CUSTOMER GUIDE · DBENK CLOUD COMING SOON

AutoOps Cloud without a Worker: conditions and risks

When the direct-SSH option may be used, its risks, who is responsible for what, the required setup, and the agreement text you tick.

Public VPS
the only place this option may be used

IP allowlist
SSH port for DBenk IPs only

Agreement required
ticked and recorded with its time

In short

Without a Worker is for public VPS only. The SSH key is stored encrypted at DBenk, the SSH port is open to DBenk's IPs only, and you must tick an agreement that is recorded with its time. For servers on an office network, use a DBenk Worker.

Status today

DBenk Cloud and DBenk AutoOps Cloud are **coming soon**: not for sale yet. This guide describes the designed behaviour so your IT team can assess and prepare for it. AVAILABLE means usable today; DESIGNED means it opens together with Cloud.

VERSION
1.0 · 4 November 2026

FOR
Decision makers and IT teams

LATEST VERSION
lisensi.dbenk.com/panduan

CONTENTS

Table of contents

01 When it is allowed 3
public VPS only

02 Risks 4
what differs from a Worker

03 Shared responsibility 5
DBenk and customer

04 Required setup 6
user, key, allowlist, sshd

05 Keys and incidents 7
rotation, revocation, incidents

06 Agreement text 8
identical to the form

All DBenk Cloud guides

- DBenk Worker guide for AutoOps Cloud
- AutoOps Cloud without a Worker: conditions and risks
- DBenk Cloud: what is included

The latest version is always at **lisensi.dbenk.com/panduan**. Prices and the agreement text in this guide come from the same source as the dbenk.com pricing page.

01 WHEN IT IS ALLOWED

When AutoOps Cloud may run without a Worker

The default for AutoOps Cloud is a DBenk Worker in your network. Running without one is an exception with strict conditions.

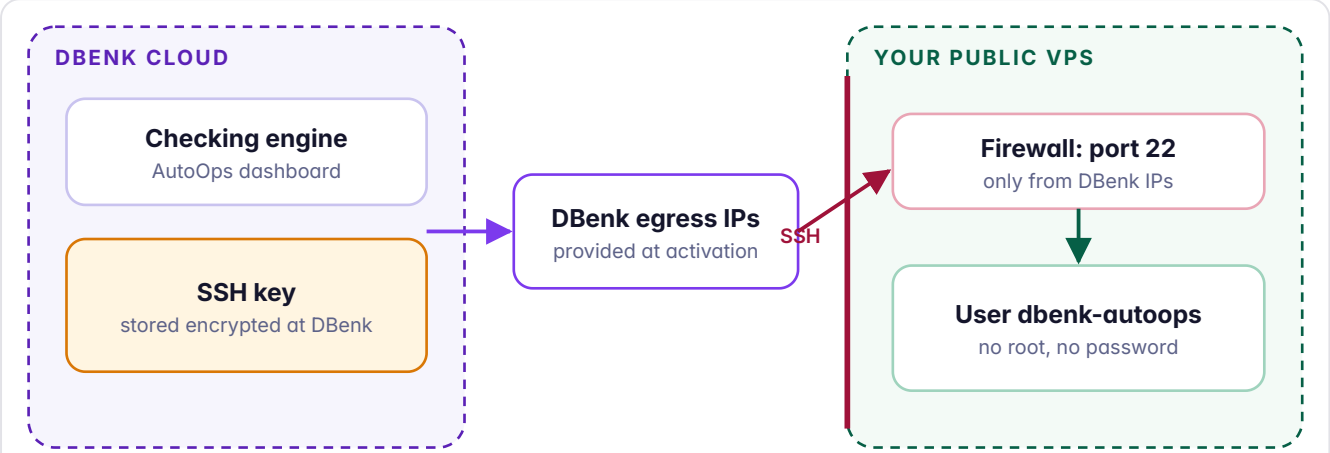


Figure 1. Without a Worker, the checking engine in the DBenk cloud connects over SSH directly to your public VPS from DBenk's egress IP addresses. The SSH key is stored encrypted at DBenk, and the VPS firewall only accepts port 22 from those addresses.

Allowed

- Public VPS (servers with a public IP at a cloud/hosting provider) that are reachable from the internet anyway.
- You can set a firewall or security group that restricts the SSH port per IP address.
- You can create a dedicated non-root SSH user on every VPS.

Not allowed

- Servers on an office network, LAN or behind NAT: use the DBenk Worker.
- Opening the SSH port to the whole internet so DBenk can get in.
- Using root or a key that other people or systems also use.

You choose this option in the DBenk Cloud access form, and it only applies after you tick the agreement on page 8. Its text, version, fingerprint (sha256) and time are stored with your request and recorded on your customer record in the DBenk Konsol.

02 RISKS

The risks you need to accept

This is not the way we recommend. This list explains what differs from using a DBenk Worker.

RISK	WHAT IT MEANS	MITIGATION
SSH key outside your network	The private key for your VPS is stored at DBenk (encrypted). If DBenk's systems were breached, that key would be at risk.	Per-customer key, encrypted, used only by the checking engine; minimum-rights user; rotation and revocation (page 7).
SSH port open to the internet	The VPS port 22 must accept connections from DBenk's IP addresses. A firewall mistake can open it to everyone.	IP allowlist, key-only login, `AllowUsers`, fail2ban or similar.
Dependency on DBenk's IPs	If DBenk's egress IPs change, your firewall rules need updating.	Changes are announced in advance by e-mail; old addresses keep working during a transition period.
Misuse of rights	Whoever holds the key can use the rights of the user `dbenk-autoops`.	No root, no sudo by default; changing actions only where you allow them per server; every action is logged.
Path over the internet	SSH traffic crosses the public internet, not an internal network.	SSH is encrypted; the host fingerprint is pinned from the first connection, and changes are refused until you confirm.

Safer: use a DBenk Worker

A Worker needs no inbound port and the SSH keys stay in your network. When you have one always-on Linux server, switch to a Worker at any time; the guide: DBenk Worker guide for AutoOps Cloud.

03 RESPONSIBILITY

Shared responsibility matrix

Who looks after what when AutoOps Cloud connects directly to your VPS.

RESPONSIBILITY	DBENK	CUSTOMER
Security of the SSH key stored at DBenk (encryption, access, logging)	●	—
Security of the checking engine and DBenk egress IPs	●	—
Telling you about any incident involving your key	●	—
Announcing egress IP changes in advance	●	—
Creating and restricting the `dbenk-autoops` user	—	●
Firewall/security group: SSH port for DBenk IPs only	—	●
OS and SSH security updates on the VPS	—	●
Deciding which changing actions are allowed per server	—	●
Revoking access (removing the public key) when needed	—	●
Deleting the stored key on request or when the subscription ends	●	—
Keeping the record of this agreement	●	●

● = responsible. This split is the same as point (4) of the agreement text.

04 SETUP

Required setup

Do this on every VPS before adding it to AutoOps Cloud.

1 Dedicated minimum-rights SSH user

```
sudo useradd --create-home --shell /bin/bash dbenk-autoops
sudo passwd --lock dbenk-autoops
sudo install -d -m 700 -o dbenk-autoops -g dbenk-autoops /home/dbenk-autoops/.ssh
```

2 DBenk's public key, restricted

The public key made for you appears in the dashboard after activation. Add it with restrictions so it only works from DBenk's addresses and without forwarding:

```
from="<IP-DBenk-1>,<IP-DBenk-2>",no-agent-forwarding,no-port-forwarding,no-X11-forwarding
ssh-ed25519 AAAA… dbenk-autoops-cloud
```

Save it in `/home/dbenk-autoops/.ssh/authorized_keys` (600, owned by `dbenk-autoops`).

3 IP allowlist

DBenk egress IP addresses: **provided at activation**. Allow the SSH port only from those addresses, on the VPS firewall and in the provider's security group if there is one:

```
sudo ufw allow from <IP-DBenk-1> to any port 22 proto tcp
sudo ufw allow from <IP-DBenk-2> to any port 22 proto tcp
# keep your own admin access before closing anything else
```

4 Harden sshd

```
# /etc/ssh/sshd_config.d/dbenk.conf
PasswordAuthentication no
PermitRootLogin no
AllowUsers dbenk-autoops <your-admin>
# then: sudo sshd -t && sudo systemctl reload ssh
```

05 KEYS AND INCIDENTS

Rotation, revocation and incident handling

Key rotation

1. Request a new key in the dashboard (**Servers › Key › Create new key**) or through support.
2. Add the new public key on every VPS, next to the old one.
3. Press **Test connection**; once all pass, remove the old key from the VPS.
4. The old key is deleted from DBenk's storage and recorded in the history.

We recommend rotating every 90 days and right after anyone with admin access leaves the team.

Revoking access

- **Immediately, by you:** remove DBenk's key line from `authorized_keys`, or close the firewall rule for DBenk's IPs.
- **Deletion at DBenk:** request it in the dashboard or through support; the stored key is deleted and you get a written confirmation.
- When the subscription ends, the stored key is deleted.

If there is an incident

SITUATION	WHAT YOU DO	WHAT DBENK DOES
You suspect a VPS is compromised	Remove DBenk's key and close the SSH port; secure the VPS; tell us.	Stops checks to that VPS, sends the history of AutoOps actions on it for your investigation, creates a new key on request.
Incident at DBenk	Follow the notice; remove the key if asked.	Disables the affected keys, tells you without delay, explains what was affected, and issues new keys.
Unexpected action in the log	Report the time and the server.	Matches it against the AutoOps audit log and explains where the action came from.

06 AGREEMENT

Agreement text

This text is exactly the one you tick in the access form. If it changes, its version goes up and the agreement has to be given again.

> I choose DBenk AutoOps Cloud WITHOUT a DBenk Worker for my public VPS servers and understand the conditions: (1) the SSH key for these servers is stored encrypted at DBenk and used only by the AutoOps checking engine; (2) the SSH port of my servers is open to DBenk's outbound IP addresses (provided at activation) and I restrict access to those addresses only; (3) I create a dedicated SSH user with minimum rights (not root), and changes only run where I allow them per server; (4) DBenk is responsible for the security of the key and the checking engine in DBenk's cloud, I am responsible for my servers, users and firewall; (5) I can revoke access at any time by removing DBenk's public key from the servers and asking DBenk to delete the key.

Version	`autoops-ssh-langsung/1`
Text fingerprint (sha256)	`8933256a8e5f100ad5c874c42c223cde23b78b7ba0f902d39220a478e11c5ffc`
What is recorded	the text and its language, version, fingerprint, time ticked, name, e-mail and company; stored with the request and on the customer record in the DBenk Konsol
Withdrawing	switch to a DBenk Worker or stop monitoring that VPS; the stored key is deleted

The fingerprint is computed from the text above (UTF-8), so anyone can check that the agreed text has not changed.