GARMIN INTERNATIONAL

Garmin Connect Developer Program
Start Guide

Version 1.1.0

CONFIDENTIAL

Contents

1 Revision History

Version	Date	Revisions
1.0.0	12/01/2020	First release
1.1.0	06/30/2025	Developer Account section added

2 Getting Started

Support Email: connect-support@developer.garmin.com

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 download workout plans and courses to their devices from corporate partners.

The 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 the corresponding specification documentation.

Access to GCDP APIs is restricted to server-to-server communication; access by end user devices is not allowed. APIs are designed for a secure one-time transfer of data from Garmin to Partner servers; ad-hoc requests for data are not permitted. Partners are responsible for receiving and storing data in a timely manner. PING notifications are guaranteed 7 days after receipt (Activity Files – 24 hours).

2.2 Client ID and Client Secret

To gain access to the APIs, please create a client ID and secret. The client ID is used to identify a partner uniquely, and the client secret is used to validate that the requests received are from that partner and not from a third party that has gained unauthorized access to the client ID.
The client ID can be considered public information, but the secret is private. For the security of users, developers must never include their client secret in public (mobile or browser-based) clients.

A client ID and secret credentials are created using the Developer Portal and the creation of 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 client ID that is rate-limited**. Once your integration has been verified for production, **subsequent apps will create a client ID with production-level access**. Please see “Requesting a Production-level APP” below for more information.

Note:
Multiple client IDs should be created to correspond to projects or implementations whose user base is logically separated. A typical scenario involves one partner managing user data from various other companies. A new client ID should be created and associated with each managed company, allowing Garmin users to make an informed decision about sharing their data with that specific 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 OAuth2 documentation at https://developerportal.garmin.com/developer-programs/content/829/programs-docs

2.4 Setting up Client ID 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 client ID and secret applicable to the program they want to configure.

2.4.1 API Configuration

You will be able to edit the API selection for your client ID if necessary for the evaluation-level apps. If changes are 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 the partners' app)
-user permission (through this endpoint, we notify if the user has removed authorization to share data)
Other endpoints are available based on API selection

2.4.3 User Authorization tool

This tool describes and performs the OAuth2 process.

2.5 Requesting a Production-level App

The **first client ID** 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 the corresponding specification document.

2.6 Endpoint Configuration

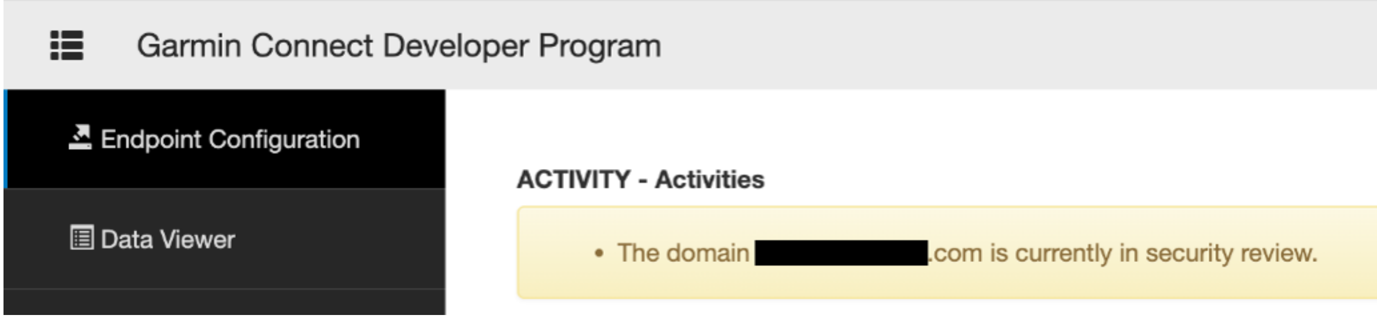
We are webhook-based APIs, and all data will be delivered to your server via PING or PUSH notifications.
You can configure your endpoints at API tools https://apis.garmin.com/tools/endpoints

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 the API tools are subject to a security review. You may see a warning if a review is triggered. It will clear automatically within 24- 48 hours.



ACTIVITY - Activities

- The domain [redacted].com is currently in security review.

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

Deregistration notification notifies your app if the user is disconnected from their GC account, or your app calls DELETE /registration

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.

Examples:

```
{
   "deregistrations": [
      {
         "userId": "4aacafe82427c251df9c9592d0c06768"
      }
   ]
}
```

2.6.3 User Permission endpoint

Users can opt out of data sharing by turning off the toggle at their account https://connect.garmin.com/modern/settings/accountInformation; in this case, the user's access token will still be valid, but no data will be shared from or to the user's account. The user permission summary will notify your app if the user has changed their permission post-connection. You can configure this summary via https://apis.garmin.com/tools/login

Example Notification:

```
{"userPermissionsChange":[{
  "userId" : "31be9cac-5bf9-406b-9fa8-89879bcaceac",
  "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/wellness-api/rest/user/permissions

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 client ID being used, by deleting the registration. 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 user ID will be rejected as unauthorized. The deleted user connection cannot be restored.

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.

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"}`

4 Developer Account

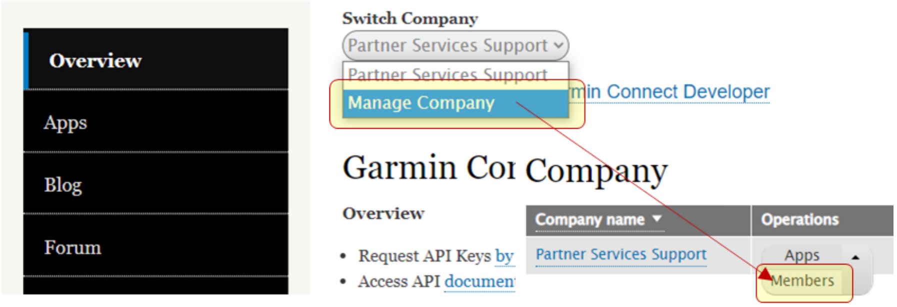
4.1 Team Members and Accesses

All individuals who require access to API specifications, internal tools, app credentials, or development code must be added to the list of verified users at developerportal.garmin.com.

Please note the following restrictions:

- Generic or non-personalized email addresses (e.g., support@, info@, contact@, dev@) are not allowed.
- Email addresses using non-company domains or free email services (e.g., Gmail, Outlook, Hotmail) are also prohibited.
- Third-party integrator domains are only allowed after providing a copy of the NDA between your organizations.
- As stated in Section 5.2 of the API Agreement, support will not be provided to users who have not verified their accounts. Sharing access, documentation, or app credentials with unverified individuals will result in the revocation of your app access without prior notice.

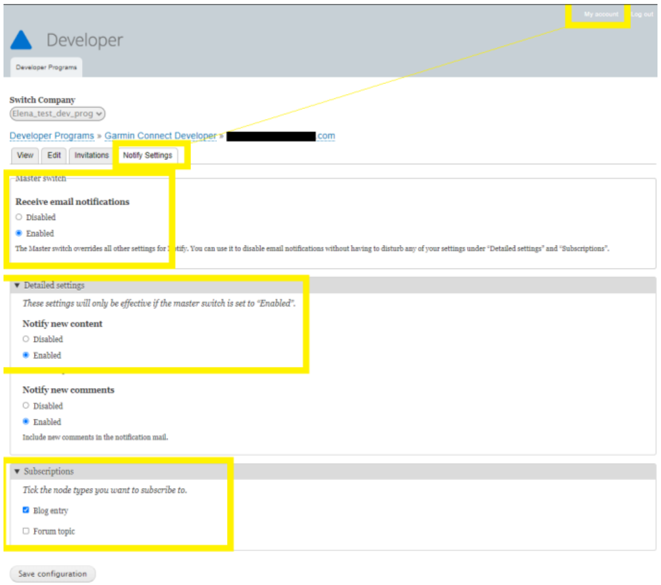
To add Developers/users to the account, log in, click on your company name, and select the "Members" section.



4.2 API Updates: sign-up steps

You may also **sign up for API Update Release Notifications** by going to 'My Account' - Notify Settings - Receive Email - Subscriptions - Blog Entry.

It is highly recommended to sign up for the Blog so that you will be aware of all future API updates.



Master switch

Receive email notifications

○ Disabled
● Enabled

The Master switch overrides all other settings for Notify. You can use it to disable email notifications without having to disturb any of your settings under "Detailed settings" and "Subscriptions".

▾ Detailed settings

These settings will only be effective if the master switch is set to "Enabled".

Notify new content

○ Disabled
● Enabled

Notify new comments

○ Disabled
● Enabled

Include new comments in the notification mail.

▾ Subscriptions

Tick the node types you want to subscribe to.

☑ Blog entry
☐ Forum topic