baramundi

Information on Data Security and Data Protection

baramundi
Argus Cockpit

baramundi
Argus Experience

Empower your IT

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

Frank Heider
Director R&D Argus Cloud

Subject to change - DocID: ARGUS-230100-INFO-231001-EN

1 Contents

2 Infrastructure and service provider

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

2.1 Microsoft Azure

baramundi Argus is operated in Microsoft Azure and is distributed as follows:

- The baramundi Argus application modules are hosted in the **Azure Region Western Europe (Netherlands)**.
- The Azure Active Directory B2C used to register and manage authorised users is hosted in the Azure Region Europe.

For more information, see:
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 Argus modules.

2.3 RapidMail GmbH

Notifications in baramundi Argus Cockpit are sent by mail via the service provider "RapidMail". RapidMail's data centre is located in Germany.

For more information, see:
GDPR and data security for newsletters - rapidmail knowledge & help

2.4 SoftwareONE Deutschland GmbH

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

3 Data processing and data security

3.1 Microsoft Azure Infrastructure and resources

3.1.1 Data retention

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

For more information, see:
AAD B2C Monitoring protol

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

For more information, see:
Activate Azure Log Analytics Manually

3.1.2 Access permission

Both the console output at runtime and the recorded log and monitoring data can only be viewed **be viewed by authorised administrators of baramundi software GmbH**. The recorded log and monitoring data is also viewed by development and support staff together with the authorised administrators, if necessary, in order to analyse application errors. In addition, SoftwareONE has access to the resources of the Azure infrastructure for cost monitoring and cost reporting. By using the Customer Logbox, Microsoft employees have no access to data within the Azure resources without the approval of our responsible administrators at baramundi. The available accounts within the Microsoft Azure infrastructure are configured to only have the minimum necessary rights (Azure RBAC). Privileged administrative rights can only be obtained via the Azure AD PIM that is used.

For more information, see:
Azure Role-Based Access Control (RBAC)
What is Privileged Identity Management?

3.1.3 Data protection declarations of the baramundi Argus modules

- Data protection declaration Argus Cockpit: *baramundi Argus Cockpit*
- Data protection declaration Argus Experience: *baramundi Argus Experience*

3.2 MongoDB Atlas database

3.2.1 Data retention

MongoDB Atlas retains the last **30 days** of logs and system event messages for each tier in a cluster. Performance Advisor logs are retained for a maximum of **7 days** for each cluster.

For more information, see:
View and Download MongoDB Logs

3.2.2 Access permission

The recorded log and monitoring data can **only be viewed by authorised administrators of baramundi software GmbH**. The recorded log and monitoring data is also viewed by development and support staff together with the authorised administrators, if necessary, in order to analyse application errors. Access to customer data by MongoDB employees can only take place with the consent of our responsible.

3.2.3 Data storage

The application data of the baramundi Argus modules is stored in an Azure storage 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 key management of the keys used is carried out by Platform Managed Keys (PMKs), via **Azure Key Vault** in the case of baramundi Argus.

For more information, see:
Key Vault | Microsoft Azure
Storage Engine and Cloud Backup Encryption — MongoDB Atlas

3.2.4 Data backups

Database backups are created at different time intervals to ensure swift data recovery in the event of a disaster. The maximum retention time of the database backups is **90 days.** Backups are stored and secured both in an Azure storage facility and in a dedicated infrastructure at baramundi with 256-bit AES encryption.

For more information, see:
Key Vault | Microsoft Azure
Storage Engine and Cloud Backup Encryption — MongoDB Atlas

3.3 Data collection by module

In the following you will find out which data is recorded and transmitted by the respective baramundi Argus modules at runtime.

3.3.1 baramundi Argus Cockpit

The data is transmitted from the baramundi Management Suite (bMS) to baramundi Argus Cockpit (bAC) via cloud connectors. These are Windows services that read relevant data from the bMS via baramundi bConnect and transfer it authorised and authenticated to the cloud. The following data is synchronised in the process.

3.3.1.1 baramundi Cloud Connector Server State

This Cloud Connector transmits information on the BMS server and its system state and includes the following values:

- Server
  - GUID
  - Name
- Server services:
  - Name
  - Execution state

3.3.1.2 baramundi Cloud Connector Job Information

This Cloud Connector transmits information about jobs, job instances and their execution status that have been released for transmission to bAC and includes the following values:

- Job definition
  - GUID
  - Display name
  - Description
  - Name
- Job instance
  - GUID
  - Endpoint GUID
  - Endpoint Name
  - Time of last action
  - BMS Execution status
  - Status text

3.3.1.3 baramundi Cloud Connector Dynamic Groups

This Cloud Connector transmits information about the endpoints that met the criteria of the universal dynamic groups (UDG) at the time of transmission. The following information from an endpoint is transmitted:

- General
  - GUID
  - Type
  - Display name
  - Host name
  - Domain
  - Local ID
  - Information about the operating system and version
  - Version of Internet Explorer
  - Identification of the boot environment used
  - Last boot time
  - Power scheme used

- Hardware information
  - Serial number
  - Manufacturer
  - Model
  - Primary MAC address
  - MAC address list
  - Logical MAC address
  - Memory size
  - CPU - Information
  - List of existing storage media with associated details such as
    - Volume ID
    - Size
    - Free memory
    - File system
    - File system type
    - Partitioning type
    - Drive letter
    - Identifier
    - Information on Bitlocker (see Bitlocker)

- baramundi Management Agent
  - Version of the agent
  - Status of the agent
  - Information on the management mode (IEM) of the client
  - Last activity of the agent
  - Last change of the agent
  - Last seen date of the agent

- Patch management information
  - Patch configuration information
  - Information about the configured update source
  - Date of last update inventory
  - Number of missing patches by different categories

- System health information
  - Administrative status information
  - Information about compliance status and compliance configuration
  - Virus and threat status information
  - Information about inventory and inventory configuration
  - Information about SecureBoot activation status
  - TPM module information and status
  - Automatic updates status
  - Firewall and network protection status
  - App and browser protection status
  - Windows Security Service status
  - User account protection status

- Information about Bitlocker
  - Bitlocker activation status
  - Startup Pin Activation status
  - Network Unlock status
  - Startup USB Key Activation status
  - Per drive:
    - Conversion status
    - Encryption level in percent
    - Bitlocker version
    - Drive protection status
    - Drive lock status
    - Number of reboots before reactivating Bitlocker

- Information about Microsoft Defender
  - Status of all Defender engines and modules
  - All version and definition information of the Defender engines and modules
  - Date of the last full scan
  - End of the last full scan
  - Active threats
  - Resolved problems and threats
  - Highest severity

- Information about Industrial Endpoints
  - Type of gateway used
  - Date of last inventory
  - Information on CPU
  - Firmware and hardware version information
  - Location of the device
  - Runtime

- Information about mobile endpoints
  - Type of Android Enterprise management mode (for Android)
  - Type of Apple management mode (at Apple)
  - Update availability from Apple (at Apple)

3.3.1.4 Typical purposes

The above-mentioned data is required to be able to record the overall status of the environment managed by the bMS. By configuring Universal Dynamic Groups, it is possible to determine individually for each environment which of the above-mentioned data should be evaluated. This enables the IT admin or other roles in the company to identify anomalies in the IT environment.

3.3.2 baramundi Argus Experience

The data is transmitted to baramundi Argus Experience via an agent installed on the end devices used. Only authenticated and authorised clients can connect to baramundi Argus.

3.3.2.1 baramundi Argus Experience Agent

- Agent's last contact (date)
- Logged in user name
- Host name of the endpoint
- IP address of the endpoint
- Logged process crashes
- Logged process hangers
- Information about the operating system, architecture and version
- File path of the suspicious applications

3.3.2.2 Typical purposes

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

3.4 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 correspond to current security standards and, in addition to the **SHA256** hash algorithm, use a key length of **2048 bits**. All active communication interfaces are provided with SSL certificates. The corresponding web servers have an A+ rating.

3.5 Multifactor authentication (MFA)

MFA is not currently supported.