

Authentication

29/09/2026 3:32 pm BST

[Relates to version](#)

Tags: 8.0

Eyelit MES offers integration with third-party applications through the use of a Public API. A series of endpoints are exposed and can be called by an external system (normally a middleware provider) to make changes directly within a given instance of the Eyelit software. The calls to these endpoints are done through the use of pre-formatted JSON packets and are authorised through OAuth 2.0.

The Eyelit MES-M Public API requires authentication to be accessed.

- The method used by Eyelit MES is OAuth 2.0 – *Password* and *Username*.
- A call to `[environment].mestec.net/Token` is needed to create the authentication token. This token has a lifespan of 12 hours.
- The username and password required are that of an Eyelit user account within the target environment.
- This user account must be appropriately licensed and have the correct roles to carry out any transactions attempted by the endpoints.
- Management of this user account is the customer's responsibility.

Request

MethodURL Structure

POST /Token

The following table lists all parameters and request body fields accepted by this endpoint.

Name	Location or Type	Required	Description
tenant	Query parameter	Yes	The unique identifier for the tenant environment against which authentication is performed. This value is supplied by Eyelit when your environment is provisioned.
grant_type	Form field (application/x-www-form-urlencoded)	Yes	The OAuth 2.0 grant type. Must be set to <code>password</code> for resource owner password credentials authentication.
username	Form field (application/x-www-form-urlencoded)	Yes	The username of the Eyelit MES account for which the token is being requested.
password	Form field (application/x-www-form-urlencoded)	Yes	The password associated with the specified username. Transmitted securely and never returned in any response.

Response

Status Code Description

200 OK	Authentication was successful. The response body contains the bearer access token, its type, and its expiry duration in seconds. Include the returned <code>access_token</code> value in the <code>Authorization: Bearer</code> header of all subsequent API calls.
400 Bad Request	The request was malformed. This typically occurs when a required form field is missing, the <code>grant_type</code> value is not <code>password</code> , or the request body is not encoded as <code>application/x-www-form-urlencoded</code> .
401 Unauthorized	The supplied username and password combination is invalid for the specified tenant, or the tenant identifier does not exist.
500 Internal Server Error	An unexpected error occurred on the server. If this error persists, contact Eyelit support with the request details and the time of the failure.

