PRODAT Systemanforderungen

Server und Clients · Einrichtung und Betrieb · Stand 28.10.2026

Stand der Angaben zu Einrichtung und Betrieb: 28.10.2026. Diese Seite dient der Abstimmung zwischen Kunden-IT und PRODAT. Betriebssystem, Datenbankversion, Ressourcen und Zugänge sind vor Installation oder Migration für die eingesetzte PRODAT-Version zu bestätigen.

Systemanforderungen für Server und Client

Für Neuinstallationen sind Betriebssysteme mit laufender Sicherheitsversorgung und bestätigter PRODAT-Kompatibilität einzusetzen. Die früheren Angaben „Windows Server 2012 R2 aufwärts“ und „Windows 7 aufwärts“ gelten nicht mehr als aktuelle Beschaffungsempfehlung. Eine allgemeine Freigabe zukünftiger Versionen ist damit nicht verbunden.

Bereich	Abstimmung vor Installation
Windows-Server	Windows Server 2022 oder 2025 als Planungsoption mit PRODAT abstimmen; die Nennung ist keine pauschale Versionsfreigabe.
Windows-Client	Unterstützte Windows-11-Version und benötigte Anwendungen, Treiber sowie Peripherie prüfen.
Datenbank und Linux	PostgreSQL-Version und gegebenenfalls Linux-Distribution passend zur PRODAT-Version mit PRODAT festlegen.
Virtualisierung und RDS	Ressourcen, Betriebsart, Lizenzen sowie Drucker- und Scanneranbindung abstimmen.

Die Dimensionierung richtet sich nach gleichzeitig aktiven Nutzern, Modulen, Schnittstellen und Dokumentenaufkommen. CPU-Leistung, tatsächlich verfügbare RAM-Ressourcen, SSD/NVMe-Speicher und Netzwerk sind gemeinsam zu betrachten. Bei virtuellen Servern sind konkurrierende Lasten zu berücksichtigen. Programmdateien, Datenbank, DMS, temporäre Daten und Sicherungen sind getrennt mit Wachstumsreserve zu planen. Frühere pauschale Größenangaben ersetzen keine kundenspezifische Auslegung.

Installation und Freigaben

Installationsverzeichnisse, Dienstkonten und Netzwerkfreigaben werden mit der Kunden-IT festgelegt. Nur die für den jeweiligen Benutzer beziehungsweise Dienst erforderlichen Rechte vergeben. Datenbankverzeichnisse sind keine allgemeinen Clientfreigaben.

Die Ausführung über eine Netzwerkfreigabe, eine lokale Programmkopie oder einen Terminalserver ist entsprechend der Installation abzustimmen. Für lokale Programmkopien siehe 105 Prodat Lokales Start Script (RunLocal). Die Aussage „keine lokale Installation erforderlich“ ist nicht auf jede Betriebsart übertragbar. Drucker und Scanner sind mit dem vorgesehenen Benutzerkonto und insbesondere bei RDS im tatsächlichen Sitzungsbetrieb zu testen.

Firewall und Ports

Nur tatsächlich benötigte Verbindungen freigeben. Quelle, Ziel, Transportprotokoll und konfigurierte Ports müssen anhand der jeweiligen Installation bestätigt werden. Die folgenden PRODAT-Portangaben stammen aus der bisherigen Dokumentation und sind keine Aufforderung, sämtliche Ports zu öffnen.

Verbindung	Port	Verwendung und Gültigkeit
PRODAT-Client bzw. berechtigter Dienst → Datenbankserver	5432/TCP	PostgreSQL-Standardport; tatsächliche Konfiguration prüfen. Keine direkte Internetfreigabe.
PRODAT-Client → ApplicationServer	212	HelpPort laut bisheriger Dokumentation ab Version 12.3; Transportprotokoll und Bedarf prüfen.
PRODAT-Client → ApplicationServer	211	CachingPort laut bisheriger Dokumentation; Transportprotokoll und Bedarf prüfen.
PRODAT-Komponente ↔ Datafox-Terminal	8000	Richtung und Transportprotokoll gemäß Gerätekonfiguration prüfen; siehe 9050 DataFox Terminal.
Client → Dateiserver	445/TCP	SMB-Netzwerkfreigabe, sofern benötigt; intern beschränken.
PRODAT-Fernwartung → vereinbartes Zielsystem	RDP, üblicherweise 3389/TCP	Externe Portzuordnung und gegebenenfalls UDP separat abstimmen; Quell-IP-Beschränkung siehe Fernwartung.

Historische Ports: DMS-StreamPort 212 für Version 12.0 bis 12.1; ApplicationServer-ListenPort 5431 bis Version 11. Diese Angaben betreffen Altversionen und sind nicht zusätzlich für aktuelle Installationen freizugeben.

Virenscanner und Endgeräteschutz

Die Kunden-IT stellt den Zugang zur Administration des eingesetzten Virenscanners beziehungsweise EDR bereit. PRODAT und Kunden-IT stimmen erforderliche Ausnahmen anhand der tatsächlichen Datenbank- und Anwendungsinstallation ab. Schutzsoftware darf den laufenden Datenbankbetrieb nicht durch Dateisperren oder Quarantäne beeinträchtigen.

Für jede Ausnahme dokumentieren: System, vollständiger Pfad beziehungsweise Prozess, Ausnahmeart, Begründung und verantwortlicher Administrator. Konkrete Pfade sind bei der Einrichtung zu ermitteln; diese Seite legt keine pauschale Ausschlussliste fest. Nicht das gesamte Laufwerk, alle ausführbaren Dateien oder das komplette DMS ungeprüft ausschließen. Nach der Einrichtung PRODAT, Datenbank und Dokumentenzugriff mit aktivem Schutz testen.

Fernwartung

Als erste Ausbaustufe wird ein verschlüsselter RDP-Zugang zum vereinbarten Kundensystem mit Beschränkung auf die folgenden öffentlichen PRODAT-Quell-IP-Adressen eingerichtet, sofern mit der Kunden-IT vereinbart:

Standort	Zulässige Quell-IP
Rechenzentrum	116.202.227.166
Office	24.134.240.97

Ein zusätzliches VPN ist bei dieser Variante nicht vorgesehen. Es wird kein pauschaler Netzwerkzugang angefordert. Der Zugriff vom Zielsystem auf weitere Ressourcen ist durch Berechtigungen und Netzwerkregeln auf den erforderlichen Umfang zu begrenzen. Abweichende Kundenrichtlinien sind vor Einrichtung abzustimmen.

RDP ausschließlich von den beiden genannten Quell-IP-Adressen auf das vereinbarte Zielsystem freigeben; keine allgemeine Internetfreigabe.

Unterstütztes und aktualisiertes Windows, aktive Netzwerkauthentifizierung (NLA), verschlüsselte Verbindung und geprüfte Serveridentität verwenden.

Eigenes Supportkonto mit starkem, kundenspezifischem Passwort und erforderlichen Rechten einrichten; personenbezogene Konten bevorzugen.

Erfolgreichen Zugriff von PRODAT und die Sperre von anderen Quelladressen prüfen. Zugangsdaten über einen vereinbarten geschützten Kanal übergeben.

Anmeldung protokollieren und Zuständigkeit für Sperrung, Passwortwechsel und Pflege des Zugangs festlegen.

Nach erfolgreicher Umstellung nicht mehr benötigte Fernwartungszugänge gemeinsam mit der Kunden-IT deaktivieren.

Die IP-Beschränkung reduziert die Erreichbarkeit des RDP-Dienstes. Sie ersetzt keinen Nachweis der einzelnen Person oder des Gerätezustands. Ein kompromittierter Rechner hinter einer erlaubten Quell-IP bleibt ein Risiko. MFA und eine weitergehende Zentralisierung des Fernzugangs sind als spätere Ausbaustufe vorgesehen; bereits vorhandene Schutzmaßnahmen werden nicht zurückgebaut.

Datensicherung und Betrieb

Kunden-IT und PRODAT legen Zuständigkeiten für Betrieb, Aktualisierungen und Datensicherung fest. Maximal tolerierbarer Datenverlust und Wiederanlaufzeit sind zu vereinbaren. Das Sicherungskonzept umfasst Datenbank, DMS und erforderliche Konfigurationen und muss eine konsistente Wiederherstellung ermöglichen. RAID und VM-Snapshots allein ersetzen kein abgestimmtes Backupverfahren.

Sicherungsergebnisse, freier Speicher und Dienstausfälle überwachen; einen Empfänger für Alarme festlegen. Eine gegen Manipulation oder Löschung geschützte Sicherungskopie vorsehen. Wiederherstellung vor Betriebsfreigabe in einer separaten Umgebung testen und regelmäßig überprüfen.

Hinweise zu Windows Server 2025 und Netzwerkfreigaben

Nach einer Servermigration können sich die Antwortzeiten beim Zugriff auf PRODAT-Programmdateien und Dokumente über Netzwerkfreigaben verändern. Neben Server- und Netzwerkressourcen sind die wirksamen SMB-Einstellungen, die zugriffsbasierte Auflistung von Dateien und Ordnern (ABE) sowie Virenscanner und weitere Schutzsoftware zu berücksichtigen.

Bei Auffälligkeiten die betroffenen Arbeitsabläufe mit einem normalen Benutzerkonto messen und mit einer geeigneten lokalen beziehungsweise RDP-Ausführung vergleichen. Dabei dokumentieren, ob lokale Dateien oder weiterhin Netzwerkfreigaben verwendet werden. Jeweils nur eine Einstellung verändern und das Ergebnis festhalten.

SMB-Signierung, SMB-Verschlüsselung und ABE sind mögliche Prüfpunkte, keine pauschal bestätigten Fehlerursachen. Änderungen erfolgen gezielt nach Abstimmung zwischen Kunden-IT und PRODAT. Eine generelle Deaktivierung von Sicherheitsfunktionen ist keine Voraussetzung für den PRODAT-Betrieb.

Microsoft unterscheidet bei den Standardanforderungen zwischen Client und Server sowie Verbindungsrichtung: Windows Server 2025 verlangt standardmäßig ausgehende SMB-Signierung; Windows 11 24H2 Pro/Enterprise/Education ein- und ausgehende Signierung. Daher stets die tatsächlich verwendete Verbindung prüfen. Die Einstellung EnableSecuritySignature ist für SMB 2/3 nicht maßgeblich; entscheidend ist die Signierungsanforderung auf beiden Seiten.

Microsoft: SMB-Signierung — https://learn.microsoft.com/windows-server/storage/file-server/smb-signing

Microsoft: Bedeutung der Signierungseinstellungen — https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-signing-overview

Microsoft: Langsame SMB-Übertragungen — https://learn.microsoft.com/en-gb/troubleshoot/windows-server/networking/slow-smb-file-transfer

Checkliste vor Inbetriebnahme oder Migration

Kunde: _____ PRODAT-Version: _____
Kunden-IT: _____ PRODAT: _____
Geplanter Produktivstart: _____

Pro Punkt Status (offen / erfüllt / nicht relevant / Abweichung vereinbart), Verantwortlichen und Nachweis beziehungsweise offenen Punkt festhalten.

☐ Kunde, PRODAT-Version, gleichzeitige Nutzer, Module und Schnittstellen erfasst

Status / Verantwortlicher / Nachweis: _____

☐ Betriebssysteme und Datenbankversion mit PRODAT abgestimmt

Status / Verantwortlicher / Nachweis: _____

☐ CPU, RAM, Speicherbedarf und Wachstumsreserve abgestimmt

Status / Verantwortlicher / Nachweis: _____

☐ Installationspfade, Dienstkonten, Freigaben und Berechtigungen dokumentiert

Status / Verantwortlicher / Nachweis: _____

☐ Benötigte Verbindungen mit Quelle, Ziel, Protokoll, Port und Zweck getestet

Status / Verantwortlicher / Nachweis: _____

☐ Virenscanner-Ausnahmen konkret dokumentiert und Betrieb mit aktivem Schutz geprüft

Status / Verantwortlicher / Nachweis: _____

☐ Fernwartung von PRODAT erfolgreich getestet und andere Quelladressen gesperrt

Status / Verantwortlicher / Nachweis: _____

☐ Supportkonto, Zugangsdatenübergabe, Protokollierung und Sperrverfahren geregelt

Status / Verantwortlicher / Nachweis: _____

☐ Nicht mehr benötigte Fernwartungszugänge nach Umstellung deaktiviert

Status / Verantwortlicher / Nachweis: _____

☐ Sicherung von Datenbank, DMS und Konfiguration eingerichtet und Wiederherstellung getestet

Status / Verantwortlicher / Nachweis: _____

☐ Überwachung, Alarmempfänger und Wartungszuständigkeiten festgelegt

Status / Verantwortlicher / Nachweis: _____

☐ PRODAT-Start, DMS und typische Abläufe mit normalem Benutzer geprüft

Status / Verantwortlicher / Nachweis: _____

☐ Bei Migration: SMB-Einstellungen und Vergleichsmessungen dokumentiert

Status / Verantwortlicher / Nachweis: _____

☐ Drucker, Scanner, Terminals und Schnittstellen geprüft, soweit eingesetzt

Status / Verantwortlicher / Nachweis: _____

☐ Offene Punkte mit Termin erfasst und Betriebsfreigabe durch Kunden-IT und PRODAT dokumentiert

Status / Verantwortlicher / Nachweis: _____

Freigabe Kunden-IT / PRODAT und Datum: _____

Geräteempfehlungen und weitere Einrichtungsanleitungen: siehe PRODAT-Wiki. Peripherie vor Beschaffung oder Migration abstimmen.