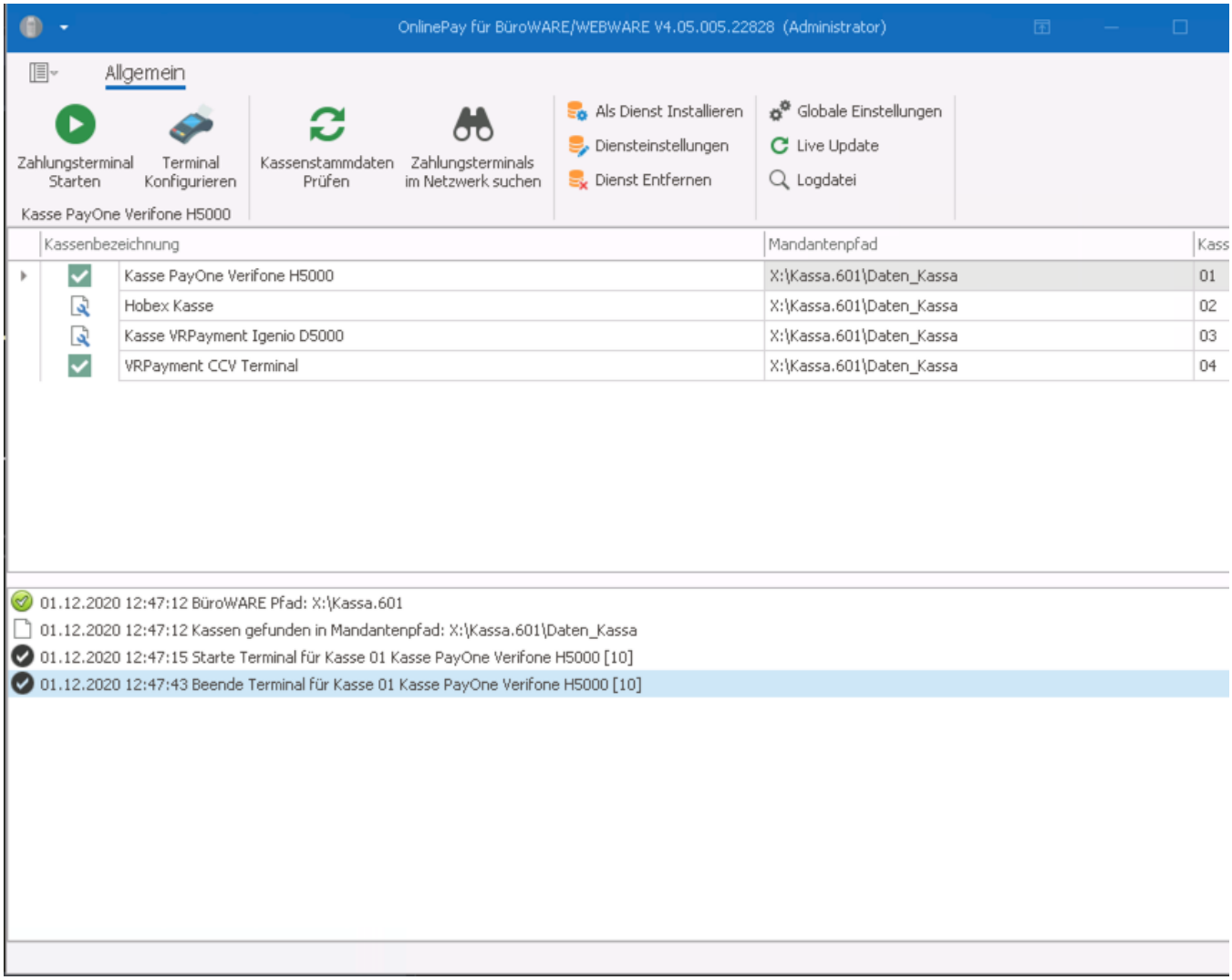
OnlinePay Zahlungsmodul

- Einrichtung
- getestete Terminals/Anbieter
- Online-Pay Tray
- Übersicht der Einstellungen
- Voraussetzungen und FAQ
- Was muss ich bei einem SumUp Zahlungsterminal einstellen?
- Was muss ich bei einem Zahlungsterminal mit O.P.I. Schnittstelle einstellen?

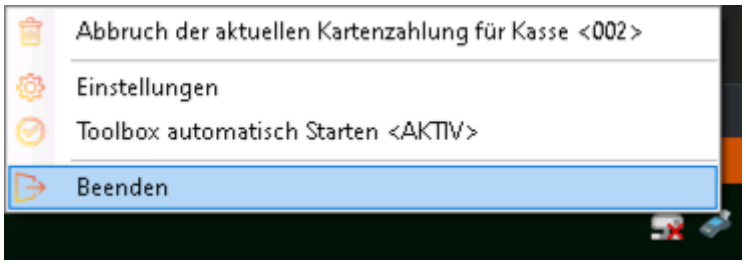
Umfang

Die Installation von Online-Pay enthält zwei ausführbare Programme:

- **Online-Pay.exe**
  Mit diesem Tool werden die Terminals konfiguriert und können auch getestet werden.
  Die Schnittstelle kann als Applikation oder Dienst laufen.



- **Online-PayTray.exe**
  Dieses Tool kann optional pro Windows-User für Kassenarbeitsplätze eingerichtet werden um ggf. Zahlungen oder Terminalfunktionen abzubrechen und die Steuerung wieder an die Handelskasse zu übergeben.



Installation

Wichtig

Für die Einrichtung von OnlinePay sind folgende Informationen erforderlich:

- Verbindungsart: TCP/IP oder seriell

- TCP/IP: IP-Adresse und Port (Zahlungsanbieter/IT-Betreuer)
  - (beides kann aber auch über den integrierten Netzwerkscan gefunden werden)
  - **wichtig ist eine fixe IP**

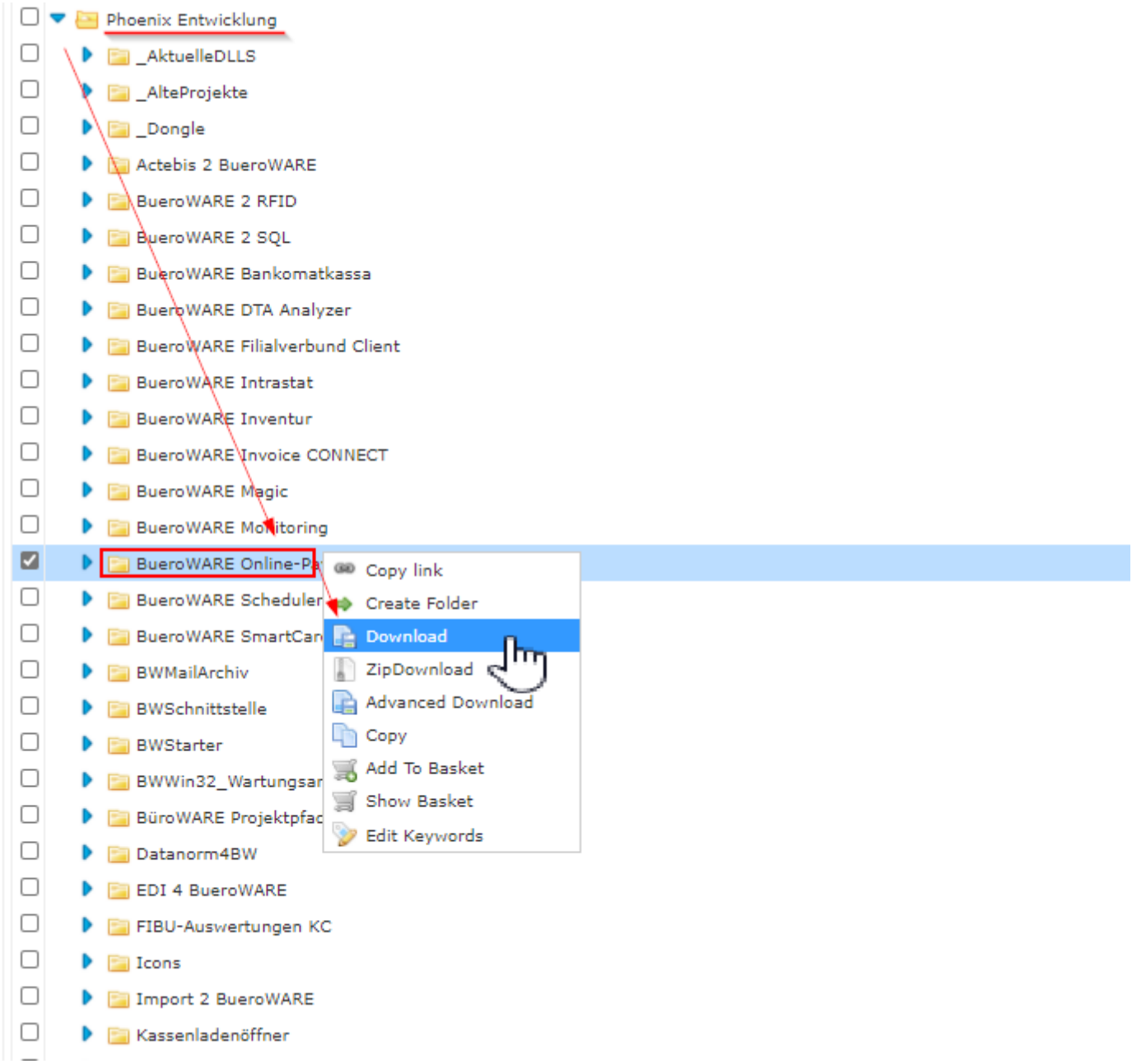
- seriell: Serieller Anschluss (COM-Port)
  - Baud-Rate
  - Stop Bits, ParityBits und FlowControl

Die Terminalkennwörter liegen dem Terminal üblicherweise bei bzw. müssen beim Anbieter erfragt werden. Je nach Zahlungsanbieter werden auch nicht alle Kennwörter genutzt.

- Registrierung
- Initialisierung
- Autorisierung Gutschriften

1. Download

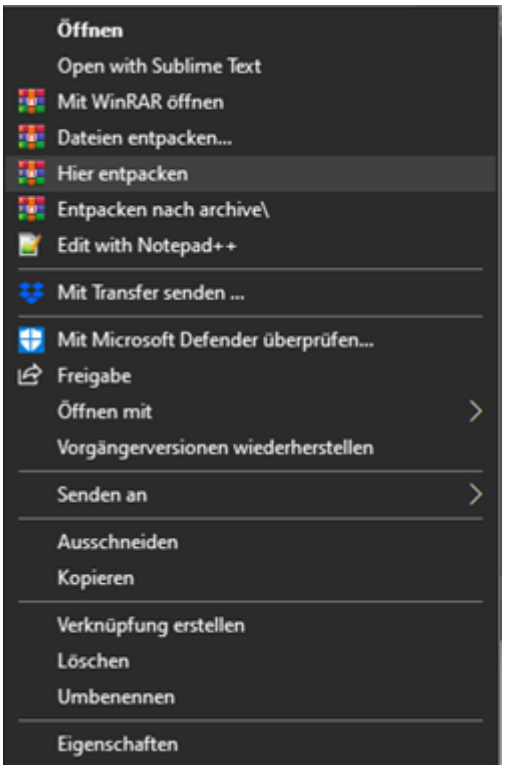
Die OnlinePay Bankomatschnittstelle kann über unseren FTP-Server heruntergeladen werden. Dieser ist erreichbar unter ftp.erpaustria.com. Melden Sie sich hier einfach mit "bwpartner" als Benutzername und Passwort an.
Navigieren Sie hier zu Phoenix Entwicklung und rechtsklicken Sie auf das Verzeichnis BueroWARE Online-Pay, um über das Menü den Download zu starten.



Nun sollte der Download eines Archives (Archiv.zip) gestartet werden.

2. Entpacken

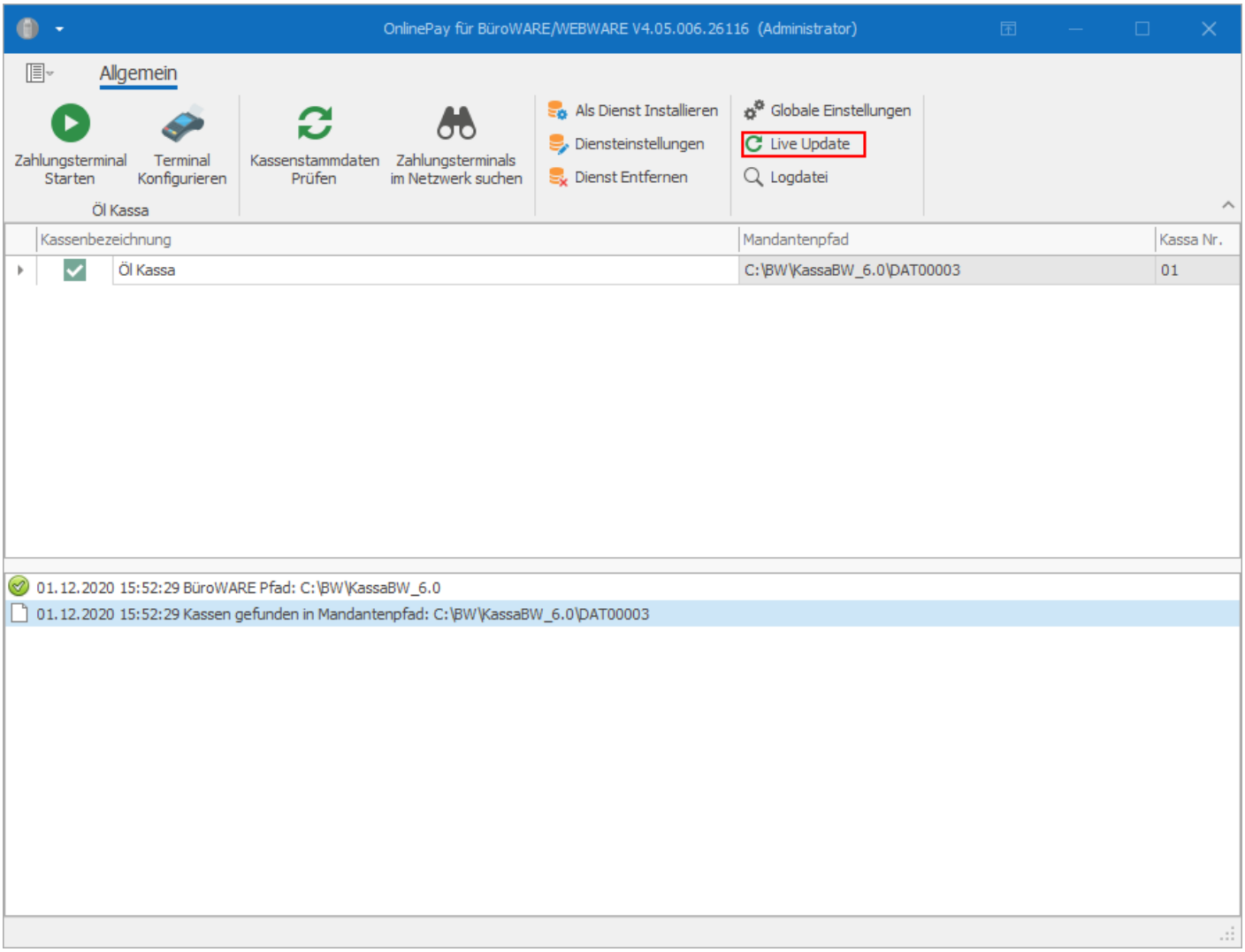
Sobald dieses fertig heruntergeladen ist, kann es in das richtige Verzeichnis verschoben und dort entpackt werden:
Sollte sich zB. am gleichen Laufwerk wie die BüroWARE-Installationen bereits ein Verzeichnis mit dem Namen APP.PhoenixDS befinden, wird das Archiv am besten dorthin verschoben und entpackt:



3. Live Update

Öffnen SIe im daraufhin erstellten Verzeichnis die Anwendung Online-Pay.exe

Bevor mit der Anbindung an die BüroWARE und das Terminal fortgefahren werden kann, muss die Schnittstelle als erstes auf die neueste Version Version aktualisiert werden.



Folgen Sie hier einfach dem Assistenten durch das Update.
OnlinePay startet sich dabei neu.

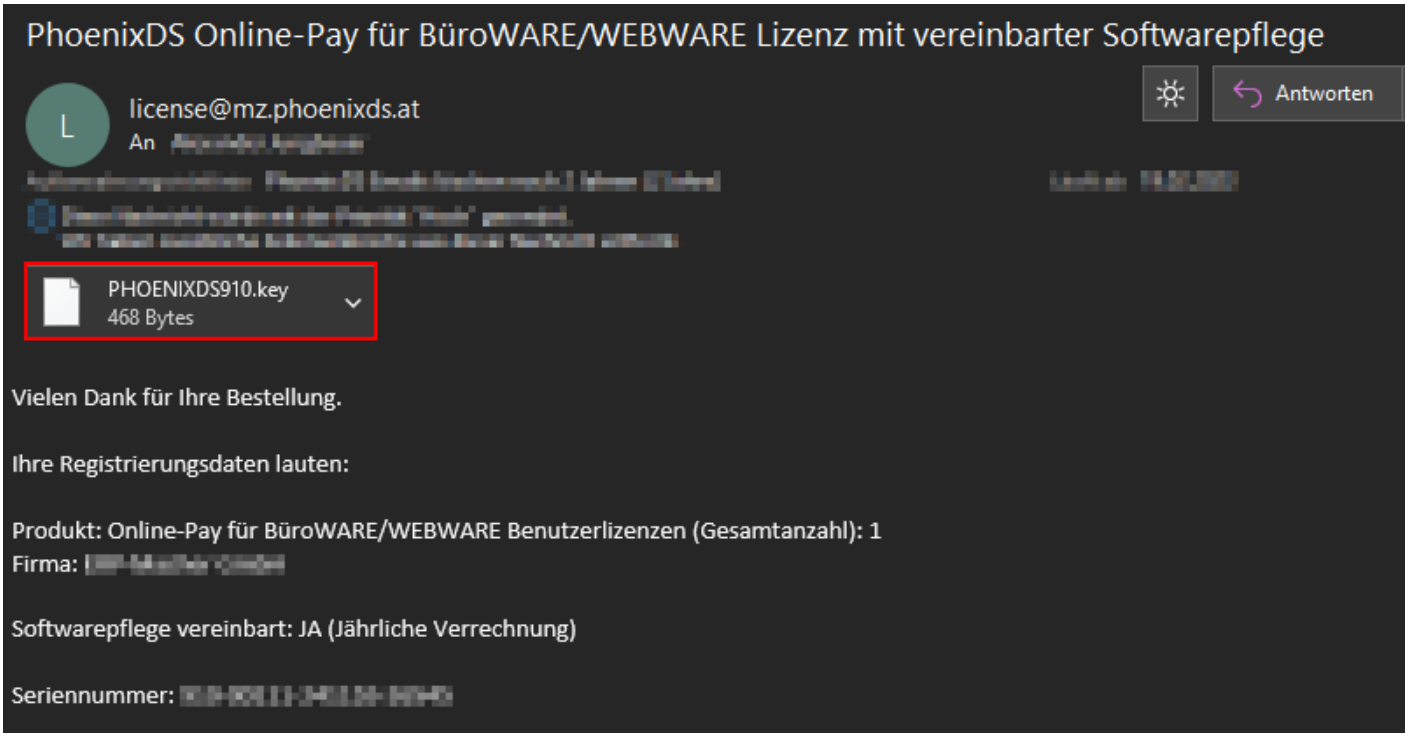
Wichtig: bei Updates muss der Dienst SoftENGINE OnlinePay (wenn OnlinePay als Dienst installiert worden ist) sowie falls verwendet die OnlinePay-Tray.exe beendet werden , damit alle Komponenten aktualisiert werden können.

Lizenz

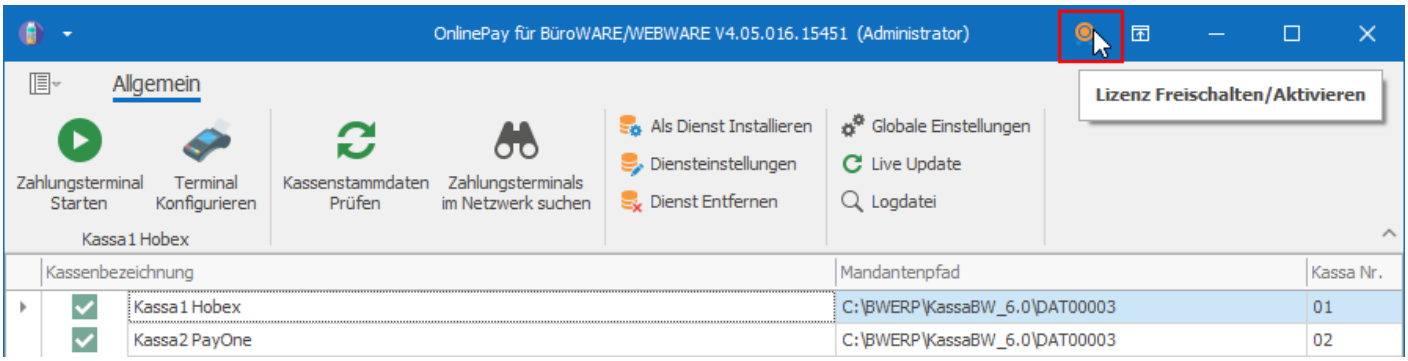
Jede Kassa wird in Onlinepay einzeln lizenziert. Werden mehrere Schnittstellen auf getrennten PCs ausgeführt (ohne zentralen Server), müssen auch getrennte Lizenzen verwendet werden.
Läuft OnlinePay am Server, können in einer Lizenz auch mehrere Kassen lizenziert werden.

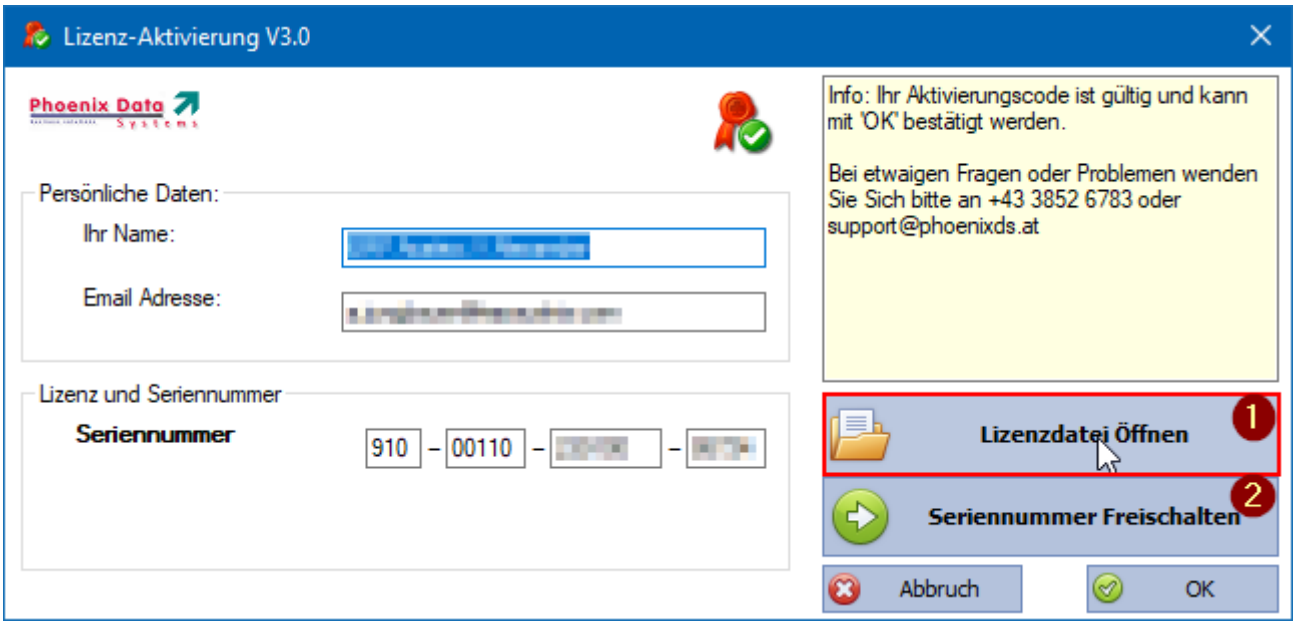
Die Anzahl der lizenzierten Kassen bezieht sich dabei nur auf die laufenden Kassen.
Die Lizenzen werden nicht einzelnen Kassen zugeordnet, die Sie in OnlinePay eingerichtet haben.
Wenn Sie zB. 5 Kassen lizenziert haben, können Sie 10 Kassen einrichten, aber es können nur 5 (beliebige) Kassen zugleich laufen.
Lizenz einspielen

Ihre Lizenz für OnlinePay erhalten Sie von ERP Austria per Mail.



Die angehängte Lizenzdatei können Sie herunterladen und in OnlinePay importieren.





Hier können Sie den Lizenzschlüssel über "Lizenzdatei öffnen" importieren, die Seriennummer und Name werden dann automatisch befüllt. (Alternativ kann die Seriennummer auch manuell eingetragen werden)

Anschließend auf "Seriennummer Freischalten" klicken.

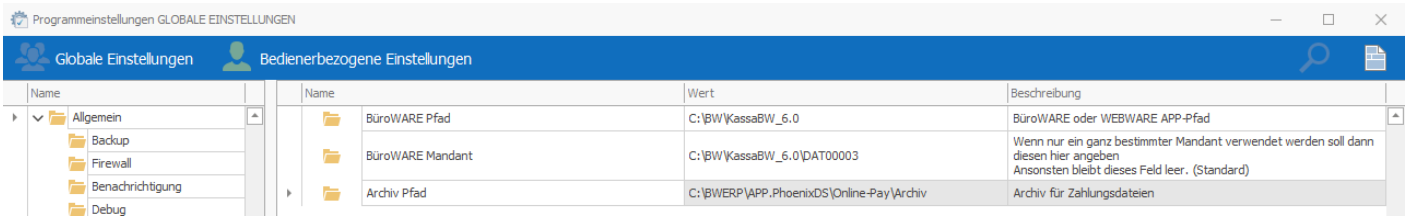
Sollte sich die Lizenz nicht freischalten lassen, wenden Sie sich bitte an den Support.

Verwendung ohne Lizenz

OnlinePay lässt sich auch ohne Lizenz als Demoversion verwenden.
Dabei läuft die Schnittstelle in einem eingeschränktem Modus mit einem erhöhten Resourcenverbrauch.

BüroWARE Kassa verbinden

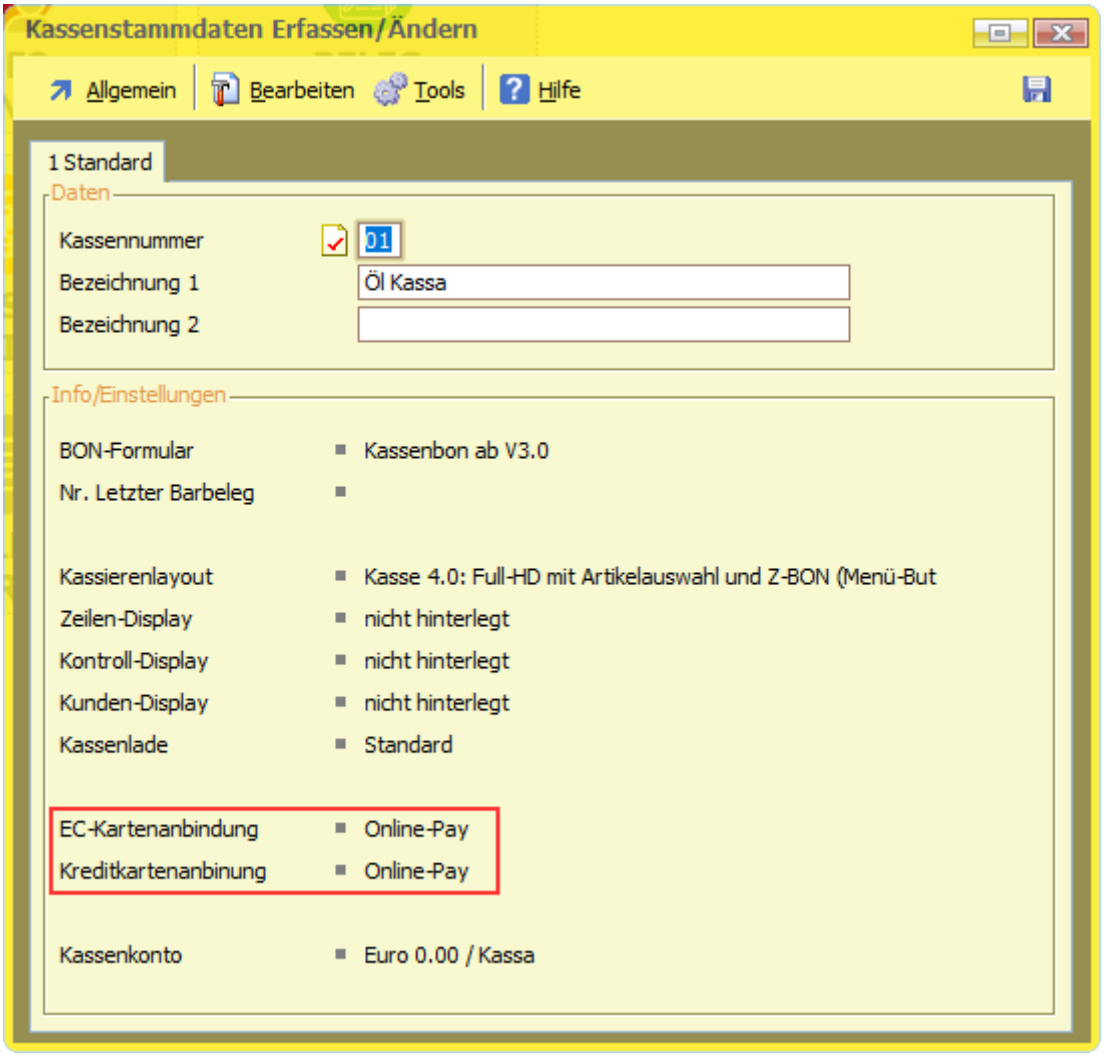
Im nächsten Schritt muss über die globalen Einstellungen rechts oben der Programm- und Mandantenpfad der zu verwendenden BüroWARE definiert werden.



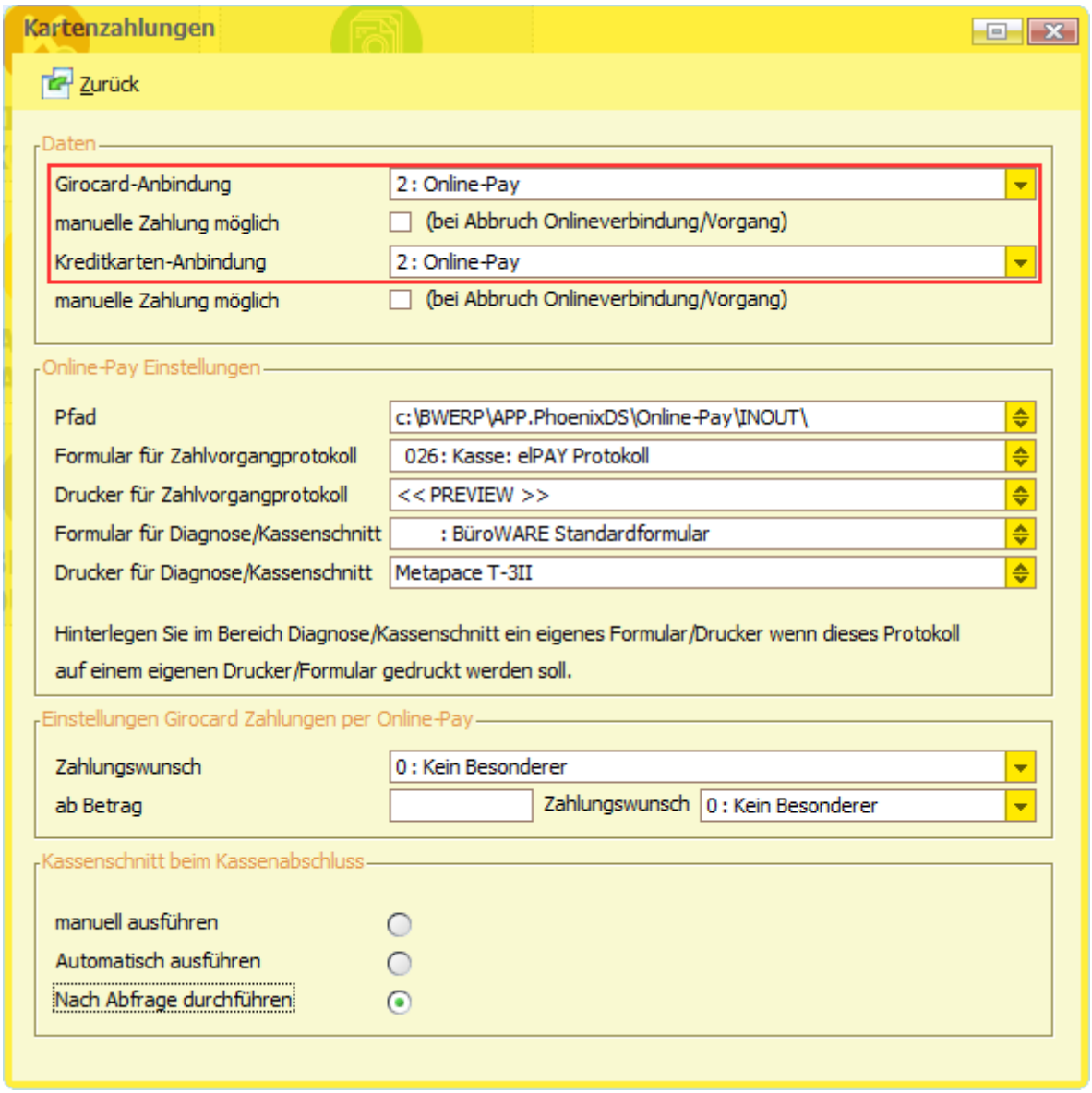
Der Mandantenpfad muss nur befüllt werden, wenn die Schnittstelle grundsätzlich nur mit einem Mandanten arbeiten soll. ansonsten kann dieses Feld leer gelassen werden.

In der SoftENGINE Kassa sind folgende Einstellungen notwendig:

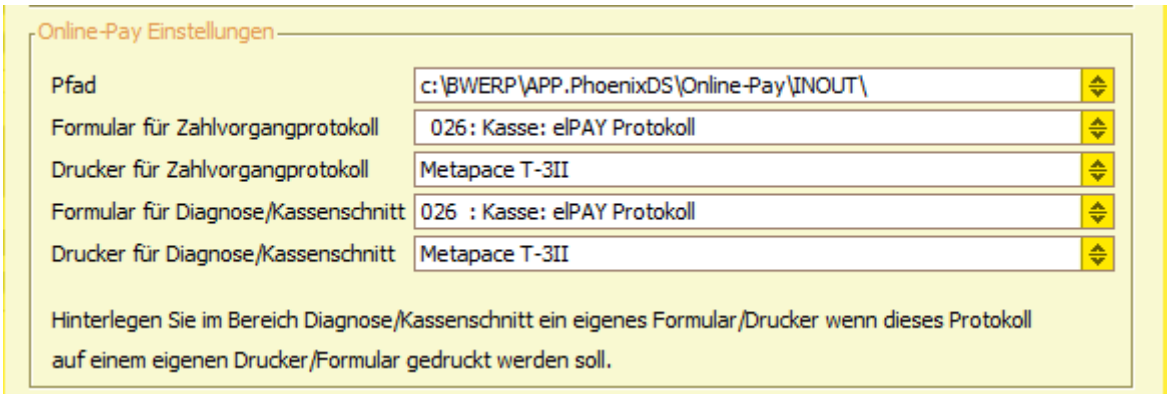
Navigieren Sie in den Kassenstammdaten zu den OnlinePay-Einstellungen:

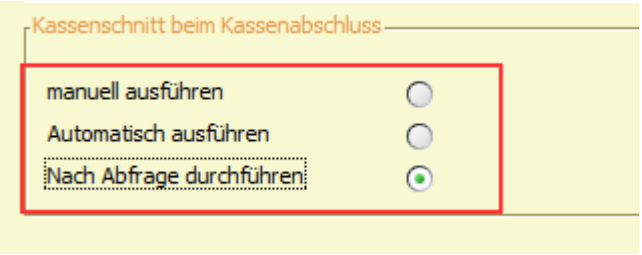


Hier muss die Giro-/Kreditkartenanbindung entsprechend auf 2: Online-Pay umgestellt werden.



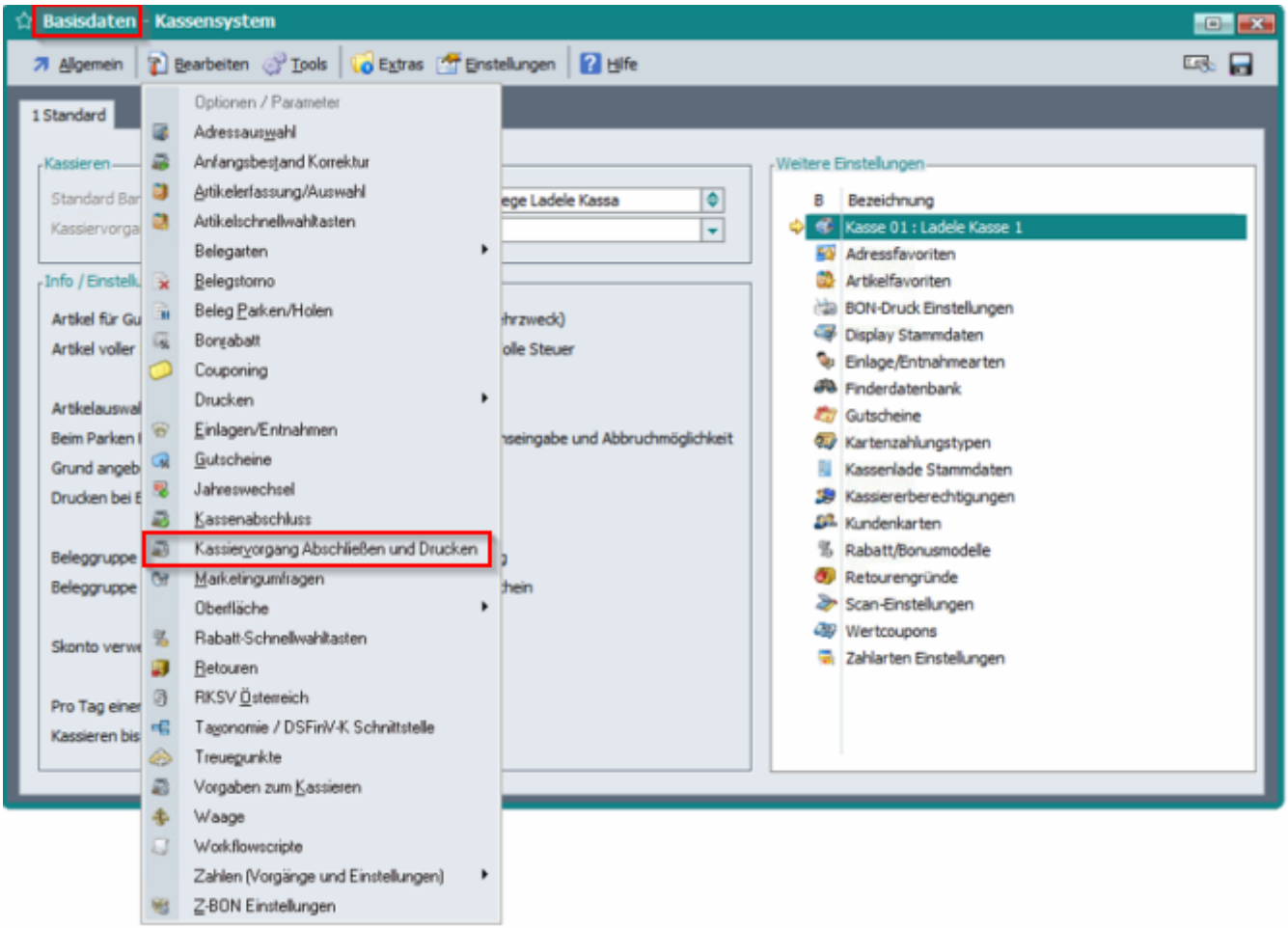
Tragen Sie den Kommunikationspfad entsprechend ein. Legen Sie diesen bitte zuvor im OnlinePay-Programmpfad als Unterordner an.
Hinterlegen Sie bitte das Formular 026 als Zahlvorgangsprotokoll und hinterlegen Sie den gewünschten Drucker.

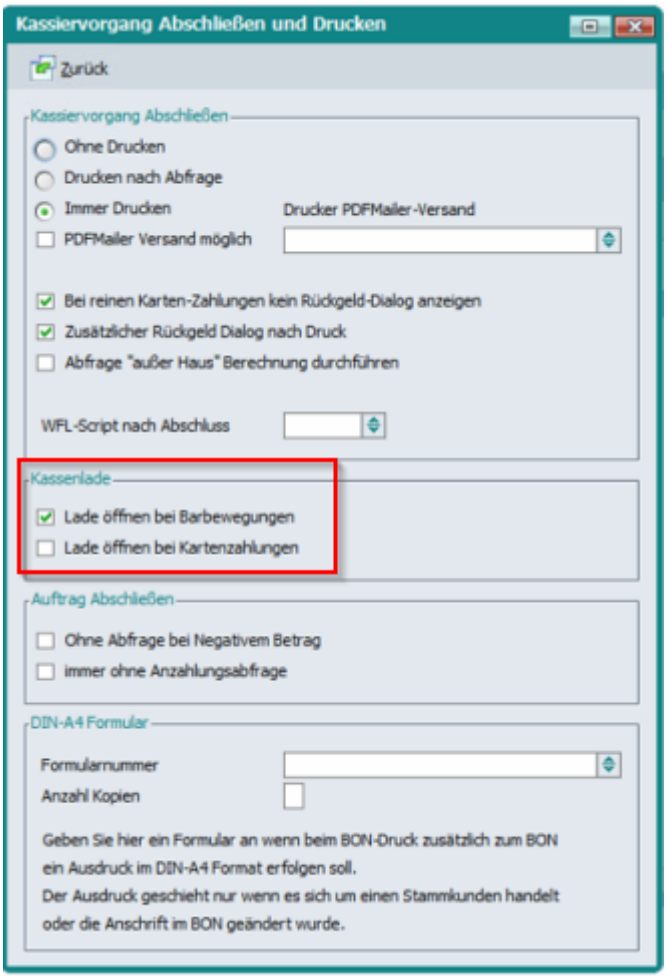




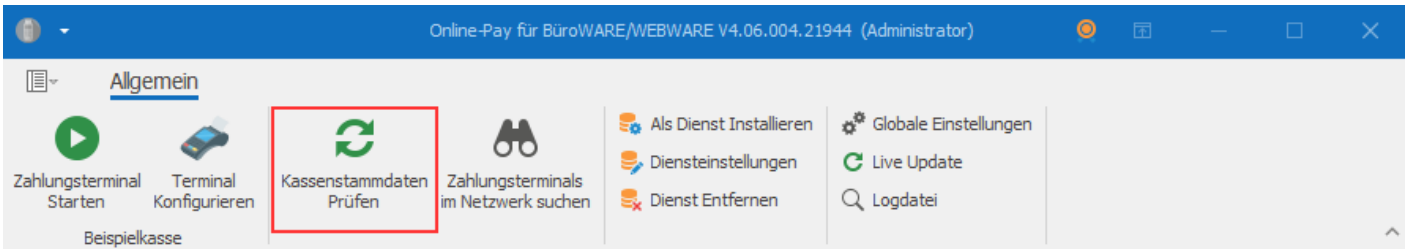
Beim Kassenschnitt sollte entweder "automatisch ausführen" oder "Nach Abfrage" ausgewählt werden.
Damit kann der Tagesabschluss im Bankomatterminal nicht übersehen oder vergessen werden.

In den Basisdaten ist dann im Menü "Bearbeiten/Kassiervorgang Abschließen und Drucken" noch einzustellen, wie die Kassenlade bei reinen Kartenzahlungen reagieren soll:





Wenn in der SoftENGINE Kassa alle Einstellungen getroffen sind, können Sie in der Schnittstelle über den Button "Kassenstammdaten prüfen"
die neuen Einstellungen aus der Kassa laden.



mehrere Kassen

Werden im eingetragenen BüroWARE-Pfad mehrere (in der BüroWARE konfigurierte Kassen) erkannt, legt OnlinePay für jede Kassa einen eigenen Punkt in den Einstellungen an:

hier kann dann für jede Kassa das Terminal und die restlichen Einstellungen vorgenommen werden. Dabei können auch unterschiedliche Terminals/Verbindungsprotokolle usw. verwendet werden, da die Terminalkonfiguration nur für die jeweilige Kassa gilt.

Wichtig:

Jedes Bankomatterminal darf nur einer Kassa zugeordnet werden, da es sonst zu Problemen bei der Zuordnung/Kommunikation kommen kann.

Bankomatterminal verbinden

Bankomatterminals können sowohl über TCP/IP als auch den COM-Port an OnlinePay angebunden werden.
In beiden Fällen müssen die entsprechenden Initialsierungs/Registirierungskennwörter des Terminals in der Schnittstelle eingetragen werden.
Sie erhalten diese von Ihrem Zahlungsanbieter.

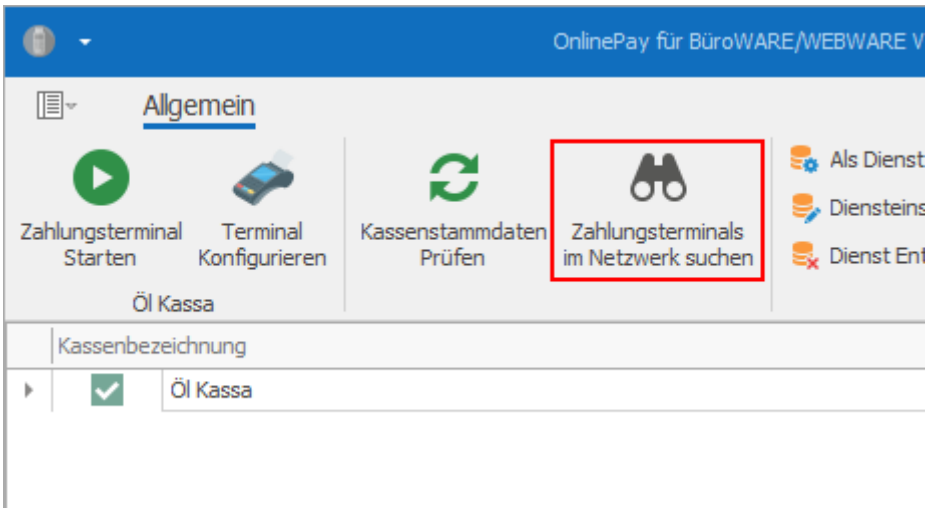
Name	Wert	Beschreibung
Kasse	01	Kassennummer (01-99)
Kassenname	Kassa1 Hobex	Bezeichnung der Kasse
Mandantenpfad	C:\BWERP\KassaBW_6.0\DAT00003	Mandantenpfad zur SoftENGINE Handelskasse
IOPfad	c:\BWERP\APP.PhoenixDS\Online-Pay\INOUT\	Datenpfad für die SoftENGINE Kasse (Einzusteller
Aktiv	☑	Aktiviert die BüroWARE/WEBWARE Anbindung zu
Terminalprotokoll	Hobex ZVT	Das zu verwendete protokoll für das Zahlungsterr
Verbindungsart	TCP/IP	Wie wird das Zahlungsterminal angebunden TCP-IP oder seriell
IP-Adresse	10.10.10.141	IP-Adresse die das Zahlungsterminal im Netzwerk
Port	20007	TCP-IP Port an dem das Zahlungsterminal erreichb 5577...
Serieller Anschluss	1	COM-Anschlussnummer für das Zahlungsterminal
Baud	9600	Serielle Schnittstellengeschwindigkeit (9600, 1920
Stop Bits	2	0-2 0=keine, 1=ein StopBit, 2=zwei StopBits
Initialisierungspasswort		Terminalkennwort für die Initialisierung (5-6 Stelle
Registrierungspasswort		Terminalkennwort für die Registrierung (5-6 Stelle
Autorisierungspasswort für Gutschriften	000000	Kennwort für das autorisieren von Gutschriften (r
Timeout 1	5000	Timeout 1 für das ZVT-Terminal (nur HobexZVT) Standardwert: 5000
Timeout 2	180000	Timeout 2 für das ZVT-Terminal (nur HobexZVT) Standardwert: 180000

TCP/IP

für die Anbindung per TCP muss die Verbindungsart auf TCP/IP umgestellt werden (Online Pay startet sich dabei neu)
Ist die IP Adresse und der Port des Terminals bekannt, können diese Daten direkt eingetragen werden.

	Verbindungsart	TCP/IP	Wie wird das Zahlungsterminal angebunden TCP-IP oder seriell
	IP-Adresse	192.168.0.5	IP-Adresse die das Zahlungsterminal im Netzwerk erhalten hat
123	Port	20007	TCP-IP Port an dem das Zahlungsterminal erreichbar ist. z.B. 20007, 557
123	Serieller Anschluss	6	COM-Anschlussnummer für das Zahlungsterminal (1-99)
123	Baud	9600	Serielle Schnittstellengeschwindigkeit (9600, 19200,115200...)
123	Stop Bits	2	0-2 0=keine, 1=ein StopBit, 2=zwei StopBits

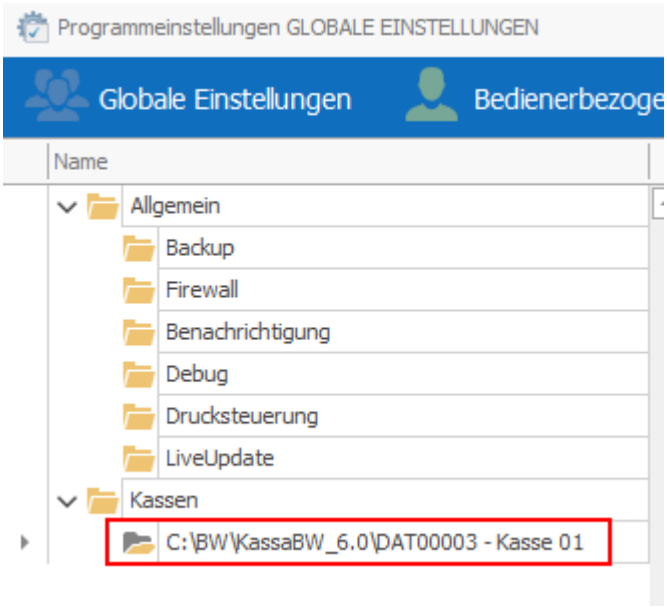
Online Pay bietet aber auch die Möglichkeit, Zahlungsterminals im Netzwerk zu suchen und die Schnittstelle darauf einzustellen. Verlassen Sie hierfür die Einstellungen und starten Sie über das Fernglas "Zahlungsterminals im Netzwerk suchen" den entsprechenden Assistenten.



Der Assistent führt Sie durch die Suche. Es können immer nur 254 IP-Adressen durchsucht werden. Natürlich können auch externe Netzwerkscanner verwendet werden, um vorhandene Terminals zu finden.

RS-232

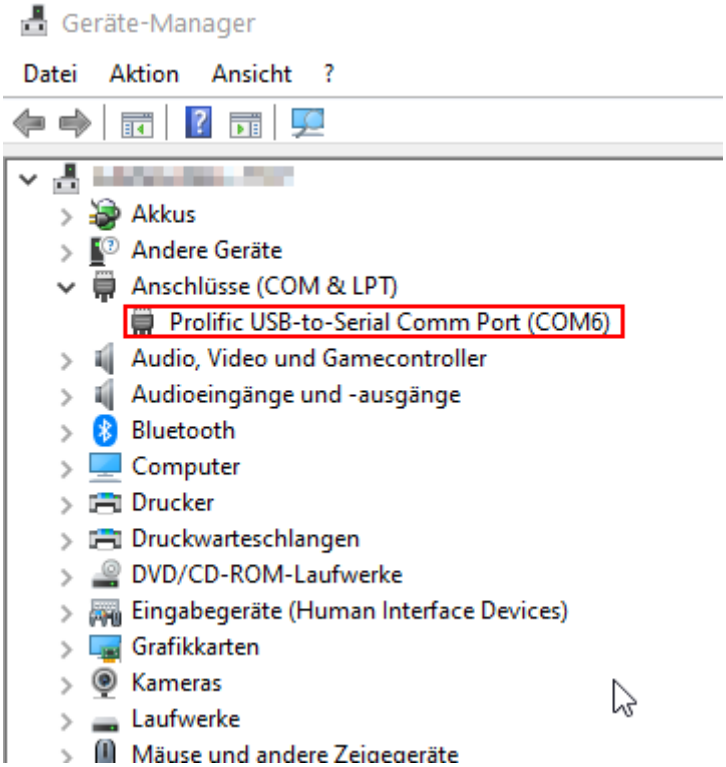
Soll das Terminal über eine serielle Schnittstelle /RS-232 angebunden werden, navigieren Sie in die Einstellungen der Kassa:

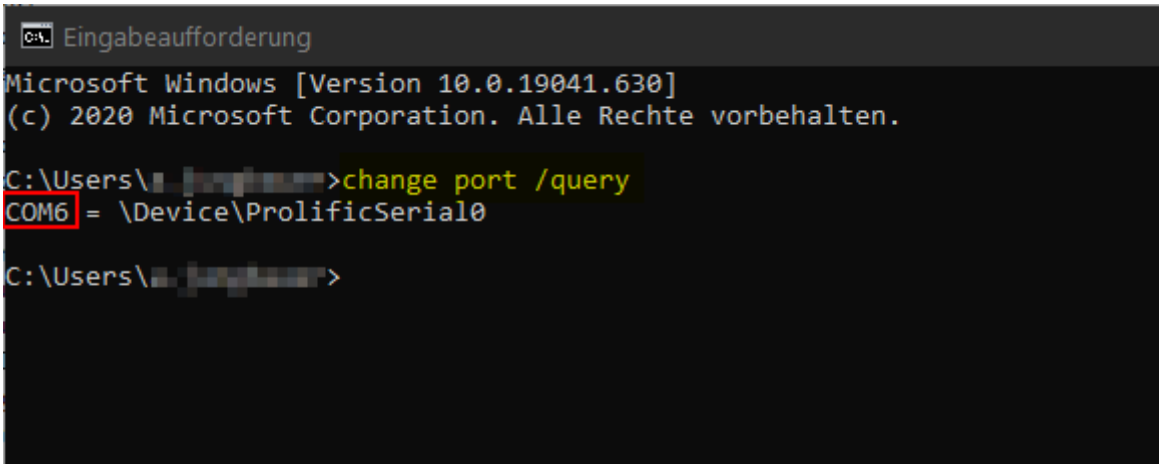


Dort muss die Verbindungsart auf "Seriell" gestellt werden, außerdem der verwendete COM-Port mit der entsprechenden Baud-Rate und der Anzahl der Stopbits konfiguriert werden.

Aktiv	☑
Terminalprotokoll	ZVT
Verbindungsart	Seriell
IP-Adresse	
Port	20007
Serieller Anschluss	6
Baud	9600
Stop Bits	2

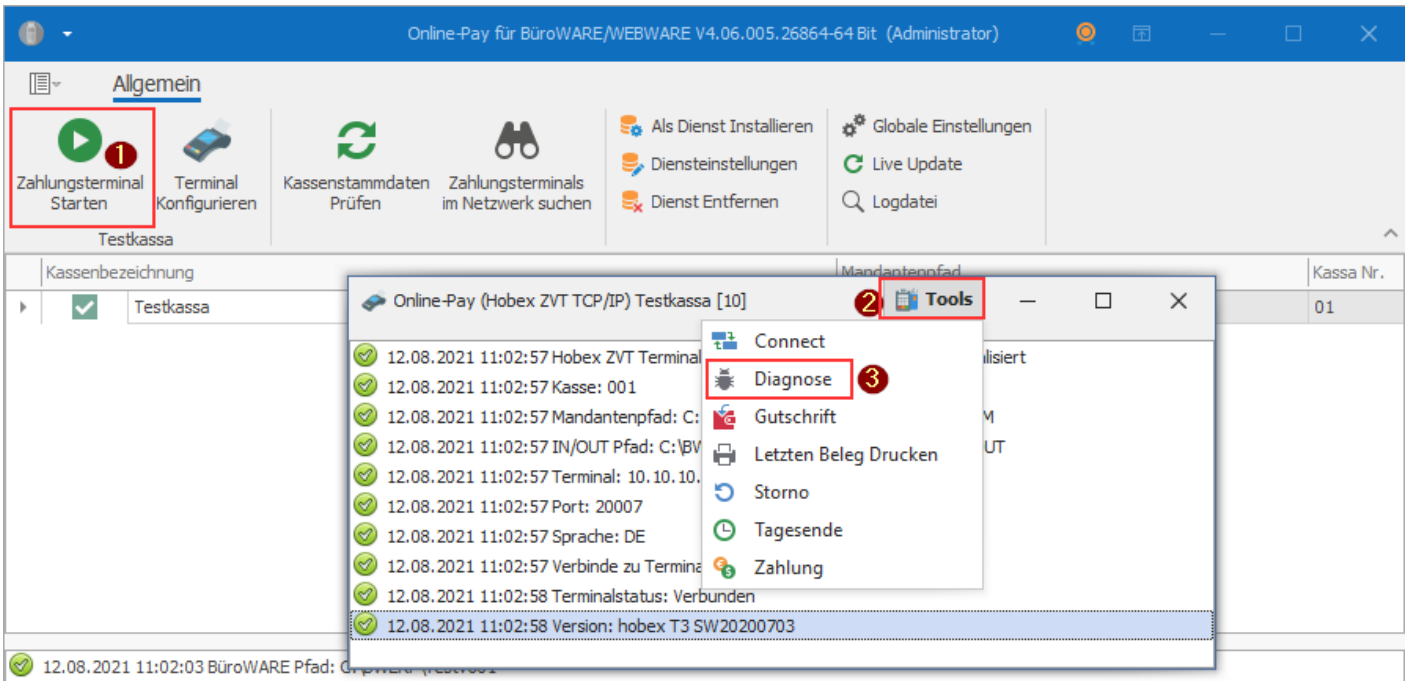
Welcher COM-Port verwendet wird, kann über den Gerätemanager oder den Konsolenbefehl change port /query herausgefunden werden.

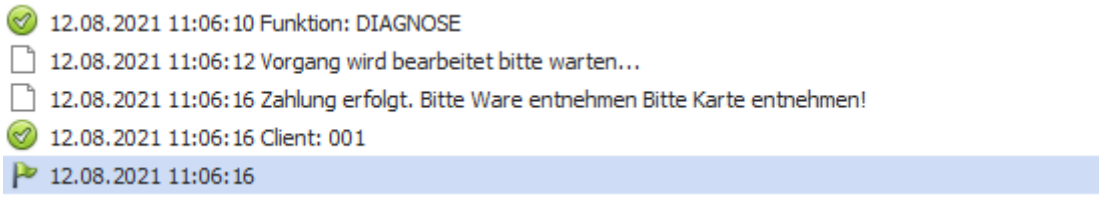




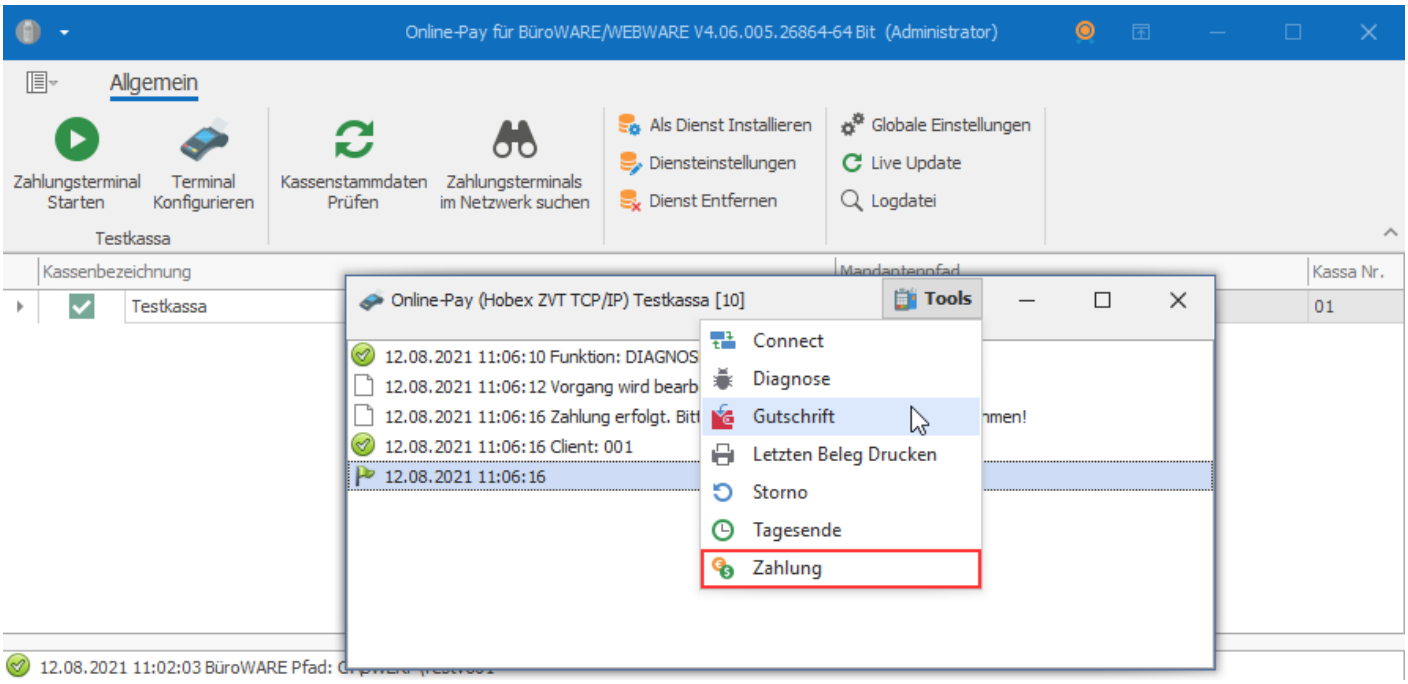
OnlinePay testen

Starten Sie die Schnittstelle der jew. Kassa in der Applikation und führen Sie eine Diagnose durch:





Hier sollten keine Fehler = roten Einträge auftauchen.
Starten Sie über die Online Pay-Applikation einen Zahlungsvorgang:



hierbei wird eine Zahlung über 1 € an das Terminal gesendet.

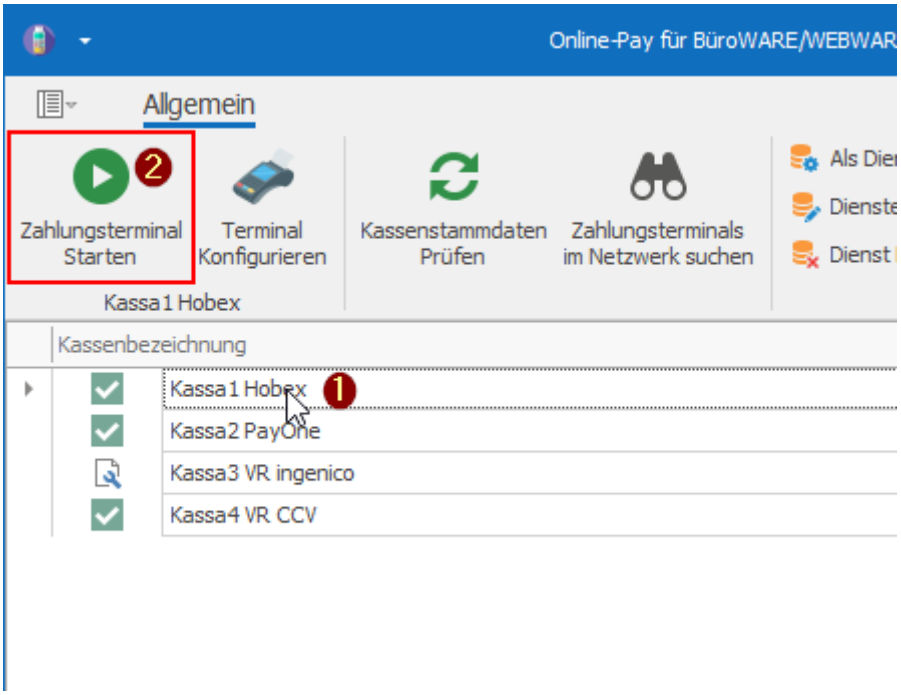
bei erfolgreicher Zahlung kommt vom Bankomatterminal eine entsprechende Rückmeldung, die auch in der Schnittstelle angezeigt wird.
Im letzten Schritt sollten die Vorgänge von der SoftENGINE Kassa aus getestet werden.

1. Starten Sie über Kassendesktop - Einstellungen eine elPAY Diagnose
2. Die Rückmeldung vom Terminal sollte nun auf dem richtigen Drucker ausgedruckt werden
3. Kassieren Sie in der Kassa einen Testbeleg und führen Sie eine Bankomatzahlung durch
4. Die Zahlung sollte am Bankomaten aufgerufen werden und nach erfolgreichem Abschluss auch an die Kassa zurückgegeben werden. Die Bankomatbons sollten auf dem eingestellten Drucker ausgedruckt werden.

OnlinePay verwenden

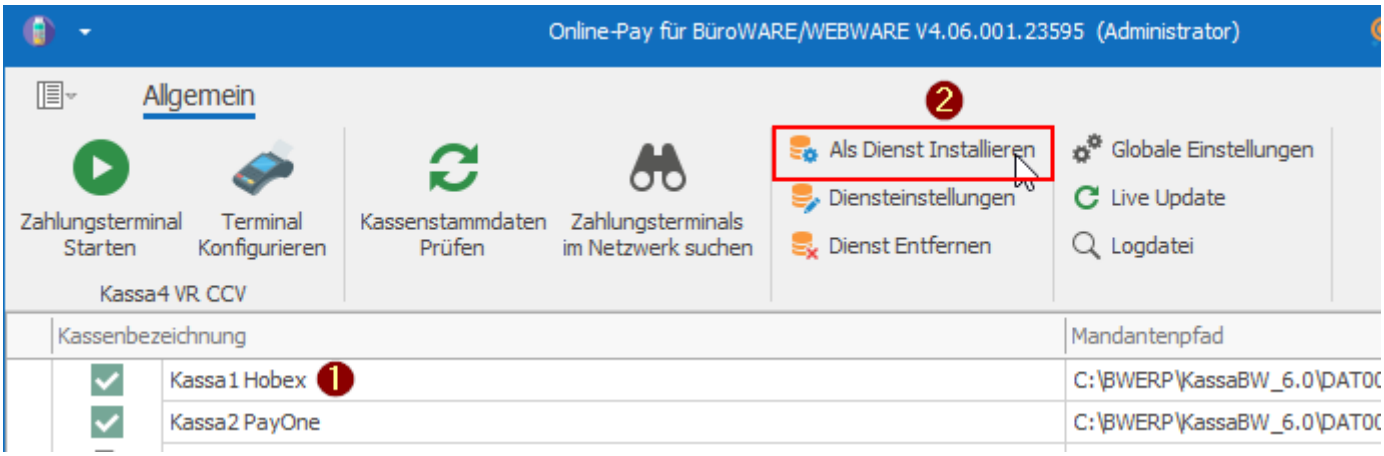
Wenn die OnlinePay Bankomatschnittstelle soweit erfolgreich eingerichtet und getestet worden ist, kann sie für den Produktiveinsatz gestartet werden.
Das ist entweder als Applikation oder als Dienst möglich.

Zum Start der Applikation einfach die jeweilige Kassa auswählen und über den grünen Pfeil starten.

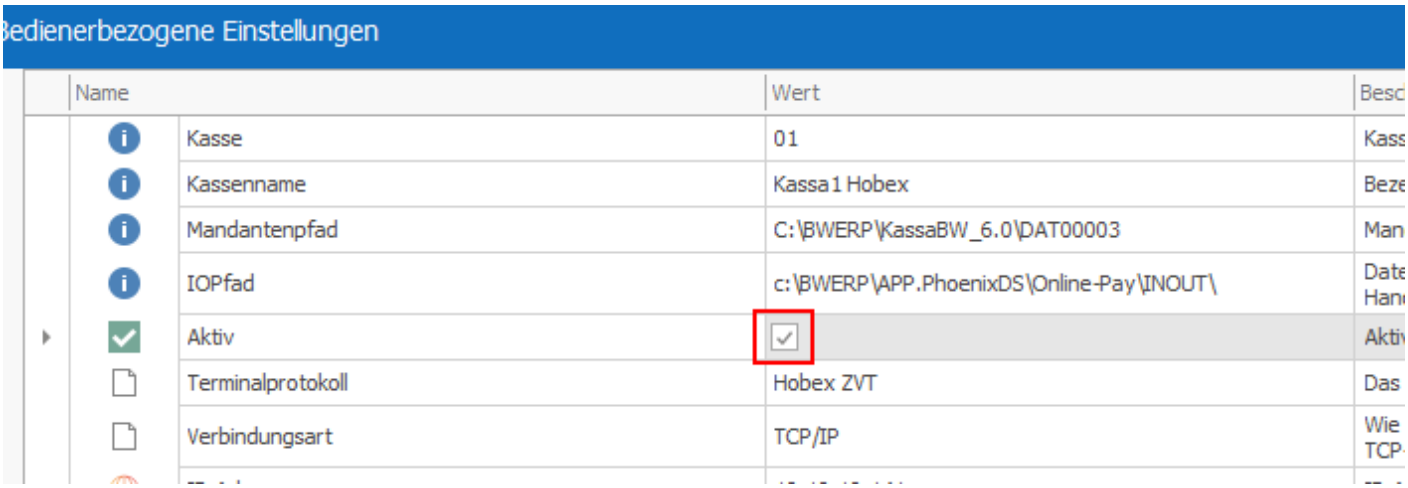


Jede Kassa muss einzeln gestartet werden.

alternativ kann OnlinePay als Dienst installiert werden.
Hierbei muss einfach "Als Dienst Installieren" ausgewählt werden. Der Dienst wird standardmäßig unter der Bezeichnung "SoftENGINE Online-Pay Service" installiert.



Der Dienst beinhaltet immer alle aktiven Kassen. Soll eine Kassa nicht mitgestartet werden, kann dies in den Kasseneinstellungen festgelegt werden:



Hier muss das Häkchen "aktiv" entfernt werden.

Wichtig

die selbe Kassa darf nicht zugleich als Dienst und Applikation laufen/gestartet werden!

getestete Terminals/Anbieter

Anbieter	Terminal	funktioniert	Einschränkungen	Ticket/Partner/Kunde
Hobex		ja		mehrere
telecash	CCV Plus Mobile A960	ja	Rückmeldung vom Terminal dauert länger wegen Cloudupload des Zahlungsbelegs	**#11102** Partner: Comfuse 02.2026
telecash	clover flex 4	nein		Partner: Comfuse 12.2025

Online-Pay Tray

Über das Zusatztool "Online-Pay Tray.exe" kann die Schnittstelle auch Admin-Zugang auf dem Server direkt mit dem Windowsbenutzer der Kassa gesteuert werden.

Funktionen

Online-Pay Tray stellt dabei folgende Funktionen zur Verfügung:

- aktuelle Kartenzahlung abbrechen: wenn das Terminal blockiert ist bzw. keine Rückmeldung an die Kassa erfolgt, legt Online-Pay ein Outfile mit Fehlercode an, damit die aktuelle Zahlung auch vor erreichen des 5-min Timeouts der SoftENGINE Kassa abgebrochen und ggf. neu gestartet werden kann.
- Infopanel mit Terminalstatus
- Terminalfunktionen wie Initialisierung, Diagnose und Kassenabschluss

Konfiguration

Wie kann das Zusatztool “Online-PayTray.exe” konfiguriert werden?

1. Starten Sie im Programmordner der Schnittstelle bei dem entsprechenden Windows-User das Programm Online-PayTray.exe

AD_4nXeLyJ3iBpENY7B2Xm8FVgL4KI

Nach dem Starten befindet sich dieses Tool in der Taskleiste ganz rechts unten im Tray-Bereich:

AD_4nXfNwwbVbEsQ›

Klicken Sie mit der rechten Maustaste auf das Symbol und dann mit der linken Maustaste auf “Einstellungen”

AD_4nXcBDHnDuM_ozUlhwTSicRN-_0(

Anschließend öffnen sich die Einstellungen und sie können die gewünschte Kasse für den angemeldeten Windows-User einstellen.
AD_4nXcceKx7Fu0RYQ25f9TpC3DCdDcUC4a-38YHRXv3XNBb6tJ6g_aWEwMW1n55WszNeXenwYl

Wichtig: Die Einstellungen sind IMMER mit dem aktuellen Windows Anmeldebenutzer verknüpft.

Um auch aktive Informationen über den aktuellen Status des Terminals zu erhalten, können Sie den Verbindungsserver aktivieren.
Mit einem Klick (linke Maustaste) auf das Symbol können Sie die Infomaske öffnen, wenn der direkte Verbindungsserver für diese Kasse aktiviert wurde.
AD_4nXfMXXyM43bVJ1g6FzsPzecboNXta0f229h_TEJThPRovJ1KuAn9QT-5m-5pIAxubQgEg6_uvHs

Dieser ist pro Kasse freizuschalten und per 23.07.2024 noch im Betastatus.
Öffnen Sie dazu die globalen Einstellungen und wählen Sie unter der gewünschten Kasse die Toolbox-Einstellungen aus.
Aktivieren Sie hier den “Direkten Verbindungsserver”.
Sollte der Dienst oder die Toolbox bereits laufen, ist ein Neustart des Online-Pay Dienstes über den Windows Dienstmanager und der damit verbundenen Toolbox (Online-PayTray.exe) erforderlich.

AD_4nXc4JV8aCO-I3IdIz27zZJqSRFrwDQlDMMY9aHtrsD4yJFNRyFMuq8uqJHUbBjgyKR47YjtZGG3

Die Toolbox benötigt hierfür keine weiteren Einstellungen und übernimmt diese automatisch.

Hinweise/bekannte Probleme:
Wenn der Verbindungsserver neu gestartet wird, muss die Oberfläche der Toolbox einmal beendet und wieder geöffnet werden, damit die geänderten Einstellungen übernommen werden.

Übersicht der Einstellungen

Hier werden die wichtigsten Einstellungen für OnlinePay erläutert. Änderungen werden jeweils nach einem Neustart der Schnittstelle (als App bzw. Dienst) berücksichtigt.

Globale Einstellungen

...

Terminal

Serviceart

Über die Serviceart wird definiert, wie OnlinePay die Infiles aus dem Kassensystem im INOUT-Ordner erkennt.

Eventgesteuert - Modus Change (Standard): OnlinePay prüft den Change-Timestamp der Infile.XXX-Dateien. Es werden nur Infiles mit "jüngeren" Änderungszeitstempel verarbeitetet, ältere werden ignoriert und im Log protokolliert.

Eventgesteuert - Modus Create: OnlinePay prüft den Create-Timestamp der Infile.XXX-Dateien. Es werden nur Infiles mit "jüngeren" Erstellungszeitstempel verarbeitetet, ältere werden ignoriert und im Log protokolliert. Abhängig vom System cached Windows uU. die Erstellungszeit kürzlich gelöschter Dateien und setzt diese auch für neu erstellte Dateien mit dem gleichen Namen. In dem Fall sollte die Serviceart "Modus Change" verwendet werden.

Zeitgesteuert: OnlinePay prüft unabhängig von den Timestamps alle 0,1 Sekunden auf vorhandene Infiles und verarbeitet diese.

Voraussetzungen und FAQ

Die OnlinePay Bankomatschnittstelle von ERP Austria ermöglicht ein Zusammenspiel Ihrer SoftENGINE Kassa 4.x mit
einem ZVT-fähigen Bankomatterminal. An dieser Stelle sollen einige häufig gestellte Fragen beantwortet werden.

Voraussetzungen:

In der Kassa (BW Kassa 4.x) muss die Option „Online Pay“ lizenziert sein.
Das Terminal muss vorweg im Netzwerk mit einer statischen IP-Adresse eingerichtet werden,
die Terminalkennwörter müssen für die Installation bereitgehalten werden - diese erhalten Sie vom Provider.

Einrichtung

Wir unterstützen Sie gerne bei der Ersteinrichtung , die Installation und Anbindung an Kassa und Bankomatterminal
inkl. Tests ist üblicherweise in ca. 30-45 Minuten erledigt. Dabei wird die OnlinePay Schnittstelle installiert, die Verbindung
zum Terminal hergestellt, weitere Einstellungen zur Anbindung an die Kassa vorgenommen und einige Tests durchgeführt.
OnlinePay wird dabei üblicherweise direkt am Terminal-/BüroWARE-Server installiert, bei Betrieb von lokal installierten
Kassen wird die Schnittstelle auf den einzelnen PCs eingerichtet.

Kosten

Verrechnung pro Monat und Terminal per SEPA Einzug und jährlich möglich.
Kündbar schriftlich 3 Monate vor Jahresende.
Die Anzahl der Lizenzen richtet sich nach der Anzahl der Bankomatterminals .
4 Kassen und insg. 1 Bankomatterminal = 1 Lizenz
4 Kassen und 4 Terminals = 4 Lizenzen
OnlinePay kann sowohl am Terminalserver als auch für zB. Standalone Kassen direkt auf dem Kassen-PC eingerichtet
werden.
Bei Interesse senden wir Ihnen gerne ein konkretes Angebot.

Demoversion/Testmodus

Die Verbindung zu vorhandenen Terminals kann vorweg auch ohne OnlinePay-Lizenz getestet werden (eingeschränkter
Funktionsumfang)

Verwendbare Geräte/Anbieter

Grundvoraussetzung ist ein ZVT-fähiges Bankomatterminal (zB. ingenico Desk/3500, yomani touch XR PINPAD), das per
TCP/IP (LAN/WLAN) oder COM an den Kassen-PC oder Server angebunden werden kann. Vom Zahlungsanbieter
bekommen Sie normalerweise ein aktuelles Terminal angeboten.
Zu den folgenden Anbietern gibt es bereits zertifizierte Anbindungen oder erfolgreiche Tests:

- hobex (zertifiziert)
- VR Pay
- PayONE/SIX (zertifiziert)
- Global Payments (zertifiziert)

Für Kunden in AT würden wir hobex empfehlen .
Generell sind auch Anbindungen zu anderen Terminals/Anbietern möglich, diese müssten von Ihnen getestet werden.
(auch ohne Lizenz, aber mit eingeschränktem Funktionsumfang möglich). Die OnlinePay-Schnittstelle wird laufend
weiterentwickelt und bei Bedarf gerne an weitere Terminals/Zahlungsanbieter angebunden.

Umstieg von elPay-Terminals

Wichtig: PayONE lässt den Support für die alte elPay-Schnittstelle auf. Vorhandene Terminals können zwar noch verwendet werden, ein Umstieg auf ein neues ZVT-fähiges Terminal ist hier aber sinnvoll. Dieses kann ebenfalls über PayONE oder einen alternativen Anbieter wie hobex bezogen werden.

Was muss ich bei einem SumUp Zahlungsterminal einstellen?

SumUp-Terminal in PhoenixDS Online-Pay

Zweck dieser Dokumentation

Diese Anleitung beschreibt die Einrichtung eines **SumUp Solo** oder **Virtual Solo** in **PhoenixDS Online-Pay**.

Die Anbindung erfolgt über die **SumUp Cloud API**. Online-Pay und das SumUp-Terminal kommunizieren daher nicht direkt über eine lokale IP-Adresse miteinander. Beide Geräte benötigen eine funktionierende Internetverbindung.

> **Wichtig:** Für Zahlungen werden ein SumUp-Händlerkonto, ein geheimer API-Key und die für Kartenpräsenz-Zahlungen vorgesehenen Affiliate-Daten benötigt. Die Zugangsdaten müssen vertraulich behandelt werden.

Funktionsprinzip

```
PhoenixDS Online-Pay  ------ HTTPS ------>  SumUp Cloud API
                                                  |
                                                  |
                                                  v
                                        SumUp Solo / Virtual Solo
```

Online-Pay übermittelt die Zahlungsanforderung an SumUp. Die SumUp Cloud leitet sie an den gekoppelten Reader weiter. Das Ergebnis wird anschließend von Online-Pay abgefragt und an das Kassensystem zurückgegeben.

Das SumUp-Terminal muss sich nicht im selben lokalen Netzwerk wie der Online-Pay-Server befinden. Beide Seiten müssen jedoch das Internet erreichen können.

Unterstützte Funktionen

Die aktuelle SumUp-Anbindung unterstützt:

- Zahlung
- Zahlungsablehnung und Abbruch am Terminal
- Abbruch eines laufenden Reader-Checkouts durch Online-Pay
- Diagnose und Reader-Status
- Geräteinformationen
- Kopplung eines Solo oder Virtual Solo

Folgende Vorgänge werden derzeit nicht über die SumUp-Anbindung angeboten:

- Gutschrift
- Storno einer bereits abgeschlossenen Zahlung
- Belegwiederholung
- Tagesabschluss

Diese Funktionen werden in Online-Pay für eine SumUp-Kasse nicht angeboten beziehungsweise mit einer eindeutigen Meldung abgewiesen.

Voraussetzungen

Vor der Einrichtung müssen folgende Voraussetzungen erfüllt sein:

- Ein vollständig eingerichtetes SumUp-Händlerkonto ist vorhanden.
- Ein unterstützter SumUp Solo oder Virtual Solo ist vorhanden beziehungsweise im SumUp-Konto freigeschaltet.
- Online-Pay kann die SumUp Cloud über HTTPS erreichen.
- Das SumUp-Terminal besitzt eine aktive Internetverbindung über WLAN oder Mobilfunk.
- Ein geheimer SumUp API-Key ist vorhanden.
- Affiliate-Key und zugehörige Affiliate-App-ID sind vorhanden.
- Der Reader ist für eine neue API-Kopplung vom bisherigen Benutzerkonto abgemeldet.

> Eine lokale Terminal-IP-Adresse und ein lokaler Terminalport werden für SumUp nicht benötigt.

SumUp API-Key erstellen

Der API-Key gehört zum SumUp-Händlerkonto und erlaubt Online-Pay den Zugriff auf die benötigten SumUp-Funktionen.

1. Im SumUp Dashboard anmelden.
2. Das Profil öffnen und **Einstellungen** auswählen.
3. **Für Entwickler** und anschließend **Toolkit** öffnen.
4. Den Bereich **API Keys** auswählen.
5. Einen neuen geheimen API-Key erstellen und eindeutig benennen, beispielsweise `PhoenixDS Online-Pay`.
6. Den Schlüssel unmittelbar sicher speichern.

> Der im Dashboard angezeigte **Public Key** ist nicht der benötigte API-Key. Für Online-Pay wird der geheime API-Key verwendet, der üblicherweise mit `sup_sk_` beginnt.

SumUp zeigt einen neu erzeugten geheimen Schlüssel möglicherweise nur einmal vollständig an. Geht er verloren, muss ein neuer Schlüssel erstellt und der alte Schlüssel widerrufen werden.

Affiliate-Daten

Für Zahlungen an einem physischen oder virtuellen SumUp-Reader werden zusätzlich benötigt:

- **Affiliate-Key**
- **Affiliate-App-ID**

Diese Daten identifizieren die Kartenpräsenz-Integration gegenüber SumUp. Sie werden von PhoenixDS beziehungsweise im Rahmen der Freigabe durch SumUp bereitgestellt und dürfen nicht durch frei erfundene Werte ersetzt werden.

Allgemeine Kasseneinstellungen in Online-Pay

1. Online-Pay öffnen.
2. Mit der rechten Maustaste auf die gewünschte Kasse klicken.
3. **Zahlungsterminal konfigurieren** auswählen.
4. Die allgemeinen Einstellungen der Kasse öffnen.

Einstellung	Empfohlener Wert	Beschreibung
Aktiv	aktiviert	Aktiviert die Verarbeitung für diese Kasse.
Terminalprotokoll	`SumUp`	Verwendet die SumUp Cloud API.
Verbindungsart	ohne Bedeutung für SumUp	SumUp verwendet immer eine HTTPS-Verbindung zur Cloud.
IP-Adresse	leer beziehungsweise ohne Bedeutung	Für SumUp wird keine lokale Terminal-IP verwendet.
Port	ohne Bedeutung	Für SumUp wird kein lokaler Terminalport verwendet.
Timeout 1	`5000`	Zeitlimit für den Aufbau einer Cloud-Verbindung in Millisekunden.
Timeout 2	`180000`	Maximale Wartezeit für einen Zahlungsvorgang in Millisekunden.
Protokollierung	`Erweitert`	Empfohlen für Einrichtung und Fehleranalyse.
Sprache	`DE`	Gemeinsame Spracheinstellung der Kasse.
Währung	`EUR`	ISO-Währungscode für Zahlungen.
Zeichensatz/CodePage des Terminals	ohne Bedeutung für SumUp	Die SumUp Cloud API überträgt Daten als Unicode.

Andere Kassen auf demselben Online-Pay-System können weiterhin mit ZVT, PhoenixDS ZVT, Hobex ZVT oder O.P.I. betrieben werden.

SumUp-Einstellungen

Die anbieterspezifischen Einstellungen befinden sich im Unterordner **SumUp Einstellungen** der betreffenden Kasse.

Sie können außerdem in der geöffneten Terminalserver-Oberfläche aufgerufen werden:

- Rechtsklick in die Meldungsliste und **SumUp-Einstellungen und Kopplung** auswählen.
- Alternativ im Menü **Tools** den Eintrag **SumUp-Einstellungen und Kopplung** auswählen.

Beschreibung der Einstellungen

Einstellung	Eingabe	Beschreibung

API-Key	erforderlich	Geheimer API-Key des SumUp-Händlerkontos. Er wird verschlüsselt gespeichert und nicht protokolliert.
Merchant-Code	optional	Händlercode des SumUp-Kontos. Bleibt das Feld leer, versucht Online-Pay ihn automatisch über die SumUp API zu ermitteln.
Reader-ID	automatisch	Eindeutige ID des gekoppelten Readers. Sie wird nach erfolgreicher Kopplung automatisch gespeichert.
Affiliate-Key	für Zahlungen erforderlich	Geheimer Schlüssel für Kartenpräsenz-Zahlungen. Er wird verschlüsselt gespeichert und nicht protokolliert.
Affiliate-App-ID	erforderlich	Zum Affiliate-Key gehörende Anwendungs-ID, beispielsweise `at.phoenixds.onlinepay`. Den von PhoenixDS oder SumUp vorgegebenen Wert verwenden.
Reader-Name	frei wählbar	Bezeichnung des Readers im SumUp-Konto, beispielsweise `PhoenixDS Kasse 01`.
Kopplungscode	nur zur Kopplung	Einmaliger 8- oder 9-stelliger Code, der am Solo oder Virtual Solo angezeigt wird.

> API-Key und Affiliate-Key sind geheime Zugangsdaten. Sie dürfen nicht per unverschlüsselter E-Mail versendet, in Screenshots veröffentlicht oder in Supportprotokolle kopiert werden.

SumUp Reader koppeln

1. Reader vorbereiten

Für die API-Kopplung darf der Solo nicht mit einem Benutzer am SumUp-Konto angemeldet sein.

Falls der Reader bereits angemeldet ist:

1. Das obere Menü am Solo öffnen.
2. **Einstellungen** öffnen.

3. Den Bereich **Über / About** auswählen.
4. Vom bestehenden Konto abmelden.

Anschließend:

1. Den Solo einschalten.
2. Eine Internetverbindung herstellen.
3. **API** auswählen.
4. **Connect / Verbinden** auswählen.
5. Den angezeigten Kopplungscode bereithalten.

Der Kopplungscode ist laut SumUp nur für kurze Zeit gültig. Die Kopplung sollte daher unmittelbar abgeschlossen werden.

2. Kopplung in Online-Pay starten

1. Die betreffende Kasse in Online-Pay öffnen.
2. **SumUp-Einstellungen und Kopplung** aufrufen.
3. API-Key, Affiliate-Key und Affiliate-App-ID kontrollieren.
4. Einen eindeutigen Reader-Namen eintragen.
5. Den am Reader angezeigten Kopplungscode eingeben.
6. **Speichern und koppeln** auswählen.
7. Die Kopplung am SumUp-Gerät bestätigen.
8. In Online-Pay anschließend **Connect** auswählen.

Nach erfolgreichem Start der Kopplung speichert Online-Pay die von SumUp zurückgegebene Reader-ID automatisch. Der verwendete Kopplungscode wird danach aus den Einstellungen entfernt.

> Beim normalen Programm- oder Dienststart wird niemals automatisch ein neuer Reader gekoppelt. Die Kopplung ist eine bewusst ausgelöste Aktion in der Oberfläche.

Verbindung und Zahlung testen

Nach der Kopplung sollte die Inbetriebnahme in folgender Reihenfolge geprüft werden:

1. In Online-Pay **Connect** auswählen.
2. Reader-Status und Geräteinformationen über die Diagnose prüfen.
3. Eine Testzahlung mit einem kleinen Betrag, beispielsweise 1,00 EUR, starten.

4. Eine Zahlung bewusst am Reader abbrechen und die Rückmeldung prüfen.
5. Eine Zahlung erfolgreich durchführen.
6. Kontrollieren, ob Betrag, Ergebnis und Belegnummer korrekt an das Kassensystem zurückgegeben werden.

Das SumUp-Terminal sollte während des Betriebs eingeschaltet, mit dem Internet verbunden und nach Möglichkeit mit Strom versorgt sein.

Netzwerk und Firewall

Online-Pay benötigt eine ausgehende HTTPS-Verbindung zur SumUp Cloud:

Richtung	Quelle	Ziel	Port
Ausgehend	Online-Pay / RDS-Server	`api.sumup.com`	TCP `443`

Es wird kein eingehender Port auf dem RDS-Server für das SumUp-Terminal benötigt.

Falls ein Proxy, Webfilter oder eine Firewall eingesetzt wird, muss die HTTPS-Kommunikation zur SumUp API erlaubt sein. Eine TLS-Auftrennung oder Inhaltsmanipulation durch Sicherheitssoftware kann die Verbindung beeinträchtigen.

Protokolldateien

Die SumUp-Protokolle werden je Kasse unterhalb des Online-Pay-Programmordners gespeichert:

```
<Programmordner>\Log\SumUp\PHXFrameworkSumUp_Kasse001_YYYYMMDD.log
```

Für die Einrichtung und Fehleranalyse sollte die gemeinsame Einstellung **Protokollierung** auf `Erweitert` stehen.

API-Key und Affiliate-Key werden nicht in das Protokoll geschrieben. Identifikatoren und technische Transaktionsangaben können für die Nachverfolgung eines Vorgangs enthalten sein.

Fehlerbehebung

API-Key fehlt oder ist ungültig

Mögliche Ursachen:

- Es wurde versehentlich der öffentliche Schlüssel statt des geheimen API-Keys eingetragen.
- Der API-Key wurde widerrufen.
- Beim Kopieren wurden Zeichen ausgelassen.
- Der Schlüssel gehört nicht zum erwarteten SumUp-Händlerkonto.

Lösung: Im SumUp Dashboard einen gültigen geheimen API-Key kontrollieren oder neu erstellen und anschließend in Online-Pay speichern.

Merchant-Code konnte nicht ermittelt werden

Mögliche Ursachen:

- Der API-Key ist ungültig.
- Das SumUp-Konto ist noch nicht vollständig eingerichtet.
- Der Zugriff zur SumUp API wird blockiert.

Lösung: Zuerst API-Key und Internetverbindung prüfen. Falls erforderlich, den Merchant-Code aus dem SumUp-Konto ausdrücklich in Online-Pay eintragen.

Affiliate-Key oder Affiliate-App-ID fehlt

Ohne gültige Affiliate-Daten kann Online-Pay keine Kartenpräsenz-Zahlung am Reader starten.

Lösung: Die von PhoenixDS beziehungsweise SumUp bereitgestellten Werte vollständig eintragen. Die Affiliate-App-ID darf nicht unabhängig vom zugehörigen Affiliate-Key geändert werden.

Kopplungscode wird nicht akzeptiert

Mögliche Ursachen:

- Der Kopplungscode ist abgelaufen.
- Der Reader ist noch mit einem SumUp-Benutzer angemeldet.
- Der Code wurde falsch eingegeben.
- Reader und Online-Pay haben keine Internetverbindung.

Lösung: Am Reader einen neuen Code erzeugen und die Kopplung innerhalb weniger Minuten erneut durchführen.

Reader-ID fehlt

Ohne Reader-ID ist noch kein Gerät vollständig mit dieser Kasse gekoppelt.

Lösung: Die Kopplung über **SumUp-Einstellungen und Kopplung** durchführen. Die Reader-ID nicht manuell erfinden.

Reader ist gekoppelt, aber nicht erreichbar

Prüfung:

- Ist der Reader eingeschaltet?
- Besteht eine Internetverbindung?
- Ist der Reader im richtigen SumUp-Händlerkonto vorhanden?
- Zeigt das Gerät noch einen Kopplungs- oder Anmeldebildschirm?
- Ist in Online-Pay die zur Kopplung gehörende Reader-ID gespeichert?

Zeitüberschreitung oder unklares Zahlungsergebnis

Wenn eine Zahlungsanforderung bereits von SumUp angenommen wurde und danach die Verbindung abbricht, kann das Ergebnis zunächst unklar sein.

> **Nicht sofort erneut kassieren.** Zuerst den Vorgang im SumUp Dashboard beziehungsweise anhand der im Protokoll enthaltenen Transaktionskennungen prüfen. Dadurch wird eine mögliche Doppelzahlung vermieden.

Der interne Fehlercode `7005` kennzeichnet in der SumUp-Anbindung ein unklares Ergebnis, das manuell überprüft werden muss.

Vorgang wird als „nicht unterstützt“ gemeldet

Gutschrift, Storno einer abgeschlossenen Zahlung, Belegwiederholung und Tagesabschluss sind in der aktuellen SumUp-Anbindung nicht umgesetzt. Für diese Vorgänge muss der vorgesehene Ablauf im SumUp Dashboard beziehungsweise nach Vorgabe des Zahlungsdienstleisters verwendet werden.

Test- und Produktivbetrieb

SumUp bietet für API-Tests ein Sandbox-Händlerkonto an. Die Sandbox verarbeitet keine echten Zahlungen. Sie ersetzt jedoch nicht in jedem Fall das Verhalten eines realen oder von SumUp bereitgestellten virtuellen Readers.

Vor dem Produktivbetrieb müssen deshalb mindestens folgende Fälle mit dem vorgesehenen SumUp-Gerät getestet werden:

- erfolgreiche Zahlung
- abgelehnte Zahlung
- Abbruch am Terminal
- Verbindungsunterbrechung während einer Zahlung
- Verhalten bei Zeitüberschreitung
- Wiederanlauf von Online-Pay und Reader

Abnahmecheckliste

- ☐ SumUp-Händlerkonto ist vollständig eingerichtet.
- ☐ Geheimer API-Key wurde erstellt und sicher hinterlegt.
- ☐ Affiliate-Key und Affiliate-App-ID sind vorhanden.
- ☐ Online-Pay kann `api.sumup.com` über HTTPS erreichen.
- ☐ SumUp-Terminal besitzt eine stabile Internetverbindung.
- ☐ Terminalprotokoll der Kasse steht auf `SumUp`.
- ☐ Währung ist korrekt eingestellt, beispielsweise `EUR`.
- ☐ Reader-Name ist eindeutig.

- [ ] Reader wurde über einen aktuellen Kopplungscode gekoppelt.
- [ ] Reader-ID wurde automatisch gespeichert.
- [ ] Diagnose und Reader-Status funktionieren.
- [ ] Erfolgreiche Zahlung wurde getestet.
- [ ] Ablehnung und Zahlungsabbruch wurden getestet.
- [ ] Vorgehen bei einem unklaren Zahlungsergebnis ist bekannt.
- [ ] Erweiterte Protokollierung wurde während der Abnahme geprüft.

Sicherheitshinweise

- API-Key und Affiliate-Key wie Passwörter behandeln.
- Schlüssel niemals in Tickets, Screenshots oder normalen E-Mails veröffentlichen.
- Bei Verdacht auf Offenlegung den betreffenden Schlüssel unverzüglich widerrufen und ersetzen.
- Nur berechtigten Mitarbeitern Zugriff auf die SumUp-Einstellungen geben.
- SumUp Dashboard und hinterlegte Transaktionen regelmäßig kontrollieren.

Weiterführende Informationen

- SumUp – Autorisierungsverfahren
- SumUp – API-Keys erstellen und schützen
- SumUp – Solo über die Cloud API anbinden
- SumUp – Reader API

Die verfügbaren Funktionen und Freigabeanforderungen können sich durch Änderungen bei SumUp verändern. Bei einer Neueinrichtung sollten die aktuellen SumUp-Unterlagen geprüft werden.

Was muss ich bei einem Zahlungsterminal mit O.P.I. Schnittstelle einstellen?

O.P.I.-Zahlungsterminal in PhoenixDS Online-Pay

Zweck dieser Dokumentation

Diese Anleitung beschreibt die Einrichtung eines Zahlungsterminals über die O.P.I.-Schnittstelle in **PhoenixDS Online-Pay**.

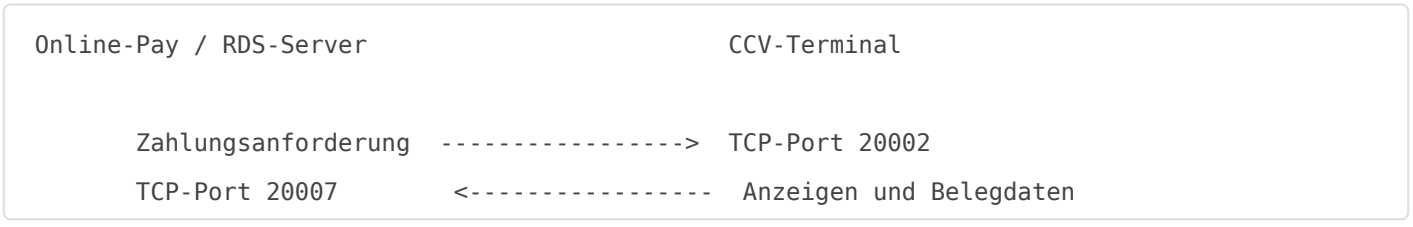
Als Beispiel wird ein **CCV Pad Next** verwendet. Die genaue Bezeichnung der Menüpunkte am Terminal kann abhängig von Firmware, Netzbetreiber und Terminalkonfiguration abweichen.

> **Wichtig:** Die O.P.I.-Funktion muss am Terminal beziehungsweise durch CCV oder den Netzbetreiber freigeschaltet und eingerichtet sein. Die Konfiguration in Online-Pay allein aktiviert O.P.I. nicht am Terminal.

Funktionsprinzip

O.P.I. verwendet zwei getrennte TCP-Verbindungen:

1. **Befehlskanal:** Online-Pay verbindet sich mit dem Zahlungsterminal.
2. **Rückkanal:** Das Zahlungsterminal verbindet sich zurück mit Online-Pay auf dem RDS-Server.



Für eine funktionierende Verbindung müssen beide Kommunikationsrichtungen im Netzwerk und in der Firewall freigegeben sein.

Beispielkonfiguration

Komponente	Beispielwert
IP-Adresse des CCV-Terminals	`10.10.10.140`
IP-Adresse des RDS-Servers	beispielsweise `10.10.10.10`
O.P.I.-Befehlsport am Terminal	`20002`
O.P.I.-Rückkanal-Port in Online-Pay	`20007`
Kasse	`01`
Workstation-ID	`01`

> Die im Online-Pay-Protokoll angezeigte Adresse `127.0.0.1` mit einem zufälligen hohen Port gehört zur internen Kommunikation von Online-Pay. Sie ist nicht der O.P.I.-Port des Terminals.

Voraussetzungen

Vor der Einrichtung müssen folgende Voraussetzungen erfüllt sein:

- Das CCV-Terminal ist für O.P.I. freigeschaltet.
- Terminal und RDS-Server können sich gegenseitig über das Netzwerk erreichen.
- Das Terminal besitzt nach Möglichkeit eine feste IP-Adresse oder eine feste DHCP-Zuordnung.
- Der O.P.I.-Befehlsport des Terminals ist bekannt. Beim CCV Pad Next ist dies häufig `20002`.
- Der Rückkanal des Terminals ist auf die IP-Adresse des RDS-Servers und den vorgesehenen Rückkanal-Port eingestellt.
- Die Windows-Firewall erlaubt die benötigten Verbindungen.
- Bei mehreren Kassen wird für jede gleichzeitig aktive Kasse ein eigener Rückkanal-Port verwendet.

Vorbereitung des CCV-Terminals

Am Terminal oder durch den zuständigen Netzbetreiber müssen mindestens folgende Werte eingerichtet werden:

Einstellung am Terminal	Beispiel	Bedeutung

Schnittstelle	O.P.I.	Aktiviert die Kassenanbindung über O.P.I.
Befehlskanal / Port	`20002`	Port, auf dem das Terminal Anforderungen von Online-Pay annimmt
Zieladresse des Rückkanals	IP-Adresse des RDS-Servers	Adresse, zu der das Terminal Anzeigen und Belegdaten sendet
Rückkanal-Port	`20007`	Muss mit der Einstellung in Online-Pay übereinstimmen
Workstation-ID	`01`	Kennung der zugeordneten Kasse

Die Änderung dieser Werte kann sich im geschützten Servicebereich des Terminals befinden. Falls die Einstellungen nicht sichtbar sind, muss CCV, der Terminalbetreuer oder der Netzbetreiber die O.P.I.-Konfiguration durchführen.

Einrichtung in Online-Pay

1. Online-Pay öffnen.
2. Mit der rechten Maustaste auf die gewünschte Kasse klicken.
3. **Zahlungsterminal konfigurieren** auswählen.
4. Zuerst die allgemeinen Kasseneinstellungen bearbeiten.
5. Anschließend den Unterordner **O.P.I. Einstellungen** öffnen.

Allgemeine Kasseneinstellungen

Einstellung	Empfohlener Wert für das Beispiel	Beschreibung
Aktiv	aktiviert	Aktiviert die Verarbeitung für diese Kasse.
Terminalprotokoll	`O.P.I.`	Verwendet die O.P.I.-Schnittstelle.
Verbindungsart	`TCP/IP`	Verbindung zum Terminal über das Netzwerk.
IP-Adresse	`10.10.10.140`	IP-Adresse des Zahlungsterminals.
Port	`20002`	O.P.I.-Befehlsport des Terminals.
Timeout 1	`5000`	Zeitlimit für den Verbindungsaufbau in Millisekunden.
Timeout 2	`180000`	Maximale Wartezeit für einen Zahlungsvorgang in Millisekunden.

Einstellung	Empfohlener Wert für das Beispiel	Beschreibung
Protokollierung	`Erweitert`	Empfohlen für Einrichtung und Fehleranalyse.
Sprache	`DE`	Sprache für die Kommunikation mit dem Terminal.
Währung	`EUR`	ISO-Währungscode für Zahlungen.
Zeichensatz/CodePage des Terminals	`28591 - Westeuropäisch (ISO)`	Entspricht ISO-8859-1 und ist für das getestete CCV-Terminal erforderlich.

> **Zeichensatz:** Für die getestete CCV-Konfiguration ist `28591 - Westeuropäisch (ISO)` korrekt. Dadurch werden Umlaute in Beleg- und Anzeigetexten richtig verarbeitet.

O.P.I. Einstellungen

Einstellung	Empfohlener Wert für das Beispiel	Beschreibung
Rückkanal-Port	`20007`	Port, auf dem Online-Pay Verbindungen vom Terminal annimmt.
Lokale IP-Adresse	`0.0.0.0`	Online-Pay lauscht auf allen lokalen Netzwerkadressen. Alternativ kann die feste IP-Adresse des RDS-Servers eingetragen werden.
Workstation-ID	`01`	Kassenkennung im O.P.I.-Protokoll. Muss zur Terminalkonfiguration passen.
POP-ID	leer	Optionale Point-of-Payment-ID. Nur eintragen, wenn CCV oder der Netzbetreiber einen Wert vorgibt.
Application-Sender	`PhoenixDS Online-Pay`	Name der sendenden Kassenanwendung.
XML-Namespace verwenden	deaktiviert	Beim getesteten CCV Pad Next muss diese Option deaktiviert sein.
Unterschrift automatisch bestätigen	deaktiviert	Nur aktivieren, wenn ein organisatorisch und technisch abgesicherter Freigabeablauf besteht.
Nachlaufzeit Rückkanal ms	`500`	Kurze Wartezeit, damit abschließende Anzeige- oder Belegdaten übernommen werden können.

Einstellung	Empfohlener Wert für das Beispiel	Beschreibung
Diagnose-Anforderung	`Diagnosis`	Herstellerabhängiger O.P.I.-Befehlsname für die Diagnose.
Tagesabschluss-Anforderung	`ReconciliationWithClosure`	Herstellerabhängiger O.P.I.-Befehlsname für den Tagesabschluss.

> **CCV Pad Next:** Die Option **XML-Namespace verwenden** muss für die getestete Konfiguration deaktiviert sein. Bei aktiviertem Namespace antwortete das Terminal mit `FatalError` und `ParsingError`.

Windows-Firewall und Netzwerk

Für das Beispiel werden folgende Verbindungen benötigt:

Richtung	Quelle	Ziel	TCP-Port
Ausgehend	RDS-Server / Online-Pay	CCV-Terminal	`20002`
Eingehend	CCV-Terminal	RDS-Server / Online-Pay	`20007`

Der eingehende Port muss auf dem RDS-Server in der Windows-Firewall freigegeben sein. Zusätzlich dürfen Netzwerk-Firewalls oder VLAN-Regeln die Kommunikation nicht blockieren.

Mehrere Kassen auf demselben RDS-Server

Jede gleichzeitig aktive O.P.I.-Kasse benötigt einen eigenen Rückkanal-Port.

Kasse	Beispiel Rückkanal-Port
Kasse 01	`20007`
Kasse 02	`20008`
Kasse 03	`20009`

Der jeweilige Port muss sowohl in Online-Pay als auch im zugehörigen Terminal eingetragen und in der Firewall freigegeben werden.

Verbindung testen

Nach dem Speichern der Einstellungen sollte Online-Pay beziehungsweise die betreffende Terminalverbindung neu gestartet werden.

Die Inbetriebnahme sollte in folgender Reihenfolge getestet werden:

1. Anmeldung beziehungsweise Initialisierung des Terminals.
2. Diagnose über das Kontextmenü der Kasse.
3. Testzahlung mit einem kleinen Betrag, beispielsweise 1,00 EUR.
4. Abbruch einer Zahlung am Terminal.
5. Erfolgreiche Zahlung einschließlich Kunden- und Händlerbeleg.
6. Tagesabschluss.

Bei einer erfolgreichen Initialisierung enthält das erweiterte Protokoll unter anderem:

```
PROVIDER PHXFrameworkOPI initialize Command=10.10.10.140:20002 DevicePort=20007
OPI TX <ServiceRequest RequestType="Login" ...>
OPI RX <ServiceResponse ...>
```

Im XML der Anforderung darf für die beschriebene CCV-Konfiguration kein zusätzliches `xmlns`-Attribut enthalten sein.

Protokolldateien

Die O.P.I.-Protokolle werden unterhalb des Online-Pay-Programmordners gespeichert:

```
<Programmordner>\Log\OPI\PHXFrameworkOPI_Kasse001_YYYYMMDD.log
```

Für die Einrichtung und Diagnose sollte die Einstellung **Protokollierung** vorübergehend auf `Erweitert` stehen.

Sensible Kartendaten wie PAN, Track-Daten, PIN-Informationen und Zugangsdaten werden nicht im Klartext protokolliert.

Fehlerbehebung

`FatalError` / `ParsingError`

Mögliche Ursache: Das Terminal kann die gesendete XML-Struktur nicht verarbeiten.

Prüfung:

- **XML-Namespace verwenden** deaktivieren.
- Als Zeichensatz `28591 - Westeuropäisch (ISO)` einstellen.
- Verbindung anschließend neu initialisieren.

Ungültige O.P.I.-Nachrichtenlänge oder negativer Längenwert

Mögliche Ursache: Es wird der falsche Terminalport verwendet oder die Gegenstelle liefert auf diesem Port kein O.P.I.-XML.

Prüfung:

- Für das CCV-Beispiel den Befehlsport `20002` verwenden.
- Nicht den Rückkanal-Port als Befehlsport eintragen.
- Prüfen, ob O.P.I. am Terminal wirklich aktiviert ist.

Keine Verbindung zum Terminal

Mögliche Ursachen:

- IP-Adresse oder Port ist falsch.
- O.P.I. ist am Terminal nicht aktiviert.
- Eine Firewall blockiert den Befehlsport.
- Terminal und RDS-Server befinden sich in getrennten Netzen ohne passende Freigabe.

Zahlung startet, aber Anzeigen oder Belege fehlen

Mögliche Ursache: Der Rückkanal erreicht Online-Pay nicht.

Prüfung:

- Zieladresse des Rückkanals am Terminal kontrollieren.

- Rückkanal-Port am Terminal und in Online-Pay vergleichen.
- Eingehende Windows-Firewall-Regel prüfen.
- Bei mehreren Kassen sicherstellen, dass jeder Rückkanal-Port nur einmal verwendet wird.

Rückkanal-Port ist bereits belegt

Mögliche Ursache: Eine zweite Kasse oder ein anderes Programm verwendet denselben lokalen Port.

Lösung: Für jede O.P.I.-Kasse einen eigenen Rückkanal-Port konfigurieren.

Umlaute werden falsch dargestellt

Prüfung:

- Zeichensatz auf `28591 - Westeuropäisch (ISO)` stellen.
- Beachten, dass eine fehlerhafte Darstellung nur im verwendeten Logreader auftreten kann, obwohl die eigentliche Datei korrekt gespeichert wurde.

Abnahmecheckliste

- ☐ O.P.I. ist am Terminal aktiviert.
- ☐ Terminal-IP-Adresse ist fest vergeben oder reserviert.
- ☐ Befehlsport stimmt mit der Terminalkonfiguration überein.
- ☐ Rückkanal zeigt auf die IP-Adresse des RDS-Servers.
- ☐ Rückkanal-Port stimmt in Terminal und Online-Pay überein.
- ☐ Windows-Firewall erlaubt beide Kommunikationsrichtungen.
- ☐ Workstation-ID ist eindeutig und korrekt zugeordnet.
- ☐ Zeichensatz ist `28591 - Westeuropäisch (ISO)`.
- ☐ XML-Namespace ist für das CCV Pad Next deaktiviert.
- ☐ Anmeldung und Diagnose wurden erfolgreich getestet.
- ☐ Erfolgreiche Zahlung wurde getestet.
- ☐ Zahlungsabbruch wurde getestet.
- ☐ Belegtexte und Umlaute wurden geprüft.
- ☐ Tagesabschluss wurde erfolgreich getestet.

Wichtige Hinweise

- O.P.I.-Details können abhängig von Terminalmodell, Firmware und Netzbetreiber abweichen.
- Die Befehlsnamen für Diagnose und Tagesabschluss sind herstellerabhängig und müssen im Zweifelsfall mit CCV oder dem Netzbetreiber abgestimmt werden.
- Bei einem unklaren Zahlungsergebnis darf eine Zahlung nicht ungeprüft wiederholt werden. Zuerst muss der Status am Terminal beziehungsweise beim Netzbetreiber kontrolliert werden.
- Die beschriebenen Werte bilden die erfolgreich getestete XML-Verarbeitung mit einem CCV-Terminal ab. Zahlung, Storno, Diagnose und Tagesabschluss müssen vor dem Produktivbetrieb vollständig abgenommen werden.

Weiterführende Herstellerinformationen

- CCV Pad Next – Produktinformation
- CCV System Manual mit O.P.I.-Hinweisen

Die vollständige CCV-O.P.I.-Spezifikation ist gegebenenfalls direkt bei CCV anzufordern.