VeriDas

/Phygital

/Integration watchlists API

/Scope

The scope of this document is to provide a guide to integrate upload of watchlist files to veridas phygital access control system. This system consists of a Credential Service Provider (CSP) from now on referred to as **Welcome API** and biometric terminals used for user authentication and access control in physical locations.

Welcome API deals with watchlist upload, management and distribution across biometric terminals. In this document we will present how to integrate watchlist upload.

/1. API Authentication

Authentication within the **Welcome API** is based on **OpenID Connect (OIDC)**, which is an authentication protocol implemented on top of the OAuth 2.0 authorization framework.

In the following sections, the authentication process for API calls is specified in more detail with examples and the available resources are also described in a detailed way.

1.1 Token generation

Veridas will provide the client with two pieces of information that identify the client and are necessary to obtain the access token: *client_id* and *client_secret*. With these two pieces of information an access token must be obtained by calling the API endpoint /token as follows:

```
POST /auth/realms/{TENANT_ID}/protocol/openid-connect/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: */*
Host: iam.work-srv.das-gate.com
content-length: XX

grant_type=client_credentials&scope=roles&client_id=CLIENT_ID&client_secret=CLIENT_SECRET
```

Veridas will provide for each customer with: ***CLIENT_ID, TENANT_ID*** *and* ***CLIENT_SECRET***, so the integration solution will allow us to configure these parameters for every client.

The obtained response is a json with the following format:

```
{'access_token': 'eyJhbGc....',
 'expires_in': 300,
 'token_type': 'bearer',
 'not-before-policy': 0,
 'session_state': '3f9a7a76-cd4a-4082-b3e0-95686bac24ee',
 'scope': 'email profile roles'
}
```

From this response the *access_token* shall be extracted for use in API requests as follows. The *expires_in* field indicates the validity period of the token in seconds.

1.2 Refreshment of tokens

When the token expires, it is necessary to generate a new one. To do so, it is necessary to carry out the operation indicated in point 1.1 again.

It is also possible to use the **Refresh Token grant**, although it involves sending practically the same as in previous section *"Token generation"*:

```
POST /auth/realms/{TENANT_ID}/protocol/openid-connect/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: */*
Host: iam.work-srv.das-gate.com
content-length: XX

grant_type=refresh_token&refresh_token=REFRESH_TOKEN&client_id=CLIENT_ID&client_secret=CLIEN
T_SECRET
```

/2. POST /watchlists

Once you have got the access token, **ACCESS_TOKEN** from the previous step, this token needs to be included in the request headers as a bearer token.

- **Headers**:
  - **Authorization**: "Bearer **ACCESS_TOKEN"**, being **ACCESS_TOKEN** the token obtained from the authentication step.
  - **Content-type**: multipart/form-data
  - **x-api-key** (*string*): Welcome API key. The **API key** will be provided by Veridas for **each customer**, so the solution will be prepared to have this field customizable for each integration.
  - **x-dasgate-tenant-id** (*string*): Veridas tenant id. We will provide the tenant to you for each customer.

- **Request Body:**
  - **file**: This field corresponds to the watchlist file to be uploaded. It must be a csv file.
    - Value type: csv file
  - **domain**: This field corresponds to the legal/geographical scope.
    - Value type: string
    - Possible values: See Annex.
  - **watch_type**: This field indicates the type of registration.
    - Value type: string
    - Possible values: interdicted

```
POST /public/watchlists HTTP/1.1
Content-Type: multipart/form-data
Accept: */*
Host: api.work.das-gate.com
Authorization: Bearer ACCESS_TOKEN
x-api-key: APIKEY
x-dasgate-tenant-id: TENANT

{
    "file": "watchlist_file.csv",
    "domain": "es-ri",
    "watch_type": "interdicted"
}
```

/Annex Available domains

Veridas integrates watchlists files from most of those spanish regions that operate based on this system in gambling prevention for interdicted users. We have adopted the iso code 3166:ES for labeling the domain field within the request.

The following table shows the domain field that Welcome API will understand along with some requirements of the csv file v

Domain	Region	File characteristics	
		has header	Delimiter
es-an, es-al, es-ca, es-co, es-gr, es-h, es-j, es-ma, es-se	Andalucía, Almería, Cádiz, Córdoba, Granada, Huelva, Jaén,	False	,

	Málaga, Sevilla		
es-as	Asturias	True	;
es-cn	Canarias	True	;
es-ct	Cataluña	False	;
es-mc	Murcia	False	;
es-nc	Navarra	True	,
es-ri	La Rioja	True	;