EUROPEAN ANTI-FRAUD OFFICE

Notice: Upcoming Changes to the AFIS B2B API

Dear Technical Contact,

We are writing to inform you of the upcoming migration of our AFIS B2B applications to a modernised platform. This initiative is part of our ongoing efforts to enhance system reliability, security and long-term maintainability. The following document outlines the technical changes, their impact on your integration and the recommended migration timeline.

Background and Objectives

We are currently transitioning our AFIS B2B applications to a new architecture. This migration will consolidate our infrastructure under a unified, versioned API framework, standardise authentication mechanisms and enforce stricter compliance with published OpenAPI specifications. These improvements will provide greater stability, an improved developer experience and alignment with modern industry standards.

Key Changes

1. Unified API Endpoints

The AFIS B2B endpoints will be consolidated under a single, versioned API structure, available at:

- **Production Environment:** `api.olaf.europa.eu`
- **Testing Environment:** `api-qa02.olaf.europa.eu`

2. Simplified Endpoint Paths

To reduce complexity and improve consistency, endpoint paths will be streamlined:

- **Previous:** `/afis/application/api/resource`
- **New:** `/api/resource`

3. Standardised Authentication

Authentication will transition to the widely supported OAuth 2.0 Client Credential flow. This change simplifies integration across standard libraries and improves security.

- **New Production Authentication Host:** `identity.olaf.europa.eu/sso`
- **New Testing Authentication Host:** `identity-qa.olaf.europa.eu/sso`

4. Enhanced API Specification Enforcement

The new infrastructure enforces the published OpenAPI specifications strictly. While this ensures higher data quality and reliability, requests that previously succeeded due to lenient parsing may now be rejected if they deviate from the official specification.

Impact and Backward Compatibility

We are committed to minimising disruption during this transition. The following compatibility measures will be in place during the transition period (until 30 September 2027):

- **Credentials**: Existing B2B credentials and client certificates will remain valid for the production and testing environments.
- **Production Compatibility:** Current authentication methods, hostnames and API paths will continue to function in the production environment.
- **Testing Environment:** Current authentication methods and API paths remain supported. Please note that the testing host has been updated to `sta91-b2b.olaf.europa.eu`.
- **Technical Considerations:** As the B2B endpoints now run on updated infrastructure, minor behavioural differences may occur. We recommend thorough validation during the transition period.

Migration Timeline and Next Steps

Date	Milestone	Action Required
01 July 2026	New AFIS B2B endpoints available in **Testing**	You must validate the correct functioning of your existing B2B client against the testing environment. You can start adapting your B2B client to support the new authentication, hosts and paths.
01 October 2026	New AFIS B2B endpoints available in **Production**	Please ensure all request payloads comply with the updated OpenAPI specifications.
30 September 2027	End of backward compatibility window	We stop supporting the legacy authentication methods, hosts and paths. Please ensure you complete the migration to these new hostnames, paths and authentication methods by this time.

Please note that strict enforcement of the updated OpenAPI specifications will take effect on **01 July 2026 (Testing)** and **01 October 2026 (Production)**. This aligns with our backward compatibility commitment, providing time for validation and adjustment.

Support and Contact Information

Our integration support team is available to assist with testing, troubleshooting or migration guidance. Please contact us at:

- **Email:** OLAF-AFIS-IT-HELP-DESK@ec.europa.eu
- **Phone:** +32 2 296 27 27
- **AFIS-Mail**: EC-OLAF-IT
- **Documentation & Developer Resources:** https://api-qa02.olaf.europa.eu/docs
- **Support Hours:** Monday–Friday, 08:30–18:30 (Brussels Time)

Thank you for your understanding. We appreciate your cooperation as we implement these improvements to deliver a more robust and secure API experience.

Sincerely,

The Anti-Fraud Digital Information Solutions Sector

Technical Reference Summary

Aspect	Current Implementation	Target Implementation	Timeline
Hostnames	***Testing****: pil-b2b.olaf.europa.eu* ***Production****: afis-b2b.olaf.europa.eu*	***Testing****: api-qa02.olaf.europa.eu* ***Production****: api.olaf.europa.eu*	Transition period until 30 September 2027
Authentication	**Testing**: OAuth 2.0 with DPoP against pil-b2b.olaf.europa.eu/sso/o*auth2/pil*/access_token **Production**: OAuth 2.0 with DPoP against afis-b2b.olaf.europa.eu/sso/o*auth2/afis*/access_token	**Testing**: OAuth 2.0 against identity-qa.olaf.europa.eu/sso/oauth2/qa02/access_token **Production**: OAuth 2.0 against identity.olaf.europa.eu/sso/oauth2/a*fis*/access_token	Transition period until 30 September 2027
Paths	/afis/appname/api/resource	/api/resource	Transition period until 30 September 2027
OpenAPI Enforcement	Not enforced	Enforced	Test*ing* environment: 01 July 2026 Production environment: 01 October 2026

Additional Information on the AFIS unified API

Gaining Access and Authenticating

The unified AFIS B2B API allows access to all B2B endpoints through a single, common interface. As a client organisation you may onboard your B2B systems once and subsequently gain access to the B2B endpoints for which you have requested access and for which access has been granted. You are encouraged to create different B2B client accounts for different internal systems.

1. Request access to AFIS B2B by sending a request to the AFIS Service Desk specifying:
    a. The name of your organisation as registered in the AFIS User Registration Tool (URT)
    b. The business contact for your B2B client system (e.g. business owner)
    c. The technical contact for your B2B client system (e.g. development team lead)
    d. The security contact for your B2B client system (e.g. security operations centre)
    e. Your reference of the B2B client system (e.g. org_sys_1)
    f. The public keys corresponding to the key pair generated for your B2B client system (one for testing and one for production)[1]
    g. The B2B endpoints or logical group for which you would like to receive access (e.g. IMS B2B endpoints)
    h. If available: the IP ranges from which B2B requests will originate to facilitate troubleshooting
2. Upon review and approval, the AFIS Service Desk will return you with the following:
    a. Two B2B client identifiers:
        i. B2B client for the testing environment (e.g. org_sys_1_api-qa02)
        ii. B2B client for the production environment (e.g. org_sys_1_api)
    b. One interactive account for verification:
        i. Interactive account to access the testing environment to browse the contents of the application allowing you to verify the functioning of your B2B tests (e.g. org_sys_1_qa02)
3. You should now we able to obtain an access token at the following endpoints:
    a. For the testing environment: https://identity-qa.olaf.europa.eu/sso
    b. For the production environment: https://identity.olaf.europa.eu/sso
4. You should now be able to login to the AFIS testing environment using the provided credentials to verify the correct functioning of your B2B client by connecting to https://api-qa02.olaf.europa.eu.
5. You are requested to test your implementation in the testing environment before trying to interact with the production environment. You may request assistance and verification by the AFIS Service Desk if required

[1] A RSA public/private key pair with 2048-bit modulus must be generated to gain access to the AFIS B2B. Please do not mix testing and production keys for security reasons.

Available Endpoints

An overview of the available endpoints and pointers to additional guidance is provided below. The API specification for these endpoints can be consulted on the documentation website located at https://api-qa02.olaf.europa.eu/docs.

Logical Grouping	Legacy Endpoint (afis-b2b.olaf.europa.eu)	Unified Endpoint (api.olaf.europa.eu)	Additional documentation
Authentication	/sso/	/sso/	Please see section "Gaining Access and Authenticating".
IMS	/api/irregularity-cases/beneficiaries/search /api/irregularity-cases/search /api/irregularity-cases/{id} /api/irregularity-requests /api/irregularity-requests/attachments /afis/b2b/ims/api/v2/beneficiaries/search /afis/b2b/ims/api/v2/cases/search /afis/b2b/ims/api/v2/case	/api/irregularity-cases/beneficiaries/search /api/irregularity-cases/search /api/irregularity-cases/{id} /api/irregularity-requests /api/irregularity-requests/attachments	
CISCash	/afis/api/v1/cashdeclaration /api/cashdeclarations /api/cashdeclarations/{id} /api/cashdeclarations/search /api/cashdeclarations/count	/api/cashdeclarations /api/cashdeclarations/{id} /api/cashdeclarations/search /api/cashdeclarations/count	Please note that systems using the deprecated afis/api/v1/cashdeclaration endpoint must adapt their request payloads to align with the updated OpenAPI specifications.
CIS		/api/fraudcases /api/fraudcases/{id} /api/fraudcases/{id}/attachments /api/fraudcases/{id}/publish /api/fraudcases/search	
COPIS	/afis/b2b/copis/api/v1/infringement /afis/b2b/copis/api/v1/upload	/api/infringements /api/infringements/upload	

Troubleshooting

Our system performs input validation and the OpenAPI specification is enforced at several layers in our environment. Depending on the type of issue detected different return codes and formats are used:

Error Type	Status Code	Format	Next steps
Syntactic OpenAPI Specification Validation Error detected by the API gateway	400	HTTP/1.1 400 Bad Request X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Access-Control-Allow-Headers: authorization,content-type Access-Control-Allow-Methods: PUT,DELETE,GET,POST,OPTIONS Access-Control-Allow-Origin: * Access-Control-Expose-Headers: * Access-Control-Max-Age: 600 Cache-Control: no-cache Connection: close Content-Type: application/json; charset=utf-8 Pragma: no-cache Source: BigIP Content-Length: 37 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-afis-req-uid: AES 128 [UID] {"supportID": "[SUPPORTID]"}	Contact AFIS Service Desk with Support ID for more information.
Semantic OpenAPI Specification Validation Error detected by the application	422	HTTP/1.1 422 Unprocessable Entity x-content-type-options: nosniff x-xss-protection: 0 cache-control: no-cache, no-store, max-age=0, must-revalidate pragma: no-cache expires: 0 x-frame-options: SAMEORIGIN content-type: application/json date: Mon, 13 Jul 2026 10:31:04 GMT x-envoy-upstream-service-time: 15 Transfer-Encoding: chunked Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-afis-req-uid: AES 128 [UID]	Check your request against the OpenAPI specifications and provided documentation. Contact AFIS Service Desk for assistance if required.

		{"validationErrors":[{"reason":"Not a valid number","field":"id"}],"detail":"Validation failed","instance":"Irregularity API","status":422,"title":"Validation failed","type":"https://api-errors.afis.europa.eu/IrregularityCases/invalid-request"}	
Authentication Error: non-existent user	400	HTTP/1.1 400 Bad Request Cache-Control: no-store Date: Mon, 13 Jul 2026 08:50:26 GMT Pragma: no-cache Accept-Ranges: bytes Server: Restlet-Framework/2.1.7 Content-Type: application/json; charset=UTF-8 Vary: Accept-Charset, Accept-Encoding, Accept-Language, Accept Strict-Transport-Security: Max-age=31536000; preload X-Frame-Options: SAMEORIGIN X-afis-req_uid: [UID] Transfer-Encoding: chunked Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-afis-req-uid: AES 128 [UID] {"error_description":"Client authentication failed","error":"invalid_client"}	
Authentication failed: expired or not a correct token	403	HTTP/1.0 403 Forbidden Content-Type: application/json Server: BigIP Connection: Keep-Alive Content-Length: 55 {"error":"Forbidden","message":"Authentication failed"}	
Authorization Error	403	HTTP/1.1 403 Forbidden x-content-type-options: nosniff x-xss-protection: 0 cache-control: no-cache, no-store, max-age=0, must-revalidate pragma: no-cache expires: 0 x-frame-options: SAMEORIGIN content-type: application/problem+json content-length: 149 date: Mon, 13 Jul 2026 09:21:33 GMT	Check validity of your credentials and providing the required authentication headers.

x-envoy-upstream-service-time: 38
Set-Cookie: TS01116269=[VALUE]; Path=/
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-afis-req-uid: AES 128 [UID]
{"detail":null,"instance":null,"properties":null,"status":403,"title":"Authorization failed","type":"https://api.afis.europa.eu/errors/unauthorized"}