INSTALLATIONSANLEITUNG

Eigenen SRM-Server installieren

Von der leeren Debian-Maschine bis zur ersten gekoppelten Kunden-Anlage – Schritt für Schritt. Der SRM-Server läuft nach der Installation 14 Tage im Testmodus, eine Lizenz brauchen Sie erst danach.

Downloads

⬇ SRM-Server 2.4.4
Installationspaket für Debian (srm-server-2.4.4.tar.gz)

⬇ SRM-Client 2.4.4
für Windows, als ZIP – entpacken und starten

SHA-256 des Installationspakets:
`ca106a123b3faebe4823e82b174cc6d540f131b575654ddff82f4a122b36f796`

Die App für die innovaphone App Platform laden Sie später direkt im SRM-Client herunter (Schritt 6).

Was Sie brauchen

- **Eine Maschine mit Debian 13** (64 Bit, amd64) – als VM unter Proxmox, VMware, Hyper-V o. ä. oder direkt auf Hardware. Empfohlen: 2 CPU, 2 GB RAM, 10 GB Platte, feste IP-Adresse im LAN.
- **Internetzugang** für die Maschine (die Installation lädt einige Debian-Pakete nach).
- **Einen DNS-Namen** (z. B. `srm.ihre-firma.de`), der auf Ihre öffentliche IP zeigt, und eine Portweiterleitung **TCP 443** auf den SRM-Server – damit die Kunden-Anlagen ihn aus dem Internet erreichen.
- **Einen Windows-PC** für den SRM-Client.
- Beim Kunden: eine **innovaphone App Platform** (Firmware 13r2 bis 16r1) und Administratorzugang zur PBX.
- Eine **Authenticator-App** auf dem Smartphone (z. B. Microsoft oder Google Authenticator) für die Zwei-Faktor-Anmeldung.

1. Debian 13 bereitstellen
2. SRM-Server installieren
3. SRM-Client einrichten
4. Testmodus starten oder Lizenz einspielen
5. Aus dem Internet erreichbar machen
6. App beim Kunden installieren (ohne App Platform: 6b)
7. Kunden koppeln und loslegen

---

1 Debian 13 bereitstellen

Installieren Sie ein minimales Debian 13 (Netinst-Image von debian.org). Bei der Softwareauswahl genügen **„SSH-Server“** und **„Standard-Systemwerkzeuge“** – keine Desktop-Umgebung. Vergeben Sie eine feste IP-Adresse (bei der Installation oder per DHCP-Reservierung im Router).

Ob die Maschine eine VM oder echte Hardware ist, spielt keine Rolle. Die Installation richtet die passenden Gast-Werkzeuge des Hypervisors selbst ein.

---

2 SRM-Server installieren

Melden Sie sich per SSH (oder an der Konsole) als `root` an und geben Sie ein:

```
cd /root
wget -O srm-server.tar.gz https://srm.tm-nettech.de/download/srm-server
tar xzf srm-server.tar.gz
cd srm-server-*/
bash srm-install.sh
```

Alternativ kopieren Sie das Paket aus den Downloads oben z. B. mit WinSCP nach `/root` und starten ab `tar xzf …`.

Das Skript erledigt alles Weitere:

- installiert die benötigten Pakete (u. a. Caddy für den eingebauten Proxy mit Let's-Encrypt-Zertifikat),
- legt den Dienst `srmserver` an (Benutzer `srm`, Ordner `/opt/srm`) und startet ihn,
- richtet die Firewall ein – offen sind SSH (22), 443 sowie die SRM-Ports 7778 und 7779,
- schaltet die automatischen Debian-Sicherheitsupdates ein.

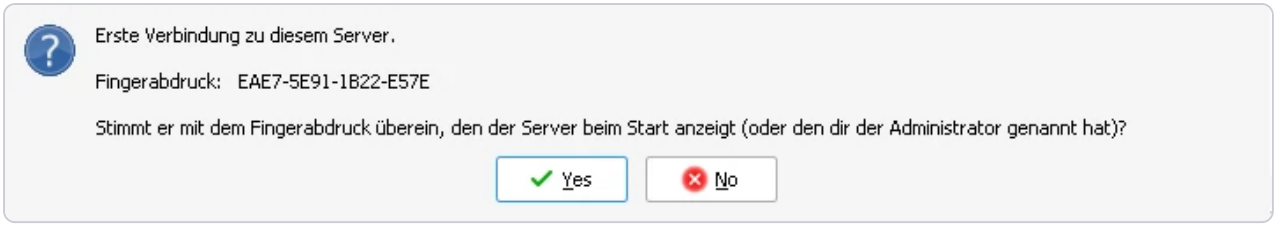
Am Ende zeigt es **Adresse**, **Fingerabdruck** und den **Einrichtungscode** für das erste Konto. Diese Angaben zeigt jederzeit auch der Befehl `srm-info`.

Optionen: `--keine-firewall` (eigene Firewall-Regeln), `--keine-autoupdates`.

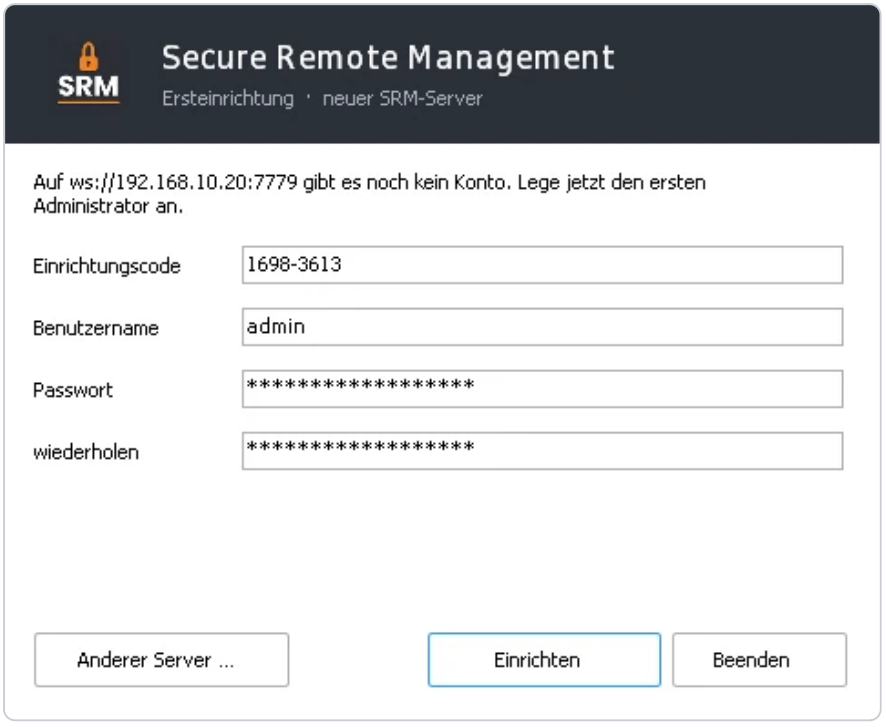
3 SRM-Client einrichten

Entpacken Sie **SRM-Client** (Download oben) auf Ihrem Windows-PC in einen eigenen Ordner und starten Sie `srmclient.exe`. Als **Server** tragen Sie im LAN zunächst `ws://<IP-des-SRM-Servers>:7779` ein.

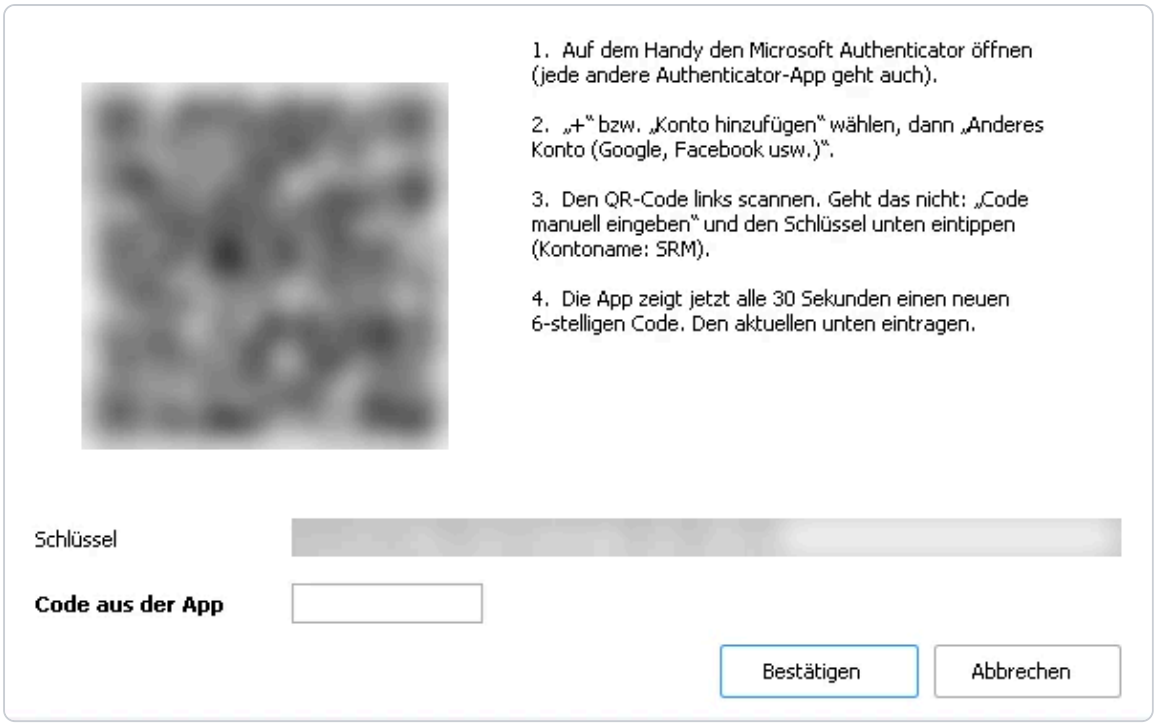
1. **Fingerabdruck vergleichen.** Beim ersten Verbinden zeigt der Client den Fingerabdruck des Servers. Er muss mit dem übereinstimmen, den `srm-info` anzeigt.



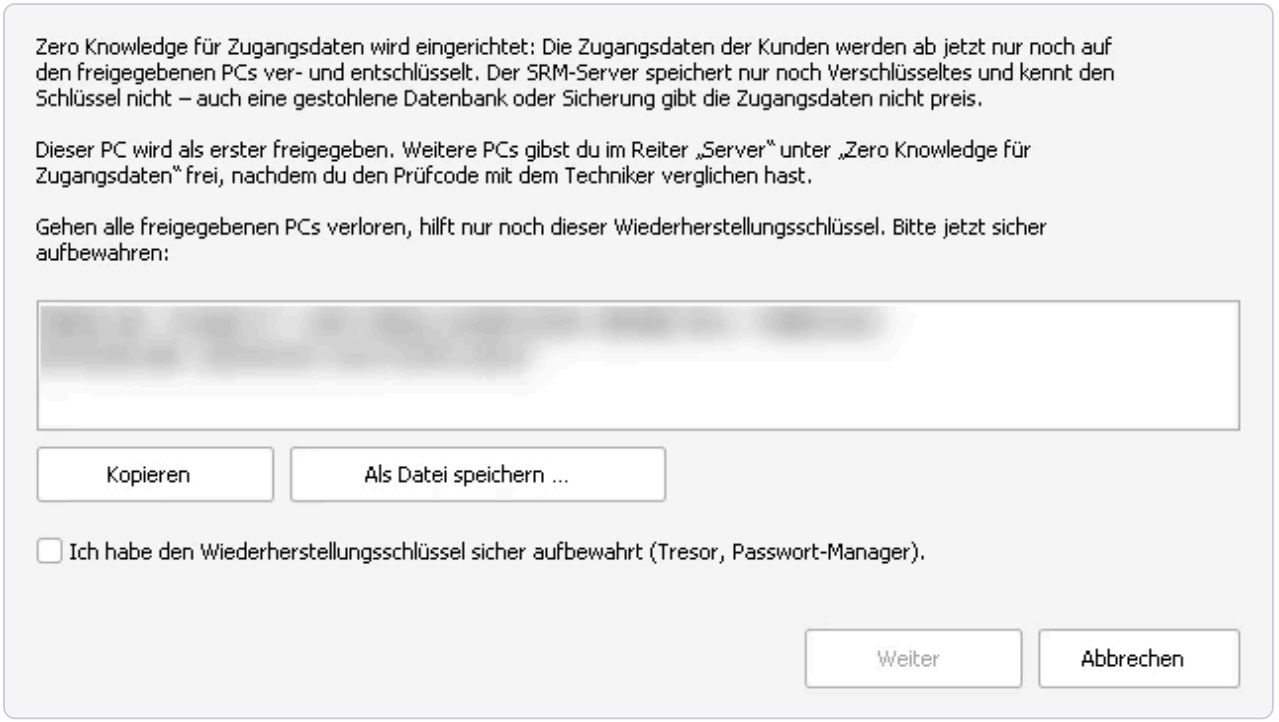
2. **Ersten Administrator anlegen.** Einrichtungscode eingeben, Benutzername und Passwort (mindestens 8 Zeichen) wählen.



3. **Zweiten Faktor einrichten.** QR-Code mit der Authenticator-App scannen und den angezeigten 6-stelligen Code eingeben. Ab jetzt fragt jede Anmeldung danach.



4. **Wiederherstellungsschlüssel sichern.** Die Zugangsdaten Ihrer Kunden werden per Zero Knowledge nur auf freigegebenen PCs entschlüsselt. Bewahren Sie den angezeigten Wiederherstellungsschlüssel sicher auf (Tresor, Passwort-Manager) – ohne ihn sind die Zugangsdaten verloren, wenn alle freigegebenen PCs ausfallen.



4 Testmodus starten oder Lizenz einspielen

Ohne Lizenz ist der Zugriff auf Kunden gesperrt. Im Reiter **„Server"** öffnet **„Lizenz ..."** diesen Dialog:



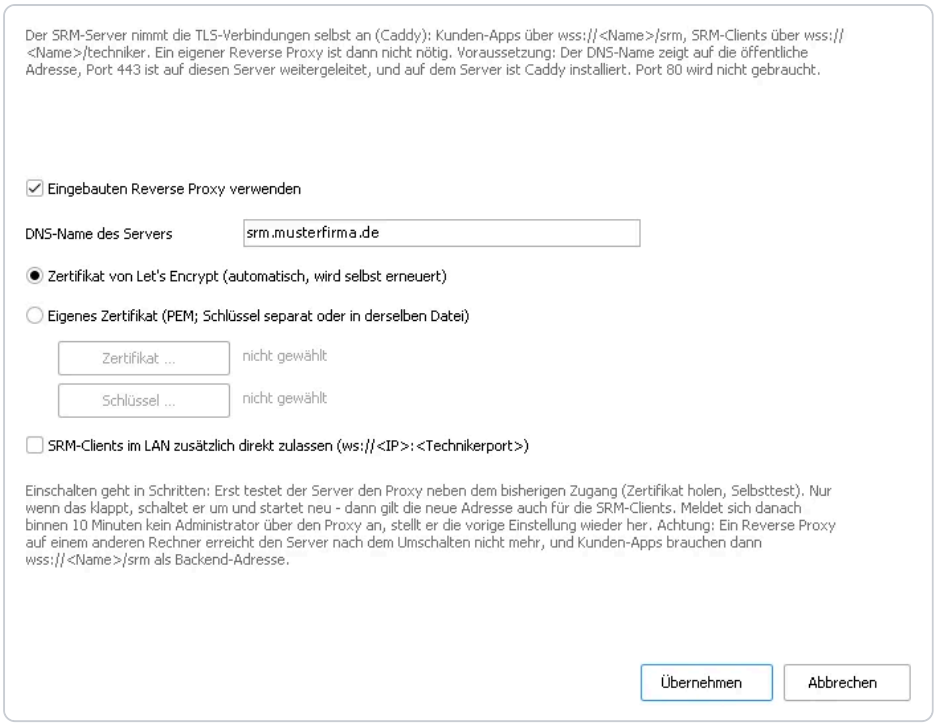
- **Testmodus starten:** 14 Tage, bis zu 10 Kunden und 3 gleichzeitig angemeldete Techniker – einmalig je Server.
- **Lizenz kaufen:** auf der Preisseite das passende Paket wählen. Bei der Bestellung geben Sie den hier angezeigten **Fingerabdruck** an (Sie können ihn auch nachreichen). Den Lizenzschlüssel (beginnt mit `SRM2-`) erhalten Sie per E-Mail, fügen ihn in diesem Dialog ein und klicken auf **„Einspielen“**.

Läuft der Testmodus ab, bleiben alle Kunden und Einstellungen erhalten; nach dem Einspielen der Lizenz ist sofort alles wieder frei. Die Lizenz gilt nur für diesen Server (Fingerabdruck) und zieht mit der Sicherung auf einen neuen Server um.

---

5 Aus dem Internet erreichbar machen

1. **DNS:** Legen Sie bei Ihrem DNS-Anbieter einen A-Eintrag an, z. B. `srm.ihre-firma.de` → Ihre öffentliche IP-Adresse.
2. **Router/Firewall:** Leiten Sie **TCP 443** auf den SRM-Server weiter. Port 80 wird nicht gebraucht.
3. **Eingebauten Proxy einschalten:** Reiter „Server“ → „Reverse Proxy“ → **„Proxy …“**. Haken setzen, DNS-Namen eintragen, „Zertifikat von Let's Encrypt“ wählen und „Übernehmen“. Der Server holt das Zertifikat selbst, testet den neuen Zugang und schaltet erst dann um.



Danach gelten diese Adressen:

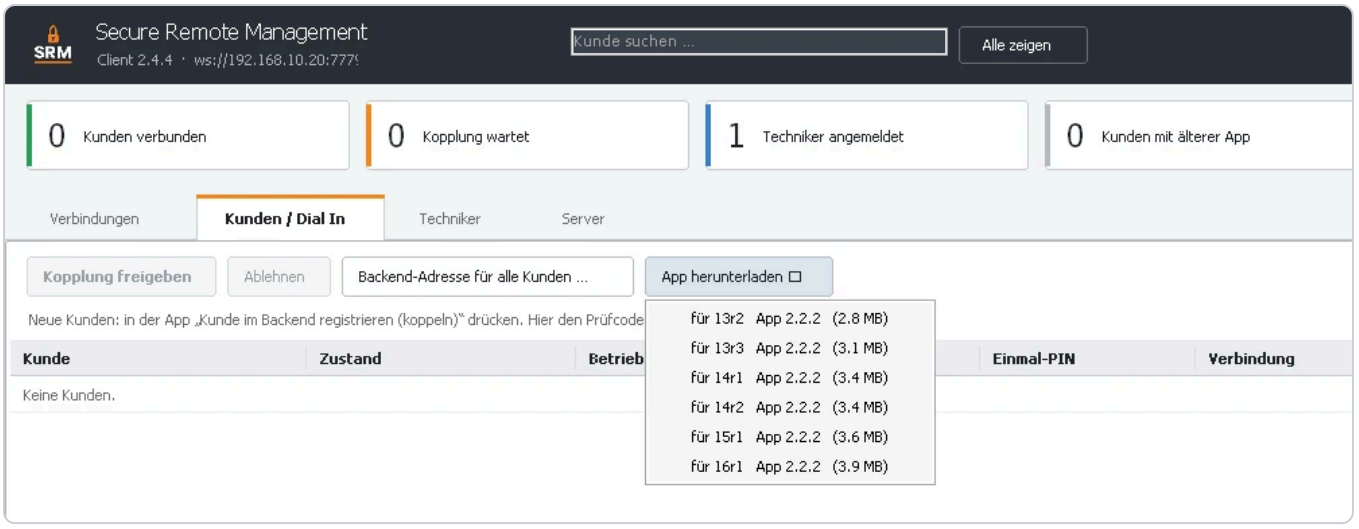
Wer	Adresse
Kunden-Apps (Backend-Adresse)	`wss://srm.ihre-firma.de/srm`
SRM-Clients der Techniker	`wss://srm.ihre-firma.de/techniker` (stellt sich beim nächsten Anmelden selbst um)

Eigenes Zertifikat statt Let's Encrypt: im selben Dialog „Eigenes Zertifikat“ wählen. Sie haben schon einen eigenen Reverse Proxy? Dann lassen Sie den eingebauten aus und leiten `/srm` an Port 7778 und `/techniker` an Port 7779 des SRM-Servers weiter.

---

6 App beim Kunden installieren

Im SRM-Client, Reiter **„Kunden / Dial In“** → **„App herunterladen“**, wählen Sie das Paket für die Firmware-Version der App Platform des Kunden (13r2 … 16r1). Die ZIP enthält je einen Ordner für `arm`, `arm64` und `x86_64` – welche Plattform die App Platform hat, zeigt der AP Manager.



1. **AP Manager** (Entwicklermodus): aus dem passenden Ordner `srm-remote`, `srm-remote.png` und `httpfiles.zip` hochladen.
2. **Instanz anlegen:** Name `srm-remote`, Domain = Systemname der PBX, Instanz-Passwort und Datenbank-Passwort vergeben, Instanz starten.
3. **App-Objekt in der PBX:** Name `srm`, Passwort = Instanz-Passwort, URL `https://<AP>/<domain>/srm/srm`. Haken **Websocket**, **PBXSignal** und **Services** setzen und im Reiter „Apps" den AP Manager `apps` anhaken (PBXSignal braucht Dial In, Services + apps das App-Update über den SRM-Server). Bei Master/Slave im App-Objekt die Master-PBX fest eintragen.
4. **Optional für Dial In:** einen Benutzer mit Rufnummer und Hardware-Id anlegen; dieselbe Hardware-Id tragen Sie in der App ein.
5. **App zuweisen und öffnen:** die App einem Benutzer zuweisen und in myApps öffnen.

6b Ohne App Platform: Devices-Registrierung

Hat der Kunde nur eine innovaphone-PBX bzw. ein Gateway ohne App Platform (z. B. IP411, ab Firmware 13r1), verbindet sich die PBX selbst mit dem SRM-Server – ganz ohne App:

1. In der Weboberfläche der PBX (Advanced UI) unter **General → Devices Registration** als Adresse die Backend-URL `wss://srm.ihre-firma.de/srm` eintragen – dieselbe wie für die Apps.
2. **„TLS/SSL certificate checking"** dort **nicht** anhaken – mit diesem Haken kommt keine Verbindung zustande.
3. Im SRM-Client erscheint die PBX im Reiter „Kunden / Dial In" als wartend (mit Seriennummer). Nach **„Kopplung freigeben"** ist sie ein Kunde mit der Betriebsart „nur Weboberfläche".

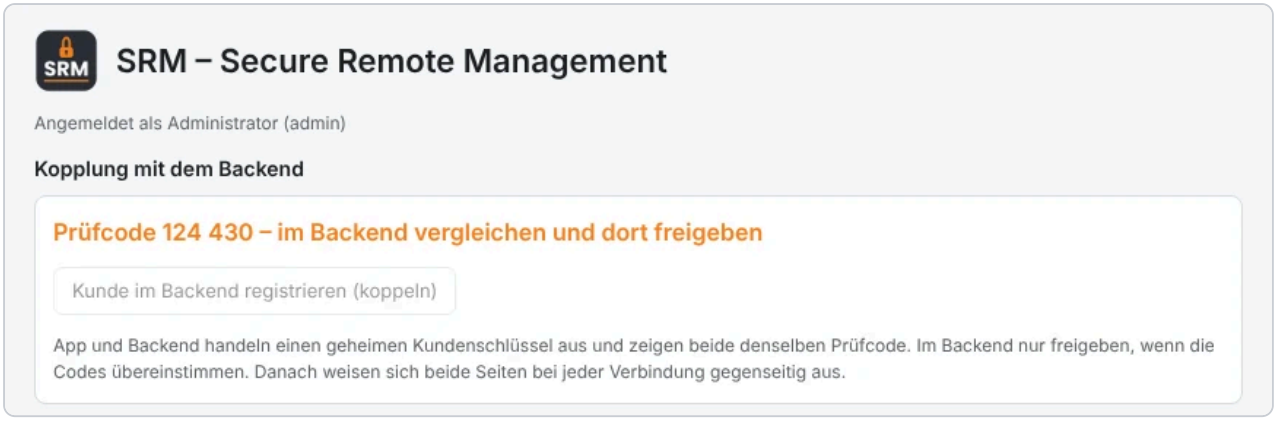
Erreichbar ist auf diesem Weg nur die Weboberfläche der PBX – keine weiteren Ziele, kein Dial In, keine App-Einstellungen. Voraussetzung ist der Zugang über `wss://` mit gültigem Zertifikat (Schritt

5). An die PBX wird kein Passwort geschickt und an ihrer Konfiguration nichts geändert. Die PBX zählt als ein Kunde für die Lizenz.

---

7 Kunden koppeln und loslegen

1. **In der App** Backend-Adresse (`wss://srm.ihre-firma.de/srm`), Kundenname und Ziele eintragen (eine Zeile je Gerät, z. B. `PBX = 192.168.0.2:443`), „Übernehmen“ und dann **„Kunde im Backend registrieren (koppeln)“**. Die App zeigt einen Prüfcode.



2. **Im SRM-Client** erscheint der Kunde unter „Kopplung wartet“. Prüfcode vergleichen (am besten am Telefon vorlesen lassen) und **„Kopplung freigeben“**.



3. **Betriebsart wählen** (in der App oder per Stift-Symbol im SRM-Client): **Dauerverbindung** oder **Dial In Aktivierung** (Verbindung erst nach Anruf mit Einmal-PIN).
4. **Fernwarten:** Im Reiter „Verbindungen“ den Kunden wählen und **„Im Browser öffnen“**.

Weitere Techniker legen Sie im Reiter **„Techniker“** an. Das Symbol „Client-Paket (ZIP)“ erzeugt für jeden Techniker einen fertig eingerichteten SRM-Client – er muss nur noch sein Passwort eingeben.

Update

Ein neues Paket installieren Sie mit denselben Befehlen wie in Schritt 2. Datenbank, Schlüssel, Lizenz, Einstellungen und Protokolle bleiben erhalten; startet der neue Server nicht, holt das

Skript den bisherigen automatisch zurück. Neue App-Versionen verteilen Sie danach im SRM-Client mit **„App aktualisieren“** – ohne Besuch beim Kunden.

Sicherung

- **SRM-Sicherung:** Reiter „Server“ → „Sicherung“ → **„Exportieren …“** – Kunden, Schlüssel, Konten, Richtlinie und Lizenz in einer Datei, mit eigenem Passwort verschlüsselt. Damit ziehen Sie auch auf einen neuen Server um.
- **Sicherung der ganzen VM:** Die Datei `/opt/srm/srmserver.secretkey` muss mit dabei sein, sonst startet der Server aus der Sicherung nicht.
- **Wiederherstellungsschlüssel** für Zero Knowledge (Schritt 3) getrennt davon sicher aufbewahren.

Nützliche Befehle auf dem Server

Befehl	Wirkung
`srm-info`	Zustand, Version, Adresse, Fingerabdruck, Einrichtungscode
`systemctl restart srmserver`	Server neu starten
`less /opt/srm/srmserver.log`	Protokoll (täglich gewechselt, 60 Tage aufbewahrt)
`/opt/srm/srmserver reset2fa <Name>`	Notweg: zweiten Faktor eines Kontos zurücksetzen (z. B. Smartphone verloren)
`runuser -u srm -- /opt/srm/srmserver proxy off` und `systemctl restart srmserver`	Notweg, wenn der eingebaute Proxy nicht mehr erreichbar ist

Fragen?

Schreiben Sie uns an srm@tm-nettech.de. Lieber erst ausprobieren ohne eigene Installation? Dann fordern Sie einen kostenlosen Demo-Server an.