GARMIN INTERNATIONAL

Garmin Connect Developer Program Start Guide

Version 1.0.0

CONFIDENTIAL

Contents

1 Revision History

Version	Date	Revisions
1.0.0	12/01/2020	First release

2 Getting Started

2.1 Purpose of the Garmin Connect Developer programs

The Garmin Connect Developer Program is the mechanism by which Garmin users can share the data they generate on their activity trackers and fitness devices with non-Garmin corporate partners and downloading workout plans and courses to their devices from corporate partners.

Garmin Connect Developer Program is made up of 5 APIs:

- **Training API** (uploading workouts to Garmin Connect)
- **Courses API** (uploading courses to Garmin Connect)
- **Health API** (importing wellness data from Garmin Connect)
- **Activity API** (importing activities from Garmin Connect)
- **Women's Health API** (importing women's' health data)

Each API is fully described in corresponding specification documentation.

2.2 Consumer Key and Secret

To gain access to the APIs please create consumer key and secret. The consumer key is used to uniquely identify a partner and the consumer secret is used to validate that the requests received are from that partner and not a third-party that has gained unauthorized access to the consumer key.
The consumer key can be considered public information, but the consumer secret is private. For the security of users, the consumer secret should be secured and never sent over a network in plain text. It is not permitted to embed the consumer secret into consumer products like mobile apps.

Consumer key credentials are created using the Developer Portal and creating *Apps* (https://developerportal.garmin.com/user/me/apps?program=829). Each app represents a unique Consumer Key.

During key creation, you will also be able to select api's.

Your **first app** will generate an **evaluation-level consumer key that is rate-limited**. Once your integration has been verified for product, **subsequent apps will create consumer keys with production-level access**. Please see "Requesting a Production Key" below for more information.

Note:
Multiple consumer keys should be created to correspond to projects or implementations whose user base is logically separated. A common scenario is for one partner to manage user data from multiple other companies. A new key should be created and associated with each managed company so that Garmin users can make an informed decision to consent to sharing their data with just that company.

2.3 User Registration

Before a partner can access a user's data, the user must grant the partner access. Please refer to the detailed Garmin OAuth documentation at https://developerportal.garmin.com/developer-programs/content/829/programs-docs for details on acquiring, authorizing, and signing with a User Access Token (UAT) to access Garmin user data. The Developer Program web tools (see Web Tools below) also contain additional demonstrations of user authorization and request signing. **User ID must be used as a main user identifier.**

2.4 Setting up Consumer Key with API Tools

Several web-based tools are available to assist partners with integration in addition to the Endpoint Configuration tool. These tools are all available by logging in to https://apis.garmin.com/tools/login using the consumer key and secret applicable to the program they want to configure.

2.4.1 API Configuration

You will be able to edit API selection for your consumer key if necessary for the evaluation level apps. If changes needed in the production, please reach out to connect-support@developer.garmin.com

2.4.2 Endpoint configuration

By default, any API has 2 endpoints available
-deregistration (through this endpoint we notify partners if the user disconnected from partners' app)
-user permission (through this endpoint we notify if the user removed permission to share data)
Other endpoints are available based on API selection

2.4.3 User Authorization

This tool describes and performs the entire 3-legged OAuth process. It can be used to manually generate a User Access Token and authorize it for the currently used consumer key prior to any partner OAuth infrastructure being written. **User ID must be used as a main user identifier.**

2.4.4 Request Signing

This tool describes and demonstrates how to perform OAuth 1.0a request signing. The use of a third-party library is recommended, however manual signing can be useful for initial integration and debugging purposes. See the OAuth Specification document for more information on OAuth 1.0a request signing.

2.5 Requesting a Production Key

The **first consumer key** generated through the Developer portal **is an evaluation key**. This key is rate-limited and should only be used for **testing, evaluation, and development**. To obtain a production-level key please email first to connect-support@developer.garmin.com providing your evaluation key and list of API pillars that are being used.

For individual API requirements, please refer to corresponding specification document.

2.6 Endpoint Configuration

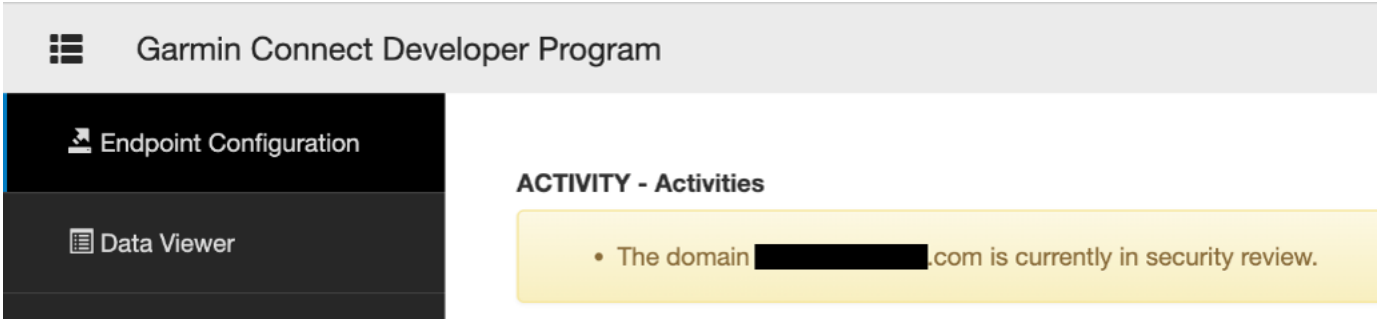
We are wenhooks based APIs and all data will be delivered to your server via PING or PUSH notifications.
You can configure your endpoints at API tools https://apis.garmin.com/tools/endpoints

Like the Ping Service, the Push Service allows partners to receive near-real-time updates of Garmin user data without delay or duplication associated with regularly scheduled update jobs. Unlike the Ping Service's callback URLs, the Push Service generates HTTPS POSTs that contain the updated data directly within the POST as JSON. This data is the exact same data that would have been returned by a Ping notification been generated and its callback URL invoked; it is purely a matter of preference and ease of integration whether to use the Ping or Push Service.

Note: Push notifications have the same retry logic using the same definition of a failed notification as the Ping Service and support the same On Hold functionality as the Ping service.

2.6.1 Security Review

All new domains provided at API tools are subject to a security review. You may see a warming if review is triggered.
It will clear automatically within 24- 48 hours.



If you are making any changes in production, you can reach out to connect-support@developer.garmin.com to validate new domain beforehand.

2.6.2 Deregistration endpoint

https://apis.garmin.com/tools/login

JSON Element	Description
summary type (list key)	The summary type of this list of pings.
userId	A unique user identifier corresponding to the underlying Garmin account of the user. This userId is *not* used as a parameter for any call to the API. However, it will persist across userAccessTokens should the user re-register to generate a new UAT.
userAccessToken	The UAT corresponding to the user that generated the new data.

Examples:

```
{
   "deregistrations": [
      {
         "userId": "4aacafe82427c251df9c9592d0c06768",
         "userAccessToken": "8f57a6f1-26ba-4b05-a7cd-c6b525a4c7a2"
      }
   ]
}
```

2.6.3 User Permission endpoint

https://apis.garmin.com/tools/login

User can opt-out from data sharing by turning off toggle at their account https://connect.garmin.com/modern/settings/accountInformation, in this case user access token will be still valid, but no data will be shared from or to users' account.

```
{"userPermissionsChange":[{
  "userId" : "31be9cac-5bf9-406b-9fa8-89879bcaceac",
  "userAccessToken" : "11613065858",
  "summaryId" : "x120d383-60256e84",
  "permissions" : [ "ACTIVITY_EXPORT",
        "WORKOUT_IMPORT",
        "HEALTH_EXPORT",
        "COURSE_IMPORT",
        "MCT_EXPORT"
],
  "changeTimeInSeconds": 1613065860
}]}
```

Consumer can have multiple permissions like "Activity Export" and "Workout Import", etc. set up. While signing up, user may only opt in for fewer permissions, so this endpoint helps in fetching the permissions for that particular user.

Method & URL: GET https://apis.garmin.com/userPermissions/

Response body: The retrieved user permissions in JSON.

Example response for this endpoint:

```
      {[
           "ACTIVITY_EXPORT",
           "WORKOUT_IMPORT",
           "HEALTH_EXPORT",
           "COURSE_IMPORT",
           "MCT_EXPORT"
          ]}
```

3 User Endpoints

Unlike Summary endpoints which fetch user data, User Endpoints perform operations on the user's account itself. The availability and scope of the operations are intentionally limited to protect the user's privacy.

3.1 Delete User Access Token

This service provides the ability to remove a user from your program, specific to the consumer key being used, by deleting the UAT. After being called, a final User Deregistration notification will be sent as though the user had withdrawn access through Garmin Connect (if enabled).

Immediately following the Deregistration ping, all notifications for that user will immediately stop and any attempts to request data with that UAT will be rejected as unauthorized. The deleted UAT cannot be restored. The same user (with the same Garmin Connect account) going through the OAuth a second time will generate a completely different UAT.

This endpoint must be called if the partner website or application provides a "Delete My Account" or "Opt-Out" mechanism outside of the normal Garmin Connect consent removal process or in any other case where the user would reasonably believe the partner program is giving them the opportunity to remove their consent to share Garmin data.

Request URL to delete a user registration
DELETE : https://apis.garmin.com/wellness-api/rest/user/registration

No parameters are required for this request. The user access token is taken from the OAuth header.

Response: On a successful request, this service returns HTTP 204 (no content) with no response body.

3.2 Get User ID

Each Garmin Connect user has a unique API ID associated with them that will persist across multiple UATs. For instance, if a user deletes their association through Garmin Connect and then, later, completes the OAuth process to generate a new User Access Token with the same Garmin Connect account, the second token will still have the same API User ID as the first token. Similarly, if a partner is managing multiple programs and the user signs up for each of them, the API User ID returned for each of the UATs will match.

The API ID provides no identifying information and is not used in any other Garmin API, web service, or system. There is no reason to ever pass the API User ID back to the API as user lookup will always be performed using the User Access Token in the Authorization header. **User ID must be used as a main user identifier.**

Request URL to fetch API User ID
GET https://apis.garmin.com/wellness-api/rest/user/id

No parameters are required for this request.

Response: `{"userId": "d3315b1072421d0dd7c8f6b8e1de4df8"}`