Aagon

E-BOOK

WINDOWS-UPDATES MIT GRUPPENRICHTLINIEN VERWALTEN

August 2023

www.aagon.com

Inhalt

Über den Autor

Das E-Book wurde erstellt von Wolfgang Sommergut – Fachautor, Berater und Konferenzsprecher zu verschiedenen Themen der IT.

Überblick

Wie in praktisch allen anderen Bereichen, fährt Microsoft auch beim Update-Management einen Kurs in Richtung Cloud.

Das lässt sich schon daran erkennen, dass die Windows Server Update Services (WSUS) seit mehreren Generationen keine nennenswerten neuen Funktionen mehr erhalten, obwohl sie in vielen Unternehmen nach wie vor das wichtigste Bordmittel für das Patch-Management von Microsoft-Produkten sind.

Die um Jahre verspätete und kürzlich angekündigte Unterstützung der *Unified Update Platform* für WSUS lässt aber zumindest erwarten, dass dieser On-prem-Dienst noch eine Weile erhalten bleibt.

OS-Patches bevorzugt über Windows Update

Allerdings kommt WSUS offiziell immer mehr die Rolle zu, Patches für Office, Exchange oder andere Produkte zu verteilen, jedoch nicht mehr für das Betriebssystem. Microsoft empfiehlt nämlich schon seit längerem, die Patches für Windows direkt von Windows Update zu beziehen.

Die Gruppenrichtlinien bieten neuerdings die Möglichkeit, für Feature-, Qualitäts- und andere Updates jeweils WSUS oder Windows Update als Quelle festzulegen. Dies erleichtert den schrittweisen Abschied von WSUS für OS-Updates.

Microsoft will Windows-Updates selbst koordinieren

Der Grund für Bevorzugung von Windows Update liegt vor allem darin, dass bei größeren Malware-Wellen immer wieder zahlreiche Systeme verwundbar sind, obwohl die entsprechenden Schwachstellen vom Hersteller schon geschlossen wurden. Offensichtlich versäumen es viele Admins, kritische Updates rechtzeitig einzuspielen.

Microsoft möchte daher bei der Verteilung von OS-Updates stärker die Kontrolle übernehmen und dafür sorgen, dass die Mehrzahl der PCs innerhalb kurzer Zeit auf dem neuesten Stand kommt. Systemverwalter sollten deshalb möglichst wenig in die Verteilung von Patches eingreifen oder am besten die gleichen Mechanismen für das Update-Management nutzen wie private Anwender.

Updates als Vertrauenssache

Umgekehrt misstrauen IT-Verantwortliche in Unternehmen einer weitgehend selbständigen und möglichst schnellen Installation von Updates, weil deren Qualität immer wieder Mängel aufweist und damit die Funktion und die Sicherheit der Firmen-PCs beeinträchtigen kann.

Wenn Admins dem Rat von Microsoft folgen und OS-Patches über Windows Update verteilen, so möchten sie daher diesen Vorgang zumindest zu einem gewissen Grad steuern können. Diese Aufgabe kommt primär den Gruppenrichtlinien zu, auch wenn es mit dem *Windows Update for Business Deployment Service* eine neue Alternative aus der Cloud gibt.

Aufschub von Updates

Die Gruppenrichtlinien bieten unter anderem Einstellungen, mit denen sich sowohl Qualitäts- als auch Feature-Updates zurückstellen lassen. Über verschieden lange Fristen für den zeitlichen Aufschub lassen sich so in begrenztem Rahmen Verteilerringe für einen gestaffelten Rollout von Updates realisieren.

Steuerung des PC-Reboots

Ein wesentlicher Aspekt bei der Installation von Updates ist der oft danach erforderliche Reboot der Rechner. Microsoft hat über die Jahre immer wieder neue Konzepte ausprobiert, die eine Balance zwischen Sicherheit und möglichst geringer Beeinträchtigung der Benutzer finden sollten.

Daraus resultieren zahlreiche Einstellungen für die Gruppenrichtlinien, die zu einem Großteil obsolet sind und im Wesentlichen auf eine empfohlene Policy eingedampft wurden.

Netzwerk-Traffic durch Updates

Neben der Kontrolle über die Freigabe von Updates bestand in der Vergangenheit ein Grund für den Aufbau einer WSUS-Infrastruktur darin, dass Firmen die Netzwerkbelastung reduzieren konnten, indem PCs ihre Updates in jeder Niederlassung von einem lokalen WSUS-Server beziehen.

Dieser Aspekt ist mittlerweile dank der Übermittlungsoptimierung (Windows Update Delivery Optimziation, WUDO) weitgehend hinfällig.
Es handelt sich dabei um ein verteiltes Caching von Updates, das man auch im Zusammenspiel mit WSUS nutzen kann.

Das Feature lässt sich in einem professionellen Umfeld über Gruppenrichtlinien konfigurieren, beispielsweise um den Bandbreitenverbrauch zu kontrollieren oder um PCs abhängig von der Netzwerktopologie zu gruppieren.

Best Practices als Baseline

Microsoft gibt für alle Schritte und Komponenten des Update-Managements Best Practices vor. Um deren Umsetzung zu vereinfachen, stehen die empfohlenen Einstellungen für die Gruppen- richtlinien als Update Baseline zur Verfügung. Sie enthält Backups von Muster-GPOs inklusive der dazugehörigen Dokumentation.

On-prem-Lösung von Drittanbietern als Alternative

Anwender, die seit mehreren Jahren Microsofts Bordmittel für das Management von Windows- Updates einsetzen, sind entweder mit der mangelnden Produktpflege von WSUS oder mit den ständigen Änderungen in den Gruppen- richtlinien konfrontiert.

Auch wenn sich die WSUS schon lange am Markt befinden, so würde ihnen eine Rundumerneuerung wahrlich guttun. Alleine die aufwändige Wartung von WSUS verschlingt zu viel Zeit in der Systemverwaltung.

Der Zickzackkurs des Herstellers bei der Konfiguration von Windows Update erfordert zudem einigen Lernaufwand und eine laufende Anpassung der GPOs.

Ein ausgereiftes Patch-Management für Windows wie Aagons CAWUM (Complete Aagon Windows Update Management) schirmt Anwender von den ständigen und kurzlebigen Änderungen bei Windows Update ab und bietet zudem eine flexible und robuste Alternative zu den vernachlässigten WSUS. Außerdem entfällt damit der permanente Druck vonseiten Microsofts, das Update-Management in einen Cloud-Service zu verlagern.

Windows 11 räumt Update-Policies auf

Über die Jahre haben sich Dutzende von Gruppenrichtlinien für Windows Update angesammelt, von denen viele keine Funktion mehr haben oder von denen Microsoft abrät. Bei vielen Einstellungen war dies für Admins aufgrund mangelnder Dokumentation gar nicht erkennbar.

Der Grund für die inflationäre Entwicklung bei den Gruppenrichtlinien für Windows Update liegt vor allem darin, dass Microsoft das Neustartverhalten von Windows nach einem Update mehrfach geändert und dafür jedes Mal neue Einstellungen eingeführt hat.

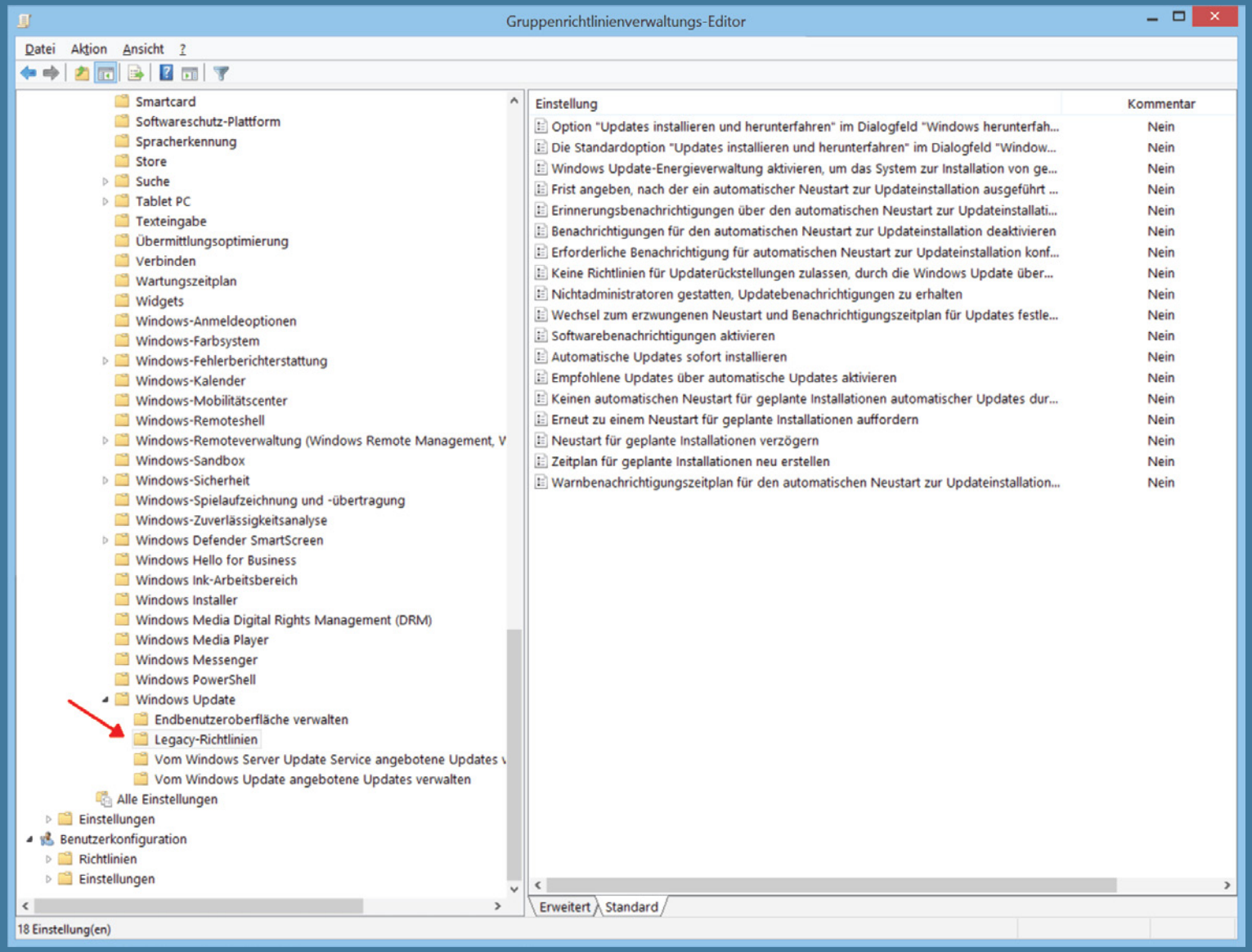
Hinzu kamen die Richtlinien für Windows Update for Business (WUfB), die ebenfalls mehrfach umgebaut wurden.

Neue Aufteilung im GPO-Editor

Microsoft kann die veralteten Einstellungen nicht einfach aus den administrativen Vorlagen entfernen, weil sich sonst vorhandene GPOs, in denen diese Settings verwendet werden, nicht mehr korrekt bearbeiten lassen.

Daher entschloss er sich, in den ADMX für Windows 11 den Wust an Einstellungen zugunsten einer besseren Übersichtlichkeit auf vier Ordner zu verteilen. Einer davon heißt *Legacy-Einstellungen* und beherbergt die nicht mehr zeitgemäßen Optionen.

Dagegen sind die administrativen Vorlagen für Windows 10 21H2 und 22H2 nicht bloß inkompatibel mit jenen von Windows 11, sondern verzichten auch auf diese neue Gruppierung der Einstellungen. Dort finden Admins weiterhin ein Kunterbunt aus aktuellen und überholten Settings in einer langen Liste vor.



Die Templates für Windows 11 lagern die veralteten Einstellungen in einen eigenen Ordner aus

Nicht mehr unterstützte Einstellungen

Ein Blog-Post in Microsofts TechCommunity gibt Aufschluss darüber, welche Einstellungen vermieden werden sollten. Ziemlich einfach fällt die Entscheidung bei den folgenden acht Optionen, weil sie ab Windows 10 gar nicht mehr implementiert wurden. Mancher Admin mag sich gewundert haben, warum sie nach der Migration auf Windows 10 nicht mehr greifen.

- Option "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anzeigen (Do not display 'Install Updates and Shut Down" option in Shut Down Windows dialog box)
- Die Standardoption "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anpassen (Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box)
- Neustart für geplante Installationen verzögern ("Delay Restart for scheduled installations")
- Softwarebenachrichtigungen aktivieren ("Turn on Software Notifications")
- Automatische Updates sofort installieren ("Allow Automatic Updates immediate installation")
- Erneut zu einem Neustart für geplante Installationen auffordern ("Re-prompt for restart with scheduled installations")
- Zeitplan für geplante Installationen neu erstellen ("Reschedule Automatic Updates scheduled installations")
- Empfohlene Updates über automatische Updates aktivieren ("Turn on recommended updates via Automatic Updates")

Änderung für Dual Scan

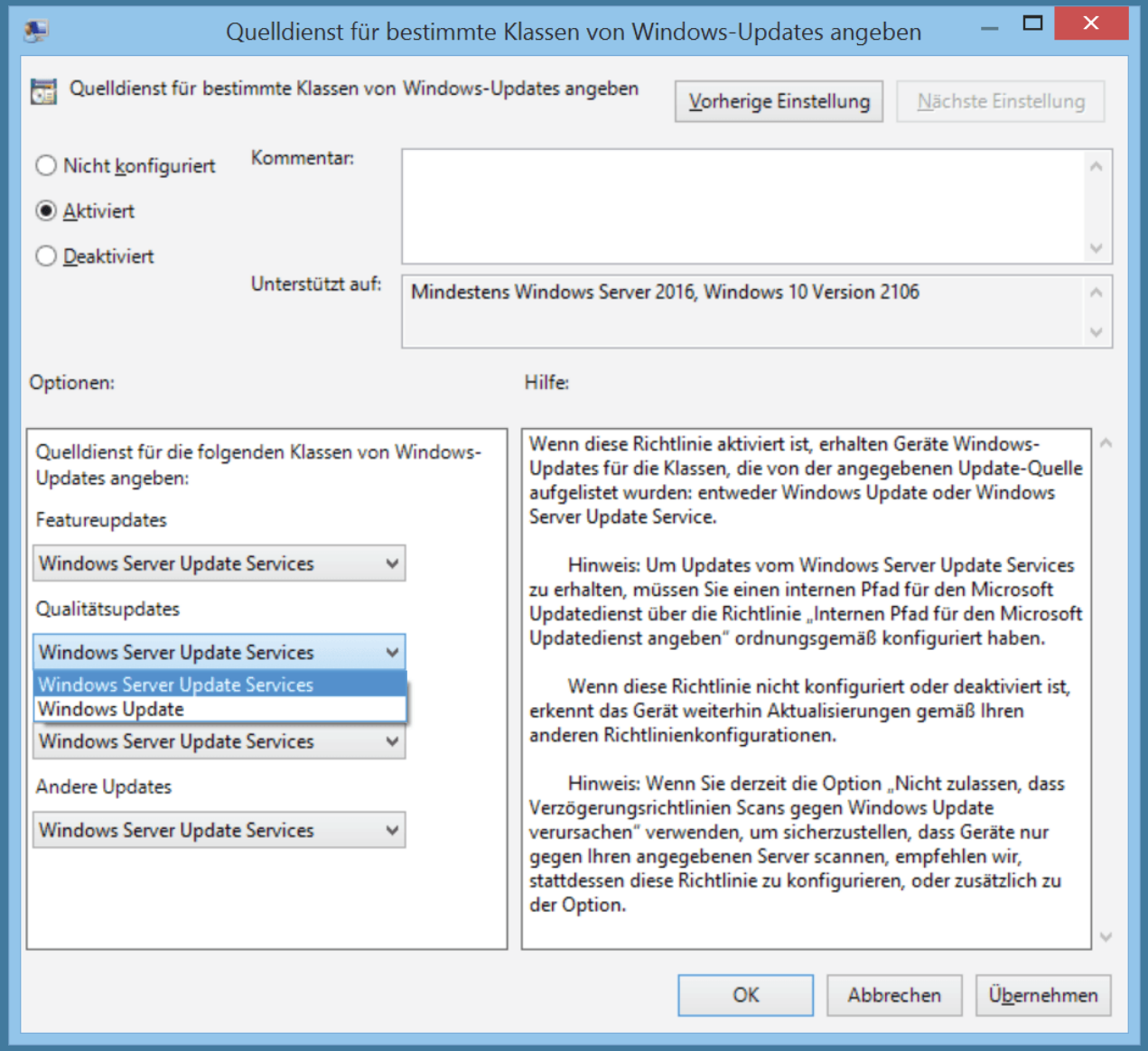
Eine weitere Einstellung, die bei Windows 10 zwar noch vorhanden, aber bei der Version 11 über Bord ging, betrifft Dual Scan:

- Keine Richtlinien für Updaterückstellungen zulassen, durch die Windows Update überprüft wird ("Do not allow update deferral policies to cause scans against Windows Update")

Zur Erläuterung: Dual Scan wird immer dann eingeschaltet, wenn man Clients einem WSUS-Server zuordnet und gleichzeitig bei ihnen die Qualitäts- oder Feature-Updates über WUfB zurückstellt.

Die Rechner erhalten OS-Updates dann nicht mehr über WSUS, sondern über Windows Update. Mit der obigen Richtlinie lässt sich dies vermeiden und WSUS auch als Quelle für die Updates des Betriebssystems beibehalten.

An die Stelle dieser Option tritt nun in Windows 10 ab Version 21H2 und in Windows 11 die Einstellung *Quelldienst für bestimmte Klassen von Windows-Updates angeben* ("Specify source service for specific classes of Windows Updates"). Über sie kann man für jeden Update-Typ entweder WSUS oder Windows Update als Quelle angeben.



Windows 10 ab 21H2 und Windows 11 unterstützen verschiedene Quellen für jeden Update-Typ

Neustart bei angemeldetem Benutzer

Eine weitere Einstellung, die User vor dem Reboot zu unpassenden Zeiten schützt, ist zwar noch an Bord, soll aber laut Microsoft nicht mehr verwendet werden:

- Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind ("No auto-restart with logged on users for scheduled automatic updates installations")

Laut Blog-Post verhalte sich diese Option zudem nicht so wie beschrieben.

Empfohlene Gruppenrichtlinien für Windows Update

Grundsätzlich empfiehlt Microsoft schon länger, dass Unternehmen ihre PCs mit den standardmäßigen Einstellungen von Windows Update aktualisieren sollten. Ein unmodifiziertes Windows Update biete den besten Kompromiss zwischen Sicherheit und Komfort.

Wenn Kunden jedoch das Standardverhalten von Windows Update modifizieren möchten, dann sieht der Hersteller nur relativ wenige Policies für die Anpassung vor. Das gilt besonders für die Konfiguration des Client-Neustarts. Für die Änderung des Zeitpunkts zur Installation von Updates dienen die Einstellungen von Windows Update for Business (WUfB).

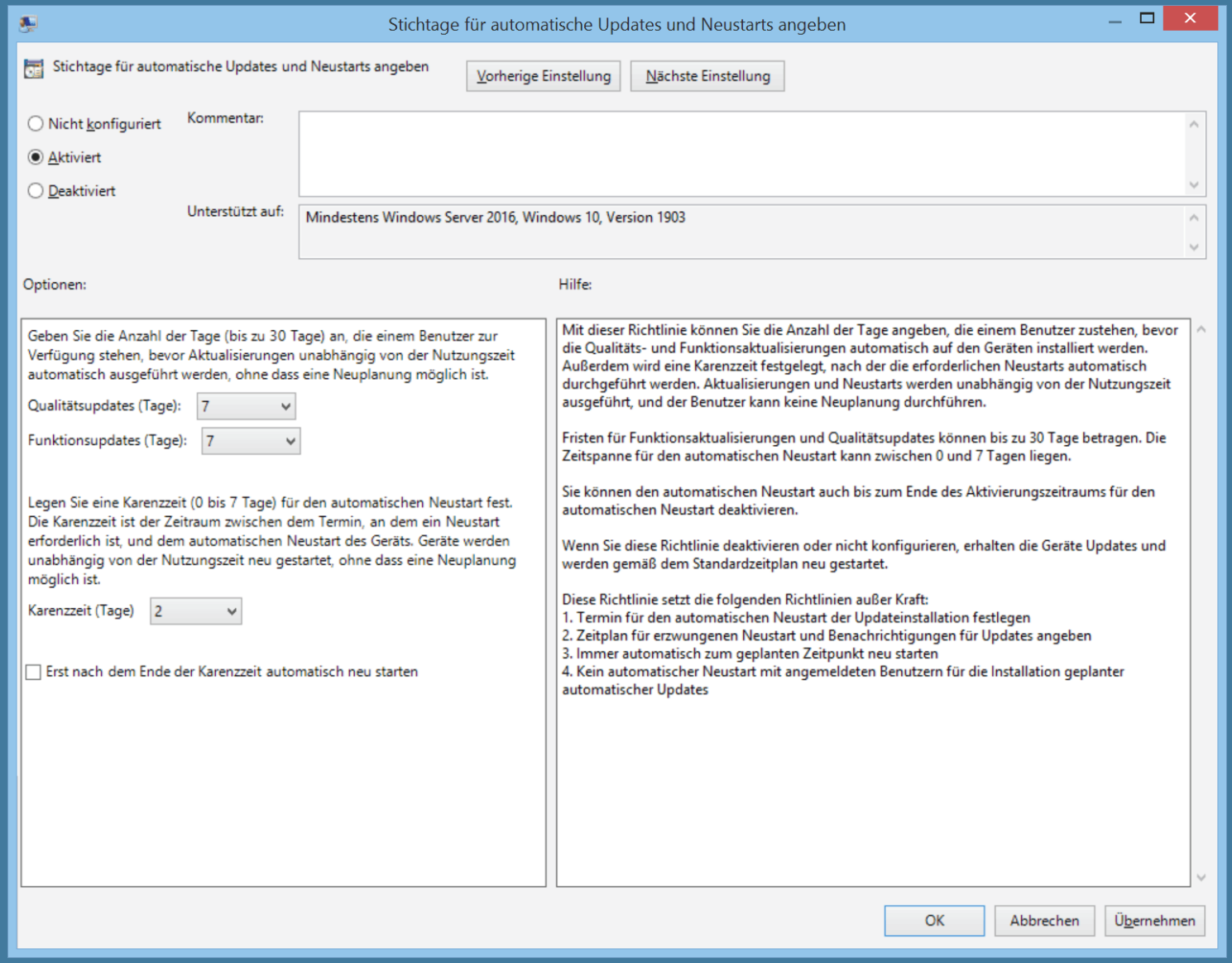
Für eine feinere Steuerung des Update-Managements über WUfB bietet Microsoft den Deployment Service an. Dieser erhielt nun vor einiger Zeit die Fähigkeit für einen stufenweisen Rollout von Patches.

Einstellungen für spezifische Umgebungen

Aus Sicht von Microsoft hat die möglichst rasche Installation von Updates die höchste Priorität, um die Sicherheit der Rechner zu gewährleisten. Daher empfiehlt der Hersteller, grundsätzlich die neue Einstellung *Stichtage für automatische Updates und Neustarts angeben* ("Specify deadlines for automatic updates and restarts") zu konfigurieren.

Abhängig von der Nutzungsart kommen weitere Richtlinien hinzu, die primär steuern, wie die Anwender die Installation von Patches beeinflussen können. So ist es in der Regel auf PCs, die sich mehrere User teilen, nicht erwünscht, dass diese den Zeitpunkt für den Neustart bestimmen oder den Download von Updates aktiv anstoßen.

Daher sollte man in solchen Umgebungen, die typischerweise auch in Schulen oder anderen Bildungseinrichtungen existieren, die Steuerungsmöglichkeiten der Benutzer weitgehend einschränken. Diesem Zweck dient die Policy *Zugriff auf alle Windows Update-Funktionen entfernen* ("Remove access to use all Windows Update features").



Mit einer neuen Einstellung für Windows Update lässt sich das Einspielen von Patches in einer bestimmten Frist erzwingen

Reboot steuern

Überall dort, wo Rechner über einen festen Zeitplan in Prozesse eingebunden sind, empfiehlt Microsoft die Installation von Updates über *Automatische Updates konfigurieren => Updates automatisch herunterladen und laut angegebenem Zeitplan installieren* ("Configure Automatic Updates => Schedule install time: Daily at X time"). Das gilt zum Beispiel für PCs in der Produktionssteuerung oder solche, die von mehreren Mitarbeitern im Schichtbetrieb verwendet werden.

Die automatische Ermittlung eines günstigen Zeitpunkts für den Neustart kann unter solchen Bedingungen ebenfalls schwierig sein. Admins haben in diesem Fall die Möglichkeit, über die Einstellung *Automatischen Neustart nach Updates während der Nutzungszeit deaktivieren* ("Turn off auto-restart for updates during active hours") einen bestimmten Termin vorzugeben.

Updates aufschieben oder vorziehen

Mit Windows as a Service entstand das Bedürfnis, die Installation der relativ häufigen Funktions-Upgrades zu verschieben. Auch die monatlichen kumulativen Updates sollen meist nicht sofort installiert werden.

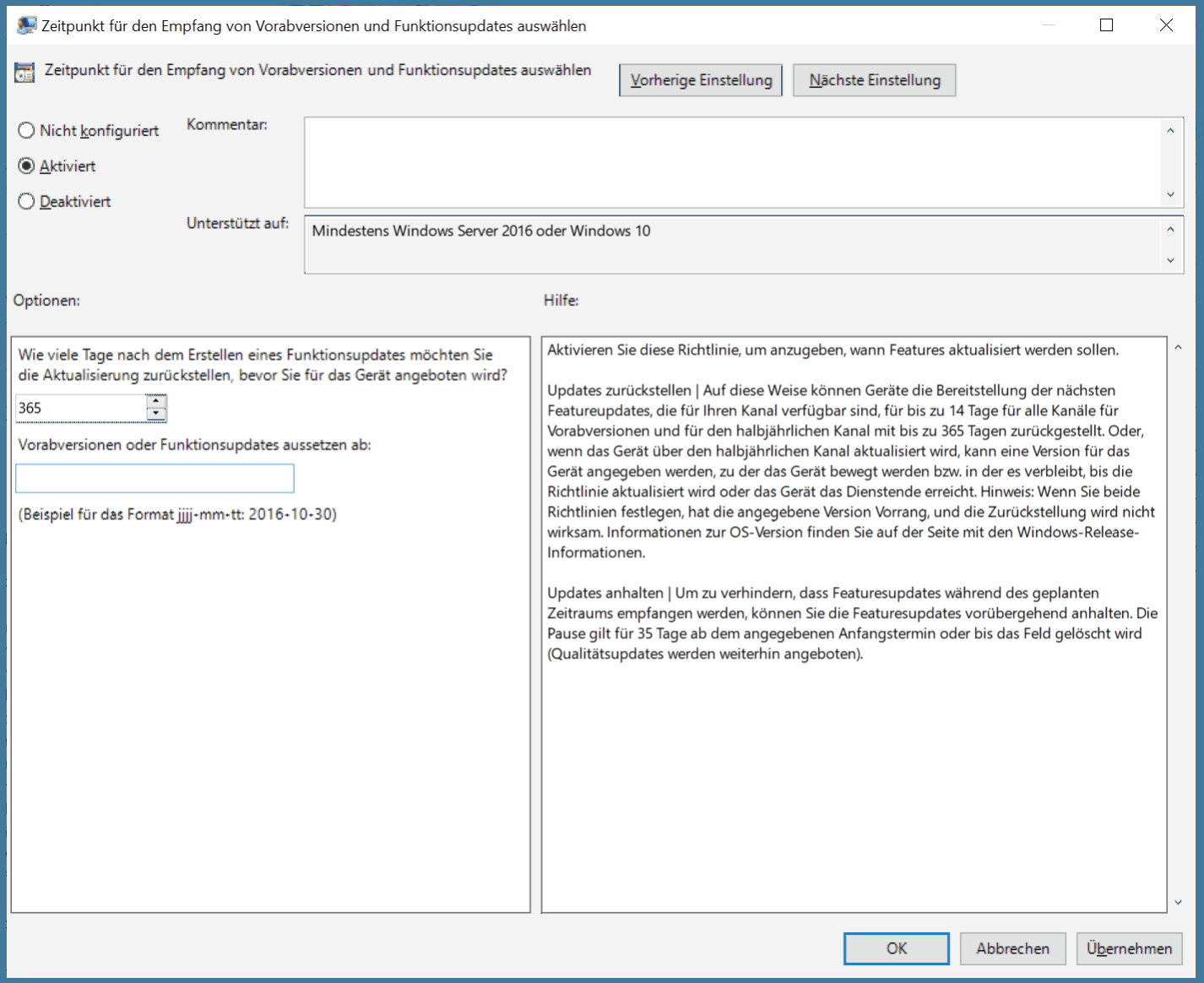
Für Admins, die WSUS für das Patchen von Windows nutzen, reduziert sich die Wahl des richtigen Zeitpunkts darauf, die Updates früh genug zu genehmigen, um die Sicherheit der Systeme zu gewährleisten bzw. nicht den Support-Zeitraum für das installierte Release zu überschreiten.

Stellt man jedoch auf WUfB um, dann muss das Einspielen von Updates mit Hilfe von Gruppenrichtlinien gesteuert werden. Die Optionen zum Aufschieben von Updates haben sich aber mehrfach verändert. Das betraf die maximal möglichen Fristen ebenso wie die laufenden Umstellungen bei den Verteilerringen.

Feature-Updates verzögern

Seit Windows 10 1903 heißt die Einstellung für diesen Zweck *Zeitpunkt für den Erhalt von Vorabversionen und Funktionsupdates auswählen* ("Select when Preview Builds and Feature Updates are received"). Hier kann man für Feature-Updates maximal 365 Tage einstellen.

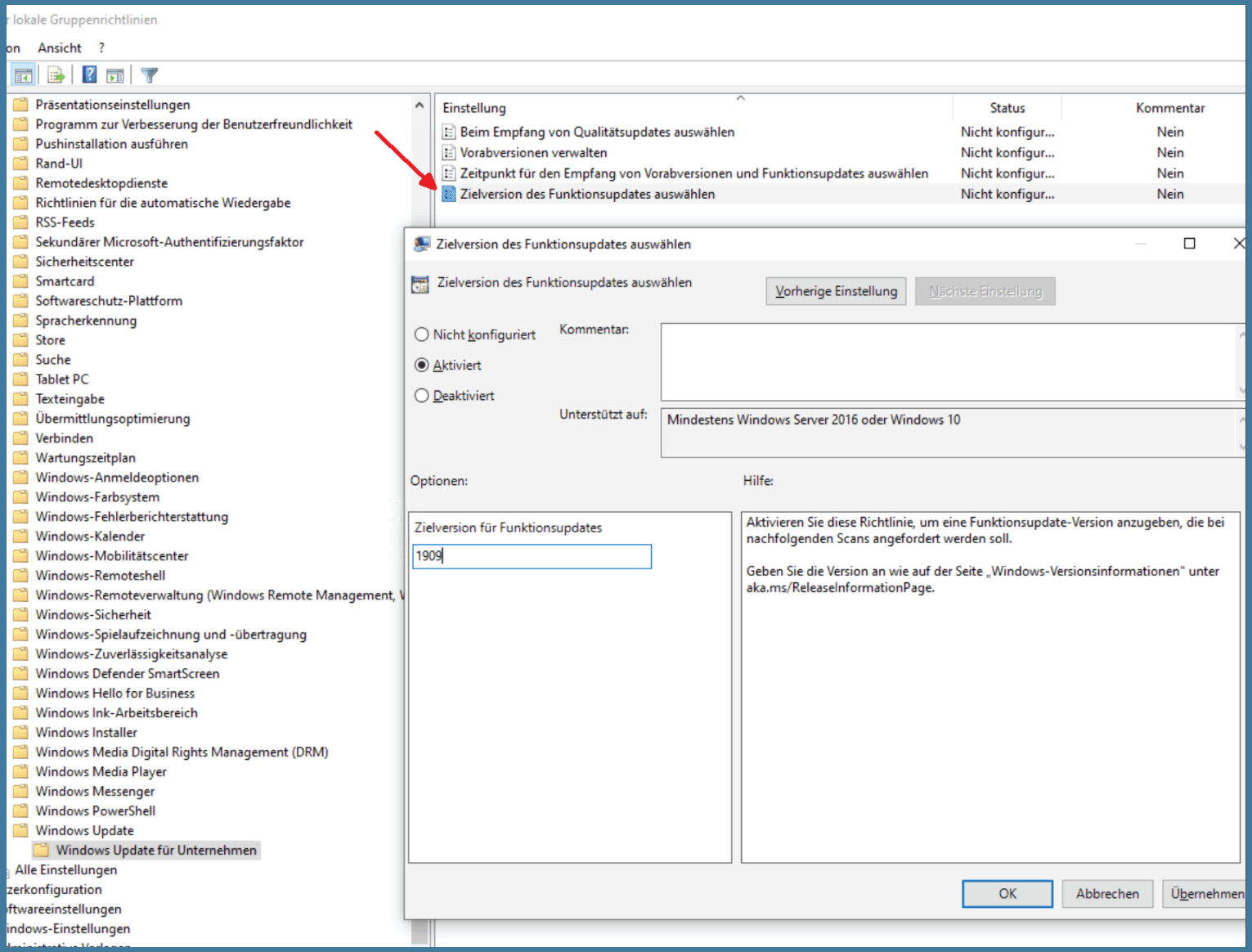
Darüber hinaus lassen sich die Updates über das Feld *Vorabversionen und Funktionsupdates aussetzen ab* bis zu 35 Tage nach dem angegebenen Datum pausieren. Theoretisch könnte man diese Einstellung alle 34 Tage um die volle Frist verlängern, um einen unbegrenzt langen Aufschub zu erreichen.



Aufschub von Feature-Updates über die entsprechende Einstellung in den Gruppenrichtlinien

Unbegrenzter Aufschub durch neue Einstellung

Da dies nicht sehr praktikabel ist, führte Microsoft mit Windows 10 2004 die Einstellung *Zielversion des Funktionsupdates auswählen* ein. Sie erlaubt es, eine beliebige zukünftige Version zu definieren, bis zu der alle Upgrades übersprungen werden. Dies betrifft auch das Upgrade von Windows 10 auf 11. Damit erhalten Admins den gleichen Spielraum für das Verteilen von Feature-Updates wie mit WSUS.



Der Scan für Feature-Updates lässt sich auf bestimmte Releases eingrenzen

Qualitäts-Updates

Beim Ausrollen von Qualitäts-Updates empfiehlt Microsoft, keinen zeitlichen Verzug festzulegen (mittels *Beim Empfang von Qualitätsupdates auswählen*, was die Übersetzung von *Select when Quality Updates are received* sein soll).

Vielmehr soll man hier mit der in 1903 eingeführten Einstellung *Stichtage für automatische Updates und Neustarts angeben* dafür sorgen, dass der Aufschub für Updates ab deren Erscheinen gezählt wird.

Inkrementelle Feature-Updates vorziehen

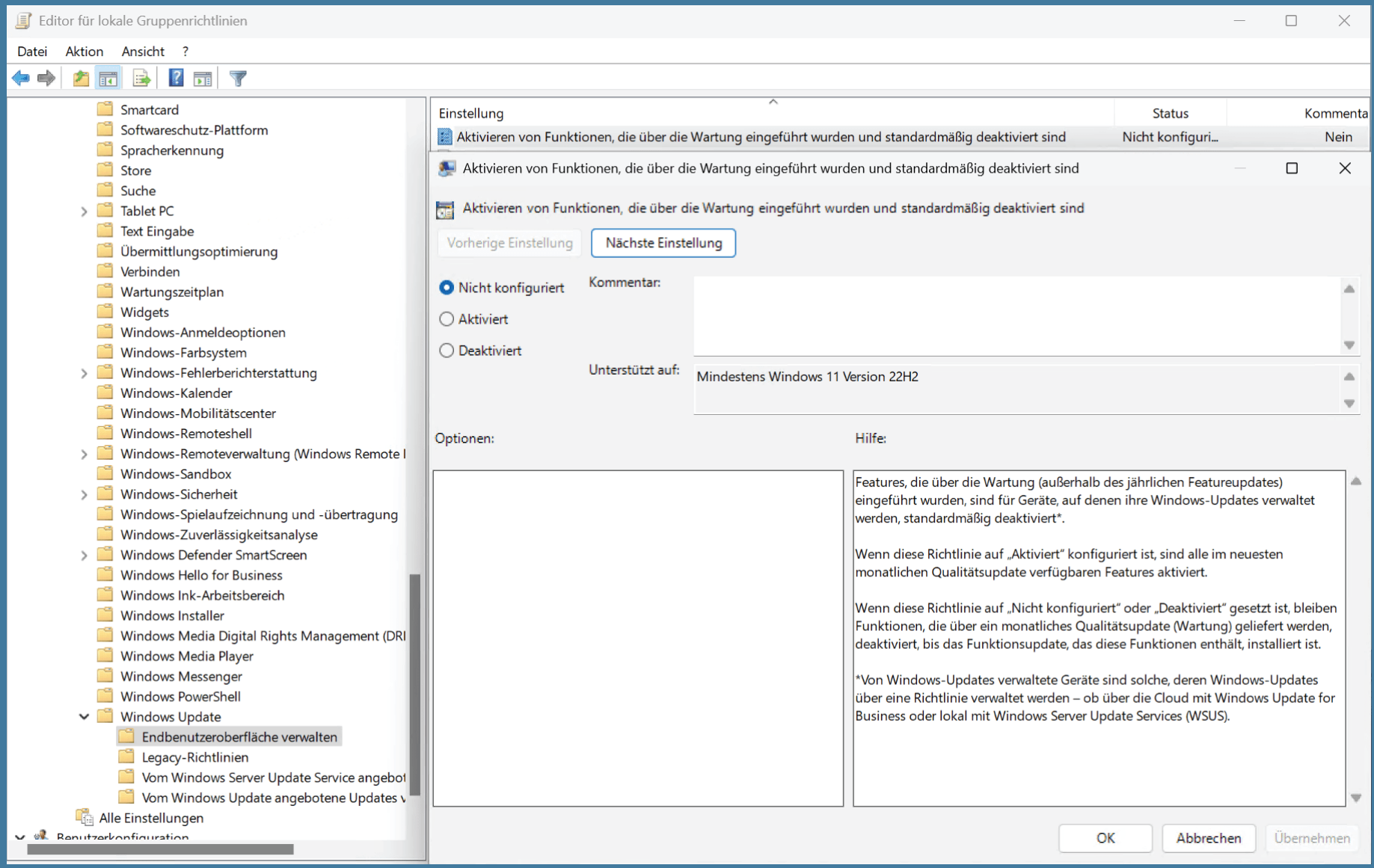
Die monatlichen kumulativen Updates (CUs) für Windows 11 enthalten nicht nur Security-Patches und Bugfixes, sondern regelmäßig auch neue Features. Je nachdem wie weit diese Neuerungen in das System eingreifen, können sie zu Kompatibilitätsproblemen mit bestehenden Anwendungen führen.

Größere Umstellungen auf der Bedieneroberfläche erfordern unter Umständen eine Einweisung der User in die neue Funktionalität, so dass Unternehmen diese koordiniert einführen möchten.

Die Neuerungen werden zwar mit den CUs heruntergeladen, bleiben auf verwalteten Geräten aber bis zur Installation des nächsten jährlichen Feature-Updates inaktiv. Als verwaltet gelten PCs, die ihre Updates entweder über Windows Update for Business oder über WSUS beziehen.

Wenn Unternehmen ihren Benutzern die neuen Features jedoch gleich zur Verfügung stellen möchten, dann können sie das Standardverhalten mit einer neuen Gruppenrichtlinie bzw. CSP-Policy (für MDM) überschreiben.

Die 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"). Sie befindet sich unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows Update => Endbenutzeroberfläche bearbeiten*. Bei der CSP-Policy handelt es sich um AllowTemporaryEnterpriseFeatureControl.



Die neue Gruppenrichtlinie, mit der sich die Aktivierung neuer Features in Windows 11 steuern lässt

Die neue Richtlinie wurde mit dem optionalen kumulativen Update im Februar 2023 für Windows 11 22H2 ausgeliefert und kann von dort in einen zentralen Store übernommen werden.

Wie man leicht erkennen kann, erlaubt die neue Richtlinie keine granulare Steuerung, sondern man hat damit nur die Möglichkeit, alle neuen Features bis zum nächsten OS-Release aufzuschieben oder sie sofort vollständig zuzulassen.

Technisch gesehen bedient sich Microsoft dabei desselben Verfahrens wie bei den letzten Feature-Updates von Windows 10 und 11. Auch dort erhielten Anwender die neuen Funktionen schon vorab über die kumulativen Updates, und ein so genanntes Enablement Package schaltete sie dann nur mehr frei.

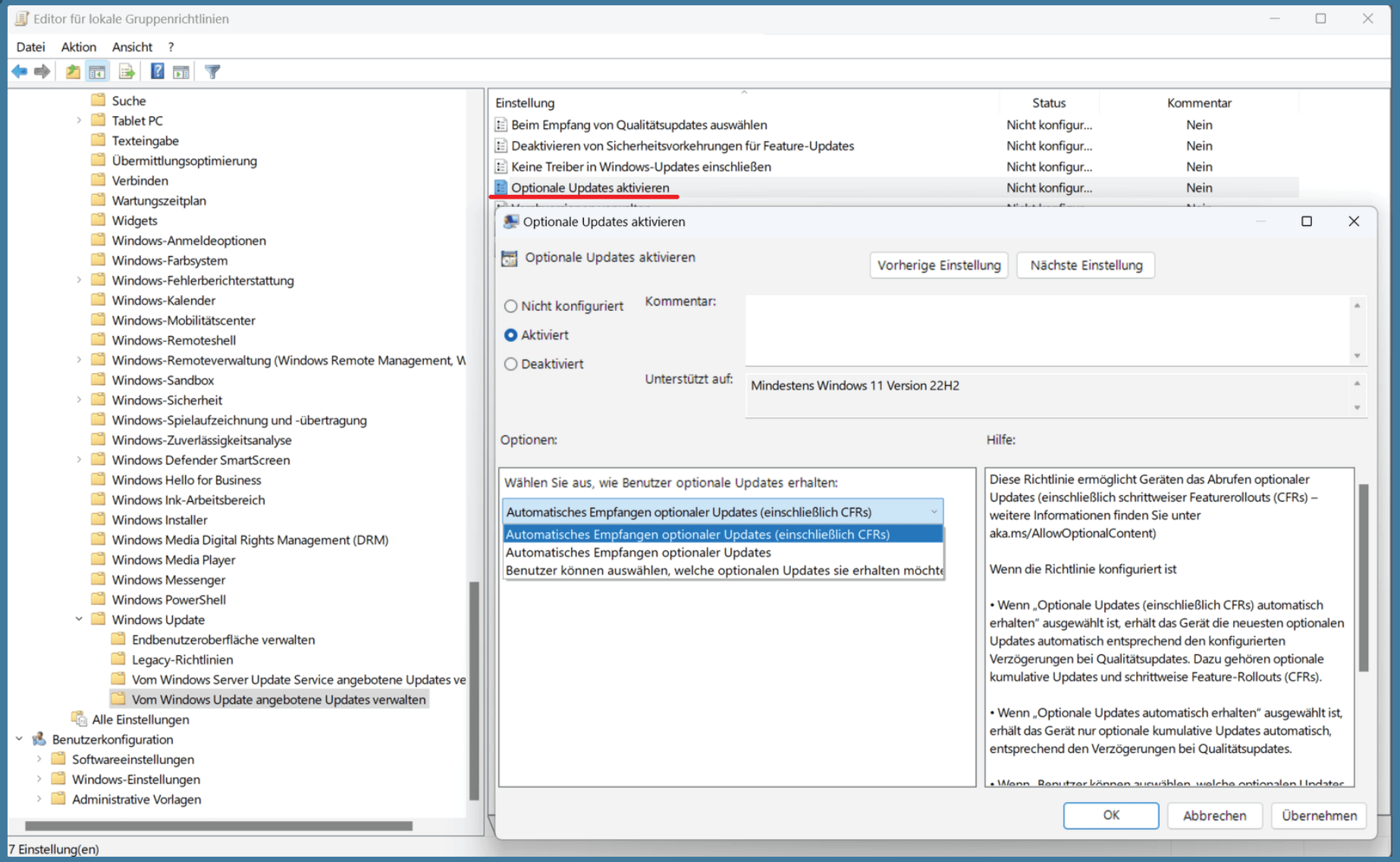
Optionale Updates automatisch installieren

Mit dem Update für August 2023 kam für Windows 11 22H2 eine weitere Richtlinie hinzu, mit der sich bestimmen lässt, wie optionale Updates installiert werden und wie Benutzer diesen Vorgang beeinflussen können.

Die Einstellung heißt *Optionale Updates aktivieren* ("Enable optional updates") und befindet sich unter *Computer¬konfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Windows-Update => Von Windows Update angebotene Updates verwalten.*

Nur für WUfB und Intune relevant

Aus dem Pfad für die Einstellung erkennt man, dass sie nur für Rechner gilt, die über Windows Update for Business (WUfB) aktualisiert bzw. über Intune verwaltet werden.



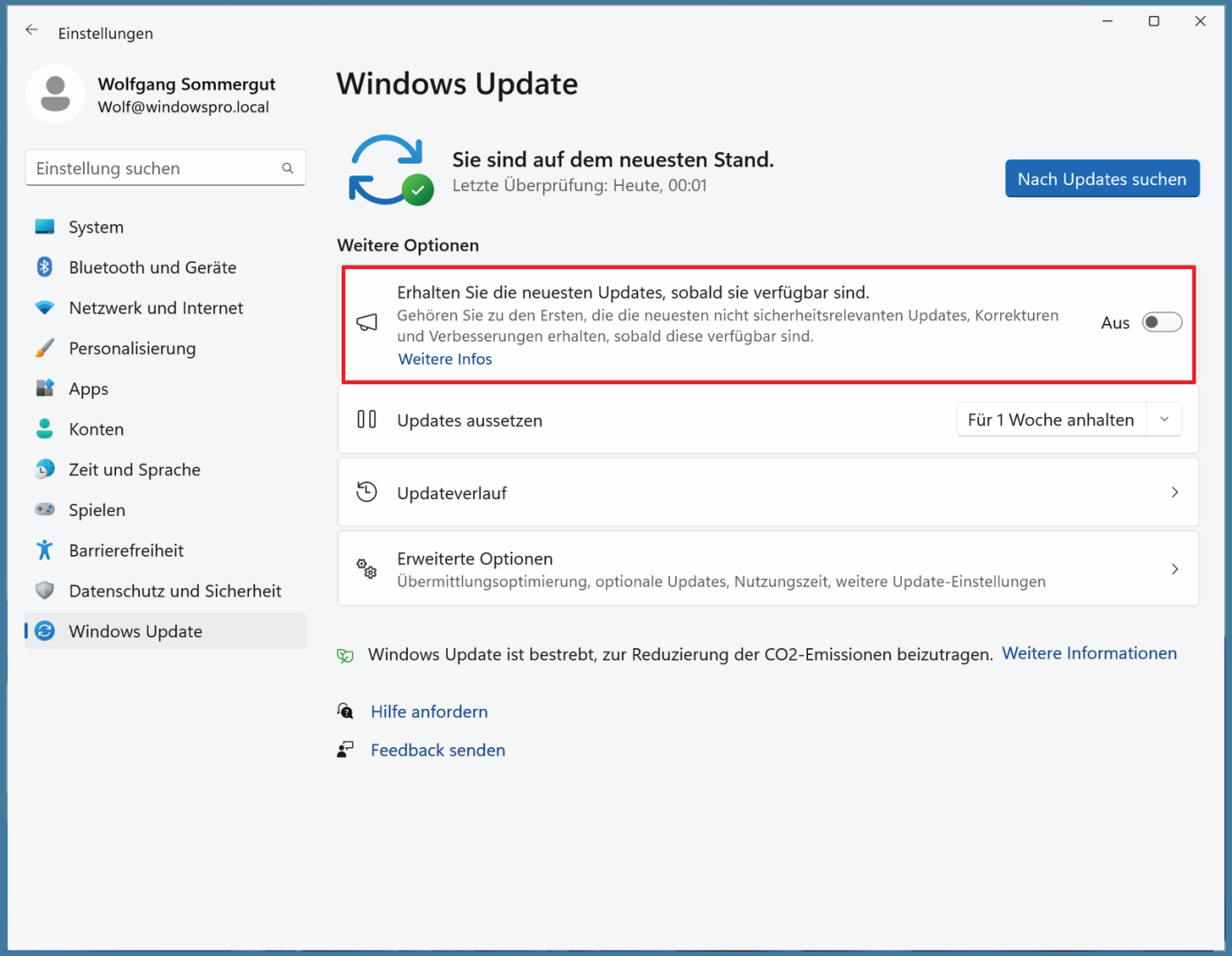
Neue Gruppenrichtlinie zur Installation von optionalen Updates

Wenn man sie nicht konfiguriert oder deaktiviert, dann ändert sich das bisherige Verhalten des PCs nicht, d.h., er erhält keine optionalen Updates. Allerdings können Endbenutzer dann über die App *Einstellungen* den Bezug der optionalen Updates nach eigenem Gutdünken konfigurieren.

Aktiviert man sie, dann bietet sie drei Optionen:

- Automatisches Empfangen optionaler Updates (einschließlich CFRs) ("Automatically receive optional updates (including CFRs)"): Damit erhalten Geräte die aktuellen Non-Security Updates inklusive der neuen Features (CFRs - Controlled Feature Rollouts);
- Automatisches Empfangen optionaler Updates ("Automatically receive optional updates"): Damit erhalten Geräte die aktuellen Non-Security Updates, aber ohne die neuen Features;
- Benutzer können auswählen, welche optionalen Updates sie erhalten möchten ("Users can select what optional updates to receive"): Die Anwender können bei dieser Option in der App *Einstellungen* selbst festlegen, wann optionale Updates installiert werden.

Die beiden ersten Optionen führen dazu, dass die optionalen Updates nach ihrem Erscheinen automatisch installiert werden, und zwar wahlweise mit bzw. ohne neue Features. In beiden Fällen blockiert das GPO dann in der App *Einstellung* die Option *Erhalten Sie die neuesten Updates, sobald sie verfügbar sind*.



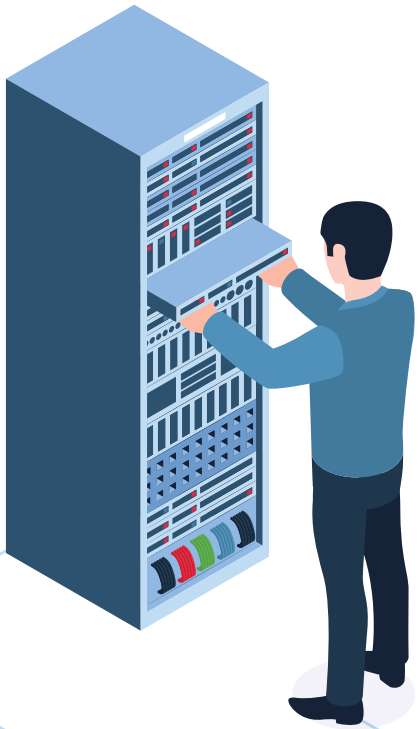
Das August-Update bringt auch eine neue Update-Option in der App Einstellungen

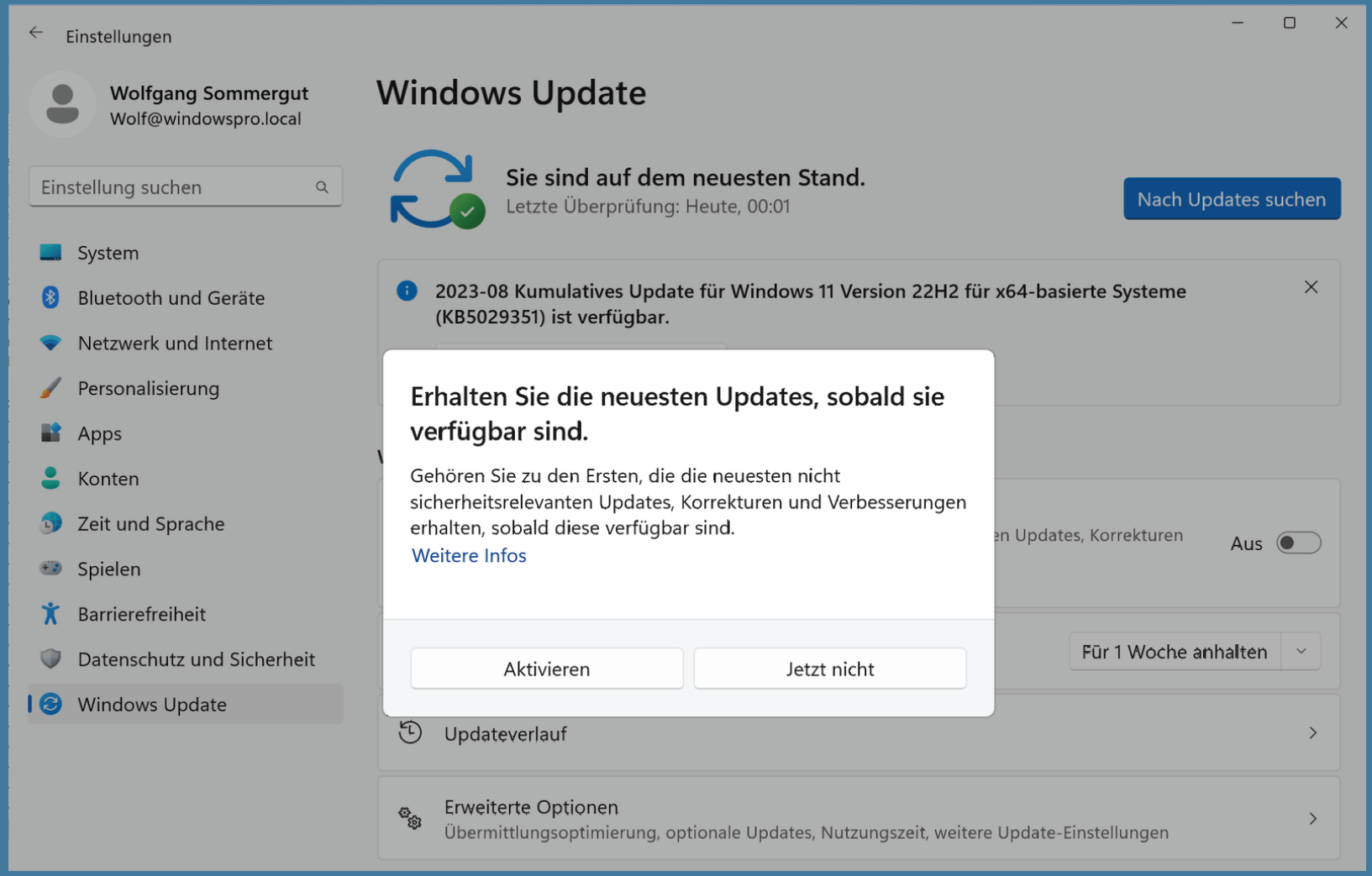
Wählt man hingegen die dritte Option, dann können Benutzer in der App Einstellungen selbst festlegen, ob sie optionale Updates bekommen möchten.

Entscheidet sich ein User dagegen, dann werden die optionalen Updates zwar heruntergeladen, aber er muss die Installation unter *Windows Update => Erweiterte Optionen => Optionale Updates* erst selbst auslösen. Darin sind auch neue Features enthalten, wobei Microsoft diese dann aber nicht unmittelbar nach ihrer Verfügbarkeit, sondern erst später installiert.

Aktivieren Benutzer hingegen in der App *Einstellungen* die Option *Erhalten Sie die neuesten Updates, sobald sie verfügbar sind*, dann verhält sich WUfB genauso wie bei der ersten Option der neuen Gruppenrichtlinie (automatische Installation optionaler Updates inklusive CFRs).

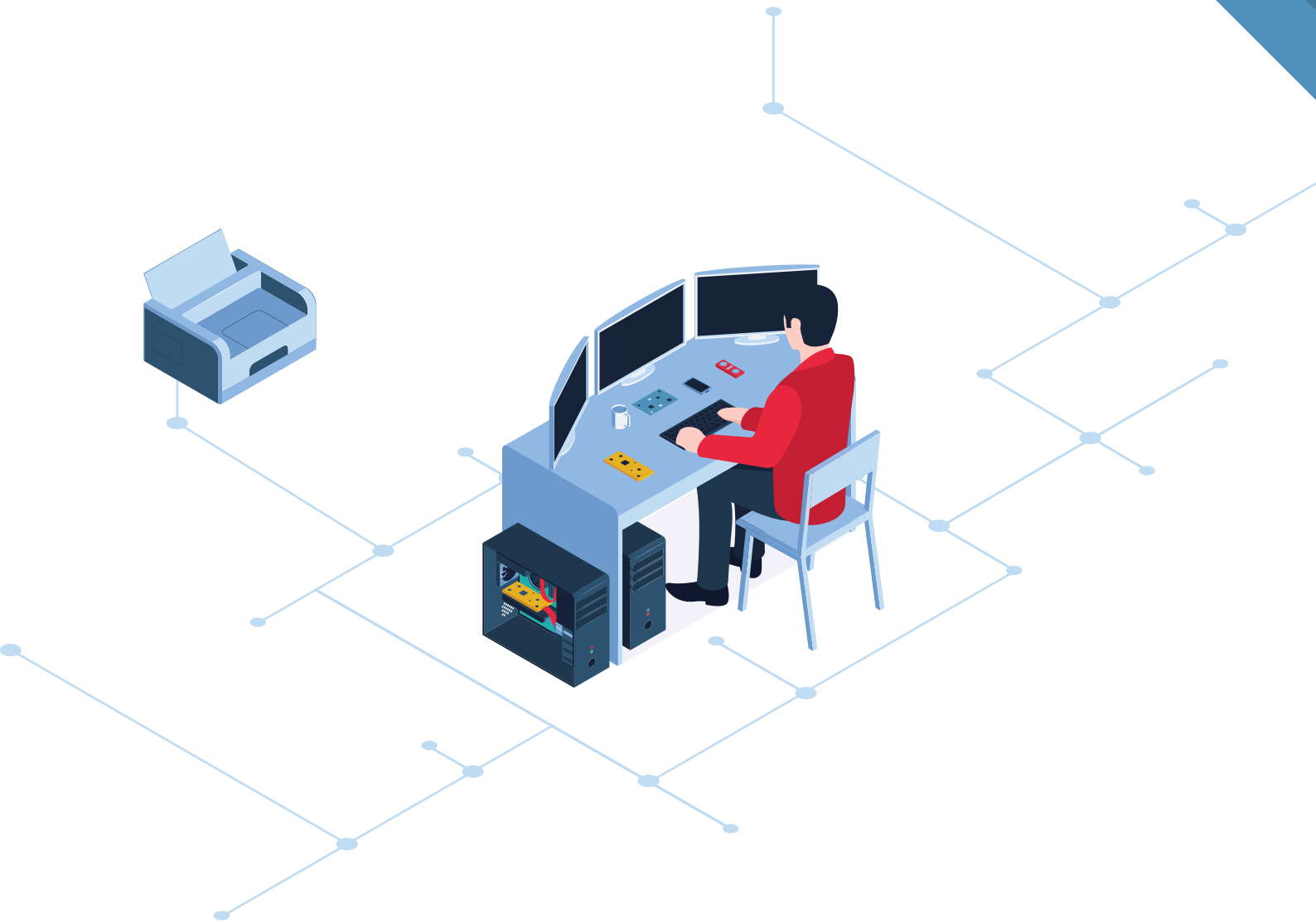
Bei der Installation fragt das August-Update die Benutzer schon vorab danach, für welche Variante sie sich entscheiden möchten.



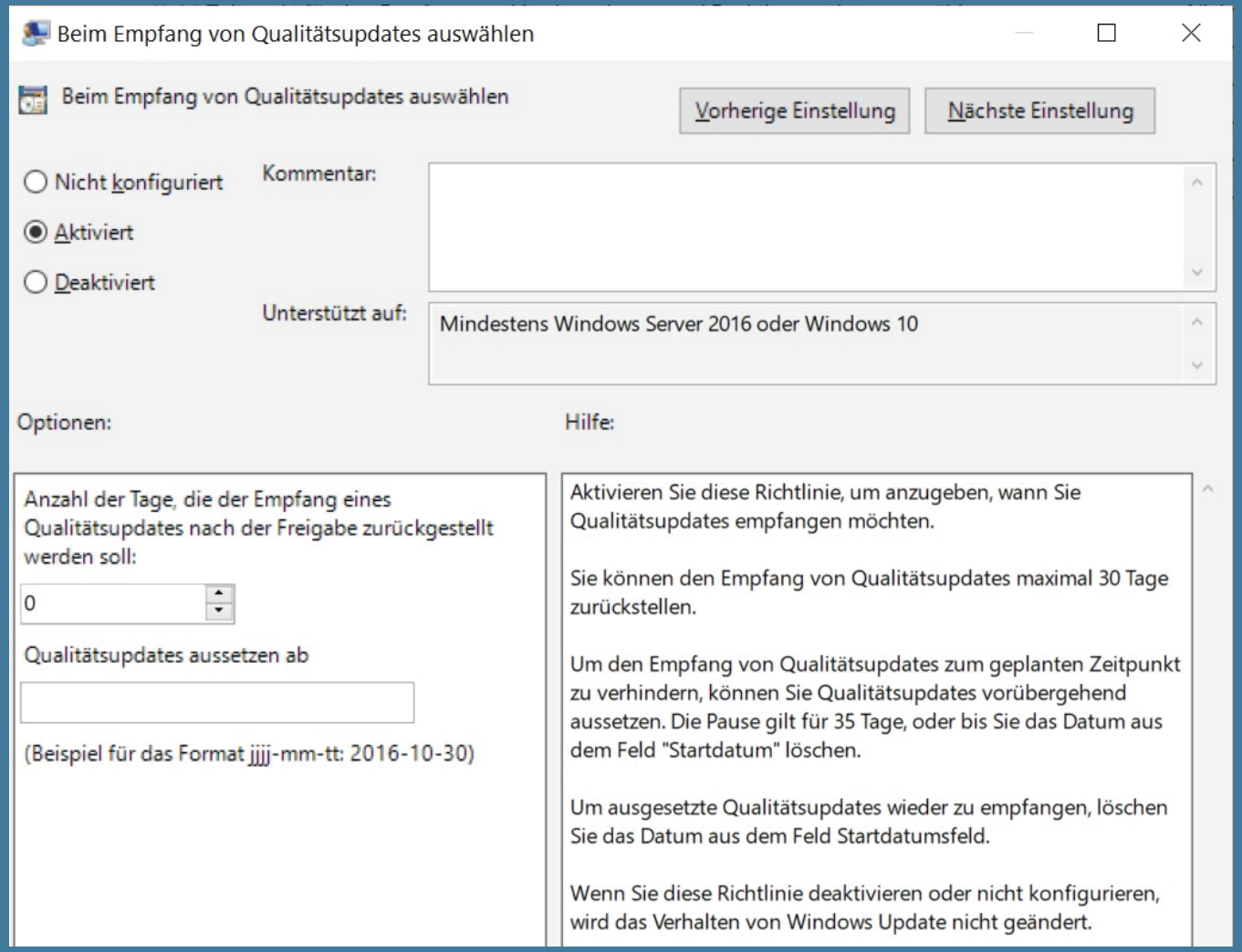


Das August-Update fragt Benutzer nach der gewünschten Einstellung für optionale Updates

Unabhängig davon, welche der drei Möglichkeiten man auswählt, die neue Gruppenrichtlinie respektiert grundsätzlich den Aufschub für optionale Updates, wenn man einen solchen konfiguriert hat.



Die neue Richtlinie erlaubt es Admins, optionale Updates für Windows 11 22H2 oder höher automatisch zu beziehen, wenn die PCs über Windows Update for Business aktualisiert werden. Neue Features kann man bei dieser Gelegenheit mit installieren oder auf sie verzichten.

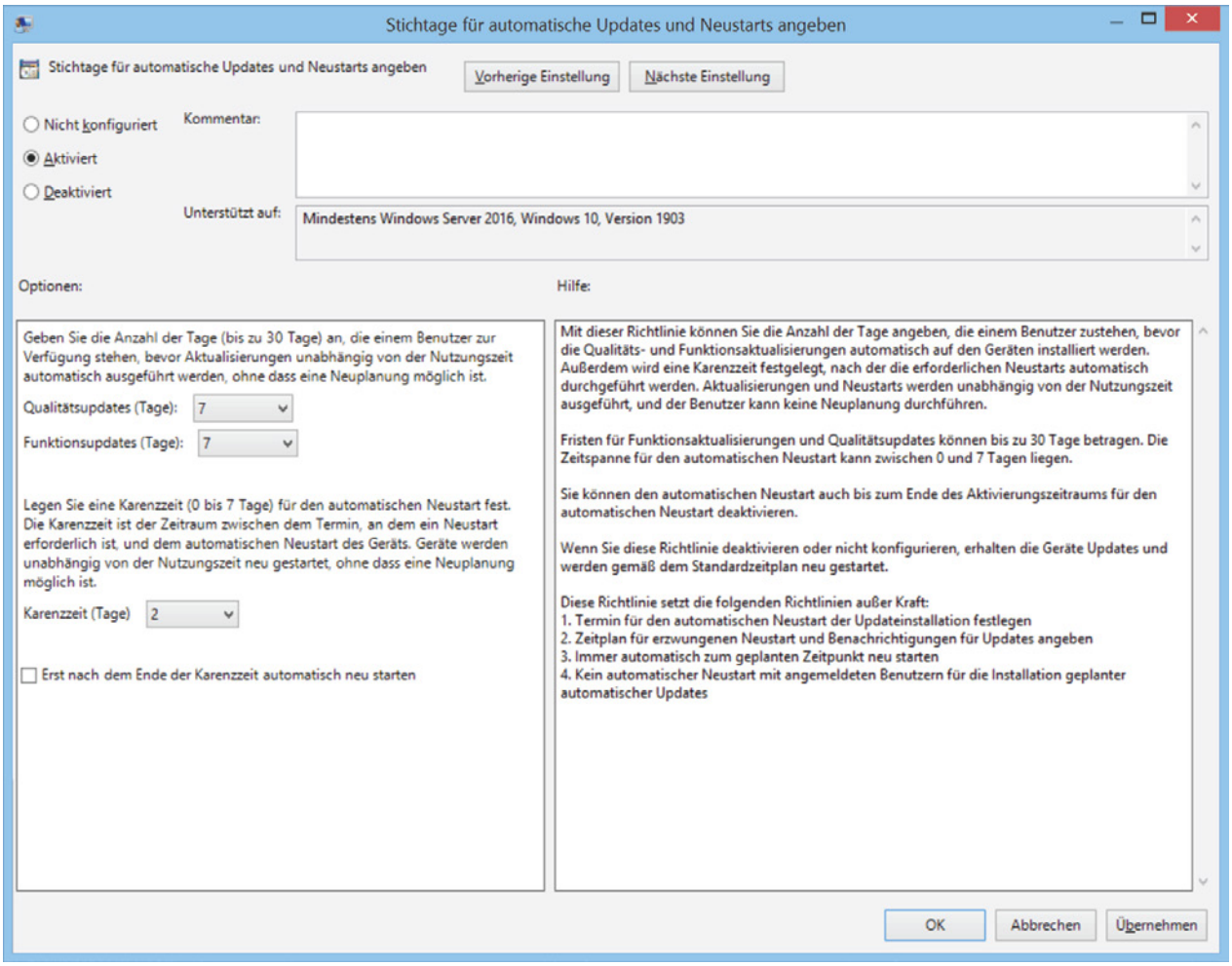


Das August-Update fragt Benutzer nach der gewünschten Einstellung für optionale Updates

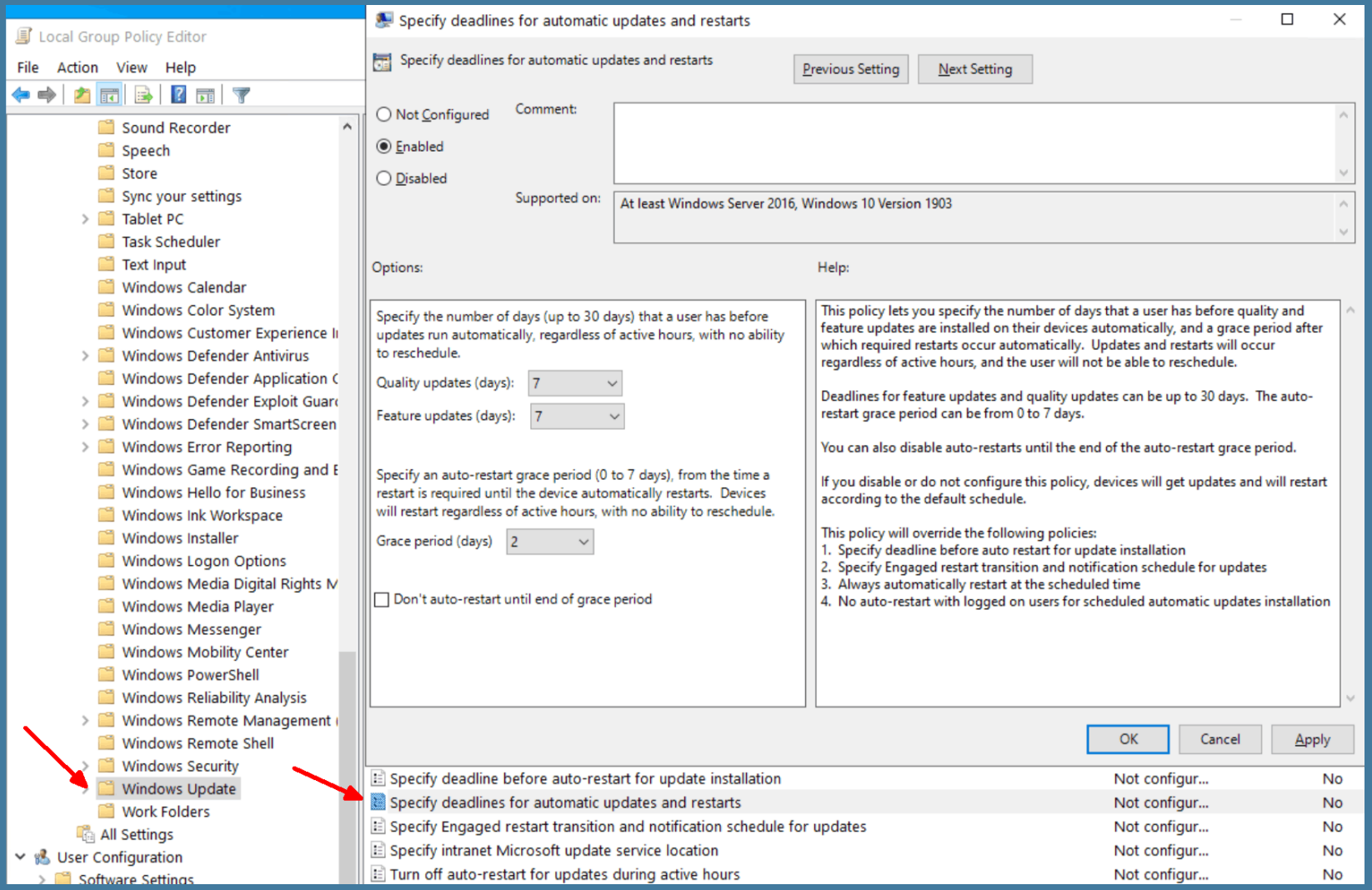
Reboot konfigurieren über Gruppenrichtlinien

Um den Zeitpunkt für den Download und die Installation von Updates sowie für den Neustart des Rechners zu bestimmen, führte Microsoft immer wieder neue Konzepte ein. Das Bestreben bei allen Methoden besteht darin, sicherheitskritische Updates möglichst schnell auf die Rechner zu bringen und den Neustart so legen, dass sich die Benutzer dadurch nicht allzu sehr gestört fühlen.

Die neue Einstellung *Stichtage für automatische Updates und Neustarts* angeben soll vor allem dafür sorgen, dass Updates möglichst schnell verteilt werden. Daher gelten dort die konfigurierten Fristen bereits ab dem Erscheinungsdatum der Patches.



Mit dieser Einstellung für Windows Update lässt sich das Einspielen von Patches innerhalb einer bestimmten Frist erzwingen



Alte und neue Einstellung zur Konfiguration der Update-Fristen im englischen GPO-Editor

Alle früheren Optionen für die Steuerung von Reboots begannen erst ab dem Zeitpunkt zu zählen, an dem das Update installiert und ein Neustart fällig war.

Das gilt etwa für *Frist festlegen, nach der ein ausstehender Neustart außerhalb der Nutzungszeit automatisch ausgeführt wird*. Diese Einstellung wurde erst mit Windows 10 eingeführt und ist der Vorgänger der neuen Option. Das erkennt man sofort, wenn man den englischen GPO-Editor nutzt.

Da heißt die bisherige Einstellung *Specify the deadline before a pending restart will automatically be executed outside of active hours* während die neue auf *Specify deadlines for automatic updates and restarts* lautet.

Beide erlauben die Festlegung einer jeweils eigenen Frist für Qualitäts- und Feature-Updates, und zwar maximal 30 Tage (Vorgabe sind 7 Tage). Nach ihrem Ablauf kann der Anwender den Neustart des Rechners nicht mehr aufschieben, so dass Updates unmittelbar danach wirksam werden.

Der gleiche Zeitraum steht Admins in Windows Update for Business zur Verfügung, um Qualitäts-Updates aufzuschieben. Nachdem die Uhr bei der neuen Einstellung ab Erscheinen eines Updates tickt, lässt sich dadurch aber keine zusätzliche Zeit gewinnen.

Diese Einstellung bietet noch zwei weitere Optionen, und zwar zur Definition einer Karenzzeit sowie eine Möglichkeit, um diese Schonfrist voll auszuschöpfen.

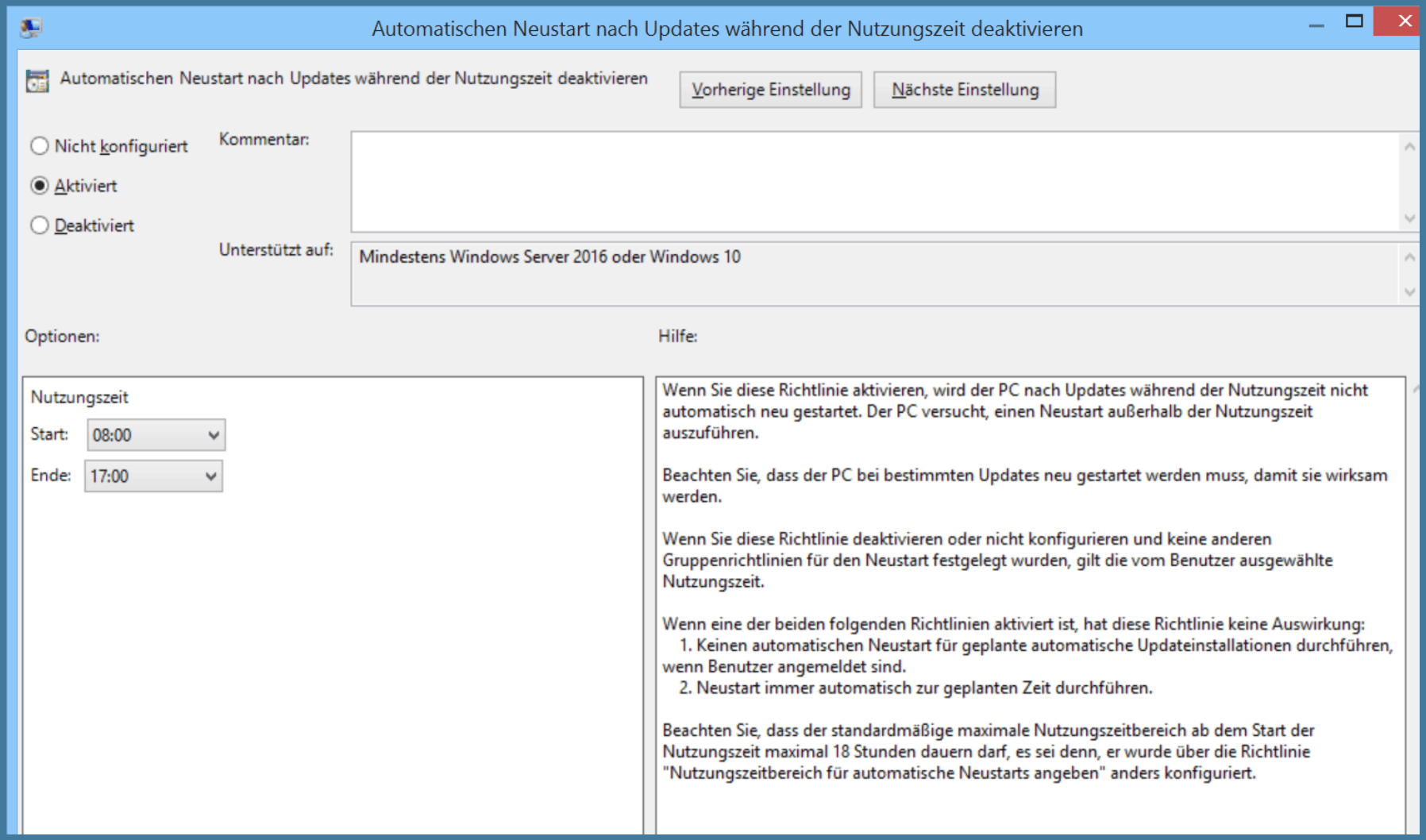
Die zusätzliche Gnadenfrist ("Karenzzeit") bewirkt, dass Benutzer nach einer längeren Abwesenheit, etwa wegen Urlaubs, ihren Rechner nicht sofort neu starten müssen, kaum dass sie mit der Arbeit begonnen haben.

Zusammenspiel mit Active Hours

Darüber hinaus kann ein Admin den Anwendern noch weiteren Spielraum gewähren, indem er die Option *Erst nach dem Ende der Karenzzeit automatisch neu starten* aktiviert. Sie führt dazu, dass Rechner innerhalb der gesetzten Frist nur durch einen manuellen Reboot aktualisiert werden. Setzt man dieses Häkchen nicht, dann versucht Windows bereits vorher, außerhalb der Nutzungszeit ("Active hours") einen günstigen Zeitpunkt für einen Neustart zu finden.

Nach Ablauf der Gnadenfrist nimmt Windows Update auch darauf keine Rücksicht mehr und zwingt den Benutzer zu einem Reboot sogar während der Arbeitszeit.

Diese Option hat die gleiche Wirkung wie die Einstellung *Automatischen Neustart nach Updates während der Nutzungszeit deaktivieren* ("Turn off auto-restart for updates during active hours "). Diese erfordert aber eine statische Festlegung der Nutzungszeit.



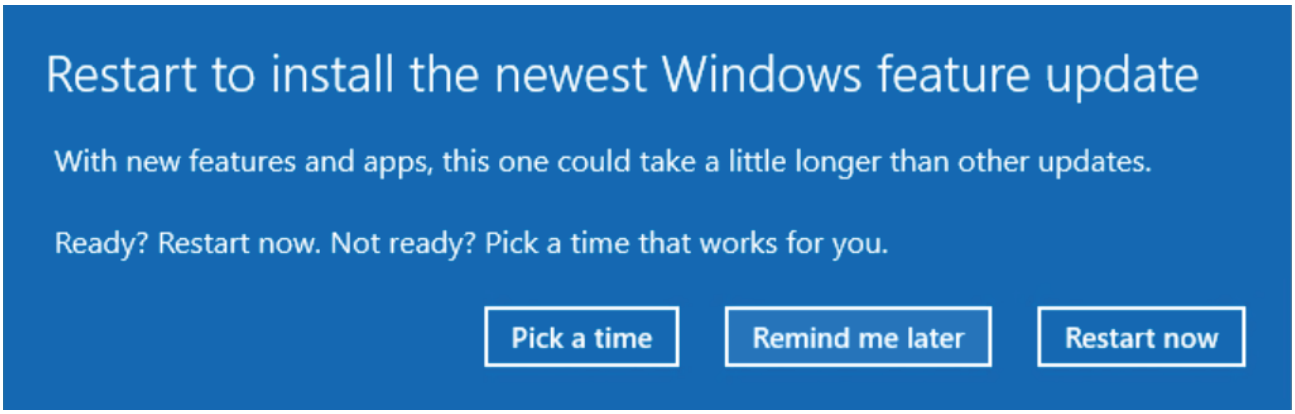
Möchte man Neustarts während der Nutzungszeit verhindern, dann muss man dafür die Uhrzeiten festlegen

Seit der Version 1903 ermittelt Windows 10 die Active Hours aber selbständig anhand der User-Aktivitäten. Wenn man dieses Feature nutzen möchte, sollte man daher auf die Eingabe von festen Uhrzeiten verzichten.

Umstellung von Info-Dialog auf Erinnerung

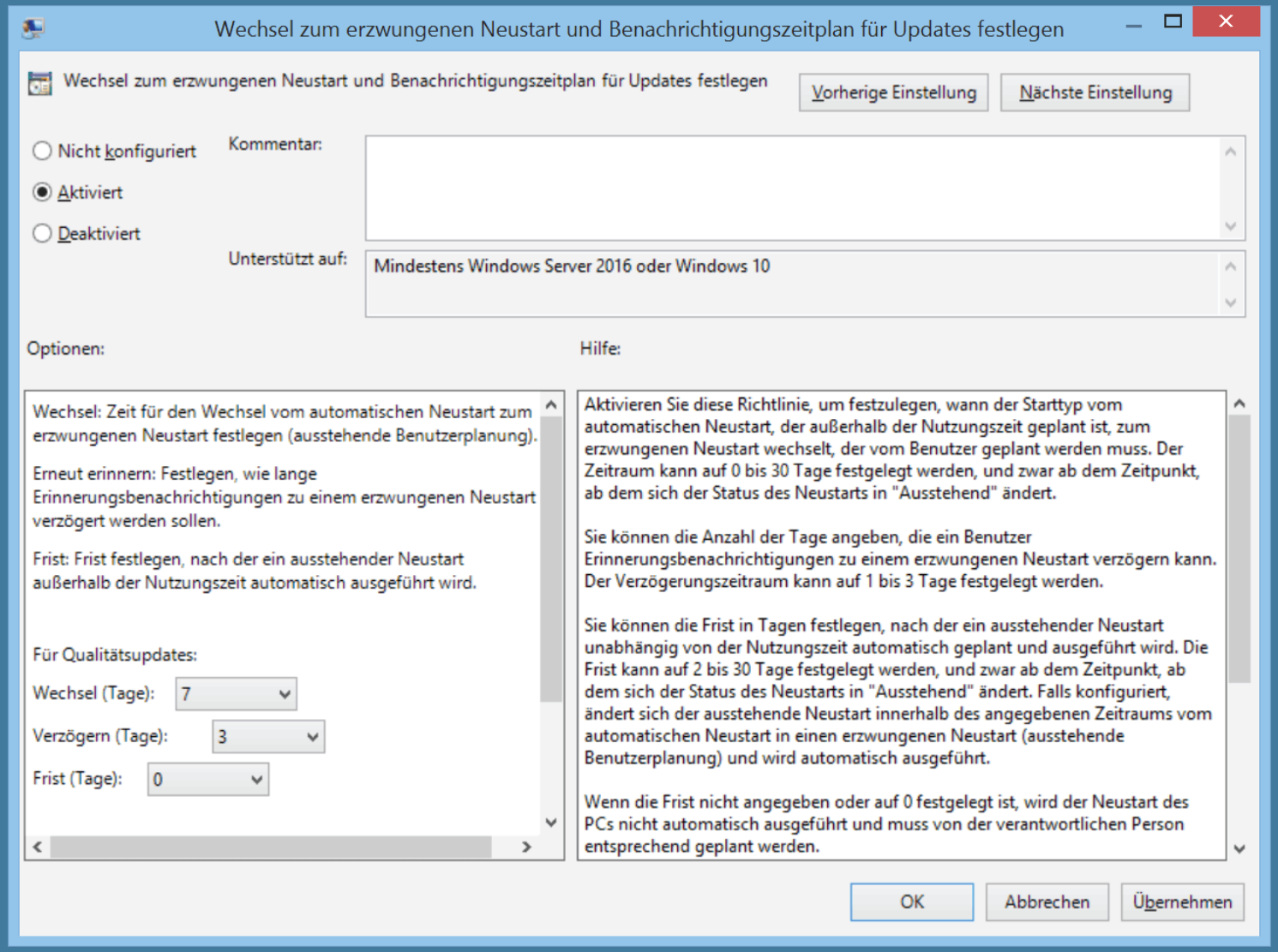
Während der definierten Frist ändert der Update-Client die Ansprache gegenüber dem Benutzer. In den ersten Tagen macht es ihn über Toast-Benachrichtigung auf ein anstehendes Update aufmerksam.

Danach wechselt es automatisch auf eine verbindliche Erinnerung ("Engaged restart reminder"), bei welcher der User einen Reboot sofort veranlassen, für einen bestimmten Zeitpunkt planen oder einfach aufschieben kann.



Nach einigen Tagen schaltet Windows 10 auf die nachdrückliche Erinnerung um

Die explizite Umstellung von der Toast-Nachricht auf die dringlichere Variante bewirkt man über die Einstellung *Wechsel zum erzwungenen Neustart und Benachrichtigungszeitplan für Updates festlegen* ("Specify Engaged restart transition and notification schedule for updates"). Dabei kann man die Fristen selbst bestimmen.



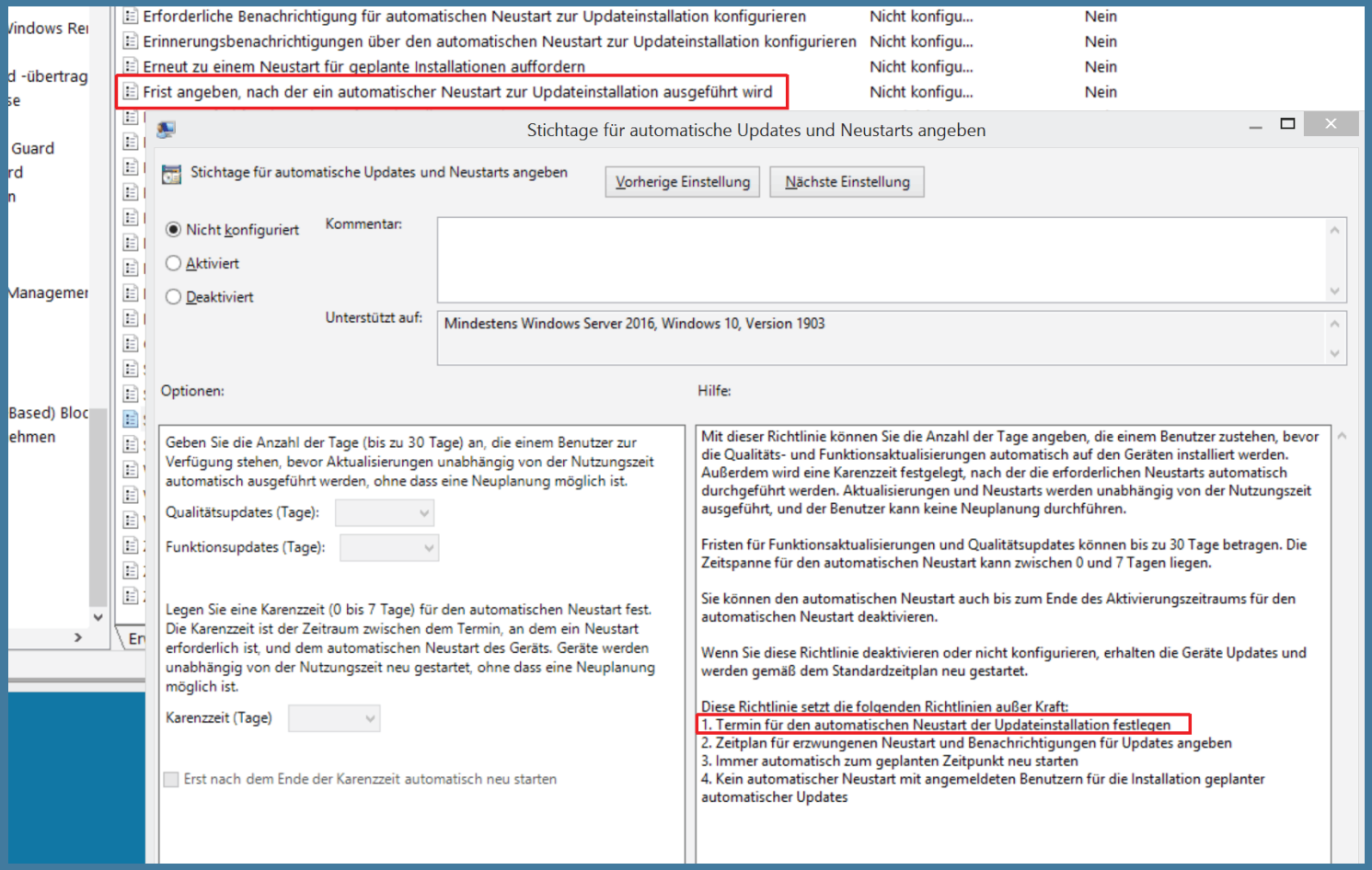
Die Umstellung der Benachrichtigung über anstehende Updates ließ sich bisher exakt konfigurieren.
Die neue Option verhindert das

Sie wird aber durch die neue Einstellung zur Planung des Neustarts ("Stichtage für automatische Updates und Neustarts angeben") außer Kraft gesetzt. Diese Option zeigt sich also wesentlich resoluter als die Vorgängervariante, die sich bei Konflikten immer selbst deaktivierte.

Neue Einstellung deaktiviert vier alte

Die Absicht, mit einer einzigen Einstellung das Verhalten für die Installation von Updates und den Neustart weitgehend vorzugeben, zeigt sich auch durch den Wegfall einer weiteren Option. Bis dato konnte man den Reboot verhindern, solange ein Benutzer angemeldet war. Die neue Einstellung kümmert sich jedoch nicht darum.

In Summe setzt sie vier bisherige Settings außer Kraft, falls diese aktiviert sind. Verwendet man den deutschen GPO-Editor, dann kann man nicht erkennen, welche das sind, weil die Übersetzungen der Optionen voneinander abweichen.



Aufgrund der schlechten Übersetzung ist im deutschen GPO-Editor nicht erkennbar, welche Einstellungen deaktiviert werden

Es handelt sich dabei um:

- Frist festlegen, nach der ein ausstehender Neustart außerhalb der Nutzungszeit automatisch ausgeführt wird.
- Wechsel zum erzwungenen Neustart und Benachrichtigungszeitplan für Updates festlegen
- Neustart immer automatisch zur geplanten Zeit durchführen
- Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind

Insgesamt ist es das Ziel der geänderten Reboot-Policy, das Verteilen von Updates zu beschleunigen, indem die Benutzer den Neustart des Rechners maximal 30 Tage nach dem Erscheinen eines Updates verzögern dürfen.

Übermittlungsoptimierung (WUDO) konfigurieren

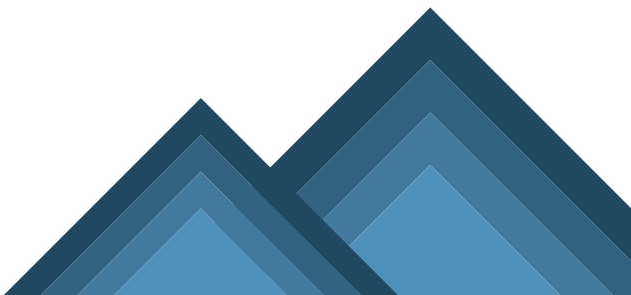
Die kontinuierlichen Upgrades des Betriebssystems sowie die regelmäßigen Patches erzeugen einen erheblichen Traffic. Innerhalb eines Standorts oder einer Hauptniederlassung stellt dies gewöhnlich kein Problem dar. Anders sieht es dagegen in Zweigstellen oder kleinen Firmen aus, die nur über ein WAN angebunden sind.

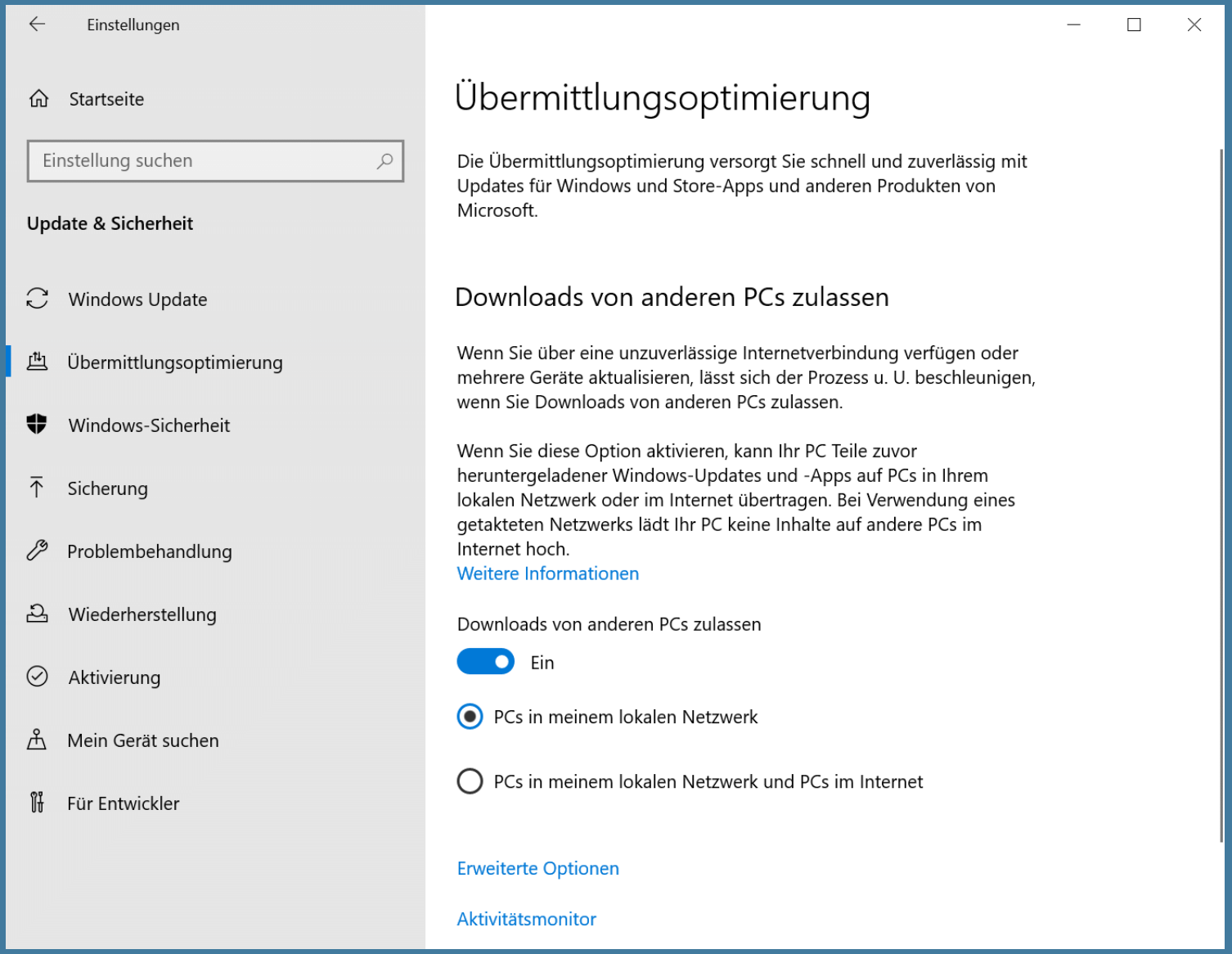
Hier ist es nicht wünschenswert, dass alle Rechner ihre Updates einzeln von Microsoft Update oder von einem WSUS in der Hauptniederlassung beziehen. Daher können PCs dank WUDO als Cache für die anderen Computer einspringen. Das Feature lässt sich über GPOs oder MDM-Schnittstellen konfigurieren.

Seit Windows 10 1709 verarbeitet WUDO neben Feature- und Qualitäts-Updates für Windows, Treibern, sowie Dateien aus dem Store auch Click-to-Run-Updates für Office. Mit dem Release 2004 kam die Unterstützung für herkömmliche Office-Updates und MSIX hinzu.

Die Übermittlungsoptimierung ist standardmäßig in allen Editionen von Windows aktiviert. In der Enterprise Edition beschränkt es sich aber auf das Caching von Update-Dateien im LAN, während die Consumer-Varianten auch Rechner über das Internet einbinden.

Grundsätzlich können auch Windows Server ihre Updates von PCs im Netzwerk beziehen, per Voreinstellung ist die Übermittlungsoptimierung dort jedoch abgeschaltet.





Auf einem frisch installierten Windows 10 ist die Übermittlungsoptimierung per Voreinstellung aktiviert

Dabei werden alle heruntergeladenen Dateien verschlüsselt und signiert, so dass sich eine Manipulation ausschließen lässt. Bei der Übertragung von zwischengespeicherten Inhalten verzichtet Microsoft zudem auf die Nutzung von Netzwerken, die als getaktet markiert sind.

Voraussetzung für die Übermittlungsoptimierung ist, dass die Rechner mit dem Internet verbunden sind, weil die Orchestrierung der Caches über einen Cloud-Service erfolgt.

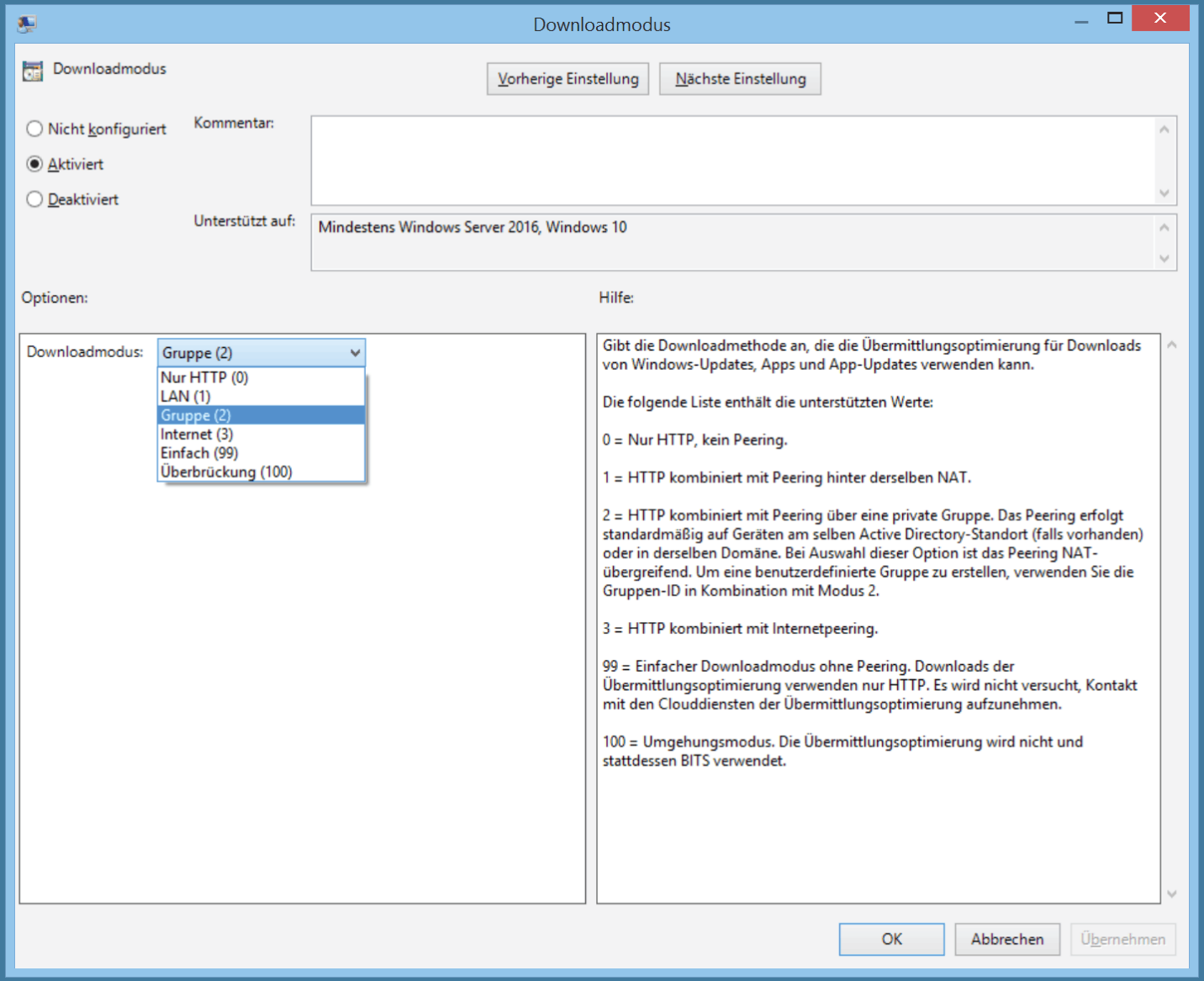
Gruppierung von PCs für Übermittlungsoptimierung

Damit sich die Clients gegenseitig die Updates effizient zuspielen können, ist es wichtig, sie passend zur Netzwerktopologie in Gruppen zusammenzufassen. Bei der erwähnten Option, Inhalte nur für PCs im gleichen Netzwerk bereitzustellen, packt WUDO einfach alle Rechner in eine Gruppe, die über die gleiche öffentliche IP (sprich: gleiche Firewall) an das Internet angebunden sind.

Wenn die solchermaßen gruppierten Clients jedoch über mehrere Standorte verteilt und über ein langsames Netzwerk verbunden sind, dann wird man eher das Gegenteil des gewünschten Ergebnisses erreichen. Obendrein geht dann der Transfer der Cache-Inhalte zu Lasten anderer Anwendungen.

Aus diesem Grund bietet die Gruppenrichtlinie *Downloadmodus* unter *Computerkonfiguration => Richtlinien => Administrative Vorlagen => Windows-Komponenten => Übermittlungsoptimierung* weitere Einstellungen, um Windows-PCs in Gruppen einzusortieren:

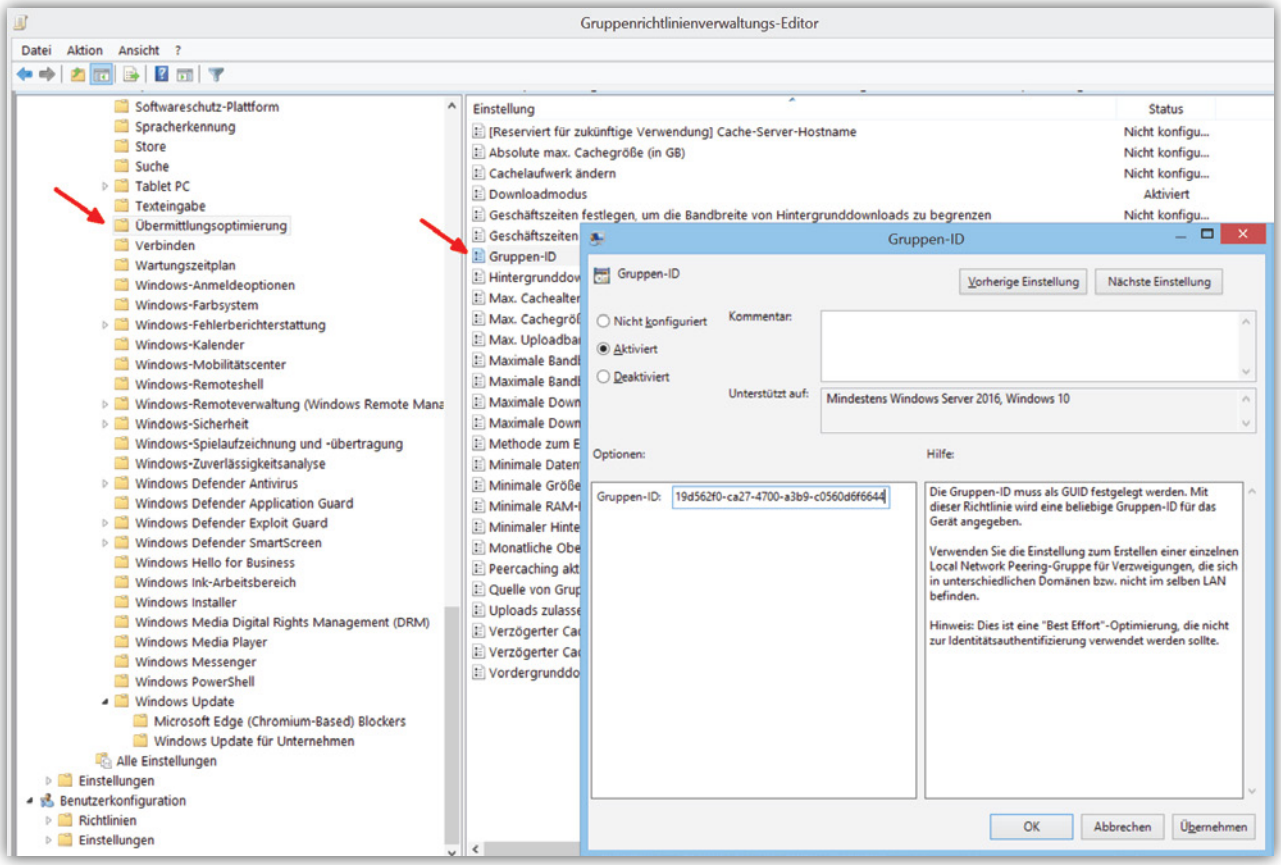
- Nur http (0): Das Feature wird de facto deaktiviert, da kein Peering erfolgt
- LAN (1): Nur PCs im gleichen NAT-Netzwerk können als Cache fungieren
- Gruppe (2): Sendet und empfängt Updates von/zu Rechnern im LAN, die der gleichen Domäne angehören
- Internet (3): Auch Computer außerhalb des Firmennetzes dienen als Quelle und Ziel für Updates



Über die Einstellung Downloadmodus lässt sich das Feature einschränken oder abschalten

Microsoft empfiehlt die Verwendung von *Gruppe (2)*. Dabei erfolgt das Peering standardmäßig zwischen Geräten derselben Active Directory-Site, oder falls nicht vorhanden, in derselben Domäne.

Wenn die Domänen-basierte Gruppe zu groß wäre oder AD-Sites nicht an der Netzwerktopologie ausgerichtet sind, dann bieten sich alternative Möglichkeiten, Peers zusammenzufassen.



Rechner lassen sich über eine gemeinsame GUID zu einer Update-Gruppe zusammenfassen

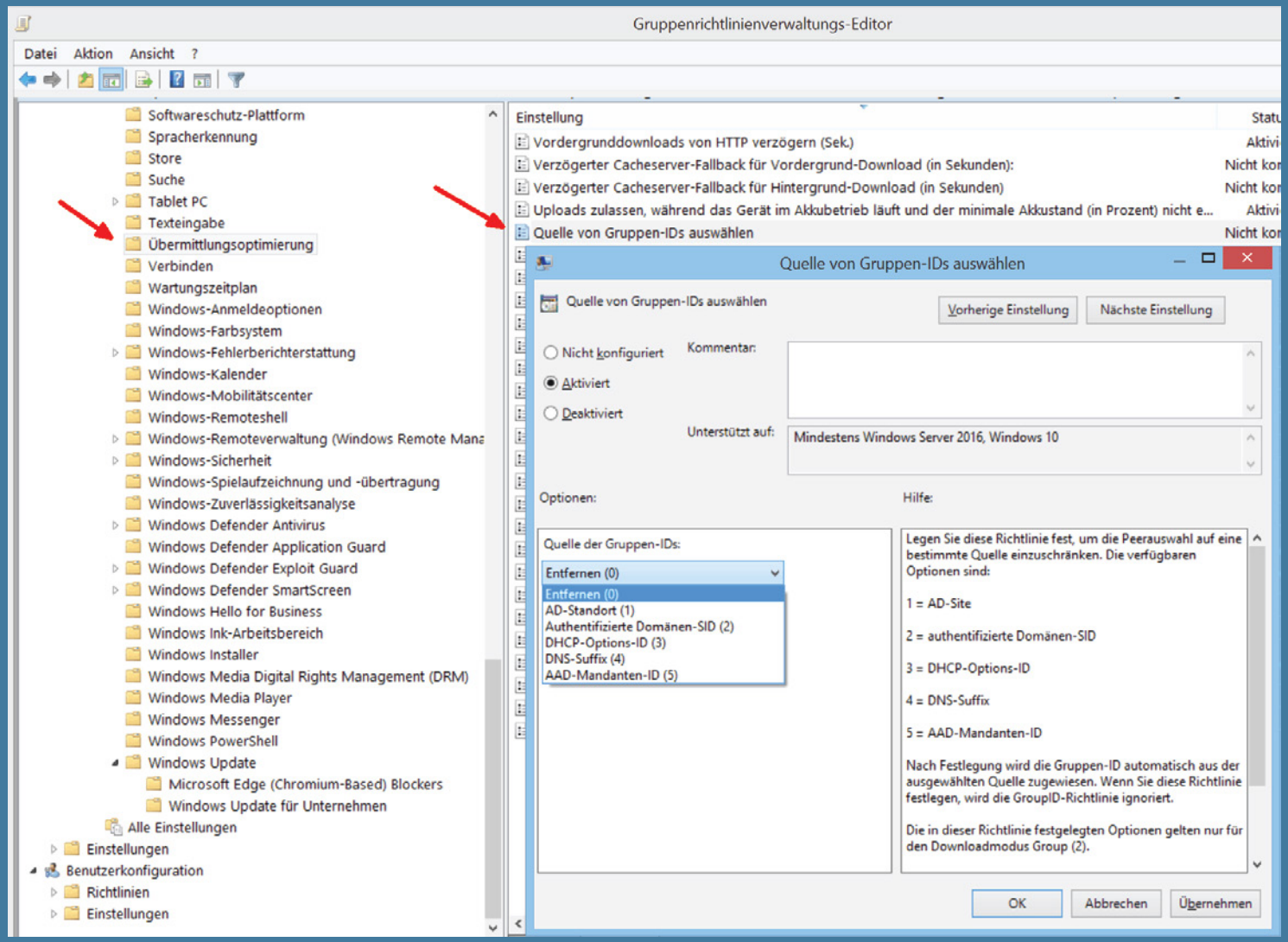
So lassen sich PCs alternativ zu Gruppen zusammenschließen, indem man ihnen über die Einstellung Gruppen-ID die gleiche GUID zuweist. Eine solche könnte man in PowerShell mit diesem Befehl generieren:

```
[guid]::NewGuid()
```

Idealerweise befinden sich die betreffenden Rechner dafür in den gleichen organisatorischen Einheiten, so dass man sie mit der gleichen ID versehen kann, indem man das GPO mit diesen OUs verknüpft.

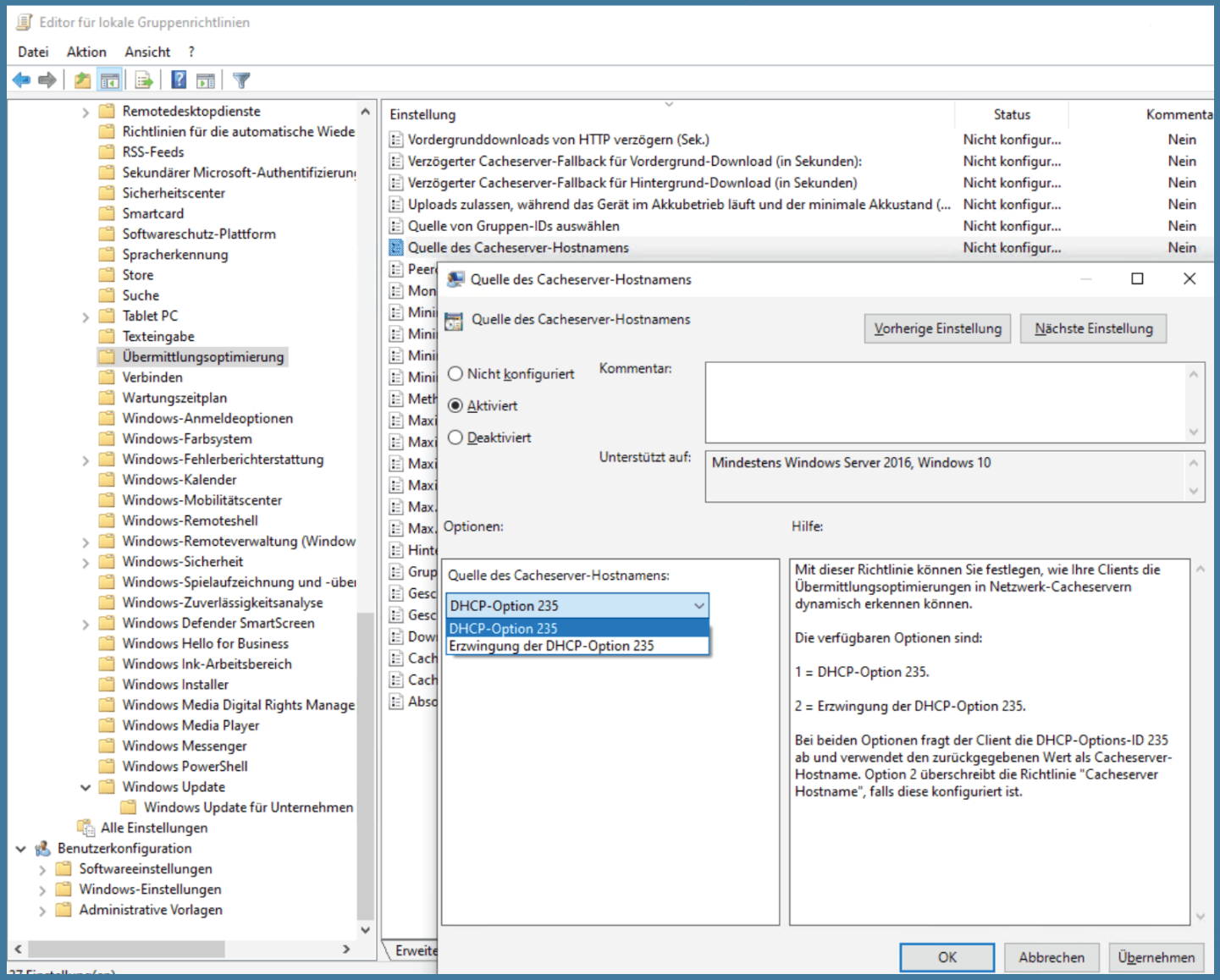
Eignet sich die GPO-Verknüpfung nicht, um die gewünschten PCs für WUDO zu organisieren, dann bietet *Quelle für Gruppen-IDs auswählen* weitere Optionen. Diese Einstellung überlagert die Gruppen-ID.

Zu den zusätzlichen Kriterien gehört dort neben dem gemeinsamen DNS-Suffix vor allem die Zuteilung einer GUID über die DHCP-Option 234. Sie bietet sich besonders dann an, wenn sich auf diesem Weg bestimmte Subnets gezielt erreichen lassen.



Alternative Methoden, um Rechner für die Übermittlungsoptimierung in Gruppen zu organisieren

Eine weitere Einstellung dient dazu, den Clients einen Cache-Host über DHCP (Option 235) zuzuweisen. Sie heißt *Quelle des Cacheserver-Hostnamens*. Mit dem Wert 2 erzwingt man diese Form der Zuordnung, auch wenn sie bereits auf andere Weise festgelegt wurde, zum Beispiel über die GPO-Einstellung *Cacheserver Hostname*.



Einstellung, um den Cache-Host über DHCP zuzuweisen

VPN-Management

Wenn Benutzer über ein VPN an das Firmennetz angeschlossen sind, dann handelt es sich dabei oft um relativ langsame Verbindungen. In diesem Fall ist es nicht wünschenswert, dass solche Remote-PCs als Update-Cache für die Rechner im LAN dienen.

Die Delivery Optimization versucht selbständig herauszufinden, ob ein Rechner via VPN angebunden ist, indem es den Typ des Netzadapters prüft und zudem schaut, ob dessen Beschreibung bestimmte Schlüsselwörter wie "VPN" oder "secure" enthält.

Trifft dies zu, dann deaktiviert WUDO alle Peer-to-Peer-Aktivitäten. Möchte man dieses Standardverhalten ändern, dann kann man dies mit der Einstellung *Peercaching aktivieren, während das Gerät über ein VPN verbunden ist* tun.

Bandbreitenkontrolle

Die Gruppenrichtlinien bieten darüber hinaus zahlreiche Einstellungen unabhängig vom Typ der Verbindung, um die Belastung des Netzwerks durch die Kommunikation zwischen den Peers zu kontrollieren.

Sie reichen von maximalen Download-Bandbreiten (in Prozent oder seit Windows 10 2004 auch absolut) im Vorder- und Hintergrund über monatliche Obergrenzen in GB bis zur Festlegung von Geschäftszeiten, in denen sich das übertragene Volumen limitieren lässt.

Einstellung	Status	Kommentar
[Reserviert für zukünftige Verwendung] Cache-Server-Hostname	Nicht konfigu...	Nein
Absolute max. Cachegröße (in GB)	Nicht konfigu...	Nein
Cachelaufwerk ändern	Nicht konfigu...	Nein
Downloadmodus	Aktiviert	Nein
Geschäftszeiten festlegen, um die Bandbreite von Hintergrunddownloads zu begre...	Nicht konfigu...	Nein
Geschäftszeiten festlegen, um die Bandbreite von Vordergrunddownloads zu begre...	Nicht konfigu...	Nein
Gruppen-ID	Nicht konfigu...	Nein
Hintergrunddownloads von HTTP verzögern (Sek.)	Aktiviert	Nein
Max. Cachealter (in Sekunden)	Aktiviert	Nein
Max. Cachegröße (in Prozent)	Nicht konfigu...	Nein
Max. Uploadbandbreite (in KB/s)	Nicht konfigu...	Nein
Maximale Bandbreite für Downloads im Hintergrund (Prozent)	Nicht konfigu...	Nein
Maximale Bandbreite für Downloads im Vordergrund (Prozent)	Nicht konfigu...	Nein
Maximale Downloadbandbreite (in KB/s)	Nicht konfigu...	Nein
Maximale Downloadbandbreite (in Prozent)	Nicht konfigu...	Nein
Methode zum Einschränken der Peerauswahl auswählen	Nicht konfigu...	Nein
Minimale Datenträgergröße, die zur Verwendung des Peercachings zulässig ist (in ...	Nicht konfigu...	Nein
Minimale Größe der Inhaltsdatei für das Peercaching (in MB)	Aktiviert	Nein
Minimale RAM-Kapazität (einschließlich), die zur Verwendung des Peercachings erf...	Nicht konfigu...	Nein
Minimaler Hintergrund-QoS-Wert (in KB/s)	Nicht konfigu...	Nein
Monatliche Obergrenze für Uploaddaten (in GB)	Nicht konfigu...	Nein
Peercaching aktivieren, während das Gerät über ein VPN verbunden ist	Nicht konfigu...	Nein
Quelle von Gruppen-IDs auswählen	Nicht konfigu...	Nein
Uploads zulassen, während das Gerät im Akkubetrieb läuft und der minimale Akkus...	Aktiviert	Nein
Verzögerter Cacheserver-Fallback für Hintergrund-Download (in Sekunden)	Nicht konfigu...	Nein
Verzögerter Cacheserver-Fallback für Vordergrund-Download (in Sekunden):	Nicht konfigu...	Nein
Vordergrunddownloads von HTTP verzögern (Sek.)	Aktiviert	Nein

Mehrere Einstellungen helfen dabei, die Überlastung des Netzwerks durch die WUDO zu vermeiden

WUDO überwachen und Aktivitäten auswerten

Hat man die Delivery Optimization entsprechend den eigenen Anforderungen und Gegebenheiten konfiguriert, dann wird man wissen wollen, ob sich dieses Feature auch so verhält wie geplant. Dazu kann man auf einzelnen Rechnern in der App *Einstellungen* unter *Update und Sicherheit => Übermittlungsoptimierung* den *Aktivitätsmonitor* starten.

Wesentlich mehr Informationen erhält man mit PowerShell. Dafür sind in Windows 10 2004 die Cmdlets *Get-DeliveryOptimizationStatus* und *Get-DeliveryOptimizationLogAnalysis* dazugekommen. Das erste erlaubt einen Einblick in Peer-to-Peer-Aktivitäten wie IP-Adressen oder gesendete und empfangene Bytes.

Das zweite liefert eine Zusammenfassung der WUDO-Logs, darunter die Zahl der heruntergeladenen Dateien, Downloads von anderen PCs im Netz und der Effizienz insgesamt. Der Schalter *ListConnections* informiert über die Peer-to-Peer-Verbindungen.

Für die Problemanalyse kann man zudem mit *Enable-DeliveryOptimizationVerboseLogs* eine detaillierte Aufzeichnung starten.

Best Practices mit Update Baseline

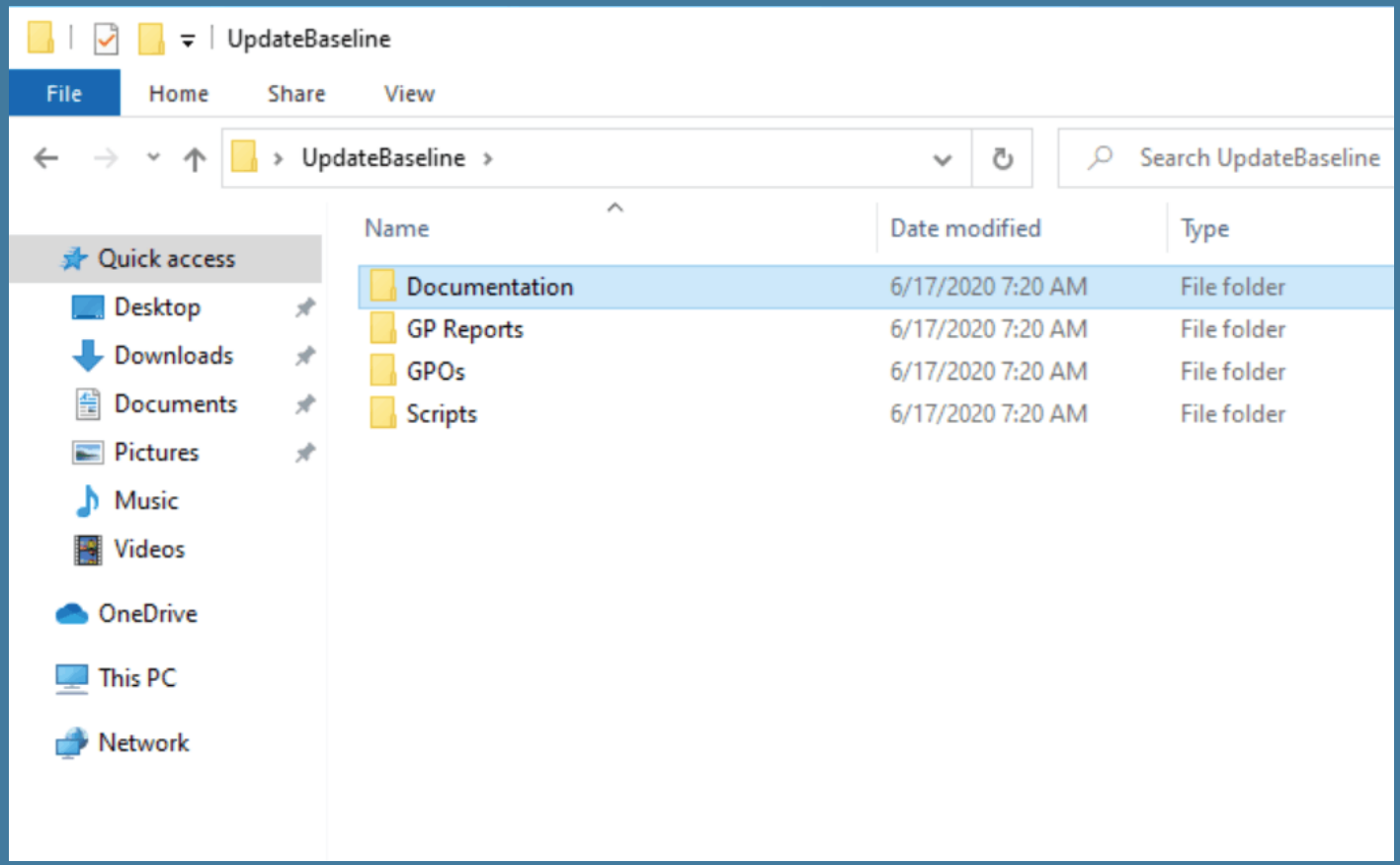
Microsoft stellt ein Toolkit namens Update Baseline zur Verfügung, das alle empfohlenen Gruppenrichtlinien zur Installation von Updates konfiguriert. Die Einstellungen betreffen neben Windows Update die Übermittlungsoptimierung und das Energie-Management.

Das große Aufräumen bei den GPO-Einstellungen für Windows Update spiegelt sich auch in der Update Baseline wider. Sie deaktiviert einen Großteil der über die Jahre gewachsenen Optionen.

Unvollständiges Script für den GPO-Import

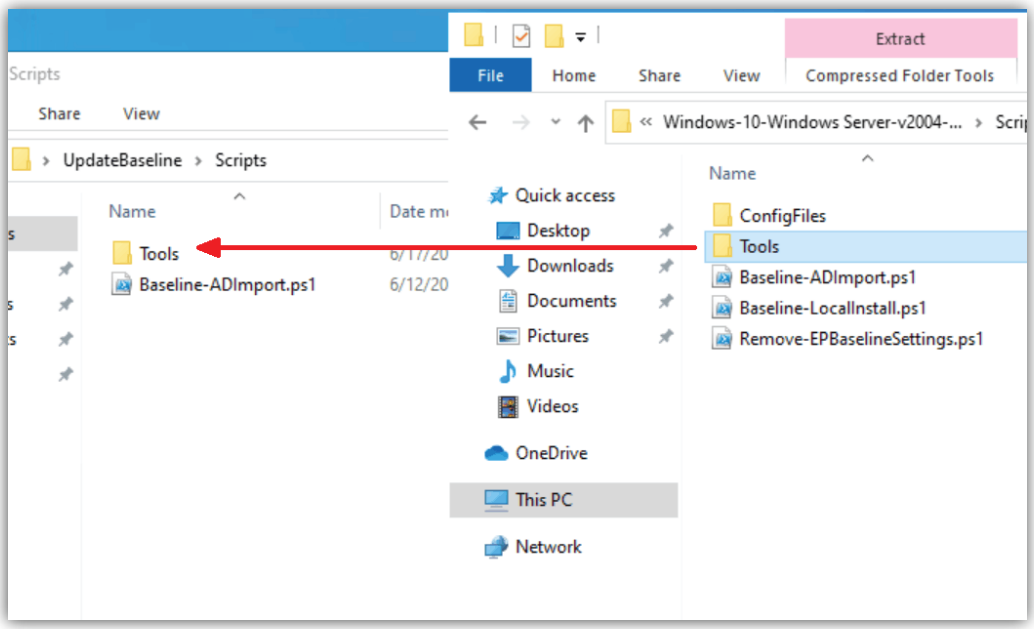
Nach dem Vorbild der Security Baseline umfasst die Update Baseline das Backup eines GPO für den Import in die GPMC, eine Dokumentation im PDF-Format, eine Excel-Tabelle mit den konfigurierten Einstellungen sowie einen mit gpresult erzeugten HTML-Bericht.

Für den Import des GPO enthält das Toolkit ein PowerShell-Script namens *Baseline-ADImport.ps1*. Wenn man es wie im PDF-Dokument beschrieben startet, dann bricht es mit der Fehlermeldung ab, dass es die Datei *MapGuidsToGpoNames.ps1* nicht finden kann.



Inhalt der Update Baseline

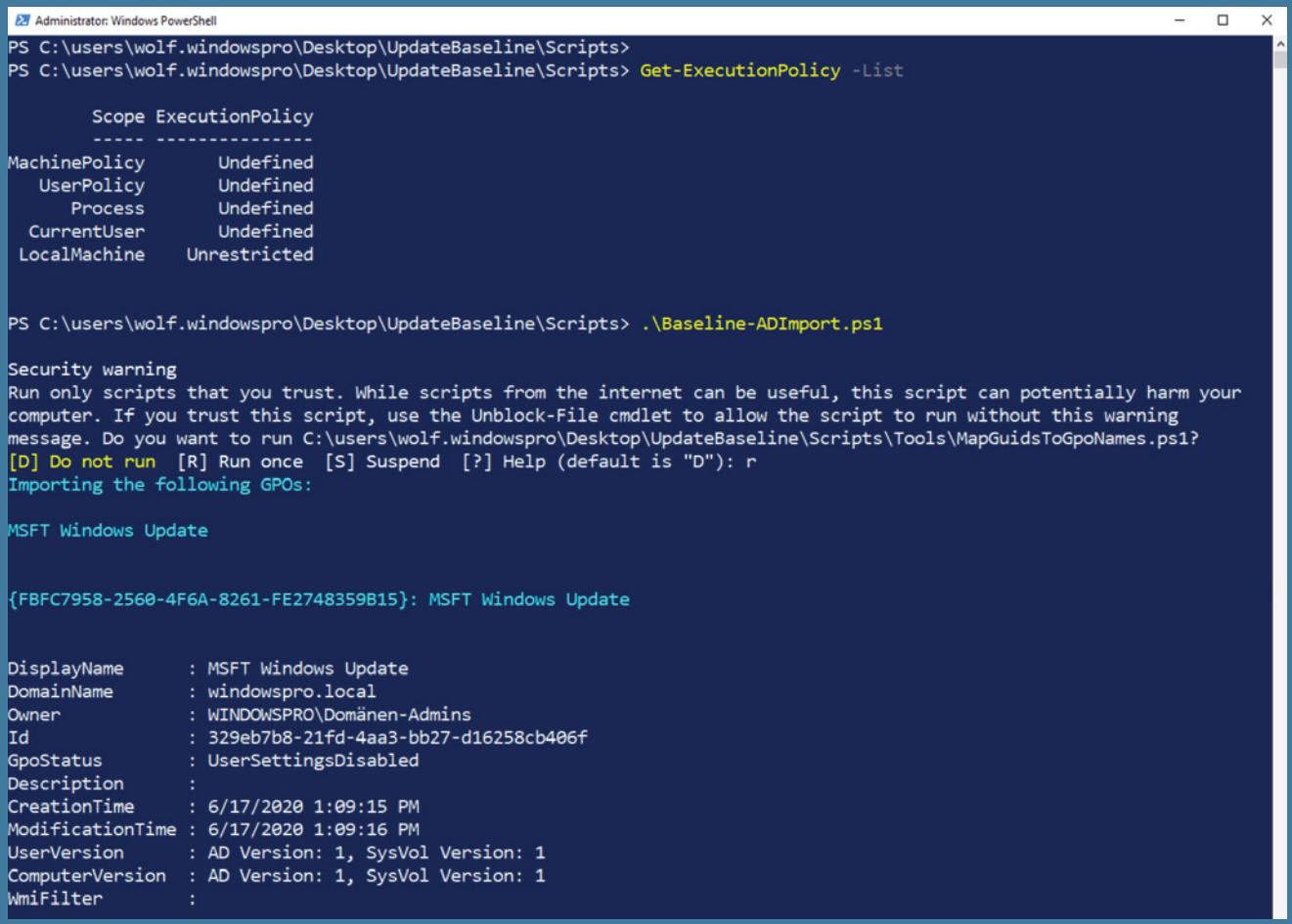
Wie sich schnell zeigt, gehört diese nicht zum Lieferumfang der Update Baseline. Vielmehr ist es Bestandteil der Security Baseline, so dass man diese zusätzlich herunterladen und von dort den Ordner Tools in das Scripts-Verzeichnis der Update Baseline kopieren muss.



Das Script in der Update-Baseline benötigt das Tools-Verzeichnis aus der Security Baseline

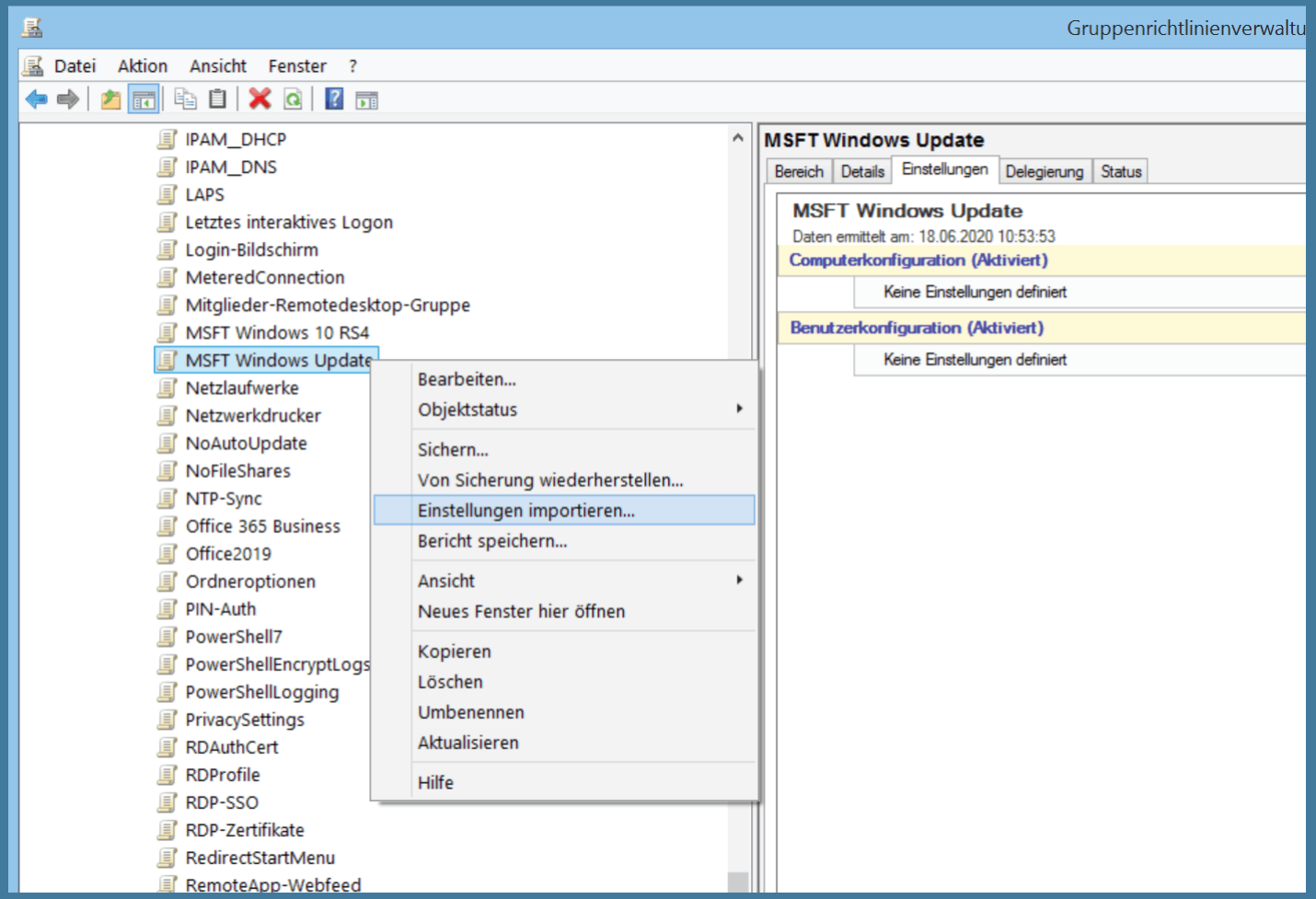
Anschließend kann die Ausführung des Scripts noch an der Execution Policy scheitern, die man dann temporär auf *Unrestricted* setzen müsste.

Nach der erfolgreichen Ausführung des Scripts findet man in der Gruppenrichtlinienverwaltung (GPMC) unter *Gruppenrichtlinienobjekte* eine neue GPO namens *MSFT Windows Update*. Es ist mit keiner OU oder Domäne verknüpft und wird daher auf keine Rechner angewandt.



Das Import-Script erstellt ein nicht verlinktes GPO namens MSFT Windows Update

Wem das Hantieren mit diesem unvollständigen PowerShell-Script zu umständlich ist, kann alternativ ein leeres GPO in der GPMC erstellen und aus dessen Kontextmenü den Assistenten für den Import von Einstellungen starten. Als Verzeichnis gibt man den *GPOs*-Ordner der User Baseline an.



Alternativ zum PowerShell-Script kann man die Import-Funktion der GPMC nutzen

Anpassung der vorgegebenen Einstellungen

Admins können das GPO daher erst an die Bedürfnisse des Unternehmens anpassen, bevor sie es verlinken. So ist etwa die Nutzungszeit ("Active Hours") fest auf 18 Stunden eingestellt. Seit Windows 10 1903 kann man diese Option auf *Nicht konfiguriert* zurücksetzen, weil das System dann automatisch die Nutzungszeit anhand der Arbeitsgewohnheiten des Benutzers ermittelt.

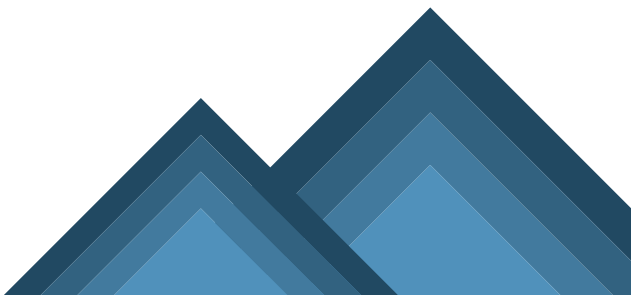
Ziel der Baseline ist es, die Installation von Updates und den Neustart der Rechner zu steuern, sobald die Updates verfügbar sind. Dagegen konfiguriert sie keine Einstellung für den Aufschub von Updates.

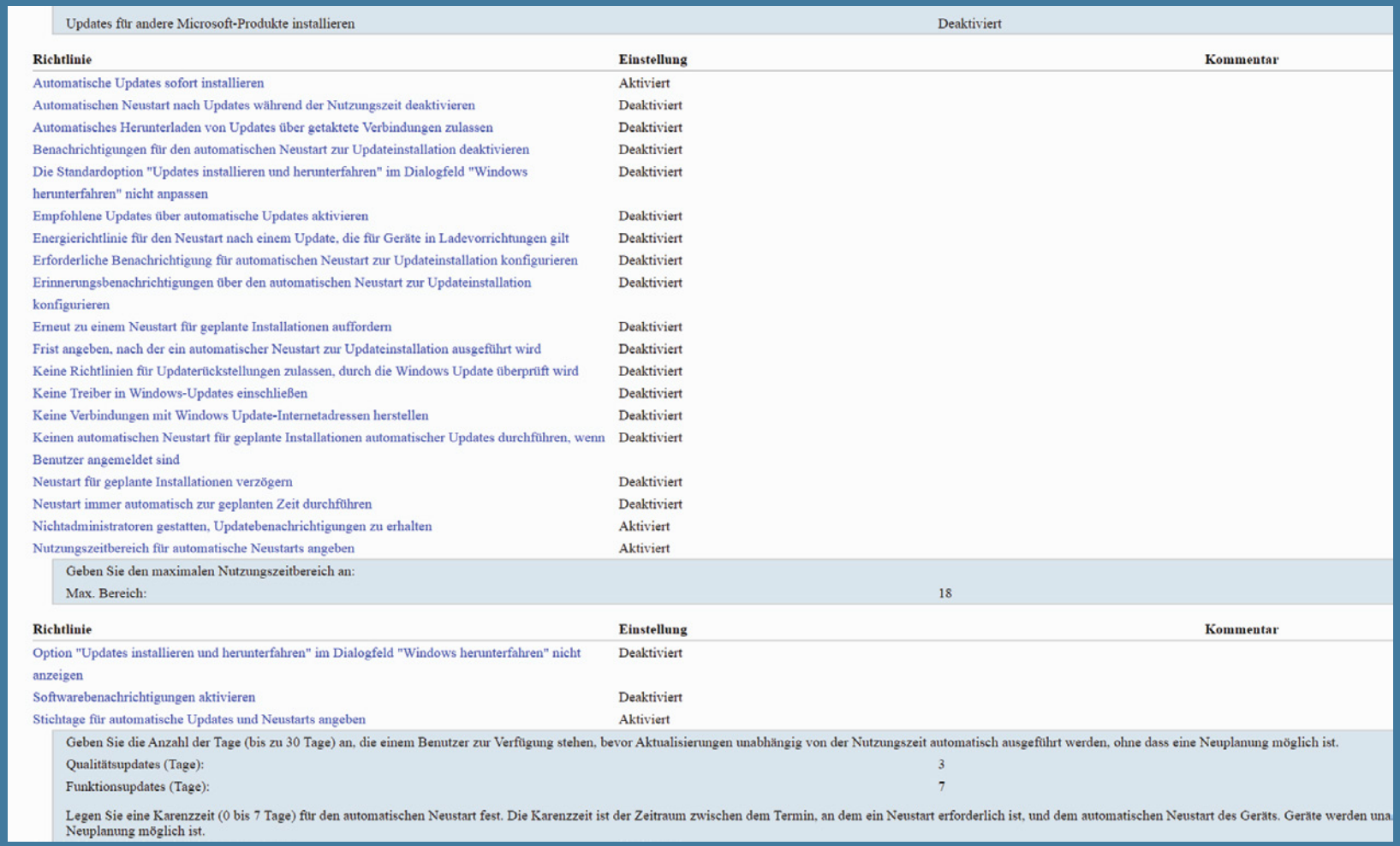
Energieverwaltung und Delivery Optimization

Wenn man alle Einstellungen des GPOs durchsieht, dann zeigt sich, dass sie nicht nur den Update-Dienst selbst konfigurieren, sondern auch die Energieverwaltung. Sie sollen etwa bei Notebooks dafür sorgen, dass diese nach dem Zuklappen in den Standby gehen und nicht ausgeschaltet werden, um Updates einspielen zu können.

Die Update Baseline konfiguriert zudem eine ganze Reihe von Einstellungen für die Übermittlungsoptimierung. Das Neustartverhalten regelt Update Compliance ausschließlich für die erwähnte Einstellung *Stichtage für automatische Updates und Neustarts angeben*.

Nachdem es für das Update-Management eine Vielzahl von Optionen gibt, die teilweise aber seit Windows 10 keinen Effekt mehr haben oder durch neuere Einstellungen ersetzt werden, deaktiviert die Baseline einen großen Teil dieser Altlasten. Auf diese Weise lassen sich mögliche Konflikte ausschließen.





Updates für andere Microsoft-Produkte installieren	Deaktiviert	

Richtlinie	Einstellung	Kommentar
Automatische Updates sofort installieren	Aktiviert	
Automatischen Neustart nach Updates während der Nutzungszeit deaktivieren	Deaktiviert	
Automatisches Herunterladen von Updates über getaktete Verbindungen zulassen	Deaktiviert	
Benachrichtigungen für den automatischen Neustart zur Updateinstallation deaktivieren	Deaktiviert	
Die Standardoption "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anpassen	Deaktiviert	
Empfohlene Updates über automatische Updates aktivieren	Deaktiviert	
Energierichtlinie für den Neustart nach einem Update, die für Geräte in Ladevorrichtungen gilt	Deaktiviert	
Erforderliche Benachrichtigung für automatischen Neustart zur Updateinstallation konfigurieren	Deaktiviert	
Erinnerungsbenachrichtigungen über den automatischen Neustart zur Updateinstallation konfigurieren	Deaktiviert	
Erneut zu einem Neustart für geplante Installationen auffordern	Deaktiviert	
Frist angeben, nach der ein automatischer Neustart zur Updateinstallation ausgeführt wird	Deaktiviert	
Keine Richtlinien für Updaterückstellungen zulassen, durch die Windows Update überprüft wird	Deaktiviert	
Keine Treiber in Windows-Updates einschließen	Deaktiviert	
Keine Verbindungen mit Windows Update-Internetadressen herstellen	Deaktiviert	
Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind	Deaktiviert	
Neustart für geplante Installationen verzögern	Deaktiviert	
Neustart immer automatisch zur geplanten Zeit durchführen	Deaktiviert	
Nichtadministratoren gestatten, Updatebenachrichtigungen zu erhalten	Aktiviert	
Nutzungszeitbereich für automatische Neustarts angeben	Aktiviert	
Geben Sie den maximalen Nutzungszeitbereich an:		
Max. Bereich:	18	

Richtlinie	Einstellung	Kommentar
Option "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anzeigen	Deaktiviert	
Softwarebenachrichtigungen aktivieren	Deaktiviert	
Stichtage für automatische Updates und Neustarts angeben	Aktiviert	
Geben Sie die Anzahl der Tage (bis zu 30 Tage) an, die einem Benutzer zur Verfügung stehen, bevor Aktualisierungen unabhängig von der Nutzungszeit automatisch ausgeführt werden, ohne dass eine Neuplanung möglich ist.		
Qualitätsupdates (Tage):	3	
Funktionsupdates (Tage):	7	
Legen Sie eine Karenzzeit (0 bis 7 Tage) für den automatischen Neustart fest. Die Karenzzeit ist der Zeitraum zwischen dem Termin, an dem ein Neustart erforderlich ist, und dem automatischen Neustart des Geräts. Geräte werden una Neuplanung möglich ist.		

Den Neustart der PCs steuert die Baseline über eine Einstellung. Viele alte Optionen wurden deaktiviert

Updates verteilen mit ACMP CAWUM von Aagon

Eine Alternative sowohl zu Windows Update als auch zu den WSUS bietet Aagon mit CAWUM (Complete Aagon Windows Update Management). Dabei handelt es sich um ein Modul für die Client-Management-Suite ACMP. Es kann zusammen mit ACMP Core auch unabhängig von den anderen Komponenten erworben werden.

Diese On-prem-Lösung beherrscht nicht nur alle Aspekte des Update-Managements für Windows, sondern erspart Admins auch die lästige Auseinandersetzung mit den ständig geänderten Grupperichtlinien für Windows Update.

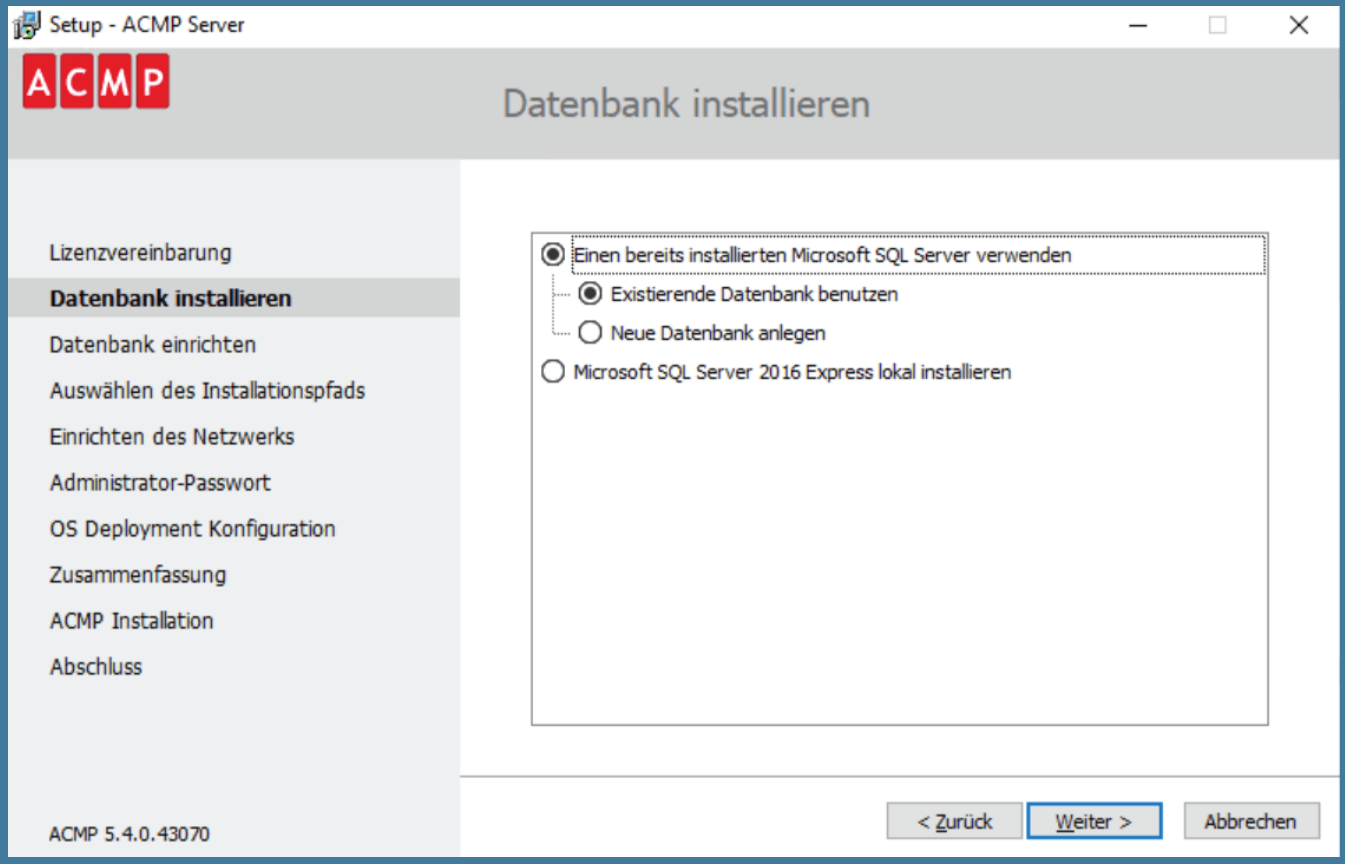
CAWUM kann darüber hinaus WSUS vollständig ersetzen und befreit die Systemverwalter damit von der aufwändigen Wartung für diesen Dienst. Außen vor bleibt auch das Management der Delivery Optimization, weil ACMP über eigene Mechanismen zur effizienten Bereitstellung von Patches verfügt.

Aagon beschränkt sich jedoch nicht einfach darauf, die Bordmittel mit einem Tool zu ersetzen, das sich einfacher nutzen und warten lässt. Vielmehr bietet CAWUM einige Funktionen, die man bei WSUS vergeblich sucht:

- Ein sehr flexibles Konzept zur Definition von Verteilerringen, wobei beliebig viele Test- und Freigabeprozesse unterstützt werden.
- Detailliertes Reporting sowie ein Dashboard, so dass sich der aktuelle Update-Status schnell ermitteln lässt.
- Einsparen von Bandbreite, da Updates nur einmal heruntergeladen werden.
- Eine Aufräumfunktion, die dem von WSUS leidlich bekannten Problem des ständig wachsenden Speicherbedarfs vorbeugt.

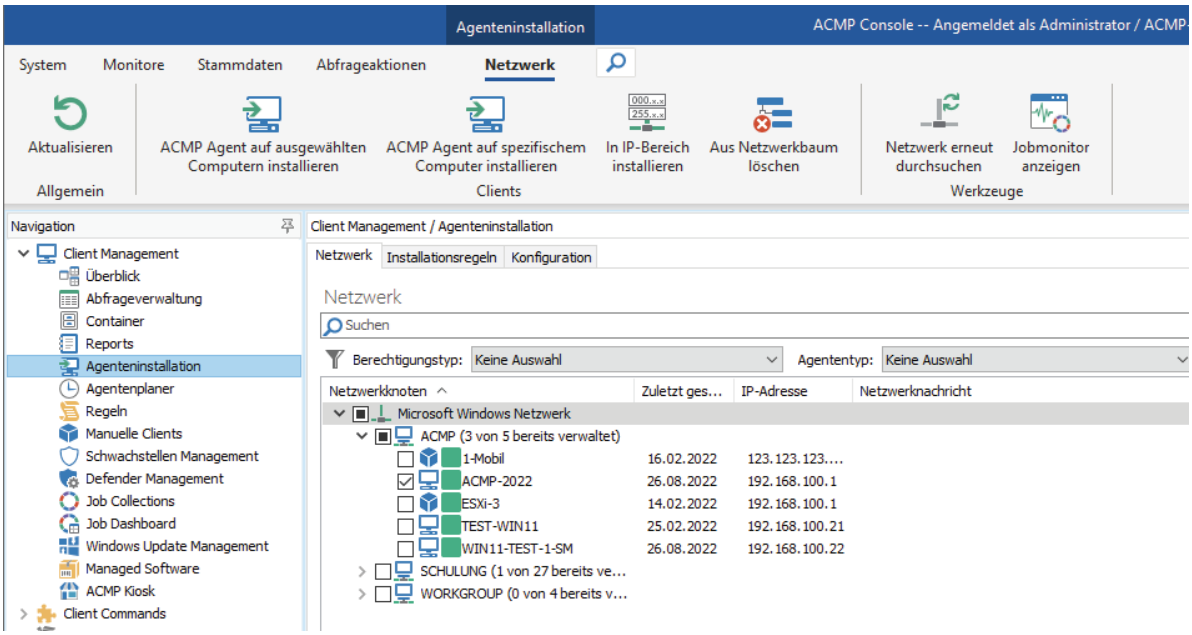
Installation und Agent-Deployment

Die Installation umfasst immer das ganze ACMP-Paket, wobei nicht lizenzierte Module später aus der Konsole ausgeblendet werden können. Das Setup beschränkt sich auf das Durchlaufen eines grafischen Wizards. Dieser sieht auch das Anlegen einer neuen Datenbank oder die Installation von SQL Server Express vor, der zum Lieferumfang des Pakets gehört.



SQL Server Express gehört zum Lieferumfang von ACMP und kann beim Setup gleich installiert werden

Die Möglichkeit, Microsofts kostenlose Datenbank einzusetzen, ist bereits ein Unterschied zu WSUS. Aufgrund der schnell wuchernden SUSDB erreicht WSUS meist schnell das 10GB-Limit der Express Edition. Als Alternative bleiben die WID, welche sich remote nicht verwalten lassen, oder die kostenpflichtige Vollversion von SQL Server. Aagon hingegen kann für das reine Update-Management deutlich mehr PCs mit SQL Server Express verwalten als WSUS.

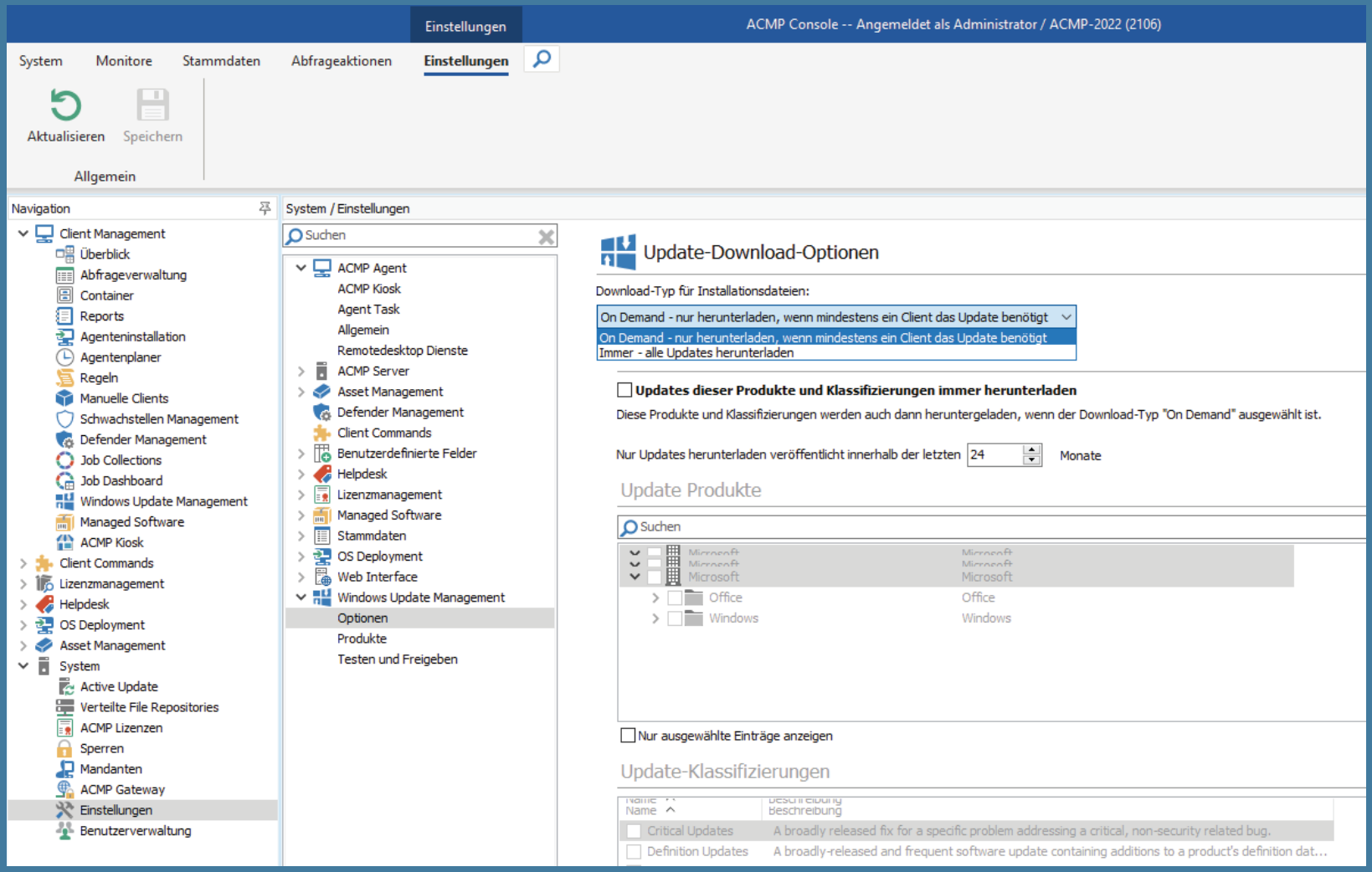


Der ACMP-Agent kann von der Konsole aus auf die Zielrechner installiert werden

Nach erfolgter Installation besteht die erste Aufgabe darin, den Agent auf die Endgeräte auszubringen. Dieser inventarisiert die Rechner nicht nur, sondern wird auch für das Management der Updates benötigt. Das Agent-Deployment lässt sich zentral von der ACMP-Konsole aus erledigen, wobei diese verschiedene Methoden unterstützt, um die Geräte im Netz zu finden.

Basiskonfiguration

Im nächsten Schritt kann man sich daran machen, das Update Management zu konfigurieren. Unter *Optionen* finden sich dafür drei grundlegende Einstellungen. Dazu gehört wie bei WSUS, dass man Updates generell oder nur nach Bedarf herunterlädt, in der Regel wird man sich für Letzteres entscheiden.



Konfiguration der Optionen, darunter jener für die automatische Bereinigung

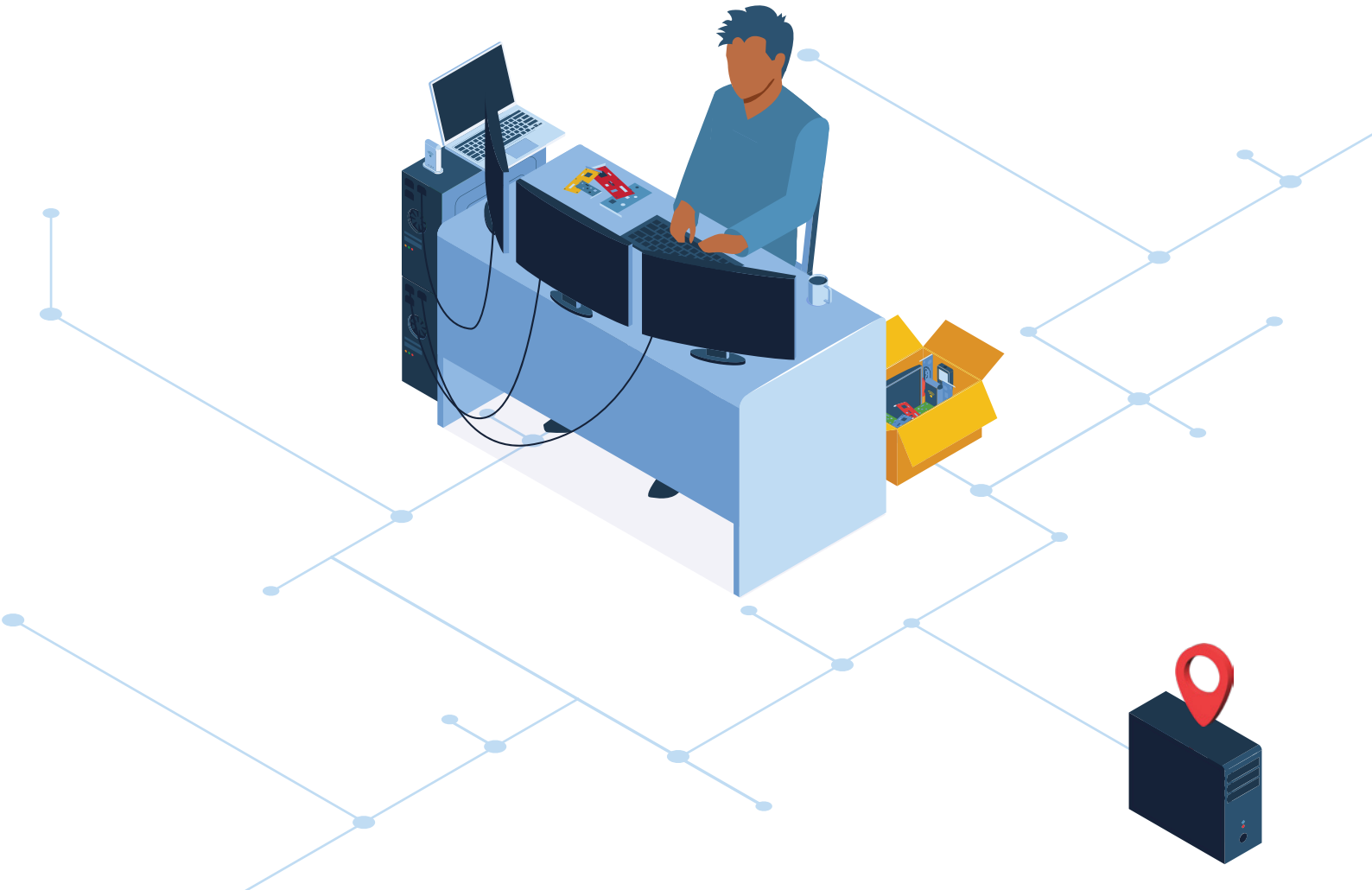
Darüber hinaus legt man hier fest, nach wie vielen Tagen nicht genutzte Updates automatisch abgelehnt und anschließend gelöscht werden. Fordert ein Client diese später trotzdem an, dann lädt ACMP diese wieder nach. Ein manuelles Bereinigen wie bei WSUS kann dadurch entfallen.

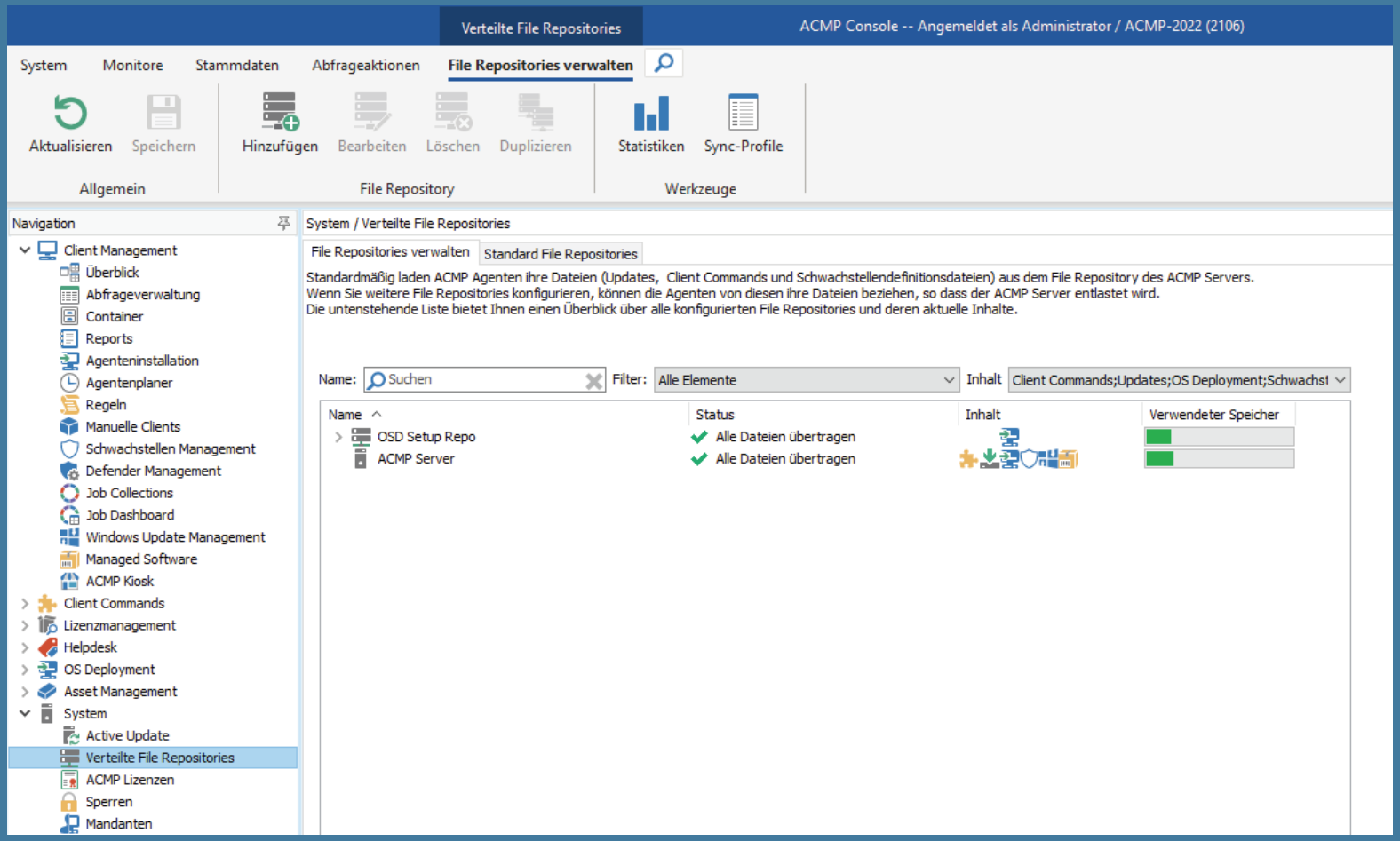
Zum Schluss bestimmt man die Quelle, von der CAWUM die Updates beziehen soll. Voreingestellt ist Microsoft Update, aber für die Migration kann man hier einen bestehenden WSUS-Server angeben. Dies bedeutet aber nicht, dass Aagon ein Konzept kaskadierender Server verfolgt wie WSUS.

Kein Update-Server für Außenstellen nötig

Vielmehr reicht ein ACMP-Server, um alle Clients mit den Metadaten über die anstehenden Updates zu versorgen. In Niederlassungen können Admins die eigentlichen Update-Dateien dann auf einem File Repository ablegen und die lokalen PCs ziehen die Patches anschließend von dort.

Für diesen Zweck reicht eine einfache Dateifreigabe, etwa auf einem preisgünstigen NAS. In dieser Hinsicht lassen sich also gegenüber den WSUS Kosten einsparen, die in größeren Umgebungen eine ganze Hierarchie aus Upstream- und Downstream-Servern benötigen.

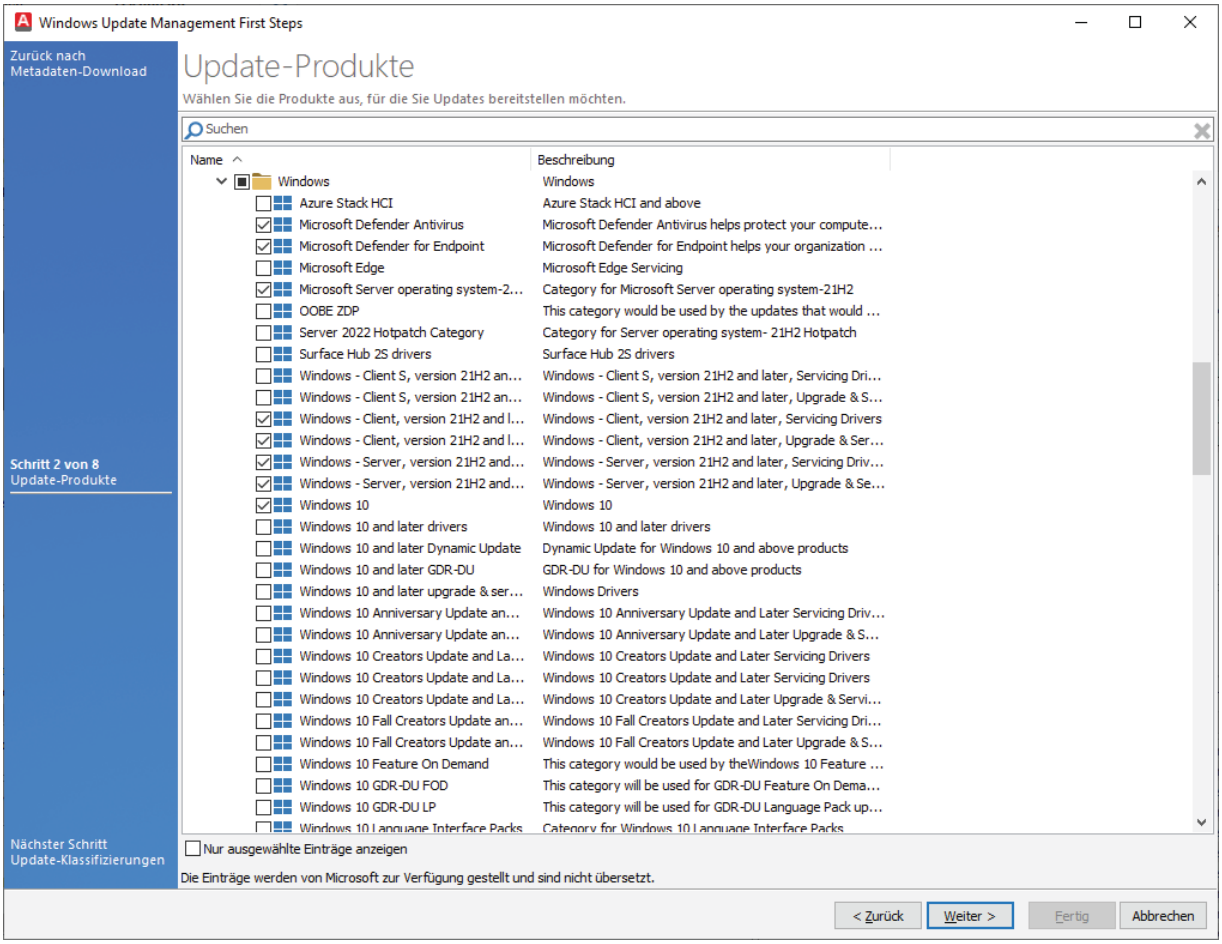




Rechner in Niederlassungen können ihre Updates von File Repositories vor Ort beziehen

Update-Katalog beziehen, Produkte auswählen

Für die Ersteinrichtung von CAWUM steht ein Wizard zur Verfügung, der automatisch startet, sobald man in der Navigation zum ersten Mal auf den Eintrag *Windows Update Management* wechselt. Im ersten Schritt lädt er den Update-Katalog von der konfigurierten Quelle herunter. Man kann die Auswahl aus den Produkten und Klassifizierungen schon hier treffen oder später in den Einstellungen nachholen.

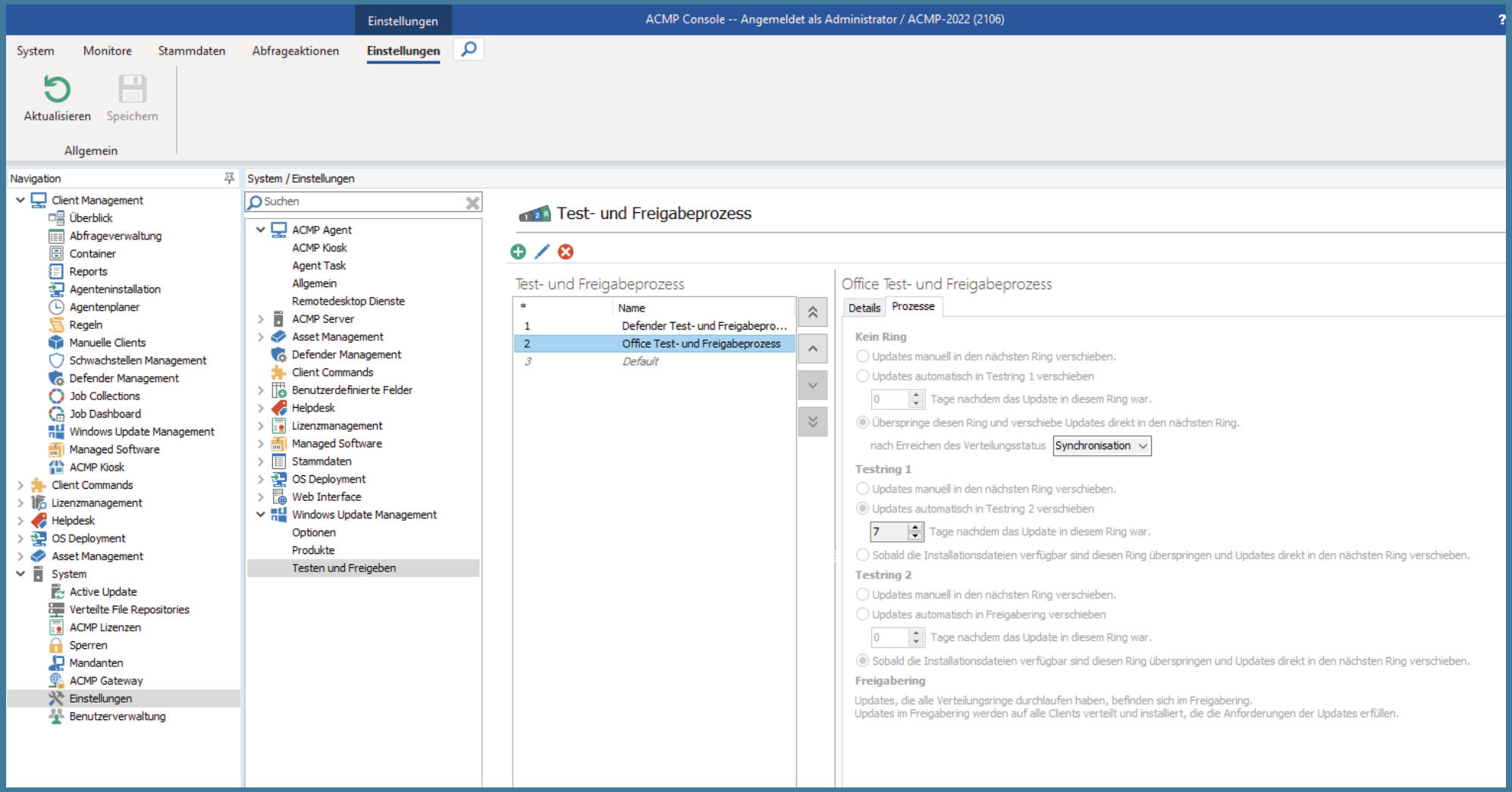


Der Wizard für die CAWUM-Konfiguration lädt den Update-Katalog von Microsoft herunter

Es folgt die Festlegung der Sprachen für die Updates und schließlich wählt man aus der Liste der ACMP-Clients aus, welche von ihnen mit CAWUM verwaltet werden sollen. Von den PCs meldet der Agent künftig an den ACMP-Server, welche Updates die jeweiligen Clients benötigen.

Konfiguration der Verteilerringe

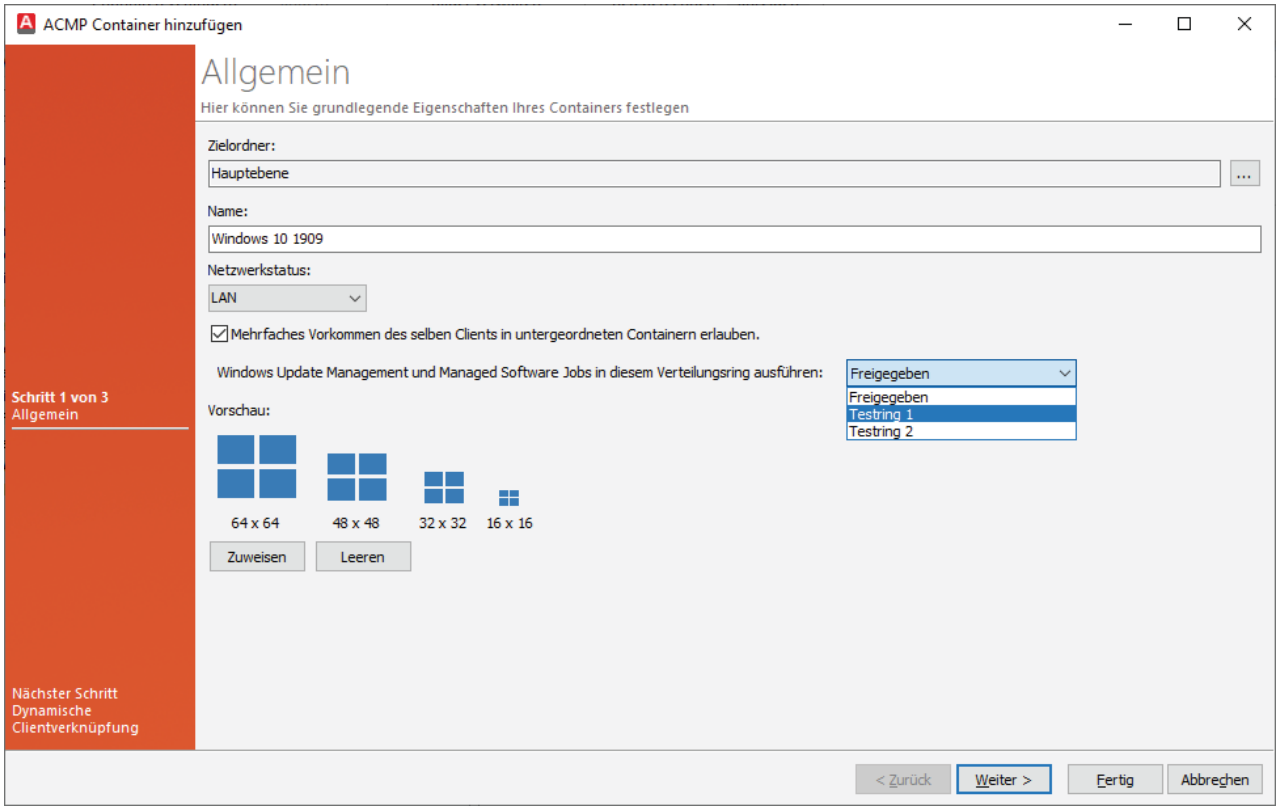
ACMP sieht für die Verteilung der Updates Verteilerringe vor, und zwar sowohl Test- als auch Freigaberinge. Diese sind aber nicht starr vorgegeben, vielmehr können Anwender diese flexibel handhaben.



ACMP sieht 3 Verteilerringe vor, die sich flexibel konfigurieren oder überspringen lassen

Eine weitgehend automatisierte Variante bestünde darin, dass Updates nach und nach in den nächsten Ring nachrücken. Die Intervalle für das Weiterreichen von Updates in den nächsten Ring lassen sich einstellen. Alternativ kann man diesen Vorgang auf *manuell* setzen oder bestimmte Ringe ganz überspringen.

Erwartungsgemäß besteht die nächste Aufgabe darin, die Rechner diesen Verteilerringen zuzuordnen. Weniger kritische Systeme würde man in die Testringe aufnehmen, um zu sehen, ob Updates Probleme bereiten. In den Freigabering schließlich kommen alle wichtigen produktiven PCs.

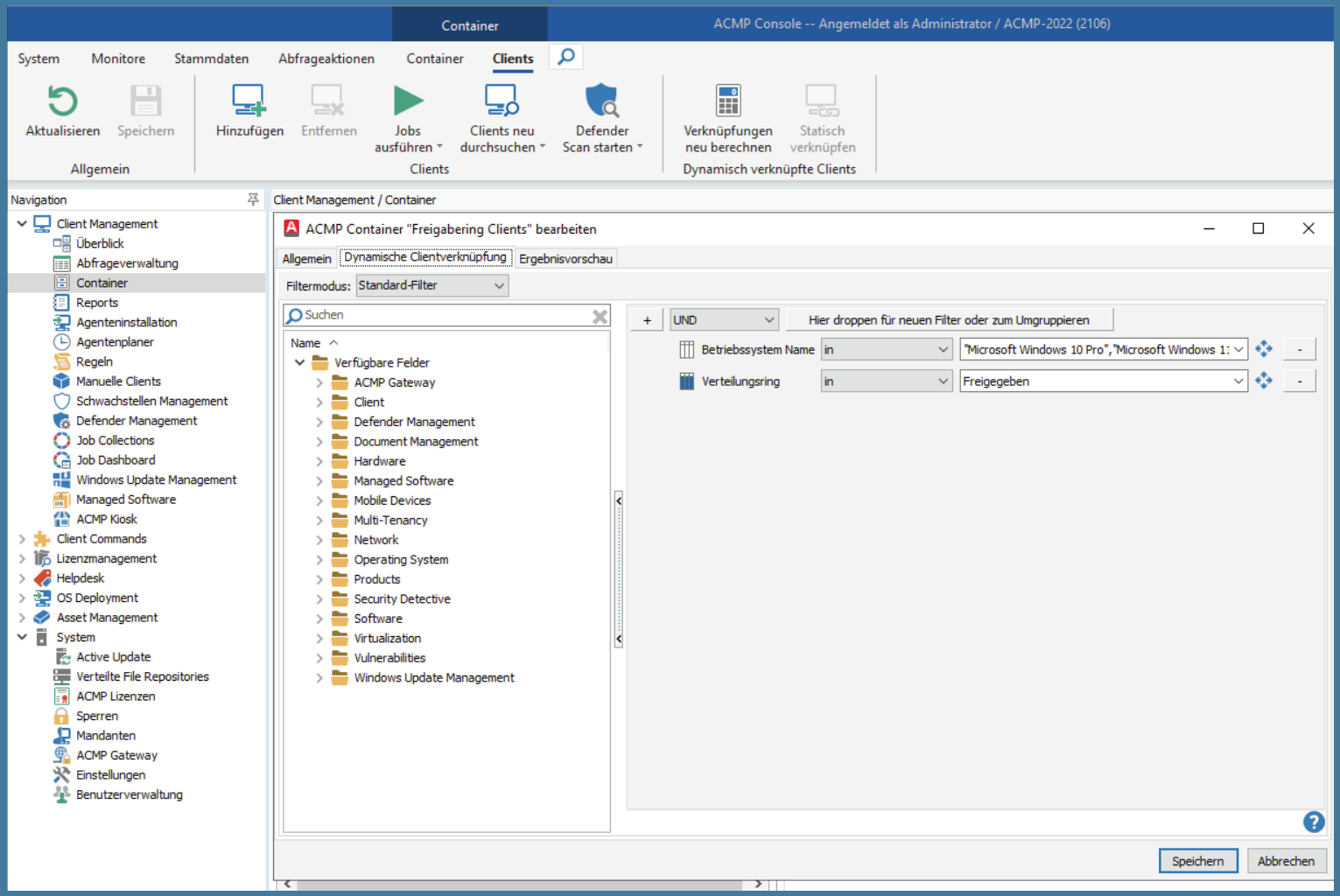


Rechner werden in Containern zusammengefasst und diese weist man an Verteilerringe zu

Rechner gruppieren

In WSUS fasst man die Rechner, welche man einem Update-Server zugeordnet hat, entweder manuell auf der Konsole in Gruppen zusammen oder weist sie per GPO einer bestimmten Sammlung zu.

CAWUM zeigt sich auch hier wesentlich flexibler, weil man die PCs mit Hilfe von Abfragen dynamisch in Container einsortieren kann. Als Kriterien kommen alle erdenklichen Merkmale eines Rechners in Frage, die der Agent erfassen kann.

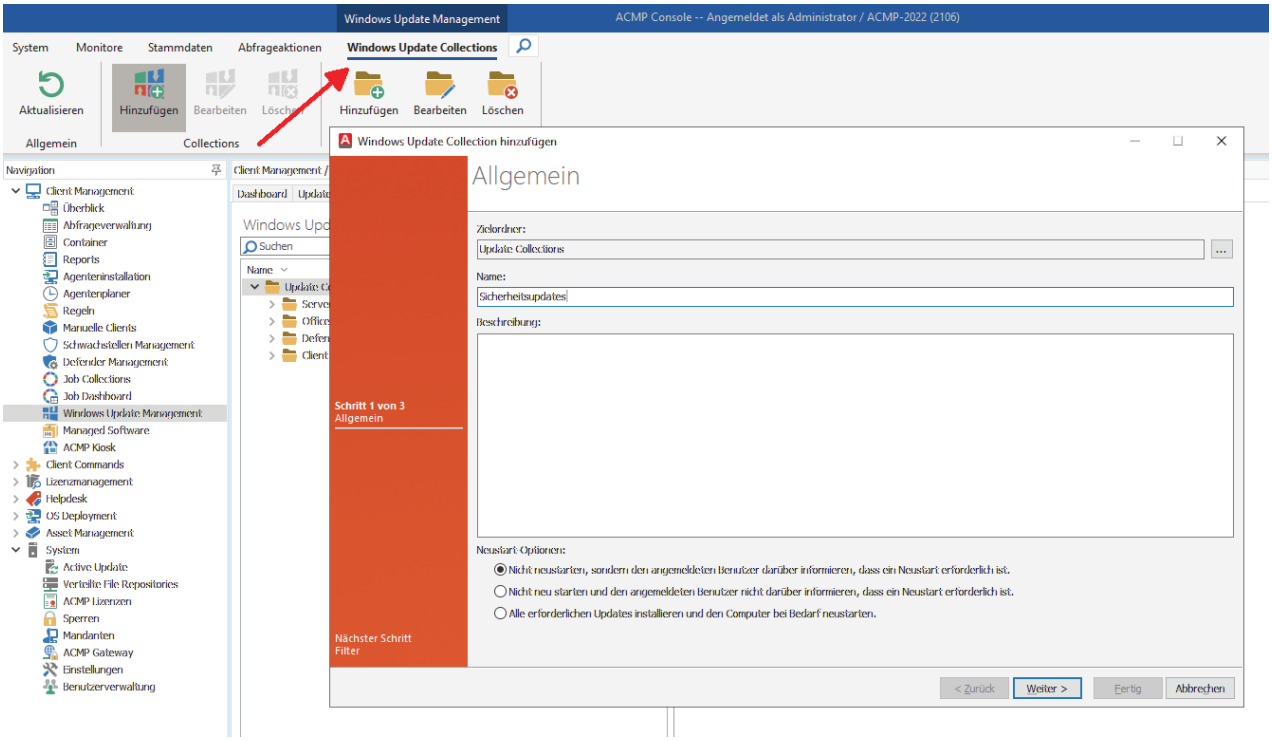


Container lassen sich über fast beliebige Filter mit Computern befüllen

Profile für Updates

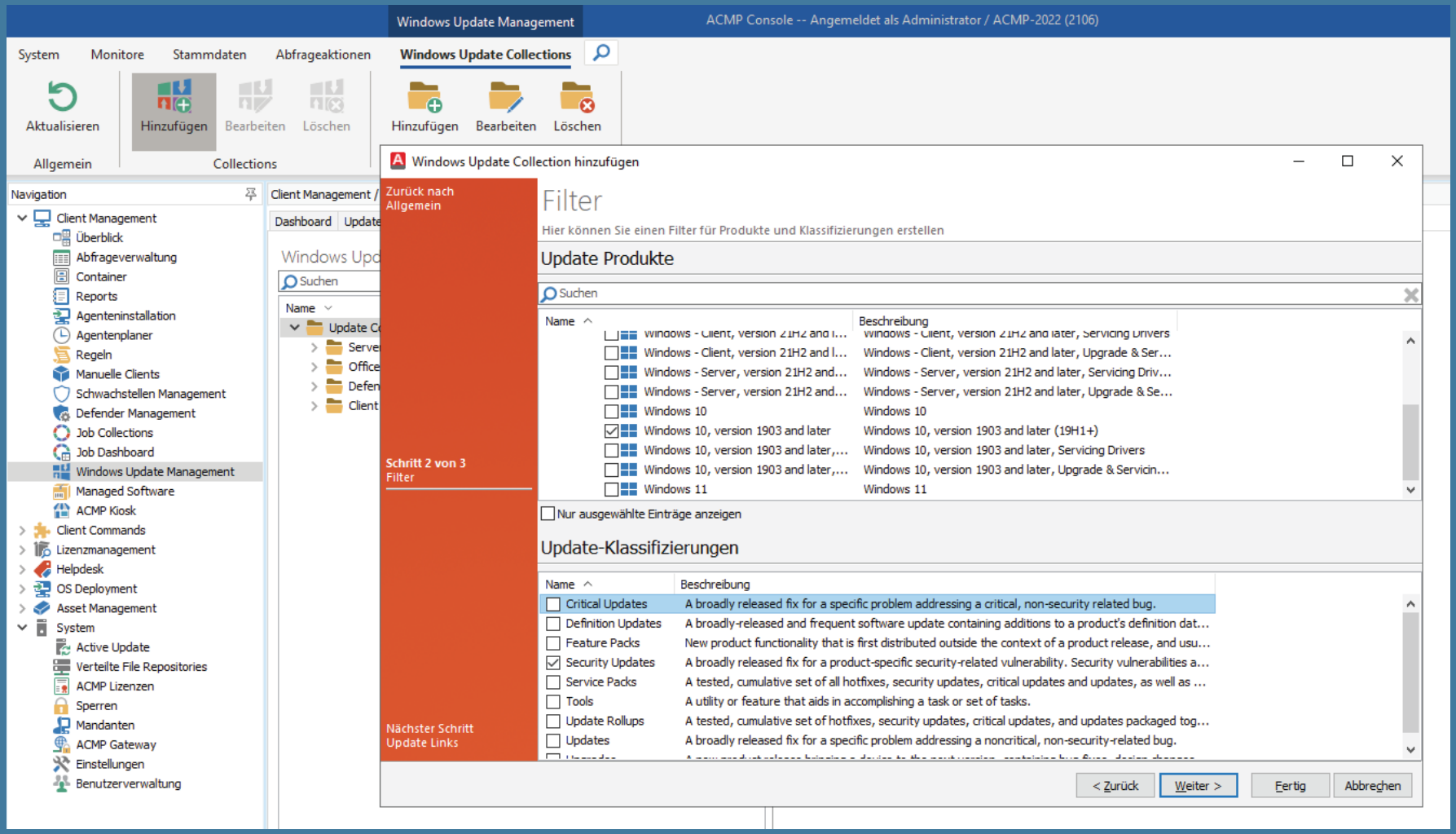
Theoretisch wären mit den PC-Containern und den Verteilerringen schon die Voraussetzungen gegeben, um Updates auf die Rechner zu verteilen. Allerdings würden dann immer sämtliche Updates für ein Produkt installiert, und zwar aus allen abonnierten Klassifizierungen.

Daher schaltet ACMP noch so genannte Collections dazwischen. Dabei handelt es sich um Profile für Updates, bei denen man nur bestimmte Produkte und Klassifizierungen auswählt. Über eine Collection legt man zudem das Verhalten des Rechners fest, wenn ein Neustart fällig ist.



Über Collection legt man auch die Neustartoptionen für die Rechner fest

Mit Hilfe von Collections könnte man zum Beispiel Sicherheits-Updates von Feature-Upgrades trennen oder Updates für Workstations zu einem anderen Zeitpunkt verteilen als jene für Server.

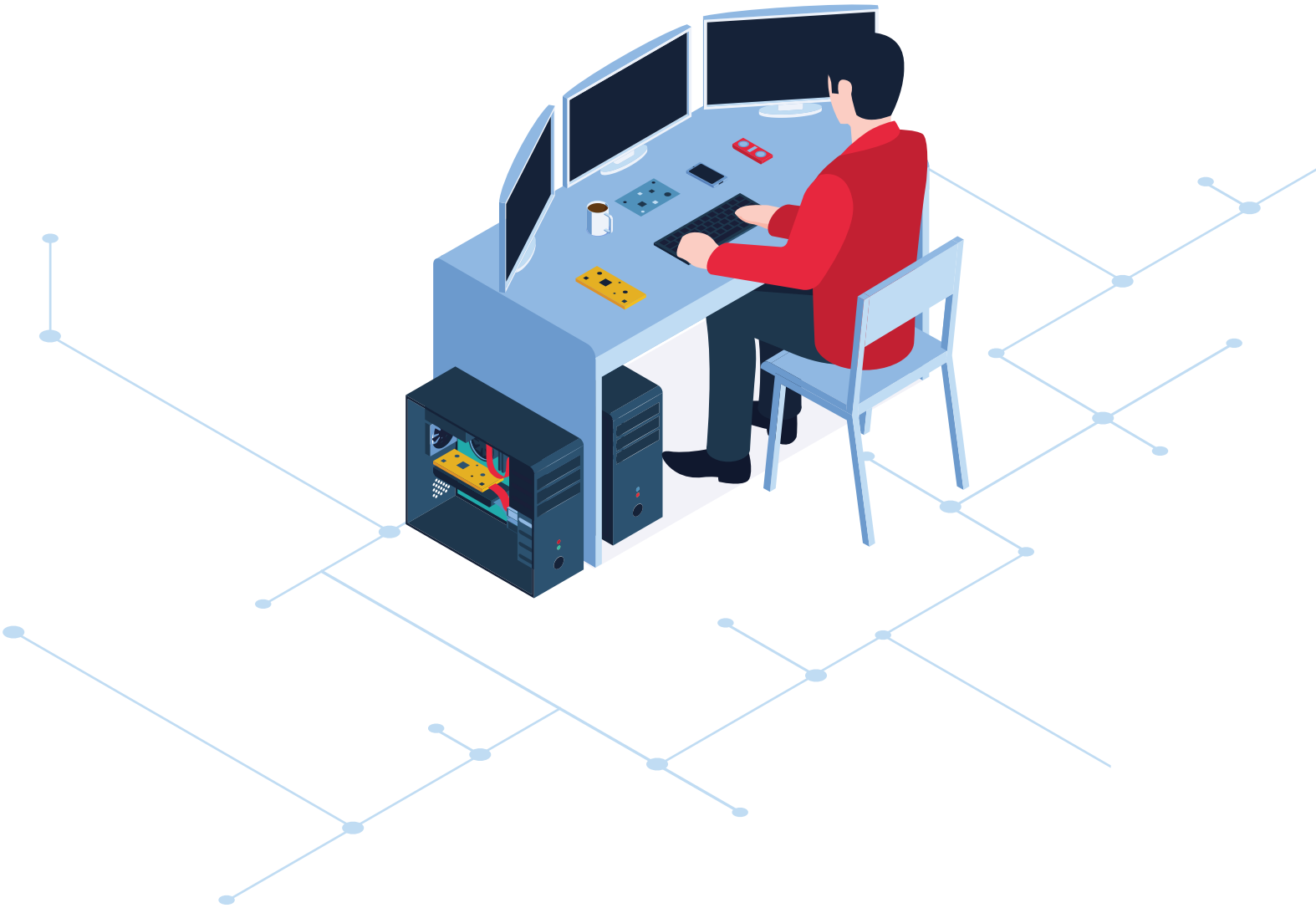


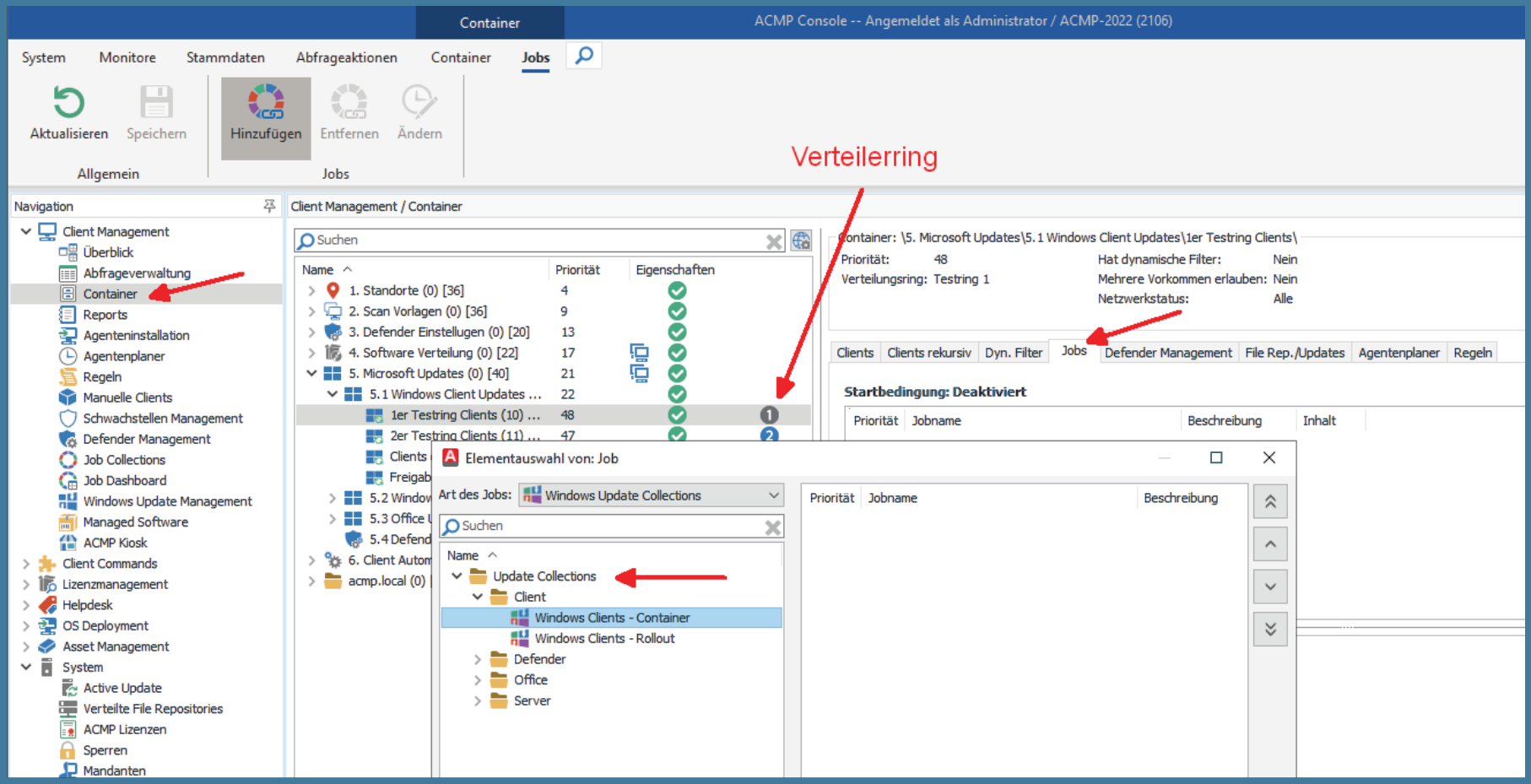
Collections sind quasi Update-Profile, für die man Produkte und Klassifizierungen auswählt

Zusammenspiel aus Containern, Verteilerringen und Collections

Um also die Rechner im Netz mit Updates zu versorgen, gruppiert man sie in einem Container (manuell oder dynamisch über Abfragen) und weist diesen einem Verteilerring zu. Um zu bestimmen, welche Art von Updates die PCs in einem Container erhalten sollen, verknüpft man diesen zudem mit einer Collection.

Dabei hat der Admin fast überall die Möglichkeit, die über Filter generierten Listen von Updates oder Rechnern manuell zu übersteuern. Zusätzliche Flexibilität ergibt sich dadurch, dass man einen Container mit mehreren Collections und eine Collection mit mehreren Containern verbinden kann.



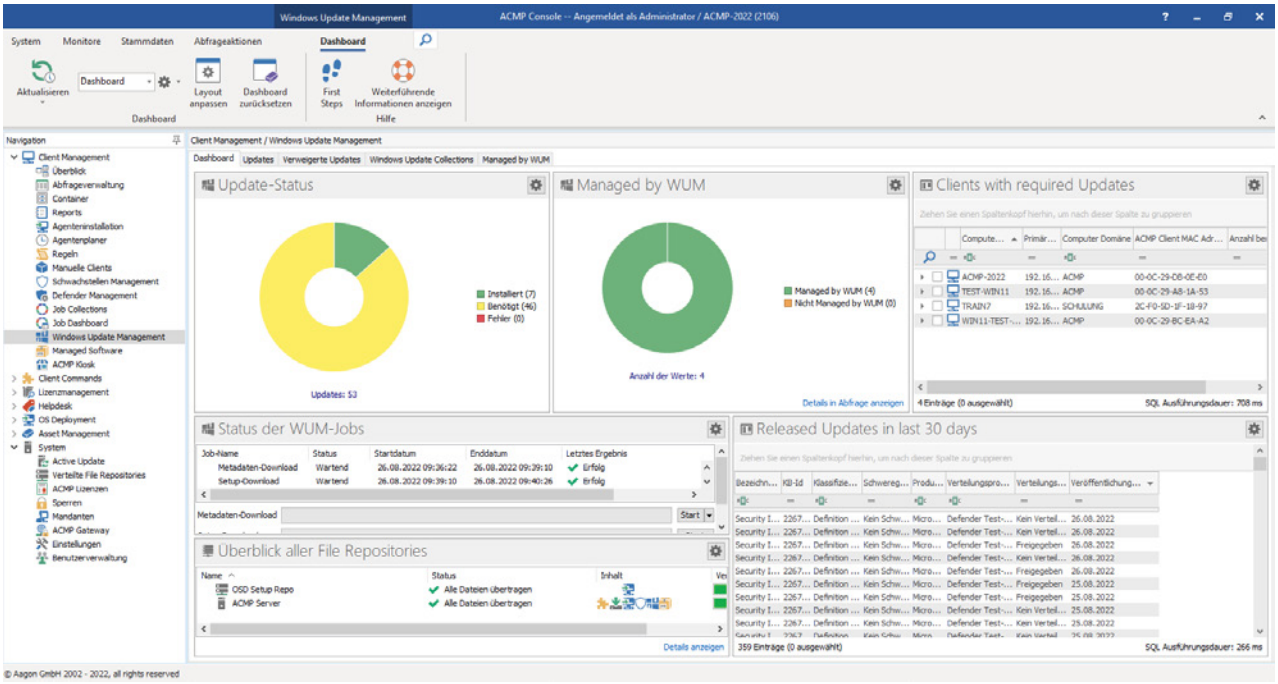


Verknüpfung von Containern mit Verteilerringen und Update-Collections

Kontrolle des Update-Prozesses

Da es sich beim Patch-Management um eine sicherheitsrelevante Aufgabe handelt, sollen Admins schnell erkennen, dass bestimmte Updates auf einzelnen Rechnern nicht installiert wurden.

Für diesen Zweck bietet CAWUM ein Dashboard, das alle wichtigen Kennzahlen auf einen Blick zugänglich macht. Hinzu kommen vorkonfigurierte Berichte, die auch zeitgesteuert generiert werden können. Dem stehen bei WSUS nur vorsintflutliche Reporting-Tools gegenüber.



Das Dashboard von CAWUM gibt Aufschluss über alle Vorgänge beim Patch-Management

Fazit

Aagon kombiniert ein verständliches Konzept für das Windows Update Management mit einer modernen grafischen Konsole, die dem Admin alle benötigten Informationen zu Updates und dem Status der Rechner gibt.

Im Unterschied zu WSUS lassen sich Patches mit Hilfe von Verteilerringen und dynamischen Containern für Rechner sehr flexibel verteilen. Viele Wartungsarbeiten, die der Admin bei WSUS selbst erledigen muss, entfallen bei CAWUM. Dazu zählen etwa das regelmäßige Indizieren der Datenbank oder das Ablehnen und Löschen nicht benötigter Updates.

Anwender, die eine Alternative zu Microsofts Bordmittel für das Update-Management suchen, sollten einen Blick auf CAWUM werfen. Eine kostenlose Testversion kann über die Website des Herstellers bezogen werden.

ÜBER AAGON

„Manage any device in a connected world!" – Aagon entwickelt seit 30 Jahren Client-Management- und -Automation-Lösungen und ist der Spezialist für die Verwaltung von Endgeräten und die Automatisierung von Standardaufgaben. Durch sorgfältige Entwicklungen, mehr als 20 Jahre Marktreife und die enge Zusammenarbeit mit unseren Kunden und Partnern sind unsere Produkte perfekt auf Ihre Anforderungen und Bedürfnisse zugeschnitten.

Individuelle Beratung und die beste Unterstützung von Kunden und Partnern bei der Installation und ersten Einrichtung gehören deshalb zum Standard von Aagon. Ein umfassendes Verständnis von Kundenbedürfnissen und der ständige Kontakt zu unseren Kunden und Partnern ermöglichen Softwareentwicklung auf Augenhöhe.

Webinare-on-Demand, zahlreiche Whitepaper und die beliebten Treffen zum Anwendertreffen an Standorten in ganz Deutschland sind nur drei Beispiele, wie nahe am Kunden ACMP wirklich entwickelt wird.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

EIN PRODUKT DER
Aagon GmbH
Lange Wende 33
D-59494 Soest
Fon: +49 (0)2921 - 789200
Fax: +49 (0)2921 - 789244
sales@aagon.com
www.aagon.com

READERS' CHOICE
IP INSIDER AWARD 2022

techconsult
PUR 2023
Professional User Rating
★ 4-FACH ★
★ CHAMPION ★