



baramundi Management Suite as a Service

Guida

Indice

1	Vantaggi.....	3
1.1	Vantaggi operativi.....	3
1.2	Vantaggi di sicurezza	3
1.3	Parametri tecnici.....	3
2	Ambito di applicazione	4
2.1	Variante “Internet Enabled Management Only”:	5
2.2	Variante con VPN.....	5
2.3	Panoramica delle funzionalità	6
3	Applicazioni ausiliarie e limitazioni.....	7
3.1	Applicazioni ausiliarie.....	7
3.2	Limitazioni	8
4	VPN	9
4.1	Porte.....	9
4.2	Crittografia.....	9
4.3	Instradamento	9
5	Requisiti tecnici	10

1 Vantaggi

La baramundi Management Suite as a Service è una soluzione ospitata dalla Management Suite di baramundi. Questa variante basata su cloud consente alle aziende di gestire i propri dispositivi in modo più efficiente, senza dover ospitare server autonomamente. Ecco i punti salienti della baramundi Management Suite as a Service:

Accesso facile tramite browser: la baramundi Management Suite as a Service è comodamente accessibile tramite browser web. Gli amministratori possono accedere agli endpoint e gestirli da qualsiasi luogo.

Nessuna infrastruttura server propria necessaria: utilizzando la baramundi Management Suite as a Service, non è necessario gestire server propri per fornire la Management Suite. Questo riduce il carico amministrativo e i costi.

Gamma completa di funzioni: la baramundi Management Suite as a Service offre le stesse funzionalità della Suite tradizionale, inclusa l'installazione del sistema operativo, la sincronizzazione con Active Directory e altre funzioni. Per usufruire dell'intera gamma di funzionalità, è necessaria la connessione tramite VPN site-to-site.

1.1 Vantaggi operativi

- Messa in servizio rapida della baramundi Management Suite
- Sempre aggiornata all'ultima versione della baramundi Management Suite
- Nessun costo di investimento per il cliente finale o il partner relativo all'infrastruttura
- Fatturazione mensile per client, per una maggiore trasparenza dei costi

1.2 Vantaggi di sicurezza

- Separazione tra i client
- Autenticazione a più fattori (MFA)
- Le istanze sono ospitate in un data center certificato ISO 27001
- Security Operation Center con monitoraggio della sicurezza dei server 24/7
- Manutenzione a cura di baramundi

1.3 Parametri tecnici

- Larghezza di banda da 1 a 10 Gbit per cliente
- 500 GB di storage veloce per i pacchetti di distribuzione

2 Ambito di applicazione

Con la baramundi Management Suite as a Service, baramundi si occupa interamente dell'hosting. Non è necessario alcun server nella propria infrastruttura per utilizzare la baramundi Management Suite. Tutti i servizi necessari vengono forniti, scalati e costantemente aggiornati.

baramundi Management Server:

Il baramundi Management Server è disponibile su un server ad alte prestazioni. Ciò garantisce performance ottimali e tempi di risposta rapidi.

Gateway-Server:

Il gateway server aumenta la sicurezza e consente la gestione dei dispositivi finali tramite Internet. Viene fornito completamente configurato.

SQL-Server:

Non è più necessario preoccuparsi della scalabilità e della licenza del server SQL. Questo è ospitato da baramundi e scalato in base all'ambiente. Inoltre, è protetto secondo i più alti standard per garantire la sicurezza dei dati.

Punto di installazione distribuito:

Il punto di installazione distribuito è la posizione centrale di archiviazione per script, file e applicazioni necessari alla gestione degli endpoint. Questa soluzione cloud elimina la necessità di fornire capacità di archiviazione locale.

baramundi Management Center:

Il baramundi Management Center è lo strumento centrale per la gestione degli endpoint. È accessibile direttamente tramite browser.

baramundi Automation Studio:

Il baramundi Automation Studio è il miglior assistente per l'automazione dei processi e per risparmiare tempo nelle attività quotidiane. Per avere una panoramica di tutti gli script e delle loro funzioni, l'Automation Studio è disponibile anch'esso via browser per consultare gli script esistenti.

2.1 Variante “Internet Enabled Management Only”

Questa versione della baramundi Management Suite è uno strumento completo che offre le seguenti funzionalità:

- **Inventario:** una panoramica completa di tutta l'attrezzatura hardware e software.
- **Gestione IT:** gestione centralizzata delle licenze, gestione energetica e manutenzione remota di tutti i client per un'amministrazione efficiente.
- **Distribuzione del software:** per automatizzare e distribuire qualsiasi tipo di software.
- **Sicurezza:** protezione completa degli endpoint per una maggiore sicurezza IT, grazie alla gestione e distribuzione centralizzata degli aggiornamenti di sistema operativo e software, e alla scansione dei dispositivi per individuare vulnerabilità.
- **Defense Control:** gestione di misure di sicurezza aggiuntive per contrastare le minacce.

2.2 Variante con VPN

Questa variante estende le funzionalità della versione Internet Enabled Management Only aggiungendo i seguenti strumenti:

- **Mobile Device Management (MDM):** gestione dei dispositivi mobili, inclusi quelli con sistema operativo macOS.
- **OS Install:** installazione e configurazione del sistema operativo.
- **Remote Control:** manutenzione da remoto per dispositivi Windows.

2.3 Panoramica delle funzionalità

Attività	Funzionalità	Disponibilità	Modalità
Inventario	Network Devices		VPN & IEM
Inventario	Application Usage Tracking		VPN & IEM
Inventario	Inventario OT		VPN & IEM
Installazione OS	OS-Install		Solo VPN
Installazione OS	OS Install Customization		Solo VPN
Installazione OS	OS Install Boot Media Wizard		Solo VPN
Distribuzione del software	Deploy		VPN & IEM
Distribuzione del software	Automate		VPN & IEM
MDM	Dispositivi mobili		VPN & IEM
MDM	Mobile Devices Premium		VPN
Gestione IT	Remote Control		VPN
Gestione IT	Remote Desk		VPN & IEM
Gestione IT	Energy Management		VPN & IEM
Gestione IT	License Management		VPN & IEM
Sicurezza	Vulnerability Scanner		VPN & IEM
Sicurezza	Patch Management		VPN & IEM
Sicurezza	MSW		VPN & IEM
Defense Control	Bitlocker Network Unlock	 *	Solo VPN
Defense Control	Bitlocker Management		VPN & IEM
Defense Control	Defender Management		VPN & IEM
Monitoraggio	Connessione ad Argus Cockpit		VPN & IEM
ITSM	Sistema di ticketing	 *	VPN & IEM
Varie	baramundi User Permissions	 *	VPN & IEM
Varie	Sincronizzazione con Active Directory		Solo VPN
Varie	Management Agent Windows Kiosk		Solo VPN

 completamente supportato  tramite applicazione ausiliaria  non disponibile  limitazione

*Disponibile su richiesta.

3 Applicazioni ausiliarie e limitazioni

3.1 Applicazioni ausiliarie

Le applicazioni ausiliarie sono strumenti che fanno parte dei moduli baramundi e servono per utilizzarli o integrarli. Alcune di queste applicazioni richiedono accesso diretto all'infrastruttura baramundi, motivo per cui non sono disponibili nella versione IEM, ma solo nella versione VPN. Inoltre, alcune applicazioni ausiliarie devono essere eseguite con privilegi amministrativi direttamente sui moduli presenti nel server baramundi. In questi casi, baramundi offre l'uso dell'applicazione come servizio.

Applicazione ausiliaria	Internet Enabled Endpoint	VPN
Management Agent (Windows)	Fat-Client	Fat-Client
Management Center	Browser web	Browser web Fat-Client
Application Wizard	Browser web ¹	Browser web ¹ Fat-Client
Automation Studio	Browser web (sola lettura) Fat-Client	Browser web (sola lettura) Fat-Client
OS Customization Wizard	[non applicabile]	(opzionale) Servizio offerto da baramundi Fat-Client
Boot Media Wizard	[non applicabile]	1 richiesta gratuita al mese come Servizio offerto da baramundi
Relay-Server	[non applicabile]	Fat-Client

¹ - Solo per tipi di setup con parametri (es. file MSI)

“Servizio offerto da baramundi” significa che, dopo aver creato un ticket all'indirizzo supportbmsaas@baramundi.com, verrà fissato un appuntamento con un esperto baramundi. Durante tale appuntamento, le configurazioni verranno eseguite insieme allo specialista.

3.2 Limitazioni

OS Install:

L'**OS Customization Tool** può essere eseguito localmente dopo l'installazione del baramundi Management Center e dello strumento stesso.

L'**OS Install Boot Media Wizard** può essere eseguito solo da baramundi. I driver necessari possono essere archiviati sul DIP e poi integrati tramite apertura di un ticket.

Distribuzione del software:

Il **baramundi Automation Studio** è accessibile via browser solo per la visualizzazione degli script. Per modificare e testare gli script, è necessario installarlo su un client.

MDM:

L'MDM è disponibile in entrambe le varianti, ma con differenze: le funzionalità di enrollment Apple DEP e Android Zero Touch richiedono una VPN, poiché l'autenticazione utente si basa sulla sincronizzazione con Active Directory, eseguita nel baramundi Management Center. L'uso del "normale" MDM tramite installazione dell'agente da App Store/Play Store e enrollment con token/QR non richiede VPN.

Sicurezza:

La funzione **Bitlocker Network Unlock** non è utilizzabile di default nella versione cloud della baramundi Management Suite. Tuttavia, può essere attivata su richiesta.

Varie:

I **permessi utente baramundi** possono essere modificati nel baramundi Management Center da baramundi una volta al mese gratuitamente.

Il **baramundi Management Agent per Windows Kiosk** può essere utilizzato solo con autenticazione client. Non è possibile accedere con un utente.

Gestione utenti: la creazione di nuovi utenti è possibile su richiesta, tramite il sistema di ticketing.

Caricamento file: l'interfaccia web consente l'upload di file fino a 2 GB. Nella versione VPN, è possibile caricare file di dimensioni superiori tramite protocollo SMB.

4 VPN

Per le edizioni Advance e Premium, è necessario configurare una connessione VPN. Con l'utilizzo di una VPN IPsec-IKEv2, baramundi offre un metodo sicuro per lo scambio di dati tra l'azienda e la baramundi Management Suite as a Service. Trattandosi di una connessione site-to-site, è possibile disconnettere e reinizializzare la connessione in qualsiasi momento. La connessione non richiede NAT, quindi le reti possono essere instradate direttamente tramite la VPN e gli indirizzi IP possono essere raggiunti in modo diretto.

IPsec consente la trasmissione sicura delle informazioni nelle reti dati basate su IP, garantendo riservatezza, integrità e autenticità delle informazioni trasmesse tramite il protocollo IP.

4.1 Porte

La VPN utilizza le seguenti porte:

UDP 500 e 4500

All'interno della VPN, è necessario abilitare tutte le porte utilizzate dalla baramundi Management Suite nella rete interna. Una panoramica completa è disponibile nella documentazione ufficiale: [baramundi Management Suite \(baramundi.com\)](https://baramundi.com/baramundi-management-suite)

4.2 Crittografia

Per crittografare e autenticare la connessione viene utilizzata una chiave precondivisa. I metodi di crittografia adottati si basano sulle raccomandazioni del BSI ([Federal Bureau for Security in Information Technology](https://www.bsi.gov.uk/Pages/Security-in-Information-Technology.aspx)) contenute nella Linea Guida Tecnica TR-02102-3 (Versione 2023-01).

4.3 Instradamento

Affinché i client possano comunicare con la baramundi Management Suite, è necessario che l'IP interno del baramundi Management Server sia instradato tramite la VPN. Deve essere garantito che tutte le reti contenenti client gestiti conoscano una route valida tramite la connessione VPN.

baramundi si occupa del routing dal baramundi Management Server verso le reti client; per farlo, è necessario comunicare a baramundi tutti i network esistenti, così come eventuali nuove reti aggiunte in futuro.

5 Requisiti tecnici

Connettività di rete e internet

- Connessione internet minima: 250 Mbit/s / raccomandata: 500 Mbit/s
- Per le versioni Advance e Premium è necessario configurare una VPN. È richiesto un gateway compatibile con VPN IPsec-IKEv2 e il NAT deve essere disattivato.
- Browser con supporto HTML5 su PC (i browser mobili non sono supportati)
 - Supportati: Edge, Chrome, Firefox

Porte

- TCP 443 (Se si utilizza la VPN: UDP 500 e 4500)
- All'interno della VPN, è necessario abilitare tutte le porte utilizzate dalla bMS nella rete interna. Vedi i requisiti di sistema nella nostra homepage. (<https://www.baramundi.com/sys-req-de>)

Crittografia

- Per crittografare e autenticare la connessione viene utilizzata una chiave precondivisa
- Gli algoritmi di crittografia seguono le raccomandazioni del BSI secondo la Linea Guida Tecnica TR-02102-3 (version 2023-01).

Instradamento

- Affinché i client possano comunicare con la baramundi Management Suite, è necessario che l'IP interno del baramundi Management Server sia instradato tramite la VPN. Deve essere garantito che tutte le reti contenenti client gestiti conoscano una route valida tramite la connessione VPN.
- baramundi gestisce il routing dal baramundi Management Server verso la tua rete; per farlo, è necessario comunicare al proprio referente baramundi tutte le reti esistenti e anche quelle che verranno aggiunte in futuro.

Autorizzazioni

- È richiesto un account amministrativo per l'installazione iniziale di alcune applicazioni ausiliarie, ad esempio il baramundi Management Agent (Windows).
- Per la distribuzione automatica del baramundi Management Agent, è necessario inserire nel baramundi Management Center un account di dominio con diritti amministrativi locali sugli endpoint, al fine di installare il software.

DHCP

- Per fornire immagini Windows PE tramite PXE nella variante VPN, è necessario configurare le opzioni DHCP nell'intervallo di indirizzi dei dispositivi finali.

**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