

FYDO API Security Changes

How the move from Legacy API Keys to HMAC authentication affects your FYDO API integrators, and what to do before enforcement.

FYDO is enhancing security around API usage. The authentication model is changing from Legacy API Keys to a HMAC (Hash-Based Message Authentication Code) model.

There will be a 2-month grace period where the Legacy API Key model will be supported, while hospital API Integrators work towards transitioning to the HMAC method of authentication.



Security screen changes

- Existing API Keys are now hidden.
- A key can now be rotated manually, which also gives the old key a 72-hour grace period, so the old key will work for 72 hours, giving integrators time to change to the new key at a time that suits them.

New API Integrators screen

- All existing API Users from the Security screen automatically have an Integrator ID set up.
- Under each Integrator, there is now the ability to add a contact email and phone number.
- All API endpoints are listed, with permissions that can be set to “Allowed” or “Not Allowed” for each user.
- An IP address allow list is available to restrict API Integrators to specific IP addresses.
- An HMAC Secret Key can be generated to support the new method of making API calls, which will be replacing the Legacy API Key in 2 months’ time.

API Log screen

- A new Audit Log screen is available, logging changes made to the API Integrator screen.



Under this screen, you will have a 1-time opportunity to edit any API Usernames that are generic,

such as “FYDO User”, so these users can be properly identified by the name only. A warning screen will prompt you to update any usernames upon the first save.



Settings > Security

If an API Key is lost or forgotten, it will need to be rotated:

1. Click on the Edit button.
2. Click on the Rotate API Key (Legacy) button to generate a new API Key.



Rotating a Legacy API Key

- Copy the API Key shown and click Confirm to save.



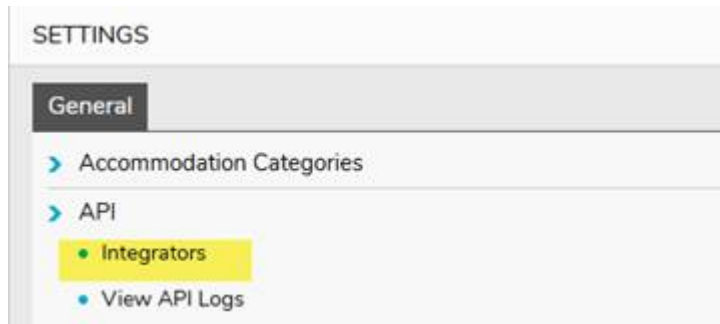
The new key is shown once — copy it before confirming

[REDACTED]

All existing API Users that were set up in the Security screen will have an Integrator ID created within the Integrators screen. This ID is used along with the HMAC Secret Key generated on the same screen, which will replace the Legacy API Key for authentication in 2 months.

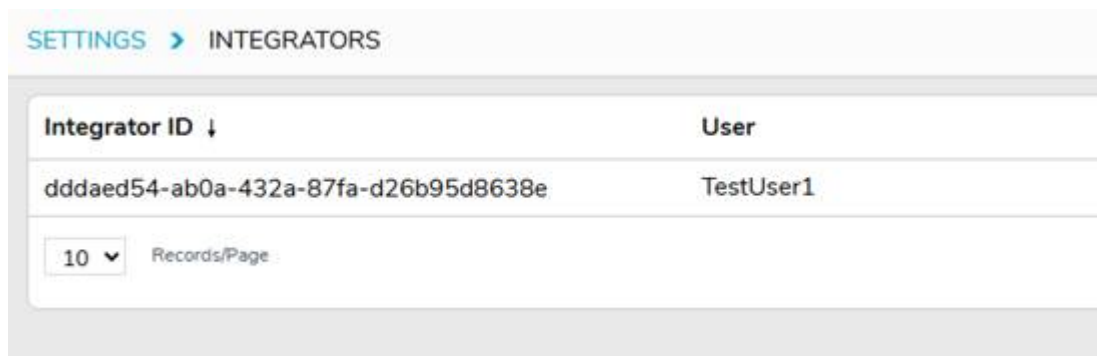
To access the Integrators screen:

1. Go to Settings > Integrators, under the API menu.



Settings > API > Integrators

2. Open an Integrator's settings by clicking on the Integrator.



The Integrators list

3. Within the Integrator screen, you can:
 - Add the contact details (email and phone) of the API Integrator, used for future contact.
 - Generate an HMAC Secret Key, used for authenticating API calls along with the Integrator ID.
 - Set a restriction on IP addresses that are allowed to make API calls to your FYDO database.
 - Set Endpoint Permissions — to either allow or deny access to particular data within FYDO.

SETTINGS > INTEGRATORS > TESTUSER1 Save

User Details

Integrator ID: dddaed54-ab0a-432a-87fa-d26b95c

User: TestUser1

Email: Testuser@gmail.com

Phone: (08)9876-5432

HMAC Secret: Generate Secret Key

IP Allowed:

IP	Action
203.0.113.25	✗
	✗

EndPoint Permissions

Endpoint	Allowed	Not Allowed
AnaesthesiaTypes	Allowed	Not Allowed
getAnaesthesiaTypesSyncList	Allowed	Not Allowed
AppointmentTypes	Allowed	Not Allowed
getAppointmentTypesSyncList	Allowed	Not Allowed
BookingCodes	Allowed	Not Allowed
getBookingCodesSyncList	Allowed	Not Allowed
cGovtsFYDO	Allowed	Not Allowed
CheckPractitioner	Allowed	Not Allowed
UpdatePractitioner	Allowed	Not Allowed
Clinic	Allowed	Not Allowed
getClinicAppointments	Allowed	Not Allowed
Codingdiag	Allowed	Not Allowed

Integrator detail — contact details, HMAC Secret, IP allow list and Endpoint Permissions



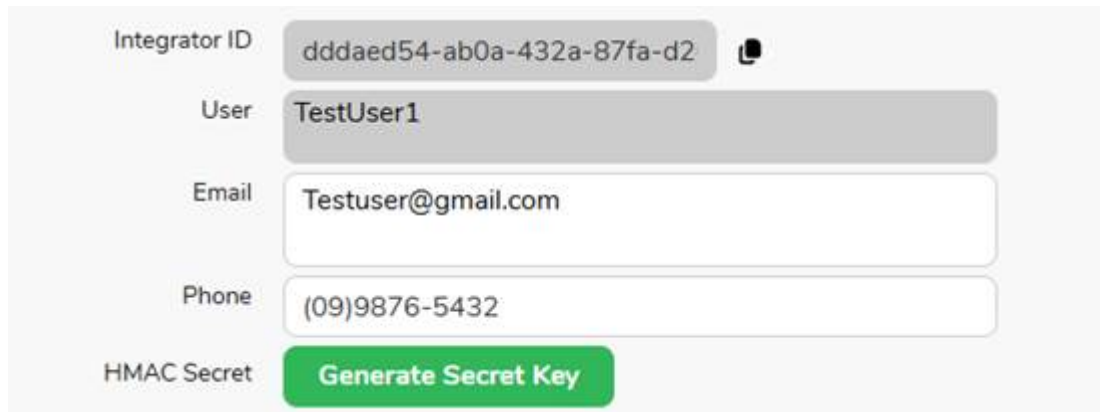
The details of each endpoint are described in the FYDO Wiki here: [FYDO API Details - FYDO Wiki](#)



The HMAC Secret Key is the new method of authenticating an API Integrator with your FYDO database. This is required along with the Integrator ID.

To create an HMAC Secret Key:

1. While editing the Integrator screen, click on the Generate Secret Key button.



Integrator ID: dddaed54-ab0a-432a-87fa-d2

User: TestUser1

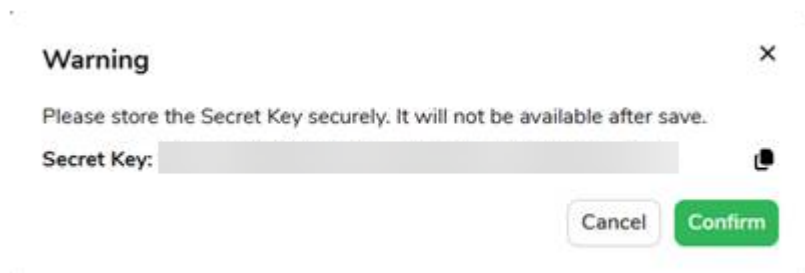
Email: Testuser@gmail.com

Phone: (09)9876-5432

HMAC Secret: [Generate Secret Key](#)

Generate Secret Key

- Click Yes to confirm.
- Click the copy button to copy the key and store it securely, then confirm to save the HMAC Key.



Warning

Please store the Secret Key securely. It will not be available after save.

Secret Key: [Redacted]

[Cancel](#) [Confirm](#)

The Secret Key is shown once — copy it before confirming



1. Edit the Integrator screen.
2. Click on the Regenerate Secret Key button, and click Yes to confirm.
3. Copy the new key and store it securely.



1. Under the Integrators list, click on the Action function
2. Click on the “Disable Access” button
3. Click on Yes to confirm
4. Once confirmed the Status will show “Inactive” for that Integrator and they will not be able to make any further API calls.

SETTINGS > INTEGRATORS

Integrator ID ↓	User	Linked Api EndPoints	Status	Action
5f7afb8-1b69-4c42-b863-c5624396a836	NewUserTest	0	Active	Edit Disable Access

10 Records/Page Page 1 of 1

Note- Under the same action function, you can re-enable an Integrator which will give them access also.