Trust.med

DataX Developer API Guide

Document Details

Document Status	Approved
Date Modified	Oct 1, 2025
Document Owner	John Winkler
Reviewers	Dan Kraciun
Distribution	External

Introduction

Welcome to the Trust.med API documentation, your gateway to seamless integration with Trust.med's utilities for secure and efficient healthcare supply chain communication. Trust.med empowers partners with a suite of powerful communication utilities to enhance transparency, streamline operations, and ensure the highest standards of product quality and patient safety.

Our API enables you to perform the following actions:

1. **Submit EPCIS Data:** Seamlessly exchange Electronic Product Code Information Services (EPCIS) data with your trading partners. Whether you prefer direct file transfers or transmitting EPCIS data as an XML string body, Trust.med provides you with the flexibility you need. Your XML data should encompass an EPCIS Header, complete with a Standard Business Document Header, and an EPCIS Body housing an Event List.

2. **EPCIS Data Publishing**: Trust.med's DataX is able to send data to your downstream partners via API. Much like the Submission of EPCIS data, Trust.med will deliver the EPCIS document as an XML post body to an API endpoint via secure channels.

3. **Search for EPCIS Datafiles:** Search through the list of EPCIS documents sent to your companies utilizing the company identifier + a list of filter options. The logs will be provided in JSON format.

4. **Generate Download Link for EPCIS**: Create a short-lived link that allows for a user to download the raw, original, EPCIS file that was stored in the system.

Table of Contents

Authentication

The Trust.med API utilizes two methods for Authentication:

1. mTLS Certificate based authentication
2. JWT Token based authentication
    a. Backed by Basic Authentication: Username and Password

Certificate Authentication

In order to authenticate via certificate, you must complete the following:

1. Generate a self-signing CA Certificate (or use an accepted signed like Verisign)
2. Trade Public keys of CA or CA bundles with Trust.med.
3. Generate and sign your client certificate using the CA.
4. Provide your signed client certificate with all requests.

After Step 3, Trust.med support will need to associate the CN value from your certificate with an account in the system. If your CN value changes at any time, Trust.med will need to verify the new CN value and update this within our platform.

JWT Token Authentication

Authentication Type: Username/Password Basic Authentication
TEST Domain: https://demo.dashboard.trust.med/v1.0
PROD Domain: https://dashboard.trust.med/v1.0

POST /token/

API endpoints contained in this document that require the use of an access token passed within the header of the request in order to facilitate authentication.

Example Header:

```
"Authorization: Bearer 123abc...987zyx"
```

In order to generate the access token, follow these steps:

1. Gather your username and password.
2. Send a request to the Access Token Generation endpoint.
3. You will send the username, password, scope, grant_type and client_id as Post Body elements.
4. Gather the access token from the response that comes back.

Example

Request Body

Data	Format	Description
username	string	The Username for your API account
password	string	The Password for your API account
client_id	Exact	dotmed
scope	Exact	openid

```
{
       "username": "your-username",
       "password": "your-password",
       "client_id": "dotmed",
       "scope": "openid"
}
```

Response

When successful, the API will return a HTTP 200_OK response with the following body:

```
{
  "access_token": "abc123...987zyx",
  "expires_in": 2592000,
  "token_type": "Bearer"
}
```

EPCIS Data Submission

Note: The EPCIS Data Submission endpoint and authentication type are different from the other endpoints in this document, please ensure you are using the right domain, endpoint, and authentication for the request you are looking to make.

Authentication Type: mTLS Certificate Based Authentication
TEST Domain: https://demo.partner.trust.med/v1
PROD Domain: https://partner.trust.med/v1

POST: /client/storage/

By submitting a file as an “application/xml” or “text/xml” content type, Trust.med will capture, consume, and route the appropriate EPCIS information to your, and the downstream partner’s, data repositories.

If the downstream partner has been configured with a service provider integration, we will also deliver the information to the partner via that service provider method configured.

It is important that the Sender GLN and the Receiver GLN be provided within the Standard Business Document Header for identification and routing purposes for all **Standard/Direct Ship** data communications. **Drop Ship** data communications will utilize the Trust.med GLN as the receiver GLN.

Example

Request Body

```
<?xml version="1.0" encoding="utf-8"?>
<EPCISDocument xmlns:cbvmda="urn:epcglobal:cbv:mda" xmlns:gs1ushc="http://epcis.gs1us.org/hc/ns"
schemaVersion="1.2" xmlns="urn:epcglobal:epcis:xsd:1">
  <EPCISHeader>
    <StandardBusinessDocumentHeader
xmlns="http://www.unece.org/cefact/namespaces/StandardBusinessDocumentHeader">
      …
    </StandardBusinessDocumentHeader>
  </EPCISHeader>
  <EPCISBody>
    <EventList>
      …
    </EventList>
  </EPCISBody>
</EPCISDocument>
```

Response

When successful, the API will return a HTTP 200_OK response with the following body:

```
{
    "id": UUID4 ID,
    "created_at": Datetime
}
```

EPCIS Data Publishing

Authentication Type: mTLS Certificate Based, Basic Authentication, Header Based (E.G. API-Key)

Our system is designed to reliably and securely transmit EPCIS data to downstream partners, ensuring data integrity and confidentiality throughout the process. By leveraging HTTPS endpoints and adhering to industry-standard authentication protocols the system guarantees that data is delivered only to explicitly authorized recipients.

Trust.med is also able to publish EPCIS over AS2 and SFTP protocols. If interested, reach out to your support representative for documentation surrounding these protocols.

EPCIS Datafile Search

Authentication Type: Basic Authentication (Token)
TEST Domain: https://demo.dashboard.trust.med/v1.0
PROD Domain: https://dashboard.trust.med/v1.0

GET: /de-status/company/{COMPANY_ID}/log/

The system was designed to allow for easy access to your data via an API based approach. With a quick query, you can see all of the recent files that have been sent to, from, or both to and from you over a set period of time. This API endpoint features pagination as well as in-depth filtering.

Request Parameters & Query String Parameters

Data	Format	Description
company_id	string	The numerical ID of your company
start	Datetime	YYYY-MM-DDTHH:mm:ssZ format
end	Datetime	YYYY-MM-DDTHH:mm:ssZ format
page	Number	Pagination page
filetype	Choice	epcis1.2 **OR** edi856 - default is epcis1.2
gtin	String	Global Trade Item Number value
bt	String	Business Transaction Value (desadv, po, rma, etc…)
lot	String	Lot Number
iid	String	EPCIS Document Identifier from the SBDH
filter_receiver	String	Downstream partner name, fuzzy search
pl	Choice	Direction of data. Can be used if you both send and receive files through Trust.med. • **b** - Both Directions • **s** - Sender Only • **r** - Receiver Only

Example

Response

When successful, the API will return a HTTP 200_OK response with the following body:


```
{
    "count": 5000,
    "next":
"http://demo.api.trust.med:8081/api/v1.0/de-status/company/1/log/?page=2",
    "previous": null,
    "results": [

          {
            "logGuid": "X-UUID-VALUE-X",
            "created_at": "2025-01-01T12:00:00Z",
            "updated_at": "2025-01-01T12:00:00Z",
            "source_file": "mytest.xml",
            "source_name": "Development Testing",
            "sender": "12345678901234",
            "sender_name": "Testing Manufacturer",
            "is_sender": true,
            "receiver": "43210987654321",
            "receiver_name": "Testing Dispensary",
            "outbound_logs": [
                {
                    "created_at": "2024-04-12T12:21:58Z",
                    "updated_at": "2024-05-10T19:54:32.996062Z",
                    "file_name": "mytest.xml",
                    "success": true,
                    "status_code": "1",
                    "log_msg": "",
                    "mdn_id": "success_12345_test",
                    "pipeline_name": "Test Pipeline"
                },
            ],
            "status": 4,
            "statusMsg": "Success",
            "fail_point": null,
            "fail_reason": null,
            "is_dropship": false,
            "filetype": "epcis1.2",
            "content_hash": null,
            "receiver_reference": null
        }, …
     ]
}
```


Generate EPCIS Raw Download Link

Authentication Type: Basic Authentication (Token)
TEST Domain: https://demo.dashboard.trust.med/v1.0
PROD Domain: https://dashboard.trust.med/v1.0
GET: /de-status/log/{LOG_UUID}/download

This system was developed to work in tandem with the endpoint to search for a datafile. This is necessary because of the way we store and secure datafiles. They are normally private, locked to the outside world. This endpoint allows us to authenticate a user and verify that they are who they say they are before they are granted access to the datafile requested. Once approved, a download link is provided via a link, which lives for 10 minutes.

The LOG_UUID value is the logGuid from the response above.

The response is a Download link as a string.

Contact Details

If you require assistance please contact Trust.med at:

Email: support@trust.med
Phone: 855-630-0633

