

API Authentication Guide for Paramount Faspex Platform

Overview

This document provides step-by-step guidance on how to:

1. Generate a JWT token to authenticate with the Paramount Faspex system using provided API credentials.
2. Generate and send your SSH public key so we can associate it with your API account on our Faspex platform.

Requirements

Before you begin, ensure you have the following:

- Client ID (provided by Paramount)
- Registered Email Address (used with Faspex)
- Private Key file in PEM format (private_key.pem)
- Python 3.x with the following libraries:
 - requests
 - PyJWT (jwt)
 - urllib3

Step 1: Generate SSH Key Pair

We require your public SSH key to associate with your API identity. Follow these steps:

For Linux / macOS / Git Bash on Windows:

```
ssh-keygen -t rsa -b 2048 -f partner_api_key
```

You will get:

- partner_api_key (private key)
- partner_api_key.pub (public key)

For Windows with PuTTY:

Use PuTTYgen to generate RSA key pair and export the public key.

Important Notes:

- Never share your private key (partner_api_key).
- Email your public key file (partner_api_key.pub) to: contentdelivery@paramount.com

Step 2: JWT Token Generation with Sample Code

The following Python script demonstrates how to generate a JWT token and request an access token from the Faspex API.

Sample Script (get_faspex_token.py):

```
import requests
import jwt
import time
import uuid
import json
import urllib3

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

EMAIL = "your_email@example.com"
PRIVATE_KEY_PATH = "private_key.pem"
JWT_EXPIRY_SEC = 103600

FASPEX_HOST = "mach.paramountmsc.com"
CLIENT_ID = "your-client-id-guid"

def generate_jwt(client_id, email):
    now = int(time.time())
    payload = {
        'iss': client_id,
        'aud': client_id,
        'sub': f'user:{email}',
        'exp': now + JWT_EXPIRY_SEC,
        'iat': now,
        'jti': str(uuid.uuid4())
    }
    with open(PRIVATE_KEY_PATH, "rb") as key_file:
        private_key = key_file.read()
    return jwt.encode(payload, private_key, algorithm="RS256", headers={"typ": "JWT"})

def get_token(host, client_id, jwt_token):
    auth_data = {
        "client_id": client_id,
        "grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
        "assertion": jwt_token,
        "redirect_uri": "/",
        "state": str(uuid.uuid4())
    }
    response = requests.post(
        f"https://{host}/aspera/faspex/auth/token",
        json=auth_data,
        headers={"Accept": "application/json", "Content-Type": "application/json"},
        verify=False
    )
    response.raise_for_status()
    return response.json().get("access_token")
```

```
# --- Run example ---  
jwt_token = generate_jwt(CLIENT_ID, EMAIL)  
access_token = get_token(FASPEX_HOST, CLIENT_ID, jwt_token)  
print("Access Token:", access_token)
```

Setup Instructions

1. Install dependencies:

```
pip install requests PyJWT
```

2. Save your private key as private_key.pem.
3. Replace placeholders in the script with values provided by Paramount.
4. Run the script:

```
python get_faspex_token.py
```

Security Notes

- Your access token is valid for 24 hours by default.
- Always store your private key securely and never share it.
- If your key is compromised, notify Paramount immediately so we can revoke access.

Need Help?

If you encounter any issues or have questions, contact us at:

contentdelivery@paramount.com