

Audit Connector

Installation Guide

Version 0.8.0

This program runs on your own computer or server. It looks at your database, and only shares the parts you specifically choose to allow — nothing is sent anywhere until you say so. You are always in control, and you can stop sharing at any time.

This guide has one section for each type of computer. Find your computer below and follow only that section — you do not need to read the others.

Your computer	Typical use	Section
Windows	Most office and home computers	1
Mac (Apple computers)	MacBook, iMac, Mac mini, Mac Studio	2
Linux — Ubuntu or Debian	Common on cloud servers (e.g. AWS, DigitalOcean)	3
Linux — Oracle Linux, RHEL, AlmaLinux, CentOS, Rocky	Common on business servers, hospital and ERP database servers	4
Docker / Podman	For IT teams who already run everything in containers	5

After installing, everyone continues with **Finishing setup in your browser**, then **Sharing your data**. If you are replacing an earlier version, see **Upgrading from an earlier version** at the end.

NOTE: This is a 30-day free evaluation. You can start using it immediately — no payment details are needed. The program will tell you clearly, inside its own screen, how many days are left. To keep using it afterwards, enter the licence key your provider gives you (see **Licence key** near the end).

1 · Windows

For most office and home computers running Microsoft Windows

The file you need: **Windows → connector-windows-amd64-0.8.0.exe**

How to install it (you will type two short commands — copy and paste them exactly):

- 1 Open the **Windows** folder in the ZIP file you received and copy **connector-windows-amd64-0.8.0.exe** to a permanent place, for example **C:\AuditConnector**. (Create the folder if it doesn't exist.)
- 2 Open a Command Prompt **as administrator**: press the Windows key, type **cmd**, right-click **Command Prompt** and choose **Run as administrator**. Click **Yes** when Windows asks for permission.
- 3 Windows may show a blue screen that says “Windows protected your PC” the first time the program runs. This is normal for new software — click **More info**, then **Run anyway**.
- 4 Copy and paste these two lines, pressing Enter after each. They register the program as a Windows service that starts with the computer:

```
cd C:\AuditConnector
connector-windows-amd64-0.8.0.exe install -data "C:\ProgramData\AuditConnector" -listen :8443
```
- 5 Then start it:

```
connector-windows-amd64-0.8.0.exe start
```
- 6 Continue with **Finishing setup in your browser**.

Only open port 8443 in Windows Firewall if your provider told you to — with the “no firewall changes needed” relay option there is nothing to open.

To remove it later:

```
connector-windows-amd64-0.8.0.exe stop
connector-windows-amd64-0.8.0.exe uninstall
```

Your settings stay in C:\ProgramData\AuditConnector in case you install it again.

2 · Mac (Apple computers)

MacBook, iMac, Mac mini, Mac Studio

Which file do you need? Most Macs sold since 2021 use an Apple Silicon chip (M1, M2, M3 or M4). Older Macs use an Intel chip. If you are not sure, click the Apple menu (top-left corner) → About This Mac — it will say “Chip” or “Processor”.

The file you need: **macOS-AppleSilicon** folder (M1 / M2 / M3 / M4 Macs) · **macOS-Intel** folder (older Macs)

How to install it (this uses the Terminal app — you only need to copy and paste the lines below):

- 1 Open the Terminal app (press Cmd + Space, type Terminal, press Enter).
- 2 Type **cd** (with a space after it), then drag the correct macOS folder from the unzipped package into the Terminal window, and press Enter.
- 3 Copy and paste each of these lines one at a time, pressing Enter after each one. It will ask for your Mac password — type it and press Enter (the password will not appear as you type, that is normal). If you are on an Intel Mac, replace connector-darwin-arm64 with connector-darwin-amd64 in the first two lines:

```
chmod +x connector-darwin-arm64
sudo mv connector-darwin-arm64 /usr/local/bin/audit-connector
sudo xattr -d com.apple.quarantine /usr/local/bin/audit-connector
sudo audit-connector install -data /usr/local/var/audit-connector -listen :8443
sudo audit-connector start
```
- 4 Continue with **Finishing setup in your browser**.

To remove it later:

```
sudo audit-connector stop
sudo audit-connector uninstall
```

3 · Linux — Ubuntu or Debian

Common on cloud servers such as AWS, DigitalOcean, Hostinger

The file you need: **Linux-Ubuntu-Debian** → **audit-connector_0.8.0_amd64.deb** (or **_arm64.deb** on ARM servers)

How to install it (run these in your server's terminal / SSH window):

- 1 Copy the file to your server (for example with scp, or upload it through your hosting provider's file manager).
- 2 Run this one line. It installs the program and starts it running — nothing else to do:
`sudo dpkg -i audit-connector_0.8.0_amd64.deb`
- 3 If you are not using the “no firewall changes needed” relay option your provider may have set up for you, allow the connection through your server's firewall:
`sudo ufw allow 8443/tcp`
- 4 Continue with **Finishing setup in your browser**.

IMPORTANT: If the last step didn't work, or the address in “Finishing setup in your browser” doesn't load: port 8443 may already be used by something else on this server — this is common on servers that also run a control panel such as Plesk or cPanel. Install again on a different port instead (9443 is a safe choice), then use that port number in the browser address:

```
sudo audit-connector uninstall
sudo audit-connector install -data /var/lib/audit-connector -listen :9443
sudo audit-connector start
sudo ufw allow 9443/tcp
```

To remove it later:

```
sudo dpkg -r audit-connector
```

To install a newer version later, just run the `dpkg -i` command again with the new file — no need to remove the old one first.

4 · Linux — Oracle Linux, RHEL, AlmaLinux, CentOS, Rocky

Common on business servers, hospital and ERP database servers

The file you need: Linux-RHEL-AlmaLinux-CentOS → **audit-connector-0.8.0-1.el7.x86_64.rpm** for version 7 systems, ...**el9.x86_64.rpm** for version 8 and 9 (.aarch64.rpm on ARM servers)

Which file is mine? Type **cat /etc/oracle-release** (or **cat /etc/redhat-release**) in the terminal. If it says release 7.x (for example “Oracle Linux Server release 7.9”), use the **el7** file; if it says 8 or 9, use the **el9** file. Using the wrong one does no harm — it simply refuses to install with a message about “Failed dependencies”.

The server says	File to use
Oracle Linux 7.x · RHEL 7 · CentOS 7	audit-connector-0.8.0-1.el7.x86_64.rpm
Oracle Linux 8 / 9 · RHEL 8 / 9 · AlmaLinux · Rocky	audit-connector-0.8.0-1.el9.x86_64.rpm

How to install it (run these in your server's terminal / SSH window):

- 1 Copy the file to your server (for example with scp, or upload it through your hosting provider's file manager).
- 2 Run this one line (with the el7 or el9 file name from the table above). It installs the program and starts it running — nothing else to do:

```
sudo rpm -i audit-connector-0.8.0-1.el7.x86_64.rpm
```
- 3 If you are not using the “no firewall changes needed” relay option your provider may have set up for you, allow the connection through your server's firewall:

```
sudo firewall-cmd --permanent --add-port=8443/tcp
sudo firewall-cmd --reload
```
- 4 Continue with **Finishing setup in your browser**.

(Some servers manage the firewall directly with nftables instead of firewall-cmd — if the command above says “command not found”, ask whoever manages the server to open the port for you. The el7 package was verified on Oracle Linux Server 7.9; the el9 package on AlmaLinux 9.)

IMPORTANT: If the last step didn't work, or the address in “Finishing setup in your browser” doesn't load: port 8443 may already be used by something else on this server — this is common on servers that also run a control panel such as Plesk or cPanel. Install again on a different port instead (9443 is a safe choice), then use that port number in the browser address:

```
sudo audit-connector uninstall
sudo audit-connector install -data /var/lib/audit-connector -listen :9443
sudo audit-connector start
sudo firewall-cmd --permanent --add-port=9443/tcp && sudo firewall-cmd --reload
```

To remove it later:

```
sudo rpm -e audit-connector
```

To install a newer version later, use rpm -U with the new file — no need to remove the old one first.

5 · Docker / Podman

For IT teams who already run their systems in containers

The file you need: **Docker → audit-connector-docker-0.8.0.tar.gz**

How to run it:

- 1 Load the image:

```
docker load < audit-connector-docker-0.8.0.tar.gz
```
- 2 Start it. The -v part keeps your settings safe even if the container restarts:

```
docker run -d --name audit-connector \  
-p 8443:8443 \  
-v audit_connector_data:/data \  
audit-connector:0.8.0
```
- 3 Continue with **Finishing setup in your browser**, using this server's address instead of "localhost".

IMPORTANT: If port 8443 is already used by something else on this server (common alongside a control panel like Plesk or cPanel), just change the first 8443 above to a free port instead, e.g. -p 9443:8443 — no need to change anything inside the container. Then use that port number in the browser address.

To stop it later:

```
docker rm -f audit-connector
```

Finishing setup in your browser

The same for every type of computer — do this last

- 1** Open your web browser (Chrome, Edge, Firefox, or Safari) and go to this address: **https://localhost:8443/admin/**
If you installed this on a separate server rather than the computer you are sitting at, use that server's address instead of "localhost" — your provider will tell you what it is. If you switched to port 9443 during installation, use 9443 here too — e.g. **https://your-server-address:9443/admin/**.
- 2** Your browser will warn that the connection "is not private" or "isn't secure". This is expected and nothing to worry about — it happens because the program made its own security certificate for you. Click **Advanced**, then **Proceed** (the exact wording differs slightly by browser).
- 3** You will see a Welcome page. Type your company or organisation name, choose an administrator password (write it down somewhere safe — at least 10 characters), and click **Create administrator**.
- 4** You're in. Across the top of the page you'll see tabs: **Connections**, **Datasets**, **Procedures**, **API keys**, **Audit log**, and **Settings**. Your provider will guide you through which database to connect and what to share.

NOTE: You are always in control. Nothing is shared until you specifically approve it on the Datasets or Procedures tab, and you can pause everything instantly from Settings at any time.

IMPORTANT: This copy is a 30-day free evaluation. The days remaining are always shown at the top of the page in the final week, so there are no surprises.

Sharing your data and creating an API key

What to do after setup — with screenshots of the actual screens

This is the part your provider will usually walk you through, but here is exactly what it looks like so you know what to expect. Nothing here shares any data until you reach the last step.

1. Choose what to share (the Datasets tab)

On the Datasets tab, click **Expose a dataset**, pick a table from your database, and tick the columns you're comfortable sharing. Nothing outside this list can ever be seen by your provider — it's a whitelist, not a filter.

Datasets
Only what is listed here is reachable by the audit application — nothing else exists from its point of view. Most datasets should stay **read only**; turn on insert/update only where you intend it.

Expose a dataset

DATASET	ENTITY	SOURCE	COLUMNS	ROW FILTER	RIGHTS	INCREMENTAL	STATUS	
products	Inventory	ERP Production > dbo.demo_products	5	—	read + insert + update	—	exposed	<button>Edit</button> <button>Remove</button>

A dataset once created. The “Rights” column shows exactly what it allows — here, read, insert and update.

2. Decide if your provider may also add or change data

By default, sharing is read-only — your provider can only look. If they need to write something back (for example, marking an item as reviewed), open the dataset's **Rights** tab and turn on **Insert** and/or **Update** for that one table only. You'll also be shown the exact database permission to grant, so nothing happens without your knowledge.

Edit dataset products

1 · Source 2 · Columns & masking 3 · Rules 4 · Rights 5 · Preview

Read (SELECT) — always allowed

Insert and update are off by default. Turning either on lets any API key you separately grant write access to change data in this table — through only the columns you approved above.

☒ Allow inserting new rows (INSERT)

☒ Allow updating existing rows (UPDATE)

Match column — identifies the one row to change (usually the primary key). Every update must target exactly one row.

id

Grant this on the database user, for this table only

```
-- Run as db_owner or higher, in the target database.  
GRANT INSERT ON demo_products TO audit_reader;  
GRANT UPDATE ON demo_products TO audit_reader;
```

Turning on Insert/Update for one table. Read access is always on and cannot be turned off; write access is opt-in, per table.

Two optional fields on the same tab (new in 0.7.0), only needed if your provider asks for them: **Sequences an insert may draw from** — lets the database itself assign the next number for new records (e.g. an order number), so your provider never has to guess one; and **Columns returned after an insert** — lets your provider see the number that was assigned. Both apply to this one table only.

One more optional field, on the **Rules** tab (new in 0.8.0), only needed if your provider asks for it: **File store folder** — if this table's records point at documents kept in a folder on this server (scanned invoices, contract PDFs), enter that folder here and your provider can fetch those documents read-only. Nothing outside the folder you enter can ever be read, and every fetch appears in your audit log like any other request.

3. Letting your provider use one of your own database procedures (the Procedures tab) — new in 0.7.0

Some records must be created by a procedure that already exists in your database, because that procedure applies your own rules (numbering, checks, several tables filled together). Rather than giving write access to those tables, you can approve the **procedure** instead: your provider can then only call it, with only the values you allow. Go to **Procedures**, click **Approve a procedure**, and fill in:

Field	What to enter
Public name	A short name your provider will use, e.g. post_order
Connection · Schema · Package · Procedure	Where the procedure lives in your database (your provider or DBA will tell you; Package only applies to Oracle)
Parameters	One row per value the procedure takes, in its own order — name, type, whether it is an input or an output, whether it is required
Callable	Untick at any time to pause it without deleting it

A call that passes anything you did not list is refused and recorded in the Audit log, together with every accepted call and what it returned.

4. Create the API key (the API keys tab)

Go to the API keys tab and click **Create key**. Give it a name so you remember who it's for, tick the dataset(s) it may read, and — only if you want this particular key to be able to write, not just read — tick **also write** next to that dataset as well. If you approved procedures, tick the ones this key may call under **Procedures this key may call**.

Create API key

Name (who holds it)

Expires

Requests per minute

Max rows per page

Audit Application — production

09/19/2027

120

1000

Allowed caller IPs (comma-separated
IPs/CIDRs, blank = any)

203.0.113.10, 198.51.100.0/24

Datasets this key may read

1 of 1 selected

The key can only ever reach what is ticked here. Everything else answers 403 — it cannot even see that other datasets exist. For any dataset with insert/update turned on, you can also grant this key write access to it.

☒ products Inventory

☒ also write
(insert+update)

☐ All exposed datasets — including any you expose in future. Only for a fully-trusted consumer.

Creating a key scoped to one dataset, with write access ticked on for it specifically.

5. Copy the key — you won't see it again

The key is shown once. Copy it (or use the **Copy all details for email** button) and send it to whoever asked you for access. If you ever lose it or want to stop using it, come back to this tab and click **Revoke** — access stops immediately.

Key created — Audit Application — production

Give this key to the audit application. It is stored encrypted on this server; an administrator can show it again from the API keys tab.

3 · API key

```
ac_frBNld8_2yKqtyT8ZvMpG-Ceq6YUptZ91WB3YYpK19c
```

The key, shown exactly once at creation time.

6. Manage it any time

Every key you've created is listed on the API keys tab, showing which datasets it can reach, whether it can write to any of them and which procedures it may call. You can pause, edit or revoke any key here whenever you want, with no need to involve your provider.

NAME	KEY	DATASETS	EXPIRES	RATE / PAGE	IP ALLOW	LAST USED	STATUS				
Audit Application — production	ac_frBNld8_2...	products	2027-09-19	120/min · 1000	any	—	active	Show key	Pause	Edit	Revoke
		write									
								Delete			

The API keys list — a “write” label appears next to any dataset a key can also change.

Licence key

What happens after the 30-day evaluation

When the evaluation ends, the program stops answering requests until a licence key is entered — your settings, connections and keys are kept. Your provider issues the licence key for your organisation; it may be perpetual or for a fixed term.

- 1 Open the admin page and go to **Settings** → **Evaluation license**. (This page stays reachable even after the evaluation has expired.)
- 2 Paste the key you received — it starts with **AC-LIC-** — and click **Activate**.
- 3 The banner at the top of the page disappears and Settings shows who the licence is issued to. The check is done on your own computer; no internet connection is needed.

Upgrading from an earlier version

If Audit Connector 0.5.0 or 0.6.0 is already installed

Your computer	What to do
Windows	Stop the old service (Settings → Apps → Audit Connector → Uninstall, or audit-connector stop then uninstall in an administrator Command Prompt), then follow section 1 with the new executable. Your settings in C:\ProgramData\AuditConnector are kept.
Mac	Run the five lines of section 2 again with the new file; the install command reuses your existing data folder.
Ubuntu / Debian	sudo dpkg -i audit-connector_0.8.0_amd64.deb — the service restarts on the new version by itself.
Oracle Linux / RHEL family	sudo rpm -U audit-connector-0.8.0-1.el7.x86_64.rpm (version 7) or ...el9.x86_64.rpm (version 8/9)
Docker	docker rm -f audit-connector , load the new image, run the same docker run line with audit-connector:0.8.0 — the -v volume keeps your settings.

Everything you configured — connections, datasets, API keys and the audit log — is kept. After the upgrade the admin page shows the new **Procedures** tab and the extra fields described above.

Need help?

If anything on this page doesn't match what you see, or you get stuck at any step, contact whoever gave you this guide and let them know which numbered step you were on.