



Microsoft Update Management Guide

CONTENTS

1	From a quick patch to a monthly routine.....	2
1.1	From Patch to Update	2
1.2	The Microsoft Update Paradigm.....	3
1.3	Microsoft Deployment Rings.....	3
2	How baramundi Microsoft Update Management Works.....	4
2.1	Update Profiles.....	4
2.2	Classifications	4
2.3	Microsoft Update for Business (starting with Windows 10)	5
2.4	Prerequisites	6
2.5	Group Policy Configuration	6
3	Microsoft Update Online.....	7
3.1	Pros	7
3.2	Cons	7
4	Windows Server Update Services	8
4.1	Pros	8
4.2	Cons	8
5	Working with baramundi Microsoft Update Management	9
5.1	Managing Update Profiles	9
5.2	Job Configuration	11
5.3	Evaluation at the Endpoint	12
5.4	Evaluation for Groups.....	13

© 2021 baramundi software GmbH

Statements about equipment and technical functionalities are non-binding and serve only as information.
Subject to change without notice. DocID BMUM-210200-WP-211014-EN

1 From a quick patch to a monthly routine

1.1 From Patch to Update

Over the past two decades, admins and IT managers have been excellently conditioned: The software in use must be updated regularly. With increasing digitization and networking, an endpoint could no longer be isolated, but had to be viewed as part of a collective of connected IT assets worth protecting. Security vulnerabilities at an endpoint no longer simply compromised the security of the individual device, they weakened the security of the entire enterprise.

Software vendors responded by providing patches for individual vulnerabilities -- allowing managers to decide for themselves whether and which gaps to patch. As time went on, more and more patches were provided at irregular intervals. This made it difficult to keep track of overall security status. To address this issue, more and more companies -- first and foremost Microsoft -- introduced the so-called "Patch Day". On a fixed day each month, software vendors released a mixed bag of security patches. The IT department then had the regular task of testing and distributing these patches throughout the company. Elaborate tests were sometimes necessary because a patch could, under certain circumstances, "brick" a system and render it unusable. Over time, operating system feature updates and security-related patches were added to the Patch Day line-up, further increasing the time and effort that IT admins needed for testing. Even after a new installation of Windows, all the required patches had to be installed in the appropriate order, often with numerous reboots.

IT departments managed the growing workload by prioritizing or "cherry picking" the various updates and patches. Particularly critical patches were tested and installed, while less critical patches and function updates were omitted.

Microsoft countered this problem by introducing cumulative updates. These monthly update packages contain the latest security patches and feature updates, as well as the patches and updates from the previous packages. For example, after a new installation, only the latest cumulative update needs to be installed instead of what had been an average of 100+ patches. This saves time and eliminates the need to choose which patches are installed or skipped.

1.2 The Microsoft Update Paradigm

Like any responsible software vendor, Microsoft naturally recommends keeping endpoints as up-to-date as possible. At the same time, however, it is understandable that not all endpoints can or should be provided with the same updates at the same time. After all, some endpoints are more critical than others. A standard office PC, for example, is generally less critical for company operations than a specially configured CAD or data acquisition system. In the event of a problem, the former could be replaced much more easily than the two specialized devices.

1.3 Microsoft Deployment Rings

The Microsoft deployment ring concept is based on the update paradigm¹. A deployment ring comprises groups of devices that receive an update at the same time. These devices should represent a broad and representative cross-section of systems categorized by criticality. Typical rings could be:

- **Preview and first tests**
The preview ring is not intended for broad use in the company and is used to evaluate new features included in an update. Dedicated test clients and the devices of technically experienced people primarily are in this ring. They don't automatically lose productivity when something doesn't go according to plan.
- **Early adopters - pilots and testing**
Putting this ring together requires proper planning. It should be made up of representative devices with the company's typical hardware and applications installed. Of course, these should be devices in regular use in order to identify problems quickly. The IT department and dedicated test devices do not belong in this ring because they usually do not represent typical company endpoints.
- **Broad distribution**
This ring contains all remaining devices not included in the other rings.

These three rings enable very timely distribution of updates and patches. However, experience shows that three rings often are not sufficient for pre-deployment testing in more complex network environments. For this reason, Microsoft does not limit the number of rings to enable further subdivision of endpoints based on locations or purposes (client/server). In large companies it is also advisable to consider the capacity of the helpdesk when deciding on the size of the rings.

You can improve efficiency and optimize overall deployment times by using the automation of the baramundi Management Suite (bMS) so that IT teams only have to intervene manually in the event of an error. That means you that you can provide updates to each ring in sequence with some overlap, with the devices in each ring automatically updated following a time offset defined by IT.

¹ <https://docs.microsoft.com/en-us/windows/deployment/update/create-deployment-plan>

2 How baramundi Microsoft Update Management Works

2.1 Update Profiles

Update Management with the bMS consistently relies on the deployment ring concept and extends it with the option to exclude individual updates, entire product lines and even complete categories of updates from deployment. With the help of a blocklist, there is no need to manually approve the updates. New updates are released automatically and are installed with a configured time offset from the release date, starting with the least critical ring.

The division into the different rings as well as the configuration of the blocklists is done with update profiles for each ring. The settings in the applicable update profile are also taken into account when evaluating the update status of an endpoint. The management of update profiles is described in chapter 5.1.

2.2 Classifications

All updates from Microsoft are divided into classifications, which Microsoft describes as follows²:

- **Security Updates**
A generally released fix for a product-specific vulnerability. Vulnerabilities are classified as critical, important, moderate, or low based on their severity level in the Microsoft Security Bulletin.
- **Critical Updates**
A generally released fix for a specific issue that addresses a critical, non-security-related bug.
- **Definition Updates**
A frequently released software update that contains additions to a product's definition database. Definition databases are often used to detect objects with certain attributes, such as malicious code, phishing websites, or junk email.
- **Updates**
A generally released fix for a specific non-critical, non-security-related bug.
- **Upgrades**
In-place upgrade of Windows 10 (e.g., from 1909 to 2004). These are performed via the baramundi OS-Install module, as this is the only way to tailor the Windows installation to company guidelines.
- **Service packs**
A tested, cumulative set of all hotfixes, security updates, critical updates and updates. Service packs may also contain additional fixes for issues found internally since the product's release, as well as a limited number of customer-requested design changes or features.

² <https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates>

- **Tools**
A utility or feature that helps perform a task or group of tasks.
- **Feature Packs**
New product functionality that is first distributed outside the context of a product version and is often included in the next full product release.
- **Update Rollups**
A tested, cumulative set of hotfixes, security updates, critical updates, and updates packaged for easy deployment. A rollup generally targets a specific area.
- **Drivers**
Software that controls interaction with devices.

2.3 Microsoft Update for Business (starting with Windows 10)

With Microsoft Update for Business, Microsoft has introduced a new nomenclature for updates. Microsoft does not differentiate on the basis of the classifications above, but as follows:

- **Feature Updates**
Released twice a year, in the first and second half of each calendar year. Feature Updates add new features and functionality to Windows 10.
- **Quality Updates (Cumulative Updates).**
Provide both security updates and non-security-related fixes for Windows 10. Quality updates include security updates, critical updates, Servicing Stack Updates (SSUs), and driver updates. They are usually released on the second Tuesday of each month but can be released at any time. The Second Tuesday release focuses on security updates. Quality updates are cumulative, so installing the latest quality update is enough to get all available fixes for a given Windows 10 feature update, including any out-of-band security updates and SSUs that were released previously.
- **Driver updates**
These update drivers apply to your devices. Driver updates are disabled by default in Windows Server Update Services (WSUS), but for cloud-based update methods you can control whether or not they are installed.
- **Microsoft product updates**
These update other Microsoft products, such as Office. You can enable or disable product updates using policies controlled by various maintenance tools.
- **Updates definition**
A commonly released and frequent software update that contains additions to a product's definition database. Definition databases are often used to detect objects with certain attributes, such as malicious code, phishing websites, or junk email.
- **Servicing Stack Updates (SSUs)**
SSUs have a special role and cannot be installed automatically via Update Management. They update the components that are needed for the other updates. SSUs appear irregularly and much less frequently than the regular updates.

2.4 Prerequisites

baramundi Microsoft Update Management supports Windows from version 8.1 without further adjustments. For Windows 7 SP1 and Windows Server 2008 R2 SP1, at least the following requirements must be met:

- Support for SHA-2 code signing as of September 2019 (KB4474419³).
- Servicing Stack Update as of March 2019 (KB4490628⁴)

Windows Server 2008 SP 2 must meet at least the following prerequisites:

- SHA-2 code signing support as of September 2019 (KB4474419³)
- Servicing Stack Update as of April 2019 (KB4493730⁵)

Older Windows versions are not supported.

2.5 Group Policy Configuration

Since Microsoft recommends that endpoints always be kept up-to-date, Windows is delivered with a corresponding standard configuration. In order to use the full potential of the ring concept and baramundi update profiles, the standard configuration must be modified.

The following configurations are particularly noteworthy:

- **Automatic updates**
Automatic updates must be deactivated when using the online sources and when using WSUS. Otherwise, Windows will update itself and the baramundi central management system will no longer be in control.
- **Dual scan**
When using WSUS, care must be taken to ensure that dual scan has been deactivated. Otherwise, there are functional limitations, for example, in the delay of updates.
- **Update source**
If a WSUS is used as the source for the updates, the URL to the corresponding system must be specified via group policy.

A detailed list of the required and recommended settings as well as instructions for configuration can be found in the baramundi Knowledge Base.⁶

³ <https://support.microsoft.com/en-us/topic/2019-sha-2-code-signing-support-requirement-for-windows-and-wsus-64d1c82d-31ee-c273-3930-69a4cde8e64f>

⁴ <https://support.microsoft.com/en-us/topic/servicing-stack-update-for-windows-7-sp1-and-windows-server-2008-r2-sp1-march-12-2019-b4dc0cff-d4f2-a408-0cb1-cb8e918fee8a>

⁵ <https://support.microsoft.com/en-us/topic/servicing-stack-update-for-windows-server-2008-sp2-april-9-2019-8f49b928-2090-0cce-3ed6-21b6dc8c494b>

⁶ <https://feedback.baramundi.de/knowledge-base/article/KB10911-EN>

3 Microsoft Update Online

Microsoft provides all relevant updates via its own service "Microsoft Update." Another online service is "Windows Update." This is basically the same source, but with a reduced scope. While "Microsoft Update" provides updates for all supported Microsoft products (Exchange Server, MSSQL server, etc.), operating system updates can only be found via "Windows Update".

Using an online source offers several advantages and disadvantages. It is important to understand them to choose the right source for your environment.

3.1 Pros

- Immediate availability after release by Microsoft.
- Assurance of always receiving the correct update in the correct revision.
- No central storage required -- endpoints obtain installation sources directly from Microsoft or via peer-to-peer (P2P).
- There is no need to operate a WSUS.

3.2 Cons

- Internet connection required – cannot be used if endpoints do not have internet access.

4 Windows Server Update Services

With "Windows Server Update Services" or "WSUS" for short, Microsoft provides a software component which, among other things, makes it possible to mirror the Microsoft online services in the company's own network. This enables local availability of the data required for updating endpoints.

There are advantages and disadvantages here as well.

4.1 Pros

- Endpoints do not require an Internet connection.
- Updates are downloaded only once and kept locally.

4.2 Cons

- Additional effort for the maintenance of the required infrastructure.
- Possible delayed availability of updates.
- Different data between local and online sources, since WSUS always uses the time stamp of the local deployment.

5 Working with baramundi Microsoft Update Management

5.1 Managing Update Profiles

First, the rings relevant to your own company are defined using your own criteria. Then the update profiles required to map the rings are created in the baramundi Management Suite. Meaningful names and, if necessary, supplementary comments should be used here. The delay of the updates is specified in days.

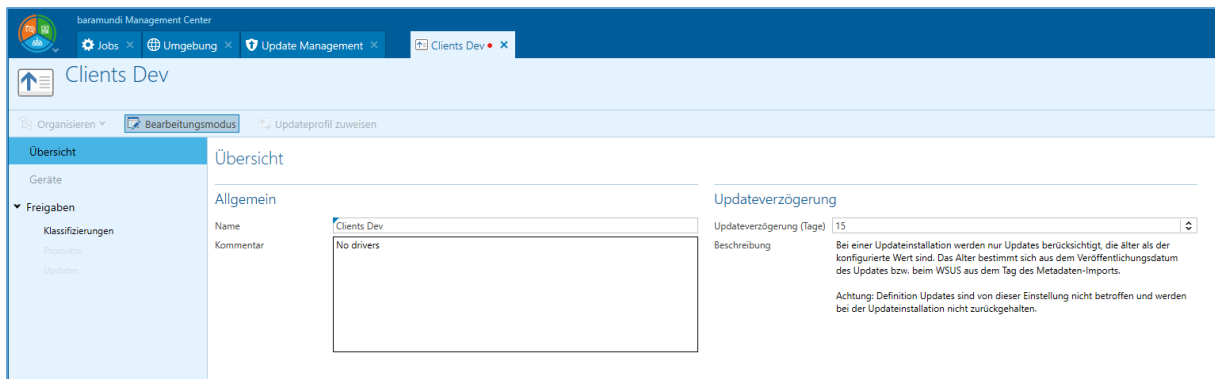


Figure 1 – Creation of an update profile

It should be noted here that definition updates are generally not delayed by the baramundi Management Suite, as this would impair the function of Windows Defender Antivirus.

In the next step, the classifications to be generally released are determined. For security reasons -- and to ensure that the system is continuously as up-to-date as possible -- all classifications should be selected whenever possible. The "Upgrades" and "Drivers" classifications are an exception to this recommendation (see Section 2.2).

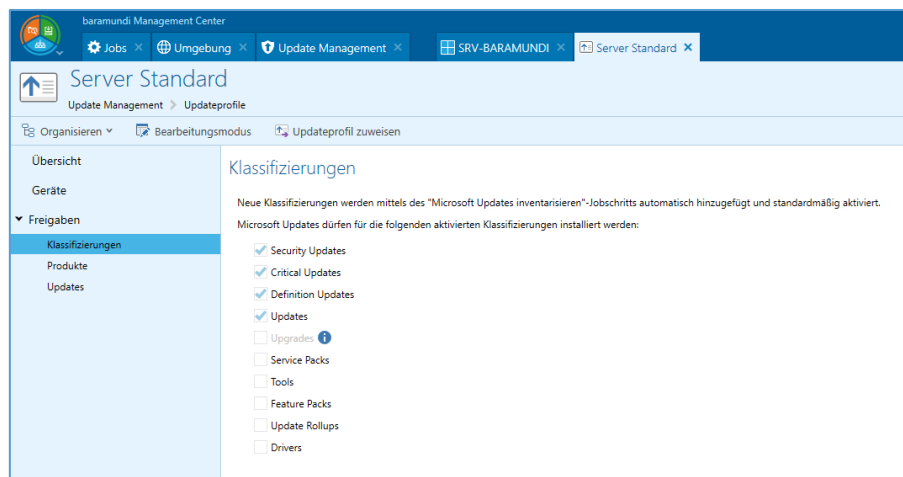


Figure 2 - Released classifications of an update profile

Depending on requirements, complete products or granular individual updates can be blocked in the update profile.

For example, if "Microsoft Silverlight" should not be installed and updated on company computers, it can be marked as blocked in the update profile and excluded from distribution.

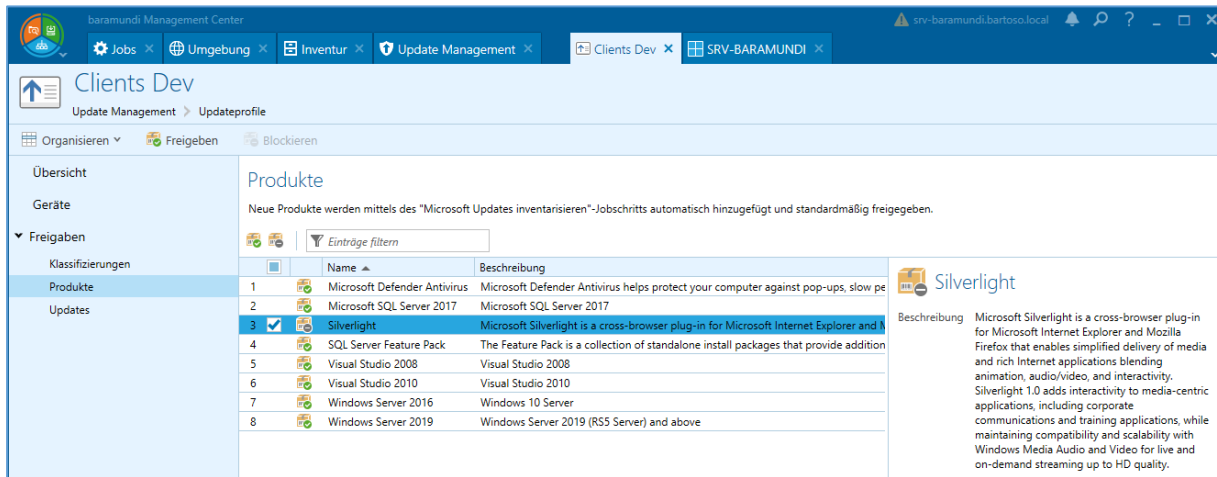


Figure 3 - Release and blocking of products in the update profile

These releases not only affect the distribution, but also directly affect the inventory. That ensures that it is always apparent whether updates are missing on the endpoint and whether they are delayed or blocked.

5.2 Job Configuration

All actions relevant to the endpoint are combined in the "Manage Microsoft Updates" job step. Both an inventory and the update can be selected there.

In both cases, three sources are available for selection:

- Microsoft Update Online⁷
Includes updates for both Windows and many other Microsoft products.
- Windows Update Online⁷
Includes updates for Windows only. Other products are not covered.
- Windows Server Update Services (WSUS)⁸
Includes all updates that are also available through Microsoft Update Online. The scope offered to the endpoints can be configured and customized by the admin.

An inventory should be performed regularly, at least once a week. Inventory determines the current update status of the endpoint but does not install updates.

Although the choice of source in the job step allows the greatest possible flexibility, you should decide on one source in advance and stick to it. Mixing online and offline sources is strongly discouraged. In practice, the data from WSUS sometimes deviates from the data from the online sources. This leads to inconsistencies and can become problematic especially with regard to the release date and proper operation of the time offset or delay that you define.

The action "Distribute Microsoft Updates" is used to install the updates. You should always select the same source that was used for the inventory.

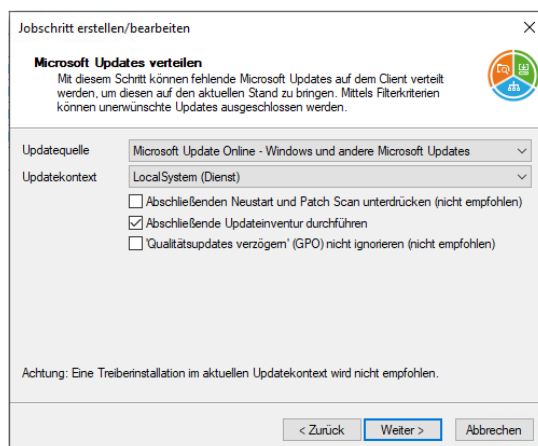


Figure 4 - Configuration of the "Distribute Microsoft Updates" action in the "Manage Microsoft Updates" job step "

For special cases, it is also possible to suppress the restart normally required for updates. This is not recommended. System updates usually are not completed until the reboot, so some installed updates will not be detected correctly until after the next reboot.

⁷ Endpoint requires an internet connection.

⁸ The WSUS must be installed, configured and operated in your own infrastructure.

The final inventory, on the other hand, is strongly recommended. It ensures that the endpoint update status resulting from the update process is correctly reported to the baramundi Management Server and accurately displayed in subsequent endpoint update status evaluations.

In the next step, you can select the specifications for updating endpoints as part of a job:

- **Manual configuration**
All settings such as classification, included and excluded products/updates and time delay are granularly adjustable.
- **Update profile**
The update process applies the settings in the update profile assigned to the endpoint. If no update profile is assigned, the job step is aborted and the endpoint is not updated.

For a consistent and predictable update strategy, the use of update profiles is strongly recommended. Manual configuration should only be used in individual cases or for test purposes.

5.3 Evaluation at the Endpoint

The current update status of an endpoint is displayed with a colored status bar for a quick overview, and with a detailed list of the relevant updates.

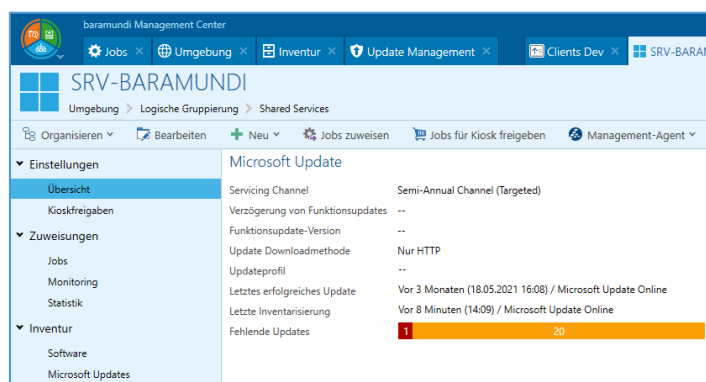


Figure 5 - Update state on the overview page of an endpoint

The evaluation of the update status is based on the settings of the update profile if assigned. An endpoint is not evaluated as up-to-date until the required updates are installed, blocked or delayed. Without an update profile, neither the blocking nor the delay of updates can be taken into account.

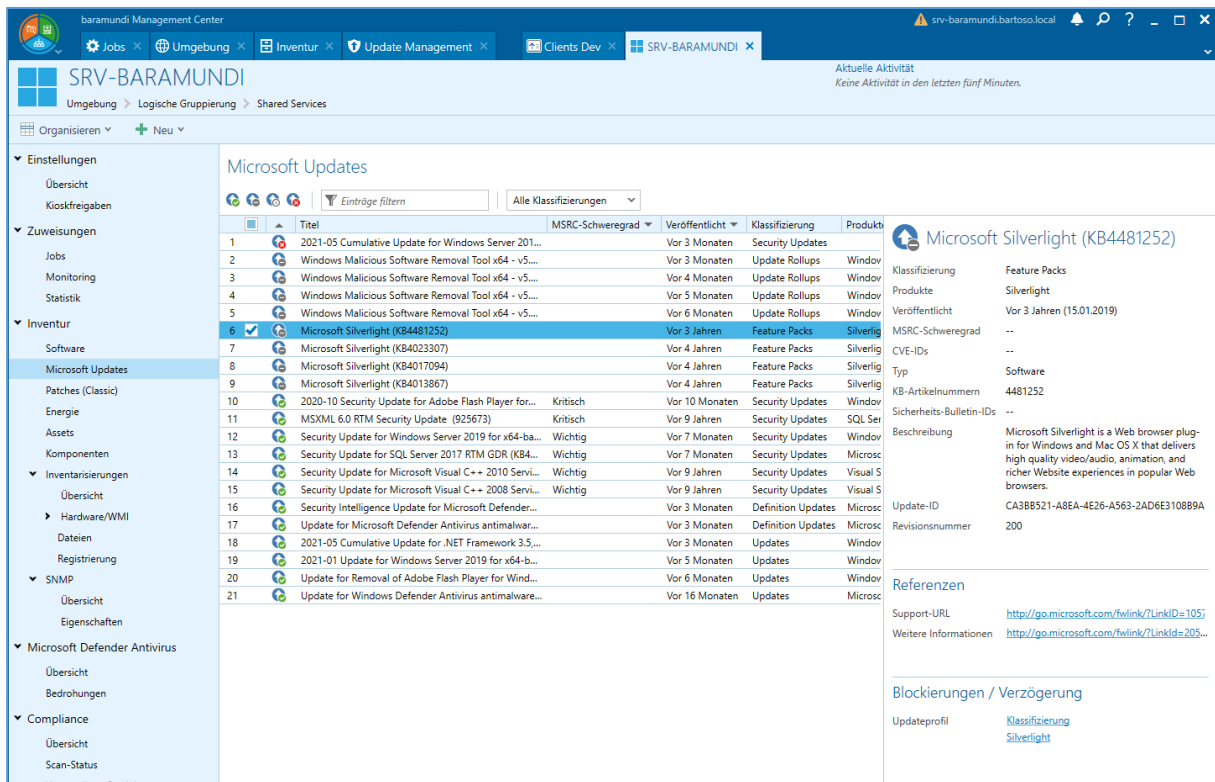


Figure 6 – Update inventory at the endpoint

5.4 Evaluation for Groups

Update profiles are not only used to release/block and delay updates, but also to evaluate the update status. This allows you to quickly see whether an endpoint complies with the specifications of the update profile, whether all endpoints assigned to the update profile are compliant, or if action is required.

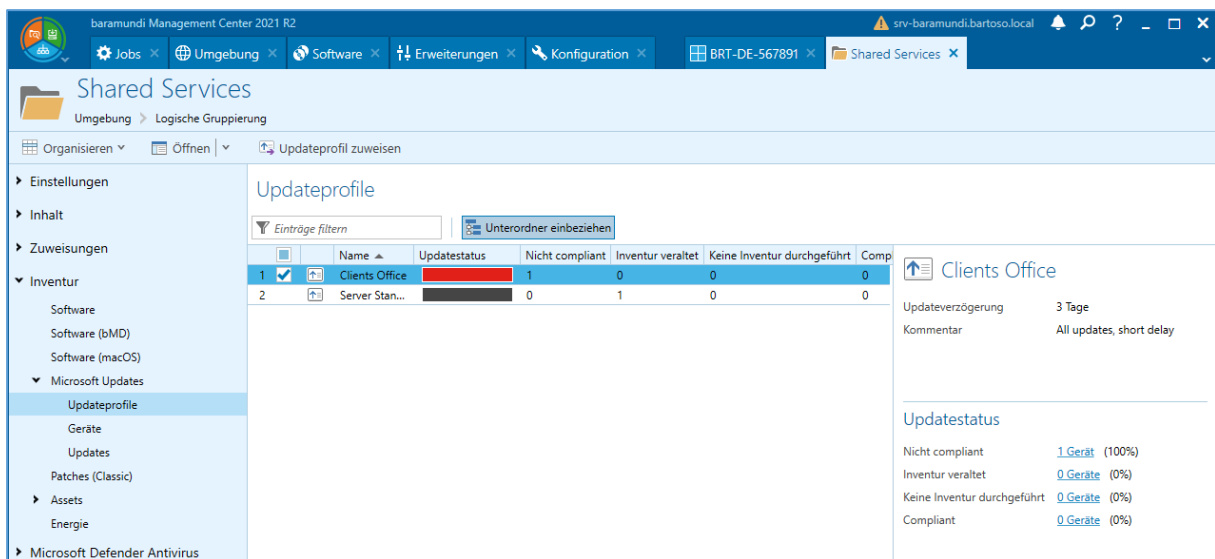


Figure 7 – Endpoint compliance with update profiles

Links in the detail view can also be used to jump directly to the list with the corresponding endpoints. All lists can of course also be exported directly for further processing or reporting purposes.

5.4.1 Detailed Overview of Update Status

Endpoint update status can be displayed according to group membership.

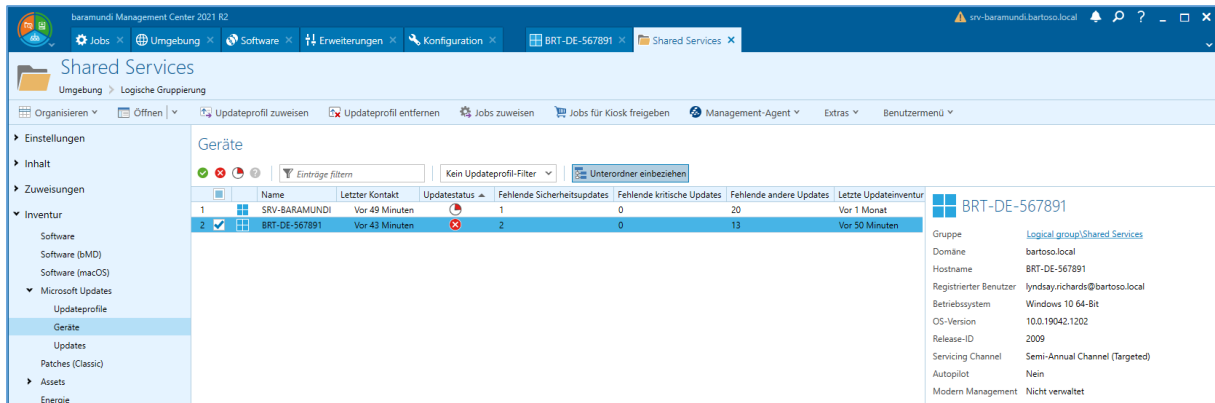


Figure 8 - Overview of the update states of the endpoints within a group

In this way, you can evaluate individual groups (e.g., departments) as well as nested subgroups or branches (e.g., locations). You can see at a glance whether the devices meet the specifications of the update profile, whether and how many updates are missing, and when the last inventory or update was performed. It is also possible to filter by update status and update profiles.

5.4.2 Detailed Overview of all Updates

The listing of all referenced updates within a group and nested subgroups is also essential.

The screenshot shows the 'Updates' section in the baramundi Management Center. The main table lists various updates with columns for 'Titel', 'Gerät Name', and 'Blockierung / Verzögerung'. The selected update is '2021-09 .NET 5.0.10 Update for x64 Client (KB5006192)'. The right-hand pane provides details for this update, including its classification, products, installation deadline, and release date.

Titel	Gerät Name	Blockierung / Verzögerung
19 Microsoft Silverlight (KB4017094)	BRT-DE-567891	
20 Microsoft Silverlight (KB4013867)	BRT-DE-567891	
21 Microsoft Silverlight (KB3193713)	BRT-DE-567891	
22 Microsoft Silverlight (KB3182373)	BRT-DE-567891	
23 Microsoft Silverlight (KB3162593)	BRT-DE-567891	
24 Microsoft Silverlight (KB3126036)	BRT-DE-567891	
25 Microsoft Silverlight (KB3106614)	BRT-DE-567891	
26 Microsoft Silverlight (KB3080333)	BRT-DE-567891	
27 Microsoft Silverlight (KB3056819)	BRT-DE-567891	
28 2021-09 .NET 5.0.10 Update for x64 Client (KB5006192)	BRT-DE-567891	Bis 23.09.2021 verzögert
29 Windows Malicious Software Removal Tool x64 - v5...	SRV-BARAMUNDI	Klassifizierung blockiert
30 Windows Malicious Software Removal Tool x64 - v5...	SRV-BARAMUNDI	Klassifizierung blockiert
31 Windows Malicious Software Removal Tool x64 - v5...	SRV-BARAMUNDI	Klassifizierung blockiert
32 Windows Malicious Software Removal Tool x64 - v5...	SRV-BARAMUNDI	Klassifizierung blockiert
33 Microsoft Silverlight (KB4481252)	SRV-BARAMUNDI	Klassifizierung blockiert
34 Microsoft Silverlight (KB4023307)	SRV-BARAMUNDI	Klassifizierung blockiert
35 Microsoft Silverlight (KB4017094)	SRV-BARAMUNDI	Klassifizierung blockiert
36 Microsoft Silverlight (KB4013867)	SRV-BARAMUNDI	Klassifizierung blockiert
37 Security Intelligence Update for Microsoft Defender...	BRT-DE-567891	
38 Windows Malicious Software Removal Tool x64 - v5...	BRT-DE-567891	
39 Update for Microsoft Defender Antivirus animalwar...	BRT-DE-567891	
40 2021-08 Update for Windows 10 Version 20H2 for x...	BRT-DE-567891	
41 2021-08 .NET Core 3.1.18 Security Update for x64 Cli...	BRT-DE-567891	
42 2021-08 Cumulative Update for .NET Framework 3.5...	BRT-DE-567891	
43 2021-08 .NET 5.0.9 Security Update for x64 Client (K...	BRT-DE-567891	

Figure 9 - Listing of all referenced updates of the endpoints within a group.

All installed, missing, delayed or blocked updates for the endpoints contained in the group are listed. You can filter the list by status, name, KB number and other properties.


We are looking forward
to meeting you!


Get in touch!





baramundi software GmbH


Forschungsallee 3
86159 Augsburg, Germany


 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com


 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

 +48 735 91 44 54
request@baramundi.com
www.baramundi.com


 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

 +43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 401
Framingham, MA 01701, USA

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com