SalesDesk Installations- und Betriebsanleitung (Firmenserver)

Für die IT: Firmenserver installieren, absichern, aktualisieren, sichern, wiederherstellen und Fehler beheben.

Stand: App 1.13.0, Server 0.22.0, 02.11.2026

Ingenieur-Kontor-Sottrum GmbH · salesdesk-app.iks-solutions.com

Inhalt

Vorbereitung

Überblick und Voraussetzungen

Vorbereitung – DNS und SSH

Installation

Installation Schritt für Schritt

Webserver und HTTPS – mit oder ohne Plesk

Windows Server (Hyper-V)

Erste Einrichtung im Browser

E-Mail-Versand und Microsoft 365

Betrieb

Updates einspielen

Datensicherung und Wiederherstellung

Betrieb, Wartung und Sicherheit

Fehlersuche und Fragen

Fehlersuche

Fragen der IT

Überblick und Voraussetzungen

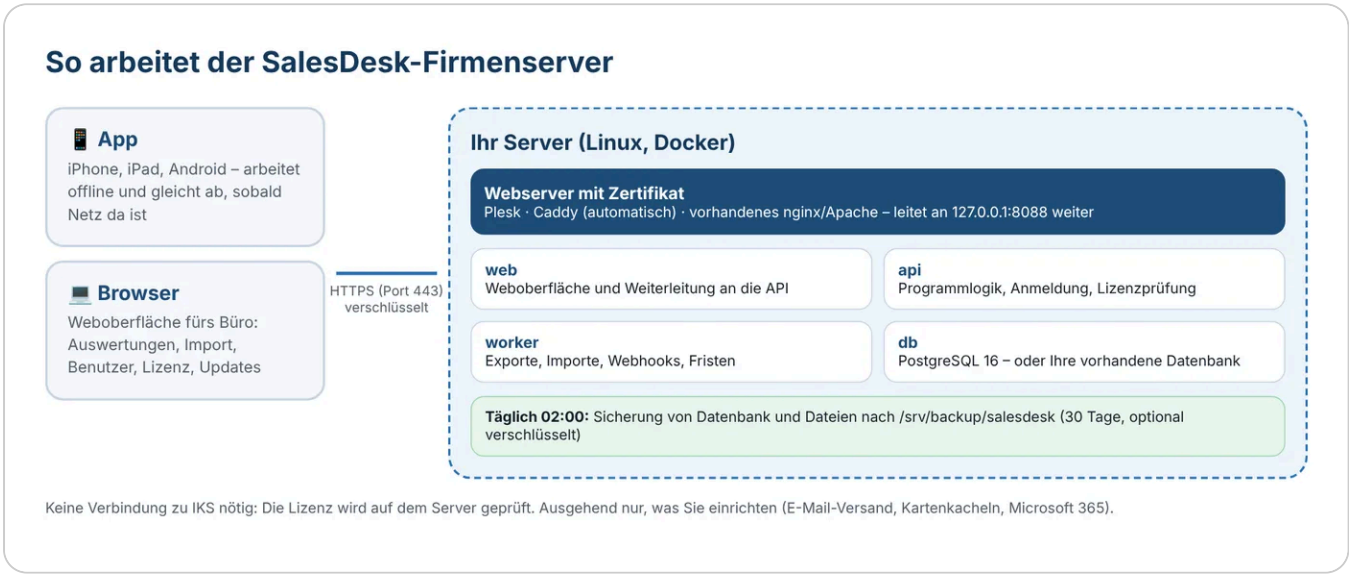
Was installiert wird, welcher Server passt, was Sie vorher brauchen und wie lange es dauert.

Diese Anleitung richtet sich an die Person, die den SalesDesk-Firmenserver installiert und betreut, meist die IT oder ein Dienstleister. Für die tägliche Arbeit mit App und Weboberfläche gibt es die Bedienungsanleitung.

> Sie brauchen keinen eigenen Server? Die **SalesDesk Cloud** bietet denselben Funktionsumfang, betrieben von IKS in Deutschland. Dann brauchen Sie diese Anleitung nicht, siehe Bedienungsanleitung, Kapitel „SalesDesk Cloud“.

Was wird installiert?

Der Firmenserver ist eine fertige Software-Ausstattung aus vier Docker-Containern. Sie wird mit **einer Installationsdatei** eingerichtet, die alles Nötige erledigt: Docker installieren, Programm bauen und starten, Datenbank anlegen, ersten Administrator anlegen, HTTPS einrichten, tägliche Sicherung und Update-Dienst einrichten.



Aufbau: App und Browser verbinden sich über HTTPS mit dem Webserver auf Ihrem Server, der an die SalesDesk-Container web, api, worker und db weiterleitet

Teil	Aufgabe
web	liefert die Weboberfläche aus und leitet Anfragen an die API weiter. Lauscht nur lokal auf `127.0.0.1:8088`.
api	die eigentliche Programmlogik: Anmeldung, Rechte, Abgleich mit der App, Lizenzprüfung
worker	arbeitet im Hintergrund: Exporte, Importe, Webhooks, Aufbewahrungsfristen
db	PostgreSQL 16 mit allen Daten. Alternativ nutzen Sie Ihren vorhandenen PostgreSQL-Server (ab Version 14).
Webserver	nimmt HTTPS-Verbindungen von außen an und hat das Zertifikat: Plesk, Caddy (richtet die Installation selbst ein) oder Ihr vorhandenes nginx/Apache

Welcher Installationsweg passt?



Vier Wege: Linux mit Plesk, Linux ohne Plesk, Linux mit vorhandenem nginx oder Apache, Windows Server über eine Linux-VM

Ihr Server	Weg	Aufwand
Linux-Server mit **Plesk**	Installationsdatei starten, alles Weitere automatisch	ca. 20 Minuten
Linux-Server **ohne Plesk**, Ports 80/443 frei	Installationsdatei starten, bei „HTTPS jetzt automatisch einrichten?“ **j**	ca. 20 Minuten
Linux-Server mit **vorhandenem nginx oder Apache**	Installationsdatei starten, fertige Konfiguration einfügen, Zertifikat mit certbot	ca. 30 Minuten
Windows Server (2019, 2022, 2025)	Linux-VM im Hyper-V anlegen, darin wie „ohne Plesk“	ca. 60 Minuten
Mietserver/VM in der Cloud (Azure, AWS, Hetzner Cloud …)	wie „ohne Plesk“ – Ubuntu 24.04 wählen	ca. 20 Minuten

Alle Wege nutzen **dieselbe Installationsdatei** und führen zum selben Ergebnis. Die Kapitel Webserver und HTTPS und Windows Server beschreiben die Unterschiede.

Voraussetzungen

Was	Mindestens	Empfohlen
Betriebssystem	Ubuntu 22.04, Debian 12, AlmaLinux 9 oder Rocky Linux 9 (64 Bit, x86_64)	**Ubuntu 24.04 LTS**
Prozessor	2 vCPU	4 vCPU
Arbeitsspeicher	4 GB	8 GB
Festplatte	40 GB SSD	80 GB SSD, dazu Platz für Sicherungen
Zugang	**root** oder ein Benutzer mit `sudo`, per SSH	SSH mit Schlüssel statt Passwort
Netzwerk	eingehend Port **80** und **443** aus dem Internet; ausgehend HTTPS (für Docker-Images und Zertifikat)	feste öffentliche IP-Adresse
Adresse	eine (Sub-)Domain, z. B. `salesdesk.ihre-firma.de`, mit **DNS-A-Eintrag** auf die IP des Servers	eigene Subdomain nur für SalesDesk

⚠ Ein **reines Webhosting-Paket** (nur PHP/FTP, kein Root-Zugang) genügt nicht. Sie brauchen einen V-Server, Root-Server, eine VM oder einen eigenen Rechner, auf dem Sie Programme installieren dürfen.

Wie viele Nutzer schafft welcher Server?

Nutzer	Server
bis 10	2 vCPU, 4 GB RAM, 40 GB
bis 50	4 vCPU, 8 GB RAM, 80 GB
über 50	8 vCPU, 16 GB RAM, 160 GB oder eigene Datenbank

Der Speicherbedarf wächst vor allem mit Fotos und Anhängen (Besuchsfotos, Visitenkarten, Dokumente). Rechnen Sie grob mit 1 GB je Nutzer und Jahr.

Was Sie vorher bereitlegen

1. **Zugangsdaten zum Server**: IP-Adresse, Benutzername (meist `root` und Passwort oder SSH-Schlüssel – vom Hoster oder Ihrer IT.
2. **Zugang zur DNS-Verwaltung Ihrer Domain** (beim Domain-Anbieter oder in Plesk), um einen A-Eintrag anzulegen.
3. **Die Adresse**, unter der SalesDesk erreichbar sein soll, z. B. `salesdesk.ihre-firma.de`.
4. **Ihre E-Mail-Adresse** für den ersten Administrator und das HTTPS-Zertifikat.
5. Optional: **Zugangsdaten für den E-Mail-Versand** (SMTP-Postfach oder Microsoft 365), damit „Passwort vergessen“ und Follow-up-Mails funktionieren. Das geht auch später, siehe E-Mail-Versand.
6. Einen **Passwort-Tresor** (z. B. KeePass, Bitwarden), um die Geheimnisse des Servers sicher aufzubewahren.

Zeitplan

Schritt	Dauer
DNS-Eintrag anlegen und warten, bis er gilt	5 Minuten bis einige Stunden
Installationsdatei laden und starten	2 Minuten
Fragen beantworten	3 Minuten
Docker installieren, SalesDesk bauen und starten	5–15 Minuten (beim ersten Mal)
Erste Einrichtung im Browser	15 Minuten

Lizenz

Nach der Installation läuft der Server **30 Tage mit allen Funktionen** zum Testen, ohne Kauf und ohne Registrierung. Danach brauchen Sie eine Lizenz:

- **Team-Server-Abo** in der SalesDesk-App (App Store bzw. Google Play), monatlich, für 5, 10 oder 25 Nutzer. Wer kauft, meldet sich danach mit der App als Administrator am Server an – das Abo wird automatisch übertragen.

- **Jahresvertrag per Rechnung** direkt bei IKS: Sie erhalten eine Lizenzdatei und laden sie in der Weboberfläche unter **Verwaltung › Lizenz** hoch, siehe Jahresvertrag.

Gezählt werden **benannte Benutzer**: Jedes aktive Benutzerkonto belegt einen Platz, auch der Administrator. Wie viele Geräte jemand nutzt oder ob er gerade angemeldet ist, spielt keine Rolle. Die Lizenz wird auf Ihrem Server geprüft – **ohne Verbindung zu IKS**.

Vorbereitung – DNS und SSH

DNS-Eintrag anlegen und prüfen, per SSH von Windows oder Mac auf den Server, Dateien übertragen.

1. DNS-Eintrag anlegen

SalesDesk braucht eine eigene Adresse, z. B. `salesdesk.ihre-firma.de`. Damit die Adresse auf Ihren Server zeigt, legen Sie bei Ihrem Domain-Anbieter (oder in Plesk unter **Websites & Domains › DNS-Einstellungen** einen **A-Eintrag** an:

Feld	Eintrag
Typ	`A`
Name / Host	`salesdesk` (nur der vordere Teil; manche Anbieter wollen den vollen Namen `salesdesk.ihre-firma.de`)
Wert / Ziel	die **öffentliche IPv4-Adresse** Ihres Servers, z. B. `203.0.113.25`
TTL	Standard (z. B. 3600)

Hat Ihr Server auch eine IPv6-Adresse, legen Sie zusätzlich einen `AAAA`-Eintrag mit dieser Adresse an. Haben Sie **keine** IPv6 am Server, darf es auch **keinen** AAAA-Eintrag für diese Adresse geben – sonst schlägt das Zertifikat fehl.

Prüfen, ob der Eintrag gilt

Unter Windows (PowerShell oder Eingabeaufforderung), Mac oder Linux:

```
nslookup salesdesk.ihre-firma.de
```

Richtig ist es, wenn unter **Address** die IP Ihres Servers steht:

```
Nicht autorisierte Antwort:
Name:    salesdesk.ihre-firma.de
Address: 203.0.113.25
```

Steht dort „Non-existent domain“ oder eine andere IP, warten Sie noch. Neue Einträge gelten meist nach wenigen Minuten, manchmal erst nach einigen Stunden.

> Sie können mit der Installation schon beginnen, während der DNS-Eintrag noch nicht gilt. Nur das Zertifikat kommt dann später – die Installation sagt Ihnen, was zu tun ist.

2. Mit dem Server verbinden (SSH)

Die Installation läuft im **Terminal des Servers**. Sie verbinden sich dorthin per SSH. Das Programm dafür ist in Windows 10/11, macOS und Linux bereits enthalten.

Unter Windows

1. Drücken Sie die **Windows-Taste**, tippen Sie `PowerShell` und öffnen Sie **Windows PowerShell** (normale Rechte genügen).
2. Geben Sie ein (IP-Adresse Ihres Servers einsetzen):

```
ssh root@203.0.113.25
```

3. Beim **ersten** Verbinden fragt Windows, ob Sie dem Server vertrauen:

```
The authenticity of host '203.0.113.25' can't be established.
ED25519 key fingerprint is SHA256:...
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Tippen Sie `yes` und drücken Sie **Enter**.

4. Geben Sie das **Passwort** ein. Beim Tippen erscheinen **keine Zeichen und keine Sternchen** – das ist richtig so. Mit **Enter** bestätigen.
5. Sie sind verbunden, wenn die Eingabezeile mit `root@…` beginnt, z. B. `[root@server ~]#` oder `root@server:~#`.

> **Einfügen** in PowerShell und im Terminal: **rechte Maustaste** oder **Strg+V**. Kopieren Sie Befehle aus dieser Anleitung mit dem Knopf **Kopieren** neben dem Befehl. Geben Sie mehrere Befehle **nacheinander** ein und warten Sie jeweils, bis die Eingabezeile wieder erscheint.

> Verbinden Sie sich mit der **IP-Adresse** des Servers, nicht mit dem Domainnamen. Manche Hoster leiten den Domainnamen über einen anderen Dienst; dann bricht die Verbindung mit „Connection closed“ ab.

Unter macOS und Linux

Öffnen Sie **Terminal** (macOS: Programme › Dienstprogramme) und geben Sie denselben Befehl `ssh root@203.0.113.25` ein.

Kein root, sondern ein eigener Benutzer?

Viele Server (z. B. Ubuntu in der Cloud) lassen sich nur mit einem normalen Benutzer anmelden. Dann verbinden Sie sich mit diesem Benutzer und wechseln zu root:

```
ssh benutzername@203.0.113.25
sudo -i
```

Zwei Fenster: Ihr PC und der Server

Merken Sie sich, **wo** ein Befehl hingehört:

Fenster	erkennbar an	wofür
PowerShell auf Ihrem PC	`PS C:\Users\Name>`	`ssh`, `scp`, `nslookup`
Terminal auf dem Server	`root@server:~#` bzw. `[root@server ~]#`	alle Befehle der Installation

Mit `exit` verlassen Sie den Server und sind wieder auf Ihrem PC.

3. Dateien übertragen (nur falls nötig)

Normalerweise lädt der Server die Installationsdatei selbst aus dem Internet (nächstes Kapitel). Hat der Server keinen Internetzugang zur Webseite oder möchten Sie eine Datei von Ihrem PC hochladen, nutzen Sie `scp` **in PowerShell auf Ihrem PC** (nicht auf dem Server):

```
scp $env:USERPROFILE\Downloads\salesdesk-installer-latest.sh root@203.0.113.25:/root/
```

Alternativ mit dem kostenlosen Programm **WinSCP**: Neue Sitzung, Protokoll **SFTP**, Rechnername = IP, Benutzer `root`, Passwort – dann die Datei per Ziehen nach `/root/` kopieren.

4. Firewall und Ports

Von außen müssen **Port 80** (für das Zertifikat) und **Port 443** (für SalesDesk) erreichbar sein. Port 22 brauchen Sie für SSH.

- Die **Firewall auf dem Server** (firewalld oder ufw) öffnet die Installation selbst, wenn sie Caddy einrichtet. Plesk regelt das selbst.
- Viele Hoster haben **zusätzlich eine Firewall im Kundenmenü** (z. B. „Firewall“, „Sicherheitsgruppen“, „Netzwerk-Regeln“). Dort müssen eingehend TCP 80 und 443 erlaubt sein.
- Steht der Server in Ihrem Firmennetz, muss der **Router bzw. die Firmen-Firewall** Port 80 und 443 an den Server weiterleiten (Portweiterleitung / NAT).

Installation Schritt für Schritt

Installationsdatei laden und prüfen, starten, alle Fragen beantworten – mit der Ausgabe, die Sie bei jedem Schritt sehen.

1. Installationsdatei laden und prüfen

Melden Sie sich per SSH am Server an (siehe Vorbereitung und geben Sie im **Terminal des Servers** ein:

```
cd /root
curl -fLO https://salesdesk-app.iks-solutions.com/download/files/salesdesk-installer-latest.sh
```

Die Datei ist rund 11 MB groß. Prüfen Sie danach, ob sie unverändert ist. Die **Prüfsumme** (SHA-256) der aktuellen Version steht im Download-Bereich:

```
sha256sum salesdesk-installer-latest.sh
```

Die angezeigte Zeichenfolge muss **genau** mit der Prüfsumme auf der Webseite übereinstimmen. Weicht sie ab, laden Sie die Datei erneut und starten sie nicht.

> Im Download-Bereich steht ein fertiger Block mit Laden, Prüfen und Starten für die jeweils aktuelle Version. Mit **Befehle kopieren** übernehmen Sie ihn in einem Schritt.

2. Installation starten

```
sudo bash salesdesk-installer-latest.sh
```

Sie sehen zuerst:

```
SalesDesk 0.22.0 entpackt – Installation startet ...
SalesDesk-Installation 2026-11-02T10:15:00+01:00 – Instanz salesdesk in /opt/salesdesk, Port 8088
Es gelten die Lizenzbedingungen für den SalesDesk-Firmenserver:
  https://salesdesk-app.iks-solutions.com/lizenzbedingungen/
Ohne Lizenz läuft der Server 30 Tage zum Testen. Open-Source-Hinweise: THIRD-PARTY-NOTICES.txt
```

Die Installation läuft in acht Schritten. Alles, was sie ausgibt, steht zusätzlich im Protokoll `/var/log/salesdesk-install.log`.

> ⚠ Lassen Sie das Fenster offen, bis **FERTIG** oder eine rote Meldung erscheint. Bricht die SSH-Verbindung ab, starten Sie die Installation erneut; sie erkennt den Stand und macht weiter (ohne erneut zu fragen). Fehlt danach noch der Administrator, zeigt sie den Befehl `create-org` zum Anlegen. Tipp für langsame Verbindungen: die Installation in `screen` starten `apt-get install -y screen` bzw. `dnf install -y screen`, dann `screen`, nach einem Abbruch mit `screen -r` wieder verbinden).

3. Schritt 1/8 – die Fragen

Die Installation stellt einige Fragen. In eckigen Klammern steht der Vorschlag; **Enter** übernimmt ihn.

Frage	Was Sie eingeben
Adresse von SalesDesk ohne https://	Ihre Adresse aus dem DNS-Eintrag, z. B. `salesdesk.ihre-firma.de`
Datenbank: [1] eingebaute PostgreSQL [2] eigene/externe PostgreSQL	**1** (empfohlen). **2** nur, wenn Ihre IT einen vorhandenen PostgreSQL-Server (ab Version 14) nutzen möchte – dann folgen Server, Port, Datenbankname, Benutzer und Passwort.
Erster Administrator: [1] jetzt hier anlegen [2] später im Browser	**1**: Sie legen Firma und Administrator gleich im Terminal an. **2**: Sie erhalten einen Einrichtungsschlüssel und legen beides im Browser an – praktisch, wenn ein Dienstleister installiert und die Firma selbst einrichtet.
E-Mail für Let's Encrypt (und den Administrator)	Ihre E-Mail-Adresse. Sie wird Anmeldename des Administrators und Kontakt für das Zertifikat.
Firmenname in SalesDesk	Name Ihrer Firma, wie er in SalesDesk erscheinen soll (nur bei 1)
Name des Administrators	Vor- und Nachname (nur bei 1)
E-Mail-Versand: [1] Microsoft 365 [2] SMTP [0] später	Siehe E-Mail-Versand. Wenn Sie die Angaben nicht zur Hand haben: **0** – Sie können es jederzeit nachholen.

Passwörter und geheime Schlüssel werden **unsichtbar** eingegeben (keine Zeichen sichtbar) und nur in der geschützten Datei `/opt/salesdesk/deploy/prod.env` gespeichert.

4. Schritt 2/8 – Docker

Fehlt Docker, wird es installiert (1–3 Minuten). Auf Ubuntu und Debian über das offizielle Docker-Skript, auf AlmaLinux und Rocky über die offizielle Docker-Paketquelle. Am Ende:

```
== 2/8 Docker ==
Docker version 28.x.x, build ... · Docker Compose version v2.x.x
```

5. Schritt 3/8 – Dateien und Geheimnisse

Die Programmdateien kommen nach `/opt/salesdesk`. Die Installation erzeugt zufällige Geheimnisse (Datenbank-Passwort, Schlüssel für die Anmeldung) und speichert sie in `/opt/salesdesk/deploy/prod.env`:

```
Geheimnisse erzeugt und in /opt/salesdesk/deploy/prod.env gespeichert (nur root lesbar).
Bitte eine Kopie dieser Datei sicher aufbewahren (Passwort-Tresor) — ohne sie sind Backups
nicht nutzbar.
```

⚠ Bewahren Sie eine Kopie von `prod.env` sicher auf (Passwort-Tresor). Wer diese Datei hat, hat Zugriff auf alle Daten. Ohne sie sind Sicherungen auf einem neuen Server nur eingeschränkt nutzbar: Zwei-Faktor-Anmeldungen und gespeicherte Zugangsdaten (Microsoft 365, Schnittstellen) wären nicht mehr lesbar. Anzeigen mit `cat /opt/salesdesk/deploy/prod.env`.

6. Schritt 4/8 – bauen und starten

Beim ersten Mal lädt Docker die Grundbausteine und baut SalesDesk. Das dauert **5 bis 15 Minuten**, je nach Server und Internetanbindung. Es erscheinen viele Zeilen; das ist normal. Danach wartet die Installation, bis SalesDesk antwortet:

```
Warte auf SalesDesk ......
SalesDesk läuft lokal (Port 8088).
```

7. Schritt 5/8 – Administrator

Bei Variante **1** legen Sie jetzt das Passwort fest – mindestens **12 Zeichen** mit Groß- und Kleinbuchstaben und einer Ziffer:

```
Passwort für it@ihre-firma.de festlegen (mind. 12 Zeichen, Groß- und Kleinbuchstaben, eine
Ziffer):
Passwort:
Passwort wiederholen:
Administrator it@ihre-firma.de angelegt.
```

Bei Variante **2** erscheint stattdessen der **Einrichtungsschlüssel**. Notieren Sie ihn; Sie geben ihn beim ersten Öffnen im Browser ein:

```
Ersteinrichtung im Browser: https://salesdesk.ihre-firma.de öffnen und diesen
Einrichtungsschlüssel eingeben:
    Kq3…(24 Zeichen)
```

8. Schritt 6/8 – Webserver und HTTPS

Jetzt sorgt die Installation dafür, dass SalesDesk unter Ihrer Adresse mit HTTPS erreichbar ist. Was hier passiert, hängt vom Server ab – alle drei Fälle beschreibt das Kapitel Webserver und HTTPS:

Situation	Ausgabe
Plesk gefunden	`Plesk gefunden — Subdomain, Zertifikat und Weiterleitung werden eingerichtet.`
kein Plesk, Ports 80/443 frei	Frage `HTTPS jetzt automatisch einrichten? [j/n]` – mit **j** richtet SalesDesk Caddy ein
kein Plesk, aber nginx/Apache vorhanden	`Kein eigener Webserver eingerichtet — Ports 80/443 belegt durch: nginx` und die Pfade zur fertigen Konfiguration

9. Schritt 7/8 – Sicherung und Update-Dienst

```
Tägliches Backup 02:00 nach /srv/backup/salesdesk (30 Tage aufbewahrt) eingerichtet
(/etc/cron.d/salesdesk).
Update-Dienst eingerichtet: künftige Updates in SalesDesk unter Verwaltung › Updates.
```

Mehr dazu in Datensicherung und Wiederherstellung und Updates.

10. Schritt 8/8 – Ergebnis

Die Installation zeigt die laufenden Container (hier gekürzt) und prüft die Erreichbarkeit von außen:

```
NAME                IMAGE              SERVICE   STATUS
salesdesk-api-1     salesdesk-api      api       Up 2 minutes
salesdesk-db-1      postgres:16        db        Up 2 minutes (healthy)
salesdesk-web-1     salesdesk-web      web       Up 2 minutes
salesdesk-worker-1  salesdesk-worker   worker    Up 2 minutes

FERTIG: https://salesdesk.ihre-firma.de ist aus dem Internet erreichbar.
Anmelden:  https://salesdesk.ihre-firma.de   (Browser, und als Server-Adresse in der App)
Protokoll: /var/log/salesdesk-install.log
```

Steht statt **FERTIG** der Hinweis `Von außen noch nicht erreichbar – DNS/Zertifikat prüfen`, läuft SalesDesk bereits, nur der Weg von außen fehlt noch. Gehen Sie das Kapitel Webserver und HTTPS durch und prüfen Sie den DNS-Eintrag.

Weiter geht es mit der ersten Einrichtung im Browser.

Was wo liegt

Pfad	Inhalt
`/opt/salesdesk`	Programm (Installationsordner)
`/opt/salesdesk/deploy/prod.env`	Einstellungen und Geheimnisse – **sicher aufbewahren**
`/opt/salesdesk/deploy/webserver-beispiele/`	fertige Konfiguration für Plesk, nginx und Apache
`/srv/backup/salesdesk`	tägliche Sicherungen
`/etc/cron.d/salesdesk`	Zeitplan für Sicherung und Wartung
`/var/log/salesdesk-install.log`	Protokoll der Installation
`/var/log/salesdesk-backup.log`	Protokoll der Sicherungen
`/opt/salesdesk/updates/update.log`	Protokoll der Updates über die Weboberfläche
Docker-Volumes `salesdesk_pgdata`, `salesdesk_files`	Datenbank und hochgeladene Dateien

Einstellungen vorab festlegen (für Dienstleister)

Alle Fragen lassen sich vorab als Umgebungsvariablen setzen, z. B. für eine unbeaufsichtigte Installation:

```
sudo SD_DOMAIN=salesdesk.ihre-firma.de SD_ADMIN_MODE=2 SD_ADMIN_EMAIL=it@ihre-firma.de
SD_DB_MODE=1 SD_MAIL_MODE=0 SD_PROXY=caddy bash salesdesk-installer-latest.sh
```

Variable	Bedeutung
`SD_DOMAIN`	Adresse ohne https://
`SD_DB_MODE`	1 = eingebaute Datenbank, 2 = eigene (dann `SD_DB_HOST`, `SD_DB_PORT`, `SD_DB_NAME`, `SD_DB_USER`, `SD_DB_PASSWORD`
`SD_ADMIN_MODE`	1 = Administrator im Terminal, 2 = Ersteinrichtung im Browser
`SD_ADMIN_EMAIL`, `SD_ADMIN_NAME`, `SD_ORG_NAME`	Administrator und Firma
`SD_MAIL_MODE`	0 = später, 1 = Microsoft 365, 2 = SMTP
`SD_PROXY`	`plesk`, `caddy` oder `manuell` – sonst automatisch erkannt
`SD_DIR`, `SD_INSTANCE`, `SD_PORT`	Ordner, Name und lokaler Port – nur für mehrere Instanzen auf einem Server, siehe Wartung

Webserver und HTTPS – mit oder ohne Plesk

Die drei Wege zu einer sicheren Adresse – Plesk, Caddy (automatisch) oder vorhandenes nginx/Apache – mit allen Handgriffen und Prüfungen.

SalesDesk selbst lauscht nur lokal auf `127.0.0.1:8088` und ist von außen nicht direkt erreichbar. Ein Webserver nimmt die verschlüsselten Verbindungen (HTTPS) an, hat das Zertifikat und reicht alles an SalesDesk weiter. Die Installation erkennt selbst, welcher Weg passt:

Erkannt	Weg	Was Sie tun
Plesk ist installiert	**A: Plesk**	nichts – Subdomain, Zertifikat und Weiterleitung legt die Installation an
kein Plesk, Port 80 und 443 frei	**B: Caddy**	bei der Frage „HTTPS jetzt automatisch einrichten?“ **j** eingeben
kein Plesk, Port 80/443 belegt (nginx, Apache …)	**C: vorhandener Webserver**	fertige Konfiguration einfügen und Zertifikat holen

Weg A: Server mit Plesk

Die Installation erledigt per Plesk-Befehl:

1. Subdomain anlegen, falls es sie noch nicht gibt (z. B. `salesdesk` unter `ihre-firma.de`.
2. Proxy-Modus der Subdomain ausschalten und die Weiterleitung an `127.0.0.1:8088` eintragen.
3. Let's-Encrypt-Zertifikat anfordern und die Umleitung von HTTP auf HTTPS einschalten.

Ausgabe bei Erfolg:

```
Plesk gefunden – Subdomain, Zertifikat und Weiterleitung werden eingerichtet.
Subdomain salesdesk.ihre-firma.de angelegt.
Plesk leitet salesdesk.ihre-firma.de an SalesDesk weiter.
Zertifikat eingerichtet.
```

Falls etwas fehlt: in Plesk von Hand

1. **Websites & Domains › Subdomain hinzufügen**: Name `salesdesk`, übergeordnete Domain Ihre Domain.
2. Bei der Subdomain **SSL/TLS-Zertifikate › Let's Encrypt**: Zertifikat holen (der DNS-Eintrag muss gelten).
3. **Hosting-Einstellungen**: „Permanente SEO-sichere 301-Weiterleitung von HTTP zu HTTPS“ einschalten.
4. **Apache- & nginx-Einstellungen**: **Proxy-Modus ausschalten** und bei **Zusätzliche nginx-Anweisungen** einfügen:

```
location / {
    proxy_pass http://127.0.0.1:8088;
    proxy_http_version 1.1;
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_read_timeout 300s;
}
```

5. **OK** klicken. Meldet Plesk „duplicate location /“, ist der Proxy-Modus noch eingeschaltet (Schritt 4).

Dieselben Zeilen liegen auf dem Server in `/opt/salesdesk/deploy/webserver-beispiele/plesk-nginx.txt`.

> Plesk-Firewall: Ist unter **Werkzeuge & Einstellungen › Firewall** eine eigene Regel aktiv, müssen 80 und 443 erlaubt sein – das ist bei Plesk Standard.

Weg B: Server ohne Plesk – Caddy richtet HTTPS automatisch ein

Auf einem leeren Linux-Server (V-Server, Cloud-VM, VM im Hyper-V) gibt es noch keinen Webserver. Die Installation fragt:

```
Kein Plesk und kein Webserver gefunden. SalesDesk kann HTTPS selbst einrichten
(Caddy als kleiner Webserver; das Let's-Encrypt-Zertifikat wird automatisch geholt und
verlängert).
HTTPS jetzt automatisch einrichten? [j/n] [j]:
```

Mit **Enter** (bzw. **j** passiert Folgendes:

1. Die Datei `/etc/salesdesk-proxy/Caddyfile` wird angelegt – mit Ihrer Adresse und der Weiterleitung an SalesDesk.
2. Ist eine Firewall aktiv (firewalld oder ufw), werden Port 80 und 443 geöffnet.
3. Der Container `salesdesk-proxy` (Caddy) wird gestartet. Er startet nach jedem Neustart des Servers automatisch.
4. Caddy holt das Zertifikat bei Let's Encrypt und **verlängert es selbstständig** alle 60–90 Tage. Sie müssen sich darum nie kümmern.

Ausgabe bei Erfolg:

```
Firewall (firewalld): Ports 80 und 443 geöffnet.
Warte auf das HTTPS-Zertifikat (bis 2 Minuten) ....
Caddy leitet https://salesdesk.ihre-firma.de an SalesDesk weiter, Zertifikat gültig
(Verlängerung automatisch).
```

Kommt stattdessen „Noch kein Zertifikat“, fehlt fast immer der DNS-Eintrag oder Port 80/443 ist **beim Hoster** gesperrt. Caddy versucht es selbstständig weiter; sobald DNS und Ports stimmen, ist SalesDesk erreichbar – ohne erneute Installation. Den Stand sehen Sie mit:

```
docker logs --tail 40 salesdesk-proxy
```

So sieht die Caddy-Konfiguration aus (zur Information; Sie müssen nichts ändern):

```
{
        email it@ihre-firma.de
}

# salesdesk-instanz salesdesk
salesdesk.ihre-firma.de {
        encode gzip
        reverse_proxy 127.0.0.1:8088
}
```

Caddy verwalten

Aufgabe	Befehl
Status	`docker ps --filter name=salesdesk-proxy`
Protokoll	`docker logs --tail 60 salesdesk-proxy`
Neu starten (z. B. nach Änderung am Caddyfile)	`docker restart salesdesk-proxy`
Zweite Adresse für denselben Server	im Caddyfile einen weiteren Block wie oben ergänzen (Adresse, dann `{`, in der nächsten Zeile `reverse_proxy 127.0.0.1:8088`, dann `}` in einer eigenen Zeile), dann neu starten

Weg C: vorhandener nginx oder Apache

Läuft auf dem Server schon ein Webserver für andere Seiten, richtet SalesDesk keinen eigenen ein. Die Installation schreibt eine fertige Konfiguration mit Ihrer Adresse:

```
Kein eigener Webserver eingerichtet – Ports 80/443 belegt durch: nginx
Fertige Konfiguration zum Einfügen in Ihren Webserver:
  nginx:  /opt/salesdesk/deploy/webserver-beispiele/nginx-salesdesk.conf
  Apache: /opt/salesdesk/deploy/webserver-beispiele/apache-salesdesk.conf
```

nginx

```
cp /opt/salesdesk/deploy/webserver-beispiele/nginx-salesdesk.conf
/etc/nginx/conf.d/salesdesk.conf
nginx -t && systemctl reload nginx
```

Zertifikat mit certbot (holt das Zertifikat und trägt es in die Konfiguration ein; die Verlängerung läuft danach automatisch):

```
apt-get install -y certbot python3-certbot-nginx      # Ubuntu/Debian
dnf install -y certbot python3-certbot-nginx          # AlmaLinux/Rocky (vorher: dnf install
-y epel-release)
certbot --nginx -d salesdesk.ihre-firma.de
```

Apache

Ubuntu/Debian:

```
cp /opt/salesdesk/deploy/webserver-beispiele/apache-salesdesk.conf /etc/apache2/sites-
available/salesdesk.conf
a2enmod proxy proxy_http headers
a2ensite salesdesk
systemctl reload apache2
apt-get install -y certbot python3-certbot-apache
certbot --apache -d salesdesk.ihre-firma.de
```

AlmaLinux/Rocky:

```
cp /opt/salesdesk/deploy/webserver-beispiele/apache-salesdesk.conf
/etc/httpd/conf.d/salesdesk.conf
systemctl reload httpd
dnf install -y epel-release && dnf install -y certbot python3-certbot-apache mod_ssl
certbot --apache -d salesdesk.ihre-firma.de
```

⚠ Bei SELinux (AlmaLinux/Rocky) darf der Webserver standardmäßig keine Verbindung zu `127.0.0.1:8088` aufbauen. Freigeben mit `setsebool -P httpd_can_network_connect 1`. Plesk und Caddy brauchen das nicht.

Wichtig für eigene Konfigurationen: Uploads bis mindestens **30 MB** erlauben (die Vorlage setzt nginx `client_max_body_size 50m;`, Zeitlimit mindestens **300 Sekunden**, und die Kopfzeilen `Host`, `X-Forwarded-For` und `X-Forwarded-Proto` weitergeben.

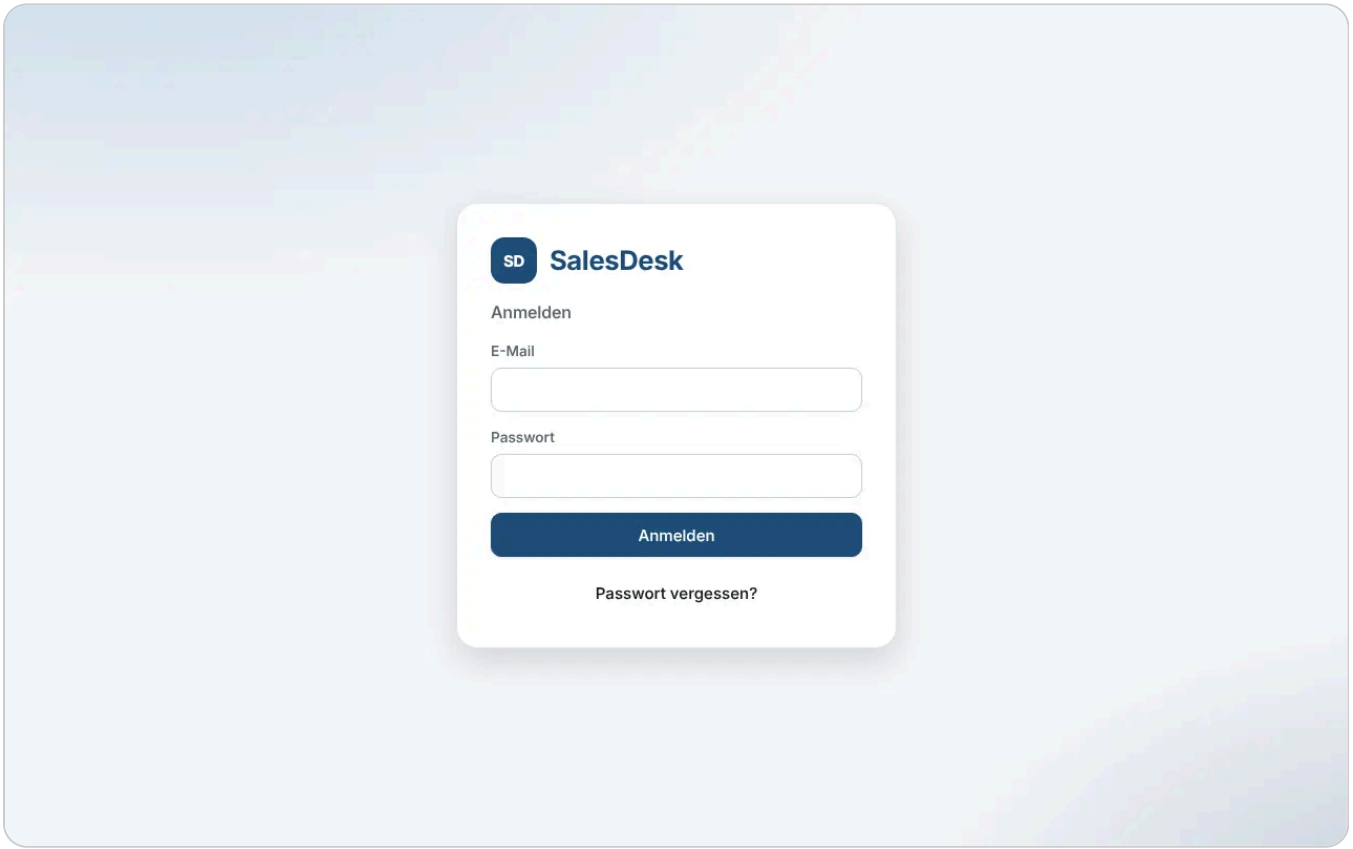
Prüfen, ob alles stimmt

Auf dem Server:

```
curl -s http://127.0.0.1:8088/api/v1/health
curl -s https://salesdesk.ihre-firma.de/api/v1/health
```

Beide Male muss `{"status":"ok"}` erscheinen. Die erste Zeile prüft SalesDesk selbst, die zweite den Weg über Webserver und Zertifikat.

Im Browser auf Ihrem PC: `https://salesdesk.ihre-firma.de` öffnen. Es erscheint die Anmeldeseite von SalesDesk, das Schloss-Symbol in der Adresszeile zeigt ein gültiges Zertifikat.



Anmeldeseite der Weboberfläche mit E-Mail und Passwort

Ergebnis	Bedeutung
erste Zeile kein `ok`	SalesDesk läuft nicht – siehe Fehlersuche, Abschnitt „SalesDesk startet nicht“
erste ok, zweite Zeitüberschreitung	Port 443 ist von außen zu (Hoster-Firewall) oder DNS zeigt woanders hin
zweite Zeile Zertifikatsfehler	Zertifikat fehlt oder gehört zu einer anderen Adresse
`502 Bad Gateway` im Browser	Webserver läuft, SalesDesk nicht – `docker compose … ps` prüfen
Plesk-Standardseite statt SalesDesk	Weiterleitung fehlt – Weg A, „Falls etwas fehlt“

Windows Server (Hyper-V)

SalesDesk auf Windows Server 2019, 2022 oder 2025 – mit einer Linux-VM im Hyper-V, Schritt für Schritt per PowerShell.

SalesDesk besteht aus Linux-Containern. Windows Server kann diese nicht direkt ausführen, und Docker Desktop ist für Windows Server nicht vorgesehen. Der zuverlässige Weg ist eine **kleine Linux-VM im Hyper-V**, das in Windows Server bereits enthalten ist. In dieser VM läuft die normale Installation („ohne Plesk“, Caddy richtet HTTPS ein). Für Ihre IT ist es eine VM wie jede andere: sichern, überwachen, verschieben wie gewohnt.

> Läuft Ihr Windows Server selbst schon als VM (z. B. bei VMware, Proxmox oder in Azure), legen Sie die Linux-VM besser **direkt daneben** auf derselben Plattform an statt verschachtelt im Hyper-V. Danach geht es weiter mit Installation Schritt für Schritt.

Was Sie brauchen

- Windows Server 2019, 2022 oder 2025 (Standard oder Datacenter) auf echter Hardware oder mit aktivierter verschachtelter Virtualisierung
- Administratorrechte auf dem Windows Server
- 4 GB freien Arbeitsspeicher (besser 8 GB) und 80 GB freien Speicherplatz für die VM
- Das Installationsabbild **Ubuntu Server 24.04 LTS** (ISO, ca. 3 GB) von ubuntu.com, Bereich „Ubuntu Server“
- Eine freie IP-Adresse in Ihrem Netz für die VM (oder die NAT-Variante unten)

1. Hyper-V einschalten

PowerShell als Administrator öffnen (Rechtsklick auf Start › „Windows PowerShell (Administrator)“ bzw. „Terminal (Administrator)“):

```
Install-WindowsFeature -Name Hyper-V -IncludeManagementTools -Restart
```

Der Server startet neu. Danach ist der **Hyper-V-Manager** im Startmenü.

2. Netzwerk für die VM

Die VM braucht eine eigene Adresse im Netz. Den Namen Ihrer Netzwerkkarte zeigt `Get-NetAdapter` (Spalte **Name**, z. B. `Ethernet`.

```
Get-NetAdapter
New-VMSwitch -Name "Extern" -NetAdapterName "Ethernet" -AllowManagementOS $true
```

Die Netzwerkverbindung des Servers ist dabei für einige Sekunden unterbrochen. Bei einer Fernwartungssitzung (RDP) verbindet sie sich von selbst wieder.

3. VM anlegen

Ubuntu-ISO z. B. nach `C:\ISO\` legen, dann (Pfade bei Bedarf anpassen):

```
New-VM -Name "SalesDesk" -Generation 2 -MemoryStartupBytes 8GB -NewVHDPath "C:\Hyper-
V\SalesDesk.vhdx" -NewVHDSizeBytes 80GB -SwitchName "Extern"
Set-VMProcessor -VMName "SalesDesk" -Count 4
Set-VMMemory -VMName "SalesDesk" -DynamicMemoryEnabled $false
Add-VMDvdDrive -VMName "SalesDesk" -Path "C:\ISO\ubuntu-24.04-live-server-amd64.iso"
Set-VMFirmware -VMName "SalesDesk" -SecureBootTemplate MicrosoftUEFICertificateAuthority -
FirstBootDevice (Get-VMDvdDrive -VMName "SalesDesk")
Set-VM -Name "SalesDesk" -AutomaticStartAction Start -AutomaticStartDelay 30 -
AutomaticStopAction ShutDown
Start-VM -Name "SalesDesk"
vmconnect localhost "SalesDesk"
```

Für kleine Teams (bis 10 Nutzer) genügen `4GB` Arbeitsspeicher und `-Count 2`. Die Zeile mit `AutomaticStartAction` sorgt dafür, dass SalesDesk nach einem Neustart des Windows Servers von selbst wieder läuft.

> ⚠ Die Zeile mit `SecureBootTemplate MicrosoftUEFICertificateAuthority` ist wichtig. Ohne sie startet Ubuntu in einer Generation-2-VM nicht („The image's hash and certificate are not allowed“).

4. Ubuntu Server installieren

Im Fenster der VM läuft das Ubuntu-Installationsprogramm. Bedienung mit Pfeiltasten, **Enter** und **Tab**:

1. **Sprache**: English oder Deutsch.
2. **Tastatur**: German.
3. **Art der Installation**: Ubuntu Server (nicht „minimized“).
4. **Netzwerk**: Die VM bekommt per DHCP eine Adresse. Für einen Server ist eine **feste Adresse** besser: bei `eth0` **Edit IPv4** › **Manual** und Subnetz, Adresse, Gateway und DNS-Server Ihres Netzes eintragen (z. B. Adresse `192.168.10.50`, Subnetz `192.168.10.0/24`, Gateway `192.168.10.1`. Notieren Sie die Adresse.
5. **Proxy** und **Mirror**: leer bzw. Vorgabe lassen.
6. **Speicher**: „Use an entire disk“ – die virtuelle 80-GB-Platte.
7. **Profil**: Ihr Name, Servername (z. B. `salesdesk`, Benutzername (z. B. `itadmin` und ein sicheres Passwort.
8. **Ubuntu Pro**: überspringen.
9. **SSH**: **Install OpenSSH server** ankreuzen.
10. **Featured snaps**: nichts auswählen.
11. Am Ende **Reboot Now**. Erscheint „Please remove the installation medium“, einfach **Enter** drücken.

Danach das ISO aus der VM entfernen (PowerShell auf dem Windows Server):

```
Get-VMDvdDrive -VMName "SalesDesk" | Set-VMDvdDrive -Path $null
```

5. Von außen erreichbar machen

SalesDesk in der VM braucht von außen die Ports **80** und **443**:

- **Firmennetz mit Router/Firewall**: Portweiterleitung TCP 80 und 443 auf die **Adresse der VM** (z. B. `192.168.10.50` – nicht auf den Windows Server.
- **DNS-Eintrag** `salesdesk.ihre-firma.de` auf die **öffentliche** IP Ihres Anschlusses, siehe Vorbereitung.
- Nur intern genutzt (ohne Zugriff von unterwegs)? Dann reicht ein interner DNS-Eintrag. Für das Zertifikat muss die Adresse aber einmal aus dem Internet erreichbar sein – sonst siehe Fragen für die IT, „Ohne Internet“.

Variante: Windows-Mietserver mit nur einer öffentlichen IP (NAT)

Haben Sie keinen Router davor (z. B. gemieteter Windows-Root-Server mit einer IP), verbinden Sie die VM über ein internes Netz und leiten 80/443 vom Windows Server weiter. Statt Schritt 2:

```
New-VMSwitch -Name "SalesDeskNAT" -SwitchType Internal
New-NetIPAddress -IPAddress 192.168.200.1 -PrefixLength 24 -InterfaceAlias "vEthernet
(SalesDeskNAT)"
New-NetNat -Name "SalesDeskNAT" -InternalIPInterfaceAddressPrefix 192.168.200.0/24
Add-NetNatStaticMapping -NatName "SalesDeskNAT" -Protocol TCP -ExternalIPAddress 0.0.0.0 -
ExternalPort 80 -InternalIPAddress 192.168.200.10 -InternalPort 80
Add-NetNatStaticMapping -NatName "SalesDeskNAT" -Protocol TCP -ExternalIPAddress 0.0.0.0 -
ExternalPort 443 -InternalIPAddress 192.168.200.10 -InternalPort 443
New-NetFirewallRule -DisplayName "SalesDesk HTTP/HTTPS" -Direction Inbound -Protocol TCP -
LocalPort 80,443 -Action Allow
```

Bei `New-VM` dann `-SwitchName "SalesDeskNAT"` verwenden und in Ubuntu die feste Adresse `192.168.200.10/24`, Gateway `192.168.200.1`, DNS z. B. `1.1.1.1` eintragen.

> ⚠ Läuft auf dem Windows Server bereits ein IIS auf Port 80/443, ist diese Variante nicht möglich. Dann braucht die VM eine eigene öffentliche IP (beim Hoster bestellen) oder Sie leiten im IIS mit „Application Request Routing“ weiter – das ist Sache Ihrer IT.

6. SalesDesk in der VM installieren

Vom Windows Server oder Ihrem PC per SSH in die VM (siehe Vorbereitung:

```
ssh itadmin@192.168.10.50
sudo -i
cd /root
curl -fLO https://salesdesk-app.iks-solutions.com/download/files/salesdesk-installer-
latest.sh
bash salesdesk-installer-latest.sh
```

Ab hier läuft alles wie in Installation Schritt für Schritt. Bei „HTTPS jetzt automatisch einrichten?“ wählen Sie **j** (Caddy, Weg B im Kapitel Webserver und HTTPS.

7. Sichern und Betrieb

- Die **tägliche SalesDesk-Sicherung** läuft in der VM nach `/srv/backup/salesdesk`. Kopieren Sie diese Sicherungen auf ein anderes System, siehe Datensicherung.
- Zusätzlich können Sie die **ganze VM** mit Ihrer üblichen Lösung sichern (Windows Server-Sicherung, Veeam o. Ä.). Hyper-V-Prüfpunkte sind **keine** Sicherung – nutzen Sie sie nur kurzzeitig, z. B. vor einem Update.
- Ubuntu-Sicherheitsupdates spielt die VM automatisch ein (unattended-upgrades ist bei Ubuntu Server Standard). Einmal im Monat `apt-get update && apt-get -y upgrade` und ein Neustart der VM schaden nicht.
- Herunterfahren des Windows Servers fährt die VM sauber herunter `AutomaticStopAction ShutDown`, beim Start läuft sie nach 30 Sekunden wieder an.

Nur zum Ausprobieren: WSL2

Auf Windows Server 2022/2025 und Windows 10/11 lässt sich SalesDesk auch im **Windows-Subsystem für Linux (WSL2)** starten `wsl --install -d Ubuntu-24.04`, dann in Ubuntu die Installationsdatei ausführen). WSL2 ist für Entwicklung gedacht: Es startet nicht ohne angemeldeten Benutzer, die Netzwerkadresse wechselt und Ports müssen von Hand weitergeleitet werden. Für den echten Betrieb nehmen Sie bitte die Hyper-V-VM.

Erste Einrichtung im Browser

Erste Anmeldung, Zwei-Faktor, Firmendesign, Verkaufsphasen, Benutzer, Lizenz und App verbinden – mit Checkliste für die Übergabe.

1. Erste Anmeldung

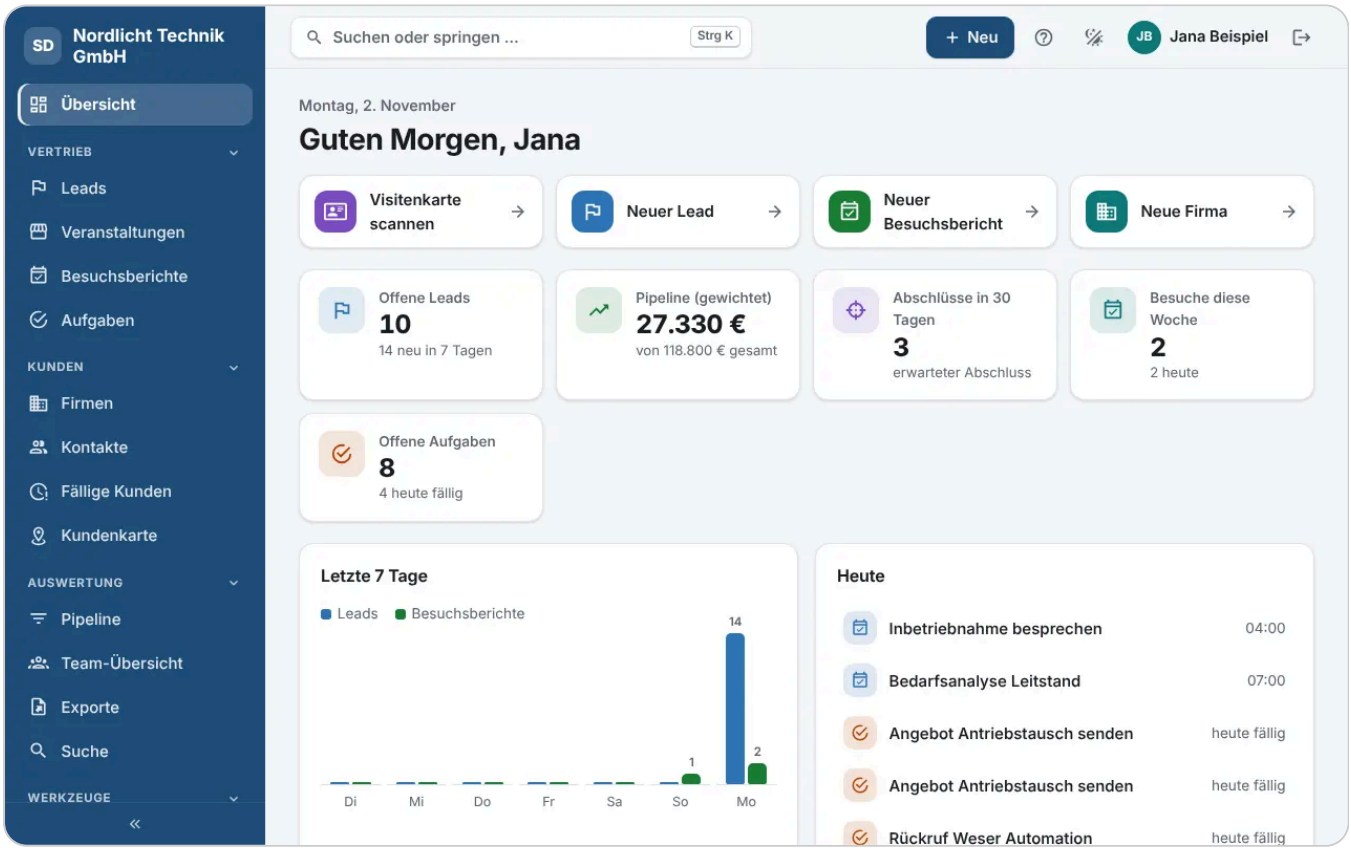
Öffnen Sie `https://salesdesk.ihre-firma.de` im Browser (Edge, Chrome, Firefox oder Safari in aktueller Version).

- **Administrator im Terminal angelegt** (Variante 1): Melden Sie sich mit E-Mail und Passwort an.
- **Ersteinrichtung im Browser** (Variante 2): Statt der Anmeldung erscheint **Ersteinrichtung**. Tragen Sie den **Einrichtungsschlüssel** aus der Installation ein, dazu **Name der Firma**, **Ihr Name**, E-Mail und ein Passwort (mindestens 12 Zeichen) und klicken Sie auf **Einrichten und anmelden**. Der Schlüssel gilt nur, solange noch keine Firma existiert.

Den Einrichtungsschlüssel vergessen? Er steht auf dem Server in der Datei `prod.env`:

```
grep SETUP_TOKEN /opt/salesdesk/deploy/prod.env
```

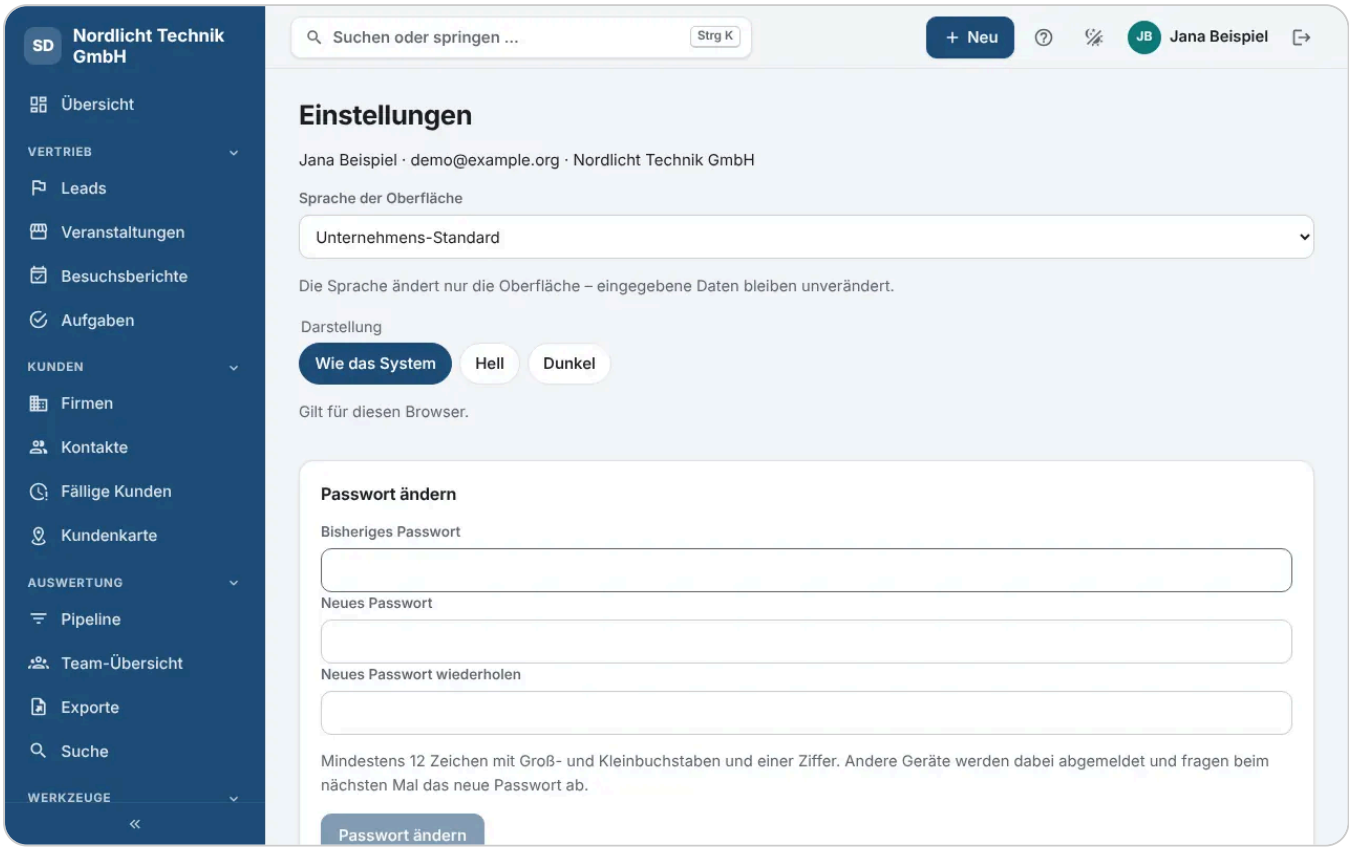
Nach der Anmeldung sehen Sie die **Übersicht**. Der erste Administrator ist zugleich **Server-Administrator** und sieht zusätzlich den Menüpunkt **Verwaltung › Server**.



Übersicht der Weboberfläche mit Kennzahlen, Diagramm der letzten sieben Tage und Terminen von heute

2. Sicherheit zuerst

1. Im Menü links **Verwaltung › Einstellungen**.
2. Im Abschnitt **Zwei-Faktor-Anmeldung** auf **Einrichtung starten** klicken, den QR-Code mit einer Authenticator-App (Microsoft Authenticator, Google Authenticator, 1Password …) scannen, den sechsstelligen Code eingeben und **Aktivieren**. Die **Wiederherstellungscodes** ausdrucken oder im Passwort-Tresor ablegen.
3. Unter **Sicherheit und Datenschutz** können Sie die Zwei-Faktor-Anmeldung für alle Verwaltungsrollen zur Pflicht machen (empfohlen).



Einstellungen mit Sprache, Darstellung, Passwort ändern und Zwei-Faktor-Anmeldung

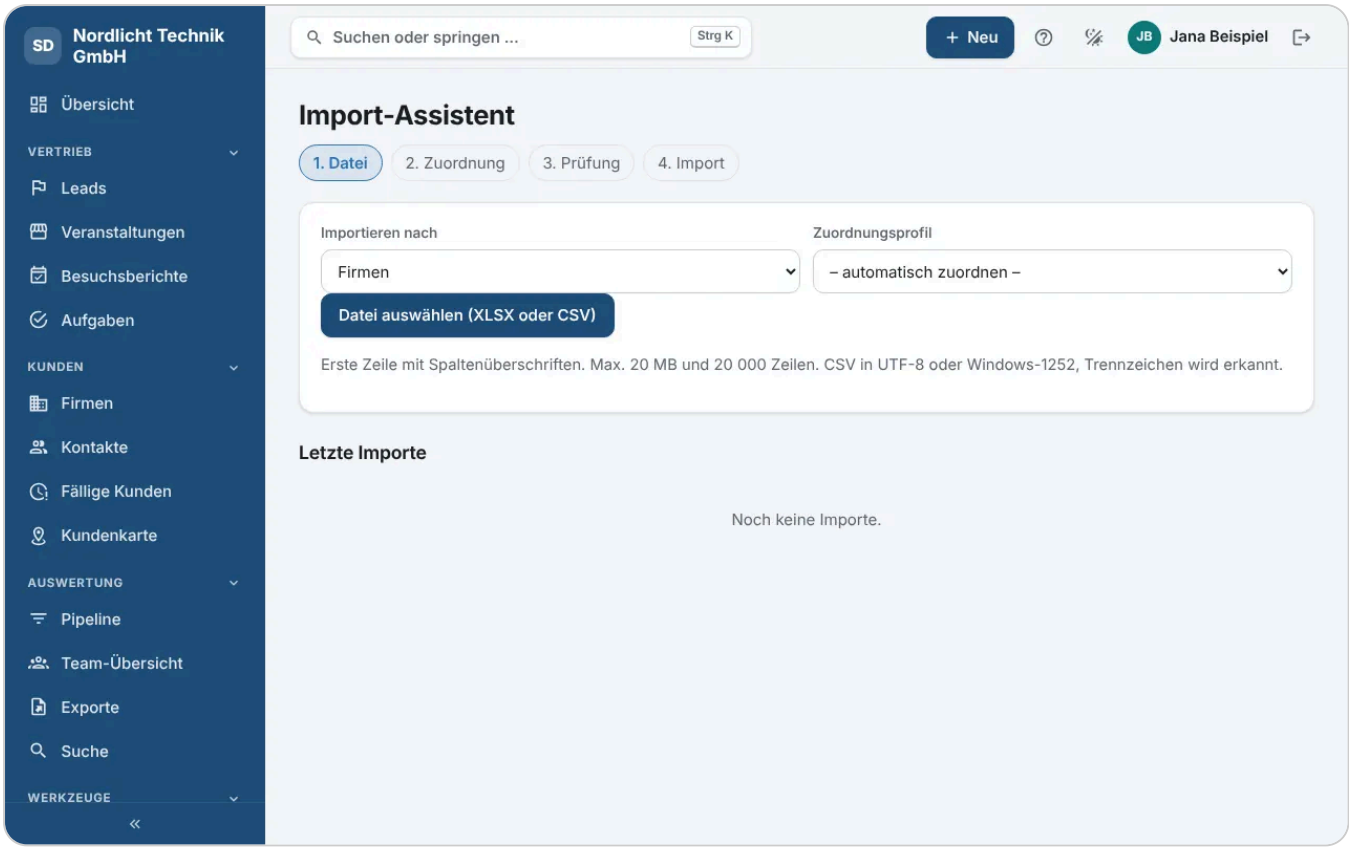
3. SalesDesk an Ihre Firma anpassen

Was	Wo	Kapitel der Bedienungsanleitung
Logo und Farben, Name in Berichten	Verwaltung › Einstellungen, Abschnitt Firmendesign	Einstellungen
Verkaufsphasen mit Wahrscheinlichkeit	Verwaltung › Einstellungen, Abschnitt Verkaufsphasen	Einstellungen
Wer sieht welche Firmen, Gebiete	Verwaltung › Vertriebsorganisation	Vertriebsorganisation
Produkte und Hersteller	Verwaltung › Produkte & Hersteller	Produkte
Fragebögen und Checklisten	Verwaltung › Fragebögen & Checklisten	Fragebögen
E-Mail- und Dokumentvorlagen	Verwaltung › Einstellungen, Abschnitt Vorlagen	Einstellungen

Die Vorgaben sind sofort nutzbar. Sie können also auch erst einmal starten und später anpassen.

4. Bestandsdaten übernehmen

Kunden und Kontakte aus Excel, Outlook oder einem anderen CRM übernehmen Sie unter **Werkzeuge › Importe**. Der Import-Assistent erkennt die Spalten selbst, zeigt vor dem Speichern eine Prüfung und findet Dubletten. Ablauf siehe Bedienungsanleitung, Kapitel „Import“.



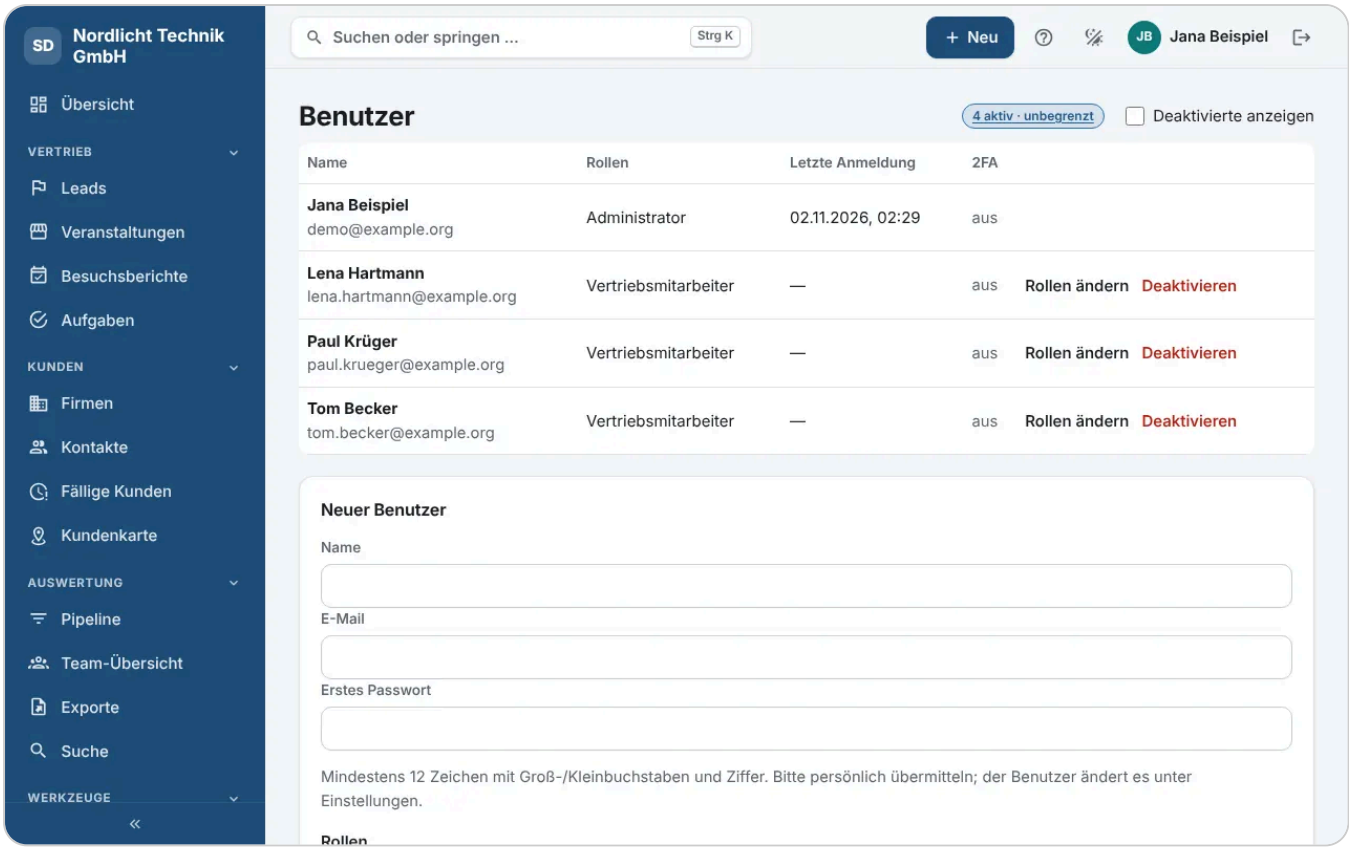
Import-Assistent in vier Schritten: Datei, Zuordnung, Prüfung, Import

5. Benutzer anlegen

Unter **Verwaltung › Benutzer** legen Sie für jede Person ein Konto an:

1. **Name** und **E-Mail** eintragen.
2. **Erstes Passwort** vergeben (mindestens 12 Zeichen) – bitten Sie die Person, es nach der ersten Anmeldung unter Einstellungen zu ändern.
3. **Rolle** wählen: **Vertriebsmitarbeiter** für den Außendienst, **Vertriebsleitung** für Auswertungen des Teams, **Administrator** für die Verwaltung, **Leser/Auditor** nur lesend.
4. **Benutzer anlegen**.

Jedes aktive Konto belegt einen Lizenzplatz, auch Ihres. Wer ausscheidet, wird **deaktiviert** – der Platz ist sofort frei, die Daten bleiben.

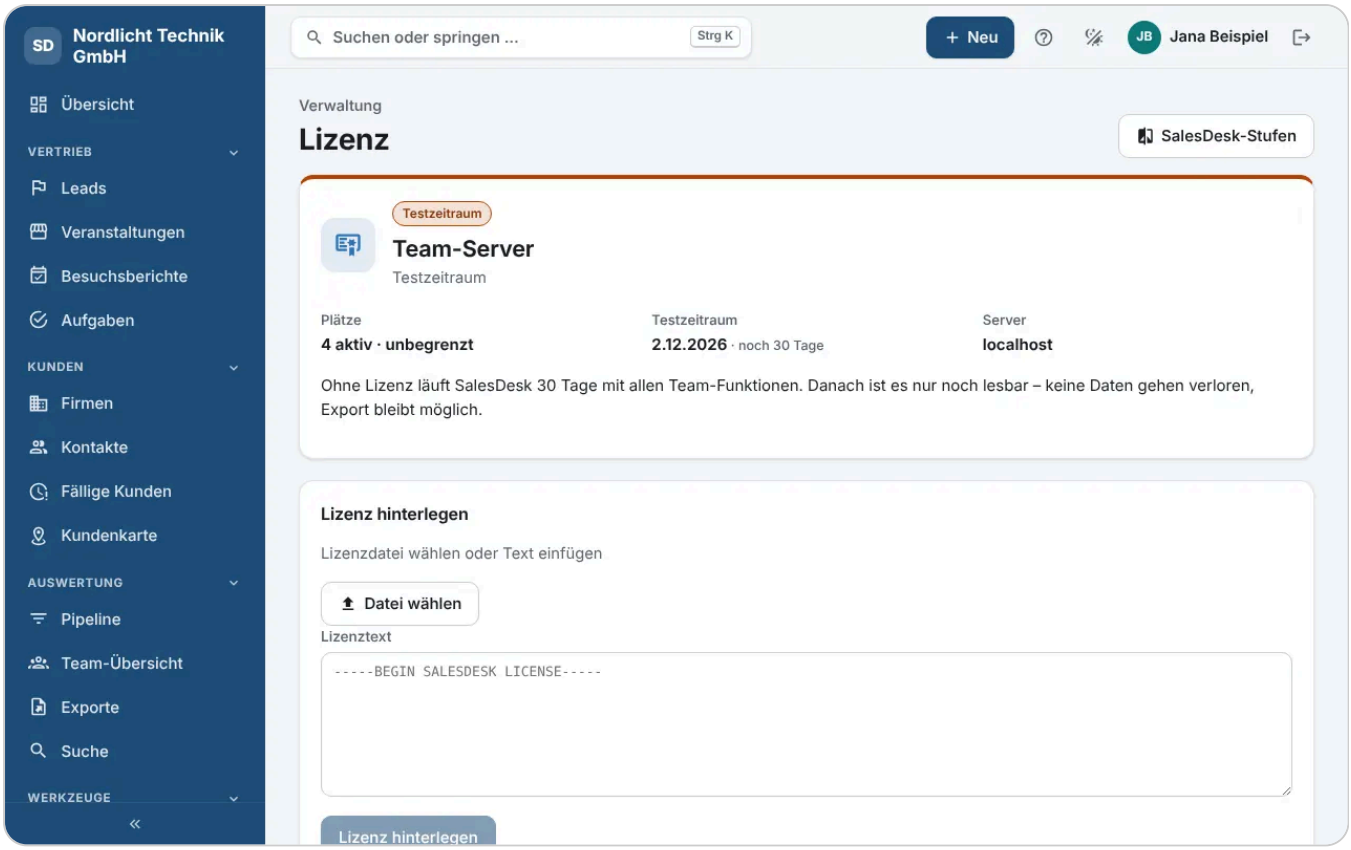


Benutzerverwaltung mit Liste der Benutzer, Rollen und Formular für neue Benutzer

Geben Sie jeder Person drei Angaben: die **Server-Adresse**, ihre **E-Mail** und das **erste Passwort**. Mit Microsoft 365 geht es auch ohne Passwort, siehe E-Mail-Versand, Abschnitt „Anmeldung mit Microsoft“.

6. Lizenz

In den ersten 30 Tagen läuft alles als Test. Unter **Verwaltung › Lizenz** sehen Sie Stufe, Plätze und Laufzeit.



Lizenzseite mit Stufe Team-Server, Plätzen, Testzeitraum und Feld zum Hinterlegen einer Lizenzdatei

- **Abo aus der App**: Die Person, die das Team-Server-Abo im App Store bzw. bei Google Play abschließt, meldet sich danach **mit der App als Administrator** an diesem Server an. Die App überträgt den Kauf automatisch; die Lizenzseite zeigt dann „Team-Server“ mit Plätzen und Laufzeit. Verlängerungen kommen beim nächsten Öffnen der App mit diesem Konto an.
- **Lizenzdatei (Jahresvertrag)**: **Datei wählen** oder den Text einfügen und **Lizenz hinterlegen**. Die Datei ist an die Adresse Ihres Servers gebunden; geben Sie bei der Anfrage deshalb die genaue Adresse an.

7. App verbinden

Jede Person installiert die kostenlose App **SalesDesk** aus dem App Store bzw. von Google Play und wählt **Mit Firmenserver verbinden**:



App: Anmeldung mit Server-Adresse, E-Mail und Passwort

1. **Server-Adresse**: `salesdesk.ihre-firma.de` (ohne https:// geht auch).
2. **E-Mail** und **Passwort** eingeben, **Anmelden**.
3. Die App lädt die Daten der Firma und ist danach auch offline nutzbar.

Mitarbeiter kaufen **nichts** in der App – die Lizenz liegt auf dem Server.

Checkliste für die Übergabe

- ☐ `https://salesdesk.ihre-firma.de` öffnet die Anmeldeseite mit gültigem Zertifikat
- ☐ `prod.env` liegt als Kopie im Passwort-Tresor
- ☐ Zwei-Faktor-Anmeldung für den Administrator eingerichtet, Wiederherstellungscodes abgelegt
- ☐ E-Mail-Versand eingerichtet und mit `mail-test` geprüftE-Mail-Versand
- ☐ Erste Sicherung vorhanden: `ls /srv/backup/salesdesk`Datensicherung
- ☐ Sicherungen werden auf ein zweites System kopiert
- ☐ Benutzer angelegt, App bei mindestens einer Person verbunden
- ☐ Lizenz hinterlegt oder Ende des Testzeitraums im Kalender notiert

E-Mail-Versand und Microsoft 365

Versand über ein SMTP-Postfach oder Microsoft 365 (Graph) einrichten und testen, Anmeldung mit Microsoft-Konto.

Wofür braucht SalesDesk E-Mail?

SalesDesk **versendet** E-Mails, es liest kein Postfach. Gebraucht wird das für:

- **Passwort vergessen** – Link zum Zurücksetzen
- **Follow-up-Mails** nach Messe oder Besuch und **Besuchsberichte** per Mail aus der Weboberfläche
- Hinweise an die Verwaltung (z. B. Lizenz läuft ab)

Ohne E-Mail-Versand funktioniert alles andere. Passwörter setzt dann die Verwaltung unter **Verwaltung › Benutzer** neu.

Weg	Wann	Was Sie brauchen
SMTP	Postfach bei einem Hoster oder eigener Mailserver	Server, Port, Benutzername, Passwort, Absenderadresse
Microsoft 365 (Graph)	Ihre Firma nutzt Microsoft 365 / Exchange Online	App-Registrierung in Entra ID (10 Minuten), freigegebenes Postfach als Absender

⚠ Microsoft schaltet die SMTP-Anmeldung mit Benutzername und Passwort („SMTP AUTH“) für Exchange Online schrittweise ab. Nutzen Sie bei Microsoft 365 deshalb den Weg **Graph** – er braucht kein Postfach-Passwort.

Einrichten bei der Installation

Die Installation fragt nach dem VersandInstallation, Schritt 1). Haben Sie dort **0 – später** gewählt, tragen Sie die Angaben in `/opt/salesdesk/deploy/prod.env` ein und starten SalesDesk neu, wie unten beschrieben.

Die Datei bearbeiten Sie auf dem Server mit dem Editor **nano**:

```
nano /opt/salesdesk/deploy/prod.env
```

Pfeiltasten zum Bewegen, Werte hinter dem `=` eintragen (ohne Anführungszeichen), **Strg+O** und **Enter** speichert, **Strg+X** beendet.

SMTP

In `prod.env`:

```
EMAIL_PROVIDER=smtp
SMTP_HOST=mail.ihr-anbieter.de
SMTP_PORT=587
SMTP_USER=vertrieb@ihre-firma.de
SMTP_PASSWORD=das-passwort-des-postfachs
SMTP_FROM=vertrieb@ihre-firma.de
```

Einstellung	Bedeutung
`SMTP_PORT`	`587` = STARTTLS (üblich), `465` = SSL/TLS, `25` = ohne Verschlüsselung – nur für einen internen Mail-Relay im Firmennetz
`SMTP_USER`	Anmeldename des Postfachs, meist die E-Mail-Adresse. Leer lassen, wenn ein interner Relay keine Anmeldung verlangt.
`SMTP_FROM`	Absenderadresse. Sie muss zum Postfach passen, sonst lehnt der Mailserver ab oder die Mail landet im Spam.

Die Zugangsdaten finden Sie in der Hilfe Ihres Mail-Anbieters unter „SMTP-Server“ oder „Postausgangsserver“.

Microsoft 365 über Graph

1. Absender-Postfach

Legen Sie im **Exchange Admin Center** (admin.exchange.microsoft.com) unter **Empfänger › Postfächer › Freigegebenes Postfach hinzufügen** ein Postfach an, z. B. `salesdesk@ihre-firma.de`. Freigegebene Postfächer brauchen keine Lizenz. Ein normales Benutzerpostfach geht auch.

> ⚠ Eine **Microsoft-365-Gruppe** (Gruppenpostfach) kann über Graph nicht als Absender dienen. Nehmen Sie ein freigegebenes Postfach.

2. App in Entra ID registrieren

1. **entra.microsoft.com** › Identität › Anwendungen › **App-Registrierungen** › **Neue Registrierung**.
2. Name `SalesDesk Mailversand`, Kontotyp **Nur Konten in diesem Organisationsverzeichnis**, keine Umleitungs-URI › **Registrieren**.
3. Auf der Übersicht notieren: **Anwendungs-ID (Client-ID)** und **Verzeichnis-ID (Mandanten-ID)**.
4. **Zertifikate & Geheimnisse › Neuer geheimer Clientschlüssel**, Ablauf 24 Monate › **Hinzufügen**. Kopieren Sie sofort den **Wert** (nicht die „Geheimnis-ID“) – er wird nur einmal angezeigt. Tragen Sie das Ablaufdatum in Ihren Kalender ein.

3. Senden erlauben – auf ein Postfach beschränkt (empfohlen)

So darf SalesDesk **nur** aus dem einen Postfach senden. In Entra fügen Sie dafür **keine** API-Berechtigung hinzu. Stattdessen in **PowerShell** (auf Ihrem PC, als Exchange-Administrator):

```
Install-Module ExchangeOnlineManagement -Scope CurrentUser
Connect-ExchangeOnline
New-ServicePrincipal -AppId <Client-ID> -ObjectId <Objekt-ID der Unternehmensanwendung> -
DisplayName "SalesDesk Mailversand"
New-ManagementScope -Name "SalesDesk Absender" -RecipientRestrictionFilter
"PrimarySmtpAddress -eq 'salesdesk@ihre-firma.de'"
New-ManagementRoleAssignment -App <Client-ID> -Role "Application Mail.Send" -
CustomResourceScope "SalesDesk Absender"
Test-ServicePrincipalAuthorization -Identity <Client-ID> -Resource salesdesk@ihre-firma.de
```

Die **Objekt-ID** steht in Entra unter **Unternehmensanwendungen** › „SalesDesk Mailversand“ – nicht die Objekt-ID der App-Registrierung. Die letzte Zeile muss bei `Application Mail.Send` den Wert **InScope True** zeigen. Neue Berechtigungen gelten nach 30 Minuten bis 2 Stunden.

Einfacher, aber für alle Postfächer: In Entra › App › **API-Berechtigungen › Berechtigung hinzufügen › Microsoft Graph › Anwendungsberechtigungen › Mail.Send** › **Administratorzustimmung erteilen**. Dann dürfte die App aus jedem Postfach Ihres Mandanten senden – nur nutzen, wenn die Beschränkung nicht möglich ist.

4. In SalesDesk eintragen

In `prod.env` (oder bei der Installation Auswahl **1**:

```
EMAIL_PROVIDER=graph
GRAPH_TENANT_ID=<Verzeichnis-ID>
GRAPH_CLIENT_ID=<Anwendungs-ID>
GRAPH_CLIENT_SECRET=<Wert des geheimen Schlüssels>
GRAPH_SENDER=salesdesk@ihre-firma.de
SMTP_FROM=salesdesk@ihre-firma.de
```

Übernehmen und testen

Nach jeder Änderung an `prod.env`:

```
cd /opt/salesdesk
docker compose -f deploy/docker-compose.plesk.yml --env-file deploy/prod.env up -d
docker compose -f deploy/docker-compose.plesk.yml --env-file deploy/prod.env exec api python
-m app.cli mail-test --to ihre.adresse@ihre-firma.de
```

Die Datei heißt `docker-compose.plesk.yml` auf **allen** Servern – mit oder ohne Plesk. Der Name ist historisch.

Erwartete Ausgabe:

```
Versand: graph (configured)
Testmail an ihre.adresse@ihre-firma.de gesendet.
```

Fehlermeldung	Ursache und Lösung
`Kein E-Mail-Versand eingerichtet`	`EMAIL_PROVIDER` fehlt oder ist leer, oder SalesDesk wurde nach der Änderung nicht neu gestartet `up -d`
`401` (Graph)	Clientschlüssel falsch, abgelaufen oder die Geheimnis-ID statt des Werts eingetragen
`403 ErrorAccessDenied` (Graph)	Berechtigung fehlt, noch nicht wirksam (bis 2 Stunden warten) oder Absender liegt außerhalb der Beschränkung
`ErrorInvalidUser` / `MailboxNotEnabledForRESTAPI` (Graph)	Absender ist eine Gruppe oder existiert nicht – freigegebenes Postfach nehmen
`535 Authentication failed` (SMTP)	Benutzername oder Passwort falsch; bei Microsoft 365 SMTP AUTH abgeschaltet – Graph nutzen
`Connection refused` / Zeitüberschreitung (SMTP)	Port falsch oder ausgehend gesperrt (manche Hoster sperren 25/465/587 – im Kundenmenü freischalten)
Mail kommt an, aber im Spam	Absender `SMTP_FROM` passt nicht zur Domain des Postfachs, oder SPF/DKIM der Domain fehlen

Anmeldung mit Microsoft (optional)

Unabhängig vom Versand können sich Mitarbeiter mit ihrem Microsoft-Konto anmelden – in der Weboberfläche und in der App. Dafür ist eine **zweite** App-Registrierung nötig (mit Umleitungs-URI). Die Schritte stehen in der Weboberfläche unter **Verwaltung › Einstellungen › Microsoft 365**, dort steht auch die Umleitungs-URI zum Kopieren:

1. Entra › **App-Registrierungen › Neue Registrierung**, Name `SalesDesk Anmeldung`, nur dieses Verzeichnis.
2. **Umleitungs-URI**: Plattform **Web**, Adresse aus SalesDesk, z. B. `https://salesdesk.ihre-firma.de/api/v1/auth/m365/callback`.
3. Geheimen Clientschlüssel anlegen und den **Wert** kopieren.
4. In SalesDesk **Verzeichnis-ID**, **Anwendungs-ID** und **Wert** eintragen, **Anmeldung mit Microsoft anbieten** einschalten, mit Ihrem Passwort bestätigen.
5. Optional: **Neue Mitarbeiter dürfen sich selbst registrieren** für Ihre E-Mail-Domain – jedes neue Konto belegt einen Lizenzplatz.

Die normale Anmeldung mit E-Mail und Passwort bleibt immer bestehen.

Schlüssel erneuern

Geheime Clientschlüssel laufen ab (meist nach 24 Monaten). Rechtzeitig vorher: neuen Schlüssel in Entra anlegen, in `prod.env` bei `GRAPH_CLIENT_SECRET` eintragen bzw. in **Einstellungen › Microsoft 365** neu speichern, SalesDesk mit `up -d` neu starten, `mail-test` ausführen – danach den alten Schlüssel in Entra löschen.

Updates einspielen

Neue Versionen per Weboberfläche oder Installationsdatei einspielen – mit automatischer Sicherung und Rückfall auf die alte Version.

Wo erfahre ich von neuen Versionen?

- Im Download-Bereich steht immer die aktuelle Server-Version mit Datum. Die Änderungen jeder Version stehen in der Datei `CHANGELOG.md` im Installationsordner.
- Die installierte Version sehen Sie in der Weboberfläche unter **Verwaltung › Updates** oder auf dem Server mit `cat /opt/salesdesk/VERSION`.
- Die App aktualisiert sich über den App Store bzw. Google Play. Ältere Apps funktionieren mit neueren Servern weiter; umgekehrt kann eine sehr neue App einen aktuellen Server voraussetzen und sagt das dann.

> Spielen Sie Updates zeitnah ein – sie enthalten auch Sicherheitskorrekturen. Ein guter Zeitpunkt ist außerhalb der Arbeitszeit; SalesDesk ist beim Update 1–5 Minuten nicht erreichbar. Die App arbeitet in der Zeit offline weiter und gleicht danach ab.

Weg 1: über die Weboberfläche (empfohlen)

Sie brauchen das **Update-Paket** `salesdesk-update-<Version>.tar.gz` aus dem Download-Bereich und ein Konto mit der Berechtigung für Updates (Administrator).

1. **Verwaltung › Updates** öffnen.
2. Bei **Update-Paket hochladen** die Datei wählen.
3. **Ihr Passwort zur Bestätigung** eingeben und **Update einspielen** klicken.
4. Es erscheint „Version … wartet auf den Update-Dienst …“, dann „Update auf … läuft – SalesDesk startet dabei kurz neu.“ Lassen Sie die Seite offen.
5. Nach 1–5 Minuten: **„Update auf … erfolgreich eingespielt.“** Die Seite lädt neu und zeigt die neue Version.

Das passiert dabei automatisch auf dem Server:

1. Das Paket wird auf dem Server erneut geprüft (Aufbau, Dateitypen, Größe, Version).
2. Die **Datenbank wird gesichert**.
3. Die bisherige Version wird beiseitegelegt.
4. Die neuen Programmdateien werden eingespielt, SalesDesk neu gebaut und gestartet; Änderungen an der Datenbank laufen automatisch.
5. SalesDesk wird geprüft. **Schlägt etwas fehl, läuft automatisch die vorherige Version weiter** und die Seite zeigt „Update … fehlgeschlagen“ mit dem Protokoll. Die Datenbank wird dabei nicht zurückgesetzt; die Sicherung von vor dem Update steht im Protokoll, falls sie gebraucht wird.

⚠ Ein Update über die Weboberfläche tauscht nur das Programm aus. Die Server-Einrichtung (Ordner `deploy/`: Webserver, Sicherung, Skripte, `prod.env` bleibt unverändert. Neue Werkzeuge der Server-Einrichtung kommen nur mit **Weg 2** auf den Server. Steht im Änderungsprotokoll einer Version „Installationsdatei erneut ausführen“, nehmen Sie Weg 2.

Erscheint stattdessen „Updates über die Weboberfläche sind auf diesem Server noch nicht eingerichtet“ oder „Der Update-Dienst hat das Paket noch nicht übernommen“, prüfen Sie den Update-Dienst:

```
systemctl status salesdesk-update.path
systemctl enable --now salesdesk-update.path
```

Weg 2: Installationsdatei erneut ausführen

Die Installationsdatei erkennt eine vorhandene Installation und aktualisiert sie. **Daten, Einstellungen und `prod.env` bleiben erhalten.**

```
cd /root
curl -fLO https://salesdesk-app.iks-solutions.com/download/files/salesdesk-installer-
latest.sh
sha256sum salesdesk-installer-latest.sh
sudo bash salesdesk-installer-latest.sh
```

Ausgabe am Anfang:

```
== 1/8 Angaben ==
Vorhandene Installation in /opt/salesdesk gefunden → UPDATE (Daten und prod.env bleiben
erhalten).
...
== 3/8 Dateien nach /opt/salesdesk ==
Backup der Datenbank vor dem Update ...
Backup fertig: /srv/backup/salesdesk/salesdesk-20261102T091500Z
```

Es werden keine Fragen gestellt (außer bei neuen Funktionen, die eine Angabe brauchen). Eine Kopie der bisherigen `prod.env` legt die Installation zusätzlich unter `/root/salesdesk-prod.env.<Datum>` ab.

Bricht die Installation mit „Die Sicherung vor dem Update ist fehlgeschlagen“ ab, wurde **nichts geändert**. Meist ist die Festplatte voll `df -h` oder ein Container läuft nicht `docker compose … ps`. Siehe Fehlersuche.

Nach dem Update prüfen

```
cat /opt/salesdesk/VERSION
curl -s https://salesdesk.ihre-firma.de/api/v1/health
```

In der Weboberfläche anmelden und kurz eine Liste öffnen. In der App **Mehr › Synchronisierung › Jetzt abgleichen**.

Zurück zur vorherigen Version

Ist nach einem erfolgreichen Update etwas nicht in Ordnung:

1. Melden Sie sich bei IKS (siehe Kontakt – meist ist eine Korrektur schneller als ein Rückschritt.
2. Ein Zurück auf die alte Version heißt: alte Installationsdatei ausführen **und** die Sicherung von vor dem Update einspielenWiederherstellung, weil die Datenbank bereits auf den neuen Stand gebracht wurde. Änderungen seit dem Update gehen dabei verloren.

Protokolle

Was	Wo
Update über die Weboberfläche	`/opt/salesdesk/updates/update.log` und in der Weboberfläche unter **Protokoll**
Update per Installationsdatei	`/var/log/salesdesk-install.log`
Sicherung vor dem Update	`/srv/backup/salesdesk/salesdesk-<Datum>`

Datensicherung und Wiederherstellung

Tägliche Sicherung prüfen, auf ein zweites System kopieren, verschlüsseln, im Notfall wiederherstellen und die Wiederherstellung üben.

Was wird gesichert?

Jede Nacht um **02:00** sichert der Server automatisch:

Datei	Inhalt
`db.dump`	die komplette Datenbank (alle Firmen, Kontakte, Leads, Berichte, Benutzer, Einstellungen)
`files.tar.gz`	alle hochgeladenen Dateien (Fotos, Visitenkarten, Anhänge, Logos)
`alembic_version.txt`	Stand der Datenbankstruktur – für die passende Programmversion beim Einspielen
`SHA256SUMS`	Prüfsummen, um Beschädigungen zu erkennen

Ziel ist `/srv/backup/salesdesk/salesdesk-<Datum und Uhrzeit in UTC>`, z. B. `salesdesk-20261102T010000Z`. Sicherungen älter als **30 Tage** werden um 04:15 gelöscht.

> ⚠ Die Datei `/opt/salesdesk/deploy/prod.env` ist **nicht** Teil der Sicherung, weil sie die Schlüssel enthält. Bewahren Sie eine Kopie im Passwort-Tresor auf. Ohne die Schlüssel daraus lassen sich auf einem neuen Server gespeicherte Zugangsdaten (Microsoft 365, Schnittstellen) und die **Zwei-Faktor-Anmeldungen** nicht mehr lesen – jeder Benutzer müsste die Zwei-Faktor-Anmeldung neu einrichten.

Prüfen, ob die Sicherung läuft

```
ls -lt /srv/backup/salesdesk | head
tail -5 /var/log/salesdesk-backup.log
```

Die oberste Zeile muss die Sicherung der letzten Nacht sein; im Protokoll steht `Backup fertig: /srv/backup/salesdesk/salesdesk-…`. Eine Sicherung **sofort** anlegen:

```
cd /opt/salesdesk
BACKUP_DIR=/srv/backup/salesdesk SALESDESK_COMPOSE=deploy/docker-compose.plesk.yml bash
deploy/backup-docker.sh
```

Sind die nächtlichen Sicherungen verschlüsselt, stellen Sie `BACKUP_GPG_RECIPIENT=<Schlüssel-ID>` vor den Befehl – sonst ist diese Sicherung unverschlüsselt.

Zusätzlich lädt der Server-Administrator in der Weboberfläche unter **Verwaltung › Server** eine **SQL-Sicherung** der Datenbank herunter – praktisch vor größeren Änderungen.

Zeitplan und Aufbewahrung ändern

Der Zeitplan steht in `/etc/cron.d/salesdesk`:

```
BACKUP_DIR=/srv/backup/salesdesk
BACKUP_KEEP_DAYS=30
BACKUP_GPG_RECIPIENT=
0 2 * * *  root  cd /opt/salesdesk && ./deploy/backup-docker.sh >> /var/log/salesdesk-backup.log 2>&1
```

`BACKUP_KEEP_DAYS` legt fest, wie viele Tage Sicherungen bleiben. Die Uhrzeit ändern Sie in der Zeile `0 2 * * *` (Minute, Stunde). Aufbewahrung, GPG-Schlüssel und Uhrzeit bleiben bei Updates erhalten; **andere eigene Zeilen in dieser Datei nicht** – die legen Sie in einer eigenen Datei ab (siehe unten).

Auf ein zweites System kopieren (wichtig)

Eine Sicherung auf demselben Server schützt nicht vor einem Ausfall des Servers. Kopieren Sie die Sicherungen jede Nacht auf ein anderes System. Drei bewährte Wege:

a) Auf einen anderen Linux-Server oder ein NAS per rsync

Einmalig einen SSH-Schlüssel anlegen und auf das Ziel kopieren:

```
ssh-keygen -t ed25519 -N "" -f /root/.ssh/salesdesk_backup
ssh-copy-id -i /root/.ssh/salesdesk_backup.pub backup@nas.ihre-firma.de
```

Dann eine **eigene** Datei `/etc/cron.d/salesdesk-kopie` mit dieser Zeile anlegen (03:30, nach der Sicherung; z. B. mit `nano /etc/cron.d/salesdesk-kopie`. In einer eigenen Datei bleibt sie bei Updates erhalten:

```
30 3 * * * root rsync -a --delete -e "ssh -i /root/.ssh/salesdesk_backup" /srv/backup/salesdesk/ backup@nas.ihre-firma.de:salesdesk/ >> /var/log/salesdesk-backup.log 2>&1
```

b) Plesk-Backup-Manager

In Plesk unter **Werkzeuge & Einstellungen › Backup Manager › Einstellungen für Remote-Speicher** ein externes Ziel (FTP, S3, Google Drive …) einrichten und eine geplante Sicherung des **ganzen Servers** anlegen, die `/srv/backup` einschließt.

c) Sicherung Ihrer Virtualisierung

Läuft SalesDesk in einer VM (Hyper-V, VMware, Proxmox), sichern Sie zusätzlich die ganze VM mit Ihrer üblichen Lösung. Die SalesDesk-Sicherung bleibt trotzdem wichtig – sie lässt sich einzeln und auf jedem Server einspielen.

Sicherungen verschlüsseln (empfohlen, wenn sie das Haus verlassen)

Die Sicherung enthält alle Kundendaten. Mit GPG wird sie so verschlüsselt, dass nur der Besitzer des **privaten Schlüssels** sie öffnen kann – und der liegt **nicht** auf dem Server.

1. Auf einem **anderen** Rechner (z. B. Linux-PC oder Windows mit Gpg4win) ein Schlüsselpaar erzeugen:

```
gpg --quick-generate-key "SalesDesk Sicherung <it@ihre-firma.de>" rsa4096 encrypt never
gpg --armor --export it@ihre-firma.de > salesdesk-sicherung.pub
gpg --armor --export-secret-keys it@ihre-firma.de > salesdesk-sicherung-PRIVAT.asc
```

2. Die Datei `salesdesk-sicherung-PRIVAT.asc` und das Kennwort **sicher verwahren** (Tresor, zwei Orte). Ohne sie sind verschlüsselte Sicherungen wertlos.
3. Nur den **öffentlichen** Schlüssel auf den Server kopieren und dort importieren:

```
gpg --import salesdesk-sicherung.pub
gpg --list-keys
```

4. Die angezeigte Schlüssel-ID (40 Zeichen) in `/etc/cron.d/salesdesk` eintragen: `BACKUP_GPG_RECIPIENT=<Schlüssel-ID>`.
5. Prüfen: In der nächsten Sicherung heißen die Dateien `db.dump.gpg` und `files.tar.gz.gpg`.

Wiederherstellen

So holen Sie einen früheren Stand zurück – z. B. nach versehentlichem Löschen vieler Daten oder auf einem neuen Server.

> Einzelne gelöschte Einträge holen Sie einfacher aus dem **Papierkorb** der Weboberfläche zurück (Verwaltung › Papierkorb) – ohne Wiederherstellung.

Auf demselben Server

```
cd /opt/salesdesk
ls /srv/backup/salesdesk
bash deploy/restore-docker.sh /srv/backup/salesdesk/salesdesk-20261102T010000Z
```

Das Skript fragt nach einer BestätigungJA eingeben) und arbeitet dann sieben Schritte ab. Dabei wird **nichts gelöscht**:

```
== 1/7 Sicherung prüfen: /srv/backup/salesdesk/salesdesk-20261102T010000Z ==
Sicherung in Ordnung (Datenbankstand 0042_...).
Die Daten auf diesem Server werden durch den Stand der Sicherung ersetzt (der jetzige Stand
bleibt als Rückweg erhalten).
Fortfahren? Bitte JA eingeben: JA
== 2/7 Aktuellen Stand sichern ==
Backup fertig: /srv/backup/salesdesk/salesdesk-20261102T143000Z
== 3/7 SalesDesk anhalten ==
== 4/7 Aktuelle Datenbank umbenennen → salesdesk_vor_wiederherstellung_20261102153000 ==
== 5/7 Datenbank einspielen ==
Datenbank eingespielt.
== 6/7 Dateien einspielen ==
Dateien eingespielt (bisherige Dateien liegen im Volume unter .vor-wiederherstellung-
20261102153000).
== 7/7 Starten und prüfen ==
FERTIG: Sicherung vom 20261102T010000Z ist wiederhergestellt.
```

Am Ende zeigt das Skript die Befehle für den **Rückweg**, falls der vorherige Stand doch gebraucht wird. Tritt unterwegs ein Fehler auf, holt das Skript die bisherige Datenbank automatisch zurück und startet SalesDesk wieder. Geschieht der Fehler erst beim Einspielen der Dateien (Schritt 6), liegen die bisherigen Dateien im Volume unter `.vor-wiederherstellung-<Zeit>` – melden Sie sich dann bei IKS.

Für **verschlüsselte** Sicherungen muss der **private** GPG-Schlüssel auf dem Rechner importiert sein, auf dem Sie wiederherstellen `gpg --import salesdesk-sicherung-PRIVAT.asc`. Entfernen Sie ihn danach wieder `gpg --delete-secret-keys <Schlüssel-ID>`.

Auf einem neuen Server (Umzug oder Totalausfall)

1. Neuen Server vorbereiten und SalesDesk mit **derselben Adresse** installierenInstallation. Bei „Erster Administrator“ **2** wählen – die Firma kommt ja aus der Sicherung.
2. Die Werte `JWT_SECRET` und `INTEGRATION_SECRET_KEY` aus Ihrer gesicherten `prod.env` in die neue `/opt/salesdesk/deploy/prod.env` übernehmen. Ebenso die Einstellungen für den E-Mail-Versand `EMAIL_PROVIDER`, `SMTP_…` bzw. `GRAPH_…` und ggf. `MERP_…`, falls Sie sie bei der Neuinstallation nicht eingegeben haben. Die Datenbank-Passwörter des neuen Servers bleiben. Dann `cd /opt/salesdesk && docker compose -f deploy/docker-compose.plesk.yml --env-file deploy/prod.env up -d`.
3. Sicherungsordner auf den neuen Server kopieren, z. B. nach `/srv/backup/salesdesk/`.
4. `cd /opt/salesdesk && bash deploy/restore-docker.sh /srv/backup/salesdesk/salesdesk-<Datum>` ausführen.
5. DNS-Eintrag auf die IP des neuen Servers umstellen. Die Apps verbinden sich danach von selbst wieder; die Lizenz gilt weiter, weil die Adresse gleich bleibt.

Mit eigener (externer) Datenbank

Nutzt SalesDesk Ihren eigenen PostgreSQL-Server, spielen Sie die Sicherung mit `scripts/restore.sh` in eine **leere** Datenbank ein und stellen danach `DATABASE_URL_EXTERNAL` in `prod.env` auf diese Datenbank um. Auf dem Server müssen dafür `psql` und `pg_restore` ab **Version 16** installiert sein (Paket `postgresql-client-16` bzw. `postgresql16`:

```
DATABASE_URL=postgresql://benutzer:passwort@dbserver/salesdesk_neu
STORAGE_LOCAL_PATH=/srv/restore/dateien \
  sh /opt/salesdesk/scripts/restore.sh /srv/backup/salesdesk/salesdesk-20261102T010000Z
```

Die Dateien landen dabei im Ordner `/srv/restore/dateien`. Danach kopieren Sie sie in SalesDesk:

```
cd /opt/salesdesk
tar -C /srv/restore/dateien -czf - . | docker compose -f deploy/docker-compose.plesk.yml --
env-file deploy/prod.env run --rm --no-deps -T api sh -c "cd /app/data && tar -xzf -"
docker compose -f deploy/docker-compose.plesk.yml --env-file deploy/prod.env up -d
```

Wiederherstellung üben

Eine Sicherung ist erst etwas wert, wenn die Wiederherstellung geklappt hat. Üben Sie **einmal im Quartal** auf einem Testsystem (z. B. einer kleinen VM): SalesDesk installieren, eine aktuelle Sicherung einspielen, anmelden, Stichproben prüfen. Notieren Sie Datum und Ergebnis – das ist auch der Nachweis für Ihre Datenschutz-Dokumentation (Art. 32 DSGVO).

Betrieb, Wartung und Sicherheit

Die wichtigsten Befehle, Überwachung, Passwort zurücksetzen, mehrere Firmen und Instanzen, Server-Absicherung, Umzug und Deinstallation.

Die wichtigsten Befehle

Alle Befehle als root im Installationsordner. Damit es kürzer wird, legen Sie einmal eine Abkürzung an:

```
cd /opt/salesdesk
alias sd='docker compose -f deploy/docker-compose.plesk.yml --env-file deploy/prod.env'
```

Die Abkürzung `sd` gilt bis zum Abmelden. Dauerhaft: die `alias`-Zeile an das Ende von `/root/.bashrc` anhängen.

Aufgabe	Befehl
Zustand aller Teile	`sd ps`
Läuft SalesDesk?	`curl -s http://127.0.0.1:8088/api/v1/health` → `{"status":"ok"}`
Protokoll der API (letzte 100 Zeilen)	`sd logs --tail 100 api`
Protokoll live mitlesen (Ende mit Strg+C)	`sd logs -f api web`
Neu starten	`sd restart`
Nach Änderung an `prod.env` übernehmen	`sd up -d`
Anhalten / starten	`sd stop` / `sd up -d`
Passwort eines Benutzers neu setzen	`sd exec api python -m app.cli set-password --email name@ihre-firma.de`
Testmail senden	`sd exec api python -m app.cli mail-test --to name@ihre-firma.de`
Weitere Firma anlegen	`sd exec api python -m app.cli create-org --name "Firma" --admin-email a@b.de --admin-name "Name"`
Sicherung jetzt	`BACKUP_DIR=/srv/backup/salesdesk SALESDESK_COMPOSE=deploy/docker-compose.plesk.yml bash deploy/backup-docker.sh`
Installierte Version	`cat VERSION`
Speicherplatz	`df -h /` und `docker system df`
Alte Docker-Images aufräumen	`docker image prune -f`



Das Passwort des **Administrators** vergessen und keine zweite Verwaltung vorhanden? Dafür ist `set-password` da – es fragt das neue Passwort zweimal ab und meldet alle Geräte dieses Benutzers ab.

Überwachung

- Adresse für Ihre Überwachung (z. B. Uptime-Kuma, PRTG, Checkmk): `https://salesdesk.ihre-firma.de/api/v1/health` – Antwort `{"status":"ok"}` mit HTTP 200.
- Festplatte: Warnung ab 80 % Belegung. Sicherungen und Fotos wachsen mit der Zeit.
- Zertifikat: Plesk und Caddy verlängern automatisch; certbot ebenfalls `systemctl list-timers | grep certbot`. Eine Überwachung des Ablaufdatums schadet nicht.
- Sicherung: Täglich prüfen, ob eine neue Sicherung entstanden ist (z. B. Alter des neuesten Ordners in `/srv/backup/salesdesk` < 26 Stunden).

Server-Neustart

SalesDesk startet nach einem Neustart des Servers **von selbst** (Docker-Einstellung `restart: unless-stopped`). Prüfen Sie nach dem Neustart mit `sd ps`, dass alle vier Teile laufen.

Betriebssystem aktuell halten

System	Sicherheitsupdates automatisch	von Hand
Ubuntu / Debian	`apt-get install -y unattended-upgrades` (bei Ubuntu Standard)	`apt-get update && apt-get -y upgrade`
AlmaLinux / Rocky	`dnf install -y dnf-automatic && systemctl enable --now dnf-automatic-install.timer`	`dnf -y upgrade`
Plesk	Werkzeuge & Einstellungen › Aktualisierungen	–

Nach Kernel-Updates einmal neu starten (z. B. nachts). Docker-Updates aus der Paketverwaltung sind unbedenklich; SalesDesk startet danach wieder.

Server absichern

- **SSH mit Schlüssel** statt Passwort; danach in `/etc/ssh/sshd_config` `PasswordAuthentication no` setzen und `systemctl restart sshd` (vorher prüfen, dass die Anmeldung mit Schlüssel klappt).
- **Fail2ban** gegen Passwort-Raten: `apt-get install -y fail2ban` bzw. `dnf install -y fail2ban && systemctl enable --now fail2ban`. Plesk bringt das als „IP Address Banning“ mit.
- **Firewall**: eingehend nur 22 (am besten nur von Ihrer Firmen-IP), 80 und 443. SalesDesk selbst ist nur über `127.0.0.1` erreichbar.
- In SalesDesk: **Zwei-Faktor-Pflicht** für Verwaltungsrollen einschalten (Verwaltung › Einstellungen › Sicherheit und Datenschutz).
- `prod.env` ist nur für root lesbar – so lassen.

Mehrere Firmen auf einem Server

Ein SalesDesk-Server kann mehrere, streng getrennte Firmen führen – z. B. für Tochterfirmen. Der Server-Administrator legt sie in der Weboberfläche unter **Verwaltung › Server** an (Name, Administrator, Start-Passwort), kann sie umbenennen, sperren und entsperren. Jede Firma braucht eine **eigene Lizenz**.

Mehrere Instanzen auf einem Server

Für eine völlig getrennte zweite Installation (eigene Datenbank, eigene Adresse, z. B. Test- und Echtsystem) installieren Sie mit eigenem Namen, Ordner und Port:

```
sudo SD_INSTANCE=salesdesk-test SD_DIR=/opt/salesdesk-test SD_PORT=8090 bash salesdesk-installer-latest.sh
```

Name und Port merkt sich die Installation. Den **Ordner** geben Sie bei Updates per Installationsdatei immer wieder mit an `SD_DIR=/opt/salesdesk-test bash salesdesk-installer-latest.sh` – sonst wird die Hauptinstanz in `/opt/salesdesk` aktualisiert. Updates über die Weboberfläche finden die Instanz von selbst. Sicherungen liegen unter `/srv/backup/salesdesk-test`, der Zeitplan in `/etc/cron.d/salesdesk-test`. Für die Befehle oben dann `cd /opt/salesdesk-test`, Port `8090` und bei der Sicherung `BACKUP_DIR=/srv/backup/salesdesk-test` verwenden.

Umzug auf einen anderen Server

1. Auf dem alten Server eine Sicherung anlegen (siehe Datensicherung.
2. Auf dem neuen Server SalesDesk mit derselben Adresse installieren und die Sicherung einspielen – Abschnitt „Auf einem neuen Server“.
3. DNS auf den neuen Server umstellen, eine Stunde warten, prüfen.
4. Alten Server erst abschalten, wenn alles läuft.

Die **Lizenz** ist an die Adresse gebunden, nicht an die Maschine – sie zieht mit um. Ändert sich die Adresse, schreiben Sie IKS wegen einer neuen Lizenzdatei; ein Store-Abo überträgt die App bei der nächsten Anmeldung neu.

Deinstallieren

⚠ Das löscht alle SalesDesk-Daten auf diesem Server endgültig. Vorher eine Sicherung anlegen und auf ein anderes System kopieren.

```
cd /opt/salesdesk
docker compose -f deploy/docker-compose.plesk.yml --env-file deploy/prod.env down -v
docker rm -f salesdesk-proxy 2>/dev/null; docker volume rm salesdesk-proxy-data salesdesk-
proxy-config 2>/dev/null
systemctl disable --now salesdesk-update.path
rm -f /etc/systemd/system/salesdesk-update.* /etc/cron.d/salesdesk
rm -rf /opt/salesdesk /etc/salesdesk-proxy
```

Die Sicherungen in `/srv/backup/salesdesk` bleiben, bis Sie sie selbst löschen. Bei Plesk die Subdomain in Plesk entfernen. Ein Store-Abo kündigen Sie in den Abo-Einstellungen Ihres Apple- bzw. Google-Kontos.

Fehlersuche

Jede bekannte Fehlermeldung von SSH über Installation, Zertifikat und Start bis Update, Sicherung und Anmeldung – mit Ursache und Lösung.

Suchen Sie mit **Strg+F** im Browser nach einem Wort aus Ihrer Fehlermeldung. Hilft nichts davon, schicken Sie IKS das Protokoll `/var/log/salesdesk-install.log` bzw. die Ausgabe von `sd logs --tail 200 api` (siehe Wartung – vorher Passwörter und Schlüssel darin unkenntlich machen.

Verbindung zum Server (SSH)

Meldung	Ursache und Lösung
`Connection closed by …` direkt nach dem Verbinden	Mit dem **Domainnamen** verbunden, der über einen anderen Dienst läuft. Mit der **IP-Adresse** verbinden: `ssh root@203.0.113.25`.
`Connection timed out`	IP falsch, Server aus, oder Port 22 in der Firewall des Hosters gesperrt.
`Permission denied (publickey)`	Der Server erlaubt nur SSH-Schlüssel. Mit dem Benutzer und Schlüssel anmelden, den der Hoster vorgibt, dann `sudo -i`.
`Permission denied, please try again`	Passwort falsch. Beim Tippen sind keine Zeichen zu sehen – langsam neu eingeben oder mit Rechtsklick einfügen.
`WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`	Der Server wurde neu installiert. Auf **Ihrem PC**: `ssh-keygen -R 203.0.113.25`, dann neu verbinden.
`ssh: The term 'ssh' is not recognized` (Windows)	Sehr altes Windows: Einstellungen › Apps › Optionale Features › **OpenSSH-Client** hinzufügen, oder PuTTY verwenden.
Befehl tut nichts / falsches Fenster	Steht vorne `PS C:\…>`, sind Sie auf Ihrem PC. Installationsbefehle gehören auf den Server `root@…`. `scp` dagegen läuft auf dem PC.
Mehrere eingefügte Zeilen laufen durcheinander	Befehle einzeln einfügen und jeweils auf die Eingabezeile warten.

Laden und Starten der Installation

Meldung	Ursache und Lösung
`curl: (22) The requested URL returned error: 404`	Adresse falsch abgetippt. Befehl aus dem Download-Bereich kopieren.
`curl: (6) Could not resolve host`	Der Server hat kein DNS/Internet. Netzwerk des Servers prüfen oder Datei per `scp`/WinSCP hochladenVorbereitung.
Prüfsumme weicht ab	Download unvollständig oder verändert. Datei löschen `rm salesdesk-installer-latest.sh`, neu laden. Nicht starten.
`Bitte als root ausführen`	Mit `sudo bash …` starten oder vorher `sudo -i`.
`Programm tar fehlt` (bzw. base64, curl)	`apt-get install -y tar curl coreutils` bzw. `dnf install -y tar curl coreutils`.
`SD_INSTANCE darf nur a-z, 0-9 und - enthalten`	Instanzname ohne Großbuchstaben, Leerzeichen und Sonderzeichen wählen.

Docker

Meldung	Ursache und Lösung
AlmaLinux/Rocky: Konflikt mit `podman` oder `buildah`	Die Installation nutzt `--allowerasing` und ersetzt podman. Erscheint der Fehler trotzdem: `dnf remove -y podman buildah`, dann erneut starten.
`Cannot connect to the Docker daemon`	Docker läuft nicht: `systemctl enable --now docker`, dann `systemctl status docker`.
`toomanyrequests: You have reached your pull rate limit`	Docker Hub begrenzt anonyme Downloads. 6 Stunden warten oder mit einem kostenlosen Docker-Konto anmelden: `docker login`.
`no space left on device`	Festplatte voll: `df -h`. Platz schaffen`docker image prune -f`, alte Sicherungen verschieben) und erneut starten.
Bau bricht mit `Killed` oder `exit code 137` ab	Zu wenig Arbeitsspeicher. Mindestens 4 GB, oder eine Auslagerungsdatei anlegen: `fallocate -l 4G /swapfile && chmod 600 /swapfile && mkswap /swapfile && swapon /swapfile`.

SalesDesk startet nicht

Meldung	Ursache und Lösung	
`Port 8088 ist schon belegt`	Eine andere Anwendung oder zweite Instanz nutzt den Port. `ss -ltnp`	grep 8088 `zeigt welche. Andere Instanz: mit` SD_PORT=8090` installieren.
`SalesDesk startet nicht. Protokoll:`	Die letzten Zeilen darunter lesen. Häufig: Datenbank nicht erreichbar (bei eigener Datenbank Adresse/Passwort/Firewall prüfen) oder zu wenig Speicher.	
`POSTGRES_PASSWORD fehlt`	`prod.env` fehlt oder ist leer. Sicherungskopie aus `/root/salesdesk-prod.env.<Datum>` oder dem Tresor zurücklegen.	
`password authentication failed for user "salesdesk"`	`POSTGRES_PASSWORD` in `prod.env` wurde nachträglich geändert. Den ursprünglichen Wert zurückschreiben – das Passwort der bestehenden Datenbank ändert sich dadurch nicht.	
API startet, Weboberfläche zeigt nur weiße Seite	Browser-Zwischenspeicher: Seite mit **Strg+F5** neu laden.	
Eigene Datenbank: `permission denied for schema public`	Die Datenbank muss dem SalesDesk-Benutzer **gehören**: `CREATE DATABASE salesdesk OWNER salesdesk;`	

Webserver, Zertifikat und Erreichbarkeit

Meldung	Ursache und Lösung
`Von außen noch nicht erreichbar – DNS/Zertifikat prüfen`	SalesDesk läuft, der Weg von außen fehlt. Der Reihe nach: `nslookup` (zeigt die richtige IP?), Hoster-Firewall (80/443 offen?), dann Kapitel Webserver.
Let's Encrypt: `DNS problem: NXDOMAIN`	DNS-Eintrag fehlt oder gilt noch nicht. Warten, mit `nslookup` prüfen, Installation erneut starten.
Let's Encrypt: `Timeout during connect (likely firewall problem)`	Port 80 von außen gesperrt. Hoster-Firewall bzw. Router prüfen.
Let's Encrypt schlägt fehl, obwohl IPv4 stimmt	Es gibt einen **AAAA-Eintrag** (IPv6), der nicht zum Server führt. AAAA löschen oder richtig setzen.
`Too many certificates already issued`	Zu viele Versuche für diese Adresse in einer Woche. Einige Tage warten; bis dahin nichts weiter versuchen.
Caddy: „Noch kein Zertifikat“	`docker logs --tail 40 salesdesk-proxy` lesen. Meist DNS oder Port 80. Caddy versucht es selbstständig weiter.
Plesk: `duplicate location "/"`	Proxy-Modus der Subdomain ist noch an. **Apache- & nginx-Einstellungen › Proxy-Modus** ausschalten.
Plesk-Standardseite statt SalesDesk	Weiterleitung fehlt. Installation erneut starten oder Weg A „von Hand“Webserver.
`502 Bad Gateway`	Der Webserver läuft, SalesDesk nicht. `sd ps`, `sd logs --tail 100 api`.
`504 Gateway Timeout` bei großen Exporten	Zeitlimit des eigenen Webservers zu kurz – auf 300 Sekunden setzen.
`413 Request Entity Too Large` beim Hochladen	Upload-Grenze im eigenen nginx zu klein – `client_max_body_size 50m;`
Browser: „Die Verbindung ist nicht sicher“	Zertifikat fehlt, ist abgelaufen oder gilt für eine andere Adresse. Plesk: SSL/TLS-Zertifikate; Caddy: Protokoll; certbot: `certbot renew`.
SELinux (AlmaLinux/Rocky) mit eigenem nginx/Apache: 502	`setsebool -P httpd_can_network_connect 1`

Meldung	Ursache und Lösung
Aus dem Firmennetz nicht erreichbar, von außen schon	Router kann die eigene öffentliche IP nicht „zurück“ ansprechen (NAT-Loopback). Internen DNS-Eintrag auf die interne IP des Servers anlegen.

Updates

Meldung	Ursache und Lösung
Installation endet nach `Backup der Datenbank vor dem Update ...` ohne weitere Meldung	Betrifft Installationsdateien **vor 0.22**. Mit der aktuellen Datei erneut starten – sie meldet den Grund. Für die alte Datei: `cd /opt/salesdesk && SALESDESK_COMPOSE=deploy/docker-compose.plesk.yml bash -x deploy/backup-docker.sh` zeigt, woran es hängt.
`Die Sicherung vor dem Update ist fehlgeschlagen – Update abgebrochen, nichts geändert`	Meist Festplatte voll oder Datenbank-Container gestoppt `sd ps`, `sd up -d`. Danach erneut starten.
Weboberfläche: „Updates … noch nicht eingerichtet“	Update-Dienst fehlt. Einmal die Installationsdatei per SSH ausführen.
Weboberfläche: „Der Update-Dienst … hat das Paket noch nicht übernommen“	`systemctl status salesdesk-update.path` – nicht aktiv? `systemctl enable --now salesdesk-update.path`.
„Update … fehlgeschlagen – die vorherige Version läuft weiter“	Das Programm läuft in der alten Version weiter. Hatte die neue Version die Datenbank schon umgestellt, steht im Protokoll die Sicherung von vor dem Update – IKS sagt Ihnen, ob sie eingespielt werden muss. **Protokoll** in der Weboberfläche bzw. `/opt/salesdesk/updates/update.log` an IKS senden.
„Paket ist kein gültiges .tar.gz“ oder abgelehnt	Hochgeladen werden darf nur das Update-Paket `salesdesk-update-<Version>.tar.gz` – nicht die Installationsdatei (.sh) und nicht das Gesamt-ZIP.

Sicherung und Wiederherstellung

Meldung	Ursache und Lösung
Keine neue Sicherung in `/srv/backup/salesdesk`	`tail -30 /var/log/salesdesk-backup.log`. Gibt es `/etc/cron.d/salesdesk`? Läuft cron `systemctl status cron` bzw. `crond`?
`gpg: … There is no assurance this key belongs to the named user`	Betrifft Sicherungsskripte vor 0.22. Installationsdatei erneut ausführen (aktualisiert die Skripte).
`gpg: … No public key`	`BACKUP_GPG_RECIPIENT` passt zu keinem importierten Schlüssel. `gpg --list-keys` prüfen.
`Prüfsummen stimmen nicht`	Sicherung beschädigt oder unvollständig kopiert. Eine andere Sicherung nehmen; Kopiervorgang prüfen.
`Entschlüsseln fehlgeschlagen`	Der **private** GPG-Schlüssel ist auf diesem Rechner nicht importiert.
`Diese Installation nutzt eine eigene (externe) Datenbank`	Wiederherstellung mit `scripts/restore.sh` in eine leere DatenbankDatensicherung.

E-Mail-Versand

Alle Fehlermeldungen von `mail-test` stehen im Kapitel E-Mail-Versand, Abschnitt „Übernehmen und testen“.

Anmeldung, Lizenz und App

Meldung	Ursache und Lösung
Administrator-Passwort vergessen	Zweiter Administrator setzt es unter **Verwaltung › Benutzer** neu. Sonst: `sd exec api python -m app.cli set-password --email …`
Zwei-Faktor: Telefon und Wiederherstellungscodes verloren	Anderer Administrator: **Benutzer › 2FA zurücksetzen**. Einziger Administrator: `sd exec api python -m app.cli reset-mfa --email …`
„Zu viele Versuche. Bitte später erneut versuchen.“	Schutz gegen Passwort-Raten nach 5 Fehlversuchen. 5 Minuten warten.
„Ersteinrichtung“ erscheint nicht, nur Anmeldung	Es gibt schon eine Firma, oder `SETUP_TOKEN` in `prod.env` ist leer. Administrator im Terminal mit `create-org` anlegen.
`Der Einrichtungsschlüssel ist falsch`	`grep SETUP_TOKEN /opt/salesdesk/deploy/prod.env` – genau diesen Wert eingeben.
Lizenz: „Diese Lizenz gilt für einen anderen Server“	Lizenzdatei ist an eine andere Adresse gebunden. IKS mit der richtigen Adresse um eine neue Datei bitten.
Lizenz: „Diese Lizenzdatei passt nicht zu diesem Server“	Eine Cloud-Lizenz wurde auf dem eigenen Server hochgeladen (oder umgekehrt). Für den Firmenserver eine Team-Server-Lizenz anfordern.
Lizenz: „Diese Lizenzdatei ist abgelaufen“	Neue Datei bei IKS anfordern (Jahresvertrag verlängern).
Lizenz: „Es sind mehr Benutzer aktiv, als die Lizenz erlaubt“	Vor dem Hochladen einer kleineren Lizenz Benutzer deaktivieren.
„Die Lizenz ist abgelaufen – SalesDesk ist nur lesbar“	Testzeitraum bzw. Abo und Kulanzfrist sind vorbei. Lesen und Export gehen weiter; neue Lizenz hinterlegen schaltet sofort frei.
Store-Abo erscheint nicht auf dem Server	Die Person, die gekauft hat, muss sich **mit der App** als Administrator am Server anmelden – erst dann überträgt die App den Kauf.
„Alle Plätze der Lizenz sind belegt“	Jeder aktive Benutzer belegt einen Platz. Ausgeschiedene Benutzer **deaktivieren** oder größeres Paket wählen.

Meldung	Ursache und Lösung
App: „Keine Verbindung zum Server. Ihre Eingaben bleiben erhalten.“	Im Browser des Handys `https://salesdesk.ihre-firma.de/api/v1/health` öffnen. Geht das nicht: Zertifikat/DNS. Geht es: App-Adresse prüfen (ohne Pfad).
App: „Die Server-Adresse ist ungültig“	Nur den Namen eingeben, z. B. `salesdesk.ihre-firma.de` – ohne `/api` oder andere Pfade.

Fragen der IT

Datenschutz, Netzwerk, Datenbank, Lizenzprüfung, Hochverfügbarkeit, Betrieb ohne Internet, Kosten und Zuständigkeiten.

Datenschutz und Sicherheit

Hat IKS Zugriff auf unseren Server oder unsere Daten?

Nein. Die Software läuft vollständig auf Ihrem Server. Es gibt keinen Fernzugang, keine Telemetrie und keine Verbindung zu IKS. Die Lizenz wird auf dem Server mit einer digitalen Signatur geprüft – ohne Rückfrage bei IKS.

Welche Verbindungen baut der Server nach außen auf?

Ziel	Wann	abschaltbar
Docker Hub, Paketquellen des Betriebssystems	Installation und Updates	–
Let's Encrypt	Zertifikat holen und verlängern	bei eigenem Zertifikat
Ihr Mailserver bzw. Microsoft 365	E-Mail-Versand	ja (leer lassen)
OpenStreetMap (Kacheln, Adresssuche)	Kundenkarte in der Weboberfläche, über den Server mit Zwischenspeicher	ja `MAP_TILE_URL` und `MAP_GEOCODER_URL` leer)
Microsoft Entra ID	Anmeldung mit Microsoft, wenn eingerichtet	ja
Apple / Google	nur Prüfung von Store-Käufen, wenn ein Abo aus der App übertragen wird	–

Wie sind die Daten geschützt?

- Übertragung nur verschlüsselt (HTTPS); die App lehnt Server ohne HTTPS ab.
- Passwörter nur als Argon2-Hash gespeichert; optional Zwei-Faktor-Anmeldung, für Verwaltungsrollen erzwingbar.
- Gespeicherte Zugangsdaten (Microsoft 365, Schnittstellen) verschlüsselt mit `INTEGRATION_SECRET_KEY`.
- Rollen und Rechte, Sichtbarkeit nach Gebieten und Teams, Protokoll aller Änderungen (Audit).
- Datenbank und API sind von außen nicht erreichbar – nur über den Webserver.
- Aufbewahrungsfristen und Anonymisierung für die DSGVO einstellbar.

Brauchen wir einen Vertrag zur Auftragsverarbeitung mit IKS?

Beim eigenen Firmenserver nicht – IKS verarbeitet keine Daten für Sie. Anders bei der SalesDesk Cloud, dort schließen Sie den AV-Vertrag beim Anlegen der Firma ab.

Wo speichert die App Daten?

Auf dem Gerät in einer lokalen Datenbank, damit sie offline arbeitet. Anmeldedaten liegen im sicheren Schlüsselbund (iOS Keychain / Android Keystore). Deaktiviert die Verwaltung einen Benutzer, kann dieser sich nicht mehr anmelden und nicht mehr abgleichen. Für Firmengeräte empfehlen wir eine Geräteverwaltung (MDM) mit Gerätesperre.

Netzwerk und Infrastruktur

Geht es ohne Zugriff aus dem Internet, nur im Firmennetz?

Ja. Dann braucht die App aber eine Verbindung ins Firmennetz (VPN), um abzugleichen; unterwegs arbeitet sie offline weiter. Das Zertifikat ist die Hürde: Let's Encrypt braucht einmal Port 80 aus dem Internet. Ohne Internet richten Sie den Webserver mit einem Zertifikat Ihrer **eigenen Zertifizierungsstelle** ein (Weg C im Kapitel Webserver und verteilen dieses Stammzertifikat per MDM auf die Geräte – die App akzeptiert nur Zertifikate, denen das Gerät vertraut.

Kann SalesDesk hinter unserem vorhandenen Reverse-Proxy laufen (z. B. Sophos, F5, Traefik, HAProxy)?

Ja. Leiten Sie die Adresse an `http://<Server>:8088` bzw. an den Webserver auf dem Server weiter und geben Sie die Kopfzeilen `Host`, `X-Forwarded-For` und `X-Forwarded-Proto` weiter. Lauscht SalesDesk nur auf `127.0.0.1`, muss der Proxy auf demselben Rechner laufen – oder Sie installieren auf dem Server zusätzlich Caddy/nginx als Zwischenstufe.

Unterstützt SalesDesk eine eigene, vorhandene PostgreSQL-Datenbank?

Ja, ab PostgreSQL 14. Bei der Installation Auswahl **2**. Die Datenbank muss leer sein und dem SalesDesk-Benutzer gehören. Die Sicherung sichert dann diese Datenbank.

Gibt es Hochverfügbarkeit oder einen Cluster?

Nicht eingebaut. Für die üblichen Teamgrößen genügt ein Server mit täglicher Sicherung und gesicherter VM. Weil die App offline arbeitet, merken Mitarbeiter einen kurzen Ausfall kaum – sie gleichen danach ab.

Läuft SalesDesk auf ARM-Servern (z. B. Ampere)?

Die Bausteine gibt es auch für ARM, wir testen und liefern aber für x86_64. Nehmen Sie für den Echtbetrieb einen x86_64-Server.

Läuft SalesDesk auf Windows Server?

Ja, in einer Linux-VM im Hyper-V. Schritt für Schritt im Kapitel Windows Server.

Können wir Kubernetes nutzen?

Die Lieferung ist für Docker Compose gebaut. Die Container lassen sich grundsätzlich auch in Kubernetes betreiben; das ist dann Sache Ihrer IT und nicht Teil des Supports.

Betrieb

Wie viel Aufwand ist der laufende Betrieb?

Wenige Minuten im Monat: Updates einspielen (per Knopfdruck in der Weboberfläche), ab und zu prüfen, ob Sicherungen entstehen und kopiert werden, Betriebssystem aktuell halten. Zertifikate verlängern sich selbst.

Wie viele Firmen und Nutzer passen auf einen Server?

Mehrere Firmen sind möglich (Verwaltung › Server), jede mit eigener Lizenz. Für bis zu 50 Nutzer genügt ein Server mit 4 vCPU und 8 GB RAM.

Können wir Daten wieder herausbekommen?

Jederzeit und vollständig: Gesamtexport als Excel/CSV in der Weboberfläche, SQL-Sicherung unter Verwaltung › Server, und die tägliche Sicherung im offenen PostgreSQL-Format. Es gibt keine Bindung an IKS.

Gibt es eine Schnittstelle zu ERP, CRM oder Marketing-Werkzeugen?

Ja: eine REST-API mit API-Schlüsseln (Lesen bzw. Lesen und Schreiben) und Webhooks für Ereignisse. Einrichtung unter **Verwaltung › Einstellungen › Schnittstellen**. Die technische Beschreibung liegt auf dem Server unter `/opt/salesdesk/docs/api.md` und `docs/integration.md`.

Lizenz und Kosten

Was passiert, wenn die Lizenz abläuft?

Nach Ende eines Abos bzw. einer Lizenzdatei läuft der Server noch **14 Tage** normal weiter, danach ist er **nur lesbar**. Nach dem 30-tägigen Testzeitraum ist er sofort nur lesbar. Nur lesbar heißt: Alle sehen und exportieren weiter, Änderungen sind gesperrt. Es werden **nie Daten gelöscht**. Eine neue Lizenz schaltet sofort frei; die Änderungen, die in der App gewartet haben, werden dann übertragen.

Zählt die Lizenz Geräte, gleichzeitige Verbindungen oder Personen?

Personen: jedes **aktive Benutzerkonto** (benannte Benutzer), auch die Verwaltung und technische Schnittstellen-Benutzer. Geräte und gleichzeitige Verbindungen zählen nicht. Deaktivierte Konten belegen keinen Platz.

Können wir per Rechnung kaufen?

Ja, als Jahresvertrag direkt bei IKS – auch für mehr als 25 Nutzer. Sie erhalten eine Lizenzdatei für Ihre Server-Adresse. Siehe Jahresvertrag per Rechnung.

Wer hilft bei Problemen?

Zuerst diese Anleitung und das Kapitel Fehlersuche. Danach IKS per E-Mail (Adresse im Impressum – mit Version `cat /opt/salesdesk/VERSION`, Betriebssystem, Fehlermeldung und Protokollauszug, aber **ohne** Passwörter und Schlüssel.

Stand: App 1.13.0, Server 0.22.0, 02.11.2026. Die aktuelle Fassung steht immer unter salesdesk-app.iks-solutions.com/installation/.