document 1.0

This is the document of the ERP API version 1.0.

# Login API Endpoint

# Login API Endpoint

This endpoint is used to authenticate a user by logging them into the system. It accepts a username and password, and upon successful authentication, returns a token that can be used for subsequent requests.

## Request

- **Method**: POST
- **URL**: `http://avantemedicals.com/API/api.php?action=login`
- **Content-Type**: application/json

### Request Body Parameters

The request body should be a JSON object containing the following parameters:

- `username` (string): The username of the user attempting to log in.
- `password` (string): The password associated with the provided username.

**Example Request Body:**

JSON

{

"username": "exampleUser",

"password": "examplePassword"

}

## Response

Upon making a successful request, the server will respond with a JSON object containing the authentication status and tokens.

### Successful Response Structure

- **Status Code**: 200
- **Content-Type**: application/json

The response will include the following fields:

- `status` (string): Indicates the success or failure of the login attempt.

- `token` (string): A JWT token that can be used for authenticated requests.
- `refresh_token` (string): A token used to obtain a new access token when the current one expires.

**Example Successful Response:**

JSON

```
{
 "status": "success",
 "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...",
 "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9..."
}
```

**Error Response Structure**

In case of an unsuccessful login attempt, the response will still return a 200 status code but with an empty status and message fields.

**Example Error Response:**

JSON

```
{
 "status": "",
 "message": ""
}
```

## Additional Notes

- Ensure that the username and password are correctly provided in the request body.
- The server may return warnings related to PHP configurations, but these do not affect the functionality of the API.
- The tokens returned should be stored securely and used in subsequent requests that require authentication.

This API endpoint is essential for user authentication and should be used to obtain access tokens for secured API operations.

protected

## Protected – Auth-Only Operation

This request invokes a **protected** operation in the Avante ERP API. It is intended to be called only by authenticated clients and is identified by the `action=protected` query parameter.

---

## HTTP Request

Plain Text
POST https://avantemedicals.com/API/api.php?action=protected

- `localhost`
  - Base host for the ERP API (for example, `localhost:8000`, a dev/stage domain, or a production host).
  - Provided as a variable so that the same request can be reused across environments.
- `avante-medicals-erp/API`
  - Path segment for the ERP application folder (for example, `avante-erp`).
  - Also defined as a variable to keep the request reusable when the application is deployed in different directories.
- `api.php`
  - The main entry point script for the ERP API.
- `action=protected` (query parameter)
  - Identifies this call as a **protected/auth-only** operation.
  - The server is expected to treat this as an endpoint that requires a valid authenticated context (for example, a verified session or token) before returning the protected content.

---

## Method and Headers

- **Method:** `POST`
- **Headers:**
  Plain Text
  Content-Type: application/json
  - Declares that the request body is JSON.

---

## Request Body

Body type: **raw JSON**

Current configured body:

```
JSON
{
 "action": "protected"
}
```

Body fields:

- `action` (string, required in this request configuration)
  - Set explicitly to `"protected"`.
  - Used by the backend to route the request to the logic that handles protected operations.

Note: This description is intentionally limited to the fields currently present in the body (`action` only) and does not assume any additional payload fields.

---

## Authentication and Protection Semantics

This operation is **protected**:

- The `action=protected` query parameter and `"action": "protected"` body value both indicate that the server should handle this as an authenticated/protected call.
- In many implementations, such endpoints will require a valid authentication context (for example, a bearer token or session), often provided via an `Authorization` header.
- The exact authentication mechanism depends on your server configuration; enable and configure headers (such as `Authorization: Bearer` ) as required by your deployment.

No additional authentication parameters (such as refresh tokens or credentials) are present in the current request body.

---

## Sample Successful Response (200)

A known successful response for this request shape is:

```
JSON
{
 "status": "success",
 "message": "Welcome u2vp8kb, You are protected."
```

}

Interpretation:

- `status: "success"`
  - Indicates that the protected operation completed successfully and that the caller satisfied the protection/authentication requirements enforced by the server.
- `message: "Welcome u2vp8kb, You are protected."`
  - Confirms that the user or client (example identifier `u2vp8kb`) has accessed the protected resource or action.
  - The exact identifier value is implementation-specific and serves here as an example of a user- or session-related message.

Clients can use this response to verify that:

1. The request structure (URL, headers, and body) is correct.
2. The authentication context for protected operations is correctly established on the server side.

# Refresh Token API

# Refresh Token API

This endpoint is used to refresh an authentication token for a user session. It allows clients to obtain a new access token using a valid refresh token, thereby extending the user's session without requiring them to log in again.

## Request

- **Method**: POST
- **URL**: `http://avantemedicals.com/API/api.php?action=refresh_token`

### Request Body

The request body must be in JSON format and should contain the following parameter:

- **refresh_token** (string): The refresh token issued during the initial authentication process. This token is used to generate a new access token.

**Example Request Body**:

JSON

```
{
 "refresh_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6Ik ..."
}
```

## Response

Upon successful execution, the API will return a response with a status code of 200. The response body will be in JSON format and may include the following fields:

- **status** (string): Indicates the status of the request.
- **token** (string): The newly generated access token.
- **refresh_token** (string): The refresh token that can be used for future requests.

**Example Response Body:**

JSON

```
{
 "status": "",
```

"token": "",

"refresh_token": ""

}

## Related Responses

In addition to the primary response, the API may return related responses for other methods called at the same URL, which typically include:

- **success** (boolean): Indicates whether the request was successful.
- **message** (string): A message providing additional information about the request.
- **data** (object): Contains user-specific information such as:
    - **api_user_id** (string): The unique identifier for the user.
    - **name** (string): The name of the user.
    - **username** (string): The username of the user.
    - **token** (string): The access token.

**Example Related Response**:

JSON

{

"success": true,

"message": "",

"data": {

"api_user_id": "",

"name": "",

"username": "",

"token": ""

}

}

## Notes

- Ensure that the refresh token provided is valid; otherwise, the request may fail, and an appropriate error message will be returned.

- The structure of the response may vary slightly based on the outcome of the request, but the fields mentioned above are commonly included.

# Logout API

# Logout API

This endpoint is used to log out a user from the application. It effectively terminates the user's session and ensures that any subsequent requests require re-authentication.

## Request

- **Method**: POST
- **URL**: `http://avantemedicals.com/API/api.php?action=logout`
- **Request Body**: The request does not require any parameters in the body. It uses the `x-www-form-urlencoded` format but does not include any specific key-value pairs.

## Response

Upon a successful logout, the API will return a JSON response with the following structure:

JSON

{

"status": "",

"message": ""

}

- **status**: A string indicating the status of the logout operation. It may be empty or contain a relevant message.
- **message**: A string providing additional information about the logout operation. It may also be empty.

## Status Codes

- **200 OK**: Indicates that the logout was successful.

## Related Responses

Other methods called to this API endpoint may return similar structures, such as:

JSON

{

"success": true,

```
 "message": "",
 "data": {
   "api_user_id": "",
   "name": "",
   "username": "",
   "token": ""
 }
}
```


This indicates that the API is designed to handle various authentication-related operations, providing consistent response formats across different actions.

## Summary

This logout API is essential for maintaining user session integrity and ensuring that users can securely end their sessions.

# Get Sales Report

## Protected – Auth-Only Operation

This request invokes a **protected** operation in the Avante ERP API. It is intended to be called only by authenticated clients and is identified by the `action=protected` query parameter.

---

## HTTP Request

Plain Text

POST https://{{localhost}}/{{erp_api_folder}}/api.php?action=protected

- `{{localhost}}`
  - Base host for the ERP API (for example, `localhost:8000`, a dev/stage domain, or a production host).
  - Provided as a variable so that the same request can be reused across environments.
- `{{erp_api_folder}}`
  - Path segment for the ERP application folder (for example, `avante-erp`).
  - Also defined as a variable to keep the request reusable when the application is deployed in different directories.
- `api.php`
  - The main entry point script for the ERP API.
- `action=protected` (query parameter)
  - Identifies this call as a **protected/auth-only** operation.
  - The server is expected to treat this as an endpoint that requires a valid authenticated context (for example, a verified session or token) before returning the protected content.

---

## Method and Headers

- **Method:** `POST`
- **Headers:**
  Plain Text
  Content-Type: application/json
  - Declares that the request body is JSON.

---

## Request Body

Body type: **raw JSON**

Current configured body:

JSON

```
{
 "action": "protected"
}
```

Body fields:

- `action` (string, required in this request configuration)
  - Set explicitly to `"protected"`.
  - Used by the backend to route the request to the logic that handles protected operations.

Note: This description is intentionally limited to the fields currently present in the body (`action` only) and does not assume any additional payload fields.

---

## Authentication and Protection Semantics

This operation is **protected**:

- The `action=protected` query parameter and `"action": "protected"` body value both indicate that the server should handle this as an authenticated/protected call.
- In many implementations, such endpoints will require a valid authentication context (for example, a bearer token or session), often provided via an `Authorization` header.
- The exact authentication mechanism depends on your server configuration; enable and configure headers (such as `Authorization: Bearer <token>`) as required by your deployment.

No additional authentication parameters (such as refresh tokens or credentials) are present in the current request body.

---

## Sample Successful Response (200)

A known successful response for this request shape is:

JSON

```
{
 "status": "success",
 "message": "Welcome u2vp8kb, You are protected."
}
```


Interpretation:

- `status: "success"`
  - Indicates that the protected operation completed successfully and that the caller satisfied the protection/authentication requirements enforced by the server.
- `message: "Welcome u2vp8kb, You are protected."`
  - Confirms that the user or client (example identifier `u2vp8kb`) has accessed the protected resource or action.
  - The exact identifier value is implementation-specific and serves here as an example of a user- or session-related message.

Clients can use this response to verify that:

1. The request structure (URL, headers, and body) is correct.
2. The authentication context for protected operations is correctly established on the server side.