



# Quicksilver by System Locker

Official documentation

Last updated July 29th, 2026.  
Revision 3

## Quicksilver by System Locker Next-gen auth

Original designs for System Locker authentication were based on the idea that authentication is a once-per-run event. While this isn't inherently insecure, it's far from perfect. A determined attacker only needs to fool the program once to gain unauthorized access.

Some clients have attempted to utilize our authentication endpoints more than once during their program's lifecycle. This is one way to improve security, however, the existing authentication endpoints are resource intensive and result in far too many database calls.

Quicksilver is the next iteration of our standard offerings, created to meet the growing security requirements of our clients while also optimizing the way authentication is handled. The first request to Quicksilver is handled in a similar manner to any other authentication request, however, the response also contains a token that is used for all subsequent "heartbeat" requests.

The heartbeat endpoint uses just two database requests to authenticate the client, and has strict timing requirements on how frequently heartbeat requests must be made. The default frequency is one "beat" every 30 seconds; this rate can optionally be adjusted to any number of seconds between 25 and 3600 (1 hour).

Each time a heartbeat request is made, a new heartbeat token is generated and the beat counter is incremented. This helps prevent session hijacking and increases security. Key expirations are also checked to prevent users from squatting on a valid session past a key's expiration.

Always use `POST` requests over HTTPS. `GET` is not supported.

The server response also contains the username and a hash, both of which your program should verify.

**Total Usage Time (TUT) tracking will be rolled out soon, allowing clients to track how long their program has been used between all users.**

## Documentation (Initial Request)

The first request must be made to the Quicksilver endpoint found at <https://systemlocker.net/quicksilver/init> for username and password authentication. For key-only Quicksilver, use [/quicksilver/init-mikros](#).

You do not need to send this request more than once during the lifetime of your program.

The request should include the following information:

|              |                                                                                                                                                                                                    |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| username* ** | The username of the user to authenticate.                                                                                                                                                          |
| password* ** | The password 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.                                                                                         |
| 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 <code>bypass</code> .                                  |
| beatrate     | The frequency at which your program will make heartbeat requests. If this is not set, the server will expect a beat every 30 seconds. This value is in seconds and must be in the range [25, 3600] |

\*Required    \*\*Send `key` instead of the `username` and `password` fields.

If successful, the response will be in the following format:

`var1|username|timestamp:hash`

|           |                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------|
| var1      | Either the reason for failure (list of reasons below) or the token for the heartbeat request                                                   |
| username  | The username of the matching account. Verify this against the original user input to prevent replay attacks)                                   |
| timestamp | The current Unix timestamp, divided by 29 and rounded down. Check to make sure this matches the same operation performed on the local machine. |
| hash      | A <code>sha1</code> hash of everything before the <code>:</code> (colon)                                                                       |

*Scroll to the next page for information on the heartbeat request*

# Documentation (Heartbeat Request)

The heartbeat request must be made to the Quicksilver endpoint found at <https://systemlocker.net/quicksilver/beat>

You must first send a request to the `init` endpoint and save the token.

The request should include the following information:

|                      |                                                                                                                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>token*</code>  | The heartbeat token. For the first heartbeat, you must use the token from the response to the initial request. For each subsequent heartbeat, you must use the updated token sent in the response to this request. |
| <code>system*</code> | The system ID (this is listed on the client page, it's a hexadecimal string such as <code>5c514edddcc4f019d5c19</code> ). It must match the system ID for which the token was originally created                   |

\*Required

If successful, response will be in the following format:

|                   |                                                                                                    |
|-------------------|----------------------------------------------------------------------------------------------------|
| <code>var1</code> | Either the reason for failure (list of reasons below) or the token for the next heartbeat request. |
|-------------------|----------------------------------------------------------------------------------------------------|

*A list of all possible responses can be found on the last page.*

# Server Responses

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

|                              |                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| false                        | A piece of data required to complete the request is missing. For example, the hwid field is missing or empty.                                                                                                                                                                                                                              |
| no u/p                       | The username or password could not be found in the request data.                                                                                                                                                                                                                                                                           |
| no sys                       | The system ID was not found in the request.                                                                                                                                                                                                                                                                                                |
| dbe                          | The server cannot connect to the database.                                                                                                                                                                                                                                                                                                 |
| not verified                 | The user's account does not have a verified email or discord account.                                                                                                                                                                                                                                                                      |
| bad u/p                      | The username and password do not match any existing accounts.                                                                                                                                                                                                                                                                              |
| bad keys                     | The user does not have access to this system.                                                                                                                                                                                                                                                                                              |
| frozen                       | The user's key has been frozen and cannot access this program.                                                                                                                                                                                                                                                                             |
| spoofsuspected               | The HWID of the user is fake and cannot be trusted.                                                                                                                                                                                                                                                                                        |
| expired key                  | The user's key is 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<br><b>If this response is received, a heartbeat token won't be provided. Any program utilizing Quicksilver should send "bypass" as the value for the version data to avoid this. If version checking is necessary, the best option is to also send a normal auth request as well.</b> |
| digest                       | The provided hash doesn't match the system's hash.                                                                                                                                                                                                                                                                                         |
| beat rate...                 | This indicates the specified beat rate (if provided) is too fast or too slow. You must fix this error.                                                                                                                                                                                                                                     |
| A string beginning with "TT" | This is your heartbeat token. The user has a valid account and key and should be authorized to access your program. Begin sending heartbeat requests with this token. <b>This is the only response indicating success.</b>                                                                                                                 |

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

|                               |                                                                                                                                                                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bad request                   | The heartbeat token or system could not be found in the request.                                                                                                                                                                              |
| bad session token             | The heartbeat token sent is invalid. It may be old, already used or entirely wrong.                                                                                                                                                           |
| stale token                   | The time since the last heartbeat request is too long.                                                                                                                                                                                        |
| terminated                    | The developer has terminated this session. <b>Replace "terminated " with "" to obtain the reason.</b> Example:<br>terminated We don't like you!                                                                                               |
| rate limit                    | The time since the last heartbeat request is too short. You cannot send requests this fast.                                                                                                                                                   |
| expired key                   | The user's key has expired.                                                                                                                                                                                                                   |
| A string beginning with "TTr" | This is your <b>new</b> heartbeat token. The token you sent is valid and the request was sent on time. Your next heartbeat request should include this new token instead of the old one. <b>This is the only response indicating success.</b> |