

**Status Dashboard service
Cookbook
Version 1.3**

This document is provided to you free, of charge, by the

eHealth platform

**Willebroekkaai 38 – 1000 Brussel
38, Quai de Willebroek – 1000 Bruxelles**

Anyone is free to distribute this document, referring to the URL source.

Table of contents

Table of contents	2
1. Document management	3
1.1 Document history (to complete)	3
2. Introduction	4
2.1 Goal of the service	4
2.2 Goal of the document	4
2.3 Service history	4
3. Support	5
3.1 Helpdesk eHealth platform	5
3.1.1 Certificates	5
3.1.2 For issues in production	5
3.1.3 For issues in acceptance	5
3.1.4 For business issues	5
3.2 Status	5
4. Global overview	6
5. Step-by-step	7
5.1 Technical requirements	7
5.1.1 Tracing	7
5.2 Process overview	7
5.3 Web service	8
5.3.1 Method #1	8
6. Risks and security	10
6.1 Security	10
6.1.1 Business security	10
6.1.2 Web service	10
6.1.3 The use of username, password and token	10
7. Test and release procedure	11
7.1 Procedure	11
7.1.1 Initiation	11
7.1.2 Development and test procedure	11
7.1.3 Release procedure	11
7.1.4 Operational follow-up	11
7.2 Test cases	11
8. Error and failure messages	12

To the attention of: "IT expert" willing to integrate this web service.



1. Document management

1.1 Document history (to complete)

Version	Date	Author	Description of changes / remarks
1.0	17/01/2025	Smals	First version of the document by Lionell Fernandez
1.1	07/02/2025	Smals	First review by Mathieu De Keyzer
1.2	13/02/2025	Smals	Changes made by Lionell Fernandez after first review of 1.1
1.3	05/03/2025	Smals	Changes made after the review of eHealth Service Management

2. Introduction

2.1 Goal of the service

The primary goal of the Status Dashboard service is to provide real-time monitoring and visualization of the operational status of various eHealth services. This service ensures that stakeholders can easily access and utilize the provided data through a simple API.

2.2 Goal of the document

This document is not a development or programming guide for internal applications. Instead, it provides functional and technical information to enable an organization to integrate and use the eHealth platform service.

However, ensure smooth, consistent and risk controlled interactions with a maximum number of partners, these partners must commit to complying with the specifications, data format and release processes of the eHealth platform as described in this document.

Both technical and business requirements must be met, to allow the integration and validation of the eHealth platform service in the client application.

2.3 Service history

This chapter contains the list of changes made to the service with respect to the previous version.

Previous version	Previous release date	Changes
1.0 Current version	15/01/2025	INITIAL REST version
1.1 First review	07/02/205	Review by Mathieu De Keyzer
1.2 Second version	13/02/2025	Changes made by Lionell Fernandez after first review of 1.1
1.3 Third version	05/03/2025	Changes made after the review of eHealth Service Management

3. Support

3.1 Helpdesk eHealth platform

3.1.1 Certificates

To access the secured eHealth platform environment you must obtain an eHealth platform certificate, which is used to identify the initiator of the request. If you do not have one, please consult the chapter about the eHealth Certificates on the portal of the eHealth platform

- <https://www.ehealth.fgov.be/ehealthplatform/nl/ehealth-certificaten>
- <https://www.ehealth.fgov.be/ehealthplatform/fr/certificats-ehealth>

For technical issues regarding eHealth platform certificates

- Acceptance: acceptance-certificates@ehealth.fgov.be
- Production: support@ehealth.fgov.be

3.1.2 For issues in production

eHealth platform contact centre:

- Phone: 02 788 51 55 (on working days from 7 am till 8 pm)
- Mail: support@ehealth.fgov.be
- Contact Form :
 - <https://www.ehealth.fgov.be/ehealthplatform/nl/contact> (Dutch)
 - <https://www.ehealth.fgov.be/ehealthplatform/fr/contact> (French)

3.1.3 For issues in acceptance

Integration-support@ehealth.fgov.be

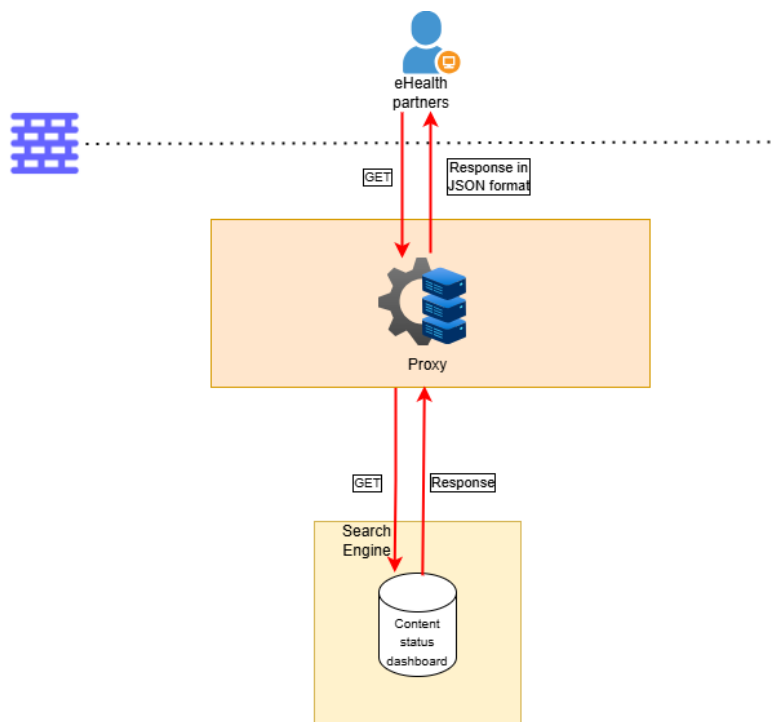
3.1.4 For business issues

- regarding an existing project: the project manager in charge of the application or service
- regarding a new project or other business issues: info@ehealth.fgov.be

3.2 Status

The website <https://status.ehealth.fgov.be> is the monitoring and information tool for the ICT functioning of the eHealth services that are partners of the Belgian eHealth system.

4. Global overview



URL :

- PROD

<https://status.ehealth.fgov.be/api/v1/dashboard>

5. Step-by-step

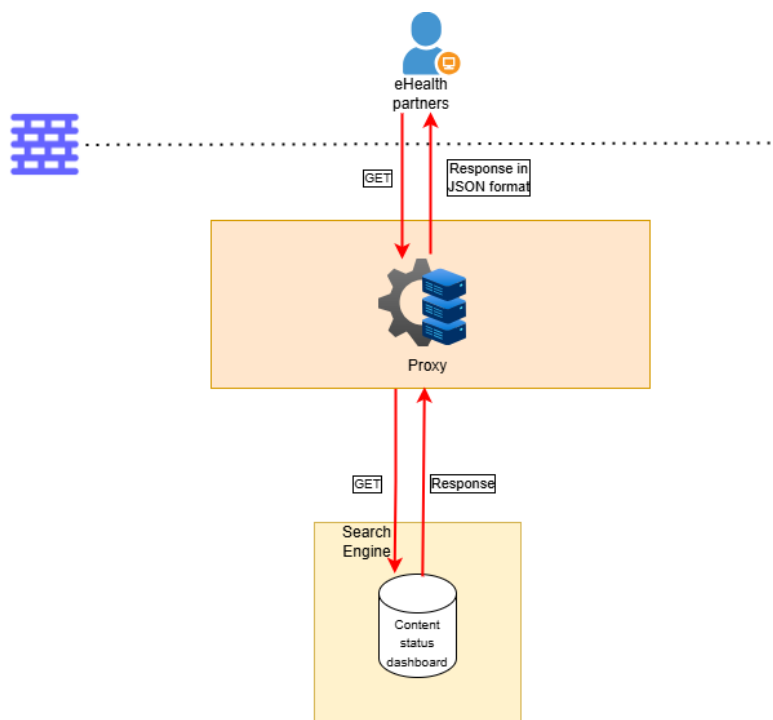
5.1 Technical requirements

5.1.1 Tracing

To use this service, the request SHOULD contain the following two http header values (see RFC <https://datatracker.ietf.org/doc/html/rfc7231#section-5.5.3>):

1. User-Agent: information identifying the software product and underlying technical stack/platform. It MUST include the minimal identification information of the software such that the emergency contact (see below) can uniquely identify the component.
 - a. Pattern: {minimal software information}/{version} {minimal connector information}/{connector-package-version}
 - b. Regular expression for each subset (separated by a space) of the pattern: `[[a-zA-Z0-9-V]*V[0-9azA-Z-_.]*`
 - c. Examples:
User-Agent: myProduct/62.310.4 Technical/3.19.0
User-Agent: Topaz-XXXX/123.23.X freeconnector/XXXXX.XXX
2. Accept must be specified with the value application/json

5.2 Process overview



The eHealth partner sends a GET request via an URL: <https://status.ehealth.fgov.be/api/v1/dashboard>
The response is in JSON format.

URL :

- PROD

<https://status.ehealth.fgov.be/api/v1/dashboard>

- INT

<https://status.ehealth.fgov.be/api/v1/dashboard/int>

- ACC

<https://status.ehealth.fgov.be/api/v1/dashboard/acc>

5.3 Web service

5.3.1 Method #1

5.3.1.1 Input arguments #1

The eHealth partner sends a GET request via an URL : <https://status.ehealth.fgov.be/api/v1/dashboard>

5.3.1.2 Output arguments #1

The response is in JSON format, as shown in the following example:

```
{
  groups: [
    {
      id: "AXAQooF-9v9nOdhekPYm",
      name: "1. IAM - Identity & Access Management",
      items: [
        {
          id: "715d31b5a498a4587fedc57dada6a9df",
          order: 1,
          status_code: 1,
          last_updated: "2025-04-08T11:30:00+02:00",
          name: "eHealth IDP - Identity provider - Authorization management",
          description: "User can not select profile anymore for each online services protected by IDP"
        }
      ]
    }
  ]
}
```


}

Field name	Description
groups	List of groups containing monitored items.
id (group)	Unique identifier of the group (e.g., "AXAQooF-9v9nOdhekPYm").
name (group)	The name of the group (e.g., "1. IAM - Identity & Access Management"). All the names used on the dashboard eHealth Status are in English.
items	List of individual items belonging to the group.
id (item)	A unique identifier for this specific status entry.
order	The order or priority of this status entry within its group (e.g. first line seen on the front-end).
status_code	A numerical code representing the current status : - 1 = The status is considered Operational - 2 = The status is considered Disrupted - 3 = The status is considered Unknown
last_updated	The timestamp indicating when this status entry was last updated. The format is in ISO 8601 format (e.g., "2025-03-05T09:25:00+01:00")
name (item)	The name of the specific service or component in English (e.g., "eHealth IDP - Identity provider - Authorization management"). All the names used on the dashboard eHealth Status are in English.
description	A description of the issue or status in English (e.g., "User can not select profile anymore for each online services protected by IDP"). All the description encoded on the dashboard eHealth Status are in English.

6. Risks and security

6.1 Security

6.1.1 Business security

If the development adds a use case based on an existing integration, the eHealth platform must be informed at least one month in advance. A detailed estimate of the expected load is necessary to be able to ensure effective capacity management.

When technical issues occur with the WS, the partner can obtain support from the contact centre (see Chap 3).

If the eHealth platform identifies a bug or vulnerability in its software, the partner must update his application with the latest version of the software, within ten (10) business days.

If the partner finds a bug or vulnerability in the software or web service provided by the eHealth platform, he is obliged to contact and inform us immediately. He is not allowed, under any circumstances, to publish this bug or vulnerability.

6.1.2 Web service

WS security used in this manner is in accordance with the common standards. Your call will provide:

- SSL one way

6.1.3 The use of username, password and token

Not applicable

7. Test and release procedure

7.1 Procedure

This chapter explains the procedures for testing and releasing an application in acceptance or production.

7.1.1 Initiation

If you intend to use the eHealth platform service, please contact:

ehealth_service_management@ehealth.fgov.be

The project department will provide you with the necessary information and mandatory documents.

7.1.2 Development and test procedure

You need to develop a client to connect to our WS. Most of the information for integration is published within this document.

Upon request and depending on the case, the eHealth platform provides you with a **test case** to test your client before releasing it in the acceptance environment.

7.1.3 Release procedure

For further information and instructions, please contact: integration-support@ehealth.fgov.be.

7.1.4 Operational follow-up

Once in production, the partner using the eHealth platform service for one of his applications must always test in the acceptance environment first before releasing any adaptations of his application in production. In addition, he will inform the eHealth platform on the progress and test period.

7.2 Test cases

The eHealth platform recommends performing tests for all of the following cases:

- <https://status-sim.ehealthplatform.info/api/v1/dashboard>

8. Error and failure messages

We rely on standard HTTP error codes.

