



# **baramundi Management Suite**

2021 R2

*Empower your IT*

Dear reader,

With the support of **Windows Autopilot**, it is now possible to deliver new Windows PCs and laptops to end users directly from the manufacturer with out-of-the-box convenience and usability. The integration of Autopilot with the bMS ensures automatic, secure and seamless device configuration and enrollment. IT admins can provide positive end-user experiences while maintaining familiar bMS endpoint management options.

**Windows Update Management** is constantly evolving. In addition to functions added in previous bMS releases, new views available for device groups enable more efficient management and reporting. Device update status also can be determined at a glance and compared to its specified update profile.

IT admins gain another tool for providing quality user experiences with the new user-activated **Do Not Disturb mode**. It enables users to define time windows when they need uninterrupted use of their computers for presentations, to meet deadlines and similar situations. Execution of bMS jobs that require system or application restarts (e.g., updates and patches) or other interruptions will be deferred until the Do Not Disturb time period expires. In addition, there are numerous feature updates and enhancements to Argus Cockpit, License Management, Network Devices and other modules.

Armin Leinfelder

*Director Product Management*

## baramundi Management Suite – Version 2021 R2

---

### TABLE OF CONTENTS

<b>1</b>	<b>Release 2021 R2</b>	<b>5</b>
1.1	Windows Autopilot	5
1.2	Microsoft Update Management	6
1.3	Do Not Disturb mode	9
1.4	Additional enhancements	12
1.5	Product Improvements in Detail	23
1.6	System Requirements and Compatibility	31
1.7	Known Limitations	40
<b>2</b>	<b>Release 2021 R1U1</b>	<b>52</b>
2.1	baramundi Ticketing System	52
2.2	Microsoft Update Management	56
2.3	Management of Microsoft Defender Antivirus	58
2.4	baramundi Argus Cockpit	60
2.5	bCenter – the Pocket-bMC	63
2.6	Additional enhancements	65
2.7	Product Improvements in Detail	74
<b>3</b>	<b>Release 2020 R2 U1</b>	<b>80</b>
3.1	Product Improvements in Detail	80
<b>4</b>	<b>Release 2020 R2</b>	<b>82</b>
4.1	iOS “User Enrollment”	82
4.2	Automatic updates of apps on mobile platforms	85
4.3	Inventory of Microsoft Updates	86
4.4	Automatic BitLocker unlocking on secure networks	88
4.5	baramundi Argus Cockpit	90
4.6	Additional enhancements	95
4.7	Product Improvements in Detail	103
<b>5</b>	<b>Release 2020</b>	<b>109</b>
5.1	Android Enterprise: Dedicated Devices	109
5.2	baramundi Argus Cockpit	113
5.3	General Development	118
5.4	Product Improvements in Detail	125
<b>6</b>	<b>Release 2019 R2</b>	<b>130</b>
6.1	Android Enterprise: Work Profile	130

6.2	Windows BitLocker.....	133
6.3	General Improvements.....	136
6.4	Product Improvements in Detail .....	147
7	<b>Release 2019.....</b>	<b>152</b>
7.1	Windows 10 Configuration .....	152
7.2	Android Enterprise .....	155
7.3	Extension of the new Kiosk .....	156
7.4	E-mail Notifications .....	159
7.5	Integration with DriveLock .....	163
7.6	General Development .....	165
7.7	Product Improvements in Detail .....	171
8	<b>Appendix.....</b>	<b>176</b>
8.1	Glossary.....	176
8.2	Third Party Components.....	177
8.3	List of Figures .....	178



# 1 Release 2021 R2

## 1.1 Windows Autopilot

### 1.1.1 Out-Of-Box-Experience (OOBE)

Even before the new "normal" of remote and home office work, users appreciated the convenience of being equipped with pre-configured, ready-to-use systems. Platforms such as Apple iOS and Google Android have set the standard for out-of-the-box usability. Users simply unbox, power up and connect to wifi, then all needed settings, apps and accounts are installed and configured automatically "like magic." Microsoft's Windows Autopilot enables a similar experience for Windows devices.

### 1.1.2 Process

Users simply switch on their new Windows device and log in with their company account. The device is automatically added to the bMS and can then be managed by the admins as usual, with existing and proven jobs. For example, the device can be sent directly from the manufacturer to the new users. Commissioning by the administration in the company network is no longer necessary.

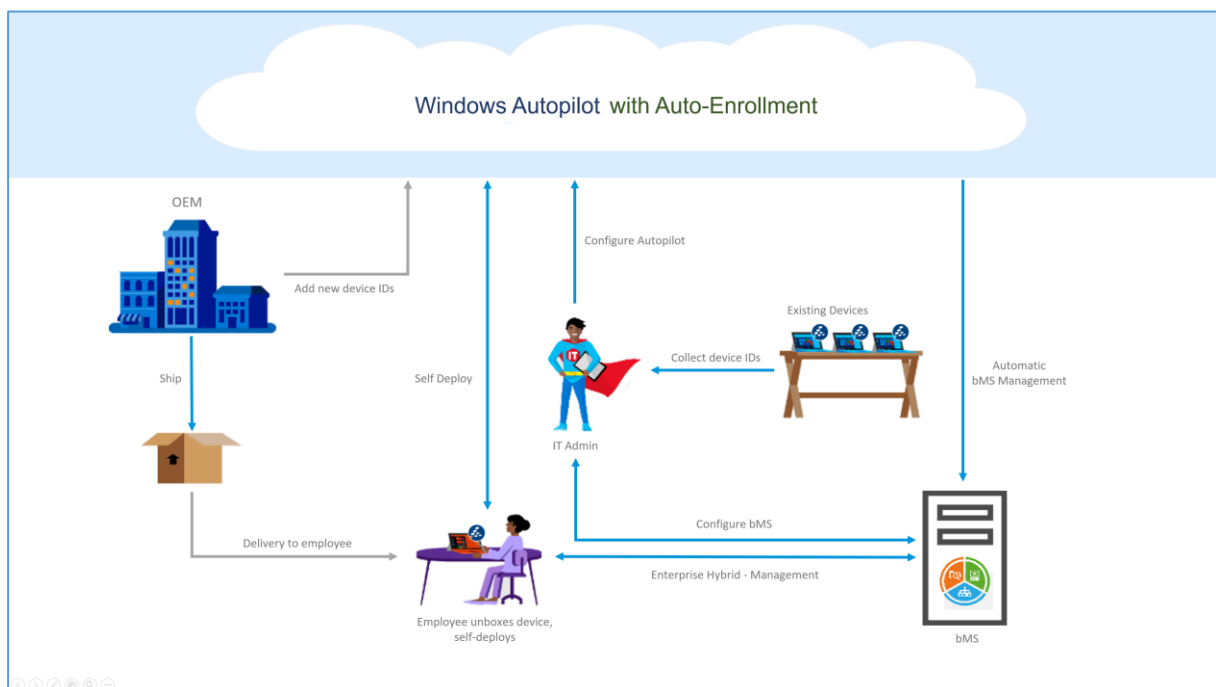


Figure 1 - Schematic illustration of the enrollment process

This saves unnecessary shipping and also makes it much easier for administrators to issue new Windows endpoints. During automatic enrollment via Autopilot, the device is created in

the bMS and supplied with the baramundi Management Agent. This is installed in IEM mode and establishes a secure connection to the bMS via the gateway. This enables management to the usual extent: inventory, software distribution, update management and much more - the existing jobs can be used directly without further adaptation.

### 1.1.3 System requirements

To be able to use Windows Autopilot, an Azure Active Directory is required. The bMS must be accessible from outside the company network via baramundi Gateway. The Autopilot functionality is only provided by Microsoft as of Windows 10. Windows Autopilot is another option to initially enroll Windows endpoints and does not require a separate baramundi license.

### 1.1.4 Autopilot with the bMS

In order to connect the bMS to the company's own Autopilot, a corresponding one-time configuration must be made in both Azure Active Directory (AAD) and bMS. Several keys are generated in the AAD, which must be transferred to the bMS.

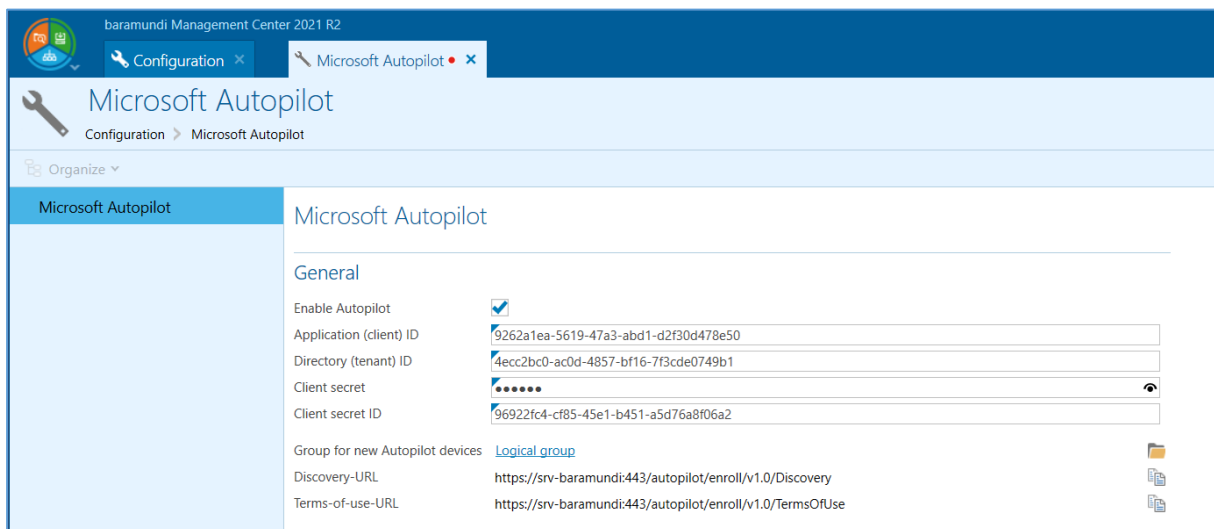


Figure 2 - Configuration of AAD keys in the bMS

After completion of the setup, all Windows 10 endpoints put into operation via Autopilot are automatically enrolled in the bMS.

## 1.2 Microsoft Update Management

### 1.2.1 The path to Modern Update Management

The comprehensive inventory of Microsoft updates enabled in the bMS 2020 R2 established the foundation for the new Microsoft Update Management. The subsequent release

introduced update profiles and staggered update rollouts. The bMS version 2021 R2 continues that development path.

## 1.2.2 Update Profiles and Compliance

Not only can update profiles be used to release/block and delay updates, they can evaluate endpoint update status. That allows you to quickly see whether an endpoint meets update profile requirements, whether all endpoints assigned to the update profile are compliant, or if action is required.

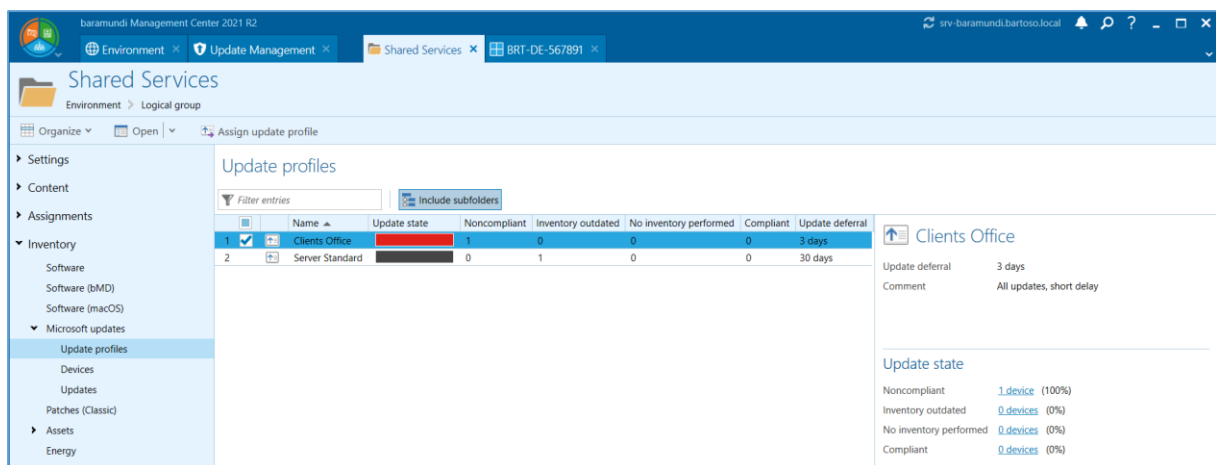


Figure 3 - Degree of fulfillment of the update profiles

Links in the detail view can also be used to jump directly to the list of the corresponding endpoints. Of course, all lists can be exported for further processing.

### 1.2.3 Detailed overview of update states

The update status of endpoints can now be displayed according to group membership. Both "Logical Groups" with optionally included subgroups, and "Universal Dynamic Groups" are supported.

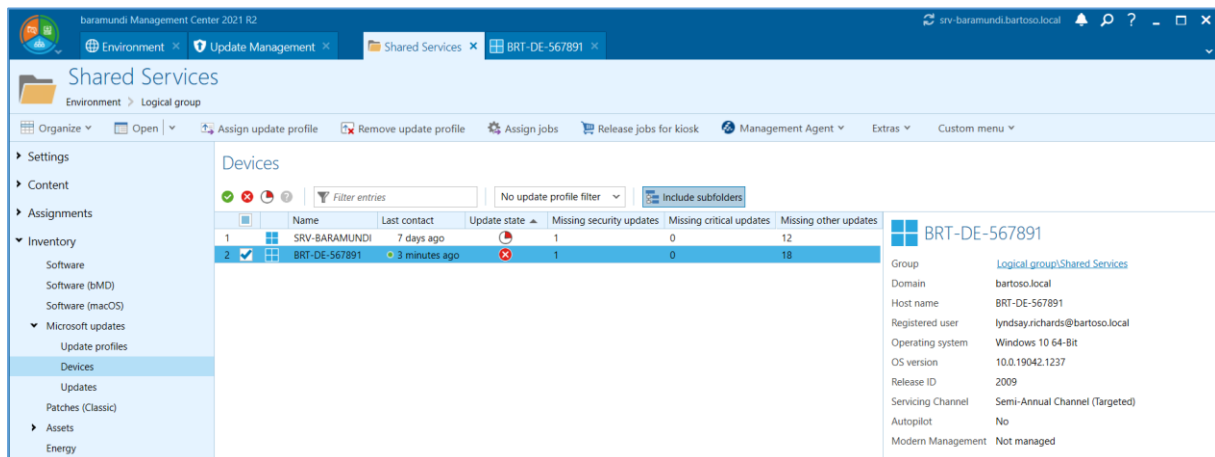


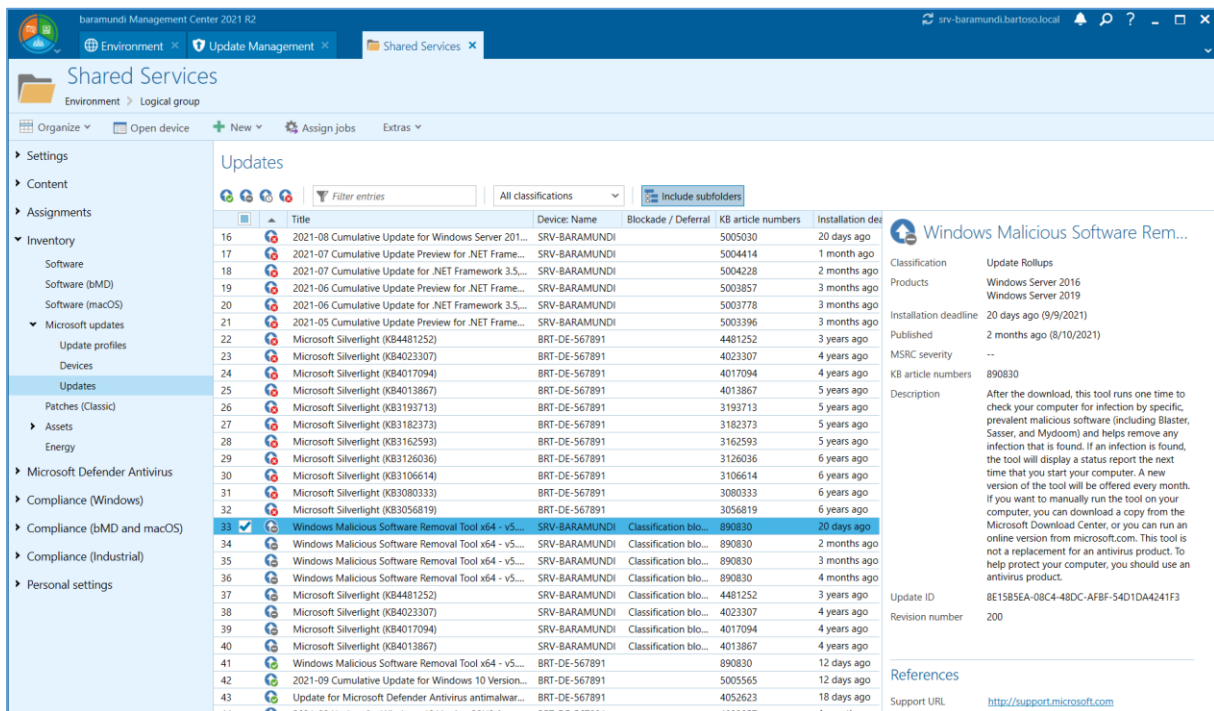
Figure 4 - Overview of the update states of the endpoints within a group

In this way, individual groups (e.g., departments) as well as nested branches (e.g., locations) can be evaluated in a targeted manner. You can see at a glance whether the devices meet the requirements of the update profile, whether and how many updates are missing, and when devices were last inventoried or updated. You can also filter by a specific status and by update profiles.

### 1.2.4 Detailed overview of all updates

Also new is the listing of all updates within a group and its subgroups. All installed and missing updates are listed, including those delayed or blocked. You can also filter by status, name, KB number and other properties.





	Title	Device Name	Blockade / Deferral	KB article numbers	Installation deadline
16	2021-08 Cumulative Update for Windows Server 201...	SRV-BARAMUNDI		5005030	20 days ago
17	2021-07 Cumulative Update Preview for .NET Frame...	SRV-BARAMUNDI		5004414	1 month ago
18	2021-07 Cumulative Update for .NET Framework 3.5...	SRV-BARAMUNDI		5004228	2 months ago
19	2021-06 Cumulative Update Preview for .NET Frame...	SRV-BARAMUNDI		5003857	3 months ago
20	2021-06 Cumulative Update for .NET Framework 3.5...	SRV-BARAMUNDI		5003778	3 months ago
21	2021-05 Cumulative Update Preview for .NET Frame...	SRV-BARAMUNDI		5003396	3 months ago
22	Microsoft Silverlight (KB4481252)	BRT-DE-567891		4481252	3 years ago
23	Microsoft Silverlight (KB4023307)	BRT-DE-567891		4023307	4 years ago
24	Microsoft Silverlight (KB4017094)	BRT-DE-567891		4017094	4 years ago
25	Microsoft Silverlight (KB4013867)	BRT-DE-567891		4013867	5 years ago
26	Microsoft Silverlight (KB3193713)	BRT-DE-567891		3193713	5 years ago
27	Microsoft Silverlight (KB3182373)	BRT-DE-567891		3182373	5 years ago
28	Microsoft Silverlight (KB3162593)	BRT-DE-567891		3162593	5 years ago
29	Microsoft Silverlight (KB3126036)	BRT-DE-567891		3126036	6 years ago
30	Microsoft Silverlight (KB3106614)	BRT-DE-567891		3106614	6 years ago
31	Microsoft Silverlight (KB3080333)	BRT-DE-567891		3080333	6 years ago
32	Microsoft Silverlight (KB3056819)	BRT-DE-567891		3056819	6 years ago
33	Windows Malicious Software Removal Tool x64 - v5...	SRV-BARAMUNDI	Classification blo...	890830	20 days ago
34	Windows Malicious Software Removal Tool x64 - v5...	SRV-BARAMUNDI	Classification blo...	890830	2 months ago
35	Windows Malicious Software Removal Tool x64 - v5...	SRV-BARAMUNDI	Classification blo...	890830	3 months ago
36	Windows Malicious Software Removal Tool x64 - v5...	SRV-BARAMUNDI	Classification blo...	890830	4 months ago
37	Microsoft Silverlight (KB4481252)	SRV-BARAMUNDI	Classification blo...	4481252	3 years ago
38	Microsoft Silverlight (KB4023307)	SRV-BARAMUNDI	Classification blo...	4023307	4 years ago
39	Microsoft Silverlight (KB4017094)	SRV-BARAMUNDI	Classification blo...	4017094	4 years ago
40	Microsoft Silverlight (KB4013867)	SRV-BARAMUNDI	Classification blo...	4013867	4 years ago
41	Windows Malicious Software Removal Tool x64 - v5...	BRT-DE-567891		890830	12 days ago
42	2021-09 Cumulative Update for Windows 10 Version...	BRT-DE-567891		5005565	12 days ago
43	Update for Microsoft Defender Antivirus animalwar...	BRT-DE-567891		4052623	18 days ago
44	2021-08 Update for Windows 10 Version 20H2 for v...	BRT-DE-567891		4023057	1 month ago

**Windows Malicious Software Rem...**  
Classification: Update Rollups  
Products: Windows Server 2016, Windows Server 2019  
Installation deadline: 20 days ago (9/9/2021)  
Published: 2 months ago (8/10/2021)  
MSRC severity: --  
KB article numbers: 890830  
Description: After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.  
Update ID: 8E15B5EA-08C4-48DC-AFBF-54D1DA4241F3  
Revision number: 200  
References: <http://support.microsoft.com>

Figure 5 - List of all updates of an endpoint group.

## 1.3 Do Not Disturb mode

### 1.3.1 The End User Experience

Due to the ubiquitous use of mobile devices and the pandemic-related shift to remote and home office work, users have high expectations for the devices they rely on for work and personal use. They want devices to simply work without restriction or interruption, and they want a say in device settings and installed software.

For IT admins, this complicates implementation of company guidelines even for simple installations. Ideally, admins enforce policies and update software without disturbing users. However, it's typically impossible to predict the best time to manage remote devices unless you actively involve users.

### 1.3.2 Do Not Disturb mode in the bMS

The bMS has always allowed IT admins to coordinate with users when distributing a job and to display specific job-related notifications via the Tray Notifier. When the job is ready to start, users receive a pop-up message with the option to specify another start time. But this poses a problem for some users who find job notifications intrusive or annoying even with the option to select a better time.

With the bMS 2021 R2, administrators can now activate and configure the Do Not Disturb mode within an updated bMA configuration page.

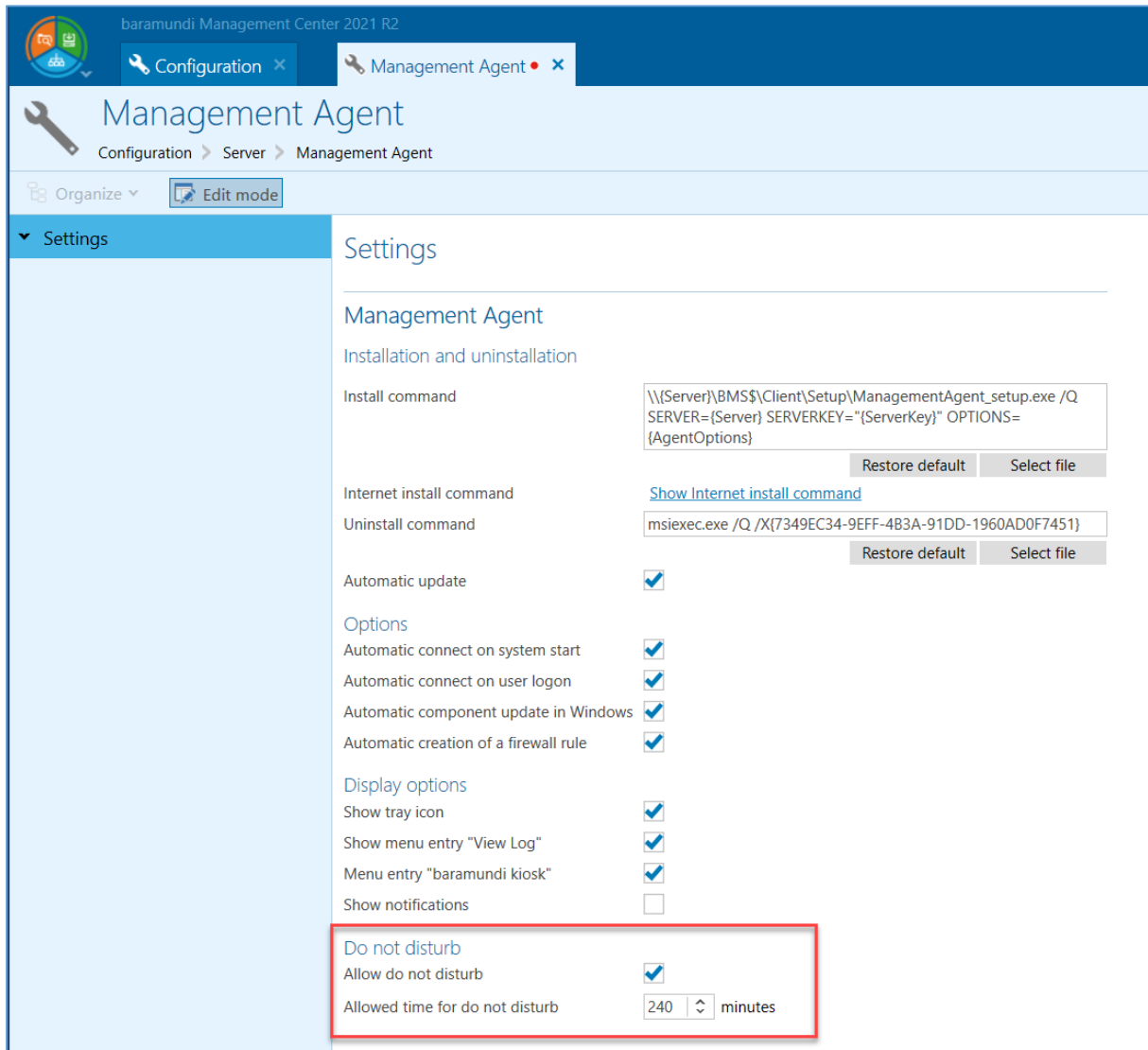
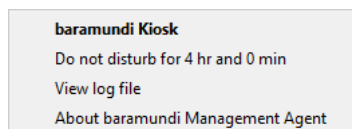


Figure 6 - bMA configuration page with options for "Do Not Disturb" mode

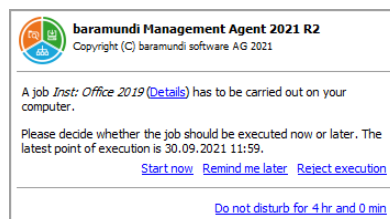
### 1.3.3 The User View

Users can specify a time period when they want to activate (and later deactivate) "Do Not Disturb" mode for their own Windows device in the Tray Notifier message itself or via the context menu of the bMA. This is useful, for example, before starting a presentation, a meeting or at other times when they do not want to be interrupted by job-related messages from IT.

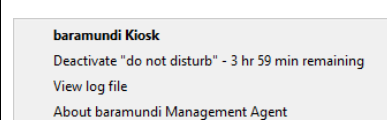
Activate "Do Not Disturb"  
via the bMA context menu



Activate "Do Not Disturb"  
via the Tray Notifier



Deactivate "Do Not Disturb"  
via the bMA context menu



### 1.3.4 The Administrator View

Admins can view endpoint "Do Not Disturb" status in baramundi Management Center. List views can be sorted by the new column, "Do Not Disturb mode ends"

Content

Overview


Assignments


Software


Software (bMD)


Update profiles


Compliance (Wind
















 Filter entries

 Include subfolders









	<div><div></div><div></div></div> Name ▲	Last contact	Operating system	Do not disturb	Do not disturb end
1	<div></div> Deactivated				
2	<div></div> ACER03	1 month ago	Windows 10 64-bit	Inactive	
3	<div></div> ASPIRE03	1 month ago	Windows 10 64-bit	Inactive	
4	<div><div></div><div></div></div> DEMOCLIENT-01	<div><div></div>1 minute ago</div>	Windows 10 64-bit	Active	In 56 minutes

Figure 7 - List view with the new columns for "Do Not Disturb" Mode

These values can also be used as a condition for defining Universal Dynamic Groups (UDG).

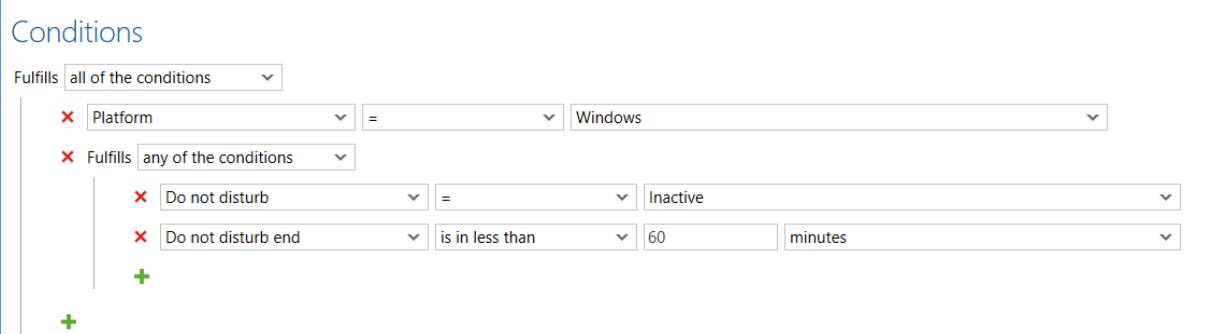


Figure 8 - Do Not Disturb mode as a condition for a UDG

### 1.3.5 APIs

The "Do Not Disturb" mode can also be controlled via the bMA Command Line Interface (the bMACmd). For this purpose, the bMACmd.exe has been extended with commands for setting and showing the "Do Not Disturb" mode. bConnect can also be used to read out whether the "Do Not Disturb" mode has been activated at the endpoint and how long it will remain active.

## 1.4 Additional enhancements

### 1.4.1 baramundi Argus Cockpit (bAC)

The range of capabilities in the bAC is growing continuously, making work easier and more efficient for IT admins and other IT stakeholders such as CISOs. What's more, new bAC features can be used without requiring a version update of the bMS, meaning that the enhancements described below are already available to current bAC users. <sup>1</sup>

#### 1.4.1.1 (Historical) Export UDG result sets to Excel

With the help of the new Excel export functionality, IT admins can now share relevant IT information with other company personnel such as IT managers or CISOs. These reports can be customized to meet regular and ad hoc reporting needs, to document compliance status, review software licensing data, and other use cases.

For example, UDG result sets showing "All end devices with pending critical updates" or "End devices without BitLocker encryption" can be exported for increased transparency.

<sup>1</sup> <https://www.baramundi.com/en-us/management-suite/module/argus-cockpit/updates/>




Historical results can be compared to current data to determine trends, assess performance and set operational objectives.

**NRD-BMS #1**

encryption possible

on 05/26/2021



Endpoint name	Endpoint type	Operating system	OS version	Last contact (UTC)
Acert02	Windows	Windows 10 64-Bit	10.0.16299.2166	26.05.2021 09:12
Acert03/Net-02010	Windows	Windows Server 2016	10.0.14393.0	21.10.2019 17:28
Acert03/Net-04-01-01	Windows	Windows 10 64-Bit	10.0.10586.0	21.10.2019 16:27
Acert03/Net-04-01-02	Windows	Windows 10 64-Bit	10.0.18362.30	21.10.2019 16:31
Acert03/Net-04-01-03	Windows	Windows Server 2019	10.0.17763.1577	25.05.2021 20:33
Acert03/Net-04-01-04	Windows	Windows 10 64-Bit	10.0.10586.0	08.11.2019 10:55
Acert03/Net-04-01-05	Windows	Windows 10 64-Bit	10.0.18363.418	19.03.2021 03:25
Acert03/Net-04-01-06	Windows	Windows 10 64-Bit	10.0.18363.592	27.01.2020 16:10
Acert03/Net-04-01-07	Windows	Windows Server 2016	10.0.14393.3242	11.10.2019 16:25

Figure 9 - Exported data with defined criteria

#### 1.4.1.2 Share relevant data in comprehensive reports

The new reporting interface in the baramundi Argus Cockpit enables you to display, analyze and plot bAC data in analytics applications (e.g., MS Power BI, MS Excel) and deliver comprehensive and customized reports. IT admins can fulfill a range of reporting objectives by searching for data related to:

- bMS environment,
- Time period
- Universal Dynamic Group (UDG)
- Topic (e.g., Security)

and many other parameters. Searches can also include or exclude data based on conditions you can define as needed. For example, IT admins can generate reports for the CISO, or MSPs can create client reports, documenting the current and historical IT system status for audits, certifications, or SLAs.



Figure 10 - Example of a Power BI Report

We make it easy for IT admins to get started by providing a standard reporting template for MS Power BI Desktop. You can also design and use your own templates. The bAC Reporting Template <sup>2</sup> Marketplace also enables you to share templates that you create, or use templates created by other baramundi customers.

#### 1.4.1.3 Comparison of two points in time in UDG result sets

With the help of the Universal Dynamic Groups (UDG), important results sets can be displayed the bAC and in Argus Trends to visualize trends and changes over time. However, IT admins may want to know, for example, not just how many endpoints were added or removed over a specific period of time, but also the details of those devices to understand why, when and how those changes occurred. You can do that easily in the new "delta view" by selecting any two points in time.

<sup>2</sup> <https://forum.baramundi.de/index.php?threads/marktplatz-f%C3%BCr-bac-reporting-templates.11864/>

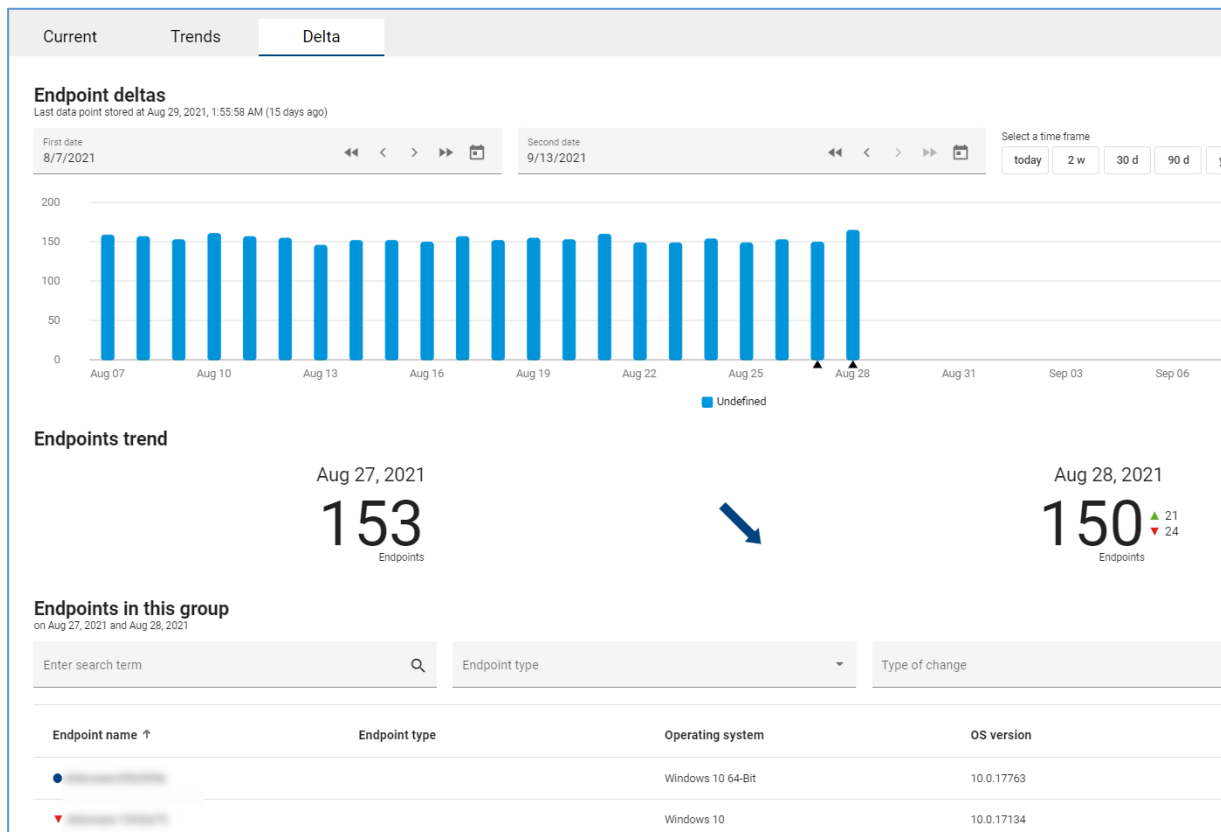


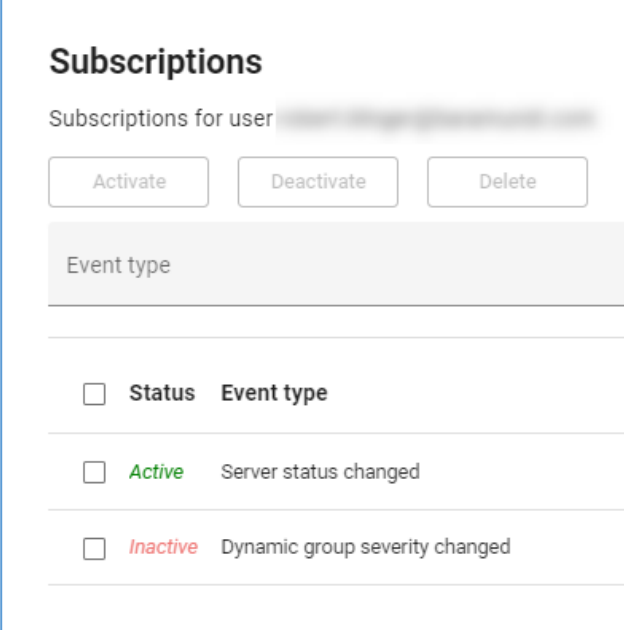
Figure 11 - Comparison of two points in time for UDG result sets

#### 1.4.1.4 Email notifications of important changes

Argus Cockpit makes it easy to see IT status metrics at any time. However, IT admins do not constantly watch the bAC display to monitor UDGs results to see if action is required. Now, bAC lets IT admins set up proactive notifications for status changes, especially when "normal" or expected values approach or reach pre-defined thresholds or critical states.

bAC e-mail notifications can be defined for:

- Status changes of bMS services, and
- Reaching defined UDG threshold values.



**Subscriptions**

Subscriptions for user XXXXXXXXXXXX@XXXXXX.XXX

Event type

<input type="checkbox"/>	Status	Event type
<input type="checkbox"/>	Active	Server status changed
<input type="checkbox"/>	Inactive	Dynamic group severity changed

Figure 12 - List of selected notifications



## 1.4.2 Automation Studio - Embedded Script Return Value

The baramundi Automation Studio has long supported the use embedded scripts such as VBScript, JScript or, PowerShell. PowerShell is frequently used, and users wanted the ability to incorporate results from PowerShell scripts within Automation Studio scripts. You can do this now in bMS 2021 R2 by defining PowerShell results codes as Automation Studio variables.

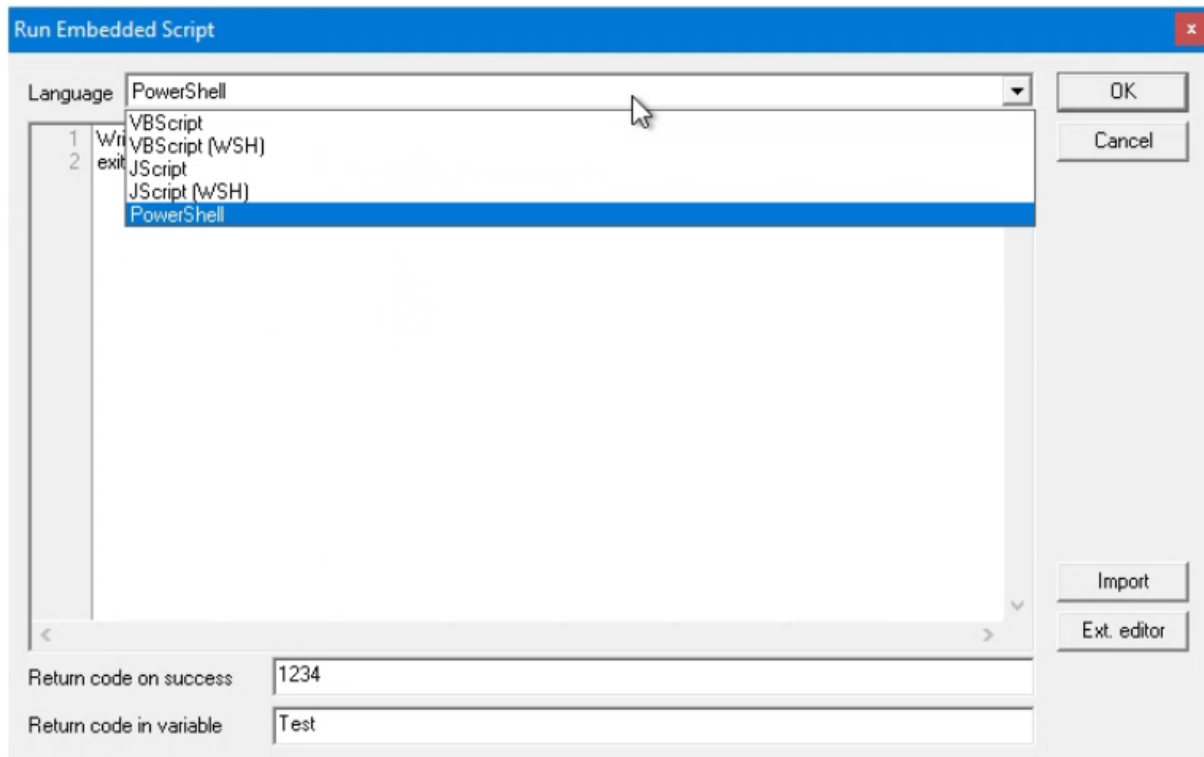


Figure 13 - Return an embedded script value as an Automation Studio variable

### 1.4.3 baramundi License Management – Email Notification

You can now configure and receive timely email notifications when software license agreements are nearing expiration or renewal dates. This provides a better overview of software license status and better options for managing costs, renewal options or changes in packages or vendors. You can define different events with configurable check intervals to simplify and improve planning and budgeting.

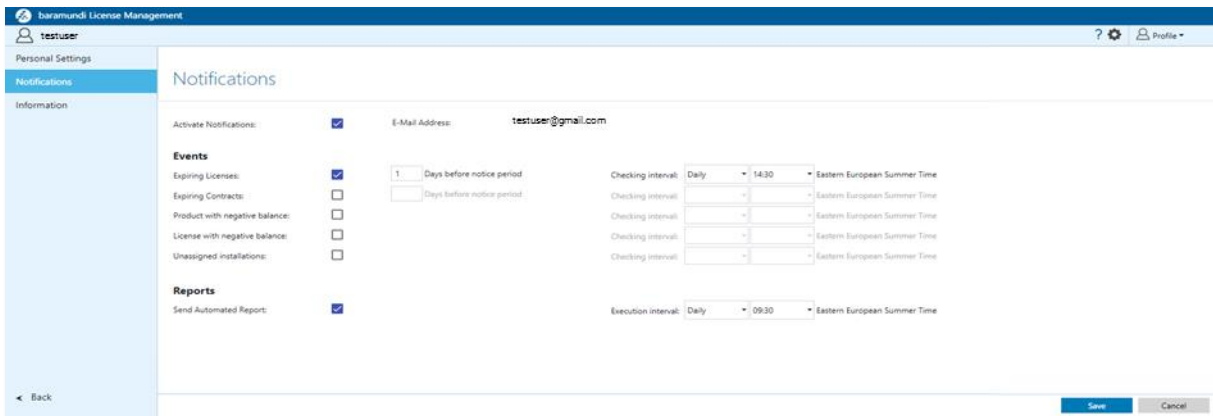


Figure 14 - bLM configuration for email notifications

Note: The new functionality will be made available through MSW. Watch for more information about this in the baramundi Forum.

## 1.4.4 baramundi Network Devices

### 1.4.4.1 Advanced scanning methods

In addition to capturing the details of network devices via SNMP, we now give you the option to see and inventory network endpoints via Address Resolution Protocol (ARP).

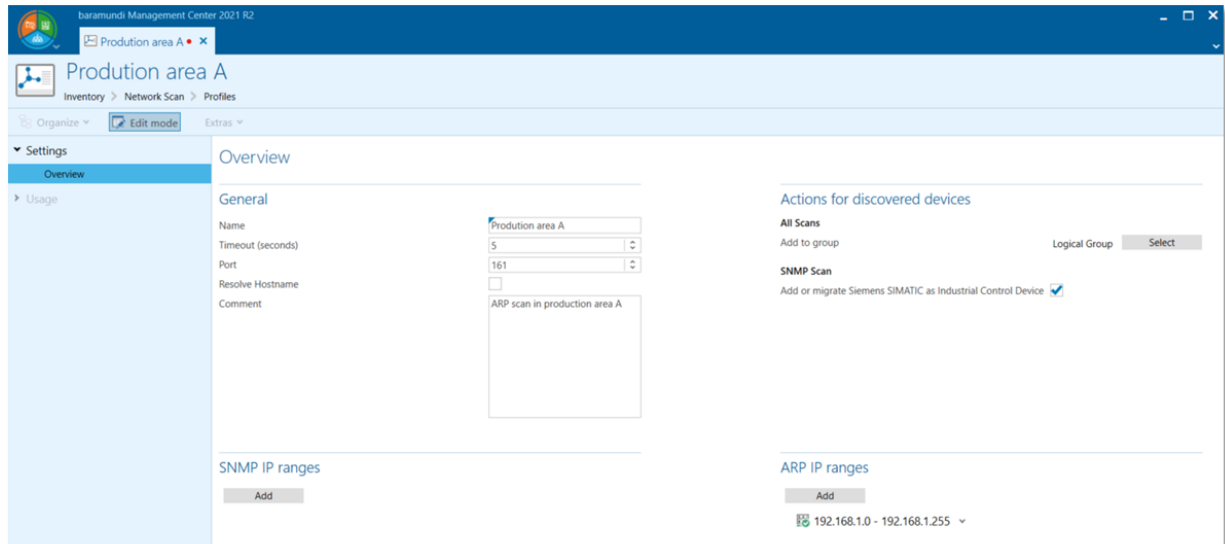


Figure 15 - Advanced scanning using ARP IP range

ARP scanning captures both the IP and MAC addresses and the host name if available. This allows you to increase the number of devices detected and improve network transparency and visibility. Information obtained is available in various group views.

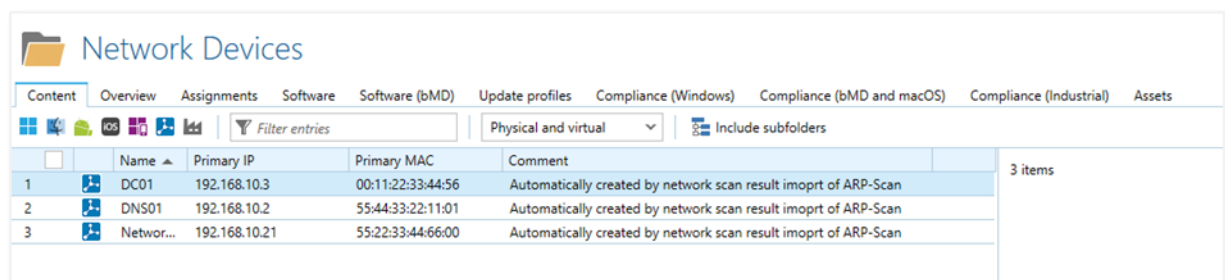
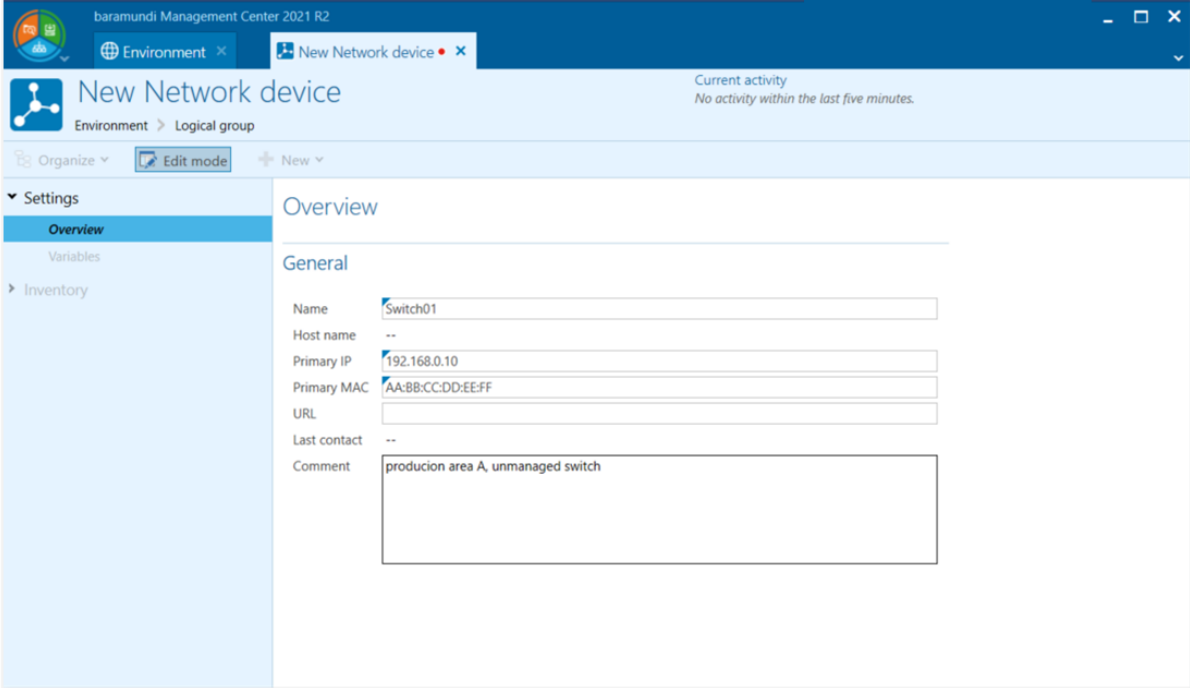


Figure 16 - Logical Group - network devices captured via ARP

### 1.4.4.2 Manual creation of network devices

If network devices are in an unreachable segment, temporarily offline or cannot be accessed for any reason, the bMS 2021 R2 lets you maintain IT visibility by manually creating a network endpoint.



The screenshot shows the 'baramundi Management Center 2021 R2' interface. The top navigation bar includes 'Environment' and 'New Network device'. The main header area displays 'New Network device' and 'Environment > Logical group'. Below this is a toolbar with 'Organize', 'Edit mode', and 'New' buttons. A left sidebar contains 'Settings' (with 'Overview' selected), 'Variables', and 'Inventory'. The main content area is titled 'Overview' and 'General', featuring a form with the following fields:

Name	Switch01
Host name	--
Primary IP	192.168.0.10
Primary MAC	AA:BB:CC:DD:EE:FF
URL	
Last contact	--
Comment	production area A, unmanaged switch

Figure 17 - Manually creating network devices

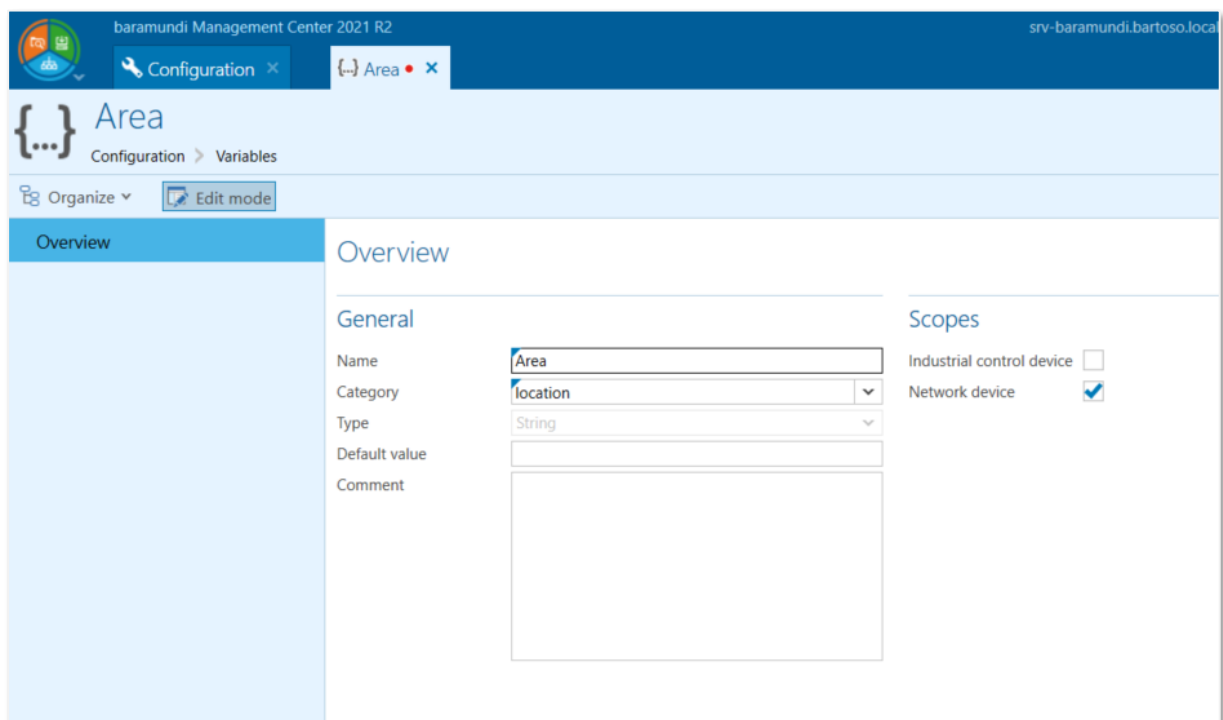
In addition to reading and deleting network devices, you can also create or update manual entries via the bConnect interface.



### 1.4.4.3 User-defined variables on network devices

In addition to the device data captured via SNMP and ARP, you can add and update other customized data for network device endpoints.

For example, you can define variables such as cost center, room number, building or date of purchase, and show devices matching specified values in group list views.



baramundi Management Center 2021 R2

Configuration × Area ×

Area

Configuration > Variables

Organize Edit mode

Overview

Overview

General

Name: Area

Category: location

Type: String

Default value:

Comment:

Scopes

Industrial control device ☐

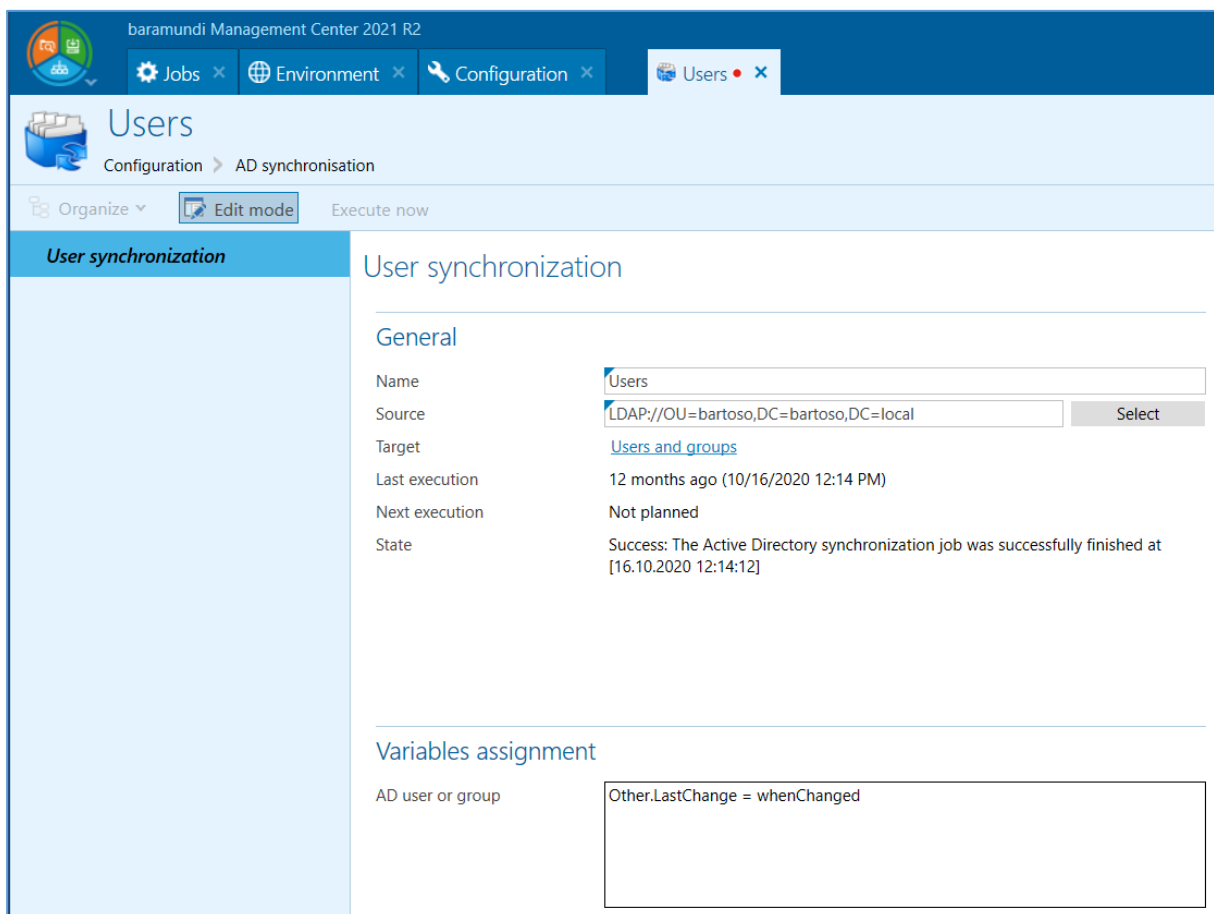
Network device ☒

Figure 18 - Variable definition with assignment to multiple areas

## 1.4.5 Active Directory Synchronization

As the basis for essential functions in the baramundi Management Suite, AD-Sync is a convenient way to synchronize computer and user objects. In 2021 R1 earlier this year we revised the administration dialog, optimized the performance and added synchronization options. In 2021 R2, we're extending the functionality of machine synchronization to user synchronization, enabling AD properties in baramundi variables to be flexibly synchronized to users and groups.

In addition to the generic fields such as first and last name, AD properties can include address data or the distinguishedName.



The screenshot shows the 'baramundi Management Center 2021 R2' interface. The top navigation bar includes 'Jobs', 'Environment', 'Configuration', and 'Users'. The 'Users' section is active, showing 'Configuration > AD synchronisation'. The left sidebar has 'User synchronization' selected. The main content area is titled 'User synchronization' and contains two sections: 'General' and 'Variables assignment'.

**General**

Name	Users
Source	LDAP://OU=bartoso,DC=bartoso,DC=local <span>Select</span>
Target	<a href="#">Users and groups</a>
Last execution	12 months ago (10/16/2020 12:14 PM)
Next execution	Not planned
State	Success: The Active Directory synchronization job was successfully finished at [16.10.2020 12:14:12]

**Variables assignment**

AD user or group	Other.LastChange = whenChanged
------------------	--------------------------------

Figure 19 - User Synchronization with Variable Mapping

User or group object data is displayed in the baramundi Management Center. For mobile devices (iOS and Android) where the syntax {RegisteredUser.VariableName} is already known, the other synced fields can also be accessed. This is done with the new syntax for your own variables {RegisteredUser.Category.Name}.

Registered user and group variables cannot be used on Windows devices and associated bMS jobs.

## 1.5 Product Improvements in Detail

### 1.5.1 Windows Agent (bMA)

- Local administration rights are required to access the `bMA.log` file. If the action `Open log file` is used with the bMA icon, a UAC query appears. Please also note the remarks under Q

- Notes on modification Access bMA.log
- `Do not disturb` mode allows the user of the terminal device to prevent a job execution.
- If a `User Defined Variable` of type `Date` is set via `bMACmd`, the value is written in the correct date format. If a conversion of the date is not possible, an empty value is written.
- If the `Open log file` action is used on the bMA icon, a UAC prompt appears. The bMA.log file can only be opened by users with local administration rights.
- The functionality to automatically update the Windows Update API in the context of `Manage Microsoft Update` jobs has been removed because it is no longer necessary from Windows 7. The `bwumgr` parameter `/SkipUpdateCheck` is obsolete and ignored.
- Bugfix: The shutdown after a `WakeOnLan` job may not work correctly because the wakeup time is determined incorrectly.
- Bugfix: Sporadically the message "Local install user ['baralnstLocal'] group membership could not be retrieved, no group membership removed!" is logged in the bMA.log, although there is no misbehavior.

### 1.5.2 Management Center (bMC)

- A new baramundi licensing enables more convenient licensing of the baramundi Management Suite modules.
- The `Boot time` field is available in `Dynamic groups (Universal)` and references the last boot time of Windows devices.
- The configuration of the baramundi Management Agent for Windows (bMA) is now under `Configuration - Server - Management Agent` and contains new setting options for `Do not disturb`.
- Permissions for `Jobs - Folder` and `Environment - Users and groups` are now configured in a modern dialog.
- If download jobs fail, a bMC message is displayed.

- Numerous improvements in Windows Update Management. New views on groups, static groups and universal groups (Windows). The update status uses the configured delay time of the update profile and displays the delay time as "Installation Deadline".
- Bugfix: If multiple Windows clients are selected under `Environment` to change the mode of the bMA, an error message is not always displayed if the permissions for individual clients are not sufficient.
- Bugfix: If the bMS is operated on a virtual server system, a license violation due to hardware replacement is detected under different circumstances.
- Bugfix: bMUM inventory jobs sometimes cause a large TempDB.
- Bugfix: If an already existing application is re-imported via bDX import, existing `Installed on` entries are removed.
- Bugfix: At the client compliance overview, `Vulnerabilities found` are counted incorrectly if partial exceptions are set.
- Bugfix: In some job steps for patch (classic) and driver installations, additional GUIDs are displayed.
- Bugfix: In rare cases the bMC crashes when the `job details` view was opened for a large number of job instances.
- Bugfix: Dynamic Group (Windows) does not show a result if the manually created SQL statement returns machines multiple times.

### 1.5.3 OS-Install

- Firewall disabling has been removed from the `unattend.xml` files. Additionally, the port shares required for communication have been added. Thus, after OS installation, the Windows firewall remains active, but the communication between the server and the agent is still guaranteed.
- Disabling of AntiSpyware has been removed from the `unattend.xml` files.
- The partitioning of GPT-initialized hard disks with Windows recovery partition was adapted for the Windows PE of the "*Microsoft ADK for Windows 11*".

- To enable the installation of Windows 11 with the `InstallToAvailablePartition` configuration, the `osinstall_presetup_win11.bds` is now executed, which removes the drive letter of the Windows partition.
- Bugfix: The `update profile` stored on the Windows device is removed by an OS install job.

### 1.5.4 Mobile Devices

- Profiles that are neither linked to a job step nor inventorized on a device are automatically purged on a daily basis.
- The iOS Exchange module has been extended to include `OAuth`.
- The settings of the security modules have been rearranged.
- Bugfix: iOS profiles with the `Block safari cookie setting` `Allow from websites I visit` cannot be distributed.
- Bugfix: An Android Enterprise device cannot be created if read permissions to the Android Enterprise configuration are missing.

### 1.5.5 Mobile Devices Android 12 and up

- On fully managed devices, only WiFi networks installed via the bMS are displayed in the inventory. Private networks are no longer visible.
- The baramundi agent does not require access to the permissions for capturing the location.
- New password quality levels are configurable.
- In the "Work profile" enrollment mode, the hardware inventory does not read data for IMEI and serial number.

### 1.5.6 bServer

- Download jobs run into a timeout error if the download was not possible for more than 4h. A BMC message is displayed in these cases.
- If the BitLocker network unlock is not configured on a PXE relay, it behaves there as configured for the main server. On the PXE relay the network unlock is activated by default and not deactivated.
- Job instances are no longer set to error if a job step cannot be loaded. This improves error handling for repeated jobs that ran into a job timeout error.
- An error without further information is now set to "Unspecified Error" for job instances.
- Job instances with unknown error status are now set to `Unspecified Error` instead of `Operation successful`.
- Bugfix: If the bServer is operated in a virtual environment, the hardware binding of the licensing can cause that a new license is needed.
- Bugfix: `Inventory Microsoft updates` job steps may cause a large TempDB.
- Bugfix: An incorrectly entered gateway hostname leads to the bServer service not starting any more in rare cases.

### 1.5.7 bServer – AD synchronization

- The setting `"Only sync enabled devices"` for machine sync jobs is automatically set during the database update. If migrating from a bMS 2021R1, the jobs are not changed.
- Attribute names in AD machine sync are no longer case sensitive.
- User AD synchronization supports synchronization of AD properties in variables that can be used in MDM profiles, MDM jobs or MDM email templates.
- Bugfix: Device Sync does not recognize Windows 11 clients as Windows devices and moves them to the recycle bin depending on the configuration.
- Bugfix: Kiosk assignments to users may be lost by a user sync.



- Bugfix: Under certain circumstances many warning messages of the type "unable to determine if Baramundi.Bms.Common.Entities.AdGroupMappingLight" are written to the log file.
- Bugfix: When synchronizing AD attributes, errors of the form `Active Directory attribute [] could not be parsed` occur although the job is configured correctly.
- Bugfix: When configuring the interval, an incorrect validation occurs on English systems.
- Bugfix: The configuration of SingleLevelDomains or domains with 1-n DC tags is rejected as invalid. The input cannot be saved.
- Bugfix: Existing `dynamically loaded users` are not updated correctly by AD synchronization.
- Bugfix: Saving an AD Sync job for machines takes unexpectedly long time if the `Delete` option is set.
- Bugfix: If a user automatically created by the AD User Sync under `dynamically re-loaded users` is deleted in AD and recreated there, the AD Sync aborts.
- Bugfix: The AD user sync terminates if two users with identical AD paths exist in the baramundi database. (The sync still terminates, but with a meaningful error message).
- Bugfix: The LDAP path of a single layer domain cannot be configured via the bMC because the GUI recognizes the path as invalid.
- Bugfix: Spaces at the beginning or end of the source path of an ad synchronization job lead to incorrect job execution.

### 1.5.8 Automation Studio (bDS)

- New online and offline help.
- Bugfix: Adding/deleting users to/from local groups is not possible when using an alternative UPN suffix.

### 1.5.9 Argus-Connect

- The handling of sporadic connection errors has been improved.
- Bugfix: The status message `Cloud connection is established` is sometimes displayed even though the connection was established correctly.
- Bugfix: In rare cases the transmitted terminal device list contains duplicates.

### 1.5.10 bConnect

- bMUM update profiles can be assigned to endpoint devices. The assignment of an update profile to an endpoint is also possible via the ID of an update profile.
- The ID of an assigned update profile (property named "GuidMicrosoftUpdate-Profile") can be retrieved via GET request (EndpointController).
- On network devices the CRUD operations can be performed.
- On IP networks the CRUD operations can be executed.
- Global bMUM settings for inventory validity period and tolerance time of missing updates can be read and written.
- Bugfix: When creating Windows jobs, the option "UserConsentRequired" is not handled correctly.

### 1.5.11 Defense Control

- In the bMC, a custom BitLocker Network Unlock certificate can be imported under `Defense Control - Settings`.

### 1.5.12 MAC OS

- Improved error messages in case of problems during SSH enrollment.
- BugFix: An MDM license is required for native Mac enrollment.

### 1.5.13 Network Scanner

- A scan via the Address Resolution Protocol (ARP) is possible.

## 1.6 System Requirements and Compatibility

### 1.6.1 baramundi Management Server and baramundi PXE Relay

- Supported platforms: see 1.6.17 (bMS column)
- .NET 4.7.2, as well as .NET Core Runtime 3.1. x64 is required.
- Supported languages German and English.
- It is recommended to use a dedicated server for the baramundi Management Server.
- Certain ports must be available for the baramundi Management Server. <sup>3</sup>
- Integration into a Windows domain - Windows Active Directory is recommended.
- Server/Network Hardware Requirements:
  - Available RAM: at least 8 GB; recommended 16 GB
  - Processor: at least 2 cores
  - Storage space for installing the bMS: at least 5 GB
  - Network card: at least 1 Gigabit

### 1.6.2 Database connection

- Supported platforms:
  - SQL Server 2019
  - SQL Server 2017
  - SQL Server 2016 SP3
  - SQL Server 2014 SP3
  - Oracle 19c
  - Oracle 12c R2 (will no longer be supported as of 2022 R1)
- At least 10 GB of hard disk space for the baramundi database.
- The baramundi Management Server is a database-oriented system, so it is important to ensure sufficient database performance and a high-performance connection.
- For testing purposes and environments with less than 250 endpoints, SQL Express Edition can be used ([Microsoft Download](#)).
- Operation of the database server and the baramundi management server on one system is permitted. For higher requirements and larger environments, a stand-alone database server is recommended.

---

<sup>3</sup> A list of ports used on the server is available in the appendix of the manual.

### 1.6.3 baramundi Management Center

- Supported platforms for the baramundi Management Center, as well as the add-ons Automation Studio, License Management, Remote Control and ImageMount: see 1.6.17 (column bMC).
- .NET 4.7.2 is assumed.
- Screen resolution:
  - Minimum screen resolution of 1024 x 768 pixels.
  - Resolution of 1280 x 800 pixels or higher is recommended.
  - All resolutions refer to a font size display of 100%.

### 1.6.4 baramundi OS-Customization Tool

- This baramundi Management Center add-on provided via Managed Software for customizing Windows 10 images is supported on the platforms visible in MSW
- .NET 4.7.2 is assumed.
- To customize the Windows images (Windows 10 and Windows 11), the "[Microsoft ADK for Windows 11](#)" is required to create Windows PE boot images (Windows 10 and Windows 11). The ADK is available in Managed Software under `Microsoft Windows ADK - ADK10 - 2111` and `Microsoft Windows ADKWinPE - ADK10 - 2111`.

### 1.6.5 baramundi DIP

- Supported platforms: see 1.6.17 (column bDIP).
- .NET 4.7.2 is assumed.
- Additional hard disk space is recommended:
  - 10 GB for applications
  - 90 GB for Managed Software (MSW)
  - 6 GB for each operating system to be distributed with the baramundi OS-Install module
  - 400 GB for patch data if offline patch management is to be used.

### 1.6.6 baramundi Gateway

- Supported Platforms: see 1.6.17 (column bGW)
- .NET 4.7.2 is assumed.

- It is recommended that the baramundi Gateway not be operated with other services on the same system.
- Integration into an Active Directory is not necessary.

#### Server/Network Hardware Requirements:

- Available RAM: at least 4 GB; recommended 8 GB
- Storage space for installing the bMS: at least 1 GB
- Network card: at least 1 Gigabit

### 1.6.7 baramundi Management Agent (Windows)

- Supported Platforms: see 6.1.5 (column bMA)

### 1.6.8 baramundi OS-Install

- The "[Microsoft ADK for Windows 11](#)" is required to create Windows PE boot images (Windows 10 and Windows 11). The ADK is available in Managed Software under Microsoft Windows ADK - ADK10 - 2111 and Microsoft Windows ADKWinPE - ADK10 - 2111.

### 1.6.9 baramundi License Management

- Storing license documents in the database can increase storage requirements on the database server.
- The MS-SQL Express database server is limited by Microsoft to 10 GB database size, so it is not recommended to use it for baramundi License Management.
- baramundi License Management supports current versions of the following browsers:
  - Microsoft Edge
  - Google Chrome
  - Mozilla Firefox

### 1.6.10 Network Scanner

- The Network Scanner is an add-on to the Windows bMA. It is available to all customers via Managed software.
- .NET 4.7.2 is assumed.
- Supported platforms: see 6.1.5 (column bScan)

### **1.6.11 baramundi Kiosk**

- Supported platforms: see 6.1.5 (column bMA)
- Windows Active Directory including configured baramundi AD Sync is required for user logon and job assignment on a per-user basis.
- baramundi Kiosk supports current versions of the following browsers:
  - Microsoft Edge
  - Google Chrome
  - Mozilla Firefox

### **1.6.12 baramundi Management for iOS**

- Supported platforms:
  - iOS Version 15
  - iOS Version 14
  - iOS Version 13
  - iOS Version 12
  - iOS Version 11
  - iOS Version 10
  - iOS Version 9

### **1.6.13 baramundi Management for Android**

- Supported platforms:
  - Android Enterprise 12
  - Android Enterprise 11
  - Android Enterprise 10
  - Android Enterprise 9
  - Android Enterprise 8
  - Android Enterprise 7
  - Android Version 4.0.4. to Version 9 with Legacy Agent
  - Samsung KNOX on Android version 4.0.4 to version 9 with Legacy Agent

### **1.6.14 baramundi Management for macOS**

- Supported platforms:
  - macOS 10.16 (Monterey)
  - macOS 10.15 (Catalina)
  - macOS 10.14 (Mojave)
  - macOS 10.13 (High Sierra)



- macOS 10.12 (Sierra)
- Mac OS X 10.11 (El Capitan)
- Mac OS X 10.10 (Yosemite)
- Mac OS X 10.9 (Mavericks) (64 Bit)
- Mac OS X 10.8 (Mountain Lion) (64 Bit)
- Mac OS X 10.7 (Lion) (64 Bit)

### 1.6.15 baramundi Virtual

- Supported platforms:
  - VMware vSphere vCenter 6.0, 6.5
  - VMware vSphere Hypervisor 6.0, 6.5
- Note: bVirtual is not compatible with VMware vSphere v6.5 Update 1 or later.
- The following components are required on the baramundi server:
  - PowerShell version 4 or 5 or 5.1
  - VMware PowerCLI 6.5 Release 1

### 1.6.16 baramundi APIs

- bConnect is available in version 1.1.
- Deprecated - The bMOL (baramundi Management Object Language) interface is no longer in development. We recommend switching to and using our interface bConnect.
- Deprecated - The httpMOC interface is no in development. We recommend to change and use our interface bConnect.
- Deprecated - Direct access to the database (SQL/Oracle) is not supported. We recommend to change and use our interface bConnect.

\*Deprecated: - Feature updates and bug fixes are no longer provided. Critical security updates will be provided for the current version.

## 1.6.17 Supported Operating Systems

- bMS/R: baramundi Management Server, baramundi PXE Relay
- bMC: baramundi Management Console, including bRemote, ImageMount and License Management Add-On
- bAS baramundi Automation Studio
- bGW: baramundi Gateway
- bDIP: baramundi DIP, bBT and DipSync service
- bMA: baramundi Agent for Windows
- bND: baramundi Network Scanner as an add-on to Windows bMA
  
- X: Fully supported
- (X): Supported in productive environment with limitations

### 1.6.17.1 Server Operating Systems

Platform	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows Server 2022 Standard/Datacenter (Desktop display) <sup>4</sup>	(X)	(X)	(X)	(X)	(X)	(X)	(X)
Windows Server 2019 Standard/Datacenter (Desktop display)	X	X	X	X	X	X	X
Windows Server 2016 Standard/Datacenter (Desktop display)	X	X	X	X	X	X	X

<sup>4</sup> See [Known Limitations](#)

### 1.6.17.2 Client Operating Systems

Platform	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows 11 Pro / Enterprise (N) <sup>5</sup>		(X)	(X)		(X)	(X)	(X)
Windows 10 Pro / Enterprise 21H2 (N)(32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 21H1 (N)(32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 20H2 (N)(32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 2004 (N)(32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 1909 (N)(32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 1903 (N)(32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 1809 (N)(32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 1803 (N)(32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 1709 (N)(32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Enterprise 2019 LTSC (32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Enterprise 2016 LTSC (32 Bit and 64 Bit)		X	X		X	X	X
Windows 10 Enterprise 2015 LTSC (32 Bit and 64 Bit)		X	X		X	X	X

<sup>5</sup> See [Known Limitations](#)

### 1.6.18 Operating Systems with limited support

These operating systems are only supported to a limited extent. This means that new baramundi components and functions may not be usable, or that existing components and functions can no longer be used. Due to the complexity and variety of systems, baramundi cannot guarantee functionality on these systems. Due to the limitations, we recommend the use of more modern operating systems.

- (E): Supported to a limited extent because Microsoft has ended (basic) product support.

#### 1.6.18.1 Server Operating Systems

	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows Server 2012 R2 Standard/Datacenter (server with graphical user interface)	(E)	(E)	(E)	(E)	(E)	(E)	(E)
Windows Server 2012Standard/Datacenter (GUI server)	(E)	(E)	(E)	(E)	(E)	(E)	(E)
Windows Server 2008 R2 SP1 Standard/Enterprise/Datacenter		(E)	(E)	(E)		(E)	(E)

#### 1.6.18.2 Client Operating Systems

	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows 7 SP1 Professional/Enterprise/Ultimate (N) (32 Bit and 64 Bit)		(E)	(E)			(E)	(E)
Windows Server 2008 SP2Standard / Enterprise / Datacenter (32 Bit / 64 Bit)			(E)			(E)	(E)
Windows 10 Pro / Enterprise 1703 and older (N) (32-bit and 64-bit)			(E)			(E)	(E)
Windows 8.1 Pro / Enterprise (32 Bit / 64 Bit)		(E)	(E)			(E)	(E)
Windows Vista SP2(32 Bit / 64 Bit)			(E)			(E)	(E)
Windows XP SP3 (32 Bit)			(E)			(E)	

### 1.6.19 Languages

The baramundi Management Center, baramundi License Management and the Automation Studio are available in the following languages:

German, English

The bMA for Windows clients supports user messages in the following languages:

German, English, Bulgarian, Chinese, Danish, Finnish, French, Greek, Italian, Dutch, Norwegian, Polish, Portuguese, Romanian, Russian, Swedish, Slovak, Spanish, Turkish, Czech, Hungarian

The baramundi Kiosk supports the following languages:

German, English, Polish

Additional languages can be added by the administrator.

For all server-side services (i.e. baramundi Management Server, baramundi Gateway, DIP) the following languages are supported:

German, English

## 1.7 Known Limitations

### 1.7.1 Windows 11

- Windows 11 is currently treated like Windows 10 and can be used as a client to a limited extent.
- baramundi Managed Software (MSW) treats Windows 11 like Windows 10.
- The OS installation wizard does not automatically detect the Windows version.
- The release ID is not displayed correctly.
- OS cloning is not supported.
- The OS Customization Tool `<= 21.1.8` cannot be used.
- Further notes are published in the forum. ([Forum](#))

### 1.7.2 Windows Server 2022

- Windows Server 2022 is not yet recommended as a server platform for baramundi Management Suite modules. However, ASP.Net is required to run the bMS on Server 2022.
- Server 2022 can be operated as a client to a limited extent. It is treated like a Server 2019.
- The OS installation wizard does not automatically detect the Windows version.
- The OS installation may remain in the operating system edition selection.
- OS cloning is not supported.
- The release ID and display version are not shown.
- Further notes are published in the forum. ([Forum](#))

### 1.7.3 Notes on modification Access bMA.log

- Local administration rights are required to access the `bMA.log` file. Please also note the following comments.
- Existing rollover `bMA*.log` files are not re-authorized.
- In the bMC, the `Management Agent Log` action under `Custom Client Commands` is no longer usable in most environments and should be removed. The `bMA.log` can be accessed from the bMC via the user-defined client command `Explorer Drive C`. Here the user with local administration rights required for the client can be specified.
- Since local users usually do not have local administration rights, the bMA menu item "View Log" should be disabled under `bMC - Settings - Server - Management Agent`.
- If the access to the `bMA.log` should be adapted, the rights can be added via the bDS function `Edit permissions - Add access rights`.

### 1.7.4 General

- Note: Internet Explorer is no longer supported for Kiosk and bLM.
- Note: The bMS version 2020 R2 can no longer communicate with bMAs older than version 2019 R2.
- Note: Operating the bServer on Windows Server 2008 R2 is no longer supported.
- The bMA version must correspond to the bMS version.
- If the default web server port for the baramundi server is changed, OS Install, OS Cloning and Imaging are no longer possible.

### 1.7.5 Inventory 2016

- The optional offline-inventory does not use the `PreInvent.bds` and therefore does not fully support MSW.



### 1.7.6 Server (bServer)

- The modules under `Server Status Cloud Connector` are only active if the Argus Cockpit is configured and the connectors have been installed.
- On the baramundi Server no other software that uses WIBU CodeMeter runtime must be installed.
- The AD synchronization is not supported in networks in which the primary DNS-Suffix is different to the domain name.
- If an endpoint switches from an IP network in which a job cannot be run into an IP Network in which the job can be run, the job start will be delayed by up to 60 minutes.
- If a client changes from an IP network, where jobs can be executed, to a network, where no job execution has been configured, a job execution can still take place, since the bServer may have already run the check for the IP network.
- The management server starts jobs simultaneously and uses lots of database connections to communicate with the database server. In particular with Oracle databases it is imperative to have a sufficient number of available sessions and processes configured.
- When using an Oracle database system a given Tablespace for indexes will not be considered for all tables. With newly created as well as updated data-bases, some indexes will be created within the regular user Tablespace.
- If the bServer service is stopped while it is still queuing messages, these messages will be dropped. This can result in job targets getting stuck in a certain state. Do not stop bServer service while running multiple jobs.
- In the case of job steps, which dynamically generate further job steps, e.g. Patch or MSW scans, "resume" or "re-schedule" does not work in the event of an error.

### 1.7.7 Argus Cloud Connectoren

- Note: To enable the `baramundi Cloud Connector Dynamic Groups` to synchronize the desired `Universal Dynamic Groups (UDG)` to Argus, the bConnect user stored under `Configuration-Interface-Cloud Connection` must have at least read access to the UDG.

- The proxy stored with the downloader is not taken into account. A proxy can be configured via the .config file.

### 1.7.8 PXE Boot

- Use the ADK recommended by baramundi.
- When using the baramundi Syslinux bootloader (configurable from the PXE Support settings) some Windows device may get stuck when trying to boot from their hard drive. Please follow the instructions from this forum post to fix the problem:  
<https://forum.baramundi.de/index.php?threads/5339>

### 1.7.9 Windows Agent (bMA)

- If `Do not disturb mode` is active on the client, jobs that are to be executed during shutdown cannot be assigned correctly. The jobs will then not be executed during shutdown.
- If a job is already scheduled on the client for the shutdown time and the user then sets the `Do not disturb mode`, the job may only be executed after a waiting time during the shutdown. The waiting time then corresponds to the time set under `bMC - Configuration - Server - Settings - Job execution`.
- Note: Backup files created with Disaster Recovery of a bMS 8.5 or older cannot be restored from version 2020 R1.
- Note: Newly introduced job steps, such as `Bitlocker Network Unlock` or `Inventory Microsoft updates`, are not considered during job execution if an older bMA is installed on the target system.
- In version 2020 R1 there were changes to the bDS engine when using embedded scripting languages, which in very rare cases result in script abort with the error message "Use of an outdated syntax: The expression {=VBScript} is no longer supported". Conversion by Automation Studio is not sufficient, manual adaptation of the affected scripts is necessary. Further information can be found in the forum at: <https://forum.baramundi.de/index.php?threads/10458>
- If a manually modified bMA installation command is used, it must be updated to the new setup format. The default is "`\\{Server}\BMS$\Client\Setup\ManagementAgent_setup.exe /Q SERVER={Server} SERVERKEY="{ServerKey}" OPTIONS={AgentOptions}`".

- Windows 10 Virtual Desktop is detected as Server 2016.
- The HW inventory uses a SHA256 driver signature and is not executable on XP, Server 2008 and Vista. For Windows 7 KB3033929 is required.
- The keyboard and mouse lock can not lock touch input on operating systems lower than Windows 8.
- The keyboard and mouse lock fails to lock mouse orientated control options at the edge of the screen. Operation of the charm bar or the Apps is locked.
- A (patch-)job of the type Active with WakeOnLAN will not shut down as configured if a reboot was performed during job execution.
- The security context „Local Install User“ cannot be used on systems with the role „Domain Controller“.
- The file inventory shows files larger than 2GB with a file size of 2GB.

### **1.7.10 Automation Studio**

- Notes on bDS files from version 2020 R1:
  - When a bDS file is opened, a message is displayed indicating that conversion to the new format is necessary. A converted script can only be executed by bMAs of version 2020 R1 or higher.
  - In environments with multiple baramundi servers, please take care that bDS scripts are not converted until all servers/clients are on version 2020 R1 or higher. If conversion to the new format is not yet desired, Automation Studio version 2019 R2 can still be used.
  - The bMA from 2020 R1 on will be able to run both the new bDS format and the previous format. A conversion of all bDS scripts is not necessary.

### **1.7.11 Defense Control**

- BitLocker cannot be paused for jobs that boot directly into WinPE
- Prerequisite is Windows 10 1511 or later.
- An activated TPM 2.0 is required.

- Connected iSCSI drives are also encrypted with drive encryption type "Full Encryption".
- The startup PIN function must be set via a group policy. GPO "Require additional authentication at startup".

### **1.7.12 Mobile Devices**

- Certificate deployment by SCEP using baramundi Mobile Devices profiles does not support profile certificate renewal. Repeat profile deployment to issue new certificates.

### **1.7.13 Mobile Devices – Android Enterprise**

- App installation and configuration jobs for mobile devices will perform a locking load operation in display mode for very large app configurations (e.g. Zebra OEMConfig).
- Devices with a set unlock code will not execute jobs after a restart of the device until the unlock code is entered correctly. This also applies if the unlock code is only set for the working profile and the working profile is reactivated from the pause mode.
- From Android 10 no inventory and no uninstallation of Wi-Fi is possible if the location access for the device or the work profile is deactivated.
- Work Profile: Starting with Android 9, sharing files in the work profile via Bluetooth does not work.
- The display lock on Android Enterprise only works with Android 9.
- It is not possible to assign a company with the baramundi Evaluation license. This requires a full bMS license.
- If the bServer/bGateway cannot be reached when enrolling the device, this process can only be left by "reset to factory settings".
- On Huawei devices, which do not fulfill password guidelines, apps cannot be reliably hidden/blocked.

### **1.7.14 Mobile Devices – Android**

- Starting with Android version 9, static IPs cannot be set in a Wifi profile.
- The user field in the WLAN configuration of TLS is not supported.
- The operations set/reset password no longer work with Android 7.

- The Samsung Knox Extension App must be deployed via deploy job to support Samsung Knox devices < Version 4.2.2. The App has been removed from the google PlayStore.
- When first installing baramundi Apps on a Samsung device running Android 4.2 or newer users will see an additional dialog. Here, they have to agree to the ELM Service usage conditions. Without approval no jobs will be executed on such a device.
- Deploying Enterprise WiFi configurations using client certificates requires a configured display lock (PIN, pattern) on Android devices.
- Deploying Enterprise WiFi configurations to Samsung devices running Android versions older than 5.0 (Lollipop) requires an additional certificate configuration block in the same profile. As the device only accepts the WiFi connection if it has a complete trust chain for the access points certificate, make sure to deploy all necessary CA certificates as well. If it is missing no specific error message is given.
- When removing a profile containing a WiFi configuration with TLS from a Samsung device running Android 4.3 the client certificate is not completely removed. The remains are non-functional.
- Note: Deploying a client certificate via SCEP to an Android device without a corresponding WiFi or exchange configuration block is only supported for Samsung Knox compatible devices. For other Android devices running at least version 4.3, SCEP is supported for deployment of Enterprise WiFi (TLS) configurations.
- Enrollment links from emails may fail to work correctly from the Android default mail app if the option "Activate verification of the server identity on the first connection" is disabled.

### 1.7.15 Mobile Devices – iOS

- The „Migrate from device to device“ option in Apple DEP does not work correctly.
- Note: The automatic VPP app update is not possible with iOS14. This bug has been fixed by Apple in iOS 14.2.
- The bServer must run on a Windows Server 2016 or higher to manage iOS devices.
- The following restrictions are only usable in supervised mode from iOS 13: "Disallow camera", "Disallow iCloud backup", "Disallow explicit content", "Disallow safari automatic fill", "Disallow safari".

- From iOS 13, devices are always supervised, regardless of the configuration in the enrollment profile.
- Starting with iOS 13, profile installation on devices is always mandatory, regardless of the configuration in the enrollment profile.
- After enrolling an iOS device it can take several minutes until the Agent on the bMD device recognises the enrollment.
- Using iOS App Push requires each iOS device to register their Push Token with the bMS server. To do this, the user has to start bMA manually, once. After restoring a device backup it can be necessary to repeat the registration. Older devices (like iPad 2) may still reconnect only once within several days, even with regular push signals being sent.
- Because of restrictions for iOS background updates, compliance information generated by bMA may be delayed. To ensure regular updates users have to start the bMA from time to time. Alternatively, enable the new iOS App Push service.
- The Apple Device Enrollment Program (DEP) is supported with iOS versions 8.3 and later.
- As of iOS version 8.0 an MDM software inventory will not recognize if an app had been installed correctly. The App is registered as managed and installed after the confirmation of the installation by the end user, however if for example the download aborts after the user confirmation and the App cannot be used, it will still be shown as correctly installed in the Inventory data.

### 1.7.16 Mobile Devices – Windows Phone

- Will no longer be supported from Release 2020 R1.

### 1.7.17 Management Center (bMC)

- On English systems the sorting in the bulletin selection of a patch job (classic) does not work as expected.
- If UniCode characters are used in the name or comment in `Inventory - Network Scan - Profiles`, this leads to errors in the display during job creation or bDX import/export.
- Crystal Reports version 13.0.8 is required to view reports. A newer version is not supported.

- The help system shows only limited content when used offline.
- Under "Configuration - License configuration", "No data available" is displayed if the new licensing is not used.
- The Universal Dynamic Groups cannot be used in reports.
- bMC users without the setting "Display endpoint user identities" can view the users of the endpoints on clients via the properties dialog if they have write access to the endpoint.
- bMC users and end user names are partly visible in log files or certain status messages and cannot be suppressed there.
- Import/Export (bDX) does not support jobs with backups, restore data from backup, deploy energy policies, manage virtual machine.
- Correct or higher rights are required for all import actions that access BMS\$. To import SSA or OS Install scripts, it is useful to start the bMC in the administrative context.
- The bMC supports only the languages German and English. On servers in other languages, the English language pack must be installed.
- The report "List SNMP Devices" does not work correctly on Oracle databases.
- Permissions on Mac OS X or mobile devices are always inherited from their parent logical group. Setting individual permissions is currently not supported.
- Using the integrated reports requires enabled remote authentication for the backend SQL server system.
- Using the Store Search feature with a network proxy only works with proxies without authentication, or by using a logged on AD user.
- New Edit dialogs do not lock objects. When editing objects simultaneously the first user can save his changes. Other user will see the error message „Can't save stale data object“ when trying to save changes.
- When using bMC in a time zone different to the Management server, time values may differ.
- The Revision log does not recognize the following activities: „Defer Job“, „Start/Resume/Cancel/Delete Job Target“, „Set Job OK“, „Move Group“, „Move Device“, „Cre-

ate/Edit/Delete Static Group”, ”Delete Pending Downloads for MSW and Patch Management” and ”Delete File and Registry Entries from Inventory”.

### 1.7.18 macOS devices

- Automatic device registration methods may create new Windows device objects for macOS-devices, even if they already exist in the database. This cannot be prevented. Disable such Windows devices.
- Compliance rules for jailbreaks and last agent contact will be ignored for macOS-devices.
- If a variable used in a shell script contains shell commands, such commands will get executed during a job execution (Command Injection). This behaviour is intended for use by users with advanced scripting know how.

### 1.7.19 Compliance

- No bMS variables can be used in the user defined compliance bDS scripts.
- A dynamic group using CVE filters will also refer to disabled rules.
- When using an Oracle database system the ”Vulnerable Products” view on logical groups may encounter errors while loading a detail pane. This problem occurs when a high number of devices or vulnerabilities is present.

### 1.7.20 Remote

- Connecting to the desktop session of the Local Install User is not supported.

### 1.7.21 Update Management (Patch Management)

- Job steps `Distribute Microsoft Updates with Update Profile` lead to an error, if the client has not assigned an update profile. If a job retry is configured in case of an error, this error pattern is not always immediately apparent.
- After reinstalling a client the `Client-Microsoft Updates` view continues to show the data before the reinstallation.
- A new class of Microsoft updates named „Upgrades” has been introduced to bMS. Usage of this term is inconsistent between WSUS and online update services. Currently, we advise against using this for patch deployment.



### 1.7.22 Virtual

- Controlling and creating virtual machines requires a VMware license containing the „vSphere API” feature. This feature is not a part of the free ESXi license. Therefore with the free ESXi Version only inventory is possible.
- When running an inventory of a hypervisor, data on a virtual machine operating system is only available if that machine is turned on and has the VMware tools installed and running.

### 1.7.23 OS Install

- In some cases it may not be possible to boot older systems with ADK 10. In this event a separate boot image can be created with WAIK 8.1. We recommend saving this in the path “WAIKPE”
- The Windows 10 Inplace-Upgrade first runs a system check and then stops with warning messages, if these messages should be ignored the script InPlaceUpgrade.bds can be edited accordingly.
- Jobs with Inplace-Upgrade steps that also contain patch steps may abort with the error "The operating system installation of job [...] is not allowed for client [...]".

### 1.7.24 Clients in Internet Mode / Dynamic Mode

- Automatic update of agents in the jobs is not possible.
- If a CEM endpoint is returned to LAN mode, the bMA needs to be reinstalled.
- The client announcement can not be disabled for clients in dynamic mode. In this case, the default value is 30 minutes.

### 1.7.25 Network Devices (bND)

- If a context is specified in the SNMPv3 scan, some devices (e.g. Cisco Catalyst switch) are not detected.
- Devices with more than one IP address at a MAC address might be detected and created as independent devices.
- During scans HUAWEI switches are sometimes not responding to multiple SNMP requests.

- In order to determine an ideal IT map STP (Spanning Tree Protocol) should be activated.
- Note: The data determined by the scans are used to display the IT map. It is not a live view of the network environment.

### **1.7.26 Comparex Miss Marple**

- The Report names are in German on English operating systems.
- The reporting server has to be able to support authentication via negotiate.
- As of Windows 2008 R2 SQL Server Reporting Services are supported in native mode.

## 2 Release 2021 R1U1

### 2.1 baramundi Ticketing System

Whether it's setting up new workstations, providing support for end users or generally troubleshooting network problems, IT admins are constantly busy as internal service providers. Keeping track of the multitude of tasks can be a challenge. Email and telephone requests for support are often lost in the daily flood of changing tasks or quickly displaced by higher priorities.

The baramundi Ticketing System powered by OMNINET offers a simple and quick solution. The cloud-based tool helps you organize and track IT support requests easily and efficiently, and generates progress reports automatically.

 This module is currently only available in German.

#### 2.1.1 Ready-made Workflow Templates

The baramundi Ticketing system comes with five ready-to-use workflow templates for rapid deployment without any special configuration. Up to eight pre-defined and user-definable workflows are available with no limit on the number of tickets.

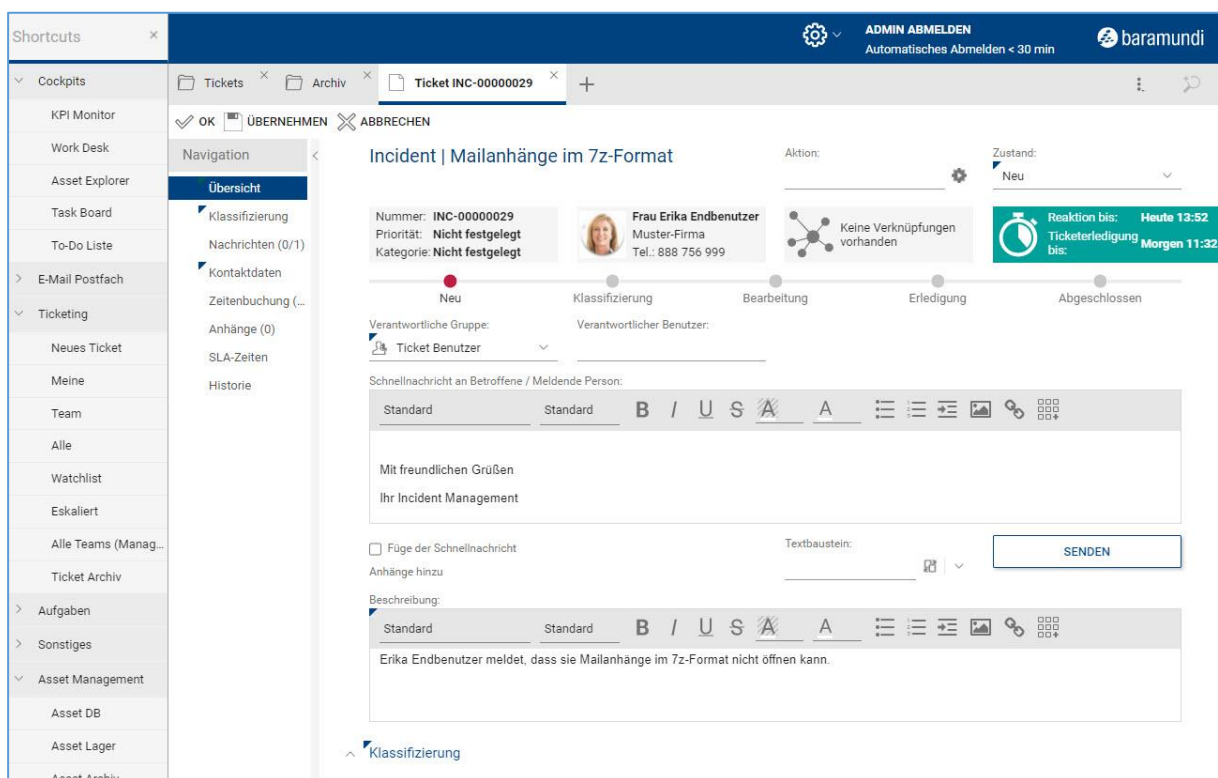
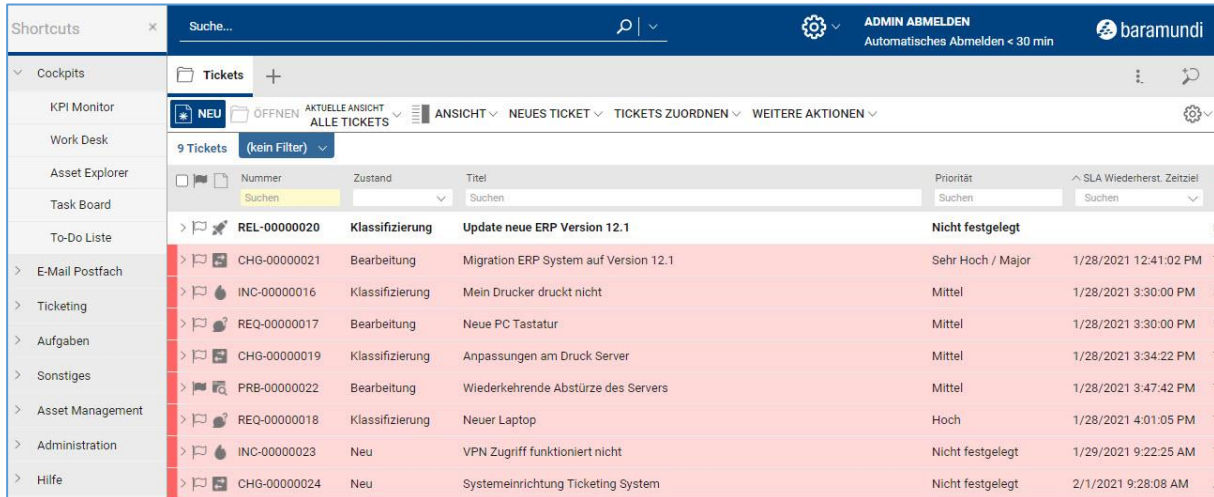


Figure 1 Ticket as seen by the admin

The module also includes email integration and service level management (SLM) to ensure compliance with request handling best practices.

## 2.1.2 Scope of application

The ticketing system supports you in processing tickets in six different ticket scenarios.



Nummer	Zustand	Titel	Priorität	SLA Wiederherst. Zeitziel
REL-00000020	Klassifizierung	Update neue ERP Version 12.1	Nicht festgelegt	
CHG-00000021	Bearbeitung	Migration ERP System auf Version 12.1	Sehr Hoch / Major	1/28/2021 12:41:02 PM
INC-00000016	Klassifizierung	Mein Drucker druckt nicht	Mittel	1/28/2021 3:30:00 PM
REQ-00000017	Bearbeitung	Neue PC Tastatur	Mittel	1/28/2021 3:30:00 PM
CHG-00000019	Klassifizierung	Anpassungen am Druck Server	Mittel	1/28/2021 3:34:22 PM
PRB-00000022	Bearbeitung	Wiederkehrende Abstürze des Servers	Mittel	1/28/2021 3:47:42 PM
REQ-00000018	Klassifizierung	Neuer Laptop	Hoch	1/28/2021 4:01:05 PM
INC-00000023	Neu	VPN Zugriff funktioniert nicht	Nicht festgelegt	1/29/2021 9:22:25 AM
CHG-00000024	Neu	Systemeinrichtung Ticketing System	Nicht festgelegt	2/1/2021 9:28:08 AM

Figure 2 View of the agent on his open tickets

### 2.1.2.1 Incident Management

Restore IT services to users as quickly as possible in the event of a disruption and minimize downtime in business operations.

### 2.1.2.2 Problem Management

Reduce incidents and prevent their recurrence through structured diagnoses of technical problems.

### 2.1.2.3 Task Management

Manage all IT tasks from a central interface and accelerate single tasks and entire projects.

### 2.1.2.4 Request Fulfillment

Achieve higher customer and user satisfaction by standardizing and reducing the administrative burden for service requests.

### 2.1.2.5 Knowledge Management

Achieve higher IT and end-user satisfaction through standardization of support processes and reduced administrative effort for service requests.

### 2.1.2.6 Change Management

Manage all activities and improve the quality and consistency of IT processes in both small- and large-scale organizational changes.

### 2.1.3 Integration of Jobs

Automate the completion of standard requests using familiar bMS jobs. All jobs created in the baramundi Management Suite, including common tasks such as software deployment and endpoint configuration, can be completed directly within a ticket.

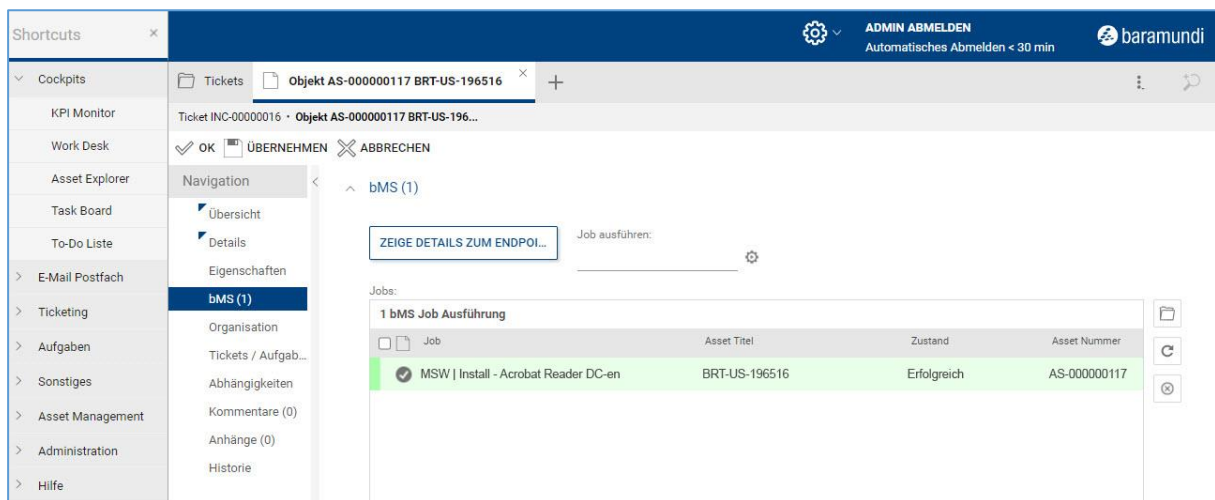


Figure 3 Job-history of an endpoint

New jobs can be added to an existing ticket. The system also automatically documents Job execution and completion for evaluation immediately or to identify and analyze trends over time.

### 2.1.4 Automated processing

Up-to-date information on managed endpoints can also be called up from the asset database as required for ticket processing. This allows one or more jobs to be executed consecutively on a respective endpoint. It is also possible to schedule Jobs, e.g., a new installation can be set to run in the evening. Once the job is successfully completed the ticket is closed automatically.

Requests for approval of installation of licensed software are predefined and automatically sent to an authorized supervisor. This workflow also can be stored in ticket templates and offered as a self-service for end users if desired. An integrated knowledge base enables the management, tagging and linking of articles, self-help guides as well as recorded solutions. This database can be made available to both internal editors and end users via a customer portal.

### 2.1.5 Reporting

All requests and outcomes are automatically recorded. Comprehensive evaluations can be created at any time using individually definable filters and views, then exported to external BI

systems via the reporting interface. In addition, an individually configurable KPI dashboard is available for a quick overview.

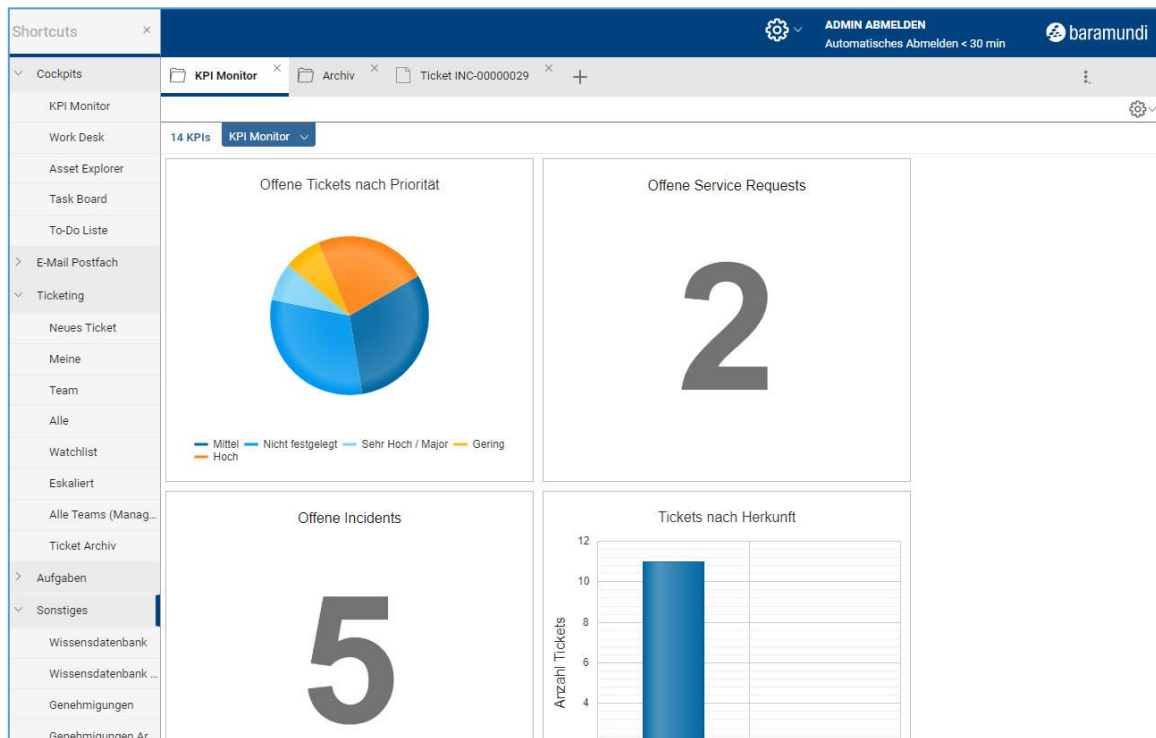


Figure 4 KPI dashboard for a quick overview

## 2.1.6 Ticketing from the cloud

The ticketing system is cloud-based for fast and simple deployment. It is linked to your baramundi Management Suite via a Connector.

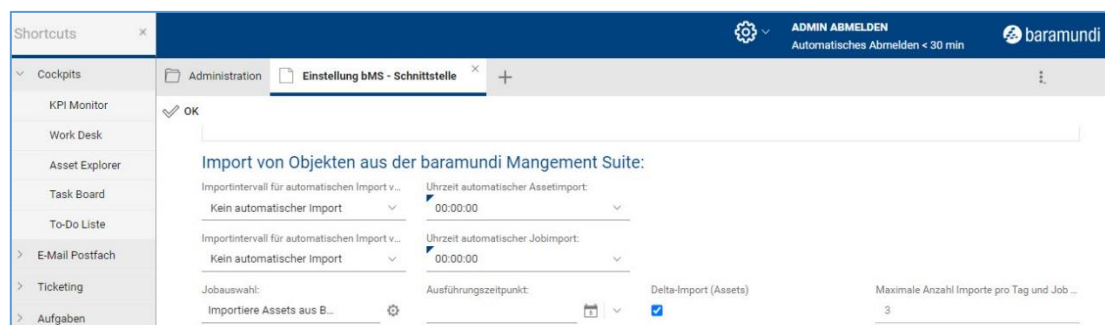


Figure 5 Configuration of the bMS-connector

Communication takes place exclusively via the Connector and is encrypted according to industry standards.

## 2.2 Microsoft Update Management

Administrators face the same challenge every month when installing updates: security gaps must be closed quickly, but the function and thus the regular operation of the endpoints must remain stable. Staggered rollout of updates has proven to be a best practice. Here, updates are first installed and tested on a small subset of the endpoints in the company - regardless of department or criticality - before they are distributed in waves throughout the rest of the company. These waves can overlap in order to close security gaps as quickly as possible, or they can start at different times - e.g., several days apart - in order to identify problematic updates early on and interrupt the rollout if necessary.

### 2.2.1 The update profile as central configuration

Update profiles are now available for granular control of update behavior. You can define how long after an update is published that it may be installed up to a maximum of 30 days.

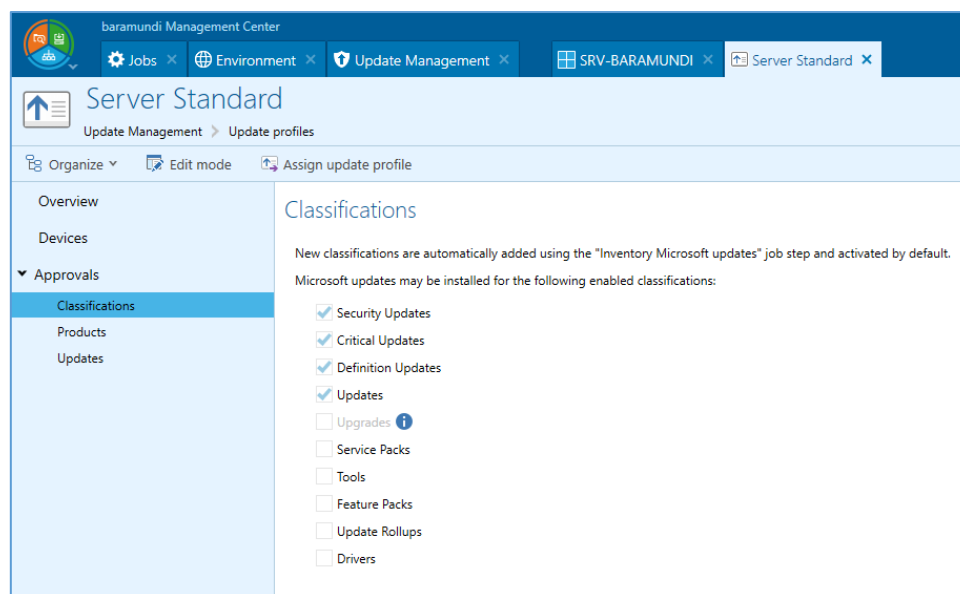
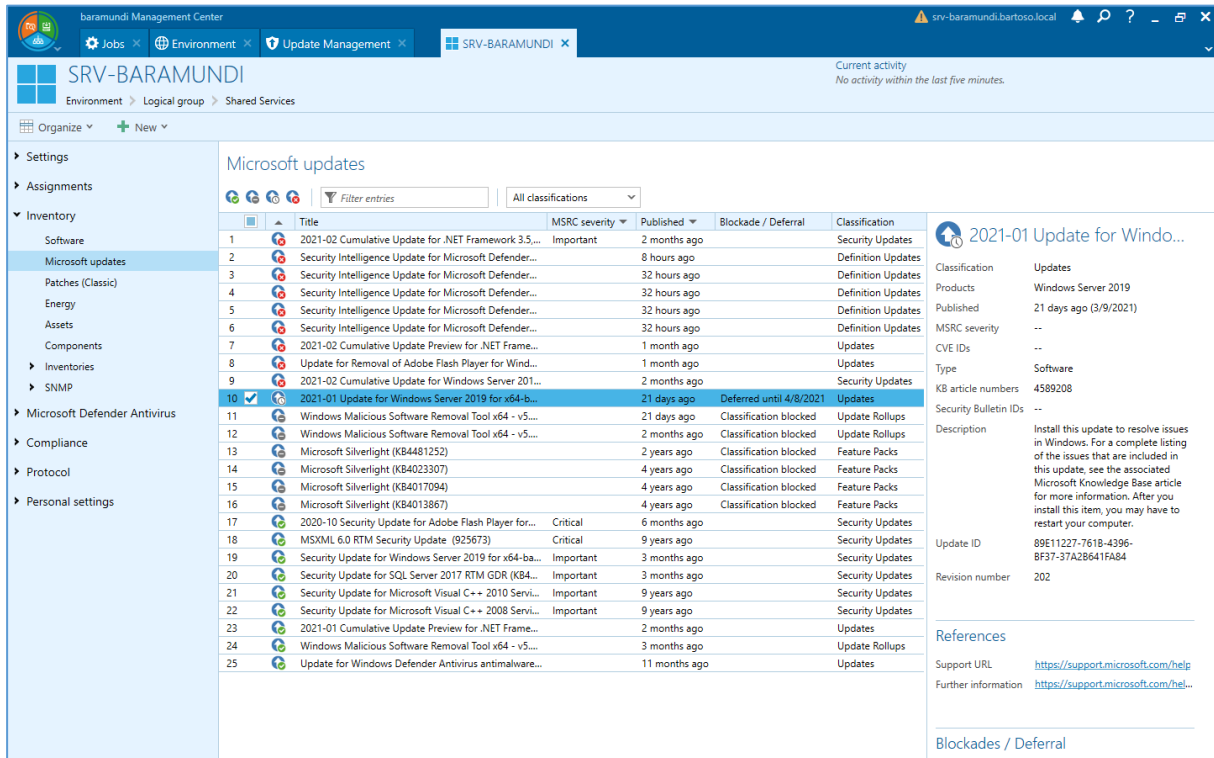


Figure 6 Configuration of the supported classifications of an update profile

Similarly, update categories such as device drivers, specific products or even an entire update can be excluded in the update profile to ensure that problematic installations are not distributed to affected endpoints.

### 2.2.2 Detailed information about the update status

The inventory of Microsoft updates introduced with the bMS 2020 R2 now also reflects the configuration by the update profile. You can see at a glance which updates are missing and why, and view when delayed updates can be installed.



**Microsoft updates**

	Title	MSRC severity	Published	Blockade / Deferral	Classification
1	2021-02 Cumulative Update for .NET Framework 3.5...	Important	2 months ago		Security Updates
2	Security Intelligence Update for Microsoft Defender...		8 hours ago		Definition Updates
3	Security Intelligence Update for Microsoft Defender...		32 hours ago		Definition Updates
4	Security Intelligence Update for Microsoft Defender...		32 hours ago		Definition Updates
5	Security Intelligence Update for Microsoft Defender...		32 hours ago		Definition Updates
6	Security Intelligence Update for Microsoft Defender...		32 hours ago		Definition Updates
7	2021-02 Cumulative Update Preview for .NET Frame...		1 month ago		Updates
8	Update for Removal of Adobe Flash Player for Wind...		1 month ago		Updates
9	2021-02 Cumulative Update for Windows Server 201...		2 months ago		Security Updates
10	2021-01 Update for Windows Server 2019 for x64-b...		21 days ago	Deferred until 4/8/2021	Updates
11	Windows Malicious Software Removal Tool x64 - v5...		21 days ago	Classification blocked	Update Rollups
12	Windows Malicious Software Removal Tool x64 - v5...		2 months ago	Classification blocked	Update Rollups
13	Microsoft Silverlight (KB4481252)		2 years ago	Classification blocked	Feature Packs
14	Microsoft Silverlight (KB4023307)		4 years ago	Classification blocked	Feature Packs
15	Microsoft Silverlight (KB4017094)		4 years ago	Classification blocked	Feature Packs
16	Microsoft Silverlight (KB4013867)		4 years ago	Classification blocked	Feature Packs
17	2020-10 Security Update for Adobe Flash Player for...	Critical	6 months ago		Security Updates
18	MSXML 6.0 RTM Security Update (925673)	Critical	9 years ago		Security Updates
19	Security Update for Windows Server 2019 for x64-ba...	Important	3 months ago		Security Updates
20	Security Update for SQL Server 2017 RTM GDR (KB4...	Important	3 months ago		Security Updates
21	Security Update for Microsoft Visual C++ 2010 Servi...	Important	9 years ago		Security Updates
22	Security Update for Microsoft Visual C++ 2008 Servi...	Important	9 years ago		Security Updates
23	2021-01 Cumulative Update Preview for .NET Frame...		2 months ago		Updates
24	Windows Malicious Software Removal Tool x64 - v5...		3 months ago		Update Rollups
25	Update for Windows Defender Antivirus animalware...		11 months ago		Updates

**2021-01 Update for Windows Server 2019 for x64-based systems**

Classification: Updates

Products: Windows Server 2019

Published: 21 days ago (3/9/2021)

MSRC severity: --

CVE IDs: --

Type: Software

KB article numbers: 4589208

Security Bulletin IDs: --

Description: Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

Update ID: 89E11227-7618-4396-BF37-37A2B641FA84

Revision number: 202

References:

Support URL: <https://support.microsoft.com/help>

Further information: <https://support.microsoft.com/help>

Blockades / Deferral

Figure 7 List of all updates of an endpoint with respective update status

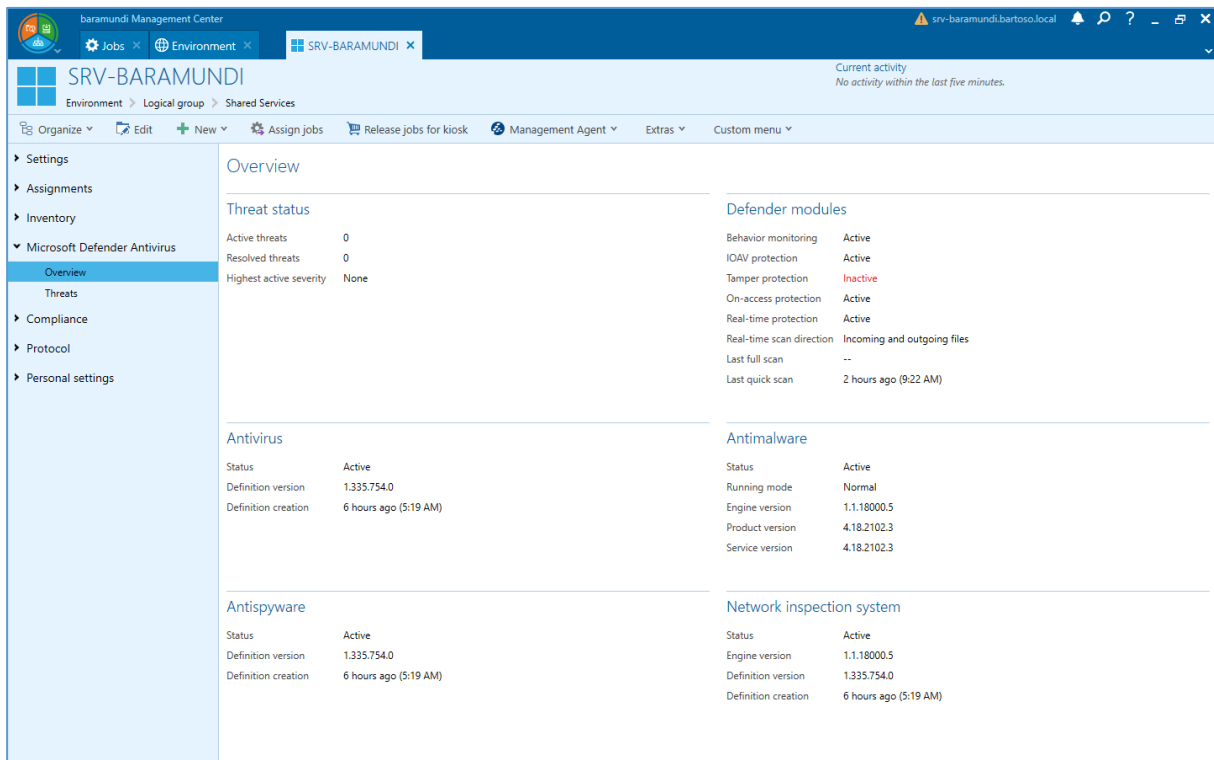


## 2.3 Management of Microsoft Defender Antivirus

Microsoft Defender Antivirus is a reliable antivirus solution integrated into Windows at no additional cost. That makes it both widely used and the subject of an increasing number of requests from baramundi users for a centralized management capability. We've done exactly that by including it as a function in the baramundi Defense Control module.

### 2.3.1 Central view of threat conditions

Endpoint status is now displayed in detail in the bMC so you can immediately see if Defender Antivirus and the underlying modules and components are working properly.



The screenshot displays the baramundi Management Center interface for SRV-BARAMUNDI. The left sidebar shows a navigation menu with options like Settings, Assignments, Inventory, and Microsoft Defender Antivirus. The main content area is titled 'Overview' and provides a detailed status of the Defender Antivirus. It includes sections for Threat status, Defender modules, Antivirus, Antispyware, and Network inspection system.

Threat status	
Active threats	0
Resolved threats	0
Highest active severity	None

Defender modules	
Behavior monitoring	Active
IOAV protection	Active
Tamper protection	Inactive
On-access protection	Active
Real-time protection	Active
Real-time scan direction	Incoming and outgoing files
Last full scan	--
Last quick scan	2 hours ago (9:22 AM)

Antivirus	
Status	Active
Definition version	1.335.754.0
Definition creation	6 hours ago (5:19 AM)

Antispyware	
Status	Active
Definition version	1.335.754.0
Definition creation	6 hours ago (5:19 AM)

Network inspection system	
Status	Active
Engine version	1.1.18000.5
Definition version	1.335.754.0
Definition creation	6 hours ago (5:19 AM)

Figure 8 Details on Defender Antivirus status at the endpoint

In addition, all threats found on an endpoint are transmitted to the bMS for evaluation and any needed remediation.

Since this data is collected centrally at the bMS for all endpoints you can easily determine the protection and threat levels for the entire network, specific subnets or workgroups, or individual endpoints.



The bMS now also enables you to actively resolve identified threats. Virus definitions can now be updated in a job step. You also can trigger a quick or full scan while the system is running. For particularly stubborn cases when a threat cannot be removed while Windows is running you can initiate an offline scan in WindowsPE.



## 2.4 baramundi Argus Cockpit

The capabilities of the baramundi Argus Cockpit (bAC) module have been growing continuously since the 2020 release. Many of the new features can be used in versions of the bMS prior to Release 2021 R1<sup>6</sup>.

### 2.4.1 Set individual threshold values for UDG

Since Release 2020 R2, Universal Dynamic Groups (UDG) in the bMS can be synchronized with the Argus Cockpit and the corresponding results list shared with authorized employees who do not have access to the baramundi Management Center.

To make it easier for bAC users to recognize the endpoint or Job status in their applicable UDGs, at-a-glance traffic light colors indicators are displayed in the Argus Cockpit.

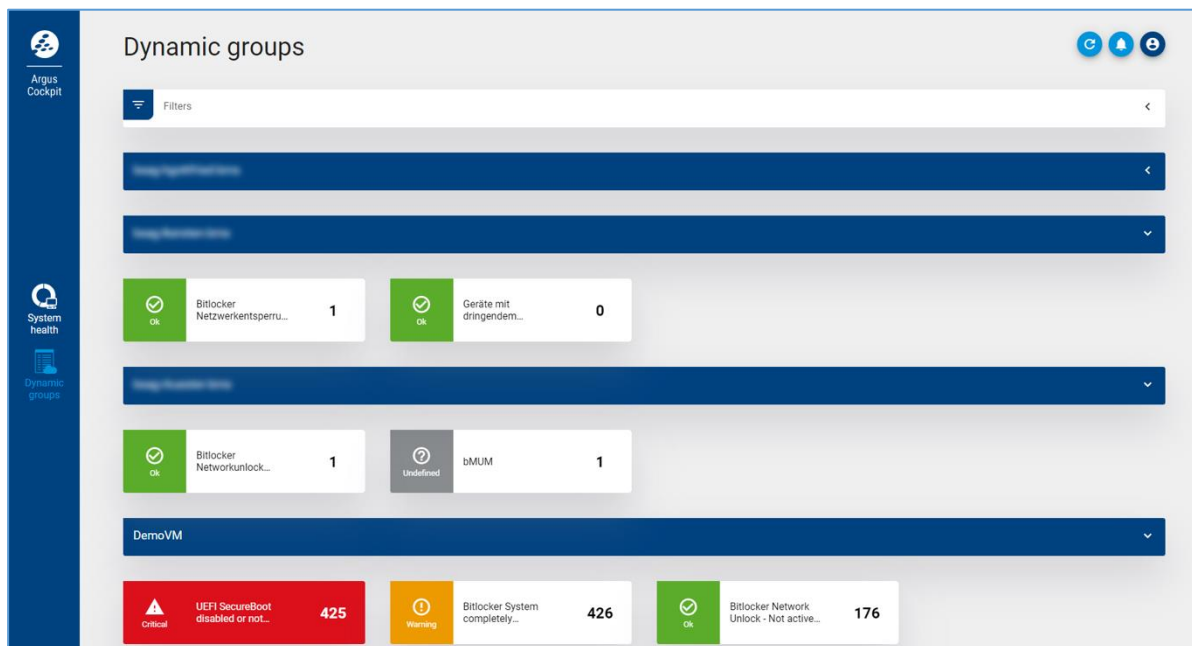


Figure 11 Traffic light indicators show UDG status at a glance

<sup>6</sup> <https://www.baramundi.com/en-us/management-suite/module/baramundi-argus-cockpit/updates/>

bAC users can now define individual threshold values for each synchronized UDG. When the defined threshold values are reached, the UDGs are highlighted accordingly. This signals to the IT administrator that action may be required in the bMS.

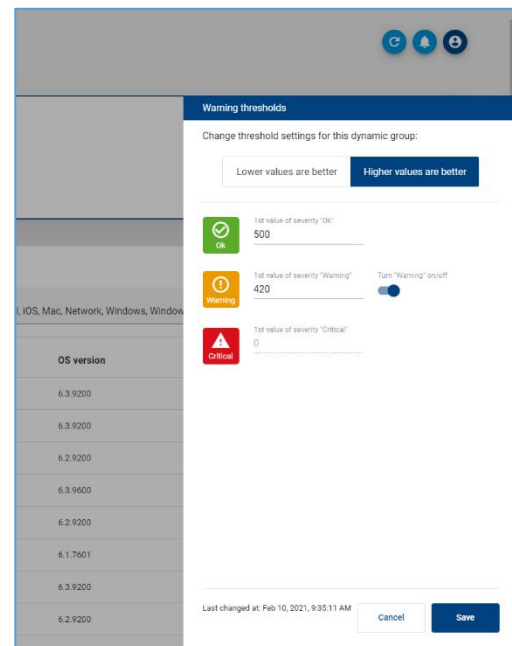


Figure 12 Set individual UDG thresholds

## 2.4.2 Display historical data with Argus Trends

One of the distinguishing features of the bMS is that it provides the IT admin with a very good overview of the entire IT environment. It displays current parameters and conditions of end devices so that appropriate actions can be initiated if their ACTUAL state does not correspond to the TARGET state.

It's also helpful in certain situations to view and analyze the states of the end devices over time. The new Argus Trends feature make this retrospective view possible.

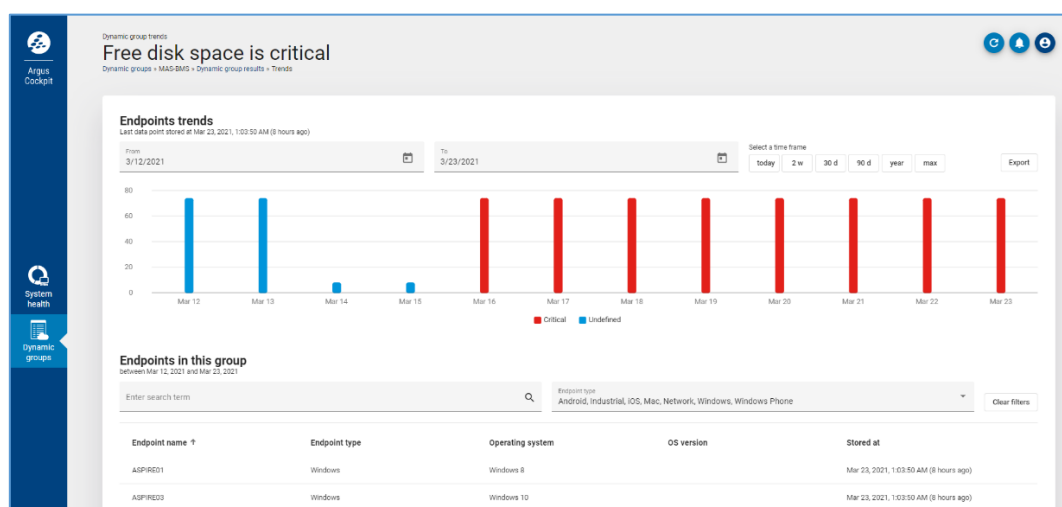


Figure 13 Trends of UDG results

For example, IT admins can now see how many critical updates have not been installed on one or more end devices in the last 4 weeks. This information is particularly helpful for an upcoming security audit or reporting to the CISO.

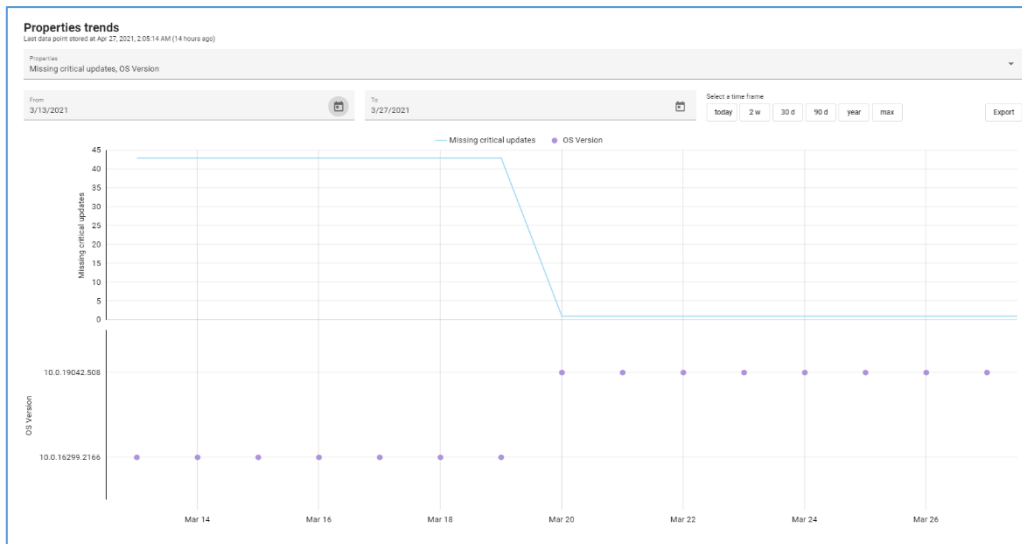


Figure 14 View historical data in Argus Trends

The following historical endpoint information is available in Argus Cockpit:

- Missing Critical Updates
- BitLocker Network Unlock Status
- System Volume BitLocker Status
- OS Version
- Last Channel

It's also helpful for MSPs to view, analyze and generate reports on UDG results and their defined thresholds. For example, the number of end devices that required an in-place upgrade in the last few days or weeks can now be easily reported to MSP staff or to customers.

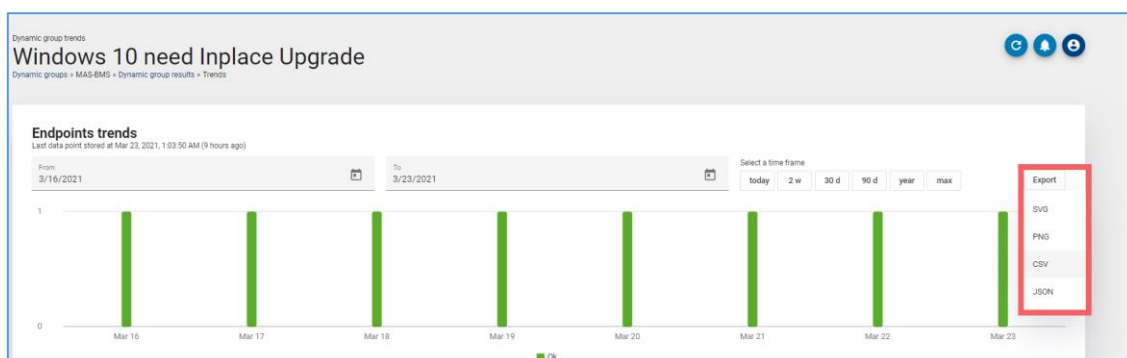


Figure 15 Easy export of relevant UDG trends

### 2.4.3 Other relevant data visible in Argus

As described in [Section 3](#), Microsoft Defender information will be recorded in the bMS from Release 2021. This information will also be transferred to Argus Cockpit and can be viewed by IT admins at any time and/or used to define UDGs.

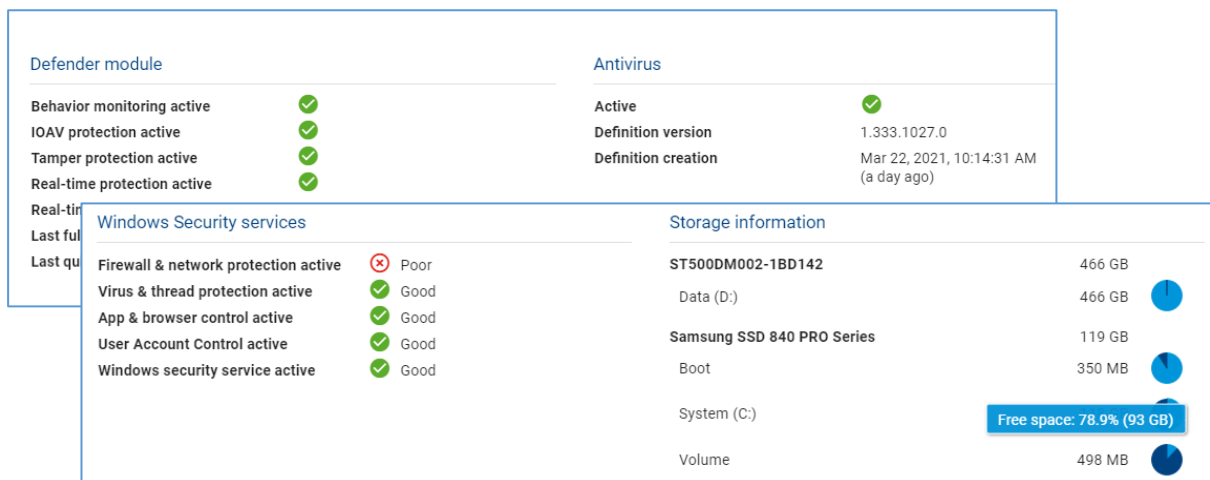


Figure 16 Concise view of MS Defender and related information

## 2.5 bCenter – the Pocket-bMC

The mobile version of the baramundi Management Center has been completely revised and is now available for Apple iOS and Google Android.



With the mobile bCenter, you can, for example, start an update job from a smartphone or tablet or also check the status of the endpoints; no Windows PC with baramundi Management Center installed is required.

### 2.5.1 Manage Endpoints

With the bCenter you can navigate and search your IT environment. For example, you can locate individual endpoints using the search function (including QR, barcode and NFC scanner)

<sup>7</sup> <https://apps.apple.com/de/app/baramundi-management-center/id1069301410>

<sup>8</sup> <https://play.google.com/store/apps/details?id=com.baramundi.android.bcenter>

to view individual endpoint information and system details, assign jobs, check status, and even view and edit variables.

## **2.5.2 Assign Jobs**

The Job view gives you access to all existing jobs. You can either navigate through the folders or find the desired job using the search function. The selected job can then be assigned to an endpoint.

## **2.5.3 Usability**

We prioritized implementation of customer requests in the feedback portal. In addition to multi-platform compatibility, we focused on usability with the following new functions:

### **2.5.3.1 Dark mode**

The display can now be changed to an eye-friendly dark mode display if desired

### **2.5.3.2 Added language support**

bCenter now supports English and German with additional language support planned.

### **2.5.3.3 Login with biometric sensors**

Login information including the server, username and password can be securely stored on the device and unlocked via biometric sensor. This eliminates the need to reenter login credentials when the app is restarted.

### **2.5.3.4 Favorites**

Critical, priority or frequently used endpoints and jobs can be marked as favorites and pinned on the starting page for quick and efficient access.

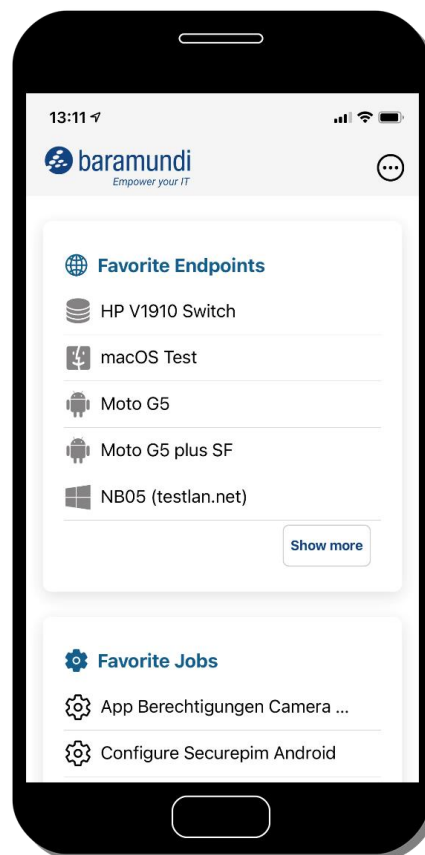


Figure 17 Home screen with favorites

### 2.5.3.5 Filter

All views in bCenter now have platform filters. For example, you can specifically list only Windows endpoints or only iOS and Android mobile endpoints. All other platforms are hidden. Likewise, you can display just the jobs applicable to the desired target platforms.

### 2.5.3.6 NFC-Tags

In addition to capturing QR and barcodes, the bCenter can also read and write NFC tags. This allows you to write endpoint data to an NFC tag within the app. As soon as a corresponding NFC tag is read in the app, the associated endpoint opens immediately with all relevant data.

## 2.6 Additional enhancements

### 2.6.1 License Management

The baramundi License Management module offers a concise and simple way to show where licenses are deployed in the company for increased transparency of license usage and availability. Licenses with multiple usage rights also can be displayed.



### 2.6.1.1 Concept

Software installations offer different usage rights according to the respective license types. In the case of multiple usage, this can be associated with specific devices and/or users.

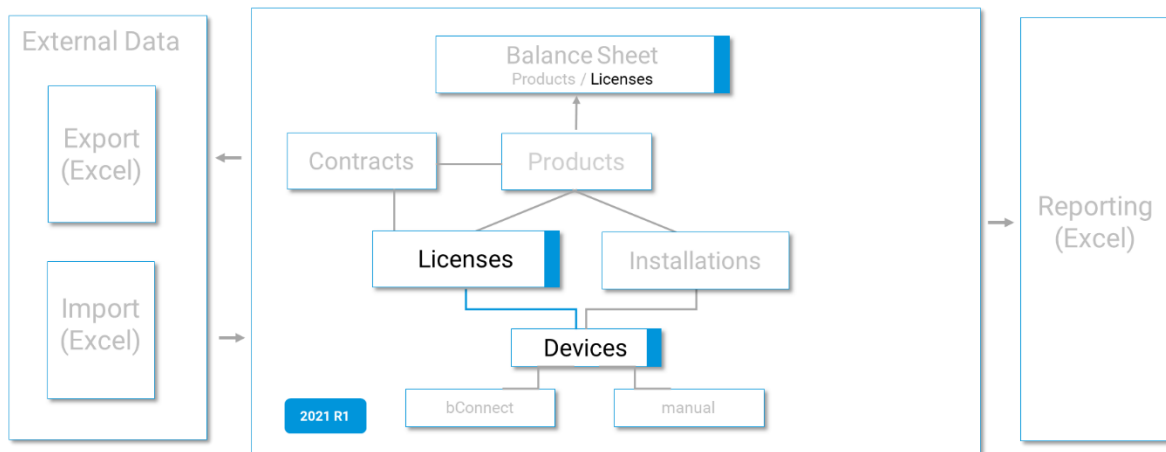


Figure 18 Enhanced License Management in 2021 R1

### 2.6.1.2 Multiple use of licenses via device groups

With Release 2021, the License Management module now includes the option to display device groups for the corresponding product. This replaces the previous mapping of multiple usages and manual adjustment of the totals.

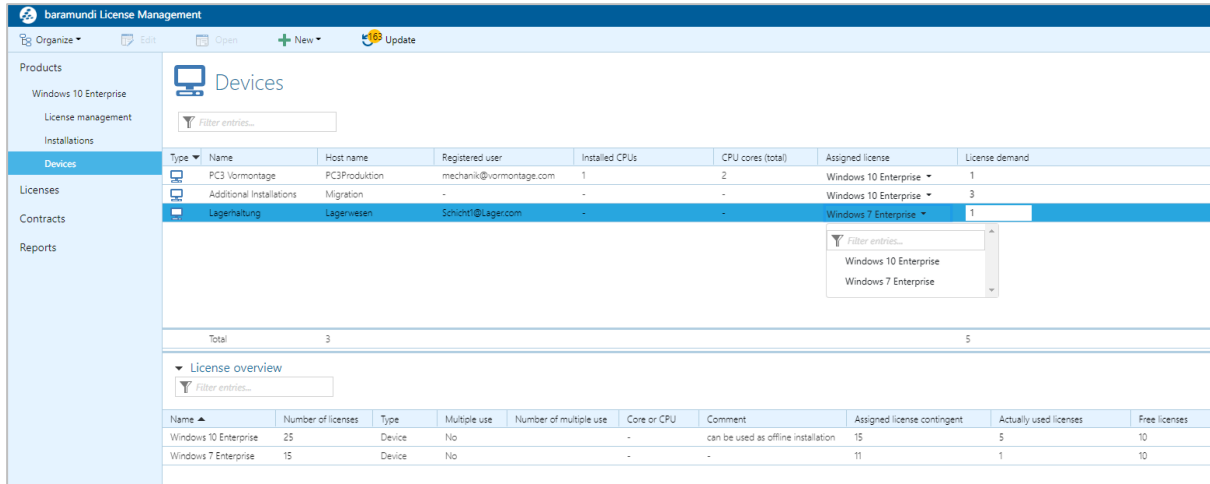
A variety of usage scenarios can now be mapped by creating device groups. If a license enables use for one user on multiple devices, usage can be mapped via a device group for that user.

The license requirement of this group can be entered as 1 according to the usage right, for example. This adjusts the license balance accordingly.

Figure 19 Multiple Usage Licenses through device groups

### 2.6.1.3 Flexible license usage on devices

You can flexibly allocate different licenses for a product. Individual license requirements can be defined per device to map core and CPU license models.



Type	Name	Host name	Registered user	Installed CPUs	CPU cores (total)	Assigned license	License demand
PC3	PC3 Vornontage	PC3Produktion	mechanik@vornontage.com	1	2	Windows 10 Enterprise	1
Additional Installations	Migration	-	-	-	-	Windows 10 Enterprise	3
Lagerhaltung	Lagerwesen	Schicht@Lager.com	-	-	-	Windows 7 Enterprise	1

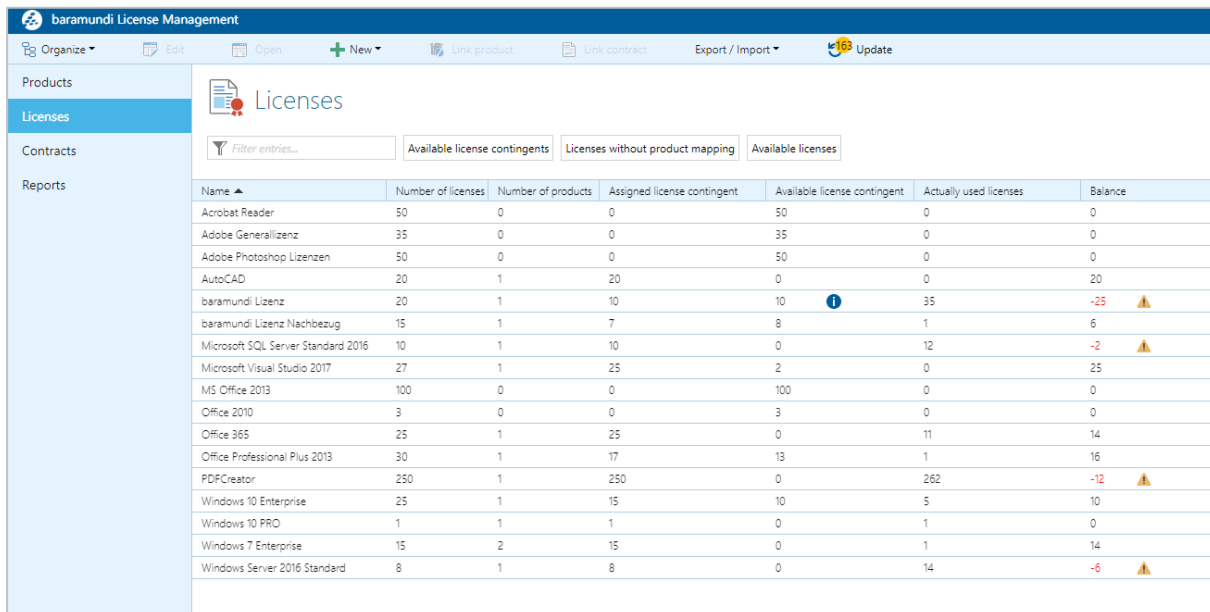
  

Name	Number of licenses	Type	Multiple use	Number of multiple use	Core or CPU	Comment	Assigned license contingent	Actually used licenses	Free licenses
Windows 10 Enterprise	25	Device	No	-	-	can be used as offline installation	15	5	10
Windows 7 Enterprise	15	Device	No	-	-	-	11	1	10

Figure 20 Flexible License Management by device

### 2.6.1.4 License balance

A license balance is now displayed in the Licenses view. Under- and over-coverage can be easily spotted. Appropriate and highly targeted corrections can be made by using display filters.



Name	Number of licenses	Number of products	Assigned license contingent	Available license contingent	Actually used licenses	Balance
Acrobat Reader	50	0	0	50	0	0
Adobe Generalizenz	35	0	0	35	0	0
Adobe Photoshop Lizenzen	50	0	0	50	0	0
AutoCAD	20	1	20	0	0	20
baramundi Lizenz	20	1	10	10	35	-25
baramundi Lizenz Nachbezug	15	1	7	8	1	6
Microsoft SQL Server Standard 2016	10	1	10	0	12	-2
Microsoft Visual Studio 2017	27	1	25	2	0	25
MS Office 2013	100	0	0	100	0	0
Office 2010	3	0	0	3	0	0
Office 365	25	1	25	0	11	14
Office Professional Plus 2013	30	1	17	13	1	16
PDFCreator	250	1	250	0	262	-12
Windows 10 Enterprise	25	1	15	10	5	10
Windows 10 PRO	1	1	1	0	1	0
Windows 7 Enterprise	15	2	15	0	1	14
Windows Server 2016 Standard	8	1	8	0	14	-6

Figure 21 License balance

## 2.6.2 baramundi Network Devices – Network-Map

As part of the further development of the network map (formerly IT map) in Release 2021 R1, a new, optional algorithm can be used as a preview. This uses additional data for topology calculation.

In addition to mapping via the Spanning Tree Protocol (STP), we are extending the representation of the network based on the Forwarding Database (FDB) entries.

Previous multiple representations of connections as well as unmanaged areas are now avoided. In networks where no STP is active, a high-performance network map is now available.

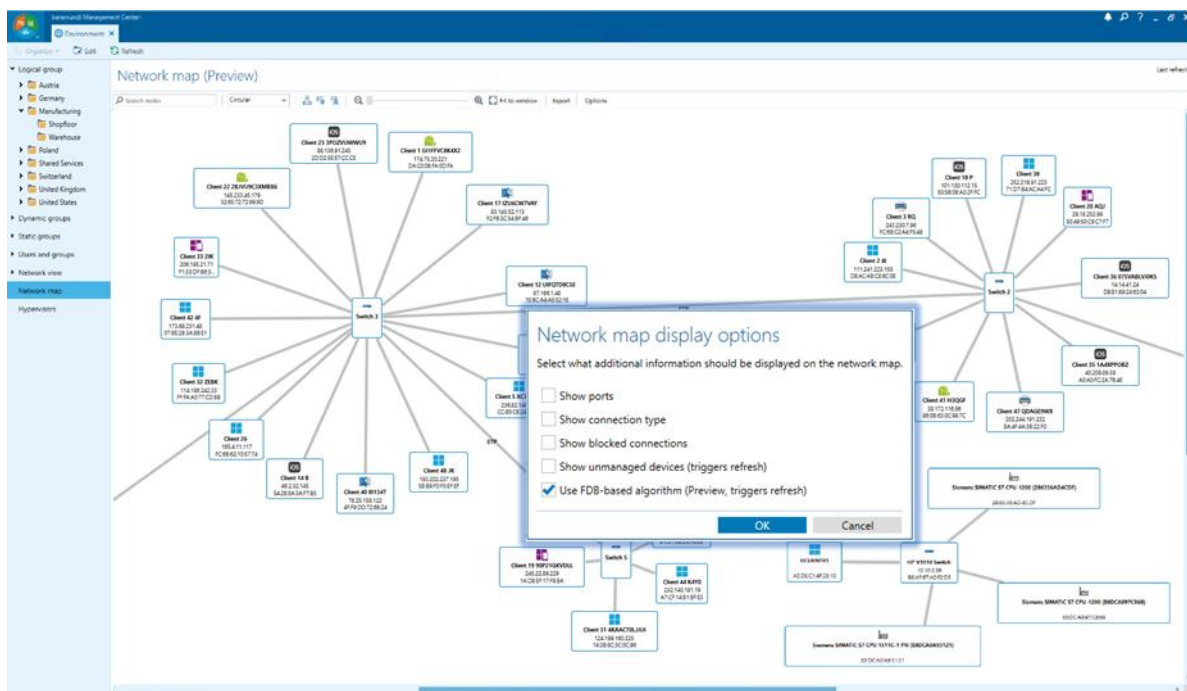
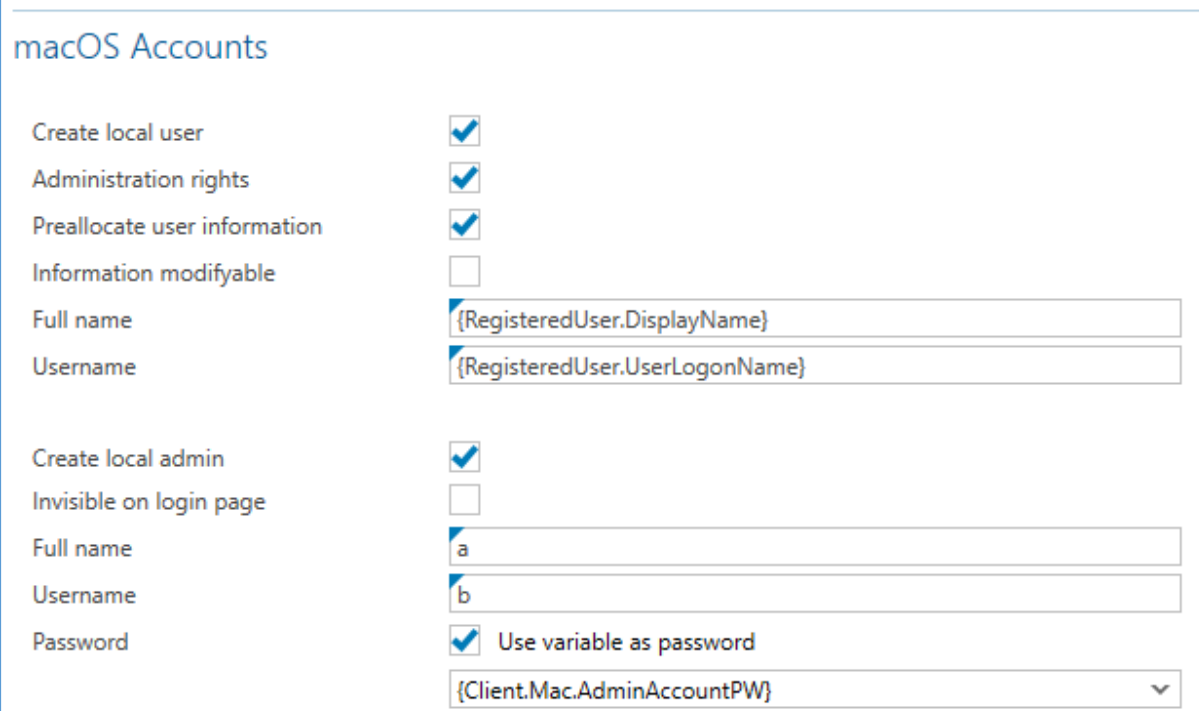


Figure 22 Network map with optional algorithm

## 2.6.3 New features for Apple macOS

### 2.6.3.1 Apple Automated Device Enrollment for macOS

The enrollment of Apple devices with macOS has also been enhanced. The bMS now supports automated enrollment of devices through the Apple Automated Device Enrollment (formerly Device Enrollment Program / DEP), including convenient setup of the administrative account.



The screenshot shows the 'macOS Accounts' configuration window. It contains two sections for creating local users. The first section has checkboxes for 'Create local user', 'Administration rights', 'Preallocate user information', and 'Information modifyable', all of which are checked. Below these are text fields for 'Full name' and 'Username', both containing baramundi variables: '{RegisteredUser.DisplayName}' and '{RegisteredUser.UserLogonName}' respectively. The second section has checkboxes for 'Create local admin' (checked) and 'Invisible on login page' (unchecked). Below these are text fields for 'Full name' (containing 'a') and 'Username' (containing 'b'). The 'Password' field has a checked checkbox for 'Use variable as password' and a dropdown menu showing the variable '{Client.Mac.AdminAccountPW}'.

Figure 23 Configuration of macOS-accounts with baramundi-variables

MacOS devices added in this way are natively included in management and can also be managed via the baramundi gateway, i.e., they can also be managed securely from outside the company network.

### 2.6.3.2 Management of macOS-Apps per VPP

Natively managed macOS devices now also benefit from Apple's Volume Purchase Program. This means that you can now distribute apps from the Apple App Store to managed devices via the bMS.

## 2.6.4 Windows 10 In-place Upgrade via IEM

The job step for in-place updates of Windows 10 endpoints can now also be used via IEM. This means that you can now also conveniently update remote endpoints in users' home offices to the latest Windows 10 release.

## 2.6.5 Active Directory Synchronization

As the basis for essential functions in the baramundi Management Suite, AD-Sync provides a convenient way to synchronize computer and user objects.

The administration dialog been completely revised for intuitive usability in the familiar baramundi Management Center interface. Two further synchronization options have also been integrated:

- **Only synchronize active devices**  
Deactivated computer accounts in AD are synchronized/skipped.
- **Synchronize Windows devices only**  
Synchronize/skip other operating system objects such as macOS.

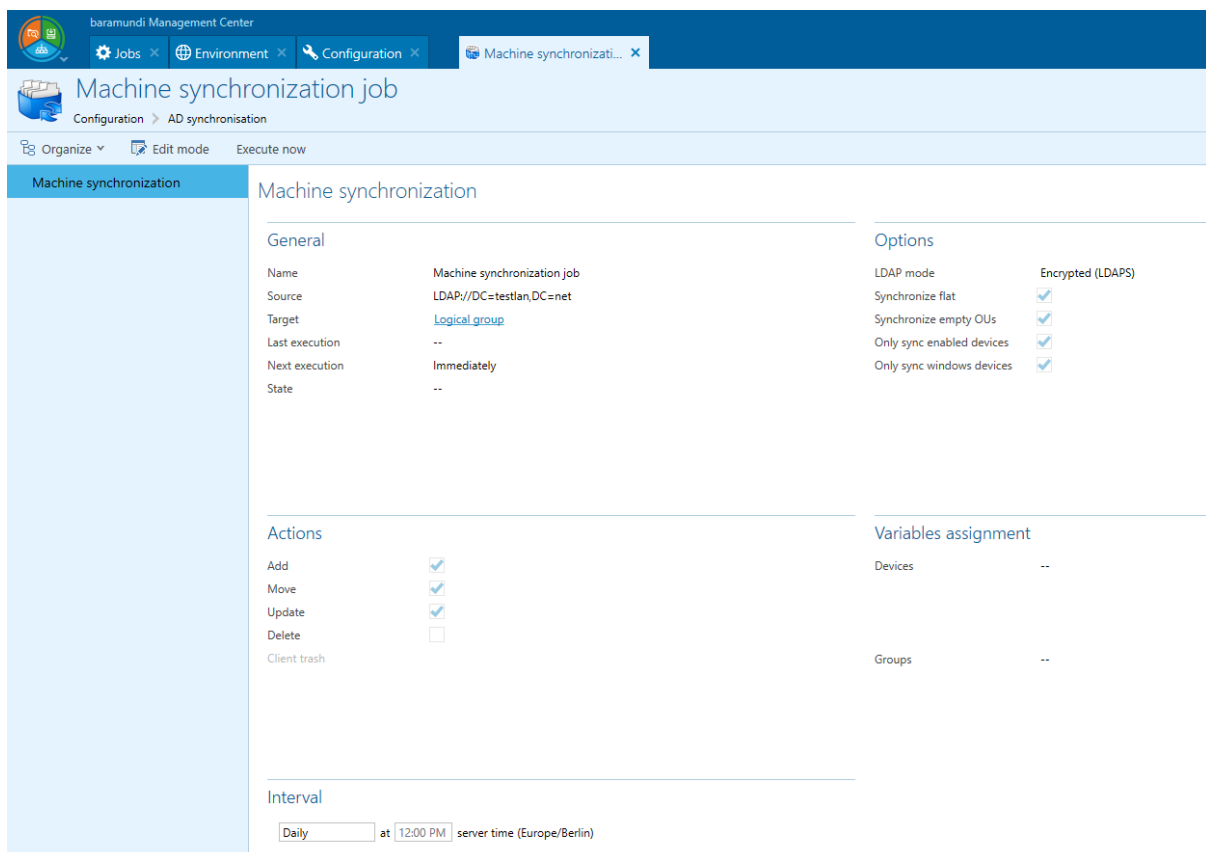


Figure 24 AD-Sync - Machine Synchronization

Microsoft also refined the standard for communication to the domain controller and implemented LDAPS. In version 2021, this communication method is supported by AD-Sync to switch to more secure TLS communication (port 636 as standard). The other communication methods (without signature and signed with channel binding) are still supported.

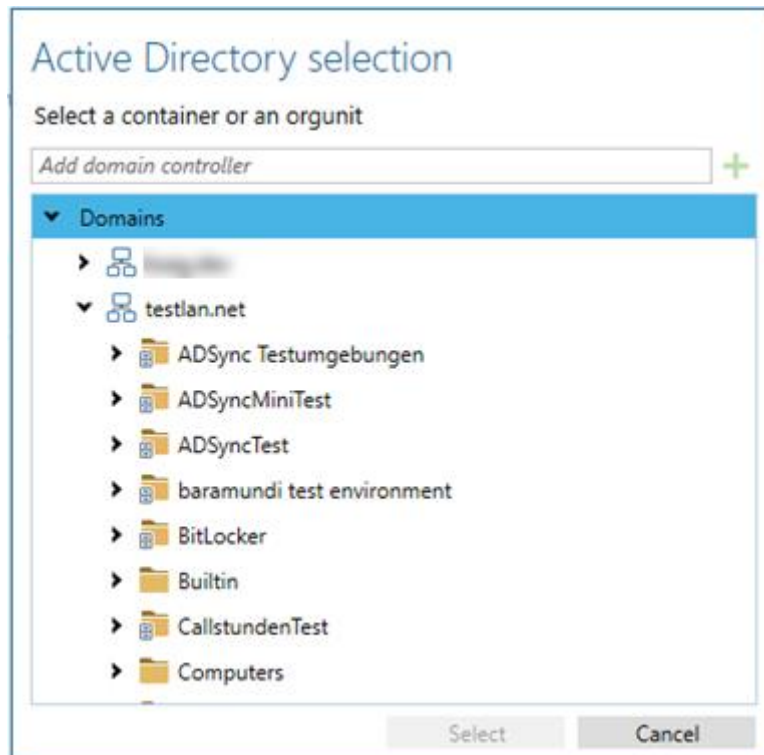


Figure 25 New AD synchronization LDAPS selection dialog

The basic operation of the synchronization jobs has also been optimized in version 2021. This means on one side that a machine and a user synchronization job can run parallel instead of sequentially and on the other hand the synchronization itself gained a dramatic reduction in synchronization runtime.

### 2.6.6 bMC dark mode support (Preview)

In addition to the numerous functional enhancements, there is also a visual innovation. The bMC can now be switched to the eye-friendly Dark Mode. The setting can be made by each user in the "Personal Settings".

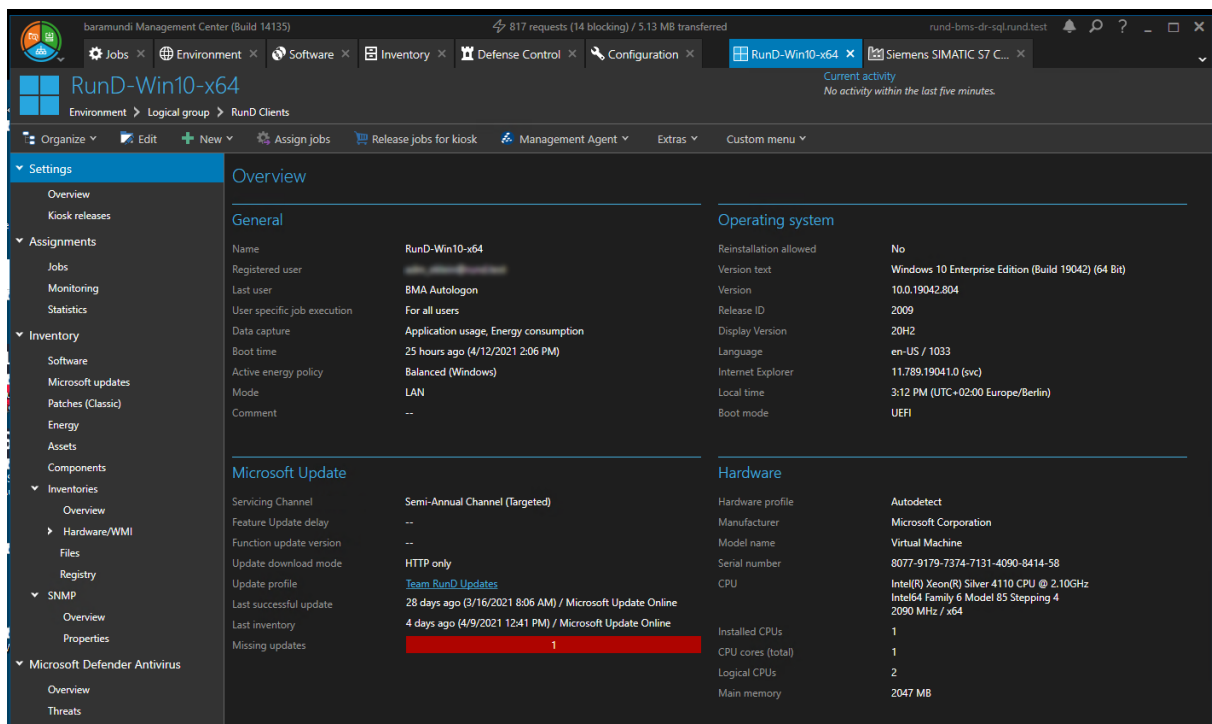


Figure 26 The bMC in Dark Mode

We look forward to your feedback to further enhance this feature.

## 2.6.7 Bitlocker Network Unlock

The functionality of 2020 R2 to use a baramundi relay server as a Bitlocker unlock server has already found its way into many environments. Feedback on this function reached us and was implemented with this version. It is now possible to configure a timeout in hours for these relay servers, in which the relay servers continue to unlock Windows endpoints to bypass the PIN query despite a master server being unavailable.

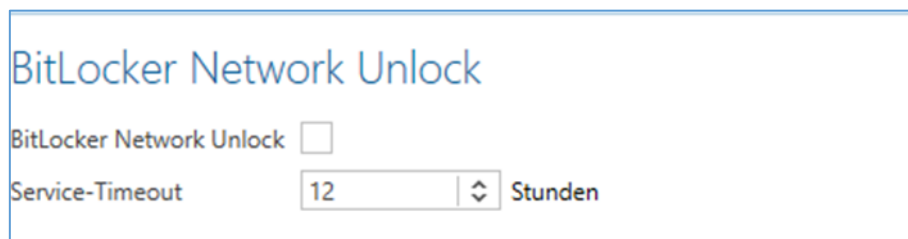


Figure 27 – New Service Timeout for Bitlocker Network Unlock



## 2.7 Product Improvements in Detail

### 2.7.1 Windows Agent (bMA)

- Bugfix: Files larger than 5GB often cannot be transferred via bBT.

### 2.7.2 Management Center (bMC)

- The calculation of the IP networks can now be done via the CIDR standard. To do this, you must switch to this improved procedure once in maintenance mode and then close the bMC. The new procedure leads in some constallations to the fact that the IP networks are not mapped as before. The IP networks must be corrected in these cases.
- The IT map was largely revised and renamed to Network map.
- Under Personal settings - Notifications the Download job notification and the DB maintenance job notification can be configured.
- Under Environment - End Device - Overview, the Primary subnet mask is displayed in addition to the IP.
- The Primary subnet mask can be used in Dynamic group (Universal)
- Under Environment the same columns as for Dynamic Groups (Universal) are available in all device lists. Note: Due to this change of the device lists, the relevant columns are reset to default when the bMC is started for the first time.
- Under Environment - End Device - Overview, BitLocker Network Unlock Status, BitLocker Startup PIN enabled and BitLocker Startup USB Key enabled are additionally displayed under System security.
- Patches has been renamed to Patches (Classic). The jobstep Deploy Microsoft patches has been renamed to Deploy Microsoft patches (classic).
- Under Configuration - Security Management - Security profile, a new right for Defense Control is available for use in a security profile.

- For a software, the `Settings - Overview` page can be exported to an Excel file.
- Under `Personal Settings`, `Themes (Experimental)` are available. This allows the BMC to be set to `Dark` or `Classic`.
- For new databases, the sample asset types are displayed in English.
- Crystals Reports Runtime version 13.0.29 (SP29) is used as the report runtime.
- On the Windows endpoint, when setting the Windows domain, the drop-down menu displays the list of configured domains.
- After a successful BDx import, a corresponding message is displayed.
- Bugfix: In certain constellations, withdrawing kiosk shares from a group or device creates orphaned kiosk shares that can no longer be deleted.
- Bugfix: Job assignment via the `Software - Managed Software - Installed on` page is very sluggish in certain constellations.
- Bugfix: The name and comment of the personal Backup default templates is also displayed in German on English systems.
- Bugfix: The Jobtarget progress bar is not reset when a Jobtarget is restarted.
- Bugfix: When deactivating the revision log, the dialog for changing the password is displayed
- Bugfix: When scrolling fast in the `Extensions - Mobile devices profiles`, wrong icons are displayed.
- Bugfix: If the name of a software, which is already used in job steps, is changed, the name in the detail view of the job steps is not updated.
- Bugfix: Settings for Argus Cloud Connectors are partially reset when changing the bConnect port.

### 2.7.3 Update Management

- The jobstep `Deploy Microsoft patches with update source baramundi Patch Management` has been renamed to `Deploy Microsoft patches (classic)`.

- The jobstep `Deploy Microsoft patches with update source WSUS, Windows Update Online or Microsoft Update Online` has been renamed to `deploy Microsoft Updates`.
- Note: To get consistent `Inventory - Microsoft updates` views it is recommended to adjust jobs with steps `Deploy Microsoft updates`. At the last patch step, the checkbox `Perform final update inventory` should be set or a dedicated step `Inventory Microsoft updates` should be included.
- For detailed control of update rollouts, the configuration of update profiles is possible.
- Update profiles can be assigned to one or more endpoints and are visible on the client and client lists.
- At the `Manage Microsoft Update - Deploy Microsoft updates` step, an `Update delay in day(s)` can be set.
- New option at the patch step: `Do not ignore 'Defer Quality Updates' (GPO)`
- Bugfix: In certain situations, already replaced patches are downloaded although they are not required.

## 2.7.4 OS-Install

- The jobstep `Deploy operating system - In-Place Upgrade` now supports baramundi Background Transfer and can be executed on devices in internet mode.
- Improved logging at PXE Boot via set DHCP option / boot loader.
- When creating an OS install job with the `Operating system from image file`, the additional boot environments `Autodetect` and `Autodetect x86` are now available.
- Workgroup clients join the workgroup specified in the bMC.
- For the hardware profile, an example path is displayed in the path for manual driver assignment.
- The options `Boot prompt duration` and `Unknown clients` have been removed from the PXE server active box because they are used independently of the PXE server.

- Bugfix: The description of blmaging.exe shows a wrong syntax at `Example`.
- Bugfix: If in a hardware profile the main memory is specified with more than 16GB, a corresponding message appears and saving is not possible.
- Bugfix: If in a hardware profile the processor clock is specified with more than 4GHz, a corresponding message appears and saving is not possible.
- Bugfix: The UEFI boot order is not set correctly in certain constellations.
- Bugfix: The installation user of the domain specified at the logical group of the client is used. As of Release 2021, the installation user of the domain specified at the client is used.

### 2.7.5 Mobile Devices

- When the Apple profile signing certificate expiration is approaching, a BMC notification is displayed.
- Improved delivery of push notifications for Android devices in standby mode.
- The `Assign to new devices` job option can be set only by users who have the `Job:Edit auto assign` right.
- When unrolling a device, a warning is displayed if necessary settings are missing under `Configuration - Mobile devices`.
- Bugfix: The `Manage Dedicated Device - Android Enterprise` job step cannot distribute a `Layout template` if no `List of executable apps` is set.
- Under `Configuration - Mobile Devices - General - E-Mail` the `SMTP server Port` is set to 465 when activating `SSL encryption`, if the port has not yet been configured manually.
- In the job step `Manage Dedicated Device - iOS/iPadOS` imported `*.ipa` Apps can now also be selected.
- Bugfix: App Permissions are displayed for local apps in the BMC if the same app was also imported from the App Store.

### 2.7.6 bServer – AD-Synchronisation

- The `User synchronization job` and `Machine synchronization job` have been fundamentally revised.
- `InetOrgPerson` objects are supported.
- Group memberships are now resolved across domain boundaries when possible.
- The LDAPS communication mode is supported.
- The sync job is always rescheduled even in the event of an error. The specification of special error codes is no longer required.
- New options: `Only sync enabled devices` and `Only sync windows devices`.
- In AD variable mapping, the baramundi variable is set to its default value if in AD the attribute has the value `<not set>`.
- Note: Users/machines/groups/folders containing ASCII control characters or Unicode characters will be ignored.

### 2.7.7 Automation Studio (bDS)

- An html hyperlink in a `Show Message` window now opens the window in the active user's default browser.
- The progress window can be resized manually.
- Bugfix: The assignment of rights for printers is partly not possible.

### 2.7.8 Argus-Connect

- Additional endpoint fields are transferred to the Argus Cockpit.

### 2.7.9 Gateway

- The gateway setup changes a system setting (Windows registry) to disable sending the server information in the http response header for all http.sys based interfaces.

### 2.7.10 bConnect

- UpdateGroups can be read and written for Microsoft Update Management.
- The UpdateGroups can be read or written for a Windows endpoint.
- Bugfix: If endpoints of a dynamic group are read out, the value "Lastboot" is wrong.

### 2.7.11 baraDIP

- When baraDIP is started, an event log entry of the form `The system cannot find the file specified, No installed ConfigArgs for the service "baraDIPhttpd", using Apache defaults is logged`
- Bugfix: In rare situations the DipServers do not receive further synchronization jobs from the bServer. The synchronization of the DipServers then takes place only after a restart of the bServer service.

### 2.7.12 Defense Control

- The Bitlocker network unlock can be configured per PXE relay. In addition, a "Network Unlock Relay Server Timeout" can be set.

### 2.7.13 License Management

- The configuration options `Additional installations` (not managed with baramundi) and `Manual adjustment` (e.g. +10 or -10) under `Products - Product - Installations` have been removed and automatically migrated to fictitious devices named `Additional Installations` or `Installation Correction`.

## 3 Release 2020 R2 U1

### 3.1 Product Improvements in Detail

#### 3.1.1 General

- The log4net framework used has been updated. CVE-2018-1285 is no longer detected as a false positive.
- Bugfix: The table of restricted operating systems could be misinterpreted. The table has been simplified and a note has been included.
- Bugfix: The database schema update takes a long time to convert the data for DiskInventory and Bitlocker.

#### 3.1.2 Server (bServer)

- The bServer now reliably deletes its generated entries under `bMC-Configuration Lock Manager`.
- In case of an unexpected license break, e.g. a detected hardware change, server operation is still possible without restriction for a few days, even if an Eval license has been activated before.
- Bugfix: Numerous SQL database errors can occur during job execution. In this case the status text of the affected job instances contains the text `Database error` and in the details `deadlock situation` is visible in the text. (For this the FixIt\_Moc for 2020 R2 was provided).

#### 3.1.3 Windows Agent (bMA)

- Bugfix: When deploying using bBT, the message `File list: Invalid XML (not well-formed)` appears sporadically.
- Bugfix: The bDS action Unpack Archive sometimes creates files with wrong names for files with umlauts.
- Bugfix: After the automatic bMA update the setup files of the agent remain in the folder `C:\AppData\Roaming\baramundi software AG`.

### 3.1.4 Management Center (bMC)

- Bugfix: Some special characters like "&" lead to a bMC error in the `Personal Settings` dialog.
- Bugfix: The dialog `Search Folder` in the OS Wizard does not use the path entered at `Source`, but starts in the folder of the current user.
- Bugfix: The tools `baretail` and `baregrep` under `\Management Server\Shared\Tools` can no longer be started.
- Bugfix: The `Double Driver` tool is no longer included in the delivery.

### 3.1.5 Argus-Connect

- Bugfix: The change of the bConnect port is not transferred to the connectors.

### 3.1.6 Mobile Devices

- Bugfix: Apple Push via a stored proxy is not possible.
- Bugfix: When trying to configure the app `Zebra OEMConfig` powered by MX from the Android Enterprise Store the bMC crashes with a `Null Reference Exception`.

### 3.1.7 Update Management (Patch Management)

- Bugfix: Job steps `Deploy Microsoft patches` with update source `WSUS` or `Online` may run into the error `The string was not recognized as a valid DateTime`.
- Bugfix: Windows Update Service is not automatically activated and deactivated again when performing the `Inventory Microsoft updates` step.

### 3.1.8 OT Edition

- Bugfix: During SNMP network scan SIMATIC devices are not completely migrated to IC Devices.



## 4 Release 2020 R2

### 4.1 iOS "User Enrollment"

At the 2019 WWDC, Apple presented its enhanced concept for data separation, extending protections designed for business data to user private data. This means that user data privacy needs can be met system-wide to significantly increase user acceptance and trust of IT device management while giving IT admins robust MDM controls.

Apple calls this management method – available in iOS 13 and later - "User Enrollment". Here, the user independently includes his mobile device in the IT management framework. They can also remove it from management at any time. If they do, company data is automatically removed from their device.

#### A new management method

The previous mechanisms for managing iOS devices were designed to meet the needs of administrators and enable extensive control of device settings. For example, an administrator can deactivate the camera system-wide, which also makes private apps that need camera access unusable. In supervised mode, the App Store can be completely blocked, or individual apps can be deactivated. Access to in-depth system information is also possible, which makes it possible to identify and trace the device.

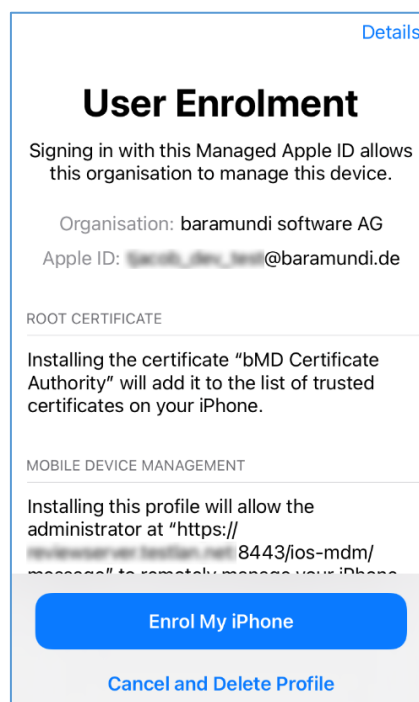


Figure 28 - Dialog during user enrollment

This is where the concept of “User Enrollment” comes in. Instead of fully controlling the device, management now takes place in a defined area on the device. The user can access company data to work productively without the usual restrictions in their private apps and data. User data and self-installed apps are hidden from the administrator.

## The difference

The biggest difference between the previous administration methods and the new "User Enrollment" lies in the privileges of the EMM system on the device.

The administrator no longer has access to data used to identify the device (serial number, UDID, IMEI or MAC address). This is particularly useful for BYOD scenarios. Instead, there is now a special ID that is only assigned to the device management profile. A new ID is generated for each new enrollment.

Separation is even more important for apps. Previously, the administrator could see both company apps and private apps installed by the user. User-installed apps are no longer visible to the administrator in "User Enrollment" to protect user privacy.

There also is greater separation for device configurations and direct management action. It is no longer possible to wipe the entire device remotely – just the company profile together with the encrypted storage area created for it and the contained company data.

Restrictions

Common
iOS/iPadOS
Android
Android Enterprise
Windows Mobile

☒ Use iOS/iPadOS specific settings

☐ Disallow screen capture
☐ Force code on initial airplay connection
☐ Force encryption of backups
☐ Disallow submitting diagnostic reports automatically
☐ Disallow usage of unmanaged documents in managed targets
☐ Disallow usage of managed documents in unmanaged targets
☐ Allow managed targets to read unmanaged contacts
☒ Force Airdrop as an unmanaged drop target
☐ Disallow iCloud sync for managed apps
☐ Disallow Siri
☐ Disallow Siri on lockscreen
☐ Disallow NotificationCenter on lock screen
☐ Disallow ControlCenter on lock screen
☐ Disallow TodayView on lock screen
☐ Force Safari fraud warnings

☒ Use device enrollment specific settings

☐ Disallow installation of configuration profiles \*
☐ Disallow account modifications \*
☐ Disallow device name modification \*
☐ Disallow passcode settings modification \*
☐ Disallow camera \*
☐ Disallow AirPrint \*
☐ Disable AirDrop \*
☐ Force limited ad tracking
☐ Disallow QuickPath keyboard feature \*
☐ Force WiFi connection \*
☐ Disallow Touch ID and Face ID
☐ Disallow erase content and settings in the UI \*
☐ Disallow requesting passwords from nearby devices \*
☐ Disallow sharing passwords with Airdrop \*
☐ Disallow global background fetch activity when roaming
☐ Disallow modifications to the eSIM setting \*
☐ Disallow modifications on data plan \*
☐ Disallow app cellular data modification \*
☐ Force delayed software updates
 Days until forced software update \*
 30
☐ Disallow Bluetooth settings \*

Figure 29 - Profile differences in User Enrollment and Device Enrollment

Probably the most important difference is in the type of data separation and transparency for users and apps. With the data separation in "Device Enrollment" - whether manually or via DEP - company content is *marked* as business but is in the same memory area as private data. With "User Enrollment", another encrypted storage area is created on the device, which exclusively contains business data and is under the control of the EMM solution.

## Managed Apple ID

Since iOS "User Enrollment" provides strict separation between private and business use, it relies on a separate ID for the user - the so-called "Managed Apple ID". This ID is used to license apps from the App Store.

Managed Apple IDs can be created by the administrator in the Apple Business Manager<sup>9</sup>. The Managed Apple ID is then assigned to the device within the baramundi Management Suite.

<sup>9</sup> <https://business.apple.com/>

## 4.2 Automatic updates of apps on mobile platforms

With this release, the most popular customer request in the “Mobile Devices” category in the feedback portal now finds its way into the bMS:

### 4.2.1 Automatic update of VPP apps on iOS

With this new function, administrators can ensure that devices always have the latest - and hopefully most secure - version of an app installed. At the same time, mobile data allowances are spared and users are not unnecessarily disturbed.

The 2020 R2 release introduces a new job step for that purpose that can be carried out regularly on managed Apple devices as a job. The process is based on our established MSW logic: First, an inventory of the installed apps is carried out to determine if a newer version of the app is available in the App Store. If a newer version is found, the job step for installing the new version is automatically added to the job. This ensures that each device only downloads the updated versions of apps that were already installed.

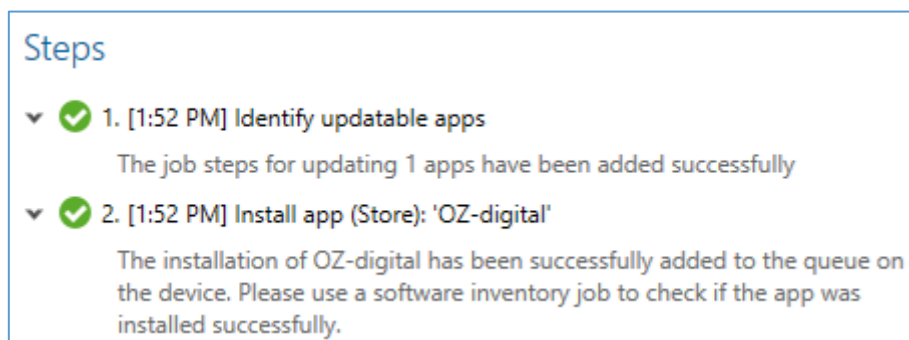


Figure 30 - Overview of the job steps for an automatic update

Of course, the availability of new versions is not only determined as part of the new job step. This function has also been added to the existing app inventory. Immediately after an inventory, the administrator can find out whether an outdated version of an app is installed or whether updates are available.

This state of the device - whether app updates are available or not - can also be filtered using Universal Dynamic Group (UDG) filters.

### 4.2.2 Configuration of the app update policy for Android

Apps should also be kept up to date on Android Enterprise. Unfortunately, that platform does not have a specific automatic update function. However, the update behavior can be configured.

This configuration is now also possible via the bMS using a configuration profile.

System update policy	Automatically in daily maintenance window ▾
Time window for the system update	3:00 AM ▾ - 5:00 AM ▾

Figure 31 - Setting update behavior in the profile

The configuration enables the specification of how (left to the user, only if connected to Wi-Fi, etc.) and when (time window) an update should take place.

## 4.3 Inventory of Microsoft Updates

Starting with the bMS 2020 R2, patch management will be completely revised. The first step was to provide a new inventory of the missing and installed updates. A new job step has been introduced for this purpose. Within this job step, the new functions are extended with the following releases.

### 4.3.1 Update selection

When selecting the new job step, the action "Inventory Microsoft updates" can now be selected.

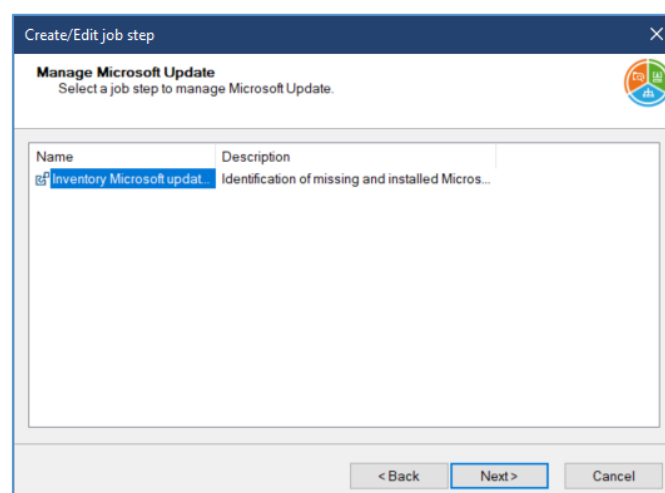


Figure 32 – New job step for the identification of missing and installed updates

You can choose between Microsoft's own online service "Microsoft Online" and - if available and configured in your own network - a WSUS.

After this job has been finished on an endpoint, the results are available in two views.

### 4.3.2 Endpoint Overview

A new information field appears on the overview page of the Windows endpoint. This field contains all relevant data on the Microsoft Updates for the endpoint. In addition to the servicing channel, the missing updates are displayed here. A special highlight is the graphical display of the number of missing updates grouped by criticality, showing at a glance if action is needed.

Microsoft Update	
Servicing Channel	Semi-Annual Channel (Targeted)
Feature Update delay	--
Function update version	--
Update download mode	HTTP only
Last successful update	--
Last inventory	1 minute ago (4:25 PM) / Microsoft Online
Missing updates	14

Figure 33 - Information about Microsoft updates in the overview page

If no missing updates are found, the bar appears green.

### 4.3.3 List of missing and installed updates

In order to get a detailed overview of endpoint updates, the administrator can use the new view "Microsoft Updates" in the endpoint inventories. All relevant information about missing and installed updates are shown. Updates are initially sorted by priority: missing updates first then the installed updates. Secondary sorting is by Microsoft Security Response Center (MSRC) severity level then by date of publication. This ensures that the most important updates are visible at a glance.

Sorting can be changed by clicking on the column headers. Filters for state, classification and text-based are also available.

Microsoft updates					
<div> <span>Filter entries</span> <span>All classifications</span> </div>					
	Title	MSRC severity	Published	Classification	Products
1	Update for Microsoft Defender Antivirus antimalware...		1 month ago	Definition Updates	Microsoft Defender Antivir...
2	Update for Windows Defender Antivirus antimalware...		7 months ago	Updates	Microsoft Defender Antivir...
3	Update for Windows Defender Antivirus antimalware...		7 months ago	Updates	Microsoft Defender Antivir...
4	Microsoft Silverlight (KB4481252)		2 years ago	Feature Packs	Silverlight
5	Microsoft Silverlight (KB4023307)		3 years ago	Feature Packs	Silverlight
6	Microsoft Silverlight (KB4017094)		3 years ago	Feature Packs	Silverlight
7	Microsoft Silverlight (KB4013867)		4 years ago	Feature Packs	Silverlight
8	Microsoft Silverlight (KB3193713)		4 years ago	Feature Packs	Silverlight
9	Microsoft Silverlight (KB3182373)		4 years ago	Feature Packs	Silverlight
10	Microsoft Silverlight (KB3162593)		4 years ago	Feature Packs	Silverlight
11	Microsoft Silverlight (KB3126036)		5 years ago	Feature Packs	Silverlight
12	Microsoft Silverlight (KB3106614)		5 years ago	Feature Packs	Silverlight
13	Microsoft Silverlight (KB3080333)		5 years ago	Feature Packs	Silverlight
14	Microsoft Silverlight (KB3056819)		5 years ago	Feature Packs	Silverlight
15	2020-06 Security Update for Adobe Flash Player for...	Critical	4 months ago	Security Updates	Windows 10, version 1902
16	MSXML 6.0 RTM Security Update (925673)	Critical	8 years ago	Security Updates	SQL Server Feature Pack...
17	2020-09 Cumulative Update for .NET Framework 3.5...	Moderate	20 days ago	Security Updates	Windows 10, version 1902
18	Security Intelligence Update for Microsoft Defender...		14 hours ago	Definition Updates	Microsoft Defender Antivir...
19	Windows Malicious Software Removal Tool x64 - v5...		20 days ago	Update Rollups	Windows 10; Windows 10
20	2020-09 Cumulative Update for Windows 10 Version...		20 days ago	Security Updates	

### Update for Microsoft Defender Antivir...

Classification: Definition Updates

Products: Microsoft Defender Antivirus

Published: 1 month ago (8/28/2020)

MSRC severity: --

CVE IDs: --

Type: Software

KB article numbers: 4052623

Security Bulletin IDs: --

Description: This package will update Microsoft Defender Antivirus antimalware platform's components on the user machine.

Update ID: 0CCTABA2-AFBE-4A75-9A89-044155F18682

Revision number: 200

References

Support URL: <https://go.microsoft.com/fwlink/?linkid=862339>

Further information: <https://support.microsoft.com/en-us/help/4052623/...>

Figure 34 - List of missing updates

Additional information can be displayed by clicking on an update. This includes the KB number, affected products, the update GUID, and other references to CVE entries (if available) and to Microsoft's explanations.

#### 4.3.4 Use in Universal Dynamic Groups

The number of missing updates on the overview page described above can also be used as a filter for Universal Dynamic Groups (UDGs). For example, queries can now be generated taking into account the number of missing security updates and synchronized with the Argus Cockpit.

### Conditions

Fulfills: all of the conditions

Platform
=
Windows

Missing security updates
>
0

+

Figure 35 - New criteria for UDGs

## 4.4 Automatic BitLocker unlocking on secure networks

With the Defense Control module, it is possible to securely encrypt the volumes of a Windows endpoint with BitLocker. For extended protection, you can also require a PIN to be entered when the computer is started. This additional protection ensures that the computer can only be started up by an authorized person.

### 4.4.1 Need for protection vs. convenience

Since the PIN has to be entered locally on the computer at startup, this protective mechanism may make it impossible to maintain the endpoint remotely. If the endpoint is switched off, the management solution cannot wake it up or start it up without someone at the computer to enter the correct PIN.

Since this discrepancy between protection and convenience is impractical - especially with many more remote machines in distributed locations - the bMS now includes the ability to automatically unlock PIN-protected endpoints.

### 4.4.2 Functionality

Network unlocking requires that the endpoint is able to determine whether it is on a secure network. To do this, some information is retrieved on the network at startup. This information is provided by both the baramundi Management Server and the baramundi PXE relays. To ensure that only an authorized bMS can unlock an endpoint, a trust relationship must first be established. This trust is based on a certificate as a kind of ID card. As a result, the endpoint unlocks only if it can reach a server that has the trusted certificate.

### 4.4.3 Activate network unlocking

Since automatic unlocking interfere in the company's security program, it must first be explicitly enabled or activated by the administrator in the bMS. This is done in the settings of the *baramundi Defense Control* module .

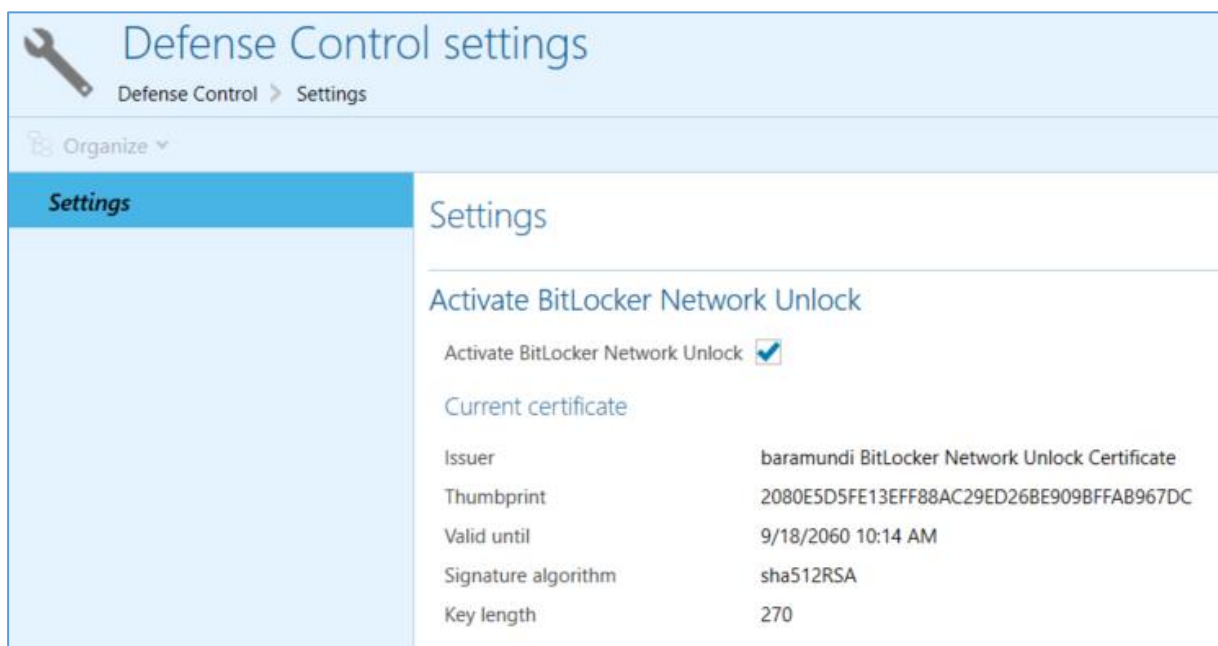


Figure 36 - Network unlock configuration



Activating the function ensures that the bMS carries out the required configuration on the bMS infrastructure. This includes generating the required certificate and providing the information for the connected PXE relays - after all, the unlocking process should also work at remote or field offices when needed.

#### 4.4.4 Authorization of the endpoints

Depending on the security program, there may be endpoints that should be excluded from automatic unlocking. Therefore, an endpoint must be explicitly authorized to automatically unlock itself in a secure network. This is done using the well-known job step "Manage BitLocker", which has been expanded to include the "Turn on BitLocker Network Unlock" action.

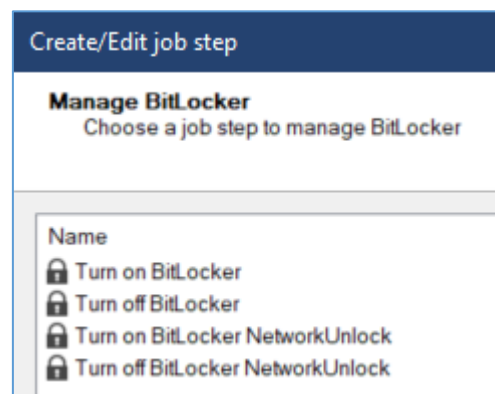


Figure 37 - Actions of the "Manage BitLocker " job step

When this job step is performed, the required certificate is installed, and the endpoint is configured correctly. Network unlocking can also be deactivated by a job step.

### 4.5 baramundi Argus Cockpit

In 2020 R2 version, the baramundi Argus Cockpit (bAC) has been expanded with features for synchronizing and displaying relevant data from the connected IT environments. In addition, system performance - especially for larger IT environments - has been optimized and the UI has been adapted.

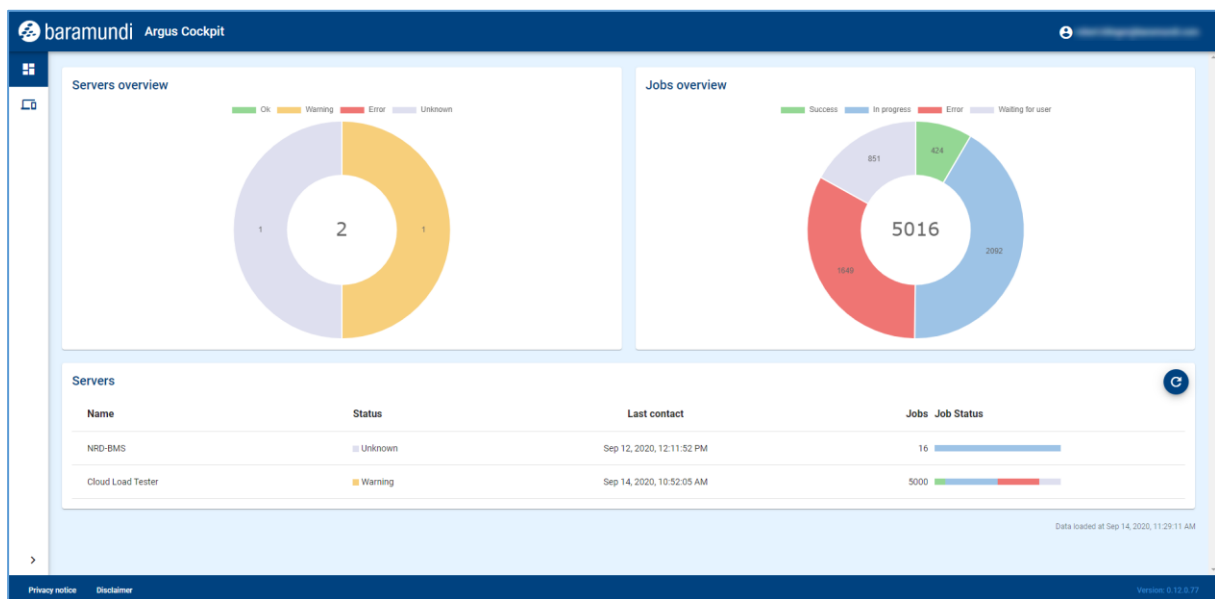


Figure 38 – Display of status data in bAC

### 4.5.1 Selection of relevant IT data

The baramundi Argus Cockpit keeps IT administrators informed of the current status of the connected IT environments anytime, anywhere, to rapidly identify IT problems and initiate actions locally. But every company defines the "health status" of its IT environment differently. For example, in company A the environment is healthy when all PCs are patched, but for company B, the environment is healthy when all PCs have the current version of Windows 10 installed and BitLocker is activated. Obviously, the data monitored and displayed differs for each.

Beginning with 2020 R2, up to 10 Universal Dynamic Groups (UDGs) with data selections for different status displays can be synchronized with the Argus Cockpit. Each IT administrator can choose the specific status data they want to monitor and synchronize with the bAC.

### 4.5.2 Synchronize Universal Dynamic Groups

Extensions have been added to the bMC to synchronize UDGs with the baramundi Argus Cockpit. Up to 10 UDGs can be activated in the menu for synchronization.

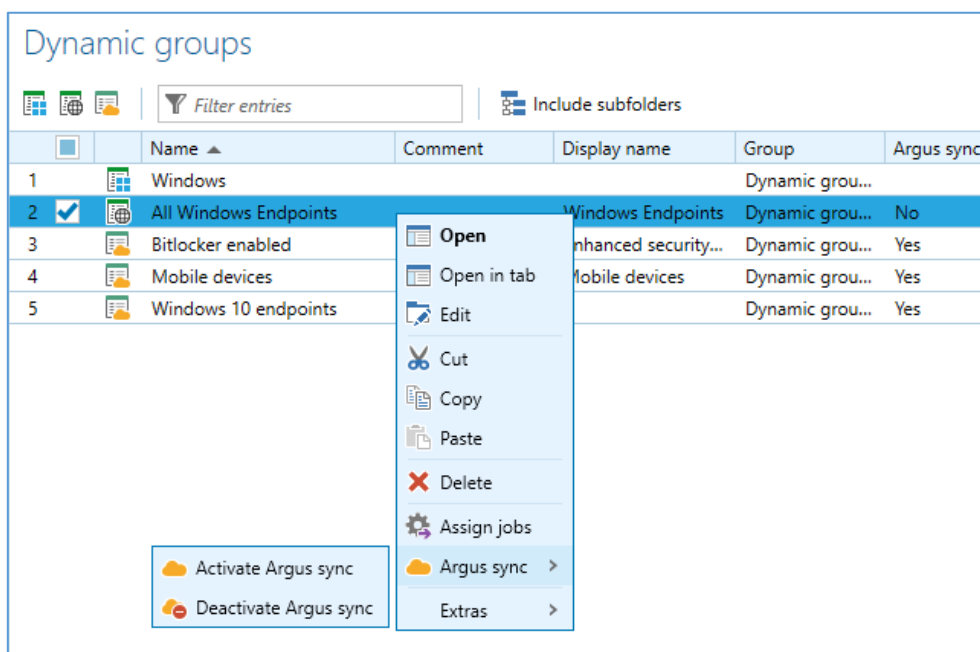


Figure 39 – Activating UDG synchronization

To improve clarity, synchronized UDGs are displayed with a different symbol in the bMC. Entering a UDG display name also helps to identify the specific UDG displayed in the Argus Cockpit.

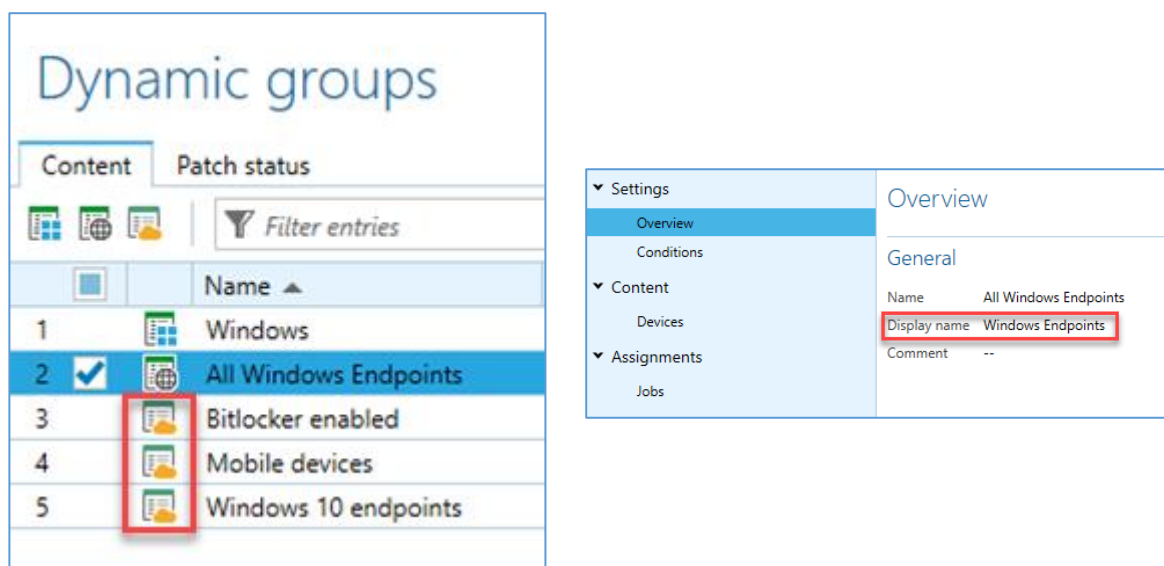


Figure 40 - Identifying a synchronized UDG

It may be important that not every bMC user is allowed to enable this synchronization. A new special right has been added to comply with data protection regulations and policies.

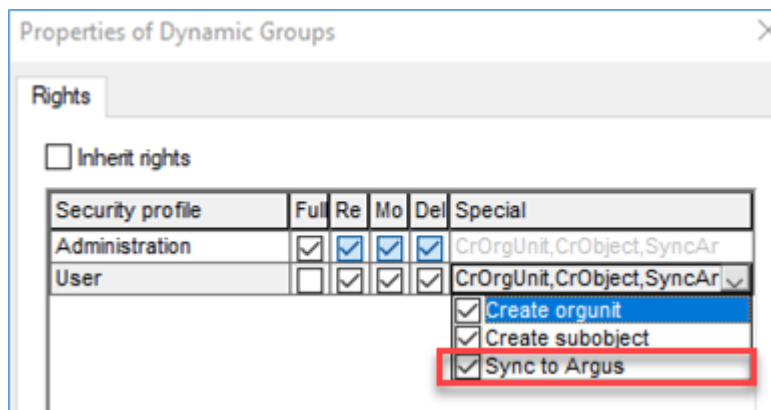


Figure 15 - New special right for synchronization for the Argus Cockpit

### 4.5.3 Displaying UDGs in the Argus Cockpit

Defining and synchronizing UDGs makes it possible to display relevant data in the Argus Cockpit. The UDGs created are now clearly displayed in the baramundi Argus Cockpit. Every Argus user who has access to the corresponding baramundi Management Server can see the associated synchronized UDGs.

The IT administrator can, for example, delegate monitoring and control of synchronized data to another employee while the IT administrator takes care of other important operational tasks.

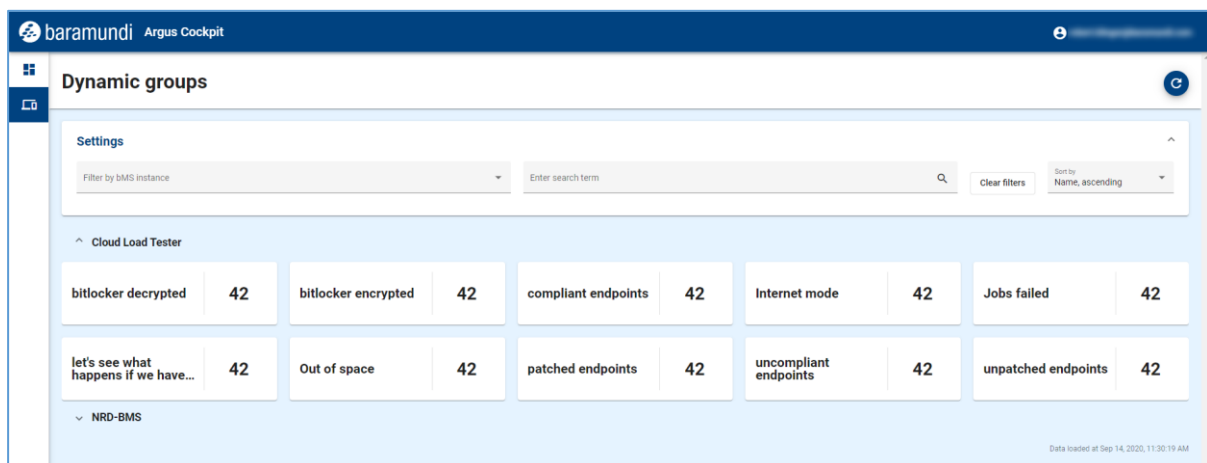


Figure 41 - Clear presentation of UDG data from the baramundi Management Server

The “Dynamic groups” dashboard shows the IT admin all synchronized UDGs on each baramundi Management Server and the data reported at a glance. Filters and sorting options can show the desired data quickly.

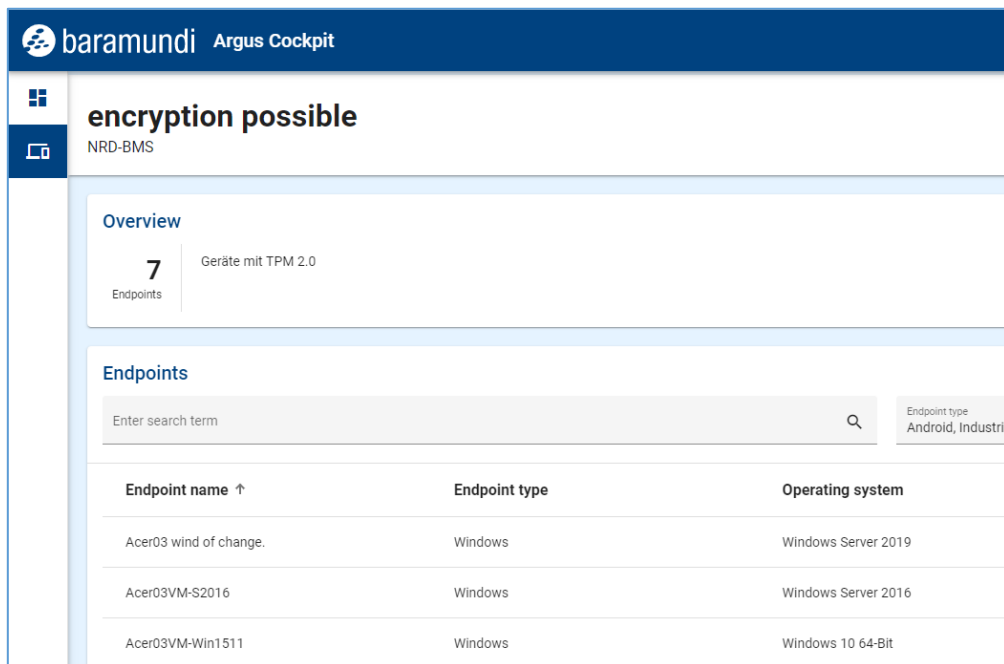


Figure 42 - Detailed view of a UDG

Argus Cockpit users also can view the details of a specific UDG. All devices that meet the defined UDG criteria are displayed, with filtering and sorting options available to show the most important and relevant data first.

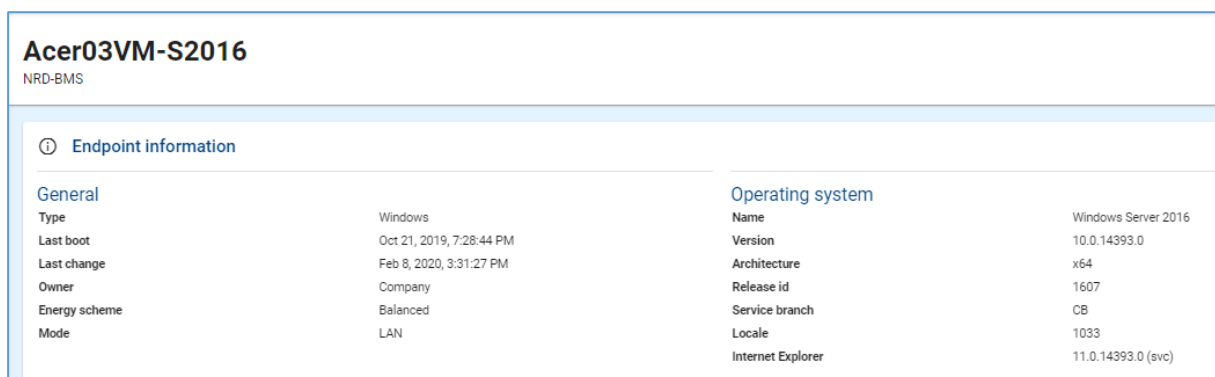


Figure 43 - Detailed view of an end device

More information about a specific device is a click away. In the detailed view of an endpoint, in-depth information is shown based on the type of endpoint. Among other things, the IT administrator can see:

- ✓ Has BitLocker encryption been activated on the end device?
- ✓ Are there any critical patch updates<sup>10</sup> for this device?
- ✓ Which operating system is installed?
- ✓ In which other UDG is this end device included?
- ✓ When was the last successful contact from the management server to the end device?

## 4.6 Additional enhancements

### 4.6.1 License Management

baramundi License Management offers a compact and easy way to record licensing information for better visibility of used and available licenses for installed software.

Optimized assignment of installations has been implemented in 2020 R2 for streamlining recording of license data when deploying or updating software.

#### 4.6.1.1 Concept

The status of software installations (software detection rules) changes frequently as new software or new versions of existing software are installed on company computers.

Unassigned installations can now be easily assigned using various options.

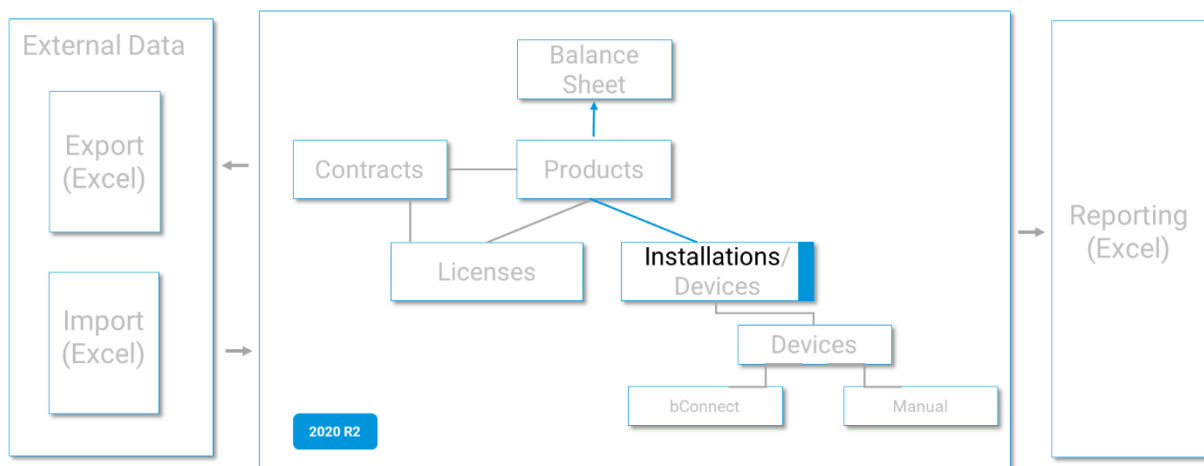


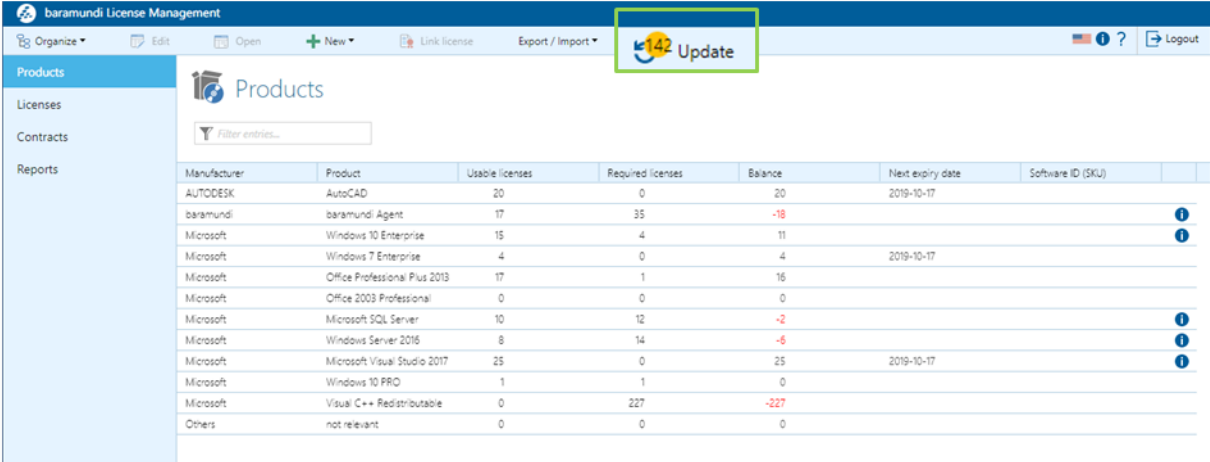
Figure 44 – Overall license management concept in bMS 2020 R2

<sup>10</sup> Also see: 3.3 List of missing and installed updates

#### 4.6.1.2 Display of installations not yet assigned

For licensing data to be kept up to date, it is important to assign all relevant installations (software recognition rules) to the respective products.

Up-to-date information about the number of installations that have not yet been assigned is shown in the menu bar of the new version of baramundi License Management for instant visibility.

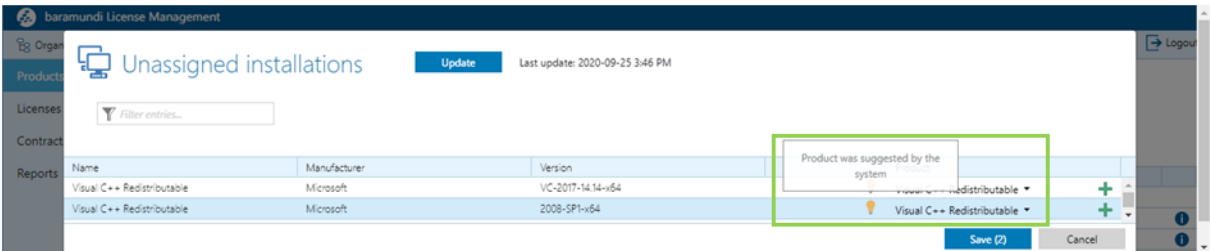


Manufacturer	Product	Usable licenses	Required licenses	Balance	Next expiry date	Software ID (SKU)
AUTODESK	AutoCAD	20	0	20	2019-10-17	
baramundi	baramundi Agent	17	35	-18		
Microsoft	Windows 10 Enterprise	15	4	11		
Microsoft	Windows 7 Enterprise	4	0	4	2019-10-17	
Microsoft	Office Professional Plus 2013	17	1	16		
Microsoft	Office 2003 Professional	0	0	0		
Microsoft	Microsoft SQL Server	10	12	-2		
Microsoft	Windows Server 2016	8	14	-6		
Microsoft	Microsoft Visual Studio 2017	25	0	25	2019-10-17	
Microsoft	Windows 10 PRO	1	1	0		
Microsoft	Visual C++ Redistributable	0	227	-227		
Others	not relevant	0	0	0		

Figure 45 — Products with the number of installations not yet assigned

#### 4.6.1.3 Optimized assignment of installations

If the name and manufacturer of newly installed software correspond to an existing installation associated with a product, the system automatically proposes the assignment.



Name	Manufacturer	Version
Visual C++ Redistributable	Microsoft	VC-2017-14.14-x64
Visual C++ Redistributable	Microsoft	2008-SP1-x64

Figure 46 — Automatic proposal for the assignment of new installations

Alternatively, the person responsible for the license has the option of quickly assigning the installation using a selection of existing assigned products.

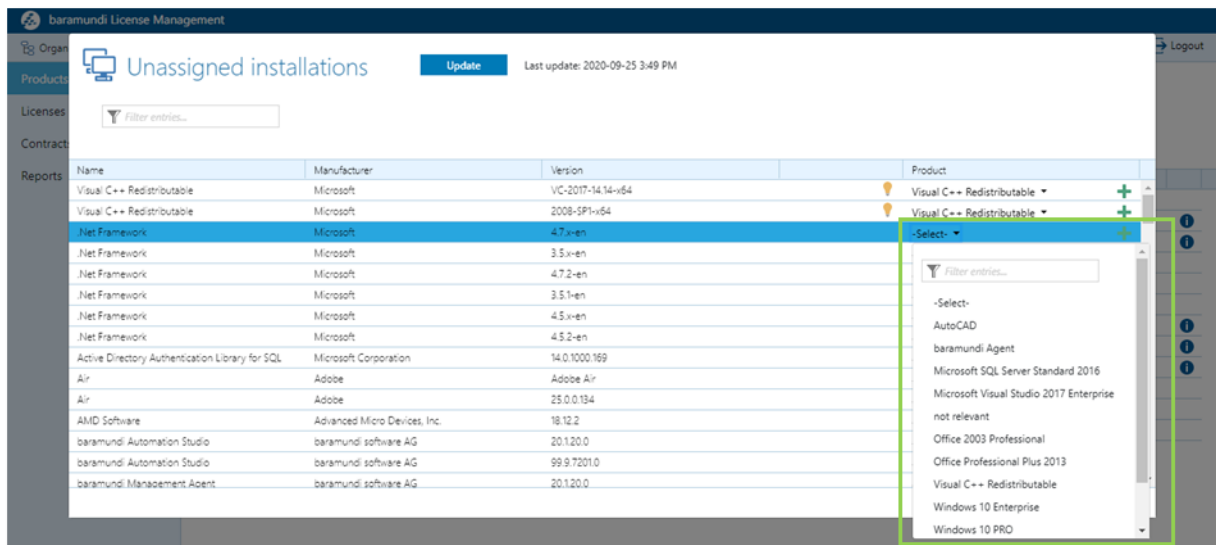


Figure 47 – Unassigned installations - selecting existing products

If no suitable product is available, the selection of the + symbol enables a new product to be created directly. The name and manufacturer are automatically adopted as a suggestion in the corresponding view to simplify creation.

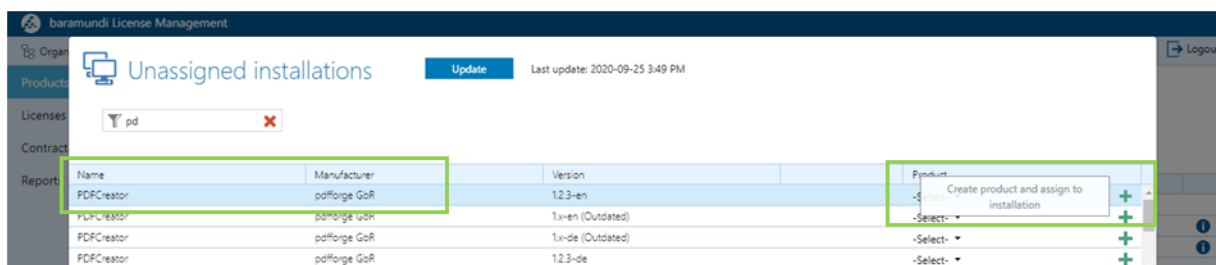


Figure 48 – Unassigned installations - direct creation of new products

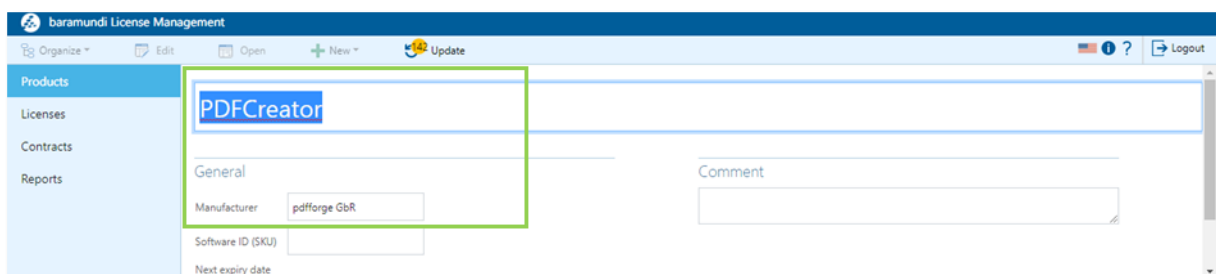


Figure 49 – Simplified creation of new products

All assignments proposed by the system or intended by the user are displayed before they are saved.



With 2020 R2, bLM offers various options for assigning new installations quickly and clearly, making it considerably easier for the license manager when there are frequent changes due to new versions and when newly acquired software is deployed.

#### 4.6.2 Optimization of the bBT downloads for IEM clients

Optimizations to transmission logic significantly increased the speed of bBT downloads via the gateway. The downloads are now up to 25 times faster than before.

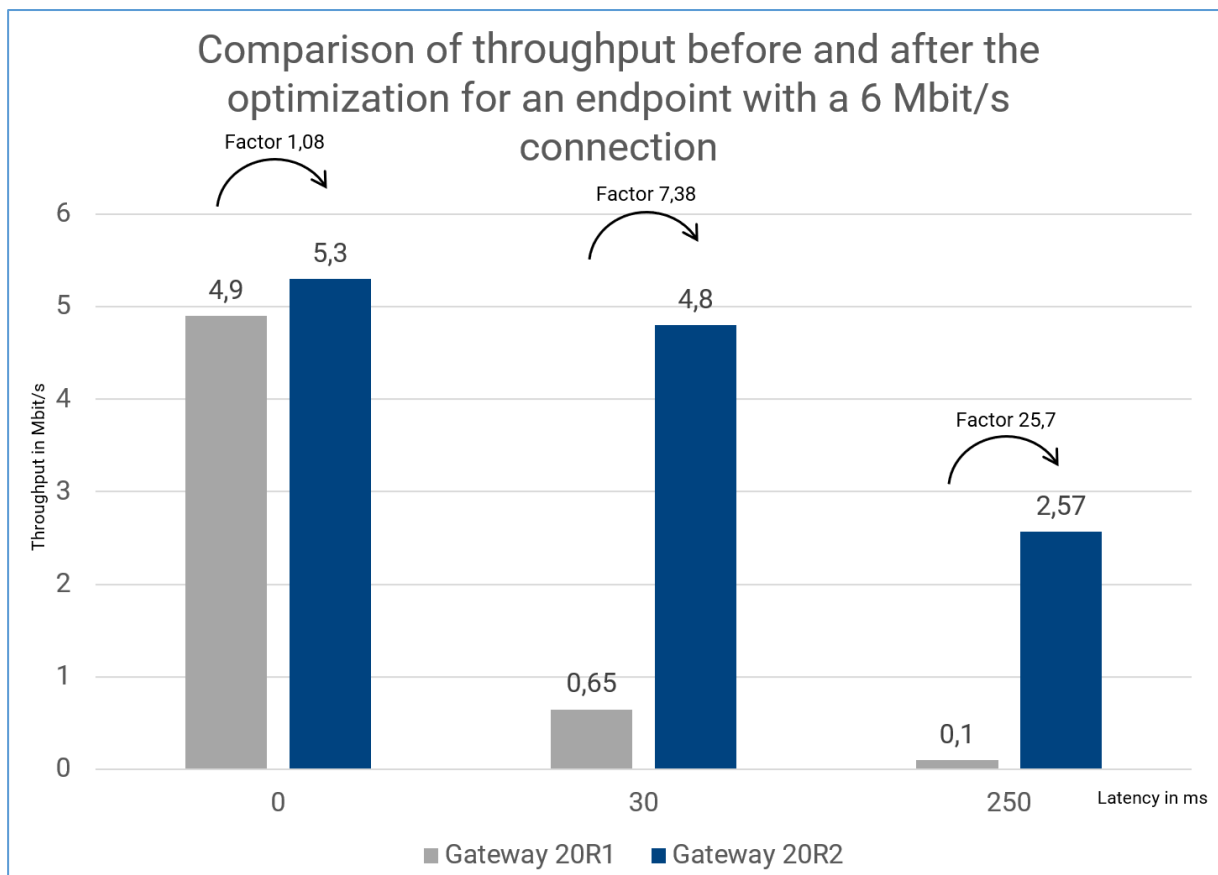


Figure 50 - Measured increase in speed through optimizations

Endpoints with poor connectivity or high latencies benefit the most from these optimizations.

#### 4.6.3 Dedicated device mode for iOS

The dedicated device capability in Android Enterprise for configuring warehouse barcode scanners, retail sales tablets and other applications that was introduced in 2020 R1 is now available for iOS-based devices in 2020 R2.

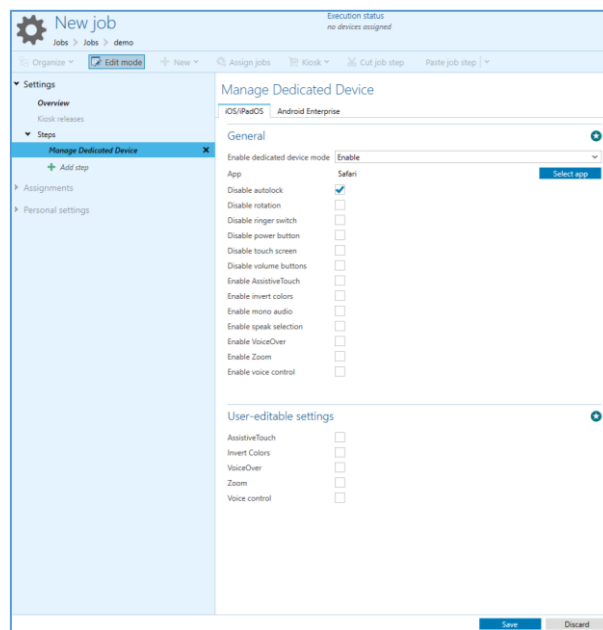


Figure 51 - Dedicated Mode Configuration for iOS

Admins can lock down iOS devices for specific uses by configuring a job step that specifies the app to be launched and the degree to which the user can change the display. As long as the device is in dedicated mode, the selected app is launched directly after powering on. Switching to or adding other apps is not possible.

#### 4.6.4 Filters for job steps for mobile / macOS jobs

The selection of the job steps for mobile devices and macOS has been simplified with filters for platforms and management profiles. This means that when the job is created it can be seen whether the selected job steps are supported by the desired platform.

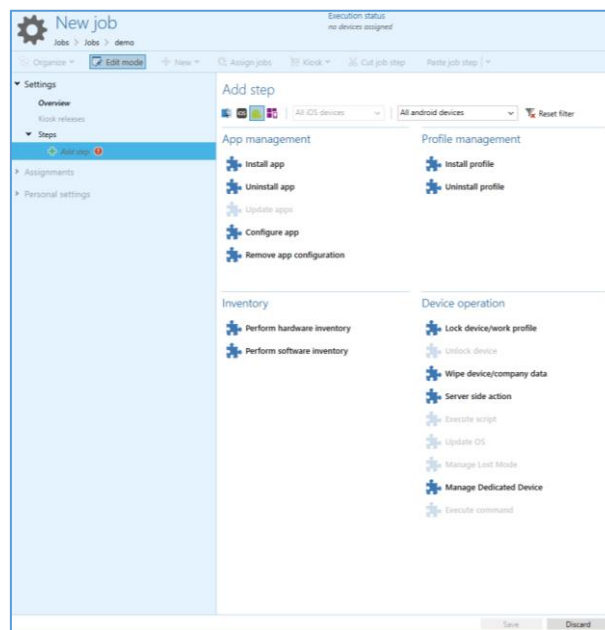


Figure 52 - Filtered job steps that can be executed on Android.

#### 4.6.5 Filters for items in configuration profiles for mobile devices

A filter has also been added to the selection of profile items for mobile devices. When creating the profile, you can see whether the item can be used on the desired platform.

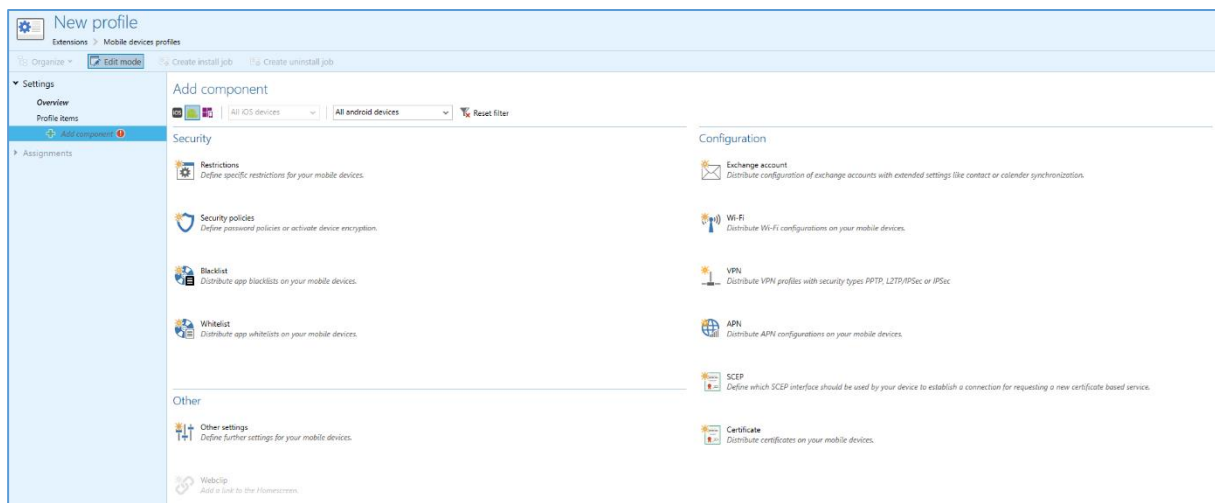


Figure 53 - Filtered profile modules for Android

#### 4.6.6 Transfer of configuration files for Android

With the introduction of Android Enterprise support in the bMS, we have emphasized support for the Managed Configuration - the configuration of Play Store apps by the EMM. But not all of the available apps are configurable by this Managed Configuration. Some app developers still rely on app configuration via a file on the device.

In order to be able to deploy these apps in a meaningful way, the bMS now also supports the transfer of textual app configuration files.

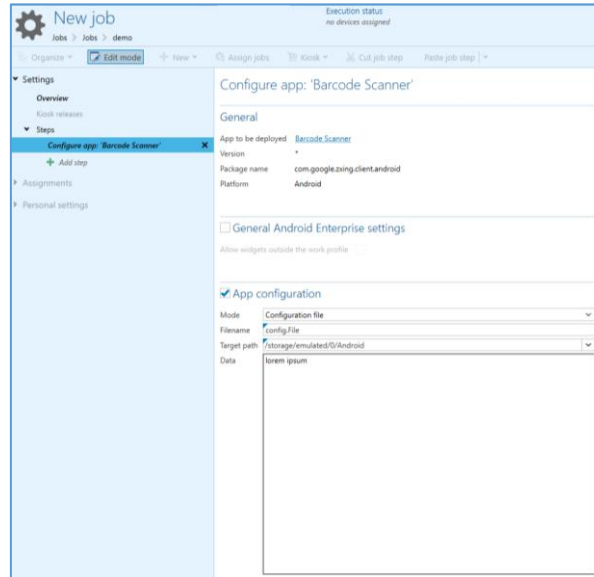


Figure 54 - App configuration via file

In order to create a configuration file for a specific app on the Android device, you can now choose between the Managed Configuration and the configuration file in the "App configuration" area. If configuration file is selected, the file name, storage location and content must be specified.

When the job step is executed the baramundi agent creates the file with the specified parameters on the device.

#### 4.6.7 Language selection for enrollment emails

With the bMS 2020 R2, the administrator can now also create language-specific templates for the enrollment of mobile devices, macOS and Windows in IEM mode. These templates are then available in the enrollment dialog and are also used when creating an endpoint via bConnect.

Add device

Add a new device

Platform
Android Enterprise

Management mode
Work profile

Owner
Company

Registered user

Display name

E-mail
☒ Send enrollment e-mail

E-mail language
English (United States) | en-US

Recipient
Deutsch (Deutschland) | de-DE
English (United States) | en-US

☒ Check compliance

Save
Close

Figure 55 - Language selection for enrollment emails

## 4.7 Product Improvements in Detail

### 4.7.1 General

- All setups were changed from MSI to .EXE.
- The bMS own licensing was improved. The error code 233 shows possible causes. Furthermore, in case of an unexpected license break, e.g. in case of detected hardware changes, the server operation is still possible for a few days without restrictions. In addition, no Eval-License must have been activated.
- Improved log message `External component has thrown an exception in bServer.log` in case of database problems.
- Bugfix: Jobs with `user must confirm execution` setting, which are rescheduled using job interval, ask the user only once for his approval.
- Bugfix: The proxy setting stored in the `Configuration-Server-Settings-Downloader` is not considered for Apple VPP and Apple push.

### 4.7.2 Windows Agent (bMA)

- For the enrollment of a Windows client (IEM) administrator rights are no longer necessary. For this purpose, the bMA must be installed in advance without enrollment.
- Wipe disk now works under Windows PE x64 and UEFI too.

### 4.7.3 Management Center (bMC)

- The new Windows 10 naming scheme (20H2) is shown as `Display Version` under `Client-Settings-Overview`. Usage in Universal Dynamic Groups is possible.
- The compatibility mode for communication with obsolete bMAs (older than version 2019 R2) has been removed.
- Under `Windows-Client-Overview`, the assigned IP network of the client is displayed.
- The License Configuration page has been improved to better reflect the workflow.

- The offline help including Cobrili is now a standalone setup. It is listed as optional in the overall setup. The use of the online help is strongly recommended because it is more up-to-date.
- BitLocker keys can be viewed even if the device is deactivated.
- A log message `Failed login attempt for user name` is written to the `bServer.log` file if a login attempt fails.
- A new `Manage Microsoft Update` job step to inventory missing and installed Microsoft updates.
- In a `dynamic group (Universal)` there are new conditions for industrial control device, Microsoft Updates and MDM devices.
- New command line parameters for the bMC
  - `/bServer=bmsname` sets the bMS server name to `bmsname`
  - `/useLoggedInUser` sets the check-box to single sign-on;
  - `/autoConnect` resolves an automatic login at bMC startup.
- The `personal settings` and `notifications` have been changed to the modern GUI format.
- Bugfix: Under `Configuration` some headings are missing.
- Bugfix: When changing the name of an IP network an SQL error message appears.
- Bugfix: In rare cases no productive license could be imported after expiration of the evaluation license.
- Bugfix: If the edit mode is quickly switched on and off while editing jobs, the job category is sporadically reset.
- Bugfix: During automatically repeated job execution the job step counter (e.g. 5/5) is not reset and shows a wrong value until the first step is finished.

#### 4.7.4 Argus-Connect

- Under `Dynamic Group (Universal)` a new `Sync to Argus` permission enables one to configure which bMC users can synchronize universal groups to Argus-Cockpit.
- Up to 10 Universal Groups can be synchronized to Argus-Cockpit.

- The cloud connectors will terminate automatically if the bMS Server version is incompatible.

#### 4.7.5 Mobile Devices

- It is possible to store your own e-mail templates without having to re-import them when changing versions. (File name e.g. MailTemplate.VPPUser.Custom.html)
- In the bMC, example command is displayed for the job step `Execute iOS command`.
- iOS devices from iOS 13.1 can be managed as user registered (BYOD) devices.
- When creating SSA job steps, the name of the selected script is now also displayed at the job step in edit mode.
- The `Installed On` view for MDM apps now also contains a column for the installed version of the app
- Android Enterprise improvements:
  - Control of the `auto app update policy` including maintenance window .
  - New restriction: `allow apps from unknown sources`.
  - Configuration files can be transferred to the device via a new step.
  - The Android Enterprise restriction `Disallow backup to Google Drive` is now also available for work profiles.
  - For Android Enterprise Dedicated Device Mode, a template can now be selected additionally. This makes it possible to flexibly adapt the layout on the device Moreover, there is the possibility to let the user control options like screen brightness.
- The iOS Dedicated Device Mode (COSU) can be activated/deactivated and configured via job step.
- When sending enrollment emails, the language of the email can be selected.
- When selecting a profile item and a job step, it is possible to filter for which platform and which management method these are suitable.



- Under `Profile-Restrictions-iOS/iPadOS` the text `Allow managed targets to read unmanaged contacts` is not clearly formulated. (New: `Allow unmanaged targets to read managed contacts`).
- Bugfix: If variables are created at a group and at an endpoint with the same scope and the same name, the variables at the client were partially overwritten with the values of the variable at the group during job execution.
- Bugfix: If an attempt is made to end the compliance check for an MDM device using "Pause compliance check", an exception message appears.
- Bugfix: When deleting a black/white list for MDM, the bMC displays a false message with low significance if there are linked elements which prevent the deletion. (The linked elements are now displayed here).
- Bugfix: A compliance violation is triggered only once for Android Enterprise devices and is not updated.
- Bugfix: In rare cases the Apple Push Service can crash when a device is re-rolled.
- Bugfix: The bMC column `BMA version` shows a wrong version for iOS devices.
- Bugfix: iOS devices cannot be deleted if VPP licenses are linked to the device and the VPP token is invalid.
- Bugfix: In rare cases, no APN-CSR can be created via `Configuration-Mobile Devices-Common`, an exception message appears.

#### 4.7.6 OS-Install

- Bugfix: An inplace upgrade job fails if no hardware profile is set in the bMC for this client.

#### 4.7.7 bConnect

- New controller: `UniversalDynamicGroups`.
- Parameters have been added to the Endpoint Controller so that the endpoints of a Universal Group can be read.
- The enrollment of IEM clients can be managed via the `EndpointEnrollment` Controller.

- For MDM and MacOS devices it can be specified if and in which language an enrollment email should be sent.
- New controller: Dynamic Groups Cloud Connector to synchronize up to 10 universal dynamic groups including endpoint results with Argus Cockpit.
- For Windows clients the list of installed and missing updates, including update metadata, can be queried.

#### 4.7.8 bMOL

- Note: We generally recommend to switch from bMOL to bConnect.
- Bugfix: Reading of applications and bundles does not deliver any data.

#### 4.7.9 baraDIP

- The bBT throughput has been significantly improved, especially for Internet connections with high latency.
- Bugfix: The log file is getting bigger continuously. This can limit the performance of baraDIP in large environments.

#### 4.7.10 Defense Control

- Under `Defense Control-Settings` the Bitlocker Network Unlock can be switched on/off.
- Two new job steps under `Manage Bitlocker` to enable/disable BitLocker Network Unlock.

#### 4.7.11 License Management

- An info page shows useful information like version number, database and user data.
- The registration token has a longer runtime.
- A manual logout is possible.
- Bugfix: If the name of a product is changed, this can lead to data loss.

- Bugfix: After the update the message `Can't parse cpus as licenseType` appears in some cases.
- Bugfix: The F1 help always opens in German by default.

#### 4.7.12 Mac OS

- Bugfix: When enrolling a Mac device, the server name, which must be specified when installing `bma.pkg`, is not displayed.
- Bugfix: A mac OS update may have reset the `sudoers` file and no more jobs could be executed afterwards.

## 5 Release 2020

### 5.1 Android Enterprise: Dedicated Devices

#### 5.1.1 Overview: Android Enterprise Profile

Android offers three management options<sup>11</sup> for business devices in the form of Android Enterprise Profiles:

- for business only
- for private use
- as a dedicated device

This enables companies to best manage a variety of Android devices for specific application scenarios.

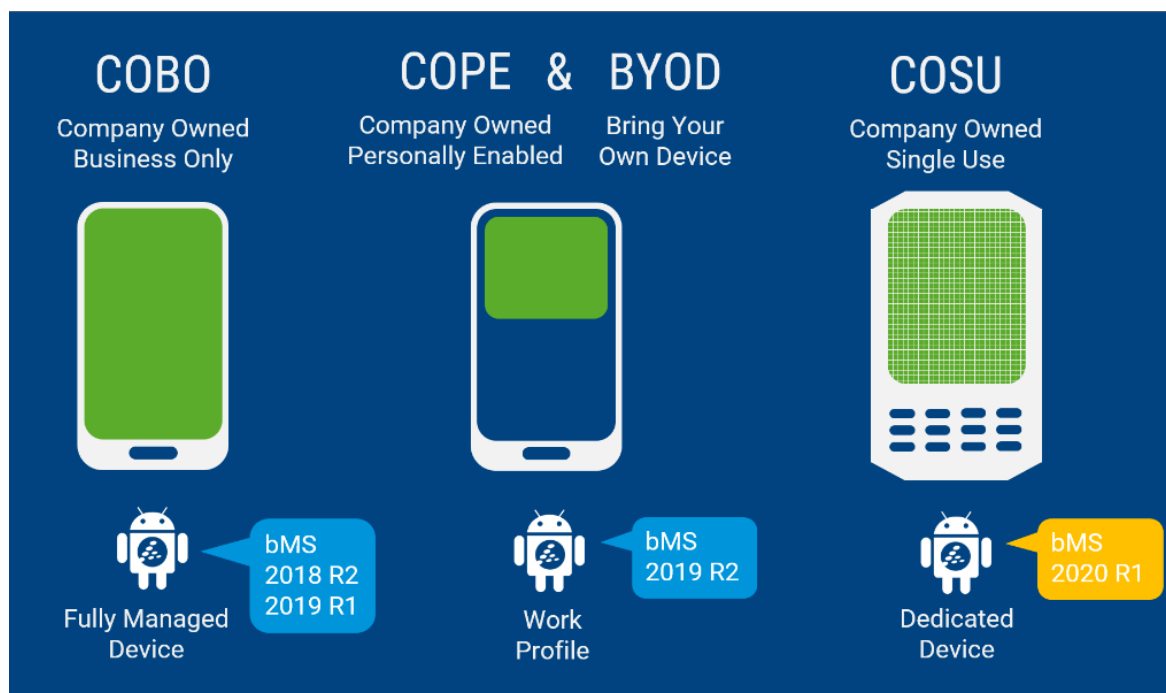


Figure 20 – Android Enterprise Profile and application scenarios

Up to now, the baramundi Management Suite has supported two profiles: *Fully Managed Device* and *Work Profile*. Dedicated devices with the *Dedicated Device* Profile will be also supported with the 2020 release. The administrator can determine for each managed device which management mode best suits the application.

<sup>11</sup> Android Enterprise management options: [https://www.android.com/intl/en\\_us/enterprise/management/](https://www.android.com/intl/en_us/enterprise/management/)

### 5.1.2 Application scenarios for dedicated devices

Classic mobile devices are typically assigned to an employee and are used exclusively by this one person. Dedicated devices serve for a certain business purpose and are usually not assigned to a specific employee, but used alternately by different people.

For example, Android operating system bar code scanners are used in logistics. They are used alternately in shift operations by employees in the warehouse. Only the scanning code app is used on such devices. All other apps are therefore hidden. This increases user convenience and prevents incorrect operations.

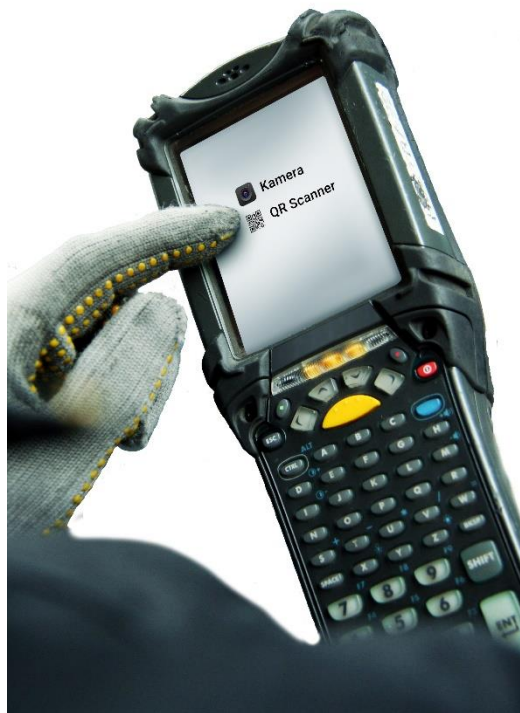


Figure 21 – Barcode Scanner in dedicated mode for selected apps

Android tablets can also be used in retail industry: Using these, sales reps can show product demos to customers, and product configurations can be completed. This ensures that the customer does not accidentally open other apps.

### 5.1.3 Configuration with baramundi Mobile Devices Premium

baramundi Mobile Devices Premium manages the "Dedicated device" profile. After enrollment, devices are identified as "dedicated device" in the bMC. This identification can be found as a column in the group list view, universal dynamic groups and also on the device overview page.

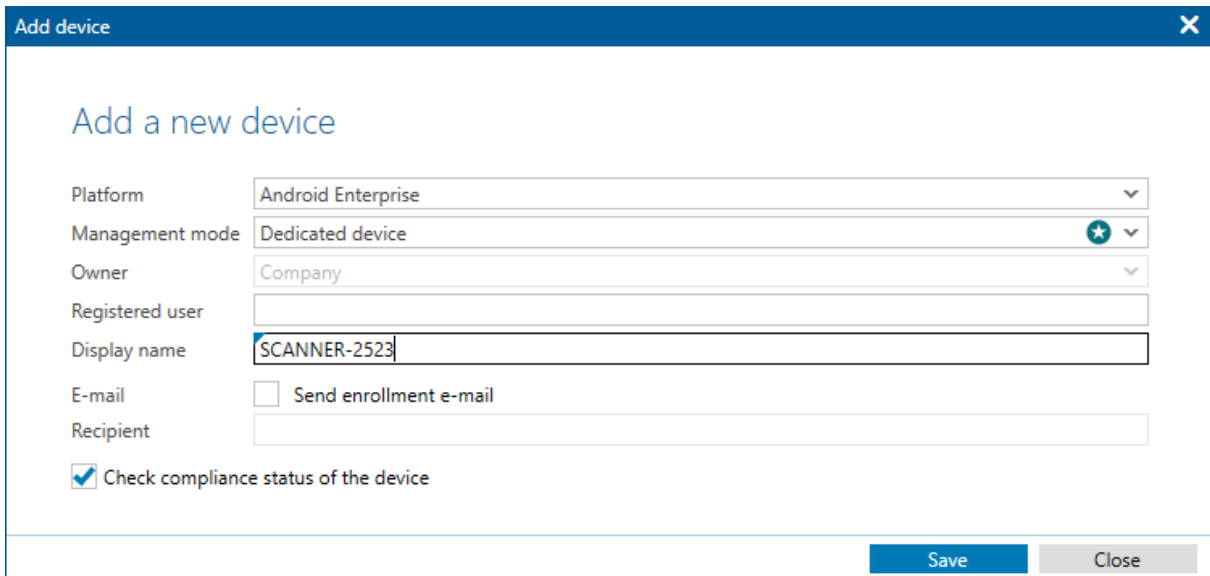


Figure 22 – Adding a new dedicated device

Dedicated devices can be limited to one or more apps. This limitation is based on the already known whitelists. Additional settings can also be made, such as the availability of system functions (home button, notifications, etc.).

"Manage dedicated device", a new job step, was added to device set-up. The device can be also put into a maintenance mode in this job step if no whitelists are distributed. The device cannot start any apps with it.

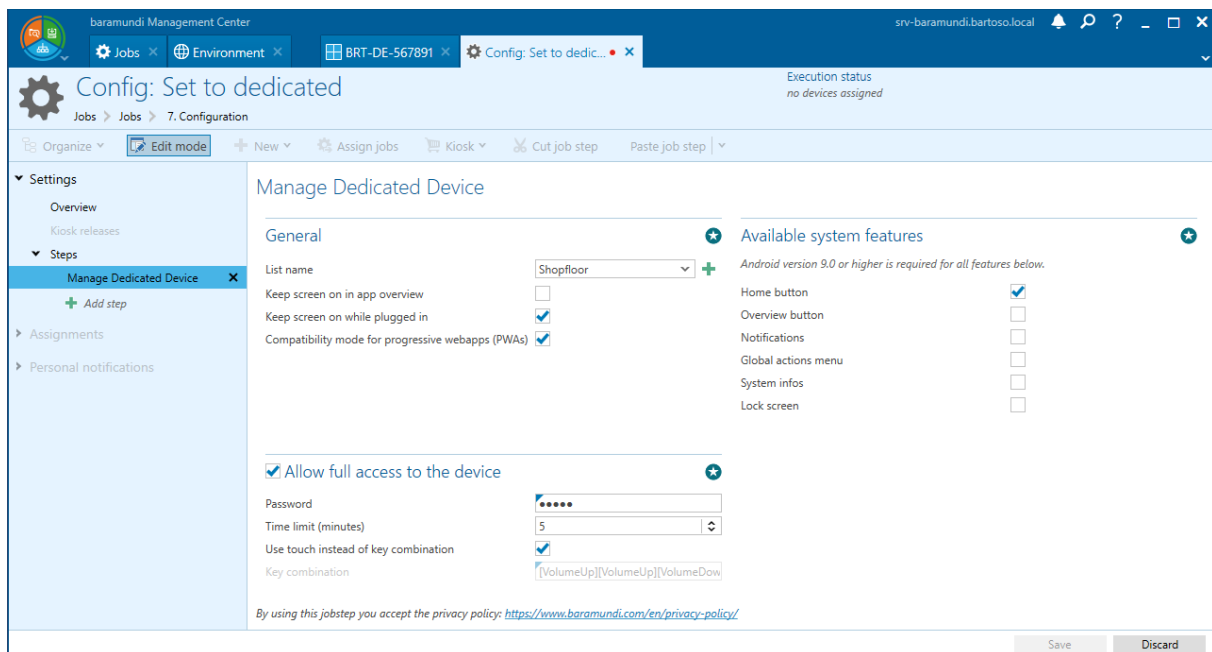


Figure 23 – Settings for the "Manage dedicated device" job step

After a job is completed on the device, they are "locked" accordingly. From now on, the user can only start the apps when released by the administrator. If only one app has been implemented, it is started automatically after device startup.

Using a special key combination and a password, the administrator can switch to an administrative mode on any device, and can change settings in this mode.

## 5.2 baramundi Argus Cockpit

Administrators face a huge task. They must keep an eye on the "health" of one or more various IT environments 'round the clock. Titan Argus helps them here: This tireless guard from Greek mythology, equipped with hundreds of eyes, is the inspiration for baramundi Argus Cockpit.

Argus Cockpit allows IT administrators to control the "health" of their bMS environment(s) from any web-enabled device with a clear visual user interface. In addition to the baramundi Argus Cockpit, the baramundi Management Suite is now provided with a cloud-based dashboard. This combines "On-Prem" architecture of the baramundi Management Suite with the cloud architecture of the dashboard. A new hybrid solution is born.

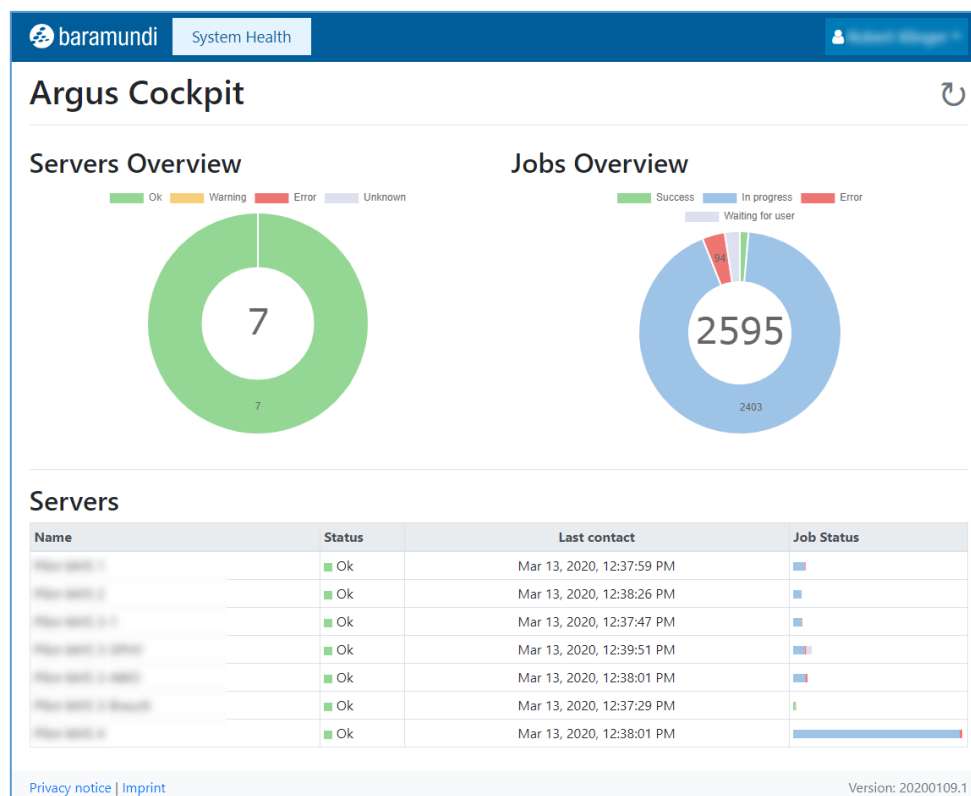


Figure 24 – baramundi Argus Cockpit start page

Another great advantage of the Argus Cockpit hybrid approach is that baramundi provides the necessary infrastructure in the cloud. It therefore does not have to be implemented in each individual company. Functional updates can be continuously imported by baramundi in this cloud environment. This means, that the Cockpit is (to a great extent) developed independently of bMS release cycles.



### 5.2.1 Data retrieval regardless of time and place

An important criterion for the concept and implementation of the Argus Cockpit is that, the relevant IT data can be retrieved by the administrators without any infrastructure hurdles. In 2020 release, the status of bServer services and information is shown during job execution. This eliminates the need to establish a direct VPN connection to managed networks. Necessary data can be retrieved directly in a dashboard view using the browser of any current, web-enabled device. In a responsive view, IT administrators have access to relevant IT environment data and its key figures anytime and anywhere - on the go or in their home office.

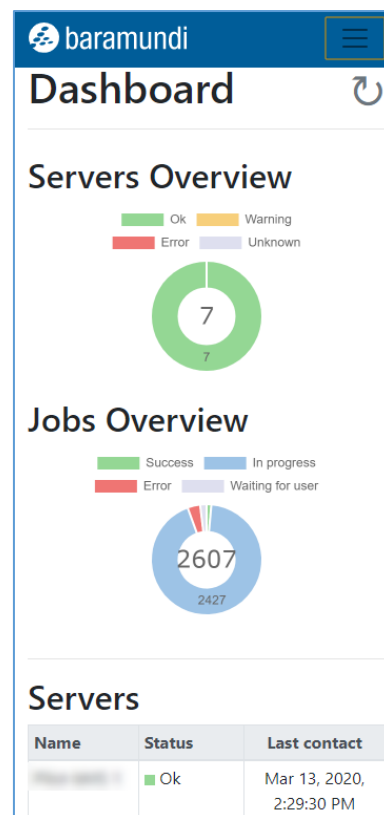


Figure 25 – Responsive presentation on a mobile device

### 5.2.2 Secure access to the data in the Argus Cockpit

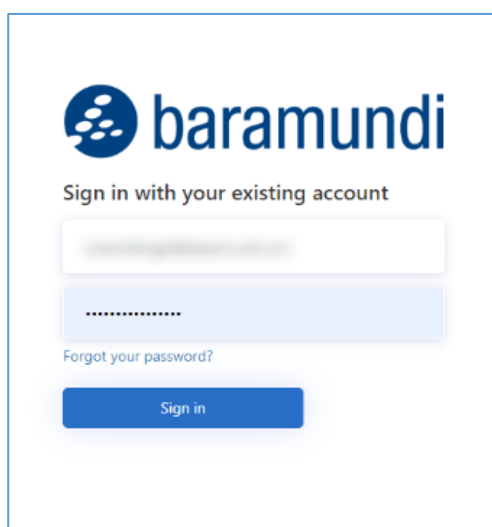


Figure 26 – Secure registration in the Argus Cockpit

Information about the “health” of the connected systems is provided via the cloud. To ensure that every IT admin in the Argus Cockpit can only see the data for which he is authorized, the Argus Cockpit starts with a simple but very secure user administration. baramundi can thus provide access to interested customers. Their IT admins can log in with their email address and self-selected password.

### 5.2.3 Secure bMS connection to the Cloud

The Cockpit User can securely log in to the cloud and use the dashboard. This action is just as secure as transferring the data to the cloud from the respective baramundi Management Server. From that point, the data "leave" the network boundaries of the respective company and must be protected. baramundi has placed special emphasis on secure implementation and applies the most modern components, interfaces and hosting of the Cloud components in the EU e.g. with Microsoft Azure AD, Identity Server, baramundi Connect and HTTPS. Secure data processing is guaranteed with the baramundi Argus Cockpit for subsequent processing, in compliance with data protection and data transmission, providing protection against unauthorized access thanks to proven security standards.

From 2020 R1, IT administrators can select whether to synchronize relevant data with the baramundi Argus Cockpit in the bMC. IT admin can configure a decision whether the data should be sent to the Cloud in the bMC at any time.

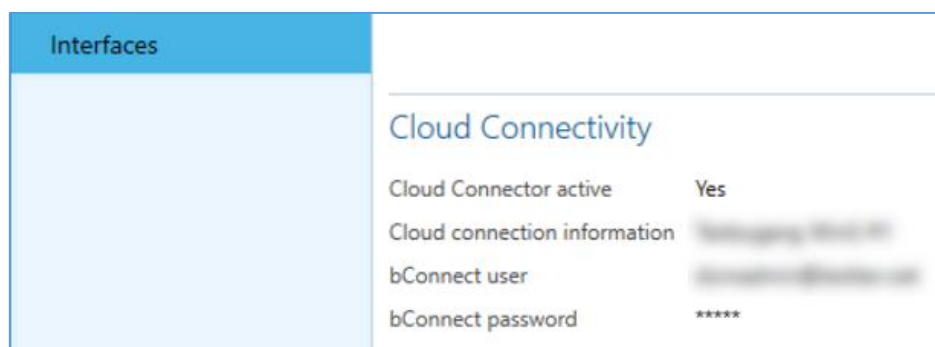


Figure 27 – Configure the connection to the Argus Cockpit

## 5.2.4 Overview of one or several systems

The baramundi Argus Cockpit is multi-client capable. It provides simultaneous monitoring of several IT environments managed with the baramundi Management Suite. Administrators in multiple company locations and Managed Service Providers (MSP) who are responsible for multiple customer environments can monitor the status of all their systems directly in a single user interface. The Argus Cockpit provides information on whether there is an action required for one of the connected systems, and enables fast detection of how the interruption of the regular process came about.








Servers			
Name	Status	Last contact	Job Status
bMS 1	Ok	Mar 13, 2020, 2:41:30 PM	
bMS 2	Ok	Mar 13, 2020, 2:41:59 PM	
bMS 3-1	Ok	Mar 13, 2020, 2:41:18 PM	
bMS 3-2	Ok	Mar 13, 2020, 2:43:21 PM	
bMS 3-3	Ok	Mar 13, 2020, 2:41:31 PM	
bMS 3-4	Ok	Mar 13, 2020, 2:41:01 PM	
-bMS 4	Ok	Mar 13, 2020, 2:41:34 PM	

Figure 28 – Status overview of several bMS instances

#### 5.2.4.1 Problem detection with bServer services and job execution

Administrators who are responsible for more than one baramundi Management Server in their IT infrastructure often face a dilemma: How can you monitor baramundi jobs and bServer services that work on independent systems when working outside the company network?

Maintaining several VPN connections to the respective servers is both confusing and challenging for implementation. In addition, access can only be made from equipped work areas. This is too much effort for a short "health check."

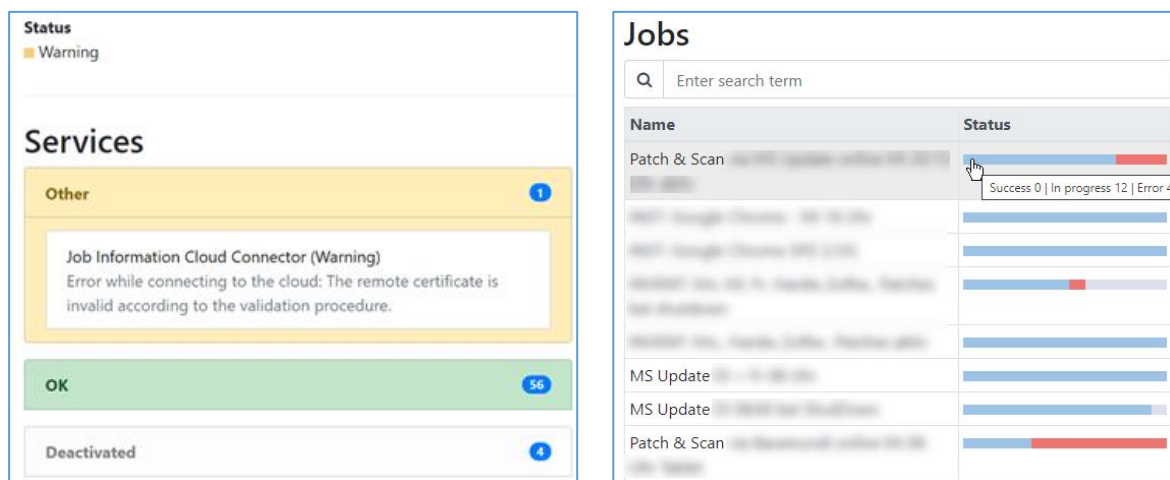


Figure 29 – Status via bServer services and baramundi jobs

The baramundi Argus Cockpit can quickly detect problems and warnings about individual bServer services and identify failed job instances. Error messages and other status information can be selected per job instance and thus addressed locally on the respective bMS instance using searches and filters of the result lists.

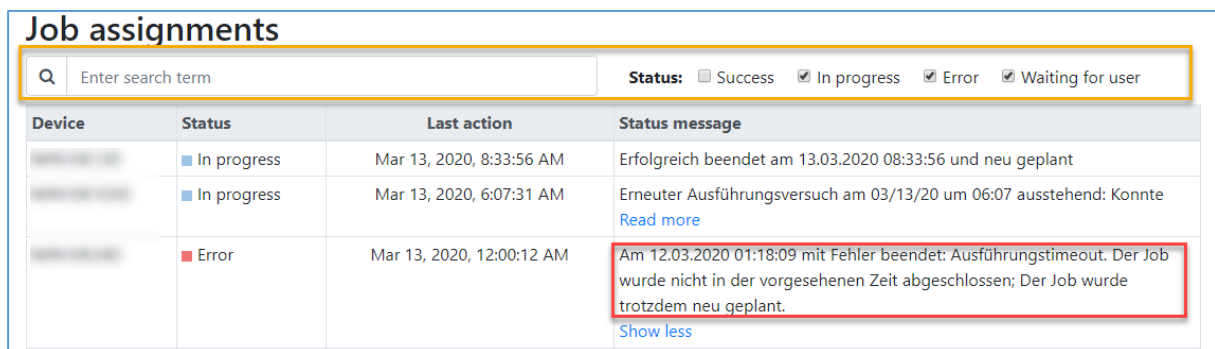


Figure 30 – View of the detailed information per job instance

## 5.3 General Development

### 5.3.1 License Management

*baramundi License Management* offers a compact and easy way to manage license management commercial information to achieve better transparency of available company licenses.

The new version was enhanced to import external data for e.g. Products, Licenses and Contracts.

#### 5.3.1.1 Concept

A template for Products, Licenses and Contracts is generated ① and exported to Excel on the basis of the data available in bLM,

After completing, for example, an overview of products in an XLS template, this information can be integrated into bLM with an import ②

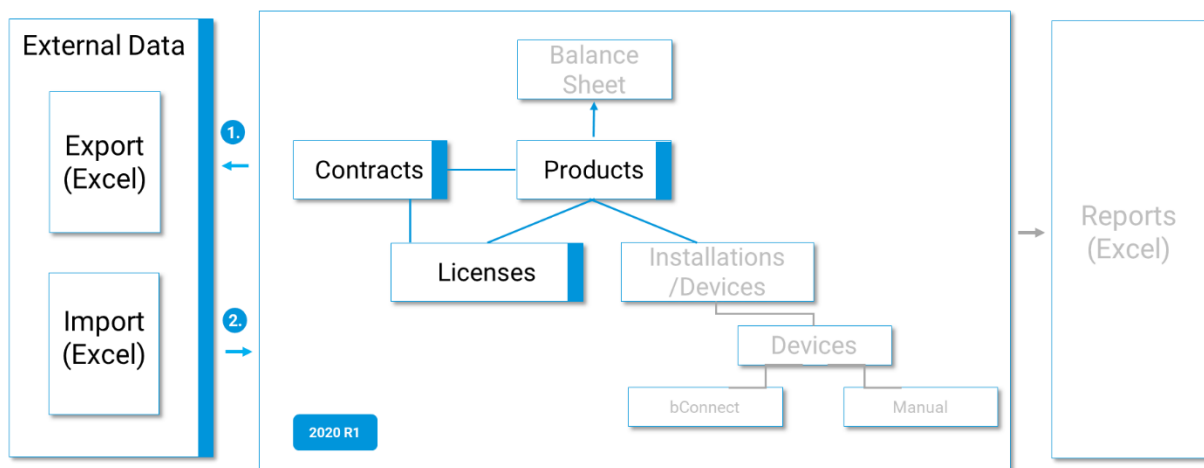


Figure 31 – License Management general concept 2020 R1

### 5.3.1.2 Importing Products, Licenses and Contracts

It can be helpful to be able to integrate already available data on Products, Licenses or Contracts as part of the initial setup or enhancement of a bLM environment, 2020 R1 offers the ability to import data from external sources.

Data from Products, Licenses and Contracts can be imported from Excel into bLM, an easier alternative to the manual system. An Excel format template exported from bLM serves as the basis for the import of external data in order to reduce setup outlays in bLM.

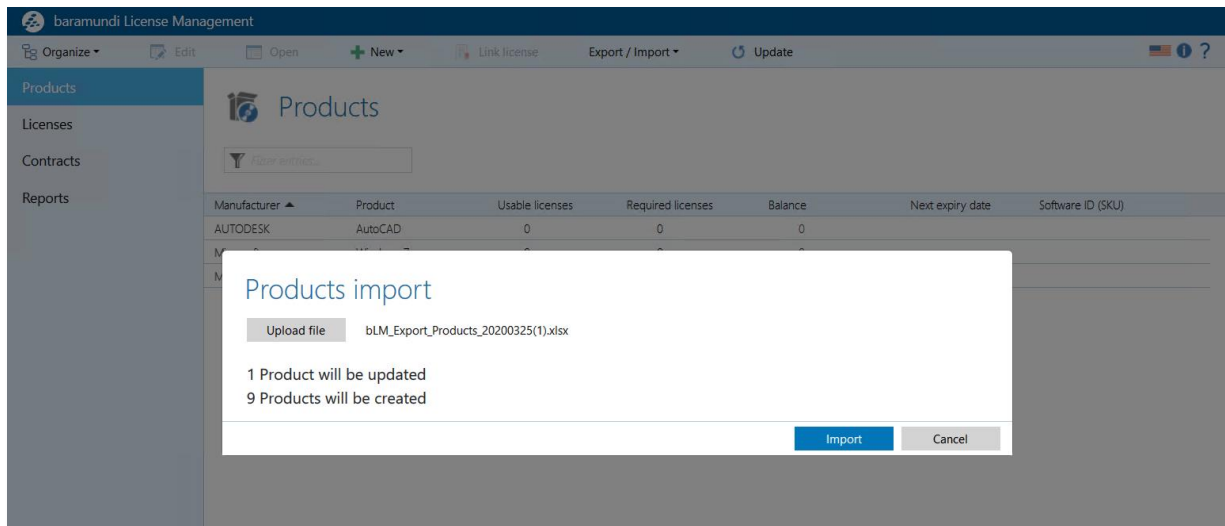
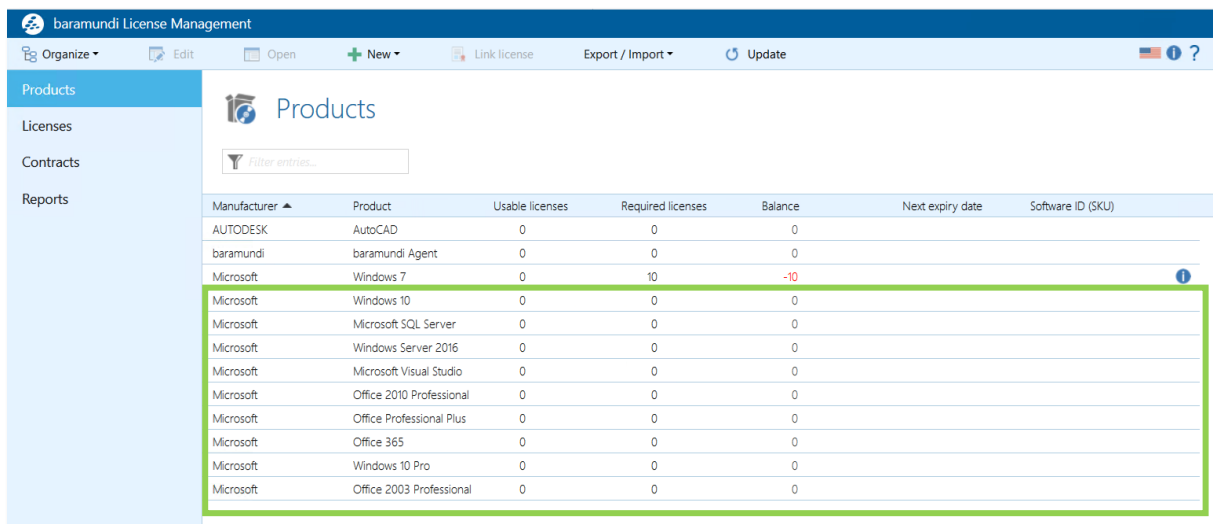


Figure 32 – License Management importing external product data



The screenshot shows the 'baramundi License Management' application with the 'Products' section selected. The table displays a list of products with the following columns: Manufacturer, Product, Usable licenses, Required licenses, Balance, Next expiry date, and Software ID (SKU). The table is highlighted with a green border.

Manufacturer	Product	Usable licenses	Required licenses	Balance	Next expiry date	Software ID (SKU)
AUTODESK	AutoCAD	0	0	0		
baramundi	baramundi Agent	0	0	0		
Microsoft	Windows 7	0	10	-10		
Microsoft	Windows 10	0	0	0		
Microsoft	Microsoft SQL Server	0	0	0		
Microsoft	Windows Server 2016	0	0	0		
Microsoft	Microsoft Visual Studio	0	0	0		
Microsoft	Office 2010 Professional	0	0	0		
Microsoft	Office Professional Plus	0	0	0		
Microsoft	Office 365	0	0	0		
Microsoft	Windows 10 Pro	0	0	0		
Microsoft	Office 2003 Professional	0	0	0		

Figure 33 – License Management extended product overview of importing external data

### 5.3.2 Inventory of Windows Security Center

As an administrator, you always want to be informed about the current security status of the endpoints. That is why bMS now also inventories the status of the individual categories in the Windows Security Center. You can see at any time whether e.g. virus protection is active and up-to-date in the bMC. Firewall status and other module statuses can also be retrieved.

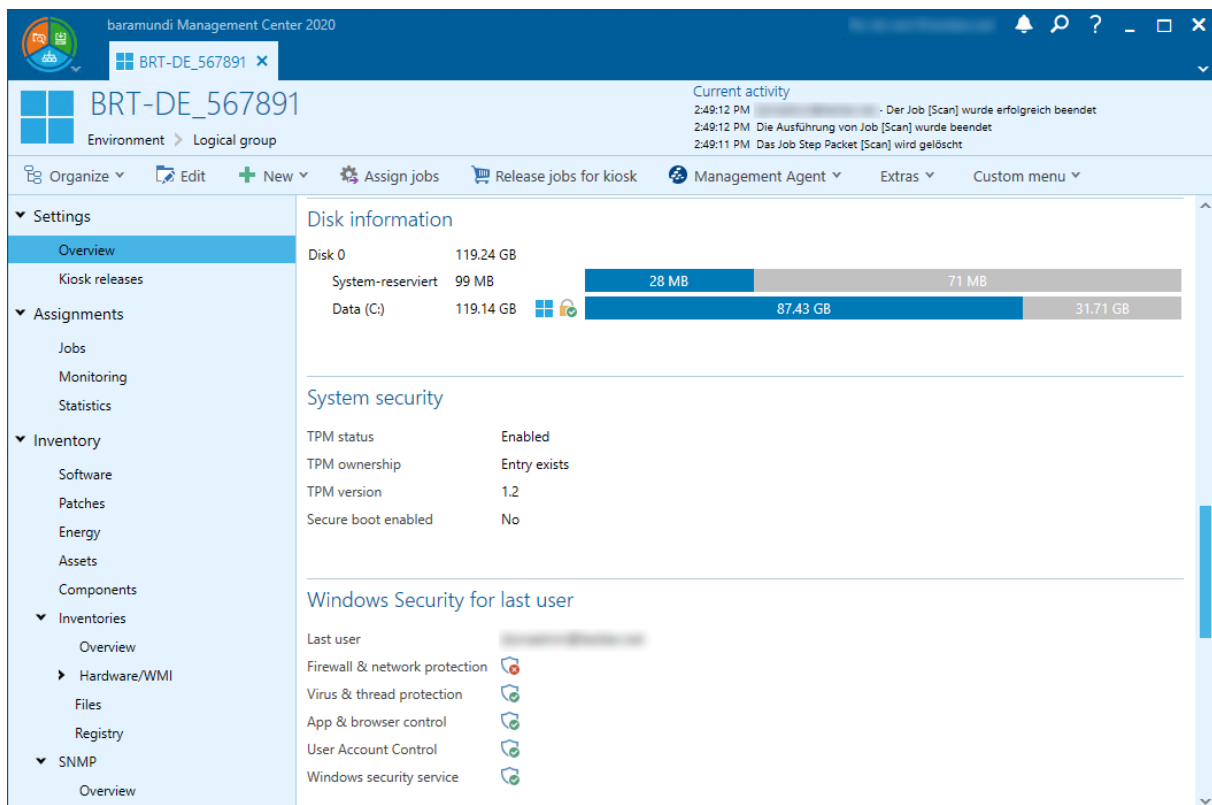


Figure 34 – Inventory of the Windows Security Center

Obviously, these values can also be used as filters and columns in a universal dynamic group (UDG). The status or the combination of statuses can thus be conveniently monitored.

### 5.3.3 Client variables in universal dynamic groups

Endpoint variable can now be displayed at the universal dynamic groups. Mobile device variables as well as Windows endpoints can now be shown and used both as filters and columns.

	Name	Last contact	ContractStart (TEM)	ContactPeriod (TEM)
1	BRTM-DE-237792	1 month ago	2019-10-18	24
2	BRTM-DE-557736	30 days ago	2019-05-24	24
3	BRTM-US-687961	29 days ago	2019-05-12	24
4	BRTM-DE-835484	1 month ago	2019-03-08	24
5	BRTM-CH-307590	29 days ago	2019-01-14	24
6	BRTM-US-845081	29 days ago	2018-07-02	24
7	BRTM-US-335306	30 days ago	2018-02-14	24

Figure 35 – Mobile endpoints with variables in a UDG

	Name	Last contact	Operating system	Inventory id (Warranty data)	Warranty expiration (Warranty data)
1	BRT-AT-985325	28 days ago	Windows 10 64-bit	985325	2021-02-20
2	BRT-DE-844876	28 days ago	Windows 10 64-bit	844876	2020-05-17
3	BRT-DE-612715	28 days ago	Windows 10 64-bit	612715	2020-10-15

Figure 36 – Windows endpoints with client variables in a UDG

### 5.3.4 Starting the Kiosk from the Desktop or Start menu

The device-centric Kiosk can now be opened on client systems without the baramundi Symbol in the tray. Using this, a user-accessible link can be placed at any spot (e.g. desktop or start menu).

By calling up `BMACmd.exe /Cmd:OpenKiosk` the Kiosk is loaded with the device-centric view in the standard browser of the user.

A release in the forum will provide a simple script for creating and distributing these links.



### 5.3.5 MDM commands for Apple devices

A new job step is now available for Apple devices.

The "Execute command" job step can be used to send MDM commands to all supported Apple devices. It is now possible, for example, to change the background image on iOS or change the device name with a job.

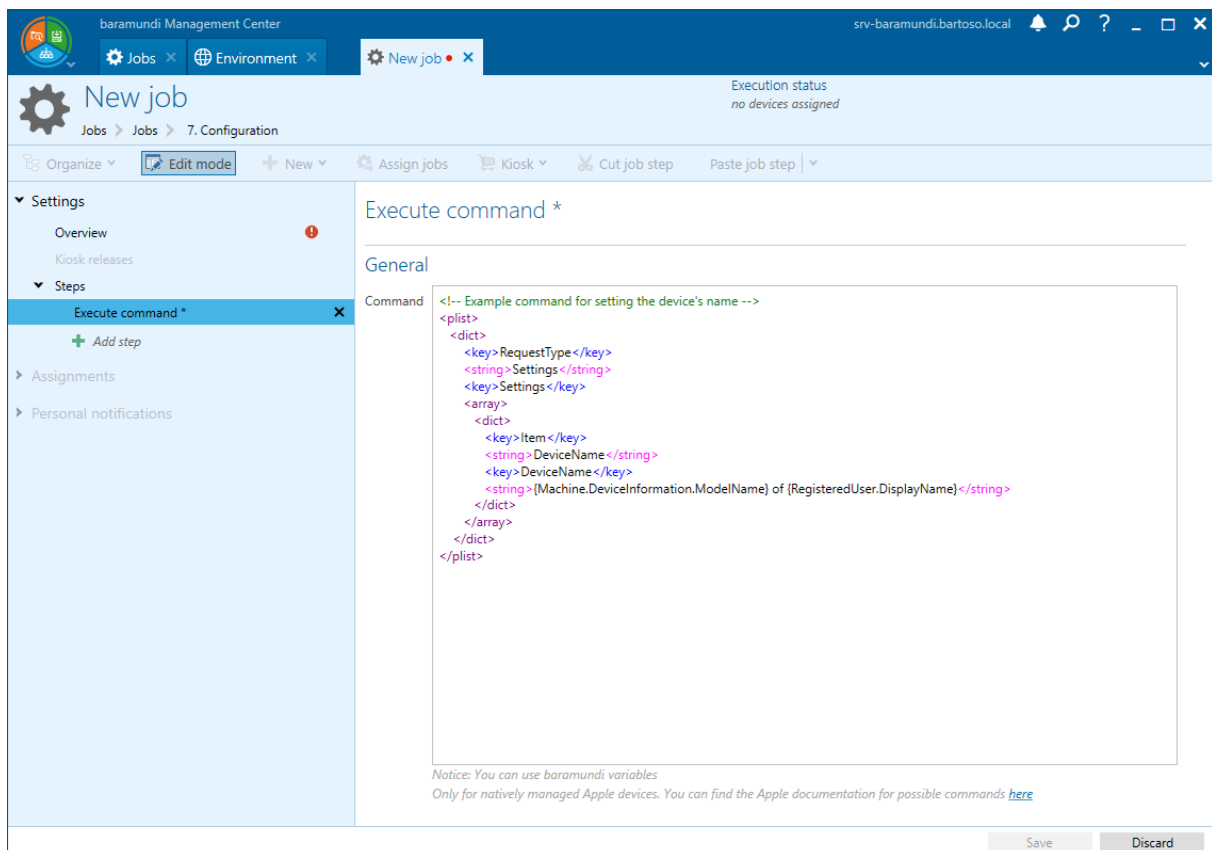


Figure 37 – Changing the device name with baramundi variables

A list of commands provided by Apple is available online and is regularly expanded<sup>12</sup> by Apple.

baramundi variables can also be used within the command.

<sup>12</sup> Apple MDM Commands and Queries: [https://developer.apple.com/documentation/devicemanagement/commands\\_and\\_queries](https://developer.apple.com/documentation/devicemanagement/commands_and_queries)

Since release 2016 R2, the bMS can also be used to manage Windows endpoints outside the local network and without a VPN. Until now, the integration into the management and thus the establishment of the relationship of trust was only done in the local network or manually by importing the public key from the client certificate.

With the bMS 2020, Windows endpoints can now also be securely enrolled from outside of the local network. To this end, enrollment functionality for Windows endpoints was integrated - similar to the enrollment at baramundi Mobile Devices. The administrator can now create a new Windows endpoint and enter an email address. All relevant information on the installation of the baramundi Management Agent and enrollment are sent to this address.

Figure 38 – Enrollment-Dialog in the bMC

After receiving an email, the user can install the agent and establish a secure connection to the baramundi Management Server. Enrollment information can be given directly on the command line during installation. Alternatively, the agent can also be initially connected to the server after installation. A new entry is then added to the agent's context menu.

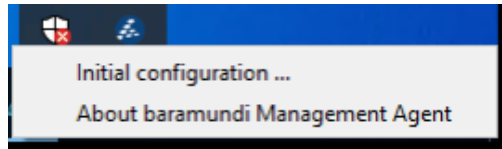


Figure 39 – Context menu of the Agent

Clicking on "Initial configuration" opens a dialog for entering enrollment information. The complete installation command from the enrollment email can be inserted into this dialog. The agent starts the enrollment and connects to the Management Server by clicking on "OK". After enrollment, the endpoint can be provided with jobs as usual.

## 5.4 Product Improvements in Detail

### 5.4.1 Windows Agent (bMA)

- The Compliance-Vulnerability Scan has been improved and now requires significantly less memory, but requires more temporary disk space.
- In the kiosk the assignment to the current device was simplified.
- The kiosk can be started via bMACmd. A shortcut can be created to the bmaCmd command on desktop to open the kiosk.
- Simplified IEM Enrollment. IEM endpoints can now be conveniently enrolled using the "Initial Configuration" menu item of the bMA Tray Notifier.
- Support for the deprecated disk image format (.bdi) has been removed.
- A SingleExeSetup for bMA installation is available, for usage with IEM enrollment.
- Bugfix: The ascertained boot time shows the last wake-up time instead of the real system boot time.
- Bugfix: On servers that have not activated bitlocker feature, an error is logged in bMA.log if bitlocker should be deactivated.

### 5.4.2 bMA on Mac

- Script execution is also possible on macOS 10.14.3
- Bugfix: A reinstallation of the agent is not possible on Catalina.

### 5.4.3 Management Center (bMC)

- The bMA installation command for a single IEM client can be generated by the clicking `Extras-New Registration` menu item on the client. This can also be sent automatically by mail if the mail server is configured. The enrollment of a Windows IEM client thus resembles the enrollment of an MDM device.
- Universal Dynamic Groups queries now also support client variables.

- New columns in the list view of Windows applications show used login bDS, installation command, uninstallation command and file for installation mechanism.
- New columns File Entries and Registry Entries in Inventory - Software Detection Rules.
- Under Software - Managed Software, the icon of the MSW product shows the set default release.
- There a new setting in BitLocker job type to deactivate BitLocker
- Restrictions for iOS device endpoints were extended.
- New download job Industrial Data for inventory of SIMATIC S7 available.
- Deploy-bDS files stored in the application can be opened directly for editing.
- New endpoint type "Industry Control Device" for creating a SIMATIC S7, including querying option using universal dynamic group and detection via network scan.
- Inventory job for SIMATIC S7 devices possible.
- Industrial control device endpoints are shown on the IT map.
- In the MSW overview, the link to the forum entry is now opened in the system default browser.
- On the Software - Applications - Overview page of a software application, a bDS file stored as a installation mechanism can be opened quickly in AutomationStudio.
- The status of the respective Windows security settings can be viewed in the client - overview page.
- Bugfix: For assets the cost center data was not exported.
- Bugfix: The commands 'Abort' and 'Set OK' for job does not change the time of 'Last Action'.
- Bugfix: To register a Mac device at least one free MDM license is required.

- Bugfix: A job generated automatically via the `Extras- Reinstall` command on a client partially boots into a wrong PE image.
- Bugfix: On an application the stored login bDS is not described correctly.
- Bugfix: On a client the command '`Extras - Shutdown/Restart`' displays a German error message on English systems, in case of an error.
- Bugfix: In the energy default values for monitors more consumption is calculated for a switched off monitor than for a monitor in standby mode.
- Bugfix: If a list of clients is imported in the job assignment dialog, the display name is needed instead of the host names in the imported data. (New: display name and host name is possible).

#### 5.4.4 Mobile Devices

- Knox support is now only shown for legacy Android devices.
- The geocoordinates for the LostMode can now be opened directly in the browser.
- Installation jobs and uninstallation jobs can be created by multi-select for several apps.
- Uninstallation jobs can be created directly from the app inventory of a device.
- Visibility of the widgets in the Android Enterprise Work Profile can be configured.
- New job step "`Execute command`" for iOS devices.
- System updates (OTA) are now configurable for dedicated devices and fully managed devices (Android Enterprise)
- Bugfix: The iOS SystemApps iMovie, Clips, iTunes U and GarageBand could not be distributed per job.
- BugFix: In rare cases database errors occur when using VPP licenses. A VPP-sync is no longer possible in these cases.

#### 5.4.5 Automation Studio

- It is possible to disable logging for individual actions.

- Note: When opening existing bDS files, a message will appear to convert the bDS script to the current format. bDS files created with Automation Studio 2020 cannot be executed by baramundi agents (bMA) smaller than 2020.

#### 5.4.6 bRemote

- Bugfix: In certain cases the connection is aborted and a new connection shows the error "The remote connection will not be established because another user already tries to open a connection."

#### 5.4.7 bConnect

- The registration of IEM clients can be controlled via the `EndpointEnrollment Controller`.
- A high-performance query of job data has been added to the Job Instance object.
- Industrial Control Device (ICD) jobs can be read, created and changed.
- New controller "ServerState" allows reading the status information of each server module.
- Android Enterprise devices and dedicated devices can be created.
- Bugfix: Reading hardware data for mobile devices leads to errors and does not deliver results.

### **5.4.8 License Management**

- The setup was decoupled from the bMC setup. It is still included in the overall setup.
- Bugfix: When importing the inventory data, performance problems and SQL error messages may occur.
- BugFix: Under certain circumstances the license utilization is determined incorrectly.

### **5.4.9 ICD – Industrial Control Devices**

- New module "IC Inventory" for the administration of industrial devices and inventory of SIEMENS SIMATIC devices.
- New job type for IC-Devices.



## 6 Release 2019 R2

### 6.1 Android Enterprise: Work Profile

#### 6.1.1 Native containment

The transparent data separation in iOS is just one approach, deeply embedded in the operating system, for keeping private and company data separate. Android's Work Profile goes one step further: The user receives an entirely separate area for business apps and data on his smartphone or tablet. This area is managed by the company and is not visible to apps in a private context. The concept of separation exists in both directions, for example the administrator cannot see which apps the user has installed privately.

This resolute form of app and data separation, and thus isolation of all information, is only possible using the native solution within Android Enterprise.

Seamless integration within the firmware means that security updates from device manufacturers can also be applied immediately, ensuring compatibility. Similarly, all apps from the Enterprise PlayStore can also be used without having to request specially customized or wrapped versions from the manufacturer.



Figure 40 - Symbolic representation of the Work Profile

#### 6.1.2 The Work Profile in detail

With the bMS 2019 R2, the administrator now has the choice between “Fully Managed Device” – introduced in bMS 2018 R2 – and the “Work Profile”. While the Fully Managed Device is intended for business use only (COBO), the Work Profile allows company devices to be used for private purposes and even private devices to be used for company purposes (BYOD) while being compliant with data protection policies.

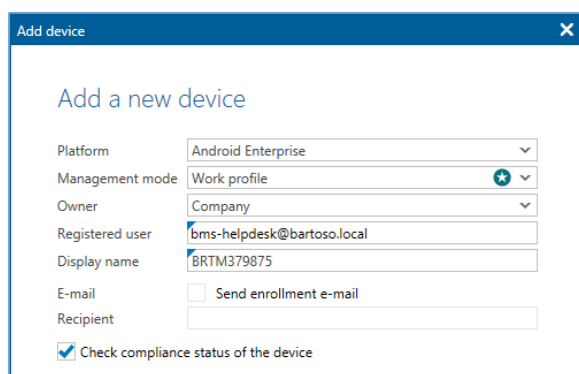


Figure 41 – Enrollment dialog for the Work

The mode in which the device is to be operated is defined during enrollment.

On the device itself, the user installs the baramundi EMM Agent from the Play Store and, for example, adds it to management via a QR code.

During the enrollment process, the user receives instructions on how to use the Work

Profile (manufacturer-dependent), while the agent provides the environment. Once successfully configured, the business environment is available to the user.

The style of the Work Profile varies depending on both the device manufacturer and the version of Android used. Private and company apps are either sorted into their own tabs or simply displayed together in a list. In both cases, the user can clearly recognize company apps by the briefcase icon.

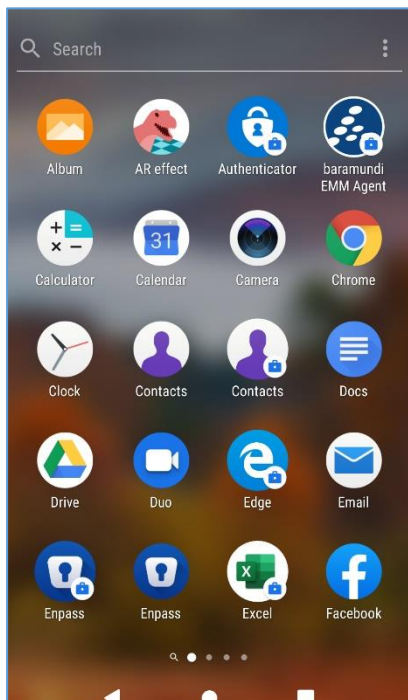


Figure 42 - The Work Profile on a Sony XA2 running Android 9

The administrator can easily specify which apps are available to the user via the app list in the baramundi Management Center.

This is also one of the great strengths of the Work Profile:

A given app can be installed from the PlayStore either by the user or by the administrator via bMD.

The user's app is downloaded, installed and configured by the user. It has no access to data

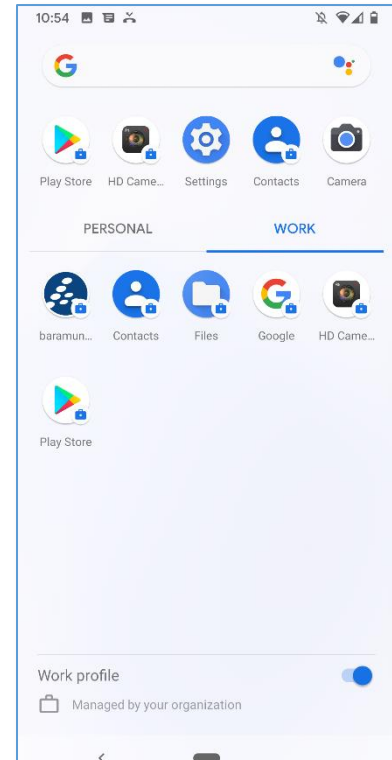


Figure 43 - The Work Profile on a Google Pixel 3 running

within the company environment. The app in the Work Profile can be installed and configured by the administrator and has no access to the user's private data. In addition, the user can use apps in the business PlayStore that have been checked, approved and pre-configured by the

Of course, security settings and restrictions can also be applied to the Work Profile. Note that these settings can now be applied specifically to the company environment. These restrictions then only apply in the Work Profile. For example, the administrator can prohibit use of the camera in the company environment, but the user can still use it in a private context.

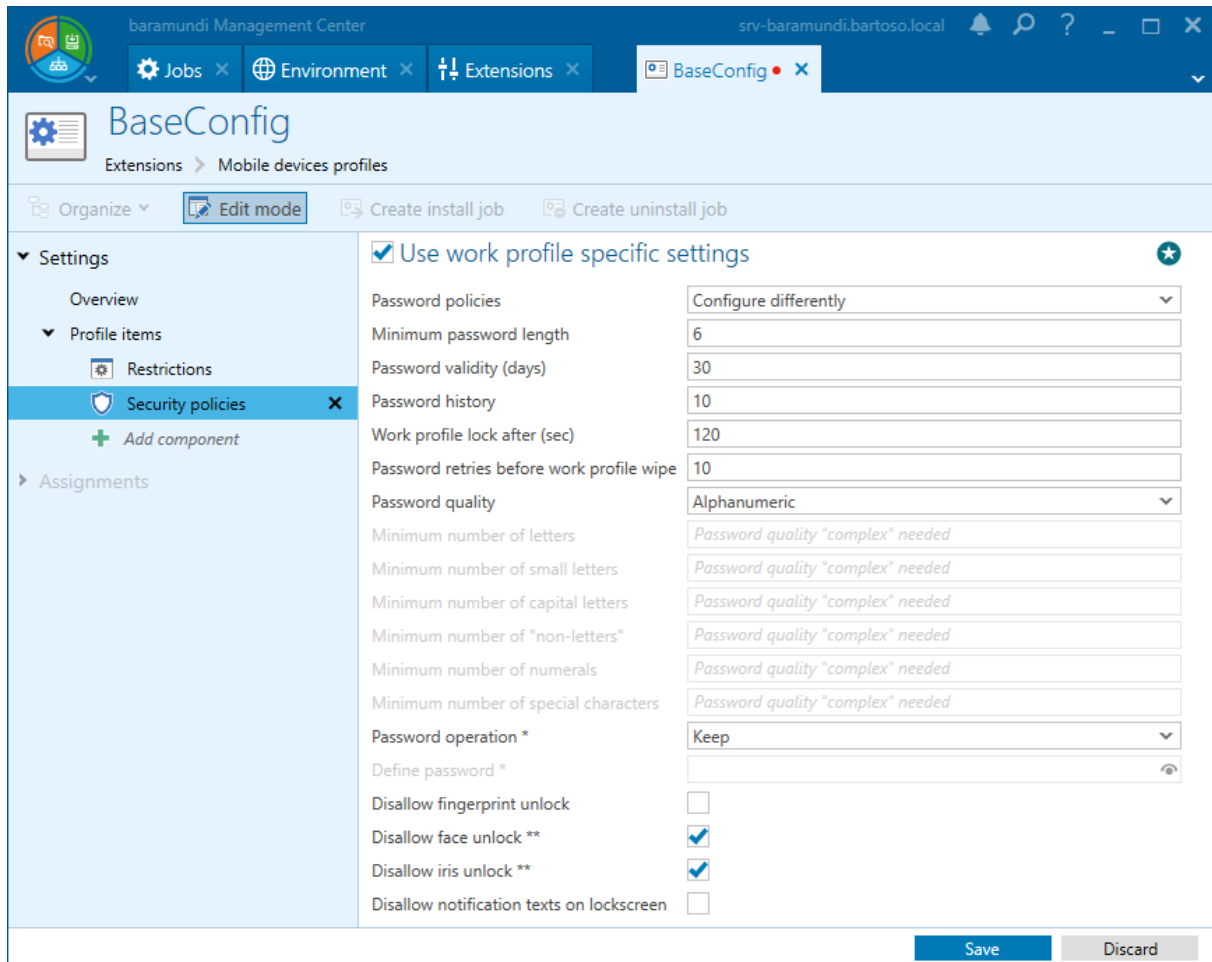


Figure 44 – Security settings for the Work Profile

When using the Work Profile, the administrator has only limited options to restrict device functions, since these apply to the entire device and would therefore also restrict the private area. In the baramundi Management Center, the settings are clearly displayed by application area and can be enabled and used as required.

The Android Enterprise Work Profile and other controls to finely tune data separation on iOS are included in the *baramundi Mobile Devices Premium* module. The module adds these data separation functions to all previous functionalities of the *baramundi Mobile Devices* module.

## 6.2 Windows BitLocker

### 6.2.1 Transparency

BitLocker securely and transparently encrypts volumes on a Windows system to prevent data being accessed by simply removing and reinstalling the disk. In addition, the system can be protected by a PIN when booting. This ensures that the system can only be started by an authorized person.

In order to keep track of which systems are fully encrypted, not encrypted at all, or only partially encrypted, the baramundi Management Agent now also inventories the status of BitLocker on managed systems and provides detailed information on the encryption status of the various partitions.

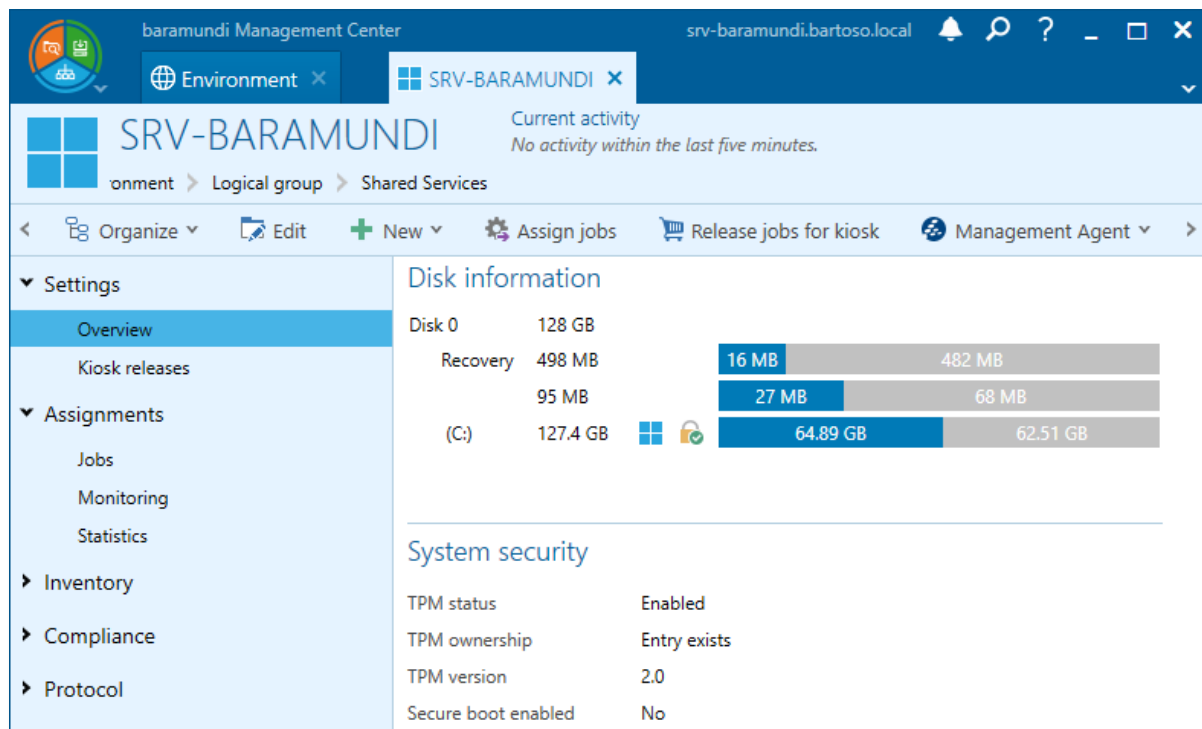


Figure 45 - BitLocker information on the overview page of a Windows endpoint  
This information is displayed on the Windows endpoint overview page and is also available as a filter for Universal Dynamic Groups (UDG). This provides a quick and convenient summary of the encryption status of the managed endpoints.

### 6.2.2 Configuration

In order to achieve reliable protection by BitLocker, it must first be configured and activated properly.

To this reason, the baramundi Management Suite now allows you to manage your own BitLocker configuration profiles. The administrator defines the encryption method and the drives to be encrypted in a profile. This allows you to specify whether only the system drive should be encrypted, or all data drives as well. It is also possible to specify whether a PIN is required for the operating system start, with corresponding complexity. This PIN is automatically generated and set according to the rules of the profile when encryption is set up.

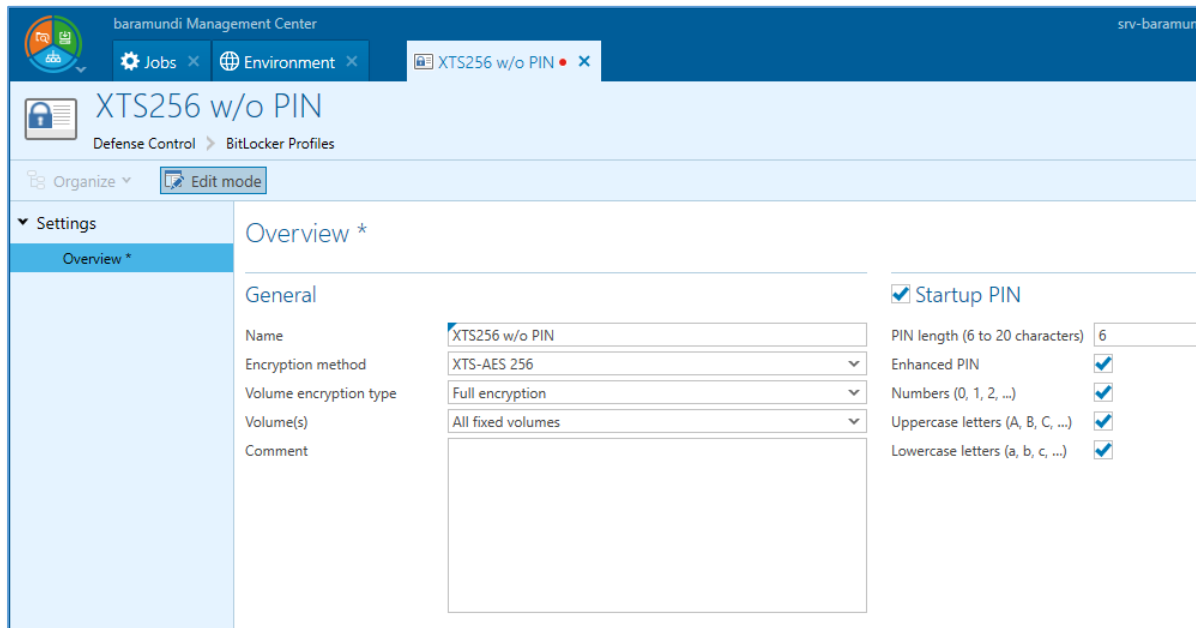


Figure 46 - Configuration profile for BitLocker

### 6.2.3 Recovery keys and PIN

The recovery keys and PIN are stored in the bMS when encryption is activated via baramundi. The recovery keys for the volumes are regularly inventoried and also displayed. This information is a valuable part of the BitLocker recovery strategy for the administrator.

BitLocker recovery keys

The BitLocker recovery key can be used to unlock BitLocker protected disks.

The following keys are known for the device **SRV-BARAMUNDI**:

Partition	System partition	Generated recovery key	Inventoried recovery key	Last up
(C:)	Yes	695200-277541-601106-4549	695200-277541-601106-454960-184690-232485-399300-437349	10/8/2

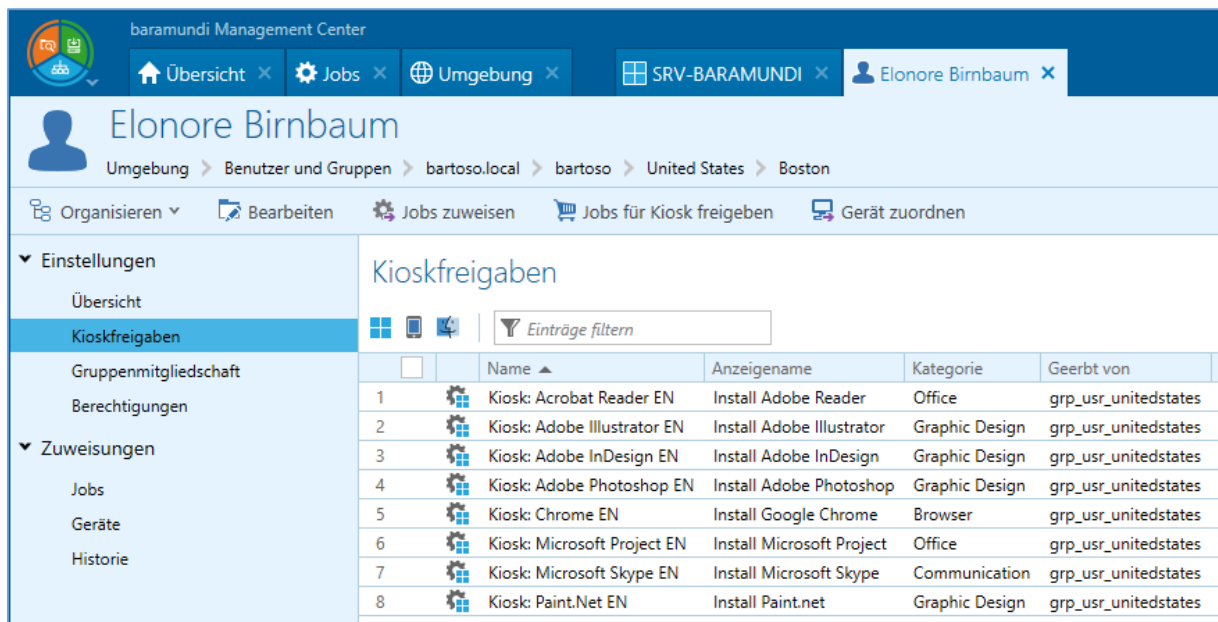
Copy to clipboard
Close

Figure 47 - List of recovery keys

This data is stored in encrypted form and secured by the baramundi permissions concept. This means that an administrator can only access the recovery keys for systems for which he has explicitly been granted this permission.

## 6.3 General Improvements

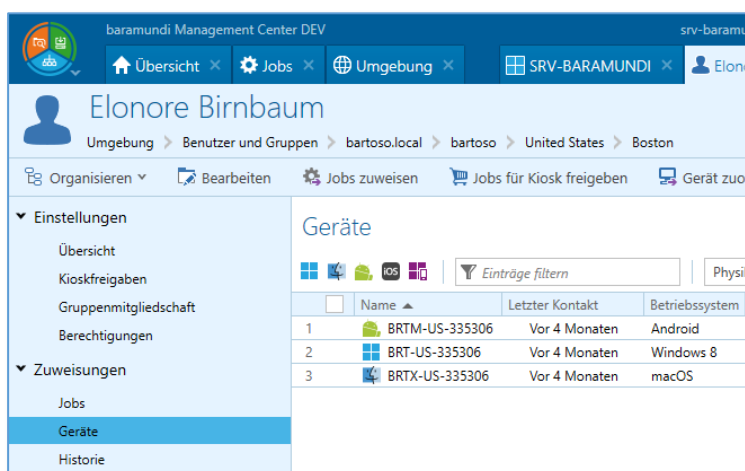
### 6.3.1 Kiosk: Overview of job and device assignments to users



	Name	Anzeigenname	Kategorie	Geerbt von
1	Kiosk: Acrobat Reader EN	Install Adobe Reader	Office	grp_usr_unitedstates
2	Kiosk: Adobe Illustrator EN	Install Adobe Illustrator	Graphic Design	grp_usr_unitedstates
3	Kiosk: Adobe InDesign EN	Install Adobe InDesign	Graphic Design	grp_usr_unitedstates
4	Kiosk: Adobe Photoshop EN	Install Adobe Photoshop	Graphic Design	grp_usr_unitedstates
5	Kiosk: Chrome EN	Install Google Chrome	Browser	grp_usr_unitedstates
6	Kiosk: Microsoft Project EN	Install Microsoft Project	Office	grp_usr_unitedstates
7	Kiosk: Microsoft Skype EN	Install Microsoft Skype	Communication	grp_usr_unitedstates
8	Kiosk: Paint.Net EN	Install Paint.net	Graphic Design	grp_usr_unitedstates

Figure 48 - Jobs visible to the user in the Kiosk

There are also new features for displaying users and groups, and for listing assigned jobs and devices. So now it is possible to see via users and groups under the environment, which jobs users can see in the Kiosk as soon as they log in. Users' group memberships are also taken into account to display inherited jobs.



	Name	Letzter Kontakt	Betriebssystem
1	BRTM-US-335306	Vor 4 Monaten	Android
2	BRTM-US-335306	Vor 4 Monaten	Windows 8
3	BRTX-US-335306	Vor 4 Monaten	macOS

Figure 49 - List of the user's devices

In addition to job assignments, the devices on which this user is stored as a registered user are also listed.

## 6.3.2 License Management

*baramundi License Management* offers a compact and simple way of taking commercial information from license management into account and thereby achieving better transparency of the licenses currently available in the company.

The new version now features direct license management, a display of devices, and various workflow improvements.

### 6.3.2.1 Concept

The ledger provides an overview of the products presented with the allocated licenses and the corresponding installations from the baramundi inventory.

In the new version, it is possible to create licenses ① directly alongside the initial setup of a product ①. Assignment ② is therefore possible in both directions.

The installations (software recognition rules) from the baramundi inventory are assigned to the corresponding product ③. In 2019 R2, the respective device information is also displayed according to the installations.

The view of devices ④ shows the devices managed by baramundi. For a more comprehensive view of the ledger, it may also be necessary to consider devices not managed by baramundi. For example, devices of an offline instance can be created manually ⑤ and directly assigned to a product.

Information on contracts ⑥ can be created and additionally linked to products and/or licenses. A report ⑦ in Excel offers different views for flexible processing and to create custom reports.

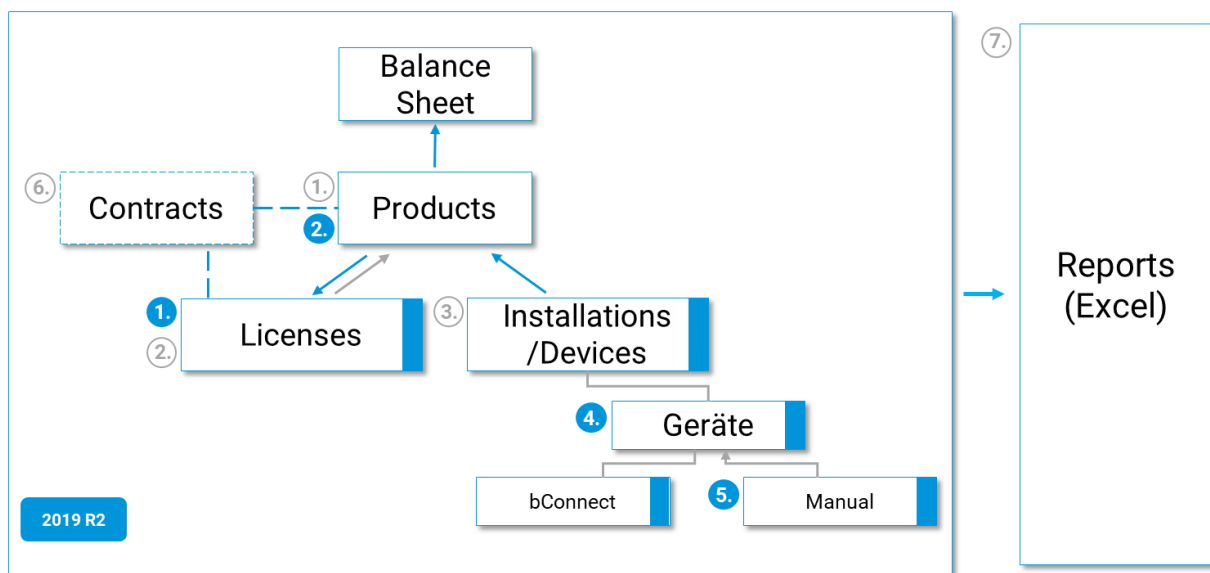


Figure 1 – Overall concept 2019 R2



### 6.3.2.2 Direct license management

The direct view of created licenses means it is possible to get an overview of all information on the respective license.

The compact summary shows the license inventory, the licenses already assigned to a product, and any licenses that are still available. As a result, the user can easily recognize the current situation and make appropriate adjustments.

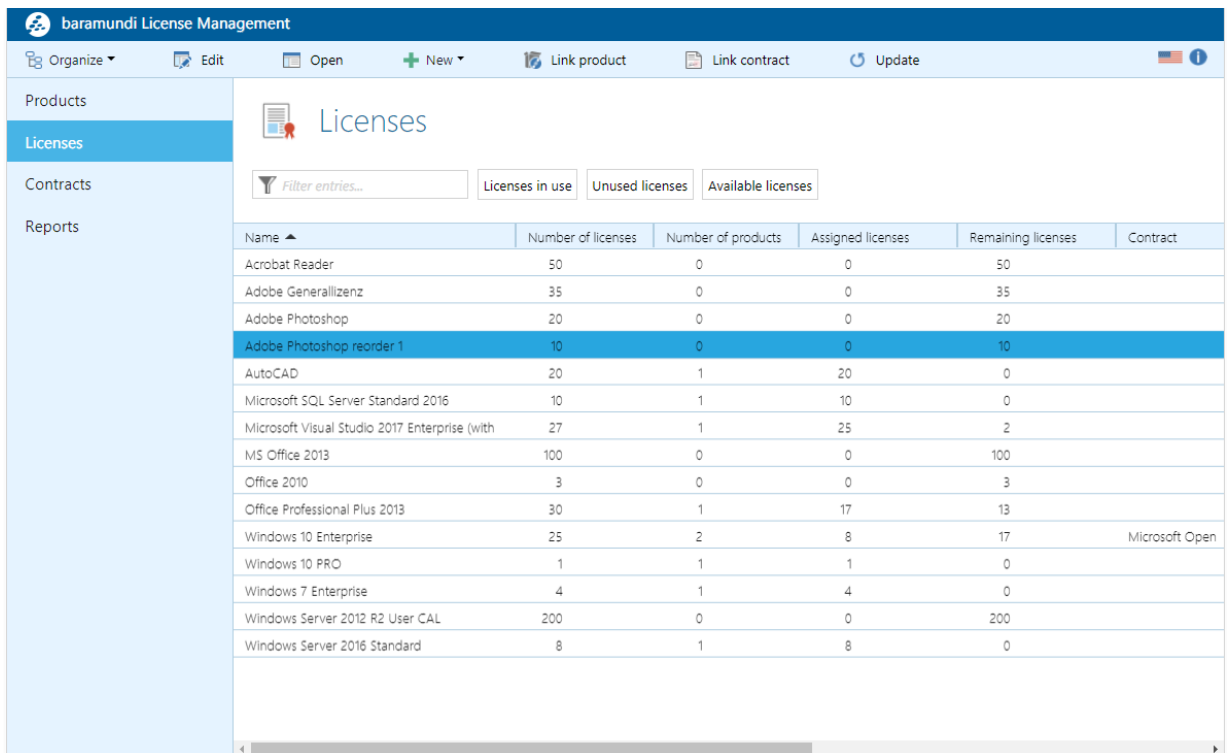
A license can be created without first defining a product.

Subsequently, the created license can be directly linked to a product or contract.

Filters and search functions make managing licenses easier. The multiple use property can be represented with the specific number of usage rights.

The original license can be copied. This template makes it easier to reuse information that has already been created in order, for example, to quickly purchase additional licenses.

Reports are enhanced with information from direct license management.



Name	Number of licenses	Number of products	Assigned licenses	Remaining licenses	Contract
Acrobat Reader	50	0	0	50	
Adobe Generalizenz	35	0	0	35	
Adobe Photoshop	20	0	0	20	
Adobe Photoshop reorder 1	10	0	0	10	
AutoCAD	20	1	20	0	
Microsoft SQL Server Standard 2016	10	1	10	0	
Microsoft Visual Studio 2017 Enterprise (with	27	1	25	2	
MS Office 2013	100	0	0	100	
Office 2010	3	0	0	3	
Office Professional Plus 2013	30	1	17	13	
Windows 10 Enterprise	25	2	8	17	Microsoft Open
Windows 10 PRO	1	1	1	0	
Windows 7 Enterprise	4	1	4	0	
Windows Server 2012 R2 User CAL	200	0	0	200	
Windows Server 2016 Standard	8	1	8	0	

Figure 2 – Licenses direct view

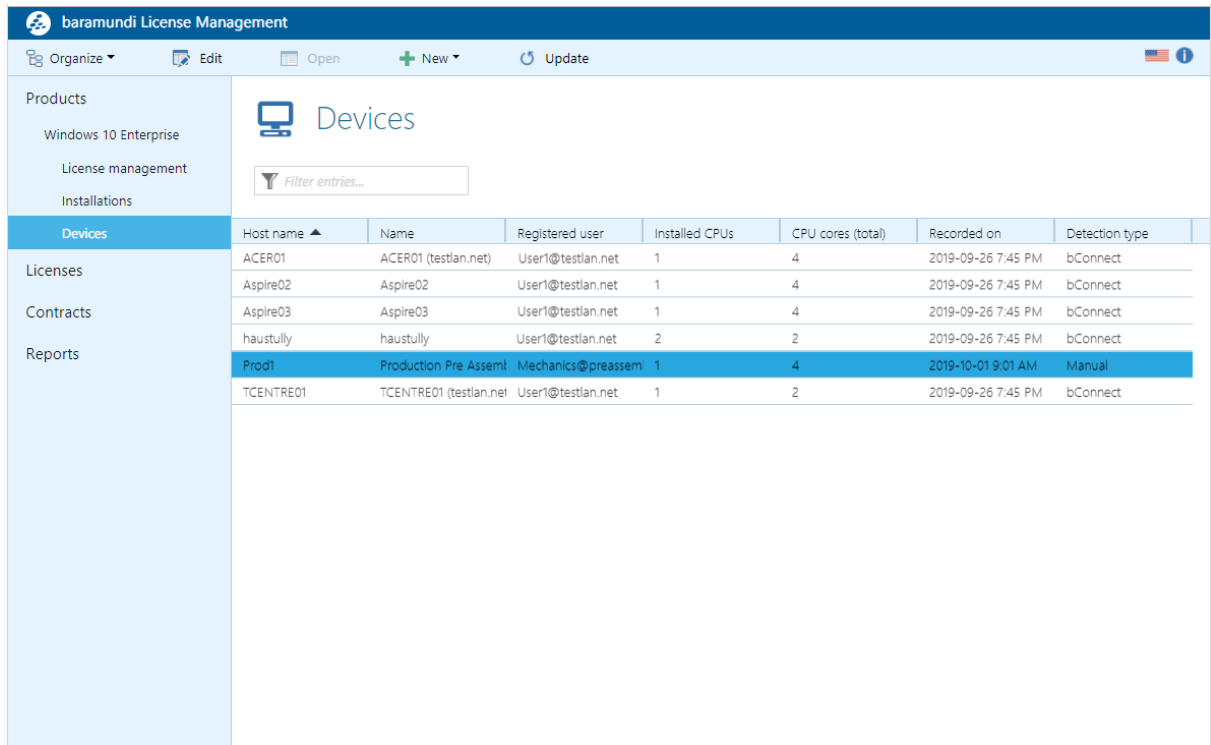
### 6.3.2.3 Device information in products

The table shows devices recorded by *baramundi Inventory* in relation to the installations linked to the product. This makes it possible to link to the “consumers” of the respective license. License-relevant information such as CPU, cores or the registered user is displayed. From the point of view of a license ledger, it is not just those devices recorded during the inventory that might be relevant; so it is also possible to create devices manually. For example,

devices from an “offline instance” such as production or running a Linux OS can be included in an overall view.

The display differentiates between devices from *baramundi Inventory* and devices created manually. Once created manually, devices can be reused in other products.

Reporting has been improved to include information relevant to devices.



Host name	Name	Registered user	Installed CPUs	CPU cores (total)	Recorded on	Detection type
ACER01	ACER01 (testlan.net)	User1@testlan.net	1	4	2019-09-26 7:45 PM	bConnect
Aspire02	Aspire02	User1@testlan.net	1	4	2019-09-26 7:45 PM	bConnect
Aspire03	Aspire03	User1@testlan.net	1	4	2019-09-26 7:45 PM	bConnect
haustully	haustully	User1@testlan.net	2	2	2019-09-26 7:45 PM	bConnect
Prod1	Production Pre Assem	Mechanics@preassem	1	4	2019-10-01 9:01 AM	Manual
TCENTRE01	TCENTRE01 (testlan.net)	User1@testlan.net	1	2	2019-09-26 7:45 PM	bConnect

Figure 3 – Device display

#### 6.3.2.4 Other functions

If you are in editing mode and have not saved your entries, the system informs you before leaving the view that unsaved entries will be lost.

Users who want to display the value of the license in different currencies can select the respective national currency that matches the procurement process.

A free text filter in all views with table displays makes it easy to quickly narrow down and search entries. Users can find the information they want in a targeted manner.

Other direct actions such as linking license, contract and product make it simpler to use.

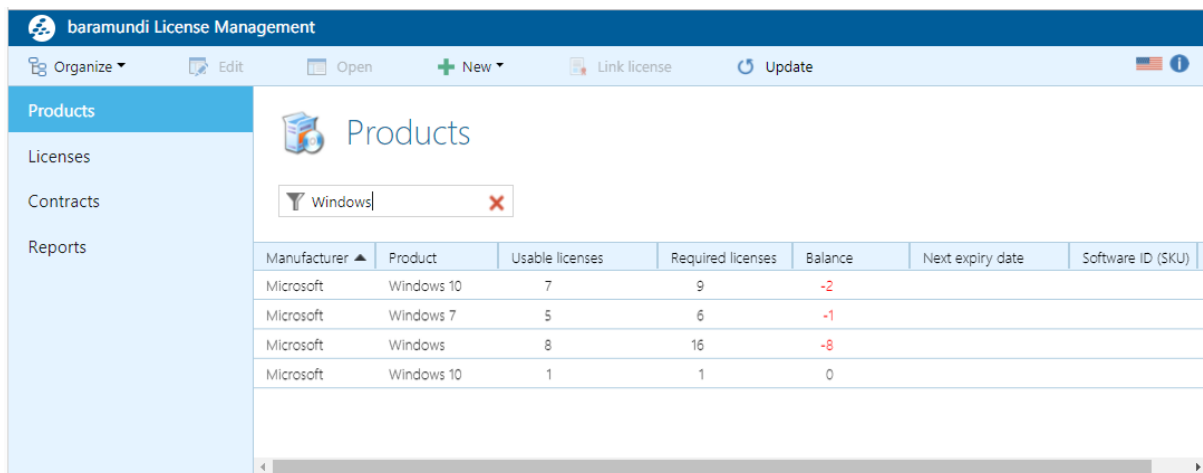


Figure 4 – Quick search filter

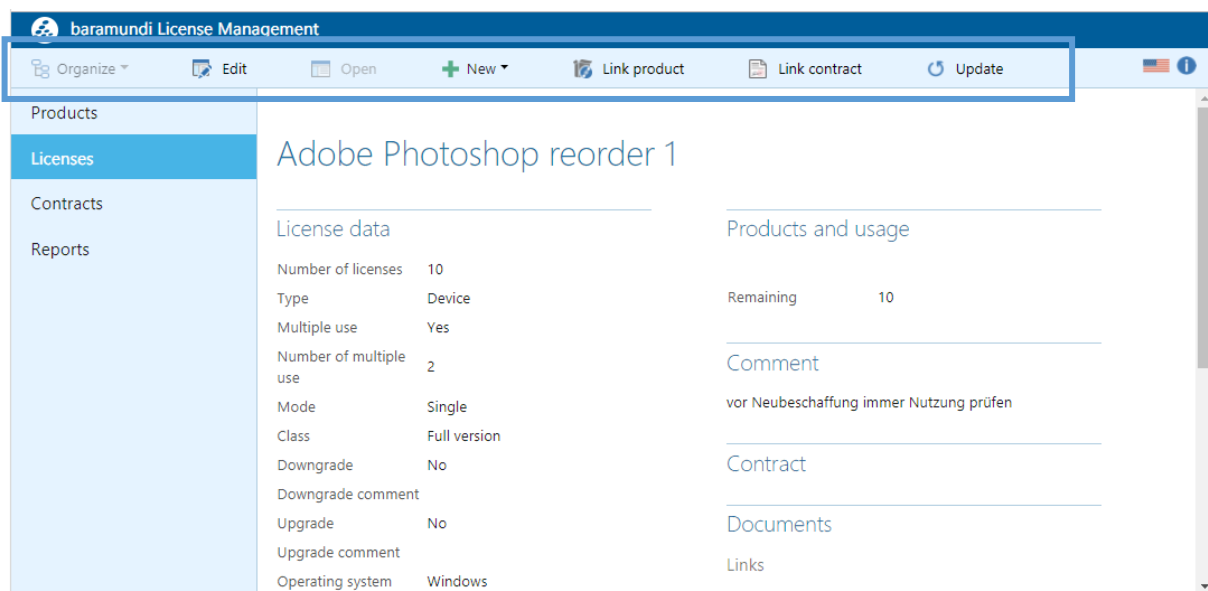


Figure 5 – Direct actions

### 6.3.3 Job assignment dialog

The job assignment dialog in the bMC has been revitalized. The view is now adapted to the modern layout, performance is significantly improved and new assignment options have been added. A uniform, modern dialog is now available in the bMC for all job types.

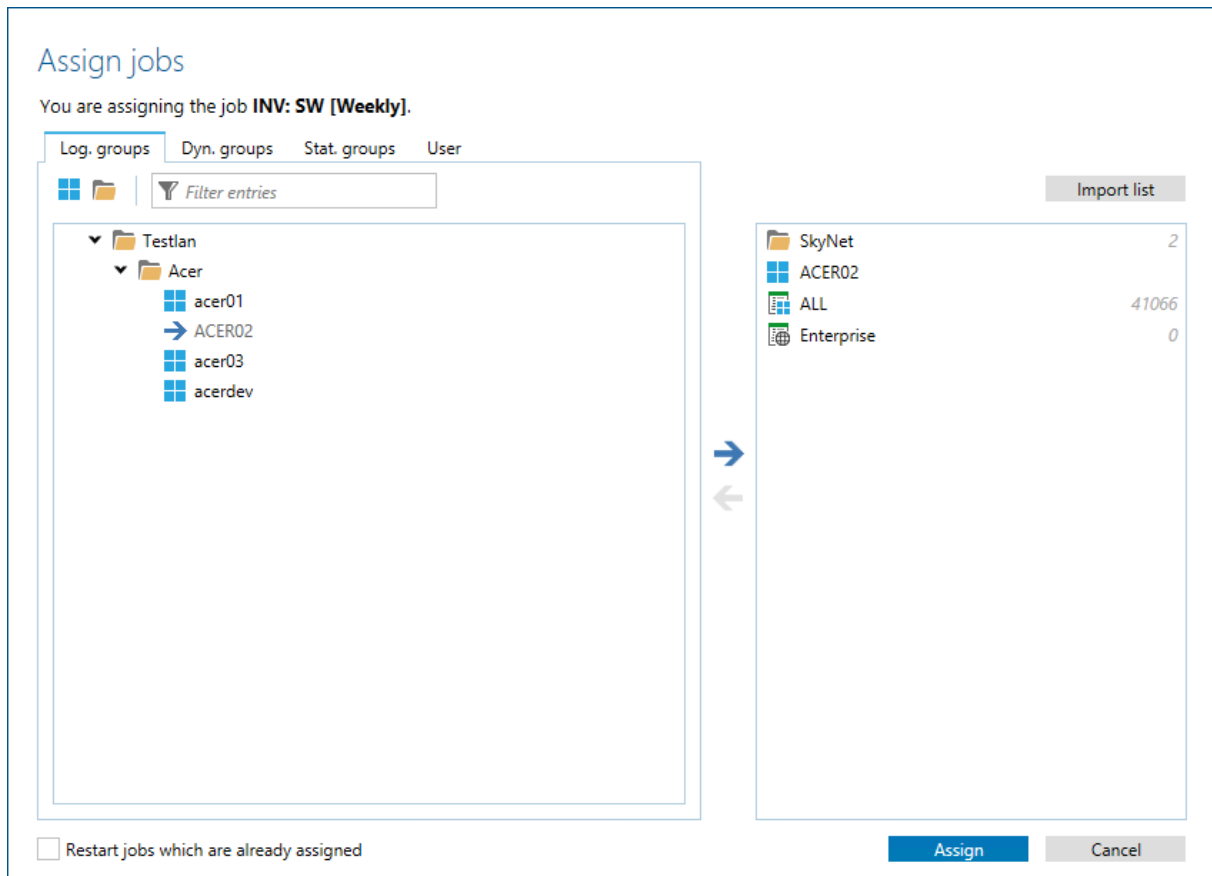


Figure 50 - New job assignment dialog

Administrators now have the ability to assign jobs to individual endpoints, to logical, (universal) dynamic or static groups, as well as to users.

It is also possible to import a list of endpoints into the assignment dialog. Companies often already have lists of endpoints on which, for example, certain software is to be rolled out. These existing lists can now be used to quickly and easily assign a job to these devices. A defined list form, as well as useful error messages, help administrators avoid errors when importing lists or when assigning jobs.

### 6.3.4 Managed Software

*baramundi Managed Software* contains more than 70 applications and allows administrators to check their IT environment for new software versions and updates and install them promptly. Given the large number of versions, it is important that tests and roll-outs can be performed quickly and effectively.

In 2019 R2, the performance of the *bMSW* view has been optimized and setting release levels is now much faster.

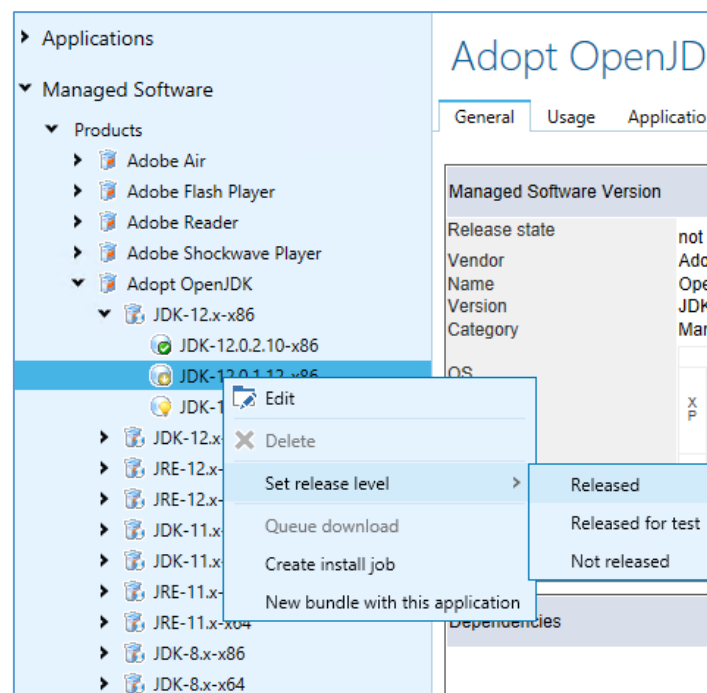


Figure 51 - Define release levels in the context menu

In addition, the files required for an MSW installation can now be downloaded quickly and easily to perform update jobs more quickly and without error messages.

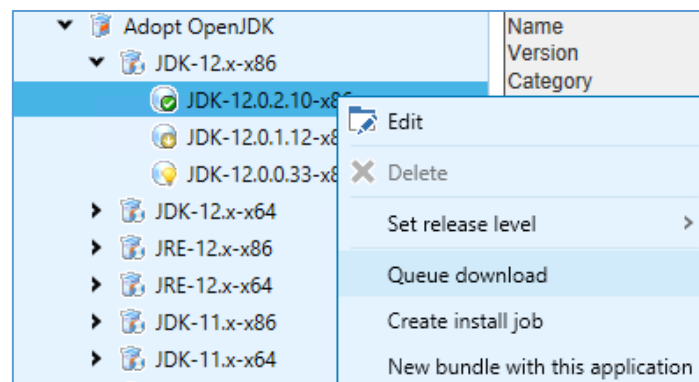


Figure 52 - Create download jobs for missing files

## 6.3.5 Documentation

In recent years, the baramundi Management Suite has gained considerable functionalities. All these new and old views, functions and procedures were previously documented in the baramundi online help and in the manual.

With the release of 2019 R2, a new baramundi documentation portal will be launched: docs.baramundi.com will in future be used to display all documentation content in one place.

### 6.3.5.1 Online and offline availability

An important factor for documentation is the availability of information. If administrators press the F1 key in the baramundi Management Suite, in future they will also be taken to the corresponding help page. As of 2019 R2, this will take them to the corresponding online reference. This also ensures that the correct and up-to-date documentation is always displayed.

In the bMC, however, there is also the option to switch to an offline version of the documentation if, for example, online availability is not available or desired.

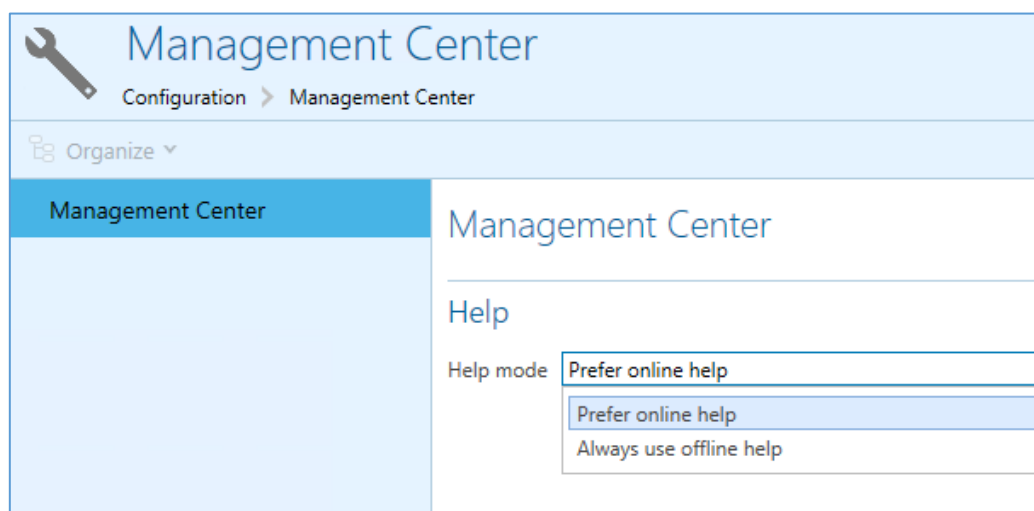


Figure 53 - Choice of online or offline documentation

### 6.3.5.2 Search & find

It is a great challenge on the one hand to provide as comprehensive documentation as possible and on the other hand not to overload the person searching with too much information. The new baramundi documentation uses various approaches to overcome this challenge. Firstly the F1 references – clearly arranged and analogous to the display in the bMC – are displayed in the main “References” navigation. The aim here is to provide quick help on menus and dialogs in the bMC.

In addition, related content such as on the subject of Android Enterprise or Kiosk, is summarized in the “Topics” section – at this point entirely detached from the place it appears in the bMC.

Detailed instructions on the main topics can then be found in the “Tutorials” section, replacing the baramundi manual.

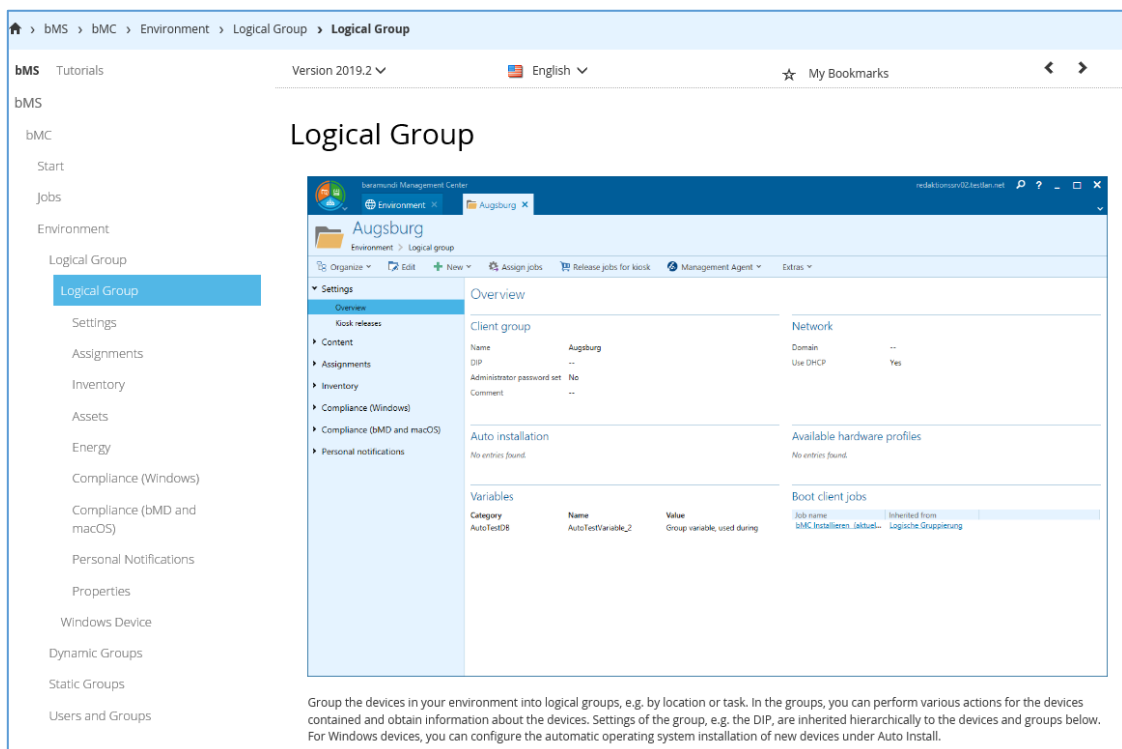


Figure 54 – Detailed information in the new documentation

Secondly, the information is not just structured into different subjects: Information can also be presented using a drill-down search. If you search for a specific search term, the results are divided into matching criteria and can be filtered accordingly.

This makes it much easier to move from a very large set of results to a smaller list of search hits.

The individual search results can then also be stored in personal bookmarks and saved for a later date.

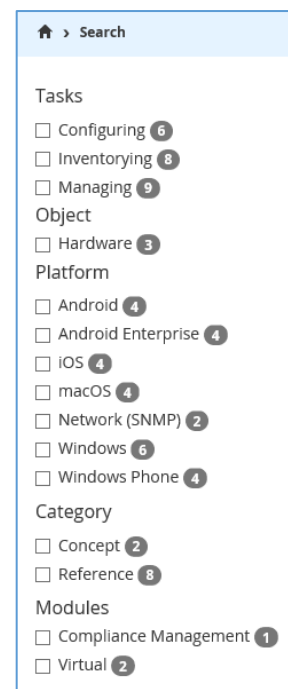


Figure 55 - Drill-down search

### 6.3.5.3 Networking with other baramundi portals

In addition to the availability, up-to-dateness and ease with which documentation content can be found, it is equally important that content from other sources is networked with it. For example, if an administrator is looking for information about how to configure Kiosk, he can find

it in the new baramundi documentation. But if he wants to know how to change the language of the Kiosk, he can find this information in the knowledge base or related topics in the forum. In the new baramundi documentation portal, exactly this information is linked at suitable points in order to be able to answer both general and specific questions.

### 6.3.6 Notification Center

In 2019 R2 a new Notification Center has been introduced to the bMC. In the past, important notifications were displayed as a dialog when the bMC started up. These messages include notifications about expired Apple Push certificates, communication problems with Apple in the case of DEP/VPP, or license warnings. These and similar messages are now displayed together in the new Notification Center. The administrator can read and react to important current and older messages at any time via an icon in the top right corner of the window.

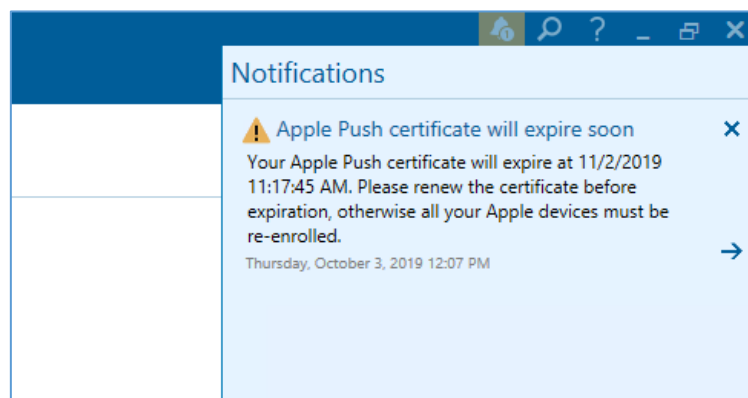


Figure 56 - New Notification Center in the bMC



### 6.3.7 Security

As already announced with the release of bMS 2019 R1, backwards compatibility with old agents prior to version 2015 R2 will be removed with release 2019 R2.

In order to maintain communication between Windows endpoints and baramundi Management Server, a current agent, at least version 2015 R2, must be installed on all Windows endpoints before updating to bMS 2019 R2. Automatic bMA update should therefore always be enabled. We strongly recommend that you use the same version of server and agent and set the communication mode to "Default (recommended)". This is the only way to ensure cryptographically secure communication between baramundi Management Agent and baramundi Management Server.

The 2019 R2 release includes several security-related enhancements.  
We therefore recommend a timely upgrade to the current version.

## 6.4 Product Improvements in Detail

### 6.4.1 General

- The baramundi setup files have been substantially revised.

### 6.4.2 Windows Agent (bMA)

- The bMA-bServer communication has been updated and is now done in the same way as with IEM clients via HTTPS. In order to guarantee a prompt job execution even on clients that change the network connection, the UDP channel from bServer to bMA is still available.
- Log files in case of erroneous bDS for user setting (UBDS) are now stored under "%LocalAppData%\baramundi\BDS". In previous versions these were stored under "%ProgramData%\baramundi\BDS".
- Bug-fix: With active LSA protection, mode execution of actions in LocalSystem context is not possible.

### 6.4.3 Server (bServer)

- The access rights for the folder "%ProgramData%\baramundi" have been restricted.
- The database manager can set an active database via parameters.
- Bug-fix: The automatic client acquisition via PXE server is not possible if the new licensing is used.
- Bug-fix: The server and the database manager do not work on systems with activated LSA protection mode.

### 6.4.4 Management Center (bMC)

- New dialog for assigning jobs to devices.
- Under "Configuration - License Configuration" the license configuration for baramundi can be viewed and changed. This data is only displayed if you have switched to the new license. Old licensing is still valid and visible under "Configuration - Server - Licenses"

- The new help system (Cobrili) can be configured under "Configuration - Management Center".
- Log files and error reports are now stored in the user directory "%LocalAppData%\baramundi\Logs". In previous versions, these were stored under "%ProgramData%\baramundi\Logs".
- Warning messages are no longer displayed as popup when starting the bMC, but as notification in the bMC.
- As long as there is a "\*" security profile, a notification is displayed.
- The communication modes "Compatible with 2015 R1/2014 R2" and "Compatible with 2014 R1 and older" which could be set under "Base Settings - Communication - Management Agent Options" have been removed.
- Under "Server - Base settings - Communication" the backward compatibility to bMA with the versions 2015R2 to 2019R1 can be configured.
- New special right "BitLocker" for Windows clients.
- The disk information under "Windows - Client - Overview" has been completely revised. New data will only be displayed after the bMA has been updated to 2019R2.
- The TPM status and TPM version are displayed under "Windows - Client - Overview - System Security".
- Universal groups contain query options for BitLocker, TPM and new disk information.
- The software version is now displayed in the "Software - Overview" view under Dependencies.
- A new database maintenance task of the type "Clean up software detection rules" removes all automatically created rules that were not found on any clients. This can reduce the size of the software inventory rule set.
- The action "Database maintenance task - Export audit log" now deletes only the exported entries from the database. The number of revision log entries to be exported in the DB maintenance task is configurable.
- baramundi password type variables are now stored encrypted in the database.
- The type of a baramundi variable can no longer be changed.

- The action "bDX-Export" was extended by the option "Export automatic assignment" setting.
- The view "Managed Software - Products" is completely revised and the performance significantly improved.
- Under "Software - Managed Software" the download status is displayed in the bMC. Additionally, the download can be initiated from this view.
- Under "Software - Managed Software" the release level can be set directly via the actions menu.
- Tabs in edit mode can be saved with Ctrl+S key combination.
- By clicking "Open baramundi license activation portal" under "Configuration – License configuration" a license can be activated using a license ticket.
- Bug-fix: The names of "Personal Notifications" are incorrect from the second copy onwards.
- Bug-fix: The HTML-view sporadically shows a "problem solving page of baraNet" as error page.
- Bug-fix: If the view "Open group as tab - Inventory asset content" is sorted by the column Assigned, a SQL error message is displayed.
- Bug-fix: Deactivated clients are not displayed correctly in the "MSW Installed on" view.
- Bug-fix: A bDX container with files containing Unicode characters is exported incorrectly and thus cannot be imported.
- Bug-fix: The detail view of an asset does not show names and categories.
- Bug-fix: Under "Patches - Overview - Patches tab" the links of the type MS\*2019 do not work.
- Bug-fix: The jobs created via the button "Create installation job" do not use default values for job parameters.
- Bug-fix: The jobs created with the button "Create uninstall job" do not contain any useful steps if no uninstall command is stored in the software.
- Bug-fix: The Excel export cannot be used with Open Office programs.

- Bug-fix: If a file rule is added to an automatically generated software detection rule, the rule is not marked as manually generated, thus may be evaluated incorrectly during import.
- Bug-fix: The "Registered User" on the Windows device cannot be set correctly if there is no UPN in the Active Directory.
- Bug-fix: In "Personal Notification", the detail view sometimes shows a wrong time.
- Bug-fix: If the variable `{Notification.EventsWithLinks}` is used for "Personal Notification", the automatically generated email contains a link, which cannot be opened in Outlook.

#### **6.4.5 bConnect**

- The primary IP can be set via bConnect when creating and updating a Windows endpoint.
- "CustomStateType" and "CustomStateText" can be set via bConnect when updating a Windows endpoint.
- Bug-fix: The creation of OrgUnits for Apps and Applications results in an error.
- Bug-fix: Changing the name of mobile devices and Macs is not possible.

#### **6.4.6 Mobile Devices**

- When enrolling DEP devices, six setup dialogs can now be skipped.
- The SSL certificates have been modified to be compatible with iOS13.
- New restrictions for iOS13 added.
- Bug-fix: The action "Apps - Android Enterprise - Update Apps" in certain constellations returns "Managed Play Store Apps could not be synchronized" error.
- Bug-fix: If "Enrollment of mobile devices via gateway" is used, a SCEP certificate request for iOS is not possible.

#### **6.4.7 OS-Install**

- Compatibility with Windows 10 Version 1909.

- Windows 10 master images now use MultiSource-Unattended.xml by default.
- The unattend.xml entry "install to available Partition" is now also set dynamically for server operating systems.
- If a hard disk is included in the hardware profile, "partition types to be ignored" are no longer preset.

#### **6.4.8 Kiosk**

- Bug-fix: Device icons are scaled incorrectly in Internet Explorer.
- Bug-fix: Filters are lost when navigating back to the start page.

#### **6.4.9 License Management**

- Navigation between licenses and contract has been improved.
- New license node for direct management of licenses independent of the product.
- Copy functionality for licenses to be able to map a license replenishment.
- A search function for all products and contracts has been implemented.
- The data privacy option "Display endpoint user identities" is checked during login.
- New hint message when leaving the input field unsaved.
- The bConnect address can be configured.
- Error messages for failed logins have been improved.
- The currency is now stored in the numeric value regardless of the selected language. During migration, the value of the currency is not set.

#### **6.4.10 OS-Customization Tool**

- New area "Privacy" to preconfigure activity history, app permissions, diagnostics and feedback, speech recognition and clipboard.
- The log file now contains the version of the OS CustomizationTool.
- Bugfix: Temporary mount folders are not deleted.

## 7 Release 2019

### 7.1 Windows 10 Configuration

Windows 10 allows many configuration options during installation.<sup>13</sup> The baramundi OS Customization Tool<sup>14</sup> enables the most important settings to be configured using a graphical interface when preparing the installation image.

Using this tool, IT administrators can, for example, make an important contribution to data protection, as there are some Windows apps and functions that do not, or do not fully, meet the provisions of the EU GDPR. The OS Customization Tool permits IT administrators to disable such functions and perform configuration in accordance with their corporate compliance guidelines.

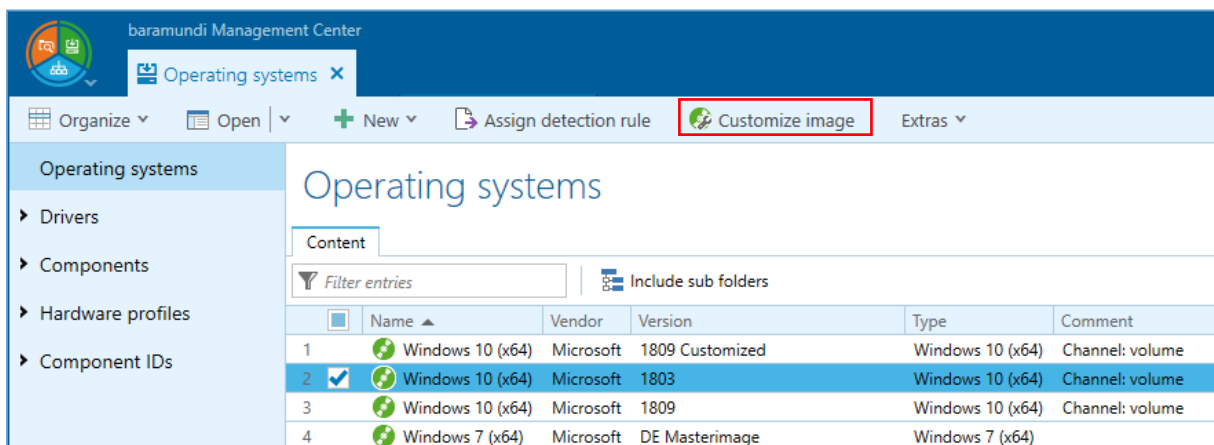


Figure 57 - Calling the OS Customization Tool in the Operating Systems area

#### 7.1.1 Versatile Customizations Options for a Windows Image

There are a large number of options for configuring a Windows image and some of these settings are complex. This is why similar options are clearly bundled into themes as a way of addressing this complexity.

To avoid having to perform each configuration again, it is possible to store the customizations in a configuration template and reuse them for further images as necessary.

<sup>13</sup> Configuration options are dependent on the Microsoft Windows Edition (for example Pro, Enterprise)

<sup>14</sup> Provision via baramundi Managed Software (freely available area)

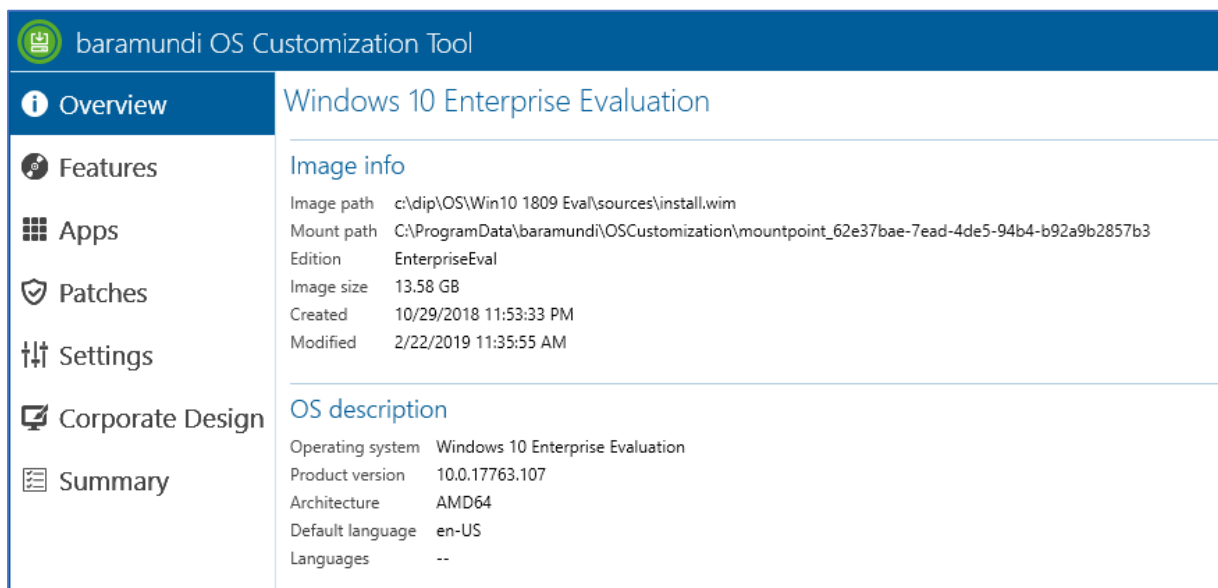


Figure 58 – Clear presentation of information in the OS Customization Tool

## 7.1.2 Features and Apps

Numerous functions and apps are installed with Microsoft Windows by default. These options include applications such as “Sticky Notes”, “MS Paint” and “Bing Weather” as well as “Skype” or “OneNote”. IT administrators can remove apps and enable/disable features here to control and restrict the collection and transmission of diagnostic or functional data<sup>15</sup> to Microsoft.

## 7.1.3 Patches

This is where IT administrators can customize the Windows image so that they can include Microsoft patches directly in a Windows image or remove obsolete cumulative patches in order to subsequently install this image directly with OS-Install. Separate installation of the patches at a later date is then obsolete.

## 7.1.4 Settings and Corporate Design

There are also numerous settings that an IT administrator can define at a very detailed level. File Explorer and Internet Explorer user default settings as well as taskbar and clipboard customization are just some of the available options. Similarly, administrators can allow the “Bing Search” or “Cortana” and make many further settings.

<sup>15</sup> See: <https://docs.microsoft.com/en-gb/windows/privacy/configure-windows-diagnostic-data-in-your-organization>



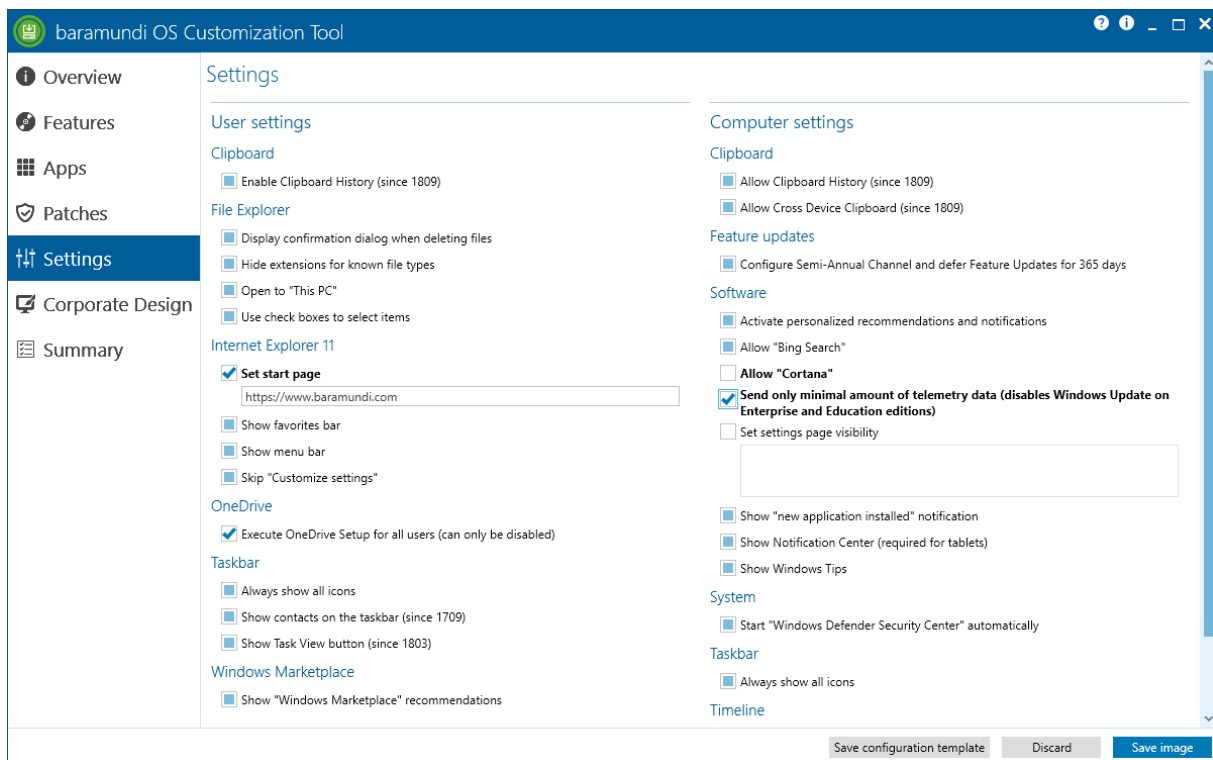


Figure 59 - Numerous settings at user and endpoint level

Besides functional settings, however, UI customization often requires a lot of rework when rolling out a new operating system, in order to conform to the requirements of the respective company. The OS Customizing Tool offers valuable support in customizing the Windows image to enable applicable compliance and corporate identity requirements to be implemented in the company.

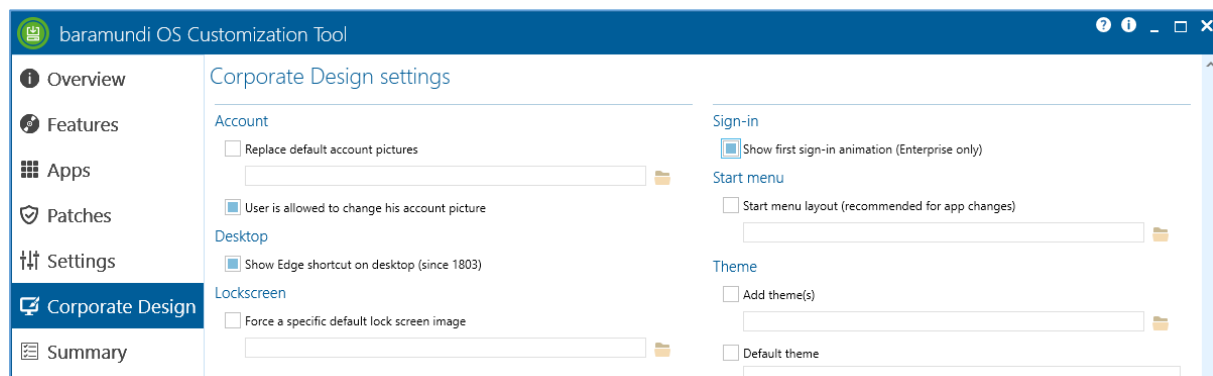


Figure 60 - Possible customizations for the corporate UI

## 7.2 Android Enterprise

With the advent of bMS 2019 R1, further profile modules and settings familiar from Android and Samsung Knox are available on Android Enterprise (Fully Managed Device).

A number of new options have been added to the “Restrictions” profile module, in particular.

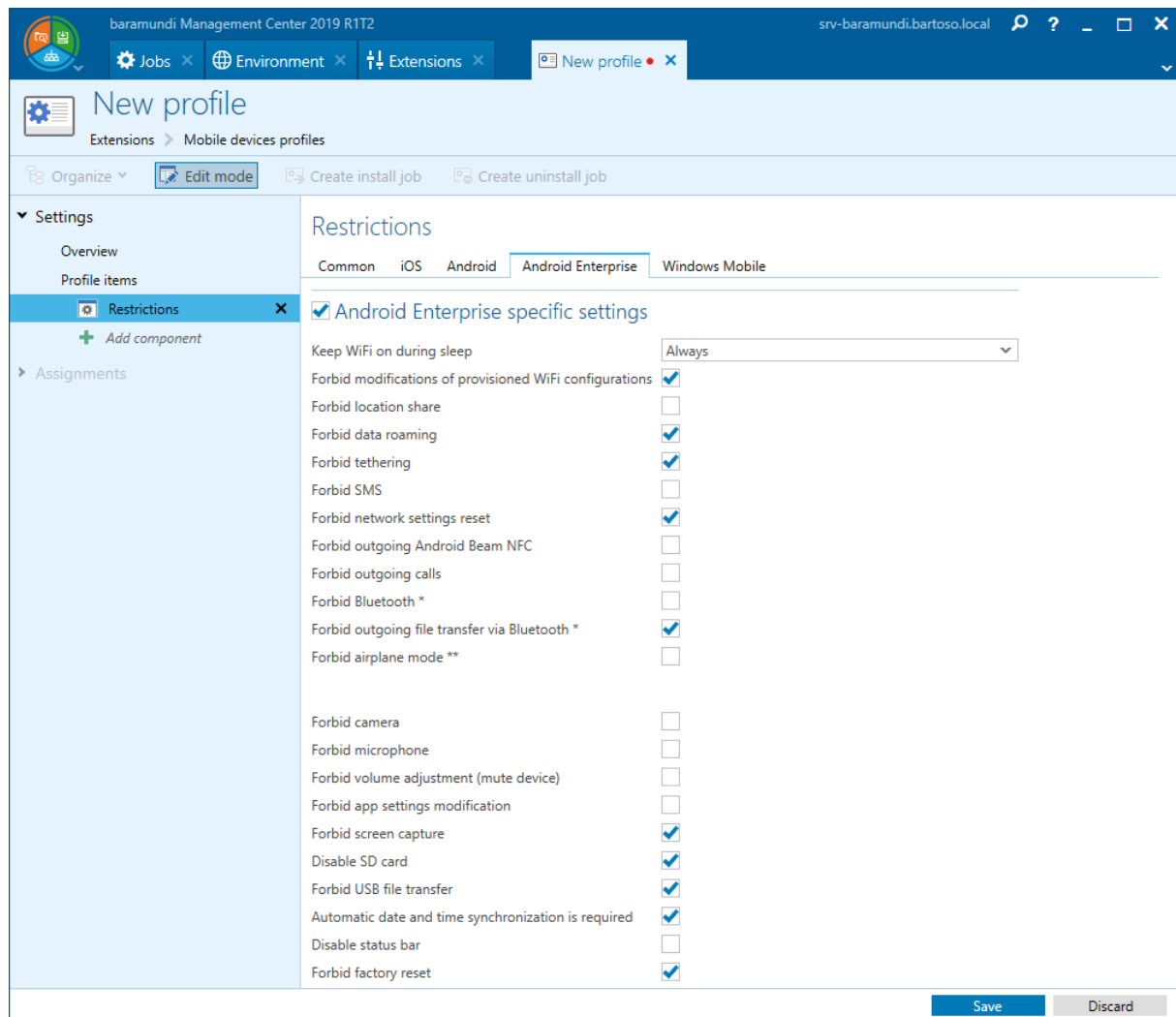


Figure 61 - New options in the “Restrictions” profile module

This means that far-reaching restrictions can now also be set up on the device. For example, the camera can be prohibited and screenshots blocked. A factory reset by the user can also be prevented.

The AE-specific configuration of the unlocking of the device using biometric characteristics and the display of notifications in the lock screen are now also possible in the “Security Policies” profile module. In addition, the baramundi Agent can now display the compliance status and list pending violations in detail on Android Enterprise devices.

## 7.3 Extension of the new Kiosk

With version 2018 R2, a completely new Kiosk was added to the baramundi Management Suite. For the first time, the new Kiosk enables a user-centric view based on AD users and groups. It requires user administration in the Active Directory and an active AD-sync in the bMS.

With Release 2019, the Kiosk has been extended to include a device-centric view, and is thus no longer exclusively available to logged-in users, but can also be used without the user logging in. As a result, jobs can now also be released for devices and logical groupings.

**Note:** After installation of the current baramundi Management Suite, the old Kiosk (prior to bMS 2018 R2) is automatically replaced by the new Kiosk. Job releases based on “logical grouping” are retained and are available in the new Kiosk after the update of the baramundi Management Agent on the endpoints.

### 7.3.1 Scenarios

In addition to the user-centric view familiar from bMS 2018 R2, there are now two additional views: A device-centric view and a mixed view.

### 7.3.2 User-Centric View

As known from Release 2018 R2, users can log in to the Kiosk with their login information from the Active Directory. Users are then shown all the endpoints on which they are set as registered user. Users also receive a list of all jobs released for them. Users can now assign all released jobs to their endpoints and track the execution state.

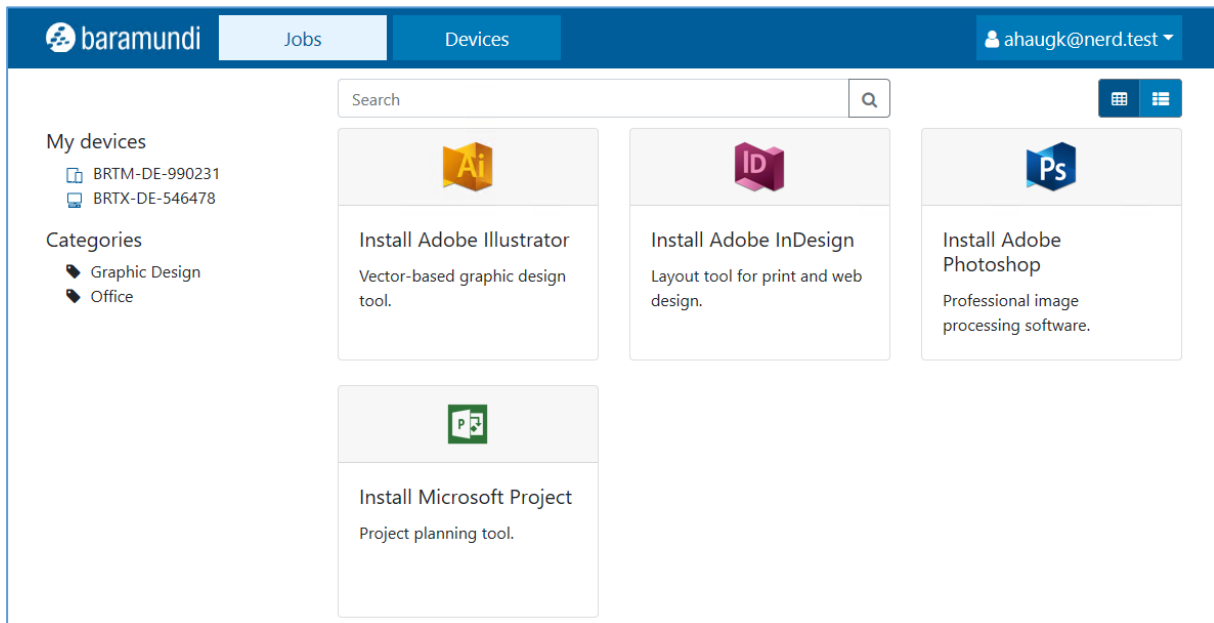


Figure 62 - Kiosk in the user view

### 7.3.3 Device-Centric View

Users launch the Kiosk by double-clicking on the baramundi Management Agent (bMA). They will automatically see the view of the endpoint without having to log in manually. All jobs released for this endpoint are displayed there. Jobs can only be assigned to the current endpoint which is already preselected.

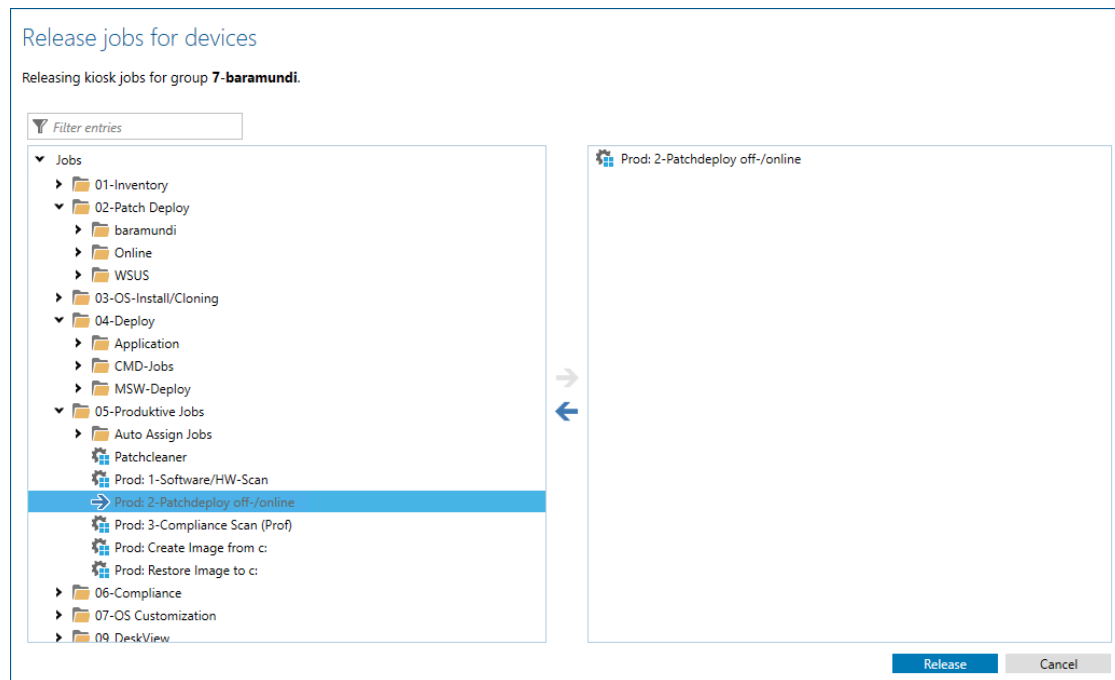


Figure 63 - Dialog box for releasing jobs to devices and logical groups

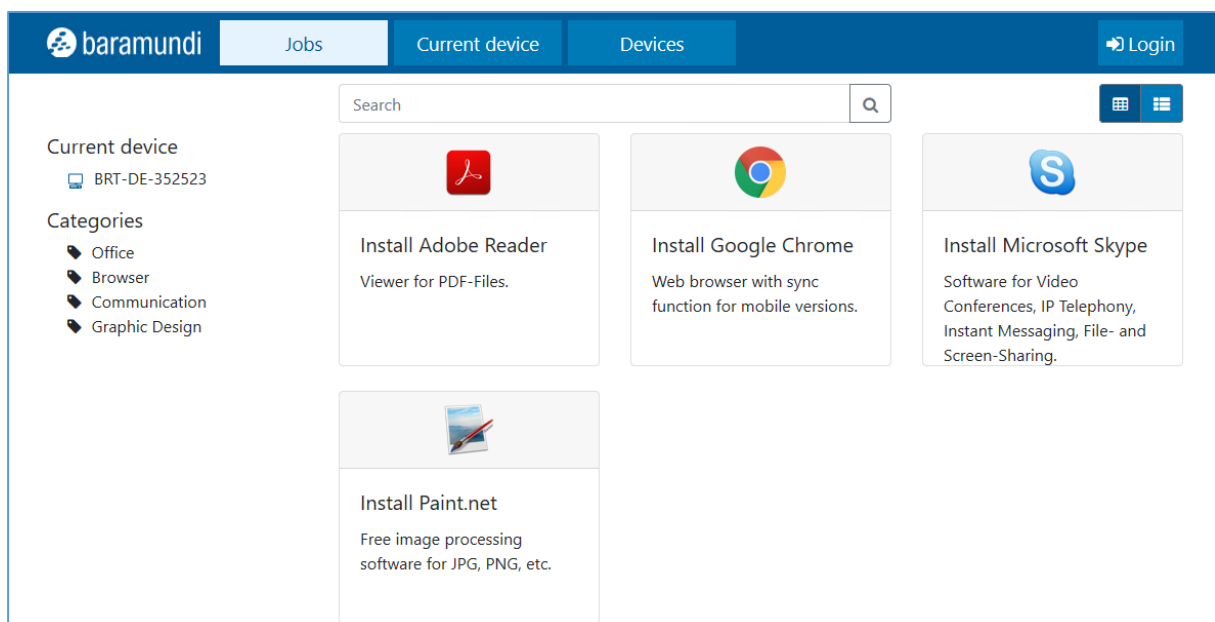


Figure 64 - Kiosk in device mode

### 7.3.4 Mixed View

The mixed view combines the endpoint view with the user view. If the Kiosk is called using the agent and then users log in, users can manage both the current endpoint and all endpoints on which they are set as registered user. With regard to jobs, those released for the current endpoint as well as jobs released for the user are displayed. Jobs for devices can be pre-filtered using filters in the navigation area.

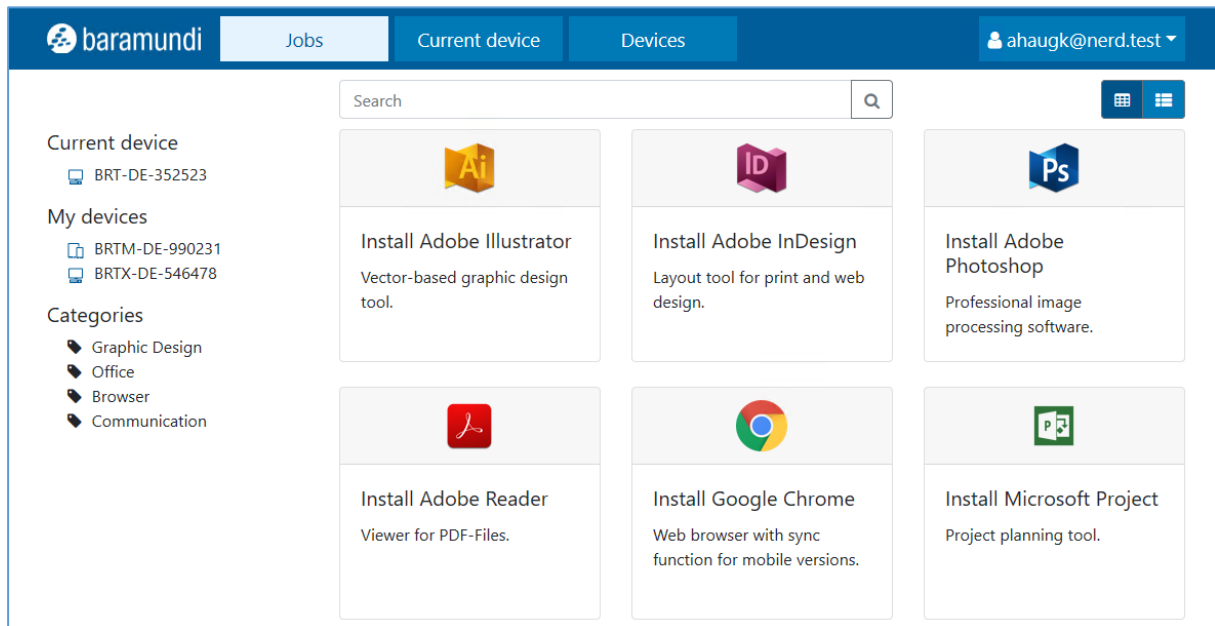


Figure 65 - Kiosk in mixed mode

## 7.4 E-mail Notifications

IT administrators use the baramundi Management Center to carry out important IT routine tasks and manage the endpoints in the company. However it is also important for them to have a good, up-to-date overall view of the IT infrastructure and monitor the overall status. Personal notifications have been introduced in Release 2019 to facilitate the up-to-date overview and to keep the IT administrator actively informed (particularly when problems occur).

### 7.4.1 Job-Related E-mail Notification

This implementation corresponds to one of the TOP requests in the feedback portal. It enables IT administrators to be notified by e-mail when a job reaches a particular configured state in order to allow them to respond quickly to a job error, for example.

### 7.4.2 Activate Notifications

The new functionality can be activated and deactivated both globally and personally for each administrator – by default, it is activated globally and for all administrators.

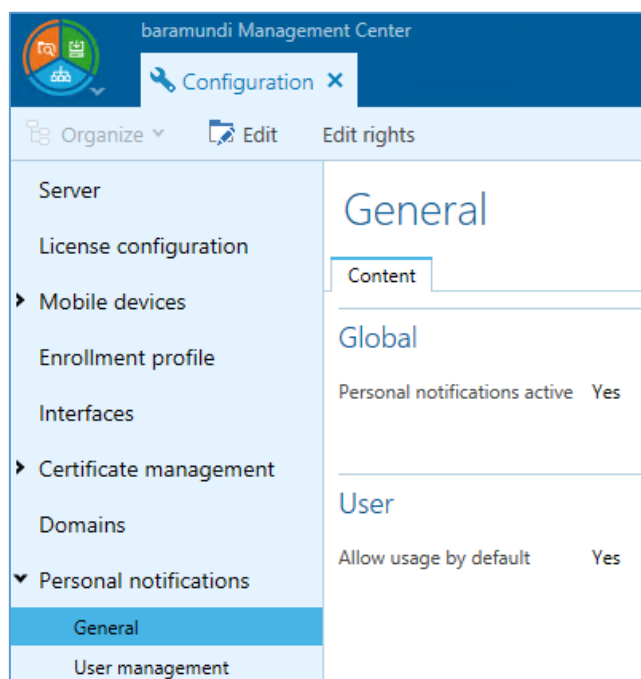


Figure 66 - Activate/deactivate notifications

bMC administrators can use the different activation options to decide whether to activate this feature for all or just some administration colleagues. They can also view and, if necessary, restrict active and inactive notifications at user level when, for example, colleagues leave the company or are on holiday.

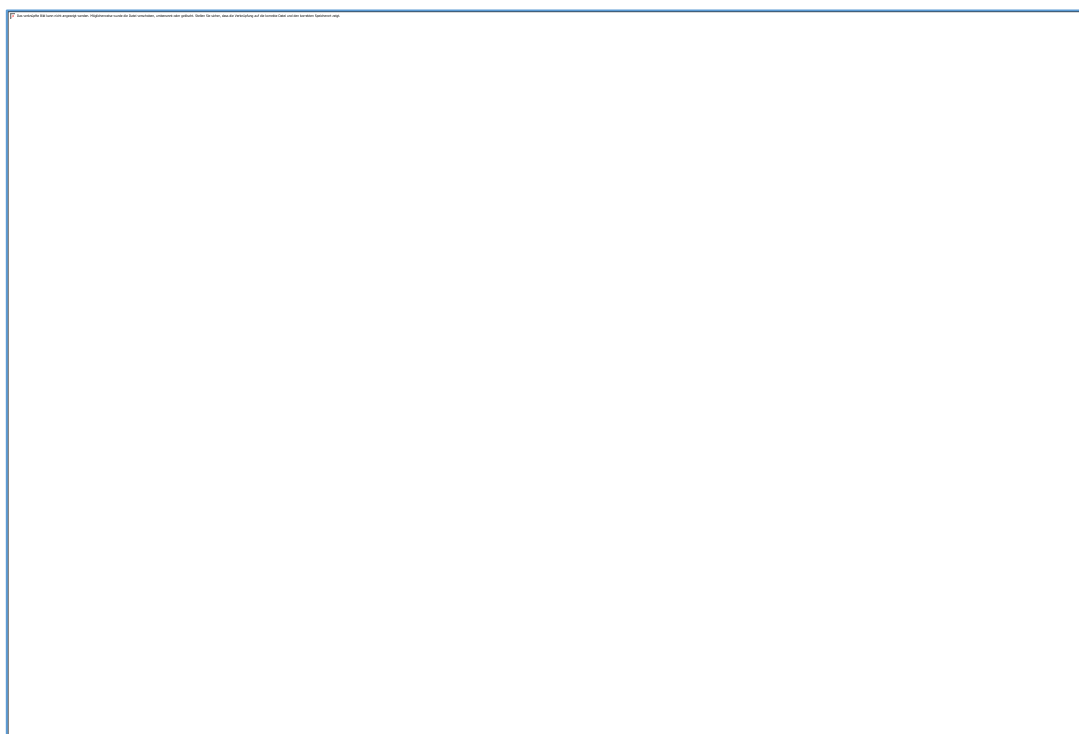
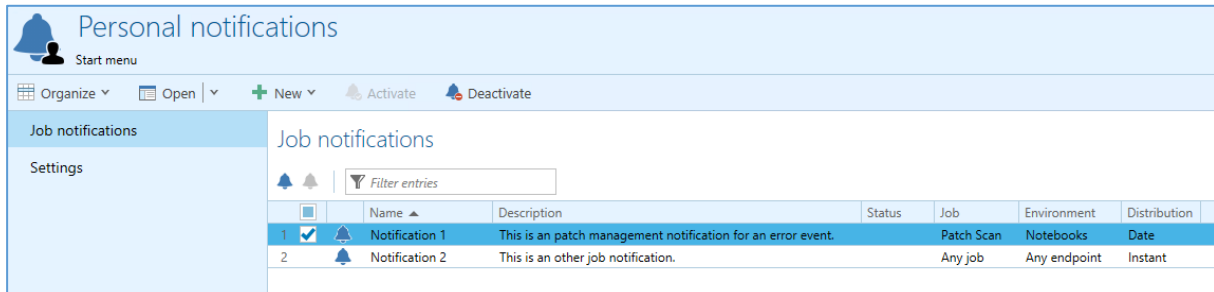


Figure 67 - Restrict notifications at user level

### 7.4.3 Displaying and Editing Job Notifications

E-mail notifications are displayed clearly in a new table, where administrators can create, edit and delete their notifications.



The screenshot shows the 'Personal notifications' interface. It has a sidebar with 'Job notifications' and 'Settings'. The main area displays a table of job notifications with columns: Name, Description, Status, Job, Environment, and Distribution. There are two notifications listed: 'Notification 1' and 'Notification 2'.

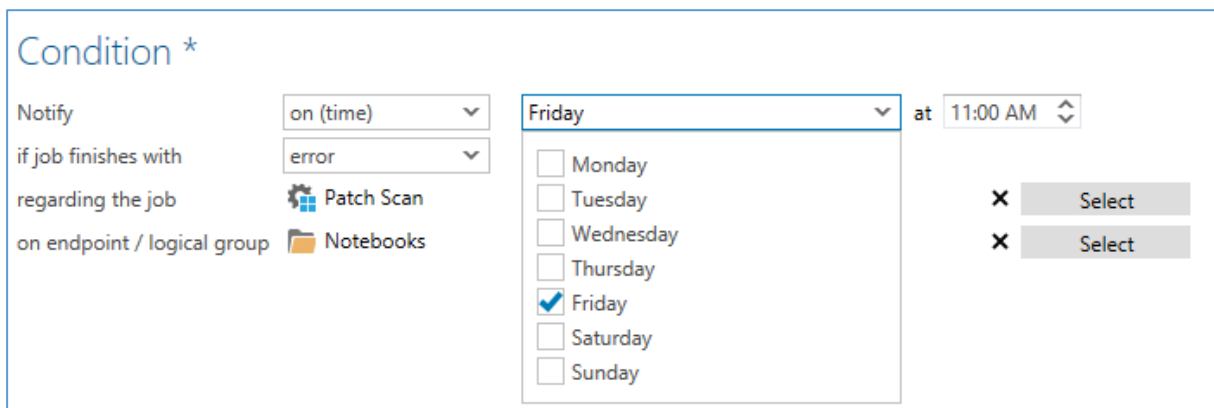
	Name	Description	Status	Job	Environment	Distribution
1	Notification 1	This is an patch management notification for an error event.		Patch Scan	Notebooks	Date
2	Notification 2	This is an other job notification.		Any job	Any endpoint	Instant

Figure 68 - Overview for personal notifications

IT administrators have various options when defining notifications. Besides defining general information such as name, description and status, they can also set conditions for the notification. Conditions include:

- When the IT administrator would like to be informed,
- When a particular event occurs,
- Concerning which jobs, and
- For which device or logical grouping.

IT administrators can select the time as they see fit, and can choose between *immediately*, *at an interval* or *at time X*. IT administrators can therefore choose whether they wish to be informed immediately by e-mail when e.g. an error occurs or receive a cumulative summary at the end of the week.



The screenshot shows the 'Condition' configuration form. It includes fields for 'Notify' (on (time)), 'if job finishes with' (error), 'regarding the job' (Patch Scan), and 'on endpoint / logical group' (Notebooks). There is a dropdown for 'Friday' and a time field set to '11:00 AM'. A list of days is shown with checkboxes, where 'Friday' is selected. There are 'Select' buttons for each day.

Figure 69 - Granular options for the time of notification

Similarly, administrators can flexibly determine whether they wish to receive the information for all jobs or a particular job, and whether this notification applies to a specific endpoint or to all endpoints/group.



## 7.4.4 Content of E-mail Notifications

Besides offering flexible control, the content of notifications can also be customized. Generally, an e-mail template is provided for the bMC user to use. This can however be flexibly adapted, and a number of variables can be added.

A preview of the notification makes it easier for IT administrators to find the correct format that suits them best.

Content

E-mail

Subject

[[Notification.Name]]: {Notification.TriggerReason}

Content

```

<html>
<p style="font-family: 'Segoe UI';font-size:14px;">
You received the notification due to the following events:<br/> <br/>

{Notification.EventsWithLinks}
</p>

<br/> <br/>
<p style="font-family: 'Segoe UI';font-size:12px;">{Notification.Footer}</p>
</html>

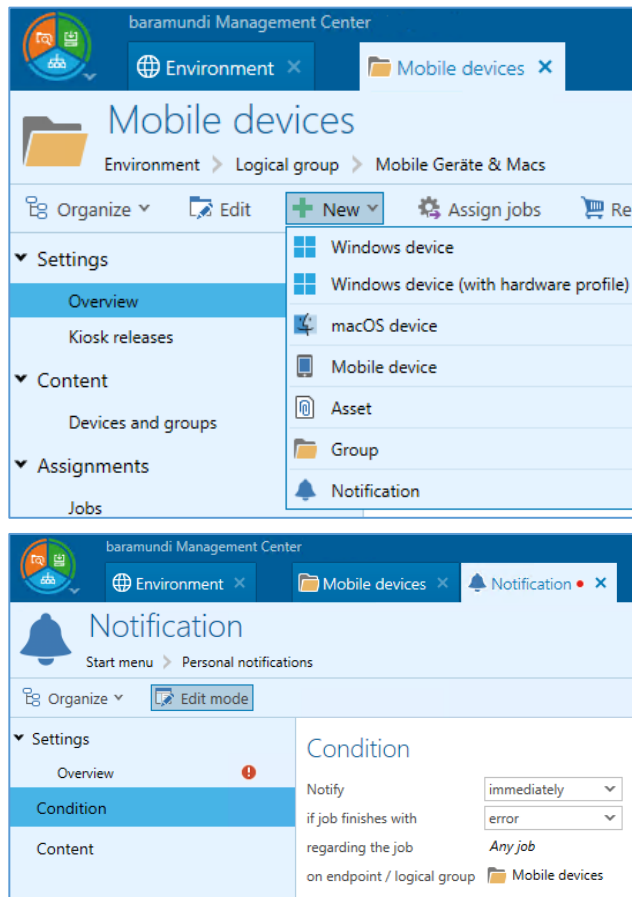
```

Preview

Figure 70 - E-Mail template for a notification

## 7.4.5 Define Notifications

A central overview showing all notifications ensures transparency. However, in an IT administrator's daily work it is often more effective to be able to create a notification on the spot



when, for example, an endpoint is being edited in the BMC. This is why it is also possible for IT administrators to create and configure an e-mail notification for a job, endpoint or logical group. Corresponding conditions are then already preset in each case for faster editing.

Figure 71 - Example of a new notification for a logical group

## 7.5 Integration with DriveLock

The baramundi Management Suite is an important component of a company's effective security strategy. It reveals security vulnerabilities, for example, and enables IT administrators to seek an immediate remedy.

The solutions from DriveLock such as Smart DeviceGuard or File Protection are a further component in this strategy. These components are more closely integrated in bMS Release 2019. IT administrators who use both DriveLock and baramundi can now use BMC entry points into the DriveLock UI to launch necessary actions and make settings more quickly.

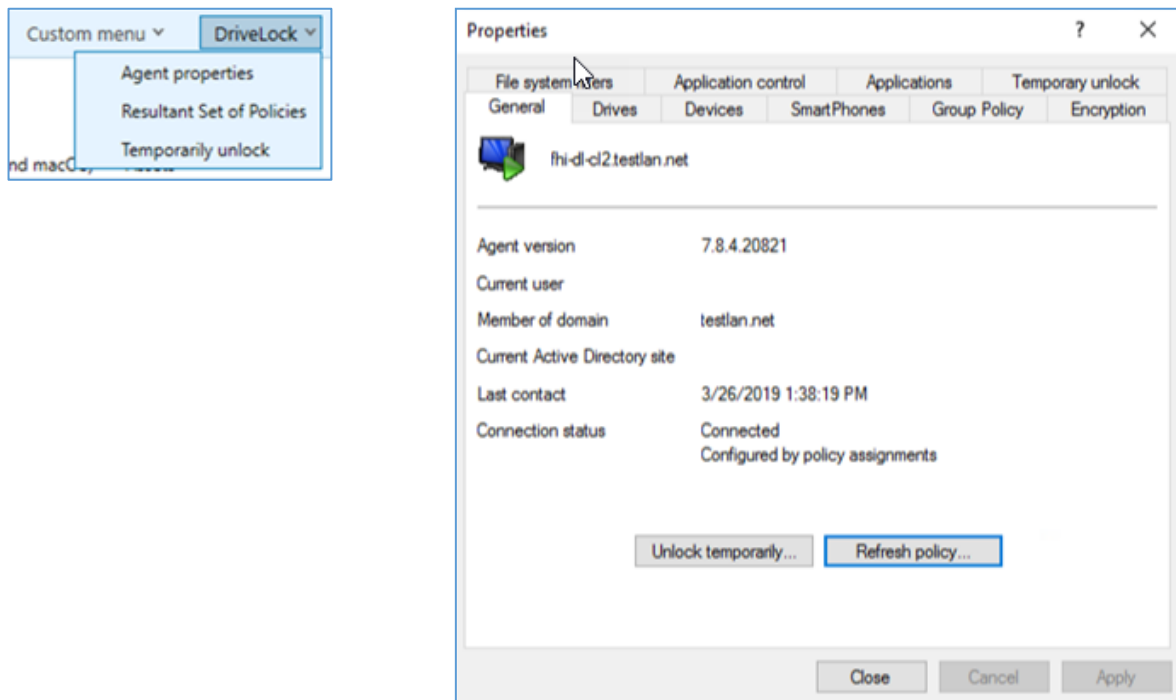


Figure 72 – bMS entry points to the DriveLock UI

Agent properties, sets of policy results, and an assistant for releasing devices can be displayed for each Windows endpoint.

## 7.6 General Development

### 7.6.1 Windows Server 2019

From bMS Release 2019 onwards, the new Windows Server 2019 operating system will be supported both as a manageable endpoint and as a host system for the bMS.

### 7.6.2 Prioritize the Processing of Jobs for Individual Endpoints

In the event of large ‘waves’ of job allocations, as is the case with a patch rollout across all company endpoints, it can be useful and necessary for an IT administrator to prioritize individual endpoints in the execution of jobs.

A user might contact the IT administrator regarding particular software that they urgently require. With Release 2019, the IT administrator can prioritize the user’s endpoint and so satisfy the user’s request. Irrespective of the number of job allocations currently in the environment, job allocations for this endpoint will then be executed as a matter of priority.

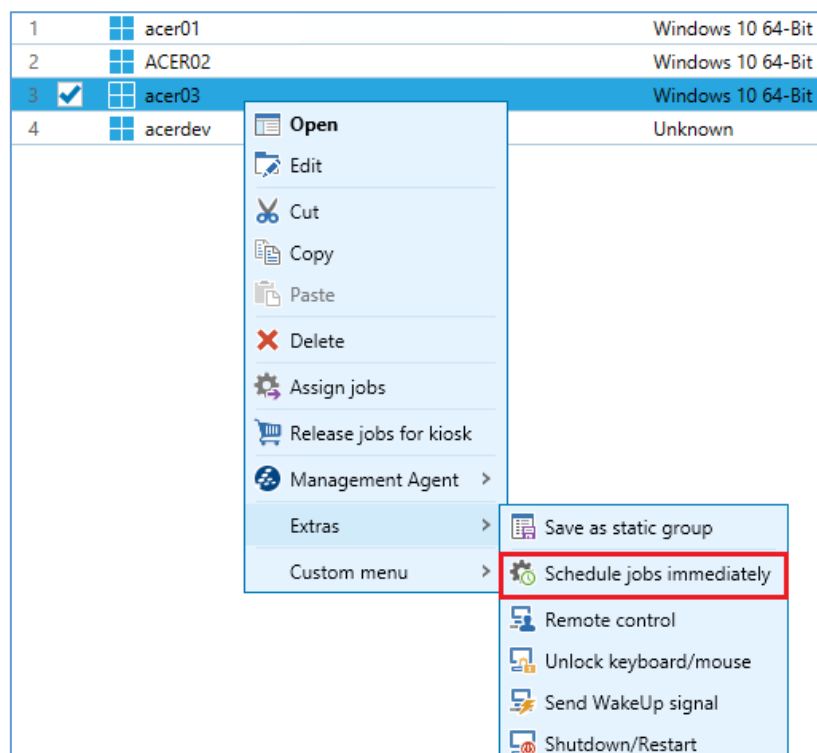


Figure 73 - Immediate job scheduling on the endpoint

### 7.6.3 Patch Management Clean-up

In the previous release, it was possible for IT administrators to clean up the DIP and remove bMSW data that was no longer needed. This functionality has been extended in Release 2019 and it is now possible to clean up unnecessary patch data as well. Patch files for patches that are no longer released can now be simply removed from the master DIP.

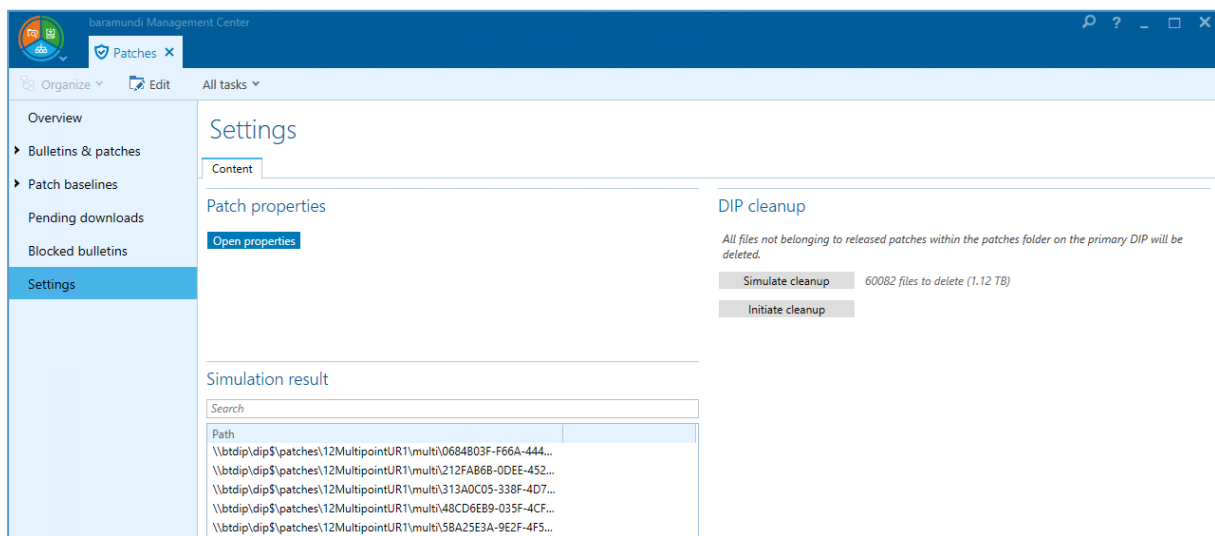
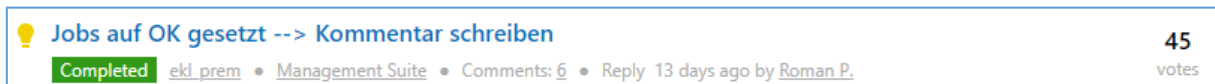


Figure 74 - Clean-up of the master DIP and removal of unnecessary patch data

## 7.6.4 Improvements in Usability

For enhancing the usability, some requests from the feedback portal were implemented.

### 7.6.4.1 Set Allocated Job to OK with Reason



A dialog box for entering a reason now appears if a failed job is set to OK. Input is optional and is discarded when the job is next started on the corresponding endpoint.

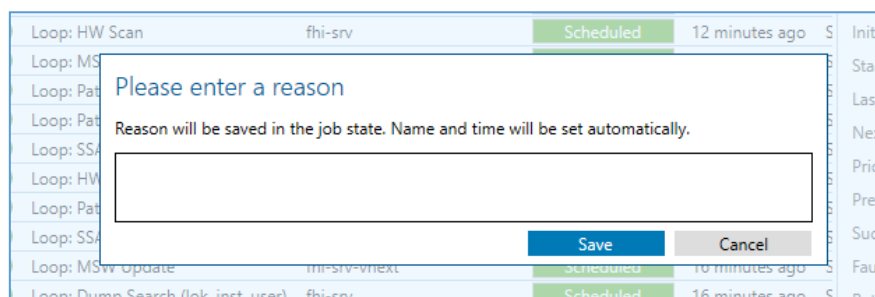


Figure 75 - New dialog box when setting "OK" on the job target

### 7.6.4.2 Extension of Expert Mode in the Job Wizard

Some settings have been added to the Expert mode of the wizard for creating jobs. They include the full selection of the "Action at end of job" and the "Log in as late as possible" option.

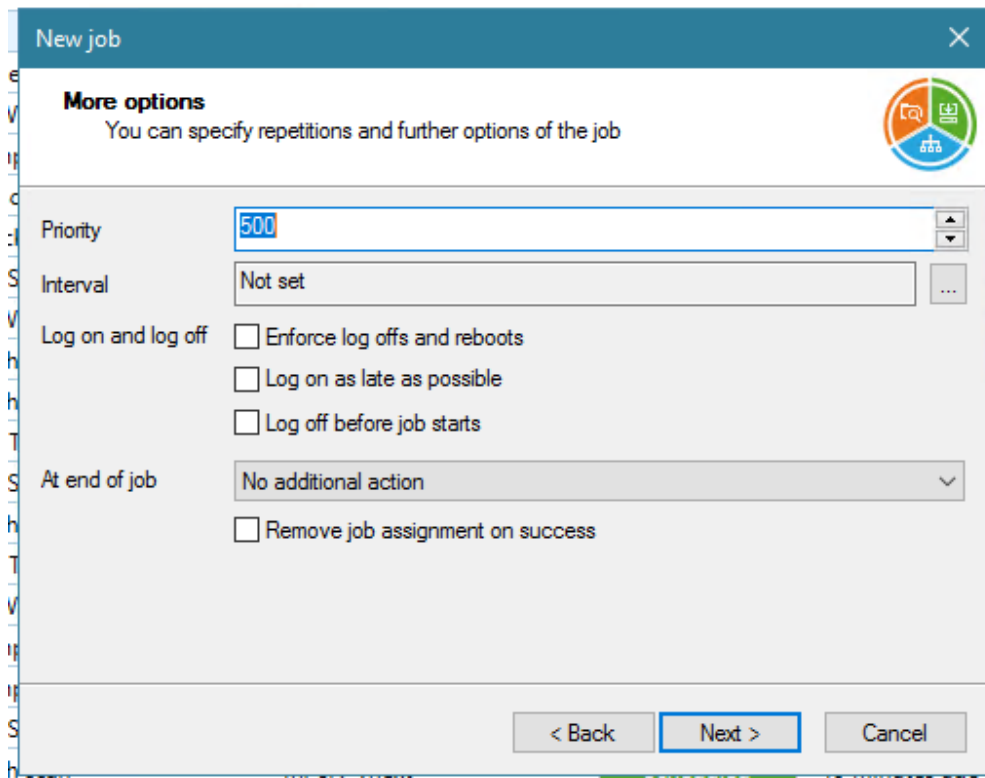


Figure 76 - Expert mode in the Job Wizard

#### 7.6.4.3 Creation of an (Un)Installation Job from the Software View

Installation and uninstallation jobs can now be created directly from the software view using the context menu and toolbar. The behavior familiar from baramundi Mobile Devices can now also be used for Windows software.

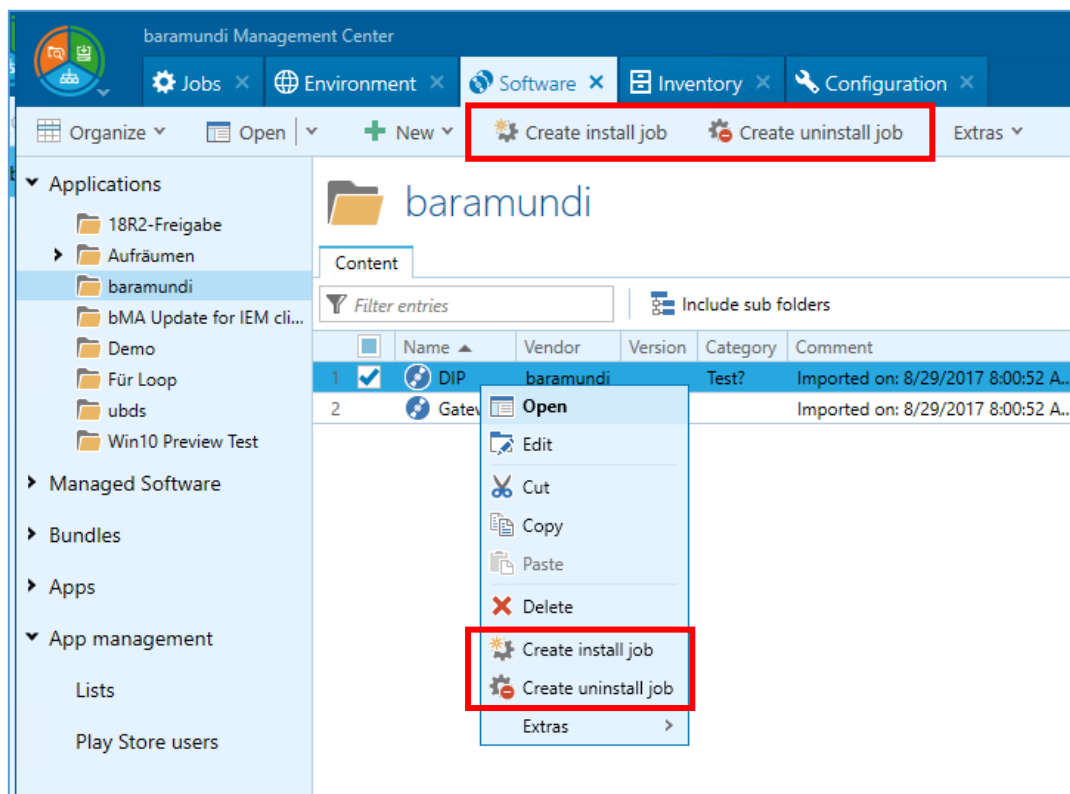


Figure 77 - New possibilities for creating installation/deinstallation jobs

#### 7.6.4.4 Improved Dialog Box for Column Selection in List Views

The dialog box for selecting the columns to be displayed in the list views was completely revised. It is now clearer and makes column selection much easier.

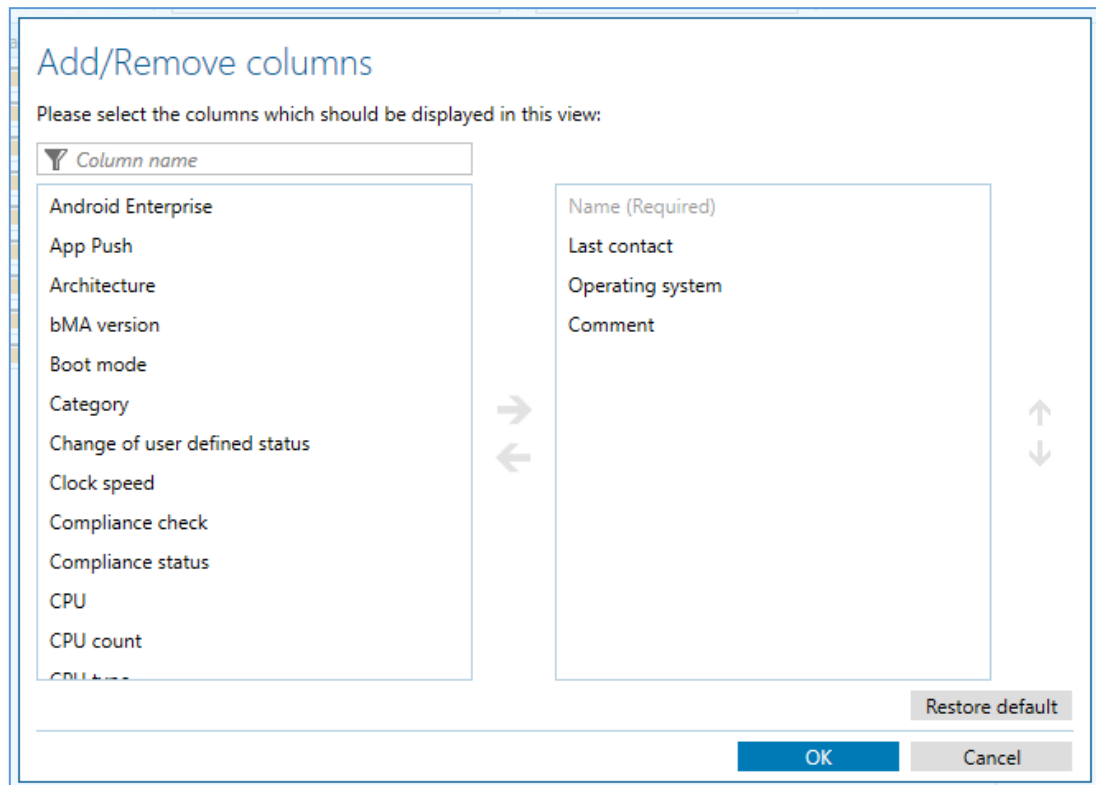


Figure 78 - New dialog box for column selection in list views



### 7.6.5 MSW: OpenJDK as an Alternative for Oracle JDK

At the start of 2019, Oracle modified the license terms for the Oracle JDK and JRE products, which is why not all of these products can be released in baramundi Managed Software at present. This resulted in the request to provide a Java alternative in bMSW. The new OpenJDK products “Alexander Hass OpenJDK” and “Amazon Corretto” have been available in bMSW since February 2019.

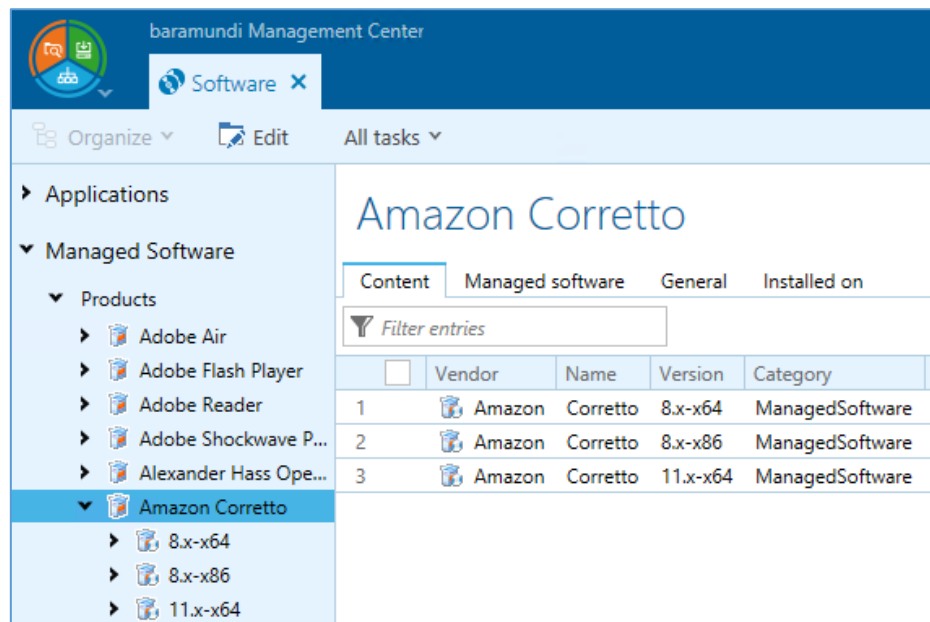


Figure 79 - OpenJDK: Amazon Corretto available in MSW

Likewise there are plans to integrate corresponding OpenJRE versions in MSW.

### 7.6.6 Security

The 2019 release includes several security-related enhancements. We therefore recommend a timely upgrade to the current version.

## 7.7 Product Improvements in Detail

### 7.7.1 Windows Agent (bMA)

- Bug-fix: Hardware inventory leads to a blue screen on some current models.

### 7.7.2 Server (bServer)

- A change to the log level takes effect without requiring service restart.
- The service restart via "bMC –Server state - Restart" now restarts the bServer service completely.
- The database manager can set an active database via command line.
- Bug-fix: If jobs with "User has to confirm job" are used, then bServer may sporadically not execute any more jobs for a longer time.
- Bug-fix: After a restart of the host system, sporadically there are no baramundi licenses available (only affects new licensing).

### 7.7.3 Management Center (bMC)

- Convenient column configuration for the table views.
- Create deployment jobs quickly from an application, including managed software.
- Prioritize a single windows client for job execution using the "Schedule jobs immediately" menu item.
- You can enter a reason when setting a job to OK
- When copying jobs, the display name is now extended with "Copy".
- The options of the wizard for Windows jobs have been adapted to the options in the properties dialog.
- Automatic job assignment is removed when copying windows jobs.
- When copying MDM jobs, the "Assign new devices" job option is removed.
- Jobs can now also be terminated even when the scheduler is currently preparing them.

- AD-Sync jobs can be copied.
- Asset types can be copied.
- Universal dynamic groups can be copied
- Sorting by remaining time for DIP sync jobs has been improved.
- The command line parameter can be used to open the bMC view for a specified client.
- A new status icon indicates a pending bServer restart.
- The display of the server status only refers to the current server, no longer to all PXE relays.
- The bServer processes the management agent actions "Start, Stop, Restart" instead of the bMC.
- Bug-fix: MDM jobs cannot be aborted or deleted in rare cases.
- Bug-fix: From compliance dashboard, navigating via "Scan status" from a top group to lower group does not work correctly.
- Bug-fix: The rights check under "Inventory - Software - Windows devices" is not correct.
- Bug-fix: Even when a product license has been applied, a message "Evaluation license has expired" is displayed.
- Bug-fix: "Used" in the detail view and overview of a "\*" app counts wrong if the app with the same ID occurs on different platforms.

#### **7.7.4 DIP-Sync / baraDIP**

- For new installations, the maximum number of concurrent threads is set from 64 to 150.

#### **7.7.5 bConnect**

- bConnect is now available in version 1.1. Version 1.0 requests are still possible without code changes.
- New parameters for reading, deleting and creating applications.

- Variable definitions can be read, written, deleted and created.
- When reading job objects, windows deploy steps are provided.
- Jobs with only windows deploy steps can be created.
- Bug-fix: The primary user cannot be updated on windows endpoint.
- Bug-fix: Last change in endpoint property returns an invalid date.
- Bug-fix: An application query in Oracle DB only returns MSW applications.
- Bug-fix: Hardware inventory queries run on errors in Oracle DB.

### **7.7.6 Compliance**

- The handling of exclusions has been improved.

### **7.7.7 Mobile Devices**

- Manual rule checking for MDM compliance is no longer necessary. The buttons are removed from the bMC.
- The agent for Android Enterprise has been enhanced with a compliance view.
- APN blocks can be installed and uninstalled in Android Enterprise.
- It is possible to select system apps for uninstallation for Android Enterprise.
- On iOS and Android Enterprise Wi-Fi configuration via a Microsoft Radius server is possible.
- The Android Enterprise app configuration has been improved.
- Bug-fix: A job for uninstalling an App on Android Enterprise runs into error sporadically.
- Bug-fix: Apps that have the same package name in iOS and Android are counted wrongly and handled incorrectly in bMC
- Bug-fix: If the wipe job step is not the first job step, no device wipe occurs.
- Bug-fix: Performance problems occur with large amounts of MDM compliance data.

- Bug-fix: Deleted Android Enterprise Apps are synchronized even if they are no longer approved.

### **7.7.8 OS-Install**

- The "Security-Malware-Windows-Defender" section to disable Defender has been removed from the unattend.xml files for Windows 10.
- Microsoft ADK 1903 is supported.
- The variables {Software.Version} and {OSType} can now be used in the driver path.
- For the OS-Install job step, the network boot can be set to "Autodetect".

### **7.7.9 Kiosk**

- The kiosk web server is now managed directly via the bServer.
- Kiosk uses the https port specified for MDM.
- The bServer Root CA is automatically registered by the bMA. As a result, the kiosk can be used now without a certification warning in Internet Explorer and Edge browser.
- Jobs that have been configured for the old kiosk are automatically taken over as device-related jobs for the new kiosk.

### **7.7.10 License Management**

- The language selection is now saved.
- Depending on the language selection, local currencies \$ and £ are available.
- Improved SQL error messages for connection problems; especially the initial setup has been improved.
- Bug-fix: An SQL error message is displayed when updating large amounts of inventory data
- Bug-fix: Long strings do not wrap correctly.
- Bug-fix: Oracle database cannot be used.
- Bug-fix: Creating data with more than 255 characters leads to database errors.

### **7.7.11 General**

- Windows Server 2019 is supported.
- The ISO image now contains the EN variant of SQL Server 2017 Express.

## 8 Appendix

### 8.1 Glossary

ACPI	Advanced Configuration and Power Interface
AE	Android Enterprise
AMT	Active Management Technologie (Intel vPro)
APN	Access Point Name (context: mobile network)
APNS	Apple Push Notification Service
bAPSI	baramundi Push Service Infrastructure
bBT	baramundi Background Transfer
bCenter	baramundi Management Center for iOS (app)
bCM	baramundi Compliance Management
bDS	baramundi Deployment Script
bDX	baramundi Data Exchange
BIOS	Basic Input Output System
Blacklist	Negative list of unwanted apps (see baramundi Mobile Devices)
bLM	baramundi License Management
bMA	baramundi Management Agent
bMC	baramundi Management Center
bMD	baramundi Mobile Devices
bMS	baramundi Management Suite
bMS/R	baramundi Management Server/Relay
bMSW	baramundi Managed Software
bND	baramundi Network Devices
bPM	baramundi Patch Management
Client	Synonym for endpoint
CEM	Cloud-Enabled Endpoint Management (i.e. without VPN)
DC	Domain Controller
DEP	Device Enrollment Program (from Apple)
DIP	Distributed Installation Point
EMM	Enterprise Mobility Management
Endpoint	Synonym for client
FDB	Forwarding Database
JSON	JavaScript Object Notation
GCM	Google Cloud Messaging (Android)
GDPR	General Data Protection Regulation (EU GDPR)
IPv6	Internet Protocol Version 6
MAM	Mobile Application Management
MCM	Mobile Content Management

MDM	Mobile Device Management
PCI	Peripheral Component Interconnect
PKI	Private Key Infrastructure
REST	Representational State Transfer
SAFE	Samsung For Enterprise (MDM-API)
SAM	Software Asset Management
SCEP	Simple Certificate Enrollment Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TLS	Transport Layer Security
TMG	Threat Management Gateway (Microsoft)
TOM	Technical-organizational measures
UEM	Unified endpoint management
UDG	Universal dynamic groups
USB	Universal Serial Bus
UEFI	Unified Extensible Firmware Interface
UI	User Interface
VM	Virtuelle Maschine
VPN	Virtual Private Network
VPP	Volume Purchase Program (Apple)
Whitelist	Positive list of permitted apps (see baramundi Mobile Devices)
WoL	Wake-On-LAN

## 8.2 Third Party Components

Information about 3rd party licenses can be found on the ISO image under:

<ISOIMAGE>\bms2020R1\3rdParty-Licensing\3rdPartyLicenses.pdf



## 8.3 List of Figures

Figure 1 - Schematic illustration of the enrollment process.....	5
Figure 2 - Configuration of AAD keys in the bMS.....	6
Figure 3 - Degree of fulfillment of the update profiles .....	7
Figure 4 - Overview of the update states of the endpoints within a group .....	8
Figure 5 - List of all updates of an endpoint group. ....	9
Figure 6 - bMA configuration page with options for "Do Not Disturb" mode .....	10
Figure 7 - List view with the new columns for "Do Not Disturb" Mode .....	11
Figure 8 - Do Not Disturb mode as a condition for a UDG .....	12
Figure 9 - Exported data with defined criteria .....	13
Figure 10 - Example of a Power BI Report .....	14
Figure 11 - Comparison of two points in time for UDG result sets.....	15
Figure 12 - List of selected notifications.....	16
Figure 13 - Return an embedded script value as an Automation Studio variable .....	17
Figure 14 - bLM configuration for email notifications.....	18
Figure 15 - Advanced scanning using ARP IP range .....	19
Figure 16 - Logical Group - network devices captured via ARP .....	19
Figure 17 - Manually creating network devices.....	20
Figure 18 - Variable definition with assignment to multiple areas.....	21
Figure 19 - User Synchronization with Variable Mapping.....	22
Figure 20 – Android Enterprise Profile and application scenarios .....	109
Figure 21 – Barcode Scanner in dedicated mode for selected apps .....	110
Figure 22 – Adding a new dedicated device .....	111
Figure 23 – Settings for the "Manage dedicated device" job step .....	112
Figure 24 – baramundi Argus Cockpit start page.....	113
Figure 25 – Responsive presentation on a mobile device.....	114
Figure 26 – Secure registration in the Argus Cockpit.....	114
Figure 27 – Configure the connection to the Argus Cockpit .....	115
Figure 28 – Status overview of several bMS instances.....	116
Figure 29 – Status via bServer services and baramundi jobs .....	117
Figure 30 – View of the detailed information per job instance .....	117
Figure 31 – License Management general concept 2020 R1 .....	118
Figure 32 – License Management importing external product data.....	119
Figure 33 – License Management extended product overview of importing external data ..	119
Figure 34 – Inventory of the Windows Security Center .....	120
Figure 35 – Mobile endpoints with variables in a UDG .....	121
Figure 36 – Windows endpoints with client variables in a UDG .....	121
Figure 37 – Changing the device name with baramundi variables .....	122
Figure 38 – Enrollment-Dialog in the bMC .....	123
Figure 39 – Context menu of the Agent .....	124

Figure 21 - Symbolic representation of the Work Profile .....	130
Figure 22 – Enrollment dialog for the Work Profile.....	130
Figure 23 - The Work Profile on a Sony XA2 running Android 9 .....	131
Figure 24 - The Work Profile on a Google Pixel 3 running Android 10 .....	131
Figure 44 – Security settings for the Work Profile .....	132
Figure 45 - BitLocker information on the overview page of a Windows endpoint .....	133
Figure 46 - Configuration profile for BitLocker .....	134
Figure 47 - List of recovery keys.....	135
Figure 48 - Jobs visible to the user in the Kiosk.....	136
Figure 30 - List of the user's devices .....	136
Figure 50 - New job assignment dialog.....	141
Figure 51 - Define release levels in the context menu .....	142
Figure 52 - Create download jobs for missing files .....	142
Figure 53 - Choice of online or offline documentation .....	143
Figure 54 – Detailed information in the new documentation .....	144
Figure 55 - Drill-down search.....	144
Figure 56 - New Notification Center in the bMC.....	145
Figure 57 - Calling the OS Customization Tool in the Operating Systems area .....	152
Figure 58 – Clear presentation of information in the OS Customization Tool .....	153
Figure 59 - Numerous settings at user and endpoint level .....	154
Figure 60 - Possible customizations for the corporate UI.....	154
Figure 61 - New options in the “Restrictions” profile module .....	155
Figure 62 - Kiosk in the user view.....	157
Figure 63 - Dialog box for releasing jobs to devices and logical groups.....	158
Figure 64 - Kiosk in device mode .....	158
Figure 65 - Kiosk in mixed mode .....	159
Figure 66 - Activate/deactivate notifications.....	160
Figure 67 - Restrict notifications at user level .....	160
Figure 68 - Overview for personal notifications .....	161
Figure 69 - Granular options for the time of notification .....	161
Figure 70 - E-Mail template for a notification .....	162
Figure 71 - Example of a new notification for a logical group .....	163
Figure 72 – bMS entry points to the DriveLock UI.....	164
Figure 73 - Immediate job scheduling on the endpoint .....	165
Figure 74 - Clean-up of the master DIP and removal of unnecessary patch data .....	166
Figure 75 - New dialog box when setting “OK” on the job target .....	166
Figure 76 - Expert mode in the Job Wizard.....	167
Figure 77 - New possibilities for creating installation/deinstallation jobs .....	168
Figure 78 - New dialog box for column selection in list views.....	169
Figure 79 - OpenJDK: Amazon Corretto available in MSW .....	170




**baramundi software AG**

Beim Glaspalast 1  
86153 Augsburg, Germany

 +49 821 5 67 08 - 500  
[support@baramundi.com](mailto:support@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)

 +49 821 5 67 08 - 500  
[support@baramundi.com](mailto:support@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)

 +48 735 91 44 54  
[support@baramundi.com](mailto:support@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)

 +49 821 5 67 08 - 500  
[support@baramundi.com](mailto:support@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)

**baramundi software USA, Inc.**

30 Speen St, Suite 401  
Framingham, MA 01701, USA

 +1 800 470 3410  
[support@baramundi.com](mailto:support@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)

**baramundi software Austria GmbH**

Landstraßer Hauptstraße 71/2  
1030 Wien, Austria

 +49 821 5 67 08 - 500  
[support@baramundi.com](mailto:support@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)