Security audit

# Security audit#

You can run a security audit on your n8n instance, to detect common security issues.

## Run an audit#

You can run an audit using the CLI, the public API, or the n8n node.

### CLI#

Run n8n audit.

n8n audit

### API#

Make a POST call to the /audit endpoint. You must authenticate as the instance owner.

POST

/audit

### n8n node#

Add the n8n node to your workflow. Select Resource > Audit and Operation > Generate.

## Report contents#

The audit generates five risk reports:

### Credentials#

This report shows:

• Credentials not used in a workflow.

• Credentials not used in an active workflow.

• Credentials not use in a recently active workflow.

### Database#

This report shows:

• Expressions used in Execute Query fields in SQL nodes.

• Expressions used in Query Parameters fields in SQL nodes.

• Unused Query Parameters fields in SQL nodes.

### File system#

This report lists nodes that interact with the file system.

### Nodes#

This report shows:

• Official risky nodes. These are n8n built in nodes. You can use them to fetch and run any code on the host system, which exposes the instance to exploits. You can view the list in n8n code | Audit constants, under OFFICIAL\_RISKY\_NODE\_TYPES.

OFFICIAL\_RISKY\_NODE\_TYPES

• Community nodes.

• Custom nodes.

### Instance#

This report shows:

• Unprotected webhooks in the instance.

• Missing security settings

• If your instance is outdated.