



WHITEPAPER

Windows 11 an die Leine nehmen

Migration, Anpassung und Absicherung

INHALT

1	Windows 11 – Jährliches Release.....	2
2	Risiko alter Windows Versionen	3
3	Aktualisierung von Windows 11.....	4
3.1	Planung und Durchführung	4
3.2	Vorbereitung und Analyse	4
3.3	Umsetzung.....	4
3.4	UEM-Hilfsmittel zur erfolgreichen Migration.....	4
3.5	Anpassung von Windows 11 Images.....	5
4	Absicherung Windows 11.....	8
4.1	Hilfsmittel zur Absicherung von Windows 11	8
4.2	Konfiguration.....	9
4.3	Wiederherstellungsschlüssel und PIN	9

© 2026 baramundi software GmbH

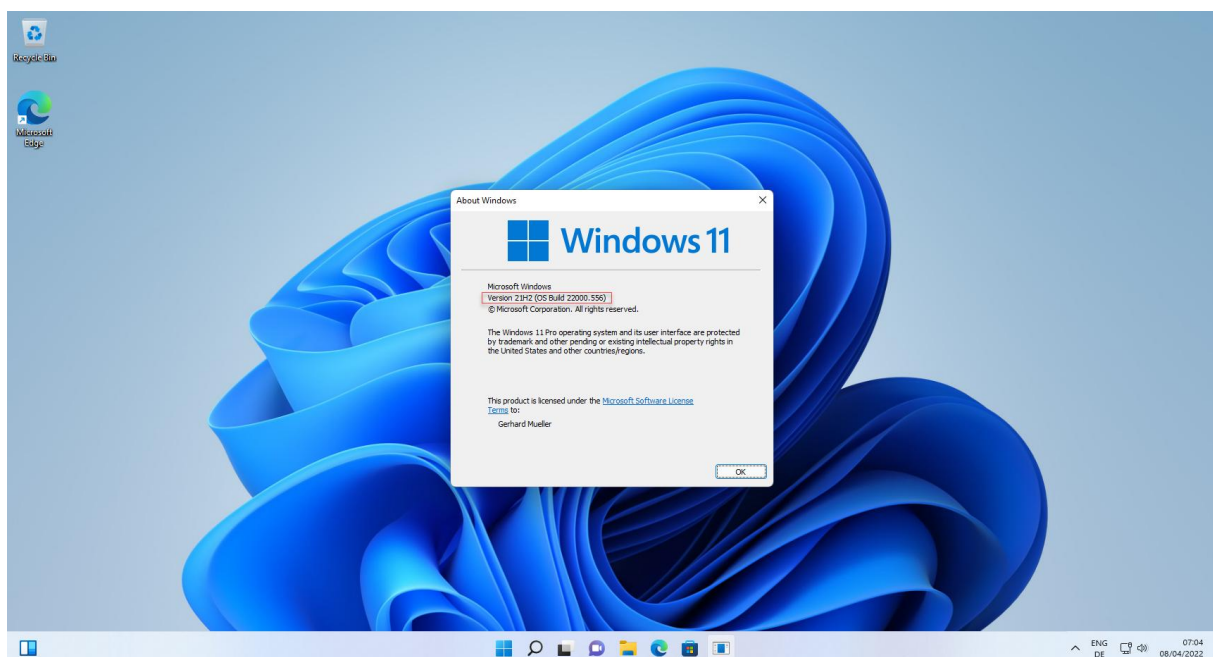
Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information.
Änderungen vorbehalten.

1 Windows 11 – Jährliches Release

Windows 11 Funktionsupdates werden nach dem "Windows as a Service"-Ansatz von Microsoft veröffentlicht. Theoretisch ist es relativ einfach, die neuen und verbesserten Funktionen dieser einmal jährlich erscheinenden Updates zu installieren, indem man den in den Windows Pro und Enterprise Editionen unterstützten In-Place-Upgrade-Prozess verwendet. In der Praxis müssen IT-Manager jedoch mit einem scheinbar endlosen Prozess des Testens und Verteilens von Updates für die verschiedenen Windows-Releases in ihren Netzwerken Schritt halten.

Sicherheitsupdates werden mindestens monatlich nach dem bekannten "Patch Tuesday"-Verfahren veröffentlicht. Darüber hinaus gibt es Ad-hoc-"Out-of-Band"-Patches, um schwerwiegendere Sicherheitslücken zu schließen, wenn sie entdeckt werden, oder um bestimmte Leistungsprobleme zu beheben, die sich aus früheren Updates ergeben.

Für Windows-Server und andere kritische oder spezialisierte Systeme bietet Microsoft eine Reihe von Serviceoptionen an. Viele Unternehmen entscheiden sich für den Long-Term Servicing Channel (LTSC), bei dem der Schwerpunkt auf der Stabilität liegt und alle zwei bis drei Jahre neue Versionen sowie bis zu zehn Jahre lang Sicherheitsupdates und Support angeboten werden. Letztendlich muss jedes Unternehmen selbst entscheiden, welcher Servicekanal seinen Leistungs- und Kostenanforderungen entspricht.



Windows 11 - Feature Release einmal im Jahr

2 Risiko alter Windows Versionen

Ältere Systeme sind anfälliger für Stabilitätsprobleme, die nicht mehr behoben werden, und stellen aufgrund ungepatchter Sicherheitslücken ein erhöhtes Sicherheitsrisiko dar. In vielen Fällen reicht ein einziger infizierter Computer aus, damit ein Angreifer das gesamte Netzwerk von innen heraus infiltrieren kann.

Die Nutzung von Windows 11 bringt nützliche Verbesserungen und Möglichkeiten für Benutzer und Administratoren. Sie birgt aber auch die typischen Risiken, die mit jeder Aktualisierung wichtiger Software einhergehen, darunter Inkompatibilitäten mit bereits verwendeter Software.



Die Situation verschärft sich noch, wenn eine Anwendung über verschiedene Betriebssystemreleases hinweg ausgeführt und unterstützt werden muss. Für Unternehmen, die Software verwenden, die angepasst oder intern entwickelt wurde, ist ein erheblicher Zeitaufwand erforderlich, um die Kompatibilität sicherzustellen.

Zeitmangel ist in der Regel eines der größten Hindernisse für eine saubere Versionsmigration. Eine unzureichende Vorbereitung bereitet Administratoren und Anwendern gleichermaßen langfristig Kopfzerbrechen. Andererseits kann eine sorgfältige Vorarbeit und die Verwendung der richtigen Tools langfristige Vorteile bringen und den laufenden Supportbedarf reduzieren.

3 Aktualisierung von Windows 11

3.1 Planung und Durchführung

Am Anfang steht eine Aufwandsabschätzung: Abhängig von der Unternehmensgröße und der Anzahl der betroffenen Endgeräte kann eine Versionsmigration durchaus einige Wochen in Anspruch nehmen.

Beim Durchdenken aller notwendigen Schritte gilt es nicht vom Optimalfall auszugehen, sondern einen großzügigen Puffer miteinzuplanen, um den mit an Sicherheit grenzender Wahrscheinlichkeit auftretenden Problemen zu begegnen.

3.2 Vorbereitung und Analyse

Als erstes muss eine Standardkonfiguration definiert werden, in dem die verfügbaren Optionen festgelegt werden. Damit ergibt sich auch die Rollout-Strategie. Sobald man einmal all diese Elemente durchdacht hat, kann man darangehen eine realistische Timeline zu definieren.

3.3 Umsetzung

Am Anfang steht ein Test, in der die Versionsmigration mit Testdaten simuliert und bereits die ersten Probleme aufgedeckt werden. In der zweiten Phase können ausgewählte Key User mit der neuen Version ausgestattet werden. In dieser Phase lassen sich dann die auftretenden Probleme dank der überschaubaren Nutzerzahl zügig beheben. Als nächstes erfolgt dann der eigentliche Rollout im Unternehmen. Hier gilt es zu jeder Welle an Rollouts auch Zeit für eine Nacharbeitsphase einzuplanen und die gewonnenen Erkenntnisse in der jeweils nächsten Welle mitaufzunehmen.

3.4 UEM-Hilfsmittel zur erfolgreichen Migration

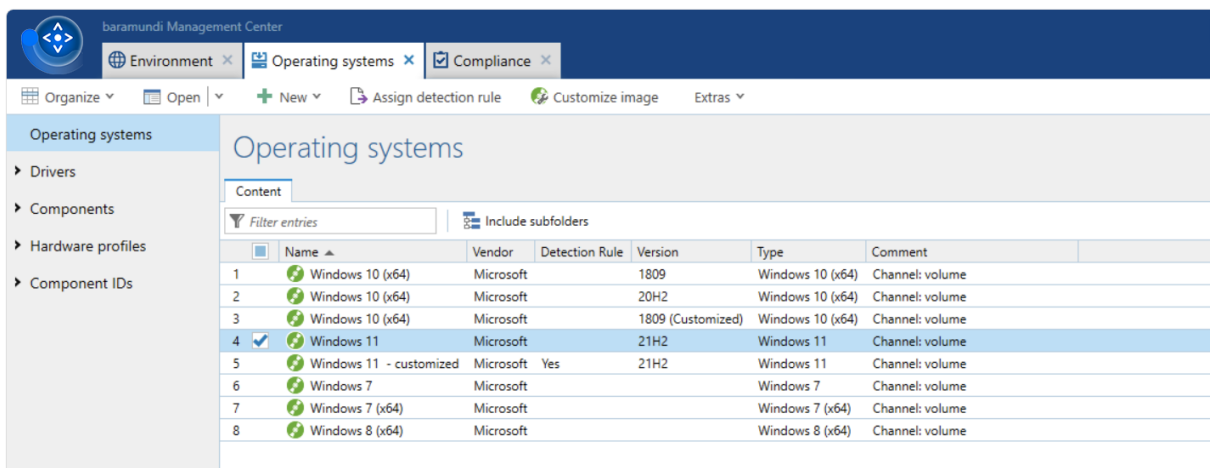
Um die Migration innerhalb Windows 11 möglichst reibungslos im ganzen Unternehmen durchzuführen, ist es für IT-Admins ratsam, die Vorteile einer Unified Endpoint Management (UEM) Lösung zu nutzen.

Der IT-Administrator muss also dafür sorgen, dass das neue Release möglichst schnell, sicher und unkompliziert auf die definierten Endpoints ausgerollt wird. Er sollte auch darauf achten, dass dabei unternehmensrelevante und userspezifische Einstellungen gesetzt bzw. beibehalten werden. Dabei kann ein UEM-System unterstützen. Die baramundi Management Suite bietet dafür z.B. folgende Funktion an: baramundi OS-Deployment und Configuration erlaubt eine vordefinierte Windows 11 Version mit allen Einstellungen sowie verfügbaren

Apps flächendeckend zu installieren, wobei die Qualität der einer manuellen, nativen Installation entspricht. baramundi Endpoint Automation ergänzt dies um die automatisierte Installation aller jeweils benötigten Anwendungen auf den Rechnern. baramundi Managed Software und Patch Management sorgen dann dafür, dass sowohl das OS als auch die Anwendungen kontinuierlich auf dem neuesten Patchstand gehalten werden und Sicherheitslücken schnell geschlossen werden.

3.5 Anpassung von Windows 11 Images

Windows 11 ermöglicht bereits während der Installation viele Konfigurationsmöglichkeiten, die wiederum abhängig vom eingesetzten Windows 11 Release sind. So kann der IT-Administrator bereits vor der Aktualisierung von Windows 11 unternehmensspezifische Anpassungen vornehmen. Diese Anpassungen können IT-Admins entweder durch manuelle Konfigurationen des Windows 11 Images vornehmen oder sie nutzen Tools, die sie dabei unterstützen. baramundi bietet hier das OS Customization Tool an, mit dem sich wichtige Windows 11 Optionen konfigurieren lassen.



Aufruf des baramundi OS Customization Tools im Bereich Betriebssysteme

3.5.1 Vielfältige Anpassungen für ein Windows-Image

Um nicht jede Konfiguration erneut durchführen zu müssen, besteht die Möglichkeit, die Anpassungen am Windows-Image in einer Konfigurationsvorlage zu speichern und ggf. bei weiteren Images wieder zu verwenden.



Übersichtliche Informationen der geladenen *.wim Datei

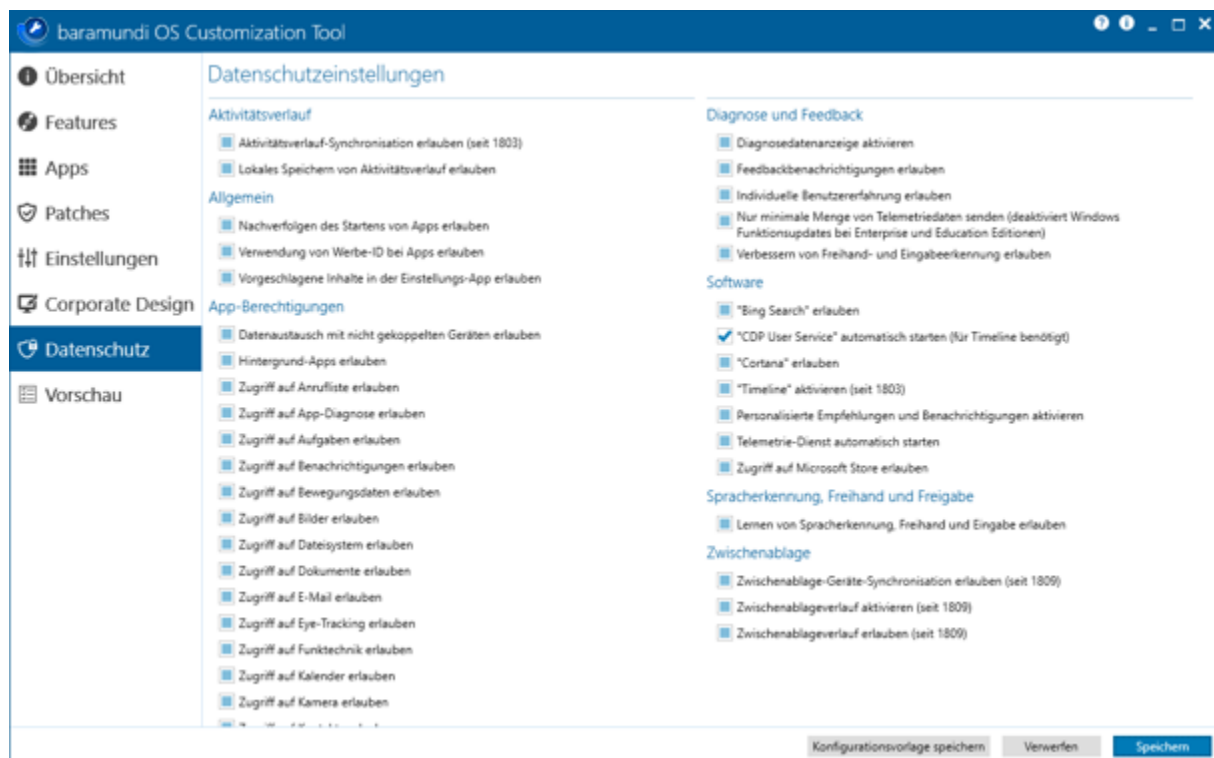
3.5.2 Patches

In diesem Bereich wird es dem IT-Admin ermöglicht, das Windows Image so anzupassen, dass er Microsoft Patches direkt in ein Windows Image aufnehmen oder veraltete kumulative Patches wieder entfernen kann, um dieses Image anschließend z.B. mit baramundi OS Deployment & Configuration zu installieren. Die separate Installation der Patches im Nachhinein ist damit nicht mehr nötig.

3.5.3 Einstellungen und Corporate Design und Datenschutz

Auch um geltende Compliance-Anforderungen und Corporate Identity Vorgaben im Unternehmen umsetzen zu können, bietet das baramundi OS Customizing Tool wertvolle Unterstützung bei der Anpassung des Windows-Images zum Thema Datenschutz. Denn es gibt einige Windows-Apps und Funktionen, die die Vorgaben der EU-DSGVO nicht oder nur zum Teil berücksichtigen. Mit dem OS Customization Tool haben IT-Admins die Möglichkeit, solche Funktionen zu deaktivieren und entsprechend ihrer Unternehmens-Compliance zu konfigurieren. So können IT-Admins z. B. schon in der Konfiguration Apps entfernen und Features aktivieren bzw. deaktivieren, um das Sammeln und Senden von Diagnosedaten oder funktionalen Daten¹ an Microsoft zu steuern bzw. einzuschränken.

¹ <https://docs.microsoft.com/de-de/windows/privacy/configure-windows-diagnostic-data-in-your-organization>



Zahlreiche Einstellungen für UI und Datenschutz

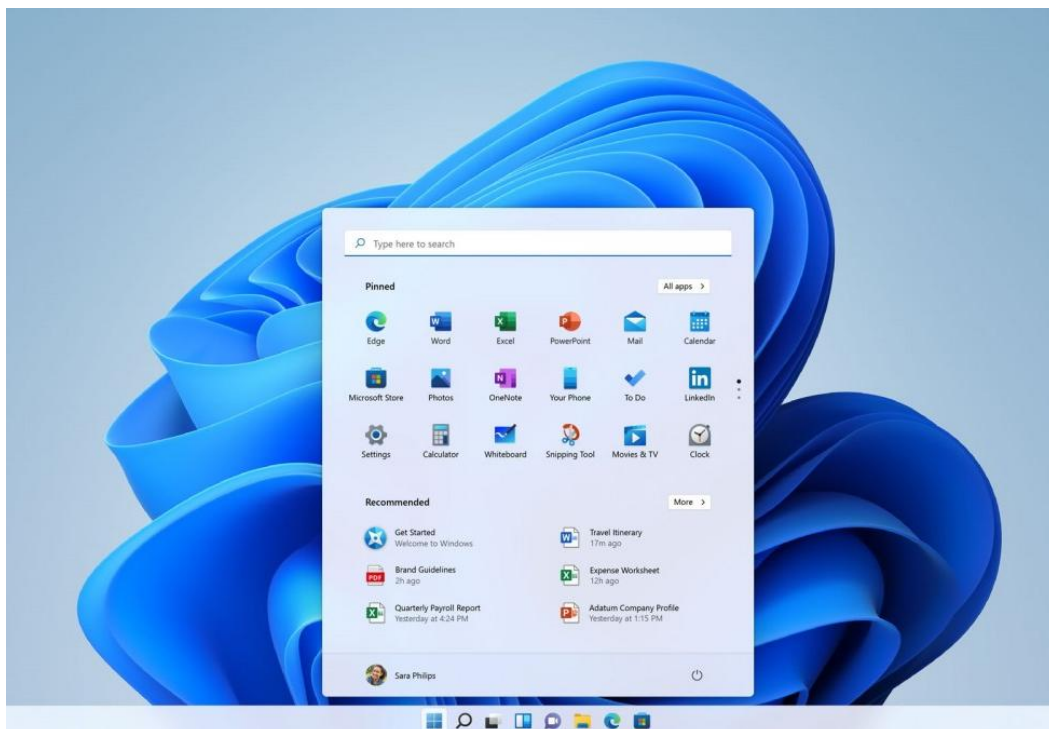
4 Absicherung Windows 11

4.1 Hilfsmittel zur Absicherung von Windows 11

Perfekte IT-Sicherheit gibt es nicht. Ein Administrator ist aber sehr wohl in der Lage Unbefugten den Zugriff auf die Systeme seiner IT-Infrastruktur so schwer wie möglich zu machen – die richtigen Tools vorausgesetzt.

Für die sichere und transparente Verschlüsselung der Datenträger eines Windows-Systems steht in Windows 11 Bitlocker zur Verfügung, um den unbefugten Datenzugriff durch einfaches Aus- und Umbauen des Datenträgers zu unterbinden. Zusätzlich kann das System beim Booten durch eine PIN geschützt werden. So wird sichergestellt, dass das System nur von einer befugten Person gestartet werden kann.

Um den Überblick darüber zu behalten, welche Systeme ganz, gar nicht oder nur zum Teil verschlüsselt sind, inventarisiert der baramundi Management Agent den Status des Bitlocker auf verwalteten Systemen und gibt detailliert Auskunft über den Zustand der Verschlüsselung auf den verschiedenen Partitionen. Diese Informationen werden sowohl auf der Übersichtsseite der Windows-Endpoints angezeigt und stehen auch als Filter für universelle dynamische Gruppen (UDG) zur Verfügung. So lässt sich schnell eine Übersicht über den Verschlüsselungszustand der verwalteten Endpoints gewinnen.



4.2 Konfiguration

Um einen zuverlässigen Schutz durch den Bitlocker zu erreichen, muss dieser zuerst entsprechend konfiguriert und aktiviert werden.

Hierzu bietet die baramundi Management Suite die Verwaltung eigener Bitlocker-Konfigurationsprofile an. Per Profil legt der Administrator die Verschlüsselungsmethode und die zu verschlüsselnden Laufwerke fest. So kann gezielt vorgegeben werden, ob nur das Systemlaufwerk oder auch zusätzlich alle Datenlaufwerke mitverschlüsselt werden sollen. Auch ob eine initiale PIN für den Betriebssystemstart mit entsprechender Komplexität verwendet werden soll kann vorgegeben werden. Diese PIN wird beim Einrichten der Verschlüsselung automatisch nach den Regeln des Profils generiert und gesetzt.

4.3 Wiederherstellungsschlüssel und PIN

Wiederherstellungsschlüssel und PIN werden bei der Aktivierung der Verschlüsselung in der baramundi Management Suite gespeichert. Die Wiederherstellungsschlüssel der Laufwerke werden regelmäßig inventarisiert und ebenfalls angezeigt. Diese Informationen stellen für den Administrator einen wertvollen Teil seiner Bitlocker Recovery Strategie dar. Diese Daten werden verschlüsselt gespeichert und durch das baramundi Berechtigungskonzept abgesichert. So erhält ein Administrator nur die Wiederherstellungsschlüssel für Systeme auf denen ihm dieses Recht explizit gewährt wurde.

Über die baramundi software GmbH

Die baramundi software GmbH sorgt als Spezialist für Unified Endpoint Management (baramundi Management Suite) und Proactive Endpoint Operations (baramundi Proactive Hub) dafür, dass Unternehmen und Organisationen effizient, sicher und plattformübergreifend Arbeitsumgebungen und digitale Arbeitsplätze managen – On-Prem und in der Cloud. Der Hauptsitz der baramundi software GmbH befindet sich in Augsburg. Die Produkte und Services des im Jahr 2000 gegründeten Unternehmens sind komplett Made in EU. Beim Vertrieb, der Beratung und Betreuung von Kunden arbeitet baramundi weltweit erfolgreich mit Partnerunternehmen zusammen.

www.baramundi.com

Sie möchten mehr über die baramundi Management Suite erfahren?

Melden Sie sich zum Live-Webinar an!

Erleben Sie im kostenfreien Webinar, wie Sie die baramundi Management Suite Ihre Endpoints, Server und Mobilgeräte automatisiert verwaltet und absichert.

www.baramundi.com/de/events-trainings/webinare/

Kontaktieren Sie uns.

Wir freuen uns auf Sie!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+49 821 56708-390
request@baramundi.com

Making IT Admins *Smile*

