OneNet Framework and Components Final Release

D6.8

Authors:

Anastasis Tzoumpas (UBE)

Apostolos Kapetanios (ED)

Eleni Panagou (UBI)

Ferdinando Bosco (ENG)

Angelo Triveri (ENG)

Konstantinos Kotsalos (ED)

Kostas Mylonas (UBI)

Magda Foti (UBI)

Vassilis Sakas (ED)

Responsible Partner	European Dynamics
Checked by WP leader	Vassilis Sakas (ED), 27/11/2023
Verified by the appointed Reviewers	Nejc Petrovic (EG), 22/11/2023 Boris Turha (EL), 16/11/2023
Approved by Project Coordinator	Padraic McKeever (Fraunhofer), 20/12/2023

Dissemination Level	Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Issue Record

Planned delivery date	30/09/2023
Actual date of delivery	20/12/2023
Version	1.0

Version	Date	Author(s)	Notes
0.1	06.09.2023	ED / ENG / UBE	ToC & Main Chapters
0.2	22.09.2023	UBI / UBE	Legal, Regulatory, Privacy and Cybersecurity Management & Compliance Tools Section
0.3	07.11.2023	UBI / UBE	Network Monitoring and Analytics User Manual
0.9	8.11.2023	ED	Review version
1.0	4.12.2023	ED / ENG	Updated after review. Additions and Corrections following comments of the Project Coordinator

Disclaimer:

All information provided reflects the status of the OneNet project at the time of writing and may be subject to change. All information reflects only the author's view and the European Climate, Infrastructure and Environment Executive Agency (CINEA) is not responsible for any use that may be made of the information contained in this deliverable.

.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

About OneNet

The project OneNet (One Network for Europe) will provide a seamless integration of all the actors in the electricity network across Europe to create the conditions for a synergistic operation that optimizes the overall energy system while creating an open and fair market structure.

OneNet is funded through the EU's eighth Framework Programme Horizon 2020, "TSO – DSO Consumer: Large-scale demonstrations of innovative grid services through demand response, storage and small-scale (RES) generation" and responds to the call "Building a low-carbon, climate resilient future (LC)".

As the electrical grid moves from being a fully centralized to a highly decentralized system, grid operators have to adapt to this changing environment and adjust their current business model to accommodate faster reactions and adaptive flexibility. This is an unprecedented challenge requiring an unprecedented solution. The project brings together a consortium of over seventy partners, including key IT players, leading research institutions and the two most relevant associations for grid operators.

The key elements of the project are:

1. Definition of a common market design for Europe: this means standardized products and key parameters for grid services which aim at the coordination of all actors, from grid operators to customers;
2. Definition of a Common IT Architecture and Common IT Interfaces: this means not trying to create a single IT platform for all the products but enabling an open architecture of interactions among several platforms so that anybody can join any market across Europe; and
3. Large-scale demonstrators to implement and showcase the scalable solutions developed throughout the project. These demonstrators are organized in four clusters coming to include countries in every region of Europe and testing innovative use cases never validated before.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

List of Figures

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

List of Abbreviations and Acronyms

Acronym	Meaning
AI	Artificial Intelligence
API	Application Programming interface
CH	Clearing House
CIM	Common Information Model
CSV	Comma-Separated Values (table)
DAPS	Dynamic Attribute Provisioning Service
DB	Database
DoA	Description of Action
DSO	Distribution System Operator
DTM	Dynamic Trust Monitoring
ECC	Execution Core Container
FSP	Flexibility Service Provider
FTC	FIWARE TRUE (TRUsted Engineering) Connector
GUI	Graphical User Interface
IDM	Identity Manager
IDS	International Data Spaces
IDSA	International Data Space Association
IoT	Internet of Things
IP	Internet Protocol
KPI	Key Performance Indicator
LD	Linked Data
LFE	Linux Foundation Energy
ODRL	Open Digital Rights Language
PNG	Portable Network Graphics
SLA	Service Level Agreement
SSL	Secure Sockets Layer
SVG	Scalable Vector Graphics
TSO	Transmission System Operator
UC	Use Case
UC App	Usage Control App
UI	User Interface
WP	Work Package
XML	Extensible Markup Language

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Executive Summary

The **OneNet Framework** demonstrates that the ideas conceived and developed throughout the various stages of the OneNet project can lead to the creation of an architecture and a practical and efficient system. This reference implementation seamlessly connects different flexibility platforms and energy stakeholders, allowing various stakeholders to exchange reliable and trusted data with one another through a secure and smooth process. Key elements of this work include:

- A Reference Architecture that combines the structure of IDS and FIWARE.
- The classification of Services (referred to as "cross-platform services") and Data (termed "Business Objects") designed to facilitate specific transactions among stakeholders.
- The development of frameworks and tools to ensure compliance with legal, regulatory, and cybersecurity requirements for the system.
- The development of the appropriate software components which constitute the OneNet Framework (OneNet Middleware, OneNet Workbench, OneNet Monitoring & Analytics Dashboard).

The OneNet Framework enables direct communication between the participating stakeholders (data producers and data consumers). The Middleware, Workbench, Monitoring and Analytics components use only meta-data in order to facilitate such communication but do not have access to the actual data exchanged. Every data producer maintains control of its data and determines what data can be provided to which data consumer. The predefined Cross-Platform-Services and Business Objects facilitate such exchange to be in a harmonized way, while stakeholders have the possibility to define new Services and/or Business Objects.

The final release of the OneNet Framework focuses on establishing its fundamental communication capabilities integrated with the refined functional specifications (enhanced programmatic and UI-related interfaces). It offers an easy-to-install IDS-based connector (OneNet Connector), to establish connectivity with the OneNet Middleware that in turn enables the discoverability compatible with all among stakeholders (data providers, data consumers and service providers). This connector can be deployed within each platform or stakeholder's environment. Its purpose is to identify each participant and facilitate the exchange of data between them.

The OneNet Framework is not intended to replace any existing flexibility or TSO-DSO coordination platform, but is interoperable with other platforms, systems or services. The OneNet Framework does not inspect the data being exchanged, nor does it serve as a data repository. Its primary role is to enable communication with other OneNet participants exploiting secured and trusted infrastructure that assures data provenance and sovereignty.

The OneNet Framework has been made available for piloting in the demos of the OneNet project (four geographical clusters with 10 demos in total), proving its capability to be easily deployed in various ICT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

environments and communicate with different stakeholders' platforms (provided that the ICT policies within the respective IT environments allow for such direct communication with the counterparty's site(s)).

The OneNet Connector has been reported in the respective IDSA connectors' report(s) and will remain available under an Open-Source S/W license beyond the duration of the OneNet project. Horizon Europe projects that recently started or will start (such as Enershare, TwinEU, RESONANCE) will further exploit the OneNet Framework and its components. In addition, the developers intend to submit the OneNet Framework and components as a project to the Linux Foundation of Energy as a unified approach to developing non-differentiating code that can serve stakeholders and IT development in the field of Energy in a coordinated and efficient manner.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

1 Introduction

The OneNet Framework is based a fully replicable, open, flexible, and scalable architecture that enables the whole European electrical system to operate as a single efficient system provided the secured and trusted connection of energy stakeholders Through a variety of markets OneNet allows the universal participation of stakeholders regardless of their physical location, at every level from small consumer to large producers. Also, by clearly defining stakeholders' interactions and bringing all possible data exchanges to a European level of harmonization, it unlocks extended data and service interoperability among actors, systems and platforms enabling also connectivity for cross-border flexibility markets.

The OneNet results are:

- A data management framework which supports flexibility markets, but also monitors and optimizes the overall European electrical infrastructure.
- A clear and open architecture which enables any player to participate at innovative market structures.
- A smooth integration of the grid and market operation for TSO and DSO in the innovative market structure.
- A new set of customer-centric business models which supports next generation service-based markets.

1.1 Objectives of the Work Reported in this Deliverable

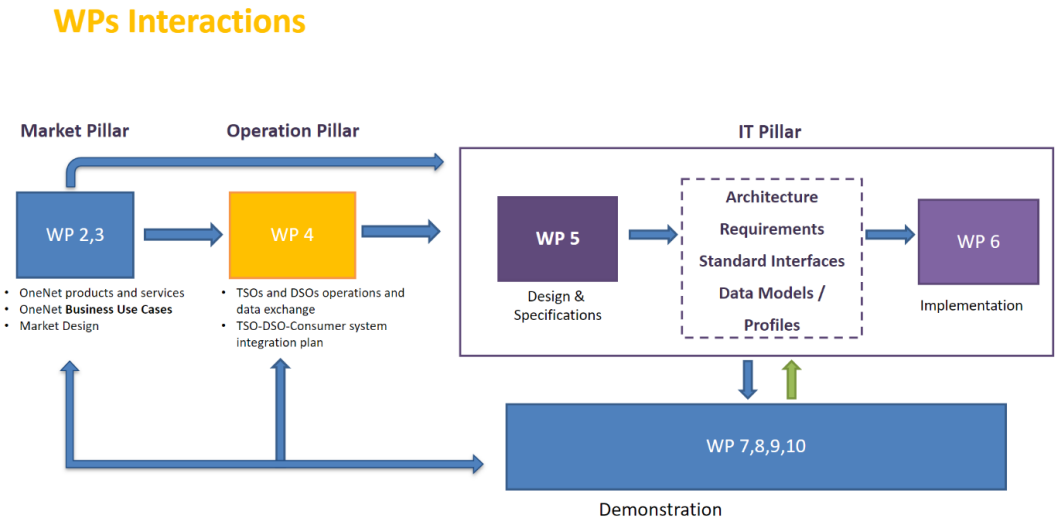


Figure 1: WPs interdependencies in OneNet project

OneNet's WP6, provides for the implementation of the IT pillar, contributed to the development of the OneNet system, starting from the design of the OneNet Reference Architecture described in D5.2 [2] and all the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

necessary requirements and specification provided in the other WP5 tasks. In addition, the WP6 also performed monitoring and evaluation activities during the integration and execution phase, specifically focused on the compliance with the OneNet Reference Architecture and the Cybersecurity aspects.

1.2 Outline of the Deliverable

This report has the following structure:

- **Chapter 2** presents a generic description of the OneNet Framework focusing on the Reference Architecture and the specific software components overall,
- **Chapter 3** presents the components' technical characteristics and architecture focusing on the updates and enhancement from the previous version [5] & [9], as well as the compliance of the architecture with legal, regulatory and privacy requirements for cyber-security,
- **Chapter 4** presents the results of monitoring the evolution and the compliance of the implemented components of the OneNet Framework, with the OneNet Reference Architecture as per D5.2 [2] and D6.7 [11].

The **ANNEX** chapter presents the final version of the OneNet Framework's manuals.

1.3 How to Read this Document

This document shall be read in combination with the deliverables D5.1 [1], D5.2 [2], D5.6 [4] as the OneNet Reference Architecture Implementation is the result of the OneNet Reference Architecture, the Cross-Platform-Services and the Business Objects described in those documents, as well as D6.1 [5], D6.3 [7], D6.4 [8], and D6.5 [9] that describe earlier implementation phases

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

2 OneNet Framework

The analysis of OneNet's architectural approach, as depicted in Figure 2, and its structural aspects as separate software components can be found in Deliverable 5.2 [1]. OneNet relies on a decentralised data interoperability mechanism that serves the purpose of facilitating data exchange. This process aims to support market and network operations but also fosters collaboration among various network operators, such as Transmission System Operators (TSOs), Distribution System Operators (DSOs), as well as stakeholders like prosumers and aggregators.

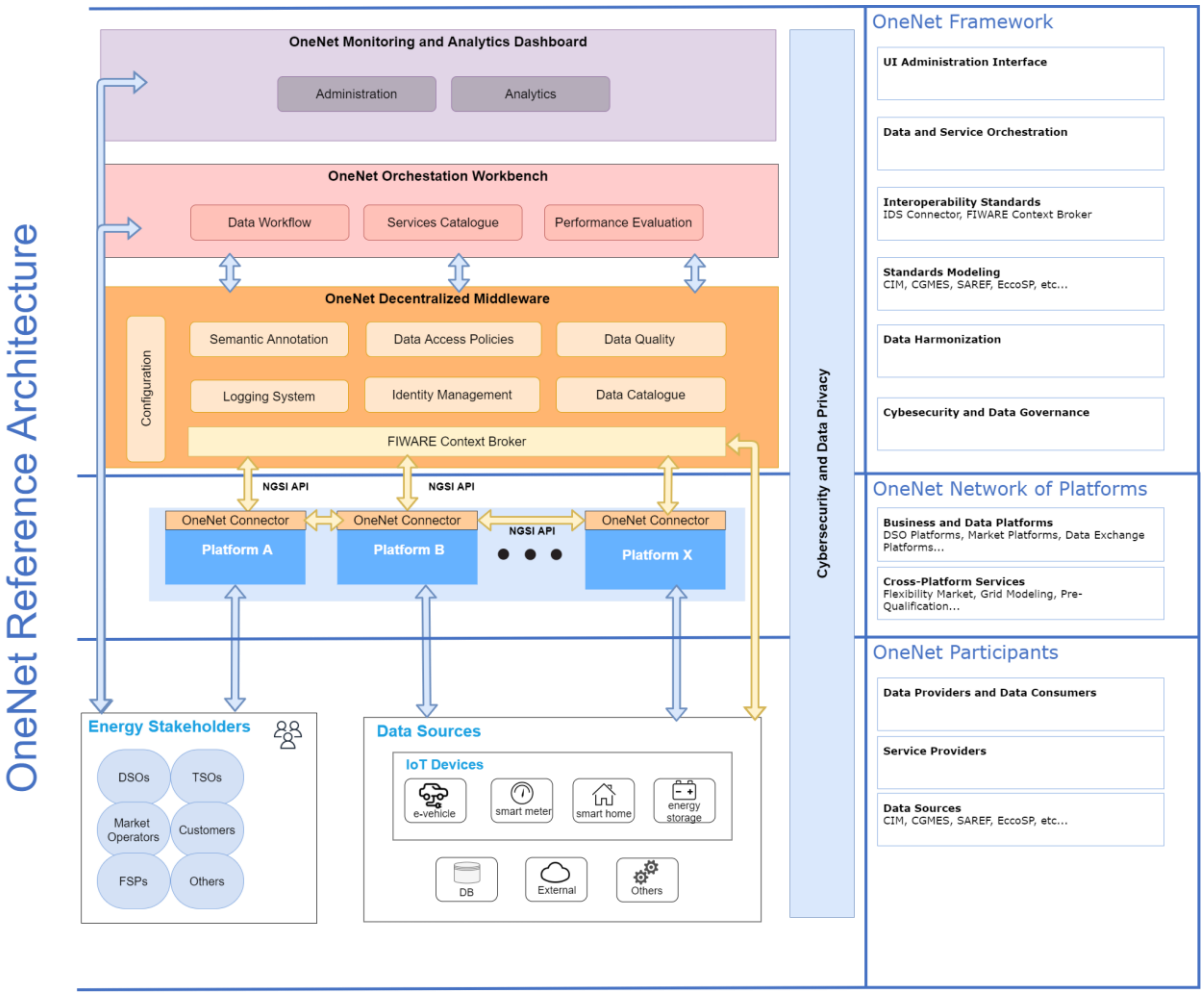


Figure 2: OneNet Reference Architecture

In order to achieve seamless interoperability, several essential characteristics needed to be addressed, including the adoption of open standards and interfaces, ensuring data privacy and regulating data access for each stakeholder, defining standard models and protocols for data exchange, providing robust data management and dataflow monitoring, and establishing robust identification, authentication, and authorization

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

mechanisms. The decentralized approach, along with the use of standardized interfaces and mechanisms, assumes paramount importance to meet these criteria and ensure the necessary scalability for near real-time data integration and management, thereby enabling multi-country and multi-stakeholder near real-time services. The analysis of the IDS reference model and FIWARE interfaces led to the development of a hybrid solution that incorporates standard models for implementing the OneNet Decentralized middleware and the OneNet Connector. The utilization of the IDS Connector and FIWARE Context Broker was identified as the most suitable solution to ensure a high level of standardization, interoperability, scalability, and the potential for reusing the OneNet solution.

OneNet Framework: the core layer of the OneNet Architecture. It consists of three main components, i) the **OneNet Decentralized Middleware**, ii) the **OneNet Orchestration Workbench**, and iii) the **OneNet Monitoring and Analytics Dashboard.** In Chapter 3 below we proceed to provide an explanation of these components within the OneNet Framework as outlined in the Reference Architecture, detailing how these components have been conceptualized with emphasis on overall functionality and important updates.

OneNet Decentralized Middleware: The core component of the OneNet system. It is implemented using a decentralized approach based on the more used and promising standard architecture and interfaces, namely IDS and FIWARE. It allows the integration and collaboration of the OneNet participants, facilitating the cross-platform market and network operations, ensuring scalability and interoperability, while maintaining the data ownership.

OneNet Connector: This is a specific instance of the OneNet Decentralized Middleware, which will be placed inside each platform to facilitate an easy integration and cooperation among the platforms, maintaining the data ownership and preserving access to the data sources.

OneNet Decentralized Middleware and OneNet Connector are strictly linked. The Decentralized Middleware is the middleware that enables the identification of Connectors as well the creation of services and catalogues. The Connector enables the data exchange in an end-to-end way; thus the Connector can be perceived as the Middleware abstracting the central administration components.

OneNet Orchestration Workbench: One of the components of the OneNet system. It acts as a data orchestrator to evaluate the performance and scalability of the cross-platform services that aims to use near real-time IoT metering and Big Data at consumer and/or network level.

The terms **OneNet Framework, OneNet System, OneNet Solution** referred in the present document, as well as in other deliverables of the OneNet project (as included in the reference list) shall be understood as equivalent, i.e. they have the same meaning.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The **OneNet Interoperable Network of Platforms** (defined in D5.2 [2]), is a conceptual layer of the OneNet Architecture (not part of the OneNet Framework) which identifies the "interaction" of the existing platforms, exploiting the OneNet Connector.

Based on the functionality of the final version of the OneNet in conjunction with the Reference Architecture Compliance analysis we can deduce that the overall platform:

- allows **cross-countries participation of stakeholders at all levels**, from TSOs to DSOs, from small consumers to large producers.
- facilitates the platforms integration and cooperation for cross-platform market and network operation services.
- makes available and accessible data from different sources (actors) in a secure and trusted way ensuring data ownership and privacy.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3 OneNet Components

3.1 Decentralized edge-level middleware for scalable platform agnostic data management and exchange

3.1.1 Introduction

The basic objective of Task 6.1 was to create a decentralized edge-level middleware layer enabling the exchange of information between all assets and various components fully integrated in the OneNet Interoperable Network of Platforms. The edge-level middleware includes the following modules:

- Interfaces between involved actors to enable the handling and management of data;
- Semantics layer interface able to support the definition of data sharing requirements and how these will be implemented in the components of the system;
- Data Quality and harmonisation module with a capability to "tag" exchanged datasets with specific parameters as metadata;
- The Linked Data (LD) Context Broker responsible for information context management;
- The Clearing house and Usage Control modules responsible for the data exchange process logging and exchange process policies (contracts) between data produces and consumer.

The OneNet Decentralized Middleware, a fundamental element within the OneNet Framework, functions as a "facilitator" for managing and sharing information. The OneNet Framework comprises of various components which collaborate functionally to support the controlled and administratively regulated exchange of information. It is crucial to emphasize that this framework neither accesses nor processes the data shared by participants in the OneNet system. As a result, data owners retain full control over the sovereignty of their data. The OneNet Decentralized Middleware takes on the responsibility of coordinating specific processes, including identity management, the management of a data catalogue (which includes the administration of the OneNet Cross-Platform Services list), data quality procedures, logging processes, and data access policies (including the discoverability of connectors based on metadata information).

It is important to be noted that all the deployed OneNet Connectors communicate with the OneNet decentralized Middleware via the local data App. From one side the Connector publish essential meta-data descriptions for the available data sources/services (i.e., entities), including information on the persisting policies enabling the discoverability of them by other stakeholders. The availability and accessibility to such entities is performed solely in a decentralized manner via the Connectors. On the other side, the decentralized

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

middleware covers all the administration purposes for user management (integrated with keycloak service), maintenance of cross-platform services, clearing house persistence database (meta-data of transactions, service recordings, policies).

3.1.2 Technical Description and final Updates

The OneNet Connector, as described in D5.2 [1], is the core component capable of enabling decentralized data exchanges in the OneNet ecosystem. The OneNet Connector is a deployment instance of the OneNet Decentralized Middleware and, once deployed and integrated within the platforms of each OneNet participant, it allows a trusted pan-European data space, defined as OneNet Network of Platforms, to be created. The development of the first and intermediate version of the OneNet Connector, guided in Task 6.1 meets all functional and non-functional requirements collected starting from the different use cases described in D5.1 [2] and D5.4 [3]. This chapter contains a general technical overview of the OneNet Connector with the addition of the updates in the intermediate version.

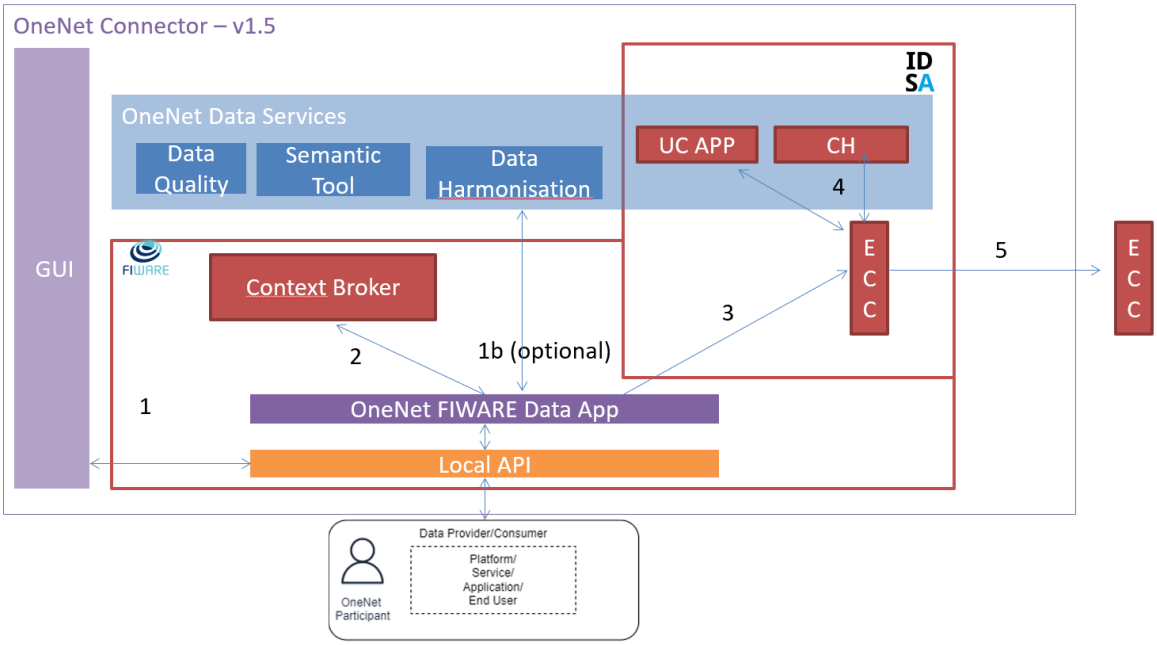


Figure 3: Connector Architecture

As show in Figure 3 (which shows the overall OneNet Connector architecture), the Connector is composed of several components:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- **GUI:** is the graphic interface that allows to configure the OneNet Connector and use the main features. Each OneNet participant can access their own Connector's GUI once installed. The final version of the GUI includes:
  - Registration as data provider / consumer
  - Creation of new data offerings
  - Creation of data entities
  - Registration / consumption of data offerings and data entities
  - Definition of configuration settings for the user and its local OneNet Connector
  - Provision and Subscription of Cross-Platform services (Service Management)
  - Expose OneNet Connector's APIs
  - Several GUI functionality and stability enhancements listed below:

    - A new dashboard (entitled Data Exchanges Timeline) has been added which contains a timeline of activities providing useful information about the user data exchange history.
    - A new card can be found in the dashboard, which is called Connector Check in the main screen, supporting the user in an automated manner to check if connector's configuration is correct. To this end, direct URL checking has been also added in this regard, as well.
    - The OneNet Users has now the capability to send comments to the system administrator on the cross-platform services enabling their continuous update upon request.
    - A specific menu for a dedicated account (i.e., for cross-platform services administrator) has been created to receive and manage the user's comments and accordingly make updates or even create new cross-platform services.
    - In the Connector settings section, a new tab has been added which show to the data producer all the users who consume their data.
    - The User can add a title to an offer service.
    - Service Provider can deactivate a service.
    - Pagination functionality has been added for the 'Provided Data' & 'Consumed Data' lists.
    - The error messaging functionality has been enhanced.
    - The User Interface can now be used also locally.
    - Functional integration with CH and Usage Control
    - Several UI enhancements in performance, stability and security are part of the new Connector version. The general User Experience has been evolved.

- **OneNet Data App**: the main goal of the OneNet data app is to be the entry point of the OneNet Connector. In fact, it provides access to all the main features of the OneNet Connector, including those for data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

exchange, through standard interfaces based on the NGSI-LD REST API[*]. From a technical point of view, the OneNet Data App is developed using a Java Architectural Stack, based on Spring Boot[†] framework and a NoSql database, MongoDB[‡]. All the services made available by the OneNet Data App can be used both from the GUI of the Connector and directly from the external platforms that need to be integrated with the OneNet Connector. The final version of the OneNet Connector Data App implements three main interactions, provided as a standard REST API and available using the GUI (see Annex) or the API interfaces directly. These three interactions are:

  - **Entity creation (Create Entity):** a data provider can create new entities within its own environment and makes them available to all the other OneNet Participants.
  - **Registration / Subscription (Registration)**: a data consumer can register to specific data entities for receiving data in automatic or manual way, after the acceptance of the data provider. The data consumer can register itself to many data providers and many data entities
  - **Data retrieving (Get Entity):** the data consumer, after the registration, can retrieve specific data entity from the data provider.

- **Context Broker**: is the FIWARE component that manages the overall data exchange in the standard NGSI-LD format.
- **IDS-based components**: a series of components and tools, extended from the open-source TRUE Connector, that enable the IDS processes for the data exchange.
  - Execution Core Container (ECC), has the task of implementing IDS-based data exchange processes (authentication, metadata exchange, access control, logging, etc.)
  - Clearing House, logging system of all data exchanges (not available in the first version but being integrated)
  - Usage Control App, module for verifying access and use of data (not available in the first version, but being integrated)
- **OneNet Data services**: additional data services provided by the OneNet Connector not included in previous versions.

Extensive technical details regarding the OneNet Connector, the IDM functionality and the local API implementation are presented in D6.1 [4] along with a detailed technological stack, interfaces and sequence diagrams.

[*] https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.04.01_60/gs_cim009v010401p.pdf

[†] https://spring.io/projects/spring-boot

[‡] https://www.mongodb.com/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.1.3 Architectural Update

The main update related to the OneNet Connector Architecture for the final version was the introduction of an additional layer which is the Local API Layer. In the first version of the OneNet Connector the APIs exposed to the GUI and the external platforms was embedded in the OneNet FIWARE Data App, to provide an access to the FIWARE based functionalities (creation of an entity, subscription and retrieving of an entity). After a more detailed analysis, it was decided to decouple the API layer from the FIWARE Data App, to provide a more independent a generic access to all the features offered by the OneNet Connector. In fact, the new Local API Layer, which was deployed locally in the OneNet Participant environment, can act as an interface for both the central features offered by the middleware (discover of sources and services, vocabularies, etc..) and the data exchange process, implemented in the FIWARE Data App. The specification of OneNet APIs is described in D5.5 [9].

3.2 Data and Service Interoperability, Integration with FIWARE, and Homogenization Management

An important part of the OneNet Connector is the Data Integration & Homogenization sub-layer, which is in charge of managing the end-to-end data exchange process, as well as providing a number of additional data-based services, directly at the connector layer.

The Data Integration & Homogenization sub-layer adopts FIWARE for facilitating the decentralized and interoperable approach in in the implementation of the OneNet Solution and includes the OneNet Data Service Layer.

The Data Services Layers offers three main services for enriching the data-driven aspects of the OneNet Connector:

- Data Homogenization Tool, capable to support the integration of the CIM standards with the FIWARE NGSI-LD information;
- the Clearing House;
- the Usage Control App;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.2.1 Description

A described in D6.3 [7], the Data Integration and Homogenization sub-layer is an important part of the OneNet Connector related to the Data Integration, Homogenization, Access Management and Logging. The Data Integration and Homogenization sub-layer consists of:

- FIWARE Data App (and FIWARE Context Broker)
- Data Homogenization Tool
- Clearing House and Usage Control App (as IDS core services)

FIWARE Data App and Context Broker

The FIWARE Data App and the NGSI-LD Context Broker are two core components of the OneNet connector as can be seen in Figure 4, and it is responsible for implementing the complete end-to-end data exchange process leveraging on the NGSI-LD standard, as well as for offering standardized interfaces for the integration of the external platforms and systems through the OneNet Connector GUI and/or Local API components.

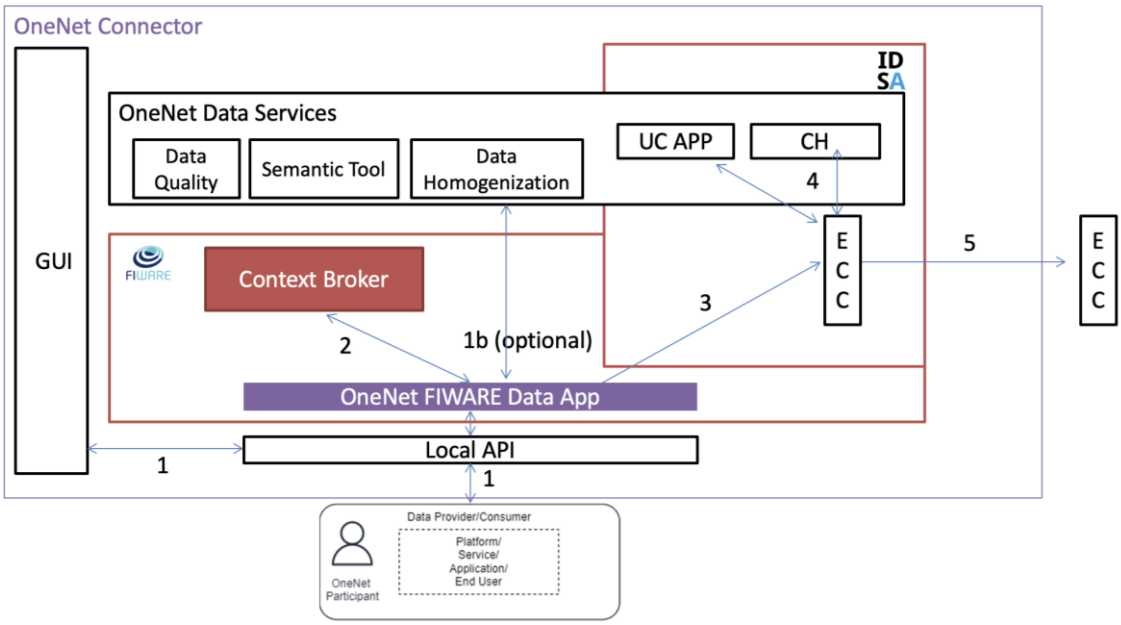


Figure 4 - OneNet FIWARE Data App and Content Broker

The FIWARE Data App is compatible with the NGSI-LD standard, supporting the integration with the NGSI-LD Orion Context Broker as well as with the Execution Core Container of the OneNet Connector (as described in D6.1 [5]) for implementing the IDS-based Data Exchange process.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

In addition, the FIWARE Data App, as part of the Data Integration and Homogenization sublayer is also integrated with the OneNet Data Services, including the Data Homogenization tool, Usage Control App and Clearing House (additional data services were not implemented at this stage).

Data Homogenization Tool

The OneNet Data Homogenization Tool has the purpose of integrating IEC 62325-451 entities with the FIWARE NGSI-LD information model. To perform this integration, its core functionalities include the validation of these entities as well as the conversion from XML or JSON formats into NGSI-LD valid format. This means that not only the previously mentioned data models can be the input of this tool, but it can also accept other data models that conform to XML or JSON format.

As shown in Figure 5 the Data Homogenization tool is part of the OneNet Data services within the OneNet Connector Architecture and it is accessible for the validation and conversion of data into a format that can be accepted by the FIWARE context broker.

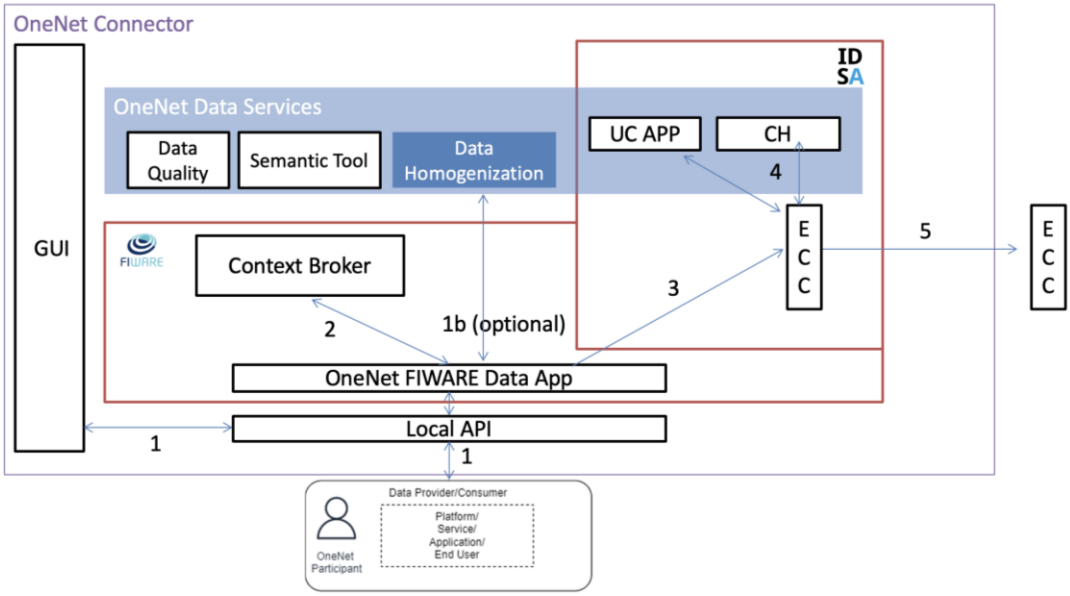


Figure 5: Data Homogenization Tool

Clearing House and Usage Control App

The OneNet Connector offers additional data services based on IDS specifications and guidelines. In fact, the IDSA building blocks for the implementation of the data space includes among other two important components oriented to the data management: the Clearing House and Usage Control.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The Clearing House act as an intermediary that logs all activities performed in the course of data exchange in the IDS ecosystem and it therefore provides clearing and settlement services for all financial and data exchange transactions.

Usage Control App allow to define Usage Policies and Usage Enforcement. Each Data Owner & Data Provider can define usage control policies for their data, attached to the outbound data. Therefore, IDS participants can be sure, that their data are treated according to their usage policies.

Clearing House and Usage Control App are strictly connected in the OneNet Connector implementation, since following the IDS specifications, the Clearing House is able to ensure that Data Provider and Consumer meet their contractual obligations, such as:

- The Data Provider sharing data with the Data Consumer according to Usage Contracts and Data Usage Policies defined.
- The Data Consumer using data according to Usage Contracts and Data Usage Policies defined.

For each data exchange transaction, the OneNet Connector is able to apply the contract negotiation between Data Provider and Consumer (e.g., data access, data usage restrictions, time of validity, etc.) logging all the authorized data transactions, making sure data sovereignty is guaranteed.

In Figure 6 are shown the Clearing House (CH) and Usage Control App (UC App) in the overall OneNet Connector Architecture, as part of the OneNet Connector Data Services.

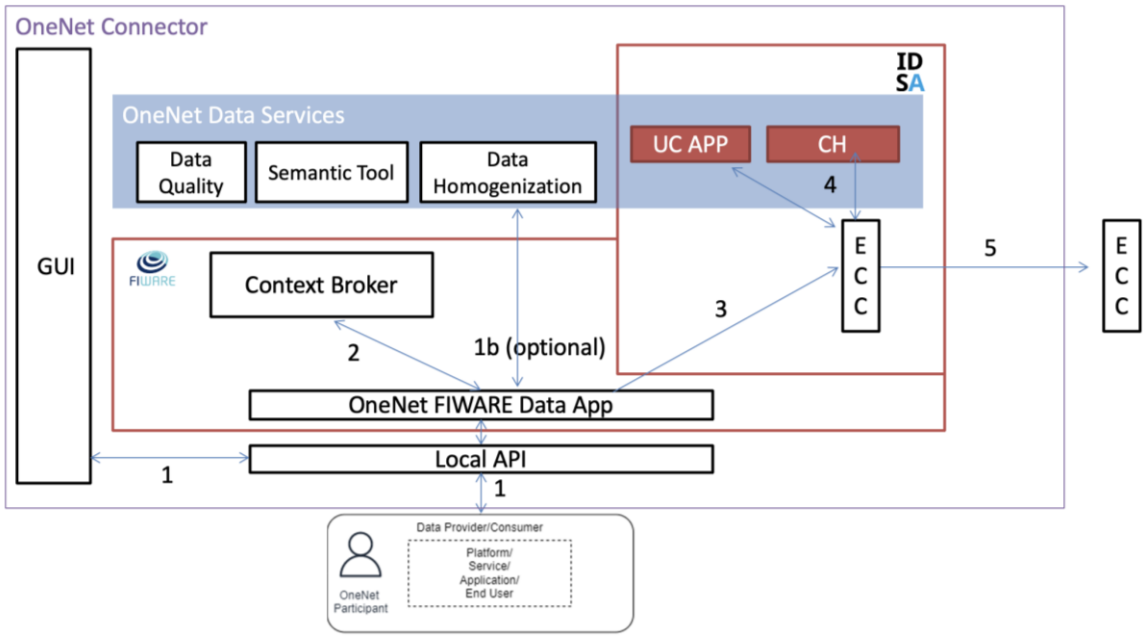


Figure 6: Clearing House (CH) and Usage Control App (UC App)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

3.2.2 New features/functionalities in final version

The final version of the Data Integration and Homogenization sub-layer was released at M34 and integrated in the final version of the OneNet Connector. Below is reported a short summary of the functionalities included in this final version of the components. More details can be found in D6.3 [7].

FIWARE Data App and Context Broker

In order to implement the creation of Data Offering in the Data Catalogue the FIWARE Data App supports the creation and retrieving of data entities through three main functionalities:

- ***Create Entity***: a Data Provider can create new entities (in a specific data offering) within its own environment and makes them available to all the other OneNet Participants.
- ***Registration***: a Data Consumer can register to specific data offering (and related data entities) for receiving data in automatic or manual way, after the acceptance of the Data Provider. The Data Consumer can register itself to many data providers and many data offerings.
- ***Get Entity***: the Data Consumer, after the registration, can retrieve specific data entity from the data offering.

The entity creation and the consumer registration are implemented using the FIWARE Data App and the FIWARE Context Broker.

The retrieving of a specific entity is instead implemented passing through the IDS services of the OneNet Connector (mainly the Execution Core Container) ensuring the decentralization of the data exchange and the application of the IDS information model, security and privacy aspects.

Data Homogenization Tool

The Data Homogenization tool implements two main functionalities: the validation and conversion of market data entities. Upon reception of an XML or JSON entity, a validation of the data is applied for ensuring the compliance with the IEC 62325-451 standard. Successful validation facilitates subsequent entity conversion to NGSI-LD.

Validation

Request data is validated before conversion into NGSI-LD format. The tool offers a specific API for validation only. The API check whether an entity corresponds to the IEC standard. On successful entity validation, the API returns the HTTP status code 200 [OK] to confirm the validity of the request data.

Conversion

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Figure 7 illustrates the data conversion flow of the data homogenization tool. An entity (XML or JSON format) is sent to the API with a POST request, it gets validated and converted into NGSI-LD format. After successful conversion, the converted entity is returned, facilitating entity storage in the FIWARE context broker.

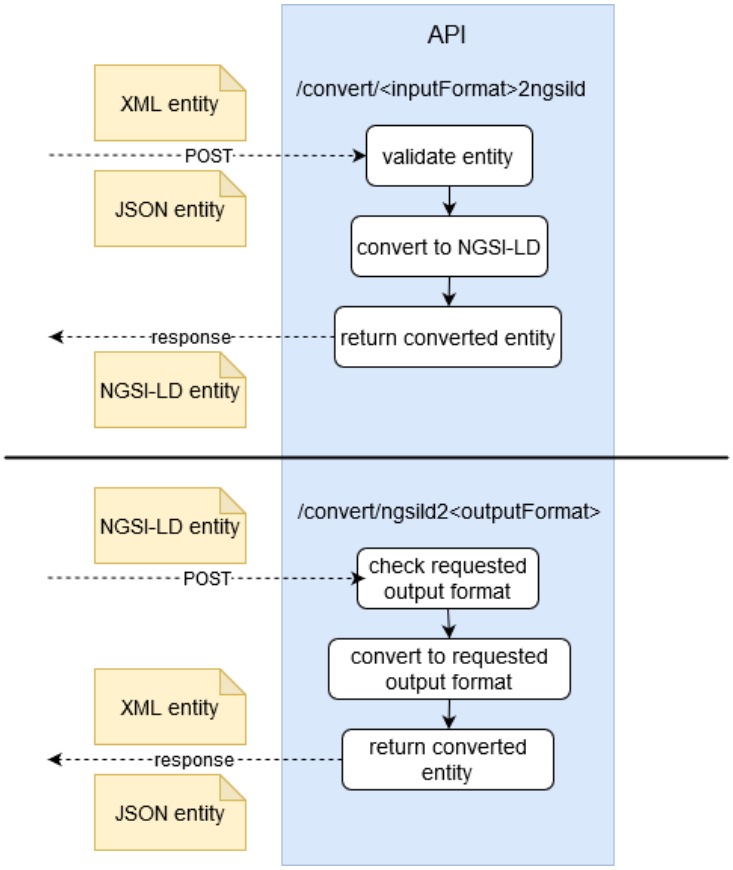


Figure 7 – Data conversion flow

The lower half of Figure 7 illustrates reconversion from NGSI-LD format: the POST request includes the entity to convert, the format to convert to is determined by the API endpoint which is addressed in the request. The entity in NGSI-LD format is then converted to the requested format (XML or JSON) and returned to the caller of the API.

Clearing House

The OneNet Clearing House is implemented starting from the Fraunhofer IDS Clearing House and take advantage of its main functionalities.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- The logging-service is capable to store data in the Clearing House in encrypted way and make them practically immutable (it requires an access token to be retrieved and decrypted)
- The document-api allow to retrieve encrypted logs via REST APIs and to decrypt them using validated tokens.

In addition, the OneNet Clearing House is also:

- completely integrated in the FIWARE Data App and could be enabled/disabled from config file.
- requires a valid DAPS certificate for logging system and data retrieving, as well as a contract negotiation between provider and consumer
- The contract negotiation is automatically activated during the registration phase within the FIWARE Data App
- OneNet Connector is able to log any data exchange both at consumer and provider level.

Usage Control App

The OneNet Usage Control App is implemented starting from the open-source IDS Dataspace Connector. In addition, it includes the following new functionalities:

- REST API to get, upload and remove the Contract Agreements from the Contract Agreements storage. The format of these Contract Agreements is the one specified by the IDS Information Model. These contracts will be used to apply the Data Usage Control enforcement.
- REST API to apply the Data Usage Control enforcement on the input data according to the Contract Agreements related to the pair consumer-producer indicated as input parameters.
- Policy Enforcement, the Usage Control module supports usage policies written in the IDS Usage Control Language based on ODRL.
- A new policy is supported which indicates if the data contains Personal Data

3.3 OneNet Orchestration Workbench to support integration and evaluation of data-driven services

As described in D6.4 [**Error! Reference source not found.**] the OneNet System consists of three main components. In addition to the OneNet Decentralized Middleware (which include the OneNet Connector) that is at the base of the data exchange, there are two additional components that enrich the OneNet offer for the integration, monitoring and evaluation of data and services.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Among these, the OneNet Orchestration Workbench allows to interconnect the OneNet Network of Platforms with specific data-driven services to be tested and evaluated in the Workbench environment.

3.3.1 Description

The OneNet Orchestration Workbench is able to orchestrate and evaluate the performance and scalability of the cross-platform services that are being integrated and implemented in the OneNet System.

Any OneNet Participant and in particular the Service Providers is able to deploy, test and evaluate a specific service, integrating data coming from the OneNet Connector and to implement a data pipeline orchestration, supported by analytics and data visualisation features.

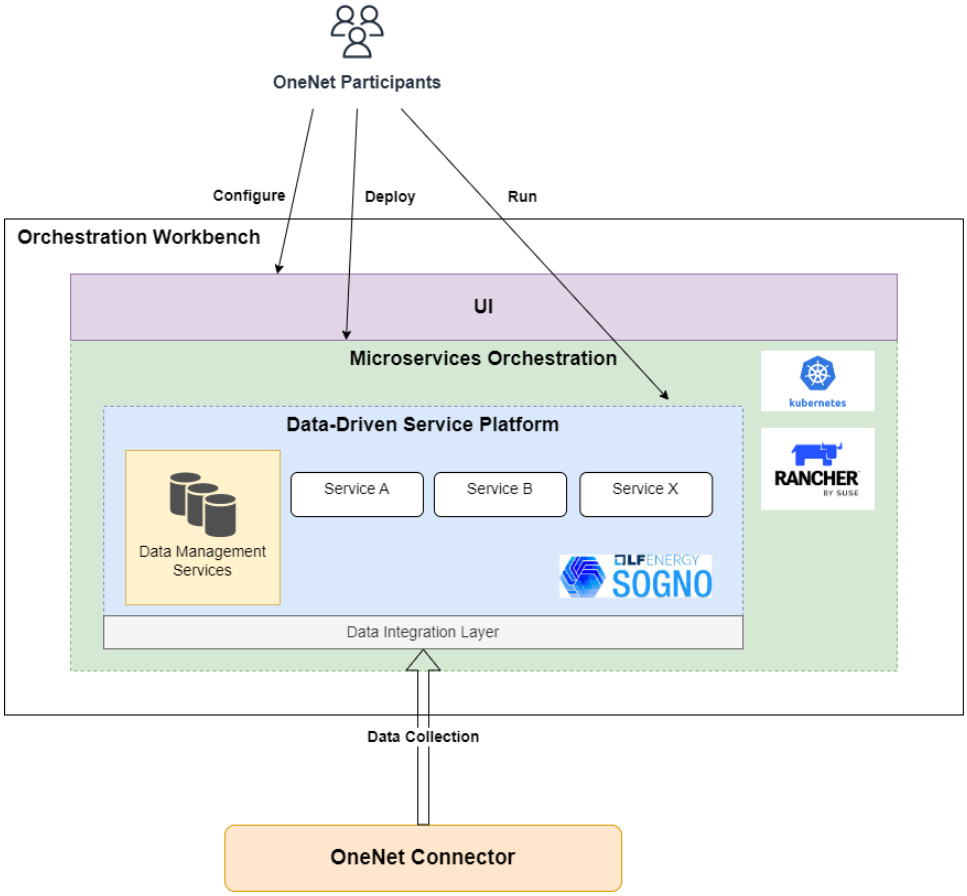


Figure 8 - OneNet Orchestration Workbench

The OneNet Orchestration Workbench consists of a four-layer architecture:

- **UI Layer**: access for configuration and visualization of services and data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- **Microservice Orchestration Layer**: based on Rancher 2.0 and Kubernetes, allows the deployment and orchestration of services.
- **Service Platform Layer**: based the Linux Foundation Energy (LFE) SOGNO[§] platform, allows to integrate data (Data Management Services) and run the deployed services; and
- **Data Integration Layer**: integrates the OneNet Connector data sources via APIs and create a bridge with the Service Platform

The OneNet Orchestration Workbench architecture is shown in Figure 8.

3.3.2 New features/functionalities in final version

The OneNet Orchestration Workbench was released in two versions:

- First release in January 2023, reported in MS16.
- Final release in July 2023, reported in D6.4 [8].

Below is reported a short summary of the functionalities included in this final version of the components. More details can be found in D6.4 [8].

The OneNet Orchestration Workbench provides a Graphical User Interface (GUI) with the following sections:

- Login, the OneNet Participant can login through OneNet credentials (OneNet Identity Manager).
- Service Catalogue, the OneNet Participant can explore the service catalogue for testing one of the services.
- Service Deployment, the OneNet Participant can Deploy and Orchestrate services.
- Running and Testing, the OneNet Participant can integrate data coming from the OneNet Connector in a specific service, run it and test it, evaluating its performance exploiting SLAs tracking, analytics, alerting and notification.
- Data Visualization, the OneNet Participant can monitor the services and the data injected (e.g., measurement and grid topology)

A typical workflow in the OneNet Orchestration Workbench is shown in Figure 9 and includes:

- OneNet Participant (Data Provider) can **create new data** using its own connector.
- OneNet Participant (Data Consumer) can **subscribe/consume data** using its own connector.
- OneNet Participant (Service Provider) can **deploy a data-driven service.**

[§] https://lfenergy.org/projects/sogno/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

- OneNet Participant (Data Consumer) can **run services** using consumed data.

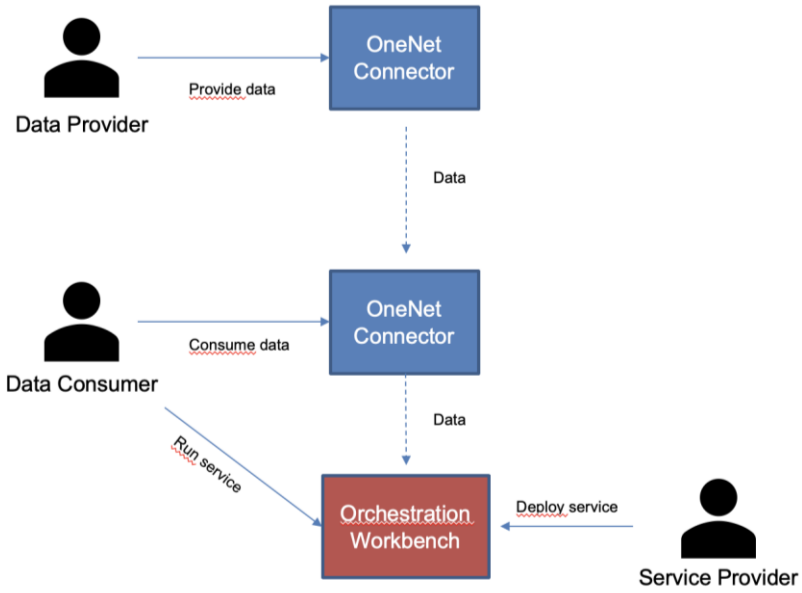


Figure 9 - typical workflow in the OneNet Orchestration Workbench

3.4 Legal, Regulatory, Privacy and Cybersecurity Management & Compliance Tools

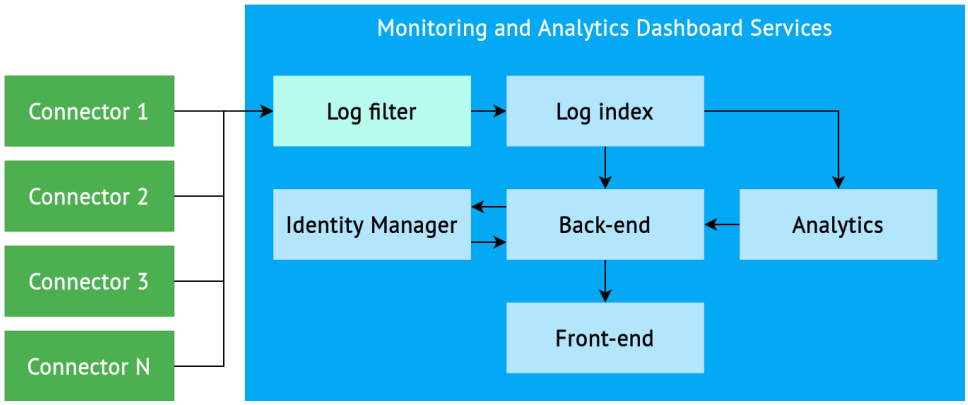


Figure 10 - OneNet Monitoring and Analytics Dashboard service architecture

This section provides an overview of the tools comprising the OneNet Monitoring and Analytics Dashboard, which provides historical as well as real-time analytics by monitoring, filtering and processing logs from all connectors participating in the OneNet Interoperable Network of Platforms. The following figure depicts the architecture of the OneNet Monitoring and Analytics Dashboard. The reader is referred to D6.4 [8] for a detailed

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

description of the services architecture and their interconnection. Furthermore, deliverable D6.6 [10] offers a comprehensive presentation of the features, functionality and implementation of the first version of the OneNet Monitoring and Analytics Dashboard.

3.4.1 Description

The cornerstone of the OneNet Monitoring and Analytics Dashboard functionality is security through analytics. Core features include a data analytics dashboard that displays various information regarding connector usage arranged in a number of charts. Charts depict data such as number of requests per country, number of requests per day, live monitoring of requests, data sent over time and response codes over time. Another feature of the dashboard is anomaly detection, which allows dashboard users to monitor the activity of potentially malicious clients detected by an anomaly detection machine learning model. The dashboard also offers the ability to generate a security report based on the results of the anomaly detection algorithm and to use the advanced filtering tool to query any connector logs which fulfil certain criteria. Finally, it provides alerting functionality as well as administrative and configuration tools for OneNet participants through the account management page.

To achieve security through analytics, OneNet Connectors are configured to forward their logs to a specific endpoint of the OneNet Monitoring and Analytics Dashboard infrastructure. Incoming connector logs are filtered and transformed using Logstash and indexed using ElasticSearch to facilitate queries. Next, the aforementioned Dashboard functionality is implemented collectively by a number of tools and components using the indexed connector logs.

First, the OneNet Network Traffic & Endpoint Infrastructure Monitoring Tool is responsible for the aggregation and visualization of both historical and real-time data regarding Connector access and usage. A Spring Boot back-end service has been implemented which interfaces with the ElasticSearch instance using its Java API to perform complex queries and exposes endpoints to be used by the Dashboard front-end service.

Furthermore, the Keycloak Identity and Access Management tool has been integrated through the Spring Boot back-end. It utilizes the JSON Web Tokens provided and managed by Keycloak to secure the available endpoints and also to provide endpoints for authentication and authorization purposes.

Second, the OneNet Data Analysis, Rating & Classification Tool leverages the information extracted from collected logs to train a machine learning model which utilizes the Isolation Forest algorithm to detect anomalous client behaviour.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The Dashboard Graphical User Interface was developed using Angular, the Angular Material UI Component library and two libraries, ApexCharts.js and amCharts 5, for data visualization purposes. We also leverage Keycloak for its native account administration and configuration capabilities. Through the Account Management Console, the user may edit their personal information and credentials, as well as track and manage device and application activity.

Within the overall OneNet architecture, the OneNet Monitoring and Analytics Dashboard enhances the collection of services offered by the OneNet Interoperable Network of Platforms by providing a platform that procures monitoring, alerting and analytics data visualization for OneNet participants. The provided tools also facilitate the review and assessment of the behaviour of potentially malicious clients, which offers valuable aid in the decision-making of the OneNet administrator. Finally, the automated machine learning-based rating and classification mechanisms exemplify how machine learning can be employed to augment the cybersecurity aspect of the OneNet system.

3.4.2 New features/functionalities in final version

One of the new features implemented in the final version of the OneNet Monitoring and Analytics Dashboard is advanced filtering, which allows submitting queries for connector logs that fulfil certain criteria and receiving non-aggregated results. Through advanced filtering, the Dashboard user can narrow down their search for connector logs and refine their selection of results for a more specific analysis.

In the back-end, advanced filtering is implemented through the creation of a new API endpoint, `POST /monitoring/network/advanced-filtering`, which accepts a number of fields representing criteria and their values in its request body. Depending on which search criteria were specified by the user or not, the appropriate ElasticSearch query is constructed. Finally, it executes the query and returns the list of results. Each result represents a connector log and its respective related information.

In the front-end, the advanced filtering page is accessible through the navigation sidebar of the OneNet Monitoring and Analytics Dashboard. On the left side of the advanced filtering page, there is a set of labelled input boxes which allow the user to set a number of filter criteria before executing the search query. The following search criteria are available:

- Date range
- Request method
- Response size range
- Response code
- Client IP address
- Country

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The right side of the page is where the search results are rendered. Results are initially folded, and each result may be expanded when clicked on to reveal all available information. Each result includes the following information:

- Timestamp
- Connector ID
- Request path
- Request size
- Request method
- Response code
- Response size
- Client IP address
- Country and city
- Operating system
- Browser

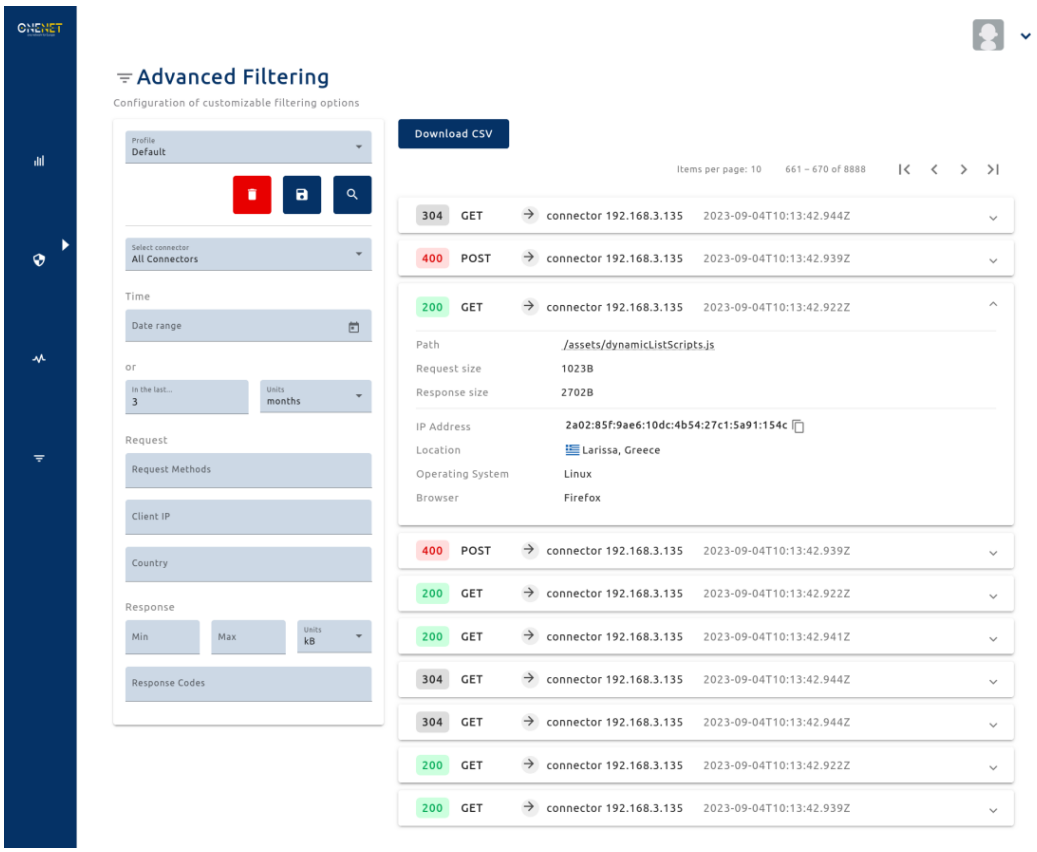


Figure 11 - The advanced filtering page of the OneNet Monitoring and Analytics Dashboard

Furthermore, it is possible to save any advanced filtering configuration so that it may be reused in the future. By clicking on the save button under Profile, the user is presented with a dialog where they may enter a

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

descriptive name for their current profile. Advanced filtering profiles are stored in the browser local storage. Saved profiles may be accessed through the profile selection menu as seen below.

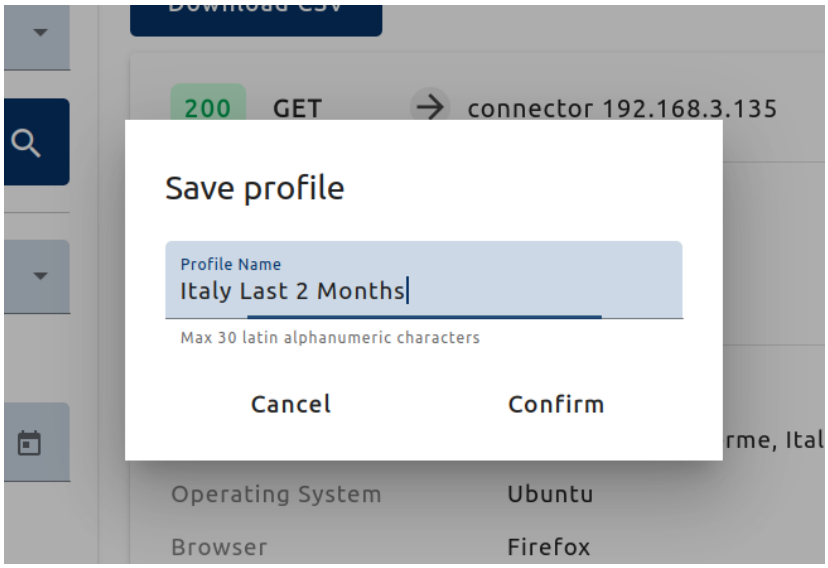


Figure 12 - The advanced filtering profile save dialog

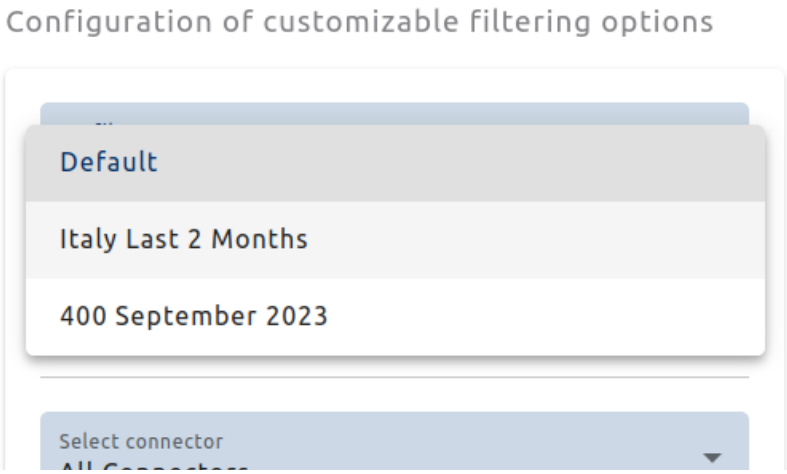


Figure 13 - The advanced filtering profile selection menu

The next feature included in the final version of the Dashboard is the exporting of analytics results. Data from charts, the security report page and advanced filtering results can be exported to CSV and downloaded directly through the browser. Charts include more exporting options, such as downloading a still image of the chart in PNG or SVG format.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

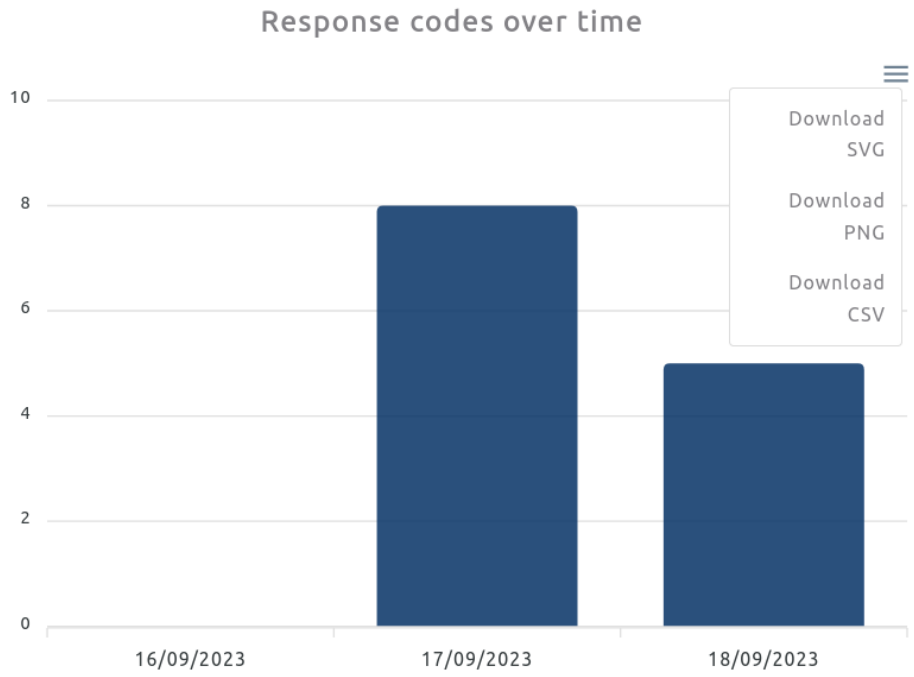


Figure 14 - The export and download menu of the Response codes over time chart of the Dashboard

Timestamp	Connector	Request Method	Request Path	Content Length	Response Code	Bytes Sent	Client IP	Operating System	Browser	Country Code	Country	City
2023-08-15T15:42:54.913Z	192.168.3.135	GET	/api/info/version	1170	200	28	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.912Z	192.168.3.135	GET	/api/info-card/dynamic-javascript/50c2	1746	200	788	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.911Z	192.168.3.135	GET	/api/info-card/by-id?id=67fff749-1b82-	1258	200	541	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.912Z	192.168.3.135	GET	/api/custom-query/data-objects/?id=e	1280	200	290	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.911Z	192.168.3.135	GET	/api/info-card/by-id?id=963afe17-fb48	1258	200	545	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.912Z	192.168.3.135	GET	/api/info-card/dynamic-javascript/62e	1750	200	4024	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.912Z	192.168.3.135	GET	/api/info-card/dynamic-javascript/67ff	1748	200	788	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.911Z	192.168.3.135	GET	/api/info-card/by-id?id=50c25b58-1d4	1258	200	590	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.912Z	192.168.3.135	GET	/api/info-card/dynamic-javascripts/fac	1668	200	779	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.912Z	192.168.3.135	GET	/api/info-card/dynamic-javascript/822	1746	200	788	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.912Z	192.168.3.135	GET	/api/info-card/dynamic-javascript/07bf	1748	200	788	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.911Z	192.168.3.135	GET	/api/settings/sidebar-image	1196	200	10434	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.911Z	192.168.3.135	GET	/api/info-card/by-id?id=07bf99ed-80ea	1258	200	545	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.911Z	192.168.3.135	GET	/api/info-card/by-id?id=62e528c2-971f	1260	200	5348	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.911Z	192.168.3.135	GET	/api/dashboard/by-id?id=b9b1394b-42	1260	200	1708	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.911Z	192.168.3.135	GET	/api/info-card/by-id?id=8228f43d-327d	1258	200	569	45.14.71.9	Linux	Firefox	JP	Japan	Osaka
2023-08-15T15:42:52.912Z	192.168.3.135	GET	/api/info-card/dynamic-javascript/963	1746	200	788	45.14.71.9	Linux	Firefox	JP	Japan	Osaka

Figure 15 - The exported CSV of an advanced filtering query displayed using the LibreOffice Calc program.

Next, a connector health page has been added to the Dashboard. Its main purpose is to display the health status of each connector IP address detected in the logs. Based on the latest log received, each connector is classified as Online if a recent log (within the last week) exists, Idle if a log within the last 60 days exists and offline otherwise.

For this purpose, in the back-end, a new endpoint, GET /monitoring/network/connectors-health-check, was implemented which returns every unique Connector IP and the respective timestamp of the last log received. In the front-end these results are displayed in a list where a circular icon is used to display the health status: Green for Online, orange for Idle, grey for Offline. Next to this icon, the IP of the Connector and the date and time of the last received log are printed.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

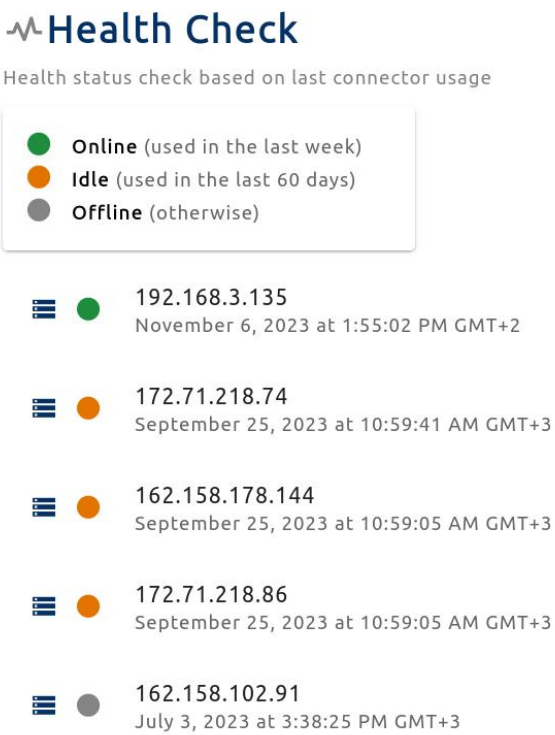


Figure 16 - Health check page results

Finally, alerting functionality has been integrated in the Dashboard. Using Server-Sent Events, a new endpoint, GET /alerts/latest-alert-sse, has been implemented for receiving updates regarding abnormal clients. Caching of abnormal IPs takes place in the back-end so that the anomaly detection endpoint is not hit more than once per 2 minutes, which is the time required for each consecutive model prediction. In the front-end, abnormal IPs are stored in memory and also browser local storage. An alert is shown only when the difference between the last and current updates contains new abnormal client IPs. As a result, the user receives notifications that direct them to the security report whenever a new abnormal client is detected by the anomaly detection algorithm.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

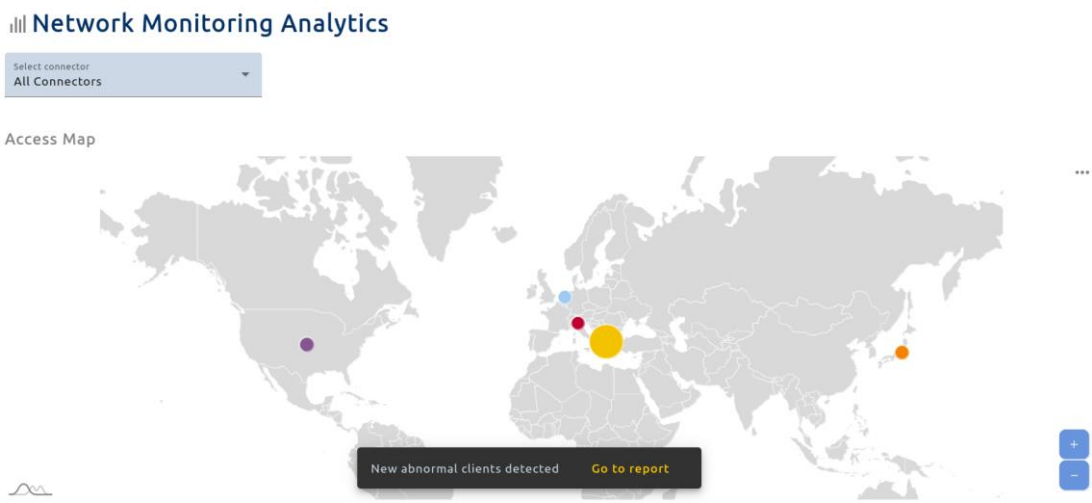


Figure 17 - An alert at the bottom of the page that notifies of new abnormal clients and directs the user to the security report

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

4 Tools evolution and compliance with OneNet Reference Architecture

Within Task 6.7 was defined a standard methodology for integrating and evaluating components compliance with the OneNet reference architecture. As first step, a review of various approaches for the software integration and reference architecture compliance was identified and the selected approach was reported in D6.7 [11] at M15 (December 2021) of the project.

In the following period an iterative approach was implemented for evaluating the quality and compliance of the tools implemented in WP6 and integrated within the overall OneNet system. This iterative approach is described in the next paragraph.

4.1 Methodology

The methodology for monitoring the tools evolution and their compliance with the OneNet Reference Architecture, followed an iterative approach in line with the implementation one, based on three releasees of the software:

- first release of the software in July 2022,
- intermediate release in January 2023
- final release in July 2023.

The selected methodology, described more in detail in D6.7 [11] foreseen seven different steps:

1. Review of business goals & functional requirements
2. Review Software Component/Tool architecture
3. Create/update the component quality attribute tree matrix
4. Review the architectural approaches & the quality attribute utility tree
5. Brainstorm and prioritize scenarios
6. Analyse the architectural approaches
7. Capture the results & create final compliance report

Some of these steps were iterated after each release of the software:

1. Review of implemented functional requirements.
2. Update the component quality attribute tree matrix.
3. Brainstorm and prioritize next implementation and evaluation.
4. Check the results & create report.

The results of each iteration led to an evolution (based on prioritized requirements) and a consolidation (based on the compliance with the architecture and the integration results) of the implemented tools.

All the activities conducted have been tracked and the final outcomes are included in Ch. 4.2 and Ch. 4.3.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

4.1.1 List of tools and components

The OneNet Reference Architecture described the implementation of the overall OneNet systems, which consists of several tools and components.

All these tools and components must be integrated in a compliant way with the OneNet Reference Architecture, satisfying all the specific functional requirements and business goals elicited during the design phase (see D5.1 [1]) and enhanced during the preliminary stage of the implementation phase (see D6.1 [5]).

Below is reported the list of tools taken into account for the implementation of the overall OneNet system and for the evaluation of the requirements and compliance with the architecture. More details about the tools are described in D6.7 [11].

- OneNet Decentralised Middleware (and OneNet Connector)
    - Context Broker
    - Vocabulary provider, Semantic Tools and Services
    - Identity Provider and Management (Authentication & Authorization)
    - Data Access Control (Usage Control)
    - Clearing House
    - Data Quality Tool
    - User Interface
- OneNet Orchestration Workbench
    - Data Process Management (Orchestration & Workflow)
    - Service Management
    - Performance Evaluation
- OneNet Monitoring & Analytics Dashboard
    - Administration
    - Analytics & KPIs
- Cyber-security & Data Privacy
    - Network Traffic & Endpoint Infrastructure Monitoring
    - Data Analysis, Rating & Classification

4.2 Business Goals and Functional Requirements

This chapter reports the analysis of the business goals and requirements expected for the overall OneNet System.

The first activities conducted for monitoring the advancement of the components´ development and integration within the OneNet Architecture was reporting the status of the developed components. Table 4.1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

reports the list of components and the status on the three main release: first release of the system in September 2022, intermediate release on January 2023 and final release on July 2023.

Table 4.1 – OneNet Framework Components – Per-release information

Tool/Component	Responsible	Sept 2022	Jan 2023	July 2023
OneNet Decentralised Middleware (and OneNet Connector)				
Context Broker (and FIWARE Data App)	ENG	First Release	Not updated	Final Release, updated version of the FIWARE Data App
Vocabulary provider, Semantic Tools and Services	ED	First Release	Updated	New entries have been added in the OneNet Cross-Platform services, based on demo needs.
Identity Provider and Management (Authentication & Authorization)	ED/UBE/ENG	First Release (partially, user/pass)	Updated (Keycloak)	Integration of DAPS Certificates
Data Access Control (Usage Control)	ED/ENG	First Release (partially, only data access control)	Updated	Final Release (Usage Control App integrated in the OneNet Connector + Control rules in the cross-platform services)
Clearing House	ENG	No	Minor enhancements	First release of the CH (already integrated with the OneNet Connector). The data exchange timeline has been further enhanced to include more attributes for the occurred transactions
Data Quality Tool	ED/ENG	No	No	Considering that Demo partners has been extensively basing their data exchange on custom profiles, this feature shall be part of a central, yet, external (SaaS) at the Workbench layer, provided by external service providers.
User Interface	ED	First Release	Updated	Final Release
OneNet Orchestration Workbench				
Data Process Management (Orchestration & Workflow)	ENG	No	First Release	Final Release

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Service Management	ENG	No	First Release	Final Release
Performance Evaluation	ENG	No	No	Integrated
OneNet Monitoring and Analytics Dashboard				
Administration	UBE	No	First Release	Final Release
Analytics & KPIs	UBE	No	First Release	Final Release
Cybersecurity and Data Privacy				
Network Traffic & Endpoint Infrastructure Monitoring	UBE	No	First Release	Final Release
Data Analysis, Rating & Classification	UBE	No	First Release	Final Release

The second main activities conducted was tracking the advancement on the satisfaction of the functional requirement in the different release. (see also D6.1 [5] p.37ff).

Table 4.2 below reports the final status of the functional requirements (as such functional requirement are reported in D6.1 p. 37ff 58[5]).

Table 4.2 - Functional Requirements Status

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
Configuration			
FRIDS01b.7	Configuration of OneNet Connector: Configure data format/ semantic annotation	OneNet Participants have to be able to select the data formats and configure semantic annotation to be applied by the OneNet Connector so that data is harmonized (via OneNet Connector GUI)	Done
FRIDS02b.8	Configuration of OneNet Connector: Configure data quality	OneNet Participants have to be able to select and configure data quality requirements and data quality checks to be applied by the OneNet Connector on outgoing data (via OneNet Connector dashboard)	Not implemented, such data specific data processing shall take place upon a data retrieval and handled by third party service providers, potentially hosted at Workbench.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
FRIDS02b.6	Configuration of OneNet Connector: Configuration of transaction logging	OneNet Participants have to be able to configure transaction logging (activate/ deactivate, logging intensity and details etc.) of the OneNet Connector (via OneNet Connector dashboard)	Done
FRIDS02b.7	Configuration of OneNet Connector: Configuration of data reception endpoints	OneNet Participants have to be able to configure data reception endpoints in their systems/ platforms to subscribe themselves to the OneNet Connector context broker and receive incoming data in their systems	Done
FRIDS02b.9	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model- General information	Service provider to define general information including connector type, version, timestamp of last change made to the configuration, configuration, name of contact person	Done
FRIDS02b.10	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model- Lifecycle- Data Flow	Service provider to define the configuration of tasks and connections established by the Data Router between the Data Services and the Data Bus (i.e., Networking: ports/IPs, for internal and external connections, Security: SSL certificates or publics keys, Compliance/Data Sovereignty: rules before connector deployment (preventing incorrect configuration)	Done
FRIDS01b.6	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model- Service Configuration	App service provider to define how configuration parameters for Data services or other connector components have to be set, i.e., metadata describing datatypes for input/output among different components.	Done

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
Data Catalogue			
FFRA03.8	Middleware Features: Available services and data sources discovery	The middleware must allow to discovery for data sources	Done
Identity Management			
FFRA03.9	Middleware Features: Registration of the OneNet Connector	The middleware must allow to uniquely identify each OneNet connector	Done
FFRA05.3	Cybersecurity: Ensuring that all the processes can be uniquely identified and related to a specific user		Done
FRC12	IDS-based Service: Identity Management	OneNet Connector is able to verify the identity of the participants	Done
FRIDS01b.4	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model- Publishing: Identity Management	Proper identity management interface closely to integrated with the connector defining the Identity Provider	Done
REST APIs			
FRUC01a	Data exchange through REST APIs: Exchange harmonized payload data	OneNet Participants have to be able to exchange harmonized payload data between OneNet Connectors using OneNet REST APIs	Done
FRUC01b	Data exchange through REST APIs: Authentication in OneNet System	OneNet Participants have to be able to authenticate themselves/ their platform/ system for exchanges through the OneNet Middleware	Done
FRUC01c	Data exchange through REST APIs: Data Retrieval	OneNet Participants can retrieve data from a specific data source.	Done
FFRA02.1	Platforms integration: Platforms are able to connect with the OneNet Framework	OneNet Connector must be able to connect any kind of Platforms using REST APIs	Done
FFRA03.1	Middleware Features: Any Data sources is integrable with OneNet Middleware		Done
FFRA03.6	Middleware Features: Interfaces for reading/writing data	The middleware must provide standard interfaces for reading/writing data	Done

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
FRC05	Data Exchange: Publish Data	Publish new data using the Connector	Done
FRC06	Data Exchange: Subscribe as service consumer	Register as consumer to a specific service	Done
FRC07	Data Exchange: Subscribe to a data source	Register as consumer as subscriber (publish/subscribe mechanism)	Done
FRC08	Data Exchange: Retrieve data	Retrieve data from a specific data source	Done
User Interface			
FRUC03a	Monitor OneNet Connector status: Monitor network traffic	OneNet Participants have to be able to monitor the network traffic between their own OneNet Connector and other OneNet Connectors and have to be notified about potential security breaches (metrics to be defined) through the OneNet Connector dashboard.	Done Connection with the Context Broker via reverse proxy (Logs)
FRUC03b	Monitor OneNet Connector status: Monitor known data sources	OneNet Participants have to be able to monitor the connected data sources (other OneNet Participants and their Connectors) and the current authentication and authorization status through the OneNet Connector dashboard; sensitive information should only be exposed if a OneNet Participant agrees	Done
FRUC03c	Monitor OneNet Connector status: Monitor health status	OneNet Participants have to be able to monitor the health status of their OneNet Connector and the included active data services through the OneNet Connector dashboard.	Done
FRUC03d	Monitor OneNet Connector status: Monitor transaction logs	OneNet Participants have to be able to monitor the transaction logs through the OneNet Connector dashboard	Done

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
FRUC04	Software update	OneNet Participants have to be able to update the software of the OneNet Connector or any of these modules.	Done
FRUC05	Browse and test REST API endpoints	OneNet Participants have to be able to browse and test REST API endpoints of the OneNet APIs through the OneNet Connector dashboard.	Done
FRC01	Registration and Configuration: Registering as OneNet Participant		Done
FRC02	Registration and Configuration: Discovery/search data sources		Done
FRC03	Registration and Configuration: Change configuration settings		Done
FRC04	Registration and Configuration: Register new data source	Register an endpoint for making available a set of data.	Done
FRC10	IDS-based Service: Usage Control - Policy definition	Data Provider is able to define policies for a specific data source	Done
FRC16	File Upload	OneNet Participant are able to upload files and use them as data sources using the Connector GUI.	Done
FRIDS01c.3	ONBOARDING_Security Setup: IDS Consumer/Provider configures data access restrictions	Connector provide appropriate functionality for Data Provider or Data Consumer to configure custom access restrictions for bilateral communications; The Data Provider may serve the same data using different representations or pricing options, so the Data Consumer may select a suitable offer from the Data Provider's Connector description.	Done. No pricing option or different representation implemented.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
FRIDS03b.1	PUBLISHING AND USING DATA APPS_Use Data App: App User UI to search for available Data Apps	App User UI to search for available Data Apps	Implemented at the OneNet Workbench.
Clearing House			
FRC09	IDS-based Service: Clearing House	All the data transactions are logged in	Done
FRIDS01b.6	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model- Publishing: Clearing	Connector to provide interface to describe which Clearing House should be informed regarding a certain data exchange transaction	Done
FRIDS02b.6	EXCHANGE OF DATA_Invoke Data Operation: Notification of data operation call at clearing House	Upon data consumer request for data a notification is sent at clearing house for logging data operation request	Done
FRIDS02b.7	EXCHANGE OF DATA_Invoke Data Operation: Notification of data operation call reception at clearing House	Upon data providers reception of data consumer's request, a notification is sent at clearing house for logging reception	Done
FRIDS02b.9	EXCHANGE OF DATA_Invoke Data Operation: Notification of data operation result sent at clearing House	Notification of data operation result sent at clearing House from data provider	Done
FRIDS02b.10	EXCHANGE OF DATA_Invoke Data Operation: Notification of data operation result received at clearing House	Notification of data operation result received at clearing House	Done
Context Broker			
FFRA02.2	Platforms integration: Platforms are able to exchange data each other	OneNet Connector must be able to exchange data with other OneNet Connector	Done
FFRA03.3	Middleware Features: Categorization of services and data	The middleware should support the categorization of data in unstructured (text data), semi-structured (e.g., XML/JSON formalized data) and structured	Done
FRIDS01d.2	ONBOARDING_Availability Setup: Broker provider functions for searching	Broker provides functions for searching/browsing/querying for and retrieving registered Connector self-descriptions,	N/A. Searching feature not implemented within Context Broker but

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
		including data sources, interfaces, security profiles, and current levels of trustworthiness.	only at catalogue level.
FRIDS02a.1	EXCHANGE OF DATA_Find Data Provider: Connector provides proper interface to find data provider	Connector offers functionality to Data Consumer to be able to send a query to a Broker Service Provider upon selection of a suitable Broker (e.g. based on thematic coverage) and determine the query capabilities (e.g. a graphical search interface or a domain-specific query language)	N/A. Implemented through UI.
FRIDS02a.2	EXCHANGE OF DATA_Find Data Provider: Broker communicate to data consumer the queried result	The Broker then returns the query result to the Data Consumer (via Connector), who needs to interpret the result to find out about the different data sources available in the IDS for providing the data specified in the query	N/A. Implemented through UI.
FRIDS02a.3	EXCHANGE OF DATA_Find Data Provider: Connector provide a human readable and technical interpretation of result from Broker	Each query result must provide information about each IDS Connector capable of providing the desired data, so that the Data Consumer can retrieve each Connector's self-description to learn more about how to receive the desired dataset from a technical point of view (e.g., endpoint addresses, protocol).	N/A. Implemented through UI.
FRIDS02a.4	EXCHANGE OF DATA_Find Data Provider: Data consumer direct contact with data provider	Data Consumer may already know a suitable Data Provider. In this case, the Data Consumer can contact the Data Provider directly (i.e. without invoking a broker).	Done
FRIDS02b.1	EXCHANGE OF DATA_Invoke Data Operation: Data consumer -via connector-	Data consumer -via connector- retrieve usage policies based on data provider's self-description	Done

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
	retrieve usage policies from data provider		
Data Access Policies			
FRUC06d	Access OneNet Framework: Register or change data access consents	OneNet Participants have to be able to register and change data access consents through accessing the OneNet Framework dashboard	Done
FRC11	IDS-based Service: Usage Control - Access Control and Enforcement	Usage Control App verify all the polices during data exchange	Done
Data Quality			
FFRA03.5	Middleware Features: Data Quality Checking	The middleware should include tool for data quality check	Not implemented, agreed to be part of external services (3rd parties at workbench level)
Semantic Annotation			
FFRA03.2	Middleware Features: Development of semantic models	The Middleware should provide a semantic tool for the development of semantic models	Done
FRC13	OneNet Additional Services: Data Harmonization	OneNet Connector is able to map CIM Data models	Done
FRC14	OneNet Additional Services: Semantic Annotation		Not implemented. Such a requirement has not been identified from demos. The sole connection of data sources can be attributed with the assigned services, and subsequent connections with data producer and consumer.
UC Data App			
FRIDS01b.5	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model- Publishing: Accounting	Connector interface to define information for a data exchange transaction between participants, it is necessary to record additional information, such	Done. No pricing model or billing information implemented.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
		as contract specifications, pricing models, or billing details.	
FRIDS01d.1	ONBOARDING_Availability Setup: Connector option to select a set of available Broker services	Connector provider proper interface for Data Provider/Consumer to select a Broker from a set of available Broker services (i.e., a registry for Connector self-descriptions) to publish the self-description of their Connector	N/A. Only a Broker is expected to be linked with each connector.
FRIDS02b.2	EXCHANGE OF DATA_Invoke Data Operation: Data consumer negotiate policy with data provider	Data consumer to be able to negotiate with data providers sending counter offers for data usage policy	Done.
FRIDS02b.3	EXCHANGE OF DATA_Invoke Data Operation: IDS participants reach agreement on policy	Accept policies to be deployed in both sides and send in policy persistence	Done.
FRIDS02b.4	EXCHANGE OF DATA_Invoke Data Operation: Policies locally deployed at IDS , informing policy persistence	Negotiated polices are deployed at connectors' level	Done.
FRIDS02b.5	EXCHANGE OF DATA_Invoke Data Operation: Data consumer conducts data operation call		Done
FRIDS03b.2	PUBLISHING AND USING DATA APPS_Use Data App: App User selects Data App compatible format	App User selects Data App compatible format being compatible with user's connector specifications packaging format	N/A. Data App concept not implemented in OneNet.
FRIDS03b.3	PUBLISHING AND USING DATA APPS_Use Data App: IDS user retrieves Data App	IDS user retrieves Data App (same as 2b. process)	N/A. Data App concept not implemented in OneNet.
Cybersecurity			
FFRA05.1	Cybersecurity: Ensuring the security and privacy of data exchanged		Done
FFRA05.2	Cybersecurity: Tracking all the data processes and flows		Done
FFRA05.4	Cybersecurity: Providing a testing environment to identify and solve potential security breaches		Done

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
Monitoring & Analytics: Administration			
FRUC06b	Access OneNet Framework: Register or modify account	OneNet Participants have to be able to register themselves with a username and email in the OneNet System with a new account or modify their existing accounts (i.e. change username, email or password) through accessing the OneNet Framework dashboard	Done
FRUC06e	Access OneNet Framework: Login to Framework Dashboard	OneNet Participants have to be able to login to the OneNet Framework dashboard after successful authentication; access to the dashboard shall not be possible without authentication	Done
FRUC06f	Access OneNet Framework: Logout from Framework Dashboard	OneNet Participants have to be able to logout form the OneNet Framework dashboard after successful login	Done
FRRA01.1	OneNet Participant Access: Direct Access to OneNet Monitoring and Analytics Dashboard	Each OneNet Participant must be able to access with unique credentials to the OneNet System	Done
FFRA01.2	OneNet Participant Access: Direct Access to OneNet Orchestration Workbench GUI		Done
FFRA04.1	Monitoring and Analytics Tools: Administrative and configuration tools	The Monitoring and Analytics dashboard must include administrative and configuration tools for the administrator and OneNet Participants (see FFRA01)	Done
FFRA04.4	Monitoring and Analytics Tools: Data Sources Catalogue (UI)	The Monitoring and Analytics dashboard should provide Data Source Catalogue UI	Done (in Connector UI).
FFRA04.5	Monitoring and Analytics Tools: Service Catalogue (UI)	The Monitoring and Analytics dashboard should provide Service Catalogue UI	Done (in Orchestration Workbench UI).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
FFRA06.1	Orchestration Workbench: OneNet Orchestration Workbench GUI	The Orchestration Workbench must offer a GUI to the OneNet Participant through the OneNet Dashboard (see FFRA01)	Done
FRIDS01a.1	ONBOARDING_Acquire identity: Acquire identity for new OneNet participant	Interested party willing to become IDS member makes request form Evaluation Facility	Done
FRIDS01c.1	ONBOARDING_Security Setup: Issue certificate for IDS participant	Connector interface to enable secure communication contacts Certification Authority to issue certificate to the Data Provider or Data Consumer.	Done
FRIDS01c.2	ONBOARDING_Security Setup: Connector deploys locally IDS certificate	Connector deploys locally IDS' participant certificate and identification of IDS and self-description as received from DAPS	Done
Monitoring & Analytics: Analytics			
FRUC06c	Access OneNet Framework: Monitor overall performance	OneNet Participants have to be able to monitor performance KPIs (to be defined) and results from analytics algorithms (to be defined) in the OneNet Framework dashboard	Done
FFRA03.7	Middleware Features: Import/Export for analytics	The middleware should allow the possibility to export analytics result	Done. The export of analytics results is supported through the Monitoring and Analytics Dashboard.
FFRA04.2	Monitoring and Analytics Tools: Data Analytics Dashboard	The Monitoring and Analytics dashboard must include a dashboard with analytics	Done
FFRA04.3	Monitoring and Analytics Tools: Monitoring and Alerting Dashboard	The Monitoring and Analytics dashboard must include a dashboard for monitoring data exchanges and setup alert notifications	Done. Addressed by Connector GUI.
FRIDS01a.2	ONBOARDING_Acquire identity: Acquiry of evaluation for a Service Provider's component	Service provider requests the evaluation of new service component from the Evaluation Facility	Done. Services are included in OneNet Orchestration Workbench.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
FRIDS01a.3	ONBOARDING_Acquire identity: Certification Body notifies certification authority for successful certification	Validity certificates are provided to certification authority	Done
FRIDS01a.4	ONBOARDING_Acquire identity: Generating IDS-ID	The Certification Authority generates a unique IDS ID	Done
FRIDS01a.5	ONBOARDING_Acquire identity: Provisioning of Digital certificate	The Certification Authority issues a digital certificate (X.509) to the participant and notifies the DAPS	Done
FRIDS01a.6	ONBOARDING_Acquire identity: Register of component at DAPS	Digital certificate is deployed at the side of the component(connector) and the component registers at DAPS	Done
FRIDS01a.7	ONBOARDING_Acquire identity: DTM Interaction	Dynamic Trust Monitoring (DTM) implements a monitoring function for every IDS Component. The DTM shares information with the DAPS to notify each of the two participants in a data exchange transaction of the current level of trustworthiness of the other participant.	This approach is suggested by the IDS. In OneNet the identity was support from a Keycloak service.
Orchestration Workbench: Performance Evaluation			
FFRA06.2	Orchestration Workbench: Evaluate Service Performance		Done
Orchestration Workbench: Service Catalogue			
FRUC06a	Access OneNet Framework: Browse potential data sources	OneNet Participants have to be able to browse potential data sources, services, and cooperation partners (=other OneNet Participants) and get contact information through the OneNet Framework Dashboard to establish a connection or contractual agreement on data access consent	Done
FRIDS03a.1	PUBLISHING AND USING DATA APPS_Data App Certification: App Provider assesses request for a data App	App Provider assesses request for a data App	N/A. Data App concept is not implemented in OneNet, as services are hosted in the OneNet Workbench.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Functional Requirements			
ReqId	**Title**	**Description**	**Status**
FRIDS03a.2	PUBLISHING AND USING DATA APPS_Data App Certification: App Provider sends certification request result to Certification Body	App Provider sends certification request result to Certification Body	N/A. Data App concept is not implemented in OneNet.
FRIDS03a.3	PUBLISHING AND USING DATA APPS_Data App Certification: Certification Body performs certification process	Certification Body performs certification process for Data App	N/A. Data App concept is not implemented in OneNet.
FRIDS03a.4	PUBLISHING AND USING DATA APPS_Data App Certification: Certification body issues certificate	Certification body issues certificate for Data App	N/A. Data App concept is not implemented in OneNet.
FRIDS03a.5	PUBLISHING AND USING DATA APPS_Data App Certification: App provider receives certificate for data App	App provider receives and deploys certificate for data App	N/A. Data App concept is not implemented in OneNet.
FRIDS03a.6	PUBLISHING AND USING DATA APPS_Data App Certification: App provider publishes data App Data App Store -Provider-	Data App that was successfully certified, the corresponding metadata is stored in the App Store for being retrieved by users (e.g., Data Consumers or Data Providers) via a search interface	N/A. Data App concept is not implemented in OneNet.

4.3 Software Components Quality Attributes Matrix

The main approach was to create a specific quality model for the OneNet tools and components evaluation process based on specific characteristics (attributes) which are be taken into account while evaluating any software component.

The quality of a system is the degree to which the system satisfies the stated and implied needs of its various stakeholders, and thus provides value. Those stakeholders' needs (functionality, performance, security, maintainability, etc.) are precisely what is represented in the quality model, which categorizes the product quality into characteristics and sub-characteristics.

The product quality model defined in ISO/IEC 25010 comprises the eight quality characteristics shown in the following figure:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Figure 18 - Product Quality Model (ISO/IEC 25010)

The main quality attributes for evaluation are:

1. Functional Suitability
2. Performance Efficiency
3. Compatibly
4. Usability
5. Reliability
6. Security
7. Maintainability
8. Portability

Table 4.3 – Quality Attributes description

Attribute	Evaluation
Functional Suitability How a product or system provides functions that meet stated and implied needs when used under specified conditions	Functional completeness - Degree to which the set of functions covers all the specified tasks and user objectives Functional correctness - Degree to which a product or system provides the correct results with the needed degree of precision Functional appropriateness - Degree to which the functions facilitate the accomplishment of specified tasks and objectives
Performance Efficiency Performance relative to the amount of resources used under stated conditions	Time behaviour - Degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements Resource utilization - Degree to which the amounts and types of resources used by a product or system, when performing its functions, meet requirements Capacity - Degree to which the maximum limits of a product or system parameter meet requirements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Compatibility Degree to which a product, system or component can exchange information with other products, systems or components, and/or perform its required functions while sharing the same hardware or software environment	Co-existence - Degree to which a product can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product Interoperability - Degree to which two or more systems, products or components can exchange information and use the information that has been exchanged
Usability Degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use	Appropriateness recognizability - Degree to which users can recognize whether a product or system is appropriate for their needs Learnability - Degree to which a product or system can be used by specified users to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use Operability - Degree to which a product or system has attributes that make it easy to operate and control User error protection - Degree to which a system protects users against making errors User interface aesthetics - Degree to which a user interface enables pleasing and satisfying interaction for the user Accessibility - Degree to which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use
Reliability How a system, product or component performs specified functions under specified conditions for a specified period of time	Maturity - Degree to which a system, product or component meets needs for reliability under normal operation Availability - Degree to which a system, product or component is operational and accessible when required for use Fault tolerance - Degree to which a system, product or component operates as intended despite the presence of hardware or software faults Recoverability - Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Security Degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization	Confidentiality - Degree to which a product or system ensures that data are accessible only to those authorized to have access Integrity - Degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data Non-repudiation - Degree to which actions or events can be proven to have taken place so that the events or actions cannot be repudiated later Accountability - Degree to which the actions of an entity can be traced uniquely to the entity Authenticity - Degree to which the identity of a subject or resource can be proved to be the one claimed
Maintainability This characteristic represents the degree of effectiveness and efficiency with which a product or system can be modified to improve it, correct it or adapt it to changes in environment, and in requirements	Modularity - Degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components Reusability - Degree to which an asset can be used in more than one system, or in building other assets Analysability - Degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified Modifiability - Degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality Testability - Degree of effectiveness and efficiency with which test criteria can be established for a system, product or component and tests can be performed to determine whether those criteria have been met
Portability Degree of effectiveness and efficiency with which a system, product or component can be transferred from one hardware, software or other operational or usage environment to another	Adaptability - Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments Installability - Degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment Replaceability - Degree to which a product can replace another specified software product for the same purpose in the same environment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Table 4.4 - Software Components Quality Attributes Matrix

Tool/Component	Functional completeness	Functional correctness	Functional appropriateness	Time behaviour	Resource utilization	Capacity	Co-existence	Interoperability	Appropriateness recognizability	Learnability	Operability	User error protection	User interface aesthetics	Accessibility	Maturity	Availability	Fault tolerance	Recoverability	Confidentiality	Integrity	Non-repudiation	Accountability	Authenticity	Modularity	Reusability	Analysability	Modifiability	Testability	Adaptability	Installability	Replaceability
Context Broker (and FIWARE Data App)	X	X	X				X	X							X	X			X	X	X	X	X	X	X				X	X	
Vocabulary provider, Semantic Tools and Services	X	X	X					X	X	X	X	X	X	X	X	X			X	X	X	X			X				X		X
Identity Provider and Management (Authentication & Authorization)	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X	X				X	X			X		X		
Data Access Control (Usage Control)	X	X	X									X			X	X			X	X	X	X	X	X	X					X	X
Clearing House	X	X	X									X			X	X			X	X	X	X	X	X	X					X	X

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

User Interface (OneNet Connector)	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X		X	X	X	X
Data Process Management (Orchestration & Workflow)	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X					X	X
Service Management	X	X	X		X	X				X	X	X			X	X			X	X	X	X	X	X	X	X	X	X		X	X
Performance Evaluation	X	X	X		X	X				X	X	X			X	X			X	X	X	X	X	X	X	X	X	X		X	X
Administration	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X	X				X	X			X		X	
Analytics & KPIs	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X	X				X	X			X		X	
Network Traffic & Endpoint Infrastructure Monitoring	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X	X				X	X			X		X	
Data Analysis, Rating & Classification	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X	X				X	X			X		X	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

5 Conclusion

This report has provided a presentation of the evolution of the OneNet Framework focusing on the enhancements that have been included in its final version. The OneNet Framework offers a robust infrastructure to support and orchestrate trusted, secure and seamless interconnectivity of energy stakeholders. The overall design and development of the OneNet System has considered and combined features of the IDS and FIWARE initiatives adopting data space traits to ensure data and service interoperability among service providers, data producers/consumers.

The evolution of the OneNet Framework along three releases, emphasized on the technological enhancement and the evaluation on quality attributes to assure, beyond the fulfilment of the functional requirements related to the data exchange, also compliance with legal, privacy and regulatory requirements as they have been described in the OneNet System design ([1][2][3][4].

The OneNet Framework sets up a reference data space and hybridizes it towards the development of energy specific features. It is the OneNet Connector that delivers a distributed software component that can be deployed on the premises of any stakeholder that wishes to enter in the OneNet data and service ecosystem. It allows data to be exchanged directly (P2P) between the participating stakeholders, without the intermediation of any data hub or other kind of data repository.

The OneNet Middleware provides for the incoming meta-data orchestration from the OneNet connectors, assuming also for the administration of the OneNet ecosystem (meta-data logging, OneNet cross-platform services maintenance, user management). This central component of the OneNet Workbench allows for third party applications to be deployed (considering different orchestration types) there and allow for the open access to OneNet stakeholders.

The OneNet Network Monitoring and Analytics Dashboard is also present as a central component designed to provide the OneNet administrator and OneNet users with historical and real-time data regarding requests to Connectors, security reporting, alerting and filtering capabilities.

The final release of the OneNet Framework as presented here, has demonstrated its fundamental communication capabilities in several pilots within the OneNet project by being deployed in different operational environments and stakeholders' platforms.

The OneNet Framework implementation has demonstrated that a seamless, secure and trusted data exchange among different stakeholders in the energy domain is possible in a structured and harmonised way, overcoming regional and national borders without the necessity to change current IT platforms and systems or losing control over data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The developed concepts within the OneNet project (see [1][2][3][4]) and the OneNet Framework implementation as presented in this document and the other deliverables of the OneNet project ([5], **Error! Reference source not found.**, [7], [8], [9], [10], [11]) form a solid and high TRL basis (8) for further exploitation:

- A set of S/W components, the OneNet Reference Architecture is being and will be further exploited in subsequent Horizon Europe Projects (Enershare, TwinEU, RESONANCE etc.), and will remain accessible beyond the OneNet project's duration under respective Open-Source licenses.
- The methodology of defining Cross-Platform-Services and respective Business Objects ([3], [4]) along with a repository of 64 Cross-Platform-Services and the data schemata for their Business Objects will also remain available.
- An application to include the OneNet Framework and Components as a project under the Linux Foundation Energy will be also submitted by the respective project partners.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

References

[1] D5.1 - OneNet Concept and Requirements. Available at https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5e2ad20de&appId=PPGMS.

[2] D5.2 - OneNet Reference Architecture. Available at https://onenet-project.eu/wp-content/uploads/2022/12/OneNet_D5.2_v1.0.pdf.

[3] D5.3 - Data and Platform Assets Functional Specs and Data Quality Compliance. Available at https://onenet-project.eu/wp-content/uploads/2022/12/OneNet-D5.3-v1.0.pdf.

[4] D5.6 - Report on Extended Data, Platform and Service Interoperability. Available at https://onenet-project.eu/wp-content/uploads/2022/12/OneNet_D5.6_v1.0.pdf.

[5] D6.1 - Report on decentralized edge-level middleware for scalable platform agnostic data management and exchange. Available at https://onenet-project.eu/wp-content/uploads/2023/02/D6.1-OneNet-v1.0.pdf.

[6] D6.2 - Cross stakeholder Data Governance for Energy Data Exchange. Available at https://onenet-project.eu/wp-content/uploads/2023/04/D6.2-OneNet-v1.0.pdf.

[7] D6.3 - Extended Interoperability and Management with FIWARE. Available at https://onenet-project.eu/wp-content/uploads/2023/09/OneNet_D6.3_v1.0.pdf.

[8] D6.4 - AI, Big Data, IoT Orchestration Workbench. Available at https://onenet-project.eu/wp-content/uploads/2023/09/OneNet_D6.4_v1.0.pdf.

[9] D6.5 - OneNet Reference Platform First Release. Available at https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f01ba432&appId=PPGMS.

[10] D6.6 - Tools for Legal, Regulatory, Privacy and Cybersecurity Compliance. Available at https://onenet-project.eu/wp-content/uploads/2023/09/OneNet_D6.6_v1.0-1.pdf.

[11] D6.7 - Compliance to Reference Architecture Management Tools. Available at https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5ee422a5f&appId=PPGMS.

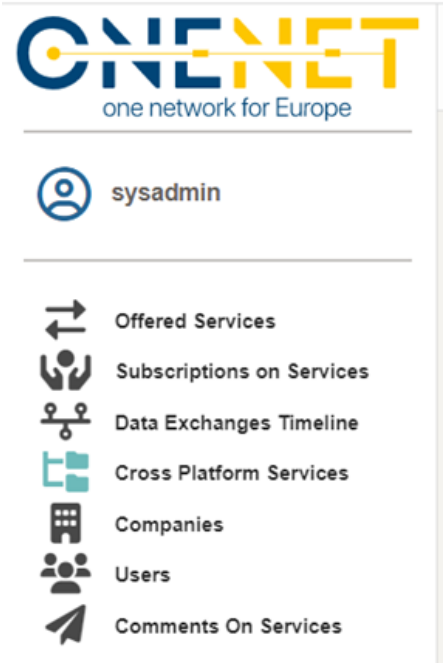
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Annex A Component Manuals – Final version

A.1 OneNet Middleware and OneNet Connectors GUI

The final OneNet Reference Framework release is available on the project's Github repository.[5]

The system administrator is essentially responsible for the administering the operation of the OneNet central Middleware. Accordingly, the creation/registration of new OneNet users takes place solely through the system administrator's environment. The administrator menus are illustrated in Menu A.1.



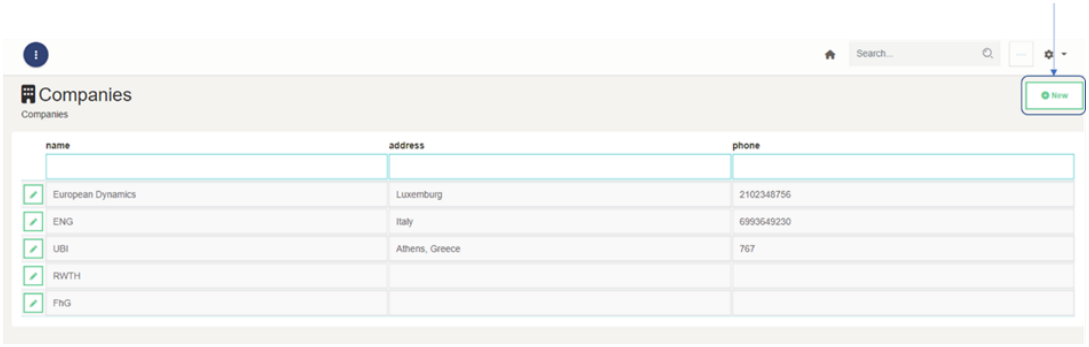
Menu A.1 Administrator's menu

Therefore, the admin can have an overview on the different processes for all OneNet users, observing only meta-data which are stored in the OneNet middleware and not the actual data that are exchanged directly between Producer and Consumer. For instance, offered services details (meta-data here refers to the service specification and the service provider etc.), all the offered services that they are available in the ecosystem; subscription on services that details all the registered subscriptions; cross-platform services which contain the open and configurable (by admin user and the following to be explained in Section 8.2) list of OneNet cross-platform services; the Companies and the Users registered on the Middleware upon request.

[5] https://github.com/european-dynamics-rnd/OneNet

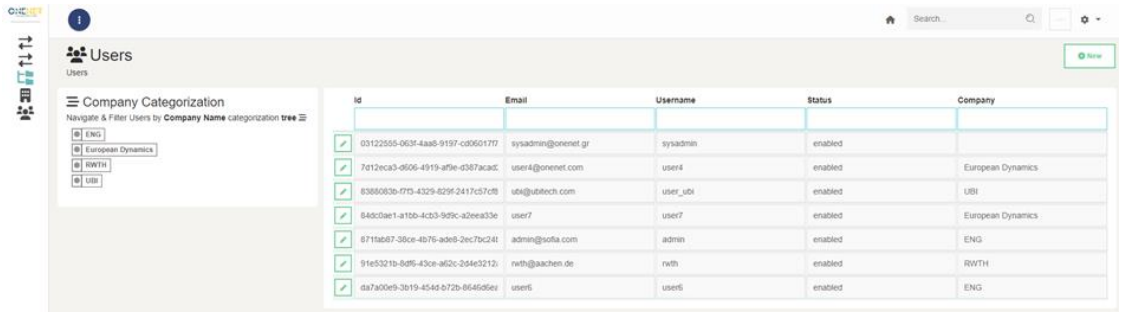
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A system administrator might create new user profiles which always have to be assigned with an affiliated Company. Screen 1 illustrates the respective dashboard in which the system administrator might add or edit companies in the ecosystem.



Screen 1: Companies registry.

The corresponding dashboard for user management (configuration of existing and creation of new users) is presented in Screen 2. Multiple users might be assigned with a company.

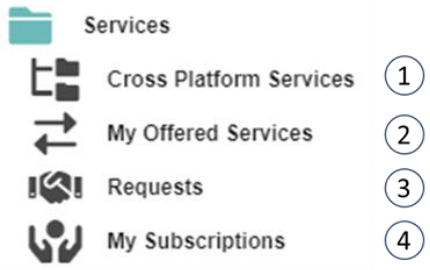


Screen 2: User Management.

The system administrator might view from Services tab (Screen 3):

1. any information related cross-platform services and update this information. It is the system administrator's sole responsibility to add or update a new cross-platform service. For instance, a system administrator might wish to update the semantic definition of a cross-platform service,
2. all offered services from all users,
3. all requests sent to services providers to accept/reject a service subscription,
4. any service subscriptions to any cross-platform service.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



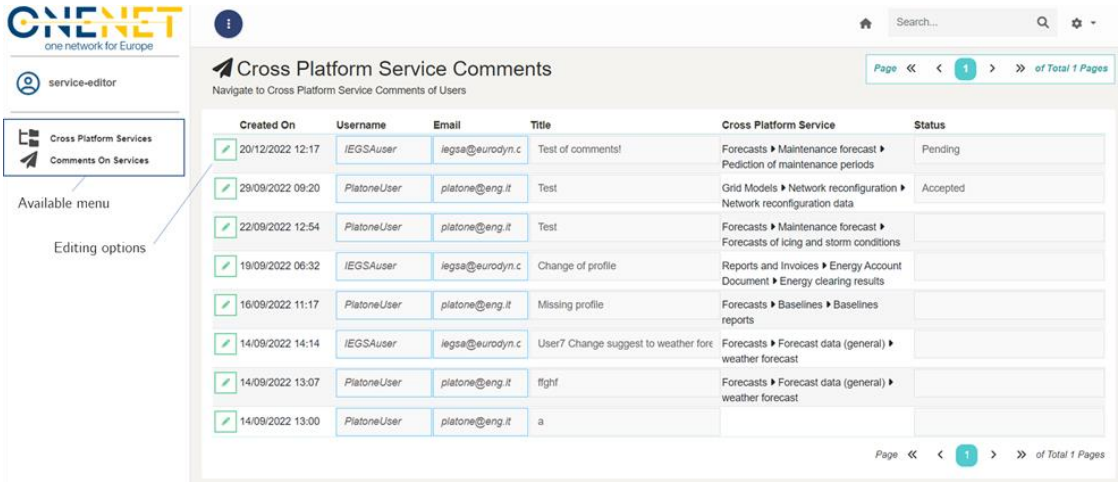
Screen 3: Services dashboard and sub-menus

The system administrator has also the capability to view meta-data information about OneNet data exchanges (Screen 4):

1. any data provisions from OneNet data providers,
2. any **meta-data** information for data available for consumption,
3. a dashboard with a list of completed data exchanges.

Screen 4: Data exchanges dashboard and sub-menus.

A.1.1 Data profile manager



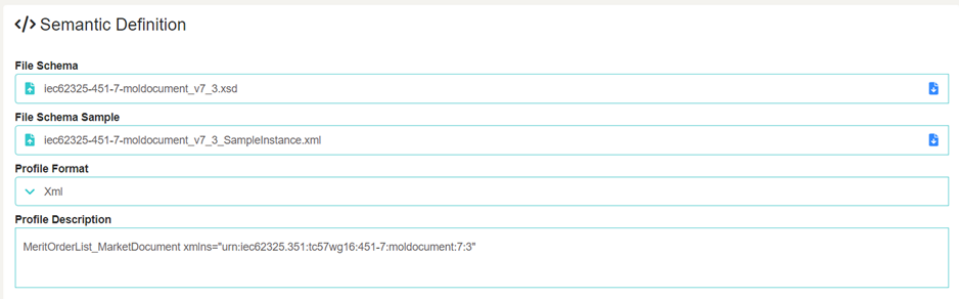
Screen 5: Data profile manager menu

The data profile manager is an essentially one additional administration menu which is dedicated to the configuration and maintenance of the cross-platform services list. As the cross-platform services list is an

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

evolving directory, in the sense that new entries might need to be registered or existing services might need updates either to their functional description or to their semantic definition. The data profile manager's menu is presented in Screen 5.

The data profile manager essentially gives access to the comments received from users. Accordingly, the data profile manager can access the comment with the edit button and change status (Pending, Accepted, Rejected) on the comments when this is properly addressed. On the corresponding cross platform services tab this admin role can edit a specific service to provide any kind of updates. Particularly on the semantic definition of a service the profile manager can upload the harmonized semantic schemas as in Screen 6.



Screen 6: Semantic definition of a cross-platform service.

A.1.2 OneNet users

Prior to the description of the OneNet Connector's GUI, it is vital to highlight the key concept/workflow that is designed to provide seamless and secure data exchange among platforms. As illustrated in the figure below, there are certain preconditions for new OneNet entrants, to provide or consume data:

- **Data provision**: OneNet user that wishes to act as a data provider, needs primarily, to register (i.e. in the OneNet Middleware) what type of services will be offered. This is performed in centralized manner, to inform all the potentially interested parties about this new service offering. The service offering is assigned with cross-platform service type, as defined in OneNet, so that there is common understanding (description, syntactics/semantics). Once this new service offering is registered, then a service provider can make available data items in the OneNet ecosystem. In fact, only meta-data information will be made available (for this new data item) to all OneNet users that have an active subscription for this service.
- **Data consumption**: OneNet user that wishes to consume data, needs firstly, to express the interest for a specific cross-platform services, by making a service subscription, accordingly. Once the subscription is marked accepted by the service provider, then the data consumer will be able to get updates (i.e., given proper meta-data descriptions) on new data items assigned with this service. For new data items, the data consumer can make a GET request to the provider by clicking the respective button as it is explained in the forthcoming sections.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

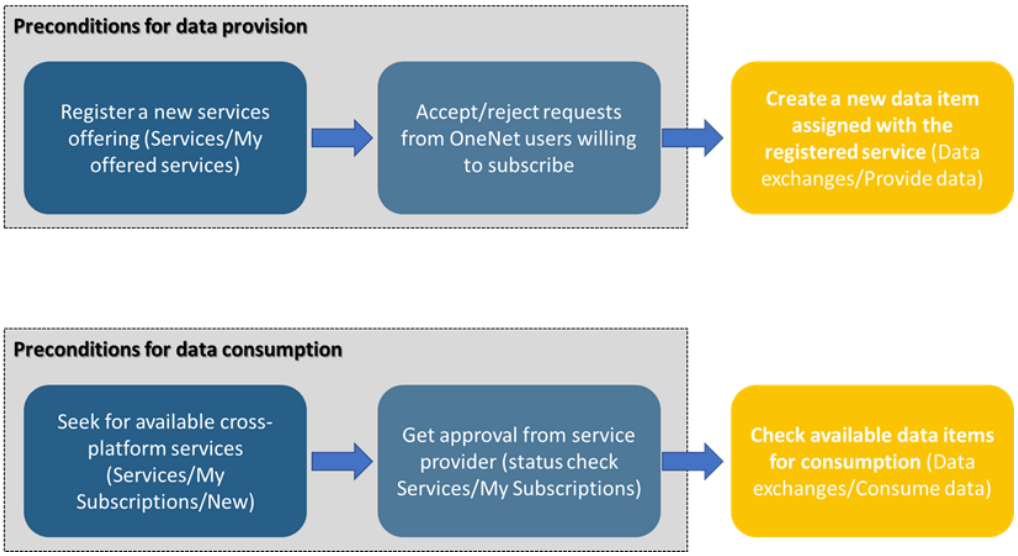
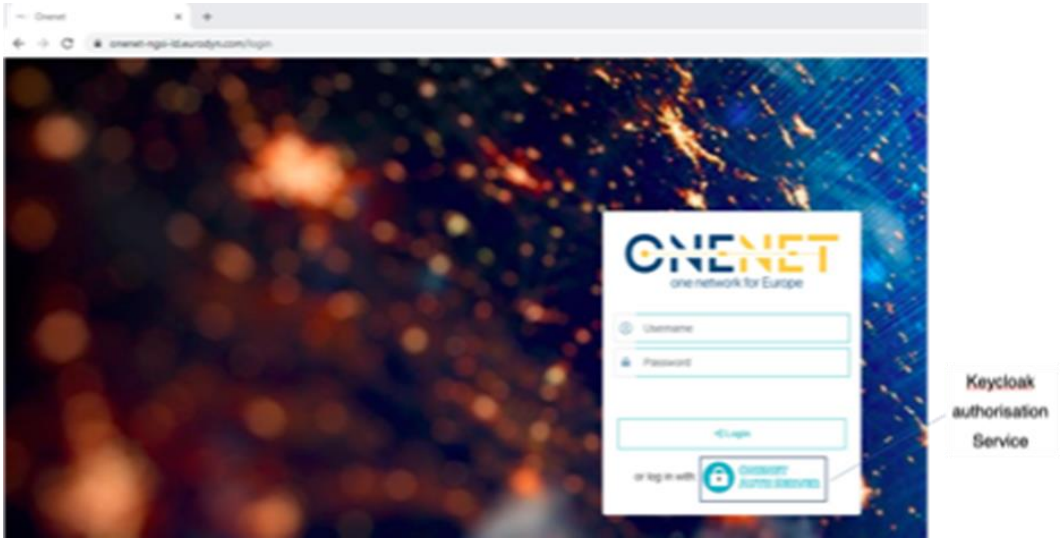


Figure: Key concept for exchanging data through OneNet Connector.

A.1.3 Accessing OneNet GUI

For companies/users that are willing to deploy the OneNet connector proper user profiles will be created and shared with them, which will be used to get access to the GUI of OneNet (https://onenet-ngsi-ld.eurodyn.com/login). The Log-in screen appears in Screen 7. A user will notice the Keycloak authorization service which enables a common authorization mechanism along the OneNet solutions.



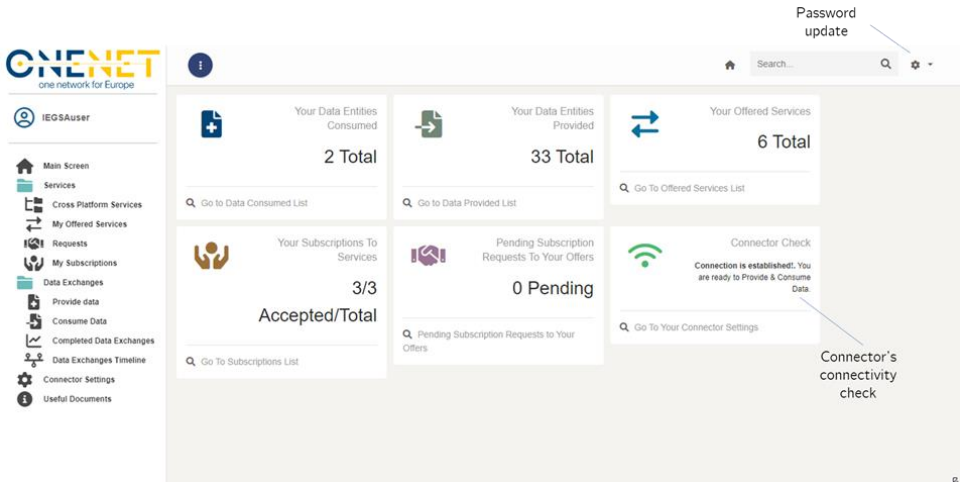
Screen 7: OneNet Connector's GUI log-in screen.

A.1.4 Main screen

The main screen that the user will be redirected to is presented in Screen 8, which essentially provides an overview of KPIs calculated at the OneNet connector's level. Such information might refer to data items

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

consumed/provided, offered services, active subscriptions, along with the connector's connectivity check. All the presented analytics provide a go to button that shift the user to the corresponding menu.



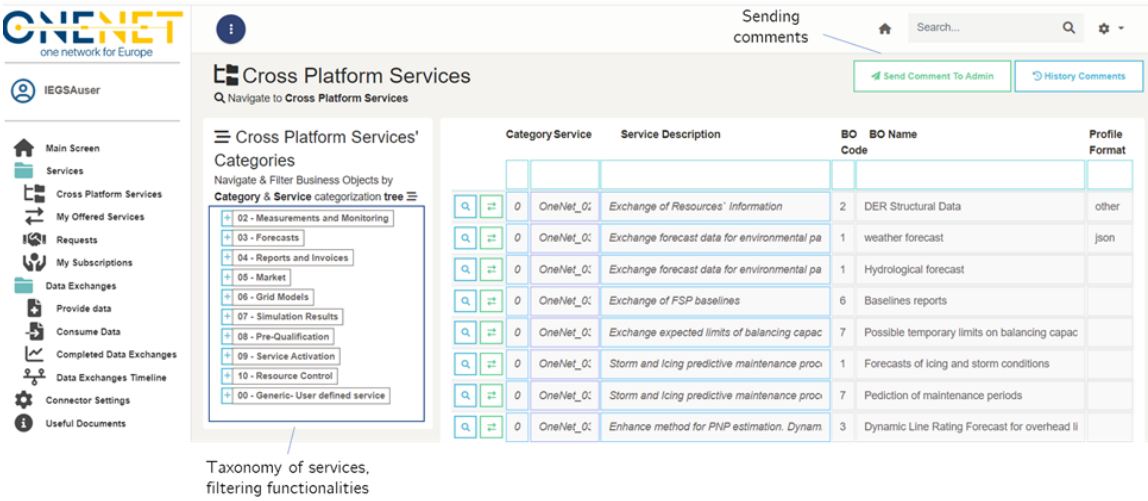
Screen 8: Main screen.

A user can update the pre-set password by clicking on settings as illustrated in Screen 8.

A.1.5 Services

In general, the services framework is designed to provide all the necessary details about the definition of OneNet cross platform services (i.e. business objects, functional description, semantic definition), the offering of a cross-platform service into the OneNet ecosystem as well as the subscription in a cross-platform service.

A.1.5.1 Cross-Platform Services

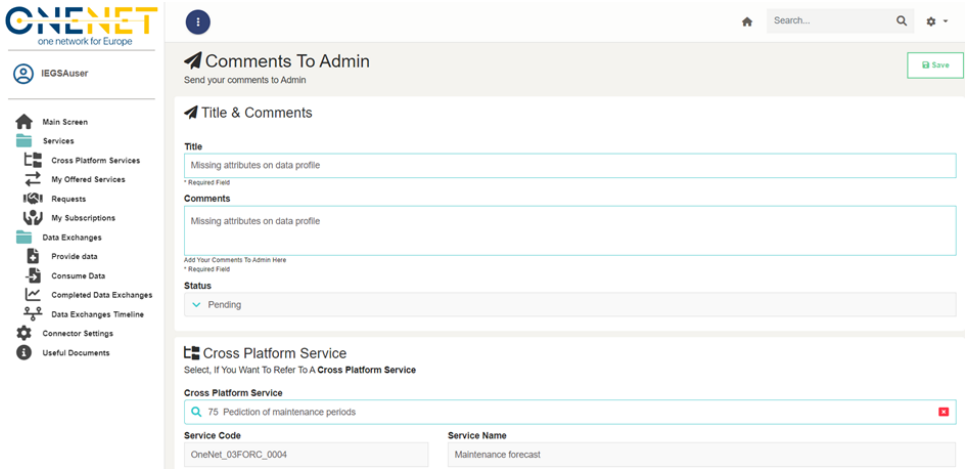


Screen 9: Cross-platform services tab.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

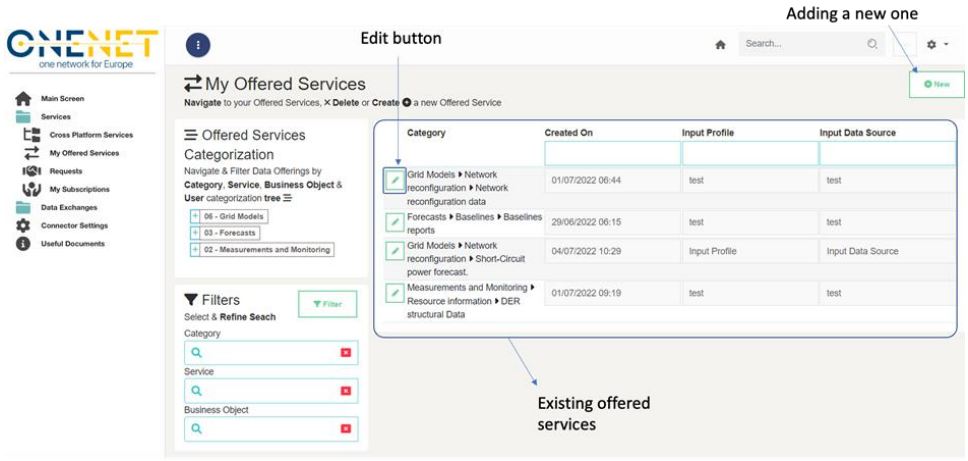
The cross-platform services tab is essentially a view-only environment which provides a directory on cross-platform services as they are proposed and categorized in OneNet project (see Screen 9). It should be noted that if an OneNet user cannot find a matching cross-platform service, then it is indicated that the 00- Generic- Non-existing shall be used providing analytical descriptions for this cross-platform service. The latter will ease the evolution of cross-platform services and proceed with updates on the catalogue.

To send comments for updates or omissions for a specific cross-platform service, a user needs to click the button “Send Comments To Admin”, which will redirect to a new dashboard where the user needs to select the referencing service along with the comments as in Screen 10.



Screen 10: Comments to admin screen.

A.1.5.2 My offered Services



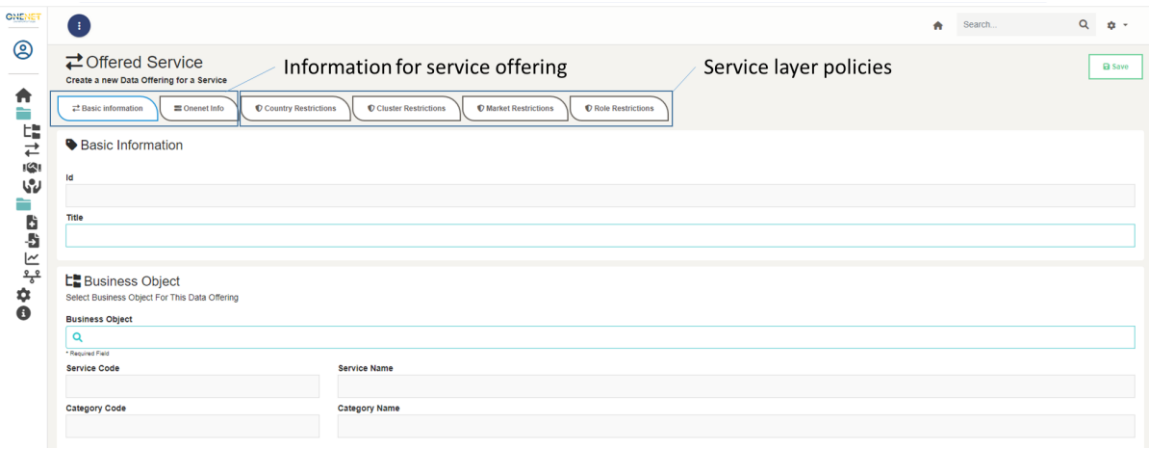
Screen 11: My offered services tab.

This tab is when a user wishes to provide/deliver a new cross-platform service. By clicking this tab, see Screen 11, the user can preview existing offered services by the same user, to which one sort based on the filters. The

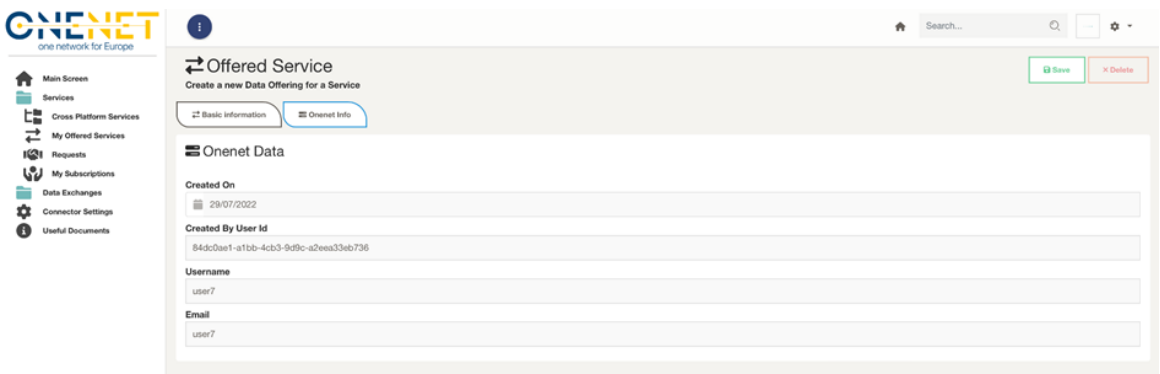
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

user has the option to edit an existing service and proceed with updates on the offering, by clicking on the edit Button. For a new offering, the user needs to click New.

By clicking New, the user will view a pop window as in Screen 12. The user must assign this new service with a business object that is in turn under a cross-platform service. By clicking in the Business Object, the list that is presented in the Cross-platform Services tab will again appear. The user has also to claim whether service delivery will occur using OneNet harmonized data profiles, else to define the data profile of information to be shared. In the OneNet info there is information regarding the service provider timestamp, the assigned by the system unique user-ID as well the information of the service provider as in Screen 13. The semantic definition area is the one where the service provider states details on how the data to entities (assigned with this service) will be formatted. For this reason, once a user selects a specific cross-platform service then the harmonized -if any- will be loaded automatically. In case the services provider wishes to set custom profile, then, needs to check the box “Custom Semantics”.



Screen 12: Adding a new cross-platform service offering.



Screen 13: OneNet Info on my offered services.

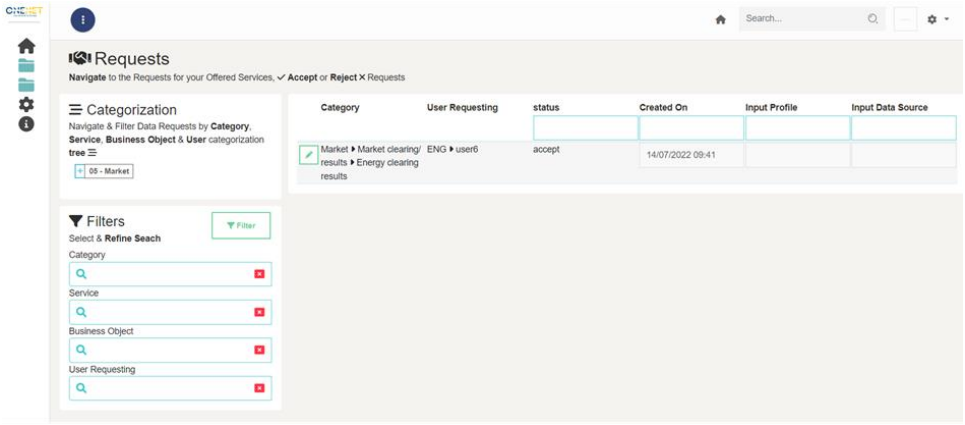
The remainder tabs (Country Restrictions, Cluster Restrictions, Market Restrictions and Role Restrictions) are policies that may be applied into a new service offering. Applying a policy into a service poses limitations to the

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

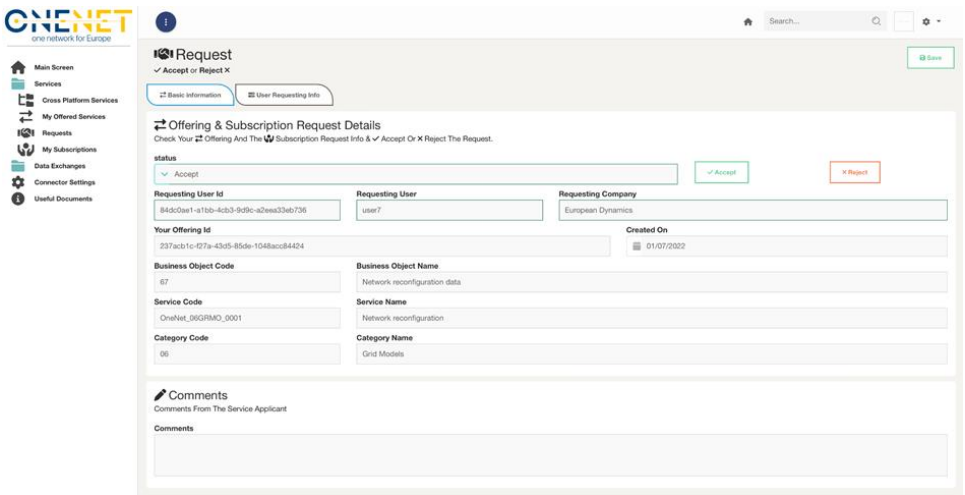
actors that will be able to view that this service is available in the OneNet ecosystem, avoiding for unwished service requests. This is a practical feature particularly for services that have a strict regional application. The Role Restriction though can allow multiple users from other countries to access and view meta-data of the offering such as Weather Data Provider, DSO, TSO, TSO DSO Coordination Platform, System Operator, Service Provider, Scheduling Coordinator, Retailer, Renewable Energy Source Manager, etc.

A.1.6 Requests

This tab provides a listed summary of incoming requests from other OneNet users for the Offered services, as in Screen 14. The service can view the list of pending or already responded requests. The requests can be addressed by clicking the Edit button. The window that appears accordingly is on Screen 15, which, essentially, provides information about requesting user and company. From this tab, a service can even change the status of a service from “Accept” to “Reject.” Note that, once a request is accepted or rejected then it cannot change again.



Screen 14: Requests, incoming request for offered services.

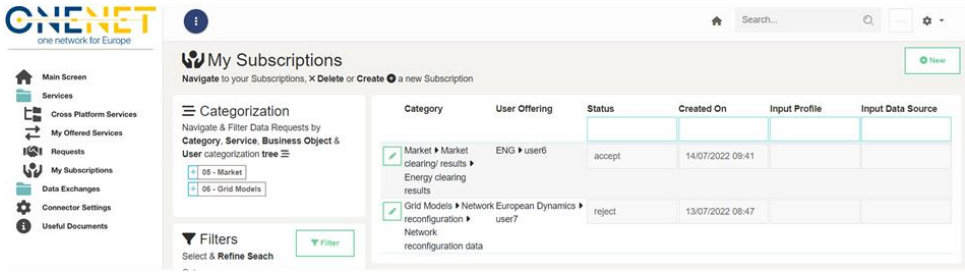


Screen 15: Responding a request on offered service.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739

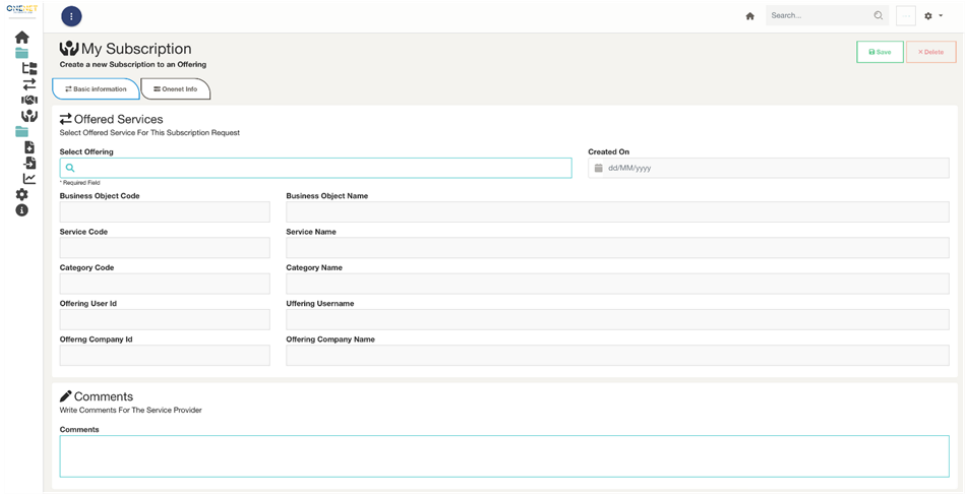
A.1.7 My subscriptions

Accordingly, the “My subscriptions” tab is for a user to make subscription to available services. The main screen on this tab is a listed summary of current subscriptions as in Screen 16.



Screen 16: My subscriptions.

A user can make a new request to service providers by clicking the “New” button, where the tab that appear is on Screen 17.



Screen 17: New subscription.

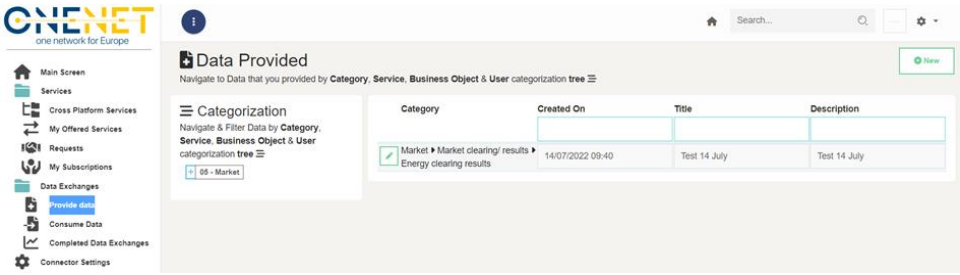
A.1.8 Data exchanges

The data exchanges framework is the one to perform actual data exchanges (data provision or consumption) among OneNet users serving offered services and subscriptions, accordingly. This framework is organized in three self-explanatory tabs: “Provide data”, “Consume data” and “Completed Data Exchanges”.

A.1.8.1 Provide data

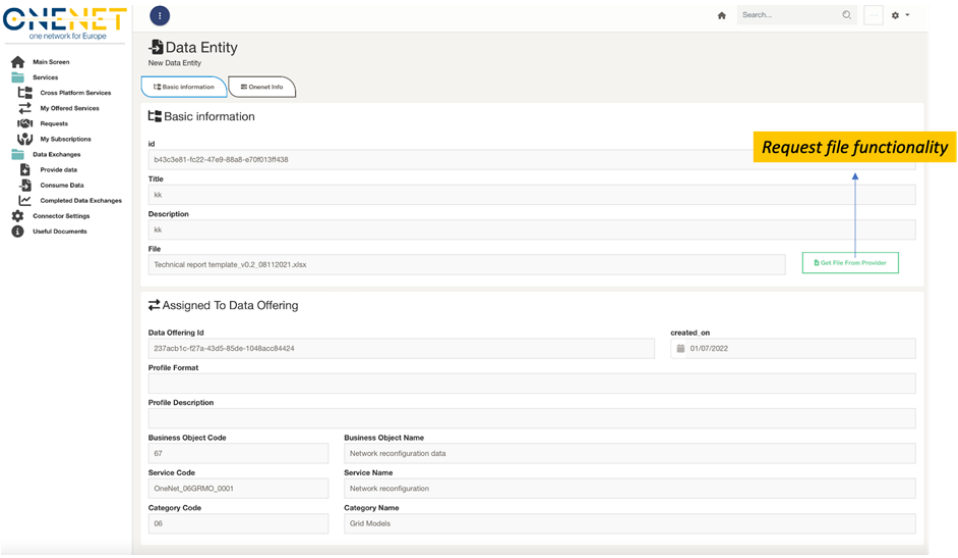
Screen 18 shows the main Provide data tab, where it presents a list of the current user’s data item provisions. It is essential to note that for an existing data provision the file cannot be changed; due to issues related the operation of OneNet Connector. Therefore, the user might create a new entry for the data provision. To do so, the user must click on “New”, where a window will pop up as in Screen 18.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 957739



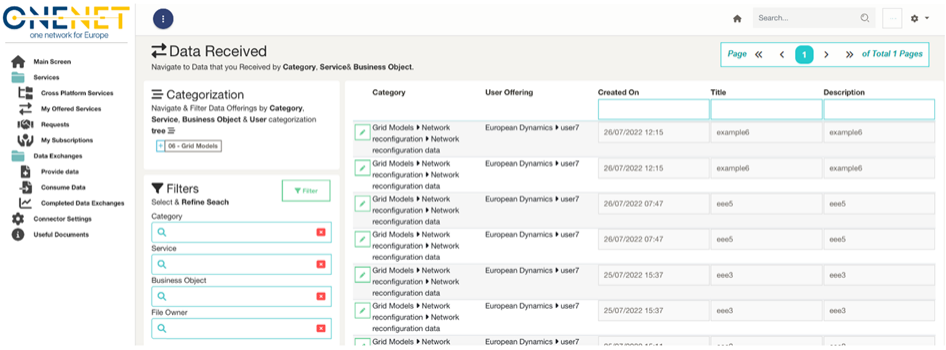
Screen 18: Provide data tab

The user will have to assign the new data item with an existing offering and then upload a file through the upload file functionality. The input shall be aligned with the definition of the offered service in order the potential data consumer can utilize it.



Screen 19: Adding a new data item.

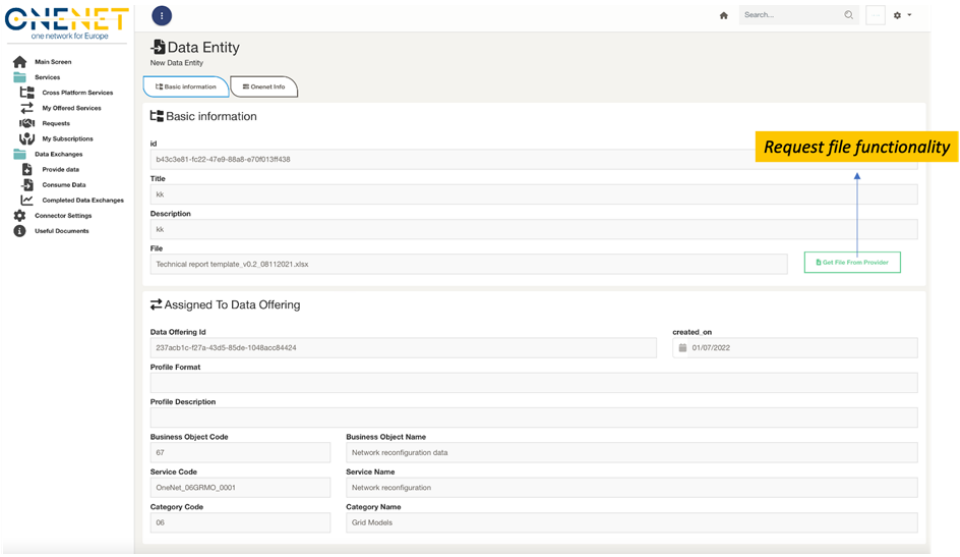
A.1.8.2 Consume data



Screen 20: Consumer data tab.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

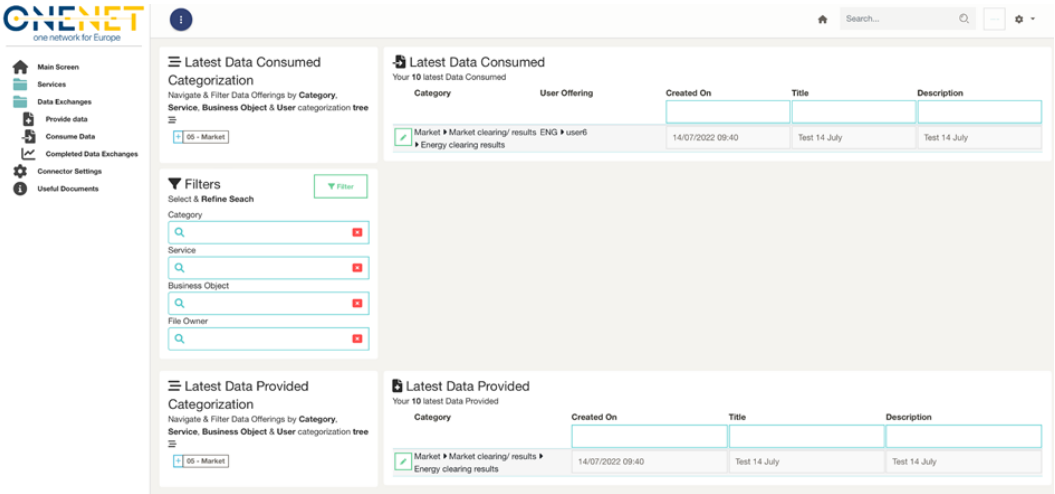
This tab for consuming data provides listed information for available data items (related to My subscriptions services) -see Screen 20-. To consume any of these data items, a user needs to click on the data entity and a new pop-up will appear as in Screen 21, which provides multiple meta-data information about provided data. There is this streamlined process of requesting the data by clicking a button as a download functionality, yet the UI deals in the backend to trigger the necessary processes related to IDSA and FTCs.



Screen 21: Data entity information and get functionality.

A.1.8.3 Completed data exchanges

This tab provides an overview/history (see Screen 22) of completed data exchanges (data provided/consumed), where a user can check analytical information by clicking in any of those.

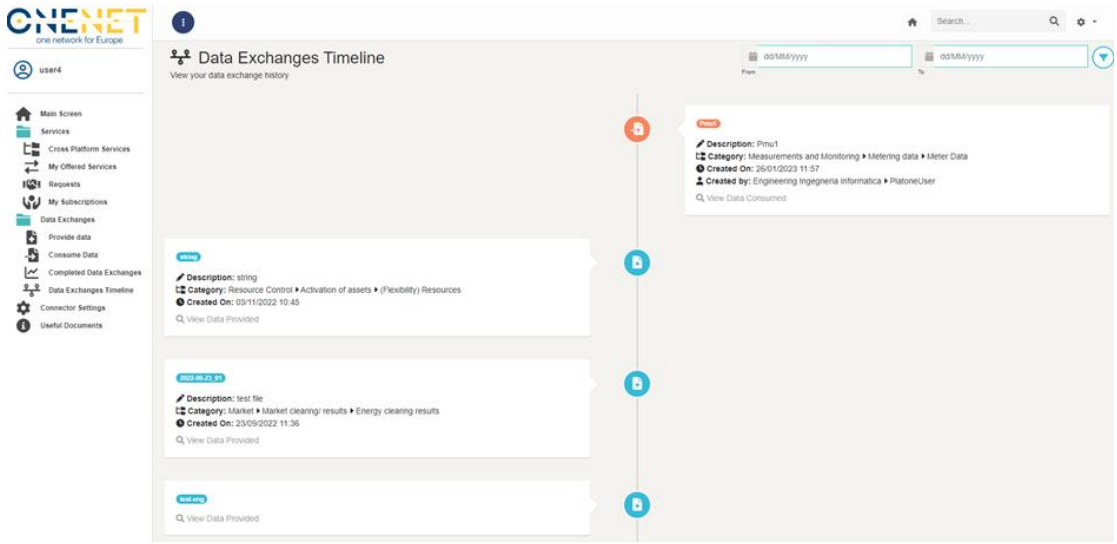


Screen 22: Completed data exchanges tab.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A.1.9 Data Exchanges Timeline

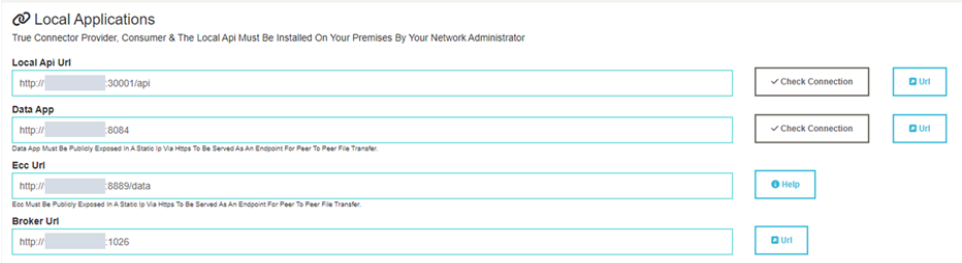
This dashboard is a rather a visualized Timeline (see Screen 23) that contains all the completed data exchanges for the user. Essentially is a supportive dashboard to improve user's experience, as multiple data exchanges are performed.



Screen 23: Data Exchanges Timeline.

A.1.10 Connector Settings

This tab is rather a configuration/setting one which provides the option to user to change the configuration files of the OneNet connector. Obviously, this can harm the connectivity and operation of the OneNet connector, therefore it is not suggested for typical (i.e., non-IT users) to test it. A user can have an overview of the actual endpoints configuration and test their connectivity (see Screen 24).



Screen 24: Connector settings.

A.1.11 Documents & Downloads

This tab provides useful documents (like the latest versions of the Manual and Deployment Guide) as well as for the latest S/W packages of OneNet (see Screen 25).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Screen 25: Documents & Downloads

A.2 OneNet Orchestration Workbench

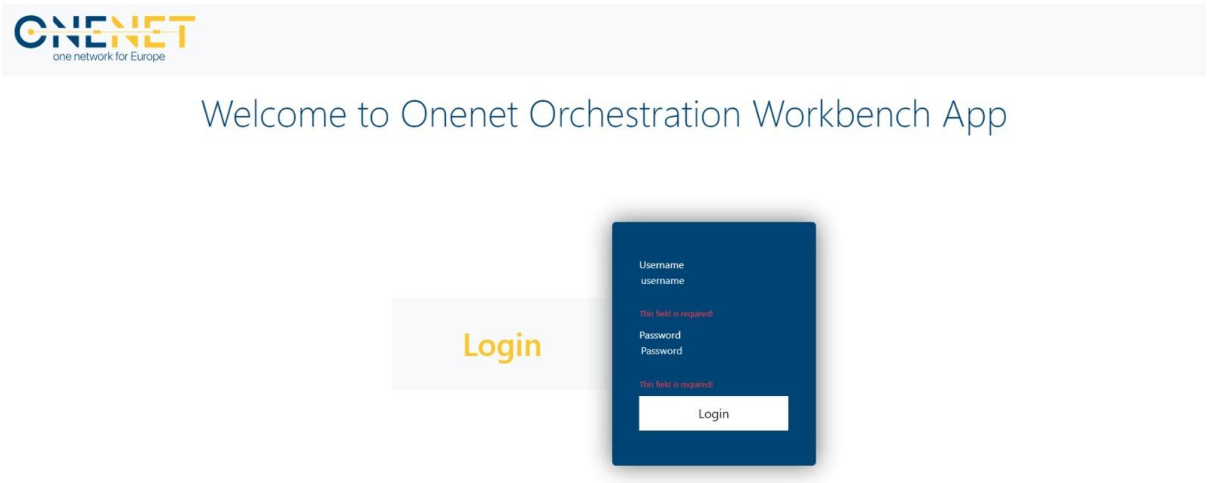
The OneNet Orchestration Workbench provides a web-based platform to any OneNet Participants, offering the possibility to:

- Login through OneNet credentials (integrating the centralized OneNet Identity Manager).
- Integrate data sources using the OneNet Connector.
- Deploy, Orchestrate and Monitoring data-driven services.
- Explore Service Catalogue.
- Run services.
- Evaluate service performance.

A.2.1 Login

The login section allows any OneNet Participant to access the OneNet Orchestration Workbench using its own OneNet credentials. The OneNet Orchestration Workbench authentication mechanisms is synchronized with the OneNet Connector and Decentralized Middleware, ensuring a unique identification mechanism.

The Screen 26 below shows the login section in the Orchestration Workbench GUI.

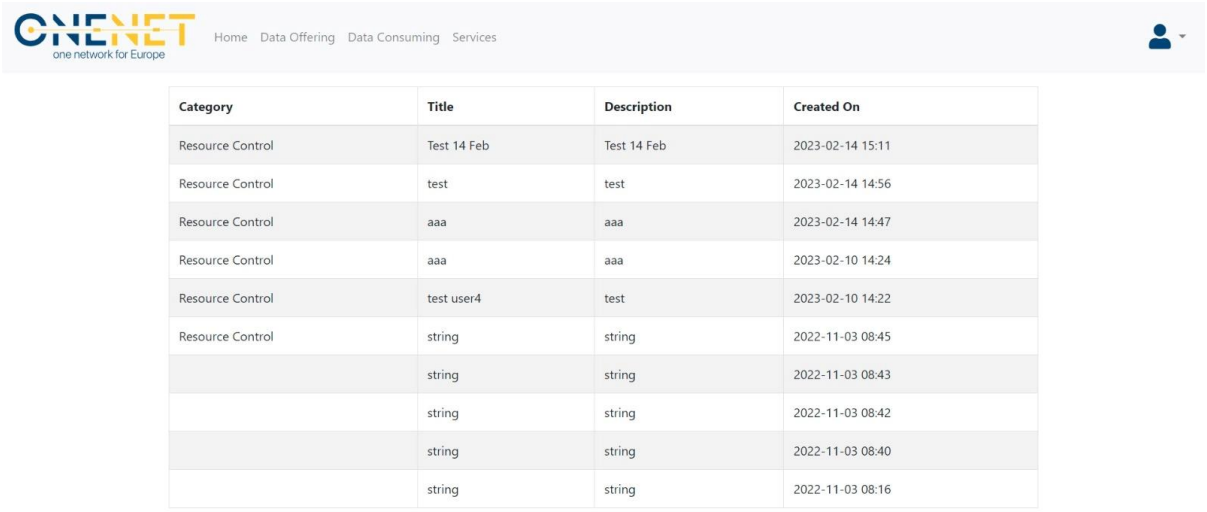


Screen 26: OneNet Orchestration Workbench Login section

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A.2.2 Data Integration

After login into the OneNet Orchestration Workbench the OneNet Participant is able to integrate data using the OneNet Connector. The Workbench shows all the data offerings, subscriptions and data consumed using the OneNet Connector. No data are stored in the OneNet Orchestration Workbench, unless a user explicitly wants to transfer data to a specific OneNet service. The two screens below show the data offerings (Screen 27) and data consumed (Screen 28) retrieved from the OneNet Connector APIs.



Category	Title	Description	Created On
Resource Control	Test 14 Feb	Test 14 Feb	2023-02-14 15:11
Resource Control	test	test	2023-02-14 14:56
Resource Control	aaa	aaa	2023-02-14 14:47
Resource Control	aaa	aaa	2023-02-10 14:24
Resource Control	test user4	test	2023-02-10 14:22
Resource Control	string	string	2022-11-03 08:45
	string	string	2022-11-03 08:43
	string	string	2022-11-03 08:42
	string	string	2022-11-03 08:40
	string	string	2022-11-03 08:16

Screen 27: OneNet Orchestration Workbench Data Offerings section

Category	Title	Title	Description	Created On	Data Provider	
Forecasts_03_113	test-service-20-07	test-data-20-07	test-data-20-07	2023-07-20 11:11	Engineering Ingegneria Informatica-PlatoneUser	Download
Forecasts_03_113	test19-07	test19-07_2	test19-07_2	2023-07-19 13:50	Engineering Ingegneria Informatica-PlatoneUser	Download
Forecasts_03_113	test19-07	test19-07_1	test19-07_1	2023-07-19 11:11	Engineering Ingegneria Informatica-PlatoneUser	Download
Forecasts_03_113	Malta	d	d	2023-06-05 09:02	Engineering Ingegneria Informatica-PlatoneUser	Download
Forecasts_03_113	Malta	c	c	2023-06-05 08:59	Engineering Ingegneria Informatica-PlatoneUser	Download
Forecasts_03_113	Malta	b	b	2023-05-24 12:56	Engineering Ingegneria Informatica-PlatoneUser	Download
Forecasts_03_113	Malta	docker2	docker2	2023-05-22 07:37	Engineering Ingegneria Informatica-PlatoneUser	Download
Forecasts_03_113	Malta	docker		2023-05-12 12:17	Engineering Ingegneria Informatica-PlatoneUser	Download
Forecasts_03_113	Malta	ch-test2	ch-test2	2023-05-12 09:58	Engineering Ingegneria Informatica-PlatoneUser	Download
Forecasts_03_113	Malta	ch-test	ch-test	2023-05-12 09:41	Engineering Ingegneria Informatica-PlatoneUser	Download

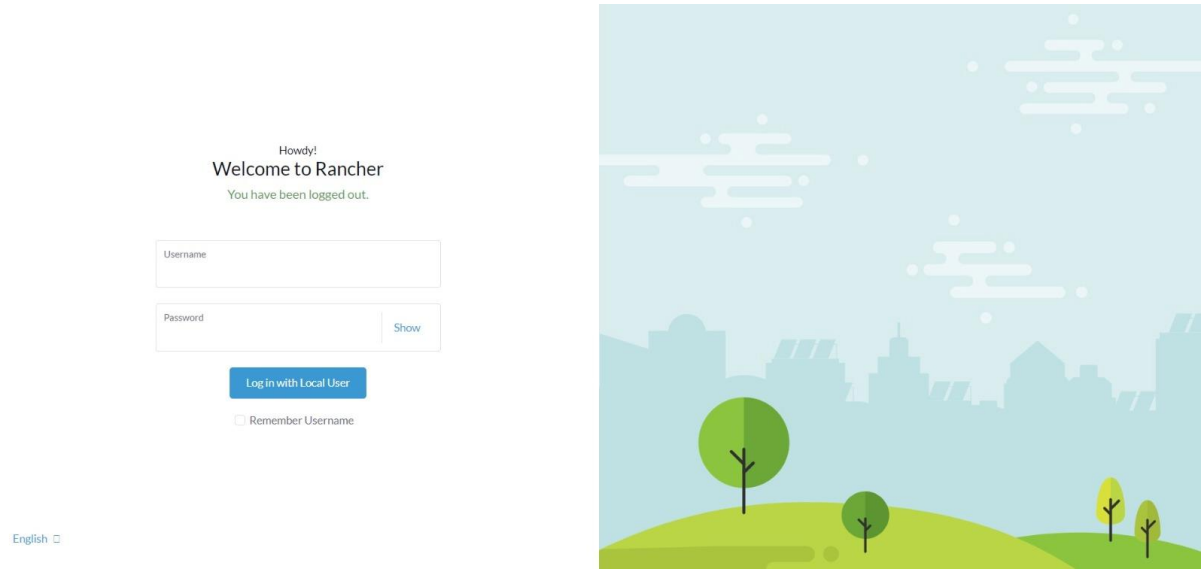
Screen 28: OneNet Orchestration Workbench Subscriptions and Data Consumption section

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

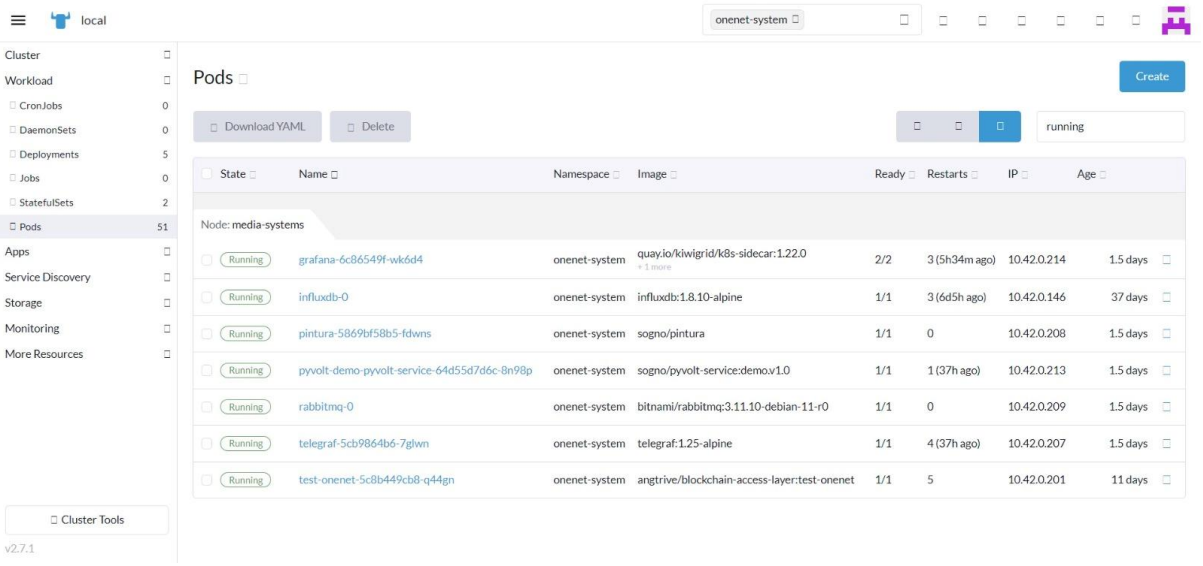
A.2.3 Service Deployment, Orchestration and Monitoring

The OneNet Participant, acting as Service Provider can deploy its own service into the Microservice Orchestration Layer, based on Rancher 2.0 and Kubernetes. This platform allows to deploy, monitoring and orchestrate service in automatic way.

The Rancher GUI is available only for the administrator of the Orchestration Workbench, while all the provided functionalities (deploy, monitoring, etc..). are available via APIs through the Orchestration Workbench GUI. The screens below show some sections of Rancher GUI: login (Screen 30), deployed services (Screen 31), services status and monitoring (Screen 32).

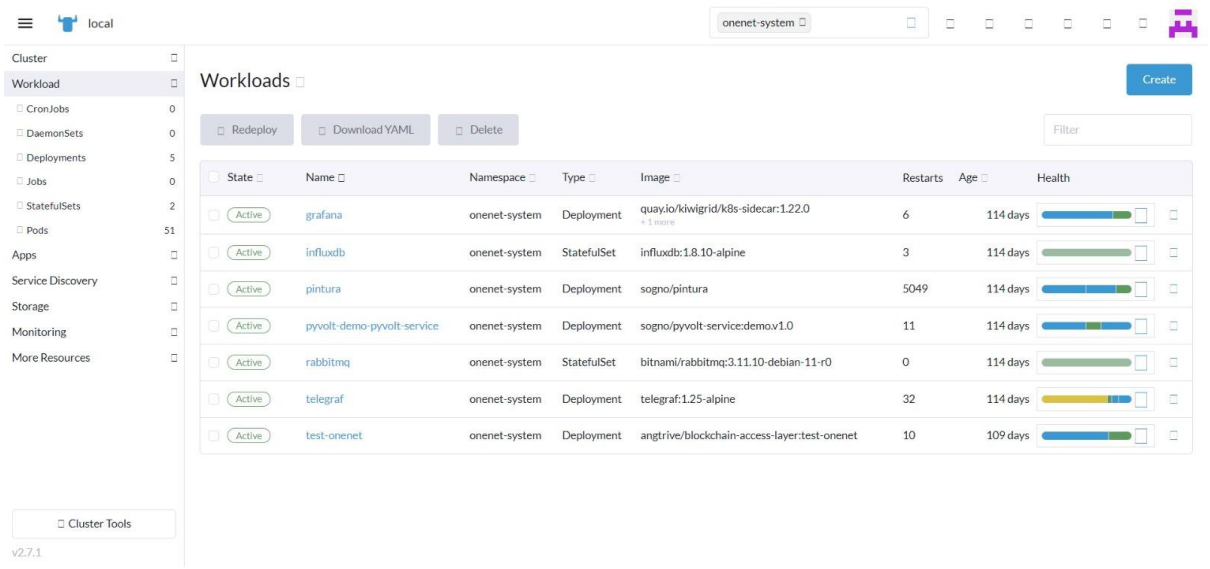


Screen 30: Microservice Orchestration Layer - Rancher Login



Screen 31: Microservice Orchestration Layer - Deployed services

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

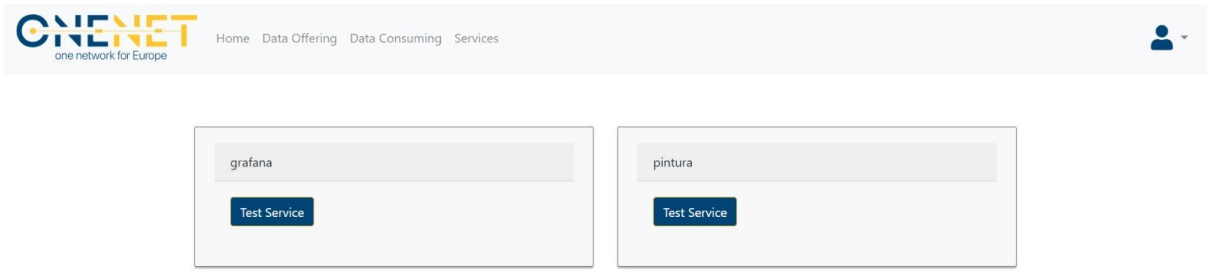


Screen 32: Microservice Orchestration Layer - Services monitoring

A.2.4 Service Catalogue

All the service deployed shown in the Orchestration Workbench Dashboard can integrate data coming from the OneNet Connector. The OneNet Orchestration Workbench provides an interface for exploring the Service Catalogue and test any available service with the integrated data.

The Screen 33 below shows an example of Service Catalogue with two services ready to be tested.

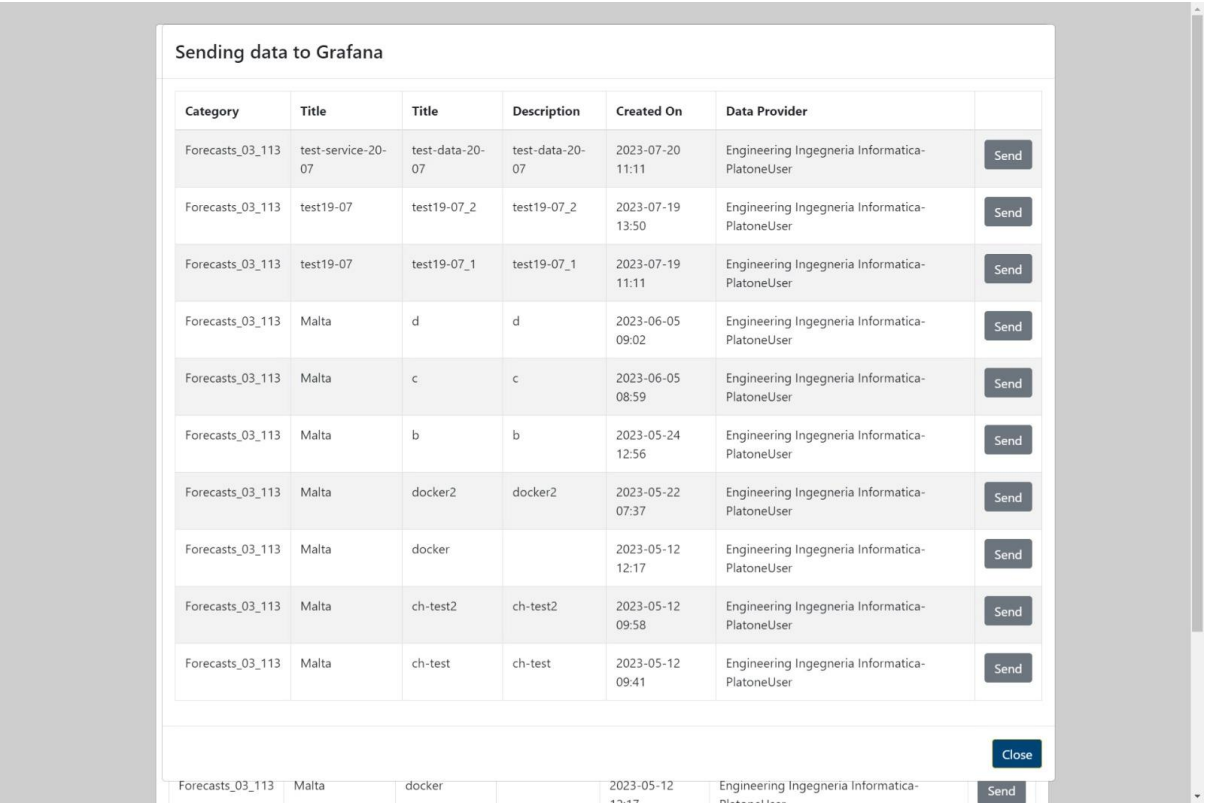


Screen 33: OneNet Orchestration Workbench - Service Catalogue

A.2.5 Service Execution

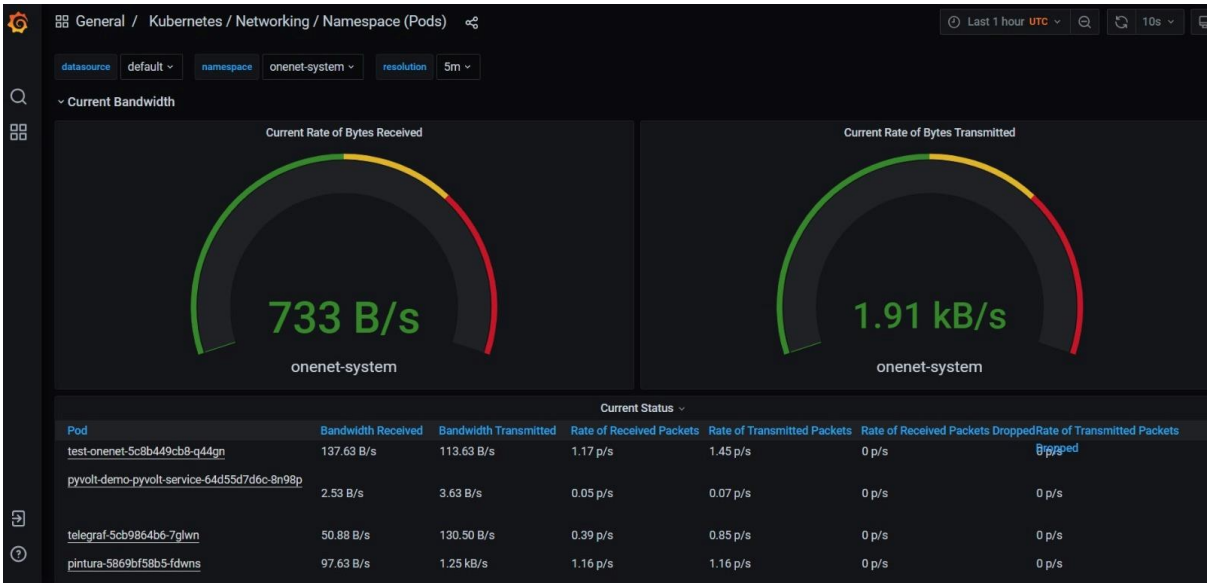
After exploring the Service Catalogue, the OneNet Participant can test any of the service available, using OneNet Connector integrated data. The Screen 34 shows an example of service execution, in which the OneNet Participant can select the data to be provided to Grafana for data visualization.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



Screen 34: OneNet Orchestration Workbench - Service execution and data integration

A.2.6 Performance evaluation

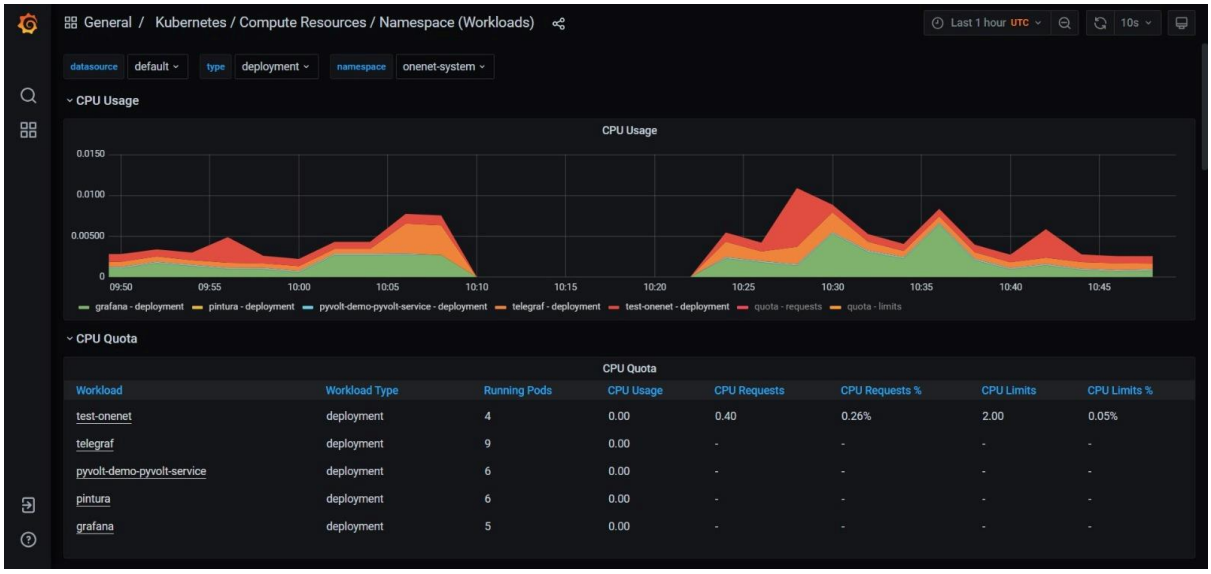


Screen 35: OneNet Orchestration Workbench - Overall system evaluation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

The Orchestration Workbench also includes an open-source monitoring solution based on Prometheus.io. It allows to monitor any service deployed in the Orchestration Workbench and to provide and kind of insights and alerting.

The screens show how the monitoring service, integrated with Grafana is able to monitor the overall system (Screen 35) and a specific service (Screen 36).



Screen 36: OneNet Orchestration Workbench - Service monitoring

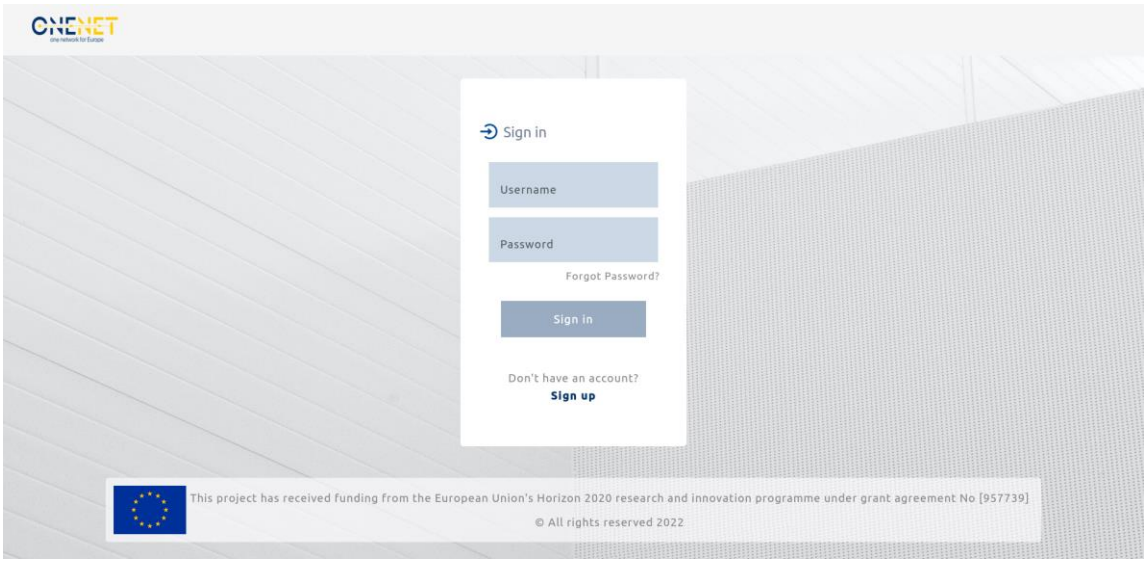
A.3 OneNet Monitoring and Analytics Dashboard

The OneNet Network Monitoring and Analytics Dashboard is designed to provide the OneNet administrator and OneNet users with historical and real-time data regarding requests to Connectors, security reporting, alerting and filtering capabilities. This section will guide the user through the key available features of this web application.

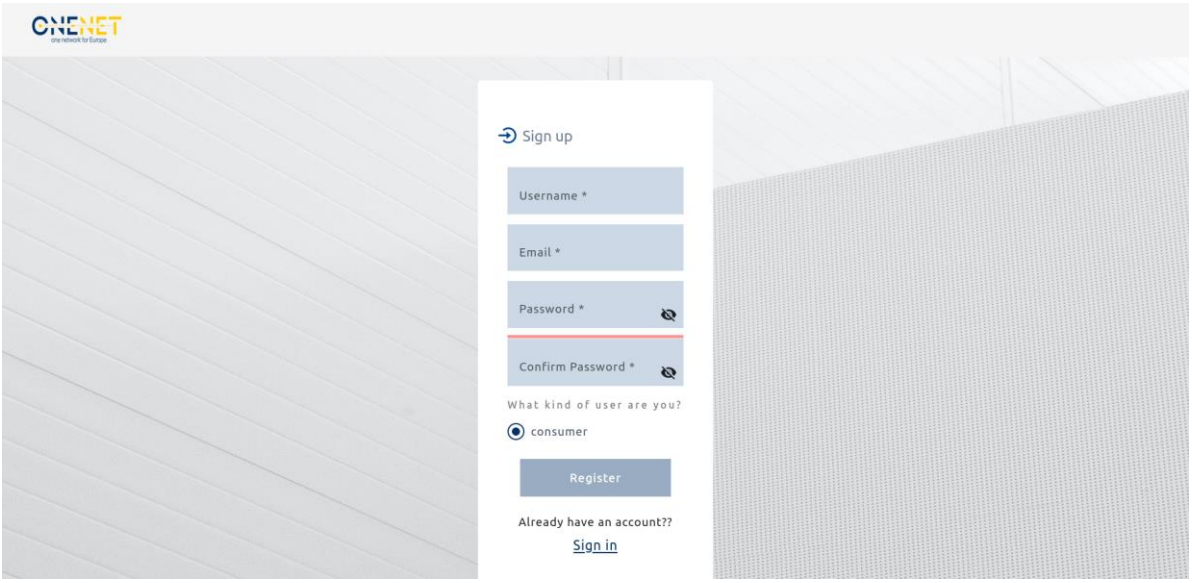
The Dashboard may be accessed by navigating to the following URL: https://dashboard-eu-onenet.euprojects.net

The Dashboard user may authenticate using their username and password credentials through the authentication page. In the same page, the user may click on the Sign up link to register an account if it is their first time using the Dashboard.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



Screen 37: Dashboard login page

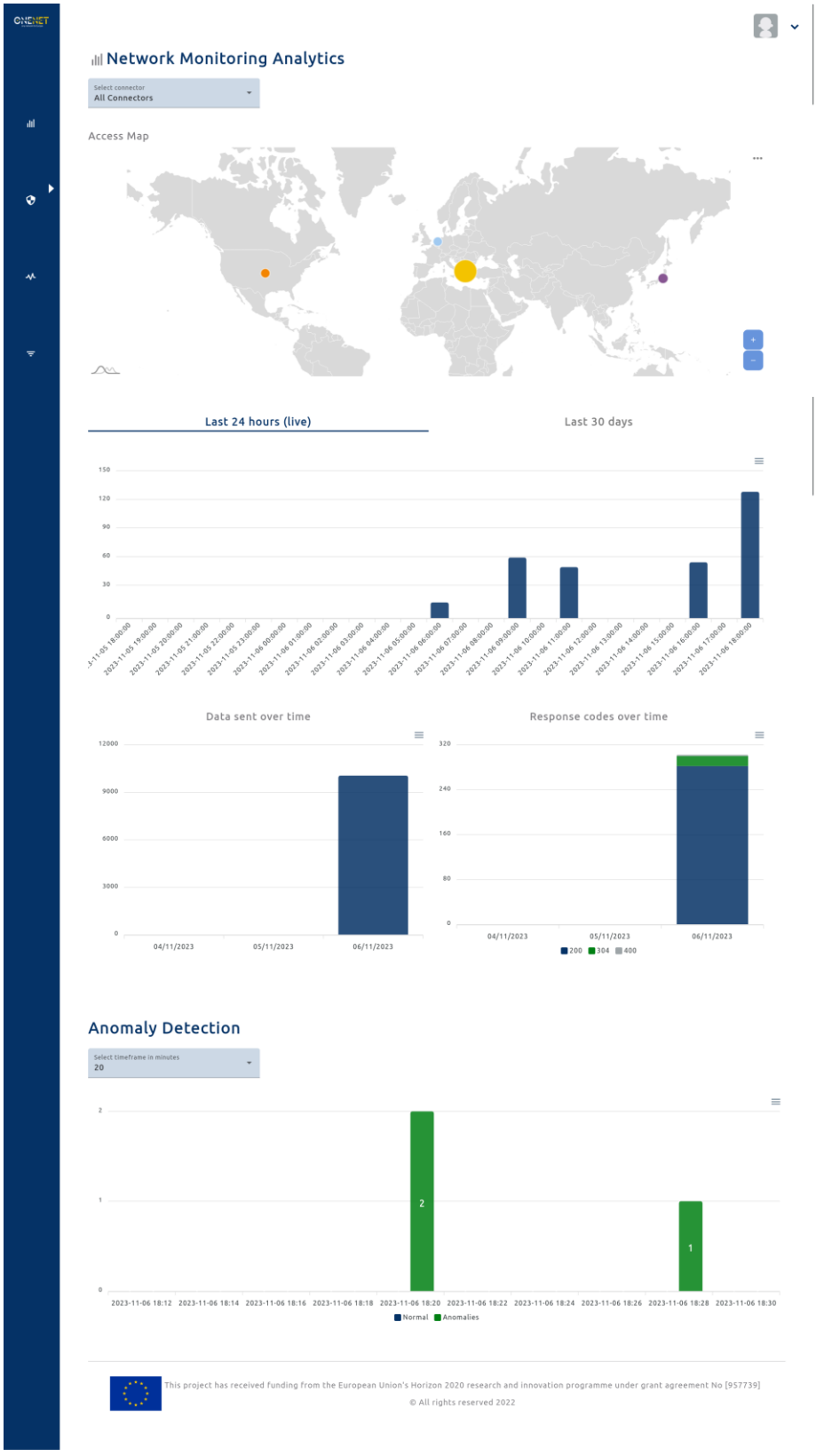


Screen 38: Dashboard register page

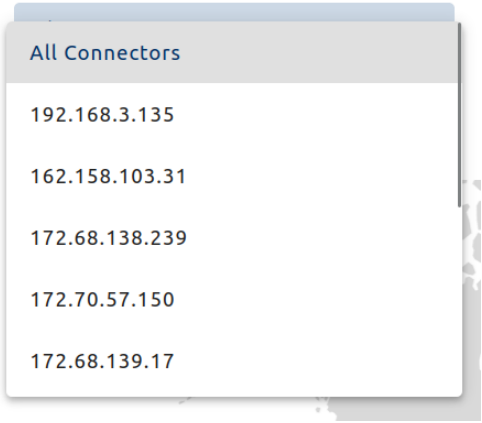
A.3.1 Network Monitoring Analytics

Upon successful authentication, the user is presented with the Network Monitoring Analytics page which provides information organized in a number of charts. Firstly, at the top of the page, a dropdown menu allows the user to select a specific Connector whose statistics they are interested in. By default, the data displayed is an aggregate of all Connectors.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



Screen 39: A full view of the Network Monitoring Analytics page



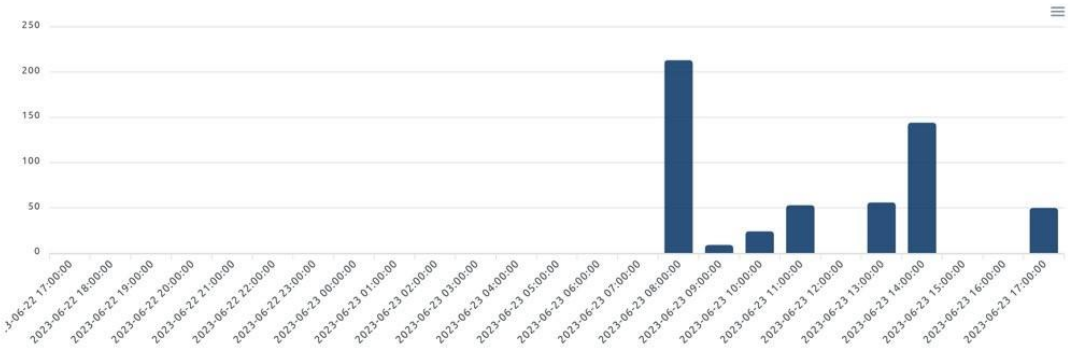
Screen 40: Connector selection dropdown menu

Under this menu, a map chart displays a visual representation of requests per country of origin as circles on the world map. Each country is colour coded and the size of the circle represents the volume of requests from the respective country. It is possible to hover over a circle to view the country name and the total number of requests. Zooming is supported with the plus and minus signs on the bottom right corner of the chart, while panning is supported by clicking and dragging on the chart.

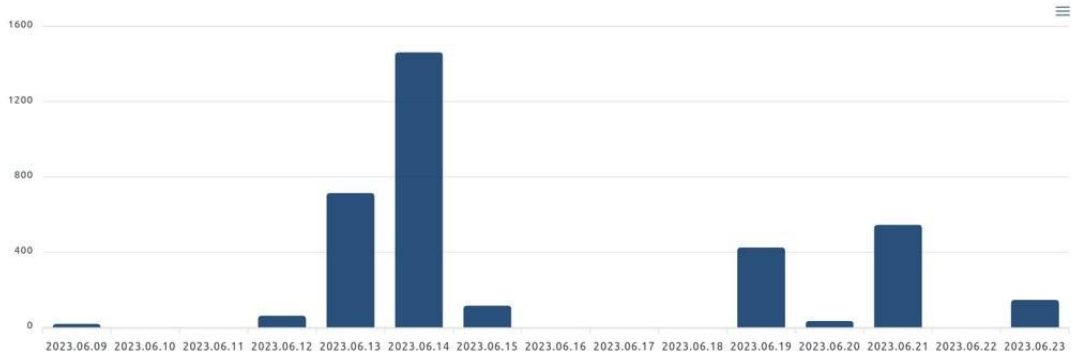
Screen 41: Requests per country map chart

Next, the two following charts visualize the number of requests being made in the last 24 hours and in the last 14 days respectively. The user may switch between viewing these two charts by clicking their respective tab. The total requests per time slot are represented as bars which may be hovered over to display the exact number of requests as well as the time slot. The first chart displays real-time data per hour, without the need of reloading or re-navigating to the page, updated roughly every 10 seconds, while the second chart displays historical data per day.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



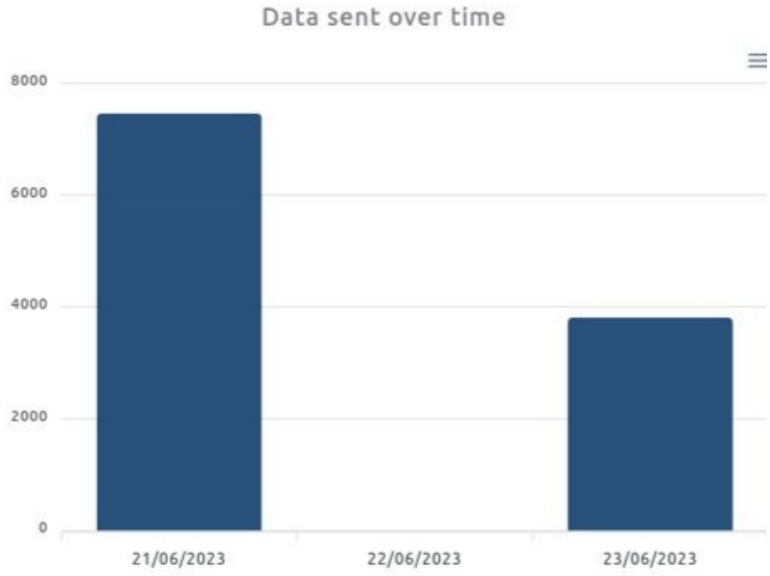
Screen 42: Requests in the last 24 hours (live) bar chart



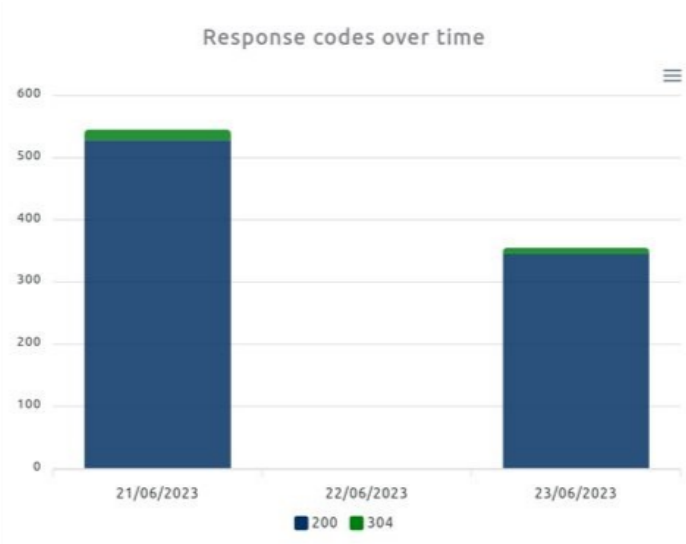
Screen 43: Requests in the last 14 days bar chart

In the next row of charts, there is the data sent over time chart on the left and the response codes over time chart on the right. The data sent over time chart displays the total number of bytes sent per day by the selected Connector for the last three days. Similarly, the response codes over time chart visualizes the number of responses sent by the selected Connector, grouped by response code, for the last three days.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



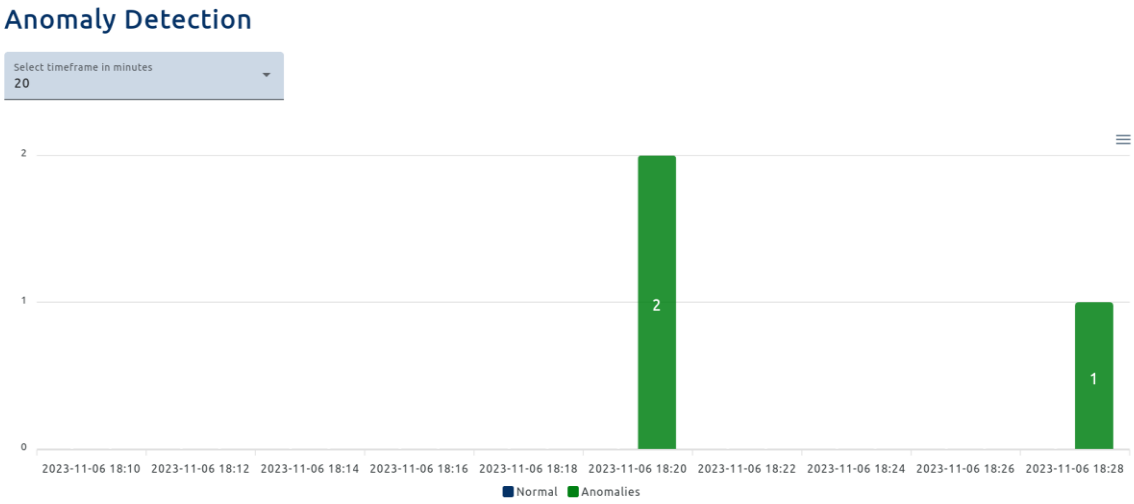
Screen 44: Data sent over time



Screen 45: Response codes over time

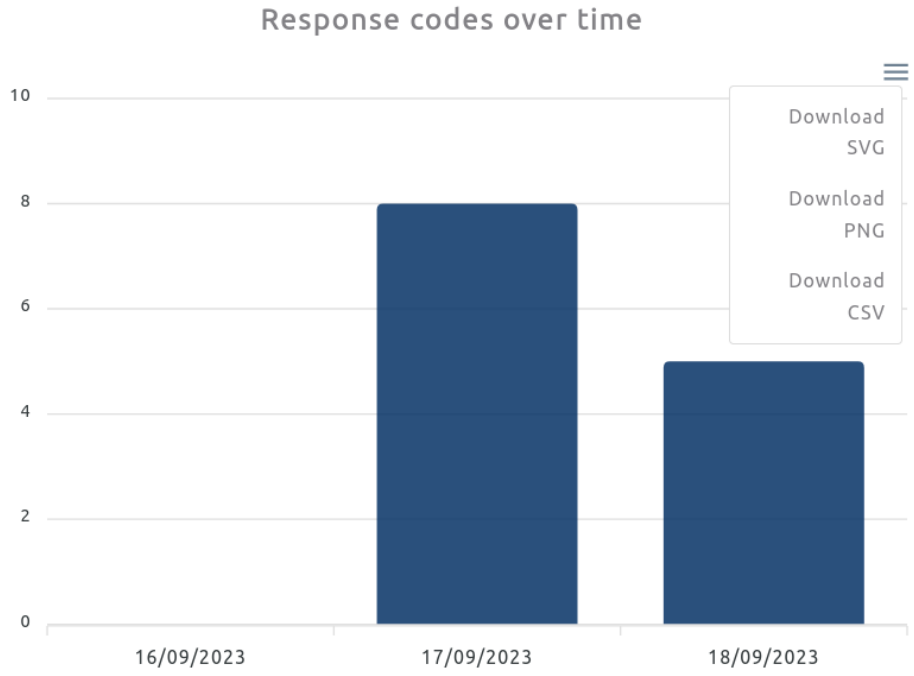
Finally, the anomaly detection chart employs machine learning algorithms to identify irregular client behaviour. It may display information regarding the last 20, 40 or 60 minutes. The user may select the desired time frame by using the dropdown menu at the top of the chart. Each time slot is represented by a maximum of two bars, one displaying the number of normal clients and one displaying the number of abnormal clients within a given time slot.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



Screen 46: Anomaly detection bar chart

By clicking on the button on the top right corner of each chart surface, the user may download a still image of the associated chart in PNG format or export and download the chart's data in CSV format.

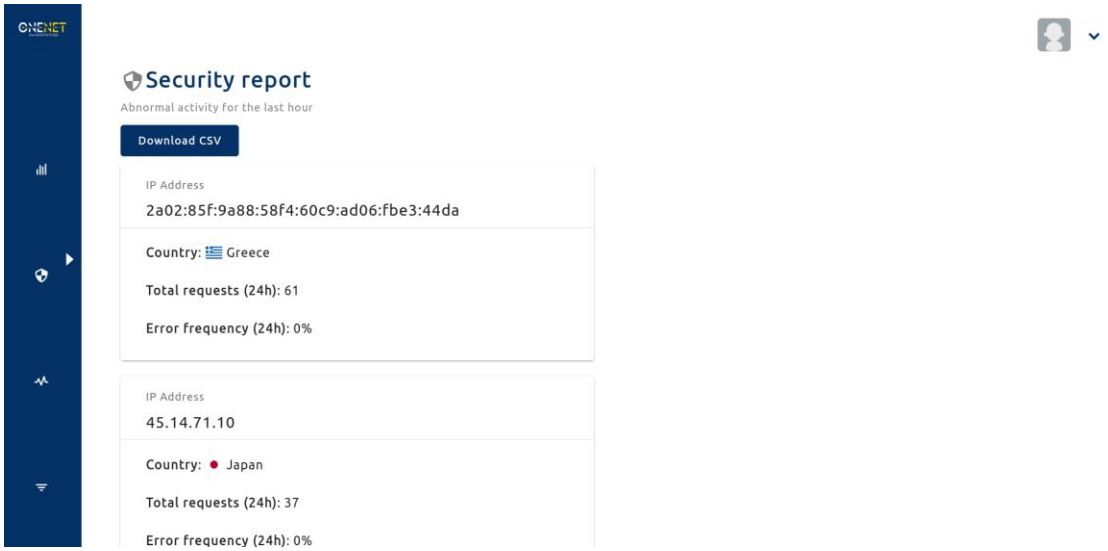


Screen 47: The export and download menu of the Response codes over time chart of the Dashboard

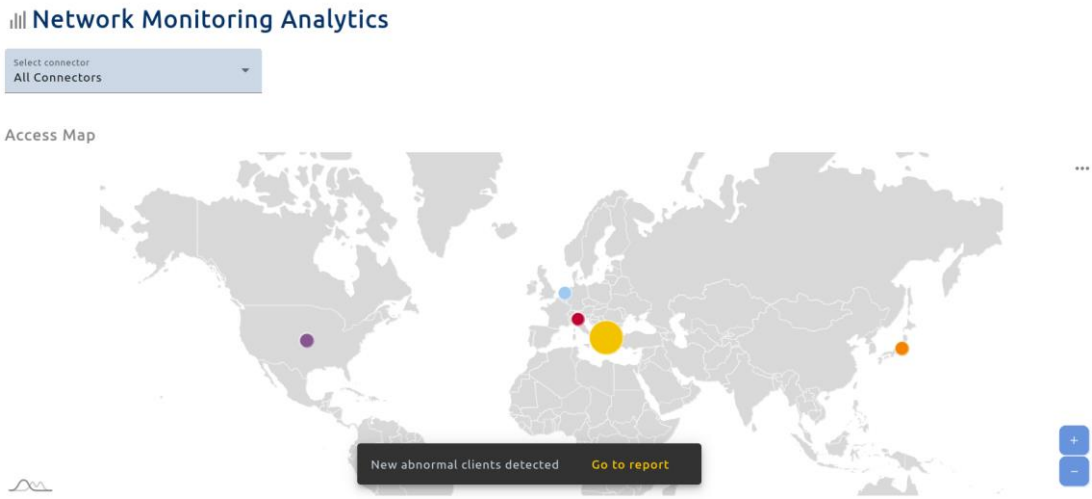
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A.3.2 Security Report

Navigating to the security report page, marked by a shield icon in the sidebar, a security report is generated which displays information about any detected abnormal clients. This information includes the IP address and the country of the client, the number of requests made in the last 24 hours and the percentage of these requests that led to an error. The user may export and download the data in CSV format by clicking on the Download CSV button at the top of the page. Furthermore, the user is alerted whenever a new abnormal client is detected, through a notification that appears at the bottom of the page which includes a button that redirects the user to the security report page.



Screen 48: Security report page



Screen 49: An alert that notifies of new abnormal clients and directs the user to the security report page

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

A.3.3 Health Check

The health check page displays a list of Connector IP addresses and the last time their web page was used by a client. It is used to classify the Connector as Online with a green icon if it has been used in the last week, as Idle with an orange icon if it has been used in the last 60 days and offline otherwise.

Screen 50: Health check page

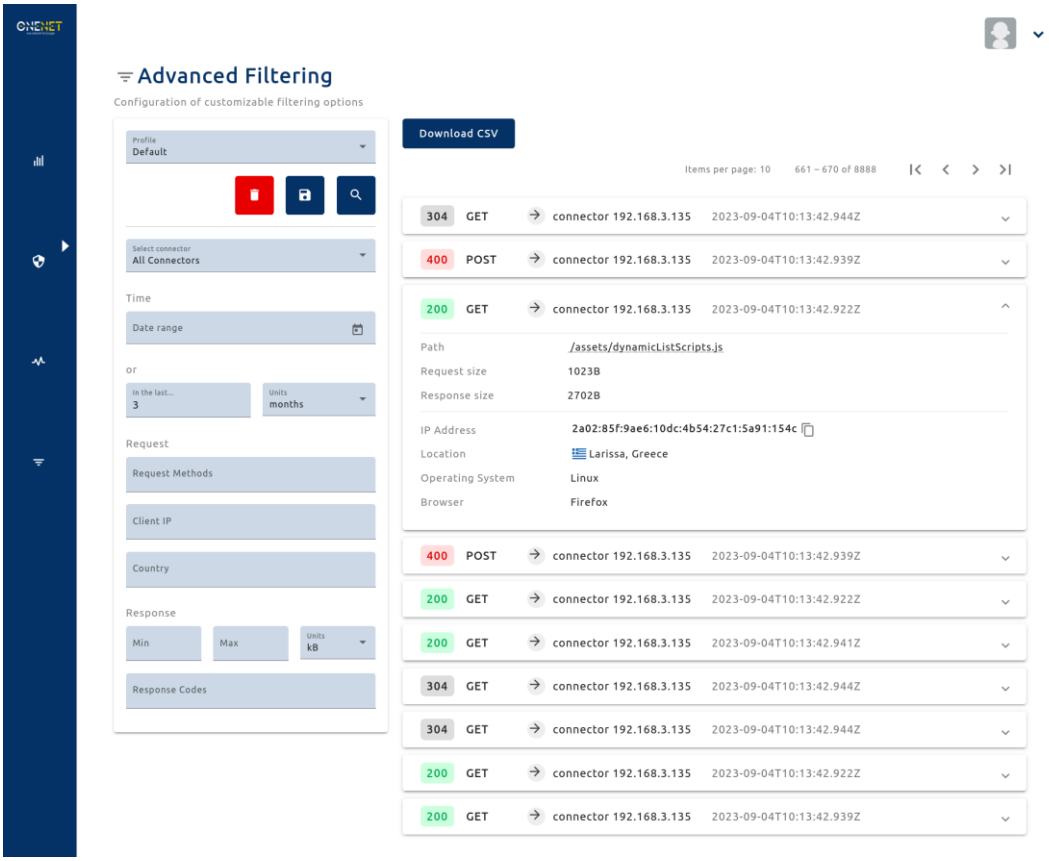
A.3.4 Advanced Filtering

The advanced filtering page allows searching for requests with specific properties based on the search criteria used, such as date, request method, response size, response code, client IP address and country. The left side of the page is used to configure the search criteria while the right side of the page is reserved for the list of results.

After selecting the desired criteria, the user may click on the lens icon to initiate a search. Initially, results are folded so that only minimal information is visible. Each result may be expanded when clicked on to reveal all available information, such as the request timestamp, the Connector IP address, the request path, size and method, the response code and size, the requesting client's IP address, country, city, operating system and browser.

By clicking on the save button under Profile, it is possible to save an advanced filtering configuration so that it may be reused in the future. Clicking the button brings up a dialog where the user may enter the name under which the current advanced configuration profile will be saved. The profile will then be stored in the browser cache and will persist across page reloads. By selecting a profile from the Profile dropdown menu at the top, the saved search criteria are automatically filled in.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739



Screen 51: Advanced filtering page

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739