Guardian

Guardian Connect User Guide

(Developer Portal)

Version 3

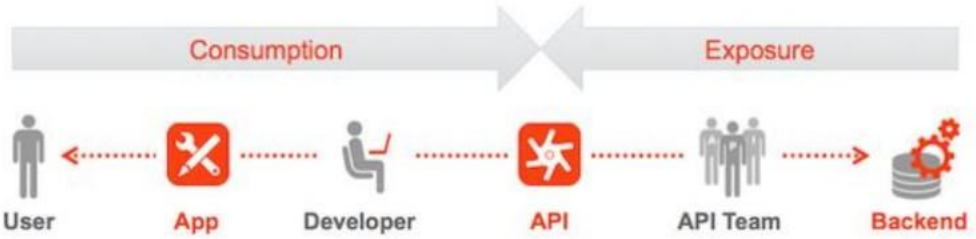
Last updated January 30, 2025

Table of Contents

Guardian Connect

Guardian Connect is an API Developer portal, which is a user friendly, self-service portal that enables API owners to publish their API documentation for application developers.

Application developers from external partners can leverage Guardian APIs within their applications they are planning to build for their customers. Application developers can browse through the APIs published on the portal, if the APIs meet their requirements, request access to try them in test environment.



Registration

Developers on the partner side to get access to APIs, the person(administrator) who is responsible to manage carrier connections, should email their company name, administrator first name, last name and contact email address to API_Admin@glic.com. Once we receive the required details, an account will be created in Guardian Connect and email will be shared with partners to register in Guardian Connect. If you do not receive the email, please check your spam folder. If still not found contact API_Admin@glic.com.

Sample Email:

From: noreply-guardian-connect@glic.com <noreply-guardian-connect@glic.com>

Sent: Saturday, January 7, 2025, 8:40 AM

To: <PARTNER EMAIL ADDRESS>

Subject: Welcome to Guardian Connect

Dear <Partner Name>

Welcome to Guardian Connect!

To activate your new Guardian Connect Account, you will need to verify a few pieces of information along with your one time use registration code:

Guardian

Registration Code: 61bb569b-359a-475e-8417-658e1c8e4228

For account verification and activation please navigate to the following link:

Click here to continue your PartnerAdmin Registration

Happy Building!

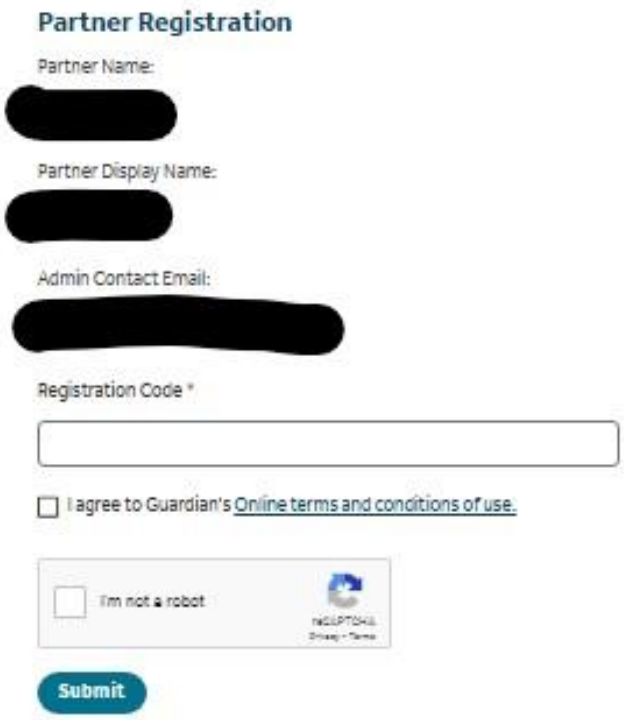
Sincerely,

The Guardian Connect Team

PLEASE DO NOT REPLY TO THIS EMAIL******

Clicking the above link will route to Guardian Connect registration page. Follow instructions from the table below to fill in the registration details.

Registration code	**Enter code received from email**

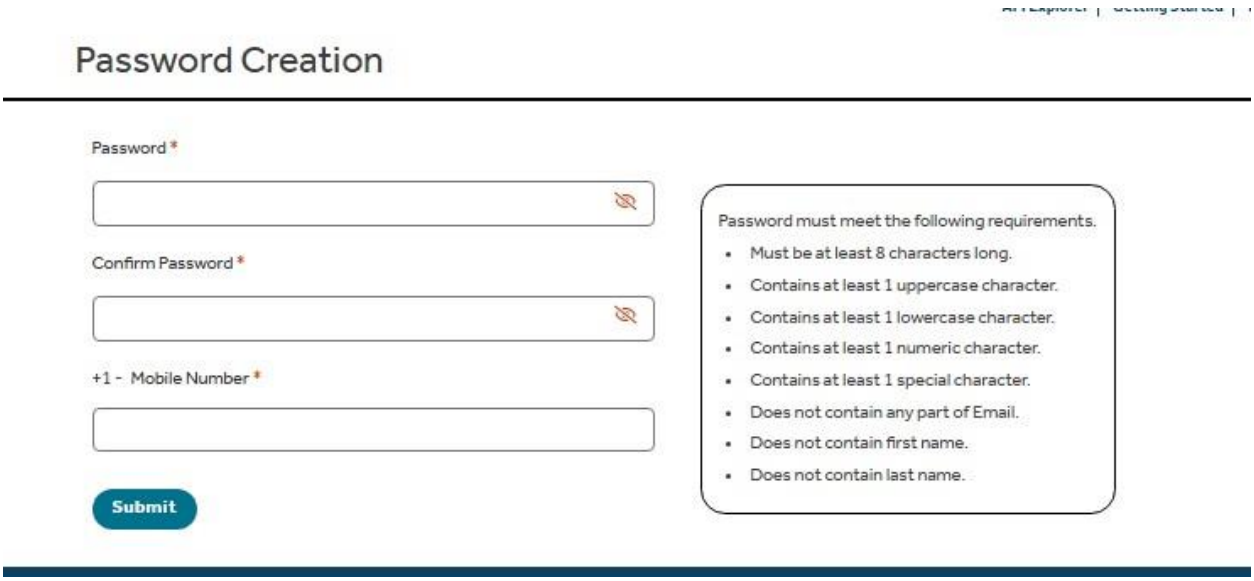


Once the above details are validated, you can create passwords as below. After entering password and mobile number, click submit.

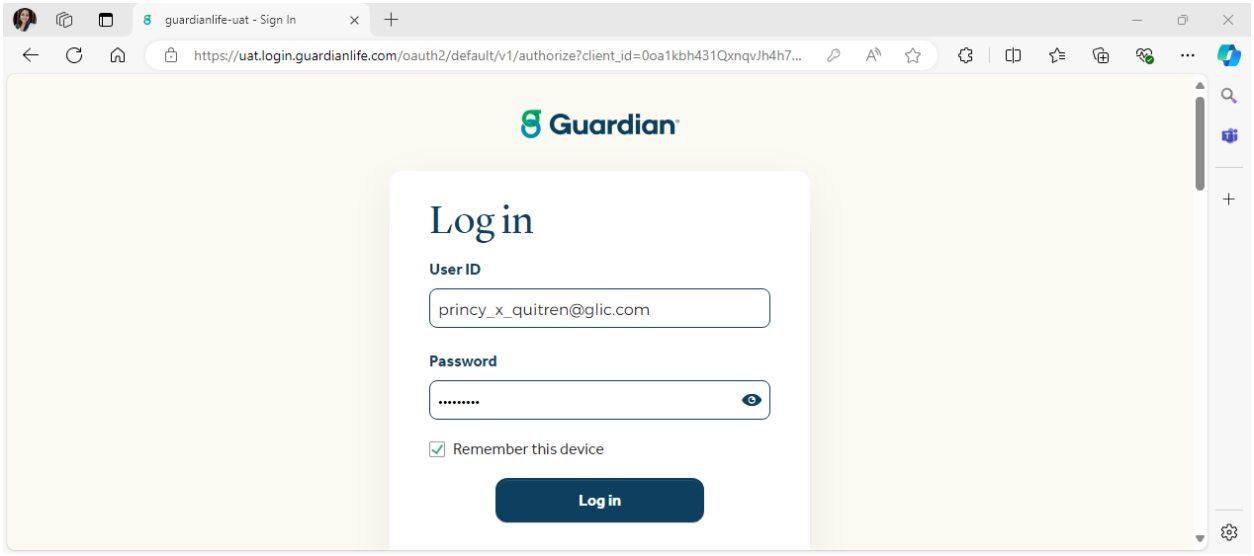
Password	**Enter Password (Password requirements are listed on the page)**
Confirm Password	**Re-Enter Password**
+1 – Mobile Number	**Enter number with no dashes starting with area code i.e. 232124323**

Password Requirements.

- Must be at least 8 characters long.
- Contains at least 1 uppercase character.
- Contains at least 1 lowercase character.
- Contains at least 1 numeric character.
- Contains at least 1 special character.
- Does not contain any part of email.
- Does not contain first name.
- Does not contain last name.

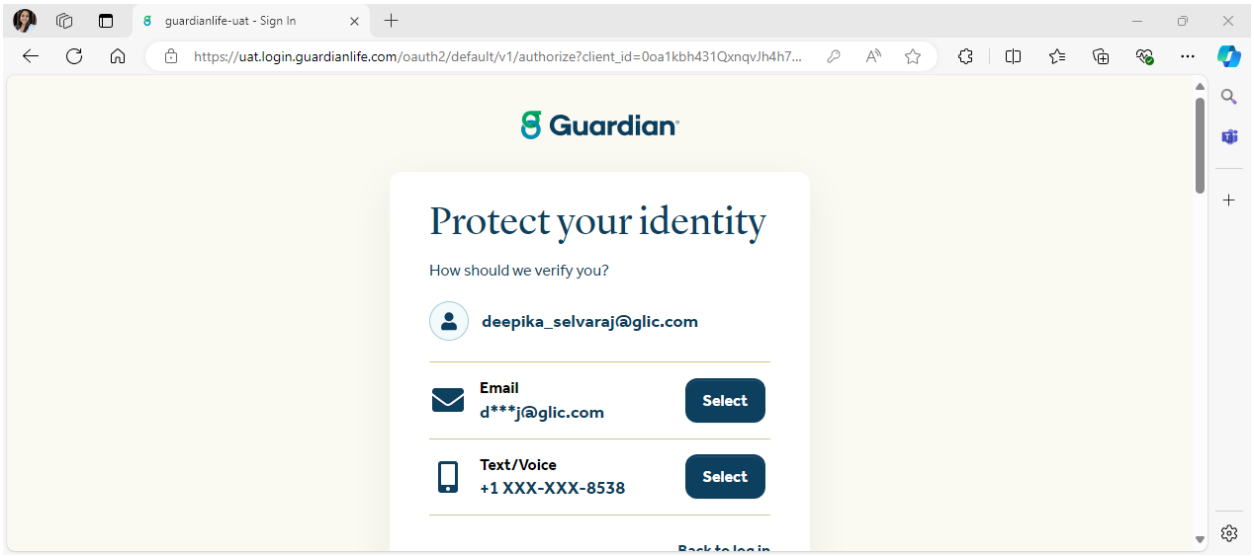


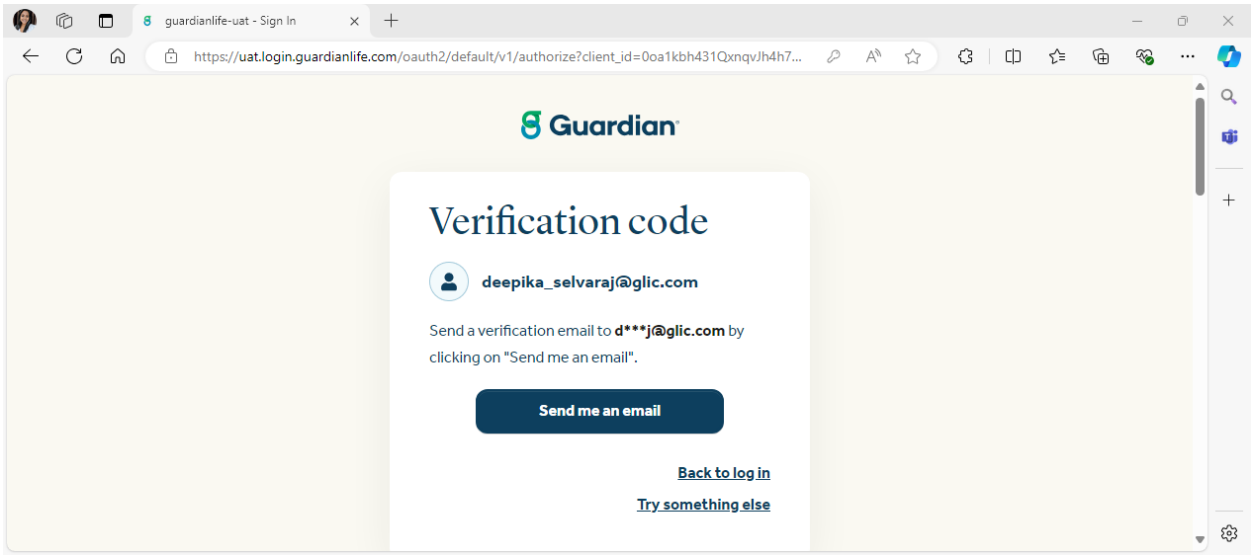
Once an account is created in Guardian Connect, the system will route to the sign in page. Please enter User ID (Email address) and password.

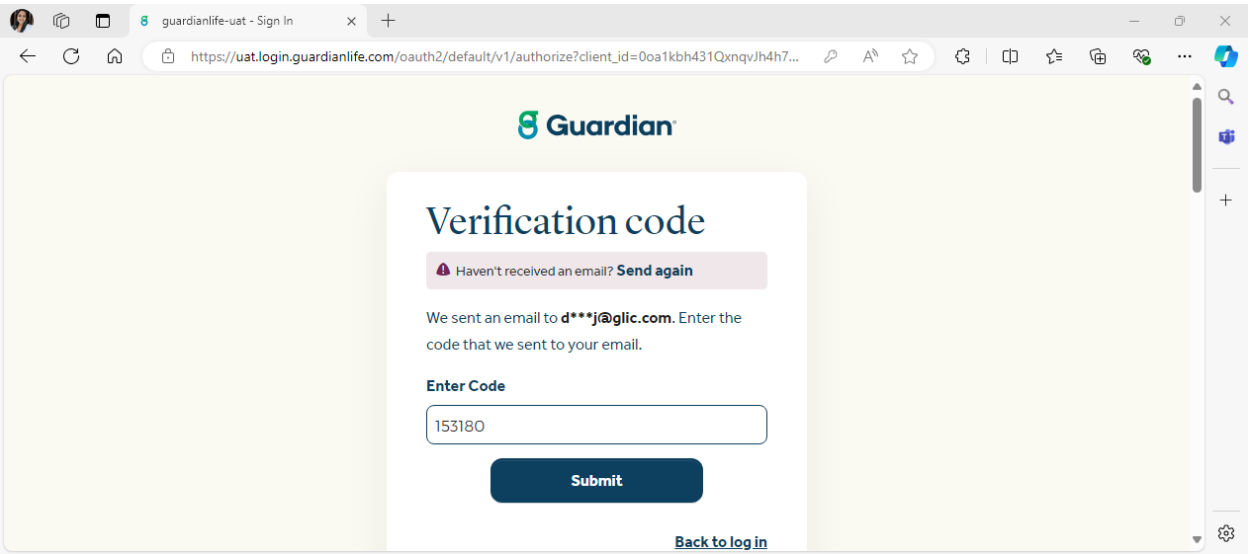


Please select Email or Phone number for Identity verification. The verification code will be sent based on your selection.

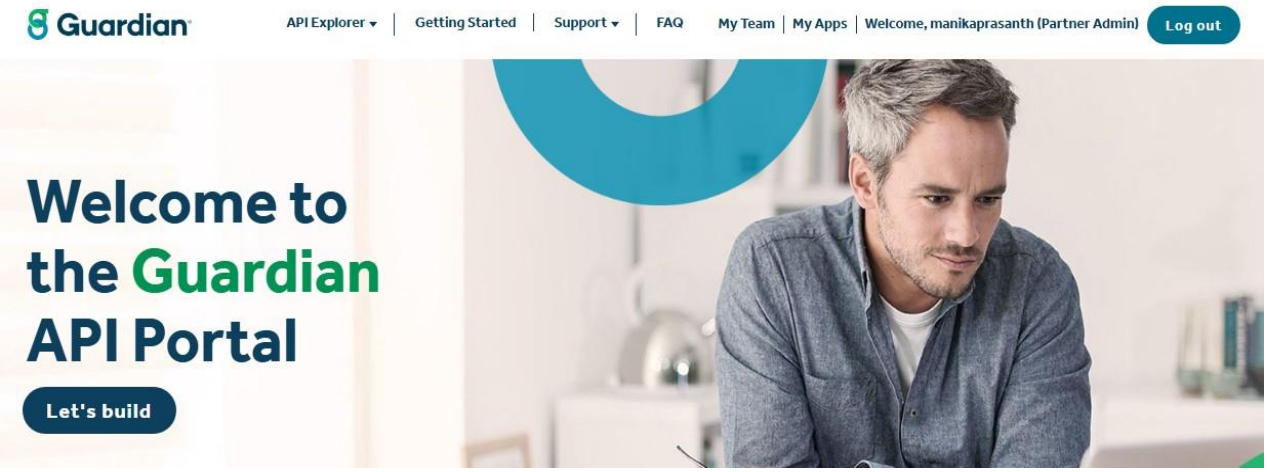
Guardian


guardianlife-uat - Sign In
https://uat.login.guardianlife.com/oauth2/default/v1/authorize?client_id=0oa1kbh431QxnqvJh4h7...
Guardian
Protect your identity
How should we verify you?
deepika_selvaraj@glic.com
Email
d***j@glic.com
Select
Text/Voice
+1 XXX-XXX-8538
Select


guardianlife-uat - Sign In
https://uat.login.guardianlife.com/oauth2/default/v1/authorize?client_id=0oa1kbh431QxnqvJh4h7...
Guardian
Verification code
deepika_selvaraj@glic.com
Send a verification email to d***j@glic.com by clicking on "Send me an email".
Send me an email
Back to log in
Try something else

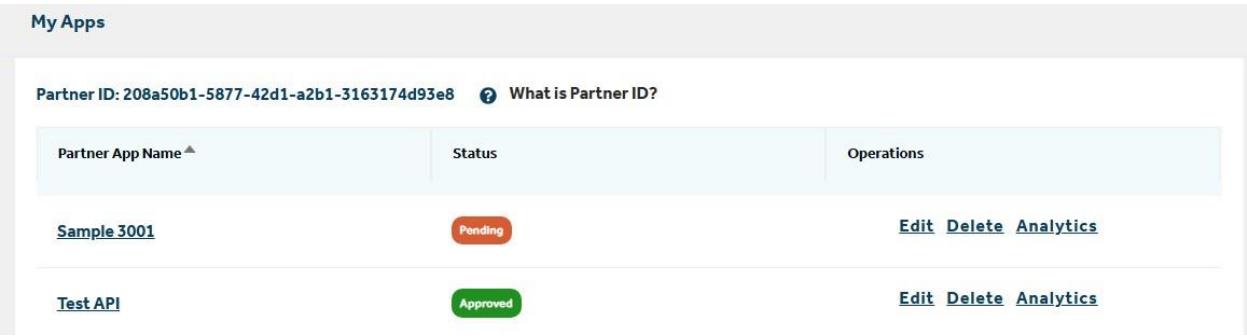


Please enter the received verification code in the box and you will be redirected to Guardian Connect Developer portal Home page as a logged in User.

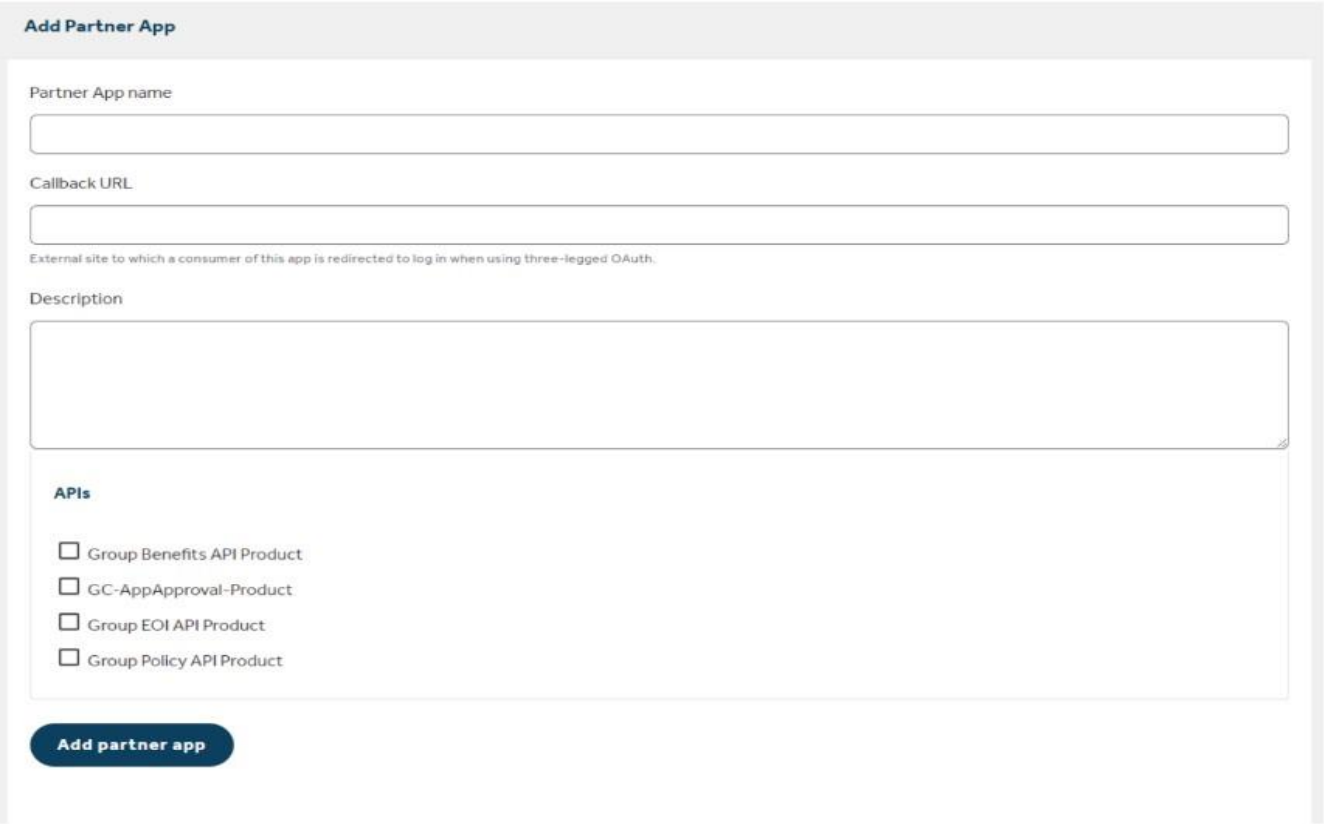


Creation of Developer APP

From the home page, select My Apps. Select Register new partner app



Partner App name	Enter the name you would like to identify the partner app as
Callback URL	Field can be left blank
Description	Freeform to describe the partner app
API's	Select the required APIs in the list. We can select multiple APIs in app



Once app is created, the partner app will appear in MyApps. Under Products your new products will appear. The Blue boxes will state Pending. Once your products have been approved the status will update to Enabled

Once all steps are completed and app is approved, the consumer key and secret will be active.

The reference ID section can be found in top of my apps page

Once the consumer key, consumer secret and reference ID have been received, the next steps can be started.

Security: OAuth 2.0 and JWT

Introduction

A JSON Web Tokens (JWT) is a self-contained, open standard JSON object used to securely exchange information between 2 or more parties. This information is in the form of a set of

claims, which are key/value pairs generally used to provide unique attributes about a user or a 3rd party. JWT is commonly implemented in OAuth 2.0 and OpenID Connect (OIDC) type integrations. The following document provides detailed guidelines on usage, generation, consumption, and validation of JWT using Apigee Edge.

JWT as OAuth 2.0 Access Tokens

JSON Web Tokens are used as OAuth 2.0 tokens while requesting access to protected resources, such as APIs. The authorization severs or issuer is responsible to generate the JWT after successfully authenticating and Authorizing a client App. These apps identify themselves using an API key and secret along with some other additional attributes. This token is signed by the issuer/authorization server using a private key or shared key. Signing the token ensure that payload will immediately become invalid if tampered by the client application or user. This ensures that the integrity of the payload is intact. These tokens are used as short lived bearer token, which means the bearer of the token will be able get access to the requested data when they present it to the authorization server, hence it is important to ensure this token is protected and securely stored. A compromised token can be revoked by the authorization server. To provide maximum security, it is important to ensure these tokens have a short life, typically 30mins to an hour.

Generate JWT Token

JWT Token Endpoint

Environment	Method	Endpoint	IP whitelisting Needed
PROD	POST	https://api.guardianlife.com/auth /oauth/v2/toke n/generate	Yes

Input parameters

Here are the required inputs to the JWT token endpoint

Environment	Method	Endpoint	IP whitelisting Needed
query param	grant_type	client_credentials	grant_type=client_crede ntials
query param	nonce	Unique random	nonce=randomvalue

		alphanumeric string. This string must be unique for each token request. The purpose of this attribute is to prevent replay attacks.	
Header	Authorization	Basic <Base64 encoded (Consumer Key: Consumer Secret)	Basic RUefddfZzMVrfRgfmxUA=='
Body	Claims-subject	Reference ID provided as part of partner registration process. {"claims": {"subject": "<reference id>"}}	{"claims": {"subject": "9ef4a793-c9fe-456d-99ae6a53d866e3e7"}}

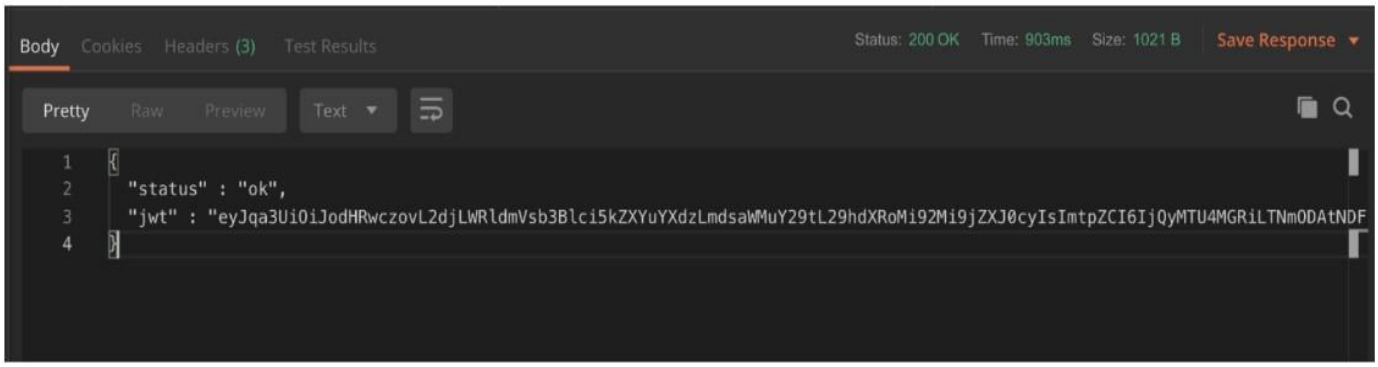
Valid Token Endpoint Response

{

"status" : "ok",

"jwt":"eyJqa3UiOiJodHRwczovL2djLWRldmVsb3Blci5kZXYuYXdzLmdsaWMuY29tL29hdXRoMi92Mi9jZXJ0cyIsImtpZCI6IjQyMTU4MGRiLTNmODAtNDFhZi1iNzU1LWQ1OTEyZjA5NDgxZiIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJzdWIiOiI5ZWY0YTc5My1jOWZlLTQ1NmQtOTlhZS02YTUzZDg2NmUzZT16ciLCJhdWQiOiJFRnNqR0xVV0VqOFBydUFoaWRTQWFSUWxxMGQ5QVpEWSIsInZlbmRvcl9pZCI6IjllZjRhNzkzLWM5ZmUtNDU2ZC05OWFlLTZhNTNkODY2ZTNlNyIsImlzcyI6ImFwaXN2Y2F1dGguZGV2LmF3cy5nbGjLmNvbSIsImV4cCI6MTU3MjI3NTIzMiwiaWF0IjoxNTcyMjcxNjMyLCJub25jZSI6ImdkZmdkczEiLCJqdGkiOiJiOTNlYTNiNi03NjU4LTQxYzgtOGQ2YS1jZTQ1NTJmZjY3OGYifQ.U1pHvXUaSEwbJRsZR928aH162lBpFwZf7vz_wtPUrisPWiI27eqMPEwRJUNap2v6uDJmLlBzWFtza_5UsWu6p7y9KOI1NHoSwiGaS4K1lBk0fyqGSXMxgXqklpeI_EkDRGcjS0rZ7D5uC1ivHrhVoEiMVB_9WRXKEQYOKrgxNGM7JlnLy8PXxN6BcmEWTAmXeViU9WerjrstUkErH7RqtlhffB4dKPtgamTAtPlh9W3TUJ0OlxrkfkisIJlgmA3ReDjidkFn926jRzgA237qnF5pDwjrbXDH3jaNPNVVsWnvg2OrR5L9Rn6PDbZUOYVr7iknFMup6vi94wPA"

}



Status Codes

Status codes	Response	Reason
200 OK	Valid JWT response	NA

401 Request missing Authorization Data	"error": {
	"code": 401.01, "message": "Request missing Authorization Data"
	}
		Authorization header missing

400 - Bad Request	"error": {
	"code": 400.01,
	"message": "Missing required fields"
	}
		Any required attribute is missing such as nonce or subject

401 -unauthorized	"error": {
	"code": 401.01,
	"message": "Invalid Nonce"
	}
		Same nonce used again. Nonce should be unique for each token request

401 - Invalid Subject or Partner/App not active	"error": {
	"code": 401.01,
	"message": "Unauthorized user"
	}
		Subject is invalid - Subject must be the unique vendor reference id provided by the Guardian Connect API during new partner registration process. All API keys are associated with a given subject and must match for validation to be successful.
		
		App/Partner is invalid or not active - Partner is marked inactive in the system.

Guardian

JWT Verification by Client App

Since we are using JWT as OAuth 2.0 access tokens, the token verification needs to happen first at the client end and later when the client requests access to a resource using a bearer token, the issuer (authorization server) will do token verification again before giving access to the requested resource.

Steps to validate a JWT

Step #	Validation	Reason
Signature Verification		
1	Decode the JWT. The header and the payload are encoded and separated by "." (period)	
2	Read the header section and look for "jku" and "kid" claims	
3	Verify the url against whitelisted JWKS urls	
4	Download the JWKS from the url provided in the "jku" claim	
5	Read the "n" attribute for the given "kid" claim	
6	Check the algorithm used to sign the payload using the "alg" claim from the header section	
7	Use the "n" value from the JWKS to validate the signature of the JWT payload. Proceed to next step if signature is valid	Integrity of the token is intact
Additional Security Validations (JWT validation beyond signatures)		
8	verify subject (sub)	subject must match the subject provided during token request

9	verify nonce	nonce must match the nonce provided during token request
10	verify issuer (iss)	Issuer must match the below listed issuers by Environment **Environments** / **Issuer** PROD / https://api.guardianlife.com/
11	verify expiry (exp)	current time should be prior to the value in the expiry (exp) claim.
12	verify audience (aud)	(aud) claim will contain API key. (aud) must match API key provided during token request

Token Expiry

Please note tokens are only valid for 30 minutes from the time of issuance. A new token can be requested after 30 mins with a new nonce.

Verification of JWT by Issuer

Input parameters

Attribute	type	Expected value	Example
nonce	query params	The nonce must match the nonce provide during token request	nonce=gdfgds1
Authorization	Headers	he JWT used as a bearer token for verification	Authorization: Bearer'eyJqa3sdjfksjdfks'

Steps to validate a JWT

Step #	Validation	Expected results (by environments)
Signature Verification		
1	Decode the JWT. The header and the	

	payload are encoded and separated by "." (period)	
2	Read the header section and look for "jku" and "kid" claims	
3	Download the JWKS from the url provided in the "jku" claim	
4	Read the "n" attribute for the given "kid" claim	
5	Check the algorithm used to sign the payload using the "alg" claim from the header section	
6	Use the "n" value from the JWKS to validate the signature of the JWT payload. Proceed to next step if signature is valid	Integrity of the token is intact
Additional Security Validations (JWT validation beyond signatures)		
7	verify nonce	nonce must match the nonce provided during token request
8	verify expiry (exp)	Current time should be prior to the value in the expiry (exp) claim.

Status Codes

Status code	Response	Reason
200 OK	Valid response from the backend after successful validation of JWT	

401 Request missing Authorization Data	"error": {
	"code": 401.01,
	"message": "Request missing Authorization Data"
	}
		Bearer token missing

400 Bad Request	"error": {
	"code": 400.01,
	"message": "Missing required attributes"
	}
		Nonce is missing

401 Unauthorized	"error": {
	"code": 401.01,
	"message": "Token expired orinvalid"
	}
		Token as either expired or already revoked

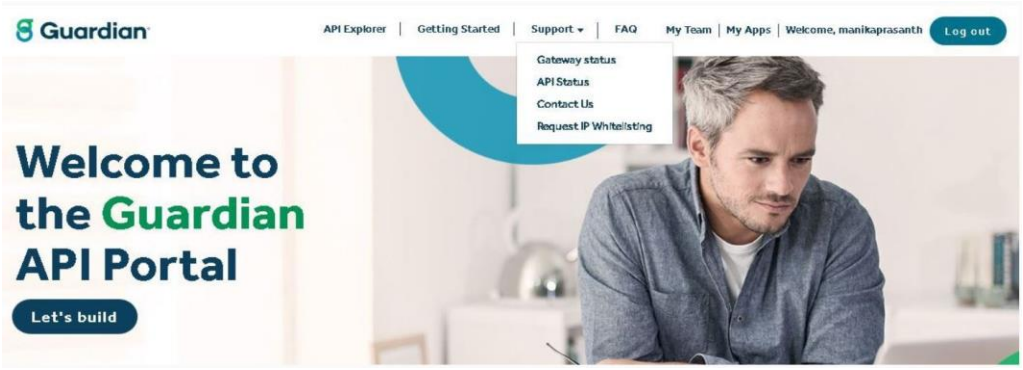
401 Invalid Nonce	"error": {
	"code": 401.01,
	"message": "Invalid Nonce"
	}
		Invalid Nonce. Nonce does not match the nonce provided using token request

IP Whitelisting

Whitelisting the IP addresses is necessary to gain access to the Guardian Connect APIs.

To request an IP Whitelisting, follow the following methods.

Locate the **Request IP Whitelisting** URL in the support menu.



To access the IP Whitelist request form, click on the **Submit a New Request** button.

Select the Environment. Environment options are,

a. Non-Production
b. Production

Please submit the IP address details that are valid. The submitted data will be sent as a GSC (Guardian Service Center) request and sent by email for approval. At the top of the page, the success message will be displayed. An error message will appear at the top of the page if there are any errors in the submission.

After the approval or rejection of your request. The email will be sent in accordance with the status. The approval of your request and the whitelisting of IP addresses are necessary for this communication to occur.

The list page can be found under the same menu to check existing requests.

Guardian


Submit a New Request
Filter by Environment: *
All
All
Non Production
Production
Date
Partner Name
Environment
IP Details
Status
11/17/2023 ashwini Non Production 127.0.0.1 In Progress
11/16/2023 manik Non Production 127.0.0.1/10 In Progress 05/16/2024 View Details
11/16/2023 manik Non Production 12.0.0.1/101 In Progress 05/16/2024 View Details
11/16/2023 manik Non Production 127.0.0.1/10 In Progress 05/16/2024 View Details
11/16/2023 manik Non Production 127.0.0.1/31 In Progress 05/16/2024 View Details