

IMD API Portal

User Guide: Generate API Keys & Test APIs Online

Step-by-step guide for registered API users

Purpose: This guide explains how to use the IMD API Management Platform to generate a Development or Production API key, understand the server/IP binding requirements, obtain a JWT bearer token, and test an API directly from the online API Test Console.

Official portal: <https://api.imd.gov.in/public/index.php>

Official API reference: [IMD API Reference](#)

Contents

- 1. Before you start
- 2. Log in to the IMD API Portal
- 3. Understand the API Usage Summary
- 4. Generate an API Key
- 5. Understand the API Key fields and limits
- 6. Test an API using the online API Test Console
- 7. Authentication: API Key + JWT Bearer Token
- 8. Generate a JWT token
- 9. Complete online API test workflow
- 10. Common issues and checks
- 11. Security recommendations

1. Before you start

- You should have an active account on the IMD API Management Platform.
- For government-organization registration, use the official organization email address accepted by the portal.
- Decide whether the key is for DEV (Development) or PROD (Production).
- The server that will call the API must have a static public IP address.
- Keep your registered email/password available because the JWT token is generated using the same user account.
- Have the API endpoint and any required query parameters ready before using the Test Console.

Important: Do not publish API keys, passwords, or JWT tokens in screenshots, source code repositories, public documents, or support tickets.

2. Log in to the IMD API Portal

Open the official IMD API Management Platform: <https://api.imd.gov.in/public/index.php>

1. Select Login and sign in with your registered account.
2. After successful login, open API Keys from the left navigation menu.
3. The dashboard displays your API usage and key-related information.

3. Understand the API Usage Summary

The dashboard provides a quick view of API activity and the validity of your API access.



Figure 1. API Usage Summary dashboard

- Validity Expiry shows the date until which the current validity is active.
- The portal indicates when a validity-extension request becomes available.
- Total shows the overall API usage count displayed by the portal.
- Today shows API usage for the current day.
- This Month and This Year show the corresponding usage totals.

Portal requirement: The dashboard states that API usage statistics must be shared with IMD upon request.

4. Generate an API Key

From the left-side navigation, select API Keys. The Generate API Key section is used to create a key for the selected environment.

Generate API Key

Maximum 2 Dev + 2 Prod keys allowed

Environment

Select

Server Name

Server OS (Linux, Windows)

Server Public IP Address

Generate API Key

Note: The IP address must be a static public IP. To find your public IP address assigned by your ISP, copy and open the following URL directly from the server where API access is required:

<https://api.imd.gov.in/public/ip.php>

Your API Keys

Environment	Server	IP	API Key	Status	Action
DEV	localhost	127.0.0.1	07551408fe61	Active	Delete
PROD	apiserver	203.0.113.10	3ad3fb4f	Active	Delete

Figure 2. Generate API Key page

Step-by-step

- Open API Keys from the portal navigation.
- In Environment, select DEV or PROD.
- Enter the Server Name. Use a meaningful name that identifies the machine/application using the API.
- Enter Server OS, for example Linux or Windows.
- Enter the Server Public IP Address. This should be the static public IP from which the API requests will originate.
- Click Generate API Key.
- After successful creation, the new key appears under Your API Keys.

Public IP check: The portal instructs users to find the public IP from the server where API access is required. Use the portal's displayed IP-check URL or another trusted method from that server.

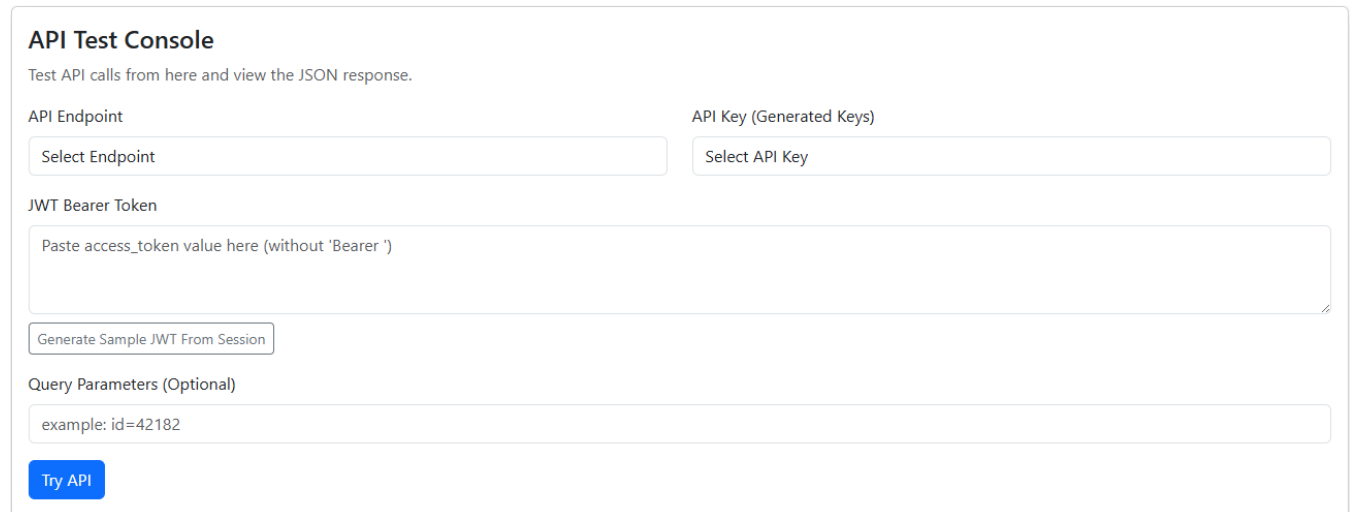
5. Understand the API Key fields and limits

Field	What to enter	Example
Environment	DEV or PROD	DEV
Server Name	Name/identifier of the server or application	api-server-01
Server OS	Operating system of the server	Linux
Server Public IP Address	Static public IP used to access IMD APIs	203.0.113.10

- The portal indicates a maximum of 2 Development keys + 2 Production keys.
- The API key is associated with the server public IP entered while generating the key.
- If your server's public IP changes, API access may fail because the key is tied to the registered server/IP.
- The key list displays Environment, Server, IP, API Key, Status, and Action.
- Use Delete only when you are sure a key is no longer required.

6. Test an API using the online API Test Console

The API Test Console lets you make a request from the portal and view the JSON response without first writing application code.



The screenshot shows the 'API Test Console' interface. At the top, it says 'Test API calls from here and view the JSON response.' Below this, there are two main sections: 'API Endpoint' and 'API Key (Generated Keys)'. The 'API Endpoint' section has a dropdown menu labeled 'Select Endpoint'. The 'API Key (Generated Keys)' section has a dropdown menu labeled 'Select API Key'. Below these, there is a 'JWT Bearer Token' section with a text input field labeled 'Paste access_token value here (without 'Bearer ')' and a button labeled 'Generate Sample JWT From Session'. At the bottom, there is a 'Query Parameters (Optional)' section with a text input field containing the example 'id=42182' and a blue button labeled 'Try API'.

Figure 3. API Test Console

Fields in the Test Console

Field	Purpose	What to do
API Endpoint	Select the API you want to call.	Choose an endpoint from the dropdown.
API Key (Generated Keys)	Select the API key to use.	Choose the key matching the server/environment.
JWT Bearer Token	Provides authenticated user identity.	Paste only the access_token value; do not add the word Bearer if the field says not to.
Query Parameters (Optional)	Adds URL parameters required by the selected API.	Enter parameters in the requested format, e.g. id=42182.

11. Select the required API Endpoint.
12. Select the matching generated API key.
13. Paste a valid JWT access_token into the JWT Bearer Token field.
14. Enter query parameters if the endpoint requires them.
15. Click Try API.
16. Review the JSON response returned by the API.

7. Authentication: API Key + JWT Bearer Token

Authentication

All IMD APIs are protected and require authentication.

Required Headers

X-API-KEY: YOUR_API_KEY

Authorization: Bearer YOUR_JWT_TOKEN

- **X-API-KEY** is mandatory and is bound to your server IP.
- **JWT Bearer Token** is mandatory, represents user identity, and expires automatically.
- The JWT must belong to the same user as the API key.

JWT Token Generation

Use the following endpoint to generate a JWT token:

POST <https://api.imd.gov.in/api/oauth/token.php>
Content-Type: application/json

```
{
  "email": "your_registered_email",
  "password": "your_password"
}
```

Response:

```
{
  "access_token": "eyJhbGciOi...",
  "token_type": "Bearer",
  "expires_in": 3600
}
```

Figure 4. Authentication and JWT token instructions

According to the portal's Authentication section, IMD APIs require two authentication headers:

X-API-KEY: YOUR_API_KEY

Authorization: Bearer YOUR_JWT_TOKEN

Authentication rules

- X-API-KEY is mandatory and is bound to your server IP.
- JWT Bearer Token is mandatory and represents the authenticated user identity.
- The JWT expires automatically.
- The JWT must belong to the same user/account as the API key.

Think of it this way: The API key identifies the authorized server/application, while the JWT authenticates the user making the request.

8. Generate a JWT token

The portal provides the following endpoint for JWT token generation:

POST <https://api.imd.gov.in/api/oauth/token.php>

Content-Type: application/json

Request body:

```
{
  "email": "your_registered_email",
  "password": "your_password"
}
```

A successful response contains an access_token, token_type, and expiry information. The portal shows a response structure similar to:

```
{
  "access_token": "eyJhbGciOi...",
  "token_type": "Bearer",
  "expires_in": 3600
}
```

For the Test Console: Copy the value of access_token only into the JWT Bearer Token field. Follow the field instruction and do not manually prepend 'Bearer ' when the console asks for the token value without it.

Example cURL for JWT generation

```
curl -X POST "https://api.imd.gov.in/api/oauth/token.php" ^
-H "Content-Type: application/json" ^
-d "{\"email\":\"your_registered_email\",\"password\":\"your_password\"}"
```

For Linux/macOS, replace the Windows line-continuation character ^ with \ and use normal shell quoting as appropriate.

9. Complete online API test workflow

Use the following sequence whenever you want to test an authenticated IMD API from the portal:

17. Log in to the IMD API Management Platform.
18. Confirm that the required API key is Active under API Keys.
19. Confirm that the server public IP registered with the key is the IP from which the request is expected to originate.
20. Generate a JWT token using your registered email and password.
21. Copy the access_token from the JWT response.
22. Open the API Test Console.
23. Select the required API endpoint.
24. Select the matching generated API key.
25. Paste the access_token into JWT Bearer Token.
26. Enter query parameters, if required by the endpoint.
27. Click Try API.
28. Check the JSON response. If successful, use the same authentication pattern in your application.

Example: API with a query parameter

For an endpoint documented as:

```
https://api.imd.gov.in/api/v1/cityforecast?id=42182
```

enter the query parameter in the console as:

```
id=42182
```

The official IMD API reference lists the City Weather Forecast API and this parameterized URL format. [View official API reference](#)

10. Common issues and checks

Problem	Likely cause	Check
API key rejected	IP mismatch or inactive/deleted key	Check the key status and confirm the server's current public IP.
JWT rejected	Expired token or wrong user	Generate a fresh token and ensure it belongs to the same account as the API key.
401/Authentication error	Missing API key or Authorization token	Confirm both required headers/console fields are populated.
Wrong API response/error	Incorrect endpoint or parameters	Check the official API reference for the endpoint and parameter names.
API works from one server but not another	API key is bound to a different public IP	Use the key from the registered server/IP or create an appropriate key.
Cannot create another key	Key limit reached	The portal allows up to 2 DEV + 2 PROD keys.

Support: For API access/portal support, use the official IMD contact/support information available from the portal. When reporting a technical issue, include the API endpoint and relevant station ID where applicable.

11. Security recommendations

- Never share your API key publicly.
- Never share your IMD portal password or JWT access_token.
- Store API keys and passwords in environment variables or a secure secret manager in production applications.
- Do not hard-code credentials into publicly accessible source code.
- Use a separate DEV key for development/testing and a PROD key for production where appropriate.
- Delete unused keys to reduce the number of active credentials.
- If a credential is accidentally exposed, treat it as compromised and take the appropriate revocation/replacement action.

Quick Reference

Item	Value / Action
Portal	https://api.imd.gov.in/public/index.php
API Reference	https://api.imd.gov.in/public/api_reference.html
JWT Endpoint	POST https://api.imd.gov.in/api/oauth/token.php
Required API authentication	X-API-KEY + Authorization: Bearer <JWT>
API key environments	DEV / PROD
Key limit shown by portal	Maximum 2 DEV + 2 PROD keys
Key binding	Server public IP
JWT	Must belong to the same user as the API key and expires automatically
Online testing	API Test Console → Endpoint → API Key → JWT → Parameters → Try API

End of Guide