

KNOWLEDGE BASE · PUBLIC DOCUMENT

Securing n8n: access, credentials and exposed webhooks

Automation & n8n

CODE

RLX-INT-KB-2886

VERSION

v2026.10.10

COUNTRY · LANGUAGE

International · English

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

<https://www.my.mozout.com/knowledgebase/2886>



An n8n holds the keys to everything it automates: e-mail, sheets, shop, WhatsApp. Whoever gets into it **reaches all of that**. Securing n8n comes down to three fronts: **who gets into the editor**, **how the credentials are stored** and **who may call the webhooks**. On top of that, the VPS itself, which is yours.

1. Who gets into the editor

1

HTTPS only. Put n8n behind a proxy with a certificate and leave port 5678 on the server itself (127.0.0.1), as in **n8n behind HTTPS on your own domain**.

2

An owner account with a strong, unique password, and two-step verification if your version offers it. See the n8n documentation.

3

Few accounts. One per person, and remove the ones that no longer need access.

4

Limit the editor by address, if you can. You can ask the proxy to open it only from your own addresses, leaving public just the path of the production webhooks (the one starting with `/webhook/`).

2. Credentials

Rule	Why
Keep everything in n8n credentials, never typed into a node	Credentials are encrypted with the encryption key; text typed into a node is in plain view of whoever opens the workflow.
Keep N8N_ENCRYPTION_KEY off the server	It is the key to everything. See backing up n8n .
Give each credential the fewest powers	A read-only key deletes nothing if someone steals it. See API tokens: automating without handing over your password .
One credential per purpose	If one is stolen, revoke it without breaking the rest.
Spending limits on AI keys	See getting an API key for an AI model, and keeping it safe .

3. Exposed webhooks

A production webhook is an address **open to the internet**. Whoever knows it can call it. So:

1

Put authentication on the Webhook node. The node offers authentication options (for instance a header carrying a secret); see the n8n documentation and pick one.

2

Choose a path that is hard to guess and do not publish it. It does not replace authentication, but it helps.

3

Validate what arrives. Many services sign the request with a shared secret: check the signature before acting.

4

Never return sensitive data in a webhook reply.

5

Beware of nodes that run commands or code fed by data from outside. Whoever controls that data controls the command.

Executions keep the data that passed through, names, e-mails and messages included. Clear out old executions and do not keep those of sensitive workflows longer than you need to.

The VPS counts too. System updates, firewall, SSH key access: see **keeping your VPS secure: the six that matter**. And n8n itself must be updated: **updating n8n safely**.

Think someone got into your VPS? Open a ticket with what you saw.

[Open a support ticket](#)

SEE ALSO

Keeping your VPS or dedicated server secure: the six that matter
n8n webhooks: test URL and production URL
Securing Evolution API: key, HTTPS and the open port
Support Policy



Online version of this document

MozOut is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

MozOut International

RLX Holdings (Pty) Ltd. • Group RLX Holdings

TAX NO. (SARS)

943 907 6234

REGISTRATION NO.
(CIPC)

2025/667953/07

REGISTERED OFFICE

1111 Olive Street
Saint Louis 63101, Missouri, United States

CONTACT

info@mozout.com • +27 78 823 3325 • www.mozout.com

OPENING HOURS

Monday to Friday - 08 AM to 04 PM
Saturday & Sunday - Closed