OMNINET
SOFTWARE SOLUTIONS

OMNITRACKER service parameters for private hosting

15.11.2019

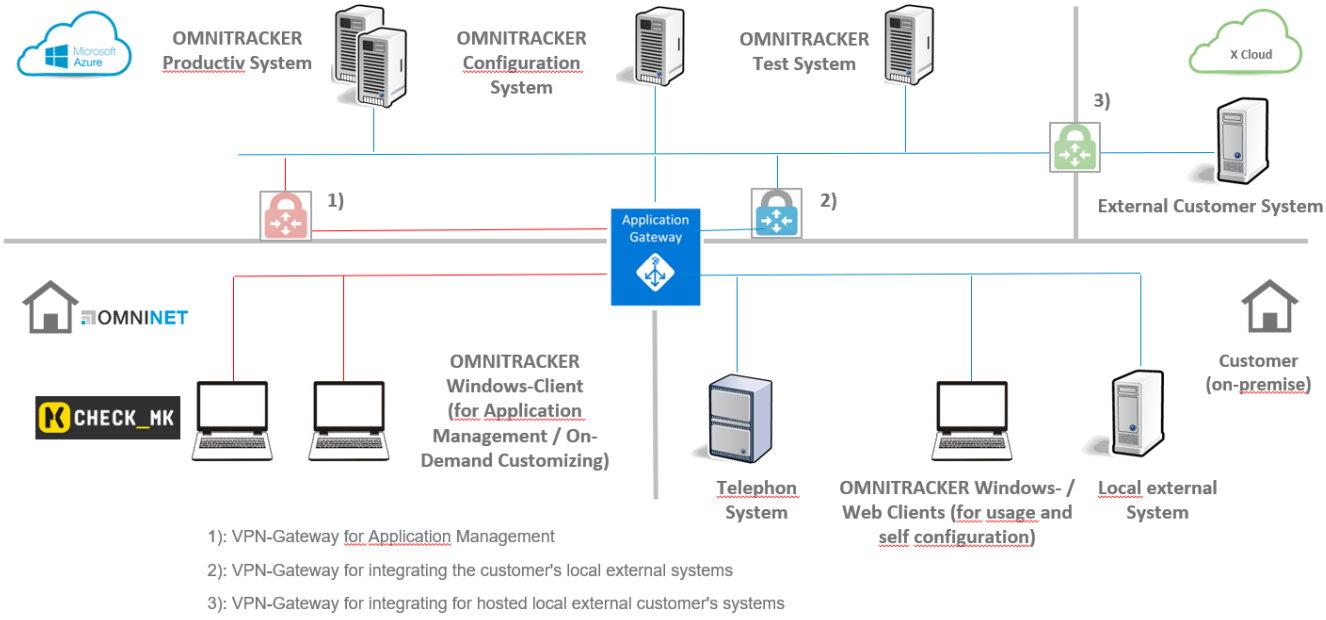
OMNINET SOFTWARE SOLUTIONS

Contents

1 Range of services

OMNINET provides services in the field of “Software as a Service” (SaaS) to the Company XYZ. This document serves as a Service Level Agreement between Company XYZ and OMNINET and describes the services, including the service parameters, to be provided by OMNINET. Optional services can also be provided; volume-based services arise monthly. The selected specification is described in the associated commercial agreement. Only those technical service features specifically listed in this appendix represent part of the contract.

2 Reference architecture



3 Installation, updates and patches

3.1 Installation

The contract software is installed by OMNINET. The OMNITRACKER client software, which is installed locally by the Company XYZ where applicable, is the exception to this. OMNINET provides a corresponding MSI file for this.

3.2 Updates

OMNINET regularly (at least twice a year) provides an update to the latest version of the contract software. The client will be informed of this at least one month in advance.

The client is responsible for updating the OMNITRACKER client software on the Windows client installed on the client’s system. OMNINET provides a corresponding MSI file for this.

3.3 Patches

Where necessary, OMNINET installs patches to increase the stability and security of the contract software; this also applies to patches or hotfixes provided by Microsoft® for operating systems or databases.

4 Security and continuity

OMNINET provides the procedures and infrastructure elements described below to secure and protect client data and to ensure an uninterrupted service.

4.1 Certified server locations

The systems are provided to OMNINET by an external data processing centre, currently Microsoft Azure. The data processing centre is certified in accordance with the requirements facing information security management systems (ISMS) in line with DIN ISO / IEC 27001. The certificate attests that the data processing centre has implemented and adapted suitable security measures.

The servers are situated and configured in an external data processing centre with various locations in Germany or in Europe. The locations provide a high level of reliability in relation to bandwidth, power supply, cooling, fire protection and physical access controls. OMNINET will inform the client accordingly in the case of a change to the data processing centre during the contract period. It will be ensured that the new data processing centre has at least the same quality standards.

Access to the systems by OMNINET only ever takes place via secure connections or directly in the data processing centre. OMNINET's technical organisational measures apply to access.

4.2 Network connection

The network connection between the OMNITRACKER cloud and client network takes place via a TLS-encrypted internet connection; a corresponding SSL certificate is provided by OMNINET. A bandwidth of up to 1,000 Mbit/s - guaranteed over 200 Mbit/s - is provided at the server location for the host system. It is the responsibility of the client to provide access to the internet from the client side.

4.3 Data separation

The SaaS offered by OMNINET provides the Company XYZ with a private cloud, i.e. the client’s data is stored by itself on the live application server and within a live database entity. In the case of a system failure at the location and the emergency operation in a different location of the data processing centre as a result, this data separation will lapse until normal operation has been restored.

4.4 Data storage

Each OMNITRACKER entity contains the following data storage locations:

- "OMNITRACKER database" (OMNITRACKER applications, configuration settings and all user data)
- "OMNITRACKER attachments" (user data attachments are stored separately at the file system level)
- "OMNITRACKER full text search (database for indexed keywords to enable efficient full text search)

4.5 Data backup

4.5.1 Database

Complete backups of the OMNITRACKER database are made weekly; differential database backups generally take place every few hours and transaction protocol backups every 5-10 minutes. The database backups have a retention period of 7 days.

4.5.2 Storage

"OMNITRACKER attachments" are fully backed up each night; the retention period is 7 days. OMNINET regularly checks to ensure the backups have been completed correctly. The full text index is also fully backed up once a night, but can be restored where necessary from database information and attachment files without loss of data.

4.6 Backup / continuity

The data listed under 4.4 is stored in a redundant backup area in the basic specification. The hard drives of all virtual machines (VMs), i.e. operating systems and data, are stored three times.

The VMs relevant for operation are also stored as an image. In the case of an unplanned VM outage, the VM is restored from the image and the data restored from the data backup.

5 System and application management

5.1 Monitoring

OMNINET carries out automated system monitoring. In the case of an alert, OMNINET receives an automated message to which it responds immediately and carries out response or remedial measures. The following components are monitored as standard, insofar as they are part of the infrastructure relevant to / required by the client:

- System resources: including hard drive capacity, RAM use, CPU use

- Service availability: including database services, IIS-relevant services, OMNITRACKER services
- Infrastructure services: including network connectivity, DNS services

5.2 System maintenance

All of the systems relevant to the provision of the SaaS solution are regularly maintained. OMNINET checks the availability of system updates / security updates from third-party manufacturers (e.g. Microsoft® Windows operating systems). Following successful verification and, taking the defined procedure for planned changes into account, the software is installed on the respective systems. Necessary disk clean-ups (e.g. deletion of system logs) are carried out; unnecessary system data is deleted after 30 days as required.

5.3 Change management

OMNINET documents all system-relevant changes internally. The OMNINET internal solution is processed following the formal change process.

Planned changes with a direct effect on the Company XYZ are carried out within the associated maintenance interval defined under 9.5. An email notification is sent in advance to the distribution list defined by the Company XYZ. Unplanned yet necessary short-term changes (hotfixes) with a direct impact on the Company XYZ (e.g. in the case of a system outage) are carried out immediately. Information about the implementation of the change is provided via a service report.

6 System environment

Below you can find a description of the possible IT systems, their applications and roles relating to the OMNITRACKER application.

6.1 Involved IT systems

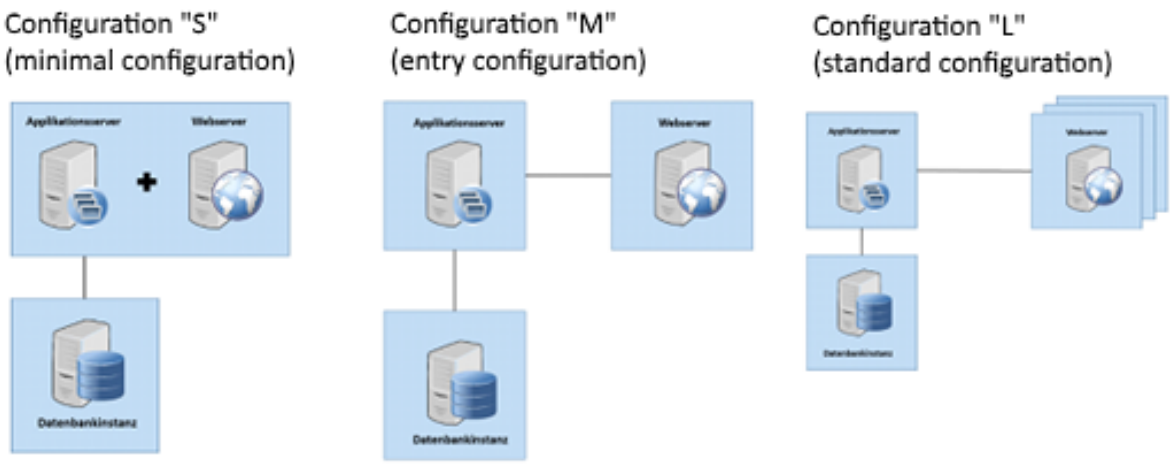
No.	Title	Description
01	Application server	Server for one or more entities of the OMNITRACKER application plus one or more web entities
02	Web server	Dedicated web server for one or more web entities of the OMNITRACKER application
03	Database service	Database service operated on a non-dedicated database server and used by an OMNITRACKER application
04	Load balancer	The load balancer serves to distribute the load across different web servers

6.2 Involved applications

No.	Title	Can be installed on IT system	Description
01	OMNITRACKER	01	OMNITRACKER server application; can be operated individually (e.g. development environment, staging environment, production environment) so that each application has its own database.
02	Database system	03	Database system for the OMNITRACKER application database. Operated via a database service.
03	OMNITRACKER web gateway	01.02	OMNITRACKER web application for access via a web browser. The application can be installed on several web servers and/or application servers. A load balancer can be used prior to the web server if needed.
04	Crystal Report runtime component	01.02	This component is required to execute reports. It can be installed on web servers, application servers and on the client side.

6.3 System architecture

The system architecture can be extremely varied due to the client's existing IT system landscape. Below we describe some of the possible development stages for the OMNITRACKER infrastructure. The actual specification will be decided upon together with the client.



7 Infrastructure

7.1 Integration into the client's architecture

7.1.1 Authentication

Authentication generally takes place via a username and password. A Site2Site VPN connection is required on the client side for Windows login, incl. Microsoft Active Directory Trust. SAML2.0 (Security Assertion Markup Language) is solely supported in the Artefact Binding method. Microsoft Active Directory Federation Services (ADFS) are supported, if a corresponding Microsoft Office 365 licence can be used (already owned by the client or procured by OMNINET on the client's behalf for a fee).

7.1.2 Email

The Company XYZ's mail server can be connected. A corresponding SSL encryption is supported by OMNINET. The availability of the client's own mail service remains the responsibility of the Company XYZ. If desired, mailboxes can be made available and integrated for the Company XYZ. The availability of the mail server is regularly checked through monitoring.

7.2 Interfaces

Additional interfaces to the systems hosted locally with the client or in cloud environments can be integrated in the OMNITRACKER application. These integrations take place as part of separate projects and are billed separately. All open import and export standards, e.g. *.csv, *.txt, are supported in principle. Microsoft Office imports and exports are supported, if a corresponding Microsoft Office 365 licence can be used (already owned by the client or procured by OMNINET on the client's behalf for a fee).

7.3 Customising

Qualified OMNITRACKER administrators on the Company XYZ side have the opportunity to make changes to the configuration using the OMNITRACKER configuration schema. Changes to the schema within the production environment, which could impact availability, must only be carried out outside of service hours and with the permission of OMNINET. Additional data backups, replacement of databases, resolution of old datasets can be requested as optional services from OMNINET and only take place once agreed between the client and OMNINET. The client has the option of using additional OMNITRACKER entities as development and staging environments. Thus, changes to the configuration schema can be made offline and transferred to the production environment after testing via the aforementioned schema transfer. Email functionality is deactivated within the development environment, if present.

7.4 Access to the application server

Only OMNINET employees can access the application server; the client has no access.

8 Service catalogue

8.1 Basic services / basic parameters

8.1.1 OMNITRACKER updates

Two OMNITRACKER updates are carried out per annum.

8.1.2 Data storage

The database can grow to a size of 250 GB.

Up to 256 GB of premium storage is provided for the “OMNITRACKER attachments” and “OMNITRACKER full text search” files.

8.1.3 Email integration

The email mailboxes are checked every two minutes for new emails.

8.1.4 Data separation

The client is provided with their own application server, including their own database.

8.1.5 Web application firewall

The client is provided with a web application firewall to safeguard access to the web server. The data processing volume included is 10 TB/month (see 8.4.2).

8.2 Optional services (flat rate)

8.2.1 Additional OMNITRACKER updates

In addition to the updates listed under 3.2, the client can also request further updates.

8.2.2 Extension to retention period for data backups

The retention period for data backups (see 4.5.1) can be increased upon request.

8.2.3 Provision of a Site2Site VPN connection

In order to improve integration in the client infrastructure, a Site2Site VPN connection can be provided between the OMNITRACKER cloud and the client infrastructure (locally installed or cloud-hosted systems). This Site2Site VPN connection is based on IPsec and IKEv2 (AES-256) and can establish a secure connection between the client’s IP address and the OMNITRACKER cloud.

8.2.4 Increase storage capacity

The storage capacity can be increased from 256 GB to 1 TB.

8.2.5 Increase database size

The database capacity can be increased from 250 GB to 1 TB.

8.3 Optional services (charged on a time and material basis)

8.3.1 Expansion of the infrastructure / new installation of existing infrastructure after tender preparation

If additional IT systems / infrastructures are required at the behest of the client once the contract has begun, necessary applications can be installed, monitoring configured and operational measures defined.

8.3.2 Data maintenance / administrative tasks in OMNITRACKER

If needed and in addition to regular projects, OMNINET can handle data maintenance and configuration tasks, e.g.

- OMNINET adds users at the request of the client and allocates these to the existing groups / roles.
- OMNINET creates filters, layouts or views to the client's specifications.
- OMNINET issues authorisations to the client's specifications.

The assessment and implementation of the requirements is completed by trained OMNITRACKER consultants. Requirements that take <=1 hr are implemented directly; if the work is expected to take >1 hr, it only takes place after discussions between the client and OMNINET. This presumes an appropriately commissioned service contingent.

8.3.3 Creation of MMSQL database backups

OMNINET creates a backup file on an MSSQL-server-operated database at the client's request.

8.3.4 Input of an MMSQL database backup

At the client's request, OMNINET creates a copy of the database for an OMNITRACKER application, which is operated on an MSSQL server, and makes this database accessible to a different OMNITRACKER application on an MSSQL server.

8.3.5 Input of schema changes

Where required, OMNINET can input schema changes. Prepared schema packages are provided by the client or OMNINET Consulting (as part of additional assignments), which are then applied in the target environment by OMNINET. Prior to importing the packet, OMNINET generates a copy of the database.

8.4 Volume-based services

8.4.1 Traffic

Traffic is understood to refer to data transfer in and out of the data processing centre.

Incoming traffic is free of charge; outgoing traffic is billed per GB/month.

8.4.2 Web application firewall data processing

Processed data over 10 TB/month is charged per GB/month.

9 Operating hours, service level and availability

9.1 General information

The Company XYZ can create service tickets at any time (i.e. 24/7, excluding possible associated maintenance intervals) via email (support@omninet.biz) and via the service portal (www.omni-tracker.biz -> Service / Support) and can ascertain the latest status of the service tickets via the service portal. Access to the service portal is approved on a person-by-person basis and must be submitted / approved by the respective licence contact person or their representative.

9.2 Operating hours

Operating hours are Monday to Sunday, midnight to midnight.

9.3 Service hours

Service hours are Monday to Friday from 8am to 6pm (CET) on working days for the main location of OMNINET. The OMNINET service desk is also available to answer telephone calls between these hours. A German-language service is guaranteed between 9am and 5pm (CET); the service is in the English language at all other times.

9.4 Response times

The following response times for new enquiries apply during the service hours:

Priority	Response time (min / hr)
Very high	60 / 01
High	240 / 04
Medium	480 / 08
Low	960 / 16

The priority levels are implemented in line with the following categorisation:

Fault category	Description
Very high	▪ Critical operating error in the production system
High	▪ Operating error in the production system relating to essential performance features
Medium	▪ Limitations to the production system without serious hindrances
Low	▪ Incorrect fulfilment of non-essential performance feature ▪ Minor flaw ▪ Others

9.5 Associated maintenance intervals

Associated maintenance intervals are scheduled to take place between 5pm and 9pm on Sundays and public holidays at the main location of OMNINET in Germany and on Mondays between 8pm and 11pm. Associated maintenance intervals are announced at least 3 days in advance, unless they relate to short-term security measures or activities agreed between the client and OMNINET. Inevitable maintenance work, which affects the entire infrastructure in terms of availability, performance and security, may differ from the regular associated maintenance intervals.

9.6 Service availability

OMNINET aims for a service availability of 99.1% for the OMNITRACKER service for the productive system.

$$Availability = \frac{(Service\ Time - Time(unplanned\ malfunction))}{Service\ Time}$$

System outages and incidents from priority levels 1 and 2 are taken into account.

If incidents are due to faults within the contract software, which can only be corrected through the provision of a new version, the incident is considered to have been resolved as soon as a workaround has been provided, which does not involve any essential changes to the user behaviour. If there is no workaround available, the outage time is considered to have ended as soon as a fault resolution is confirmed for one of the next releases.

No liability is accepted for telecommunication lines which lie beyond OMNINET's area of influence and which is the responsibility of the client.

Any outages caused by the actions of the client, e.g. schema changes, exchanging files, are not considered in this availability summary. Similarly, outages and impairments caused by a force majeure or other events for which OMNINET is not responsible are also excluded. This applies in particular to configuration changes to the OMNITRACKER applications (by the client, OMNINET or third parties), which are not part of this contract.

If configuration changes within the OMNITRACKER applications are the cause of a lack of system availability, OMNINET will provide support in analysing the cause of the error and will ensure that the system is fully restored as quickly as possible.

It is not possible for OMNINET to provide a general promise for the overall availability of the service. The following availability targets are currently promised by the data processing centre, and these are checked by OMNINET using monitoring wherever possible.

9.6.1 Availability of individual systems

An availability of 99.9% is guaranteed for individual virtual machine entities; the database service has an availability of 99.99%.

9.6.2 Availability of network infrastructure

Connected storage for individual virtual machine entities, Site2Site VPN services and backup/recovery services have an availability of 99.9% respectively. The web application firewall has an availability of 99.95%.

10 Reporting

The following reports are created for the previous month and sent as a document to the distribution list defined by the Company XYZ by the 10th working day of the month.

10.1 Availability report

A monthly report for the overall availability of the service solution is created and provided to the client. It can be used to see whether the targets listed under 9.6 have been met or not.

10.2 Service report

A detailed report, including a description of the fault, root cause analysis and measures introduced to avoid a repeat fault, is compiled for every fault reported or every registered incident, which represents an impairment to the overall availability in accordance with 9.6. This service report is created for each relevant and recorded ticket.

10.3 Security incidents

The infrastructure is constantly monitored and optimised for security reasons. Non-authenticated access for client-relevant systems outside the OMNITRACKER application or data (outside the OMNITRACKER application) is monitored and recorded. Security incidents recorded here and confirmed, as well as identified weaknesses on client-relevant systems, are reported to the client within 5 working days.