes Benutzerprofil inklusive eines separaten HKCU-Hives in der Registry. Malware im Kontext des Standardbenutzers kann Ressourcen des privilegierten Users daher nicht manipulieren.

Insgesamt führt die AP aufgrund ihres restriktiven Charakters zu einer spürbaren Zunahme an UAC-Dialogen. Nachdem die häufige Eingabe von Benutzername und Passwort die Akzeptanz des Features beeinträchtigen würde, integriert Microsoft AP mit ***Windows Hello***, so dass sich Admins über biometrische Verfahren authentifizieren können.

7.2 SMART APP CONTROL

Bereits mit Windows 11 22H2 wurde Smart App Control eingeführt. Microsoft blockiert damit Apps, die der zugehörige Cloud-Service aufgrund ihres Verhaltens als bösartig oder unerwünscht einstuft. Wenn das Feature die Vertrauenswürdigkeit eines Programms nicht einschätzen kann, dann prüft es dessen Signatur. Ist diese nicht vorhanden oder ungültig, lässt sich die App nicht ausführen.

Die größte Einschränkung des Features bestand neben den fehlenden Management-Funktionen bis dato darin, dass es sich nur auf einem frisch installierten Windows aktivieren ließ. 26H2 beseitigt dieses Defizit, so dass Smart App Control ohne Neuinstallation des Rechners beliebig ein- und ausgeschaltet werden kann.

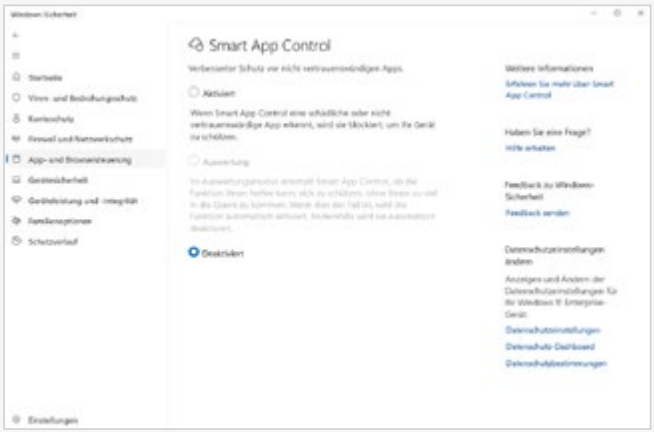


Abb. 26: Smart App Control lässt sich jetzt jederzeit ein- und ausschalten.

7.3 IAKERB UND LOKALES KDC NICHT AN BORD

Eine wesentlich Rolle bei der endgültigen Ausmusterung von NTLM spielen ***Initial and Pass Through Authentication Using Kerberos (IAKerb)*** und ein lokales KDC. Als Ziel für die allgemeine Verfügbarkeit war das zweite Halbjahr 2026 angekündigt.

Nachdem diese Features erst im Juni 2026 als öffentliche Preview in den Canary Channel kamen, war jedoch absehbar, dass aus diesem Datum nichts wird. IAKerb und LocalKDC lassen sich dort bis dato nur über die Registry steuern, die Verwaltung über Gruppenrichtlinien und MDM soll erst später folgen.

Dafür enthält dieses OS-Release jedoch eine neue Gruppenrichtlinie, mit der sich NTLM differenziert nach Szenarien blockieren lässt:

- Erweiterte NTLM-Blockierung („NTLM Enhanced Blocking“)

Sie befindet sich unter ***Computerkonfiguration*** => ***Richtlinien*** => ***Administrative Vorlagen*** => ***System*** => ***NTLM***. Admins können dort für jedes Szenario zwischen Audit, Aktiviert und Deaktiviert wählen. Ersteres protokolliert die dazu passenden Events, während Aktiviert die betreffende Aktion blockiert.

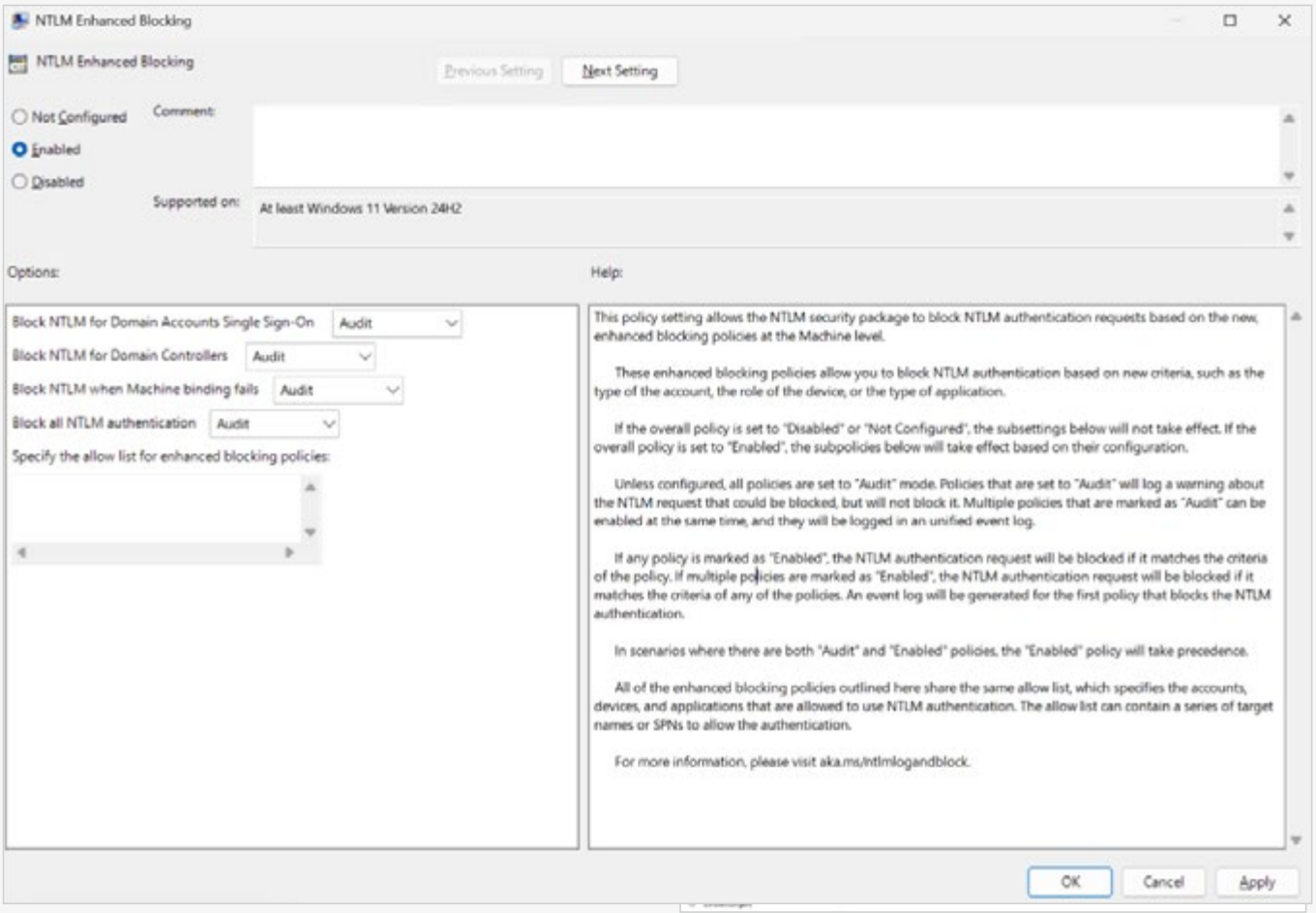


Abb. 27: NTLM für unterschiedliche Szenarien gezielt überwachen oder blockieren

7.4 WSLC: LINUX-CONTAINER OHNE DOCKER AUSFÜHREN

Bisher benötigte man ein Produkt von Drittanbietern wie Docker Desktop oder Podman Desktop, um Linux-Container auf Basis von WSL auszuführen. Docker bietet dabei die Wahl zwischen Prozess- und VM-Isolierung, wobei ersteres weniger Ressourcen verbraucht. Bei der VM-Isolierung läuft nämlich jeder Container in einer eigenen virtuellen Maschine.

Mit WSL 2.9.3.0 führt Microsoft eine eigene Infrastruktur für das Management von Linux-Containern ein. Zuständig ist dafür das Kommandozeilen-Tool wslc.exe (Alias: ***container.exe***). Die Syntax und die Namen der Befehle lehnen sich an Docker an, zum Beispiel ***wslc run*** oder ***wslc pull*** statt ***docker run*** oder ***docker pull***.



Abb. 28: Unterstütze Befehle für das Kommandozeilen-Tool wslc.exe.

Aktuell befindet sich WSL 2.9.3.0 inklusive seiner Container-Infrastruktur in der Preview-Phase. Um eine Installation von WSL2 auf die Preview zu aktualisieren, führt man diesen Befehl aus:

wsl --update --pre-release

Anschließend startet man das Terminal neu, und danach sollte sich wslc.exe im Suchpfad befinden. Man muss keine Distro wie Ubuntu oder Debian in WSL installieren, um Linux-Container ausführen zu können. Die dafür benötigte Infrastruktur ist nun in WSL enthalten, das CLI-Tool startet man direkt von der Windows-Shell.

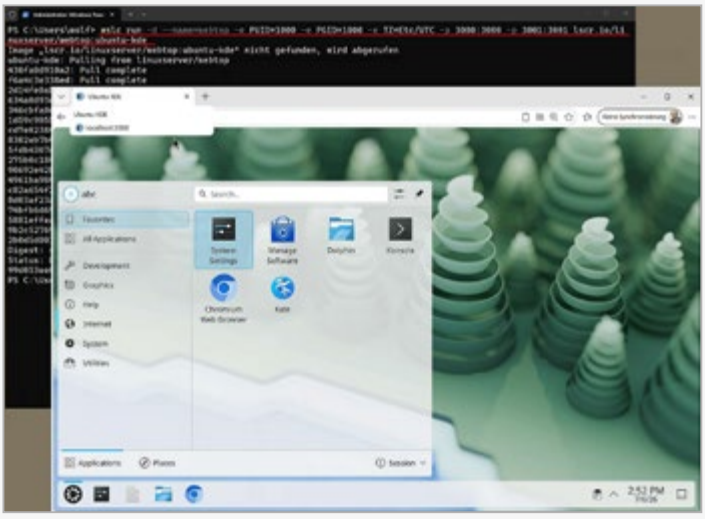


Abb. 29: Container mit KDE Webtop via WSLc starten, Verbindung über den Web-Browser herstellen.

7.4.1 Einschränkungen von WSL-Containern

Im Unterschied zu Docker unterstützt WSLc keine Prozessisolierung, sondern es startet eine eigene Hyper-V-VM für jeden Container. Das erhöht zwar den Ressourcenverbrauch, die stärkere Isolierung kommt jedoch der Sicherheit und Stabilität zugute.

Eine weitere Einschränkung im Vergleich zu Docker besteht darin, dass WSLc aktuell kein Äquivalent zu ***Docker Compose*** bietet, also nur einzelne Container ausführen und Multi-Container-Apps nicht orchestrieren kann. Allerdings plant Microsoft, eine solche Fähigkeit nachzurüsten.

Wenn man weder Compose noch Docker-Plugins benötigt, dann ist ein wesentliches Argument für WSLc, dass man sich damit die Lizenzkosten für einen Drittanbieter erspart.

Im Unterschied zu gängigen Produkten von Drittanbietern beschränkt sich WSLc auf die Kommandozeile und bietet keine grafische Oberfläche. Diese Lücke schließt vorerst das textbasierte Dashboard lazywslc von Microsofts Product Manager Craig Loewen.

WSL-Container bieten neben der Kommandozeile allerdings noch ein API für die Sprachen C, C++ und C#, so dass Entwickler relativ einfach Dienste in Windows-Programme integrieren können, die über Linux-Container bereitge



Abb. 30: Container mit KDE Webtop via WSLc starten, Verbindung über den Web-Browser herstellen.

7.4.2 Anstehende WSL-Verbesserungen

WSL-Container nutzen per Voreinstellung das Dateisystem ***virtiofs***, das den Zugriff auf Windows-Dateien laut Microsoft doppelt so schnell macht. Aufgrund der kritischen Natur des Dateizugriffs wird dieses Feature vorerst nur in Containers aktiviert, WSL selbst soll jedoch zu einem späteren Zeitpunkt folgen.

Darüber hinaus erhalten WSL-Container einen neuen standardmäßigen Netzwerkmodus namens ***consomme***. Es handelt sich laut Doku dabei um ein User-Mode-NAT/Proxy über Host-Sockets. Der Gast bekommt eine eigene interne IP und der Traffic läuft über den Netzwerk-Stack des Hosts inklusive dessen VPNs bzw. Firewall-Policies. Standardmäßig liefert Consomme nur ausgehende Verbindungen, inbound braucht ein explizites Port-Forwarding.

Schließlich sollen verbesserte Techniken für das Zurückfordern von Speicher nicht mehr benötigtes RAM von der Linux-VM an den Host zurückgeben. Auch diese Neuerung bleibt wie ***consomme*** als Standardeinstellung vorerst auf Container beschränkt.

7.5 INTELLIGENT TERMINAL

Mit der ***AI Shell*** unternahm Microsoft im letzten Jahr einen ersten Anlauf zur Integration von AI mit der Kommandozeile. Dieses Projekt wird nicht mehr weitergeführt, ihm folgt nun das Intelligent Terminal. Es liegt aktuell in der Version 0.1 vor.

Die Umgebung selbst beruht auf Windows Terminal und verwandelt dieses quasi in einen Agent-Client. Der AI-Agent übernimmt bei fehlerhaften und gescheiterten Befehlen automatisch den Kontext aus der Konsole und schlägt Korrekturen vor, die man sofort ausführen kann.

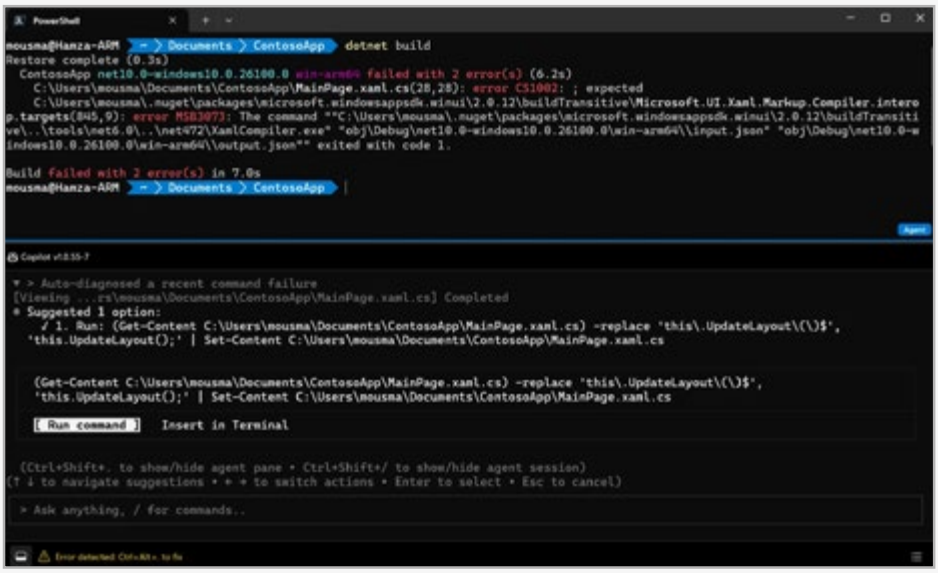


Abb. 31: Intelligent Terminal erkennt Fehler in Befehlen selbstständig und versucht diese zu korrigieren.

Die Kommunikation erfolgt über das Agent Communication Protocol (ACP), so dass man verschiedene Agenten hinzufügen kann. Per Voreinstellung nutzt Intelligent Terminal den GitHub Copilot.

7.6 WINDOWS DEVELOPER CONFIG

Einige der für Developer gedachten Neuerungen sind auch für DevOps interessant. So lässt sich eine frische Windows-Installation mit Hilfe einer WinGet-Konfiguration in einem Durchgang mit allen gängigen Tools ausstatten, darunter VS Code, WSL, PowerShell 7, Python und weitere. Dieses Feature firmiert unter der Bezeichnung ***Windows Developer Config*** und ist bereits auf GitHub verfügbar.

Das Cloud-Pendant dazu ist ***Windows 365 with Developer Configuration***, ein virtueller Desktop, der eine komplette Developer-Umgebung bereits enthält. Das vorkonfigurierte Image umfasst unter anderem Visual Studio Code, Git, GitHub CLI und WSL.

08 ADMX V3.0: 17 NEUE EINSTELLUNGEN

Rund ein halbes Jahr vor dem Erscheinen von 26H2 veröffentlichte Microsoft die ADMX-Vorlagen für Windows 11 und Server 2025 in der Version 3.0. Im Vergleich zu den ADMX, die gleichzeitig mit dem der Version 25H2 freigegeben wurden, kommen 17 Einstellungen hinzu. Diese betreffen unter anderem Windows Update, IPv6, MSIX-Pakete, Dateifreigaben und Copilot.

Zwei Policies betreffen die KI-Konfiguration. Dabei handelt es sich erstens um die zahnlose Einstellung zur Entfernung der Copilot-App, die nur unter bestimmten Voraussetzungen greift und vom Benutzer wieder rückgängig gemacht werden kann:

- Microsoft Copilot-App entfernen („Remove Microsoft Copilot App“)

Zum anderen können Admins nun einen Wert zur Kontrolle von AI-Agents festlegen, wobei 0 für „User in control“, 1 für „Restricted“ und 2 für „Bypass“ steht. Die Policy heißt

- Mindestrichtlinie für Agent Connector („Agent Connector Minimum Policy“)

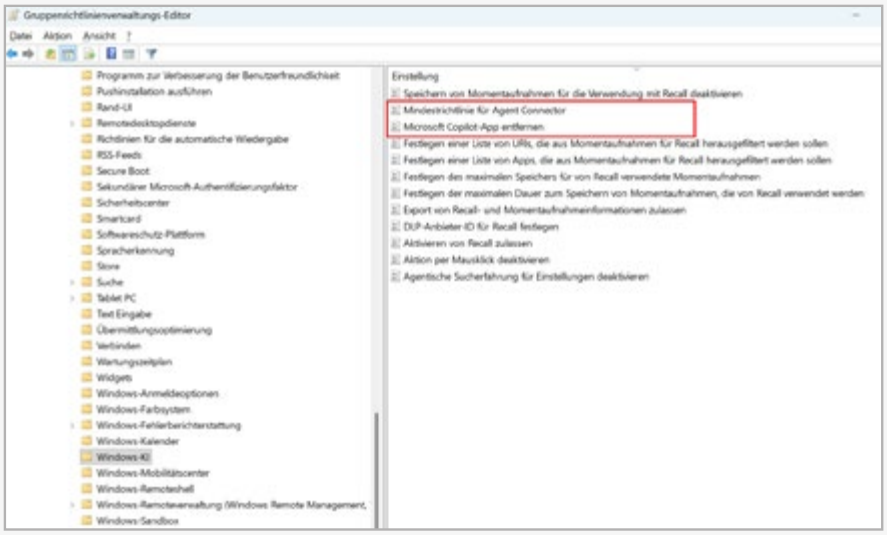


Abb. 32: Die neuen Gruppenrichtlinien für die Konfiguration von KI-Features.

8.1 MSIX-PAKETE

Für das Management vom MSIX-Paketen bringen die aktuellen ADMX folgende neuen Einstellungen:

- Microsoft SmartScreen-Überprüfungen für MSIX-Pakete aktivieren („Enable Microsoft SmartScreen checks for MSIX Packages“)
- Zugelassene Zonen für MSIX-Pakete aktivieren („Enable Allowed Zones for MSIX Packages“)

Dabei handelt es sich um Sicherheitseinstellungen, die bestimmen, ob SmartScreen MSIX-Pakete aus bestimmten URL-Zonen prüfen soll, und ob Pakete, die aus bestimmten URL-Zonen stammen, installiert werden dürfen.

8.2 DREI EINSTELLUNGEN FÜR CLAT

464XLAT ist ein IPv4-IPv6-IPv4-Übersetzungsverfahren für den Zugriff auf IPv4-Ressourcen in reinen IPv6-Netzwerken. Der Client nutzt dabei einen SIIT-Übersetzer (CLAT), um IPv4-Pakete in IPv6 zu konvertieren.

Dieser lässt sich nun über die folgenden drei Einstellungen konfigurieren:

- CLAT-Zulassung festlegen („Set CLAT Permit“)
- Festlegen von CLAT: Abrufen von Präfixinformationen von RA („Set CLAT Get Prefix Information from RA“)
- Festlegen von CLAT: Abrufen von Präfixinformationen aus DNS („Set CLAT Get Prefix Information from DNS“)

8.3 SHARING SHEET

Nachdem die ADMX 25H2 v2.0 die Möglichkeit boten, die Anzeige von Apps auf der Freigabeseite für Dateien einzuschränken, lässt sich nun auch verhindern, dass Benutzer Texte inline auf dem Sharing Sheet verfassen.

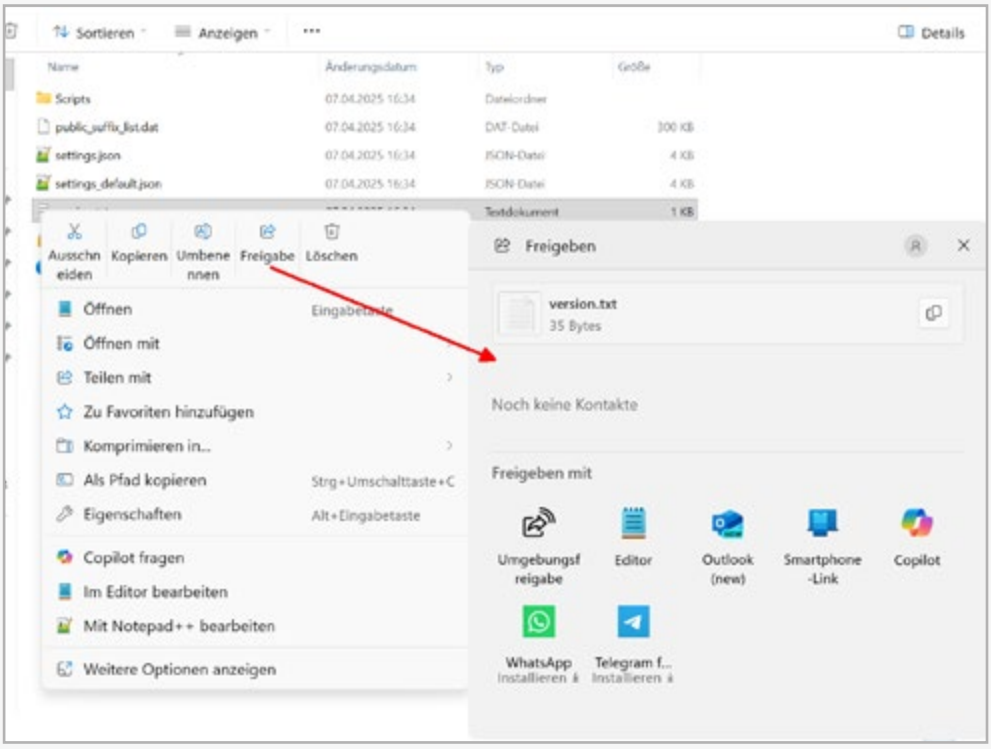


Abb. 33: Sharing Sheet im Explorer von Windows 11.

Zuständig ist dafür die Einstellung

- DisableInlineCompose

Sie wurde bis dato nicht lokalisiert und verfügt im GPO-Editor noch über keinen Hilfetext.

8.4 RESTORE VON WINDOWS BACKUP FOR ORGANIZATIONS

Intune bietet seit Oktober 2025 eine Einstellung, mit der sich die Wiederherstellung aus Backup für Organisationen aktivieren lässt. Die Gruppenrichtlinien ziehen nun mit einer entsprechenden Policy nach:

- Windows-Wiederherstellung aktivieren („Enable Windows Restore“)

8.5 ACTIVE DIRECTORY UND ENTRA ID

Domänenbenutzer verschlüsseln Daten über das DPAPI mit Keys, die von ihrem Passwort abgeleitet sind. Wenn sie dieses vergessen und es von einem Admin zurückgesetzt wird, dann lassen sich bereits verschlüsselte Daten nicht mehr dekodieren. In diesem Fall helfen die Backup-Keys, die auf dem Domain Controller gespeichert sind. Sie entschlüsseln die Daten aller Domänenbenutzer.

Im Januar kündigte Microsoft an, dass Admins künftig festlegen können, wie oft diese Schlüssel erneuert werden. Standardmäßig erfolgt dies alle 90 Tage. Zuständig ist dafür nun die Richtlinie

- Rotationszeitraum für Datenschutz-API-Sicherungsschlüssel festlegen („Set the DPAPI backup keys rotation period“)

Eine weitere neue Einstellung sorgt dafür, dass alle RDP-Clients die RDS AAD-Authentifizierung verwenden müssen, um sich bei RD-Sitzungs-Hosts anzumelden. Diese Richtlinie erlaubt keinen Rückfall auf andere Authentifizierungsmethoden. Sie verlangt zudem, dass die Authentifizierung auf Netzwerkebene (NLA) aktiviert ist. Es handelt sich dabei um folgende Policy:

- Microsoft Entra ID-Authentifizierungsdurchsetzung aktivieren („Enable Microsoft Entra ID Authentication Enforcement“)

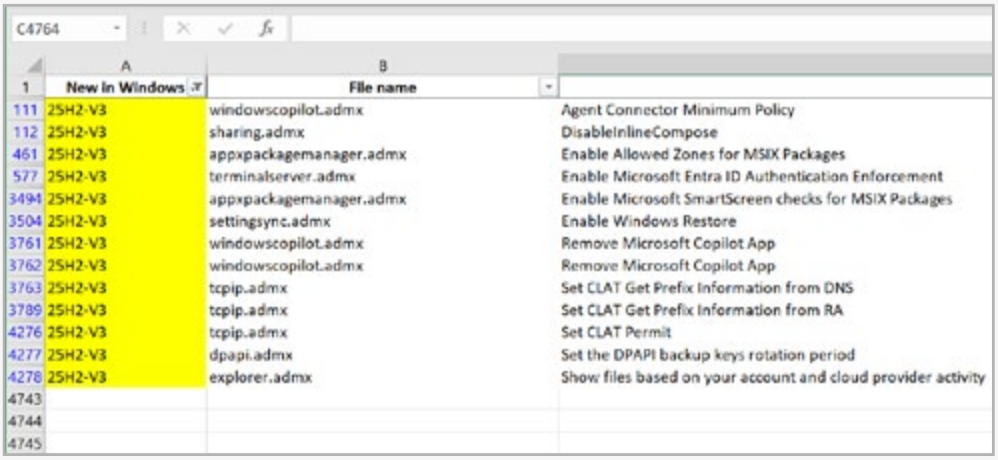
8.6 WINDOWS UPDATE

Sie hießt ***Wartungsfenster für automatische Updates konfigurieren*** („Configure maintenance windows for automatic updates“) und findet sich unter ***Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Windows-Update => Endbenutzeroberfläche verwalten***. Details zu dieser Einstellung siehe weiter oben.

8.7 INKONSISTENZEN IN DER DOKUMENTATION

Parallel zu den neuen administrativen Vorlagen erschien als Dokumentation wie gewohnt das aktualisierte Group Policy Settings Reference Spreadsheet.

Es weist 12 Änderungen gegenüber der Version 2.0 aus, allerdings fehlt dort die Einstellung „Configure maintenance windows for automatic updates“. Dafür weist es „Show files based on your account and cloud provider activity“ als neu aus.



	A	B	
1	New in Windows	File name	
111	25H2-V3	windowscopilot.admx	Agent Connector Minimum Policy
112	25H2-V3	sharing.admx	DisableInlineCompose
461	25H2-V3	appxpackagemanager.admx	Enable Allowed Zones for MSIX Packages
577	25H2-V3	terminalserver.admx	Enable Microsoft Entra ID Authentication Enforcement
3494	25H2-V3	appxpackagemanager.admx	Enable Microsoft SmartScreen checks for MSIX Packages
3504	25H2-V3	settingsync.admx	Enable Windows Restore
3761	25H2-V3	windowscopilot.admx	Remove Microsoft Copilot App
3762	25H2-V3	windowscopilot.admx	Remove Microsoft Copilot App
3763	25H2-V3	tcpip.admx	Set CLAT Get Prefix Information from DNS
3789	25H2-V3	tcpip.admx	Set CLAT Get Prefix Information from RA
4276	25H2-V3	tcpip.admx	Set CLAT Permit
4277	25H2-V3	dpapi.admx	Set the DPAPI backup keys rotation period
4278	25H2-V3	explorer.admx	Show files based on your account and cloud provider activity
4743			
4744			
4745			

Abb. 34: Die seit 25H2 v2.0 laut Reference Spreadsheet eingeführten 12 Richtlinien.

Diese Richtlinie gab es allerdings schon zuvor, da hieß sie jedoch noch „Turn off account-based insights, recent, favorite, and recommended files in File Explorer“. Die deutsche Bezeichnung dafür lautet ***Deaktivieren von kontobasierten Einblicken, letzten, bevorzugten und empfohlenen Dateien im Datei-Explorer.***

09 ZUSAMMENFASSUNG

Windows 11 26H2 wird als drittes Release in Folge als Enablement Package ausgeliefert, weil es auf dem gleichen Branch beruht wie seine Vorgänger 24H2 und 25H2. Für Admins hat ein solches kleines Upgrade einige Vorteile, da es über den normalen Update-Kanal erfolgt und kaum Kompatibilitätsprobleme erwarten lässt.

Allerdings erhält 26H2 im Vergleich zu seinen Vorgängern keine neuen Funktionen, so dass seine Aufgabe im Wesentlichen darin besteht, den Support-Zeitraum neu zu starten. Auf verwalteten Geräten schaltet es zudem die neuen Features frei, die schon zuvor über die monatlichen Updates ausgeliefert wurden.

Obwohl der Unterbau des Systems das dritte Jahr in Folge unverändert bleibt, nimmt sich Microsoft einige grundsätzliche Änderungen bei der Produktphilosophie vor. Die im März angekündigte Qualitätsoffensive für Windows 11 begründete Microsoft vor allem mit der in sozialen Medien artikulierten Unzufriedenheit der Kunden.

Erheblicher Druck dürfte aber auch von den OEMs wegen der rückläufigen PC-Verkäufe kommen. Diese sind nicht zuletzt den relativ hohen Hardware-Anforderungen des OS geschuldet. Microsoft verspricht nun, den Speicherverbrauch von Windows 11 so weit zu optimieren, dass Rechner mit 8 GB RAM für gängige Aufgaben ausreichen. Neu in WinUI 3 geschriebene GUI-Komponenten verbessern zudem das Ansprechverhalten des Systems.

Microsoft reagiert zudem auf die Beschwerden vieler Benutzer über zu häufige oder zeitlich unwillkommene Updates, indem es den Anwendern die weitgehende Kontrolle über die Installation von Patches überlässt. Das betrifft primär den Zeitpunkt, den User praktisch beliebig lang verschieben können. Aber selbst ein Neustart bei einem ausstehenden Update erzwingt keine Installation mehr und auch beim Setup des OS kann man die Updates überspringen.

Mit Point-in-Time Restore und Cloud Rebuild erhält Windows 11 zwei weitere Funktionen, um einen havarierten PC wieder in Gang zu bringen. Erstere setzt das System inklusive Anwendungen und Benutzerdaten auf einen früheren Zustand zurück. Cloud Rebuild bewirkt eine Bare-Metal-Installation des Betriebssystems, wobei die Medien dafür aus der Cloud heruntergeladen werden.

Die Wiederherstellung der individuellen Benutzerumgebung übernimmt Backup für Organisationen (neuerdings „Windows settings backup and restore“), das außerhalb der EU künftig per Voreinstellung aktiv ist. Für das Roaming der Einstellungen ist ESR zuständig, dessen Management zum 1. Juli 2026 umgestellt wurde.

Aus der Sicht von Admins und DevOps bringt 26H2 ebenfalls einige interessante Neuigkeiten. Dazu zählen die Portierung der GNU Coreutils auf Windows, ein Management-Layer für Linux-Container, der Produkte von Drittanbietern wie Docker ersetzen soll, oder Intelligent Terminal, das bei fehlerhaften Befehlen mit Korrekturen hilft.

Mit der Public Preview von IAKerb und LocalKDC ist Microsoft auf Kurs, um das veraltete NTLM abzulösen. Ob diese Kerberos-Erweiterungen in 26H2 noch über ein Update nachgeliefert werden, steht aktuell aber genauso wenig fest wie bei der Administrator Protection.

EXTRA
COMPUTER GMBH

Ihnen gefällt, was Sie lesen?

Mehr E-Books gibts‘s hier:
extracomputer.de/medien-downloads

Keine News mehr verpassen!

Abonnieren Sie unseren Newsletter
extracomputer.de/newsletter/

Hauptsitz

EXTRA Computer GmbH
Brühlstr. 12
89537 Giengen
Deutschland

07322 / 9615 - 0
info@extracomputer.de

Druckfehler, Irrtümer und Änderungen vorbehalten.
V10-2026