



baramundi Management Suite as a Service

Leitfaden

Inhalt

1	Vorteile	3
1.1	Operative Vorteile.....	3
1.2	Security-Vorteile	3
1.3	Technische Parameter	3
2	Leistungsumfang	4
2.1	Internet-Enabled-Management-Only-Variante.....	5
2.2	VPN-Variante	5
2.3	Funktions-Übersicht.....	6
3	Companion-Applikationen & Limitierung.....	7
3.1	Companion-Applikation	7
3.2	Limitierungen	8
4	VPN	9
4.1	Ports.....	9
4.2	Verschlüsselung.....	9
4.3	Routing.....	9
5	Technische Anforderungen	10

1 Vorteile

Die baramundi Management Suite as a Service ist eine gehostete Lösung der baramundi Management Suite. Diese cloudbasierte Variante ermöglicht Unternehmen, die Verwaltung ihrer Endgeräte effizienter zu gestalten, ohne selbst Server hosten zu müssen. Hier sind die wichtigsten Punkte dazu:

Einfacher Zugriff über den Browser: Die baramundi Management Suite as a Service kann bequem über den Webbrowser aufgerufen werden. Administratoren können von überall aus auf die Endpoints zugreifen und sie verwalten.

Keine eigene Serverinfrastruktur erforderlich: Durch die Nutzung der baramundi Management Suite as a Service entfällt die Notwendigkeit, eigene Server für die Bereitstellung der Suite zu betreiben. Dies reduziert den administrativen Aufwand und die Kosten.

Funktionsumfang: Die baramundi Management Suite as a Service bietet Funktionen der herkömmlichen Suite, einschließlich OS-Installation, AD-Synchronisation und weiteren Features. Je nach Funktionsumfang bedarf es einem Site-to-Site-VPN.

1.1 Operative Vorteile

- schnelle Inbetriebnahme der baramundi Management Suite
- immer aktuelle Version der baramundi Management Suite
- keine Capex-Kosten beim Endkunden oder Partner für Infrastruktur
- monatliche Abrechnung pro Client bedeutet Kostentransparenz

1.2 Security-Vorteile

- Mandantentrennung
- Multi Factor Authentication (MFA)
- Instanzen liegen in einem nach ISO 27001 zertifizierten Rechenzentrum
- Security Operation Center: 24/7-Sicherheitsüberwachung der Server
- Instandhaltung durch baramundi

1.3 Technische Parameter

- 1 – 10 Gbit Bandbreite pro Kunde für nahtlose Anbindung
- 500 GB-schneller Speicherplatz für Deploymentpakete

2 Leistungsumfang

Mit der baramundi Management Suite as a Service wird das komplette Hosting von baramundi übernommen. Es wird kein Server in der eigenen Infrastruktur benötigt, um die Suite zu betreiben. Alle nötigen Dienste werden zur Verfügung gestellt, skaliert und stets up-to-date gehalten.

baramundi Management Server:

Der baramundi Management Server wird auf hoch performanter Hardware zur Verfügung gestellt. Dadurch werden eine optimale Leistung und schnelle Reaktionszeit erzielt.

Gateway-Server:

Der Gateway-Server erhöht die Sicherheit und ermöglicht das Verwalten der Endgeräte im Internet. Dieser steht fertig konfiguriert zur Verfügung.

SQL-Server:

Über die Skalierung und Lizenzierung des SQL-Servers muss man sich keine Gedanken mehr machen. Dieser wird von baramundi gehostet und passend an die Umgebung skaliert. Zusätzlich wird dieser nach höchstem Standard abgesichert, damit alle Daten sicher sind.

Distributed Installation Point:

Der zentrale Speicherort für Skripte, Dateien und Applikationen, die zur Verwaltung der Endpunkte benötigt werden, wird durch die Cloud-Lösung bereitgestellt. Dies erspart die Bereitstellung der erforderlichen Speicherkapazitäten in der lokalen Umgebung.

baramundi Management Center:

Das baramundi Management Center ist das zentrale Werkzeug zur Verwaltung der Endpunkte. Dieses kann direkt über den Browser aufgerufen werden.

baramundi Automation Studio:

Das baramundi Automation Studio ist der beste Assistent, um Prozesse zu automatisieren und sich Zeit im Alltag zu sparen. Um einen Überblick über alle Skripte und deren Funktion zu bekommen, steht das Automation Studio zum Einsehen der bestehenden Skripte auch im Browser zur Verfügung.

2.1 Internet-Enabled-Management-Only-Variante

Diese Variante unserer baramundi Management Suite ist ein umfassendes Werkzeug und bietet folgende Funktionen:

- **Inventory:** eine übersichtliche Zusammenfassung der gesamten Hard- und Software
- **IT-Management:** zentralisierte Lizenzverwaltung, Energiemanagement und Remote-Wartungen auf allen Clients für eine effiziente Verwaltung
- **Softwareverteilung:** zum Automatisieren und Bereitstellen jeglicher Software
- **Security:** schützt Endpunkte umfassend für eine erhöhte IT-Sicherheit, indem Updates für Betriebssystem und Software zentral verwaltet und verteilt sowie Geräte auf Schwachstellen gescannt werden
- **Defense Control:** Verwalten zusätzlicher Sicherheitsmaßnahmen zur Abwehr von Bedrohungen

2.2 VPN-Variante

Diese Variante erweitert die IEM-Only-Variante um folgende Funktionen:

- **Mobile Device Management (MDM):** die Verwaltung mobiler Geräte, einschließlich macOS
- **OS Install:** Installieren und Konfigurieren der Betriebssysteme
- **Remote Control:** Fernwartung für Windows Geräte

2.3 Funktions-Übersicht

Funktion	Feature	Verfügbarkeit	Modus
Inventory	Network Devices	✓	VPN & IEM
Inventory	Application Usage Tracking	✓	VPN & IEM
Inventory	OT Inventory	✓	VPN & IEM
OS Deployment	OS Install	✓	VPN only
OS Deployment	OS Install Customization	✓	VPN only
OS Deployment	OS Install Boot Media Wizard	✓	VPN only
Softwareverteilung	Deploy	✓	VPN & IEM
Softwareverteilung	Automate	✓	VPN & IEM
MDM	Mobile Devices	✓	VPN & IEM
MDM	Mobile Devices Premium	✓	VPN only
IT Management	Remote Control	✓	VPN
IT Management	Remote Desk	✓	VPN & IEM
IT Management	Energy Management	✓	VPN & IEM
IT Management	License Management	✓	VPN & IEM
Security	Vulnerability Scanner	✓	VPN & IEM
Security	Patch Management	✓	VPN & IEM
Security	MSW	✓	VPN & IEM
Defense Control	Bitlocker Network Unlock	✗*	VPN only
Defense Control	Bitlocker Verwaltung	✓	VPN & IEM
Defense Control	Defender Verwaltung	✓	VPN & IEM
Monitoring	Anbindung des Argus Cockpits	✓	VPN & IEM
ITSM	Ticketing System	✓*	VPN & IEM
Misc	baramundi Benutzerberechtigungen	✓*	VPN & IEM
Misc	AD-Synchronisation	✓	VPN only
Misc	Management Agent Windows Kiosk	✗	VPN only

 Vollständig verfügbar
  per Companion Applikation
  nicht verfügbar
  eingeschränkt

*Auf Anfrage verfügbar.

3 Companion-Applikationen & Limitierung

3.1 Companion-Applikation

Companion-Applikationen sind Anwendungen innerhalb unserer Suite. Einige dieser Anwendungen benötigen einen direkten Zugriff auf die baramundi-Infrastruktur, weshalb diese nicht in der IEM-Variante, sondern nur in der VPN-Variante zur Verfügung stehen. Zusätzlich haben einige Companion-Applikationen die Anforderung, in den Modulen administrativ auf dem baramundi-Server selbst ausgeführt zu werden. In diesem Fall bietet baramundi dies als zusätzlichen Service an.

Companion-Applikation	Internet Enabled Mangement	VPN
Management Agent (Windows)	Fat-Client	Fat-Client
Management Center	Webbrowser	Webbrowser Fat-Client
Application Wizard	Webbrowser ¹	Webbrowser ¹ Fat-Client
Automation Studio	Webbrowser (lesend) Fat-Client	Webbrowser (lesend) Fat-Client
OS Customization Wizard	[nicht anwendbar]	(Optional) Service durch baramundi Fat-Client
Boot Media Wizard	[nicht anwendbar]	1x Anfrage pro Monat als Service durch baramundi kostenfrei
Relay-Server	[nicht anwendbar]	Fat-Client

¹ – Nur für Setuptypen mit Parametern (z.B. MSI)

„Service durch baramundi“ bedeutet, dass nach Erstellung eines Tickets unter supportbMSaaS@baramundi.com ein Termin mit baramundi vereinbart wird. In diesem Termin werden gemeinsam die Anpassungen mit einem erfahrenen baramundi-Spezialisten vorgenommen.

3.2 Limitierungen

OS Install:

Das **OS Customization Tool** kann nach einer Installation des baramundi Management Centers auf einem lokalen Endgerät ausgeführt werden. Der **OS Install Boot Media Wizard** kann nur durch baramundi ausgeführt werden. Die benötigten Treiber können auf dem **Distributed Installation Point** abgelegt werden und anschließend mit Hilfe eines Supporttickets von baramundi eingebunden werden.

Softwareverteilung:

Das **baramundi Automation Studio** steht im Browser zur Ansicht von Skripten zur Verfügung. Für das Bearbeiten und Testen von Skripten muss dieses auf einem Client installiert werden.

MDM:

Die Nutzung von MDM ist in beiden Varianten möglich unterscheidet sich jedoch folgendermaßen:

MDM benötigt einen VPN, wenn die Nutzung der Enrollment Programme von Apple und Android, DEP und Zero Touch, benötigt werden, da hier eine Authentifizierung auf Benutzerbasis stattfindet, welche durch einen AD Sync in der baramundi Management Suite hinterlegt werden müssen.

Die Nutzung der "normalen" Verwaltung durch die Installation des Agenten aus dem App/Play Store und das Enrollment mit Token/QR ist ohne VPN möglich.

Security:

Die Funktion **Bitlocker Network Unlock** kann standardmäßig nicht mit der baramundi Management Suite aus der Cloud genutzt werden. Dieses Feature kann auf Anfrage umgesetzt werden.

Misc:

Die **baramundi Benutzerberechtigungen** zum Anpassen der Berechtigungen innerhalb des baramundi Management Centers können einmal pro Monat kostenfrei durch baramundi angepasst werden.

Der **baramundi Management Agent Windows Kiosk** kann nur über die Clientauthentifizierung genutzt werden. Das Anmelden mit einem Benutzer ist nicht möglich.

Benutzerverwaltung: Das Anlegen neuer Benutzer ist auf Anfrage über das Ticketsystem möglich.

File Upload: Die Weboberfläche ermöglicht das Hochladen von Dateien bis 2 GB Größe. In der VPN-Variante können über SMB größere Files hochgeladen werden.

4 VPN

Für die Advance- und Premium-Edition ist die Einrichtung eines VPN notwendig. Mit einem IPsec-IKEv2-VPN bietet baramundi eine sichere Möglichkeit, Daten zwischen Unternehmen und der baramundi Management Suite as a Service auszutauschen. Da es sich hierbei um eine Site-to-Site-Verbindung handelt, besteht die Möglichkeit, die Verbindung jederzeit zu trennen und neu zu initialisieren. Die Verbindung benötigt kein NAT, daher können die Netze direkt über die VPN-Verbindung geroutet und IPs direkt angesprochen werden.

IPsec ermöglicht eine sichere Übertragung von Informationen in IP-basierten Datennetzwerken, wobei insbesondere die Vertraulichkeit, die Integrität und die Authentizität der mittels des IP-Protokolls übertragenen Informationen gewährleistet werden können.

4.1 Ports

Der VPN selbst verwendet folgende Ports:

UDP 500 und 4500

Innerhalb des VPN müssen alle Ports, die die baramundi Management Suite im internen Netzwerk verwendet, freigegeben sein. Eine Übersicht hierzu kann in unserer Online-Dokumentation eingesehen werden: [baramundi Management Suite \(baramundi.com\)](https://baramundi.com)

4.2 Verschlüsselung

Zur Verschlüsselung und Authentifizierung der Verbindung wird ein Pre-Shared-Key verwendet. Die Verschlüsselungsmethoden orientieren sich an der Empfehlung des BSI in der Technischen Richtlinie TR-02102-3 (Version 2023-01).

4.3 Routing

Damit die Clients mit der baramundi Management Suite kommunizieren können, muss die interne IP des baramundi Management Servers über den VPN geroutet werden. Hier muss sichergestellt werden, dass alle Netze, die verwaltete Clients enthalten, eine passende Route über die VPN-Verbindung, kennen.

Das Routing vom baramundi Management Server in die Client-Netze übernimmt baramundi. Dafür müssen alle bestehenden Netze sowie zukünftig neu hinzugefügte Netze an den Ansprechpartner weitergegeben werden.

5 Technische Anforderungen

Netzwerk- und Internetkonnektivität

- min. 250 Mbit empfohlen, 500 Mbit Internetanbindung
- Für die Advance- und Premium-Variante ist die Einrichtung eines VPN notwendig. Dafür ist ein IPsec-IKEv2-VPN-fähiges Gateway und deaktiviertes NAT nötig.
- direkter HTML-5-fähiger Browser auf einem PC (keine mobilen Browser)
- unterstützt: Edge, Chrome, Firefox

Ports

- TCP 443 (unter Verwendung von VPN: UDP 500 und 4500)
- Innerhalb des VPN müssen alle Ports, die die Suite im internen Netzwerk verwendet, freigegeben sein. Beachten Sie hierzu die Vorgaben in den Systemanforderungen, einsehbar auf unserer Homepage (<https://www.baramundi.com/sys-req-de>).

Verschlüsselung

- Zur Verschlüsselung und Authentifizierung der Verbindung wird ein Pre-Shared-Key verwendet. Die Verschlüsselungsmethoden orientieren sich an der Empfehlung des BSI in der Technischen Richtlinie TR-02102-3 (Version 2023-01).

Routing

- Damit die Clients mit der Suite kommunizieren können, muss die interne IP des baramundi Management Servers über das VPN geroutet werden und alle Netze, die verwaltete Clients enthalten, eine geeignete Route über die VPN-Verbindung kennen.
- Das Routing des baramundi Management Server in Ihr Netz übernimmt baramundi. Dafür müssen alle Netze (bestehend wie neu hinzugefügte) an Ihren Kontakt gemeldet werden.

Berechtigungen

- Für die initiale Installation einiger Companion-Applikationen (bspw. Dem baramundi Management Agent (Windows)) ist ein administrativer Account erforderlich.
- Für die automatisierte Verteilung des baramundi Management Agents muss im baramundi Management Center ein Domain-Account eingetragen werden, welcher auf den Endpunkten lokale administrative Rechte hat, um Software zu installieren.

DHCP

- Für die Bereitstellung von Windows PE Images über PXE ist es in der VPN-Variante erforderlich, DHCP-Optionen in der Range der Endgeräte zu konfigurieren.

**We are looking forward
to meeting you!**

Get in touch!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

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

 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

 +43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com