1 Systemanforderungen und Kompatibilität

1.1 baramundi Management Server und baramundi PXE Relay

- Unterstützte Plattformen: siehe 1.16 (Spalte bMS)
- .NET 4.7.2 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 dem 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
    - Speicherplatz zur Installation der bMS: mindestens 5 GB
    - Netzwerkkarte: Mindestens 1 Gigabit

1.2 Datenbankanbindung

- Unterstützte Plattformen:
    - SQL Server 2017
    - SQL Server 2016 SP2
    - SQL Server 2014 SP3
    - SQL Server 2012 SP3
      → wird ab Release 2020 R2 nicht mehr unterstützt
    - Oracle 12c R2
    - 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[1].
- Bei Umgebungen bis zu 250 Clients kann die SQL Express Edition verwendet werden.

[1] Eine Liste der am Server genutzten Ports steht im Anhang des Handbuchs zur Verfügung.

- 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.

1.3 baramundi Management Center

- Unterstützte Plattformen für das baramundi Management Center, sowie die Add-Ons Automation Studio, License Management, Remote Control und ImageMount: siehe 1.16 (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%.

1.4 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 10 Images ist das Microsoft ADK in der Version 1903 erforderlich.

1.5 baramundi DIP

- Unterstützte Plattformen: siehe Übersichtstabelle Spalte baraDIP.
- .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.
    - Es wird empfohlen den baraDIP auf HTTPS umzustellen.

1.6 baramundi Gateway

- Unterstützte Plattformen: siehe 1.16 (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

1.7 baramundi Management Agent (Windows)

- Unterstützte Plattformen: siehe 1.16 (Spalte bMA)

1.8 baramundi OS-Install

- Zur Erstellung der Windows PE-Bootimages ist das Microsoft ADK in der Version 1903 erforderlich.
- Das ADK steht in Managed Software zur Verfügung.

1.9 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:
    - Internet Explorer
    - Microsoft Edge
    - Google Chrome
    - Mozilla Firefox

1.10 Networkscanner

- 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 1.16 (Spalte bScan)

1.11 baramundi Kiosk

- Unterstützte Plattformen: siehe 1.16 (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 Internet Explorer
  - Microsoft Edge
  - Google Chrome
  - Mozilla Firefox

1.12 baramundi Management Agent (iOS)

- Unterstützte Plattformen:
  - iOS Version 9 oder neuer
  - iPad OS Version 13

1.13 baramundi Management Agent (Android)

- Unterstützte Plattformen:
  - Android Enterprise 7.0 oder neuer
  - 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

1.14 baramundi Management Agent (Windows-Phone)

- Unterstützte Plattformen:
- Windows Mobile 10[2]
  → **wird ab Release 2020 R1 nicht mehr unterstützt**

1.15 baramundi Management Agent (MacOS)

- Unterstützte Plattformen:
  - macOS 10.15 (Catalina) (64 Bit)
  - 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)

1.16 baramundi Virtual

- Unterstützte Plattformen:
  - VMware vSphere vCenter 6.0, 6.5
  - VMware vSphere Hypervisor 6.0, 6.5
- Auf dem baramundi Server werden Komponenten benötigt:
  - Powershell in der Version 4 oder 5 oder 5.1
  - VMware PowerCLI 6.5 Release 1

[2] Vgl.: https://support.microsoft.com/de-de/lifecycle/search?alpha=Windows%2010%20Mobile

1.17 Unterstützte Betriebssysteme

- 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

Plattformbezeichner	**bMS/R**	**bMC**	**bAS**	**bGW**	**bDIP**	**bMA**	**bND**
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 Server 2012 R2 Standard/Datacenter (Server mit grafischer Benutzeroberfläche)	X	X	X	X	X	X	X
Windows Server 2012 Standard/Datacenter (Server mit grafischer Benutzeroberfläche)	X	X	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 2019 LTSC (32 Bit und 64 Bit)		X	X		X	X	X
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

1.18 Eingeschränkt unterstützte Betriebssysteme

	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows Server 2008 R2 SP2 Standard/Enterprise/Datacenter	(E3)	(E3)	(E3)	(E3)	(E3)	(E3)	(E3)
Windows 7 SP1 Professional/Enterprise/Ultimate (N) (32 Bit und 64 Bit)		(E3)	(E3)		(E3)	(E3)	(E3)
Windows Server 2008 SP2 Standard / Enterprise / Datacenter (32 Bit / 64 Bit)			(E1)			(E1)	(E1)
Windows 10 Pro / Enterprise 1703 und älter (N) (32 Bit und 64 Bit)			(E1)			(E1)	(E1)
Windows 8.1 Pro / Enterprise (32 Bit / 64 Bit)		(E1)	(E1)		(E1)	(E1)	(E1)
Windows Vista SP2 (32 Bit / 64 Bit)			(E1)			(E1)	(E1)
Windows XP SP3 (32 Bit)			(E1)			(E1) (E2)	

(E1): Wird nur noch eingeschränkt unterstützt, da Microsoft den grundlegenden Produkt-Support beendet hat.

(E2): Keine Unterstützung für TLS/https Zugriff per bBT auf den baraDIP.

(E3): Wird nur noch eingeschränkt unterstützt, da Microsoft den grundlegenden Produkt-Support im Januar 2020 beenden wird.

Hinweis: Windows Server 2008 wird ab bMS Release 2020 R1 nicht mehr unterstützt.

1.19 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

2 Bekannte Einschränkungen

2.1 Allgemein

- **Hinweis: Die kommende bMS Version 2020 R1 kann mit bMA älter Version 2019 R2 nicht mehr kommunizieren.**
- **Hinweis: Der Download von Managed Software (MSW) ist ab März 2020 nur mit einer bMS 2019R1 oder höher möglich.**
- Die bMA-Version muss der Server-Version entsprechen.
- Bei Änderung des Default Webserver Port für den baramundi Server ist OS-Install und OS-Cloning, sowie Imaging nicht mehr möglich.

2.2 Inventur 2016

- Nach der Umstellung muss der bServer neu gestartet werden und die bMCs müssen alle komplett geschlossen werden. Wird die bMC nur abgemeldet, so werden die neuen Inventurknoten nicht angezeigt.
- Die optionale Offline-Inventur verwendet kein PreInvent.bds und unterstützt damit MSW nicht komplett.

2.3 Server (bServer)

- 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.

- Dateien aus noch vorhandenen Downloadjobs für „PCI device database“ werden nach Invalid verschoben. Dieser Downloadjob ist nicht mehr notwendig und kann gelöscht werden.

- 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.

2.4 PXE-Boot

- Es ist das von baramundi empfohlene ADK zu verwenden.

- Es müssen neue Windows PE Images erstellt werden. Grund sind größere Änderungen am bMA welche einen Dateiaustausch im PE Image notwendig machen.

- 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/5706.

2.5 Windows Agent (bMA)

- Hinweis: Backupdateien welche mit Disaster Recovery einer bMS 8.5 oder älter erstellt wurden, können ab Version 2020 R1 nicht mehr zurückgespielt werden.

- 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.

2.6 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"

2.7 License Management

- Eine Umstellung auf die neue baramundi Lizenzierung (Wibu) ist notwendig um dieses Modul nutzen zu können. Bei neu erstellten Datenbanken erfolgt dies automatisch.

2.8 Mobile Devices

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

2.9 Mobile Devices – Android Enterprise

- Ab Android 10 ist keine Inventur und keine Deinstallation von Wifis möglich, wenn der Standortzugriff für das Gerät bzw. das Arbeitsprofil deaktiviert ist.
- Ab Android 9 ist keine Installation und keine Deinstallation von Wifis möglich, wenn der Endanwender des Gerätes dem baramundi EMM Agent das Recht zur WLAN-Steuerung entzogen hat.
- 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.
- Die Webseite von Google zur Verknüpfung des Unternehmens kann unter Microsoft Edge nicht korrekt verwendet werden.
- 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.

2.10 Mobile Devices – Android

- 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.

- Bei der Root-Zertifikatsinstallation auf HTC Geräten wird dem Client ein Dialog zur Eingabe eines Namens des Zertifikates angezeigt. Um die Zertifikatsinstallation erfolgreich abzuschließen, ist die manuelle Eingabe eines Zertifikatnamens notwendig.

- 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.

2.11 Mobile Devices – iOS

- 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.

- Hinweise: 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.

2.12 Mobile Devices – Windows Phone

- **Wird ab Release 2020 R1 nicht mehr unterstützt.**

- Nach der Deinstallation einer App-Blacklist kann ein Neustart des Geräts nötig sein, bevor Apps wieder als aktiviert dargestellt werden.

- Bei der Inventur von alten WP8.1 Apps unter W10 Mobile wird vom Endgerät die falsche Versionsnummer zurückgeliefert.

- Bei einigen Geräten mit Windows Phone 8.1 sollte bei den erweiterten Einstellungen unter WLAN die Option „WLAN bei Bildschirmtimeout aktiviert lassen“ aktiviert werden, damit der native Client die Verbindung zum Management Server aufrechterhalten kann.

- Der native Client lässt sich nur mit einer E-Mail-Adresse enrollen, wenn diese Adresse an einem AD-User hinterlegt ist, ansonsten muss mit den AD-Credentials enrolled werden.

- Ein Windows Phone Gerät wechselt erst auf „verwaltet", wenn es sich das erste Mal erfolgreich nach dem Enrollment beim Server meldet. Standardmäßig erfolgt dies etwa 60 Minuten nach dem Enrollment, kann aber durch einen manuellen „Sync“ ausgelöst werden. Solange der native Agent nicht auf verwaltet wechselt, lässt sich auch der baramundi Agent nicht enrollen. Es wird ein entsprechender Hinweis angezeigt.

- Aufgrund eines Fehlers in Windows Phone ist es dem Endgerät nicht möglich, ein per SCEP verteiltes Client Zertifikat automatisch an einen Exchange Account zu binden. Der Endbenutzer muss das verteilte Zertifikat manuell im Exchange Account auswählen.

- In der Softwareinventur unter Windows Phone 8.1 fehlen bestimmte, nicht deinstallierbare Apps, wie z.B. OneNote oder Office.

- Der Verbindungsaufbau zum AccessPoint über eine EAP TLS Verbindung (mit Client-Zertifikat) schlägt in der aktuellen Version von Windows 10 Mobile fehl.

2.13 Management Center (bMC)

- Das neue Hilfesystem zeigt bei Offline-Verwendung nur eingeschränkte Inhalte.

- Unter „Konfiguration – Lizenzkonfiguration“ wird „keine Daten verfügbar“ angezeigt, wenn nicht auf die neue Lizenzierung umgestellt wurde.

- Eine Umstellung auf die neuen baramundi Lizenzen ist notwendig um baramundi License Management, baramundi Defense Control oder baramundi Mobile Prämium verwenden zu können.

- Es wird eine Warnmeldung angezeigt, wenn das Installationskommando für den Management Agent nicht „ManagementAgent_setup.exe“ enthält.

- Die Möglichkeit „Betriebssysteme – Image anpassen“ um Windows Betriebssystemimages anzupassen ist nur möglich, wenn das „OS Customization Tool“ zur Imageanpassung installiert wurde. Dieses ist über das freie MSW Paket verfügbar.

- 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.

- Die von Microsoft neu eingeführte Bezeichnung „Servicing Channel“ wird bei Dynamischen Gruppen, automatischer Zuweisung und bConnect noch im alten Format („Service Branch“) behandelt.

- Die globalen Einstellungen zur Softwareinventur (Ordner für neu verknüpfte Software/Betriebssysteme und AUT-Aktiv für neue Geräte) können nur nach Umstellung auf die Inventur 2016 gespeichert werden. Der Knopf „Speichern“ bleibt sonst deaktiviert.

- 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 Proxy 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.

- Die html-Softwareansicht an Clients und Gruppen zeigt beim ersten Laden öfters einen Fehler, oder eine leere Seite. (Nur bei Verwendung der Legacy Software-Inventur.)

2.14 macOS-Geräte

- 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.

2.15 Compliance

- In benutzerdefinierten Compliance-bDS-Skripten stehen keine bMS-Variablen zur Verfügung.

- Eine dynamische Gruppe mit einem CVE Filter enthält auch ignorierte Regeln.

- Mit älteren Versionen angelegte dynamische Gruppen für Compliance berücksichtigen das neue Feature „Dateiausnahmen“ nicht korrekt.

- 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.

2.16 bRemote

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

2.17 Patch Management

- 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.

2.18 Virtual

- bVirtual ist nicht kompatibel mit VMware vSphere v6.5 Update 1 oder höher.
- 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.

2.19 OS-Install

- Alte Systeme können ggf. mit ADK 10 nicht gebootet werden. Hierfür kann ein eigenes Bootimage mit Waik 8.1 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.
- Wird ein Windows 10 System mit einem anderen Betriebssystem, wie z.B. Windows 7 neu installiert, bleiben die Werte für Release-ID und Service Branch erhalten.

2.20 OS-Cloning

- OS-Cloning wird für veraltete Betriebssysteme Windows Vista und Windows 2008 nicht mehr korrekt unterstützt.

2.21 Clients im Internet Modus / Dynamischen Modus

- Es ist kein automatisches Agent-Update im Job möglich.
- Nur ausgewählte Jobschritte sind möglich, siehe IEM Handbuch.
- 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.

2.22 Network Devices (bND)

- Das Öffnen der IT-Landkarte kann bei größeren Umgebungen länger dauern. Die bMC wird dadurch nicht dauerhaft blockiert.
- Geräte mit mehr als einer IP-Adresse an einer MAC-Adresse werden u.U. als unabhängige Geräte erkannt und angelegt.
- Die im Visio-Format exportierte IT-Landkarte wird im Visio-Viewer nicht korrekt dargestellt.
- 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.

2.23 Comparex Miss Marple

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