



LogiqSuite

Architecture, Security & System requirement



Document History

Version	Date	Author(s)	Comment
0.1	2022-01-17	Inés Beekers	First draft, based on PFF document v1.0
0.2	2022-03-07	Steven van Dijk	Review and added comments
0.3	2022-03-25	Inés Beekers	Resolve feedback Steven
0.4	2022-09-29	Sandy Pratama	Review and further revision
0.5	2022-11-21	Inés Beekers	Processed all changes and comments.
1.1	2023-07-05	Inés Beekers	Updated to LogiqSuite and added authentication details.

Document Approval

Version	Date	Approved by	Signature
1.0	2023-06-26	Steven van Dijk	Synergy 15.140.937
1.1	2023-07-06	John Jacobs	Synergy 15.711.746



Table of contents

sl

1	Introduction	5
1.1	What's in this document?	5
1.2	Who should read this document?	5
1.3	A globally available SaaS solution	6
1.4	Focus on security	6
2	LogiqSuite Server architecture	7
2.1	Principles involved	7
2.2	Components	8
2.3	What makes LogiqSuite cloud-native?	8
2.4	Integration with third party systems	9
3	Reliability	11
3.1	Continuous Integration and Continuous Delivery (CI/CD)	11
3.2	Environments	11
3.3	Feature toggle	11
4	Availability	12
4.1	Business continuity and disaster recovery	12
5	Scalability	13
5.1	Possibility to run multiple instances of app services	13
5.2	Database indexes	13
6	Security	14
6.1	Measures taken	14
6.2	User provisioning	14
6.3	Authentication	14
6.4	Authorization	15
7	Privacy and data protection	17
7.1	Data storage	17
7.2	User data	17



7.3	Access to the data	17
7.4	Personally Identifiable Information in logging	18
8	Minimal system requirements	19
8.1	Supported web browsers	19
8.2	Screen resolution	19
8.3	User authentication	19



1 Introduction

In current medical practice, a big challenge is that treatment may appear effective in the overall population but is often ineffective for the individual patient. Personalized medicine uses data and data science to predict if a specific therapy will be effective for an individual patient. Data science and mathematics aid development of personalized medicine and hence, high-quality data is key. A **medical data management system** is desired in health care to analyze real-world patient data, expedite medical research, share data across different institutes, and facilitate real-time complex analytics. Current data management systems used in medical practice lack important features such as: rich support for structuring data, data validation, possibilities of sharing data for collaboration, and advanced analytics capabilities.

ORTEC has empowered organizations with data science and optimization solutions since the early 1980s. ORTEC **LogiqSuite** is a fully cloud-native solution that allows management and stewardship of healthcare data for patient care and scientific research. Leveraging the proven data science expertise of ORTEC, it offers the ideal solution for complex healthcare data management and analytics. LogiqCare provides a data management system for clinical care, where data structuring, validation, and secure sharing for collaboration are key. Not only do we facilitate data sharing and collaboration across institutes, but also secure collaboration between clinicians and researchers by the combined synergy of the Logiq**Care** and Logiq**Science** solutions.

LogiqSuite provides real-time synchronization with a privacy unenriched **LogiqAnalytics**, for data analysis to empower clinical research. The LogiqAnalytics is integrated with a powerful dashboarding tool, PowerBI, for data visualization and analysis. Additionally, it is accompanied with a **data dictionary** to facilitate collaborative analysis.

1.1 What's in this document?

This document describes the architectural aspects of LogiqSuite, the underlying technologies, their advantages, and the details pertaining to security. Also, the minimal system requirements are described.

1.2 Who should read this document?

The contents of this document are most relevant to readers who wish to know the architectural and security aspects of LogiqSuite and the related technical details—security officers, IT Managers, implementation consultants, and solution architects, among others. If you have any questions, please consult your ORTEC representative.

1.3 A globally available SaaS solution

Designed and developed as a cloud-native solution, LogiqSuite is hosted on Microsoft Azure, a trusted provider of cloud environments. ORTEC, as a Gold-Certified partner, closely collaborates with Microsoft to provide a globally available solution to our customers.

As a result of being fully cloud native, LogiqSuite offers the typical benefits of a SaaS solution:

- Accessible from anywhere via the Internet
- Fast delivery of new features and software updates compared to an on-premises installation
- Highly available and scalable
- Reduced cost of owning and maintaining hardware such as servers and other equipment

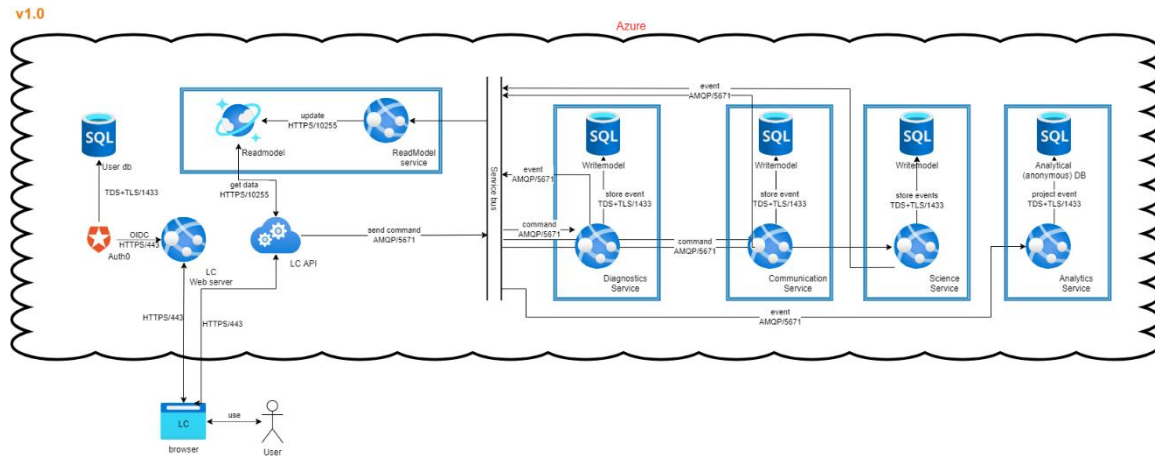
1.4 Focus on security

Security is always a primary focus for ORTEC. We employ best practices and adhere to standards in designing and developing our solutions. Especially for medical data, security (Section 6) and privacy (Section 7) are crucial to ensure data handling in LogiqSuite, all in agreement with the GDPR and according to the ISO27001 and NEN7510¹ regulatory guidelines.



¹ The NEN7510 standard is a standard developed by the Netherlands Standardization Institute for Information Security for the healthcare sector in the Netherlands. (<https://www.nen.nl/en/certificatie-en-keurmerken-nen-7510>)

2 LogiqSuite Server architecture



2.1 Principles involved

The following sections describe the fundamental principles involved in the design and development of LogiqSuite.

2.1.1 Cloud-native solution

LogiqSuite is designed and developed as a fully cloud-native solution. We've made use of the best practices of designing a cloud-native solution, resulting in a modern and robust solution.

2.1.2 Privacy-by-design

LogiqSuite is designed and developed according to the privacy-by-design principles. Therefore, privacy is embedded into the design of the solution and integrated in the development lifecycle in a proactive and preventative manner. For example, data access is by default denied and requires explicitly adding privileges based on a need-to-know basis. Additionally, the patient's privacy is central in our approach, and we aim for transparency to our users.

To find out more about Privacy, we direct you to Section 7.

2.1.3 Persona-based UX

The user experience of LogiqSuite is designed based on certain established personas in the domain of clinical care and medical research. The personas are independent and autonomous. As a result, the user interfaces are simple, intuitive, and easy-to-use; whilst still allowing great flexibility in customization for the vast variety in medical fields and corresponding needs.

2.1.4 Web-based UI

All user interfaces are web-based, developed with latest technologies (e.g., HTML5 and browser-side dynamic) and designed for optimal security and user experience. LogiqSuite supports all modern web browsers, including Chrome, Edge, and Firefox, with an experimental support for Safari.

2.1.5 Use of standard protocols

LogiqSuite uses standard protocols, facilitating easy integration with the solution.

- REST API for querying data and data ingress (migration)
- CSV/JSON serialization for import/export of data
- TLS 1.2 for encryption of communication channels
- OIDC or SAML for integrations with Identity Providers (e.g., Active Directory)

2.2 Components



LogiqSuite uses Microsoft Azure as its cloud platform. It consists of a web front-end, a REST API and various background services. State is persisted in a shared (per environment) Azure SQL database with back-up policies that support restore to various points in time in case of an emergency. Data exported real-time for purposes of analytics is stored in a dedicated Azure SQL database. Real-time communication between the components is facilitated with the Azure Service Bus. Real-time pushing of events to users of the web application is handled using SignalR (WebSockets).

2.3 What makes LogiqSuite cloud-native?

LogiqSuite is built upon the Service-Oriented Cloud Architecture platform, which uses cloud-native hosting in Azure App Services. No virtual machines are used. Besides this LogiqSuite uses cloud-native technologies, such as Azure SQL databases, the Azure Service Bus, and the Azure Key Vault. Application Insights is used to collect telemetry and exceptions that allow for real-time monitoring of the application's state and pre-emptive action if something goes wrong.

Furthermore, the architecture of LogiqSuite adheres to cloud-native principles such as microservices, scalability by design and resilience against failure.

2.3.1 Application structure

The following components are used:

Angular-based User Interface (UI)

A web application with an Angular-based UI, also known as the front end, allows users to interact with the solution.

Azure App Service

LogiqSuite's REST API, front-end applications and background services are hosted in Azure App Services.

Azure SQL Database

Used to persist the applications state, in other words, the data managed in the application. The Azure SQL Server is set up in such a way that it only accepts connections from the solution's app service and from the ORTEC network. The latter is required for performing upgrades to the data model and in certain support and fire-fighting scenarios.

Azure Cosmos DB

Used as the read-model for the application.

Azure Key Vault

The Key Vault is used to store various secrets used by the application, such as connection strings, but also client certificates for interfaces with external products that require an extra layer of security.

Azure Service Bus

The Service Bus is used for real-time communication between the various app services so that they can act upon events that happen within the application.

Application Insights

Application Insights collects telemetry and exceptions and allows for post-mortem and real-time analysis and monitoring of the application's health.

Grafana



Grafana is used at ORTEC to monitor the aggregated information from Application Insights in an easily actionable manner. It allows ORTEC to preemptively act if there is an indication of problems with the application.

Auth0

Auth0 provides the bridge between any customer's identity provider (IDP) and our applications.

2.4 Integration with third party systems

In addition to user interfaces, LogiqSuite provides a set of APIs for integration with third party systems. All network communication is done over HTTPS.

2.4.1 Identity Provider interface

LogiqSuite uses Auth0 to offer authentication over OIDC. Upon request, Auth0 can be set up to serve as a bridge between the application and the customer's own IP so that LogiqSuite can be accessed using Single Sign-On (SSO). Access to LogiqSuite can be governed by passing a claim from the IDP that a given user has access to the application.

Connection of the Identity Gateway (Auth0) with the ADFS service is done over HTTPS and uses the standard SAML protocol.

2.4.2 REST API

LogiqSuite uses a dedicated REST API for its own front-end, but also offers a REST API for general use that can be used to query information about resources and planning data. This general use REST API will henceforth be called “REST API” for short.

The data that can be accessed by the REST API is governed by the permissions granted to the authenticated user, just like in LogiqSuite itself. The REST API offers an (OAuth) authentication flow with Auth0 to facilitate authentication.




3 Reliability

We have incorporated several best practices to ensure that our solution is highly reliable.

3.1 Continuous Integration and Continuous Delivery (CI/CD)

We follow the process of CI/CD to ensure frequent and reliable delivery of software changes. This ensures all of our customers have access to the latest features and updates. Implementation of automatic testing ensures our software's reliability and eliminates the chances of human errors.

3.2 Environments



Continuous and reliable development of LogiqSuite is guaranteed by working with *test*, *pilot*, and *production* environments. The test environment is used to test newly developed functionality and intended for ORTEC employees only. Once the new functionality is deployed to the pilot environment, final acceptance testing can take place by the product owner and/or customer. After approval, the new functionality will be deployed to the production environment. This is the environment used by customers and where medical data will be stored. Hereby we ensure only approved functionalities are released to the production environment.

Each environment is capable of multi-tenancy, using a data *Account* as logical separation between tenants. However, upon request, each customer can have a dedicated production environment. In LogiqSuite, a data *Account* represents both a data isolation boundary and the scope of a user session. Upon login, a user selects one of the *Accounts* they are authorized to access, after which their data access is limited to that *Account*, subjected to other authorization rules.

3.3 Feature toggle

New features could be first released with a toggle as a controlled rollout to customers, so that they can be switched off in case of any undesirable effects without a complete roll back to the previous version. Feature toggles are turned off by default, and they are (de-)activated on the data *Account* level (see 3.2 for more details about data *Account*).

4 Availability

We make use of the underlying Azure infrastructure to ensure high availability of our solution as described in the following sections. We make use of Microsoft Azure in the EER, conform the GDPR.

Availability targets are defined in the [ORTEC Cloud SLA](#). Recovery time objective (RTO) is 4 hours, meaning we guarantee availability to be restored within 4 hours of the solution becoming unavailable. Guaranteed uptime is 99.5%. The recovery point objective (RPO) is 30 minutes, meaning that even in the event of a complete disaster no more than 30 minutes of data mutations will be lost.

4.1 Business continuity and disaster recovery

The Azure SQL Server is equipped with automated backups for both point-in-time restore and long-term full backups. Point-in-time restore can be executed up to 7 days into the past. Weekly backups are retained for 30 days. And monthly backups are kept for 365 days.

Automated backups are also created for application logs via continuous export into a dedicated data storage. They are retained for 90 days, during which they are kept in a non-erasable and non-modifiable state (for non-repudiation). Note that this retention period can be arbitrarily increased if desired.

Data, backups, and all services are hosted in the Western Europe region of Azure.

Customers can request a quote for adding more redundancy to web, compute, and data tiers if so desired.



5 Scalability

5.1 Possibility to run multiple instances of app services

The architecture allows for multiple instances of resource-intensive app services to exist so that jobs can be distributed between them. By design, the architecture is set up with multiple loosely coupled services that communicate through messaging so that more instances of a service can be created if a part is overloaded. Care has been taken to avoid that the database becomes a bottleneck by carefully managing strong consistency demands on data.

5.2 Database indexes

Indexes are used in the database to allow for optimal query performance.



6 Security


Security has been a focal point in the design and development of LogiqSuite. We have taken several measures to ensure the confidentiality, integrity, and availability (commonly abbreviated as CIA) of our applications and the data handled by them.

6.1 Measures taken

6.1.1 Secure communication

The secure protocol HTTPS is used for all communication—from and to LogiqSuite, between the modules, and within the modules. SSL is also used for communication between components and the database. For all SSL connections, TLS 1.2 is used.

6.1.2 Authentication based on OpenID Connect

 All the user interfaces and APIs are designed to support authentication via OpenID Connect 1.0, which is an identity layer based on the OAuth 2.0 protocol.

6.1.3 DDoS protection

By default, the solution provides out-of-the-box basic DDoS protection from Microsoft Azure.

6.1.4 Firewalls

Firewalls are used to restrict access to the Azure SQL Servers. Access is limited to LogiqSuite's app services and ORTEC.

6.2 User provisioning

Users are automatically provisioned in the application based on a claim received by the IDP through Auth0. This claim both governs access and provisioning. This means that access to LogiqSuite can be granted or revoked at the IDP.

6.3 Authentication

LogiqSuite is designed to support authentication using OpenID Connect 1.0, which is a token-based authentication method.

6.3.1 Authentication via Auth0

Auth0 is a third-party organization that focuses on providing authentication and authorization as a service. The process of authenticating users and systems is delegated to Auth0, which also acts as a gateway between LogiqSuite and your Identity Provider. By delegating authentication to Auth0, ORTEC is not required to handle the complexities of providing interfaces for a myriad of identity providers and the various underlying protocols. This significantly reduces the complexity of our solutions, making them more secure and less error prone. In addition, by using Auth0, ORTEC does not have to accommodate the constantly evolving technology around authentication directly into its solutions.

6.3.2 User authentication

The responsibility of authenticating a user lies with your Identity Provider (IdP). LogiqSuite supports a wide range of identity providers. Single sign-on is also supported. We have tested some of the most commonly used IdPs via Auth0.

The following IdPs are known to work readily with LogiqSuite:

- Azure Active Directory (Azure AD)
- Microsoft AD FS

In addition, we have tested that LogiqSuite readily works with SAML 2.0 protocol.



For individual users, LogiqSuite will provide its own Azure AD as IDP equipped with two-factor authentication, to which members of an external Azure AD can be invited. Authenticating to the LogiqSuite Azure AD requires an MFA (enforced after 14 days), in addition to the external Azure AD's authentication policy.

6.3.3 User authentication for LogiqAnalytics

LogiqAnalytics data can be made available via Power BI workspaces which, by default, are *not* accessible to LogiqCare/-Science users. Access control to these datasets will be managed by ORTEC by inviting authorized users to LogiqSuite's own Azure AD. Users authenticate with this AD using two-factor authentication, and access Power BI workspaces they have been granted access to.

6.3.4 System authentication

Systems require appropriate tokens to access LogiqSuite. Every API request must contain a valid access token. To get the tokens, they must authenticate themselves with Auth0 using the OpenID protocol.

6.4 Authorization

LogiqCare/-Science has an authorization model within the application that combines role-based access control (RBAC) and attribute-based access control (ABAC). Users are assigned to specific roles to give them permissions to use certain parts of the application. Additionally, users are assigned specific

attributes to determine what part of the data they are allowed to see. For further details we refer you to Section 7.2.



7 Privacy and data protection

As a provider of data-driven solutions, ORTEC considers it extremely important to protect the data in its purview and to act responsibly in conformation with applicable laws, regulations, and generally accepted standards.

The following sections describe the details of the data that is stored in LogiqSuite and how it is protected.

7.1 Data storage

Data is stored in so-called read-model and write-model databases. The write-model is the “single source of truth”, whereas the read-model is basically a fast cache of aggregated data. A read-model is stored in Cosmos DB to accommodate specific queries. The read-model can be reconstructed from the write-model (Azure SQL). These databases employ encryption at rest.



The data is stored in Azure datacenters. The physical location of a datacenter depends on the Azure geography of the deployment. The default region is Western Europe.

7.2 User data

LogiqCare/-Science stores information about users that is needed to identify them, both for authentication/authorization and to allow assigning the required attributes to users to specify data access permissions. The information about these users consists of username, email address, and first and last name and the specific assigned attributes (see 7.3.2).

7.3 Access to the data

ORTEC requires access to the data in customer environments only for support purposes. Our internal organizational governance ensures that this access is restricted to a limited set of employees. This is in compliance with ISO270001 and NEN7510 certifications.

7.3.1 RBAC

As previously mentioned in Section 6.4, user permissions in LogiqCare/-Science are assigned based on role-based access control. Below we specify the various roles possible:

- **Admin:** administrative role for an ORTEC employee to manage the accounts, users, departments, and groups in LogiqCare/-Science.

- **Account Manager:** administrative role for an ORTEC employee to manage users, departments, and groups in a specific account.
- **Configurator:** role for an ORTEC employee to configure data templates, e-mail templates, reports, and studies.
- **Data Editor:** role for an authorized ORTEC employee to erase data from the recycle bin, update data that is no longer editable to the normal user.
- **User:** role for a user of LogiqCare/-Science that needs access to the patient/subject specific data stored with edit rights (limited according to ABAC, see Section 7.3.2).
- **Viewer:** like the User role, however limited to view-only rights.

7.3.2 ABAC

As previously mentioned in Section 6.4, user access to data is limited based on user attributes. Below we specify the various attributes that can be assigned in LogiqCare/-Science:

- **Account:** defined by the admin or account manager to fully separate different projects and without allowing any exchange of data within LogiqCare/-Science. This separates data templates, patient and subject data, and anything underneath.
- **Department:** user group of persons belonging to the same department to allow access to patient- or subject-data on a need-to-know basis. Users only have access to data of subject/patients of their department and are only allowed to edit data created by a user of their own department.
- **Domain:** separation of data based on the domains Care and Science to allow collaboration between clinical practice and research without revealing unnecessary sensitive data. Data templates can be assigned to Care and/or Science and the domain of the user will define access to the data.
- **Group:** groups can be created to provide a subset of users with additional rights and functionality, for example to referrers or authorizers.

With ABAC, LogiqCare/-Science supports addition of custom authorization rules based on customer needs.

7.4 Personally Identifiable Information in logging

While user actions and mutations to entities are logged, it is done in such a manner that PII is not exposed. This means that user actions are logged with the user's id, not their username or full name. Similarly, logging of operations on fields that are expected to contain PII is sanitized so that PII will never end up logs with normal usage of the application. It is the responsibility of users to not enter PII in fields that are obviously not intended for them, e.g., free text fields, comments, etc., as these will show up in mutation logs. Logs are retained for 90 days or more (see Section 4.1 for more details).

8 Minimal system requirements

8.1 Supported web browsers

LogiqSuite is a cloud-native solution that can be accessed using your web browser. The following web browsers are supported:

Google Chrome - latest version

Mozilla Firefox - latest version

Microsoft Edge - latest version

Safari (on iOS and macOS) – latest version (limited functionality)

8.2 Screen resolution



For optimal use of LogiqSuite, we recommend using a Full HD screen (resolution 1920x1080 or higher) with 100% font scaling. When using a screen with a lower resolution, the application will work, but the user experience will be affected.

8.3 User authentication

The responsibility of authenticating a user lies with your Identity Provider (IdP). LogiqSuite supports a wide range of identity providers. Single sign-on is also supported. See Section 6.3.2 for more details.