



WHITE PAPER

Taking Control of Windows 11

Migration, Customization, and Securing

CONTENTS

1	Windows 11 – Annual Release.....	2
2	Risk of Outdated Windows Versions.....	3
3	Updating Windows 11	4
3.1	Planning and Execution.....	4
3.2	Preparation and Analysis	4
3.3	Implementation.....	4
3.4	UEM Tools for a Successful Migration.....	4
3.5	Customizing Windows 11 Images.....	5
4	Securing Windows 11	8
4.1	Tools for Securing Windows 11	8
4.2	Configuration.....	9
4.3	Recovery Key and PIN	9

© 2026 baramundi software GmbH

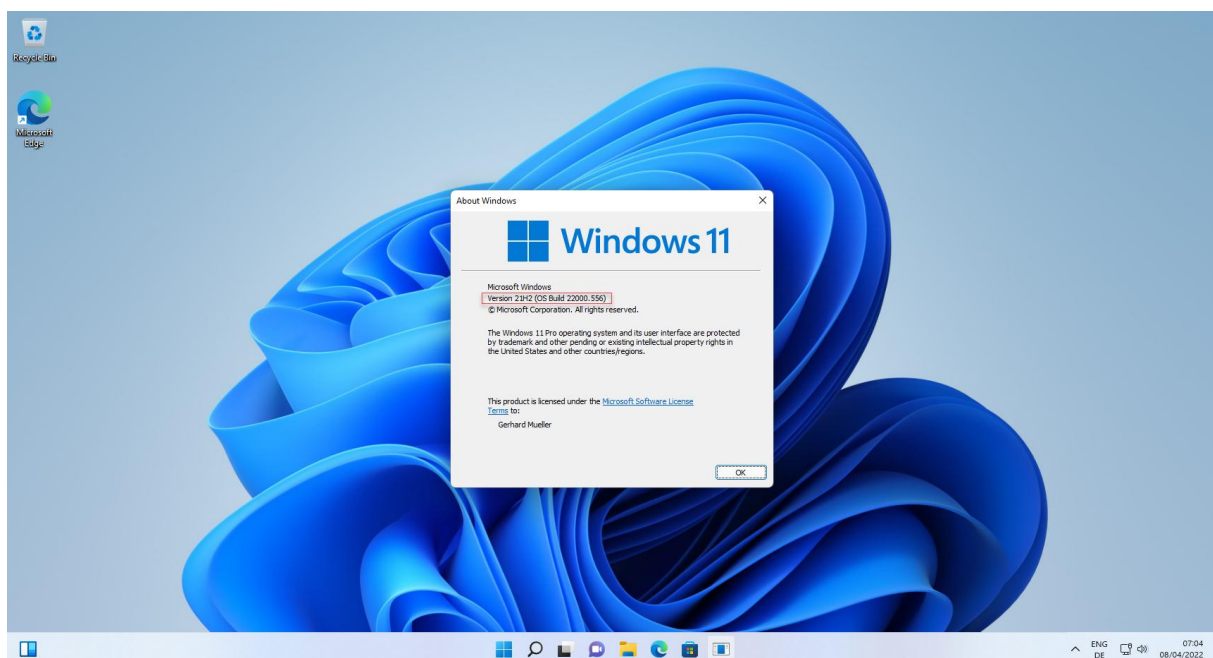
Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information.
Änderungen vorbehalten.

1 Windows 11 – Annual Release

Windows 11 feature updates are released by Microsoft following the "Windows as a Service" approach. In theory, it is relatively straightforward to install the new and improved features of these annually released updates by using the in-place upgrade process supported in the Windows Pro and Enterprise editions. In practice, however, IT managers must keep pace with a seemingly endless process of testing and deploying updates for the various Windows releases across their networks.

Security updates are released at least monthly under the well-known "Patch Tuesday" process. In addition, there are ad hoc "out-of-band" patches to close more serious vulnerabilities as they are discovered, or to fix specific performance issues resulting from earlier updates.

For Windows Server and other critical or specialized systems, Microsoft offers a range of servicing options. Many organizations opt for the Long-Term Servicing Channel (LTSC), which focuses on stability and provides new versions every two to three years along with up to ten years of security updates and support. Ultimately, every organization must decide for itself which servicing channel best fits its performance and cost requirements.



Windows 11 – Feature Release once a year

2 Risk of Outdated Windows Versions

Older systems are more susceptible to stability issues that are no longer fixed and pose an increased security risk due to unpatched vulnerabilities. In many cases, a single infected computer is enough for an attacker to infiltrate the entire network from within.

Using Windows 11 brings useful improvements and capabilities for users and administrators alike. However, it also carries the typical risks associated with any major software update, including incompatibilities with software already in use.



The situation becomes even more challenging when an application must run and be supported across multiple operating system releases. For organizations using customized or in-house developed software, ensuring compatibility requires a significant investment of time.

Lack of time is typically one of the biggest obstacles to a clean version migration. Inadequate preparation causes long-term headaches for administrators and users alike. On the other hand, careful groundwork and the use of the right tools can deliver long-term benefits and reduce ongoing support requirements.

3 Updating Windows 11

3.1 Planning and Execution

The starting point is an effort estimate: depending on the size of the organization and the number of affected endpoints, a version migration can easily take several weeks.

When thinking through all the necessary steps, it is important not to assume a best-case scenario but instead to plan in a generous buffer to address the problems that will almost certainly arise.

3.2 Preparation and Analysis

The first step is to define a standard configuration that specifies the available options. This also determines the rollout strategy. Once all these elements have been thought through, a realistic timeline can be defined.

3.3 Implementation

The process begins with a test in which the version migration is simulated using test data, uncovering the first issues early on. In the second phase, selected key users can be equipped with the new version. Thanks to the manageable number of users in this phase, any issues that arise can be resolved quickly. Next comes the actual company-wide rollout. For each rollout wave, it is important to also plan time for a follow-up phase and to incorporate the lessons learned into the next wave.

3.4 UEM Tools for a Successful Migration

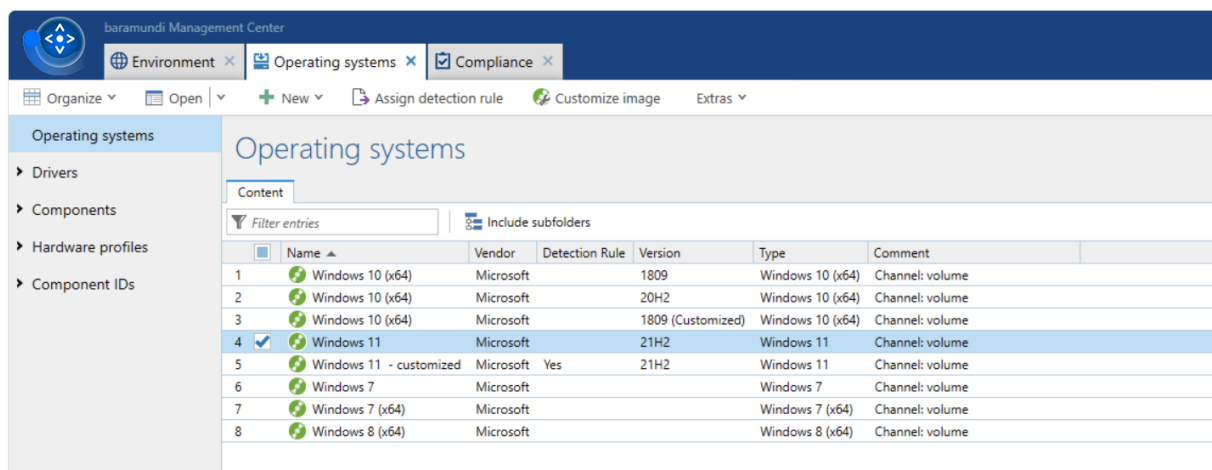
To carry out the Windows 11 migration as smoothly as possible across the entire organization, IT admins are well advised to take advantage of a Unified Endpoint Management (UEM) solution.

The IT administrator must ensure that the new release is rolled out to the defined endpoints as quickly, securely, and straightforwardly as possible. They should also make sure that business-relevant and user-specific settings are applied or retained accordingly. A UEM system can provide valuable support here. The baramundi Management Suite, for example, offers the following functionality: baramundi OS Deployment and Configuration enables a predefined Windows 11 version, complete with all settings and available apps, to be installed enterprise-wide at a quality level equivalent to a manual, native installation. baramundi Endpoint Automation complements this with the automated installation of all applications

required on each machine. baramundi Managed Software and patch management then ensure that both the OS and the applications are continuously kept up to date with the latest patches, closing vulnerabilities quickly.

3.5 Customizing Windows 11 Images

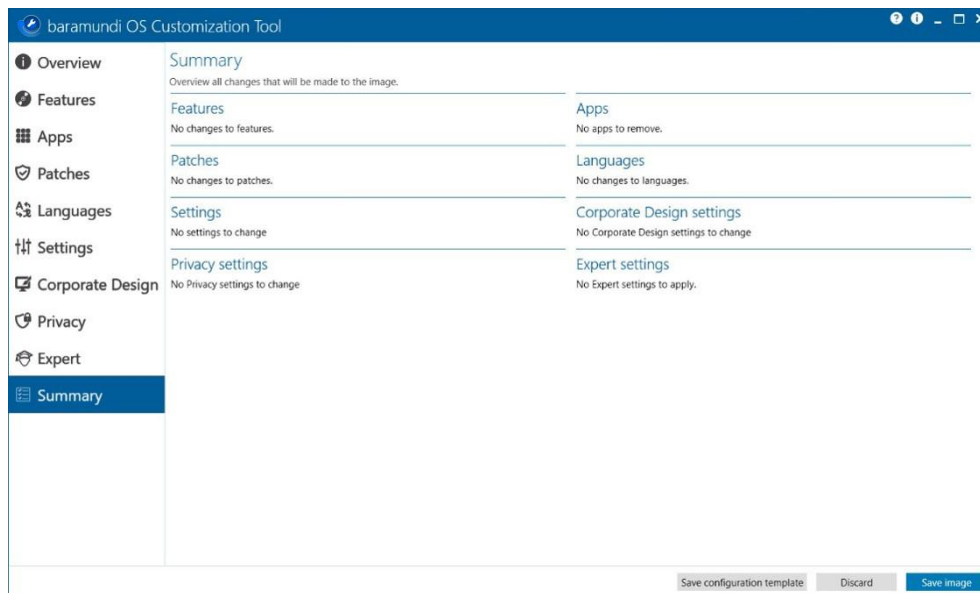
Windows 11 already offers many configuration options during installation, which in turn depend on the Windows 11 release in use. This allows the IT administrator to make company-specific customizations even before updating Windows 11. IT admins can make these customizations either through manual configuration of the Windows 11 image or by using tools that support them in this process. baramundi offers the OS Customization Tool for this purpose, which allows important Windows 11 options to be configured.



Launching the baramundi OS Customization Tool in the Operating Systems section

3.5.1 Extensive Customization Options for a Windows Image

To avoid having to repeat every configuration step, customizations to the Windows image can be saved in a configuration template and reused for additional images as needed.



*Clear overview of information for the loaded *.wim file*

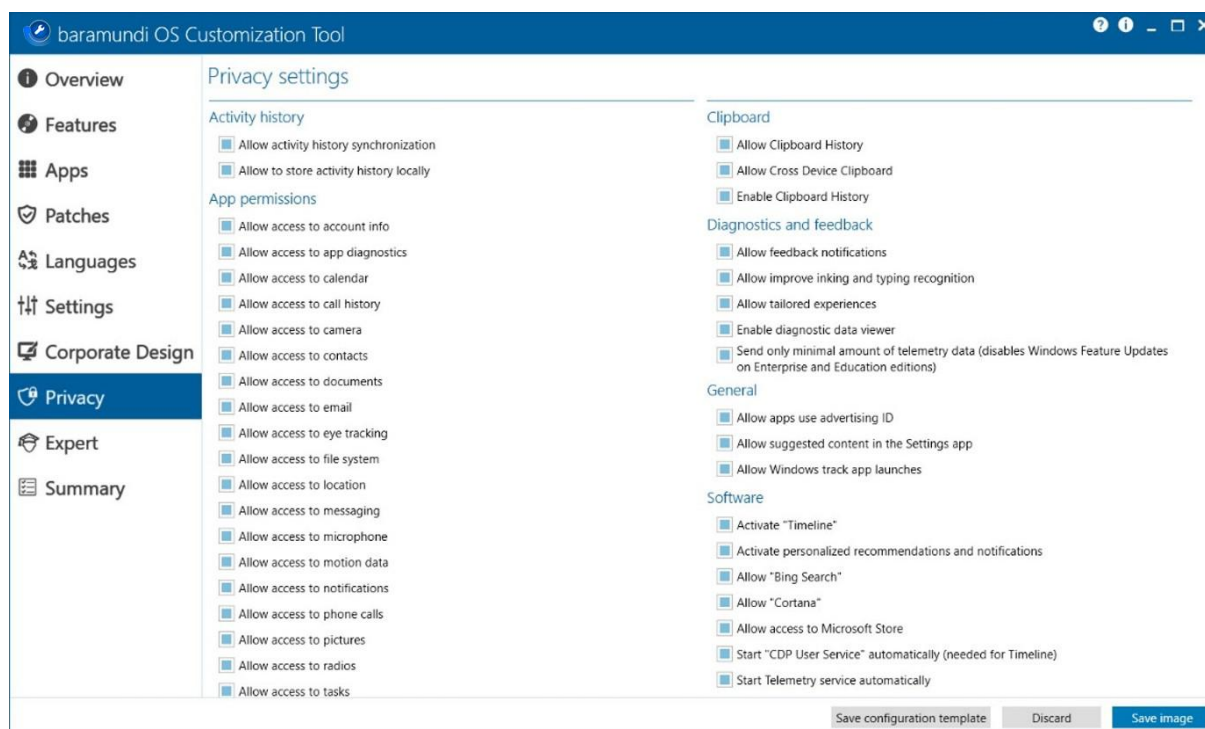
3.5.2 Patches

In this area, IT admins can customize the Windows image so that Microsoft patches can be integrated directly into a Windows image, or outdated cumulative patches can be removed, in order to subsequently install this image using, for example, baramundi OS Deployment & Configuration. This eliminates the need to install patches separately afterward.

3.5.3 Settings, Corporate Design, and Data Protection

To help implement applicable compliance requirements and corporate identity guidelines within the organization, the baramundi OS Customization Tool also provides valuable support for adapting the Windows image with regard to data protection. This is because there are several Windows apps and features that do not fully – or only partially – comply with GDPR requirements. With the OS Customization Tool, IT admins can disable such features and configure them according to their organization's compliance requirements. For example, IT admins can already remove apps and enable or disable features during configuration to control or restrict the collection and transmission of diagnostic or functional data¹ to Microsoft.

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



Numerous settings for UI and data protection

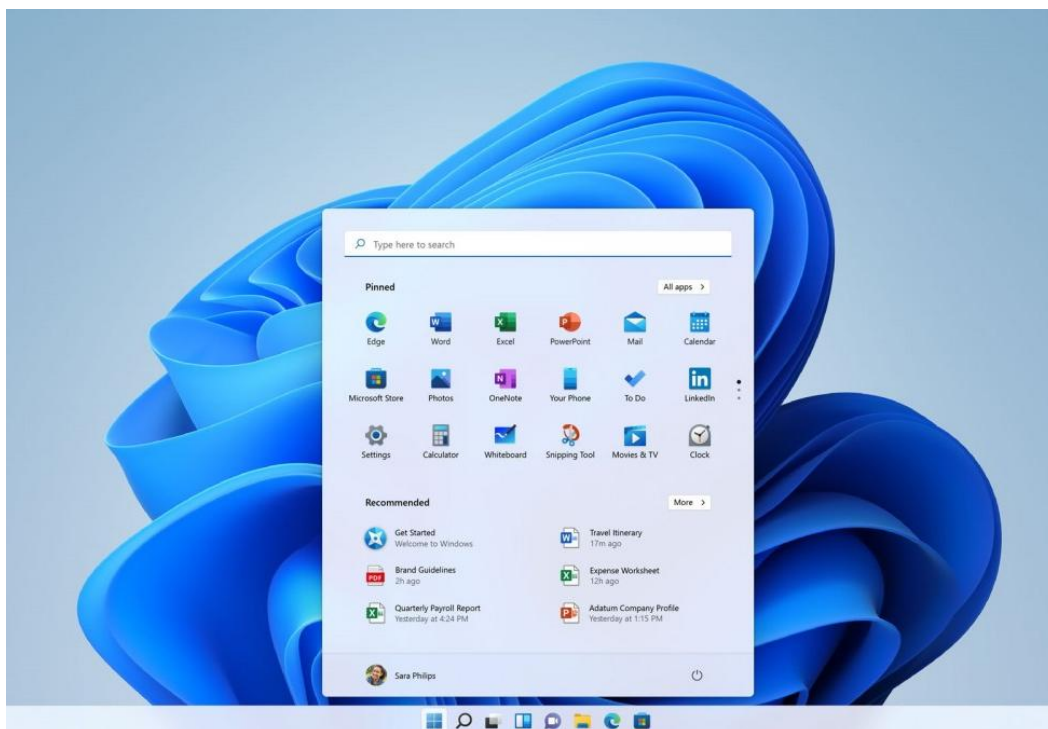
4 Securing Windows 11

4.1 Tools for Securing Windows 11

There is no such thing as perfect IT security. However, an administrator is very much able to make it as difficult as possible for unauthorized parties to access the systems in their IT infrastructure — provided the right tools are in place.

Windows 11 includes BitLocker for secure and transparent encryption of a Windows system's storage drives, preventing unauthorized data access through simple removal or swapping of the drive. In addition, the system can be protected during boot with a PIN, ensuring that it can only be started by an authorized person.

To maintain an overview of which systems are fully, partially, or not at all encrypted, the baramundi Management Agent inventories the BitLocker status on managed systems and provides detailed information on the encryption status of the various partitions. This information is displayed on the overview page for Windows endpoints and is also available as a filter for universal dynamic groups (UDGs). This makes it possible to quickly gain an overview of the encryption status of managed endpoints.



4.2 Configuration

To achieve reliable protection through BitLocker, it must first be configured and activated accordingly.

For this purpose, the baramundi Management Suite offers management of dedicated BitLocker configuration profiles. Through a profile, the administrator defines the encryption method and the drives to be encrypted. This allows precise control over whether only the system drive or additionally all data drives should be encrypted. It is also possible to specify whether an initial PIN with a defined level of complexity should be used for operating system startup. This PIN is automatically generated and set according to the profile's rules when encryption is configured.

4.3 Recovery Key and PIN

Recovery keys and PINs are stored in the baramundi Management Suite when encryption is activated. The recovery keys for the drives are regularly inventoried and also displayed. This information represents a valuable part of the administrator's BitLocker recovery strategy. This data is stored in encrypted form and protected by the baramundi permission concept. As a result, an administrator only receives the recovery keys for systems for which they have been explicitly granted this right.

About baramundi software GmbH

baramundi software's Unified Endpoint Management (baramundi Management Suite) and Proactive Endpoint Operations (baramundi Proactive Hub) solutions enable organizations to manage IT environments and digital workplaces efficiently, securely, and across platforms – on-premises and in the cloud. baramundi software GmbH is headquartered in Augsburg, Germany. Founded in 2000, the company develops its products and services in the EU and supports them through offices in the U.S., Italy, and Poland. baramundi also collaborates with sales, consulting, and customer support partners worldwide.

More information about baramundi: www.baramundi.com

Register for our live webinar to learn more about the baramundi Management Suite!

Discover how the baramundi Management Suite automatically manages and secures your endpoints, servers, and mobile devices, then try it free for 30 days in your own network.

www.baramundi.com/EN/events-trainings/webinars/

Get in Touch!

We are looking forward to meeting you!



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



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



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



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+49 821 56708-390
request@baramundi.com

Making IT Admins *Smile*