baramundi

Release Notes

baramundi Management Suite

2023 R2

Empower your IT

Dear reader,

This release provides a variety of usability optimizations to improve the use of the bMS for both IT admins and end-users.

We also have a staggered rollout of updates and improvements to cloud-based services (Argus Module, Ticketing System and Vulnerability Catalog) and other functional modules.

To expand management options and network transparency, we've added support for endpoint devices using **Linux** operating systems. You can now collect essential inventory data without an agent.

With flexible and hybrid work arrangements increasingly common, the bMS now offers powerful tools for **end user experience management (EUEM)**. The new cloud-based **Argus Experience module** enables IT admins to proactively spot, analyze and fix common endpoint issues that affect user productivity such as long boot times, failing notebook batteries, and software hangs and crashes.

The **baramundi Kiosk** now provides a **Single Sign-On (SSO)** option for easier and faster secure end user access to self-service software installations and other tasks.

Android users benefit from an out-of-the-box (OOBE) experience with support for **Android Zero-Touch** provisioning. Similar to the existing process for Apple devices, zero-touch speeds deployment and startup for end users while reducing burdens on IT admins.

IT admins sometimes require direct interaction with managed Windows PCs and servers to complete endpoint maintenance tasks or provide support without end user involvement. While the existing baramundi Remote Control module enables connections to LAN devices, the new **baramundi Remote Desk** capability available with 2023 R2 gives IT admins fast and secure access to managed endpoints in any location via the cloud without a VPN connection.

We also further enhanced Universal Dynamic Groups (UDGs), script execution on network devices and much more.

I wish you an informative and stimulating read.

Armin Leinfelder
Director Product Management

baramundi Management Suite – Version 2023 R2

TABLE OF CONTENTS

1 Release 2023 R2

1.1 baramundi Remote Desk

The baramundi Management Suite 2023 R2 now offers integrated support for the new baramundi Remote Desk module, an addition to the existing baramundi Remote Control module for remote endpoint maintenance. In cooperation with our partner AnyDesk Software GmbH, we have created a direct remote maintenance option to access endpoints from the baramundi Management Center. baramundi Remote Desk enables fast and secure IT access to managed Windows devices regardless of their location directly from the baramundi Management Center without the need for a LAN or VPN connection.

1.1.1 Advantages of Partnership

Remote Maintenance via the Cloud

With baramundi Remote Control, it was not possible to access devices outside the LAN due to the limitations of Windows Remote Support. baramundi Remote Desk instead uses the baramundi Management Agent to establish a secure tunnel directly between the endpoint and the baramundi Management Server via the cloud to transfer the required session ID. IT admins can connect either to devices on the LAN or to remote internet-connected devices without the need for a VPN session, through AnyDesk's underlying cloud network, called "AnyNet".

Data Centers

All data centers are certified according to ISO/IEC 27001 and are located in the following locations:

- USA (west & east coast) and parts of Latin America
- Brazil (areas not covered by Latin American data centers)
- Spain
- France
- Great Britain
- The Netherlands
- Luxembourg
- Germany
- Finland
- Bulgaria
- Turkey
- Israel
- Kazakhstan
- Singapore
- China
- Japan
- Australia

Personal data for customers in the EU is processed at data centers in Germany and France.

Multi-User Scenarios

The existing baramundi Remote Control module creates a single session between an endpoint and the admin console using the Windows Remote Support function. The new baramundi Remote Desk solution instead enables multiple different sessions.

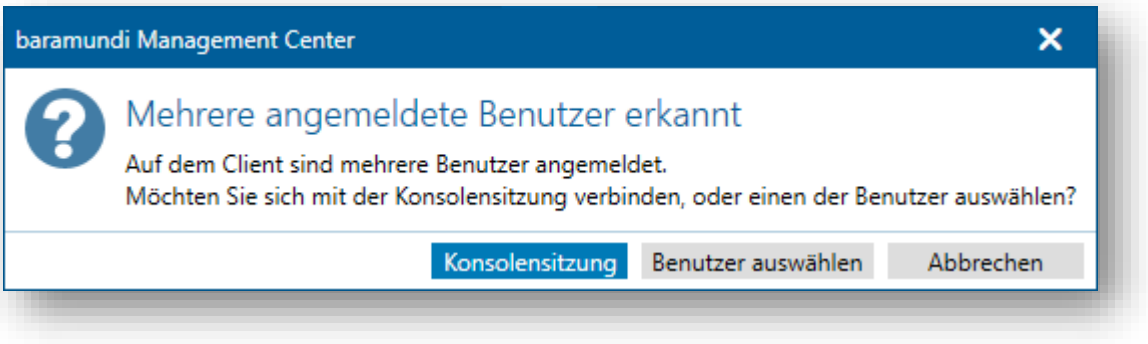


Figure 1 baramundi Remote Desk - Multiple User Sessions

When the connection is established, the baramundi Management Agent checks the users currently logged in and offers a selection of which session to take over.

UAC Management

Windows User Account Control (UAC) prevents unauthorized users from making changes to the system without the administrator's permission.

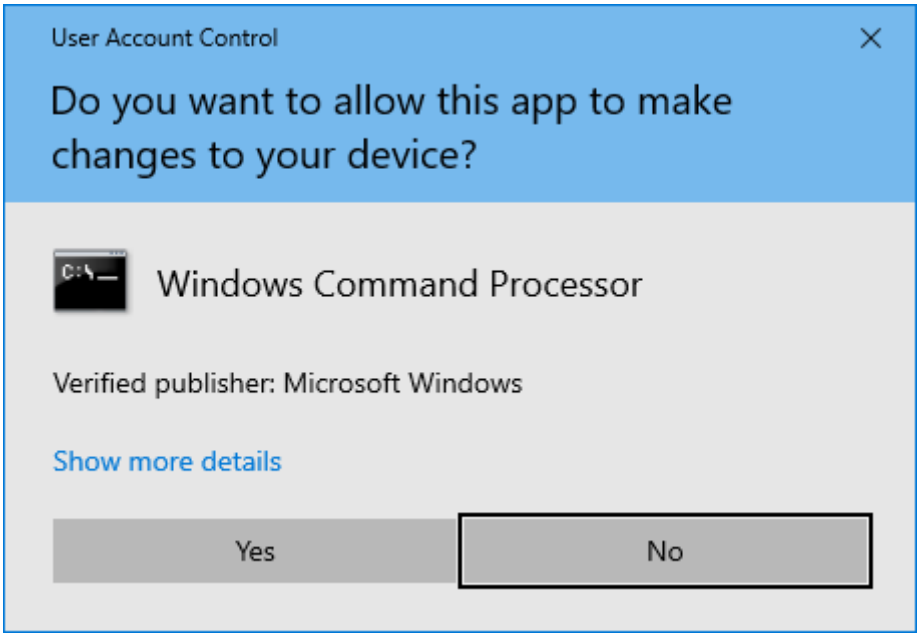


Figure 2 Windows User Account Control

Access to certain administrative applications is permitted only if the remote maintenance solution is run with extended rights. With baramundi Remote Desk, you can do this through the baramundi Management Agent at startup to interact with prompts and settings "behind" the UAC.

Keyboard & Hotkeys

Key combinations are passed through the session to the target device. This means that you can work as usual with CTRL+C and CTRL+V, for example, or open the Task Manager with CTRL+Shift+ESC.

For international users, baramundi Remote Desk offers a function to seamlessly interact with a system using a different keyboard layout. For example, a user in Poland using a Polish keyboard layout can connect to a computer in France using a French keyboard layout and work regardless of the different layouts. In most cases, baramundi Remote Desk will choose the best mode for the user. You can also manually select the appropriate keyboard if needed.

File Transfer

baramundi Remote Desk offers options for transferring files between local and remote devices via a "File Manager" session or via "File Transfer" during a Remote Control session.

File Manager

The special File Manager feature is available on Windows. To start a special File Manager session, simply click on the icon

To use the File Manager during an interactive remote session, simply launch it from the toolbar. If you also switch an active user session, the file transfer must be approved by the user in advance so that files are not transferred in the background without permission.

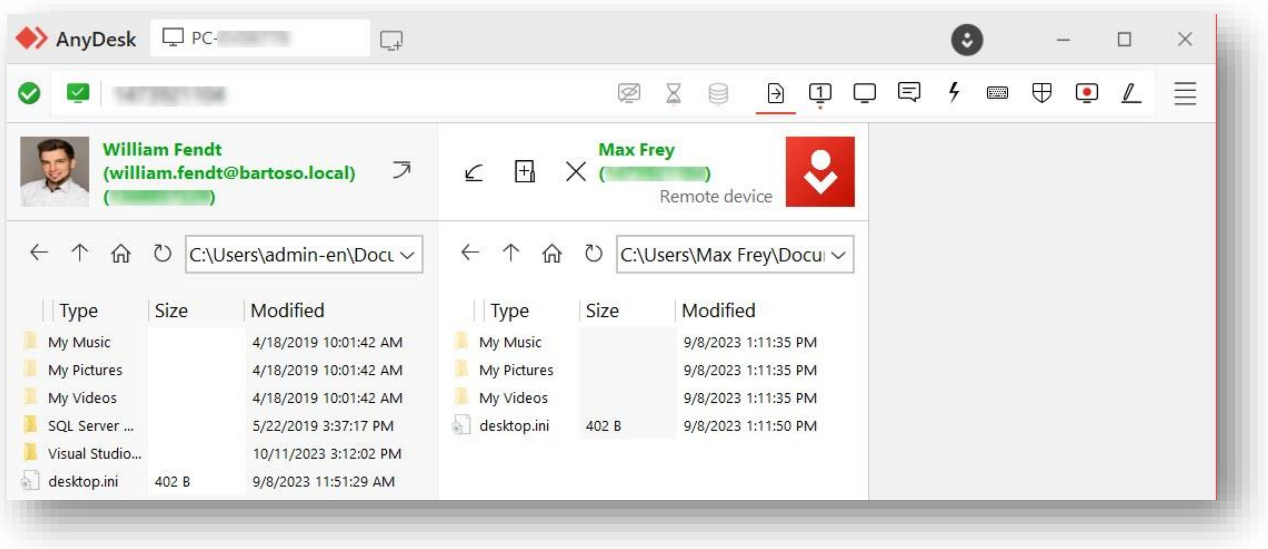


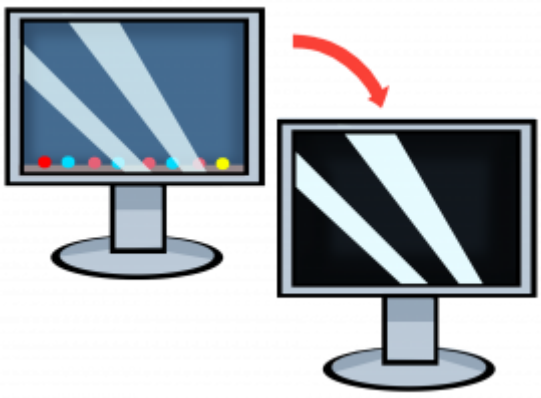
Figure 3 baramundi Remote Desk - File Manager

File Transfer

baramundi Remote Desk offers the option of synchronizing clipboards between the local and remote end devices. It can apply to both text and files.
This function is offered via the "Copy & Paste" functions of all common platforms.

Privacy Mode

"Privacy mode" allows you to hide the content of a session by disabling the remote display to prevent viewing by anyone with physical access to it. Input and sound from the remote side are also blocked until the session is ended or private mode is turned off manually.



However, private mode does not hide any actions of the operating system or any history on the local or remote device.

For private mode to be enabled, consent is required on both sides of the session.

Chat Function

baramundi Remote Desk offers the option of sending messages between two endpoints both during a connection request and during a session.

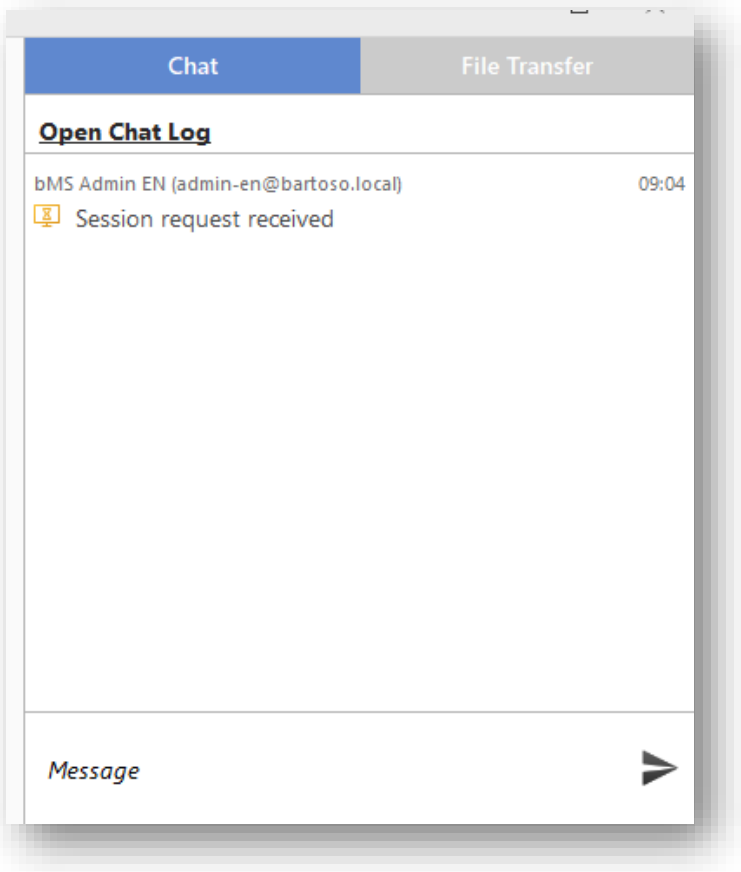


Figure 4 baramundi Remote Desk - Chat Client

Chat histories are ordered by the ID of the connected end device. Multiple chats between the same IDs in different sessions are combined into one file locally.

1.1.2 Advantages of baramundi-Integration

The baramundi Management Center in use as well as the bMA already installed on the system result in several advantages for the remote connections.

Usable Without Additional Installations

Due to the automatic distribution of the baramundi Management Agent to each client, no additional remote installations are needed. You only need to update the bMA to version 2023 R2. From then on, remote sessions can be conducted directly from the baramundi Management Center.

"Known" Personal Settings

You can use the Remote Control interface to transfer its personal settings to the new baramundi Remote Desk solution without any further action. baramundi Remote Desk will then show the existing Remote Control display name and user image.

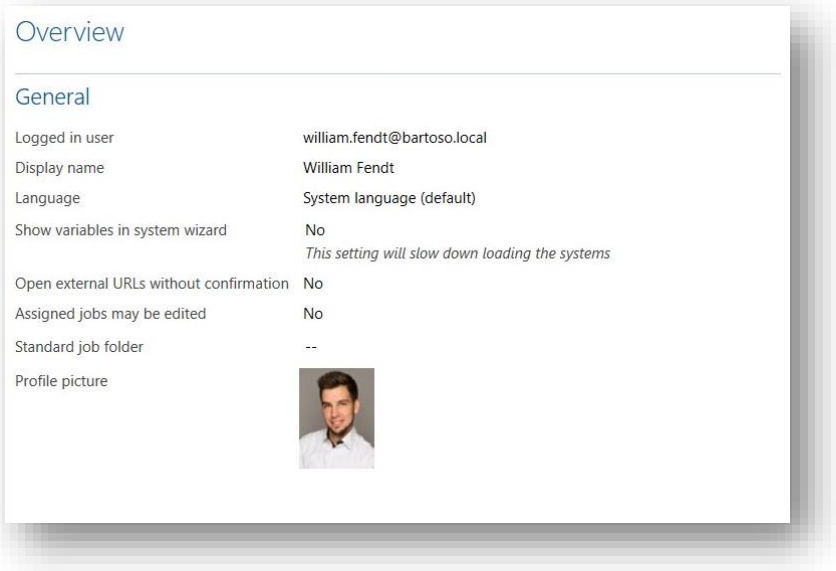


Figure 5 baramundi Remote Desk – Personal Settings

It is also a familiar image for the user at the target system. The initial communication takes place via our TrayNotifier and provides a known and familiar layout for the user to confirm the switch.

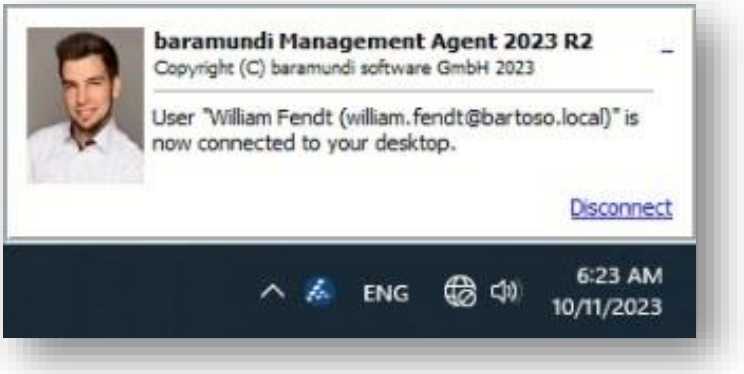


Figure 6 baramundi Remote Desk - Tray Notification

Logged on / Not logged on

A Remote Desk session can be initiated even if no user is logged on to the remote system. The bMA will use the existing communication with the baramundi server to perform the logon automatically to start a new session or resume an earlier one. A user session or even a specific user session (see 0) can be used. Logoff is automated when the session is terminated to avoid leaving it open accidentally.

AnyDesk only runs after bMA is started

In the case of baramundi Remote Desk, our baramundi Management Agent functions like a kind of gateway: The actual application for establishing a remote maintenance session is only started by the bMA when it receives this command from the server. Thus, despite the accessibility of the end devices on the Internet, it is not possible to access a target system that works with baramundi Remote Desk solely through the session ID or even only through "ID-guessing".
This is a security aspect in that the time window for possible queries is reduced enormously and only after a request from the authorized bMA.

Whitelisting Through bMC and bMA

By default, the baramundi Remote Desk (even if it had been started; see 0) does not accept requests to establish a session and only allows sessions already on a whitelist. The bMA adds the session ID of a source system to the whitelist before the session. This is an additional security step to ensure that no unauthorized IDs have access to baramundi Remote Desk on an end device.

1.2 Inventory by SSH for Linux Devices

2023 R2 Inventory functions now include support for endpoints running various versions of the Linux OS (e.g. Red Hat, Debian, Ubuntu, OpenSUSE, Raspberry Pi OS).
Once added to the bMS manually or automatically via a Network Devices scan, Linux systems can be inventoried via a job using SSH and without the need for an agent. SSH authentication can be done via username/password or an SSH Key.
Agent-less inventory is especially important in Operational Technology (OT) networked production environments where installation of a management agent is either impractical or very difficult.

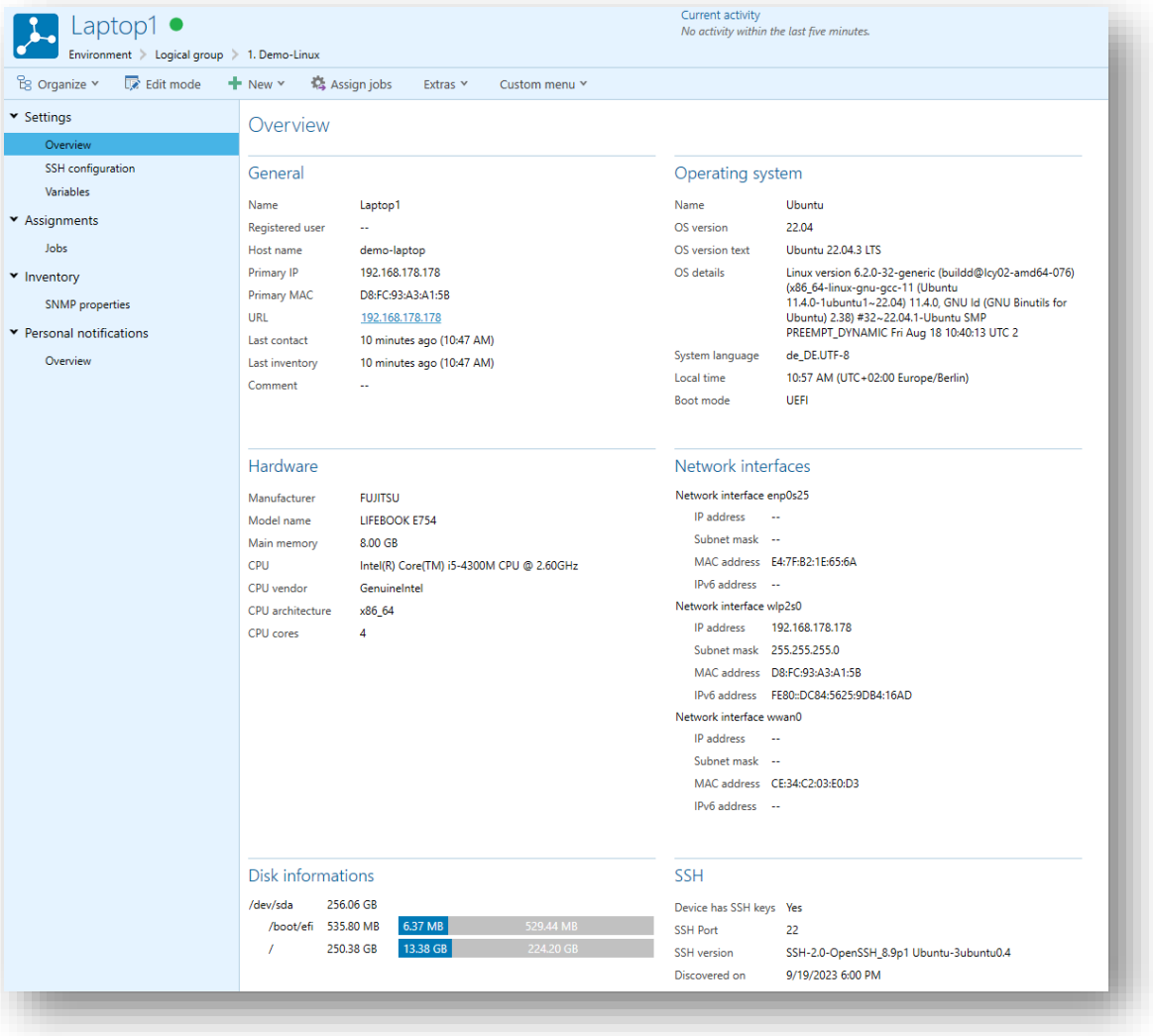


Figure 7 The Result of an Inventory Job of a Linux Device

The newly acquired information can be used in UDGs and read out via bConnect.

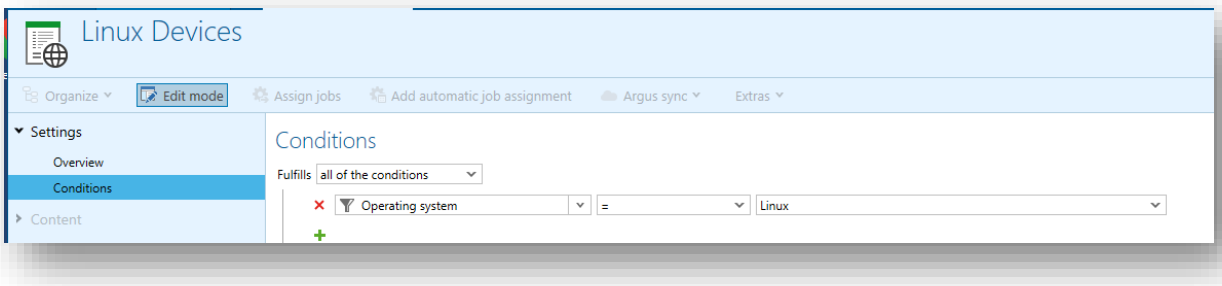


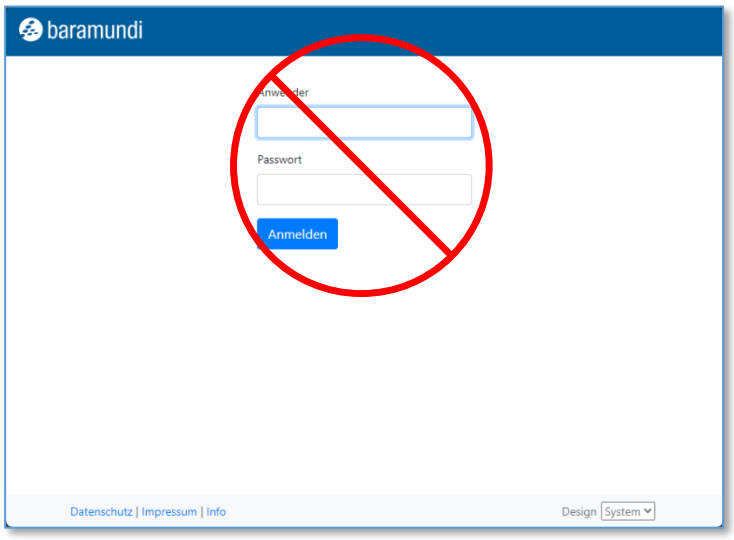
Figure 8 Creating a UDG for Linux endpoints

1.3 Single Sign-On (SSO) In The Kiosk

The baramundi Kiosk for user self-service has had the capability to provide jobs specifically for individual users and user groups since we introduced it in 2018. That requires users to log in to the Kiosk with a username/password that meets company requirements for length and complexity. That can become a barrier to users and limit the usefulness of the Kiosk.

Accordingly, 2023 R2 adds SSO support for Kiosk access.

If the Kiosk is opened via URL in a supported browser, login data is passed through to provide access. If jobs are available for the individual user, they can assign them to their registered devices.



If the Kiosk is started via the icon in the tray, the "Log in" button must be clicked first and an automatic log in will occur.

1.4 Mobile Devices

1.4.1 Android Zero-Touch

In addition to automated provisioning support for Apple devices via DEP, and Windows devices via Autopilot, 2023 R2 now includes support for Android device Zero-Touch enrollment.

Android devices can now be automatically registered in the bMS during commissioning and immediately configured with the specified settings and apps..

Process

Zero-Touch can be set up via a portal provided by Google. New devices can then be entered by the supporting supplier and are immediately visible.
Once registered with Google during commissioning, device information is forwarded to the baramundi Management Server to begin the enrollment process. The device is then visible in the baramundi Management Console and can be provided with a predefined default (or other) enrollment profile. "Fully managed device" or "Dedicated device" are available as profile types.

Zero-Touch in the bMS

To be able to use Zero-Touch in the bMS, a connection must be established once between the bMS and the Zero-Touch infrastructure. After successful commissioning, it is possible in the bMS to determine whether a previously assigned device reset to factory settings may be rolled out again. You can specify that only rule-compliant devices are accepted and define a default logical group of allowed users.

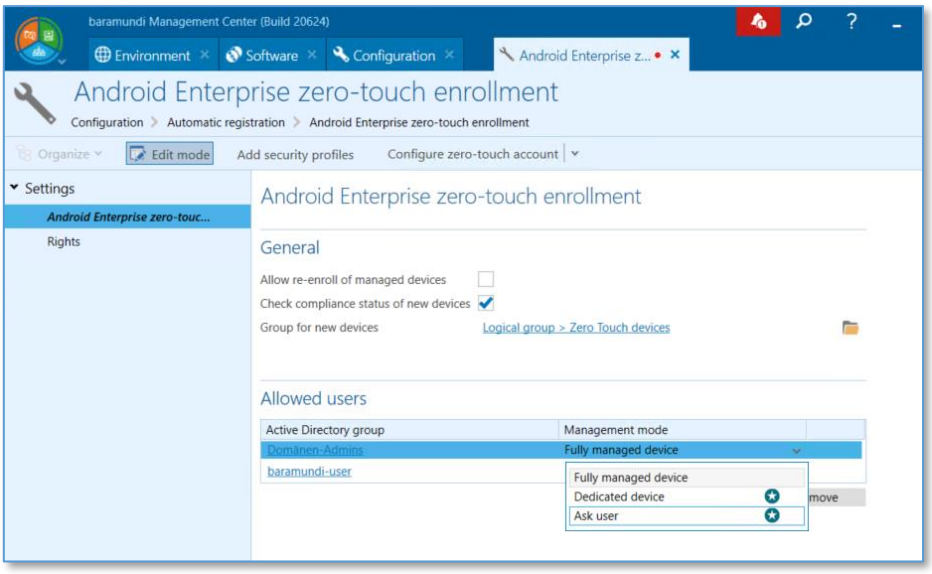


Figure 9 Configuration Page for Zero-Touch

The device can be enrolled as "Fully managed" or "Dedicated" based on the user group or the username. It's also now possible to authorize a user to select the mode during enrollment instead of requiring a separate process in the baramundi Management Suite.

1.4.2 Further Improvements

Improve location accuracy

The "Execute Command" job step for Android Enterprise has been extended with the "Improve Location Accuracy" command.

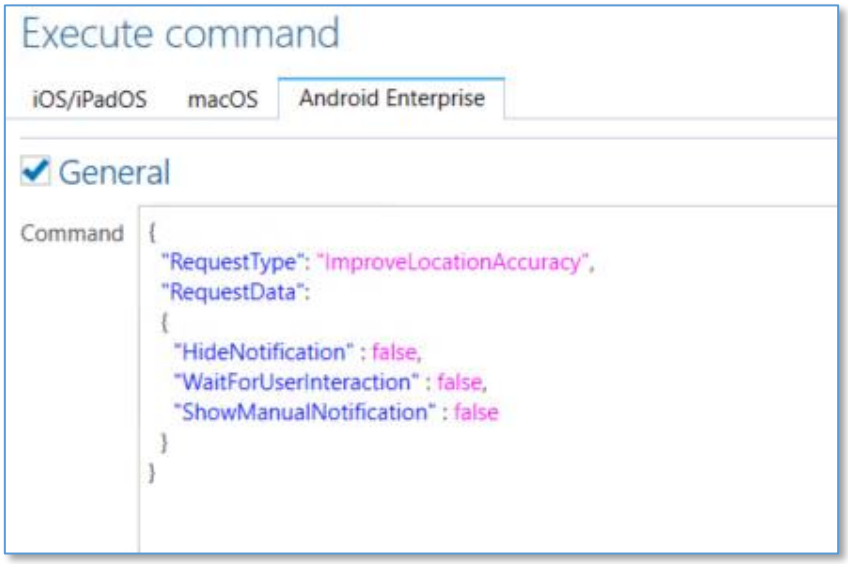


Figure 10 Configuration of the "Improve Location Accuracy" Command

This command invokes the location accuracy enhancement query for the user to enable more accurate location detection.

App Start per Activity

In the template for a Dedicated Device, you can specify activities that initiate the launch of an app, including those that cannot be launched directly from the launcher/home screen (e.g., some system apps).

1.5 Universal Dynamic Groups

1.5.1 New Conditions for UDGs

We have added a new Boolean query for filtering MacOS devices using Apple Silicon processors in UDGs and implemented the ability to a cross reference a UDG that defines a group of devices included in other UDGs.

1.5.2 UDG in UDG

Often there is a certain UDG condition used frequently in various UDGs. To simplify usage, it is now possible to simply include an existing group of devices matching those conditions with a "Group membership".

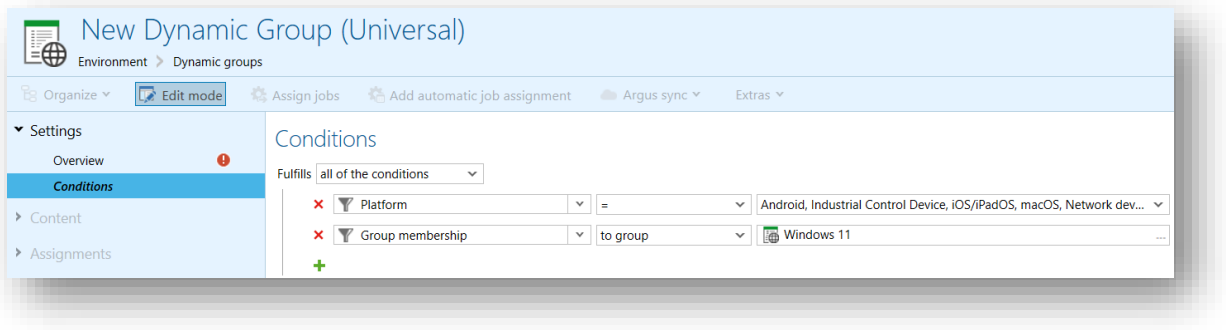


Figure 11 UDG Group Membership

UDGs also support error handling in the event of a circular reference. i.e., when an existing UDG referenced within a new UDG could cause unintended follow-on actions. This is intercepted when saving a new UDG.

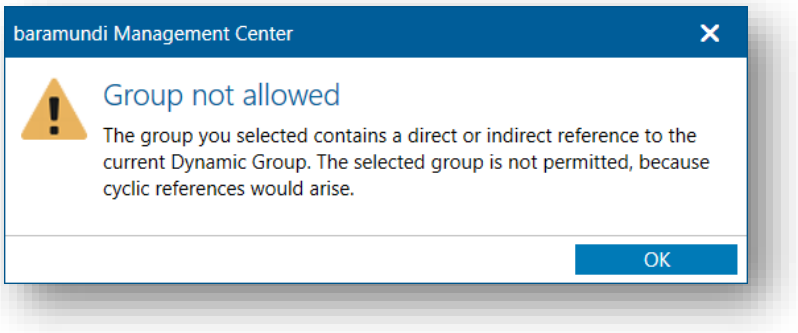


Figure 12 UDG Circular Reference Handling

The baramundi Management Center will also display a warning if a UDG being processed affects a referencing UDG with a stored automatic job assignment.

1.5.3 Apple Silicon

For macOS devices there was a requirement to filter them by processors, i.e., Intel or Apple Silicon. This is now a new query-able condition.

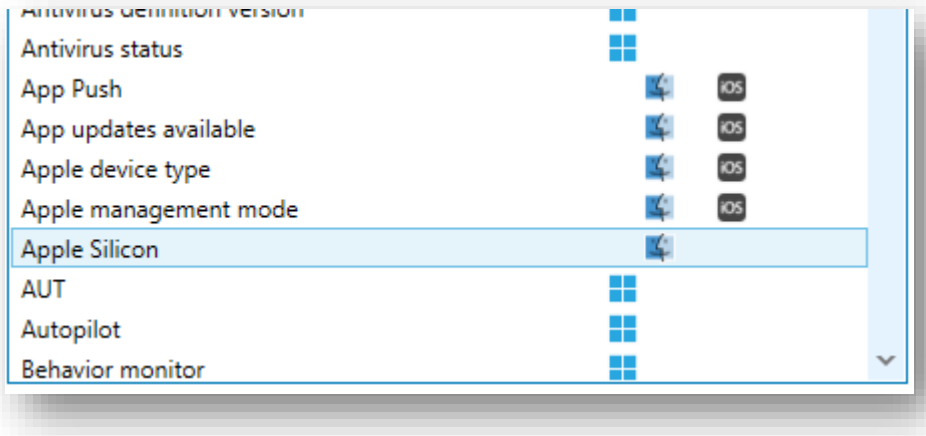


Figure 13 UDG Conditions

The property is easily determined with a Boolean field (Yes/No) for UDG filtering and for automatic job assignments.

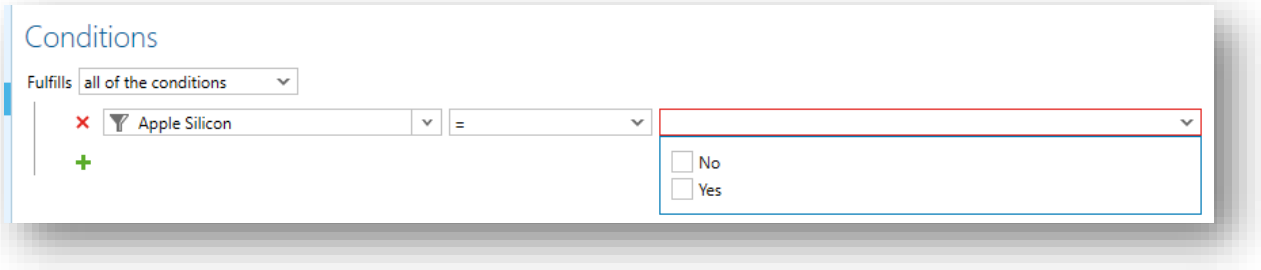


Figure 14 UDG Apple Silicon Filter Query

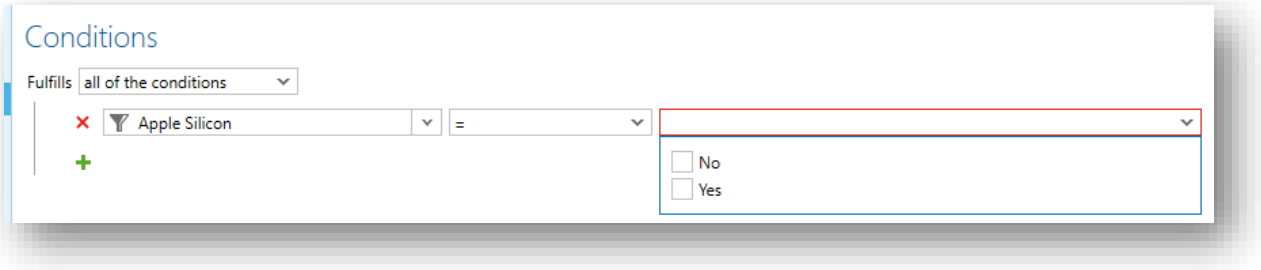


Figure 15 UDG Apple Silicon Filter Query

1.6 Network Devices

1.6.1 Script Execution via SSH

As part of the management of all network devices, it is advantageous to assign script executions to them using baramundi job logic. This is simply done as a new job step in the new "Job for OT or network devices".

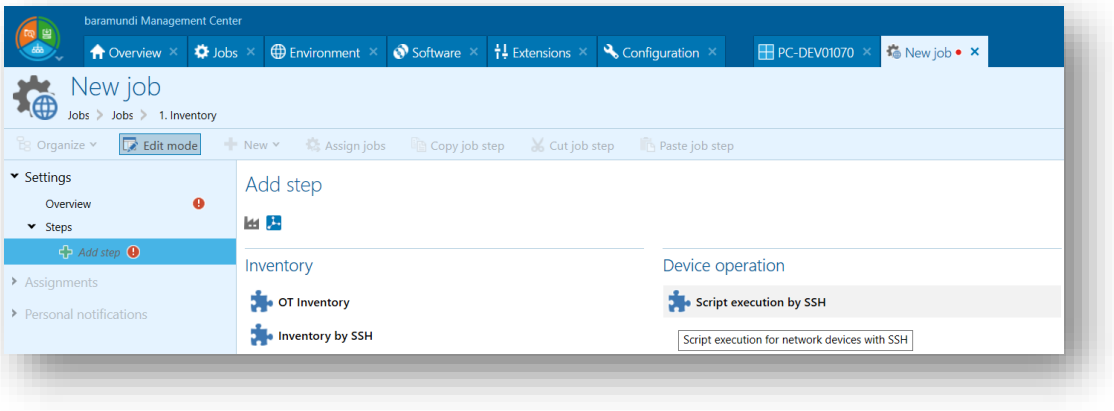


Figure 16 New Job Step

That enables you to refer directly to a script on the DIP to be started for the respective assigned device.

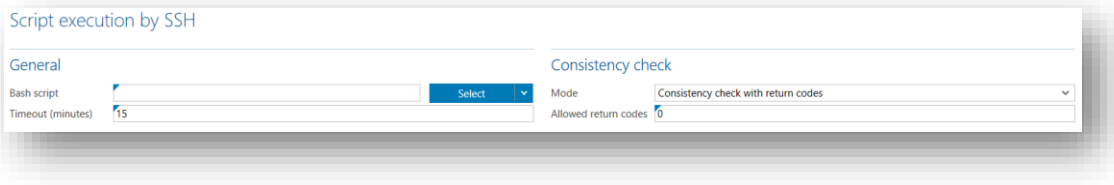


Figure 17 Script Execution via SSH

Example Script:

```
#!/bin/bash
# Choose port between 1024 and 65535
$SSHPORT = 1025
sed -i -e "/Port /c\Port $SSHPORT" /etc/ssh/sshd_config
sleep 5
# Restart SSH service
service sshd restart
exit 0
```

1.6.2 Network Scan Profile

Working with network scan profiles has been extended. The creation of jobs for scans has been simplified by adding the option to create a job directly in the menu of the network scan profile.

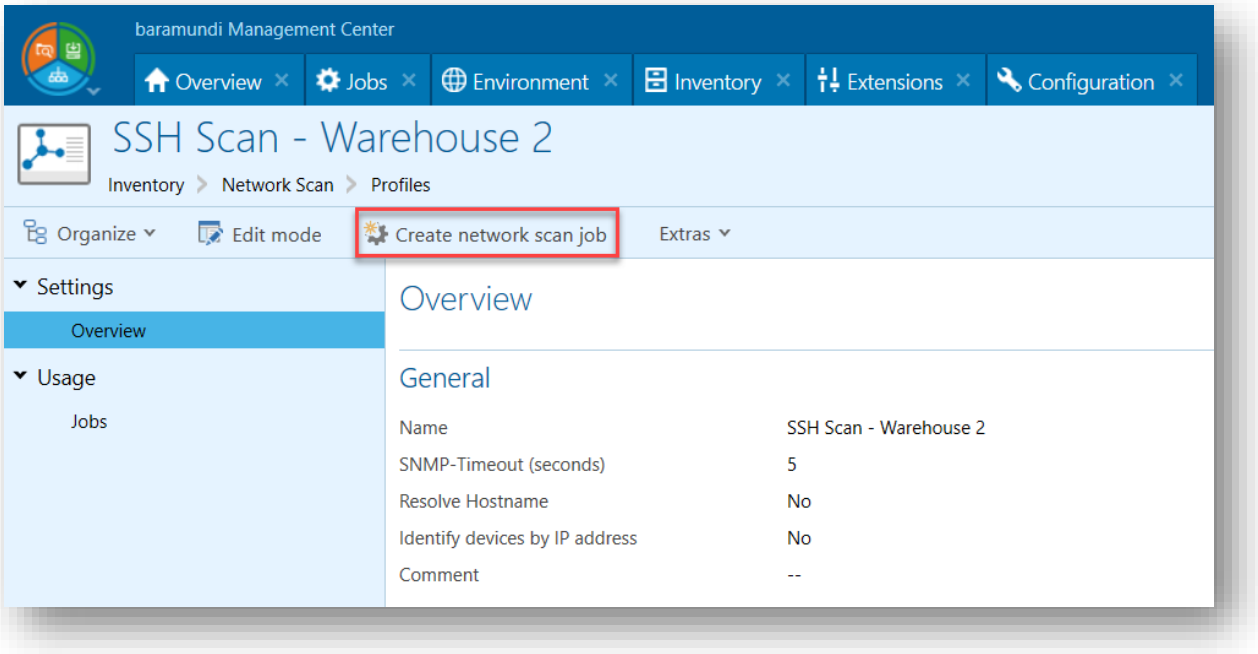


Figure 18 Network Scan Profile – Create New Job

In addition, there is now an option to exclude other matching end devices outside the target group from the profile, such as when network devices with the same identifiers (e.g., name and IP address) exist in several locations.

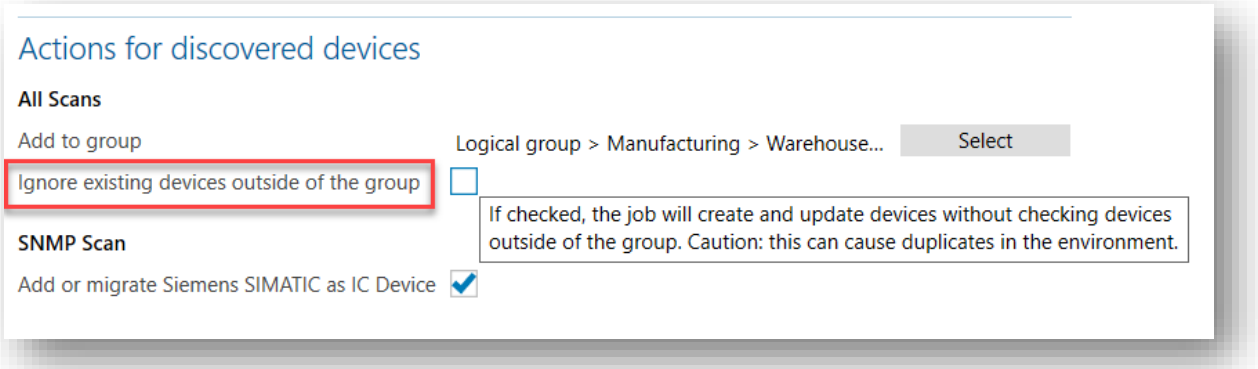


Figure 19 Network Scan Profile – Ignore Other Devices

1.7 Further developments in Argus Experience

Some endpoint problems can occur suddenly and without warning. But the vast majority of issues make themselves known more or less slowly or subtly. Those type of problems are a common source of frustration for end users and a regular time sink for IT admins. baramundi Argus Experience (bEX) provide tools for detecting, analyzing and addressing many typical endpoint performance and reliability issues early and proactively to improve user experiences, productivity and IT efficiency.

1.7.1 Slow Computer Start Up Times

One of the most common user complaints is long boot times. Shortening startup time offers enormous potential for helping users begin productive work more quickly. That's just one example of how Argus Experience provides valuable data and insights for optimizing endpoint and network performance. You can also examine factors such as:

- Are individual devices or groups of endpoints particularly troublesome?
- Are there certain periods when long boot times are more frequent?
- Which software and hardware is installed in problematic devices?
- Are certain startup processes associated with long boot times?

These elements can be captured and evaluated with bEX. This enables IT admins to overcome these bottlenecks company-wide, e.g. through software updates, operating system upgrades or hardware replacements.

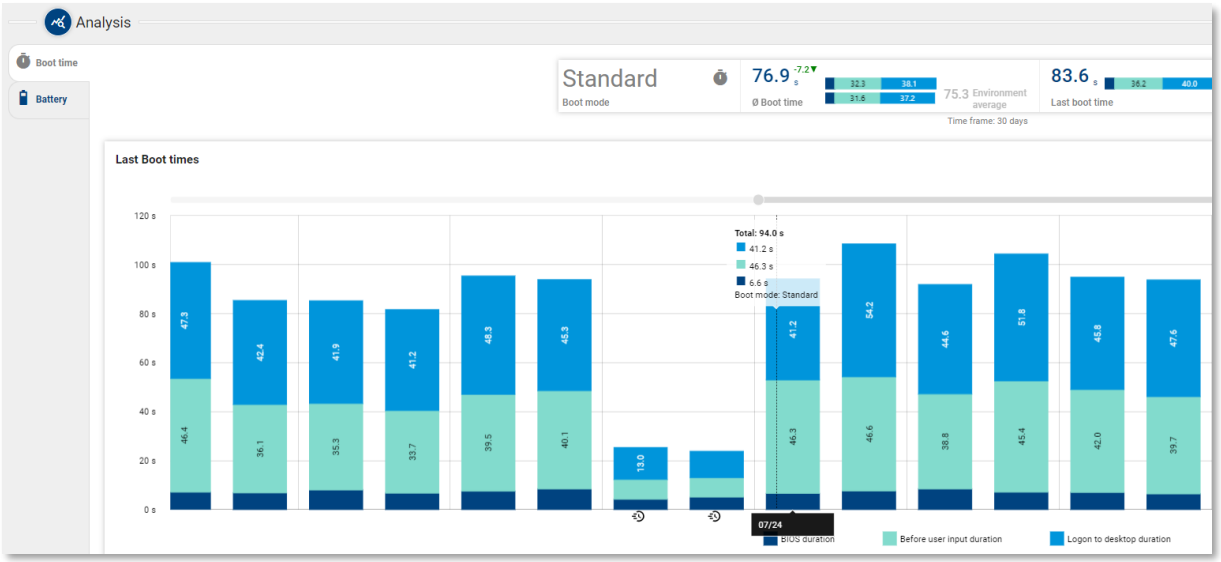


Figure 20 Detailed Start Times of An End Device

1.7.2 Declining Battery Life in Laptops

Batteries in electronic devices naturally lose capacity over time, especially in laptops subject to heavy and frequent mobile use. Users often don't notice the decline until only a few

minutes of power remain and they immediately must find a place to plug it in before the computer shuts down at a critical moment.

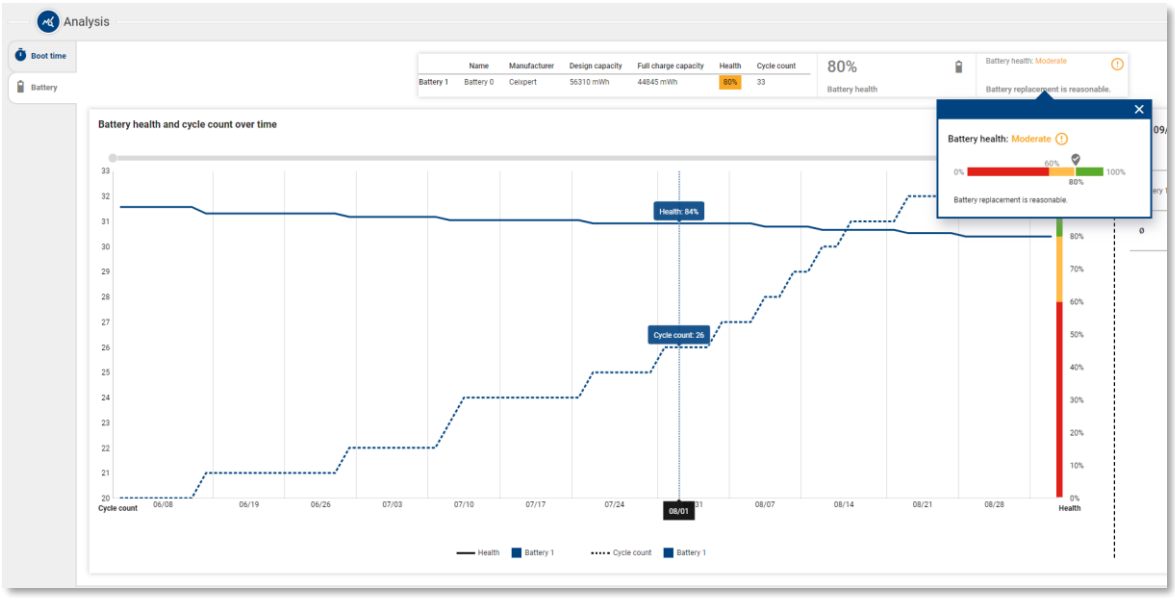


Figure 21 Declining Laptop Battery Capacities

This scenario can be effectively avoided with baramundi Argus Experience. Battery performance data figures can be recorded and evaluated so IT admins can provide affected users employees with a new battery before the problem becomes acute.

1.7.3 Program Crashes

Changes in different versions of applications can trigger far-reaching problems. One example is PowerPoint. Functional differences over time could cause presentations created in one version to not work properly or at all on devices with a different version. That in turn puzzled and frustrated users.

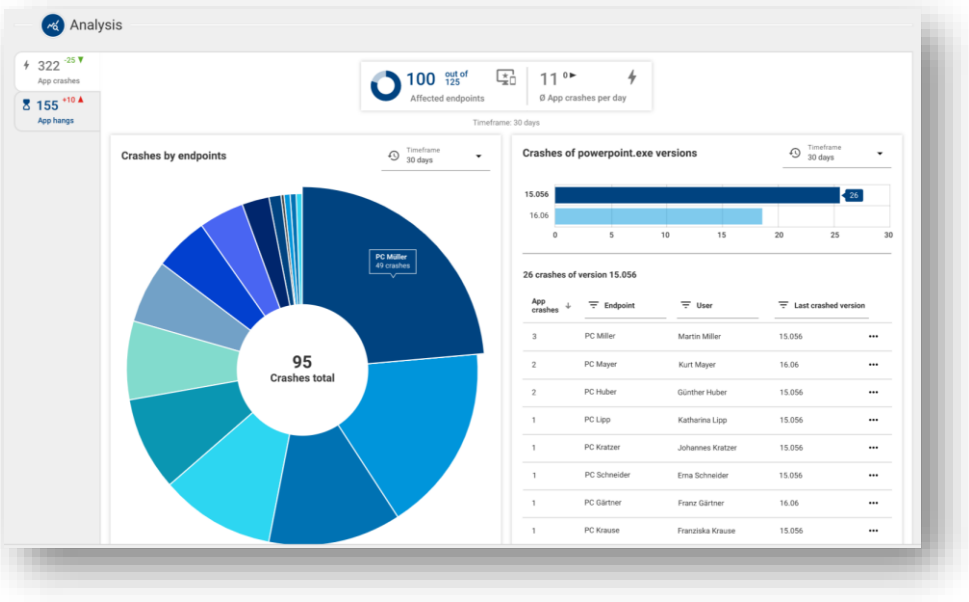


Figure 22 Detailed Display of Application Crashes

IT admins can eliminate these frustrations with bEX, which shows a correlation of which application versions cause more crashes or aborts. Troublesome versions can be updated promptly.

1.7.4 Benchmarking Results

The wealth of data collected in Argus Experience can seem overwhelming at first. But when used in a logical and structured approach to establish performance benchmarks, aggregated bEX data can provide highly valuable insights for classifying, understanding and implementing appropriate responses to performance trends and anomalies.

For example, the environment evaluation can show day-to-day system stability relative to other environments managed in baramundi Argus Experience.

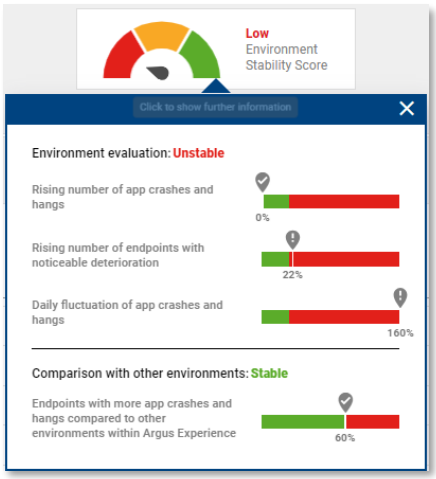


Figure 23 Benchmarking Environment Stability

Concrete comparisons of individual measures to average values of the entire environment are provided in many places in bEX.

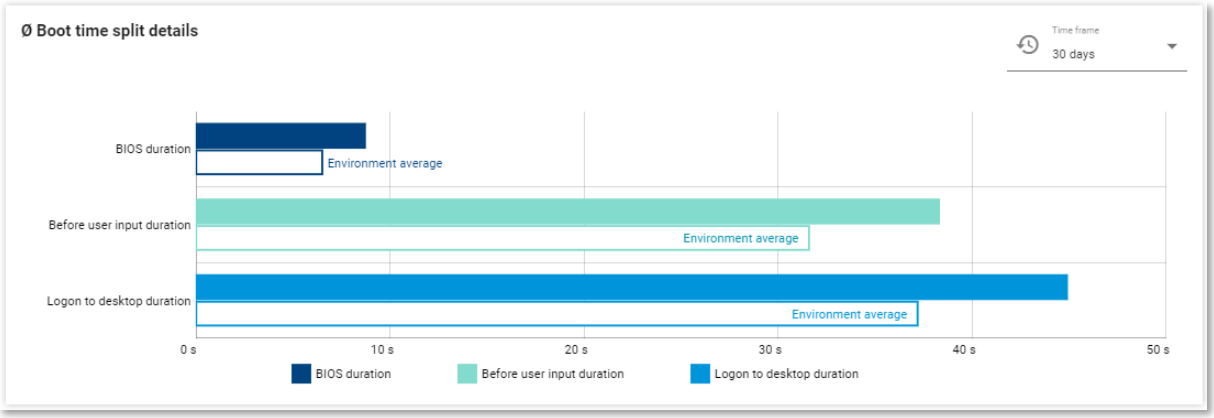


Figure 24 Overview of Endpoint Start Times Compared to the Environment Average

1.7.5 Collect End User Feedback

The endpoint stability and performance data does not always provide a holistic picture of the IT environment. Employees are often unable to work productively because the device is performing poorly, or the software is unstable. Sometimes employees will submit a support ticket, but many often instead decide to tolerate problems. The causes of the problems will remain unknown to and unaddressed by IT, even when other users may be experiencing the same issues.

Consequently, it is critical not only data to capture and analyze objective endpoint performance data, but also to correlate it with subjective user feedback so an appropriate fix can be implemented. That's why Argus Experience makes it possible to collect and analyze user reports on a regular basis.

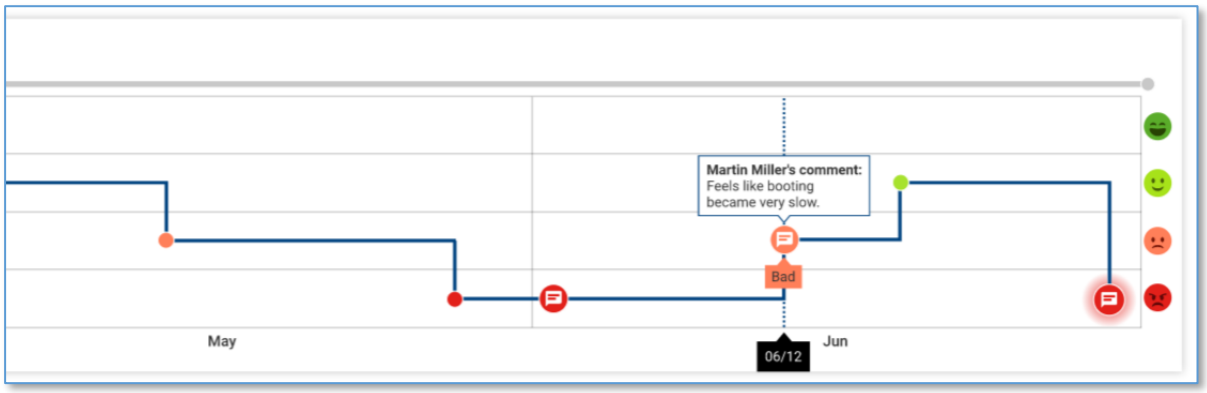


Figure 25 Employee Feedback on an Endpoint Device

The employee can easily provide feedback via the tray notifier. IT admins can define in advance the type of data to be collected and how frequently.
The combined analysis of objective and subjective performance data provides IT admins with a more holistic understanding of the IT environment they manage so they can optimize performance, productivity and user satisfaction.

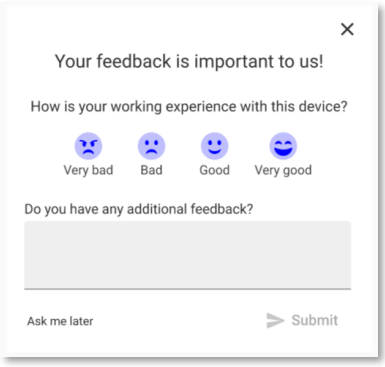


Figure 26 Tray Notifier for End User Feedback

1.8 Miscellaneous

1.8.1 Identification Of Endpoints through UUID (Preview)

The Universal Unique Identifier - UUID for short - is stored in the firmware (UEFI) of modern computers and enables the system to be uniquely identified. In the context of endpoint management, it is essential to identify the targets for management actions beyond doubt so that the wrong endpoint is not accidentally reset, for example.

If a baramundi Management Agent is installed, the bMS uses a client-side certificate to confirm the identity. When a system is to be reinstalled and no agent is onboard yet, the bMS has used the network card MAC address during boot to ID the system. But more recently, hardware vendors have created increasingly slimmer hardware, often with no integrated network cards. Users instead have turned to external network adapter dongles or multi-port docking stations, making it difficult to identify an endpoint with its MAC address.

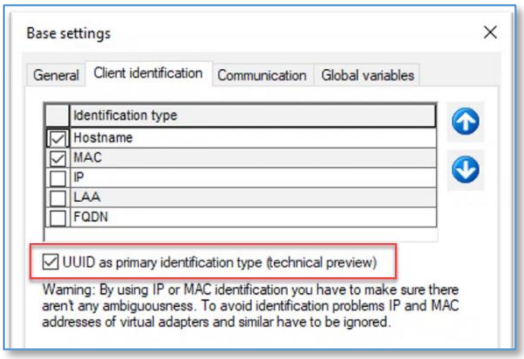


Figure 27 Activation of UUID-Support

In order to continue to ensure reliable identification, the bMS now supports use of the UUID identifier. Initially in Preview, the UUID can be used if it is already known in the bMS. For example, endpoints whose UUID was transferred by the bMA can be reinstalled with OS-Install. However, automatic UUID recording during the boot process is not yet possible for new endpoints whose UUIDs have not yet been transferred to the bMS. But they can be installed if the UUID has been manually stored in the endpoint entry in the bMC.

Note: If the DHCP options required for the network boot are set via configuration on the DHCP server, a MAC address is also required for identification in the preview.

1.9 System Requirements and Compatibility

1.9.1 baramundi Management Server and baramundi PXE Relay

- Supported platforms: see 1.9.16 (bMS column).
- .NET Core 6.x, Asp.Net Core Framework 6.x and .NET Core Desktop 6.x in the same versions is required.
- German and English are supported languages.
- We recommend using a dedicated server to operate the baramundi Management Server.
- Certain ports[1] must be available for the baramundi Management Server.
- Integration into a Windows domain - Windows Active Directory is recommended.
- Hardware requirements server/network:
  - Available RAM: at least 8 GB; recommended 16 GB
  - Processor: at least 4 cores
  - Disk space for installing the bMS: at least 5 GB
  - Network card: at least 1 GB

1.9.2 Database connection

- Supported platforms:
  - SQL Server 2022
  - SQL Server 2019
  - SQL Server 2017
  - SQL Server 2016 SP3 (deprecated)
  - SQL Server 2014 SP3 (deprecated)
    Note: bMS versions from 2024 R1 are no longer compatible with SQL Server 2014.
  - Oracle 19c (deprecated)
    Note: bMS versions from 2025 R2 are no longer compatible with Oracle databases. A switch to MS-SQL or our cloud solution (bMSaaS) is recommended.
- At least 10 GB hard drive space for the baramundi database.
- The baramundi Management Server is a database-oriented system, so ensure sufficient database performance and a high-performance connection.

[1] A list of ports used is available in our online help https://docs.baramundi.com.

- For environments with up to 250 clients, SQL Express Edition can be used.
- Operation of the database server and the baramundi Management Server on one system is permissible. For greater requirements and larger environments, a dedicated database server is recommended.

1.9.3 baramundi Management Center

- Supported platforms for the baramundi Management Center, as well as Automation Studio, License Management, Remote Control and ImageMount: see 1.9.16 (Column bMC).
- Microsoft Edge WebView2 Runtime is required.
- Screen resolution:
    - Minimum screen resolution 1024 x 768 pixels.
    - Recommended resolution is 1280 x 800 pixels or higher.
    - All resolutions refer to a font size display of 100%.

1.9.4 baramundi OS-Customization Tool

- This baramundi Management Center add-on for customizing Windows 10 or Windows 11 images, provided via managed software, is supported on the platforms visible in MSW.
- The Microsoft ADK for Windows 11 is required to customize the Windows images.

1.9.5 baramundi DIP

- Supported platforms: see 1.9.16 (Column bDIP).
- Microsoft Visual C++ Redistributable in version 2015.x-x64 - VC-2022 is required.
- .NET Core 6.x, Asp.Net Core Framework 6.x and .NET Core Desktop 6.x in the same versions is required.
- A 64-bit system is required for the baraDIP installation.
- 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.

1.9.6 baramundi Gateway

- Supported platforms: see 1.9.16 (Column bGW)
- We recommend not operating other services on the same system as the baramundi Gateway.
- Integration in an Active Directory is not necessary.
- The baramundi Gateway should be operated in a DMZ environment to ensure strict separation from the bMS server. Operation of baramundi Gateway and bMS on one system is not supported.

Hardware requirements server/network:

- Available memory: at least 4 GB; recommended 8 GB
- Disk space for installing the baramundi Gateway: at least 1 GB
- Network card: at least 1 GB

1.9.7 baramundi OS-Install

- The Microsoft ADK for Windows 11 is required to customize the Windows images.
- The ADK is available in Managed Software as ADK10, version 2209.

1.9.8 baramundi License Management

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

1.9.9 baramundi Interfaces

- bConnect version 1.1 and version 2.0 are both available.
- Deprecated - The bMOL (baramundi Management Object Language) interface is no longer being developed. We recommend switching to and using our bConnect interface.
  Note: The bMOL interface will no longer be available as of bMS version 2024 R2.
- Deprecated - The httpMOC interface is no longer being developed. We recommend using our interface bConnect.
  Note: The httpMOC interface will no longer be available as of bMS version 2024 R2.
- Deprecated - Direct access to the database (SQL/Oracle) is not supported. We recommend using our interface bConnect.
  Note: The DB-Doku will therefore no longer be delivered with 2023 R2.

*) Deprecated: Feature updates and bug fixes are no longer provided. Critical security updates are provided for the current version.

1.9.10 baramundi Network Devices

- Supported platforms: see 1.9.16 (Column bND)
- Network scanner is an add-on to Windows bMA. It is available to all customers via Managed Software.
- .NET 4.7.2 is required.

1.9.11 baramundi OT Devices

- Data acquisition is done via SNMP version1, version2c, version3.
- Supported platforms: Siemens SIMATIC S7 1200 and 1500

1.9.12 baramundi Kiosk

- Supported platforms: see 1.9.16 (Column bND)
- For user logon and job assignment on a per-user basis, a Windows Active Directory including configured baramundi AD-Sync is required.
- baramundi Kiosk supports the following browsers, each in the current version:
  - Microsoft Edge
  - Google Chrome
  - Mozilla Firefox

1.9.13 Support for Android

- Supported Versions:
    - Android Enterprise 13
    - Android Enterprise 12
    - Android Enterprise 11
    - Android Enterprise 10
    - Android Enterprise 9
    - Android Enterprise 8 *)
    - Android Enterprise 7 *)
    - Android version 4.0.4. up to version 9 with Legacy Agent
      Note: No longer supported on version 2024 R1 or later.
    - Samsung KNOX on Android version 4.0.4 up to version 9 with Legacy Agent
      Note: No longer supported as of version 2024 R1.

*) This operating system has limited support. This may mean that new features are not usable on this operating system or features can no longer be used as before. No support for Zero-Touch.

1.9.14 Support for iOS

- Supported Versions:
    - iOS Version 17
    - iOS Version 16
    - iOS Version 15
    - iOS Version 14
    - iOS Version 13
    - iOS Version 12

1.9.15 Support for macOS

- Supported Versions:
    - macOS 14.x (Sonoma)
    - macOS 13.x (Ventura)
    - macOS 12.x (Monterey)
    - macOS 11.x (Big Sur)
    - macOS 10.15 (Catalina)

1.9.16 Support for Windows

- 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 und DipSync Service
- bMA: baramundi Agent for Windows
- bND: baramundi Network scanner as add-on to Windows bMA
- X: Completely supported.

Platform	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows Server 2022 Standard/Datacenter (Desktop display)	X	X	X	X	X	X	X
Windows Server 2022 Standard/Datacenter (Core)						X	
Windows Server 2019 Standard/Datacenter (Desktop display)	X	X	X	X	X	X	X
Windows Server 2019 Standard/Datacenter (Core)						X	
Windows Server 2016 Standard/Datacenter (Desktop display)	X	X	X	X	X	X	X
Windows 11 Pro / Enterprise (N)		X	X		X	X	X
Windows 10 Pro / Enterprise 22H2 (N) (32 Bit und 64 Bit)		X	X		x64	X	X
Windows 10 Pro / Enterprise 21H2 (N) (32 Bit and 64 Bit)		X	X		x64	X	X
Windows 10 Enterprise 2021 LTSC (32 Bit and 64 Bit)		X	X		x64	X	X
Windows 10 Enterprise 2019 LTSC (32 Bit and 64 Bit)		X	X		x64	X	X
Windows 10 Enterprise 2016 LTSB (32 Bit and 64 Bit)		X	X		x64	X	X
Windows 10 Enterprise 2015 LTSB (32 Bit and 64 Bit)		X	X		x64	X	X

1.9.17 Windows support with limitations

These operating systems are supported by baramundi components only to a limited extent. This may mean that new functions are not usable or that other functions can no longer be

used. Due to the complexity and large number of legacy systems, baramundi cannot guarantee functionality on these systems. Due to the limitations, we recommend the use of newer and current operating systems. We cannot provide support for the baramundi server components on operating systems that are out of Microsoft mainstream support.
baramundi server components (bMS/R, bMC, bAS, bGW, bDIP)

- (1): Is only supported to a limited extent now that Microsoft has ended (basic) product support.
- (2): Version 2021 R2 of the bMA must be used for this operating system. A more recent bMA cannot be run on this operating system. There will be no more security improvements for the bMA 2021 R2.

	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows Server 2012 R2 Standard/Datacenter (Server mit grafischer Benutzeroberfläche)						1	1
Windows Server 2012 Standard/Datacenter (Server mit grafischer Benutzeroberfläche)						1	1
Windows Server 2008 R2 SP1 Standard /Enterprise / Datacenter						1	1
Windows Server 2008 SP2 Standard / Enterprise / Datacenter (32 Bit / 64 Bit)						1	1
Windows 10 Pro / Enterprise 1703 bis 21H1 (N) (32 Bit und 64 Bit)						1	1
Windows 8.1 Pro / Enterprise (32 Bit / 64 Bit)						1	1
Windows 7 SP1 Professional/Enterprise/Ultimate (N) (32 Bit und 64 Bit)						1	1
Windows Vista SP2 (32 Bit / 64 Bit)						1	1
Windows XP SP3 (32 Bit)						2	

1.9.18 Languages

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

German, English

The bMA for Windows clients supports user messages in:

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

The baramundi Kiosk supports:

German, English, Polish

More languages can be added by administrators.

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

German, English

1.10 Product improvements in detail

1.10.1 Removed discontinuations / removed properties

- The reports "Comparex Miss Marple" are no longer supported and have been removed.
- The baraDIP transmission path HTTP has been removed. Only HTTPS is supported now.
- The documentation file for the database schema is no longer available. To access baramundi data, bConnect is recommended.
- Under `Application - Installation - Parallel installation mechanism`, as well as `Application - Uninstallation - Parallel uninstallation mechanism`, only the `baramundi Deploy Script (bDS)` is supported since 2023 R2. This means that the obsolete baramundi Deploy Package and Rational Visual Test 6.5 are no longer supported. Note: It can still be selected in the bMC, but is no longer supported.
- The `baramundi Virtual` module, including the `Manage Virtual Machine` job step, will be discontinued in version 2023 R2 and will then no longer be available. It can still be selected in the bMC, but is no longer supported.

1.10.2 General

- The signing of our setups/files now shows baramundi software GmbH as the manufacturer, instead of baramundi software AG.
- For new customers, the outdated Patch Management Patches (Classic) is no longer displayed in the bMC. Existing customers are advised to switch to the `Manage Microsoft Updates` job step. The provision of the patch data `bpmda-ta3_reduced_signed.zip/bpmdata3_ signed.zip` will be discontinued as of April 2024.
- If an Eval license is used (e.g. in the test environment), the outdated Patch Management Patches (Classic) is no longer visible in the bMC.
- The baramundi licensing now also allows the specification of an activation date, the date can be viewed under `bmc - Configuration - License configuration - Licenses`.

1.10.3 Windows Agent (bMA)

- If the bMA triggers a restart of the device, the user now receives a further message in the form of a dialog box, with which he can delay the restart by a few seconds.
- Under `bMC - Configuration - Server - Management Agent`, the option `Allow setCustomVar via BMACMD` can be used to set whether the setting of variables via BMACMD.exe from the client is allowed. After the Up-date the option is switched on. Switched off by default for new databases.
- The baramundi TrayNotifier window can now no longer be accidentally closed using Alt+F4 or the ESC key.
- When executing a file copy operation of a bD script, incorrect path specifications are now automatically corrected by whitespaces at the beginning or end of the path. This means that the copy operation now also works correctly when installing drivers for Surface Pro 9 devices.
- Bugfix: The timeout set on the job is reset if the situation "a job is already active" occurs. Sometimes the job is then never automatically canceled on the client.
- Bugfix: The hardware inventory runs with special Windows 11 clients on the error "clinvent.exe has returned no result". This means that the bDX update "Upgrade_hwinfo.dll_to_v7.47.bdx" is no longer necessary.
- Bugfix: If variables are set in jobs via bMACMD.exe, performance losses can occur on the bServer if a large number of variables is set and the job is executed on many clients simultaneously.
- Bugfix: The software inventory needs very much memory with some systems and crashes under circumstances with error code 309.
- Bugfix: An (offline) software inventory runs into an SQL error if very long file paths are captured.
- Bugfix: If an application is redistributed with the option `Application restarts client`, the bMA waits only 120 seconds after the end of the installation for the reboot and then triggers the reboot itself. (Now it waits for the reboot until the job timeout).
- Bugfix: In rare cases, the agent cannot perform hash validation of MSW files and the job aborts with error "The hashes for file validation could not be retrieved from the server". The error frequency has been significantly reduced.

1.10.4 Management Center (bMC)

- The name of the `industrial control unit` no longer has to be unique. Any number of devices with the same name can now be created.
- The setting for the `security context` under `Job - Step - Server side Action` has been renamed to `bServer context (LocalSystem or Service user)` so that it is clear which user is used to execute the baramundi Deploy script.
- Under `bMC - Environment - Client - Overview` the version of the operating system is also correctly detected/displayed for clients with Windows 11 IoT Enterprise.
- When copying a `Universal Dynamic Group`, the name and the display name are adjusted if both were the same before.
- If an attempt is made to switch a client to Internet mode even though no gateway is configured, a warning message appears.
- `Dynamic groups (Universal)` can now be used within other `dynamic groups (Universal)`.
- Bugfix: If a password is stored for an SNMP profile under `bMC - Inventory - Network Scan`, this password is overwritten when the configuration is reopened.
- Bugfix: At the automatically created energy asset for monitors, the energy data are also displayed for the standby mode, although these cannot be recorded.
- Bugfix: If a `Dynamic Group (Universal)` is created with the property `Primary IP is empty` or `is not empty`, another useless input field appears.
- Bugfix: If a `Dynamic Group (Windows)` is modified in such a way that it contains an invalid `SQL statement`, it is not possible to save it, but after leaving the dialog via Cancel the Dynamic Group disappears from the bMC and reappears only after a module restart.
- Bugfix: The option `Job - Advanced - Activate screen saver at job end` has no effect. This option has been removed. If this option was set in the job, it is automatically switched to `no additional action`.
- Bugfix: Under `bMC - Inventory - Software detection rules` the deletion of rules is not possible if the column `Type` is hidden.

- Bugfix: In multi-domain environments the login to the bMC is partly not possible if the access authorization is configured via a group membership.
- Bugfix: If an existing job is read in again via bDX import, job steps that have already been performed are deleted and can therefore no longer be used.
- Bugfix: Some HTML views hide the display of a bMC notification.
- Bugfix: `Personal notifications`, which should be issued in the interval, do not appear exactly in the specified interval.
- Bugfix: If the dialog `bMC - Configuration - Server - Settings - PXE support` is opened and confirmed with OK, a restart of the bServer is requested even if no changes were made.

1.10.5 OS Install

- The option `Join domain only after OS installation` under `bMC - Operating system - Hardware profiles - Hardware profile` has been removed.
- In the `Boot Media Wizard` x64 UEFI is now the default.
- Bugfix: When adding a driver via the deprecated method `bMC - Operating Systems - Driver - New - Windows Driver` a database error may appear.
- Bugfix: If under `bMC - Configuration - Boot Environments` at a boot environment the option `Visible in the boot menu` is not set, then this cannot be used correctly also in the job or by setting at the client.

1.10.6 Microsoft Autopilot

- Under `bMC - Configuration - Automatic Registration - Microsoft Autopilot`, an Azure AD group can be stored in the Azure AD Group ID field. Only devices of this group will then be synchronized to the bMS.
- During synchronization, an attempt is now made to match new Autopilot devices with existing devices on the basis of the Mac address and the host name. This also marks existing devices as autopilot devices.
- Bugfix: If an error occurs while synchronizing Autopilot devices, the whole process terminates.

- Bugfix: The serial number of autopilot devices overwritten by the hardware ID on every autopilot sync.

1.10.7 Mobile Devices

- Enrollment of Android Enterprise devices from Android 9 is possible using Android Zero Touch.
- In the template for the management of dedicated devices on Android devices, it is now possible to specify the start activity of an app that is started instead of the default activity.
- In a Universal Dynamic Group, the `Apple Silicon yes/no` condition can be used.
- The Android Enterprise Agent now understands the `ImproveLocationAccuracy` command to be able to configure the accuracy of the location detection on the device. This can be executed by an execute command - Andro-id Enterprise step. Furthermore, there is a fallback for the `GetLocation` command so that at least a rough location is returned.
- `Ultra-wideband (UWB)` is now also displayed on the Android Enterprise device under Device inventory.
- Bugfix: The rights inheritance for the node `bMC - Configuration - Automated Enrollment - Apple Automated Device Enrollment` does not work correctly.
- Bugfix: Search for IOS devices does not support phone number, ICCID and IMEI.
- Bugfix: When installing an Enterprise Wifi on Android Enterprise devices the error message "The enterprise network is missing either the root CA or domain name" may appear. To be able to install the profile correctly, it is now possible to specify a domain at the Wi-Fi profile module under bMC - Extensions - Profiles for mobile devices.
- Bugfix: If an iOS device does not provide valid XML data, e.g. the name of a CurrentCarrierNetwork in the hardware inventory, jobs can no longer be executed on this system.
- Bugfix: The enrollment URL for Android Enterprise devices displayed in the bMC leads to an error on the device. However, the QR code worked correctly.
- Bugfix: To be able to edit MDM jobs, rights on `bmc - environment` are required.

- Bugfix: If a user is accidentally deleted from an Android Enterprise device, it cannot be set again. (Now an AD sync will restore the user).

1.10.8 bServer

- Jobs with steps for `Server Side Actions` (SSA) now no longer require an interactive login in the LocalSystem security context and are therefore also executed in hardened environments.
- Improved database queries when restarting job targets, resulting in significantly fewer SQL deadlocks.
- Bugfix: For jobs scheduled by interval, the error counter for `retry in case of error` is not reset even after a successful run and rescheduling of the job.
- Bugfix: Notifications stored under `bMC – Personal Settings – Notifications` may lead to other users not being able to log on to the bMC after the user has been deleted.

1.10.9 AD Sync

- At the AD user (`bMC – Environment – Users and Groups`) the fields `First name`, `Last name` and `Supervisor` are now additionally available.
- Bugfix: If certain replication projects are available in AD, a `user synchronization job` may run into the error "Object reference not set to an instance of an object".
- Bugfix: A `user synchronization job` may run permanently on error if a user group has been moved in AD.

1.10.10 PXE relay

- Bugfix: Client hangs in PXE phase when booting via PXE relay if boot is used without DHCP options.
- Bugfix: If the latency from the PXE relay to the database is high, opening the bMC on the PXE relay (to configure the PXE relay) can cause a timeout. The maximum wait time for this has been increased significantly.

1.10.11 bConnect

- `networkEndpoints` are available.

- `sshConfiguration` and `snmpProperties` can be read.
- Query of `PatchLevel` on AppleEndpoint is available.

1.10.12 Network devices

- A mini inventory for selected Linux distributions is possible. The determined data can be used in universal groups and is also available via bConnect.
- The specification of a `Registered User` on a `network device` is now supported.
- In the `job for OT or network device` steps `script execution via SSH` are now possible.
- Under `bMC – Inventory – Network Scan – Profile` there is a new setting `Ignore existing devices outside the group`.
- Under `bMC – Inventory – Network Scan – Profile` a job can now be generated quickly via the `Create Network Scan Job` button.
- Under `bMC – Environment` a `personal notification` can be configured on the network device as well as on the industrial control device.
- Bugfix: If a comment is set on the network device, this may be reset by another SNMP scan.
- Bugfix: Under `bMC – Inventory – Network Scan – Detection Rules` certain valid OID can not be configured because they are rejected as invalid.

1.10.13 macOS

- Bugfix: Some devices are detected incorrectly, e.g. a MacBook Air M2 is recognized as iMac 27" (Late 2013).
- Bugfix: Installation of local macOS PKGs larger than 2 GB fails with the message "No manifest data recieved".

1.10.14 baraDIP

- The baraDIP service for bBT transfer and DipSync has been deeply reworked. Note: a bMS version 2023 R2 or higher is not compatible with older baraDIP. When

updating, it is therefore mandatory to replace the baraDIP services on all DIP servers in a timely manner.

- Under `bMC – Configuration – DIP – DIP management`, the trust position can now be conveniently removed for individual DIP servers by resetting TLS and restored by configuring TLS.

1.11 Notes and known Limitations

1.11.1 Discontinuations

- Patch updates via the `Deploy Microsoft Patches (Classic)` job step are discontinued. The provision of the patch data `bpmdata3_reduced_signed.zip/bpmdata3_signed.zip` will be discontinued as of April 2024. It is recommended to switch to the `Manage Microsoft Updates` job step.
- bMS versions 2024 R1 and later are no longer compatible with MS-SQL Server 2014.
- Android version 4.0.4. up to version 9 is no longer supported as of bMS version 2024 R1.
- Samsung KNOX on Android version 4.0.4 up to version 9 is no longer supported as of bMS version 2024 R1.
- Offline help will no longer be available from bMS version 2024 R1. We recommend using the online help on a device with Internet access.
- The bMOL interface will no longer be available as of bMS version 2024 R2.
- The httpMOC interface will no longer be available as of bMS version 2024 R2.
- bMS versions 2025 R2 and later will no longer be compatible with Oracle databases. A switch to MS-SQL Server or our cloud solution is recommended.

1.11.2 General notes

- As of version 2023, only the new baramundi licensing is supported. If an existing installation has not yet been converted to the new licensing, a valid license is no longer available and must then be added.
- The bMS setup should always be started locally, e.g. directly from the ISO image. An installation via a share can lead to misbehavior.

1.11.3 Notes on the .NET Framework

- The .NET Frameworks are called by different names, or have changed their names. This overview can help with questions:

In baramundi software inventory and in MSW displayed as	In Windows displayed as:
`Asp.Net Core Framework 6.x.x-x64`	`Microsoft ASP.NET Core 6.x.x - Shared Framework`
`NET Core Desktop 6.x-x64`	`Microsoft Windows Desktop Runtime - 6.x.x`

- The required .NET x64 versions `Asp.Net Core Framework 6.x` and `NET Core Desktop 6.x` should correspond to the same version to avoid misbehavior of the baramundi modules.

- If a .NET Framework is uninstalled and then reinstalled, a restart of the entire baramundi server is necessary. Although the bMC module view shows no errors, various malfunctions occur during this action.

1.11.4 baraDIP

- The bMS 2023 R2 does not work with older baraDIP versions. To avoid problems, the baraDIP services should be updated before updating the bMS to a 2023 R2 version.

- If manual changes have been made in the `httpd.conf.dist` file in the baraDIP directory of the DIP server, these will be overwritten by the update to the baraDIP 2023 R2. If these are still required, they must be entered manually again.

- After installing the baraDIP, temporary folders "C:\baramundi soft-ware GmbH" or "AppData\Rooming\baramundi software GmbH" may remain.

1.11.5 Management Center (bMC)

- The help system shows only limited content when used offline.

- In the `criteria` of a `Dynamic Group (Windows)`, the query `Properties.operating system is not empty` or `Properties.operating system is empty` does not work correctly.

- If `Repeated Fast Discovery` or `Repeated Full Discovery` is configured under `Managed Software Data Security`, the time should be chosen so that it does not intersect with the import of the `Managed Software Data Signed`, as well as the subsequent automatic download of new or modified MSW files. Otherwise, hash changes may be displayed unexpectedly, which then have to be confirmed manually.

- In the bMC `Assignments` view, OS Install jobs may be seen twice for a short time.

- When closing the bMC, a program crash may occur in rare cases. However, subsequent errors have not been observed.

- The `List SNMP-Devices` report cannot be opened in environments with an Oracle database.

- When creating an operating system, the new Windows 11 23H2 is not recognized correctly. The version must be entered manually.

1.11.6 Mobile Devices

- Due to a change in behavior in Android 14, an action is required on dedicated devices: the `Manage dedicated device job step` must be performed once with the new version of the baramundi EMM Agent, otherwise the system functions allowed in the job step are disabled.

- Apple's newly introduced " Rapid Security Responses " are available as `Patch Level`, but they cannot be used under `Compliance - Mobile and macOS Devices - Rules`.

1.11.7 Inventory via SSH for Linux devices

- Boot time ist not recorded on Linux distribution OpenSuse.

1.11.8 Inventory

- Note: The old software inventory is no longer supported from version 2022 R2 on. If it is still in use, the bMC will display a note.

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

- Windows 11 is recognized by the software inventory as Windows 10 and can be distinguished on the basis of the version number.

1.11.9 Windows Agent (bMA)

- The User Data Collector (UDC.exe) was removed with bMS version 2023 R2.
- Variable values for variables of type `Password` used in bD-Scripts are only resolved correctly if the bMA can recognize the variables when parsing the script. Contents for variables, where the variable name is only created at runtime of the bDS, are not recognized and also not filled with values.
- Energy options applied via Energy Management profiles may not be displayed correctly under Windows in the System settings - Energy options. A query of the setting on the command line provides the correct values and these are also used by the system.

1.11.10 Kiosk

- To use single sign-on (SSO), Active Directory and group policies may need to be modified. In multi-domain environments, a trust may be required.

1.11.11 UUID (Technical Preview)

- Under `bMC - Configuration - Server - Settings - Basic settings`, `UUID` can now be enabled as `Client-identification` feature. This currently only works with `Microsoft Windows PE Loader` or the `PXE boot menu` for BIOS, the baramundi boot loaders (DHCP options 66/67) are currently not supported.

1.11.12 Automation Studio and bD-Script

- The bDS action `Perform variable substitution in file` only replaces variables of the type password that are also recognizable in the bDS file itself.
- Notes on bDS files from version 2022 R2:
    - 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 2022 R2 or higher.
    - In environments with multiple baramundi servers, please take care that bDS scripts are not converted until all servers/clients are on version 2022 R2 or higher. If conversion to the new format is not yet desired, Automation Studio version 2022 R1 can still be used.

- The bMA from 2022 R2 on will be able to run both the new bDS format and the previous format. A conversion of all bDS scripts is not necessary.

1.11.13 macOS

- As of macOS-14, the baramundi Agent icon is no longer automatically displayed in the menu bar.

1.11.14 Windows Agent (bMA) note on Windows XP

- Development of the bMA for Windows XP has been discontinued.
- It is possible to continue to operate Windows XP with the bMA version 2021 R2. The bMA 2021 R2 is approved for this purpose with the bMS 2022 R1 (and higher).
- The features OS-Install and automatic bMA deployment are no longer available. The bMA may have to be installed manually.
- Note: Since the current bMA can not be used on Windows XP, new security updates for the bMA are also not available.

2 Release 2023 R1

2.1 Windows Vulnerability Catalog 2.0

Because of continuous increases in the number and types of software and system vulnerabilities in recent years, we overhauled the vulnerabilities catalog to improve scanning speed, accuracy and efficiency with extensive changes in scanner rules, techniques and logic.

We began by removing the legacy "Community" scan profile. It was originally intended to let baramundi users add and share scanning rules. It was only sporadically updated so we added the Professional profile in 2016 but kept the Community profile to maintain compatibility.

The catalog used in the Professional profile has grown considerably in recent years along with scanning times, sometimes drastically. A new solution was needed so we created the new "Professional 2.0" profile. It uses a new catalog with optimized rules, modified mechanics and scanning logic to detect vulnerabilities that affect your existing software installations, not merely the existence of individual files, libraries or components cited in CVEs. That significantly improves scan times and accuracy with fewer false positives.

Read our blog posts in English or German for more background:
https://www.baramundi.com/en-us/blog/article/new-vulnerability-catalog-2-0/

2.2 bConnect 2.0

The number of connected systems managed by IT are increasing, along with customer requests for a compliant bMS interface. Our previous bConnect 1.x interface provided a way to implement system calls for many environments. However, in-house developers found that it also required maintenance of the controllers and corresponding documentation. We developed the OpenAPI-based[2] bConnect 2.0 interface to improve overall API performance, flexibility and efficiency.

2.2.1 Handling Data

Due to the change in the underlying technology, the performance of individual calls has accelerated noticeably. This is especially apparent in program sections with many calls.
The amount of data retrieved has been reduced to the essentials so that not all objects have to be loaded. This is better handled by paging results and counteracts earlier timeouts (30 sec.) for larger queries such as the query for <All Endpoints>.

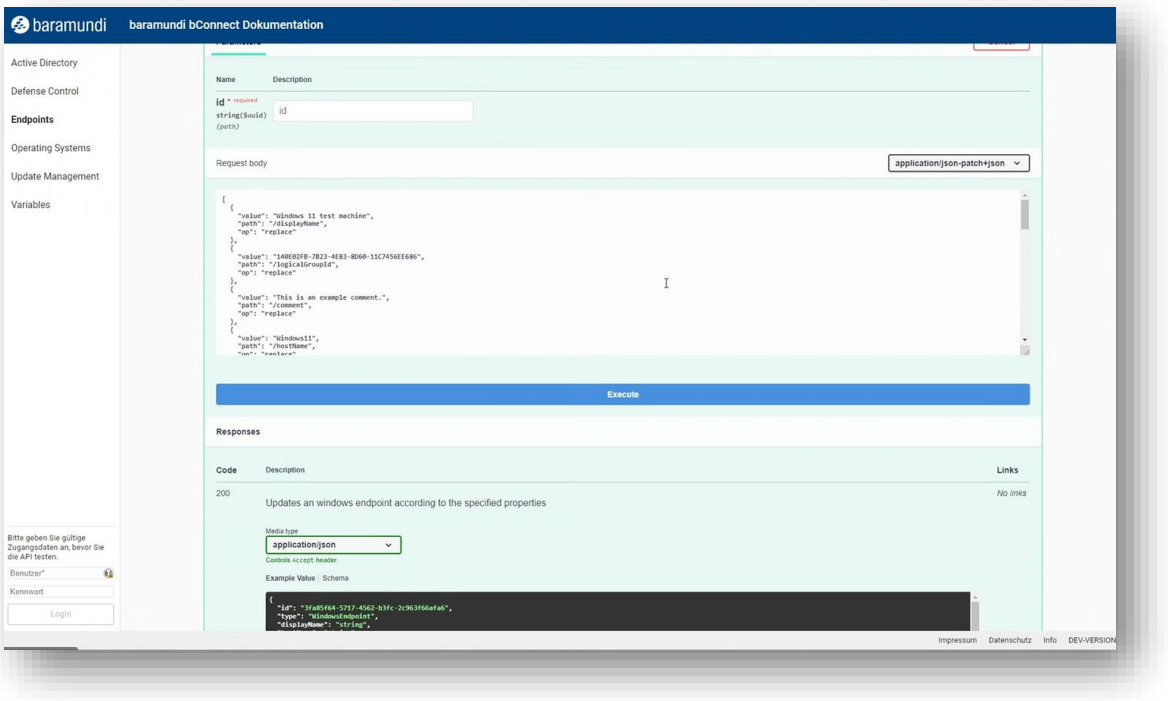


Figure 1 - bConnect 2.0 function details

2.2.2 Structure

The structure of the individual controllers can be viewed directly in the web interface of the API and executed at the push of a button. This means that in addition to a "live" overview of

[2] https://www.openapis.org/

possible functions (without a separate document) and navigation through the menu on the left, it is possible to work directly with parameters and sample calls in each individual function.

This leads to a better overview of the API and helps avoid incorrect calls or wrong parameters.

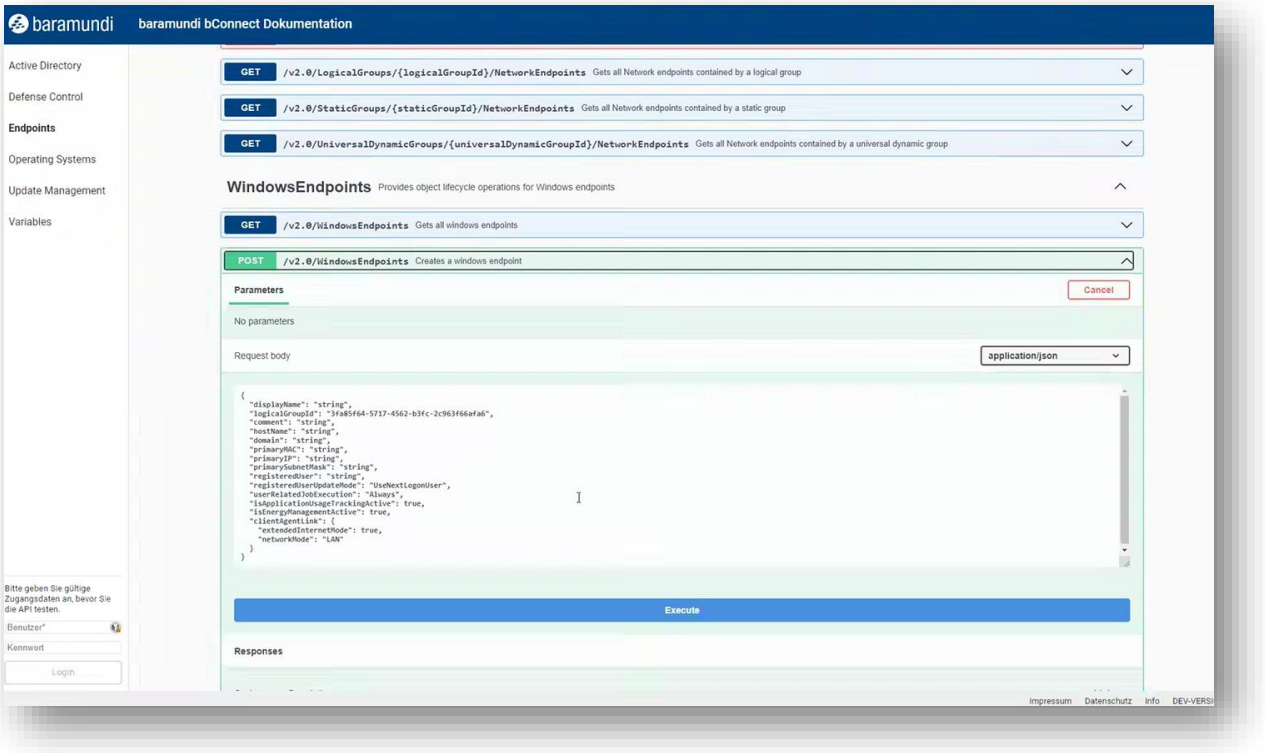


Figure 2 - bConnect 2.0 Controller - List of functions

2.2.3 Further Development

The initial feature set of bConnect 2.0 includes the following controllers:

Controller	Description
Active Directory	Active Directory objects such as users, groups or organizational units.
Endpoints	The primary objects of the baramundi environment such as Windows, Android, iOS, Mac, industrial and network endpoints.
Operating Systems	Manages OS installation information and configuration for Windows endpoints.
Update Management	Manages update management information and configuration for Windows endpoints.
Variables	Variables are an essential component of the baramundi Management Suite. The controller enables cross-object access to the variable definition as well as the actual variable values.

bConnect 1.x is still available in the transition phase so you can combine the functions of both interfaces. The controllers mentioned above have already been implemented in bConnect 2.0. bConnect 2.0 also offers the following functions:

- Disable endpoints, disable clients
- AD users and groups readable
- Variable access to AD objects

The conversion of the API to OpenAPI also enables a consistent and easier implementation of future features and extensions.

2.3 baramundi Ticketing System [Preview]

The redesigned baramundi Ticketing System is expected to be released in the summer of 2023 with a number of new functions and changes.

The technology and design of the user client will be completely revised with greater flexibility, improved interfaces and the ability to incorporate enhancements in future releases to improve end-user experiences.

Application accessibility also will be a focus of future releases that will add functions and make all common forms, functions and client components fully screen reader and keyboard accessible.

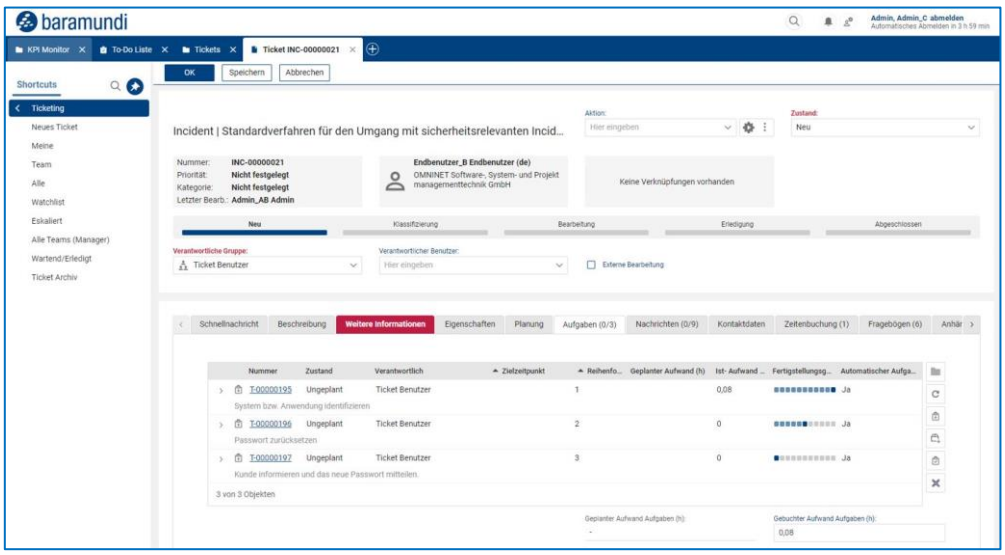


Figure 3 - bTS new design

2.3.1 New Design

The entire client GUI will be revised, retaining essential existing functions while optimizing the arrangement and appearance of many controls and fields.

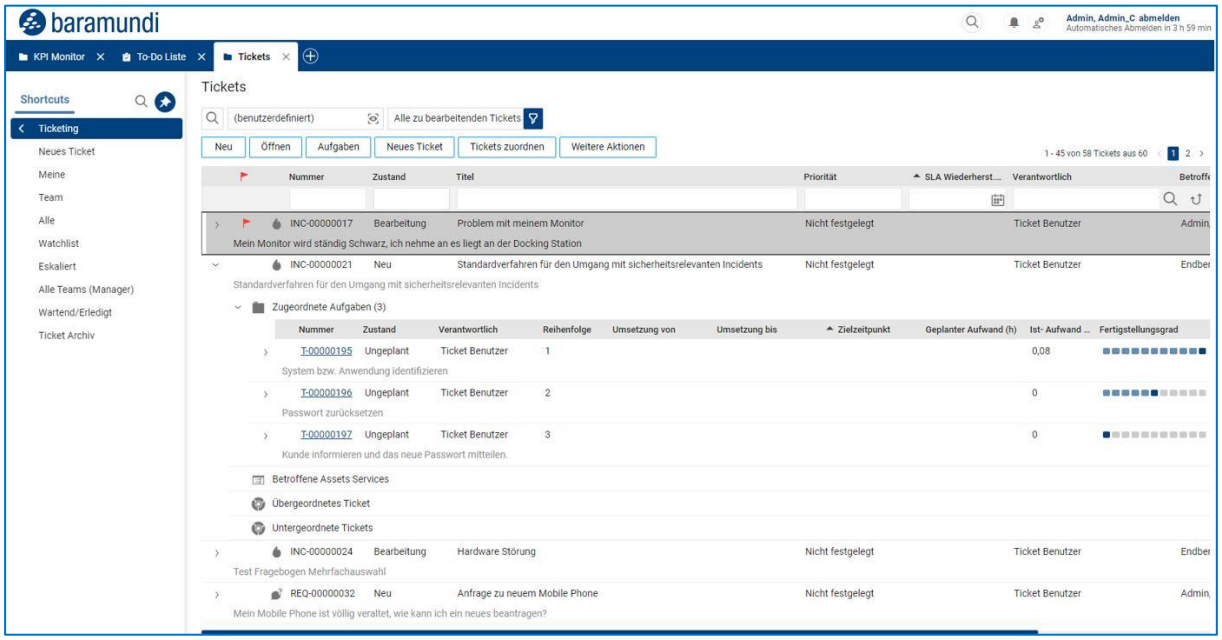


Figure 4 - bTS – Ticket list

2.3.2 Form Re-Design

The design and structure of the forms for tickets, assets, tasks and knowledge base will be revised. The previously stacked form sections will be shown in tabs, and the arrangement and sequence of fields and lists will be revised and reorganized. The resulting appearance will make forms easier and more efficient to use with important contents available at a glance and longer lists displayed in full.

2.3.3 Improved Performance

The performance of the entire system is significantly improved with many actions up to 90% faster.

2.3.4 New Session Handling

When logging in, each user will be able to decide whether to continue using an open session or to terminate it and initiate a new one. That eliminates waiting to log in if previous sessions were not terminated properly.

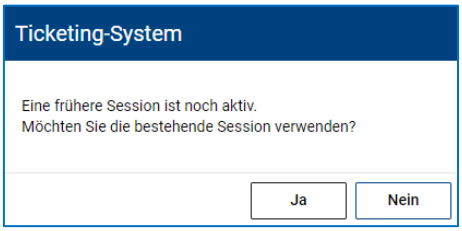


Figure 5 - bTS – Session login option

2.3.5 Responsive Design for Mobile Use

The entire client will have a fully responsive design to enable use of all interfaces, forms and functions on any screen size (smaller tablets and smartphone screens). The system automatically detects screen size and adapts the display for intuitive mobile use.

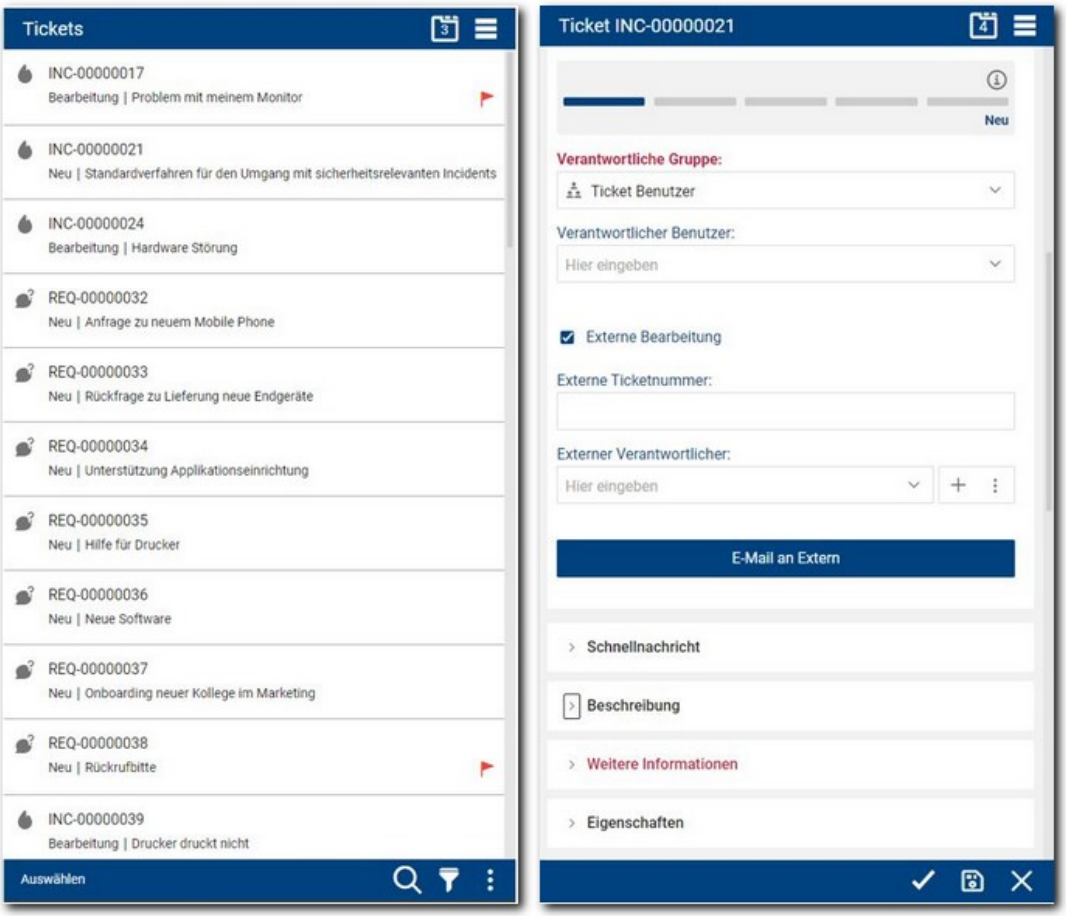


Figure 6 - bTS - mobile display

2.3.6 AD Sync through the bMS Interface

With the new bConnect 2.0 interface, Active Directory information on persons, users and other variables can also be updated directly from the bMS in the ticketing system via automatic and time-controlled import. This means that information from the AD no longer has to be imported separately into the ticketing system. Additional information from other data sources can still be imported and supplemented via CSV.

2.4 baramundi Argus Cockpit and Argus Experience [Preview]

New features in Argus Cockpit and Argus Experience[3] give IT departments more options for endpoint monitoring and for identifying the causes of software hangs and crashes for faster and more accurate resolution.

2.4.1 More UDGs In Argus Cockpit

Previously, the baramundi Argus Cockpit supported up to 10 UDGs per environment that could be synchronized with the baramundi Management Server. Since we added the ability to "tag" these UDGs in the bMS 2022 R2, usage has increased significantly. To meet this growing demand, more UDGs per environment can be assigned to various users. For example, instead of just enabling IT admins to monitor UDGs based on their areas of responsibility, IT departments can define UDGs appropriate for Chief Information Security Officers (CISOs), location managers and other authorized users.

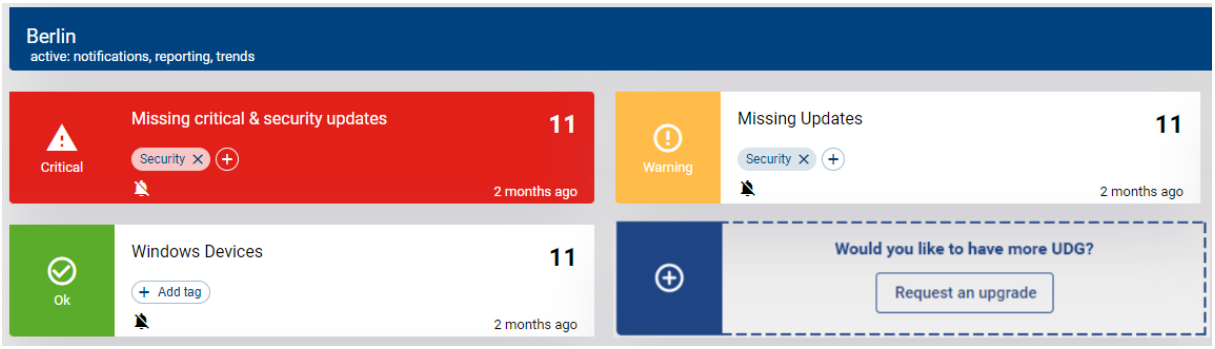


Figure 7 – Requesting more UDGs in Argus Cockpit

2.4.2 Analyzing Problematic Software in Argus Experience

baramundi Argus Experience (bEX) now adds views for analyzing the causes and frequency of endpoint software hangs and crashes. It enables you to detects trends or patterns for specific applications, versions or groups of computers.

[3] Market launch for the baramundi Argus Experience is expected to be summer 2023.

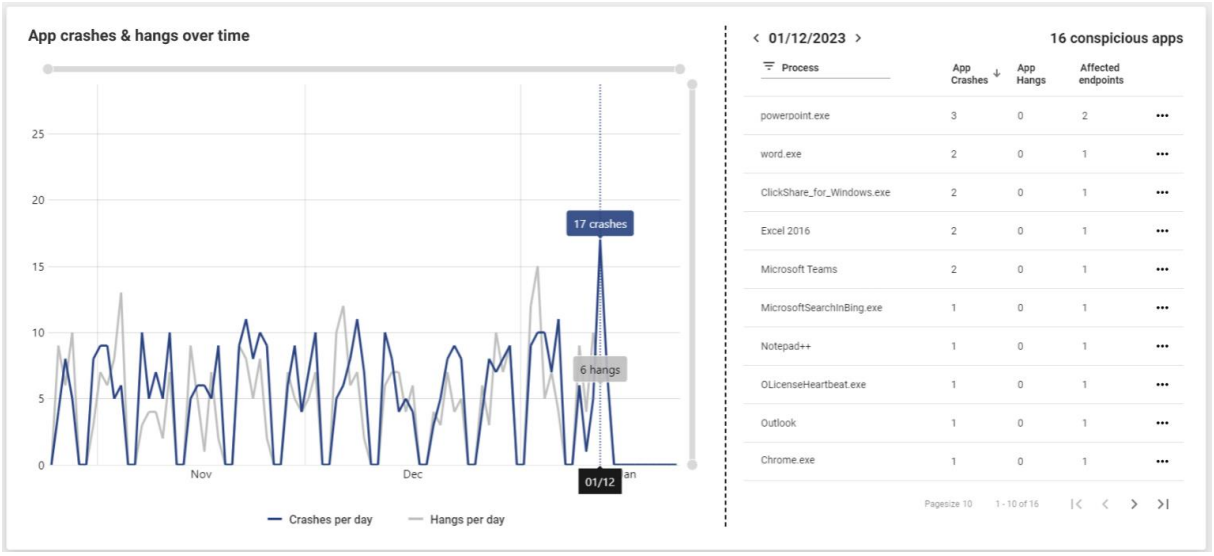


Figure 8 - bEX-Preview: Crashes and freezes per application

Detailed views per application allow IT admins to recognize whether there is a particular software version that crashes or freezes more frequently. This information can be used, for example, to update the problematic version on a specific endpoint or all affected endpoints using baramundi Managed Software.

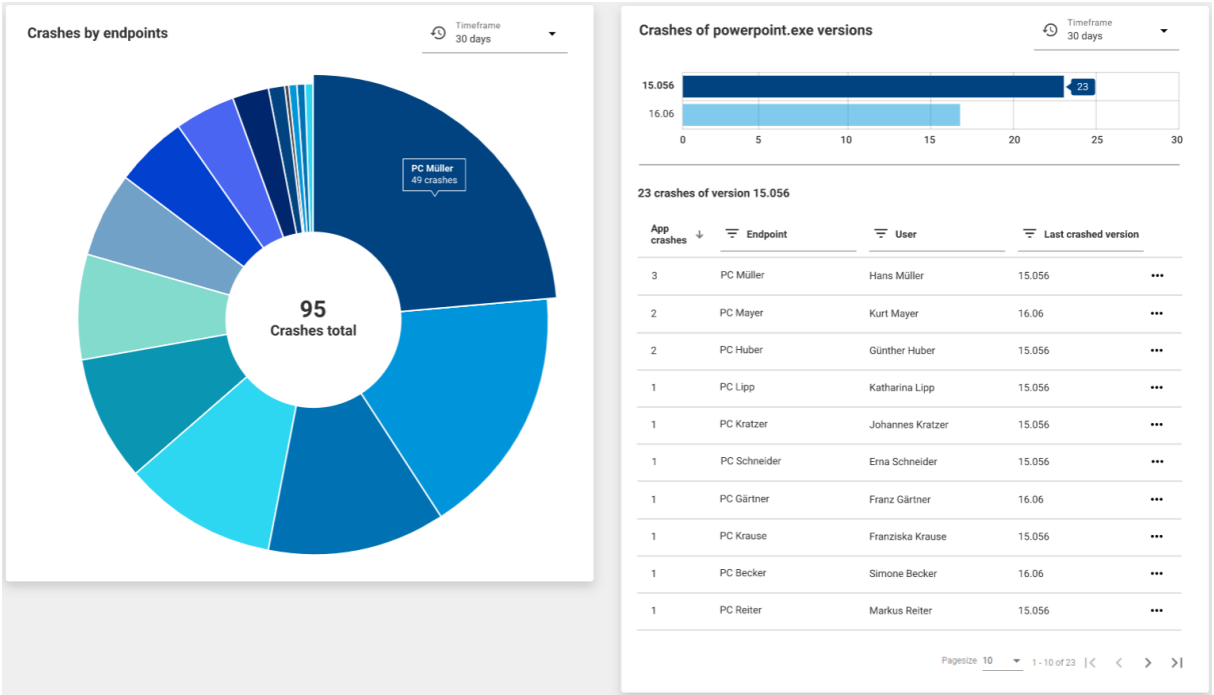


Figure 9 - bEX-Preview: Software crashes per endpoint and software version

Once an update for software identified as "frequently crashing" the results can be viewed with the following display.

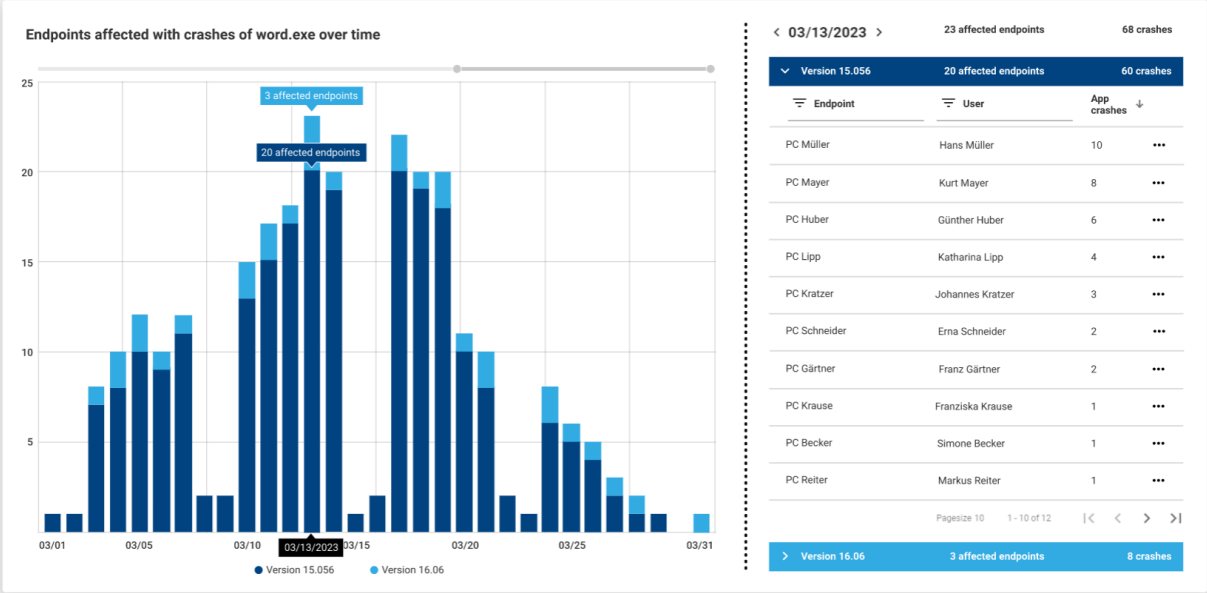


Figure 10 - bEX-Preview: Number of endpoints with problematic software versions

Example: Starting March 19, an IT admin began rolling out updated version 16.06 of a problematic application throughout the company. The diagram shows that the total number of crashes for that application started to decrease on March 20. There were no crashes from March 30 onward indicating that all end-users have the more stable and secure version.

2.4.3 Benchmarking System Stability

It can be a challenge to determine whether data collected from end devices is normal or indicates a problem. Whether 20 crashes caused by 2 applications on 5 devices in one department over two weeks, or 50 crashes caused by 10 applications on 20 devices at a large branch office in a month indicate a need for action is often based on experience and "gut feeling." The bEX "Environment Stability Score" can help.

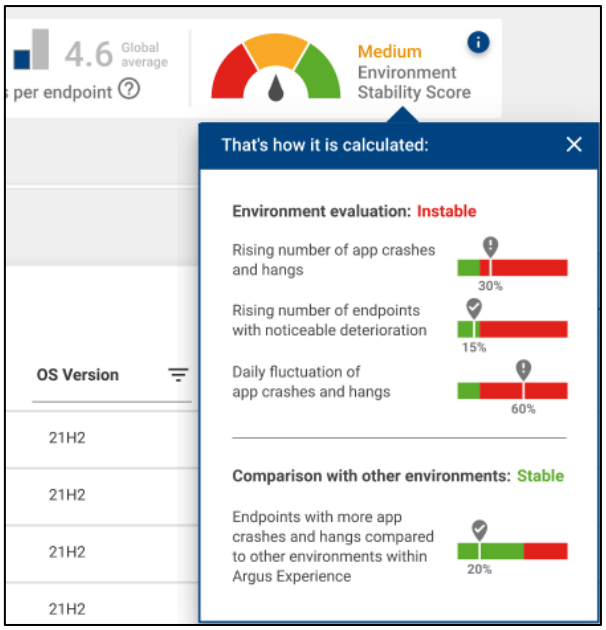


Figure 11 – bEX preview: Scoring of overall stability

It indicates how stable your IT environment is compared to other IT environments, and explains how the number of software crashes/hangs affects scoring.

2.4.4 Rapid Error Analysis

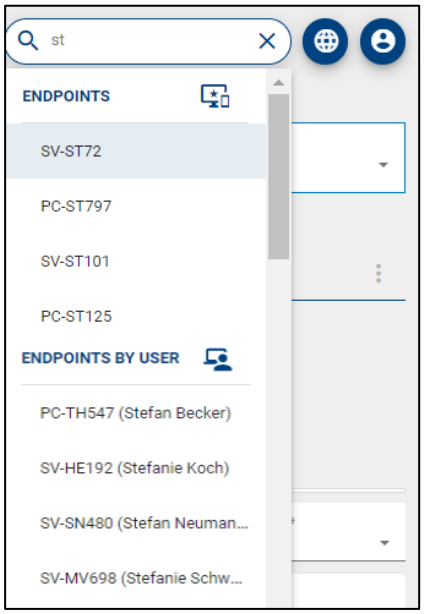


Figure 12 – Search for IT assets

End-user support tickets need to be resolved quickly and efficiently. bEX makes it easy to quickly identify:

- the end device in question
- the problematic software
- the (frustrated) end user

A new search function in bEX enables IT teams to find what they're looking for, dive into error analysis, and implement a fix quickly and efficiently.

2.5 Universal Dynamic Groups

2.5.1 Platform Icons

UDGs offer numerous deployment scenarios based on a wide variety of conditions across endpoint types. To make it quicker and easier to select conditions and endpoints when defining UDGs, we have added corresponding platform symbols to the list to provide an intuitive visual cue.

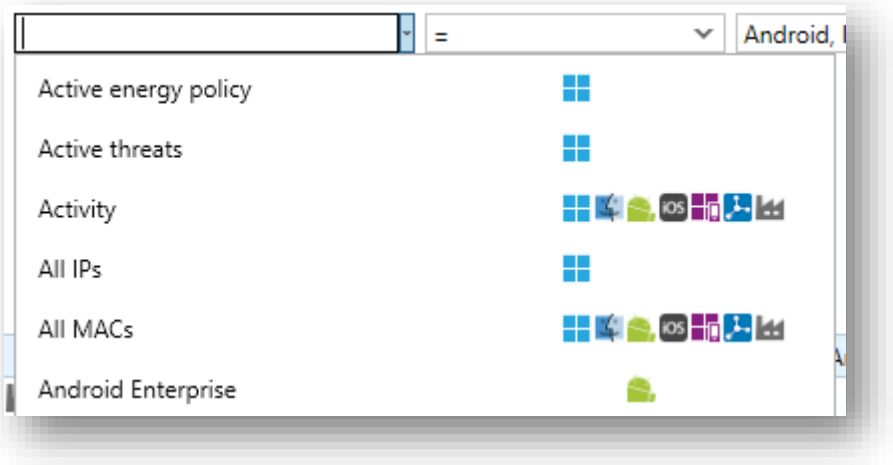


Figure 13 - UDG conditions – Icons

2.5.2 User Text Filter

It is now possible to filter endpoint properties with free text keywords when creating/editing a UDG. It will display endpoints with properties matching the search term. If there are multiple words in the search text it will display entries that contain all of the words, e.g. a search for "antivirus status" will show entries that contain both "antivirus" and "status".

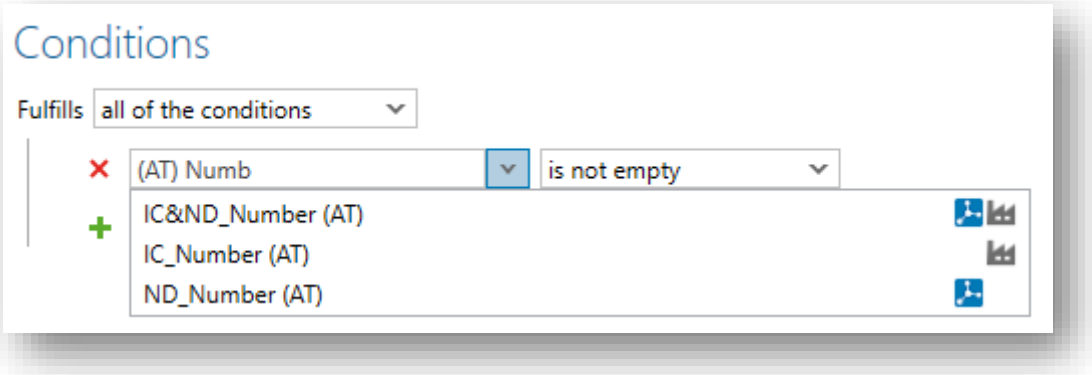


Figure 14 - UDG conditions – Text Filter

2.6 Product improvements in detail

2.6.1 Fixing the known problems of the bMS 2022 R2

- The 2022 R2 issues documented in the forum have been addressed in the 2023 R1.
- The `bMS2022R2-U1` bug fix is included in the 2023 R1 release.
- Bugfix: The bMC view `Inventory - Software - Windows Devices` shows unexpectedly many software.
- Bugfix: For assigning jobs the Modify right on the client is sometimes required.
- Bugfix: If folders are deleted under `bMC - Environment - Dynamic Groups`, which contain `Dynamic Groups (Universal)` with a configured automatic job assignment, constantly recurring database errors occur in the bServer.log.
- Bugfix: bD script for user settings is not executed under certain circumstances because of "Access denied (code = 5)". Note: The bMA as of 2023 R1 now accesses the user settings bDS file in the context of the logged-in user again.

2.6.2 Windows Agent (bMA)

- The `Distribute Microsoft Patches (Classic)` job step now uses the 64 bit Windows API to determine the patch status of x64 systems.
- The bMA now uses the native expand.exe to extract .cab files.
- The overview page of Windows endpoints now lists eMMC disks under `Disk Information`.
- Bugfix: Energy consumption data for clients `in standby` is not determined and always reported as 0, and displayed as 0.00 kWh in the bMC on the endpoint.
- Bugfix: The hardware inventory leads to a BlueScreen on the end device on newer systems.
  Note: Unfortunately, it cannot currently be ruled out that bluescreens will continue to occur on systems with new hardware.

2.6.3 Management Center (bMC)

- The detailed display of `Client - Compliance - Vulnerabilities – Detected` has been optimized for the new `Vulnerability Scan: Windows (Profes-sional 2.0)`. In particular, the Analyzed items are now more verbose and show only the relevant locations.
- The configuration for columns in Universal Dynamic Groups (UDG) can be saved as default.
- On the Windows end device, the properties `Delay of function updates` and `Function update version` are visible again under `Overview - Microsoft Update`.
- The selection dialog of the `Dynamic Group (Universal)` properties has been improved and extended by endpoint type icons.
- With the command line parameter `/username=n` it is possible to pass a user name to the bMC login dialog.
- The `Logical Group - Content - Extras - Shutdown/Restart` action now no longer requires individual confirmation if multiple clients have been selected.
- Bugfix: In the `Software - Managed Software – Settings` dialog, changes made are not applied if they were made via keyboard operation.
- Bugfix: The display of Crystal Reports is not possible if a port for the database is additionally specified in the database manager.
- Bugfix: To assign a job to an end device, modify rights are required in addition to job assignment rights. (Behavior of the 2023 R1 corresponds again to the behavior of the 2022 R1)
- Bugfix: The display of the password input field at `Configuration – Domain` is partly not consistent.
- Bugfix: Under `Inventory - Network Scan – Profiles` invalid network profiles with smaller end address than start address can be specified in the `SNMP IP range`.
- Bugfix: Under `Inventory - Asset Types` an invalid icon file can be selected for an `asset type`.

- Bugfix: When creating an asset on the client, the bMC sometimes crashes, e.g. if there are many asset types.
- Bugfix: The action `Organize - Export All to Excel` shows an error like "*The maximum number of Cell styles was exceeded*.", especially if the view to be exported contains many entries and many columns.
- Bugfix: Opening a Windows device in a tab may take a long time, especially if there are groups with many clients.
- Bugfix: `Configuration - Management Center` is displayed on the PXE relay, but the settings made there are not saved.
- Bugfix: The bMC is closed unexpectedly when clicking on the open arrow under `Jobs - Job - Settings - Overview` during a `hardware inventory` step.
- Bugfix: Some elements were displayed in the `Theme - Dark` with unreadable colors.
- Bugfix: The display `Environment - Client - Inventory - Software` is sometimes very slow and scrolling in the software list is then not possible.
- Bugfix: In the bMC in the detail view of a job target, the step number of a step is sometimes displayed incorrectly if the job target is currently being executed.

2.6.4 bMUM Windows Update Management

- Bugfix: If a job with a `manage Microsoft Update` step is changed from `manual configuration` to `update profile`, the previously existing configurations (e.g. patch filter) are still used in some cases.

2.6.5 Mobile Devices

- The " Rapid Security Responses" newly introduced by Apple are displayed in the bMC on the end device under `Overview - Patch Level`, as well as in `Device Inventory`. The `Patch Level` column can be displayed in the grid view and can be used in Universal Dynamic Groups.
- The Android Enterprise Root Check was switched to google Play Integrity API. For this purpose, the bServer communicates with the baramundi online service baramundi Root Check Service via https/443.

- It is now possible for the administrator to specify which services should be active for synchronization when distributing an Exchange account for iOS devices. It is also possible to specify whether the individual settings can be changed by the end user on the device.
- In WLAN profiles for Android Enterprise devices, random generation of the MAC address can be disabled, analogous to iOS.
- In the bMC, a `default Play Store app availability` can now be set under `Configuration - Mobile Devices - Android Enterprise`.
- Bugfix: If very long texts are entered in the free text fields of a profile in the bMC under `Configuration - Automatic Registration - Apple Automated Device Enrollment / DEP`, exceptions occur.
- Bugfix: Assignment of VPP licenses via `bMC - Apps - Licenses linked` fails if many users are specified.
- Bugfix: The view `bMC - Logical Groups - Inventory - Software (bMD)` is sometimes very delayed, especially if the bMC user does not have the right to view all end devices.
- Bugfix: If mobile variables are used in a `Dynamic Group (Universal)`, this UDG may no longer deliver the expected end devices after updating to a baramundi version 2022 R1 or 2022 R2.

2.6.6 bServer

- It is possible in the baramundi database manager to configure the communication mode with the MS-SQL server, e.g. TLS with certificate validation.
- Unpacking and processing of large client messages, e.g. inventory and compliance data, has been improved and now requires less memory.
- Bugfix: Creating a new baramundi database is not possible for time zones with UTF+5 and shows an error "External component has thrown an exception".
- Bugfix: The Modern Management microservice does not start if a TLS connection to the database is configured.

2.6.7 bConnect

- bConnect v2 is now part of the product.
  bConnect v1.1 can still be used.
- Bugfix: The VLSM option cannot be configured correctly for IP networks.

2.6.8 Network devices

- In the bMC, the `Network Device - SNMP - Serial Number` field can now also be filled manually.
- For a Network Scan Profile, the `Identify devices by their IP address` setting is now default.

2.6.9 macOS

- Bugfix: The "Restore device" dialog is displayed on the device although it is configured as suppressed in the enrollment profile.
- Bugfix: Enrollment via SSH without push certificate does not work if an enrollment with push certificate was performed before.

2.6.10 baraDIP

- The Apache included in baraDIP has been converted to 64-bit architecture. It can therefore only be installed and operated on 64-bit operating systems.
- Note: With the upcoming release 2023 R2, only secure communication via https will be supported for baraDIP.
- Entries under `DIP Administration - DIP Server - Synchronization - Includes` now also support entries with wildcard `xxx*`.

2.6.11 bMOL

- bMOL automatically binds to the server certificate on first contact. Any existing bMOL scripts must be checked.
- Please note that bMOL is an obsolete interface. A switch to bConnect is recommended.

3 Release 2022 R2

3.1 baramundi Argus Experience – Improving end-user experiences

A lot has changed in IT in recent years. Not only is technology constantly evolving, but working environments have changed significantly as well. The challenge of enabling and supporting mobile and home office work for employees is enormous. If IT infrastructure doesn't work as employees need and expect, frustration rises and overall end-user experiences suffer. This often results in a flood of support tickets that IT admins must add to existing workloads. The best way to avoid such situations, of course, is to improve and reliably maintain end-user satisfaction.

With baramundi Argus Experience (bEX), IT admins achieve just that by proactively providing better endpoint stability and performance. IT admins benefit from the intelligent collection, visualization and evaluation of end-user experience data to help troubleshoot and correct problems. This reduces the number of support requests and leaves more time for higher-priority and strategic IT projects.

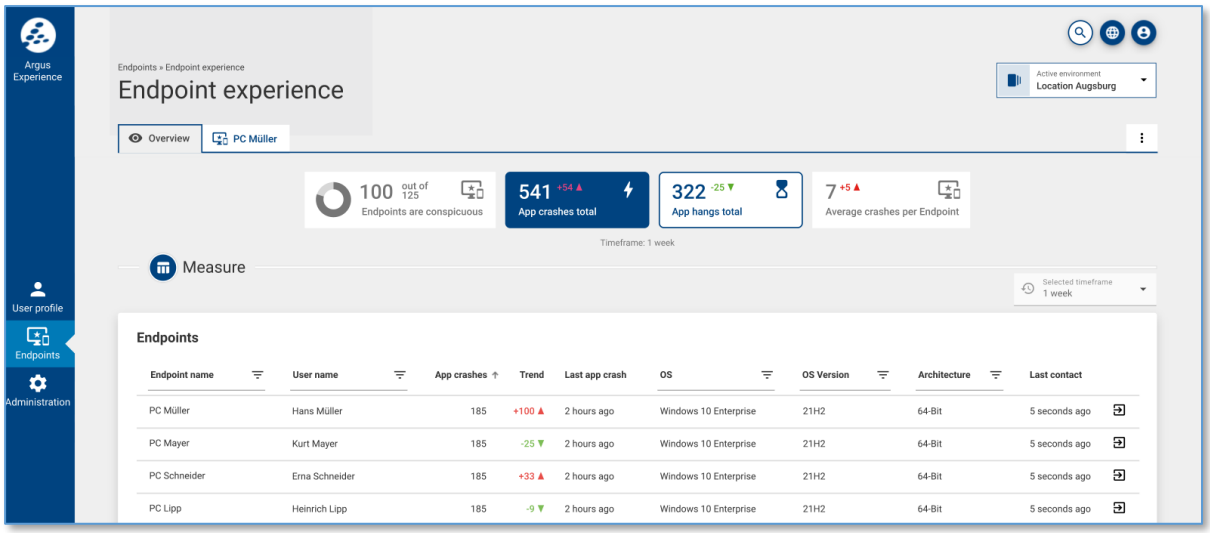


Figure 15 - bEX Preview - IT environment with conspicuous endpoints

3.1.1 Registering software crashes and freezes

One of the first bEX use cases is the reduction of frustrating endpoint software crashes. Employees often report application crashes or freezes without being able to identify possible causes. They'll then submit support tickets that are virtually impossible to resolve and close without extensive troubleshooting.

Argus Experience records and clearly displays the details of software crashes and hangs, giving IT admins the information needed to identify, solve or prevent problems sometimes even before a support ticket is submitted. Up to 3 months of software incident data can be analyzed to spot patterns and assigned to support tickets.

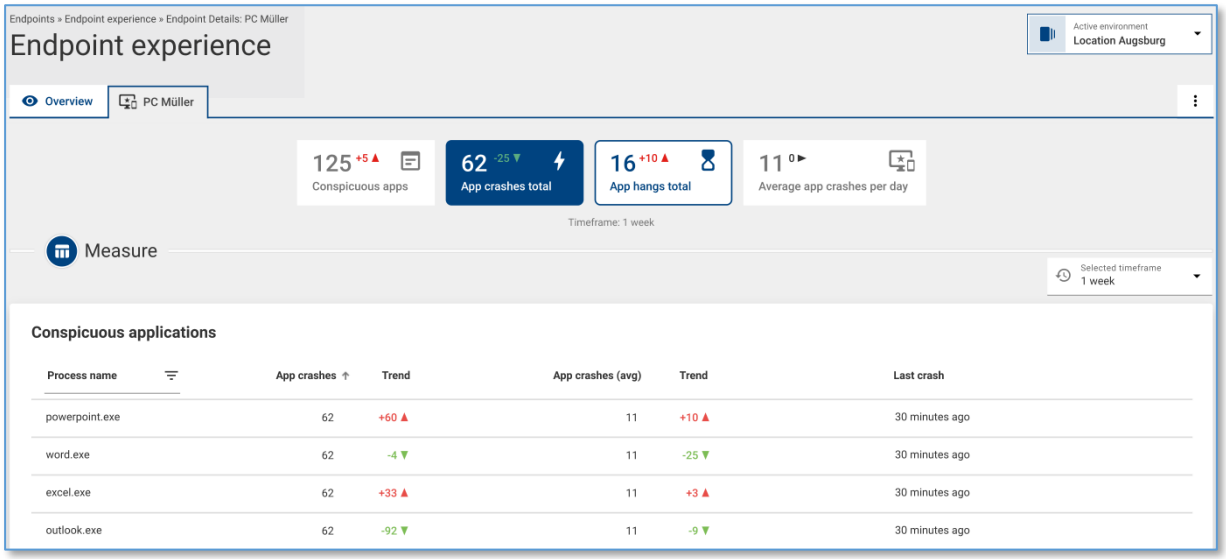


Figure 16 - bEX (UI Prototype) – Endpoint with conspicuous software

3.1.2 Analyzing trouble-prone software

Knowing which software is particularly troublesome is helpful in itself. But more information is needed to isolate causes and implement effective solutions.

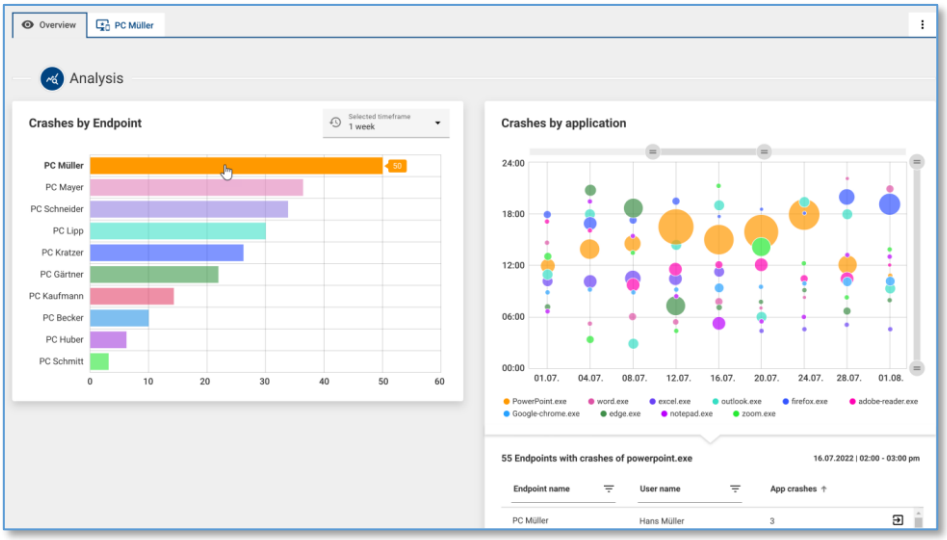


Figure 17 - bEX (UI Prototype) – Problematic endpoints and applications

Dashboards for time-based analysis show periods in which one or more software crashes occur more frequently. This would reveal, for example, if a software rollout is the likely cause, or if known periods of high network loads are a factor.

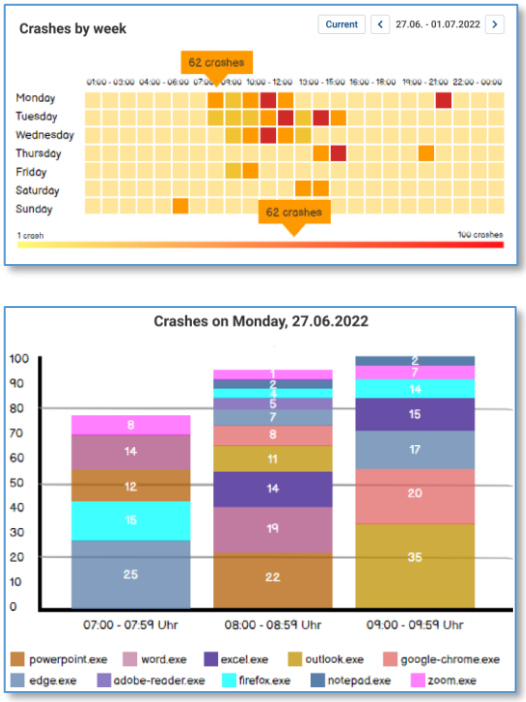


Figure 18 - bEX (UI Prototype) – time-based analysis

These views can be used to identify more problematic end devices, applications or time periods and inform additional analysis leading to an effective resolution.

Identifying differences in the stability of software versions

Particular versions of some software packages can be the cause of application issues. For example, changes in the app's UI can frustrate end-users, or technical issues -- "bugs" – can cause crashes or hangs.

IT admins may roll out security-related software updates to the entire company. However, that may obscure the cause of both existing and newly introduced problems that only come to light some time after the support tickets start coming in.

With the help of Argus Experience, IT admins now can effectively plan for and possibly avoid potential issues and maintain end-user satisfaction during software deployments by assigning and viewing the stability of specific software versions during different time periods.

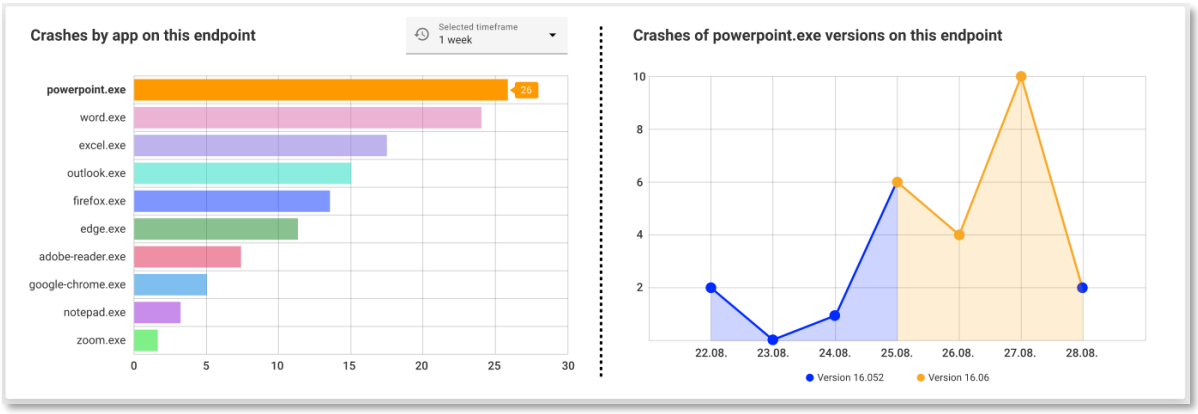


Figure 19 - bEX (UI Prototype) - Crashes of different software versions

3.1.3 Technical framework for bEX

baramundi Argus Experience builds on the established Microsoft Azure cloud-based architecture of baramundi Argus Cockpit. The shared technology platform for Argus makes it possible for us to continuously enhance existing capabilities and add new modules for different use cases while ensuring overall security, performance and reliability. The architecture also gives IT admins the flexibility to select and use individual Argus modules independently based on their specific needs and goals.

3.2 baramundi Argus Cockpit – Environment & User Management

With the baramundi Argus Cockpit (bAC), it is possible to monitor their IT environments from anywhere and at any time so they can quickly assess and respond to performance issues. A key advantage of the bAC is that multiple IT environments can be watched simultaneously. For example, an IT admin with "Argus eyes" can monitor several company locations at once. Managed Service Providers (MSP) also can monitor and manage several different customer environments using a single consistent interface.
With bMS 2022 R2, it is easy to configure Argus Cockpit to onboard additional IT users and assign specific management responsibilities for a variety of different environments.

3.2.1 All environments at a glance

As a "Company Administrator," IT admins now can clearly display all connected bMS environments in the new administration area of the baramundi Argus Cockpit and specify location name and other details.

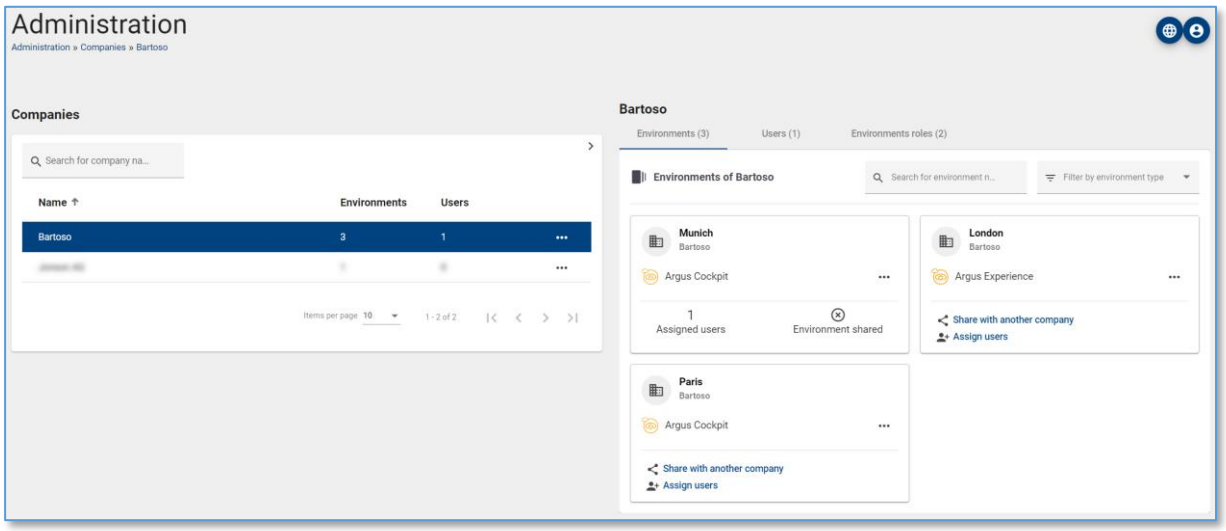


Figure 20 – bAC - Overview of all IT environments

As described above in section 3.1.3, the Argus modules run on the same Azure-based platform so IT admins can also manage their relevant environments (and associated users & roles) using either Argus Cockpit or Argus Experience, or both[4].

3.2.2 Invite and authorize users

Often, a team of IT admins looks after one or more environments. To assign specific team member assignments, "Company Administrators" can create and add Argus Cockpit users. Each IT admin using bAC also can be given specific access privileges that corresponding to their assigned areas of responsibility.

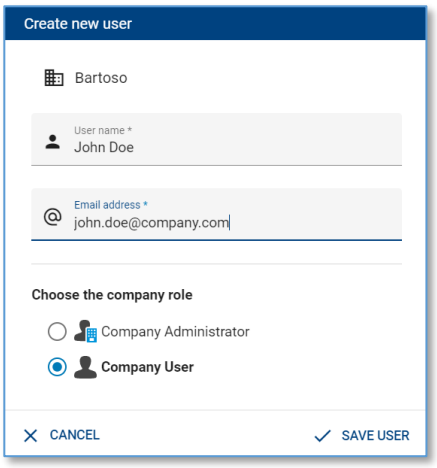


Figure 21 – bAC – Register new users

For example, a Company Administrator can now assign one or more bAC environments to individual IT admins at different locations, as well as customize user details.

[4] Provided that the company is registered for both modules.

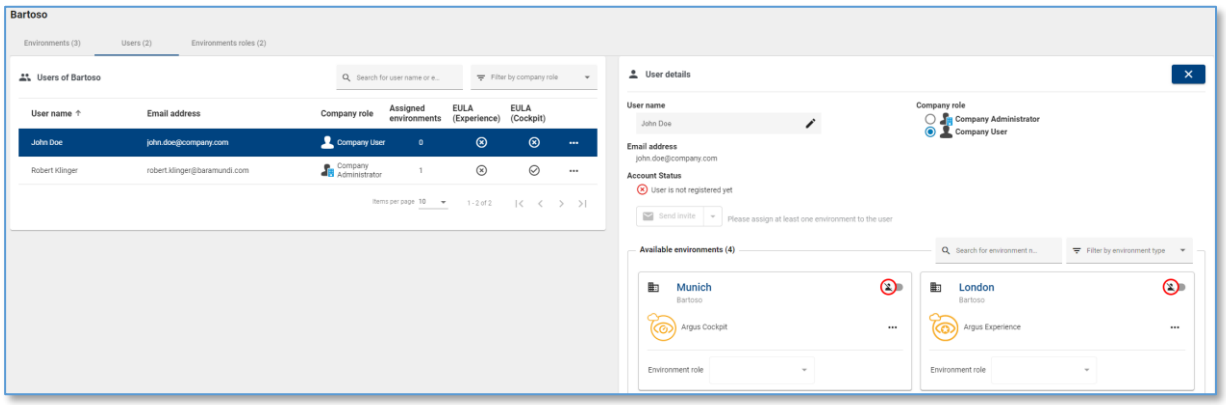


Figure 22 – bAC - Assignment of users to environments

3.2.3 Enabling customer environments for Managed Service Providers

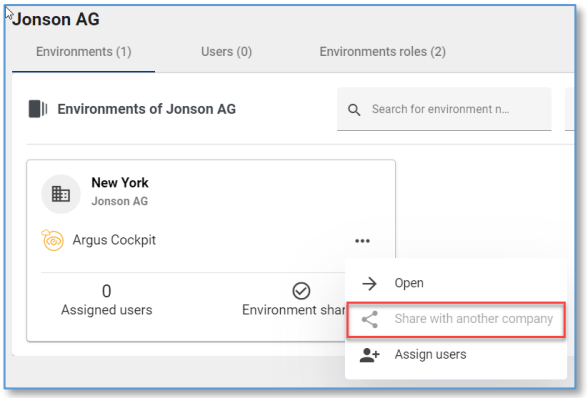


Figure 23 - bAC - Share IT management with an MSP

At companies where all or parts of its IT infrastructure are handled by a MSP instead of or in addition to internal staff, there is now an option to share management with designated MSP staff. The MSP can keep an eye on the customer's IT environment at all times with the help of the baramundi Argus Cockpit.

3.2.4 Assigning dedicated roles and permissions

After environments and users have been set up and assigned, Company Administrators must now ensure that that each IT admin can access only the specific bAC functions they need to fulfill their responsibilities. The new release makes it possible to define and assign environment roles and users.

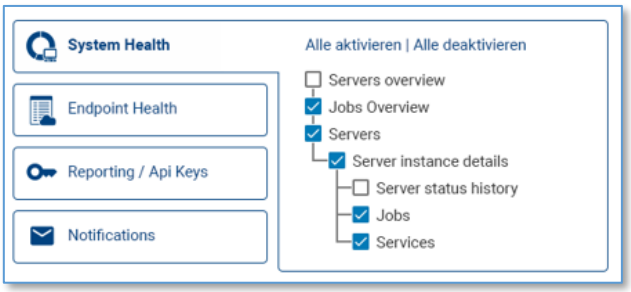


Figure 24 - bAC - Configuring environment roles

The following environment roles are distinguished:

- *Environment admin: default role with administrative permissions.*
- *Reader: Environment role with read-only permissions.*
- *Self-defined: Specific roles that can be authorized individually*

For example, Company Administrators can use these predefined or self-defined roles to give a CISO restricted access to bAC reporting, or to give IT admins read-only access to UDG legacy sets without the avility to change configurations.
Each assigned role complies with GDPR data protection requirements.

3.2.5 Intelligent control of object access

In some companies it is necessary to block or release certain functionalities or make content visible to IT admins according to their assigned roles. The bMS and baramundi Argus Cockpit enable that using Universal Dynamic Groups (UDG). For example, MSPs using the bMS to manage several customers can assign and authorize individual UDGs for specific customers or clients.

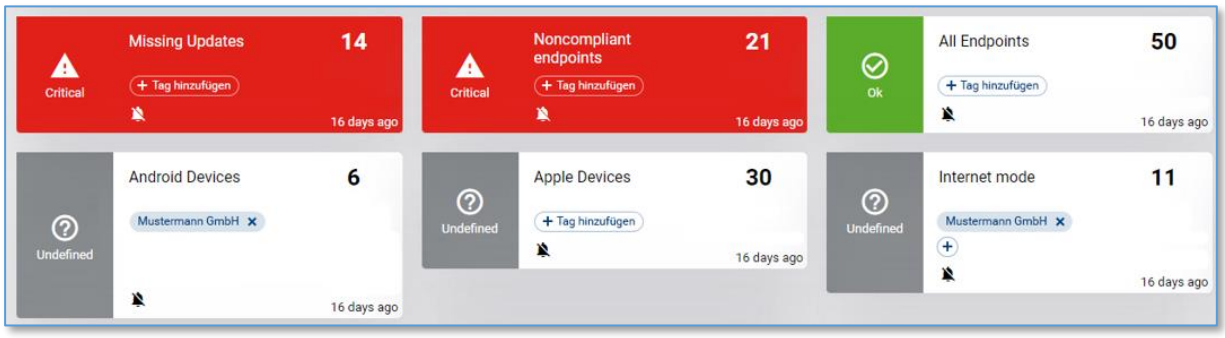


Figure 25 - bAC - Assign tags for access control

IT admins can now also set "tags" for this use case. For each UDG in Argus Cockpit, the IT admin can store one or more "tags" to control access flexibly and securely.

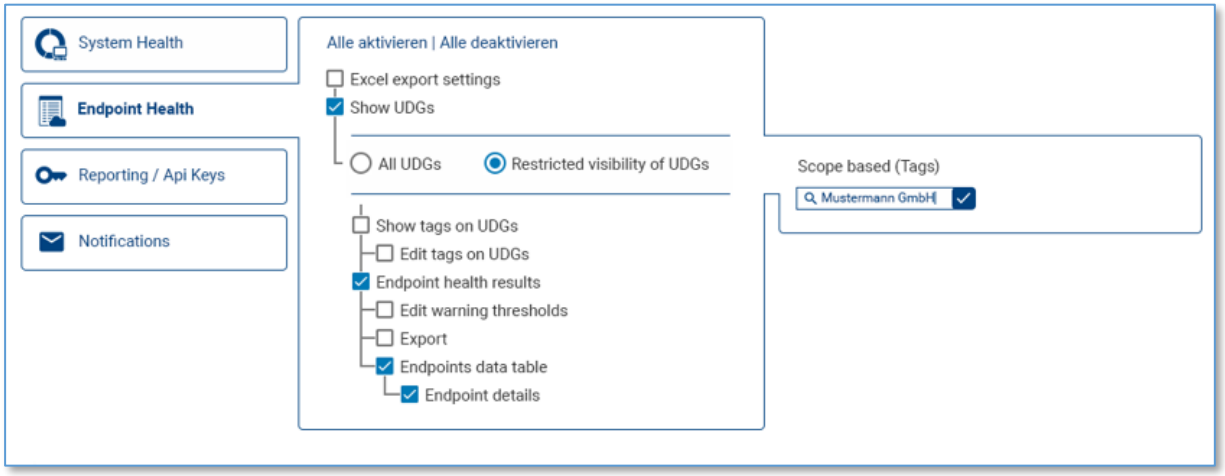


Figure 26 - bAC - Assign environment roles for defined tags

3.3 Automatic job assignments for UDGs

3.3.1 Assignments across all endpoint types

The functional scope of UDGs and task automation is further extended so you can select the desired endpoint devices with a high degree of flexibility.

The "universal" in UDG describes the goal of performing tasks across diverse endpoints in a single job. The new release makes it is possible to define automatic job assignments via UDGs not only for Windows but also for iOS, macOS, Android and IC devices.

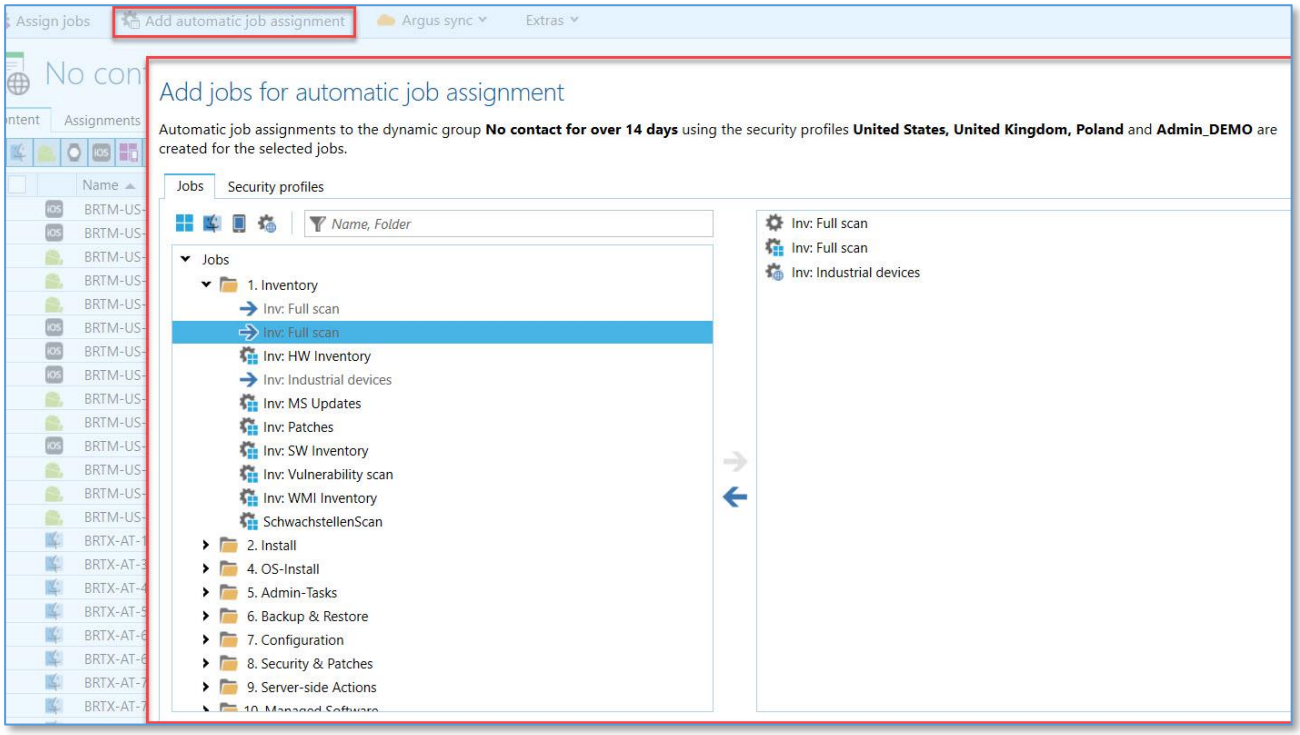


Figure 27 - Automatic job assignment of a UDG

3.3.2 Control via security profiles

This new assignment type also proves the given rights of the individual users. So the automatic assignments by UDGs offers the advantage that, based on the security profile(s) of the bMC user, only endpoints on which the user also has the corresponding rights are affected by this assignment.

3.3.3 MDM assignment more flexible

With this new feature it is now possible to work more flexibly with automatic job assignments even for endpoint types outside of Windows even in larger environments or more complex constellations. The job assignments for new MDM devices, for example, can now also be restricted granularly with conditions by using the UDGs instead of acting globally on all new MDM devices (iOS, Android).

3.4 baramundi Automation Studio

3.4.1 Search in the script

In Automation Studio in the bMS 2022 R2, the new search function enables you to locate text strings quickly using a free text field. The search function also lets you search for text strings in sub scripts called by the main script.

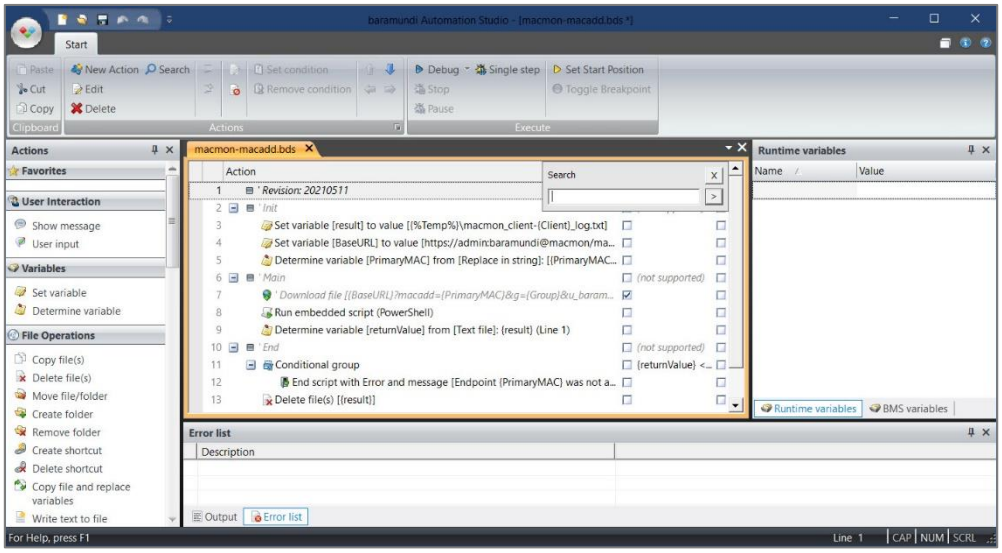


Figure 28 - Automation Studio – Search in Script

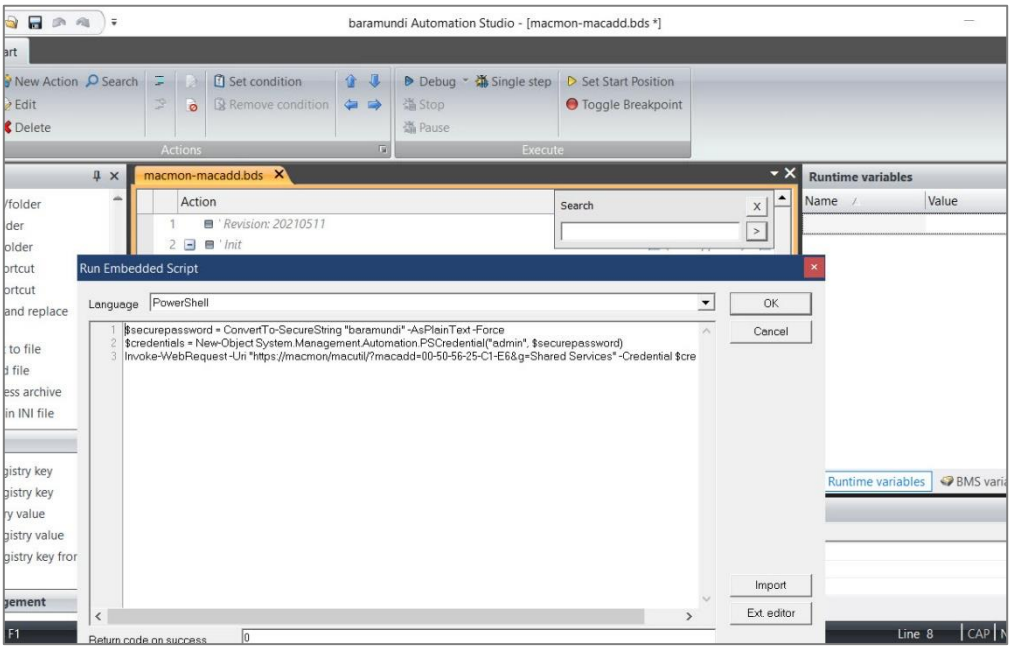


Figure 29 - Search in called subscripts

3.4.2 Compatibility with PowerShell Core

PowerShell is one of the most popular scripting languages for Windows administration. With PowerShell Core, Microsoft offers a more modern and cross-platform variant. This is supported in the bMS 2022 R2 and can be selected in Automation Studio.

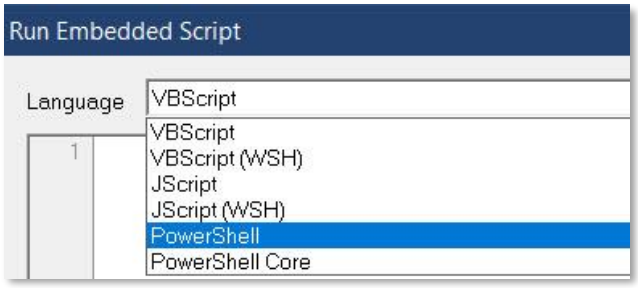


Figure 30 - Automation Studio Embedded Script - PowerShell

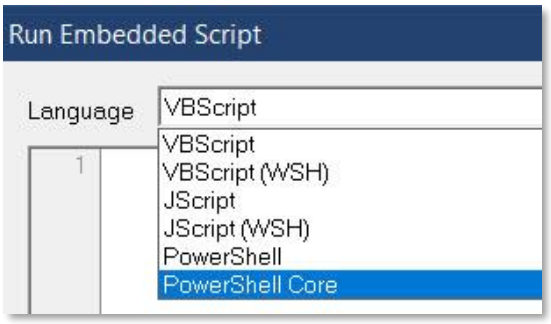


Figure 31 - Automation Studio Embedded Script - PowerShell Core

This means that you can continue to use the Windows-specific functionality of classic "Desktop Edition" of PowerShell while also taking advantage of the cross-platform capabilities of the new "Core Edition."

3.5 baramundi Ticketing System

3.5.1 Exchange Online

Exchange Online is supported as an additional option for incoming and outgoing email accounts. It enables Office 365 mailboxes to be securely integrated and supports modern authentication methods. Authentication is done via the "Application Secret Key" which the customer must generate and then secure within the Azure Key Vault.

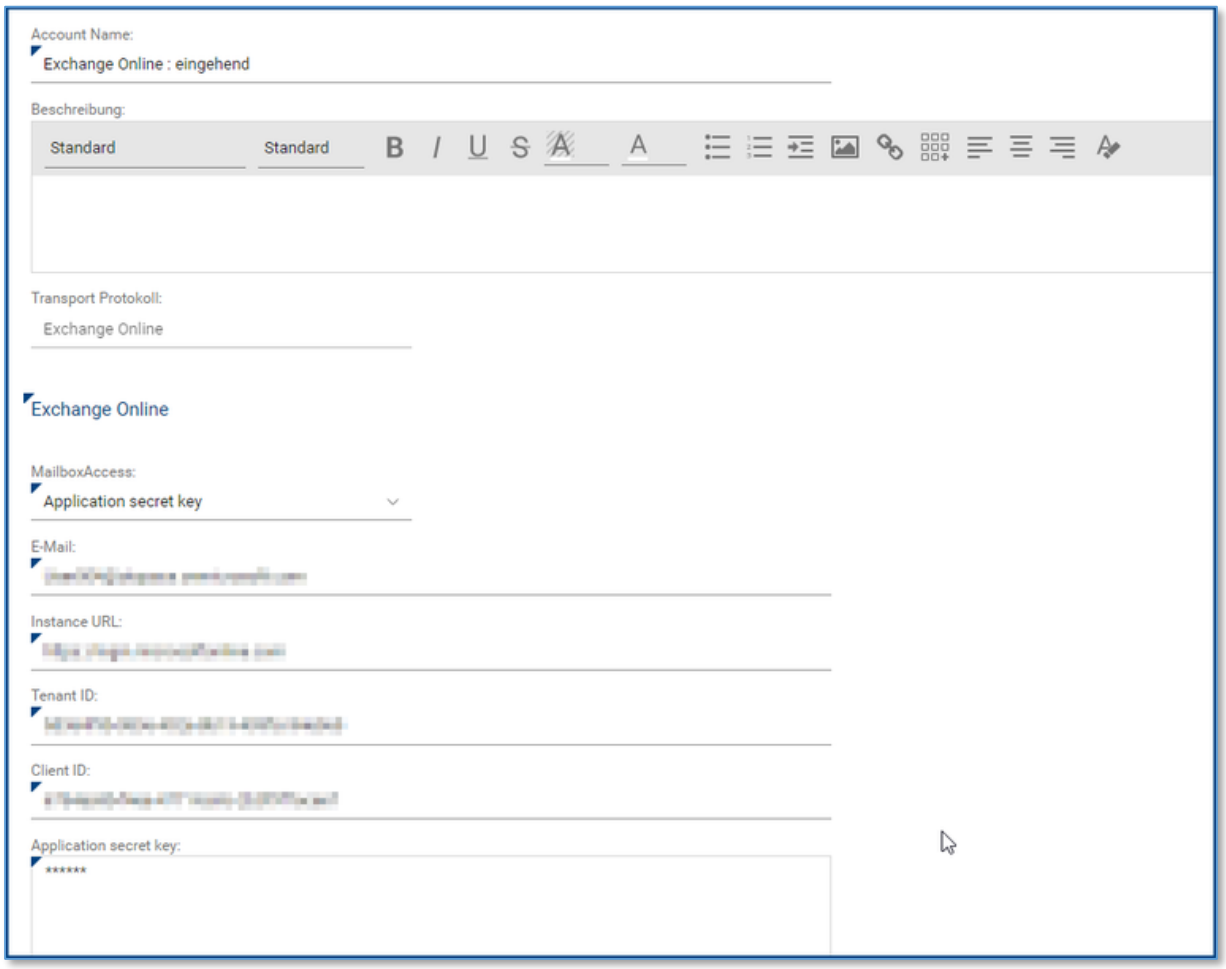


Figure 32 - bTS - Exchange Online Configuration

3.5.2 Reservations Management

Each asset can optionally be marked as "reservable," indicating if it can only be reserved by internal users or also in the self-service portal. Asset reservations can also be enabled either for all users or only by users within specific departments.

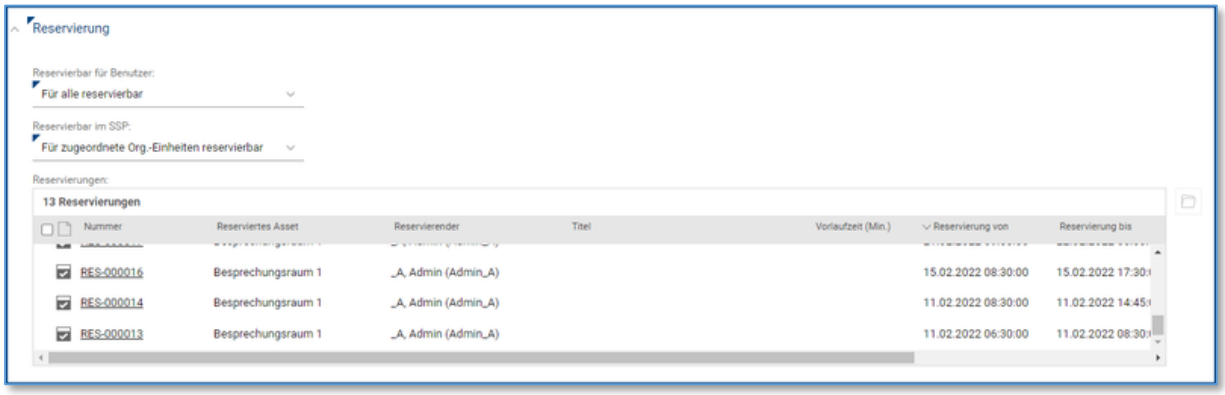


Figure 33 - bTS - Reservation setting on asset

Reservations can be created by users via the "Reservations" shortcut in the "Asset Management" area or in the self-service portal via corresponding new function tiles (if activated by the administrator). Reservations are made graphically via a timeline view or via a form. Asset descriptions are visible during the reservation. For a time-based reservation, lead and lag time can be specified (e.g., as buffers). The person responsible for the asset and the person making the reservation are informed by email about the progress of the reservation (new standard email templates have been integrated). Existing as well as previous reservations are documented in the asset.

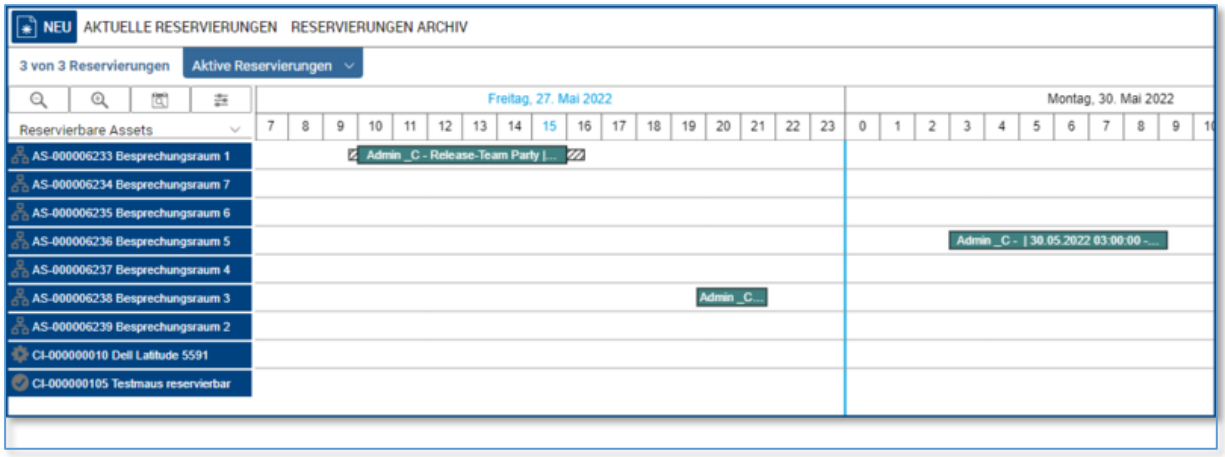


Figure 34 - bTS - Calendar view for asset reservations

3.5.3 Combination of orders

The extension of the ticket template using the "Combination with article order" option allows to order a store article package with any ticket at the same time. For example, for an on-boarding

process, a template including questionnaire and special task workflows can be combined with the order (e.g., "new workstation").

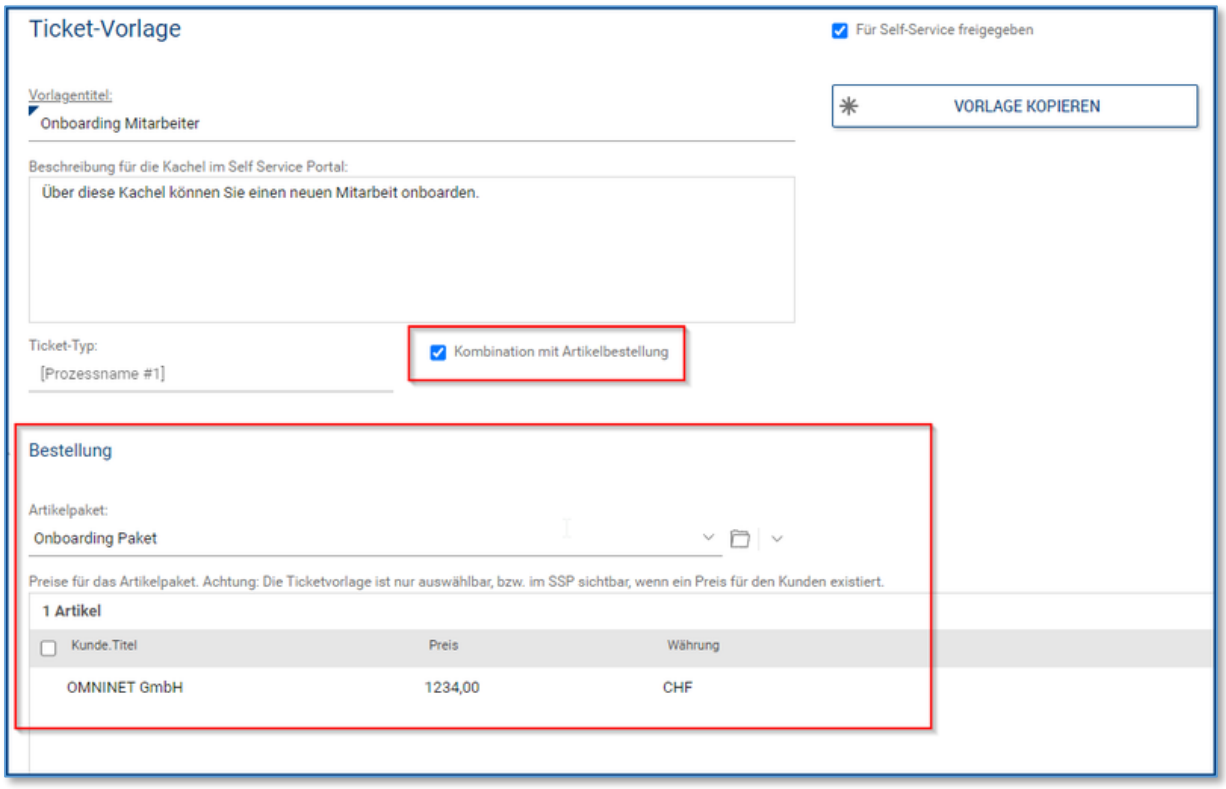


Figure 35 - bTS – Combining an article order

3.5.4 Global search

Until now, users could only search a list (e.g., tickets) by filter, full text or field search. A global search function now enables an additional, simple full-text search simultaneously in the most important system areas (tickets, assets, knowledge base, tasks).

The search allows the use of simple Boolean operators (AND/OR) and also has a fuzzy search for finding terms with typos or inconsistent spellings (e.g. search for "printer" also finds hits with "printr" or " pritner" etc.; the fuzziness can include up to 4 characters). Depending on the type, all titles, description and solution fields, as well as person and number fields are indexed in the objects. History tables or special additional fields are deliberately excluded from the index to reduce the amount of unwanted search hits.

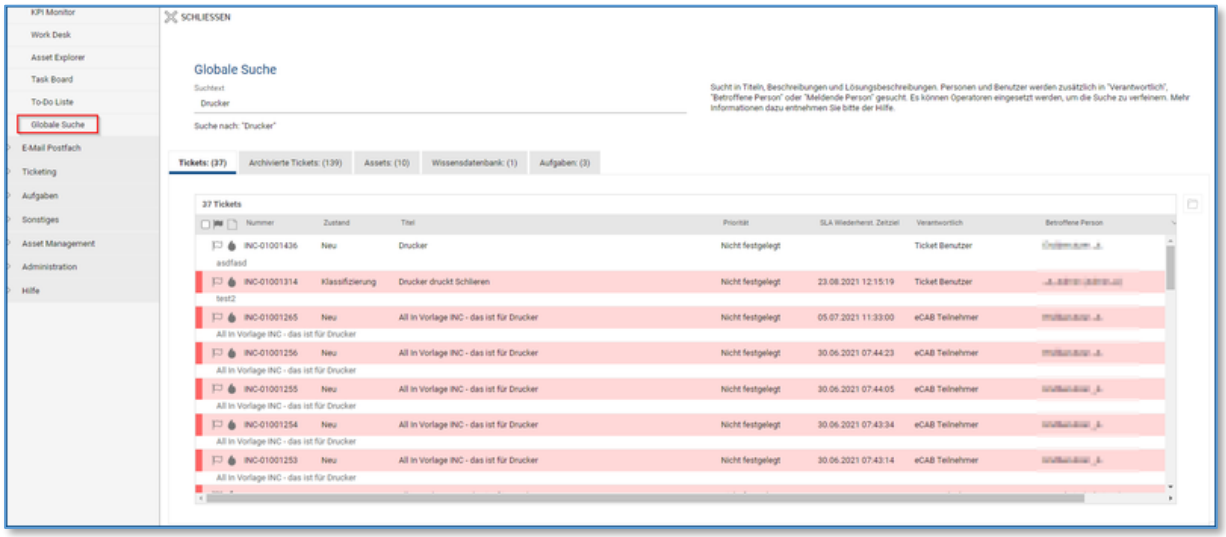


Figure 36 - bTS – Global search function

3.5.5 Ending sessions

For cases where users have accidentally closed the browser without logging out but need to log in again without waiting for the auto log off, or if a session is no longer responding, a user with administrator role can actively end the session of any other user. An overview of all current sessions is visible at the same time.

The function can be found in system administration under "license administration."

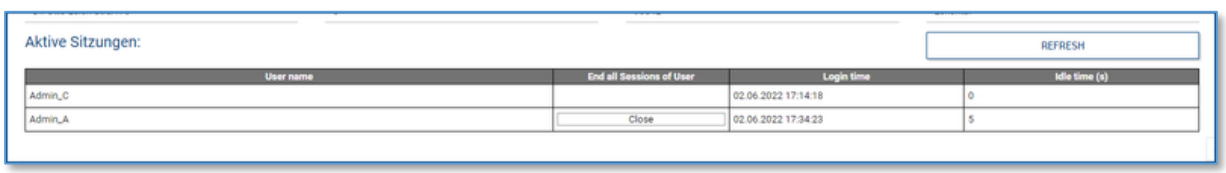


Figure 37 - bTS - View of active sessions

3.5.6 Improved import performance

The baramundi ticketing system regularly imports inventory data from other modules. Import performance is significantly improved even with many endpoints.

3.5.7 Ticket cost centers

Tickets have an optional new, permanently defined, "cost center" field. Cost centers can be managed as an administrator in the administration master data settings. The "ticket form" setting also let you activate the field cost center based on ticket type, making it a mandatory field for all of those tickets. The cost center is automatically entered when only one cost center is defined for a department or other organizational unit. Otherwise you can select one from a list of applicable cost centers for each unit.

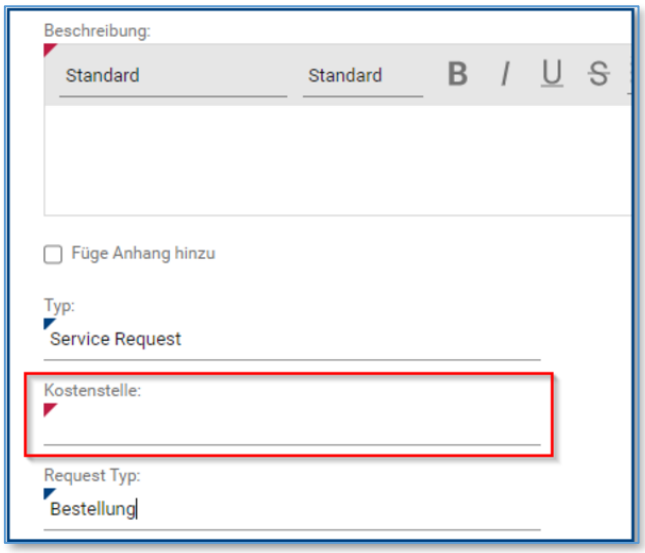


Figure 38 - bTS - Cost center as mandatory field

This allows cost centers to be directly assigned to tickets. Tickets with chargeable costs can be evaluated via filter, export or reporting interface to simplify management and processing.

3.5.8 Creation of teams

It's now possible to define individual teams consisting of people and users in addition to user groups. Teams can be used in different places in the system to simplify and organize administration.

Approvers for a specific topic can be defined as a group of several people stored in the approval model. Previously, each approver had to be defined individually. Changes to teams also have a direct effect on usage points.

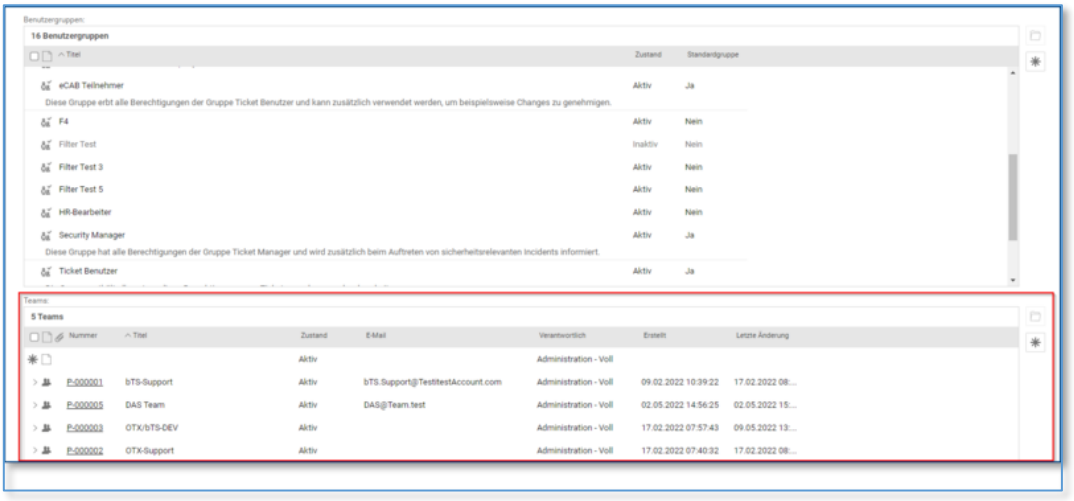


Figure 39 - bTS - Team management of members

Example: Add team as approver

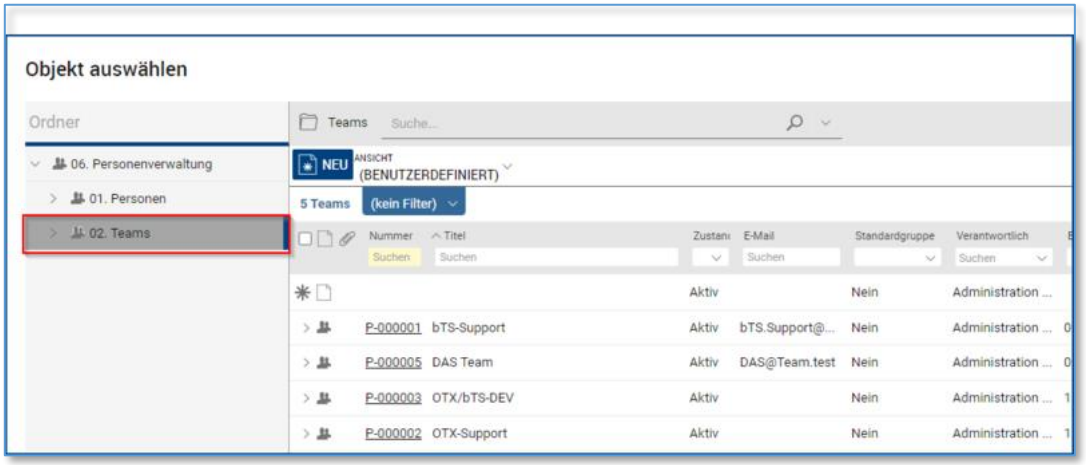


Figure 40 - bTS - Assignment of a team as approver

3.5.9 Default currency for item prices

For organizations that work completely in one currency, all price information can be converted centrally to other currencies. After the changeover, each store item or package will be displayed in this currency and new tickets with orders will be calculated accordingly.

Caution: This is a central setting. It is not yet possible to manage article prices with different currencies in parallel.

The setting can be made in system administration under "Articles." The following currencies are currently available:

- Euro | EUR
- US Dollar | USD
- Swiss Franc | CHF
- Czech Crown | CZK
- Danish krone | DKK
- British Pound | GBP
- Polish Złoty | PLN

Figure 41 - bTS - Item setting with default currency

3.5.10 Access to completed tickets in the Self-Service Portal

Users in the Self-Service Portal can now view all of their completed tickets by selecting the corresponding button in the "My tickets" list. A full-text search also shows the user's completed tickets.

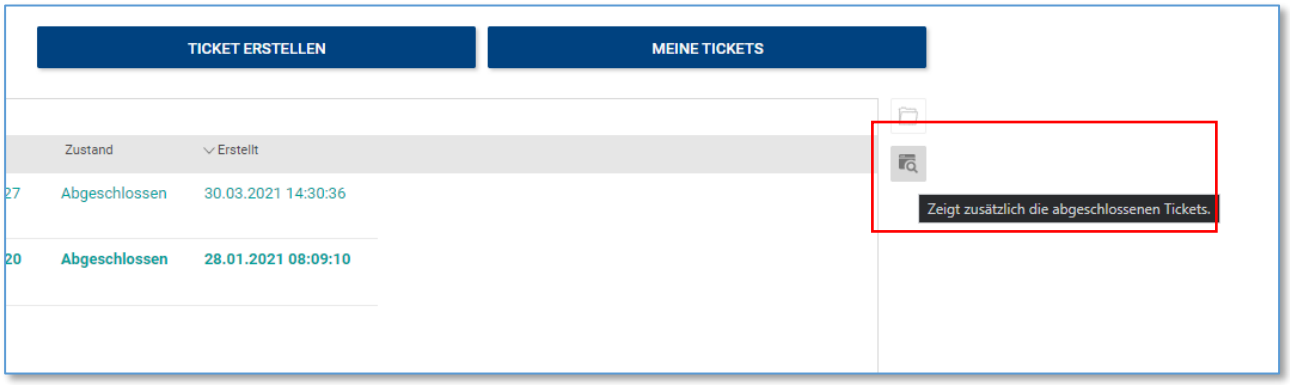


Figure 42 - bTS - Showing completed tickets

3.5.11 Extension of approval forms

Details have been added to the permit forms for permittees to evaluate:

- Ticket title
- List of order items
- List questionnaire answers

3.6 Other improvements

3.6.1 Windows Server Core 2019/2022 Support

With baramundi version 2022 R2, the baramundi Management Agent now supports Windows Server Core, a slimmer server edition that requires fewer resources and reduces attack surfaces. The agent inventory also returns the server version. This means that Windows Server Core installations can be detected using the "Version text" column.

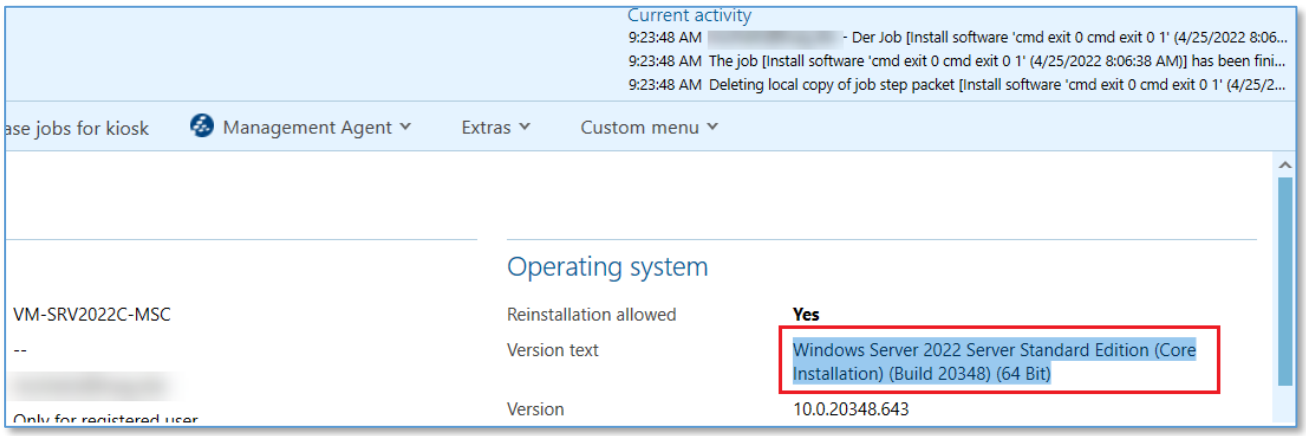


Figure 43 - Windows Server Core as Version text

Likewise, these installations can be mapped per Universal Dynamic Groups by accessing the "OS version text" field.

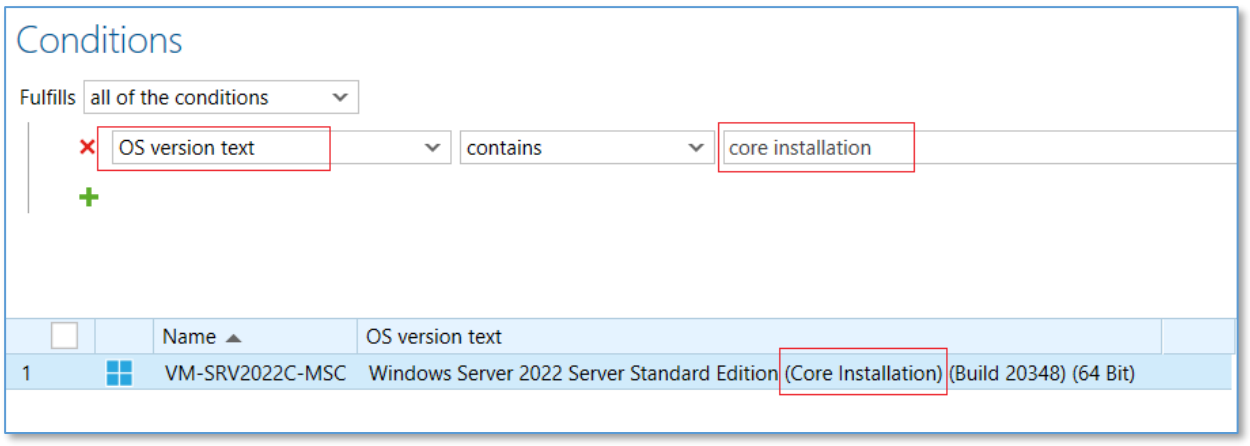


Figure 44 - Windows Server Core filterable in the "OS version text" of a UDG

The agent is installed and executed on core systems. User interface actions cannot be completed as indicated with a corresponding error message. It is also not possible to start a remote maintenance session on these systems with bRemote.

3.6.2 OS Customization Tool

We've updated the baramundi OS Customization Tool match new versions of Windows.
It can be installed and updated using MSW. The updated Tool addresses differences between Windows 10 and Windows 11 versions.

- The tool only displays options for the operating system in use. (inapplicable features are grayed out).
- The tool now offers an easy way to integrate language packs
- Internet Explorer options were replaced by Microsoft Edge configuration settings.

- Inclusion of custom registry files allows any kind of registry change to be made directly in the image.
- Options for older, unsupported Windows 10 versions have been removed.
- The tool now also supports the ‘dark mode’ for easier readability
- Special settings for Windows 11
    - Edge browser options with Google as search provider
    - Start menu left/center
    - Hide or show widgets
    - Open window or move minimized, if second monitor is missing
    - Window positions after hibernation
    - Hide Teams Chat icon

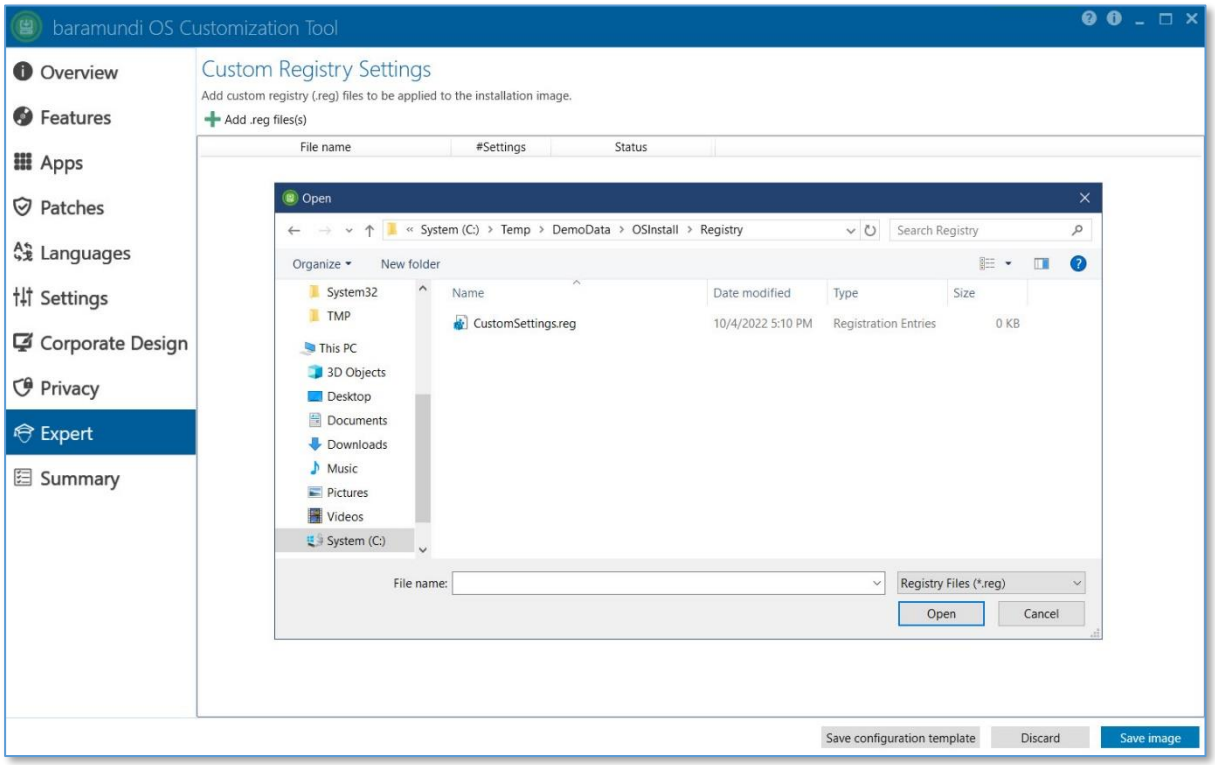


Figure 45 – OS Customization Tool – Registry Settings

3.6.3 Android Support

Restrictions

With Android 13, Google enables two more Wifi configuration restrictions. bMS 2022 R2 now makes it possible to prohibit sharing and adding Wifi networks.

Inventory

Data is also recorded in the inventory area. Hardware information indicates if biometric sensors (fingerprint, facial recognition) are available and whether they can be used or are already being used for unlocking. In addition, information about a configured eSIM is now recorded.

Execute command

The "Execute command" job step has been extended to include support for Android. If a current agent is installed on the device, defined commands can now be transferred to the agent. For example, it is possible to set the background image per job (on fully managed devices). Likewise, the device can be locked and located in case of loss. It is also possible to show customized messages on the display. Additional command can be conveniently selected via a menu.

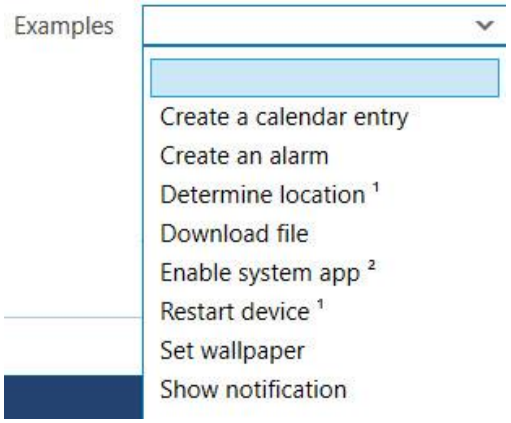


Figure 46 - List of currently available commands

Multiple selection in the Managed Play Store

Multiple apps can now be easily selected in the Google Managed Play Store dialog (Add App).

3.6.4 Mac and iOS support

AppClips

As of iOS 16, it is now determined whether an app is fully installed or merely created as an AppClip (e.g., by automatic memory optimization).

Accessibility

On iOS devices, activation of accessibility data and settings such as larger texts, zoom, VoiceOver or reduced movements are determined.

Apple Silicon CPU

For Macs, it is determined whether an Apple Silicon CPU or an Intel CPU is installed.

3.6.5 baramundi License Management – User defined variables

We've expanded information that can be included in bLM with the option to create custom variables for text, number and date. They are easily to be assign to the objects product, license and contract. This way you can individually store relevant information such as department, payment details or others.

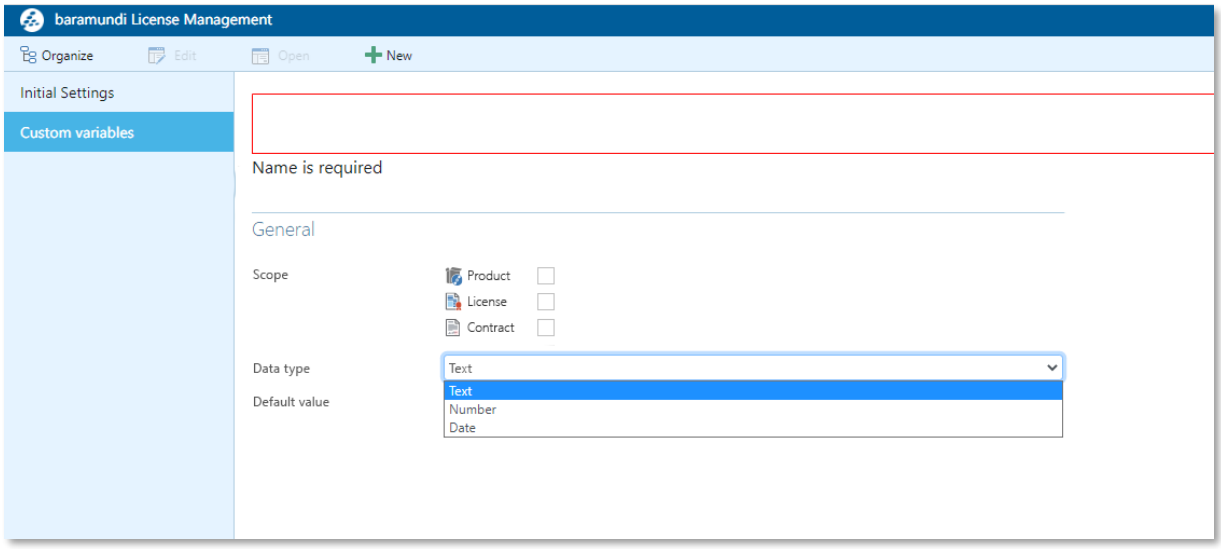


Figure 47 - bLM - Create variables and assign them to objects

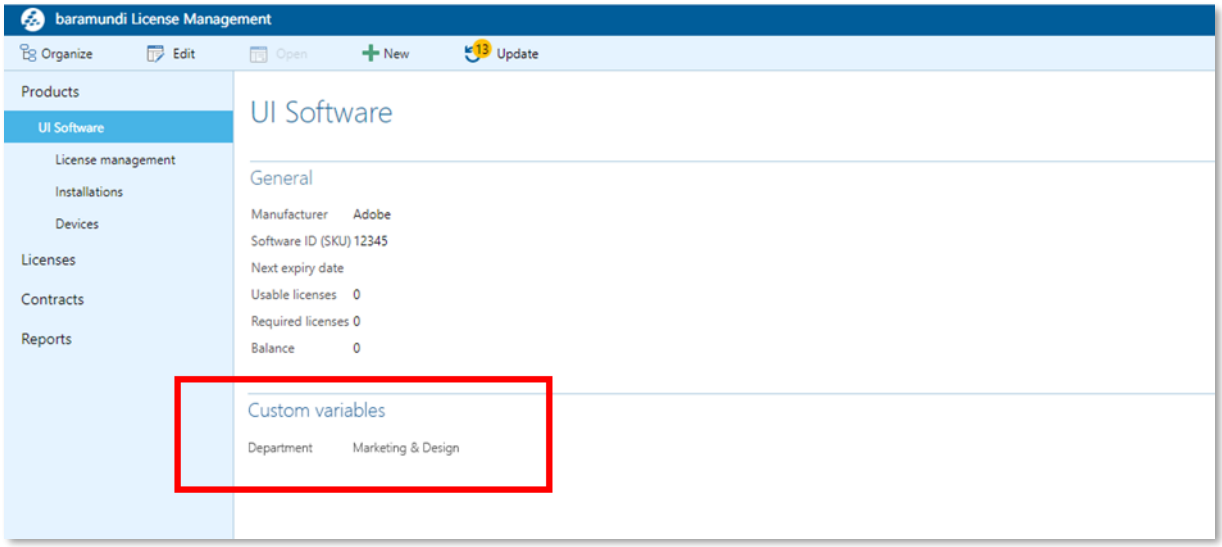


Figure 48 - bLM - Display of individual variables

Note: The new functionality will be made available via MSW. We will provide additional details about this when available in the baramundi Forum.

3.6.6 bMC Gridviews

The baramundi Management Center in the bMS 2022 R2 has also multiple enhancements. You can now hide individual grid columns directly in the so-called grid views via the contextual menu.

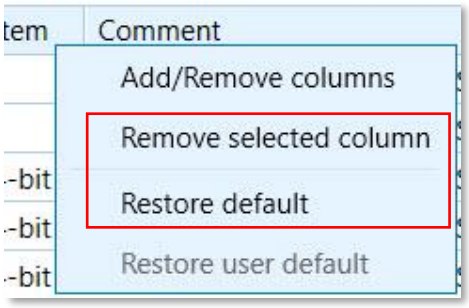


Figure 49 - bMC - Contextual menu of Grid View columns

The default view also can be restored in the column configuration dialog.

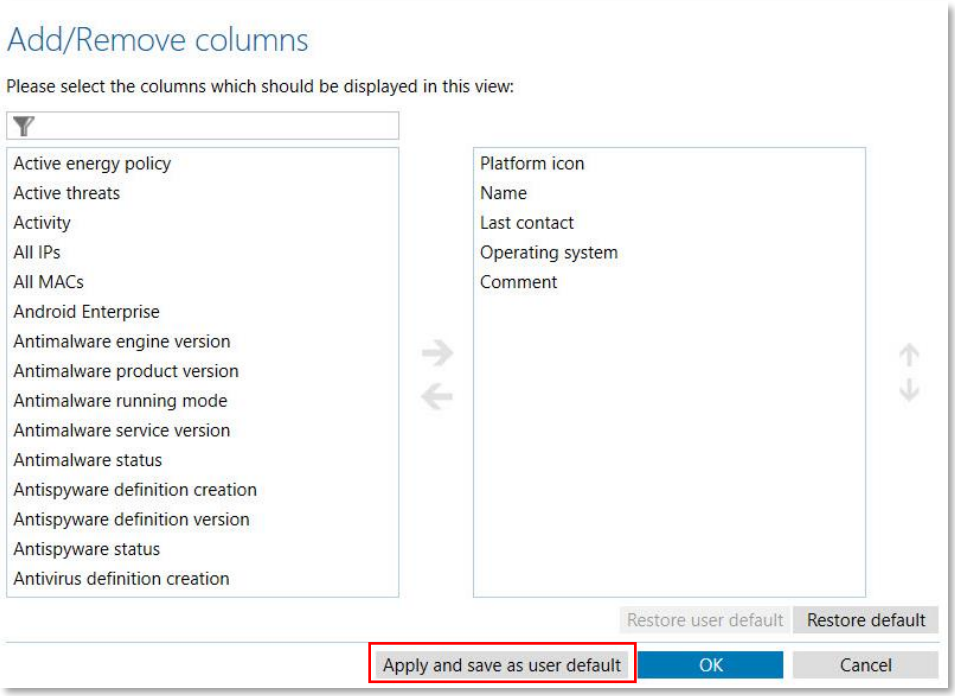


Figure 50 - bMC – Save Grid Views

3.6.7 Custom Commands

User-defined commands can now be set and enabled for all endpoint types and executed directly from the bMC. External applications also can now be called with endpoint variables using these parameters.

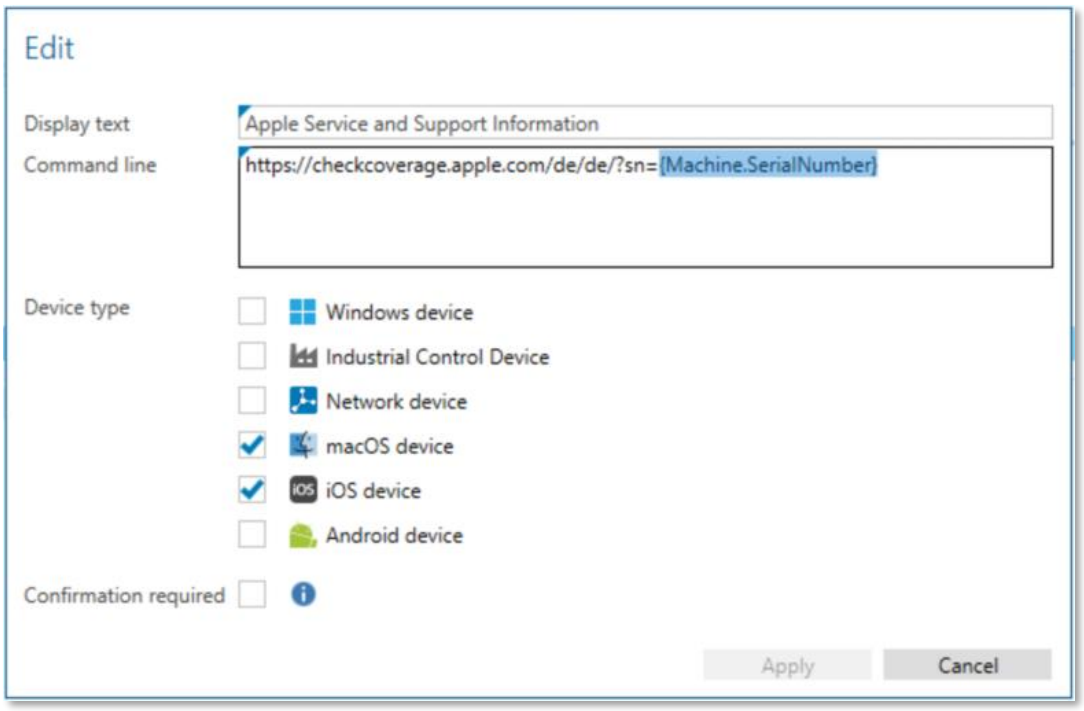


Figure 51 - Custom client commands for all endpoint types

This selection is available for your own custom commands as well as the global client commands.
The platform-specific variables from the inventory, such as IMEI, serial number and the unique device ID, can also be used.

3.7 Product improvements in detail

3.7.1 Windows Agent (bMA)

- The security update S-2022-01 is integrated.
- The `Distribute Microsoft patches (Classic)` job step now uses the 64 bit Windows API to determine the patch level. For x86 systems the 32 bit API is still used.
- Bugfix: The hardware inventory leads to a blue screen on the end device on newer systems.
- Bugfix: The hardware inventory does not read serial numbers of monitors under certain circumstances.
- Bugfix: The hardware inventory may not detect drives.
- Bugfix: Hardware inventory runs on various systems, e.g. HyperV virtual machines on timeout, whereby the process itself is not terminated and continues to consume resources.

3.7.2 Automation Studio and bDS

- Note: The schema of the bDS files has been increased. This means that the bDS scripts created by Automation Studio 2022 R2 cannot be executed by older bMA versions. As long as end devices are operated with older bMA versions, it is recommended to use an older, suitable Automation Studio version. These are available free of charge in Managed Software.
- Favorites stored in Automation Studio are reset.
- It is possible to execute embedded `PowerShell Core` scripts.
- In Automation Studio it is possible to search with Ctrl+F.

3.7.3 Management Center (bMC)

- To display the reports under `Extension - Reporting Management Suite` a database user is required. It is recommended to use a read-only database user for this purpose.
- The network map now shows which algorithm is used (STP or STP & FDB). The algorithm for STP & FDB is now no longer a preview.

- The outdated information for `Servicing Channel`, `Delay of feature updates` and `Feature update version` has been removed. Dynamic groups using these properties are marked with a `[CHECK]` prefix.
- The configuration for columns in Universal Dynamic Groups (UDG) can be saved as default.
- The device URL can be opened in the network map for industrial control devices.
- The configuration and functionality `Domain – Automatic inclusion in group` has been removed.
- Unwanted grid columns can be quickly removed via context menu using `Remove selected column`.
- Windows Server Core installations can now be detected by the `OS version text` column.
- Bugfix: If AUT is activated on a software, the processing of this software and also other software is sometimes strongly delayed.
- Bugfix: In rare constellations, some nodes in the bMC are not loaded for certain users or are displayed incorrectly.
- Bugfix: The view `Assignments Monitoring` sometimes does not display any data.
- Bugfix: When deleting the energy assets for an endpoint, all assets of the endpoint are deleted.
- Bugfix: At the Windows endpoint as well as at group views strongly increased and therefore wrong energy consumption data are displayed.
- Bugfix: In DarkMode some elements were displayed with an unreadable color scheme.
- Bugfix: Dynamic groups or a configured automatic job assignment may not work correctly when using a custom rule set and the query `number of violated rules on scan profile`.
- Bugfix: The bDX export/import of `Dynamic groups (Windows)` is only possible with restrictions

3.7.4 OS Install

- Bugfix: The OS patch level is sometimes displayed incorrectly if the upgrade was done via an enablement package.
- Bugfix: During OS installation of Windows 11, on a client with multiple partitions, an error message may appear `A partition on disk 0 could not be formed`.

3.7.5 Mobile Devices

- The Apple DEP synchronization interval has been increased from 5 minutes to 2 hours. This means that FAILED messages occur much less frequently when assigning the DEP profile to Apple devices.
- Bugfix: On Android Enterprise, the maintenance window for updating apps that are in the foreground was not set when rolled out with 2022R1.

  Note: To fix the bug on the device, the profile must be rolled out again.
- The `execute command` MDM job step is now available for Android Enterprise.
- In the `New-App Android Enterprise` action, multiple apps can also be selected in the Google Managed Play Store.
- DEP/iOS agent authentication now uses the SamAccountName. This makes account verification in secondary domains work more robustly.
- Hardware inventory on Apple devices detects more data and works more robustly.
- Software inventory on Apple devices detects app clips.
- Hardware inventory on Android now additionally detects fingerprint sensor, face recognition, EUICC (eSim) and whether fingerprint unlock is active.
- New restrictions for Android Enterprise to prohibit sharing distributed Wi-Fi networks or adding Wi-Fi networks.
- Skipping the specification of salutation are configurable in Apple Device Enrollment profiles for both a macOS profile and an iOS profile for languages where gender has an impact on the formal salutation.

- The creation and renewal of the Apple Push certificate takes place completely without interaction with baramundi. For bMS systems without an Internet connection, the certificate must be requested by email as before.
- The `Execution timeout` setting is now also taken into account for MDM jobs.
- Bugfix: Android Enterprise app configuration schemas are not always downloaded immediately when importing apps.
- Bugfix: The optional grid column `last contact bMD agent` is not updated.
- Bugfix: When copying MDM profiles with SCEP modules, links to Exchange and Wifi profiles may not be set correctly.
- Bugfix: Navigation from device to Android PlayStore user shows an error message if the user is not visible in the grid due to a filter.
- Bugfix: The bMC notification when the Apple DEP token expires points to an incorrect bMC view.
- Bugfix: Password type variables are not resolved correctly in MDM profiles.
- Bugfix: Distribution of apps with a very large store ID (e.g. by using a custom business app store) is not possible.

3.7.6 bServer

- AD Synchronization detects changes to AD-PrincipleNames and also changes them on the linked endpoint.
- The AD synchronization supports the synchronization of machines and users with Polish characters (ąćęłńśźżĄĆĘŁŃŚŹŻ) in the name or path. The representation in the bMS is in the equivalent ASCII representation (acelnszzACELNSZZ).
- Bugfix: Windows jobs with the setting `User must confirm` execution are sometimes not executed if the user has used the `Do not disturb` action.
- Bugfix: If under `Configuration-Domains` a very long password is entered for a domain, the bServer service does not start after the update.
- Bugfix: Variables in file lists are not resolved if `Copy files locally` is activated at the software and no bBT is used.

- Bugfix: The AD synchronization recognizes Mac and Linux operating systems partly wrong and creates these clients as Windows operating systems.
- Bugfix: In certain constellations the AD synchronization for machines runs into a NullReferenceException.

3.7.7 bConnect

- The string values `DenyAll` and `UseBandwith` of the parameter `BandwidthMode` of the controller `IpNetwork` were changed to `BlockAll` and `UseBandwidth`.

3.7.8 macOS

- The MDM job step `Execute Command` is now also available for the macOS platform.
- Bugfix: The import of certain .PKG files, e.g. the Microsoft Defender App for macOS, fails with "Error opening file".

3.7.9 bDX Im/Export

- Applications with the security context `Specify user` are switched to LocalSystem on export. This prevents username/password from being included in the bDX file.

3.7.10 baraDIP

- The security update S-2022-01 is integrated.
- Bugfix: The configured In-/Excludes lead to unexpected behavior. For example, the specification "Folder1" also transfers "Folder1b". If the behavior is still desired, the wild-card "Folder1*" can be used.

4 Appendix

4.1 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

4.2 Third Party Components

Information about 3rd party licenses can be found on the ISO image under:
`..\3rdParty-Licensing\3rdPartyLicenses.pdf`

baramundi

baramundi software AG
Forschungsallee 3
86159 Augsburg, Germany

+49 821 5 67 08 - 500
support@baramundi.com
www.baramundi.com

+49 821 5 67 08 - 500
support@baramundi.com
www.baramundi.com

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

+49 821 5 67 08 - 500
support@baramundi.com
www.baramundi.com

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

+1 800 470 3410
support@baramundi.com
www.baramundi.com

baramundi software Austria GmbH
Landstraßer Hauptstraße 71/2
1030 Wien, Austria

+49 821 5 67 08 - 500
support@baramundi.com
www.baramundi.com

Empower your IT