



ORTEC Multi Resource Planning

Architecture, Security & System requirements

Document History

Version	Date
1.0	16-02-2021
1.1	03-03-2021
1.2	07-04-2021
1.3	26-05-2021



Table of contents

1	Introduction	3
1.1	A globally available SaaS solution	3
1.2	Focus on security	3
1.3	What's in this document?	3
1.4	Who should read this document?	3
2	OMRP Server architecture	4
2.1	Principles involved	4
2.2	Components	5
2.3	What makes ORTEC MRP cloud-native?	5
2.4	Integration with third party systems	6
3	Reliability	9
3.1	Continuous Integration and Continuous Deployment (CI/CD)	9
3.2	Feature toggle	9
4	Availability	10
4.1	Multi-region deployment (optional)	10
4.2	Business continuity and disaster recovery	10
5	Scalability	11
5.1	Possibility to run multiple instances of app services	11
5.2	Per-tenant dedicated resources	11
5.3	Database indexes	11
5.4	Relevance filtering of application events	11
6	Security	12
6.1	Measures taken	12
6.2	User provisioning	13
6.3	Authentication	13
6.4	Authorization	14
7	Privacy and data protection	15
7.1	Data storage	15
7.2	Access to the data	15
7.3	Personally Identifiable Information in logging	16
8	Minimal system requirements	17
8.1	Supported web browsers	17
8.2	Screen resolution	17
8.3	User authentication	17



1 Introduction

ORTEC has empowered organizations with optimization solutions since the early 1980s. ORTEC Multi Resource Planning (henceforth abbreviated as ORTEC MRP) is a fully cloud-native solution that helps you optimize your multi resourcing planning and reduce costs. Leveraging the proven optimization technology of ORTEC, it offers the ideal solution for complex scheduling and optimization issues.

1.1 A globally available SaaS solution

Designed and developed as a cloud-native solution, ORTEC MRP 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, ORTEC MRP offers the typical benefits of a SaaS solution:

- Accessible from anywhere via the Internet
- Faster 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



1.2 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.

1.3 What's in this document?

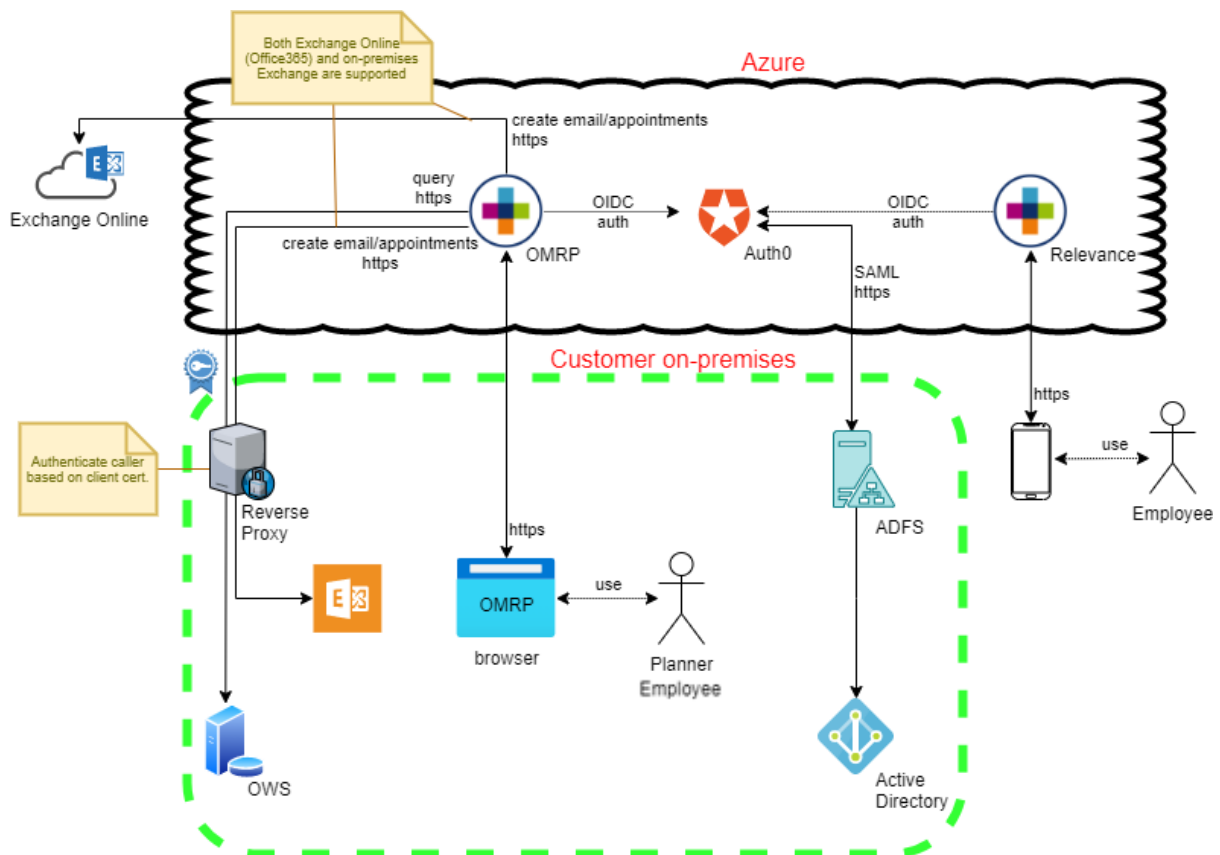
This document describes the architectural aspects of ORTEC MRP, the underlying technologies, their advantages, and the details pertaining to security. Also the minimal system requirements are described.

1.4 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 ORTEC MRP 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.

2 OMRP Server architecture



2.1 Principles involved

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

2.1.1 Cloud-native solution

ORTEC MRP 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 Persona-based UX

The user experience of ORTEC MRP is designed based on certain established personas in the domain of planning services. The personas are independent and autonomous. As a result, the user interfaces are simple, intuitive, and easy-to-use.

2.1.3 Web-based UI

All user interfaces are web-based and developed with latest technologies for best user experience.

2.1.4 Use of standard protocols

ORTEC MRP uses standard protocols, facilitating easy integration with the solution:

- REST API for reading planning and resource data from the application, e.g. for creating custom reports.
- Exchange Web Services (EWS) for integration with MS Exchange, to be replaced with MS Graph to remain future-proof.
- SOAP interface for integration with ORTEC Workforce Scheduling (ORTEC WS).

2.2 Components

ORTEC MRP 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 per-tenant Azure SQL database with back-up policies that support point-in-time restore in case of an emergency. 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 WebSockets, soon to be replaced with SignalR.



2.3 What makes ORTEC MRP cloud-native?

ORTEC MRP is built upon the Service-Oriented Cloud Architecture platform, which can be and was designed to be hosted natively in Azure App Services. Besides this ORTEC MRP 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.

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.

Application Shell

The shell is the front-end's point of entry, that is responsible for handling user authentication. Based on the user's identity, the shell offers opaque access to the correct tenant.

Azure App Service

ORTEC MRP'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 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.

Azure SignalR Service

Azure SignalR Service is used to notify the UI in real time when data is updated in the back end.

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, ORTEC MRP provides a set of APIs for integration with third party systems.

All network communication is done over HTTPS. To connect from the cloud service to on-premises resources (ORTEC Workforce Scheduling, Exchange) a reverse proxy should be configured that provides an endpoint for each on-premises resources and forwards the request. The reverse proxy guarantees the validity of the caller using a client certificate presented by the cloud service.

2.4.1 Identity Provider interface

ORTEC MRP uses Auth0 to offer authentication over OIDC. Auth0 serves as a bridge with the customer's own IDP so that ORTEC MRP can be accessed using Single Sign-On (SSO). Access to ORTEC MRP can be governed by passing a claim from the IDP that a given user has access to the application. If a user is new the necessary information within ORTEC MRP's database will be provisioned automatically.

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

2.4.2 Exchange interface

ORTEC MRP allows for keeping resources up-to-date about their schedules that are planned within the application. It does so by using a background service that utilizes the Exchange Web Services for making calendar appointments and sending emails in Exchange.

For writing and keeping the appointments up-to-date there are two options:

- 1) Using the main calendar folder: The appointments are written and kept up-to-date in the employee's main calendar folder
- 2) Using a dedicated calendar folder: The appointments are written and kept up-to-date in a separate dedicated folder in an employee's calendar. The name of this folder is the same for every employee that has an account on the same Exchange server.

In OMRP, under system configuration, the name of the dedicated calendar folder to use can be configured. When this is left blank, the Exchange interface service will instead attempt to write to employees' main calendar folders instead.

Both options in the Exchange interface will require an Exchange account that is given editor permissions to calendar folders and to send emails. Option one requires permissions to employees' main calendar folders. Option two will not require any permissions for the Exchange account to employees' main calendar folders. For option two this means that any personal information in employees' calendars will not be exposed to ORTEC MRP's Exchange interface. The credentials are configured in the application.



The Exchange interface uses the Exchange Web Services (EWS) for communication with the Exchange server. This can be used with any publicly accessible EWS endpoint. When an organization chooses not to host a publicly accessible endpoint, a proxy set-up can be provided that utilizes a client certificate. That can be used to validate that a request is indeed from ORTEC before it's passed to the internal EWS endpoint.

A migration to Microsoft Graph is planned for the near future.

2.4.3 ORTEC Workforce Scheduling interface

Integration with ORTEC Workforce Scheduling is achieved using a SOAP interface over CAIS. The CAIS endpoint will need to be exposed for external access so that ORTEC MRP's ORTEC WS interface can access this. The CAIS endpoint can be secured by requiring a client certificate that is used to sign requests from ORTEC MRP's ORTEC WS interface. This check can for example be done by a reverse proxy that serves as a point of entry that is responsible for checking whether requests are signed using the correct certificate before passing on the request to the internally hosted CAIS endpoint.

The data from ORTEC WS that is exposed to ORTEC MRP is governed by setting a property on roster groups that indicates that they should be discoverable by ORTEC MRP.

2.4.4 REST API

ORTEC MRP 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 REST API exposes planning information and resource information, such as name, resource types, skills and parttime schedules. The REST API is used by ORTEC MRP’s own overviews, Excel download and the ORTEC MRP mobile app and can also be used to create custom reports using a reporting tool of one’s choice.

The data that can be accessed by the REST API is governed by the permissions granted to the authenticated user, just like in ORTEC MRP 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 Deployment (CI/CD)

We follow the process of CI/CD; all new developments are automatically tested and deployed. Automation eliminates the chances of human errors.

3.2 Feature toggle

New features could be first released with a toggle as a controlled rollout to the customers, so that they can be switched off in case of any undesirable effects without a complete roll back to the previous version.



4 Availability

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

4.1 Multi-region deployment (optional)

It is possible to deploy the solution in multiple regions to achieve very high degrees of availability and disaster recovery. The incoming requests to the applications are managed by Azure Traffic Manager, which is a DNS-based traffic load balancer. The requests are routed to the primary region under normal circumstances and in case of a regional failure, they're routed to the failover (secondary) region.

Attention:

Multi-region deployment is optional and incurs additional costs. Please contact your ORTEC representative for more details.



4.2 Business continuity and disaster recovery

The Azure SQL Server is configured with both point-in-time restore and long-term back-ups. Point-in-time restore can be executed up to 7 days into the past. Weekly back-ups are kept for 7 days. Monthly back-ups are kept for 30 days.

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

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.

5.2 Per-tenant dedicated resources

ORTEC MRP offers per-tenant dedicated resources that can be scaled up to higher Azure tiers to accommodate a given tenant's load.

5.3 Database indexes



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

5.4 Relevance filtering of application events

When application events trigger clients to (re)load certain data these events are filtered on relevance for clients. This prevents the execution of unnecessary requests.

6 Security

Security has been a focal point in the design and development of ORTEC MRP. 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 ORTEC MRP, between the modules, and also within the modules. SSL is also used for communication between components and the database. For all SSL connections, TLS 1.2 is used.

When background services connect to external endpoints an extra layer of security can be added by signing requests with a client certificate. This is for example required when connecting to an on-premises instance of ORTEC WS.



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 IP whitelisting

It is possible to limit access to ORTEC MRP using IP whitelists.

6.1.4 DDoS protection

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

6.1.5 Firewalls

Firewalls are used to restrict access to the Azure SQL Servers. Access is limited to ORTEC MRP'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 ORTEC MRP can be granted or revoked at the IDP.

6.3 Authentication

ORTEC MRP 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 ORTEC MRP and your Identity Provider.

By delegating authentication to Auth0, ORTEC isn't 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 doesn't 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). ORTEC MRP 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 ORTEC MRP:

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

In addition, we've tested that ORTEC MRP readily works with SAML 2.0 protocol.

Note

If you have an IdP not listed above, or it uses a protocol other than SAML 2.0, contact your ORTEC representative to know if it can be supported.

6.3.3 System authentication

Systems require appropriate tokens to access ORTEC MRP. Every API request must contain a valid access token. To get the tokens, they must authenticate themselves with Auth0 using the OAuth 2.0 protocol.

6.4 Authorization

ORTEC MRP has a fine-grained authorization model within the application. Users belong to user groups. User groups can be given permissions to use certain parts of the application and permissions on the organization units modelled within the application. Management permissions on other entities are derived from permissions on the associated organization units.

Furthermore, a distinction is made between managing entities and using entities in planning (or when consulting the planning, e.g. when viewing overviews or using the REST API). This means that permission to *use* entities can be handed out without simultaneously handing out permission to *manage* them.



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 ORTEC MRP and how it is protected.

User

ORTEC MRP stores information about users that is needed to identify them, both for authentication/authorization and to allow putting users into user groups. The information about these users are user name (the nickname from the identity provider), email address and first+last name.

Employee

The name of employees is stored in Resource Management. In addition, extra resource properties can be configured that may be used to store Personally Identifiable Information (PII). It is the responsibility of the customer to use these fields in accordance with laws and regulations.



For employees the following will also be stored within the application:

Resource types

Resource types to which resources belong. This can say something about their profession.

Skills + levels

Skills that a resource has. This can say something about their professional abilities.

Preferred/unfavorable cooperation

This could say something about personal relationships between resources.

Availability, activities

This can be used to infer when someone is at work or not.

7.1 Data storage

ORTEC MRP uses Azure SQL databases. 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 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.

7.3 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 user name 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. display names of activity types, skills, resource types, etc., as these will show up in mutation logs.

Logs are saved for 90 days.




8 Minimal system requirements

8.1 Supported web browsers

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

- Google Chrome - most recent version
- Mozilla Firefox - most recent version
- Microsoft Edge - most recent version

8.2 Screen resolution

 For optimal use of ORTEC MRP, 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). ORTEC MRP supports a wide range of identity providers. Single sign-on is also supported.