



# baramundi Management Suite

2024 R1

*Empower your IT*

Dear reader,

This release offers useful new features and numerous product enhancements to improve the use of bMS for both IT admins and end users.

To increase IT security:

- **Defense control** enables IT admins to configure temporary **dynamic passwords** for local administrator account access, adding flexibility for managing endpoints while reducing potential attack vectors.
- Even with readily available cloud storage, **mobile devices** still need secure access to on-premises company data. The new **per-app VPN** allows secure tunnel connections between specific authorized apps and company data sources.

To optimize end-user experiences, admins can use graphical analysis of quantitative and qualitative **user feedback** via **Argus Experience** to spot problems and determine solutions in advance to avoid an increase the number of support tickets.

To increase management flexibility, there also are detailed improvements for Universal Dynamic Groups (UDGs), device identification via UUID, Linux inventory, Android and iOS management and our bConnect interface.

I wish you a stimulating read.

Armin Leinfelder  
*Director Product Management*

# baramundi Management Suite – Version 2024 R1

---

## TABLE OF CONTENTS

<b>1</b>	<b>Release 2024 R1</b>	<b>4</b>
1.1	Defense Control	4
1.2	Mobile devices	5
1.3	User feedback & analytics in Argus Experience	12
1.4	Additional improvements	16
1.5	System requirements and compatibility	25
1.6	Product improvements in detail	33
1.7	Notes and known Limitations	40
<b>2</b>	<b>Release 2023 R2</b>	<b>45</b>
2.1	baramundi Remote Desk	45
2.2	Inventory by SSH for Linux Devices	51
2.3	Single Sign-On (SSO) In The Kiosk	53
2.4	Mobile Devices	54
2.5	Universal Dynamic Groups	56
2.6	Network Devices	58
2.7	Further developments in Argus Experience	60
2.8	Miscellaneous	65
2.9	Product improvements in detail	68
<b>3</b>	<b>Release 2023 R1</b>	<b>77</b>
3.1	Windows Vulnerability Catalog 2.0	77
3.2	bConnect 2.0	78
3.3	baramundi Ticketing System [Preview]	81
3.4	baramundi Argus Cockpit and Argus Experience [Preview]	85
3.5	Universal Dynamic Groups	89
3.6	Product improvements in detail	90
<b>4</b>	<b>Appendix</b>	<b>95</b>
4.1	Glossary	95
4.2	Third Party Components	96

# 1 Release 2024 R1

## 1.1 Defense Control

### 1.1.1 Management of local administrator passwords

When hardening IT environments, it is important that users have limited -- and especially no administrative -- authorizations on their devices. However, in some cases it may be necessary to log on to the device as a local admin, for example, when an on-site technician needs to troubleshoot and fix problems. Deactivating local admin account access on all endpoints would make that difficult. But it's also inadvisable to enable local access across the board because that would degrade security.

To provide the management flexibility enabled by local administrative access while maintaining security, the bMS now lets IT admins configure temporary dynamic passwords for local admin account access even if there is no network connection.

IT admins first set conditions such as the local administrator username (also with variables), the length of the password and how long the password remains valid. The bMS then manages the endpoint admin accounts and the generation of new passwords.



Illustration 1 – Configuring a local administrator managed by the bMS

IT admins can view passwords via the baramundi Management Center and provide them to authorized personnel to complete needed tasks. Passwords can then immediately be reset or re-generated.

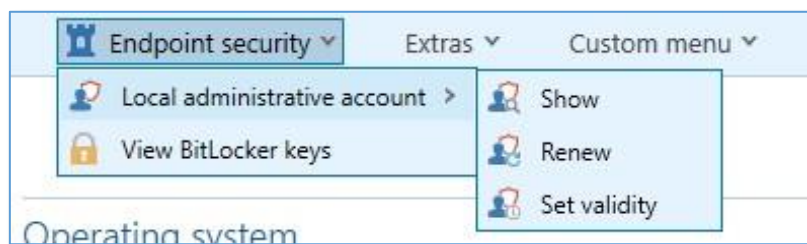


Illustration 2 - New "Endpoint security" contextual menu

The dynamic login data for the local admin account managed by the bMS also is available for use as a variable in the bMC, e.g. in "User-defined client commands".

## 1.2 Mobile devices

### 1.2.1 Per-app VPN access to company data

Mobile and hybrid work is the new "normal" and an integral part of modern business. Secure access to company data is essential for productive work when away from the company network. Company data and services in the cloud are readily accessible from any authorized device. But what about data and services not yet available in the cloud or deliberately not stored there?

VPNs are typically used to give mobile devices secure access to apps and resources on the company network. The bMS has long enabled IT admins to configure and manage VPN connectivity for mobile devices. However, this gives all apps installed on a mobile device, e.g., an ERP app and a private messenger app, access to the company network. With the widespread adoption of BYOD and COPE, it's essential to have clear and consistent separation between private and business usage of mobile devices.

#### 1.2.1.1 Concept

The answer is simple: configure VPN access on a per-app basis. That means that only specific authorized apps can use the VPN to establish secure encrypted connections to the company network. While that would typically require complex configurations for both the internal network and mobile devices, the bMS now handles per-app VPN set-up and management quickly and easily.



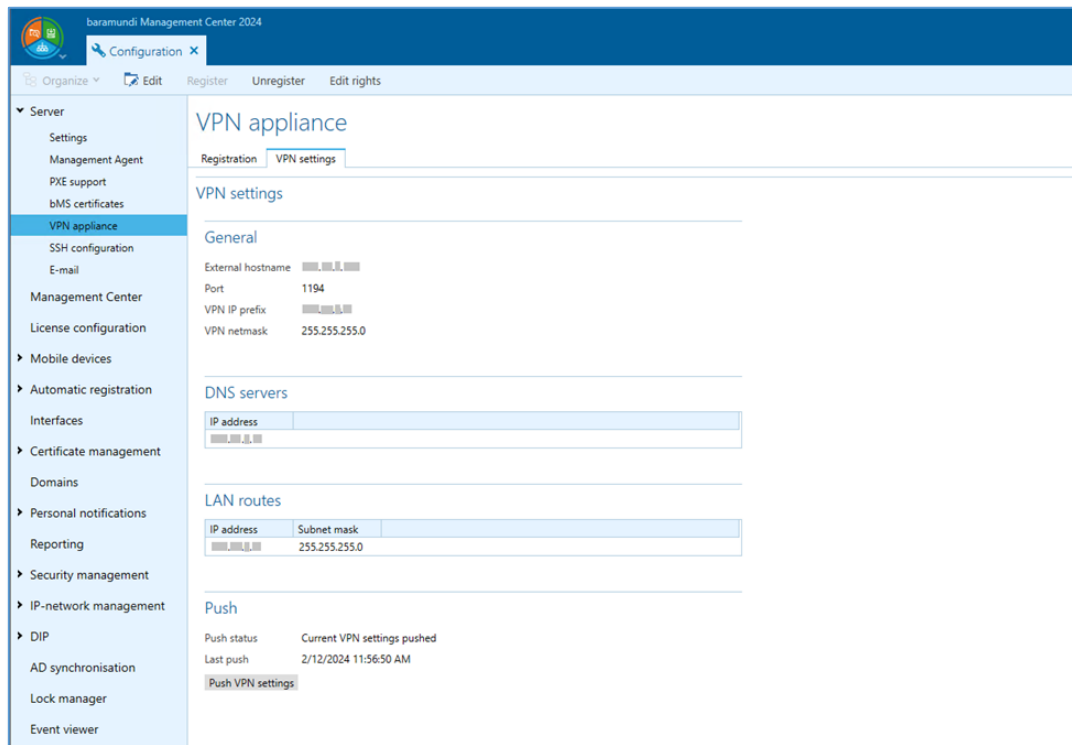


Illustration 3 - Configuration page for the VPN appliance

The solution consists of an app on the end device (iOS/Android) and a virtual appliance in the DMZ (demilitarized zone). After initial setup, the appliance is completely managed by the bMS. Access via the VPN is secured using a client certificate - only valid certificates issued by bMS are accepted.

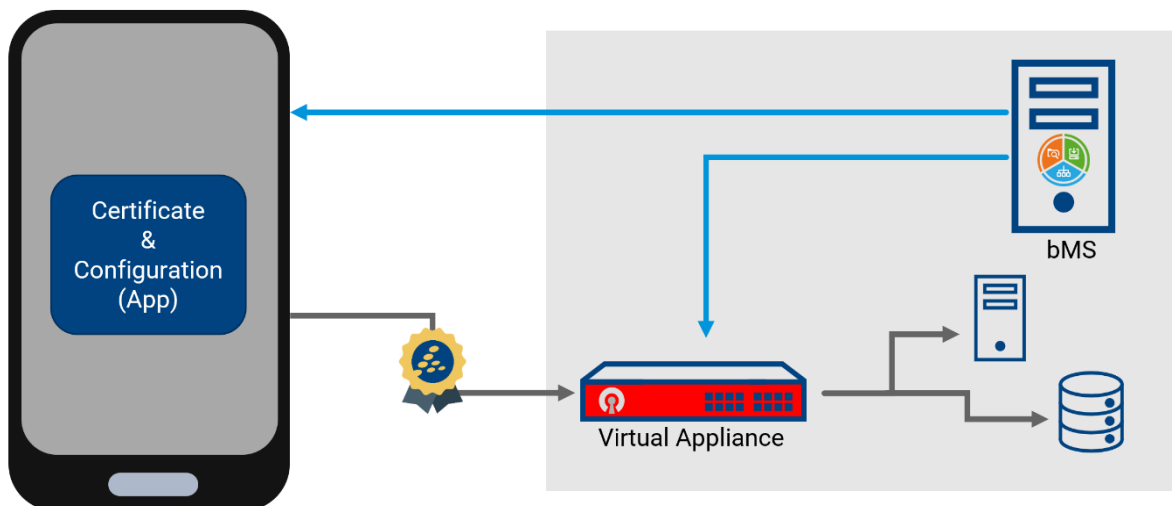


Illustration 4 - Representation of the VPN setup process

### 1.2.1.2 Set-up and management

To enable per-app access, a VPN app must first be installed and configured on the device. That allows the device to establish a connection to the baramundi VPN appliance for authentication. Both tasks can be completed with a job to simplify deployment.

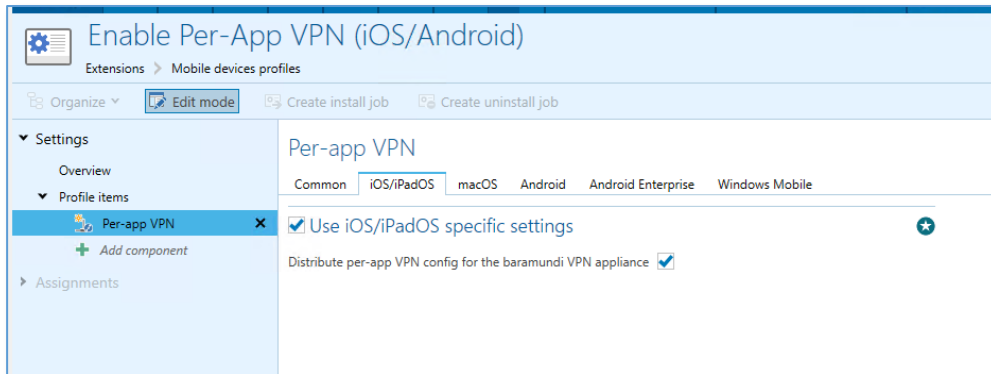


Illustration 5 - Activation of the VPN function via profile module

You can also use a job to revoke VPN access. The bMS-issued certificate is removed from the device and blocked on the appliance even if the certificate has been lost.

Once basic access has been set up, authorized apps can be configured to use the VPN. The use of the VPN only needs to be activated in the job step to install the app.

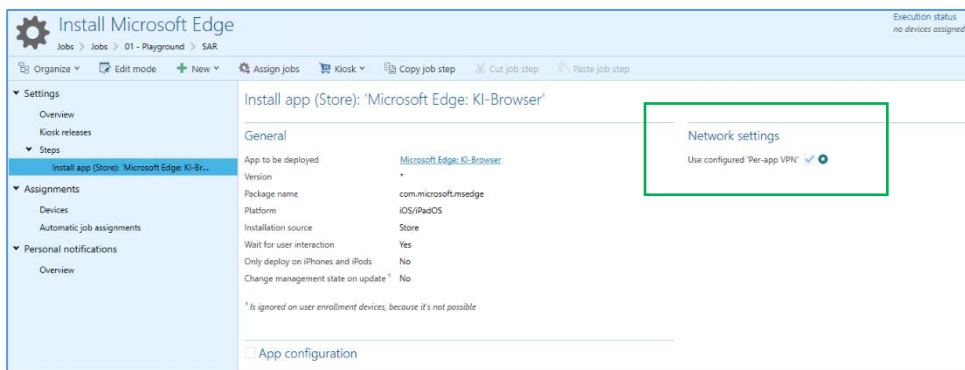


Illustration 6 - Activating the VPN function during app installation

### 1.2.1.3 Transparency for users

The use of the VPN is completely transparent for device users and no special actions are required. The system automatically establishes the VPN tunnel when authorized company apps are used.

#### 1.2.1.3.1 Apple iOS

In iOS, the connection status and the apps set up to use the VPN can be viewed in "Settings."

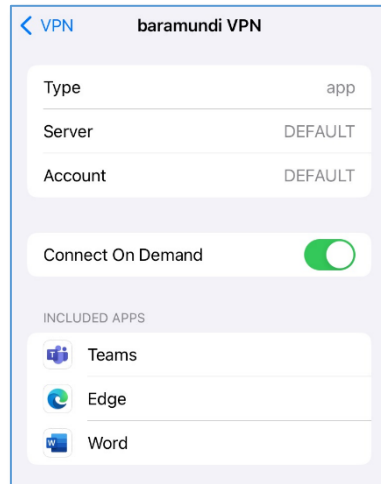


Illustration 7 - Per-app VPN settings in iOS



### 1.2.1.3.2 Google Android

On Android devices, the connection status can be seen in the "baramundi VPN" app.

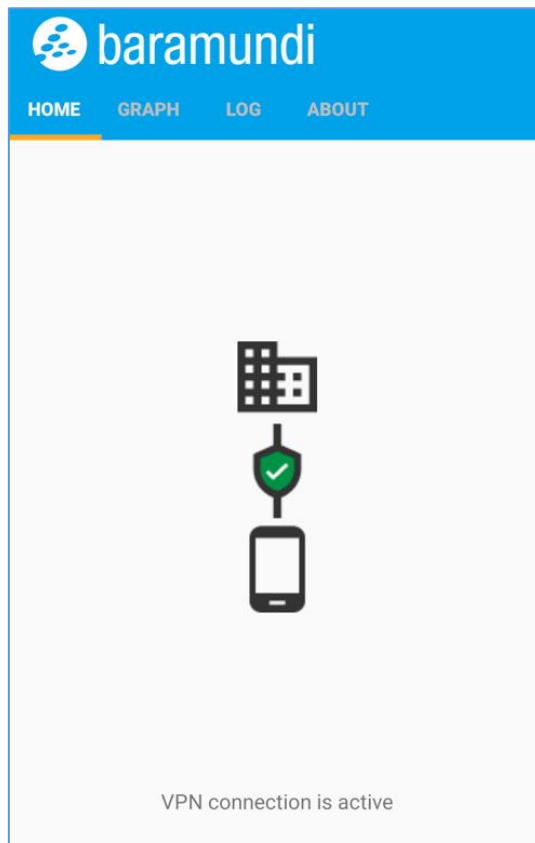


Illustration 8 – Connection status shown in the baramundi VPN app for Android

## 1.2.2 Further MDM improvements

### 1.2.2.1 Support for WPA3

The Wifi module supports the configuration of WPA3 Personal and Enterprise on Apple iOS, Apple macOS and Google Android.

WPA3 Personal	WPA3 Enterprise
from iOS 13	from iOS 13
as of macOS 10.15	as of macOS 10.15
from Android 11	from Android 12

### 1.2.2.2 Android

#### 1.2.2.2.1 New push service for job processing

Beginning with bMS 2024 R1, all push messages required for the management of Android devices will be sent via the central baramundi infrastructure. This means that local configuration of Android push services (Firebase Cloud Messaging/FCM) is no longer necessary.

**Note<sup>1</sup>** : From June 20, 2024, push will no longer work with older versions of the bMS up to and including 2023 R2. Devices will then only work via cyclical job retrieval. To ensure seamless job processing via push, you should update to the current bMS 2024 before June 20, 2024.

#### 1.2.2.2.2 WLAN configuration in the enrollment code

When enrolling Android devices via QR code, a Wi-Fi configuration can now also be provided.

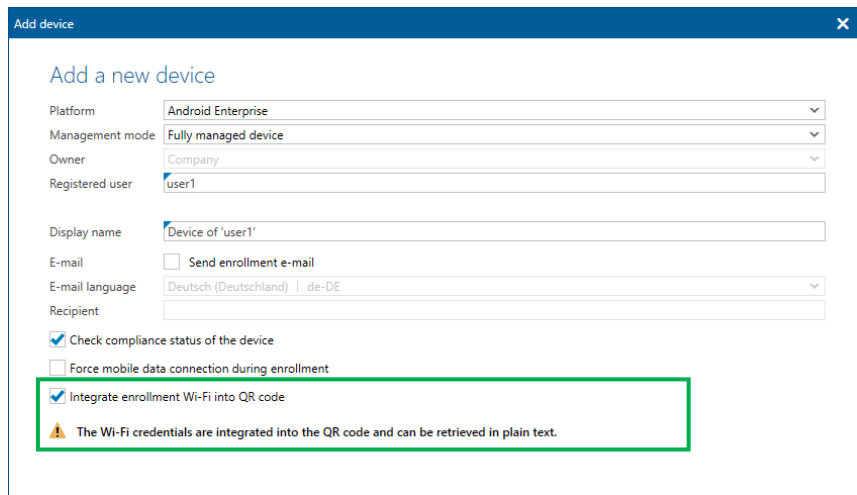


Illustration 9 - Enrollment dialog with option for Wifi configuration and corresponding note

No manual connection needs to be established before enrollment, making the process simpler and less complicated.

<sup>1</sup> <https://forum.baramundi.com/index.php?threads/16099/>

#### 1.2.2.2.3 Activate developer options

Developer options can now be controlled via the "Restrictions" module. For example, users can be granted access to the debug options to select which mode ("Charge only", "Data transfer", "Android Auto" etc.) the device should use when connecting a USB cable.

**Note:** *Activating the developer options should only be done for brief periods and not used on devices in active use. Many device security measures could be bypassed when developer options are enabled!*

#### 1.2.2.3 iOS

##### 1.2.2.3.1 Set time zone

Device time zone settings can now be defined with the new "Execute command" job step. This is necessary if location services on the device have been deactivated and the local time zone cannot be determined automatically.

##### 1.2.2.3.2 Third-party App stores

Starting with iOS 17.4 Apple will now allow other App stores besides their own and also they allow sideloading for Apps. Because this behavior allows the installation of potentially untrusted or malicious apps, the bMS now offers a restriction setting to deactivate sideloading and third-party App stores.

## 1.3 User feedback & analytics in Argus Experience

### 1.3.1 Recording end user feedback

baramundi Argus Experience reaches another important milestone with the collection of end-user feedback. Instead of just analyzing device data, IT admins can now also solicit employee feedback on their IT environment and experiences. This gives IT admins a holistic view of device and network performance and the ability to detect and analyze and proactively address potential problems and incidents in a targeted manner.

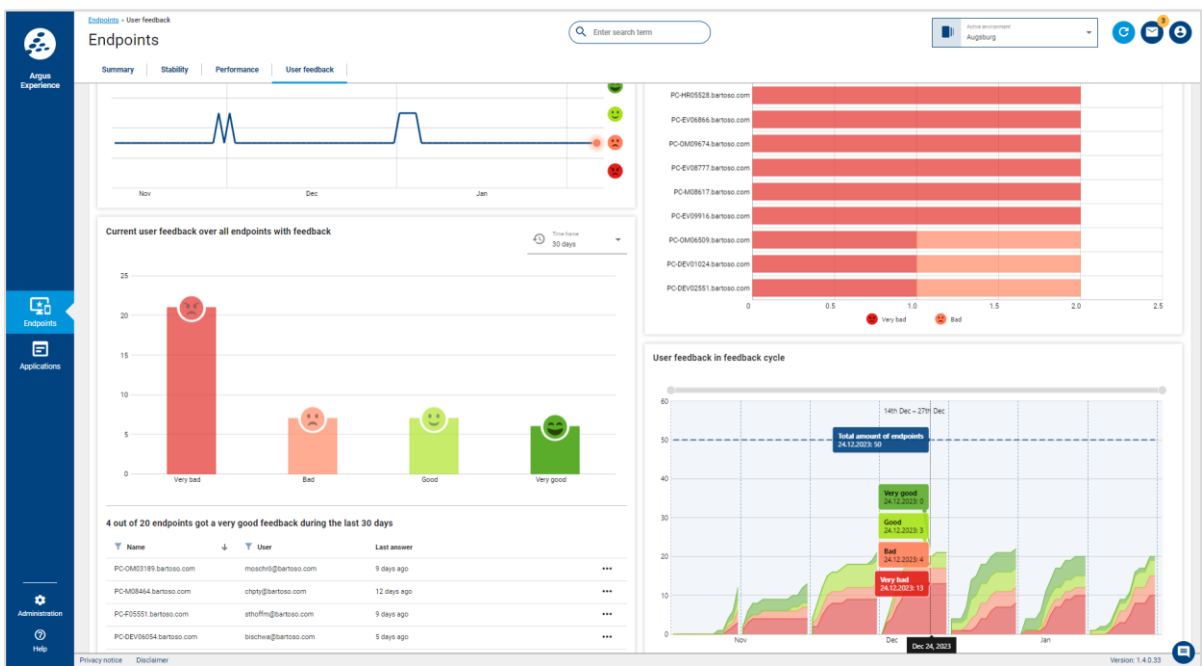


Illustration 10 - Overview of collected user feedback

1.3.1.1 "Hidden" need for action through end-user feedback

You could argue that admins already receive sufficient feedback from their end users through support tickets. However, such feedback is usually negative because it is generated after an incident. It is more useful and productive for IT staff and users alike to collect feedback continuously by making it easy for users to provide input.

For example, user feedback helps IT admins prioritize responses when:

- Many applications crash + negative feedback increases  
→ **Urgent need for action**
- Many applications crash + feedback is neutral or nominal  
→ **Urgent action not needed**
- Few applications crash + negative feedback increases  
→ **Urgent need for action**

While urgent action is indicated by user feedback in point 1, the priority in points 2 and 3 varies based on user feedback.

If IT admins relied solely on device data they might have intervened unnecessarily, e.g., because crashes occurred in the background and did not affect employees. Or, they may have delayed action on fewer crashes despite a spike in user frustration and a drop in productivity.

In Argus Experience, IT admins can configure and evaluate user feedback surveys based on the specific needs of their IT environment.

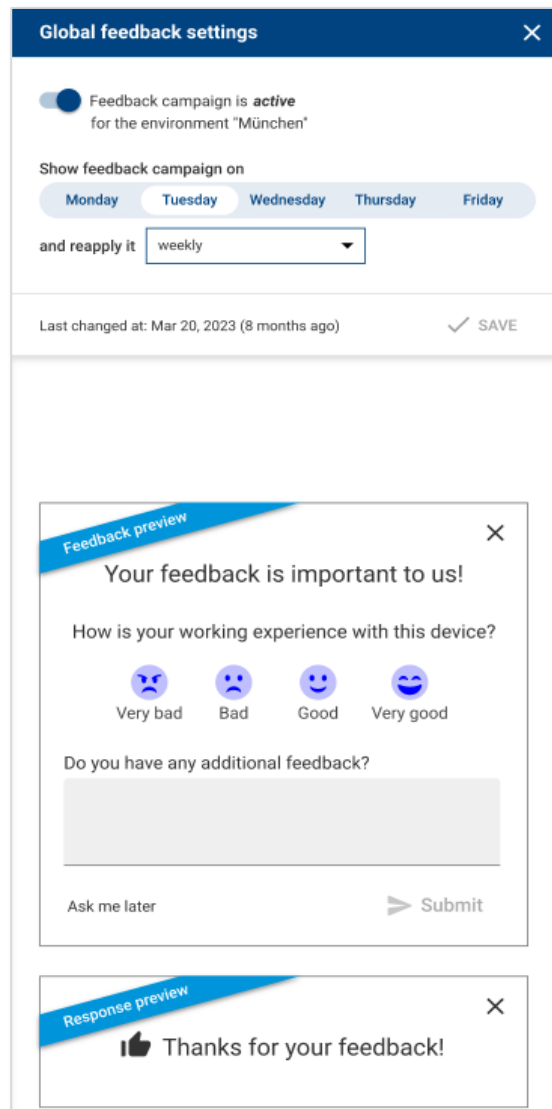


Illustration 11 - Configuration of user feedback surveys

### 1.3.1.2 View detailed feedback

User feedback is helpful, but the content of feedback is important for prioritizing responses. For example, if employees continuously "complain" or provide negative feedback about certain software, IT admins can troubleshoot and resolve the issue proactively - *before* support tickets are submitted. Possible responses could include installing needed updates, offering training or suggesting alternative applications.

In Argus Experience, user feedback is clearly displayed on endpoint detail pages.

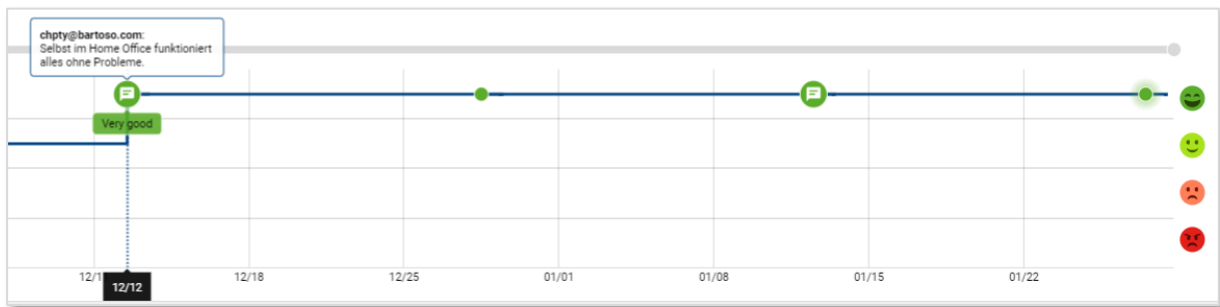


Illustration 12 - Feedback details in Argus Experience

### 1.3.1.3 Compare survey cycles

Collecting user feedback is not an episodic or "one-and-done" process, rather, it should be regular and continuous. This enables IT admins to recognize changes and trends at an early stage and take appropriate action.

With the clear presentation of feedback surveys in time-based cycles, the results of IT responses can be analyzed and compared. For example, a survey cycle after a Windows 11 rollout can be used to determine if employees are satisfied and comfortable with the new operating system or if they have questions or issues that should be addressed. Similarly, survey cycles could be synchronized with each wave of the deployment of new or updated applications to gauge user experiences and software performance.



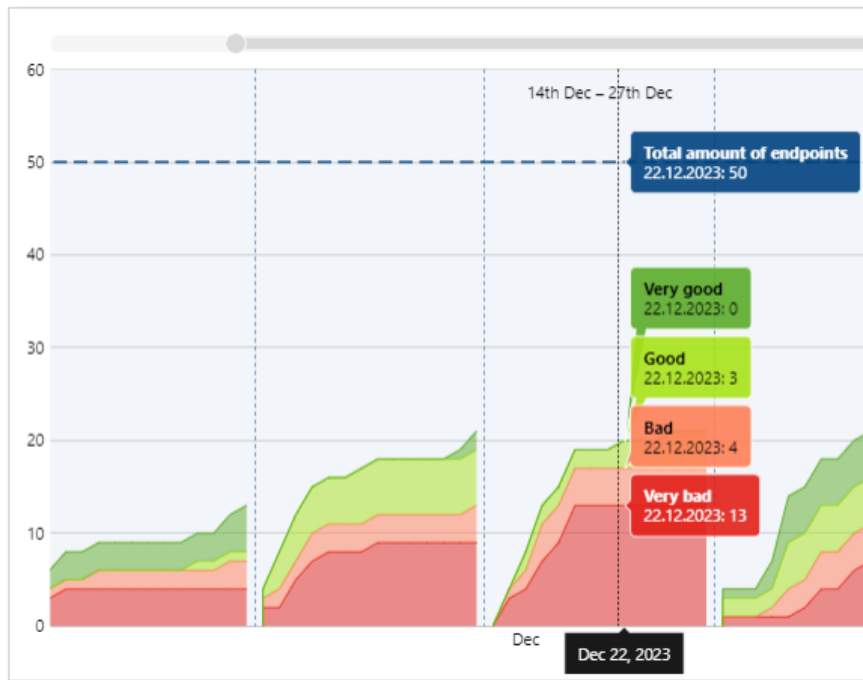


Illustration 13 - Compare survey cycles

### 1.3.2 Other endpoint data

To further improve user experiences and optimize IT productivity, we plan to add the ability to record and analyze other endpoint performance data in Argus Experience including<sup>2</sup> :

- Bluescreens**  
 “BSOD” and other system crashes can be very frustrating to users and negatively affect productivity. While error analysis in such cases can often be difficult, data from Argus Experience can give IT admins valuable insights for efficient troubleshooting and problem resolution.
- CPU and memory utilization**  
 Some endpoint computers are heavily utilized while others are often idle or "twiddling their thumbs." CPU and memory utilization data recorded by Argus Experience can better align procurement of new computers with expected usage.
- Application-based boot time**  
 While it's easy to determine which end devices have very long start-up times, it was not possible to see which applications were causing the slowdowns. Argus Experience will record and display granular application-level boot time data so IT admins can proactively update or replace problematic software.

<sup>2</sup> Due to the continuous release of updates for Argus Experience, implementation of some features will not be available until after this document is published. To check for updates please see: <https://www.baramundi.com/en-us/management-suite/modules/argus-experience/argus-experience-updates/>

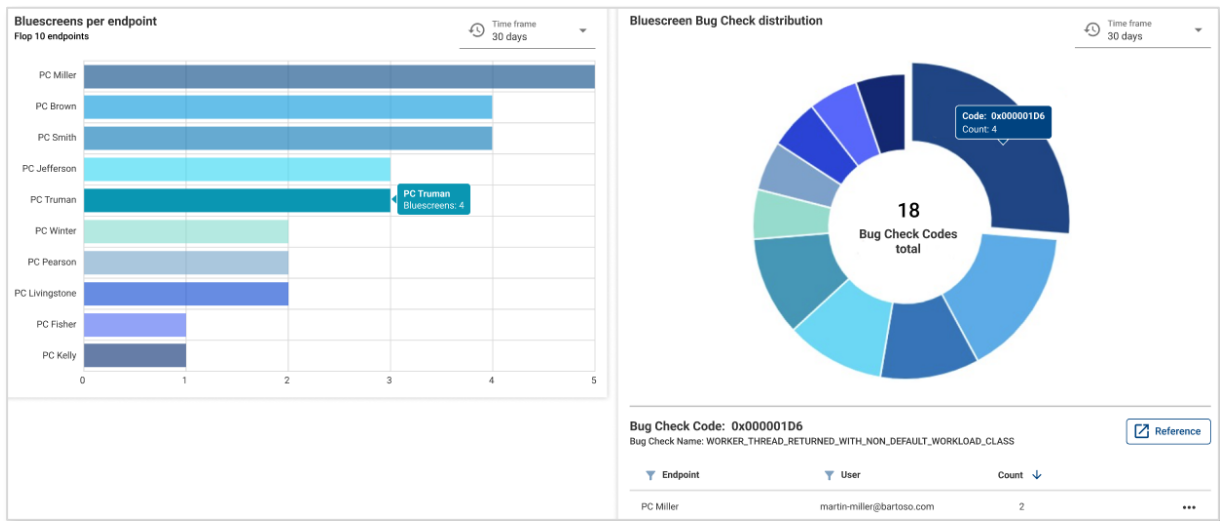


Illustration 14 - Prototype UI showing data from bluescreen crashes

## 1.4 Additional improvements

### 1.4.1 New criteria for Universal Dynamic Groups

Universal Dynamic Groups (UDGs) have been continuously enhanced since their introduction to make them increasingly customizable, including the ability to define automatic job assignments added with bMS 2022 R2.

Three new conditions make it possible to create even more granular groups. These can be provided with all UDG features, including automatic job assignments and sync to Argus Cockpit.

#### 1.4.1.1 Software

UDGs receive a new condition for software installed on endpoints that can be used in many common scenarios.

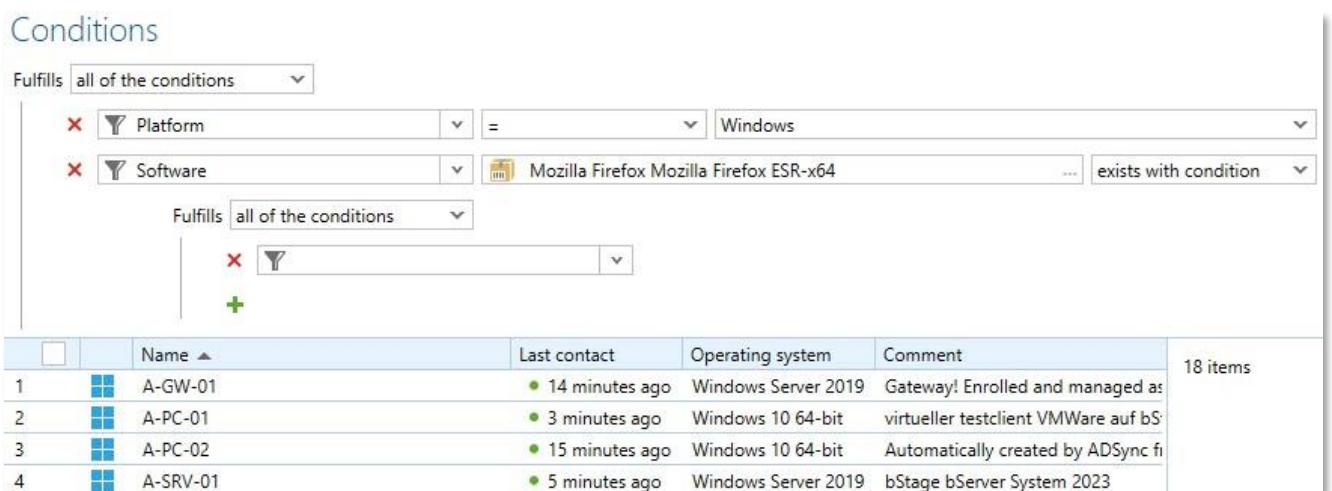


Figure 16 - Conditions for installed software

For example, the condition "Software" (Windows) allows you to search your own software in the Windows environment. The dropdown for "exists/does not exist/exists with condition" enables even more precise criteria.

- **exists:** checks whether endpoints have specific software installed
- **does not exist:** Checks whether the selected software is missing on the endpoints; this applies to software installed via the Deploy module as well as inventoried installations.
- **exists with condition:** checks whether endpoints have specific software installed and if so, with granular conditions:
  - **was installed before/after/on:** only installations with a corresponding installation date; this applies to installations by Deploy as well as the "initial" inventory.
  - **was last found before/after/on:** checks when the corresponding software was last inventoried on the endpoint

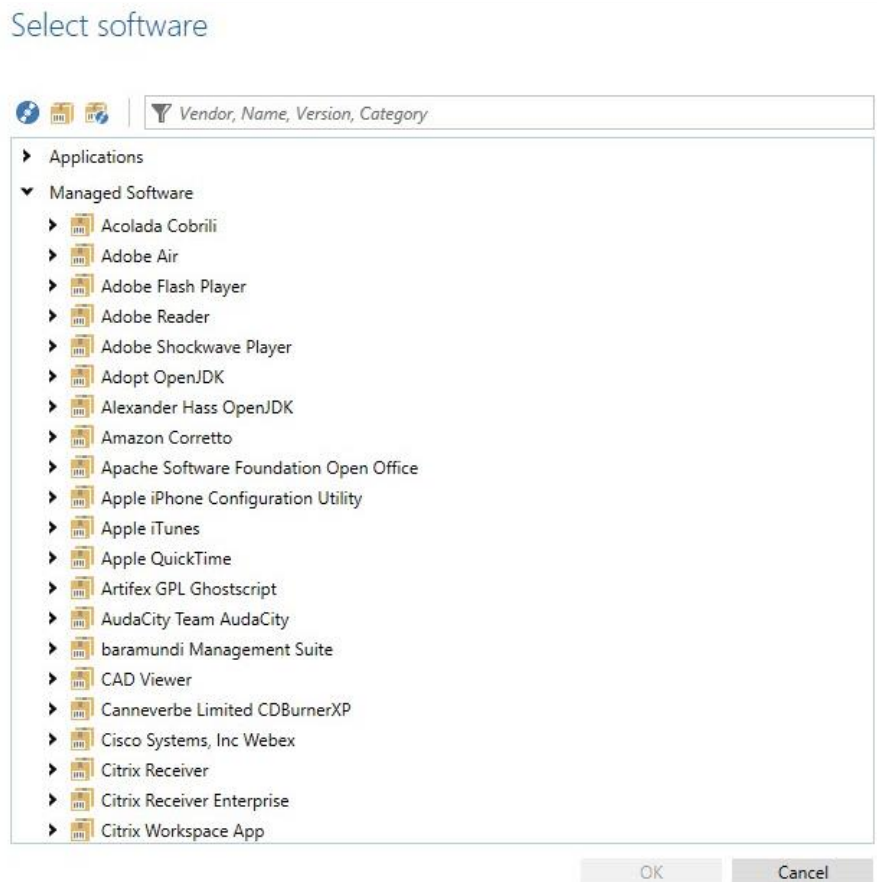


Figure 17 - Dialog for the selection of UDG criteria for installed software

There is a new dialog for selecting software for UDGs that gives IT admins the ability to define both very specific and very broad criteria. This enables the creation of dynamic groups, such as:

- All Windows endpoints on which specific software is installed or inventoried.
- Endpoints automatically assigned the "Enterprise Chrome Customization" job that have Google Chrome-x64 (or any underlying MSW version) installed.

### 1.4.1.2 Jobs

It is now also possible to check jobs assigned to endpoints in UDGs through the new "Job assignment" entry in the properties.

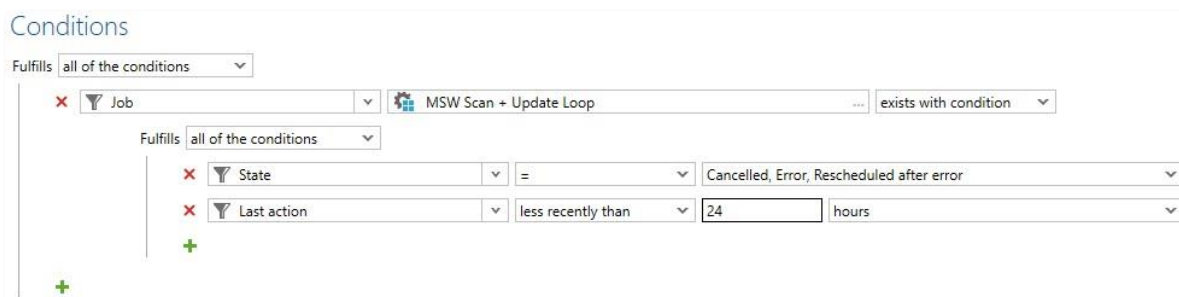


Figure 18 - UDG - New condition "Job assignment" with "exists with condition"

After clicking on the empty field, a dialog opens in which a specific job can be selected. If further conditions are configured for the job assignment, you can select whether all, some or none of those conditions should apply, just as you can with other UDG criteria.

There are three options for filtering:

- **exists:** checks whether endpoints have been assigned the selected job
- **does not exist:** checks whether endpoints have not been assigned the selected job
- **exists with condition:** checks whether the assignment exists and allows selection of additional properties of the job assignment:
  - **Rejections by user:** How often has the user rejected the job execution?
  - **Executions:** How often was the job performed?
  - **Successful executions:** How often was the job successfully executed?
  - **Created:** When was the job assignment created?
  - **Incorrect execution:** How often was the execution of the job unsuccessful?
  - **Last action:** When was the last change to the job assignment?
  - **Next start:** When has the next start of the job been scheduled?
  - **Start time:** When was the job started?
  - **Retries after error:** How often was an attempt made to run the job again after

- an error?
- **State:** What is the state of the job assignment? (which allows you to choose several states).
- **Status message:** is specific text included in the status description?

## 1.4.2 Extension of bConnect

### 1.4.2.1 Controller extensions

#### 1.4.2.1.1 Assets

Our bConnect interface has an expanded range of functions. Previously, assets in the baramundi environment were only accessible via our old (deprecated) interfaces. With 2024 R1, assets can now be queried via bConnect via the new assets controller, which is accessible with the familiar convenience of the Swagger UI.

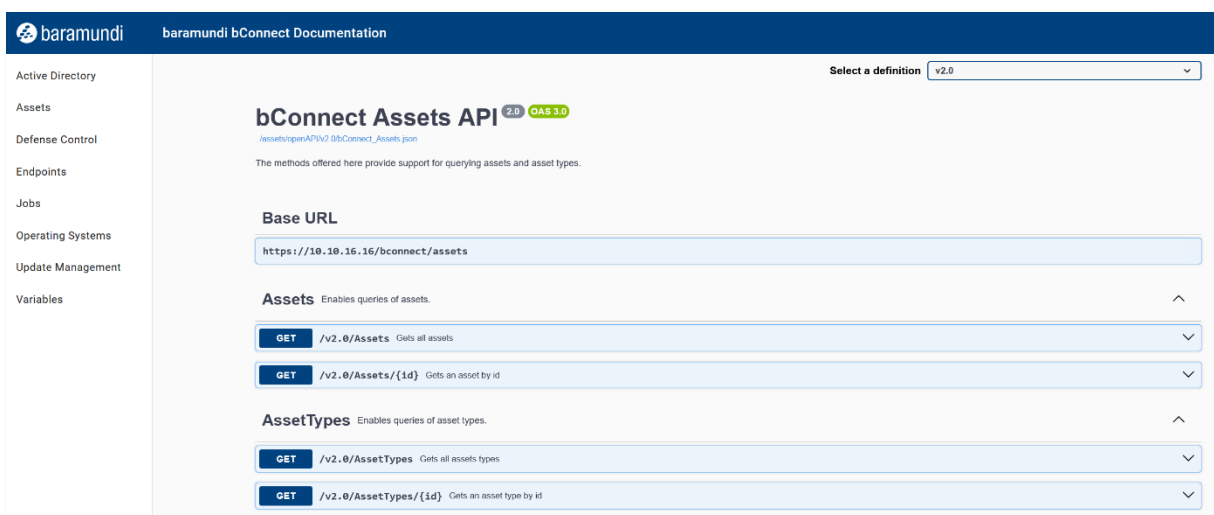


Illustration 15 - Querying the assets via bConnect

The user can either retrieve, create, edit or delete all assets or an asset based on its GUID. This changeover is also another step towards making the old interfaces obsolete. We recommend that you continue migrating all active scripts and programs that are still based on httpMOC or bMOL to bConnect.

### 1.4.2.1.2 System language

In order to accommodate the process of adding new endpoints in international environments, the existing controller has been extended to include the system language of Windows endpoints. It can be set in the OperationSystems properties in bConnect V2.

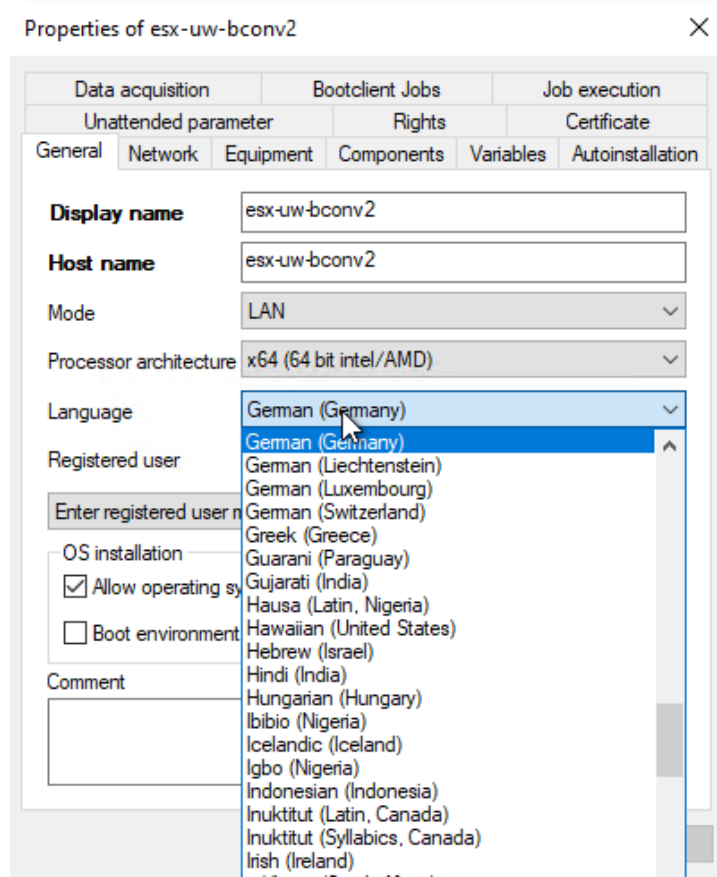


Illustration 16 - Windows endpoint language selection of the BMC

### 1.4.3 User-defined SSH inventory

With increased device diversity, a growing number of endpoints can only be reached via SSH because of their operating system or for security reasons. New Linux-based appliances or devices on which no changes (agent installation) may take place also fall into this category.

We have expanded our inventory method precisely for these device types. It is now possible to create templates and customize the standard commands, parameters and attributes previously provided by baramundi.

These new templates for SSH inventory can now be found under the inventory templates. For example, new SSH inventory templates can be created for similar device classes.



In contrast to the default template, existing commands can be customized in user-created templates and user-defined commands can be easily added to create more detailed queries. The use of several templates adds convenience as they can be adapted precisely to the respective device class.

The templates can be selected below the job step.

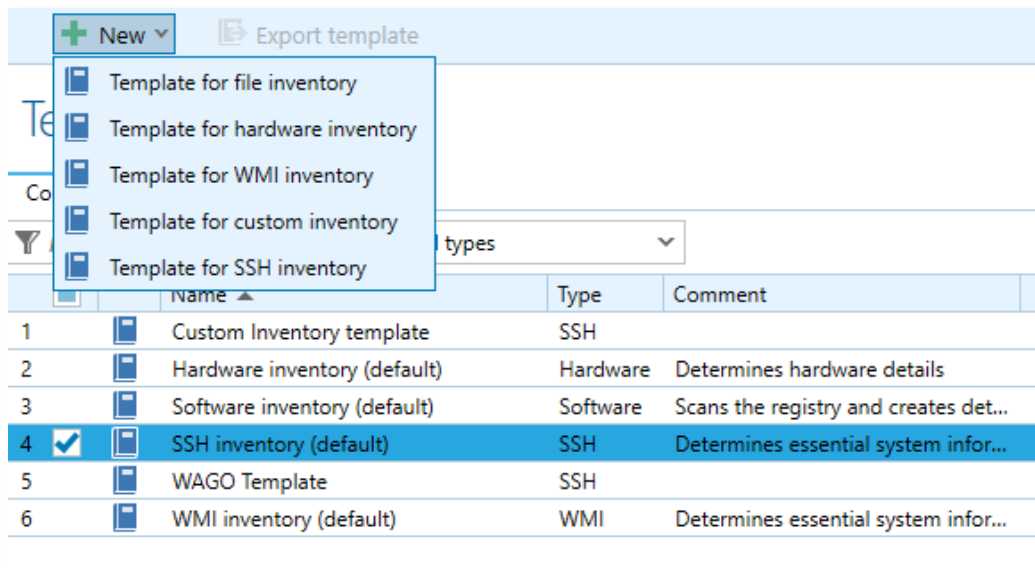


Illustration 17 - New template - SSH inventory

The individual inventory commands correspond to a type of user-defined variable. This means that each value can be stored as a property with the underlying command. See screenshot:

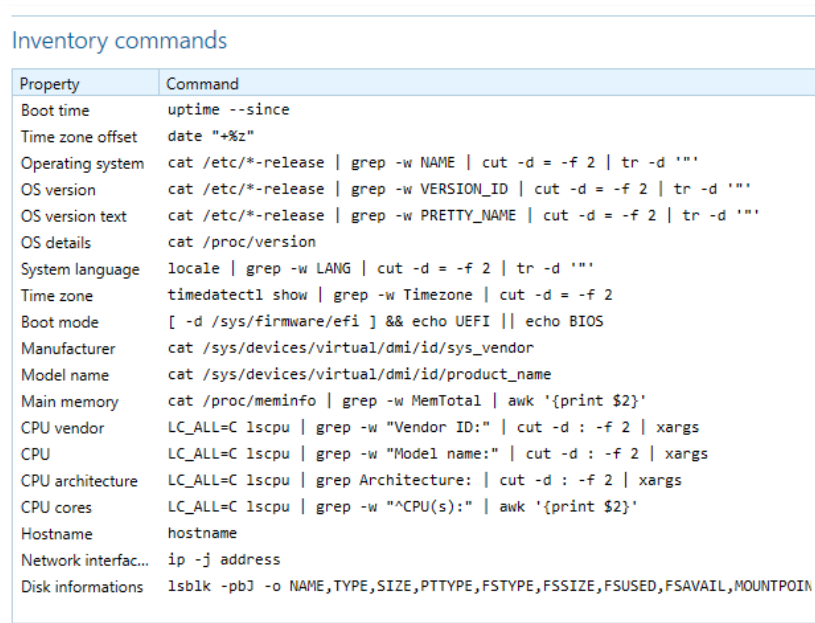


Illustration 18 - SSH inventory template with commands

These commands can be edited simply by double-clicking, just like the user-defined commands that have been available for some time.

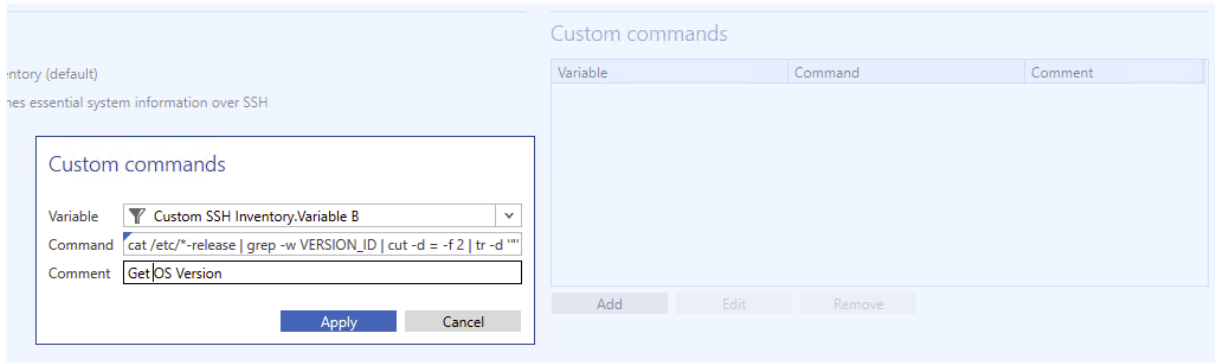


Illustration 19 - Dialog for adding new SSH commands

#### 1.4.4 Automatic job delay for active full-screen/presentation applications

To avoid user disruptions during presentations and other scenarios, 2024 R1 puts the baramundi Tray Notifier to sleep when Windows is set to Do Not Disturb and the endpoint display is in full-screen mode. The tray notifier returns after exiting full-screen mode.

This uses a Windows function that not recognizes presentations, screensavers and other full-screen or Direct3D applications.

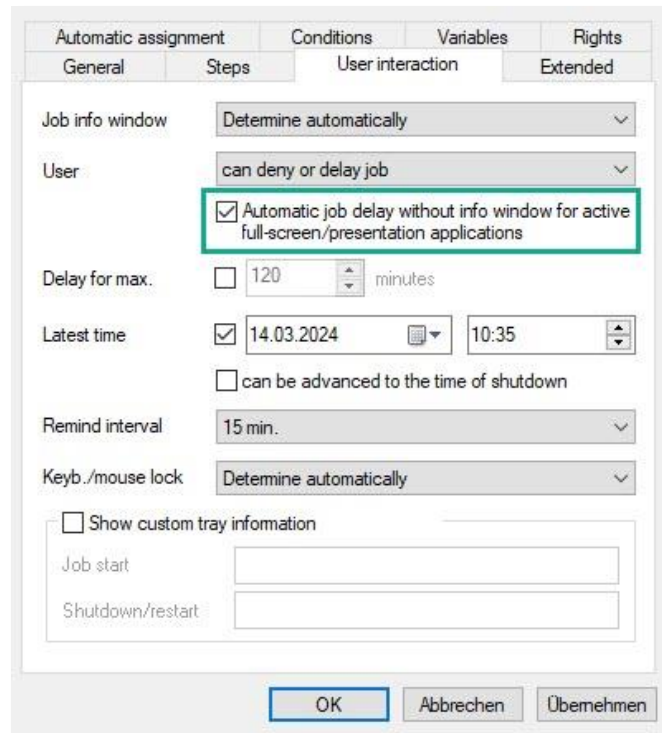


Illustration 20 - Configuration options in the job

The new option is activated by default for a new job where users are allowed to postpone job execution. However, if the maximum job deferral time has been reached the job info window is still displayed above the full screen.

### 1.4.5 Identification of endpoints based on UUID

The Universal Unique Identifier - UUID for short - is stored in the computer firmware (UEFI) and enables the system to be accurately identified. It's essential in endpoint management to unambiguously identify the targets for management actions to avoid, for example, accidentally resetting the wrong endpoint.

If the baramundi Management Agent (bMA) is installed, the bMS uses a client-side certificate to confirm the device identity. When the bMA has not yet been installed, the MAC address of the network card is used for the network boot. However, many new devices lack a built-in network port to minimize size. That requires the use of dongles or docking stations with network adapters, making it difficult to clearly identify the MAC address.

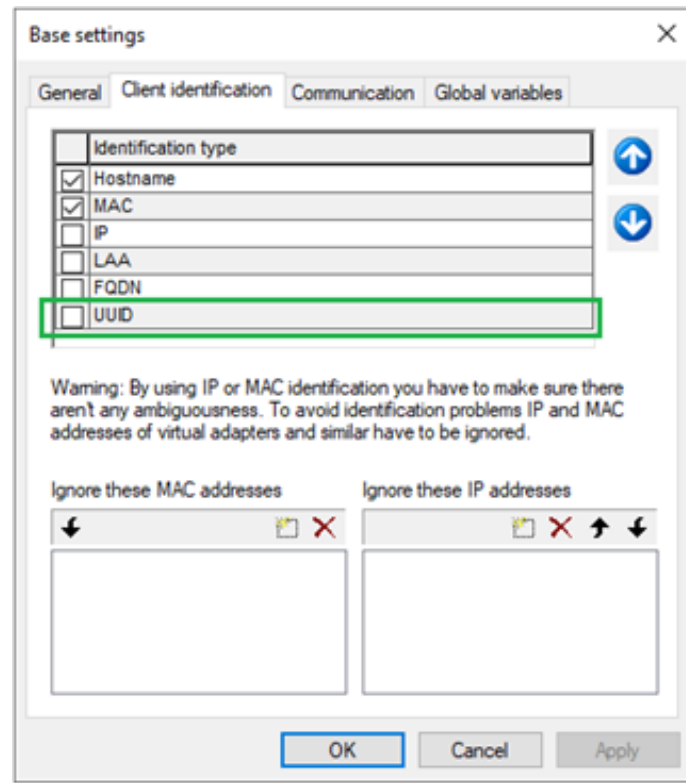


Illustration 21 - Client identification with new field for UUID

The bMS now supports the UUID as the primary identification feature. The UUID is automatically set as an identification feature for newly created databases. For existing databases, the UUID is available as a feature in 2024 R1 that users can activate.

**Note:** In environments that had UUID activated as Technical Preview with bMS 2023 R2, the UUID must be reconfigured as the primary identification feature; the settings from the Technical Preview are not migrated.

## 1.5 System requirements and compatibility

### 1.5.1 baramundi Management Server and baramundi PXE Relay

- Supported platforms: see 1.5.17 (column bMS)
- .NET Core 6.x, ASP.NET Core Framework 6.x and .NET Core Desktop 6.x in the same versions are required.
- Supported languages: German and English
- It is recommended to use a dedicated server for operating the baramundi Management Server.
- Certain ports must be available for the baramundi Management Server<sup>3</sup>.
- Integration into a Windows domain - Windows Active Directory - is recommended.
- Hardware requirements server/network:
  - Available RAM: at least 8 GB; 16 GB recommended
  - Processor: at least 4 cores
  - Storage space for installing the bMS: at least 5 GB
  - Network card: at least 1 Gigabit

### 1.5.2 Database connection

- Supported platforms:
  - SQL Server 2022
  - SQL Server 2019
  - SQL Server 2017
  - SQL Server 2016 SP3 (deprecated)
  - Oracle 19c (deprecated)

**Note:** bMS versions from 2025 R2 will no longer be compatible with Oracle databases. Switching to MS SQL or our cloud solution (bMSaaS) is recommended.
- at least 10 GB hard disk space for the baramundi database
- The baramundi Management Server is a database-oriented system. Sufficient database performance and a high-performance connection must be ensured.
- The SQL Express Edition can be used for environments with up to 250 clients.

---

<sup>3</sup> A list of the ports used on the server is available in our online help <https://docs.baramundi.com> under Documentation > Suite Handling > Extras > Port assignment.

- Operation of the database server and the baramundi Management Server on one system is permitted. For higher requirements and larger environments, an independent database server is recommended.

### 1.5.3 baramundi Management Center

- Supported platforms for the baramundi Management Center and the add-ons Automation Studio, License Management, Remote Control and ImageMount: see 1.5.17 (bMC column)
- Microsoft Edge WebView2 Runtime is required.
- Screen resolution:
  - Minimum screen resolution 1024 x 768 pixels
  - A resolution of 1280 x 800 pixels or higher is recommended.
  - All resolutions refer to a font size display of 100%.

### 1.5.4 baramundi OS Customization Tool

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

### 1.5.5 baramundi DIP

- Supported platforms: see 1.5.17 (bDIP column)
- .NET Core 6.x, ASP.NET Core Framework 6.x and .NET Core Desktop 6.x in the same versions are required.
- Additional hard disk space is recommended:
  - 10 GB for applications
  - 90 GB for Managed Software (MSW)
  - 8 GB for each operating system to be distributed with the baramundi OS Install module

### 1.5.6 baramundi Gateway

- Supported platforms: see 1.5.17 (column bGW)
- It is recommended not to operate the baramundi Gateway together with other services on the same system.
- Integration into 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 RAM: at least 4 GB; 8 GB recommended
  - Storage space for installing the baramundi Gateway: at least 1 GB
  - Network card: at least 1 Gigabit

### 1.5.7 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.

### 1.5.8 baramundi License Management

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

### 1.5.9 baramundi interfaces

- bConnect is available in versions 1.1 and 2.0.
- 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 from bMS version 2025 R1.
- Deprecated - The httpMOC interface is no longer being developed. We recommend switching to and using our bConnect interface.  
**Note:** The httpMOC interface will no longer be available from bMS version 2025 R1.
- Deprecated - Direct access to the database (SQL/Oracle) is not supported. We recommend switching to and using our bConnect interface. The DB documentation has not been supplied since 2023 R2.

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

### 1.5.10 baramundi Network Devices

- Supported platforms: see 1.5.17 (column bND)
- The Network Scanner is an add-on to Windows bMA. It is available to all customers via Managed Software .
- .NET 4.7.2 is required.

### 1.5.11 baramundi OT Devices

- Data is recorded via SNMP Version1, Version2c, Version3.
- Supported platforms: Siemens SIMATIC S7 1200 and 1500

### 1.5.12 baramundi Kiosk

- Supported platforms: see 1.5.17 (column bMA)
- A Windows Active Directory including a configured baramundi AD Sync is required for user login and job assignment on a user basis.
- baramundi Kiosk supports the following browsers, each in the current version:
  - Microsoft Edge
  - Google Chrome
  - Mozilla Firefox

### 1.5.13 Support for Android

- Supported versions:
  - Android Enterprise 14
  - Android Enterprise 13
  - Android Enterprise 12
  - Android Enterprise 11
  - Android Enterprise 10
  - Android Enterprise 9
  - Android Enterprise 8 \*)
  - Android Enterprise 7 \*)

\*) Support is limited. New functions may not be available and existing functions may not work as before; no support for zero-touch.

### 1.5.14 Support for iOS

- Supported versions:
  - iOS version 17
  - iOS version 16
  - iOS version 15
  - iOS version 14
  - iOS version 13
  - iOS version 12

### 1.5.15 Linux support

- The standard template provided by baramundi for the SSH inventory supports the following distributions:
  - Debian: Version 11 and 12
  - OpenSuse: from version 15
  - Ubuntu Server: Version 21 and 22
- By customizing templates, the commands can be adapted accordingly by the user to achieve individual compatibility with other operating systems.

### 1.5.16 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)

## 1.5.17 Windows support

- bMS/R: baramundi Management Server, baramundi PXE Relay
- bMC: baramundi Management Console, including bRemote, ImageMount and License Management AddOn
- bAS baramundi Automation Studio
- bGW: baramundi Gateway
- bDIP: baramundi DIP, bBT and DipSync service
- bMA: baramundi Agent for Windows
- bND: baramundi Network Scanner as an add-on for Windows bMA
- X: fully supported

Platform identifier	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows Server 2022 Standard/Datacenter (desktop view)	X	X	X	X	X	X	X
Windows Server 2022 Standard/Datacenter (Core)						X	
Windows Server 2019 Standard/Datacenter (desktop view)	X	X	X	X	X	X	X
Windows Server 2019 Standard/Datacenter (Core)						X	
Windows Server 2016 Standard/Datacenter (desktop view)	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 and 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 LTSC (32 bit and 64 bit)		X	X		x64	X	X
Windows 10 Enterprise 2015 LTSC (32 bit and 64 bit)		X	X		x64	X	X

## 1.5.18 Windows support with restrictions

The following operating systems are only supported by baramundi components to a limited extent. This may mean that new functions cannot be used or that existing functions may no longer work as before. Due to the complexity and large number of legacy systems, baramundi cannot guarantee functionality on these systems. We recommend the use of more modern operating systems. We can no longer provide support for baramundi server components (bMS/R, bMC, bAS, bGW, bDIP) on operating systems that are outside of Microsoft's mainstream support .

- (1): is only supported to a limited extent, as Microsoft has ended (basic) product support
- (2): A current bMA cannot be executed on Windows XP. These instructions must be observed when using, see 1.7.15 Windows Agent (bMA) note on Windows XP
- (3) No more support as of bMS 2024 R2

	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows Server 2012 R2 Standard/Datacenter (Server with graphical user interface)						1	1
Windows Server 2012 Standard/Datacenter (Server with graphical user interface)						1	1
Windows Server 2008 R2 SP1 Standard/Enterprise/Datacenter						3	3
Windows Server 2008 SP2 Standard/Enterprise/Datacenter (32 Bit/64 Bit)						1	1
Windows 10 Pro/Enterprise 1703 to 21H1 (N) (32 bit and 64 bit)						1	1
Windows 8.1 Pro/Enterprise (32 bit/64 bit)						1	1
Windows 7 SP1 Professional/Enterprise/Ultimate (N) (32 bit and 64 bit)						1	1
Windows Vista SP2 (32 Bit/64 Bit)						1	1
Windows XP SP3 (32 bit)						2	

## 1.5.19 Languages

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

German, English

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

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

The baramundi Kiosk supports the following languages:

German, English, Polish

Further languages can be added by IT administrators.

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

German, English

## 1.6 Product improvements in detail

### 1.6.1 Removed discontinuations / removed properties

- 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` is discontinued as of April 2024.
- Windows Vista and Windows Server 2008 SP2 are no longer supported.
- MS-SQL Server 2014 is no longer supported.
- Android version 4.0.4. up to version 9 is no longer supported.
- Samsung KNOX on Android version 4.0.4 up to version 9 is no longer supported.

### 1.6.2 General, when creating a new baramundi database

- The default server settings for new databases are now:

<code>Client identification</code>	<code>Host name, UUID, MAC</code>
<code>IP validity period</code>	<code>192</code>
<code>Connection mode</code>	<code>IP address if available</code>
<code>ICMP</code>	<code>yes</code>
- Under `Settings-Job execution`, the maximum number of simultaneously active clients is now 250.
- When creating new baramundi databases, it is now possible to set the currency used for energy management.
- No `DIP` is now written in the `logical group`.

### 1.6.3 Windows Agent (bMA)

- The password length for the automatically generated password for the local installation user (`baralnstLocal`) has been increased from 14 to 64 characters.
- Bugfix: In rare cases, the info window of the baramundi Traynotifier remains permanently visible after unlocking the keyboard and mouse and may block a logout.

## 1.6.4 Management Center (bMC)

- Under `Configuration - Variables`, the new field `Usage` shows how this variable can be referenced. Copying is also possible here.
- The menu for the PXE configuration has been changed to `bMC - Configuration - Server - PXE support`. There, the client identification can now be changed from MAC to UUID. See note [1.7.13](#).
- Under `bMC - Configuration - Server - Settings - Basic settings`, UUID is now also possible for client identification.
- Under `bMC - Job - Properties - User interaction`, the option `Automatic job delay without info window for active full screen/presentation applications` is now available. This means that no job info window appears on the client if, for example, a PowerPoint presentation has been recognized. If the presentation is ended, the info window appears after a few minutes.
- Under `bMC - Configuration - Server - Settings - Job execution`, the option `Clean up job targets with invalid status at module start` has been removed.
- The condition `Software` is now available in a `Dynamic Group (Universal)` and thus enables detailed queries on `installed (exists)` or `missing (does not exist)` applications.
- In a `Dynamic Group (Universal)`, the `Job` condition is now available and thus enables queries on `successful/unsuccesful job executions` including the specification of times.
- If a new application is created, only the client operating systems `Windows 10/11` and the server operating systems from 2016 are selected by default as `Supported operating systems`.
- If a new application is created, the option `bBT supported` is now active by default.
- The sub-nodes under `bMC - Configuration` are now collapsed.
- Bugfix: A `Dynamic Group (Universal)` cannot be saved if variables of type `Date` are used in a condition. An exception "Could not cast..." appears.
- Bugfix: Under `Client - Inventory - Inventories` the action `Back to overview` does not work. It has been removed.



- Bugfix: The action `Client - Management Agent - Activate Dynamic Mode` fails if the BMC user has no rights for `Configuration - Server - Settings`.
- Bugfix: If the folder specified under `Personal settings - Default job folder` is deleted, an error message "The node with the ID was not found" appears when using the `Create installation job` action, for example.

### 1.6.5 bRemote

- To use bRemote to connect to Windows PE, the `Connect to PE` command is now available in the `Client Custom menu`.
- Note: Support for Windows XP has been removed.

### 1.6.6 Remote Desk (AnyDesk)

- The bMA setup contains the `AnyDesk*.exe` files, these are now installed quickly and without disturbing the user in the bMA folder when the first connection is made with Remote Desk.
- The BMC Setup contains the `AnyDesk*.exe` files, these are now installed subsequently when using `Client - Remote access` for the first time. To perform this action, the BMC user requires administrative rights. With the setup parameter `ManagementCenter_setup.exe /qn ADDLOCAL=ALL AnyDesk*.exe` can be installed automatically.
- Bugfix: If special characters (e.g. from the Extended ASCII table) are used under `bMC personal settings - display name`, this user cannot perform remote maintenance. If a connection is triggered, no message is displayed for the user of the terminal device. The connection is terminated after some time on the BMC side with the error "Connection error".
- Bugfix: When using `client Remote access`, an error message "Value can not be null" appears if the BMC user has not stored a profile picture. Only occurs when using an Oracle database.

### 1.6.7 Defense Control

- The feature "Local administrative user accounts" can be configured under `bmc - Defense Control - Local administrative user accounts`.

- In the bMC, the automatically generated password can be managed on the client under `Endpoint security - Local administrative account`. Provided the bMC user has the new right `Special - Local administrative account` for this client and the feature is activated globally.
- Bugfix: In rare cases, the `bMC - Client - Microsoft Defender Antivirus - Threats` view displays an error message "Not all required server modules are running", although all server modules are running correctly.

### 1.6.8 Update Management

- Bugfix: In some cases, a `Personal notification` stored in the job is not sent in the event of an error in a job with Microsoft Update Management steps.
- Bugfix: The configured `Standard update profile` for new devices is not assigned to a new client if it is recorded via the client recording under PE.

### 1.6.9 OS install

- The baramundi server is now automatically stored as the FQDN in the `Boot Media Wizard`.
- When creating a new operating system, `Recreate before installation` is now preset for `Computer account`.
- A job created via the bMC action `Client - Extra - Reinstall` now contains the action `Finally restart client at the OS step`.
- The size of the WindowsRecovery (WinRE) partition is now 1024 MB.
- Bugfix: If a client is detected via the automatic MAC detection during PXE boot via a PXE relay, this client may only be visible in the bMC after restarting the `QueryService`.

### 1.6.10 baraDIP

- In order to support multi-domain authentication more conveniently with bBT, additional client domains can now be specified for bBT download under `bMC - Configuration - DIP - DIP management` on the individual DIP server.
- baraDIP no longer uses an Apache web server.

- Note: baraDIP now locks files while they are being transferred from DipSync or downloaded from Clients via bBT.
- Bugfix: If a proxy is entered under `bMC - Configuration - Server - Settings - Downloader - Use proxy`, the TLS configuration for DIP servers may not be possible.
- Bugfix: If faults occur during network communication on DIP servers, it has been observed that the baraDIP service may switch to a state where the service is still running but no longer synchronizing.

### 1.6.11 Mobile devices

- Apple's newly introduced "Rapid Security Responses" are available as `Patch Level`, and can be used under `Compliance - Mobile and macOS Devices - Rules`.
- WPA3 Personal/Enterprise is now supported for iOS/iPadOS from version 16.
- WPA3 Personal is now supported for Android Enterprise from version 11.
- WPA3 Enterprise is now supported for Android Enterprise from version 12.
- The EAP method `TTLS with PAP` is supported in WiFi profiles for iOS/iPadOS and Android Enterprise.
- For MDM profiles, the option `Prohibit installation of alternative marketplace apps` is available under `Restrictions - iOS/iPadOS - Use specific settings for device enrollment`. Usable from iOS 17.4.
- A template for setting the time zone is available for iOS under `Job - Execute command`.
- New profile restriction `Prohibit activation or access to debugging functions` available for Android Enterprise devices.
- The push to Android devices now works via the baramundi cloud service. Therefore, the configuration of the `Google Sender ID` and `server key` under `Configuration - Mobile Devices - General - Google Android` is no longer necessary and has been removed.

- Bugfix: If the number of licensed devices is reached when enrolling an iOS device, the enrollment fails when logging on to the baramundi bMD Agent and the device is removed from the administration.
- Bugfix: A BMC user without read rights on `Configuration - Mobile Devices - General` cannot see any apps on mobile devices under `Inventory - Installed Apps` and under `Software - Apps`.
- Bugfix: Jobs with the option `Assign to new devices` are not assigned to newly enrolled devices if they were enrolled via `Android Zero-Touch`.
- Bugfix: When adding an Android app via the google store, a message "At least one error has occurred" or the message "The value must not be NULL" appeared in rare cases.

### 1.6.12 Network devices

- A new template for identifying network devices SSH inventory (standard) is available under `Inventory - Templates`.
- You can create your own inventory template via `Inventory - Templates - New - Template for SSH inventory`. This makes it possible to adapt the default inventory commands or add your own.
- Bugfix: The Inventory via SSH job step is not available if a Network Device license is available but no OT Inventory license.

### 1.6.13 macOS

- WPA3 is now supported for macOS from version 13.
- The EAP method `TTLS with PAP` is supported in WiFi profiles on macOS.
- Bugfix: With macOS 14.0, the baramundi Agent icon is not displayed in the menu bar. Note: Reassigning a job with step `Enroll SSH interface` fixes the missing icon in the menu bar.

### 1.6.14 bConnect

- It is now possible to create and delete asset types.  
Note: Only the `String` type is currently supported for `additionalProperties` of an `AssetType`.
- Creating, modifying and deleting assets is now possible.
- The value `Client - Properties - General - Language` can now also be changed via bConnect.

## 1.7 Notes and known Limitations

### 1.7.1 Discontinuations

- Windows Vista and Windows Server 2008 SP2 are no longer supported.
- The Windows Server 2008 R2 operating system is no longer supported from bMS version 2024 R2.
- The bMOL interface will no longer be available as of bMS version 2025 R1.
- The httpMOC interface will no longer be available as of bMS version 2025 R1.
- 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.

### 1.7.2 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.

### 1.7.3 Notes on the .NET Framework

- The required .NET x64 versions `AspNetCoreFramework 6.x` and `NETCoreDesktop 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.

### 1.7.4 OS Install

- Note on the bDX import of OS files with unattend files: It is recommended that the bDX import is carried out directly on the baramundi server in this case so that the unattend files can be stored correctly in the server directory under `..\Shared\Scripts\OS`.
- A job with step `Create master image of an operating system` may run into an error during the Sysprep process if it was assigned to a Windows 11 client.

### 1.7.5 baraDIP

- The bMS 2024 R1 does not work with older baraDIP versions. To avoid problems, the baraDIP services can be updated to a 2024 R1 version before updating the bMS
- Notes on the use of own certificates in baraDIP:
  - The baraDIP-Config-Tool can be used to configure your own PKI certificates for the baraDIP if required.
  - When updating to bMS 2024 R1, existing PKI certificate configurations are not migrated and must therefore be carried out manually.

### 1.7.6 Management Center (bMC)

- Under `bMC - Configuration - Domains`, only an "s" is displayed in the detail view instead of the text "Use local installation user".
- 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.
- The `List SNMP-Devices` report cannot be opened in environments with an Oracle database.

### 1.7.7 bRemote

- The connection to Windows PE with `client - user menu command Connect to PE` may result in an authentication error if the logged-in user was not used for the bMC login. This can be solved by storing the login data in the baramundi RemoteViewer.

### 1.7.8 Remote Desk (AnyDesk)

- Sporadically, an “AnyDesk crashed” message appears after starting the `bMC - Client - Remote access` action.

### 1.7.9 Mobile Devices

- Due to the changeover to push for Android devices, it may take up to 24 hours after the update to bMS 2024 R1 for the end devices to receive push messages again.
- In very rare cases, the enrollment of Android Enterprise devices fails with the error “javax.net.ssl.SSLHandshakeException: The expected fingerprint does not match the fingerprint received from the server”. This occurs if the automatic gateway certificate renewal has updated the certificate but the gateway has not yet been restarted manually.

### 1.7.10 Inventory via SSH for Linux devices

- Boot time is not recorded on Linux distribution OpenSuse.

### 1.7.11 Inventory

- 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.



### 1.7.12 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.

### 1.7.13 UUID

- Switching the `client-identification` from `MAC` to `UUID` is only recommended when a signed baramundi UEFI bootloader is available. Until then, we recommend leaving the setting on `MAC`.

### 1.7.14 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.

### 1.7.15 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 bRemote, OS-Install and automatic bMA deployment are no longer available. The bMA may have to be installed manually.
- Note: Windows XP can only be used with an outdated bMA, which is no longer maintained by baramundi and contains known security vulnerabilities. There are no new security updates available for the outdated bMA. The Customer is aware of this. baramundi provides no guarantee for the secure use of XP and the outdated bMA version. Use is at the Customer's own risk.

## 2 Release 2023 R2

### 2.1 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.

#### 2.1.1 Advantages of Partnership

##### 2.1.1.1 *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".

##### 2.1.1.2 *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.

### 2.1.1.3 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.

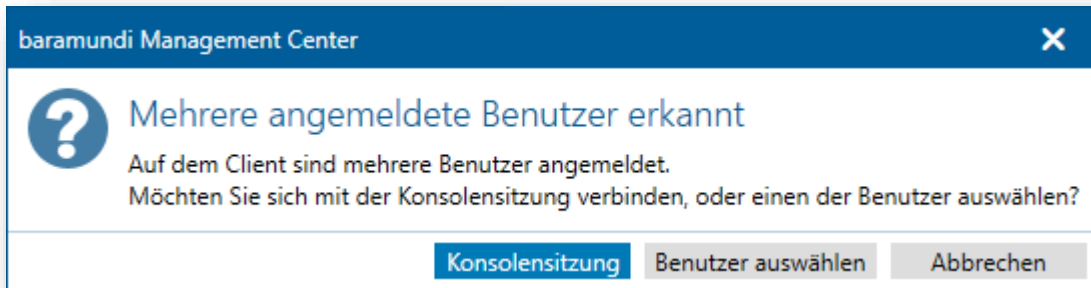


Figure 1 baramundi Remote Desk - Multiple User Sessions

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.

### 2.1.1.4 UAC Management

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

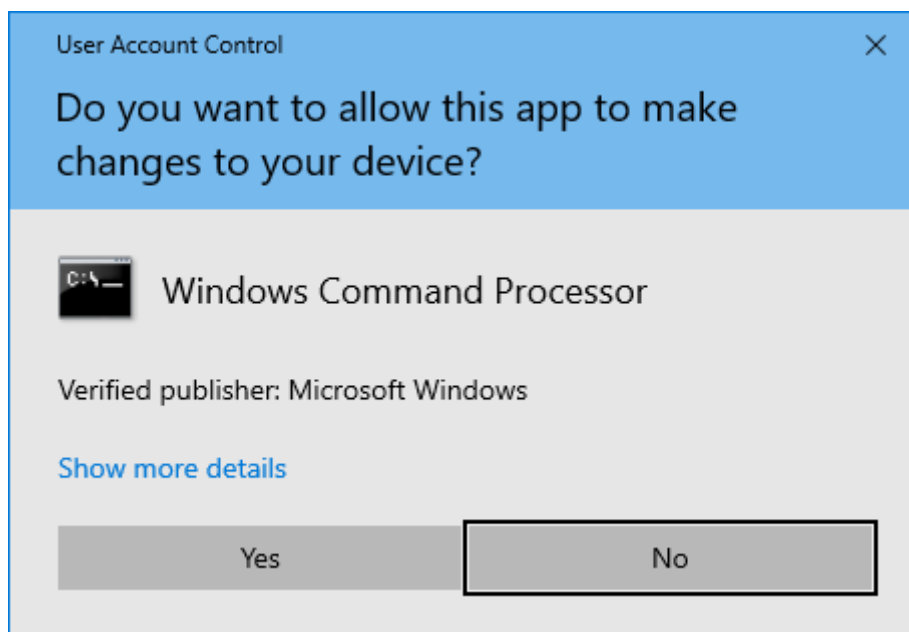


Figure 2 Windows User Account Control

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.

#### *2.1.1.5 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.

#### *2.1.1.6 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.

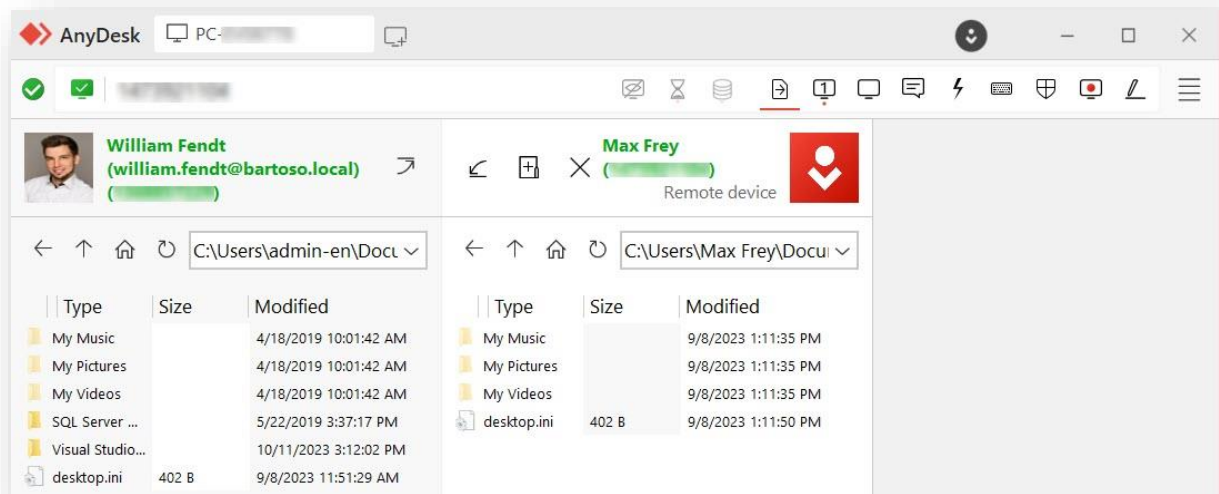


Figure 3 baramundi Remote Desk - File Manager

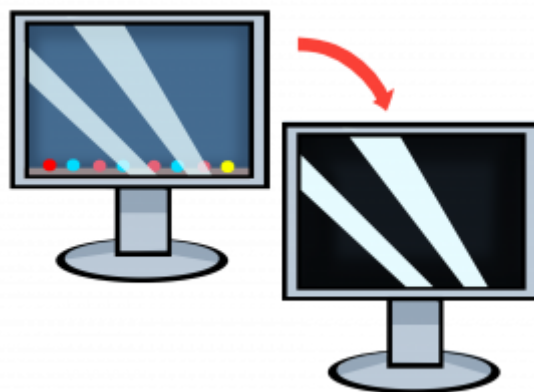
## File Transfer

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.

### 2.1.1.7 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.

### 2.1.1.8 Chat Function

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

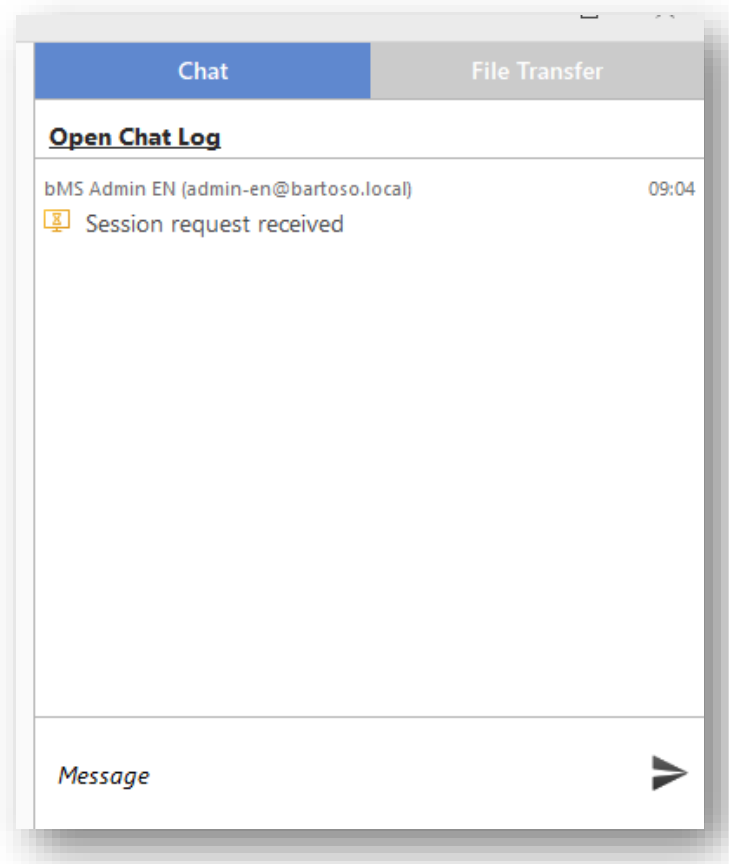


Figure 4 baramundi Remote Desk - Chat Client

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.

## 2.1.2 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.

### 2.1.2.1 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.

### 2.1.2.2 "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.

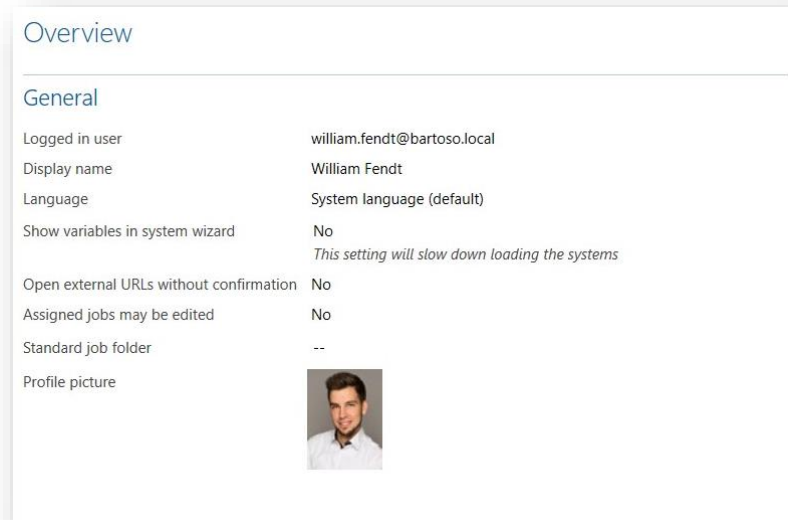


Figure 5 baramundi Remote Desk – Personal Settings

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



### *2.1.2.3 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 2.1.1.3) can be used. Logoff is automated when the session is terminated to avoid leaving it open accidentally.

### *2.1.2.4 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.

### *2.1.2.5 Whitelisting Through bMC and bMA*

By default, the baramundi Remote Desk (even if it had been started; see 2.1.2.4) 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.

## **2.2 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.

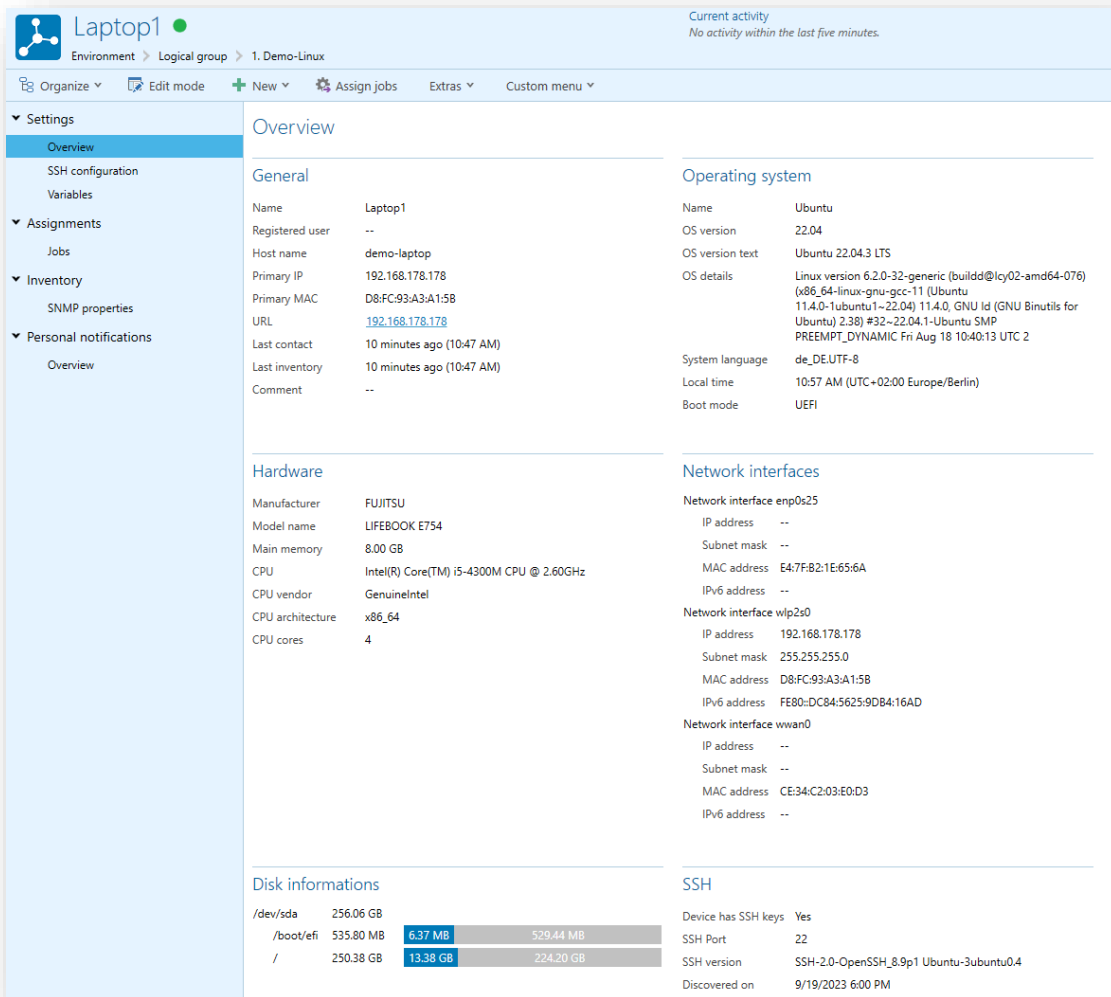


Figure 7 The Result of an Inventory Job of a Linux Device

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

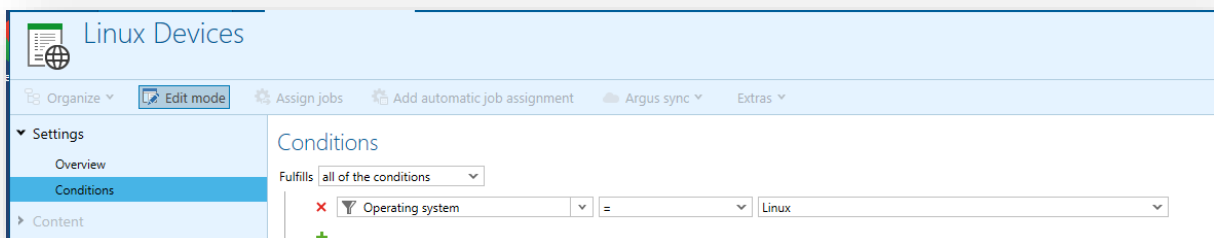


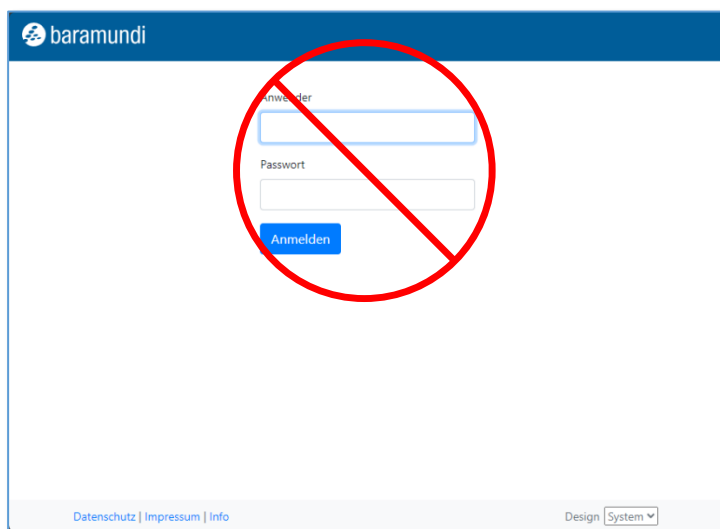
Figure 8 Creating a UDG for Linux endpoints

## 2.3 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.

## 2.4 Mobile Devices

### 2.4.1 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..

#### 2.4.1.1 *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.

#### 2.4.1.2

#### 2.4.1.3 *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.

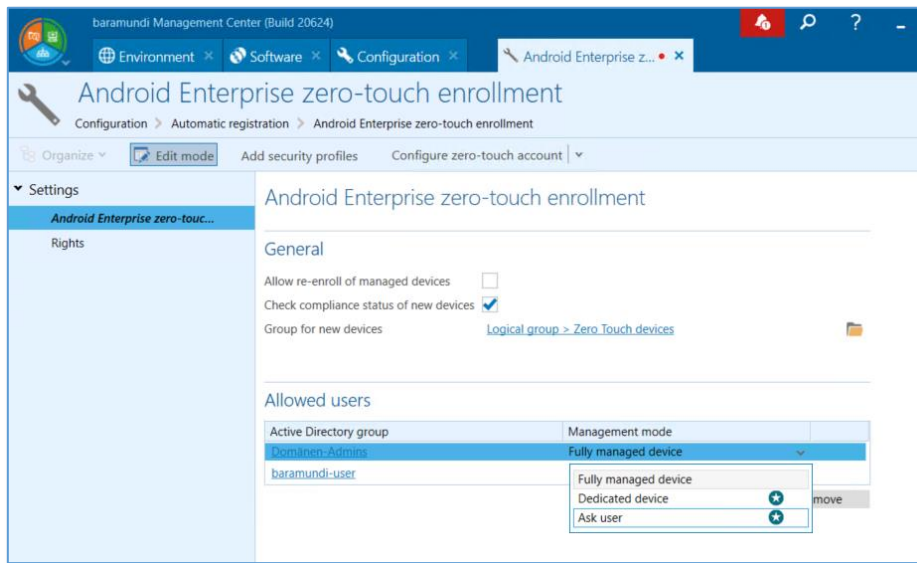


Figure 9 Configuration Page for Zero-Touch

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.

## 2.4.2 Further Improvements

### 2.4.2.1 Improve location accuracy

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

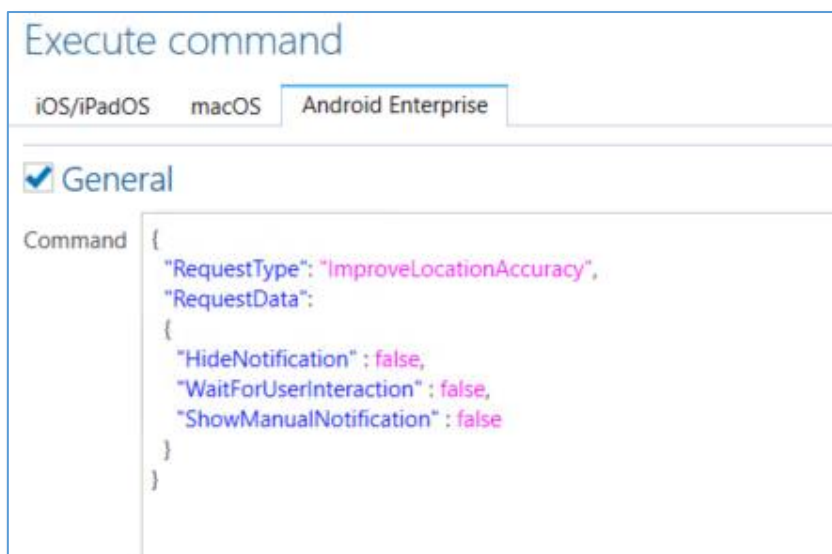


Figure 10 Configuration of the "Improve Location Accuracy" Command

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

### 2.4.2.2 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).

## 2.5 Universal Dynamic Groups

### 2.5.1 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.

### 2.5.2 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".

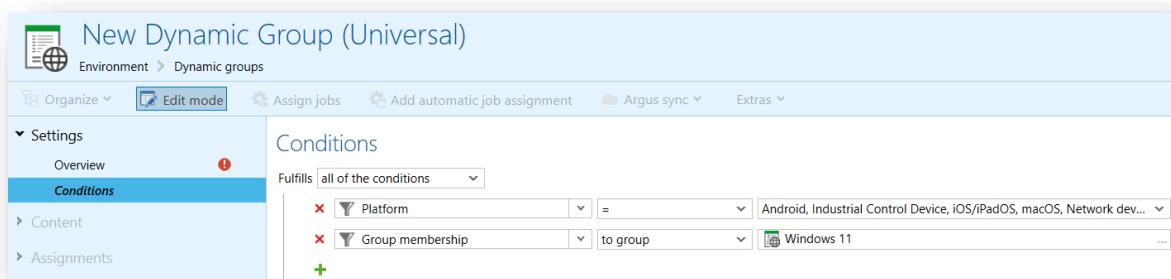


Figure 11 UDG Group Membership

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.

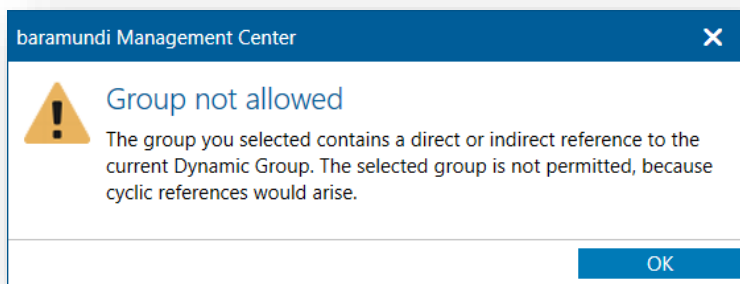


Figure 12 UDG Circular Reference Handling

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

### 2.5.3 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.

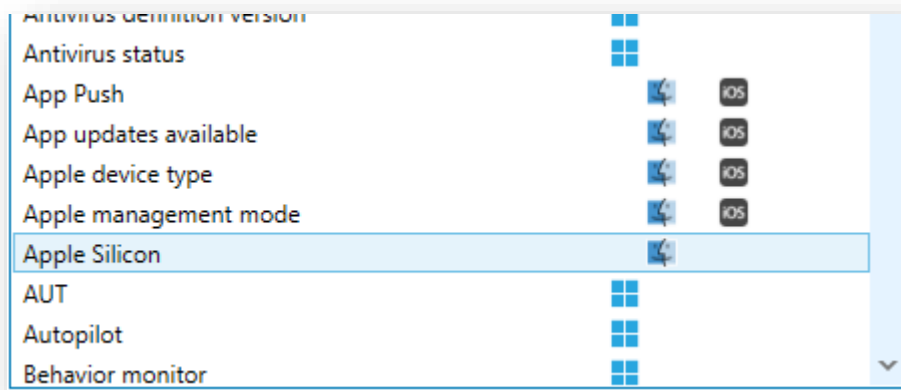


Figure 13 UDG Conditions

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

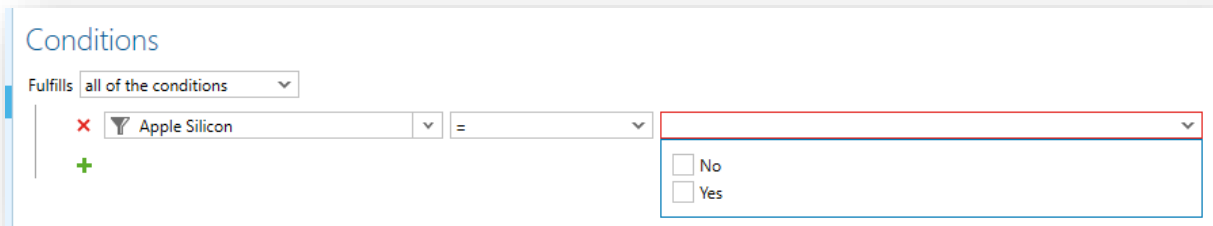


Figure 14 UDG Apple Silicon Filter Query

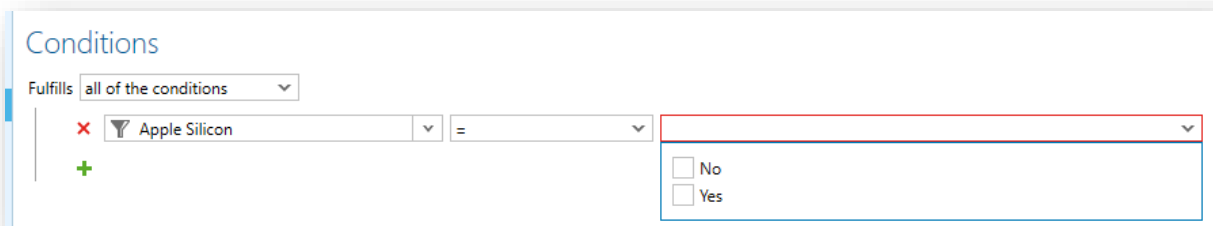


Figure 15 UDG Apple Silicon Filter Query

## 2.6 Network Devices

### 2.6.1 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".

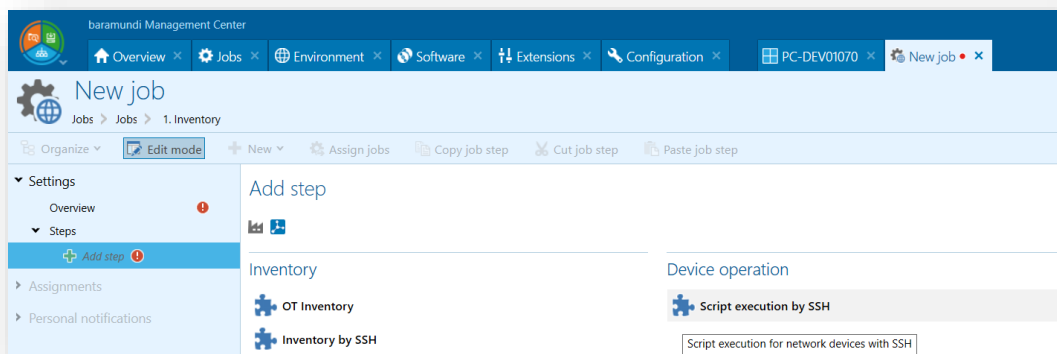


Figure 16 New Job Step



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

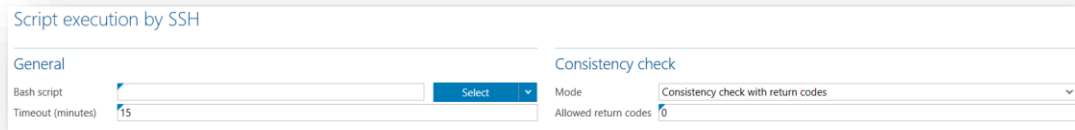


Figure 17 Script Execution via SSH

### 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
```

## 2.6.2 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.

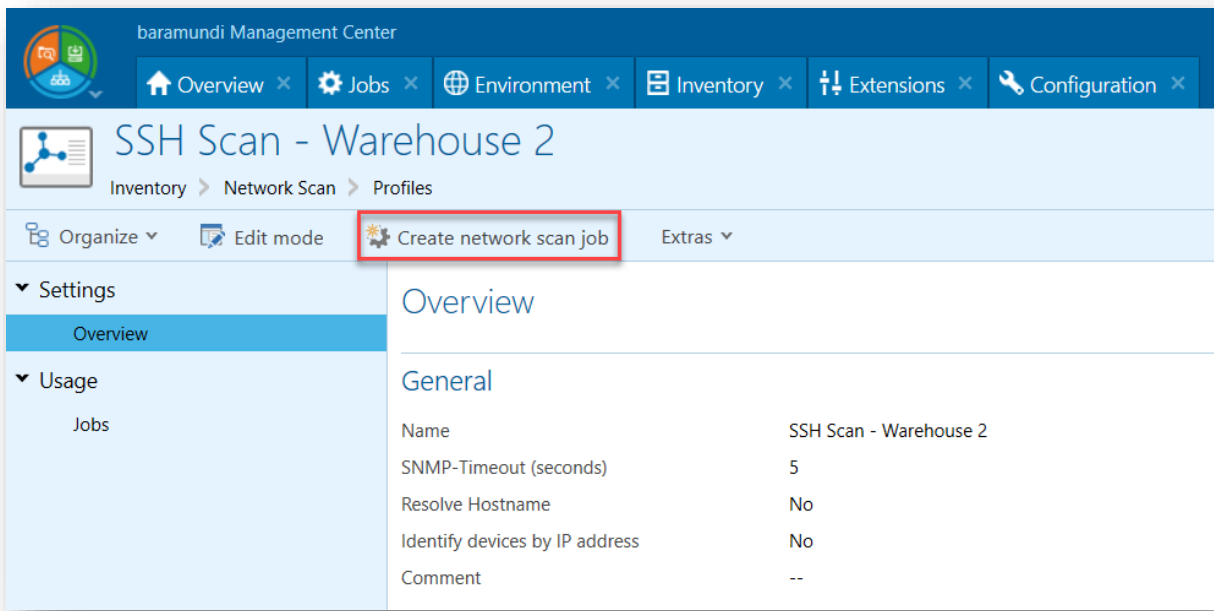


Figure 18 Network Scan Profile – Create New Job

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.

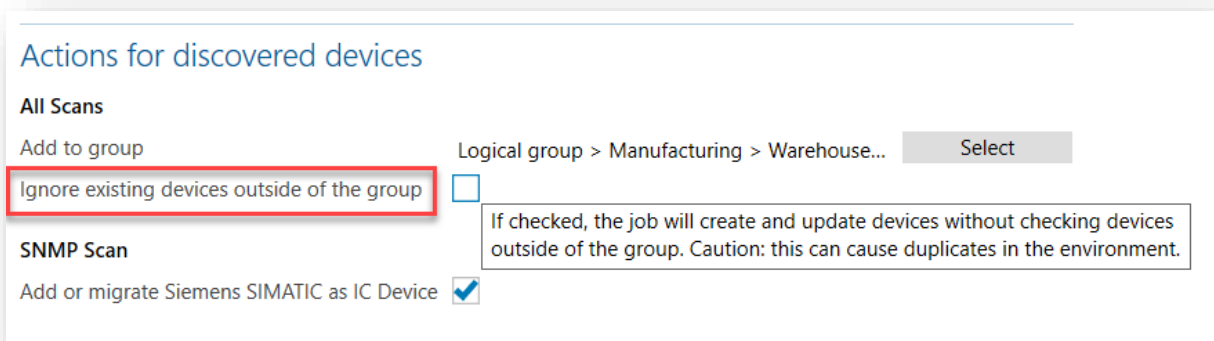


Figure 19 Network Scan Profile – Ignore Other Devices

## 2.7 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.

### 2.7.1 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.

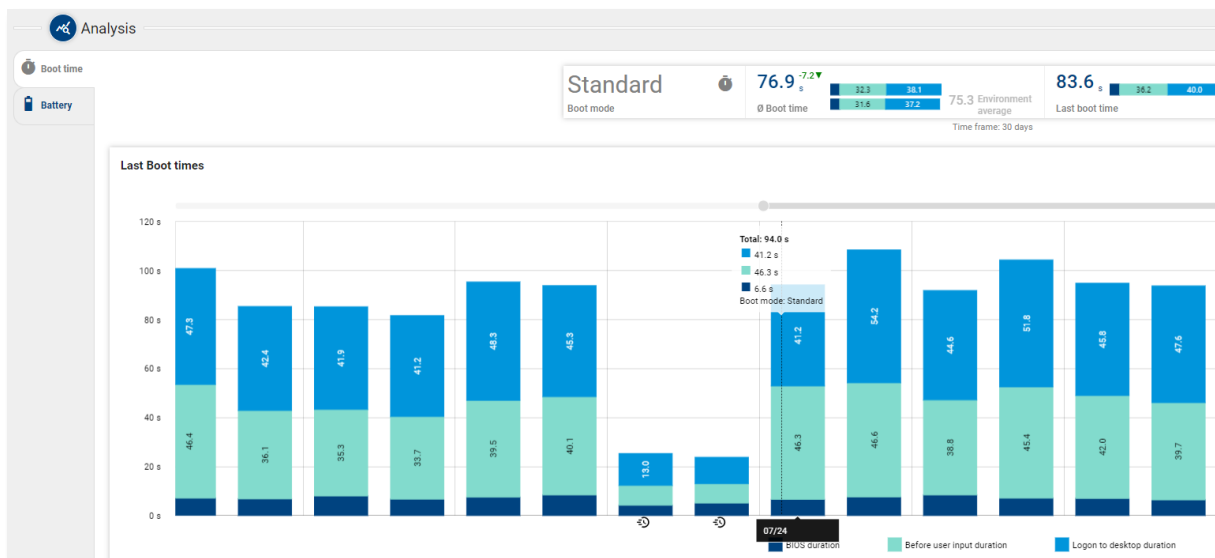


Figure 20 Detailed Start Times of An End Device

### 2.7.2 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.

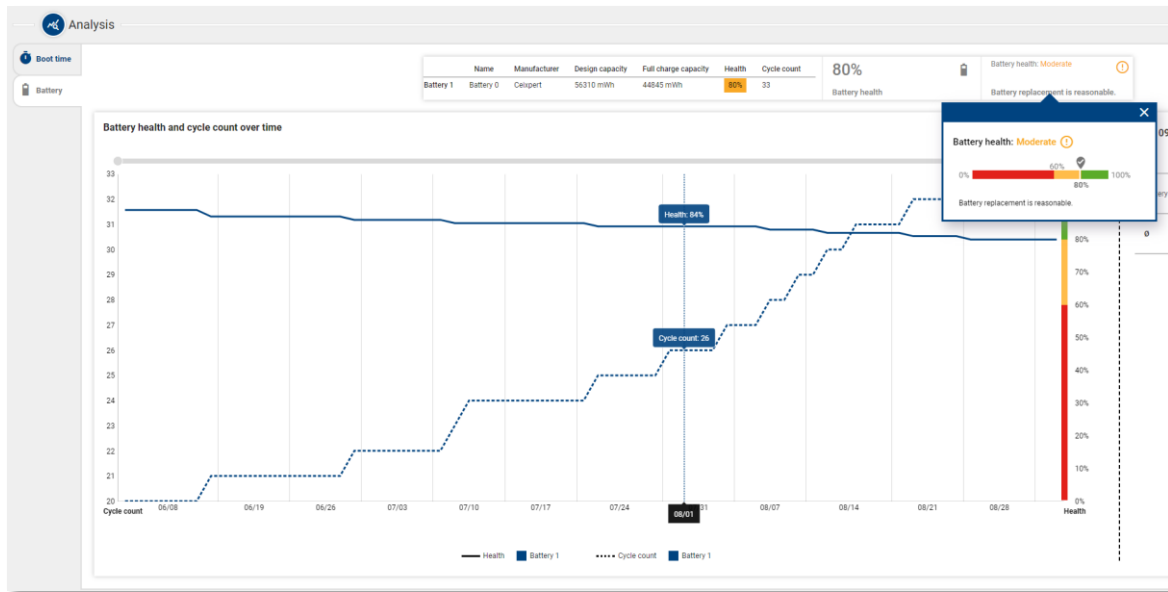


Figure 21 Declining Laptop Battery Capacities

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.

### 2.7.3 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.

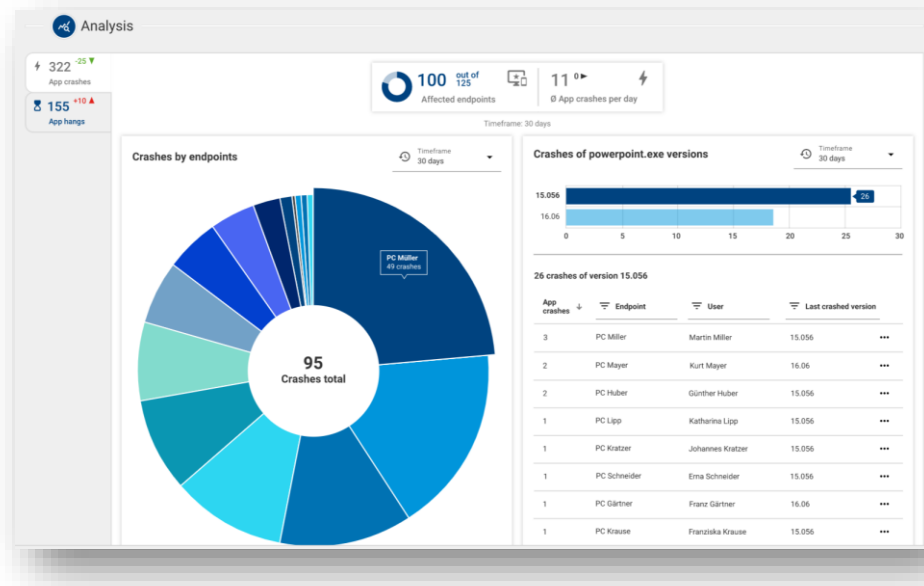


Figure 22 Detailed Display of Application Crashes

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.

### 2.7.4 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.

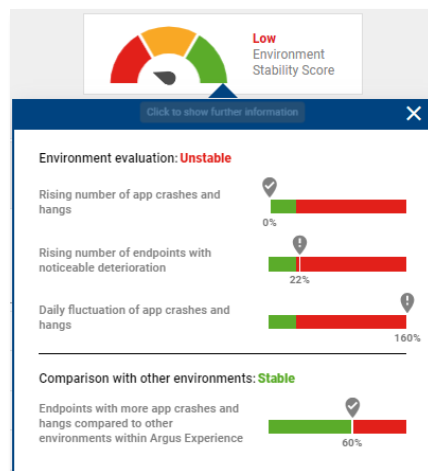


Figure 23 Benchmarking Environment Stability

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

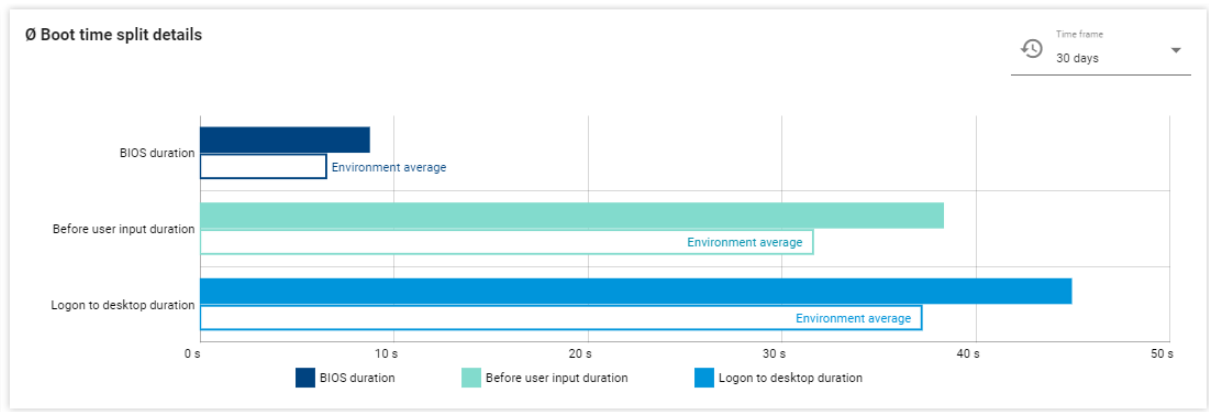


Figure 24 Overview of Endpoint Start Times Compared to the Environment Average

### 2.7.5 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.

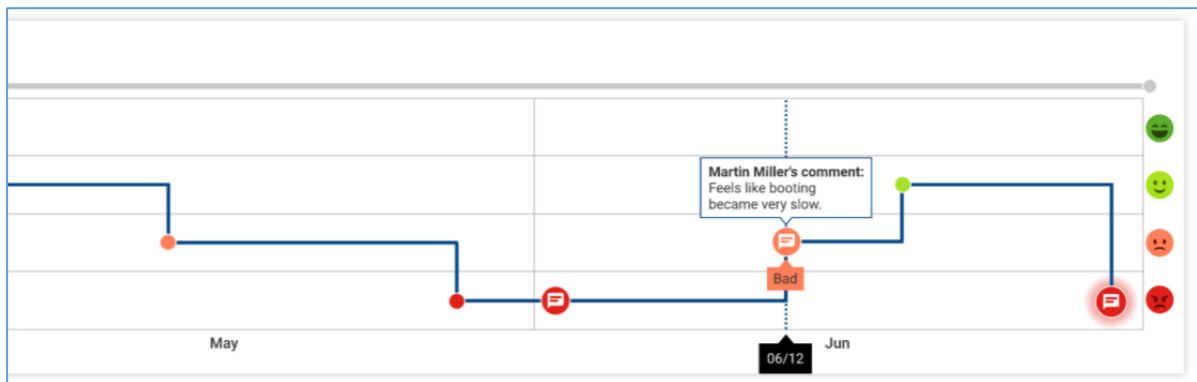


Figure 25 Employee Feedback on an Endpoint Device

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.

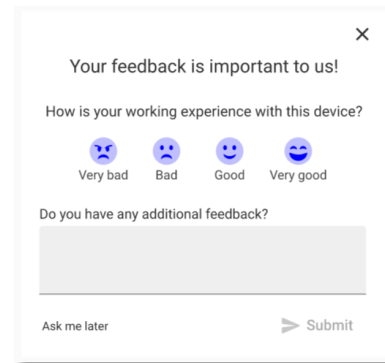


Figure 26 Tray Notifier for End User Feedback

## 2.8 Miscellaneous

### 2.8.1 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.

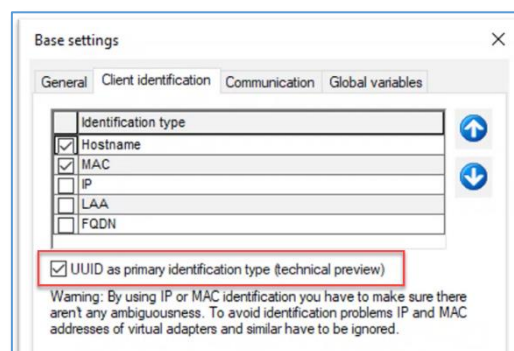


Figure 27 Activation of UUID-Support

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.





## 2.9 Product improvements in detail

### 2.9.1 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.

### 2.9.2 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/bpmda3_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`.

### 2.9.3 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.

## 2.9.4 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.

## 2.9.5 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.

## 2.9.6 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.

## 2.9.7 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 - Android 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 `Current-CarrierNetwork` 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).

### 2.9.8 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.

### 2.9.9 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.

### 2.9.10 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.

### 2.9.11 bConnect

- `networkEndpoints` are available.

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

### 2.9.12 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.

### 2.9.13 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".

### 2.9.14 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.



## 3 Release 2023 R1

### 3.1 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/>

## 3.2 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<sup>4</sup> bConnect 2.0 interface to improve overall API performance, flexibility and efficiency.

### 3.2.1 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>.

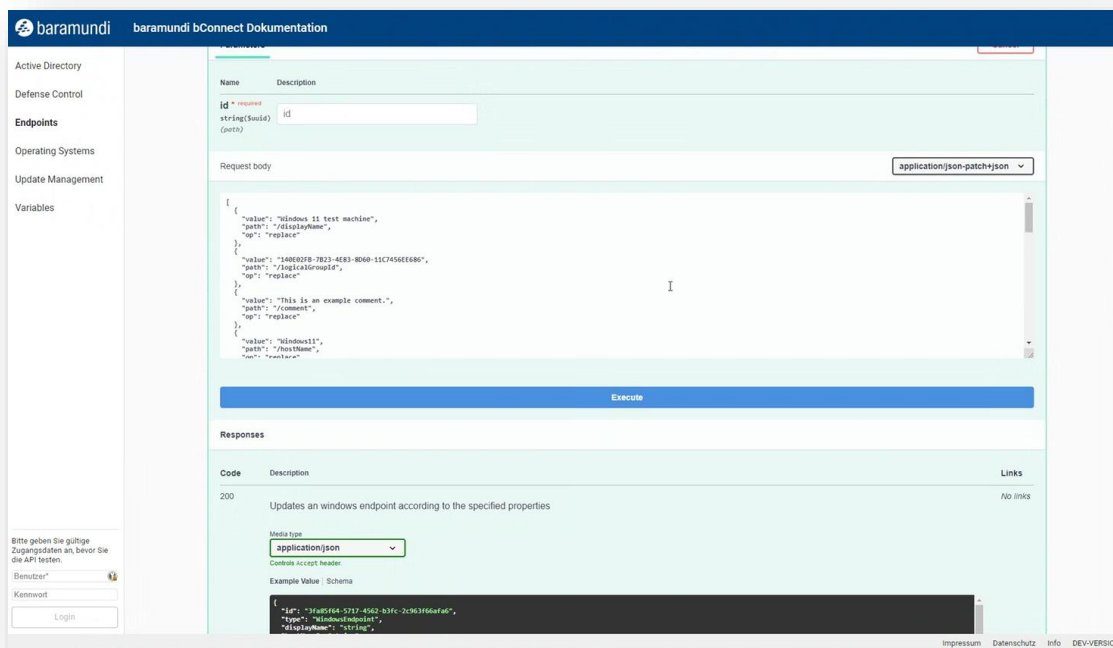


Figure 22 - bConnect 2.0 function details

### 3.2.2 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

<sup>4</sup> <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.

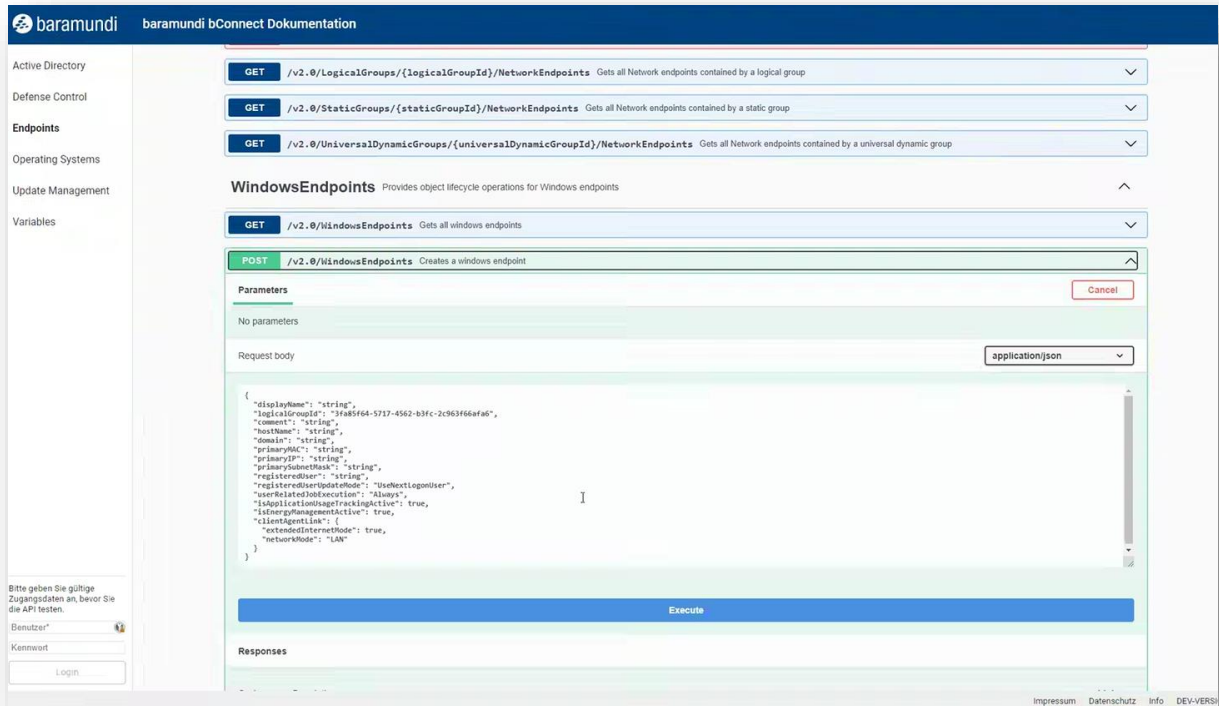


Figure 23 - bConnect 2.0 Controller - List of functions

### 3.2.3 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.

### 3.3 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.

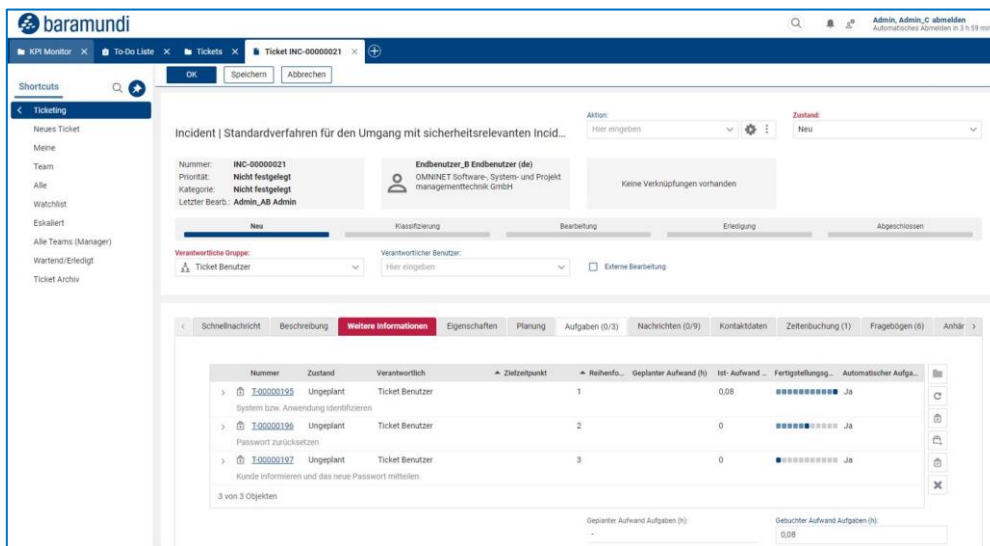


Figure 24 - bTS new design

### 3.3.1 New Design

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

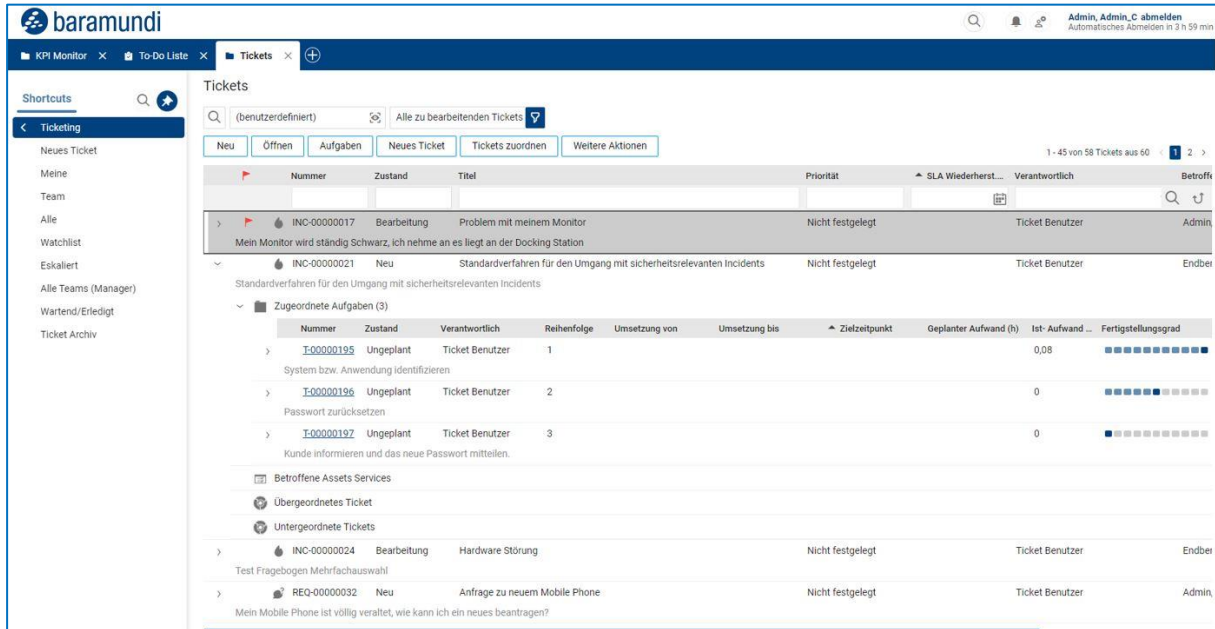


Figure 25 - bTS – Ticket list

### 3.3.2 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.

### 3.3.3 Improved Performance

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



### 3.3.4 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.

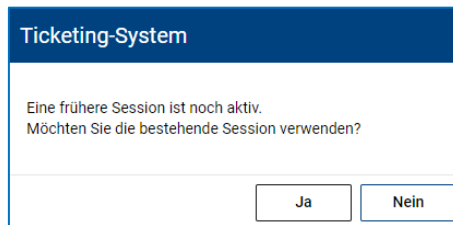


Figure 26 - bTS – Session login option

### 3.3.5 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.

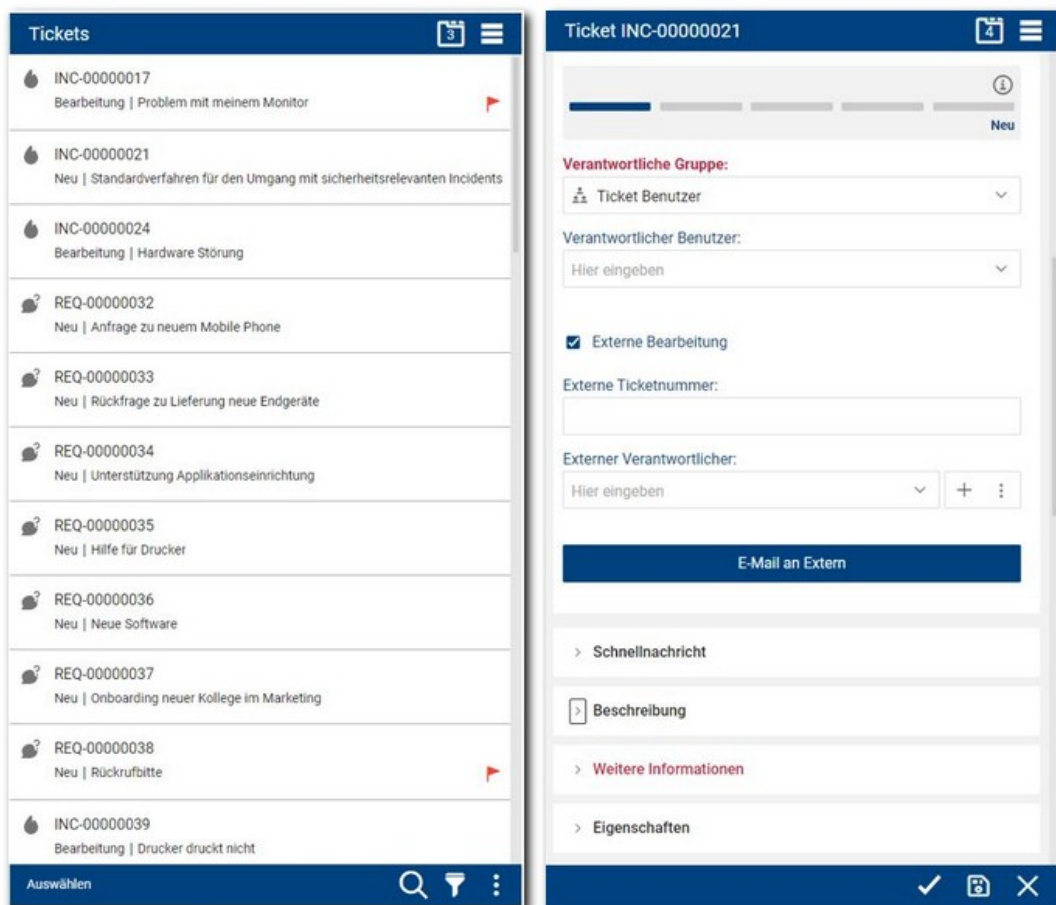


Figure 27 - bTS - mobile display

### **3.3.6 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.

### 3.4 baramundi Argus Cockpit and Argus Experience [Preview]

New features in Argus Cockpit and Argus Experience<sup>5</sup> give IT departments more options for endpoint monitoring and for identifying the causes of software hangs and crashes for faster and more accurate resolution.

#### 3.4.1 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.

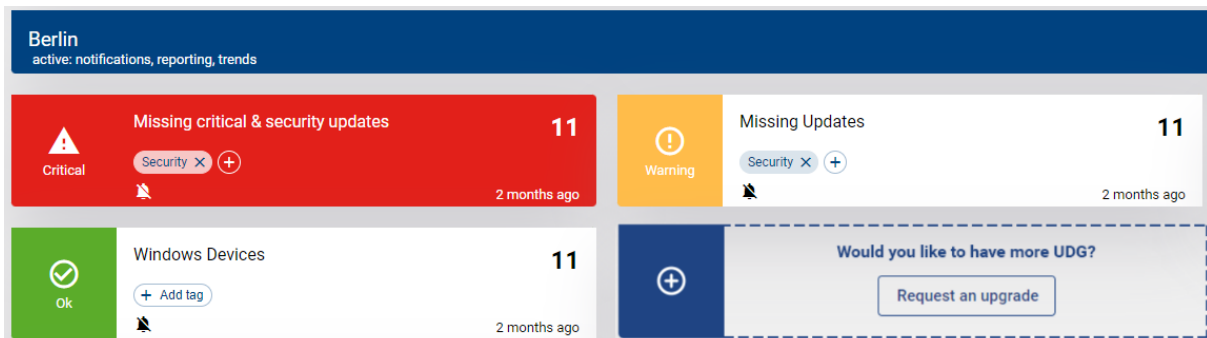


Figure 28 – Requesting more UDGs in Argus Cockpit

#### 3.4.2 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 detect trends or patterns for specific applications, versions or groups of computers.

<sup>5</sup> Market launch for the baramundi Argus Experience is expected to be summer 2023.

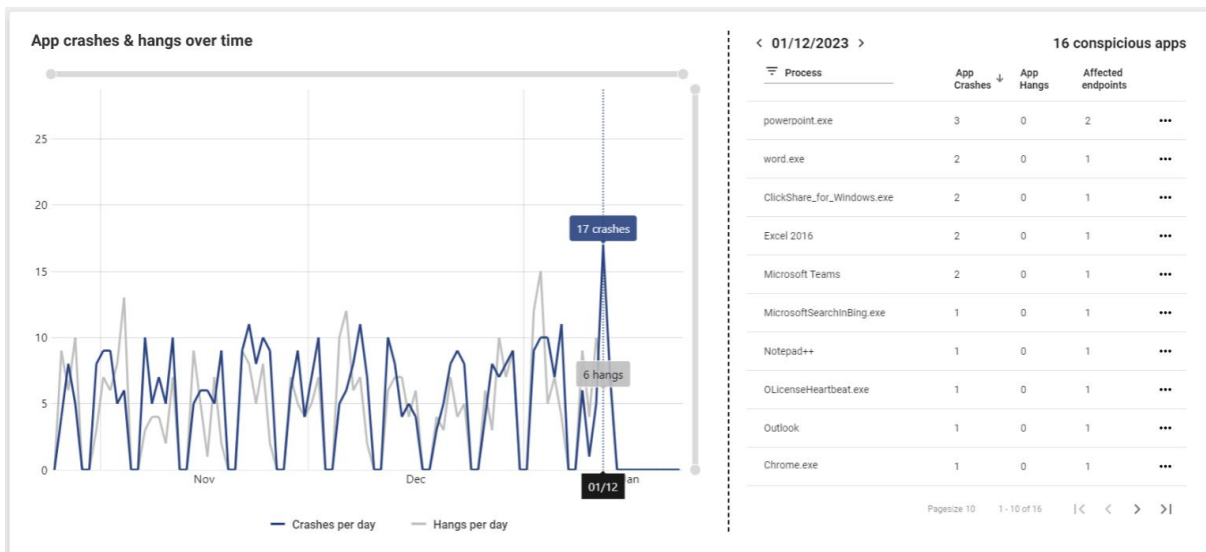


Figure 29 - bEX-Preview: Crashes and freezes per application

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.

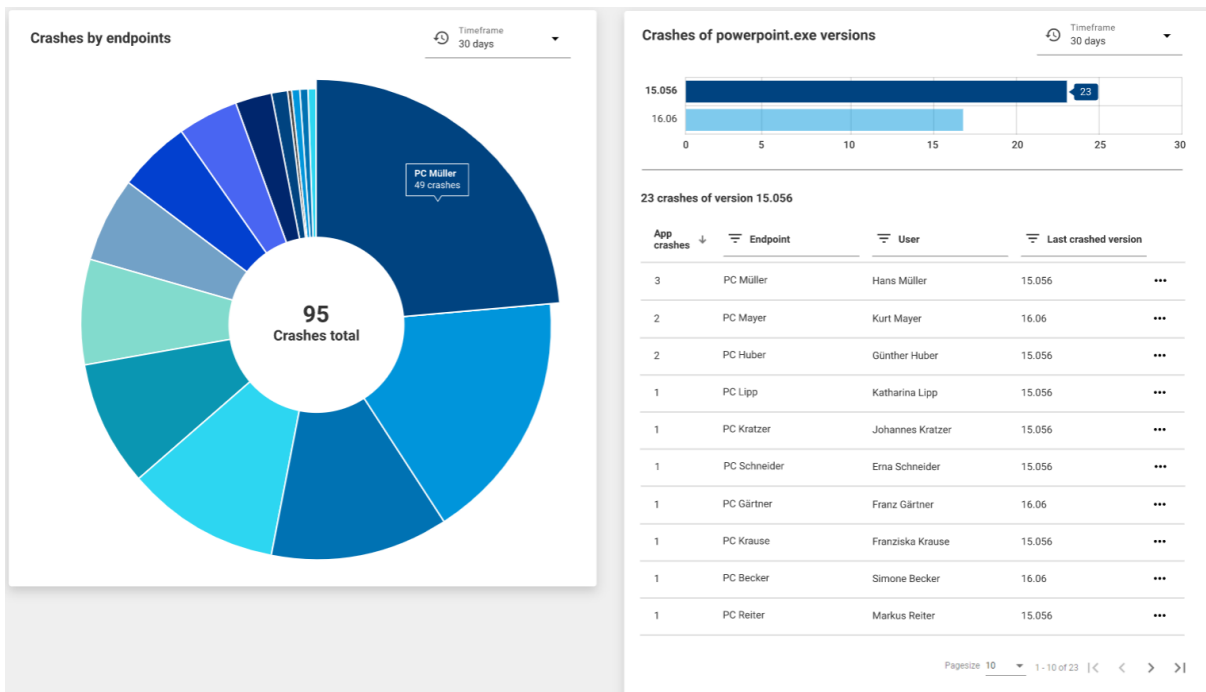


Figure 30 - bEX-Preview: Software crashes per endpoint and software version

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

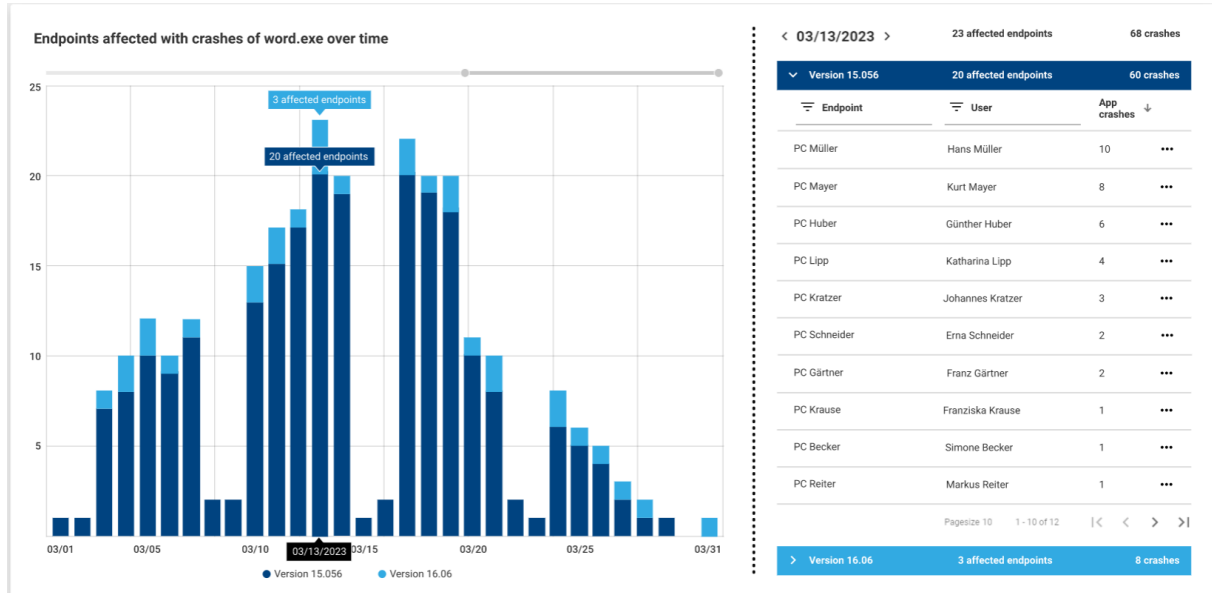


Figure 31 - bEX-Preview: Number of endpoints with problematic software versions

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.

### 3.4.3 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.

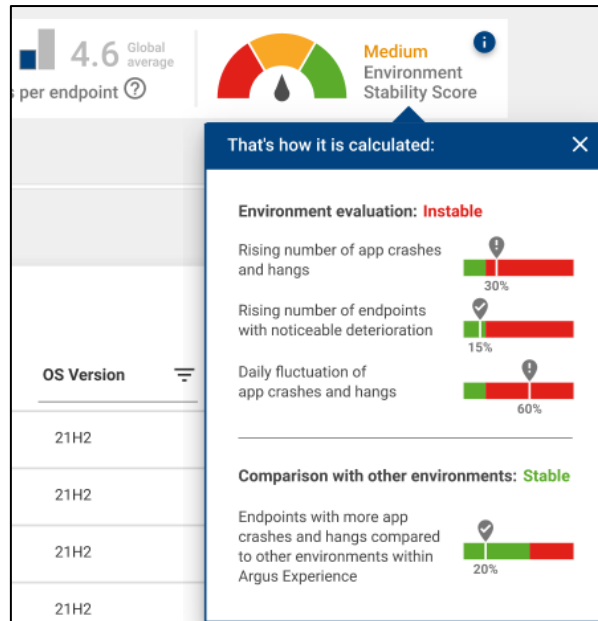


Figure 32 – bEX preview: Scoring of overall stability

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

### 3.4.4 Rapid Error Analysis

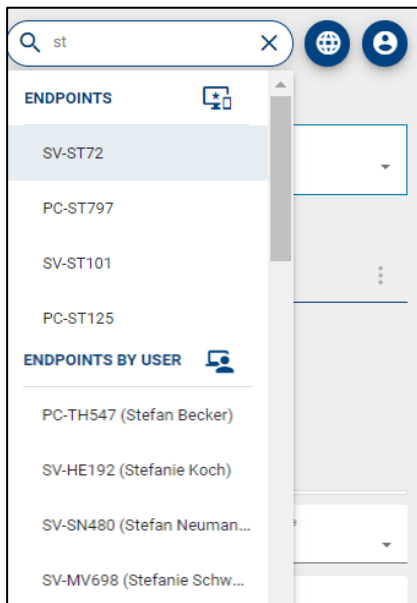


Figure 33 – Search for IT assets

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.

### 3.5 Universal Dynamic Groups

#### 3.5.1 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.

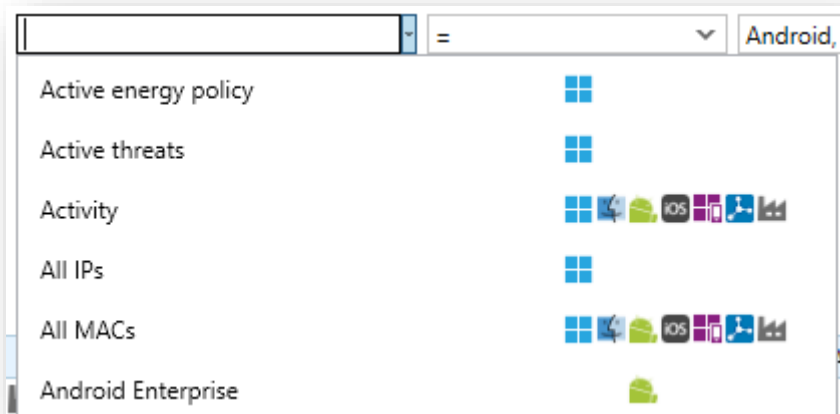


Figure 34 - UDG conditions – Icons

#### 3.5.2 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".

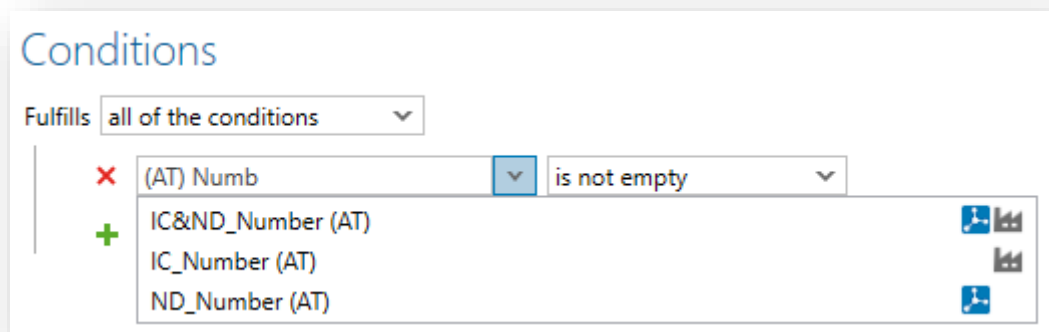


Figure 35 - UDG conditions – Text Filter

## 3.6 Product improvements in detail

### 3.6.1 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.

### 3.6.2 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.



### 3.6.3 Management Center (bMC)

- The detailed display of `Client - Compliance - Vulnerabilities - Detected` has been optimized for the new `Vulnerability Scan: Windows (Professional 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.

### 3.6.4 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.

### 3.6.5 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.

### 3.6.6 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.

### 3.6.7 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.

### 3.6.8 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.

### 3.6.9 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.

### 3.6.10 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*`.

### 3.6.11 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.

## 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 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