

Systemvoraussetzungen Cloud

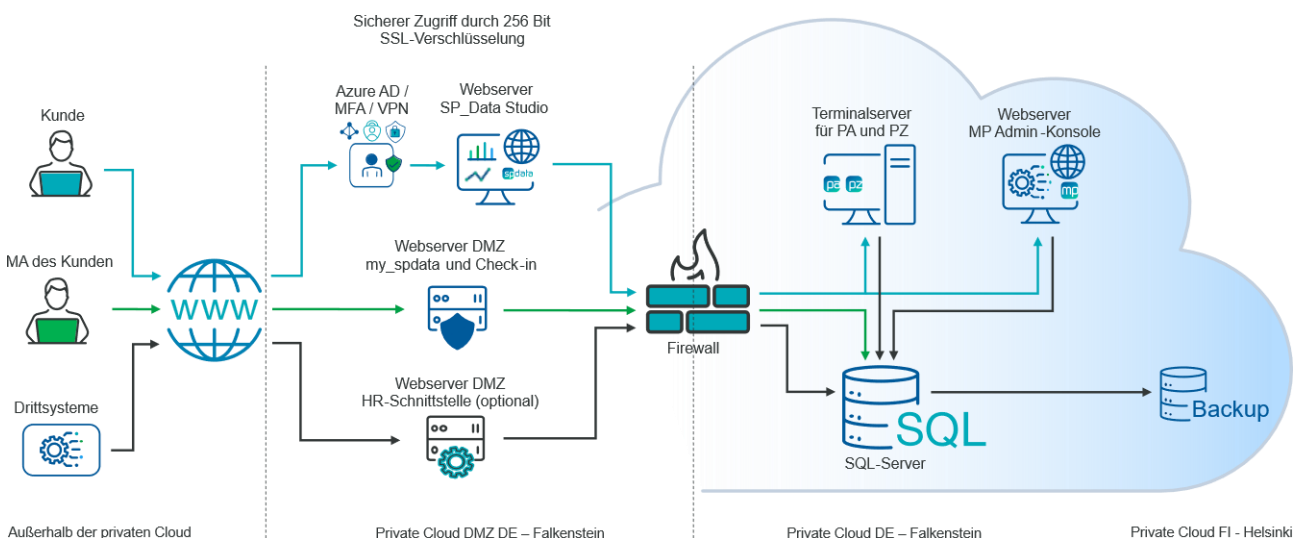
Das vorliegende Dokument informiert über die Möglichkeiten und Systemvoraussetzungen des Zugangs zur SP_Data Cloud.

1. Umfang der SP_Data Cloud

Jeder SP_Data Kunde erhält eine separate Cloudumgebung. Diese verfügt über einen Terminalserver, welcher für die vereinbarte Anzahl an Benutzern lizenziert ist. Zusätzlich wird eine SQL-Instanz zur Verfügung gestellt, welche nur vom Terminalserver des Kunden aufrufbar ist. Für die HR-Schnittstelle und my_spdata kann ein separater DMZ-Zugang eingerichtet werden, über den die entsprechenden Anwendungen kommunizieren.

Microsoft hat folgende Empfehlungen über die Bandbreite in der Cloud (Arbeiten mit RDP):

<https://learn.microsoft.com/de-de/azure/virtual-desktop/rdp-bandwidth>



Grafik: Aufbau der SP_Data Cloud

2. Cloud Zugangsformen

Folgende Zugangsmöglichkeiten zur SP_Data Cloud stehen zur Verfügung:

a. VPN Site-to-Site

- Gesamtes Netzwerk wird mit der Cloud "vernetzt"
- Ipsec oder OpenVPN
- Installation muss auf dem Router des Kunden oder über eine VM-Appliance umgesetzt werden.

- b. VPN Client-to-Site
 - Nur Client wird mit Cloud vernetzt (mehrere möglich)
 - Nur OpenVPN
- c. Zero-Trust über das SP_Data-Studio
 - Administration über das Azure Active Directory des Kunden
 - Der Zugang zum Terminalserver erfolgt ausschließlich über das SP_Data Studio. Eine VPN-Verbindung wird nicht benötigt.
 - Dies ist unsere Empfehlung aufgrund der einfachen Administration.
 - Optional „Mit Microsoft anmelden“
- d. Besonderheiten bei Hardware für die Zeitwirtschaft (Zutritt und Terminals)
 - Sofern Terminals für Zeiterfassung in der SP_Data Cloud über deren IP-Adressen angebunden werden sollen, ist in der Regel ein VPN Site-to-Site erforderlich.
- e. Mischformen sind möglich, bitte im Detail mit SP_Data abstimmen.
Beispielsweise wäre Folgendes möglich:
Das Firmennetz ist per IPSec Site-to-Site angebunden und zusätzlich sind einzelne Tele-Clients per OpenVPN Client-to-Site angebunden.

3. Anbieter von VPN Software

- a. Ipvsec (IKEv1(nicht aggressiver Modus) & IKEv2)
 - Nur für Site-to-Site-Verbindungen.
 - Ipvsec IKEv2 ist unsere Empfehlung, da Hardwareunterstützung für Ipvsec weiter verbreitet ist als für OpenVPN.
- b. [OpenVPN](#) (v2.4+) via UDP.
 - Client-to-Site und Site-to-Site
 - Kein HTTP-Multiplex. Jeder Kunde muss in seiner Firewall ausgehend einen Port öffnen.
 - In allen Fällen Zugriff auf vpn.in-reach.de (ein zugewiesener ausgehender Port zwischen 200 und 1500 - UDP), nur TLS-Auth
 - Unsere Empfehlung: Die meiste Hardware unterstützt OpenVPN nicht mehr. Aus diesem Grund bieten wir optional eine VM-Appliance hierfür an (siehe 4.)

4. VM-Appliance

Sollte bei einer gewünschten Cloud-Zugangsform via Site-to-Site das Netzwerk angebunden werden und auf dem Router des Kunden werden die Hardwareanforderungen der VPN-Software nicht erfüllt, kann dies über eine VM-Appliance gelöst werden. Das ist eine von SP_Data vorbereitete virtuelle Maschine mit installierter Software für das VPN, die im Kundennetzwerk eingerichtet wird.

5. Anforderungen an beide VPN-Zugangsformen

- Da SP_Data keinen Zugriff ins Kundennetzwerk möchte, müssen NAT-Regeln von Firewall/Appliance zu den Terminals „forwarden“ (Port 8000/TCP).
- Die Firewall muss so konfiguriert sein, dass Ports 3389TCP+UDP + 443,80/TCP im Cloudnetzwerk (172.x.x.x wird zugewiesen) erreichbar sind.
- Zur Einrichtung wird eventuell Zugriff auf sx-share.in-reach.de:443/TCP zur Zertifikatsübergabe benötigt.

6. Datenzugriff (SEPA-Datei und andere)

In der Remotesession wird eine Laufwerksfreigabe eingerichtet und genutzt. Hierüber können Dateien aus der SP_Data Cloud auf den lokalen Computer direkt aus der SP_Data Anwendung gespeichert werden. Dies gilt für alle Cloud Zugangsformen.

Der Zugriff auf die Personalakten und die Mandantenakten erfolgt entweder über das SP_Data Studio oder die SP_Data PA oder PZ.

7. Microsoft Office

In der SP_Data Cloud sind die Office 365 Apps oder Office 2021 installiert.

Die Office Installation wird zur Verfügung gestellt und der Kunde kann seine eigene Lizenz hinterlegen und aktivieren. Sollte keine Lizenz vorliegen kann diese bei SP_Data in Auftrag gegeben werden.

8. E-Mail-Versand

- a. kundeneigener Mailserver
 - IT des Kunden muss einen „Connector“ zur Verfügung stellen.
- b. kein kundeneigener Mailserver
 - Fallback SMTP Gateway: Eine Relaisstation, welche die E-Mails an den entsprechenden Mailserver des Kunden weiterleitet. Erfordert mindestens einen DNS-Eintrag beim Kunden.
- c. Wenn der Mailserver des Kunden nicht aus dem Internet aufrufbar ist, gibt es mehrere mögliche Umsetzungsformen. Die Möglichkeiten im Detail müssen mit SP_Data geklärt werden.

Hinweis

Die in diesem Dokument enthaltenen Informationen sind ausdrücklich keine zugesicherten Eigenschaften im Rechtssinne und können ohne vorherige Ankündigung geändert werden. SP_Data haftet nicht für fehlerhafte oder unvollständige Informationen in diesem Dokument. Weitere Informationen über die Produkte von SP_Data erhalten Sie unter <https://www.spdata.de>, weitere Informationen über unser Rechenzentrum und unsere Sicherheitsmaßnahmen unter <https://www.spdata.de/vertraege>.

Stand: 17.03.2026