Mikros by System Locker

Official documentation

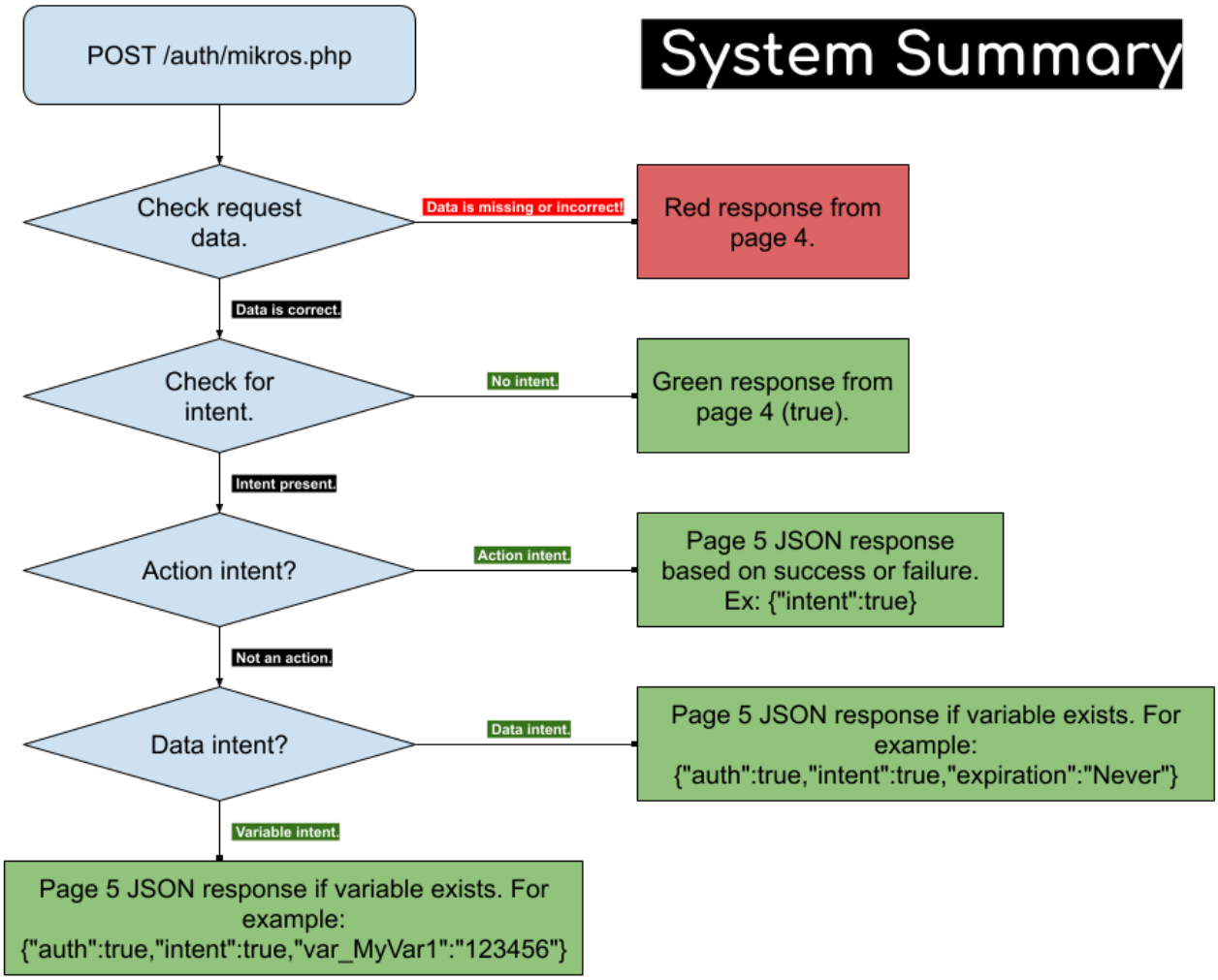
Last updated July 29th, 2026.
Revision 3

Mikros by System Locker A streamlined auth API

Basic System Locker authentication requires account registration and verification. For many devs, this is undesirable: the process isn't very fast and it lets users know what authentication system is being used.

With Mikros (Greek for "small") authentication, the username and password fields are exchanged for a license key. The user no longer has to redeem a key, since the key is redeemed and HWID locked on first usage. Users never have to visit systemlocker.net. HWID resets for Mikros keys are available if a user redeems the key on our website, or via the new Intent expansion, or if a system controller resets hwid manually.

Mikros is only available for paid users.



Documentation

The authentication request must be made to the Mikros endpoint found at https://systemlocker.net/auth/mikros.php. Only POST requests are permitted.

If you choose to send this request multiple times during the lifetime of your program, please do not send it more than once per minute.

The request should include the following information:

key*	The license key of the user to authenticate.
system*	The system ID (this is listed on the client page, it's a hexadecimal string such as `5c514eddcc4f019d5c19`).
hwid	A unique identifier of the machine. This can be a fixed value such as `1` if you do not need device locking. * Required for auth; data intents. Optional for action requests.
version	If you specify a version for the system, this must match. If the version is set, but you don't wish to check the version, the value must be `bypass`.
intent	Optional. Default is "auth", for which the server returns a response from the auth request table. Other values include: `hwidreset`, `expiration`, and `variable` (info on page 5). These values will change the server response to JSON.
variable	Optional. If specified, the intent must be `variable`. The response will include the value of the requested Server Side Variable in a JSON format.
clean	Optional. If specified, data or variable values will be the entire response (no JSON).

*required

The response for an auth request will be in the following format:

`var1`

var1	The status of the authentication request (possible values are listed on the next page).

Scroll to the next page for more information on the response. Then, go to page 5 to learn about intents and variables.

Server Responses - Auth

The responses for the **auth request** are as follows:

false	The request is missing required data. The system specified may not exist, or the request did not include a hwid or version.
no key	The license key could not be found in the database.
no sys	The system ID was not found in the request.
not mikros	The system is not enabled for Mikros authentication.
bad key	The user does not have access to this system.
frozen	The user's key has been frozen and cannot access this program.
expired key	The user's key has expired.
hwid	The user's hwid does not match.
hwid banned	The user's hwid is banned.
banned	The user has been banned.
outdated	The user is using an outdated version of the program **(only applies if the version is set for this system)** If you receive this response, all other checks are complete. You *could* allow a user to access your software with this response.
digest	The provided hash doesn't match the system's hash.
destitute	Your dev account's plan expired, and there were not enough tokens to renew it automatically.
dbe	The server cannot connect to the database.
true	The user has a valid key and should be authorized to access your program.

Server Responses - Intents and Server Side Variables

The server responds to a **request with intent** differently than an auth request. The flowchart on page 2 explains this visually.

1. If any of the security checks fail on your request with intent, one of the red responses from page 4 will be sent.
    - Otherwise, the response body will be formatted in JSON.
2. Action intents will be processed *before* HWID checks, and thus do not contain an auth response. Every other check must succeed to reach this point.
    - The response will take the form of `{"intent":true}`
3. Data intents are processed after *every* security check passes, including HWID.
    - The response will take the form of `{"auth":true,"intent":true,"expiration":"Never"}`
        - If `clean` is set to `1` or `true`, then the response will only contain the data if all checks pass.
    - If the data requested is a variable, the value of the variable will also be put inside the JSON
        - The value will live under the key `var_SSVNAME`. So, if the variable is `UPDATEURL`, then the JSON will look like this:

```
{"auth":true,"intent":true,"var_UPDATEURL":"https://systemlocker.net"}
```