

LINE Notify API Document

Changes

Date	Description
2016-10-24	Add description for uploading image.
2016-09-29	Initial version

Overall flow and possible implementations of the API

The API consists of an OAuth2 authentication part and a LINE notification part. The overall flow of the API is as follows.

1. Intended users: Plan to configure LINE notifications
2. Connected service: Redirect to OAuth2 authorization endpoint
3. LINE: Select notification channel and check user agreement status. Redirect to connected service.
4. Connected service: Receive access token by accessing OAuth2 token endpoint using the parameters given during redirection
5. Connected service: Stores access tokens
6. (When sending notification) Connected service: Calls notification API using stored access tokens
7. (When checking notification settings) Connected service: Calls connection status check API and then displays connection status to user
8. (When disabling notifications) Connected service: Calls disconnection API

From the flow above, features that need to be implemented on connected services are as follows

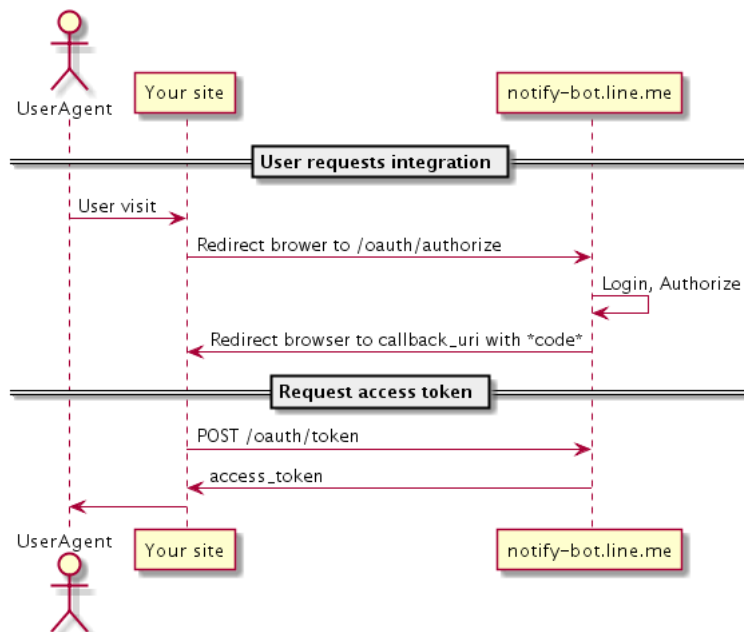
- Generating OAuth2 URL addresses and redirecting
- Storing OAuth2 access tokens connected to users
- Calling the notification API at the time of a notification
- (If there is a page for checking connection status) Displaying connection status through connection status API
- (When the connected service is disabling a notification) Calling notification revoke API

As notifications can be configured and revoked on the web page, implementation of the API is optional.

Authentication

Overview: Becomes a provider based on OAuth2 (<https://tools.ietf.org/html/rfc6749>). The authentication method is authorization_code. The access token acquired here can only be used for notification services.

The host name for authentication API endpoint is notify-bot.line.me.



GET <https://notify-bot.line.me/oauth/authorize>

The following is the OAuth2 authorization endpoint URI.

Request method

Request methods/headers	Value
Method	GET

Request parameters

The received parameters are as follows.

Parameter name	Required/optional	Type	Description
response_type	Required	fixed value	Assigns "code"
client_id	Required	string	Assigns the client ID of the generated OAuth
redirect_uri	Required	URI	Assigns the generated redirect URI. We recommend using HTTPS on redirect URI to prevent code parameter leaks.
scope	Required	fixed value	Assigns "notify"
state	Required	string	Assigns a token that can be used for responding to CSRF attacks CSRF attacks are typically countered by assigning a hash value generated from a user's session ID, and then verifying the state parameter variable when it attempts to access redirect_uri. LINE Notify is designed with web applications in mind, and requires state parameter variables.
response_mode	Optional	string	By assigning "form_post", sends POST request to redirect_uri by form post instead of redirecting Extended specifications: https://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html We recommend assigning this to prevent code parameter leaks in certain environments Reference: http://arstechnica.com/security/2016/07/new-attack-that-cripples-https-crypto-works-on-macs-windows-and-linux/

Response

When successful, redirects to the assigned redirect_uri or posts according to the form with the parameters below attached.

Parameter name	Type	Description
code	string	A code for acquiring access tokens
state	string	Directly sends the assigned state parameter

When there is a failure, redirects to the assigned reirect_uri with the parameters below attached.

Parameter name	Type	Description
error	string	Assigns error codes defined by OAuth2 https://tools.ietf.org/html/rfc6749#section-4.1.2
state	string	Directly send the assigned state parameter
error_description	string	An optional huma-readable text providing additional information, used to assist the client developer in understanding the error that occurred.

POST <https://notify-bot.line.me/oauth/token>

The OAuth2 token endpoint.

Request methods

Request methods/headers	Value
Method	POST
Content-Type	application/x-www-form-urlencoded

Request parameters

The parameters are as follows.

Parameter name	Required/optional	Type	Description
grant_type	Required	fixed value	Assigns "authorization_code"

code	Required	string	Assigns a code parameter value generated during redirection
redirect_uri	Required	uri	Assigns redirect_uri to assigned authorization endpoint API
client_id	Required	string	Assigns client ID to issued OAuth
client_secret	Required	string	Assigns secret to issued OAuth

Response

Response header	Value
Status	200: Success 400: Unauthorized request Other: Processed over time or stopped
Content-Type	application/json

Response body

The response body is a JSON object type.

Name	Type	Value description
access_token	string	An access token for authentication. Used for calling the notification API to be mentioned below.

Notification

Overview: An API for LINE notifications. OAuth authentication is required in advance. It can be used to check connection status, actual notifications, and disconnecting.

The host name for notification API end point is notify-api.line.me.

Authentication method

Request header authorization: Grants bearer <access_token> and accesses. If the access token used is invalid, a 401 status code and WWW-Authenticate header is returned according to RFC6750.

POST https://notify-api.line.me/api/notify

Sends notifications to users or groups that are related to an access token.

If this API receives a status code 401 when called, the access token will be deactivated on LINE Notify (disabled by the user in most cases). Connected services will also delete the connection information.

Requests use POST method with application/x-www-form-urlencoded (Identical to the default HTML form transfer type).

Expected use cases

When a connected service has an event that needs to send a notification to LINE

Request method

Request methods/headers	Value
Method	POST
Content-Type	application/x-www-form-urlencoded OR multipart/form-data
Authorization	Bearer <access_token>

Request parameters

The parameters are as follows.

Parameter name	Required/optional	Type	Description

message	Required	String	1000 characters max
imageThumbnail	Optional	HTTP/HTTPS URL	Maximum size of 240×240px JPEG
imageFullsize	Optional	HTTP/HTTPS URL	Maximum size of 1024×1024px JPEG
imageFile	Optional	File	<p>Upload a image file to the LINE server. Supported image format is png and jpeg.</p> <p>If you specified imageThumbnail ,imageFullsize and imageFile, imageFile takes precedence.</p> <p>There is a limit that you can upload to within one hour. For more information, please see the section of the API Rate Limit.</p>

Limitations are identical to Business Connect API

ref. https://developers.line.me/businessconnect/api-reference#sending_message

Response

Response headers	Value
Status	200: Success 400: Unauthorized request 401: Invalid access token 500: Failure due to server error Other: Processed over time or stopped
Content-Type	application/json

Response body

The response body is a JSON object type.

Name	Type	Value description
status	number	Value according to HTTP status code 200: Success 400: Unauthorized request 401: Invalid access token
message	string	Message visible to end-user

Sample

```
$ curl -X POST -H 'Authorization: Bearer <access_token>' -F 'message=foobar' \
https://notify-api.line.me/api/notify
{"status":200,"message":"ok"}

$ curl -v -X POST -H 'Authorization: Bearer invalidtoken' -F 'message=foobar' \
https://notify-api.line.me/api/notify
{"status":400,"message":"Invalid access token"}
```

GET https://notify-api.line.me/api/status

An API for checking connection status. You can use this API to check the validity of an access token. Acquires the names of related users or groups if acquiring them is possible.

On the connected service side, it's used to see which groups are configured with a notification and which user the notifications will be sent to. There is no need to check the status with this API before calling /api/notify or /api/revoke.

If this API receives a status code 401 when called, the access token will be deactivated on LINE Notify (disabled by the user in most cases). Connected services will also delete the connection information.

Expected use cases

If a connected service wishes to check the connection status of a certain user

As LINE Notify also provides the same feature, support for this API is optional.

Request methods

Request methods/headers	Value
Method	GET
Authorization	Bearer <access_token>

Response

The message body contains detailed information in JSON

Response headers	Value
Status	200: Success · Access token valid 401: Invalid access token Other: Processed over time or stopped
Content-Type	application/json

Response body

The response body is a JSON object type.

name	type	value description
status	number	Value according to HTTP status code 200: Success · Access token valid 401: Invalid access token
message	string	Message visible to end-user
targetType	string	If the notification target is a user: "USER" If the notification target is a group: "GROUP"
target	string	If the notification target is a user, displays user name. If acquisition fails, displays "null." If the notification target is a group, displays group name. If the target user has already left the group, displays "null."

Sample

```
$ curl -H 'Authorization: Bearer <access_token>' \
https://notify-api.line.me/api/status
{"status":200,"message":"ok","target":"foobar"}
```

```
$ curl -H 'Authorization: Bearer invalidtoken' \
https://notify-api.line.me/api/status
{"status":400,"message":"Invalid access token"}
```

POST <https://notify-api.line.me/api/revoke>

An API used on the connected service side to revoke notification configurations. Using this API will revoke all used access tokens, disabling the access tokens from accessing the API.

The revocation process on the connected service side is as follows

1. Call /api/revoke
2. If step 1 returns status code 200, the request is accepted, revoking all access tokens and ending the process
3. If step 1 returns status code 401, the access tokens have already been revoked and the connection will be d
4. If step 1 returns any other status code, the process will end (you can try again at a later time)

Expected use cases

When the connected service wishes to end a connection with a user

As LINE Notify also provides the same feature, support for this API is optional.

Request methods

Request methods/headers	Value
Method	POST
Content-Type	application/x-www-form-urlencoded
Authorization	Bearer <access_token>

Request parameters

There are no parameters.

Response

The message body contains detailed information in JSON

Response headers	Value
Status	200: Success 401: Invalid access token Other: Processed over time or stopped
Content-Type	application/json

Response body

The response body is a JSON object type.

name	type	value description
status	number	Value according to HTTP status code 200: Success 401: Invalid access token
message	string	Message visible to end-user

Sample

```
$ curl -X POST -H 'Authorization: Bearer <access_token>' \
https://notify-api.line.me/api/revoke
{"status":200,"message":"ok"}

$ curl -X POST -H 'Authorization: Bearer invalidtoken' \
https://notify-api.line.me/api/revoke
{"status":400,"message":"Invalid access token"}
```

API Rate Limit

There is a limit to the number of times an API can be called on each service.
The default number is set to 1000.

The limit is per access token.

The API Rate Limit status, can be checked on the response header of the API.

Header name	Description
X-RateLimit-Limit	The limit of API calls per hour
X-RateLimit-Remaining	The number of possible remaining API calls
X-RateLimit-ImageLimit	The limit of Uploading image per hour
X-RateLimit-ImageRemaining	The number of possible remaining Uploading image
X-RateLimit-Reset	The time when the limit is reset (UTC epoch seconds) ex:1472195604