

GARMIN INTERNATIONAL

Garmin Connect Developer Program

사용 설명서

버전 1.0.0

비밀 문서

목차

1	수정사항	1
2	시작하기	2
2.1	Garmin Developer Program 의 목적	2
2.2	Consumer Key 와 Secret	2
2.3	사용자 등록	3
2.4	API 톨을 사용하여 Consumer Key 설정하기	3
2.4.1	Consumer API	3
2.4.2	Endpoint configuration	3
2.4.3	User Authorization	3
2.4.4	Request Signing	3
2.5	Production Key 요청하기	3
2.6	Endpoint 구성	4
2.6.1	Deregistration 엔드포인트	4
2.6.2	User Permission 엔드포인트	4
3	User Endpoint	5
3.1	User Access Token 삭제하기	5
3.2	User ID 얻기	5

1 수정사항

버전	날짜	수정사항
1.0.0		최초 발행

2 시작하기

2.1 Garmin Developer Program 의 목적

Garmin Connect Developer Program 은 Garmin 사용자들이 그들의 액티비티 트래커와 피트니스 디바이스에서 생성된 데이터를 Garmin 외의 기업 파트너들에게 공유하고 워크아웃 플랜과 코스를 이러한 기업 파트너로부터 자신의 디바이스에 다운로드할 수 있는 메커니즘입니다.

Garmin Connect Developer Program 은 5 가지 API 로 구성됩니다:

- **Training API** (Garmin Connect 에 워크아웃을 업로드)
- **Courses API** (Garmin Connect 에 코스를 업로드)
- **Health API** (Garmin Connect 로부터 건강 데이터를 가져오기)
- **Activity API** (Garmin Connect 로부터 액티비티를 가져오기)
- **Women's Health API** (여성의 건강 데이터를 가져오기)

각각의 API 에 대한 모든 정보는 개별 문서에서 설명하였습니다.

2.2 Consumer Key 와 Secret

API 에 대한 액세스 권한을 얻으려면 **consumer key** 와 **secret** 을 생성하여 주십시오. **Consumer key** 는 파트너를 식별하는 데 사용되며 **consumer secret** 은 수신된 요청이 파트너로부터 온 것이며 **consumer key** 에 대한 허가되지 않은 액세스 권한을 획득한 제 3 자가 보낸 것이 아니라는 점을 검증하는 데 사용됩니다.

consumer key 는 공공 정보로 간주할 수 있지만, **consumer secret** 은 개인 정보입니다. 사용자의 보안을 위하여 **consumer secret** 은 보호되며 일반적인 텍스트의 형태로 네트워크에 전송되지 않습니다. **Consumer secret** 을 모바일 앱과 같은 **consumer product** 에 삽입하는 것은 허용되지 않습니다.

Consumer key credential 은 Developer Portal 을 사용하고 앱(app)을 만들면 생성됩니다.

(<https://developerportal.garmin.com/user/me/apps?program=829>). 각각의 앱은 고유의 **consumer key** 를 나타냅니다.

키 생성 도중이라도, **api's** 를 선택할 수 있습니다.

첫 번째 **app** 은 횟수가 제한된 **evaluation-level consumer key** 를 생성할 것입니다. 일단 해당 **production** 에 대한 통합이 검증되었다면, 그 다음 **app** 들이 **production-level access** 권한이 있는 **consumer key** 들을 생성합니다. 자세한 사항은 “**production key** 요청하기” 부분을 참조하여 주십시오.

참고:

User base 가 논리적으로 구분된 **project** 또는 **implementation** 에 각각 상응하도록 다수의 **consumer key** 를 생성해야 합니다. 일반적인 시나리오는 하나의 파트너가 여러 개의 다른 회사로부터 제공된 사용자 데이터를 관리하는 것입니다. Garmin 사용자들이 충분한 정보에 입각하여 각각의 회사에게 데이터를 공유하는 것에 동의하는 결정을 내릴 수 있도록, 각각의 관리된 회사마다 새로운 키를 생성하여 연결시켜야 합니다.

2.3 사용자 등록

파트너가 사용자 데이터에 액세스하기 위해서는, 먼저 사용자는 파트너 액세스를 승인해야 합니다. Garmin user data 에 접근하기 위한 User Access Token (UAT)을 획득하고, 허가하고, 이를 사용해 서명을 하는 것에 관한 상세한 정보는 <https://developerportal.garmin.com/developer-programs/content/829/programs-docs> 에서 세부적인 Garmin OAuth 문서를 참조하십시오. Developer Program 웹 툴(아래 웹 툴 부분 참조)은 사용자 허가 및 signing 요청에 대한 추가적인 시범 설명을 포함하고 있습니다.

2.4 API 툴을 사용하여 Consumer Key 설정하기

Endpoint Configuration 툴 외에도 몇몇 웹 기반 툴은 파트너들의 통합을 지원할 수 있습니다. 이러한 툴은 설정하기를 원하는 프로그램에 적용할 수 있는 consumer key 와 secret 을 사용하여 <https://apis.garmin.com/tools/login> 에서 로그인을 하여 얻을 수 있습니다.

2.4.1 Consumer API

필요하다면 자신의 consumer key 에 대하여 API selection 을 편집할 수 있습니다.

2.4.2 Endpoint configuration

기본적으로 모든 API 는 다음 2 개의 endpoint 를 사용할 수 있습니다.

-deregistration (이 엔드포인트를 통해 우리는 사용자가 파트너 app 으로부터 연결을 끊으면 이를 파트너에게 알려줍니다.)

-user permission (이 엔드포인트를 통해 우리는 사용자가 데이터 공유의 허가를 제거하면 이를 알려줍니다.)
API selection 에 따라 그 밖의 엔드포인트를 사용할 수 있습니다.

2.4.3 User Authorization

이 툴은 전체 3-legged OAuth(3 자 인증) 과정을 설명하고 수행합니다. 이 툴은 User Access Token 을 수동으로 생성하여, 모든 파트너 OAuth infrastructure 가 작성되기 전에 현재 사용되는 consumer key 에 대하여 권한을 부여하는 데 사용할 수 있습니다.

2.4.4 Request Signing

이 툴은 OAuth 1.0a 서명 요청을 수행하는 방법을 설명하고 시연합니다. 서드파티 라이브러리의 사용이 권장되지만, 첫 번째 통합 및 디버깅의 목적으로는 수동 서명이 유용할 수도 있습니다. OAuth 1.0a 서명 요청에 대한 더 자세한 정보는 OAuth Specification 문서를 참조하여 주십시오.

2.5 Production Key 요청하기

Developer portal 을 통해 생성된 첫 번째 consumer key 는 evaluation key 입니다. 이 키는 요청수가 제한되며(rate-limit) 테스트, 평가, 개발의 목적으로만 사용해야 합니다. production-level key 를 얻으려면 먼저 [connect-support@developer.garmin.com](mailto:support@developer.garmin.com) 에 이메일을 보내 귀하의 evaluation key 와 현재 사용되고 있는 API pillar 의 목록을 제공하여 주십시오.

개별 API 요구사항에 대해서는 관련된 specification 문서를 참조하십시오.

2.6 Endpoint 구성

Ping Service 와 마찬가지로 Push Service 를 통해 파트너는 정기적으로 예정된 업데이트 작업에 관련된 중복이나 지연 없이 거의 실시간으로 Garmin 사용자 데이터의 업데이트를 수신할 수 있습니다. Ping Service 의 Callback URL 과는 달리 Push Service 는 JSON 으로서 POST 내에 직접적으로 업데이트된 데이터를 포함하고 있는 HTTPS POST 를 생성합니다. 이 데이터는 생성된 Ping notification 과 호출된 callback URL 에 의해 반환되는 데이터와 정확히 동일한 데이터입니다. Ping Service 와 Push Service 중 어느 것을 사용할 것인지는 순전히 선호도와 통합 용이성의 문제입니다.

참고사항: 푸시 알림은 Ping Service 와 동일한 실패한 알림의 정의를 사용하는 동일한 retry logic 을 가지고 있으며, Ping service 와 동일한 ON Hold 기능을 지원합니다.

2.6.1 Deregistration 엔드포인트

JSON Element	설명
summary type (list key)	이 Ping 목록의 summary type
userId	사용자의 기본 Garmin 계정에 해당되는 고유의 사용자 식별자. 이 userId 는 모든 API 호출에 대한 파라미터로서 사용되지 않습니다. 하지만 사용자가 새로운 UAT 를 생성하기 위해 재등록을 한다면, 이것은 userAccessTokens 에서 유지될 것입니다.
userAccessToken	새로운 데이터를 생성한 사용자에게 해당되는 UAT.

예시:

```
{  "deregistrations": [
    {
      "userId": "4aacaefe82427c251df9c9592d0c06768",
      "userAccessToken": "8f57a6f1-26ba-4b05-a7cd-c6b525a4c7a2"
    }
  ]
}
```

2.6.2 User Permission 엔드포인트

사용자는 자신의 계정 <https://connect.garmin.com/modern/settings/accountInformation> 에서 토글을 해제하여 데이터 공유에서 옵트 아웃 할 수 있습니다. 이 경우 사용자 액세스 토큰은 여전히 유효하지만 데이터가 공유되지 않습니다. 사용자 계정에.

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

3 User Endpoint

사용자 데이터를 fetch 하는 Summary endpoint 와는 달리 User Endpoint 는 사용자의 계정 자체에 대한 operation 을 수행합니다. 사용자의 프라이버시를 보호하기 위하여 이 Operation 의 가용성과 범위는 의도적으로 제한됩니다.

3.1 User Access Token 삭제하기

이 서비스는 UAT 를 삭제함으로써 사용되는 consumer key 를 기준으로 하여 프로그램으로부터 사용자를 제거할 수 있는 능력을 제공합니다. 호출이 이루어지면, 마치 사용자가 Garmin Connect 를 통한 액세스를 취소한 것처럼(이러한 기능이 활성화된 경우), 최종적인 User Deregistration(사용자 해지) 알림이 전송될 것입니다.

Deregistration 펄 직후에, 해당 사용자에 대한 모든 알림은 즉각적으로 중단되며 이 UAT 를 사용하는 데이터 요청 시도는 권한이 없는 시도로서 전부 거부됩니다. 삭제된 UAT 는 복구할 수 없습니다. 동일 사용자(즉, 동일한 Garmin Connect 계정을 가진 사용자)가 OAuth 를 두 번째로 진행한 경우, 완전히 다른 UAT 가 생성될 것입니다.

이 엔드포인트는 파트너 웹사이트 또는 애플리케이션이 정상적인 Garmin Connect consent removal process 외의 “Delete My Account” 또는 “Opt-Out” 메커니즘을 제공하는 경우 또는 파트너 프로그램이 사용자에게 Garmin 데이터 공유에 대한 동의를 철회할 기회를 제공하고 있다는 점을 합리적으로 신뢰할 수 있는 다른 모든 경우에 호출되어야 합니다.

사용자 등록을 삭제하기 위한 Request URL 은 다음과 같습니다

DELETE <https://apis.garmin.com/wellness-api/rest/user/registration>

이 요청에는 파라미터가 요구되지 않습니다. 해당 user access token 은 OAuth 헤더로부터 제거될 것입니다.

응답: 성공적인 요청 시, 이 서비스는 response body 없이 HTTP 204 (no content)를 반환합니다. 가능한 에러 반환에 대해서는 부록 E 를 참조하여 주십시오.

3.2 User ID 얻기

각각의 Garmin Connect 사용자는 자신과 관련된 고유의 API ID 를 가지고 있으며, 이것은 여러 개의 UAT 에서 유지됩니다. 예를 들어 사용자가 Garmin Connect 를 통한 association 을 삭제한 다음, 나중에 동일한 Garmin Connect 계정에서 새로운 User Access Token 을 생성하기 위한 OAuth 프로세스를 완료한 경우, 두 번째 token 은 첫 번째 토큰과 동일한 API User id 를 가질 것입니다. 이와 비슷하게 파트너가 여러 개의 프로그램을 운영하고 있으며 사용자가 각각의 프로그램에 sign up 한 경우, 각각의 UAT 에 대하여 반환되는 API User ID 가 매칭될 것입니다.

API ID 는 식별 정보를 제공하지 않으며 다른 Garmin API, 웹 서비스, 시스템에서 사용되지 않습니다. 언제나 Authorization header 의 User Access Token 을 사용하여 user lookup 이 수행되기 때문에, API User ID 를 API 에 되돌려 보낼 이유는 없습니다.

API User ID 를 fetch 하기 위한 Request URL

GET <https://apis.garmin.com/wellness-api/rest/user/id>

이 요청에는 파라미터가 요구되지 않습니다.

응답: {"userId": "d3315b1072421d0dd7c8f6b8e1de4df8"}