BankingManager

Technische Voraussetzungen und Konfigurationshinweise für Administratoren

Stand 18.12.2025

Für eine reibungslose Implementierung des BankingManagers in Ihrer IT-Infrastruktur sind die folgenden technischen Rahmenbedingungen und Konfigurationsschritte zu beachten.

1. Client-Systemanforderungen

- **Betriebssystem:** Windows 10 oder Windows 11 (64-Bit) mit aktuellem Service Pack / Funktionsupdate.
    - **Hinweis:** Aufgrund des Support-Endes von Windows 10 am 14. Oktober 2025 empfehlen wir, das Upgrade auf Windows 11 proaktiv zu planen, um die Systemsicherheit zu gewährleisten.
- **Hardware:**
    - **Arbeitsspeicher:** min. 4 GB RAM
    - **Bildschirmauflösung:** min. 1.440 x 900 Pixel
- **Peripherie (je nach Sicherheitsverfahren):**
    - **Schlüsseldatei:** USB-Wechsellaufwerk
    - **HBCI-Chipkarte:** Chipkartenleser der Sicherheitsklasse 2 oder höher (Secoder empfohlen)
    - **smartTAN/chipTAN USB:** Spezifischer chipTAN-USB-Kartenleser

2. Netzwerk- und Server-Anforderungen

- **Datenbank-Ablage:** Für die Mehrplatzinstallation wird ein zentraler Netzwerkpfad (Share) benötigt.
- **Berechtigungen:** Alle Benutzerkonten, die den BankingManager ausführen, benötigen **Lese- und Schreibberechtigungen** auf den konfigurierten Netzwerkpfad (sowohl NTFS- als auch Freigabeberechtigungen).

3. Firewall- und Proxy-Konfiguration

Die Anwendung erfordert Freigaben für spezifische Ports und URLs.

- **Port-Freigaben:**
    - **Port 443 (TCP/outbound):** Erforderlich für HTTPS-Kommunikation (Updates, Lizenzprüfung, FinTS mit PIN/TAN).
    - **Port 3000 (TCP/outbound):** Nur erforderlich bei Nutzung von Schlüsseldateien oder FinTS-Chipkarten.
- **URL-Whitelist:**
    - **Core Services (Lizenz & Updates):**
        - https://api-access.atruvia.de
        - https://cdn-ms.bankingmanager.de
        - https://cdn-ka.bankingmanager.de
        - https://bankingmanager.atruvia.de/
    - **FinTS-Kommunikation (Atruvia Rechenzentrum):**
        - https://fints1.atruvia.de/cgi-bin/hbciservlet
        - https://fints2.atruvia.de/cgi-bin/hbciservlet
        - fints1.atruvia.de
        - fints2.atruvia.de

Hinweis: Für Banken außerhalb des Atruvia-Rechenzentrums müssen deren spezifische FinTS-URLs freigegeben werden.

- **Proxy-Server-Konfiguration:**
    - Der BankingManager nutzt die systemweiten Proxy-Einstellungen von Windows (WinINET).
    - Eine notwendige individuelle Anmeldung am Proxy wird durch den BankingManager temporär zwischen gespeichert.
    - **Achtung:** Für die Kommunikation über Port 3000 (Schlüsseldatei/Chipkarte) ist zwingend die Konfiguration eines **SOCKS5-Proxy-Eintrags** in den Windows-Einstellungen erforderlich. Ein reiner HTTP-Proxy ist für diesen Anwendungsfall nicht ausreichend.

4. Hinweise zur Installation und Konfiguration

- **Installationskontext:** Die Installation kann pro Benutzer oder systemweit ("für alle Benutzer") erfolgen. Für Mehrbenutzer-Arbeitsplätze ist die systemweite Installation mit administrativen Rechten zwingend erforderlich, um eine gemeinsame Konfiguration sicherzustellen.
- **Antivirus / Endpoint Protection:** Erstellen Sie eine Ausnahme für die ausführbare Datei BankingManager.exe im Virenscanner und in der Firewall (insbesondere bei verhaltensbasiertem Schutz/Heuristik).
- **TLS-Protokoll:** Stellen Sie sicher, dass TLS 1.2 in den Internetoptionen des Betriebssystems aktiviert ist.

5. Aktuell nicht unterstützte Umgebungen

Die Installation und der Betrieb auf **Windows Server-Betriebssystemen** sowie in **Terminalserver-Umgebungen** (z.B. Citrix, RDS) sind derzeit nicht freigegeben. Eine Freigabe ist für eine spätere Version geplant.

6. Lizenzierung

Für die Funktionalität ist das Modul „Mehrplatz-Installation“ erforderlich. Dieses ist im 60-Tage-Testzeitraum standardmäßig aktiv und muss danach über die lizenzgebende Bank dauerhaft freigeschaltet werden.

7. Management von Programmupdates

- **Update-Mechanismus:** Die Anwendung prüft täglich auf verfügbare Updates. Wird eine neue Version gefunden, kann der Anwender den Installer an seinem Client im Hintergrund herunterladen lassen.
- **Verteilung und Berechtigungen:** Die Installation des heruntergeladenen Updates erfordert in der empfohlenen Installationsvariante administrative Berechtigungen auf dem Client-System.
- **Netzwerk-Bandbreite:** Im Standardverhalten lädt jeder Client das Update-Paket individuell von den unter Punkt 3 genannten Update-Servern herunter. Es existiert keine integrierte Funktion für eine zentrale Verteilung (Software-Repository).
- **Versioninkompatibilität und Rollout-Planung:** Ein Update kann Änderungen am Schema der zentralen Datenbank beinhalten. In einem solchen Fall können Clients mit einer veralteten Version nicht mehr auf den Datenbestand zugreifen, bis sie ebenfalls aktualisiert wurden. Der Anwender erhält eine entsprechende Meldung. Ein koordinierter und zeitnaher Rollout des Updates auf allen Clients ist daher für den reibungslosen Betrieb empfohlen.
- **Steuerung der Update-Funktion:** Die Berechtigung zur Update-Prüfung und zum automatischen Download kann innerhalb der Anwendung auf Benutzerebene konfiguriert werden. Dies ermöglicht es Administratoren, den Update-Prozess zu steuern, indem die Funktion für Standardanwender deaktiviert und das Rollout zentral gesteuert wird.