baramundi

Release Notes

baramundi Management Suite

2022 R1

Empower your IT

Liebe Leser,

Dieses Release bietet eine Vielzahl von **Usability**-Optimierungen, um die Nutzung der bMS sowohl für IT-Admins als auch für Endbenutzer:innen zu verbessern.

Für IT-Admins bieten die **Universellen Dynamischen Gruppen** nun speicherbare Anpassungen von Spaltenlayouts. Häufige individuelle Befehle sind über die erweiterten **Custom Commands** einfach zu erreichen.

Für Endbenutzer:innen steht der verbesserte **Kiosk** mit alternativen Sichten in Tabellen oder Kacheldarstellung, in Light- oder Dark-Mode zur Verfügung. Darin werden auch Mehrfach-Zuweisungen an Geräte ermöglicht.

In **baramundi Managed Software** wird per durchgängiger **Versiegelung** sichergestellt, dass Anwendungen unverändert auf den Endgeräten ankommen. Dadurch werden etwaige Angriffe auf die Lieferkette verhindert.

Das Modul **baramundi Network Devices** findet über das alternative Protokoll **Secure Shell (SSH)** weitere Endgeräte aus IT- und OT-Umgebungen. Dies eignet sich insbesondere für die Erkennung von Linux-Geräten.

Im neuen **Argus Cockpit** informieren individuelle E-Mail-Benachrichtigungen frühzeitig über kritische Zustandsänderungen.

Weitere Verbesserungen finden Sie zur App-Installation für Endpunkte mit **macOS**- und **Android:** Dies betrifft den Umgang mit PKG-Dateien bzw. der Freigabe von eigenen Apps und PlayStore-Apps direkt in der bMC.

Ich wünsche Ihnen eine anregende Lektüre.

Armin Leinfelder

Director Product Management

© 2022 baramundi software AG - Änderungen vorbehalten - DocID: BMS-220100-RN-220621-DE
Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information.

baramundi Management Suite – Version 2022 R1

INHALTSVERZEICHNIS

1 Release 2022 R1

1.1 baramundi Kiosk

Der Kiosk ist um viele spannende Funktionen erweitert worden. Hierbei stand die Usability im Fokus. Wir haben aber auch Optimierungen unter der Haube vorgenommen.

1.1.1 Dark Mode

Der Kiosk erscheint nun – auf Wunsch – auch im dunklen Gewand. Maßgebend ist die System- bzw. Browsereinstellung. Der Kiosk orientiert sich an dieser Einstellung, um im hellen oder dunklen Design zu erscheinen. Die User können aber auch gezielt zwischen hell und dunkel umschalten.

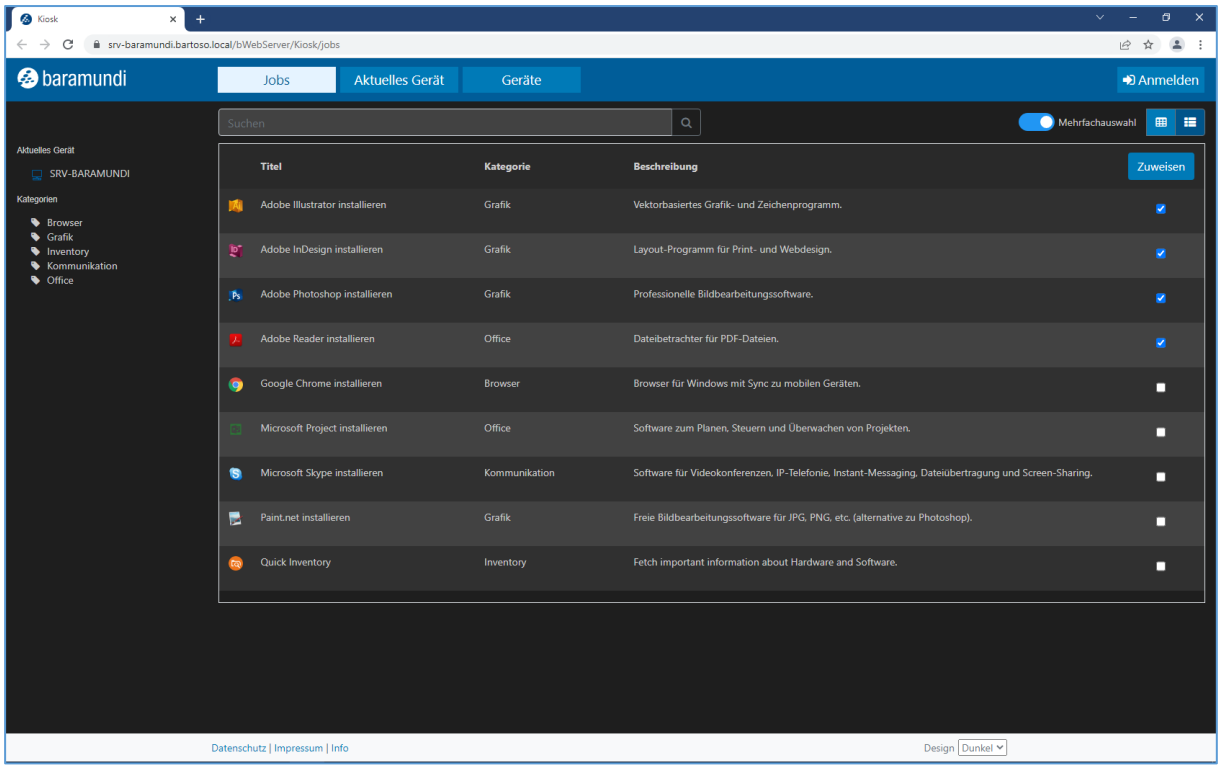


Abbildung 1 - Kiosk im Dark Mode in der Listenansicht und aktiver Mehrfachauswahl

1.1.2 Ein Endpoint, mehrere Jobs…

In der Listenansicht ist nun eine Mehrfachauswahl verfügbar. Ist die Mehrfachauswahl aktiv, können alle Jobs in der Liste ausgewählt und mit einem Klick zugewiesen werden. Das erleichtert und beschleunigt die Zuweisung mehrerer Jobs auf einem Endpoint erheblich.

1.1.3 Ein Job, mehrere Endpoints…

Auch umgekehrt wurde die Zuweisung von einem Job an mehrere Endpoints erleichtert. In der Auswahlliste des Zielgeräts können nun mehrere Endpoints angewählt werden. Ein Klick auf „Zuweisen“ sorgt dann für die Zuweisung auf allen gewählten Endpoints.

1.1.4 Kommentare im HTML-Format

Die Beschreibungstexte für die Anzeige im Kiosk dürfen nun auch HTML enthalten. Bisher wurden HTML-Tags vom Kiosk herausgefiltert und ignoriert. Nun kann die Interpretation von HTML im Kiosk global aktiviert werden (aus Sicherheitsgründen ist die Interpretation von HTML bei Auslieferung deaktiviert).

1.1.5 Standardansicht konfigurierbar (Kachel/Liste)

Gerade in Umgebungen, in denen häufig mit der Mehrfachauswahl von Jobs gearbeitet werden soll, ist es sinnvoll, den Kiosk direkt mit der Listenansicht zu starten. Daher kann nun über die Konfiguration global vorgegeben werden, ob der Kiosk in der Kachel- oder in der Listenansicht startet.

1.1.6 Hinweis für User im Kiosk

Wichtige Hinweise können nun im Kiosk bzw. auf der Anmeldeseite angezeigt werden. Wird eine Meldung über die Konfiguration des Kiosks eingetragen, erscheint im Kiosk sowohl ein Glockensymbol im rechten oberen Bereich als auch eine Hinweisbox auf dem Anmeldebildschirm mit der entsprechenden Nachricht.

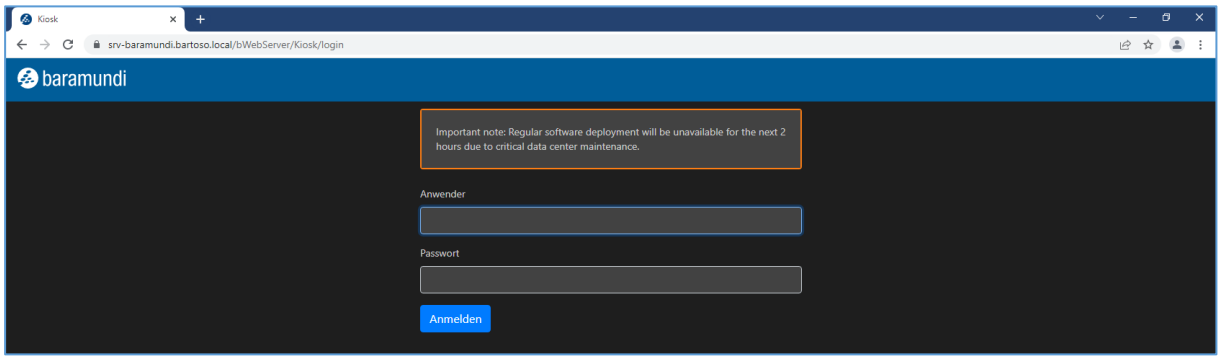


Abbildung 2 - Hinweistext auf dem Anmeldebildschirm des Kiosks

1.1.7 Automatische Aktualisierung der Liste zugewiesener Jobs

Im Kiosk können User selbst nachsehen, welche Jobs sie sich zugewiesen haben und ich welchem Zustand sie sich befinden. Diese Liste wird nun automatisch alle 30 Sekunden aktualisiert. Das Intervall ist konfigurierbar.

1.2 Update Management

1.2.1 Standard-Updateprofil

Bisher wurde neuen Endpoints kein Updateprofil automatisch zugewiesen. Das hat den Vorteil, dass neue Endpoints nicht versehentlich mit Updates versorgt werden, welche eigentlich nicht für sie freigegeben sind. In Folge werden Update-Jobs auf diesen Endpoints umgehend mit einem sprechenden Fehler beendet. Das Feedback unserer Kunden hat uns aber auch gezeigt, dass es gerade in hochstandardisierten Umgebungen ein Nachteil sein kann, wenn Updateprofile zuerst explizit zugewiesen werden müssen.

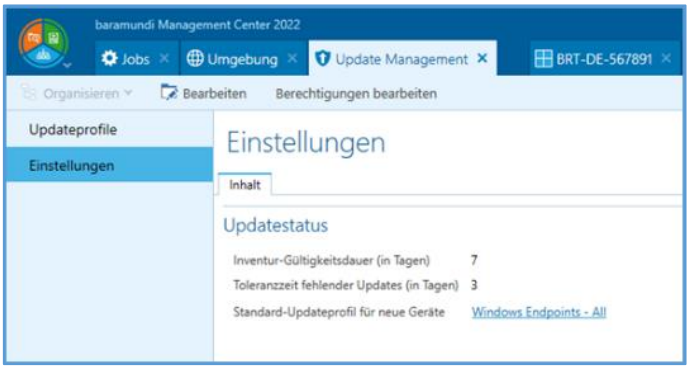


Abbildung 3 - Update Management Einstellungen mit gewähltem Standard-Updateprofil

Aus diesem Grund kann nun ein Updateprofil als globaler Standard vorgegeben werden – alle neuen Endpoints bekommen dieses Profil umgehend zugewiesen und aktualisieren sich mit dem nächsten Update-Job anhand der Konfiguration dieses Profils.

1.2.2 Deinstallation von Updates

Die Vergangenheit zeigt, dass Updates nicht immer nur Schwachstellen schließen oder neue Funktionen mitbringen. Manchmal schleichen sich auch neue Fehler oder Probleme ein und so funktioniert ein Update evtl. nicht immer ganz einwandfrei. Aus diesem Grund ist es wichtig, im System installierte Updates auch wieder entfernen zu können. Dies ist nun über eine Erweiterung des Jobschritts „Microsoft Updates verwalten“ möglich.

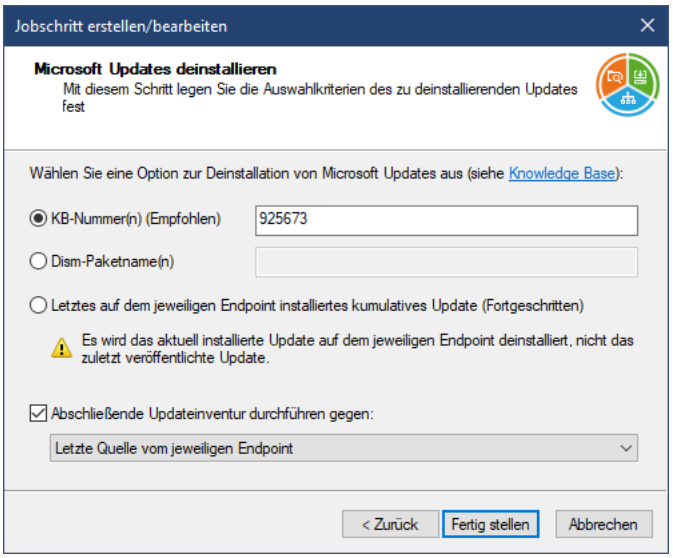


Abbildung 4 - Optionen zur Deinstallation eines Microsoft Updates

Hier können durch Angabe der KB-Nummer oder des DISM-Paketnamens gezielt einzelne Updates deinstalliert werden. Zusätzlich besteht auch die Möglichkeit, das letzte kumulative Update zu deinstallieren.
Nach Abschluss der Deinstallation wird eine Inventur durchgeführt. Hierfür wird die Gegenstelle verwendet, die auch zuletzt für die Inventur oder Aktualisierung des Endpoints ausgewählt wurde. Auch diese Option kann frei konfiguriert werden um bspw. gezielt eine andere Gegenstelle zu erzwingen.

1.3 baramundi Managed Software

1.3.1 Versiegelte Applikationen

Pakete für den baramundi Managed Software Service werden von unserem Managed Software Team handverlesen und genaustens geprüft. Dazu gehört nicht nur die Sicherstellung der Funktionen Installation, Aktualisierung und Update. Ebenso ist es essenziell, dass die heruntergeladenen, paketierten und somit weiterverteilten Dateien frei von Schadsoftware ist. Zu diesem Zweck durchlaufen die Dateien eine Prüfung mit den gängigsten Virenscannern, bevor sie zur Paketierung freigegeben werden.
Nach erfolgter Paketierung wird von jeder Datei die Prüfsumme ermittelt und zentral abgelegt. So können die baramundi Management Server unserer Kunden beim Download direkt sicherstellen, dass die heruntergeladene Datei intakt und nicht korrupt ist bevor sie auf dem Haupt-DIP in der Kundenumgebung abgelegt wird.

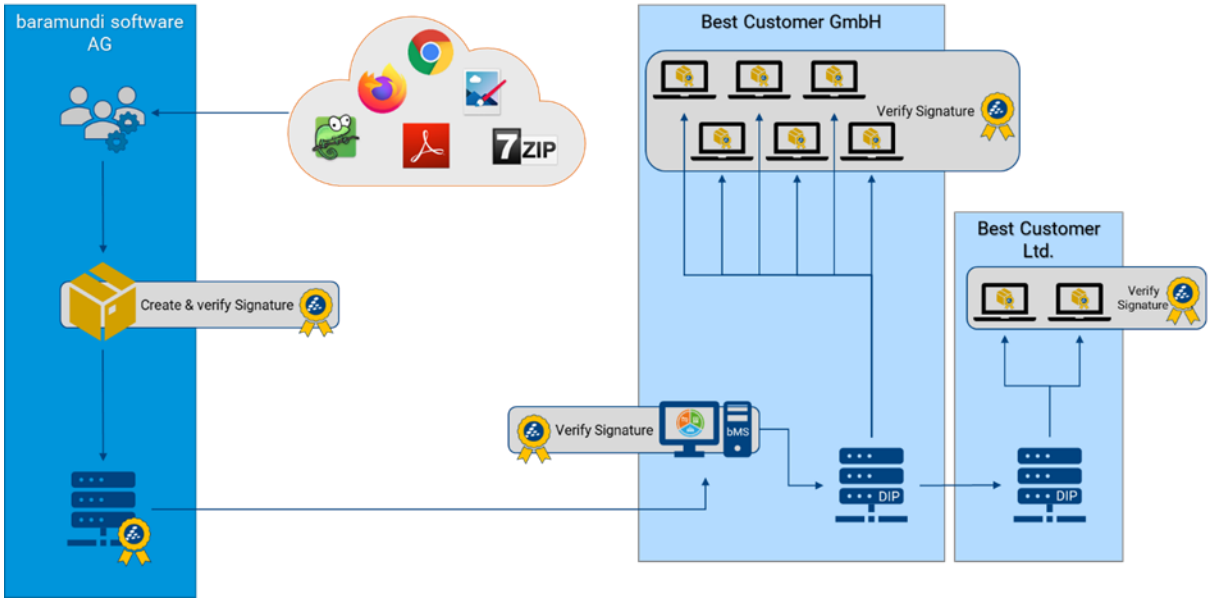


Abbildung 5 - Schematische Darstellung für den verbesserten Schutz von MSW-Paketen

Mit dem aktuellen Release wird die Sicherheitskette nun bis hin zum Agenten verlängert. Das bedeutet, dass nun auch der baramundi Management Agent die Installationsquellen vor der Installation lokal herunterlädt. Nach dem Download werden die Dateien erneut verifiziert und nur ausgeführt, wenn alle Dateien vollständig und unverändert sind.

Die Validierung der Pakete erfolgt im Hintergrund, ein manuelles Eingreifen ist – sofern keine eigenen Anpassungen vorgenommen werden – nicht erforderlich. Doch eigene Anpassungen sind selbstverständlich weiterhin möglich. Hierfür muss das Paket aber nach der bewussten Änderung erneut versiegelt werden.

Abbildung 6 - Benachrichtigung in der bMC über Änderungen an versiegelten Paketen

Nicht autorisierte Änderungen, Manipulationen oder defekte Downloads werden direkt als Hinweis im Notification Center der bMC angezeigt – eine Verteilung durch den Agenten findet nicht statt.

Die Managed Software Datensicherheit wird in der bMC unter `Software – Managed Software – Einstellungen` konfiguriert.

1.3.2 Versiegelter baramundi Management Agent

Im Zuge der weiteren Absicherung der Managed Software-Pakete wurde auch die Installation des baramundi Management Agents in das Sicherheitskonzept einbezogen. So prüft der Server nun, ob die Installationsquellen des Agents verändert wurden.

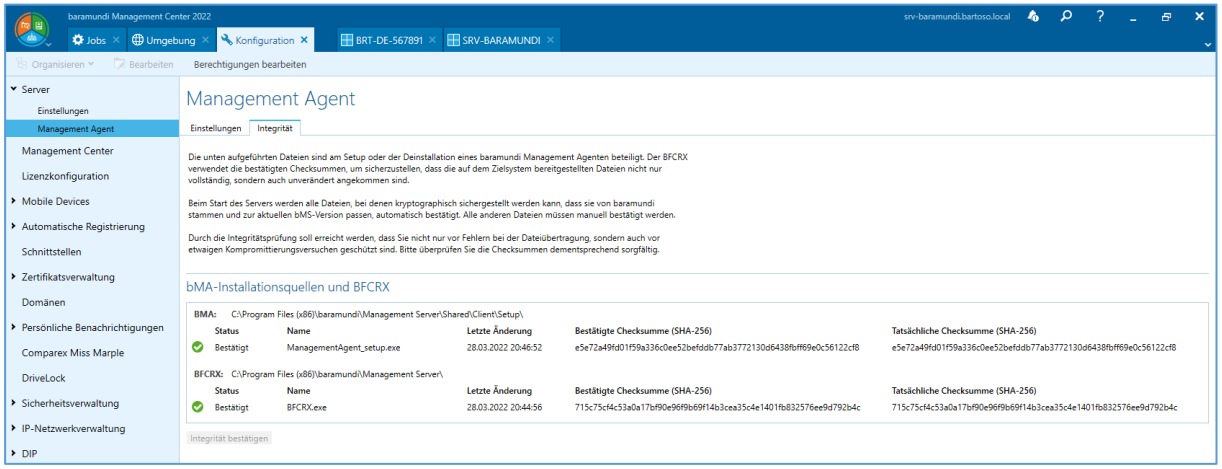


Abbildung 7 - Integritätsprüfung der bMA-Installationsdateien

Bei der Installation oder Aktualisierung des Agents wird die Integrität der Installationsdateien verifiziert. Nur bei bestätigter Integrität werden diese Dateien auch verwendet. Sollte eine kundenspezifische Anpassung an der Installation nötig sein, kann die Integrität der veränderten Dateien durch die Administration bestätigt werden.

1.4 baramundi Mobile Devices – Android Enterprise

Google entwickelt Android und auch die Management API Android Enterprise kontinuierlich weiter. Das hat zur Folge, dass neue Funktionen hinzugefügt aber auch bestehende Funktionen ausgebaut werden. Da Google zum September 2022 eine weitere Änderung der API erzwingen wird, haben wir diese Änderungen schon jetzt in die bMS übernommen.

Hinweis: Ab September 2022 ist für das Verwalten von Android Enterprise Geräten zwingend eine bMS 2022 R1 oder neuer erforderlich – planen Sie das Update rechtzeitig ein.

1.4.1 App Management

Die größte Änderung betrifft die Verwaltung der Android Apps. Diese können zukünftig nicht mehr direkt über den Play Store freigegeben werden. Stattdessen werden die Apps nun auf einer extra hierfür angelegten Seite verwaltet. Dort können Apps freigegeben und auch wieder entfernt werden. Auch WebApps können nun hinzugefügt werden.

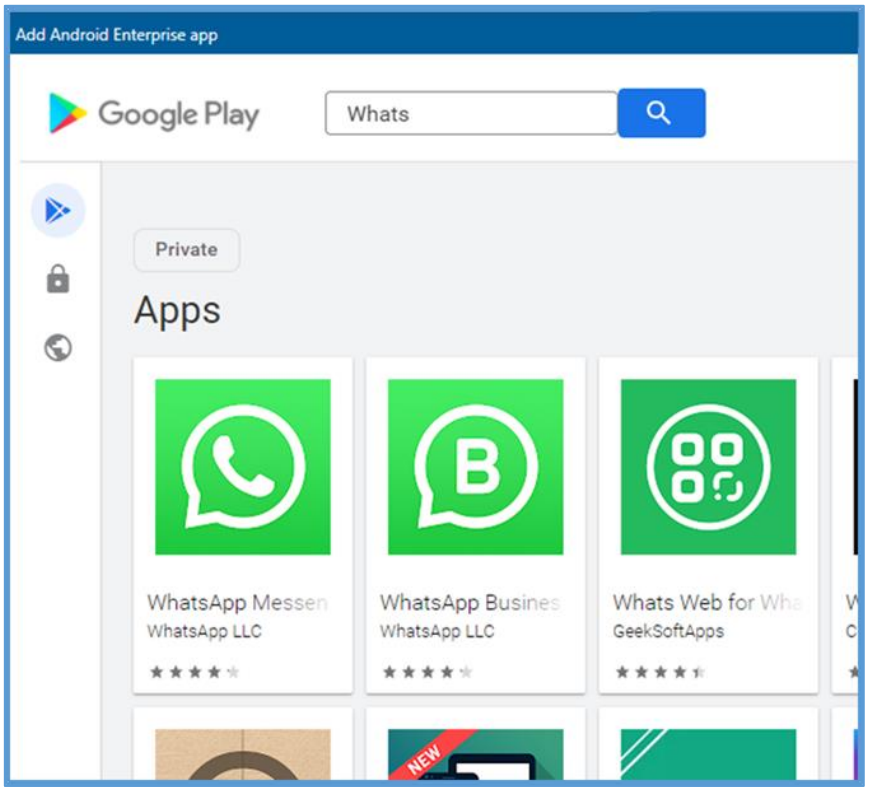


Abbildung 8 - Neuer Dialog zur Verwaltung von Android Apps

Ebenso ist es möglich, firmeneigene Apps ohne Umweg über einen Developer Account direkt aus der bMC für die eigene Umgebung freizugeben – auch das war ein Wunsch aus unserem Feedback Portal.

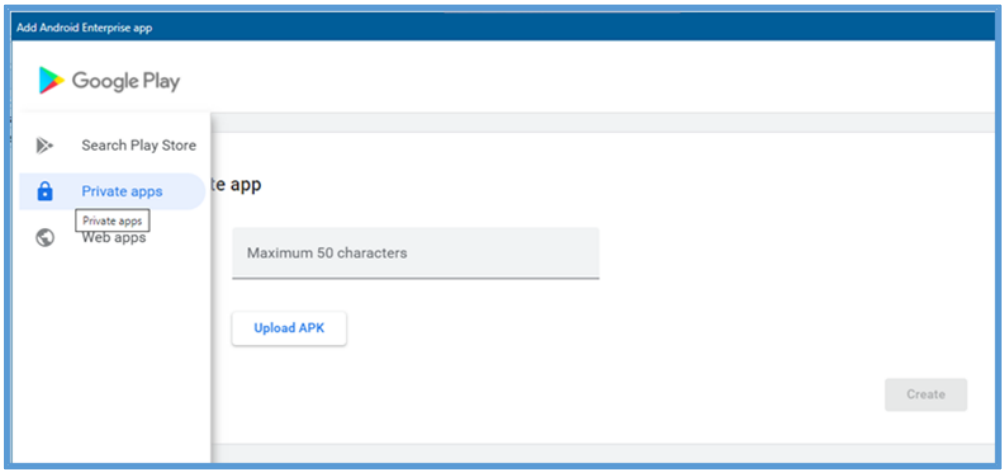


Abbildung 9 - Dialog zum Hinzufügen von firmeneigenen Apps

1.4.2 Update-Modus

Mit Umstellung auf die neue API kann nun der Update-Modus für jede App gezielt konfiguriert werden.

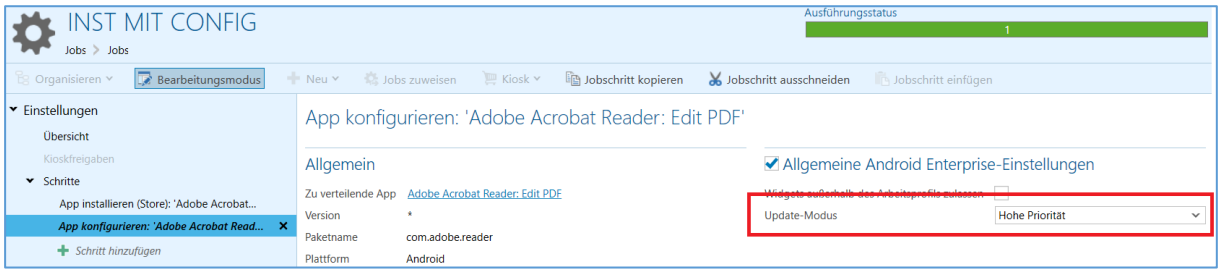


Abbildung 10 - Konfiguration des Update-Modus direkt an der App

Somit werden nun nicht mehr alle Apps nach der systemweiten Einstellung aktualisiert und es können bewusst Apps auf einem älteren Stand gehalten werden (z.B. für den Fall, dass auch ein internes Serversystem zuvor aktualisiert werden muss, o.ä.).

1.5 baramundi Ticketing System

1.5.1 Englische Sprach-Option

Die komplette Oberfläche des Systems, inkl. der Admin-Einstellungen, stehen auf Englisch zur Verfügung.

Jeder User (Benutzer und Enduser im SSP) kann **auf der Log-In Seite** die Sprache für den Log-In entscheiden. Die Standardeinstellung bleibt weiterhin Deutsch.
Alle **unveränderlichen** Standardinhalte werden automatisch übersetzt angezeigt. Die **freien** Inhalte (z.B. Beschreibungsfelder in Tickets, Aufgaben etc.) werden natürlich nicht je Sprachoption übersetzt.
Der Admin bzw. Benutzer mit entsprechenden Berechtigungen kann bestimmte individuelle Nutzungs-Inhalte auch **selbst individuell je Sprache übersetzen**. Hierzu muss man sich nur auf Englisch anmelden und die **benötigten Texte einfach übersetzen und ersetzen** (z.B. Titel und Beschreibungen von Ticket-Vorlagen, SSP Kacheltexte, Prio-Bezeichnungen etc.).

- E-Mailvorlagen sind doppelt vorhanden und können je Sprache gepflegt werden.
- Weitere Objekte (z.B. Textbausteine) haben eine eigene Sprachkennung und können entsprechend angelegt entsprechend der Sprache angeboten werden
- Manche Felder (v.a. Beschreibungsfelder die Screenshots enthalten können, z.B. Wissensdatenbank Artikel) können nicht unterschiedlich übersetzt angezeigt werden, hier muss der Inhalt für den Beschreibungstext z.B. untereinander in 2 Sprachen gepflegt werden

In der Onlinehilfe wird eine Liste der übersetzbaren Inhalte enthalten sein.

Eine Besonderheit stellt die Funktionalität der Kommunikation mit Kunden im Ticket dar

Hier kann je Kunde (Person) die **bevorzugte Kommunikationssprache** eingestellt werden. Diese wird auch im Ticket an der Person dargestellt. Damit sieht der Ticket-Bearbeiter, auch wenn dieser in anderer Sprache eingeloggt ist, in welcher Sprache er mit dem Kunden kommunizieren sollte.
Die Kommunikationssprache steuert zudem die automatische Auswahl der E-Mailvorlage oder Textbasteine in der richtigen Sprache für das Ticket.
Hinweis: die automatische Kommunikationssprache des Tickets richtet sich ausschließlich nach der **betroffenen Person des Tickets**.

1.5.2 Mehrstufige Genehmigungen

Use Case

Es gibt organisatorische Abläufe in denen bestimmte **Tickets nacheinander in mehreren Stufen von unterschiedlichsten Rollen geprüft und zur Bearbeitung freigegeben** werden müssen.

Beispiele:

- Es gibt organisatorische und technische Genehmigungen: Zunächst wird eine Freigabe der Fachabteilung für ein Beschaffungsbudget erteilt, danach folgt die technische Prüfung, ob dies umsetzbar ist (oder umgekehrt).
- Weitere Szenarien ergeben sich in klassischen „Umläufen“ von Vorgängen, die auch durchaus deutlich mehr Stufen beinhalten können.

Umsetzung

- Die bestehenden **Genehmigungsmodelle** eines Ticket-Typs (z.B. für Service Anfragen) können **beliebig mit Folgemodellen dieses Typs verkettet** werden.
- Im Ticket werden automatisch nach erfolgreicher Freigabe die Genehmigung(en) der nächsten Stufe verteilt.
- Je Genehmigungsstufe kann entscheiden werden, ob das Ticket weiter geprüft oder abgelehnt wird.

1.5.3 Neue Integrationsfunktionen mit bMS

Folgende neue Funktionen wurden in Verbindung mit der bMS Integration umgesetzt:

- Zuordnung von Genehmigungen auf bMS Jobs damit eingeschränkt werden kann, welcher Benutzer oder Benutzergruppe bestimmte Jobs im Ticketsystem ausführen darf
- Einschränkung von angezeigten/ ausführbaren Jobs im Asset bzw. Ticket: Im Asset werden nur noch diejenigen Jobs angeboten die gem. Endpoint Typ zulässig sind. Im Ticket (ggf. mehrere Endpoints in der Auswahl) erfolgt diese Prüfung ebenfalls bei Versuch der Ausführung und der Bearbeiter erhält eine entsprechende Meldung

1.5.4 Sonstige Erweiterungen

Genehmigungen - Erweiterungen für Genehmigungsprozesse

- Ergänzung Genehmigungskriterium „Organisations-Einheit“: Bestimmte Genehmigungen müssen nur bei Anfragen von bestimmten Org-Einheiten ausgeführt werden
- Anpassung des Genehmigungsmodells für Change Tickets: Genehmigungskriterium für „Normale Changes“ einzeln ergänzt, Notfall Changes und Standard Changes sind gem. ITIL Definition Genehmigungsfrei
- Option für generelle Genehmigungsausnahmen: bei einzelnen Personen kann die Option „muss nie genehmigt werden“ aktiviert werden. Alle Genehmigungsregeln werden bei dieser Person ignoriert, z.B. für den Geschäftsführer, der keine Genehmigung einholen muss

Erweiterungen CSV Importe/ Exporte

- In diversen CSV Importen/ Exporten wurden kleinere Verbesserungen/ Erweiterungen für einzelne Felder vorgenommen, z.B. Personen Import/ Export erweitert um:
  - Vorgesetzter (setzt vorherigen Import aller Personen mit Personalverantwortung voraus)
  - Sprache (für E-Mail-Kommunikation)
  - Funktion
  - Interne Information
  - Zugeordnete Kostenstelle (Vorbereitung für Erweiterung der Kostenstellenfunktionen im Folgerelease)

Ticketvorlage um Priorität Erweitert

Use Case

- Die Ticketvorlagen dienen zur schnellen Erfassung von wiederkehrenden Tickets bzw. zur automatischen Definition von Tickets, die per E-Mail-Regel oder aus dem Self-Service Portal erstellt werden
- Eine vorgegebene Priorität ist wichtig, wenn z.B. ein automatisches System per Email ein Ticket eröffnet und eine kritische Störung meldet, die gemäß SLA Stufe schneller bearbeitet werden muss

Umsetzung

- Die Ticketvorlage wurde um das Feld „Priorität“ erweitert
- Die weiteren Klassifizierungen (z.B. Auswirkung / Dringlichkeit) werden dabei nicht mitgegeben, da ggf. nicht verwendet bzw. von dem Ticketbearbeiter je Ticket individuell eingeschätzt und in der Ticketklassifizierung bei Bedarf noch angepasst werden

Regeln für eingehende E-Mails erweitert

Use Case

- Wenn eine neue unstrukturierte E-Mail ankommt, muss es auch die Möglichkeit geben, ohne separate Prüfung des Posteingangs direkt ein Ticket anzulegen. Die Klassifizierung um welchen Ticket-Typ es sich handelt erfolgt dann direkt in der Ticketliste

Umsetzung

- Für die E-Mail Regel vom Typ „immer“ ist die Angabe einer Ticketvorlage kein Pflichtfeld mehr. Wenn keine Ticketvorlage definiert ist, werden alle E-Mails von diesem eingehenden E-Mail Account ohne weitere manuelle Prüfung im Posteingang als Ticket angelegt und entsprechend als „unklassifiziertes Ticket“ markiert.
- Achtung:
  - Bei Nutzung dieser Funktion hat ein Ticket zunächst noch keinen SLA, da dieser erst i.V.m. dem Tickettyp berechnet werden kann
  - „Spam-Emails“ werden in dem Fall auch als Ticket angelegt und müssen dann abgelehnt werden, dies muss bei Auswertungen ggf. gesondert berücksichtigt werden

Erweiterte Unterstützung bei der AD SSO Einrichtung

Um ein Single-Sign-On (SSO) für bTS zu nutzen, muss im lokalen Netzwerk ein Relay eingerichtet werden, welches mit dem lokalen AD kommuniziert.
Mit dem Release wird eine neue Version des Authentifizierungstools bereitgestellt, welches diese neuen Features unterstützt:

- Um die Analyse von Problemen während der Einrichtung zu unterstützen, stellt das Ticket-System ein Hilfe Tool zur Verfügung, mit dessen Hilfe der Admin die aktuellen internen Authentifizierungsinformationen seines verwendeten Netzwerk Users überprüfen kann
- Weiterhin kann entschieden werden, welches AD Property für die Authentifizierung verwendet wird (UserPrincipalName oder (wie bisher) SamAccountName)

1.6 Weitere Verbesserungen

1.6.1 baramundi Network Devices – SSH als weiteres Protokoll

Mit dem neuen Release bieten wir Ihnen die Möglichkeit, Geräte die das Netzwerkprotokoll Secure Shell (SSH) unterstützen, gezielt zu erfassen.

Damit steht Ihnen neben SNMP, ARP und jetzt auch SSH eine weitere Erfassung Ihrer im Netzwerk befindlichen Systeme zur Verfügung und ist so eine Grundlage bspw. Geräte mit LINUX zu erfassen.

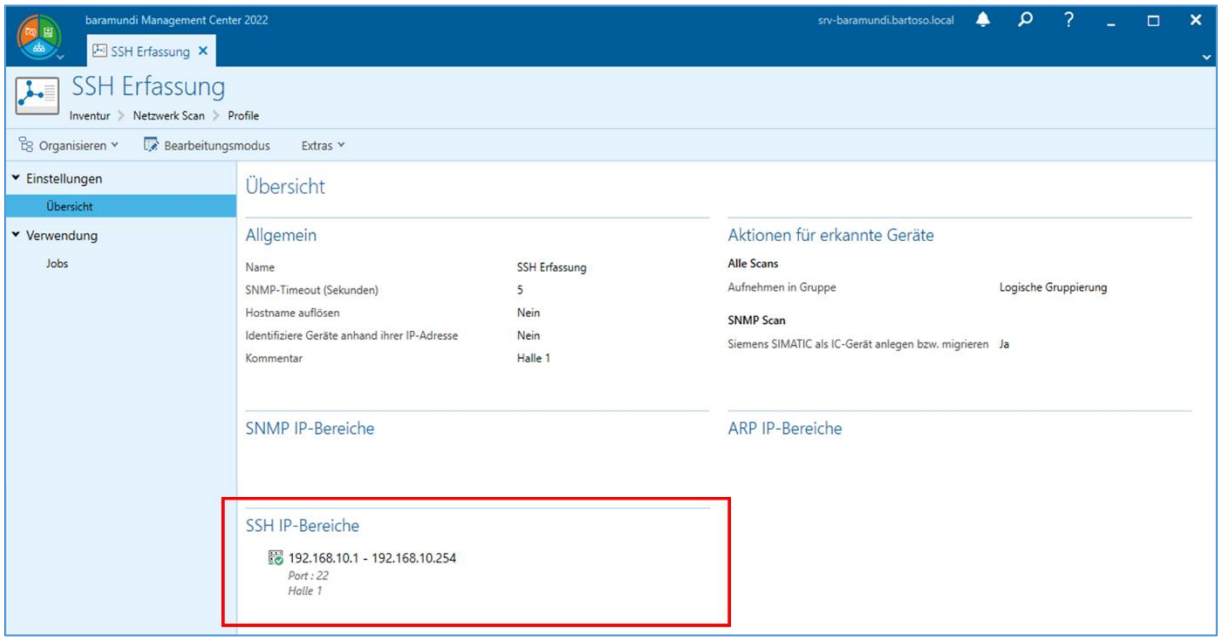


Abbildung 11 - Scanprofil über SSH

Als SSH-spezifische Informationen stehen Ihnen am Netzwerkgerät SSH Port, Server, Version oder die spezifischen Keys zur Verfügung. So ist bspw. eine Überprüfung, in wie weit das Netzwerkgerät eine sichere SSH Version verwendet, gegeben.

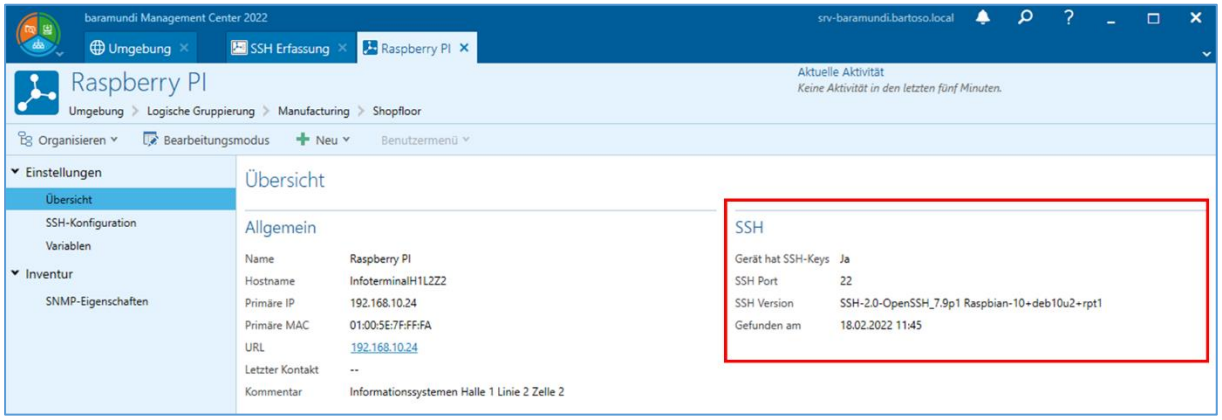


Abbildung 12 - Netzwerkgerät mit SSH Informationen

1.6.2 Clientbefehle an Network Devices und Industriellen Steuergeräten

Ein direktes Ausführen von Aktionen auf Netzwerkgeräten oder industriellen Steuergeräten steht Ihnen mit der bMS 2022 R1 über eigendefinierbare Clientbefehle zur Verfügung.

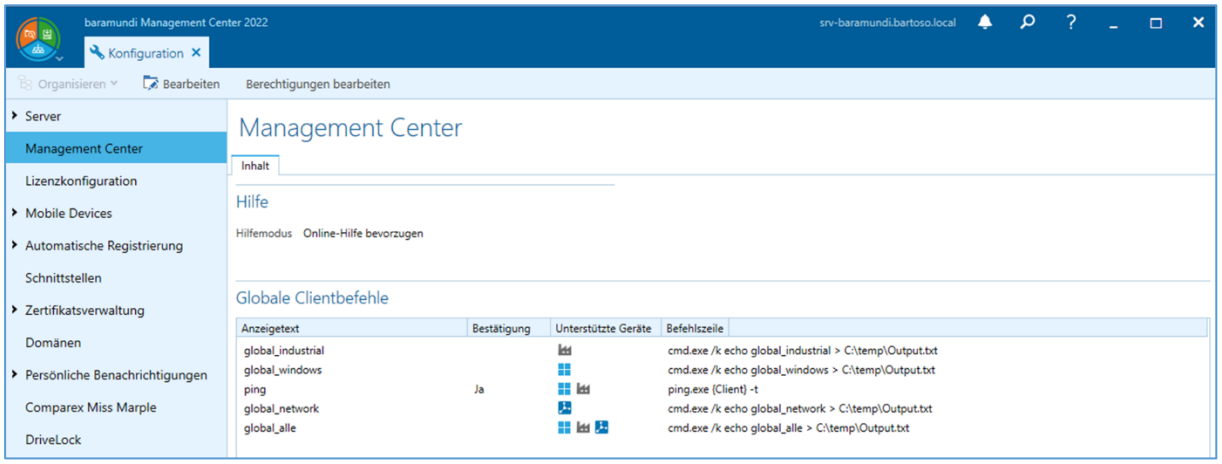


Abbildung 13 - Globale Clientbefehle im Management Center

Befehle können global festgelegt und so für alle Nutzer verfügbar gemacht werden. Weitere Kommandos können ergänzend dazu individuell auf Nutzerebene erstellt werden. Die vorbereiteten Kommandos erleichtern Ihnen so das Verwalten und die Betreuung Ihrer im Netzwerk vorhandenen Geräte.

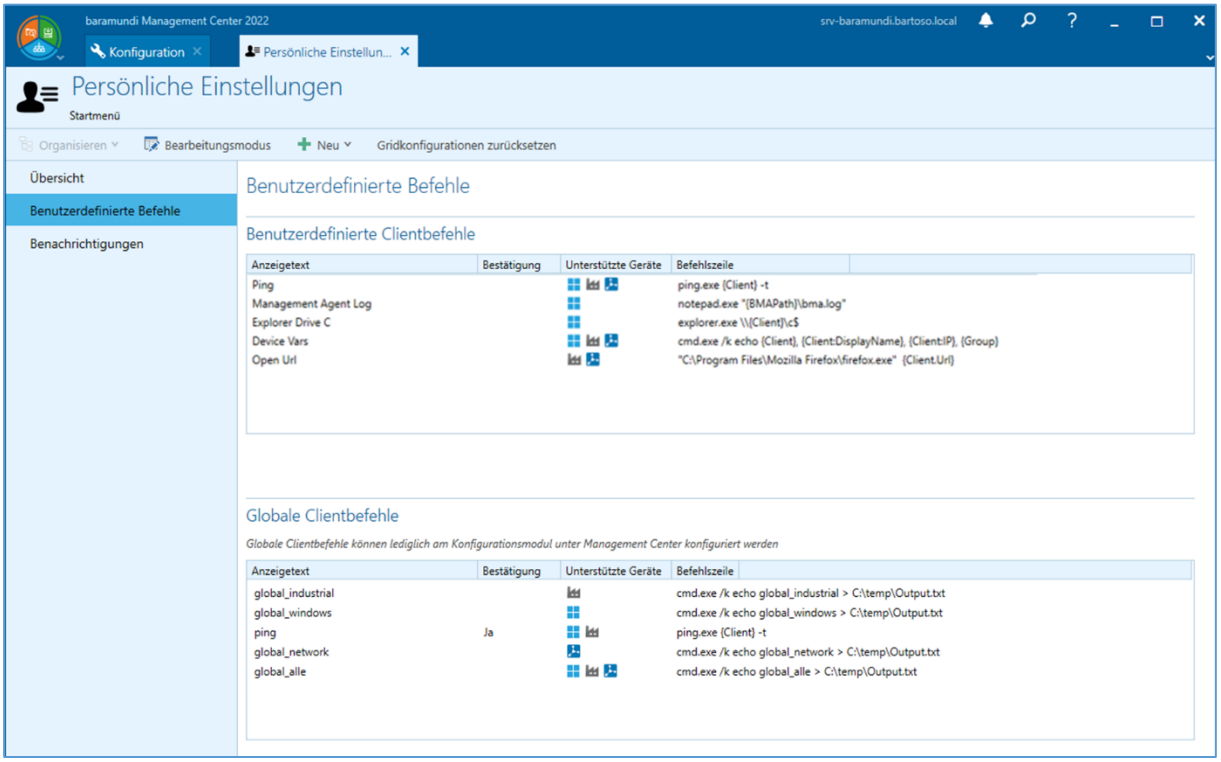


Abbildung 14 - Übersicht benutzerdefinierter Clientbefehle

Durch die Einrichtung von spezifischen Kommandos für Ihre Netzwerk- oder industriellen Steuergeräte, unterstützt dies im Falle von Supportanfragen unmittelbar, um zeitsparend reagieren zu können. So können z.B. direkt Verbindungsprobleme zu einem Drucker analysiert oder ein Auslesen von gerätespezifischen Daten wie z.B. die Seriennummer des Toners durchgeführt werden.

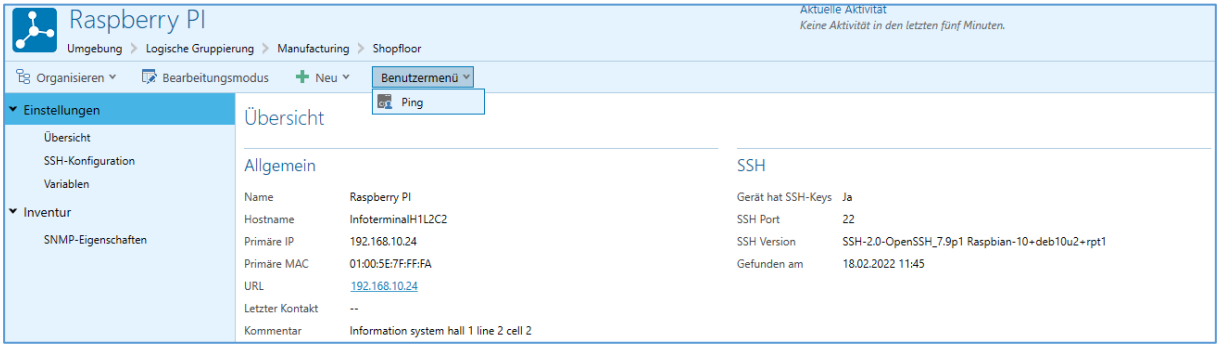


Abbildung 15 - Aufruf von benutzerdefinierten Clientbefehlen

1.6.3 UDG – Speichern von Spalteneigenschaften

Als Verbesserung der Universellen Dynamischen Gruppen (UDG) bieten wir Ihnen die Möglichkeit die Spalten Eigenschaften der jeweiligen UDG individuell zu speichern. So können Sie jede UDG individuell nach Ihren Bedürfnissen festlegen und darstellen. Vor allem

bei Gruppen für spezifische Plattformen können somit diese plattformspezifischen Spalten pro Gruppe gespeichert werden. Dies erfolgt für jeden angemeldeten bMC Benutzer separat und können individuell gemerkt werden.

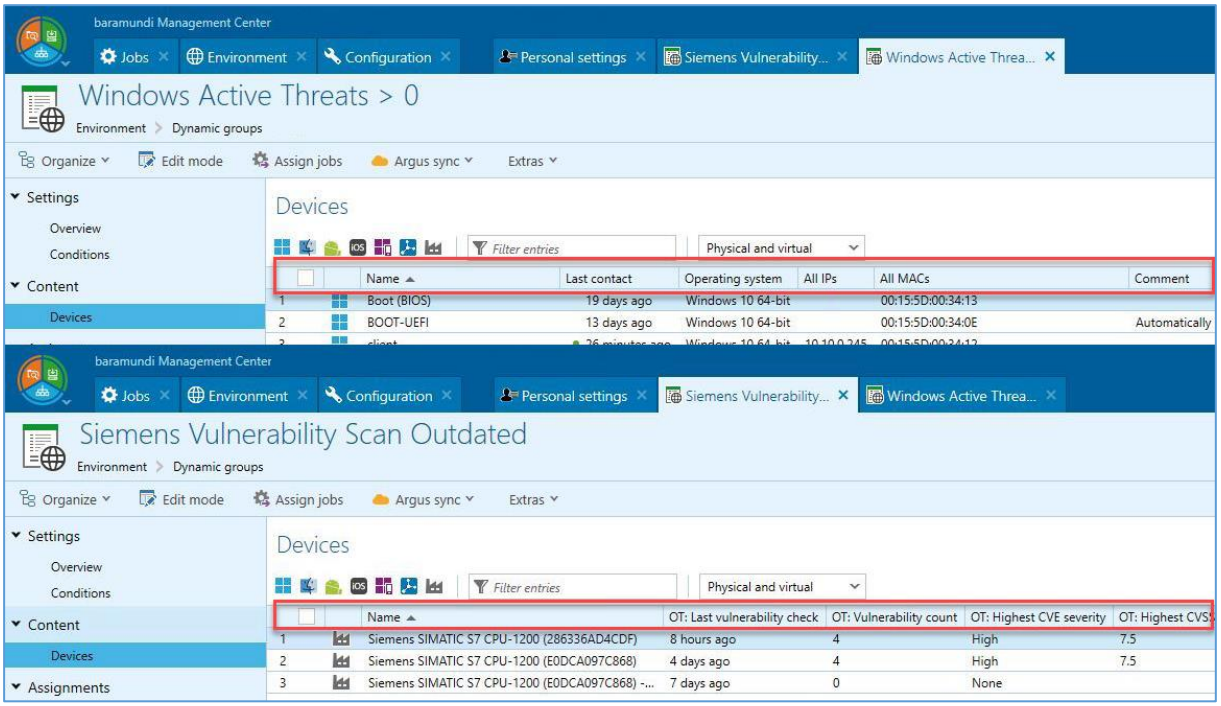


Abbildung 16 – UDG - Spaltenansicht pro Gruppe

1.6.4 Endpoint-übergreifende Variablen

Im neuen Release haben Sie beim Erstellen Ihrer individuellen Variablen die Möglichkeit, eine Variable gleichzeitig mehreren Endpunkttypen zuzuordnen.

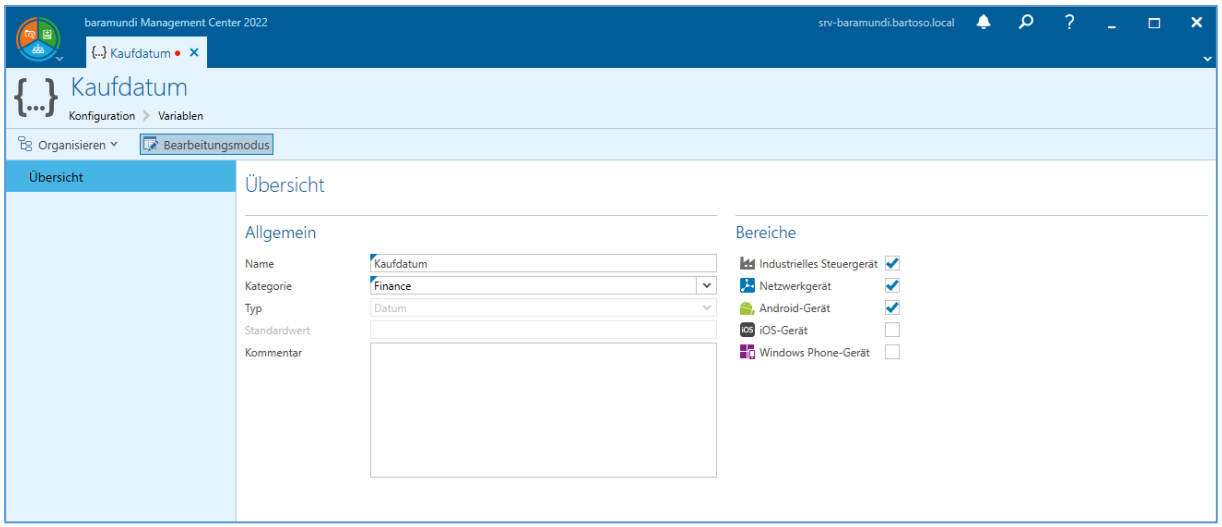


Abbildung 17 – Anlage einer neuen Variable mit Auswahl der Bereiche

1.6.5 macOS – Installation von PKG-Paketen ohne App Store

Die Verteilung von Applikationen mit PKG-Installation wurde deutlich vereinfacht. So können diese PKG-Dateien nun zentral abgelegt und als App in die bMC importiert werden.

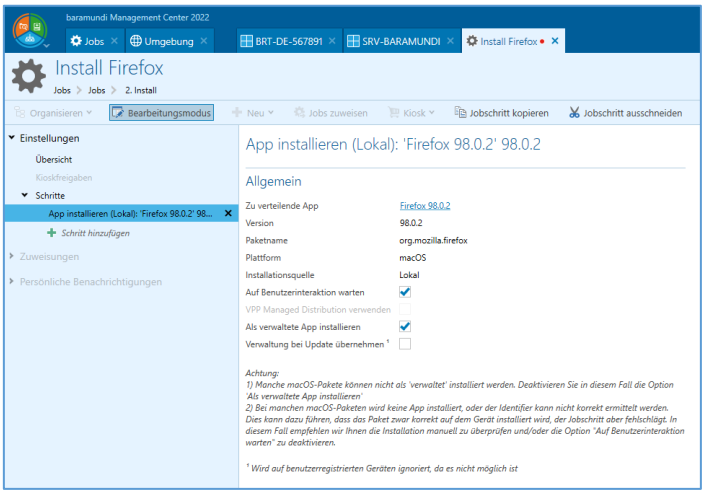


Abbildung 18 - Jobschritt zur Verteilung eines PKG-Pakets auf macOS

Im Anschluss werden die Applikationen per Job mit dem Jobschritt „App installieren“ auf die gewünschten macOS-Endpoints verteilt. Hierfür ist keine Verbindung zum Apple App Store notwendig.

1.6.6 Argus Cockpit – Benachrichtigungen

Zahlreiche Security-Vorfälle wie zuletzt z.B. der Log4J-Zwischenfall zeigen, wie wichtig es ist, dass IT-Verantwortliche so schnell wie möglich über kritische Zustände Ihrer IT informiert werden müssen. Nur so können Gegenmaßnahmen rechtzeitig eingeleitet werden. Mit dem baramundi Argus Cockpit haben IT-Admins die Möglichkeit, wichtige Kennzahlen der Endgeräte jederzeit im Blick zu behalten. Mit Hilfe der Universellen Dynamischen Gruppen (UDG) können sie bspw. den Bitlocker-, Firewall- oder Antivirus-Status tracken oder das Microsoft Update-Level aller Endgeräte beobachten.

Mit den neuen Argus Cockpit Benachrichtigungen haben IT-Admins die Möglichkeit, sich frühzeitig über kritische Zustandsänderungen per E-Mail informieren zu lassen, in dem sie die UDG-Schwellwerte entsprechend konfigurieren und die E-Mail-Benachrichtigungen individuell aktivieren. Diese Schwellwert-Konfigurationen können nun auch jederzeit zurückgesetzt und verändert werden.

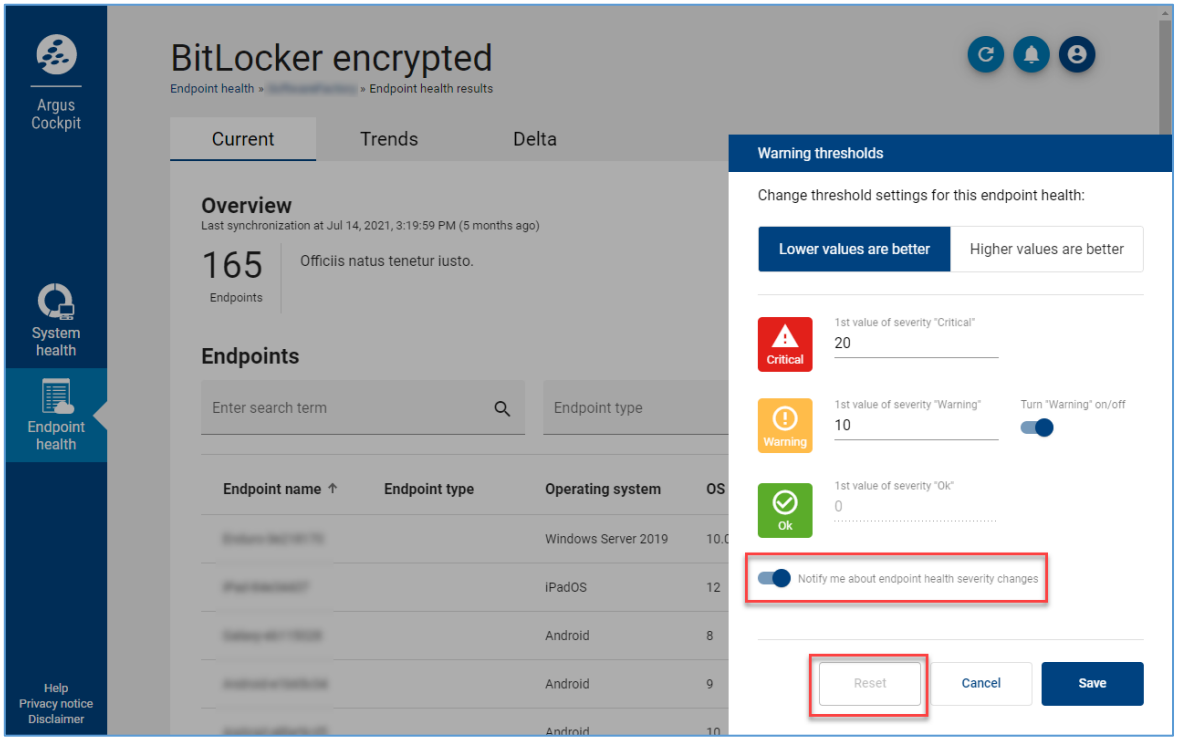


Abbildung 19 - Notifications für Über-/Unterschreitungen v. UDG-Schwellwerten aktivieren

Darüber hinaus wurden auch Benachrichtigungen für bMS-Dienste und (ablaufende) Reporting-API-Keys ermöglicht, so dass IT-Verantwortliche bei Unregelmäßigkeiten des bMS-Betriebs schneller informiert werden können.

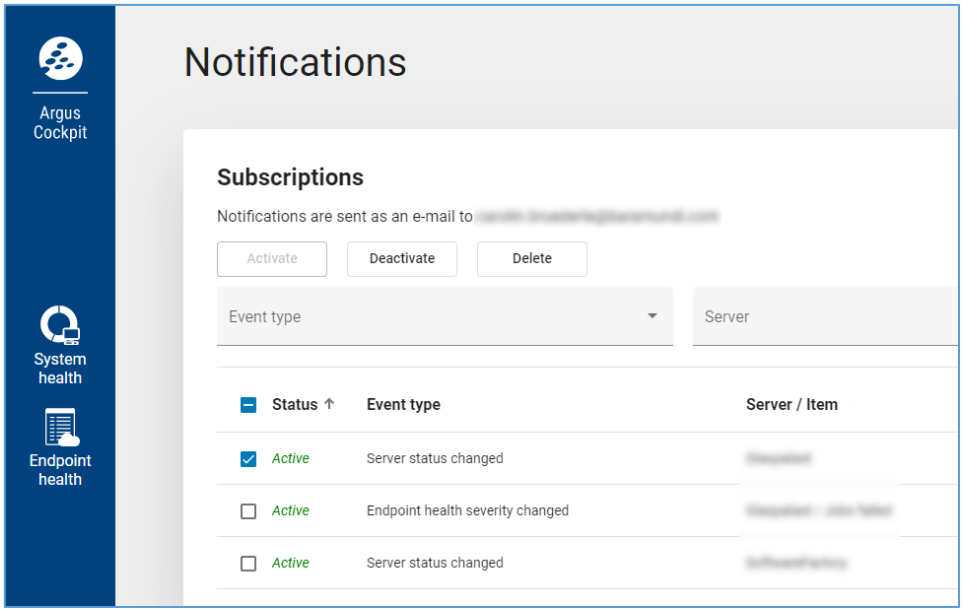


Abbildung 20 - Aktive Benachrichtigungen konfigurieren

1.6.7 Lizenzierung der baramundi Management Suite

Bereits mit der bMS 2021 R2 wurde eine neue Lizenzprüfung für die Lizenzen der Suite integriert. Diese neue Lizenzprüfung ermöglicht eine einfache und schnelle Onlinelizenzierung der Suite. Nach Bestellung einer neuen Lizenz muss nur die Ticket-Nummer innerhalb der Suite aktiviert werden – die Suite ist nun mit der Onlinelizenzierung verbunden und lädt automatisch neue Lizenzen nach.

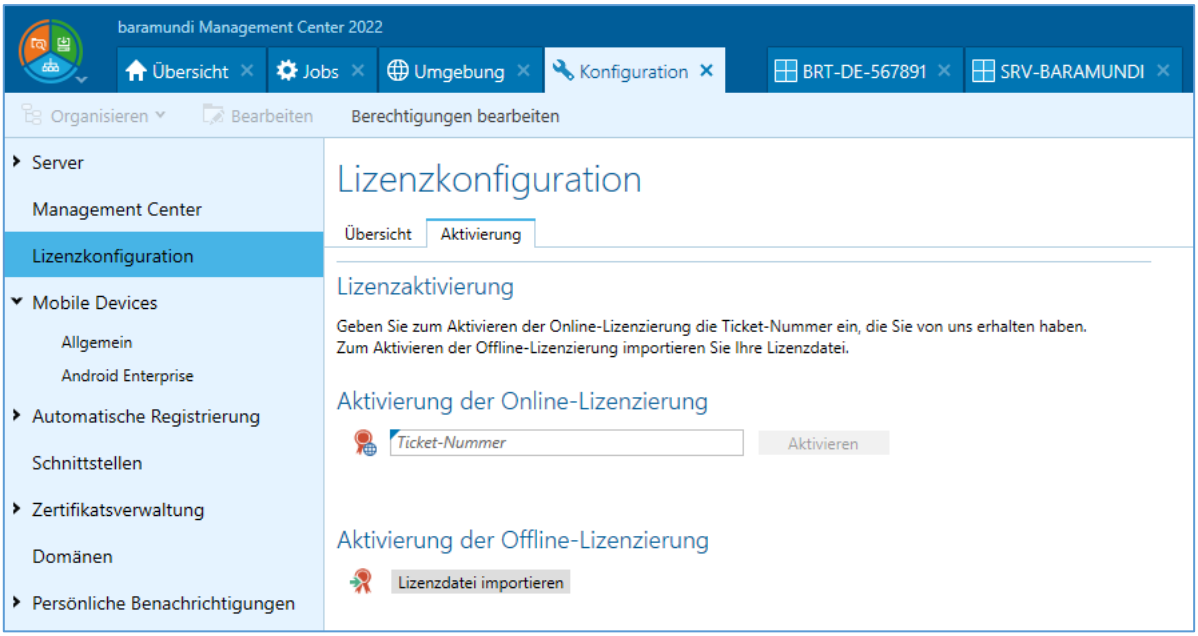


Abbildung 21 - Dialog zur Aktivierung einer neuen Lizenz

Für Sie bedeutet das, dass sie nach Bestellung einer neuen Lizenz keine weiteren Aktionen durchführen müssen. Sobald die Bestellung durch baramundi bearbeitet wurde, lädt der baramundi Management Server die entsprechenden Lizenzen online nach und aktiviert sie beim nächsten Start des Servers.
Selbstverständlich ist auch weiterhin eine Aktivierung ohne Internetverbindung möglich – allerdings ohne den Komfort der automatischen Lizenzaktivierung und -aktualisierung.

Hinweis: Die neue Lizenzprüfung ist automatisch für neue Datenbanken aktiv. Bei bestehenden Installationen muss manuell auf die neue Lizenzprüfung umgestellt werden. Hierzu benötigen Sie lediglich eine Ticket-Nummer für Ihre vorhandenen Lizenzen. Diese Ticket-Nummer können Sie unter license-migration@baramundi.com anfordern.
Ab der kommenden bMS 2022 R2 werden alte Lizenzen nicht mehr unterstützt.

1.6.8 baramundi User Interface Anpassungen

Mit diesem Release haben einige Anpassungen in der Benutzeroberfläche umgesetzt.

1.6.8.1 Fensteroptionen

Die Schaltflächen zum Schließen, Maximieren, Minimieren sind jetzt alle ohne Zwischenräume zusammen und mit rotem MouseOver Effekt beim Schließen.

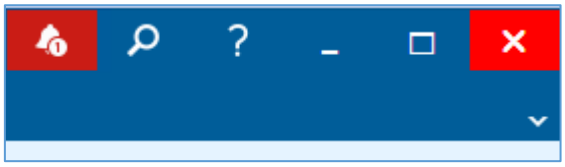


Abbildung 22 - Schaltflächen neu angeordnet

1.6.8.2 "Grüner Punkt" am Endpoint-Namen

Der bereits bekannte „Grüne Punkt“ des letzten Kontakts wurde neben der Grid View nun auch an den Endpoint-Tab neben dessen Namen kopiert um einen schnelleren Überblick der geöffneten und aktiven Endpunkte zu erhalten.

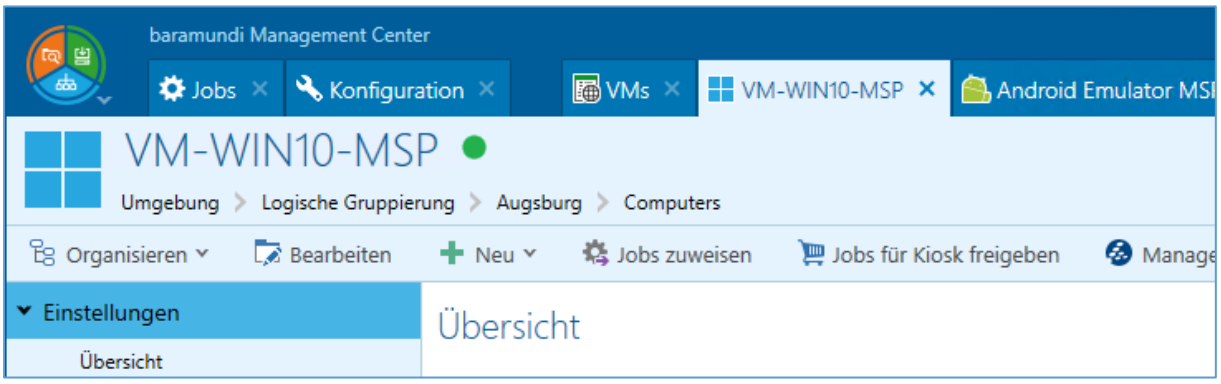


Abbildung 23 - "Grüner Punkt" im Endpoint-Tab

1.6.8.3 Schnellsuche

Für die Suchbegriffe in der Schnellsuche werden nun alle Leerzeichen vor und nach dem Text entfernt.

1.6.8.4 Objekttab-Liste

Bei vielen geöffneten Objekten können nun Tabs direkt im "Tab Dropdown" geschlossen werden. Durch deinen Klick auf X oder mit dem mittleren Mouse Button.

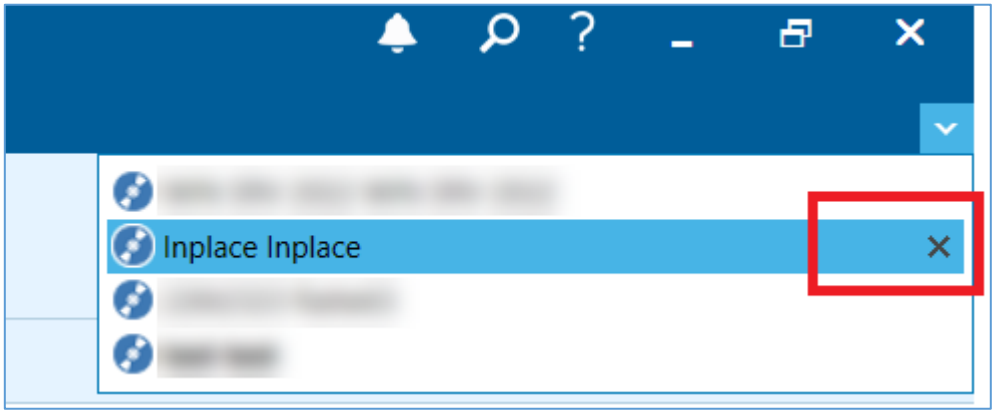


Abbildung 24 - Schließen geöffneter Objekte

1.6.8.5 Tastenkürzel für Tabwechsel

Mittels "Strg + TAB" (vorwärts) oder "Strg + Shift + TAB" (rückwärts) kann man nun durch die Tabs im Management Center springen. Wenn man beim ersten oder letzten Tab angelangt ist, wird als nächstes der erste oder letzte Tab genommen, je nach Tastenkombination.

1.6.8.6 Spalten „Alle IPs“ und „Alle MACs“

In den Gridviews gibt es nun zwei neue Spalten:

- "Alle IPs" - zeigt alle IP-Adressen die für das Gerät bekannt sind an (nur für Windows-Geräte verfügbar)
- "Alle MACs" - zeigt alle MAC-Adressen die für das Gerät bekannt sind an.

1.6.8.7 Asset Spalten

In Asset Gridviews können nun die Eigenschaften von Assets in die Spalten ein- oder ausgeblendet werden.

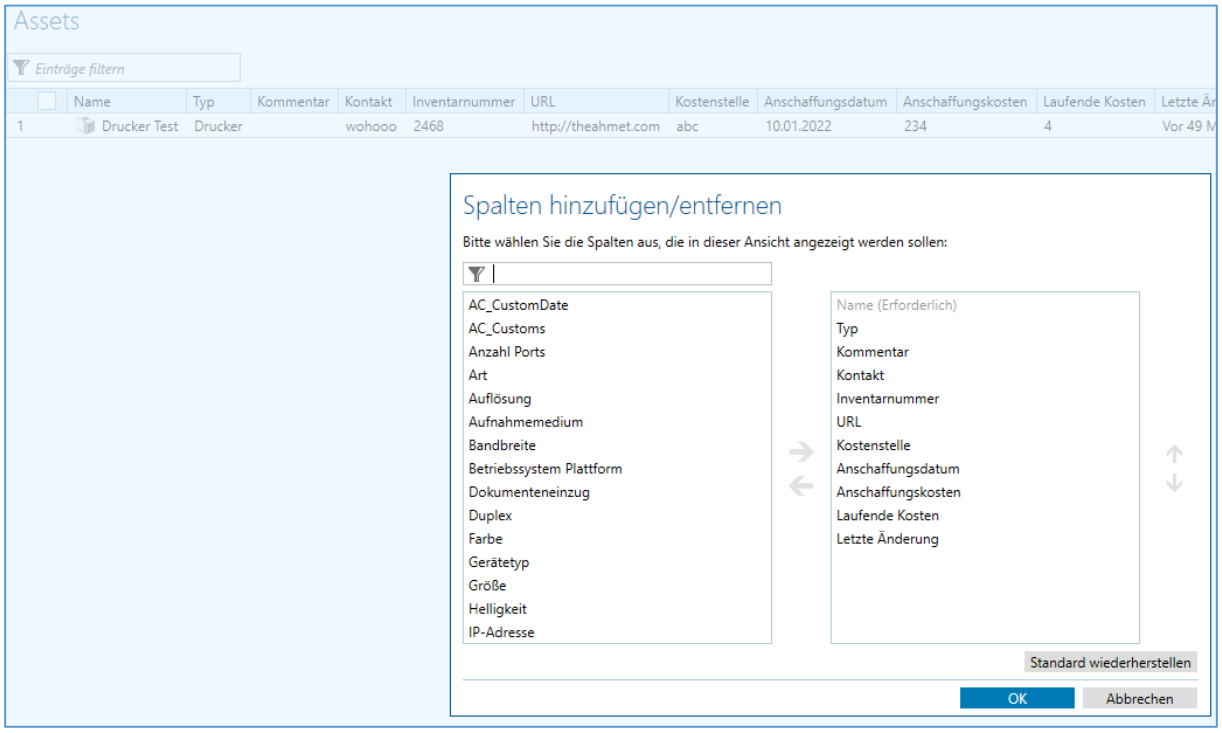


Abbildung 25 - Asset Gridview Spaltenanzeige

1.6.9 bConnect Log

Zur administrativen Nachvollziehbarkeit werden und bei bConnect Requests der Benutzername im Server.log mitprotokolliert.

Beispiel:

```
Received [GetAllApplications] request from user
[gmueller@bartoso.local] for bConnect v1.1. [Params: ]
```

1.7 Produktverbesserungen im Detail

1.7.1 Windows Agent (bMA)

- Hinweis: Die Weiterentwicklung des bMA für Windows XP wurde eingestellt. (Siehe auch 1.9.1)

- Eine unter `Jobs – Job – Eigenschaften – Erweitert – Ausführungstimeout` konfigurierte maximale Laufzeit des Jobs, wird nun auch vom bMA überwacht. Hinweis: Ein Job, der einen längeren Ausführungszeitraum benötigt als die voreingestellte Timeout-Zeit, wird jetzt nicht mehr fertiggestellt. Ein Beispiel ist der Jobschritt Complince Scan, der mehrere Stunden benötigen kann.

- Unter `Konfiguration – Server – Management Agent – Integrität` wird die Integrität des bMA dargestellt. Wird nicht der Standardmechanismus für den bMA verwendet, so kann dort eine abweichende Integrität bestätigt werden.

- Unter `Konfiguration – Server – Grundeinstellungen – bMA Installationsart` werden die Einstellungen `BFCRX mit Installationsbenutzer` und `Veralteter BFCRX` nur noch mit Version 2022 R1 unterstützt. Ein bMC-Hinweis wird eingeblendet, dass diese Einstellung noch gewählt ist.

- Das Selbstupdate des bMA ist erheblich robuster. Es erkennt laufende Jobs besser und wird bei sporadischen Fehlern, wie z.B. bei parallelen MSI Installationen durch automatisches Patchen, bis zu 10 Stunden lang erneut versucht.

- Bugfix: Eine Software-Installation mit der Option `lokal kopieren` beachtet das minimale Restspeicherlimit nicht.

1.7.2 Management Center (bMC)

- Es wird ein Hinweistext angezeigt, wenn eine veraltete Art der Lizenzprüfung verwendet wird. Auch ohne Umstellung der Lizenzierung kann die bMS weiterhin uneingeschränkt verwendet werden. Eine zeitnahme Umstellung wird jedoch empfohlen.

- Es wird ein Hinweistext angezeigt, wenn noch die alte Software-Inventur verwendet wird.

- Die Loginprüfung wurde verbessert und erkennt jetzt u.A. einen versehentlich aktivierten Windows-Gast-Account.

- Die Möglichkeiten unter `Persönliche Einstellungen - Benutzerdefinierte Befehle` wurden überarbeitet und verbessert.
- Unter `Umgebung` sind zusätzlich die Spalten `Alle IPs` und `Alle MACs` verfügbar.
- Unter `Dynamische Gruppe (Universell)` steht als Bedingung für `Primäre IP` jetzt `ist im Subnetz` und `ist nicht im Subnetz` bereit.
- Hinweis: Bei `Dynamische Gruppe (Universell)`, welche für `Primäre IP` einen Vergleich mit `<(=)` oder `(=)>` konfiguriert haben, wird ein Hinweistext angezeigt. Diese Gruppen sind nicht mehr verwendbar und sind manuell anzupassen.
- Unter `Dynamische Gruppe (Universell)` ist die Spaltenkonfiguration für jede Gruppe separat konfigurierbar.
- Im Jobschritt `Microsoft Update verwalten` ist jetzt die Aktion `Microsoft Updates deinstallieren` verfügbar. Bei Problemen während der Deinstallation werden hilfreiche DISM Fehlercodes am Jobschritt angezeigt.
- Benutzereinstellungen für die Spalteneinstellungen der verschiedenen Tabellenansichten können unter `Persönliche Einstellungen – Gridkonfigurationen zurücksetzen` für den aktuellen Benutzer zurückgesetzt werden.
- Bei einer `Suche` werden Leerzeichen am Anfang und Ende automatisch entfernt.
- Die Shortcuts `STRG+TAB(vorwärts)` und `STRG+SHIFT+TAB(rückwärts)` ermöglichen den schnellen Wechsel der geöffneten Reiter/Tabs.
- Schließen geöffneter Reiter/Tabs ist direkt über das Dropdown-Menü des Reiters möglich.
- Jobschritte für mobile Geräte und industrielle Steuergeräte können kopiert und eingefügt werden.
- Die bMC kann mittels des Kommandozeilenparameters `/language=de-DE` auf Deutsch oder `/language=en-US` auf Englisch gestartet werden.
- Alle zuletzt geöffneten Reiter/Tabs und Ansichtseinstellungen können mittels des Kommandozeilenparameter `/resetUserSettings` zurückgesetzt werden.
- Unter `Status – Serverstatus – Neustart planen` kann der Neustart des bServer zu einem bestimmten Zeitpunkt geplant werden.

- Bugfix: Wird der Import eines bDX-Containers abgebrochen, so informiert ein Dialogfenster dennoch über einen erfolgreichen Import.

- Bugfix: Ist in den Eigenschaften einer `Software – Applikation` unter `Datei` ein Ordner konfiguriert, welcher nicht existiert, so wird bei der Jobausführung keine Fehlermeldung ausgegeben, wenn die Einstellung `lokal kopieren` verwendet wird.

1.7.3 OS-Install

- Bugfix: Der Bootvorgang über TFTP arbeitet in manchen Umgebungen sehr langsam oder bricht ganz ab.

1.7.4 Mobile Devices

- Variablen für mobile Geräte werden jetzt unter `Konfiguration – Variablen – Neu – Variable (Mobile, Netzwerk, Industrie)` angelegt.

- Unter `Konfiguration – Variablen` steht bei einer Variablen als `Bereich` die Auswahl für `Mobiles Gerät` nicht mehr zur Verfügung. Bestehende Variablen werden automatisch konvertiert.

- Der bisher zur Verfügung stehende Variablentyp `Zertifikat` im Bereich `Mobile Geräte` wurde entfernt. Um diese Funktionalität weiterhin zu nutzen, können die Variablentypen `Passwort` oder `Zeichenkette` verwendet werden. Hierzu wird das Zertifikat Base64-enkodiert eingelesen. Über den Bereich `Zertifikatsverwaltung` können Zertifikate eingebunden sowie über Profilbausteine an die Geräte verteilt werden. Bestehende Variablen werden auf den Typ Zeichenkette migriert.

- Für Android Enterprise-Geräte kann beim Enrollment erzwungen werden, dass eine mobile Datenverbindung verwendet wird (Modi: vollständig verwaltetes Gerät, zweckbestimmtes Gerät).

- Android-App-Installation ist nun „forciert". Solche Apps können vom Endgeräte-Benutzer nicht mehr manuell gelöscht werden.

- Jobs für iOS/macOS-Geräte werden nun erneut gepusht, wenn ein Jobschritt länger als 15 Minuten ohne Reaktion bleibt.

- Android Enterprise: Der Administrator kann nun über das integrierte „Managed Google Play Store iFrame“ seine Apps verwalten. Dazu gehört auch das Hochladen von

WebApps/Private Apps sowie das Verwalten von Collections bzgl. der Google Play Store-Ansichten auf den Endgeräten.

- Android Enterprise-Geräte erhalten erst 2 Minuten nach erfolgreichem Enrollment vorhandene automatische Jobzuweisungen.
- Bei Änderungen an einer Whitelist, welche einem Google Play Store-Benutzer zugewiesen ist, ist nun eine Bestätigung erforderlich, da auch die App-Sichtbarkeiten der verknüpften Benutzer geändert werden.
- Für Android Enterprise-Geräte kann nun der automatische App-Update-Modus pro App konfiguriert werden (siehe App-Installations- und App-Konfigurations-Jobschritt).
- Bugfix: Per DEP aufgenommene Geräte werden nun korrekt mit dem registrierten Benutzer verknüpft, sodass diese auch im baramundi Kiosk korrekt angezeigt werden.
- Bugfix: iOS-Geräte installieren Apps nicht korrekt, wenn das Gerät auf das initiale Installationskommando mit „nicht jetzt“ antwortet.
- Bugfix: Die Installation von SCEP-Bausteinen funktioniert nicht ordnungsgemäß, wenn sich das Gerät im Zustand „Warte auf Benutzer-Aktion“ befindet.
- Bugfix: Das Android Enterprise Unternehmens-Enrollment mit bOLS-Lizenzen funktioniert nicht, wenn der Unternehmensname Umlaute enthält.

1.7.5 bServer

- Bugfix: Wird eine baramundi Datenbank mit gesetztem Datenbankverschlüsselungspasswort auf einem neuen System erstmalig in Betrieb genommen und wird in diesem Zuge auch ein Schemaupdate auf eine neue baramundi Version durchgeführt, so wird das Passwort nicht abgefragt und die Datenbank ist danach nicht verwendbar.

1.7.6 Argus-Connect

- Allgemeine technische Verbesserungen der Cloud-Connectoren.

1.7.7 bConnect

- Bei Get-Anfragen gegen den VariableDefinitions-Controller in der Version 1.1 in Verbindung mit der Verwendung der Variablen-ID als Parameter wird der Scope der ehemaligen Variablen „MobileDevice“ im neuen Multiscope-Format zurückgegeben. Ältere Versionen dieses Controllers sind hiervon nicht betroffen.

- Der Benutzername wird nun bei allen Anfragen im Log hinterlegt.

1.7.8 Defense Control

- In einigen Netzwerkszenarien wird IP-Helper verwendet, um den Netzwerkbroadcast wie er z.B. für PXE-Boot verwendet wird, so zu konfigurieren, dass nicht für jedes Netzwerk ein eigener PXE-Server notwendig ist. Der Bitlocker-Netzwerkunlock unterstützt jetzt diese IP-Helper Szenarien.

1.7.9 macOS

- Bugfix: macOS-Geräte installieren Apps nicht korrekt, wenn das Gerät auf das initiale Installationskommando mit „nicht jetzt“ antwortet.

1.7.10 bDX Im/Export

- Beim bDX-Import von Windows-Applikationen werden nun die in der Datenbank bereits vorhandenen identischen Applikationen überschrieben. Damit werden u.A. auch Änderungen der Abhängigkeiten aktualisiert.

1.7.11 baraDIP

- Es werden nur noch TLS 1.2 und 1.3 Verbindungen zugelassen.
  Hinweis: Windows XP Clients können daher keine Dateien über bBT mehr herunterladen.

1.8 Systemanforderungen und Kompatibilität

1.8.1 baramundi Management Server und baramundi PXE Relay

- Unterstützte Plattformen: siehe 1.8.17 (Spalte bMS)
- .NET 4.7.2, sowie .NET Core Runtime 3.1. x64 wird vorausgesetzt.
- Unterstützt werden die Sprachen Deutsch und Englisch.
- Es wird empfohlen einen dedizierten Server für den Betrieb des baramundi Management Servers zu verwenden.
- Für den baramundi Management Server müssen bestimmte Ports verfügbar sein[1].
- Eine Einbindung in eine Windows Domäne - Windows Active Directory wird empfohlen.
- Hardwareanforderungen Server/Netzwerk:
    - Verfügbarer Arbeitsspeicher: mindestens 8 GB; empfohlen 16 GB
    - Prozessor: mindestens 2 Kerne
    - Speicherplatz zur Installation der bMS: mindestens 5 GB
    - Netzwerkkarte: Mindestens 1 Gigabit

1.8.2 Datenbankanbindung

- Unterstützte Plattformen:
    - SQL Server 2019
    - SQL Server 2017
    - SQL Server 2016 SP3
    - SQL Server 2014 SP3
    - Oracle 19c
- Mindestens 10 GB Festplattenplatz für die baramundi Datenbank.
- Der baramundi Management Server ist ein datenbankorientiertes System, daher ist auf ausreichend Performance der Datenbank und eine performante Anbindung zu achten.
- Bei Umgebungen bis zu 250 Clients kann die SQL Express Edition verwendet werden.
- Ein Betrieb des Datenbankservers und des baramundi Management Server auf einem System ist zulässig. Bei höheren Anforderungen und größeren Umgebungen wird ein eigenständiger Datenbankserver empfohlen.

[1] Eine Liste der am Server genutzten Ports steht in unserer Online-Hilfe https://docs.baramundi.com zur Verfügung.

1.8.3 baramundi Management Center

- Unterstützte Plattformen für das baramundi Management Center, sowie die Add-Ons Automation Studio, License Management, Remote Control und ImageMount: siehe 1.8.17 (Spalte bMC).
- .NET 4.7.2 wird vorausgesetzt.
- Bildschirmauflösung:
  - Mindestbildschirmauflösung 1024 x 768 Pixel.
  - Empfohlen wird eine Auflösung von 1280 x 800 Pixel oder höher.
  - Alle Auflösungen beziehen sich auf eine Schriftgrößendarstellung von 100%.

1.8.4 baramundi OS-Customization Tool

- Dieses per Managed Software bereitgestellte baramundi Management Center Add-On zur Anpassung von Windows 10 Images wird auf den in MSW ersichtlichen Plattformen unterstützt.
- .NET 4.7.2 wird vorausgesetzt.
- Zur Anpassung der Windows Images ist das Microsoft ADK für Windows 11 erforderlich.

1.8.5 baramundi DIP

- Unterstützte Plattformen: siehe 1.8.17 (Spalte bDIP).
- .NET 4.7.2 wird vorausgesetzt.
- Empfohlen wird zusätzlicher Festplattenspeicherplatz:
  - 10 GB für Applikationen
  - 90 GB für Managed Software (MSW)
  - 6 GB für jedes Betriebssystem, das mit dem Modul baramundi OS-Install verteilt werden soll
  - 400 GB für Patchdaten, wenn offline Patch Management eingesetzt werden soll.

1.8.6 baramundi Gateway

- Unterstützte Plattformen: siehe 1.8.17 (Spalte bGW)
- .NET 4.7.2 wird vorausgesetzt.

- Es wird empfohlen das baramundi Gateway nicht zusammen mit anderen Diensten auf dem gleichen System zu betreiben.
- Eine Einbindung in ein Active Directory ist nicht notwendig.

Hardwareanforderungen Server/Netzwerk:

- Verfügbarer Arbeitsspeicher: mindestens 4 GB; empfohlen 8 GB
- Speicherplatz zur Installation der bMS: mindestens 1 GB
- Netzwerkkarte: Mindestens 1 Gigabit

1.8.7 baramundi OS-Install

- Zur Anpassung der Windows Images ist das Microsoft ADK für Windows 11 erforderlich.
- Das ADK steht in Managed Software zur Verfügung.

1.8.8 baramundi License Management

- Die Ablage von Lizenzdokumenten in der Datenbank kann großen Speicherbedarf auf dem Datenbankserver verursachen.
- Der MS-SQL Express Datenbankserver ist von Microsoft auf 10 GB Datenbankgröße begrenzt, daher wird die Verwendung für baramundi License Management nicht empfohlen.
- baramundi License Management unterstützt die folgenden Browser, jeweils in der aktuellen Version:
  - Microsoft Edge
  - Google Chrome
  - Mozilla Firefox

1.8.9 baramundi Virtual

- Unterstützte Plattformen:
  - VMware vSphere vCenter 6.0, 6.5
  - VMware vSphere Hypervisor 6.0, 6.5
- Hinweis: bVirtual ist nicht kompatibel mit VMware vSphere v6.5 Update 1 oder höher.
- Auf dem baramundi Server werden folgende Komponenten benötigt:
  - Powershell in der Version 4 oder 5 oder 5.1
  - VMware PowerCLI 6.5 Release 1

1.8.10 baramundi Schnittstellen

- bConnect steht in der Version 1.1 zur Verfügung.
- Deprecated - Die Schnittstelle bMOL (baramundi Management Object Language) wird nicht mehr weiterentwickelt. Wir empfehlen die Umstellung und Verwendung von unserer Schnittstelle bConnect.
- Deprecated – Die Schnittstelle httpMOC wird nicht mehr weiterentwickelt. Wir empfehlen die Umstellung und Verwendung von unserer Schnittstelle bConnect.
- Deprecated – Der direkte Zugriff auf die Datenbank (SQL/Oracle) wird nicht unterstützt. Wir empfehlen die Umstellung und Verwendung von unserer Schnittstelle bConnect.

Deprecated: Es erfolgen keine Featureupdates und Bugfixes mehr. Kritische Sicherheitsupdates werden für die aktuelle Version zur Verfügung gestellt.

1.8.11 baramundi Network Devices

- Der Networkscanner ist ein Add-On zum Windows bMA. Es steht allen Kunden über Managed Software zur Verfügung.
- .NET 4.7.2 wird vorausgesetzt.
- Unterstützte Plattformen: siehe 1.8.17 (Spalte bND)

1.8.12 baramundi OT Devices

- Datenerfassung erfolgt per SNMP Version1, Version2c, Version3
- Unterstütze Plattformen: Siemens SIMATIC S7 1200 und 1500

1.8.13 baramundi Kiosk

- Unterstützte Plattformen: siehe 1.8.17 (Spalte bMA)
- Zur Benutzeranmeldung und Jobzuordnung auf Benutzer-Basis ist ein Windows Active Directory inklusive eingerichtetem baramundi AD-Sync notwendig.
- baramundi Kiosk unterstützt die folgenden Browser, jeweils in der aktuellen Version:
  - Microsoft Edge
  - Google Chrome
  - Mozilla Firefox

1.8.14 Unterstützung von Android

- Unterstützte Versionen:
    - Android Enterprise 12
    - Android Enterprise 11
    - Android Enterprise 10
    - Android Enterprise 9
    - Android Enterprise 8
    - Android Enterprise 7
    - Android Version 4.0.4. bis Version 9 mit Legacy Agent
    - Samsung KNOX auf Android Version 4.0.4 bis Version 9 mit Legacy Agent

1.8.15 Unterstützung von iOS

- Unterstützte Versionen:
    - iOS Version 15
    - iOS Version 14
    - iOS Version 13
    - iOS Version 12
    - iOS Version 11
    - iOS Version 10
    - iOS Version 9

1.8.16 Unterstützung von macOS

- Unterstützte Versionen:
    - macOS 12.x (Monterey)
    - macOS 11.x (Big Sur)
    - macOS 10.15 (Catalina)
    - macOS 10.14 (Mojave)
    - macOS 10.13 (High Sierra)
    - macOS 10.12 (Sierra)
    - Mac OS X 10.11 (El Capitan)
    - Mac OS X 10.10 (Yosemite)
    - Mac OS X 10.9 (Mavericks) (64 Bit)
    - Mac OS X 10.8 (Mountain Lion) (64 Bit)
    - Mac OS X 10.7 (Lion) (64 Bit)

1.8.17 Unterstützung von Windows

- bMS/R: baramundi Management Server, baramundi PXE Relay
- bMC: baramundi Management Console,
  inclusive bRemote, ImageMount und License Management AddOn
- bAS baramundi Automation Studio
- bGW: baramundi Gateway
- bDIP: baramundi DIP, bBT und DipSync Dienst
- bMA: baramundi Agent für Windows
- bND: baramundi Networkscanner als Add-On zum Windows bMA
- X: Vollständig unterstützt.

Plattformbezeichner	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows Server 2022 Standard/Datacenter (Desktopdarstellung)	X	X	X	X	X	X	X
Windows Server 2019 Standard/Datacenter (Desktopdarstellung)	X	X	X	X	X	X	X
Windows Server 2016 Standard/Datacenter (Desktopdarstellung)	X	X	X	X	X	X	X
Windows 11 Pro / Enterprise (N)		X	X		X	X	X
Windows 10 Pro / Enterprise 21H2 (N) (32 Bit und 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 21H1 (N) (32 Bit und 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 20H2 (N) (32 Bit und 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 2004 (N) (32 Bit und 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 1909 (N) (32 Bit und 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 1903 (N) (32 Bit und 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 1809 (N) (32 Bit und 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 1803 (N) (32 Bit und 64 Bit)		X	X		X	X	X
Windows 10 Pro / Enterprise 1709 (N) (32 Bit und 64 Bit)		X	X		X	X	X
Windows 10 Enterprise 2021 LTSC (32 Bit und 64 Bit)		X	X		X	X	x
Windows 10 Enterprise 2019 LTSC (32 Bit und 64 Bit)		X	X		X	X	X

Plattformbezeichner	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows 10 Enterprise 2016 LTSB (32 Bit und 64 Bit)		X	X		X	X	X
Windows 10 Enterprise 2015 LTSB (32 Bit und 64 Bit)		X	X		X	X	X

1.8.18 Unterstützung von Windows mit Einschränkungen

Diese Betriebssysteme werden von den baramundi Komponenten, inklusive aller baramundi Managed Software, nur eingeschränkt unterstützt. Das kann bedeuten, dass neue Funktionen auf diesem Betriebssystem nicht nutzbar sind, oder dass Funktionen nicht mehr wie bisher verwendet werden können. Aufgrund der Komplexität und Vielzahl der Altsysteme kann baramundi die Funktionalität auf diesen Systemen nicht gewährleisten. Aufgrund der Einschränkungen empfehlen wir den Einsatz modernerer Betriebssysteme. Auf Betriebssystemen, welche außerhalb des Mainstream Supports von Microsoft sind, können wir keine Unterstützung der baramundi Serverkomponenten mehr leisten (bMS/R, bMC, bAS, bGW, bDIP).

- (1): Wird nur noch eingeschränkt unterstützt, da Microsoft den (grundlegenden) Produkt-Support beendet hat.
- (2): Für dieses Betriebssystem muss der bMA in Version 2021 R2 verwendet werden. Ein aktuellerer bMA kann auf diesem Betriebssystem nicht ausgeführt werden. Für den bMA 2021 R2 wird es keine Sicherheitsverbesserungen mehr geben.

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

1.8.19 Sprachen

Das baramundi Management Center, baramundi License Management sowie das Automation Studio sind in folgenden Sprachen verfügbar:

Deutsch, Englisch

Der bMA für Windows-Clients unterstützt Benutzernachrichten in folgenden Sprachen:

Deutsch, Englisch, Bulgarisch, Chinesisch, Dänisch, Finnisch, Französisch, Griechisch, Italienisch, Niederländisch, Norwegisch, Polnisch, Portugiesisch, Rumänisch, Russisch, Schwedisch, Slowakisch, Spanisch, Türkisch, Tschechisch, Ungarisch

Der baramundi Kiosk unterstützt die folgenden Sprachen:

Deutsch, Englisch, Polnisch

Weitere Sprachen können durch den Administrator hinzugefügt werden.

Für alle serverseitigen Dienste (d.h. baramundi Management Server, baramundi Gateway, DIP) werden folgender Sprachen unterstützt:

Deutsch, Englisch

1.9 Bekannte Einschränkungen

1.9.1 Windows Agent (bMA) Hinweis für Windows XP

- Die Weiterentwicklung des bMA für Windows XP wurde eingestellt.
- Es ist möglich Windows XP mit dem bMA der Version 2021 R2 weiterhin zu betreiben. Der bMA 2021 R2 ist für diesen Zweck mit der bMS 2022 R1 (und höher) kompatibel und freigegeben.
- Die Features OS-Install und automatisches bMA Deployment stehen nicht mehr zur Verfügung. Der bMA muss ggf. manuell installiert werden.
- Hinweis: Da auf Windows XP kein aktueller bMA verwendet werden kann, sind auch neue Sicherheitsupdates für den bMA nicht verfügbar.

1.9.2 Hinweise zur Änderung Zugriff bMA.log (ab 2021 R2)

- Zum Zugriff auf die `bMA.log` Datei werden lokale Administrations-Rechte benötigt. Beachten Sie hierzu auch die folgenden Anmerkungen.
- Bereits vorhandene Rollover-bMA*.log Dateien werden nicht neu berechtigt.
- Die bMC-Aktion `Management Agent Log` unter `Benutzerdefinierte Clientbefehle` ist in den meisten Umgebungen nicht mehr verwendbar und sollte entfernt werden. Der Zugriff von der bMC aus auf das bMA.log kann über den benutzerdefinierten Clientbefehl `Explorer Drive C` erfolgen, hier kann der für den Client notwendige Benutzer mit lokalen Administrationsrechten angegeben werden.
- Da lokale Benutzer meist keine lokalen Administrationsrechte besitzen, sollte der bMA `Menüpunkt "Logdatei einsehen"` unter `bMC – Einstellungen – Server – Management Agent` deaktiviert sein.
- Falls der Zugriff auf das bMA.log angepasst werden soll, können die Rechte über die bDS Funktion `Berechtigungen bearbeiteten – Zugriffsrechte hinzufügen` ergänzt werden.

1.9.3 Allgemein

- Hinweis: Für Kiosk und bLM wird der Internet Explorer nicht mehr unterstützt.

- Hinweis: Die bMS Version ab 2020 R2 kann mit bMA älter Version 2019 R2 nicht mehr kommunizieren.
- Hinweis: Der Betrieb des bServers auf Windows Server 2008 R2 wird ab 2021 R2 nicht mehr unterstützt.
- Die bMA-Version muss der Server-Version entsprechen. (Ausnahme Windows XP)
- Bei Änderung des Default Webserver Port für den baramundi Server ist OS-Install und OS-Cloning, sowie Imaging nicht mehr möglich.

1.9.4 Management Center (bMC)

- Hinweis: Aus Sicherheitsgründen wird empfohlen, auf den Knoten `bMC – Erweiterungen -Reporting` nur vertrauenswürdige Personen/Gruppen zu berechtigen. Wir empfehlen hier ausschließlich das Sicherheitsprofil `Administration` zu berechtigen.
- In den `benutzerdefinierten Befehlen` stehen die veralteten Aliase `KitsServer`, `Depot`, `BDPPath` und `BaramundiPath` nicht mehr zur Verfügung.
- Die Information am Windows Endpunkt zum `Servicing Channel` wird seit Windows 10 mit der Release-ID 1903 nicht korrekt angezeigt. Microsoft hat für die Felder `Servicing Channel`, `Verzögerung von Funktionsupdates` und `Funktionsupdate-Version` die Möglichen der Konfigurationen reduziert und seit der Release-ID 21H2 komplett entfernt. Diese Felder haben somit keinen Mehrwert mehr und werden in einer kommenden baramundi Release entfernt.

1.9.5 Inventur

- Hinweis: Die veraltete Softwareinventur wird ab der Version 2022 R2 nicht mehr unterstützt. Wird diese noch verwendet, so zeigt die bMC einen Hinweistext dazu an.
- Die optionale Offline-Inventur verwendet kein PreInvent.bds und unterstützt damit MSW nicht komplett.

1.9.6 Server (bServer)

- Die Module unter `Serverstatus-Cloud Connector` sind nur aktiv, wenn das Argus Cockpit konfiguriert ist und die Konnectoren installiert worden sind.

- Auf dem baramundi Server darf keine Software installiert sein, welche die CodeMeterRuntime von Wibu verwendet.
- Die AD-Synchronisation wird in Netzen, in denen das primäre DNS-Suffix vom DNS-Domänennamen abweicht, nicht unterstützt.
- Wechselt ein Client von einem IP-Netzwerk, in dem keine Jobs ausgeführt werden dürfen, in ein Netz, in dem die Jobausführung möglich ist, läuft der Job erst nach bis zu 60 Minuten los.
- Wechselt ein Client von einem IP-Netzwerk, indem Jobs ausgeführt werden dürfen, in ein Netz, indem keine Jobausfühung konfiguriert wurde, so kann trotzdem eine Jobausführung erfolgen, da evtl. die Prüfung nach dem IP Netzwerk schon vom bServer durchlaufen wurde.
- Der Management Server arbeitet Jobausführungen parallel ab und verwendet dabei zur Kommunikation mit dem Datenbankserver viele Datenbankverbindungen. Insbesondere bei Oracle-Datenbanken sollte darauf geachtet werden, eine ausreichend große Menge an Sessions und Prozessen konfiguriert zu haben.
- Unter Oracle wird die optionale Angabe eines eigenen Tablespace für Indizes im DB-Manager nicht für alle Tabellen beachtet. Sowohl bei neu angelegten wie auch von früheren Versionen aktualisierten Datenbanken werden einige Indizes im regulären Benutzer-Tablespace angelegt.
- Wird der bServer angehalten während noch Nachrichten in seiner Warteschlange stehen, werden diese verworfen. Werden viele Jobs gleichzeitig ausgeführt, sollte der bServer nicht beendet werden, es können sonst Jobzustände verloren gehen.
- Bei Jobschritten, die dynamisch weitere Jobschritte generieren, wie z.B. Patch- oder MSW-Scans, funktioniert das "Fortsetzen" bzw. "Neu planen" im Fehlerfall nicht.

1.9.7 Argus Cloud Connectoren

- Hinweis: Damit der `baramundi Cloud Connector Dynamic Groups` die gewünschten `Universellen Dynmischen Gruppen` (UDG) nach Argus synchronieren kann, muss der unter `Konfiguration-Schnittstellen-Cloud Verbindung` hinterlegte bConnect Benutzer an den UDG mindestens Leseberechtigungen haben.

- Der beim Downloader hinterlegte Proxy wird nicht berücksichtigt. Ein Proxy kann über die .config Datei konfiguriert werden. Diese Konfiguration wird beim Update ggf. überschrieben und muss neu gesetzt werden.

1.9.8 PXE-Boot

- Es ist das von baramundi empfohlene ADK zu verwenden.
- Die Verwendung der PXE Option „PXE-Unterstützung – Bootloader – baramundi Syslinux Bootloader“ kann dazu führen, dass Clients beim Booten von der Festplatte festhängen. Für dieses Problem steht im baramundi Anwenderforum ein Lösungsweg bereit: https://forum.baramundi.de/index.php?threads/5339.

1.9.9 Windows Agent (bMA)

- Über Profile des Energy Management angewendete Energieoptionen werden unter Windows in den Systemeinstellungen - Energieoptionen unter Umständen nicht korrekt angezeigt. Eine Abfrage der Einstellung auf der Kommandozeile liefert die korrekten Werte und diese werden vom System auch verwendet.
- Ist der `Nicht stören` Modus am Client aktiv, so können auch Jobs, welche beim Herunterfahren ausgeführt werden sollen nicht korrekt zugewiesen werden. Die Jobs werden dann beim Herunterfahren nicht ausgeführt.
- Ist auf dem Client ein Job für den Herunterfahrzeitpunkt bereits vorgesehen und setzt der Anwender danach den `Nicht stören` Modus, so wird der Job beim Herunterfahren u.U. erst nach einer Wartezeit ausgeführt. Die Wartezeit entspricht dann dem unter `bMC – Konfiguration – Server – Einstellungen – Jobausführung` eingestellten `Intervall für Verbindungsversuche zu Clients (Minuten).`
- Hinweis: Backupdateien welche mit Disaster Recovery einer bMS 8.5 oder älter erstellt wurden, können ab Version 2020 R1 nicht mehr zurückgespielt werden.
- Hinweis: Neu eingeführte Jobschritte, wie `Bitlocker Network Unlock` oder `Microsoft Updates inventarisieren`, werden bei der Jobausführung nicht berücksichtigt, wenn ein veralteter bMA auf dem Zielsystem installiert ist.
- In Version 2020 R1 gab es Änderungen an der bDS-Engine bei der Verwendung von eingebetteten Skriptsprachen, welche in sehr seltenen Fällen bei Ausführung zu Skriptabbruch mit der Fehlermeldung "`Verwendung einer veralteten Syntax: Der`

`Ausdruck {=VBScript} wird nicht mehr unterstützt."` führen. Eine Konvertierung durch das Automation Studio ist nicht ausreichend, eine manuelle Anpassung der betroffenen Skripte ist notwendig. Weitere Infos finden Sie im Forum unter: https://forum.baramundi.de/index.php?threads/10458

- Wird ein manuell angepasstes bMA Installationskommando verwendet, so muss dieses an das neue Setupformat manuell angepasst werden. Der Standart ist: `"\\{Server}\BMS$\Client\Setup\ManagementAgent_setup.exe /Q SERVER={Server} SERVERKEY="{ServerKey}" OPTIONS={AgentOptions}".`
- Windows 10 Virtual Desktop Edition wird als Server 2016 erkannt.
- Die HW-Inventur verwendet eine SHA256 Treibersignatur und ist damit auf XP, Server 2008 und Vista nicht lauffähig. Bei Windows 7 wird KB3033929 benötigt.
- Die Tastatur- und Maussperre kann bei Betriebssystemen kleiner Windows 8 Toucheingaben nicht sperren.
- Die Tastatur- und Maussperre kann die Bildschirmrandgesten nicht unterdrücken. Eine Bedienung der Apps oder der Charmbar ist aber gesperrt.
- (Patch-)Jobs mit WakeOnLan (WOL) fahren nach Beendigung des Jobs den Client nicht herunter, wenn der Job einen Reboot durchgeführt hat.
- Der Sicherheitskontext "Lokaler Installationsbenutzer" kann bei Systemen mit der Rolle "Domain Controller" nicht verwendet werden.
- Die Datei-Inventur meldet bei sehr großen Dateien (> 2GB) immer eine Dateigröße von 2GB.

1.9.10 Automation Studio

- Hinweise zu bDS-Dateien ab Version 2020 R1:
  - Beim Öffnen einer bDS-Datei wird auf eine notwendige Konvertierung in das neue Format hingewiesen. Ein konvertiertes Skript kann nur von bMAs der Version 2020 R1 oder höher ausgeführt werden.
  - In Umgebungen mit mehreren baramundi Servern ist darauf zu achten, dass bDSSkripte erst konvertiert werden, wenn alle Server/Clients auf der Version 2020 R1 oder höher sind. Falls eine Konvertierung in das neue Format noch

nicht gewünscht ist, kann das Automation Studio der Version 2019 R2 weiterhin verwendet werden.

- Der bMA ab 2020 R1 kann sowohl das neue bDS-Format, wie auch das bisherige Format ausführen. Eine Konvertierung aller bDS-Skripte ist nicht notwendig.

1.9.11 Defense Control

- Bei Jobs die direkt ins WinPE booten, kann der BitLocker nicht pausiert werden.
- Voraussetzung ist Windows 10 1511 oder neuer.
- Ein aktivierter TPM 2.0 wird benötigt.
- Verbundene iSCSI Laufwerke werden bei Laufwerksverschlüsselungstyp "Vollständige Verschlüsselung" ebenfalls mit verschlüsselt.
- Die Funktion Systemstart-PIN muss über eine Gruppenrichtlinie eingestellt werden. GPO "Require additional authentication at startup".

1.9.12 Mobile Devices

- Die baramundi SCEP-Verteilung unterstützt keine automatische Verlängerung von Zertifikaten. Neue Zertifikate können durch eine erneute Profilinstallation verteilt werden.

1.9.13 Mobile Devices – Android Enterprise

- Bei App Installations- und Konfigurationsjobs für mobile Geräte wird bei sehr großen App Konfigurationen (z.B. Zebra OEMConfig) im Anzeigemodus ein sperrender Ladevorgang durchgeführt.
- Geräte mit gesetztem Entsperrcode führen nach einem Neustart des Gerätes Jobs erst aus, wenn der Entsperrcode korrekt eingegeben wurde. Dies gilt auch wenn der Entsperrcode nur für das Arbeitsprofil gesetzt ist und dieses aus vom Pausemodus wieder aktiv geschalten wird.
- Ab Android 10 ist keine Inventur und keine Deinstallation von Wifis möglich, wenn der Standortzugriff für das Gerät bzw. das Arbeitsprofil deaktiviert ist.

- Work Profile: Ab Android 9 funktioniert das Teilen von Dateien im Arbeitsprofil über Bluetooth nicht.
- Die Displaysperre bei Android Enterprise funktioniert erst ab Android 9.
- Mit der baramundi Eval-Lizenz ist es nicht möglich, ein Unternehmen zu verknüpfen. Dazu wird eine vollwertige bMS Lizenz benötigt.
- Ist beim Enrollment des Gerätes der bServer/bGateway nicht erreichbar, so kann dieser Vorgang nur durch „Rücksetzen auf Werkseinstellung“ verlassen werden.
- Bei Huawei Geräten mit nicht erfüllter Passwortrichtlinie können Apps nicht zuverlässig versteckt/gesperrt werden.

1.9.14 Mobile Devices – Android

- Ab Android Version 9 können keine statischen IPs in eimen Wifi-Profilbaustein gesetzt werden.
- Das Benutzerfeld bei der WLAN Konfiguration von TLS wird nicht unterstützt.
- Die Operationen Passwort-setzen/zurücksetzen funktionieren ab Android 7 nicht mehr.
- Für Samsung Knox Geräte < Version 4.2.2 muss die Samsung Knox Extension via Job verteilt werden. Die App wurde aus dem Google PlayStore entfernt.
- Auf Samsung-Geräten mit Android >= 4.2 erscheint bei Neuinstallation der baramundi Apps durch einen neuen Aktivierungsmechanismus (Samsung ELM) während der ersten Jobausführung nach dem Enrollment ein zusätzlicher Dialog mit den Nutzungsbedingungen des ELM Service. Dieser muss einmalig vom Benutzer bestätigt werden, damit eine weitere Jobausführung möglich ist.
- Für Enterprise-Wifi mit Clientzertifikaten ist unter Android eine Displaysperre notwendig (PIN, Muster, etc…).
- Bei Enterprise-Wifi auf Samsung-Geräten < Android 5.0 (Lollipop) muss das Wifi Profil zusammen mit dem Root-Zertifikat des Access Points mitinstalliert werden. Die Verknüpfung mit dem Zertifikat erfolgt im Wifi Profil. Ohne das Root-Zertifikat scheitert die Verbindung, da keine Vertrauensstellung zwischen dem Samsung Gerät und dem Access Point hergestellt werden kann. Es folgt dann eine unspezifische Fehlermeldung

- Bei Samsung Geräten mit Android 4.3 hinterlässt die Deinstallation eines Wi-Fi Profils mit TLS unbrauchbare Reste des Clientzertifikats auf dem Gerät. Die weitere Verwendung ist aber nicht möglich.

- Hinweise zu SCEP auf Android: Die Installation einzelner Clientzertifikate über SCEP ohne Bindung an einen weiteren Baustein wie Wifi oder Exchange wird nur auf Samsung Knox Geräten unterstützt. Auf Nicht-Samsung-Geräten wird SCEP nur in Verbindung mit Enterprise Wifi (TLS) ab Android 4.3 unterstützt.

- Damit die Enrollment-Links in der E-Mail-Applikation unter Android korrekt funktionieren, sollte der Haken "Überprüfung der Serveridentität bei der ersten Verbindungsaufnahme aktivieren" in der bMD-Konfigurationsseite gesetzt sein.

1.9.15 Mobile Devices – iOS

- Die Option „Von Gerät zu Gerät migrieren“ bei Apple DEP arbeitet nicht korrekt.

- Hinweis: Die automatische VPP-App Aktualisierung ist mit iOS14 nicht möglich. Dieser Bug wurde von Apple in der Version iOS 14.2 behoben.

- Der bServer muss auf einem Windows Server 2016 oder höher betrieben werden um iOS-Geräte verwalten zu können.

- Folgende Restriktionen sind ab iOS 13 nur noch im supervised Mode nutzbar: "Kamera erlauben", "Backup verbieten", "Anstößige Inhalte verbieten", "Safari automatisches Ausfüllen verbieten", "Safari verbieten".

- Ab iOS 13 sind Geräte immer supervised, unabhängig von der Konfiguration im Enrollment-Profil.

- Ab iOS 13 ist die Profil-Installation auf Geräten immer verpflichtend, unabhängig von der Konfiguration im Enrollment-Profil.

- Nach dem Enrollen eines iOS Gerätes kann es mehrere Minuten dauern, bis der Agent auf dem bMD Gerät das Enrollment erkennt.

- Der iOS App Push setzt voraus, dass auf jedem iOS-Gerät der Agent einmal manuell gestartet wird und sein Token an seinen bMS übermitteln kann. Insbesondere bei älteren Gerätegenerationen, wie zum Beispiel dem iPad 2, können trotz regelmäßiger Pushes mehrere Tage zwischen den Kontakten des bMD Agents vergehen, wenn diese

Geräte nicht benutzt werden. Nach dem Einspielen eines Geräte-Backups (iTunes, iCloud) ist es unter Umständen erforderlich, die bMD Agent-App einmal manuell zu starten.

- Aufgrund von Einschränkungen in der Apple iOS Hintergrundaktualisierung kann es zu Verzögerungen in Compliance-Meldungen durch den Agent kommen. Abhilfe hierfür schafft gelegentliches Aufrufen des baramundi Agent.
- Das Apple Device Enrollment Program (DEP) wird erst ab iOS 8.3 unterstützt.
- Seit iOS 8.0 kann über die Apple-MDM Schnittstelle nicht mehr zuverlässig ermittelt werden, ob eine App vollständig installiert wurde. Die App wird bereits kurz nach der Bestätigung der Installation durch den Endbenutzer vom Gerät als installiert und verwaltet gemeldet. Bricht zum Beispiel der Download nach der Bestätigung geräteseitig ab und ist die App daher nicht nutzbar, wird sie trotzdem durch die Inventur als ordnungsgemäß installiert angezeigt.

1.9.16 Mobile Devices – Windows Phone

- Wird ab Release 2020 R1 nicht mehr unterstützt.

1.9.17 Management Center (bMC)

- Auf englischsprachigen Systemen arbeitet die Sortierung in der Bulletin-Auswahl eines Patchjobs (classic) nicht wie erwartet.
- Werden bei `Inventur – NetzwerkScan – Profile` UniCode Zeichen im Namen oder Kommentar verwendet, so führt das zu Fehlern bei der Anzeige bei der Joberstellung oder beim bDX Im-/Export.
- Benutzerdefinierte Spaltenkonfigurationen bei Endgeräteansichten werden beim erstmaligen Start der bMC zurückgesetzt.
- Zur Anzeige von Reports wird die Crystal Reports Version 13.0.8 benötigt. Eine neuere Version wird nicht unterstützt.
- Das Hilfesystem zeigt bei Offline-Verwendung nur eingeschränkte Inhalte.
- Unter „Konfiguration – Lizenzkonfiguration“ wird „keine Daten verfügbar“ angezeigt, wenn nicht auf die neue Lizenzierung umgestellt wurde.
- Universelle Dynamische Gruppen können in Reports nicht verwendet werden.

- bMC Benutzer ohne die Einstellung „Identität der Benutzer der Endgeräte anzeigen“ können an Clients über den Eigenschaftendialog die Benutzer der Endgeräte einsehen, wenn sie Schreibrechte am Client besitzen.
- bMC-Benutzer und Endbenutzernamen sind teilweise in Logzeilen oder bestimmten Statusmeldungen sichtbar und können dort nicht unterdrückt werden.
- Import/Export (BDX) unterstützt keine Jobs mit Schritten der Art Datensicherung, Daten aus Sicherung wiederherstellen, Energierichtlinie verteilen, Virtuelle Maschine verwalten.
- Für alle Import-Aktionen, die auf BMS$ schreibend zugreifen, sind korrekte bzw. erhöhte Rechte nötig. Zum Import von SSA oder OS-Install-Skripten ist es sinnvoll die bMC im Administratorkontext zu starten.
- Die bMC unterstützt nur die Sprachen Deutsch und Englisch. Auf Servern in anderen Sprachen muss das Sprachpaket für Englisch installiert sein.
- Der im Setup enthaltene Report „List SNMP Devices“ arbeitet nicht bei Verwendung einer Oracle Datenbank.
- Die Rechte sind an einem einzelnen Mac- oder mobilen Gerät nicht einstellbar, diese erben immer von ihrer jeweiligen OrgUnit.
- Zum Öffnen der Reports bei Verwendung von MS SQL Server muss für den MS SQL Server die Remote-Anmeldung zugelassen werden, damit Crystal Reports auf die Datenbank zugreifen kann.
- Die Store-Suche funktioniert bei Verwendung eines Proxys nur mit Proxy ohne Authentifizierung, oder mit angemeldetem AD-Benutzer.
- Neue Bearbeitungsdialoge sperren die bearbeiteten Objekte nicht. Bei einer gleichzeitigen Editierung gewinnt der Erste der speichert. Der zweite Benutzer erhält beim Versuch der Speicherung eine Fehlermeldung („Can't save stale data object“).
- Wird die bMC in einer anderen Zeitzone verwendet als sich der Management-Server befindet, so sind die Zeitangaben teilweise unterschiedlich.
- Das Revisionslog wird für folgende Aktionen aktuell nicht mehr geschrieben: Job verschieben, Job zuweisen, Jobtarget starten/fortsetzen/abbrechen/löschen, Jobtarget auf „OK“ setzen, Gruppe verschieben, Client verschieben, Clientmonitor erstellen/bearbeiten/löschen, Ausstehende Downloads für MSW und Patche löschen, Dateien und Registry-Einträge in der Inventur löschen.

1.9.18 macOS-Geräte

- Bei nativ aufgenommenen Geräten wird die IP-Adresse nicht bestimmt. Damit ist die DIP-Auflösung über IP-Netze nicht möglich.
- Je nach Einstellung im Management-Server werden über die automatische Netzwerkerkennung auch macOS-Geräte angelegt. Dies erfolgt auch dann, wenn dieses Gerät schon als macOS-Gerät erfasst wurde. Das automatisch angelegte Gerät wird wie ein Windows-Client dargestellt, kann aber nicht verwaltet werden und sollte daher deaktiviert werden.
- Auf macOS-Geräten werden Compliance-Regeln, die Jailbreak und den letzten Agent-Kontakt prüfen, ignoriert.
- Enthalten Variablen, die in Shell-Skripten verwendet werden, Shell-Kommandos, so werden diese auch ausgeführt (Command Injection). Dieses Verhalten ist gewollt und kann auch zum Skriptieren eingesetzt werden.

1.9.19 Compliance

- In benutzerdefinierten Compliance-bDS-Skripten stehen keine bMS-Variablen zur Verfügung.
- Eine dynamische Gruppe mit einem CVE Filter enthält auch ignorierte Regeln.
- Bei Verwendung einer Oracle-DB können in der Ansicht „Gruppe -Verwundbare Produkte“ in der Detailansicht Fehler auftreten, wenn sehr viele Clients oder Schwachstellen vorhanden sind.

1.9.20 bRemote

- Die Aufschaltung auf den Desktop des lokalen Installationsbenutzers ist nicht möglich.

1.9.21 Update Management (Patch Management)

- Jobschritte `Microsoft Updates verteilen` mit `Updateprofil` laufen bei Clients auf einen Fehler, wenn der Client kein Updateprofil zugewiesen hat. Ist eine Jobwiederholung im Fehlerfall konfiguriert ist dieses Fehlerbild nicht immer sofort ersichtlich.

- Nach der Neuinstallation eines Clients zeigt die Ansicht `Client-Microsoft Updates` weiterhin die Daten vor der Neuinstallation an.

- Die neue Microsoft-Klassifizierung "Upgrades" wurde in baramundi aufgenommen. Microsoft verwendet diese Klassifizierung im WSUS und Patchmanagement online noch nicht gleich, daher wird von der Verwendung aktuell abgeraten.

1.9.22 Virtual

- Das Steuern und Erstellen einer VM ist nur möglich, wenn die VMware-Lizenz das Feature „vSphere API“ beinhaltet. Das Feature „vSphere API“ ist nicht Teil der freien ESXi-Lizenz. Somit ist mit der freien ESXi-Version nur die Inventarisierung möglich.

- Bei der Inventur eines Hypervisors können die Daten des in einer virtuellen Maschine installierten Betriebssystems nur erfasst/aktualisiert werden, wenn die VM während der Inventur eingeschaltet ist sowie die VMware-Tools installiert und gestartet sind.

1.9.23 OS-Install

- Alte Systeme können ggf. mit ADK 10 nicht gebootet werden. Hierfür kann ein eigenes Bootimage mit Waik 3.1 erstellt werden. Es wird empfohlen dieses im Pfad „WAIKPE“ abzulegen.

- Das Windows 10 Inplace-Upgrade führt erst eine Systemprüfung durch und bricht bei Warnungen ab. Sollen diese ignoriert werden, kann das Verhalten im Skript InPlaceUpgrade.bds angepasst werden.

- Bei Jobs mit Inplace-Upgrade Schritten, welche zusätzlich Patch-Schritte enthalten bricht die Jobasuführung u.U. mit dem Fehler „Die Betriebssysteminstallation des Jobs [..] ist für den Client [..] nicht zugelassen“ ab.

1.9.24 Clients im Internet Modus / Dynamischen Modus

- Es ist kein automatisches Agent-Update im Job möglich.

- Wird ein IEM Client zurück auf LAN Modus geschalten, muss der bMA neu installiert werden. Dies erfolgt nicht automatisch.

- Der Client-Announce kann für Clients im Dynamischen Modus nicht deaktiviert werden. Hier zieht in diesem Fall der Standardwert von 30 Minuten.

1.9.25 Network Devices (bND)

- Wird beim SNMPv3 Scan ein Kontext angegeben, so werden einige Geräte (z.B. Cisco Catalyst Switch) nicht erkannt.
- Geräte mit mehr als einer IP-Adresse an einer MAC-Adresse werden u.U. als unabhängige Geräte erkannt und angelegt.
- Beim Scannen von HUAWEI Switches wurde beobachtet, dass diese teilweise auf mehrfache SNMP-Anfragen nicht antworten.
- Zur Ermittlung einer optimalen IT-Landkarte sollte im Netzwerk das STP (Spanning Tree Protocol) aktiviert sein.
- Hinweis: Zur Anzeige der IT-Landkarte werden die durch die Scans ermittelten Daten verwendet. Es ist keine Live-Ansicht der Netzwerkumgebung.

1.9.26 Comparex Miss Marple

- Die Namen der Reports sind auch auf englischen Systemen Deutsch.
- Der Reporting Server muss die Authentifizierung über Negotiate anbieten.
- SQL Server Reporting Services ab 2008 R2 im nativen Modus wird unterstützt.

2 Release 2021 R2

1.10 Windows Autopilot

1.10.1 Out-Of-Box-Experience (OOBE)

Schon vor dem neuen “Normal“ im Home-Office, wussten es die User zu schätzen, wenn ihnen ihre Arbeitsgeräte komplett eingerichtet zur Verfügung gestellt wurden. Plattformen wie Apple iOS oder Google Android machen es vor: Einschalten, Wifi einrichten, die Apps, Einstellungen und Zugänge kommen magisch von allein aufs Gerät und man ist sofort startklar. Ähnliches ist nun auch mit dem Windows Autopilot von Microsoft möglich.

1.10.2 Ablauf

Die User schalten lediglich ihr neues Windows-Gerät ein und melden sich mit dem Firmen-Account an. Das Gerät wird automatisch in die bMS aufgenommen und kann anschließend von den Admins wie gewohnt, mit bereits bestehenden und erprobten Jobs, verwaltet werden. So kann das Gerät beispielsweise direkt vom Hersteller zu den neuen Anwendern versendet werden. Eine Inbetriebnahme durch die Administration im Firmennetzwerk ist nicht mehr nötig.

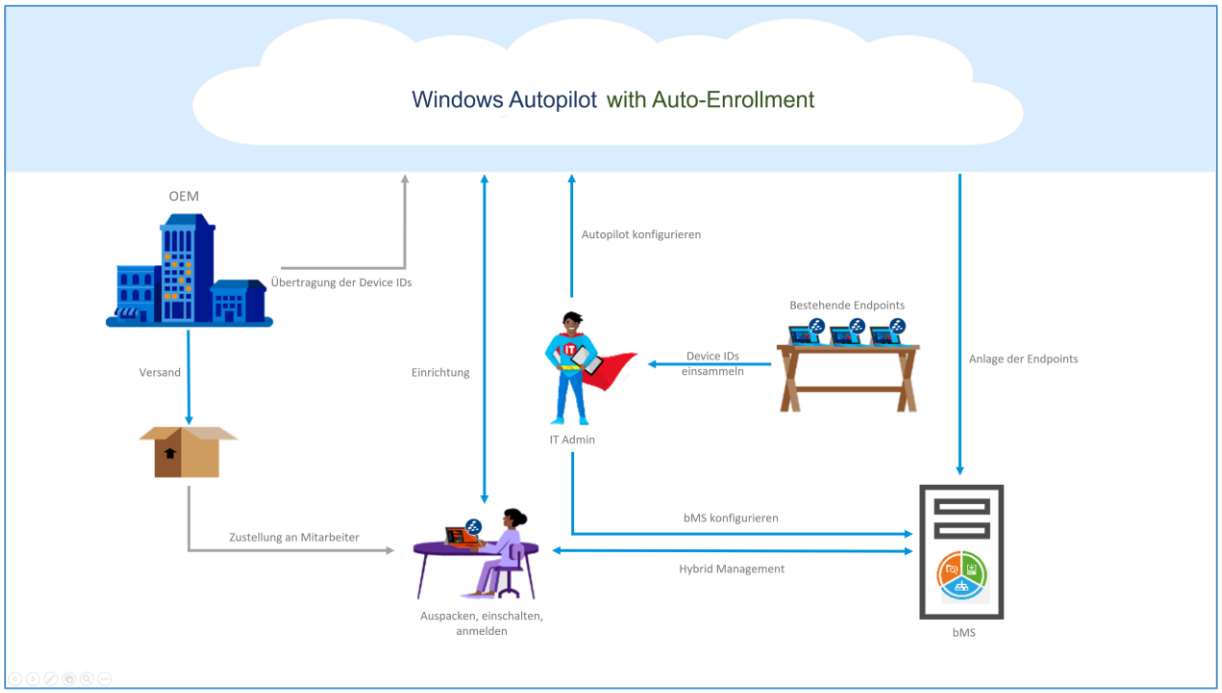


Abbildung 26 - Schematische Darstellung des Enrollmentvorgangs

Das spart unnötige Versandwege und erleichtert auch den Administratoren die Ausgabe neuer Windows Endpoints enorm. Während der automatischen Aufnahme über Autopilot wird das Gerät in der bMS angelegt und mit dem baramundi Management Agent versorgt. Dieser wird im IEM-Modus installiert und stellt über das Gateway eine sichere Verbindung zur bMS her. Das ermöglicht das Management im gewohnten Umfang: Inventarisierung, Softwareverteilung, Update Management und Vieles mehr – die bestehenden Jobs lassen sich ohne weitere Anpassung direkt weiterverwenden.

1.10.3 Voraussetzungen

Um den Windows Autopilot nutzen zu können, wird ein Azure Active Directory benötigt.
Die bMS muss von außerhalb des Firmennetzwerks per baramundi Gateway erreichbar sein.
Die Autopilot-Funktionalität wird von Microsoft erst ab Windows 10 bereitgestellt. Windows Autopilot ist eine weitere Möglichkeit initial Windows Endpunkte in die Verwaltung aufzunehmen und bedarf keiner gesonderten baramundi Lizenz.

1.10.4 Autopilot mit der bMS

Um die bMS mit dem firmeneigenen Autopilot zu verbinden, muss einmalig sowohl im Azure Active Directory (AAD) als auch in der bMS eine entsprechende Konfiguration vorgenommen werden.
Im Rahmen der Einrichtung werden im AAD mehrere Schlüssel erzeugt, welche in die bMS übertragen werden müssen.

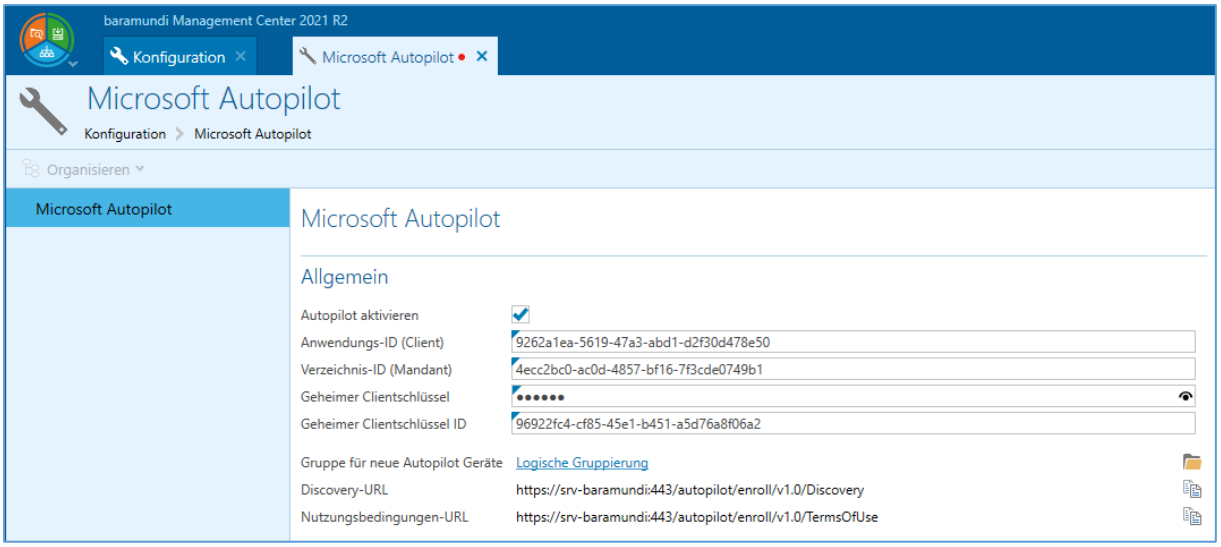


Abbildung 27 - Konfiguration der AAD Schlüssel in der bMS.

Nach Abschluss der Einrichtung ist der Autopilot direkt startklar.

1.11 Microsoft Update Management

1.11.1 Der Weg zu modernem Update Management

In der bMS 2020 R2 wurde mit der umfassenden Inventur der Microsoft Updates der Grundstein für das neue Microsoft Update Management gelegt. Mit dem Folgerelease wurden Updateprofile und damit die Möglichkeit zum gestaffelten Update Rollout eingeführt. Auch in Version 2021 R2 geht die Entwicklung konsequent weiter.

1.11.2 Updateprofile und Konformität

Updateprofile dienen nun nicht mehr nur der Freigabe/Blockierung und Verzögerung von Updates, sondern auch der Auswertung des Updatezustands – So lässt sich schnell erkennen, ob die Endpoints die Vorgaben des Updateprofils erfüllen bzw. ob alle dem Updateprofil zugeordneten Endpoints konform sind oder Handlungsbedarf besteht.

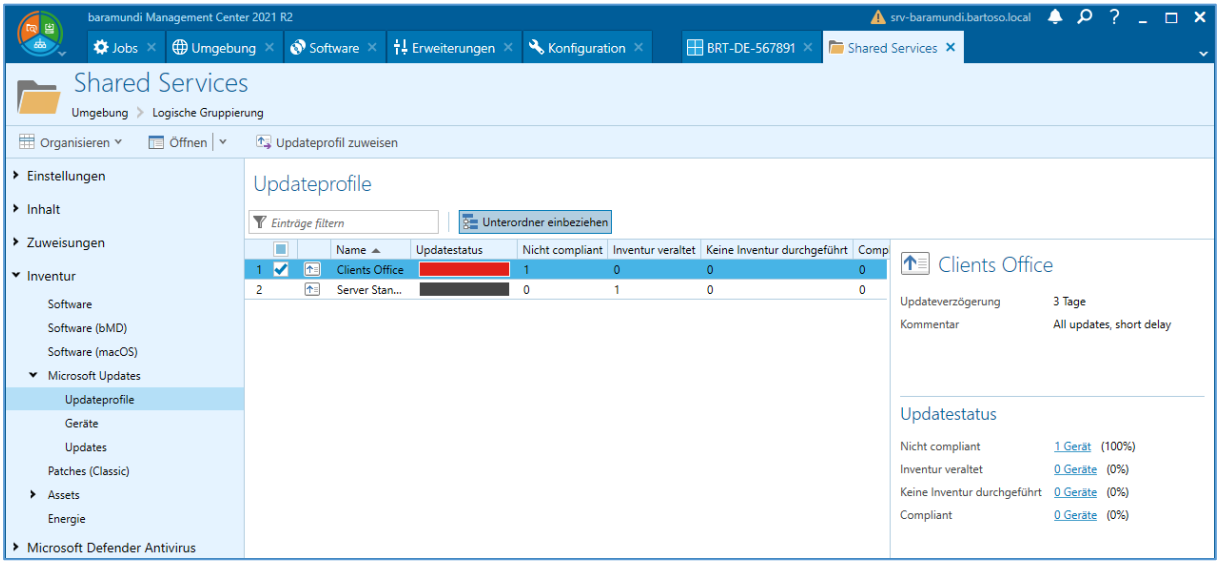


Abbildung 28 - Erfüllungsgrad der Updateprofile

Über Links in der Detailview kann auch direkt an die Liste mit den entsprechenden Endpoints gesprungen werden. Sämtliche Listen lassen sich natürlich auch direkt exportieren und weiterverarbeiten.

1.11.3 Detaillierte Übersicht über Updatezustände

Die Updatezustände der Endpoints lassen sich nun nach Gruppenzugehörigkeit anzeigen. Dabei werden sowohl die „Logischen Gruppierung“, wahlweise inklusive untergeordneter Gruppen, als auch „Universelle Dynamische Gruppen“ unterstützt.

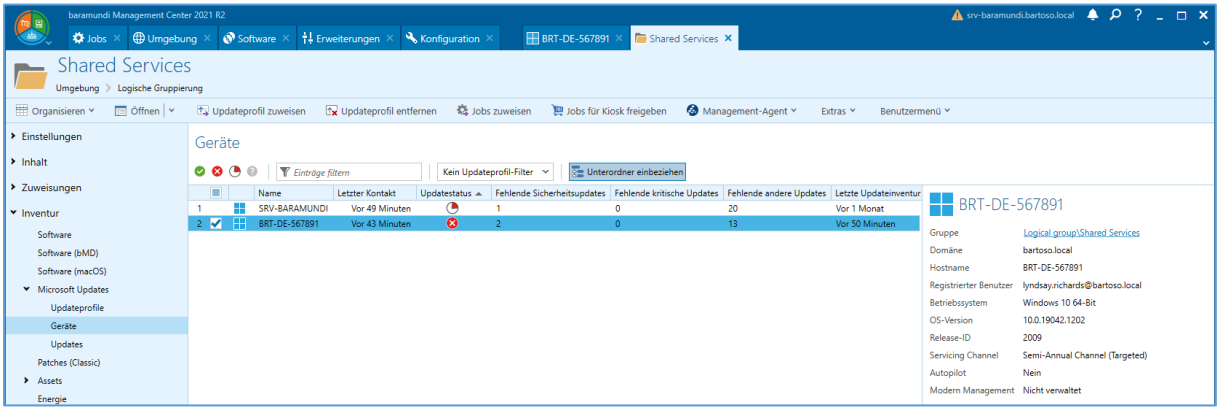


Abbildung 29 - Übersicht über die Updatezustände der Endpoints innerhalb einer Gruppe

So lassen sich einzelne Gruppen (z.B. Abteilungen) aber auch verschachtelte Zweige (z.B. Standorte) gezielt auswerten. Auf einen Blick ist erkennbar, ob die Geräte die Vorgaben des Updateprofils erfüllen, ob und wie viele Updates fehlen und auch wann zuletzt inventarisiert bzw. aktualisiert wurde. Selbstverständlich kann auch auf die verschiedenen Zustände und die Updateprofile gefiltert werden.

1.11.4 Detaillierte Übersicht aller Updates

Ebenso neu hinzugekommen ist die Auflistung aller referenzierten Updates innerhalb einer Gruppe und darunterliegender Gruppen. So werden nun alle installierten und fehlenden – damit auch die verzögerten oder blockierten – Updates der in der Gruppe enthaltenen Endpoints aufgelistet. Selbstverständlich auch hier mit der Möglichkeit zur Filterung nach Zustand, Name, KB-Nummer und weiteren Eigenschaften.

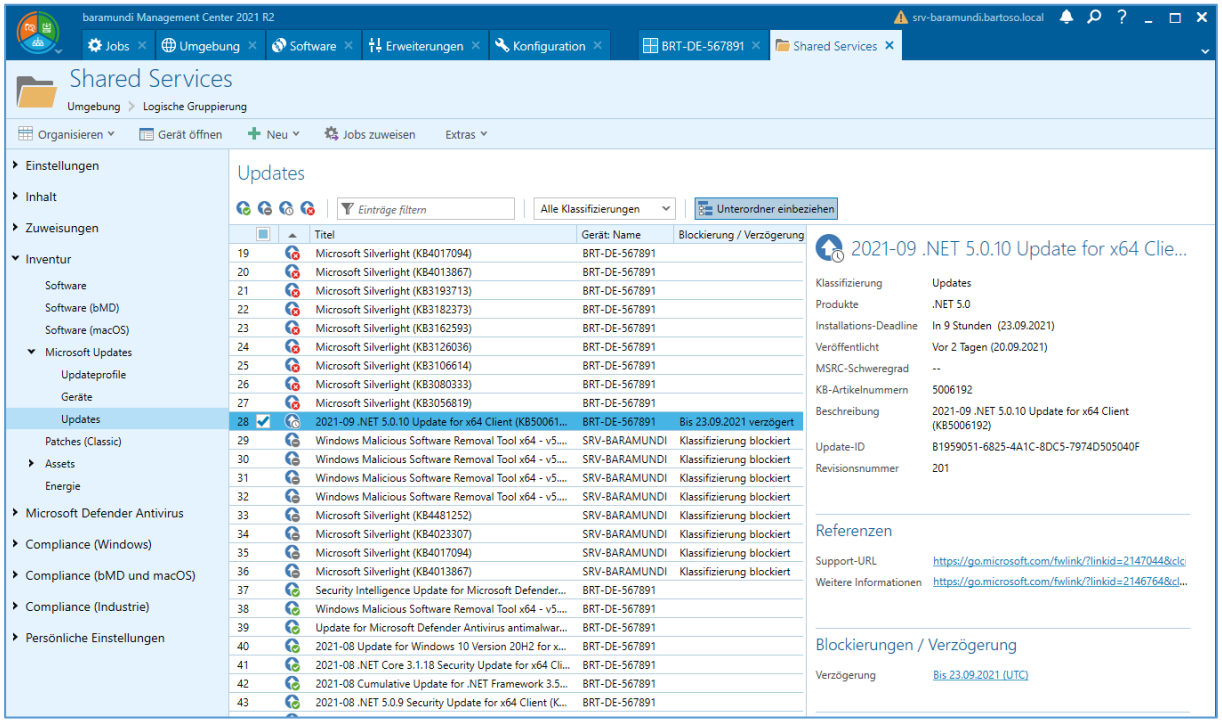


Abbildung 30 - Auflistung aller referenzierten Updates der Endpoints unterhalb einer Gruppe.

1.12 Störungsfreies Arbeiten

1.12.1 End User Experience

Durch den Siegeszug der mobilen Geräte und auch der pandemiebedingten Verlagerung vieler Arbeitsplätze ins Homeoffice, setzt sich das Paradigma, dass die User selbst sehr viele Freiheiten auf den Geräten genießen, um z.B. Apps zu installieren, immer weiter durch. Die User erwarten, dass die Geräte einfach funktionieren, möchten aber selbst – in einem gewissen Rahmen – mitbestimmen, wann was auf dem Gerät passiert. Auch möchten sie eigene Einstellungen und Anpassungen vornehmen.
Für die Admins bedeutet das häufig erschwerte Bedingungen bei der Umsetzung von Firmenrichtlinien oder auch bei einfachen Softwareinstallationen. Im Idealfall setzen die Admins die Richtlinien durch und aktualisieren Software ohne die Anwender bei der Arbeit zu stören. Da sich aber unmöglich pauschal vorhersehen lässt, wann welcher Endpoint ohne zu stören administriert werden kann, ist es wichtig, die User aktiv einzubeziehen.

1.12.2 „Nicht stören“ Modus in der bMS

Bei der Verteilung eines Jobs hat man seit jeher die Möglichkeit mit den Usern zu interagieren und über den Tray Notifier Hinweistexte anzeigen zu lassen, welche jobbasierend aber auch individuell gestaltbar sind.

Sobald der Job startbereit ist, bekommen die User diesen Text als Popup-Nachricht mit der Möglichkeit, einen gewünschten Startzeitpunkt anzugeben. Und genau hier entsteht für einige User ein Problem: Egal wann der Agent anstehende Arbeiten ankündigt, es ist häufig unpassend oder gar störend.
Mit der bMS 2021 R2 haben Administratoren nun die Möglichkeit den sogenannten „Nicht stören“ Modus zu aktivieren und zu konfigurieren. Hierbei hat ebenso die Konfigurationsseite des Management Agents eine Frischzellenkur bekommen.

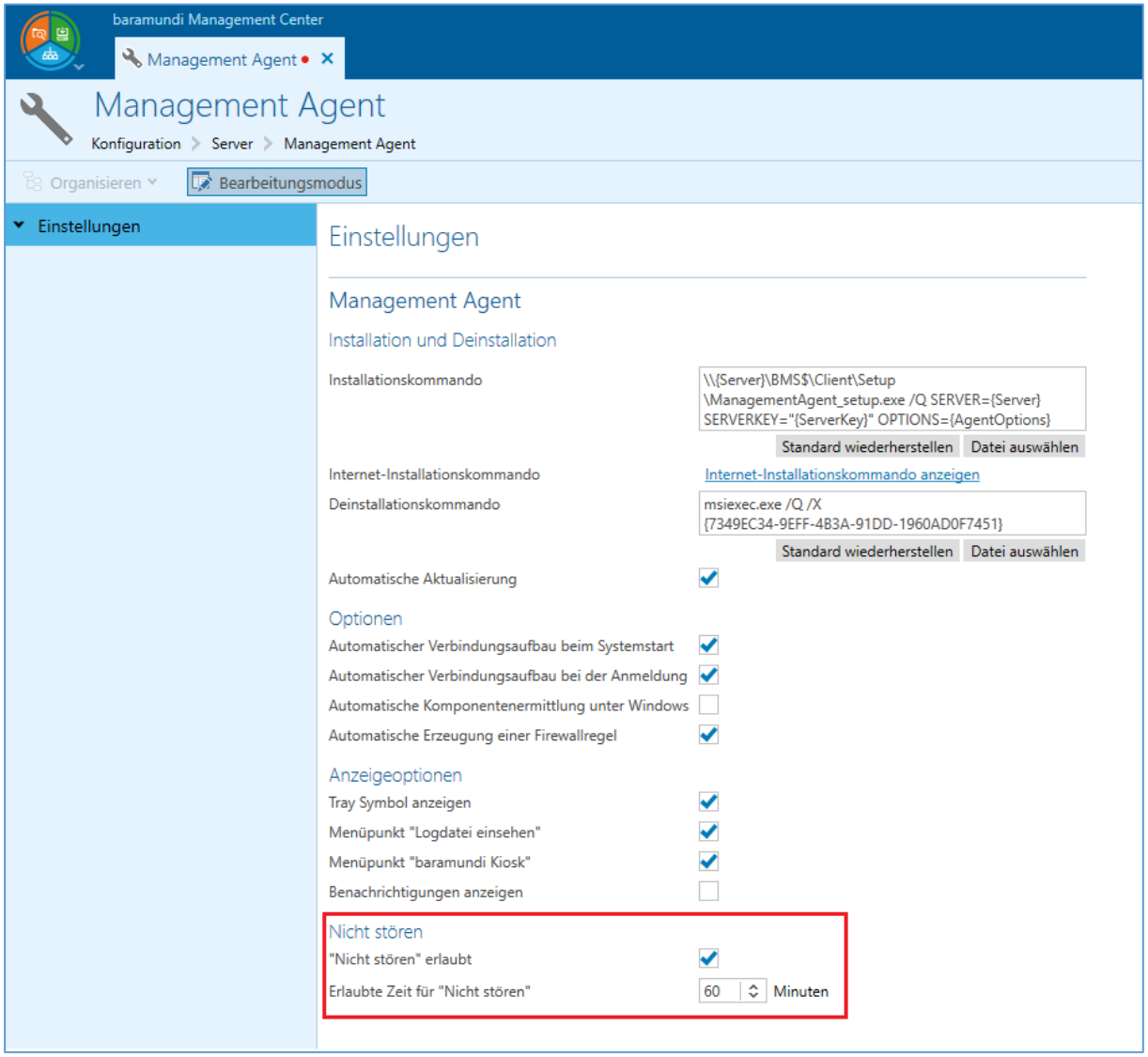
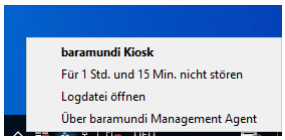
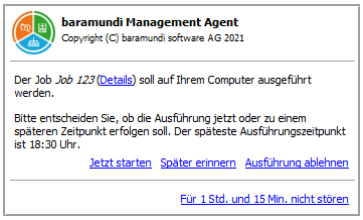
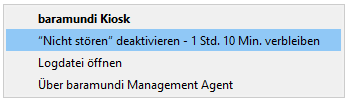


Abbildung 31 – bMA Konfigurationsseite mit den Optionen für den "Nicht stören" Modus.

1.12.3 Benutzersicht

Für die User selbst gibt es ab dem Zeitpunkt die Möglichkeit diesen „Nicht stören“ Modus für das eigene Windows Endgerät zu nutzen. Der Modus kann in der bekannten Tray Notifier Meldung selbst oder auch über das Kontextmenü des bMA für die konfigurierte Zeitspanne gestartet werden. Dies ist beispielsweise vor einer Präsentation oder einer Besprechung nützlich, um in deren Verlauf nicht von den baramundi Meldungen gestört zu werden.

„NICHT STÖREN“ PER KONTEXTMENÜ AKTIVIEREN	„NICHT STÖREN“ PER TRAYNOTIFIER AKTIVIEREN	„NICHT STÖREN“ PER KONTEXTMENÜ DEAKTIVIEREN
		

1.12.4 Administrationssicht

Für die Admins wird dies auch transparent im baramundi Management Center dargestellt. In den Listenansichten kann die neue Spalte „Nicht stören Modus endet“ eingeblendet und auch danach sortiert werden.

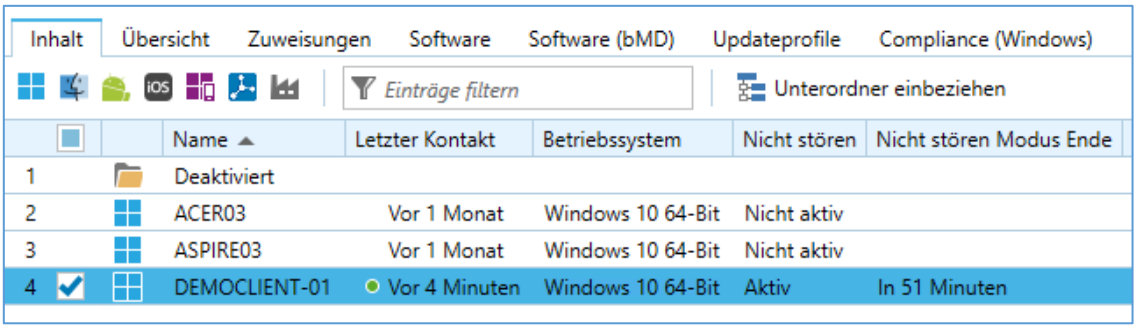


Abbildung 32 - Listenansicht mit den neuen Spalten für den "Nicht stören" Modus

Diese Werte können auch als Bedingung innerhalb von Universellen Dynamischen Gruppen (UDG) verwendet werden.

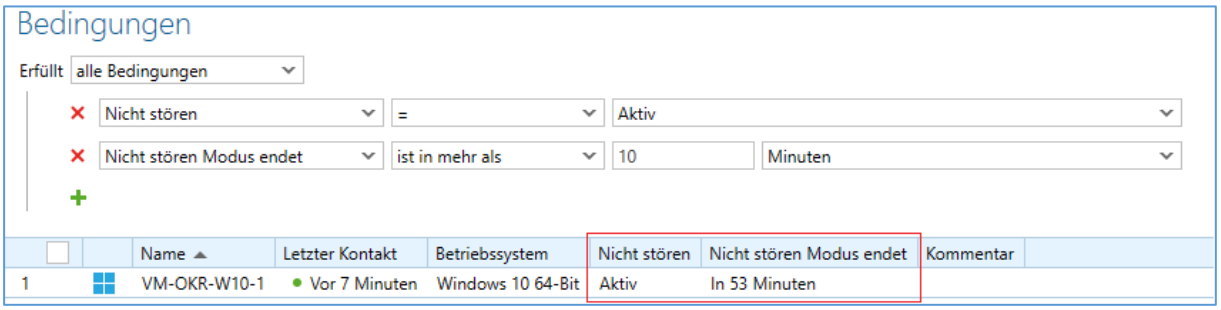


Abbildung 33 - "Nicht stören" Modus als Bedingung für eine UDG.

1.12.5 Schnittstellen

Über das bMA Command Line Interface (die bMACmd) lässt sich der „Nicht stören“-Modus ebenso steuern. Hierfür wurde die bMACmd.exe um mehrere Kommandos zum Setzen und Abfragen des „Nicht stören“-Modus erweitert. Auch über bConnect lässt sich auslesen, ob der „Nicht stören“-Modus am Endpoint aktiviert wurde und wie lange er noch aktiv ist.

1.13 Allgemeine Weiterentwicklung

1.13.1 baramundi Argus Cockpit (bAC)

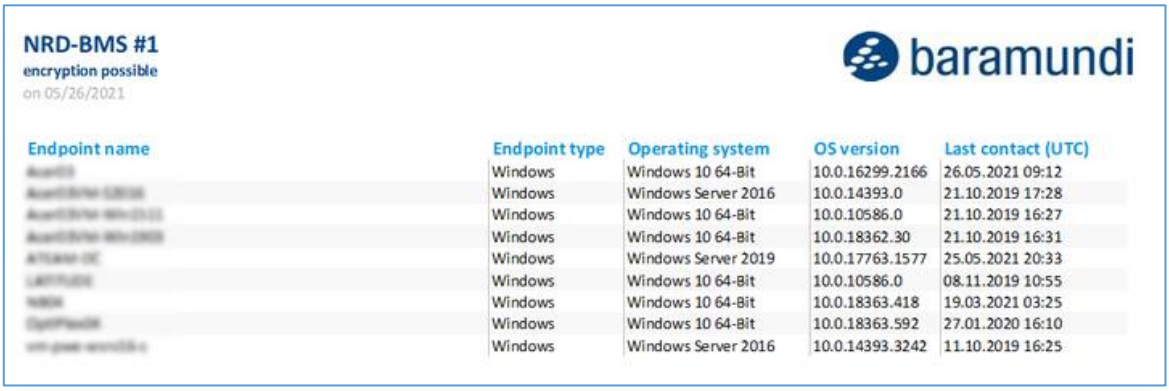
Auch mit diesem Release wächst der Funktionsumfang im bAC kontinuierlich und viele neue hilfreiche Funktionen bieten Arbeitserleichterung für IT-Admins, aber auch für andere Rollen im Unternehmen, wie z.B. dem CISO. Alle neuen Funktionalitäten können auch ohne Versionsupdate der bMS genutzt werden, so dass viele der folgenden Umsetzungen bereits vor dem bMS Release 2021 R2 zur Verfügung stehen[2].

1.13.1.1 (Historische) UDG-Ergebnismengen nach Excel exportieren

Mit Hilfe der neuen Excel-Export Funktionalität können IT-Admins nun mit anderen Rollen im Unternehmen (z.B. IT-Manager oder CISO) relevante IT-Informationen teilen. Diese Berichte können angepasst werden, so dass diese den CI-Vorgaben des jeweiligen Unternehmens entsprechen.
So lassen sich UDG-Ergebnismengen (z.B. "Alle Endgeräte mit ausstehenden kritischen Updates", "Endgeräte ohne BitLocker Verschlüsselung") im Unternehmen verteilen und

[2] https://www.baramundi.com/de-de/management-suite/module/argus-cockpit/updates/

sorgen so für mehr Transparenz über die eigene IT-Umgebung – auch über zurückliegende Zeitverläufe hinweg.



NRD-BMS #1
encryption possible
on 05/26/2021

baramundi

Endpoint name	Endpoint type	Operating system	OS version	Last contact (UTC)
[redacted]	Windows	Windows 10 64-Bit	10.0.16299.2166	26.05.2021 09:12
[redacted]	Windows	Windows Server 2016	10.0.14393.0	21.10.2019 17:28
[redacted]	Windows	Windows 10 64-Bit	10.0.10586.0	21.10.2019 16:27
[redacted]	Windows	Windows 10 64-Bit	10.0.18362.30	21.10.2019 16:31
[redacted]	Windows	Windows Server 2019	10.0.17763.1577	25.05.2021 20:33
[redacted]	Windows	Windows 10 64-Bit	10.0.10586.0	08.11.2019 10:55
[redacted]	Windows	Windows 10 64-Bit	10.0.18363.418	19.03.2021 03:25
[redacted]	Windows	Windows 10 64-Bit	10.0.18363.592	27.01.2020 16:10
[redacted]	Windows	Windows Server 2016	10.0.14393.3242	11.10.2019 16:25

Abbildung 34 - Export inkl. definierten CI-Anpassungen

1.13.1.2 Relevante Daten in umfassenden Reports teilen

Mit der neuen Reporting Schnittstelle im baramundi Argus Cockpit ist es nun möglich, alle relevanten Daten aus dem bAC auch in Reporting Anwendungen (z.B. MS Power BI, MS Excel) anzuzeigen und auszuwerten. Als IT-Admin können Sie kumulierte Daten der bMS-Umgebungen, die Sie mit dem bAC verbunden haben, so übersichtlich darstellen und mit anderen Rollen im Unternehmen teilen.
IT-Admins können dabei die Daten z.B. nach:

- bMS Umgebung,
- Zeitraum,
- Universelle dynamische Gruppe (UDG) oder
- Thema (z.B. Security)

auswählen bzw. eingrenzen.
So ist es z.B. auch als CISO möglich, generierte Reports dafür zu nutzen, um bei Audits oder Zertifizierungen (z.B. Datenschutz-Audit) den aktuellen und den Verlauf des IT-Systemzustand nachweisen zu können.

Abbildung 35 - Beispiel für ein Power BI Reporting

Um IT-Admins den Einstieg in das Reporting zu vereinfachen, stellen wir zusätzlich ein Standard Reporting-Template für MS Power BI Desktop zur Verfügung. Es können aber auch eigene oder Templates anderer Kunden auf unserem bAC Reporting Template Marktplatz[3] genutzt werden.

1.13.1.3 Vergleich zweier Zeitpunkte von UDG-Ergebnismengen

Mit Hilfe der Universellen Dynamischen Gruppen (UDG) können im bAC wichtige Daten der IT-Umgebung angezeigt werden und mit den Argus Trends können diese Ergebnismengen auch über einen längeren Zeitraum hinweg visualisiert werden.
IT-Admins möchten aber nicht nur wissen, wie viele Endpoints von einem auf den anderen Zeitpunkt hinzugekommen oder weggefallen sind, sondern auch welche Endgeräte das waren, um anschließend gezielt auf diesen Endpoint (in der bMC) Jobs zur Problembeseitigung auslösen zu können. In einer neuen „Delta-Ansicht“ ist diese Information nun sichtbar, indem zwei beliebige Zeitpunkte selektiert werden können.

[3] https://forum.baramundi.de/index.php?threads/marktplatz-f%C3%BCr-bac-reporting-templates.11864/

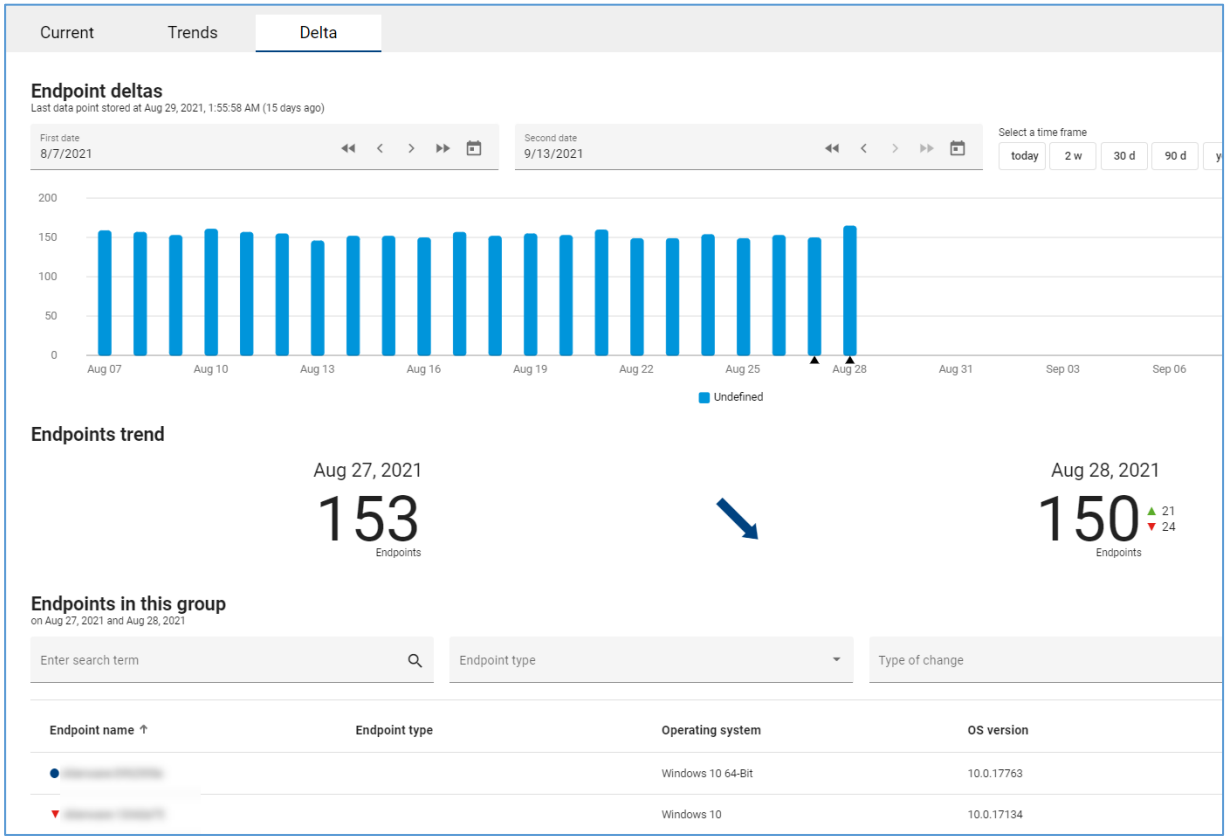


Abbildung 36 - Vergleich zweier Zeitpunkte von UDG-Ergebnismengen

1.13.1.4 E-Mail-Benachrichtigungen über wichtige Veränderungen

Im Argus Cockpit können kritische Zustände einer IT-Umgebung einfach sichtbar gemacht werden und diese Informationen sind überall und jederzeit abgreifbar. Im IT-Arbeitsalltag ist es allerdings so, dass die IT-Admins nicht ständig vor dem bAC sitzen und bspw. die UDGs mit Ihren Schwellwerten beobachten. An dieser Stelle ist es wichtig, dass die IT-Admins insbesondere beim Übergang von „normalen“ auf kritische Zustände proaktiv über diese Zustandsänderungen informiert werden können.

Die Option, sich per E-Mail beim:

- Statuswechsel von bMS-Diensten und
- Erreichen definierter UDG-Schwellwerte

benachrichtigen zu lassen, steht allen bAC-Nutzern mit dem nächsten Release zur Verfügung.

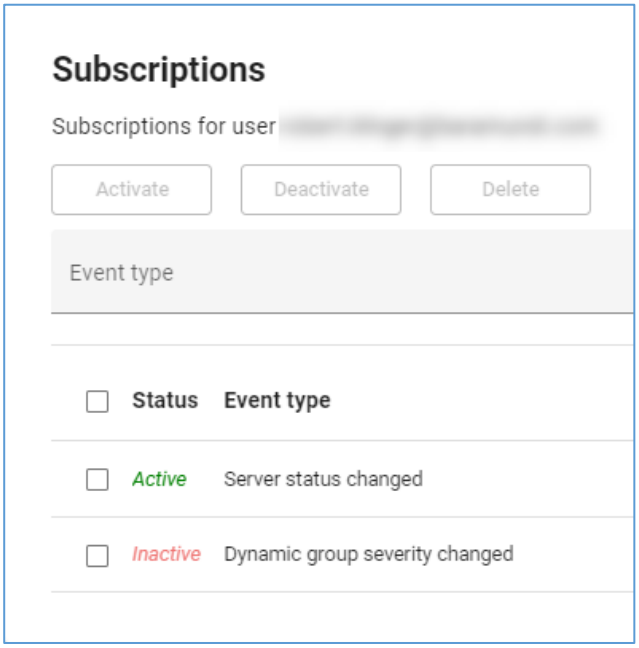


ABBILDUNG 37 - LISTE DER GEWÄHLTEN BENACHRICHTIGUNGEN

1.13.2 Automation Studio - Eingebettetes Skript Rückgabewert

Das baramundi Automation Studio bietet schon seit einiger Zeit die Möglichkeit an eingebettete Skripte wie VBScript, JScript oder Powershell. Nun gab es Feedback, dass bei der häufig verwendeten Powershell Methode das Weiterarbeiten mit den Ergebnissen direkt im Automation Studio hilfreich wäre und eben dies ist nun mit der 2021 R2 möglich. Sie können das Powershell-Skript nun einfach mit einem Rückgabewert beenden und mit diesem in einer baramundi Variablen innerhalb des Automation Studio Skriptes weiterarbeiten.

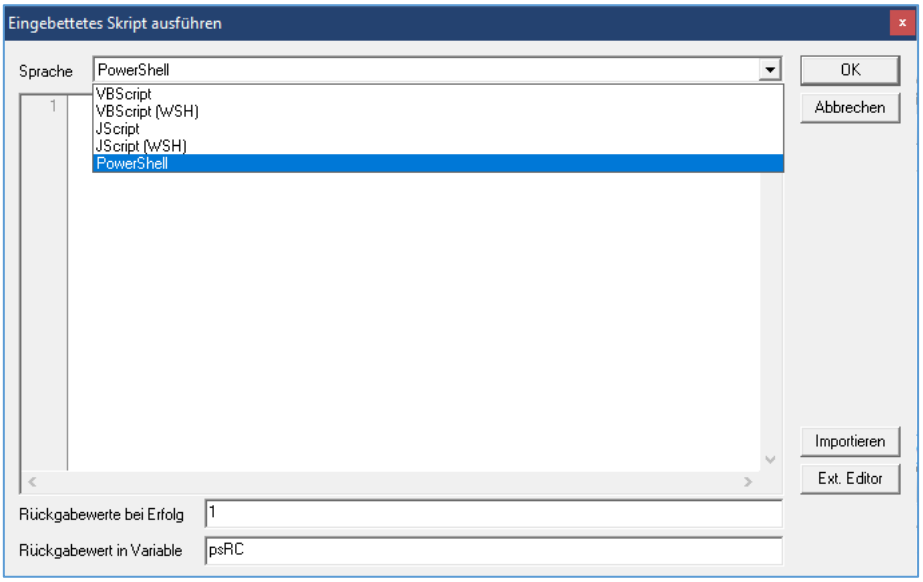


Abbildung 38 - Eingebettetes Skript ausführen. Rückgabewert in Variable

1.13.3 baramundi License Management – E-Mail-Benachrichtigung

Sind z.B. Lizenzverträge zeitlich begrenzt oder unterliegen ggf. einer Kündigungsfrist bietet die neue Funktion der Benachrichtigung per E-Mail eine verbesserte Möglichkeit Lizenzen besser im Blick zu haben und zu verwalten.
Mit dem neuen Release bieten wir Ihnen die Möglichkeit unterschiedliche Ereignisse mit konfigurierbaren Prüfungsintervallen so anzulegen, dass Sie für die gewählten Fälle benachrichtigt werden.

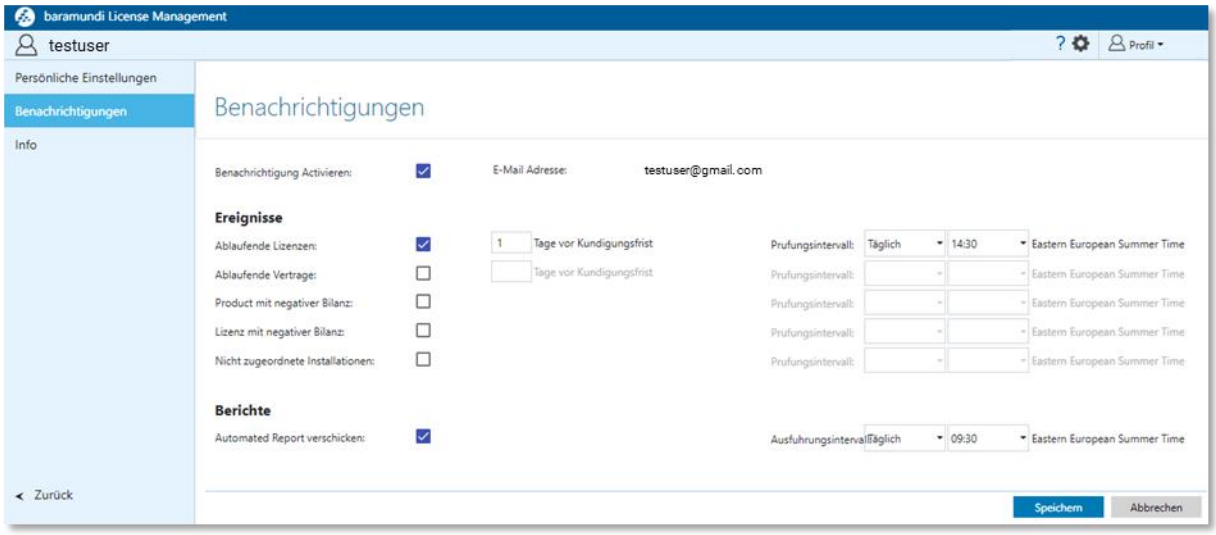


Abbildung 39 - bLM Konfiguration für individuelle E-Mail-Benachrichtigung

Anmerkung: Die neue Funktionalität wird über MSW zur Verfügung gestellt. Wir werden zu gegebener Zeit im Forum hierzu informieren.

1.13.4 baramundi Network Devices

1.13.4.1 Erweiterte Scan-Methoden

Neben der bisherigen Möglichkeit über SNMP Geräte in einem Netzwerkbereich zu erfassen, bieten wir Ihnen mit dem neuen Release auch die Option über Address Resolution Protocol (ARP) Netzwerkendpunkte zu ermitteln.

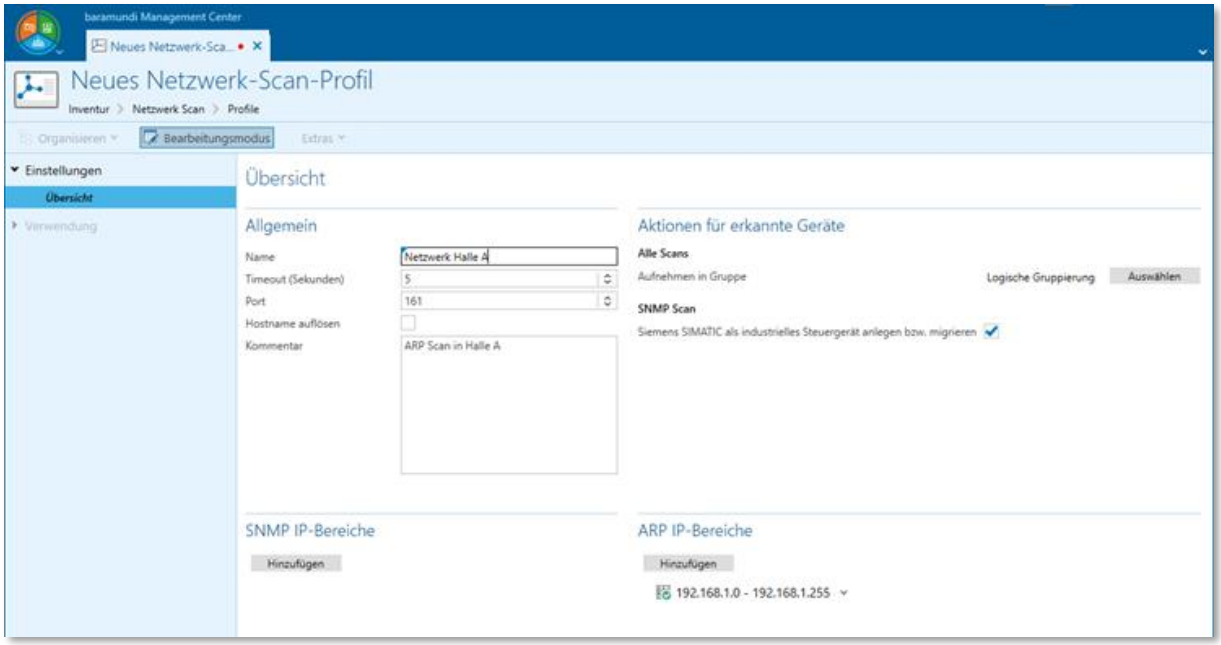


Abbildung 40 - Erweiterte Scanmethode "ARP IP-Bereich"

Über diese Methode werden sowohl die IP- als auch die MAC-Adresse erfasst. Darüber hinaus wird, wenn möglich, der Hostname aufgelöst und angezeigt.

Damit können Sie die Zahl der durch baramundi gefundenen Geräte erhöhen und somit Ihre Übersicht der in der Infrastruktur vorhandenen Systemen verbessern. Wie gewohnt stehen Ihnen die gewonnenen Informationen in verschiedenen Gruppenansichten zur Verfügung.

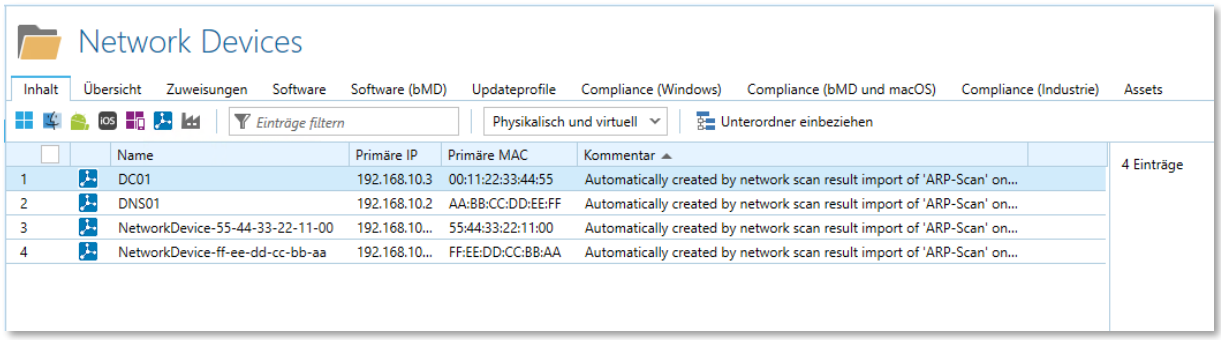


Abbildung 41 - Logische Gruppe - Netzwerkgräte über ARP erfasst

1.13.4.2 Manuelles Anlegen von Netzwerkgeräten

Befinden sich Geräte in einem nicht erreichbaren Segment oder sind z.B. vorrübergehend offline, sollen aber trotzdem in baramundi berücksichtigt werden, können diese mit dem neuen Release als Netzwerkendpunkt manuell angelegt werden.

Damit erhalten Sie einen Weg eine durch baramundi erfasste Geräteübersicht weiter anzureichern.

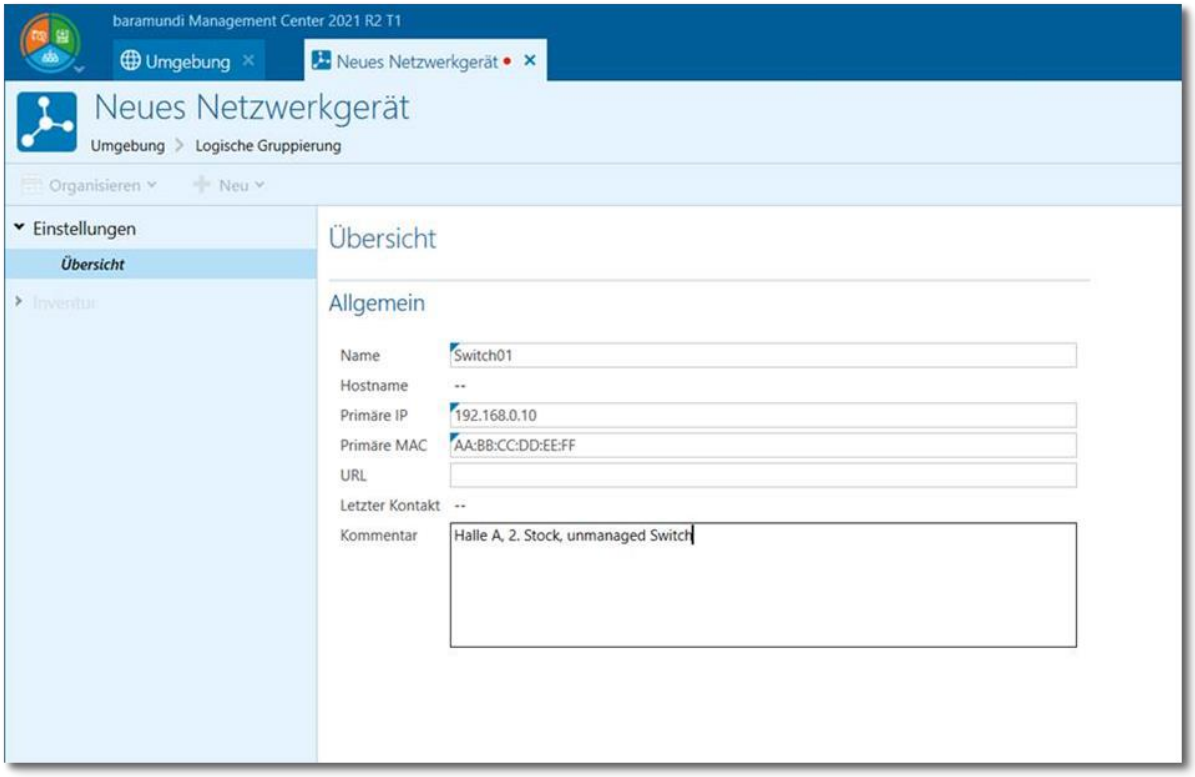


Abbildung 42 - Manuelles Anlegen von Netzwerkgeräten

Über die Schnittstelle bConnect ist es neben dem Auslesen und Löschen jetzt auch möglich Netzwerkgeräte anzulegen bzw. upzudaten.

1.13.4.3 Benutzerdefinierte Variablen an Netzwerkgeräten

Neben den automatisch erfassbaren Informationen gibt es einen Bedarf, weitere spezifische Daten an den Endpunkten zu pflegen.

So können Sie jetzt für die über SNMP und ARP erfassten Geräte Variablen mit einem ersten Umfang an Variablentypen definieren und diese mit der jeweiligen Information in den Gruppenansichten verwenden. Informationen zu z.B. Kostenstelle, Raum Nummer, Gebäude oder Kaufdatum können jetzt individuell ergänzt werden. -

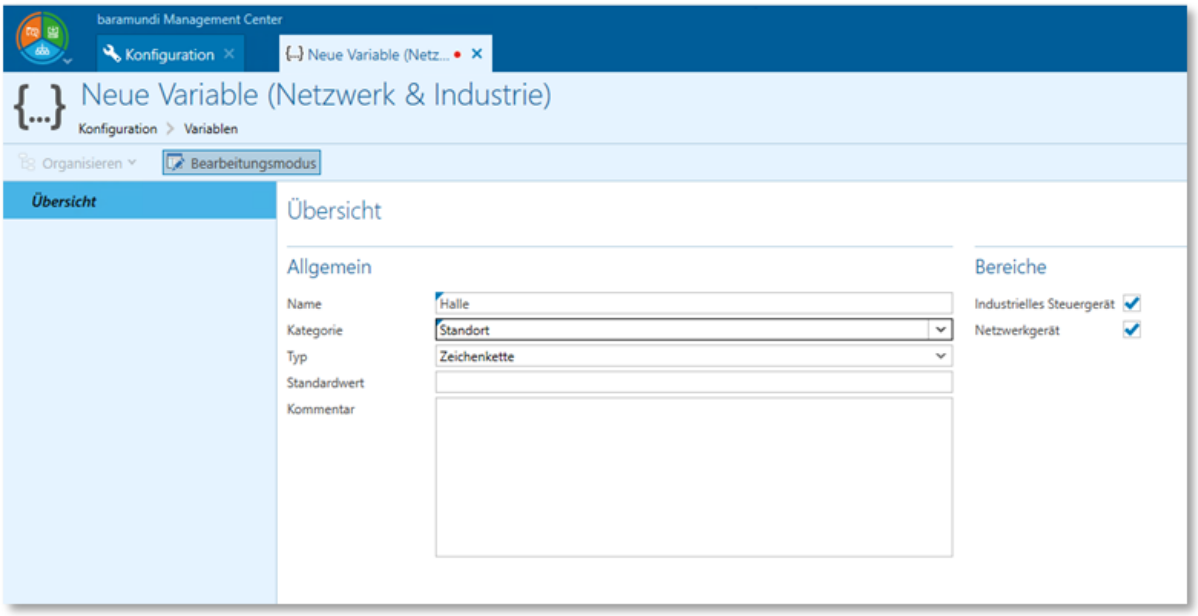


Abbildung 43 - Variablen-Definition mit Mehrfachzuordnung auf verschiedene Bereiche

1.13.5 Active Directory Synchronisation

Als Grundlage für essentielle Funktionen in der baramundi Management Suite stellt der AD-Sync eine komfortable Möglichkeit dar, Computer- wie auch Benutzerobjekte zu synchronisieren. Dabei wurde in der 2021 R1 nicht nur der Verwaltungsdialog überarbeitet und die Performance verbessert, es wurden auch zwei weitere Optionen im Bereich der Maschinensynchronisation integriert. In dieser Version 2021 R2 kommt nun die Erweiterung im Bereich Benutzersynchronisation. Die Benutzersynchronisation erhielt nun die vergleichbare Funktionalität, wie sie bereits von der Maschinensynchronisation bekannt ist und es können flexibel AD-Properties in baramundi Variablen an Benutzer und Gruppen synchronisiert werden.
Dies können neben den generischen Feldern wie Vor- und Nachname auch bestimmte AD Eigenschaften sein wie beispielsweise weitere Adressdaten oder dem distinguishedName.

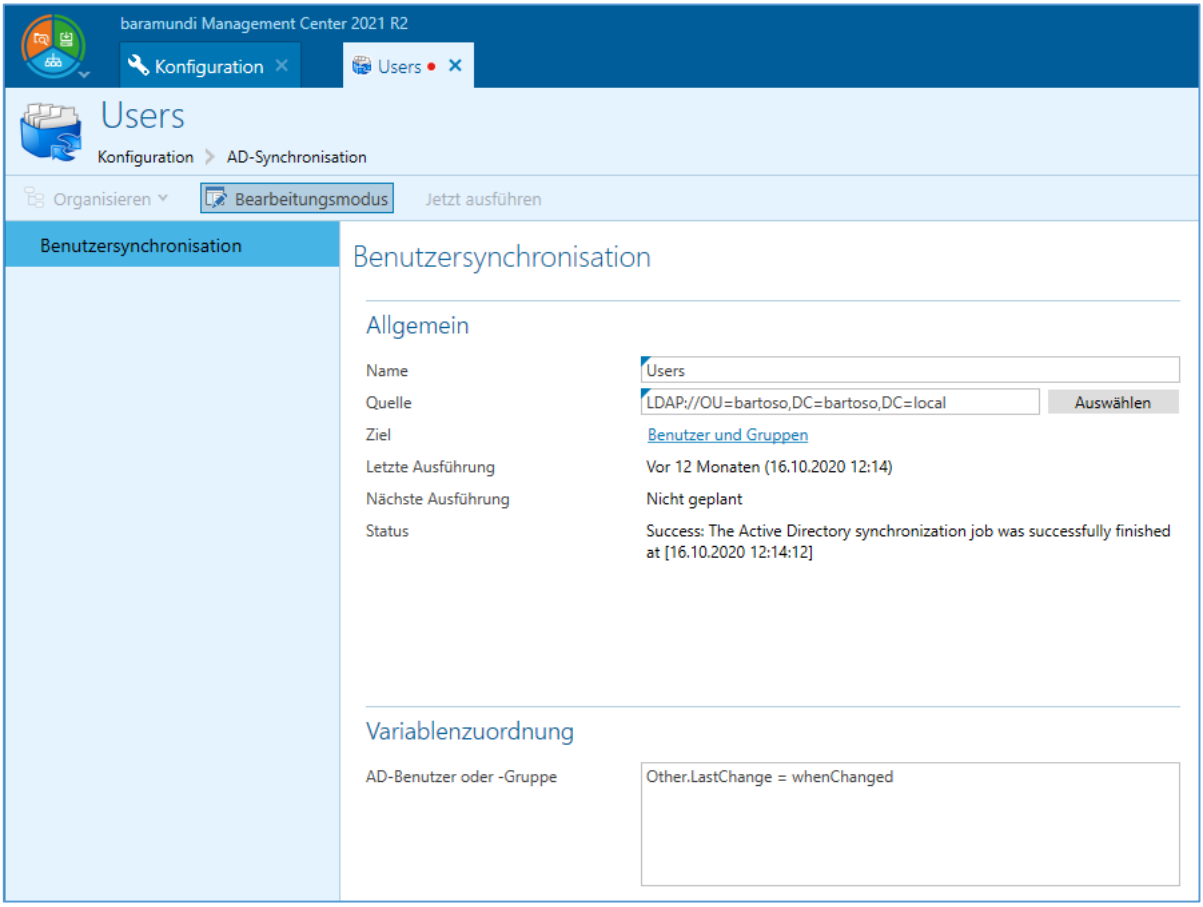


Abbildung 44 - Benutzersynchronisation mit Variablenzuordnung

Die Daten aus dem baramundi Management Center werden dann am jeweiligen Benutzer- oder Gruppenobjekt angezeigt. Im Bereich der mobilen Geräte (iOS und Android), bei welchem die Handhabung mit der Syntax {RegisteredUser.VariablenName} bereits bekannt

ist, kann somit auch auf die weiteren gesyncten Felder zugegriffen werden. Dies geschieht mit der Syntax für eigene Variablen {RegisteredUser.Kategorie.Name}.
Unter Windows Endgeräten und somit deren Jobs können diese registrierte Benutzer- und Gruppen-Variablen nicht verwendet werden.

1.14 Produktverbesserungen im Detail

1.14.1 Windows Agent (bMA)

- Zum Zugriff auf die `bMA.log` Datei werden lokale Administrations-Rechte benötigt. Wird die Aktion `Logdatei öffnen` beim bMA-Icon verwendet, so erscheint eine UAC-Abfrage.
- Der `Nicht stören` Modus ermöglicht es dem Anwender des Endgeräts eine Jobausführung zu verhindern.
- Wird über `bMACmd` eine `Benutzerdefinierte Variable` vom Typ `Datum` gesetzt, so wird der Wert im richtigen Datumsformat geschrieben. Wenn eine Konvertierung des Datums nicht möglich ist, wird ein leerer Wert geschrieben.
- Die Funktionalität zum automatischen Updaten der Windows Update API im Kontext von `Microsoft Update verwalten` Jobs wurde entfernt, da diese ab Windows 7 nicht mehr notwendig ist. Der bwumgr Parameter `/SkipUpdateCheck` ist obsolete und wird ignoriert.
- Bugfix: Der Shutdown nach einem WakeOnLan-Job arbeitet u.U. nicht korrekt, da die Wakeup-Zeit falsch ermittelt wird.
- Bugfix: Sporadisch wird im bMA.log die Meldung "Local install user ['baraInstLocal'] group membership could not be retrieved, no group membership removed!" protokolliert, obwohl kein Fehlverhalten vorliegt.

1.14.2 Management Center (bMC)

- Eine neue baramundi Lizenzierung ermöglicht eine komfortablere Lizenzierung der Module der baramundi Management Suite.
- Das Feld `Bootzeit` steht in `Dynamischen Gruppen (Universell)` zur Verfügung und referenziert die letzte Bootzeit von Windows-Geräten.
- Die Konfiguration des baramundi Management Agent für Windows (bMA) ist jetzt unter `Konfiguration – Server - Management Agent` und enthält neue Einstellmöglichkeiten für `Nicht stören`.
- Berechtigungen für `Jobs – Ordner` und `Umgebung – Benutzer und Gruppen` werden jetzt in einem modernen Dialog konfiguriert.

- Schlagen Downloadjobs fehl, wird eine bMC Nachricht angezeigt.
- Zahlreiche Verbesserungen beim Windows Update Managment. Neue Ansichten an Gruppen, statischen Gruppen und universellen Gruppen (Windows). Der Updatestatus verwendet die konfigurierte Verzögerungszeit des Updateprofils und zeigt die Verzögerungszeit als „Installations-Deadline“ an.
- Bugfix: Werden unter `Umgebung` mehrere Windows Clients ausgewählt um den Modus des bMA zu verändern, so erscheint nicht immer eine Fehlermeldung, wenn die Berechtigungen für einzelne Clients dazu nicht ausreichen.
- Bugfix: Wird die bMS auf einem virtuellen Serversystem betrieben, so wird unter verschiedenen Umständen eine Lizenzverletzung durch Hardwaretausch erkannt.
- Bugfix: Wird eine bereits vorhandene Applikation per bDX-Import erneut eingelesen, so werden vorhandene `Installiert auf` Einträge entfernt.
- Bugfix: An der Client-Compliance-Übersicht werden `Gefundene Schwachstellen` falsch gezählt, wenn partielle Ausnahmen gesetzt sind.
- Bugfix: Bei einigen Jobschritten für Patch (Classic) und Treiberinstallationen werden zusätzlich GUIDs angezeigt.
- Bugfix: In seltenen Fällen stürzt die bMC ab, wenn die Ansicht `Jobdetails` bei einer großen Anzahl von Jobinstanzen geöffnet wurde.
- Bugfix: Dynamische Gruppe (Windows) zeigt kein Ergebnis an, wenn das manuell erstellte SQL-Statement Machinen mehrfach zurückliefert.

1.14.3 OS-Install

- Aus den unattend.xml Dateien wurde die Deaktivierung der Firewall entfernt. Zusätzlich wurden die für die Kommunikation benötigten Portfreigaben hinzugefügt. So bleibt nach einer OS-Installation die Windows-Firewall aktiv, die Kommunikation zwischen Server und Agent ist dennoch gewährleistet.
- Aus den unattend.xml Dateien wurde die Deaktivierung der AntiSpyware entfernt.
- Die Partitionierung von GPT-initialisierten Festplatten mit Windows-Recovery-Partition wurde für das Windows PE des „*Microsoft ADK für Windows 11*“ angepasst.

- Um die Installation von Windows 11 mit der Konfiguration `InstallToAvailablePartition` zu ermöglichen wird jetzt das `osinstall_presetup_win11.bds` ausgeführt, welches den Laufwerksbuchstaben der Windowspartition entfernt.
- Bugfix: Das am Windows-Gerät hinterlegte `Updateprofil` wird durch einen OS-Installjob entfernt.

1.14.4 Mobile Devices

- Profile, welche weder mit einem Jobschritt verlinkt sind, noch auf einem Gerät inventarisiert wurden, werden automatisch täglich bereinigt.
- Der iOS Exchange Baustein wurde um `OAuth` erweitert
- Die Settings der Sicherheitsbausteine wurden neu angeordnet.
- Bugfix: iOS Profile mit der Einstellung `Safari-Cookie-Einstellung ‚Von besuchten Seiten erlauben‘` können nicht verteilt werden.
- Bugfix: Ein Android Enterprise Gerät kann nicht angelegt werden, wenn Leserechte auf die Android Enterprise Konfiguration fehlen.

1.14.5 Mobile Devices ab Android 12

- Auf vollständig verwalteten Geräten werden nur noch über die bMS installierte WiFi-Netzwerke in der Inventur angezeigt. Private Netzwerke sind nicht mehr sichtbar.
- Der baramundi Agent benötigt keinen Zugriff auf die Berechtigungen zum Erfassen des Standorts.
- Neue Passwortqualitätsstufen sind konfigurierbar.
- Im Enrollmentmodus "Arbeitsprofil" liest die Hardwareinventur keine Daten für IMEI und Seriennummer.

1.14.6 bServer

- Downloadjobs laufen auf einen Timeoutfehler, wenn das Herunterladen nicht innerhalb von 4h möglich war. In diesen Fällen wird eine bMC-Nachricht angezeigt.

- Ist der BitLocker Netzwerk Unlock auf einem PXE-Relay nicht konfiguriert, so verhält er sich dort wie für den Hautpserver konfiguriert. Auf dem PXE-Relay ist der Netzwerk Unlock damit per default aktiviert und nicht mehr deaktiviert.
- Jobinstanzen werden nicht mehr auf Fehler gesetzt, wenn ein Jobschritt nicht geladen werden kann. Dadurch wird das Fehlerhandling bei wiederholten Jobs, welche auf einen Jobtimeout-Fehler liefen, verbessert.
- Jobinstanzen mit unbekanntem Fehlerstatus werden jetzt auf `Unspecified Error` anstatt `Operation successful` gesetzt.
- Bugfix: Wird der bServer in einer virtuellen Umgebung betrieben, so kann die Hardwarebindung der Lizenzierung dazu führen, dass eine neue Lizenz benötigt wird.
- Bugfix: Jobschritte `Microsoft Updates inventarisieren` verursachen u.U. eine große TempDB.
- Bugfix: Ein fehlerhaft eingetragener Gateway-Hostname führt in seltenen Fällen dazu, dass der bServer Dienst nicht mehr startet.

1.14.7 bServer – AD-Synchronisation

- Die Einstellung „`Nur aktive Geräte synchronisieren`“ bei Machinensynchronisierungsjobs wird automatisch beim Datenbankupdate gesetzt. Wird von einer bMS 2021 R1 migriert, so werden die Jobs nicht geändert.
- Die Attributnamen beim AD-Maschinensync sind nicht mehr case-sensitiv.
- Die Benutzer-AD-Synchronisation unterstützt die Synchronisation der AD-Eigenschaften in Variablen, welche in MDM-Profilen, MDM-Jobs oder MDM-Emailtemplates verwendet werden können.
- Bugfix: Der Geräte-Sync erkennt Geräte mit Windows 11 und Server 2022 nicht als Windows-Geräte und verschiebt diese je nach Konfiguration in den Papierkorb.
- Bugfix: Kioskzuweisungen zu Benutzern gehen u.U. durch einen Benutzer-Sync verloren.
- Bugfix: Es werden u.U. viele Warnungsmeldungen der Art "unable to determine if Baramundi.Bms.Common.Entities.AdGroupMappingLight" in die Logdatei geschrieben.

- Bugfix: Beim synchronisieren von AD-Attributen treten Fehler der Form `Active Directory-Attribut [] konnte nicht geparst werden` auf, obwohl der Job korrekt konfiguriert ist.
- Bugfix: Beim Konfigurieren des Intervalls erfolgt auf englischen Systemen eine fehlerhafte Validierung.
- Bugfix: Die Konfiguration von SingleLevelDomains bzw. Domains mit 1-n DC-Tags wird als ungültig abgewiesen. Die Eingabe kann nicht gespeichert werden.
- Bugfix: Bestehende `Dynamisch nachgeladene Benutzer` werden durch die AD Synchronisation nicht korrekt aktualisiert.
- Bugfix: Speichern eines AD-Sync-Jobs für Maschinen dauert unerwartet lange, wenn die Option `Löschen` gesetzt ist.
- Bugfix: Wird ein vom AD-Benutzersync automatisch unter `Dynamisch nachgeladene Benutzer` angelegter Benutzer im AD gelöscht und dort neu angelegt, so bricht der AD-Sync ab.
- Bugfix: Der AD-Benutzersync bricht ab, wenn in der baramundi Datenbank zwei Benutzer mit identischem AD-Pfad vorhanden sind. (Der Sync bricht weiterhin ab, jedoch mit einer aussagekräftigen Fehlermeldung)
- Bugfix: Der LDAP Pfad einer Single Layer Domain kann über die bMC nicht konfiguriert werden, da die GUI den Pfad als invalid erkennt.
- Bugfix: Leerzeichen am Anfang oder Ende des Quellpfads eines Ad Synchronisations-Jobs führen zu fehlerhafter Job-Ausführung.

1.14.8 Automation Studio (bDS)

- Neue Online- und Offline-Hilfe.
- Bugfix: Hinzufügen/Löschen von Benutzern zu/aus lokalen Gruppen ist nicht möglich, wenn ein alternativer UPN Suffix verwendet wird.

1.14.9 Argus-Connect

- Der Umgang mit sporadischen Verbindungsfehlern wurde verbessert.
- Bugfix: Die Status-Nachricht `Cloud-Verbindung wird aufgebaut` wird u.U. auch angezeigt, obwohl die Verbindung korrekt aufgebaut wurde.
- Bugfix: In seltenen Fällen enthält die übertragene Endgeräteliste Duplikate.

1.14.10 bConnect

- bMUM Updateprofile können Endgeräten zugewiesen werden. Die Zuweisung eines Updateprofiles an einen Endpoint ist auch über die ID eines Updateprofils möglich.
- Die ID eines zugewiesenen Updateprofils (Property namens "GuidMicrosoftUpdatePro-file") ist mittels GET-Request (EndpointController) abrufbar.
- Auf Network-Geräten können die CRUD Operationen ausgeführt werden.
- Auf IP-Netzwerken können die CRUD Operationen ausgeführt werden.
- Globale bMUM Einstellungen für Inventur-Gültigkeitsdauer und Toleranzzeit fehlender Updates können gelesen und geschrieben werden.
- Bugfix: Beim Anlegen von Windows-Jobs wird die Option "UserConsentRequired" nicht richtig behandelt.

1.14.11 Defense Control

- In der bMC kann unter `Defense Control – Einstellungen` ein eigenes BitLo-cker Network Unlock Zertifikat importiert werden.

1.14.12 MAC OS

- Verbesserte Fehlermeldungen bei Problemen während des SSH Enrollments.
- BugFix: Für das native Mac Enrollment ist eine MDM Lizenz nötig..

1.14.13 Network Scanner

- Ein Scan über das Address Resolution Protocol (ARP) ist möglich.

3 Release 2021 R1

3.1 Ticketing System

Egal ob es um die Einrichtung neuer Arbeitsplätze, Support für Endbenutzer oder generelles Troubleshooting von Netzwerkproblemen geht, IT-Admins sind als Dienstleister im Unternehmen ständig beschäftigt. Umso wichtiger ist es, bei der Vielzahl an Aufgaben den Überblick zu behalten: Eine einfache E-Mail geht in der täglichen Informationsflut ebenso schnell unter, wie ein Anruf, der eine halbe Stunde später bereits von höheren Prioritäten verdrängt wird.

Das *baramundi Ticketing System powered by OMNINET* bietet hier eine einfache und schnelle Lösung. Das cloudbasierte Tool hilft Ihnen, Anfragen effizient zu organisieren, den Bearbeitungsverlauf unkompliziert nachzuverfolgen und automatisiert Berichte zu generieren.

ℹ Dieses Modul ist derzeit nur in deutscher Sprache verfügbar.

3.1.1 Vorgefertigte Workflow-Vorlagen

Dank fünf vorgefertigter Workflow-Vorlagen ohne besonderen Konfigurationsaufwand ist das Ticketsystem in kürzester Zeit einsatzfähig. Dabei sind bis zu acht verschiedene, vordefinierte und selbstdefinierbare Workflows mit unbegrenzter Ticketanzahl verfügbar.

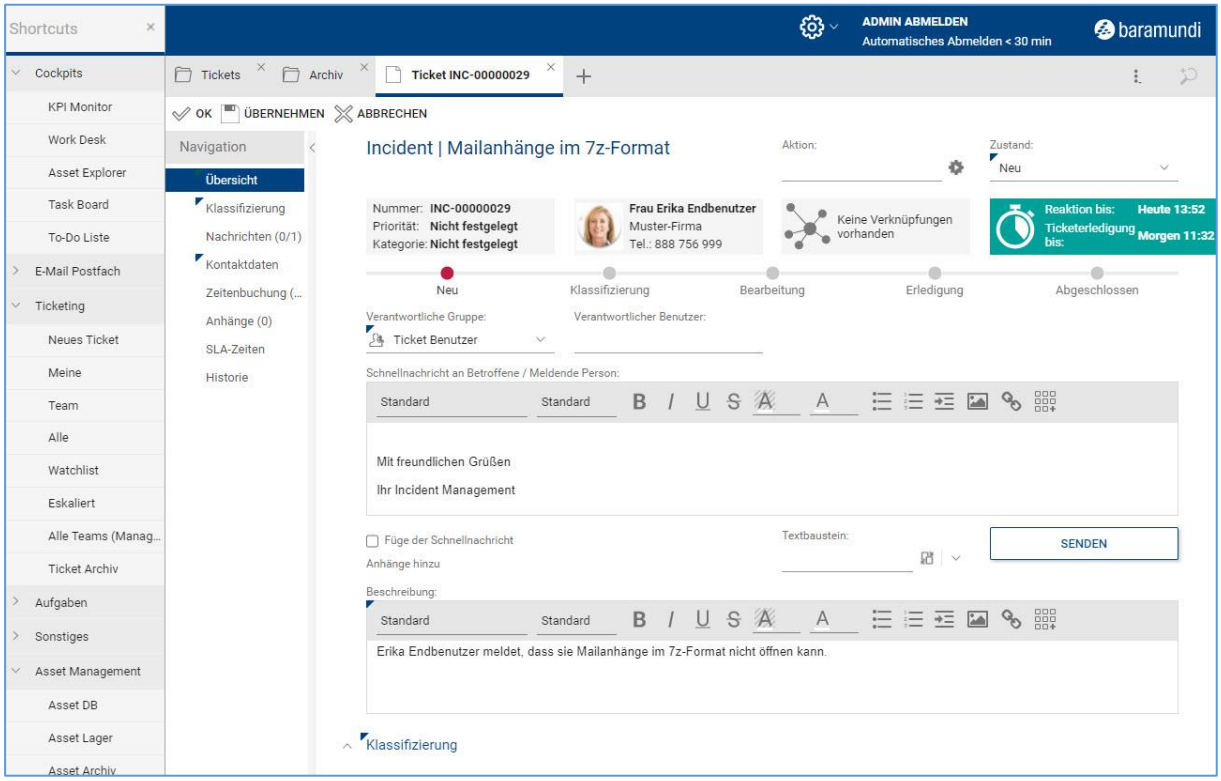


Abbildung 45 - Ticket aus Sicht des Bearbeiters

Das Modul enthält zudem E-Mail-Integration und Service Level Management (SLM) zur Einhaltung von Best Practices bei der Request-Bearbeitung.

3.1.2 Einsatzbereiche

Das Ticketing System unterstützt Sie bei der Bearbeitung von Tickets in sechs verschiedenen Szenarien.

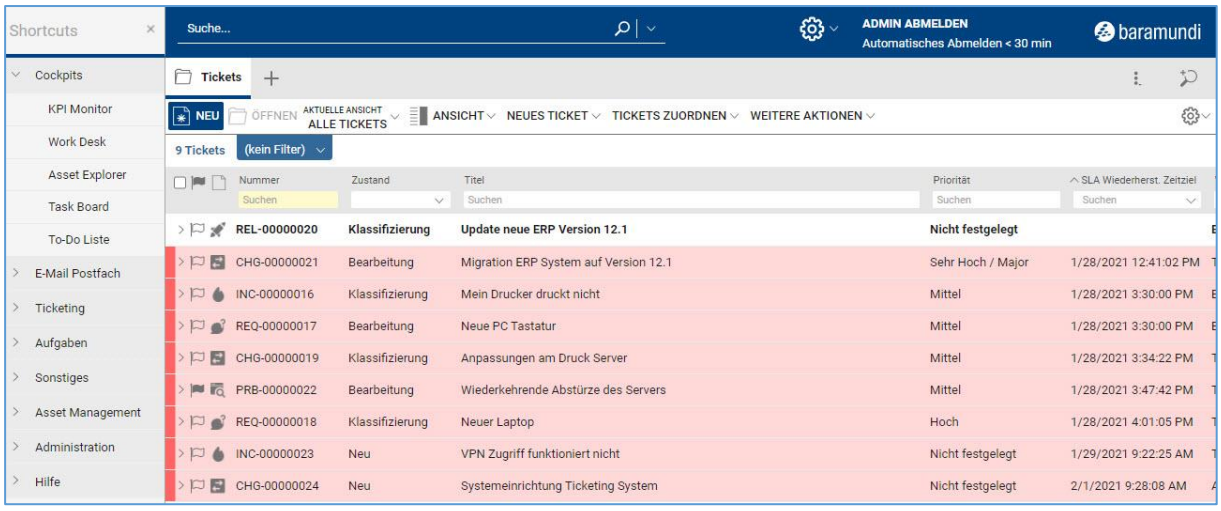


Abbildung 46 - Sicht des Bearbeiters auf seine offenen Tickets

3.1.2.1 Incident Management

Stellen Sie im Störfall IT-Services schnellstmöglich wieder für den Benutzer her und minimieren Sie Ausfälle im Geschäftsbetrieb.

3.1.2.2 Problem Management

Durch strukturierte Diagnosen technischer Probleme reduzieren Sie Incidents und verhindern ihr erneutes Auftreten.

3.1.2.3 Task Management

Verwalten Sie alle IT-Tasks über eine zentrale Oberfläche und beschleunigen Sie einzige Aufgaben und ganze Projekte.

3.1.2.4 Request Fulfilment

Erreichen Sie eine höhere Kunden- und Anwenderzufriedenheit durch Standardisierung und weniger Verwaltungsaufwand für Service-Anfragen.

3.1.2.5 Knowledge Management

Stellen Sie das richtige Wissen zur richtigen Zeit bereit und ermöglichen Sie Self Service für Ihre Anwender und Mitarbeiter.

3.1.2.6 Change Management

Managen Sie sämtliche Aktivitäten und Risiken von Change-Prozessen im Unternehmen schnell und effizient.

3.1.3 Integration von Jobs

Automatisieren Sie die Erledigung von Standardanfragen über die Integration von bMS Jobs. Alle in der baramundi Management Suite angelegten Jobs sind automatisch auch direkt im Ticketing System verfügbar. Softwareinstallationen und beliebige weitere Jobausführungen können somit direkt aus dem Ticketing erledigt werden.

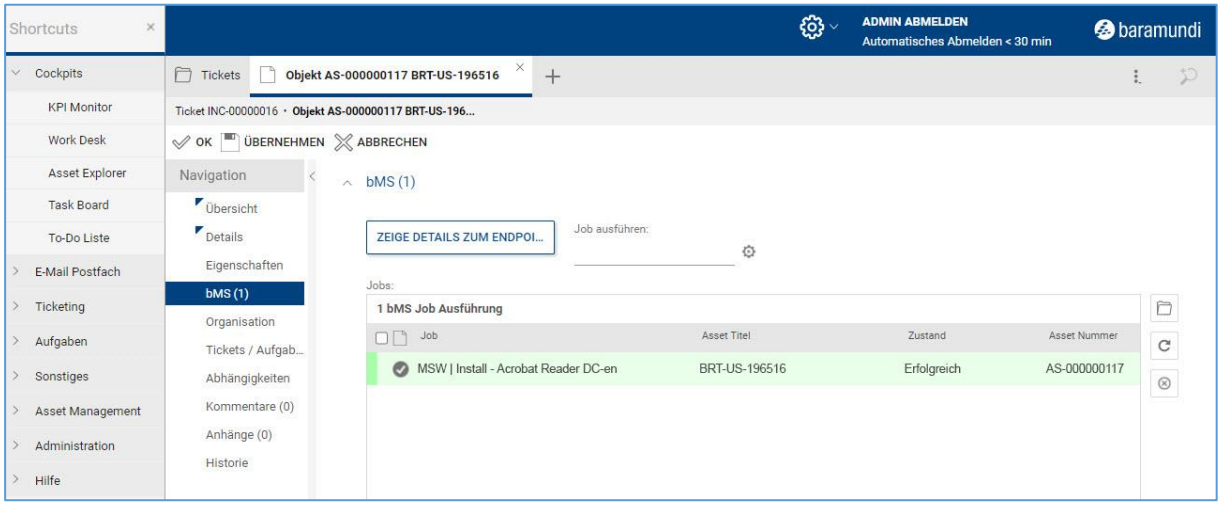


Abbildung 47 - Job-Historie eines Endpoints

Neue Jobs werden über einen Abgleich komfortabel nachträglich ergänzt. Die Ausführung der Jobs wird automatisch dokumentiert und steht für Auswertungen unmittelbar zur Verfügung.

3.1.4 Automatisierte Bearbeitung

Im Ticketsystem können zudem Informationen zu den verwalteten Endpoints in die Asset-Datenbank bei Bedarf abgerufen werden und stehen somit immer aktuell bei einer späteren Ticketbearbeitung zur Verfügung. Damit ist es möglich, einen oder mehrere Jobs hintereinander auf einem jeweiligen Endgerät ausführen zu lassen. Auch eine zeitliche Planung der Ausführung ist möglich, so kann z. B. eine Neuinstallation auf den Abend verlegt werden. Nach dem erfolgreichen Abschluss des Jobs wird dann das Ticket automatisch geschlossen. Genehmigungspflichten für die Installation lizenzpflichtiger Software werden einfach vordefiniert und die entsprechende Anfrage an den Vorgesetzen automatisch ausgelöst. Dieser Workflow kann in Ticketvorlagen gespeichert werden und so ggf. auch als Self Service für die Endnutzer angeboten werden. Eine integrierte Knowledge Base ermöglicht die Verwaltung, Verschlagwortung und Verknüpfung von Artikeln, Selbsthilfeanleitungen sowie aufgezeichnete Lösungen. Diese Datenbank kann sowohl den internen Bearbeitern als auch den Endbenutzern über ein Kundenportal zur Verfügung gestellt werden.

3.1.5 Reporting

Alle Anfragen und Maßnahmen werden automatisch erfasst. Über individuell definierbare Filter und Ansichten können jederzeit umfassende Auswertungen erstellt und über die Reporting-Schnittstelle an externe BI-Systeme exportiert werden. Darüber hinaus steht ein individuell konfigurierbares KPI-Dashboard für einen schnellen Überblick zur Verfügung.

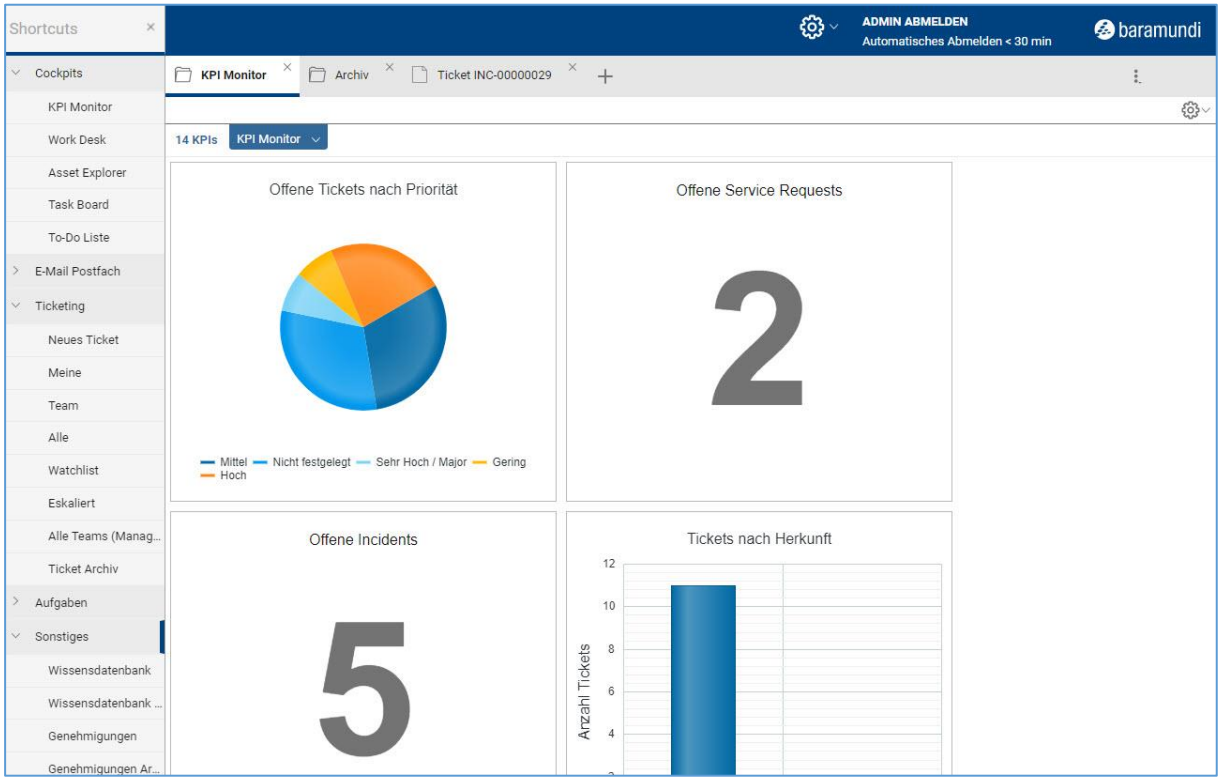


Abbildung 48 - KPI-Dashboard für einen schnellen Überblick

3.1.6 Ticketing aus der Cloud

Das Ticketing System ist cloudbasiert, so dass es sehr einfach bereitgestellt werden kann. Es wird über einen Connector mit Ihrer baramundi Management Suite verbunden.

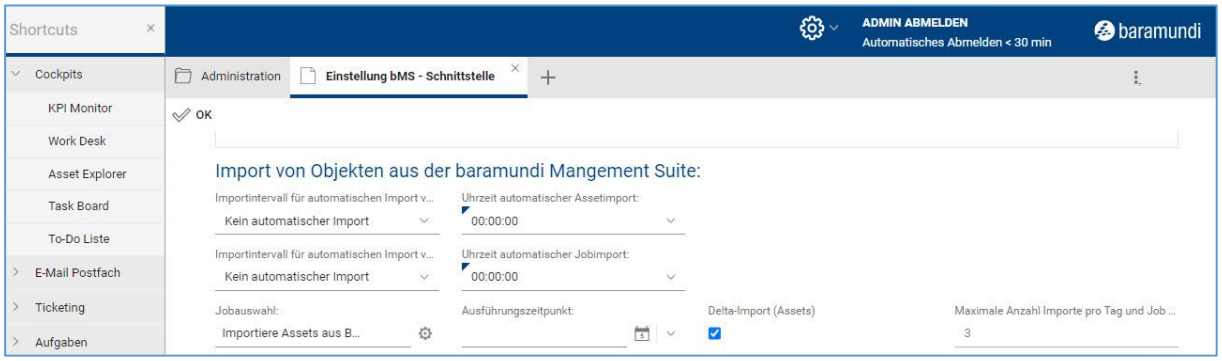


Abbildung 49 - Konfiguration der bMS-Schnittstelle

Die Kommunikation erfolgt ausschließlich über den Connector und ist nach Industriestandard verschlüsselt.

3.2 Microsoft Update Management

Bei der Installation von Updates stehen Administratoren jeden Monat vor derselben Herausforderung: Sicherheitslücken müssen zeitnah geschlossen, die Funktion und damit der reguläre Betrieb der Endpoints darf aber nicht gestört werden. Als Best Practice hat sich das gestaffelte Rollout von Updates bewährt. Hierbei werden Updates zuerst auf einer kleinen Teilmenge der im Unternehmen befindlichen Endpoints – unabhängig von Abteilung oder Kritikalität – installiert und getestet, bevor sie in Wellen im restlichen Unternehmen verteilt werden. Diese Wellen können sich überlappen, um Sicherheitslücken möglichst schnell zu schließen, oder sie starten zeitlich – z.B. um mehrere Tage – versetzt, um problematische Updates früh identifizieren und den Rollout bei Bedarf unterbrechen zu können.

3.2.1 Das Updateprofil als zentrale Konfiguration

Zur granularen Steuerung des Updateverhaltens stehen nun Updateprofile zur Verfügung. Innerhalb der Profile wird definiert, mit welchem zeitlichen Versatz ab Veröffentlichung ein Update installiert werden darf. So können Updates um bis zu 30 Tage nach hinten verschoben werden.

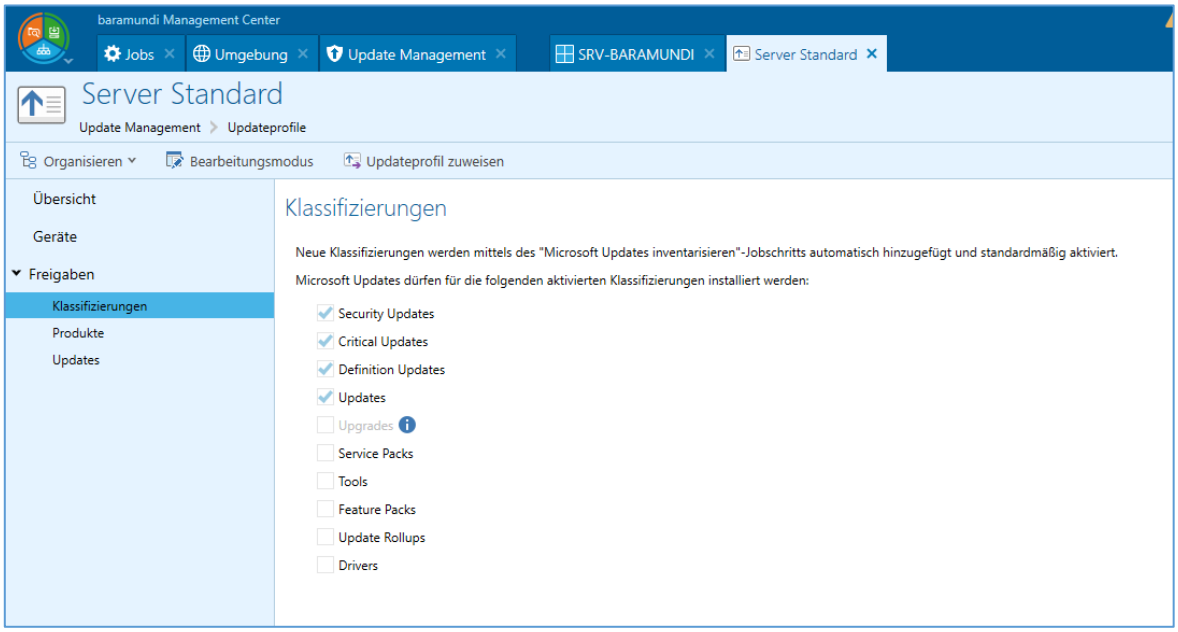


Abbildung 50 - Freigabe der Klassifizierungen im Updateprofil

Ebenso können am Updateprofil einzelne Updatekategorien komplett ausgeschlossen werden, um z.B. Treiber generell nicht über Microsoft Update zu installieren. Selbstverständlich können auch einzelne Produkte und sogar gezielt einzelne Updates vom Updatevorgang

ausgeschlossen werden – so verhindern Sie sicher, dass ein problematisches Update in einer definierten Gruppe durch den Update-Job installiert wird.

3.2.2 Detaillierte Information über den Update-Zustand

Bereits mit der bMS 2020 R2 wurde die Inventur der Microsoft Updates eingeführt. Diese Ansicht wurde um die Einstellungen durch das Updateprofil erweitert. So erkennen Sie nun nicht nur auf einen Blick, welche Updates fehlen, sondern auch aus welchem Grund. Ebenso ist sofort erkennbar, ab wann ein verzögertes Update installiert werden kann.

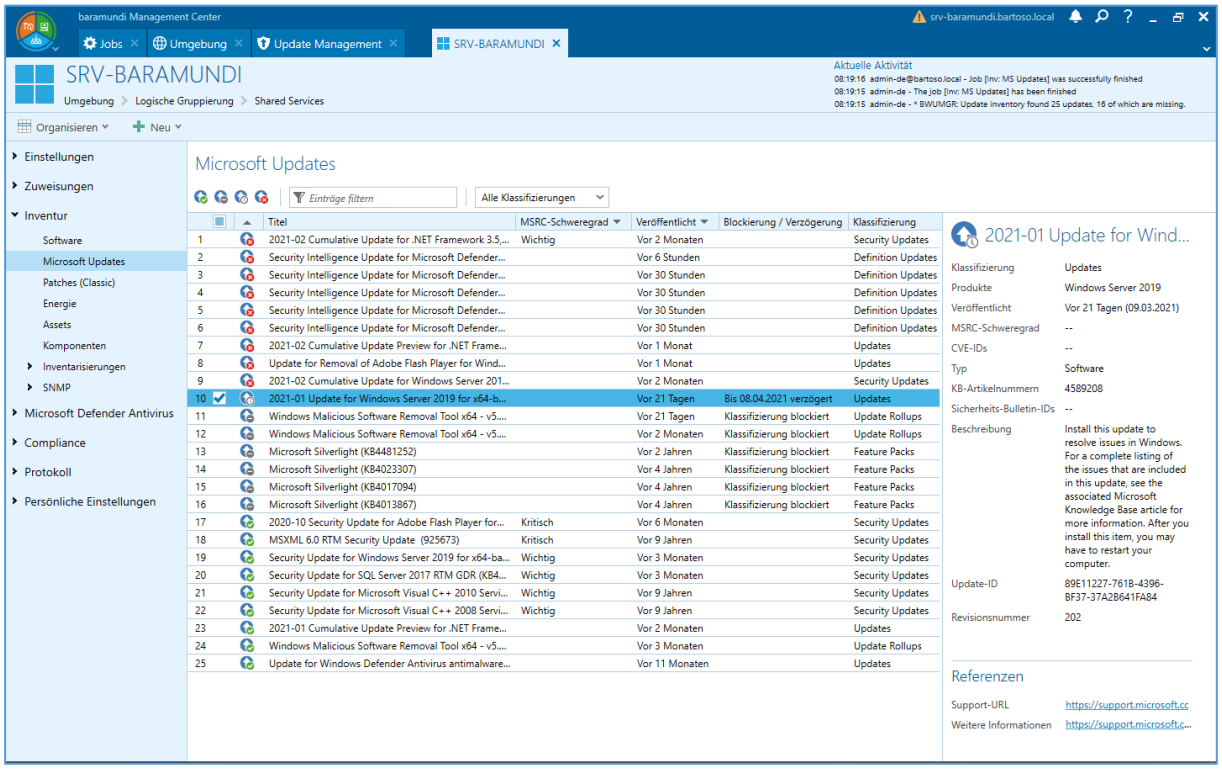


Abbildung 51 - Übersicht der Updates eines Endpoints mit jeweiligem Update-Zustand

3.3 Verwaltung des Microsoft Defender Antivirus

Microsoft liefert mit dem Defender Antivirus eine zuverlässige, in Windows integrierte Antivirus-Lösung frei Haus. So ist der breite Einsatz in Unternehmen und auch der Wunsch zur zentralen Verwaltung nicht überraschend. Da dieser Wunsch auch in unserem Feedback-Portal sehr viel Zuspruch fand, wurde die zentrale Verwaltung des Microsoft Defender Antivirus als Funktion in das Modul *baramundi Defense Control* aufgenommen.

3.3.1 Zentrale Sicht auf den Bedrohungszustand

Der Zustand des Endpoints wird nun detailliert in der bMC angezeigt. So ist sofort ersichtlich, ob der Defender Antivirus ordnungsgemäß funktioniert und auch die darunterliegenden Module und Komponenten ihren Dienst verrichten.

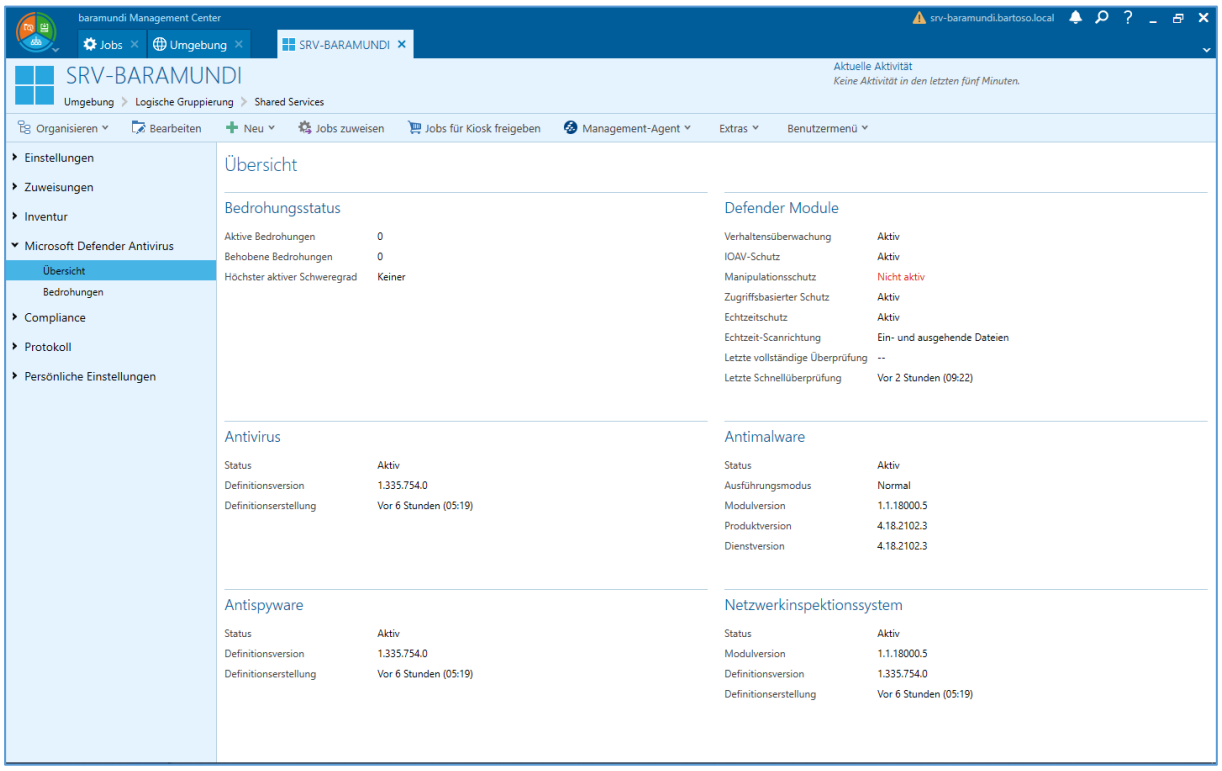


Abbildung 52 - Details zum Status des Defender Antivirus am Endpoint

Zusätzlich werden alle am Endpoint gefundenen Bedrohungen an den bMS übermittelt und stehen dort zur Auswertung zur Verfügung.

Da diese Daten für alle Endpoints in der Umgebung zentral am bMS gesammelt werden, ist die Auswertung für die gesamte Umgebung möglich. Bei Bedarf kann auf einzelne Gruppen oder Endpoints fokussiert werden.

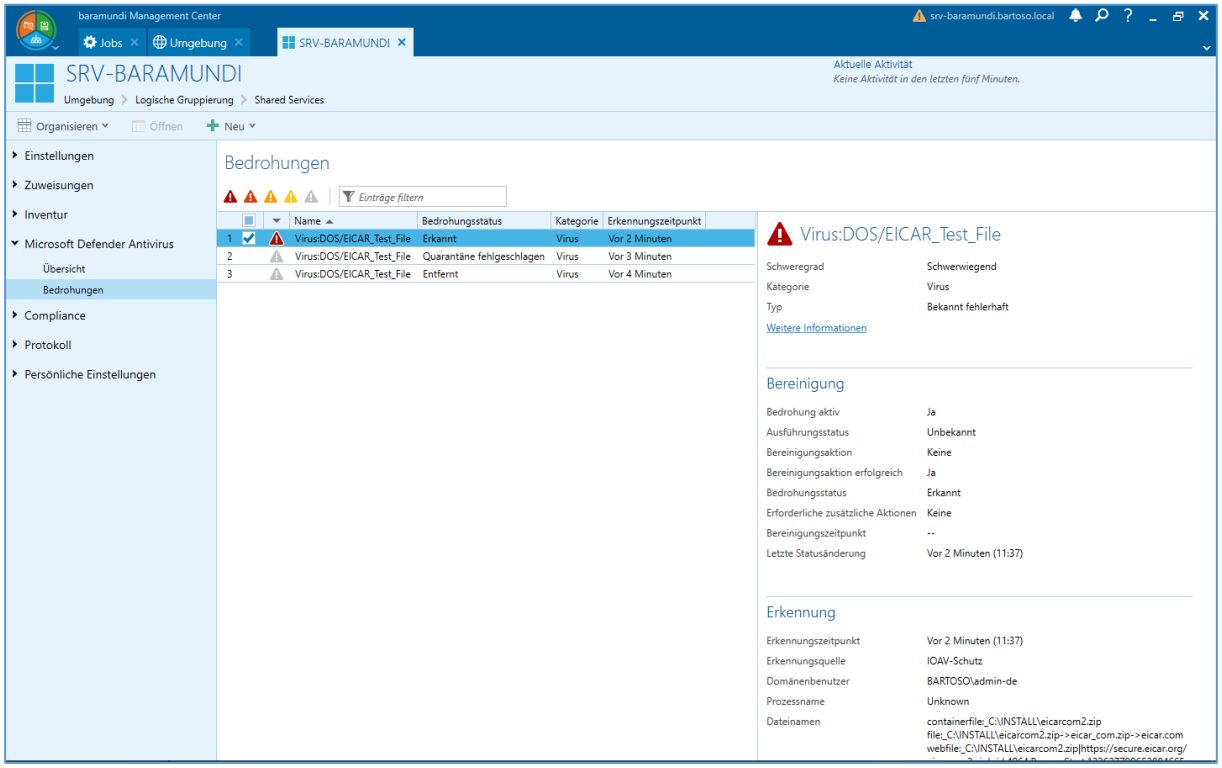


Abbildung 53 - Liste der Bedrohungen einer Gruppe inkl. Untergruppen

3.3.2 Aktiv eingreifen, Bedrohungen beseitigen

Selbstverständlich bietet die bMS nun auch Möglichkeiten um die gefundenen Bedrohungen aktiv aufzulösen. So kann nun ein Update der Virendefinitionen gezielt per Jobschritt ausgelöst werden. Ebenso kann eine Schnellüberprüfung und eine vollständige Überprüfung im laufenden System durchgeführt werden. Für besonders hartnäckige Fälle – welche sich im laufenden Windows nicht entfernen lassen – ist die Offline-Überprüfung vorgesehen. Hierbei startet der Endpoint in WindowsPE und führt dort eine Überprüfung durch.

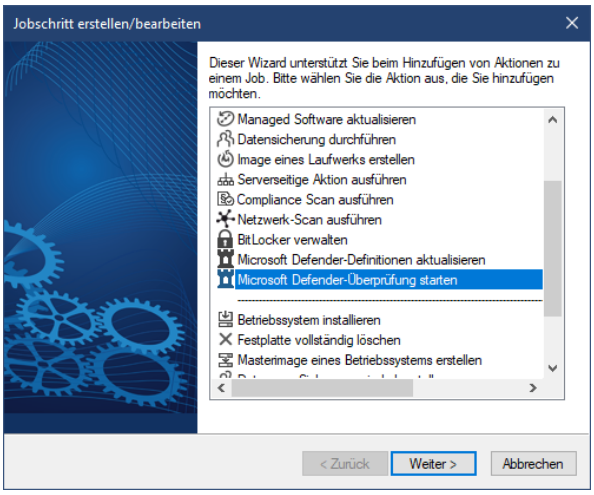


Abbildung 54 - Jobschritte zur Aktualisierung der Virendefinition und Überprüfungen

3.4 baramundi Argus Cockpit

Der Funktionsumfang des Moduls *baramundi Argus Cockpit* (bAC) wächst seit der Release 2020 kontinuierlich. Viele dieser neuen Funktionalitäten können ohne Versionsupdate der bMS genutzt werden, so dass die folgenden Umsetzungen bereits vor dem bMS Release 2021 R1 zur Verfügung stehen[4].

3.4.1 Individuelle Schwellwerte für UDG festlegen

Seit Release 2020 R2 können Universelle Dynamische Gruppen (UDG) in der bMS mit dem Argus Cockpit synchronisiert werden, so dass diese Ergebnislisten ggf. auch mit anderen Mitarbeitern im Unternehmen geteilt werden können, die keinen Zugriff auf das baramundi Management Center haben.
Um es aber dem bAC-Nutzer zu erleichtern, insbesondere kritische Zustände ihrer Umgebungen „auf einen Blick“ zu erkennen, werden diese Zustände im Argus Cockpit farblich mit Ampelfarben visualisiert.

[4] https://www.baramundi.com/de-de/management-suite/module/baramundi-argus-cockpit/updates/

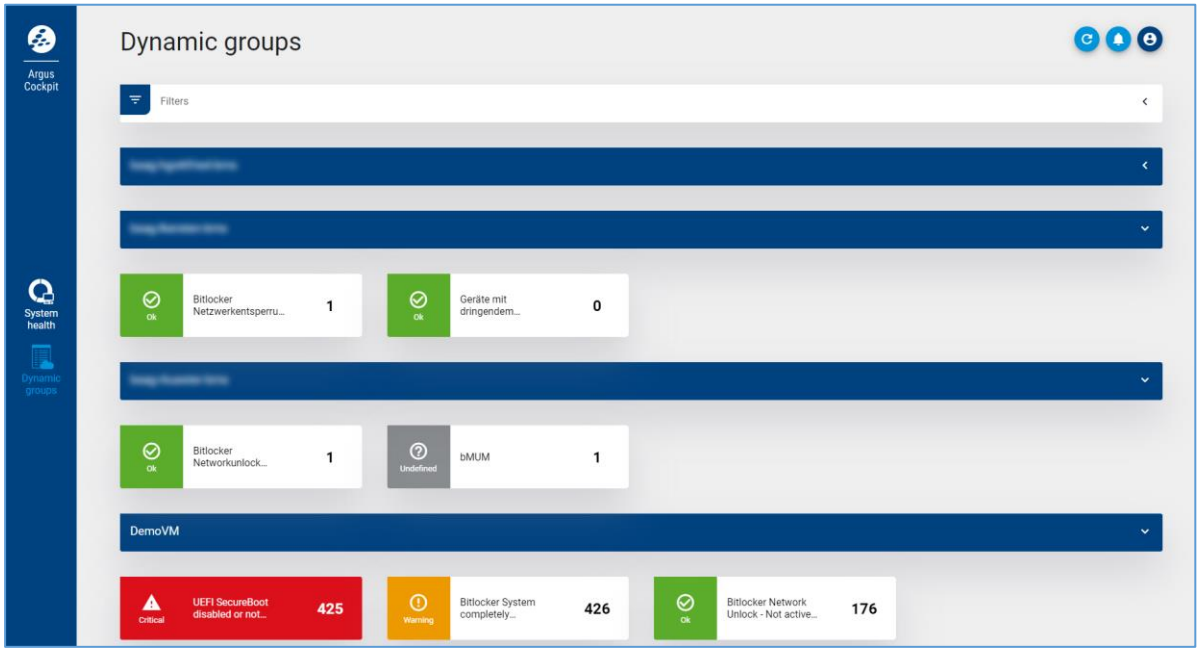


Abbildung 55 - Farbliche Markierungen der UDG

bAC-Nutzer können nun individuelle Schwellwerte für jede synchronisierte UDG im baramundi Argus Cockpit festlegen. Beim Erreichen der festgelegten Schwellwerte, werden die UDGs entsprechend farblich markiert. Damit wird dem IT-Administrator signalisiert, dass ggf. Handlungsbedarf besteht und Aktionen in der bMS initiiert werden müssen.

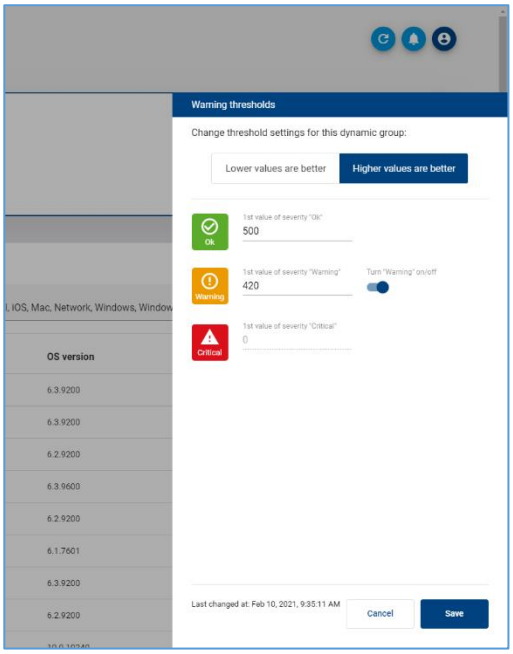


Abbildung 56 - Individuelle UDG-Schwellwerte festlegen

3.4.2 Historische Daten mit Argus Trends anzeigen

Die bMS zeichnet u.a. aus, dass sie dem IT-Admin einen sehr guten Überblick über die gesamte IT-Umgebung bietet und aktuelle Parameter der Endgeräte anzeigt, so dass er – falls

notwendig – entsprechende Aktionen auf den jeweiligen Endgeräten initiieren kann, wenn deren IST-Zustand nicht dem SOLL-Zustand entspricht.
Es ist in bestimmten Situationen hilfreich, die Zustände der Endgeräte über einen (längeren) Zeitraum hinweg zu betrachten und zu analysieren. Mit den neuen Argus Trends ist dieser „Rückblick“ nun möglich.

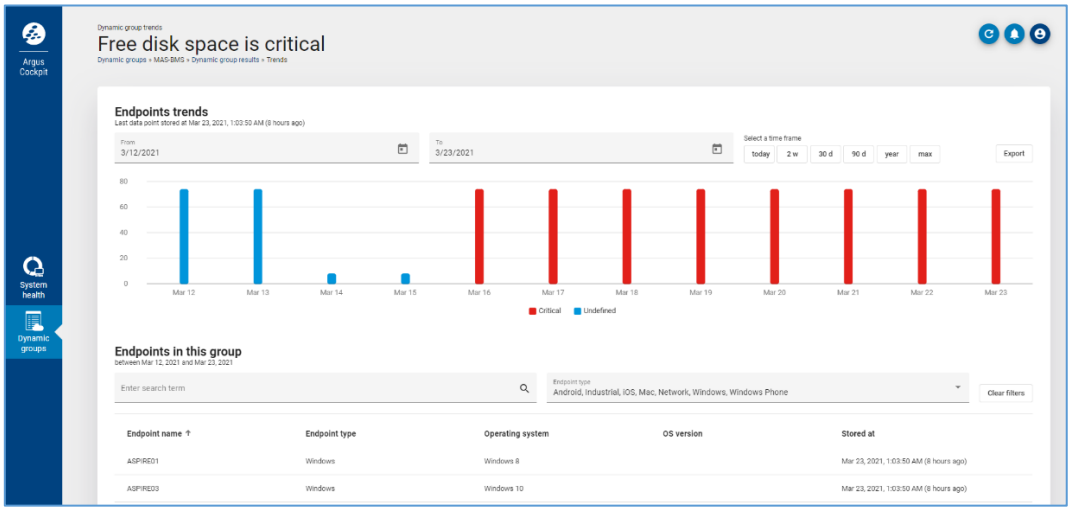


Abbildung 57 - Trends von UDG-Ergebnismengen

So können IT-Admins nun beispielsweise darstellen, wie viele kritische Updates auf einem Endgerät (oder mehreren Endgeräten) in den letzten 4 Wochen nicht installiert wurden. Insbesondere für ein bevorstehendes Security-Audit oder Reporting gegenüber dem CISO sind diese Informationen sehr hilfreich.

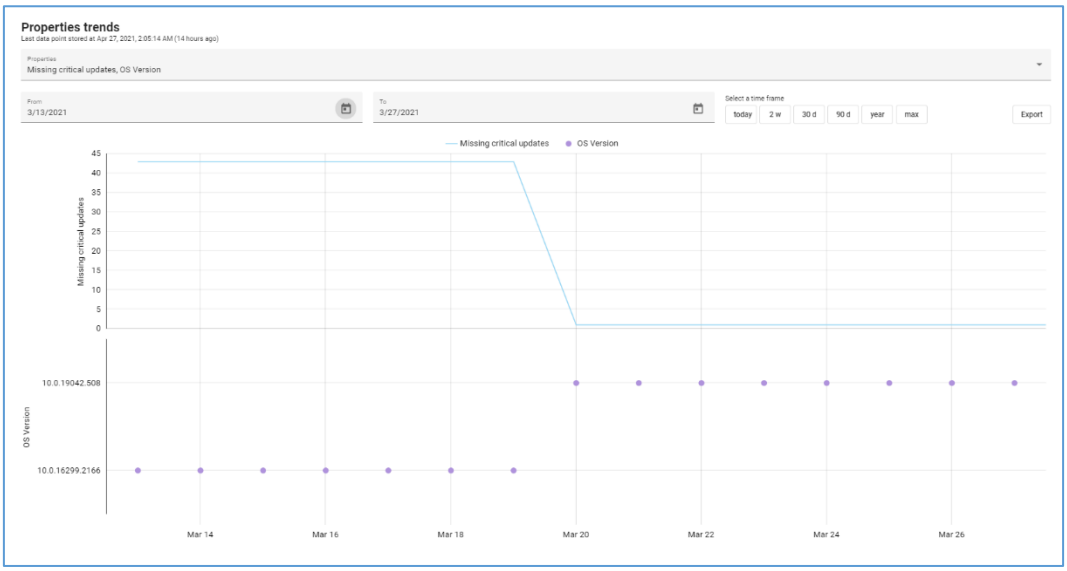


Abbildung 58 - Historische EP-Daten in Argus Trends anzeigen

Neben den Trends der fehlenden kritischen Updates stehen folgende weitere historische Endgeräte-Informationen im Argus Cockpit zur Verfügung:

- BitLocker Network Unlock Status
- System Volume BitLocker Status
- OS Version
- Last Channel

Ferner ist es für MSP auch hilfreich, die UDG-Ergebnismengen und deren definierte Schwellwerte anzeigen, analysieren und reporten zu können. Ob und wie viele Endgeräte in den letzten Tagen oder Wochen z.B. ein Inplace Upgrade benötigten, lässt sich nun ggü. Kunden oder anderen Rollen im Unternehmen einfach berichten.

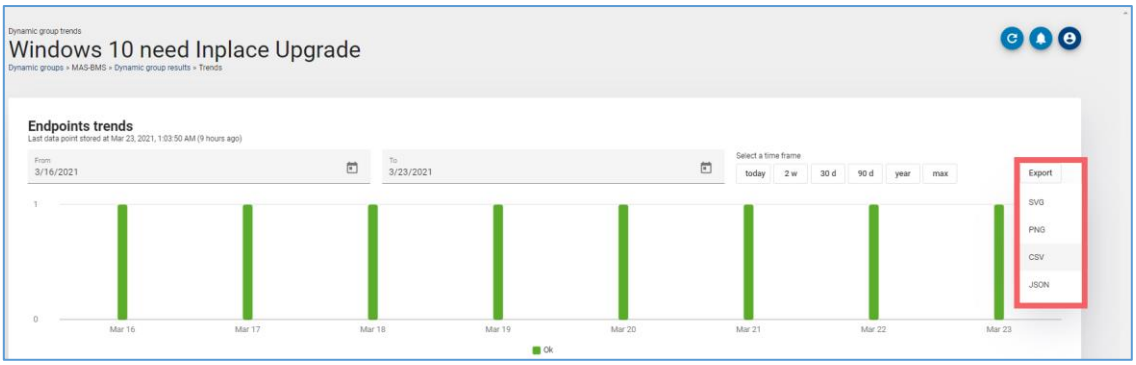


Abbildung 59 - Einfacher Export relevanter UDG-Trends

3.4.3 Weitere relevante Daten in Argus sichtbar

Wie bereits im Kapitel 0 beschrieben, werden ab dem Release 2021 die Microsoft Defender Antivirus Informationen mit der bMS erfasst. Diese Informationen werden auch ins Argus Cockpit übertragen und können somit von den IT-Admins jederzeit eingesehen werden und/oder zur Definition von UDG verwendet werden.

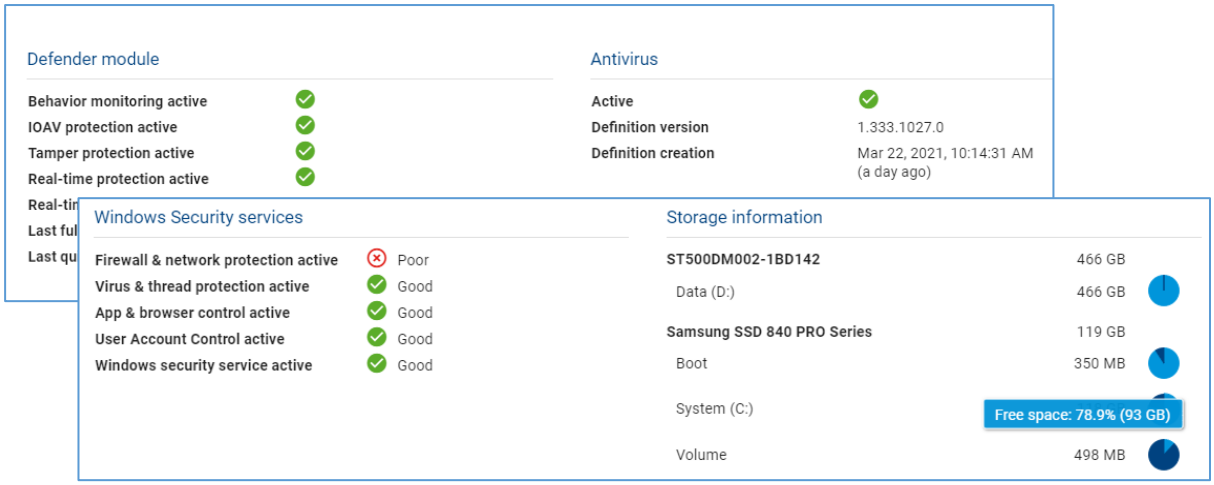


Abbildung 60 – Übersichtliche Ansicht der MS Defender und weitere Informationen

3.5 bCenter – Die Hosentaschen-bMC

Die mobile Version des baramundi Management Center wurde komplett überarbeitet und ist nun für Apple iOS und Google Android verfügbar.

[5]

[6]

Mit dem mobilen bCenter können Sie z.B. einen Update-Job vom Smartphone oder Tablet aus starten oder auch den Zustand der Endpoints kontrollieren, es ist kein Windows-PC mit installiertem baramundi Management Center nötig.

3.5.1 Endpoints verwalten

Mit dem bCenter können Sie Ihre Umgebung durchsuchen und so durch die bekannten Gruppen navigieren. Ebenso können Sie einzelne Endpoints über die Suchfunktion (inkl. QR-, Barcode- und NFC-Scanner) auffinden. So können Sie auf die Informationen der einzelnen Endpoints zugreifen, Details zum System anzeigen, Jobs zuweisen, den Status prüfen und sogar Variablen anzeigen und bearbeiten.

3.5.2 Jobs zuweisen

Über die Jobs-Sicht haben Sie Zugriff auf alle vorhandenen Jobs. Hier können Sie entweder durch die Ordner navigieren, oder den gewünschten Job per Suchfunktion finden. Im Anschluss kann der gewählte Job auf einen Endpoint zugewiesen werden.

3.5.3 Usability

Bei der Umsetzung haben wir besonderen Wert auf die Kundenwünsche im Feedback-Portal gelegt. Neben der Multiplattform-Kompatibilität stand die Usability im Vordergrund und so unterstützt die App folgende Funktionen:

3.5.3.1 Dark mode

Die Anzeige kann nun auf Wunsch in eine augenfreundliche, dunkle Darstellung geändert werden.

[5] https://apps.apple.com/de/app/baramundi-management-center/id1069301410
[6] https://play.google.com/store/apps/details?id=com.baramundi.android.bcenter

3.5.3.2 Mehrsprachigkeit

Neben Deutsch wird auch Englisch als Anzeigesprache unterstützt. Weitere Sprachen sind in Planung.

3.5.3.3 Login mit biometrischen Sensoren

Nach Eingabe des Servers, den Benutzernamens und Passworts können diese Daten sicher auf dem Gerät gespeichert und per biometrischem Sensor entsperrt werden. Somit ist bei einem Neustart der App keine erneute Eingabe des Passworts notwendig.

3.5.3.4 Favoriten

Für einen schnellen und komfortablen Zugriff auf die am häufigsten Verwendeten Endpoints und Jobs können diese als Favorit markiert und auf der Startseite gepinnt werden. So haben Sie besonders kritische Endpoints oder den Job für das aktuelle Rollout stets griffbereit und im Blick.

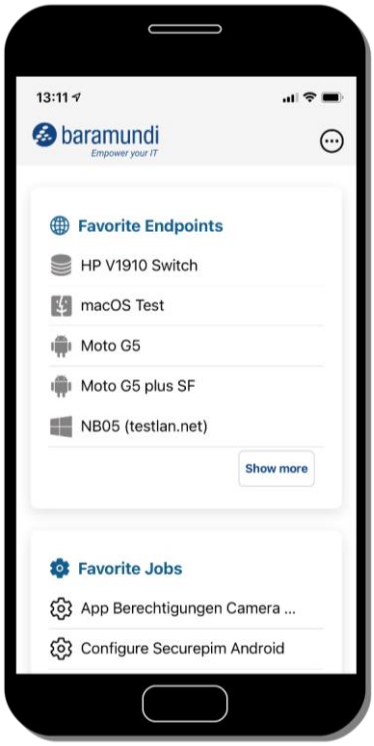


Abbildung 61 - Startseite mit Favoriten

3.5.3.5 Filter

Alle Ansichten im bCenter verfügen nun über Plattformfilter. So können Sie z.B. gezielt nur Windows-Endpoints oder auch nur die mobilen Endpoints mit iOS- und Android-Betriebssystem auflisten. Alle anderen Plattformen werden ausgeblendet. Ebenso können Sie bewusst nur Jobs für die gewünschte Zielplattform auflisten.

3.5.3.6 NFC-Tags

Neben der Erfassung von QR- und Barcodes, kann das bCenter auch NFC-Tags lesen und schreiben. So können Sie aus der App heraus Endpoint-Daten auf ein NFC-Tag schreiben. Sobald ein entsprechender NFC-Tag in der App gelesen wird, öffnet sich umgehend der assoziierte Endpoint mit allen relevanten Daten.

3.6 Allgemeine Weiterentwicklung

3.6.1 License Management

Das *baramundi License Management* bietet eine kompakte und einfache Möglichkeit, um kaufmännische Informationen aus dem Lizenzmanagement zu berücksichtigen und damit eine bessere Transparenz, der im Unternehmen vorhandenen Lizenzen zu erreichen.

Mit der neuen Version können Lizenzen mit Mehrfachnutzungsrechten dargestellt werden.

3.6.1.1 Konzept

Auf Rechnern verwendete Software-Installationen bieten über den jeweiligen Lizenztyp unterschiedliche Nutzungsrechte. Bei Mehrfachnutzung kann dies auf Geräte und/oder Benutzer bezogen sein.

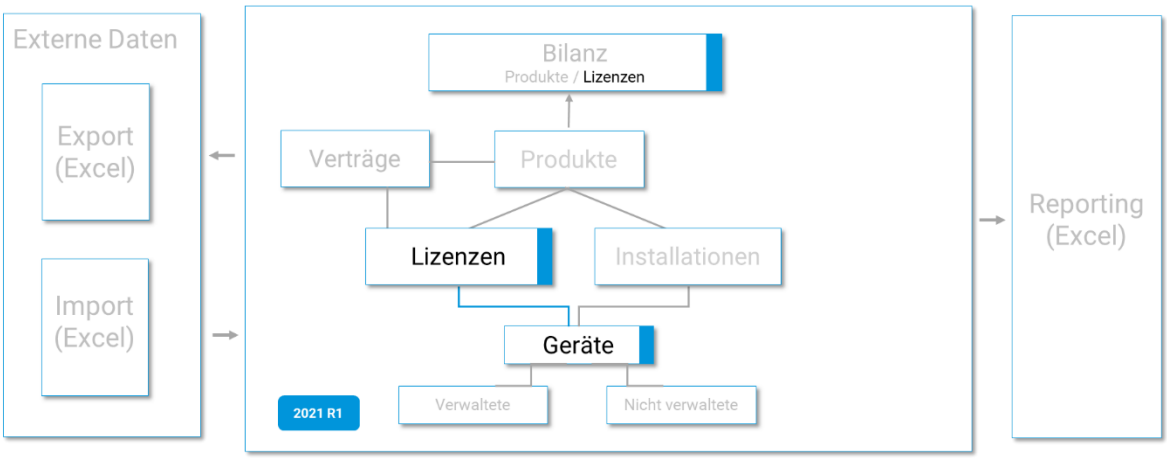


Abbildung 62 – Lizenz Management Gesamtkonzept 2021 R1

3.6.1.2 Mehrfachnutzung von Lizenzen über Gerätegruppen

Mit Release 2021 lösen wir die bisherige Abbildung von Mehrfachnutzungen ab. Statt einer manuellen Anpassung der Summen enthält das Modul jetzt die Darstellungsmöglichkeit von Gerätegruppen zum entsprechenden Produkt.

Über das individuelle Anlegen von Gerätegruppen können unterschiedliche Mehrfachnutzungsszenarien abgebildet werden.

Wenn eine Lizenz die Nutzung für einen Anwender auf mehreren Geräten ermöglicht, kann dies über eine Gerätegruppe mit Endpunkten des gleichen Benutzers abgebildet werden. Der Lizenzbedarf dieser Gruppe kann laut Nutzungsrecht bspw. mit 1 eingetragen werden. Dadurch passt sich der Lizenzbedarf der Bilanz entsprechend an.

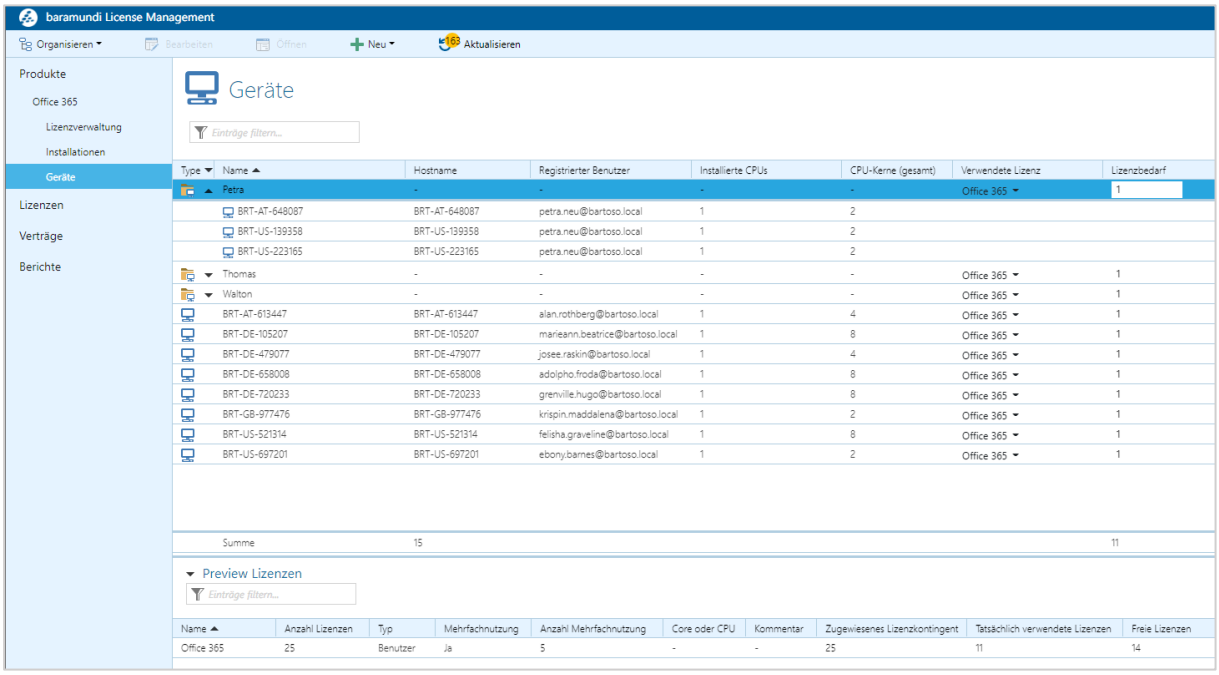


Abbildung 63 - Mehrfachnutzung von Lizenzen über Gerätegruppen

3.6.1.3 Flexible Lizenzverwendung an Geräten

Verwendet man unterschiedliche Lizenzen innerhalb eines Produktes, kann die Zuordnung flexibel erfolgen. Darüber hinaus kann ein individueller Lizenzbedarf pro Gerät definiert werden, um beispielsweise Core und CPU Lizenzmodelle abzubilden.

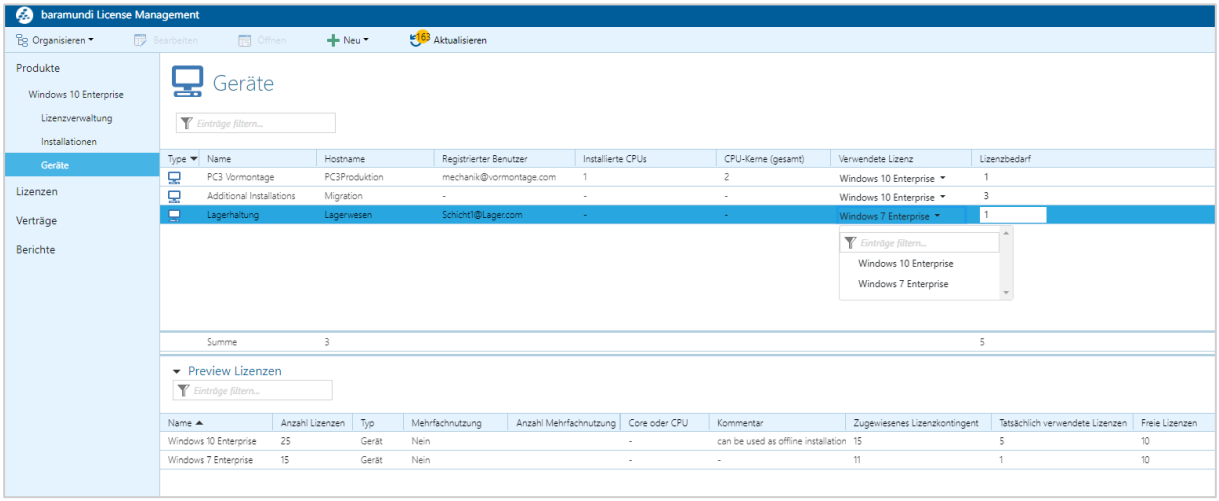


Abbildung 64 - Flexible Lizenzverwaltung an Geräten

3.6.1.4 Lizenzbilanz

In der Ansicht Lizenzen wird jetzt eine Lizenzbilanz dargestellt. Mögliche Unter- und Überabdeckungen können einfach im Blick behalten und Korrekturen zielgerichtet mit Unterstützung von Filtern durchgeführt werden.

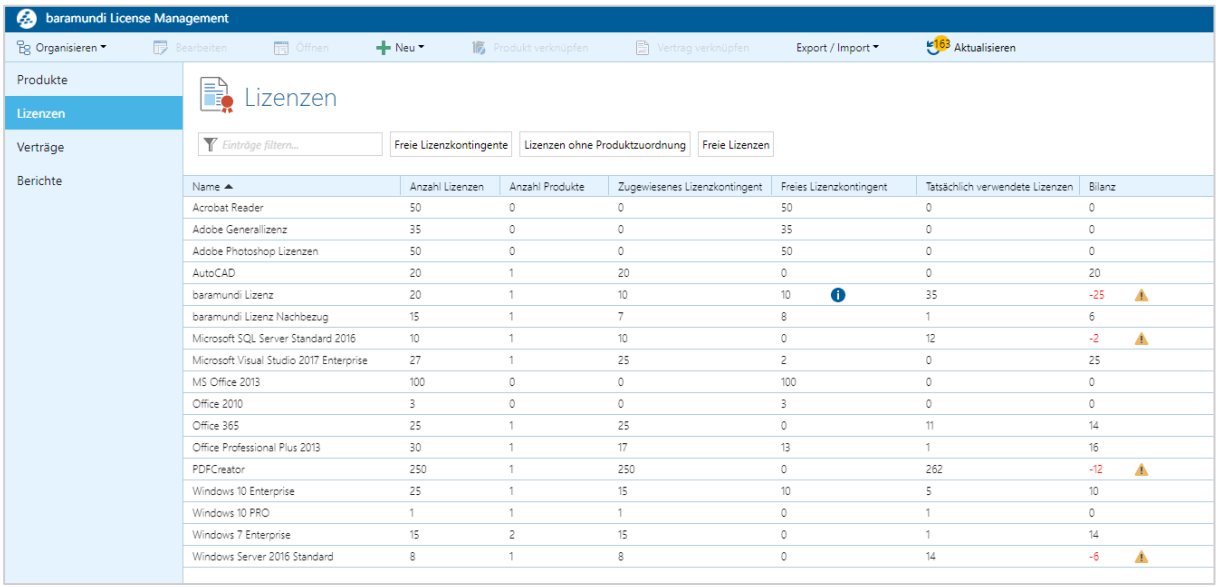


Abbildung 65 - Lizenzbilanz

3.6.2 baramundi Network Devices – Netzwerk-Landkarte

Im Rahmen der Weiterentwicklung der Netzwerk-Landkarte (früher: IT-Landkarte) kann als Preview ein neuer, optionaler Algorithmus verwendet werden. Dieser verwendet zusätzliche Daten zur Topologieberechnung.

Zusätzlich zum Strukturaufbau über das Spanning Tree Protokol (STP) erweitern wir mit dem Release 2021 die Darstellung der Netzwerk-Landkarte basierend auf den Forwarding Database (FDB) Einträgen.

Bisherige Mehrfachdarstellungen von Verbindungen wie auch nicht verwalteten Bereichen werden dadurch vermieden. In Netzwerken, in denen kein STP aktiv ist, wird nun ein performanter Aufbau der Netzwerk-Landkarte ermöglicht.

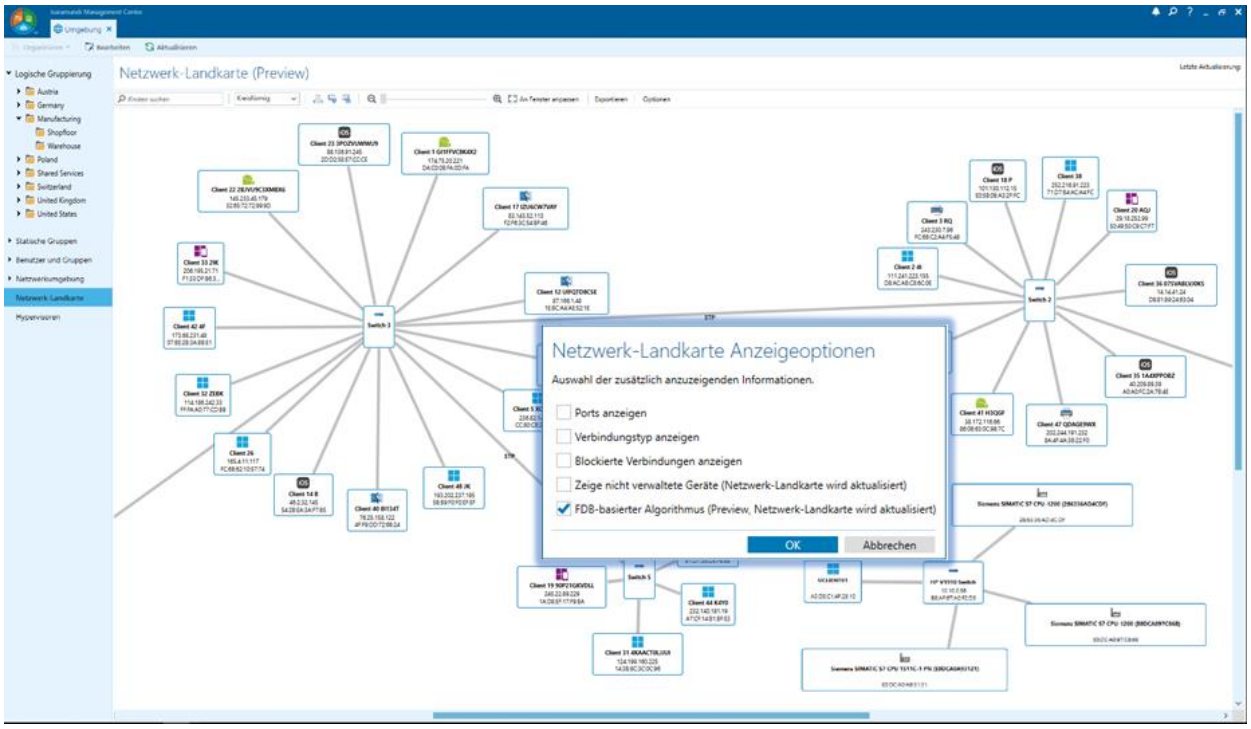


Abbildung 66 - Netzwerk-Landkarte mit optionalem Algorithmus

3.6.3 Neue Funktionen für Apple macOS

3.6.3.1 Apple Automated Device Enrollment für macOS

Auch die Aufnahme von Apple Geräten mit macOS wurde weiterentwickelt. So unterstützt die bMS nun auch die automatisierte Aufnahme der Geräte durch das Apple Automated Device Enrollment (früher Device Enrollment Program / DEP), inklusive komfortabler Einrichtung des administrativen Accounts.

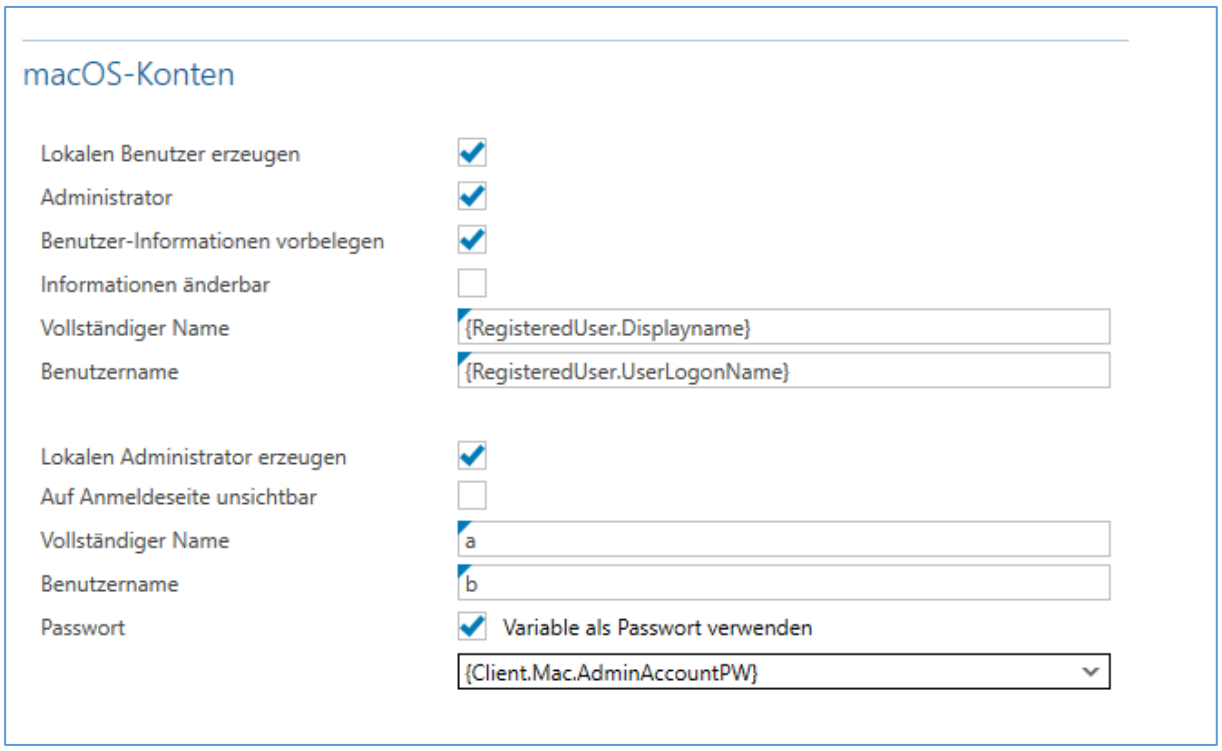


Abbildung 67 - Konfiguration der macOS-Konten mit baramundi-Variablen

Auf diesem Weg hinzugefügte macOS-Geräte werden nativ ins Management aufgenommen und können so auch über das baramundi Gateway – somit außerhalb des Firmennetzes – verwaltet werden.

3.6.3.2 Verwaltung von macOS-Apps per VPP

Nativ verwaltete macOS-Geräte profitieren nun auch von Apples Volume Purchase Program. Somit können Sie nun Apps aus dem Apple App Store über die bMS auf diese Geräte verteilen.

3.6.4 Windows 10 Inplace-Upgrade per IEM

Der Jobschritt zur Inplace-Aktualisierung eines Windows 10 Endpoints kann nun auch per IEM verwendet werden. Somit können Sie nun auch die im Home Office befindlichen Endpoints komfortabel auf die neueste Windows 10 Version aktualisieren.

3.6.5 Active Directory Synchronisation

Als Grundlage für essentielle Funktionen in der baramundi Management Suite stellt der AD-Sync eine komfortable Möglichkeit dar, Computer- wie auch Benutzerobjekte zu synchronisieren. Nicht nur der Verwaltungsdialog wurde hierbei von Grund auf überarbeitet und bietet nun eine intuitive Bedienbarkeit im gewohnten baramundi Management Center Design. Sondern es wurden auch zwei weitere Optionen im Bereich der Maschinensynchronisation integriert.

- **Nur aktive Geräte synchronisieren.**
  Deaktivierte Computerkonten im AD werden synchronisiert/übersprungen.
- **Nur Windows-Geräte synchronisieren**
  Andere Betriebssystemobjekte wie beispielsweise macOS synchronisieren/überspringen.

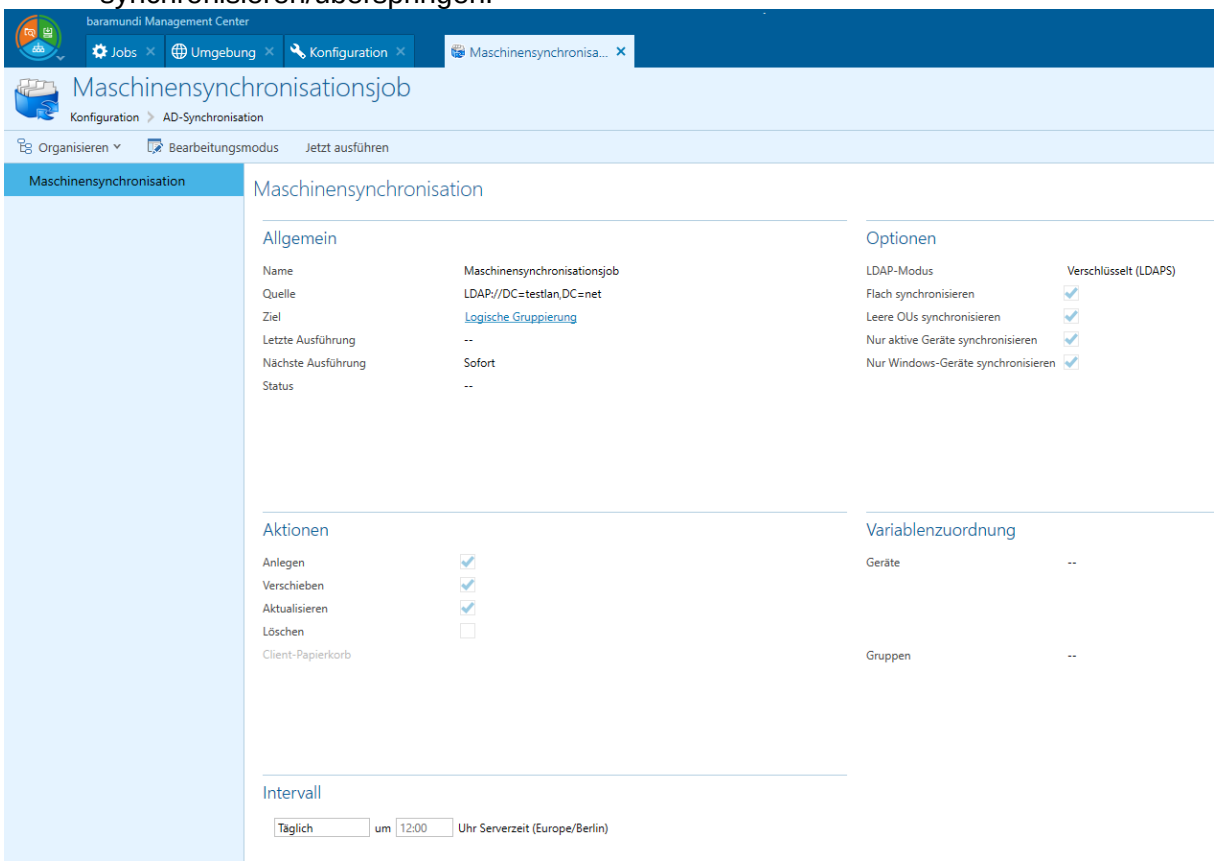


Abbildung 68 - AD-*Synchronisation* - Maschinen Synchronisation

Microsoft entwickelte darüber hinaus den Standard, um mit dem Domänencontroller zu sprechen, weiter und implementierte LDAPS. In der Version 2021 wird diese Kommunikationsmethode vom AD-Sync unterstützt und somit kann auf diese sicherere TLS Kommunikation (standardmäßig Port 636) umgestellt werden. Die weiteren

Kommunikationsmethoden (Ohne Signierung und Signiert mit Channel-Bindung) werden weiterhin unterstützt.

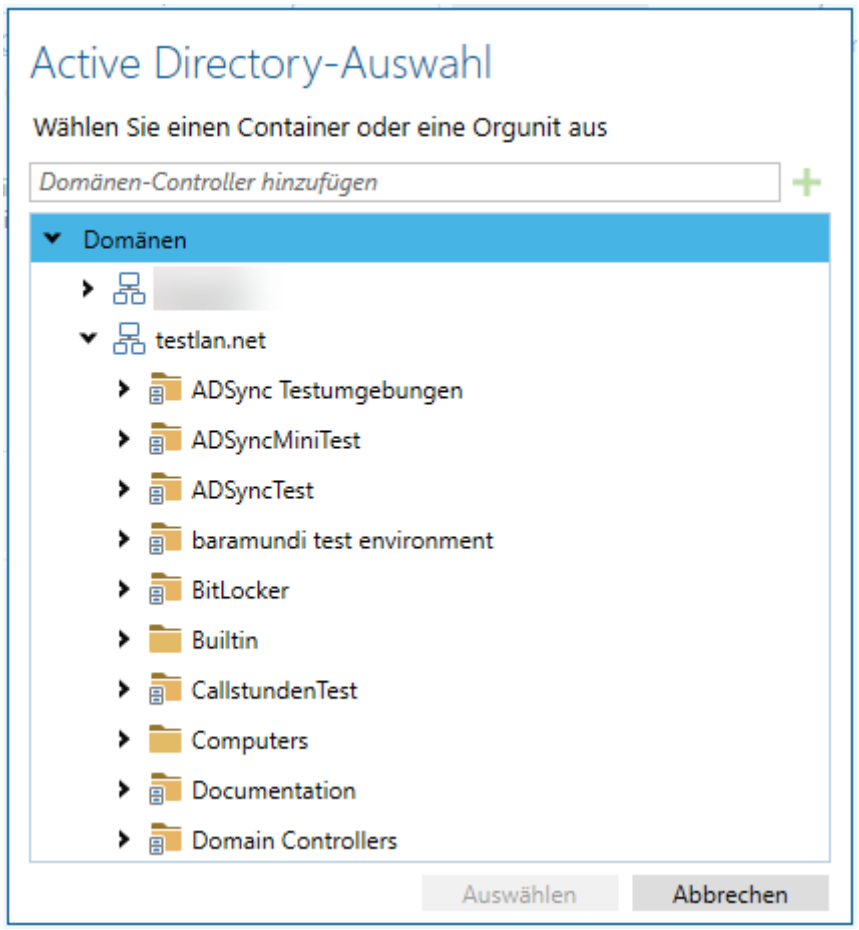


Abbildung 69 - Neuer AD-Synchronisation LDAPS Auswahldialog

Im Zuge dieser Anpassung konnte die grundlegende Arbeitsweise der Synchronisationsjobs ebenso optimiert werden. Das bedeutet, dass mit der Version 2021 R1 ein Maschinen- und ein Benutzer- Synchronisationsjob parallel laufen können und nicht sequenziell aufeinander warten müssen. Neben diesem Zeitgewinn ist die Laufzeit der Benutzersynchronisation drastisch reduziert worden.

3.6.6 Die bMC in dunklem Gewand – Dark Mode (Preview)

Neben den zahlreichen funktionalen Weiterentwicklungen gibt es auch eine optische Neuerung. So kann die bMC nun auch in den augenfreundlichen Dark Mode umgeschaltet werden. Die Einstellung kann von jedem Anwender selbst in den „Persönlichen Einstellungen“ vorgenommen werden.

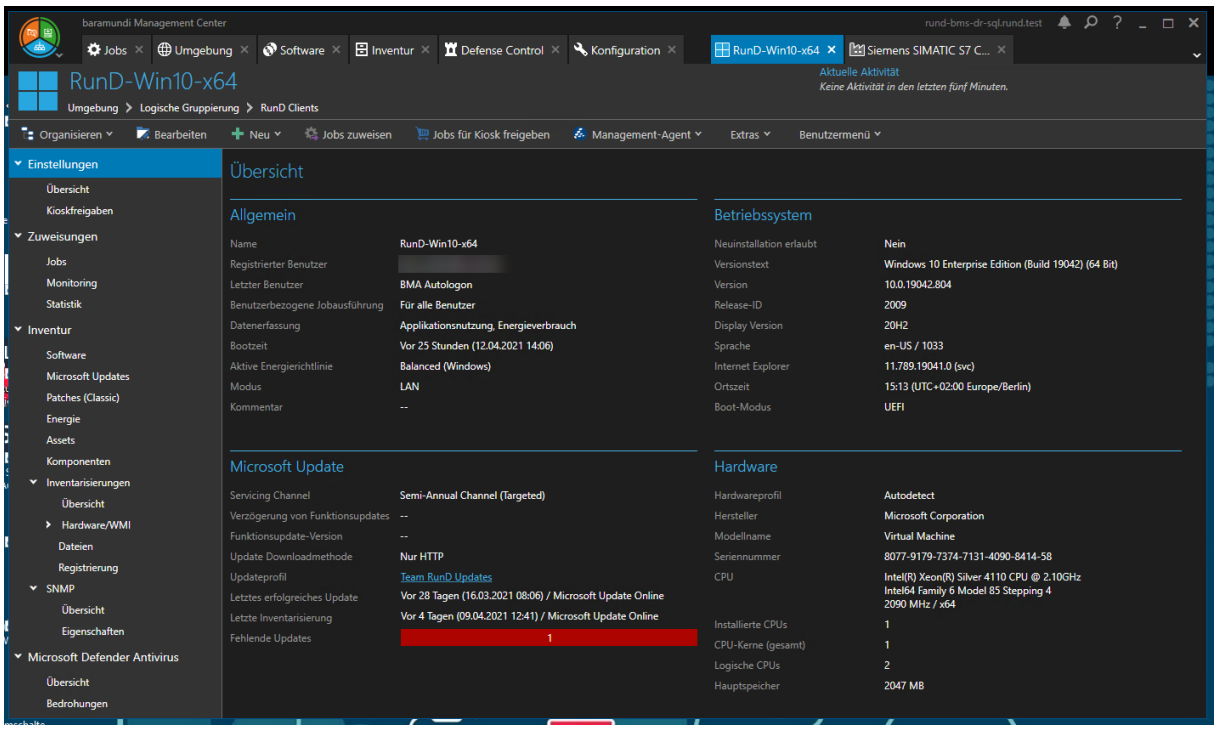


Abbildung 70 - Die bMC in der augenfreundlichen dunklen Darstellung

Wir freuen uns auf Ihr Feedback, um diese Funktion weiterzuentwickeln.

3.6.7 Bitlocker Network Unlock

Die Funktionalität der 2020 R2, einen baramundi Relay-Server als Bitlocker-Entsperr-Server einzusetzen, hat bereits Einzug in vielen Umgebungen erhalten. Das Feedback zu dieser Funktion erreichte uns und wurde mit dieser Version umgesetzt. Nun ist es möglich für diese Relay-Server einen Timeout in Stunden zu konfigurieren, in welchen die Relay-Server trotz Nichterreichbarkeit des Master-Servers, weiterhin Windows Endpoints die PIN-Abfrage ersparen.

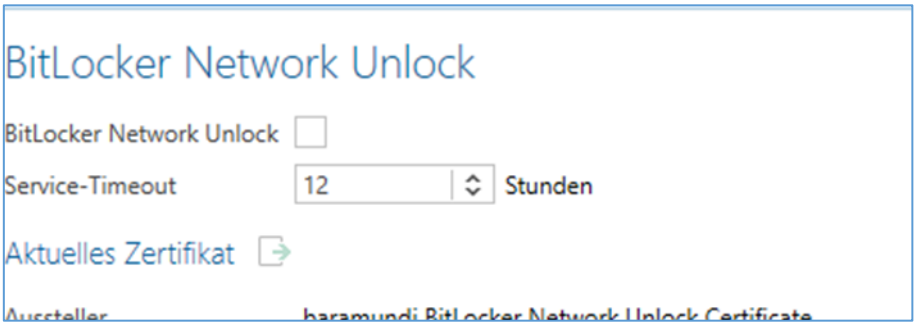


Abbildung 71 - Neuer Service Timeout bei Bitlocker Network Unlock

3.7 Produktverbesserungen im Detail

3.7.1 Windows Agent (bMA)

- Bugfix: Dateien, die größer als 5GB sind, können häufig nicht über bBT übertragen werden.

3.7.2 Management Center (bMC)

- Die Berechnung der IP-Netzwerke kann jetzt über den CIDR-Standard erfolgen. Dazu muss einmalig im Wartungsmodus auf dieses verbeserte Verfahren umgestellt werden und die bMC danach geschlossen werden. Das neue Verfahren führt in einigen Konstallationen dazu, dass die IP-Netzwerke nicht wie davor gemappt werden. Die IP-Netzwerke sind in diesen Fällen zu korrigieren.

- Die `IT-Landkarte` wurde weitgehend überarbeitet und in `Netzwerk-Landkarte` umbenannt.

- Unter `Persönliche Einstellungen – Benachrichtigungen` können `Download-Job Benachrichtigung` und `DB-Wartungsaufgabe Benachrichtigung` konfiguriert werden.

- Unter `Umgebung – Endgerät – Übersicht` wird zusätzlich zur IP die `Primäre Subnetzmaske` angezeigt.

- Die `Primäre Subnetzmaske` kann in `Dynamische Gruppe (Universell)` verwendet werden.

- Unter `Umgebung` stehen in allen Gerätelisten die gleichen Spalten wie bei `Dynamischen Gruppen (Universell)` zur Verfügung.
  Hinweis: Durch diese Umstellung der Gerätelisten werden die betreffenden Spalten beim erstmaligen Start der bMC auf Standard zurückgesetzt.

- Unter `Umgebung – Endgerät – Übersicht` werden unter `Systemsicherheit` zusätzlich `BitLocker Network Unlock Status`, `Bitlocker Status PIN aktiviert` und `Bitlocker Startup USB Key aktiviert` angezeigt.

- `Patches` wurde in `Patches (Classic)` umbenannt. Der Jobschritt `Microsoft Patches verteilen` wurde in `Microsoft Patches verteilen (Classic)` umbenannt.

- Unter `Konfiguration – Sicherheitsverwaltung – Sicherheitsprofile` ist ein neues Recht `Defense Control` für ein Sicherheitsprofil verfügbar.
- Für eine Software kann die Seite `Einstellungen – Übersicht` in eine Excel-Datei exportiert werden.
- Unter `Persönliche Einstellungen` stehen `Themes (Experimentell)` zur Verfügung. Damit kann die bMC auf `Dunkel (Preview)`, oder `Klassisch` eingestellt werden.
- Bei neuen Datenbanken werden die Beispiel-Assettypen in Englisch angezeigt.
- Als Report-Runtime wird die Crystal Reports Runtime in der Version 13.0.29 (SP29) verwendet.
- Am Windows-Endpoint wird beim Einstellen der Windows-Domäne im Dropdown-Menü die Liste der konfigurierten Domänen angezeigt.
- Nach einem erfolgreichen bDX-Import wird eine entsprechende Meldung angezeigt.
- Bugfix: In bestimmten Konstellationen entstehen beim Zurückziehen von Kioskfreigaben an einer Gruppe oder einem Gerät verwaiste Kioskfreigaben, welche nicht mehr gelöscht werden können.
- Bugfix: Die Jobzuweisung über die Seite `Software – Managed Software – Installiert auf` ist in bestimmten Konstellationen sehr träge.
- Bugfix: Der Name und Kommentar der Personal Backup Standardvorlagen wird auch auf englischen Systemen auf Deutsch angezeigt.
- Bugfix: Die Fortschrittsanzeige beim Jobtarget wird beim Neustart eines Jobtargets nicht zurückgesetzt.
- Bugfix: Beim Deaktivieren des Revisionslogs wird der Dialog zum Ändern des Passwortes angezeigt.
- Bugfix: Beim schnellen Scrollen in der Ansicht `Erweiterungen – Profile für mobile Geräte` werden falsche Icons dargestellt.
- Bugfix: Wird der Name einer Software geändert, welche bereits in Jobschritten verwendet wird, so wird der Name in der DetailView der Jobschritte nicht aktualisiert.

- Bugfix: Einstellungen für die Argus-Cloud-Connectoren werden teilweise beim Ändern des bConnect-Ports zurückgesetzt.

3.7.3 Update Management

- Der Jobschritt `Microsoft Patches verteilen` mit Updatequelle `baramundi Patch Management` (auf Basis der wsusscn2.cab) wurde umbenannt in `Microsoft Patches verteilen (Classic)`.
- Der Jobschritt `Microsoft Patches verteilen` mit Updatequelle `WSUS`, `Windows Update Online` oder `Microsoft Update Online` wurde umbenannt in `Microsoft Updates verteilen`.
- **Hinweis:** Um konsistente `Inventur-Microsoft Updates` Ansichten zu erhalten, sind bestehende Jobs mit Schritten `Microsoft Updates verteilen` anzupassen. Am letzten Patchschritt muss die Checkbox `Abschließende Updateinventur durchführen` gesetzt sein oder ein dedizierter Schritt `Microsoft Updates inventarisieren` enthalten sein.
- Zur detaillierten Steuerung der Updaterollouts ist die Konfiguration von Updateprofilen möglich.
- Updateprofile können einem oder mehreren Endpoints zugewiesen werden und sind am Client und an Clientlisten ersichtlich.
- Am Schritt `Microsoft Updates verwalten – Microsoft Updates verteilen` kann eine `Updateverzögerung in Tagen` eingestellt werden.
- Neue Option am Patchschritt `Qualitätsupdates verzögern (GPO) nicht ignorieren`.
- Bugfix: In bestimmten Situationen werden bereits ersetzte Patches heruntergeladen, obwohl diese nicht erforderlich sind.

3.7.4 OS-Install

- Der Jobschritt `Betriebssystem installieren – In-Place Upgrade` unterstütz jetzt baramundi Background Transfer (bBT) und kann auf Geräten im Internetmodus ausgeführt werden.

- Verbessertes Logging beim PXE-Boot über gesetzte DHCP Option / Bootloader.
- Beim Anlegen eines OS-Install Jobs mit der Installationsoption `Betriebssystem aus Abbilddatei` sind jetzt die zusätzlichen Boot-Umgebungen `Autodetect` und `Autodetect x86` verfügbar.
- Workgroup-Clients joinen die in der bMC angegebene Workgroup.
- Beim Hardwareprofil wird im Pfad für die manuelle Treiberzuordnung ein Beispielpfad angezeigt.
- Die Optionen `Bootpromptanzeige (Sek.)` und `Unbekannte Clients` wurden aus der `PXE-Server aktiv` Box herausgenommen, da diese unabhängig vom PXE-Server verwendet werden.
- Bugfix: Die Aufrufbeschreibung von bImaging.exe zeigt eine falsche Syntax bei `Example`.
- Bugfix: Wird in einem Hardwareprofil der Hauptspeicher mit mehr als 16GB angegeben, so erscheint eine entsprechende Meldung und das Speichern ist nicht möglich.
- Bugfix: Wird in einem Hardwareprofil der Prozessortakt mit mehr als 4GHz angegeben, so erscheint eine entsprechende Meldung und das Speichern ist nicht möglich.
- Bugfix: Die UEFI-Bootreihenfolge wird in bestimmten Konstellationen nicht korrekt gesetzt.
- Bugfix: Es wird der Installationsbenutzer der Domäne, welche an der logischen Gruppe des Clients angegeben ist, verwendet. Ab Release 2021 wird der Installationsbenutzer der am Client angegebene Domäne verwendet.

3.7.5 Mobile Devices

- Beim nahenden Ablauf des Apple-Profil-Signierungszertifikats wird eine bMC-Benachrichtigung angezeigt.
- Verbesserte Zustellung von Push-Benachrichtigungen für Android-Geräte im Standby-Modus.

- Die Joboption `Neuen Geräten zuweisen` kann nur von Benutzern gesetzt werden, welche das Recht `Job:AutoAssign bearbeiten` besitzen.
- Beim Enrollen eines Endgerätes wird eine Warnung angezeigt, wenn notwendige Einstellungen unter `Konfiguration – Mobile Devices` fehlen.
- Unter `Konfiguration – Mobile Devices – Allgemein – E-Mail` wird der `SMTP-Server Port` beim Aktivieren von `SSL-Verschüsselung verwenden` nur auf 465 gesetzt, wenn der Port nicht bereits manuell konfiguriert wurde.
- Im Jobschritt `Zweckbestimmtes Gerät verwalten – iOS/iPadOS` können jetzt auch importierte `*.ipa` Apps ausgewählt werden.
- Bugfix: Der Jobschritt `Zweckbestimmtes Gerät verwalten – Android Enterprise` kann keine `Layout-Vorlage` verteilen, wenn keine `Liste der ausführbaren Apps` gesetzt ist.
- Bugfix: App Permissions werden für lokale Apps in der bMC angezeigt, wenn die gleiche App auch aus dem App-Store importiert wurde.

3.7.6 bServer – AD-Synchronisation

- Die Funktionen `Benutzersynchronisationsjob` und `Maschinensynchronisierungsjob` wurden grundlegend überarbeitet.
- INetOrgPerson-Objekte werden unterstützt.
- Gruppenmitgliedschaften werden jetzt, wenn möglich, auch über Domaingrenzen hinaus aufgelöst.
- Der Kommunikationsmodus LDAPS wird unterstützt.
- Der Sync-Job wird auch im Fehlerfall immer neu geplant. Die Angabe spezieller Fehlercodes ist nicht mehr erforderlich.
- Neue Optionen: `Nur Windows-Geräte synchronisieren` und `Nur aktive Geräte synchronisieren.`
- Bei der AD-Variablenzuordnung wird die baramundi-Variable auf ihren Default-Wert gesetzt, wenn im AD das Attribut den Wert `<Nicht festgelegt>` hat.

- Hinweis: Benutzer/Maschinen/Gruppen/Ordner, welche ASCII-Steuerzeichen oder Unicode Zeichen enthalten, werden ignoriert.

3.7.7 Automation Studio (bDS)

- Ein HTML-Hyperlink in einem `Nachricht anzeigen` Fenster öffnet das Fenster jetzt im Standard-Browser des aktiven Benutzers.
- Das Fortschrittsfenster kann in der Größe manuell verändert werden.
- Bugfix: Die Rechtevergabe für Drucker ist teilweise nicht möglich.

3.7.8 Argus-Connect

- Zusätzliche Endpoint-Attribute werden zum Argus Cockpit übertragen.

3.7.9 Gateway

- Das Gateway-Setup verändert eine Systemeinstellung (Windows-Registry), damit wird das Versenden der Server Information im http Antwort-Header für alle http.sys basierten Schnittstellen abgeschaltet

3.7.10 bConnect

- Für das Microsoft Update Management können UpdateGruppen gelesen und geschrieben werden.
- Die UpdateGruppen können für einen Windows-Endpoint gelesen oder geschrieben werden.
- Bugfix: Werden Endpoints einer Dynamischen Gruppe ausgelesen, so ist der Wert „Lastboot“ falsch.

3.7.11 baraDIP

- Bugfix: Beim Start des baraDIP wird ein Eventlogeintrag der Form `The system cannot find the file specified, No installed ConfigArgs for the service "baraDIPhttpd", using Apache defaults` geloggt.
- Bugfix: In seltenen Situationen erhalten die DipServer vom bServer keine weiteren Synchronisierungsjobs. Die Synchronisierung der DipServer erfolgt dann erst nach einem Neustart des bServer Dienstes.

3.7.12 Defense Control

- Der Bitlocker Netzwerkunlock kann pro PXE-Relay konfiguriert werden. Zusätzlich ist ein „Network Unlock Relay Server Timeout“ einstellbar.

3.7.13 License Management

- Die Konfigurationsmöglichkeiten `Zusätzliche Installationen` (nicht mit baramundi verwaltet) und `Manuelle Anpassung (z. B. +10 oder -10)` unter Produkte – Produkt – Installationen wurden entfernt und automatisch auf fiktive Geräte mit dem Namen `Additional Installations` bzw. `Installation Correction` migriert.

4 Release 2020 R2 U1

4.1 Produktverbesserungen im Detail

4.1.1 Allgemein

- Das eingesetzte log4net Framework wurde aktualisiert. Die CVE-2018-1285 wird damit nicht mehr als false positive erkannt.
- Bugfix: Die Tabelle der eingeschränkt unterstützen Betriebssysteme konnte falsch interpretiert werden. Die Tabelle wurde vereinfacht und ein deutlicher Hinweis aufgenommen.
- Bugfix: Das Datenbank-Schemaupdate benötigt zur Konvertierung der Daten für DiskInventory und Bitlocker sehr lange.

4.1.2 Server (bServer)

- Der bServer löscht seine generierten Einträge unter `bMC-Konfiguration-Lock Manager` jetzt zuverlässig.
- Bei einem unerwartetem Lizenzbruch, z.B. bei erkannten Hardwareänderungen, ist der Serverbetrieb noch einige Tage ohne Einschränkung möglich, auch wenn davor eine Eval-Lizenz aktiviert worden ist.
- Bugfix: Bei der Jobausführung können zahlreiche SQL-Datenbankfehler auftreten. In diesem Fall beinhalt der Statustext der betroffenen Jobinstanzen den Text `Datenbankfehler` und in den Details ist `Deadlocksituation` im Text erkennbar. (Hierfür wurde der FixIt_Moc für die 2020 R2 bereitgestellt.)

4.1.3 Windows Agent (bMA)

- Bugfix: Beim Deploy mittels bBT erscheint sporadisch die Meldung `Dateiliste: Ungültiges XML (nicht wohlgeformt).`
- Bugfix: Die bDS-Aktion `Archiv entpacken` erstellt bei Dateien mit Umlauten teilweise Dateien mit falschem Namen.
- Bugfix: Nach dem automatischen bMA-Update bleiben die Setupdateien des Agenten im Ordner `C:\AppData\Roaming\baramundi software AG` zurück.

4.1.4 Management Center (bMC)

- Bugfix: Einige Sonderzeichen wie "&" führen im Dialog `Persönliche Einstellungen` zu einem bMC-Fehler.
- Bugfix: Der Dialog `Ordner suchen` im OS-Wizard verwendet nicht den bei `Quelle` eingegebenen Pfad, sondern beginnt im Ordner des aktuellen Benutzers.
- Bugfix: Die Tools `baretail` und `baregrep` unter `\Management Server\Shared\Tools` können nicht mehr gestartet werden.
- Bugfix: Das Tool `Double Driver` wird nicht mehr mit ausgeliefert.

4.1.5 Argus-Connect

- Bugfix: Die Umstellung des bConnect-Ports wird nicht zu den Connectoren übertragen.

4.1.6 Mobile Devices

- Bugfix: Apple Push über einen hinterlegten Proxy ist nicht möglich.
- Bugfix: Beim Versuch die App `Zebra OEMConfig powered by MX` aus dem Android Enterprise Store zu konfigurieren stürzt die bMC mit einer Null Reference Exception ab.

4.1.7 Update Management (Patch Management)

- Bugfix: Jobschritte `Microsoft Patches verteilen` mit Updatequelle WSUS oder Online laufen u.U. auf den Fehler `Die Zeichenfolge wurde nicht als gültiges DateTime erkannt.`
- Bugfix: Der Windows-Updatedienst wird nicht automatisch aktiviert und wieder deaktiviert, wenn der Schritt `Microsoft Updates inventarisieren` durchgeführt wird.

4.1.8 OT Edition

- Bugfix: Beim SNMP-Netzwerkscan werden SIMATIC Geräte nicht vollständig zu IC Devices migriert.

5 Release 2020 R2

5.1 iOS „User Enrollment“

Auf der Entwicklerkonferenz WWDC stellte Apple Ende 2019 sein erweitertes Konzept zur Datentrennung vor. Dieses erweitert den in iOS bekannten Schutz der geschäftlichen Daten um den Schutz der privaten Daten. Somit kann nun auch das Bedürfnis der Anwender am Schutz der Privatsphäre systemweit bedient und dadurch die Akzeptanz deutlich gesteigert werden.
Apple nennt diese Verwaltungsmethode – welche ab iOS 13 nutzbar ist – „User Enrollment“. Hierbei nimmt der Anwender sein mobiles Gerät selbstständig in das Management auf und kann es auch jederzeit wieder aus dem Management entfernen – selbstverständlich werden dabei auch die Firmendaten vom Gerät entfernt.

1.14.14 Eine neue Verwaltungsmethode

Die bisherigen Mechanismen zur Verwaltung von iOS-Geräten sind auf die Bedürfnisse der Administratoren ausgelegt und ermöglichen weitreichende Eingriffe in das System. So kann ein Administrator die Kamera systemweit deaktivieren und somit auch private Apps unbrauchbar machen. Im Supervised Mode kann sogar der App Store komplett gesperrt oder gezielt einzelne Apps deaktiviert werden. Ebenso ist ein Zugriff auf tiefgehende Systeminformationen möglich, welche eine Identifizierung und Rückverfolgung des Geräts möglich machen.

Abbildung 72 - Dialog beim Enrollment durch den Anwender

An dieser Stelle setzt das Konzept des „User Enrollment“ an. Statt das Gerät vollständig zu kontrollieren, findet die Verwaltung nun in einem definierten Bereich auf dem Gerät statt. Somit kommt der Anwender in den Genuss von Zugriff auf die Firmendaten ohne die sonst üblichen Einschränkungen im privaten Bereich. Ebenso bleiben seine Daten wie z.B. die selbst installierten Apps vor dem Administrator verborgen.

1.14.15 Der Unterschied

Der größte Unterschied zwischen den bisherigen Verwaltungsmethoden und dem neuen „User Enrollment“ liegt in den Berechtigungen des EMM-Systems auf dem Gerät.

Der Administrator hat nun keinen Zugriff mehr auf Daten, welche zur Identifizierung des Geräts dienen (Seriennummer, UDID, IMEI oder MAC-Adresse). Dies ist gerade im BYOD-Szenario essenziell. Stattdessen gibt es nun eine spezielle ID, welche nur diesem Verwaltungsprofil zugeordnet wird. Bei jedem neuen Enrollment wird eine neue ID erzeugt.
Noch wichtiger ist diese Trennung im Bereich der Apps. Bisher konnte der Administrator sowohl Firmen-Apps als auch vom Anwender selbst installierte private Apps sehen. Im „User Enrollment“ sind diese privaten Apps für den Administrator nicht mehr sichtbar. Das schützt effektiv die Privatsphäre der Anwender.

Auch im Bereich der Konfigurationen und direkten Aktion auf dem Gerät wird nun stärker getrennt. So ist es nun nicht mehr möglich, das Gerät aus der Ferne komplett zu löschen –

wohl aber das Firmen-Profil zusammen mit dem dafür angelegten verschlüsselten Speicherbereich und allen enthaltenen Firmendaten.

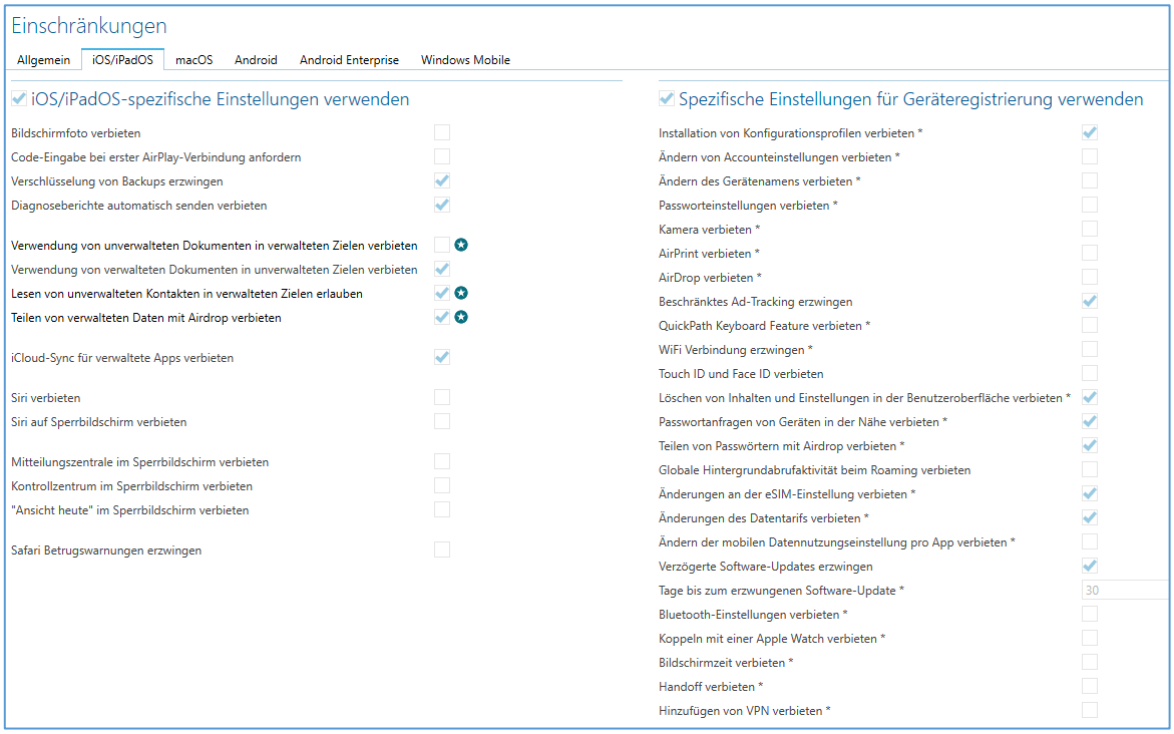


Abbildung 73 - Unterscheidung zwischen User Enrollment und Device Enrollment

Der wohl wichtigste Unterschied liegt in der Art der Datentrennung und ist transparent für Anwender und Apps. Bei der Datentrennung im „Device Enrollment“ – egal ob manuell oder per DEP – werden Firmeninhalte lediglich als geschäftlich markiert, liegen aber im selben Speicherbereich wie private Daten. Mit dem „User Enrollment“ wird auf dem Gerät ein weiterer verschlüsselter Speicherbereich angelegt, welcher ausschließlich geschäftliche Daten beinhaltet und unter der Kontrolle der EMM-Lösung steht.

1.14.16 Verwaltete Apple ID

Da im „User Enrollment“ eine strikte Trennung zwischen Privatem und Geschäftlichem vorgesehen ist, setzt es auf eine eigene ID für den Benutzer – die s.g. „verwaltete Apple ID“ oder „Managed Apple ID“. Diese ID wird zur Lizenzierung von Apps aus dem App Store verwendet.

Diese verwalteten Apple IDs können vom Administrator im Apple Business Manager[7] angelegt werden. Innerhalb der baramundi Management Suite erfolgt dann die Zuordnung von verwalteter Apple ID zu Gerät.

5.2 Automatische Aktualisierung von Apps auf mobilen Plattformen

Mit diesem Release findet nun auch der Wunsch mit den meisten Votes in der Kategorie „Mobile Devices“ im Feedback-Portal seinen Weg in die bMS:

5.2.1 Automatische Aktualisierung von VPP-Apps auf iOS

Mit dieser neuen Funktion können Administratoren sicherstellen, dass die Geräte stehts die neuste – und hoffentlich sicherste – Version einer App installiert haben. Zugleich wird das Datenkontingent geschont und der Anwender nicht unnötig gestört.
Hierfür wurde ein neuer Jobschritt eingeführt. Dieser Jobschritt kann nun per Job regelmäßig auf den verwalteten Apple-Geräten ausgeführt werden. Der Ablauf orientiert sich an unserer etablierten MSW-Logik: Zuerst wird eine Inventur der installierten Apps durchgeführt. Hierbei wird ermittelt, ob eine neuere Version der App im App Store verfügbar ist. Sofern eine neuere Version gefunden wurde, wird der Jobschritt zur Installation der neuen Version automatisch dem Job hinzugefügt. Dadurch wird erreicht, dass jedes Gerät nur die Apps herunterlädt, die bereits in einer veralteten Version installiert waren.

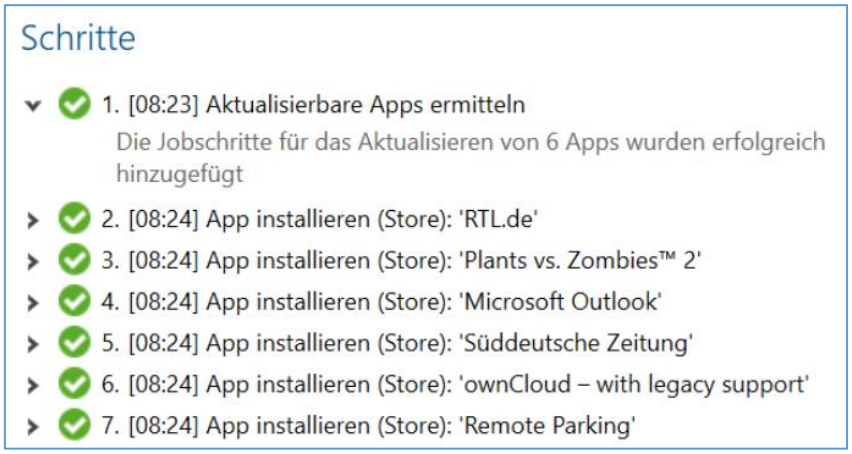
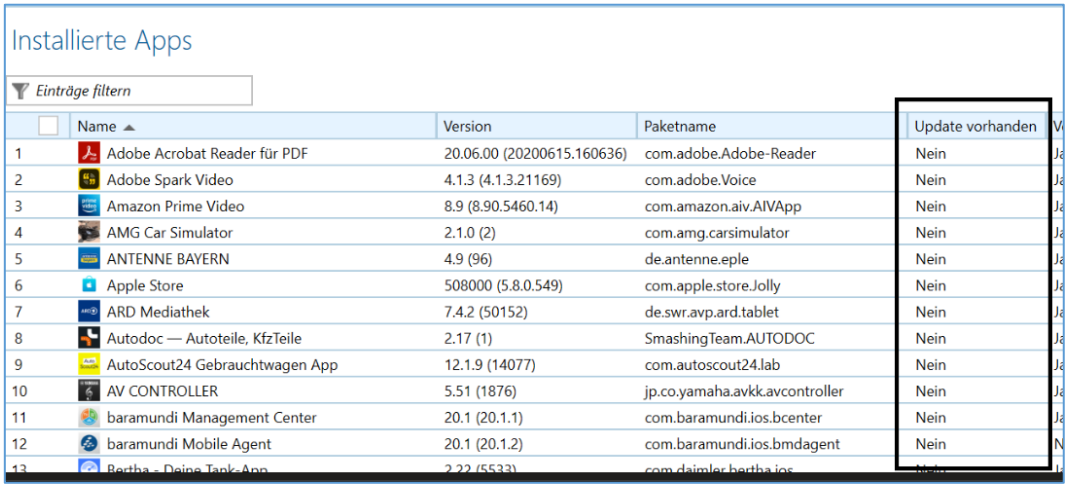


Abbildung 74 - Übersicht der Jobschritte bei einer automatischen Aktualisierung

Selbstverständlich findet die Ermittlung der Verfügbarkeit von neuen Versionen nicht nur im Rahmen des neuen Jobschritts statt. Auch die schon bestehende App-Inventur wurde um diese Funktion erweitert. So erfährt der Administrator direkt nach einer Inventur, ob eine veraltete Version einer App installiert ist bzw. ob Updates verfügbar sind.

[7] https://business.apple.com/



	Name	Version	Paketname	Update vorhanden
1	Adobe Acrobat Reader für PDF	20.06.00 (20200615.160636)	com.adobe.Adobe-Reader	Nein
2	Adobe Spark Video	4.1.3 (4.1.3.21169)	com.adobe.Voice	Nein
3	Amazon Prime Video	8.9 (8.90.5460.14)	com.amazon.aiv.AIVApp	Nein
4	AMG Car Simulator	2.1.0 (2)	com.amg.carsimulator	Nein
5	ANTENNE BAYERN	4.9 (96)	de.antenne.eple	Nein
6	Apple Store	508000 (5.8.0.549)	com.apple.store.Jolly	Nein
7	ARD Mediathek	7.4.2 (50152)	de.swr.avp.ard.tablet	Nein
8	Autodoc — Autoteile, KfzTeile	2.17 (1)	SmashingTeam.AUTODOC	Nein
9	AutoScout24 Gebrauchtwagen App	12.1.9 (14077)	com.autoscout24.lab	Nein
10	AV CONTROLLER	5.51 (1876)	jp.co.yamaha.avkk.avcontroller	Nein
11	baramundi Management Center	20.1 (20.1.1)	com.baramundi.ios.bcenter	Nein
12	baramundi Mobile Agent	20.1 (20.1.2)	com.baramundi.ios.bmdagent	Nein
13	Bertha - Deine Tank-App	2.22 (5533)	com.daimler.bertha.ios	

Abbildung 75 - Installierte Apps mit Update-Zustand

Dieser Zustand des Geräts – ob App-Updates verfügbar oder nicht – lässt sich auch per Universeller Dynamischer Gruppe (UDG) filtern.

5.2.2 Konfiguration der App Update-Policy für Android

Auch auf Android Enterprise sollten die Apps stehts auf einem aktuellen Stand gehalten werden. Leider verfügt diese Plattform über keine Funktion zur gezielten automatischen Aktualisierung. Allerdings kann das Updateverhalten konfiguriert werden.
Diese Konfiguration ist nun auch per Konfigurationsprofil über die bMS möglich.

Abbildung 76 - Einstellung des Updateverhaltens im Profil

Die Konfiguration ermöglicht die Vorgabe wie (Dem Anwender überlassen, Nur wenn mit Wifi verbunden, …) und wann (Zeitfenster) eine Aktualisierung stattfinden soll.

5.3 Inventarisierung von Microsoft Updates

Beginnend mit der bMS 2020 R2 wird das Patch Management komplett überarbeitet. Im ersten Schritt wurde hierfür eine neue Inventarisierung der fehlenden und installierten Updates bereitgestellt. Hierfür wurde ein neuer Jobschritt eingeführt. Innerhalb dieses Jobschritts werden die neuen Funktionen mit den folgenden Releases erweitert.

5.3.1 Updates erkennen

Bei Auswahl des neuen Jobschritts kann nun die Aktion „Microsoft Updates inventarisieren“ ausgewählt werden. Anschließend wird die Scan-Gegenstelle gewählt.

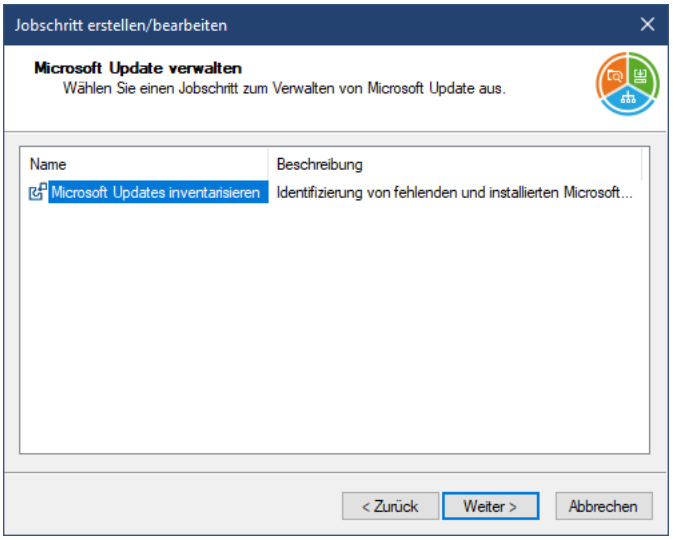


Abbildung 77 - Auswahl der Scan-Gegenstelle

In der Auswahl kann zwischen dem Microsoft-eigenen Onlinedienst „Microsoft Online“ und – sofern im eigenen Netz vorhanden und konfiguriert – einem WSUS gewählt werden.

Nach Durchführung dieses Jobs auf einem Endpoint, stehen die ermittelten Daten in zwei Ansichten zur Verfügung.

5.3.2 Endpoint Übersicht

An der Übersicht-Seite des Windows-Endpoint hält ein neues Informationsfeld Einzug. In diesem Feld finden sich alle relevanten Daten zu den Microsoft Updates des Endpoints. So wird hier neben dem Servicing Channel auch die Verzögerung der Feature-Updates angezeigt. Besonderes Highlight ist die grafische Darstellung der fehlenden Updates. In einem leicht zu interpretierenden Balken wird die Anzahl der fehlenden Updates gruppiert nach Kritikalität angezeigt.

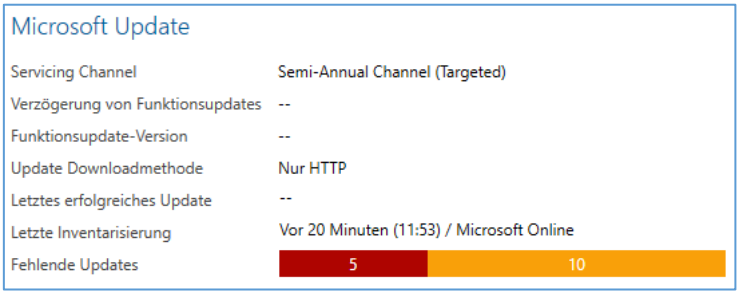


Abbildung 78 - Informationen zu Microsoft Updates in der Übersicht-Seite

Werden keine fehlenden Updates gefunden, erscheint der Balken grün. So ist auf den ersten Blick ersichtlich, ob Handlungsbedarf besteht oder nicht.

5.3.3 Auflistung der fehlenden und installierten Updates

Um einen detaillierten Überblick über die Updates eines Endpoints zu bekommen, steht dem Administrator die neue Ansicht „Microsoft Updates“ im Bereich der Inventarisierungen eines Endpoints zur Verfügung. Dort werden alle relevanten Informationen zu den fehlenden aber auch installierten Updates aufgelistet. Um auch hier sofort alle wichtigen Informationen zu bekommen, werden die Updates primär nach Zustand sortiert: Zuerst die fehlenden Updates, darunter die installierten Updates. Sekundär wird nach dem Schweregrad des Microsoft Security Response Center (MSRC) sortiert und zuletzt nach Veröffentlichungsdatum. So wird sichergestellt, dass die wichtigsten Updates auf den ersten Blick sichtbar sind. Selbstverständlich kann die Sortierung durch einen Klick auf die Spaltenköpfe geändert werden. Ebenso stehen Filter für den Zustand, die Klassifikation und auf Textbasis zur Verfügung.

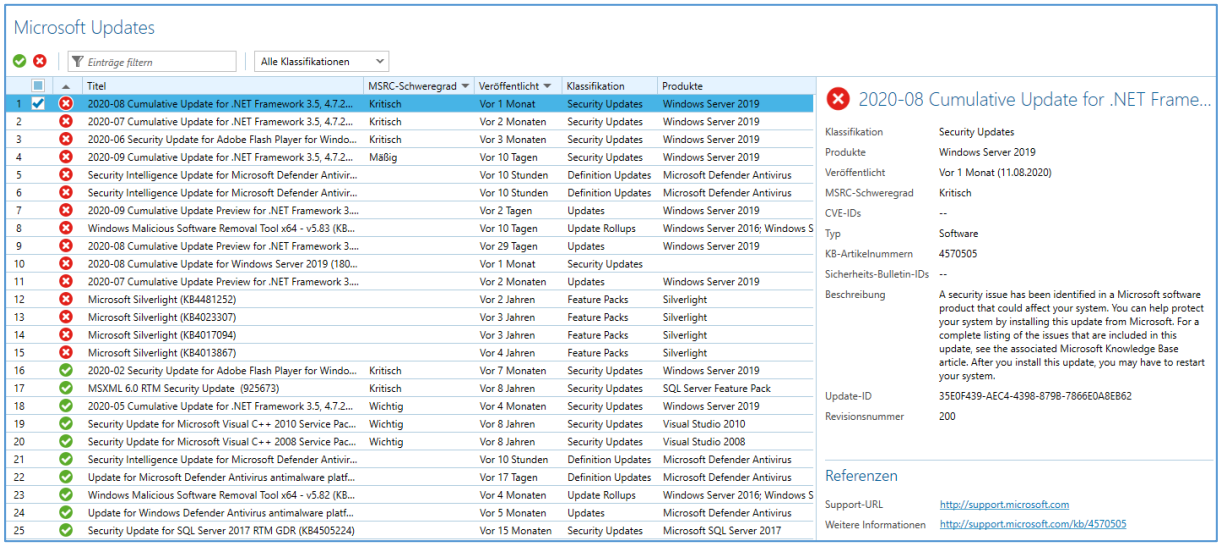


Abbildung 79 - Auflistung der fehlenden Updates

Durch einen Klick auf ein Update können weitere Informationen eingeblendet werden. Hierzu gehören unter anderem die KB-Nummer, betroffene Produkte, die Update-GUID, aber auch weitere Referenzen zu CVE-Einträgen (sofern vorhanden) und zu den Erläuterungen von Microsoft.

5.3.4 Verwendung in Universellen Dynamischen Gruppen

Die zuvor beschriebene Anzahl der fehlenden Updates an der Übersicht-Seite, ist auch als Filter bei den Universellen Dynamischen Gruppen verwendbar. Somit können nun bspw. auch Abfragen unter Berücksichtigung der Anzahl der fehlenden Sicherheitsupdates erzeugt und zum Argus Cockpit synchronisiert werden.

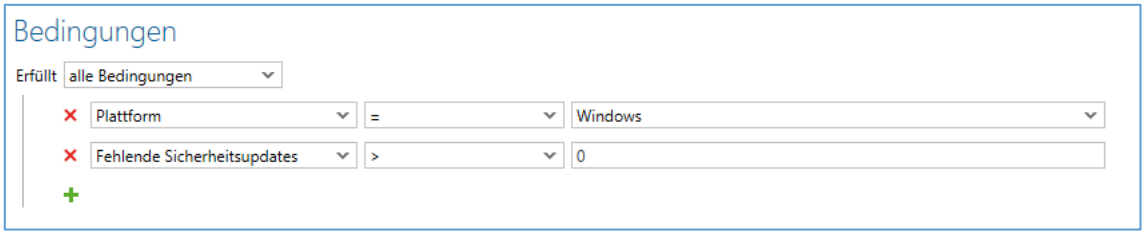


Abbildung 80 - Neue Kriterien für UDGs

5.4 Automatische BitLocker-Entsperrung in sicheren Netzwerken

Mit dem Modul „Defense Control“ ist es möglich, die Volumes eines Windows-Endpoints mit BitLocker sicher zu verschlüsseln. Für den erweiterten Schutz kann zusätzlich die Eingabe einer PIN beim Start des Rechners erzwungen werden. Durch diesen zusätzlichen Schutz wird sichergestellt, dass der Rechner nur von einer berechtigten Person hochgefahren werden kann.

5.4.1 Schutzbedürfnis vs. Komfort

Da zum Start die PIN lokal am Rechner eingegeben werden muss, kann dieser Schutzmechanismus unter Umständen die Wartung des Endpoints aus der Ferne unmöglich machen – Ist der Endpoint ausgeschaltet, kann er von der Management Lösung nicht geweckt bzw. hochgefahren werden, ohne dass eine Person die korrekte PIN vor Ort eingibt.
Da diese Diskrepanz zwischen Schutzbedürfnis und Komfort – insbesondere in verteilten Standorten – nicht praktikabel ist, wurde die bMS um die Funktion zur automatischen Entsperrung der per PIN geschützten Endpoints erweitert.

5.4.2 Funktionsweise

Für die Netzwerkentsperrung ist es nötig, dass der Endpoint feststellen kann, ob er sich in einem sicheren Netzwerk befindet. Hierfür werden beim Start einige Informationen im Netzwerk abgerufen. Diese Informationen stellen sowohl der baramundi Management Server als auch die baramundi PXE-Relays zur Verfügung. Um nun sicherzustellen, dass nicht ein beliebiger bMS einen beliebigen Endpoint entsperren kann, muss zuvor eine Vertrauensstellung hergestellt werden. Diese Vertrauensstellung basiert auf einem Zertifikat als eine Art Ausweis. Als Konsequenz entsperrt der Endpoint nur, wenn er einen Server, welcher über das vertrauenswürdige Zertifikat verfügt, erreichen kann.

5.4.3 Aktivieren der Netzwerkentsperrung

Da die automatische Entsperrung in das Sicherheitskonzept des Unternehmens eingreift, muss diese Funktion zuerst explizit durch den Administrator in der bMS grundlegend aktiviert werden. Dies geschieht in den Einstellungen des Moduls *baramundi Defense Control*.

Abbildung 81 - Konfiguration der Netzwerkentsperrung

Das Aktivieren der Funktion sorgt dafür, dass von der bMS die erforderliche Konfiguration an der bMS-Infrastruktur vorgenommen wird. Hierzu gehört die Erzeugung des benötigten Zertifikats sowie das Bereitstellen der Informationen für die verbundenen PXE-Relays – schließlich soll der Entsperrvorgang bei Bedarf auch an Außenstellen funktionieren.

5.4.4 Berechtigung der Endpoints

Es kann – je nach Sicherheitskonzept – auch Endpoints geben, welche von der automatischen Entsperrung ausgenommen sein sollen. Daher muss ein Endpoint explizit die Berech-

tigung erhalten, um sich automatisiert in einem sicheren Netzwerk zu entsperren. Dies geschieht mithilfe eines Jobschritts. Dazu wurde der bekannte Jobschritt „BitLocker verwalten“ um die Aktion „BitLocker Netzwerkentsperrung aktivieren“ erweitert.

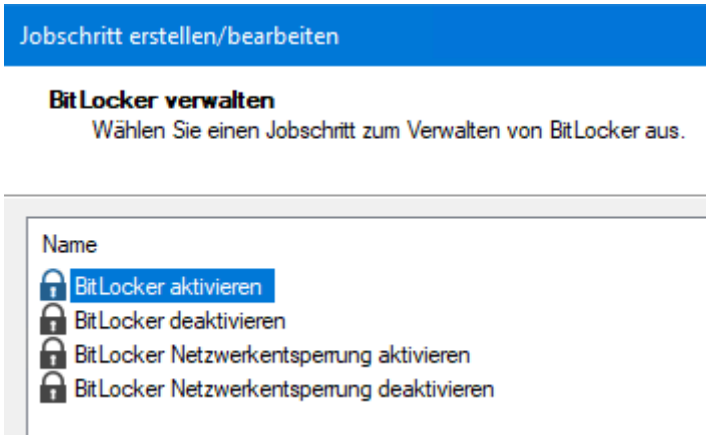


Abbildung 82 - Aktionen des Jobschritts "BitLocker verwalten"

Bei Ausführung dieses Jobschritts wird das benötigte Zertifikat installiert und der Endpoint korrekt konfiguriert. Selbstverständlich kann die Netzwerkentsperrung auch wieder durch einen Jobschritt deaktiviert werden.

5.5 baramundi Argus Cockpit

In der Version 2020 R2 wurde das in der vorhergehenden Version eingeführte baramundi Argus Cockpit (bAC) weiterentwickelt. Im Vordergrund der Verbesserungen stehen Funktionserweiterungen hinsichtlich der Synchronisation und Darstellung relevanter Daten der verbundenen IT-Umgebungen. Zudem ist auch die System-Performance – insbesondere bei Anbindung von größeren IT-Umgebungen – optimiert und die UI angepasst.

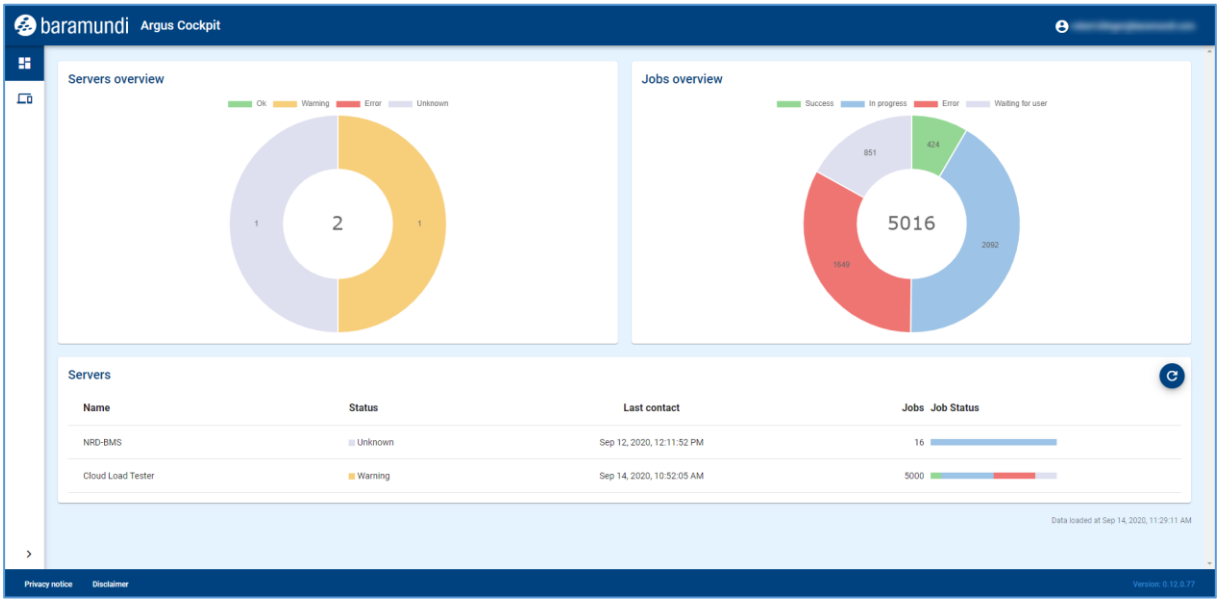


Abbildung 83 - Übersichtliche UI des bAC

5.5.1 Auswahl relevanter IT-Daten

Das baramundi Argus Cockpit hat die Aufgabe die IT-Administratoren immer und überall über den aktuellen Status der verbundenen IT-Umgebungen zu informieren. So können diese IT-Probleme rechtzeitig identifizieren und Aktionen anschließend lokal initiieren. Doch jedes Unternehmen definiert den "Gesundheitsstatus" seiner IT-Umgebung anders. Zum Beispiel ist für Unternehmen A die Umgebung gesund, wenn alle PCs gepatcht sind. Für Unternehmen B ist die Umgebung hingegen gesund, wenn alle PCs Windows 10 in der aktuellen Version installiert haben und BitLocker aktiviert ist. So unterschiedlich die Anforderungen sind, so unterschiedlich sind auch die Daten, die für die Bewertung des Gesamtstatus notwendig sind.
Daher werden ab der 2020 R2 zusätzlich zu den bMS-Diensten und Job-Informationen auch bis zu 10 universelle dynamische Gruppen mit dem Argus Cockpit synchronisiert und übersichtlich dargestellt. So kann jeder IT-Administrator auswählen, welche spezifischen relevanten Daten er benötigt und mit dem bAC synchronisieren möchte.

5.5.2 Universelle dynamische Gruppen synchronisieren

Um die universellen dynamischen Gruppen (UDG) mit dem baramundi Argus Cockpit synchronisieren zu können, wurden einige Erweiterungen in der bMC hinzugefügt. Bis zu 10 UDG können im Menü für die Synchronisation aktiviert werden.

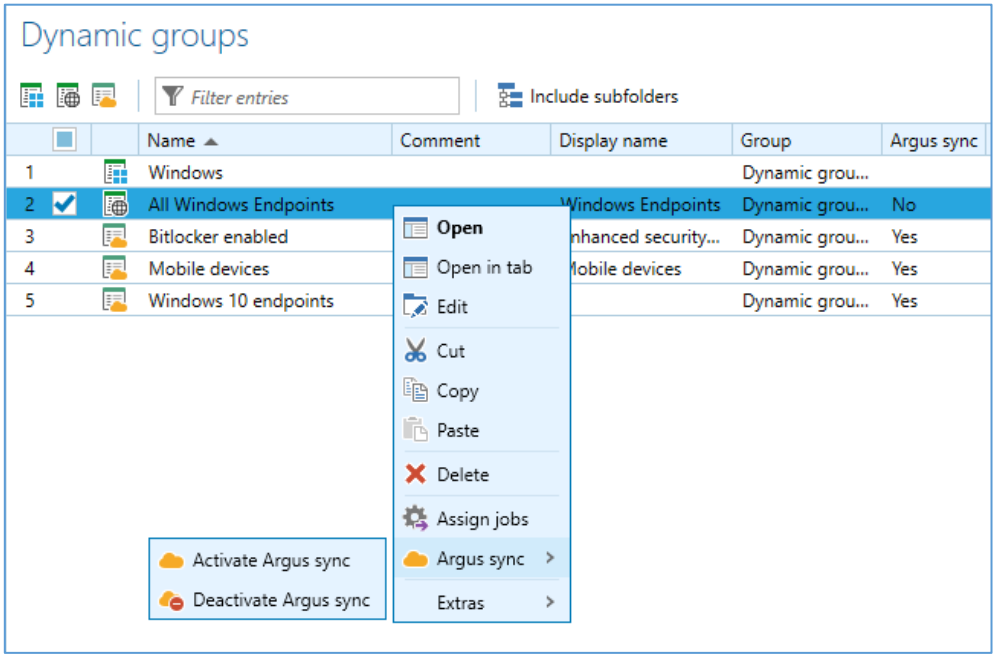


Abbildung 84 - Synchronisation für UDG aktivieren

Damit die Übersichtlichkeit steigt, werden einerseits synchronisierte UDG mit einem anderen Symbol in der bMC dargestellt und andererseits hilft die Eingabe eines UDG-Anzeigenamens die UDG im Argus Cockpit leichter identifizieren zu können.

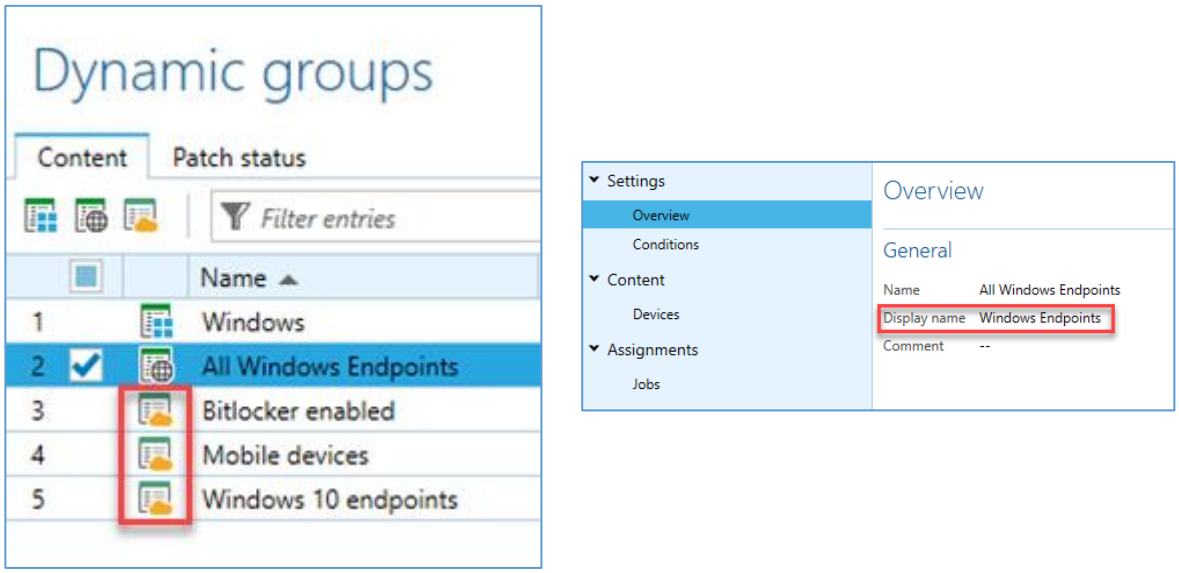


Abbildung 85 - Kennzeichnung synchronisierter UDG

Unter Umständen ist es wichtig, dass nicht jeder bMC-Nutzer diese Synchronisation aktivieren darf. Um den Bestimmungen des Datenschutzes gerecht zu werden, wurde ein neues Spezialrecht hinzugefügt.

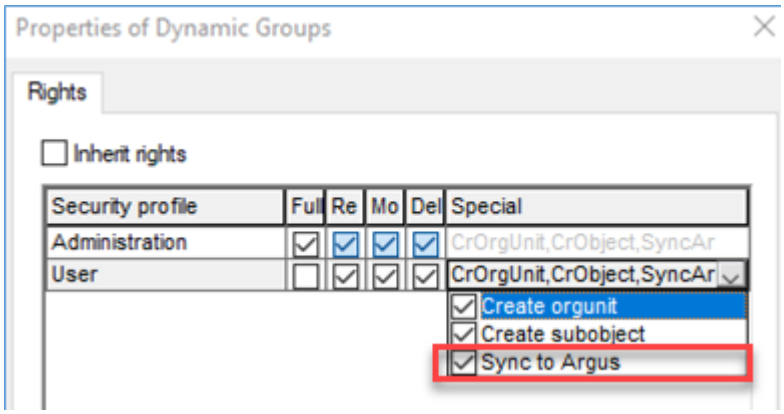


Abbildung 86 - Neues Spezialrecht für Synchronisation zum Argus Cockpit

5.5.3 Anzeige der UDG im Argus Cockpit

Mit der Definition und Synchronisation der UDG ist eine wichtige Grundlage für die Anzeige relevanter IT-Daten im Argus Cockpit geschaffen worden. Im baramundi Argus Cockpit werden nun die Ergebnismengen dieser UDG übersichtlich dargestellt. Dabei kann jeder Argus-Benutzer der Zugriff auf den entsprechenden baramundi Management Server im Argus Cockpit hat, die zugehörigen synchronisierten UDG sehen.
So kann der IT-Administrator z.B. auch das Beobachten und Kontrollieren dieser Daten delegieren und ein anderer Mitarbeiter des Unternehmens wertet die Daten im Argus Cockpit aus, während sich der IT-Administrator um andere wichtige operative Aufgaben kümmern kann.

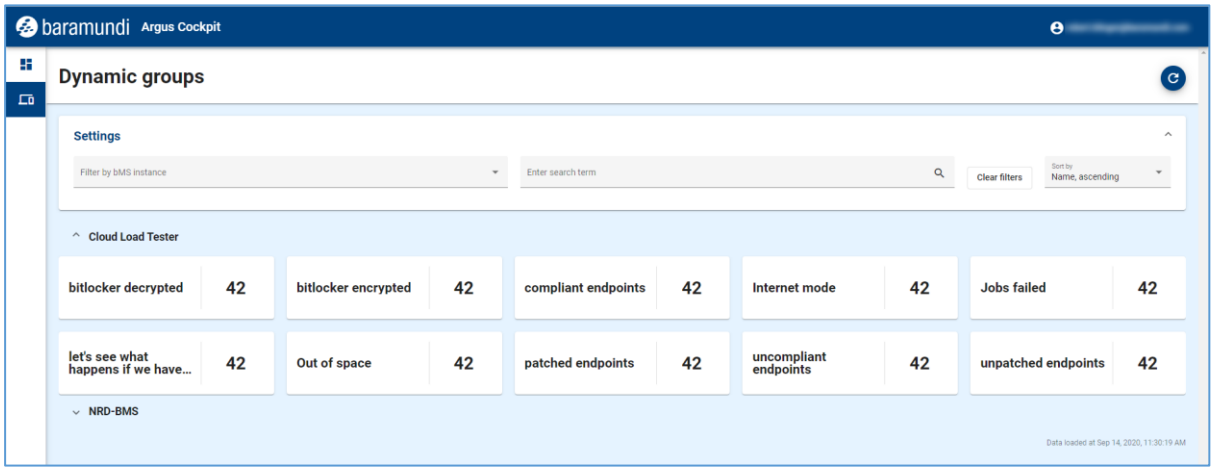


Abbildung 87 - Übersichtliche Darstellung der UDG pro baramundi Management Server

Das Dashboard der „Dynamic groups“ hilft dem IT-Admin, alle synchronisierten UDG pro baramundi Management Server einzusehen und deren Ergebnismengen auf einem Blick zu erkennen. Filter und Sortierungs-Optionen garantieren dabei die Übersichtlichkeit.

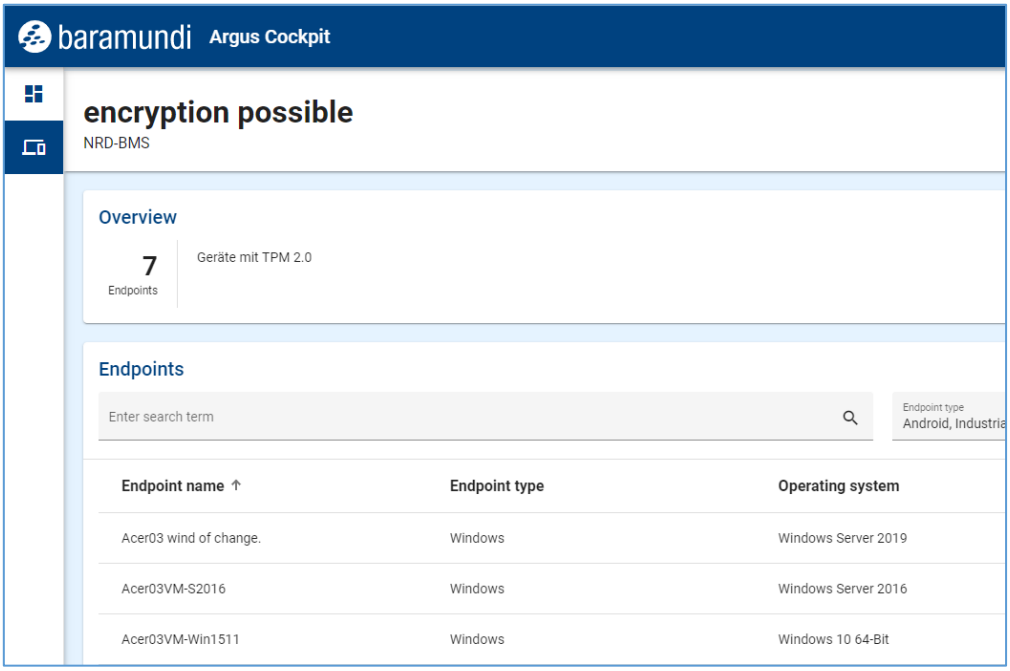


Abbildung 88 - Detailansicht einer UDG

Möchte der Argus-Benutzer mehr Informationen zu einer bestimmten universellen dynamischen Gruppe erhalten, kann er diese in einer Detailansicht einsehen. Alle Endgeräte, die den definierten Kriterien der UDG entsprechen, werden angezeigt und wiederum helfen hier Filter- und Sortierungsoptionen den Fokus auf die Darstellung wichtiger und relevanter Daten zu lenken.

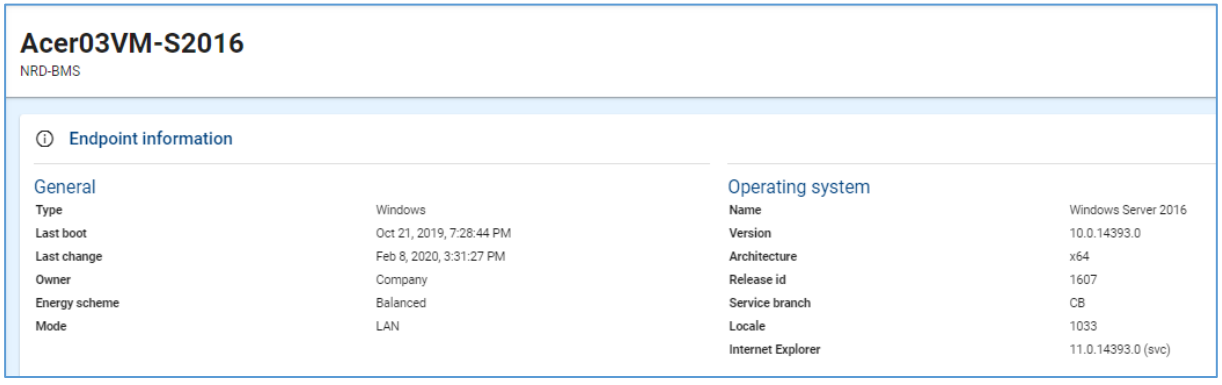


Abbildung 89 - Detailansicht eines Endgerätes

Noch mehr Informationen zu einem spezifischen Endgerät sind nur einen weiteren Klick entfernt. In der Detailansicht eines Endpoints werden zahlreiche Daten (abhängig vom entsprechenden Endpoint-Typ) angezeigt. Unter anderem kann der IT-Administrator sehen:

- ✓ Ist die BitLocker Verschlüsselung auf dem Endgerät aktiviert?

- ✓ Gibt es fehlende kritische Patch-Updates[8] für dieses Endgerät?
- ✓ Welches Betriebssystem ist installiert?
- ✓ In welchen anderen UDG ist dieses Endgerät erfasst?
- ✓ Wann war der letzte erfolgreiche Kontakt vom Management-Server zum Endgerät?

5.6 Allgemeine Weiterentwicklung

5.6.1 License Management

Das *baramundi License Management* bietet eine kompakte und einfache Möglichkeit, um kaufmännische Informationen aus dem Lizenzmanagement zu berücksichtigen und damit eine bessere Transparenz der im Unternehmen vorhandenen Lizenzen zu erreichen.

Für die neue Version wurde eine optimierte, durch das System unterstütze Zuordnung von Installationen implementiert.

5.6.1.1 Konzept

Der Stand der Installationen (Software-Erkennungsregeln) ändert sich häufig. Neue Software wird auf die Rechner der Mitarbeiter gespielt oder neue Versionen einer bereits vorhandenen Software werden installiert.

Noch nicht zugeordneten Installationen, können jetzt über unterschiedliche Optionen vereinfacht zugeordnet werden.

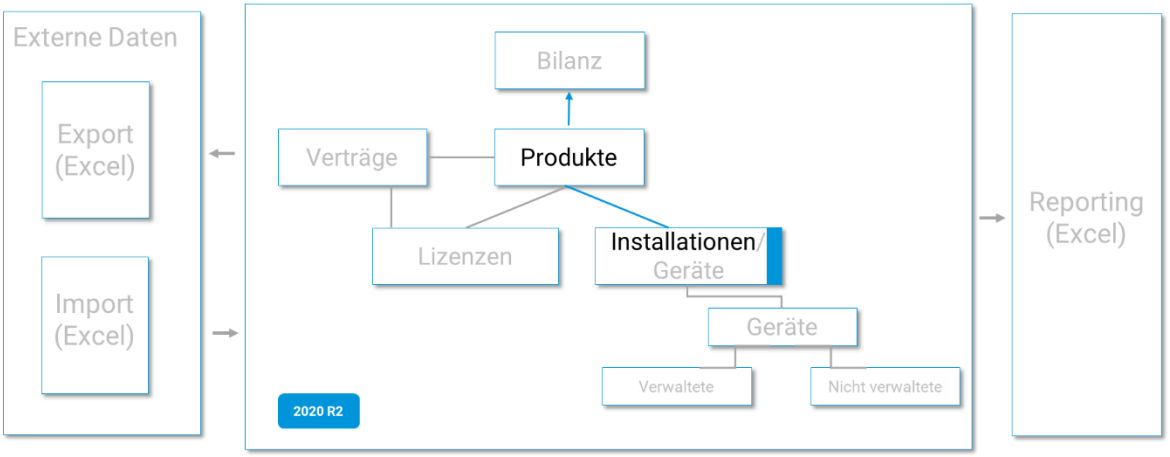


Abbildung 90 – Lizenz Management Gesamtkonzept 2020 R2

[8] Siehe dazu auch Kapitel: Inventarisierung von Microsoft Updates

5.6.1.2 Anzeige von noch nicht zugeordneten Installationen

Damit die Bilanz auf einem aktuellen Stand gehalten werden kann, ist es wichtig alle relevanten Installationen (Software Erkennungsregeln) den jeweiligen Produkten zuzuordnen.

Ein aktueller Hinweis über der Anzahl der noch nicht zugeordneten Installationen ist in der verbesserten Version von *baramundi License Management* in der Menüleiste abgebildet und dadurch immer transparent.

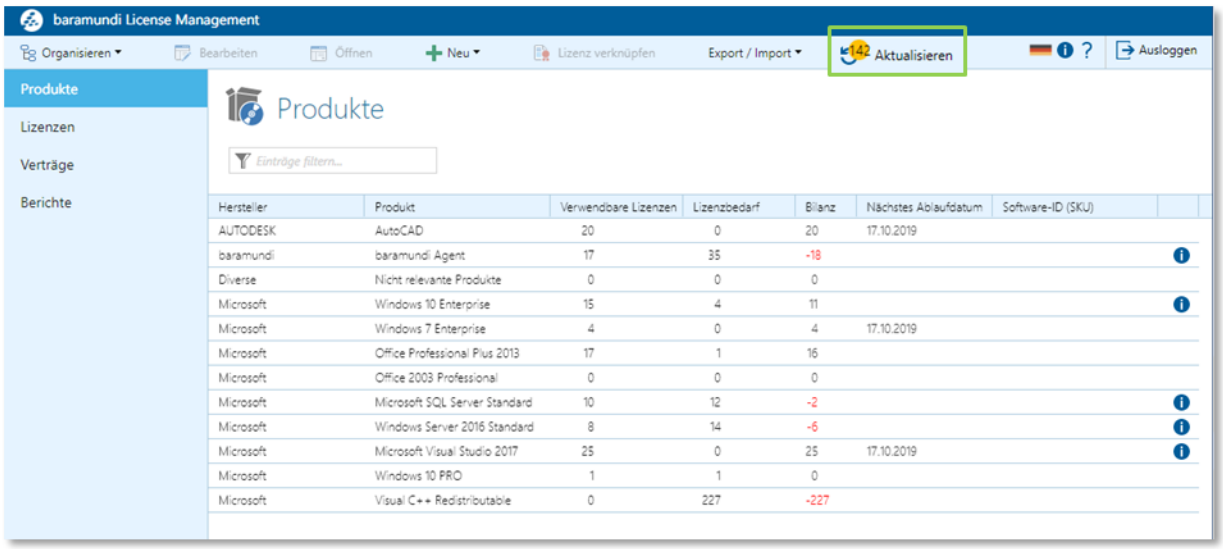


Abbildung 91 - Bilanz mit Anzahl noch nicht zugeordneter Installationen

5.6.1.3 Optimierte Zuordnung von Installationen

Wenn Name und Hersteller einer bereits vorhandenen Installation, welche einem Produkt zugeordnet ist, entsprechen, bietet das System automatisch einen Produktvorschlag an, dem diese weitere Installation zugeordnet werden kann.

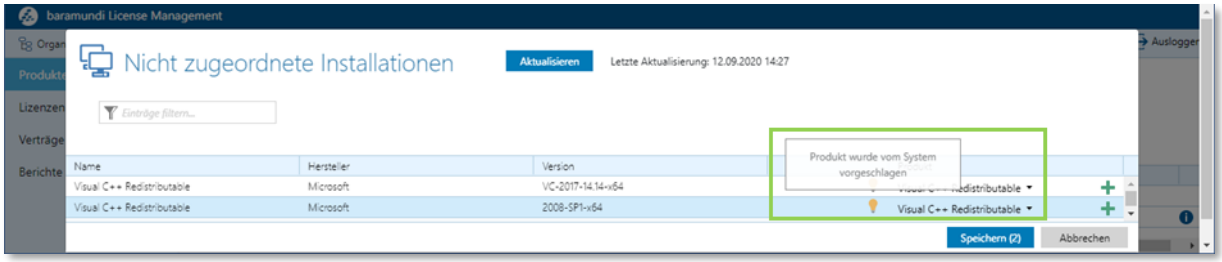


Abbildung 92 –Automatischer Vorschlag für Zuordnung neuer Installationen

Alternativ hat der Lizenzverantwortliche die Möglichkeit über eine Auswahl von bereits angelegten Produkten eine zügige Zuordnung der Installation vorzunehmen.

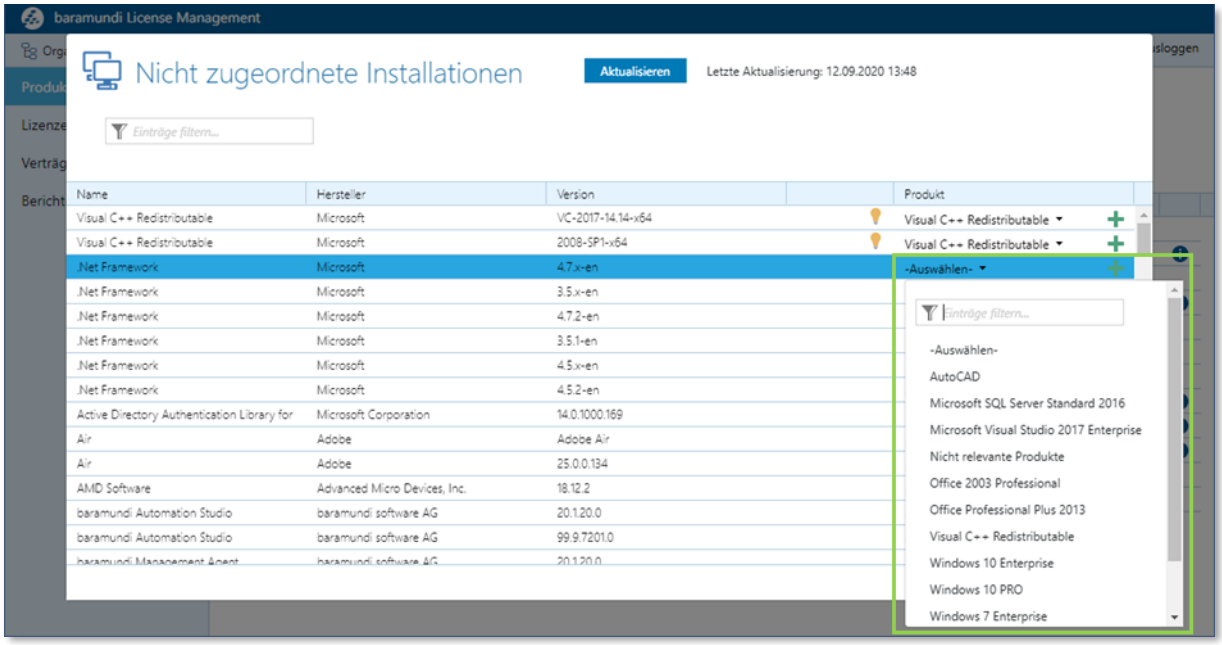


Abbildung 93 - Nicht zugeordnete Installationen - Auswählen vorhandener Produkte

Sollte kein passendes Produkt vorhanden sein, ermöglicht die Anwahl des + Symbol eine direkte Neuanlage eines Produktes. Name und Hersteller werden hierbei automatisch als Vorschlag in die entsprechende Ansicht übernommen und die Erstellung dadurch vereinfacht.

Abbildung 94 – Nicht zugeordnete Installationen – direkte Neuanlage von Produkten

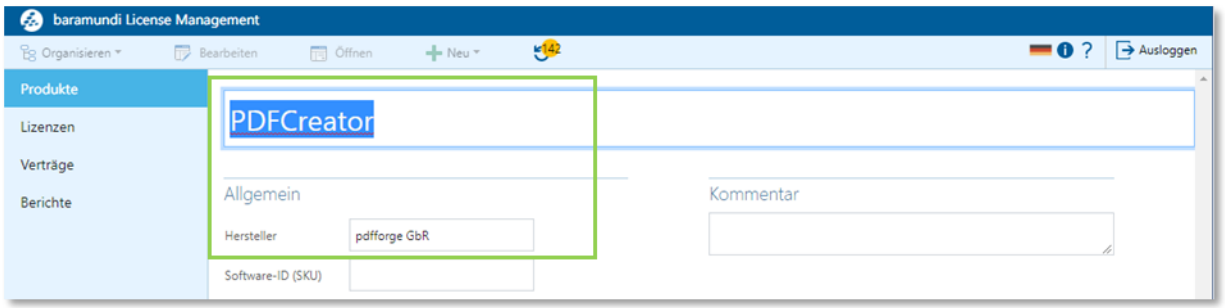


Abbildung 95 - Lizenz Management - vereinfachte Neuanlage von Produkten

Alle vom System vorgeschlagenen oder vom Anwender vorgesehenen Zuordnungen werden vor dem Speichern entsprechend angezeigt.

bLM bietet so mit der 2020 R2 unterschiedliche Möglichkeiten zügig und übersichtlich neue Installationen zuzuordnen und erleichtert dem Lizenzmanager dadurch die Arbeit erheblich – sowohl bei häufig aufkommenden Änderungen durch neue Versionen , als auch bei der Erfassung neuer Software.

5.6.2 Optimierung der bBT-Downloads für IEM-Clients

Durch Optimierungen an der Übertragungslogik konnte die Geschwindigkeit der bBT-Downloads über das Gateway deutlich gesteigert werden. Die Downloads sind nun bis zu 25 mal schneller also zuvor.

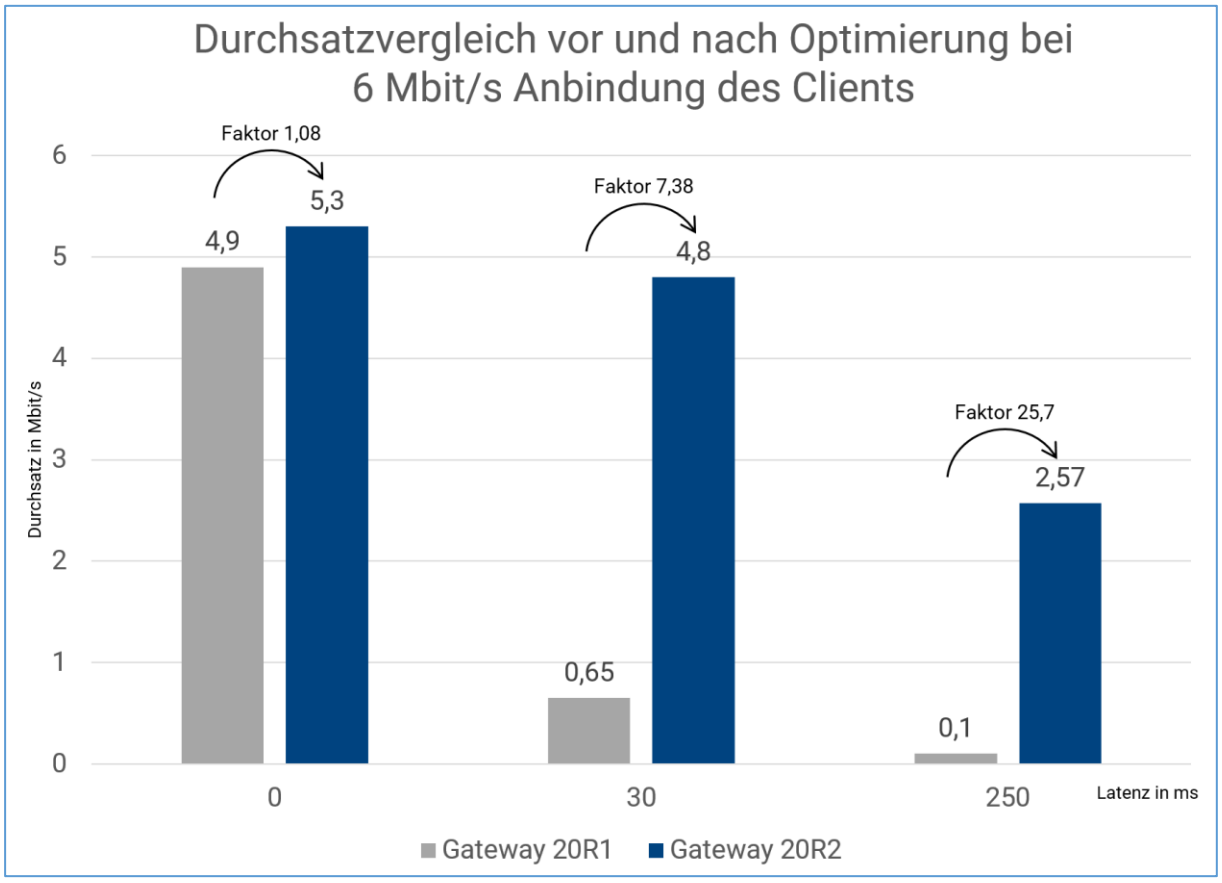


Abbildung 96 - Gemessener Geschwindigkeitszuwachs durch Optimierungen

Von diesen Optimierungen profitieren vor allem Endpoints mit eher schlechter Anbindung bzw. hohen Latenzen.

5.6.3 Zweckbestimmter Modus für iOS

Der von Android Enterprise bekannte Modus für zweckbestimmte Geräte hält nun auch bei iOS Einzug. Durch den mit der bMS 2020 R1 für Android eingeführten Jobschritt, um ein Gerät in den zweckbestimmten Modus zu bekommen, können nun auch iOS-Geräte abgeriegelt werden.

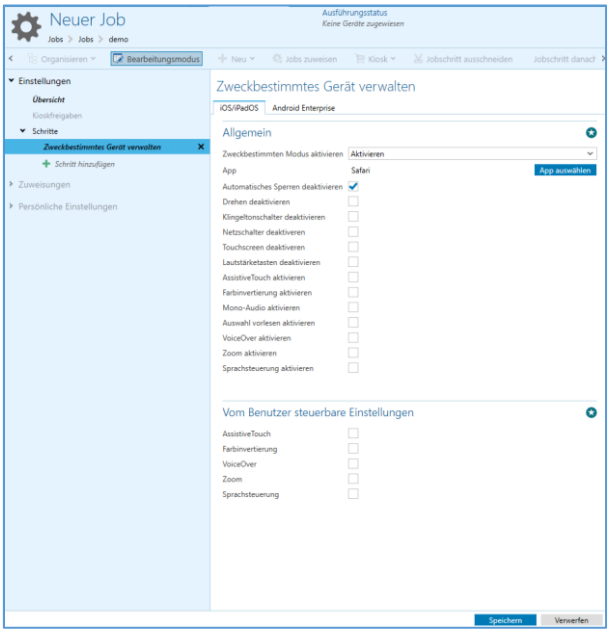


Abbildung 97 - Konfiguration des zweckbestimmten Modus für iOS

Hierfür muss der Jobschritt nur entsprechend konfiguriert werden. Dazu wird neben der zu startenden App auch vorgegeben, in welchem Rahmen der Anwender die Darstellung auf dem Gerät verändern kann.
Solange sich das Gerät im zweckbestimmten Modus befindet, wird nach dem Einschalten direkt die ausgewählte App gestartet. Ein Umschalten zu anderen Apps ist nicht möglich.

5.6.4 Filter für Jobschritte bei mobile/macOS-Jobs

Die Auswahl der Jobschritte für mobile Geräte und macOS wurde mit verschiedenen Filtern vereinfacht. So kann die Auswahl nun auf Basis von Plattformen und Verwaltungsprofilen gefiltert werden. Dadurch ist bereits bei der Erstellung des Jobs ersichtlich, ob die gewählten Jobschritte von der gewünschten Plattform unterstützt werden.

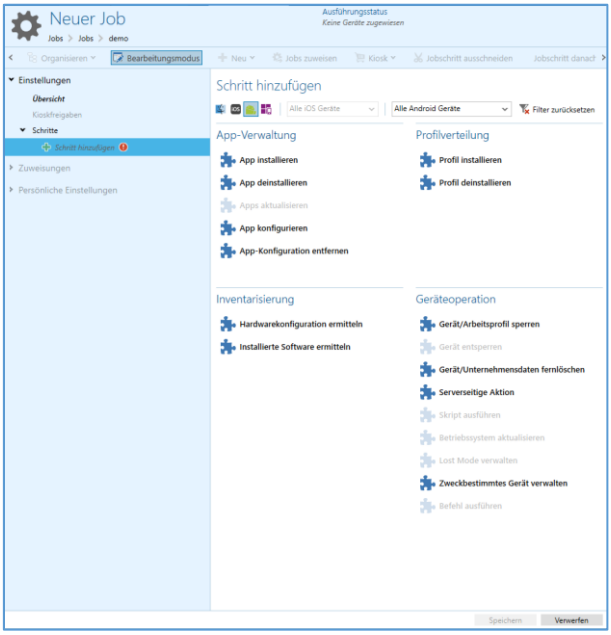


Abbildung 98 - Gefilterte Jobschritte, welche auf Android ausführbar sind.

5.6.5 Filter für Bausteine in Konfigurationsprofilen für mobile Geräte

Auch die Auswahl der Profilbausteine für mobile Geräte wurde um einen Filter ergänzt. So ist bereits beim Erstellen des Profils ersichtlich, ob das Profil auf der gewünschten Plattform anwendbar ist.

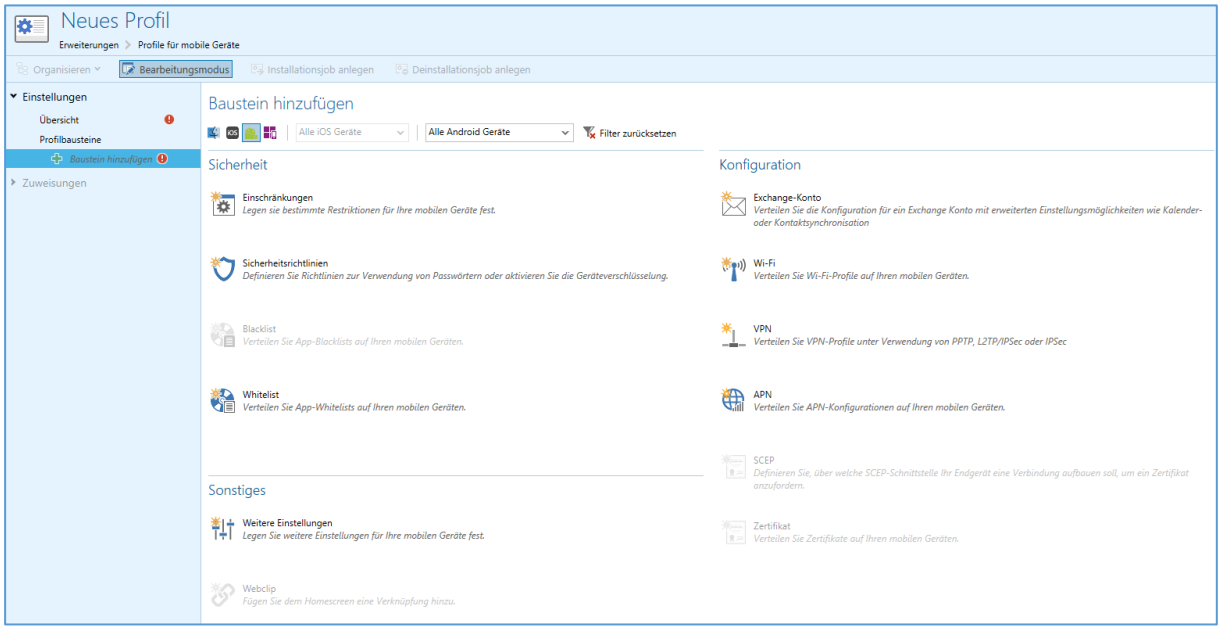


Abbildung 99 - Gefilterte Profilbausteine für Android

5.6.6 Übertragung von Konfigurationsdateien für Android

Bereits mit Einführung der Android Enterprise-Unterstützung in der bMS haben wir Wert auf die Unterstützung der sogenannten Managed Configuration – der Konfiguration von Play Store-Apps durch das EMM – gelegt. Doch nicht alle der dort verfügbaren Apps sind durch diese Managed Configuration konfigurierbar. Einige Hersteller von Apps setzen noch immer auf die Konfiguration per Datei auf dem Endgerät.
Um auch diese Apps sinnvoll ausbringen zu können, unterstützt die bMS nun auch den Transfer von textuellen Informationen zur Konfiguration von Apps.

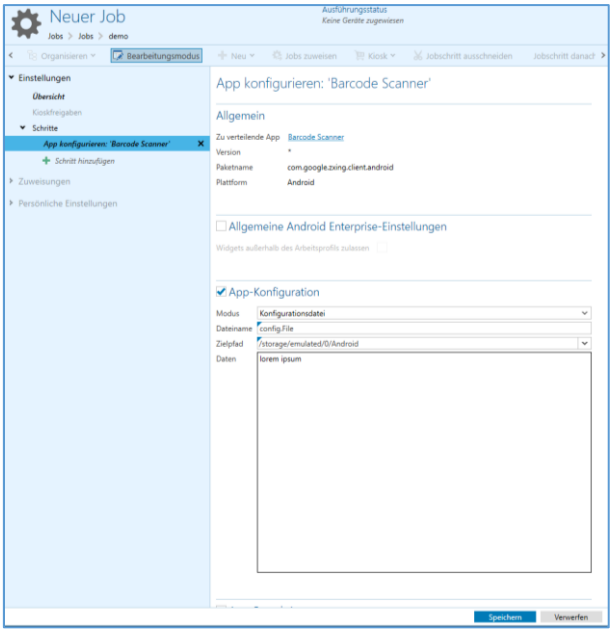


Abbildung 100 - App-Konfiguration per Datei

Um auf dem Android-Gerät eine Konfigurationsdatei für eine spezifische App anzulegen, kann nun im Bereich „App-Konfiguration“ zwischen Managed Configuration und Konfigurationsdatei ausgewählt werden. Wird Konfigurationsdatei gewählt, muss noch der Dateiname, der Speicherort und der Inhalt vorgegeben werden.
Wird nun der Jobschritt ausgeführt, legt der baramundi Agent die Datei mit den vorgegebenen Parametern auf dem Gerät an.

5.6.7 Sprachauswahl für Enrollment-Mails

Mit der bMS 2020 R2 kann der Administrator nun auch eigene, sprachspezifische Vorlagen für das Enrollment von mobilen Geräten, macOS und Windows im IEM-Modus anlegen. Diese Vorlagen stehen anschließend im Enrollment-Dialog zur Verfügung und werden auch bei der Anlage eines Endpoints per bConnect verwendet.

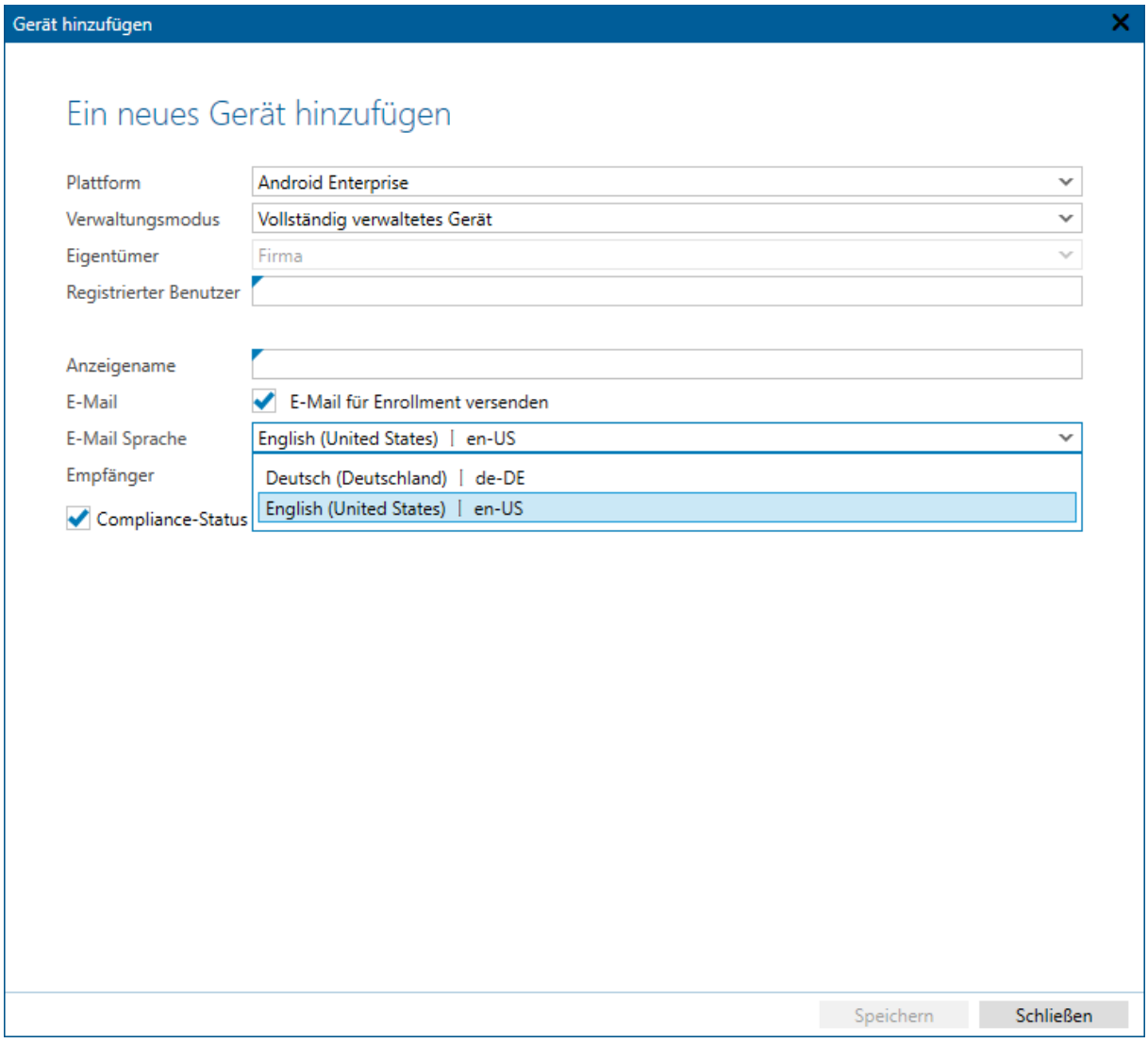


Abbildung 101 - Sprachauswahl für Enrollment-Mail

5.7 Produktverbesserungen im Detail

5.7.1 Allgemein

- Alle Setups wurden von MSI auf .EXE umgestellt.
- Die bMS eigene Lizenzierung wurde verbessert. So werden beim Fehlercode 233 mögliche Ursachen mit ausgegeben. Weiterhin ist bei einem unerwartetem Lizenzbruch, z.B. bei erkannten Hardwareänderungen, der Serverbetrieb noch einige Tage ohne Einschränkung möglich, dazu darf keine Eval-Lizenz aktiviert worden sein.
- Verbesserung der Logmeldung `External component has thrown an exception` im bServer.log bei Datenbankproblemen .
- Bugfix: Jobs mit `Benutzer muss Ausführung bestätigen`, welche per Jobintervall neu geplant werden, fragen den Benutzer nur einmalig nach dessen Zustimmung.
- Bugfix: Die unter `Server-Einstellungen-Downloader` hinterlegte Proxyeinstellung wird bei Apple-VPP und Apple-Push nicht berücksichtigt.

5.7.2 Windows Agent (bMA)

- Zum Enrollment eines Windows-Clients (IEM) sind keine Administrator-Rechte mehr notwendig. Dazu muss der bMA vorab ohne Enrollment installiert worden sein.
- Wipe-Disk ist jetzt auch unter Windows-PE x64 und UEFI möglich.

5.7.3 Management Center (bMC)

- Das neue Windows 10 Namensschema (20H2) wird unter `Client-Einstellungen-Übersicht` als `Angezeigte Version` dargestellt. Eine Abfrage über Universelle Dynamische Gruppen ist möglich.
- Der Kompatibilitätsmodus zur Kommunikation mit veralteten bMAs (kleiner Version 2019 R2) wurde entfernt.
- Unter `Windows-Client-Übersicht` wird das zugeordnete IP-Netzwerk des Clients angezeigt.
- Die Seite `Lizenzkonfiguration` wurde verbessert und bildet dadurch den Workflow besser ab.

- Die Offline-Hilfe inklusive Cobrili ist jetzt ein eigenständiges Setup. Es ist im Rahmen-Setup als optional gelistet. Die Verwendung der Online-Hilfe wird wegen besserer Aktualität ausdrücklich empfohlen.
- BitLocker Schlüssel können auch bei einem deaktivierten Gerät eingesehen werden.
- Eine Logmeldung `Failed login attempt for user name` wird bei fehlgeschlagenen Anmeldeversuchen ins bServer.log geschrieben.
- Neuer Jobschritt `Microsoft Update verwalten`, um fehlende und installierte Microsoft Updates zu inventarisieren.
- In einer `Dynamische Gruppe (Universell)` gibt es neue Bedingungen für Industrielle Steuergeräte, für Microsoft Updates und für MDM-Geräte.
- Neue Kommandozeilenparameter für die bMC
  `/bServer=bmsname` setzt den bMS Servernamen auf `bmsname;`
  `/useLoggedOnUser` setzt den Haken zum Single-Sign-On;
  `/autoConnect` löst eine automatische Anmeldung beim bMC Start aus.
- Die `Persönlichen Einstellungen` und `Benachrichtigungen` sind auf das moderne GUI Format umgestellt worden.
- Bugfix: Unter `Konfiguration` fehlen teilweise Überschriften.
- Bugfix: Beim Ändern des Names eines IP-Netzwerkes erscheint eine SQL-Fehlermeldung.
- Bugfix: In seltenen Fällen konnte nach Ablauf der Eval-Lizenz keine Produktivlizenz eingespielt werden.
- Bugfix: Wird beim Editieren von Jobs schnell der Editmodus ein und ausgeschalten, so wird sporadisch die Job-Kategorie zurückgesetzt.
- Bugfix: Bei automatisch wiederholter Jobausführung wird der Jobschrittzähler (z.B. 5/5) nicht zurückgesetzt und zeigt bis zum Ende des ersten Schritts einen falschen Wert an.

5.7.4 Argus-Connect

- Mit einem neuen Recht `Zu Argus Synchronisieren` kann unter `Dynamische Gruppe (Universell)` konfiguriert werden, welche bMC Benutzer Universelle Gruppen zum Argus Cockpit synchronisieren können.
- Bis zu 10 Universelle Gruppen können zum Argus Cockpit synchronisiert werden.
- Die Connectoren beenden sich automatisch, wenn die bMS Version zu gering ist.

5.7.5 Mobile Devices

- Es ist möglich, eigene E-Mail Templates zu hinterlegen, ohne diese beim Versionswechseln neu importieren zu müssen. (Dateinamen z.B. MailTemplate.VPPUser.Custom.html).
- In der bMC wurden am Jobschritt `iOS Befehl ausführen` Beispiele hinterlegt.
- iOS Geräte ab iOS 13.1 können als benutzerregistrierte (BYOD) Geräte verwaltet werden.
- Beim Erstellen von SSA-Jobschritten wird nun auch im Bearbeitungsmodus der Name des ausgewählten Skripts am Jobschritt angezeigt.
- Die `Installiert auf` -Ansicht bei MDM-Apps enthält nun auch eine Spalte für die installierte Version der App.
- Verbesserungen bei Android Enterprise:
    - Steuerung der `Auto-App-Update-Policy` inklusive Wartungsfenster.
    - Neue Restriktion: `Apps aus unbekannten Quellen erlauben`.
    - Konfigurationsdateien können über einen neuen Schritt auf das Gerät übertragen werden.
    - Die Android Enterprise Einschränkung `Backup auf Google Drive verbieten` ist nun auch für Arbeitsprofile verfügbar.
    - Für Android Enterprise Dedicated Device Mode kann jetzt zusätzlich ein Template ausgewählt werden, wodurch es möglich wird, das Layout auf dem

Gerät flexibel anzupassen. Zudem gibt es die Möglichkeit, den Benutzer Optionen wie die Bildschirmhelligkeit selbst steuern zu lassen.

- Der iOS Dedicated Device Mode (COSU) kann via Jobschritt aktiviert/deaktiviert und konfiguriert werden.
- Beim Versand von Enrollment Emails kann die Sprache der Email ausgewählt werden.
- Bei der Auswahl eines Profilbausteins und bei der Auswahl eines Jobschritts kann gefiltert werden, für welche Plattform und welche Verwaltungsmethode diese jeweils geeignet sind.
- Unter `Profilbausteine-Einschränkungen-iOS/iPadOS` ist die Textangabe `Lesen von unverwalteten Kontakten in verwalteten Zielen erlauben` nicht eindeutig formuliert. (Neu: `Lesen von verwalteten Kontakten in unverwalteten Zielen erlauben`).
- Bugfix: Werden Variablen bei einer Gruppe und an einem Endpoint mit gleichem Scope und gleichem Namen angelegt, so werden die Variablen am Client bei der Jobausführung teilweise mit den Werten der Variable an der Gruppe überschrieben.
- Bugfix: Wird versucht die Compliance Prüfung für ein MDM Gerät mittels „Prüfung aussetzen“ zu beenden, erscheint eine Exception-Meldung.
- Bugfix: In der bMC erscheint beim Löschen einer Black/Whiteliste für MDM eine Fehlermeldung mit geringer Aussagekraft, wenn verknüpfte Elemente vorhanden sind welche das Löschen verhindern. (Hier werden jetzt die verknüpften Elemente angezeigt).
- Bugfix: Ein Compliance-Verstoß wird bei Android Enterprise Geräten nur einmalig ausgelöst und nicht aktualisiert.
- Bugfix: Der Apple-Push Service kann in seltenen Fällen beim Neuenrollment eines Gerätes abstürzen.
- Bugfix: Die bMC-Spalte `BMA-Version` zeigt bei iOS-Geräten eine falsche Version an.
- Bugfix: iOS Geräte lassen sich nicht löschen, wenn VPP-Lizenzen mit dem Gerät verknüpft sind und das VPP-Token ungültig ist.

- Bugfix: In seltenen Fällen kann über `Konfiguration-Mobile Devices-Allgmein` kein `APN-CSR` erstellt werden, es erscheint eine Exceptionmeldung.

5.7.6 OS-Install

- Bugfix: Ein Inplace-Upgrade Job schlägt fehl, wenn in der bMC für diesen Client kein HW-Profil eingestellt ist.

5.7.7 bConnect

- Neuer Controller: UniversalDynamicGroups.
- Der Endpoint Controller wurde um Parameter erweitert, damit die Endpoints einer Universellen Gruppe gelesen werden können.
- Das Aufnehmen von IEM Clients kann über den EndpointEnrollment Controller gesteuert werden.
- Für MDM und mac OS-Geräte kann angegeben werden, ob und in welcher Sprache eine Enrollment-Email versendet werden soll.
- Neuer Controller: Dynamic Groups Cloud Connector, um bis zu 10 universelle dynamische Gruppen inkl. Endpoint-Ergebnisse mit dem Argus Cockpit zu synchronisieren.
- Für Windows-Clients kann die Liste der installierten und fehlenden Updates, inklusiver Update-Metadaten abgefragt werden.

5.7.8 bMOL

- Hinweis: Wir raten generell dazu, von bMOL zu bConnect zu wechseln.
- Bugfix: Auslesen von Applikationen und Bundles liefert keine Daten.

5.7.9 baraDIP

- Der bBT-Durchsatz wurde, insbesondere bei Internetverbindungen mit großer Latenz, deutlich verbessert.
- Bugfix: Die Logdatei wird stetig größer. Dadurch kann in großen Umgebungen die Performance des baraDIP eigeschränkt sein.

5.7.10 Defense Control

- Unter `Defense Control-Einstellungen` kann der Bitlocker Network Unlock ein/ausgeschalten werden.
- Zwei neue Jobschritte unter `Bitlocker verwalten` um die BitLocker Netzwerk-entsperrung zu aktivieren bzw. deaktivieren.

5.7.11 License Management

- Eine Infoseite zeigt nützliche Informationen wie Versionsnummer, Datenbank und Benutzerdaten.
- Das Anmeldetoken hat eine längere Laufzeit.
- Ein manueller Logout ist möglich.
- Bugfix: Wird der Name eines Produktes geändert, kann das zu Datenverlust führen.
- Bugfix: **Nach** dem Update erscheint in einigen Fällen die Meldung `Can't parse cpus as licenseType.`
- Bugfix: Die F1-Hilfe öffnet sich per default immer auf Deutsch.

5.7.12 Mac OS

- Bugfix: Beim Enrollment eines Mac Gerätes wird der Servernamen, welcher bei der Installation des bma.pkg angegeben werden muss, nicht angezeigt.
- Bugfix: Durch ein mac OS-Update wurde unter Umständen die `sudoers`-Datei zurückgesetzt und im Anschluss konnten keine Jobs mehr ausgeführt werden.

6 Release 2020

6.1 Android Enterprise: Dedicated Devices

6.1.1 Übersicht: Android Enterprise Profile

Android bietet für geschäftlich genutzte Geräte drei Verwaltungsoptionen[9] in Form von Android Enterprise Profilen an:

- nur geschäftlich
- mit privater Nutzung
- zweckbestimmtes Gerät

Damit gelingt es Unternehmen, die Vielfalt der Android-Geräte jeweils in Anbetracht des konkreten Einsatzszenarios optimal zu managen.

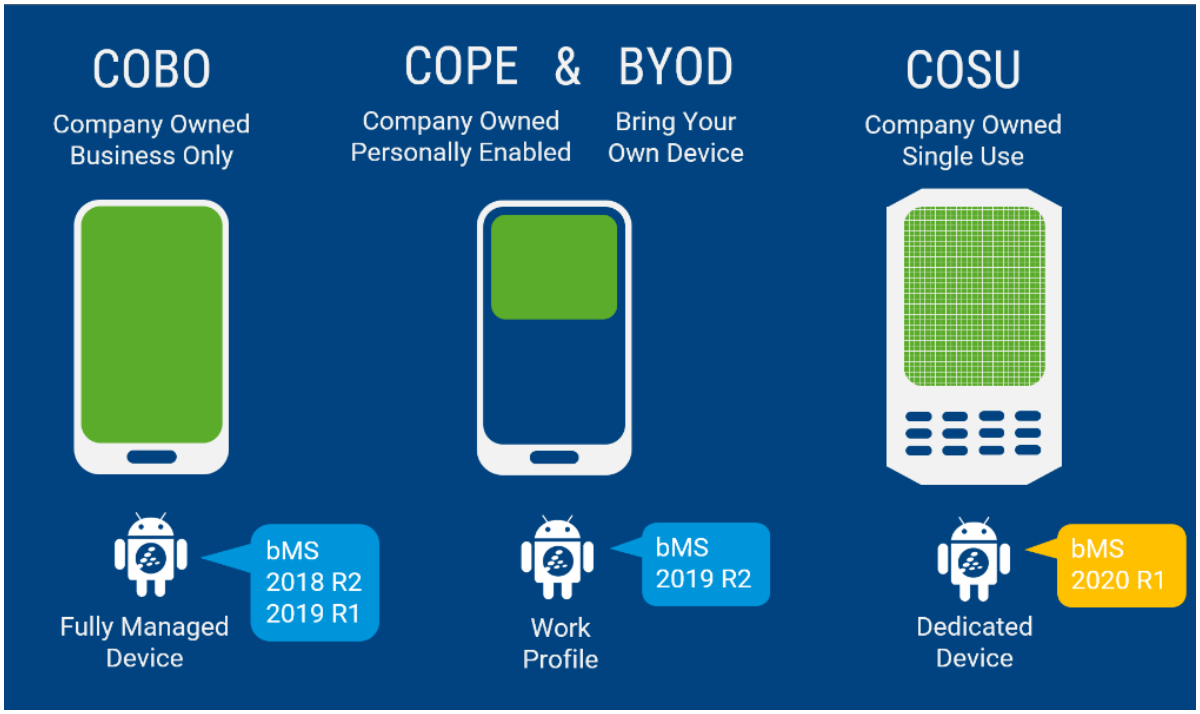


Abbildung 102 – Android Enterprise Profile und Einsatzszenarien

Bislang unterstützt die baramundi Management Suite die beiden Profile *Fully Managed Device* und *Work Profile*. Ab Release 2020 werden auch zweckbestimmte Geräte mit dem Profil *Dedicated Device* unterstützt. Der Administrator kann dabei für jedes verwaltete Gerät individuell bestimmen, welcher Verwaltungsmodus am besten für den Anwendungsfall passt.

[9] Android Enterprise Verwaltungsoptionen: https://www.android.com/intl/de_de/enterprise/management/

6.1.2 Anwendungsszenarien für zweckbestimmte Geräte

Im Gegensatz zu klassischen Mobilgeräten, die typischerweise einem Mitarbeiter fest zugeordnet werden und ausschließlich von dieser einen Person genutzt werden, dienen zweckbestimmte Geräte (engl. dedicated devices) einem gewissen Geschäftszweck und sind meist nicht einem konkreten Mitarbeiter zugeordnet, sondern werden von verschiedenen Personen abwechselnd genutzt.

Zum Beispiel gibt es im Logistikbereich Barcodescanner mit Android Betriebssystemen, die dann im Schichtbetrieb von Mitarbeitern im Lager abwechselnd genutzt werden. Auf einem derartigen Gerät soll nur noch die App zum Scannen der Codes genutzt werden. Alle anderen Apps werden daher ausgeblendet und somit der Bedienkomfort erhöht und Fehlbedienungen vermieden.

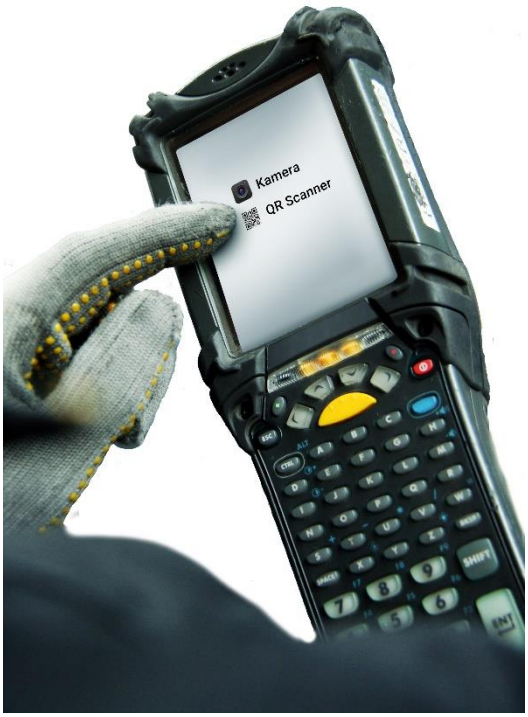


Abbildung 103 – Barcode Scanner im zweckbestimmten Modus für ausgewählte Apps

Auch im Retail-Bereich ist der Einsatz von Android-Tablets möglich: So könnte ein Kunde zusammen mit dem Verkäufer sich Produktdemos zeigen lassen und eine Produktkonfiguration durchführen. Dabei ist sichergestellt, dass der Kunde nicht versehentlich andere Apps aufruft.

6.1.3 Konfiguration mit baramundi Mobile Devices Premium

Die Verwaltung des Profils „Zweckbestimmtes Gerät“ ist Teil von baramundi Mobile Devices Premium.
Nach dem Enrollment werden die Geräte in der bMC als „Zweckbestimmtes Gerät“ gekennzeichnet. Diese Kennzeichnung ist als Spalte in der Listenansicht der Gruppen, der universellen dynamischen Gruppen und auch an der Übersichtsseite des Geräts zu finden.

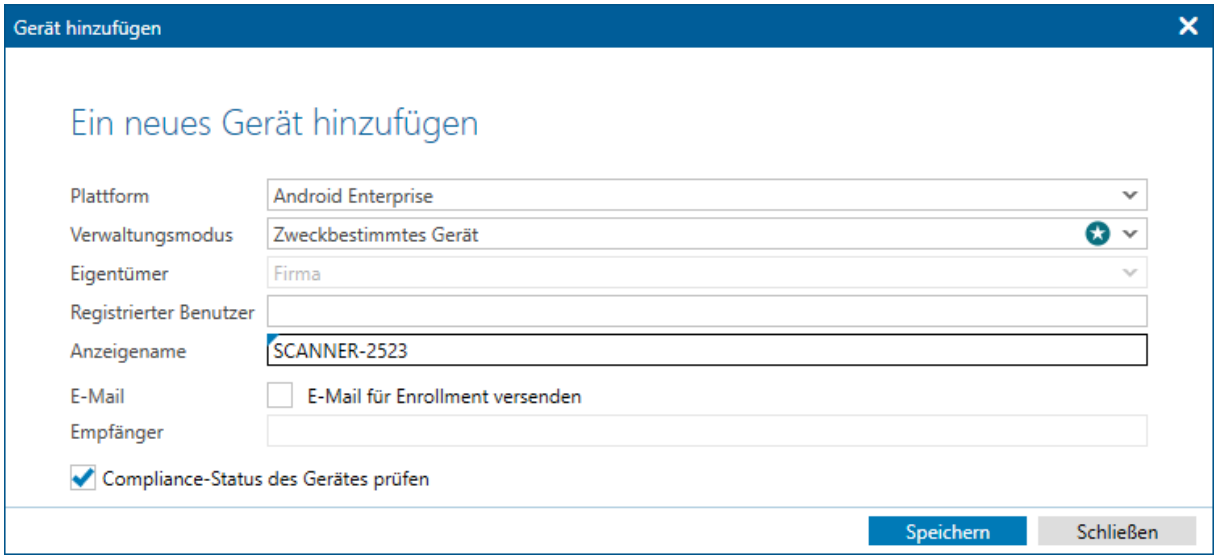


Abbildung 104 – Hinzufügen eines zweckbestimmten Geräts

Zweckbestimmte Geräte können auf eine oder mehrere Apps eingeschränkt werden. Diese Einschränkung basiert auf den bereits bekannten Whitelists. Zusätzlich können weitere Einstellungen vorgenommen werden, wie beispielsweise die Verfügbarkeit von Systemfunktionen (Home-Taste, Benachrichtigungen, etc.).

Zur Einrichtung der Geräte wurde ein neuer Jobschritt, “Zweckbestimmtes Gerät verwalten”, hinzugefügt. Mit Hilfe dieses Jobschritts kann das Gerät – sofern keine Whitelist verteilt wird – auch in einen Wartungsmodus versetzt werden. Das Gerät kann somit erst einmal keine Apps starten.

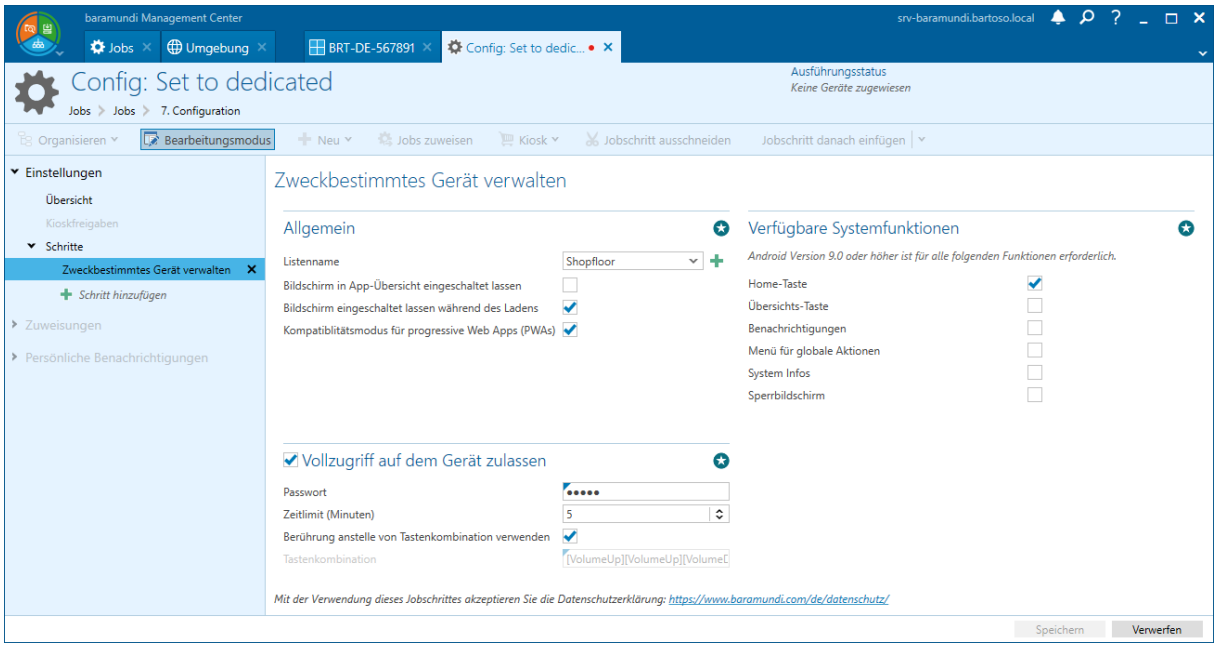


Abbildung 105 – Einstellungen am Jobschritt "Zweckbestimmtes Gerät verwalten"

Nach Ausführung des Jobs auf den Geräten, sind diese entsprechend „verriegelt“. Der Anwender kann nun nur noch die vom Administrator freigegebenen Apps starten. Sofern nur eine App freigegeben wurde, startet diese nach dem Startvorgang des Geräts automatisch.

Über eine spezielle Tastenkombination und ein Passwort ist es für den Administrator möglich, lokal am Gerät in einen administrativen Modus zu wechseln um ggf. Einstellungen vorzunehmen.

6.2 baramundi Argus Cockpit

Administratoren, die rund um die Uhr die „Gesundheit“ einer oder gleichzeitig mehrerer, unterschiedlicher IT-Umgebungen im Blick behalten müssen, stehen vor einer titanischen Aufgabe. Da hilft es sehr, auf die Fähigkeiten des Titanen Argus zurückgreifen zu können: Dieser mit hunderten Augen ausgestattete, unermüdliche Wächter aus der griechischen Mythologie ist die Inspiration für das baramundi Argus Cockpit.
Das Argus Cockpit erlaubt es IT-Administratoren von jedem internetfähigen Gerät aus mit einer übersichtlichen Oberfläche die „Gesundheit“ ihrer bMS-Umgebung(en) zu kontrollieren.
Mit dem baramundi Argus Cockpit wird die baramundi Management Suite um ein auf Cloud-Technologie basierendes Dashboard erweitert. Somit verschmelzen die Welten der „On-Prem“ Architektur der baramundi Management Suite mit der Cloud-Architektur des Dashboards und es entsteht eine neue hybride Lösung.

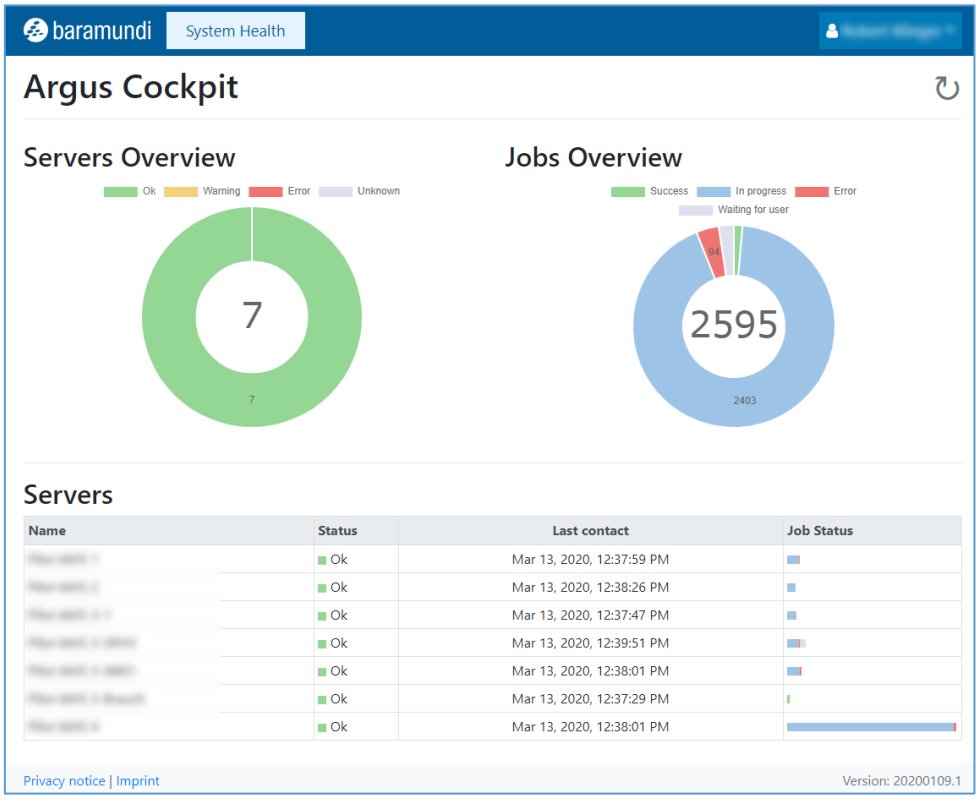


Abbildung 106 – Startseite des baramundi Argus Cockpit

Ein großer Vorteil des hybriden Ansatzes des Argus Cockpits ist zudem, dass die notwendige Infrastruktur von baramundi in der Cloud bereitgestellt wird und damit nicht von jedem einzelnen Unternehmen realisiert werden muss. In dieser Cloud-Umgebung können funktionale Updates fortwährend von baramundi eingespielt werden. Somit wird das Cockpit (in weiten Teilen) unabhängig von bMS-Release-Zyklen weiterentwickelt.

6.2.1 Zeit- und ortsunabhängiger Abruf der Daten

Ein wichtiges Kriterium für die Konzeption und Umsetzung des Argus Cockpit ist es, dass relevanten IT-Daten von den Administratoren möglichst ohne Infrastrukturhürden abrufbar sind. Im Release 2020 wird der Status der bServer-Dienste und Informationen zu Jobausführungen dargestellt. Damit entfällt die Notwendigkeit, eine direkte VPN-Verbindung zu den gemanagten Netzwerken aufzubauen. Die notwendigen Daten können direkt in einer Dashboard-Ansicht über den Browser jedes aktuellen, internetfähigen Endgeräts abgerufen werden. In einer responsiven Ansicht haben IT-Administratoren jederzeit und überall – unterwegs oder im Homeoffice - Zugriff auf relevante IT-Umgebungsdaten und deren Kennzahlen.

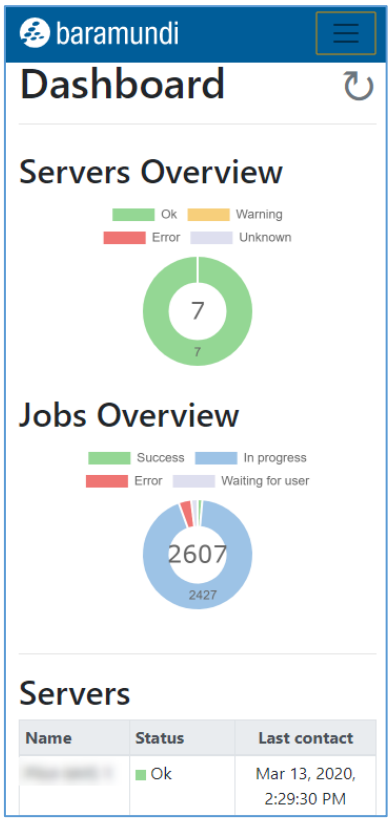


Abbildung 107 – Responsive Darstellung auf einem mobilen Endgerät

6.2.2 Sicherer Zugriff auf die Daten im Argus Cockpit

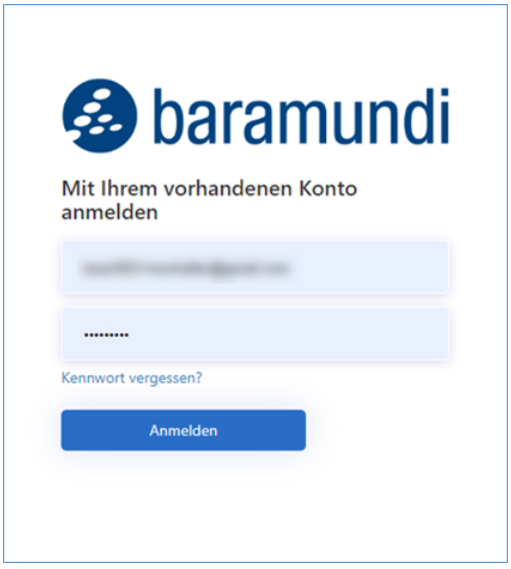


Abbildung 108 – Sichere Anmeldung im Argus Cockpit

Die Auskunft über die „Gesundheit“ der verbundenen Systeme erfolgt über die Cloud. Damit jeder IT-Admin im Argus Cockpit auch nur die Daten einsehen kann, für die er berechtigt ist, startet das Argus Cockpit mit einer einfachen, aber sehr sicheren Benutzerverwaltung. baramundi kann damit den Zugang für die interessierten Kunden ermöglichen und deren IT-Admins können sich mit E-Mail-Adresse und selbstgewählten Passwort einloggen.

6.2.3 Sichere Verbindung der bMS mit der Cloud

So sicher wie sich der Cockpit-User in der Cloud anmelden und das Dashboard nutzen kann, genauso sicher müssen auch die Daten vom jeweiligen baramundi Management Server in die Cloud übertragen werden. Denn dann „verlassen“ die IT-Daten die Netzwerkgrenzen des jeweiligen Unternehmens und müssen besonders geschützt werden. Auch hier hat baramundi besonderen Wert auf eine sichere Implementierung gelegt und verwendet z.B. mit Microsoft Azure AD, Identity Server, baramundi Connect und HTTPS modernste Komponenten und Schnittstellen und Hosting der Cloud-Komponenten in der EU. Zusätzlich wird mit einer datenschutzkonformen Verarbeitung und Übertragung der Daten, sowie dem Schutz vor unberechtigten Zugriff dank bewährter Sicherheitsstandards, eine sichere Datenverarbeitung mit dem baramundi Argus Cockpit gewährleistet.
In der bMC können IT-Administratoren ab der 2020 R1 auswählen, ob relevante Daten mit dem baramundi Argus Cockpit synchronisiert werden. Die Entscheidung, ob die Daten in die Cloud gesendet werden oder nicht, kann der IT-Admin jederzeit in der bMC konfigurieren.

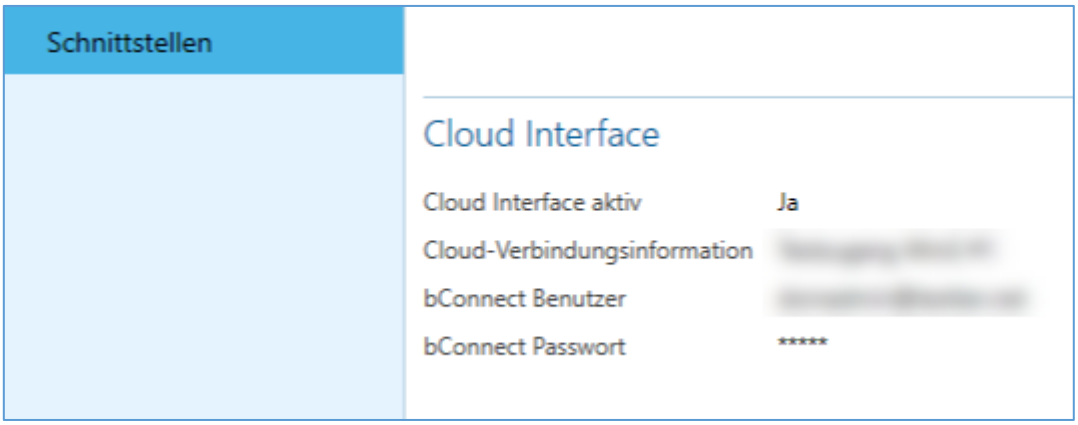


Abbildung 109 – Verbindung zum Argus Cockpit konfigurieren

6.2.4 Überblick über ein oder mehrere Systeme

Das baramundi Argus Cockpit ist mandantenfähig und ermöglicht so das gleichzeitige Monitoring mehrerer, mit der baramundi Management Suite verwalteten IT-Umgebungen. Administratoren die für mehrere Standorte ihres Unternehmens, oder Managed Service Provider (MSP), die für mehrere Kundenumgebungen verantwortlich sind, können so in einer einzigen Benutzeroberfläche den Status all ihrer Systeme unmittelbar überwachen. Das Argus Cockpit gibt Auskunft darüber, ob auf einem der verbundenen Systeme Handlungsbedarf besteht und ermöglicht eine schnelle Erkennung, wie die Unterbrechung des regulären Ablaufs zustande gekommen ist.

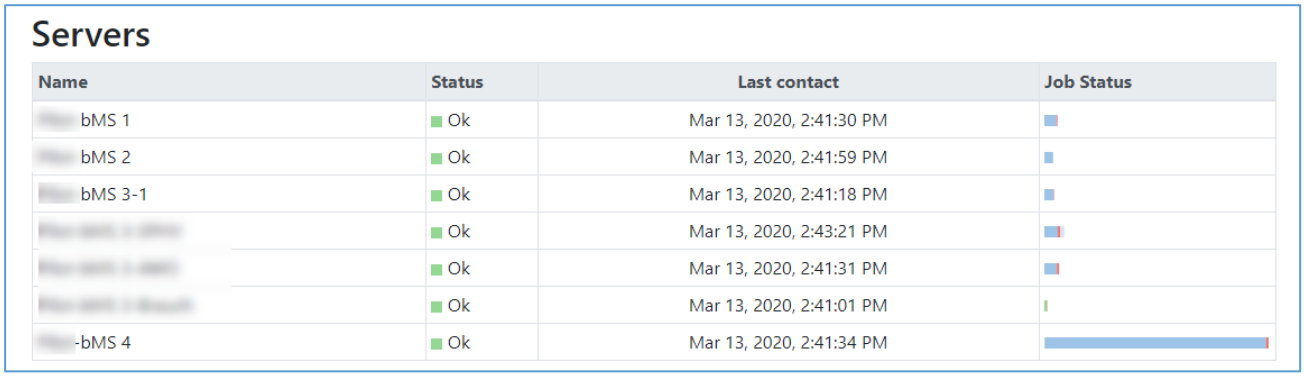


Abbildung 110 – Status-Überblick über mehrere bMS-Instanzen

6.2.4.1 Probleme bei bServer-Diensten oder Jobausführungen erkennen

Administratoren, die für mehr als nur einen baramundi Management Server in ihrer IT-Infrastruktur verantwortlich sind, stehen häufig vor einem Dilemma: Wie soll man bei einem Arbeitsplatz außerhalb des Unternehmensnetzwerks, den Überblick über baramundi Jobs und bServer-Dienste behalten, die sich auf voneinander unabhängigen Systemen abspielen? Mehrere VPN-Verbindungen zu den jeweiligen Servern gleichzeitig zu unterhalten ist unübersichtlich und in der Umsetzung anspruchsvoll. Ganz davon zu schweigen, dass in diesem Fall der Zugriff nur von dafür eingerichteten Arbeitsplätzen erfolgen kann. Für einen kurzen „Gesundheits-Check“ ist das in der Regel unverhältnismäßig.

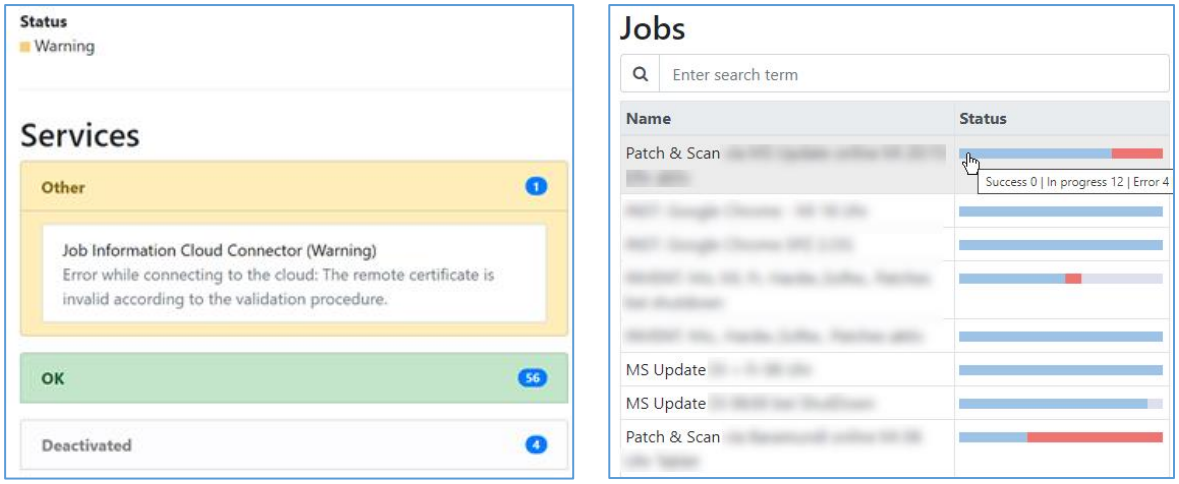


Abbildung 111 – Status über bServer-Dienste und baramundi Jobs

Mit dem baramundi Argus Cockpit ist es möglich, Probleme oder Warnungen einzelner bServer-Dienste schnell zu identifizieren und fehlgeschlagene Jobinstanzen zu erkennen. Mit Hilfe von Suchen und Filtern der Ergebnislisten, können Fehlermeldungen oder andere Statusinformationen pro Jobinstanz selektiert werden und damit gezielt auf der jeweiligen bMS-Instanz lokal adressiert werden.

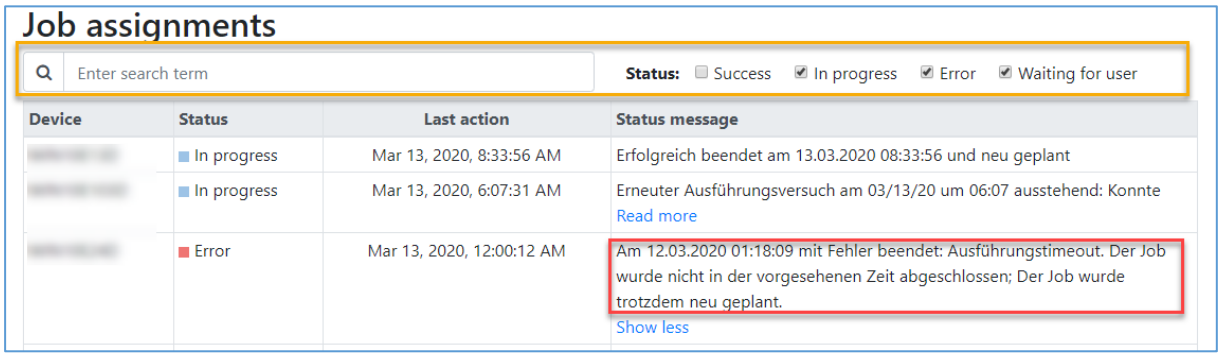


Abbildung 112 – Ansicht von Detailinformationen pro Jobinstanz

6.3 Allgemeine Weiterentwicklung

6.3.1 License Management

Das *baramundi License Management* bietet eine kompakte und einfache Möglichkeit, um kaufmännische Informationen aus dem Lizenzmanagement zu berücksichtigen und damit eine bessere Transparenz der im Unternehmen vorhandenen Lizenzen zu erreichen.

Die neue Version wurde um die Funktionalität Import von externen Daten für z.B. Produkte, Lizenzen und Verträge erweitert.

6.3.1.1 Konzept

Auf Basis der in bLM vorhanden Daten wird eine Vorlage für Produkte, Lizenzen und Verträge generiert ① und nach Excel exportiert.

Nach Ergänzung von beispielsweise einer Übersicht von Produkten in der XLS-Vorlage können diese Informationen über einen Import ② in bLM integriert werden.

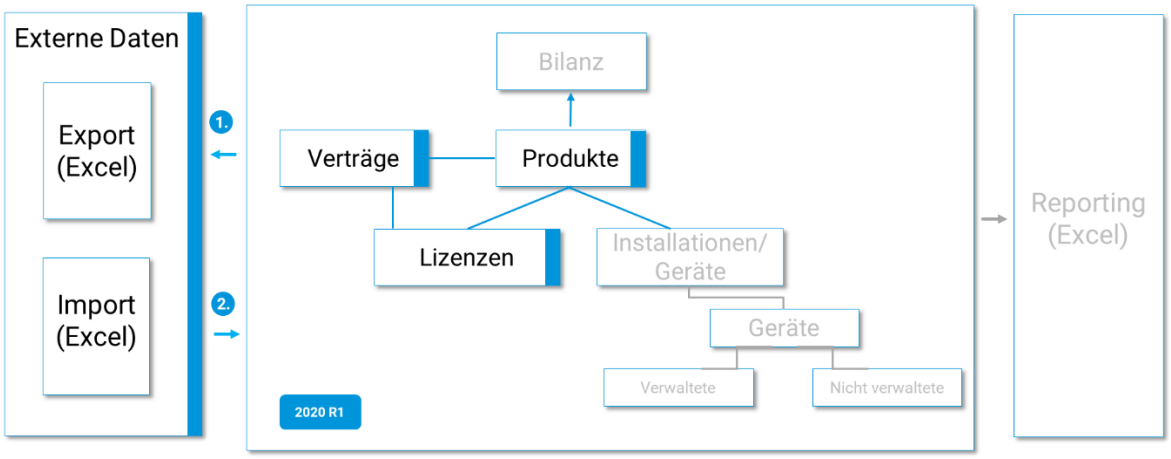


Abbildung 113 – Lizenz Management Gesamtkonzept 2020 R1

6.3.1.2 Import von Produkten, Lizenzen und Verträgen

Im Rahmen der Ersteinrichtung bzw. der Erweiterung einer bLM Umgebung kann es hilfreich sein, bereits verfügbare Daten zu Produkten, Lizenzen oder Verträgen einbinden zu können.

Mit der 2020R1 bieten wir die Möglichkeit Daten aus externen Quellen zu importieren.

Als Alternative zur manuellen Anlage können durch einen Import aus Excel, Daten zu Produkten, Lizenzen und Verträgen in bLM übernommen werden. Eine aus bLM exportierte Excel-Formatvorlage dient als Grundlage für den Import von externen Daten um Setupaufwände in bLM zu reduzieren.

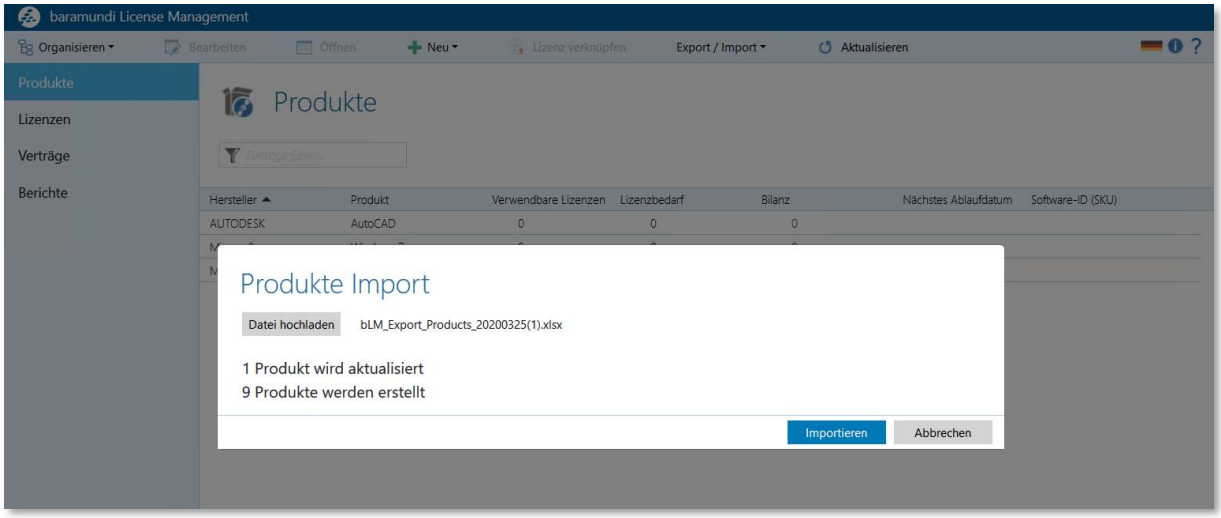


Abbildung 114 – Lizenz Management Import von externen Produktdaten

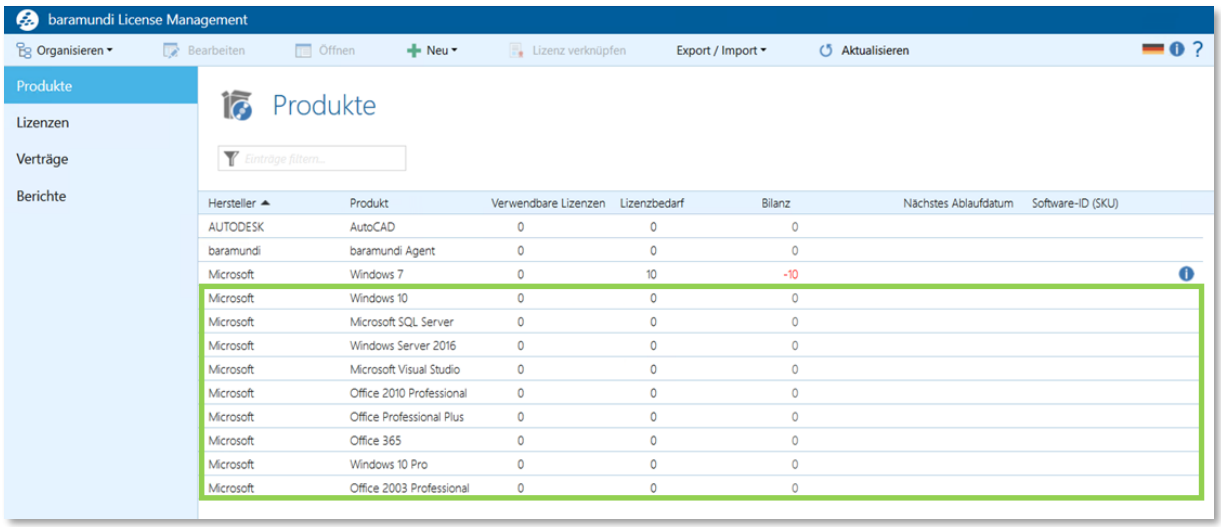


Abbildung 115 – Lizenz Management: Erweiterte Produktübersicht nach Import

6.3.2 Inventarisierung des Windows Security Center

Als Administrator möchte man stets über den aktuellen Sicherheitszustand der Endpoints informiert sein. Aus diesem Grund inventarisiert die bMS nun auch die Zustände der einzelnen Kategorien des Windows Sicherheitscenters. So ist in der bMC jederzeit ersichtlich ob z.B. der Virenschutz aktiv und aktuell ist. Ebenso kann der Zustand der Firewall und der anderen Module abgerufen werden.

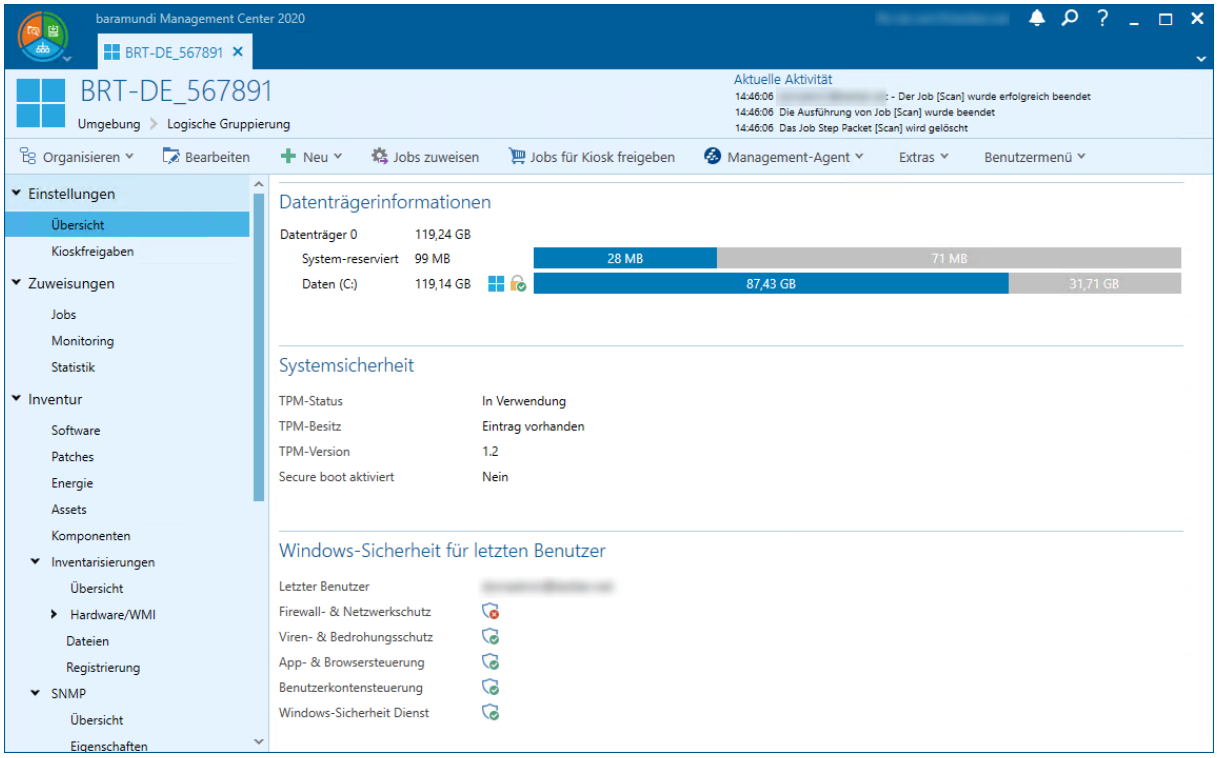


Abbildung 116 – Inventur des Windows Sicherheitscenter

Selbstverständlich sind diese Werte auch in einer universellen dynamischen Gruppe (UDG) als Filter und als Spalte verwendbar. Somit kann der Zustand bzw. die Kombination aus Zuständen bequem überwacht werden.

6.3.3 Client-Variablen in universellen dynamischen Gruppen

Die universellen dynamischen Gruppen wurden um die Anzeige der Endpoint Variablen erweitert. Somit können nun die Variablen der mobilen Geräte als auch der Windows Endpoints sowohl als Filter aber auch als Spalte eingeblendet und verwendet werden.

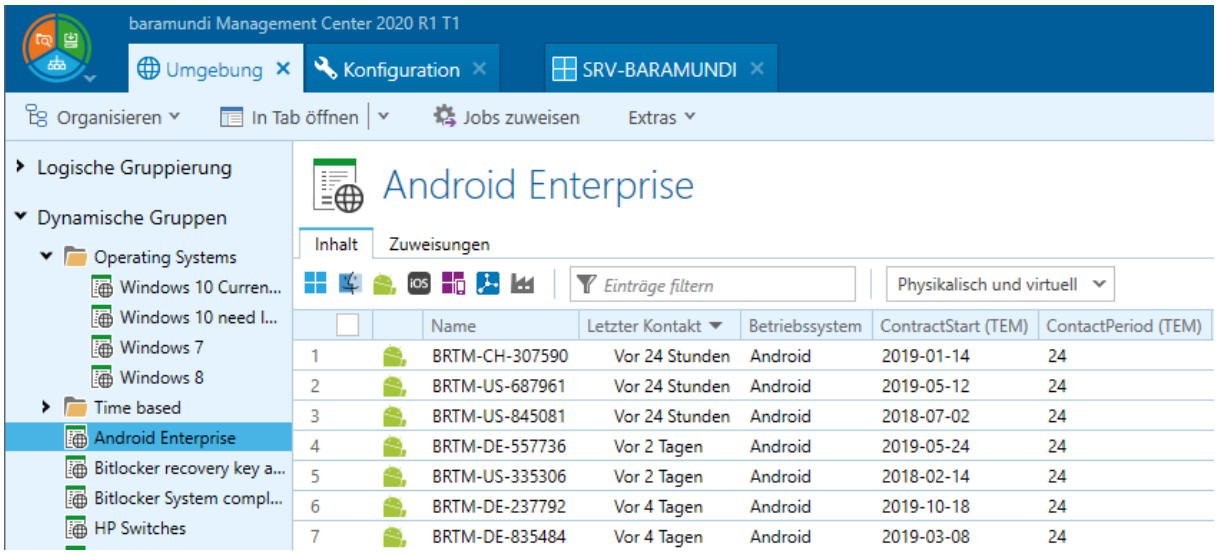


Abbildung 117 – Mobile Endpoints mit Variablen in einer UDG

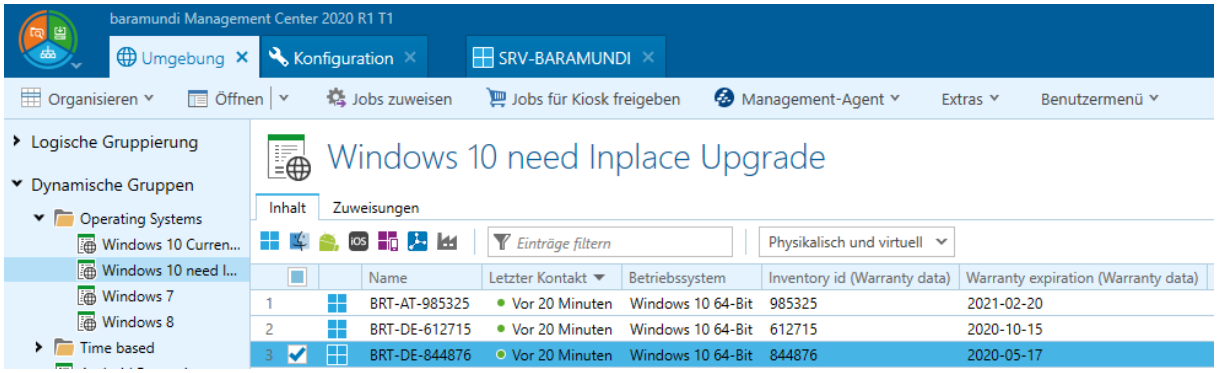


Abbildung 118 – Windows Endpoints mit Client-Variablen in einer UDG

6.3.4 Aufruf des Kiosks vom Desktop oder Startmenü

Der gerätezentrische Kiosk kann nun auf Client-Systemen auch ohne baramundi-Symbol im Tray geöffnet werden. Hierzu kann eine Verknüpfung an eine beliebige, für den Anwender erreichbare, Stelle (z.B. Desktop oder Startmenü) gelegt werden.
Durch Aufruf von `BMACmd.exe /Cmd:OpenKiosk` wird der Kiosk mit der gerätezentrischen Sicht im Standardbrowser des Anwenders geladen.
Ein einfaches Skript zur Erzeugung und Verteilung dieser Verknüpfungen wird zum Release im Forum bereitgestellt.

6.3.5 MDM-Befehle für Apple Geräte

Für Apple-Geräte ist nun ein neuer Jobschritt verfügbar.
Mit dem Jobschritt „Befehl ausführen“ können MDM-Kommandos an alle unterstützten Apple-Geräte gesendet werden. Somit ist es nun beispielsweise möglich, das Hintergrundbild unter iOS oder auch den Gerätenamen per Job zu ändern.

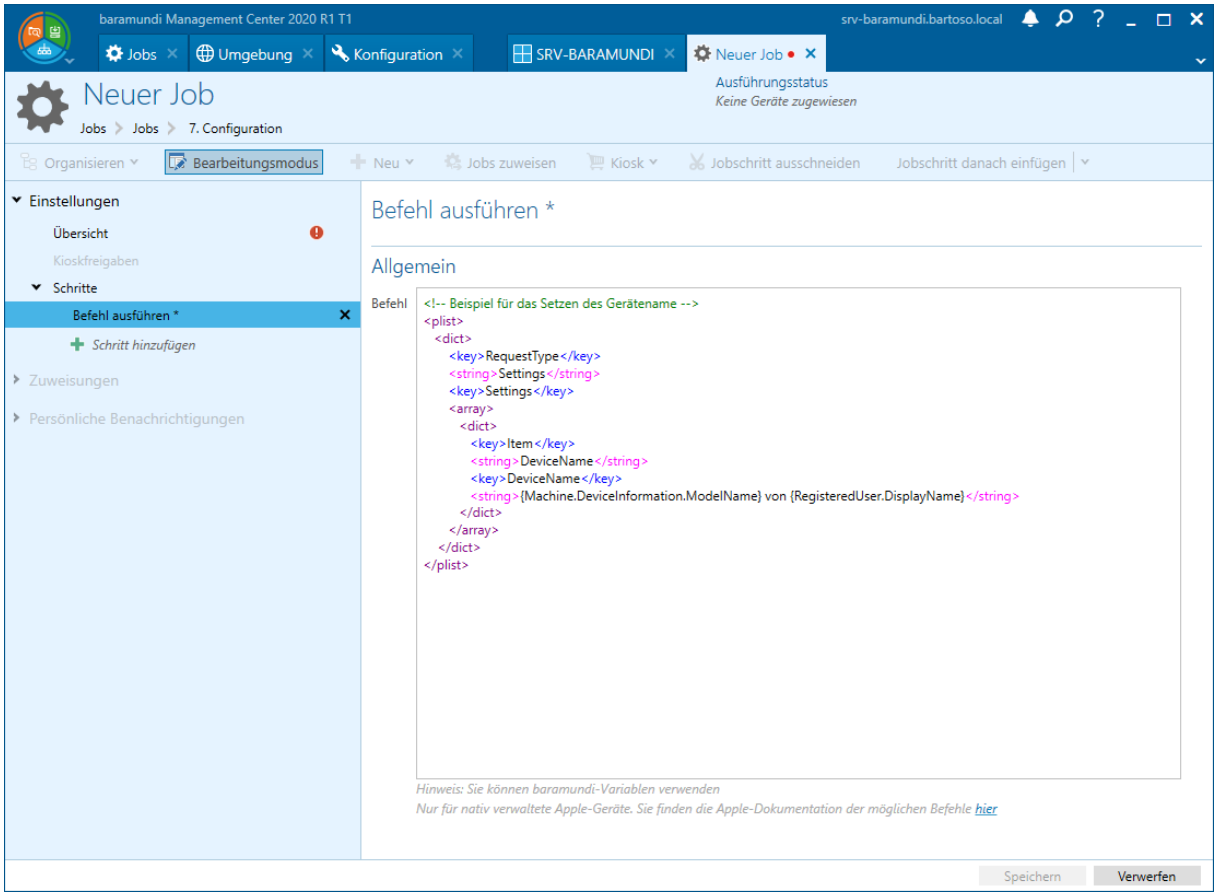


Abbildung 119 – Änderung des Gerätenamens mit baramundi Variablen

Eine Liste der von Apple vorgesehenen Kommandos ist online verfügbar und wird regelmäßig durch Apple erweitert.[10]

Selbstverständlich können auch baramundi-Variablen innerhalb des Kommandos verwendet werden.

[10] Apple MDM Commands and Queries: https://developer.apple.com/documentation/devicemanagement/commands_and_queries

6.3.6 Sichere Aufnahme von Windows Endpoints über das Internet (IEM)

Bereits seit Release 2016 R2 können mit der bMS auch Windows Endpoints außerhalb des lokalen Netzwerks und ohne VPN verwaltet werden. Die Aufnahme ins Management und damit das Herstellen der Vertrauensstellung erfolgte bisher ausschließlich im lokalen Netz oder manuell per Import des öffentlichen Schlüssels vom Clientzertifikat.

Mit der bMS 2020 können nun auch Windows Endpoints außerhalb des lokalen Netzwerks sicher aufgenommen werden. Dazu wurde eine Enrollment-Funktionalität für Windows Endpoints – ähnlich des Enrollments bei baramundi Mobile Devices – integriert. Der Administrator kann nun einen neuen Windows Endpoint anlegen und eine Mailadresse angeben. An diese Adresse werden alle relevanten Informationen zur Installation des baramundi Management Agents und für das Enrollment geschickt.

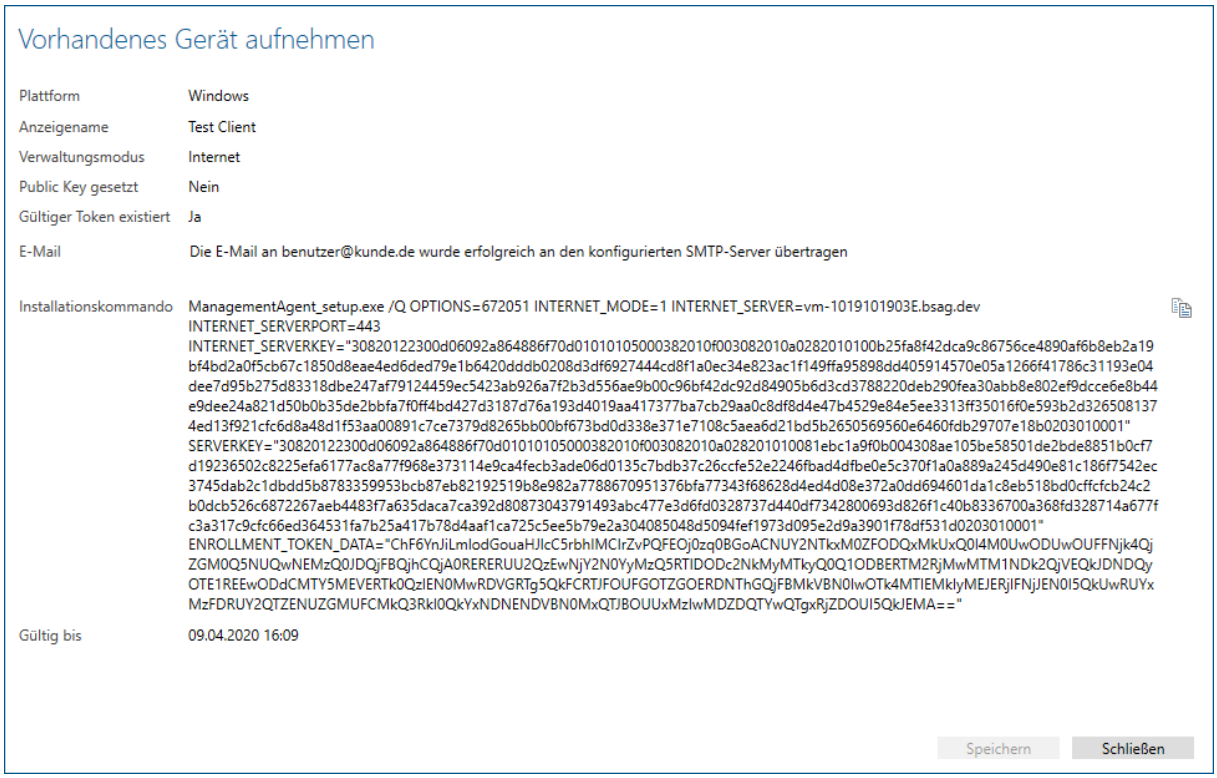


Abbildung 120 – Enrollment-Dialog in der bMC

Der Anwender kann nach Erhalt der Mail den Agent installieren und eine sichere Verbindung zum baramundi Management Server herstellen. Hierfür kann die Enrollment-Information direkt auf der Kommandozeile während der Installation mitgegeben werden. Alternativ kann der Agent auch nach der Installation initial mit dem Server verbunden werden. Hierzu wurde dem Kontextmenü des Agents ein neuer Eintrag hinzugefügt.

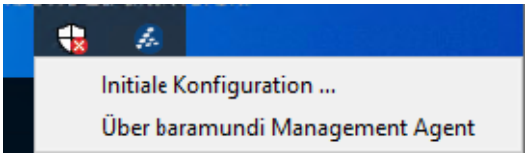


Abbildung 121 – Kontextmenü des Agents

Durch den Klick auf „Initiale Konfiguration“ öffnet sich ein Dialog zur Eingabe der Enrollment-Information. In diesen Dialog kann das komplette Installationskommando aus der Enrollment-Mail eingefügt werden, mit einem Klick auf OK startet der Agent das Enrollment und verbindet sich mit dem Management Server.
Nach erfolgtem Enrollment kann der Endpoint wie gewohnt mit Jobs versorgt werden.

6.4 Produktverbesserungen im Detail

6.4.1 Windows Agent (bMA)

- Der `Compliance-Vulnerability Scan` wurde verbessert und benötigt jetzt erheblich weniger Arbeitsspeicher, dafür wird mehr temporärer Plattenplatz benötigt.
- Im Kiosk wurde die Zuweisung an das gerade aktuelle Gerät vereinfacht.
- Der Kiosk kann über bMACmd gestartet werden. Dies ermöglicht z.B. Icons auf dem Desktop zum Öffnen des Kiosks.
- Vereinfachtes IEM Enrollment. IEM Endpoints können nun komfortabel über den Eintrag „`Initiale Konfiguration`“ des Kontextmenüs des Agents enrollt werden.
- Die Unterstützung für das veraltete Disk-Image-Format (.bdi) wurde entfernt.
- Ein SingleExeSetup zur Installation des bMA im Falle des IEM Enrollments ist verfügbar.
- Bugfix: Die ermittelte Bootzeit zeigt ab Vista den letzten Wake-Up Zeitpunkt an, statt der relaen System-Bootzeit.
- Bugfix: Im bMA.log wird bei Servern ohne aktivierten Bitlocker Feature ein Fehler geloggt, wenn Bitlocker deaktiviert werden soll.

6.4.2 bMA auf Mac

- Skriptausführung ist auch auf macOS 10.14.3 möglich.
- Bugfix: Eine Reinstallation des Agenten ist auf Catalina nicht möglich.

6.4.3 Management Center (bMC)

- Das bMA Installationskommando für einen einzelnen IEM-Client kann über die Aktion `Client-Extras-Neu aufnehmen` erzeugt werden. Dieses kann bei konfiguriertem Mail-Server auch automatisch per Mail verschickt werden. Das Enrollment eines Windows-IEM-Clients ähnelnd damit dem Enrollment eines MDM Gerätes.
- Abfragen mittels Universelle Dynamische Gruppen unterstützen jetzt auch Client-Variablen.

- Neue Spalten bei der Listenanzeige von Windows Applikationen zeigen verwendetes `Login bDS`, `Installationskommando`, `Deinstallationskommando` und `Datei für Installationsmechanismus`.
- Neue Spalten `Dateieinträge` und `Registrierungseinträge` bei `Inventur - Softwareerkennungsregeln`.
- Unter `Software - Managed Software` zeigt das Icon des MSW Produkts die eingestellte Standartfreigabe an.
- Neue Einstellung `deaktivieren` an Bitlocker Jobs.
- Restriktionen für iOS Endgeräte wurden erweitert.
- Neuer Downloadjob `Industrial Data` für die Inventur von SIMATIC S7 Geräten.
- An der Applikation können hinterlegte Deploy-bDS Dateien direkt zum Editieren geöffnet werden.
- Neuer Endpoint-Typ `Industrielles Steuergerät` zum Anlegen einer SIMATIC S7, inklusive Abfragemöglichkeit mittels universeller Dynamische Gruppe und Erkennung über Netzwerkscan.
- Inventurjob für SIMATIC S7 Geräte möglich.
- Industrielle Steuergeräte werden in der IT-Landkarte angezeigt.
- In der MSW-Übersicht wird der Link zum Forumseintrag nun im System-Standard-Browser geöffnet.
- Auf den Seiten `Software - Applikationen - Übersichtsseite` einer Software kann eine, als Mechanismus hinterlegte bDS Datei schnell im AutomationStudio geöffnet werden.
- Der Status der jeweilgen Einstellungen von `Windows - Sicherheit` kann unter `Client - Übersicht` eingesehen werden.
- Bugfix: Bei Assets wurden die Daten der Kostenstelle nicht exportiert.
- Bugfix: Die Aktion ‚`Job Abbrechen`' und Job ‚`OK Setzen`' ändert den Zeitpunkt von ‚`Letzte Aktion`' nicht.

- Bugfix: Um ein Mac-Gerät aufzunehmen ist mindestens eine freie MDM Lizenz notwendig.
- Bugfix: Ein automatisch über die Aktion `Client - Neu installieren` generierter Job bootet teilweise in ein falsches PE Image.
- Bugfix: An einer Applikation wird das hinterlegte Login bDS nicht korrekt beschrieben.
- Bugfix: Die Aktion ‚`Client - Shutdown/Neustart`' zeigt auf englischen Systemen im Fehlerfall eine deutsche Fehlermeldung an.
- Bugfix: In den Energie-Standardwerten für Monitore wird für einen ausgeschalteten Monitor mehr Verbrauch berechnet, als wie für einen Monitor in Bereitschaft.
- Bugfix: Wird im Jobzuweisungsdialog eine Liste von Clients mittels Import eingelesen, so wird der Displaynamen statt der Hostnamen in den importierten Daten benötigt. (Neu: Displaynamen und Hostnamen sind möglich).

6.4.4 Mobile Devices

- Die Knox-Unterstützung wird nur noch für Legacy Android Geräte angezeigt.
- Die Geokoordinaten für den LostMode können jetzt direkt im Browser geöffnet werden.
- Installationsjobs und Deinstallationsjobs können per Multiselekt für mehrere Apps angelegt werden.
- Deinstallationsjobs können direkt aus der App-Inventur eines Geräts angelegt werden.
- Sichtbarkeit der Widgets im Android Enterprise Work Profile kann konfiguriert werden.
- Neuer Jobschritt „`Befehl ausführen`“ für iOS Geräte.
- Systemupdates (OTA) sind nun für zweckbestimmte Geräte und vollständig verwaltete Geräte (Android Enterprise) konfigurierbar.
- Bugfix: Die iOS SystemApps iMovie, Clips, iTunes U und GarageBand ließen sich nicht per Job verteilen.

- BugFix: In seltenen Fällen kommt es bei der Verwendung von VPP-Lizenzen zu Datenbankfehlern. Ein VPP-Sync ist in diesen Fällen nicht mehr möglich.

6.4.5 Automation Studio

- Es ist möglich das Logging für einzelne Aktionen zu deaktivieren.
- Hinweis: Beim Öffnen vorhandener bDS Dateien erscheint ein Hinweis das bDS Skript in das aktuelle Format zu konvertieren. Mit Automation Studio 2020 erstellte bDS Dateien können von baramundi Agenten (bMA) kleiner 2020 nicht ausgeführt werden.

6.4.6 bRemote

- Bugfix: In bestimmten Fällen bricht die Aufschaltung ab und eine Neuverbindung zeigt den Fehler "Die Remoteverbindung wird nicht aufgebaut, da bereits ein anderer Benutzer versucht eine Verbindung aufzubauen."

6.4.7 bConnect

- Das Aufnehmen von IEM Clients kann über den `EndpointEnrollment` Controller gesteuert werden.
- Das JobInstanz-Objekt wurde um eine performante Abfrage von Job-Daten ergänzt.
- IC-Device Jobs können gelesen, angelegt und geändert werden.
- Neuer Controller „ServerState“ ermöglicht Lesen der Status-Informationen der einzelnen Server-Module.
- Android Enterprise und zweckbestimmte Android Geräte können angelegt werden.
- Bugfix: Das Lesen von Hardwaredaten für Mobile Geräte führt zu Fehlern und liefert keine Ergebnisse.

6.4.8 License Management

- Das Setup wurde aus dem bMS-Setup entkoppelt. Im Rahmensetup ist es weiterhin enthalten.
- Bugfix: Beim Einlesen der Inventurdaten kann es zu Performanceproblemen und zu SQL Fehlernmeldungen kommen.
- BugFix: Unter Umständen wird der Lizenzverbrauch fehlerhaft ermittelt.

6.4.9 IC – Industrial Control Devices

- Neues Modul „IC Inventory“ zur Verwaltung von industriellen Steuergeräten vom Typ SIEMENS SIMATIC S7 Geräten.
- Neuer Jobtyp für IC-Devices.

7 Release 2019 R2

7.1 Android Enterprise: Work Profile

7.1.1 Containment mit Bordmitteln

Die transparente Datentrennung in iOS ist nur ein Ansatz für die tief im Betriebssystem verankerte Trennung von privaten und geschäftlichen Daten. Android geht hier mit dem Work Profile noch einen Schritt weiter: Der Anwender erhält auf seinem Smartphone oder Tablet einen komplett separierten Bereich für geschäftliche Apps und Daten. Dieser Bereich wird vom Unternehmen verwaltet und ist für Apps im privaten Kontext nicht sichtbar. Das Prinzip der Trennung besteht in beide Richtungen, so kann der Administrator beispielsweise nicht sehen, welche Apps der Anwender privat installiert hat.
Diese konsequente Form der App- und Datentrennung, und damit Abschirmung aller Informationen, ist so ausschließlich mit den Bordmitteln von Android Enterprise möglich.

Abbildung 122 - Symbolische Darstellung des "Work Profile"

Durch die nahtlose Integration in die Firmware können auch Sicherheitsupdates der Gerätehersteller umgehend eingespielt werden, die Kompatibilität ist sichergestellt. Ebenso können alle Apps aus dem Enterprise PlayStore verwendet werden ohne speziell angepasste oder gewrappte Versionen beim Hersteller anfordern zu müssen.

7.1.2 Das Work Profile im Detail

Mit der bMS 2019 R2 hat der Administrator nun die Wahl zwischen dem – mit der bMS 2018 R2 eingeführten – „Fully Managed Device“ und dem „Work Profile“. Während das „Fully Managed Device“ für die ausschließlich geschäftliche Nutzung (COBO) vorgesehen ist, ermöglicht das Work Profile eine datenschutzrechtlich unbedenkliche Nutzung von Firmengeräten für private Zwecke und sogar die geschäftliche Nutzung von Privatgeräten (BYOD).

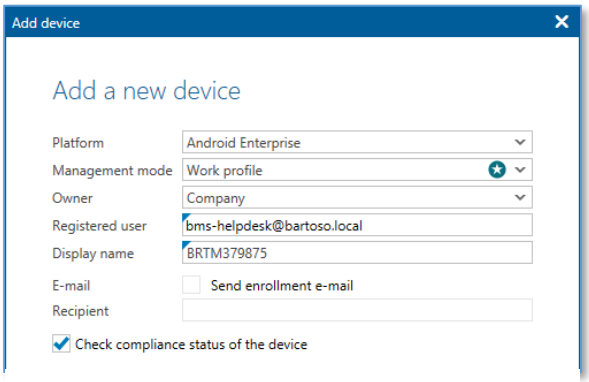


Abbildung 123 – Enrollment-Dialog für das Work Pro-

Bereits beim Enrollment wird festgelegt in welchem Modus das Gerät betrieben werden soll.

Auf dem Gerät selbst wird der baramundi EMM Agent vom Anwender aus dem Play-Store installiert und z.B. per QR-Code ins Management aufgenommen.

Im Rahmen des Enrollments erhält der Anwender einige Hinweise zum Umgang mit dem „Work Profile“ (herstellerabhängig), während der Agent die Umgebung bereitstellt. Nach erfolgreicher Einrichtung steht dem Anwender die geschäftliche Umgebung zur Verfügung.

Die Darstellung des „Work Profile“ ist dabei sowohl vom Gerätehersteller als auch von der verwendeten Android-Version abhängig. So werden die privaten und geschäftlichen Apps entweder in eigenen Tabs sortiert oder einfach gemeinsam in einer Liste dargestellt. In beiden Fällen sind die geschäftlichen Apps für den Anwender klar ersichtlich mit einem Koffersymbol gekennzeichnet.

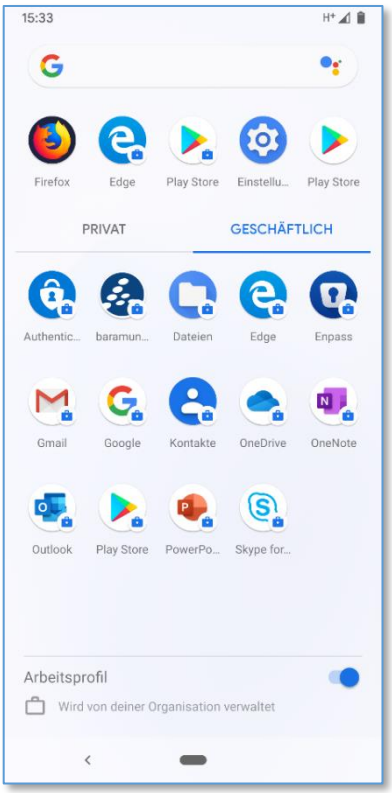


Abbildung 124 - "Work Profile" auf einem Google Pixel 3 mit Android 10

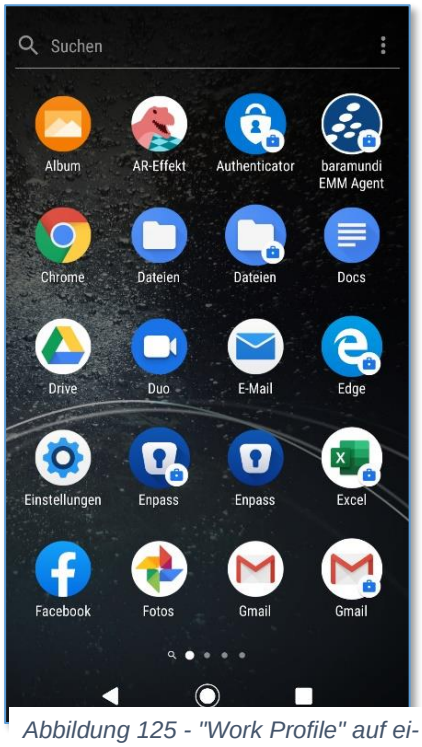


Abbildung 125 - "Work Profile" auf einem Sony XA2 mit Android 9

Hier zeigt sich auch eine der großen Stärken des „Work Profile“:

Eine gegebene App kann sowohl vom Anwender selbst, aber auch vom Administrator per bMD aus dem PlayStore installiert werden.

Die App des Anwenders wird dabei von ihm selbst aus dem PlayStore geladen, installiert und konfiguriert. Sie hat keinen Zugriff auf die Daten innerhalb der geschäftlichen Umgebung. Die App im „Work Profile“ kann vom Administrator installiert und konfiguriert werden und hat wie-

derum keinen Zugriff auf die privaten Daten des Anwenders. Zusätzlich kann sich der Anwender selbst an den – vom Administrator geprüften, freigegebenen und vorkonfigurierten – Apps im geschäftlichen PlayStore bedienen. Welche Apps dem Benutzer dort zur Auswahl stehen, kann der Administrator bequem im baramundi Management Center per App-Liste bestimmen.

Selbstverständlich können auch Sicherheitseinstellungen und Einschränkungen auf dem „Work Profile“ angewandt werden. Hierbei ist zu beachten, dass diese Einstellungen nun gezielt für die geschäftliche Umgebung angewandt werden können. Diese Restriktionen greifen dann nur im „Work Profile“. So kann der Administrator bspw. die Kamera in der geschäftlichen Umgebung verbieten, der Anwender kann diese aber im privaten Kontext noch immer verwenden.

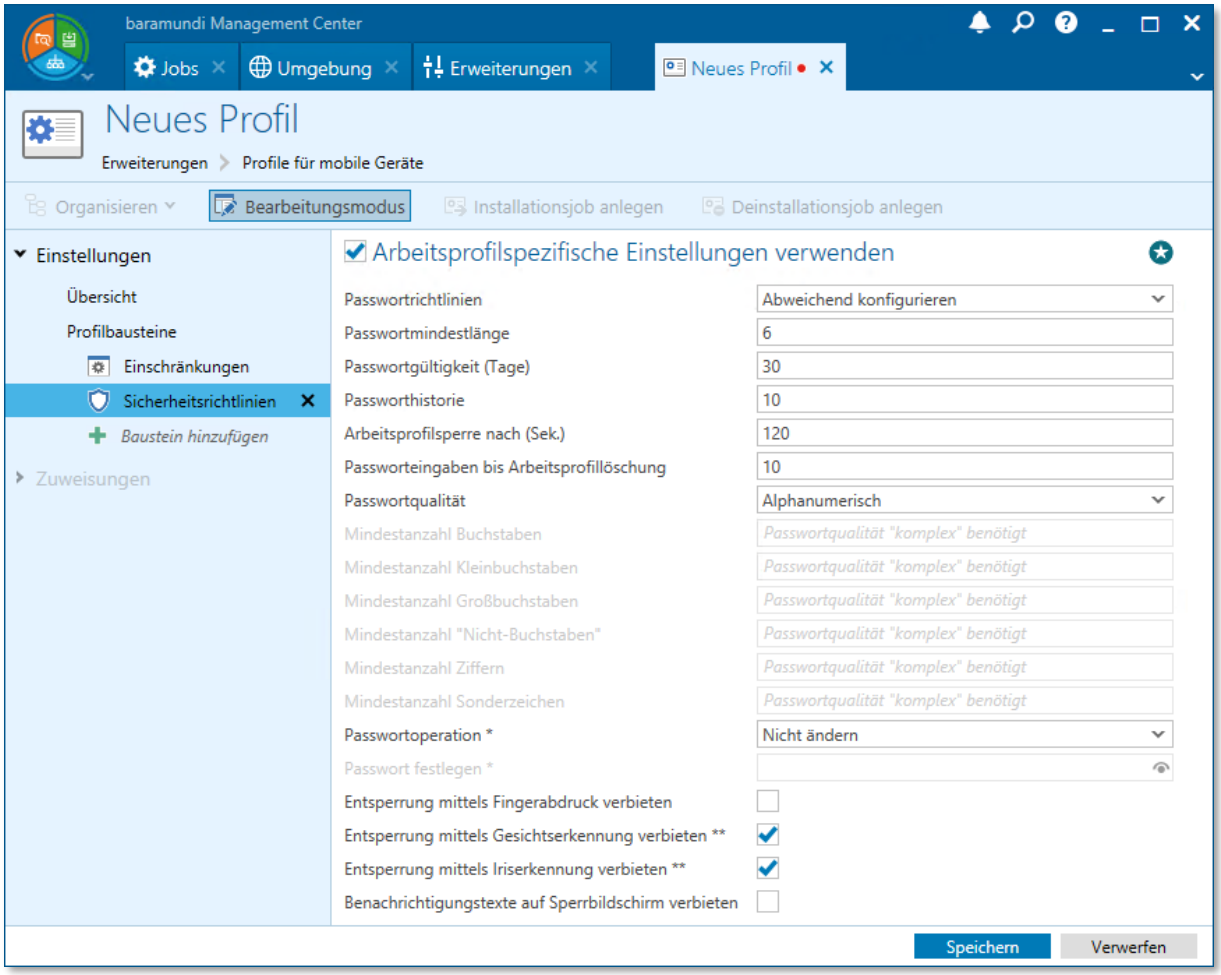


Abbildung 126 - Sicherheitseinstellungen für das "Work Profile"

Bei der Verwendung des „Work Profile“ hat der Administrator nur bedingt die Möglichkeit Gerätefunktionen einzuschränken, da diese für das komplette Gerät gelten und somit auch den

privaten Bereich einschränken würden. Im baramundi Management Center sind die Einstellungen daher übersichtlich nach Anwendungsbereich getrennt dargestellt und können nach Bedarf aktiviert und verwendet werden.

Das Android Enterprise Work Profile und weitere Schalter zur feingranularen Einstellung der Datentrennung unter iOS sind im Modul *baramundi Mobile Devices Premium* enthalten. Das Modul erweitert alle bisherigen Funktionalitäten des Moduls *baramundi Mobile Devices* um diese Funktionen zur Datentrennung.

7.2 Windows Bitlocker

7.2.1 Transparenz

Der Bitlocker ermöglicht die sichere und transparente Verschlüsselung der Datenträger eines Windows-Systems, um den Zugriff auf die Daten durch einfaches Aus- und Umbauen des Datenträgers zu unterbinden. Zusätzlich kann das System beim Booten durch eine PIN geschützt werden. So ist sichergestellt, dass das System nur von einer befugten Person gestartet werden kann.

Um den Überblick darüber zu behalten, welche Systeme ganz, gar nicht oder nur zum Teil verschlüsselt sind, inventarisiert der baramundi Management Agent nun auch den Status des Bitlocker auf verwalteten Systemen und gibt detailliert Auskunft über den Zustand der Verschlüsselung auf den verschiedenen Partitionen.

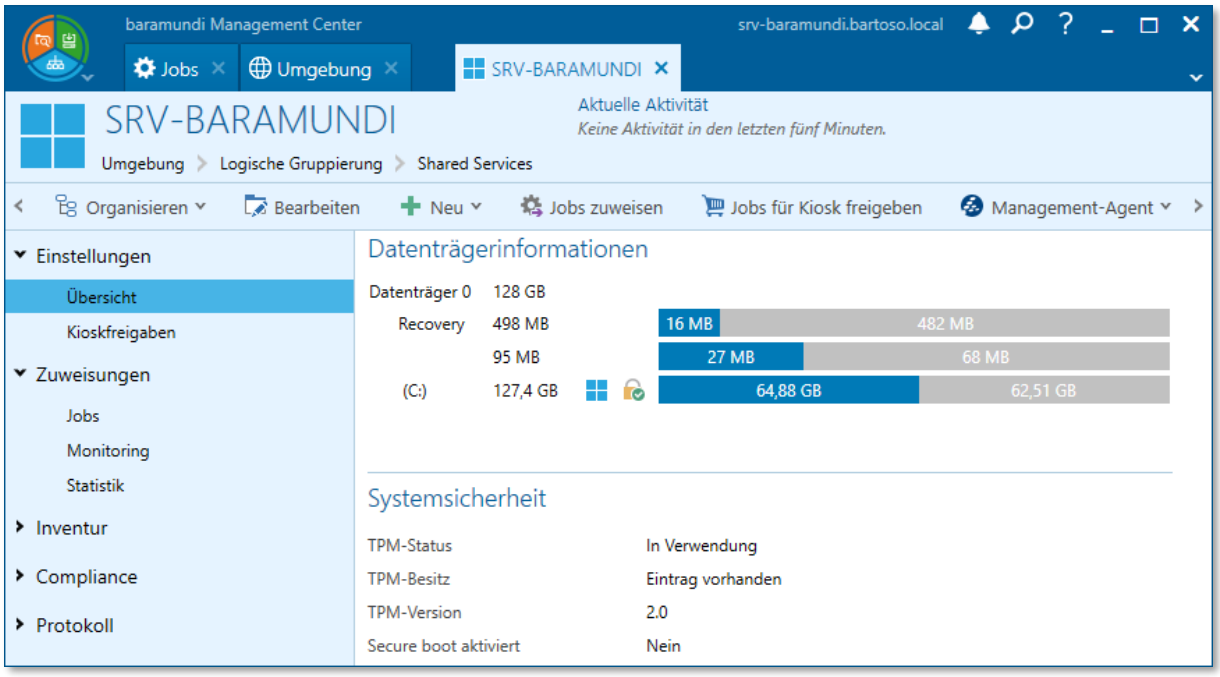


Abbildung 127 - Bitlocker-Informationen auf der Übersichtsseite eines Windows-Endpoints

Diese Informationen werden sowohl auf der Übersichtsseite der Windows-Endpoints angezeigt und stehen auch als Filter für universelle dynamische Gruppen (UDG) zur Verfügung. So lässt sich schnell bequem eine Übersicht über den Verschlüsselungszustand der verwalteten Endpoints gewinnen.

7.2.2 Konfiguration

Um einen zuverlässigen Schutz durch den Bitlocker zu erreichen, muss dieser zuerst entsprechend konfiguriert und aktiviert werden.
Hierzu bietet die baramundi Management Suite nun die Verwaltung eigener Bitlocker-Konfigurationsprofile an. Per Profil legt der Administrator die Verschlüsselungsmethode und die zu verschlüsselnden Laufwerke fest. So kann gezielt vorgegeben werden, ob nur das Systemlaufwerk oder auch zusätzlich alle Datenlaufwerke mitverschlüsselt werden sollen. Auch ob eine initiale PIN für den Betriebssystemstart mit entsprechender Komplexität verwendet werden soll kann vorgegeben werden. Diese PIN wird beim Einrichten der Verschlüsselung automatisch nach den Regeln des Profils generiert und gesetzt.

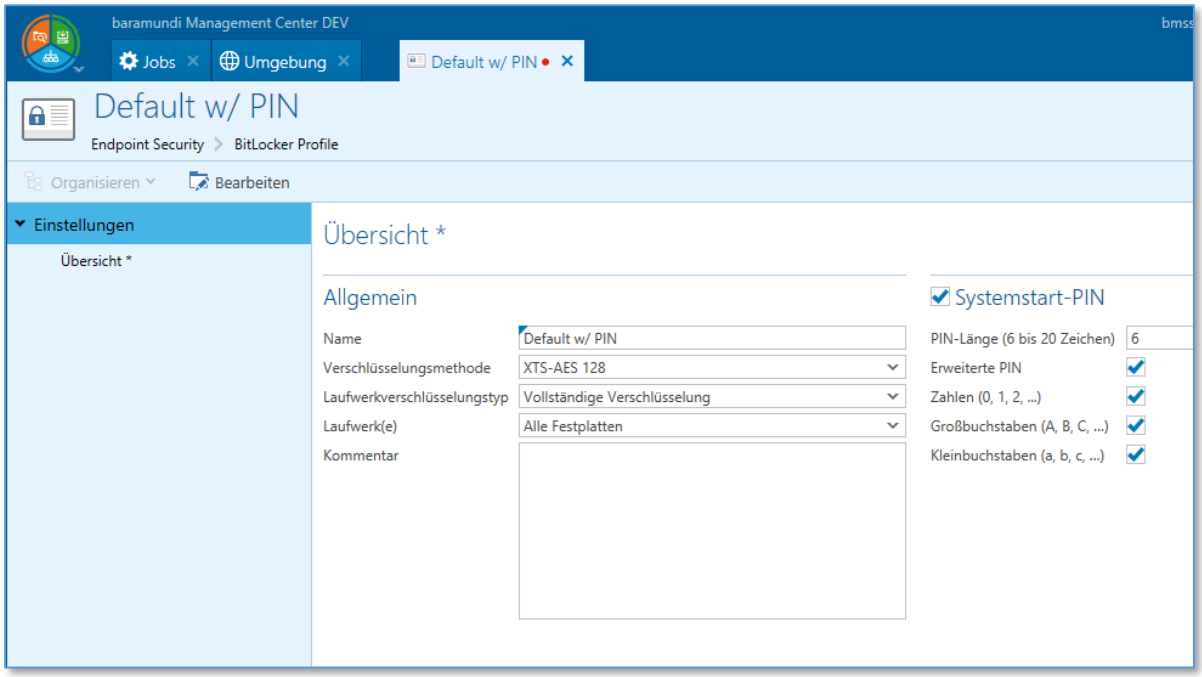


Abbildung 128 - Konfigurationsprofil für Bitlocker

7.2.3 Wiederherstellungsschlüssel und PIN

Wiederherstellungsschlüssel und PIN werden bei der Aktivierung der Verschlüsselung über baramundi in der bMS gespeichert. Die Wiederherstellungsschlüssel der Laufwerke werden regelmäßig inventarisiert und ebenfalls angezeigt. Diese Informationen stellen für den Administrator einen wertvollen Teil seiner Bitlocker Recovery Strategie dar.

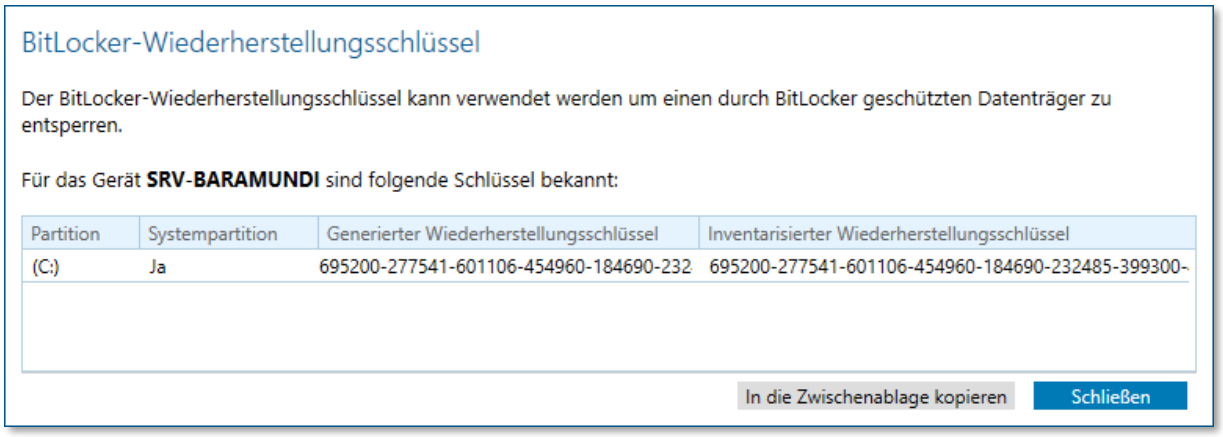


Abbildung 129 - Liste der Wiederherstellungsschlüssel

Selbstverständlich werden diese Daten verschlüsselt gespeichert und durch das baramundi Berechtigungskonzept abgesichert. So erhält ein Administrator nur die Wiederherstellungsschlüssel für Systeme auf denen ihm dieses Recht explizit gewährt wurde.

7.3 Allgemeine Weiterentwicklung

7.3.1 Kiosk: Übersicht von Job- und Gerätezuordnungen zu Benutzern

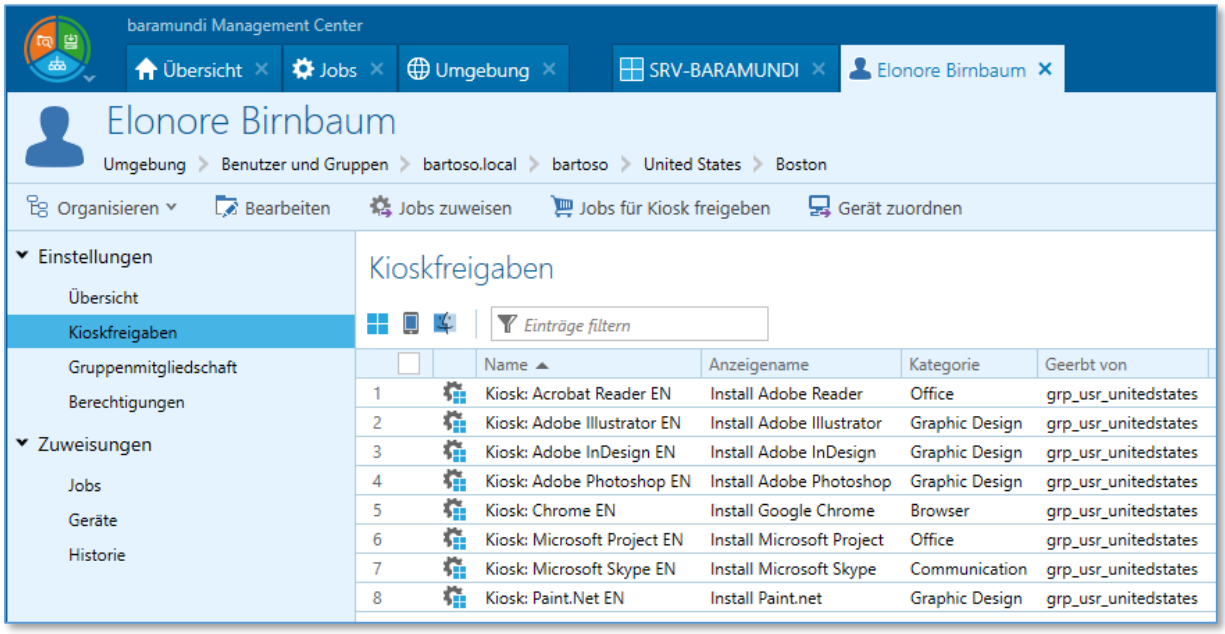


Abbildung 130 - Für den Benutzer im Kiosk sichtbare Jobs

Auch bei der Anzeige der Benutzer und Gruppen sowie der Auflistung der zugeordneten Jobs und Geräte gibt es Neuerungen. So kann nun über die Benutzer und Gruppen unterhalb der Umgebung nachvollzogen werden, welche Jobs ein Benutzer im Kiosk sehen kann sobald er sich anmeldet. Hierbei werden auch die Gruppenmitgliedschaften des Benutzers berücksichtigt um darüber vererbte Jobs anzuzeigen.

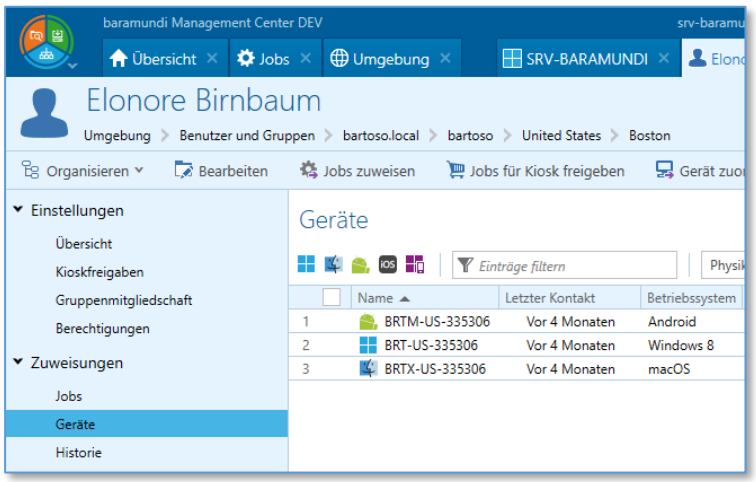


Abbildung 131 - Auflistung der Geräte des Benutzers

Zusätzlich zur Zuordnung der Jobs werden die Geräte aufgelistet, an denen dieser Benutzer als sog. „Registrierter Benutzer“ hinterlegt ist.

7.3.2 License Management

Das *baramundi License Management* bietet eine kompakte und einfache Möglichkeit, um kaufmännische Informationen aus dem Lizenzmanagement zu berücksichtigen und damit eine bessere Transparenz der im Unternehmen vorhandenen Lizenzen zu erreichen.

Die neue Version wurde um eine direkte Lizenzverwaltung, eine Anzeige von Geräten und diversen Workflow-Verbesserungen erweitert.

7.3.2.1 Konzept

Die Bilanz gibt eine Übersicht der dargestellten Produkte mit den zugeordneten Lizenzen und den entsprechenden Installationen aus der baramundi Inventur.

Mit der neuen Version gibt es neben dem ersten Aufbau eines Produktes ① auch die Möglichkeit Lizenzen ① direkt anzulegen. Eine Zuordnungsmöglichkeit ② in beide Richtungen ist in der Folge gegeben.

Die Installationen (Software Erkennungsregeln) aus der baramundi Inventur werden dem entsprechenden Produkt zugeordnet ③. In der 2019R2 werden den Installationen entsprechend auch die jeweiligen Geräteinformationen angezeigt.

Die Sicht auf die Geräte ④ zeigt über die durch baramundi verwalteten Geräte. Um die Bilanz umfassender darzustellen kann es notwendig sein, auch nicht durch baramundi verwaltete Geräte zu berücksichtigen. So können bspw. Geräte einer Offlineinstanz manuell ⑤ angelegt und so direkt einem Produkt zugeordnet werden.

Informationen zu Verträgen ⑥ können angelegt und ergänzend mit Produkten und/oder Lizenzen verknüpft werden. Ein Reporting ⑦ ausgeleitet in Excel bietet unterschiedliche Sichten zur flexiblen Weiterbearbeitung und Erstellung von individuellen Berichten.

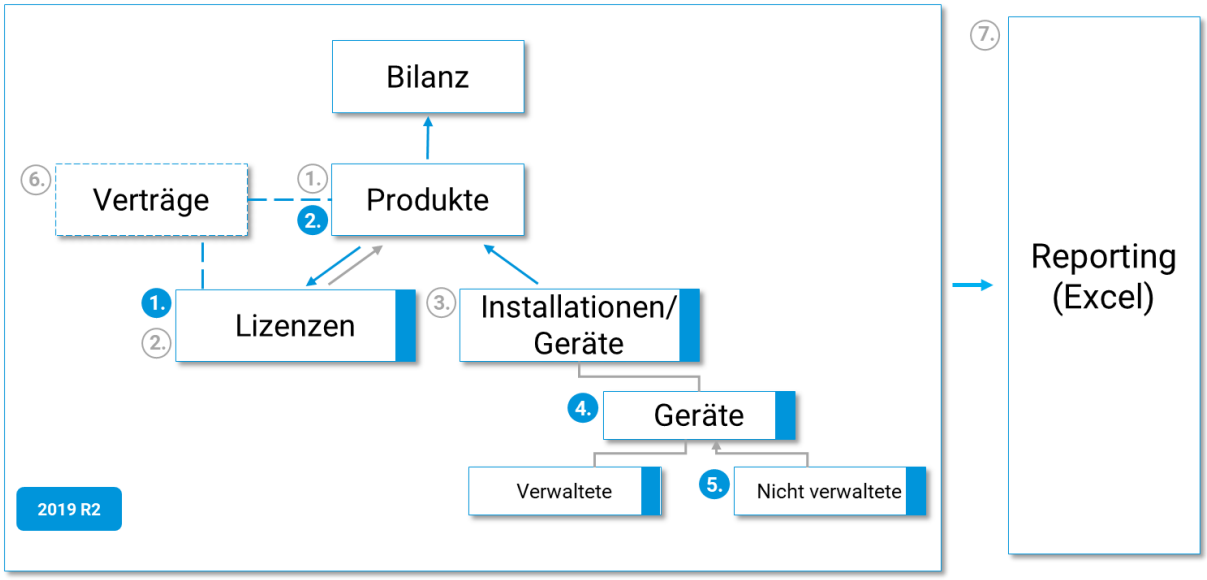


Abbildung 1 – Gesamtkonzept 2019 R2

7.3.2.2 Direkte Lizenzverwaltung

Durch die direkte Ansicht der angelegten Lizenzen besteht die Möglichkeit einen Überblick aller Informationen zur jeweiligen Lizenz zu erhalten.

Die kompakte Übersicht zeigt den Lizenzbestand, die bereits einem Produkt zugeordneten Lizenzen und die noch freien Lizenzen. So erkennt der Anwender einfach die aktuelle Situation und kann entsprechend Anpassungen vornehmen.

Eine Lizenz kann angelegt werden ohne vorher ein Produkt zu definieren.

Im Nachgang kann die angelegte Lizenz direkt mit einem Produkt oder einem Vertrag verknüpft werden.

Filter und Suchfunktionen erleichtern das Verwalten der Lizenzen. Die Eigenschaft Mehrfachnutzung kann mit der spezifischen Anzahl der Nutzungsrechte flexibel dargestellt werden.

Die originär dargestellte Lizenz kann kopiert werden. Diese Vorlage erleichtert die Wiederverwendung bereits angelegter Informationen um bspw. einen Nachbezug zügig abzubilden.

Das Reporting ist durch Informationen aus der direkten Lizenzverwaltung erweitert.

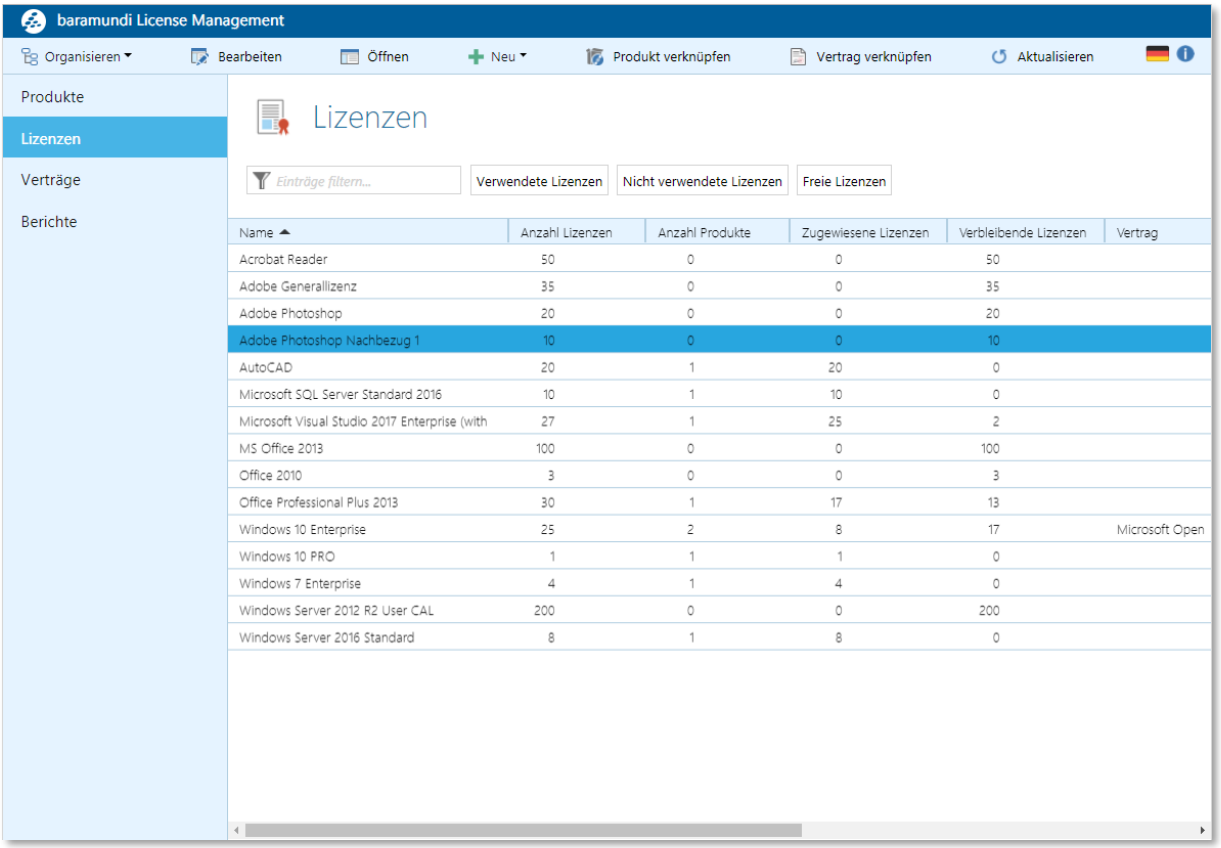


Abbildung 2 – Lizenzen direkte Ansicht

7.3.2.3 Geräteanzeige in Produkte

Die Tabelle zeigt die durch *baramundi Inventory* erfassten Geräte bezogen auf die mit dem Produkt verknüpften Installationen. Hierdurch wird ein Bezug zu den „Verbrauchern“ der jeweiligen Lizenz ermöglicht. Lizenzrelevante Informationen wie z.B. CPU, Kerne oder der registrierte Benutzer werden dargestellt.

Da aus Sicht einer Lizenzbilanz nicht nur die durch die Inventur erfassten Geräte relevant sein können, ist die Möglichkeit gegeben, Geräte manuell anzulegen. So können beispielsweise Geräte aus einer „Offline Instanz“ wie einer Produktion oder mit LINUX OS in eine Gesamtsicht aufgenommen werden.

Die Anzeige differenziert zwischen Geräten aus *baramundi Inventory* und manuell angelegten Geräten. Einmal manuell angelegte Geräte können in anderen Produkten wiederverwendet werden.

Das Reporting ist um Geräte relevante Informationen erweitert.

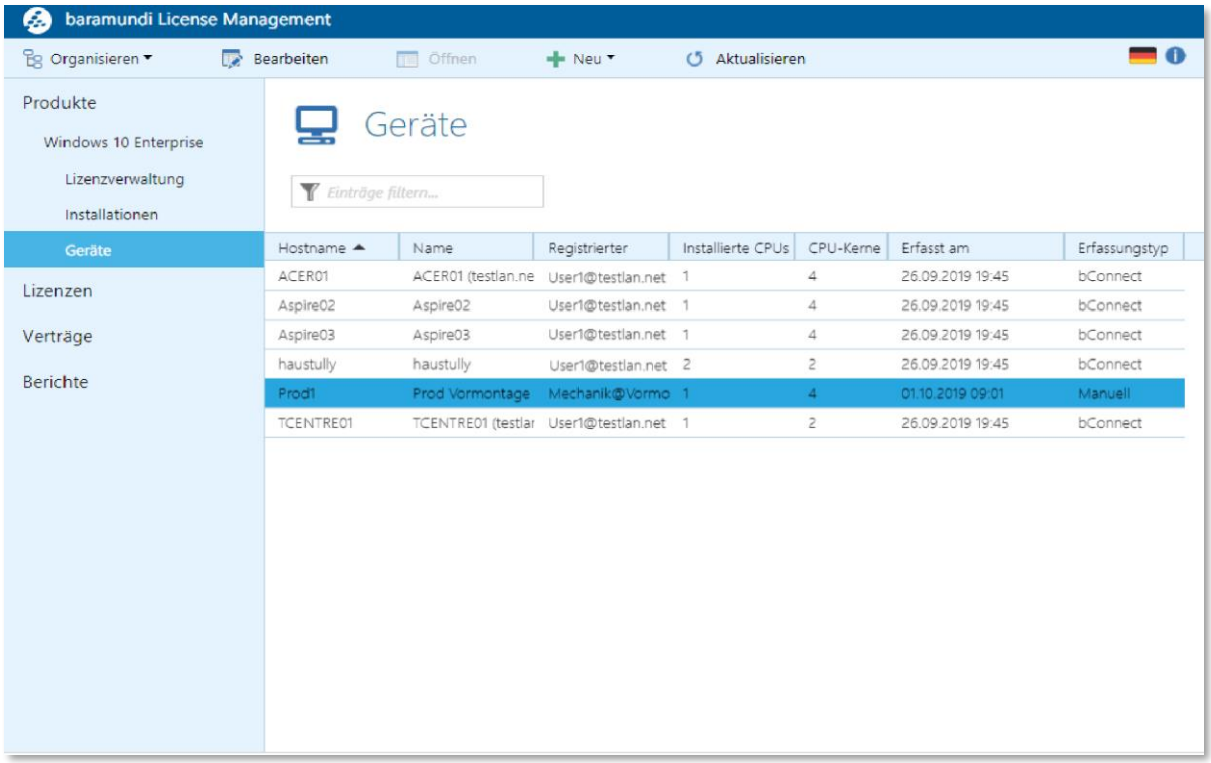


Abbildung 3 – Geräteanzeige

7.3.2.4 Weitere Funktionen

Befinden Sie sich im Bearbeitungsmodus und haben Ihre Eingaben nicht gesichert, werden Sie vor Verlassen der Ansicht hingewiesen, dass nicht gesicherte Eingaben verloren gehen.

Anwender die den Wert der Lizenz in unterschiedlichen Währungen darstellen wollen, wählen die jeweilige Landeswährung passend zum Beschaffungsvorgang.

Ein Freitextfilter in allen Ansichten mit Tabellendarstellungen ermöglichen ein schnelles Eingrenzen und Suchen von Einträgen. So findet der Anwender zielgerichtet die gewünschte Information.

Weitere Direktaktionen wie Lizenz, Vertrag und Produkt verknüpfen erleichtern die Anwendung.

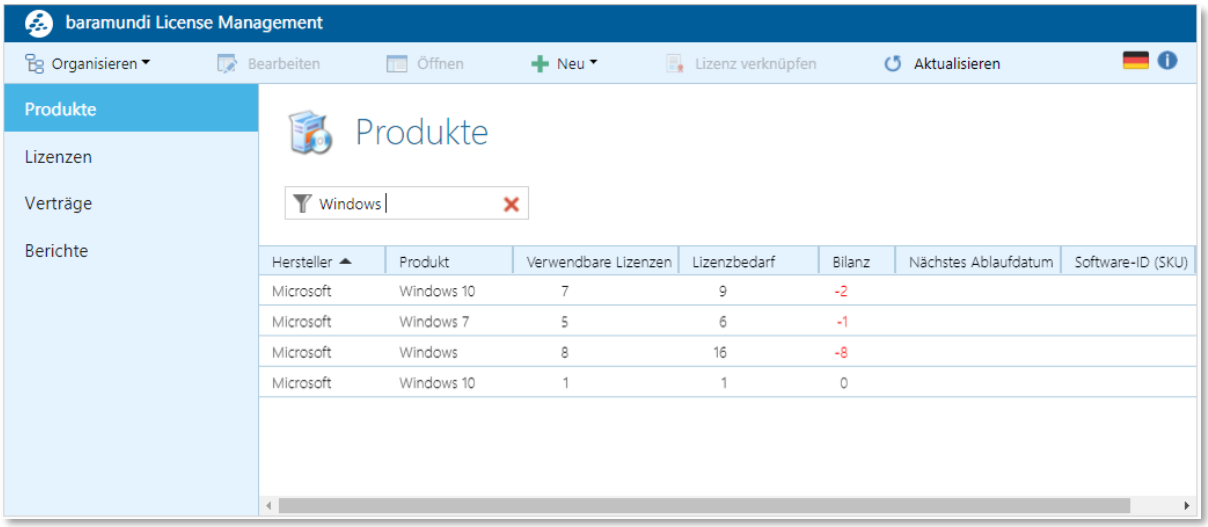


Abbildung 4 – Filter zur Schnellsuche

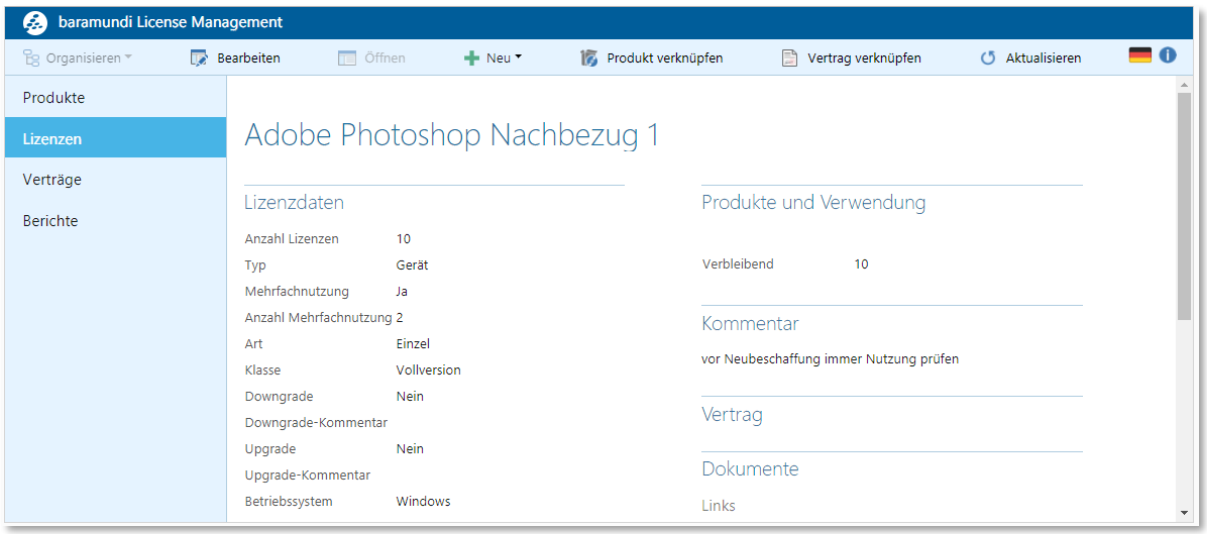


Abbildung 5 – Direktaktionen

7.3.3 Job-Zuweisungsdialog

Der Job-Zuweisungsdialog in der bMC hat eine „Frischzellenkur“ erfahren. Die Ansicht wird an das moderne Layout angepasst, die Performance deutlich verbessert und neue Zuweisungsmöglichkeiten werden hinzugefügt. Somit ist in der bMC ein einheitlicher moderner Dialog für alle Job-Typen umgesetzt.

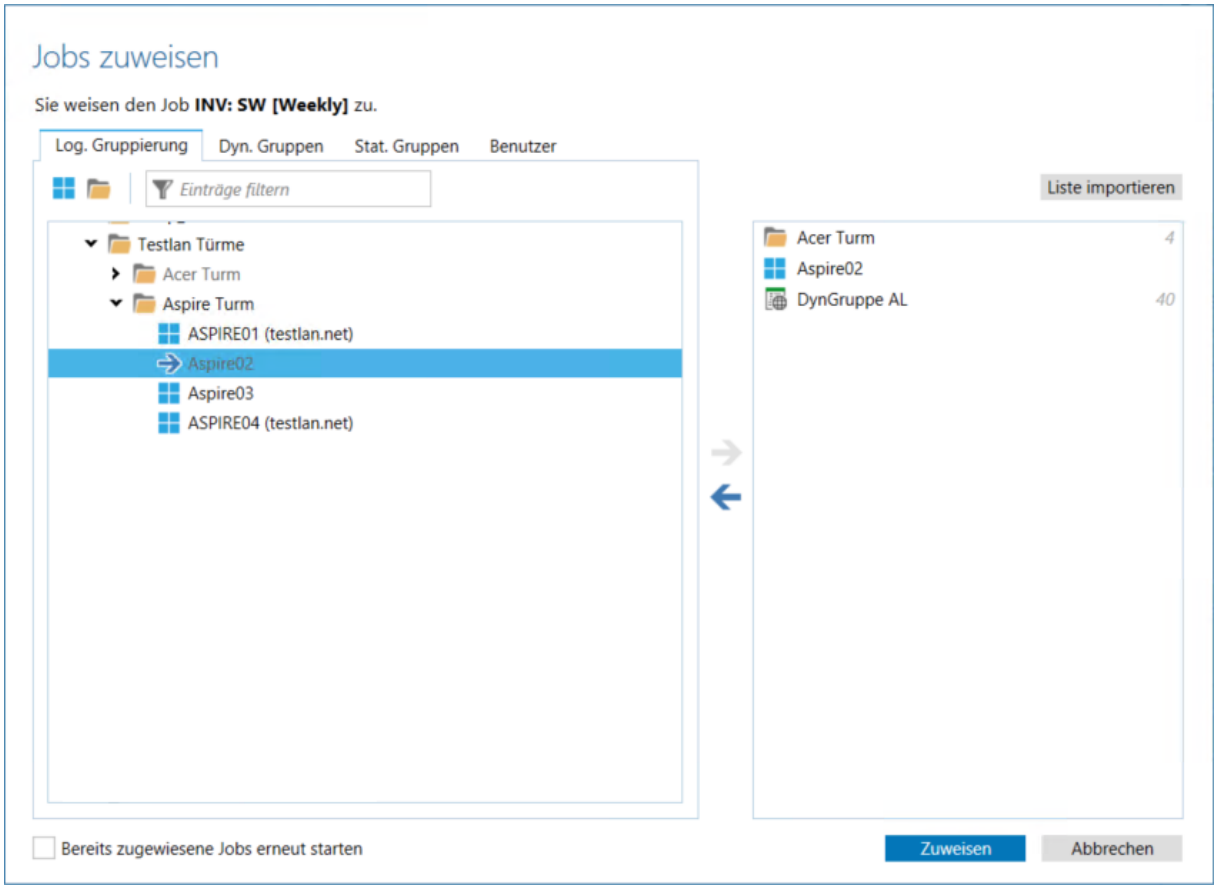


Abbildung 132 - Neuer Job-Zuweisungsdialog

So haben Administratoren nun die Möglichkeit Jobs sowohl an einzelne Endpoints, an logische, (universelle) dynamische oder statische Gruppen, als auch an Benutzer zuzuweisen.

Ferner ist es möglich, eine Liste von Endpoints in den Zuweisungsdialog zu importieren. Oft gibt es in Unternehmen bereits Listen von Endpoints, auf denen bspw. eine bestimmte Software ausgerollt werden soll. Diese bestehenden Listen können nun verwendet werden, um schnell und einfach einen Job auf diese Geräte zuweisen zu können. Eine definierte Listen-Form, sowie aussagekräftige Fehlermeldungen helfen den Administratoren, beim Import der Listen oder bei den Zuweisungen Fehler zu vermeiden.

7.3.4 Managed Software

baramundi Managed Software enthält über 70 Anwendungen und ermöglicht den Administratoren ihre IT-Umgebung auf neue Software-Versionen und Updates zu prüfen und diese zeitnah einzuspielen. Bei der großen Menge an Versionen ist es wichtig, dass Tests und Rollouts effektiv und schnell durchgeführt werden können.
Mit der 2019 R2 wurde die Performance der Ansicht von *bMSW* optimiert und das Setzen von Freigabelevels ist nun deutlich schneller möglich.

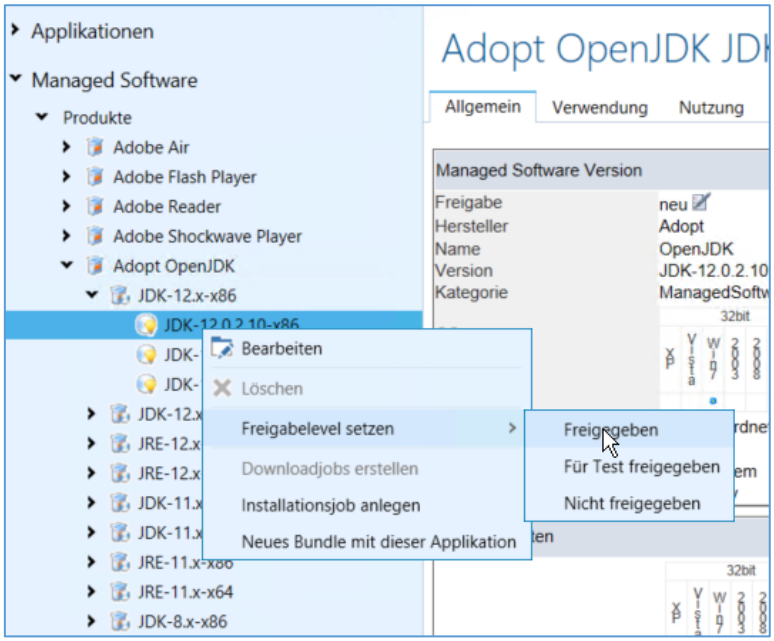


Abbildung 133 - Freigabelevel im Kontextmenü festlegen

Darüber hinaus können nun die benötigten Dateien für eine MSW-Installation schnell und einfach heruntergeladen werden, um Update-Jobs schneller und ohne Fehlermeldung durchführen zu können.

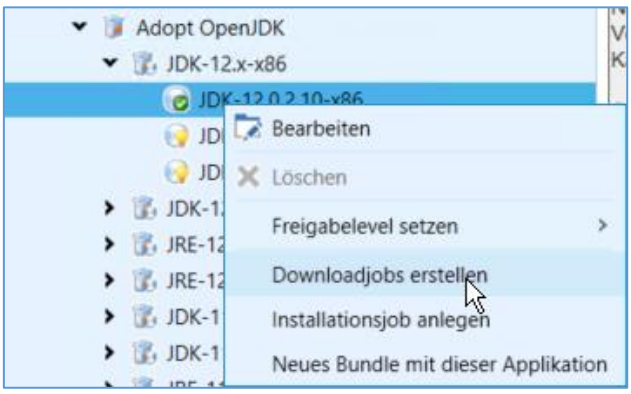


Abbildung 134 - Downloadjobs für fehlende Dateien erstellen

7.3.5 Dokumentation

Die baramundi Management Suite hat in den vergangenen Jahren deutlich an Funktionsumfang gewonnen. All diese alten und neuen Ansichten, Funktionen und Vorgehensweisen waren bisher in der baramundi Online-Hilfe und im Handbuch dokumentiert.
Mit dem Erscheinen der 2019 R2 startet ein neues baramundi Dokumentationsportal: unter docs.baramundi.com werden in Zukunft die Dokumentationsinhalte zusammengefasst angezeigt.

7.3.5.1 3.5.1 Online- und Offline Verfügbarkeit

Ein wichtiger Faktor bei der Dokumentation ist die Verfügbarkeit von Informationen. Wenn Administratoren in der baramundi Management Suite die Taste F1 drücken, werden sie auch in Zukunft auf die entsprechende Hilfe-Seite weitergeleitet. Ab der 2019 R2 erfolgt diese Weiterleitung auf die entsprechende Online-Referenz. So wird auch sichergestellt, dass stets die richtige und aktuelle Dokumentation angezeigt wird.
Es gibt in der bMC aber auch die Möglichkeit, wahlweise auf eine Offline-Variante der Dokumentation zu wechseln, wenn bspw. keine Online-Verfügbarkeit gegeben oder gewünscht ist.

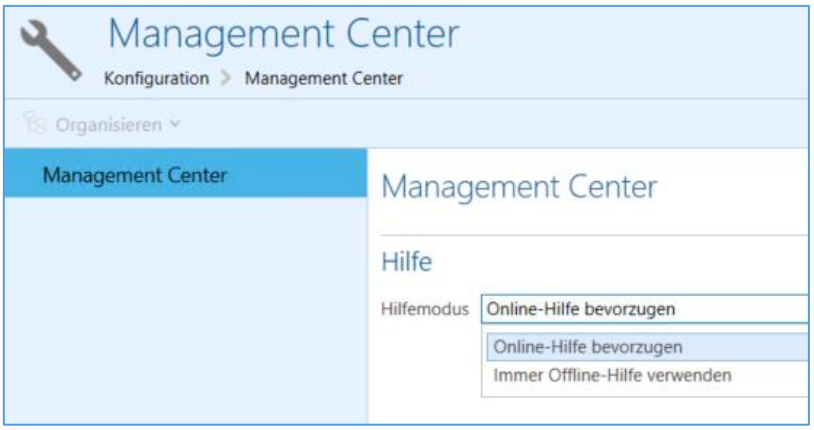


Abbildung 135 - Auswahl zwischen Online- oder Offline-Dokumentation

7.3.5.2 Suchen & Finden

Es ist eine große Herausforderung auf der einen Seite eine möglichst umfassende Dokumentation zu liefern und auf der anderen Seite den Suchenden nicht mit verfügbaren Informationen zu überfrachten. Um dieser Herausforderung gerecht zu werden, nutzt die neue baramundi Dokumentation verschiedene Lösungsansätze.
Zum einen werden die F1 Referenzen - übersichtlich und analog zur Anzeige in der bMC - in der Hauptnavigation „Referenzen“ dargestellt. Das Ziel ist hier schnelle Hilfe zu Menüs und Dialogen in der bMC aufzuzeigen.
Darüber hinaus werden zusammenhängende Inhalte z.B. zum Thema Android Enterprise oder Kiosk in dem Bereich „Themen“ zusammengefasst – an dieser Stelle völlig losgelöst vom Erscheinungsort in der bMC.

Ausführliche Anleitungen zu den wichtigsten Themen findet man dann wiederum im Bereich „Tutorials“ und ersetzen damit das baramundi Handbuch.

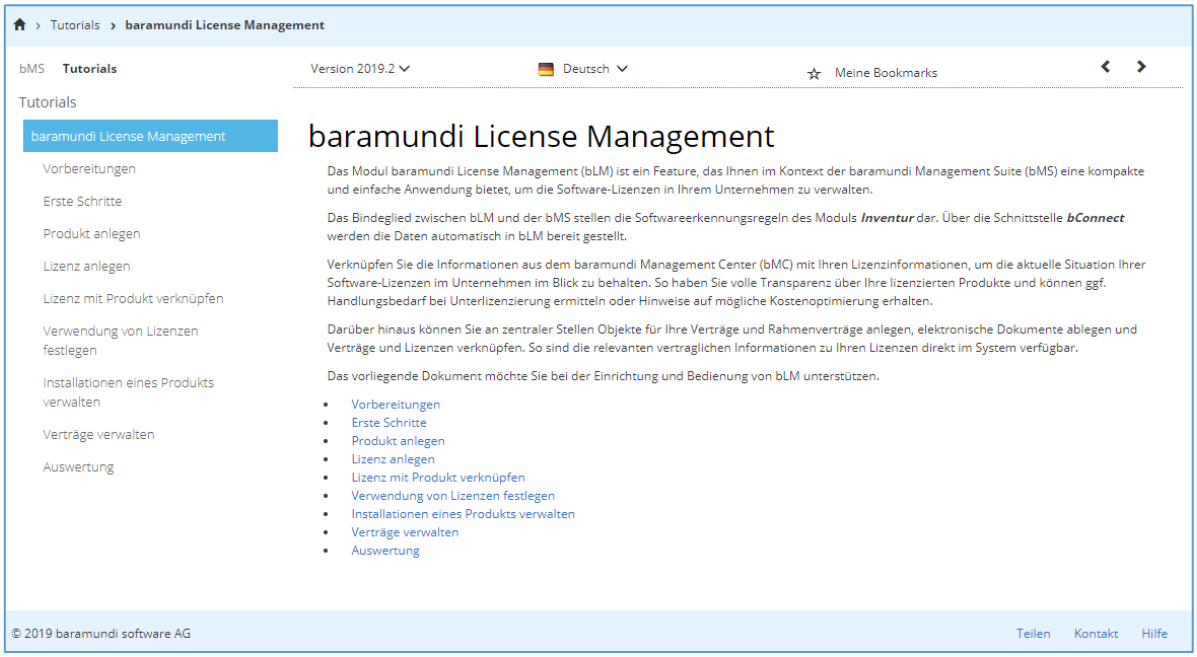


Abbildung 136 – bLM-Tutorial in der neuen Dokumentation

Zum anderen werden die Informationen aber nicht nur in verschiedenen Bereichen gegliedert, sondern eine facettierte Suche rundet die Informationsbereitstellung ab. Wird nach einem bestimmten Suchbegriff gesucht, werden die Suchergebnisse in passende Kriterien gegliedert und können danach gefiltert werden.
So fällt es deutlich leichter, von einer sehr großen Ergebnismenge zu einer kleineren passenden Trefferliste zu gelangen.

Die einzelnen Suchergebnisse können dann wiederum auch in persönlichen Lesezeichen abgelegt und zur späteren Wiederverwendung gespeichert werden.

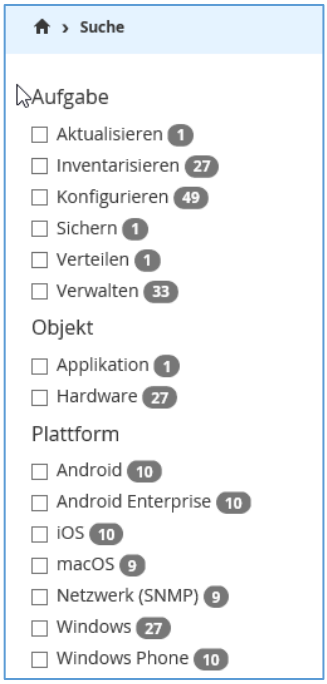


Abbildung 137 - Facettierte Suche

7.3.5.3 Vernetzung mit anderen baramundi Portalen

Neben der Verfügbarkeit, Aktualität und Auffindbarkeit von Dokumentationsinhalten ist es ebenso wichtig, dass Inhalte aus anderen Quellen damit vernetzt sind. Sucht beispielsweise ein Administrator Informationen zur Konfiguration des Kiosks, findet er diese in der neuen baramundi Dokumentation. Möchte er nun aber wissen, wie man die Sprache des Kiosks umstellt, findet er diese Information in der Knowledge Base oder verwandte Themen im Forum.
In dem neuen baramundi Dokumentationsportal werden an passenden Stellen genau diese Informationen miteinander verlinkt, um sowohl allgemeine, als auch spezifische Fragestellungen beantworten zu können.

7.3.6 Notification Center

Mit der 2019 R2 wird in der bMC ein neues Notification Center eingeführt. In der Vergangenheit wurden wichtige Hinweise beim Start der bMC als Dialog angezeigt. Diese Meldungen sind z.B. Hinweise auf ein abgelaufenes Apple Push Zertifikat, Kommunikationsprobleme mit Apple bei DEP/VPP oder Lizenzwarnungen. Diese und ähnliche Meldungen werden nun gesammelt im neuen Notification Center dargestellt. Über ein Symbol am oberen rechten Fensterrand kann der Administrator so jederzeit wichtige aktuelle, aber auch ältere Hinweismeldungen lesen und darauf reagieren.

Abbildung 138 - Neues Notification Center in der bMC

7.3.7 Sicherheit

Wie bereits mit dem Release der bMS 2019 R1 angekündigt, wird die Abwärtskompatibilität zu alten Agents vor Version 2015 R2 mit dem Release 2019 R2 entfernt.
Um die Kommunikation zwischen Windows Endpoints und baramundi Management Server aufrecht zu erhalten, muss vor dem Update auf bMS 2019 R2 ein aktueller Agent, mindestens jedoch Version 2015 R2, auf allen Windows Endpoints vorhanden sein. Das automatische bMA-Update sollte daher stets aktiv sein. Wir empfehlen dringend Server und Agent in derselben Version zu verwenden und den Kommunikationsmodus auf "Standard (empfohlen)" zu konfigurieren. Nur so wird eine kryptografisch sichere Kommunikation zwischen baramundi Management Agent und baramundi Management Server gewährleistet.

Release 2019 R2 beinhaltet verschiedene sicherheitsrelevante Verbesserungen.
Daher empfehlen wir auch diesmal das zeitnahe Upgrade auf die aktuelle Version.

7.4 Produktverbesserungen im Detail

7.4.1 Allgemein

- Die baramundi Setupdateien wurden weitgehend überarbeitet.

7.4.2 Windows Agent (bMA)

- Die bMA-bServer Kommunikation wurde modernisiert und erfolgt jetzt analog zu IEM Clients per HTTPs. Um eine zeitnahe Jobausführung auch auf Clients, welche die Netzwerkverbindung wechseln, zu gewährleisten ist weiterhin der UDP Kanal vom bServer zum bMA vorhanden.

- Logdateien im Falle von fehlerhaften bDS für Benutzereinstellungen (UBDS) werden jetzt unter `"%LocalAppData%\baramundi\BDS"` abgelegt. In älteren Versionen wurden diese unter `"%ProgramData%\baramundi\BDS"` abgelegt.

- Bugfix: Die Ausführung von Aktionen als LocalSystem ist bei aktiven LSA-Protection-Modus nicht möglich.

7.4.3 Server (bServer)

- Die Zugriffsrechte für den Ordner `"%ProgramData%\baramundi"` wurden eingeschränkt.

- Der Datenbankmanager kann über Parameter gesteuert eine Datenbank aktiv setzen.

- Bugfix: Die automatische Clienterfassung über einen PXE Server ist nicht möglich, wenn auf die neue Lizenzierung umgestellt wurde.

- Bugfix: Der Server und der Datenbankmanager arbeiten nicht auf Systemen mit aktiviertem LSA-Protection-Modus.

7.4.4 Management Center (bMC)

- Neuer Dialog bei der Zuweisung von Jobs an Endgeräte.

- Unter „Konfiguration - Lizenzkonfiguration“ kann die Lizenzkonfiguration für baramundi eingesehen und geändert werden. Diese Daten werden nur angezeigt, wenn auf die neue Lizenzierung umgestellt wurde. Alte Lizenzen sind weiterhin gültig und unter „Konfiguration –Server – Lizenzen“ sichtbar.

- Eine Lizenzaktivierung über Ticket kann unter „Konfiguration – Lizenzkonfiguration - Aktivierung“ mit der Aktion „baramundi Lizenzaktivierungsportal öffnen“ vorgenommen werden.
- Das neue Hilfesystem (Cobrili) kann unter „Konfiguration - Management Center“ konfiguriert werden.
- Logdateien und Fehlerreports werden jetzt im Benutzerverzeichnis `"%LocalAppData%\baramundi\Logs"` gespeichert. In älteren Versionen wurden diese unter `"%ProgramData%\baramundi\Logs"` abgelegt.
- Warnmeldungen werden jetzt nicht beim Start der bMC alsPopup angezeigt, sondern als Benachrichtigung in der bMC.
- Solange es ein `"*"`-Sicherheitsprofil gibt, wird eine Benachrichtigung angezeigt.
- Die unter „Grundeinstellungen – Kommunikation - Management Agent Optionen“ einstellbaren Kommunikationsmodi “Kompatibel zu 2015 R1/2014 R2“ sowie “Kompatibel zu 2014 R1 und älter“ wurden entfernt.
- Unter „Server - Grundeinstellungen - Kommunikation“ kann die Abwärtskompatibilität zu bMAs mit den Versionen 2015R2 bis 2019R1 konfiguriert werden.
- Neues Spezialrecht “Bitlocker“ für Windows Clients.
- Die Datenträgerinformation unter „Windows – Client - Übersicht“ wurden komplett überarbeitet. Neue Daten werden erst nach Update des bMA auf 2019R2 angezeigt.
- Unter „Windows – Client – Übersicht - Systemsicherheit“ wird der TPM Status und TPM Version angezeigt.
- Universelle Gruppen enthalten Abfragemöglichkeiten für Bitlocker, TPM und neue Datenträgerinformationen.
- Die Version der Software wird jetzt in der Ansicht „Software – Übersicht“ unter Abhängigkeiten angezeigt.
- Eine neue Datenbankwartungsaufgabe vom Typ „Softwareerkennungsregeln bereinigen“ entfernt alle automatisch angelegten Regeln, welche auf keinen Clients gefunden wurden. Dadurch kann das Regelwerk für die Softwareinventur verkleinert werden.

- Die Aktion „Datenbankwartungsaufgabe – Revisionslog exportieren“ löscht jetzt nur die exportierten Einträge aus der DB. Die Anzahl zu exportierenden Revisionslogeinträge in DB-Wartungsaufgabe ist konfigurierbar
- baramundi Variablen vom Typ Passwort werden jetzt in der DB verschlüsselt abgelegt.
- Der Typ einer baramundi Variable kann nicht mehr verändert werden.
- Die Aktion „bDX-Export“ wurde um die Option „Automatische Zuweisung Einstellung exportieren“ ergänzt.
- Die Ansichten „Managed Software – Produkte“ wurden komplett überarbeitet und die Performance deutlich verbessert.
- Unter „Software – Managed Software“ wird der Downloadstatus in der bMC angezeigt. Weiterhin kann der Download aus dieser Ansicht angestoßen werden.
- Unter „Software – Managed Software“ kann das Freigabelevel direkt über die Menüleiste gesetzt werden.
- Tabs im Bearbeitungsmodus können mit Ctrl+S gespeichert werden.
- Bugfix: Die Namen von „Persönliche Benachrichtigungen“ wird ab der zweiten Kopie falsch gesetzt.
- Bugfix: Die htmlView zeigt sporadisch eine „Problemlösungsseite von baraNet“ als Fehlerseite.
- Bugfix: Wird in der Ansicht „Gruppe als Tab öffnen – Inventur-Assets-Inhalt“ nach der Spalte Zugewiesen sortiert, wird nur eine SQL Fehlermeldung angezeigt.
- Bugfix: Deaktivierte Clients werden in der Ansicht „MSW-Installiert auf“ nicht richtig angezeigt.
- Bugfix: Ein BDX Container mit Dateien, die Unicodezeichen enthalten wird falsch exportiert und kann nicht mehr importiert werden.
- Bugfix: Die Detailanzeige eines Assets zeigt keine Namen und Kategorie.
- Bugfix: Unter „Patches – Übersicht – Reiter Patches“ funktionieren die Links der Art MS*2019 nicht.

- Bugfix: Die über den Button „Installationsjob anlegen“ erzeugten Jobs verwenden keine Standartwerte für Jobparameter.
- Bugfix: Die über den Button „Deinstallationsjob anlegen“ erzeugten Jobs beinhalten keine sinnvollen Schritte, wenn kein Deinstallationskommando an der Software hinterlegt ist.
- Bugfix: Der Excel-Export kann mit Open Office Programmen nicht verwendet werden.
- Bugfix: Wird einer automatisch erzeugten Softwareerkennungsregel eine Dateiregel hinzugefügt, so wird die Regel nicht als manuell erzeugt gekennzeichnet und beim Import ggf. fehlerhaft ausgewertet.
- Bugfix: Der „Registierte Benutzer“ am Windows-Gerät kann nicht korrekt gesetzt werden, wenn im Active Directory kein UPN hinterlegt ist.
- Bugfix: Bei „Persönliche Benachrichtigung“ wird in der Detailanzeige teilweise eine falsche Zeit angezeigt.
- Bugfix: Wird bei „Persönliche Benachrichtigung“ die Variable `{Notification.EventsWithLinks}` verwendet enthält die automatisch erzeugte Email einen Link, welcher in Outlook nicht geöfnet werden kann.

7.4.5 bConnect

- Die Primäre-IP kann beim Erstellen und Updaten eines Windows-Endpoints über bConnect gesetzt werden.
- "CustomStateType" und "CustomStateText" können beim Updaten eines Windows-Endpoints über bConnect gesetzt werden.
- Bugfix: Das Anlegen von OrgUnits für Apps und Applications läuft auf einen Fehler.
- Bugfix: Das Ändern des Namen von Mobilgeräten und Macs ist nicht möglich.

7.4.6 Mobile Devices

- Bei der Aufnahme von DEP-Geräten können jetzt 6 Setup-Dialoge übersprungen werden.
- Die SSL Zertifikate wurden angepasst um mit iOS13 kompatibel zu sein.

- Neue Restriktionen für iOS13 aufgenommen.
- Bugfix: Die Aktion „Apps – Android Enterprise – Apps aktualisieren“ läuft in bestimmten Konstellationen auf einen „Manged Play Store Apps konnten nicht synchronisiert werden“ Fehler.
- Bugfix: Wird „Enrollment der mobilen Endgeräte über das Gateway“ verwendet, ist eine SCEP Zertifikatsanforderung für iOS nicht möglich.

7.4.7 OS-Install

- Kompabibilität mit Windows 10 Version 1909.
- Windows 10 Master-Images verwenden jetzt standardmäßig die MultiSource-Unattended.xml
- Der unattend.xml Eintrag "install to available Partition" wird jetzt auch bei Server-Betriebssystemen dynamisch gesetzt.
- Wird im Hardwareprofil eine Festplatte aufgenommen, so sind keine „zu ignorierende Partitionstypen“ mehr voreingestellt.

7.4.8 Kiosk

- Bugfix: Geräte-Icons werdem im Internet Explorer falsch skaliert.
- Bugfix: Filter gehen verloren, wenn zur Startseite zurück gewechselt wird.

7.4.9 License Management

- Die Navigation zwischen Lizenzen und Vertrag wurde verbessert.
- Neuer Lizenzknoten zur direkten Verwaltung von Lizenzen unabhängig vom Produkt.
- Kopierfunktionalität für Lizenzen um einen Lizenznachbezug abbilden zu können.
- Eine Suchfunktion über alle Produkte und Verträge wurde implementiert.
- Die Datenschutz Option „Identität der Benutzer der Endgeräte anzeigen“ wird beim Anmelden geprüft.
- Neue Hinweismeldung beim Verlassen der Eingabemaske, wenn nicht gespeichert wurde.

- Die bConnect Adresse kann konfiguriert werden.
- Fehlermeldungen bei fehlerhafter Anmeldung wurden verbessert.
- Die Währung wird jetzt unabhänig von der gewählten Sprache beim Zahlenwert gespeichert. Bei der Migration wird der Wert der Währung nicht gesetzt.

7.4.10 OS-Customization Tool

- Die Logdatei enthält jetzt die Version des OS-Customization Tools.
- Neuer Bereich „Datenschutz“ um den Aktivitätsverlauf, Berechtigungen für Apps, Diagnose und Feedback, Spracherkennung und Zwischenablage voreinstellen zu können.
- Bugfix: Temoräre Mount Ordner werden nicht gelöscht.

8 Anhang

8.1 Glossar

ACPI	Advanced Configuration and Power Interface
AE	Android Enterprise
AMT	Active Management Technologie (Intel vPro)
APN	Access Point Name (Kontext: Mobilfunknetze)
APNS	Apple Push Notification Service
bAPSI	baramundi Push Service Infrastructure
bBT	baramundi Background Transfer
bCenter	baramundi Management Center für iOS (App)
bCM	baramundi Compliance Management
bDS	baramundi Deployment Script
bDX	baramundi Data Exchange
BIOS	Basic Input Output System
Blacklist	Negativliste unerwünschter Apps (siehe 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 für Endpoint
DC	Domain Controller
DEP	Device Enrollment Program (von Apple)
DIP	Distributed Installation Point
Endpoint	Synonym für Client
FDB	Forwarding Database
IEM	Internet-Enabled Endpoint Management (d.h. ohne VPN)
IPv6	Internet Protocol Version 6
JSON	JavaScript Object Notation

GCM	Google Cloud Messaging (Android)
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
TMG	Threat Management Gateway (Microsoft)
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
UI	User Interface (Benutzerschnittstelle)
VM	Virtuelle Maschine
VPN	Virtual Private Network
VPP	Volume Purchase Program (Apple)
Whitelist	Positivliste erlaubter Apps (siehe baramundi Mobile Devices)
WoL	Wake-On-LAN

8.2 Komponenten von Drittherstellern

Informationen zur Lizenzierung von Drittanbietern finden Sie auf dem ISO Image unter:
`..\3rdParty-Licensing\3rdPartyLicenses.pdf`

8.3 Abbildungsverzeichnis

baramundi

baramundi software AG
Forschungsallee 3
86159 Augsburg, Germany

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

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

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

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

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

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

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

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

Empower your IT