Information on data security and data protection for baramundi Proactive Hub products and Argus Cockpit

Empower your IT

Dear readers,
When using cloud solutions, the main focus is on protecting the data collected. Strict company guidelines for compliance with cloud governance and legal requirements such as the EU GDPR must be observed when using these solutions. baramundi software GmbH attaches great importance to data security in the development and operation of its cloud solutions and ensures that you are in compliance with the required guidelines. The following document provides answers to the most frequently asked questions that arise in this context and gives an overview of the technologies and security mechanisms used.

Frank Heider
Director Product Development Argus Cloud

Subject to change without notice - DocID: PROACTIVEHUB-250100-INFO-250501-EN

Statements about equipment and technical functionalities are non-binding and are for information purposes only.

1 Contents

2 Infrastructure and service providers

The baramundi cloud applications are operated exclusively via the Microsoft Azure infrastructure. In addition, service providers are used, which are described in more detail below.

2.1 Microsoft Azure

The baramundi Proactive Hub as well as Argus Cockpit is operated in Microsoft Azure and is distributed as follows:

- The baramundi Proactive Hub products as well as Argus Cockpit are hosted in the **Azure Region Western Europe (Netherlands)**. This applies to all customers whose company headquarters are in Europe.
- The baramundi Proactive Hub products as well as Argus Cockpit are hosted in the **Azure Region East US**. This applies to all customers whose company headquarters are in the USA.
- The Azure Active Directory B2C used to register and manage authorized users is provided by Microsoft via globally replicated services

Further information can be found at

Region availability and data residency - Azure AD B2C

2.2 MongoDB Inc.

- The MongoDB Atlas databases used are hosted by MongoDB Inc. in the Azure Region **Western Europe** (Netherlands) for all baramundi Proactive Hub products as well as for Argus Cockpit. This applies to all customers whose company headquarters are in Europe.
- The MongoDB Atlas databases used are hosted by MongoDB Inc. in the Azure region **Azure Region East US** for all baramundi Proactive Hub products as well as for Argus Cockpit. This applies to all customers whose company headquarters are in the USA.

2.3 Rapidmail GmbH

Notifications are sent by email for the baramundi Proactive Hub as well es for Argus Cockpit via the service provider "Rapidmail". Rapidmail's data center is located in Germany.

Further information can be found on:

https://www.rapidmail.com/

2.4 SoftwareONE Germany GmbH

As a cloud service provider, SoftwareONE Deutschland GmbH is responsible for billing baramundi software GmbH for the Microsoft Azure infrastructure.

2.5 Cloudflare Germany GmbH

Cloudflare services such as DDoS protection and web application firewall are used to protect the baramundi Proactive Hub infrastructure as well as Argus Cockpit from various types of attacks to improve application security.

2.6 Hetzner Online GmbH

A customized configuration package is required for the commissioning of Argus Cockpit. These packages are made available via a password-protected download service from Hetzner with customized downloads

2.7 MicroNova AG

Site24x7 ManageEngine is used to monitor and provide a website for availability control of the baramundi Proactive Hub as well as for Argus Cockpit, represented by MicroNova AG in Germany.

3 Data processing and data security

3.1 Microsoft Azure Infrastructure and resources

3.1.1 Data retention

The **Azure AD** B2C monitoring log records the service and user logins for up to 7 days.

The *Log Analytics Workspaces* from Microsoft Azure have the option *Data Retention*, which sets the duration of data retention. This setting is set to the minimum duration of **90 days** . In addition, the maximum amount of recorded data can be limited via the Daily cap option. This limit is currently **2.0 GB per day**.

3.1.2 Access authorization

3.1.2.1 Microsoft

Both the console output at runtime and the recorded log and monitoring data of the Azure environment can only be viewed **by authorized administrators of baramundi software GmbH**. If necessary, the recorded log and monitoring data can also be viewed by development and support staff in collaboration with the authorized administrators to analyze application errors. With the Customer Logbox, Microsoft employees have no access to data within the Azure resources without the consent of our responsible IT administrators at baramundi. The available accounts within the Microsoft Azure infrastructure are configured to have only the minimum necessary rights (Azure RBAC). Privileged administrative rights can only be obtained via the Azure AD PIM used

3.1.2.2 SoftwareONE

SoftwareONE has limited access to the resources of the Azure infrastructure in the course of cost monitoring and cost reporting. In the case of support, approval from the baramundi software GmbH administrators is required for more extensive rights.

Further information can be found at:
Azure Role-Based Access Control (RBAC)
What is Privileged Identity Management?

3.1.3 Data protection declarations of the baramundi Proactive Hub products and Argus Cockpit

- Privacy Policy baramundi perform2work: *baramundi perform2work*
- Privacy policy Argus Cockpit: *Argus Cockpit*

3.2 MongoDB Atlas database

3.2.1 Data retention

MongoDB Atlas stores the logs and system event messages of the last **30 days** for each rank in a cluster. The Performance Advisor logs are kept for a maximum of **7 days** for each cluster.

Further information can be found at:
View and Download MongoDB Logs

3.2.2 Access authorization

The recorded log and monitoring data can **only** be viewed **by authorized administrators of baramundi software GmbH**. If necessary, the recorded log and monitoring data can also be viewed by development and support staff in collaboration with the authorized administrators to analyze application errors. Access to customer data within the MongoDB Atlas databases used by MongoDB employees can only take place with the consent of our responsible administrators.

3.2.3 Data storage

The application data of the baramundi Proactive Hub products as well as Argus Cockpit are stored in an Azure storage with running MongoDB Atlas with **256-bit AES** encryption. **FIPS 140-2** compliance is ensured both by MongoDB Atlas and by Microsoft Azure in the Western Europe region. The keys used are managed by Platform Managed Keys (PMKs) in **Azure Key Vault.**

Further information can be found on:
Key Vault | Microsoft Azure
Storage Engine and Cloud Backup Encryption - MongoDB Atlas

3.2.4 Database backups

Database backups are created at various time intervals to ensure that data can be restored quickly in an emergency. The maximum retention period for database backups is **4 weeks.** Backups are stored and secured both in Azure storage and in a dedicated infrastructure at baramundi with 256-bit AES encryption. The backups are stored on tape for a maximum of **12 months**.

Further information can be found on:
Storage Engine and Cloud Backup Encryption - MongoDB Atlas

3.3 Rapidmail Germany by module

3.3.1 Data retention

The e- mails sent are logged as part of the emailing process. Logging is limited to 500 emails. As part of this logging, all information related to the sending of an email is recorded, including the recipient's email address. Personal data is deleted in accordance with EU GDPR regulations and in a timely manner.

Further information can be found at:
Privacy policy - Rapidmail

3.3.2 Access authorization

Both Rapidmail as the service provider for sending emails and the administrators of baramundi software GmbH have access to these logs.

3.4 Data acquisition by products and modules

Below you can find out which data is recorded and transferred by the respective baramundi Proactive Hub products and Argus Cockpit.

3.4.1 baramundi perform2work

Data is transmitted to baramundi perform2work via the baramundi Proactive Hub Agent installed on the end user devices. Only authenticated and authorized clients can establish a connection to the baramundi Proactive Hub and its corresponding products.

3.4.1.1 Typical purposes

The data is required to be able to assign the results of critical anomalies in the IT environments to the corresponding end devices and initiate appropriate solutions in a targeted manner by the IT manager. Machine learning algorithms and artificial intelligence can then derive predictions about the stability, performance and connectivity of the IT environment from this – anonymized – database. This makes it easier for IT managers to promote end user satisfaction in the long term.

3.4.2 Argus Cockpit

Data is transferred from the baramundi Management Suite to Argus Cockpit via Cloud Connectors. These are Windows services that read relevant data from the baramundi Management Suite via baramundi bConnect and transfer it to the cloud in an authorized and authenticated manner.

3.4.2.1 Typical purposes

The transmitted data is required to record the overall status of the environment managed by the baramundi Management Suite. By configuring universal dynamic groups, it is possible to determine individually for each environment which data should be evaluated. This enables the IT admin or other roles in the company to identify anomalies in the IT environment.

3.5 Encryption

All components and end devices communicate asymmetrically encrypted via **TLS 1.2 or TLS 1.3** on all communication channels. The SSL certificates used comply with current security standards and use the **SHA256** hash algorithm and a key length of **2048 bits**. All active communication interfaces are provided with SSL certificates. The corresponding web servers have an A+ rating at.

3.6 Multifactor authentication (MFA)

All baramundi Proactive Hub products and Argus Cockpit offer the option of adding a second level of security in addition to the user password.

The options for multi-factor authentication:

- **Email**: Users receive a security code by email, which they must enter when logging in.
- **Authenticator app**: Users generate a security code via an app such as Google Authenticator, which they can install on their smartphone.

We recommend using the authenticator app, as this method offers protection even if access to emails is compromised. Multi factor authentication can be activated directly by the company admin in the administration area.

The sysadmin also has the option of resetting the MFA for individual users, for example in the event of device loss or a change of email addresses.